MANUAL DE INFORMÁTICA FORENSE II

(Prueba Indiciaria Informático Forense)

Bases teóricas complementarias.
Metodología suplementaria:
computación móvil (tablet, celulares, iPhone, iPad, iPod, GPS, Mac, imágenes, audio, video, Android, CD, DVD)

INCLUYE DVD CON LA DISTRIBUCIÓN HUEMUL DEL PROYECTO CENTRUX

INCLUYE ACTUALIZACIÓN ON-LINE

María Elena Darahuge
Luis E. Arellano González

Prólogo del Ing. Jorge Omar Del Gener

ERREPAR

María Elena Darahuge Luis E. Arellano González

MANUAL DE INFORMÁTICA FORENSE II

(Prueba Indiciaria Informático Forense)

Bases teóricas complementarias.

Metodología suplementaria: computación móvil (tablet, celulares, iPhone, iPad, iPod, GPS, Mac, imágenes, audio, video, Android, CD, DVD)

Darahuge, María Elena
Manual de Informática Forense II / María Elena Darahuge y Luis Enrique Arellano González. 1a ed. Ciudad Autónoma de Buenos Aires : Errepar, 2014.
E-Book.
ISBN 978-987-01-1682-0
1. Informática. Informática Forense. I. Arellano González, Luis Enrique II. Título
CDD 657.4

Manual de informática forense II Primera edición
ERREPAR S.A.
Paraná 725 (1017) Buenos Aires República Argentina
Tel.: *4370-2002*
Internet: *www.errepar.com*
E-mail: *clientes@errepar.com*
ISBN: 978-987-01-1682-0
Nos interesan sus comentarios sobre la presente obra: editorial@errepar.com

ACTUALIZACIÓN ON-LINE

El contenido del presente libro se actualiza por Internet a través de nuestra página web. Deberá ingresar a www.errepar.com/libros.

Seleccione la presente obra presionando el botón Ingresar, visualizará la siguiente pantalla:

La primera vez que intente consultar el material tendrá que registrarse como usuario, para lo cual se le pedirá que ingrese la clave de de acceso (22462691) y que complete una serie de datos personales.

Tenga presente que es muy importante que ingrese correctamente su dirección de correo electrónico, debido a que allí se le enviará su usuario y contraseña para acceder a los servicios asociados al libro.

Finalmente, presionando el icono correspondiente, tendrá acceso a las actualizaciones de esta obra.

LOS AUTORES

Prof. Ing. María Elena Darahuge

Licenciada e Ingeniera en Informática.

Profesora Universitaria en Ingeniería en Informática, UCSA.

Secretaria Académica del Curso de Experto en Informática Forense, FRA (UTN).

Profesora Asociada de la materia Sistemas Operativos, UAJFK.

Prof. Ing. Luis Enrique Arellano González

Abogado con orientación Penal, UBA.

Licenciado e Ingeniero en Informática.

Profesor Universitario en Ingeniería en Informática y en Criminalística, UCSA.

Licenciado en Criminalística.

Perito en Documentología, Balística y Papiloscopía, IUPFA.

Director del Curso de Experto en Informática Forense, FRA (UTN).

Profesor Asociado de la materia Sistemas Operativos, UAJFK.

PRÓLOGO

Es indiscutible en la Argentina de hoy que la generación de conocimiento científico y de la innovación tecnológica ha tenido un desarrollo sustancial y un creciente reconocimiento en el papel clave que juega para generar respuestas efectivas a los requerimientos de la sociedad; concomitantemente, se ha revalorizado, de manera taxativa, el rol de las políticas públicas para su promoción y se han jerarquizado las instituciones con incumbencias en ese campo.

Indudablemente, no hay problema de conocimiento laboral, médico o de cualquier campo que no se relacione con el desarrollo exitoso de la ciencia y la tecnología. Las herramientas tecnológicas nos permiten hoy explorar nuevos campos y, por su parte, la investigación tecnológica nos permite favorecer y propiciar el desarrollo de software para la aplicación de técnicas científicas y analíticas especializadas que posibilitan identificar, preservar, analizar y presentar datos válidos dentro de un proceso legal, como es el caso de la Informática forense. Esta relación entre los desarrollos de la Universidad Tecnológica Nacional-Facultad Regional Avellaneda y la presente publicación no es más que compartir otro nuevo desarrollo sobre el cual la tecnología echa luz.

El sistema operativo para forenses desarrollado en nuestra Facultad y que hoy se presenta en este ejemplar es el producto de diversos factores que lo han impulsado: los programas de incentivos que favorecen y promueven el desarrollo de software libres, la línea de desarrollo en investigación-acción en la que trabaja nuestra universidad y la definición intrínseca de una institución como la nuestra cuya búsqueda se centra en dar respuesta efectiva a la creciente demanda de conocimiento en las diferentes áreas.

El software libre desarrollado para Informática forense es el primero en habla hispana en esta línea y, sin duda, marca un camino de fortalecimiento de las tecnologías específicas en América Latina. Según diversos críticos, en un futuro cercano no será el inglés la única lengua de la tecnología, evidentemente, han de ser los desarrollos tecnológicos generados en nuestros países los que inicien este proceso de cambio.

Es en esta línea en la cual la tecnología de software libre, como toda tecnología, involucra conocimientos, destrezas, herramientas, recursos y valores cuyo sentido debe centrarse en el compromiso intelectual como inclusión social; en este nuevo orden no nos queda más que dar la bienvenida a un nuevo libro que desde la concepción de libertad nos permite generar conocimiento y ofrecer respuestas a una sociedad mejor y en expansión.

Ing. Jorge Omar Del Gener
Decano Facultad Regional Avellaneda
Universidad Tecnológica Nacional

A calvo ad calvum, bove maiori discit arare minor: fronte praecipitium tergo lupi, ergo a priori, barba stulti discit tonsor.
(Anónimo)

PREFACIO

Superada la instancia de reunir, clasificar, organizar y presentar conceptos constitutivos de la Informática forense, actividad que hemos concretado en el Manual de Informática Forense, con los errores, equívocos y falacias que el mismo pueda contener, ya que es obra de seres humanos y los seres humanos somos falibles, intentamos esta vez complementar aquellos puntos que quedaron poco claros y que luego, a partir de la práctica diaria, las consultas, y en particular los intercambios de opinión, es decir, gracias a la afortunada participación de tantos colegas profesionales, nos inducen a intentar complementar dicha obra.

Diversos problemas se han ido presentando respecto del tratamiento de la Prueba Documental Informática: el rechazo o desestimación de la misma, en diversos fueros, como resultante de errores metodológicos en el proceso de recolección de la prueba indiciaria informático forense, su certificación digital (eventualmente por autoridad competente), la preservación del material recolectado, su traslado y puesta a disposición del tribunal interventor. Estos temas ya han sido tratados en la obra antes referida, no obstante esta carece de una explicación explícita y detallada del procedimiento a realizar para asegurar la cadena de custodia del material probatorio obtenido.

A medida que explicitábamos dicho procedimiento, fueron surgiendo nuevos interrogantes, que ampliaron considerablemente los temas a tratar. Estos interrogantes forman parte de la propuesta académica que ofrecemos a nuestros lectores en la parte teórica que da inicio a la presente obra.

Por supuesto, aún nos restaba trabajar sobre los elementos innovadores que se agregan e integran diariamente a la tecnología informática: computación móvil, celulares, receptáculos de información variados, todos ellos susceptibles de análisis pericial informático forense y, por lo tanto, objeto de recolección de prueba documental informática. En la segunda parte del libro, se ofrecen una serie de procedimientos particulares para los casos más frecuentes. Esperamos que este se constituya en una guía de trabajo útil, para el profesional de la Informática forense que lo requiera y en particular para la formación académica de quienes sientan vocación por integrarse a esta actividad tan propia de este siglo en que vivimos.

Hemos preservado la metodología general de tratamiento teórico y práctico ofrecida en la obra anterior; el lector encontrará sustento para las afirmaciones, considerando los marcos criminalístico, informático (general y específico) y legal. Reiteramos lo expresado anteriormente: estamos seguros de no haber podido realizar una obra adecuada a las pretensiones anteriores, pero también podemos asegurar que, aunque se trata de una propuesta

complementaria, dispersa, con fallas, criticable y perfectible, tiene el valor de ser una propuesta al fin.

ESTRUCTURA GENERAL

La metodología de recolección de prueba indiciaria informático forense
es, al tratamiento de la prueba documental informática ofrecida,
lo que la norma jurídica escrita es a la decisión consagrada
por el Tribunal que juzga (obligación de sentenciar).

Este segundo tomo ha sido planificado y desarrollado con el objeto de aportar al perito informático forense una guía de referencias y consultas rápida, sencilla y fundamentada que complemente los conceptos vertidos en el Manual de Informática Forense.

El primer tomo se sustentaba en la aplicación del método científico, con soporte metodológico sistémico y criminalístico, haciendo uso de tecnología pericial reconocida por su utilidad práctica y en especial en un marco legal estricto e ineludible. En este nuevo volumen, se intentó integrar dichos marcos, para conformar una Metodología Pericial Informático Forense estricta y científicamente fundamentada, la que se concreta en el correspondiente informe pericial.

En esta ampliación doctrinaria, hemos intentado completar los conceptos que establecimos con anterioridad y en especial poner énfasis en los mecanismos alternativos necesarios para el tratamiento de los elementos de computación móvil que nos inundan a diario y se integran a nuestra vida familiar, profesional y social.

Orientación para la lectura del manual

Pensamos que la mejor manera de acercarse a la obra es realizar una lectura detallada del cuerpo principal teórico (es decir de la primera parte). Esto debería ser suficiente para aquellos profesionales que se aproximan a la especialidad forense con fines de obtener conocimientos generales y/o interactuar con otros profesionales, empleando un lenguaje en común, algo de suma utilidad para los operadores del Derecho a la hora de interactuar con la prueba documental informática y sus características específicas. En lo que respecta a los interesados en llevar a la práctica la disciplina informático forense, deberían acceder a la segunda parte (práctica) con el fin de reconocer e implementar, a posteriori, los procedimientos propuestos para los distintos tratamientos de recolección de prueba documental informática, que no forman parte del clásico equipo de computación personal, con el que frecuentemente se trata en la actividad pericial habitual. Todos los documentos que constituyen la obra se encuentran disponibles en su versión digital, para uso de quienes los necesiten y los consideren pertinentes.

Es imprescindible tener en cuenta cuál es el rol del perito dentro del proceso judicial:

1. El perito debe conocer en profundidad el Derecho procesal (de todos y cada uno de los fueros en que participa), en especial si este Derecho procesal pertenece a un país cuya estructura federal lo hace diferente entre los distintos Estados o provincias que lo conforman y delimitan (caso de Argentina), ya que ignorar las normas podría implicar
2. la anulación de la prueba en detrimento del sustento argumental que fuere (todo litigio judicial no es otra cosa que la discusión fundada de una pretensión, a efectos de convencer al juez sobre su validez y pertinencia).
3. El perito no debe opinar sobre el Derecho procesal; para el perito el Derecho procesal es un hecho al que debe acogerse y limitarse, ya que es el marco legal en el que debe desempeñarse. Sin embargo, puede hacerlo como ciudadano, pero en el ámbito que corresponda y por los medios democráticamente vigentes; si la ley no es buena, la solución no es transgredirla, sino modificarla o derogarla: “Dura lex, sed lex”. De ahí la necesidad de especificar claramente su rol dentro del tema en análisis (opinión ciudadana vs. opinión profesional, testimonio vs. testimonio experto).
4. Un perito en funciones no puede ni debe actuar como: juez, detective, cronista, “opinólogo”, difusor mediático, etc. Su función debe limitarse a actuar como testigo experto, limitando su tarea a los resultados fundados (científica, tecnológica y técnicamente) obtenidos a partir de la aplicación de las técnicas periciales de su especialidad sobre los indicios (testigos mudos) obrantes en un determinado lugar (lugar del hecho real o lugar del hecho virtual propio e impropio), que puede o no constituir una escena del crimen, ya que la tarea criminalística se ha expandido desde el Derecho penal a todos los fueros y a todos los ámbitos (empresarial, educativo, laboral, académico, familiar, etc.).

Coincidiendo con la doctrina establecida por los distintos tribunales de EE.UU., consideramos que resulta imposible generar una doctrina y una metodología, particularizadas y personalizadas, para cada tipo de soporte de información posible. El desarrollo científico, tecnológico y técnico, que nos inunda a diario, avanza en progresión geométrica; los mecanismos criminalísticos lo siguen en progresión aritmética, y el Derecho observa todo el proceso desde lejos, sin involucrarse demasiado, hasta que arrollado por la realidad, se ve obligado a adaptarse al cambio y adecuarse a la realidad social en que se encuentra inmerso (firma digital, expediente digital, notificaciones digitales, entre otros temas), produciendo continuas adaptaciones legislativas, reglamentarias o simples acordadas que reducen un poco la distancia cada vez más extensa que separa a la tecnología de uso diario de las normas jurídicas

que deberían regularla.

No es, por lo tanto, posible ni necesario crear un procedimiento para cada nueva tecnología que aparece en el mercado. De ahí que sostenemos con vehemencia que las bases sentadas en el Manual de Informática Forense deben ser sostenidas a ultranza, salvo que sean francamente incompatibles con la nueva tecnología analizada. La prueba documental informática y sus principios deben prevalecer. Los mecanismos de recolección, certificación, traslado, verificación y supervisión deben mantenerse en cuanto a sus principios básicos, agregando únicamente aquellos elementos propios de la nueva tecnología analizada que deban ajustarse para asegurar la preservación y confiabilidad de la documental informática recolectada.

En el campo de los procedimientos, ya no es posible aplicar uno solo a todos los casos posibles “one-size-fits-all”), por el contrario, deben adecuarse los modelos a cada caso en particular, integrando las formas de recolectar y seleccionando el modo pertinente a cada situación planteada, pero respetando los principios criminalísticos, establecidos para el tratamiento de la prueba indiciaria informático forense y su especie la prueba documental informática. El investigador necesita libertad para seleccionar aquellas acciones puntuales que requiere para el caso en particular, pero siempre dentro del marco general del procedimiento válido. Este acto debe ser susceptible de revisión, debate y confrontación con la contraparte, para establecer su pertinencia y validez científica, criminalística e informático forense. El Tribunal debe analizar el problema planteado y decidir, acorde a su evaluación legal, si la prueba obtenida en estos casos mantiene su confiabilidad procesal y puede ser utilizada como elemento de apoyo a la decisión estructura general judicial impuesta al Magistrado que interviene (obligación de dictar sentencia); ante la duda, en el caso de que no pueda ser resuelta por medios técnicos o argumentales científicos, criminalísticos e informático forenses, la prueba obtenida debe ser descartada y declarada nula para el proceso en curso. El patrimonio y la libertad de una persona no pueden estar supeditados al antojo de un profesional, del área que fuere, de ahí la necesidad de seguir los procedimientos estricta y constantemente; el procedimiento es al tratamiento de la prueba documental informática lo que la ley es al Tribunal que juzga.

PRIMERA PARTE
TEORÍA

CAPÍTULO 1
REVISIÓN DE CONCEPTOS

"Probatio est demonstrationis veritas"

La naturaleza pericial de la Informática forense

La Informática forense es a la Informática lo que la Medicina legal es a la Medicina. Esta frase sintetiza y a la vez especifica la complejidad del tema involucrado en la definición que pretende expresar. Desde sus comienzos, la Medicina legal y la Criminalística han desarrollado una metodología general de análisis pericial estandarizada luego de un extenso proceso de desarrollo teórico práctico que les ha dado la eficiencia, eficacia y efectividad[1] que las caracteriza. Se ha conformado por un modo de analizar la prueba indiciaria (testigos mudos) que obran en el lugar del hecho, como consecuencia de las acciones que ocurrieron en el mismo, por la interacción de elementos físicos, lógicos y humanos. A partir de dicho análisis se constituye la llamada "reconstrucción del hecho", cuya finalidad principal es brindar soporte a la decisión judicial (sentencia) que está legalmente obligado a brindar el Tribunal que interviene en cada caso, sea este uni o multi-personal.

En Medicina legal, la historia pericial coincide con la historia humana. Desde los comienzos de esta, la aparición de un cadáver, un herido, un lesionado o un enfermo, indujo a sus congéneres a determinar las causas de dichos resultados perturbadores. La curiosidad, establecida por los griegos como el motor principal de la conducta filosófica humana, evidenciada en el asombro ante la naturaleza, propia de la condición de la especie, no solo con fines intelectuales, sino con intereses prácticos orientados a convertir al mundo en un lugar previsible, ha llevado a nuestros antepasados a intentar conocer las causas de los eventos que se presentaban ante sus ojos. Eventos entre los cuales la afectación en la salud del prójimo es de importancia vital para la seguridad del individuo y del clan al cual pertenece. Es por esto que, aunque no sistematizada, ni en los términos de la moderna Medicina legal, la investigación de la causa de la muerte ha sido preocupación humana consustancial con el desarrollo de la sociedad considerada y enmarcada en cada situación espacio temporal analizada. En el siglo pasado, este desarrollo culmina con figuras de la talla y el peso intelectual de los doctores Emilio Bonnet, Alfredo Achával, Mariano Castex y sus sucesores, como el doctor Osvaldo Raffo, que prolongan su vigencia hasta nuestros días, y han consolidado la estructura científica, metodológica, tecnológica y técnica de dicha especialidad médica integrada de manera transdisciplinaria a las restantes disciplinas criminalísticas.

Por su parte, la Criminalística nacional ha reunido los resultados teórico prácticos de la investigación y experiencia de figuras como Juan Vucetich, Roberto Albarracín, Pedro Lago, Ricardo Rosset, que nos han aportado metodologías de difusión internacional, como el Sistema Dactiloscópico Argentino, o instrumentos de aplicación directa en la investigación pericial, como el escopómetro o el fotocomparador sistema Belaunde. En este marco académico y científico se ha desarrollado el prestigio de nuestras instituciones periciales, que migraron desde su original función de apoyo a la investigación criminal hacia la de soporte de la decisión judicial en todas las jurisdicciones, mediante metodologías y técnicas orientadas al análisis de la prueba indiciaria, enmarcada en el lugar del hecho (delictivo o no) y con la pretensión de brindar un argumento racional compatible con los resultados obtenidos y justificado de manera científica, tecnológica y técnica. Este argumento alcanzado debería constituirse en un elemento más de apoyo a la decisión judicial.

A partir de los antecedentes especificados en los apartados anteriores, se conforma la credibilidad en la prueba pericial, la que se ha constituido en elemento principal en diversas áreas del Derecho, por ejemplo en el denominado derecho al ambiente sano y representado en la investigación de los delitos ambientales. La prueba pericial se conforma de manera propia o en subsidio de otros mecanismos probatorios procesalmente establecidos. Es así que existe una clara dependencia entre la prueba documental clásica bibliográfica y la pericia documentológica (caligráfica), las que aparecen de manera conjunta y relacionada en una gran proporción de litigios judiciales.

La prueba documental informática no es otra cosa más que una especie de la prueba documental clásica (género) y también tiene su correlación pericial en la pericia informático forense. Las similitudes son incontables; a modo de ejemplo:

1. reconstruir un documento en papel a partir de los restos quemados del mismo es una tarea pericial equivalente a la de reconstruir un archivo digital a partir de las trazas obrantes en el disco que lo alojaba antes de ser borrado (en particular, el espacio no asignado);
2. utilizar las marcas de presión escritural sobre hojas en blanco, que obraban bajo el original en el momento de escribir, equivale a rescatar los archivos temporales para recuperar las trazas resultantes de las actividades computacionales realizadas.

Sin embargo, la realidad judicial imperante en esta segunda década del siglo XXI nos hace pensar que allí terminan las similitudes. Mientras que la formación pericial de los peritos en documentología o documentoscopía incluye un conocimiento profundo de la metodología criminalística y de la

inserción legal de la prueba pericial, especialmente vista desde el Derecho procesal vigente, la mayoría de los denominados expertos en Informática forense carecen de dicha formación particular e imprescindible para interactuar ante los estrados judiciales argentinos.

La diferencia radica en el origen de las especialidades consideradas. Mientras los peritos en documentología son una consecuencia del desarrollo armónico y prolongado en el tiempo de las distintas disciplinas periciales criminalísticas, los peritos en Informática forense surgen como una necesidad inmediata e inevitable, estimulada e impulsada por el desarrollo tecnológico informático que evidencia la segunda mitad del siglo pasado. La Informática entra como un huracán y se incorpora a la sociedad y al individuo, modificando sus hábitos, aumentando su radio de acción, reduciendo tiempos y distancias, permitiendo interacciones remotas impensables e insospechables en la primera mitad del siglo referido. Por supuesto, esta modificación social implica una modificación en el modus operandi delictivo y, como respuesta a esta última, se produce el surgimiento de la Informática forense.

Como la tecnología se desplaza en sentido norte-sur y atraviesa el Ecuador con cierta reticencia, las primeras manifestaciones de Informática forense surgen en el hemisferio Norte y en particular de países cuyo sistema judicial está basado en el Common Law y no en la estructura codificada más propia de la Europa continental, que ha constituido la base de nuestro derecho. Si a esta diferencia le agregamos que nuestros referentes europeos más cercanos por historia y afinidad, los españoles, ni siquiera disponen de una tradición universitaria criminalística, el panorama adquiere transparencia. Los recién llegados peritos y expertos en Informática forense, surgen desde cualquier área del conocimiento (administración de empresas, contabilidad, electrónica, sistemas de información, computación y excepcionalmente informática), impulsados por la necesidad de brindar respuesta a la problemática inmediata (“apagar el incendio”, como se dice en la jerga empresarial). Por ejemplo, el contador que requiere de datos borrados para realizar una auditoría contable aprende a utilizar herramientas informático forenses en soporte de su actividad principal. Por supuesto, esta multiplicidad de visiones e intereses multidisciplinarios conforma una situación en la cual la metodología pericial y el encuadre legal de los procedimientos se constituyen en los convidados de piedra del proceso en desarrollo.

A esta situación caótica general, se agregan los intereses de diversas empresas de origen extranjero que desarrollan productos de análisis informático forense llave en mano (las conocidas utilidades computacionales “enlatadas”), adaptadas a los mecanismos, métodos y normativa procesal obrantes en el Common Law y sin ninguna relación con nuestro sistema legal y

mucho menos con nuestra raigambre de análisis pericial criminalístico. Estos enlatados solucionan el problema del momento, pero olvidando un tema principal: la herramienta no puede sustituir al conocimiento. Es decir, aunque pueda proveer a un usuario final el mejor de los procesadores de textos, no puede transmitirle la capacidad de un escritor de renombre (Borges no necesitaba de computadoras para realizar su tarea). Análogamente, por muy prácticos que resulten los enlatados para la labor pericial, se muestran inútiles para suplir la falta de formación profesional legal y criminalística, por parte del profesional que los utiliza.

El empleo de estos productos con fines periciales no solo contribuye a estimular el desinterés por la capacitación permanente de quienes los emplean, que lo hacen a modo de herramienta práctica, sin conocimientos respecto de su operación y estructura operativa. En efecto, al ser vendidos como enlatados, sus componentes, algoritmos, estructuras de datos, metodología, sistemas de búsqueda, en definitiva su concepto de trabajo, se muestran al usuario como una "caja negra", cuya eficiencia, eficacia y efectividad se basa en la confianza que él mismo deposita en la idoneidad profesional de la empresa que lo vende al mercado y en sus desarrolladores. Es imposible corroborar el método utilizado para recolectar la información que luego brinda al usuario, porque forma parte del "secreto comercial", preservado por la empresa y que por supuesto no se ofrece al adquirente. En términos informáticos, no es posible disponer del código fuente de los programas que integran el paquete de Informática forense que se utiliza.

En síntesis, o bien no es posible realizar el análisis crítico de los algoritmos que justifican los resultados obtenidos a partir de la aplicación del "enlatado" utilizado, que solo están disponibles para ciertas instituciones policiales o judiciales propias del país de origen. En ambos casos, resulta en el impedimento práctico de ejercer supervisión y auditoría metodológica y de resultados sobre la prueba presentada como "confiable" a quien está obligado a tomar una decisión judicial (sentencia). Dicho impedimento conforma una clara ruptura del equilibrio judicial de las partes constitucionalmente protegido y preservado a ultranza en el Derecho penal, mediante las normas que reglamentan el debido proceso a que tiene derecho, en nuestro país, todo habitante del mismo (permanente o circunstancial).

Los hechos antes descriptos son claramente contradictorios respecto de la práctica criminalística, ya que una de las necesidades de quien debe utilizar los resultados periciales en apoyo a una decisión que debe tomar (sentencia) reside en la posibilidad cierta de comprobar la forma en que dichos resultados fueron obtenidos. Esta comprobación la puede realizar el juez por sí mismo o por interpósita persona (otro perito de su confianza en la figura del reconocido

amicus curiae) y es una potestad clara de la parte contradictoria en el litigio (actor-demandado, ministerio fiscal-acusado, administrado-administración, según se trate de uno u otro fuero). Este poder de revisión de resultados se denomina genéricamente "auditoría" y consiste en la inspección y evaluación sistemáticas de las operaciones realizadas para comprobar los resultados obtenidos y su correspondencia con el informe pericial presentado. Si no es posible conocer los algoritmos de búsqueda a partir de los cuales se obtienen los datos ofrecidos, la única manera de confiar en su certeza y pertinencia reside en adoptar una actitud de credulidad respecto de esta (efectuar un auténtico acto de fe, indemostrable ante la ignorancia del código fuente que sustenta a la aplicación).

Completando el cuadro, dicha confianza debe ser colocada en cabeza de una empresa extranjera, que utiliza metodología adaptada al Common Law, y sin emplear metodología criminalística alguna, lo que se hace evidente únicamente por los resultados, ya que los algoritmos, como dijimos, son secretos. Esta empresa, por otra parte, no se encuentra radicada en el país y ofrece sus productos por medio de representantes, por lo que no asume responsabilidad alguna sobre los resultados obtenidos a partir de su empleo pericial; ofrece una obligación de medios y no de resultados, la que por otra parte no es reclamable en la práctica, por ninguna vía judicial disponible. Además, exige la formación de operadores capacitados, los que por supuesto deben adquirir dicha capacitación, mediante cursos pagos ofrecidos por la misma empresa, cursos que no implican formación criminalística, ni pericial alguna, y que podrían asimilarse a los cursos de operador de un determinado paquete de ofimática que en nada contribuyen a la capacidad literaria de quien los emplea. Una circunstancia de este tipo no sería tolerada en ninguna otra especialidad criminalística. Si los operadores del Derecho no la utilizan como argumento para solicitar la nulidad de la pericia es simplemente porque no han tenido en cuenta dicha característica violatoria de los principios de transparencia (evidencia demostrable y comprobable) y revisión judicial que toda prueba debe incluir, a efectos de ser confirmada o refutada por la parte que lo desee, utilizando medios científicos, tecnológicos, técnicos y metodológicos similares.

Por otra parte, toda tarea pericial debe ser factible de repetición, por otros expertos y en similares circunstancias. A tales fines, el Código Procesal Penal de la Nación establece claramente la necesidad de repetitividad del acto pericial: "Conservación de objetos. Art. 261. Tanto el juez como los peritos procurarán que las cosas a examinar sean en lo posible conservadas, de modo que la pericia pueda repetirse. Si fuere necesario destruir o alterar los objetos analizados o hubiere discrepancias sobre el modo de conducir las operaciones,

los peritos deberán informar al juez antes de proceder".

Pero si el instrumento utilizado para realizar la pericia consiste en un enlatado, cuya forma de operar aparece oculta tras el secreto comercial, es un producto comercial de alto precio y solo está disponible para quienes dispongan del poder adquisitivo necesario para adquirirlo (rondan los 20.000 dólares por licencia); esto constituye un obstáculo firme e irremovible para los fines de auditoría, pretendidos por quien es perjudicado por el dictamen expedido. Circunstancia absolutamente intolerable dentro del Derecho penal vigente y el debido proceso pretendido y asegurado constitucionalmente.

Si a esto agregamos los desconocimientos operativos que el uso de este tipo de programas estimula en los supuestos expertos, haciendo que ellos ignoren los más básicos principios asociados a la manipulación de la prueba indiciaria informática (por ejemplo, por falta de empleo de bloqueadores de escritura al acceder a los repositorios de información) y de esta manera ocasionando la inmediata contaminación de la prueba recolectada, hecho que es irreversible desde el punto de vista informático, se está produciendo una afectación clara y directa al derecho de defensa del afectado y la igualdad de partes en el proceso judicial en desarrollo, tornando imposible la revisión técnica de la prueba pericial producida.

En oposición a los enlatados, aparecen los desarrollos basados en el denominado "software libre", la mayoría de ellos soportados por el sistema operativo Linux, a partir del cual se han implementado aplicaciones de Informática forense cuyo código fuente es de libre disponibilidad, permitiendo su revisión y auditoría por cualquier persona que cuente con los conocimientos suficientes para utilizarlos. Y, es precisamente en este punto donde se genera el problema, ya que resulta mucho más fácil utilizar un enlatado que genere un resultado a partir de un procedimiento desconocido (un acto de magia tecnológico) que adquirir los conocimientos necesarios para interpretar el código fuente de un programa y analizar la pertinencia de sus algoritmos implícitos y explícitos.

Los profundos errores evidenciados en el tratamiento de la prueba documental informática, que dieran lugar a los recientes fallos declarando la nulidad de la misma, se producen por desconocimiento metodológico criminalístico por parte de quienes la operan. Este desconocimiento es difundido intencional, masiva y popularmente como una circunstancia cuasi delictiva, se deja entrever la existencia de al menos un dolo eventual en la comisión de errores tan notorios como los evidenciados (falta de cadena de custodia, no utilización de bloqueadores de escritura, secuestros de elementos computacionales sin su correspondiente aislamiento instrumental y lógico, etc.) y, sin embargo, es el resultado esperable ante el hecho evidente de

analizar a los peritos involucrados, desde la clásica visión criminalística ya impuesta y consolidada en la justicia y en la sociedad, olvidando la falta de capacitación profesional criminalística y legal, que forman parte consustancial al acerbo operativo de los "expertos", que actuaron como peritos en los procesos sospechados de irregularidad.

Si un médico legista "olvida" mantener la cadena de frío de una muestra biológica, o un perito en documentología omite recolectar elementos indubitados anteriores, posteriores y contemporáneos a la fecha supuesta del documento incriminado, con fines de cotejo, podemos hablar de una actitud claramente indolente, donde el dolo eventual o al menos la culpa con representación parecen surgir de manera espontánea. Sin embargo, si un funcionario policial, cuya única formación pericial ha sido la práctica profesional a la que se ha visto obligado por el desarrollo de los requerimientos judiciales, contando únicamente con un título secundario, sin formación criminalística ni legal alguna, trabajando en una dependencia institucional, que curiosamente no depende del área de Criminalística, sino del área de comunicaciones, comete un error, es muy probable que dicho error sea absolutamente culposo (proveniente de su impericia metodológica, criminalística y legal). Considerado a priori, el resultado alcanzado no solo era posible, sino altamente probable y por supuesto esperable (previsible) con carácter probabilístico de cuasi certeza. El principio general básico indica "primero enseñar y luego evaluar", en este caso podría expresarse como "primero capacitar y luego exigir", algo que no ha ocurrido en el ejemplo particular considerado.

Confiar en el cargo y no exigir idoneidad

Cuando se recibe un informe pericial, correspondiente a una pericia química, realizado por una Fuerza de Seguridad cualquiera (tomemos como ejemplo el caso particular de la Policía Federal Argentina), dicho informe está refrendado por un funcionario policial y a veces convalidado por la firma de quien realizó efectivamente la tarea pericial. Se trata en general de funcionarios distintos, uno ostenta el cargo de Jefe del Laboratorio Químico y el otro es un profesional que ha realizado la tarea encomendada. Sin embargo, más allá de su jerarquía institucional (representada por el grado que aparece en el sello aclaratorio de firma, por ejemplo, Comisario López), estos funcionarios poseen carreras de grado universitarias directamente relacionadas con la tarea que cumplen (licenciados, ingenieros o doctores en Química, entre otras posibilidades). Es decir que los resultados periciales son certificados y avalados no desde el cargo y jerarquía del funcionario que la firma, sino desde su idoneidad profesional certificada en el título universitario que posee (firma el Comisario NN, pero en su condición de Licenciado en

Química, por ejemplo). En el caso particular de la Informática forense, esta circunstancia no ocurre por varias razones:

1. en primer lugar, porque no existen carreras universitarias que aseguren una idoneidad profesional equivalente,
2. en segundo lugar, porque son múltiples los profesionales de diversas áreas del conocimiento que se atribuyen idoneidad propia y capacidades periciales informático forenses[2],
3. en tercer lugar, porque incluso dentro del área informática existe multiplicidad de denominaciones y títulos terciarios de grado y de posgrado (ingenieros, licenciados, doctores, en informática, sistemas de información, computación, computadores científicos, etc.) cuyas diferencias particulares en cuanto a incumbencias no están demasiado claras ni siquiera para los titulares de dichas formaciones profesionales,
4. en cuarto lugar, porque a esto se agrega la costumbre inveterada de los colegios profesionales, tendiente a reunir "matrícula" a cualquier precio, lo que lleva a matricular ingenieros, licenciados, analistas de sistemas y hasta técnicos con formación puramente secundaria, a efectos de incrementar la matrícula y por ende los ingresos del colegio considerado. Luego, con esta matrícula se presentan ante los distintos estrados judiciales y son designados como peritos, basando dicha resolución, precisamente en la falta de reglamentación de la profesión y avalados legalmente por el artículo 464, segunda parte, del Código Procesal Civil y Comercial de la Nación o sus equivalentes procesales para otros fueros[3]. Esta aceptación, sin embargo, se encuentra determinada en la letra de la ley, que establece una excepción particular que no debería ser interpretada en forma extensiva, sino de manera restrictiva. Y aun en el supuesto de que el Tribunal sea restrictivo en cuanto a las designaciones de peritos, no puede impedir la intervención de otros profesionales como "perito de parte, asesor o consultor técnico" a pedido de las partes. Esto genera la increíble circunstancia de que en un mismo acto procesal (por ejemplo, en una audiencia oral en un Tribunal Oral de Sentencia) se reúnan en discusión pericial equivalente (al menos desde el punto de vista legal) personas con formación de posgrado, de grado, de pre-grado, terciarias y/o secundaria, con similar credibilidad pericial (y, por ende, demostrativa y probatoria).

Resulta sencillo de fundar el hecho evidente de que la incumbencia sobre las tareas periciales de revisión de prueba indiciaria informática (entre otras, la gestión integral de la prueba documental informática) corresponde a la Informática forense como disciplina particular de la Criminalística. No estamos ante la presencia de pericias "electrónico forenses" o "contables forenses" o "administrativas forenses", sino ante pericias informático forenses.

La calidad académica del título de grado correspondiente a la disciplina informática es evidente y aunque la profesión no se encuentre reglamentada (en especial por la oposición férrea de quienes aprovechan esta dispensa legal, para realizar sus tareas desde otras disciplinas académicas en el mejor de los casos o desde el cargo que ostentan en el peor de ellos) su propia denominación señala el título exigible al profesional que la realiza. Nadie aceptaría un médico legista que no posea título de médico, se encuentre o no reglamentada tal profesión (algo que ocurría en los tiempos coloniales y que diera lugar a la institución del Protomedicato, que ampliaremos más adelante); este mismo criterio debería aplicarse a la Informática forense, como paso previo a la reglamentación efectiva de las incumbencias profesionales periciales. En contrapartida, ningún profesional de la Informática puede postularse como síndico, perito en electrónica o perito contable, lo que parece una contradicción evidente: todos pueden hacer pericias informático forenses, pero los informáticos no pueden realizar ninguna pericia ajena a la Informática.

¿Nos resulta al menos curioso? No, simplemente estamos comprobando la resultante obligada de los intereses económicos contrapuestos. La Informática forense se constituye en un campo de interacción rentada, donde se puede actuar con cualquier título similar o no, aportar ganancias extras a quienes actúan como tales y que por supuesto constituyen una mayoría absoluta, ya que la suma de los contadores, administradores de empresas, ingenieros industriales y electrónicos, etc., que participa de este proceso es numéricamente superior, respecto de sus iguales que poseen títulos en Informática. Actúa como salida laboral alternativa o principal, a partir de la cual se pueden obtener beneficios sin tener que demostrar idoneidad alguna. El problema de fondo radica en que este beneficio es obtenido reemplazando a quienes tienen legítimo derecho de efectuarlas, por poseer título en Informática, lo que sería impensable en otras profesiones. Pensemos en un abogado, especializado en Derecho penal; aunque no existiera el título específico de “abogado penalista”, es evidente que nunca sería aceptado si no posee título de abogado, ni siquiera podría matricularse en el colegio profesional correspondiente, lo mismo ocurre con un médico legista o un contador. Al parecer, la Informática es una disciplina secundaria que actúa como polo de atracción de otros trabajadores que, abandonando su profesión voluntaria y vocacionalmente elegida, prefieren actuar en esta área, ya que no requiere demostrar aptitud ni idoneidad alguna.

Extrañas dependencias periciales

Si consideramos la falta de dependencia del área informático forense en una fuerza de seguridad, respecto de su correspondiente área criminalística,

estamos ante una falla notoria e incomprensible. En la actual situación académica, donde la Informática forense es una especialidad criminalística que no es brindada por entidad universitaria alguna como carrera terciaria, de grado o de posgrado y la idoneidad de los peritos solo se puede establecer por su práctica profesional forzada, la relación diaria con otros peritos estimula la adquisición de buenas prácticas periciales, históricamente consolidadas. La falta de esta interacción deviene en un proceso de aislamiento y de soluciones de compromiso que terminan deteriorando la calidad del procedimiento pericial informático forense implementado.

Esto se hace evidente en las diferencias formales que se aprecian en la presentación de los informes periciales. La ya consolidada, establecida y aceptada forma general (objeto de la pericia, elementos ofrecidos, operaciones realizadas y conclusiones), es dejada de lado, simplemente por desconocimiento sobre su existencia (se construye, se explica y se difunde académicamente durante el proceso de formación criminalística del futuro perito en las restantes disciplinas criminalísticas). De esta manera, se elimina un elemento de particular importancia formal, ya que constituye un auténtico instrumento de comparación de resultados. El juez que no tiene la obligación de ser idóneo en todas las áreas periciales, cuenta de este modo con un "formulario" de exposición de resultados, ordenado y fácil de interpretar, donde encuentra la información pericial en el lugar preciso donde espera encontrarla. Esta facilidad es eliminada de cuajo por las nuevas formas de presentar los informes, que se limitan a responder los puntos de pericia, en una estructura sin orden alguno y donde el lector debe primero organizar la información presentada, para intentar comprender los resultados periciales alcanzados. Separar formalmente el objeto de la pericia implica facilitar al lector la visión directa de los puntos de pericia solicitados, los elementos ofrecidos permiten conocer directamente los elementos involucrados en la tarea pericial (prueba indiciaria, instrumental y marco de referencia pericial), las operaciones realizadas aportan todas las tareas efectuadas y fundadas científica, tecnológica, técnica y metodológicamente, y las conclusiones permiten entender con rapidez los resultados alcanzados respecto del objeto de la pericia (los puntos de pericia solicitados).

Cualquier profesional de la criminalística formado académicamente es capaz de reconocer de inmediato la importancia de la cadena de custodia en la preservación de la prueba indiciaria. La implementa en sus aspectos legales y técnicos específicos, para asegurar la confiabilidad de la prueba secuestrada y asignar responsabilidades legales durante su manipulación. Algo que resulta obvio para quien identifica, registra, certifica, traslada y entrega elementos probatorios (prueba indiciaria) balísticos, documentales, biológicos, químicos,

etc., simplemente es desconocido por los “expertos o peritos en Informática forense”, que muchas veces no se encuentran en capacidad de instrumentar un documento (formulario) útil y completo que acompañe a la prueba recolectada, ni adoptar las medidas necesarias para asegurar la confiabilidad probatoria de la misma. No obstante, este tema será motivo de tratamiento más amplio en esta obra.

No nos es posible aportar una solución de implementación inmediata a la problemática planteada. La respuesta se basa nuevamente en una tarea inter y transdisciplinaria orientada a la solución general del problema, seguramente sus pilares deberían constituir:

1. La implementación de carreras universitarias en el área pericial informático forense, que por supuesto deben incluir formación legal y criminalística de sus egresados (en consonancia con cualquier otra carrera pericial vigente en nuestro país).
2. El desarrollo de una ley que normalice la profesión informática, delimitando específicamente sus alcances respecto de otras formaciones similares, y que establezca los perfiles de cada formación académica, sus incumbencias profesionales y periciales, en particular en el ámbito judicial.
3. La participación proactiva de los colegios profesionales relacionados con la temática.
4. El dictado de cursos de actualización tecnológica y técnica, dirigidos a la totalidad de los operadores del Derecho, que les permitan interactuar con la prueba indiciaria informática de forma eficiente, efectiva y eficaz.

Comparación de perfiles profesionales

De la misma forma que no es aceptable confundir a un médico generalista con un médico legista, ya que este último profesional comparte con el primero únicamente su formación profesional básica, a la que debe agregar su especialización en clínica médica, traumatología, cirugía y especialmente la realización de la carrera de médico legista, no es posible confundir a un profesional de la informática con un profesional de la Informática forense, los que analógicamente solo deberían compartir su formación profesional básica: informática, ya que estamos en presencia de Informática forense y no de otra especialidad pericial. A efectos de simplificar esta explicación, incluimos la siguiente tabla comparativa (algunos de cuyos componentes comparativos han sido reformulados para adaptarlos a nuestra realidad jurídica imperante, a partir de los conceptos propuestos en: Larry Daniel y Lars Daniel, Digital Forensics for legal professionals, Ed. Elsevier-Syngress, Robert Maxwell, Sue Spielman, technical editors, 2012):

TABLA COMPARATIVA DE REQUERIMIENTOS, CONOCIMIENTOS Y

CAPACIDADES	
Comparación técnica de capacidades/idoneidades	
Perito/Experto en Informática forense	Experto en Informática/Computación
Adquisición y resguardo de prueba indiciaria informática, con fines legales.	Instalación y configuración de computadoras, programas y redes.
Recuperación de prueba documental informática, desde múltiples medios de almacenamiento, procesamiento y desplazamiento, incluyendo copias de seguridad.	Recuperación de datos a partir de copias de seguridad.
Análisis forense de datos.	Solución de problemas y reparación de equipos de computación y comunicaciones digitales.
Identificación y resguardo de la evidencia digital generada por el accionar de programas maliciosos (virus, troyanos, etc.) en los equipos infectados (no con el fin de eliminar dichos programas).	Detección y eliminación de programas maliciosos (virus, troyanos, etc.) en los equipos informáticos infectados (no la recuperación de evidencia digital de dichas acciones maliciosas).
Análisis de las trazas digitales resultantes de la acción de programas de aplicación, a fin de determinar su efecto sobre la evidencia recolectada.	Instalación y mantenimiento de programas de aplicación para usuarios finales.
Análisis de la prueba indiciaria informática resultante de la acción de aplicaciones de Internet para establecer su valor probatorio judicial.	Instalación y configuración de redes de computadoras y accesos a Internet, con el propósito de permitir al usuario final acceder a estos servicios.
Conocimientos profundos, de bajo nivel, sobre el funcionamiento de estructuras de datos, arquitectura de discos y sistemas de archivos con el fin de identificar y resguardar las trazas digitales resultantes de la acción e interacción de sistemas operativos, programas de aplicación y almacenamiento de datos.	Dar formato a unidades de almacenamiento secundario e instalar múltiples sistemas operativos.

Analizar e informar resultados periciales informático forenses a partir de la prueba documental informática recolectada, en calidad de testigo experto (imágenes DD, imágenes de acceso a datos e imágenes inteligentes). Asegurar la cadena de custodia, autenticación, verificación y certificación digital de las pruebas digitales recolectadas.	Interactuar con los diversos formatos de archivos (a partir de distintos sistemas operativos) con el fin de instalarlos, efectuar búsquedas y realizar copias de seguridad.
Realizar copias forenses (digitales) desde todo tipo de dispositivo de almacenamiento físico, incluyendo datos eliminados, a efectos de ser utilizados como prueba indiciaria informático forense, prueba documental informática, o elementos sub peritia, en pericias informático forenses.	Realizar copias de seguridad de distintos medios de almacenamiento (no incluye los datos eliminados), con el fin de recuperar los documentos perdidos para asegurar la continuidad de la operación informática relacionada (preservar el negocio).
Comparación criminalística de capacidades/idoneidades	
Perito/Experto en Informática forense	Experto en Informática/Computación
Identificación, resguardo, verificación y certificación digital de lugares del hecho virtuales propios e impropios.	
Interacción multi y transdisciplinaria con otros peritos de distintas ramas criminalísticas, a efectos de participar en la reconstrucción del hecho (criminal o no).	
Identificación, protección, resguardo y traslado de evidencia no digital de todo tipo (prueba indiciaria en general) en caso de ausencia de otros peritos en el lugar del hecho.	
Gestión integral del accionar pericial en ocasión de inspecciones y reconocimientos judiciales.	
Participación en carácter de testigo experto ante las distintas instancias judiciales (escritas y orales).	
Generación de lugares del hecho virtuales impropios a partir de los datos obtenidos en la inspección judicial del lugar del hecho real.	

Apoyo informático a la integración de datos periciales (digitales o no) provenientes de todas las restantes áreas periciales, a efectos de realizar una reconstrucción integral de los hechos acaecidos.	
Generación de sistemas automatizados de hipótesis reconstructivas a idénticos fines que el texto de la celda superior.	
Interacción reconstructiva con lugares del hecho virtuales propios existentes o históricos (ídem celda superior).	
Participación en reuniones locales o remotas, con otros peritos o miembros del Poder Judicial (ídem celda superior).	
Identificación e integración de elementos comunes con otras áreas criminalísticas (por ejemplo, con los resultados obtenidos por la Medicina legal), con fines de simulación, reconstrucción virtual local o remota, y participación en discusiones periciales judiciales o no.	
Conocimientos profundos técnicos y metodológicos criminalísticos.	
Conocimientos criminalísticos profundos, específicos y formales (en particular sobre el modelo de informe pericial –Objeto de la pericia, elementos ofrecidos, operaciones realizadas y conclusiones–, que le permitan interactuar con otros peritos e informes periciales similares: balísticos, documentológicos, papiloscópicos, etc.). El modelo de informe formal permite comparar, cotejar e integrar los resultados obtenidos por distintos peritos en áreas periciales diversas. A partir de esta integración es que la prueba indiciaria informático forense adquiere validez y confiabilidad como soporte a la decisión judicial (sentencia).	
Comparación judicial de capacidades/idoneidades	
Perito/Experto en Informática forense	Experto en Informática/Computación
Conocimientos básicos sobre el orden jurídico y el sistema judicial obrantes en el país de referencia.	Ídem.
Conocimientos desarrollados sobre Derecho	Ídem.

constitucional y códigos de fondo.	
Conocimientos desarrollados sobre Derecho civil (obligaciones y contratos en particular, incluyendo sus versiones informáticas digitales o electrónicas).	Ídem.
Conocimientos desarrollados sobre Derecho penal (en particular lo referido a participación primaria, falso testimonio y falsa denuncia) y leyes complementarias (Propiedad Intelectual, Firma Digital, Hábeas Data, Delitos Informáticos, Expediente Digital).	Ídem.

Conocimientos profundos sobre Derecho procesal (códigos de forma), referidos a la jurisdicción y competencia judiciales en las que realiza cada labor pericial específica.
Conocimientos profundos sobre causas de nulidad específicas (ídem celda superior), relacionadas con la prueba pericial en general y con la prueba indiciaria informático forense en particular.
Conocimientos profundos sobre lenguaje jurídico a efectos de establecer un nexo comprensible con los destinatarios de la información pericial informático forense recolectada (apoyo a la decisión judicial-sentencia).
Conocimientos profundos sobre las normas administrativas procesales vigentes en el área judicial en la que se desempeña, su zona de influencia y su interacción con otras áreas judiciales.
Conocimientos profundos sobre gestión de la cadena de custodia informático forense.
Conocimientos profundos sobre la gestión e implementación técnico pericial de las órdenes de allanamiento, recolección o reconocimiento emanadas de la autoridad judicial competente.
Conocimientos profundos sobre la gestión de cédulas judiciales y otros medios de notificación.
Asistencia técnica informático forense a los operadores del Derecho (a priori, a posteriori y durante el desarrollo del litigio judicial).
Nota: En el estado actual del desarrollo académico de esta especialidad criminalística no existen carreras de formación universitaria (terciarias, de grado o posgrado) específicas en la temática. Por esa razón, al evaluar al postulante a perito o experto en Informática forense, es necesario considerar: 1. Títulos de grado (específicos en Informática, ya que estamos ante la especialidad criminalística denominada “Informática forense”).

2. Títulos complementarios (abogacía, criminalística, otras formaciones periciales) en instituciones educativas oficiales, no en capacitaciones empresariales y/o comerciales.
3. Títulos extranjeros (para que sean pertinentes deben ser posibles de clasificar dentro de la estructura educativa de nuestro país: terciarios, de grado, de posgrado, y haber sido revalidados formal, legal y administrativamente).
4. Experiencia pericial criminalística en general y en Informática forense en particular.
5. Membresías nacionales e internacionales en organismos relacionados con la Informática forense.
6. Gestión y cargos de investigación y docencia.
7. Publicaciones.

La Informática forense y sus especialidades

Como toda disciplina criminalística, la Informática forense se compone de varias especialidades, integradas bajo el mismo método, pero que difieren entre sí por sus particularidades físicas o lógicas; esta es una de las razones de ser de este libro. Debemos considerar la siguiente clasificación general, para facilitar su lectura:

Informática forense:

1. Computacional
   a. fija.
   b. móvil.
   c. integrada al atuendo (vestimenta).
   d. de base (sistemas operativos).
   e. de aplicación (programas ejecutados en un determinado sistema operativo).
2. Conectividad.
3. Telefonía forense.
4. Sistemas de posicionamiento global GPS.
5. Archivos documentales digitalizados (tratamiento de imágenes, video y audio).
6. Residuos informáticos (tratamiento de residuos físicos y lógicos).

El vocablo “prueba”

Sentido amplio: Como instituto de Derecho procesal (o como subsistema del proceso judicial), consiste en el conjunto de actos y elementos interrelacionados, destinados al cumplimiento de un objetivo, por lo que en

principio la prueba es un medio de verificación de las proposiciones que los litigantes formulan en el juicio.

Es también una operación que se ejecuta para comprobar que otra, ya realizada, lo fue correctamente (metodología y resultados). Una razón, argumento, instrumento u otro medio con que se pretende mostrar y hacer evidente la verdad o falsedad de algo.

El Derecho probatorio, como parte integrante del Derecho procesal, aparece regulando la admisibilidad, ejecutoriedad y valoración de la prueba en el proceso.

La probática, fuera del conocimiento estrictamente jurídico, trata los hechos en el proceso, abarcando un aspecto epistemológico (filosofía de la prueba) y un aspecto técnico orientado al arte o ejercicio de probar tales hechos.

Sentido restringido: Para la siguiente argumentación adoptaremos el concepto de prueba como medio (sentido instrumental): probar significa determinar o fijar formalmente los hechos mismos mediante procedimientos determinados (Carnelutti).

Relaciones: Con los conceptos articulantes de medio de prueba, fuente de prueba, elemento de prueba y carga de la prueba.

Prueba documental clásica

Para aquellos que llevamos cierto tiempo participando de los procesos judiciales, la presencia de la prueba nos resulta un elemento típico y absolutamente imprescindible para llevar a buen término un litigio cualquiera, ya sea que se resuelva mediante el proceso judicial o por medios alternativos de resolución de conflictos (negociación, conciliación, mediación, arbitraje, entre otros).

En lo referente al proceso judicial, para que este pueda ser instalado es necesario que exista una pretensión por alguna de las partes[4]. Siguiendo el orden lógico, no excluyente de los acontecimientos, es posible prever:

1. La presencia de un cliente, que refiere hechos, a partir de los cuales surge la transgresión a una norma jurídica que lo perjudica.
2. La necesidad de resarcimiento de esta situación, mediante una acción positiva obligatoria (es imposible concebir acciones negativas de este tipo), que constituye la pretensión.
3. Desde los hechos y desarrollo circunstanciado, hasta la convalidación o denegación de la pretensión, en el acto de sentencia, discurre un camino signado por la argumentación del operador del Derecho, que gestiona o participa de dicho desarrollo procesal.
4. Este camino encuentra sustento en los elementos probatorios ofrecidos.

5. No hay proceso sin pretensión, no hay argumentación sin prueba relacionada.

Los Códigos de Procedimientos, por formar parte de las Leyes de Forma de la Nación, son aplicables a cada jurisdicción y competencia, ya que son parte de los poderes no delegados por las provincias en el Gobierno Central. De hecho, la prueba forma parte de un capítulo específico en todos ellos. Como parte de dicha prueba, encontramos la prueba documental.

Concepto: Prueba documental es la que se constituye mediante documentos.

Documento: Es una cosa, con función representativa de hechos.

- Es toda representación material destinada e idónea para reproducir cierta manifestación del pensamiento (Chiovenda).
- Todo objeto producto de un acto humano que represente a otro hecho u objeto (Devis Echandía).
- Un objeto material originado por un acto humano, susceptible de representar por sí mismo y para el futuro un hecho o una serie de hechos percibidos en el momento de su concepción (Kielmanovich).
- Todo objeto que represente una manifestación del pensamiento (Falcón).

Clasificación: Esta prueba documental, a la que denominaremos "clásica", es posible de clasificar por distintos criterios, dando origen a las siguientes categorías:

1. Según su condición material:
   a. Bibliográfica: Referida a escritos (manuscritos e impresos), que normalmente suelen llevar en subsidio pruebas periciales documentológicas, documentoscópicas o caligráficas.
   b. Foliográfica: Referida a gráficos, esquemas y representaciones de situaciones o lugares (planimetría, cursogramas, planos, entre otros), cuya prueba pericial relacionada depende del tipo de gráfico y puede incluir agrimensores, arquitectos, ingenieros, expertos en accidentología vial, entre otros.
   c. Pictográfica: Referida a fotografías, incluyendo el cine (no digitales), en este caso las pericias las realizan expertos en cada tema (fotografía pericial, operadores cinematográficos, etc.). En este grupo se incluyen, por su relación directa respecto del soporte involucrado, todas las pruebas de sonido no digitalizado.
2. Según su integración al proceso:
   a. Aportados por el actor.
   b. Aportados por la contraparte.

c. Aportados por terceros.

3. Según su autoría:

a. Generados por quien los acompaña.

b. Generados por la contraparte.

c. Generados por terceros.

A partir de esta clasificación, surgen algunas relaciones que es necesario tener en cuenta:

Documentos privados: Requieren una copia por cada parte y su firma; pueden carecer de fecha[5].

Documentos públicos: (Artículo 979 del Código Civil): Solo pueden ser atacados por redargución de falsedad (Artículo 395 del CPCCN).

Acciones posibles ante la documental ofrecida: Se puede reconocer, negar o guardar silencio[6]. En el caso del desconocimiento de la documental, existe un vacío legal, ya que no se asigna carga de probar su autenticidad o falsedad.

Silencio: Respecto del silencio, este puede generarse a partir de la no contestación de la demanda o no manifestarse en relación con el documento (no reconocer ni negar la firma)[7].

Negativa: En cuanto a la negativa general de los documentos en la contestación de demanda, la misma debe ser clara, expresa y sin condicionamientos.

Respuestas evasivas: En lo referido a las respuestas evasivas, se las asimilaría al reconocimiento.

De ahí que podamos interpretar tres situaciones:

1. Reconocimiento.

2. Silencio (no contestar o no expedirse).

3. Respuestas evasivas.

No están sujetos a lo anterior, el defensor oficial y el sucesor a título universal (Artículo 358 del CPCCN).

En lo que se refiere a los documentos de terceros, estos solo pueden ser reconocidos por ellos. Las partes, como máximo, podrían decir que los desconocen o no les constan. En lo referente a los documentos oficiales, cada día se agregan nuevas formas aceptadas[8].

Efectos del desconocimiento

1. Atribuidos a la contraria[9]. Quien la aportó debe ofrecer otra prueba en subsidio[10]. La parte que desconoció debe ofrecer prueba para desvirtuarla. Toda prueba documental lleva implícito otro medio probatorio para acreditar su autenticidad[11].

2. Emanados de terceros. La parte que acompañó el documento de un tercero debe acreditar su autenticidad, el juez realiza la valoración en relación con la conducta de las partes, las demás pruebas y las características particulares del documento. El desconocimiento no libera al demandado de producir prueba en contrario. El que desconoce debe producir la prueba en contrario. La carga de la prueba, acorde con el caso, puede estar en cabeza de quien la acompaña o en cabeza de quien la desvirtúa.

3. Si resulta de autoría de quien la ofrece. Emanadas por el propio oferente. El desconocimiento no tiene valor probatorio. Nadie puede procurarse prueba sobre su propia autoría. El silencio actúa como elemento indiciario, corroborante de otra prueba.

Cuestiones atinentes:

- Indivisibilidad del desconocimiento.
- Documental improcedente.
- Rebeldía o incontestación de demanda.
- Negativa general.
- Medida para mejor proveer.

Prueba documental informática

La prueba documental informática es una especie del género prueba documental clásica, que difiere de esta únicamente en el soporte. En la clásica, el soporte consiste generalmente en papel o elementos contenedores analógicos (películas, papel, cintas), mientras que la prueba documental informática se caracteriza por la digitalización de sus componentes y su resguardo en medios aptos para esta (soporte magnético u óptico en general, pero no de manera excluyente).

Como características propias, podemos señalar:

1. Principio de identidad atípico: Mientras que siempre es posible identificar entre el original y una copia de un documento en soporte de papel, en el caso de la copia digital (bit a bit) de un archivo, estos son inidentificables, ya que un bit es idéntico a otro y la suma de bits componen ambos archivos, que en este caso se constituyen en dos originales indistinguibles.

2. Posibilidad de modificación por medios locales o remotos, accidentales, culposos o dolosos.

3. Divisibilidad del documento: Esta característica es fácilmente comprensible por medio de un ejemplo: Dos comerciantes intercambian mensajes de correo electrónico, el primero con una oferta y el segundo, la respuesta con su aceptación; se ha conformado un contrato comercial. Llegado el momento, una de las partes toma el mensaje de su interlocutor y lo

modifica, agregándole o quitándole texto. En el momento del reconocimiento por parte del supuesto autor del mensaje, este no puede, ni debe, impugnar la totalidad del mensaje, sino únicamente la parte que fue modificada y que no coincide con sus propios resguardos de información.

4. De la misma forma en que el Código de Procedimientos de la Provincia de Córdoba establece la subsidiariedad automática de la pericial caligráfica, respecto de la prueba documental, la prueba documental informática lleva implícita la prueba pericial informático forense, para el caso de negativa[12]. Por otra parte, y de manera sumamente frecuente, requiere de su convalidación mediante una prueba de informes[13] (por ejemplo, dirigida al ISP, en el caso de los mensajes de correo electrónico). Aunque aún no se ha implementado en nuestro país, la firma digital confiere al documento electrónico la misma credibilidad que el documento público clásico y debería ser tratada en similares condiciones legales y sobre todo procesales.

Breve guía de recolección de prueba documental informática

1. Se puede recolectar toda la información en poder de la parte consultante, que sea privada (la que tiene en cualquiera de sus máquinas), y la información pública de la web (páginas, grupos de discusión, en fin, todo lo que no requiera violar una clave para ingresar).

2. Hay que hacerlo antes de realizar la denuncia o la demanda.

3. Se hace en presencia de un escribano, se certifica y se inicia la cadena de custodia (esto elude los errores policiales más frecuentes).

4. Para realizar los pasos anteriores, no hace falta requerir autorización judicial alguna.

5. A continuación, se realiza la denuncia, solicitando el resguardo de la documental informática en poder de la contraparte (o acusado en caso de querella penal) o de terceros; conviene hacerlo “in audita altera pars”, como medida previa, preliminar o prueba anticipada[14], justificando el derecho invocado, el riesgo en la demora y ofreciendo contracautela de privacidad (asegurar el no acceso a ninguna información que no sea conducente y pertinente a los fines de argumentar la pretensión del caso).

6. Siempre que sea posible se convalida la prueba mediante prueba de informes complementaria, por ejemplo, en el caso de los mensajes de correo electrónico, se solicita informe al ISP (Proveedor de Servicios de Internet, por ejemplo: Yahoo o Google), para que certifiquen la existencia de los mensajes intercambiados. Esto es vital a fin de sostener la prueba justificándola con el informe de un tercero no involucrado en la causa.

7. Se planifican los puntos de pericia informático forense, en subsidio, a

partir de la documental informática recolectada. Deben ser conducentes y pertinentes (es muy raro que su número sea superior a diez, de serlo conviene revisarlos para que no sean reiterativos, ambiguos o inconducentes).

Nota: No se debe confundir recolectar prueba con inducir al delito; recordemos las figuras:

- agente encubierto (ley que lo convalida e institución que lo designa, ejemplo: lucha contra el narcotráfico);
- agente provocador (solo posee institución que lo designa y a veces una normativa administrativa que lo convalida, ejemplo: inspectores de la AFIP);
- partícipe primario (fuera de la normativa, no actúa en nombre de institución judicial, de seguridad o de prevención alguna, ejemplo: compradores de computadoras con el fin de denunciar falta de licencia de programas instalados).

[1] Eficiencia: Optimización de recursos (máximos resultados con mínimos recursos-costos). Eficacia: Relación entre el objetivo propuesto y el alcanzado (en condiciones ideales, no es cuantificable). Efectividad: Ídem eficacia (en condiciones habituales, es cuantificable, es decir permite realizar comparaciones objetivas con otro producto equivalente o similar).

[2] *Contadores, administradores de empresas, ingenieros en electrónica, ingenieros industriales, etc., que fundan, afirman y sostienen per se su capacidad pericial o utilizan las incumbencias arbitrarias que asigna la Universidad de origen al título que ostentan.*

[3] Código Procesal Civil y Comercial de la Nación: Idoneidad. Art. 464. "Si la profesión estuviese reglamentada, el perito deberá tener título habilitante en la ciencia, arte, industria o actividad técnica especializada a que pertenezcan las cuestiones acerca de las cuales deba expedirse. En caso contrario, o cuando no hubiere en el lugar del proceso perito con título habilitante, podrá ser nombrada cualquier persona con conocimientos en la materia".

[4] *Pretensión, pretencioso: La escritura de estas dos palabras de origen común –una con s y otra con c– es una de las muchas paradojas de la ortografía castellana, que se explica porque la primera nos llegó directamente desde el latín, mientras que la segunda pasó antes por el francés. Ambos vocablos provienen del latín praetensio –onis, formado a partir del verbo praetendere, que a su vez se formó del verbo tendere (estirar, extender, montar una tienda) con el prefijo prae– (ante, delante, enfrente). Para los romanos, praetendere era equivalente a "poner por delante", "interponer" y, en sentido figurado, "poner un pretexto". Praetendere muros Marti era "colocar murallas entre sí y el enemigo" (Virgilio). En la inexorable evolución del significado de las palabras, praetendere se convirtió en inglés en to pretend, con el sentido de "fingir", "simular", y en portugués, en pretender, con la denotación de "aspirar a", "proponerse", "tener intención de". En español, pretender significa "querer ser o conseguir algo", "intentar conseguir algo" y también "aspirar al amor de una persona del sexo opuesto", mientras que pretensión expresa el "derecho que alguien cree tener sobre algo". En francés, el verbo latino evolucionó a prétendre, del que se derivaron, entre otras, las palabras prétendant (pretendiente), prétendu (pretendido), y prétentieux. Esta última llegó a nuestra lengua como pretencioso, cambiando la t por una c, con el significado de "presuntuoso", pero fue criticado durante muchos años como un galicismo indeseable. Pretencioso apareció por primera vez en el diccionario de la Academia en la edición de 1927, marcado como "galicismo", pero 43 años después, en la actualización de 1970, quedó consagrado como vocablo castellano castizo, sin marca de extranjerismo, tal como ha ocurrido incontables veces a lo largo de la Historia con muchas voces de nuestro idioma. La c galicada (afrancesada) no fue recogida por el portugués, una lengua más fiel al latín, que se quedó con pretensão y pretensioso. Fuente: www.rae.es*

[5] *Código Civil, Art. 1012. – "La firma de las partes es una condición esencial para la existencia de todo acto bajo forma privada. Ella no puede ser reemplazada por signos ni por las iniciales de los nombres o apellidos".*

Art. 1021. – "Los actos, sin embargo, que contengan convenciones perfectamente bilaterales deben ser redactados en tantos originales como partes haya con un interés distinto".

[6] *CPCCN, Art. 356. – "En la contestación opondrá el demandado todas las excepciones o defensas de que intente valerse. Deberá, además:*

1) Reconocer o negar categóricamente cada uno de los hechos expuestos en la demanda, la autenticidad de los documentos acompañados que se le atribuyeren y la recepción de las cartas y telegramas a él dirigidos cuyas copias se acompañen. Su silencio, sus respuestas evasivas, o la negativa meramente general podrán estimarse como reconocimiento de la verdad de los hechos pertinentes y lícitos a que se refieran. En cuanto a los documentos se los tendrá por reconocidos o recibidos, según el caso. No estarán sujetos al

cumplimiento de la carga mencionada en el párrafo precedente, el defensor oficial y el demandado que interviniere en el proceso como sucesor a título universal de quien participó en los hechos o suscribió los documentos o recibió las cartas o telegramas, quienes podrán reservar su respuesta definitiva para después de producida la prueba. 2) Especificar con claridad los hechos que alegare como fundamento de su defensa. 3) Observar, en lo aplicable, los requisitos prescritos en el artículo 330".

Traslado de la reconvención y de los documentos, Art. 358. – "Propuesta la reconvención, o presentándose documentos por el demandado, se dará traslado al actor quien deberá responder dentro de quince (15) o cinco (5) días respectivamente, observando las normas establecidas para la contestación de la demanda. Para el demandado regirá lo dispuesto en el artículo 335".

7 Código Civil, Art. 919. – "El silencio opuesto a actos, o a una interrogación, no es considerado como una manifestación de voluntad, conforme al acto o a la interrogación, sino en los casos en que haya una obligación de explicarse por la ley o por las relaciones de familia, o a causa de una relación entre el silencio actual y las declaraciones precedentes".

Art. 1031. – "Todo aquel contra quien se presente en juicio un instrumento privado firmado por él, está obligado a declarar si la firma es o no suya".

8 Acordada 3/2012 CS (Corte Suprema de Justicia de la Nación). Sistema de Notificaciones por Medios Electrónicos reglamentado por Acordada 31/2011 CS. Aplicación. Recurso de queja por denegación de recurso extraordinario federal. Código de usuario. Acordada 4/2007 CS.

Acordada 31/2011 CS (Corte Suprema de Justicia de la Nación). Constitución de domicilio electrónico, por toda persona que litigue por propio derecho o en ejercicio de una representación legal o convencional, para las causas judiciales que tramiten ante la Corte Suprema de Justicia de la Nación. Entrada en vigencia.

9 CPCCN, Reconvención, Art. 357. – "En el mismo escrito de contestación deberá el demandado deducir reconvención, en la forma prescripta para la demanda, si se creyere con derecho a proponerla. No haciéndolo entonces, no podrá deducirla después, salvo su derecho para hacer valer su pretensión en otro juicio. La reconvención será admisible si las pretensiones en ella deducidas derivaren de la misma relación jurídica o fueren conexas con las invocadas en la demanda".

10 CPCCN, Carga de la prueba, Art. 377. – "Incumbirá la carga de la prueba a la parte que afirme la existencia de un hecho controvertido o de un precepto jurídico que el juez o el tribunal no tenga el deber de conocer".

11 Código Procesal Civil y Comercial de la Provincia de Córdoba, Ley 8.465, Pericial Caligráfica Subsidiaria, Art. 242.

– "Todo ofrecimiento de prueba documental lleva implícita la pericial caligráfica para el supuesto de negarse la autenticidad".

12 Prueba pericial: La suministrada por un tercero que a raíz de un encargo judicial a uno o varios testigos expertos, que fundados en los conocimientos científicos o prácticos que poseen, comunican al juez las comprobaciones, opiniones o deducciones extraídas de los hechos sometidos a su dictamen (Palacio).

13 Prueba de informes: Es el medio para aportar al proceso datos sobre hechos concretos, claramente individualizados y controvertidos, que resulten de la documentación, archivos o

registros de terceros o de las partes (aportar al proceso datos preexistentes, que constan documentalmente en poder del informante y cuyo conocimiento no tenga carácter personal, sino instrumental).

14 "Aguilar y Asociados SRL c/Native Software SRL s/ordinario", CNCom, 17/04/2012. Proceso civil y comercial.

Prueba anticipada. Copia de seguridad de los sistemas informáticos ubicados en la sede de la demandada. Vulnerabilidad y fragilidad de los registros informáticos en general. Necesidad de asegurar la obtención de elementos necesarios para la posterior producción de prueba. Verosimilitud del derecho y peligro en la demora. Procedencia de la obtención anticipada de una copia o back up de los registros informáticos. Respeto a las garantías constitucionales en juego. Derecho de defensa de la demandada. Participación del Oficial de Justicia que corresponda y citación del Defensor Oficial.

"La solicitud de prueba anticipada se dirige a asegurar la obtención de elementos de información necesarios para la posterior producción de tal medio probatorio. Así planteada la cuestión, dentro del marco de provisionalidad con sujeción al cual es aprehensible toda petición de estas características y a partir de lo que prima facie surge de la documentación acompañada aparece verosímil la motivación del demandante sobre la necesidad de obtener una medida como la de la especie con el claro propósito de aventar el ulterior ocultamiento, modificación, destrucción, alteración o pérdida en el objeto probatorio".

"[...] la imposibilidad o dificultad en la posterior producción probatoria que exige el artículo 326 citado debe ser entendida en un sentido amplio; sobre todo en esta particular temática, donde la vulnerabilidad y fragilidad que los registros informáticos ofrecen permiten presuponer el peligro en la demora, ya que pueden desaparecer o resultar afectados por algún virus".

"[...] resulta conducente la disposición de medidas tendientes a asegurar la verdadera eficacia del proceso judicial, siempre procurando el mayor de los respetos a las garantías constitucionales en juego: el debido derecho de defensa y el aseguramiento del principio de bilateralidad [...] habiéndose juzgado acreditados la verosimilitud del derecho invocado y el peligro en la demora de conformidad con lo dispuesto por el artículo 326 del Código Procesal, admítese la obtención de una copia o back up de toda la información contenida en los discos rígidos, extraíbles o no, servidores y cualquier otro tipo de respaldo posible existente en los diversos ordenadores que se encuentren en el domicilio de la demandada".

"La diligencia deberá cumplirse mediante la designación de un perito licenciado o ingeniero en sistemas que deberá designar la jueza de grado, con la participación del Oficial de Justicia que corresponda y con citación del Defensor Oficial. Este último, en razón del derecho de defensa previsto por el

artículo 327 del Código Procesal y para representar a la parte contra la que se lleva a cabo la medida, a la cual no podría serle notificada ya que su anticipación en el conocimiento podría posibilitar la alteración o modificación del objeto probatorio a adquirir".

CAPÍTULO 2
LAS MEDIDAS PREVIAS, PRELIMINARES O PRUEBA ANTICIPADA EN INFORMÁTICA FORENSE

Respecto de este tema hay que decir que la recolección de prueba documental informática suele darse, entre otros, en dos entornos principales:

1. Antes de presentar una demanda, sin intervención judicial. En este sentido, basta con que se conserven los recaudos que dicha tarea requiere:
   a. Solo se puede recolectar información propietaria (es decir de propiedad de quien solicita la recolección) y/o pública.
   b. Certificada ante escribano público.
   c. Autenticada mediante el correspondiente digesto matemático (hash).
   d. Con su correspondiente cadena de custodia.
2. El paso anterior suele efectuarse para alcanzar alguna negociación previa a la acción judicial (métodos alternativos de resolución de conflictos) o como fundamento para justificar la solicitud de una medida previa, preliminar o prueba anticipada (acorde al fuero en que estemos operando). Este es el caso que me interesa analizar en el presente resumen.

La autorización para realizar una medida preliminar implica, en el caso de la Informática forense, una estricta observación del principio in audita altera pars. Esta característica se funda en la especial volatilidad y volubilidad de la prueba documental informática, la cual puede ser modificada, alterada o eliminada, no solo por medios locales, sino también por medios remotos (acciones directas o virtuales, que incluyen la denegación de servicio).

Lleva implícita en su naturaleza una profunda relación con las medidas cautelares y es así que conserva al menos dos de sus tres requisitos clásicos:

- Fumus bonis iuris: Verosimilitud del derecho invocado.
- Periculum in mora: Peligro en la demora.

Y difiere relativamente en el tercero, la contracautela, ya que este se reemplaza por el aseguramiento de la privacidad de los datos hallados durante la actividad y que no sean estrictamente conducentes y pertinentes a la requisitoria ordenada por el tribunal interventor que autoriza y convalidad la medida:

- Servare secreto private: Preservar la privacidad.

El fundamento de esta medida es mantener la igualdad de las partes en el litigio, preservando la prueba existente al momento de presentar la demanda y evitando que la pretensión se vuelva ilusoria.

Características

Instrumentalidad: No tienen un fin en sí misma, sino que constituyen un medio de preservación de prueba, que luego podrá ser utilizado y eventualmente considerado a efectos de fundamentar la sentencia proveída, respecto de la pretensión argumentada por cada una de las partes. No se trata de medidas autónomas, porque no tienen razón de ser fuera del contexto del fin pretendido.

Sumariedad: La superficialidad del conocimiento judicial, por parte del tribunal al que le es requerida la medida, ya que no pueden establecerse con certeza los requisitos antes detallados, los que en todos los casos dependerán de una evaluación somera y en condiciones de incerteza, por parte de quien deba proveerla. Recordemos, no obstante, que no es menester probar plenamente la existencia del derecho invocado, sino su verosimilitud comprobada sobre tablas (en esto se parece mucho a las condiciones del amparo).

Provisionalidad: Al respecto, es necesario destacar que difieren de las medidas cautelares en el sentido de que estas no son definitivas y terminan con la sentencia consentida y ejecutada, mientras que la recolección efectuada constituye un hecho definitivo y muy difícil de repetir. Sin embargo, son provisionales en el sentido de que generalmente requieren una prueba de informes complementaria y/o una prueba pericial en subsidio (por el contrario, no resultan necesarias estas pruebas complementarias en caso de que la contraparte se allane ante la evidencia recolectada).

Perennis in iudicium: Aunque son susceptibles de revisión por prueba de informes y pericial, no deberían modificarse durante su empleo judicial, ya que en dicha inalterabilidad se funda gran parte de su poder de convicción probatorio. No caducan con el tiempo, porque una vez admitidas como elemento probatorio conservarán este carácter durante todo el desarrollo del litigio.

Reserva: Por su necesidad de concesión inaudita altera pars, preservando los derechos procesales establecidos para estos casos (presencia del Ministerio Público en representación del propietario de los datos accedidos); de lo contrario, la medida carece de eficacia.

Se trata entonces de una acción jurisdiccional con características propias (cautelares en el sentido de preservar la prueba y asegurar su sobrevida durante el proceso). Aunque carece de autonomía respecto del proceso

principal cuya eficacia garantiza, parece mantenerla al menos en el ámbito conceptual, anticipando la tutela del derecho invocado y la pretensión que funda al proceso en ciernes.

Requisitos doctrinarios

1. **Verosimilitud del derecho** *(fumus bonis iuris)*: Para que se conceda no es necesario un estudio exhaustivo y profundo de la materia controvertida en el proceso principal, sino de un conocimiento superficial; la certeza aparecerá a posteriori en la sentencia. No se requiere prueba plena y concluyente, sino un acreditamiento convincente para que se ordene la providencia solicitada. Es necesario destacar que cuando la contraparte es la administración pública, como esta goza del principio de presunción de legalidad de sus actos, la verosimilitud del derecho invocado debe comprender la acreditación de las arbitrariedades o irregularidades manifiestas en ella.

2. **Peligro en la demora** *(periculum in mora)*: Aunque en el caso de la prueba documental informática, el riesgo de su modificación, adulteración o eliminación es prácticamente evidente, en razón de su debilidad manifiesta frente a las acciones dolosas o culposas de los actores físicos, lógicos o humanos con los que se relaciona, siempre es necesario fundar con claridad este riesgo. Quien debe decidir tendrá siempre sobre su cabeza la espada de Damocles del derecho a la privacidad (de raigambre constitucional). En este sentido, es necesario destacar en la fundamentación que:

a. En caso de pérdida, adulteración o modificación de la prueba, se torna prácticamente imposible realizar tareas que permitan reconstituirla.

b. Por la naturaleza específica de la prueba documental informática, esta no se somete al clásico y reconocido principio lógico de identidad. Mientras que, en otras áreas criminalísticas, este principio es uno de los rectores (siempre es posible identificar el original y las copias) en los archivos digitales; dos archivos iguales bit a bit no son similares sino idénticos y es imposible determinar cuál es copia de cuál, sin recurrir a otros medios secundarios para establecer la precedencia, medios que siempre requerirán de un testigo humano[15], con las dificultades que esto trae. Es decir, si alguien está observando cómo se efectúa la copia de un archivo desde un disco rígido a un soporte externo (por ejemplo, un disquete), es evidente que podrá luego afirmar que el archivo del disco precedía al que obra en el disquete. Sin embargo, si no ha presenciado esta acción, no podrá decir si la situación no era la inversa (el archivo estaba en el disquete y fue copiado al disco duro de la máquina considerada).

c. Suele afirmarse que los archivos borrados siempre pueden ser recuperados a posteriori. Esta afirmación se ha llegado a utilizar en jurisprudencia,

afirmando que si la información es borrada, entonces el requirente de la medida previa negada siempre podrá demostrar que fue borrada. Este aserto adolece de serios defectos conceptuales y racionales:

i. ¿De qué sirve que pueda mostrar que algo se borró, si no puedo mostrar el contenido que fue borrado?

ii. La recuperación de archivos borrados, como casi todo en Criminalística en general y en Informática forense en particular, depende de la inexperiencia del actor que realiza la acción de borrado. Existen mecanismos de borrado seguro (establecidos y normados por instituciones del nivel de credibilidad del FBI y el IEEE de los EE.UU.) que aseguran la irrecuperabilidad absoluta de los datos eliminados.

iii. Aun en el mejor de los casos, la recuperación de los archivos borrados siempre será parcial y los modificará, ya que el acto de recuperar impone su fecha sobre los datos recuperados, siendo muy difícil establecer con certeza la fecha original de los archivos modificados (conjuntamente con su carácter de original y copia ya expresados en el punto b.) y, por lo tanto, se perderá una de las características principales de este tipo de prueba: la determinación de su contemporaneidad (precedencia y sucedencia relativas) con los hechos que se intenten probar, en aras de brindar soporte a la argumentación que pretende hacer convincente la pretensión expresada, al juzgado interventor.

iv. Si no se concede la medida, el demandado puede eliminar la prueba ante la notificación de la demanda. Suponer que no lo hará es tan posible y probable como suponer que se la allanará (que en caso de certeza, hace innecesaria la demanda).

3. **Preservar la privacidad** *(Servare secreto private)*: Cuanto menor sea la verosimilitud del derecho invocado, tanto mayor es la necesidad de asegurar este requisito. En el Derecho penal, se justifica claramente por la doctrina del árbol envenenado. En el resto de los fueros, siempre es posible que como resultado de esta medida se produzcan violaciones al derecho a la privacidad del futuro demandado. En este sentido, es preciso considerar que:

a. Analógicamente con el caso de la intervención de comunicaciones telefónica o la revisión de correspondencia privada, el acceder a documentos resguardados en las computadoras de una determinada persona, siempre e inevitablemente hará que el técnico que realiza la tarea, el personal que lo certifica y los testigos que asisten al acto accedan a información privada que no tenga relación con los hechos investigados (hechos conducentes y pertinentes a la argumentación expresada). Esto es inevitable de la misma manera en que al abrirse un sobre o una carpeta es imposible determinar a priori su contenido. Se revisa la correspondencia por orden judicial, los hechos pertinentes se utilizan y el resto se descarta y se devuelve a su legítimo

propietario. No obstante, en el caso de documentos impresos, esto requiere de acciones que pueden ser revisadas por el funcionario interventor, dependiendo de su criterio si autoriza su apertura o no. Pensemos al respecto en la situación particular de un reconocimiento judicial en un estudio contable. Por el contrario, al acceder a la cuenta de correo electrónico de una determinada persona con el objeto de recolectar algunos de los mensajes, es inevitable observar los restantes (incluyendo en general su contenido). Para evitar este problema es necesario que en la autorización de medida previa, preliminar o prueba anticipada, el tribunal establezca con claridad y precisión meridiana cuál es el tenor de la tarea y con qué alcance y magnitud se desarrollará, especificando estricta y detalladamente la cantidad y calidad de información a recolectar. Este pedido debe ser fundado y declarado específicamente por quien solicita la medida. Una solicitud que pretende la descarga indiscriminada, indeterminada o indeterminable con precisión meridiana de los datos de una persona debe ser descartada in limine por el tribunal requerido.

b. Asegurar la privacidad de la información accidentalmente accedida requiere de un proceso de selección y descarte que es responsabilidad de la parte requirente, del tribunal requerido y de los funcionarios designados para participar en el acto, en particular del representante del Ministerio Público que actúa en lugar del futuro demandado, preservando por sobre todo sus derechos (la verdad objetiva de un evento siempre debe ser la resultante del debido proceso y nunca el objetivo principal de este) y del profesional que realiza la labor técnica.

c. Si bien la presencia del requirente y de sus consultores técnicos es un derecho que figura en la mayoría de los códigos de procedimiento de los distintos fueros, incluyendo al laboral, que curiosamente no admite la figura del consultor técnico*16*, pero que permite la presencia en ciertos actos jurídicos de las partes y sus consultores técnicos*17*, la tarea siempre debe ser encomendada por el tribunal a un perito de oficio (seleccionado de entre la lista disponible) el que deberá ajustarse estrictamente a la solicitud de recolección aprobada por el juzgado que la ordena, debiendo actuar con carácter restrictivo en todos los casos. Es una tarea transdisciplinaria, que requiere de una interacción constante entre los actores y que de preferencia debería ser supervisada por algún funcionario del tribunal interventor.

d. Por supuesto, esta medida podría llegar a afectar a los Poderes Legislativo, Ejecutivo y Judicial, al Ministerio Público, a los órganos constitucionales autónomos, a los gobiernos regionales y locales y a las entidades autárquicas (entes todos ellos que respecto de las medidas cautelares están exceptuados de prestar contracautela), las embajadas, consulados y entidades dependientes

del cuerpo diplomático o consular extranjero. En estos casos, es posible que participen otros derechos tan importantes como la privacidad, entre ellos: el secreto de Estado, el secreto profesional, los funcionarios determinados en la Ley de Inteligencia Nacional[18] y todo otro privilegio que en razón de su cargo o investidura detente el propietario de la información a ser accedida.

e. Por otra parte, siempre debe tenerse en cuenta la jurisdicción y competencia del tribunal que autoriza la medida. De hecho, muchas de las ubicaciones espaciales de la información a ser accedida pueden resultar ajenas a dicha jurisdicción o competencia, ya sea porque el contenedor se encuentra fuera de los límites de nuestro país o porque el tema considerado en el litigio difiere en su competencia respecto del país al que se necesita acceder. Este tema es crítico y actualmente apenas en etapa de desarrollo, especialmente en las relaciones comerciales de alcance internacional, transnacional o regional. Por otra parte, es frecuente que el servidor en que obra la información a ser accedida se encuentre allende las fronteras patrias, en este caso la decisión deberá ser tomada considerando las relaciones internacionales vigentes entre los países afectados.

f. Es normal que muchos de los contratos comerciales que afectan a los importadores-exportadores de bienes de servicios de nivel PyMEs se realicen por intercambio de mensajes de correo electrónico. Considerando que en nuestro país existen jurisdicciones donde las competencias civil y comercial están unificadas y otras en que no, lo mismo se puede afirmar respecto de otros países especialmente limítrofes (caso Brasil). En tanto y en cuanto el alcance de la medida previa, preliminar o prueba anticipada se limite a servidores dentro de nuestro país, el tema resulta sencillo, pero como la mayoría de las empresas que operan en el Mercosur resguardan sus datos donde les resulta más económico hacerlo (en nuestro país, en su país o en otro lugar del mundo, acorde con la oferta y demanda de almacenamiento disponible en un determinado entorno temporo-espacial), es muy importante que se aclare la ubicación física de la información a recolectar, para facilitar la decisión judicial aprobando o denegando la medida solicitada.

g. En todos los casos, los criterios de selección de la información recolectada deberán ser revisados a posteriori por el tribunal interventor y por la parte demandada, a efectos de establecer el carácter estrictamente pertinente y conducente de estos.

h. La información que no sea utilizada para la causa, o que no termine en una demanda formal, deberá ser destruida, bajo la supervisión del juzgado que autorizó la medida. Esta es la razón principal por la cual la prueba documental informática que ha sido recolectada debe encontrarse resguardada en un recipiente que asegure su transporte, preservación y disponibilidad por parte

del tribunal interventor. Una inveterada costumbre hace que, al ser entregada en barandilla, dentro de un sobre lacrado, con el acta correspondiente y la cadena de custodia preservada, el empleado de turno proceda a abrir el sobre exponiendo su contenido (CD o DVD, con su hash y protección contra escritura). Esta práctica debe ser desterrada de los estrados tribunalicios, ya que en el hipotético caso de que el titular del estrado decida que la prueba no es pertinente y ordene su destrucción, nada puede asegurar que no se hayan efectuado copias de esta, destinadas a otros fines espurios que nada tienen que ver con la supuesta demanda argumentada.

i. La confiabilidad de la prueba depende de su estricto confinamiento, secuestro formal (orden de secuestro, acta, testigos, funcionario certificante y representante del Ministerio Público, preferentemente miembro del tribunal que autoriza la medida) y cadena de custodia estricta. En este sentido, deben colaborar todos los actores involucrados en la tarea y en particular los miembros del tribunal que interviene[19].

La recolección de prueba documental informática como paso previo a la presentación de una demanda (in audita altera pars), como medida preliminar o prueba anticipada, es una herramienta de enorme valor para el proceso judicial, que debe ser gestionada y producida mediante una acción transdisciplinaria integradora y conjunta que permita la participación efectiva, eficiente y eficaz de la totalidad de los actores involucrados en ella.

Su aceptación y aprobación por parte del tribunal interventor es un tema que trasciende a la mera tarea técnico pericial y que involucra en particular un proceso de toma de decisión signado por sus características propias y particulares. No nos es posible establecer una norma precisa y rigurosa que indique en cuáles circunstancias debe ser otorgada y en cuáles denegada. Como todo en el Derecho, debe ser analizado en relación con cada caso en particular; no obstante, este como tantos otros intentos es una forma de aproximar información que facilite al juez el proceso de toma de decisión en el momento de resolver el incidente detallado.

Fallo relacionado

El siguiente fallo tal vez sea de utilidad al momento de analizar la argumentación antes presentada:

"Aguilar y Asociados SRL c/Native Software SRL s/ordinario" – CNCOM – Sala F – Buenos Aires, 17 de abril de 2012.

Y Vistos:

1. Viene apelado por el accionante, el pronunciamiento del apartado cuarto de fs. 141vta./42 que denegó la solicitud tendiente a obtener una copia de seguridad de los sistemas informáticos ubicados en la sede de Native

Software SRL.

Juzgó la a quo que la sola invocación de la posibilidad de adulteración de la información contenida en los ordenadores de la accionada no constituía elemento suficiente para justificar la medida, además que tampoco avizoraba la urgencia evidente exigida por el artículo 326 CPCC a partir del hecho que la mediación prejudicial había concluido por decisión de las partes hacía más de un año (v.gr. el 7/12/2010). El memorial de agravios corre en fs. 154/55.

2. Acerca de la cuestión, cabe referir que la prueba anticipada constituye un modo excepcional de producir prueba ante tempus. Su naturaleza es de carácter conservatorio y su finalidad tuitiva en relación a una probanza que se considera trascendente para el proceso. De ahí que esa finalidad protectoria haga acercar los conceptos de prueba anticipada y medida cautelar (cfr. Arazi-Rojas, Código Procesal Civil y Comercial de la Nación, ed. Rubinzal Culzoni, Santa Fe, 2007, Tº II, p. 136).

Si bien en el caso el promotor no pretende la producción de la prueba pericial informática indicada en el apartado D de fs. 139, lo concreto es que su solicitud se dirige a asegurar la obtención de elementos de información necesarios para la posterior producción de tal medio probatorio.

Así planteada la cuestión, dentro del marco de provisionalidad con sujeción al cual es aprehensible toda petición de estas características y a partir de lo que prima facie surge de la documentación acompañada –v.gr. acta de constatación notarial de fs. 7/16 y contenido de la correspondencia epistolar de fs. 18/21– aparece verosímil la motivación del demandante sobre la necesidad de obtener una medida como la de la especie con el claro propósito de aventar el ulterior ocultamiento, modificación, destrucción, alteración o pérdida en el objeto probatorio (cfr. en este mismo sentido, CNCom. Sala E, 17/11/11, "Softmind Sistema SA c/Cardoso Cristian Hugo y otros s/diligencia preliminar").

Es que ciertamente, la imposibilidad o dificultad en la posterior producción probatoria que exige el artículo 326 citado debe ser entendida en un sentido amplio (cfr. Di Iorio, Alfredo, Prueba anticipada, Abeledo-Perrot, Bs. As., 1970, p. 30); sobre todo en esta particular temática, donde la vulnerabilidad y fragilidad que los registros informáticos ofrecen permiten presuponer el peligro en la demora, ya que pueden desaparecer o resultar afectados por algún virus (cfr. CNCiv., Sala J, 17/05/07, "Asociación de Beach Soccer Argentina c/Asociación del Fútbol Argentino", cita La Ley on line: AR/JUR/2852/2007).

En suma, resulta conducente la disposición de medidas tendientes a asegurar la verdadera eficacia del proceso judicial, siempre procurando el

mayor de los respetos a las garantías constitucionales en juego: el debido derecho de defensa y el aseguramiento del principio de bilateralidad.

3. Sentado lo expuesto, habiéndose juzgado acreditados la verosimilitud del derecho invocado y el peligro en la demora de conformidad con lo dispuesto por el artículo 326 del Código Procesal, admítese la obtención de una copia o back up de toda la información contenida en los discos rígidos, extraíbles o no, servidores y cualquier otro tipo de respaldo posible existente en los diversos ordenadores que se encuentren en el domicilio de Native Software SRL.

La diligencia deberá cumplirse mediante la designación de un perito licenciado o ingeniero en sistemas que deberá designar la jueza de grado, con la participación del Oficial de Justicia que corresponda y con citación del Defensor Oficial. Este último, en razón del derecho de defensa previsto por el artículo 327 del Código Procesal y para representar a la parte contra la que se lleva a cabo la medida, a la cual no podría serle notificada ya que su anticipación en el conocimiento podría posibilitar la alteración o modificación del objeto probatorio a adquirir (cfr. Falcón, Enrique M., Código Procesal Civil y Comercial, Ed. Abeledo-Perrot, Tº. I, p. 538).

Se estima pertinente que, a fin de evitar todo tipo de especulaciones sobre la factibilidad de una modificación ulterior de los datos obtenidos, una vez efectuada la copia de seguridad, el auxiliar interviniente haga entrega de la misma al Oficial de Justicia quien, a su turno, deberá adjuntarla al expediente para su correspondiente reserva.

4. Por lo expuesto, se resuelve: revocar el decisorio del apartado 4° de fs. 141vta./42 y admitir la realización de la copia de seguridad en cuestión con los alcances estipulados en el decurso de la presente.

Encomiéndase a la a quo la designación de un perito, único y de oficio, licenciado y/o ingeniero en informática, así como las diligencias tendientes a la citación del Defensor Oficial y del Oficial de Justicia de la zona correspondiente.

El doctor Rafael F. Barreiro no interviene en la presente decisión por encontrarse en uso de licencia (art. 109 del Reglamento para la Justicia Nacional).

Notifíquese y oportunamente devúelvase. Fdo.: Alejandra N. Tévez, Juan Manuel Ojea Quintana Ante mí: María Florencia Estevarena, Secretaria.

15 Uno de los fundamentos más absurdos y sin embargo más comunes es mostrar dos contenedores de información similares o disímiles (por ejemplo, dos CDs) que contienen un mismo archivo y decir: "cualquiera se da cuenta de que este es el CD 'A' y este es el CD 'B'", intentando desacreditar esta afirmación sobre la identidad estricta entre ambos archivos. Esta identidad de los archivos y su copia digital (bit a bit) debe ser destacada en todo momento, ya que implica la imposibilidad de revertir los procesos de modificación sobre un archivo determinado, por medios directos. En consonancia con esta falacia argumentativa, se suelen resguardar las sesiones orales realizadas en los tribunales correspondientes, mediante la filmación y grabación del audio en soporte digital (normalmente DVD), luego el original es firmado por el secretario del tribunal y en el mejor de los casos identificado y autenticado por el número de serie del DVD. Luego se realizan copias y se entregan a las partes que lo requieran. Sin embargo, no se efectúa certificación alguna (digesto digital: rutina de hash) sobre los datos contenidos en el DVD. Si una de las partes a posteriori edita el material y lo ofrece a su vez como elemento indubitado (ya que está externamente certificado por el tribunal), el conflicto subsiguiente puede llegar a ser indecidible por medios informático forenses.

16 *Ley 18.345, Art. 91. Prueba pericial – "Si la apreciación de los hechos controvertidos requiriere conocimientos especiales en alguna ciencia, arte, industria o actividad técnica especializada, se podrá proponer prueba de peritos, indicando los puntos sobre los cuales habrán de expedirse. Los peritos serán nombrados de oficio en todos los casos y su número podrá variar de uno a tres, a criterio del juez y de acuerdo con la índole o monto del asunto, circunstancias que también se tomarán en cuenta para fijar el plazo dentro del cual deberán expedirse. Únicamente en casos excepcionales los peritos podrán pedir y el juez ordenar que, con carácter previo, la o las partes interesadas depositen la suma que se fija para gastos de las diligencias. Los peritos podrán ser recusados con causa en el plazo de tres días posteriores a su designación". Art. 92. Peritos de la Administración Pública – "El juez podrá designar peritos a profesionales o técnicos dependientes de la Administración Nacional".*

17 *Ley 18.345, Título V. Aplicación del Código Procesal Civil y Comercial. Art. 155. Disposiciones aplicables – "Se declaran aplicables, salvo colisión con norma expresa de esta ley, las siguientes disposiciones del Código Procesal Civil y Comercial: artículos... 457, 459, 464, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477... Las demás disposiciones del Código Procesal Civil y Comercial serán supletorias en la medida que resulte compatible con el procedimiento reglado en esta ley".*

CPPN, Práctica de la pericia, Art. 471. – "La pericia estará a cargo del perito designado por el juez. Los consultores técnicos, las partes y sus letrados podrán presenciar las operaciones técnicas que se realicen y formular las observaciones que considera pertinentes. Presentación del dictamen, Art. 472. – "El perito presentará su dictamen por escrito, con copias para las partes. Contendrá la explicación detallada de las operaciones técnicas realizadas y de los principios científicos en que se funde. Los consultores técnicos de las partes dentro del plazo fijado al perito podrán presentar por separado sus respectivos informes, cumpliendo los mismos requisitos". Dictamen inmediato, Art. 474. – "Cuando el objeto de la diligencia pericial fuese de tal naturaleza que permita al perito dictaminar inmediatamente, podrá dar su informe por escrito o en audiencia; en el mismo acto los consultores técnicos podrán formular las observaciones pertinentes".

18 *Ley 25.520, Art. 17. – "Los integrantes de los organismos de inteligencia, los legisladores miembros de la Comisión Bicameral de Fiscalización de los Organismos y Actividades de Inteligencia y el personal afectado a la misma, así como las autoridades judiciales, funcionarios y personas que por su función o en forma circunstancial accedan al conocimiento de la información mencionada en el artículo anterior deberán guardar el más estricto secreto y confidencialidad. La violación de este deber hará pasible a los infractores de las sanciones previstas en el Libro II, Título*

IX, Capítulo II, artículo 222 y/o 223 del Código Penal de la Nación, según correspondiere".

19 Una metodología típica y frecuente de obtener información para la toma de decisiones consiste en solicitar una medida previa, preliminar o prueba anticipada, ante una supuesta violación de un derecho propio (normalmente un incumplimiento contractual). Acordada la medida, se recolecta información de manera legal y aparentemente legítima, luego se desiste de la acción y se conserva la información (este método de espionaje industrial y comercial es un clásico desde antes de la aparición de la informática, solo ha cambiado el medio para efectuarlo). De ahí la necesidad de imponer un estricto cuidado al analizar y aprobar estas medidas para evitar que el tribunal se convierta en partícipe primario de un delito o en cómplice involuntario de actividades ilegítimas (aunque frecuentes en el ámbito civil y comercial). Lo mismo es aplicable a la correspondencia de una persona cualquiera; cada día se producen más divorcios por temas relacionados con el chat y el correo electrónico. La virtualidad de la correspondencia es un hecho, la preservación de su privacidad un derecho, no absoluto, pero derecho al fin.

CAPÍTULO 3
REVISIÓN JURISPRUDENCIAL

Fallos relacionados

La gestión de la prueba documental informática se halla limitada por algunos elementos esenciales, que no pueden ser soslayados por quien la solicita ni por los encargados de llevar a cabo la tarea pretendida. Al respecto, es necesario considerar el Fuero en que se está realizando la labor técnica:

1. En el Fuero Penal, la decisión de recolectar prueba documental informática estará fundada en un documento emanado del fiscal o del juez que intervienen en la causa; para que esta recolección se realice en condiciones óptimas de validación, certificación y traslado, es necesario que cuente con los siguientes elementos esenciales:

a. órdenes de secuestro y allanamiento, confeccionadas en legal forma.

b. Descripción detallada y explícita de las tareas a realizar. Entre ellas, el secuestro de elementos físicos, la inspección de programas y determinación de sus relaciones lógicas, el criterio de selección de la información a recolectar. Pero, sobre todo, los límites de dicha recolección para asegurar el derecho a la privacidad de las partes de la causa y de terceras personas. Esta última consideración raras veces aparece en la orden de secuestro emitida por la autoridad judicial correspondiente.

c. Presencia de un funcionario judicial que convalide el acto y pueda tomar decisiones al respecto, ante las posibles dudas surgidas entre los funcionarios de las Fuerzas de Seguridad, que brindan asistencia policial a la tarea, y los técnicos que la realizan. Esto debe incluir la presencia de testigos imparciales y culturalmente capacitados para entender lo que se les pide que observen (al menos la secuencia de acciones a registrar en el acta que describe los hechos y actos jurídicos realizados).

d. Presencia de personal técnico capacitado para que realice la tarea. Este tema es ineludible y sumamente polémico. Para dilucidarlo, voy a recurrir a la analogía: Nadie aceptaría la revisión de un cadáver por otro funcionario que no fuere el médico legista. Esta característica de médico legista brinda seguridad jurídica respecto de la necropsia realizada por el profesional, el informe que la describe y su validez legal. A partir de ese aserto, es suficiente con afirmar y aceptar que: “La Informática forense es a la Informática lo que la Medicina legal es a la Medicina”. Los requisitos académicos y profesionales establecidos para la Medicina legal y para la Informática forense deberían ser similares, desde sus respectivos campos de acción. En particular, los títulos

que certifican la idoneidad del profesional: Un médico legista es un médico que luego de recibido ha realizado una carrera de posgrado de médico legista, de por lo menos dos años de duración; no es concebible que la tarea pericial informático forense la realice un funcionario policial que en algunos casos solo cuenta con un título secundario y alguna instrucción somera impartida por la fuerza a la que pertenece. Este accionar es violatorio de los principios de debido proceso y legítima defensa, porque permite la manipulación de prueba que puede ser decisoria para la causa, por parte de personal cuya idoneidad profesional es al menos dudosa.

2. En el Fuero Civil y Comercial, la gestión de la prueba documental informática depende directamente de la acción de las partes y, por lo tanto, requiere otro tipo de recaudos y otra sucesión de actos, entre ellos:

a. Luego de la entrevista previa entre el cliente y el abogado que le brindará soporte técnico legal (patrocinio o representación), este último ante la necesidad de recolectar prueba documental informática con fines probatorios, debería requerir de inmediato la participación de un consultor técnico especializado (experto en Informática forense). La razón de esta reunión reside en la necesidad cierta de recolectar prueba que puede estar en poder de la parte consultante, de la futura contraparte o de terceros, clasificable como información privada o pública, que tal vez sea necesario certificar por medio de pruebas de informes (en particular, a los proveedores de servicios –ISP–) y en caso de negativa, revisadas, analizadas y resueltas por medios periciales (puntos de pericia previsibles). Seguidamente, describiremos el caso más complejo, a partir del cual es posible insertar otros ejemplos con menos requisitos.

b. Establecida la necesidad de recolectar información privada en poder de la contraparte o de terceros, se hace necesario solicitar esa medida como prueba anticipada, ya que el riesgo de pérdida por borrado doloso de los datos, al tener noticias de la futura demanda, es algo posible y sumamente probable como estrategia de defensa del demandable.

c. Para solicitar esa medida preliminar es necesario fundamentarla, evitando el rechazo in limine, por parte del juzgado que debe resolver el incidente previo, ante la falta de justificación cierta, evidente y comprobable de dicha medida. Esto significa que es necesario comprobar el peligro en la demora y la posibilidad de desaparición de la prueba pretendida, ante acciones positivas por aporte del futuro demandado. Una de las formas de comprobarlo es presentar documentos digitales que brinden credibilidad a la pretensión. Esos documentos digitales están conformados por la información en poder de la parte consultante.

d. Actuando en consonancia, la primera acción a realizar es la recolección,

certificación, preservación y resguardo de la información en poder del consultante. Esta acción requiere de la intervención del consultante, el abogado patrocinante, el consultor técnico y un escribano público. Consiste en las tareas ya descriptas en otros artículos anteriores[20], las que finalizan generalmente con el resguardo de los datos en un disco óptico no regrabable, con su correspondiente digesto (hash), acta de recolección protocolizada por el escribano y dentro de un sobre lacrado y certificado por el escribano. Este digesto debe colocarse a su vez en el acta realizada por el escribano, en el exterior del sobre lacrado y en la cadena de custodia que se inicia en ese momento. Es también conveniente realizar varias copias de los sobres y sus discos ópticos contenidos, ya que por error en su manipulación puede producirse la ruptura de la cadena de custodia, anulando la prueba recolectada. Esta circunstancia es frecuente al entregar la prueba en el juzgado, donde, sin tomar recaudo legal alguno, el funcionario a cargo de la barandilla simplemente rompe el sobre, extrae el contenido y se niega a firmar la cadena de custodia. El tener otros facsímiles para presentar alternativamente es una muestra de buenas costumbres por parte del abogado patrocinante. En la práctica, se realizan copias para: el escribano, la parte consultante y por lo menos cuatro para el abogado (al solicitar la prueba anticipada deberá presentar una copia en el tribunal designado y seguramente necesitará otras dos al presentar la demanda, para el juzgado y para la contraparte), todas con sus correspondientes cadenas de custodia, iniciadas, firmadas y certificadas por el escribano interventor, con su correspondiente constancia en el acta protocolizada.

e. Es necesario destacar que la documental informática puede constituirse en elemento probatorio de muchos hechos jurídicos. Por esta razón, es menester analizar su pertinencia probatoria. Por ejemplo, ante el constante aumento de los contratos a distancia, utilizando la modalidad de intercambio de mensajes de correo electrónico (vulgarmente denominado “contrato por e-mail”), se genera el problema de su validez como instrumento privado. Evidentemente, no lo es por carecer de firma comprobable[21] (son muy escasos los mensajes que se intercambian utilizando firma electrónica y prácticamente inexistentes aquellos que cuentan con firma digital). Esta circunstancia no lo invalida totalmente, ya que puede ser aceptado como una prueba por escrito[22], de ahí la necesidad imperiosa de preservarlo mediante los recaudos antes establecidos, para que pueda ser considerado válido por el tribunal interventor. Teniendo siempre en cuenta que, aunque por sí solo no tenga la entidad de instrumento privado, concatenado causalmente y relacionado con la correspondiente prueba de informes, con la prueba pericial y con toda otra prueba indiciaria aportable, puede conformar una estructura probatoria sólida, coherente, creíble y comprobable.

f. La solicitud de prueba anticipada se respalda mediante la argumentación que corresponda (para justificar el peligro en la demora y el riesgo de pérdida de prueba) y con la documental informática resguardada según el procedimiento anterior. Es decir, se acompaña de la misma manera en que se agrega cualquier otro documento en soporte de papel. La documental informática es solo una especie de la documental clásica (bibliográfica, foliográfica o pictográfica), que difiere de aquella únicamente en el soporte (digitalizado por medios ópticos o magnéticos). Los resguardos de esta prueba anticipada son similares a los referidos a la primera recolección frente al escribano, si bien la realizará un experto designado por el tribunal de entre los que obran en la lista. Es importante, al solicitar la prueba, especificar claramente el perfil del profesional que debería realizarla, en razón de las múltiples listas de peritos similares, de ahí que el abogado debe interiorizarse de las incumbencias profesionales de cada uno. También es de rigor la concurrencia del abogado al acto, ya que como tiene experiencia en el tema (por lo menos a partir de la acción primigenia de resguardo de datos de su cliente) puede hacer observaciones y exigir el cumplimento de todas y cada una de las tareas necesarias para asegurar la prueba (digesto, acta, cadena de custodia, etc.).

g. Al confeccionar la demanda, es necesario tener en cuenta de manera relacional, integrada y transdisciplinaria, la estrategia procesal a utilizar en el caso particular considerado. Respecto de la documental informática, recolectada por medio de la acción directa sobre la información obrante en poder de la futura actora y a partir de la implementación de la prueba anticipada, en general debe ser convalidada por medio de prueba de informes. Esta prueba, por ejemplo, en el caso de los mensajes de correo electrónico resguardados, consistirá en el pedido de informes al proveedor del servicio de mensajería y correo (ISP), para que convalide el origen, destino, hora GMT de cada mensaje recolectado y, de ser posible, su contenido. Este último punto dependerá de los resguardos que mantenga el ISP y de la antigüedad del mensaje considerado: cuanto más reciente mayor es la posibilidad de alcanzar éxito en esta gestión, de ahí que, en temas informático forenses, la celeridad constituye la norma.

h. Por supuesto, es muy posible que la contraparte niegue el contenido de la documental informática presentada. Por esta razón, es imprescindible preparar los puntos de pericia necesarios para respaldarla oportunamente. La mejor forma de realizar esa tarea y limitarla a los puntos pertinentes y conducentes que brinden soporte a la estrategia procesal planificada, es efectuarla en conjunto entre el consultor técnico seleccionado (experto en Informática forense) y el abogado patrocinante.

3. En lo que se refiere al Fuero Contencioso Administrativo, este guarda relación directa con el Procedimiento Penal, con algunos visos del Procedimiento Civil y Comercial; por esta razón es necesario analizar cada caso en particular y actuar en consecuencia, adaptando cada accionar a las necesidades del administrado o de la administración representados. En particular, pero no exclusivamente, ante la comprobación de pagos impositivos, declaraciones juradas y otras acciones que pueden ser realizadas mediante medios digitales (electrónicos, magnéticos u ópticos).

4. Respecto del Fuero Laboral, el accionar es muy similar al Fuero Civil y Comercial, pero hay que tener especialmente en cuenta el principio de in dubio pro operario al momento de analizar las relaciones contractuales que rigen para este último. En particular, los convenios de confidencialidad y los reglamentos internos que organizan y norman el uso de la tecnología informática propietaria de la empresa empleadora. El experto deberá analizar en profundidad a la hora de recolectar datos solicitados por la empresa para no vulnerar la privacidad del trabajador; por ejemplo, los datos obrantes en la base de datos del personal de la empresa son de propiedad de esta, pero contienen datos sensibles que seguramente están protegidos por la ley 25.326. De la misma manera, la cuenta de correo electrónico personal del empleado es de su propiedad exclusiva y no puede ser accedida a pedido del empleador, sin la correspondiente orden judicial. Aunque a veces es consultada por el empleado desde su lugar de trabajo, quedando indicios ciertos y factibles de recolección en las computadoras donde se produce la consulta y/o en los servidores que las administran, a pesar de la prohibición explícita y firmada ante el empleador, esto no autoriza su acceso sin autorización de su legítimo propietario (el empleado a quien pertenece). Es quizás el caso más delicado y requiere del accionar integrado y transdisciplinario estricto entre el operador del Derecho y el experto que realiza la tarea.

Los errores cometidos en la planificación, desarrollo, implementación y certificación descriptos en los puntos anteriores generan dificultades muchas veces insalvables, las que pueden llevar a la anulación y descarte de la prueba producida. En tal sentido, es interesante analizar los siguientes fallos:

1. Cámara Nacional de Apelaciones en lo Criminal y Correccional. Sala V. Causa N° 39.803 “V. C. W. E. s/infr. ley 11.723”. Procesamiento 49/169, Buenos Aires, 22 de septiembre de 2010.

En este caso, se desestima el acta de secuestro por fallas en la individualización de los elementos secuestrados:

“La presente instrucción adolece de un vicio insalvable que impide su subsistencia como actuación válida, por su incidencia negativa en el derecho de defensa del imputado. En efecto, la reconstrucción de la materialidad del

suceso y la subsiguiente responsabilidad se han estructurado en base al acta de secuestro documentada a fs. 35/37, que, no obstante cumplir con algunas de las formalidades legalmente previstas, carece de la debida individualización del material incautado".

"Esa falencia se reiteró en los actos siguientes, destinados a determinar positiva o negativamente la ilegalidad de ese material".

"En efecto, ni en el acta de apertura para el inicio pericial, ni en el curso del examen de la especialidad se procedió a su íntegra individualización (fs. 61 y 68/71)".

"El mentado informe concluyó que la totalidad de los soportes ópticos tipo DVD-R eran apócrifos; sin embargo, no se dio cumplimiento al punto 1 de la respectiva orden pericial (fs. 41), tendiente a identificar la totalidad de los discos compactos secuestrados…".

"[…] al momento de recibírsele declaración indagatoria al imputado (fs. 316/320), oportunidad en que este introdujo una duda directamente vinculada con el defecto que se viene señalando; dijo entonces que no podía asegurar que las películas que se encontraban en el juzgado fueran las mismas que se secuestraran en el allanamiento".

"Esa duda y las consecuencias que de ella emergen constituyen la médula de la apelación por la que en este momento intervenimos".

"Las particularidades del caso y la falencia especificada afectaron el derecho de defensa del imputado […], cabe remarcar que el defecto señalado en párrafos anteriores impide asegurar fehacientemente que la cadena de custodia de los elementos inicialmente secuestrados no haya sido vulnerada".

"Atento a lo expuesto, decretaremos la nulidad del acta de secuestro de fs. 35/37 y de los actos consecuentes: el informe pericial fs. 69/71, la declaración indagatoria de fs. 316/320, el auto que dispuso la falta de mérito de fs. 323/327/vta., y, finalmente, la resolución recurrida (artículo 168 del Código Procesal Penal de la Nación)".

Aunque las razones aducidas en el caso considerado aparecen como sólidas y convincentes, es conveniente que el lector analice esta resolución en relación con la que sigue, ya que podrá comprobar por sí mismo notorias diferencias en el criterio procesal aplicado en cada caso. Este es el tipo de inconvenientes en la gestión de la prueba documental informática que el operador del Derecho debe prevenir y evitar a toda costa. Solo la labor técnica transdisciplinaria (operador del Derecho – consultor técnico) e integrada permitirá arribar a buen puerto en la gestión de la documental informática y sus pruebas relacionadas.

2. Expte. N° 14.349/2010. "C. S. D. G. c/CPACF" (Expte. 24.233/09). Cámara

Nacional de Apelaciones en lo Contencioso Administrativo Federal. Sala V. 10/02/2011.

En este fallo, el tribunal admite como prueba válida la impresión de un mensaje de correo electrónico, sin el resguardo técnico informático forense de dicho mensaje:

"Por otra parte, si bien el recurrente pone en duda que el mensaje (cuya existencia también niega) haya sido enviado por él, ya que pudo haber sido enviado por otra persona con acceso a la cuenta, es importante observar que no niega la existencia de la cuenta: [...], desde la que se envió el mensaje cuestionado. En tal contexto, el hecho de que el nombre de usuario de la cuenta coincidiera con las iniciales de su nombre y apellidos, así como la 'firma' que aparece al final del mensaje (indicando su nombre completo, nombre del estudio jurídico, domicilio y teléfonos; v. fs. 9), abonan la tesis del a quo, en cuanto a que el envío se produjo desde esa cuenta".

Esto es equivalente a considerar que el texto que aparece como opción en los aplicativos de correo electrónico, denominada "firma" por la aplicación, pero sin condición alguna que la asimile a la firma ológrafa, a la digital o a la electrónica, ya que es solo texto introducido por el usuario y que puede ser perfectamente simulado por un operador calificado, debería ser equiparado con una firma ológrafa. Esto transformaría a los mensajes de correo electrónico que tienen un texto dudosamente autenticatorio respecto de la identidad de su autor en un instrumento privado, algo que no tiene asidero técnico o legal alguno.

"En ese entendimiento, no aparece debidamente refutada la afirmación del tribunal actuante en cuanto a que 'corre por su exclusiva responsabilidad [del imputado] permitir el acceso al mismo a pocos colaboradores de su confianza' (considerando 6). Aun cuando la dirección electrónica de origen fuera una cuenta 'masiva', el recurrente reconoce que estaba afectada al uso de sus tareas profesionales, ya que desde allí se evacuaban consultas".

"Aun cuando el recurrente afirma que personas allegadas profesionalmente a él y con acceso a la cuenta de correo electrónico pudieron enviar el mensaje, la presunción de inocencia se debilita en la medida en que este tenía responsabilidad exclusiva en la decisión de quiénes podían hacer uso de esa cuenta y enviar mensajes desde ella".

El tribunal ignora la posibilidad del acceso a la cuenta por parte de terceros, utilizando herramientas de violación de la seguridad informática (hacking, cracking, etc.) y otorga a una cuenta de correo electrónico una característica de credibilidad, confiabilidad y autenticidad que no están respaldadas por criterio científico, tecnológico o técnico alguno; de hecho, esta seguridad es violada a diario, de lo contrario no serían posibles los delitos informáticos propios e

impropios[23].

"En efecto, atento a los elementos de juicio que revelan las condiciones de tiempo, lugar y modo en que se emitió el mensaje cuestionado, era una carga procesal del recurrente desvirtuar los elementos de juicio que, inequívocamente, conducen a considerarlo autor de la conducta susceptible de reproche ético".

Aunque parece de sentido común que no es el administrado quien debe probar su inocencia, sino la administración quien tendría que probar su culpabilidad, por esas peculiaridades del Derecho administrativo (evidentes en el solve et repete, el deber de colaboración y la implícita presunción de culpabilidad) se invierte la carga de la prueba.

3. Cámara Nacional de Apelaciones en lo Criminal y Correccional Federal. Sala I. "Vázquez, Manuel y otros sobre Rechazo del Planteo de Nulidad". 5 de mayo de 2011.

En este fallo, la Cámara Nacional en lo Criminal y Correccional Federal ordenó que se realicen nuevas pruebas sobre las computadoras secuestradas en el marco de la investigación en desarrollo por presunto enriquecimiento ilícito, con el fin de establecer los motivos de disparidad entre las conclusiones a las que arribaron los peritos de la Policía Federal Argentina y los de la Universidad de Buenos Aires.

Se trata de un fallo paradigmático y ejemplificador, donde la potestad aparentemente ilimitada en el decisorio del a quo es encausada y analizada desde la más pura racionalidad y teniendo en cuenta la naturaleza de la ciencia, tecnología y técnicas que brindan soporte a la Informática forense.

"En su escrito impugnativo, los defensores de Manuel y Julián Vázquez insistieron en señalar que la cadena de seguridad de los ordenadores peritados había sido violada, y que ello era 'responsabilidad de quienes hicieron el allanamiento, ya que por desidia o ignorancia efectuaron deficientemente el sellado de las máquinas, o fue mal hecho, ya que... los puertos podían ser usados sin necesidad de romper faja alguna'. Destacaron las declaraciones testimoniales de los peritos – 'ratificando que la cadena de seguridad de los ordenadores se encontraban violada'– y 'se preguntaron cómo era posible que la División Apoyo Tecnológico Judicial de la Policía Federal Argentina, pese a poseer la misma tecnología, no encontrara los archivos descubiertos por los expertos de la UBA'".

"Por otro lado, destacaron que el a quo no los notificó de los resultados de la pericia efectuada por la UBA, sino que tomaron conocimiento de ello a través de la prensa, por lo que debieron concurrir al tribunal a peticionar copias de las actuaciones correspondientes. Hicieron saber que, a partir de allí, se denunció penalmente la filtración de información".

A pesar de los evidentes e insalvables errores procedimentales ocurridos en esta causa, los que son de conocimiento público, es preciso destacar que: muchas veces las Fuerzas de Seguridad deben cumplir su tarea sin contar con los recursos apropiados (carencias instrumentales, de programas específicos y en especial de personal capacitado). Por otra parte, en lo referido a la Universidad, es frecuente que allí se recurra a supuestos "gurús" de la Informática forense, cuyo único título académico informático consiste en la credulidad de sus seguidores. Es así que se designa como peritos a: matemáticos, contadores, administradores de empresas o informáticos sin especialización alguna. Esta característica es propia del ambiente universitario, donde se acostumbra dar por sentado que todo el que opina con fervor y grandilocuencia es un catedrático de peso[24] y su análisis es creíble por la misma razón, sin analizar los antecedentes de quien expone y sin siquiera establecer la correspondencia de su título de grado con el tema que analiza.

Por otra parte, la prensa (eterno adversario de la ciencia) intenta adecuar la información a su propia visión personal de los hechos, lo que contribuye a complicar y desacreditar a las instituciones participantes. Son innegables los errores cometidos, pero no son propios de una sola institución, sino del sistema en general; pocos son los que conocen realmente de Informática forense, menos aún los que tienen los títulos que se requiere, pero son muchos los que opinan sobre el tema y son convalidados únicamente gracias al poder discrecional del juez para admitir y convalidar peritos, sean cuales fueran sus capacidades e incumbencia profesionales (bajo la triste y obsoleta figura del "idóneo").

"II.Observado el tenor de los planteos originarios, el confronte con las constancias actuariales nos permite advertir una seria falencia en el decisorio del juez de grado a la hora de responderlos. Básicamente, bajo pretexto de un relevamiento superficial de los cuestionamientos, como si fueran meros quebrantamientos formales, el magistrado ha esquivado la dimensión sustancial del sistema de garantías que es el verdadero eje de la crítica (Binder, Alberto, El incumplimiento de las formas procesales. Elementos para una crítica a la teoría unitaria de las nulidades en el proceso penal, Ed. Ad-Hoc, Buenos Aires, 2000, p. 84)".

Es destacable este párrafo del fallo, ya que implica la obligación por parte del juez de escuchar a las partes en relación con los cuestionamientos referidos a la posibilidad de introducción de prueba espuria durante el resguardo de esta en sede policial o judicial. En efecto, el criterio anterior establecía una especie de regla de honestidad implícita en los juzgados, que los eximía de responsabilidades y cuidados, respecto de los elementos probatorios

almacenados. Es común observar el trato desprejuiciado, indolente y desprevenido, en cuanto a los elementos que se entregan en custodia, desde el momento en que son dejados en barandilla (rotura de lacres, sellos, fajas de clausura, incumplimiento de cadena de custodia, etc.) hasta el almacenamiento (apilados en cualquier lugar, sometidos a condiciones extremas de temperatura, presión por estiba inadecuada, campos electromagnéticos de todo tipo y accesibles por cualquier persona que ingrese al recinto del juzgado). Por una vez, surge la duda respecto de la idoneidad implícita en los juzgados para proteger la prueba retenida en custodia y bajo su responsabilidad.

"En relación al peritaje elaborado por los expertos de la UBA, el Dr. Oyarbide recordó que la defensa de Manuel y Julián Vázquez había designado perito de parte y que no era posible que se plantee una nulidad luego de haberse consentido el acto por conocerlo y dejarlo avanzar. Un argumento del mismo tenor fue dirigido a la defensa de Ricardo Jaime".

"Finalmente, sostuvo que la cadena de custodia no fue violada –'en ningún momento los elementos han estado fuera del ámbito de control jurisdiccional'– y aseguró, ergo, que el contenido de las máquinas permaneció inalterado".

"Si bien incumbe a los jueces determinar cuáles son los extremos comprendidos en el litigio, sin que estén obligados a seguir a las partes en todas sus alegaciones, sí deben dar tratamiento a los puntos propuestos que sean conducentes para la solución del juicio (Fallos 233:147). Según se advierte, este tratamiento no ha sido el debido en este caso pues se ha abusado de afirmaciones dogmáticas, rituales, sacrificando 'la justicia sustancial a formas vacías' (Carrió, Genaro y Alejandro, El recurso extraordinario por sentencia arbitraria, Abeledo-Perrot, Buenos Aires, 1987,

p. 194). Al mismo tiempo, más allá de la discrecionalidad del juez como director de la encuesta, ha prescindido de realizar prueba decisiva, conforme más adelante se verá".

En efecto, cuando se habla de cadena de custodia, referida a la prueba indiciaria informática, esta debe ser estricta, documentada y suscripta por todos los que han intervenido en el proceso de recolección, traslado y resguardo, incluyendo a los miembros del tribunal que reciben y entregan los elementos probatorios. La práctica pericial nos indica que este último hecho constituye la excepción y no la norma en el accionar judicial.

"III.La verdadera discusión que encierra esta incidencia se vincula con la posibilidad de utilizar prueba obtenida por medios ilícitos o prohibidos".

"Más allá de la autenticidad o no de los intercambios epistolares, las partes introducen la posibilidad de que los documentos electrónicos hayan sido

colocados clandestinamente en las computadoras mientras ellas se encontraban secuestradas a disposición del juzgado".

"La CN, como derivación del derecho a la intimidad, declara inviolables la correspondencia epistolar y los papeles privados (art. 14). Esta protección, sin embargo, encuentra limitaciones en la ley reglamentaria (art. 28) y serán los jueces quienes en cada caso autorizarán las injerencias en el ámbito de la intimidad de las personas cuando ellas se encuentren justificadas. Así fue como se llevó adelante el allanamiento y el secuestro de las computadoras de las oficinas de Manuel y Julián Vázquez, diligencias legalmente ordenadas por el Dr. Norberto Oyarbide a fs. 937/938".

"Mas si esas computadoras fueron contaminadas con información introducida luego del secuestro, se abren, al menos, dos posibilidades: una, que esos datos no sean auténticos; y la otra, que aun siéndolo no estuviesen albergados originariamente en ese soporte cuya inspección ordenara el juez".

Por lo tanto, el juez debe asegurar la protección estricta de los activos informáticos secuestrados, durante toda su gestión, incluyendo su almacenamiento dentro del local del juzgado. Debiendo cumplir todas las normas de seguridad informática e Informática forense establecidas al respecto, las que no solo son dejadas de lado en la mayoría de los casos, sino simple y llanamente desconocidas por los miembros de los tribunales actuantes. No existe un tratamiento equivalente entre el resguardo en caja fuerte de ciertos documentos en papel, respecto de sus similares en soporte informático instalado (PC, notebook, netbook, etc.).

"De darse tanto uno como otro supuesto los archivos encontrados por los expertos de la UBA debieran ser excluidos de la prueba. La sospecha introducida por las defensas pretende en última instancia que así sea y encuentra, en respaldo de su postura, la llamada 'regla de exclusión', receptada localmente a partir del caso 'Charles Hermanos' (Fallos 46:36) y consolidada de allí en adelante en numerosas ocasiones (Fallos 303:1938; 306:1752; Peralta Cano; 333:1674). La regla no se conforma con proscribir la prueba falsa sino que está dirigida a excluir la prueba obtenida ilegalmente, sin importar su autenticidad ni la sospecha de culpabilidad (Carrió, Alejandro D., Garantías Constitucionales en el proceso penal, Hammurabi, Buenos Aires, 2003, p. 230), pues, frente a la investigación de la verdad como meta del procedimiento penal, hace valer la dignidad del ser humano y cierto ámbito de privacidad que le garantiza el Estado de Derecho (Maier, Julio B. J., Derecho procesal penal. I. Fundamentos, Editores Del Puerto, Buenos Aires, 1999, pp. 663/664 y sgtes.)".

"En síntesis, la eventual violación de la cadena de custodia impide asegurar

que los elementos secuestrados por orden del juez hayan contenido originariamente los archivos encontrados en el estudio de la UBA, lo que, en otras palabras, implica admitir que existen dudas no solo acerca de su autenticidad sino también del modo en que ingresaron a la encuesta. Estos interrogantes plantean, como posibilidad, que en autos se haya producido una actuación ilegítima –incluso de quienes participan o auxilian a la instrucción– o bien un hecho ilícito –en perjuicio de derechos constitucionales– del que la administración de justicia no puede pretender ser beneficiaria (Fallos 303:1938; 306:1752)".

"V.En otro orden, teniendo en consideración las manifestaciones vertidas por los defensores de Manuel Vázquez al momento de informar oralmente ante esta Alzada en relación con el estado público que han tomado los correos electrónicos que fueron extraídos de las computadoras –cuyas impresiones pudieron observarse en algunos diarios del país–, y con el objeto de asegurar, del modo más amplio posible, la efectiva vigencia de la presunción de inocencia de la que goza todo imputado, se torna necesario instar al magistrado de primera instancia a extremar las medidas necesarias a fin de evitar que, en el futuro, vuelva a presentarse una situación similar a aquella".

"En virtud de los argumentos desarrollados en los párrafos que anteceden, el tribunal resuelve: Declarar la nulidad del auto de fecha 23 de diciembre de 2010 –fs. 78/89–, debiendo el a quo proceder de acuerdo a lo expresado en los considerandos (arts. 123 y 166 del CPPN)".

Estamos ante una resolución contundente y conteste con los hechos acaecidos; sería de esperar que se constituya en referente y ejemplo para otros juzgados, intentando armonizar las acciones imprescindibles para el resguardo y protección de la documental informática, en condiciones técnicas y procedimentales ajustadas a la disciplina informático forense.

La resolución por Cámara

Cámara Federal. Sala I. Causa Nº 46.744. "Fiscal s/apela declaración de nulidad de informe pericial" Jdo. Fed. Nº 7 Sec. Nº 14. Reg. Nº 458.

Buenos Aires, 24 de mayo de 2012.

"2°) Al pronunciarse esta Cámara el pasado 5 de mayo de 2011 en este mismo incidente (resolución registrada bajo el n° 428), se indicó que '...la verdadera discusión se vinculaba con la posibilidad de utilizar prueba obtenida por medios ilícitos o prohibidos...' pues '... más allá de la autenticidad o no de los intercambios epistolares, las partes introducen la posibilidad de que los documentos electrónicos hayan sido colocados clandestinamente en las computadoras mientras se encontraban

secuestradas a disposición del juzgado…' y expresamente se señaló que la sospecha introducida por las defensas, que resultaba necesario disipar a través de las diligencias pertinentes, se nutría '…primero, del escaso control permitido a las partes –por ejemplo, omitiendo notificaciones–; segundo, de la existencia de dos estudios con resultados opuestos (v. fs. 1093/1099 y 12.319); y tercero, de la afirmación de los expertos de la Universidad de Buenos Aires que manifestaron […] en virtud del estado del material a periciar que nos fuera entregado, no puede asegurarse que se haya mantenido la cadena de custodia…'"[25].

Es de destacar la sospecha sobre la contaminación de la prueba en sede judicial y la necesidad de mantener la cadena de custodia, para asegurar la confiabilidad de la prueba y que esta pueda ser utilizada como elemento de apoyo a la decisión judicial (sentencia).

"4°B) El carácter 'irreproducible' de la primera de las pericias practicada (División Apoyo Tecnológico de la Policía Federal) si bien resultó acreditado con las comprobaciones efectuadas posteriormente sobre el modo como aquélla se llevó a cabo y sobre el resguardo (mejor dicho, no resguardo) de la evidencia por parte de dicha autoridad policial, ya se proclamaba –en esencia– desde mucho antes".

"En efecto, la sola naturaleza de los elementos sometidos al examen pericial era ya suficiente alerta sobre la cautela y precauciones que correspondía adoptar, especialmente la observación de cada una de las solemnidades que debía revestir todo acto que los tuviera por objeto, tal como el máximo control en su desarrollo. Sin embargo, ninguna de esas circunstancias halló lugar aquí. Ello condujo, tal como los peritos de la UBA primero sugirieron y luego comprobaron, a la imposibilidad de aseverar que las computadoras secuestradas contuvieran –sin alteraciones, supresiones o adiciones– los mismos archivos que tenían registrados al momento de su secuestro y, por tanto, a tornar ilusoria la exacta reproducción de un estudio sobre ellas. La forma en que fue ordenado y conducido el peritaje hecho por la Policía Federal frustró así un segundo examen que, sin resquicio a duda, permitiera afirmar que los archivos consultados eran los mismos que se encontraban presentes en los ordenadores desde su incautación".

"Al respecto cabe recordar, en primer lugar, el informe producido por los técnicos de la Facultad de Ciencias Exactas y Naturales de la UBA obrante a fs. 12.318/12.323, donde previnieron expresa y puntualmente acerca de las condiciones en que recibieron las computadoras y dieron cuenta de la imposibilidad de asegurar –en vistas del modo como se llevó a cabo el estudio anterior– la cadena de custodia de la evidencia que habrían de analizar".

"En ese informe, a fs. 12.318/12.319, se da cuenta de lo siguiente: '…1) Encabezado del informe… 2) Introducción… 3) Validación y verificación de la cadena de custodia: A. Mediante escrito de fecha 22/12/2009 se fijó fecha para el inicio de la pericia el día 2 de febrero de 2010. En el mismo escrito se solicitó al juzgado la información correspondiente que avale el mantenimiento de la cadena de custodia del material secuestrado en donde se indicase fechas y horas en que dicho material fue obtenido por primera vez, y las fechas y horas en que el mismo fue utilizado en previa/s pericia/s si las hubiere, como así también los métodos informáticos utilizados para evitar la contaminación de la prueba'".

Nuevamente, se señala la necesidad de preservar la cadena de custodia y se destaca la característica de "prueba irreproducible". Este tema ya lo hemos tratado, pero es necesario reiterarlo: los actos y actividades periciales deben poder ser reproducidos por otros profesionales, en igualdad de condiciones, en cualquier lugar del mundo, con elementos similares, a posteriori, y obtener idénticos resultados. Si una tarea pericial implica riesgo de perder la prueba o modificarla, impidiendo su reproducción, dicha circunstancia debe ser informada al tribunal interventor, para que el juez determine su pertinencia o no y en particular para asegurar la notificación de las partes y facilitar la presencia de todos los interesados en asistir al acto pericial.

"B. En la fecha 2 de febrero de 2010 al iniciarse la pericia, y en el momento de entrega del material a periciar, el juzgado no proveyó la correspondiente documentación respaldatoria del mantenimiento de la cadena de custodia, indicando solamente en forma verbal que el material habría sido secuestrado el día 28/7/2009 y la pericia anterior fue finalizada el día 3/8/2009".

"C. La cadena de custodia se refiere a la fuerza o cualidad probatoria de la evidencia. Debe probarse (si fuese requerido por el juez o fiscal) que la evidencia presentada es realmente la misma evidencia recogida en la escena del crimen, o recuperada a través de algún testigo, entregada por la víctima, o por otros sujetos o adquirida originalmente de alguna otra forma".

"D. Para cumplir con este requisito debemos mantener un registro minucioso de la posesión y de la cadena de custodia de la evidencia. Este puede asegurarse mediante un sistema de recibos y registro minucioso".

"E. La cadena de custodia también implica que se mantendrá la evidencia en un lugar seguro, protegida de los elementos, que no se permitirá el acceso a la evidencia a personas que no están autorizadas".

"F. En el documento anexo denominado 'Descripción narrativa de la recepción de los efectos' puede observarse que el material recibido del juzgado no se encontraba adecuadamente protegido para su uso, ya que los puertos de alimentación eléctrica no estaban adecuadamente inhabilitados".

"G. Es una buena práctica de la profesión forense informática 'mantener y verificar la cadena de custodia' para asegurar que todos los registros electrónicos originales no han sido alterados".

"H. En tal sentido y en virtud del estado del material a periciar que nos fuera entregado, no puede asegurarse que se haya mantenido la cadena de custodia".

"De los rudimentarios métodos utilizados por la Policía Federal Argentina para la preservación de la evidencia es muestra también el hallazgo posterior de numerosos 'archivos con fecha de modificación anterior a la fecha de creación' lo que resulta una 'inconsistencia […] inexplicable desde el punto de vista técnico' (ver informe … Universidad Tecnológica Nacional a fs. 281 y Anexo VIII al que remite)".

"Véase además que el propio perito […] , que citan los Sres. Fiscales, da cuenta en su informe en copia obrante a fs. 244/248 que '…del análisis de los informes técnicos periciales existentes a fs. 1093 y 1098 del Expte. 12446/2008 del Juzgado Federal N° 7, se observa que en ninguno de ellos se describe con claridad las operaciones técnicas utilizadas, herramientas empleadas, ni se hace mención a la utilización de bloqueadores de escritura. Tampoco se precisan las fechas en que se realizaron las operaciones…', como así también que '…las alteraciones a las que se refiere… serían producto de una negligencia operativa en las pericias informáticas efectuadas…'".

Aunque los requisitos detallados en el fallo no se corresponden estrictamente con las necesidades de resguardo de la prueba documental informática, sino más bien con las condiciones genéricas de toda cadena de custodia, adecuándolos a las características particulares de la prueba tratada, constituyen una buena guía a respetar. Por ejemplo, no se ha señalado la especial circunstancia que afecta a la documental informática: el principio de identidad atípico que la caracteriza (un bit es idéntico a otro bit y, por lo tanto, la copia digital de un archivo es imposible de distinguir de su original).

"De lo dicho hasta acá se desprende que las prácticas llevadas adelante por la Policía Federal Argentina sobre el material secuestrado contaminaron la evidencia, convirtiendo lo que el juez instructor había considerado una 'operación pericial extremadamente simple' y 'repetible' en una medida irreproducible. De haberse dado la debida intervención a las defensas para que pudiesen presenciar y controlar aquellas prácticas, tal como sucedió con el estudio de la UBA, el inconveniente podría haberse superado, pero ello no sucedió. Se violó la regla de garantía contemplada expresamente por el artículo 201 del código de rito –como derecho constitucional reglamentado– lo cual conduce a la necesaria aplicación de la sanción que allí mismo también se establece (cfr. Maier, ob. cit., p. 163)".

"Es por eso que se afirma que la peritación recién adquiere estado procesal cuando se cumplen todas las formalidades previstas por la ley (Clariá Olmedo, Jorge A., Derecho procesal penal", Tomo segundo, Marcos Lerner, 1984, Córdoba, p. 401); y que 'cuando la ley impusiera alguna formalidad especial para su producción, relacionada con el derecho de defensa de las partes, la observancia de ella será también condición sine qua non para que la prueba que se obtenga pueda ser regularmente incorporada. Por ejemplo, si se tratara de un acto definitivo e irreproducible, se deberá notificar previamente a los defensores (art. 201)…' (Cafferata Nores, José I. La Prueba en el Derecho penal, Ed. Depalma, Buenos Aires, 1994, p. 18)".

Nuevamente nos encontramos ante el problema de las tareas periciales irreproducibles y la necesidad de notificación a las partes para facilitar su presencia durante el acto pericial.

"Por lo expuesto, corresponde por confirmar la anulación de los peritajes producidos a fs. 1093/1095 y fs. 1097/1099 por la Policía Federal y a fs. 12.318/12.323 por la UBA (con sus respectivos anexos), debiendo proseguirse con la investigación del delito de enriquecimiento ilícito denunciado".

"En mérito de los argumentos expuestos, el tribunal resuelve: confirmar la resolución de fs. 288/309 en cuanto anula los peritajes producidos a fs. 1093/1095 y fs. 1097/1099 por la Policía Federal y a fs. 12.318/12.323 por la UBA (con sus respectivos anexos), debiendo proseguirse sin esos elementos con la investigación del delito de enriquecimiento ilícito denunciado".

"Regístrese, hágase saber a la Fiscalía de Cámara y devuélvase al Juzgado de Primera Instancia para que se cumpla con el resto de las notificaciones.

Sirva la presente de atenta nota de envío.

Jorge L. Ballestero Eduardo G. Farah Ante mí: Eduardo Ariel Nogales – Prosecretario de Cámara".

Aún queda mucho por tratar, pero al parecer el decisorio judicial se inclina en el mismo sentido que los requerimientos específicos que permiten asegurar la confiabilidad en la recolección de la prueba documental informática y su complemento: la prueba pericial informático forense, a los fines de brindar soporte al decisorio judicial.

[20] Recolección de información pública y privada en poder de nuestro consultante y de información pública obrante en Internet. No se puede recolectar en esta etapa información privada de terceros o de la contraparte, para hacerlo es preciso contar con orden judicial específica.

[21] Código Civil, Art. 1012. – "La firma de las partes es una condición esencial para la existencia de todo acto bajo forma privada. Ella no puede ser reemplazada por signos ni por las iniciales de los nombres o apellidos".

[22] *Código Civil, Art. 1190. – "Los contratos se prueban por el modo que dispongan los códigos de procedimientos de las Provincias Federadas: Por instrumentos públicos. Por instrumentos particulares firmados o no firmados. Por confesión de partes, judicial o extrajudicial. Por juramento judicial. Por presunciones legales o judiciales. Por testigos".*

Art. 1192. – "Se juzgará que hay imposibilidad de obtener o de presentar prueba escrita del contrato, en los casos de depósito necesario o cuando la obligación hubiese sido contraída por incidentes imprevistos en que hubiese sido imposible formarla por escrito. Se considerará principio de prueba por escrito cualquier documento público o privado que emane del adversario, de su causante o de parte interesada en el asunto, o que tendría interés si viviera y que haga verosímil el hecho litigioso".

[23] *Delito informático propio es el que afecta a la información como bien jurídico protegido (ejemplo: sustitución de identidad). Delito informático impropio es el delito ya tipificado (robo, hurto, defraudación, extorsión, etc.) cometido utilizando herramientas informáticas.*

[24] *En especial si es extranjero, posee un apellido anglosajón o es políticamente correcto.*

[25] *Ver capítulo correspondiente a cadena de custodia en esta misma obra.*

CAPÍTULO 4
CRITERIOS A TENER EN CUENTA

Las posibilidades de falsificación de mensajes de correo electrónico

Técnicamente es posible falsificar un mensaje de correo electrónico y luego insertarlo en un determinado puesto de trabajo. Esta falsificación puede soportar el análisis pericial prima facie, sin embargo, debemos decir que aunque el juez no sea un experto en informática y los restantes operadores del Derecho se limiten al análisis jurídico de la prueba, sin intentar entender la naturaleza propia de esta, es posible brindar soporte probatorio a la justicia, si se mantienen ciertos recaudos procesales y técnicos. De ahí la imperiosa necesidad de planificar la recolección, sus relaciones y la posterior pericial en subsidio. Este, creemos, es el principal problema a resolver: la falta de predisposición profesional para trabajar en equipos mancomunados y con objetivos comunes.

Analizando la situación punto por punto, ¿es posible falsificar un mensaje de correo electrónico e insertarlo en un puesto de trabajo? Sí. ¿Qué debería hacer el experto ante esta posibilidad?

1. Efectuar la recolección de prueba en la máquina de su cliente, conjuntamente con toda la información pública disponible (en Internet, esto implica incluir los datos públicos obrantes respecto de la contraparte).
2. Solicitar una medida previa o preliminar (in audita altera pars, en Civil y Comercial), para resguardar la información obrante en las máquinas de la contraparte y de terceros relacionados.
3. Al presentar la demanda, ofrecer los elementos recolectados en su totalidad y solicitar una prueba de informes al ISP, para que nos diga si los mensajes recolectados coinciden en fecha, hora, origen y destino, con los que hemos reunido.
4. Idéntica constatación por informes respecto de los alojamientos de información propia y de la contraparte (alocación de páginas web, reservorios externos de información, mecanismos de comunicaciones, cuentas de correo públicas, empresariales y privadas, etc.).
5. Ante la posible negativa por la contraparte de los elementos ofrecidos en los puntos anteriores, solicitar pericia informático forense en subsidio, para resolver las cuestiones planteadas. Es necesario ponerse en lugar del adversario y prevenir sus acciones legítimas o ilegítimas (esta es una tarea que todo buen operador del Derecho debería efectuar rutinariamente), entre ellas

la posibilidad de falsificación de algún mensaje de correo electrónico.

6. Ahora la cosa se pone más compleja para el falsario, porque debe sustituir no solo un mensaje, sino también los datos obrantes en el servidor del ISP, para que coincidan en hora GMT, origen y destino.

7. Por supuesto, hay que explicar a S. Sa. que es preciso analizar la prueba en conjunto y luego tomar decisiones acordes con este análisis integrador. Un mensaje de correo electrónico (que no es un instrumento público, ni privado, según nuestro Código Civil), por sí solo no debería ser prueba suficiente, pero relacionado con el resto de la prueba (información confirmatoria o negatoria, informes diversos y pericial en subsidio) puede constituir un excelente conjunto indiciario probatorio, donde se deben tener en cuenta las posibilidades de falsación.

8. Es claro que la labor pericial se basa principalmente en el desconocimiento del delincuente; si este conoce en profundidad los mecanismos periciales, tiene más posibilidades de burlarlos. En nuestro caso, el problema reside en que los delincuentes estudian, aprenden, intercambian información y mantienen una permanente actitud de actualización tecnológica y técnica[26]. En ese sentido, los profesionales involucrados en la prueba indiciaria informático forense (operadores del Derecho, criminalistas e informáticos), por diversas razones no corren a la par de los delincuentes ya que tenemos la ventaja de la formación científica, que es poco frecuente en la delincuencia (la proporción de hackers con formación universitaria completa es mínima), la interacción profesional y académica, la posibilidad de actuar de manera inter y transdisciplinaria, deberíamos poder compensar las ventajas que nos sacan los delincuentes a diario. ¿Qué hay que hacer? Simplemente estudiar e interactuar.

Ejemplo de accionar ante eventualidad previsible

Ante una visita de cualquier empresa que reivindica derechos de terceros (en particular, comprobación de la existencia de licencias de programas instalados), pero sin el poder de policía para efectuarlo in situ, lo que implica que debe contar con la autorización específica del visitado para acceder a sus sistemas, o limitarse a actuar conforme a la ley (hay que tener un protocolo de procedimiento en la empresa, para actuar ante la visita sorpresiva, es decir un plan de acción y un plan de contingencia, para que sepan cómo actuar) y cuya solicitud ha decidido ser aceptada por aquel funcionario (público o privado) que tenga la potestad de hacerlo:

1. Recibirlos y hacerlos acompañar, durante toda la visita, por personal de la empresa.

2. Autorizarlos a comprobar la existencia de las licencias en las máquinas. No

se los autoriza a operar las máquinas en modo alguno.

3. Toda la inspección se hace en presencia de un abogado de la empresa y de sus administradores de sistemas y de seguridad informática, que comprobarán paso a paso:

a. Que únicamente se acceda a los registros de las licencias.

b. Que no se visualice ninguna otra información pública, privada, reservada, confidencial o secreta de la empresa, ni de terceros.

c. Que se cumplan con los requisitos de privacidad que la gestión de información requiera.

d. Que las máquinas sean operadas únicamente por sus operadores naturales (usuarios de la empresa).

e. Que la autorización para observar información de la empresa sea explícitamente otorgada por el propietario de la información, acorde con la distribución de roles, funciones y organigrama de la empresa.

f. Que no se realice registro informático alguno de las tareas realizadas, salvo a solicitud de un miembro de la empresa (ni captura de pantallas, ni transferencia de archivos, ni ninguna otra tarea informática empleando las computadoras de la empresa).

g. En caso de transgresión, se dará por finalizada la inspección y se exigirá, para concurrir nuevamente, la orden judicial que corresponda.

h. No se permitirá que ninguna persona extraña a la empresa conecte equipo alguno a la red de datos y/o eléctrica de esta.

i. Los concurrentes deberán demostrar su representatividad para el acto (algo así como la legitimación activa para el acto), es decir, poder, orden judicial, título que los habilita para realizar este tipo de tarea, matrícula, etc.

No existe peor enemigo del seudoinocente que la conciencia culpable. Para ingresar a los activos informáticos de una persona (física o jurídica) de manera compulsiva, es necesario, en un Estado de Derecho, contar con autorización legal expresa, representada por una orden de allanamiento, confeccionada en tiempo y forma, por aquellas autoridades judiciales que tienen la potestad de hacerlo. Si quien quiere revisar los activos no la tiene, simplemente debe ser invitado a abandonar el lugar y regresar cuando disponga de ella. Aun en el caso de que la consiga, debemos recordar:

1. La orden de allanamiento debe especificar estrictamente el o los locales a ser accedidos, la oportunidad y horarios dispuestos para esa diligencia.

2. No puede tener cláusulas ambiguas ni genéricas infundadas (por ejemplo: “que se acceda a todos los locales del establecimiento”), ya que esto implicaría una grave violación al derecho a la privacidad de sus ocupantes. La determinación específica e inconfundible de los locales a acceder está implícita

en el derecho de defensa y debe estar fundada en la necesidad de recolectar elementos probatorios conducentes y pertinentes a la investigación judicial en proceso.

3. En el caso de la orden de allanamiento con autorización de recolección de prueba documental informática, este documento debe contener, de manera precisa, clara y sin posibilidad de falsas interpretaciones, su alcance y extensión. No se deben admitir generalidades que provoquen claras indeterminaciones en el acceso a la información, que podrían derivar en robo, sustracción o derivación de datos innecesarios para el proceso (incluyendo la factibilidad de instrumentar subrepticiamente mecanismos de espionaje comercial y/o industrial)[27].

4. Los datos a recolectar deben estar detallados de manera precisa y estar conformados únicamente por aquella información disponible, necesaria para constituir la prueba documental informática estrictamente pertinente y conducente a los fines de asegurar el debido proceso a las partes. Nada debe quedar a criterio del profesional que realice la tarea, o al arbitrio de las partes y autoridades que lo certifiquen. La responsabilidad por la enumeración, descripción, selección y requerimiento de información, detallada en la orden de registro, es exclusiva del tribunal que la autoriza y solicita, lo que debe constituir un elemento de control de oficio o a pedido de parte, para el órgano judicial de instancia superior que deba convalidar el empleo procesal de la prueba documental informática secuestrada.

El uso de formas alternativas de resolución de conflictos

Otro elemento que se ha integrado definitivamente a la problemática informático forense es su posible y altamente probable participación en controversias a resolver mediante métodos alternativos de resolución de conflictos. El auge del comercio internacional a nivel binacional, regional o mundial y la necesidad de reducir tiempos de negociación, costos operativos y principalmente movimiento de personal con el consiguiente desgaste del elemento humano y costo agregado de horas hombre destinadas a viajes, alojamiento, concertación de entrevistas y recuperación, hacen que muchos de estos negocios se realicen por medio de intercambio de mensajes de correo electrónico o por ingreso a páginas web comunes, compartidas o no.

La conexión y relación de comerciantes con intereses afines es un servicio de amplia difusión en otros países y que ya ha dejado de ser incipiente en el marco del Mercosur para pasar a ser una realidad bastante accesible, para los que prefieren el elemento electrónico-digital como medio de negociación comercial. La necesidad de que los peritos nos capacitemos para interactuar

en casos en que nuestra actividad sea requerida, ya no desde el ambiente judicial o empresarial, sino con fines de asesoramiento o consultoría para conciliaciones, arbitrajes, etc., es una realidad ineludible si no queremos quedar fuera del sistema (no es el Derecho quien impone las normas al comercio, sino el comercio quien impulsa la evolución del Derecho y, como auxiliares de este, es preciso estar a la altura de las circunstancias).

Es imprescindible asegurar la disponibilidad de la tarea de recolección metodológicamente realizada, para resguardar la prueba documental informática a presentar en el litigio alternativo. Recordemos que este tipo de procesos no judiciales se caracteriza por la flexibilidad e informalidad, de manera similar a las presentaciones del administrado ante un reclamo contra la administración dentro del Derecho administrativo.

Para poder consensuar un nombre con las partes, es necesario conocer, reconocer y acceder a una lista de expertos disponibles. Esta es una deuda con el sistema, dado que no existe o solo es accesible in voce. Lamentablemente, ni siquiera los Colegios de Profesionales pueden aportarla. Ante un pedido ofrecen lo que tienen, mezclando informática con electrónica, contabilidad, administración de empresas, etc., lo que aumenta la confusión a la hora de seleccionar un perito con el perfil pretendido para la tarea a realizar. Esta circunstancia no solo afecta a los tribunales arbitrales no permanentes, ya que no conocemos ningún caso de un tribunal arbitral en lengua castellana que tenga un listado de peritos en Informática forense.

En cuanto a la remisión de los puntos de pericia, nos encontramos en lo que los informáticos llamamos un caso de “abrazo mortal”, ya que para confeccionar los puntos de pericia, de manera profesional y seria, es preciso ser asesorado por un experto, pero para conseguir el perfil del experto es necesario contar con los puntos de pericia. Otra tarea que debería realizar el consejo profesional respectivo, pero que generalmente es postergada ante otras tareas más urgentes.

Respecto de mantener el secreto del arbitraje a priori, al seleccionar al experto, es una condición especialmente importante porque permite preservar el secreto comercial y su socio directo: el secreto industrial. Creemos que es una costumbre que debería extenderse a los litigios judiciales en su totalidad, evitando de esta manera estimular la susceptibilidad del posible elegido, en relación con la causa a discutir y los montos involucrados.

La audiencia de conciliación local o remota constituye una sana costumbre, que en nuestro Derecho suele utilizarse con bastante frecuencia en el Derecho penal y en menor grado en las restantes ramas judiciales. La explicación in voce de los peritos y sus argumentos, esta especie de careo entre pares, suele clarificar más las cosas que el análisis puro y llano de los puntos

controvertidos y su justificación científica, criminalística, tecnológica y técnica. En particular (y en el ámbito judicial en general), no se hace mención a una alternativa válida y sumamente importante en el ambiente arbitral del Derecho internacional privado: la teleconferencia. Esta forma de comunicación constituye la solución más adecuada para la separación física de las partes, el tribunal y los expertos, evitando todos los problemas que una reunión física in personae trae aparejados, que no difiere de los inconvenientes de la negociación comercial, de la que hablamos con anterioridad.

En lo que hace a la retribución de tareas, es algo sumamente particular y que dependerá de la tarea a realizar y la negociación entre el experto, el tribunal y las partes. Lo importante es fijar los precios por anticipado para evitar malos entendidos, pero esta es una norma general para cualquier tarea profesional onerosa que se deba encarar.

Aunque no escapa a las reflexiones anteriores, es preciso destacar que las citadas tareas también pueden incluir accesos e inspecciones individuales o colectivas por medios remotos. En efecto, el ambiente de negociación al que me he referido suele incluir hechos jurídicos que transcurren en muy distintas jurisdicciones, dentro o fuera de un mismo país. De ahí que el lugar del hecho real sea reemplazado por el lugar del hecho virtual propio, y que los medios de simulación y modelado de intercambio de información sean el instrumento más adecuado para representar, interpretar, comprender, analizar, modelar y explicar de manera argumentativa y lógicamente coherente, con su correspondiente soporte científico, tecnológico y técnico.

La decisión de quienes van a participar de una determinada inspección ocular virtual corresponde al tribunal arbitral (o al negociador, conciliador, mediador, etc.), pero debería ser analizada de forma transdisciplinaria e interdisciplinaria por todos los actores de la disputa (incluyendo partes, operadores del Derecho y expertos). La minimización de costos y tiempos se logra utilizando los medios virtuales disponibles, igual que en el tema anterior.

Como pregoneros de la Informática forense, tenemos la visión futura de una inserción adecuada y profunda de esta especialidad criminalística no solo en el ambiente judicial y empresarial, sino en todos los medios alternativos de resolución de conflictos, ya sea por medios adversariales o no adversariales. Como toda futurología, habrá que esperar el paso del tiempo para conocer los resultados.

Tratamiento de residuos informáticos

En este caso, la Informática forense actúa brindando soporte conceptual y procedimental a las ciencias aplicadas que se relacionan con la protección del

medioambiente. Sin embargo, su aporte es sustancial, en razón de que:

1. Es de conocimiento general el problema de la eliminación de los desechos instrumentales informáticos, los cuales básicamente se dividen en dos grupos:
2.

a. Elementos propios de computadoras e instrumentos similares (PC, celulares, componentes dispersos, teclados, pilas, baterías, fuentes de alimentación, gabinetes, parlantes, mouse, etc.).

b. Elementos de conectividad (cables, conectores, fibra óptica, antenas, etc.).

3. También es fácilmente reconocible la contaminación del medioambiente por saturación con ondas del espectro radioeléctrico (antenas de microondas, reproductores de señal de telefonía móvil, etc.).

4. No es tan conocida la contaminación producida directamente en el ciberespacio y que termina afectando al medioambiente real en que se desenvuelve la vida humana. A este punto en particular nos referiremos en el presente capítulo.

La basura ciberespacial

Desde las ciencias reconstructivas de la historia humana (arqueología, paleontología, paleografía, etc.) ha sido costumbre establecida la búsqueda y revisión de los basureros que han dejado los grupos humanos en proximidades de sus asentamientos poblacionales. Comenzando con el análisis de los coprolitos (técnica también utilizada para entender las costumbres de los animales, en particular los extintos) para determinar las costumbres alimenticias, hasta la revisión de sus instrumentos para comprender el grado de avance tecnológico alcanzado por el grupo considerado, la basura ha sido y es una fuente de información sumamente interesante. Podemos afirmar que donde va el hombre va su basura. Estos desechos lo han acompañado en sus viajes fuera del planeta (la saturación del espacio por basura espacial es un problema de todos los días, que amenaza al individuo con recibir un premio, no pretendido, proveniente del cielo, en el momento menos esperado) y hasta otros planetas (banderas, robots de exploración, satélites que aterrizaron, etc.). No podía quedar fuera el ciberespacio.

Cuando el usuario interactúa con la red informática global (la famosa nube), no está tratando con un elemento esotérico situado fuera del universo, en una especie de limbo o nirvana desprendido de la realidad. Está interactuando con componentes informáticos físicos, de procesamiento, almacenamiento o conectividad, que se encargan de resguardar, transmitir, transportar, almacenar y distribuir la información a la que diariamente accedemos. Como resultado de esta interacción, se genera basura, que no es recolectada, por lo que sigue ocupando su lugar en el referido ciberespacio, y que por supuesto

nadie se ocupa de eliminar.

Entre los programadores es frecuente, al estudiar la historia de los sistemas operativos y sus desarrollos progresivos, referir una anécdota clásica: por un problema de prioridades, al revisar las tareas de una computadora correspondiente a la segunda generación (basadas en transistores) se descubrió un proceso que había estado suspendido durante más de un año, sin llegar a ejecutarse, porque su prioridad era muy baja y siempre quedaba en segundo plano ante otros procesos de mayor prioridad. La anécdota sirve para estimular al estudiante a revisar concienzudamente las prioridades que asignará a sus procesos durante la programación. Pero analizando el problema desde otro ángulo, vemos que el referido proceso, si no hubiera sido detectado y eliminado del sistema, habría continuado indefinidamente ocupando lugar en la computadora, sin esperanzas de ejecutarse, ni finalizar su cometido, con lo que es el primer ejemplo de basura informática lógica, detectado y referido anecdóticamente.

Cuando un usuario recibe decenas o miles de avisos, propagandas, cadenas solidarias, ofertas, etc., no solicitadas, en su casilla de correo electrónico, suele ignorarlas, borrarlas o colocarlas en el área denominada “Spam”. Normalmente, el proveedor de servicios de Internet, y en particular el proveedor del servicio de mensajería y correo electrónico, tiene implementados sistemas automatizados para que periódicamente eliminen el contenido de Spam y de la pape lera de reciclaje de cada usuario. Esto no evita que muchos usuarios creen carpetas y guarden en ellas sus mensajes. Por ejemplo, quien escribe ha creado una carpeta por año para guardar los mensajes que intercambia con sus estudiantes. Tal vez fue necesario hacerlo en su momento, pero estas carpetas, a medida que pasan los años, pierden importancia y no vuelven a ser revisadas, ni accedidas, y se convierten entonces en basura informática que contamina y no aporta utilidad alguna. Tal vez esta conducta sea producto de la costumbre humana inveterada de actuar como auténticas vizcachas, que reúnen en sus hogares toda cosa que encuentran a su alrededor. Aunque nos duela reconocerlo, basta con observar nuestra biblioteca y reflexionar acerca de cuántos años de vida nos quedan (con cierta tolerancia basada parcialmente en la probabilidad y seguramente en el último mal de la caja de Pandora: la esperanza) y nos daremos cuenta de que hay muchos libros que nunca más serán abiertos. En este caso, podemos pensar que los estamos resguardando para la próxima generación (aunque al parecer el hábito de la lectura no está en expansión, ni mucho menos).

Algo similar pasa con los archivos informáticos. Escribimos, operamos, interactuamos y por supuesto resguardamos los resultados, para luego de un tiempo más o menos prolongado, olvidarnos totalmente de ellos. Esto

podemos comprobarlo simplemente revisando nuestra carpeta de “Mis Documentos”, o su equivalente, donde veremos que tenemos decenas, cientos y hasta miles de documentos de los que no solo desconocemos el contenido, sino que ni siquiera podemos imaginarlo a partir de su nombre y que si los abrimos con la aplicación que corresponda suelen sorprendernos porque ya habían pasado al olvido o porque nos habrían sido muy útiles ayer, si los hubiéramos tenido presentes.

Nos damos cuenta en particular cuando nos vemos obligados a dar formato al disco rígido de nuestra PC (“formatear” en la jerga informática). Si quien va a hacer la tarea nos pide que identifiquemos los archivos que debe resguardar, para luego reinsertarlos una vez finalizado el formateo del disco y lo hacemos a conciencia, veremos que más de la mitad de los archivos que hemos resguardado no tienen necesidad de ser preservados (música, películas, imágenes, textos, etc.) y que nuestra carpeta de almacenamiento que ocupa 1 Gigabyte se reduce a 5 o 10 Megabytes útiles e importantes. Hemos limpiado (higienizado, sanitizado nuestro sistema, obligados por la necesidad de formatear).

Este proceso se repite en la interacción con la red mundial: quedan almacenadas búsquedas, elementos de clasificación, estructuras de datos, programas inconclusos totales o parciales, archivos almacenados y cuyo propietario ya ha desaparecido (física o lógicamente) de la red; en definitiva, una multiplicidad de datos que se incrementan día a día, que van saturando la red, complicando su funcionamiento y que, por estar ocultos a la vista de los usuarios, no pueden ser fácilmente detectados ni eliminados. Esto se ha extendido a la telefonía móvil y sus dispositivos de comunicación y almacenamiento.

Así como se identifica, reúne, clasifica, procesa y almacena definitivamente la basura física producida por la sociedad humana, es necesario realizar una tarea similar con la basura ciberespacial. Este procedimiento requiere de la colaboración de todos los usuarios, al menos en los siguientes niveles de compromiso:

1. Usuarios individuales, respecto de sus equipos de computación y sus interacciones con las distintas redes a las que pertenecen.
2. Proveedores y programadores de Servicios de Internet y/o correo electrónico.
3. Organismos de control y supervisión de servicios de Internet (algo odiado por todos los cibernautas, pero de existencia real e innegable).

Los riesgos de contaminarse

En ocasión de realizar algunas pericias informático forenses en colaboración

directa con el Poder Judicial, hemos podido comprobar la siguiente serie de hechos:

1. Ante la aparición de algunas imágenes y videos pornográficos que involucraban evidentemente la participación de menores y hacían suponer la existencia de una red de producción e intercambio de este material, procedimos a realizar una búsqueda del material referido en la red. Búsqueda abierta, sencilla, mediante palabras claves (por ejemplo, utilizando un buscador del tipo "Ares" o similar y palabras comunes en el ambiente de pedofilia, como es el caso de "pthc").
2. Como resultado de la búsqueda anterior, recibimos miles de resultados concordantes, entre ellos algunos relacionados con la búsqueda real que estábamos realizando y que permitían relacionar a sus difusores con la red (y legalmente asociación ilícita) investigada. Esto es algo común en el ciberespacio, donde pululan auténticas bandas dedicadas a diversos delitos (terrorismo, narcotráfico, lavado de dinero, estafas, defraudaciones, pedofilia, trata de personas, hackers, crackers, "bobers", etc.), por lo que el resultado fue de utilidad a la investigación practicada.
3. Sin embargo, un porcentaje muy elevado de los resultados (más del treinta por ciento en el caso referido) se trataba de archivos que habían sido desvinculados de sus propietarios. Esto sucedía porque habían sido, entre otras razones, almacenados en reservorios públicos de información, se había difundido su localización y nada más. Quien los había colocado en el reservorio había desaparecido y la relación no podía ser restaurada. Mientras el reservorio exista, la información estará disponible para el que desee accederla.
4. Resumiendo, existe en la red gran cantidad de información perniciosa para los intereses de determinados usuarios (por ejemplo, pornografía infantil, para un padre que pretende alejar a sus hijos de este tema, o métodos caseros para fabricar drogas o narcóticos al alcance de los adolescentes, o difusión de prácticas sexuales perversas –sadomasoquismo, coprofagia, etc.–) que ha sido abandonada por sus generadores en el ciberespacio y está disponible para cualquiera que intencional o accidentalmente choque con ella.
5. Detectado el archivo, por supuesto no es posible identificar culpables, ni accionar contra persona alguna (directa o indirectamente). Es equivalente a cortarse con un vidrio, arrojado por el mar, en una playa remota. Lo que es evidentemente doloso (la creación y difusión de pornografía infantil, por ejemplo) ha devenido en accidental.

¿Por qué debemos proteger el ciberespacio?

Lo que sigue no deja de ser una verdad de Perogrullo, ya que se hace

evidente que los mismos riesgos que afectan al medioambiente real, físico, con el que convivimos, afectan a los cibernautas en su relación con el ciberespacio. Solo que parecemos no darnos cuenta de nuestro rol de cibernautas. Cibernauta no es solo el concentrado fanático de Internet, que pasa catorce horas diarias frente a la computadora, cuya vida es más virtual que real, también lo es nuestro hijo de cinco años que interactúa con la computadora y se reúne con otros amiguitos a disfrutar de esa amistad que la red le facilita, que acorta distancia y que permite acceder al conocimiento.

Esa misma red está cargada de basura informática peligrosa: películas pornográficas disponibles y sin propietario asociado, propagandas de elementos de todo tipo, desde armas hasta juguetes sexuales, en resumen todo lo que la sociedad real ofrece, pero que restringe a los menores. No nos estamos refiriendo a la pornografía infantil en particular, orientada precisamente a los fines de su difusión o a capturar menores con fines delictivos. En ese caso, se trata de un delito y debe ser analizado por las autoridades correspondientes (esa auténtica policía ciberespacial que lo recorre y diariamente da noticias de la detección, procesamiento y apresamiento de redes de pedofilia), pero restan aquellos casos en que el dueño de la información ha desaparecido, por cualquier razón dolosa, culposa o accidental que fuere, y la información permanece en la red, disponible para cualquiera que intencional o accidentalmente la encuentre y la acceda (sin importar la edad, ni la intención real de quien lo hace).

Como decíamos, existe una auténtica policía del ciberespacio, donde cada día irrumpen más policías reales[28] y miembros del Poder Judicial (no me interesa entrar en una discusión sobre la pertinencia de esta irrupción y si va a favor o en contra de los principios filosóficos de Internet), que la regula desde la lisa y llana prohibición (en países como China), hasta la revisión y monitoreo con fines particulares (EE.UU. y su control de mensajes de correo electrónico en búsqueda de palabras clave: “bomba”, “terrorismo”, etc.). Pero no existe ningún servicio de detección y recolección de basura lógica digital, con lo cual los efectos de la interacción ilegítima e ilegal en la red quedan preservados indefinidamente y al alcance de cualquier cibernauta que los encuentre en su camino.

Inserción legal de la problemática

Si nos basamos en el concepto clásico de persona, establecido en el Código Civil, veremos que básicamente nos encontramos con personas de existencia real (física, seres humanos, nosotros y nuestros prójimos) y personas de existencia ideal (las empresas). Hasta hace un par de décadas, estos elementos eran suficientes para establecer las relaciones jurídicas entre ellas, los hechos y actos jurídicos eran adjudicables y sometidos al control, supervisión y

resguardo judicial.

Ahora en el ciberespacio tenemos personas de existencia virtual. No son otra cosa más que perfiles creados en la red, que pueden o no relacionarse con una persona de existencia real o de existencia ideal, obrante en la realidad en que todos convivimos. Estas personas de existencia virtual pueden a su vez ser de existencia virtual real (imitan a personas físicas) o de existencia virtual ideal (imitan a empresas). De hecho, son susceptibles de adquirir y transferir derechos y obligaciones. A diario compramos elementos en empresas que ni siquiera tienen un local físico de ventas, referibles a direcciones en nuestro país o fuera de él. Sin embargo, de ninguna manera esta dirección nos permite asegurar la residencia real de quienes la gestionan.

Intentaremos clarificar esta afirmación: cuando vemos una dirección del tipo www.vendoinmuebles.com.ar, o www.mascotas.com.cl, o www.books.com, tendemos a suponer que estamos ante sitios situados, en este caso, en Argentina, Chile y EE.UU. No obstante, cualquier residente de Angola podría haber creado estos sitios, simplemente cumpliendo los requisitos del país respectivo (registro, en nuestro caso, ante NIC Argentina). De ahí que no tengamos forma efectiva de conocer la residencia real de dichas empresas.

En cuanto a las personas físicas, por lo menos los que interactúan con Internet, suelen tener varias personalidades virtuales (perfiles en la jerga informática). En el caso de quien habla, utiliza un perfil y un vocabulario particular y diferente para interactuar en estos entornos: el grupo de Informática forense de UTN, FRA, la lista de discusión de MENSA Argentina, su página de Facebook, el club de fanáticos de Gardel, el grupo de simpatizantes de su club favorito, etc. Cada uno de estos perfiles constituye una auténtica personalidad virtual, probablemente ninguna se aproxime a la realidad constituida por la persona física que la creó. Tanto es así que, visitando otras páginas de Facebook, suele ocurrir que la agraciada veinteañera que aparece en la página (foto incluida) nada tiene que ver con la también agraciada cincuentona que podemos contactar en la realidad. Sabemos cuál es la persona física, pero no podemos ignorar ni descartar a la persona virtual, porque esta persona virtual está interactuando con muchas otras personas virtuales y reales que tienen la imagen y la convicción (tal vez, en el fondo la esperanza) de estar interactuando con la veinteañera (esto incluye la más absoluta libertad de género real o virtual).

Hasta aquí estamos hablando de personalidades virtuales vs. personalidades reales e ideales. Sin embargo, la afectación de una de esas personalidades virtuales en particular puede dar lugar a acciones judiciales, por ejemplo, si los datos de una persona obrantes en una base de datos (perfil virtual) son erróneos, apócrifos, falsos, etc., puede prosperar perfectamente la acción de

amparo establecida en el artículo 43 de la Constitución Nacional (párrafo de Hábeas Data), solicitando su remoción o corrección, como medida autosatisfactiva o no. Luego podrá atribuir responsabilidades a quienes los introdujeron, de forma dolosa o culposa y pedir resarcimiento económico. Pero si esta modificación es producto de la interacción del precitado perfil (base de datos) con basura ciberespacial, deja de existir el responsable y cesa la posibilidad efectiva de eliminar el riesgo que esta implica (al desconocer su origen, desconocemos la forma de eliminarla).

En general, las relaciones entre determinadas personalidades virtuales (por ejemplo, el perfil de una joven modelo) y sitios inconvenientes para su perfil (asociaciones con páginas pornográficas, a partir del uso de buscadores de uso corriente), pueden ser atribuidas o asociadas con los proveedores del servicio de búsqueda, con los resultados jurisprudenciales antagónicos que todos conocemos, pero si es el resultado de una colisión con basura ciberespacial, esta relación se torna accidental y el Derecho deviene en abstracto. Como entre la basura ciberespacial pululan los programas maliciosos (virus, troyanos, agentes, etc.), la posibilidad de que ocurran estos "accidentes" es tanto mayor como mayor sea la basura ciberespacial que dejamos de recolectar, procesar y eliminar.

División de responsabilidades y tareas

Volviendo a nuestra clasificación original, podemos decir que:

1. Los residuos sólidos provenientes de los equipos de computación y las redes de conexión deben ser tratados acorde con lo que determina la ley y las normas en vigencia.

2. Los residuos provenientes de ondas del espectro electromagnético que saturan la biosfera deben ser tratados mediante acciones conjuntas y multidisciplinarias entre los organismos que los generan y quienes están encargados de su control (proveedores de telefonía móvil, emisores de microondas, entes de control de radiodifusión, etc.).

3. Los residuos ciberespaciales constituyen un riesgo para la integridad psicológica, moral y social de los cibernautas (considerando como tales a cualquiera que interactúe con la red local o mundial) y al menos deberían ser tenidos en cuenta en una interacción conjunta de las autoridades judiciales, los entes de regulación y los proveedores de servicios digitales (Internet, mensajería, correo electrónico, etc.). En este punto, el auxilio de los métodos informático forenses puede resultar en un auténtico servicio de detección y eliminación de basura lógica ciberespacial. ¿Es un tema primordial respecto de otros temas de seguridad? Seguramente no lo es, pero al menos deberíamos tenerlo en cuenta para algún futuro mejor.

26 Internet, además de sus insustituibles aportes a la difusión del conocimiento humano y su democratización relativa, ha tenido como complemento su falta de supervisión y mayor o menor ejercicio del libre albedrío de quienes la utilizan como herramienta de comunicación personal y social. Es por eso que también se ha conformado en una auténtica fuente de instrucción de delincuentes. Basta con colocar bomba o iniciador, o cualquier otra palabra clave, en el entorno de búsqueda adecuado, para que podamos acceder a métodos más o menos sofisticados de realización y consumación de delitos (contra la vida, la libertad y el patrimonio de terceros). Los delitos informáticos propios e impropios no escapan a esta realidad que nos toca vivir, apenas finalizada la primera década del siglo XXI.

27 Como ya hemos señalado, sería fácil solicitar una prueba anticipada, requiriendo acceder a un determinado sistema informático de una empresa, argumentando un incumplimiento contractual. Luego de acceder, robar la información crítica de negocios de la empresa (por ejemplo, la fórmula de una gaseosa archiconocida). Copiar dichos datos y luego simplemente no litigar. En este caso, el órgano judicial que autorizó la invasión en la privacidad comercial de la empresa estaría actuando como partícipe primario (involuntario, por supuesto) en la comisión del hecho. De ahí que la necesidad de determinar exactamente el alcance y extensión del material informático a recolectar como parte de la prueba documental informática pretendida, no es un tema superficial, sino un componente básico y elemental en la orden compulsiva de recolección. Ningún funcionario público puede aducir ignorancia al respecto, porque no hace falta conocimiento técnico alguno para prever y prevenir este tipo de actos; alcanza con el más puro y llano sentido común y el cuidado de un buen pater familiae, virtudes que deben formar parte de todo funcionario judicial que se precie de tal.

28 *Resumen de "Interceptación y monitoreo del correo electrónico", publicado en el Dial (http://www.eldial.com.ar/) por Federico Bueno de Mata, Humberto Martín Ruani y Aislan Basilio Vargas:*

"Marco general acerca de la interceptación del correo electrónico en España: La tecnología proporciona al ser humano un instrumento adecuado para obtener una comunicación instantánea y directa, pero a su vez, al tratarse de un mundo demasiado reciente para el mundo del derecho, algunas personas ven en ello una forma de cometer actos ilícitos y salir impunes, lo cual provoca episodios de inseguridad jurídica o posible vulnerabilidad de derechos fundamentales de los ciudadanos.

Para solucionar y combatir estas situaciones vemos como solución la interceptación del correo electrónico. En España la intervención de las comunicaciones consiste en la restricción del derecho fundamental al secreto de las comunicaciones contenido en el artículo 18.3 de la Constitución Española, efectuada por una resolución judicial motivada, en cuya virtud se autoriza a la policía judicial a entrar en un procedimiento de comunicación o base de datos personal, con el objeto de conocer y, en su caso, recabar y custodiar, una noticia, pensamiento o imagen penalmente relevante para su reproducción en un juicio oral como prueba.

En la STC 49/1999, del 5 de abril, detallan los requisitos de la siguiente manera: 'La intervención de las comunicaciones telefónicas solo puede considerarse constitucionalmente legítima cuando, además de estar legalmente prevista con suficiente precisión, se autoriza por la autoridad judicial en el curso de un proceso mediante una decisión suficientemente motivada y se ejecuta con observancia del principio de proporcionalidad; es

decir, cuando su autorización se dirige a alcanzar un fin constitucionalmente legítimo, como acontece en los casos en que se adopta para la investigación de la comisión de delitos calificables de graves y es idónea e imprescindible para la determinación de hechos relevantes para la misma'. Por ello, destaca el TC que el órgano judicial habrá realizado de forma correcta la intervención y estará legitimada la medida limitativa del derecho al secreto de las comunicaciones cuando se hagan constar en el auto de intervención: los presupuestos materiales de la intervención (datos de los posibles delitos, la conexión de los dueños del dominio del e-mail con su verdadero autor, la identificación asignada de usuario, número de teléfono, nombre y dirección del usuario o abonado registrado y los datos necesarios para identificar el destino de la comunicación), necesidad, idoneidad y proporcionalidad de la medida; y determinar con precisión características temporales, quién debe llevarla a cabo y los períodos en los que deba darse cuenta al juez de sus resultados a los efectos de que este controle su ejecución.

El polémico sistema de interceptación de e-mails usado en España en el orden penal: SITEL. ¿Qué es y en qué consiste SITEL?

Desde hace un tiempo, un mecanismo de interceptación de comunicaciones copa decenas de debates políticos, los cuales versan acerca de la licitud de la vía empleada, sus posibles ventajas o los posibles defectos y vulneraciones que puede conllevar su uso. Nos estamos refiriendo a SITEL, Sistema Integral de Interceptación de las Comunicaciones Electrónicas, una figura conocida para la sociedad española hace un par de años, pero que se fraguó y se utilizó cuando aún los españoles no teníamos idea alguna de su existencia.

Cuando hablamos del sistema SITEL estamos hablando, ante todo, de un software espía puramente informático utilizado por la Policía Nacional, la Guardia Civil y el Centro Nacional de Inteligencia. Este sistema se sustenta de forma física a través de dos centros de monitorización, diversas salas destinadas a este monitoreo y terminales remotos distribuidos por lo largo y ancho del territorio nacional.

Este sistema informático ofrece un espionaje íntegro de comunicaciones electrónicas, debido a que puede interceptar cualquier actividad que salga de nuestro dispositivo móvil. Actualmente los móviles no solo sirven para hacer llamadas de un terminal a otro, sino que estos dispositivos cuentan con envío de mensajes de texto, mensajes de video o fotografía y, muchos de ellos cuentan también con acceso a Internet, con lo que se producen también envíos de correos electrónicos o actividades propias del comercio electrónico, las cuales todas ellas entran dentro del ojo de SITEL.

De esta forma, este software lo que hace es recopilar y copiar toda esta marabunta de información para enviarla a las salas y centros de

monitorización a través de las distintas terminales remotas, donde se produce el control, investigación y seguimiento de estas comunicaciones para obtener evidencias electrónicas suficientes para imputar determinados hechos delictivos a sus presuntos autores.

La regulación de SITEL. ¿Es legal SITEL?: Según las referencias aportadas acerca de SITEL, queda reflejado que el sistema se aprobó hace diez años, en 2001, y que, dependiendo de las referencias periodísticas, el sistema empezó a funcionar de manera, ya sea puntual o continua sobre los años 2003 o 2004.

A finales de 2002 la Unión Europea aprueba la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

Como cualquier texto comunitario inmediatamente tiene un reflejo en la regulación nacional mediante una transposición, en este caso concretamente en la ley 32/2003, del 3 de noviembre, General de Telecomunicaciones (LGT), con lo que se daba una base a la interceptación de las comunicaciones electrónicas pero que seguía sin ofrecer una regulación concreta a la figura de los sistemas propios de interceptación.

Por último, todo este proyecto, con leves modificaciones técnicas, fue reproducido en el RLGT; dándose definitiva carta de naturaleza al sistema con la elevación de rango normativo a ley ordinaria propiciada por la ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (LCDCE), en concreto mediante la reubicación en el artículo 33, LGT, de la mayor parte de su articulado. De esta forma existe un periodo entre los años 2001 a 2007 en los que a nuestro parecer no existía un mínimo de regulación suficiente para poner en marcha SITEL con un respaldo legal suficiente, por lo que se deberían considerar ilegales las escuchas realizadas en este periodo de tiempo mediante dicho sistema.

Llegados a este punto pensamos que las escuchas a día de hoy realizadas por el Sistema no son ilegales, ya que gozan de una previsión legal y un marco normativo bastante completo, aunque a nuestro parecer insuficiente. ¿Por qué insuficiente? Pues porque lo normal sería que en España una figura como SITEL, que colisiona y menoscaba el derecho fundamental al secreto de las comunicaciones, fuera regulado por una ley orgánica y no por una ordinaria.

Las leyes ordinarias en España son las aprobadas por mayoría simple en el Congreso de los diputados (más votos positivos que negativos), mientras que las leyes orgánicas, aquellas que protegen derechos fundamentales, son aprobadas por más de la mitad de personas que conforman el Congreso (50+1). ¿A qué se debe entonces que un mecanismo como SITEL no esté

regulado por ley orgánica? Pues según nuestra propia opinión, a una cuestión puramente política.

Derecho a la intimidad, Responsabilidad Objetiva y derecho de propiedad. Conceptos generales y Estado de situación en Argentina. Entre los temas a tener en cuenta es necesario realizar ciertas consideraciones: la primera de ellas versa sobre la consistencia del correo electrónico. Así, en el diccionario de la Real Academia Española, encontramos que se lo define como: 'm. Sistema de comunicación personal por ordenador a través de redes informáticas'. Dos cosas son destacables de esta definición, la negativa es lo escaso y posiblemente erróneo de la misma, al referirse a este sistema como de comunicación personal –ya que en principio este tipo de comunicaciones no tienen un carácter necesariamente personal V.G.: el spam-. Pero más interesante aun es la positivamente relevante desde lo jurídico, el hecho de que la misma definición habla de comunicación, lo que implica una amplia gama de aristas y de contenido, pero específicamente que requiere de un feedback (retroalimentación) entre sus interlocutores o específicamente entre remitente y destinatario para que exista un correo electrónico.

El segundo aspecto que requiere una consideración previa es el de la propiedad de la casilla de correo electrónico. Una casilla de correo electrónico es susceptible de apropiación, ya sea de modo gratuito, como de modo oneroso. Lo que no significa que el titular de la casilla se apropie del lugar donde se almacena. Es decir, si se envía un sobre al correo, a una casilla postal, el receptor o en su defecto quien envía el sobre, serán titulares del sobre y de su contenido, pero no del continente del sobre, o sea que no podría ir al correo y reclamar la propiedad de las maderas de las que está hecha la respectiva casilla postal. De esta manera, quien contrata con un servidor, obtiene justamente el 'servicio' de utilización y almacenamiento de una o varias casillas de correo electrónico, pudiendo elegir el nombre e incluso brindarlas a sus dependientes para su utilización empresarial, sin que esto implique la transferencia de la titularidad, ya que quien contrata con el servidor es la empresa y cuando el empleado se desvincule deberá reintegrar el uso de la casilla que le fuera cedido por el principal.

El empleador da al trabajador una herramienta, cuya titularidad continúa siendo de la empresa, es decir que el empleado podrá utilizar esa casilla de correo bajo la regulación que reglamente esa utilización y en el espacio temporal comprendido desde que el empleador se la otorga, hasta que se la retire o se desvinculen de la relación que los uniera. De manera que la utiliza no en carácter de titular, sino como usuario de una herramienta de trabajo perteneciente a la empresa. VG.: en el ejemplo anterior, el empleador le da al empleado el sobre, el papel (que además van con el membrete de la empresa –

en este caso @empresa–), el instrumento de escritura, la tinta y además le paga por el tiempo que pasa escribiendo y recibiendo esta 'correspondencia' y le paga también por lo que produce intelectual y comercialmente mediante esas herramientas. De esta manera, la hipótesis de que el empleador no tenga legitimidad para revisar la casilla que utiliza el empleado ya no parece tener tanto sustento.

Conflicto de valores: Adentrándonos en el objeto que nos ocupa, pareciera ser clara la disyuntiva de los valores que se enfrentan en este paradigma, por un lado el valor intimidad, amparado claramente en el derecho a la privacidad, un derecho de raigambre constitucional (Art. 19, CN: 'Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están solo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe'), indiscutido e irrenunciable, un derecho inherente al ser humano, intransferible y personalísimo para el derecho argentino. Ampliamente reconocido por todos los estados de derecho en mayor o menor medida; por el otro lado, el conflicto que esto representa frente a los derechos de propiedad (Art. 14, CN: 'Todos los habitantes de la Nación gozan de los siguientes derechos conforme a las leyes que reglamenten su ejercicio; a saber: de trabajar y ejercer toda industria lícita; de navegar y comerciar; de peticionar a las autoridades; de entrar, permanecer, transitar y salir del territorio argentino; de publicar sus ideas por la prensa sin censura previa; de usar y disponer de su propiedad; de asociarse con fines útiles; de profesar libremente su culto; de enseñar y aprender'. Y Art. 17: 'La propiedad es inviolable, y ningún habitante de la Nación puede ser privado de ella, sino en virtud de sentencia fundada en ley. La expropiación por causa de utilidad pública, debe ser calificada por ley y previamente indemnizada. Solo el Congreso impone las contribuciones que se expresan en el artículo 4º. Ningún servicio personal es exigible, sino en virtud de ley o de sentencia fundada en ley. Todo autor o inventor es propietario exclusivo de su obra, invento o descubrimiento, por el término que le acuerde la ley. La confiscación de bienes queda borrada para siempre del Código Penal Argentino. Ningún cuerpo armado puede hacer requisiciones, ni exigir auxilios de ninguna especie') –que tiene la empresa sobre la casilla que otorga al empleado como herramienta de trabajo– y los derechos de control laboral que asisten al empleador respecto de sus operarios, lo cual funda el principio de responsabilidad sobre los actos de sus dependientes establecida por el artículo 1113, CCN (La obligación del que ha causado un daño se extiende a los daños que causaren los que están bajo su dependencia, o por las cosas de que se sirve, o que tiene a su cuidado [Párrafo agregado por ley 17.711]. En los supuestos de daños causados con las cosas, el

dueño o guardián, para eximirse de responsabilidad, deberá demostrar que de su parte no hubo culpa; pero si el daño hubiere sido causado por el riesgo o vicio de la cosa, solo se eximirá total o parcialmente de responsabilidad acreditando la culpa de la víctima o de un tercero por quien no debe responder. Si la cosa hubiese sido usada contra la voluntad expresa o presunta del dueño o guardián, no será responsable). Conclusiones: De lo propuesto, la principal conclusión que se pretende es evidenciar la clara falta de hermenéutica y consistencia lógica que ofrece el actual criterio jurisprudencial y doctrinario en algunos casos. Como propuesta, en primer lugar recurrimos a la lógica y a la coherencia que son grandes fuentes del derecho a pesar de su escaso reconocimiento. Desde ahí partiremos hacia la idea de que podemos estar de acuerdo con la responsabilidad objetiva o no, pero en lo que no podemos detenernos a discutir es en el hecho de que si hacemos responsable a alguien objetivamente, debemos necesariamente brindarle la garantía del control del objeto que lo hace responsable. Nunca podemos atribuir una carga tan grande como la del artículo 1113 CCN, sin dar al eventual victimario la posibilidad mínima de controlar y prevenir un posible daño.

Por otro lado, y si fuéramos ciegos como la justicia, pero no para ser imparciales, sino que realmente no viéramos la gravísima falta de criterio descripta en el párrafo anterior, y además pretendiéramos definir el contenido de una casilla de correo electrónico laboral como perteneciente a la intimidad de un trabajador, estaríamos nuevamente en un claro error conceptual. Como dijéramos anteriormente respecto de la definición de intimidad –zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia–, o de privacidad –ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión–, está claro que no es el tipo de información que un empleado debería verter en este tipo de herramientas, por el contrario, lejos de violarse un derecho a la intimidad por parte del empleador, hay una grave injuria del trabajador para con su principal por utilizar recursos de la empresa y su tiempo de trabajo en cuestiones de índole privada o íntima. Según la tendencia actual, pareciera que el empleado tiene derecho a realizar un uso abusivo e indiscriminado del material de trabajo, mientras que el empleador no solo que no puede realizar un control de dicho material (del cual es titular y le pertenece) sino que además tiene que responder por esa gran incógnita que representa el contenido de una casilla de correo electrónico de la empresa. Finalmente, y por si no fuese claro el criterio, los correos electrónicos empresariales no deben contener información privada o íntima de los usuarios, de esta manera, el control de contenido es completamente legítimo y legal ya que los correos en definitiva pertenecen a la empresa y no están sujetos a las protecciones del derecho a la privacidad o intimidad. Consecuencia de esto, podemos estar en contra o de acuerdo y en

mayor o menor medida con la responsabilidad objetiva (en mi caso parcialmente de acuerdo) pero ahora sí tendríamos al menos la fundamentación básica que requiere dicha responsabilidad que es precisamente el derecho/obligación de control sobre el accionar de los dependientes".

CAPÍTULO 5
LA CADENA DE CUSTODIA INFORMÁTICO FORENSE

La preservación de la cadena de custodia sobre la prueba indiciaria criminalística es un objetivo que afecta a la totalidad de los miembros del Poder Judicial, los operadores del Derecho y sus auxiliares directos.

Entre estos últimos debemos incluir al personal de las fuerzas de seguridad, a las policías judiciales y al conjunto de peritos oficiales, de oficio y consultores técnicos o peritos de parte.

Por esta razón, el establecer mecanismos efectivos, eficientes y eficaces que permitan cumplir con dicha tarea a partir de métodos y procedimientos que aseguren la confiabilidad de la información recolectada, único elemento integrador a proteger en los activos informáticos cuestionados, ya que incluye la trazabilidad[29], la confidencialidad, la autenticidad, la integridad y el no repudio de estos, es una necesidad imperiosa para asegurar el debido proceso en cualquiera de los fueros judiciales vigentes.

En términos sencillos, implica establecer un mecanismo que asegure a quien debe juzgar que los elementos probatorios ofrecidos como prueba documental informática son confiables. Es decir, que no han sufrido alteración o adulteración alguna desde su recolección, hecho que implica su uso pertinente como indicios probatorios, en sustento de una determinada argumentación orientada a una pretensión fundada en derecho.

El juez debe poder confiar en dichos elementos digitales por considerarlos auténticos “testigos mudos”, desde el punto de vista criminalístico clásico, y evaluarlos en tal sentido desde la sana crítica, la prueba tasada o las libres convicciones según sea el caso y la estructura judicial en que se desarrolle el proceso.

Consideramos a la cadena de custodia como un procedimiento controlado que se aplica a los indicios materiales (prueba indiciaria) relacionados con un hecho delictivo o no, desde su localización hasta su valoración por los encargados de administrar justicia, y que tiene como fin asegurar la inocuidad y esterilidad técnica en el manejo de dichos indicios, evitando alteraciones, sustituciones, contaminaciones o destrucciones, hasta su disposición definitiva por orden judicial.

Para asegurar estas acciones es necesario establecer un riguroso y detallado registro, que identifique la evidencia y su posesión, con una razón que indique lugar, hora, fecha, nombre y dependencia involucrada, en el secuestro, la

interacción posterior y su depósito en la sede que corresponda (judicial o no).

Desde la detección, identificación, fijación, recolección, protección, resguardo, empaque y traslado de la evidencia en el lugar del hecho real o virtual, hasta la presentación como elemento probatorio, la cadena de custodia debe garantizar que el procedimiento empleado ha sido exitoso, y que la evidencia que se recolectó en la escena es la misma que se está presentando ante el evaluador y/o decisor.

Para quienes deseen ampliar el tema referido a cadena de custodia en general, existen muchas analogías con la cadena de custodia utilizada en la preservación de muestras biológicas (para realizar estudios comparativos de ADN, entre otras posibilidades)[30].

Subsidiariamente, pero a idéntico tenor, es importante considerar el significado implícito en los indicios recolectados, el valor que van a tener en el proceso de investigación, análisis y argumentación del cual dependen. En dicho marco de referencia, adquirirán su relevancia y pertinencia, de ahí la necesidad de evitar en lo posible la impugnación de ellos en razón de errores metodológicos propios de cada disciplina en particular (no son idénticas las cadenas de custodia de muestras biológicas y las de armas o documentos impresos o virtuales). Es por esta razón que existen componentes genéricos y componentes particulares en toda cadena de custodia. Por ejemplo, el realizar un acta de secuestro es un elemento genérico, pero el asegurar la integridad de la prueba mediante un digesto (hash) sobre el archivo secuestrado es un elemento propio de la cadena de custodia informático forense.

Suele asociarse a la cadena de custodia con el proceso judicial orientado a dilucidar acciones delictivas, sin embargo esta no se agota en el orden penal. En particular, la cadena de custodia informático forense debe preservarse en todas las transacciones virtuales susceptibles de ser valoradas económicamente. Cuando un banco realiza una transferencia de fondos o un consumidor adquiere un producto por medios virtuales (Internet, entre otros) requiere de esa operación la misma confiabilidad que puede aportarle la cadena de custodia informático forense, es decir, afecta en todo momento a la comunidad virtual y a sus actores involucrados.

Al recolectar las pruebas, lo importante es el significado, el valor que van a tener en el proceso de investigación, y por medio de la cadena de custodia, este valor va a ser relevante, debido a que no se va a poder impugnar al haberse acatado el procedimiento.

Para que la prueba documental informática sea tenida por válida y adquiera fuerza probatoria ante el encargado de decidir a partir de ella, es necesario que sea garantizada respecto de su confiabilidad, evitando suplantaciones, modificaciones, alteraciones, adulteraciones o simplemente su destrucción

(algo muy común en la evidencia digital, ya sea mediante borrado o denegación de servicio). Desde su recolección hasta su disposición final, debe implementarse un procedimiento con soporte teórico, científico, metodológico criminalístico, estrictamente técnico y procesalmente adecuado. Si carece de alguno de estos componentes, la prueba documental informática recolectada no habrá alcanzado el valor probatorio pretendido. Este procedimiento se caracteriza por involucrar múltiples actores, los que deben estar profundamente consustanciados de su rol a cumplir dentro de este, sus actividades a desarrollar durante la manipulación de la prueba y sus responsabilidades derivadas.

Definición: Podemos definir a la cadena de custodia informático forense como un procedimiento controlado y supervisable, que se aplica a los indicios materiales o virtuales relacionados con un hecho delictivo o no, desde su localización hasta su valoración por los encargados de administrar justicia, y que tiene como fin asegurar la confiabilidad de la prueba documental informática recolectada en un determinado lugar del hecho real o virtual desde su identificación hasta su disposición definitiva por orden judicial.

Sin embargo, esta definición es abarcativa, pero genérica; la prueba documental informática tiene componentes particulares diferenciativos que la tornan sumamente diversa a la hora de recolectarla, preservarla y trasladarla.

La prueba documental informática consiste en indicios digitalizados, codificados y resguardados en un contenedor digital específico. Es decir, toda información es información almacenada (aun durante su desplazamiento por una red, está almacenada en una onda electromagnética). Es necesario diferenciar entre el objeto que contiene a la información (discos magnéticos, ópticos, cuánticos, ADN, proteínas, etc.) de su contenido, información almacenada, y sobre todo de su significado.

Para este caso consideramos:

1. Información: Todo conocimiento referido a un objeto o hecho, susceptible de codificación y almacenamiento.
2. Objeto: Conjunto físicamente determinable o lógicamente definible.

La información puede estar en uno de los siguientes estados:

1. Almacenada: Se encuentra en un reservorio a la espera de ser accedida (almacenamiento primario, secundario o terciario), es un estado estático y conforma la mayoría de las recolecciones posibles; sin embargo, difiere de la mayoría de los indicios recolectables en que puede ser accedida por medios locales y/o remotos.
2. En desplazamiento: Es decir, viajando en un elemento físico determinado (cable, microonda, láser, etc.), es susceptible de recolección mediante

intercepción de dicho elemento y está condicionada por las mismas cuestiones legales que la escucha telefónica o la violación de correspondencia.

3. En procesamiento: Es el caso más complicado y constituye la primera decisión a tomar por el recolector. Ante un equipo en funcionamiento, donde la información está siendo procesada, es decir modificada, actualizada y nuevamente resguardada, debe decidir si apaga o no el equipo. Esta decisión es crítica y puede implicar la pérdida de información y la destrucción de la prueba documental informática pretendida[31]. La solución por medio del acceso remoto, indetectable por el accedido, es un tema que aún no se encuentra en discusión en nuestro país[32].

En cuanto a su significancia probatoria, tendrá la validez que le asigne su inserción como elemento pertinente y conducente a la argumentación presentada como sustento de la pretensión jurídica manifestada. Es decir, no deja de ser un documento más, que difiere de la prueba documental clásica (bibliográfica, foliográfica y pictográfica) únicamente en el soporte (digital vs. papel).

Sin embargo, es necesario tener en cuenta que un bit no es similar sino idéntico a otro bit. De ahí que una copia bit a bit de un archivo digital es indiferenciable de su original, esto significa que no puede establecerse cuál es el original y cuál su copia, salvo que hayamos presenciado el proceso de copiado y tengamos conocimiento sobre cuál era el contenedor del original y cuál el de la copia (método indirecto e independiente de los archivos considerados). Esto no resulta en un inconveniente sino en una ventaja, desde el punto de vista de la cadena de custodia, ya que permite preservar las copias, manteniendo el valor probatorio del original y evitando riesgos para este. Se puede entregar al perito una copia de los archivos dubitados y preservarlos en su reservorio original en el local del tribunal y con las seguridades que este puede ofrecerle (entre otros, caja fuerte)[33].

Mientras que en la recolección física de prueba indiciaria tradicional se secuestra el indicio y se lo traslada, en la recolección de documental informática esta acción puede realizarse o no, ya que es suficiente con copiar bit a bit la prueba y luego trasladar dicha copia. Es una extensión del caso anterior, donde no es necesario entregar el original al perito, sino que alcanza con su copia. La recolección de prueba, mediante copia debidamente certificada, puede sustituir perfectamente al original, es aplicable a los casos en que la información esté almacenada en reservorios vitales para la operación de una determinada entidad u organización estatal o privada. Supongamos la necesidad de secuestrar información almacenada en uno de los servidores operativos del Banco Central. Es evidente que el secuestro de dicho servidor podría sacar de operación a la entidad con las consecuencias que dicho hecho

implicaría, mientras que su copia, certificación mediante hash y ante la autoridad judicial, administrativa o notarial correspondiente, en nada afectaría a la continuidad del servicio y serviría perfectamente como elemento probatorio.

Los mecanismos de certificación digital (hash, firma electrónica, firma digital) son mucho más confiables y difíciles de falsificar que los mismos elementos referidos a la firma y certificación ológrafas. Sin embargo, la susceptibilidad de los operadores del Derecho ante el nuevo mundo virtual hace que tengan sensaciones de inseguridad que no tienen sustento alguno en la realidad matemática que brinda soporte a los mecanismos referidos. Se adopta una actitud sumamente crítica y negativa frente a la seguridad que estos brindan, en parte como consecuencia de la necesidad implícita de confiar en algoritmos que no se conocen. Entender, comprender y analizar un algoritmo de cifrado por clave pública es una tarea de expertos y que no está al alcance de una formación matemática básica como la que posee la mayoría de los operadores del Derecho. Por otra parte, el individuo inserto en la sociedad tiende más a confiar en la medicina (por eso no cuestiona los métodos del médico legista o del psiquiatra forense) que en la matemática, con la que se relaciona mucho menos[34]. Es un proceso lento de aceptación, que como todo en Derecho seguramente llegará a posteriori del desarrollo social y tecnológico que nos rodea e impulsa hacia el futuro.

La cadena de custodia informático forense tiene por objeto asegurar que la prueba ofrecida cumple con los requisitos exigibles procesalmente, lo que implica que debe asegurar:

1. Trazabilidad:
   a. Humana (determinación de responsabilidades en la manipulación de la prueba, desde su detección y recolección hasta su disposición final).
   b. Física (incluyendo la totalidad de los equipos locales o remotos involucrados en la tarea, sean estos de almacenamiento, procesamiento o comunicaciones).
   c. Lógica (descripción y modelización de las estructuras de distribución de la información accedida y resguardada).
2. Confiabilidad (integridad, autenticidad, confidencialidad, no repudio).

Cadena de custodia vs. privacidad

La cadena de custodia se constituye de hecho en un elemento que permite asegurar la confiabilidad de la información recolectada, implica su trazabilidad estricta, pero no protege por sí sola el derecho a la privacidad. Es un componente que asegura que la prueba recolectada se puede seguir metodológica y procesalmente, desde su origen hasta su disposición final, pero

nada dice respecto de su legalidad, ni de la legitimidad del proceso de recolección autorizado.

En efecto, la protección de la privacidad de la información no se conforma de manera exclusiva con la cadena de custodia. La privacidad requiere por supuesto confiabilidad, pero también respeto estricto de las normas procesales que resguardan el legítimo proceso asegurado constitucionalmente. Podríamos estar en presencia de una cadena de custodia bien realizada, con una trazabilidad adecuada, con preservación estricta criminalística, informática y procesal, pero que se haya realizado a partir de una acción ilegal o ilegítima. Ilegal, por ejemplo, por falta de orden de allanamiento y secuestro previa a la recolección de prueba documental informática en una causa penal, e ilegítima en el caso de una recolección de información privada, no determinada específicamente y que al ser practicada excede los límites de lo necesario (elementos conducentes y pertinentes), a efectos de justificar la pretensión litigada, resguardando otros elementos que nada tienen que ver con dicha cadena argumental-causal.

La cadena de custodia en la práctica informático forense

En el momento de revisar la integridad material y formal de la cadena de custodia, en el caso particular analizado, el profesional deberá considerarla desde tres puntos de vista complementarios:

1. Validez técnica informática: Implica el control, revisión y auditoría de todas las operaciones técnicas informáticas, realizadas desde el momento de la identificación de la prueba documental informática recolectada hasta el presente, de análisis considerado (el momento en que se realiza dicha evaluación técnica). En este sentido, deben tenerse en cuenta los recursos involucrados e integrados en dicha tarea (edilicios, instrumentales, lógicos y humanos). Este análisis debe efectuarse de manera holística, es decir, teniendo en cuenta los resultados técnicos alcanzados a partir de las operaciones efectuadas sobre la totalidad de los recursos considerados y su consecuencia inmediata (validación informática de la cadena de custodia implementada o su desacreditación como prueba documental informática válida).

2. Validación técnica criminalística: Se trata en este caso del control, revisión y auditoría de todas las operaciones técnicas criminalísticas, realizadas desde el momento de la toma de contacto, de los actores participantes en la tarea analizada, es decir desde que se involucran con la problemática pericial propuesta. Se extiende espacio temporalmente más allá de la revisión especificada en el apartado anterior, ya que implica la interacción multi y

transdisciplinaria de todos los participantes (peritos, expertos o no) en la preservación de la prueba[35]. Al igual que en la validación anterior, la revisión debe ser transdisciplinaria, ya que de esta confirmación criminalística devendrá su aceptación como prueba indiciaria en general y como prueba indiciaria informático forense en particular. Comprobados los procedimientos criminalísticos utilizados mediante metodología criminalística y convalidados estos, la prueba indiciaria informática recolectada será garantizada como prueba indiciaria válida para su empleo pericial, en caso contrario, deberá ser descartada a tales efectos.

3. Validación técnica legal: Esta validación es la resultante del análisis en subsidio, a partir de las dos validaciones anteriores. Si bien dichas validaciones pueden ser efectuadas por separado y en distinto orden, esta (a la que nos estamos refiriendo) solo se efectuará cuando las dos anteriores hayan arrojado resultados positivos. Consiste en el análisis integrador de la prueba indiciaria informática recolectada y disponible, a efectos de determinar su confiabilidad probatoria legal. En efecto, el objetivo principal de las tareas efectuadas reside en constituirse en un elemento más de apoyo a la decisión judicial (sentencia) en el momento oportuno. La confiabilidad que a esta altura ha sido comprobada técnicamente, desde los puntos de vista informático y criminalístico, se constituye en un pilar que brindará soporte pertinente al decisor, que previamente determinará la pertinencia y conducencia de este como elemento probatorio. Implica el control, revisión y cotejo de los mecanismos utilizados desde el punto de vista legal, considerando que acorde con la normativa, doctrina y jurisprudencia vigentes, el objeto jurídico principal a preservar durante la intervención judicial es el debido proceso (lo que implica la preservación a ultranza de las garantías constitucionales vigentes). Este hecho no invalida la búsqueda de la verdad material de los hechos acaecidos, pero lo supedita y subordina al cumplimiento estricto de las normas procesales. Su violación trae como consecuencia inmediata la nulidad de la prueba recolectada.

Nota: Es importante destacar que excepcionalmente y en muy raras ocasiones (acorde a la experiencia de los autores) es posible subsanar los resultados negativos de fallas en la validación técnica informática y/o criminalística. Esto dependerá del carácter reversible o irreversible de los errores cometidos.

Por el contrario, las fallas en la validación técnica legal no son subsanables, ya que en general afectan derechos constitucionalmente protegidos (legítima defensa, intimidad, protección de datos personales) y, por ende, al aseguramiento judicial del debido proceso (en especial, en Derecho penal por aplicación complementaria de la doctrina del árbol venenoso).

[29] *Se trata de establecer un mecanismo que permita realizar un seguimiento estricto de los elementos probatorios, desde su detección hasta el momento de su disposición definitiva.*

[30] *SOCIEDAD LATINOAMERICANA DE GENÉTICA FORENSE: Precauciones durante la recolección y envío de muestras.*

Recomendaciones de la sociedad latinoamericana de genética forense basadas en la International Society for Forensic Genetics –ISFG– y en el GEP-ISFG:

1. Protección del personal:
   a. Las muestras biológicas potencialmente pueden contener agentes patógenos (VIH, hepatitis, meningitis…).
   b. Evitar contacto con la muestra mediante uso de guantes, mascarilla y bata.
   c. Si es posible emplear material desechable.
   d. Prohibir comer, beber o fumar durante el proceso de recolección.
   e. Recomendar la vacunación al personal que trabaje con este tipo de muestras.
2. Protección de la muestra:
   a. Contaminación por material biológico humano: Se debe a la aparición en el propio indicio biológico de un aporte de material biológico humano ajeno al propio indicio. Produce como resultado la mezcla de perfiles genéticos.
   b. Contaminación anterior o previa: Se debe a la aparición de material biológico en el lugar donde luego aparecerán los indicios. Es inevitable y generalmente dificulta la valoración de la prueba.
   c. Contaminación coetánea o paralela: El material genético de un indicio se mezcla con ADN de otro origen en el momento de los hechos. Es inevitable y favorece la valoración.
   d. Contaminación posterior: Debido al depósito de material genético de diversos orígenes en el indicio con posterioridad al momento de los hechos. Es evitable mediante estrictos protocolos de recolección, embalaje y envío de las muestras, que se detallan en el presente documento.
   e. Transferencia de indicios biológicos: Traslado accidental de los indicios de un lugar a otro, ocasionando contaminación o pérdida de la muestra (por ej. pelos).
   f. Contaminación biológica no humana: Producida por microorganismos que acaban degradando el ADN por acción, fundamentalmente de exonucleasas (humedad y altas temperaturas).
      i. Puede ocurrir “a priori” a la recolección de indicios (muestras expuestas a condiciones que favorecen la proliferación bacteriana).
      ii. Tras la recolección del indicio si el empaquetado y conservación no es el adecuado.

iii. Produce la degradación del ADN y ausencia de resultados, pero nunca la alteración de los patrones genéticos.

g. Contaminación química: Producida cuando las muestras se preservan (formol) o se tratan con determinados productos químicos. Por ejemplo, es nocivo cuando para el estudio de huellas dactilares se utilizan líquidos reactivos; los polvos minerales –carbón, talco, etc.– no producen alteración alguna. Afecta principalmente a las fases de extracción y amplificación del ADN, ya que modifican la estructura química del mismo, lo cual se manifiesta como ausencia de resultados evaluables, pero nunca como modificación del patrón genético.

¿Qué precauciones adoptar?

- Aislar y proteger, lo más rápidamente posible, la escena del delito.
- Recoger, si es posible, en primer lugar los indicios biológicos.
- Usar guantes limpios que deben cambiarse con frecuencia.
- Evitar hablar o estornudar sobre las muestras. Usar mascarilla.
- Usar bata u otro tipo de ropa protectora.
- Utilizar material desechable, siempre que sea posible.
- No añadir conservantes a las muestras.
- Dejar secar a temperatura ambiente previamente a ser empaquetadas.
- Empaquetar por separado las muestras.
- Empaquetar en bolsas de papel o cartón, evitar las bolsas de plástico, que condensan la humedad y favorecen la proliferación de bacterias que degradan el ADN.
- Eliminar todo el material desechable empleado en la recogida de muestras.

Toma de muestras de referencia

Personas vivas:

1. Siempre con consentimiento informado.

2. Debe existir un documento firmado con la autorización expresa para realizar el análisis. Muestra sanguínea:

- Existe la creencia popular de que en personas transfundidas se cambia el patrón genético. Esto es así solo en teoría, ya que en la práctica la persona debería transfundirse un gran volumen de sangre (casi toda) y concurrir inmediatamente a la toma de muestra para ADN, lo cual le produciría una debilidad y características físicas fácilmente detectables por el personal que realiza la toma. Un par de horas después, ya aparece en la sangre el patrón genético real del individuo, al principio mezclado con el donante de la sangre. De todos modos, en caso de duda pueden tomarse hisopados

bucales.

- Se sugiere realizar punción dactilar, depositar una gota –de aproximadamente 1 cm de diámetro– en cualquier tipo de papel de filtro y dejar secar a temperatura ambiente. Embalar en sobres de papel común. En estas condiciones, la muestra dura más de 10 años.
- No tomar sangre líquida ya que debe conservarse en freezer o se deteriora rápidamente. Hisopados bucales:
- No se trata de "saliva" sino de células epiteliales retiradas de la mucosa bucal.
- Hisopos de ambos carrillos, que se colocan en sobres de papel –nunca de polietileno– para evitar la proliferación bacteriana. Los envoltorios de polietileno o celofán condensan la humedad y favorecen la degradación.

Pelos con bulbo:

- No se recomiendan como muestras de referencia, deben preferirse hisopados bucales o muestras sanguíneas.
- De ser necesario, un solo pelo con bulbo es suficiente, pero se recomienda recolectar no menos de tres mediante arrancado, y fijarlos mediante una cinta adhesiva a una placa de cartulina o plástico. Se sugiere no usar portaobjetos de vidrio, ya que pueden romperse durante el traslado.

Cadáveres:

En buen estado de conservación:

- Sangre postmortem: 200 microlitros (anticoagulante tipo EDTA), colocar sobre papel de filtro.
- Músculo esquelético: Aproximadamente 1 gr. Se almacena en un recipiente de plástico y tapón de rosca. Conservar en fre in the middle with you ezer.
- Piezas dentales: 2 (molares). Dejar en reserva a temperatura ambiente, con el fin de evitar la exhumación si se requieren estudios de ADN meses o años después.

En avanzado estado de putrefacción o esqueletizados:

- Hueso largo: Fémur, húmero.
- Piezas dentales: 2 (molares). No dañados externamente ni sometidos a endodoncias. Quemados o parcialmente carbonizados:
- Cuando la carbonización no es total, es posible analizar músculo esquelético de zonas profundas.
- Cuando la carbonización es total, es recomendable recolectar huesos o dientes, seleccionando aquellos que a simple vista se encuentren en mejor estado. De existir dudas, contactar con el laboratorio.

Otras muestras de referencia de individuos fallecidos

- En hospitales (muestras de sangre, biopsias en parafina, o preparaciones histológicas). No utilizar tejidos fijados en formol.
- Ámbito familiar (peines, maquinillas de afeitar, saliva en sellos o sobres…). Toma de indicios biológicos en el lugar de los hechos
- Manchas secas:

✓ En soportes pequeños y de fácil transporte: Colillas, armas blancas, monedas, llaves, piedras, ramas, papeles. Recoger por separado e introducirlas en bolsas de papel o cajas.

✓ En soportes grandes no transportables:

■ Soporte no absorbente (cristal, metal…): Recoger con un hisopo mojado en agua destilada

(dejar secar antes de guardar) o raspar con bisturí y guardar en bolsa de papel.

■ Soporte absorbente (telas, tapicerías…): Recortar la mancha y guardar en bolsa de papel.

- Indicios húmedos, ropas, tapicerías, toallas:

✓ Introducir por separado en bolsas de papel madera.

✓ Trasladar rápidamente a instalaciones adecuadas.

✓ Dejar secar en lugar protegido y sobre una superficie limpia y envolver en papel (por separado).

✓ Guardar en bolsas de papel.

- Indicios líquidos (guardar siempre en freezer):

✓ Sangre:

■ En gran cantidad: recoger con pipeta de plástico y depositarla en un tubo con EDTA.

■ En pequeña cantidad: recoger con hisopo y dejar secar.

■ Coagulada: recoger con una cucharita e introducir en tubo o frasco de plástico.

✓ Semen:

■ Preservativos con semen líquido: atar e introducir en un frasco de plástico.

■ En escasa cantidad: recoger con hisopo y dejar secar.

✓ Líquido amniótico: 10 ml, que se introducen en un tubo.

✓ Orina: Recoger con pipeta de plástico desechable y depositarla en un tubo o frasco.

- Pelos: Recolectar cada pelo con pinzas (desechables o bien limpias) y guardarlo en una bolsa de papel.

- Restos cadavéricos:

✓ Buen estado de conservación: Tejido muscular sin líquido fijador en frasco de boca ancha y tapón de rosca.

✓ Carbonizados: Músculo esquelético de zonas menos afectadas sin líquido fijador y en frasco de boca ancha y tapón de rosca.

✓ Avanzado estado de putrefacción o esqueletizados: Hueso largo (limpio sin putrílago) y dientes (2 molares).

Toma de indicios biológicos en el cuerpo de la víctima

- Manchas de sangre, semen u otros fluidos biológicos: Recoger con un hisopo húmedo (agua destilada) la mancha en cuestión, dejar secar a TA y enfundar el hisopo.
- Saliva en marcas de mordedura: Recoger con un hisopo húmedo (agua destilada) la mancha en cuestión, dejar secar a TA y enfundar el hisopo.
- Uñas: Recoger con una pinza posibles pelos o fibras. Posteriormente, cortar el borde superior de las uñas para búsqueda de sangre o piel. Recoger en bolsas de papel por separado.
- Pelos dubitados: Recoger cada pelo con unas pinzas y colocar en un papel que será doblado e introducido en una bolsa de papel.

Toma de indicios biológicos en casos de agresión sexual:

- Dos tomas bucales mediante hisopos, pasando por debajo de la lengua, encías y dientes.
- Búsqueda de manchas de semen, saliva o mordeduras: según se indicó anteriormente.
- Dos tomas cervicales, dos tomas vaginales y una de genitales externos, con hisopos estériles limpiando cuello uterino, cavidad vaginal y la región vulvar.
- Lavado vaginal, empleando 10 ml de suero fisiológico que se recogerá en un frasco o tubo de plástico.
- Dos tomas anales, con hisopos estériles limpiando el conducto ano-rectal y el margen anal.
- Ropas que portaba la víctima: Guardar en bolsas de papel por separado. Toma de indicios biológicos en casos de investigación biológica de la paternidad:
- Si presunto padre, madre e hijo están vivos: descripto anteriormente.
- Si el presunto padre está fallecido:

✓ Restos óseos o piezas dentales procedentes de la exhumación del cadáver.

✓ Análisis de muestras biológicas del fallecido existentes en hospitales o en el ámbito familiar.

✓ Análisis de muestras biológicas procedentes de familiares del fallecido.

- A partir de restos fetales: Recogerlos con unas pinzas en un frasco de boca ancha y con tapón de rosca (sin formol ni otros líquidos fijadores).

Sistemas de empaquetamiento y preservación de muestras

Importante: mantener y enviar refrigeradas y por un medio de transporte rápido cuando se trata de: indicios líquidos, tejidos blandos y órganos, y otras muestras húmedas (que no puedan secarse).

Enviar toda muestra seca sin refrigeración. Identificación de la muestra:

- Tipo de muestra.
- Pertenencia y/o procedencia.
- Nº de referencia de la muestra.

Custodia de la muestra:

- Identificación y firma de la persona que recoge la muestra.
- Fecha y hora de recolección. Empaquetado:
- Evitar el uso de bolsas de plástico.
- Evitar emplear frascos de cristal.
- Emplear cajas de cartón o sobres de papel.
- Cada muestra en un recipiente precintado o cerrado herméticamente.

Recepción de muestras en el laboratorio:

1º Rellenar la hoja de custodia.

- Nombre de la persona que entrega las muestras.
- Fecha y hora de entrega.
- Nombre de la persona que recibe las muestras.
- Empresa que realiza el transporte.

2º Chequear número de referencia de cada muestra y contrastar con el formulario enviado.

3º Comprobar la integridad de los precintos.

4º Al abrir los recipientes comprobar que identificación y descripción son correctas

5º Si fuera posible, fotografiar las muestras.

Anotar discrepancias si las hubiera y establecer acciones correctoras.

Fuente: http://www.slagf.org/toma.html.

31 Es una decisión en evidentes condiciones de incertidumbre. Si decide mantener el equipo encendido, corre el riesgo de haber sido detectado durante su aproximación al equipo y que en realidad la actividad del mismo esté consistiendo en borrar de manera segura (técnicas específicas de eliminación de la información que la hacen irrecuperable a los métodos informático forenses, es decir borra sin dejar trazas), con lo que cuanto más tiempo permanezca el equipo funcionando mayor será el daño producido. Si por el contrario decide apagar el equipo, es posible que este tenga un mecanismo de seguridad ante estos eventos que dispare las mismas acciones de borrado

detalladas, sobre los equipos remotos, eliminando enlaces y reservorios dentro de la misma red o en redes externas (es muy común que con fines delictivos o no, la información sea almacenada en un reservorio remoto, lo que aumenta su seguridad y confiabilidad, ya que está exenta de los riesgos edilicios, físicos y lógicos, del local donde se utiliza).

La mejor manera de solucionar este problema es la labor de inteligencia previa judicialmente avalada y ordenada (ataques pasivos, consistentes en interceptación, escucha o análisis de tráfico, por medios remotos). Esta tarea resuelve el problema, pero requiere disponer de recursos técnicos y sobre todo humanos sumamente escasos; por otra parte, debe ser autorizada judicialmente y la práctica nos indica que la mayoría de los Juzgados, por muy diversas causas, son sumamente reacios a la hora de autorizar estas intervenciones (lo mismo ocurre con las clásicas y siempre restringidas medidas previas o preliminares, aunque constituyan prueba anticipada y reúnan las condiciones requeridas para esta: periculum in mora, fumus bonis iuris y servare secreto private).

32 Con los medios adecuados es perfectamente posible acceder a un equipo remoto y recolectar la información pretendida, preservando las condiciones legalmente establecidas desde la Constitución Nacional y sus normas derivadas. Sin embargo, en un ambiente donde la diferencia entre el delito informático impropio (delitos clásicos cometidos utilizando medios informáticos) tipificado en la ley 26.388 y el delito informático propio (que afecta al bien jurídico protegido, "información", algo que ni siquiera está contemplado en nuestro Código Penal) es un tema propio solo de algunos operadores del Derecho especializados en derecho de alta tecnología, el suponer la comprensión real de las particularidades que identifican al lugar del hecho virtual (propio e impropio) respecto del lugar del hecho real parece ser más una esperanza posible que una realidad jurídica tangible en el mediano plazo.

33 Si un documento en papel es reservado en secretaría, en la caja fuerte, y luego se le debe realizar una pericia caligráfica, debe ser entregado al perito, porque solo puede trabajar sobre originales. Esto implica la salida de la prueba, abandonando la protección del tribunal, hasta que regrese este, si durante ese desplazamiento es destruido en forma dolosa o culposa, la prueba se pierde. En cambio, si la documental informática es resguardada en el tribunal (por ejemplo, en un CD o DVD) y al perito se le entrega una copia, podrá realizar su tarea sin inconveniente y, si su copia es destruida, en nada afecta al original resguardado en el Juzgado.

34 Las posibilidades reales de ser engañados al comprar un libro por Internet son mucho menores que sus similares ante un vendedor ambulante; sin embargo, sentimos cierta aprensión al ingresar el código de seguridad de nuestra tarjeta de crédito para confirmar la compra, algo que ocurre mucho menos con los jóvenes y los adolescentes, es un problema generacional que supongo se superará con el simple paso del tiempo.

35 *Por ejemplo, si como consecuencia del accionar imprudente, en la manipulación de la prueba recolectada, en alguna de las instancias involucradas (sede policial, tribunal, desplazamientos, etc.) se produce una ruptura en la cadena de custodia, que afecta las condiciones de preservación técnicas (no informáticas). Entre ellos, la apertura de un envase contenedor de información resguardada mediante acta, sin respetar los procedimientos criminalísticos de rigor (se abren los sobres que contienen discos con información, de manera anticipada, prematura y/o innecesaria, destruyendo como consecuencia la credibilidad de la información almacenada).*

CAPÍTULO 6
EL CONTRATO ELECTRÓNICO Y LA INFORMÁTICA FORENSE

Como introducción al presente capítulo, haremos una muy breve descripción conceptual a modo de glosario que facilitará al lector la aproximación a la temática principal pretendida: *"El contrato electrónico en el marco regional internacional y su factibilidad de prueba utilizando metodología informático forense"*.

Documento: Es una unidad significativa de información registrada en un soporte que permite almacenarla y luego recuperarla preservándola en el tiempo.

Independencia del soporte: Un documento mantiene su carácter documental independientemente del soporte que lo contenga (papiros, pergaminos, tablillas de arcilla, papel, cartón, muros, placas de bronce, etc.).

Clasificación como prueba documental: Desde la documentología, se la clasifica en:

- bibliográfica = textos
- foliográfica = gráficos
- pictográfica = fotografías
- informática = incluye las tres anteriores, pero en soporte digital

Documento electrónico: Cualquier conjunto de información que conforme una unidad significativa independiente, registrada en un soporte electrónico (magnético, óptico, cuántico, biológico –cadenas de ADN, proteínas–, entre otros).

Documento digital: Está constituido por información codificada en base numérica binaria, como forma de registrar la información[36].

Estos documentos contienen datos. Dichos datos pueden incluir documentos bibliográficos, foliográficos o pictográficos, separados o integrados en un solo cuerpo documental. Están codificados por medio de señales eléctricas que representan los dígitos "0" y "1", luego se almacenan mediante cambio de polaridad magnética (cinta, disquete, disco rígido) o tecnología óptica (CD, DVD). Ocho bits se reúnen en un conjunto denominado un byte, luego cada byte se relaciona con un carácter del teclado, mediante una tabla de traducción de doble entrada llamada "Tabla ASCII"[37].

Como, en definitiva, las señales que codifican los textos, sonidos o imágenes son reducidas a combinaciones de ceros y unos, a combinaciones de dígitos, la

información así registrada se denomina “información digital”. Y los conjuntos independientemente significativos de esta información, “documentos digitales o electrónicos”.

Características del documento digital

Documentos interactivos: El documento en soporte digital escapa a la fijación definitiva sobre un soporte (papel) y permite su modificación durante la lectura, acorde con las necesidades del lector-editor. Además, dispone de mecanismos de búsqueda por palabras o signos de tipografía que facilitan el acceso inmediato a la información buscada (función buscar, reemplazar, etc.) y diversas facilidades propias de la edición de textos.

Documentos multimediales: Como dijimos, en un solo documento digital se pueden integrar documentos de texto, gráficos o fotografías, agregando además la transición automática o comandada por quien ejecuta la acción (presentaciones, música, videos, simulaciones, realidad virtual, etc.).

Estructura de red conceptual: Mientras el libro en soporte papel debe leerse en forma secuencial (comenzando por la página 1 y finalizando por la última), el documento digital permite moverse libremente, recurriendo a marcadores, llamados “hipertexto”, que enlazan distintas partes del documento, incluyendo índices por palabras clave (tablas de contenidos).

El documento contractual: El contrato en su forma canónica más frecuente se presenta en un documento con soporte en papel. Es decir, es un tipo más de documento, reconocible y gestionable por el operador del Derecho, como una prueba documental más.

El contrato a distancia (entre ausentes): En realidad, no estamos hablando de un tipo de documento, sino de una forma particular de conclusión de un contrato (que puede luego convertirse en un documento contractual del modo descripto en el párrafo anterior).

Tecnología asociada: Incluye varias formas de celebración, por medio de cartas (epistolar), por medio de telefonía (telefónico) y su instrumento directamente relacionado, el fax. En su momento se utilizaron modos de comunicación cuyo uso en esta función ha caído en desuetudo, como el telégrafo y el teletipo. Por supuesto, el avance tecnológico y técnico han permitido la aparición de una nueva forma de contrato a distancia (entre ausentes): el contrato electrónico.

Contrato electrónico (o contrato digital): Se trata de una especie contractual que se celebra por medio del intercambio de documentos digitales (electrónicos). Como el instrumento electrónico que se corresponde con el correo epistolar es el correo electrónico, esta facilidad ha permitido la celebración contractual utilizando este medio de comunicación remota.

Es de destacar que ha corrido mucha agua doctrinaria bajo el puente de las analogías: correo epistolar = correo electrónico[38], firma ológrafa = firma digital, telefonía convencional = telefonía digital (más conocida como telefonía IP) y, aunque no es el objetivo de este capítulo esta problemática en profundidad, en el momento de recurrir a dichas equivalencias es necesario analizar la jurisprudencia más actualizada posible[39].

El contrato digital no solo facilita la celebración al permitir que dos contratantes situados en las antípodas del globo puedan celebrar una transacción comercial (entre otras innumerables) utilizando este medio, sino que les permite reducir costos de viaje (con los riesgos que esto trae aparejados), obtener una forma de transacción de una celeridad imposible de concebir fuera de estos medios y dar forma a muchas de las necesidades particulares de los pequeños productores y sus compradores directos. Este es el caso de aquellos exportadores nacionales cuyo volumen de exportación es reducido (dulces regionales, jugo de arándano, miel, jalea real, carnes exóticas, etc.), cuya colocación efectiva se realiza del otro lado del Ecuador; es la manera habitual de contratar y, respecto de la consideración del Derecho, es un hecho (nos guste o no a los operadores del Derecho, las cosas se hacen así y la costumbre, en especial la costumbre comercial, siempre se termina imponiendo, porque constituye una de las fuentes principales del Derecho comercial).

El contrato digital, como forma de celebración contractual a distancia (entre ausentes)

De inmediato surgen diferencias, no presencial no significa necesariamente “a distancia”, este es un concepto que los educadores han aprendido a fuerza de chocar contra la pared. Está más relacionado con un tema de tiempos disponibles y desplazamientos innecesarios que de una distancia media o larga real entre los contratantes. Es posible que se celebre un contrato mediante el intercambio de un mensaje de correo electrónico entre un vendedor de repuestos de librería y una oficina cualquiera, situados a no más de veinte cuadras de distancia y que se resuelve contra la entrega del elemento por parte de un mensajero. Incluso el pago puede consistir simplemente en una transacción utilizando una tarjeta de crédito (caso típico de las formas contractuales de lugares como www.mercadolibre.com.ar). Como ya hemos referido, este contrato puede involucrar a personas reales o virtuales (relacionadas o no con una persona física determinada o determinable); es el caso de los contratos de compraventa en comunidades que se limitan a identificar al contratante por el apelativo que utiliza para conectarse a la referida comunidad. Asimismo, no queda clara la calidad y validez contractual del intercambio de elementos puramente virtuales (fichas de casino,

armaduras, armas, dinero virtual), pero que para su obtención deben ser abonados con dinero real (físico, transaccional, plástico, pero dinero al fin) y que pueden generar lucro y obligaciones en la sociedad física (comunal, nacional o internacional). Intentaremos destacar algunas de las diferencias entre el contrato a distancia convencional y esta nueva especie contractual:

1. En el contrato a distancia, los medios de comprobación (prueba indiciaria a aducir en el momento de probar la existencia de sus elementos esenciales, en especial del consentimiento) son soportados por elementos físicos o lógicos sumamente diferentes:

a. En el contrato entre ausentes, celebrado por medio de intercambio epistolar, en definitiva el soporte sigue siendo papel, solo se trata de un contrato firmado con cierta separación de tiempo entre una y otra parte (lo mismo pasa en el contrato presencial, ya que las partes firman sucesivamente las copias, por lo que hay también un momento en que el contrato está firmado por una parte y falta la firma de la otra).

b. En su homólogo por medio de fax, las condiciones son similares, la firma es un gráfico, pero su existencia se configura por las certificaciones automáticas que la máquina realiza al enviar el documento (fecha, hora, origen, destino). Probar el contenido del documento es otro tema.

c. En cuanto a la celebración por teléfono, depende de la posibilidad de grabar dicha conversación y que luego el tribunal lo acepte como una prueba válida.

d. Sin embargo, las tres especies anteriores pueden distinguir entre el original y la copia, porque son físicamente distinguibles utilizando técnicas de documentología o análisis de comunicaciones.

2. En el contrato electrónico, existen diversas especies (no intercambiables, ni asimilables unas a otras). Al igual que en Derecho penal, en ciencias en general y en ingeniería en particular, las analogías están específicamente prohibidas[40], salvo como disparador de ideas e investigaciones:

a. El contrato interpersonal, donde dos interlocutores (físicamente determinados, determinables o no) deciden realizar un contrato (por ejemplo, la compraventa de productos, a nivel nacional o internacional).

b. El contrato entre una "tienda virtual" y sus compradores (caso típico de Amazon).

c. El contrato de adhesión (generalmente de servicios) que me permite solicitar, obtener y pagar en línea, desde el acceso a un servicio de cable hasta la gestión remota de mis cuentas bancarias (e-banking), cursar carreras de todo tipo (e-learning), o adquirir productos mediante el mecanismo de remate aceptando las condiciones del portal de ventas (ejemplo, Mercado Libre).

d. La licitación pública, que finaliza en contrato siguiendo los procedimientos establecidos por la respectiva unidad administrativa (entre otros, los contratos de servicios para entidades que forman parte de la APN, en licitación pública, donde todo el intercambio se realiza por medios electrónicos, cuyo ejemplo más empleado por los ofertantes es www.argentinacompra.gov.ar).

e. Otro grupo de contratos que, sin estar específicamente incluidos en alguna de las formas canónicas anteriores, se celebran por medios similares.

3. Diferencias insalvables entre un contrato y otro:

a. Entre los contratos celebrados a distancia (entre ausentes) por medios convencionales, es posible determinar la diferencia entre un original y su copia, recurriendo al principio de identidad[41]. En el caso del contrato electrónico, el original y la copia son indistinguibles porque son idénticos[42].

Ley 25.506 de Firma Digital. Artículo 11. – "Original. Los documentos electrónicos firmados digitalmente y los reproducidos en formato digital firmados digitalmente a partir de originales de primera generación en cualquier otro soporte, también serán considerados originales y poseen, como consecuencia de ello, valor probatorio como tales, según los procedimientos que determine la reglamentación".

b. Certificación del documento (e implícitamente de la existencia de los elementos esenciales del contrato: consentimiento, objeto y causa). Un contrato convencional (local o entre ausentes) se puede certificar sin inconvenientes por medio de uno o más escribanos públicos. Un contrato electrónico, al día de la fecha, no se puede certificar mediante mecanismos digitales válidos (certificados digitales basados en mecanismos de firma digital, generados por autoridades certificantes válidas) de manera alguna en nuestro país, mucho menos en su entorno internacional, enmarcado en el Derecho internacional privado. De ahí la importancia perentoria e ineludible de gestionar la prueba documental, la de informes y la pericial informático forense, tomando los recaudos necesarios que dicha prueba implica y su consecuencia directa, como soporte argumental de la pretensión solicitada (la vigencia contractual o precontractual en este caso).

¿Por qué razón afirmamos que en este momento no hay manera de validar un contrato electrónico, salvo recurriendo a la solución heurística de imprimirlo y tratarlo como si fuera un documento más (bibliográfico, pictográfico o foliográfico)? Por diversas razones, algunas de legalidad, otras de hecho:

Ley 25.506 de Firma Digital

Artículo 1. – "Objeto. Se reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en las condiciones que establece la presente ley".

Artículo 2. – "Firma Digital. Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose esta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma".

"Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes".

Hasta la fecha (pese a que la ley lo determina y faculta), no ha sido implementado sistema alguno de validación que otorgue poder de Autoridad Certificante, con validez nacional, a institución alguna. Existen referentes limitados como el Ar-CERT, aplicado a aquellos organismos de la APN, que actualmente se encuentran en vías de implementarlo; y en el caso particular del Poder Judicial, para algunos, muy escasos y limitados documentos, generalmente de circulación interna específica. En realidad, al carecer de estas autoridades certificantes, estamos ante la presencia de firmas electrónicas, que de ninguna manera tienen el mismo alcance y validez que la firma digital.

De más está decir que no existen autoridades digitales certificantes reconocidas universalmente en el Derecho internacional privado (ni en las relaciones bilaterales, ni en las multilaterales, ni en el Derecho de integración), salvo acuerdo de partes que debe figurar específicamente detallado en el contrato y con la aclaración de los organismos que deberán resolver la cuestión (el Lloyd's de Londres o los organismos internacionales de mediación y conciliación comercial). De hecho, algunos organismos se comportan como tales (Validate, Certificate), pero dependen de la confianza que sus usuarios pongan en sus servicios y no de una normativa preestablecida.

Artículo 3. – "Del requerimiento de firma. Cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital. Este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia".

Artículo 5. – "Firma electrónica. Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez".

El artículo 3 establece la equivalencia entre la firma digital y su homóloga ológrafa, pero el artículo 5 nos indica que en el caso de la firma electrónica

corresponde acreditar su validez a quien la invoca y esto ¿cómo se logra en la práctica? Mediante una gestión adecuada de la prueba documental informática, de la prueba de certificación mediante informes y de la prueba de revisión técnica pericial. En definitiva, mediante la gestión estrictamente legal, metodológicamente criminalística y técnicamente informático forense de la prueba indiciaria informática.

Artículo 6. – "Documento digital. Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura".

La importancia de este artículo reside en que el denominado contrato electrónico no es más que una especie del documento digital.

Artículo 7. – "Presunción de autoría. Se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma".

En este caso, se refiere a la firma digital, que como vimos no está implementada en nuestro país y mucho menos en el Derecho de integración que nos une a otros países.

Artículo 8. – "Presunción de integridad. Si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento digital es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma".

Esto se hace mediante una rutina de hash y la certificación mediante un escribano público, pero forma parte de la gestión de la prueba documental informática, juntamente con su correspondiente cadena de custodia.

Artículo 9. – "Validez. Una firma digital es válida si cumple con los siguientes requisitos:

a) Haber sido creada durante el período de vigencia del certificado digital válido del firmante;

b) Ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente;

c) Que dicho certificado haya sido emitido o reconocido, según el artículo 16 de la presente, por un certificador licenciado".

Artículo 10. – "Remitente. Presunción. Cuando un documento digital sea enviado en forma automática por un dispositivo programado y lleve la firma digital del remitente se presumirá, salvo prueba en contrario, que el documento firmado proviene del remitente".

Artículo 12. – "Conservación. La exigencia legal de conservar documentos,

registros o datos, también queda satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente, según los procedimientos que determine la reglamentación, siempre que sean accesibles para su posterior consulta y permitan determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/o recepción".

Estos artículos serán aplicables cuando se implemente el mecanismo de firma digital establecido por la ley, hoy no tienen utilidad práctica procesal alguna (con las excepciones antes detalladas).

El problema de la jurisdicción en el contrato electrónico internacional

Determinar el momento, el lugar y la jurisdicción ante la cual litigar es un problema local sumamente complejo[43] y que atañe a los especialistas en el tema; hacerlo en el ámbito internacional incrementa la dificultad a niveles superlativos. Considerando que siempre que hay comercio surgen "problemas" y que muchos de ellos requieren sino la acción litigante directa, al menos el empleo de formas alternativas de resolución de conflictos, es evidente que el crecimiento de estas formas conflictivas continuará siendo exponencial como hasta la fecha[44]. La decisión sobre la elección de la forma de gestionar el conflicto y, de ser necesario, la jurisdicción ante la cual litigar, es compleja. En general, se prefiere optar por recorrer todas las gamas de resolución alternativa de conflictos disponibles (negociar, conciliar y por fin recurrir al arbitraje). El arbitraje internacional es una costumbre comercial inveterada, desde el clásico Lloyd's londinense hasta los nuevos organismos multinacionales públicos y privados. En cuanto a la jurisdicción, depende de la teoría de conclusión del contrato que se adopte:

1. De la declaración (manifestación): Hay consentimiento y se considera concluido el contrato desde que el aceptante declara, manifiesta, por cualquier medio la conformidad con la oferta recibida (todo tipo de prueba).
2. De la expedición (emisión): El contrato queda concluido desde que se envía la aceptación (mensaje aceptando y su hora GMT).
3. De la recepción: Se requiere que el oferente haya recibido la aceptación (momento de apertura del mensaje aceptando; no siempre es posible de determinar por medios periciales, depende del servicio de validación y confirmación de recepción – "Aviso de Retorno"– que ofrece el proveedor del servicio de correo electrónico).
4. De la información: La aceptación debe llegar efectivamente a conocimiento del oferente (no de otra persona, muy difícil de probar pericialmente).
5. Recordemos que nuestro Código Civil sigue la teoría de la expedición (art. 1154) con dos excepciones para la teoría de la información (arts. 1149 y 1155).

6. En cuanto a los servicios, se comportan en general como contratos de adhesión (especialmente las empresas de seguros internacionales y sus relaciones con sus homólogas nacionales y las nuevas formas específicas como el Contrato Internacional de Outsourcing de Sistemas de Información[45]).

El Derecho internacional privado es sumamente complejo e incluye relaciones bilaterales, multilaterales, regionales; se encuentra en constante evolución y cambio, lo que requiere de una actividad de adecuación normativa y actualización profesional agotadora. Esta actividad se caracteriza (como todas las normas del Derecho) por consumarse a posteriori de la evolución tecnológica y de la forma contractual evolucionada que, como decía, ya es un hecho y no una posibilidad.

Una opción prometedora en el ámbito regional aparece actualmente en plena etapa de desarrollo e implementación dentro de nuestro Derecho de integración. El proyecto Mercosur Digital es una iniciativa de cooperación internacional entre la Comisión Europea y el Mercosur[46]:

1. Tiene como objetivo promover políticas y estrategias comunes en el área de la sociedad de la información y reducir las asimetrías en el campo de las tecnologías de la información y de la comunicación.

2. Busca aumentar las competencias y el uso de las tecnologías de la información y comunicación (TICs) entre las instancias de decisión de los sectores público, privado y de la sociedad civil en el Mercosur, por medio de actividades conjuntas de capacitación, desarrollo de infraestructura de TICs, relacionadas con la formación de recursos humanos y aplicaciones de comercio electrónico.

3. Está incluido en el documento de estrategia regional de la Comisión Europea, que establece la cooperación con el Mercosur para el período 2007-2013, teniendo como beneficiarios los cuatro miembros plenos del Grupo Mercado Común del Mercosur: Argentina, Brasil, Paraguay y Uruguay.

4. La Red Nacional de Enseñanza e Investigación, delegada por el GMC, cumple la función de la Entidad Gestora del Mercosur Digital, que se encarga de controlar y auditar el cumplimiento del contrato de gestión. Es una organización social supervisada por el Ministerio de Ciencia y Tecnología de Brasil.

5. Intereses particulares:

a. Comercio electrónico y beneficios: Creación de un marco regulatorio común para el Grupo Mercado Común, con base en firma digital, protección de datos, crímenes electrónicos y factura electrónica. Optimización de la infraestructura para disminuir las asimetrías en la región: certificación digital, certificación de tiempo (timestamp) y firma digital. Construcción de una plataforma común de comercio virtual para las pequeñas y medianas

industrias (PyMEs).

b. Escuela Virtual para la Sociedad de la Información en función del concepto de educación continua. Implantación de una red de capacitación virtual, interconectando los países del Mercosur para capacitación en temas de economía digital.

c. Inversión prevista, 9.600.000 euros (7.000.000 de euros por la Comisión Europea y el resto el Mercosur).

La prueba documental informática en el entorno regional

Aunque, como vimos, el problema es complicado y la solución regional por medio del Mercosur Digital podría facilitar la tarea no solo respecto de la región, sino también en lo referente a las relaciones comerciales con Europa, queda un enorme nicho sin regulaciones comunes aplicables.

En relación con el ámbito nacional, el correo electrónico en general es aceptado como elemento probatorio[47]. No obstante, a los efectos prácticos, el operador del Derecho, una vez seleccionada la estrategia judicial a seguir, su argumentación y su respaldo probatorio, en lo referente a la gestión de la prueba documental informática, debe seguir las normas y protocolos que ya hemos revisado en el Manual de Informática Forense[48]. En particular, sobre la protección de la privacidad de los interlocutores externos a nuestro consultante legal[49]. Debe tenerse en cuenta que la preservación de los datos en poder de nuestro consultante será realizada respetando estrictamente las condiciones establecidas para las diligencias previas o preliminares, en especial porque normalmente deben ser efectuadas in audita altera pars y al solicitar la diligencia al juez, cualquier error procedimental implicará la inmediata negativa a dicha diligencia; como ejemplo queremos ofrecer al lector un fragmento de la resolución del Expediente 39.749, "G., D.E.c/C. SA. s/diligencia preliminar", Juzgado Comercial 18, Secretaría, 16 de octubre de 2001.

"Que en ese marco normativo, y a la luz de la señalada garantía del art. 18 de la Constitución Nacional (cfr. Fernández – Gómez Leo, ob. cit., t. II, p. 126), debe distinguirse entre el efecto probatorio de la correspondencia epistolar entre comerciantes (sea para la celebración del contrato, sea para su ejecución, o sea para su rescisión) de la posibilidad de ordenar, de manera genérica, el allanamiento de su correspondencia en busca de la que presume el contrario será favorable a sus intereses".

"Que, a tal efecto, la exhibición de la correspondencia entre comerciantes con motivo de una negociación debe asimilarse a la parcial de los libros de comercio, que es admitida por la legislación mercantil en caso de pleito

pendiente, o como medida preliminar, pues reposa en el principio de la comunidad de los asientos (art. 59, Código de Comercio; cfr. Fernández – Gómez Leo, ob. cit., t. II, p. 127 y sgtes.)".

"Sin embargo, se ha dicho que ello no autoriza a efectuar esa exhibición en forma compulsiva, ya que la negativa trae aparejada la sanción prevista por el art. 56, es decir, el litigio será resuelto en función de los libros de su adversario (cfr. Fernández – Gómez Leo, ob. cit., t. II, p. 137)".

"3.4. Que, además de lo expuesto, no puede dejar de merituarse que si bien es cierto el art. 387 del Código Procesal Civil y Comercial de la Nación establece que 'Las partes y los terceros en cuyo poder se encuentren documentos esenciales para la solución del litigio, estarán obligados a exhibirlos o a designar el protocolo o archivo en que se hallan los originales', y que 'El juez ordenará la exhibición de los documentos, sin sustanciación alguna, dentro del plazo que señale', no es menos cierto que el art. 388 que le sigue y el 36, inc. 2 c, con el que ambos concuerdan, no autorizan al juez al secuestro o exhibición compulsiva de esos documentos sino tan solo a considerar la negativa a presentarlos, como una presunción en contra del renuente, en concordancia también con la mencionada normativa del Código de Comercio".

"Que por otra parte, tampoco puede dejar de advertirse que mientras la medida que pide el demandante supone el allanamiento de equipos de computación de la demandada para determinar la existencia de correos electrónicos por aquella supuestamente remitidos, o enviados a su parte por la propia demandada, ha omitido toda mención al texto de esos correos y los por ella misma recibidos, ni acompañado copia de los mismos, siendo que, por los usos y costumbres comerciales (art. 5 del Título Preliminar del Código de Comercio), la existencia de esas copias puede presumirse tanto en los propios equipos de computación de la accionante como en los de su Proveedor de Servicios de Internet (ISP), a quien tampoco individualizó. Siendo así, la medida requerida aparece violatoria del principio de igualdad procesal que este juez debe preservar (art. 34, inc. 5 c, del Código Procesal)".

"Nótese además en tal sentido que en aplicación de ese principio, el art. 356 del mismo Código obliga a la demandada a '...Reconocer o negar categóricamente [...] la autenticidad de los documentos acompañados que se le atribuyeren y la recepción de las cartas y telegramas a él dirigidos cuyas copias se acompañen', contemplando seguidamente que '...su silencio, sus respuestas evasivas, o la negativa meramente general podrán estimarse como reconocimiento de la verdad de los hechos pertinentes y lícitos a que se refieran. En cuanto a los documentos se los tendrá por reconocidos o recibidos, según el caso'".

“3.5. Que, por último, no empece a lo expuesto la previsión del art. 326, inc. 2, del Código Procesal, desde que el ámbito de aplicación de dicha norma no invade las limitaciones impuestas por el resto de las citadas en los párrafos precedentes”.

“Por todo lo expuesto, y con el alcance que se desprende de la presente, RESUELVO rechazar la medida de prueba anticipada. Notifíquese por cédula por Secretaría. Fdo. Javier E. Fernández Moores. Juez”.

En este sentido, y para no abundar en temas ya tratados, debemos decir que respecto de la información en poder de nuestro consultante, es decir, de la que obra en el disco rígido de su máquina, dicha información es de su propiedad y no requiere ningún pedido de autorización para ser resguardada. Él tiene la potestad de hacerlo y salvo que él mismo la elimine o no la resguarde de manera adecuada, seguirá en su poder durante todo el transcurso de la causa.

Por lo tanto, si uno pretende una medida anticipada sobre la información obrante en discos de la contraparte o de terceros, es necesario recolectar, resguardar, certificar ante escribano público e iniciar la correspondiente cadena de custodia sobre la información propia.

Al momento de solicitar la medida anticipada, se agrega este material (y de ser necesario su copia impresa), con lo que se justifica la solicitud. En cuanto a la aceptación de la medida por parte del juez, no está asegurada, pero al menos podremos presentar nuestra prueba documental informática en el momento de iniciar la demanda (junto con el resto de la prueba documental).

Es preciso recordar que respecto del origen, destino y hora de los mensajes de correo electrónico, siempre hay que solicitar una prueba de informes que certifique dichos datos al proveedor de servicios que corresponda (ISP) y luego, de ser preciso, requerir la correspondiente prueba pericial informático forense.

En general, al producirse un problema internacional, como la pérdida de mercadería perecedera, consecuencia de un corte de rutas internacionales (por ejemplo, en el caso de los camiones que traen bananas desde San Pablo y regresan con manzanas del Alto Valle de Río Negro), intervienen los productores, los compradores, las empresas de transporte y por supuesto las empresas de seguros[50].

En las ocasiones en que el litigio se judicializa y es posible elegir la jurisdicción (por ejemplo, en los problemas relacionados con los cruces de fronteras), la decisión mayoritaria se define por litigar en el país que brinda más facilidades para establecer el pleito. Lamentablemente, no somos ese país, es tiempo de hacer algo al respecto, para recuperar nuestra posición internacional.

Ser elegidos como país para litigar implica ser respetados por la comunidad

jurídica internacional, como referentes de Derecho internacional privado, algo que suponemos de interés para toda la comunidad jurídica y, si no lo fuere, al menos es nuestro deseo particular, producido como consecuencia de interpretar una realidad que vemos desde atrás, cada vez más lejos en el horizonte normativo.

36 El uso de distintas bases numéricas es algo común en la vida diaria, solo que normalmente no le prestamos atención.

El sistema decimal lo tenemos integrado a nuestra cultura (la base 10), pero no es el único. Cuando una persona nos pregunta la hora y decimos doce menos cuarto (implica decir, falta un cuarto de hora para las doce o, lo que es lo mismo, una hora dividida en cuatro partes), sabemos que ese cuarto de hora está compuesto de 15 minutos y no de 25, como sería lo lógico en el sistema decimal. ¿Por qué esta división? Porque estamos utilizando una base sexagesimal (60) típica de los griegos. Por eso, las dificultades al dividir horas por un número dado y procesar los minutos y segundos (la famosa multiplicación del resto por 60, antes de volver a dividir), pero sin embargo, a partir de los segundos se utilizan décimas y centésimas (vuelta a la base decimal). ¿Por qué esta nueva característica? Simplemente porque la división del tiempo en décimas y centésimas de segundo es un tema científico avanzado que nunca fue intentado por los griegos y que no formaba parte de la cultura. No necesitaban tanta precisión y, de hecho, no tenían instrumentos para medirla. Bien, hoy somos capaces de pasar de una base a otra sin dificultad no solo con la medición del tiempo, sino también con los ángulos. Existen entonces por lo menos dos bases numéricas de uso frecuente: la decimal (10) y la sexagesimal (60), ahora es solo cuestión de extender la idea y tendremos una aproximación a las bases binaria (2), octal (8), hexadecimal (16) y cualquier otra que podamos concebir y utilizar de manera práctica (de hecho, los mayas tenían un sistema de numeración sumamente curioso, en base 20).

37 Este tecnicismo probablemente le resulte extraño al lector; sin embargo, está más acostumbrado a él de lo que aparenta: cuando al escribir un texto no podemos encontrar por ejemplo, la letra "ñ", la "fabricamos" oprimiendo la tecla "Alt" y el número 164 (utilizando el teclado numérico) y aparece como por arte de magia. Pero, ¿en qué consiste esa "magia"? Simplemente en el uso de la tabla ASCII, incorporada al sistema operativo de la computadora. Si pensamos que el primer byte es 00000000, el segundo 00000001 y el último 11111111, y los representamos uno a continuación de otro en sucesivas filas, nos daremos cuenta de que suman un total de 256 filas, cada una de ellas ha sido asignada a un carácter del teclado que utilizamos. De ahí que el renglón número 164 se corresponde con la letra "ñ" (160=á, 130=é, 161=í, 162=ó, 163=ú), al oprimir la tecla "Alt", el programa "entiende" que a continuación le pasaremos un renglón determinado de la tabla ASCII y al anotar 164 desde el teclado numérico, selecciona y muestra en pantalla dicho renglón que se corresponde con la "ñ" que buscábamos (si hubiéramos oprimido el 97, mostraría la letra "a") y así con todos y cada uno de los caracteres del teclado y su correspondiente fila en la tabla ASCII.

38 Tal vez la primera referencia jurisprudencial equiparando el correo electrónico con el correo epistolar sea el caso Martolio/Lanata, de 1999. El señor Edgardo Héctor Martolio inició una querella penal contra el periodista Jorge Ernesto Lanata por los delitos de violación de correspondencia y publicidad de correspondencia con fundamento en los arts. 153 y 155 del Código Penal. Intervino el Juzgado Nacional en lo Correccional Nro. 6 de la Capital Federal, ante quien el demandado planteó la falta de acción por hecho atípico, la que fue rechazada y luego apelado dicho rechazo. En diciembre de 1999, la Sala VI de la Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Capital Federal confirmó el rechazo de la excepción opuesta. El querellado

interpuso recurso de casación, y rechazado este, recurso de queja, que también fue rechazado. Los fallos citados establecieron que tanto el artículo 153 como el 155 del Código Penal, han dejado abierta la descripción típica a cualquier "otro papel privado" y a "despachos de otra naturaleza"; pudiendo considerarse equiparado entonces el correo electrónico a la correspondencia tradicional. Para estos fallos, "el tan difundido e-mail de nuestros días es un medio idóneo, certero y veloz para enviar y recibir todo tipo de mensajes, misivas, fotografías, archivos completos, etc.; es decir, amplía la gama de posibilidades que brindaba el correo tradicional al usuario que tenga acceso al nuevo sistema. Es más, el correo electrónico posee características de protección de la privacidad más acentuadas que la inveterada vía postal a la que estábamos acostumbrados, ya que para su funcionamiento se requiere un prestador del servicio, el nombre de usuario y un código de acceso que impide a terceros extraños la intromisión en los datos que a través del mismo puedan emitirse o archivarse. Sentadas estas bases preliminares, nada se opone para definir al medio de comunicación electrónico como un verdadero correo en versión actualizada" (extractado del fallo de la Sala VI).

39 Este tema se relaciona directamente con la contraposición permanente entre dos o más derechos que se intersectan y/o se contradicen, en especial al momento de ser utilizados en el marco del derecho procesal correspondiente. Estas parejas de derechos (por ejemplo, el derecho a la privacidad y el Derecho a la jurisdicción) constituyen controversias doctrinarias muy difíciles de resolver. Para tomar un caso de entre los múltiples que se producen: si consideramos que el correo electrónico es solo una variante más de la clásica correspondencia epistolar y que difiere de esta nada más que en el soporte (papel vs. digital), entonces ¿es posible utilizar las mismas reglas para autorizar su secuestro (interceptación) e inspección durante la investigación judicial? Una respuesta desde el conocimiento vulgar posiblemente resultaría positiva (circunstancia extensiva a los medios de comunicación) y que algo similar ocurre en cuanto a la telefonía digital respecto de la telefonía convencional. Sin embargo, en Derecho penal no está admitida la analogía, y la tecnología y técnica involucradas en cada caso difieren sustancialmente. En particular, porque las adulteraciones y falsificaciones que se pueden realizar por medios electrónicos (falsificaciones idénticas, entre otros supuestos), no son siquiera concebibles para los documentos con soporte en papel. Estamos en presencia de nuevas formas de comunicación, que requieren de normativa específica y clara en consonancia con la tecnología analizada, uno de estos ejemplos es la Ley de Firma Digital, algo similar debería ocurrir respecto de la telefonía IP, el correo electrónico y los contratos digitales.

40 Para ejemplificar estas analogías científicas de uso diario, podemos considerar que a partir de la observación de la caída de los cuerpos, fue posible crear una ley de gravitación (toda ley humana es solo un modelo de comportamiento inventado para dar sentido racional a la realidad física y social en que se encuentra inserto el ser humano), de validez humana y local respecto de la porción de universo en que habitamos y con la que nos relacionamos directamente; si tratamos de extenderla analógicamente a todo elemento real o virtual del universo, veremos que resulta imposible de comprobar. Otro ejemplo: todo electrón permanece en su orbital, mientras no obtenga energía adicional para abandonarlo, sin embargo, a veces puede obtener esa energía de la "nada" o del "vacío" y escapar por "efecto túnel".

41 Principio de identidad clásico: Un objeto material es idéntico a sí mismo y diferente de todos los demás.

42 Principio de identidad impropio (de copias): Del original, ya que cuando se duplica un archivo informático, la copia no es igual a la original, sino idéntica (un bit no difiere de otro bit y entre sí son inidentificables unívocamente).

43 Un ejemplo de resolución a este problema lo constituye el siguiente fallo: "Martino, Daniel Alejandro s/estafa" CSJN 23/05/2006: "La presente contienda negativa de competencia suscitada entre el Juzgado Nacional en lo Criminal de Instrucción n° 1 y el Juzgado de Garantías n° 4 del departamento judicial de San Isidro, provincia de Buenos Aires, se refiere a la causa instruida con motivo de la denuncia efectuada por Gabriel Leonardo Rotzejd. En ella manifiesta que el 15 de octubre de 2005 en horas del mediodía, efectuó una compra por Internet desde su computadora personal, a través del portal de subastas denominado 'más oportunidades.com', donde la firma

'Tecnocel' ofertaba televisores marca 'Philips' de 25 pulgadas.

Agrega que en esas circunstancias, recibió un mensaje desde una casilla de correo perteneciente a una persona que se identificó como Ariel, quien le suministró un número de teléfono celular con el que debía comunicarse para concretar la operación y, a su vez, le manifestó que para que le enviaran el aparato tenía que depositar por medio de 'Western Unión' la suma de novecientos cuarenta y nueve pesos con ochenta y siete centavos a nombre de Daniel Alejandro Martino D.N.I. ..., con domicilio en Francia ..., de la localidad bonaerense de Luján, o Agustín Álvarez ... de Vicente López. Señala también que se dirigió a la agencia nº 126 de esa empresa –sita en avenida Córdoba y Jorge Newbery– donde efectuó un depósito por el referido monto y, no obstante, que el giro fue cobrado por el supuesto destinatario, no logró que le enviaran el televisor a su domicilio. El juez nacional declaró su incompetencia a favor de la justicia provincial, con base en que el perjuicio patrimonial se habría producido en la localidad de Martínez, donde fue retirado el dinero (fs. 27/29). El magistrado local rechazó esa atribución, con fundamento en que la disposición patrimonial se habría producido en la Capital Federal, donde el denunciante efectuó el depósito (fs. 34/35). Con la insistencia del juzgado capitalino quedó formalmente trabada esta contienda (fs. 36/38). Advierto que de acuerdo con la calificación escogida por ambos magistrados, la contienda debería resolverse atendiendo a razones de economía procesal y teniendo en cuenta los distintos lugares donde se desarrollaron actos con relevancia típica (conf. Fallos: 311:2055; 317:915; 318:2509 y 323:174, entre otros). Sin embargo, entiendo que los elementos hasta ahora incorporados al incidente, no resultan suficientes para formular un juicio cierto en tal sentido, ya que aún no se individualizó a los imputados, ni se agregaron los resultados de las investigaciones referidas a las líneas telefónicas que se habrían utilizado para cometer el hecho (vid. fs. 22), ni la pertenencia de la dirección de correo electrónico ..., desde la que se habrían contactado con el denunciante.

De acuerdo con este criterio, atento a que Gabriel Leonardo Rotzejd concertó la operación vía Internet, y realizó las llamadas telefónicas mediante las cuales se lo instruyó para que hiciera la transferencia monetaria desde su domicilio sito en esta Capital, donde además depositó el dinero, opino que corresponde al Juzgado Nacional en lo Criminal de Instrucción nº 1, que previno (Fallos: 311:67; 317:486 y 319:753, entre otros) y a cuyos estrados concurrió el denunciante a hacer valer sus derechos (Fallos: 291:272; 293:405; 311:487, y Competencias nº 1818 L. XXXVII in re "Gómez, Lucrecia Lleana s/denuncia", y 735, L.XL in re "Stocker, Héctor Raúl y otros s/defraudación a un menor o incapaz", resueltas el 13 de noviembre de 2001 y 14 de octubre de 2004, respectivamente), continuar conociendo en la causa, sin perjuicio de lo que surja ulteriormente". Bs. As., 6 de marzo de 2006. Fdo.: Casal. Adhieren a

la opinión del Procurador Fiscal, Fdo.: Petracchi, Highton de Nolasco, Maqueda, Zaffaroni, Lorenzetti, Argibay.

44 Para ampliar esta afirmación, recurriré a mi experiencia personal, son cada vez más frecuentes las ocasiones en que debo realizar recolección de prueba documental informática para ser empleada luego como soporte argumental, en un posible litigio de Derecho internacional privado (un pequeño productor de jalea real vende su producto a un revendedor en Bélgica, realizando toda la contratación mediante el intercambio de mensajes de correo electrónico y luego se produce algún incumplimiento contractual). En general, estos temas se terminan resolviendo por conciliación entre las partes y sus representantes legales, en particular porque los comerciantes, pese a sus técnicas dilatorias, normalmente prefieren mantener su actividad (por supuesto sin olvidar las posibles quiebras o actividades netamente delictivas): el que vende jalea real quiere seguir vendiendo a Bélgica (entre otras cosas, por las divisas que recibe y las ganancias que obtiene respecto del mercado local) y el comprador en Bélgica tiene su propio mercado cautivo que está pendiente del producto y lo seguirá requiriendo. Sin embargo, sea cual fuere la manera de resolver las cosas (conciliación, mediación, arbitraje, hasta finalizar en el pleito judicial), lo cierto es que la gestión de la prueba se constituye en un elemento primordial a la hora de planificar la estrategia de reclamo (pretensión) a desarrollar e implementar.

45 *Ver Altmark, Daniel Ricardo, El contrato de Outsourcing de Sistemas de Información, Lexis Nexis, Bs. As., 2006.*

46 Fuente: http://www.mercosurdigital.org/.

47 *Incorporación de un correo electrónico como prueba: "Steinhaus, Raquel y otros", Cámara Nacional en lo Penal Económico, Sala A, 13/09/2002. Se cuestionó la incorporación como prueba de cargo de comunicaciones de correo electrónico aportadas a la instrucción por la denunciante. La Cámara revocó la resolución apelada y declaró la nulidad de la incorporación de dichas piezas, se accedió a ellas en razón de desempeñarse la denunciante como secretaria privada del imputado, ya que las comunicaciones que se cursan por vía electrónica constituyen correspondencia epistolar cuya inviolabilidad se encuentra garantizada por la Constitución Nacional, por lo que no puede entenderse que la autorización con que contaba para abrirla y enterarse de su contenido suponía la atribución de disponer de ella o comunicarla a terceros, siendo únicamente el juez quien puede disponer su incautación. Desestimación de un correo electrónico como prueba: "Grimberg, Alfredo H. s/sobreseimiento". Cámara Nacional Criminal y Correccional de la Capital Federal, Sala I, 11/02/2003. La Cámara decretó la invalidez como prueba de un correo electrónico al que se había accedido ilegalmente. "El correo electrónico es sin lugar a dudas correspondencia privada que está protegida por la Constitución Nacional y otros tratados sobre derechos humanos incorporados a ella. El reconocimiento de la libertad de intimidad, y el consecuente derecho a la vida privada, configuran un valor que está estrechamente relacionado con la dignidad del ser humano en función de la idea política dominante en las sociedades en vísperas del siglo XXI. La violación de estas garantías básicas conllevan la nulidad de las actuaciones que dependen de esos actos procesales, más allá de la distinción que la doctrina ha hecho sobre prohibición de prueba y prohibición de valoración de la prueba. La única forma en que se puede ingresar al ámbito privado es por orden de juez competente, mediante auto fundado, ya que esa es la autoridad a la que se refiere la Constitución Nacional. El hecho de que anónimamente se haya hecho llegar la correspondencia del correo electrónico de la parte imputada lleva sin duda a la invalidez de dicho acto que es la base de toda posible acusación".*

48 Arellano González, Luis Enrique, "La prueba documental informática (recaudos procesales)", Compendio Jurídico de doctrina, jurisprudencia y legislación, Erreius, Errepar, Nº 44, septiembre de 2010, pp. 13 a 33.

49 *El derecho a la privacidad, es decir, ese derecho individual a no sufrir intromisiones en la intimidad por parte del Estado, encuentra hoy reconocimiento internacional en diversos documentos. Así, se desprende de los artículos 11, inc. 2, del Pacto de San José de Costa Rica; 17.1 del Pacto Internacional de Derechos Civiles y Políticos; 12 de la Declaración Universal de Derechos Humanos; 5 de la Declaración Americana de Derechos y Deberes del Hombre; 8, inc. 1, de la Convención Europea de Salvaguarda de los Derechos del Hombre y de las Libertades Fundamentales; y 5 de la Declaración de Bogotá 1948, entre otros instrumentos internacionales*

vigentes. Fuente: http://www.terragnijurista.com.ar/doctrina/escuchas.htm (en este documento se hace una recopilación sumamente completa de la normativa internacional vigente relacionada con el problema de las escuchas).

50 Legislación de referencia, a tener en cuenta en el momento de patrocinar:

Naciones Unidas

- Ley Modelo de las Naciones Unidas sobre Comercio Electrónico.
- Ley Modelo de las Naciones Unidas sobre Firma Electrónica.
- Directrices de las Naciones Unidas para la Protección del Consumidor (en su versión ampliada de 1999).

Unión Europea

- Directiva 1999/93/CE del Parlamento Europeo y del Consejo de la Unión Europea estableciendo un marco comunitario para la firma electrónica.
- Decisión Marco 2005/222/JAI del Consejo del 24 de febrero de 2005 relativa a los ataques contra los sistemas de información. Conforme a ella los países miembros de la Unión Europea deberán incorporar en sus legislaciones la figura penal del hacking.
- Convention on Cybercrime Budapest 23/11/2001.

Brasil

- Decreto 3587 Infraestructura de Clave Pública del Poder Ejecutivo Federal de Brasil.
- Anteproyecto Ley Comercio Electrónico, Documento Electrónico y Firma Digital de Brasil.
- Medida Provisoria 2200-2 de 2001. Se instituye la infraestructura de claves públicas brasilera ICP-Brasil. Regula la certificación electrónica y la firma digital, confiriendo autenticidad, integridad y validez jurídica a los documentos electrónicos.
- Portaria Interministerial MC/MCT 147 de 1995. Crea el Comité Gestor de Internet del Brasil (CGIbr).
- Comité Gestor de Internet del Brasil, Resolución 001. Resumen de reglas actualmente adoptadas para el registro de dominio en el país.
- Comité Gestor de Internet del Brasil, Resolución 002. Delega a la FAPESP las actividades de registro de dominio, distribución de direcciones IPs y su mantenimiento en Internet.

Chile

- Ley de Delitos Informáticos de Chile.
- Decreto de Firma Digital para la Administración del Estado de Chile.
- Ley 19.799 sobre Firma Electrónica de Chile.

Colombia

- Ley 1065 de Nombres de Dominio de Colombia.
- Ley 527/99 de Mensajes de Datos, Comercio Electrónico y Firma Digital de Colombia.
- Decreto 1747 Reglamentario de la ley 527 de Colombia.
- Resolución 26.930 de Entidades de Certificación de Colombia.
- Ley 679 Abuso y Pornografía de Menores en Internet.

Ecuador

- Ley de Comercio Electrónico, Firmas y Mensajes de Datos de Ecuador.
- Decreto 3496 Reglamento General a la Ley de Comercio Electrónico, Firmas y Mensajes de Datos.

España

- Orden 662/2003 del 18 de marzo de 2003 que aprueba el Plan Nacional de Nombres de Dominio Internet bajo el Código de País correspondiente a España, "es" (modificada).
- Nuevo Plan Nacional de Nombres de Dominio de Internet correspondiente a España "es". Orden ITC/1542/2005 del 19 de mayo de 2005.
- Real Decreto 14/1999. Firma Electrónica en España (derogado por la ley 59).
- Ley 59/2003. Firma Electrónica en España.
- Ley 34 de Servicios de la Sociedad de la Información y Comercio Electrónico del 11/07/2002 (incluye modificaciones introducidas por las leyes 32/2003 y 59/2003).

México

- Código Penal Federal de México. Delitos Informáticos.
- Código Penal Estado para el Estado de Sinaloa. México. Art. 217. Delito Informático.

Paraguay

- Ley 1682. Reglamenta la información de carácter privado.

Perú

- Ley 27.269 del Perú de Firma y Certificado Digital.
- Ley 27.310. Modifica art. 11, ley 27.269.
- Decreto Reglamentario Ley de Firma y Certificado Digital.
- Ley 27.291 del Perú que modifica el Código Civil Medios Electrónicos y Firma Digital.
- Ley 27.309 de Delitos Informáticos del Perú.
- Ley 27.419 sobre Notificación por Correo Electrónico del Perú.

- Ley 27.444. Notificación por Correo Electrónico en los Procedimientos Administrativos.
- Ley 28.493 del 18 de marzo de 2005. Regula el uso del correo electrónico no solicitado.

Uruguay

- Ley 16.736. Expediente Electrónico.

Venezuela

- Ley sobre Mensajes de Datos y Firma Electrónica de Venezuela.
- Ley Especial sobre los Delitos Informáticos Nº 48 de Venezuela.

CAPÍTULO 7
EL ROL DEL PERITO INFORMÁTICO FORENSE EN EL PROCESO JUDICIAL

Cada día nos sorprende alguna novedad jurisprudencial que modifica nuestra forma de interpretar y especialmente de practicar el Derecho, ante los distintos estrados judiciales. Esto debería ser una circunstancia enriquecedora y una prueba directa sobre el carácter evolutivo de las Ciencias Jurídicas, acompañando el desarrollo científico, tecnológico y técnico de la sociedad en la cual están insertas y que son la razón de su existencia.

Sin embargo, a poco de leer los fallos, nos encontramos que muchos de ellos muestran graves falencias en la gestión de la prueba, por parte de los operadores del Derecho y de sus colaboradores directos: los peritos. Muchos de estos fracasos probatorios tienen su origen en la falta de formación profesional de los abogados, en lo referido a las disciplinas criminalísticas. Es curioso y preocupante que la mayoría de los planes universitarios vigentes no contemplen la materia Criminalística en su currícula académica. Incluso, la materia Criminología suele ser optativa, por lo que se da el absurdo conceptual de que el abogado recién egresado confunde ambos términos: Criminalística y Criminología, debiendo recurrir a la experiencia de sus colegas para actuar en aquellos casos en que requiere de la acción pericial probatoria.

Esta es la razón principal de ser del presente capítulo. Tomemos como punto de partida la lectura de los siguientes fallos jurisprudenciales:

1. "El fallo de la Sala VI de la Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Capital Federal, en autos 'C., N. s/nulidad' (causa 40.856) rta. 24/2/2011, donde la Sala declara la nulidad de un registro domiciliario, del secuestro de los elementos hallados en el patio de dicha finca y de la declaración testimonial en la cual una madre involuntariamente incrimina a su hijo, el cual, a su vez, es sobreseído por la Sala al no existir un cauce independiente de investigación. Respecto de su consorte de causa, no se adopta un criterio desvinculante por ser distinta su situación procesal. Precisan los magistrados que el caso en estudio presenta una característica particular porque la ocupante del inmueble prestó el consentimiento de su registro sin saber que con su acción facultaba la recolección de elementos de prueba incriminantes en relación a su hijo, al que no imaginó siquiera vinculado a un episodio delictivo. Asimismo, destacan que el inciso 3ro. del artículo 227 CPC autoriza la práctica de un registro domiciliario sin orden judicial cuando la policía persigue a algún imputado para su aprehensión, pero que tal excepción no se verificó en el caso. Agregan que el consentimiento del

morador debe ser expresado de manera que no queden dudas en cuanto a la plena libertad del individuo al formular la autorización. Así, al carecer de efectos el allanamiento realizado, pierde también virtualidad el secuestro de la campera hallada en el patio de la finca (consecuencia directa y necesaria) que el imputado utilizara al momento del hecho. Resolución: '...el Tribunal RESUELVE: I.Declarar la nulidad del registro domiciliario practicado en la vivienda de la calle '(...)' de esta ciudad y del secuestro de los elementos hallados en el patio de la citada finca. II.Declarar la nulidad de la declaración testimonial de fs.10 en cuanto incrimina a G. A. F. y de todo lo actuado en su consecuencia y a su respecto. III.Disponer el sobreseimiento de G. A. F. (art. 336, inc. 4° del Código Procesal Penal de la Nación), dejándose constancia que la formación del sumario no afecta el buen nombre y honor del que hubiera gozado con anterioridad. IV.No hacer lugar a la solicitud de sobreseimiento respecto de C. N. C. Devuélvase a primera instancia en donde deberán practicarse las notificaciones pertinentes y sirva lo proveído de atenta nota de envío. Julio Marcelo Lucini Mario. Filozof. Ante mí: Cinthia Oberlander Secretaria de Cámara'".

2. Causa 39.779 -"G. R. y otro s/procesamientos"Interlocutoria Sala 6ª. Juzgado de Instrucción 2. "Que no se hayan verificado, en el caso, todos los pasos del procedimiento del 'phishing' como alega especialmente la asistencia técnica de G. o que no se haya determinado de qué computadora se realizó las transferencias, no altera de momento los graves indicios cargosos. Julio Marcelo Lucini Mario Filozof. Ante mí: Carlos E. G. Williams Secretario Letrado de Corte".

3. Cám. 1ª Civ. y Com. Bahía Blanca "Microsoft Corporation c/Cooperativa Agraria Ts. As. s/medidas preliminares". Jurisdicción: Buenos Aires. "Corresponde declarar la nulidad de la diligencia preliminar ordenada, toda vez que no se citó a la otra parte, impidiéndole controlar adecuadamente la prueba, ni tampoco se dio intervención al defensor oficial, en clara violación del último párrafo del artículo 327 del Código Procesal Civil y Comercial de la Nación y del derecho de defensa de garantía constitucional (art. 18, CN). Bahía Blanca, 21 de diciembre de 2010. Peralta Mariscal Pilotti. Ante mí: Vera (Diligencias preliminares. Prueba anticipada. Nulidad)".

Los referidos fallos, aparentemente independientes, y sin relación entre sí, guardan las siguientes similitudes:

· En el caso del apartado 1, un error procesal por parte del personal interventor provoca la pérdida de la prueba, que hubiera resultado decisoria para la evaluación de los hechos y la correspondiente sentencia judicial.

· En el caso del apartado 2, el resultado de un informe pericial es considerado en el momento de tomar sentencia, pero no define la cuestión,

específicamente porque aunque no se ha establecido la computadora desde donde se efectuó la presunta acción delictiva, el resto de los indicios probatorios es suficiente para que el Tribunal adjudique una posible autoría material.

· En el caso del apartado 3, las fallas formales en la recolección de la prueba indiciaria informático forense, como medidas preliminares y particularmente sin tomar los requisitos legales que son de rigor en este tipo de prueba, obtenida rutinariamente in audita altera pars, provocan su anulación.

Podemos inferir que el problema mostrado en el apartado 1 está referido a defectos formales, los que podrían ser asignados a la falta de capacitación legal del personal interviniente; en el segundo caso, al permanente choque cultural que la informática provoca en la sociedad y que impide que ciertas analogías, que surgen de manera consciente o subconsciente en el ánimo de quien debe decidir, se correspondan con la realidad; y en el tercero, a errores en quien solicita la medida y falta de asesoramiento por parte del profesional que la lleva a cabo (más allá del acuerdo tácito o explícito del a quo).

¿Poseen los peritos formación suficiente en la gestión de la prueba indiciaria que deben recolectar? La respuesta es ambigua: En razón de la particular característica que la prueba indiciaria representa, en la cual cualquier persona que sea "experta" en un área científica o arte determinado (sea lo que fuere que esto signifique e indistintamente del mecanismo de selección), puede modificar, adulterar o fabricar la prueba necesaria para delinquir impunemente desde el punto de vista pericial. Entre una multitud de posibilidades queremos destacar:

· El perito es egresado de un instituto universitario dependiente de una fuerza de seguridad (por ejemplo, el IUPFA). En este caso, en su currícula contará con una materia específica relacionada con el Derecho procesal y la gestión de la prueba pericial. Debería estar capacitado para asesorar al letrado ante una circunstancia como la descripta en el apartado tercero.

· El perito es miembro de una fuerza de seguridad, egresado como oficial del escalafón de peritos y actúa como tal. En este caso, su formación particular no difiere de la de otros oficiales y escalafones (seguridad, comunicaciones, etc.), por lo que podría incurrir en errores similares a los que obran en el apartado primero.

· El perito es egresado de una universidad no dependiente de fuerzas de seguridad. En este caso, al igual que lo expresado respecto del abogado novel, todo depende de la currícula de la carrera. Es necesario analizar cada caso en particular.

· El perito no ha realizado carrera específica alguna (típica situación en la inspección mecánica de automotores, realizada en algunas jurisdicciones por

un mecánico de la zona o, en el mejor de los casos, por un especialista enviado por la compañía de seguros), y participa de la labor pericial en forma no habitual, esporádica o excepcional. Nada podemos exigir a este tipo de experto ad hoc.

Ante esta situación de hecho, intentaremos analizar la problemática, a partir de dos ejes principales discursivamente integrados:

· Lo que es dable esperar de la tarea pericial: La acción esperada y pretendida del operador del Derecho respecto del perito considerado, en particular del consultor técnico (con otros matices, en el caso del perito oficial y su homólogo de oficio).

· La relación operador del Derecho perito: La relación interdisciplinaria y transdisciplinaria que une al operador del Derecho y al perito, para llevar a buen término la recolección de la prueba indiciaria requerida, su resguardo, protección, certificación, traslado, entrega formal y posterior revisión mediante una prueba pericial.

Lo que se espera

El abogado (en especial, el profesional novel) supone que el perito tendrá suficientes conocimientos y experiencia como para decidir por sí mismo el tipo, cantidad y calidad de la prueba a recolectar. De ahí la aparición de puntos periciales como: "Y toda otra actividad técnico pericial que estime necesaria para la resolución de los interrogantes planteados". Aunque esta frase parece clara, sencilla y determinante, en realidad solo contribuye a modificar el rol original del perito referido. En efecto, el Código Procesal Civil y Comercial de la Nación declara:

"Sección 6° – Prueba de peritos. Procedencia, art. 457. – Será admisible la prueba pericial cuando la apreciación de los hechos controvertidos requiere conocimientos especiales en alguna ciencia, arte, industria o actividad técnica especializada".

Por su parte, el Código Procesal Penal de la Nación, se expresa en términos similares:

"Capítulo V – Peritos. Facultad de ordenar las pericias, art. 253. – El juez podrá ordenar pericias siempre que para conocer o apreciar algún hecho o circunstancia pertinente a la causa, sean necesarios o convenientes conocimientos especiales en alguna ciencia, arte o técnica".

Como podemos ver, el rol del perito no es nada más y nada menos que el de un testigo experto, de ahí su enorme diversidad cualitativa. Queda claro que el perito no es:

· Un investigador privado con facultades propias.

· Un sustituto del juez.

Esto parecería una obviedad, sin embargo, el perito muchas veces, en su afán de colaborar con la ley[51], sobreactúa. La Criminalística, disciplina integradora de las tareas periciales, se define:

1. *Por el Director de Investigaciones de la Policía Federal Argentina, Inspector General Roberto Albarracín, en su obra Manual de Criminalística, de la Editorial Policial, Buenos Aires, 1969, como: "La materia que encierra el estudio de las técnicas del crimen".*

2. *Más recientemente, por el eminente peruano Dr. Pablo A. Rodríguez Regalado, Doctor en Ciencias Forenses y Criminalística, como: "La Criminalística, como sabemos, es aquella parte del conocimiento humano que se hace cargo del estudio o también, digamos, del procesamiento de los rastros, indicios o evidencias que resultan de la comisión de un hecho particular, con el objeto de lograr la información que estos nos provean para un esclarecimiento o identificación de lo ocurrido –no me estoy refiriendo en especial a procesos penales, puesto que también la Criminalística aporta al conocimiento y generación de la prueba en los procesos civiles y administrativos–, ciencia que, como es lógico, se constituye en una herramienta de provecho a la humanidad, como lo son todas las demás ya conocidas, como la Sociología, la Antropología, la Lógica, la Biología, la Química, la Medicina, etc."* [52].

Esta disciplina se manifiesta por medio de algunas características propias que le otorgan entidad técnica independiente, entre ellas:

1. Se basa en consideraciones científicas, tecnológicas y técnicas.

2. Se implementa mediante métodos de análisis de la prueba indiciaria propios de cada disciplina criminalística.

3. En casi todos los casos, esos métodos se concretan por medio de comparaciones[53]. Simplemente, el perito debe limitarse a comparar, cotejar, registrar resultados y luego volcarlos en un informe que se entregará como elemento de apoyo a la decisión del juez que lo requiere.

El grado máximo de participación, en modo de opinión del perito, se produce en el momento de modelar la reconstrucción del hecho. Ocurra en el lugar del hecho real o en el lugar del hecho virtual (propio e impropio) que ya hemos tratado en el manual anterior. Aquí se ve obligado a realizar suposiciones soportadas por la prueba cotejada, por ejemplo, posición probable del tirador, distancia de disparo, mecanismo de transacciones que conformaron la acción delictiva que finaliza en una defraudación internacional mediante herramientas informáticas (delito informático propio o impropio) y muchos otros supuestos.

Pero el perito nunca puede determinar autoría. La determinación de autoría (o la falta de ella) es una atribución exclusiva e irrenunciable del juez.

Esta circunstancia es ignorada de hecho por algunos operadores del Derecho. Sin embargo, su correcta interpretación le facilitará la impugnación de muchos informes periciales que adolecen de estos defectos. La siguiente tabla simplificará la comprensión de lo afirmado:

Afirmación correcta	Versión detectivesca	Versión sustitutiva del juez
La posición probable del tirador es… (se adjunta gráfico demostrativo).	El tirador ingresó al lugar, discutió con la víctima y luego le disparó desde… (se adjunta gráfico demostrativo).	El imputado disparó desde la posición… (se adjunta gráfico demostrativo).
El calco digital peritado guarda correspondencia total con su homólogo obrante en la ficha decadactilar de NN (RENAPER).	El asesino ingresó al lugar, se apoyó en la mesa del estudio y dejó su huella dactilar en el jarrón peritado. Esta huella corresponde de manera categórica al titular de la ficha dactilar NN (RENAPER).	El procesado ingresó al estudio y dejó su huella dactilar en el jarrón peritado. Este calco guarda correspondencia total con su homólogo en la ficha decadactilar de NN (RENAPER).
El texto mecanografiado y el cuerpo de escritura ofrecido por la demandada muestran coincidencias que señalan de manera categórica que han sido efectuados por la misma máquina de escribir mecánica.	La máquina de escribir secuestrada en el consultorio del prevenido fue empleada para realizar la carta que indujo a la defraudación acaecida.	El prevenido realizó la carta utilizada para consumar la defraudación investigada.
El mensaje de correo electrónico analizado fue enviado desde la dirección IP … (se recomienda su confirmación mediante prueba de informes al ISP que presta el correspondiente servicio de correo electrónico).	El mensaje de correo electrónico, utilizado para amenazar a la víctima, fue enviado desde la computadora del procesado.	El mensaje electrónico utilizado para amenazar a la víctima fue realizado por el procesado.

Aunque los casos anteriores suenen inverosímiles, se debe recordar que están fuera de contexto y que muchas veces aparecen disimulados entre la

argumentación esgrimida por el experto que realiza el examen pericial.

Como ejemplo, podemos referir el caso de la identificación del autor de un mensaje de correo electrónico. Hace muchos años, cuando la tecnología era otra y las comunicaciones también, en lo referido a las máquinas de escribir mecánicas era bastante sencillo determinar la marca (paso mecánico y tipografía). Un poco más complejo era establecer correspondencia entre un texto de relativa longitud (digamos una carilla) y la máquina con que se confeccionó.

Y mucho, pero mucho más difícil, establecer la identidad del dactilógrafo. Existía, no obstante, una técnica (probabilística, no categórica) para identificar al autor de un texto mecanografiado. Entre otras características, se determinaba el presionado de los tipos sobre el soporte, que en casi todos los casos era papel (si el escritor era dactilógrafo, la fuerza del presionado era variada, en razón de que los dedos meñiques tienen menos fuerza que los índices al presionar las teclas, lo que se evidenciaba por un menor entintado sobre el papel, en tanto que los que escribían con "dos dedos" mostraban un entintado más homogéneo) y otras propias de la llamada identidad mecanográfica del autor (errores al escribir a máquina, de ortografía y dicción, lugares comunes, diversas particularidades reiteradas en los textos analizados). A veces, con mucha suerte se lograba establecer cierta correspondencia entre el presunto autor del texto y su obra mecanografiada. Pero siempre en carácter de probabilidad y sujeto a confirmación mediante otros medios probatorios. Y, nunca determinando la autoría de un falsario, particularmente porque el falsario intenta desprenderse de su personalidad gráfica (en el caso de los manuscritos[54]) o mecanográfica (en los escritos realizados con máquinas de escribir mecánicas) y asumir la del imitado.

Por supuesto, con el surgimiento de las máquinas electromecánicas con sistemas de impresión independientes del cuerpo del instrumento (bochita, margarita), el tema del entintado dejó de ser útil, al igual que en las actuales impresoras de matriz de puntos, chorro de tinta o láser, que usamos a diario en nuestras oficinas (la máquina de escribir mecánica es prácticamente una pieza de museo).

Hace muy poco recibí un artículo acerca de una técnica denominada White Print: "Su método se basa en la búsqueda e identificación de patrones frecuentes, una combinación de características de estilo, gramática y ortografía que se repiten en los correos electrónicos de un sospechoso. De acuerdo con …, esta información es suficiente para determinar la edad, género, nacionalidad y educación de una persona". Se pretendía, mediante esta técnica, establecer la identidad del autor de un mensaje de correo electrónico. Supongamos por un momento que la decisión recayó luego de analizar los

miembros de una familia, con acceso a la computadora secuestrada, en un determinado hogar y que se estableció que el autor era el hijo menor de la familia (integrada por los padres, ambos profesionales y el hijo preadolescente). Este parecería ser un caso con visos de solución categórica.

Recordemos que la Criminalística es una ciencia de cotejos, comparaciones, soporte científico, tecnológico y técnico y que las disciplinas dependientes de ella, como ser la Documentología, también deben cumplir estos requisitos. En Derecho, es común escuchar la frase "el que puede lo más puede lo menos", y en este caso es de aplicación directa. Dudosamente, el hijo preadolescente pueda imitar la escritura de la madre (aunque pensándolo bien, algunas veces falsifiqué la firma de mi padre en el informe de calificaciones semanal que me entregaban en la escuela primaria, hecho que nunca fue detectado; claro que no se lo sometió al control pericial, pero igual la acción resultó impune) o del padre. Sin embargo, la consideración anterior no es extensiva al padre, este sí puede imitar el lenguaje de su hijo, con soltura. En especial, considerando que el mensaje se envía por medio de una computadora, cuyos caracteres son iguales en todos los casos y cuyo autor no está a la vista del destinatario. ¿Estamos seguros de que el contrato de compraventa internacional por un tambor de jugo de arándanos, que celebramos con un interlocutor europeo, está siendo realizado por la persona con quien pretendemos contratar? (salvo que contemos con mecanismos de firma digital que por experiencia considero sumamente raros que se utilicen efectivamente en este tipo de intercambios) ¿Es posible que en realidad estemos tratando con su secretaria? ¿O con un empleado cualquiera de la empresa?

¿O con una entidad virtual que representa a una persona física? ¿O con una entidad virtual que no tiene correspondencia con ninguna persona física? Esto puede repetirse en el tiempo y tal vez nunca tengamos idea cabal de si estamos tratando con una misma o varias personas físicas y tampoco si dichas personas físicas (de existir) son determinables (por ejemplo, los mecanismos de adquisición de libros, en el más conocido y utilizado de los sitios web actuales, son automáticos y prácticamente realizan toda la operación [pedido, adquisición, cobro, envío y seguimiento del producto] sin supervisión ni participación humana alguna).

Esto se hace evidente ante la acción de determinados sujetos que, con fines delictivos, ingresan a las páginas de los adolescentes o niños para seducirlos de manera virtual, lograr una cita (casi siempre, pero no estrictamente, sin conocimiento de sus padres) y realizar sus fines delictivos[55].

La comparación entre la identificación del autor de un manuscrito, que ya en su oportunidad mostraba un aspecto probabilístico, nada tiene que ver con la identificación del autor de un mensaje de correo electrónico. Un operador con

mínima formación en paquetes de oficina puede imitar correctamente la forma de escribir de otra persona, limitándose a cortar oraciones completas y reensamblarlas en un documento nuevo. Recordemos que en Informática forense no se cumple el principio de identidad criminalístico "todo objeto es idéntico a sí mismo y diferente de los demás", lo que permite distinguir entre original y copia, factibilizando el cotejo pericial[56]. Por lo tanto, un carácter (letra, número, etc.) es idéntico a otro y las frases en realidad han sido escritas por el autor del texto reordenado. Pensemos en los viejos métodos extorsivos, consistentes en recortar y pegar palabras de un periódico, el mensaje de correo electrónico puede ser conformado de la misma manera, pero con la ventaja adicional de que las frases recortadas han sido efectivamente escritas por aquel que se pretende imitar. ¿Cómo entonces podríamos distinguir al falsario, si en realidad el texto lo escribió el imitado?

Las obras de Borges están disponibles en formato digital (de manera legal y legítima o no, pero disponibles en la red). Un falsario podría tomar dichos textos, cortar una frase aquí y otra allá, reorganizarlas en una estructura literaria similar a la del referido autor y construir un nuevo cuento atribuible a Borges: "El cuento perdido de Jorge Luis". ¿Alguien podría determinar su falsedad?

¿Es realmente falso? ¿Acaso dichas frases no fueron escritas por nuestro desaparecido gigante literario? ¿Quién se atrevería a afirmar que es falso? ¿Con qué sustento científico o metodológico? Aunque eventualmente lograse relacionar las frases con otros escritos anteriores, ¿constituiría dicha relación una anomalía literaria? Seguramente, las frases utilizadas por los autores en esta obra ya han sido empleadas anteriormente en otros contextos y circunstancias (los autores tendemos a repetirnos ad infinitum). De ahí que pretender identificar al autor de un escrito analizando el texto es solo una utopía que no se puede sostener científica, metodológica, ni técnicamente.

Tal vez, y esto es solo una expresión de deseo, sea posible determinar la falsedad de un escrito, pero hasta este tema es dudoso, ya que ¿quién conoce mejor la forma de escribir de un autor que el mismo autor? Por lo tanto, ¿quién está más capacitado para hacerla aparecer como falsa a los ojos de un tercero? Por ejemplo, la siguiente frase: "Che, deja de ortibar y pasame el brillo, manya lo que te digo, el que no carpetea el lunfa tumbero, se queda de araca", ¿es una copia de un texto externo a esta obra? ¿Ha sido realizada por alguno de los autores? De ser así, ¿a cuál de ellos? El accionar pericial debe limitarse al ámbito de lo probable (todo lo probable debe ser posible, lo inverso no es real). Imaginen que la encuentran fuera de este contexto y que deben compararla con el resto del texto que nos ocupa para establecer su autoría.

síntesis

No todo lo concebible es posible y mucho menos probable, en especial en materia pericial. Es evidente que el perito debe limitarse a su función de testigo experto y evitar los roles detectivescos o la sustitución del juez como responsable de determinar autoría.

La interacción operador del Derecho perito: A partir del análisis anterior, podemos vislumbrar la necesidad de interacción mutua entre los actores de la tarea pericial, expresada por el perito en su actuar profesional, tendiente a cumplir el rol que estrictamente le fija la ley, y por parte del operador del Derecho, una condición de control estricta, cuya falta puede llevar a errores procesales insalvables.

Al respecto, es necesario (aunque no suficiente) tener en cuenta que las conclusiones periciales deben estar soportadas por demostraciones:

1. Científicamente consistentes.
2. Tecnológicamente adecuadas.
3. Técnicamente demostradas:
   a. Análisis físico-químicos que aporten resultados categóricos y repetibles (fuera del índice de error absoluto y con el mínimo error relativo).
   b. Metodológicamente analizados (metodología criminalística).
   c. Lógicamente demostrados (argumentación pericial silogísticamente sustentada).
4. Desarrolladas en una estructura demostrativa propia sin errores procesales.

En cuanto a la credibilidad de los resultados periciales, depende de la relación entre el resultado y la ciencia que le brinda soporte. No tienen la misma contundencia demostrativa la identificación positiva de una muestra de ADN, dos calcos dactilares, dos proyectiles, dos vainas servidas, dos textos mecanografiados, dos textos manuscritos, dos firmas[57], dos perfiles psicológicos o dos análisis grafológicos, por mostrar solo algunas de las situaciones más frecuentes.

El ADN constituye la identidad genética del individuo considerado y si este está disponible es revisable las veces que sea necesario. Algo similar ocurre con las huellas dactilares que gozan de los principios de diversidad (variedad), inmutabilidad y perennidad[58] que aseguran una identificación humana confiable (de hecho, nuestros sistemas de identificación se han basado en estos principios durante más de un siglo)[59], otros métodos también pueden ser útiles, pero su grado de certeza es menor[60]. En cambio, establecer si un mensaje de correo electrónico (parco, resumido, apenas comprensible, utilizando el slang (argot, lunfardo) de moda entre su grupo de pertenencia ha

sido realizado por el precitado adolescente o por un falsario, es un tema sumamente opinable, aun entre los expertos en grafología. De ahí que el operador del Derecho que solicita la prueba pericial debe ajustarse a estas circunstancias. Una cosa es una prueba de paternidad por medio de un examen de ADN y otra muy distinta establecer la autoría de un mensaje anónimo (sobre cualquier soporte que se encuentre).

Como ejemplo de lo afirmado, aprovecharé una anécdota que me ocurrió durante el cursado de la materia Estructuras Argumentales, en el marco del Doctorado en Derecho de la UBA, dictada por el Dr. Ricardo Guibourg. Era necesario realizar un trabajo práctico y defenderlo durante la evaluación final. Para cumplir el requisito académico y ante la siempre recurrente discusión sobre la inveterada costumbre de algunos profesionales, consistente en agregar a su apellido el título de Doctor, que se afirmaba estaba autorizada por una supuesta acordada de la CSJN (la que por cierto nunca apareció efectivamente), concebí la idea de fabricar la referida acordada, atribuirla al insigne Sebastián Soler, fecharla de manera adecuada y distribuirla entre los demás asistentes a la materia doctoral (todos ellos avezados juristas de antigua data, ya que el único ingeniero integrante de la clase era quien escribe).

Realizada la tarea y distribuida entre los asistentes a la materia (unos treinta cursantes), esta fue aceptada por la totalidad de los destinatarios, analizada como si fuera verdadera (aunque era un disparate jurídico), revisada por dos informáticos que actuaban para los estudios profesionales de los referidos abogados (expertos en seguridad informática, no en Informática forense) y dada por válida. Por supuesto, con las permanentes alusiones al tema (“viste G. que la acordada existía y nada menos que de Soler”), durante todo el desarrollo del curso[61].

La falsificación me resultó muy útil, porque al aclararse las cosas, en oportunidad del examen final, me aportó una excelente nota, pero esta experiencia propia me lleva a ser muy cuidadoso a la hora de brindar una conclusión categórica.

¿Qué método utilicé para concretar la falsificación? El más sencillo y al alcance de todos, reuní un conjunto de documentos originales del prestigioso autor, luego me limité a cortar y pegar sus escritos, con lo cual no tuve necesidad alguna de imitar su increíble cultura legal y su capacidad argumental, y luego le di el formato y las condiciones necesarias para aparentar autenticidad informática. Complementariamente al informe del Procurador General de la Nación (el referido e ilustre Sebastián Soler) agregué la acordada, fundada en quince artículos, el primero de ellos una forma típica de falacia formal y los restantes, un ejemplo individual de las conocidas falacias no formales. Esto pasó totalmente desapercibido ante un público

acostumbrado a la lectura legislativa y jurisprudencial.

¿Qué enseñanza nos puede dejar esta sencilla anécdota?

· Que cada uno ve en primer lugar lo que quiere ver y acomoda los resultados a sus intereses particulares.

· Que no es bueno afirmar hechos sin tener los elementos probatorios necesarios para justificar la tarea.

· Que los elementos probatorios deben ser confiables (auténticos y comprobables).

· Que aunque un texto aparente ser de autoría de un determinado escritor, no debemos considerarlo auténtico hasta que no lo hayamos comprobado efectivamente, mediante un conjunto de pruebas interrelacionadas (en especial, respecto de las frecuentes referencias y afirmaciones que se efectúan en una audiencia oral y cuyo registro fílmico y/o auditivo puede ser editado y modificado por cualquier falsario con un mínimo de entrenamiento informático).

· Que al parecer no existe tal acordada.

Un objeto material o ideal, desde el más puro sentido común, puede ser a la vez especie de un género y género de otro (los vegetales respecto de los seres vivos y de la zanahoria), pero también pueden ser especie subordinada y dependiente de diversos géneros. A esto hay que agregarle la característica transdisciplinaria de disciplinas como la Química forense y la Informática forense, considerando:

· La Química forense es una especie del género Química (palabra química y sus connotaciones directas).

· La Química forense es una especie del género Criminalística (palabra forense y sus connotaciones directas).

· La Química forense es una especie del género Legal (no aparece en su nombre, pero sí en su naturaleza de ciencia auxiliar de la ley).

¿Cuál de las afirmaciones anteriores es verdadera y cuáles falsas?

La respuesta es: son todas verdaderas, simplemente porque es una disciplina transdisciplinaria, que se nutre de la Química, la Criminalística y la ley, para conformar su propio carácter transdisciplinario. Y digo transdisciplinario y no interdisciplinario porque si representáramos este problema con diagramas de Venn, ocuparía el área de intersección de las disciplinas Química, Criminalística y Legal, mientras que su interdisciplinariedad sería una relación entre diagramas que no se intersectan (tal vez, un producto cartesiano u otra relación similar).

Con la Informática forense pasa algo similar, es un corte transdisciplinario que integra la Informática (en particular a la Seguridad Informática), la

Criminalística y la ley vigente. Podríamos discutir si el nombre está bien o mal puesto, podría llamarse con más propiedad Informática criminalística (o viceversa), aunque tal vez llevara a la confusión de su independencia como disciplina, ya que se la podría confundir con una aplicación ofimática que apoya a la Criminalística (paquetes de oficina).

La Informática forense requiere de una nueva forma de concebir a la Criminalística y a su objeto de estudio, la prueba indiciaria informático forense. Aparecen condiciones particulares que es imprescindible destacar:

1. Se rompe, como dijimos, con el principio científico, lógico y criminalístico de identidad, ya tratado en este capítulo.
2. El lugar del hecho real se amplía, agregándose el concepto de lugar del hecho virtual.

Algo así como el lugar del hecho en el ciberespacio pero sin la connotación esotérica que suele acompañar a este vocablo, se trata del lugar del hecho ubicado y representado por los bits que lo componen. Que por cierto no tienen carácter mágico, sino que están almacenados en forma de electrones, orientaciones magnéticas de elementos magnetosensibles, fotones, modificaciones de índices de reflexión y refracción lumínicos, cadenas de ADN o de proteínas. Es decir, componentes físicos tan tangibles y mensurables como cualquier otro que sea objeto de análisis pericial. Claro, el lugar del hecho virtual no podía ser una excepción y se divide en dos subespecies:

a. El lugar del hecho virtual impropio: Consistente en la representación mediante herramientas informáticas (simulaciones que integran técnicas de realidad virtual, redes neuronales de datos e inteligencia artificial). Es útil para modelar lo que pudo haber ocurrido y, en particular, permite la interacción simultánea o sucesiva de todos los actores que participan del tema investigado. El juez no necesita establecer un momento para la inspección judicial, menos aún para el reconocimiento del lugar del hecho; si puede confiar en los expertos y su tecnología, podrá disponer de la información en su despacho, e intercambiar datos con quienes desee, llegando a conformar auténticas audiencias virtuales (por teleconferencia, con mensajes cifrados y firma digital incluidos). Es solo aplicar los mecanismos de uso diario en telemedicina (robots que operan a distancia y consultas de igual tenor entre profesionales físicamente situados en las antípodas) o en entrenamientos técnicos específicos (simuladores de vuelo, de navegación, de cirugía, etc.)[62].

b. El lugar del hecho virtual propio: En general, estamos en presencia de Delitos Informáticos Propios[63]. La informática simula lo que realmente ocurre cuando un falsario, desde Buenos Aires, sustrae la clave de una cuenta radicada en Suiza, utilizando un método de ataque por “fuerza bruta”, apoyado con máquinas distribuidas globalmente, para transferir fondos, sobre una

cuenta corriente en las Islas Caimán y cobrar los fondos en Uruguay. Aquí la determinación del lugar del hecho real (clásico) es prácticamente imposible. Salvo que asumamos la entidad del ciberespacio como algo más que una característica indeterminable, definida únicamente por la realidad virtual.

c. La participación interactiva de entidades virtuales, que pueden corresponderse o no con personas físicas existentes en el mundo real. Relaciones del tipo: personalidad virtual vs. personalidad física en entornos reales o virtuales y sus combinaciones posibles, incluyendo y utilizando bienes virtuales susceptibles de valoración económica (armas, construcciones, equipos y hasta personajes de existencia puramente virtual en la respectiva comunidad digital considerada, esto incluye a los casinos digitales, sus contratos, obligaciones y consecuencias jurídicas ante el incumplimiento de estas, tema que como dijimos aún se encuentra en vías de discusión doctrinaria), que no son asimilables al concepto de cosa, establecido por el Código Civil[64]. No son objetos materiales, no es energía, no son fuerzas naturales, solo existen en el mundo virtual considerado. Son solo representaciones virtuales de objetos de existencia real posible o no; por ejemplo, se puede comprar en Internet un aliado virtual, para integrarlo a un juego de rol, pagando con dinero en efectivo o mediante una transacción electrónica que lo representa y esta mascota puede ser, por ejemplo, un hipogrifo, un dragón, un fauno, una mantícora o cualquier otra forma imposible de encontrar en la naturaleza, pero que sin embargo ha sido tasada y vendida, como si fuera un objeto material factible de comercialización. Esta mantícora ha sido valuada y vendida, por lo tanto es un bien. ¿Forma parte del patrimonio de la persona que lo adquirió? ¿Del patrimonio de la persona real o del patrimonio del personaje que solo existe en la comunidad virtual referida? De ser así, ¿qué significado tiene la venta del personaje, con todos sus atributos y pertenencias, en una subasta por Internet?[65]. ¿Qué ocurre si uno de los compra-vendedores virtuales no cumple con su obligación (obligación de entregar dinero en el mundo real, no en la ficción)? ¿Ante quién se presenta la demanda? ¿Es susceptible de compensación por daños y/u oportunidad perdida dentro del juego (recordemos que puede ser un juego de azar asegurado por un casino virtual, con su correspondiente autorización nacional o provincial para funcionar como tal)?

3. Es por esa sencilla razón que, sin pretender autoridad alguna, proponemos una nueva definición de Criminalística, que resulte abarcativa de estas circunstancias:

a. Criminalística: Es la metodología integradora multidisciplinaria que provee la información tendiente al esclarecimiento del hecho, a partir de los indicios recolectados (prueba indiciaria).

b. Prueba indiciaria: Es la prueba integrada por el conjunto de elementos físicos y virtuales que obran en un lugar determinado, necesarios y suficientes para efectuar una reconstrucción lógica, científica, tecnológica y técnica de los hechos investigados, por medio del correspondiente análisis pericial forense.

En este marco, resulta interesante analizar las diferentes combinaciones que se producen entre los escenarios posibles, los actores y sus acciones:

1. Lugar del hecho real + actor real + acción típica, antijurídica y culpable = delito clásico (Código Penal). Ejemplo: robo de una PC o un celular.

2. Lugar del hecho virtual + actor real + acción típica, antijurídica y culpable = delito informático impropio (ley 26.388). Ejemplo: sustracción de dinero de un cajero automático, utilizando una tarjeta robada y la clave obtenida a partir de la intercepción de los mensajes digitales intercambiados por el propietario de la tarjeta con su entidad bancaria.

3. Lugar del hecho virtual impropio + actor real + acción típica, antijurídica y culpable = delito clásico (Código Penal + ley 26.388). Ejemplo: secuestros virtuales.

4. Lugar del hecho virtual propio + actor real + acción típica, antijurídica y culpable = delito informático propio (Código Penal + leyes específicas). Ejemplo: empleo de claves falsificadas o generadores de claves apócrifas para obtener licencias apócrifas de aplicaciones disponibles en la red.

5. Lugar del hecho virtual impropio + actor virtual + actor real = simulación. Ejemplo: apoyo informático al Derecho, la Criminalística o la Informática forense. Puede utilizarse como instrumento delictivo (Ingeniería social e Ingeniería social inversa).

6. Lugar del hecho virtual propio + actor virtual + actor real = delitos informáticos propios.

No tipificados en las normas. Ejemplo: robo de identidad, phishing, etc.

7. Lugar del hecho virtual propio + actor virtual = ¿? Ejemplos: a) los ya referidos contratos en entornos virtuales, susceptibles de valoración económica, pero sin relación con elementos existentes en la realidad; b) las personalidades virtuales múltiples, asociables o no con una persona de existencia física o jurídica (los llamados perfiles) susceptibles de adquirir derechos y contraer obligaciones, tanto en la comunidad virtual como en el mundo real (sustitución de identidad, creación de identidad virtual independiente, etc.).

En todos los casos descriptos, la Informática forense puede actuar, ya sea gestionando la prueba documental informática relacionada con el tema investigado, provocando la prueba de informes que la convalide y/o ratificando los resultados obtenidos mediante prueba pericial informático

forense.

Si los asertos anteriores son considerados válidos, entonces solo podemos resumir lo expresado diciendo que: La ciencia, la tecnología y la técnica modernas, integradas por una estructura lógica demostrativa estricta y una metodología criminalística precisa y minuciosa, tienen serias probabilidades de actuar de manera efectiva, eficiente y eficaz en la reconstrucción de los hechos acaecidos en una determinada locación espacio temporal. Está claro que la gestión de la prueba documental informática y su comprobación pericial son tareas multidisciplinarias, algo que los operadores del Derecho están acostumbrados a utilizar. También es una tarea interdisciplinaria ya que requiere colaboraciones y aportes provenientes de diferentes áreas del saber. Pero, en particular, es una tarea transdisciplinaria, porque las conclusiones periciales no pueden ser extraídas de forma adecuada (so pena de ser referidas absolutamente fuera de contexto) si no integran las fases informática, criminalística y legal, aunando sus participaciones en un proceso integral. Distinguidos operadores del Derecho y estimados peritos en Informática forense: la única manera de enfrentar el futuro que ya nos deja atrás es trabajar en forma mancomunada y con objetivos comunes.

51 El perito es un auxiliar de la ley (Sistema Judicial imperante). No podría ser auxiliar de la Justicia, porque la Justicia es un bien intangible, controversial, ambiguo, vago y que depende de la particular concepción filosófica que posea quien lo analiza. Por el contrario, el orden jurídico, su implementación práctica mediante un sistema jurídico, que se hace real en el sistema judicial, es expresado en nuestro país, mediante un sistema normativo codificado en forma de leyes y de raigambre constitucional. Con la implicancia que dicha forma de expresar la organización judicial tiene respecto de los derechos individuales de cada ciudadano, a partir del artículo 16, segundo párrafo de la Constitución Nacional, los Tratados Internacionales, referidos en el artículo 75, inciso 22 de la precitada Carta Magna y sus normas relacionadas.

52 Fuente: http://criminalisticaycienciasforenses.blogspot.com.

53 Es la disciplina de las comparaciones por excelencia: proyectil testigo vs. proyectil incriminado (ídem vainas); firma dubitada vs. firma indubitada; calco dactilar secuestrado vs. calco dactilar, obrante en la ficha decadactilar de NN; resultados de la prueba de alcoholemia vs. tabla de valor máximo de alcohol en sangre permitido para conducir; resultados de la prueba cromatográfica sobre la tinta dubitada vs. resultados de la misma prueba sobre la tinta obrante en el elemento escritor secuestrado; huellas de frenado en la calzada vs. tablas de huellas de frenado para el tipo de vehículo, y la situación considerada, fotografía digital obrante en la página web analizada vs. fotografía obrante en el disco rígido de la máquina sub peritia, etc.

54 En cuanto a la identificación de manuscritos, cuando un escritor imita la firma o la escritura de otro se desprende de su "personalidad gráfica" para intentar asumir la de aquel que se pretende imitar. Por supuesto, no logra plenamente su propósito, pero en general se queda "a medio camino". Por eso, se determina técnicamente la falsificación, pero no se puede determinar al falsario (me refiero a determinarlo por medios periciales, la prueba confesional o la de testigos, siempre puede hacerlo). Aunque no existe una denominación propia para la "cultura mecanográfica", lo que se estaba pretendiendo al identificar al autor del texto mecanografiado es precisamente eso, establecer una especie de "cultura mecanográfica". Es un buen intento, pero tiene el mismo problema, cuando imito, intento imitar esa cultura, puedo lograrlo a medias o un poco más, nunca por completo, pero seguro que abandono la propia. Esta salvedad es aplicable directamente al método que nos ocupa y cualquier operador del Derecho medianamente avezado con toda seguridad lo hará.

55 *Cuando un pedófilo se presenta en un sitio de chat de niños y se comunica con ellos, su "personalidad virtual" real se convierte en una personalidad virtual simulada. ¿Acaso no intenta imitar el lenguaje y las actitudes de sus posibles presas? En la naturaleza, el mejor predador ¿no es acaso el que mejor se oculta? (¿Para qué correr si me puedo acercar sin ser visto?). ¿Esto es un delito? Por supuesto que nos parece delictivo, sin embargo, cuando mentimos sobre nuestra edad en Facebook, o ponemos una foto nuestra pero de hace veinte años, ¿estamos cometiendo un delito? ¿Qué tan grave es la sustitución de identidad virtual, cuando afecta solo a los datos del propio falsario? Por ejemplo, cuando miente en su disponibilidad financiera, edad, profesión o cualquier otro dato, para acceder a una promoción ofrecida por una página web. Podría ocurrir que una madre simule ser su propio hijo para obtener un par de entradas de distribución gratuita de un concierto de rock y regalarlas luego al hijo de una amiga para que concurra con su novia. ¿Qué clase de infracción es esta? No parece ser un delito, en última instancia sería dudoso que un Juez condenara a la madre por esta acción, que podría eventualmente perjudicar los intereses de quien organiza el evento. En fin, ¿ante qué figura estamos? En informática no todo es posible, pero muchos de los imposibles físicos tienen solución en el campus virtual, entre ellos, la imitación por mecanismos de cortar y pegar.*

56 Principio de identidad impropio (de copias): Del original, ya que cuando se duplica un archivo informático, la copia no es igual a la original, sino idéntica (un bit no difiere de otro bit y entre sí son inidentificables unívocamente).

57 La firma es un caso especial en el análisis e identificación de manuscritos, ya que reúne características propias de este tipo de expresión escrita y otras típicas de la expresión gráfica del individuo. La firma en general se practica y se dibuja, antes de volverse un gesto espontáneo y rutinario, recordemos cuántas veces la practicamos y cómo ha evolucionado a lo largo de nuestra vida.

58 *Todos los sistemas dactiloscópicos se basan en tres principios fundamentales, que son: perennidad, inmutabilidad y diversidad. Algunos autores agregan otros como los de individualidad, especificidad, posibilidad y facilidad de clasificación.*

Perennidad: Son perennes porque las crestas del dibujo dactilar se forman a partir de la sexta semana de vida intrauterina y participan en el crecimiento de la persona hasta su muerte y su putrefacción o momificación. Inmutabilidad: Son inmutables porque los dibujos dactilares no varían en sus características individuales y porque no les afectan fenómenos patológicos, y en caso de desgaste voluntario su tejido epidérmico se regenera formando su dibujo con o sin solución de continuidad.

Diversidad: Son diversiformes por el sinnúmero de variaciones que evidencian las crestas papilares y por los puntos característicos que se distribuyen en particular en los dactilogramas haciéndolos individuales y no habiéndose encontrado hasta la fecha dos huellas iguales.

59 *Se hace evidente que en estos casos la conclusión puede ser efectivamente categórica: "El calco dactilar, relevado y revelado en el lugar del hecho... en relación son su homólogo obrante en la ficha decadactilar de NN, muestran las siguientes características identificatorias dactiloscópicas: mismo tipo fundamental, misma clasificación, misma subclasificación y 30 puntos característicos igualmente situados, orientados y dirigidos (según el sistema de clasificación de Vucetich y la obra de Rosset-Lago), por lo que podemos afirmar, que corresponden al mismo dedo, de la misma mano, de una sola y única persona: NN".*

60 Entre otros, el sistema antropométrico (retrato hablado de Bertillón) sumamente útil para describir las características faciales de una persona, otométrico de Frigerio, oftalmoscópico de Levinsohn, ocular de Capdevielle, craneográfico de Anfosso, dentario de Amoedo, radiográfico de Levinsohn.

61 Aunque parezca absurdo, esta anécdota es real y comprobable testimonialmente por todos los asistentes al curso, incluido su conductor académico (Guibourg, Ricardo, "La credulidad en el Derecho", Revista La Ley, Año LXXV Nº 122, del jueves 30 de junio de 2011, primera página, columna de opinión). ¿Cómo es posible que personas, *acostumbradas y entrenadas profesionalmente para lidiar con la normativa vigente olviden la más pura estructura piramidal de Kelsen? Considerando que la CSJN posee un poder relativo para dictar normas mediante acordadas limitadas al procedimiento (en general, administrativo) y no tiene capacidad de legislar (salvo el caso particular de la sentencia). ¿Qué abogado podría suponer que mediante una acordada la CSJN tiene potestad para modificar una ley de fondo de la Nación (artículo 247, segundo párrafo) y exceptuar de su cumplimiento a un grupo particular de la sociedad (en este caso, los abogados)? Por supuesto que a la hora de discutir la aplicación o no del precitado artículo a un caso en particular, mucha tinta ha corrido bajo el puente judicial, pero ese es otro tema, forma parte de la jurisprudencia y no de una implementación normativa de la Corte. Si puede hacer eso, ¿por qué no excluir a los camaristas de la aplicación del artículo 79 del CP? Se puede argumentar que son cosas distintas, sin embargo, tanto el artículo 79 como el 247 son normas vigentes en el Código Penal y quien las transgrede es un delincuente (en el segundo caso tal vez no un criminal, dependiendo de la concepción que tengamos respecto de este término, pero categóricamente un delincuente). ¿Por qué no excluir a un grupo determinado de la aplicación total del Código Penal, o el Civil, o el Comercial, o el de Minería, o eximirlos de pagar impuestos? Por último, si podemos generar un grupo especial de ciudadanos exceptuados de cumplimentar la ley vigente (destruyendo lisa y llanamente lo establecido en el artículo 16, segundo párrafo, de la CN), ¿por qué no utilizar ese mecanismo para modificar la Constitución? y como valor agregado nos evitamos tanta discusión parlamentaria en el momento de aplicar el sistema especial que permite su modificación. Todo esto es obvio y redundante, en especial para un abogado, pero recordemos que "no hay peor ciego que el que no quiere ver".*

Constitución de la Nación Argentina, Art. 16 (segundo párrafo). – "Todos sus habitantes son iguales ante la ley y admisibles en los empleos sin otra

condición que la idoneidad. La igualdad es la base del impuesto y de las cargas públicas".

62 Pensemos en las ventajas que podría aportar a la reconstrucción del hecho, la incorporación de exoesqueletos interactivos dinámicos, similares a los que se emplean en las fuerzas militares para la detección y transporte de explosivos o la inspección de edificios en el combate en localidades urbanas. Las posibilidades de empleo solo dependen del interés y la iniciativa de los operadores del Derecho, mancomunados con los expertos correspondientes.

63 *Delito Informático Impropio: Es aquel en el que se utilizan herramientas informáticas para cometer delitos comunes (tipificados históricamente en el Código Penal), por ejemplo, defraudaciones, estafas, extorsiones (en nuestro país están referidos en la ley 26.388, que si observamos atentamente se limita a modificar algunos conceptos del Código Penal, incluyendo tipificaciones ampliatorias de figuras ya existentes y de los mecanismos procesales asociados). Delito Informático Propio: Es el que afecta a la información, como bien jurídico a proteger, como por ejemplo la sustitución de identidad; está muy poco desarrollado legislativa y jurisprudencialmente.*

64 *Código Civil de la Nación Argentina, Art. 2311. – "Se llaman cosas en este Código, los objetos materiales susceptibles de tener un valor. Las disposiciones referentes a las cosas son aplicables a la energía y a las fuerzas naturales susceptibles de apropiación". Modificado por ley 17.711, Art. 1. Sustituido por inciso 89. BO: 26/04/68. A partir del 01/07/68, por Art. 7.*

Art. 2312. – "Los objetos inmateriales susceptibles de valor, e igualmente las cosas, se llaman 'bienes'. El conjunto de los bienes de una persona constituye su 'patrimonio'".

65 *Es frecuente que, en los juegos de rol en red, donde múltiples participantes compiten en forma mancomunada, formando alianzas ofensivo-defensivas para poder cumplir ciertas misiones que el juego impone, la aparición de jugadores que luego de alcanzar altos niveles con un determinado personaje, lo subastan al mejor postor. La compraventa del personaje se efectiviza mediante una transacción económica (normalmente, mediante el pago por medios electrónicos) y la entrega por el vendedor del nombre de usuario y la clave de la cuenta con que su dueño original se conectaba a la comunidad de juegos referida. El comprador ingresa, cambia la clave y el personaje pasa a ser definitivamente suyo (una especie de esclavitud virtual). Puede ocurrir ante una compraventa de este tipo que una de las dos partes contratantes (comprador/vendedor) no cumpla con su parte del trato,*

¿estamos entonces ante un incumplimiento de contratos? Imaginemos la demanda: "...que se presenta ante S. Sa. con el objeto de reclamar a N.N. por no haberle entregado en el marco del juego de roles: 'La magia ancestral', un hechicero de nivel 74, armado con una esfera multidimensional con aptitud congelante, una capa de invisibilidad multifuncional, habilidad de resurrección sobre los muertos, acompañado por cinco vampiros y un hombre lobo de su propiedad, a pesar de haber realizado el correspondiente pago por medio de transacción electrónica, cuya copia impresa se acompaña, al igual que los mensajes intercambiados donde se hace referencia a la transacción acordada, recolectados y certificados ante escribano público, según acta notarial que también se acompaña". También puede pasar que un hacker robe las pertenencias del personaje (cuando no al personaje completo). ¿Estaríamos ante un hurto o ante un rapto de personaje virtual? "XX... se presenta ante el Sr. fiscal a efectos de denunciar el robo de dos armaduras

mágicas, una espada con poder electrificante y un escudo antigravedad, que adquiriera la semana pasada al denominado JJ en el marco del juego…" (adjunta recolección de prueba documental informática relacionada con el evento denunciado).

SEGUNDA PARTE
PROCEDIMIENTOS

CAPÍTULO 8
PROCEDIMIENTO DE APLICACIÓN GENERAL PARA TELÉFONOS CELULARES

Etapa de identificación, registro, protección, embalaje y traslado

Identificación y registro

a. Colocarse guantes.

b. Fotografiar el dispositivo.

c. Registrar marca y modelo.

d. Si es factible solicitar al gabinete de criminalística para que registre la existencia de huellas digitales o cualquier otro elemento químico, acorde a sus procedimientos.

e. Disponer, según sea el caso, las pruebas obtenidas en una zona despejada, para su posterior rotulado y registro.

f. Registrar en el formulario de registro de la evidencia el o los dispositivos hallados, acorde a lo especificado en dicho formulario y agregando cualquier otra información que considere pertinente el perito informático forense.

Protección del dispositivo

Posibles estados en que se puede encontrar el dispositivo

Encendido

i. Mantener la batería cargada y no manipularlo. Según el tipo de dispositivo, evitar tocar la pantalla táctil.

ii. Efectuar las maniobras necesarias para aislar el teléfono de la red, cubriéndolo con varias capas de papel de aluminio, o colocándolo en una jaula de Faraday o configurándolo en Modo Avión.

En el Modo Avión, el celular no puede enviar o recibir llamadas telefónicas, mensajes de texto, mensajes con imágenes o mensajes de video; el usuario no podrá navegar por Internet o utilizar los dispositivos Bluetooth. El resto de las aplicaciones siguen en funcionamiento –reproductor de música, juegos, agenda, etc.– y pueden seguir siendo utilizadas. En los dispositivos en general, se debe oprimir el botón de apagado y seleccionar Modo Avión. Otro modo es presionar Menu de la pantalla inicial, luego Configuración o Ajustes, luego la opción Redes Inalámbricas o Wireless Networks, y luego aparece la opción

Modo Avión.

iii. Si el dispositivo es del tipo GSM (Global Systems for Mobile communications), remover la tarjeta SIM, deshabilita en forma efectiva todos los celulares de voz, SMS y transmisión de datos. No desactiva las redes inalámbricas. No funciona en dispositivos que no sean GSM, incluyendo los teléfonos CDMA (Code Division Multiple Access, Acceso Múltiple por División de Código) o iDEN (Integrated Digital Enhanced Network, Red Mejorada Digital Integrada) y tecnología inalámbrica creada por Motorola.

iv. La suspensión de la cuenta con el proveedor del servicio de la red inalámbrica celular, deshabilita de manera efectiva todos los celulares de voz, SMS y transmisión de datos, pero requiere la autorización del juez.

Apagado

i. Dejar el dispositivo apagado, encenderlo implicaría la sobrescritura de datos.

ii. Se recomienda apagar el equipo por la posibilidad de que se pierdan datos ya sea porque la batería se agotó o porque ocurrió alguna pérdida de señal de la conexión con la red telefónica. Los datos de carácter temporal se perderán con el apagado del equipo. Al encenderlo, es posible que el dispositivo tenga una clave de acceso y por consiguiente el acceso al celular será restringido.

Observación: Si el teléfono está apagado y se lo conecta al cargador es como si se lo hubiera encendido. Por esta razón, se recomienda esperar hasta que se pueda iniciar el dispositivo en el modo de recuperación o en modo a prueba de fallos (DFU, Device Failsafe Utility, utilidad a modo de prueba de fallos del dispositivo) para la recolección de datos y en esta situación conectarlo al cargador.

Embalaje y traslado

a. Colocar el celular en una bolsa de aluminio o en una jaula de Faraday que evite el acceso a las señales de la red y permita su aislamiento:

i. Sellar la bolsa para evitar su apertura.

ii. Rotular.

b. Colocar el equipo en un recipiente donde se mantenga inmovilizado para su traslado (cajas, etc.).

c. Iniciar e ingresar los datos requeridos en el formulario para la cadena de custodia (Ver Anexo “Procedimiento para la cadena de custodia en la pericia de Informática forense”).

Procedimiento para la recolección y protección de información – Elementos a recolectar

1. Sistema operativo.

2. Llamadas realizadas (fecha, hora, duración).
3. Llamadas recibidas (fecha, hora, duración).
4. Último número marcado (LDN Last Dialed Number).
5. Lista de contactos.
6. Mensajes de texto.
7. Fotografías.
8. Archivos.
9. Archivos borrados.
10. Espacio desperdiciado.
11. Videos.
12. Agenda.
13. Correo electrónico.
14. Tonos de timbres (ringtones) personalizados, los cuales pueden ser identificados por un testigo permitiendo ubicar a alguien en un determinado lugar.
15. Ubicación, establece la ubicación física de una persona o su dirección de traslado o viaje.
16. Tarjeta SIM (Subscriber Identity Module) –contiene un procesador con memoria no volátil–, se utiliza como dispositivo de almacenamiento de información relacionada con el subscriptor, incorporada a la red global de celulares GSM (Global Systems for Mobile communications). En la tarjeta se puede obtener:

a. Identificador de área local, identifica dónde está ubicado actualmente el celular.

Este valor permanece almacenado en el SIM luego de apagado el celular. Es útil para identificar cuál fue la última ubicación donde se utilizó el celular.

b. Número de serie, se puede obtener sin tener el PIN (Personal Identification Number) e identifica al SIM mismo.

c. Número de cliente, se refiere al IMSI (International Mobile Subscriber Identity), que es el número de identificación del cliente que permitirá, junto con la ayuda del proveedor de servicio, identificar al cliente propietario del celular.

d. Número de teléfono del celular. Se refiere al MSISDN (Mobile Subscriber Integrated Services Digital Network).

Recolección de información de la tarjeta SIM

1. **Mensajes de texto:** Existe un espacio en la tarjeta que mostrará los últimos 12 mensajes enviados. Los celulares almacenan los mensajes en

memoria. La mayoría utiliza la memoria de la tarjeta SIM primero antes de usar la memoria interna.

2. **Mensajes borrados:** Similar al borrado de archivos en un disco rígido, el primer byte es configurado en cero. Esto significa que los mensajes borrados pueden recuperarse, excepto el primer byte mientras no se sobrescriba con nuevos mensajes.

3. **Guía de teléfonos:** La mayoría de los celulares tienen la capacidad de almacenar un mínimo de 100 números marcados con su respectivo nombre asociado.

4. **Últimos números marcados:** La mayoría de las tarjetas almacenan aproximadamente los últimos cinco números marcados en la tarjeta SIM. No obstante, la mayoría de los celulares almacenan muchos más en la tarjeta interna de memoria del celular.

Dispositivos iPhone

El teléfono iPhone[66] es un dispositivo inteligente inalámbrico que combina las funciones de un teléfono celular, cámaras, asistente digital personal (PDA), iPod y acceso a Internet a través de un navegador móvil –primera generación desarrollada por Apple en 2007–. El dispositivo permite el acceso a: mensajes de texto, correo electrónico, contactos, historial de llamadas, fotos, música y video. El acceso a Internet a través de un navegador web es similar al de una computadora personal, por lo tanto la recolección de datos también se realiza de forma similar a la de una computadora personal. El perito informático forense puede efectuar el seguimiento revisando el historial del navegador y de las páginas marcadas como favoritos y la información borrada.

sistema de archivos

El esquema de partición de iPhone es semejante al de Apple TV, consta de dos particiones:

- Master Boot Record (MBR), tiene la longitud de un sector y es responsable de la carga del sistema operativo en el iPhone.
- Seguida de un área libre de Apple (Free).
- Primera partición se encuentra el sistema de archivo jerárquico HFSX[67] (Hierarchical File System): almacena el sistema operativo de iPhone (BigBear)[68], generalmente tiene un tamaño de 500 Mb y es utilizada por el sistema de archivo HFSX, semejante a sus antecesores iPod y Apple TV.
- Seguida de otra área libre de Apple (Free).
- La Segunda partición HFSX (Hierarchical File System) contiene información individual del usuario y de evidencia para el perito (videos, fotografías, información de contacto).

Procedimientos y medidas preventivas para la protección, embalaje y traslado de dispositivos

Los procedimientos para la identificación, registro, protección, embalaje y traslado de los teléfonos inteligentes son similares a los enunciados para los teléfonos celulares. No obstante, para los teléfonos inteligentes se deben efectuar los siguientes:

Consideraciones previas

Los dispositivos poseen actualmente una serie de funcionalidades que les permiten efectuar la protección de estos a través del ingreso de códigos de acceso. En el momento de la identificación del dispositivo, el perito informático forense deberá considerar si posee un código de acceso para deshabilitarlo inmediatamente o eludirlo.

Si el dispositivo iPhone se encuentra con la pantalla activa, es importante verificar si tiene activado el código de acceso y cambiar la configuración. En el caso de que se encuentre activado, se debe proceder rápidamente a cambiar la opción de bloqueo, cuyo rango puede ir desde un minuto a la opción nunca, permitiendo de esta forma el acceso total al dispositivo evitando el ingreso de un código de acceso.

El cambio de configuración del tiempo de bloqueo implica una modificación y escritura de datos en el dispositivo que debe ser registrada y documentada por el perito como así también deberá fundamentar esta operación realizada en el caso de que sea cuestionada en el proceso judicial.

iPhone e iPad son similares a los dispositivos BlackBerry, los cuales poseen la funcionalidad de efectuar la limpieza (wipe) o borrado remoto de los datos, esto puede ocurrir aun en los casos en que el usuario no se encuentre en posesión del dispositivo. El borrado puede ser realizado por el propietario o por cualquier otra persona que tenga acceso a la cuenta MobileMe asociada al dispositivo.

MobileMe es un servicio de Internet diseñado por Apple, reemplaza a Mac, provee el servicio a los dispositivos iPhone, iPod Touch e iPad y a los sistemas operativos Mac OS X, Windows. La empresa Apple posee el control de estas cuentas y pueden ser utilizadas por la justicia para solicitar la prueba documental informática de informe del proveedor del servicio, en este caso Apple.

El servicio Find My iPhone dentro de una cuenta MobileMe requiere estar conectado a la web o a la red 3G. Este servicio permite a los usuarios conocer la ubicación de su dispositivo iPhone, iPod Touch o iPad en el sitio web www.me.com/find.

El servicio de MobileMe venció el 30 de junio de 2012 y es reemplazado por iCloud (https:// www.icloud.com), en donde el usuario podrá almacenar todos sus archivos (disponibles 5 GB) en servidores de Apple a los que puede acceder desde cualquier dispositivo. El id o identificador de Apple es la dirección de correo electrónico que el usuario empleará para el intercambio de información con la empresa Apple y para el servicio de iCloud, para la compra en iTunes Store o descarga de aplicaciones del App Store.

Procedimiento para iPhone encendido

Pantalla activa: Puede o no tener el código de acceso y la opción auto-bloqueo activa

1. Visualizar la pantalla del dispositivo y registrar por medio de fotografía, filmación o en forma manuscrita la fecha y hora del sistema.
2. Seleccionar el ícono Configuración.
3. Seleccionar la opción General, si aparece la siguiente configuración, el dispositivo tiene un código de acceso:
   a. Período de bloqueo automático del teléfono o auto-bloqueo (configurado, por ejemplo, en 2 minutos).
   b. Bloqueo de código de acceso: Activo (On).
   c. Restricciones: Inactivo (Off).
4. En esta pantalla se requiere cambiar la configuración de la opción de Período de bloqueo automático del teléfono de 2 minutos a la opción Ninguno o Nunca, con el fin de efectuar la recolección lógica de datos. Es importante para el perito tener un cargador de iPhone como parte del equipo de herramientas.

Aislamiento del dispositivo de la red celular e inalámbrica

1. **Oprimir el ícono de Configuración.**
2. Seleccionar la configuración de Modo Avión (Modo desconectado).
3. Cambiar de desconectado a activo (apagado a encendido).
4. Verificar la opción de Wi-Fi, en algunos dispositivos puede estar activa:
   a. Seleccionar la opción de configuración de Wi-Fi.
   b. Cambiar a desactivado o apagado.
5. En los dispositivos iPod táctil y Wi-Fi iPad solamente es necesario desactivar la opción de Wi-Fi.
6. Remover la tarjeta SIM o mini SIM del dispositivo iPhone o de iPad, esta acción solo desconecta el dispositivo de la red celular, no del punto de acceso inalámbrico:

a. Utilizar una herramienta para remover la tarjeta o un clip para papel.

b. Extraer la tarjeta colocando la herramienta en la parte superior del dispositivo o en un costado, según el modelo de dispositivo: iPhone 2G, 3G y 3GS:

– En los dispositivos iPhone 4, la tarjeta SIM está en el lado derecho.

– En los dispositivos iPad, la tarjeta se encuentra en el lado izquierdo.

7. Aislar el dispositivo y la tarjeta con varias capas de papel de aluminio o caja de Faraday.

8. Identificar y registrar el dispositivo.

Procedimiento: El dispositivo tiene el código de acceso activado y está bloqueado para responder

1. Aislar el dispositivo con varias capas de papel de aluminio o jaula de Faraday.

2. Identificar y registrar el dispositivo.

Procedimiento para la comprobación del estado del código de acceso

Verificar si el bloqueo de código de acceso está activado:

a. Si la ventana de Ingresar código de acceso no aparece en respuesta al dispositivo, entonces el código de acceso ha sido activado.

b. Aquí se requiere encontrar y recuperar los certificados de bloqueo.

En los casos en que el iPhone se encuentre conectado y eventualmente sincronizado con una computadora cuyo sistema operativo sea Mac o Windows y la computadora forme parte también de la recolección, se facilitará la tarea de obtener información de un iPhone con la pantalla bloqueada, la cual requiere el ingreso del código de acceso de un número de cuatro dígitos o de una clave más fuerte.

c. Conectar el dispositivo a una estación de trabajo de Informática forense y efectuar la recolección o adquisición lógica de los datos utilizando el método manual con el reproductor multimedia iTunes o con otra herramienta de extracción.

La versión iOS 4 incorpora la opción de contraseñas más complejas. En esta situación es posible obtener los certificados de bloqueo del código de acceso en el laboratorio del perito. Los directorios en donde se pueden encontrar los pares de certificados, archivo .plist son los siguientes:

A. En Windows:

a. 7: C:\ProgramData\Apple\Lockdown

b. Vista: C:\Users\username\AppData\Roaming\Apple

Computer\Lockdown

c. XP: C:\Document and Settings\username\LocalSettings\Application Data\Apple Computer\Lockdown

B. En OS X:

a. /Private/var/db/Lockdown

Los pasos a seguir son:

1. Copiar la carpeta Lockdown en un dispositivo externo de almacenamiento para su posterior recolección.
2. La lista de propiedad (plists) contiene las claves de autenticación y se pueden utilizar en los casos en que se requiera ingresar el código de acceso sin necesidad de que el perito utilice otros métodos intrusivos para determinar el código.

Para el perito es importante ubicar estos archivos no solo en los sistemas operativos, sino también en aquellos casos en que los certificados de autenticación se encuentren almacenados en dispositivos externos.

Procedimiento para la verificación y secuencia del posible borrado remoto (wipe)

1. Desde la cuenta MobileMe el servicio Find My iPhone debe estar activado.
2. Desde el dispositivo se debe agregar una cuenta MobileMe.
3. El servicio Find My iPhone debe estar activado o encendido.

A partir de esta configuración, cualquier usuario con acceso web a la cuenta MobileMe puede borrar la información en forma remota o bloquear el acceso al dispositivo.

El usuario puede realizar dos acciones:

1. Colocar un código de acceso.
2. Borrar en forma remota los datos.

Secuencia para ingresar en forma remota el código de acceso:

1. Ingresar a MobileMe.
2. Ir a la opción Find My iPhone.
3. Seleccionar el dispositivo.
4. Seleccionar la opción Bloquear.
5. Ingresar dos veces un nuevo código de acceso y seleccionar Bloquear.

Secuencia para el borrado remoto del dispositivo:

1. Ingresar a la cuenta MobileMe.
2. Seleccionar Find My iPhone.
3. Seleccionar el dispositivo apropiado.

4. Seleccionar Borrar o Wipe.

5. Aparece un mensaje emergente de advertencia y si es aceptado el dispositivo será borrado.

Procedimiento para iPhone apagado

Identificación y registro

1. Fotografiar o filmar el dispositivo.

2. Registrar el modelo.

3. Efectuar el procedimiento para embalaje y traslado del dispositivo.

Procedimiento para la identificación de dispositivos iPhones liberados (jailbroken)

Los dispositivos pueden haber sido liberados con el fin de permitir la escritura en el sistema operativo iOS e incorporar aplicaciones no ofrecidas o limitadas por el fabricante Apple, utilizando herramientas como: Qwkpwn, Blackra1n, Pwnage, JailBreak. En la versión del iOS 4 resulta más difícil determinar si el dispositivo ha sido liberado.

1. El perito deberá conocer cuáles son las aplicaciones propias de un dispositivo Apple sin liberar.

2. A través de la observación del dispositivo, identificar en la pantalla inicial la existencia de aplicaciones que no se corresponden con la versión original o no liberada: mayor número de íconos en los diferentes menús del dispositivo y en la pantalla inicial personalizada por el usuario.

3. El proceso de recolección de datos es el mismo que en los dispositivos no liberados descriptos anteriormente.

Etapa de recolección y adquisición de datos

Procedimientos de recolección de datos en dispositivos iPhone e iPad

Consideraciones previas

Existen tres métodos:

- Recolección física.
- Recolección lógica.
- Recolección a partir de archivos de resguardo.

Método de recolección física

Los mecanismos de seguridad de iPhone impiden realizar una imagen física si no se tienen los privilegios de acceso, pero existen algunos métodos que pueden utilizarse para acceder a la memoria del dispositivo y obtener una

imagen completa de memoria Flash no volátil: NAND[69].

Esta memoria guarda no solo el sistema de archivos sino también información del usuario. El archivo ADDataStor.sqlitedb contiene información detallada de la memoria Flash NAND. La recolección física crea una copia bit a bit del sistema de archivo.

La versión del iOS 4 ofrece el encriptado de hardware en el iPhone 4, 3GS, iPod Touch (3 G o posteriores) y en los modelos de iPad. Por lo tanto, si se efectúa la imagen bit a bit, todos los datos estarán encriptados.

Los métodos de obtención o adquisición física en iPhone e iPad son:

- Zdziarski, Jonathan (http://www.zdziarski.com/blog/). Experto en telefonía forense de iPhone. Las herramientas de automatización solo están disponibles para organismos policiales o judiciales.
- iXAM, programa comercial desarrollado por FTS (Forensic Telecommunications Services) http://www.ixamforensics.com/.
- A través de un dispositivo liberado y funcionan en versiones de firmware anteriores a la 4.x.

Los métodos Zdziarski e iXAM fueron comprobados por el NIST (National Institute of Standards and Technology Instituto Nacional de Tecnologías y Estándares), los resultados se pueden visualizar en http://www.cftt.nist.gov/mobile_devices.htm. Ambas herramientas han desarrollado las acciones necesarias que permiten realizar una copia bit a bit, accediendo al dispositivo como usuario administrador (root), sin modificar la partición del usuario. Un dispositivo liberado efectúa esta acción modificando la partición de datos del usuario, es decir, sobrescribiendo la información y, por lo tanto, modificando la evidencia.

El método de copia bit a bit de un dispositivo liberado se puede realizar con el comando “dd”, pero solo se podría utilizar a modo de investigación o aprendizaje, pero no se puede presentar como método de imagen forense en un tribunal.

El dispositivo iPod Touch ejecuta el iOS y los datos pueden ser recolectados con muchas de las herramientas existentes para iPhone. Las técnicas de adquisición física, lógica o de resguardo utilizadas en iPhone también pueden aplicarse a iPad. El dispositivo iPod ejecuta tanto el sistema de archivo HFS+ como FAT32, dependiendo del sistema operativo en el cual fue inicializado.

En el caso de Apple TV, dependiendo de las versiones y modelos, se podrá efectuar una imagen del disco bit a bit –en el caso de la primera versión–, ya que ejecuta una versión modificada del sistema operativo OS X. La segunda generación tiene una versión de iOS que es casi idéntico al de la cuarta generación de iPod Touch. La segunda generación de Apple TV no tiene disco

rígido de almacenamiento, pero posee almacenamiento Flash NAND de 8GB.

Procedimiento para la preparación de la duplicación de la memoria Flash NAND

Determinar el modelo y versión de firmware iOS, de esta forma el perito puede seleccionar la herramienta adecuada para efectuar la duplicación, acorde a la versión del sistema operativo que soporte la misma.

a. La información del modelo se encuentra en la parte posterior del dispositivo.

b. La versión de firmware (sistema operativo) se obtiene accediendo a la memoria ROM:

i. Encendiendo el dispositivo.

ii. Desbloqueando el código de acceso.

iii. Ingresando al menú: Configuración > General > Acerca de > Versión.

Si el teléfono se encuentra apagado o está bloqueado se deben implementar otros métodos. La herramienta iRecovery (utilidad USB para Mac OS X, Linux y Windows, que permite dialogar con el proceso iBoot, inicia en la memoria ROM, segundo paso del gestor de arranque del teléfono, a través de una conexión USB, Licencia GNU GPL v3), para obtener la versión de firmware iRecovery.

Procedimiento para ejecutar la herramienta iRecovery

1. En la estación de trabajo informático forense, instalar la herramienta iRecovery:

a. En Linux y en Mac, solo es necesario descargar los archivos fuentes.

b. En Windows, se debe instalar la biblioteca libusb, para permitir el acceso a los dispositivos USB.

2. Colocar el dispositivo en el modo de funcionamiento: Recuperación (Recovery), iniciando con iBoot, sin cargar el sistema operativo, para ingresar en este modo:

a. Apagar el dispositivo, manteniendo apretado el botón de la parte superior del teléfono hasta que se visualice el texto “deslice hasta que se apague” (slide to power off).

3. Mantener apretado el botón Inicio (Home) y conectarlo a una estación de trabajo informático forense por medio del conector USB, hasta que aparezca el texto “Conectar a iTunes” y liberar el botón Inicio (Home).

Al colocar el cable USB el dispositivo recibe la alimentación eléctrica. Otro modo sería:

a. Primero, conectar el dispositivo a la estación de trabajo.

b. Apagar el dispositivo.

c. Mantener el botón Inicio (Home) presionado mientras se oprime el botón de encendido del dispositivo.

4. En la estación de trabajo informático forense, abrir una consola de terminal y ubicar el directorio en donde se instaló iRecovery.

a. Ejecutar el comando:

i. iRecovery -s, para identificar la versión de iBoot y generar una salida con la información requerida.

Ejemplo de la salida generada por el comando iRecovery -s:

http://theiphonewiki.com/wiki/index.php?title=IRecovery#Example_Output

==========

::

: iBSS for n82ap, Copyright 2009, Apple Inc.

::

:: BUILD_TAG: iBoot-596.24

::

:: BUILD_STYLE: RELEASE

::

:: USB_SERIAL_NUMBER: CPID:8900 CPRV:30 CPFM:03 SCEP:05 BDID:04 ECID:000003293C113D76 IBFL:00

::

==========

Entering recovery mode, starting command prompt

] printenv

build-style = “RELEASE”

build-version = “iBoot-596.24”

config_board = “n82ap”

loadaddr = “0x9000000”

boot-command = “fsboot”

bootdelay = “0”

auto-boot = “true”

idle-off = “true”

boot-device = “nand0”

boot-partition = “0”

boot-path = “/System/Library/Caches/com.apple.kernelcaches/kernelcache.s5l8900x”

display-color-space = “RGB888”

display-timing = “optC”

framebuffer = “0xfd00000”

secure-boot = “0x1”

Sitios en donde se puede obtener el Listado de versiones de firmware y de iTunes:

- http://support.apple.com/downloads/
- http://theiphonewiki.com/wiki/index.php?title=Firmware
- http://www.trejan.com/projects/ipod/#FIRMWARE

ii. Si la herramienta iRecovery no encuentra un dispositivo, mostrará el siguiente mensaje: No iPhone/iPod found, no se encontró iPhone/iPod.

5. Instalar la versión iTunes adecuada para la versión de iOS hallada en el paso anterior.

Si la versión de iTunes es anterior o inferior a la versión del iOS, no se podrá efectuar la recolección o adquisición física.

a. Si se debe instalar una versión de iTunes anterior a la instalada, se debe desinstalar la herramienta completamente quitando todos los accesorios e instalar la versión más antigua.

6. Reiniciar la estación de trabajo informático forense.

Descripción del método de duplicación de la partición de datos de usuario del dispositivo utilizando el método de Jonathan Zdziarski (http://www.zdziarski.com/blog/)

Las herramientas de automatización se ejecutan en un entorno de línea de comandos. El método requiere modificar una partición del sistema de solo lectura que está completamente separada de la partición en donde se encuentran los datos del usuario. El proceso instala un agente de recuperación de la partición del sistema del dispositivo. Se debe reiniciar el dispositivo para que se active el agente de recuperación. Posteriormente, se inicia la línea de comandos de recuperación que crea una copia bit a bit de la imagen del disco en el dispositivo y lo envía a la estación de trabajo informático forense a través de la conexión USB. Los pasos que realiza la herramienta serían los siguientes:

1. El iPhone debe estar en el modo de Recuperación (Recovery) o en modo a prueba de fallos (DFU, Device Failsafe Utility, Utilidad a modo de prueba de fallos del dispositivo), dependiendo de la versión de firmware del dispositivo.

2. Conexión del dispositivo a la estación de trabajo de Informática forense a través del cable USB. La aplicación iTunes puede ejecutarse automáticamente luego de conectado el iPhone, se debe salir del programa de iTunes.

3. Configuración de las herramientas de automatización. La mayoría de las

herramientas funciona en un entorno Linux o en una máquina virtual con el sistema operativo Linux y no requieren de la aplicación iTunes. Al completarse la configuración, aparecerá un mensaje que indica que el primer script puede ejecutarse, también indicará el modo de operación en que debe estar el dispositivo.

4. Posteriormente, indicará desconectar y conectar el dispositivo del cable USB, en esta operación se pasará una serie de datos que se puede visualizar en la pantalla. Luego se reinicia el dispositivo y el agente de recuperación queda instalado y activo.

5. El segundo script se ejecuta e indica colocar el dispositivo en uno de los modos establecidos en el punto 1, y deberá conectar y desconectar el dispositivo de la conexión USB, siguiendo las instrucciones del programa, indicando al final si se ejecutó con éxito o no la instalación. La herramienta iRecovery iniciará el dispositivo, luego de esta acción el agente de recuperación estará activo.

El dispositivo iPhone o iPad se reiniciará en el modo normal, en este momento comienza la recuperación. El archivo usbmux-proxy, que es propietario de iTunes, es reemplazado por la herramienta de Zdziarski, por una versión de código abierto denominada usbmuxd (USB multiplexing daemon), y permite la comunicación entre el dispositivo y la conexión USB, evitando de esta manera el uso de la aplicación iTunes y permitiendo la adquisición de datos.

6. En la ejecución del script de recuperación se producirá la duplicación de los datos en el dispositivo. Se crea un archivo de la imagen en la estación de trabajo. El proceso no se debe interrumpir, si el archivo se mantiene en 0 bytes, es posible que el agente de recuperación en vivo no se encuentre instalado correctamente o no ha sido activado correctamente.

7. El proceso de duplicación estará terminado cuando aparezca en la ventana de la terminal el siguiente mensaje: “No se puede conectar al usbmux” (Cannot connect to usbmux).

8. Una vez finalizada la copia bit a bit, acorde a las instrucciones de la herramienta se debe ejecutar una serie de comandos para detener la ejecución del agente de recuperación.

9. Posteriormente, se debe renombrar la imagen con la nomenclatura seleccionada por el perito. Si la imagen se monta en un sistema operativo Mac, se debe cambiar la extensión a “.dmg”. Luego de esta acción se pueden cambiar los permisos a solo lectura. En Mac, con el botón derecho del mouse, seleccionar la opción “Obtener Información” (Get Info). Esta acción mostrará las propiedades del archivo y se debe seleccionar la casilla de verificación “Bloqueado” (Locked).

10. Posteriormente, se debe efectuar la certificación matemática (hash) del archivo de la imagen, que se debe luego ingresar en el informe pericial.

a. En Mac:

$md5 iPhone.dmg

$shasum iPhone.dmg

b. En Linux:

$sha256sum iPhone.dmg

$md5sum iPhone.dmg

En ambos casos, se puede reenviar la salida del comando de hash utilizado para conservarlo en un archivo de texto: $shasum iPhone.dmg > shasum.txt

11. La imagen bit a bit ya se puede montar para efectuar el análisis de los datos correspondientes.

Ejemplo del método de duplicación en un dispositivo liberado

Este método puede ser utilizado tanto para dispositivos iPhone como iPad.

1. Se debe crear una red inalámbrica en la estación de trabajo informático forense y asignar direcciones ip fijas para esta y para el dispositivo iPhone.

a. En Mac:

$sudo ifconfig en1 inet 192.168.0.1 netmask 255.255.255.0

b. En el iPhone:

Configuración – Wi-Fi, conectar a la red inalámbrica creada anteriormente, seleccionar la opción de dirección ip estática, ingresar el valor 192.168.0.2 y la máscara 255.255.255.0. Seleccionar la opción Redes Wi-Fi en la esquina superior izquierda del dispositivo y guardar los cambios.

La estación de trabajo y el iPhone se encuentran en la misma sub red y pueden comunicarse entre ellos.

2. Conexión remota al dispositivo iPhone por medio de SSH, utilizando en forma predeterminada en los dispositivos liberados el usuario “root” y la contraseña “alpine”. La aplicación Cydia (http://www.saurik.com/, creada por Jay Freeman para descargar programas en el iPhone, similar al APT de Debian) se suele utilizar para liberar los iPhone; se deberá verificar si SSH está instalado de lo contrario se deberá instalar en el dispositivo OpenSSH.

a. En Mac:

$ssh root@192.168.0.2

root@192.168.0.2´s

password: 3GS-40:~root#

3. Se deben verificar en el iPhone las particiones existentes para determinar

de cuál de ellas se efectuará la copia bit a bit: rdisk0, es el disco completo; rdisk0s1, es la partición del firmware; rdisk0s2, es la partición de los datos del usuario; rdisk0s2s1, es única para el dispositivo 3GS.

a. En el iPhone:

3GS-40:~root# ls –l /dev/rdisk*

crw r-------1 root user 19, 0 Mar 12 13:26 rdisk0

crw r-------1 root user 19, 1 Mar 12 13:26 rdisk0s1

crw r-------1 root user 19, 2 Mar 12 13:26 rdisk0s2

crw r-------1 root user 19, 3 Mar 12 13:26 rdisk0s2s1

4. Para efectuar la copia bit a bit, se debe verificar si en el iPhone se encuentran instalados los comandos dd y netcat.

a. En el iPhone:

3GS-40:~root#which dd

3GS-40:~root#which nc

Ambos comandos deben devolver como resultado la ruta en donde se encuentran en el sistema de archivo del dispositivo.

Si no se encuentran y el resultado de which devuelve el indicador del intérprete de comando 3GS-40:~root#, se deberán copiar desde la estación de trabajo con el comando “sc” (secure copy). Ambos comandos se copiarán en el directorio /bin.

Mac: ~usuario$ /usr/bin/scp /usr/bin/nc root@192.168.0.2:/bin/nc Mac: ~usuario$ /usr/bin/scp /usr/bin/dd root@192.168.0.2:/bin/dd

Efectuar nuevamente la comprobación de la existencia de los archivos en el iPhone, el comando debe devolver como resultado el directorio /bin.

3GS-40:~root#which dd

/bin/dd

3GS-40:~root#which nc

/bin/nc

5. La copia bit a bit se efectuará a través del comando netcat. La utilización de este comando se describió en detalle en el Manual de Informática Forense.

a. En la estación de trabajo, ejecutar netcat:

Mac: ~usuario$ nc –l 7000 | dd of=~/Escritorio/rdisk0s2.dmg bs=1048516

b. En el iPhone, para iniciar la copia bit a bit, se debe ingresar:

3GS-40:~root# /bin/dd if= /dev/rdik0s2 bs= 1M | /bin/nc 192.168.0.1 7000

En la medida que se vayan copiando los bloques, el archivo rdisk0s2.dmg que se encuentra en la estación de trabajo incrementará su tamaño. Dependiendo del tamaño de partición, la copia bit a bit puede llevar varias

horas. Finalizada la copia de la imagen, al archivo rdisk0s2. dmg se le debe asignar el permiso de solo lectura, efectuarle la certificación matemática (hash), para su posterior montaje y análisis.

Método de recolección lógica

Este método se refiere a la copia del sistema de archivos activo desde el dispositivo en otro archivo; de esta forma, los datos almacenados en el dispositivo se recuperan y pueden ser analizados posteriormente. Es una forma rápida y fácil para el perito de obtener una considerable cantidad de información del dispositivo. La recolección física brinda mayor información, pero es más compleja para su análisis y conlleva un mayor esfuerzo dependiendo siempre del hardware y software utilizado y de la capacitación del perito.

Las herramientas de telefonía móvil forense que permiten la obtención o recolección lógica de datos de los dispositivos iPhone también pueden generar informes, exportando la información recolectada a una serie de archivos que pueden ser visualizados por medio de una interfaz de usuario gráfica. El inconveniente radica en que el perito visualiza los datos en modo de informe o reporte, pero no puede ver el origen de los datos. Por esta razón, se recomienda utilizar herramientas que efectúen la recolección lógica y permitan también la visualización de la información en binario, de donde fue originada.

Procedimiento para la recolección lógica de dispositivos iPhone

El procedimiento es independiente del programa o herramienta utilizada:

1. Ejecutar el programa de telefonía forense seleccionado.
2. Conectar el dispositivo.
3. Iniciar la adquisición de la imagen. Este proceso recolectará los datos del dispositivo que fueron oportunamente resguardados utilizando el protocolo de sincronización de Apple. Los datos son obtenidos directamente del dispositivo y no del resguardo (como ocurre en el método de recolección por resguardo).
4. Acorde a la aplicación de recolección utilizada, la información será desplegada dentro del programa y puede ser posteriormente exportada para la generación de un informe.

Método de recolección a partir de archivos de resguardo

En este método los datos a recolectar han sido almacenados previamente a través de una copia de resguardo desde el dispositivo hacia la computadora del usuario.

El resguardo de datos incluye: música adquirida, shows de televisión,

aplicaciones, libros electrónicos, fotos, videos, configuración del dispositivo (Favoritos, Papel tapiz, Correo electrónico, Contactos, Agenda, Cuentas), datos de las aplicaciones, organización de los datos, mensajería (SMS: Short Message Service, MMS: Multimedia Message Service e iMessage), tonos de timbres, entre otros. Se utiliza cuando el dispositivo original no está disponible. Considerando que el origen de los datos está constituido por los datos resguardados previamente con el protocolo de sincronización de Apple, solamente estos archivos serán recuperados.

Existen diferentes herramientas comerciales (Paraben Device Seizure, Oxygen Forensic Suite, Mobile Sync, Mobilyze, iPhone Analyzer, Lantern, Susteen Secure View 2Encase Neutrino) y de código abierto que pueden obtener información de los archivos de resguardo de iPhone, iPad o iPod Touch.

Al conectar el dispositivo iPhone a la computadora se efectúa un resguardo automático durante el proceso de sincronización o cuando se realiza una actualización o restauración. Los datos resguardados por medio de iTunes se almacenan en una ubicación predeterminada acorde al sistema operativo de la computadora receptora de los archivos resguardados:

· Windows XP:

C:\Documents and Settings\<nombre de usuario>\Application Data\Apple Computer\ MobileSync\Backup\

· Windows Vista. Windows 7:

C:\Users\<nombre de usuario>\AppData\Roaming\Apple Computer\MobileSync\Backup\

· Mac OS X:

· Users/<nombre de usuario>/Library/Application Support/MobileSync/Backup/ Los archivos resguardados en las carpetas son:

· Status.plist, brinda información del estado de la última sincronización/resguardo.

· Info.plist, contiene información del dispositivo en general: nombre del dispositivo, versión, IMEI (International Mobile Equipment Identity, Identidad Internacional de Equipo Móvil), número del teléfono, entre otros.

· Manifest.plist, incluye una lista de todos los archivos resguardados, fecha y hora de modificación y valor del hash.

· El resto contiene varios archivos del tipo “*.mddata” y “*.mdinfo”; en versiones anteriores a la 8.x de iTunes, aparecen como “*.mdbackup”. Estos archivos son los que interesan en el momento de efectuar la recolección, ya que contienen datos del usuario, no pueden ser abiertos tal como aparecen, son binarios y para poder acceder a su contenido se debe utilizar una

herramienta de conversión. Cada archivo .plist debe ser convertido a XML[70] (Extensible Markup Language), para su análisis correspondiente.

La adquisición o recolección de los datos resguardos almacenados en las carpetas predeterminadas, se pueden extraer con herramientas que no son específicamente de telefonía forense. La aplicación iPhone Backup Extractor se puede descargar libremente del sitio http://www.iphonebackupextractor.com/free-download/ y se puede ejecutar en los sistemas operativos Windows, OS X y Linux. Esta herramienta convierte los archivos plist de su formato binario a un formato comprensible y de fácil lectura en Mac.

Existen otros programas de código abierto que realizan una extracción similar y se ejecutan en diferentes sistemas operativos.

Procedimiento para la recolección lógica a partir de los archivos resguardados con la herramienta iPhone Backup Extractor

1. Descargar e instalar la herramienta.
2. Ejecutar el programa; en el caso de utilizar la herramienta iPhone Backup Extractor, listará en forma automática los resguardos de diferentes dispositivos: iPhone, iPad o iPod ubicados en su carpeta predeterminada según el sistema operativo de la estación de trabajo.

3. Seleccionar el dispositivo del cual se obtendrán los archivos de resguardo.
4. Seleccionar del listado de datos resguardos, por ejemplo, “iOS Files”.
5. Extraer los archivos del paso anterior en una carpeta de la estación de trabajo para su posterior análisis.
6. Efectuar su certificación matemática (hash).
7. Registrar y documentar el resultado.

Resguardos encriptados

La herramienta iTunes permite efectuar un resguardo encriptado ingresando una contraseña antes de realizar la sincronización y resguardo. Los resguardos encriptados complican la recuperación de datos (*.mddata y *.mdinfo) a partir

del resguardo y si la contraseña es compleja puede resultar imposible acceder a estos. En la versión de iOS 4, la encriptación se realiza en forma diferente en el dispositivo.

Si un resguardo no está protegido con clave, el archivo de clave que contiene el nombre del usuario y los datos de la clave es cifrado utilizando las claves de hardware almacenadas en el iPhone. Si la base de datos de claves es abierta, cierta información puede verse, pero las claves aparecerían encriptadas.

Si el resguardo está protegido con clave, el archivo con el usuario y clave estará cifrado utilizando las claves generadas por el programa a partir de la contraseña de resguardo, es decir que si la clave que se utilizó para el resguardo es conocida, entonces es posible obtener los datos cifrados del archivo que contiene el nombre de usuario y la clave. Esto es factible solamente en un dispositivo que ejecute un firmware de versión 4.x.

La herramienta ElcomSoft´s iPhone Password Breaker puede recuperar el texto en claro de la clave que protege los archivos de resguardo encriptados y desencriptar el archivo Manifest.plist que forma parte de los archivos cifrados al realizar el resguardo con protección de contraseña. La aplicación permite explorar el conjunto usuario y clave y recuperar servicios protegidos con contraseña como los puntos de acceso inalámbricos, los mensajes de voz, claves de cuentas de correo y de aplicaciones que utilicen la base de datos de nombre de usuario y clave de Apple.

Las claves del tipo numérica de cuatro dígitos pueden ser develadas en poco tiempo[71]. Luego de la versión de iOS 4, Apple comenzó a implementar un nivel de cifrado por hardware: luego de que el usuario crea la contraseña en el dispositivo, tiene la posibilidad de verificar la opción de Protección de datos habilitada (Data protection is enabled).

1. Ubicar la carpeta en donde se encuentran los archivos de resguardo efectuado con iTunes y copiarlos en un dispositivo de almacenamiento externo para su posterior análisis; recordar que no se debe trabajar sobre los archivos originales.
2. Efectuar su certificación matemática (hash).
3. Registrar y documentar el resultado.

Procedimiento para la recolección lógica de dispositivo iPhone, iPod táctil e iPad del resguardo efectuado con iTunes

Consideraciones previas a la recolección

Los dispositivos iPhones y la herramienta iTunes, opción Resguardo de iDevice (iDevice Backup), tienen la capacidad de resguardar los datos en los casos de fallas del hardware o del software o en las situaciones en que se configura el dispositivo a los valores iniciales de fábrica.

La adquisición de los datos se puede realizar tanto en los dispositivos bloqueados como en los no bloqueados. En el caso del dispositivo bloqueado, se procede de la misma forma que lo expresado anteriormente en la situación: “Comprobación del estado del código de acceso”.

Otra alternativa es a través de una orden judicial dirigida a la empresa Apple para que remueva el código de acceso de bloqueo del dispositivo.

1. Ubicar el archivo de certificados .plist del sistema operativo con el cual se efectuó la sincronización en la ruta del directorio o carpeta correspondiente.
2. Iniciar iTunes:

a. Menú Archivo Preferencias Dispositivos; se debe estar seguro de que la opción

Evitar la sincronización automática de iPods e iPhones se encuentre seleccionada.

3. Conectar el dispositivo a una computadora Mac por medio de un conector USB para iPod.
4. Aparecerá un ícono que representa al teléfono en la barra lateral izquierda debajo del menú Dispositivos.

Procedimiento para la recolección en iPhones

1. Visualizar la pantalla del dispositivo y registrar:

a. Fecha y hora del sistema.

2. A partir de los menús de Correo electrónico, Contacto y Agenda, registrar:

a. Las cuentas de correo electrónico.

3. Desde el menú Teléfono, registrar el número de teléfono.
4. Desde el menú General, opción Acerca de, registrar:

a. Tamaño del iPhone.
b. Versión del sistema operativo.
c. Empresa prestadora del servicio.
d. Número de serie del iPhone.
e. Modelo.
f. Direcciones MAC de Wi-Fi y Bluetooth.
g. IEMI (International Mobile Equipment Identity, Identidad de Equipo Móvil Internacional).
h. ICCID (Integrated Circuit Card ID, Identificador de tarjeta de circuito integrado).
i. Firmware.

Etapa de análisis de datos

Análisis de la primera partición del sistema de archivo de iPhone (liberado)

Consideraciones previas

La etiqueta de la primera partición es del tipo Big Bear 5B108, este número indica la versión de firmware o del sistema operativo. En esta primera partición, existe muy poca evidencia para el análisis del perito. La estructura es la siguiente:

Carpeta	Descripción
Aplicaciones	Es un enlace simbólico a /var/stash/ que se encuentra en la segunda partición.
bin	Contiene los archivos binarios de la línea de comando.
boot	Vacía.
cores, dev y developer	Hierarchical File System.
Damaged files	Contiene un enlace simbólico a un archivo de propiedad .plist y un archivo que es un remanente de la liberación del dispositivo.
Carpeta	Descripción
Etc.	Es un alias a la ubicación de la carpeta actual /private/etc., que contiene el archivo más importante, que es el de claves (passwd).
Lib	O Library, está vacía. Conocida como Local Library dentro de las versiones de sistema operativo: Tiger (10.4) y Leopard (10.5), contiene configuraciones del sistema y no posee información de evidencia.
Sbin	Contiene los archivos binarios de la línea de comando, comunes en OS X (fsck, fsck_hfs, fstyp, fstyp_hfs, kextload, launchd, mount, mount_hfs, newfs_hfs
Sms migration	Vacía.
System	/System/Library: Contiene un archivo .plist de configuración (USBDeviceConfiguration.plist), del dispositivo Apple Mobile y del protocolo de transferencia de imágenes (PTP-Picture Transfer Protocol).
	/System/Library/CoreServices, contiene un archivo .plist de versión del sistema (SystemVersion.plist).
	/System/Library/DataClassMigrator, contiene ejecutables para la

	libreta de contactos y para la migración del calendario.
	/System/Library/LaunchDaemon, contiene elementos que inician automáticamente. El primero es el archivo AddressBook.plist

1. Verificar los usuarios en el archivo passwd:

#vi /private/etc/passwd

El usuario root es el administrador de sistema.

El usuario mobile tiene el número de identificación de usuario (UID) 501 y el identificador de grupo 501, luego del nombre de usuario aparece el valor de hash que es el mismo que tiene el usuario root. El usuario mobile posee permisos y accesos limitados, por esta razón no se puede acceder a todos los datos en el análisis forense de un dispositivo no liberado, solamente se podrá acceder a los datos que tiene permitido el usuario mobile (contactos, registros de llamadas, SMS). Este usuario también interviene en la sincronización del dispositivo con iTunes y crea los resguardos.

a. Utilizar la herramienta John the Ripper[72] para analizar el archivo passwd, generalmente es "alpine". Esta clave es la misma tanto en el archivo firmware.dmg como en el /private/etc/passwd.

b. Verificar el duplicado del archivo passwd en la carpeta /private/etc/master passwd.

Análisis de la información adquirida o recolectada de los dispositivos iPhone

Procedimiento para la conversión de los archivos ".plists"

Consideraciones previas

Los archivos Property lists son utilizados por los programas de los dispositivos con iOS o Mac OS X, para almacenar datos, organizar y acceder a la información. En iPhone los archivos *.p* lists son utilizados por los programas para darle al usuario diferentes opciones, como por ejemplo, Safari, historiales web, marcadores, datos de YouTube, Favoritos, facilitando el desarrollo de aplicaciones para la telefonía móvil.

Estos archivos se conocen como plists. Su estructura es jerárquica y está compuesta por tres tipos de clases (Cocoa Foundation[73], Core Foundation[74] y XML). Estos archivos se pueden guardar en formato XML o en binario (utilizado en la arquitectura de capas del sistema operativo Mac OS X, en su capa de aplicación[75]). Al guardar ciertos archivos en binario se reduce su tamaño y se incrementa la eficiencia del desempeño de la aplicación. Si el archivo property list fue almacenado con una estructura del tipo XML, se puede visualizar con cualquier editor de texto. Si fue almacenado en binario,

deberá utilizarse una aplicación que convierta el archivo al formato ASCII; puede ser, por ejemplo, la herramienta Plutil[76] (Property List Utility). Esta herramienta puede, además, verificar el archivo para determinar una correcta sintaxis del lenguaje XML. Plutil está disponible para los sistemas operativos Windows, Linux o Mac OS X. El archivo .plist en binario no se puede leer y aparecer como "bplist00×". En Mac la herramienta se instala en el directorio /jusr/bin/pluti[77].

1. Instalar la herramienta Plutil acorde al sistema operativo de la estación de trabajo informático forense.
2. Situarse en el directorio donde se encuentra la herramienta, por ejemplo, en Mac o Linux y verificar errores de sintaxis en los archivos .plist:

$/usr/bin/plutil – lint nombredelarchivo.plist

3. Para convertir de binario a XML:

$/usr/bin/plutil – convert xml1 nombredelarchivo.plist

4. Para convertir de XML a binario:

$/usr/bin/plutil -convert binary1 nombredelarchivo.plist

5. Efectuar el análisis forense de los archivos .plist.

Procedimiento para el montaje de imágenes ".dmg*" en Mac*

Las imágenes adquiridas con extensión ".dmg" se deben montar en el sistema operativo para su posterior análisis. En los sistemas operativos de Mac se debe:

1. Seleccionar y abrir el archivo de la imagen y se abrirá automáticamente la aplicación DiskImageMounter.

Procedimiento para el montaje de imágenes ".dmg*" en Linux*

1. Verificar el tipo de archivo para determinar si está comprimido o no con el comando file:

#file iphone.dmg

2. Crear el directorio en donde se montará la imagen:

#mkdir /mnt/dmg

3. Montar la imagen, utilizando el comando mount, especificando el tipo de sistema de archivo, la opción ro de solo lectura y loop que permite la visualización de la imagen como un dispositivo de bloques:

#mount -t hfsplus -o ro, loop iphone.dmg /mnt/dmg

Procedimiento para el análisis del sistema de

archivos de las imágenes montadas en Linux – Recuperación de archivos fragmentados

Consideraciones previas

Una de las técnicas de análisis de las imágenes implica recuperar archivos, sin importar en qué estructura de archivos se encuentren. Para esto se utiliza una herramienta que efectúa la extracción de fragmentos de datos a partir de un gran conjunto de archivos (carving)[78], en particular de aquellas áreas del sistema de archivo que contienen espacio no asignado. El análisis se efectúa utilizando los valores de encabezado (inicio del archivo) y pie (fin de archivo) del tipo de archivo conocido.

Cada tipo de archivo posee una firma[79] o estructura de encabezado que lo reconoce como un determinado tipo de archivo, por ejemplo: jpg, doc, tga. De esta forma, se pueden recuperar archivos que no tienen una estructura de metadatos que apunten hacia ellos, ya sea porque las entradas a su sistema de archivo no se encuentran o están corruptas. La búsqueda se realiza bloque por bloque de datos desperdiciados que coincidan con el encabezado y pie de un determinado tipo de archivo.

Mientras los datos no sean sobrescritos o borrados de forma segura (sobrescrito con ceros), los datos borrados en cualquier tipo de dispositivo de almacenamiento pueden recuperarse con esta técnica, incluso en los teléfonos móviles.

Esta estructura analiza el contenido interno de los archivos en binario (inicio y fin de archivo). Por ejemplo, un archivo jpeg tiene por encabezado o inicio el valor 0x FF D8, finaliza con 0x FF D9 y tiene un tamaño de 166 kb; la herramienta buscará las porciones del archivo a partir del encabezado y si alcanza el tamaño máximo del archivo y no encuentra su fin, la herramienta se detiene en ese punto y no continúa la búsqueda[80].

En este procedimiento se utilizará la herramienta Scalpel (http://www.digitalforensicssolutions.com/Scalpel/) licencia GPL.

1. Determinar la ubicación de la imagen del dispositivo a analizar en la estación de trabajo informático forense.
2. Instalar la herramienta Scalpel[81]:

   #apt-get install scalpel
3. Descomprimir la herramienta y compilar:

   #Tar xzvf scalpel-2.0tar.gz

   #cd scalpel-2.0/

   #make
4. Configurar el archivo predeterminado (scalpel.conf) de tipos de archivos a

buscar, agregando tipos de archivos y guardarlo, como por ejemplo: iphone.conf, aquí se observa el archivo plist:

extensión tamaño encabezado pie plist y 4096 <plist </plist

5. Ejecutar el comando en Linux:

#scalpel –c iphone.conf /mnt/iphone.dmg

En forma predeterminada, Scalpel crea un directorio de salida con los resultados denominado “scalpel-output”. En esta carpeta se almacena el archivo audit.txt.

6. Editar el archivo audit.txt, se podrán visualizar los archivos recuperados y ordenados por tipo, por ejemplo[82]:

Tipo de archivo	Descripción
Amr (Adaptative Multi-Rate Codec)	Los archivos de voz se almacenan en este tipo de archivo. Es un archivo de audio comprimido.
Bplist/plist	Archivos binarios y XML plist.
Dat	Archivo de datos, el archivo de diccionario dinámico es un archivo que se encuentra en la categoría dat (contiene una lista de palabras claves propias del usuario).
Correo electrónico (Email)	Archivos de correo electrónico, generalmente existen muchos correos electrónicos dentro de un archivo email.
Gif/jpg/png	Aquí almacena imágenes, fotos e íconos.
Htm	Archivos del historial web en caché.
Mov	Videos tomados del dispositivo o sincronizados a este.
Doc/pdf	Archivos de texto.
Sqlitedb	Archivos de la base de datos SQLite; pueden ser consultados para recuperar datos.

Otras herramientas que efectúan la búsqueda de fragmentos de archivos

1. Foremost: Recupera archivos basados en su encabezado, pie y estructura de datos interna. http://foremost.sourceforge.net.

2. Scalpel4: Es una reescritura de la herramienta Foremost, mejora el desempeño y disminuye el uso de memoria. Es independiente del sistema de archivo (FATx, NTFS, EXT2/3).

3. Photorec5-Photorec: Recupera archivos perdidos de diferentes dispositivos

de almacenamiento (CompactFlash, Memory Stick, Secure Digital, SmartMedia, Microdrive, MMC, USB flash).

4. Adroit Photo Forensics: Utiliza diversas técnicas para la recuperación de imágenes y fotos, utiliza técnicas de búsqueda de fragmentos en forma inteligente (SmartCarving). Es un producto comercial. http://digital-assembly.com/products/adroit-photo-forensics/features/.

5. MacForensicsLab de SubRosaSoft.com Inc., comercial, con versión de prueba disponible para descargar en http://www.macforensicslab.com/ProductsAndServices/, recuperación de datos en plataformas Mac.

6. Forensic Tool Kit FTK de la empresa Access Data: Disponible como software de libre disponibilidad diseñado para Windows, pero se puede utilizar por medio de una máquina virtual para analizar el iPhone. http://accessdata.com/support/adownloads.

Procedimiento para el análisis del sistema de archivos de las imágenes montadas en Linux – Recuperación de archivos con cadenas de caracteres ASCII

Consideraciones previas

En los archivos recuperados, se pueden analizar las cadenas de caracteres de por lo menos cuatro de longitud ya sea de texto o binario. El comando strings[83] en Linux permite efectuar un análisis rápido de los datos binarios para determinar si la información es o no de interés para ser extraída en un archivo de datos (por ejemplo, datos relacionados con los números de teléfono, nombres, ciudades, coordenadas de GPS, fechas, etc.).

Las opciones recomendadas del comando son:

- -all, la cual examina el archivo completo.
- --radix, muestra el desplazamiento dentro del archivo en donde la cadena fue encontrada. El valor del desplazamiento puede ser expresado en: ---o para octal, x para hexadecimal, d para decimal.
- --encoding, selecciona el conjunto de caracteres de codificación de las cadenas de caracteres encontradas, los valores posibles son:

s = single-7-bit-byte caracteres (ASCII, ISO 8859, etc., predeterminado), S = single-8bit-byte caracteres, b = 16-bit bigendian, l = 16-bit littleendian, B = 32-bit bigendian, L = 32-bit littleendian[84].

1. Determinar la ubicación de la imagen iPhone.dmg.
2. Ejecutar el comando strings, direccionando la salida a un archivo de texto:

#strings --all –radix=x –encoding=b iPhone.dmg > resultados-strings.txt

3. Ejecutar el comando strings, para visualizarlo en pantalla:

#strings --all –radix=x –encoding=b iPhone.dmg | less

Procedimiento para la creación de una línea de tiempo

Consideraciones previas

La creación de la línea de tiempo permite determinar cuándo los archivos fueron compilados o abiertos. La primera fuente de información sobre la línea de tiempo es el metadato del sistema de archivo, que incluye la fecha de modificación (metadato), la fecha de acceso y modificación (contenidos) y la fecha de creación. Este metadato se refiere normalmente a las siglas de tiempo MAC o MACB, siendo B la referencia a la fecha de creación (Birthed). El sistema de archivo registra diferentes líneas de tiempo y adquieren diversas características en el análisis forense.

La herramienta TSK (The Sleuth Kit)*85*, de Brian Carrier, soporta diversos sistemas de archivos, incluyendo HFS y HFS+. En este procedimiento se utilizarán dos herramientas incluidas en TSK:

- Fls: se utiliza para listar los nombres de archivos y directorios en la imagen de disco. El comando busca información del sistema de archivos, del registro, de eventos y los guarda dentro de un formato de archivo del tipo cuerpo (body).
- Mactime: es una secuencia (script) de líneas que se utiliza para ordenar y unir los datos en una línea de tiempo.

1. En la estación de trabajo informático forense con el sistema operativo Linux: descargar la herramienta TSK (The Sleuth Kit) de http://www.sleuthkit.org./sleuthkit/download. php. En este sitio también se puede descargar la herramienta para Windows sleuthkitwin32-3.2.3.zip, debiendo ejecutarse en un emulador como Cygwin*86*.

2. Extraer la herramienta:

#tar xvf sleuthkit-3.2.3.tar

3. Compilar la herramienta, ubicándose en el directorio de extracción:

#cd sleuthkit-3.2.3/

#./configure

4. Instalar la herramienta:

#make install

La herramienta estará instalada en el directorio /usr/bin en Linux o en /usr/local/bin en Mac.

5. Crear la línea de tiempo con la herramienta fls[87], la cual recorrerá en forma completa la estructura de archivo de la imagen y listará cada archivo, tanto el asignado como no asignado; se puede utilizar con diferentes argumentos:

#fls –z EST3EDT -s 0 -m "/" -f hfs -r /iphone.dmg > iphone.body

El resultado devuelve el listado de todos los archivos, rutas y metadatos. El archivo no está organizado, aparecen varios textos con las líneas de tiempo.

6. Ejecutar el comando mactime[88] para ordenar y unir los datos, para obtener la información organizada de modo que el perito pueda analizar los datos obtenidos.

#mactime –b /iphone.body –z EST3EDT –d > iphone-lineatiempo.csv

7. Análisis de la línea de tiempo: abrir el archivo iphone-lineatiempo.csv en una planilla de cálculo. El perito podrá observar las acciones realizadas en el dispositivo y la fecha y hora en que ocurrieron. El cuerpo de la línea de tiempo creado por fls incluye diversos campos:

- Fecha: contiene la fecha y hora según lo especificado en la zona horaria (-z).
- Tamaño: tamaño de los archivos en bytes.
- Tipo: muestra la fecha de MACB que indica si el archivo fue modificado, accedido o creado:
  - m: indica modificado (metadata del archivo ha sido modificada).
  - a: acceso (al mismo archivo).
  - c: cambio o modificación (el contenido del archivo se ha modificado).
  - b: creación del archivo (birthed).
- Modo: contiene los permisos de archivo en el formato Unix. Cada archivo del sistema tiene un conjunto de permisos de lectura, escritura y ejecución (r: read, w: write, x: execute) para el usuario (user) o propietario del archivo, grupo (group) o conjunto de usuarios que tienen permisos sobre el archivo y otros (other), cualquier usuario que posea cuenta en el sistema.
- UID: identificador del usuario.
- GID: identificador del grupo.
- Metadato: se corresponde con número de inodo del archivo, el cual contiene información del archivo.
- Nombre de archivo: contiene la ruta de acceso al archivo y el nombre de este.

El perito deberá analizar el archivo acorde al requerimiento pericial, fecha y hora de determinado evento o conjunto de acciones, con el fin de no dedicarle demasiado tiempo a la lectura de toda la información generada en la línea de tiempo, por ejemplo:

- Visualizar una lista de archivos contenido en una carpeta /mobile/Media/DCIM. En el dispositivo iPhone esta carpeta contiene fotografías tomadas por el dispositivo o sincronizadas hacia el dispositivo. El perito puede seleccionar un determinado archivo IMG_0006.JPG. La línea de tiempo muestra que este archivo fue creado, accedido, y modificada su metadata a las 13:06:09; se sabe que las fotografías en la carpeta "100APPLE" son tomadas por la cámara del iPhone, se puede deducir que dicha foto fue entonces tomada en esa fecha y hora. El perito luego podrá visualizar la fotografía buscándola en el sistema de archivo.
- También puede visualizar si la aplicación de mail ha sido utilizada. Se mostrará, por ejemplo, una cuenta de correo iPhone forense de Ymail que fue creada y accedida a las 13:39. En otra línea de tiempo podrá ver la opción Descarga automática habilitada (AutoFetchEnabled), la cual fue actualizada cuando el correo electrónico se sincronizó entre el dispositivo y el servidor de correo, esto permitiría deducir que la cuenta de correo de Ymail estaba sincronizada con el dispositivo en esa fecha y hora.
- Otro ejemplo sería visualizar que la base de datos de notas fue modificada y que el metadato cambió; esto implica que una nota fue visualizada, creada o borrada.

Procedimiento para el análisis de las bases de datos de sms con un editor en hexadecimal

Consideraciones previas

El editor de hexadecimal permite visualizar con más detalle la información de la imagen adquirida, determinando firmas de archivos, datos eliminados o visualizando diferentes patrones. La herramienta a utilizar es un editor en hexadecimal[89].

1. Instalar en la estación de trabajo informático forense en Linux el editor en hexadecimal:

#apt-get install hexedit

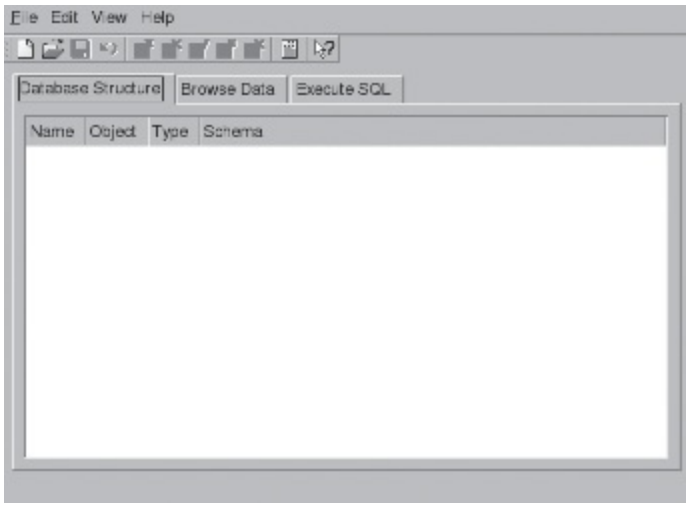
2. El comando strings se utilizará para acceder a la base de datos sms.db ubicada en el directorio /mobile/Library/SMS, para determinar si se encuentra algún mensaje de texto borrado. Por ejemplo: el mensaje de texto para 1551234567 fue borrado del iPhone, primero se utilizará el comando strings para ver si se encuentra el número de teléfono en el archivo SQLite. El comando accederá a la base de datos, la salida del comando será la entrada ("|" pipe o tubería) para el comando (grep) que filtra el número de teléfono que se le indica como patrón de búsqueda, luego la salida del filtro es la entrada del comando que cuenta las palabras, pero en este caso son líneas (word count, wc -l).

#strings --all –radix=x sms.db | grep –A 1 1551234567 | wc –l 6

3. El resultado es de 6 líneas o coincidencias, lo que indica que el número de teléfono se ha comunicado con el dispositivo iPhone. Para visualizar con más detalle el contenido de los mensajes, se incluye una línea de texto después del número de teléfono agregando la opción para filtrar "–A 1", la opción "–A" muestra el número de líneas coincidentes y para ver el resultado por pantalla se utiliza otra tubería "| less".

#strings --all –radix=x sms.db | grep –A 1 1551234567 | less

4. El resultado indica que el número está contenido en la base de datos SQLite[90] con los mensajes de texto. Para visualizar la base de datos, el visor de SQLite puede ser por línea de comando o el explorador del entorno gráfico:



Línea de comando	Descripción
#sqlite3 sms.db	Abre la base de datos para consulta.
sqlite>.help	Ayuda de las opciones de SQLite
sqlite>.tables	Listado de las tablas de la base de datos.
sqlite>.schema sms	Estructura de la base de datos.
sqlite>.modeline	Despliega los datos en líneas.
sqlite>select * from sms limit 1;	Consulta que indica seleccionar 1 registro (limit 1) de la base de datos sms y mostrar todas las columnas.
sqlite>.quit	Salir del programa.

5. A partir de la consulta anterior, se puede observar que existe una serie de campos en la base de datos sms. Por ejemplo: luego del número de teléfono que aparece en el campo dirección (address), está la fecha y hora (date), seguido del texto del mensaje (text). Para visualizar la fecha y hora de la base de datos sms.db, será necesario abrir este archivo en un visor en hexadecimal,

donde se mostrará la información en formato hexadecimal y las cadenas de caracteres ASCII en la columna de la derecha.

#hexedit sms.db

Se muestra la información y, al presionar la tecla Enter, se puede especificar el valor del desplazamiento obtenido en el paso 2 con el comando strings y ubicarse en el valor en hexadecimal donde se encuentra el número de teléfono 1551234567 y mensaje requerido. Al visualizar los datos en hexadecimal, luego del número de teléfono (5C75F607), aparece en los próximos cuatro bytes el campo de fecha y hora (timestamp) (4FAFB675). Este valor convertido a decimal sería: 1336915573, valor de la fecha y hora (timestamp) presentada en el formato de tiempo de Unix (Unix Epoch), que es el número de segundos contados desde el 1 de enero de 1970. Este valor se puede convertir a su equivalente, utilizando un convertidor en línea[91] de Unix, el cual devolverá el valor de fecha y hora en una forma inteligible: 13 May 2012 13:26:13 GMT. Por línea de comando en Mac:

#date –r @ 1336915573

En los dispositivos Apple se puede utilizar otro convertidor de tiempo CFA (Core Foundation AbsoluteTimeConverter), el cual mide el tiempo en segundos desde el 1 de enero de 2001 y es utilizado por la representación del tipo de datos de CFAbsoluteTime[92], este convertidor solo convertirá el formato de tiempo de OS X a un formato comprensible. Al convertir la fecha y hora, se debe tener especial cuidado en determinar cuál es el tipo de formato (Unix o CFA) ya que si se utiliza el convertidor de CFA con un valor de formato Unix, el día, el mes y la hora serán iguales, pero cambiará el valor del año. La fecha y hora de la base de datos sms.db están en el formato de tiempo de Unix, pero a veces muchas fechas y horas dentro de los archivos de un iPhone y otros dispositivos iOS están en el formato de tiempo OS X.

Procedimiento para el análisis de la estructura de directorios y partición de almacenamiento de datos en iPhone

Consideraciones previas

La segunda partición o también llamada partición de datos es, en un iPhone de 16GB, de 14.1 GB; en uno de 8GB, es de 7.07GB; se puede visualizar con la herramienta hdiutil imageinfo de Apple para trabajar con imágenes de disco. En esta partición está la información más importante para el perito. La estructura se compone de las siguientes carpetas y archivos[93]:

Carpeta/Archivos	Descripción
.DS_Store	Contiene información de la ruta del archivo borrado en la

	papelera.
.fseventsd	Contiene eventos producidos en el sistema de archivos.
.SymAVQSFile	Archivo no visible del antivirus Symantec.
.Trashes	Normalmente no contiene evidencia.
backups	Contiene archivos de resguardo del dispositivo.
cache	No contiene evidencia, pero existe evidencia de que el dispositivo fue liberado.
db	Contiene 3 subcarpetas: cliente dhcp (dhcpclient): contiene un archivo con las configuraciones de la red, dirección IP y direcciones física y lógica del router, reporte de pánico (Panic Reporter) y zona horaria (timezone): en esta carpeta están las configuraciones de fecha y hora del dispositivo. El archivo de hora local (localtime) es un alias del archivo de ejemplo: /usr/share/ zoneinfo/US/Eastern /usr/share/ es un alias en la primera partición de /var/stash, el cual es un puntero a la carpeta /stash en la raíz (root) de la segunda partición. Dependiendo de la zona horaria del dispositivo dubitado, la ruta común del archivo de información de zona es: /stash/share.spOSjO/zoneinfo.
empty folders	Carpetas vacías.
Keychains	Contiene dos bases de datos SQL, Keychain-2.db puede abrise con SQLite Database Browser29.
Lib	No contiene evidencia.
Local	No contiene evidencia.
Lock	No contiene evidencia.
Log	No contiene evidencia.
Logs	Contiene datos y subcarpetas. La subcarpeta Soporte Apple (Apple Support), tiene un archivo general.log. La subcarpeta banda base (baseband), es el área de comunicaciones que se relaciona con las funciones del celular y GPS y está vacía. La subcarpeta de reporte de fallas o caídas (Crash Reporter) posee registros de servicios como MediaServer (aplicación para transformar un iPhone o iPod en un disco externo), MobileSafari (navegador web) y reinicio de contador. Generalmente, contienen poca o ninguna evidencia.
Mobile	Presenta las subcarpetas: Biblioteca (Library), Media y Aplicaciones, aquí se encuentra gran cantidad de datos para

	analizar.
MobileDevice	Presenta una subcarpeta mobile, no contiene evidencia.
ManagedPreferences	No contiene evidencia la subcarpeta mobile.

*Existe un complemento para instalar en el navegador de Internet Mozilla que permite abrir cualquier extensión del tipo .sqlitedb, https://addons.mozilla.org/es-es/firefox/addon/sqlite-manage/ mayo 2012.

Carpeta/Archivos	Descripción
Root (usuario)	Contiene los mismos datos que los que se encuentran en la carpeta Mobile. La subcarpeta Biblioteca (Library) tiene otras subcarpetas: • Contactos, tiene una carpeta AddressBook.AddressBook con una base de datos vacía. • Caches, contiene el archivo cache.plist con la última posición del GPS y fecha y hora, el archivo: cells.plist, el archivo clients-b. plist, que contiene la lista negra o de bloqueo de aplicaciones, la carpeta Wi-Fi, que contiene archivos .dat que no son legibles. • Calendario, está vacía. • Cookies, Teclado, Preferencias, no contienen evidencia. • Bloqueo (Lockdown), contiene las claves privadas y públicas para activar el iPhone a través de iTunes en el archivo data_ Ark.plist; una vez activado, la información se almacena en este archivo. Safari no contiene evidencia.
Run	Contiene archivos que no presentan validez para la evidencia.
spool	
Stash	Contiene todas las aplicaciones que están en el iPhone.
Tmp	Denominada también actualización de instantáneas (Updated Snapshots), contiene archivos jpg de las capturas de pantalla con cierto valor para la evidencia.
Vm	

1. Analizar la carpeta de zona horaria (timezone). Los archivos de zona horaria no se pueden leer; para poder leer, por ejemplo, el archivo Eastern, se debe ejecutar:

#strings /usr/share/zoneinfo/UTC o ART http://www.timeanddate.com/worldclock/city.html?n=51

i. El resultado muestra la zona horaria y el EDT (Eastern Daylight Time) u Hora Oficial del Este, siendo esta la única referencia de la zona horaria encontrada. Registrar o capturar la información de la zona horaria.

ii. Registrar, documentar y/o capturar pantallas con la información requerida.

2. Visualizar con SQLite Database Browser la base de datos Keychain-2.db:

i. Ejecutar en Windows o Linux SQLite Browser.

ii. Abrir la base de datos Keychain-2.db.

iii. Navegar dentro de la base de datos.

iv. Seleccionar la tabla genp.

v. Registrar y/o capturar la información de las contraseñas de las cuentas, servicios y datos cifrados.

3. Visualizar el contenido del archivo general.log de la subcarpeta Apple Support:

i. Abrir el archivo general.log con un editor de texto.

ii. Registrar el contenido de la versión del sistema operativo, modelo y número de serie del iPhone, listado de fechas y horas y nombres de servicios.

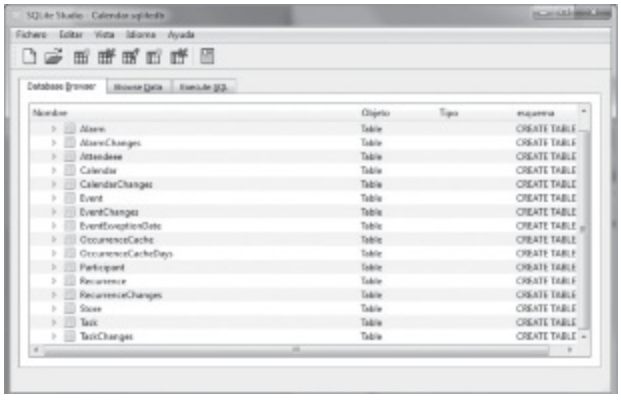
4. Analizar de la subcarpeta Biblioteca (Library):

i. Listar el contenido:

#tree –L Library/

Se visualizan los datos almacenados de: Contactos (AddressBook), Agenda (Calendar), Historial de llamadas (Call History), Notas (Notes), SMS y Mensajería de voz (Voicemail).

ii. Esta información se puede visualizar con el navegador de base de datos de SQLite (SQLite Database Browser) o SQLite Studio para Windows (http://sqlitestudio.one.pl).



Por ejemplo, en la base de datos de la Agenda (Calendar.sqlitedb), se puede observar las numerosas tablas que integran su esquema. En muchas oportunidades, es necesario acceder a cada una de las tablas para analizar sus

registros y determinar qué dato se puede recuperar.

iii. Seleccionar la opción Navegar datos (Browse Data), para acceder a una tabla determinada, por ejemplo: Suceso o Evento (Event) que contiene los eventos de la tabla Agenda (Calendar).

En esta tabla aparece un resumen del evento, como así también la fecha de inicio, fecha de finalización, zona horaria y otra información opcional que el usuario puede o no haber ingresado, por ejemplo, la localidad y la descripción. La fecha y hora utilizada en estos archivos es del formato tiempo de OS X Epoch. Por lo tanto, se utiliza el Convertidor de Tiempo de CFA (Core Foundation AbsoluteTimeConverter), acorde a lo explicado en el "Procedimiento para el análisis de las bases de datos de sms con un editor en hexadecimal".

iv. Analizar los archivos app en la forma de .plists. Estos archivos incluyen:

- Direcciones de Google Maps e historial.
- Marcadores del navegador de Internet Safari y su historial.
- Numerosas configuraciones de preferencia como números de marcado rápido.
- Datos de YouTube.
- Listado de aplicaciones instaladas.

a. Seleccionar el archivo .plist, y oprimir la barra espaciadora para obtener una vista previa del archivo y de su contenido.

b. Abrir el archivo en un editor de texto (en Mac, TextEdit o Text Wrangler) para efectuar búsqueda de palabras claves.

c. Ejemplo de visualización y análisis de datos del archivo .plist del historial del navegador de Internet Safari, la imagen de iphone.dmg es de solo lectura, por lo tanto se debe:

Copiar el archivo en otro directorio para convertirlo a un formato ASCII. Efectuar la conversión del archivo binario a XML:

#plutil –convert xml1 History.plist Editar el archivo en el formato XML.

En el archivo History.plist, cada sitio web visitado está organizado dentro de su propia sección, etiquetas: <dict> y </dic>. Entre estas dos etiquetas, la URL del sitio web y la fecha de última visita se muestran como una cadena. La fecha está en el formato de hora OS X Epoch y deberá ser convertida con el Convertidor de Tiempo de CFA (Core Foundation AbsoluteTimeConverter).

v. Registrar, documentar y/o capturar pantallas con la información requerida.

5. Analizar la subcarpeta Media. Esta carpeta contiene los archivos de:

- Fotografías.

- Videos.
- Música.
- Descargas.

i. Listar el contenido de la carpeta:

#tree –L 3 Media/

ii. Verificar el número de fotografías borradas. En la subcarpeta de Imágenes de cámara digital, DCIM (Digital Camera Image), cuando se toma una fotografía con la cámara del iPhone, se almacena como archivo jpg en forma predeterminada en la carpeta Media/DCIM/100Apple, con el nombre IMG_000X.JPG (la X sería el número a asignar y que se incrementa en 1 con cada nueva fotografía). Por ejemplo: IMG_0001.JPG, IMG_0002.JPG, IMG_0003.JPG. Si se borra una fotografía, por ejemplo, IMG_0002.JPG, este número no se reutilizará para otra fotografía; a la nueva que se tome con la cámara, se le asignará el número siguiente a la última fotografía tomada, por ejemplo: IMG_0004.JPG. De esta forma, el perito podrá identificar por el número de secuencia si alguna fotografía fue borrada.

iii. Verificar capturas de pantallas (screen shot). En el iPhone, si se mantiene presionada la tecla Inicio (Home) y se oprime el botón de Apagado/Encendido (Power), se produce una captura de pantalla que se almacena en Media/DCIM/999Apple. Esta carpeta no aparece cuando se lista el contenido de la carpeta Media.

iv. Verificar el contenido de la subcarpeta Fotos (Photos). Al sincronizar el dispositivo con la herramienta iTunes, las fotografías se almacenan en una base de datos dentro del iPhone en la subcarpeta Photos/Photo Database. En Mac, esta base de datos se puede abrir con la aplicación iPhoto para visualizar las fotografías.

v. Verificar el contenido de videos. En versiones anteriores a 3GS, los videos no se podían tomar desde el dispositivo sin descargar primero una aplicación que grabara video. Desde iPhone 3GS y posteriores, existe una cámara de video incorporada y se almacenan en la carpeta /DCIM/100/Apple junto con las fotografías.

vi. Verificar el contenido de música. La música sincronizada al dispositivo por medio de iTunes se almacena en la carpeta Media/iTunes_Control/Music, y los archivos actuales de audio en subcarpetas del tipo F00, F01, F02, F03.

vii. Registrar, documentar y/o capturar pantallas con la información requerida.

6. Análisis de la subcarpeta Aplicaciones (Applications) que contiene todas las aplicaciones precargadas en el iPhone y aquellas descargadas por medio de la compra o en forma libre a través de App Store.

i. Listar el contenido de la carpeta:

#tree –L 2 Applications/

Las aplicaciones están organizadas en: Documentos, que pueden tener valor como evidencia; Biblioteca (Library): aquí se encuentra el archivo .plist para aquellas aplicaciones; tmp: normalmente no tiene alojada información; iTunesMedata.plist: se encuentra el nombre de la aplicación, información de compra, nombre de usuario, dirección de correo electrónico, etc.

Por cada aplicación descargada se crea un único directorio en la carpeta Aplicaciones, la cual contiene el archivo ejecutable, documentación y cualquier otro archivo necesario para la ejecución de la aplicación. Se mantiene una estructura jerárquica general para todas las aplicaciones.

La aplicación se instala en la raíz de su carpeta. Este archivo es una agrupación que contiene varios archivos necesarios para la ejecución de la aplicación. Algunos archivos son comunes en las aplicaciones de terceros incluyendo Info.plist, ResourceRules.plist; sin embargo, el contenido de estos archivos es único para cada aplicación.

Cada aplicación contiene también directorios comunes a todas como: Documentos (Documents), Biblioteca (Library) y tmp (Temporal). Por ejemplo, en la carpeta Documentos de la aplicación Foursquare, se pueden almacenar lugares donde el usuario se registró; en la carpeta Documentos de la aplicación de Facebook, se puede guardar una base de datos de los amigos de Facebook. La carpeta Biblioteca (Library) contiene muchos subdirectorios: Cache, Cookies y Preferencias.

La carpeta llamada Preferencias contiene normalmente un archivo plist, por ejemplo: com.ApplicationName.plist. El archivo plist a menudo suele tener el usuario y a veces la clave que se utiliza para iniciar sesión en una determinada aplicación. Se puede recuperar también información como versión, descripción o información de GPS.

La carpeta tmp generalmente está vacía, debido a que el dispositivo no está siendo duplicado mientras se ejecuta la aplicación. Si un iPhone es liberado y físicamente se crea una imagen mientras una transacción está en progreso, es posible que algunos archivos temporales se almacenen en esta carpeta.

ii. Registrar, documentar y/o capturar pantallas con la información requerida.

7. Analizar los datos del sistema de posicionamiento global (GPS, Global Positioning System). Varias aplicaciones suelen preguntar al usuario si desean almacenar en caché su ubicación actual o las aplicaciones (app)[94], según su funcionalidad almacenarán los datos de GPS.

La mayoría de las aplicaciones de iPhone y de terceros almacenan la

información del GPS en el iPhone. Los programas de la cámara de fotografías o video y de Mapas de Google preguntan al usuario si desean guardar la información de la posición geográfica actual antes de tomar la fotografía o de buscar una dirección. El perito puede recuperar esta información guardada en el sistema de archivos del iPhone.

La aplicación de Mapas de Google (Google Maps) incluida en el dispositivo de iPhone almacena en forma predeterminada la ubicación actual del usuario, como así también cualquier otra ubicación solicitada en una búsqueda. Existen muchas aplicaciones que permiten rastrear las coordenadas del sistema de posicionamiento global.

El archivo consolidated.db es nuevo en la versión del iOS 4. El archivo almacena datos del GPS y Wi-Fi en una ubicación central, probablemente para mejorar la eficiencia del dispositivo, ya que puede enviar y recibir datos de posicionamiento accediendo a un único archivo. La base de datos contiene las siguientes tablas que ofrecen información significativa para el perito:

- WifiLocation
- CellLocacion

i. Listar el contenido de la base de datos consolidated.db con SQLite:

```
#sqlite3 consolidated.db
...
...
sqlite> .tables
Cell Fences
CellLocation Location
CellLocationBoxes LocationHarvest
CellLocationBoxes_node LocationHarvestCounts
CellLocationBoxes_parent Wifi
CellLocationBoxes_rowid WifiLocation
CellLocationCounts WifiLocationCounts
CellLocationHarvest WifiLocationHarvest
CellLocationHarvestCounts WifiLocationHarvestCounts
CompassSettings
sqlite>
```

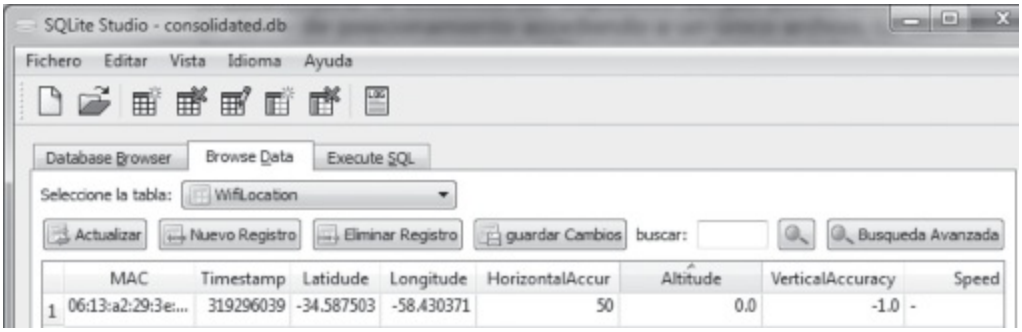
La tabla WifiLocation contiene las direcciones Wi-Fi (MAC)[95], fecha y hora, coordenadas de latitud y longitud y otros campos que pueden determinar en qué ubicación inalámbrica se pudo haber conectado el dispositivo a un cierto punto de acceso y a qué hora.

ii. Analizar las filas de la tabla WifiLocation con el navegador de base de

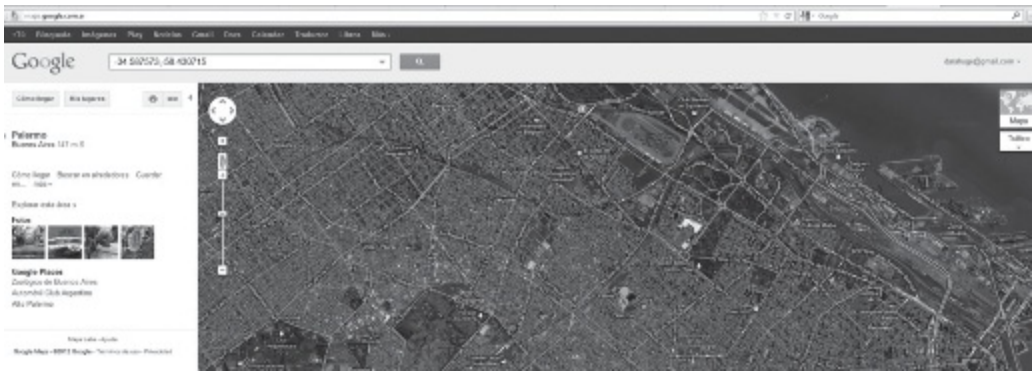
datos SQLite Database Browser:

- Abrir la base de datos consolidated.db.
- Seleccionar la ficha de Navegar datos (Browse Data).
- Seleccionar la tabla WifiLocation.

a. Elegir la primera fila y convertir primero la columna de fecha y hora (timestamp), por ejemplo: 319296039 que se encuentra en el formato de OS X Epoch, usando el convertidor de tiempo (CF AbsoluteTimeConverter)[96]. En el ejemplo sería: dom, 13 febrero 2011 08:20:39 -0500.



b. Observar las coordenadas de latitud y longitud para determinar la ubicación; se puede utilizar Google Maps (http://maps.google.com.ar/), ingresando la latitud y la longitud:



Analizar de la misma forma la tabla CellLocation; en esta tabla aparecerán los registros de las torres de celulares, fecha y hora (timestamp) y coordenadas del sistema de posicionamiento global (GPS). Con estos datos el perito podrá determinar a qué torre de celular el dispositivo estuvo conectado a una determinada hora. Los registros de las torres o antenas se clasifican de la siguiente forma:

- MCC: Código de país de telefonía móvil (Mobile Country Code)[97].
- MNC: Código de red de telefonía móvil (Mobile Network Code)[98].
- LAC: Código de área de la localidad (Location Area Code).
- CI: Identificador de célula (Cell ID).

iii. Correlacionar los datos de las tablas de WifiLocation y CellLocation para

obtener una idea de la posible ubicación geográfica del dispositivo en determinado horario.

Esta información no debe tomarse como definitiva, ya que ingresan un gran número de coordenadas al dispositivo al mismo tiempo, por lo tanto, de acuerdo a la fecha y hora y a la ubicación, el dispositivo puede estar en diferentes áreas al mismo tiempo, no obstante estas áreas se encuentran en un radio de pocos kilómetros entre una y otra.

Esto puede ocurrir porque la base de datos no se actualiza constantemente cada vez que surge una nueva área en el desplazamiento del iPhone. Puede haber 3, 4 o 20 ubicaciones que se actualizan al mismo tiempo. Por esta razón, es muy importante no basarse únicamente en la fecha y hora (timestamp) hasta que se efectúe una exhaustiva búsqueda de datos en la base de datos consolidated.db y se comprenda con claridad la información contenida, que debe ser manejada con cautela.

iv. Analizar otra área del sistema de archivo que contiene información sobre la posición geográfica y se encuentra en /private/var/root/Library/Caches/locationd.

- Listar el contenido de la carpeta locationd:

#tree locationd/

- Aparecen los archivos:
  - cache.plist
  - cells-local.plist
  - clients-b.plist
  - clients-b.plist
  - ephemeris
  - h-cells.plist
  - foo2.dat
  - stats.plidt
  - wifi
- Analizar el archivo cache.plist: contiene la información del último lugar en donde estuvo el celular antes de ser apagado o desconectado de la red Wi-Fi o celular en base a lo obtenido de las señales inalámbricas y ajuste del GPS (Core Location).

El archivo cache.plist muestra las coordenadas de latitud y longitud, las que se traducirán a una ubicación geográfica aproximada, sin embargo las fechas y horas (timestamp) no aparecen en el archivo. El perito puede determinar la fecha y hora en que se encontró el dispositivo en un lugar particular fijándose en la fecha y hora de modificación del archivo cache.plist.

La primera línea del archivo en la etiqueta <key>, muestra la última ubicación del dispositivo, posteriormente muestra la información de latitud y longitud que debe ser convertida para recuperar la actual dirección de la ubicación, se puede realizar con Google Maps o por un convertidor en línea para GPS (http:// boulter.com/gps/). El archivo contiene también los registros de la torre del celular y la fecha y hora en formato OS X Epoch, que el perito deberá convertir con un convertidor en línea.

<key>LLocationCore:klastFix</key>
<key>Latitude</key>
<key>Longitude</key>
<key>Suitability</key>
<key>SupportInfo</key>
<key>kCLSupportInfoCell</key>
<key>kCLSupportInfoCell_CI</key>
<key>kCLSupportInfoCell_Index</key>
<key>kCLSupportInfoCell_LAC</key>
<key>kCLSupportInfoCell_MCC</key>
<key>kCLSupportInfoCell_MNC</key>
<key>kCLSupportInfoCell_RSSI</key>
<key>kCLSupportInfoCell_TA</key>
<key>kCLSupportInfoCell_TATime</key>
<key>Timestamp</key>
<key>VerticalAccuracy</key>

· Analizar el archivo cells.plist: contiene numerosos registros de la ubicación de las torres o antenas de celular a las que se conectó el dispositivo, es similar a la tabla CellLocations que se encuentra en la base de datos consolidated.db:

(1) El archivo muestra una etiqueta <key> que se corresponde con los mismos números mostrados en la tabla CellLocations de la base de datos consolidated.db: MCC, MNC y LAC en hexadecimal: 0x2D47 (decimal 11591).

<key>722,340, 0x2D47 </key>

(2) La etiqueta <strings> contiene las coordenadas de latitud y longitud y la fecha y hora (timestamp) en el formato OS X Epoch (319296039) y equivalente a dom, 13 febrero 2011 08:20:39 -0500; es similar a los datos de la tabla CellLocations de la base de datos consolidated.db. Esto se debe a que las torres de celulares y los datos del GPS fueron consolidados en una base de datos en la versión del sistema operativo iOS 4. Para el perito es importante saber que esta información se encuentra en ambos archivos y se pueden recuperar los datos de la ubicación geográfica, sin tener en cuenta si la versión

del sistema operativo es iOS 4 o anterior:

<string> -34.587503, -58.43037, 319296039</string>

· Analizar el archivo clients-b.plist: contiene una lista negra (black list) de aplicaciones no autorizadas.

· Analizar el archivo h-cells.plist: contiene información adicional de los registros de las torres o antenas de celular, coordenadas del GPS y fecha y hora.

v. Registrar, documentar y/o capturar pantallas con la información requerida.

8. Analizar la base de datos de usuarios y claves. La base de datos keychain-2db está almacenada en la raíz del dispositivo en: /private/var/Keychain. La base de datos contiene seis tablas:

i. Genp, contiene evidencia de la lista de las cuentas que han iniciado sesión en el dispositivo, de los puntos de acceso inalámbrico al que se conectó el dispositivo, de inicio de sesión en el dispositivo (passcode) y de cualquier otra aplicación descargada al dispositivo que requiera el uso de la base de datos Keychain para almacenar las credenciales de inicio de sesión. Cada cuenta está formada por el nombre de la cuenta de usuario, su descripción y un campo de datos que contiene la clave encriptada. La estructura de la tabla genp es la siguiente:

· Cuenta (Acc): nombre de usuario, conexión inalámbrica Wi-Fi, dirección de correo electrónico.

· Descripción de la cuenta (svce): correo de voz mejorado, com.apple.itunestored. keychain, aplicaciones de terceros.

· Datos (data): contiene generalmente la clave cifrada.

· Nombre de grupo de acceso (agrp): el nombre del grupo de acceso de Keychain

se utiliza para compartir datos entre aplicaciones.

ii. sqlite_sequence

iii. Inet, contiene evidencia de cualquier cuenta de correo electrónico que se haya sincronizado con el dispositivo a través de la cuenta de la aplicación de correo. La información que se puede encontrar en cada cuenta es la siguiente:

· Cuenta (Account): dirección de correo electrónico o dominio/nombre de usuario, aparece en la columna “acct”.

· Servidor de correo electrónico al que se conectó el dispositivo, aparece en la columna “srvr”.

· Protocolo utilizado para conectarse al servidor de correo electrónico (imap, smtp, pop3, https, etc), aparece en la columna “ptcl”.

- Número de puerto (143, 25, 443, etc.), aparece en la columna “port”.
- Datos (clave encriptada), aparece en la columna “data”.

iv. Cert

v. Keys

vi. Tversion

Aunque las dos tablas, genp e inet, son las que contienen datos de interés para el perito, el análisis del resto de las tablas también es conveniente para descartar cualquier pérdida de información no verificada.

Las claves en ambas tablas, genp e inet, están encriptadas y existen dos formas de desencriptarlas. En la versión iOS 4, el cifrado se realiza a nivel del dispositivo. Cuando se inicia un resguardo del dispositivo sin encriptar el archivo Keychain es encriptado utilizando las claves por hardware almacenadas en el dispositivo, al abrir la base de datos la mayor parte de la información se puede ver, pero las claves permanecen encriptadas.

Si el resguardo se realiza de manera encriptada, el archivo de Keychain se encriptará utilizando las claves por software generadas a partir de la clave de resguardo.

Una de las formas de desencriptar las claves en el archivo Keychain y visualizar el texto en claro es utilizando la herramienta comercial para descifrar claves de iPhone Elcomsoft Phone Password Breaker[99]. Esta técnica es aplicable solamente en dispositivos que poseen una versión de sistema operativo (firmware) 4.0 o superior.

Otra de las formas de desencriptar requiere tener el dispositivo y el conocimiento para efectuar su liberación (jailbreak):

- Efectuar el proceso de liberación.
- Instalar un servidor de SSH, intérprete de comandos seguro (secure Shell) para permitir que el software funcione en el iPhone.
- Copiar el script de acceso a la base de datos Keychain, que permitirá comunicarse con la base de datos y extraer información y contraseñas.

Esta técnica funciona con la versión iOS 4 porque la clave se puede generar dentro del dispositivo sin necesidad de conocer el código de acceso del dispositivo[100].

La herramienta keychain_dumper, desarrollada por Patrick Toomey[101], se ejecuta desde el dispositivo, que debe estar previamente liberado (jailbreak), y permite desencriptar las contraseñas almacenadas en Keychain del tipo genéricas y de Internet. Según las opciones de ejecución de la herramienta se puede descifrar información adicional contenida en la base de datos Keychain. La herramienta se puede descargar de https://github.com/ptoomey3/Keychain-Dumper. El dispositivo iPhone solo

permite la instalación de aplicaciones que poseen certificados. El perito deberá seguir los siguientes pasos para su instalación y ejecución en el iPhone:

· Liberar el dispositivo.

· Descargar la herramienta.

· Leer el archivo Readme.md (https://github.com/ptoomey3/Keychain-Dumper/blob/master/README.md) para los detalles de instalación.

· Verificar la existencia de la herramienta ldid (necesaria para la firma de las aplicaciones a instalar en el dispositivo liberado, que genera hash del tipo SHA-1 y que son verificados por el núcleo del sistema operativo del iPhone de Apple). Para instalar ldid, descargar Aptbackup del paquete de Cydia, y ejecutar en el dispositivo el siguiente comando:

$apt-get install ldid (también se puede realizar desde el programa Terminal Móvil de Cydia, ver conexión remota a un dispositivo liberado en el etapa de adquisición en el apartado "Ejemplo del método de duplicación en un dispositivo liberado", 2).

· Subir la aplicación keychain_dumper al iPhone en /usr/bin, a través de scp (ver conexión remota a un dispositivo liberado en el etapa de adquisición en el apartado "Ejemplo del método de duplicación en un dispositivo liberado", 4).

· Verificar los modos de uso de la aplicación keychain_dumper con sus diferentes opciones (https://github.com/ptoomey3/Keychain-Dumper).

· Descargar entitlements (grupos de acceso) o autorizaciones, de la base de datos

Keychain:

#./keychain_dumper –e> /var/tmp/entitlements.xml

· Firmar el archivo entitlements.xml dentro de keychain_dumper (http://www. saurik.com/id/8):

#ldid –S/var/tmp/entitlements.xml keychain_dumper

· Mostrar los resultados en pantalla o redireccionarlos a un archivo de texto donde se visualizará el texto en claro de las cuentas y las contraseñas:

#./keychain_dumper > keychain_resultados.txt Service: Facebook

Account: grupo-tr abajo@gmail.com

Entitlement Group: R96HGCUQ8V.* Label: Generic

Field: data

Keychain Data: LaClaveEs613

viii. Registrar, documentar y/o capturar pantallas con la información requerida.

9. Analizar capturas del estado del dispositivo o instantáneas (Snapshots); se producen cuando el usuario selecciona el botón Inicio (Home) para salir o

abandonar algún programa y regresar a la pantalla principal del dispositivo. Esto dependerá del tipo de aplicación y de cómo fue diseñada por el desarrollador, si está habilitada la instrucción de tomar instantánea en el programa de forma predeterminada, entonces quedarán almacenadas en el dispositivo y se podrán recuperar.

Las imágenes se almacenan en /private/var/mobile/Library/Cache/Snapshots, el nombre del archivo puede ser del tipo: com.apple.mobilemail-Default.jpg o com.apple. mobilesafari-Default.jpg o com.apple.mobilenotes-Default.jpg. Estos archivos suelen tener información útil para el perito, ya que se van tomando en forma aleatoria en diversos momentos de la ejecución de la aplicación. Por ejemplo, al dejar el programa de correo electrónico y volver al menú principal. En el caso de las aplicaciones de terceros, y si esta opción de tomar instantáneas está habilitada, las imágenes de la captura se guardarán en el directorio de la propia aplicación.

La técnica de recuperación de las imágenes es a través de una herramienta que efectúe la búsqueda de fragmentos de archivos (carving), ya que las imágenes pueden estar en espacios no asignados, aparte de encontrarse en la carpeta Snapshots.

a. Ejecutar Scalpel, Foremost u otra herramienta similar acorde al "Procedimiento para el análisis del sistema de archivos de las imágenes montadas en Linux. Recuperación de archivos fragmentados". Las imágenes se guardarán en una de las carpetas "jpg".

b. Registrar, documentar y/o capturar pantallas con la información requerida.

10. Análisis de la información de los dispositivos emparejados (Paired Devices). En determinadas requisitorias, el perito deberá determinar el par de dispositivos sincronizados. Esta tarea puede realizarse a partir de los registros de sincronización de dispositivos almacenados en uno de ellos. Por ejemplo, cuando el iPhone se sincroniza con la computadora, se guarda una clave en ambos equipos permitiendo que ambos dispositivos compartan información. Si el certificado del iPhone coincide con el de la computadora, entonces los dispositivos están emparejados o sincronizados. Esta información se encuentra en el iPhone en un archivo del tipo plist.

Existe un archivo por dispositivo y se encuentra en:

- iPhone: /var/root/Library/Lockdown/pair_records
- Mac OS X: /Users/username/Library/Lockdown/
- Windows XP: C:\DocumentsandSettings\username\LocalSettings \ApplicationData\AppleComputer\Lockdown

· WindowsVista: C:\Users\username\AppData\Roaming\AppleComputer\Lockdown

Pueden aparecer varios archivos y el perito deberá analizar la modificación de la fecha y hora para determinar qué dispositivo analizar.

a. En el iPhone, abrir el archivo plist.

b. Buscar en el formato XML del archivo la clave DeviceCertificate, certificado del dispositivo, esta clave está codificada en base 64.

c. Decodificar el certificado con un decodificador en línea (http://ostermiller.org/ calc/encode.html, http://www.motobit.com/util/base64-decoder-encoder.asp). El resultado obtenido es el certificado.

d. En la computadora, buscar el certificado; su ubicación en la estructura de archivos y directorios dependerá del sistema operativo instalado en la computadora dubitada.

Comparar el certificado del archivo plist del iPhone con el de la computadora, con la herramienta diff, en Windows[102] se puede utilizar para comparar archivos la herramienta de código abierto WinMerge (http://winmerge.org/):

#diff iPhoneplist computadoraplist > resultados.txt

Si los resultados de los certificados coinciden, entonces los dos dispositivos están emparejados o sincronizados.

e. Registrar, documentar y/o capturar pantallas con la información requerida.

Procedimiento para el análisis de las aplicaciones preinstaladas en iPhone

Consideraciones previas

En el dispositivo iPhone se encuentra una serie de aplicaciones que ya vienen incorporadas por la empresa Apple. Cada aplicación presenta una estructura determinada, la base de datos o archivos plist y un conjunto de datos a recuperar por parte del perito que son significativos para el análisis de la información.

1. Analizar la aplicación SMS:

Ubicación en la estructura de archivos: /private/var/mobile/Library/SMS:

· Borradores (drafts): Contiene los mensajes SMS en borrador en la forma de messages.plist

· Partes (parts): Contiene archivos adjuntos a los mensajes SMS o MMS, la mayoría .jpg

· Base de datos de SMS (sms.db): Es la base de datos que contiene los

mensajes de texto y de multimedia, como así también aquellos que fueron borrados, es el archivo más importante en este directorio.

· Tablas que componen la base de datos de SMS:

– message, contiene evidencia de los mensajes de textos enviados o recibidos.

– sqlite_sequence

– msg_group

– group_member

– msg_pieces, contiene evidencia del contenido del texto de los MMS.

2. Identificar y analizar los campos de las columnas en la tabla mensajes (message), visualizar la tabla con el navegador de base de datos SQLite:

· Identificador de fila (ROWID): Número secuencial asignado para cada mensaje.

· Dirección (address): Los número de teléfono desde o hacia donde se envió el mensaje, si está en blanco el mensaje es del tipo multimedia, el número de teléfono aparece en el campo receptor (recipient).

· Fecha (date): Fecha y hora (timestamp) en el formato de Unix Epoch, requiere conversión, indica la fecha y hora del mensaje en que fue enviado o recibido.

· Texto (text): Contenido del mensaje, si es un MMS, este campo está en blanco.

· Banderas (flags): Indica si el mensaje fue recibido (valor = 2) o enviado (valor = 3).

• Replace: Desconocido y siempre tiene valor cero.

· Svc_center: desconocido y siempre tiene valor null.

· Identificador de grupo (group_id): Un valor entero asignado a un único número de teléfono. Todos los mensajes enviados a o recibidos de un número en particular son considerados un grupo y por lo tanto se le asigna un identificador de grupo.

· Identificador de asociación (asociation_id): Desconocido. Puede tener un cero y otras veces la misma fecha y hora en formato Unix Epoch que la que aparece en el campo fecha (date).

· País (country): Muestra el código del país, .ar para Argentina.

· Receptor (recipients): Para un mensaje de texto este campo está vacío, si es del tipo multimedia, el campo contiene el número de teléfono desde o hacia donde se mandó el mensaje. El número de teléfono está codificado en XML.

· Leído (read): Indica si el mensaje fue leído por el usuario con valor =1.

a. Registrar, documentar y/o capturar pantallas con la información

requerida.

3. Identificar y analizar los campos de las columnas en la tabla partes del mensaje (msg_ pieces), visualizar la tabla con el navegador de base de datos SQLite:

- Identificador de fila (ROWID): Número secuencial asignado para cada mensaje.
- Identificador de mensaje (message_id): Un identificador único asignado a cada mensaje. Un registro MMS tiene tres filas: la primera tiene valor en blanco/cero/ null, la segunda contiene el mensaje dentro de un texto o documento plano y la tercera es la imagen que fue adjuntada. Las tres filas conforman un mensaje MMS, y tendrán el mismo identificador de mensaje. El perito debe comprobar que el identificador del mensaje en la tabla msg_pieces coincide con el identificador de fila en la tabla de mensajes (message).
- Datos (data): El contenido de texto enviado en el MMS con el adjunto.
- Tipo de contenido (content_type): Puede ser null, texto (plano), imagen (jpeg), video (3gpp) o aplicación (smil).
- Versión (versión): Puede ser 0 o 1, posiblemente se refiera a la versión del plist mostrada en el campo receptor de la tabla mensaje.
- Content_loc: Este campo puede ser de valor = null o mostrar texto en el formato text_###.txt o imagen en el formato IMG_###.jpg. El nombre de IMG no es el nombre de la imagen actual que está almacenada en el iPhone (IMG_0001, IMG_0002, etc.).
- Encabezados (headers): Tiene valor null.

a. Registrar, documentar y/o capturar pantallas con la información requerida.

4. Analizar la aplicación de manejo de preferencias BossPrefs; aparece cuando el dispositivo está liberado.

Ubicación en la estructura de archivos:

/private/var/mobile/Library/BossPrefs df.txt

a. Visualizar el contenido del archivo df.txt con un editor de texto. El archivo muestra las particiones y puntos de montaje en el iPhone.

/dev/disk0s1 devfs

/dev/disk0s2

b. Registrar, documentar y/o capturar pantallas con la información requerida.

5. Analizar la aplicación Contactos (Address Book), la cual contiene dos archivos: AddressBookimages.SQLitedeb y AddressBook.SQLitedb que contiene la base de datos de los contactos sincronizados con Mac.

Ubicación en la estructura de archivos:

/private/var/mobile/Library/Address Book

a. Analizar la base de datos AddressBook.SQLitedb, visualizar las tabla con el navegador de base de datos SQLite:

– Si es requerido, exportar la base de datos a otro archivo desde el navegador de base de datos SQLite:

(1) Seleccionar Archivo | Exportar | Tablas como CSV, seleccionar la tabla ABPerson, indicar el lugar de almacenamiento en donde se exportará el archivo y el nombre y oprimir Guardar. Ubicar el archivo .csv exportado y abrirlo con una planilla de cálculo.

– Identificar los campos de la tabla ABPerson; contiene información del contacto e incluye la fecha de creación y modificación.

b. Registrar, documentar y/o capturar pantallas con la información requerida.

6. Analizar la aplicación Calendario o Agenda (Calendar), contiene los eventos almacenados en el iPhone que fueron ingresados manualmente por el usuario o sincronizados utilizando una aplicación de correo electrónico, con la cuenta MobileMe u otro programa.

Ubicación en la estructura de archivos:

/private/var/mobile/Library/Calendar:

Tablas que componen la base de datos de Calendar.sqlitedb:

- Alarm • OccurrenceCache
- AlarmChanges • OccurrenceCacheDays
- Attendee • Participant
- AttendeeChanges • Recurrence
- Calendar • RecurrenceChanges
- CalendarChanges • Store
- Event • Task
- EventChangesT • askChanges
- EventExceptionDate_ • Sqlite

7. Identificar y analizar los campos de las columnas en la tabla Evento o Suceso (Event), contienen información relevante para el perito; visualizar la tabla con el navegador de base de datos SQLite:

- Identificador de fila (ROWID): Número secuencial asignado para cada evento del calendario.

- Resumen (summary): El contenido de texto actual del evento del calendario.

• Ubicación (location): Un campo opcional donde el usuario puede ingresar el lugar del evento.

• Descripción (description): Campo opcional donde el usuario puede ingresar una descripción del evento.

• Fecha de inicio (start_date): La fecha y hora de inicio del evento en formato OS X Epoch; convertir esta fecha con el convertidor explicado en procedimientos anteriores.

• Inicio zona horaria (start_tz): La zona horaria en la que está configurado el dispositivo.

• Fecha de finalización (end_date): La fecha y hora de finalización del evento en formato OS X Epoch, convertir esta fecha con el convertidor explicado en procedimientos anteriores.

• Identificación del calendario (calendar_id): El identificador asignado al calendario en donde está almacenado el evento. El usuario pudo sincronizar múltiples calendarios que serán mostrados en la tabla Calendario (Calendar). El identificador de fila asignado (ROWID) a cada calendario es también su identificador de calendario (calendar_id) en la tabla Evento (Event).

a. Registrar, documentar y/o capturar pantallas con la información requerida.

8. Analizar de la aplicación Historial de llamadas (Call History); contiene las llamadas realizadas o recibidas por el usuario, junto con otros metadatos que son de particular interés para el perito.

Ubicación en la estructura de archivos:

/private/var/mobile/Library/CallHistory:

Tablas que componen la base de datos de call_history.sqlitedb:

• Call.

• Sqlite_sequence: Rastrea el identificador de fila más recientemente usado para ciertas tablas en la base de datos.

• Data.

9. Identificar y analizar los campos de las columnas en la tabla Llamada (Call). En esta tabla se encuentra mucha información de interés para el perito; visualizar la tabla con el navegador de base de datos SQLite:

• Identificador de fila (ROWID): Número secuencial asignado para cada registro de llamada, la tabla Secuencia Sqlite (Sqlite_sequence) rastrea el identificador de fila más recientemente usado para ciertas tablas en la base de datos.

• Dirección (address): El número de teléfono desde o hacia donde tuvo lugar la llamada. Si está en blanco, es probable que sea una dirección desconocida.

· Fecha (date): Fecha y hora de la marca de tiempo en el formato Unix Epoch. Convertir con el convertidor en línea y determinar la fecha y hora en que una llamada se realizó o se recibió.

· Duración (duration): Muestra la duración de llamada en segundos. Si el valor aparece en cero, indica que fue una llamada perdida.

· Banderas (flags): Muestra si la llamada fue entrante (valor = 4) o saliente (valor = 5).

· Identificador (id): Al realizar la llamada a un teléfono cargado en contacto dentro de la libreta de direcciones, el identificador representa a ese contacto o identificador de fila (ROWID) asignado a dicho contacto.

· Nombre (name): Tiene valor null.

· Código de país (country_code): Es el código MCC de país móvil descripto en el Análisis de posicionamiento global (GPS). Para la República Argentina es 722.

a. Verificar el número de registros (logs); en iPhone el límite del historial de llamadas es cien. Se almacenan en la tabla Llamada (Call); si superan este valor se eliminará el registro más antiguo y ocupará el lugar el registro de la nueva llamada entrante o saliente. El perito solo podrá observar cien registros en la tabla; para visualizar registros más viejos se pueden utilizar las herramientas de análisis específico (comando strings, editor en hexadecimal, Foremost, Scalpel).

b. Registrar, documentar y/o capturar pantallas con la información requerida.

10. Análisis del archivo de historial de Teclado y Diccionario del Usuario (User dictionary/ keyword): Contiene un diccionario dinámico que se genera en el momento en que el usuario ingresa una palabra (escrita en el mensaje de texto, correo electrónico, nota, calendario o agenda, etc.) en el iPhone; es único para ese usuario. Funciona como un registro de teclado (keylogger) de iPhone. No es una base de datos, ni tampoco un archivo plist, solo es un archivo de datos; su visualización depende del contenido, considerando que almacena texto, se puede abrir en un editor de texto. Una vez abierto, todas las palabras ingresadas aparecen en el archivo que resulta de difícil análisis a simple vista. En este archivo no se encuentran las claves ingresadas para el inicio de sesión en diversas aplicaciones.

Ubicación en la estructura de archivos:

/private/var/mobile/Library/Keyboard:

· Archivo de almacenamiento: dynamic-text.dat

12. Identificar y analizar el archivo dynamic-text.dat:

#strings dynamic -text.dat | less o

#strings dynamic -text.dat > resultado-dynamic.txt

a. Efectuar búsquedas de palabras claves en el archivo resultado-dynamic.txt.

b. Registrar, documentar y/o capturar pantallas con la información requerida.

13. Visualizar el archivo de imagen del fondo del escritorio:

/private/var/mobile/Library/LockBacground.jpg

a. Registrar, documentar y/o capturar pantallas con la información requerida.

14. Analizar la subcarpeta Preferencias (Preferences); contiene numerosos archivos .plist: Ubicación en la estructura de archivos:

/private/var/mobile/Library/Preferences: AccountName String

AccountPath String

AccountType String

AuthenticationScheme String

DraftsMailboxName String

FullUserName String

IsActive String

LastSequenceNumber Number SentMessagesMailboxName String StoreDraftsOnServer String StoreSentMessagesOnServer String StoreTrashOnServer String

TimeLastProvisioned Number

TrashMailboxName String

UDPHost String

UDPPort Number

uniqueld String

Username String

Dictionary

AccountName String

AccounthPath String AccountServerCertificate Data

AccountType String

DeletionPolicy String

DraftsMailboxName String

a. Analizar el contenido de los archivos plist.

Los archivos plist en forma predeterminada se encuentran en el formato binario. En Mac se pueden abrir y examinar con facilidad oprimiendo la barra espaciadora. Si el perito intenta visualizarlos en un editor de texto, los datos no se verán apropiadamente, por lo tanto deberá convertir los archivos plist a

XML, donde la información se encuentra más organizada.

- Visualizar el contenido del archivo plist, convertirlo de binario al formato XML, utilizando la herramienta Plutil o cualquier otra disponible.
- Analizar el archivo com.apple.carrier.plist: Es un alias que apunta a un archivo en la primera partición llamado /System/Library/CarierBundles/2624/carrier. plist. El número indica el código de área de la localidad.

b. Registrar, documentar y/o capturar pantallas con la información requerida.

15. Analizar las cuentas de correo electrónico (Mail). En la carpeta Mail, se encuentra el archivo Accounts.plist, que muestra la información de las cuentas de correo electrónico del iPhone. El archivo puede contener muchas carpetas con los mensajes de correo electrónico: cuentas POP e IMAP de Microsoft Exchange, Gmail, Yahoo, MobileMe, AOL, Fibertel, etc., cada una con sus respectivas carpetas de Buzón de entrada, Salida, Enviados y Papelera. La herramienta comercial Emailchemy (http://www.weirdkid.com/) permite realizar la extracción de las cuentas de correo electrónico y convertirlas para su posterior visualización en el correo electrónico del sistema operativo Mac, también está disponible para Linux y Windows. La herramienta comercial File Juicer (http://echoone.com) con versión de prueba para descargar permite extraer correo del tipo IMAP (además de otros formatos de archivos: JPEG, PNG, GIF, PDF, BMP, WMF, EMF, PICT, TIFF, Flash, ZIP, HTML, WAV, AVI, MOV, MPEG, WMV, MP3, MP4, AU y AIFF).

a. Editar el archivo Account.plist y determinar las cuentas de correo existentes.

b. Registrar, documentar y/o capturar pantallas con la información requerida.

16. Analizar la base de datos contenida en la carpeta Mail. Al sincronizar las cuentas de correo electrónico a un dispositivo, la información de las cuentas y el contenido de los mensajes se almacenan dentro del dispositivo.

Ubicación en la estructura de archivos:

/private/var/Keychain:

· Keychain-2db: Contiene la información de las cuentas de correo electrónico.

/private/var/mobile/Library/Mail/:

· Carpeta de correo (Mail folder): Para cada cuenta de correo electrónico sincronizada al dispositivo (contiene los archivos .emlx y emlxpart).

· Descarga automática activada (AutoFetchEnabled).

· Índice del sobre (Envelope Index).

· Archivo Account.plist: Contiene información de todas las cuentas de correo de iPhone.

/private/var/mobile/Library/Webkit/Databases:

· Databases.db: Contiene una lista de archivos de bases de datos de Webkit en el dispositivo.

· Carpeta mail.yahoo.com: Contiene una base de datos .db con los datos relacionados con la cuenta de correo electrónico de Yahoo.

· Carpeta mail.google.com: Contiene una base de datos .db con los datos relacionados con la cuenta de correo electrónico de Google.

· Otras carpetas con la url del proveedor de correo electrónico.

17. Analizar la base de datos de usuarios y claves. La base de datos keychain-2db, almacenada en la raíz del dispositivo, en: /private/var/Keychain. Ver el punto 8 del "Procedimiento para el análisis de la estructura de directorios y partición de almacenamiento de datos en iPhone".

18. Análisis de la base de datos databases.db:

Tablas que componen la base de datos databases.db:

· Databases

· Origins

· Sqlite_sequence

19. Identificar y analizar la tabla Base de datos (databases). Esta tabla contiene datos únicos y el perito puede observar varios archivos de la base de datos Webkit en el dispositivo. Si el usuario sincronizó ambas cuentas de correo de Yahoo y Gmal, la carpeta que contiene cada base de datos se encuentra en la tabla orígenes (origins). Un ejemplo sería: http_m.mg.mail.yahoo.com_0 y https_mail.google.com_0, estas son subcarpetas que contienen archivos de base de datos. El perito puede ver en la tabla Base de datos (databases) la dirección de correo electrónico del usuario. En el caso de la carpeta de http_m. mg.mailyahoo.com_0>0000000000000006.db, la base de datos dentro de la carpeta del correo de Yahoo contiene información importante, incluyendo las direcciones de correo electrónico de los emisores y receptores del correo electrónico, los asuntos, fecha y hora (timestamp) y datos parciales del contenido.

Tablas que componen la base de datos de las cuentas de correo:

· _webKitDatabaseInfoTable_

· Action

· Message, contiene evidencia

· Folder, contiene evidencia

- Vfolder
- Contact

20. Analizar las tablas carpeta (folder) y mensaje (message), visualizar las tablas con el navegador de base de datos SQLite.

La tabla mensaje (message) contiene:

- Asunto del mensaje.
- Contenido parcial del mensaje, columna (snippet).
- Dirección de correo electrónico del receptor y emisor.
- Fecha y hora en el formato Unix Epoch. Utilizar el convertidor de fecha y hora para determinar la fecha y hora de recepción del mensaje.
- La columna tiene adjunto (hasAttachment); si aparece el valor = 1 tiene adjunto, el valor = 0 indica que no tiene archivo adjunto.

La tabla carpeta (folder) contiene:

- Una lista de todas las carpetas de una determinada cuenta de correo electrónico: Buzón de entrada, Enviados, Papelera, estas carpetas no son tan importantes. El perito debe fijarse en las carpetas creadas por el usuario que se encuentran también en esta tabla. Aparte de los nombres de las carpetas, se encuentra el total de los mensajes dentro de cada una de las carpetas y el número de mensaje.

a. Analizar la base de datos dentro de la cuenta de correo electrónico, por ejemplo de Gmail:

https_mail.google.com_0>0000000000000006.db.

La base de datos contiene las direcciones de correo del emisor y receptor, asunto, fecha y hora, y parte del contenido del mensaje.

La tabla https_mail contiene:

- _webKitDatabaseInfoTable_
- action_queue_11_crf
- cached_queries
- hit_to_data
- cached_conversation_headers
- cached_messages
- cached_labels
- cached_contacts
- config_table
- log_store

b. Analizar las tablas encabezado de conversaciones en caché (cached_conversation_ headers) y la tabla mensajes en caché

(cached_messages), visualizar las tablas con el navegador de base de datos SQLite.

La tabla encabezado de conversaciones en caché (cached_conversation_headers) contiene información relevante para el perito almacenada en las siguientes columnas:

· Es bandeja de entrada; es Spam; es Papelera (isInbox/isSpam/isTrash): Si tiene valor = 1 es verdadero, si en la columna isInbox aparece "1", entonces el mensaje en esa fila fue recuperado de la bandeja de entrada del usuario.

· Asunto (subject).

· Contenido parcial del cuerpo del mensaje (snippetHtml).

· Nombre del emisor (senderListHtml): Contiene el nombre asignado al emisor, no necesariamente la cuenta de correo electrónico.

· FechaMS (dateMs): La fecha y hora de recepción del mensaje en la forma Unix Epoch en milisegundos. Convertir manualmente quitando los últimos tres dígitos o con el convertidor en línea.

· Fecha de modificación del mensaje (KmodifyDateMs): La fecha y hora en que fue modificado en el formato Unix Epoch (timestamp) el mensaje en milisegundos. Convertir la fecha y hora.

· Tiene adjunto (hasAttachment): Valor = 1 indica que tiene un archivo adjunto, sino le corresponde el valor = 0.

La tabla mensajes en caché (cached_messages) contiene información relevante para el perito almacenada en las siguientes columnas:

· Identificador de mensaje (messageID): Un único identificador de mensaje.

· Identificador de conversación (conversationId): Un identificador para cada conversación.

· Grupo de mensajes para cada emisor o remitente (AnIDassignedforeachconversation). El identificador debe ser el mismo que el del mensaje.

· Está en la Bandeja de entrada; es Spam; es Papelera (isInbox/isSpam/isTrash/ etc.): En estas columnas, valor = 1 indica verdadero, el mensaje fue recuperado de la bandeja de entrada.

· Asunto (subject): Contiene el asunto del mensaje.

· Contenido parcial de Html (snippetHtml): Contiene una porción del cuerpo del mensaje.

· Dirección de (address_from): Contiene la dirección de correo electrónico del emisor o remitente.

· Dirección para (address_to): Contiene la dirección del correo electrónico del receptor o destinatario, o la dirección del destinatario del mensaje enviado

con copia (address_cc), o la dirección del destinatario del mensaje enviado con copia oculta (address_bcc).

· Fecha de recepción del mensaje, fechaMS (receivedDateMs, dateMs): La fecha y hora de recepción del mensaje en formato Unix Epoch en milisegundos. Convertir manualmente quitando los últimos tres dígitos o con el convertidor en línea.

c. Registrar, documentar y/o capturar pantallas con la información requerida.

21. Análisis de las cuentas de correo electrónico de diversos servidores de correo; las cuentas sincronizadas con el dispositivo tienen una carpeta para cada una y pueden visualizarse con la imagen física del dispositivo:

· Cuentas de Exchange, la carpeta comienza con ExchangeActiveSync.

· Cuentas de Gmail o Yahoo, la carpeta comienza con IMAP-email@address.com.

· Dentro de estas carpetas aparecerán las siguientes subcarpetas de importancia para el perito:

– Elementos borrados (Deleted Items.mbox)

– Borrador(Drafst.mbox)

– Spam (Junk E –mail.mbox)

– Salida (Outbox.mbox)

– Elementos enviados (Sent Items.mbox)

a. Verificar en las carpetas la existencia de mensajes con la extensión ".emlx".

b. Visualizar los archivos ".emlx" con un editor de texto o importándolos a una aplicación de correo en una computador Mac.

c. Verificar en las carpetas la existencia de mensajes con la extensión ".emlxpart", que contienen archivos adjuntados a uno o más mensajes.

d. A partir de la imagen del iPhone.dmg montada como solo lectura, listar el contenido de las carpetas y determinar el tipo de archivo:

#ls -l /mount/mobile/Library/Mail/ExchangeActiveSync-[Mail-ID].mbox/Messages

#file 26.emlx

16.emlx: RFC 822 mail text

· Indica que es un archivo de correo electrónico.

#file 13.1.6.emlxpart

13.1.6.emlxpart: Ziparchivedata, at least v2.0 to extract

· Indica que el archivo está comprimido y debe ser descomprimido.

e. Copiar el archivo a la computadora de Informática forense,

descomprimirlo y visualizar el contenido y los adjuntos.

22. Analizar los mensajes de la carpeta de correo Papelera (Deleted). Los mensajes borrados se pueden recuperar, los borrados completamente o vaciados de la Papelera no se pueden encontrar en la carpeta Mail. El perito deberá utilizar una herramienta para buscar fragmentos del correo borrado completamente de la imagen iPhone.dmg, y efectuar búsquedas de palabras clave en todos los mensajes (*.email) de una determinada dirección de correo electrónico (prueba@correo.com):

#scalpel –output/email -10-0

#grep prueba@correo.com *.email

23. Analizar los mensajes a partir de los archivos adquiridos o recolectados por medio de la adquisición lógica o por medio de la adquisición de resguardo; en el caso de que la adquisición física no sea posible, el perito tiene dos lugares importantes para recuperar los correos electrónicos:

a. Verificar y analizar el contenido de la carpeta Webkit.

b. Analizar la base de datos Keychain.

c. Registrar, documentar y/o capturar pantallas con la información requerida.

24. Analizar la aplicación Mapas (Maps) que permite al usuario buscar una ubicación específica y la dirección utilizando la herramienta Google Maps y almacena la hora en que el usuario se encuentra en un determinado lugar geográfico.

Ubicación en la estructura de archivos:

/private/var/mobile/Library/Maps:

· Páginas marcadas, Bookmarks.plist: Contiene las ubicaciones marcadas por el usuario.

· Direcciones, Directions.plist: Contiene las direcciones buscadas por el usuario.

· Historial, History.plist: Contiene un historial de los mapas buscados por el usuario. El formato de estos archivos plist es en binario; se pueden editar con un editor de texto

y se podrán leer, por lo tanto, no es necesario que el perito lo convierta a XML para visualizar la información.

a. Editar los archivos .plist.

b. Extraer las direcciones que se encuentran legibles, el resto del archivo no se podrá leer.

c. Registrar, documentar y/o capturar pantallas con la información requerida.

25. Analizar la aplicación Notas (Notes): El usuario puede crear notas de texto y almacenar la fecha y hora de creación.

Ubicación en la estructura de archivos:

/private/var/mobile/Library/Notes:

• Base de datos de notas (notes.db): Almacena los contenidos de las notas y otra metadata, fecha de creación y modificación. Esta base de datos tiene información relevante para el perito.

Tablas que componen la base de datos de notes.db:

– Note

– NoteChanges

– _SqliteDatabaseProperties

– note_bodies

– sqlite_sequence

• Índice de notas (notes.idx): Comprende el archivo índice que contiene fragmentos de las notas.

a. Identificar y analizar los campos de las columnas en la tabla Nota (Note.db), visualizar la tabla con el navegador de base de datos SQLite:

• Identificador de fila (ROWID): Número secuencial asignado para cada nota, la tabla sqlite_sequence lleva un seguimiento del último identificador de fila asignado para la tabla Nota.

• Fecha de creación (creation_date): Fecha y hora en el formato OS X Epoch; convertirla con el convertidor en línea.

• Título (title): Contenido de la nota.

• Fecha de modificación (modification_date): Fecha y hora en el formato OS X Epoch; convertirla con el convertidor en línea.

b. Registrar, documentar y/o capturar pantallas con la información requerida.

26. Analizar la aplicación de navegación web de Apple denominada Safari.

Ubicación en la estructura de archivos:

/private/var/mobile/Library/Safari:

• Base de datos de marcadores (Bookmarks.db o Bookmarks.plist): Contiene los sitios marcados por el usuario. En la versión iOS 4, los marcadores se almacenan en una base de datos.

• Historial (History.plist): Contiene la dirección URL visitada por el usuario, como así también la última página visitada y la fecha y hora de acceso.

• Estado suspendido (SuspendState.plist): Puede contener el historial web borrado, términos de búsquedas en Google y la última URL visitada; no

aparece la fecha y hora como en el archivo de Historial (History.plist).

Los archivos plist de Safari en forma predeterminada se encuentran en el formato binario. En Mac se pueden abrir y examinar con facilidad oprimiendo la barra espaciadora. Si el perito intenta visualizarlos en un editor de texto, los datos no se verán apropiadamente, por lo tanto deberá convertir los archivos plist a XML, donde la información se encuentra más organizada.

a. Analizar la base de datos de marcadores o el archivo de marcadores (Bookmarks.db o Bookmarks.plist).

b. Convertir el archivo Bookmarks.plist en XML.

c. Editar el archivo plist para visualizarlo en XML:

· Los datos en el archivo se organizan colocando la URL y el sitio web visitado en la etiqueta <string>.

d. Visualizar la base de datos de marcadores Bookmarks.db con el navegador de base de datos SQLite:

· bookmark_title_words

· bookmarks

· generations

· sync_properties

e. Analizar la tabla marcadores (bookmarks) que contiene el título de la página visitada y la URL: En esta tabla se encuentra información relevante para el perito.

f. Analizar el archivo de historial (history.plist) que contiene los sitios visitados por el usuario, fecha y hora de acceso, y fecha y hora del último sitio visitado.

g. Convertir el archivo plist a XML y visualizarlo con el editor de texto.

· Convertir el formato fecha y hora OS X Epoch con el convertidor en línea.

· Analizar la tabla Estado suspendido (SuspendState.plist) con el navegador de base de datos SQLite. Verificar los sitios borrados.

h. Registrar, documentar y/o capturar pantallas con la información requerida.

27. Analizar la aplicación Correos de voz (Voicemail.db); almacena los correos de voz que recibió el usuario.

Ubicación en la estructura de archivos:

/private/var/mobile/Library/Voicemail:

· Base de datos de correos de voz (Voicemail.db): Contiene información de cada uno de los mensajes de voz.

· _suscribed: Es un archivo que está generalmente vacío.

· .amr: Son los archivos de correos de voz actuales que pueden ser

escuchados utilizando un reproductor multimedia.

a. Analizar la base de datos de correos de voz (Voicemail.db) con el navegador de base de datos SQLite:

Tablas que componen la base de datos de Voicemail.db:

- _SqliteDatabaseProperties
- Sqlite_sequence
- Voicemail: Es la tabla con información más significativa para el perito.

b. Identificar y analizar los campos de las columnas en la tabla Voicemail:

- Identificador de fila (ROWID): Número secuencial asignado para cada nota, la tabla sqlite_sequence lleva un seguimiento del último identificador de fila asignado para la tabla de mensajes de voz.
- Fecha (date): La fecha y hora en que se creó el mensaje de voz en el formato Unix Epoch; convertir la fecha y la hora con el convertidor en línea.
- Emisor (sender): El número de teléfono del usuario que dejó el mensaje de voz.
- Número de devolución de llamada (Callback_num): El número de teléfono del usuario que dejó el mensaje de voz.
- Duración (duration): La duración del mensaje.
- Caducidad (expiration): La fecha y hora en que el mensaje de voz expiró (por ejemplo: un mes después de ser creado).
- Fecha de borrado (trashed_date): Si se aplica, fecha y hora en que el usuario envió el mensaje a la carpeta de borrados o papelera.

c. Escuchar los correos de voz. El perito deberá abrir los archivos con extensión ".amr" utilizando un reproductor multimedia. Estos archivos aparecen nombrados luego del identificador de fila (ROWID), si este tiene el valor 13, el archivo de voz será 13.amr.

d. Identificar los correos de voz eliminados por el usuario: El iPhone tiene una característica denominada mensaje de voz visual que permite al usuario ver los diferentes correos de voz contenidos en el dispositivo. Si el usuario desea borrar un correo de voz, lo puede hacer con la opción de la pantalla táctil.

- El perito debe buscar en las carpetas borradas o eliminadas la existencia de algún correo de voz, ya que este es el primer lugar donde se envían los correos cuando son borrados por el usuario. Esta carpeta es visible en el menú de la aplicación de Correo de voz. El usuario puede restaurar los archivos a partir de la carpeta borrados o eliminados o puede eliminarlos en forma permanente (eliminar todos, clear all), semejante a la Papelera de reciclaje de Windows

(recycle bin). Cuando el perito realiza la adquisición lógica, la herramienta le informará sobre los correos de voz borrados que de hecho se encuentran en la papelera de reciclaje del dispositivo.

f. Determinar los correos de voz borrados en forma permanente: El perito debe observar los campos del Identificador de fila (ROWID); este valor se incrementa en forma secuencial en 1, si falta un número, esto indica que el correo de voz faltante fue eliminado por el usuario.

· Utilizar técnicas de análisis de SQLite para recuperar las filas borradas (sqlite. org).

g. Registrar, documentar y/o capturar pantallas con la información requerida.

28. Analizar la aplicación YouTube mobile. YouTube es un sitio web donde los usuarios pueden buscar, ver y compartir videos en Internet.

Ubicación en la estructura de archivos:

/private/var/mobile/Library/YouTube:

· com.apple.youtube.plist, contiene marcadores de los videos de Youtube, historial y búsquedas recientes.

a. Analizar el archivo com.apple.youtube.plist. Cuando el usuario mira un video utilizando la aplicación YouTube, se almacena como un ítem del historial. El usuario puede agregar videos a su carpeta Favoritos y que aparece como marcador (Bookmarks) en el archivo plist.

<dict>
<key>Bookmarks</key>
<array>
<string>JpbB15UoKOc&</string>
<array/>
<key>History</key>
<array>
<string>JpbB15UoKOc&</string>
<string>8ihKhH1dSJU</string>
<string>Du4I8UZqBhk</string>
<string>EHsEA8MsCLA</string>
</array>
<key>lastSearch</key>
<string>iPhone</string>
<key>slectedCategory</key>
<string>YTSearchCategoryController</string>

</dict>

El valor contenido entre las etiquetas <string> </string>, aparenta estar cifrado. No obstante, es el Identificador de un video de YouTube (<string>EHsEA8MsCLA</ string>). El perito para visualizar el video deberá:

- Copiar el identificador, por ejemplo: EHsEA8MsCLA, en la URL de YouTube: http://www.youtube.com/watch?v=EHsEA8MsCLA

La cadena de caracteres seguida del signo igual (=) es el identificador del video.

- Reemplazar el identificador con uno de los mostrados en el archivo plist para visualizar los videos.
- Identificar la última búsqueda (<key>lastSearch</key>) realizada por el usuario en YouTube, en el archivo aparece "iPhone" (<string>iPhone</string>).

b. Registrar, documentar y/o capturar pantallas con la información requerida.

29. Analizar fotos y videos que fueron tomados por el dispositivo o sincronizados a este y que se almacenan en el sistema de archivos del iPhone. El modelo original de iPhone, hasta la generación 3G, no tenía una aplicación incorporada que permitiera grabar videos desde el dispositivo. Por esta razón, los usuarios recurrieron al almacén de aplicaciones (App Store) para obtener programas que les permitieran ejecutar esta función. En los modelos posteriores, se incorporó en el iPhone la cámara o filmadora y con ella se pueden sacar fotografías y grabar videos. Los videos grabados con la cámara del iPhone pueden ser recuperados del dispositivo.

Ubicación en la estructura de archivos:

/private/var/mobile/Media/:

- /DCIM/100APPLE: La carpeta contiene fotografías y videos tomados con el iPhone.
- /DCIM/999APPLE: Contiene las capturas de pantalla (screen shot) del dispositivo tomadas por el usuario.
- /PhotoData/Photos.sqlite (solamente en iOS 4): Contiene metadatos de fotografías y videos del dispositivo.

a. Analizar la base de datos de fotografías y videos (photos.sqlite) dentro del dispositivo con el navegador de base de datos SQLite.

Tablas que componen la base de datos de photos.sqlite:

- Globals
- Keyword

- Photo
- PhotoAlbum
- PhotoAlbumToPhotoJoin
- PhotoExtras
- sqlite_sequence

b. Analizar la tabla Fotografía (Photo), que contiene información significativa para el perito: No solo obtendrá información sobre el lugar de almacenamiento de las fotografías y videos, sino también de los metadatos correspondientes a cada archivo. El perito deberá utilizar la información de la base de datos photos.sqlite en combinación con las fotografías o videos actualmente almacenados en la carpeta 100 Apple o 999 Apple para determinar fecha y hora en que se tomaron o se modificaron. Las columnas de la tabla son las siguientes:

- Título (title): El nombre del archivo, sin la extensión.
- Fecha y hora de captura (captureTime): Fecha y hora de la toma de la fotografía o del video en el formato de OS X Epoch; convertir la fecha y hora con el convertidor en línea.
- Ancho (width): Ancho de la fotografía; si el campo tiene un valor “0”, el archivo es de video.
- Altura (height): Altura de la fotografía; si el campo tiene un valor “0”, el archivo es de video.
- Directorio (directory): La ruta donde fue guardado el archivo en el sistema de archivo, generalmente en: DCIM/100APPLE.
- Nombre de archivo (filename): El nombre del archivo más la extensión: “.jpg” o “.mov”.
- Fecha y hora de modificación (recordModDate): Fecha y hora de la modificación del archivo en el formato de OS X Epoch, convertir la fecha y hora con el convertidor en línea.

c. Verificar la existencia de fotografías borradas. Los videos borrados son muy difíciles de recuperar. Para las fotografías se pueden utilizar los comandos:

#strings

#scalpel

d. Registrar, documentar y/o capturar pantallas con la información requerida.

30. Analizar las aplicaciones de terceros descargadas en el iPhone. Cada aplicación, en sus respectivas carpetas, contiene archivos específicos, los cuales se pueden visualizar y recuperar, por lo que constituye una fuente de

información relevante para el perito.

Ubicación en la estructura de archivos:

/private/var/mobile/Applications

e. Analizar la carpeta de la aplicación Facebook. En el iPhone los usuarios pueden mandar mensajes a sus amigos, subir y ver fotografías y seleccionar sus sitios favoritos (restaurante, confitería) que pueden ser consultados por sus amigos para saber en donde se encuentran dichos lugares. La mayoría de la información se almacena en el dispositivo y puede ser recuperada fácilmente.

Ubicación en la estructura de archivos:

/private/var/mobile/Applications/<Facebook Application Identifier>/:

• /Documents/friends.db, contiene la lista de todos los amigos del usuario en Facebook, como así también el enlace a sus respectivas fotografías del perfil y los campos teléfono, celular, correo electrónico; están cifrados o con un formato que no puede ser visualizado por el perito. Contiene dos tablas:

- amigos (friends)
- meta

• Library/Preferences/com.facebook.Facebook.plist, contiene el inicio de sesión del usuario en Facebook, que es al mismo tiempo una dirección de correo electrónico.

Efectuar búsquedas del nombre de usuario de inicio de sesión en Facebook en la imagen del dispositivo iPhone.dmg, con el comando strings y obtener información adicional sobre la aplicación, tal como actualización del estado, mensajes escritos en el muro y mensajes actuales enviados y recibidos por el usuario.

f. Analizar la carpeta de la aplicación Groupon[103]. Este servicio provee ofertas del día y cupones de descuentos en negocios locales o internacionales. En iPhone le permite al usuario comprar y gestionar los cupones. Parte de la información personal del usuario que se requiere para esta aplicación se almacena en el dispositivo.

Ubicación en la estructura de archivos:

/private/var/mobile/Applications/<Application Identifier>/Documents/v1/users/<username>/groupons:

• myGroupons.plist: Contiene una lista de los groupons comprados por el usuario y la fecha de compra y el precio.

• userInfo.plist: Contiene la información personal del usuario, incluye nombre completo, dirección, dirección de correo electrónico y otra información adicional. Al realizar una compra, el usuario debe ingresar o

configurar su tarjeta de crédito dentro de su cuenta. Los datos como nombre, dirección, fecha de expiración de la tarjeta y los últimos cuatro dígitos pueden ser recuperados por el perito.

Visualizar el contenido de los archivos plist, convirtiéndolos de binario al formato XML, utilizando la herramienta Plutil o cualquier otra disponible. Existen dos carpetas (dealLocation y deals) que contienen cupones que están disponibles, pero no fueron adquiridos por el usuario; el perito no debe confundirlas con aquellas carpetas listadas bajo el nombre específico del usuario.

g. Analizar la carpeta de la aplicación Kik Messenger. Se utiliza para reemplazar la aplicación de mensajes de textos del dispositivo. Es más rápida y más confiable para el intercambio de mensajes.

Ubicación en la estructura de archivos:

/private/var/mobile/Applications/<KIK Messenger Application Identifier>/:

• /Documents/kik.sqlite: Almacena el contenido de los mensajes, nombres de usuario y muestra los nombres de todos los contactos en la aplicación.

• /Library/Preferences/com.kik.chat.plist: Almacena el nombre de usuario, clave y dirección de correo electrónico.

h. Analizar la base de datos kik.sqlite con el navegador de base de datos SQlite.

Las tablas que la componen son:

– ZKIKMESSAGE: Almacena el contenido de los mensajes. Los campos que contienen información relevante para el perito son:

❑ ZTIMESTAMP: Fecha y hora de envío o recepción del mensaje, en formato OS X Epoch. Convertir la fecha con el convertidor en línea.

❑ ZBODY: Contiene el cuerpo del mensaje.

– ZKIKUSER: Guarda todos los contactos dentro de la aplicación en forma individual, su dirección de kik.com (ZJID) y su nombre visible.

i. Analizar el archivo com.kik.chat.plist: Almacena información sensible respecto del inicio de sesión, incluyendo la dirección de correo electróncio, primer nombre y apellido, nombre del usuario y clave.

– Visualizar el contenido del archivo plist, convertirlo de binario al formato XML, utilizando la herramienta Plutil o cualquier otra disponible.

– Recuperar información borrada utilizando un editor en hexadecimal para visualizar el archivo de imagen del dispositivo y buscar un nombre de usuario único para recuperar los mensajes enviados o recibidos y borrados.

j. Analizar la carpeta de la aplicación Dropbox. Se utiliza para subir o

descargar archivos, permite almacenarlos en la nube. Los usuarios pueden descargar o subir documentos, fotografías o videos.

Ubicación en la estructura de archivos:

/private/var/mobile/Applications/< Dropbox Application Identifier>/:

· /Documents/Dropbox.sqlite: Contiene los nombres de los archivos guardados en Dropbox.

· /Library/Preferences/com.getdropbox.Dropbox.plist: Contiene los nombres de usuario (correo electrónico) y favoritos de DropBox.

· /Library/Caches/Dropbox: Contiene los archivos actuales.

· /Library/Caches/Three29: Contiene imágenes jpg que fueron subidas o descargadas desde y hacia DropBox.

· /Library/Caches/Dropbox/FavoriteFile.plist: Contiene los archivos marcados por el usuario como favoritos.

k. Analizar la base de datos Dropbox.sqlite con el navegador de base de datos SQLite; las tablas que la componen son:

· ZCACHEDFILE: Almacena los archivos que fueron visitados por el usuario, como así también los metadatos asociados con esos archivos. La columna a ZPATH guarda el nombre del archivo y la ruta completa en Dropbox. La columna ZLASTVIEWED guarda la fecha y hora en que el usuario vio un determinado archivo; se encuentra en formato OS X Epoch. Convertir la fecha con el convertidor en línea.

· Z_METADATA

· Z_PRIMARYKEY

· TheZCACHEDFILEt

ii. Analizar el archivo com.getdropbox.Dropbox.plist: Lista todos los archivos marcados como favoritos por el usuario, otros metadatos relacionados con los archivos y el nombre del usuario.

· Visualizar el contenido del archivo plist, convertirlo de binario al formato XML, utilizando la herramienta Plutil o cualquier otra disponible.

· Efectuar la recuperación de fragmentos de archivos sobre la imagen del dispositivo, utilizando las herramientas como Scalpel o Foremost, para recuperar archivos borrados del tipo .jpg, .doc, .pdf, etc.

e. Analizar la carpeta de la aplicación Windows Live Messenger. Se usa para enviar mensajes instantáneos, controlar el correo electrónico y utiliza ciertas características de Windows Live, Facebook y MySpace. El perito puede recuperar información importante de esta carpeta.

Ubicación en la estructura de archivos:

/private/var/mobile/Applications/< Windows Live Messenger Application

Identifier>/:

· /Documents/CurrentUserNambe.tmp, contiene el usuario actual de la dirección de correo electrónico de Hotmail; es un archivo del tipo plist.

Visualizar el contenido del archivo plist, convertirlo de binario al formato XML, utilizando la herramienta Plutil o cualquier otra disponible.

f. Analizar la carpeta de la aplicación Mint.com. Permite al usuario manejar colectivamente sus finanzas en una forma centralizada, las cuentas bancarias, inversiones, préstamos, y manejar su dinero. El perito puede obtener información importante de esta carpeta.

Ubicación en la estructura de archivos:

/private/var/mobile/Applications/< Mint.com Application Identifier>/:

· Mint_gala.db: Contiene todas las transacciones dentro de la aplicación, cuenta de usuario, información de saldos y descripción de la transacción.

Analizar la base de datos Mint_gala.db con en navegador de base de datos SQlite; las tablas que la componen son:

Account: Contiene la lista de las cuentas sincronizadas con la aplicación. El perito puede ver el nombre de la cuenta y el saldo del usuario para cada cuenta.

Alert: Alertas enviadas al usuario. La aplicación puede notificar al usuario sobre cuándo tiene vencimientos o si el depósito en la cuenta está en negativo. El perito puede obtener información sobre las alertas y verificar la fecha y hora en que fue enviada, junto con el tipo de cuenta bancaria. La fecha y hora está en formato OS X Epoch. Convertir la fecha con el convertidor en línea.

attributes budget budget_overall category fi_login investment refresh spending

user user_tag version

transaction_usertag

Transaction_bankcc: Contiene una descripción detallada de cada transacción completada por cada una de las cuentas. Estas transacciones no necesitan hacerse dentro de la aplicación en el dispositivo. Por ejemplo, por cada compra que realiza el usuario con su tarjeta de crédito, los detalles relacionados con estas compras se mostrarán dentro de esta tabla. La fecha no requiere ser convertida, es la fecha actual. Las columnas son:

Description: Descripción de la transacción.

Amount: La cantidad de dinero acreditado o debitado por la transacción. CategoryID: La categoría de la transacción, el número se muestra en este campo. DatePostedString: La fecha en que se realizó la transacción.

YodDesc: Contiene más detalles de la transacción.

g. Registrar, documentar y/o capturar pantallas con la información requerida.

Análisis de la tarjeta sIM del teléfono iPhone

La tarjeta SIM puede ser examinada con diferentes herramientas:

· SIM Card Seizure v3.1, de Paraben Corporation, producto comercial (http://www.paraben.com/sim-card-seizure.html): Muestra el resultado de los diez últimos números marcados por el iPhone.

· Nmap[104], herramienta de código abierto para la exploración de puertos (http://www. security-database.com/toolswatch/Nmap-4-5x-for-Ipod-and-iPhone.html). Luego de ejecutar esta herramienta, aparece un puerto abierto: 62078 con el protocolo TCP para el servicio de sincronización iPhone-Sync. Este puerto lo usa para sincronizar el iPhone al conectarse al sitio de compras de aplicaciones de Apple e iTunes. Este puerto es el mismo que utiliza la consola XBOX360 y la PlayStation3.

revisión de conceptos

· El método de liberación de un dispositivo iPhone no es un procedimiento pericial válido en la telefonía forense.

· La segunda partición del dispositivo iPhone contiene información relevante para el perito.

· La primera partición del iPhone contiene el sistema operativo.

· Las herramientas para la recuperación de fragmentos y archivos borrados que puede utilizar el perito son: Código abierto: Scalpel, Foremost; libre disponibilidad: FTK; comercial: MacLabForensics.

Dispositivos iPod

Los dispositivos iPod[105] surgen en el año 2001 para reproducción de archivos de música del tipo MP3, pero también son utilizados para guardar otro tipo de datos (audiobook, libros acústicos, películas, shows de TV, fotografías, podcast [distribución de archivos de audio, video, con subtítulos o no, por medio de la difusión reiterada], juegos, navegador de Internet Safari, libros electrónicos, correo electrónico, mapas, grabación y edición de video de alta definición, Facetime [video llamada], imessage [enviar mensajes a través de Internet entre iPhone, iPad, iPod Touch, Nike+iPod: dispositivo transmisor que se coloca en la zapatilla para medir los pasos]). La capacidad de almacenamiento varía según el modelo; en el caso del modelo iPod classic[106] es de 160 GB; el perito, en este caso puede obtener información suficiente para el análisis de la evidencia. Existe una variedad de herramientas de código abierto y comercial que pueden utilizarse para crear la imagen de un dispositivo iPod. Los procedimientos de recolección y adquisición son

similares a los de una computadora. El sistema operativo de los dispositivos iPod es un sistema en vivo (live) que no se apaga. La adquisición de la imagen del sistema de archivo requiere el uso de un bloqueador de escritura por hardware o deshabilitar el demonio (servicio) de Mac denominado DiskArbitration (diskarbitrationd), que monta automáticamente los dispositivos en una computadora Mac con sistemas operativos Tiger o Leopard. Por lo tanto, el perito debe considerar el uso de bloqueadores de escritura por hardware aceptados por el NIST*107* (el Instituto Nacional de Normas y Tecnología, National Institute of Standards and Technology es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos) como pueden ser:

- Spuma (http://www.mykeytech.com/index.html).
- Tableau (http://www.forensicpc.com/).
- Super Drive Lock (http://www.ics-iq.com/).
- WiebeTech (http://www.wiebetech.com).

Etapa de identificación, registro, protección, embalaje y traslado de dispositivos iPod El procedimiento para la identificación, registro, protección, embalaje y traslado de los dispositivos iPod es similar al enunciado para los teléfonos celulares e inteligentes. En el caso del

iPod, el embalaje debe hacerse con bolsa antiestática, de la misma forma que un disco rígido,

evitando campos magnéticos que pudieran afectarlo. El perito deberá considerar el estado del dispositivo en el momento de la identificación, el cual puede ser: encendido, encendido y conectado a la computadora Mac o Windows, o apagado.

Procedimiento con el iPod encendido

1. Conectado a la computadora Mac:

a. Fotografiar o filmar el dispositivo y su entorno.

b. Verificar si está montado. Mirando en la pantalla del iPod, si dice “No desconectar”, indica que el dispositivo está montado y es necesario desmontarlo para desconectarlo de la computadora.

c. Verificar y registrar el nombre del iPod en el escritorio de la computadora Mac.

d. Registrar el nombre de la computadora (este dato se almacena en el iPod y será de utilidad en la etapa de análisis).

e. Desmontar el iPod, arrastrando el ícono a la papelera o lata de basura (trashcan) del escritorio de la computadora Mac.

2. Conectado a la computadora con Microsoft Windows:

a. Fotografiar o filmar el dispositivo y su entorno.

b. Verificar si está montado.

c. Verificar y registrar el nombre del iPod en el escritorio de la computadora.

d. Registrar el nombre de la computadora (este dato se almacena en el iPod y será de utilidad en la etapa de análisis).

e. Seleccionar en la barra de tareas el ícono para desconectar dispositivos, seleccionar

iPod y desconectar.

3. Preparar para su embalaje, protegiéndolo con bolsas antiestáticas. El contenido del disco rígido no se perderá si el dispositivo no recibe energía; en el caso de que deba permanecer mucho tiempo en depósito, se debe considerar que la batería puede agotarse y que existe la posibilidad de que no se pueda recargar, entonces será necesario reemplazarla; esto puede ocurrir si el equipo permanece varios años en depósito.

4. Iniciar e ingresar los datos requeridos en el formulario de cadena de custodia.

5. En el laboratorio, determinar si el iPod está preparado para Macintosh o Windows: En el dispositivo, acceder al menú Configuraciones, Acerca de. Desplazando la pantalla se verá Formato Windows en la parte inferior de la pantalla; si la frase no aparece, entonces está con formato HFS+ Macintosh iPod.

Etapa de recolección y adquisición de datos

Procedimientos de recolección de datos en dispositivos iPod

Consideraciones previas

La particularidad de los dispositivos iPod es que presentan, desde su aparición en el mercado en el año 2001, diferentes modelos. El perito deberá consultar el sitio del fabricante (http:// www.apple.com/ipod/) para conocer las especificaciones técnicas de cada modelo. La recolección y generación de imágenes del dispositivo dependerá del tipo de modelo de iPod. Existen dos formas de realizar la imagen del dispositivo. El perito deberá considerar, antes de aplicar el procedimiento adecuado, los siguientes aspectos:

- Modelo del dispositivo iPod:
  - Especificaciones técnicas del hardware de iPod.
- Tipo de almacenamiento:
  - Disco rígido: El perito deberá desarmar el equipo y quitar el disco rígido, luego utilizar un adaptador zif, para generar la imagen.

Adaptador zif para iPod 1

- Memoria Flash: Se puede duplicar a través del cable USB del iPod conectado a un dispositivo de bloqueo de escritura.

El perito deberá conocer los tipos de archivos multimedia que son soportados por iPod, a saber:

- aac
- AAX
- AAX+
- avi
- Mp3
- Mp3 vbr
- m4v,
- .mp4
- MPEG-4
- Apple Lossless
- Wav
- Aiff
- M4v
- Mov

Procedimiento para desactivar el demonio (servicio) de DiskArbitration en el sistema operativo Tiger en la computadora Macintosh

1. Abrir la terminal .app ubicada en el directorio Applications/Utilities/.
2. Crear una carpeta (carpeta nueva) en el escritorio adonde se moverá el archivo diskarbitrationd.plist.
3. Ingresar desde la terminal el comando:

$sudo mv /etc/mach_init.d/diskarbitrationd.plist ~/Desktop/carpetanueva

4. Ingresar la clave, si lo solicita, del usuario root; una vez movido el archivo, ingresar el comando:

sudo reboot

Procedimiento para activar el demonio (servicio) de DiskArbitration en el sistema operativo Tiger en la computadora Macintosh

1. Abrir la terminal .app ubicada en el directorio Applications/Utilities/.
2. Ingresar desde la terminal el comando:

$sudo mv
~/Desktop/carpetanueva/etc/mach_init.d/diskarbitrationd.plist
/etc/mach_init.d/

3. sudo reboot

Ingresar la clave, si lo solicita, del usuario root.

Procedimiento para desactivar el demonio (servicio) de DiskArbitration en el sistema operativo Leopard en la computadora Macintosh

1. Abrir la terminal .app ubicada en el directorio Applications/Utilities/.
2. Crear una carpeta (carpeta nueva) en el escritorio adonde se moverá el archivo diskarbitrationd.plist.
3. Ingresar desde la terminal el comando:

$sudo mv
/System/Library/LaunchDaemons/com.apple.diskarbitrationd.plist
~/Desktop/carpetanueva

4. Ingresar la clave, si lo solicita, del usuario root. Una vez movido el archivo, ingresar el comando:

sudo reboot

Procedimiento para activar el demonio (servicio) de DiskArbitration en el sistema operativo Leopard en la computadora Macintosh

1. Abrir la terminal .app ubicada en el directorio Applications/Utilities/.
2. Ingresar desde la terminal el comando:

$sudo mv
~/Desktop/carpetanueva/etc/mach_init.d/diskarbitrationd.plist
/System/Library/LaunchDaemons/

3. sudo reboot:

Ingresar la clave, si lo solicita, del usuario root.

Procedimiento para crear la imagen del dispositivo iPod con una estación de trabajo de Informática forense de Macintosh con el comando dc3dd (http://sourceforge.net/projects/ dc3dd/)

La herramienta dc3dd puede ejecutarse desde un CD forense en vivo o estar descargada como utilidad en la computadora Mac.

1. Efectuar, previamente a su utilización, un borrado seguro del contenido del dispositivo de destino de la imagen*108*.
2. Conectar el bloqueador de escritura por hardware a la computadora.
3. O desactivar DiskArbitration.
4. Abrir la terminal .app ubicada en el directorio Applications/Utilities/.
5. Verificar los discos montados:

$ls /dev/rdisk*

El disco rígido de la computadora Mac aparece como /dev/rdisk0

6. Conectar el dispositivo iPod a la computadora Mac.
7. Verificar los discos montados:

$ls /dev/rdisk*

Aparecerá /dev/rdisk1; indica que el dispositivo iPod está conectado.

8. Efectuar la certificación matemática para verificar la integridad de los datos.

$sudo md5deep –e /dev/rdisk1 | tee –a > ~/Desktop/iPodhash.md5.txt

(-e muestra el progreso del hash y lo realiza sobre todo el dispositivo /dev/rdisk1, redireccionando el resultado a un archivo txt).

9. Finalizado el proceso de hash, abrir la terminal .app ubicada en el directorio Applications/Utilities.
10. $sudo dc3dd con=sync,noerror if=/dev/rdisk1 of= ~/Desktop/iPodimagen.dmg hashwindow=1000000 hash=md5,sha1 hashlog=/~/Desktop/iPod.hashlog bs=4k progress=on*109* Descripción del comando dc3dd: (http://www.linuxcertif.com/man/1/dc3dd/).

Observación

En el caso de visualizar la imagen de un iPod en una computadora personal con sistema operativo Windows utilizando tanto EnCase como FTK, será necesario dividir la imagen con la opción split que divide la salida del archivo de la imagen en partes del tamaño de bytes. Esto es para el caso de que Windows tenga un límite de tamaño de 2GB; en el caso del sistema de archivo HFS de Mac no es necesario dividir la imagen. El comando sería el siguiente:

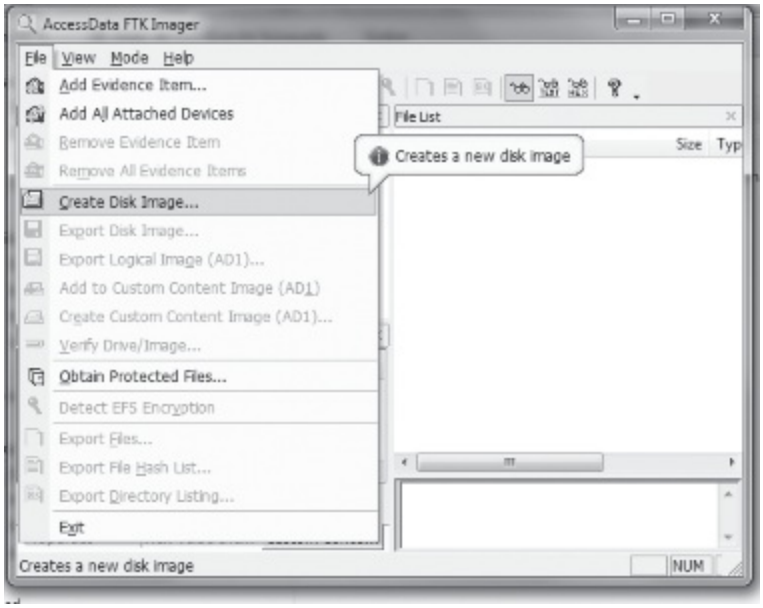
$sudo dc3dd con=sync,noerror split=650MB if=/dev/rdisk1 of=

~/Desktop/iPodimagen.dmg hashwindow=1000000 hash=md5,sha1 hashlog=/~/Desktop/iPod.hashlog bs=4k progress=on[110]

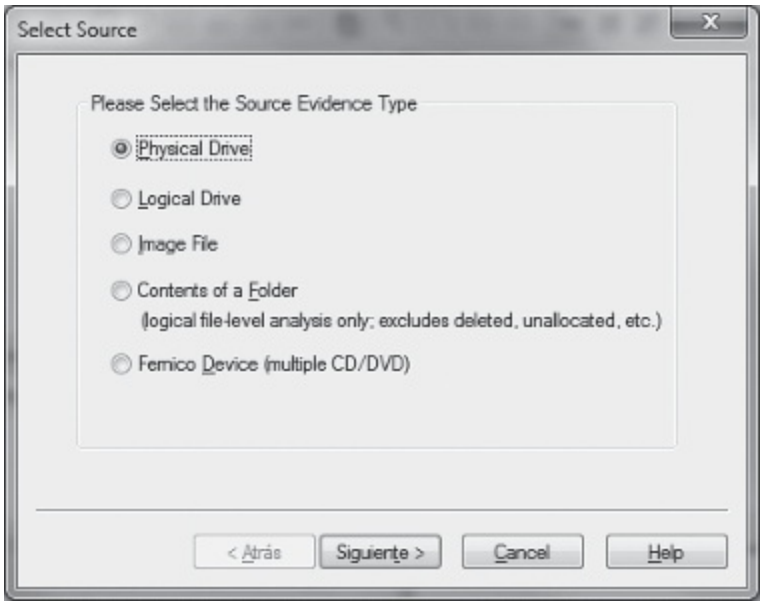
Procedimiento para crear la imagen del dispositivo iPod con la herramienta de libre disponibilidad, FTK Imager, Forensic Tool Kit (http://accessdata.com/support/adownloads) en una computadora con sistema operativo Windows

FTK Imager puede estar incorporada en otros conjuntos de herramientas para Informática forense como el producto comercial Helix (http://www.e-fense.com/products.php).

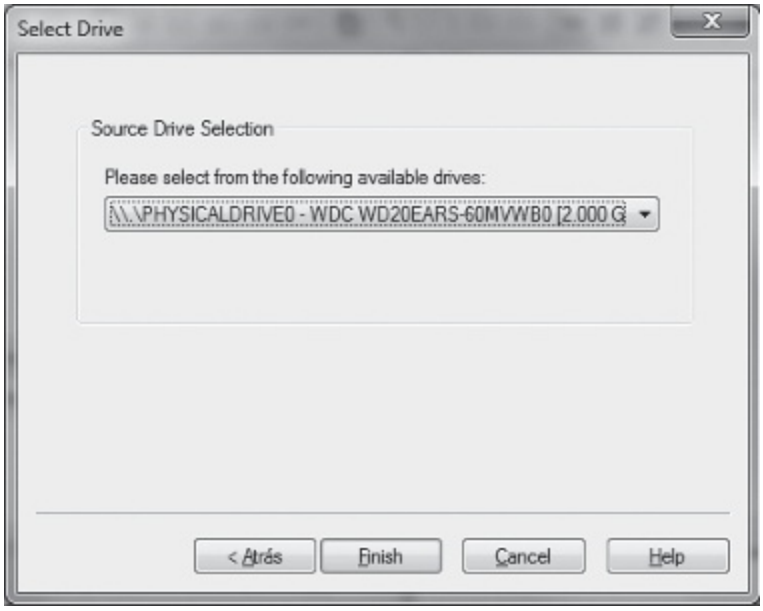
1. Abrir la aplicación FTK Imager.
2. Conectar el iPod a un bloqueador de escritura por hardware.
3. Seleccionar en el menú de FTK Imager la opción Archivo (File).
4. Seleccionar Crear imagen (Create Disk Image).



5. En la ventana emergente ingresar el Origen (Source), elegir la opción Dispositivo Físico(Physical Drive), seleccionar Siguiente (Next):



6. Desplegar el menú y seleccionar Appel iPod USB Device:



7. Oprimir el botón Fin (Finish).

8. En la ventana emergente de Crear Imagen (Create Image), seleccionar Agregar (Add).

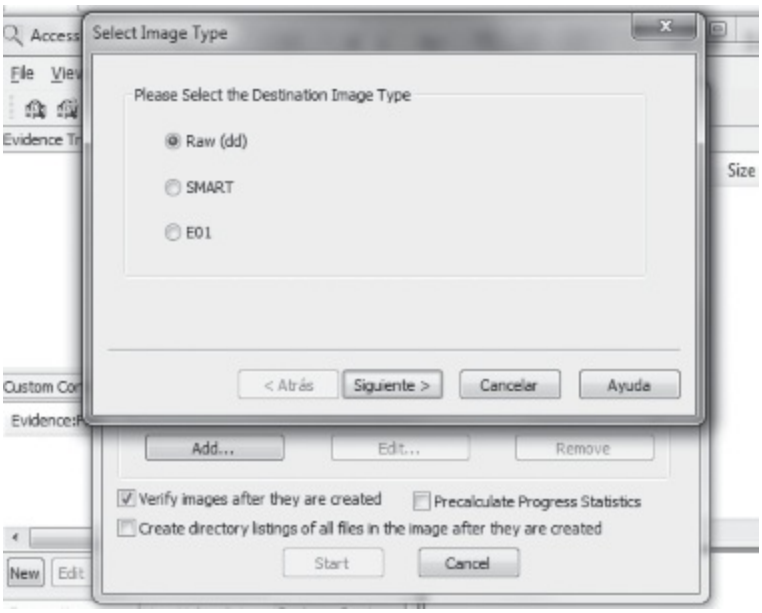
9. En la siguiente opción se debe elegir el tipo de imagen:

(1) Raw (dd), copia bit a bit.

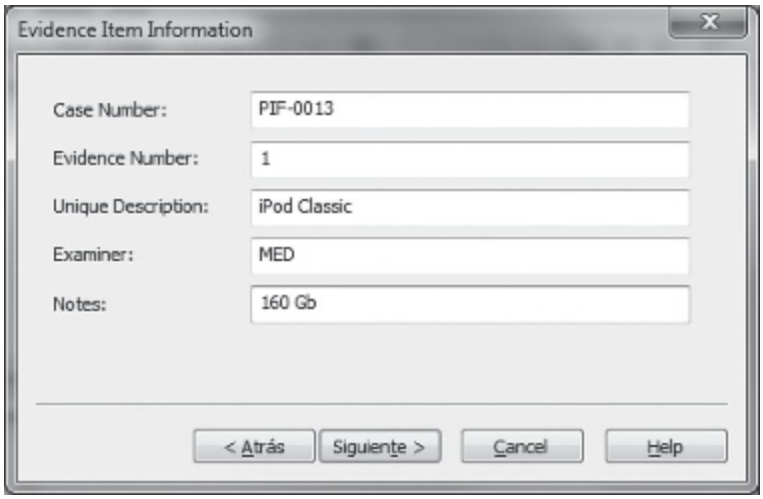
(2) Smart (s01), incorpora información sobre la imagen.

(3) EO1, de EnCase; están comprimidas y contienen información valiosa del hash, del caso y de su creación.

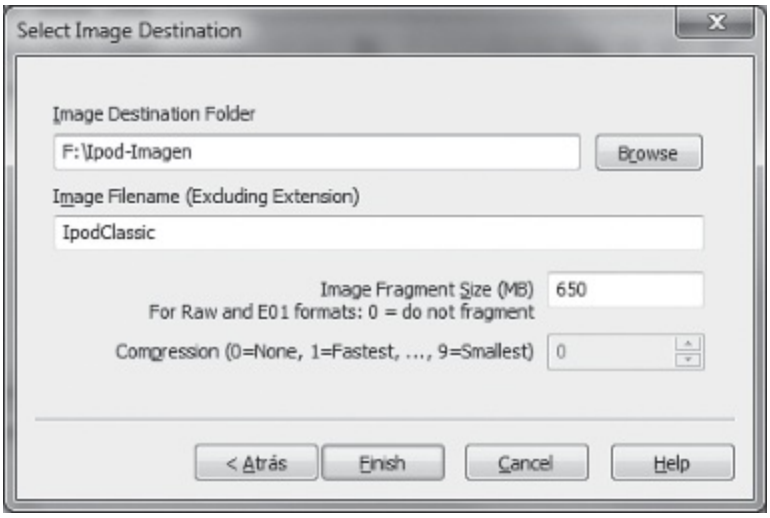
La opción recomendada es la (1) Raw (dd), oprimir Siguiente (Next).



10. En la ventana emergente de Información sobre la Evidencia (Evidence Item Information), ingresar los datos solicitados sobre el caso, oprimir Siguiente.



11. En la ventana Seleccionar Destino de la Imagen (Select Image Destination), seleccionar la carpeta destino para guardar la imagen, preferentemente un dispositivo de almacenamiento externo. Oprimir el botón Fin (Finish).



12. Aparece nuevamente la ventana de Crear Imagen, seleccionar Iniciar (Start).

13. Editar el archivo de texto generado por FTK Imager luego de crear la imagen bit a bit. El archivo contiene toda la información acerca del proceso de la obtención de la imagen: datos del caso, hashes, verificación de hashes y hora y fecha de adquisición de la imagen.

Herramientas[111]

- De código abierto:
  - dd, dcfldd (http://dcfldd.sourceforge.net/).
  - dc3dd (http://sourceforge.net/projects/dc3dd/).
- CD en vivo:
  - Backtrack 5 (http://www.backtrack-linux.org/).
- Libre disponibilidad:
  - Raptor (http://www.forwarddiscovery.com/Raptor).
- Comerciales / CD en vivo:
  - EnCase (www.guidancesoftware.com/).
  - Helix (http://www.e-fense.com/products.php).
  - MacForensicsLab (http://www.macforensicslab.com/).
  - BlackBaf BBTImagerLite (https://www.blackbagtech.com/).

Procedimientos sintetizados de recolección en diferentes modelos de iPod

1. Recolección de datos en dispositivos iPod Classic:
   a. Extraer el disco rígido.
   b. Conectarlo a un adaptador zif.
   c. Utilizar la herramienta de duplicación de disco o de generación de imagen.

i. Si se realiza en una computadora Mac, se debe desactivar el servicio de DiskArbitration, que maneja la activación y montaje de los discos cuando se conectan por USB o firewire a la computadora Mac. Considerando que no se debe montar el disco para efectuar la recolección, el perito deberá desactivar el servicio si se encuentra en la computadora Mac:

#launchctl list: Obtiene la lista de los procesos iniciados con launchd[112].

#launchctl list, grep diskarbitrationd: Filtra el listado de procesos, limitándolo al del disco Arbitration, mostrando el PID o identificador de proceso.

launchctl stop 0x10abe0.diskarbitrationd: Se ejecuta launchctl con la opción de Detener el servicio (Stop), acorde al PID del proceso devuelto.

2. Recolección de datos en dispositivos iPod Mini (solo reproduce audio):

a. Quitar la tarjeta de memoria Flash.

b. Conectar la memoria a un bloqueador de escritura.

i. Si se realiza en una computadora Mac, se debe desactivar el servicio de DiskArbitration, que maneja la activación y montaje de los discos cuando se conectan por USB o firewire a la computadora Mac. Considerando que no se debe montar el disco para efectuar la recolección, el perito deberá desactivar el servicio si se encuentra en la computadora Mac (ver pasos en iPod Classic).

c. Efectuar la imagen de la memoria Flash.

3. Recolección de datos en dispositivos iPod Shuffle (solo reproduce audio) y iPod Nano:

a. Quitar la tarjeta de memoria Flash.

b. Conectar el USB del dispositivo a un bloqueador de escritura:

i. Si se realiza en una computadora Mac, se debe desactivar el servicio de DiskArbitration, que maneja la activación y montaje de los discos cuando se conectan por USB o firewire a la computadora Mac. Considerando que no se debe montar el disco para efectuar la recolección, el perito deberá desactivar el servicio si se encuentra en la computadora Mac (ver pasos en iPod Classic).

c. Efectuar la imagen de la memoria Flash.

4. Recolección de datos en dispositivos iPod Touch (pantalla táctil múltiple). Incorporado puerto USB y conexión inalámbrica 802.11b.g:

a. Quitar la tarjeta de memoria Flash.

b. Conectar el USB del dispositivo a un bloqueador de escritura:

i. Si se realiza en una computadora Mac, se debe desactivar el servicio de DiskArbitration, que maneja la activación y montaje de los discos cuando se conectan por USB o firewire a la computadora Mac. Considerando que no se debe montar el disco para efectuar la recolección, el perito deberá desactivar el

servicio si se encuentra en la computadora Mac (ver pasos en iPod Classic).

c. Efectuar la imagen de la memoria Flash.

Etapa de análisis de datos

Procedimiento para el análisis del sistema de archivos de iPod

Consideraciones previas

Los dispositivos iPod poseen un sistema operativo y un sistema de archivo. El perito debe conocer el sistema de particiones de un iPod y cómo montar un archivo de imagen de iPod en una computadora Mac y conocer cómo acceder a sus archivos y carpetas ocultas. La evidencia que el perito puede encontrar está en los archivos de multimedia y en las imágenes. Al configurar un iPod como un dispositivo externo, el perito puede hallar cualquier tipo de archivo. La herramienta slurp.exe (http://www.sharp-ideas.net/pod_slurping.php), que se ejecuta en el iPod, recupera información desde cualquier sistema en que esté conectado el iPod.

El dispositivo iPod utiliza el esquema de partición de Apple. Las siguientes herramientas nativas (hdiutil)[113] de línea de comando de Mac permiten trabajar con imágenes de disco. Para visualizar el esquema de partición en una imagen de iPod desde una computadora Mac, el perito deberá ejecutar:

1. En la barra de menú del explorador gráfico de archivos (Finder), elegir la opción Ir (Go),

Utilidades (Utilities).

2. Seleccionar Terminal.app.

3. En la línea de comando, ingresar:

$hdiutil pmap /iPodimagen.dmg

El resultado muestra el mapa de particiones del archivo de la imagen del dispositivo iPod.

4. $hdiutil image info /iPodimagen.dmg

La opción imageinfo permite visualizar más información sobre el esquema de partición: La primera partición del mapa de particiones de Apple es el DDM (Driver Descriptor Map)

- Mapa de descripción del dispositivo). Es del tamaño de un sector y brinda información sobre

los dispositivos del sistema. Los dispositivos generalmente residen en una partición diferente.

La segunda partición es etiquetada como Apple_Free, que consta de un tamaño de pocos sectores y es espacio libre.

La siguiente partición es el mapa de partición de Apple, generalmente es del tamaño de 63 sectores y es responsable de mantener un seguimiento de todas las particiones en el iPod.

Cada partición es descripta por una entrada en el mapa de partición. El mapa de partición es descripto como una entrada en sí mismo.

La siguiente partición está etiquetada como Apple_HFS; aquí es donde reside el sistema de archivos y donde se almacenan todos los datos del usuario: música, fotografías y videos. En esta partición es donde el perito encontrará información significativa.

Procedimiento para el análisis del archivo de imagen del dispositivo iPod en una computadora Mac

Consideraciones previas

En el análisis de una imagen de un dispositivo iPod se recomienda el uso de una estación de Informática forense con sistema operativo de Mac. La ventaja radica en que no será necesario adquirir herramientas adicionales de análisis de Informática forense. La desventaja es que no se podrán recuperar archivos borrados o carpetas dentro del espacio desperdiciado (slack)*114*.

1. Montar la imagen del dispositivo iPod:

a. Visualizar la imagen del dispositivo iPod ya sea que se encuentre en formato .dmg o .dd.

b. Seleccionar la opción Archivo, Obtener información (Get Info).

c. En caso de que la imagen tenga extensión “.dd”, renombrarla a “.dmg”.

d. Bloquear el archivo: Seleccionar la casilla de verificación Bloqueado (Locked), impidiendo la escritura en la imagen, preservando la integridad del archivo.

e. Seleccionar la imagen y efectuar un doble click con el mouse y la imagen quedará montada.

f. Visualizar cinco carpetas: Calendario, Contactos, Notas, Fotografías y Grabaciones.

2. Visualizar las carpetas y archivos ocultos:

a. Abrir una terminal, en el menú Explorador (Finder), seleccionar Ir, utilidades.

b. Seleccionar Terminal.app.

c. En la línea de comando ingresar:

$defaults write com.appple.Finder AppleShowAllFiles Yes

Reiniciar el Buscador (Finder); este comando permite visualizar los archivos

ocultos:

$KillAll Finder

d. En el Buscador, seleccionar Mostrar todos para visualizar los archivos y carpetas ocultas.

3. Ocultar archivos y carpetas para que no se encuentren visibles:

a. Abrir una terminal, en el menú Buscador (Finder), seleccionar Ir, utilidades.

b. Seleccionar Terminal.app.

c. En la línea de comando ingresar:

$defaults write com.appple.Finder AppleShowAllFiles No Este comando permite reiniciar el Buscador (Finder):

$KillAll Finder

4. Reiniciar el Buscador (Finder) desde la interfaz gráfica:

a. Seleccionar el ícono de Apple (Manzana).

b. Seleccionar Ir (Go), Forzar salida (Force Quit).

c. Seleccionar el Buscador (Finder).

d. Oprimir Reiniciar (Relaunch).

5. Visualizar los archivos y carpetas del dispositivo iPod. Luego de reiniciar la aplicación de explorador de archivos del sistema operativo OS X (Finder), aparecerán también los archivos y carpetas ocultas:

- .DS_Store: Es un archivo que crea el sistema operativo OS X en cada carpeta.
- .fseventsd: Registra eventos de cada volumen.
- .metadata_never_index: Permite indexar en el volumen especificado.
- .SymAVQSFile: Archivo de Norton Antivirus.
- .Trashes: Almacena los elementos borrados.
- .Volumeicon.icns: Es el ícono que OS X utiliza para el dispositivo iPod cuando está montado en una computadora Mac.
- Calendarios (Calendars): Muestra los elementos del calendario que fueron sincronizados por el usuario desde iTunes hacia el dispositivo iPod. Los elementos del calendario se pueden visualizar en esta carpeta con la aplicación iCal.

6. Visualizar los elementos del Calendario de iPod con la aplicación de Calendario iCal.

a. Verificar que no se encuentre en ejecución la aplicación iCal en la computadora Mac.

b. Montar la imagen de iPod.

c. Verificar que las siguientes carpetas y archivos hayan sido borrados de la computadora Mac:

Carpetas:

- ~/Library/Calendar
- ~/Library/SyncServices
- ~/Library/Caches/com.apple.iCal Archivo:
- ~/Library/Preferences/com.apple.iCal.plist

d. Ubicar el archivo /Calendars/iSync-OSX iPodCalendario.ics (OSX iPodCalendario es el nombre del calendario).

e. Copiar el archivo OSX iPodCalendario.ics a una carpeta de la computadora Mac.

f. Arrastrar y tirar el archivo OSX iPodCalendario.ics; en el ícono de la aplicación iCal, aparecerán los elementos del calendario en pantalla.

g. Seleccionar cualquier día del calendario para visualizar la información contenida en cada entrada.

7. Visualizar la carpeta Contactos de iPod con una aplicación nativa de Mac denominada

Libreta de Direcciones (Address Book). La extensión de estos archivos es: ".vcf".

a. Verificar que no se encuentre en ejecución la aplicación Libreta de Direcciones (Address Book) en la computadora Mac.

b. Verificar que no exista información de contactos en la computadora Mac.

c. Borrar la carpeta ~/Library/ApplicationSupport/AddressBook.

d.

e. Copiar la carpeta Contactos del dispositivo iPod a la computadora de Informática forense Mac.

f. Seleccionar cualquier contacto para que sea abierto por la aplicación Libreta de Direcciones (Address Book).

8. Visualizar los archivos de Escritorio DB y DF; estos archivos no contienen evidencia.

9. Visualizar el contenido de la carpeta de Control iPod, donde se encuentran los archivos multimedia. Existen varias subcarpetas:

Artwork: Contiene un álbum de arte que puede ser visto en el iPod en el modo de previsualización en gran tamaño deslizándose por la pantalla (cover flow). La carpeta puede tener numerosos archivos:

- El archivo rtworkDB: Guarda el seguimiento de la sincronización del álbum artwork.
- Archivos de extensión ".ithmb": Son previsualizaciones en miniatura,

similares a las encontradas en Microsoft Windows, son archivos comprimidos de imágenes que son sincronizados desde la computadora Mac al iPod. Para ver estos archivos se puede utilizar la aplicación de libre disponibilidad denominada Keith´s iPod Photo Reader. Sitio de descarga:

http://keithwiley.com/software/keithsIPodPhotoReader.shtml

10. Visualizar el contenido de los archivos ".ithmb", con el programa lector Keith´s iPod Photo Reader:

a. Copiar los archivos con extensión ".ithmb" en una carpeta en la computadora de Informática forense Mac.

b. Ejecutar la aplicación Keith´s iPod Photo Reader.

c. Seleccionar el botón Cargar .ihtmb.

d. Seleccionar un archivo .ihtmb. Configurar la aplicación Keith´s iPod Photo Reader para visualizar las imágenes contenidas en el archivo comprimido .ihtmb (Por ejemplo: Resolución: 640x480 – Código de colores: 16 bit RGB).

i. Si la imagen no existe aparecerán valores de configuración sin formato.

ii. Si el archivo tiene una imagen, la aplicación mostrará la primera imagen en ese archivo.

Las imágenes sincronizadas a través de iTunes fueron modificadas, por lo tanto los hashes del archivo .ihtmb de fotos en un iPod serán diferentes.

e. Exportar las imágenes desde la aplicación Keith´s iPod Photo Reader y agregarlas al informe pericial, seleccionar Archivo, Guardar todas las imágenes, seleccionar el destino de la carpeta donde se exportarán. Los archivos se guardarán con la extensión ".pct".

11. Visualizar los archivos contenidos en la carpeta iTunes:

a. Editar el archivo iTunesDB contenido en la carpeta iTunes con un editor de texto. El archivo tiene información acerca de los Podcasts y videos descargados en el iPod.

b. Editar el archivo iTunes Prefs que contiene el nombre de la computadora con la cual se sincronizó. Este dato es muy importante para el perito, en el caso de tener que vincular el iPod con una determinada computadora en busca de evidencia.

c. Editar el archivo Rentals.plist, que contiene el nombre del archivo de las películas alquiladas a través de iTunes, oprimiendo la barra espaciadora en Mac, o convertir el archivo de binario al formato XML, utilizando la herramienta Plutil o cualquier otra disponible.

d. Visualizar el contenido de la carpeta Música, que contiene archivos de audio y video. El nombre actual de los archivos fueron cambiados al sincronizarse desde la computadora Mac al iPod. Los nombres de los archivos empiezan siempre con la letra "F" seguida de dos números utilizados en un

orden secuencial (F00, F01). El nombre de archivo convencional es de cuatro caracteres y la extensión del tipo de archivo (ABCD.m4v, JKLM.m4p). El hash de estos archivos coincidirá con los archivos de música encontrados en la biblioteca de iTunes de la computadora sincronizada Mac.

12. Visualizar el contenido de la carpeta Notas, solamente se podrán ver archivos de texto si el usuario tiene habilitado el uso del disco.

13. Visualizar la carpeta Fotografías (Photos):

a. Utilizar el mismo procedimiento descripto en la carpeta iTunes Control para visualizar los archivos .ithmb.

b. Visualizar el contenido de la subcarpeta Alta Resolución (Full Resolution). Los hashes de estas fotografías coincidirán con los archivos sincronizados de Mac, por lo tanto el perito obtendrá información del contenido del metadato, de la fecha y hora Mac, del tipo de cámara y modelo.

c. Visualizar el contenido de la subcarpeta Thumbs que presenta múltiples archivos del tipo .ithmb; estos archivos se pueden ver también con la aplicación Keith´s iPod Photo Reader.

d. Ubicar en la carpeta una fotografía.

e. Seleccionarla y abrirla con la aplicación iPhoto.

f. Efectuar un click en la imagen y mantener apretada la tecla Ctrl y luego seleccionar Mostrar información (Show info), para ver el metadato de la imagen (Imagen: Dimensiones de la imagen, fecha y hora original, fecha y hora de digitalización; Archivo: Nombre del archivo, tamaño, fecha y hora de modificación e importación; Cámara: Marca, modelo, software).

14. Visualizar el contenido de la carpeta Grabaciones (Recordings):

a. Verificar la existencia de archivos de grabaciones de voz del tipo ".amr" (aparece esta funcionalidad en los nuevos modelos de iPod con los nuevos auriculares de Apple).

15. Visualizar el contenido de los archivos de un dispositivo iPod utilizado como almacenamiento externo:

a. El perito podrá encontrar múltiples archivos de diferentes tipos de extensión. Efectuar un análisis individual de cada carpeta.

16. Visualizar los elementos (Artifacts) de iPod desde su correspondiente computadora Mac:

a. Verificar las aplicaciones sincronizadas con la computadora Mac, tales como: iCal, Contactos, Correo, iPhoto e iTunes, todos los datos pertenecen a un usuario específico; pueden encontrarse en el dominio del usuario.

b. Editar el archivo de propiedad (plist) que tiene cada usuario, que se encuentra en la carpeta: /[nombre de usuario]/Libreria/Preferences/com.apple.iPod.plist, oprimiendo la barra

espaciadora en Mac o convertir el archivo de binario al formato XML, utilizando la herramienta Plutil o cualquier otra disponible. El perito podrá ver en este archivo todos los iPods e iPhones conectados a la computadora Mac por cada usuario de Mac.

c. Editar el archivo de propiedad en el dominio local que se encuentra en la carpeta

/Libreria/Preferences/com.apple.iPod.plist oprimiendo la barra espaciadora en Mac, o convertir el archivo de binario al formato XML, utilizando la herramienta Plutil o cualquier otra disponible. El perito podrá ver con este archivo todos los iPods e iPhones conectados a la computadora local Mac.

d. Obtener la siguiente información de ambos archivos .plist:

- Versión de Firmware o sistema operativo.
- Número de serie del iPod.
- Fecha de la última conexión del iPod.
- Número de veces que se conectó el dispositivo.

17. Registrar, documentar y/o capturar pantallas con la información requerida.

síntesis – Lista de control

- Utilizar la herramienta de Mac hdiutil pmap para ver el esquema de partición de iPod.
- Utilizar la herramienta de Mac hdiutil imageinfo para obtener información detallada de la imagen de iPod.
- La información relevante para el perito se encuentra en las particiones HFS+.
- Para visualizar archivos y carpetas ocultas, ejecutar: defaults write com.apple.Finder AppleShowAllFiles Yes.
- Las aplicaciones Contactos, Calendarios, Correo y otro tipo de información pueden realizarse utilizando las aplicaciones Mac.
- El archivo iTunes Prefs contiene el nombre de la computadora con la cual se sincronizó.
- Los archivos de propiedad de iPod com.apple.iPod.plist de cada usuario contienen información específica del hardware del iPod y de las conexiones del dispositivo.
- Cuando un dispositivo iPod se sincroniza con una computadora Mac, esta recupera toda la información del iPod.

66 *Comparación de modelos y especificaciones técnicas de iPhone, http://theiphonewiki.com/wiki/index.php?title= IPhone mayo 2012.*

http://www.apple.com/es/iphone/compare-iphones/ mayo 2012.

67 *Evolución de HFS, http://en.wikipedia.org/wiki/HFS_Plus, http://es.wikipedia.org/wiki/HFS%2B mayo 2012.*

68 Descripción de la estructura, http://theiphonewiki.com/wiki/index.php?title=Big_Bear_5B108_%28iPhone%29 mayo 2012.

69 http://es.wikipedia.org/wiki/Memoria_flash mayo 2012.

70 *http://www.w3.org/XML/ mayo 2012.*

71 Hoog, Andrew y Strzempka, Katie, IPhone and iOS Forensics. Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS devices, Ed. Elsevier-Syngress, EE.UU., 2011.

72 *Kubasiak, Ryan, Morrisey Sean y Varsalone, Jesse, Mac OS X, iPod and iPhone Forensic Analysis DVD Toolkit, Ed.*

Elsevier-Syngress, EE.UU., 2009.

73 https://developer.apple.com/technologies/mac/cocoa.html mayo 2012.

74 https://developer.apple.com/library/mac/#documentation/CoreFoundation/Conceptual/CFDataFormatting/Articles/dfCreatingCFDateFormatters.html#//apple_ref/doc/uid/TP40002339-SW1 mayo 2012.

75 https://developer.apple.com/library/mac/#documentation/MacOSX/Conceptual/OSX_Technology_Overview/About/About.html#//apple_ref/doc/uid/TP40001067-CH204-TPXREF101 mayo 2012.

76 *https://developer.apple.com/library/mac/#documentation/Darwin/Reference/Manpages/man1/p mayo 2012.*

77 *Ayuda de Plutil. https://developer.apple.com/library/mac/#documentation/Darwin/Reference/Manpages/man1*

/plutil.1.html mayo 2012.

78 http://www.mcafee.com/us/resources/white-papers/foundstone/wp-intro-to-file-carving.pdf mayo 2012.

79 *Base de datos pública de firmas de archivos. http://www.filesignatures.net mayo 2012.*

Listado de firmas de Gary Kessler, http://www.garykessler.net/library/file_sigs.html mayo 2012.

80 Carrier, Brian, File System Forensics Analysis, Ed. Addison Wesley, EE.UU., 2005.

81 Arellano, Luis y Darahuge, María Elena, Manual de Informática Forense, Ed. Errepar, Buenos Aires, 2011.

82 Hoog, Andrew y Strzempka, Katie, IPhone and iOS Forensics. Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS devices, Ed. Elsevier-Syngress, EE.UU., 2011.

83 *Arellano, Luis y Darahuge, María Elena, Manual de Informática Forense, Ed. Errepar, Buenos Aires, 2011.*

84 *El bit menos significativo se guarda primero.*

85 Arellano, Luis y Darahuge, María Elena, Manual de Informática Forense, Ed. Errepar, Buenos Aires, 2011.

86 Ibídem.

87 http://www.sleuthkit.org/sleuthkit/man/fls.html.

88 http://www.sleuthkit.org/sleuthkit/man/mactime.html.

89 *Arellano, Luis y Darahuge, María Elena, Manual de Informática Forense, Ed. Errepar, Buenos Aires, 2011.*

90 Descargas para diversos sistemas operativos y tutorial, http://www.sqlite.org/download.html mayo 2012.

91 *Convertidor de fecha y hora, http://www.onlineconversion.com/unix_time.htm, http://www.epochconverter. com mayo 2012.*

92 El tiempo absoluto (absolute time) se calcula por el número de segundos entre la fecha de referencia y la fecha especificada. Los valores negativos indican fechas y horas anteriores a la fecha de referencia. Los valores positivos indican fechas y horas posteriores a la fecha de referencia.

93 *Kubasiak, Ryan, Morrisey Sean y Varsalone, Jesse, Mac OS X, iPod and iPhone Forensic Analysis DVD Toolkit, Ed.*

Elsevier-Syngress, EE.UU., 2009.

94 Abreviatura del término application, popularizado por Apple Computers Inc., al presentar en el mercado el dispositivo iPhone.

95 *En el dispositivo iPhone se visualiza la dirección MAC seleccionando Menú Inicio | Ajustes | General | Información*

y desplazarse hasta donde dice Dirección Wi-Fi.

96 Herramienta libre (Free) para convertir http://www.digital-detective.co.uk/freetools/decode.asp. Funciona en el sistema operativo Microsoft Windows.

97 http://en.wikipedia.org/wiki/List_of_mobile_country_codes.

98 http://en.wikipedia.org/wiki/Mobile_Network_Code.

99 Versión comercial y de prueba: http://www.elcomsoft.com/eppb.html mayo 2012.

Arellano, Luis y Darahuge, María Elena, Manual de Informática Forense, Ed. Errepar, Buenos Aires, 2011.

100 Ver el procedimiento “Recolección lógica de dispositivo iPhone, iPod táctil e iPad del resguardo efectuado con iTunes” descripto en el apartado sobre “Recolección Lógica”.

101 http://labs.neohapsis.com/2012/01/25/keychain-dumper-updated-for-ios-5/ mayo 2012.

102 En Windows XP SP2, el conjunto de herramientas de soporte contiene el programa Windiff: http://www.microsoft. com/downloads/es-es/details.aspx?familyid=49ae8576-9bb9-4126-9761-ba8011fabf38 mayo 2012.

103 *http://es.wikipedia.org/wiki/Groupon mayo 2012.*

104 *Arellano, Luis y Darahuge, María Elena, Manual de Informática Forense, Ed. Errepar, Buenos Aires, 2011.*

105 *Listado de modelos y especificaciones técnicas de iPod, http://support.apple.com/kb/ht1353 mayo 2012.*

106 Comparación de modelos de iPod, http://www.apple.com/ipod/compare-ipod-models/ mayo 2012.

107 http://www.nist.gov/ mayo 2012.

108 *Arellano, Luis y Darahuge, María Elena, Manual de Informática Forense, Ed. Errepar, Buenos Aires, 2011.*

109 *Kubasiak, Ryan, Morrisey Sean y Varsalone, Jesse, Mac OS X, iPod and iPhone Forensic Analysis DVD Toolkit, Ed.*

Elsevier-Syngress, EE.UU., 2009.

110 Ibídem.

111 *Arellano, Luis y Darahuge, María Elena, Manual de Informática Forense, Ed. Errepar, Buenos Aires, 2011.*

112 *http://krypted.com/mac-os-x/disable-disk-arbitration/ mayo 2012.*

113 *http://developer.apple.com/library/mac/#documentation/Darwin/Reference/ManPages/man1/h*

mayo 2012.

[114] *Kubasiak, Ryan, Morrisey Sean y Varsalone, Jesse, Mac OS X, iPod and iPhone Forensic Analysis DVD Toolkit, Ed.*

Elsevier-Syngress, EE.UU., 2009.

CAPÍTULO 9
COMPUTADORAS APPLE MACINTOSH

Consideraciones previas

El perito deberá ingresar al sitio del fabricante de Apple (www.apple.com) para conocer los diferentes modelos de computadoras Macintosh existentes en el mercado y sus respectivas especificaciones técnicas, como así también para determinar las últimas versiones del software de base y de aplicaciones. Esta información será relevante para el abordaje de la requisitoria pericial en los equipos de Macintosh.

El sistema operativo Mac OS X tiene sus raíces en Unix, es multiusuario y permite tener un control completo de los dispositivos en las versiones Mac OS X 10.4 o 10.5. Lo mismo ocurre con las versiones de Linux y en sus variantes disponibles como CD de arranque donde el sistema operativo fue compilado y alterado para no montar los dispositivos de almacenamiento en forma automática en el momento de arranque de la computadora.

El sistema de archivo utilizado por OS X se denomina HFS (Hierarchical File System Sistema jerárquico de archivos) Plus o Mac OS Extended (HFS+)*115*. Existen dos formatos de HFS+ para soportar la protección contra fallas de hardware y software (journalling) para el sistema de archivo HFSJ y la variante de nombres de archivos sensibles a las mayúsculas y minúsculas (HFSX). Las bases del sistema operativo Mac OS X se encuentran en el Unix BSD. El sistema de archivo es similar a Unix, posee el mismo modo de mostrar la ruta de los archivos.

La cabecera del volumen del sistema de archivo HFS es de 1024 bytes desde el comienzo del volumen y con una copia de resguardo de 1024 bytes ubicada antes del final del volumen. La cabecera contiene:

- Datos del sistema de archivo.
- El tamaño de bloques asignados, generalmente de 4 kb. Los bloques pueden estar agrupados en clusters; los datos del archivo se tratan como extensiones. Una extensión es un puntero de 4 bytes al inicio de un bloque de asignación y un valor de 4 bytes que indica la longitud de la extensión.
- La fecha y hora de la creación del volumen.
- La ubicación de los archivos especiales requeridos por HFS+ para su funcionamiento adecuado, se mantienen ocultos ($) y son cinco:
  - El archivo de asignación es un mapa de bits que efectúa el seguimiento del estado de asignación de espacio de cada bloque del volumen.
  - El archivo de catálogo contiene registros de cada archivo y directorio en el

volumen. Por necesidad, la ubicación de la primera extensión del archivo del catálogo se guarda en el encabezado del volumen. Los registros del catálogo tienen 8K de longitud y contienen:

- El nodo ID del catálogo (CNID) del archivo o carpeta.
- El nodo ID del catálogo (CNID) del padre.
- Metadatos de fecha y hora.
- Información acerca de los datos y bifurcaciones de recursos de los archivos.
  - El archivo de desbordamiento (overfolw) contiene registros para las bifurcaciones que tienen más de 8 extensiones asignadas. Esto indicaría un estado de fragmentación severa en el sistema de archivo HFS+.
  - El archivo de inicio (startup) se utiliza para mantener información empleada cuando se inicia un sistema que no conoce del sistema de archivo HFS+.
  - El archivo de atributos se puede utilizar para guardar atributos extendidos para los archivos. Se utiliza en la compresión por archivo en OS X 10.6.

Los ID (CNID) tienen un valor de asignación secuencial de 32 bits, iniciando en 16. No se reutilizan hasta que todos los 32 bits enteros (menos uno reservado para el CNID) hayan sido asignados. El CNID actuaría como una marca de tiempo. Los archivos que tienen un valor CNID más alto son más nuevos que los archivos con un valor CNID más bajo. Si un valor CNID no se encuentra, esto le indica al perito que en un momento hubo un archivo y que ha sido borrado.

Los archivos HFS+ pueden tener un nombre de hasta 255 caracteres y flujo de datos o bifurcaciones (similar a NTFS con ADS, alternative data stream, flujo de datos alternativos)*116*. Las dos bifurcaciones primarias son:

- De los datos: Posee el contenido del archivo.
- Del recurso: Está vacía o contiene información no esencial del archivo.

Las bifurcaciones adicionales pueden crearse para un archivo con fines específicos por parte del programa o aplicación.

La recuperación de datos borrados en HFS+ es difícil debido al balanceo constante de las estructuras de árboles binarios dentro del archivo de catálogo; la información de los metadatos de un archivo es sobrescrita rápidamente luego de borrar un archivo. A veces, con las herramientas de búsqueda de fragmentos (carving), es posible recuperar archivos, pero resulta complejo efectuar la correlación de los datos de los fragmentos con los nombres de archivos y fechas. Muchos formatos de datos contienen información secundaria que se puede extraer para su identificación y de esta forma efectuar la recuperación de información borrada.

Los permisos de los archivos son del estándar Posix y OS X los usa en forma

predeterminada. En versiones recientes el gestor de seguridad y protección del sistema operativo soporta las listas de control de acceso (ACL) para el control de los archivos. Esto no afecta el análisis del archivo de imagen recolectada por el perito, ya que este archivo es independiente de las restricciones del sistema operativo.

La estructura del sistema de archivo se implanta en la raíz "/" como en un sistema operativo Unix o Linux. Por debajo, se encuentran los siguientes directorios:

• Applications: Ubicación predeterminada para los programas instalados en OS X. Generalmente, programas que se ejecutarán a partir de la interfaz gráfica.

• Library: Información que se modifica en tiempo de ejecución de las aplicaciones, configuraciones de Preferencias.

• Network: Generalmente vacía.

• System: Contiene información específica del sistema operativo (similar a System32 en Windows).

• Users: El directorio padre de los directorios de inicio de los usuarios.

• Volumes: El directorio padre de los volúmenes montados (CDs, DVDs, discos de imagen DMG, semejante a /mnt o /media en Linux).

• Bin y sbin: Comandos estáticos y dinámicos.

• Dev: De archivos de dispositivo.

• Private: Versión del sistema operativo OS X de /var, /tmp y /etc.

Procedimiento para la preparación de la estación de trabajo de Informática forense Apple Macintosh

El perito deberá tener el DVD del sistema operativo OS X que acompaña al equipo Macintosh para la instalación en la arquitectura del procesador correspondiente PowerPC o Intel. En Mac OS X 10.5 ofrece un DVD de instalación tanto para Intel como para PowerPC, de requerimiento mínimo de 867 Mhz para el procesador G4[117].

Instalación del sistema operativo

1. Resguardar los datos, si los hubiera, del disco rígido o de los archivos de instalación de fábrica que no se encuentran en ningún otro dispositivo.
2. Insertar el DVD en la lectora.
3. Seleccionar el ícono Instalar Mac OS X, la computadora se reiniciará.
4. Efectuar el borrado seguro utilizando la herramienta Utilidad de disco (Disk utility) incluida en el DVD de instalación. Se puede encontrar utilizando del menú de Apple la aplicación de explorador gráfico de archivos del sistema

operativo OS X (Finder) previamente a la instalación de la actual versión del sistema operativo. La herramienta Utilidad de disco (Disk utility) permite efectuar un borrado seguro del disco rígido y particionar el disco.

5. Seleccionar el esquema de partición del disco rígido que se adecua a las necesidades del perito:

a. Una partición sola, el disco completo.

b. Dos particiones, una para el sistema operativo y otra para los datos.

6. Seleccionar el sistema de archivos. Para cada partición en un disco rígido interno debe ser del tipo extendida Mac OS Extended (Journaled). A partir de aquí, la instalación se realiza en forma desatendida y se reenviará con el sistema operativo instalado.

7. Instalar el conjunto de aplicaciones iLife (paquete de aplicaciones software orientado a la organización, visualización y edición de contenido multimedia), colocar el DVD en la lectora y buscar el ícono Instalar solamente las aplicaciones incluidas (Install Bundled Apps Only).

8. Actualizar la versión del sistema operativo instalado a través de Internet: Ir al menú de Apple y seleccionar Actualización de software (Software update). El perito deberá instalar todas las actualizaciones disponibles para el software instalado y repetir este proceso por segunda vez, con el fin de asegurarse de que el equipo posee todas las actualizaciones existentes hasta el momento.

9. Desconectar la computadora Macintosh de Internet.

10. Asegurar el equipo, desconectar los servicios de red inalámbrica y Bluetooth:

a. Ir al Menú de Apple y seleccionar Preferencias del sistema (System Preferences), la casilla de verificación de encendido de Bluetooth no debe estar seleccionada para poder deshabilitar el servicio.

b. En la ventana de red de Preferencias del sistema (Network System Preferences), aparecen todos los servicios disponibles:

i. Seleccionar servicio de Aeropuerto (AirPort) en la ventana de la izquierda y aparecerá un botón del lado de la derecha que indica Apagar Aeropuerto (Turn AirPort off); hacer click sobre el botón.

11. A partir de aquí, el perito podrá instalar las herramientas de Informática forense para Macintosh. El equipo ya no deberá conectarse a Internet.

12. Preparar las herramientas (Listado de herramientas de Informática forense para Macintosh*118*) y certificarlas matemáticamente*119*, colocarlas en un dispositivo externo e instalarlas o copiarlas en la computadora Macintosh.

13. Registrar, documentar y/o capturar pantallas con la información requerida.

a. Teclas para la captura de pantalla:

i. Comando (Command)-Shift-3: Captura el escritorio completo.

ii. Comando -Shift-4: Permite la captura de un área específica.

iii. Comando -Shift-4-Barra espaciadora: Captura la ventana activa.

iv. Comando -Control-Shift-3: Captura la pantalla y la guarda en el portapapeles. La tecla Ctrl sumada con cualquiera de las opciones anteriores envía la captura de pantalla al portapapeles.

b. En el menú Utilidades se encuentra la aplicación Grabar (Grab). Captura pantallas agregando la fecha y hora. Los archivos capturados son .TIFF y el perito le puede asignar cualquier nombre. Si se desea cambiar la extensión del archivo de captura, abrir una terminal y ejecutar:

defaults write com.apple.screencapture type png defaults write com.apple.screencapture type pdf defaults write com.apple.screencapture type jpg defaults write com.apple.screencapture type tif defaults write com.apple.screencapture type psd

killall SystemUIServer, para que los cambios sean aplicados.

síntesis – Lista de Control

· Preparar la estación de Informática forense Macintosh efectuando el borrado seguro del disco.

· Reinstalar el sistema operativo con el DVD de instalación de Mac y las aplicaciones necesarias que el perito requiera para efectuar su labor pericial.

· Deshabilitar los accesos inseguros a la computadora de redes inalámbricas y Bluetooth.

Etapa de recolección y adquisición de datos

En esta etapa se pueden aplicar diversas técnicas para efectuar la recolección de información:

· Recolección en vivo.

· Modo usuario único (Single User).

· Inicio con CD/DVD en vivo.

· Modo de disco destino (TDM Target Disk Mode).

Procedimiento de adquisición de una imagen de una computadora Macintosh con una computadora Macintosh

Consideraciones previas

El procedimiento de crear una imagen de una computadora Mac con otra Mac es un método fácil de adquisición física de evidencia. La tarea de quitar el disco rígido de una notebook Mac o de algunos modelos de computadora de

escritorio de Mac puede ser una tarea muy tediosa. Durante mucho tiempo, Macintosh ha ofrecido la característica denominada “Modo de disco destino TDM” (Target Disk Mode)[120], que permite a la computadora Mac con un puerto FireWire (computadora objetivo) ser utilizada como un disco duro FireWire externo conectado a otra computadora (el host). Una vez que la computadora se ha reiniciado como un disco FireWire y está disponible para la computadora host, el perito puede copiar de un volumen u otro. La técnica TDM facilita la tarea de abrir la computadora y quitar el disco rígido, no obstante no se encuentra disponible en todos los modelos de Mac.

Los requisitos para las computadoras host son:

- Puerto incorporado o una placa PC con puerto FireWire.
- FireWire 2.3.3 o superior.
- Mac OS 8.6 o superior.

Los modelos de computadoras TDM u objetivo son:

- iMac (Slot Loading) con firmware versión 2.4 o posterior.
- iMac (Summer 2000) y todos los modelos posteriores a julio 2000.
- eMac (todos los modelos).
- Mac Mini (todos los modelos).
- Power Mac G4 (AGP Graphics) with ATA drive.
- Power Mac G4 Cube.
- Power Mac G4 (Gigabit Ethernet), todos los modelos posteriores a julio 2000.
- Power Mac G5 (todos los modelos).
- Mac Pro (todos los modelos).
- iBook (FireWire), todos los modelos posteriores a septiembre 2000.
- PowerBook G3 (FireWire).
- PowerBook G4 (todos los modelos).
- MacBook Pro (todos los modelos).
- MacBook, modelos anteriores a octubre 2008.

FireWire TDM funciona solamente con PATA o SATA. TDM solo conecta al dispositivo maestro (master) PATA en una controladora Ultra ATA. No se conecta a dispositivos esclavos (slave) ATA, ATAPI o SCSI. Esto también se aplica a todas las computadoras Mac que soportan múltiples discos. El perito deberá verificar el interior de la computadora Power Mac, Mac Pro o XServe para determinar la existencia de múltiples discos cuando realiza la adquisición de datos. Es probable que el perito deba considerar quitar los discos rígidos y efectuar individualmente la imagen de cada uno, en el caso de que no aparezcan con TDM.

Si la computadora Mac no se encuentra incluida en el listado de computadoras TDM, el perito necesitará efectuar la imagen con un CD de arranque o físicamente remover el disco rígido de la computadora Macintosh para realizar la imagen. En este caso, el perito deberá colocar los cables respectivos para conectar el disco rígido a la computadora de Informática forense Mac, como así también necesitará una conexión externa USB o FireWire para el disco rígido que utilizará como destino de la imagen.

El perito nunca deberá conectar un dispositivo para la adquisición de la imagen como un disco interno dentro de la computadora de Informática forense Mac, porque no tendrá control cuando se monte el dispositivo.

La funcionalidad TDM no siempre está disponible. Si se ha utilizado una clave de firmware abierta, la computadora Mac no se iniciará con TDM. El perito debe verificar previamente la existencia de esta funcionalidad antes de realizar cualquier tarea de recolección o adquisición de la imagen.

Para verificar la existencia de una protección por contraseña de firmware (Open Firmware Password), simplemente reiniciar la computadora Mac presionando la tecla de Opción (Option). Si la computadora muestra un ícono de Bloqueado (Lock) con un cuadro de diálogo para clave, entonces existe una protección por contraseña de firmware; si aparecen íconos de las particiones de inicio disponibles, significa que no se aplicó ninguna clave.

Todas las computadoras Macintosh con procesadores Intel admiten la protección por contraseña de firmware.

Las siguientes computadoras de Apple pueden usar la protección por contraseña de firmware.

- iMac (carga por ranura) y modelos posteriores del iMac G3.
- iMac (pantalla plana) y modelos posteriores del iMac G4.
- iMac G5 y modelos posteriores del iMac G5.
- iBook, todos los modelos, tanto con procesadores G3 como G4.
- eMac, todos los modelos.
- PowerBook (FireWire).
- PowerBook G4 y modelos posteriores del PowerBook G4.
- Power Mac G4 (AGP Graphics) y modelos posteriores del Power Mac G4.
- Power Mac G4 Cube, todos los modelos.
- Power Mac G5 y modelos posteriores del Power Mac G5.
- Todos los Mac con procesadores Intel.
- MacBook Air.
- Todos los Mac con procesadores Intel.
- MacBook Air, consultar http://support.apple.com/kb/TS2391?

viewlocale=es_ES.

Funciones de la protección con contraseña de firmware para computadoras Mac con procesadores PowerPC e Intel*	PowerPC	Intel
Impide usar la tecla “C” para arrancar desde un disco óptico.	√	√
Impide usar la tecla “D” para arrancar desde el volumen de diagnóstico del DVD de instalación.		√
Impide usar la tecla “N” para arrancar desde un servidor NetBoot.	√	√
Impide usar la tecla “T” para arrancar en Modalidad de disco de destino (en los ordenadores que ofrecen esa característica).	√	√
Impide arrancar en modo verboso al pulsar la combinación de teclas Comando-V durante el arranque.	√	√
Impide arrancar en modo de un solo usuario al pulsar la combinación de teclas Comando-S durante el arranque.	√	√
Impide restablecer la RAM de parámetros (PRAM) al pulsar la combinación de teclas Comando-Opción-P-R durante el arranque.	√	√
Solicita la contraseña para introducir comandos tras iniciar en Open Firmware (para iniciar en esa utilidad, pulsar la combinación de teclas Comando-Opción-O-F durante el arranque).	√	
Impide arrancar en el modo de inicio seguro al pulsar la tecla Mayúsculas durante el arranque.	√	√
Solicita la contraseña para usar el gestor de arranque, al que se accede pulsando la tecla Opción durante el arranque (ver más abajo).	√	√

*http://support.apple.com/kb/HT1352?viewlocale=es_ES mayo 2012.

La contraseña de protección puede ser modificada o cambiada (excepto en MacBook Air) por:

- Un usuario administrador designado en las preferencias de Cuentas de usuarios.
- El acceso físico al disco dentro de la computadora.
- El reinicio de la computadora con un sistema operativo Mac OS 9.

El perito determinará si para la recolección utilizará la funcionalidad TDM o si removerá el o los discos para efectuar la imagen.

Secuencia de pasos para la preparación de adquisición de la imagen

La mayoría de las imágenes del sistema operativo OS X son del tipo .dmg. DMG es una imagen de un disco independiente en el formato UDIF (Universal

Disk Image Format, Formato de imagen de disco universal), siendo esta la forma nativa de archivo de imagen de OS X. Esta imagen contiene el sistema de archivo HFS+. Las imágenes UDIF pueden comprimirse, dividirse o encriptarse.

1. Verificar los discos físicos conectados en la computadora Mac:

a. Abrir una terminal y ejecutar:

$cd /dev ls disk?

El resultado devuelve los discos existentes en el sistema: disk0 disk1 disk2

2. Obtener información detallada de los discos (punto de montaje, tamaño, particiones), comando diskutil (requiere tener habilitado el demonio [servicio] de arbitraje de disco: DiskArbitration para montar y desmontar dispositivos de almacenamiento cuando se colocan en la computadora, ejemplo: dispositivos USB):

$man diskutil (ayuda del comando)

$disktutil list /dev/disk0

/dev/disk0

#: TYPE NAME SIZE IDENTIFIER

0: GUID_partition_scheme *298.1 Gi disk0 1: EFI 200.0 Mi disk0s1

2: Apple_HFS Macintosh HD 297.8 Gi disk0s2

El resultado muestra información detallada del disco 0 (disk0):

Un disco físico con tres particiones, referidas en el formato Macintosh (o Unix):

· 0: Refiere al disco físico, en la línea de referencia del disco físico (298.Gi) tiene un "*"; esto significa que informa el tamaño y que este difiere de su tamaño actual. Esto es muy importante para el perito, que siempre debe tener un disco físico preparado de mayor tamaño para efectuar la adquisición o duplicación de la imagen.

· 1: Es la interfaz de firmware extensible EFI[121] (Extensible Firmware Interface).

· 2: Es la partición del sistema de archivos jerárquico de Macintosh HFS (Hierarchical File System).

3. Obtener información del disco cuando no está habilitada la función de arbitraje de disco DiskArbitration, con el comando hdiutil, el cual se puede utilizar independientemente de la habilitación o no del demonio (servicio) DiskArbitration:

$hdiutil partition /dev/disk0

El resultado muestra un detalle del disco rígido: MBR, tabla de partición del disco de arranque, datos del fabricante y las ubicaciones de las particiones.

Para evitar confusiones respecto de los dispositivos de discos rígidos conectados en la computadora Mac, es conveniente que el perito tenga un solo disco en la computadora de Informática forense Mac, el disco de arranque será siempre el /dev/disk0; si el perito sabe que tiene un solo disco, le resultará más fácil identificar posteriormente los discos que se vayan conectando a la computadora.

4. Desactivar el demonio (servicio) DiskArbitration, en:

a. Mac OS X 10.5

$ sudo launchctl unload /System/Library/LaunchDaemons/com.apple.diskarbitrationd.plist

b. En Mac OS X 10.4

$ sudo cp /etc/mach_init.d/diskarbitrationd.plist /Backup/

$sudo rm /etc/mach_init.d/diskarbitrationd.plist

El comando rm elimina el archivo. El perito deberá tener un resguardo del archivo

diskarbitrationd.plist, de lo contrario no podrá reactivar el demonio.

Reiniciar la computadora Macintosh y el demonio (servicio) DiskArbitration estará deshabilitado.

5. Activar el demonio (servicio) DiskArbitration, en Mac OS X 10.5:

$ sudo launchctl load

/System/Library/LaunchDaemons/com.apple.diskarbitrationd.plist

$killall Finder

Los comandos de activar y desactivar el demonio de DiskArbitration le permiten al perito tener control sobre este, los cuales serán necesarios en el proceso de adquisición o duplicación de la imagen del disco.

a. En Mac OS X 10.4

$ sudo cp /Backup/diskarbitrationd.plist /etc/mach_init.d/

Reiniciar la computadora Macintosh y el demonio (servicio) DiskArbitration estará habilitado.

6. Conectar el dispositivo para adquirir o duplicar la imagen a la computadora de Informática forense Mac, utilizando tanto TDM o el método de remover el disco y conectarlo a través de un conector USB o FireWire:

a. Verificar el disco conectado:

$ls /dev/disk?

El resultado puede mostrar la asignación secuencial de números de discos o no.

7. Verificar los detalles del disco conectado utilizando el comando hdiutil:

$hdiutil partition /dev/disk4

El resultado muestra el detalle del disco y el tamaño del bloque o sector de 512 bytes. El perito deberá calcular el tamaño del disco aproximado en megabytes para determinar el tamaño del dispositivo que almacenará la imagen. El cálculo será el siguiente:

(Nro. de sectores) multiplicado por

(Tamaño del sector: 512 bytes) dividido por

(1.048.576 bytes)

Secuencia de pasos para la adquisición de la imagen

Los pasos previos le permiten al perito:

- Determinar si está habilitado TDM.
- Controlar el demonio (servicio) DiskArbitration.
- Obtener información detallada del disco.

8. Desactivar el demonio (servicio) DiskArbitration.
9. Reiniciar la computadora Macintosh presionando el botón de apagado y manteniendo presionada la tecla de Opción para verificar si existe una contraseña de protección de firmware; si no existe contraseña:
10. Apagar la computadora Macintosh presionando el botón de apagado, volver a presionarlo para encender la computadora presionando inmediatamente la tecla “T”, que le permite ingresar en el modo TDM.
11. Utilizar un cable de FireWire y conectar un extremo al TDM Mac.
12. Conectar el otro extremo del cable a la computadora de Informática forense Macintosh, que ya tiene deshabilitado el demonio (servicio) DiskArbitration. Si se conecta un disco removido (externo), se lo deberá conectar a la computadora Mac a través de la conexión apropiada USB o FireWire.
13. Ingresar en la terminal el comando $ls disk?. Se deberá ver un disco más conectado (a través de TDM o por medio del disco externo).
14. Verificar el disco agregado con el comando:

$hdiutil partition /dev/disk3 (o el número de disco que corresponda)

15. Calcular el tamaño del disco rígido interno de la computadora Mac dubitada de donde se efectuará la adquisición de la imagen, para determinar si se tiene suficiente espacio en la computadora de Informática forense Macintosh o si será necesario conectar un dispositivo externo más grande para alojar la imagen.
16. Crear una carpeta en el escritorio como destino de la imagen:

$mkdir ~/Desktop/Imagen_Mac

17. Calcular el hash del dispositivo de la Mac dubitada y enviar el resultado a un archivo de texto:

$md5 /dev/disk3 > ~/Desktop/Imagen_Mac/Mac_dubitada.md5.txt

18. Iniciar la duplicación o adquisición de la imagen, con el comando dd[122]:

$sudo dd if=/dev/disk3 conv=noerror,sync of=~/Desktop/Imagen_Mac/imagen_Mac_ dubitada.dmg

19. Al finalizar la adquisición o duplicación de la imagen, el comando dd devuelve el resultado de la adquisición (Records In y Records Out).

20. Apagar la computadora Mac dubitada presionando la tecla de apagado o desconectar el disco rígido externo utilizado en la adquisición.

21. Validar la imagen adquirida o duplicada con el cálculo del hash y el resultado a un archivo de texto:

$md5 ~/Desktop/Imagen_Mac/imagen_Mac_dubitada.dmg > ~/Desktop/Imagen_Mac/ imagen_Mac_dubitada.dmg.md5.txt

22. Cerrar la ventana de la terminal en la computadora de Informática forense Macintosh.

23. Ingresar al escritorio y abrir la carpeta Imagen_Mac.

24. En el archivo de la imagen, efectuar un solo click del mouse; si se hacen dos clicks se montará la imagen y se pueden producir cambios inmediatos en los datos del archivo.

25. En la barra de menú, seleccionar el explorador gráfico de archivos (Finder), seleccionar Archivo (File) y seleccionar Obtener Información (Get Info).

26. En el menú de Obtener Información (Get Info), seleccionar el cuadro de verificación de Bloqueado (Locked), para evitar cambios o modificaciones en el archivo de la imagen.

27. Cerrar la ventana de Obtener Información (Get Info).

28. En la carpeta Imagen_Mac, abrir los dos archivos de texto creados con el resultado del cálculo del hash MD5 y comparar los valores. Si no son iguales significa que hubo un error en el procedimiento de adquisición. Las causas pueden ser:

- Verificar el cable FireWire.
- Verificar el disco rígido destino de la imagen.

29. Registrar y documentar el resultado.

Procedimiento alternativo para la adquisición o duplicación de la imagen utilizando un CD de Linux

en vivo

Consideraciones previas

Efectuar la imagen del tipo Mac a Mac es el escenario ideal para el perito, ya que se reducen los problemas relacionados con la configuración y compatibilidad. No obstante, en otras oportunidades, el perito deberá realizar la imagen utilizando otros métodos, como iniciar la computadora Mac dubitada con un CD de herramientas de Informática forense de Linux en vivo. En el caso de Mac no cualquier CD de Linux de inicio en vivo funciona correctamente, por esta razón el perito deberá tener un conjunto de CDs de Linux de inicio en vivo para que alguno de ellos sea compatible con la versión y la configuración de la computadora Mac dubitada. Las distribuciones con kernel o núcleo de Linux compatibles con Mac son:

- De libre disponibilidad, Raptor (http://www.forwarddiscovery.com/Raptor), y
- Helix (http://www.e-fense.com/products.php), versión de evaluación por 30 días sin compromiso de compra.

Ambas distribuciones pueden iniciar el sistema en la arquitectura de microprocesador Intel. La distribución Raptor también es compatible con microprocesadores PowerPC G4 y G5 de Macintosh. Además, reconocen el sistema de archivo HFS+, por lo tanto con ambas distribuciones es posible que el perito pueda realizar una vista previa de los contenidos de la computadora Mac dubitada.

La herramienta SMART para Informática forense de http://www.asrdata.com/forensicsoftware/software-download/, presenta herramientas de evaluación, comerciales y de libre disponibilidad para Linux, Windows y Macintosh. El CD en vivo posee las distribuciones Slackware y Ubuntu.

La herramienta comercial MacQuisition de la empresa BlackBag (https://www.blackbagtech.com/forensics/macquisition/macquisition.html) permite realizar la adquisición o recolección de datos e imagen de alrededor de 185 modelos diferentes de computadoras Macintosh. Esta herramienta se ejecuta en el sistema operativo OS X y puede efectuar un inicio seguro del sistema y recolectar datos en el sistema operativo nativo de las computadoras Xserve, Mac, iMac, Mac Mini, MacBook y MacBook Air.

1. Iniciar la computadora Macintosh dubitada e inmediatamente mantener presionada la tecla de Opción (Option).
2. Si aparece el ícono de Bloqueado (Lock) y el cuadro de diálogo de autenticación, está indicando que existe una contraseña de protección del firmware.

a. El perito deberá evaluar si aplicará la técnica de Apple para remover la contraseña aunque se pierda la información de fecha y hora a raíz de este procedimiento.

3. Si aparece un listado de particiones y dispositivos, el perito tendrá acceso a la computadora Macintosh y puede insertar el CD o DVD de inicio en vivo.

4. Si el CD/DVD no muestra automáticamente la lista después de unos pocos segundos, seleccionar el ícono de Refrescar (una flecha curva); si aun así no muestra la lista, está indicando que el CD/DVD no es compatible o no lo reconoce como CD/DVD de inicio o arranque. El perito deberá evaluar el uso de otra distribución de CD/DVD.

5. Si el CD/DVD inició el sistema correctamente, el perito deberá conectar el dispositivo externo para la obtención de la imagen o conectar, si está en el laboratorio, a la red de este con un ancho de banda de Gigabit Ethernet para optimizar la adquisición.

6. Registrar y documentar los resultados.

síntesis – Lista de control

Efectuar la imagen de Macintosh a Macintosh

· Utilizar la técnica de Modo de disco destino TDM (Target Disk Mode) para que una computadora Mac actúe como un disco rígido externo FireWire, y utilizando otra computadora Mac se puede realizar la imagen bit a bit.

· Al utilizar la computadora de Informática forense Macintosh para la adquisición o duplicación bit a bit, se debe:

– Deshabilitar el demonio (servicio) DiskArbitration, para evitar el montaje automático de los dispositivos de almacenamiento.

· Utilizar las herramientas incluidas en el sistema operativo OS X para efectuar la copia bit a bit con el comando dd y la certificación de la imagen con el comando de hash MD5 o los comandos dcfldd y dc3dd instalados previamente en la computadora de Informática forense Macintosh.

Efectuar la imagen de una computadora dubitada Macintosh con un CD/DVD de arranque o inicio en vivo

· Seleccionar el CD/DVD de inicio adecuado para la Mac de distribución Linux o del sistema operativo OS X específico de Mac.

· Previo al inicio o arranque del CD/DVD, verificar si la computadora Macintosh dubitada posee contraseña de protección de firmware. El perito deberá evaluar la situación de remover la contraseña y los riesgos de modificar la información de fecha y hora con este procedimiento.

• Utilizar un dispositivo externo para el destino de la imagen a duplicar verificando que sea de un tamaño superior al de la computadora dubitada Macintosh.

• Realizar prácticas previas con diferentes métodos de obtención de imágenes para las computadoras Macintosh.

Procedimiento para determinar la fecha y hora en Macintosh

Consideraciones previas

En las computadoras Macintosh no existe la opción del BIOS o teclas de acceso al mismo (F2, Supr, etc.). En las arquitecturas PowerPC se utiliza OpenFirmware[123] de Sun Microsystems, e Intel utiliza la Interfaz Extensible del Firmware (Extensible Firmware Interface EFI)[124]. La fecha y la hora se obtienen con un procedimiento específico para Macintosh. El perito deberá conocer el tipo de arquitectura de la computadora y el firmware asociado.

1. Conectar el monitor y el teclado a la computadora Macintosh[125].
2. Presionar el botón de encendido e inmediatamente mantener apretada la tecla opción (Alt) del teclado.
3. Aparecerá una de las siguientes pantallas:

a. Particiones disponibles.

b. Cuadro de diálogo para ingresar la clave.

4. Si no existe clave de acceso y aparece la pantalla con las particiones:

a. Apagar el equipo manteniendo apretado por cuatro segundos el botón de encendido/apagado del equipo.

5. Oprimir el botón de encendido de la computadora e inmediatamente mantener apretada la tecla de comando (Apple) y la tecla “S”.

De esta forma ingresa al modo de usuario único. Aparecerá un texto en la pantalla y un cursor de línea de comando en la parte inferior de la pantalla.

6. Ingresar el comando “date” y presionar Enter.

Aparecerá la fecha y hora de la computadora Macintosh junto con la información de la zona horaria, tal como fue configurada por el usuario.

7. Apagar la computadora Macintosh.

Otras formas de acceder

• DVD de instalación de OS X:

a. Iniciar la computadora Macintosh con el DVD de instalación del sistema operativo OS X.

b. Abrir una terminal desde el DVD.

c. Ingresar el comando “date”.

Aparecerán los mismos resultados que en el proceso anterior.

· Linux CD en vivo para la computadora Macintosh:

a. Iniciar la computadora Macintosh con CD en vivo de Linux.

b. Abrir una terminal desde el CD en vivo.

c. Ingresar el comando man de “date”, para ejecutarlo con las opciones requeridas.

d. Ingresar el comando “date”.

8. Registrar y documentar los resultados.

Procedimiento para la recolección de datos de memoria volátil[126] en un sistema desbloqueado

Consideraciones previas

Los elementos a recolectar en la memoria volátil se describieron en detalle en el Manual de Informática Forense. En Mac se aclaran ciertas particularidades respecto de la recolección de la información en RAM, propias del sistema operativo Mac.

El sistema OS X debe estar funcionando y el perito debe tener permisos irrestrictos para acceder al escritorio del usuario. El perito deberá examinar si la carpeta de inicio o el directorio de trabajo del usuario tienen implementada la protección con el servicio de FileVault[127] que utiliza el algoritmo de Encripción Estándar Avanzada (Advanced Encryption Standard-AES-128) con claves de 128-bit. El servicio de cifrado de la carpeta de inicio aparece con la versión del sistema operativo OS X 10.3 (Panther) y es propietario de Apple, solo se aplica individualmente por usuario y no al disco completo.

Para habilitar el servicio se debe definir una contraseña maestra. Esta contraseña es una de las dos claves que se utilizan durante el proceso de cifrado cuando se crea la carpeta de inicio protegida o caja fuerte con el servicio de FileVault. La clave maestra se utiliza también para cambiar la contraseña. Si el perito posee la clave maestra podrá desencriptar las carpetas de inicio que se encuentren en el sistema; si no tiene acceso a la contraseña no podrá desactivar el servicio ni cambiar a una nueva clave maestra. La otra contraseña es la del usuario que se utiliza para ingresar.

La activación del servicio se realiza en la ventana de diálogo de preferencias del sistema de FileVault, seleccionando la opción de activar FileVault. Luego aparece un cuadro de diálogo de advertencia que es de importancia tanto para el usuario como para el perito:

· Para cifrar los datos se requieren dos claves: la clave de usuario y la clave maestra.

· Cualquier cuenta de usuario con FileVault activado no utilizará el servicio

del protocolo SMB (Server Message Block[128]) para compartir archivos e impresoras. En este caso, el perito deberá tener en cuenta que no podrá transmitir datos a través de SMB y copiar la carpeta de inicio del usuario.

- Existe un cambio notable en la forma de funcionar de la utilidad de resguardo (Time Machine)[129], con el servicio de FileVault activado. El resguardo de datos se producirá solamente cuando el usuario cierre la sesión.
- Existe la opción de borrado seguro de la carpeta completa de inicio o de trabajo del usuario, luego de activar el servicio de FileVault y el encriptado. El servicio FileVault crea una carpeta de inicio o de trabajo del usuario segura, utilizando el método de imagen de los espacios asignados o de los que contienen datos (sparseimage) o el método de crecimiento dinámico de la imagen a través del tiempo (sparsebundle). Ambas son similares a una imagen de disco DMG[130] (Disk Image). Cuando el sistema operativo crea la imagen de disco para la carpeta de inicio del nuevo usuario, copia la carpeta de trabajo completa del usuario en la imagen de disco. El borrado seguro ofrece al usuario la posibilidad de borrar en forma segura todas las carpetas de inicio viejas remanentes que fueron copiadas en la imagen de disco evitando de esta forma la recuperación de los datos sensibles por medio de herramientas de Informática forense.
- Para copiar la carpeta de inicio del usuario con el servicio de FileVault, es necesario enviarla a un dispositivo externo con el sistema de archivo HFS+[131], con el fin de mantener la estructura de datos. Si bien este proceso implica la modificación del estado actual del sistema dejando trazas del momento en que se realizó la copia, es el único método de recolección de la carpeta de inicio desencriptada. El perito deberá dejar constancia de esta circunstancia e informar pormenorizadamente al tribunal interventor de dicha circunstancia, ya que convierte al acto en irrepetible y modifica los archivos, contaminando la prueba. El juez determinará la pertinencia, forma y momento de realizar la tarea, en especial para notificar a las partes sobre el carácter modificatorio de la tarea pericial a realizar y su consecuencia de irrepetibilidad e imposibilidad de restaurar el estado original. Todo el acto debe ser resguardado en acta, en presencia de los autorizados por S. Sa., en forma clara, completa y detallada, para evitar futuras impugnaciones por contaminación de la prueba recolectada e imposibilidad de auditoría posterior.
- E informar oportunamente de esta característica para su posterior consideración de validez de la prueba.

9. Examinar la carpeta de inicio del usuario para determinar si se encuentra cifrada con el servicio de FileVault; en el sistema desbloqueado, visualizar el ícono de la casa con una perilla de combinación como si fuera una caja fuerte:
10. Recolectar la información contenida en esta carpeta y enviarla a un

dispositivo externo, que posee el sistema de archivo HFS+ y una carpeta creada para la recolección (por ejemplo: recolec_inicio), mientras se encuentre abierta la sesión del usuario los datos no estarán cifrados. Si se apaga la computadora, el perito necesitará las claves para acceder a la carpeta.

a. Verificar que el dispositivo externo conectado aparezca en el escritorio.

b. En la barra de menú seleccionar Ir (Go), Utilidades y seleccionar Terminal.

c. En la ventana de la Terminal, seleccionar la flecha izquierda de navegación en la esquina superior izquierda de la ventana. Aparecerán los contenidos del dispositivo externo conectado, verificar el nombre del dispositivo en el centro de la barra de título de la ventana.

d. Ingresar el siguiente comando en la Terminal:

cd /Users

Ubicarse en el directorio de Usuarios, que contiene las carpetas de inicio de los usuarios:

ls –la

Listar el contenido del directorio, visualizar la carpeta de inicio con el servicio de

FileVault activado:

cp –Rp /Users/nombre_del_usuario

(-R: copiar el directorio, -p: conservar las configuraciones) No presionar Enter.

Arrastrar la carpeta del dispositivo externo (recolec_inicio) dentro de la ventana de la Terminal, de esta forma se escribirá automáticamente el destino de la copia:

cp –Rp /Users/nombre_del_usuario

/Volumes/DiscoExterno/recolec_inicio/ Presionar Enter.

Durante la copia pueden aparecer mensajes de error indicando que ciertos archivos no serán copiados; el perito deberá registrar esta información.

Al finalizar la copia, aparece el cursor intermitente a la espera de otro comando, esto indica que la copia ha finalizado.

11. El perito no deberá desactivar la caja fuerte o el servicio de cifrado de FileVault (el proceso solicita una clave). Aun teniendo la clave del usuario, esta acción podría sobrescribir datos valiosos en el espacio no asignado del disco rígido, esto se debe a que el espacio utilizado para el proceso de desencriptar puede sobrescribir importantes datos.

12. Registrar y documentar los resultados.

Procedimiento para la recolección de datos de

memoria volátil en un sistema bloqueado

Consideraciones previas

Si el perito no posee la clave para desbloquear el acceso a la computadora, deberá utilizar la técnica de ataque por la conexión FireWire, desarrollada por Adam Boileau[132], la cual no es viable para la recolección en Informática forense, ya que implica el uso de una computadora Linux que ejecute un programa de acceso directo a la memoria a través del puerto de FireWire de la computadora Mac, convirtiéndola en una técnica invasiva que modifica los datos existentes en la memoria RAM y además engaña al sistema operativo, porque este considera que se conectó un dispositivo iPod. Por supuesto esta actividad es ilegítima e ilegal, salvo que haya sido informada previamente al tribunal interventor y el juez la haya autorizado y/u ordenado, ya que está dentro de sus facultades, cumpliendo los requisitos de preservación del debido proceso (entre otros, la notificación a las partes, para que puedan presenciar la actividad pericial, en razón de su carácter invasivo, las modificaciones que produce en la prueba a recolectar, la imposibilidad de restaurar la prueba documental informática recolectada a su estado original y el carácter irrepetible del acto pericial que impide la auditoría y control de resultados posterior).

Por lo tanto, la herramienta que se puede utilizar es el programa msramdmp, desarrollada por Wesley McGrew[133]. La herramienta captura y escribe contenidos de la memoria RAM de un sistema a un dispositivo USB. Esta técnica efectúa un apagado del equipo, seguido de su encendido, oprimiendo la tecla Opción e insertando el CD ROM con el programa msramdmp y el dispositivo USB, en el cual se crea una imagen de la memoria RAM y se puede visualizar con un editor de hexadecimal. La aplicación de este programa requiere la aplicación de los siguientes pasos para la preparación de los dispositivos a utilizar:

1. Descargar la imagen ISO del programa msramdmp del sitio del desarrollador de la herramienta: http://www.mcgrewsecurity.com/tools/msramdmp/.
2. En la estación de trabajo de Informática forense Apple Macintosh, en la barra de menú seleccionar Ir (Go), Utilidades y abrir la utilidad Disk Utility.app.
3. En el menú Archivo (File), seleccionar Abrir imagen de disco y seleccionar la imagen msramdmp_cd.iso del escritorio.
4. Seleccionar la imagen msramdmp_cd.iso del panel de Disco y Volumen y presionar Grabar.
5. Preparar el dispositivo de almacenamiento USB para la recolección de la

memoria RAM, conectar el dispositivo para efectuar el borrado seguro.

6. En la barra de menú seleccionar Ir (Go), Utilidades y abrir Disk Utility.app.

7. Seleccionar el disco USB del panel de Disco y Volumen y seleccionar el botón de Borrado

(Erase) de la barra de menú.

8. En el panel de la derecha, seleccionar el formato del volumen, desplegar el menú y elegir el sistema de archivo MS-DOS.

9. Ingresar el nombre del volumen o etiqueta: MEMDUMP.

10. Seleccionar el botón de Opciones de seguridad y elegir, en la ventana de Opciones de borrado seguro, Todos los datos a cero.

11. Seleccionar Aceptar.

12. Seleccionar el botón de radio Borrar, al lado de Opciones de seguridad, aparecerá un cuadro de advertencia.

13. Cerrar la utilidad de disco.

14. Extraer el dispositivo de almacenamiento USB, seleccionar el dispositivo y mantener apretada la tecla Control y luego Expulsar.

15. Descargar la imagen ISO de BackTrack, http://www.backtrack-linux.org/downloads/.

16. En la estación de trabajo de Informática forense Apple Macintosh, en la barra de menú, seleccionar Ir (Go), Utilidades y abrir la utilidad Disk Utility.app.

17. En el menú Archivo (File), seleccionar Abrir imagen de disco y seleccionar la imagen BT5-Gnome.iso del escritorio.

18. Seleccionar la imagen BT5-Gnome.iso del panel de Disco y Volumen y presionar Grabar.

19. Crear una partición Venix 80286. Este tipo de partición es la que busca msramdmp para efectuar la descarga de la memoria RAM. Colocar el CD en vivo de BackTrack en la lectora.

20. Reiniciar la computadora Mac, manteniendo presionada la tecla Opción.

21. Aceptar la opción predeterminada de inicio del menú de BackTrack.

22. Abrir una terminal e ingresar el comando:

$fidisk -l

23. Visualizar el resultado: Las particiones de MAC EFI (Estándar de Interfaz de Firmware Extensible Extensible Firmware Interface) y GPT[1][3][4] (Identificador Globalmente Único Globally Unique Identifier Partition Table) de tablas de particiones son reconocidas por la distribución BackTrack como /dev/sda1, dependiendo de los dispositivos instalados en la computadora, pueden aparecer también: sdb, sdc.

24. Insertar el dispositivo de almacenamiento USB o FireWire.

Ejecutar el comando $fidisk –l

25. Visualizar el resultado: El dispositivo USB aparece como /dev/sdb1, con la partición FAT32.

26. Ingresar el comando $fdisk /dev/sdb y los siguientes comandos en el orden que aparecen: m: Imprime este menú

d: Elimina una partición

n: Agrega una nueva partición

p: Imprime la tabla de particiones

1: (para nombrar la partición como 1)

Aceptar el valor predeterminado para el primer cilindro. Aceptar el valor predeterminado para el último cilindro.

t: Cambia el identificador de sistema de una partición l: Lista los tipos de particiones

40: Para cambiar el tipo de partición a 40, Venix 80286 p: Imprime la tabla de particiones

w: Escribe la tabla de particiones en el disco y sale del comando

27. $shutdown –r (reiniciar la computadora en el sistema operativo OS X).

28. Efectuar la descarga de la memoria RAM con msramdmp:

a. Apagar la computadora Macintosh dubitada inmediatamente.

b. Volver a encenderla, manteniendo presionada la tecla Opción, mientras coloca el CD de BackTrack en la lectora y luego el dispositivo de almacenamiento USB con la partición Venix 80286.

c. Si los pasos fueron correctamente realizados, aparecerá la pantalla del programa msramdmp de Wesly McGrew:

29. En el laboratorio, crear una imagen de la memoria descargada al dispositivo USB para su posterior análisis. En la estación de trabajo de Informática forense Macintosh, abrir una terminal desde el menú Ir, Utilidades, Terminal.

30. $sudo su (colocar la clave de root).

31. #ls /dev/disk?, lista los discos actuales en la Mac.
32. Insertar el dispositivo USB que contiene la descarga de la memoria RAM.
33. #ls /dev/disk?, debe aparecer listado el disco del dispositivo USB.
34. Generar la imagen de la memoria RAM con el comando dd:

#dd if= /dev/disk2 of= memdump.dd

35. Verificar si la imagen se corresponde con un inicio anterior de la computadora, buscando cadenas de caracteres que no forman parte de msramdmp, con el comando strings:

#strings memdump.dd

36. Visualizar la imagen de memdump.dd con un visor en hexadecimal: el perito podrá encontrar información de usuarios, claves, etc.

#hexedit memdump.dd

37. Registrar y documentar los resultados.

síntesis – Lista de control – Descarga de la memoria volátil

- Si la computadora está desbloqueada y FileVault en uso, copiar el directorio de inicio o trabajo del usuario.
- Si se obtiene la clave maestra, se pueden recuperar todas las carpetas de inicio.
- Si el acceso a la Mac está bloqueado, utilizar el programa msramdmp:
  - Requiere partición del tipo Venix 80286.
  - La utilidad de disco se emplea para grabar la imagen de msramdmp_cd.iso.
  - Crear una imagen de la memoria descargada con el comando dd.
  - Visualizar el contenido con un editor en hexadecimal.

Procedimiento para la recolección de datos en el modo de usuario único (single User Mode)

Consideraciones previas

Los equipos de Macintosh como computadoras de escritorio, laptop y servidores que posean el sistema operativo OS X pueden ser iniciados en el modo de usuario único. En este estado, es posible recolectar información; requiere conocimientos de Unix. Al iniciar en este modo, el sistema queda en un estado de solo lectura y tiene un limitado número de servicios en ejecución.

Fue diseñado por los administradores de sistema para desempeñarse en modo mantenimiento en un sistema Unix. Los beneficios de este modo de inicio incluyen el sistema operativo instalado, características establecidas por

Apple e incremento de la velocidad para acceder a ciertos datos. El acceso es por línea de comando únicamente. El usuario se transforma en root. Si la computadora viene configurada con la clave de protección de firmware, el acceso al modo de usuario único no se podrá ejecutar.

Existe una característica de Apple que permite deshacerse de la clave, pero esta acción también cambiará o reiniciará el reloj. Si el usuario de la Macintosh dubitada es del tipo avanzado, es probable que haya deshabilitado el modo de usuario único. En este caso, se debe registrar esta situación y apagar el equipo.

1. Presionar el botón de encendido e inmediatamente mantener presionada la tecla Opción (teclado Macintosh) o tecla Alt (teclado computadora personal).
2. Pueden presentarse dos escenarios:
   a. Cuadro de diálogo de contraseña de firmware, en este caso conviene mantener presionado el botón de apagado y terminar el proceso.
   b. Aparecen en pantalla las particiones de inicio. Esto confirma que no existe contraseña de protección de firmware.
3. Apagar el equipo manteniendo apretado el botón de apagado durante 4 segundos.
4. Presionar el botón de encendido e inmediatamente mantener apretada la tecla Comando (Command) en Apple y la tecla “S”. Esta acción permite ingresar en el modo de usuario único.

Aparece un texto y el indicador de la línea de comando y el sistema está montado en modo solo lectura. El perito deberá tener suficientes conocimientos para ejecutar los comandos en este modo, ya que al tener permisos de usuario root puede ejecutar comandos sin restricciones, y si no trabaja en forma prudente puede dañar el sistema y en consecuencia la información contenida en él.

El perito deberá leer con atención los comandos que aparecen en pantalla, por ejemplo, no deberá ejecutar los siguientes comandos:

/sbin/fsck verifica el sistema de archivos.

/sbin/mount –uw monta el sistema de archivo en modo escritura.

5. El perito podrá ejecutar los siguientes comandos, para examinar el sistema, que no modifican ni alteran la información existente y, por lo tanto, no destruyen los datos y se ejecutan en un entorno seguro:
   a. man: Para obtener ayuda de los comandos.
   b. date: Devuelve fecha, hora y zona horaria.
   c. date –U: Devuelve la fecha y hora en el modo UTC.
   d. hdiutil partition /dev/disk0: Devuelve la tabla de partición del dispositivo

de inicio o arranque.

e. hdiutil pmap2 /dev/disk0: Muestra información adicional de la tabla de partición del dispositivo de arranque.

f. ls /dev/disk?: Lista los discos actualmente en uso.

g. ls /dev/disk??: Utilizar esta opción si existen discos adicionales instalados en el sistema.

El perfil del sistema de Apple también está disponible y se puede recolectar la información a través de los siguientes comandos (si la devolución de la información toma demasiado tiempo, se puede presionar Ctrl + C, para interrumpir el proceso; algunos dispositivos no pueden ser consultados en forma apropiada en este modo):

a. system_profiler SPHardwareDataType: Muestra información del hardware de Macintosh.

b. system_profiler SPSoftwareDataType: Muestra información del sistema operativo.

c. system_profiler SPParallelATADataType: Muestra información de los dispositivos ATA.

d. system_profiler SPHardwareRAIDDataType: Muestra información sobre el hardware de RAID.

e. system_profiler SPMemoryDataType: Devuelve información sobre la memoria instalada.

f. system_profiler ParallelSCSIDataType: Devuelve información sobre los dispositivos SCSI.

g. system_profiler SPSASDataType: Devuelve información sobre los dispositivos SAS.

h. system_profiler SPSerialATADataType: Devuelve información de los dispositivos SATA.

6. Registrar, documentar y/o capturar pantallas con la información requerida.

Etapa de análisis de datos

Procedimiento para el análisis de la información del inicio del sistema operativo y los servicios asociados

Consideraciones previas

Al encender la computadora, el cargador del sistema operativo inicia el núcleo o kernel en

/mach_kernel, que luego ejecuta el proceso launchd (reemplaza a init de Linux). El proceso launchd lee y procesa listas de propiedades (plist) para ejecutar las aplicaciones requeridas de cuatro directorios:

- /System/Library/LaunchDaemons y /Library/LaunchDaemons, tareas que se ejecutan en segundo plano (servicios).
- /System/Library/LaunchAgents y /Library/LaunchAgents, tareas interactivas del usuario.

1. Analizar los archivos de propiedades contenidos en los directorios que se encuentran en formato XML y no requieren conversión para su análisis.

a. Editar los archivos plist con un editor de XML de los directorios:

i. /System/Library/LaunchDaemons

ii. /Library/LaunchDaemons

iii. /System/Library/LaunchAgents

iv. /Library/LaunchAgents

2. Analizar las extensiones agregadas al kernel. Son paquetes, o bundle, incorporados por Apple y también por aplicaciones de terceros para dispositivos de hardware o programas que requieren un bajo nivel de acceso (por ejemplo: cifrado de disco).

a. Acceder al directorio /System/Library/Extensions

3. Registrar, documentar y/o capturar pantallas con la información requerida.

Procedimiento para el análisis del sistema de archivos HFs+ de la imagen recolectada

1. Verificar en el archivo de la imagen recolectada, imagen_Mac_dubitada.dmg, la estructura del sistema de archivo, con los comandos de código abierto de Sleuth Kit, con la herramienta HFSExplorer. Se utilizará como ejemplo la imagen de http://digitalcorpora.org/corp/nps/drives/nps-2009-hfsjtest1/image.gen0.dmg. El perito utilizará la imagen recolectada.

a. $ fsstat imagen_Mac_dubitada.dmg

Los resultados serán semejantes a los siguientes: FILE SYSTEM INFORMATION

----------File System Type: HFS+ File System Version: HFS+

Volume Name: image

Volume Identifier: 9bee54da586b82f5

Last Mounted By: Mac OS X, Journaled Volume Unmounted Properly

Mount Count: 7

Creation Date: Thu Jan 29 09:33:30 2009

Last Written Date: Thu Jan 29 14:33:36 2009

Last Backup Date: Wed Dec 31 21:00:00 1969

Last Checked Date: Thu Jan 29 14:33:30 2009 Journal Info Block: 2

METADATA INFORMATION

----------Range: 2 26 Bootable Folder ID: 0 Startup App ID: 0

Startup Open Folder ID: 0

Mac OS 8/9 Blessed System Folder ID: 0 Mac OS X Blessed System Folder ID: 0 Number of files: 6

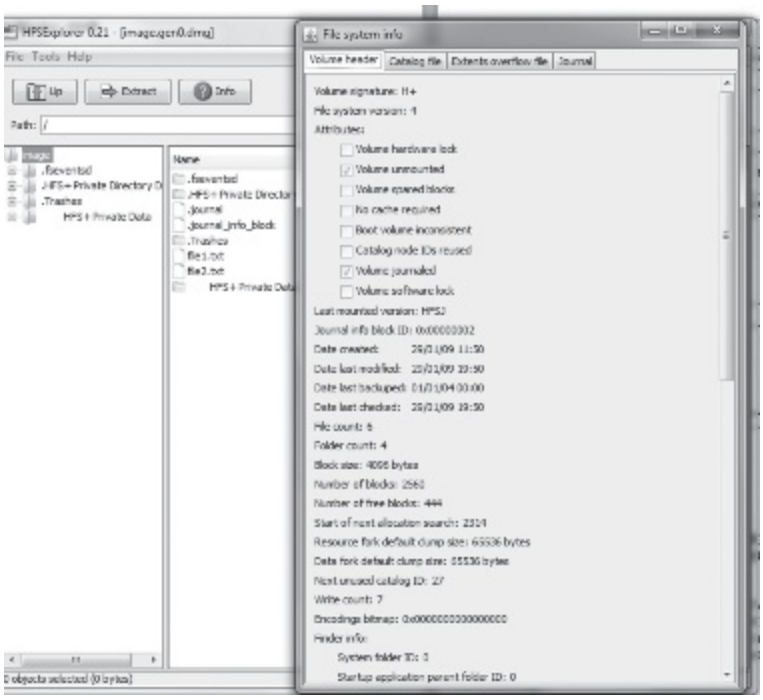
Number of folders: 4

CONTENT INFORMATION

----------Block Range: 0 2559 Allocation Block Size: 4096 Number of Free Blocks: 444

El perito puede observar que el tamaño de la asignación de bloques es de 4 Kb (4096), la fecha de creación del volumen, información del inicio (startup) del sistema operativo OS X, los cuales no son relevantes en un volumen que no es de inicio y aparece con un valor de cero (0): en los ítems de startup y en las carpetas del sistema Blessed, que apuntan a elementos en la carpeta /System/Library/CoreServices en un volumen de inicio o boot del sistema operativo OS X.

b. Visualizar el sistema de archivos HFS con la herramienta HFSExplorer:



c. $fls imagen_Mac_dubitada.dmg r/r 3: $ExtentsFile
r/r 4: $CatalogFile
r/r 5: $BadBlockFile
r/r 6: $AllocationFile
r/r 7: $StartupFile
r/r 8: $AttributesFile
d/d 21: .fseventsd
d/d 19: .HFS+ Private Directory Data^ r/r 16: .journal
r/r 17: .journal_info_block
d/d 20: .Trashes
r/r 24: file1.txt
r/r 25: file2.txt
d/d 18: ^^^^HFS+ Private Data

Los archivos con símbolo $ son archivos especiales de HFS+ utilizados como la columna vertebral del sistema de archivo.

3. Visualizar los metadatos de un archivo de la imagen en forma detallada con el comando de Sleuth Kit istat:

a. $istat imagen_Mac_dubitada.dmg 24 Catalog Record: 24
Allocated
Type: File Mode: rrw-r--r-Size: 23
uid / gid: 501 / 501

Link count: 1
Admin flags: 0
Owner flags: 0
File type: 0000
File creator: 0000
Text encoding: 0 Resource fork size: 0
Times:
Created: Thu Jan 29 14:33:35 2009
Content Modified: Thu Jan 29 14:33:35 2009
Attributes Modified: Thu Jan 29 14:33:35 2009
Accessed: Thu Jan 29 14:33:35 2009
Backed Up: Wed Dec 31 21:00:00 1969
Data Fork Blocks: 2312

El perito puede observar que el registro del catálogo posee cinco marcas de tiempo; no obstante, solo la primera está en uso en la implementación de HFS+.

- Created: Se actualiza cuando el archivo es creado.
- Content Modified: Se actualiza cuando se modifica el contenido del archivo.
- Attributes Modified: Se actualiza cuando los atributos o metadatos se modifican.
- Accessed: Se actualiza cuando el archivo es accedido.
- Backed Up: Este campo es obsoleto y generalmente tiene un valor null.

4. Extraer el contenido del archivo utilizando icat de Sleuth Kit:

a. $ icat imagen_Mac_dubitada.dmg 24 This is file 1 snarf

b. Se puede obtener el bloque asignado (2312) en forma directa con el comando de Sleuth Kit blkcat:

$ blkcat imagen_Mac_dubitada.dmg 2312 This is file 1 snarf

La herramienta no permite procesar los elementos de Journal del sistema de archivo.

5. Analizar el encabezado del sistema de archivo HFS+ de la imagen recolectada, imagen_ Mac_dubitada.dmg, con un editor en hexadecimal o con la herramienta HFSDebug de Amit Singh (http://osxbook.com/software/hfsdebug/), se puede descargar del sitio y ejecutar desde la línea de comando de la computadora de Informática forense Macintosh. Esta herramienta analiza el sistema de archivo HFS+ y obtiene un importante volumen de información útil para el perito, en particular para correlacionar las fechas incorporadas en la cadena de custodia. El manual con

las opciones de la línea de comando está disponible en el sitio: http://www.osxbook.com/software/hfsdebug/man.html.

a. Abrir una terminal y ejecutar:

$ hfsdebug –d /dev/rdisk0s2 -v

El resultado muestra gran cantidad de información del volumen HFS+, por ejemplo:

- Tamaño.
- Encabezado:
  - Firma = 0x48b (H+)
  - Versión = 0x4
  - Versión del último montaje = 0x484653a (HPSJ)
  – Atributos = 00000000000000000010000000000000
. el volumen tiene un journal
  - Información del bloque de journal = 0x801
  - Fecha de creación
  - Fecha de modificación
  - Fecha de resguardo

La lista continúa con gran cantidad de datos sobre el volumen.

b. La herramienta comercial fileXray (http://filexray.com/) es más avanzada que HFSDebug y requiere un sistema operativo Mac OS X 10.5 o superior.

6. Registrar, documentar y/o capturar pantallas con la información requerida.

Procedimiento para el análisis de directorios especiales (bundle) en el sistema de archivos HFs+ de la imagen recolectada

Consideraciones previas

En el sistema operativo OS X las aplicaciones con las que interactúa el usuario no son archivos monolíticos, son directorios especiales (bundle) que permiten a los recursos relacionados como un programa ejecutable y sus interfaces gráficas agruparse todos juntos, apareciendo ante el usuario como un solo archivo. Estos directorios ocultan sus contenidos ante la vista del usuario final a través del sistema operativo. Para ejecutar la aplicación, solo es necesario abrir el paquete o realizar un doble click con el mouse sobre el directorio. La extensión de este tipo de archivos es “.app”.

1. Analizar los grupos de archivos con extensión “.app” de la imagen recolectada, imagen_Mac_dubitada.dmg:

a. Desde la interfaz gráfica, ubicarse en las aplicaciones del tipo ".app" y con el botón del menú contextual del mouse (derecho) seleccionar Mostrar contenidos del paquete (Show Package Contents). Ejemplo de aplicaciones ".app": Libreta de direcciones, Calendario, Mail, Safari, iChat.

b. Utilizar la herramienta Sleuth Kit para mostrar el contenido del paquete, que será tratado como un directorio estándar. La identificación se realizará por medio de la extensión ".app" en el nombre del directorio y por los siguientes subdirectorios que contienen además del código ejecutable, íconos, archivos de texto, etc.:

- Contents
- Contents/Info.plist
- Contents/MacOS, contiene el código ejecutable
- Contents/Pkginfo
- Contents/Resources
- Contents/Version

c. Registrar, documentar y/o capturar pantallas con la información requerida.

Procedimiento para el análisis de archivos de configuración de red

Consideraciones previas

La información de la configuración de red se encuentra en varios archivos de propiedad en la carpeta /Library/Preferences/SystemConfiguration.

1. Analizar el contenido del archivo de lista de propiedad de preferencias (preferences.plist) de configuración de red de la imagen recolectada, imagen_Mac_dubitada.dmg, con el editor de lista de propiedad. Registrar:

a. Interfaces de red.

b. Ubicación de la configuración del perfil de red si está en uso.

c. Nombre de la computadora.

2. Analizar el contenido del archivo de lista de propiedad de identificación de la red (com. apple.network.identification.plist) de la imagen recolectada, imagen_Mac_dubitada. dmg, con el editor de lista de propiedad. Registrar:

a. La información histórica de la red.

b. La lista de asignaciones anteriores de red con fecha y hora. Esta información es de gran interés para el perito, en particular para una notebook móvil (dirección IP del router, servicios, direcciones IP, nombre de la interfaz, fecha y hora).

3. Analizar el contenido del archivo de lista de propiedad de dispositivos

Bluetooth que se han emparejado con la computadora (com.apple.Bluetooth.plist) de la imagen recolectada, imagen_Mac_dubitada.dmg, con el editor de lista de propiedad. Registrar:

a. Los nombres de los dispositivos emparejados.

b. Servicios.

c. Últimos nombres actualizados.

d. Fecha y hora.

4. Registrar, documentar y/o capturar pantallas con la información requerida.

Procedimiento para el análisis de archivos ocultos

Consideraciones previas

Por herencia del sistema de archivos del sistema operativo Unix, los archivos precedidos por un punto "." están ocultos en forma predeterminada para el usuario.

1. Analizar los archivos ocultos de la imagen recolectada, imagen_Mac_dubitada.dmg:

a. Ubicar el directorio oculto de la papelera (.Trash). A partir de la versión de Mac OS X 10.6, se guarda la ruta original del archivo borrado en un archivo oculto .DS_Store dentro de la carpeta Trash.

b. Visualizar el archivo .DS_Store con un visor en hexadecimal, por ejemplo, el nativo 0xED del sistema operativo OS X, para determinar la ruta original del archivo o con la herramienta hachoir-urwid 1.1 (http://pypi.python.org/pypi/hachoir-urwid/1.1).

2. Registrar, documentar y/o capturar pantallas con la información requerida.

Procedimiento para el análisis de aplicaciones instaladas

Consideraciones previas

En el directorio /Library/Receipts se encuentra la información de las aplicaciones instaladas a través del instalador del sistema operativo OS X. Contiene archivos del tipo ".pkg" de paquetes (bundles).

1. Analizar los archivos "pkg" de la imagen recolectada, imagen_Mac_dubitada.dmg:

a. Ubicar el directorio /Library/Receipts; verificar:

i. Nombres de los paquetes instalados.

ii. Fecha y hora de creación (debe coincidir con la fecha en que fue instalado

el programa).

3. Registrar, documentar y/o capturar pantallas con la información requerida.

Procedimiento para el análisis de espacio de intercambio (swap) y de hibernación

Consideraciones previas

Los datos de intercambio y de hibernación se almacenan en el directorio /private/var/vm. Contiene, aproximadamente, dependiendo de los recursos del sistema, de 1 a 10 elementos de intercambio, los cuales contienen las páginas intercambiadas de la memoria y pueden persistir en el disco por un tiempo. Si está habilitada la opción de hibernación, se podrá encontrar una imagen del estado: durmiendo de la computadora (sleepimage). Este archivo tiene el tamaño de la memoria RAM y contiene una copia de la memoria previamente a que se colocara la computadora en estado de hibernación o durmiendo.

1. Analizar los archivos /private/var/vm, si existen, de la imagen recolectada, imagen_ Mac_dubitada.dmg:
   a. Utilizar la herramienta de análisis de fragmentos (carving)[135] o el comando strings.
2. Registrar, documentar y/o capturar pantallas con la información requerida.

Procedimiento para el análisis de sucesos o registros (logs) del sistema

Consideraciones previas

Los sucesos del sistema se encuentran en el directorio /private/var/log. El sistema operativo OS X tiene un servicio o demonio denominado Syslog que envía información a dicho directorio.

1. Analizar los registros del sistema en el directorio /private/var/log de la imagen recolectada, imagen_Mac_dubitada.dmg; para el perito los más importantes son:
   a. Fsck_hfs.log, de los volúmenes HFS/HFS+/HFSX conectados al sistema.
   b. System.log, del sistema.
   c. Secure.log, autenticación, desbloqueo de protector de pantalla y accesos SSH.
2. Analizar los registros del directorio /Library/Logs generados por el programa que abarca a todo el sistema (system-wide):

a. Actualizaciones de software (Software Update.log), efectúa el seguimiento de las actualizaciones de software.

b. Informe de fallas (CrashReporter).

Registros de errores del kernel, de los programas, y la fecha y hora de ocurrencia.

c. Informe de suspensión del sistema (HangReporter).

d. Informe de pánico del sistema (PanicReporter).

3. Registrar, documentar y/o capturar pantallas con la información requerida.

Procedimiento para el análisis de información de las cuentas de usuarios

Consideraciones previas

La migración del sistema operativo OS X de las cuentas de usuario se encontraban en la base de datos de NetInfo. Al aparecer el servicio de directorio, la información de cada nombre de usuario o grupo en el sistema tiene un archivo de lista de propiedad (plist) en el directorio

/private/var/dv/dslocal/nodes/Default/Users/nombre_de_usuario y para el grupo /private/ var/db/dslocal/nodes/Default/groups/nombre_de_grupo.

El contenido del archivo de lista de propiedad es el siguiente:

- Identificador Único de Usuario: UUID (Universally Unique Identifier).
- Identificador de grupo: GID (group ID).
- La ruta del directorio de inicio (Home) del usuario.
- El nombre abreviado y completo del usuario.
- La ruta de la imagen elegida por el usuario.

La lista de propiedad admin.plist contiene el listado de los usuarios con privilegio de administrador o root; el archivo se encuentra en:

- /private/var/db/dslocal/nodes/Default/groups/admin.plist

1. Analizar los archivos de lista de propiedad de los usuarios y grupos en los directorios:

/private/var/dv/dslocal/nodes/Default/Users/nombre_de_usuario

/private/var/db/dslocal/nodes/Default/groups/nombre_de_grupo de la imagen recolectada, imagen_Mac_dubitada.dmg. Editar el archivo con el editor de lista de propiedad.

2. Analizar los usuarios con privilegios de administrador en el archivo de lista de propiedad en: /private/var/db/dslocal/nodes/Default/groups/admin.plist

3. Analizar los permisos asignados al resto de los usuarios con el formato POSIX y con las listas de control de acceso (ACL).

4. Analizar el archivo de lista de propiedad, ubicado en /Library/Preferences/com.apple. loginwindow.plist, para determinar cuál fue el último usuario en iniciar sesión en el sistema. El perito puede utilizar esta información en el caso de un sistema compartido.

5. Registrar, documentar y/o capturar pantallas con la información requerida.

Procedimiento para el análisis del directorio de inicio (Home)

Consideraciones previas

El directorio de inicio o Home del usuario se representa en la línea de comando con: ~/ y el directorio raíz o root con: /. En el directorio de inicio, el usuario tiene todos los elementos o Artifacts generados por el usuario. Otras actividades como inicio y cierre de sesión generan elementos en áreas del sistema. El directorio de inicio estándar de un usuario contiene los siguientes directorios:

- Escritorio (Desktop)
- Aplicaciones
- Documentos
- Descargas
- Biblioteca (Library), contiene un gran número de elementos directos e indirectos relacionados con la actividad del usuario. Archivos de registros, configuraciones de preferencia (Preferences), elementos de aplicaciones, elementos generados al conectarse con otros dispositivos o sistemas. Es un área con gran cantidad de información para el perito.
- Películas
- Música
- Imágenes
- Público
- Sitios

1. Analizar el contenido de los subdirectorios de ~/Biblioteca (Library) de la imagen recolectada, imagen_Mac_dubitada.dmg:

a. En el directorio /Preferences, editar los archivos plist con el editor de lista de propiedad:

i. Archivos abiertos o conexiones de redes abiertas.

ii. Cambios de configuración que el usuario haya personalizado.

iii. com.apple.quicktimeplayer.plist, contiene una lista de archivos de videos abiertos con QuickTime (semejantes a los plist para MPlayer y VLC), con la

ruta completa, ejemplo:

<dict>
<key>altname</key> , ruta relativa
<string>IMG_123.MOV...</string>
<key>dataRef</key>, ruta absoluta
<data> AAAAAAAAAAAdh///567AAAeKDF935CJ1AAA
</data>
<key>dataRefType</key>
<string> </string>
<key>name</key>, nombre del archivo
<string>IMG_123.MOV</string>
</dict>

La ruta absoluta en dataRef está codificada en base 64, se puede codificar de varias formas, por ejemplo, con openssl, presente en cualquier sistema operativo compatible con Unix.

Para decodificar, copiar los datos a partir de <data> hasta </data> y guardarlo en un archivo (IMG_123-base64.data) y ejecutar el comando:

$openssl enc –d base64 –in IMG_123-base64.data –out enclaro.bin

Extraer la ruta absoluta con el comando strings o con un editor en hexadecimal:

$strings enclaro.bin

iv. com.apple.recentitems.plist, contiene el número (<key>MaxAmount</key>) de archivos abiertos (<key>Name</key>) y los servidores de archivos (<key>URL</ key>) accedidos recientemente.

Estas entradas no tienen fecha y hora, por lo tanto, el perito deberá correlacionar estos datos con otras fuentes de información como los metadatos del sistema de archivo.

v. com.apple.DiskUtility.plist, contiene la etiqueta (<key>DUSavedDiskImageList

</key>), que se utiliza para completar la barra lateral de la aplicación Utilidad de Disco (Disk Utility). Los elementos listados muestran la ruta completa de las imágenes de disco (<string>imagen_Mac_dubitada.dmg</string>) que han sido abiertas en el sistema. Además, puede contener archivos que han sido borrados del sistema.

vi. com.apple.finder.plist, es el archivo principal de preferencias para la aplicación del explorador gráfico de archivos del sistema operativo OS X Finder. Contiene el número de entradas, pero para el perito las más importantes son:

(<key>FXConnectToLastUrl</key>), que muestra la URL completa del último servidor al cual se conectó el sistema operativo con la aplicación Finder.

(<key>FXDesktopVolumePositions</key>), indica el punto de montaje y nombre de los volúmenes montados con anterioridad en el sistema operativo (<key>Volumes/16GB</key>).

(<key>FXRecentFolders</key>), muestra los directorios visualizados recientemente por el usuario.

vii. com.apple.iPod.plist, en el caso de que el usuario se conecte a dispositivos iPod, iPhone o iPad, esta es una lista de propiedad a examinar por el perito que contiene información de identificación.

b. El directorio /Application Support contiene la información de soporte para las aplicaciones instaladas en el sistema operativo, generalmente se utiliza para los datos que son modificados con frecuencia o para los que se almacenan por un largo período de tiempo, como por ejemplo las aplicaciones de Libreta de direcciones, información de sincronización de iPod, datos del perfil del navegador Firefox, etc. Al eliminar o desinstalar aplicaciones del sistema, no elimina la información de soporte de la aplicación, por lo tanto, para el perito es un directorio que contiene información relevante para analizar.

i. Analizar la información de sincronización de dispositivos: iPod, iPhone o iPad en el directorio /Library/Application Support/MobileSync/Backup y en sus respectivos subdirectorios que aparecen con una cadena de 40 dígitos alfanuméricos en hexadecimal que contienen los identificadores únicos de los dispositivos (UDID). En el caso de que se hayan sincronizado varios dispositivos, aparecerán múltiples directorios con el identificador UDID o si se han realizado múltiples resguardos. En el resguardo más reciente aparece solo el UDID, si son anteriores se agregará la fecha y hora al UDID del directorio. Al realizar el resguardo, se generan tres archivos de lista de propiedad: Info.plist, Status.plist y Manifest.plist.

ii. Analizar el archivo Info.plist; para el perito es el más importante para obtener información del dispositivo resguardado, abrir el archivo con un editor de lista de propiedad o en Mac con la barra espaciadora, y registrar:

· Versión, nombre del dispositivo, IMEI, último resguardo, número de teléfono de iPhone, tipo de producto, número de serie, configuración de sincronización, etc.

c. El directorio de registros de eventos o sucesos (Logs) Library/Logs muestra información de los eventos de las aplicaciones con la extensión “.log”. Los registros de eventos de la aplicación de Utilidad de Disco (Disk Utility) son una fuente de información para el perito para determinar si se efectuaron tareas de grabación de discos ópticos o cualquier otra actividad que se haya

realizado con la aplicación Utilidad de Disco.

i. Visualizar y registrar el contenido del archivo de registro de eventos de la aplicación de Utilidad de Disco (Disk Utility).

ii. Efectuar la correlación de datos con las fechas y horas de modificación y acceso.

d. Cachés: La información de las aplicaciones permanece en este directorio por un tiempo prolongado, aun en el caso en que la aplicación se haya eliminado o desinstalado (ver el procedimiento de análisis de cachés más adelante).

e. Historial de comandos (Shell History): El sistema operativo OS X utiliza el intérprete de comandos Bourne Again Shell (BASH), por lo tanto el perito puede analizar el historial de los comandos ingresados por el usuario al utilizar una terminal. El archivo

.bash_history se encuentra en el directorio de inicio del usuario. Este archivo no contiene información de fecha y hora de ingreso de los comandos, pero el perito podrá correlacionar estos datos con otras actividades realizadas por el usuario. La mayoría de los usuarios no utilizan la terminal o consola, pero si se encuentra información de su uso es probable que el usuario sea un usuario avanzado y con conocimientos del sistema operativo o que haya utilizado la consola para efectuar una tarea particular que puede ser analizada por el perito acorde al requerimiento pericial.

i. Editar el archivo .bash_history con un editor de texto y registrar los comandos ingresados.

2. Registrar, documentar y/o capturar pantallas con la información requerida.

Procedimiento para desencriptar la carpeta de inicio del usuario cifrada por el servicio Filevault

Consideraciones previas

Existen dos técnicas que el perito puede utilizar para acceder a la información cifrada de la carpeta de inicio: a través de la fuerza bruta o fuerza bruta con ataque de diccionario. Esto dependerá de si se encuentra una imagen de los espacios asignados que contienen datos (sparseimage) o una imagen generada por el método de crecimiento dinámico de la imagen a través del tiempo (sparsebundle).

En la imagen adquirida en el proceso de duplicación se puede encontrar la carpeta de inicio del usuario cifrada y aparecerá un archivo como nombre_del_usuario.sparseimage, o una carpeta como nombre_del_usuario.sparsebundle. Los datos en ambos archivos no son de

utilidad porque están cifrados. La herramienta de libre disponibilidad MacKrack efectúa ataques de fuerza bruta (http://mac.majorgeeks.com/files/details/mackrack.html) para los casos de sparseimage. La herramienta comercial de Passware Kit Forensics 11.7 (http://www.lostpassword.com/kit-forensic.htm) en su sitio publica la característica de desencriptar FileVault2. La utilidad Spartan de libre disponibilidad (http://www.appleexaminer.com/Utils/Downloads.html) se puede utilizar para imágenes del tipo sparsebundle, que utiliza ataque de diccionario y es un procedimiento muy lento. La herramienta crowbarDMG (https://www.georgestarcher.com/) es más rápida y utiliza ataque de diccionario para imágenes DMG, sparseimage y sparsebundle. El perito deberá comprobar en el laboratorio la eficiencia de estas herramientas, sumadas a las siguientes de:

Libre distribución:

- John the Ripper (http://www.openwall.com/john/).
- HashCat (http://www.hashcat.net/) para CPU y GPU.
- crowbarKC (https://www.georgestarcher.com/?page_id=256) ataque de diccionario.
- Mike's Forensic Tools, http://www.mikesforensictools.co.uk/, sitio de Mike Harrison (herramientas: MFT Mac Salt: ataque de diccionario, MFT Mac Files From Where: consulta a bases de datos).

Comercial:

- MacLockPick 3.0 extrae cadena de claves y las desencripta (http://www.macforensicslab.com).

El mejor método que puede utilizar el perito es a través de la apertura de la carpeta de inicio del usuario cifrada con FileVault a través del mismo sistema operativo Mac OS X; para efectuar esta acción necesitará la clave maestra.

1. Con la clave maestra, cambiar la contraseña de la cuenta del usuario y la de FileVault en un solo paso:
   a. Seleccionar Ir, Preferencias del sistema, Cuentas, Restablecer contraseña.
   b. Ingresar la clave maestra.
   c. El perito puede asignar una nueva clave que será también la nueva clave de FileVault; si la clave del usuario es restablecida por cualquier otro medio, la clave de FileVault no se cambiará.
2. No iniciar la sesión y copiar la carpeta encriptada antes de iniciar sesión, de esta forma el perito siempre tendrá una copia de la carpeta descifrada pero sin modificar la carpeta de inicio del usuario al volver al sistema.
3. El perito puede encontrar en la computadora Mac las claves del usuario que posteriormente con las herramientas de descifrado por técnica de fuerza

bruta o ataque de diccionario intentará obtener el texto en claro; verificar:

a. El archivo de paginación (intercambio: swap o memoria virtual) ubicado en /var/ vm/swapfile0; si el usuario no habilitó la opción de Asegurar la Memoria Virtual, este archivo contiene el texto en claro de varias de las actividades realizadas en la computadora Mac, incluyendo las claves ingresadas a sitios en Internet.

b. El archivo de imagen de modo reposo (sleep) ubicado en /var/vm/sleepimage; si el usuario no habilitó la opción de Asegurar la Memoria Virtual, este archivo contiene claves de inicio de sesión del usuario, entre otras contraseñas.

c. Visualizar los archivos de manera legible. El perito deberá agregarlos a un diccionario de claves para descifrarlos y obtener la contraseña de acceso a FileVault.

4. Crear un diccionario con las claves obtenidas, abrir una terminal e ingresar el comando:

$sudo strings /var/vm/swapfile0 > ~Escritorio/diccionario.txt En el escritorio aparecerá el archivo diccionario.txt.

5. Utilizar las herramientas mencionadas anteriormente para descifrar el archivo diccionario.txt.

6. Registrar, documentar y/o capturar pantallas con la información requerida.

Síntesis – Lista de control

- La caja fuerte de protección (FileVault) de la carpeta de inicio del usuario utiliza el algoritmo de encriptación AES de 128 bits.
- Se utilizan dos claves para cifrar la carpeta de inicio: Clave del usuario para ingresar y clave maestra para cambiar la contraseña.
- Los formatos de imágenes que genera el demonio o servicio FileVault son: sparseimage (Mac OS X 10.3) y sparsebundle (Mac OS X 10.5).
- Visualizar el ícono de la casa con la combinación para determinar si el servicio de FileVault se encuentra activo.
- Obtener la información de la carpeta de inicio cuando no está cifrada implica utilizar el procedimiento de copiar la carpeta a un dispositivo externo con formato de archivo HFS+.
- Efectuar la copia de la carpeta implica realizar una acción con el sistema encendido y por lo tanto en tiempo real, esto significa que ocurrirán cambios en el sistema con cada acción que efectúe el perito. Siendo esta la única forma de obtener la información en claro de la carpeta. El perito deberá consultar al juez autorización para realizar esta tarea.

· El proceso implica realizar una serie de tareas que el perito debe practicar previamente en el laboratorio.

· La carpeta de inicio cifrada se puede desencriptar utilizando diversas herramientas comerciales y de libre disponibilidad que emplean el método de fuerza bruta y/o de ataque de diccionario.

· El perito puede cambiar las contraseñas de la carpeta de inicio del usuario cifradas utilizando la clave maestra, garantizándole el acceso a los datos.

· El mejor diccionario disponible de datos para utilizar con las herramientas de desencriptado es el generado por la misma computadora Macintosh, de donde provienen los datos de la carpeta de inicio del usuario.

· Las herramientas más eficientes para descifrar FileVault son las producidas por Macintosh.

Procedimiento para la recuperación de datos del navegador web safari de la imagen adquirida

Consideraciones previas

Safari es el navegador web predeterminado en Mac. El perito deberá examinar los siguientes archivos y base de datos:

· Cache.db

· webpageIcons.db

· TopSites.plist

· Bookmarks.plist

· Downloads.plist

· History.plist

· LastSession.plist

· Cookies.plist

Si el usuario habilita la opción Navegación Privada (Private Browsing), los archivos History. plist, LastSession.plist, y TopSites.plist no se actualizarán. No se capturan pantallas ni vistas previas de los sitios web.

El perito puede buscar fragmentos de los archivos de navegación en los espacios no asignados del disco. En el caso de que la computadora se encuentre encendida, una descarga de la memoria RAM puede mostrar un listado de los sitios visitados.

El perito puede utilizar una conexión remota para visualizar la memoria o utilizar las herramientas de recolección en vivo. Otro método es efectuar consultas a la base de datos Cache.db en ~/Librería/Caches/com.apple.Safari. La información desaparecerá cuando el usuario cierre el navegador que se ejecutaba en modo de navegación privada. Si el navegador en este estado se

cierra inesperadamente, el perito podrá recuperar información en los registros de la aplicación.

Caché del navegador

La información obtenida del caché de web contiene los sitios visitados por el usuario con el navegador de Internet predeterminado Safari. Entre otros, los elementos a encontrar son cookies, etc. El perito deberá analizar los datos de los diferentes navegadores de Internet que se encuentren instalados en la computadora dubitada.

1. La ubicación del archivo de caché dependerá de la versión de Safari; verificar las siguientes carpetas:
   a. Safari v 3.2 and v4/5, ~/Librería/Caches/Metadata/Safari/History
   b. Safari v3.1.1, private/var/folders
   c. ~/Librería/Preferences/com.apple.Safari.plist
   d. ~/Librería/Caches
   e. Safari en el sistema operativo Leopard se guarda como base de datos en la carpeta / [nombre_de_usuario]/Librería/Caches/com.apple.Safari
   f. Cookies.plist
2. Abrir la imagen adquirida en la etapa de recolección (imagen_Mac_dubitada.dmg).
3. Analizar la base de datos cache.db ubicada en /Librería/Caches/com.apple.Safari con el navegador de base de datos SQLite. El perito observará:
   a. Los sitios web visitados por el usuario con su correspondiente fecha y hora.
   b. Una lista de imágenes.
   c. Javascripts.
4. Visualizar las imágenes de la base de datos con la herramienta de carácter comercial File Juicer (http://echoone.com) que analiza diferentes tipos de archivos, con una versión de prueba para descargar del sitio. El manual de la herramienta se encuentra en http://echoone.com/filejuicer/userguide.
5. Ejecutar la herramienta File Juicer:
   a. Seleccionar Archivo, Abrir.
   b. Ubicar la base de datos cache.db en la carpeta /[nombre_de_usuario]/Librería/Caches/com.apple.Safari y seleccionar Abrir. La herramienta File Juicer analizará la base de datos. Al finalizar aparecerá una ventana que mostrará los resultados hallados en el escritorio (Cache Juice).
   c. Analizar el contenido de las carpetas del archivo de salida Cache Juice:

i. Bmp, bitmap.

ii. Gif (Graphic Interchange Format).

iii. Html, páginas web visitadas.

iv. Ico, íconos que aparecen en la barra de navegación de Safari.

v. Index.html, página web completa, no es la página de inicio del usuario en el navegador.

vi. JPG.

vii. Plist, listas de propiedad enumeradas que muestran las URL que visitó el usuario. viii.PNG.

ix. Sqlite.txt, archivo de texto con todos los ítems analizados por la herramienta.

x. Swf, archivos flash de los sitios visitados.

xi. Txt, numerosos archivos del código HTML de las páginas web visitadas, lo mismo para código XML.

d. Efectuar el análisis de la fecha y hora (MAC: Modificado, Accedido y Creado) de los archivos obtenidos por la herramienta File Juicer acorde a la requisitoria pericial.

6. Registrar, documentar y/o capturar pantallas con la información requerida.

Íconos de la URL de los sitios (webpageIcons.db)

La base de datos almacena los íconos de los sitios web que aparecen en la URL en la barra de direcciones del navegador Safari.

1. En la imagen recolectada (imagen_Mac_dubitada.dmg), analizar los íconos de la barra de direcciones:

a. Ejecutar la aplicación File Juicer.

b. Seleccionar Archivo, Abrir.

c. Ubicar la carpeta /Librería/Safari/.

d. Seleccionar la base de datos webpageIcons.db.

e. Seleccionar Abrir.

f. Revisar el contenido de los íconos de la barra de direcciones:

i. Archivos ico, muestra el ícono de la página web.

ii. Index.html, no contiene evidencia.

iii. png, muestra íconos adicionales de la página web.

iv. sqlite.txt, un archivo de texto que contiene todos los valores del archivo .db.

2. Registrar, documentar y/o capturar pantallas con la información requerida.

Archivos plist

Estos archivos se encuentran generalmente en ~/Librería/Safari/:

Sitios más visitados (TopSites.plist)

Esta característica aparece con Safari 3.x, registrando los sitios más visitados por el usuario, quien puede marcar o eliminar algunos de esos sitios en la lista que le muestra el navegador. La lista no provee la fecha y hora de selección del sitio. Cuando el usuario borra la caché de datos, el programa le pregunta si también quiere limpiar o reiniciar la lista de los sitios más visitados (TopSites). En caso de que el usuario la reinicie, el archivo TopSites.plist contendrá los valores predeterminados.

Los sitios marcados como más visitados se guardan bajo el nombre "TopSiteIsPinned" y pueden estar ligados con alguna otra acción del usuario. Los sitios marcados en forma predeterminada por el programa se almacenan como "TopSiteIsBuiltin".

1. En la imagen recolectada, imagen_Mac_dubitada.dmg, analizar el listado de sitios más visitados.
2. Registrar, documentar y/o capturar pantallas con la información requerida.

Marcadores (Bookmarks.plist)

Estos archivos binarios contienen el seguimiento y mantenimiento de los marcadores que el usuario creó dentro del navegador. En la versión 3 de Safari, los usuarios poseen marcadores predeterminados. Si el usuario desea agrupar los marcadores en el archivo plist estarán agrupados bajo el nombre de la carpeta. A veces, el usuario se puede equivocar y en vez de guardar el sitio en marcadores lo coloca en la opción de sitios más visitados (Top Sites).

Cada entrada del marcador es idéntica con un identificador webBookmarkUUID, de 32 caracteres en hexadecimal. Si se utiliza este identificador como nombre y la extensión ".webbookmark", se puede encontrar el archivo correspondiente. El webbookmark contiene la URL visitada, pero no la fecha y hora en que se ingresó el sitio en los marcadores.

En el sistema operativo Leopard, este archivo se encuentra en la carpeta ~/Librería/Caches/ Metadata/Safari/Bookmarks.

1. Visualizar los marcadores en el archivo de la imagen adquirida en la etapa de recolección (imagen_Mac_dubitada.dmg), con la aplicación para exportar marcadores de Mac (Tracker´s Safari Bookmark Exporter).
   a. Descargar la aplicación de libre distribución del sitio http://homepage.mac.com/ simx/sbe.html.
   b. En la estación de Informática forense Mac, ir a la carpeta

/[nombre_de_usuario]/ Librería/Safari.

c. Ubicar y borrar el archivo Bookmarks.plist.

d. Abrir el archivo de la imagen recolectada (imagen_Mac_dubitada.dmg) y ubicarse en la carpeta /[nombre_de_usuario]/Librería/Safari.

e. Copiar el archivo Bookmarks.plist de la imagen y pegarlo en la misma carpeta en el sistema operativo de la computadora de Informática forense.

f. Iniciar la aplicación para exportar marcadores de Mac (Tracker´s Safari Bookmark Exporter). Verificar que se encuentre seleccionada la casilla de Abrir Marcadores de Safari desde la ubicación predeterminada.

g. Seleccionar Analizar Marcadores.

h. Luego del análisis, seleccionar la opción HTML Simple.

i. Oprimir el botón Exportar Marcadores.

j. Seleccionar el destino, por defecto Escritorio, y guardar el archivo con extensión ".html".

k. Abrir el archivo de exportación de marcadores con extensión ".html" y analizar el contenido.

2. Registrar, documentar y/o capturar pantallas con la información requerida.

Descargas de archivos (Downloads.plist)

Es un archivo en el formato XML; contiene el historial de todos los elementos descargados por el usuario.

1. En la imagen recolectada (imagen_Mac_dubitada.dmg), ubicar la carpeta /[nombre_ de_usuario]/Librería/Safari/Downloads.plist

2. Oprimir la tecla Ctrl y botón primario del mouse sobre el archivo Downloads.plist.

3. Seleccionar Abrir con y seleccionar del menú contextual Editor de Property List.

4. Visualizar el listado de las URL de descarga de los archivos listados y su actual ubicación.

5. Editar con el visor en hexadecimal el archivo del formulario valor (Value); este archivo se encuentra en ~/Librería/Safari/ y contiene información sobre autocompletar del navegador Safari, la cual se habilita en el Menú Preferencias. Este formulario es el lugar donde se almacenan los nombres de usuario, direcciones, números de teléfonos, utilizados por el usuario en la navegación por diferentes sitios.

6. Registrar, documentar y/o capturar pantallas con la información requerida.

Historial (History.plist)

Contiene el historial de los sitios visitados por el usuario. Las fechas y horas se encuentran en el formato de OS X Epoch. El perito deberá utilizar el convertidor de tiempo (CFAbsoluteTimeConverter). En la versión 4 de Safari, por cada entrada en el archivo History.plist existe un archivo del historial web ubicado en la carpeta ~/Librería/Caches/Metadata/Safari/History. El archivo del historial web se puede abrir con el editor de lista de propiedades y analizar la URL.

Una característica nueva en Safari es crear instantáneas o capturas de pantallas o previsualizaciones y guardarlas en ~/Librería/Caches/com.apple.Safari/webpage Previews. Estos archivos están en formato JPEG o PNG con el mismo nombre de archivo pero diferente extensión. Si el usuario borra el historial, también se borran las previsualizaciones, al menos que se encuentren marcados en la lista de marcadores.

1. En la imagen recolectada (imagen_Mac_dubitada.dmg), ubicar la carpeta /[nombre_ de_usuario]/Librería/Safari/History.plist.
2. Abrir el archivo con el editor de lista de propiedades (plist) y se visualizará el archivo en XML.
3. Analizar y extraer la información de:
   a. Los sitios visitados.
   b. La última fecha y hora de visita al sitio.
   c. Los títulos de los sitios visitados.
   d. El número de veces que el usuario visitó un determinado sitio.
4. La fecha y hora se encuentra en el formato OS X Epoch; convertir la fecha con la herramienta CFAbsoluteTimeConverter:
   a. Ubicar en la imagen la carpeta /Librería/Safari/History.plist.
   b. Abrir la carpeta con el editor de listas de propiedad.
   c. Expandir la lista para mostrar los elementos, manteniendo presionada la tecla Alt y seleccionando con el mouse el triángulo en la parte superior de la lista.
   d. Ubicar el elemento de interés de la lista, por ejemplo, el primero.
   e. Efectuar doble click en el campo Valor (Value) lastVisitedDate.
   f. Marcar la cadena de caracteres contenida en el campo Valor.
   g. Seleccionar Copiar en el menú contextual (botón secundario del mouse).
   h. Abrir el programa CFAbsoluteTimeConverter.
   i. En el campo Ingresar el CFAbsoluteTime, pegar el valor del primer elemento de la lista History.plist.
   j. Seleccionar Convertir.

5. Registrar, documentar y/o capturar pantallas con la información requerida.

Última sesión (LastSession.plist)

El archivo se utiliza para realizar un seguimiento de los sitios web activos en la ejecución actual del navegador Safari. Las entradas del archivo se generan por cada ventana que se abra del navegador. Si una ventana tiene múltiples pestañas, el archivo plist tendrá una lista de los sitios web correspondientes a cada pestaña.

El archivo contiene las URL de la última vez en que se ejecutó o abrió la aplicación Safari. Si el navegador se cierra en forma inesperada, la aplicación utilizará este archivo para restaurar la sesión anterior.

1. En la imagen recolectada (imagen_Mac_dubitada.dmg), ubicar la carpeta /[nombre_ de_usuario]/Librería/Safari/LastSession.plist y:

a. Abrir el archivo con el editor de lista de propiedades, o

b. Seleccionar el archivo plist, y oprimir la barra espaciadora para obtener una vista previa del archivo y de su contenido.

2. Registrar, documentar y/o capturar pantallas con la información requerida.

Cookies.plist

Es una porción de datos enviada por el sitio web y almacenada en el navegador web del usuario mientras explora un determinado sitio. Cuando el usuario vuelve a navegar en el mismo sitio posteriormente, los datos guardados en la porción de datos cookie pueden ser recuperados por el sitio web para informar al sitio sobre la actividad de un usuario realizada previamente (inicios de sesión, ejecución de botones, registros de páginas visitadas por el usuario en meses o años anteriores). El perito puede utilizar estos datos para realizar un seguimiento del historial de navegación de un usuario.

1. En la imagen recolectada (imagen_Mac_dubitada.dmg), ubicar la carpeta /[nombre_ de_usuario]/Librería/Cookies/Cookies.plist y:

a. Abrir el archivo con el editor de lista de propiedades, o

b. Seleccionar el archivo plist, y oprimir la barra espaciadora para obtener una vista previa del archivo y de su contenido.

c. Revisar las entradas del archivo Cookies.plist:

i. La fecha y hora de creación se encuentra en el formato OS X Epoch, convertir la fecha con la herramienta CFAbsoluteTimeConverter o con el convertidor en línea.

ii. Nombre de dominio del sitio visitado.

iii. Fecha de expiración del dato o cookie, no requiere conversión.

2. Registrar, documentar y/o capturar pantallas con la información requerida.

Síntesis – Lista de control

· Ejecutar el editor de lista de propiedades para visualizar el contenido de los archivos ".plist" del navegador Safari y obtener información de:

- Sitios de navegación marcados (Bookmarks.plist).
- Descarga de archivos (Downloads.plist).
- Historial de navegación: sitios visitados, fecha, hora y frecuencia (History.plist).
- Sitios más visitados (TopSites.plist).
- Último acceso al navegador Safari (LastSession.plist).
- Sitios visitados y almacenados en las porciones de datos o cookies, la fecha y hora (Cookies.plist).

· Ejecutar la aplicación comercial File Juicer (versión de prueba para descargar) para analizar las bases de datos:

- De los sitios visitados, fecha y hora (cache.db).
- De los íconos de las URL de la barra de direcciones del navegador.

Procedimiento para la función del navegador safari como visor de archivos en el sistema operativo de Microsoft Windows

Consideraciones previas

El navegador de Internet Safari tiene versiones de instalación para Macintosh y para el sistema operativo de Microsoft Windows. En la versión para Windows se pueden visualizar los archivos .plist de Mac; para el perito esta es una forma alternativa, ya que facilita la previsualización de los archivos. La otra manera, más lenta y complicada, sería analizar los archivos plist con un visor de XML. Si el perito encuentra información de interés en la previsualización, deberá entonces analizar el o los archivos .plist con el editor de propiedades correspondiente. Los archivos

.*p* list que se pueden visualizar son:

- TopSites.plist
- Bookmarks.plist
- Downloads.plist
- History.plist
- Cookies.plist

1. Descargar el navegador Safari para Windows (http://www.apple.com/safari/download/).
2. En la estación de Informática forense de Microsoft Windows, desconectada de Internet, instalar el navegador Safari.
3. En la estación de trabajo de Informática forense de Macintosh, en la imagen recolectada (imagen_Mac_dubitada.dmg), ubicar la carpeta /[nombre_de_usuario]/Librería/ Safari/ y copiar a un dispositivo seguro los siguientes archivos:
   a. TopSites.plist
   b. Bookmarks.plist
   c. Downloads.plist
   d. History.plist
   e. Cookies.plist
4. En la estación de Informática forense de Microsoft Windows, pegar los archivos plist de Mac en su correspondiente ubicación en Windows y sobrescribirlos. Verificar en la siguiente lista la ubicación según la versión del sistema operativo:

Ubicación de los archivos plist en el sistema operativo de Microsoft Windows[136]

Windows XP:

Archivo	Ubicación
History.plist	C:\Documents and Settings\<user name>\Application Data\Apple Computer\Safari\
Bookmarks.plist	C:\Documents and Settings\<user name>\Application Data\Apple Computer\Safari\
Downloads.plist	C:\Documents and Settings\<user name>\Application Data\Apple Computer\Safari\

Archivo	Ubicación
Topsites.plist	C:\Documents and Settings\<user name>\Application Data\Apple Computer\Safari\
Cookies.plist	C:\Documents and Settings\<user name>\Application Data\Apple Computer\Safari\Cookies\
Previsualización de páginas web	C:\Documents and Settings\<user name>\Local Settings\Application Data\Apple Computer\Safari\webpage Previews\

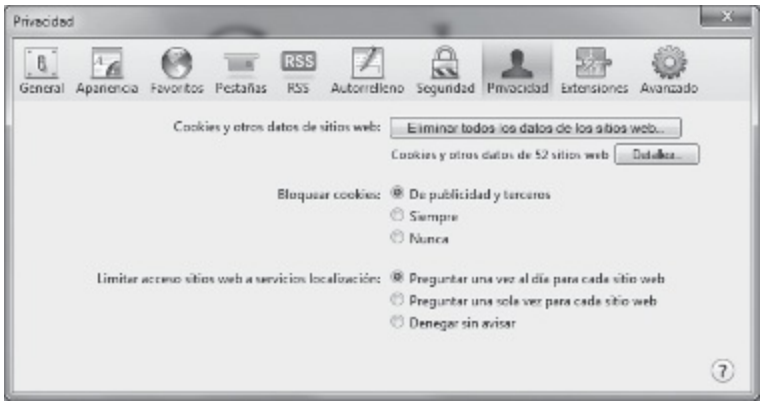
Windows 7:

Archivo	Ubicación
History.plist	C:\Users\<user name>\AppData\Roaming\Apple Computer\Safari\
Bookmarks.plist	C:\Users\<user name>\AppData\Roaming\Apple Computer\Safari\
Downloads.plist	C:\Users\<user name>\AppData\Roaming\Apple Computer\Safari\
Topsites.plist	C:\Users\<user name>\AppData\Roaming\Apple Computer\Safari\
Cookies.plist	C:\Users\<user name>\AppData\Roaming\Apple Computer\Safari\ Cookies\
Previsualización de páginas web	C:\Users\<user name>\AppData\Local\Apple Computer\Safari\ webpage Previews\

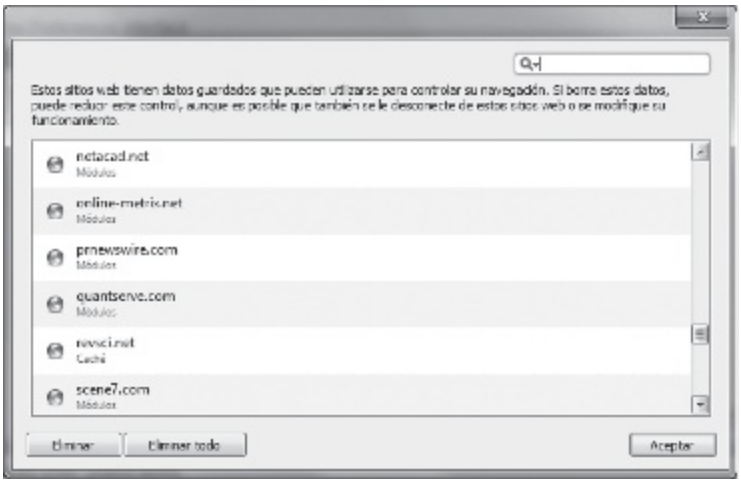
5. En el navegador Safari (5.1.7) en Microsoft Windows, visualizar cookies.plist:

a. Seleccionar en la barra de menú, el ícono de Mostrar un menú de ajustes generales de Safari.

b. Seleccionar Preferencias, Privacidad:



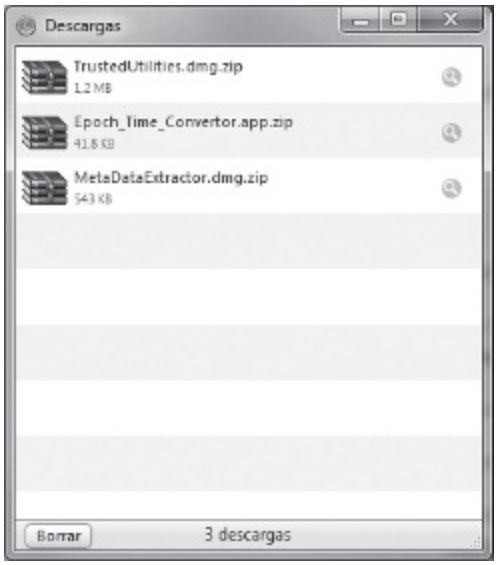
c. Oprimir el botón Detalles de la opción Cookies y otros datos de sitios web. Se abrirá una nueva ventana, donde aparece el listado de cookies y un campo para búsquedas de texto.



6. En el navegador Safari, en Microsoft Windows, visualizar downloads.plist:

a. Seleccionar en la barra de menú, el ícono de Mostrar un menú de ajustes generales de Safari.

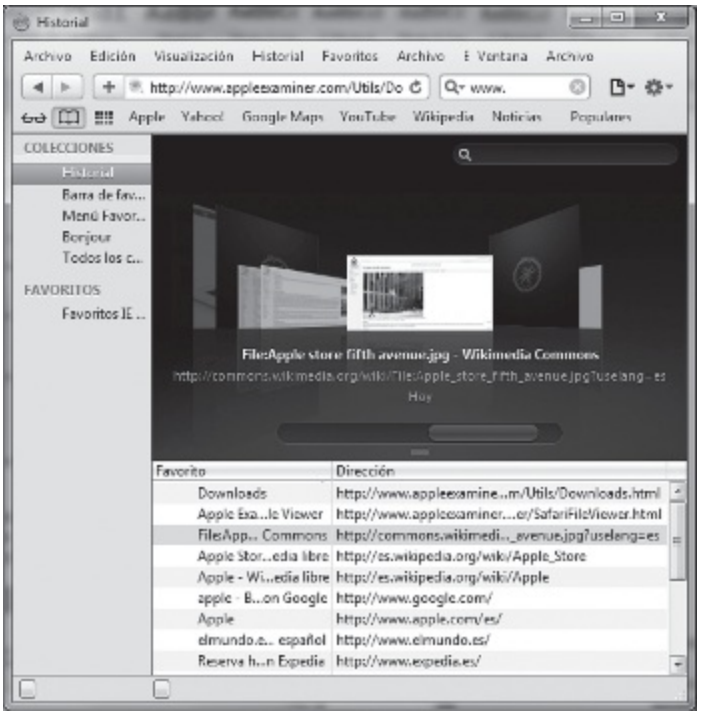
b. Seleccionar Descargas, aparecerá el listado de descargas en una nueva ventana.



7. En el navegador Safari en Microsoft Windows, visualizar history.plist:

a. Seleccionar, en la barra de menú, el ícono de Mostrar un menú de ajustes generales de Safari.

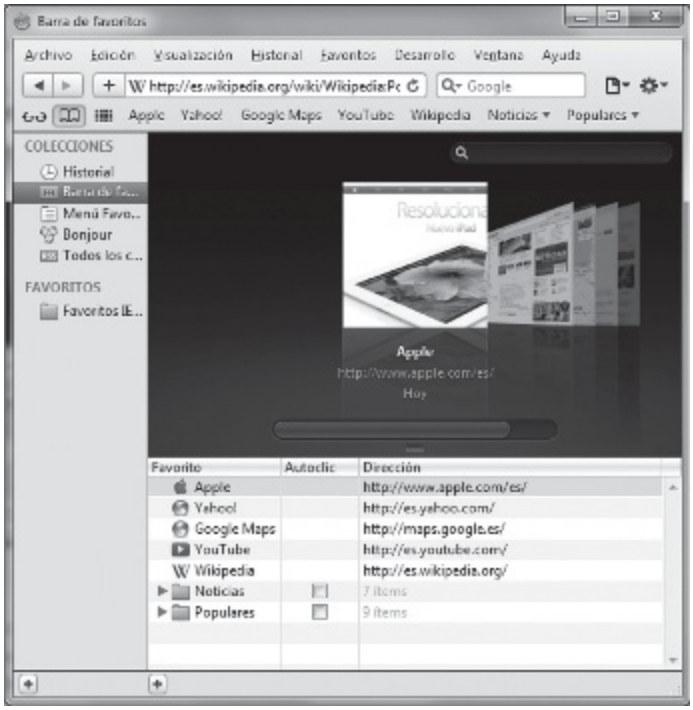
b. Seleccionar Historial; aparecerá en una nueva ventana el historial de sitios visitados con una previsualización de la página web del sitio visitado.



8. En el navegador Safari en Microsoft Windows, visualizar Bookmarks.plist.

a. Seleccionar en la barra de menú, el ícono de Mostrar un menú de ajustes generales de Safari.

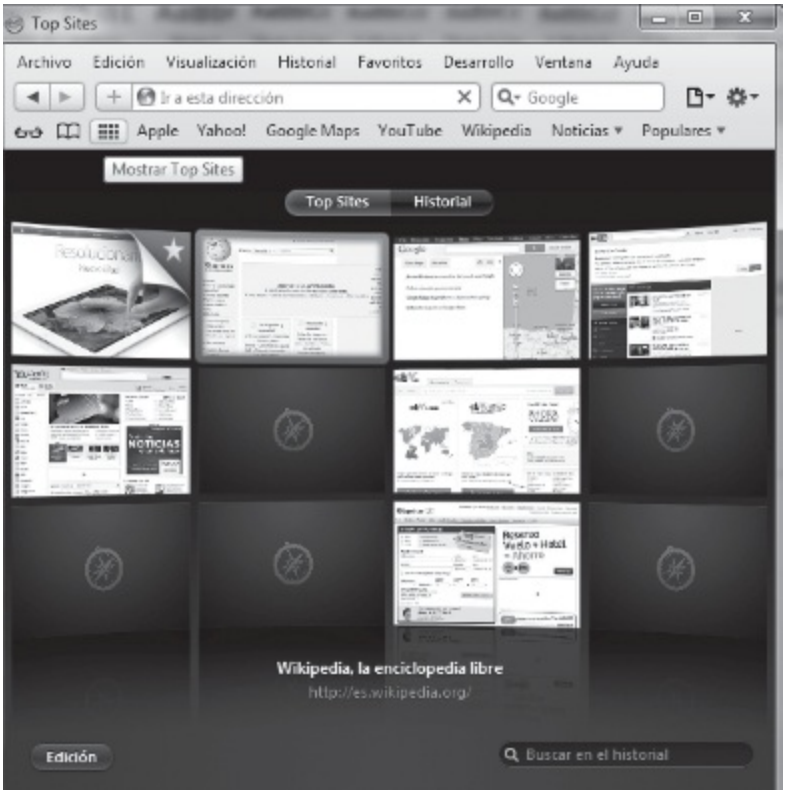
b. Seleccionar Historial; aparecerá una nueva ventana en la barra lateral, seleccionar Favoritos con una previsualización de la página web del sitio marcado como favorito y la dirección URL.



9. En el navegador Safari, en Microsoft Windows, visualizar Topsites.plist:

a. Seleccionar, en la barra de menú, el ícono de Mostrar Top Sites.

b. Seleccionar Historial, aparecerán en una vista preliminar los sitios más visitados y con un botón de edición para agregar los que aparecen vacíos como favoritos o con una X para eliminar el existente y otra opción para buscar.



Registrar, documentar y/o capturar pantallas con la información requerida.

Procedimiento para la recuperación y análisis de elementos de correo electrónico e iChat de la imagen adquirida

Consideraciones previas

La aplicación de correo Mail está incluida en el sistema operativo OS X de Macintosh, también se la conoce con los nombres de Mail.app o de Apple Mail. La aplicación utiliza los protocolos de correo POP3, SMTP, IMAP y soporta los correos de webmail Yahoo, Aol, Gmail, MobileMe (reemplazado por iCloud) y Microsoft Exchange a través del protocolo IMAP.

Obtener mail (Fetching) configura el programa para que automáticamente verifique la existencia de correo, por ejemplo, cada 13 minutos. Pushing es la actualización de la bandeja de entrada solamente cuando un correo es enviado al usuario.

La recuperación del correo electrónico dependerá del tipo de servicio de correo (almacenado localmente o basado en web) y de la aplicación utilizada por el usuario para acceder al correo electrónico.

El correo Apple Mail mantiene la estructura de archivos de Mac OS X y emplea el directorio Inicio (Home) del usuario. La carpeta Librería (Library) es la fuente de datos para la recuperación de correos electrónicos, ya sea de la aplicación Apple Mail u otro programa.

Los correos electrónicos se encuentran enumerados y poseen la extensión ".emlx" (XMLExtensible Markup Language).

1. En la estación de trabajo de Informática forense de Macintosh, en la imagen recolectada (imagen_Mac_dubitada.dmg), ubicar las carpetas:
   a. /[nombre_de_usuario]/Librería/Mail o /Mail/V2.
   b. /[nombre_de_usuario]/Librería/Mail/ o /Mail/V2/nombre_del_usuario, en esta carpeta se visualiza cada una de las casillas utilizadas por la cuenta del usuario conteniendo importante información para el perito. Las cuentas con dominio "@me.com" pertenecen al servicio MobileMe (la nueva versión es iCloud, la anterior era .Mac). Existen también buzones creados en forma predeterminada por MobileMe (Bandeja de entrada). El servicio iCloud crea automáticamente en el usuario las carpetas: Bandeja de entrada, Borradores, Enviados, Archivar, Papelera y Correo no deseado.
2. Utilizar la opción de vista previa para visualizar el contenido de cada una de las carpetas.
3. Analizar la carpeta que contiene los Mensajes (Messages):
   a. Verificar la numeración de los correos electrónicos y su extensión (por ejemplo: 19664.emlx, 19665.emlx, 19666.emlx).
   b. Identificar si los correos enumerados tienen archivos adjuntos en la carpeta Adjuntos; en el caso de que tenga un archivo adjunto, el número será el mismo que el del correo electrónico; si el mensaje contiene más de un archivo adjunto, aparecerán enumerados y en sus respectivas subcarpetas (por ejemplo: 2, 3).
   c. Verificar la existencia de cuentas de correo POP3 de proveedores de webmail (Google, Yahoo) que se encuentren almacenadas en las carpetas de Apple Mail.
4. Analizar la carpeta Preferencias del usuario, en la carpeta Librería. En Preferencias se encuentra información importante para el perito.
   a. Visualizar el contenido del archivo com.apple.mail.plist, en modo previsualización u oprimiendo la barra espaciadora para abrirlo o con el editor de lista de propiedades de Mac. El nombre de la lista de propiedad com.apple.mail es la notación reversa de la URL, correspondiente a

mail.apple.com.

b. Identificar en el archivo de propiedad la existencia de configuraciones relacionadas con las cuentas de correo:

i. Del protocolo de transferencia simple de correo SMTP (Simple Mail Transfer Protocol).

ii. Nombre de host.

iii. Número de puertos.

iv. Autenticación.

v. Nombre de usuario.

5. Generar el usuario de correo y visualizar su correo en Apple Mail.

a. Preparar un dispositivo externo con el formato del sistema de archivo HFS+ o el correspondiente a la imagen adquirida, con el fin de mantener la información de metadatos.

i. Desde la imagen recolectada (imagen_Mac_dubitada.dmg), copiar la carpeta que se encuentra en /Librería/Mail al dispositivo externo.

ii. Abrir la carpeta Preferencias y copiar el archivo com.apple.mail.plist.

iii. Otros archivos a copiar:

- MessageRules.plist, reglas de correo.
- SmartMailboxes.plist, datos de los buzones inteligentes.
- Carpeta Firmas, firmas del usuario.

b. En la estación de trabajo de Informática forense Macintosh, crear una cuenta de correo para efectuar el análisis de los mensajes.

c. En el menú de Apple, seleccionar Preferencias, Cuentas.

d. En la ventana Cuentas, seleccionar el ícono del candado para desbloquearlo.

e. En la ventana Cuentas, seleccionar el icono con el signo “+” para agregar un usuario.

f. En la ventana de Usuario Nuevo, crear una cuenta como un Administrador con el nombre de PeritoIF. Presionar la tecla Tab para que se complete el nombre abreviado. Ingresar la contraseña. No habilitar la protección de cifrado (FileVault).

g. Oprimir el botón de Crear cuenta.

h. Cerrar la sesión del usuario actual.

i. Iniciar sesión con la cuenta PeritoIF.

6. Abrir la carpeta Librería (Library) del usuario PeritoIF, seleccionar Menú, Ir, Inicio, Librería.

7. Abrir la carpeta Mail del dispositivo externo que fue copiada desde la

imagen recolectada (imagen_Mac_dubitada.dmg).

8. Organizar las dos ventanas para visualizar la carpeta Librería de la imagen recolectada y la carpeta Librería del usuario PeritoIF.

9. Arrastrar la carpeta Mail del dispositivo externo a la carpeta Librería del usuario PeritoIF.

10. Arrastrar el archivo com.apple.mail.plist del dispositivo externo a la carpeta Preferencias del usuario PeritoIF.

11. Abrir la aplicación Instantánea (Grab) que se encuentra en la carpeta Aplicaciones/Utilidades, para realizar capturas de pantalla a medida que cambia el estado del acceso a los mensajes de correo electrónico de lectura (no leído – leído).

12. Iniciar el correo Apple Mail desde la barra de accesos directos (Dock).

13. La aplicación Apple Mail abre un cuadro de diálogo para solicitar una contraseña de acceso para las cuentas de correo de POP3; esto se debe a que no se encuentra almacenada la clave y el acceso a las claves (Keychain) no tiene registro de la cuenta POP3; el perito deberá seleccionar el botón de Cancelar del cuadro de diálogo. El correo Apple Mail funcionará en el modo desconectado (offline).

14. Capturar la pantalla inicial del correo Apple Mail antes de realizar cualquier tarea.

15. Analizar los mensajes según corresponda con la requisitoria pericial, a partir de este paso el perito puede visualizar el contenido de los mensajes en forma nativa, guardar archivos adjuntos, imprimirlos como documento PDF para incorporarlos al informe pericial.

16. Registrar, documentar y/o capturar pantallas con la información requerida.

17. Asesorar al letrado para la solicitud de la prueba de informes para las cuentas del usuario asociadas con los dominios: me.com, mac.com, icloud.com, etc.

Procedimiento para la recuperación de mensajes del cliente de correo de Microsoft Entourage de Office: Mac 2008 para Mac

1. Copiar al dispositivo externo la carpeta completa de Main Identity que se encuentra en Documentos/Microsoft User Data/Office X Identities.

2. Copiar la carpeta del disco externo en la misma ubicación pero correspondiente al usuario PeritoIF.

3. Iniciar el cliente de correo Entourage.

4. Capturar la pantalla inicial con la aplicación Instantánea (Grab).

5. Analizar los mensajes según corresponda con la requisitoria pericial; a partir de este paso el perito puede visualizar el contenido de los mensajes en forma nativa, guardar archivos adjuntos, imprimirlos como documento PDF para incorporarlos al informe pericial.

6. Registrar, documentar y/o capturar pantallas con la información requerida.

7. Asesorar al letrado para la solicitud de la prueba de informes para las cuentas del usuario asociadas con los dominios pertinentes.

Procedimiento para la recuperación y análisis de la libreta de direcciones (Address Book) de la imagen adquirida

Consideraciones previas

La aplicación de la libreta de direcciones se encuentra incorporada en el sistema operativo de Mac. La aplicación de correo Apple Mail integra iPhone con la libreta de direcciones, lo mismo con los servicios MobileMe e iCloud.

La libreta de direcciones está en la carpeta Librería (Library) /Application Support/Address Book. Contiene las siguientes subcarpetas:

- Imágenes: Fotografías asociadas con las direcciones de la libreta asignadas por el usuario.
- Metadata: Contiene los archivos vCard para cada persona ingresada por el usuario en la libreta de direcciones.

En la carpeta Librería/Preferencias se encuentran los archivos de lista de propiedades asociados a la libreta de direcciones:

- AddressBookMe.plist: Archivo que se escribe solamente cuando se efectúa el registro del usuario propietario de la libreta de direcciones, puede no existir si el usuario optó por no registrarse. No se actualiza a medida que el usuario actualiza su información en la libreta de direcciones.
- com.apple.AddressBook.abd.plist: Archivo de configuración, no tiene valor como evidencia.
- com.apple.AddressBook.plist: Archivo de preferencias de la libreta de direcciones; este archivo es importante para la recuperación de datos.

1. Preparar un dispositivo externo con el formato del sistema de archivo HFS+ o el correspondiente a la imagen adquirida, con el fin de mantener la información de metadatos.

a. Desde la imagen recolectada (imagen_Mac_dubitada.dmg), copiar la carpeta que se encuentra en Librería/Application Support/AddressBook al dispositivo externo.

b. Abrir la carpeta Preferencias y copiar el archivo com.apple.AddressBook.plist.

2. En la estación de trabajo de Informática forense de Macintosh, iniciar sesión con el usuario PeritoIF.

3. Abrir la carpeta Librería, Menú Finder, Ir, Inicio, Librería del usuario PeritoIF.

4. Abrir la carpeta Librería/Application Support/AddressBook del dispositivo externo que fue copiada desde la imagen recolectada (imagen_Mac_dubitada.dmg).

5. Organizar las dos ventanas para visualizar la carpeta Librería de la imagen recolectada y la carpeta Librería del usuario PeritoIF.

6. Arrastrar la carpeta AddressBook del dispositivo externo a la carpeta Librería/Application Support/ del usuario PeritoIF. Aparece un cuadro de diálogo para reemplazar la carpeta existente; oprimir el botón Reemplazar.

7. Arrastrar el archivo com.apple.mail.plist del dispositivo externo a la carpeta Preferencias del usuario PeritoIF. Aparece un cuadro de diálogo para reemplazar el archivo existente; oprimir el botón Reemplazar.

8. Iniciar la aplicación de Libreta de direcciones para visualizar los contactos.

9. Analizar los contactos, imprimir la información a formato PDF con la opción estilo: Lista y Atributos: todos los campos seleccionados; de lo contrario, solo imprime información parcial, posteriormente agregarlo al informe pericial.

10. Registrar, documentar y/o capturar pantallas con la información requerida.

Procedimiento para la recuperación y análisis de datos del iChat de la imagen adquirida

Consideraciones previas

Los mensajes instantáneos ocurren en tiempo real, dificultando la tarea de recuperación. Los datos se almacenan en la memoria RAM del equipo y no se almacenan en el disco rígido, al menos que el usuario haya seleccionado la opción de guardar el contenido de las sesiones de iChat. Se puede encontrar información del iChat en los espacios no asignados del disco rígido.

La aplicación Adium (http://adium.im/), de código abierto, ofrece servicios de mensajería instantánea para Mac que reúne varios clientes en uno solo e integra la libreta de direcciones de Mac, además se puede conectar con múltiples servicios: AIM, MSN, Jabber, Yahoo, etc. El perito deberá verificar si esta aplicación se encuentra instalada en la computadora dubitada.

En la mensajería instantánea de iChat, no solo se intercambian mensajes de

texto, sino también videos, líneas telefónicas, mensajes de voz, que deben ser verificados y analizados por el perito, acorde a la requisitoria pericial.

1. En la estación de trabajo de Informática forense de Macintosh, en la imagen recolectada (imagen_Mac_dubitada.dmg), ubicar las siguientes carpetas y archivos:

a. Inicio (Home), Librería, Cachés; quedan datos del iChat que posteriormente se pueden efectuar correlaciones con la información obtenida.

b. Carpeta com.apple.iChat, que almacena información histórica del iChat.

c. Carpeta Fotografías, contiene archivos JPEG de los íconos de los usuarios de la lista de amigos. Los archivos JPEG no implican que se haya realizado la conversación, pero sí indican la presencia de esta persona en la lista de amigos del usuario.

d. Archivo PictureNameMap.plist, le permite al perito asociar la fotografía con un nombre de usuario.

e. Verificar la existencia de archivos de propiedad generados por otros clientes de mensajería instantánea:

- iChat AIM plist com.apple.iChat.AIM.plist
- iChat Jabber plist com.apple.iChat.Jabber.plist
- iChat Yahoo plist com.apple.iChat.Yahoo.plist

2. Preparar un dispositivo externo con el formato del sistema de archivo HFS+ o el correspondiente a la imagen adquirida, con el fin de mantener la información de metadatos.

a. Desde la imagen recolectada (imagen_Mac_dubitada.dmg), copiar la carpeta que se encuentra en Librería/Caches/com.apple.iChat/Pictures al dispositivo externo.

b. Abrir la carpeta Librería/Preferencias y copiar el archivo com.apple.iChat.plist al disco externo.

c. Abrir la carpeta Documents/iChats. Puede tener sesiones de iChat guardadas y copiar el contenido al disco externo.

3. En la estación de trabajo de Informática forense de Macintosh, iniciar sesión con el usuario PeritoIF.

4. Abrir la carpeta Librería/Caches del usuario PeritoIF.

5. Abrir la carpeta Librería/Caches/com.apple.iChat/Pictures del dispositivo externo que fue copiada desde la imagen recolectada (imagen_Mac_dubitada.dmg).

6. Organizar las dos ventanas para visualizar la carpeta Librería de la imagen recolectada y la carpeta Librería del usuario PeritoIF.

7. Arrastrar la carpeta com.apple.iChat/Pictures del dispositivo externo a la

carpeta Librería/Caches del usuario PeritoIF.

8. Arrastrar el archivo com.apple.iChat.plist del dispositivo externo a la carpeta Preferencias del usuario PeritoIF.

9. Arrastrar la carpeta iChats del dispositivo externo a la carpeta Documents del usuario

PeritoIF.

10. Iniciar la aplicación de iChat.

11. Editar el archivo PictureNameMap.plist, ubicar la sección Servicios, donde aparece listado el nombre del servicio y la cantidad de entradas con los nombres de los usuarios en el iChat. El perito puede efectuar un seguimiento de los nombres de usuario para asociarlos con una imagen JPEG que proviene de la lista de amigos del usuario, también puede estar relacionada con la libreta de direcciones y sus respectivos contactos. El archivo PictureNameMap.plist no brinda información sobre las asociaciones de la imagen con el contacto en la libreta de direcciones.

12. Analizar el archivo de transcripción de iChat, en el caso de que el usuario lo haya habilitado. La información se almacena en un archivo iChat y se visualiza con la aplicación iChat de la misma forma en que ocurrió originalmente.

13. Registrar, documentar y/o capturar pantallas con la información requerida.

Síntesis – Lista de control

Apple Mail

- Los datos a recuperar en el correo electrónico se encuentran en la carpeta de Inicio del usuario en /Librería/Mail de la aplicación Apple Mail y el archivo de lista de propiedades en /Librería/Preferencias com.apple.mail.plist.
- El dispositivo externo debe tener el formato del sistema de archivo desde donde se copiará la carpeta de mail dubitada y el archivo com.apple.mail.plist; esta información se copiará respectivamente en la misma ubicación, pero en una nueva cuenta para su posterior análisis.
- Otras aplicaciones de correo almacenan los datos en diferentes áreas del sistema de archivo, como el cliente de correo de Microsoft para Mac denominado Entourage, la carpeta a copiar es Main Identity que se encuentra en Documentos/Microsoft User Data/ Office X Identities.
- La aplicación Instantánea (Grab) permite al perito efectuar capturas de pantallas para incorporarlas al informe, en particular para registrar el estado inicial de la cuenta de correo en el nuevo usuario para establecer los mensajes leídos y no leídos.

Libreta de direcciones

· La aplicación de libreta de direcciones (Address Book) está incorporada en el sistema operativo de Mac e intercambia información con diferentes aplicaciones.

· El dispositivo externo debe tener el formato del sistema de archivo desde donde se copiará la carpeta Libreta de Direcciones dubitada, ubicada en Librería (Library) /Application Support/AddressBook; esta información se copiará en la misma ubicación pero en una nueva cuenta para su posterior análisis.

· En la recuperación de la libreta de direcciones, al generar los informes, se debe seleccionar la opción Listado en Estilo y marcar los Atributos.

iChat

· La aplicación de mensajería instantánea de Mac iChat está incorporada en el sistema operativo. Los programas de chat de Yahoo, Skype y Microsoft ofrecen clientes de mensajería instantánea para Mac.

· Los datos a recuperar en la mensajería instantánea de iChat se encuentran en la carpeta de Inicio del usuario en Librería.

· El intercambio de datos en iChat es en tiempo real, esto dificulta la recuperación de información, la cual se puede buscar en los espacios no asignados del disco, salvo que el usuario haya seleccionado la opción de guardar la sesión de chat y se transcriba a un archivo ubicado en la carpeta de Inicio del usuario /Documentos/iChats.

· El dispositivo externo debe tener el formato del sistema de archivo desde donde se copiará la carpeta iChat dubitada, ubicada en Librería (Librería/Caches/com.apple.iChat/ Pictures/) y el archivo de lista de propiedad com.apple.iChat.plist que se encuentra en Librería/Preferencias; esta información se copiará respectivamente en la misma ubicación pero en una nueva cuenta para su posterior análisis.

· La visualización del historial de iChat se debe efectuar desde la aplicación iChat.

Procedimiento para la recuperación y análisis de fotografías de la imagen adquirida

Consideraciones previas

El perito podrá encontrar archivos de fotografía almacenados en Mac de diferentes tipos:

· RAW (crudo): Formato de mejor calidad de imagen digital, tal como ha sido captada por la cámara digital.

· JPG. JPEG (Joint Photographic Experts Group): Formato que ofrece

calidad y compresión.

- GIF: Formato para imágenes pequeñas y de baja calidad.
- BMP: Formato de bitmaps, de alta resolución, de tamaño muy grande.
- PSD: Formato propietario de Photoshop.
- TIFF (Tagged Image File Format): Formato de alta calidad con compresión. Es el formato predeterminado de la aplicación Instantánea (Grab).
- PDF: Formato de documento portable, de Adobe e integrado a Mac.
- PNG (Portable Network Graphics): Formato de versión avanzada de GIF.

Asimismo, deberá conocer las aplicaciones de manejo de imágenes digitales: iPhoto, Adobe Photoshop, Graphic Converter para Mac, que permiten convertir diferentes tipos de archivos de imágenes.

La imagen encontrada en el disco del usuario puede registrar diversas modificaciones desde su captura por parte de una cámara digital o descarga a la carpeta iPhoto, que forma parte del conjunto de aplicaciones iLife, seguida de posibles modificaciones realizadas por el usuario con la aplicación Photoshop, hasta la conversión a un formato particular con el programa Graphic Converter.

El perito podrá efectuar el seguimiento de las imágenes, si no han sido eliminadas, a través de las fechas de creación y modificación para cada versión de la imagen y con los metadatos asociados a cada una para determinar la traza desde su inicio hasta el resultado final.

Características de la aplicación iPhoto

- Incorporada en el sistema operativo Mac, ofrece un manejo fácil de las imágenes y permite conectarse con la mayoría de las cámaras digitales.
- La primera vez que se inicia la aplicación pregunta si el usuario desea conectar iPhoto a la cámara digital. Si se responde que sí, a partir de ese momento iPhoto se conectará siempre con la cámara digital, permitiendo importar las imágenes a la biblioteca de iPhoto.
- Integrada a otras aplicaciones y servicios. Estos datos aparecen en el panel izquierdo de la aplicación acorde a lo que haya seleccionado el usuario (por ejemplo: iTunes, iWeb, MobileMe, iCloud).
- Trae incorporada la opción de compartir imágenes con otros usuarios, con la opción marcada de Mirar fotos compartidas (Look for shared photos).
- El usuario puede configurar iPhoto con su cuenta de MobileMe, iCloud y mostrar sus fotografías o colección (iPhoto, MobileMe, Preferencias). Las imágenes se pueden visualizar con el navegador web. A su vez, otros usuarios pueden incorporar fotografías al lugar indicado en el enlace compartido de la colección de fotografías y en el listado de álbumes publicados aparece la fecha

de publicación de estos. El nombre de la colección es un hipervínculo a un sitio web en donde se visualizan las imágenes.

· Almacena las fotografías en la carpeta Inicio, Imágenes. Dentro de esta carpeta se encuentra la biblioteca de iPhoto o fototeca, este archivo es un conjunto de archivos, para abrirlo oprimir la tecla Ctrl y el botón izquierdo del mouse sobre la carpeta y seleccionar Mostrar contenidos del paquete.

· En la Fototeca (iPhoto Library) se encuentra la subcarpeta Originales (Originals), que conserva la imagen inicial u original y la subcarpeta Modificados (Modified) que almacena las diferentes versiones de las modificaciones de la imagen o de la fotografía. Si el usuario decide que la foto modificada sea revertida al original, entonces será borrada de la carpeta Modificados.

· El archivo AlbumData.xml se puede leer con un editor de texto como TextEdit. En este archivo se encuentran las configuraciones de iPhoto, las direcciones URL de las colecciones (Gallery) y la dirección de correo electrónico para que cualquiera pueda enviar las imágenes a la colección, las cuales serán incluidas automáticamente en esta.

· En la carpeta Inicio/Librería/Preferencias, se encuentra el archivo de lista de propiedades com.apple.iphoto.plist. Contiene las configuraciones para iPhoto, incluyendo el lugar en donde se guarda la Fototeca de iPhoto. El usuario puede cambiar la ubicación predeterminada de la misma.

· El usuario puede tener múltiples Fototecas de iPhoto, por ejemplo, en un dispositivo externo. Las fotografías o imágenes están indexadas dentro de cada Fototeca con la aplicación del motor de búsqueda indexada del sistema operativo Mac: Spotlight. Esta herramienta de búsqueda es muy poderosa ya que se encuentra incorporada en el sistema operativo y es para el perito una herramienta válida para la búsqueda de datos. Spotlight indexa cualquier dispositivo conectado a la computadora siempre que se pueda escribir en el dispositivo. En el caso de utilizar la imagen dubitada, el montaje debe hacerse en solo lectura y bloquear el dispositivo pare evitar en este caso que Spotlight escriba en él. No obstante, esta herramienta no se puede utilizar para efectuar búsquedas en la imagen ".dmg" bloqueada, al menos que se monte utilizando un archivo sombra (shadow).

· La recuperación de las imágenes no se realizará de los espacios desasignados del disco o de los archivos borrados. En Mac, una vez que se borró la imagen se requiere utilizar técnicas de análisis de fragmentos (carving) almacenados en el disco, buscando el encabezado de la imagen. No existe la opción de recuperación (undelete).

Ubicación de los archivos de iPhoto

Elemento	Ubicación	Descripción
iPhoto fototeca	/Pictures/iPhoto Library (/imágenes/iPhoto Fototeca)	Contiene las imágenes de iPhoto.
Imágenes originales	/Pictures/iPhoto /Library/Originals/	Contiene la versión original de las imágenes.
Fotos modificadas	/Pictures/iPhoto /Library/Modified/	Contiene la versión modificada de la imagen.
Base de datos principal de iPhoto	/Pictures/iPhoto /Library/iPhotoMain.db	Información detallada de iPhoto.
Caché de imágenes del dispositivo iDevice	/Pictures/iPhoto /Library/iPod Photo Cache/	Carpetas con índices de imágenes sincronizadas a un dispositivo.
Reconocimiento facial	/Pictures/iPhoto /Library/	Base de datos SQLite con datos de reconocimiento facial o de rostros.
Datos del álbum	/Pictures/iPhoto /Library/AlbumData.xml	Información de álbumes, eventos, información de la imagen y su ubicación.
Elementos recientes de iPhoto	/Library/Preferences/com.apple.iPhoto.LSSharedFileList.plist	Detalle de los elementos recientes de iPhoto.
Preferencias de iPhoto	/Library/Preferences/com.apple.iPhoto.plist	Configuración de las preferencias de iPhoto.

1. En la estación de trabajo de Informática forense de Macintosh, copiar la imagen recolectada (imagen_Mac_dubitada.dmg) del dispositivo externo, en el escritorio de la estación de trabajo.
2. Bloquear la imagen ".dmg", oprimir la tecla Ctrl y con el mouse seleccionar el archivo, elegir la opción Obtener Información (Get Info) y luego seleccionar la casilla de verificación Bloqueado (Lock). Aparecerá un pequeño candado que indica que el archivo de la imagen se encuentra bloqueado para la escritura.
3. Abrir una terminal Ir, Utilidades, Terminal:

$hdiutil attach ~/Desktop/imagen_Mac_dubitada.dmg –shadow

El comando monta la imagen ".dmg" utilizando un archivo shadow:

$mdutil –sa

El comando verifica el estado (s) de la herramienta Spotlight en todos los dispositivos conectados (a); en el resultado debe aparecer /Volume/imagen_Mac_dubitada, estado: indexado deshabilitado.

$quit

Salir de la terminal.

4. Abrir una nueva ventana de Finder, seleccionar el ícono de la barra de accesos directos (Dock).

5. En el panel de la izquierda, seleccionar el volumen imagen_Mac_dubitada, se verá la carpeta Inicio de la imagen.

6. Efectuar la búsqueda de imágenes acorde a lo solicitado en la requisitoria pericial utilizando la herramienta de búsqueda Spotlight. Seleccionar la herramienta Spotlight. En la esquina superior derecha, seleccionar la lupa y en el cuadro de diálogo ingresar el criterio de búsqueda (por ejemplo: "jpg"). En forma inmediata, aparecerán los resultados.

7. En la primera línea de criterio de búsqueda ingresar: donde dice "Este Mac", colocar el nombre del usuario obtenido del archivo de la imagen Mac dubitada, en la misma línea cambiar Contenidos por nombre de archivo. En forma inmediata aparecerán los resultados.

8. En el buscador Spotlight, se pueden agregar criterios de búsqueda seleccionando el botón + en la parte superior derecha, arriba de la barra de desplazamiento, seleccionar e ingresar el criterio de búsqueda en los espacios del lado izquierdo del botón +:

a. Seleccionar Clase (Kind) y cambiar por Última apertura (Last opened is).

b. Seleccionar el campo de texto donde dice dentro de los últimos (within last), desplegar el menú y cambiar a En los últimos (Lastly), ingresar por ejemplo: 10/06/2012.

El resultado devolverá una determinada imagen del tipo "jpg", que responderá al criterio de búsqueda ingresado por el perito y en relación con la requisitoria pericial.

c. Abrir la imagen y analizar el contenido. La imagen no se modificará ya que se encuentra montado el volumen en solo lectura.

9. Analizar la información de los metadatos de la imagen seleccionada de la búsqueda anterior con el comando "mdls" (por ejemplo: imagen006.jpg):

a. Abrir una terminal: Ir, Utilidades, Terminal:

$mdls ~/Desktop/imagen006.jpg

El resultado del comando devuelve los metadatos asociados con la imagen: Marca y modelo de la cámara digital que capturó la imagen.

El perito puede utilizar este resultado para realizar una búsqueda con la marca y modelo de cámara.

b. En el buscador Spotlight, se pueden agregar criterios de búsqueda seleccionando el botón + en la parte superior derecha, arriba de la barra de desplazamiento, seleccionar e ingresar el criterio de búsqueda en los espacios del lado izquierdo del botón +, por ejemplo: Modelo de dispositivo coincide (matches) con Kodak.

c. Agregar el tercer criterio de búsqueda para acotar los resultados, por ejemplo, Fecha. Seleccionar el botón + por encima de la barra de desplazamiento y agregar el rango de fecha, también puede ser en formato absoluto, al instante en que se agregan los criterios de búsqueda, van apareciendo en la ventana del buscador los resultados. Otros criterios de búsqueda incluyen los siguientes metadatos:

i. Fecha de creación.

ii. Duración en segundos.

iii. Versión del GPS en el EXIF.

iv. Versión de EXIF para generar el metadato.

v. Editores.

vi. Dirección de correo electrónico.

vii. Software de codificación.

viii. Modo de exposición utilizado.

10. Registrar, documentar y/o capturar pantallas con la información requerida.

Síntesis – Lista de control

· Las imágenes en iPhoto pueden ser obtenidas de diversos dispositivos y pueden ser de diferentes tipos, la visualización del archivo debe realizarse con la aplicación compatible.

· Los usuarios pueden modificar la imagen original, quedando un registro en la carpeta

Modificados.

· El perito debe utilizar la información de metadatos de las imágenes para efectuar su seguimiento y sus modificaciones.

· La aplicación iPhoto le permite al usuario compartir sus fotos y publicarlas en la red local o en Internet.

· iPhoto almacena por defecto las imágenes en la carpeta de Inicio del usuario, pero el usuario puede elegir otras carpetas y/o dispositivos externos

en donde almacenar las imágenes.

· La herramienta para recuperar imágenes es el motor de búsqueda indexada de Mac denominado Spotlight, le permite al perito realizar búsquedas avanzadas sobre el contenido y los metadatos de la imagen.

· Spotlight indexa todo dispositivo conectado al sistema.

· Al analizar la imagen ".dmg", se debe bloquear para que sea de solo lectura y evitar que la herramienta de búsqueda escriba el índice al montar la imagen. La solución es utilizar el archivo shadow para simular el acceso de lectura y escritura de la imagen y luego manualmente habilitar el indexado.

· El archivo shadow es un archivo que guarda todas las posibles acciones de escritura que pudieran ocurrir del archivo ".dmg" y pueden ser borradas en forma segura después de que el archivo ".dmg" fue expulsado o desmontado.

Procedimiento para la recuperación y análisis de películas y videos de la imagen adquirida

Consideraciones previas

El perito deberá verificar la marca y modelo de la computadora Mac dubitada para determinar las especificaciones técnicas del equipo y sus configuraciones de hardware. En este caso, relacionado con las capacidades del tipo de cámara digital incorporada (iSight, a partir de junio de 2010 FaceTime, FaceTime HD), tarjetas adicionales de expansión y dispositivos para grabación de audio y video. En el sitio del fabricante www.apple.com o www.apple.com/es, se encuentran los diferentes modelos en donde el perito puede hallar la información pertinente.

El perito podrá encontrar diferentes formatos o tipos de archivos de video almacenados en Mac:

· MOV, propietario de Apple de la aplicación multimedia QuickTime, calidad y compresión.

· MP4, estándar de video digital (ISO/IEC 14496-14:2003) MPEG-4, compresión digital y alta calidad de video.

· M4V, de QuickTime de Apple, similar a MP4, utilizado en iPhone, iPod y AppleTV, iTunes descarga videos en este formato.

· FLV, es de la aplicación Flash, de Adobe. Se utiliza en la web por su capacidad de transmisión de video en el navegador. No es un formato de alta calidad.

· DV, digital video, utilizado por las cámaras de video; cuando se transfiere a Macintosh es convertido a otro formato.

· WMV, Window Media Player, desarrollado por Microsoft. El componente Flip4Mac (www.flip4Mac.com) permite soportar archivos WMV en

QuickTime.

- DivX, Div Ex, desarrollado por DivX Inc., basado en el estándar MPEG4, de alta calidad y máxima compresión. Requiere una aplicación particular para su visualización.

El perito, además de reconocer los diversos tipos de archivos de video con sus respectivos componentes de metadatos y contenido, también deberá analizar el software de reproducción y edición de películas o videos:

- La aplicación de edición de video Final Cut Pro (http://www.apple.com/es/finalcutpro/top-features/) hallada en una computadora indica un conocimiento avanzado del usuario sobre el manejo de video.
- La aplicación de Macintosh iMovie (http://www.apple.com/es/ilife/imovie/) forma parte del paquete iLife y permite importar, reenviar, compartir y editar películas; se integra a otros programas como iDVD (para agregar videos, fotos, música a un DVD) e iPhoto. Las posibilidades de publicación en Internet de la película le permiten al usuario elegir el formato apropiado (Navegador multimedia, QuickTime, Final Cut) con el objeto de publicarlo directamente desde iTunes para compartirlo. También lo puede enviar a Internet, Facebook, YouTube o Vimeo y a la videoteca de MobileMe o iCloud. En ambos casos, se requiere de una cuenta de acceso.
- En el caso de YouTube, la aplicación iMovie registra la información de la cuenta del usuario en el archivo de propiedad de iMovie.plist; para MobileMe no requiere autenticación de usuario y clave porque es un servicio que ya está integrado en el sistema operativo de Macintosh y lo reconoce como ya configurado permitiéndole publicar directamente.
- El perito deberá verificar el tipo de publicación del proyecto de película de la computadora dubitada. Otras características de la aplicación a considerar son: La creación y publicación de podcast para subirlos posteriormente al Podcast Producer de Apple. La opción Buscador de personas de iMovie analiza los videos o películas en busca de escenas con caras e informa cuántas existen en cada una; puede distinguir entre primeros planos, planos medios y planos generales.
- Los programas para reproducción de películas en Macintosh son: QuickTime Player, Flip4Mac, VideoLAN´s VLC Media Player y MPlayer OS X.

1. En la estación de trabajo de Informática forense de Macintosh, copiar la imagen recolectada (imagen_Mac_dubitada.dmg) del dispositivo externo, en el escritorio de la estación de trabajo.
2. Bloquear la imagen ".dmg", oprimir la tecla Ctrl y con el mouse seleccionar

el archivo, elegir la opción Obtener Información (Get Info) y luego seleccionar la casilla de verificación Bloqueado (Lock). Aparecerá un pequeño candado que indica que el archivo de la imagen se encuentra bloqueado para la escritura.

3. Abrir una terminal: Ir, Utilidades, Terminal:

$hdiutil attach ~/Desktop/imagen_Mac_dubitada.dmg –shadow

El comando monta la imagen ".dmg" utilizando un archivo shadow:

$mdutil –sa

El comando verifica el estado (s) de la herramienta Spotlight en todos los dispositivos conectados (a), en el resultado debe aparecer /Volume/imagen_Mac_dubitada, estado: indexado deshabilitado.

$quit

Salir de la terminal.

4. Abrir una nueva ventana de Finder, seleccionar el ícono de la barra de accesos directos (Dock).

5. En el panel de la izquierda, seleccionar el volumen imagen_Mac_dubitada, se verá la carpeta Inicio de la imagen.

6. Efectuar la búsqueda de imágenes acorde a lo solicitado en la requisitoria pericial utilizando la herramienta de búsqueda Spotlight. Seleccionar la herramienta Spotlight. En la esquina superior derecha, seleccionar la lupa y en el cuadro de diálogo ingresar el criterio de búsqueda (por ejemplo: "m4v"). En forma inmediata, aparecerán los resultados.

7. En la primera línea de criterio de búsqueda ingresar: donde dice "Este Mac", colocar el nombre del usuario obtenido del archivo de la imagen_Mac_dubitada, en la misma línea cambiar Contenidos por nombre de archivo. En forma inmediata, aparecerán los resultados.

8. En el buscador Spotlight, se pueden agregar criterios de búsqueda seleccionando el botón + en la parte superior derecha, arriba de la barra de desplazamiento, seleccionar e ingresar el criterio de búsqueda en los espacios del lado izquierdo del botón +:

a. Seleccionar Clase (Kind) y cambiar por: Última apertura (Last opened is).

b. Seleccionar el campo de texto donde dice dentro de los últimos (within last), desplegar el menú y cambiar a En los últimos (Lastly), ingresar por ejemplo: 10/06/2012.

El resultado devolverá un determinado archivo de video del tipo "m4v", que responderá al criterio de búsqueda ingresado por el perito y en relación con la requisitoria pericial.

c. Abrir el archivo de video y analizar el contenido. El archivo de video no se

modificará ya que se encuentra montado el volumen en solo lectura.

9. Abrir una nueva ventana de Finder, seleccionar el ícono de la barra de accesos directos (Dock), para crear búsquedas de películas en toda la computadora, incluye los dispositivos conectados, y luego guardarlas.

10. En el área de búsqueda de la herramienta Spotlight, ingresar el texto mov; los resultados aparecerán inmediatamente.

11. Verificar que el lugar donde se realiza la búsqueda sea “Este Mac” (This Mac) como primer criterio de búsqueda.

12. Seleccionar el botón + en la parte superior derecha, arriba de la barra de desplazamiento, para agregar un segundo criterio de búsqueda; seleccionar el menú desplegable Cualquiera (Any) y cambiar a Películas (Movies).

13. Oprimir el botón Guardar, en el extremo superior derecho debajo del cuadro de texto de Spotlight, asignar un nombre a la búsqueda y oprimir el botón Agregar; la búsqueda quedará agregada en la barra lateral. La búsqueda se podrá utilizar en futuras consultas.

14. Utilizar la misma consulta pero en vez de la opción “Este Mac”, acotar la búsqueda a otros dispositivos, seleccionándolos en el panel de la derecha donde dice Dispositivos.

15. En la imagen dubitada ubicar el nombre del archivo de un proyecto realizado con iMovie (por ejemplo: Prueba).

16. Reconstruir las acciones del usuario dentro del proyecto, abrir el archivo com.apple. iMovie11.plist de la carpeta Librería/Preferencias, para visualizar las configuraciones de la aplicación iMovie, oprimir la barra espaciadora para editar el archivo plist o editarlo con un editor de lista de propiedad.

17. Analizar la configuración del archivo com.apple.iMovie11.plist:

a. UseDotMac, con valor SÍ (Yes), implica que MobileMe está configurado para publicar videos o películas.

b. ytUsername, el valor contenido indica el nombre de usuario utilizado para publicar videos o películas, no indica necesariamente el nombre de la cuenta de YouTube, solo es un nombre tentativo para su publicación en YouTube; se deberá buscar en la lista de nombres de cuenta de YouTube válidos.

18. Ubicar la carpeta de Inicio del usuario y la subcarpeta Películas (Movies). El proyecto guardado se verá como nombre: Prueba.rcproject con el ícono de paquete y en clase: iMovie Project.

19. Visualizar el contenido del archivo Prueba.rcproject, oprimir la tecla Ctrl + el botón izquierdo del mouse sobre el archivo y elegir Mostrar contenidos del paquete y se abrirá una nueva ventana del Finder.

a. Aparecen listados los tipos de archivos para publicar en MobileMe o iCloud; el tipo de archivo dependerá del lugar en donde se lo desee publicar:

i. Nombre del archivo1, clase :m4v.

ii. Nombre del archivo2, clase: 3gp.

iii. Project, clase: Texto plano (Plain text), este archivo es una lista de propiedad y puede editarse para ver las configuraciones particulares de este proyecto, incluyendo la dirección web para la publicación en MobilMe o iCloud.

20. Registrar, documentar y/o capturar pantallas con la información requerida.

Síntesis – Lista de control

· Macintosh es compatible con la mayoría de los formatos de archivos actuales de videos o películas.

· El tipo de extensión para QuickTime puede ser ".mov" y ".mv4".

· Las aplicaciones de video incluidas en Macintosh son iMovie e iDVD, que forman parte del paquete iLife, y permiten editar, compartir y subir a Internet videos por medio de iTunes, MobileMe, iCloud, Facebook, YouTube o Vimeo.

· Verificar la publicación de podcast en el Podcast Producer de Apple.

· En el archivo de lista de propiedad iMovie.plist se encuentra evidencia de la publicación de videos en Internet.

· Los archivos creados con iMovie se almacenan en un paquete denominado proyecto.

En este archivo se encuentra información de las películas o videos digitales asociados al proyecto, como así también el archivo de lista de propiedad ".plist" mostrando la ubicación exacta para cualquier publicación realizada en Internet.

· Efectuar búsquedas de películas con la herramienta de búsqueda Spotlight en toda la computadora y luego ir acotando la búsqueda hasta incluir la imagen dubitada como archivo shadow.

· Utilizar los metadatos del archivo de la película o video para realizar búsquedas específicas a fin de determinar el tipo de aplicación con la que fue creado.

· La herramienta de búsqueda Spotlight no indexa los contenidos de un proyecto de iMovie, el perito debe buscar primero el proyecto y una vez encontrado analizar manualmente su contenido.

· Analizar los videos con la opción Buscador de personas de la aplicación iMovie.

Procedimiento para la recuperación y análisis de archivos del procesador de texto Word y de

documentos portables (PDF)

Consideraciones previas

La versión del paquete de oficina de Microsoft Office:Mac (http://www.microsoft.com/latam/mac/products) para Macintosh es idéntica en estructura a la de Microsoft Windows. Esto facilita la recuperación de información de metadatos, en este archivo se encuentra la información de la configuración realizada con la opción de preferencias de las aplicaciones del paquete Office.

Las opciones de preferencias se configuran accediendo al Menú Word, Preferencias; una de las configuraciones se relaciona con la información del usuario que contiene: Nombre, Apellido, Iniciales, Empresa, Dirección postal, Ciudad, Número de teléfono, Dirección electrónica; también se pueden agregar metadatos oprimiendo el botón Más; aquí la información a incorporar está dividida en siete categorías: Resumen, Nombre y Dirección de correo electrónico, Hogar, Trabajo, Personal, Otros, Certificados.

La información de los cameos de Nombre y Apellido se agregará al campo Autor en las propiedades del documento. Para visualizar este campo: abrir el documento en Word y seleccionar Archivo, Propiedades. La opción Resumen, en forma predeterminada, no se muestra como una parte del proceso de guardar el documento, por esta razón muchos usuarios no saben que la información se almacena en el archivo.

El paquete de oficina Microsoft Office:Mac utiliza un formato de XML orientado a objeto para almacenar el contenido de los archivos y los metadatos, esta característica permite la

compresión de datos para reservar espacio e incrementar la portabilidad del documento. Los archivos guardados con el formato XML no son más que archivos comprimidos tipo zip que contienen una serie de documentos XML.

Tipos de archivos en Microsoft Office:Mac: Word: docx, Excel: xlsx, PowerPoint: pptx.

1. Analizar los metadatos en XML de un archivo generado por el procesador de texto Word:

a. Convertir el archivo seleccionado con extensión docx a XML:

i. Borrar la extensión docx y reemplazarla por la extensión zip.

b. En el Finder aparecerá una carpeta con el mismo nombre del archivo en Word pero con la extensión zip.

c. Descomprimir el archivo; aparecerán tres carpetas y un archivo:

d. En la carpeta docProps se encuentra el archivo core.xml y app.xml. Si el archivo posee imágenes, se creará una carpeta Word/media, que contiene

copia de las imágenes usadas en el documento actual. Puede incluir imágenes que fueron utilizadas en revisiones anteriores del documento actual y fueron borradas. El archivo core. xml contiene un conjunto de información relacionada con el documento en sí mismo. Abrir el archivo core.xml con Notepad o Internet Explorer.

e. En el archivo analizar las siguientes etiquetas XML:

<dc:title>, título del documento asignado por el usuario.

<dc:subject>, tema del documento asignado por el usuario.

</dc:creator>, nombre de usuario ingresado la primera vez que se ejecutó Word.

<cp:keywords>, palabras clave definidas por el usuario.

<cp:description>, descripción del documento definida por el usuario.

<cp:lastModifiedBy>, muestra el nombre de la persona que editó por última vez el documento, no el creador original del documento.

<cp:revision>, el número de revisión del documento; Office mantiene esta información y la única forma de editarla es por medio del acceso y modificación de los datos en XML contenidos en él.

<dcterms:created>, la fecha y hora de creación del documento. La fecha y hora se basa en el reloj del sistema y es tan segura como la fecha y hora de modificación, acceso y creación normal. La información guardada en este campo es convertida a la hora UTC.

<dcterms:modified>, la fecha y hora de la última modificación del documento. Esta información se almacena de la misma forma que la hora y fecha de creación y ofrece el mismo nivel de confianza.

f. Abrir el archivo app.xml con Notepad o Internet Explorer.

g. En el archivo analizar las siguientes etiquetas XML:

<Template>, la plantilla predeterminada que se utilizó para crear el archivo (Normal.dot).

<TotalTime>, el tiempo total en que estuvo abierto el archivo para su edición y se realizan cambios; el tiempo no se cuenta cuando no se realizan cambios en el documento.

<Pages>, el número de páginas en el documento.

<Words>, el número de palabras en el documento.

<Characters>, el número de caracteres en el documento. Este valor no incluye espacios o renglones entre párrafos.

<Application>, el nombre de la aplicación utilizada para la última edición.

<DocSecurity>, el nivel de seguridad aplicado al documento, Microsoft no publica los diferentes valores de niveles de seguridad. Un análisis posterior

será necesario para determinar los diferentes valores. El valor predeterminado es cero, que indica que el documento no tiene seguridad.

<Lines>, el número de líneas o renglones del documento.

<Paragraphs>, el número de párrafos en el documento.

<ScaleCrop>, una variable booleana (Verdadero-Falso) que indica si cualquier imagen en el documento está en escala o recortada.

<Company>, el nombre de la empresa ingresado por el usuario.

<LinksUpToDate>, una variable booleana que indica si los datos enlazados han sido actualizados.

<CharactersWithSpaces>, la cantidad de caracteres, incluyendo los espacios, no los retornos de carro.

<SharedDoc>, una variable booleana que indica si el documento actual está marcado para colaboración a través de Microsoft Share Point. El valor predeterminado es FALSO.

<HyperlinksChanged>, una variable booleana que indica si han cambiado los datos enlazados dentro del archivo.

<AppVersion>, el número de versión del Office que fue utilizado en el último resguardo del documento. En Office 2008 el valor mostrado de la versión será de 12.000.

2. Visualizar los documentos con formato PDF con la aplicación de previsualización de Macintosh ya que no necesita el programa Adobe Acrobat Reader para leer el contenido de estos archivos. Los archivos PDF pueden tener diferentes firmas y esto dificulta el hallazgo de fragmentos de archivos en los espacios no asignados en el caso de que hubieran sido borrados.

3. En la estación de trabajo de Informática forense de Macintosh, abrir Finder.

a. En la parte superior de la barra de menú, seleccionar Archivo.

b. Ubicarse en Buscar.

c. Seleccionar el volumen en donde se encuentra la imagen recolectada (imagen_ Mac_dubitada.dmg).

d. Efectuar la búsqueda seleccionando nombre y coincide con.

e. En el cuadro de texto de la derecha, ingresar el parámetro de búsqueda ".doc". La herramienta Finder efectuará automáticamente la búsqueda de los archivos ".doc" y mostrará las coincidencias en la pantalla de resultados.

f. Ídem e., pero para archivos ".pdf", ".txt" o cualquier otro archivo solicitado por la requisitoria pericial.

g. Verificar la existencia de archivos de Microsoft Office:Mac: Word: docx, Excel: xlsx, PowerPoint: pptx.

4. Verificar la existencia de los documentos creados con el paquete de oficina Office:Mac en la ubicación predeterminada /Usuario/Documentos.

5. Analizar las listas de propiedades de los documentos creados con Excel y Word, ubicadas en ~/Librería/Preferencias/, con un editor de lista de propiedades u oprimiendo la barra espaciadora:

a. com.microsoft.Word.plist, muestra la ubicación de los archivos guardados y una lista de los archivos abiertos recientemente.

b. com.microsoft.Excel.plist, muestra la ubicación de los archivos guardados y una lista de los archivos abiertos recientemente.

c. com.microsoft.Excel.prefs.plist, muestra los archivos abiertos recientemente.

6. Analizar los siguientes elementos del cliente de correo Entourage de Microsoft para Macintosh:

a. Correo electrónico:

i. Información de cuentas de correo.

ii. Correos electrónicos y metadatos asociados.

b. Libreta de direcciones:

i. Información del usuario local incluyendo nombre y otra información de contacto.

ii. Información de contacto para todos los individuos asociados que se encuentren registrados en la libreta de direcciones.

c. Notas:

i. Notas escritas por el usuario a través de Entourage.

ii. Fecha y hora en que fue creada la nota.

d. Tareas:

i. Tareas programadas, fecha y hora de creación de la tarea programada.

e. Calendario:

i. Citas.

ii. Nombres y direcciones incluidas en las citas.

iii. Reuniones e información asociada.

f. Verificar la ubicación de los archivos de Entourage en la carpeta: ~/Documentos/ Microsoft User Data/

i. Aparecerán dos carpetas: Entourage Menu Items y Excel Script Menu Items, sin valor para la evidencia.

ii. La carpeta de auto recuperación de Office (versión 2008, 2011) contiene copias de archivos si la opción fue configurada en la aplicación Word dentro de Preferencias.

iii. La carpeta Office (versión 2008, 2011) Identities, contiene numerosos archivos que pueden poseer evidencia:

• Newsgroup Caché: Contiene evidencia si el usuario se suscribió a un grupo de noticias.

• Base de datos: Es el archivo principal, contiene todos los elementos dentro de Entourage; abrir con la herramienta Editor de Texto de Mac para ver correos electrónicos, calendario, etc.

• Listas de correo, Reglas de correo y Firmas.

7. Visualizar la base de datos del cliente de correo Entourage por medio de la aplicación de correo Entourage en la estación de trabajo de Informática forense Macintosh.

a. Verificar si la estación de trabajo tiene la carpeta Microsoft User Data; si existe, borrarla.

b. Verificar que no se esté ejecutando ninguna aplicación de Microsoft y que no se encuentren abiertas las conexiones de red alámbricas e inalámbricas.

c. Seleccionar el volumen en donde se encuentra la imagen recolectada (imagen_ Mac_dubitada.dmg).

d. En la imagen: ubicarse en el directorio de inicio del usuario Documents/Microsoft User Data.

e. Efectuar un click con el botón del menú contextual del mouse (derecho) sobre la carpeta Microsoft User Data y seleccionar Copiar.

f. Pegar la carpeta Microsoft User Data en la misma ubicación pero en la estación de Informática forense Macintosh.

g. Abrir el programa de cliente de correo Entourage.

h. Seleccionar el ícono de Mail del extremo superior izquierdo que tiene un sobre de carta y en el panel inferior se observarán los correos del usuario; determinar el que sea de utilidad para la evidencia.

i. Seleccionar el ícono de Libreta de direcciones, que le sigue al ícono del sobre de carta y determinar si algunos de los datos son de interés para la evidencia.

j. Seleccionar el ícono Calendario que se encuentra a continuación del ícono de Libreta de direcciones y determinar si algunos de los datos son de interés para la evidencia.

k. Seleccionar el ícono de Notas, que se encuentra al lado del ícono de Calendario y determinar si algunos de los datos son de interés para la evidencia.

l. Seleccionar el ícono de Tareas, que se encuentra a continuación del ícono de Notas y determinar si algunos de los datos son de interés para la evidencia.

m. Seleccionar el ícono Centro de proyectos (Project Center), que se encuentra al lado del ícono de Tareas y es el último de los ítems de la barra de menú, y determinar si algunos de los datos son de interés para la evidencia. Es una combinación de elementos en Entourage y puede asociar correo electrónico, calendario, contactos y notas, también puede adjuntar archivos en Word y Excel.

n. Seleccionar el ícono Mi Día (My Day), que se encuentra a la izquierda de Enviar y Recibir correo. El ícono puede aparecer también en el escritorio, contiene información sobre las tareas organizadas para el día por parte del usuario (Almuerzo, Trabajo, Cena, etc.).

8. Analizar los mensajes de correo de Entourage; seleccionar el ícono del Correo (Mail) y abrir un mensaje desde el panel de visualización de correo.

a. Verificar el nombre del remitente (Desde From) y del destinatario (Para To) del correo y la fecha y hora de envío en el campo Fecha (Date) y el Asunto.

b. Visualizar el encabezado del correo[137], seleccionar Mensaje, Código Fuente.

i. Analizar: dirección IP de origen y de destino, fecha y hora.

c. Ingresar al resto de las carpetas de correo electrónico acorde a la requisitoria pericial:

i. Bandeja de entrada.

ii. Borradores.

iii. Bandeja de salida.

iv. Elementos enviados.

v. Elementos eliminados.

vi. Correo electrónico no deseado.

d. Registrar los datos, capturar pantalla y/o imprimir.

9. Analizar la Libreta de direcciones, seleccionar el ícono de Libreta de direcciones:

a. Seleccionar el contacto de interés para la evidencia y visualizar la información de metadatos asociada al contacto.

b. Registrar los datos, capturar pantalla y/o imprimir.

10. Analizar el Calendario de Entourage, seleccionar el ícono de Calendario:

a. Visualizar en la barra de la izquierda los diferentes calendarios.

b. Seleccionar el elemento de interés para la evidencia y efectuar un doble click o abrir la cita.

c. Visualizar la fecha de creación de la cita:

i. Ir a la carpeta /usuario/Library/Caches/Metadata/Microsoft/Entourage/2008/ Main

Identity/Messages de la imagen.

ii. Ubicar la identidad (Ejemplo: /OT/OB/OM/6K); se visualizan varios archivos de eventos.

iii. Abrir el evento (archivo .rge08Event) hasta localizar el elemento requerido, seleccionarlo con el botón derecho del mouse o del menú contextual y registrar la fecha y hora de creación del evento.

iv. Registrar los datos, capturar pantalla y/o imprimir.

11. Analizar las Notas en Entourage:

a. Seleccionar el ícono de Notas y verificar detenidamente el contenido de las carpetas.

b. Abrir la nota de interés para la evidencia.

c. Registrar los datos, capturar pantalla y/o imprimir.

d. Buscar la fecha de creación de la nota:

i. Ir a la carpeta /usuario/Library/Caches/Metadata/Microsoft/Entourage/2008/ Main Identity/Notes de la imagen.

ii. Ubicar la identidad (Ejemplo: /OT/OB/OM/6K), se visualizan varios archivos de notas (.rge08Note).

iii. Abrir el archivo, seleccionarlo con el botón derecho del mouse o del menú contextual y registrar la fecha y hora de creación de la Nota.

iv. Registrar los datos, capturar pantalla y/o imprimir.

12. Analizar las Tareas en Entourage:

a. Seleccionar el ícono de Tareas y verificar detenidamente el contenido de las carpetas.

b. Abrir la tarea de interés para la evidencia.

c. Registrar los datos, capturar pantalla y/o imprimir.

d. Buscar la fecha de creación de la tarea:

i. Ir a la carpeta /usuario/Library/Caches/Metadata/Microsoft/Entourage/2008/ Main Identity/Tareas de la imagen.

ii. Ubicar la identidad (Ejemplo: /OT/OB/OM/6K); se visualizan varios archivos de notas (.rge08Task).

iii. Abrir el archivo, seleccionarlo con el botón derecho del mouse o del menú contextual y registrar la fecha y hora de creación de la tarea.

iv. Registrar los datos, capturar pantalla y/o imprimir.

13. Analizar la carpeta de archivos adjuntos, ubicada en /Usuario/Documentos/Microsoft User Data/Saved Attachments:

a. Visualizar en los correos los mensajes con archivos adjuntos; en forma predeterminada Entourage guarda los adjuntos en esta carpeta.

b. Registrar los datos, capturar pantalla y/o imprimir.

14. Analizar el contenido de información de configuración, preferencias, bases de datos, etc., de los archivos de lista de propiedad del cliente de correo Outlook 2011 para Mac, que se encuentran en la carpeta Librería/Preferencias. Editar los siguientes archivos con el editor de listas de propiedad u oprimiendo la barra espaciadora:

a. com.Microsoft.Outlook.plist

b. com.Microsoft.Outlook.database_daemon.plist

c. com.Microsoft.Outlook.database_utility.plist

d. com.Microsoft.Outlook.office_reminders.plist

e. com.Microsoft.Outlook.SyncServicesPreferences.plist

15. Registrar, documentar y/o capturar pantallas con la información requerida.

Síntesis – Lista de control

· El paquete de oficina de Microsoft Office:Mac, versiones 2008 o 2011, contiene en sus documentos información de interés para el perito.

· Las herramientas de Mac y el Office de Mac son las más adecuadas para visualizar los archivos de Office:Mac.

· La técnica de copiar los datos a analizar de la imagen dubitada de solo lectura y pegarla en la misma ubicación en la estación de Informática forense Macintosh permite visualizar la información de la misma forma que fue creada.

· El perito puede determinar las fechas de creación de Notas, Tareas, Calendario.

· Los metadatos de Office:Mac pueden contener información del usuario.

· Los metadatos pueden estar sin información para evitar la detección del usuario.

· Los archivos de Office:Mac 2008 y versiones posteriores pueden ser guardados en el formato XML.

· El cliente de correo Microsoft Entourage para Mac es similar al Microsoft Outlook de la versión de Office:Mac 2011.

· La recuperación y el análisis de los espacios no asignados o de los archivos de Office:Mac borrados deben realizarse con herramientas específicas para la detección de fragmentos de archivos. La plataforma Macintosh permite analizar los documentos pero no puede recuperar los que se encuentran eliminados y fragmentados en el espacio no asignado.

Procedimiento para el análisis del historial de conexiones de dispositivos

Consideraciones previas

El sistema operativo OS X mantiene un historial de conexiones del puerto USB; la información se encuentra en archivos de lista de propiedad y en los registros de sucesos o eventos del sistema operativo. La información contenida en los archivos plist puede ser de los dispositivos del tipo FireWire, SATA/eSATA.

1. En la estación de trabajo de Informática forense de Macintosh, en la imagen recolectada (imagen_Mac_dubitada.dmg), editar los siguientes archivos de lista de propiedad con el editor:
   a. Historial de dispositivos conectados al sistema: Users/username/Library/Preferences/com.apple.sidebarlists.plist.
   b. Historial de iPhone y iPod conectados al sistema: Library/Preferences/com.apple. iPod.plist.
   c. Historial de un usuario específico: Users/“username”/Library/Preferences/com. apple.iPod.plist.
2. Analizar los siguientes archivos de registros de eventos:
   a. Registros del sistema: system.log
   b. Registros del kernel: kernel.log
   c. Registros de conexiones USB: kernel[0]: USBMSC Identifier
   d. Registro de grabaciones de CD/DVD: DiscRecording.log
   e. Registro de inicio, borrado seguro, etc., de volúmenes: DiskUtility.log
   f. Registro de información específica del disco: fsck_hfs.log
3. Registrar, documentar y/o capturar pantallas con la información requerida.

Procedimiento para el análisis de conexiones Bluetooth

Consideraciones previas

Los dispositivos Bluetooth contienen información importante que se puede analizar con herramientas de desarrollo de Macintosh como el Explorador de Bluetooth del conjunto de herramientas de desarrollo https://developer.apple.com/technologies/tools.

1. Analizar la información de dispositivos emparejados con el programa Explorador de Bluetooth que se encuentra en la estación de Informática forense Macintosh en el directorio

Developer/Applications/Utilities/Bluetooth/Bluetooth Explorer.

2. Registrar, documentar y/o capturar pantallas con la información requerida.

Procedimiento para el análisis de conexiones vNC

Consideraciones previas

En la versión del sistema operativo Macintosh Leopard existe la facilidad de tomar el control remoto de una computadora Macintosh a través de compartir una pantalla, escritorio remoto o de computación virtual en red (VNC Virtual Network Computing) utilizando Finder u otra aplicación como Chicken VNC. El perito deberá analizar la existencia de este tipo de conexiones o accesos remotos acorde a la aplicación utilizada para efectuar el acceso al escritorio remoto.

1. En la estación de trabajo de Informática forense de Macintosh, en la imagen recolectada (imagen_Mac_dubitada.dmg), en el directorio de inicio del usuario abrir la carpeta:

~/Library/Application Support/Screen Sharing

2. Editar con el editor de lista de propiedad el archivo vncloc.plist.

3. Identificar la dirección utilizada para el escritorio remoto.

4. Registrar, documentar y/o capturar pantallas con la información requerida.

Procedimiento para el análisis de la aplicación volver a mi Mac (Back to My Mac)

Consideraciones previas

La funcionalidad de Volver a mi Mac le permite al usuario conectarse a su computadora Macintosh previamente registrada al servicio de Internet (.Mac, MobileMe, iCloud), por medio de un escritorio remoto o para compartir archivos en una red local o desde Internet; en este caso, la opción de Volver a mi Mac debe estar habilitada. El usuario debe ingresar un nombre y contraseña para obtener el acceso.

1. En la estación de trabajo de Informática forense de Macintosh, en la imagen recolectada (imagen_Mac_dubitada.dmg), verificar el nombre de usuario para la conexión al servicio de Volver a mi Mac.

2. Editar con un editor de lista de propiedad el archivo:

/Library/Preferences/SystemConfiguration/preferences.plist

3. En el archivo de propiedad verificar la clave:

Root:System:Network:BackToMyMac

a. Identificar el valor de la clave que aparece como: username.members.mac.com

b. Verificar la cuenta .Mac.

4. Registrar, documentar y/o capturar pantallas con la información requerida.

115 http://dubeiko.com/development/FileSystems/HFSPLUS/tn1150.html#HFSPlusBasics junio 2012.

116 Arellano, Luis y Darahuge, María Elena, Manual de Informática Forense, Ed. Errepar, Buenos Aires, 2011.

117 http://es.wikipedia.org/wiki/PowerPC_G4 mayo 2012.

118 http://appleexaminer.com/MacsAndOS/Recommendations/Software/Software.html

119 Arellano, Luis y Darahuge, María Elena, Manual de Informática Forense, Ed. Errepar, Buenos Aires, 2011.

120 http://support.apple.com/kb/HT1661 mayo 2012.

121 http://es.wikipedia.org/wiki/Tabla_de_particiones_GUID mayo 2012.

122 Arellano, Luis y Darahuge, María Elena, Manual de Informática Forense, Ed. Errepar, Buenos Aires, 2011. El comando dd permite realizar la imagen sin comprimir y duplicando bit a bit el original. La ausencia de compresión resulta en un archivo de imagen idéntico en tamaño al original. El comando dd está incluido en el sistema operativo Mac OS X desde la versión 10.0 a 10.5. La imagen obtenida puede ser leída por diferentes tipos de software, comercial, de libre disponibilidad o de código abierto. Otros comandos semejantes a dd de código abierto que se pueden utilizar son: dcfldd y dc3dd.

123 http://es.wikipedia.org/wiki/Extensible_Firmware_Interface junio 2012.

124 http://es.wikipedia.org/wiki/Extensible_Firmware_Interface"

125 http://appleexaminer.com/MacsAndOS/Img_Pwds/DateTime/DateTime.html junio 2012

126 Arellano, Luis y Darahuge, María Elena, Manual de Informática Forense, Ed. Errepar, Buenos Aires, 2011.

127 http://docs.info.apple.com/article.html?path=Mac/10.4/es/mh1877.html mayo 2012.

128 http://en.wikipedia.org/wiki/Time_Machine_%28Mac_OS%29 mayo 2012.

129 DMG es un formato de archivo que Apple utiliza para facilitar la distribución de archivos. Es un disco virtual que actúa tal como si fuera un disco real. Se puede montar en el escritorio, copiar archivos y expulsar el dispositivo cuando ya no se requiere su uso. La forma actual de un archivo de imagen de disco está compuesta por una serie de archivos o bandas y se denomina sparsebundle, puede funcionar como un disco individual en el escritorio del usuario. La Utilidad de Disco (Disk Utility) se emplea para crear y personalizar diferentes tipos de archivos de imagen de disco.

130 Si el perito decide utilizar un dispositivo externo con la estructura del sistema de archivo FAT32, la información recolectada será diferente. Solución: Si se requiere acceder a la información recolectada con el formato HPF+ en un sistema operativo Windows, se puede realizar una segunda copia en el laboratorio del dispositivo externo con HPF+ a un volumen con FAT32 y evaluar los cambios; otra opción es utilizar la herramienta comercial para computadoras con sistema operativo Windows, que permite visualizar los archivos y discos de Mac, denominada MacDrive7 de Mediafour; descarga disponible para prueba durante 5 días (http://www.mediafour.com/products/ macdrive/standard/).

131 http://www.theage.com.au/news/security/hack-into-a-windows-pc--no-password-needed/2008/03/04/1204402423638.html mayo 2012.

132 http://www.mcgrewsecurity.com/tools/msramdmp/mayo 2012.

133 http://es.wikipedia.org/wiki/Tabla_de_particiones_GUID mayo 2012.

134 http://www.mcgrewsecurity.com/tools/msramdmp/mayo2012

135 Ver "Procedimiento para el análisis del sistema de archivos de las imágenes montadas en Linux – Recuperación de archivos fragmentados".

136 Cavanaugh, Sean, http://www.appleexaminer.com/MacsAndOS/AppleApps/SafariFileViewer/SafariFileViewer.html junio 2012.

137 Arellano, Luis y Darahuge, María Elena, Manual de Informática Forense, Ed. Errepar, Buenos Aires, 2011.

CAPÍTULO 10
ANDROID

Consideraciones previas

Los teléfonos inteligentes son los tipos de teléfonos más comunes de Android. Los dispositivos Tablet, que incluyen hardware, software, redes móviles y aplicaciones también utilizan Android, por ejemplo, Tablet de Samsung Galaxy Tab. Otros dispositivos del mercado incorporan Android en: Netbooks, con el sistema operativo de código abierto Chromium, Televisión Google, vehículos que incluyen dispositivos Android para la ubicación geográfica o entretenimiento, sistemas de posicionamiento global o GPS, dispositivos hogareños (lavarropas, microondas), libros electrónicos (Barnes y Noble Nook), reproductores de multimedia, fotocopiadoras, consolas de juegos, impresoras, entre otros.

Componentes de hardware de los celulares Android

· CPU, del tipo ARM (Advanced RISC Machines) de la compañía ARM. Holdings, la arquitectura es del tipo RISC (Reduced Instruction Set Computer Conjunto de Instrucciones de Computadora Reducido).

· Módem y radio, de banda base. Hardware y software que permiten la conexión a la red celular y la transmisión de voz y datos.

· Memoria volátil RAM.

· Memoria no volátil Flash NAND.

· Sistema de Posicionamiento Global GPS.

· Redes inalámbricas, tipo Wi-Fi.com y Bluetooth.

· Memoria removible: Tarjeta Digital Segura (SD).

· Pantalla táctil.

· Cámara.

· Teclado por pantalla.

· Batería.

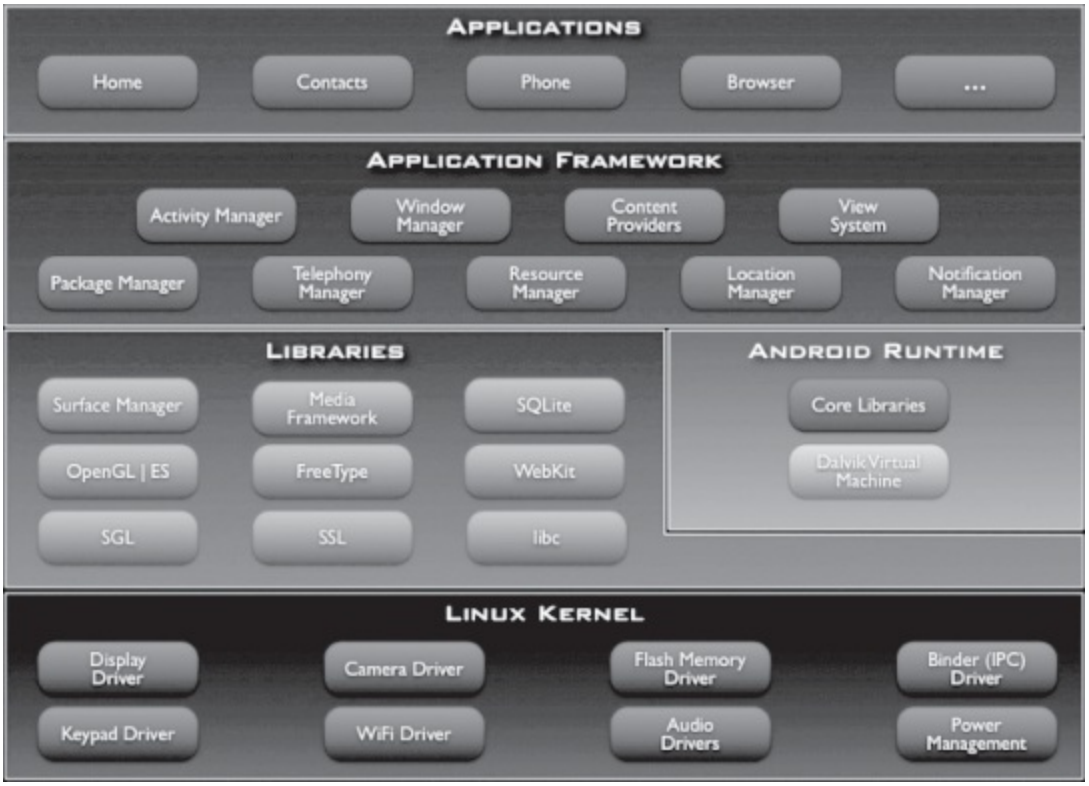
· Conector universal serial bus (USB).

· Medidor de aceleración y giroscopio, detecta y cambia la interfaz del usuario basándose en movimientos y rotaciones acordes a la forma en que es sostenido el celular.

· Parlantes y micrófono.

Componentes de software de los celulares Android

Android es un conjunto de capas o una pila de software para dispositivos móviles que incluye un sistema operativo, middleware y aplicaciones.



· Las aplicaciones incluyen cliente de correo electrónico, programas SMS, calendario, mapas, navegador de Internet, contactos, etc. Las aplicaciones son escritas en el lenguaje de programación Java.

· La infraestructura digital o framework ofrece una plataforma abierta de desarrollo que les permite a los programadores construir aplicaciones innovadoras, tomando ventaja de: los dispositivos de hardware, el acceso a la información local, la ejecución de servicios en segundo plano, la configuración de alarmas, las notificaciones en la barra de estado, entre otras capacidades. Los programadores tienen acceso completo al mismo API que utilizan las aplicaciones del sistema. La arquitectura de la aplicación está diseñada para simplificar la reutilización de los componentes, cualquier aplicación puede publicar sus capacidades y cualquier otra aplicación puede hacer uso de dichas capacidades bajo determinadas restricciones de seguridad dentro de la infraestructura de desarrollo. Este mismo mecanismo permite a los usuarios reemplazar los componentes.

· Librerías: Android incluye una serie de librerías de C y C++. Las principales son:

- System C (libc de BSD), ajustada para dispositivos con Linux incorporado.
- Multimedia, basada en OpenCore, soportan grabación y reproducción,

manejo de diferentes formatos de audio y video, imágenes estáticas (MPEG4, H.264, MP3, AAC, AMR, JPG y PNG).

- Gestor de acceso al subsistema de las pantallas y a las capas gráficas de 2D y 3D.
- LibwebCore, motor de navegación web que optimiza el navegador de Android y el visor web embebido.
- SGL, motor gráfico subyacente de 2D.
- 3D, una implementación de interfaces de programación basada en OPENGL ES 1.0; utilizan tanto el hardware acelerador de 3D, si está disponible, o el software 3D incluido y altamente optimizado.
- FreeType, gestor de tipos de letras bitmap y vector para el proceso de crear fuentes (render).
- SQLite, motor de base de datos relacional disponible para todas las aplicaciones, no requiere servidor para acceder a las bases de datos.

· La máquina virtual Dalvik VM[138] ejecuta las aplicaciones sobre el sistema operativo de los dispositivos Android y fue escrita de forma tal que un dispositivo Android pueda ejecutar múltiples máquinas virtuales de manera eficiente. Los programas son escritos en Java y compilados a un código intermedio entre el código fuente y el lenguaje de máquina (Bytecode).

· La máquina virtual Dalvik utiliza su propio conjunto de instrucciones de 16 bits que trabaja directamente sobre las variables locales. Generalmente, las variables locales eligen un registro virtual de 4 bits. La reducción del tamaño de instrucción aumenta la velocidad de su intérprete. Cada aplicación de Android ejecuta su propio proceso con su propia instancia en la máquina virtual Dalvik.

· Los archivos son ejecutados en el formato ".dex", el cual minimiza el uso de memoria y el del microprocesador. La máquina virtual está basada en registros y ejecuta clases compiladas por el compilador del lenguaje Java que fueron transformados en el formato ".dex", por una herramienta incluida en la máquina virtual denominada "dx". Dalvik VM se encuentra por sobre el sistema operativo Linux y este último se encarga de las funciones subyacentes como son los procesos hilos (thread) y el manejo de memoria de bajo nivel.

· Android está basado en el núcleo o kernel del sistema operativo Linux de la versión 2.6 y le confía la gestión de memoria, de procesos, de la pila de protocolos de red y del modelo del dispositivo. El núcleo o kernel actúa como una capa de abstracción entre el hardware y el resto de la pila de software.

· El modelo de seguridad de Android es efectivo en la restricción de los accesos a los datos de las aplicaciones. Características del modelo:

- A cada aplicación se le asigna un único usuario y grupo de Linux.

- Las aplicaciones se ejecutan utilizando su identificador único en un proceso dedicado dentro de la máquina virtual.
- Cada una de las aplicaciones tiene un espacio de almacenamiento dedicado en /data/data que solo puede ser accedido por la aplicación.

No obstante, la infraestructura digital de Android brinda mecanismos para que las aplicaciones puedan compartir datos. Por ejemplo, un desarrollador puede incluir soporte para proveedores de contenido dentro de la aplicación, permitiéndole compartir datos con otras aplicaciones. El programador controla qué datos serán expuestos a otras aplicaciones. Durante la instalación de una aplicación, un usuario puede controlar si permitirá o no que una aplicación tenga acceso a un proveedor de contenido (SMS/MMS, contactos, calendario, Facebook, Gmail).

Estructura del sistema de archivos en Android

El sistema de archivo YAFFS2 (Yet Another Flash File System)[139] es reciente y usado ampliamente en los dispositivos Android. Fue diseñado específicamente para la memoria Flash NAND, soporta enlaces duros, simbólicos y tuberías.

En el sitio de Via Forensics (https://viaforensics.com/products/tools/sleuth-kit-yaffs2/), el perito puede descargar las imágenes del sistema de archivo para analizar en el laboratorio y efectuar pruebas específicas para profundizar los conocimientos en este sistema de archivo. Las imágenes son para los siguientes modelos de dispositivos: Droid Eris, Google Nexus One, HTC Aria, HTC G1, HTC Hero, HTC MyTouch 3G, LG Optimus S, Motorola Droid, Sony Xperia Play, Sony Xperia X10.

La organización de los datos en la estructura física de una memoria Flash NAND es manejada por el dispositivo de tecnología de memoria MTD (Memory Technology Device). La organización es en 128 bloques, que consiste en fragmentos de 2048 bytes de datos seguidos de 64 bytes de datos de reserva u OOB (Out Of Band) utilizados para guardar metadatos del disco y del sistema de archivo. Los grupos de fragmentos se combinan para formar un bloque borrado, generalmente de 64 fragmentos. Los fragmentos pueden tener datos o un encabezado. El encabezado contiene información sobre el nombre del archivo, tamaño, fecha y hora de creación, identificador del padre. La información de los fragmentos también se guarda en el espacio de reserva. La combinación de la información del espacio de reseva y el encabezado son necesarios para reconstruir la estructura de archivos y directorios.

Datos – Fragmentos – Páginas (2048 bytes) Reserva u OOB (64 bytes)

Id	Id	Byte	Nro de	ECC	Bloque	Datos

Fragmento	Encabezado		secuencia			
4 bytes (si es 0 es entrada de directorio, si es > 1 es dato y posición)	4 bytes (0 si no se utiliza)	Número de bytes 2n, utilizados por el fragmento. 2048=Lleno	4 bytes	3 bytes Código de Corrección de Errores para etiquetas (tags) 24 bytes Código de Corrección de Errores de datos	1 byte Estado del bloque (dañado)	1 byte Estado de los datos (dirty inválido)

Estructura del encabezado (entrada de directorio)

Identificador del Objeto	Entero
Checksum	2 bytes
Nombre de archivo	255 bytes
Modo: protección, directorio, archivo, enlace simbólico	4 bytes
Identificador del usuario propietario	4 bytes
Identificador del grupo propietario	4 bytes
Fecha y hora de acceso atime	4 bytes
Fecha y hora de última modificación de datos mtime	4 bytes
Fecha y hora de último cambio ctime	4 bytes
Tamaño de archivo filesize	Entero, si es del tipo little endian, convertir a hexadecimal o decimal, cero si es carpeta
Equivalente a identificador de objeto para enlaces duros Alias, si es un enlace simbólico o acceso directo	Entero

La estructura de archivos se puede visualizar en el archivo mtd del directorio /proc y puede ser la siguiente, dependiendo del fabricante:

mtd0: 00040000 00020000 “misc” misceláneas

mtd1: 00500000 00020000 “recovery” recuperación mtd2: 00280000 00020000 “boot” inicio o arranque mtd3: 04380000 00020000 “system” datos del sistema mtd4: 04380000 00020000 “caché”

mtd5: 04ac0000 00020000 “userdata” datos del usuario

El área de reserva OOB puede ser un problema al momento de montar el sistema de archivo YAFFS2 para su análisis y para el uso de herramientas de análisis de fragmentos. Se pueden utilizar herramientas para remover los espacios de reserva o un simple programa[140].

En la computadora de Informática forense con el sistema operativo Linux, instalar una máquina virtual (Virtual Box, VMWare, etc.) con el sistema operativo Linux. Acorde al sistema operativo Linux instalado, el perito deberá asegurarse de que la configuración de montaje automático de dispositivos se encuentre deshabilitada.

El paquete de herramientas de desarrollo de Android contiene aplicaciones de utilidad para la recolección y análisis forense de los dispositivos, como así también el propio sistema operativo Linux sobre el cual funciona Android. En la computadora de Informática forense es recomendable que el perito instale el paquete de herramientas de desarrollo de Android (http:// developer.android.com/sdk/index.html).

En el laboratorio, el perito podrá practicar el uso de las herramientas de recolección y análisis que se encuentran en el paquete de desarrollo y luego crear un emulador de un dispositivo Android (http://developer.android.com/guide/developing/devices/emulator.html).

Los dispositivos Android contienen gran cantidad de información para recolectar y analizar, a saber:

- Mensajes de texto (SMS-MMS)
- Contactos
- Registros de llamadas
- Mensajes de correo electrónico
- Mensajería instantánea
- Coordenadas de GPS
- Fotografías y videos
- Historial web
- Historial de búsquedas web
- Directivas de manejo o conducción
- Redes sociales: Facebook, Twitter, etc.
- Archivos guardados en el dispositivo
- Música

· Citas en la agenda
· Información financiera
· Información de comercio electrónico
· Historial de compras en línea
· Archivos compartidos

Las aplicaciones en Android se pueden guardar en forma interna o externa. El almacenamiento externo se realiza en la tarjeta SD (Secure Digital) o tarjetas SD emuladas. El almacenamiento interno es controlado por las aplicaciones de Android. Al instalarse una aplicación ya sea descargada del sitio de Android o incorporada de fábrica, se guarda internamente información en el subdirectorio /data/data con el nombre de la aplicación a continuación del nombre del paquete (com.android.browser). Dentro del directorio /data/data existe un número de directorios estándar que se encuentran en varias aplicaciones, como así también los directorios de control de los desarrolladores de aplicaciones (lib/files/cache/databases).

El sistema Android provee a los desarrolladores de cinco métodos para almacenar los datos en el dispositivo, esto es muy importante para los peritos en las etapas de recolección y análisis de los datos. Los datos no volátiles se guardan tanto en la tarjeta SD como en la memoria Flash NAND o en la red (cloud). Los métodos son:

· Preferencias compartidas: Permite al desarrollador guardar pares de claves de tipos de datos primitivos en formato XML (variables booleanas, verdadero-falso, puntos flotantes, enteros, cadena de caracteres en UTF-8, etc.).

· Almacenamiento interno: Datos de estructuras más complejas de los desarrolladores se guardan en subdirectorios en /data/data, que les permiten controlar el tipo de archivo, nombre y ubicación. Son todos aquellos archivos que no están en lib, caché, databases o shared_prefs. Las aplicaciones utilizan el directorio app_ y files para guardar datos. El directorio app_ contiene varios subdirectorios y archivos de formato desconocido (cach_r.m).

· Almacenamiento externo: En la tarjeta SD con la estructura de archivo FAT32, para facilitar su montaje y lectura.

· SQLite: Gestor de base de datos.

· Red, documentación de los desarrolladores que utilizan paquetes como java.net, android.net. Por ejemplo, el sitio web Dropbox para compartir aplicaciones para Android, BlackBerry y dispositivos con sistema operativo iOS.

El perito podrá encontrar otra área de análisis en el sistema operativo estándar de Linux: Archivos de registro de eventos del núcleo o kernel del sistema operativo, inicio y depuración del sistema. El núcleo de Linux es la

capa de abstracción de bajo nivel que le permite tener acceso al hardware del dispositivo. La función del núcleo es fundamental en el desempeño del dispositivo Android y por lo tanto el perito debe verificar a través del comando dmesg las actividades del núcleo del sistema operativo.

Tipos de memoria en los dispositivos Android

El dispositivo Android posee dos memorias RAM volátil y Flash NAND no volátil. La memoria RAM se utiliza para cargar, ejecutar y manejar las partes importantes del sistema operativo, las aplicaciones o datos (claves, claves cifradas, nombres de usuario, datos de aplicaciones, datos de procesos y servicios).

La memoria Flash NAND es utilizada para guardar sistemas de archivos, datos del usuario.

sistemas de archivos

Los sistemas de archivos que soporta Android son:

$cat /proc/filesystems

nodev sysfs

nodev rootfs, donde se monta el sistema de archivo / nodev bdev

nodev proc, información de procesos, es el núcleo del sistema operativo

nodev cgroup nodev binfmt_misc nodev sockfs nodev pipefs

nodev anon_inodefs

nodev tmpfs, archivos de memoria virtual intercambiados por la RAM nodev inotifyfs

nodev devpts

ext3, sistema de archivo de Linux nodev ramfs

vfat, partición de Microsoft en las tarjetas SD y eMMC msdos

nodev nfsd nodev smbfs yaffs

yaffs2, para dispositivos Android nodev rpc_pipefs

Los sistemas de archivos nodev, que son sistemas de archivos virtuales y no se encuentran físicamente en ningún dispositivo de almacenamiento secundario –que son los que utiliza el dispositivo Android–, se encuentran resaltados en negrita.

El sistema de archivo virtual /sys contiene archivos de control y configuración del dispositivo:

$ls -l /sys

drwxr-xr-x root root 2012-06-24 23:40 block

drwxr-xr-x root root 2012-06-25 02:05 bus

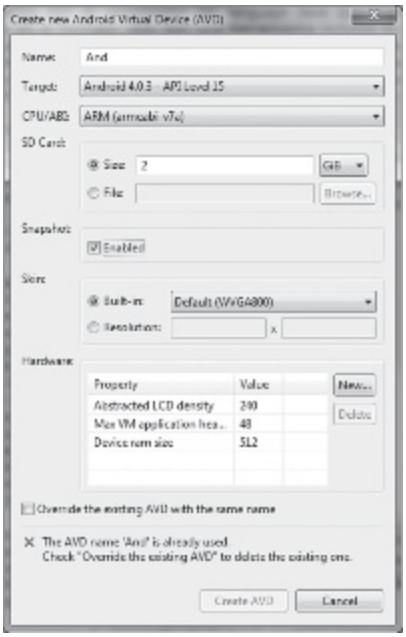
drwxr-xr-x root root 2012-06-24 23:40 class
drwxr-xr-x root root 2012-06-25 02:05 dev
drwxr-xr-x root root 2012-06-24 23:40 devices
drwxr-xr-x root root 2012-06-25 02:05 firmware
drwxr-xr-x root root 2012-06-25 02:05 fs
drwxr-xr-x root root 2012-06-24 23:40 kernel
drwxr-xr-x root root 2012-06-24 23:40 module
drwxr-xr-x root root 2012-06-24 23:40 power
drwxr-xr-x root root 2012-06-24 23:40 qemu_trace

Procedimiento para crear un emulador de un dispositivo Android

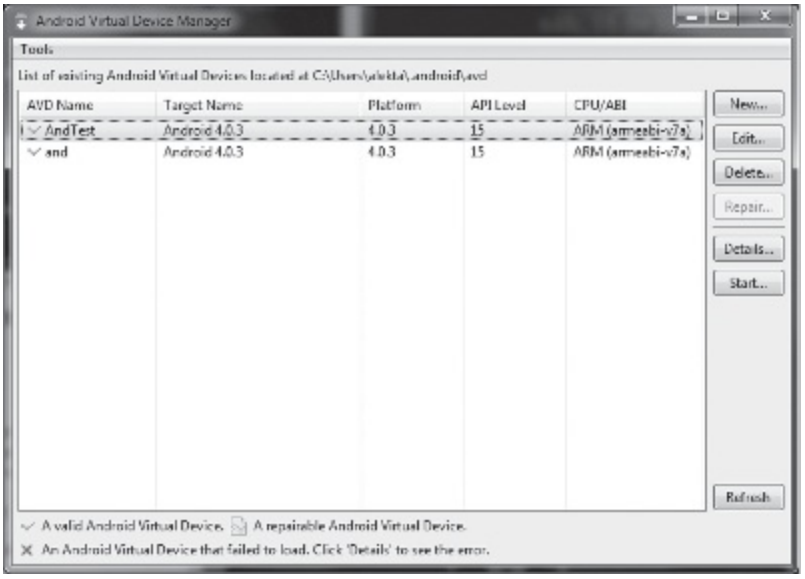
1. Descargar del sitio http://developer.android.com/sdk/index.html el archivo comprimido correspondiente al sistema operativo de la estación de trabajo de Informática forense.
2. Descomprimir e instalar el paquete de desarrollo (ver guía de instalación en http:// developer.android.com/sdk/installing.html).
3. Ejecutar el programa SDK Manager y completar la descarga de los archivos que corresponda, según la guía de instalación.
4. Ejecutar el programa gestor de dispositivos virtuales de Android (Android Virtual Device Manager).

a. Agregar un dispositivo virtual, seleccionar la opción Nuevo (New) y completar la información solicitada: (Nombre, Tipo de dispositivo, Microprocesador o CPU, Tamaño de la tarjeta SD, Habilitar captura instantánea, Tipo de tapiz, Configuración de Hardware –seleccionar las opciones que aparecen en el menú desplegable–).

b. Oprimir el botón Crear AVD (Create AVD):



c. Iniciar el emulador oprimiendo el botón Iniciar (Start):



5. En una terminal o consola ubicar el directorio de instalación del paquete SDK y verificar con el comando adb la conexión al dispositivo Android creado; el emulador utilizará un puerto al cual se conectará:

Ejemplo:

C:\Program Files (x86)\Android\android-sdk\platform-tools>adb.exe devices List of devices attached emulator-5554 device

Etapa de recolección y adquisición de datos

Procedimiento para la duplicación de los dispositivos USB de almacenamiento (UMS USB

Mass Storage) en dispositivos Android

Consideraciones previas

Los dispositivos Android pueden tener una tarjeta digital externa de seguridad (SD Secure Digital) o una tarjeta multimedia embebida (eMMC Embedded MultiMediaCard) que permite almacenar gran cantidad de información para los usuarios. Este almacenamiento existe porque los datos de las aplicaciones del usuario guardados en /data/data están separados por razones de privacidad y seguridad.

La copia de fotos, música, video, archivos de oficina, etc., entre un dispositivo Android y la computadora se realiza a través de la gran capacidad de almacenamiento de las particiones FAT y resulta más flexible para el usuario. Los datos sensibles quedan protegidos y los archivos portables quedan accesibles al usuario. El procedimiento recomendado es efectuar la duplicación sin remover del dispositivo las tarjetas SD y eMMC, utilizando el comando dd (dc3dd, del Departamento de Defensa Centro del Ciber Crimen).

1. Crear una máquina virtual con el sistema operativo Linux.
2. Descargar, descomprimir, compilar e instalar el programa dc3dd:

#mkidr -p /src cd /src

curl http://sourceforge.net/projects/dc3dd/files/dc3dd/7.1.0/dc3dd-7.1.614.tar.gz/ >

dc3dd-7

tar xzf dc3dd-7.1.614.tar.gz cd dc3dd-7.1.6.1.4

./configure make

make install

4. Desactivar la configuración de auto montaje de los dispositivos.
5. Conectar el bloqueador de escritura por hardware a la computadora de Informática forense y conectar el dispositivo móvil con Android al bloqueador de escritura.
6. Determinar los dispositivos de almacenamiento o interfaces USB que son reconocidos por el sistema operativo:

#dmesg

La información mostrada en el registro del kernel o núcleo es la siguiente: en el caso de teléfono inteligente (Smartphone, de la empresa de Taiwán HTC[141] High Tech Computer Corporation Incredible[142]) muestra tres interfaces USB:

- CD-ROM para instalación de dispositivos (sr1).
- eMMC dispositivo UMS (sdb).
- Tarjeta SD y dispositivo UMS (sdc).

Para diferenciar con claridad los dispositivos /dev/sdb y /dev/sdc es necesario habilitar la funcionalidad UMS del dispositivo con Android.

7. Ejecutar nuevamente el comando dmesg:

#dmesg

El resultado mostrará la diferencia en los dispositivos de almacenamiento: /dev/sdb es de 8GB, es decir la eMMC, y la de 2GB es la tarjeta SD en /dev/sdc.

8. Adquirir la imagen del dispositivo, a través de un script[143], o utilizando el comando dd[144] o el comando dc3dd.

#dc3dd if=/dev/sdb progress=on hashconv=after hash=md5,sha1 hashwindow=2GB splitformat=000 split=2GBlog=/tmp/resgistro_eMMC.txt bs=512 iflag=direct conv= noerror,sync of=/tmp/imagen_android_eMMC.dd

#dc3dd if=/dev/sdb progress=on hashconv=after hash=md5,sha1 hashwindow=2GB splitformat=000 split=2GBlog=/tmp/registro_SD.txt bs=512 iflag=direct conv=noerror,sync of=/tmp/imagen_android_SD.dd

El comando efectúa: Múltiples archivos de 2 GB.

Hash MD5 y SHA1 de la imagen. Crea un archivo de registro (log).

El perito podrá modificar los parámetros acorde al dispositivo.

En el caso de que las aplicaciones (apps) se encuentren instaladas en la tarjeta SD, los datos estarán encriptados y no se podrán leer; no obstante, si la tarjeta no está montada en la computadora de Informática forense, los archivos desencriptados .apk se montan en /mnt/sec. Si se deben analizar los archivos .app y .apk, el perito tendrá que realizar una copia de cada uno de ellos.

9. Registrar, documentar y/o capturar pantallas con la información requerida.

Procedimiento para la recolección lógica de datos en dispositivos Android

Consideraciones previas

Las técnicas de recolección lógica extraen la información que se encuentra almacenada o asignada. La forma de obtenerla es accediendo al sistema de archivos y le ofrecen al perito no solo facilidad para la recolección de los datos, sino que también obtiene una cantidad de información considerable para la posterior etapa de análisis acorde a la requisitoria pericial.

La recolección lógica en Android no requiere el acceso al dispositivo como usuario root. La opción de Depuración USB (USB Debugging) se utiliza con fines de desarrollo para copiar datos entre la computadora y el dispositivo, instalar aplicaciones en el dispositivo sin preguntar y para ver los registros de

eventos, por lo tanto debe estar habilitada:

En el dispositivo Android: Seleccionar Menu, Configuraciones, Opciones de Desarrollo, seleccionar la casilla de verificación para habilitarlo. Aparecerá un mensaje de advertencia y presionar Aceptar.

Para la extracción lógica de datos se pueden utilizar diferentes técnicas:

I. Comando adb

Es una herramienta del paquete de desarrollo de Android (http://developer.android.com/ guide/developing/tools/adb.html) con Licencia Pública General (GNU GPL General Public License) de línea de comando que permite comunicarse con una instancia del emulador de Android o con el dispositivo directamente; es una aplicación del tipo cliente servidor.

La herramienta obtiene información de manera recursiva del dispositivo y la copia en la estación de trabajo de Informática forense. Si se tiene acceso al dispositivo Android como usuario root o se está ejecutando una ROM personalizada, el servicio que se ejecuta de adb en el dispositivo solo funciona con permisos del intérprete de comandos o Shell, por lo que la información relevante no se puede recolectar.

No obstante, se puede acceder a otros archivos. Si se intenta copiar archivos de los cuales el usuario del Shell no tiene permisos, simplemente no se copiarán. Esta herramienta es recomendada por Andrew Hoog[145] como una de las primeras a utilizar en la recolección lógica.

1. Copiar los archivos desde el dispositivo con el comando adb, en el caso de poseer los privilegios suficientes para el acceso desde el Shell.

$adb pull /data adbpull/

Ejemplo del resultado obtenido en un emulador de Android: pull: building file list...

skipping special file ‘0’ pull: /data/backup/pending/journal-532901293.tmp -> adbpull/backup/pending/ journal-532901293.tmp

pull: /data/system/inputmethod/subtypes.xml -> adbpull/system/inputmethod/ subtypes.xml

pull: /data/system/sync/accounts.xml -> adbpull/system/sync/accounts.xml pull: /data/system/sync/status.bin -> adbpull/system/sync/status.bin

pull: /data/system/sync/pending.bin -> adbpull/system/sync/pending.bin pull: /data/system/sync/stats.bin -> adbpull/system/sync/stats.bin

pull: /data/system/registered_services/android.accounts.AccountAuthenticator.xm ->

adbpull/system/registered_services/android.accounts.AccountAuthenticator.x
pull: /data/system/registered_services/android.content.SyncAdapter.xml -> adbpull/
system/registered_services/android.content.SyncAdapter.xml
pull: /data/system/users/userlist.xml -> adbpull/system/users/userlist.xml pull: /data/system/users/0.xml -> adbpull/system/users/0.xml
pull: /data/system/usagestats/usage-20120616 -> adbpull/system/usagestats/ usage-20120616
pull: /data/system/entropy.dat -> adbpull/system/entropy.dat
pull: /data/system/batterystats.bin -> adbpull/system/batterystats.bin pull: /data/system/uiderrors.txt -> adbpull/system/uiderrors.txt
pull: /data/system/packages.xml -> adbpull/system/packages.xml pull: /data/system/packages.list -> adbpull/system/packages.list
pull: /data/system/packages-stopped.xml -> adbpull/system/packages-stopped.xml pull: /data/system/accounts.db -> adbpull/system/accounts.db
pull: /data/system/accounts.db-journal -> adbpull/system/accounts.db-journal pull: /data/property/persist.sys.profiler_ms -> adbpull/property/persist.sys.
profiler_ms
pull: /data/data/com.android.providers.settings/databases/settings.db -> adbpull
/data/com.android.providers.settings/databases/settings.db
pull: /data/data/com.android.providers.settings/databases/settings.db-wal -> adb pull/data/com.android.providers.settings/databases/settings.db-wal
pull: /data/data/com.android.providers.settings/databases/settings.db-shm -> adb pull/data/com.android.providers.settings/databases/settings.db-shm
pull: /data/data/com.android.providers.contacts/databases/profile.db -> adbpull/ data/com.android.providers.contacts/databases/profile.db
pull:
/data/data/com.android.providers.contacts/shared_prefs/ContactsUpgrade Receiver.xml -> adbpull/data/com.android.providers.contacts/shared_prefs/ ContactsUpgradeReceiver.xml
pull: /data/misc/wifi/softap.conf -> adbpull/misc/wifi/softap.conf 26 files pulled. 0 files skipped.
75 KB/s (144110 bytes in 1.876s)

En este caso, todos los datos de la partición /data se copiarán al directorio local de la estación de trabajo de Informática forense (adbpull). El perito podrá explorar los archivos en este directorio:

16/06/2012 04:28 p.m. <DIR> .

16/06/2012 04:28 p.m. <DIR> ...

16/06/2012 04:28 p.m. <DIR> backup

16/06/2012 04:28 p.m. <DIR> data

16/06/2012 04:28 p.m. <DIR> misc

16/06/2012 04:28 p.m. <DIR> property 16/06/2012 04:28 p.m. <DIR> system

Ejemplo del contenido del directorio /data: 16/06/2012 04:28 p.m. <DIR> .

16/06/2012 04:28 p.m. <DIR> ...

16/06/2012 04:28 p.m. <DIR> com.android.providers.contacts 16/06/2012 04:28 p.m. <DIR> com.android.providers.settings

La ejecución del comando puede detenerse cuando encuentra que no tiene los permisos de copia de los archivos; por lo tanto, para evitar repetidas detenciones del programa es conveniente realizar la obtención de datos de los directorios por parte y no de una sola vez. Si bien no es frecuente que se pueda acceder como root en la mayoría de los dispositivos, adb es una herramienta muy efectiva para utilizar en diferentes situaciones:

- Si no se tienen permisos de root, se puede acceder a ciertos archivos de importancia como aplicaciones no encriptadas, a la mayor parte del directorio /tempfs que puede contener datos de usuario (historial del navegador web) e información del sistema en los directorios /proc, /sys y otros directorios que tengan acceso de lectura.

2. Registrar, documentar y/o capturar pantallas con la información requerida.

II. Resguardos

Una herramienta muy difundida para realizar resguardos o backup es RerWare My Backup Pro (http://www.rerware.com/Android-Backup/default.aspx): Resguarda los datos utilizando el proveedor de contenidos y el directorio /data/data, en el caso de que el dispositivo tenga permisos de acceso de root. Esta aplicación funciona también en Windows Mobile, Blackberry y Symbian OS. Las opciones que tiene el usuario para realizar resguardos es guardar la información en la tarjeta SD y en el servidor de RerWare. La herramienta efectúa el resguardo en forma local en la tarjeta SD en un único archivo de SQLite. La aplicación puede resguardar:

- Archivos de instalación de aplicaciones (si el teléfono tiene acceso de usuario root, incluye APK, data y Enlaces de comercios o tiendas [Market Links]).
- Contactos

- Registro de llamadas
- Marcadores del navegador web
- SMS (mensajes de texto)
- MMS (adjuntos en mensajes)
- Configuraciones del sistema
- Pantallas de inicio
- Alarmas
- Diccionario
- Calendarios
- Listas de reproducción de música
- Aplicaciones de terceros integradas

Android recientemente ha desarrollado una aplicación de manejo de resguardos[146] que se integra al resto de las aplicaciones; el resguardo es manejado por Android y Google. Esto permite al usuario un resguardo continuo de sus aplicaciones guardándolo en la red (cloud) en un servidor de almacenamiento remoto, con el fin de ofrecerle a un usuario un punto de restauración en el caso de que cambie de dispositivo o pérdida de datos.

El perito deberá conocer qué tipos de resguardos existen para luego analizar el contenido de la tarjeta SD, como así también, si es posible, la computadora o notebook del usuario.

III. Herramienta AFLogical

La herramienta AFLogical se distribuye en forma libre para los organismos de gobierno y seguridad, previo registro e identificación en el sitio de la herramienta (https://viaforensics. com/products/android-forensics-tool/).

La aplicación está desarrollada por Viaforensics y utiliza las mismas técnicas que los productos comerciales de telefonía forense. El programa permite extraer la información almacenada y compartida de los proveedores de contenido (SMS/MMS, contactos, calendario, Facebook, Gmail, etc.). AFLogical aprovecha la arquitectura de los proveedores de contenido para acceder a los datos almacenados en el dispositivo.

Se debe habilitar la opción de Depuración de USB para utilizar la herramienta AFLogical para la extracción de datos. El formato del resguardo es en CSV (Valor Separado por Comas

- Comma Separated Value) y un archivo info.xml, el cual brinda información detallada del dispositivo y de las aplicaciones instaladas. La herramienta puede resguardar los siguientes proveedores de contenidos:

- Marcadores del navegador web
- Búsquedas en el navegador web

- Calendarios
- Asistente del calendario
- Eventos del calendario
- Propiedades extendidas del calendario
- Recordatorios del calendario
- Registro de llamadas
- Contactos
- Extensiones de contactos
- Grupos de contactos
- Organizaciones de contactos
- Teléfonos de contactos
- Configuración de contactos
- Discos externos (imágenes, previsualizaciones, videos)
- Mensajería instantánea (cuentas, charlas, mensajes, invitaciones, proveedores, configuración de los proveedores en la mensajería instantánea)
- Almacenamiento interno (imágenes, previsualizaciones, videos)
- Mapas (amigos, extra, contactos)
- MMS
- Notas
- Gente eliminada
- Almacenamiento de teléfono
- Historial de búsquedas
- SMS
- Charlas de mensajería instantánea
- Actividades sociales

Procedimiento para la recolección lógica de datos con AFLogical

1. En la estación de trabajo de telefonía forense, descargar la aplicación AFLogical del sitio Viaforensics o la edición de código abierto aflogical_ose (Edición de Código Abierto Open Source Edition) que se descarga del sitio:

   http://code.google.com/p/android-forensics/downloads/list

2. En el dispositivo Android retirar la tarjeta SD del usuario (la aplicación efectúa escrituras en la tarjeta SD):

   a. Activar Depuración USB.

   b. Insertar una tarjeta SD preparada para la recolección de datos.

3. Conectar el dispositivo Android a la estación de trabajo de telefonía

forense.

4. Abrir una consola de terminal y verificar si el dispositivo es reconocido:

$adb devices

5. Instalar en la estación de telefonía forense la aplicación AFLogical.

$adb install AFLogical-OSE_1.5.2.apk

57 KB/s (28794 bytes in 0.493s)

pkg: /data/local/tmp/AFLogical-OSE_1.5.2.apk

Success

6. La aplicación correctamente instalada se puede ejecutar desde el dispositivo Android o desde la línea de comando en la estación de trabajo de telefonía forense.

· Desde la estación de trabajo, ingresando los parámetros para que se ejecute automáticamente:

$adb shell am start

–n com.viaforensics.android/com.viaforensics.android.ExtractAllData

Aparece en la consola:

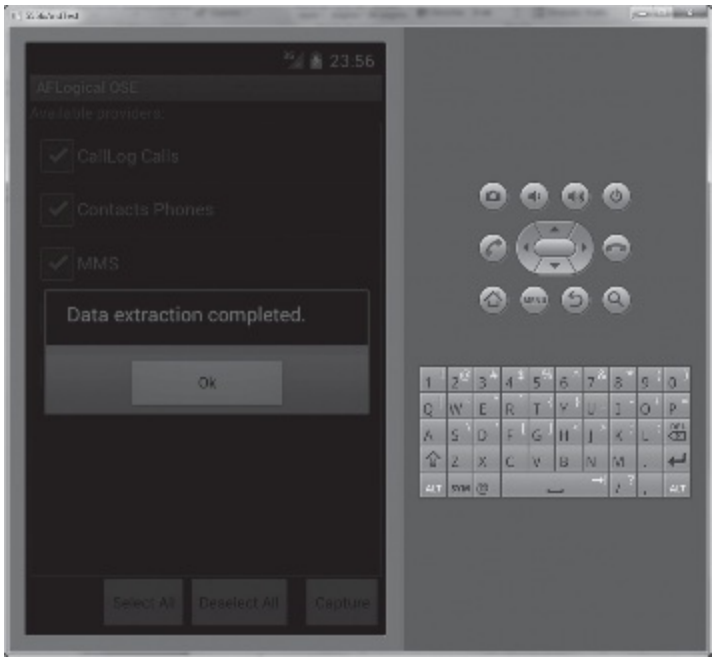
Starting: Intent { cmp=com.viaforensics.android/.ExtractAllData }

· Desde el dispositivo Android:

a. Ir al menú Inicio, Aplicaciones y seleccionar AFLogical OSE.

b. Seleccionar todas las opciones (la lista es limitada en comparación con la aplicación de Viaforensics), oprimir el botón Capturar.

c. Luego de la captura aparecerá la siguiente pantalla de finalización:



Los datos extraídos se guardan en la tarjeta SD del dispositivo en un directorio denominado forensics y en un directorio nombrado después de la fecha en formato YYYYMMDD.HHMM (año, mes, día, horas, minutos).

16/06/2012 11:12 p.m. <DIR> forensics

d. Listar el contenido del directorio forensics: 16/06/2012 11:12 p.m. <DIR> 20120616.2355

e. Listar el contenido del directorio 20120616.2355: 16/06/2012 11:12 p.m. 62 CallLog Calls.csv

16/06/2012 11:12 p.m. 267 Contacts Phones.csv
16/06/2012 11:12 p.m. 46.275 info.xml
16/06/2012 11:12 p.m. 335 MMS.csv
16/06/2012 11:12 p.m. 482 MMSParts.csv
16/06/2012 11:12 p.m. 241 SMS.csv
16/06/2012 11:12 p.m. 22.446 temp.jpg

f. Desde la estación de trabajo de telefonía forense, extraer los datos de la tarjeta SD y enviarlos al directorio AFlogic:

$adb pull /sdcard/ aflogic pull: building file list...
pull: /sdcard/Android/data/com.android.mms/cache/.temp.jpg ->
aflogic/Android/data/com.android.mms/cache/.temp.jpg pull: /sdcard/forensics/20120616.2355/temp.jpg -> aflogic/forensics/20120616.235
5/temp.jpg
pull: /sdcard/forensics/20120616.2355/Contacts Phones.csv -> aflogic/forensics/2
0120616.2355/Contacts Phones.csv
pull: /sdcard/forensics/20120616.2355/SMS.csv -> aflogic/forensics/20120616.2355
/SMS.csv
pull: /sdcard/forensics/20120616.2355/MMSParts.csv -> aflogic/forensics/20120616
.2355/MMSParts.csv
pull: /sdcard/forensics/20120616.2355/MMS.csv
-> aflogic/forensics/20120616.2355
/MMS.csv
pull: /sdcard/forensics/20120616.2355/CallLog Calls.csv -> aflogic/forensics/201
20616.2355/CallLog Calls.csv
pull: /sdcard/forensics/20120616.2355/info.xml -> aflogic/forensics/20120616.235
5/info.xml
8 files pulled. 0 files skipped.
17 KB/s (92554 bytes in 5.022s)

h. Desinstalar AFLogical del dispositivo:

$adb uninstall com.viaforensics.android.aflogical_ose

7. Verificar el contenido del directorio 20120616.2355:

a. Visualizar el contenido de los archivos CSV, con un programa de planilla de cálculo.

16/06/2012 11:12 p.m. 62 CallLog Calls.csv

16/06/2012 11:12 p.m. 267 Contacts Phones.csv

16/06/2012 11:12 p.m. 335 MMS.csv

16/06/2012 11:12 p.m. 482 MMSParts.csv

16/06/2012 11:12 p.m. 241 SMS.csv

b. Visualizar el contenido del archivo info.xml que contiene información sobre: el IMSI (International Mobile Subscriber Identity Identidad Internacional del Abonado a un Móvil), IMEI, versión de Android, proveedor de red, lista de todas las aplicaciones instaladas, con un editor de xml.

16/06/2012 11:12 p.m. 46.275 info.xml

8. Registrar, documentar y/o capturar pantallas con la información requerida.

Productos comerciales para la recolección de datos en Android

- Cellebrite UFED
- Compelson MOBILedit
- EnCase Neutrino
- Micro Systemation XRY
- Paraben Device Seizure
- viaForensics viaExtract
- Oxygen Forensic Suite

Procedimiento para la recolección física de datos

Consideraciones previas

La recolección física permite obtener datos que han sido eliminados e información obsoleta en el sistema de archivos. Las técnicas de recolección física en Android pueden ser por:

- Hardware[147]: Métodos que conectan hardware al dispositivo o físicamente extraen los componentes del dispositivo móvil. El equipamiento requerido y su respectiva capacitación suelen ser muy costosos.

  – La técnica para verificar y probar los cables e interconexiones de los circuitos impresos en la placa (PCB printed circuit board) de celulares o equipos inalámbricos responde al estándar de la IEEE 1149.1 (Standard Test Access Port and BoundaryScan Architecture) denominado JTAG (Joint Test Action Group)[148]. Requiere de conocimientos específicos y solo

se puede realizar en un laboratorio con los instrumentos adecuados y la autorización judicial correspondiente. El estándar efectúa pruebas de acceso a los puertos (TAP Test Access Port) que permiten el ingreso a la unidad central de procesamiento (CPU Central Process Unit). Las señales que se prueban en los dispositivos móviles pueden ser:

❏ TDI (Prueba de Entrada de Datos).

❏ TDO (Prueba de Salida de Datos).

❏ TCK (Prueba de Reloj).

❏ TMS (Prueba de Selector de Modo).

❏ TRST (Prueba de reinicio). Es opcional.

Esta técnica realizada de manera correcta permite la descarga de la memoria Flash NAND y el reensamblado y funcionamiento normal del equipo sin pérdida de datos.

– La técnica de remoción de la tarjeta de memoria Flash NAND se puede utilizar para recuperar datos en los dispositivos dañados y elude la configuración protección de acceso al dispositivo por contraseña. El procedimiento es destructivo y generalmente es muy difícil volver a conectar la memoria Flash NAND al circuito impreso de la placa (PCB) y que el dispositivo vuelva a funcionar correctamente. Por lo tanto, solo es recomendable en los casos en que el dispositivo se encuentre dañado y no se vuelva a utilizar. Además, es una prueba del tipo irreversible que requiere la autorización judicial correspondiente.

· Software: Técnicas que se ejecutan como programas en el dispositivo con acceso de usuario root y obtienen una imagen física de todas las particiones de datos. Las ventajas[149] sobre las técnicas de hardware son las siguientes:

- Facilidad para su ejecución.

- Generalmente, proveen acceso al sistema de archivo y permiten una copia completa de todos los archivos lógicos simplificando posteriormente el análisis de la información.

- Reduce el riesgo de daño del dispositivo o de la pérdida de datos.

Esta técnica requiere el acceso como usuario root al dispositivo y en Android no está habilitado en forma predeterminada, por lo tanto al cambiar los privilegios de acceso se producen modificaciones en el dispositivo. El procedimiento de acceso como usuario root varía según el fabricante y versión de Android y del kernel o núcleo del sistema operativo Linux. Por consiguiente, resulta ser una técnica con muchos obstáculos y agobiante para el perito. Los tipos de acceso como usuario root pueden ser:

❏ Temporales, alcanzado por un programa del tipo explotación (exploit programa que aprovecha la situación para tomar ventaja de esta, en este caso

acceso como usuario root y control total sobre el dispositivo) y que no sobrevive si se reinicia el equipo. El demonio adb no se ejecuta como root en este caso.

❏ Acceso total a través de una ROM modificada o personalizada o un programa exploit de root persistente. El demonio adb se ejecuta como root mientras que la mayoría de los programas de root persistentes no lo tienen.

❏ Modo de recuperación alcanzado por el acceso a una partición recuperada o a una parte de la ROM personalizada o modificada. En este modo, el demonio adb se ejecuta como root de la misma forma que lo hacen la mayoría de las particiones de recuperación modificadas.

Para el perito es preferible el acceso temporal como root o el acceso a través del modo de recuperación. La implementación de estas técnicas debe practicarse previamente en el laboratorio para evitar el daño o pérdida de datos en el dispositivo.

Procedimiento para el acceso como usuario root por medio de las herramientas de software

Efectuar el siguiente procedimiento en el emulador de Android:

1. En el emulador del dispositivo Android, verificar si el dispositivo ya tiene permisos de acceso como root:

a. El dispositivo debe tener habilitada la opción de depuración USB, verificar aun cuando el dispositivo esté bloqueado. Si no está bloqueado, ejecutar los pasos listados en el “Procedimiento para la recolección lógica”.

b. Conectar el dispositivo a la estación de trabajo de telefonía forense, abrir una terminal e intentar acceder como usuario root con el comando su; debe aparecer el indicador #:

```
$adb shell su
#
```

Si el resultado deniega los permisos de root, el perito podrá consultar en el sitio de programadores y desarrolladores independientes de Android http://www.xdadevelopers.com/.

c. A partir del acceso como usuario root, listar el contenido del dispositivo:

```
#ls acct
cache
config d
data default.prop dev
etc init
init.goldfish.rc init.rc
```

mnt proc root sbin sdcard sys system

ueventd.goldfish.rc ueventd.rc

vendor

2. El modo recuperación se emplea para actualizar, dar formato y ejecutar tareas de mantenimiento en el dispositivo. Tiene funciones limitadas y no permite el acceso como root desde el Shell. En el modo de recuperación personalizado sí brinda acceso como usuario root desde el Shell. Las particiones nuevas de recuperación son configuradas por el usuario. El perito deberá tener especial cuidado al utilizar este modo ya que al instalar un modo de recuperación personalizado se pueden producir daños en el dispositivo (por ejemplo: incompatibilidad entre el kernel y el firmware). El programa que permite el modo de recuperación se encuentra almacenado en una partición dedicada y es de tamaño reducido.

a. Visualizar el contenido del archivo mtd (Memory Technology Device) en el directorio

/proc.

$adb shell cat /proc/mtd dev: size erasesize name

mtd0: 0a100000 00020000 “system”

mtd1: 07c20000 00020000 “recovery” mtd2: 04000000 00020000 “cache”

El resultado muestra las particiones de recuperación: mtd1: 07c20000 00020000 “recovery”

b. Reiniciar el dispositivo utilizando la combinación de teclas correspondiente a cada modelo para ingresar al modo de recuperación.

c. Conectar el dispositivo a la estación de trabajo de telefonía forense si se utiliza un Android no emulado.

d. Verificar si el demonio adb detecta el dispositivo:

$adb devices

List of devices attached 040355321236824F recovery

e. Verificar si se tiene permisos de usuario root:

$adb shell su

#

3. El programa de inicio o de arranque (boot loader) que se ejecuta en el dispositivo Android es responsable de seleccionar y cargar el kernel del sistema operativo Linux. En algunos dispositivos, el fabricante incorpora programas que interactúan con el de inicio de Android y escriben nuevas imágenes en la memoria Flash NAND del dispositivo, con el fin de corregir errores de funcionamiento o para desarrollar o probar software. El perito

puede utilizar programas que escriban en la memoria NAND para obtener acceso como usuario root; no obstante los fabricantes bloquean el acceso a la memoria NAND y, por lo tanto, evitan las modificaciones. El programa de acceso remoto de descarga RSD Lite[150] de Motorola interactúa con dispositivos Android para usos específicos del fabricante, por consiguiente se debe utilizar con la respectiva autorización.

a. Considerando que el programa de inicio está desbloqueado, conectar el dispositivo a la estación de trabajo de telefonía forense y ejecutar el programa RSD, el cual detecta el teléfono Android.

b. El programa solicita la ruta del archivo .sdf (system data format) y luego oprimir el botón Iniciar (Start) para escribir en la memoria.

c. El dispositivo se reinicia y la nueva partición de recuperación está disponible.

4. El programa sbf_flash es similar al RSD Lite de Motorola pero no requiere de una licencia, ni tiene restricciones de uso. Se puede descargar del sitio del autor http://blog. opticaldelusion.org/. Está desarrollado en Linux y también se ejecuta en Mac OS X y simplifica la escritura de datos en la memoria NAND a través de un programa de arranque desbloqueado. Antes de utilizar el programa, verificar si soporta el dispositivo. Para este procedimiento el dispositivo debe tener la batería con carga completa y el archivo

.sdf en la estación de trabajo de telefonía forense.

a. Abrir una terminal y descargar el programa:

$wget http://dl.opticaldelusion.org/sbf_flash

Ubicar el directorio en donde se descargó y darle permisos de ejecución:

$chmod +x sbf_flash

b. Comprobar la versión del programa, ubicarse en el directorio y ejecutar:

$./sbf_flash -h

c. Oprimir las teclas correspondientes al dispositivo para ubicarlo en el modo inicio, aparecerá la siguiente información:

Bootloader

<version number> Battery OK

OK to Program Connect USB Data Cable

d. Efectuar consultas al dispositivo con sbf_flash:

$./sbf_flash –r

El resultado muestra que encontró el dispositivo.

e. Enviar la imagen del archivo .sdf desde la estación de trabajo de telefonía forense a la memoria Flash NAND del teléfono:

$./sbf_flash nombre_de_la_imagen.sdf

El programa encuentra al dispositivo en modo de arranque e inmediatamente carga el archivo con la imagen en la memoria Flash NAND.

f. Reiniciar el dispositivo en el modo recuperación con el nuevo archivo .sdf y a partir de aquí se pueden tener permisos como usuario root y aplicar las técnicas de software para la recuperación física de datos.

5. El protocolo fastboot[151] se utiliza para escribir imágenes en la memoria Flash NAND a través de un puerto USB. La utilidad fue desarrollada para dispositivos de Android de HTC y se encuentra dentro del paquete del proyecto de desarrollo de Android de código abierto impulsado por Google (AOSP Android Open Source Project[152]). El programa de inicio del teléfono debe soportar el protocolo fastboot y la seguridad debe estar deshabilitada. Esta herramienta no se puede ejecutar en el emulador.

a. Ingresar al modo de inicio rápido (fastboot), apagar el dispositivo o reiniciarlo manteniendo oprimida la tecla de retroceso, hasta que en la pantalla aparezca el texto fastboot. A partir de aquí el dispositivo puede recibir comandos u órdenes en el modo de inicio rápido. Para salir de este modo, presionar la tecla Enviar (send) o la tecla de llamar y la tecla Fin (end) o colgar o de finalizar llamada. El menú del modo de inicio rápido puede variar según los dispositivos.

b. En la estación de trabajo de telefonía forense, abrir una terminal de línea de comando e ingresar los siguientes comandos de fastboot:

i. Verificar si se detecta el dispositivo:

$./fastboot devices

ii. Obtener ayuda del comando fastboot:

$./fastboot –-help

usage: fastboot [<option>] <command> commands:

update <filename> reflash device from update.zip

flashall flash boot + recovery + system

flash <partition> [<filename>] write a file to a flash partition erase <partition> erase a flash partition

getvar <variable> display a bootloader variable

boot <kernel> [<ramdisk>] download and boot kernel

flash:raw boot <kernel> [<ramdisk>] create bootimage and flash it devices list all connected devices continue continue with autoboot reboot reboot device normally reboot-bootloader reboot device into bootloader help show this help message

options:

-w erase userdata and cache

-s <serial number> specify device serial number

-p <product> specify product name

-c <cmdline> override kernel commandline

-i <vendor id> specify a custom USB vendor id

-b <base_addr> specify a custom kernel base address

-n <page size> specify the nand page size. default: 2048

iii. Sobrescribir la partición de recuperación:

$fastboot flash recovery particion_de_recuperacion_modificada.img

c. En Windows, con el paquete Android-SDK instalado, abrir una terminal y ubicarse en el directorio de la aplicación fastboot:

i. C:\Android\android-sdk\platform-tools>fastboot.exe

d. Reiniciar el dispositivo en el modo de recuperación y proceder con la técnica de imagen física del teléfono por medio del software.

6. Registrar, documentar y/o capturar pantallas con la información requerida.

Procedimiento para el método AFPhysical de imagen física del disco de las particiones de la memoria Flash NAND de Android[153]

1. La técnica AFPhysical[154] de la empresa ViaForensics requiere permisos de usuario root. El perito debe adaptar la técnica acorde al dispositivo Android a duplicar.

a. El dispositivo debe iniciarse en el modo de recuperación.

b. Conectar el dispositivo a la estación de trabajo de telefonía forense.

c. Verificar si el demonio adb detecta el dispositivo:

$adb devices

El resultado debe mostrar la partición de recuperación.

d. Verificar si se tiene permisos de usuario root:

$adb shell su

#

e. Identificar las particiones de la memoria Flash NAND que deben duplicarse y están montadas:

mount

rootfs / rootfs ro 0 0

tmpfs /dev tmpfs rw,nosuid,mode=755 0 0

devpts /dev/pts devpts rw,mode=600 0 0

proc /proc proc rw 0 0

sysfs /sys sysfs rw 0 0

none /acct cgroup rw,cpuacct 0 0

tmpfs /mnt/asec tmpfs rw,mode=755,gid=1000 0 0

tmpfs /mnt/obb tmpfs rw,mode=755,gid=1000 0 0

none /dev/cpuctl cgroup rw,cpu 0 0

/dev/block/mtdblock0 /system yaffs2 ro 0 0

/dev/block/mtdblock1 /data yaffs2 rw,nosuid,nodev 0 0

/dev/block/mtdblock2 /cache yaffs2 rw,nosuid,nodev 0 0

/dev/block/vold/179:0 /mnt/sdcard vfat rw,dirsync,nosuid,nodev,noe id=1015,fmask=0702,dmask=0702,allow_utime=0020,codepage=cp437,ioch 1,shortname=mixed,utf8,errors=remount-ro 0 0

/dev/block/vold/179:0 /mnt/secure/asec vfat rw,dirsync,nosuid,node 000,gid=1015,fmask=0702,dmask=0702,allow_utime=0020,codepage=cp437 8859-1,shortname=mixed,utf8,errors=remount-ro 0 0

tmpfs /mnt/sdcard/.android_secure tmpfs ro,size=0k,mode=000 0 0

Acorde al listado, el dispositivo utiliza MTD para el acceso a la memoria Flash NAND, así como el sistema de archivo YAFFS2.

f. Verificar las particiones contenidas en MTD:

cat /proc/mtd

(Datos obtenidos del emulador) dev: size erasesize name

mtd0: 0a100000 00020000 “system” mtd1: 07c20000 00020000 “userdata” mtd2: 04000000 00020000 “cache”

(Otras particiones en los dispositivos no emulados) dev: size erasesize name

mtd0: 00040000 00020000 “misc”

mtd1: 00500000 00020000 “recovery”

mtd2: 00280000 00020000 “boot”

mtd3: 04380000 00020000 “system”

mtd4: 04380000 00020000 “cache”

mtd5: 04ac0000 00020000 “userdata”

El perito deberá duplicar todas las particiones listadas en el archivo MTD.

g. Existen cuatro estrategias para adquirir la imagen en Android:

i. Duplicación de todas las particiones de la memoria Flash NAND, incluyendo los datos y la información que se encuentra en el área de reserva denominada OOB (Out Of Band), que contiene metadatos de los fragmentos y los códigos de corrección de errores (ECC Error Correction Code). El área OOB se encuentra después de cada fragmento en la memoria Flash NAND, tiene un tamaño de 64 bytes, almacena la información que maneja el archivo

MTD (/proc/mtd) y metadatos críticos del sistema de archivo.

iii. Efectuar una imagen con dd de las particiones que solo obtiene los datos y no el OOB.

iv. Una adquisición lógica de los archivos utilizando el comando tar.

v. Una adquisición lógica de los archivos utilizando el demonio adb.

h. Existen dos formas principales para guardar la imagen adquirida del dispositivo:

i. Utilizar el demonio adb redireccionando el puerto para crear una conexión de red entre la estación de trabajo de telefonía forense y el dispositivo Android a través de la conexión por USB. En este caso, no es necesario colocar un dispositivo y la imagen se almacena directamente en la estación de trabajo.

ii. Colocar una tarjeta SD en el dispositivo, montarla y guardar localmente la imagen; en este caso, el proceso de adquisición es más rápido.

i. Ejemplo de duplicación o adquisición de la partición de los datos del usuario ("userdata" – mtd5).

i. Se debe evitar escribir información en la memoria Flash NAND; verificar el resultado del comando mount y observar que el directorio /dev está en tmpfs y por lo tanto guardado en RAM, por lo que resulta conveniente enviar las herramientas forenses al directorio /dev. (tar, md5sum, nanddump, nc):

$adb push AFPhysical/ /dev/AFPhysical

ii. Convertir los programas en ejecutables dentro del dispositivo:

$adb shell

#cd /dev/AFPhysical

/dev/AFPhysical#ls –l

Lista el contenido de /dev y los permisos de los archivos: tar, md5sum, nanddump, nc

/dev/AFPhysical#chmod 755 *

(Cambia los permisos para ejecución de los archivos para el propietario, grupo y otros)

/dev/AFPhysical#ls –l

(Verificar el resultado, debe aparecer: -rwxr-xr-x para los archivos tar, md5sum, nanddump, nc)

iii. En el caso de efectuar la imagen en una tarjeta SD, el perito debe verificar que esta se encuentre en el formato adecuado, y montarla en el sistema:

#/dev/AFPhysical/nanddump /dev/mtd/mtd5 > /sdcard/mtd5.nanddump
Verificar en la tarjeta si se encuentra el archivo de la imagen:

#ls –l /sdcard/mtd5.nanddump

El perito puede transferir el archivo a la estación de trabajo de telefonía

forense o remover la tarjeta SD del dispositivo y copiar la imagen a través del puerto USB de la estación de trabajo.

iv. Certificar matemáticamente la imagen adquirida con el comando md5sum en la estación de trabajo:

$md5sum mtd5.nanddump

j. Ejemplo de duplicación o adquisición de las particiones con el comando dd. Efectuar una imagen con dd de las particiones y guardar la imagen en la tarjeta SD:

$adb shell

#dd if=/dev/ block/mtdblock5/ of=/sdcard/mtd5.dd bs=4096

l. Ejemplo de duplicación o adquisición de los datos de la partición "userdata" o mtd5 con el comando nanddump y con el comando nc (netcat)*155*:

i. Abrir una terminal en la estación de trabajo de telefonía forense y habilitar la conexión de red entre los dos extremos redireccionando el puerto.

Terminal de la estación de trabajo de telefonía forense:

$adb forward tcp: 10003 tcp: 10003

El comando conecta el puerto 10003 con el dispositivo Android y la estación de trabajo.

ii. Abrir otra terminal en la estación de trabajo de telefonía forense y ejecutar el comando nanddump en el dispositivo Android y crear una tubería (pipe) o comunicación entre procesos para la salida del archivo a netcat.

Terminal del dispositivo Android:

$adb shell

#/dev/AFPhysical/nanddump /dev/mtd/mtd5 | /dev/AFPhysical/nc –l –p 10003 El dispositivo Android envía los datos a través de netcat; necesitan ser recibidos

en la terminal de la estación de trabajo de telefonía forense.

Terminal de la estación de trabajo de telefonía forense:

$nc 127.0.0.1 10003 > mtd5.nanddump

Al finalizar el comando nanddump sale sin ningún mensaje, lo mismo que netcat en la estación de trabajo.

iii. Verificar la existencia de la imagen en la estación de trabajo.

Terminal de la estación de trabajo de telefonía forense:

$ls –lh mtd5.nanddump

El resultado muestra el archivo enviado desde el dispositivo Android a la estación de trabajo.

m. Ejemplo de duplicación o adquisición de los datos del usuario con el comando dd y el comando nc (netcat), similar al ejemplo con nanddump pero sin la extracción de los datos OOB.

i. Abrir una terminal en la estación de trabajo de telefonía forense y habilitar la conexión de red entre los dos extremos redireccionando el puerto.

Terminal de la estación de trabajo de telefonía forense:

$adb forward tcp: 10003 tcp: 10003

ii. Abrir otra terminal en la estación de trabajo de telefonía forense y ejecutar el comando adb y visualizar el contenido del archivo mtd en el directorio /proc del dispositivo Android.

Terminal del dispositivo Android:

$adb shell

$su

#cat /proc/mtd

dev: size erasesize name

mtd0: 00040000 00020000 “misc”

mtd1: 00500000 00020000 “recovery”

mtd2: 00280000 00020000 “boot”

mtd3: 04380000 00020000 “system”

mtd4: 04380000 00020000 “cache”

mtd5: 04ac0000 00020000 “userdata”

Ejecutar el comando dd para crear la imagen:

#dd if= /dev/mtd/mtd5 bs=4096 | /dev/AFPhysical/nc –l –p 10003

El comando dd transfiere los datos a través de la tubería con el comando netcat.

Terminal de la estación de trabajo de telefonía forense:

$ nc 127.0.0.1 10003 > dd of=mtd5.dd bs=4096

iii. Extraer los datos de la imagen, utilizando la forma recursiva de obtener datos del comando adb ya que este demonio posee los permisos de ejecución como usuario root. Se puede utilizar también el comando tar para copiar los datos en un único archivo o guardar los archivos en la tarjeta SD. En este ejemplo es necesario montar el sistema de archivo YAFFS2 en el modo de solo lectura.

Terminal del dispositvo Android:

#mount –o ro –t yaffs2 /dev/block/mtdblock5 /data

El comando monta la partición /userdata como solo lectura:

#mount –o ro,remount –t yaffs2 /dev/block/mtdblock4 /cache

El comando toma la partición/caché, ya montada y la vuelve a montar en el modo solo lectura:

#mount

(Ejemplo de los resultados del comando mount obtenido del emulador Android, con particiones:

mtd0: 0a100000 00020000 “system” mtd1: 07c20000 00020000 “userdata” mtd2: 04000000 00020000 “caché”)

mount

rootfs / rootfs ro 0 0

tmpfs /dev tmpfs rw,nosuid,mode=755 0 0

devpts /dev/pts devpts rw,mode=600 0 0

proc /proc proc rw 0 0

sysfs /sys sysfs rw 0 0

none /acct cgroup rw,cpuacct 0 0

tmpfs /mnt/asec tmpfs rw,mode=755,gid=1000 0 0

tmpfs /mnt/obb tmpfs rw,mode=755,gid=1000 0 0

none /dev/cpuctl cgroup rw,cpu 0 0

/dev/block/mtdblock0 /system yaffs2 ro 0 0

/dev/block/mtdblock1 /data yaffs2 rw,nosuid,nodev 0 0

/dev/block/mtdblock2 /cache yaffs2 ro 0 0

/dev/block/vold/179:0 /mnt/sdcard vfat rw,dirsync,nosuid,nodev,noexec,uid=1000,id=1015,fmask=0702,dmask=0702 ow_utime=0020,codepage=cp437,iocharset=iso88591,shortname=mixed,utf8

s=remount-ro 0 0/dev/block/vold/179:0 /mnt/secure/asec vfat rw,dirsync,nosuid,

nodev,noexec,uid=000,gid=1015,fmask=0702,dmask=0702,allow_utime=002 page=cp437,iocharset=is8859-1,shortname=mixed,utf8,errors=remount-ro 0 0tmpfs /mnt/sdcard/.android_secure tmpfs ro,size=0k,mode=000 0 06

El comando muestra las particiones montadas y ahora se puede ejecutar el demonio adb para obtener los datos:

$adb pull /data/data/com.android.providers.telephony sms

adb pull /data/data/com.android.providers.telephony sms pull: building file list...

pull:

/data/data/com.android.providers.telephony/shared_prefs/preferred-apn.xml-> sms/shared_prefs/preferred-apn.xml

pull:

/data/data/com.android.providers.telephony/app_parts/PART_133988733
-> sms/app_parts/PART_1339887331550

pull: /

data/data/com.android.providers.telephony/databases/mmssms.db -> sms/databases/mmssms.db

pull:

/data/data/com.android.providers.telephony/databases/telephony.db-journal

-> sms/databases/telephony.db-journal pull:

/data/data/com.android.providers.telephony/databases/telephony.db -> sms/ databases/telephony.db

5 files pulled. 0 files skipped.

54 KB/s (65557 bytes in 1.167s)

El comando adb pull obtiene los archivos y bases de datos de la partición /data.

Terminal del dispositivo Android:

$adb shell

#/dev/AFPhyisical/tar cpv –f -/data/data/com.providers.telephony /caché /dev/ AFPhysical/nc –l –p 10003

El comando tar ubica los archivos y directorios en un solo archivo. El directorio contiene los mensajes SMS/MMS en el directorio /userdata y el directorio /caché. Se envía el archivo a través de la red y se recibe en la estación de trabajo de telefonía forense.

Terminal de la estación de trabajo de telefonía forense:

$ nc 127.0.0.1 10003 > datos-android.tar

2. Registrar, documentar y/o capturar pantallas con la información requerida.

Síntesis – Lista de control

· Existen diversas técnicas para la adquisición de datos en dispositivos con Android. Las herramientas que requieren escribir y acceder como usuario root en el dispositivo solo se pueden utilizar como práctica de laboratorio para las pruebas y aprendizaje del perito en el manejo de ellas.

· En los dispositivos protegidos con clave será necesario, según el caso, evitar la protección para extraer los datos.

· En los dispositivos que no están protegidos con clave, el perito puede decidir realizar una recolección lógica que incluye los datos accesibles a través de los proveedores de contenido o aplicar la técnica de recolección física que

requiere del perito un conocimiento más profundo de esta.

- Otras herramientas para la adquisición física:
  - xRecovery, efectúa un resguardo de las particiones del usuario y del sistema. De libre disponibilidad.

xda-developers http://forum.xda-developers.com/showthread.php?t=859571

  - yaffs2utils, conjunto de herramientas de Linux, licencia GNUGPL, http://code.google.com/p/yaffs2utils/.
  - Busybox, contiene comandos de Unix en un único ejecutable, licencia GPL. http://www.busybox.net/.
  - Mtdutils, conjunto de herramientas. http://processors.wiki.ti.com/index.php/Mtdutils processors.wiki.ti.com/index.php/Mtdutils http://www.linux-mtd.infradead.org/doc/general.html
  - AccessData's FTK Imager, de libre disponibilidad. http://accessdata.com/support/ adownloads.

Etapa de análisis de datos

La mayoría de las herramientas y técnicas que se utilizan para el análisis de celulares en particular y las que se aplican en Informática forense son válidas también en los dispositivos Android. Las herramientas a utilizar pueden ser de código abierto, de libre disponibilidad o productos comerciales o comandos del propio sistema operativo Linux.

Procedimiento para el análisis del núcleo del sistema operativo Linux

Registro de eventos o sucesos del núcleo.

1. En la estación de trabajo de telefonía forense, conectarse al dispositivo con USB Debbuging habilitado, ejecutar el comando dmesg, no requiere permisos administrativos:

$adb shell dmesg

<6>Initializing cgroup subsys cpu

<5>Linux version 2.6.29-g46b05b2 (vchtchetkine@vc-irv.irv.corp.google.com) (gccversion 4.4.3 [GCC]) #28 Thu Nov 17 06:39:36 PST 2011

<4>CPU: ARMv7 Processor [410fc080] revision 0 (ARMv7), cr=10c5387f

<4>CPU: VIPT nonaliasing data cache, VIPT nonaliasing instruction cache

<4>Machine: Goldfish
<4>Memory policy: ECC disabled, Data cache writeback
<7>On node 0 totalpages: 131072
<7>free_area_init_node: node 0, pgdat c02f5a20, node_mem_map c0383000
<7> Normal zone: 1024 pages used for memmap
<7> Normal zone: 0 pages reserved
<7> Normal zone: 130048 pages, LIFO batch:31
<4>Built 1 zonelists in Zone order, mobility grouping on. Total pages: 130048
<5>Kernel command line: qemu.gles=0 qemu=1 console=ttyS0 android.qemud=ttyS1 and roid.checkjni=1 ndns=3
<3>Unknown boot option `qemu.gles=0': ignoring
<3>Unknown boot option `android.qemud=ttyS1': ignoring
<3>Unknown boot option `android.checkjni=1': ignoring
<4>PID hash table entries: 2048 (order: 11, 8192 bytes)
<4>Console: colour dummy device 80x30
<6>Dentry cache hash table entries: 65536 (order: 6, 262144 bytes)
<6>Inode-cache hash table entries: 32768 (order: 5, 131072 bytes)
<6>Memory: 512MB = 512MB total
<5>Memory: 515712KB available (2756K code, 683K data, 108K init)
<6>Calibrating delay loop... 375.19 BogoMIPS (lpj=1875968)
<4>Mount-cache hash table entries: 512
<6>Initializing cgroup subsys debug
<6>Initializing cgroup subsys cpuacct
<6>Initializing cgroup subsys freezer
<6>CPU: Testing write buffer coherency: ok
<6>net_namespace: 716 bytes
<6>NET: Registered protocol family 16
<4>bio: create slab <bio-0> at 0
<7>Switched to high resolution mode on CPU 0
<6>NET: Registered protocol family 2
<6>IP route cache hash table entries: 16384 (order: 4, 65536 bytes)
<6>TCP established hash table entries: 65536 (order: 7, 524288 bytes)

<6>TCP bind hash table entries: 65536 (order: 6, 262144 bytes)
<6>TCP: hash tables configured (established 65536 bind 65536)
<6>TCP reno registered
<6>NET: Registered protocol family 1
<6>checking if image is initramfs... it is
<6>Freeing initrd memory: 160K
<4>goldfish_new_pdev goldfish_interrupt_controller at ff000000 irq -1
<4>goldfish_new_pdev goldfish_device_bus at ff001000 irq 1
<4>goldfish_new_pdev goldfish_timer at ff003000 irq 3
<4>goldfish_new_pdev goldfish_rtc at ff010000 irq 10
<4>goldfish_new_pdev goldfish_tty at ff002000 irq 4
<4>goldfish_new_pdev goldfish_tty at ff011000 irq 11
<4>goldfish_new_pdev goldfish_tty at ff012000 irq 12
<4>goldfish_new_pdev smc91x at ff013000 irq 13
<4>goldfish_new_pdev goldfish_fb at ff014000 irq 14
<4>goldfish_new_pdev goldfish_audio at ff004000 irq 15
<4>goldfish_new_pdev goldfish_mmc at ff005000 irq 16
<4>goldfish_new_pdev goldfish_memlog at ff006000 irq -1
<4>goldfish_new_pdev goldfish-battery at ff015000 irq 17
<4>goldfish_new_pdev goldfish_events at ff016000 irq 18
<4>goldfish_new_pdev goldfish_nand at ff017000 irq -1
<4>goldfish_new_pdev qemu_pipe at ff018000 irq 19
<4>goldfish_new_pdev goldfish-switch at ff01a000 irq 20
<4>goldfish_new_pdev goldfish-switch at ff01b000 irq 21
<4>goldfish_pdev_worker registered goldfish_interrupt_controller
<4>goldfish_pdev_worker registered goldfish_device_bus
<4>goldfish_pdev_worker registered goldfish_timer
<4>goldfish_pdev_worker registered goldfish_rtc
<4>goldfish_pdev_worker registered goldfish_tty
<4>goldfish_pdev_worker registered goldfish_tty
<4>goldfish_pdev_worker registered goldfish_tty
<4>goldfish_pdev_worker registered smc91x
<4>goldfish_pdev_worker registered goldfish_fb
<4>goldfish_pdev_worker registered goldfish_audio
<4>goldfish_pdev_worker registered goldfish_mmc
<4>goldfish_pdev_worker registered goldfish_memlog

<4>goldfish_pdev_worker registered goldfish-battery
<4>goldfish_pdev_worker registered goldfish_events
<4>goldfish_pdev_worker registered goldfish_nand
<4>goldfish_pdev_worker registered qemu_pipe
<4>goldfish_pdev_worker registered goldfish-switch
<4>goldfish_pdev_worker registered goldfish-switch
<6>ashmem: initialized
<6>Installing knfsd (copyright (C) 1996 okir@monad.swb.de).
<4>yaffs Nov 17 2011 06:39:33 Installing.
<6>msgmni has been set to 1008
<6>alg: No test for stdrng (krng)
<6>io scheduler noop registered
<6>io scheduler anticipatory registered (default)
<6>io scheduler deadline registered
<6>io scheduler cfq registered
<4>allocating frame buffer 480 * 800, got ffa00000
<6>console [ttyS0] enabled
<6>brd: module loaded
<6>loop: module loaded
<6>nbd: registered device at major 43
<4>goldfish_audio_probe
<6>tun: Universal TUN/TAP device driver, 1.6
<6>tun: (C) 1999-2004 Max Krasnyansky <maxk@qualcomm.com>
<4>smc91x.c: v1.1, sep 22 2004 by Nicolas Pitre <nico@cam.org>
<6>eth0 (smc91x): not using net_device_ops yet
<4>eth0: SMC91C11xFD (rev 1) at e080c000 IRQ 13 [nowait]
<4>eth0: Ethernet addr: 52:54:00:12:34:56
<7>eth0: No PHY found
<4>goldfish nand dev0: size a100000, page 2048, extra 64, erase 131072
<4>goldfish nand dev1: size 7c20000, page 2048, extra 64, erase 131072
<4>goldfish nand dev2: size 4000000, page 2048, extra 64, erase 131072
<6>mice: PS/2 mouse device common for all mice
<4>*** events probe ***
<4>events_probe() addr=0xe0814000 irq=18
<4>events_probe() keymap=qwerty2

<6>input: qwerty2 as /devices/virtual/input/input0
<6>goldfish_rtc goldfish_rtc: rtc core: registered goldfish_rtc as rtc0
<6>device-mapper: uevent: version 1.0.3
<6>device-mapper: ioctl: 4.14.0-ioctl (2008-04-23) initialised: dm-devel@redhat. com
<6>logger: created 64K log 'log_main'
<6>logger: created 256K log 'log_events'
<6>logger: created 64K log 'log_radio'
<6>TCP cubic registered
<6>NET: Registered protocol family 10
<6>IPv6 over IPv4 tunneling driver
<6>NET: Registered protocol family 17
<6>NET: Registered protocol family 15
<6>RPC: Registered udp transport module.
<6>RPC: Registered tcp transport module.
<6>802.1Q VLAN Support v1.8 Ben Greear <greearb@candelatech.com>
<6>All bugs added by David S. Miller <davem@redhat.com>
<6>VFP support v0.3: implementor 41 architecture 3 part 30 variant c rev 0
<6>goldfish_rtc goldfish_rtc: setting system clock to 2012-06-16 20:18:33 UTC (1 339877913)
<6>Freeing init memory: 108K
<6>mmc0: new SD card at address e118
<6>mmcblk0: mmc0:e118 SU02G 2.00 GiB
<6> mmcblk0:
<3>init: cannot open '/initlogo.rle'
<6>yaffs: dev is 32505856 name is "mtdblock0"
<6>yaffs: passed flags ""
<4>yaffs: Attempting MTD mount on 31.0, "mtdblock0"
<4>yaffs_read_super: isCheckpointed 0
<4>save exit: isCheckpointed 1
<6>yaffs: dev is 32505857 name is "mtdblock1"
<6>yaffs: passed flags ""
<4>yaffs: Attempting MTD mount on 31.1,

“mtdblock1”

<4>yaffs_read_super: isCheckpointed 0

<6>yaffs: dev is 32505858 name is “mtdblock2”

<6>yaffs: passed flags ““

<4>yaffs: Attempting MTD mount on 31.2, “mtdblock2”

<4>yaffs_read_super: isCheckpointed 0

<3>init: cannot find ‘/system/bin/drmserver’, disabling ‘drm’

<3>init: cannot find ‘/system/bin/dbus-daemon’, disabling ‘dbus’

<3>init: cannot find ‘/system/etc/install-recovery.sh’, disabling ‘flash_recovery’

<6>eth0: link up

<6>warning: `rild’ uses 32-bit capabilities (legacy support in use)

<7>eth0: no IPv6 routers present

<3>binder: release proc 152, transaction 5082, not freed

<3>binder: release proc 138, transaction 5117, not freed

<6>binder: release 276:276 transaction 6755 out, still active

<6>binder: 81:274 transaction failed 29189, size15216-0

<6>binder: send failed reply for transaction 6755, target dead

<6>binder: 298:308 refcount change on invalid ref 9

<6>binder: 298:308 refcount change on invalid ref 12

<3>init: sys_prop: permission denied uid:1000 name:user.language

<3>init: sys_prop: permission denied uid:1000 name:user.region

<6>binder: 298:308 refcount change on invalid ref 7

<6>binder: 298:308 refcount change on invalid ref 10

<6>binder: 298:308 refcount change on invalid ref 12

<6>binder: 298:308 refcount change on invalid ref 13

<6>binder: 372:381 refcount change on invalid ref 28

<6>binder: 372:381 refcount change on invalid ref 34

<6>binder: 372:381 refcount change on invalid ref 22

<6>binder: 372:381 refcount change on invalid ref 38

<6>binder: 372:702 refcount change on invalid ref 34

<6>binder: 372:702 refcount change on invalid ref 34

<3>binder: transaction release 53442 bad handle 34

<6>binder: 372:736 refcount change on invalid ref 38
<6>binder: 372:736 refcount change on invalid ref 38
<3>binder: transaction release 55129 bad handle 38
<6>binder: 372:381 refcount change on invalid ref 29
<6>binder: 372:381 refcount change on invalid ref 30
<6>binder: 372:381 refcount change on invalid ref 32
<6>binder: 372:381 refcount change on invalid ref 33
<6>binder: 372:381 refcount change on invalid ref 34
<3>init: untracked pid 1096 exited
<3>init: untracked pid 1103 exited
<6>binder: 372:381 refcount change on invalid ref 41
<6>binder: 372:381 refcount change on invalid ref 36
<6>binder: 372:381 refcount change on invalid ref 60
<6>binder: 372:707 refcount change on invalid ref 41
<6>binder: 372:707 refcount change on invalid ref 41
<3>binder: transaction release 103230 bad handle 41
<6>binder: release 1633:1633 transaction 723028 out, still active
<6>binder: 81:273 transaction failed 29189, size56-0
<6>binder: 38:1662 transaction failed 29189, size92-0
<3>init: untracked pid 1733 exited

El resultado extraído del emulador de Android muestra información acerca de la fecha y hora, del hardware, actividades del dispositivo en el inicio del sistema y del núcleo del sistema operativo. Si el dispositivo no ha sido iniciado recientemente, la información del arranque del dispositivo ya no está disponible.

Contar las líneas del resultado de dmesg, con el comando wc:

$adb shell dmesg | wc -l

El perito puede enviar el resultado del comando dmesg a un archivo de texto y guardarlo para su edición en un directorio en la estación de trabajo de telefonía forense para su análisis detallado e incluirlo como anexo en el informe pericial.

$adb shell dmesg > dmesg.txt o dmesg.log

2. Analizar la información en línea de los mensajes de depuración del sistema y de las aplicaciones con el comando logcat[156]; para detener el comando utilizar Ctrl + C. El siguiente resultado es del emulador Android:

$adb shell logcat

W/NetworkManagementSocketTagger(81): setKernelCountSet(10001, 1)

failed with

errno -2

I/Process (81): Sending signal. PID: 372 SIG: 3

I/dalvikvm(372): threadid=3: reacting to signal 3

D/dalvikvm(81): GC_CONCURRENT freed 15K, 34% free 12781K/19271K, paused 6ms+113ms

I/dalvikvm(372): Wrote stack traces to '/data/anr/traces.txt'

D/dalvikvm(181): GC_CONCURRENT freed 263K, 45% free 9933K/18055K, paused 4ms+1 8ms

I/Process (81): Sending signal. PID: 372 SIG: 3 I/dalvikvm(372): threadid=3: reacting to signal 3

I/dalvikvm(372): Wrote stack traces to '/data/anr/traces.txt' E/DefaultVoicemailNotifier(372): No voicemails to notify about: clear the notification. D/dalvikvm(372): null clazz in OP_INSTANCE_OF, single-stepping I/Process (81): Sending signal. PID: 372 SIG: 3

I/dalvikvm(372): threadid=3: reacting to signal 3 I/dalvikvm(372): Wrote stack traces to '/data/anr/traces.txt'

I/ActivityManager(81): Displayed com.android.contacts/.activities.DialtactsActivity:

+2s275ms

W/AudioTrack(372): obtainBuffer timed out (is the CPU pegged?) 0x2af660 user=0 0000800, server=00000000

E/ToneGenerator(372): --Delayed start timed out, status -110 W/ToneGenerator(372): Tone start failed!!!, time 96745117

W/AudioTrack(372): obtainBuffer timed out (is the CPU pegged?) 0x2af660 user=0 0000800, server=00000000

E/ToneGenerator(372): --Delayed start timed out, status -110 W/ToneGenerator(372): Tone start failed!!!, time 96748377

W/AudioTrack(372): obtainBuffer timed out (is the CPU pegged?) 0x2af660 user=0 0000800, server=00000000

E/ToneGenerator(372): --Delayed start timed out, status -110 W/ToneGenerator(372): Tone start failed!!!, time 96751603

W/AudioTrack(372): obtainBuffer timed out (is the CPU pegged?) 0x2af660 user=0 0000800, server=00000000

E/ToneGenerator(372): --Delayed start timed out, status -110 W/ToneGenerator(372): Tone start failed!!!, time 96754873

I/ActivityManager(81): START {act=android.intent.action.CALL_BUTTON flg=0x100 00000 cmp=com.android.contacts/.activities.DialtactsActivity}

from pid 372 I/ActivityManager(81): START {act=android.intent.action.MAIN flg=0x10840000 c mp=com.android.phone/.InCallScreen} from pid 211

W/WindowManager(81): Failure taking screenshot for (180x300) to layer 21065 D/dalvikvm(372): GREF has increased to 201

D/InCallScreen(211): onNewIntent: intent = Intent { act=android.intent.action.

MAIN flg=0x10c40000 cmp=com.android.phone/.InCallScreen }, phone state = OFFHOOK D/PhoneStatusBar(181): disable: < EXPAND* icons ALERTS ticker system_info back home recent clock >

E/DefaultVoicemailNotifier(372): No voicemails to notify about: clear the noti fication.

D/dalvikvm(181): GC_CONCURRENT freed 393K, 45% free 10022K/18055K, paused 4ms+

31ms

I/Process (81): Sending signal. PID: 211 SIG: 3 I/dalvikvm(211): threadid=3: reacting to signal 3

I/dalvikvm(211): Wrote stack traces to '/data/anr/traces.txt' I/dalvikvm(211): Jit: resizing JitTable from 4096 to 8192

W/InputManagerService(81): Starting input on non-focused client com.android.i nternal.view.IInputMethodClient$Stub$Proxy@41713a50 (uid=10001 pid=372) W/IInputConnectionWrapper(372): showStatusIcon on inactive InputConnection W/NetworkManagementSocketTagger(81): setKernelCountSet(10001, 0) failed with

errno -2

I/ActivityManager(81): No longer want com.android.customlocale2 (pid 987): hi dden #16

I/WindowManager(81): WIN DEATH: Window{4141e9d8 com.android.customlocale2/ com

.android.customlocale2.CustomLocaleActivity paused=false}

D/dalvikvm(372): GC_EXPLICIT freed 642K, 10% free 12143K/13383K, paused 4ms+17 ms

E/StrictMode(372): class com.android.contacts.activities.DialtactsActivity; in stances=2; limit=1

E/StrictMode(372): android.os.StrictMode$InstanceCountViolation: class com.and roid.contacts.activities.DialtactsActivity; instances=2; limit=1

E/StrictMode(372): at android.os.StrictMode.setClassInstanceLimit(StrictMod e.java:1)

E/DefaultVoicemailNotifier(372): No voicemails to notify about: clear the noti fication.

E/StrictMode(372): A resource was acquired at attached stack trace but never r eleased. See java.io.Closeable for information on avoiding resource leaks. E/StrictMode(372): java.lang.Throwable: Explicit termination method ‘close’ no t called

E/StrictMode(372): at dalvik.system.CloseGuard.open(CloseGuard.java:184) E/StrictMode(372): at android.content.ContentResolver$CursorWrapperInner.<i nit> (ContentResolver.java:1582)

E/StrictMode(372): at android.content.ContentResolver.query(ContentResolver .java:321)

E/StrictMode(372): at android.content.AsyncQueryHandler$WorkerHandler.handl eMessage(AsyncQueryHandler.java:79)

E/StrictMode(372): at com.android.contacts.calllog.CallLogQueryHandler$Catc

El resultado muestra el registro en línea de todas las tareas que se realizan en el dispositivo. Se puede obtener información de latitud y longitud, información de fecha y hora, detalles del uso de las aplicaciones, etc. Cada mensaje comienza con una letra que indica:

- V: verbose, detallado y de menor prioridad.
- D: debug, depuración.
- I: information, información.
- W: warning, advertencia.
- E: error.
- F: fatal.
- S: silent, silencioso, de mayor prioridad y donde no aparece nada escrito.

3. Analizar la información en línea de las conexiones del teléfono móvil con el sistema GSM, utilizando el comando logcat. La información puede ser de interés para el perito ya que muestra los datos sobre:

- Fecha y hora de los eventos en formato Unix Epoch.
- Comandos AT utilizados por el celular para comunicarse.
- Mensajes SMS: receptor, tamaño, fecha y hora.
- Dirección IP del celular.
- Red y datos de la ubicación.
- Información del proveedor del servicio.

El registro se almacena en el directorio /dev/log/radio. El siguiente resultado parcial es del emulador de Android:

$adb shell logcat –b radio

D/RILJ (211): [5616]> DIAL

D/RIL (35): onRequest: DIAL D/AT (35): AT> ATD45763890; D/AT (35): AT< OK

D/RILJ (211): [5616]< DIAL D/AT (35): AT< RING

D/RILJ (211): [UNSL]< UNSOL_RESPONSE_CALL_STATE_CHANGED D/AT (35): AT< RING

D/RILJ (211): [UNSL]< UNSOL_RESPONSE_CALL_STATE_CHANGED D/RILJ (211): [5617]> GET_CURRENT_CALLS

D/RIL (35): onRequest: GET_CURRENT_CALLS D/AT (35): AT> AT+CLCC

D/AT (35): AT< +CLCC: 1,0,0,0,0,”45763890”,129 D/AT (35): AT< OK

V/RILJ (211): Incoming UUS : NOT present! D/RILJ (211): InCall VoicePrivacy is disabled

D/RILJ (211): [5617]< GET_CURRENT_CALLS [id=1,ACTIVE,toa=129,norm,mo,0,voc,

noevp,,cli=1,,0]

D/GSM (211): [GsmDCT] handleMessage msg={ what=270343 when=-4s146ms obj=an

droid.os.AsyncResult@41641430 }

D/GSM (211): [GsmDCT] onVoiceCallStarted D/RILJ (211): [5618]> GET_CURRENT_CALLS D/RIL (35): onRequest: GET_CURRENT_CALLS D/AT (35): AT> AT+CLCC

D/AT (35): AT< +CLCC: 1,0,0,0,0,”45763890”,129 D/AT (35): AT< OK

V/RILJ (211): Incoming UUS : NOT present! D/RILJ (211): InCall VoicePrivacy is disabled

D/RILJ (211): [5618]< GET_CURRENT_CALLS [id=1,ACTIVE,toa=129,norm,mo,0,voc,

noevp,,cli=1,,0]

D/RILJ (211): [5619]> GET_CURRENT_CALLS

D/RIL (35): onRequest: GET_CURRENT_CALLS D/AT (35): AT> AT+CLCC

D/AT (35): AT< +CLCC: 1,0,0,0,0,”45763890”,129 D/AT (35): AT< OK

V/RILJ (211): Incoming UUS : NOT present! D/RILJ (211): InCall

VoicePrivacy is disabled

D/RILJ (211): [5619]< GET_CURRENT_CALLS [id=1,ACTIVE,toa=129,norm,mo,0,voc,

noevp,,cli=1,,0]

D/RILJ (211): [5620]> SET_MUTE false

D/RIL (35): onRequest: SET_MUTE

D/RILJ (211): [5620]< SET_MUTE error: com.android.internal.telephony.Comman dException: REQUEST_NOT_SUPPORTED

D/RILJ (211): [5621]> SET_MUTE false

D/RIL (35): onRequest: SET_MUTE

D/RILJ (211): [5621]< SET_MUTE error: com.android.internal.telephony.Comman dException: REQUEST_NOT_SUPPORTED

D/GSM (211): [GSMConn] update: parent=ACTIVE, hasNewParent=false, wasConne ctingInOrOut=true, wasHolding=false, isConnectingInOrOut=false, changed=true D/GSM (211): [GSMConn] onConnectedInOrOut: connectTime=1340519396496 D/GSM (211): [GSMConn] releaseWakeLock

D/PHONE (211): VM: PhoneSubInfo.getVoiceMailNUmber: D/RILJ (211): [5622]> SET_MUTE false

D/RIL (35): onRequest: SET_MUTE

D/RILJ (211): [5622]< SET_MUTE error: com.android.internal.telephony.Comman dException: REQUEST_NOT_SUPPORTED

D/RILJ (211): [5623]> SET_MUTE false

D/RIL (35): onRequest: SET_MUTE

D/RILJ (211): [5623]< SET_MUTE error: com.android.internal.telephony.Comman dException: REQUEST_NOT_SUPPORTED

D/RILJ (211): [5624]> SIGNAL_STRENGTH D/RIL (35): onRequest: SIGNAL_STRENGTH D/AT (35): AT> AT+CSQ

D/AT (35): AT< +CSQ: 7,99 D/AT (35): AT< OK

4. Analizar la información en línea de los eventos utilizando el comando logcat. Se pueden observar las acciones INSERT y SELECT en las bases de datos, por ejemplo en la de mmssms.db en donde se almacenan los mensajes de textos:

$adb shell logcat –b events

5. Analizar la información de los servicios, memoria, identificadores de

procesos (PID), bases de datos, cuentas de acceso a redes sociales, correos electrónicos, fecha y hora y otros elementos del sistema con el comando dumpsys. El resultado es del emulador Android:

$adb shell dumpsys, o enviar el resultado a un archivo de texto.

$adb shell dumpsys > dumpsys.txt, para su análisis detallado.

Analizar el contenido del archivo dumpsys.txt y obtener información de las diferentes secciones del archivo:

· Los servicios en ejecución:

Currently running services: SurfaceFlinger accessibility account activity alarm appwidget audio backup battery batteryinfo clipboard connectivity content country_detector cpuinfo device_policy devicestoragemonitor diskstats dropbox entropy gfxinfo hardware input_method iphonesubinfo isms location media.audio_flinger media.audio_policy media.camera media.player meminfo mount netpolicy netstats network_ management notification package permission phone power samplingprofiler search sensorservice simphonebook statusbar telephony.registry textservices throttle uimode usagestats USB vibrator wallpaper wifi wifip2p window

· Las cuentas:

DUMP OF SERVICE account: Accounts: 3

· Sincronizaciones: Recent Sync History

#1:

· La información del celular, irónicamente denominada iphonesubinfo, que no tiene relación con el dispositivo de Apple:

DUMP OF SERVICE iphonesubinfo: Phone Subscriber Info: Phone Type = GSM Device ID = 000000000000000

El Device ID no es el número de serie del dispositivo, pero sí el identificador del equipo móvil (MEID – IMEI), el cual identifica unívocamente al dispositivo en la red del proveedor CDMA.

· La ubicación del servicio que muestra la información de la última ubicación del dispositivo y la fecha y hora en formato Unix Epoch:

DUMP OF SERVICE location: Last Known Location:

Passive: Gps:

· Estado de la red del proveedor y de las torres de las celdas de telefonía móvil: Network Internal State:

· Estado de la memoria distribuida por procesos (PID) para determinar los procesos y bases de datos que se acceden:

** MEMINFO in pid 343 [com.android.providers.calendar] ** Shared Private Heap Heap Heap

Pss Dirty Dirty Size Alloc Free
----------Native 1194 1004 1136 3632 3410 125
Dalvik 1455 11420 848 9607 9215 392
Cursor 0 0 0
Ashmem 0 0 0
Other dev 4 0 0
.so mmap 764 1824 244
.jar mmap 4 0 0
.apk mmap 23 0 0
.ttf mmap 0 0 0
.dex mmap 689 0 0
Other mmap 28 12 20
Unknown 551 672 508
TOTAL 4712 14932 2756 13239 12625 517
Objects
Views: 0 ViewRootImpl: 0
AppContexts: 2 Activities: 0
Assets: 2 AssetManagers: 2
Local Binders: 8 Proxy Binders: 13
Death Recipients: 0
OpenSSL Sockets: 0 SQL
heap: 146 MEMORY_USED: 146
PAGECACHE_OVERFLOW: 24 MALLOC_SIZE: 46
Databases
pgsz dbsz Lookaside(b) cache Dbname 1 36 166 37/31/13 calendar.db

6. Analizar la información del estado del sistema con el comando dumpstate. El resultado parcial es del emulador Android:

$adb shell dumpstate, o enviar el resultado a un archivo de texto.
$adb shell dumpstate > dumpstate.txt, para su análisis detallado.

==========
== dumpstate: 2012-06-25 01:07:21
==========
Build: google_sdk-eng 4.0.4 MR1 302030 test-keys Bootloader: unknown
Radio: unknown Network: Android
Kernel: Linux version 2.6.29-g46b05b2 (vchtchetkine@vc-irv.irv.corp.google.com) (gcc version 4.4.3 (GCC)) #28 Thu Nov 17 06:39:36

PST 2011

Command line: qemu.gles=0 qemu=1 console=ttyS0 android.qemud=ttyS1 android. checkjni=1 ndns=3

-----UPTIME (uptime) -----up time: 01:25:33, idle time: 00:00:00, sleep time: 00:00:00 [uptime: 0.2s elapsed]

-----MEMORY INFO (/proc/meminfo) -----
MemTotal: 516312 kB

MemFree: 278028 kB

Buffers: 100 kB

Cached: 117304 kB

El resultado muestra la información por secciones que en su mayoría son obtenidas del pseudo directorio de procesos /proc. El perito puede analizar en forma individual cada uno de los subdirectorios y archivos del directorio /proc o analizar las secciones del comando dumpstate. A continuación se muestra el listado del contenido del directorio

/proc, exceptuando los directorios correspondientes a cada proceso:

$ adb shell ls /proc

- binder
- buddyinfo
- bus
- cgroups
- cmdline
- config.gz
- cpu
- cpuinfo
- crypto
- devices
- diskstats
- driver
- execdomains
- fb
- filesystems
- fs
- interrupts

- iomem
- ioports
- irq
- kallsyms
- kmsg
- kpagecount
- kpageflags
- loadavg
- locks
-

- meminfo
- misc
- mounts
- mtd
- net
- pagetypeinfo
- partitions
- sched_debug
- schedstat
- self
- slabinfo
- stat
- swaps
- sys
- sysrq-trigger
- sysvipc
- timer_list
- tty
- uptime
- version
- vmallocinfo
- vmstat
- wakelocks
- yaffs
- zoneinfo
-

7. Analizar la información del estado del sistema con el comando bugreport que efectúa una combinación de los comandos logcat, dumpsys y dumpstate en un solo comando. El resultado parcial es del emulador Android:

$adb shell bugreport, o enviar el resultado a un archivo de texto.

$wc –l bugreport.log, muestra la cantidad de líneas del archivo.

$adb shell dumpstate > dumpstate.txt, para su análisis detallado.

8. Registrar, documentar y/o capturar pantallas con la información requerida.

Procedimiento para descargar la memoria rAM en Android[157]

Este procedimiento es solo para realizar como prueba en el laboratorio y aprendizaje del perito ya que requiere la modificación de los datos del dispositivo. Android posee un mecanismo que permite descargar la memoria RAM en un archivo enviando una señal Unix del tipo SIGUSR1. En la estación de telefonía forense, conectarse al emulador del dispositivo Android con el demonio adb y en forma interactiva con el dispositivo y con permisos de usuario root, cambiar los permisos de lectura, escritura y ejecución para el usuario, grupo y otros del directorio /data/misc, para que se escriba el archivo de la descarga de la memoria RAM:

$adb shell

$su

#chmod 777 /data/misc

drwxrwxrwx system misc 2012-06-17 22:04 misc

Buscar el identificador de un proceso para enviar la señal SIGUSR1.

#ps

USER PID PPID VSIZE RSS WCHAN PC NAME

root 1 0 276 188 c0099f1c 000086e8 S /init

root 2 0 0 0 c004df64 00000000 S kthreadd

root 3 2 0 0 c003fa28 00000000 S ksoftirqd/0

root 4 2 0 0 c004abc0 00000000 S events/0

root 5 2 0 0 c004abc0 00000000 S khelper

system 213 37 163184 31996 ffffffff 400113c0 S com.android.settings

app_0 233 37 175940 37924 ffffffff 400113c0 S android.process.acore

app_4 268 37 162336 31980 ffffffff 400113c0 S com.android.calendar

app_11 297 37 161520 31448 ffffffff 400113c0 S com.android.deskclock

app_5 325 37 160268 32020 ffffffff 400113c0 S com.android.providers.calendar

app_0 340 37 162796 32408 ffffffff 400113c0 S com.android.contacts

app_13 369 37 160588 33188 ffffffff 400113c0 S android.process.media

app_14 386 37 171192 33448 ffffffff 400113c0 S com.android.email

app_24 427 37 163816 33296 ffffffff 400113c0 S com.google.android.apps.maps:FriendService

app_24 481 37 166996 34900 ffffffff 400113c0 S com.google.android.apps.maps:

LocationFriendService

root 586 1 640 288 c01abd48 4000cf98 S /system/bin/debuggerd

app_24 606 37 176340 36088 ffffffff 400113c0 S com.google.android.apps.maps

root 641 45 704 324 c003d800 4000d284 S /system/bin/sh

root 643 641 900 348 00000000 40010458 R ps

El resultado muestra un extracto del listado de los procesos en el dispositivo Android. Seleccionar un identificador de proceso (PID), por ejemplo 386 y enviar la señal SIGUSR1 con el comando kill:

#kill -10 386

En el directorio /data/misc, aparecerá un archivo con el contenido de la memoria descargada del tipo:

#ls –l /data/misc

heap-dump-tm1234567890-pid386.hprof

Descargar el archivo a la estación de trabajo de telefonía forense con el servicio adb: perito@telefoniaforense#./adb pull /data/misc/ heap-dump-tm1234567890-pid386.

hprof

Analizar el archivo con un visor en hexadecimal o con el comando strings para extraer cadenas de caracteres ASCII.

perito@telefoniaforense#strings heap-dump-tm1234567890-pid386.hprof > mail.txt Posteriormente, editar el archivo y analizar el contenido.

Procedimiento para el análisis de la línea de tiempo en yAFFs2[158]

Consideraciones previas

La fuente de información de la línea de tiempo se encuentra en los metadatos del sistema de archivo: Modificados, Accedidos, Cambiados y Creados (MAC). En el sistema de archivo YAFFS2 es más difícil obtenerla, ya que actualmente no existen herramientas que soporten a este sistema de archivo para poder crear una línea de tiempo. En cambio, en las tarjetas SD y eMMC con sistemas de archivos FAT16 o FAT32, es posible crear una línea de tiempo.

Procedimiento para el análisis del sistema de archivos yAFFs2 con las áreas de reserva OOB

Consideraciones previas

La dificultad existe en el montaje de la imagen para visualizar el sistema de archivos YAFFS2; una de las formas de hacerlo es obtener un kernel de Linux que soporte este sistema de archivos. Los archivos asignados en el dispositivo

pueden copiarse y analizarse por separado, por ejemplo, los contenidos del directorio /data/data pueden copiarse desde el dispositivo Android y analizar el contenido en la estación de trabajo de telefonía forense.

1. Verificar las particiones del sistema de archivo del dispositivo Android, en la estación de trabajo de telefonía forense, abrir una terminal y ejecutar el demonio adb y el comando mount (resultado obtenido del emulador Android):

$adb shell

mount

rootfs / rootfs ro 0 0

tmpfs /dev tmpfs rw,nosuid,mode=755 0 0

devpts /dev/pts devpts rw,mode=600 0 0

proc /proc proc rw 0 0

sysfs /sys sysfs rw 0 0

none /acct cgroup rw,cpuacct 0 0

tmpfs /mnt/asec tmpfs rw,mode=755,gid=1000 0 0

tmpfs /mnt/obb tmpfs rw,mode=755,gid=1000 0 0

none /dev/cpuctl cgroup rw,cpu 0 0

/dev/block/mtdblock0 /system yaffs2 ro 0 0

/dev/block/mtdblock1 /data yaffs2 rw,nosuid,nodev 0 0

/dev/block/mtdblock2 /cache yaffs2 rw,nosuid,nodev 0 0

Otro ejemplo obtenido con el emulador de Android: rootfs / rootfs ro 0 0

tmpfs /dev tmpfs rw,nosuid,mode=755 0 0

devpts /dev/pts devpts rw,mode=600 0 0

proc /proc proc rw 0 0

sysfs /sys sysfs rw 0 0

none /acct cgroup rw,cpuacct 0 0

tmpfs /mnt/asec tmpfs rw,mode=755,gid=1000 0 0

tmpfs /mnt/obb tmpfs rw,mode=755,gid=1000 0 0

none /dev/cpuctl cgroup rw,cpu 0 0

/dev/block/mtdblock0 /system yaffs2 ro 0 0

/dev/block/mtdblock1 /data yaffs2 rw,nosuid,nodev 0 0

/dev/block/mtdblock2 /cache yaffs2 rw,nosuid,nodev 0 0

/dev/block/vold/179:0 /mnt/sdcard vfat rw,dirsync,nosuid,nodev,noexec,uid=1000, g id=1015,fmask=0702,dmask=0702,allow_utime=0020,codepage=cp437,iocha iso8859-1,shortname=mixed,utf8,errors=remount-ro 0 0

/dev/block/vold/179:0 /mnt/secure/asec vfat rw,dirsync,nosuid,nodev,noexec,uid=1 000,gid=1015,fmask=0702,dmask=0702,allow_utime=0020,codepage=cp437 set=iso

8859-1,shortname=mixed,utf8,errors=remount-ro 0 0

tmpfs /mnt/sdcard/.android_secure tmpfs ro,size=0k,mode=000 0 0

2. Analizar el pseudo sistema de archivos /proc; utilizar el comando cat para visualizar el contenido de los archivos y estadísticas del sistema:

#ls –l /proc, listar el contenido.

cat /proc/partitions, visualizar las particiones. cat partitions

major minor #blocks name

31 0 155904 mtdblock0

31 1 127104 mtdblock1

31 2 65536 mtdblock2

179 0 9216 mmcblk0

3. Analizar el sistema de archivos YAFFS2 montado en /data/data, que contiene las aplicaciones:

ls /data/data

4. Analizar sistema de archivos YAFFS2/Ext3 montado en caché, que contiene información utilizada por ciertas aplicaciones y el sistema.

5. Analizar sistema de archivos tmpfs montado en /mnt/asec, que contiene aplicaciones descifradas, archivos .apk, los cuales se guardan cifrados en la tarjeta SD; aquí se desencriptan para utilizar las aplicaciones.

6. Analizar sistema de archivos tmpfs montado en /app-cache, sistema de archivo temporal donde com.android.browser (en HTC Incredible) guarda la caché.

7. Analizar sistema de archivos vfat montado en /mnt/sdcard, que contiene la tarjeta removible SD.

8. Analizar sistema de archivos vfat montado en /mnt/emmc, que contiene la tarjeta multimedia embebida eMMC.

9. Registrar, documentar y/o capturar pantallas con la información requerida.

Procedimiento para el análisis de fragmentos

(carving) del sistema de archivos

1. Instalar la herramienta scalpel en la estación de trabajo de telefonía forense (con sistema operativo Linux):

$sudo apt-get install scalpel

cd directorio_de_descarga_de_scalpel tar xzvf scalpel-1.60.tar.gz

cd scalpel-1.60 make

El comando scalpel tiene un archivo de configuración que se puede editar y agregar firmas de archivos.

Verificar el uso del comando scalpel explicado anteriormente en los procedimientos de análisis en iPhone.

El comando file en Linux permite determinar el tipo de archivo.

2. Registrar, documentar y/o capturar pantallas con la información requerida.

Procedimiento para el análisis del sistema de archivos con el comando strings

1. Analizar los archivos de texto, binarios con la herramienta strings.

$strings –all –radix=x mtd5.dd | less

El resultado puede mostrar datos no enlazados, borrados o bases de datos modificadas, creando archivos de actualización. Aparecen archivos de instantáneas tomadas de SQLite y cuyos valores se almacenaron en la memoria Flash NAND.

$ strings –all –radix=x –encoding=b mtd5.dd | less

El resultado muestra partes del texto que pueden ser visualizadas en un editor en hexadecimal; pueden observarse fechas y horas en el formato Unix Epoch que requieren ser convertidas con el convertidor en línea. También pueden encontrarse valores de coordenadas de latitud y longitud.

2. Visualizar el contenido con un visor en hexadecimal.

3. Registrar, documentar y/o capturar pantallas con la información requerida.

Procedimiento para el análisis del sistema de archivos con el visor en hexadecimal ncurseshexedit[159]

El editor en hexadecimal ncurses con licencia GNU GPL permite editar cualquier archivo como byte (octeto, ocho bits), visualizar y editar el disco rígido en los sistemas operativos Linux.

1. En la estación de trabajo de telefonía forense, descargar

ftp://ftp.gnu.org/pub/gnu/ ncurses/) e instalar ncurses-hexedit:

$sudo apt-get install ncurses-hexedit

2. Ejecutar el comando strings para visualizar la base de datos de mmssms.db que se encuentra en /data/data/com.android.providers.telephony/databases, para verificar si se ha borrado algún mensaje de texto proveniente de un número de teléfono determinado, en el archivo de la base de datos de SQLite:

$adb shell

ls -l data/data/com.android.providers.telephony/databases ls -l data/data/com.android.providers.telephony/databases

-rw-rw---radio radio 38912 2012-06-20 19:58 mmssms.db

-rw-rw---radio radio 4096 2012-06-22 21:54 telephony.db

-rw-rw---radio radio 0 2012-06-22 21:54 telephony.db-journal

$strings –all –radix=x mmssms.db | grep nrodetelefono | wc –l

El resultado muestra el número de teléfono filtrado con el comando grep, pero se pueden crear con esta estructura otras consultas similares. La salida del resultado de utilizar grep es la entrada de otro comando, wc, que cuenta las líneas en que aparece el número de teléfono ingresado.

$strings –all –radix=x mmssms.db | grep –A 1 nrodetelefono | less

En este comando, se reemplaza el comando de contar líneas wc incluyendo una línea de texto después del número de teléfono, filtrando A 1 y mostrando la salida por pantalla con el comando less. El resultado muestra el número de teléfono y a continuación la línea de texto.

3. Analizar la base de datos con la línea de comandos de SQLite:

$sqlite3 mmssms.db; abre la base de datos para consulta. SQLite version 3.7.4

Enter ".help" for instructions

Enter SQL statements terminated with a ";"

sqlite>.tables; lista las tablas de la base de datos. addr pdu threads

android_metadata pending_msgs words attachments rate words_content canonical_addresses raw words_segdir drm sms words_segments

part sr_pending

sqlite>.schema.sms; solicita la estructura o esquema de la tabla sms.

CREATE TABLE sms (_id INTEGER PRIMARY KEY,thread_id INTEGER,address TEXT,person INTEGER,date INTEGER,date_sent INTEGER DEFAULT 0,protocol INTEGER,read INTEGER DEFAULT 0,status INTEGER DEFAULT -1,type INTEGER,reply_

path_present INTEGER,subject TEXT,body TEXT,service_center TEXT,locked INTEGER DEFAULT 0,error_code INTEGER DEFAULT 0,seen INTEGER DEFAULT 0);

CREATE INDEX typeThreadIdIndex ON sms (type, thread_id);

CREATE TRIGGER sms_update_thread_date_subject_on_update AFTER UPDATE OF date, body, type ON sms BEGIN UPDATE threads SET date = (strftime('%s','now') * 1000), snippet = new.body, snippet_cs = 0 WHERE threads._id = new.thread_

id; UPDATE threads SET message_count = (SELECT COUNT(sms._id) FROM sms LE FT JOIN threads ON threads._id = thread_id WHERE thread_id = new.thre

ad_id AND sms.type != 3) + (SELECT COUNT(pdu._id) FROM pdu LEFT JOIN threads ON threads._id = thread_id WHERE thread_id = new.thread_id

AND (m_type=132 OR m_type=130 OR m_type=128) AND msg_box != 3) WH ERE threads._id = new.thread_id; UPDATE threads SET read = CASE (SELECT CO UNT(*) FROM sms WHERE read = 0 AND thread_id = thre

ads._id) WHEN 0 THEN 1 ELSE 0 END WHERE threads._id = new.thread_id; END; CREATE TRIGGER sms_update_thread_on_insert AFTER INSERT ON sms BEGIN UPDATE threads SET date = (strftime('%s','now') * 1000), snippet = new.body, sn ippet_cs = 0 WHERE threads._id = new.thread_id; UPDATE threads SET message_co unt = (SELECT COUNT(sms._id) FROM sms LEFT JOIN threads ON threads._i

d = thread_id WHERE thread_id = new.thread_id AND sms.type != 3) + (SELECT COUNT(pdu._id) FROM pdu LEFT JOIN threads ON threads._id = thr ead_id WHERE thread_id = new.thread_id AND (m_type=132 OR m_type=130 OR m_type=128) AND msg_box != 3) WHERE threads._id = new.thread_id;

UPDATE threads SET read = CASE (SELECT COUNT(*) FROM sms WHERE read = 0 AND thread_id = threads._id) WHEN 0 THEN 1 ELSE 0 END WHERE threads._id = new. thread_id; END;

CREATE TRIGGER sms_update_thread_read_on_update AFTER UPDATE OF read ON

sms BEGIN UPDATE threads SET read = CASE (SELECT COUNT(*) FROM sms WHERE read = 0 AND thread_id = threads._id) WHEN 0 THEN 1

ELSE 0 END WHERE threads._id = new.thread_id; END;

CREATE TRIGGER sms_words_delete AFTER DELETE ON sms BEGIN DELETE FROM words WHERE source_id = OLD._id AND table_to_use = 1; END;

CREATE TRIGGER sms_words_update AFTER UPDATE ON sms BEGIN UPDATE words SET index_text = NEW.body WHERE (source_id=NEW._id AND table_to_use=1); END; CREATE TRIGGER update_threads_error_on_update_sms AFTER UPDATE OF type ON sms WHEN (OLD.type != 5 AND NEW.type = 5) OR (OLD.type = 5 AND NEW.type != 5) BEGIN UPDATE threads SET error = CASE WHEN NEW.type = 5 THEN error + 1

ELSE error 1 END WHERE _id = NEW.thread_id; END; sqlite>.mode line; configura el modo de visualización por línea.

sqlite>select * from sms limit 1; muestra un registro de la tabla sms por columnas.

_id = 1

thread_id = 1

address = 1 234-56 person =

date = 1339887299952

date_sent = 0 protocol = read = 1

status = -1

type = 2 eply_path_present = subject =

body = Hola service_center = locked = 0

error_code = 0

seen = 1

sqlite>.quit; salir de la aplicación.

El resultado muestra que existe un número de campos en la tabla sms, el campo posterior al del número de teléfono muestra un identificador de persona seguido de la fecha y hora (1339887299952). Utilizar el editor en hexadecimal para determinar la fecha y hora del mensaje con el texto filtrado A 1.

$hexeditor mmssms.db

El resultado muestra el inicio del archivo de la base de datos en hexadecimal y con las cadenas de caracteres ASCII.

Oprimir las teclas Ctrl + T. Se puede saltar a otra posición en el editor, en este caso al valor obtenido con el comando strings radix=x, aparecerá el número de teléfono, luego el campo persona y finalmente se verá una secuencia de números que traducida a decimal sería la fecha y hora en formato Unix Epoch o en milisegundos. El comando date de Linux permite convertir a segundos, por lo tanto, omitir los últimos tres dígitos:

$date –d @1339887299

sáb jun 22:54:59 UTC 2012.

4. Registrar, documentar y/o capturar pantallas con la información requerida.

Procedimiento para el análisis del contenido de los directorios del sistema de archivos de Android

1. Listar la estructura de directorios de Android, el resultado varía según el modelo del fabricante. Ejemplo obtenido del emulador Android:

$ls -la

drwxr-xr-x root root 2012-06-22 21:53 acct

drwxrwx--system cache 2012-06-22 01:34 cache

dr-x-----root root 2012-06-22 21:53 config

lrwxrwxrwx root root 2012-06-22 21:53 d -> /sys/kernel/debug drwxrwx--x system system 2012-06-16 20:20 data

-rw-r--r-root root 116 1970-01-01 00:00 default.prop

drwxr-xr-x root root 2012-06-22 21:53 dev

lrwxrwxrwx root root 2012-06-22 21:53 etc -> /system/etc

-rwxr-x--root root 98676 1970-01-01 00:00 init

-rwxr-x--root root 2344 1970-01-01 00:00 init.goldfish.rc

-rwxr-x--root root 17105 1970-01-01 00:00 init.rc

drwxrwxr-x root system 2012-06-22 21:53 mnt

dr-xr-xr-x root root 1970-01-01 00:00 proc

drwx-----root root 2011-11-14 19:00 root

drwxr-x--root root 1970-01-01 00:00 sbin

lrwxrwxrwx root root 2012-06-22 21:53 sdcard -> /mnt/sdcard drwxr-xr-x root root 1970-01-01 00:00 sys

drwxr-xr-x root root 2012-03-27 23:21 system

-rw-r--r-root root 272 1970-01-01 00:00 ueventd.goldfish.rc

-rw-r--r-root root 3825 1970-01-01 00:00 ueventd.rc

lrwxrwxrwx root root 2012-06-22 21:53 vendor -> /system/vendor

Los siguientes directorios contienen información de interés para el perito; deberá analizarlos y correlacionarlos.

2. Analizar el directorio /cache:

$ls –l /cache

drwx-----system system 2012-06-21 00:17 backup

drwxrwx--root root 2012-06-16 20:18 lost+found

$ls –l /cache/backup

@pm@ android

com.android.calendar com.android.providers.settings

3. Analizar el directorio /data; contiene información de interés:

$ls -l

drwxrwxr-x system system 2012-06-22 21:54 anr

drwxrwx--x system system 2012-06-16 23:31 app

drwxrwx--x system system 2012-06-16 20:18 app-private

drwx-----system system 2012-06-22 21:54 backup

drwxrwx--x system system 2012-06-16 23:31 dalvik-cache

drwxrwx--x system system 2012-06-20 20:45 data

drwxr-x--root log 2012-06-16 20:18 dontpanic

drwxrwx--drm drm 2012-06-16 20:18 drm

drwxr-x--x root root 2012-06-16 20:18 local

drwxrwx--root root 2012-06-16 20:18 lost+found

drwxrwx--t system misc 2012-06-16 20:18 misc

drwxrwx--x system system 2012-03-27 23:21 nativebenchmark

drwxrwx--x system system 2012-03-27 23:21 nativetest

drwx-----root root 2012-06-22 21:54 property

drwxrwx--x system system 2012-06-16 20:18 resource-cache

drwxrwxr-x system system 2012-06-23 01:23 system

drwxr-xr-x system system 2012-06-16 20:18 user

Subdirectorio /data/anr: Información de trazas de depuración.

$ls -l anr

-rw-rw-rwsystem system 7688 2012-06-22 21:54 slow00.txt

-rw-rw-rwsystem system 7684 2012-06-22 21:54 slow01.txt

-rw-rw-rwsystem system 6436 2012-06-22 21:54 slow02.txt

-rw-rw-rwsystem system 7585 2012-06-22 21:54 slow03.txt

-rw-rw-rwsystem system 7300 2012-06-22 21:54 slow04.txt

-rw-rw-rwsystem system 8299 2012-06-22 21:54 slow05.txt

-rw-rw-rwsystem system 8172 2012-06-22 21:54 slow06.txt

-rw-rw-rwsystem system 7696 2012-06-22 21:54 slow07.txt

-rw-rw-rwsystem system 8196 2012-06-22 21:54 slow08.txt

-rw-rw-rwsystem system 7681 2012-06-22 21:54 slow09.txt

-rw-rw-rwsystem system 167259 2012-06-17 02:58 traces.txt

Subdirectorio /data/app: Contiene los archivos .apk descargados del sitio de aplicaciones de Android y otras descargas:

$ ls -l /data/app

-rw-r--r-system system 2720164 2012-03-27 23:25 ApiDemos.apk

-rw-r--r-system system 857848 2012-03-27 23:25 ApiDemos.odex

-rw-r--r-system system 13234 2012-03-27 23:25 CubeLiveWallpapers.apk

-rw-r--r-system system 16536 2012-03-27 23:25 CubeLiveWallpapers.odex

-rw-r--r-system system 18016 2012-03-27 23:25 GestureBuilder.apk

-rw-r--r-system system 22840 2012-03-27 23:25 GestureBuilder.odex

-rw-r--r-system system 31383 2012-03-27 23:25 SoftKeyboard.apk

-rw-r--r-system system 32296 2012-03-27 23:25 SoftKeyboard.odex

-rw-r--r-system system 14241 2012-03-27 23:25 WidgetPreview.apk

-rw-r--r-system system 12952 2012-03-27 23:25 WidgetPreview.odex

-rw-r--r-system system 28794 2012-06-16 23:31 com.viaforensics.android.aflogical_ose-1.apk

Subdirectorio /data/app-private: Contiene aplicaciones protegidas descargadas del sitio de aplicaciones de Android.

Subdirectorio /data/backup: Maneja y coloca en la cola los resguardos procedentes de la copia segura remota (cloud o nube):

$ ls -l /data/backup

-rw------system system 24 2012-06-21 00:17 ancestral

drwx-----system system 2012-06-21 01:20 com.androi up.LocalTransport

drwx-----system system 2012-06-21 01:20 pending

-rw------system system 186 2012-06-22 21:54 processed

Subdirectorio /data/davlik-cache: Contiene los archivos de la máquina virtual Davlik, utilizados para ejecutar las aplicaciones.

$ ls -l /data/davlik-cache

-rw-r--r-system app_40 39880 2012-06-16 23:31 data@app@

.android.aflogical_ose-1.apk@classes.dex

Subdirectorio /data/data: Contiene los datos de las aplicaciones (por ejemplo, Facebook); es el directorio más importante en donde el perito debe orientar el análisis.

$ ls -l /data/data

drwxrwxr-x root root 2012-06-20 20:38 app_parts

drwxr-x--x app_20 app_20 2012-06-16 20:19 com.android.backupconfirm

drwxr-x--x app_2 app_2 2012-06-16 20:22 com.android.browser

drwxr-x--x app_16 app_16 2012-06-16 20:19 com.android.calculator2

drwxr-x--x app_21 app_21 2012-06-16 20:20 com.android.calendar

drwxr-x--x app_9 app_9 2012-06-16 22:55 com.android.camera

drwxr-x--x app_30 app_30 2012-06-16 20:19 com.android.certinstaller
drwxr-x--x app_1 app_1 2012-06-16 22:53 com.android.contacts
drwxr-x--x app_5 app_5 2012-06-16 22:00 com.android.customlocale2
drwxr-x--x app_3 app_3 2012-06-16 20:25 com.android.defcontainer
drwxr-x--x app_34 app_34 2012-06-16 20:21 com.android.deskclock
drwxr-x--x app_32 app_32 2012-06-16 23:44 com.android.development
drwxr-x--x app_27 app_27 2012-06-16 20:21 com.android.email
drwxr-x--x app_24 app_24 2012-06-16 20:19 com.android.emulator.connectivity.test
drwxr-x--x app_4 app_4 2012-06-16 20:19 com.android.emulator.gps.test
drwxr-x--x app_17 app_17 2012-06-16 20:21 com.android.exchange
drwxr-x--x app_0 app_0 2012-06-16 20:19 com.android.fallback
drwxr-x--x app_7 app_7 2012-06-16 20:19 com.android.gallery
drwxr-x--x app_35 app_35 2012-06-16 20:20 com.android.gesture.builder
drwxr-x--x app_18 app_18 2012-06-16 20:19 com.android.htmlviewer
drwxr-x--x app_6 app_6 2012-06-16 20:20 com.android.inputmethod.latin
drwxr-x--x app_10 app_10 2012-06-16 20:19 com.android.inputmethod.pinyin
drwxr-x--x system system 2012-06-16 20:19 com.android.keychain
drwxr-x--x app_13 app_13 2012-06-16 20:21 com.android.launcher
drwxr-x--x app_28 app_28 2012-06-16 20:21 com.android.mms
drwxr-x--x app_22 app_22 2012-06-16 20:19 com.android.music
drwxr-x--x app_8 app_8 2012-06-16 20:19 com.android.netspeed
drwxr-x--x app_19 app_19 2012-06-16 20:19 com.android.packageinstaller
drwxr-x--x radio radio 2012-06-16 20:20 com.android.phone
drwxr-x--x app_31 app_31 2012-06-16 20:19 com.android.protips
drwxr-x--x app_1 app_1 2012-06-16 20:19 com.android.providers.applications
drwxr-x--x app_11 app_11 2012-06-16 20:20 com.android.providers.calendar
drwxr-x--x app_1 app_1 2012-06-16 20:20 com.android.providers.contacts
drwxr-x--x app_7 app_7 2012-06-16 20:21 com.android.providers.downloads
drwxr-x--x app_7 app_7 2012-06-16 20:19 com.android.providers.downloads.ui
drwxr-x--x app_7 app_7 2012-06-16 20:19 com.android.providers.drm

drwxr-x--x app_7 app_7 2012-06-16 20:20 com.android.providers.media
drwxr-x--x system system 2012-06-16 20:20 com.android.providers.settings
drwxr-x--x radio radio 2012-06-16 22:55 com.android.providers.telephony
drwxr-x--x app_1 app_1 2012-06-16 20:20 com.android.providers.userdictionary
drwxr-x--x app_33 app_33 2012-06-16 20:21 com.android.quicksearchbox
drwxr-x--x app_15 app_15 2012-06-16 20:20 com.android.sdksetup
drwxr-x--x system system 2012-06-16 20:35 com.android.settings
drwxr-x--x app_14 app_14 2012-06-17 08:22 com.android.sharedstoragebackup
drwxr-x--x app_25 app_25 2012-06-16 20:19 com.android.soundrecorder
drwxr-x--x app_12 app_12 2012-06-16 20:19 com.android.speechrecorder
drwxr-x--x system system 2012-06-16 20:19 com.android.systemui
drwxr-x--x system system 2012-06-16 20:19 com.android.vpndialogs
drwxr-x--x app_29 app_29 2012-06-16 20:19 com.android.wallpaper.livepicker
drwxr-x--x app_36 app_36 2012-06-16 20:20 com.android.widgetpreview
drwxr-x--x app_37 app_37 2012-06-17 01:56 com.example.android.apis
drwxr-x--x app_39 app_39 2012-06-16 20:20 com.example.android.livecubes
drwxr-x--x app_38 app_38 2012-06-16 20:20 com.example.android.softkeyboard
drwxr-x--x system system 2012-06-16 20:19 com.motorola.pgmsystem
drwxr-x--x radio radio 2012-06-16 20:19 com.motorola.programmenu
drwxr-x--x app_23 app_23 2012-06-16 23:31 com.svox.pico
drwxr-x--x app_40 app_40 2012-06-16 23:45 com.viaforensics.android.aflogical_ose

drwxrwxr-x root root 2012-06-20 20:38 databases

drwxr-x--x app_26 app_26 2012-06-16 20:19 jp.co.omronsoft.openwnn
drwxrwxr-x root root 2012-06-20 20:38 shared_prefs
drwxrwxr-x root root 2012-06-20 20:45 sms
$ ls –l /data/data/databases
-rw-r--r-root root 38912 2012-06-20 20:38 mmssms.db
-rw-r--r-root root 4096 2012-06-20 20:38 telephony.db
-rw-r--r-root root 0 2012-06-20 20:38 telephony.db-journal
Subdirectorio /data/dontpanic: Contiene algunos archivos de registros de

errores del sistema, los cuales pueden ser analizados para determinar el estado del dispositivo.

Subdirectorio /data/local: Es importante porque permite el uso del intérprete de comando (shell) del usuario con acceso en modo lectura y escritura. Cuando se instalan aplicaciones, primero se copian a /data/local, lo mismo ocurre con algunas herramientas de telefonía forense.

ls –l /data/local

drwxrwx--x shell shell 2012-06-16 23:31 tmp

Subdirectorio /data/lost+found: Cualquier archivo o directorio del sistema de archivo YAFFS2 que no encuentre su ruta o path al directorio raíz (/) aparece en este directorio, por ejemplo, se puede efectuar una búsqueda de patrones, como la siguiente:

$grep –R lost+found *.d

Subdirectorio /data/misc: Contiene archivos relacionados con la configuración de las conexiones Bluetooth, inalámbricas, vpn. Un archivo importante de analizar es el archivo que tiene el listado de las conexiones inalámbricas y claves de acceso en texto en claro, wpa_supplicant.conf o softap.conf ubicados en /data/misc/wifi.

$ ls –l /data/misc

drwxrwx--system system 2012-06-16 20:18 bluetooth

drwxrwx--bluetooth bluetooth 2012-06-16 20:18 bluetoothd

drwxrwx--x system system 2012-06-16 20:18 keychain

drwx-----keystore keystore 2012-06-16 20:18 keystore

drwx-----system system 2012-06-16 20:18 systemkeys

drwxrwx--system vpn 2012-06-16 20:18 vpn

drwxrwx--wifi wifi 2012-06-16 20:20 wifi

Subdirectorio /data/property: Contiene propiedades del sistema, como zona horaria, país, idioma.

$ls –l /data/property

rw------root root 0 2012-06-16 22:00 persist.sys.country

rw------root root 2 2012-06-16 22:00 persist.sys.language

rw------root root 0 2012-06-16 22:00 persist.sys.localevar

rw------root root 1 2012-06-22 21:54 persist.sys.profiler_ms

rw------root root 3 2012-06-16 20:20 persist.sys.timezone

$ cat persist.sys.timezone GMT

Subdirectorio /data/system: Contiene archivos importantes. La base de datos accounts.db posee una lista de las cuentas que requieren autenticación y brindan un nombre, tipo y clave cifrada. Otros archivos importantes son los relacionados con el código de acceso y PIN para el dispositivo. Los archivos son gesture.key y password.key, los cuales contienen un valor en hexadecimal encriptado o codificado para el código de acceso.

$ls –l /data/system

-rw-rw---system system 16384 2012-06-20 19:58 accounts.db

-rw------system system 338 2012-06-23 04:10 appwidgets.xml

-rw------system system 13084 2012-06-23 04:09 batterystats.bin

-rw------system system 283 2012-06-16 20:20 called_pre_boots.dat

drwx-----system system 2012-06-23 04:10 dropbox

-rw------system system 4096 2012-06-23 04:09 entropy.dat

drwx-----system system 2012-06-16 20:20 inputmethod

-rw------system system 267 2012-06-16 20:21 netpolicy.xml

-rw-rw-r-system system 301 2012-06-23 04:09 packages-stopped.xml

-rw-rw-r-system system 3355 2012-06-23 04:09 packages.list

-rw-rw-r-system system 53885 2012-06-23 04:09 packages.xml

drwxrwx--x system system 2012-06-16 20:20 registered_services

drwx-----system system 2012-06-23 04:09 sync

drwx-----system system 2012-06-16 20:21 throttle

-rwxrwxr-system system 58 2012-06-16 20:19 uiderrors.txt

drwx-----system system 2012-06-23 04:09 usagestats

drwxrwxr-x system system 2012-06-16 20:19 users

-rw------system system 97 2012-06-23 04:09 wallpaper_info.xml

Subdirectorio /mnt: Directorio donde se montan varios sistemas de archivos, la tarjeta SD y eMMC.

$ls –l /mnt

drwxr-xr-x root system 2012-06-23 04:09 asec

drwxr-xr-x root system 2012-06-23 04:09 obb

d---rwxr-x system sdcard_rw 1970-01-01 00:00 sdcard

drwx-----root root 2012-06-23 04:09 secure

El directorio /mnt/asec contiene las aplicaciones descifradas que son guardadas en la tarjeta SD. Cuando el sistema está funcionando y el acceso a los archivos descifrados es requerido, estos son descifrados y montados en

/mnt/asec.

Subdirectorio /mnt/emmc/DCIM: Contiene álbumes de imágenes en miniatura. Subdirectorio /mnt/emmc/100MEDIA: Contiene imágenes o videos capturados desde

el dispositivo.

Subdirectorio /mnt/LOST.DIR: Contiene fragmentos de particiones FAT32 de las cuales el sistema perdió su seguimiento. El perito debe analizar estos archivos.

Subdirectorio /mnt/sdcard: La tarjeta SD se puede leer o montar a partir de este directorio. Contiene imágenes, videos, música, descargas, etc.

$ls –l /mnt/sdcard

d---rwxr-x system sdcard_rw 2012-06-16 20:21 Alarms

d---rwxr-x system sdcard_rw 2012-06-16 22:55 Android

d---rwxr-x system sdcard_rw 2012-06-16 22:55 DCIM

d---rwxr-x system sdcard_rw 2012-06-16 20:21 Download

d---rwxr-x system sdcard_rw 2012-06-16 20:20 LOST.DIR

d---rwxr-x system sdcard_rw 2012-06-16 20:21 Movies

d---rwxr-x system sdcard_rw 2012-06-16 20:21 Music

d---rwxr-x system sdcard_rw 2012-06-16 20:21 Notifications

d---rwxr-x system sdcard_rw 2012-06-16 20:21 Pictures

d---rwxr-x system sdcard_rw 2012-06-16 20:21 Podcasts

d---rwxr-x system sdcard_rw 2012-06-16 20:21 Ringtones

d---rwxr-x system sdcard_rw 2012-06-17 08:35 userdata

El subdirectorio /mnt/sdcard/DCIM almacena imágenes y videos:

$ls –l /mnt/sdcard/DCIM

---rwxr-x system sdcard_rw 2012-06-16 22:55 100ANDRO

---rwxr-x system sdcard_rw 2012-06-16 22:55 Camera

El subdirectorio /mnt/sdcard/Download contiene música, videos e imágenes descargadas desde el navegador de Internet, desde el correo electrónico y de otras aplicaciones.

Subdirectorio /system/app: Contiene archivos .apk app para aplicaciones que son provistas con el sistema; incluye las aplicaciones de Google/Android del fabricante y del proveedor de red inalámbrica. El perito debe considerar este directorio en el caso de requerir el análisis de archivos app.

$ls –l /system/

drwxr-xr-x root root 2012-03-27 23:27 app

drwxr-xr-x root shell 2012-03-27 23:21 bin
-rw-r--r-root root 1450 2012-03-27 23:08 build.prop
drwxr-xr-x root root 2012-03-27 23:27 etc
drwxr-xr-x root root 2012-03-27 23:12 fonts
drwxr-xr-x root root 2012-03-27 23:25 framework
drwxr-xr-x root root 2012-03-27 23:22 lib
drw-rw-rwroot root 2012-06-23 04:09 lost+found
drwxr-xr-x root root 2012-03-27 23:12 media
drwxr-xr-x root root 2012-03-27 23:12 tts
drwxr-xr-x root root 2012-03-27 23:12 usr
drwxr-xr-x root shell 2012-03-27 23:21 xbin
$ls /system/app/*.apk
/system/app/ApplicationsProvider.apk
/system/app/BackupRestoreConfirmation.apk
/system/app/Browser.apk
/system/app/Calculator.apk
/system/app/Calendar.apk
/system/app/CalendarProvider.apk
/system/app/Camera.apk
/system/app/CertInstaller.apk
/system/app/ConnectivityTest.apk
/system/app/Contacts.apk
/system/app/ContactsProvider.apk
/system/app/CustomLocale.apk
/system/app/DefaultContainerService.apk
/system/app/DeskClock.apk
/system/app/Development.apk
/system/app/DownloadProvider.apk
/system/app/DownloadProviderUi.apk
/system/app/DrmProvider.apk
/system/app/Email.apk
/system/app/Exchange.apk
/system/app/Fallback.apk
/system/app/Gallery.apk

/system/app/GpsLocationTest.apk
/system/app/HTMLViewer.apk
/system/app/KeyChain.apk
/system/app/LatinIME.apk
/system/app/Launcher2.apk
/system/app/LiveWallpapersPicker.apk
/system/app/MediaProvider.apk
/system/app/Mms.apk
/system/app/Music.apk
/system/app/NetSpeed.apk
/system/app/OpenWnn.apk
/system/app/PackageInstaller.apk
/system/app/Phone.apk
/system/app/PicoTts.apk
/system/app/PinyinIME.apk
/system/app/Protips.apk
/system/app/QuickSearchBox.apk
/system/app/SdkSetup.apk
/system/app/Settings.apk
/system/app/SettingsProvider.apk
/system/app/SharedStorageBackup.apk
/system/app/SoundRecorder.apk
/system/app/SpeechRecorder.apk
/system/app/StingrayProgramMenu.apk
/system/app/StingrayProgramMenuSystem.apk
/system/app/SystemUI.apk
/system/app/TelephonyProvider.apk
/system/app/UserDictionaryProvider.apk
/system/app/VpnDialogs.apk

El directorio /system/bin y /system/xbin contiene los archivos binarios de Android utilizados en el sistema. El perito puede encontrar comandos útiles y no documentados (wipe, sdcard, top, etc.).

Subdirectorio /system/etc.: Android guarda la configuración típica de Linux o Unix, donde se encuentran múltiples archivos de configuración para efectuar el análisis respectivo.

$ls –l /system/etc.

-rw-r--r-root root 69064 2012-03-27 23:27 NOTICE.html.gz
-rw-r--r-root root 1471 2012-03-27 23:12 apns-conf.xml
-r--r----bluetooth bluetooth 935 2012-03-27 23:12 dbus.conf
drwxr-xr-x root root 2012-03-27 23:12 dhcpcd
-rw-r--r-root root 12863 2012-03-27 23:08 event-log-tags
-rw-r--r-root root 2689 2012-03-27 23:12 fallback_fonts.xml
-rw-r--r-root root 25 2012-03-27 23:12 hosts
-r-xr-x--root shell 1755 2012-03-27 23:12 init.goldfish.sh
drwxr-xr-x root root 2012-03-27 23:12 permissions
drwxr-xr-x root root 2012-03-27 23:21 ppp
drwxr-xr-x root root 2012-03-27 23:12 security
-rw-r--r-root root 2595 2012-03-27 23:12 system_fonts.xml
-rw-r--r-root root 1093 2012-03-27 23:12 vold.fstab

4. Registrar, documentar y/o capturar pantallas con la información requerida.

Procedimiento para la creación de la línea de tiempo*160* en el sistema de archivos FAT de la tarjeta sD

En la tarjeta SD se encuentra gran cantidad de información de interés para el perito; los datos sincronizados con el dispositivo u obtenidos a partir de este se almacenan en la tarjeta SD (videos, imágenes, grabaciones de voz, música, aplicaciones, datos de Google Map, resguardos de archivos de ciertas aplicaciones). Otra información importante es la relacionada con mms almacenados en caché en imágenes de previsualización en miniatura, archivos o elementos borrados y descarga de aplicaciones .apk.

En el caso de Google Maps, se puede obtener información de la navegación realizada por el usuario en el archivo com.google.apps.maps/cache en la tarjeta SD; con esta información es posible recuperar la imagen de la navegación geográfica y la voz de indicación de los lugares del recorrido, por lo tanto es factible para el perito reproducir el trayecto de la navegación en determinada fecha y hora.

La tarjeta SD puede ser montada a través de Android como un dispositivo externo para la transferencia de archivos entre la tarjeta SD y la computadora.

1. Analizar la línea de tiempo, se puede realizar con Sleuth Kit o con log2timeline; instalar el programa log2timeline en la estación de trabajo de telefonía forense:

$sudo apt-get install log2timeline-perl

Se analizará el archivo de la imagen recolectada de la tarjeta SD imagen_android_SD.dd y verificar el correspondiente valor del hash.

$md5sum imagen_android_SD.dd

Comparar los resultados de la certificación matemática para asegurar que se mantiene la integridad del archivo y verificar el tipo de archivo con el comando file:

$file imagen_android_SD.dd

Verificar la imagen con una partición válida con el comando de Sleuth Kit mmls:

$mmls imagen_android_SD.dd

Verificar el estado de la partición con el comando de Sleuth Kit fsstat, a partir del sector de desplazamiento 129 en donde se inicia la partición:

$fsstat –o 129 imagen_android_SD.dd

Crear la línea de tiempo con el comando de Sleuth Kit fls:

$time fls –z CST6CDT –s 0 –m /mnt/sdcard –f fat16 –r –o 129 –i raw imagen_android_ SD.dd > sdcard.body

Descripción de la línea de comando:

· -z fija la zona horaria.

· -s 0 fija el sesgo o inicio del tiempo.

· -m fija la ruta de escritura del archivo .body.

· –f fat16 fija el tipo de sistema de archivo.

· –r en forma recursiva en todos los directorios crea la línea de tiempo.

· -i raw configura el tipo de archivo de la imagen.

· > redirecciona la salida del comando a un archivo en vez de aparecer en pantalla.

Verificar las líneas de entrada para la línea de tiempo que se encuentran en el archivo sdcard.body:

$wc –l sdcard.body

Montar el sistema de archivo utilizando la imagen dd y se debe usar un dispositivo especial loopback:

$mkdir –p /mnt/sdcard

$sudo mount –t vfat –o loop, ro, offset=66068 / imagen_android_SD.dd /mnt/sdcard

Descripción de la línea de comando:

· –o loop, ro, offset=66068*161*, indica al comando mount que utilice un dispositivo de loopback, ya que se está utilizando un archivo físico en vez del dispositivo actual, ro, monta en modo solo lectura y se calcula el tamaño del

sector de 512 x 129 = 66068.

Verificar si se ha montado correctamente con el comando mount que devuelve el listado de los dispositivos montados, filtrado por el tipo de partición (vfat) y verificar el tamaño de la partición con el comando df:

$mount | grep vfat

$df –h

El resultado muestra el tamaño del dispositivo /dev/loop0 que se encuentra montado en /mnt/sdcard.

Ejecutar el comando log2timeline para analizar la línea de tiempo:

$time timescanner –d /mnt/sdcard –z GMT >> sdcard.body

En el argumento –z, colocar la zona horaria correspondiente, por ejemplo, GMT.

Descripción de la línea de comando:

- -d indica el directorio para crear la línea de tiempo.
- -z indica la zona horaria.
- >> indica agregar (append) al archivo sdcard.body; de lo contrario, si se usa solo la redirección “>” se sobrescribe el archivo.

Crear un archivo de fácil lectura, delimitado por comas (CSV), de la línea de tiempo con el comando mactime de Sleuth Kit y contar las líneas del archivo convertido csv:

$mactime –b sdcard.body –z GMT –d > sdcard-linea_de_tiempo.csv

$wc –l sdcard-linea_de_tiempo.csv

En una planilla de cálculo, OpenOffice Calc, analizar el archivo sdcard-línea_de_tiempo.csv:

- Aparece un valor que indica Enero 1, 1970, es la línea de tiempo que se inicializó en 0.
- Existen archivos borrados que se pueden recuperar con las herramientas de Sleuth Kit.
- Cuando una aplicación es movida a la tarjeta SD con el objetivo de probarla.
- La línea de tiempo puede mostrar la fecha y hora de un archivo creado o modificado.

2. Registrar, documentar y/o capturar pantallas con la información requerida.

Procedimiento para el análisis del sistema de archivos FAT de la tarjeta sD

Existen muchas herramientas[162] para el análisis del sistema de archivos

FAT tanto de código abierto como comerciales. Los archivos borrados se pueden recuperar con Sleuth Kit a través de la interfaz gráfica de gestión de casos Autopsy.

1. Ejecutar los comandos find y file para rápidamente hallar los archivos en los espacios asignados por nombre, ruta y tipo de archivo, ordenarlos e importarlos a una planilla de cálculo o base de datos para el posterior análisis[163]:

$ find /mnt/sdcard –type f –print0 | xargs -0 file

Descripción del comando:

- –type f indica que el tipo de archivo ordinario no lista directorios.
- -print0 termina cada archivo con un carácter NULL, en vez del predeterminado.
- | la salida del comando es la entrada del comando.
- Xargs crea y ejecuta líneas de comando utilizando datos.

2. Registrar, documentar y/o capturar pantallas con la información requerida.

Procedimiento para el análisis de las aplicaciones en Android

La metodología para analizar la importante cantidad de información de las aplicaciones almacenadas en /data/data es ingresar a cada una de ellas y:

- Listar los directorios (ls -l).
- Ingresar a cada subdirectorio (cd) y listar el contenido.
- Si es el directorio de bases de datos (databases), analizarlo con el gestor de bases de datos SQLite.
- Si es el directorio de preferencias compartidas (shared_prefs), editarlo con un editor de XML o con el comando cat.
- Utilizar el comando file para determinar el tipo de archivo y posteriormente la aplicación correspondiente para su visualización o edición.

El nombre de las aplicaciones y la cantidad dependerán de cada dispositivo Android; el listado que se muestra a continuación es el obtenido a través del emulador de Android:

$ls /data/data com.android.backupconfirm

com.android.browser

com.android.calculator2 com.android.calendar com.android.camera com.android.certinstaller com.android.contacts com.android.customlocale2 com.android.defcontainer com.android.deskclock com.android.development com.android.email com.android.emulator.connectivity.test

com.android.emulator.gps.test com.android.exchange com.android.fallback com.android.gallery com.android.gesture.builder com.android.htmlviewer com.android.inputmethod.latin com.android.inputmethod.pinyin com.android.keychain com.android.launcher com.android.mms

com.android.music

com.android.netspeed com.android.packageinstaller com.android.phone com.android.protips com.android.providers.applications com.android.providers.calendar com.android.providers.contacts com.android.providers.downloads com.android.providers.downloads.ui com.android.providers.drm com.android.providers.media com.android.providers.settings com.android.providers.telephony com.android.providers.userdictionary com.android.quicksearchbox com.android.sdksetup com.android.settings com.android.sharedstoragebackup com.android.soundrecorder com.android.speechrecorder com.android.systemui com.android.vpndialogs com.android.wallpaper.livepicker com.android.widgetpreview com.example.android.apis com.example.android.livecubes com.example.android.softkeyboard com.motorola.pgmsystem com.motorola.programmenu com.svox.pico com.viaforensics.android.aflogical_ose jp.co.omronsoft.openwnn

Aplicación de mensajes

1. Analizar los archivos de la aplicación Messaging, que maneja mensajes SMS – MMS; nombre del paquete com.android.providers.telephony. Está incluida de fábrica en el dispositivo:

$ cd /data/data/com.android.providers.telephony

$ls -l

drwxrwx--x radio radio 2012-06-16 22:55 app_parts

El directorio app_parts contiene adjuntos e imágenes, videos, etc. Utilizar el comando file para análisis.

drwxrwx--x radio radio 2012-06-16 20:21 databases

drwxr-xr-x system system 2012-06-16 20:20 lib

drwxrwx--x radio radio 2012-06-16 20:20 shared_prefs Bases de datos:

$cd /data/data/com.android.providers.telephony/databases

$ ls -l

-rw-rw---radio radio 38912 2012-06-16 23:44 mmssms.db

Contiene la tabla SMS con todos los mensajes; es una de las tablas principales para analizar.

-rw-rw---radio radio 0 2012-06-16 23:44 mmssms.db-journal

-rw-rw---radio radio 4096 2012-06-16 20:20 telephony.db

-rw-rw---radio radio 0 2012-06-16 20:20 telephony.db-journal

Aplicación de ayuda de mensajes

2. Analizar los archivos y directorios de la aplicación de ayuda para la aplicación principal de mensajes (Messaging app); nombre de la aplicación: com.android.mm, nombre del paquete: com.android.mms.

$cd /data/data/com.android.mms

$ls -l

drwxrwx--x app_28 app_28 2012-06-16 20:21 caché

Los archivos PART en caché son pequeñas versiones de archivos PNG de las imágenes encontradas en la aplicación de Mensajería en el directorio: /data/data/com.android. providers.telephony/app_parts

drwxr-xr-x system system 2012-06-16 20:19 lib

drwxrwx--x app_28 app_28 2012-06-16 23:44 shared_prefs

$cd /data/data/com.android.mms/shared_prefs

$ ls -l

-rw-rw---app_28 app_28 438 2012-06-16 23:44 com.android.mms_preferences.xml

Editar el archivo de preferencias de mms y verificar el tipo de codificación (UTF-8) y las primitivas utilizadas por el desarrollador (string, boolean).

$cat com.android.mms_preferences.xml

<?xml version='1.0' encoding='utf-8' standalone='yes' ?>

<map>

<string name="pref_key_ringtone">content://settings/system/notification_sound</string>

<boolean name="pref_key_auto_delete" value="true" />

<boolean name="checked_message_limits" value="true" />

<boolean name="pref_key_mms_auto_retrieval" value="true" />

<string name="pref_key_vibrateWhen">never</string>

<boolean name="pref_key_enable_notifications" value="true" />

</map>

Aplicación de Navegador de Internet

3. Analizar la aplicación predeterminada de fábrica de navegación web de Android; nombre de la aplicación de código abierto: Internet, nombre del paquete: com.android. browser.

$cd /data/data/com.android.browser

$ls -l

drwxrwx--x app_2 app_2 2012-06-17 01:59 app_appcache

drwxrwx--x app_2 app_2 2012-06-16 20:22 app_databases

drwxrwx--x app_2 app_2 2012-06-16 20:22 app_geolocation

drwxrwx--x app_2 app_2 2012-06-17 01:59 app_icons

drwxrwx--x app_2 app_2 2012-06-17 01:58 cache

drwxrwx--x app_2 app_2 2012-06-17 01:59 databases

drwxr-xr-x system system 2012-06-16 20:19 lib

drwxrwx--x app_2 app_2 2012-06-16 20:22 shared_prefs Directorio caché:

$cd /data/data/com.android.browser/cache

$ls -l

-rw------app_2 app_2 1916 2012-06-17 01:58 browser_state.parcel

drwx-----app_2 app_2 2012-06-17 01:58 webviewCacheChromium

drwx-----app_2 app_2 2012-06-16 20:22 webviewCacheChromiumStagi Bases de datos y archivos:

$cd /data/data/com.android.browser/app_databases

$ ls -l

-rw-rw---app_2 app_2 0 2012-06-16 20:22 Databases.db

-rw-r--r-root root 0 2012-06-17 19:00 databases.db

drwxrwx--app_2 app_2 2012-06-16 20:24 localstorage

Tabla ítem de http_www.google.com_0.localstorage:

$cd localstorage

$ls -l

-rw-r--r-app_2 app_2 483328 2012-06-16 20:24 http_www.google.com_0.localstorage

Contiene la tabla ítem que es una lista de pares de valores de claves, con información importante para los sitios visitados.

Base de datos de ubicación geográfica app_geolocation:

$cd /data/data/com.android.browser

$cd app_geolocation

$ls -l

-rw-rw---app_2 app_2 0 2012-06-16 20:22 CachedGeoposition.db

La tabla CachedPosition de la base de datos CachedGeoposition contiene los siguientes campos:

- latitude
- longitude
- altitude
- accuracy
- altitudeAccuracy
- heading
- speed
- timestamp

En la base de datos ubicada en /data/data/com.android.browser/app_geolocation/ GeolocationPermissions.db, que contiene la tabla Permissions, se encuentra la lista de los orígenes (sitios web) y los permisos para cada uno (allow permitido). El valor 1 en un sitio web, como por ejemplo http://www.google.com.ar, indica que el sitio tiene permisos de acceso para la ubicación geográfica.

La base de datos webpageIcons.db contiene los íconos de un sitio en particular y la URL; analizar con el manejador de base de datos SQLite:

$cd /data/data/com.android.browser/app_icons

$ls -l

-rw-rw---app_2 app_2 24576 2012-06-24 01:16 webpageIcons.db

sqlite3 webpageIcons.db SQLite version 3.7.4

Enter ".help" for instructions

Enter SQL statements terminated with a ";" sqlite> .tables

IconData IconDatabaseInfo IconInfo PageURL sqlite> .schema PageURL

CREATE TABLE PageURL (url TEXT NOT NULL ON CONFLICT FAIL UNIQUE ON CONFLICT REPLACE,iconID INTEGER NOT NULL ON CONFLICT FAIL);

CREATE INDEX PageURLIndex ON PageURL (url); sqlite> .mode line

sqlite> select * from PageURL;

url = http://www.google.com/webhp?client=android-google&source=android-home iconID = 2

url = http://www.google.com/webhp?tbm=plcs&source=mog&gl=us&client=androidgo ogle&tab=wP iconID = 2

url = http://www.google.com/search?hl=es-419&client=android-google&gl=us&outp ut=search&tbm=plcs&q=Caf%C3%A9&nmnicon=1&tbo=u&biw=320&bih=533 iconID = 2 url = http://maps.google.com/maps?gl=us&hl=es-419&gl=us&daddr=1658+Market+Street,+San+Francisco,+CA+94102&panel= iconID = 4

La base de datos browser.db contiene información de marcadores y búsquedas realizadas en el navegador de Internet; analizar con el manejador de base de datos SQLite:

$cd /data/data/com.android.browser/databases

$ls -l

-rw-rw---app_2 app_2 4096 2012-06-17 01:58 autofill.db

-rw-rw---app_2 app_2 288768 2012-06-24 01:16 browser2.db

-rw-rw---app_2 app_2 32768 2012-06-24 01:16 browser2.db-shm

-rw-rw---app_2 app_2 11560 2012-06-24 01:16 browser2.db-wal

-rw-rw---app_2 app_2 12288 2012-06-17 19:27 webview.db

-rw-rw---app_2 app_2 32768 2012-06-17 19:27 webview.db-shm

-rw-rw---app_2 app_2 3176 2012-06-17 19:27 webview.db-wal

-rw-rw---app_2 app_2 7168 2012-06-24 01:17 webviewCookiesChromium.db

-rw-rw---app_2 app_2 7168 2012-06-16 20:22 webviewCookiesChromiumPri Base de datos Bookmarks (Marcadores):

sqlite3 browser2.db SQLite version 3.7.4

Enter ".help" for instructions

Enter SQL statements terminated with a ";" sqlite> .tables

_sync_state history thumbnails

_sync_state_metadata images v_accounts android_metadata searches v_omnibox_suggestions bookmarks settings

sqlite> .schema bookmarks

CREATE TABLE bookmarks(_id INTEGER PRIMARY KEY AUTOINCREMENT,title

TEXT,url TEXT,folder INTEGER NOT NULL DEFAULT 0,parent INTEGER,position INTEGER NOT NULL,insert_after INTEGER,deleted INTEGER NOT NULL DEFAULT 0,

account_name TEXT,account_type TEXT,sourceid TEXT,version INTEGER NOT NULL DEFAULT 1,created INTEGER,modified INTEGER,dirty

INTEGER NOT NULL DEFAULT 0,sync1 TEXT,sync2 TEXT,sync3 TEXT,sync4 TEXT,sync5 TEXT);

Sqlite>.mode line

sqlite> select * from bookmarks limit 1;

_id = 1

title = Bookmarks url =

folder = 1 parent = position = 0 insert_after = deleted = 0 account_name = account_type = sourceid = version = 1 created = modified =

dirty = 1 sync1 = sync2 =

sync3 = google_chrome_bookmarks sync4 =

sync5 = sqlite>.quit

La base de datos webview.db que contiene cookies, formularios, claves, etc., y la base de datos webviewCache.db que contiene la tabla Caché con metadatos de los archivos, ambas poseen información relevante para el perito. La mayoría de los dispositivos guardan los datos de visualización web en el subdirectorio /data/data/ com.android. browser; en el teléfono HTC Incredible se guarda en RAM en el directorio tmpfs.

Analizar con el manejador de base de datos SQLite:

sqlite3 webview.db sqlite3 webview.db SQLite version 3.7.4

Enter ".help" for instructions

Enter SQL statements terminated with a ";" sqlite> .tables

android_metadata formurl password formdata httpauth

sqlite> .schema android_metadata

.schema android_metadata

CREATE TABLE android_metadata (locale TEXT); sqlite> .mode line

sqlite> select * from android_metadata; select * from android_metadata;

locale = es sqlite> .tables

.tables

android_metadata formurl password formdata httpauth

sqlite> .schema formdata

CREATE TABLE formdata (_id INTEGER PRIMARY KEY, urlid INTEGER, name TEXT, value TEXT, UNIQUE (urlid, name, value) ON CONFLICT IGNORE);

sqlite> .mode line

sqlite> select * from formdata;

_id = 1
urlid = 1 name = date
value = 17/06/12
_id = 2
urlid = 1 name = time
value = 7:26pm sqlite>.quit
Tabla cookies:
sqlite> select * from cookies; creation_utc = 12984351779332505 host_key = .google.com
name = PREF
value = ID=a773f18027748320:U=ea125d723e4e6a20:FF=0:TM=1339878292:LM=1339878293:S=jiNn-gt5FWPp19f7
path = / expires_utc = 13047423893000000 secure = 0
httponly = 0
last_access_utc = 12984974195094290
creation_utc = 12984434388728266 host_key = .google.com
name = SNID
value = 61=sJsywR18_Scd_ksZeuEZ7jorLgZDazwFsamA9LkinA=RTOy8sUBhhVF64s
path = /verify
expires_utc = 13000776680000000
secure = 0
httponly = 1
last_access_utc = 12984434388728266 sqlite> .quit

Aplicación de contactos

4. Analizar la aplicación predeterminada de fábrica de Contactos de Android; nombre de la aplicación: Contactos, nombre del paquete: com.android.providers.contacts. La aplicación contiene los registros de las llamadas, puede guardar información de contactos de diferentes cuentas de correo electrónico, Facebook, Twitter, etc. Si las fotos de los contactos están disponibles se guardan en el directorio de archivos y se crea una Previsualización de imagen del tipo .JPG. La base de datos más importante dentro de / databases es la de contacts2.db, la cual contiene cincuenta tablas.

$ cd /data/data/com.android.providers.contacts
$ls -l

drwxrwx--x app_1 app_1 2012-06-17 19:15

databases

drwxrwx--x app_1 app_1 2012-06-16 20:20 files

drwxr-xr-x system system 2012-06-16 20:19 lib

drwxrwx--x app_1 app_1 2012-06-16 22:00 shared_prefs

$cd databases

$ls -l

-rw-rw---app_1 app_1 110592 2012-06-16 22:55 contacts2.db

-rw-rw---app_1 app_1 0 2012-06-16 22:55 contacts2.db-journal

-rw-rw---app_1 app_1 110592 2012-06-16 22:00 profile.db

-rw-rw---app_1 app_1 0 2012-06-16 22:00 profile.db-journal

$sqlite3 contacts2.db sqlite3 contacts2.db SQLite version 3.7.4

Enter ".help" for instructions

Enter SQL statements terminated with a ";"

sqlite> .tables

_sync_state phone_lookup view_data_usage_stat

_sync_state_metadata photo_files view_entities accounts properties view_groups

activities raw_contacts view_raw_contacts agg_exceptions search_index view_raw_entities

android_metadata search_index_content view_stream_items calls search_index_docsize view_v1_contact_methods contacts search_index_segdir view_v1_extensions

data search_index_segments view_v1_group_membership data_usage_stat search_index_stat view_v1_groups default_directory settings view_v1_organizations directories status_updates view_v1_people

groups stream_item_photos view_v1_phones mimetypes stream_items view_v1_photos name_lookup v1_settings visible_contacts nickname_lookup view_contacts voicemail_status packages view_data

Analizar con el manejador de base de datos SQLite las tablas con información relevante para el perito. Ejemplo de la estructura de la tabla: Calls (Llamadas).

Sqlite>.schema calls number

date duration type new name

numbertype numberlabe countryiso voicemail_uri is_read geocoded_location

lookup_uri matched_number normalized_number photo_id formatted_number

_data has_content mime_type source_data source_package state

Aplicación de Explorador de Medios

5. Analizar la aplicación Explorador de Medios (Media Scanner), de almacenamiento interno como externo, también explora archivos de audio, videos, imágenes, álbumes, etc. Si un directorio tiene un archivo nombrado como .nomedia, entonces el dispositivo de almacenamiento no lo explora y registra los metadatos de los archivos en ese directorio. La base de datos de nombres contiene el identificador de volumen si es que está disponible. Si una imagen es borrada, la previsualización continúa presente; aun si el metadato se ha borrado, es factible de recuperar por el sistema de archivo YAFFS2. Nombre de la aplicación: Media Store, nombre del paquete: com.android.providers. media.

$cd /data/data/com.android.providers.media

$ls -Rl

.:

drwxrwx--x app_7 app_7 2012-06-16 20:21 databases

drwxr-xr-x system system 2012-06-16 20:19 lib

drwxrwx--x app_7 app_7 2012-06-16 20:21 shared_prefs

./databases:

-rw-rw---app_7 app_7 45056 2012-06-16 20:21 external.db

-rw-rw---app_7 app_7 32768 2012-06-16 20:21 external.db-shm

-rw-rw---app_7 app_7 14704 2012-06-16 20:21 external.db-wal

-rw-rw---app_7 app_7 38912 2012-06-16 20:21 internal.db

-rw-rw---app_7 app_7 32768 2012-06-16 20:21 internal.db-shm

-rw-rw---app_7 app_7 14704 2012-06-16 20:21 internal.db-wal

./lib:

./shared_prefs:

-rw-rw---app_7 app_7 108 2012-06-16 20:20 MediaUpgradeReceiver.xml-rw-rw---app_7 app_7 119 2012-06-16 20:21 com.android.providers.media_preferences.xml

$sqlite3 external.db SQLite version 3.7.4

Enter ".help" for instructions

Enter SQL statements terminated with a ";" sqlite> .tables

album_art audio files album_info audio_genres images

albums audio_genres_map search

android_metadata audio_genres_map_noid searchhelpertitle

artist_info audio_meta thumbnails artists audio_playlists video

artists_albums_map audio_playlists_map videothumbnails sqlite>

Analizar con el manejador de base de datos SQLite las tablas con información relevante para el perito.

Aplicación Google Maps

6. La aplicación Google Maps, incluida en el dispositivo por el fabricante, se utiliza para ver mapas, buscar localidades y direcciones. Nombre de la aplicación: Google Maps, nombre del paquete: com.google.android.apps.maps. Uno de los archivos importantes es da_destination_history, que contiene una lista de los destinos consultados, y la base de datos search_history.db es importante porque contiene las búsquedas de las diferentes ubicaciones geográficas. El directorio shared_prefs contiene información para recuperar el token de autenticación. Analizar las bases de datos con el manejador de base de datos SQLite y editar los archivos .xml para correlacionar los datos.

$cd /data/data/com.google.android.apps.maps

$ls -l

drwxrwx--x app_24 app_24 2012-06-22 02:16 app_sslcache

drwxrwx--x app_24 app_24 2012-06-24 03:23 cache

drwxrwx--x app_24 app_24 2012-06-24 03:25 databases

drwxrwx--x app_24 app_24 2012-06-24 03:35 files

drwxr-xr-x system system 2012-06-22 01:38 lib

drwxrwx--x app_24 app_24 2012-06-24 03:23 shared_prefs

$cd /data/data/com.google.android.apps.maps/databases

$ls -l

-rw-rw---app_24 app_24 5120 2012-06-24 03:35 LayerInfo

-rw-rw---app_24 app_24 0 2012-06-24 03:35 LayerInfo-journal

-rw-rw---app_24 app_24 4096 2012-06-22 02:16 da_destination_history

-rw-rw---app_24 app_24 0 2012-06-22 02:16 da_destination_history-journal

-rw-rw---app_24 app_24 18432 2012-06-24 03:23 google_analytics.db

-rw-rw---app_24 app_24 0 2012-06-24 03:23 google_analytics.db-journal

-rw-rw---app_24 app_24 5120 2012-06-24 03:28 google_latitude.db

-rw-rw---app_24 app_24 0 2012-06-24 03:28 google_latitude.db-journal

-rw-rw---app_24 app_24 5120 2012-06-24 03:25 local_active_places.db

-rw-rw---app_24 app_24 0 2012-06-24 03:25 local_active_places.db-journal

-rw-rw---app_24 app_24 5120 2012-06-24 03:26 search_history.db

-rw-rw---app_24 app_24 0 2012-06-24 03:26 search_history.db-journal

-rw-rw---app_24 app_24 12288 2012-06-24 03:23 webview.db

-rw-rw---app_24 app_24 32768 2012-06-24 03:23 webview.db-shm

-rw-rw---app_24 app_24 12608 2012-06-24 03:23 webview.db-wal

-rw-rw---app_24 app_24 7168 2012-06-24 03:23 webviewCookiesChromium.db

-rw-rw---app_24 app_24 7168 2012-06-24 03:23 webviewCookiesChromiumPrivate.db Base de datos da destination_history:

$sqlite3 da_destination_history SQLite version 3.7.4

Enter ".help" for instructions

Enter SQL statements terminated with a ";" sqlite> .tables

android_metadata destination_history sqlite> .schema destination_history time

dest_lat dest_lng dest_title dest_address dest_token source_lat source_lng day_of_week hour_of_day

Base de datos search_history.db:

$sqlite3 search_history.db sqlite3 search_history.db SQLite version 3.7.4

Enter ".help" for instructions

Enter SQL statements terminated with a ";" sqlite> .tables

android_metadata suggestions

sqlite> .schema suggestions

.schema suggestions

CREATE TABLE suggestions (_id INTEGER PRIMARY KEY AUTOINCREMENT, data1

TEXT, singleResult INTEGER, displayQuery TEXT, latitude INTEGER DEFAULT 200000000, longitude INTEGER DEFAULT 200000000);

sqlite> .mode line

sqlite> select * from suggestions;

_id = 1

data1 = fresnos singleResult =

displayQuery = Fresnos, Gregory, TX, United States latitude = 27923196

longitude = -97287642

_id = 2

data1 = stabenau sandra singleResult =

displayQuery = Stabenau Sandra, Stimbergstra ſe, Oer-Erkenschwick, Deutschland latitude = 51639294

longitude = 7260509

El directorio files contiene importante información acerca de las descripciones de las direcciones, analizar el contenido de los archivos DATA_LAYER_.

$cd /data/data/com.google.android.apps.maps/files

$ls DATA_PROTO_SAVED_CATEGORY_TREE_DB

DATA_Preferences

DATA_RECENT

DATA_RemoteStringsBlock_en DATA_Restrictions DATA_Restrictions_lock

DATA_SAVED_REMOTE_ICONS_DATA_BLOCK DATA_STARRING

DATA_SYNC_DATA_LOCAL

DATA_ServerControlledParametersManager.data DATA_ServerControlledParametersManager_DA.data DATA_TILE_HISTORY

DA_DirOpt_en_US NavigationParameters.data ZoomTables.data event_store_v2

En la tarjeta SD se almacenan datos que se utilizan para los cambios de direcciones para la navegación en Google Maps y se registra la fecha y hora de cada cambio de dirección. La función de navegación guarda los archivos en caché en la tarjeta SD con el formato

.wav de las direcciones actuales. La fecha y hora de cada archivo que está precedida con "._speech_nav" (2012-06-21 16:45 ._speech_nav13.wav) permite determinar cuándo la dirección fue utilizada y también escuchar el texto hablado de las direcciones.

$ ls -l /mnt/sdcard/Android/data/com.google.android.apps.maps

d---rwxr-x system sdcard_rw 2012-06-24 03:23 cache

d---rwxr-x system sdcard_rw 2012-06-22 02:16 debug

d---rwxr-x system sdcard_rw 2012-06-22 02:16 testdata

$cd /mnt/sdcard/Android/data/com.google.android.apps.maps/cache

$ls -l

----rwxr-x system sdcard_rw 26624 2012-06-22 02:16 cache_bd.m

----rwxr-x system sdcard_rw 22528 2012-06-22 02:16 cache_its.m

----rwxr-x system sdcard_rw 22528 2012-06-22 02:37 cache_its_bas_bic.m

----rwxr-x system sdcard_rw 22528 2012-06-22 02:37 cache_its_ter.m

----rwxr-x system sdcard_rw 414480 2012-06-24 03:26 cache_r.0

----rwxr-x system sdcard_rw 32768 2012-06-24 03:26 cache_r.m

----rwxr-x system sdcard_rw 22528 2012-06-22 02:16 cache_rgts.m

----rwxr-x system sdcard_rw 27648 2012-06-22 02:16 cache_vts.m

----rwxr-x system sdcard_rw 1236764 2012-06-24 03:27 cache_vts_GMM.0

----rwxr-x system sdcard_rw 65536 2012-06-24 03:27 cache_vts_GMM.m

----rwxr-x system sdcard_rw 27648 2012-06-22 02:37 cache_vts_inaka_GMM.m

----rwxr-x system sdcard_rw 52224 2012-06-22 02:37 cache_vts_labl_GMM.m

----rwxr-x system sdcard_rw 27648 2012-06-22 02:37 cache_vts_tran_GMM.m Filtrar los archivos de audio (wav) que indican los cambios de dirección:

$ls –lah | grep speech

Aplicación Gmail

7. La aplicación Gmail viene incorporada en el dispositivo de fábrica; nombre de la aplicación: Gmail (Google Mail), nombre del paquete: com.google.android.gm.

$ls -l /data/data/com.google.android.gm

Analizar el contenido de las diferentes tablas de la base de datos de la aplicación Gmail con el gestor de base de datos SQLite:

- Cada cuenta de correo Gmail tiene su propia base de datos SQLite con todo el contenido del correo.
- Las bases de datos downloads.db, suggestions.db y gmail.db contienen información adicional.
- Algunos archivos del tipo SQLite journal pueden recuperarse.
- La sincronización de cuentas de Gmail son referenciadas también en el archivo Gmail. xml en el directorio shared_prefs.

Aplicación de correo

8. Analizar las bases de datos de correo contenidas en com.android.mail y sus

respectivas tablas con el gestor de base de datos SQLite:

Account Mailbox Message_Updates android_metadata Attachment Message Policy

HostAuth Message_Deletes QuickResponse

Aplicación Dropbox

9. La aplicación Dropbox permite acceder al sitio web de archivos compartidos; nombre del paquete: com.dropbox.android.

$ls -l /data/data/com.dropbox.android

Analizar el contenido de las diferentes tablas de la base de datos de la aplicación Dropbox con el gestor de base de datos SQLite. La base de datos db.db contiene importante información para el perito sobre la aplicación Dropbox, sobre el dispositivo y sobre el usuario y las personas que interactúan con él. Por ejemplo: un archivo sincronizado con la cuenta de Dropbox puede ser compartido y estar en caché en la tarjeta SD. En la base de datos aparece información adicional sobre los archivos compartidos; son factibles de ser recuperados.

$sqlite3 db.db

Analizar el archivo log.txt, que muestra la actividad del uso de la aplicación, fecha y hora, autenticación de usuario y nombre otorgado, fotografía o imagen importada de la biblioteca, archivo específico en la tarjeta SD y el servicio Dropbox interrumpido por una llamada telefónica:

$cat ./files/log.txt

Editar el archivo de preferencias de la cuenta de Dropbox:

$cat /shared_prefs/DropboxAccountPrefs.xml

Aplicación Adobe Reader

10. La aplicación Adobe Reader tiene el paquete com.adobe.reader, los archivos en formato pdf se guardan en el directorio caché. La lista de archivos recientes se almacena en cache/com.adobe.reader.preferences.xml. Analizar la base de datos que se encuentra en / data/data/com.adobe.reader.

Aplicación YouTube

11. La aplicación YouTube adquirida por Google tiene desarrollada en forma nativa una aplicación para Android. Nombre del paquete: com.google.android.youtube. Analizar la base de datos que se encuentra en /data/data/com.google.android.youtube con el gestor de base de datos SQLite y editar el archivo youtube.xml que se encuentra en / data/data/com.goolge.android.youtube/shared_prefs/ y el listado de los videos ya visualizados. Verificar la existencia de capturas instantáneas de

videos con una herramienta de búsqueda de fragmentos (carving).

12.

Aplicación Cooliris Media Gallery

13. La aplicación Cooliris Media Gallery fue desarrollada por Google Nexus One y permite usar una galería de imágenes, videos, música y es un explorador. El nombre del paquete es: com.cooliris.media. La base de datos se encuentra en /data/data/com.cooliris.media. Los archivos de previsualización se encuentran en la tarjeta SD en /mnt/sdcard/ Android/data/com.cooliris.media. Analizar la base de datos con el gestor de base de datos SQLite.

Aplicación Facebook

14. La aplicación Facebook de red social tiene el paquete com.facebook.katana en el directorio /data/data/. La base de datos fb.db contiene la mayor cantidad de información (tablas: friends, user_statuses, mailbox_messages, etc.). Analizar la base de datos con el gestor de base de datos SQLite.

15. Registrar, documentar y/o capturar pantallas con la información requerida.

CAPÍTULO 11
DISCOS ÓPTICOS

Análisis forense de almacenamiento de discos ópticos

CD (Compact Disc)[164]

DVD (Digital Versatile/Video Disc)[165]

Blu-Ray[166]

Consideraciones previas

Las imágenes guardadas en CD y DVD leídas por diferentes dispositivos pueden producir resultados diferentes, debido a las distintas implementaciones de código de error en el firmware del dispositivo o en el manejador o driver o en el hardware que controla el láser y la óptica. Estas diferencias provocan que al comparar los hash o certificaciones matemáticas de los discos ópticos, estas no coincidan. El perito deberá considerar estas características en el momento de comparar imágenes a partir de CDs o DVDs. En ambos casos, se debe certificar matemáticamente la imagen duplicada o la información recolectada con un hash del tipo MD5 o SHA1 antes y después del análisis de la imagen y en lo posible trabajar a partir de un archivo de la imagen del disco óptico.

Composición física

Los discos compactos se hacen de un disco grueso, de 1,2 mm, de policarbonato de plástico, al que se le añade una capa reflectante de aluminio, utilizada para obtener más longevidad de los datos, que reflejará la luz del láser (en el rango de espectro infrarrojo, y por lo tanto no apreciable visualmente); posteriormente se le añade una capa protectora de laca, que actúa como protector del aluminio y, opcionalmente, una etiqueta en la parte superior. Son sensibles al calor, 49º C, y a los rayos ultravioletas[167].

Si la superficie de los discos está dañada o con rayas, la información no se puede recuperar.

Los discos ópticos se leen con luz ultravioleta y no con la luz visible. Los productos que rellenan las rayas de los discos pueden ocultar las rayas a la luz visible pero son opacos para los rayos ultravioletas. La selección de estos productos debe realizarse con un estudio comparativo previo para determinar su eficiencia.

Tabla de especificaciones de discos ópticos[168]

Especificaciones	Blu-ray	HD DVD	HD-VMD	DVD
Capacidad (capa simple)	23,3/25/27 GB	15 GB	19 GB	4,7 GB
Capacidad (capa doble)	46,6/50/54 GB	30 GB	24 GB	8,5GB
Longitud de onda del rayo láser	405 nm	405 nm	650 nm	650 nm
Tasa de transferencia de datos	36,0 / 54,0 Mb/s	36,55 Mb/s	40,0 Mb/s (no indica si es datos o audio/video)	11,1 / 10,1 Mb/s
Formatos soportados	MPEG-2, MPEG-4 AVC, VC-1	MPEG-2, VC-1 (basado en WMV), H.264/ MPEG-4 AVC	MPEG-1, MPEG2, MPEG-4 AVC, VC-1	MPEG-1, MPEG-2
Resistencia a rayas y suciedad	Sí	No	No	No
Resolución máxima de video compatible	1080p	1080p	1080p	480p/576p

Técnicas de escritura en los discos ópticos

1. Escritura de un conjunto de sectores (track) o bloques de una vez: Escribe una pista y luego apaga el rayo láser, forzando a una ruptura en la codificación del sector, por lo que quedan dos sectores sin poderse leer. Luego se escribe una brecha o separación del tamaño de 150 sectores, insertando dos segundos de silencio entre cada conjunto de sectores. La tabla de contenidos se construye a partir de la información del conjunto de sectores o bloques y es automáticamente escrita cuando la sesión de escritura se cierra o finaliza.
2. Escritura del disco de una sola vez: Lo primero que escribe es la tabla de contenido y luego escribe cada bloque. Se utiliza en discos de audio porque elimina los dos segundos entre bloque y bloque.
3. Grabación o escritura de paquetes en forma incremental: Escribe en modo secuencial pequeñas cantidades de información, sin la separación de los 150 sectores. Esta técnica la utilizan los programas que aplican el método de escritura de arrastrar y tirar (drag and drop). Por cada paquete de información consume siete sectores en CD-R, en CDRW es de 16 sectores al igual que en DVDs regrabables.

La recuperación de datos en un disco regrabable no es posible una vez que se efectuó un borrado completo del disco; no existen datos escritos entre los espacios de los bloques.

Si el borrado es del tipo rápido, deja los datos en el disco intactos. Para leer estos discos es necesario modificar físicamente la lectograbadora[169].

sistemas de archivos

La tabla de contenidos (TOC Table of Contents) de un disco proporciona un índice dentro de los diferentes sectores. La tabla ofrece también una indicación de si el sector contiene Red Book Audio o sector de datos.

Los discos DVD solo tienen un tipo de sector, y es posible la grabación de multisesiones. El índice de las zonas de bordes para un disco es similar al de TOC para un CD y requiere procesar correctamente la multisesión en el DVD.

Los CDs y DVDs no poseen particiones. La asignación de espacio en los discos CD y DVD de cada sector es de 2048 bytes.

HSG –High Sierra Group– formuló la primera definición de un sistema de archivo para CDROM, vista como una estandarización que posteriormente es utilizada por ISO9660 (Organización Internacional de Estándares International Standards Organization).

El sistema estándar de CD es el denominado ISO9660. El estándar para DVD es UDF (Formato Universal de Disco Universal Disk Format); también puede tener el formato ISO9660. Macintosh puede utilizar ISO9660 o su propio sistema de archivo jerárquico HFS. ISO9660 no define información de espacios de asignación ya que es un sistema de solo lectura y los archivos se guardan de manera contigua. Utiliza la misma forma de asignación de espacio que ISO9660 en CD de solo lectura. En el caso de CDs regrabables, UDF asigna el espacio sector por sector.

El disco entero es escrito antes de que cualquier espacio borrado sea reclamado para su uso, esto se debe a que los discos regrabables tienen un límite de ciclos de escritura-borradoescritura por cada sector. Por esta razón, se expanden estos ciclos a toda la superficie del disco óptico. UDF presenta errores de lectura frecuente debido a su complejidad y a errores de las herramientas de escritura o cuando se actualizan los sectores regrabables. Para el perito los problemas con los sistemas de archivos UDF son significativos, debido a que cuando los archivos se pierden (lost) el usuario a menudo no se da cuenta de que existe una copia intacta del archivo y que puede ser recuperada.

Joliet es una extensión del sistema de archivo ISO9660 definida por Microsoft para Windows 95 y utiliza la convención de nombres de archivos ASCII y de nombres largos Unicode (64) y quitando la restricción de un

máximo de 8 directorios de profundidad. Algunos programas de escritura permiten hasta 100 caracteres por nombre que son leídos en versiones del sistema operativo Windows. Utiliza la misma forma de asignación de espacio que ISO9660.

Red Book Audio, estándar definido por Philips y Sony, conocido también como IEC 908, es utilizado por todos los CDs de audio. Cada pista contiene 588 subcódigos de estéreo de 16 bit que se reproducen a 44.1KHz.

En un disco de audio no hay un sistema de archivo, solo tiene un bloque de datos a los que apunta la tabla de contenido. Sony y Philips definieron un CD de texto que permite almacenar texto en el CD de audio. El texto en el CD de Sony se guarda en el área de la tabla de contenido o de entrada.

El protocolo de sistema de uso compartido (SUSP System Use Share Protocolo, documentado en IEEE P1281 SUSP, SUSP112.doc) fue diseñado en 1993 para soportar ISO9660. La implementación específica de este protocolo es Rock Ridge (IEEE P1282, documentado RRIP112.doc) con el fin de dar soporte a los atributos (identificador de usuario y grupo, enlaces simbólicos, permisos de usuario, grupo y otros) de la interfaz del sistema operativo portable (POSIX Portable Operating System Interface). Este protocolo no se utiliza con frecuencia. Las extensiones de este protocolo son ignoradas en Windows y Macintosh. Los programas de escritura manejan las extensiones Rock Ridge escribiendo los archivos en forma contigua. Por lo tanto, si no existe un directorio válido, resulta posible separar los archivos basándose en el encabezado. Utiliza la misma forma de asignación de espacio que ISO9660.

HFS, creado en 1985 por Macintosh, maneja archivos que pueden exceder los 4 GB y por lo tanto soporta discos DVD o discos de mayor capacidad. HFS y HFS+ maneja la asignación de espacio en bloques en números de potencia de 2 (2KB, 4KB, 8KB). Existe un mapa de asignación de bloques que representa los bloques asignados y libres del disco óptico. Si el perito encuentra grandes áreas sin leer de un disco óptico, puede deberse a que este sistema de archivo no puede ser leído en determinadas plataformas o a que el disco fue creado con la herramienta mkisofs.

El Torito no es un sistema de archivo, pero interactúa con este. Fue diseñado como un mecanismo para permitir el arranque o inicio de la computadora por medio de los discos CD-ROM y es independiente del sistema operativo en que se ejecute.

Etapa de identificación, registro, protección, embalaje y traslado

Identificación y registro

1. Colocarse guantes.

2. Fotografiar o filmar ambas superficies de cada disco óptico.

3. Recolectar huellas digitales: Esta tarea la debe realizar el perito dactilóscopo en lo posible o un perito en Informática forense que se haya capacitado en el área de las especialidades de Criminalística.

4. Recolectar los discos a partir de los bordes y del orificio central, no tocar la superficie, preservar la prueba para enviar al laboratorio de dactiloscopía para la recolección de huellas digitales. El perito dactilóscopo deberá utilizar elementos que no dañen los discos ópticos, por ejemplo, polvos que luego el perito en Informática forense podrá remover fácilmente, si es necesario lavándolos con agua.

5. Documentar si los discos fueron obtenidos en áreas donde se manejan químicos o sustancias peligrosas que podrían afectar al disco óptico rompiéndolo en pequeñas partículas al colocarlos en la lectora, y por consiguiente dañar físicamente al perito.

Protección de los discos ópticos

1. No apilar los CDs, la laca se puede pegar y puede remover la superficie grabable de la parte de abajo del disco y por lo tanto perder datos.

2. No ajustar los paquetes de CD con bandas de gomas, ya que deforman los bordes del CD.

3. No envolver en plástico, ya que puede adherirse a la superficie grabable y removerla.

4. Se deben apilar sobre una base con soporte o eje como los provenientes del fabricante y colocarlos en una bolsa de papel tipo madera.

5. Los discos ópticos deformados se pueden aplanar colocando un peso encima de los discos y durante un tiempo determinado.

rotulado de los discos compactos

1. Acorde a la composición química de los discos compactos, y ya que pueden absorber humedad y otros químicos, utilizar marcadores basados en agua para escribir sobre los discos; no usar lapiceras tipo bolígrafos o rollerball*170*, no utilizar marcadores en base a alcohol.

2. Se pueden rotular con etiquetas autoadhesivas que al ser despegadas no dañen la superficie superior del disco óptico y que no produzcan un desequilibrio del disco al colocarlos en las lectoras de alta velocidad. Las etiquetas pueden ser pequeñas y circulares para cubrir alrededor del orificio del disco, como si fuera un ojalillo.

3. Identificar y rotular la bolsa con los discos compactos.

Embalaje y traslado

1. Inmovilizar los discos para evitar una posible erosión de la superficie por el roce con otros objetos, embalarlos en cajas.
2. Sellar y rotular las cajas para el transporte.
3. Iniciar e ingresar los datos requeridos en el formulario para la cadena de custodia (Ver Anexo “Procedimiento para la cadena de custodia en la pericia de Informática forense Formulario para la cadena de custodia”).
4. Trasladar los discos evitando las temperaturas superiores a los 49º C, la exposición al sol y a los rayos ultravioletas.

Etapa de recolección y adquisición de datos

Procedimiento para la duplicación de discos ópticos CD y DvD

Consideraciones previas

En la creación de imágenes de discos ópticos, cada sector debe estar en el disco con un índice detallando el tipo de sector (para CD) y la ubicación original de comienzo del sector. La herramienta comercial de InfinaDyne CD/DVD Inspector[171] permite crear imágenes binarias de cualquier disco. Otra herramienta de versión de prueba es Forensic Imager de la empresa Get Data[172].

En la estación de trabajo de Informática forense:

1. Colocar en la lectograbadora el disco óptico dubitado.
2. Crear la imagen del disco óptico CD o DVD, con el comando dd[173]:

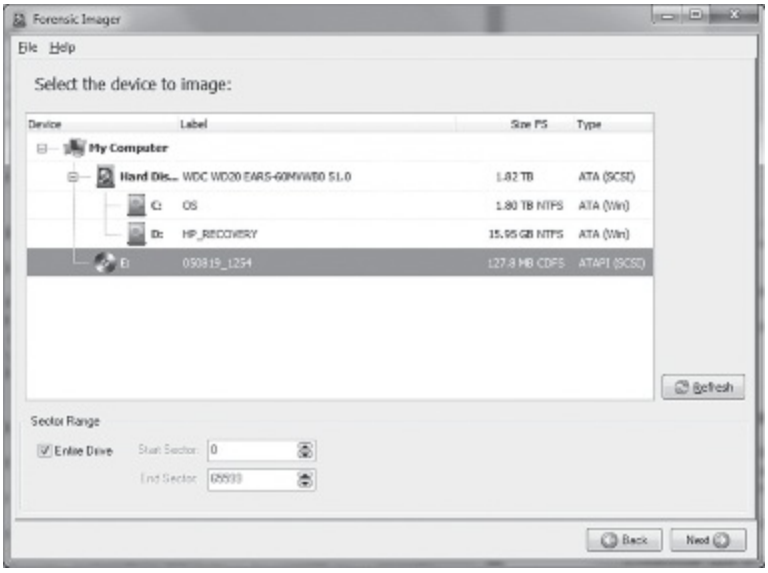
#dd if=/dev/cdrom of=/tmp/ImagenCD.iso

3. Efectuar la certificación matemática del archivo ImagenCD.iso y enviarlo a un archivo de texto:

#md5sum ImagenCD.iso > hashImagenCD.txt

4. En el sistema operativo Windows, crear la imagen con la versión de prueba Forensic Imager; ejecutar la aplicación desde el Menú de programas:

a. Seleccionar la opción Adquirir (Acquire) e indicar el dispositivo de origen:



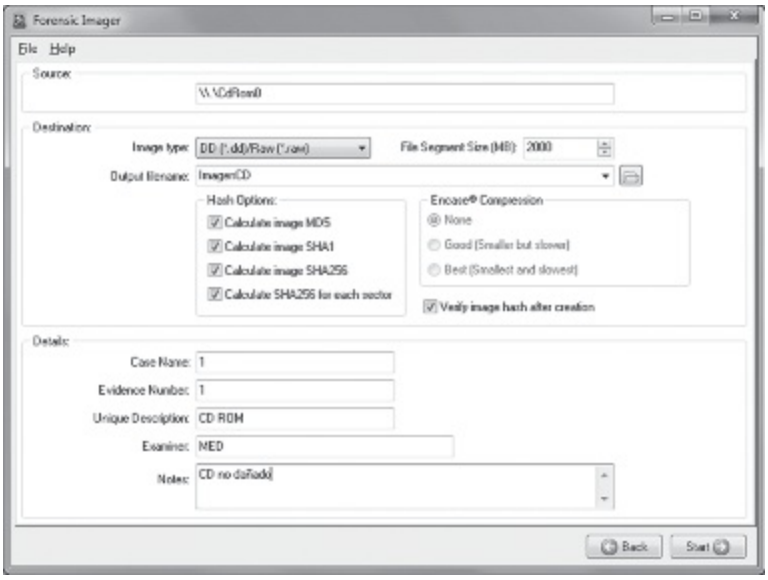
b. Completar la información requerida y oprimir el botón Iniciar (Start):

i. Tipo de imagen (binaria, Encase).

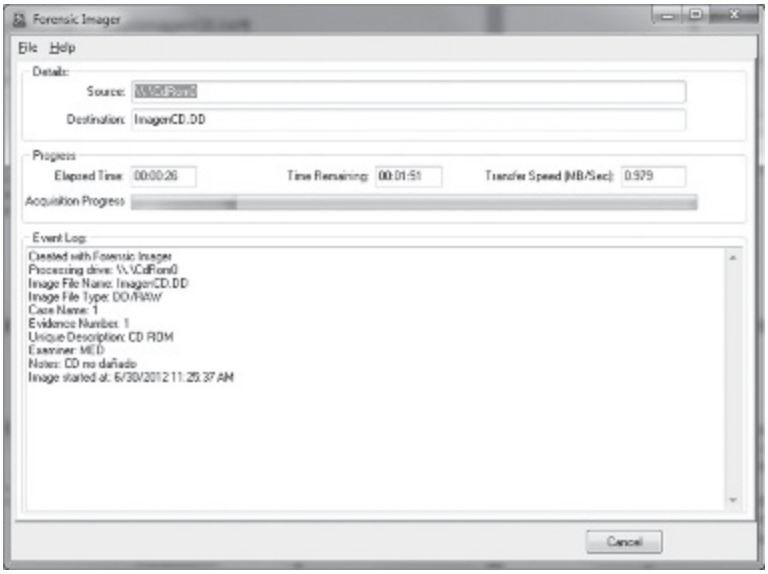
ii. Destino de la imagen.

iii. Certificación matemática y verificación.

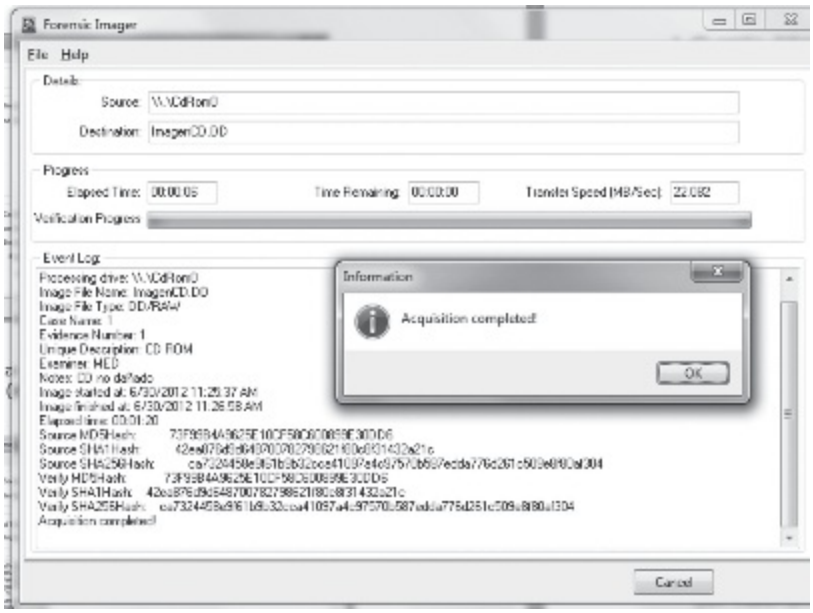
iv. Datos del caso y Notas.



c. Comienza a copiar la imagen en el destino indicado y genera un registro (event log):



d. Al finalizar, muestra el resultado de la certificación matemática y un mensaje emergente que indica que la adquisición ha finalizado:



5. Registrar, documentar y/o capturar pantallas con la información requerida.

Etapa de análisis de datos

Procedimiento para la preparación del análisis de los discos ópticos

1. El perito deberá tener especial cuidado en el manejo de los discos, en particular con aquellos expuestos a sustancias peligrosas, al momento de colocarlos en la lectora para su análisis.

2. Si es necesario, limpiar los discos con agua destilada.

3. Verificar que el inicio de la estación de trabajo de Informática forense no sea a partir de CD o DVD.

4. Verificar que no se encuentren instalados programas de escritura en los discos ópticos que sean del tipo arrastrar y tirar (drag and drop) y produzcan conflictos en el momento del análisis de la evidencia e intenten escribir en el disco óptico.

5. El perito debe tener instaladas lectograbadoras separadas para CD y para DVD. Los dispositivos que son solo lectoras no pueden acceder a sesiones abiertas del disco –por ejemplo, una sesión incompleta de arrastrar y tirar no se podrá leer– o a discos multisesiones cerrados por lo menos una vez y escritos luego con arrastrar y tirar: solamente mostrarán el contenido final.

6. Evitar las capacidades de escrituras del software del sistema operativo, por ejemplo, en Windows XP, deshabilitando la opción de grabar en el CD. En los sistemas operativos que tienen la facilidad de usar CDs y DVDs regrabables, no será sencillo anular esta opción. Por lo tanto, será necesario utilizar un

bloqueador de escritura por hardware.

7. Debido a las diferencias de la forma en que calcula MD5 las múltiples pistas, se recomienda utilizar una única pista de datos para la certificación matemática.

8. Ordenar los CDs o DVDs acorde a su capacidad de lectura, por ejemplo, si con la herramienta comercial CD/DVD Inspector[174] –cuya versión de prueba está disponible para las fuerzas de seguridad– se tarda más de cinco minutos en obtener el listado de directorios, se debe apartar el disco óptico para un análisis posterior si no se ha obtenido suficiente información con el resto de los discos ópticos recolectados.

9. Según sea el caso –los discos dañados o manchados que se puedan leer parcialmente–, es recomendable efectuar una copia antes de su limpieza.

a. La limpieza se deberá hacer colocando los discos sobre una superficie plana (la caja plástica, por ejemplo) con la parte de escritura hacia arriba, y efectuar la limpieza con agua destilada y luego secarla con un paño de microfibra (semejante a los utilizados para televisores de pantalla táctil) que no desprenda pelusa o se encuentre deshilachado.

b. Existen productos comerciales para la limpieza de discos ópticos que no son solventes y no dañan la superficie reflectora, ni absorben el policarbonato. En el caso de los discos ópticos rayados, la lectura no será posible, salvo que se cubra la superficie rayada con algún producto como puede ser alcohol isopropílico humedecido en un paño y pasándolo en forma circular sobre el disco hasta que la raya quede cubierta.

c. Existen herramientas de pulido que pueden quitar las rayas, pero requieren de un uso adecuado para no dañar más aún la superficie del disco. El sitio de la empresa española Elm-digitalia (http://www.elmdigitalia.com/) ofrece amplia información acerca de las máquinas de reparación de discos ópticos y productos de limpieza.

11. Los discos rotos por la mitad o agrietados pueden ser analizados luego de aplicar ciertas medidas de reparación:

a. Primeramente, se debe estabilizar la parte agrietada o unir las partes rotas, se puede utilizar una cinta autoadhesiva transparente o blanca (tipo Scotch).

b. Apoyar el CD o DVD sobre el disco protector de plástico que viene con el conjunto de CDs o DVDs apilables.

c. Ubicar la grieta y colocar la cinta del lado superior, no sobre el de lectura o el que tiene reflector. Según la grieta, se pueden colocar dos o tres capas de cinta, si la grieta llega hasta el orificio central o círculo del disco óptico, se puede cubrir la parte agrietada hasta el área donde empieza el texto en el círculo; no cubrir la parte escrita, de lo contrario no leerá el disco.

d. Posteriormente, probar el funcionamiento del disco en una lectograbadora, si es necesario modificada para que se pueda colocar el disco que quedó con un grosor mayor y, si se puede leer, reforzar la reparación colocando una etiqueta autoadhesiva circular, utilizando, por ejemplo, el aparato para colocar etiquetas en forma manual.

e. Otra forma es colocar un pegamento blanco (tipo Plasticola), pero se deberá esperar que se seque y la colocación debe ser muy prolija.

12. En los casos en que se haya despegado la lámina reflectora o se hayan perdido partes, la lectura convencional en un dispositivo no será factible, ya que todas las lectograbadoras deben leer la tabla de contenidos (TOC) para poder montar el disco óptico.

a. Esta es la forma en que se determina que existe un disco válido insertado en la lectograbadora. Aquí se tiene que aplicar la técnica de cambio de disco. Se debe tener un disco óptico semejante al dañado (CD-R, CD+R, CR-RW, DVD-R, DVD-RW, DVD+R, DVD+RW, etc.) y, si es posible, del mismo color, ya que la lectora efectúa medidas del disco de reemplazo y determina cómo leerlo.

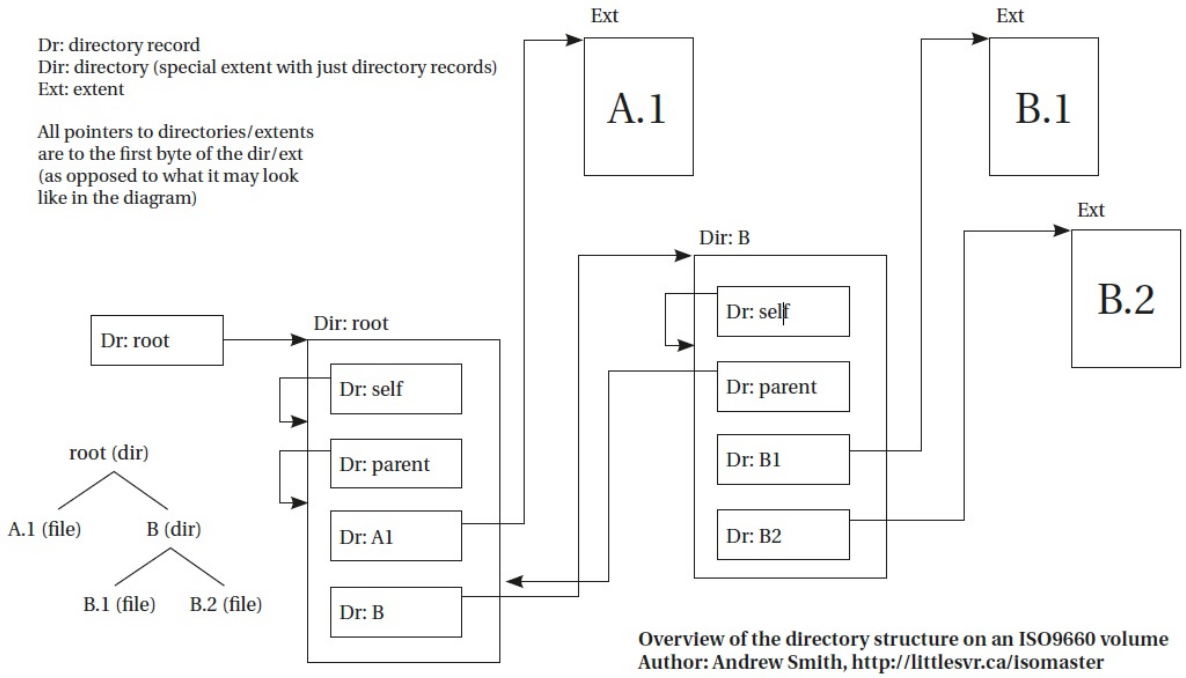
b. La técnica requiere la modificación de la lectograbadora[175].

c. Si este método no permite la lectura de los datos, la última posibilidad es enviarlo a un laboratorio experimentado en la reparación de los discos ópticos.

Procedimiento para el análisis del sistema de archivo Iso9660

Consideraciones previas

La siguiente imagen, obtenida de http://en.wikipedia.org/wiki/File:Iso9660directory Tree. png, muestra la estructura del sistema de archivo ISO9660.



La estructura está definida por:

- El descriptor de volumen.
- La tabla de rutas o path.
- La entrada de directorio.

La siguiente descripción del sistema de archivo ISO9660 es la expresada por Brian Carrier en su artículo de investigación en Informática forense sobre las diferentes interpretaciones del sistema de archivo ISO9660, http://www.dfrws.org/2010/proceedings/2010-315.pdf.

El sistema de archivo ISO9660 no es el nivel más bajo de abstracción en un CD-ROM; en el nivel más bajo existen dos o más sesiones, cada una contiene uno o más bloques. Estas sesiones y bloques son similares a las tablas de particiones en los discos rígidos.

El sistema de archivo contiene un descriptor de volumen primario y cero o más secundarios. Los descriptores de volumen comienzan en el sector 16 del sistema de archivo y contienen los datos que identifican el tamaño y disposición del sistema de archivo.

El descriptor de volumen apunta al bloque donde el directorio raíz comienza y a la ubicación de la tabla de rutas. El sistema de archivo ISO9660 almacena los datos en bloques, los cuales se agrupan en sectores consecutivos. La excepción es si el sistema de archivo usa un espacio entre sectores y ubica un intervalo constante entre grupos de bloques.

Los metadatos de los archivos se guardan en los bloques asignados al directorio padre. Cada archivo tiene una estructura de entrada de directorio en

el directorio y este contiene el nombre del archivo y otros metadatos: tamaño, fechas, ubicación del bloque de inicio.

El árbol de directorio permite ubicar un archivo al abrir el directorio raíz, encontrar el primer directorio en la ruta, abrirlo y repetir el proceso para cada directorio. Otro método alternativo de ubicar archivos es utilizar la tabla de ruta.

Esta tabla permite buscar un subdirectorio más rápido, ya que puede ser leído en memoria cuando el sistema de archivo se carga. La ubicación de la tabla está dada en el descriptor de volumen.

Cuando existen múltiples descriptores de volumen, un archivo tendrá una entrada de directorio en cada árbol de directorio que le corresponda, pero solo tendrá una copia del contenido del archivo y ambas entradas de directorio harán referencia al archivo, es decir, que ambos apuntarán al mismo bloque de inicio para el contenido del archivo.

1. Determinar la información del volumen.

a. ISO9660, 32 caracteres, letras mayúsculas, números y guión bajo (_).

b. Identificación del sistema, utilizado por el sistema operativo.

2. Analizar con un visor en hexadecimal el descriptor de volumen, ubicado en el sector 16 desde el inicio del bloque que apunta a todas las estructuras:

a. En la primera sesión en un disco que empieza en el sector 0, el descriptor de volumen se ubica en el 16; si empieza en el 20266, el descriptor (+16) debe estar ubicado en el 20282.

b. Obtener y analizar la información del descriptor:

i. Fecha de creación del disco y un área que puede llenarse con un identificador de la aplicación.

ii. Si en los contenidos del sector 16 existen dígitos hexadecimales (01 43 44 30 30 31 01), se trata entonces de un sistema ISO9660.

iii. Si el sistema de archivo está presente, entonces la fecha de creación en el disco (17 caracteres en el desplazamiento 814 [32E]) está presente en el formato: 4 dígitos para el año, 2 para el mes, 2 para día del mes, 2 para la hora, 2 para el minuto, 2 para el segundo, 1 para décimas de segundo, 1 para centésimas de segundo, 1 para la zona horaria GMT en incremento de 15 minutos, pueden ser negativos o positivos.

iv. La hora es local, refleja la zona horaria que fue configurada en la computadora en el momento de crear el CD. En el desplazamiento 575 (23F) para 128 bytes se encuentra el identificador de la aplicación que creó el CD.

v. El directorio raíz consta de una lista de entradas de directorio concatenadas en uno o más sectores. El comienzo del número del sector está en desplazamiento u offset 160 (A0 en hexadecimal) en el descriptor de

volumen como un entero de 4 bytes con formato little endian. La longitud del directorio raíz está en el offset 168 (A8 en hexadecimal) como un entero de 4 bytes con formato little endian.

vi. Los nombres de archivos son de 8 caracteres y de 3 para la extensión o tipo; los nombres de archivos solo utilizan letras mayúsculas, números y caracteres especiales. Algunos programas no respetan esta convención y pueden aparecer nombres con letras minúsculas, esto facilitará determinar el conjunto de aplicaciones que están fuera de la convención de nombres y verificar las respectivas características al efectuar el análisis del archivo.

vii. Los archivos deben ser menores de 4 GB; también está restringido por el programa de escritura a menos de 2 GB.

viii. Las entradas de directorio contienen la última fecha de modificación del archivo. El sistema ISO9660 no se actualiza. La fecha de creación es igual a la última fecha de modificación y no la última fecha de acceso. Las entradas de directorio están compuestas por: la base, el nombre del archivo y la extensión. El offset o desplazamiento son bytes con el primer byte para la entrada de directorio en 0. La tabla*176* siguiente muestra la distribución de los componentes:

Offset Desplazo	Longitud en bytes	Descripción	Tipo
0	1	Longitud de la totalidad de la entrada	Binario
1	1	Longitud de atributos extendidos	Binario
2	4	Inicio sector de datos	Entero (I)
6	4	Inicio sector de datos	Entero (M)
10	4	Longitud del archivo	Entero (I)
14	4	Longitud del archivo	Entero (M)
18	7	Fecha y hora (YMDHMSZ)	Binario
25	1	Banderas	Binario
26	1	Tamaño del sector	Binario
27	1	Tamaño del intervalo	Binario
28	2	Secuencia del volumen	Entero (I)
30	2	Secuencia del volumen	Entero (M)
32	1	Longitud del nombre del archivo	Binario
33	?	Nombre del archivo	Carácter

ix. Las aplicaciones de escritura del tipo arrastrar y tirar crean archivos fragmentados en el CD. En el análisis del disco óptico, aun en los casos en que esté dañado o roto, el perito puede recuperar información a partir de estos fragmentos.

c. Analizar los encabezados de los archivos en los límites del sector para recuperar documentos de Microsoft Office, fotos digitales.

d. Analizar con la aplicación de búsquedas de fragmentos (data carving).

e. Recuperar los archivos de la porción del disco que sean legibles; en ISO9660 los archivos están contiguos y facilita la recuperación.

3. Registrar, documentar y/o capturar pantallas con la información requerida.

Procedimiento para el análisis del sistema de archivo joliet

1. Analizar el descriptor de 8 bits que se encuentra en el sector 17, 18 o 19, con un visor en hexadecimal:

a. Ubicar el valor en hexadecimal del descriptor: 43 44 30 30 31 01.

b. Analizar los campos:

i. Del sector 16 (igual a ISO9660).

ii. Identificador de la aplicación: 64 o 16-bit Unicode en el desplazamiento 575 (23F) para 128 bytes (difiere de ISO9660).

2. Analizar las entradas de directorio; son idénticas a ISO9660:

a. Identificar nombres de archivos de 16-bit Unicode.

b. Identificar diferentes estructuras de directorios, como las que pueden ser creadas por las herramientas mkisofs.exe[177] para Windows y genisoimage[178] en Linux.

i. Analizar cada estructura detectada por separado.

c. Recuperar los archivos de la porción del disco que sean legibles, en Joliet los archivos están contiguos, lo que facilita la recuperación.

Procedimiento para el análisis del sistema rock ridge

1. Identificar el formato de las extensiones de la estructura Rock Ridge con un visor en hexadecimal:

a. AA, extensiones de Macintosh; si no están presentes, le indica al perito que el CD no fue creado por un programa de Macintosh.

b. CE, continuación de la extensión de datos:

Estructura: CE 28 1 Nro. de sector Desplazamiento Longitud

Nro. de sector, desplazamiento y longitud, valores combinados en formato big endian (almacena el byte más significativo primero) y little endian (almacena el byte menos significativo primero). Cada uno ocupa 8 bytes.

c. NM, alternar nombres largos:

Estructura: NM Longitud 1 Banderas Caracteres del Nombre

Bandera bit 0 (hexadecimal 01) está presente, el nombre se continúa en la próxima entrada.

Bandera bit 1 (hexadecimal 02) indica que el nombre corresponde a las entradas de directorio ".".

Bandera bit 2 (hexadecimal 04) indica que el nombre corresponde a las entradas de directorio "...".

d. TF, fecha y hora adicional en Posix:

Estructura: TF Longitud 1 Bandera Fecha y Hora

Las banderas indican qué fecha y hora está presente:

- 0, presente la fecha y hora de creación.
- 1, presente la fecha y hora de modificación.
- 2, presente la fecha y hora del último acceso.
- 3, presente la fecha y hora de cambios de atributos.
- 4, presente la fecha y hora de resguardo.
- 5, presente la fecha y hora de expiración.
- 6, presente la fecha y hora efectiva.
- 7, fechas y horas están en el formato de 17 bytes de longitud (YYYYMMDDHHMMSSTHZ (year, month, day, hour, minute, second, zone), año, mes, día, hora, minuto, segundo, zona horaria).
- Si no está presente el formato es del tipo corto de 7 bytes (YMDHMSZ, year, month, day, hour, minute, second zone, año, mes, día, hora, minuto, segundo, zona horaria).

2. Registrar, documentar y/o capturar pantallas con la información requerida.

Procedimiento para el análisis del sistema UDF

1. Determinar la versión de UDF; utilizar un programa que sea independiente de las versiones con un visor en hexadecimal.

a. DVD 1.02, límite máximo de archivos: 1 GB.

2. Identificar los descriptores de archivos de UDF que identifican el volumen y el puntero a la información que lo define:

a. Sector (AVDP Anchor Volume Descriptor Pointer Puntero descriptor de Volumen):

i. Bytes 02 00, para los 2 primeros bytes, los 4 bytes restantes tienen un entero little endian, igual al número de sector. Puede aparecer en diferentes áreas del disco:

- Sector 256.
- Sector 512.
- Sector escrito por última vez.
- Sector 256 escrito por última vez.
- 256 sectores después del comienzo de un bloque.
- 512 sectores después del comienzo de un bloque.

b. Luego de identificar el sector AVDP, existe un número de sector y longitud en bytes de la secuencia para el reconocimiento en el desplazamiento 16 (10 en hexadecimal), que describe el sistema de archivo; analizar:

i. Fecha y hora de creación del disco; no es la fecha en que fue escrito el contenido. Los programas que utilizan UDF para escribir soportan agregar archivos en forma incremental al disco al que se le ha dado un formato.

ii. Un identificador de la aplicación que creó el disco.

iii. El nombre o etiqueta que se le asignó al disco luego de darle formato. Puede ser diferente en el sistema operativo Windows.

3. Analizar los nombres de archivo que pueden tener 8 o 16 bits de longitud y hasta 255 caracteres.

4. Analizar la estructura de directorio que no tiene límites de profundidad, si es muy larga afecta el desempeño del disco óptico. Es difícil encontrar archivos contiguos en UDF.

5. Analizar la fecha y hora de cada archivo, pueden ser varias:

a. Creación

b. Modificación

c. Último acceso

6. Analizar fragmentos de archivos (en versiones superiores a UDF 1.02), con las herramientas de código abierto Scalpel o Foremost.

7.

a. Obtener los archivos borrados en los dispositivos de escritura de una sola vez; cuando un archivo es borrado, el archivo no se ha eliminado, solamente ha sido desasignado de la tabla.

b. En dispositivos regrabables, los programas de escritura reutilizan los espacios ocupados originalmente por un archivo borrado. Existe un límite para escribir-borrarreescribir un espacio de aproximadamente 1000 veces, después el espacio queda desgastado. En UDF es difícil que se reúse un espacio borrado antes de que se haya usado por lo menos una vez el total del

espacio no utilizado. Esto ayuda a mantener la vida útil del disco y al perito para encontrar información borrada sin dificultad.

8. Registrar, documentar y/o capturar pantallas con la información requerida.

Procedimiento para el análisis del sistema HFs y HFs+ (Apple Macintosh)

1. Verificar en HFS el nombre del disco, el mapa de particiones y el nombre del programa que creó el disco, en el bloque del sector maestro, en el sector 0.

2. Verificar en HFS+ el nombre del disco que se encuentra en el nivel superior de la estructura de árbol de directorios.

3. Verificar los nombres de archivos, que pueden ser de hasta 31 caracteres ASCII en HFS; HFS+ soporta caracteres no ASCII y nombres de archivos de hasta 255 caracteres en formato Unicode.

4. Verificar la existencia de multisesiones. Macintosh maneja de forma diferente las multisesiones que en el sistema operativo Windows.

5. Verificar si existe fragmentación o no, esto dependerá de la herramienta de escritura de CD, dependiendo de la aplicación de escritura.

6. Analizar la fecha y hora de creación, última modificación y último acceso de los archivos. La fecha y hora está en formato big endian en número de segundos.

7. Registrar, documentar y/o capturar pantallas con la información requerida.

Procedimiento para el análisis del sistema El Torito

1. Analizar el descriptor del volumen de inicio del CD, que se encuentra en el sector 17, que apunta al catálogo de inicio o arranque que a su vez apunta a una imagen (disquetes, discos rígidos emulados, memoria) de inicio.

a. Verificar cada entrada del catálogo que apunta a un hardware específico (Intel, Power PC, etc.).

i. Por cada plataforma, verificar una o más entradas de inicio y otras que no son de arranque.

2. Registrar, documentar y/o capturar pantallas con la información requerida.

Procedimiento para el análisis de la imagen adquirida con Autopsy para Windows

1. En la estación de trabajo de Informática forense, descargar e instalar la versión beta de la aplicación de código abierto Autopsy[179] para el sistema operativo Windows del sitio

http://www.sleuthkit.org/autopsy/download.php:

a. Descomprimir en un directorio el archivo autopsy-3.0.0b2.zip.

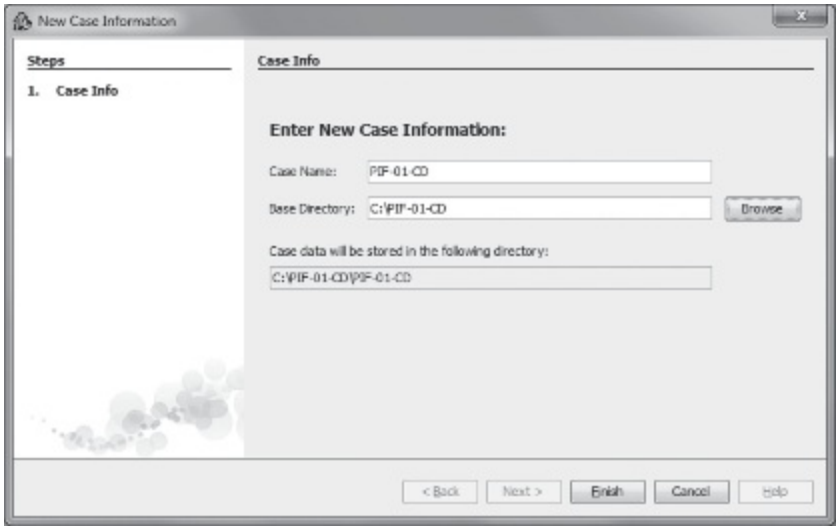
b. Leer el archivo de instalación (Readme) y:

i. Descargar el entorno de ejecución Java http://java.com/en/download/index.jsp.

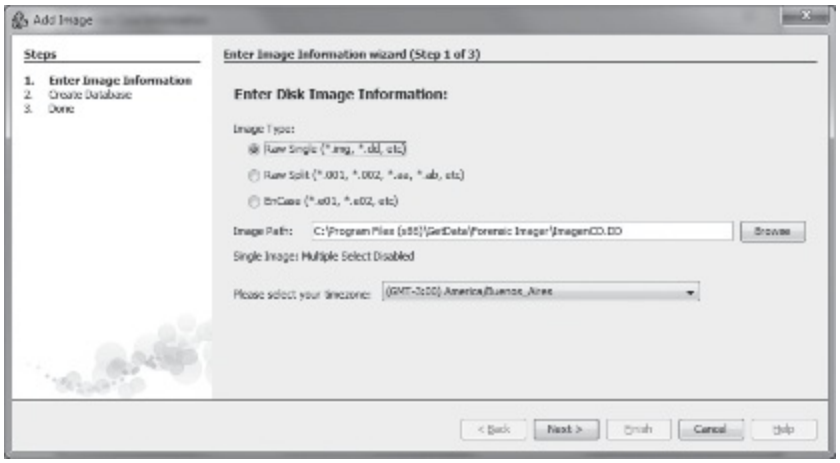
ii. O ejecutar el programa autopsy.exe desde el directorio:
C:\autopsy-3.0.0b2\autopsy-3.0.0b2\bin

iii. Aparece un cuadro de diálogo que permite seleccionar el nuevo caso:

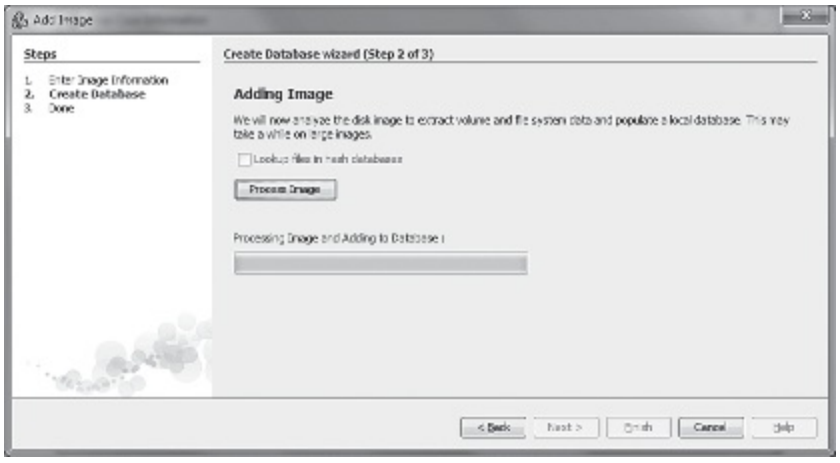
2. Ingresar los datos del caso y ubicación del archivo de evidencia y oprimir el botón Finalizar (Finish):



3. Aparece un mensaje emergente que pregunta si se desea agregar una imagen. Se debe indicar Sí y luego completar los datos en el cuadro de diálogo siguiente para indicar el lugar en donde se encuentra la imagen adquirida.



4. En el siguiente paso, se puede indicar que lea de la base de datos de hash de NSRL; si no se marca, oprimir el botón Procesar Imagen (Process Image): se crea la base de datos para la imagen.



5. Luego el programa pregunta si se quiere agregar otra imagen o finalizar, oprimir el botón Finish.

6. En la ventana del programa, aparecerá el listado del contenido del directorio de la imagen del lado izquierdo y del lado derecho la vista de la tabla de archivos; analizar la siguiente información del o los archivos dubitados:

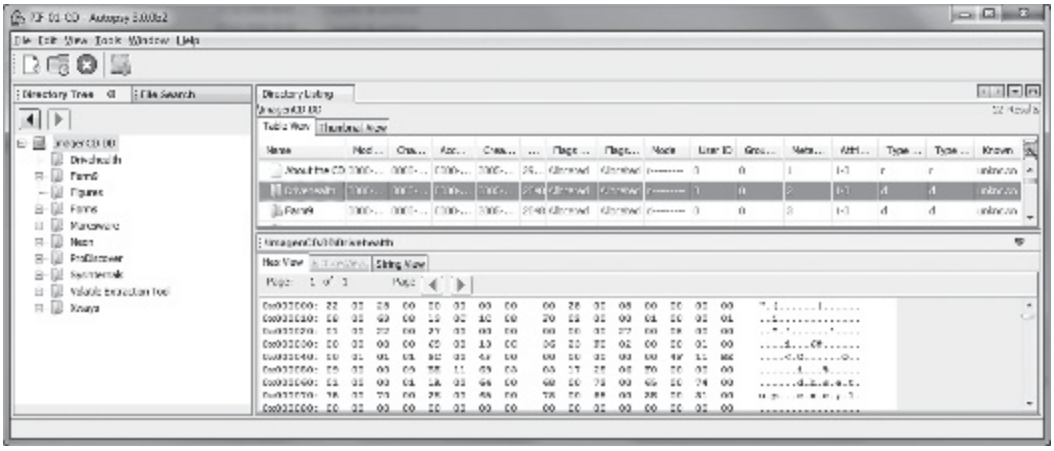
a. Fecha y hora de Modificación, Cambio, Acceso, Creación del archivo.
b. Tamaño.
c. Espacio asignado.
d. Metadatos.
e. Modo: Directorio o archivo.
f. Identificador de usuario.
g. Identificador de grupo.
h. Dirección de los metadatos.
i. Dirección de los atributos.

j. Tipo directorio.

k. Tipo metadato.

l. Estado según aparezca o no en la base de datos de hash de las aplicaciones en NSRL; el estado puede ser: desconocido, conocido por NSRL o conocido mal, no fiable.

7. Seleccionar un archivo y visualizar su contenido en hexadecimal y la cadena de caracteres en la parte inferior de la ventana de Autopsy:



8. Analizar las imágenes y visualizarlas en la opción Previsualización en la parte inferior de la ventana de Autopsy.

9. Utilizar el menú contextual sobre un archivo o directorio para:

a. Abrir el archivo en un visor externo, en general una aplicación compatible con el tipo de archivo.

b. Extraer el archivo o directorio a otro sitio de almacenamiento (disco rígido, pendrive, etc.).

10. Efectuar búsquedas de archivos, seleccionando la ficha Buscar Archivo (Search File); ingresar los datos para la búsqueda y luego oprimir el botón Buscar. Los datos pueden ser:

a. Nombre; no admite expresiones regulares.

b. Tamaño.

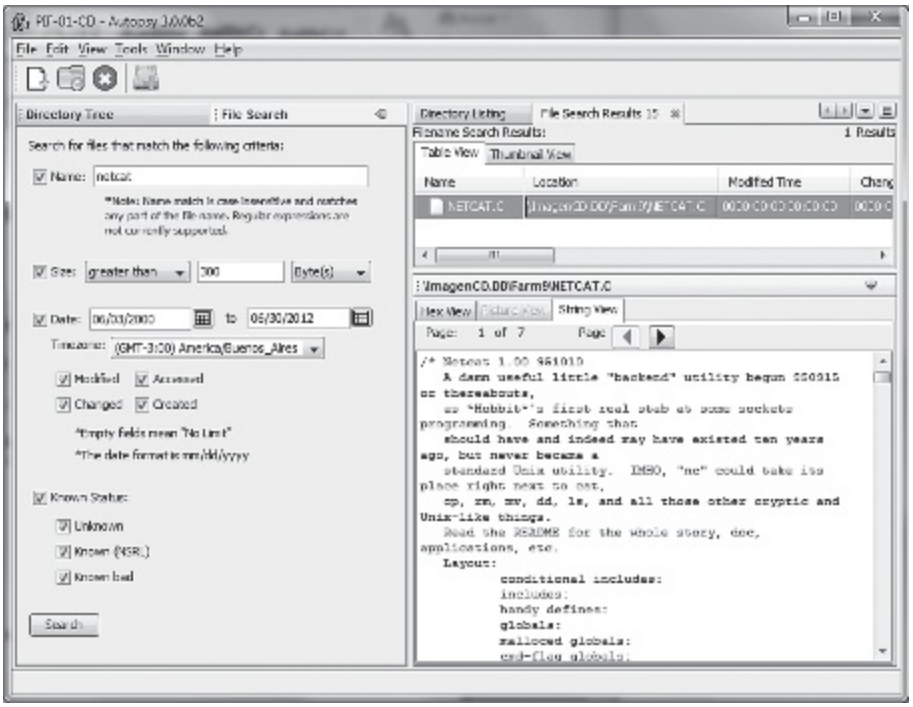
c. Rango de fecha.

d. Zona horaria.

e. Accesos: Creado, Modificado, Cambiado y Accedido.

f. Estado.

g. La visualización del resultado de la búsqueda aparece, en el panel de la derecha, en la ficha de resultados de búsqueda y en la parte inferior se puede visualizar en hexadecimal o con la cadena de caracteres.



11. Registrar, documentar y/o capturar pantallas con la información requerida.

Procedimiento general para el análisis de discos ópticos y/o de sus respectivas imágenes

Consideraciones previas

En el análisis de los discos ópticos se pueden utilizar paquetes de herramientas comerciales, de código abierto, de libre disponibilidad o comandos ejecutados en forma separada para obtener la información requerida. La información a obtener dependerá también del tipo del sistema de archivo del disco óptico. A continuación, se listan los elementos a considerar para el análisis de los discos ópticos, en donde el perito podrá seleccionar aquellos que resulten adecuados para su labor pericial o caso en particular. Analizar los siguientes elementos:

1. Información del volumen, sistema de archivo.
2. Identificación del sistema operativo.
3. Tamaño del volumen.
4. Número de discos que componen el volumen de datos.
5. Tamaño del bloque, 512 o 2048.
6. Utilización del disco.
7. Tamaño de la tabla de ruta o punteros: Contiene los nombres de los subdirectorios y el sector de inicio del subdirectorio. En Intel es little endian,

en Motorola big endian.

8. Tabla L o little endian: Contiene el número de sector en el disco óptico: Si la ruta (path) de la tabla es mayor a 2048, existirán múltiples sectores secuenciales empezando con el número de sector en este campo. Esta versión de la tabla es little endian (Intel). La tabla contiene una entrada para cada subdirectorio en el sistema de archivo, cada entrada consta de[180]:

Longitud	Tipo	Descripción
1	Binario	Longitud de la entrada a la tabla de rutas.
1	Binario	Longitud de los atributos extendidos.
4	Entero	El número del sector de inicio del subdirectorio.
2	Entero	La entrada de la ruta del directorio padre.
???	Carácter	El nombre del subdirectorio.

9. Tabla M o big endian, si la tabla es mayor a 2048, existirán múltiples sectores secuenciales empezando con el número de sector en este campo (Motorola).

10. Sector del directorio raíz: Contiene el número de sector de inicio del directorio raíz. La primera entrada tiene información del directorio.

11. Fecha y hora de la entrada del directorio raíz ".": Coincide generalmente con la fecha y hora de creación del volumen. En caso contrario, será difícil determinar la fecha de creación del volumen. En los discos de solo lectura, excepto en UDF, esta fecha debe ser la más reciente, si un archivo tiene una fecha y hora posterior, se debe inferir que ocurre alguna anomalía con las fechas y horas de disco y deben tratarse como dudosas.

En UDF, y en HFS y HFS+, se crea la fecha y hora de último acceso sumada a la de la última modificación, brindando una opción más para verificar en la última fecha de modificación. Esta última es fácil de modificar.

12. Nombre del editor del disco o de la aplicación: Se puede configurar con los programas de grabación. Si el carácter que aparece es "|" (Hexadecimal 5F), el resto del campo es el nombre de archivo en el directorio raíz que contiene el nombre del editor o de la aplicación que lo creó.

13. Archivo de derecho de autor: Contiene el nombre del archivo en el directorio raíz con la información del autor. Generalmente, está en blanco o con el valor binario 0 (cero).

14. Archivo abstracto y de bibliografía: Ambos tienen las mismas características que el archivo de derecho de autor.

15. Fecha y hora de creación, modificación, expiración del volumen.

16. Listado del contenido de los directorios, por nombre o por tipo.

17. Listado de hash o certificación matemática de los archivos.

18. Búsqueda de archivos por patrones determinados.

19. Búsqueda de fragmentos de archivos, en particular en los discos regrabables.

20. Identificación de archivos de tipo desconocido.

21. Búsqueda de archivos perdidos: Cuando están presentes múltiples sistemas de archivos, es posible que existan diferencias con los tipos de archivos que contienen. Por ejemplo, entre ISO9660 y HFS no hay correspondencia entre los archivos; sí existe entre ISO9660 y Joliet. Una forma de ocultar un archivo es que no tenga representación en un sistema de archivo, por ejemplo en Joliet (opción Ocultar Joliet en Windows), se permite remover archivos de la estructura de directorio Joliet mientras están presentes en la estructura ISO9660. La herramienta mkisofs permite efectuar esta forma de ocultar archivos.

a. Verificar la cantidad de archivos de uno y otro sistema, obtenida de los listados de directorios y archivos, y luego comparar los informes o listados.

22. Búsqueda de archivos ocultos*181*: Estos datos existen en los bloques del sistema de archivo, aunque no puedan ser visualizados por la herramienta. El contenido oculto puede encontrarse por medio de búsquedas de palabras clave o efectuando la búsqueda de fragmentos en los espacios no asignados. Formas de ocultar archivos:

a. Después de crear un disco de multisesión, la mayoría de los programas permiten borrar archivos de sesiones anteriores. Esta forma oculta realmente los archivos y no pueden ser vistos desde el sistema operativo Windows.

b. Inconsistencia en el árbol de directorios: En ISO9660 no se necesita que el árbol de directorio asociado con los diferentes descriptores de archivos tenga los mismos archivos y directorios. Una forma de ocultar archivos es tener diferentes datos en cada árbol de directorio. La herramienta y el sistema operativo pueden detectar solo uno de los árboles, por lo tanto el otro queda oculto y no se podrá analizar. Ejecutar el comando fsstat para ubicar los directorios.

c. Árbol de directorio vacío: En este caso es similar al anterior, pero utiliza dos o más descriptores de volúmenes secundarios. El primer descriptor secundario tiene un directorio raíz vacío y el segundo descriptor del volumen secundario contiene los archivos a ocultar. Generalmente, el sistema operativo y las herramientas procesan solamente el primer descriptor secundario del volumen, porque normalmente contiene los nombres de archivo Unicode de la extensión Joliet. Las herramientas no buscan en el segundo descriptor, ya que rara vez está presente. Los archivos en el segundo directorio raíz no podrán ser vistos durante el análisis.

d. Ordenamiento de bytes: La estructura de datos puede guardar valores big y little endian. Los datos se pueden ocultar si el valor de bloque de inicio en la entrada de directorio tiene diferentes valores big y little endian en los lugares de almacenamiento. Si las herramientas de análisis examinan solo una de las ubicaciones y las herramientas de ocultamiento de datos utilizan la otra, entonces los datos ocultos no se podrán encontrar. Ejemplo: una entrada de directorio con diferentes bloques de direcciones en el formato big y little endian. Ejecutar el comando fsstat para ubicar el directorio raíz para el descriptor de volumen primario y secundario.

Nombre	Bloque de Inicio (big endian)	Bloque de inicio (little endian)
Archivo1.txt	00 00 00 20	30 00 00 00

23. Identificar conjunto de bloques marcados como desconocidos, ya que no se puede determinar el tipo de sistema de archivo al que pertenece.

a. Si los bloques están contiguos, se pueden copiar los sectores y crear un archivo único binario y analizarlo en función de la información del encabezado del archivo.

b. Si el bloque está lleno de ceros, es importante analizarlo con un visor en hexadecimal para determinar si existen datos o no.

24. Registrar, documentar y/o capturar pantallas con la información requerida.

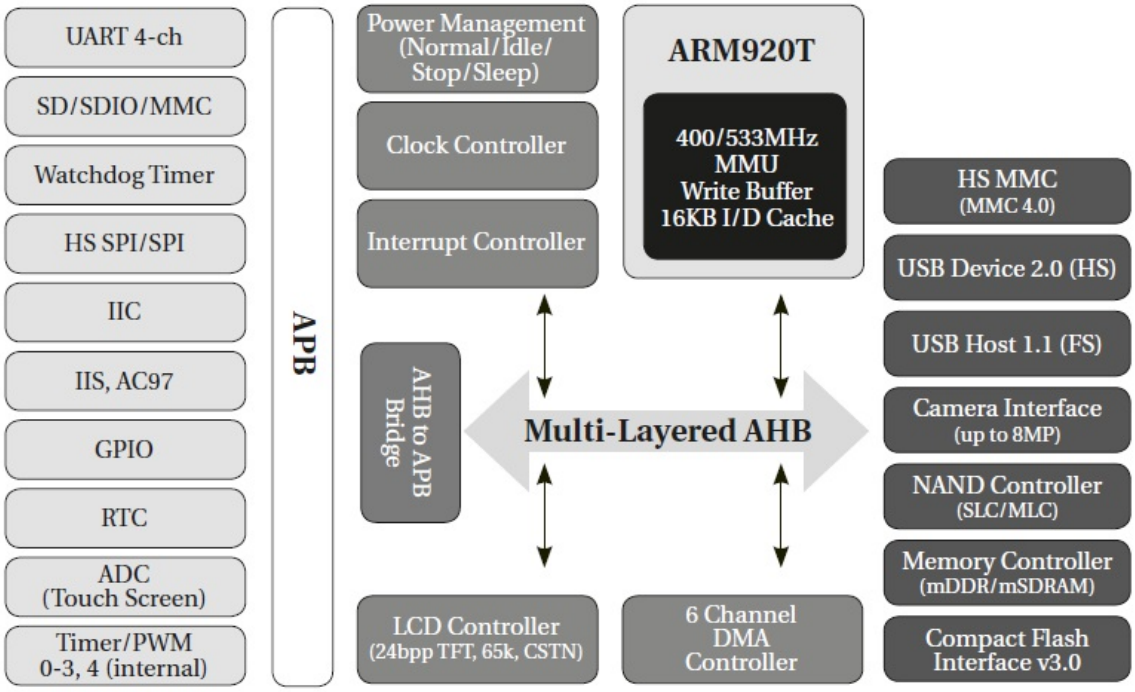
CAPÍTULO 12
DISPOSITIVOS DE NAVEGACIÓN VEHICULAR POR GPS TOM TOM[182]

Consideraciones previas

El producto de navegación de la empresa Tom Tom[183] se implementa en los dispositivos de navegación vehicular, motocicletas, teléfonos celulares, etc., y existen diversos modelos y facilidades. Todos los modelos poseen un zócalo para la tarjeta SD o un disco interno para el almacenamiento de diversos archivos (fotos, audios, videos, documentos, entre otros).

Los dispositivos Tom Tom tienen el procesador ARM de Samsung y el sistema operativo Linux, según el dispositivo pueda leer de la tarjeta SD o de la memoria interna. El programa de inicio busca el disco duro o la tarjeta el software de arranque y los datos del mapa, luego transfiere el software a la memoria RAM interna de 64 MB e inicia el programa.

El hardware inicia el GPS y la aplicación de navegación. La aplicación lee las configuraciones que se hayan instalado, como la voz preferida y la última ruta elegida. La arquitectura interna de un dispositivo Tom Tom se muestra en la siguiente imagen obtenida de http://www.gpsforensics.org/articles/tomtom/advanced.html:



El dispositivo contiene archivos tales como:

- Lugares, con diferentes direcciones, por ejemplo, la del hogar, una lista con destinos recientes y a veces del último viaje realizado.
- Información del dispositivo: Contiene el número de serie, modelo, versión del programa. Como dispositivo manos libres en teléfonos móviles, puede contener:
- Listas de llamadas entrantes y salientes.
- Buzón de entrada y salida de mensajes de texto.
- Contactos.
- Nombre de conexión para Bluetooth e identificador MAC.
- Información del usuario.

Etapa de identificación, registro, protección, embalaje y traslado de dispositivos de GPs Tom Tom

El procedimiento para la identificación, registro y traslado de dispositivos Tom Tom conlleva los mismos pasos que se deben realizar para los dispositivos móviles.

Etapa de recolección y adquisición de datos

Procedimientos de recolección de datos en dispositivos de GPS Tom Tom

1. Preparar la estación de trabajo de Informática forense para que no se encuentren archivos de instalaciones anteriores de Tom Tom que pueden ser utilizadas por el dispositivo para actualizar la información y escribir en el dispositivo. En particular, en la base del registro de Windows, los dispositivos USB que utiliza Tom Tom están configurados en la subclave CONTROL SET de USBSTOR.
2. Desconectar la estación de trabajo de Informática forense de Internet.
3. Disponer de un disco de almacenamiento preparado para guardar la imagen duplicada.
4. Si no se dispone de un bloqueador de escritura por hardware, los puertos USB se deben configurar como de solo lectura, creando en el registro, en el caso de que se utilice el sistema operativo Windows, una entrada para deshabilitar la opción de escritura a través de USB.

a. Instalar un software de verificación de la conexión USB para determinar que no se producen escrituras. El programa Sysnucleus USB Trace se puede descargar en su versión de evaluación de http://www.sysnucleus.com/usbtrace_download.html.

b. Crear una imagen en modelos de dispositivos sin tarjeta SD.

c. Iniciar la estación de trabajo de Informática forense.

d. Iniciar la aplicación de monitoreo del USB.

e. Conectar el dispositivo Tom Tom apagado a la estación de trabajo por medio del cable USB.

f. Encender el dispositivo Tom Tom, responder Sí en el dispositivo para conectarse a la estación de trabajo. Esta detecta un dispositivo USB y le asigna una unidad lógica al nuevo periférico.

g. Crear una imagen binaria con la herramienta de libre disponibilidad FTK Imager de Access Data y certificarla matemáticamente con MD5 o SHA-1 y guardarla en el disco preparado para la imagen.

5. Si el dispositivo posee una tarjeta SD, debe removerse y protegerse contra escritura, preparar una nueva tarjeta SD con borrado seguro y:

a. Conectar el dispositivo apagado Tom Tom por medio del cable USB a la estación de trabajo.

b. Insertar la nueva tarjeta SD.

c. Encender el dispositivo Tom Tom.

d. El sistema operativo solo visualiza la tarjeta SD y le asigna una unidad de disco externo e instala los dispositivos de la conexión USB.

e. Apagar el dispositivo Tom Tom.

f. Retirar la tarjeta SD.

g. Encender el dispositivo Tom Tom que se conecta con la estación de trabajo, la cual no efectúa el reconocimiento del periférico nuevamente porque ya tiene los archivos cargados anteriormente y visualiza los datos contenidos en la memoria interna del dispositivo externo asignado previamente a la tarjeta SD.

h. Crear una imagen binaria con la herramienta de libre disponibilidad FTK Imager de Access Data y certificarla matemáticamente con MD5 o SHA-1 y guardarla en el disco preparado para la imagen.

i. Crear la imagen en una estación de trabajo de Informática forense con Linux. Una vez que se inicia Linux, se conecta el dispositivo Tom Tom apagado, se enciende, Linux reconoce la conexión USB y no se necesita montar el dispositivo Tom Tom, por lo tanto queda en modo de solo lectura.

i. #mount, verificar que ni el dispositivo Tom Tom ni la partición de destino de la imagen se hayan montado automáticamente.

ii. # mount -o rw /dev/hdb5 /media/hdb5, se monta la partición de destino de la imagen en modo lectura y escritura, el disco original no se monta porque los datos son leídos directamente desde el dispositivo con el comando de copia bit a bit.

iii. #wipe /media/hd5, efectuar un borrado seguro del dispositivo de destino

con el comando wipe.

iv. # dd if=/dev/hda1 | md5sum, el dispositivo original es certificado matemáticamente con el comando dd y enviándolo al comando de hash md5sum.

v. # dd if=/dev/sdb1 of=/media/hdb5/ImagenTomTom.img, crear la imagen con el comando dd.

vi. # dd if=/media/hdb5/ ImagenTomTom.img.img | md5sum, generar el hash de la imagen o enviarlo a un archivo de texto:

dd if=/media/hdb5/ImagenTomTom.img. | md5sum > hashImagenTomTom.txt Si se dispone de bloqueador de escritura:

6. Colocar la tarjeta en un lector de tarjeta. Este debe conectarse al bloqueador de escritura por hardware con USB para la conexión con la estación de trabajo de Informática forense. El dispositivo Tom Tom no verifica si la tarjeta está protegida contra escritura e intentará escribir en ella.

- Duplicar el contenido de la tarjeta SD y generar la certificación matemática.

7. Si el dispositivo es un disco interno, aislarlo de la red para evitar que sea bloqueado por los satélites del GPS en el momento de conectarlo a la estación de Informática forense; utilizar el cable USB del dispositivo Tom Tom para conectarlo al bloqueador de escritura por hardware y este último a la estación de trabajo. Si el dispositivo es bloqueado por los satélites, se sobrescribirá la información de las últimas coordenadas del GPS en el archivo de ubicación actual (CurrentLocation.dat).

- El dispositivo puede tener clave de acceso o código de seguridad para el acceso al disco interno. Existe un método sencillo de desbloqueo que es revelado solamente a las fuerzas de seguridad a través del envío de un formulario de contacto en el sitio de gpsforensics.org.

- Duplicar el disco interno con una herramienta de imagen de disco (FTK Imager de Access Data de libre disponibilidad) y generar el hash correspondiente.

8. Registrar, documentar y/o capturar pantallas con la información requerida.

Etapa de análisis de datos

Procedimiento para el análisis de datos en dispositivos de GPs Tom Tom

1. En la estación de trabajo de Informática forense, analizar la imagen del dispositivo Tom Tom y verificar el contenido, archivos borrados y fragmentos de archivos, metadatos, etc., en particular la información de navegación satelital. En Windows se puede utilizar la aplicación FTK de Access Data

(http://ftk.accessdata.com/).

Archivo	Descripción
TTGO.BIF	Información del dispositivo, modelo, nro. de serie, idioma, mapa actual, voz.
CURRENTLOCATION.DAT	Última posición del dispositivo.
CURRENTMAP.DAT	Mapa actual.
GPRSETTINGS.DAT	Configuración del GPRS si está presente.
SETTINGS.DAT	Nombre y direcciones MAC de cualquier teléfono conectado, configuraciones de redes inalámbricas, datos del proveedor, datos del teléfono del usuario.
GPRS.CONF	Nro. de PIN GPRS PIN.
MAPSETTINGS.CFG name_map.cfg	Los archivos .CFG se encuentran en las carpetas relevantes de mapas y tienen información de favoritos, itinerarios, direcciones y puntos de interés.
\CONTACTS\ CALLED.TXT	Números de teléfonos de llamadas realizadas desde el teléfono conectado a Tom Tom.
\CONTACTS\ CALLERS.TXT	Lista de contactos del teléfono conectado a Tom Tom.
\CONTACTS\ CONTACTS.TXT	Números de teléfonos de llamadas realizadas desde el teléfono conectado a Tom Tom.
\CONTACTS\ INBOX.TXT	Mensajes recibidos desde el teléfono conectado a Tom Tom.
\CONTACTS\ OUTBOX.TXT	Mensajes enviados desde el teléfono conectado a Tom Tom.
NOMEFILE.ITI	Itinerarios guardados.
TEMPORARY.ITI	Itinerarios no guardados con un nombre.
Last GPS Fix	Últimas coordenadas del GPS.
Last Journey	Último viaje realizado.
Triplog	Recolecta información, datos de uso anónimo, del usuario que lo permita. Si se habilita esta opción mientras se configura el dispositivo, en el sistema de archivo aparecerá la carpeta statdata, que contiene archivos con el nombre “triplog-yyyy-mm-dd.dat”, que están encriptados.
Espacio no asignado	Datos borrados; si se reconfigura el dispositivo, la información en vivo se pierde. En el espacio borrado puede quedar

	información de viajes y mapas anteriores.

a. Para visualizar los archivos .DAT, descargar el programa de libre disponibilidad Poledit de Microsoft.

b. Para cada ubicación se guarda la latitud y la longitud junto con un nombre asignado automáticamente y con un nombre editable de usuario y un número de su destino (hogar).

c. Los dispositivos Tom Tom se pueden sincronizar con el teléfono móvil como manos libres; es posible recuperar información en el dispositivo que normalmente se encontraría en el celular. Estos archivos son de texto y se visualizan con un editor de texto.

2. Analizar las herramientas de libre disponibilidad y comerciales en el laboratorio para evaluar su eficiencia:

a. MapSend Lite: www.magellan.com.

b. EasyGPS: www.easygps.com.

c. GPS Utility: www.gpsu.co.uk.

d. Tomtology: http://www.forensicnavigation.com/index.php/products/tomtology2.

3. Registrar, documentar y/o capturar pantallas con la información requerida.

CAPÍTULO 13
MISCELÁNEA

Características del software de bloqueo de escritura

1. La herramienta obtenida debe tener firma o hash en el momento de descarga.
2. Si tiene firma, se debe verificar si se encuentra listada en la Biblioteca de Referencia Nacional de Software National Software Reference Library.
3. Si no es de código abierto no se puede observar el algoritmo utilizado para el bloqueo de las operaciones que efectúan modificaciones en las controladoras de los discos rígidos.
4. La herramienta debe permitir la visualización de la totalidad del disco incluyendo las zonas protegidas como:
   a. HPA Host Protected Area (HPA) y
   b. Device Configuration Overlay (DCO).
5. Se debe verificar si la herramienta trabaja sobre la interrupción 13.
6. La herramienta se debe probar en el laboratorio acorde al procedimiento sugerido por el NIST y pasar exitosamente las pruebas.
7. Verificar si la herramienta ha sido probada por el NIST.
8. Se debe efectuar el hash del disco rígido antes y después de utilizar la herramienta de software de bloqueo de escritura.

Procedimiento del uso de software bloqueador de escritura

1. Verificar la herramienta en el laboratorio.
2. Efectuar hash de la herramienta.
3. Efectuar hash de los dispositivos de almacenamiento dubitados.
4. Instalar la herramienta de software bloqueador de escritura en la computadora forense.
5. Configurar las opciones de bloqueo de escritura predeterminada de los dispositivos

   (USB, IEE1394, IDE, SCSI).
6. Reiniciar la computadora, el software debe iniciarse automáticamente y visualizarse como activo.
7. Conectar el dispositivo dubitado.
8. Visualizar el estado de los dispositivos bloqueados.

9. Analizar con la herramienta el dispositivo dubitado. La herramienta debe mostrar, si existe, los sectores de HPA y DCA del dispositivo dubitado.

10. Efectuar el hash del disco dubitado.

11. Comparar el hash del disco dubitado previo al análisis y el hash realizado posteriormente al análisis.

12. Desconectar el dispositivo dubitado.

referencia acerca del software bloqueador de escritura

Computer Forensics Tool Testing (CFTT), del NIST, Instituto Nacional de Tecnologías y Estándares, (http://www.nist.gov/index.html) del Departamento de Comercio de EEUU.

Software Write Block Tool Specification & Test Plan, Version 3.0 September 1, 2003 http://www.cftt.nist.gov/documents/SWB-STP-V3_1a.pdf

"El requisito principal de un examen forense de la evidencia digital es que no se debe modificar la evidencia original... es decir los contenidos del disco no se deben cambiar.

El investigador sigue una serie de procedimientos diseñados para evitar la ejecución de cualquier programa que pueda modificar los contenidos del disco, pudiendo utilizar algunas de las siguientes estrategias:

- Utilizar un software bloqueador de escritura (SWB) para interceptar cualquier escritura inadvertida al disco
- Utilizar un hardware bloqueador de escritura

[...] las pruebas se refieren a los bloqueadores de escritura por software que protegen el acceso al disco a través de la interrupción 0x13 del BIOS de la computadora.

Un software de bloqueo de escritura funciona monitoreando los comandos de entrada y salida del dispositivo enviados desde la computadora a través de una determinada interfaz de acceso al dispositivo. Cualquier comando u orden que pudiera modificar el disco rígido será interceptado o bloqueado y no pasará por la controladora del disco.

[...] El conjunto de comandos u órdenes para una determinada intefaz pueden dividirse en las siguientes categorías:

Write Escritura: Comandos que transfieren datos desde la memoria de la computadora al disco.

Configuration Configuración: Comandos que cambian cómo se presenta el disco en la computadora. Estos comandos a menudo destruyen los datos en el dispositivo o lo hace inaccesible a los datos.

Read Lectura: Comandos que transfieren datos desde el dispositivo a la

memoria de la computadora.

Control Control: Comandos que solicita el disco para hacer operaciones no destructivas, por ejemplo búsquedas o reinicio.

Information Información: Comandos que devuelven información sobre el disco. Miscellaneous Miscelánea: Comandos que no se incluyen en las categorías anteriores. [...] El uso de un software bloqueador de escritura cambia las operaciones normales de la interrupción 0x13.

Operación

1. Se ejecuta el software bloqueador de escritura. La herramienta guarda la dirección de memoria de entrada de la actual rutina de interrupción 0x13 e instala una nueva rutina de interrupción 0x13.
2. La herramienta inicia una operación de entrada salida en el disco invocando a la interrupción 0x13. El reemplazo de la rutina instalada por el software bloqueador de escritura intercepta el comando.
3. La herramienta determina si el comando solicitado debería ser bloqueado o si el comando debería ser permitido.
4. Si un comando es bloqueado, el software de bloqueo de escritura vuelve al programa sin pasar ningún comando a las rutinas de entrada-salida de la BIOS: Dependiendo de la configuración del software de bloqueo de escritura puede devolver un resultado de éxito o fallo.
5. Si el comando está permitido (no bloqueado), el comando pasa al BIOS y la rutina de entrada-salida del BIOS solicita el comando de entrada-salida (ATA, SCSI u otro) a la controladora del disco de manera tal que la operación de entrada-salida deseada se produce en el disco rígido.
6. Los resultados se devuelven al programa.

[...] Requisitos

Los requisitos obligatorios para las herramientas de software de bloqueo de escritura son los siguientes:

- La herramienta no debe permitir que un dispositivo protegido sea modificado.
- la herramienta no evitará la obtención de cualquier información de o acerca de cualquier dispositivo.
- La herramienta no evitará ninguna operación sobre un dispositivo que no está protegido.

Estos tres requerimientos son esenciales para una herramienta de software de bloqueo de escritura: proteger la evidencia de alteraciones mientras se permite un completo examen de la misma.

[...]

Requisitos para las funciones obligatorias

· SWB-RM-01. La herramienta deberá bloquear cualquier comando a un disco protegido en las categorías de escritura, configuración o misceláneas.

· TSWB-RM-02. La herramienta no bloqueará ningún comando a un disco protegido en las categorías de lectura, control o información.

· SWB-RM-03. La herramienta avisará al usuario que la herramienta está activa.

· SWB-RM-04. La herramienta informará sobre todos los dispositivos accesibles a través de las interfaces controladas por la herramienta.

· SWB-RM-05. La herramienta deberá informar sobre el estado de protección de todos los dispositivos.

· SWB-RM-06. La herramienta deberá, si así está configurada, ajustar el valor devuelto de cualquier comando bloqueado para indicar que la operación se llevó a cabo con éxito aun cuando la operación fuera bloqueada.

· SWB-RM-07. La herramienta, si así está configurada, ajustará el valor de cualquier comando bloqueado para indicar que la operación falló.

· SWB-RM-08. La herramienta no deberá bloquear ningún comando de un disco no protegido.

Proceso de prueba de herramientas por parte del NIsT

1. NIST obtiene la herramienta para la prueba.
2. NIST revisa la documentación de la herramienta.
3. NIST selecciona los casos relevantes de la prueba dependiendo de las funcionalidades que soporta la herramienta.
4. NIST desarrolla una estrategia de prueba.
5. NIST ejecuta las pruebas.
6. NIST genera un informe con los resultados obtenidos.
7. El comité revisa los informes de la prueba.
8. El vendedor revisa los informes de las pruebas (Vendor reviews test report).
9. NIST publica el software de soporte en la web.
10. NIJ publica el informe de la prueba en la web".

NIJ National Institute of Justice http://www.nij.gov/topics/forensics/evidence/digital/ standards/cftt.htm

El Instituto Nacional de Justicia de EE.UU. es la agencia de investigación, desarrollo y evaluación del Departamento de Justicia de EE.UU. Su misión es

mejorar la administración de justicia y seguridad pública.

Referencia

Examen forense de la evidencia digital:

Una guía para la Justicia del Departamento de Justicia de EE.UU. Programa de la Oficina de Justicia de EE.UU.

Instituto de Justicia de EE.UU.

Forensic Examination of Digital Evidence:

A Guide for Law Enforcement U.S. Department of Justice Office of Justice Programs

National Institute of Justice

"Disconnect storage devices (using the power connector or data cable from the back of the drive or from the motherboard) to prevent the destruction, damage, or alteration of data", Chapter 3. Evidence Acquisition, pág 22.

Desconectar los dispositivos de almacenamiento (utilizando el conector cable de alimentación o el cable de transmisión de datos de la parte posterior del dispositivo o de la placa madre) para evitar la destrucción, daño o alteración de los datos.

La protección de escritura se debe iniciar, si es posible, para preservar y proteger la evidencia original.

Nota: El investigador o perito debería considerar la creación de un valor conocido para el tema de la evidencia previamente a la obtención de la misma (por ejemplo, ejecutar una verificación de redundancia cíclica [CRC], hash [certificación matemática o firma]). Dependiendo del método de obtención seleccionado, este proceso pudo haberse ya completado.

- En el caso de que se utilice hardware de protección de escritura:
  - Instalar un dispositivo de protección de escritura.
  - Reiniciar el sistema con el sistema operativo del investigador.
- En el caso de utilizar software de protección de escritura:
  - Reiniciar el sistema con el sistema operativo del investigador.
  - Activar la protección de escritura.

referencia

software bloqueador de escritura

"Los bloqueadores de escritura por software no son tan efectivos como los bloqueadores por hardware porque pueden aun pasar el BIOS y escribir datos directamente a la controladora y el BIOS puede aun escribir datos al disco porque tiene acceso directo a la controladora. En general, si usted quiere controlar el acceso a un dispositivo, usted debería ubicar los controles tan

cerca del dispositivo como sea posible. El hardware de bloqueo de escritura está tan cerca del disco rígido como sea posible, sobre el cable de la controladora". Carrier, Brian. File System Forensic Analysis, Addison Wesley, USA, 2005, pág. 55.

Dispositivos BlackBerry

Imágenes del simulador de BlackBerry

Consideraciones previas

Los dispositivos de teléfonos móviles inteligentes o smartphones del tipo BlackBerry (http://www.blackberry.com/), pertenecen a la compañía RIM (Research In Motion) de Canadá. El teléfono ofrece las facilidades propias de los teléfonos inteligentes. Es reconocido en el mercado porque posee un teclado incorporado del tipo QWERTY y por su capacidad de manejo del correo electrónico de Internet por medio del acceso al proveedor de servicio de telefonía móvil.

El microprocesador varía acorde al modelo: pueden ser de la línea de Intel, de ARM y de QualComm con diseño adoptado de ARM. El sistema operativo BlackBerry es de código propietario de RIM escrito en Java y C++, el núcleo o kernel está escrito en Java (ejemplo: BlackBerry 7.01). Acorde a los modelos, el tamaño de la memoria interna (RAM), la eMMC y la memoria externa (tarjeta SD o micro SD) puede variar. El módem le permite conectar a redes GSM. Presenta conexiones para redes inalámbricas, conexiones Bluetooth y para efectuar los resguardos se conecta a la computadora por medio del puerto USB.

Los dispositivos BlackBerry se pueden integrar en un sistema de correo dentro de la organización a través de la aplicación BlackBerry Enterprise Server (BES), con versiones compatibles para el servidor de correo Microsoft Exchange, Lotus Domino y para Novell GroupWise. El servicio BES se conecta

con el servicio de Internet de BlackBerry (BlackBerry Internet Service BIS), disponible en numerosos países para los clientes y las empresas que utilizan el dispositivo, y con la posibilidad de configurar cuentas de correo no solo propietarias, sino también de proveedores como Gmail, Hotmail, Yahoo, etc.

Algunos dispositivos contienen una clave de protección de acceso. El usuario puede proteger sus datos con una clave y especificar la cantidad de intentos para ingresarla antes de que se borre en forma segura toda la información del dispositivo y vuelva a su estado original de fábrica. El perito debe tener especial cuidado en este aspecto ya que toda la información contenida en la memoria del dispositivo se borrará, sin posibilidad de recuperarla. La tarjeta micro SD no se verá afectada. El teléfono se podrá seguir utilizando y no existirán cambios en el sistema operativo.

Tipos de almacenamiento de archivos en dispositivos BlackBerry

(http://docs.blackberry.com/en/admin/deliverables/4322/Erasing%20file%on%20BlackBerry%20devices%20-%204.1.6%20-%20Technical%20Overview.pdf, junio 2012)

Tipos de memorias	Descripción
Memoria Flash interna del dispositivo	Es un sistema de archivo que almacena datos de la aplicación y del usuario. No puede ser removida físicamente del dispositivo BlackBerry. Los sectores de la memoria pueden guardar información de archivos descargados del usuario o almacenados manualmente en el dispositivo de memoria. El almacenamiento no volátil se mantiene en la memoria Flash y solo puede ser sobrescrito por el sistema operativo de BlackBerry. El código fuente de las aplicaciones de terceros no pueden escribir en el sector no volátil. El tamaño de fábrica de la memoria NAND es mayor que lo enunciado en las especificaciones de la memoria, generalmente esto soluciona los problemas de desplazamiento de las páginas dañadas que están presentes en el momento del proceso de fabricación de la memoria. Se debe tener en cuenta este aspecto al momento de realizar la adquisición física de la memoria Flash con diversas herramientas. El dispositivo elimina el contenido de la memoria durante el proceso de borrado seguro del dispositivo.
Sistema de archivo de la tarjeta de memoria,	Almacena los archivos que el usuario guarda en forma manual. El sistema de archivos de la memoria externa puede ser: instalado, accedido, encriptado y formateado en los dispositivos de BlackBerry. En el caso del inicio de un proceso de borrado seguro, no se le dará

externa al dispositivo (tarjeta removible)	formato al sistema de archivo de la memoria externa, al menos que tenga configurada una política que lo permita.

Etapa de identificación, registro, protección, embalaje y traslado

El procedimiento a seguir es similar al de aplicación general para teléfonos celulares, por lo tanto el perito debe seguir la misma secuencia de pasos.

Procedimiento: El dispositivo tiene el código de acceso

Si no se conoce la contraseña de acceso, solo recolectar la información de la tarjeta micro SD en el laboratorio.

Etapa de recolección y adquisición

Procedimiento para la adquisición física de datos

La recolección física se puede realizar utilizando productos comerciales tales como:

• Paraben

http://www.paraben-forensics.com/blackberry/forensic-software.html, la adquisición se realiza a través de RIM BlackBerry Physical Plug-in; este permite la adquisición de una imagen de la memoria y de las bases de datos del dispositivo. Dispositivos con sistema operativo Java (3.7, 3.8, 4.0.0, 4.1.0, 4.2.1, 4.5.0, 4.6.0, 4.6.1, 5.0.0, 6.0.0, 7.0.0, 7.1.0).

Los datos a adquirir son los siguientes:

- Libreta de direcciones.
- Autocompletar texto.
- Calendario.
- Categorías.
- Sistema de archivo (bases de datos).
- Agente de manos libres.
- Lista de favoritos.
- Memos.
- Mensajes.
- Registro de llamadas.
- Contactos de discado rápido.
- Libro de servicios.

- Mensajes SMS.
- Tareas.

• Cellebrite

http://www.cellebrite.com/mobile-forensics-products/solutions/blackberry-forensics.html, efectúa la adquisición física con software propietario y decodificación del dispositivo para las versiones del sistema operativo BlackBerry 4, 5, 6 y 7. El desencriptado en tiempo real está disponible para ciertas versiones del dispositivo. Los datos que obtiene la herramienta son:

- Libreta de direcciones con fotos de los contactos.
- Mensajes SMS y MMS.
- Mensajes de correo electrónico y PIN.
- Contactos de correo electrónico reciente.
- Dispositivos Bluetooth.
- Calendario.
- Notas.
- Historial del navegador web.
- Marcadores de páginas web.
- Cookies.
- Mensajería en línea de BlackBerry contactos y chats.
- Historial de la mensajería en línea de BlackBerry si está habilitada por el usuario.
- Aplicaciones instaladas.
- Información del dispositivo (modelo, IMEI, MEID, ICCID, PIN, redes soportadas por la versión del sistema operativo).

El PIN de BlackBerry asignado a cada dispositivo es un número de identificación de ocho caracteres en hexadecimal; acceder a través del menú Configuración | Opciones:

Procedimiento para la adquisición de datos a partir del archivo de resguardo

Consideraciones previas

El archivo de resguardo puede ser del tipo .ipd o .bbb para el sistema operativo Macintosh, estos archivos son del tipo .zip comprimidos que contienen al archivo .ipd. Este procedimiento es para realizar en el laboratorio de forma tal que el perito conozca las características del dispositivo.

1. En la estación de trabajo de telefonía forense instalar:

a. El programa de escritorio para el sistema operativo Mac o Windows, descargar el archivo del sitio: http://us.blackberry.com/support/apps-and-software/desktop-pc. html.

b. El simulador de BlackBerry: https://swdownloads.blackberry.com/Downloads/browseSoftware.do

c. El software de desarrollo para BlackBerry: https://developer.blackberry.com/devzone/resources#simulator

d. El software de soporte: https://swdownloads.blackberry.com/Downloads/browseSoftware.do

2. Ejecutar el simulador instalado:

a. En la barra del menú principal de la ventana del simulador, seleccionar Simular, Conectar cable USB.

3. Ejecutar el programa de Escritorio de BlackBerry:

a. Seleccionar Dispositivo, Cambiar de dispositivo, aparece la opción del BlackBerry a conectar, elegir el dispositivo.

b. En el menú Dispositivo, seleccionar la opción de Realizar copia de seguridad, elegir la carpeta en donde se guardará el archivo y realizar la copia.

4. Verificar la carpeta de destino en donde se guardó la copia de seguridad.

5. Registrar, documentar y/o capturar pantallas con la información requerida.

Etapa de análisis de datos

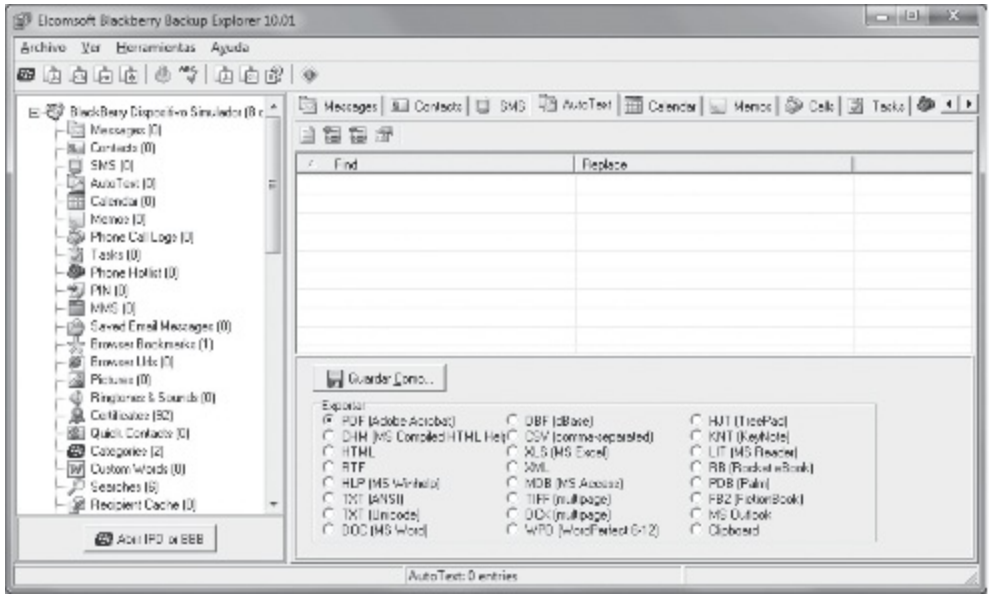
Procedimiento para el análisis de los datos del archivo de resguardo

La información recolectada en el archivo de resguardo .ipd o .bbb se puede analizar con las aplicaciones que efectúan la conversión de los archivos de resguardo:

- Herramienta ABC Amber Converter de Process Text Group (http://www.processtext.com/ abcblackberry.html), actualmente la

comercializa ElComSoft con el nombre Elcomsoft BlackBerry Backup Explorer; se puede descargar una versión de prueba de http://www.elcomsoft.com/ebbe.html.

- Soporta resguardos realizados con las computadoras de escritorio y con Mac.
- Permite analizar, imprimir y exportar la información.
- Soporta diversos formatos para exportar los datos, incluyendo PDF y HTML.
- Hipervínculos a la tabla de contenidos en diversos formatos para exportar en RTF/ DOC/PDF/HTML facilitando la navegación.
- Cifrado opcional y restricciones de acceso para los archivos exportados en PDF.
- Soporta resguardos encriptados.
- Personalización de la interfaz del usuario y multilenguaje con soporte internacional.
- Procesamiento por lotes y línea de comando.



· Herramienta de libre disponibilidad: MagicBerry, http://menastep.com/pages/magicberry.php, permite leer, convertir y extraer del resguardo .IPD las bases de datos de mensajes SMS, Registro de llamadas, Libreta de direcciones, Tareas, Memos, Calendario, archivos multimedia (PNG, JPG, MP3) y exportarlos.

· Herramienta comercial Oxygen-forensic Suite 2012, entre otras facilidades permite analizar los archivos de resguardo del tipo .ipd. La versión estándar es de libre disponibilidad por seis meses; para su descarga se solicitan los datos de nombre, empresa y correo electrónico. http://www.oxygen-

forensic.com/en/freeware/. En el sitio, se pueden descargar archivos de ejemplos de resguardo de diversos teléfonos, incluido el dispo·

sitivo de BlackBerry, los cuales se pueden utilizar con la herramienta para efectuar las pruebas en el laboratorio del perito. http://www.oxygen-forensic.com/en/download/.

Procedimiento para el análisis de archivos de imágenes

Consideraciones previas

Los archivos de imágenes se pueden adquirir a partir de la recuperación de las imágenes borradas, efectuando la recolección de los fragmentos de los archivos eliminados que aún se encuentran en la estructura del sistema de archivo. En la recuperación se pueden obtener imágenes con pérdida de fragmentos o con la falta del encabezado del archivo. La búsqueda de fragmentos de archivos se realiza a partir del encabezado conocido del archivo hasta el fin o pie del archivo. La recuperación a partir de los fragmentos puede recomponer la imagen con fragmentos que no son secuenciales. En el análisis de la imagen, es importante determinar si ha sido modificada o es original. Las imágenes pueden ser capturadas desde diferentes fuentes: cámara digital, cámaras digitales incorporadas en diferentes dispositivos como celulares, computadoras, escáner, o creadas directamente por computadora a través de un programa específico.

La cámara digital está compuesta por los siguientes elementos, los cuales pueden variar según el fabricante:

· Lente u objetivo (combinación de lentes convergentes y divergentes).

· Sensor digital, dispositivo de carga acoplada o sensor fotográfico, CCD (charge-coupled device, dispositivo de carga acoplada, células fotoeléctricas), o dispositivo del tipo CMOS (Complementary Metal Oxide Semiconductor, Semiconductor de óxido Metálico Complementario). En el caso del dispositivo CCD, el sensor captura los fotones recibidos por el objetivo o las lentes y los convierte en impulsos eléctricos analógicos, o pueden ser directamente transformados en impulsos digitalizados en el caso del sensor de tipo CMOS. Los sensores poseen un filtro de color (CFA, color filter array, RGB: Red Rojo, Green Verde, Blue Azul o CMY: Cyan, Magenta, Yellow -Amarillo).

· Dispositivo convertidor de analógico a digital (CCD, Analog Digital Converter), controla el componente electrónico de la cámara digital, efectúa el procesamiento de las imágenes para luego de la digitalización enviarlas a un área de almacenamiento como puede ser la tarjeta de memoria.

· Visor o pantalla de cristal líquido (LCD) para la visualización de la escena previamente a la captura de la imagen o posterior a su adquisición.

· Flash, micrófono, botones de control, botón de disparo, batería, cable de conexión USB y otros accesorios.

El proceso de captura de una imagen se produce cuando la luz ingresa a través de la lente y de los filtros ópticos de la cámara digital y luego es procesada por un conjunto de sensores de color CMOS (utilizado en celulares) o CCD que registran la imagen mediante un programa específico del dispositivo. Los detectores pueden contener un filtro de Bayer (colores RGB: rojo, verde y azul; la interpolación de dos cubos verdes, uno rojo y uno azul forman un pixel. http:// es.wikipedia.org/wiki/Mosaico_filtro_de_color). El número de células fotoeléctricas del sensor determinará el valor de la calidad de resolución de la imagen en píxeles. Los tipos de píxeles defectuosos están definidos en la norma ISO 13406-2 y son los máximos permitidos para los fabricantes. Pueden ser de tipo:

1. Pixel vivo o iluminado (siempre encendido, color blanco).
2. Pixel muerto (siempre apagado, color negro).
3. Pixel atascado (uno o más subpíxeles –rojo, azul, verde– siempre encendidos o siempre apagados).

Las imágenes pueden estar en blanco y negro, en escala de grises o en color.

El escáner utiliza detectores de tres líneas correspondientes a rojo, verde y azul. Las cámaras fotográficas y las de los celulares utilizan tres sensores independientes, uno para cada color. El método de captura de la imagen es de un solo disparo o de exposición única a la luz que ingresa por la lente de la cámara, registrando la escena en dos dimensiones, el conjunto o mosaico de filtro de colores (CFA, color filter array, RGB: Red Rojo, Green Verde, Blue Azul o CMY: Cyan, Magenta, Yellow -Amarillo) determina qué color se obtiene para cada pixel.

El mosaico de Bayer es un cuadrado de dos por dos, formado por un pixel rojo, uno azul y dos verdes. Por lo tanto, existe el doble de color verde, con lo cual la luminosidad se detecta mejor. El cuadrado de dos por dos se replica hasta formar la imagen completa. El resto de los dos colores para cada pixel se estima a través de un algoritmo de interpolación que es propio de cada dispositivo.

Luego de la interpolación de colores, la imagen pasa a otra etapa de procesamiento en donde se realizan las operaciones de:

· Balanceo de blanco.

· Reducción de ruidos. El ruido es la sensibilidad fotográfica a la luz o ruido digital, es un efecto no deseado que altera la imagen, es una variación en el brillo y en los valores del índice de exposición y velocidad establecidos en la norma ISO 12232:2006 –especificaciones ASA y DIN unificadas–. El ruido

puede aparecer durante la captura, transmisión o procesamiento de la imagen.

· Corrección de color.

· Compresión JPEG (Joint Photographic Experts Group). En las cámaras digitales, esta compresión puede ser del 100%, en las cámaras incorporadas en los celulares puede reducirse para preservar el espacio en memoria (generalmente 640x480 píxeles). La diferencia en la compresión define el uso de métodos de análisis diferentes para las cámaras digitales y para las incorporadas en los celulares.

El ruido es una variación aleatoria de la información del brillo o color en las imágenes, puede producirse por los sensores o circuitos de un escáner o cámara digital. Los ruidos son del tipo:

• Impulsivo o también llamada efecto de sal y pimienta, los píxeles son muy diferentes en cuanto a la intensidad o color, y por lo tanto, no tienen relación alguna con el resto de los píxeles que componen la imagen. Dicha imagen está formada por píxeles oscuros (muertos o sin luz) en zonas brillosas y píxeles brillosos en zonas oscuras. El pixel toma valores no ideales, máximo (sal) o mínimo (pimienta). Este ruido puede producirse por errores en la conversión de la imagen de analógico a digital, en la transmisión de los bits, por problemas en los sensores CCD o CMOS, se puede eliminar con herramientas como Topaz Denoise, complemento de Photoshop, versión de prueba: http://www.topazlabs.com/denoise/.

• Gaussiano o amplificador de ruido, el modelo estándar de amplificador de ruido es aditivo e independiente de la señal, afectando la intensidad de todos los píxeles. El valor del pixel tiende a ser ideal con una reducida cantidad de error, apareciendo pequeñas variaciones en la imagen.

• Uniforme, distribución uniforme del ruido en la imagen y puede ser dependiente de la señal o independiente de la señal si otra fuente produce un ruido mayor para causar un aumento de la profundidad del color (tramado). Puede ser del tipo uniforme por frecuencia: la imagen es afectada por una interferencia de señal periódica o puede ser del tipo multiplicativo: la señal es el resultado de la multiplicación de dos señales.

• De disparo, relacionado con la variación del número de fotones captados en un nivel de exposición determinado. El ruido de cada pixel es independiente del otro.

En las cámaras digitales con lentes digitales únicas o intercambiables (Digital Single Reflex Lens, DSRL), la acumulación de partículas de polvo se adosan al sensor creando un patrón o marca que se refleja en la captura de las imágenes o fotografías. Esta marca se mantiene en todas las imágenes capturadas hasta que se efectúe la limpieza de la lente.

Esta característica puede ser utilizada como un método de identificación de los dispositivos en base al rastro o marca o traza que deja el polvo en el sensor (A. Emir Dirik, Husrev T. Sencar, Nasir Memon, http://isis.poly.edu/~forensics/PAPERS/8.pdf, junio 2012).

Existen diversos métodos para analizar las imágenes, uno de ellos es a través de la identificación de las variaciones existentes entre los diferentes tipos y modelos de dispositivos de captura.

Las cámaras digitales presentan características particulares que pueden ser utilizadas para identificar las imágenes. Otro método es analizando el ruido de la imagen, comparando esta característica con el dispositivo dubitado, en el caso de que se pueda tener acceso al mismo, o comparando distintas imágenes entre sí para verificar la fuente de captura de estas. Cada modelo de cámara digital utiliza un método de interpolación, el cual puede ser utilizado para identificar el dispositivo de origen de captura de la imagen.

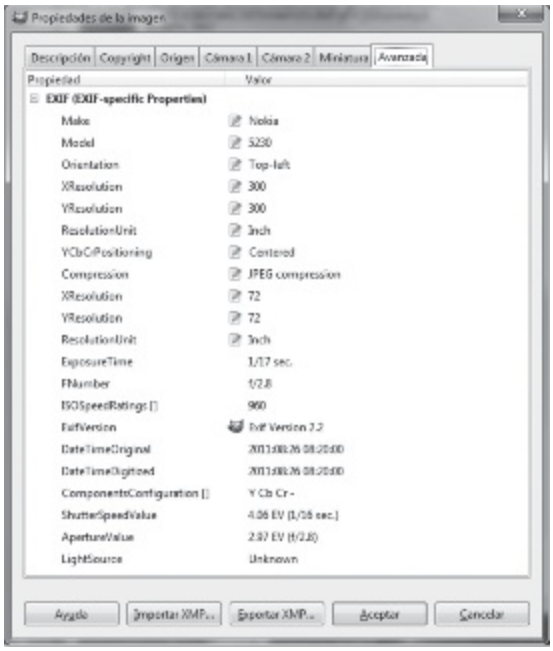
La información de la captura de la imagen se codifica según el estándar de formato EXIF (Exchangeable image file format, http://exif.org/exif2-2.pdf), en este archivo se puede obtener la descripción de cada uno de los datos incorporados a la información del archivo de tipo imagen o audio. El estándar define los valores para cada uno de los atributos que pueden ser analizados con un visor en hexadecimal. Esta información generalmente puede ser modificada o eliminada, por lo que no puede ser utilizada como información legítima y definitiva para el análisis de la imagen. La información que contiene el formato EXIF para imágenes es la siguiente:

- Fabricante.
- Modelo.
- Velocidad y latitud ISO del dispositivo de entrada o de la cámara digital, según lo especificado en la norma ISO 12232.
- Tiempo de exposición.
- Número F, apertura de la lente.
- Distancia focal.
- Modo de exposición.
- Balance de blanco.
- Fuente de luz.
- Versión de EXIF.
- Representación de color.
- Columnas de píxeles.
- Filas de píxeles.
- Coincidencia o no de luminancia y captación de color (YCbCrPositioning).

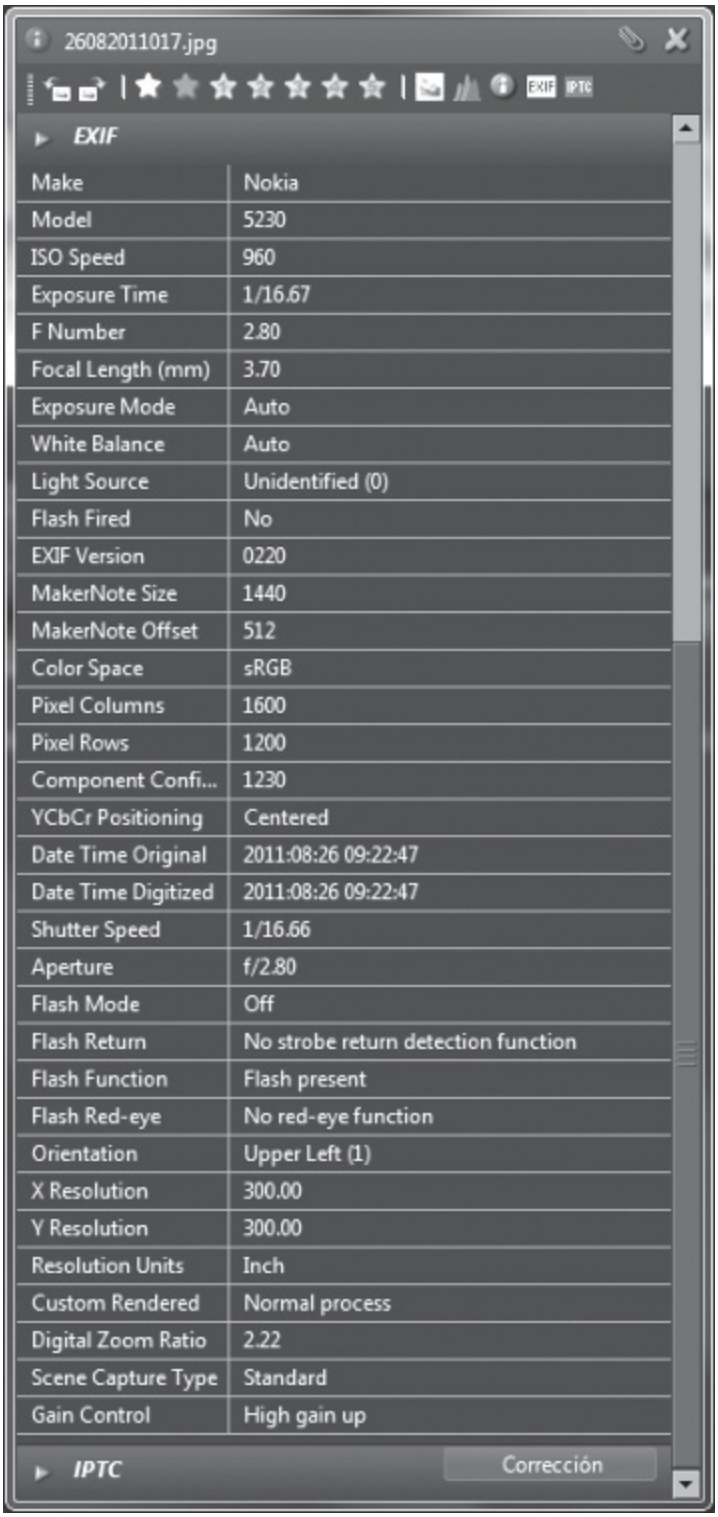
- Fecha y hora en que se capturó la imagen original.
- Fecha y hora en que la imagen se guardó como digitalizada.
- Velocidad del obturador en unidades APEX (Additive System of Photographic Exposure).
- Apertura de la lente en unidades APEX.
- Modo del flash, encendido o apagado.
- Estados del flash:
  - Disparado
  - Retornar
  - Función
  - Modo ojo rojo
- Orientación de la imagen vista en filas y columnas.
- Resolución X, ancho de la imagen en pulgadas para su impresión.
- Resolución Y, altura de la imagen en pulgadas para su impresión.
- Unidad de medida de la resolución, por ejemplo pulgadas.
- Procesamiento especial de la imagen, indica si la imagen recibió un tratamiento Normal o Personalizado.
- Coeficiente de Zoom, si no fue utilizado el valor será de 0.
- Tipo de escena capturada:
  - Estándar = 0
  - Paisaje = 1
  - Retrato = 2
  - Nocturna = 3
- Nivel de desviación de la exposición.
- Contraste.
- Saturación.
- Nitidez.

A continuación, ejemplos de la información que brinda EXIF:

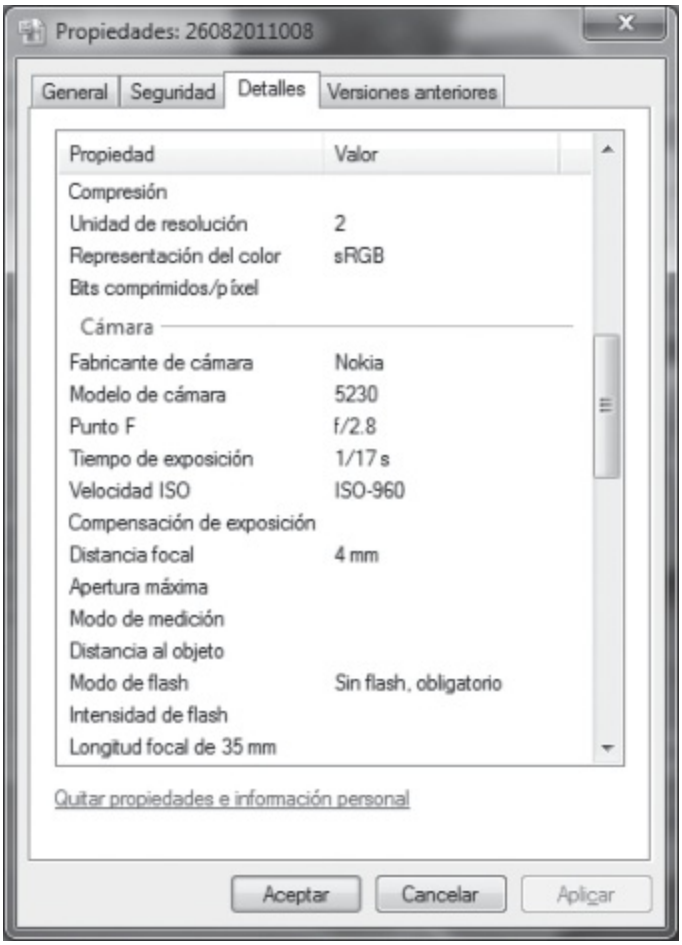
Programa Gimp (www.gimp.org)



Programa Helicon Photo Safe (http://www.heliconsoft.com/)



Propiedades de la imagen en el sistema operativo Windows



En las imágenes es posible obtener información a partir de:

- Los tres tipos de metadatos del archivo:
  - EXIF (Exchangeable image file format).
  - IPTC, se refiere al modelo de intercambio de información, Information Interchange Model, desarrollado por el Consejo de Telecomunicaciones de Prensa Internacional (IPTC, International Press Telecommunications Council). Originalmente creado para incorporar información de las imágenes utilizadas por los periódicos, lo utilizan los periodistas e industrias que producen imágenes para imprimir.
  - XMP, está basado en XML (eXtensible Metadata Platform), desarrollado por Adobe en 2001. Reemplaza a los esquemas de metadatos anteriores, es abierto y extensible.
- Los tipos o extensiones de los archivos de imágenes:
  - JPEG (Joint Photographic Experts Group), contiene una cantidad importante de metadatos, el formato JFIF: JPEG File Interchange Format, fue diseñado para incluir el modelo de colores (RGB, CMYK), densidad de píxeles, tamaño y proporciones e imágenes en miniatura para la

previsualización. Además de estos datos, el formato JPEG puede contener información de los metadatos EXIF, IPTC y XMP.

- GIF (Graphic Interchange Format), es un formato utilizado principalmente para íconos y gráficos simples, no presenta pérdidas de datos en la compresión beneficiando las zonas de color sólido. Este formato permite transparencia y animación. Este tipo de archivo no es generado por cámaras digitales o por dispositivos con cámara digital, por lo tanto no tiene incorporado información de metadatos de los dispositivos. La información que contiene se limita a los datos de la imagen y a campos de comentario. Los archivos GIF pueden tener etiquetas de metadatos XMP.

- PNG (Portable Network Graphics), formato de versión avanzada de GIF. La información se limita a los datos de la imagen, también pueden contener etiquetas de metadatos XMP como los archivos GIF.

- TIFF (Tagged Image File Format), formato de alta calidad con compresión. Es el formato predeterminado de la aplicación Instantánea (Grab). Es utilizado en publicidad y diseño gráfico. Es el formato predeterminado de muchas aplicaciones del sistema operativo Mac OS X. TIFF fue creado originalmente como un formato unificado para documentos escaneados y para fax. Estos archivos soportan etiquetas de metadatos internamente. Existen versiones extendidas de TIFF como la de GEOTIFF, utilizada para almacenar información de imágenes geográficas, y el formato de imagen de documentos de Microsoft para almacenar documentos escaneados o provenientes de fax. En muchas cámaras digitales utilizan el formato TIFF.

- Las características propias de la imagen:
  - las diferentes tonalidades de los colores de las capas de la piel de las personas, o de animales u objetos.
  - franjas o bandas de color.
  - texturas.
  - contornos o bordes.
  - ruido.
- La comparación de imágenes.
- La reconstrucción de los fragmentos de un archivo (encabezado, fin de archivo o pie).
- La identificación de rostros o caras, objetos, entorno.

Procedimiento de identificación de los metadatos del archivo de la imagen

1. Recuperar los distintos tipos de imágenes (JPG, TIFF, GIF, PNG) a partir de la imagen del dispositivo duplicado. Las herramientas a utilizar en este

procedimiento se pueden aplicar a los distintos tipos de formato de archivos de imágenes; la cantidad de información a extraer dependerá del tipo de extensión de los archivos.

2. Efectuar la certificación matemática (hash) de las imágenes.

3. En la estación de trabajo de Informática forense con el sistema operativo Linux, descargar e instalar la herramienta ImageMagick; en el sitio http://www.imagemagick.org/script/ binary-releases.php existen versiones para Linux, Windows, Mac OS X, iOS y Cygwin. Acorde al sistema operativo de la estación de trabajo de Informática forense, instalar la herramienta siguiendo las instrucciones de instalación descriptas en el sitio de descarga. Esta herramienta permite editar los metadatos.

4. Ejecutar la utilidad identify para extraer información detallada del archivo de la imagen con la opción verbose:

$identify –verbose /directoriodeimagenes/imagen01.jpg

Los datos que devuelve el comando son:

Format: JPEG (Joint Photographic Experts Group JFIF format) Class: DirectClass

Geometry: 1800x1200+0+0 Resolution: 480x480

Print size: 3.75x2.5 Units: PixelsPerInch Type: TrueColor Endianess: Undefined Colorspace: sRGB Depth: 8-bit

Channel depth: red: 8-bit green: 8-bit blue: 8-bit

Channel statistics: Red:

min: 0 (0)

max: 255 (1)

mean: 96.3031 (0.377659)

standard deviation: 65.8383 (0.258189)

kurtosis: -0.212353

skewness: 0.733548 Green:

min: 0 (0)

max: 255 (1)

mean: 96.0175 (0.376539)

standard deviation: 67.2174 (0.263598)

kurtosis: -0.317443

skewness: 0.731657 Blue:

min: 0 (0)

max: 255 (1)

mean: 99.0694 (0.388507)

standard deviation: 70.7571 (0.277479)
kurtosis: -0.774182
skewness: 0.58472 Image statistics: Overall:
min: 0 (0)
max: 255 (1)
mean: 97.13 (0.380902)
standard deviation: 67.9692 (0.266546)
kurtosis: -0.453897
skewness: 0.681507 Rendering intent: Perceptual Gamma: 0.454545
Chromaticity:
red primary: (0.64,0.33)
green primary: (0.3,0.6)
blue primary: (0.15,0.06)
white point: (0.3127,0.329)
Interlace: None
Background color: white
Border color: srgb(223,223,223)
Matte color: grey74
Transparent color: black
Compose: Over
Page geometry: 1800x1200+0+0
Dispose: Undefined
Iterations: 0 Compression: JPEG
Quality: 90
Orientation: Top
Left Properties:
date:create: 2012-08-07T18:40:38+01:00 (Metadato incorporado por el sistema de archivos)
date:modify: 2011-11-24T05:21:20+00:00 (Metadato incorporado por el sistema de archivos)
exif:ApertureValue: 316/100 exif:ColorSpace: 1
exif:ComponentsConfiguration: 1, 2, 3, 0
exif:Compression: 6
exif:Contrast: 0
exif:CustomRendered: 0
exif:DateTimeDigitized: 2011:11:23 19:33:02

exif:DateTimeOriginal: 2011:11:23 19:33:02
exif:DigitalZoomRatio: 0/10
exif:ExifImageLength: 1200
exif:ExifImageWidth: 1800
exif:ExifOffset: 340
exif:ExifVersion: 48, 50, 50, 49
exif:ExposureBiasValue: 0/10
exif:ExposureIndex: 80/1
exif:ExposureMode: 0
exif:ExposureProgram: 2
exif:ExposureTime: 13595/1000000
exif:FileSource: 3
exif:Flash: 25
exif:FlashPixVersion: 48, 49, 48, 48
exif:FNumber: 300/100
exif:FocalLength: 76/10
exif:FocalLengthIn35mmFilm: 45
exif:GainControl: 0
exif:InteroperabilityIndex: R98
exif:InteroperabilityOffset: 13816
exif:InteroperabilityVersion: 48, 49, 48, 48
exif:ISOSpeedRatings: 80
exif:JPEGInterchangeFormat: 13848
exif:JPEGInterchangeFormatLength: 4200
exif:LightSource: 0
exif:Make: EASTMAN KODAK COMPANY
exif:MakerNote: 67, 54, 49, 51, 32, 48, 48, 49, 48, 51, 48, 55, 48, 54, 0, 0
...(la información es extensa, aquí solo se muestra la primera línea)
exif:MaxApertureValue: 316/100
exif:MeteringMode: 5
exif:Model: KODAK EASYSHARE C613 ZOOM DIGITAL CAMERA
exif:Orientation: 1
exif:ResolutionUnit: 2
exif:Saturation: 0
exif:SceneCaptureType: 0
exif:SceneType: 1

exif:SensingMethod: 2
exif:Sharpness: 0 exif:ShutterSpeedValue: 620/100
exif:Software: KODAK EASYSHARE C613 ZOOM DIGITAL CAMERA
exif:SubjectDistanceRange: 0
exif:WhiteBalance: 0
exif:XResolution: 480/1
exif:YCbCrPositioning: 2
exif:YResolution: 480/1 jpeg:colorspace: 2
jpeg:sampling-factor: 2x2,1x1,1x1 signature:
6c63757b4dc2ed93e86af1dc55cb6166522e7fdb47c44a2fa1a4cf6066a0c285
Profiles:
Profile-exif: 18054 bytes Artifacts:
filename: 01.jpg verbose: true
Tainted: False
Filesize: 504KB
Number pixels: 2.16M
Pixels per second: 22.98MB
User time: 0.094u
Elapsed time: 0:01.093
Version: ImageMagick 6.7.8-7 2012-07-29 Q16 http://www.imagemagick.org identify.exe: Corrupt JPEG data: 25 extraneous bytes before marker 0xd9 `imagen01. jpg' @ warning/jpeg.c/JPEGWarningHandler/346.

5. Descargar la herramienta exiftool para la extracción de metadatos (http://www.sno.phy. queensu.ca/~phil/exiftool/), de libre disponibilidad y de licencia Perl (http://dev.perl. org/licenses/) para Windows, Mac OS X y Unix / Linux. Instalar la herramienta acorde a las instrucciones descriptas en el sitio. Esta herramienta permite editar los metadatos.

6. En la línea de comando, ejecutar el archivo exiftool.exe, previamente renombrado, asignarle la imagen a analizar y direccionar la salida a un archivo de texto, en el cual se registrará la información extraída de la imagen:

En Windows:

C:\exiftool>exiftool.exe imagen01.jpg > metadatos-imagen01.txt En Linux:

$exiftool imagen01.jpg > metadatos-imagen01.txt

La información contenida en el archivo de texto metadatos-imagen01.txt es la siguiente: ExifTool Version Number: 8.99

File Name: imagen01.jpg

Directory: .
File Size: 493 kB
File Modification Date/Time: 2011:11:24 05:21:20-03:00 File Permissions: rw-rw-rwFile Type: JPEG
MIME Type: image/jpeg
Exif Byte Order: Little-endian (Intel, II)
Make: EASTMAN KODAK COMPANY
Camera Model Name: KODAK EASYSHARE C613 ZOOM DIGITAL CAMERA
Orientation: Horizontal (normal)
X Resolution: 480
Y Resolution: 480 Resolution Unit: inches
Software: KODAK EASYSHARE C613 ZOOM DIGITAL CAMERA
Y Cb Cr Positioning: Co-sited
Exposure Time: 1/74
F Number: 3.0
Exposure Program: Program AE ISO: 80
Exif Version: 0221
Date/Time Original: 2011:11:23 19:33:02
Create Date: 2011:11:23 19:33:02
Components Configuration: Y, Cb, Cr, Shutter Speed Value: 1/74
Aperture Value: 3.0
Exposure Compensation: 0 Max Aperture Value: 3.0 Metering Mode: Multi-segment Light Source: Unknown
Flash: Auto, Fired Focal Length: 7.6 mm
Serial Number: C613 001030706 Flashpix Version: 0100
Color Space: sRGB
Exif Image Width: 1800 Exif Image Height: 1200
Interoperability Index: R98 DCF basic file (sRGB) Interoperability Version: 0100
Exposure Index: 80
Sensing Method: One-chip color area
File Source: Digital Camera
Scene Type: Directly photographed Custom Rendered: Normal Exposure Mode: Auto
White Balance: Auto Digital Zoom Ratio: 0

Focal Length In 35mm Format: 45 mm Scene Capture Type: Standard

Gain Control: None Contrast: Normal Saturation: Normal Sharpness: Normal

Subject Distance Range: Unknown Compression: JPEG (old-style) Thumbnail Offset: 13860

Thumbnail Length: 4200

Code Page: Unicode UTF-16, little endian Used Extension Numbers: 1

Extension Name: Screen Nail

Extension Class ID: 30020010-C06F-D011-BD01-00609719A180

Extension Persistence: Invalidated By Modification Extension Create Date: 1900:01:00 00:00:00

Extension Modify Date: 1900:01:00 00:00:00 Creating Application: Picoss

Extension Description: Presized image for LCD display Storage-Stream Pathname: /.Screen Nail_bd0100609719a180 Screen Nail: (Binary data 41401 bytes, use -b option to extract) Image Width: 1800

Image Height: 1200

Encoding Process: Baseline DCT, Huffman coding Bits Per Sample: 8

Color Components: 3

Y Cb Cr Sub Sampling: YCbCr4:2:0 (2 2) Aperture: 3.0

Image Size: 1800x1200

Preview Image: (Binary data 41261 bytes, use -b option to extract) Scale Factor To 35 mm Equivalent: 5.9

Shutter Speed: 1/74

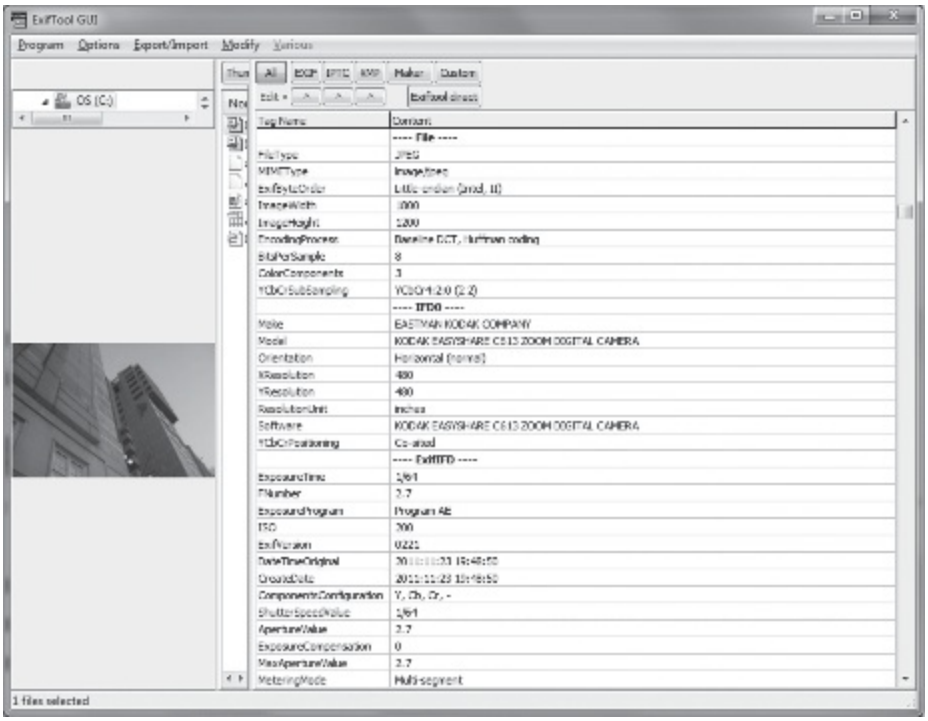
Thumbnail Image: (Binary data 4200 bytes, use -b option to extract) Circle Of Confusion: 0.005 mm

Field Of View: 43.6 deg

Focal Length: 7.6 mm (35 mm equivalent: 45.0 mm) Hyperfocal Distance: 3.79 m

Light Value: 9.7

Interfaz gráfica de la herramienta ExifToolGui en Windows: Permite ver todos los tipos de metadatos y exportarlos a un archivo de texto o html (http://freeweb.siol.net/hrastni3/)



8. Descargar e instalar la herramienta Exiv2 para la extracción de metadatos del sitio http://www.exiv2.org/download.html, disponible para Unix y Windows, de código abierto con licencia GNU GPL, también disponible en la versión comercial. Esta herramienta permite ejecutar el comando con diferentes modificadores y visualizar los datos ordenados por grupo y si es requerido en formato hexadecimal. Se deberá leer la ayuda para seleccionar los modificadores requeridos para las diferentes ejecuciones del comando. Esta herramienta permite editar los metadatos.

9. En la línea de comando ejecutar: En Windows:

C:\exiv2-0.23-win>exiv2.exe imagen01.jpg > metadatos-imagen01.txt En Linux:

$ exiv2 imagen01.jpg > metadatos-imagen01.txt

La información contenida en el archivo de texto metadatos-imagen01.txt es la siguiente: File name: 01.jpg

File size: 504452 Bytes

MIME type: image/jpeg Image size: 1800 x 1200

Camera make: EASTMAN KODAK COMPANY

Camera model: KODAK EASYSHARE C613 ZOOM DIGITAL CAMERA

Image timestamp: 2011:11:23 19:33:02 Image number:

Exposure time: 1/74 s Aperture: F3

Exposure bias: 0 EV Flash: Yes, auto Flash bias:

Focal length: 7.6 mm (35 mm equivalent: 45.0 mm) Subject distance:

ISO speed: 80 Exposure mode: Auto

Metering mode: Multi-segment Macro mode:

Image quality:

Exif Resolution: 1800 x 1200 White balance: Auto

Thumbnail: image/jpeg, 4200 Bytes Copyright:

Exif comment:

Ejecución del comando con los modificadores -pa, para obtener una información detallada (p: print, a: los metadatos EXIF, IPTC y XMP):

En Windows:

C:\exiv2-0.23-win>exiv2.exe –pa imagen01.jpg > metadatos-pa-imagen01.txt En Linux:

$ exiv2 -pa imagen01.jpg > metadatos-pa-imagen01.txt

Exif.Image.Make	Ascii	22 EASTMAN KODAK COMPANY
Exif.Image.Model	Ascii	41 KODAK EASYSHARE C613
ZOOM DIGITAL CAMERA		
Exif.Image.Orientation	Short	1 top, left
Exif.Image.XResolution	Rational	1 480
Exif.Image.YResolution	Rational	1 480
Exif.Image.ResolutionUnit	Short	1 inch
Exif.Image.Software	Ascii	41 KODAK EASYSHARE C613
ZOOM DIGITAL CAMERA		
Exif.Image.YCbCrPositioning	Short	1 Co-sited
Exif.Image.ExifTag	Long	1 340
Exif.Photo.ExposureTime	Rational	1 1/74 s
Exif.Photo.FNumber	Rational	1 F3
Exif.Photo.ExposureProgram	Short	1 Auto
Exif.Photo.ISOSpeedRatings	Short	1 80
Exif.Photo.ExifVersion	Undefined	4 2.21
Exif.Photo.DateTimeOriginal	Ascii	20 2011:11:23 19:33:02
Exif.Photo.DateTimeDigitized	Ascii	20 2011:11:23 19:33:02
Exif.Photo.ComponentsConfiguration	Undefined	4 YCbCr
Exif.Photo.ShutterSpeedValue	SRational	1 1/74 s
Exif.Photo.ApertureValue	Rational	1 F3
Exif.Photo.ExposureBiasValue	SRational	1 0 EV
Exif.Photo.MaxApertureValue	Rational	1 F3
Exif.Photo.MeteringMode	Short	1 Multi-segment
Exif.Photo.LightSource	Short	1 Unknown

Exif.Photo.Flash	Short	1 Yes, auto

Exif.Photo.FocalLength Rational 1 7.6 mm

Exif.Photo.MakerNote Undefined 12728 (Binary value sup ressed)

Ejecución del comando con el modificador -ph, para obtener la información en formato hexadecimal:

En Windows:

C:\exiv2-0.23-win>exiv2.exe –ph imagen01.jpg > metadatos-ph-imagen01.txt En Linux:

$ exiv2 -ph imagen01.jpg > metadatos-ph-imagen01.txt Ejemplo reducido del resultado del comando:

0x010f Image Make Ascii 22 22

0000 45 41 53 54 4d 41 4e 20 4b 4f 44 41 4b 20 43 4f EASTMAN KODAK CO

0010 4d 50 41 4e 59 00 MPANY.

0x0110 Image Model	Ascii	41 41

0000 4b 4f 44 41 4b 20 45 41 53 59 53 48 41 52 45 20 KODAK EASYSHARE

0010 43 36 31 33 20 5a 4f 4f 4d 20 44 49 47 49 54 41 C613 ZOOM DIGITA

0020 4c 20 43 41 4d 45 52 41 00 L CAMERA.

0x0112 Image Orientation Short 1 2

0000 01 00		..	

0x011a Image XResolution Rational 1 8

0000 e0 01 00 00 01 00 00 00 ....

0x011b Image YResolution Rational 1 8

0000 e0 01 00 00 01 00 00 00 ....

0x0128 Image ResolutionUnit Short 1 2

0000 02 00 ..

0x0131 Image Software Ascii 41 41

0000 4b 4f 44 41 4b 20 45 41 53 59 53 48 41 52 45 20 KODAK EASYSHARE

0010 43 36 31 33 20 5a 4f 4f 4d 20 44 49 47 49 54 41 C613 ZOOM DIGITA

0020 4c 20 43 41 4d 45 52 41 00 L CAMERA.

0x9003 Photo DateTimeOriginal Ascii 20 20

0000 32 30 31 31 3a 31 31 3a 32 33 20 31 39 3a 33 33 2011:11:23 19:33

0010 3a 30 32 00 :02.

0x9004 Photo	DateTimeDigitized Ascii	20 20

0000 32 30 31 31 3a 31 31 3a 32 33 20 31 39 3a 33 33 2011:11:23 19:33

0010 3a 30 32 00 :02.

10. Descargar e instalar la herramienta Hachoir-metadata para la extracción

de metadatos del sitio https://bitbucket.org/haypo/hachoir/downloads. Esta herramienta ofrece menos información que las aplicaciones Exiftool y Exiv2, pero tiene la ventaja de que en forma nativa es de solo lectura. Acorde al sistema operativo de la estación de trabajo, el perito deberá seguir las instrucciones de instalación. La aplicación está escrita en el lenguaje Python.

En Linux:

$hachoir-metadata imagen01.jpg

11. Analizar el contenido de los metadatos extraídos de la imagen e incorporarlos en una tabla o planilla para determinar:

- Origen del dispositivo que capturó la imagen (cámara fotográfica, filmadora, scanner, etc.), marca, modelo, número de serie.
- Fecha y hora de creación o captura de la imagen.
- Información de la configuración de las lentes de la cámara y/o dispositivo de captura de la imagen.
- Información de la configuración del dispositivo que capturó la imagen.
- Programa utilizado.
- Dimensiones de la imagen.
- Compresión.
- Información, si existiera, del GPS. En este caso obtener la información de las coordenadas y verificarlas en la aplicación de Google Maps, para determinar el lugar en donde se capturó la imagen.

12. Determinar el método de interpolación utilizado según marca y modelo del dispositivo.

13. Visualizar la imagen con un visor en hexadecimal, identificar la firma del tipo de archivo, encabezado y fin de archivo. Por ejemplo: TIFF: 49 20 49.

14. Efectuar la certificación matemática (hash) de las imágenes analizadas y comparar los resultados con los obtenidos en el paso 2., con el fin de verificar que no se hayan producido modificaciones en las imágenes al utilizar diversas herramientas en la extracción de los metadatos de dichas imágenes.

15. Registrar los datos, capturar pantalla y/o imprimir.

16. Efectuar el resguardo de los datos y de las herramientas utilizadas con sus respectivas certificaciones matemáticas (hash).

Análisis del contenido de la imagen

1. Identificar la presencia de ruido en la imagen.

2. Analizar los colores de la imagen, distribución y cantidad de píxeles por color, píxeles sin luz, presencia de píxeles que son diferentes en intensidad, brillo, color y que no tienen relación con el resto de los que conforman la imagen en la herramienta Gimp; en el menú principal seleccionar:

a. Imagen |Propiedades de la imagen | Propiedades y Perfil del color.
b. Colores | Info | Histograma.
c. Colores | Info | Análisis cubo de color.
d. Colores | Info | Promedio del borde.
e. Colores | Color a Alfa (convertir un color a transparente).
f. Colores | Colorear (reemplazo de colores por sombras de un color determinado).
g. Colores | Paquete de filtros (modificar colores en forma interactiva).
h. Colores | Retinex (aplicar el algoritmo MSRCR MultiScale Retinex with Color Restoration Retinex multiescala con restauración de color).
i. Colores | RGB max (reducir la imagen a colores rojo, verde y azul puros).
j. Colores | Mapa | Intercambio de color.
k. Colores | Mapa | Rotar los colores.
l. Colores | Umbral.
m. Colores | Niveles.
n. Colores | Curvas.
o. Colores | Posterizar.

3. Recortar la imagen por color, en la herramienta Gimp, en el menú principal seleccionar:

a. Imagen | Recorte Zealous (auto recortar los espacios sin los bordes).

4. Aplicación de valores de: brillo, contraste, esfumado, desenfoque, etc., en la herramienta Gimp, en el menú principal seleccionar:

a. Colores | Inversión del valor (Invertir los valores de brillo de los píxeles).
b. Colores | Balance de color.
c. Colores | Tonos de saturación.
d. Colores | Brillo y contraste.
e. Colores | Desaturar.

5. Aplicar diferentes acciones para detectar bordes y contornos de la imagen, en la herramienta Gimp, en el menú principal seleccionar:

a. Filtros | Detectar bordes:
   - Arista
   - Gaussiano
   - Laplace
   - Neón
   - Sobel
b. Imagen | Auto recortar (quitar bordes vacíos).

6. Visualizar trazas o marcas de polvo existentes en el objetivo o lente de la cámara y presentes en la imagen.

7. Analizar en las imágenes recuperadas:

a. Rotaciones.

b. Cambios en las dimensiones y perspectivas.

c. Recomposición por la acción de cortar y pegar otros elementos (objetos, rostros, etc.).

d. Diferencias de luminosidad.

e. Diferencias de colores en la piel, en el caso de las personas.

f. Estructura de las capas de colores en los objetos o animales.

8. Verificar la sensibilidad fotográfica o ruido digital, variaciones de brillo y color (uso de valores ISO –ASA y DIN unificados– elevados, exposiciones prolongadas, fotografías nocturnas).

9. Eliminar ruido de la imagen.

10. Verificar si la imagen en su totalidad ha sido generada por un único dispositivo o si alguna de las partes ha sido cortada y reemplazada por otra (cortar y pegar).

11. Verificar acciones y/o alteraciones aplicadas a la imagen como: cambios de tamaño, rotaciones, compensaciones de brillo y color, eliminación de detalles con filtros, incorporación de ruidos, compresión de una imagen ya comprimida pero con valores de calidad diferente que se reflejan en la distorsión de la suavidad y textura de la imagen en los histogramas de la imagen.

12. Efectuar correlación entre píxeles para determinar cambios de tamaño.

13. Verificar la incorporación de efectos de brillo o esfumados para determinar modificaciones de la imagen.

14. Efectuar la certificación matemática (hash) de las imágenes analizadas y comparar los resultados con los obtenidos en el paso 2., del “Procedimiento de identificación de los metadatos de la imagen” con el fin de verificar que no se hayan producido modificaciones en las imágenes al utilizar diversas herramientas para el análisis de estas.

15. Registrar los datos, capturar pantalla y/o imprimir.

16. Efectuar el resguardo de los datos y de las herramientas utilizadas con sus respectivas certificaciones matemáticas (hash).

Detección de rostros e imágenes de adultos

La dificultad en detectar imágenes de adultos se basa en algunos de los siguientes aspectos (http://www.jdl.ac.cn/user/wzeng/files/Zeng_accv2004.pdf):

- La variación de la iluminación.
- Digitalización en diferentes resoluciones.
- Las imágenes pueden ser una parte del cuerpo humano.
- La persona puede adoptar diferentes posturas.
- La persona puede estar en parte cubierta por la ropa.
- Algunas imágenes generadas por programas artísticos pueden ser semejantes a los adultos.

Los métodos de detección incluyen una serie de aspectos que permiten aislar las características necesarias para reconocer la imagen de adultos, a través de:

- La detección de los colores o píxeles de la piel, escala de grises.
- Eliminación del fondo o entorno que contiene a la imagen.
- Características de la textura de la piel, suele ser suave.
- Delimitación de los bordes y contornos de las regiones que se corresponden con el color de la piel.
- Detección de rostros para determinar si es de un adulto o de un niño.

1. Analizar en la imagen los siguientes aspectos:

a. Colores de la piel de la cara.

b. Características faciales: líneas, manchas, cicatrices, género, raza, edad (retrato hablado de Bertillón). En este sitio se pueden generar modelos de caras en línea: http://flashface.ctapt.de/.

c. Texturas.

d. Luminosidad.

e. Distancia de la captura de la imagen de la cara.

f. Calidad de la resolución de la imagen.

g. Posturas: frente, perfil, plano inclinado.

h. Expresiones de la cara: alegría, tristeza, miedo, disgusto, enojo, sorpresa, neutral.

i. Dimensiones y medidas de la cara: distancia entre cejas, entre párpados y cejas, grosor de los labios, ancho de la boca, nariz, mentón, dentadura.

Ejemplo obtenido con la herramienta Luxand FaceSDK, de Luxand, versión demo de descarga http://www.luxand.com:

2. Comparar la cara con las almacenadas en una base de datos: Consultar con bases de datos de reconocimiento de la morfología facial:

- En este sitio se encuentran referenciadas y numerosas bases de datos de rostros generadas por diversas universidades y áreas de investigación en detección y reconocimiento facial, http://www.face-rec.org/databases.
- Cohn-Kanade AU-Coded Facial Expression Database, http://www.pitt.edu/

~jeffcohn/ CKandCK+.htm.

- http://www.multipie.org/, ofrece múltiples imágenes de un conjunto de 337 personas obtenidas durante el período de cinco meses, utilizando quince puntos de enfoque diferentes y diecinueve variaciones de la iluminación.
- http://www.scface.org/, contiene imágenes estáticas de personas.
- MIT, CBCL (Center for Biological and Computational Learning), http://cbcl.mit. edu/software-datasets/heisele/facerecognition-database.html.
- Base de datos tridimensional de imágenes de rostros o caras para la investigación en la identificación y reconocimiento de personas del FBI, http://www. fbi.gov/about-us/lab/forensic-science-communications/fsc/april2008/research/2008_04_research01.htm/.

Herramientas para reconocimiento de caras

- OpenCV es una biblioteca libre de visión artificial originalmente desarrollada por Intel, http://opencvlibrary.sourceforge.net/.
- Luxand FaceSDK, de Luxand, versión demo de descarga

http://www.luxand.com.

- Detección y análisis de áreas de la piel en las imágenes, contornos:
  - Snitch, comercial, de Hyperdyne, con versión de prueba http://www.hyperdyne software.com/.
  - Paraben, comercial, de Paraben, es un dispositivo tipo pendrive que se conecta a la computadora y busca imágenes y videos pornográficos, http://www.parabensticks.com.

Herramientas para el análisis de los metadatos del archivo de la imagen

- Hachoir-metadata, de código abierto, extrae los metadatos de archivos comunes y de multimedia: música, videos y fotos, http://pypi.python.org/pypi/hachoir-metadata/1.2.1.
- Adroit Photo Forensics (Adroit Advanced Digital Recovery & Investigative Toolkit) de la empresa Digital Assembly, versión de prueba disponible luego de completar los datos de identificación. Permite recuperar las fotografías e imágenes a partir de archivos de imágenes generadas por el comando dd o por la aplicación Encase, de los espacios no asignados, de los espacios desperdiciados; efectúa análisis de los metadatos y fragmentos, de las imágenes; soporta los sistemas de archivos NTFS/FAT/HFS/HFS+; certifica matemáticamente las imágenes recuperadas con hash MD5 y SHA1/SHA256, http://digital-assembly.com/.

- Editores de imágenes y fotografías:
  - ImageMagic, de código abierto, disponible para Unix, iOS, Mac OS X y Windows. http://www.imagemagick.org.
  - HeliconFilter, comercial, de Helicon, versión de prueba, http://www.heliconsoft.com/.
  - HeliconPhotoSafe, libre disponibilidad, de Helicon, http://www.heliconsoft.com/.
  - iPhoto, comercial de Apple, http://www.apple.com.
  - Multithreaded DCRAW, código abierto, de Helicon, convierte numerosos formatos a partir de una imagen del tipo sin procesar o RAW. Soporta múltiples cámaras digitales (marcas y modelos), http://www.heliconsoft.com/dcraw.html.
  - Picasa, de Google, de libre disponibilidad, http://picasa.google.com/.
  - Photoshop, comercial, de Adobe, http://www.adobe.com/la/products/photoshop.html.
  - Complemento para eliminar el ruido en las imágenes, Neat Image Pro 5.6.
  - PhotoImpact, de Corel-Ulead, versión de prueba, http://www.corel.com/.
  - Paint Shop Pro, comercial, de Corel, versión de prueba,

http://www.corel.com/.

- Gimp, de código abierto, http://www.gimp.org/.

Procedimiento para el análisis de los archivos de audio y video

Consideraciones previas

Los archivos de audio pueden tener como contenido información de música, mensajes de voz o de cualquier otro material de grabación que permita ser escuchado. Los archivos de audio además del contenido específico que almacenan, también poseen información relevante en los metadatos, la cual le permite al perito en Informática forense identificar las características particulares del archivo. Los diferentes tipos de extensiones de los archivos de audio y video se pueden consultar en el sitio http://www.fileinfo.com/.

1. Recuperar los distintos tipos de archivos de audio y video a partir de la imagen del dispositivo duplicado. Las herramientas a utilizar en este procedimiento se pueden aplicar a los distintos tipos de formato de archivos de audio y video; la cantidad de información a extraer dependerá del tipo de extensión de los archivos.
2. Efectuar la certificación matemática (hash) de los archivos de audio y video.
3. Efectuar la certificación matemática (hash) de las imágenes analizadas y comparar los resultados con los obtenidos en el paso 2., con el fin de verificar que no se hayan producido modificaciones en los archivos de audio y video al utilizar diversas herramientas para el análisis de estos.
4. Registrar los datos, capturar pantalla y/o imprimir.
5. Efectuar el resguardo de los datos y de las herramientas utilizadas con sus respectivas certificaciones matemáticas (hash).

Tipos de archivos de audio y video

· WAV, Waveform Audio File Format, es un estándar para guardar una cadena de bits de audio, desarrollado originalmente por Microsoft e IBM para ser utilizado en las computadoras de escritorio. Los archivos de audio de tipo WAV se almacenan como una serie de fragmentos etiquetados dentro de un contenedor de formato de archivo de intercambio denominado RIFF (Resource Interchange File Format). Este formato soporta porciones de información, que contienen etiquetas de metadatos que también pueden ser del tipo XMP.

a. En la línea de comando ejecutar la herramienta:

$hachoir-metadata audio1.wav

El resultado del comando devuelve información sobre el nombre de la

aplicación que creó el archivo, nombre del autor, fecha y hora y datos relacionados con el archivo de audio.

b. En la línea de comando ejecutar la herramienta exiftool.exe, asignarle el archivo de audio a analizar y direccionar la salida a un archivo de texto, en el cual se registrará la información extraída del archivo de extensión .WAV.

En Windows:

C:\exiftool>exiftool.exe audio1.wav > metadatosaudio1.txt En Linux:

$exiftool audio1.wav > metadatosaudio1.txt

La información contenida en el archivo de texto metadatos-audio01.txt es la siguiente:

ExifTool Version Number: 8.99 File Name: AUDIO1.WAV Directory: .

File Size: 5.4 kB

File Modification Date/Time: 1997:07:11 08:37:00-03:00 File Permissions: rw-rw-rwFile Type: WAV

MIME Type: audio/x-wav Encoding: Microsoft PCM Num Channels: 1

Sample Rate: 11025

Avg Bytes Per Sec: 11025 Bits Per Sample: 8 Duration: 0.50 s

ExifToolVersion = 8.99 FileName = AUDIO1.WAV Directory = .

FileSize = 5524

FileModifyDate = 868621020

FilePermissions = 33206 FileType = WAV MIMEType = audio/x-wav

RIFF ‘fmt ‘ chunk (16 bytes of data): AudioFormat (SubDirectory) -->

+ [BinaryData directory, 16 bytes]

| Encoding = 1

| NumChannels = 1

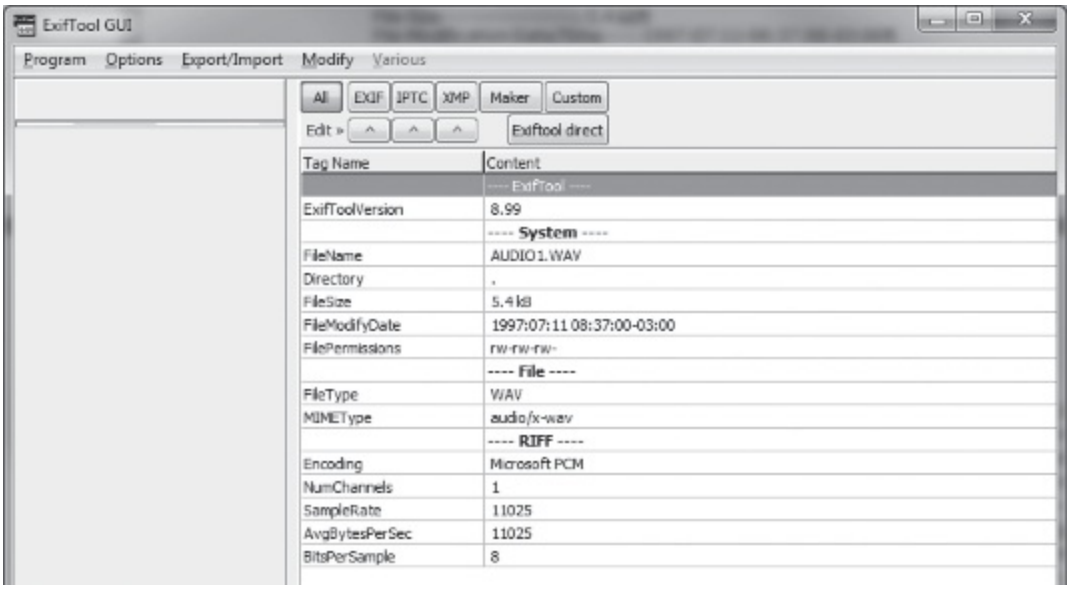
| SampleRate = 11025

| AvgBytesPerSec = 11025

| BitsPerSample = 8

RIFF ‘data’ chunk (5480 bytes of data):

c. Ejecutar en Windows la interfaz gráfica de la herramienta ExifToolGui y analizar los resultados de las diferentes etiquetas:



· MP3, o MPEG-1 Audio Capa III (estándar ISO/IEC 11172-3) o MPEG-2 Audio Capa III (estándar ISO/IEC 13818-3) es un formato de compresión de audio digital con un algoritmo de pérdida para reducir el tamaño del archivo, el cual pierde datos al ser descomprimido.

La compresión con pérdida puede realizarse con la técnica de códec (codificador-decodificador: codifica un flujo de datos o una señal para su transmisión, almacenamiento o cifrado, o lo decodifica para ser reproducido o editado; se utiliza en las aplicaciones de videoconferencias, de distribución de multimedia o de edición de video), diseñado por el grupo de expertos Moving Picture Experts Group (MPEG, estándar ISO/IEC 14496, Codificación de objetos audiovisuales) para formar parte del estándar MPEG-1 y del posterior, más extendido MPEG-2.

La tasa de compresión de bits influirá en la mayor o menor calidad del audio y en el tamaño del archivo. La compresión se basa en la capacidad de detección del oído humano para percibir la distorsión de los sonidos, es imperceptible para el oído normal a partir de los 128 Kbps o hasta 96 Kbps; en el caso de las personas con un oído experimentado, la compresión para escuchar los sonidos con claridad es desde los 192 Kbps a 256 Kbps. Los archivos MP3 contienen metadatos de dos tipos de formatos: ID3v1 e ID3v2 (http://www.id3.org/id3v2.3.0/).

Las etiquetas de ID3v1 están limitadas a un conjunto de 128 bytes agregados al final del archivo MP3. Las etiquetas ID3v1 extendidas agregan 227 bytes delante de las etiquetas ID3v1, limitando la cantidad de espacio para guardar metadatos, se crean las etiquetas ID3v2, las cuales no son de tamaño fijo y pueden contener mayor variedad de metadatos en comparación con las etiquetas ID3v1. Las etiquetas ID3v2 contienen información como: el título de

la pista, información del autor, cantante o artista e imágenes.

a. La herramienta ID3v2 obtiene etiquetas de los dos tipos de ID3. Existen versiones para Linux y Windows; acorde al sistema operativo seleccionado se deben seguir las instrucciones de instalación. Es una herramienta de código abierto y se puede descargar del siguiente sitio: http://sourceforge.net/projects/id3v2/files/latest/ download.

En Linux:

$id3info audio1.mp3

*** Tag information for audio1.mp3

*** mp3 info MPEG1/layer III Bitrate: 256KBps Frequency: 44KHz

Información de otras etiquetas en archivos de música:

= GEOB (General encapsulated object): (SfMarkers)[]: 12 bytes

= COMM (Comments): ()[eng]: Navona Records

= PRIV (Private frame): (unimplemented)

= PRIV (Private frame): (unimplemented)

= TPE3 (Conductor/performer refinement): Autor

= APIC (Attached picture): (thumbnail)[, 3]: image/jpeg, 36061 bytes

= TRCK (Track number/Position in set): 2

= TALB (Album/Movie/Show title): Nombre del álbum, Vol. 1

= TYER (Year): 2008

= TCON (Content type): (32)

= TPE2 (Band/orchestra/accompaniment): Intérprete

= TIT2 (Title/songname/content description): Nombre de la pieza musical

= TCOM (Composer): Nombre del compositor

= TPE1 (Lead performer(s)/Soloist(s)): Orquesta/Director

= COMM (Comments): ()[]:

= COMM (Comments): (ID3v1 Comment)[XXX]: Nombre de la empresa de grabación

c. En Linux, ejecutar la herramienta hachoir-metadata para analizar las etiquetas ID3:

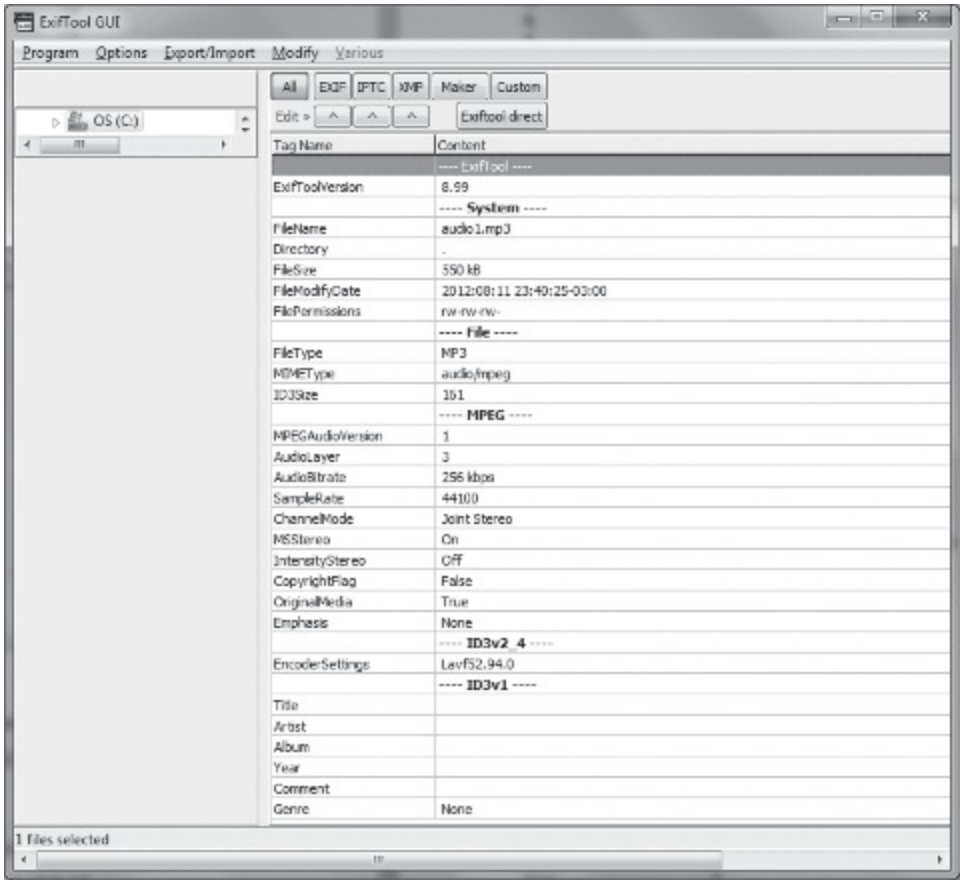
$hachoir-metadata audio1.mp3 metadatos-hachoiraudio1.txt

d. En Linux, ejecutar la herramienta exiftool:

$exiftool audio1.mp3 > metadatos-exiftool-audio1.txt

e. En Windows, en la línea de comando ejecutar la herramienta exiftool.exe, asignarle el archivo de audio a analizar y direccionar la salida a un archivo de

texto, en el cual se registrará la información extraída del archivo de extensión .MP3.



En Windows:

C:\exiftool>exiftool.exe audio1.mp3 > metadatos-exiftool-windowsaudio1.txt ExifTool Version Number: 8.99

File Name: audio1.mp3

Directory:.

File Size: 550 kB

File Modification Date/Time: 2012:08:11 23:40:25-03:00 File Permissions: rw-rw-rwFile Type: MP3

MIME Type: audio/mpeg MPEG Audio Version: 1 Audio Layer: 3

Audio Bitrate: 256 kbps Sample Rate: 44100 Channel Mode: Joint Stereo

MS Stereo: On Intensity Stereo: Off Copyright Flag: False Original Media: True Emphasis: None

ID3 Size: 161

Encoder Settings: Title:

Artist: Album: Year: Comment: Genre: None

Duration: 17.58 s (approx)

Información de otras etiquetas en archivos de música del tipo ID3: ID3v2.3.0:

+ [ID3v2_3 directory, 40662 bytes]
| ID3_GEOB =
| Comment =
| Private (SubDirectory) -->
| Private (SubDirectory) -->
| | WM_MediaClassSecondaryID =
| Private (SubDirectory) -->
| Private (SubDirectory) -->
| | WM_MediaClassPrimaryID =
| Conductor =
| Picture = image/jpeg.thumbnail, (en los casos en que contenga una imagen embebida)
| PictureMimeType = image/jpeg
| PictureType =
| PictureDescription = thumbnail
| Track 2
| Album =
| Year =
| Genre =
| Band =
| Title =
| Composer =
| Artist =
| Comment =

ID3v1:

+ [BinaryData directory, 128 bytes]
| Title =
| Artist =
| Album =
| Year =
| Comment =
| Track =
| Genre =

f. Ejecutar en Windows la interfaz gráfica de la herramienta ExifToolGui y analizar los resultados de las diferentes etiquetas:

· MPEG-4 Audio, es un método de compresión audiovisual digital, que se corresponde con el estándar ISO/IEC 14496, Codificación de objetos audiovisuales. MPEG-4 se utiliza en la compresión de datos de audiovisuales para su distribución a través de: la web, (streaming, distribución de archivos de multimedia –audio y video– por medio de una red de computadoras, es un flujo constante de datos sin interrupción), de discos compactos –CD–, de voz (teléfono, videoconferencia) y de aplicaciones para la televisión.

MPEG-4 contiene las características de MPEG-1 y MPEG-2, además incorpora las características relacionadas con:

- 3D y VRML (Virtual Reality Modeling Language, Lenguaje de modelación de realidad virtual).
- El soporte para la Gestión de Derechos Digitales (DRM, Digital Rights Management) y para varios tipos de interactividad de codificación de audio avanzada (AAC, Advanced Audio Coding).

Los archivos AAC MPEG-4 reproducen archivos del tipo M4A, creado por Apple para su aplicación iTunes, para diferenciarlo de MPEG-4 de audio –M4A– y video –M4V–.

La extensión M4B responde al tipo de archivo de audio similar al M4A, pero identificado particularmente para los archivos de audio de los libros electrónicos.

La extensión M4P es un archivo de audio o música que se descarga con iTunes del sitio de Apple.

Los archivos AAC y M4A pueden tener etiquetas ID3 como en los archivos MP3, también contienen etiquetas específicas de MPEG-4.

Los archivos M4P y M4R son utilizados por la aplicación iTunes de Apple, son archivos AAC protegidos por Apple Fairplay DRM (Gestión de Derechos Digitales, Digital Rights Management), lo cual restringe la reproducción en dispositivos no autorizados. Los archivos M4R son archivos del tipo AAC utilizados como ringtones o tonos de timbres de los dispositivos iPhone.

La herramienta AtomicParsley permite extraer las etiquetas específicas de los archivos de extensión MPEG-4, se ejecuta desde la línea de comandos, permite extraer, analizar y configurar metadatos de este tipo de extensión. La aplicación es de código abierto y está disponible para los sistemas operativos Linux, Mac OS X y Windows; se puede descargar del sitio: http://atomicparsley.sourceforge.net/.

a. En Linux o Mac OS X ejecutar el comando:

$atomicParsley audio2.m4a –tE

La opción t, muestra las etiquetas embebidas en el archivo; la opción E, permite extraer imágenes embebidas en el archivo de audio.

b. En Windows ejecutar el comando:

C:\AtomicParsley-win32-0.9.0>AtomicParsley.exe audio2.m4a -tE Major Brand: M4A version 512

Compatible Brands: isom iso2

Tagging schemes available: iTunes-style metadata allowed.

ISO-copyright notices @ movie and/or track level allowed. uuid private user extension tags allowed.

----------Track level ISO user data: Track 1:

No user data for this track.

----------3GPP assets/ISO user data:

----------iTunes-style metadata tags: Atom “©too” contains:

----------free atom space: 8

padding available: 0 (reorg) user data space: 96

media data space: 206477

----------. WMA, Windows Media Audio. ASF (Advanced System Format Formato de Sistema Avanzado), es un diseño de contenedor digital propietario de Microsoft para la distribución de multimedia (streaming). Este formato es utilizado para almacenar archivos de audio de Microsoft (WMA, Windows Media Audio) y, además, datos de video (WMV, Windows Media Video), ambos propietarios de Microsoft. Los programas de código abierto como ffmpeg o Video Lan Client, basados en la librería libavcodec de licencia GPL permiten reproducir o convertir los códecs WMA y WMV. Los contenedores digitales ASF poseen metadatos que pueden extraerse con las herramientas exiftool y hachoir-metadata.

a. En la línea de comando ejecutar la herramienta:

$hachoir-metadata audio2.wma

El resultado del comando devuelve información sobre el nombre de la aplicación que creó el archivo, nombre del autor, fecha y hora, y datos relacionados con el archivo de audio.

b. En la línea de comando ejecutar la herramienta exiftool.exe, asignarle el archivo de audio a analizar y direccionar la salida a un archivo de texto, en el cual se registrará la información extraída del archivo de extensión .WMA.

En Windows:

C:\exiftool>exiftool.exe –v audio2.wma > metadatosaudio2.txt En Linux:

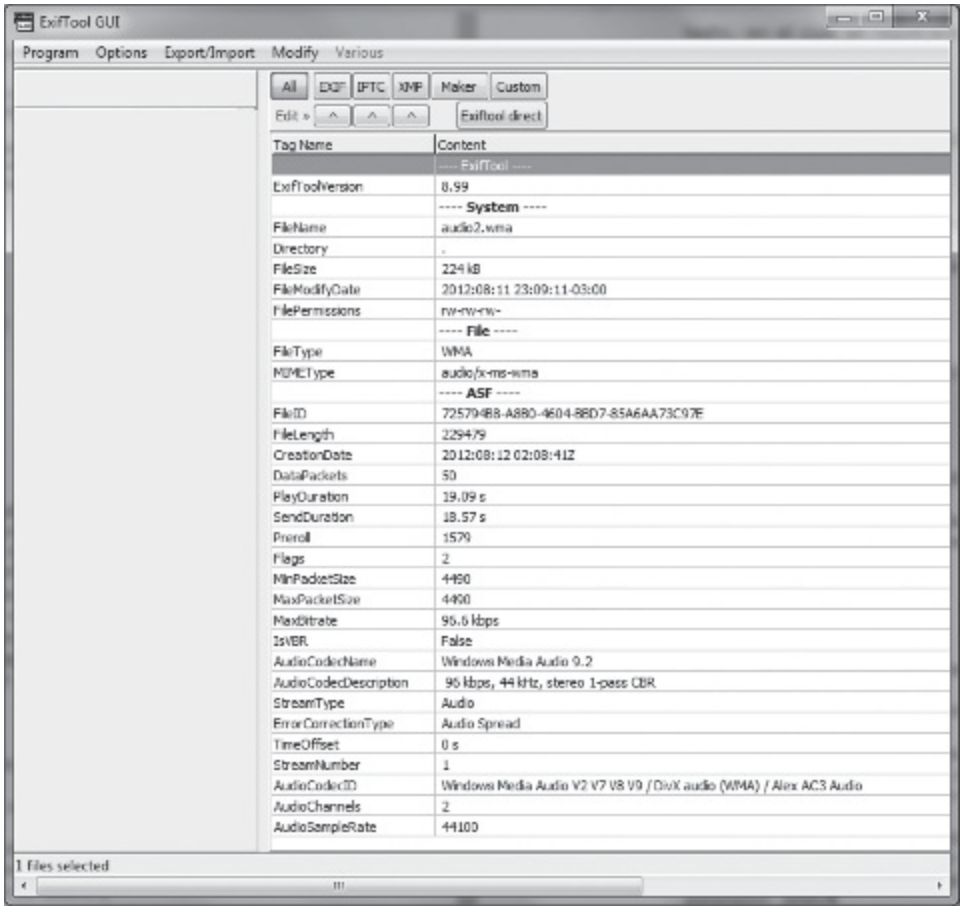
$exiftool –v audio2.wmv > metadatos-audio2.txt

La información contenida en el archivo de texto metadatos-audio2.txt es la

siguiente: ExifToolVersion = 8.99
FileName = audio2.wma
Directory = . FileSize = 229479
FileModifyDate = 1344737351
FilePermissions = 33206 FileType = WMA
MIMEType = audio/x-ms-wma Header (SubDirectory) -->
+ [Header directory]
| FileProperties (SubDirectory) -->
| + [BinaryData directory, 80 bytes]
| | FileID = ..Wr...F.....s.~
| | FileLength = 229479
| | CreationDate = 1.2989210921229e+017
| | DataPackets = 50
| | PlayDuration = 190860000
| | SendDuration = 185740000
| | Preroll = 1579
| | Flags = 2
| | MinPacketSize = 4490
| | MaxPacketSize = 4490
| | MaxBitrate = 96647
| HeaderExtension (SubDirectory) -->
| + [HeaderExtension directory]
| | LanguageList
| | 26F18B5D-4584-47EC-9F5F-0E651F0452C9
| | Metadata (SubDirectory) -->
| | + [Metadata directory with 2 entries, 98 bytes]
| | | ASF_Metadata_IsVBR = False
| | | ASF_Metadata_DeviceConformanceTemplate = L1
| | 1806D474-CADF-4509-A4BA-9AABCB96AAE8
| | ExtendedStreamProps
| | D9AADE20-7C17-4F9C-BC28-8555DD98E2A2
| ExtendedContentDescr (SubDirectory) -->
| + [ExtendedContentDescr directory with 3 entries, 144 bytes]
| | ASF_ExtendedDescr_WMFSDKVersion = 12.0.7601.17514
| | ASF_ExtendedDescr_WMFSDKNeeded = 0.0.0.0000
| | IsVBR = False

| CodecList (SubDirectory) -->
| + [CodecList directory with 1 entries, 150 bytes]
| | AudioCodecName = Windows Media Audio 9.2
| | AudioCodecDescription = 96 kbps, 44 kHz, stereo 1-pass CBR
| StreamProperties (SubDirectory) -->
| + [BinaryData directory, 90 bytes]
| | StreamType = @.i.M[....._\D+
| | ErrorCorrectionType = P....a.....
| | TimeOffset = 0
| | StreamNumber = 1
| | AudioCodecID = 353
| | AudioChannels = 2
| | AudioSampleRate = 44100
| StreamBitrateProps Data

c. Ejecutar en Windows la interfaz gráfica de la herramienta ExifToolGui y analizar los resultados del metadato extraído del archivo WMA:



Los archivos de video contienen datos que se decodifican en una serie de

imágenes en movimiento, además tienen incorporado en su mayoría componentes de audio que se sincronizan con el video. Los archivos se crean generalmente como un archivo del tipo contenedor que almacena uno o más flujos de datos (stream). El método que se utiliza para codificar los datos en el flujo de datos o stream es el códec. El archivo de video o película requiere del códec apropiado para su reproducción. Los metadatos de los archivos de video contienen entre otra información, datos sobre la fecha de creación y el nombre del programa que lo generó. Existen formatos de códec específicos, tales como:

- MPEG-1, utilizado en videos almacenados en CD o VCD (Video CD) y MPEG-2 en DVD, transmisiones satelitales y cable digital. Ambos formatos poseen escasa información de valor en sus metadatos.
- MPEG-4, la extensión del archivo es generalmente .MP4. La reproducción de archivos de video de MP4 están codificados con el códec de video avanzado MPEG-4 AAC. El flujo de datos de audio también se encuentra codificado en AAC, tal como en los archivos de audio de MP4. Los metadatos del archivo de video se pueden extraer con la misma herramienta (AtomicParsley) que se utiliza para los archivos de audio MP4, ya que ambos poseen el mismo contenedor.

a. En Linux o Mac OS X ejecutar el comando:

$atomicParsley video1.mp4 –tE

La opción t, muestra las etiquetas embebidas en el archivo; la opción E, permite extraer imágenes embebidas en el archivo de audio.

b. En Windows ejecutar el comando:

C:\AtomicParsley-win32-0.9.0>AtomicParsley.exe video.mp4 -tE Major Brand: mp42 version 0

Compatible Brands: mp42 3gp4 isom

Tagging schemes available: iTunes-style metadata allowed.

ISO-copyright notices @ movie and/or track level allowed. uuid private user extension tags allowed.

----------Track level ISO user data: Track 1:

No user data for this track. Track 2:

No user data for this track.

----------3GPP assets/ISO user data:

----------iTunes-style metadata tags:

----------free atom space: 0

padding available: 0 (reorg)

media data space: 4842616

----

c. En la línea de comando ejecutar la herramienta exiftool.exe, asignarle el archivo de video a analizar y direccionar la salida a un archivo de texto, en el cual se registrará la información extraída del archivo de extensión .MP4.

En Windows:

C:\exiftool>exiftool.exe video.mp4 > metadatos-video-mp4.txt

En Linux:

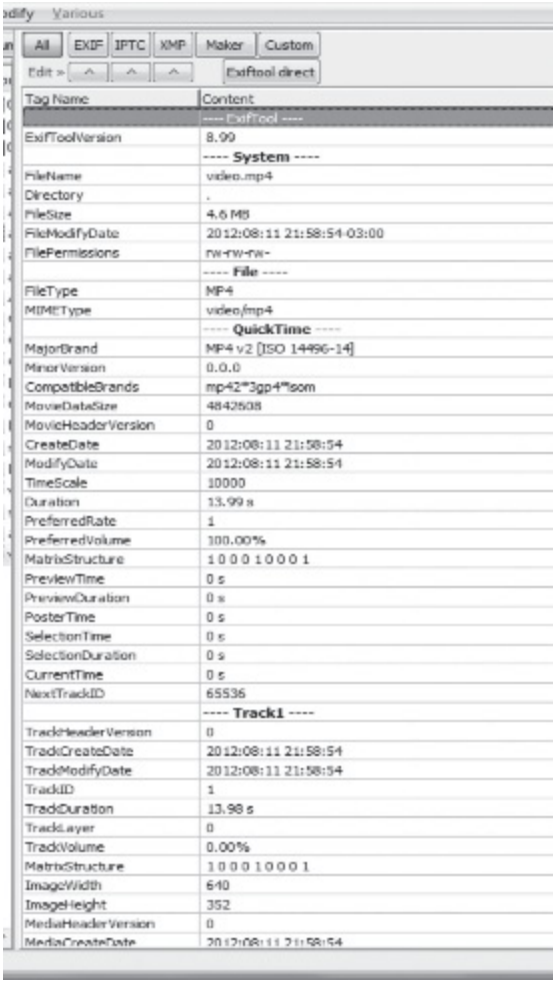
$exiftool –v video.mp4 > metadatos-video-mp4.txt

La información contenida en el archivo de texto metadatos-video-mp4.txt es la siguiente:

ExifTool Version Number: 8.99
File Name: video.mp4 Directory: .
File Size: 4.6 MB
File Modification Date/Time: 2012:08:11 21:58:54-03:00
File Permissions: rw-rw-rw
File Type: MP4
MIME Type: video/mp4
Major Brand: MP4 v2 [ISO 14496-14]
Minor Version: 0.0.0
Compatible Brands: mp42, 3gp4, isom
Movie Data Size: 4842608
Movie Header Version: 0
Create Date: 2012:08:11 21:58:54
Modify Date: 2012:08:11 21:58:54
Time Scale: 10000
Duration: 13.99 s
Preferred Rate: 1
Preferred Volume: 100.00% Preview Time: 0 s
Preview Duration: 0 s
Poster Time: 0 s
Selection Time: 0 s
Selection Duration: 0 s
Current Time: 0 s
Next Track ID: 65536
Track Header Version: 0
Track Create Date: 2012:08:11 21:58:54
Track Modify Date: 2012:08:11 21:58:54

Track ID: 1
Track Duration: 13.98 s
Track Layer: 0
Track Volume: 0.00%
Image Width: 640
Image Height: 352
Graphics Mode: src
Copy Op Color: 0 0 0
Compressor ID: mp4v
Source Image Width: 640
Source Image Height: 352
X Resolution: 72
Y Resolution: 72
Bit Depth: 24
Video Frame Rate: 29.46
Matrix Structure: 1 0 0 0 1 0 0 0 1
Media Header Version: 0
Media Create Date: 2012:08:11 21:58:54
Media Modify Date: 2012:08:11 21:58:54
Media Time Scale: 48000
Media Duration: 13.99 s
Media Language Code: und
Handler Type: Audio
Track Balance: 0
Audio Format: mp4a
Audio Channels: 2
Audio Bits Per Sample: 16
Audio Sample Rate: 48000
Avg Bitrate: 2.77 Mbps
Image Size: 640x352
Rotation: 0

e. Ejecutar en Windows la interfaz gráfica de la herramienta ExifToolGui y analizar los resultados del metadato extraído:



• WMV, Windows Media Video, se almacena en el contenedor ASF (Advanced System Format Formato de Sistema Avanzado) y va acompañado generalmente por un flujo de datos de audio del tipo WMA.

a. En la línea de comando ejecutar la herramienta:

$hachoir-metadata video1.wmv

El resultado del comando devuelve información sobre el nombre de la aplicación que creó el archivo, nombre del autor, fecha y hora, y datos relacionados con el archivo de video.

b. En la línea de comando ejecutar la herramienta exiftool.exe, asignarle el archivo de video a analizar y direccionar la salida a un archivo de texto, en el cual se registrará la información extraída del archivo de extensión .WMV.

En Windows:

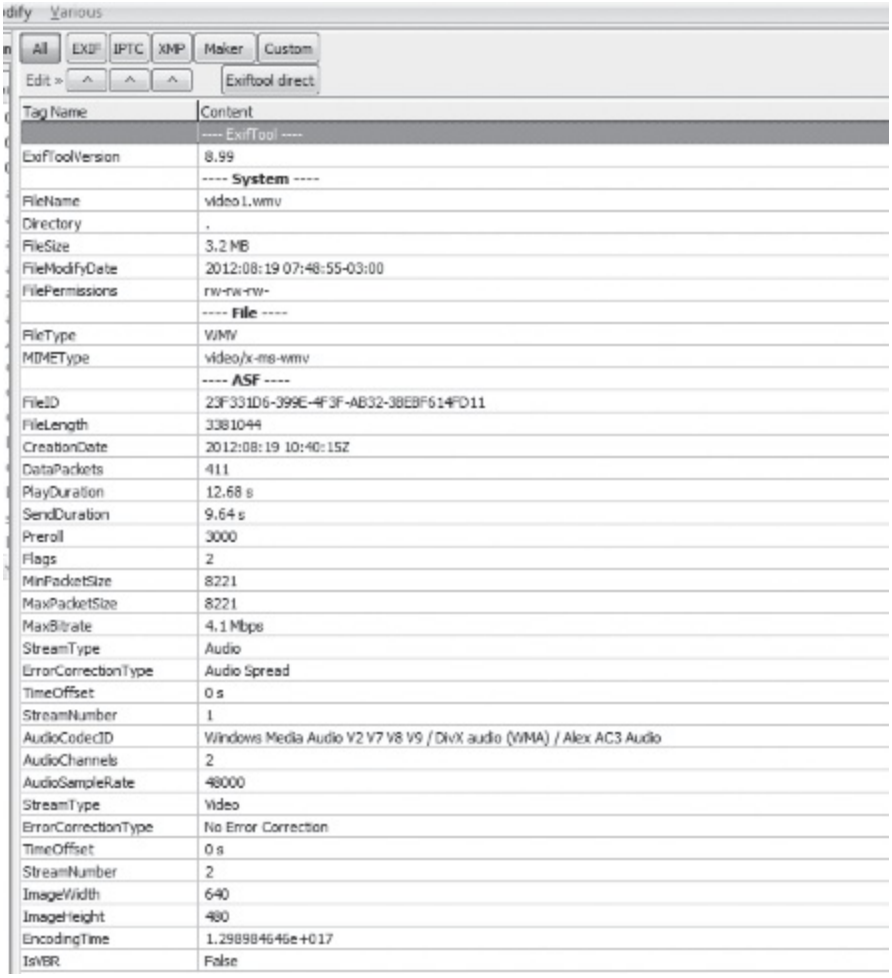
C:\exiftool>exiftool.exe video1.wmv > metadatos-video1.txt En Linux:

$exiftool video1.wmv > metadatos-video1.txt

La información contenida en el archivo de texto metadatos-video1.txt es la siguiente: ExifTool Version Number: 8.99

File Name: video1.wmv
Directory: .
File Size: 3.2 MB
File Modification Date/Time: 2012:08:19 07:48:55-03:00
File Permissions: rw-rw-rw
File Type: WMV
MIME Type: video/x-ms-wmv
File ID: 23F331D6-399E-4F3F-AB32-3BEBF614FD11
File Length: 3381044
Creation Date: 2012:08:19 10:40:15Z
Data Packets: 411
Play Duration: 12.68 s
Send Duration: 9.64 s Preroll: 3000
Flags: 2
Min Packet Size: 8221
Max Packet Size: 8221
Max Bitrate: 4.1 Mbps
Audio Codec ID: Windows Media Audio V2 V7 V8 V9 / DivX audio (WMA) / Alex AC3 Audio
Audio Channels: 2
Audio Sample Rate: 48000
Stream Type: Video
Error Correction Type: No
Error Correction Time Offset: 0 s
Stream Number: 2
Image Width: 640
Image Height: 480
Encoding Time: 1.298984646e+017
Is VBR: False
Image Size: 640x480

c. Ejecutar en Windows la interfaz gráfica de la herramienta ExifToolGui y analizar los resultados del metadato extraído:



· AVI, Audio Video Interleave, es un formato de contenedor de audio y video diseñado por Microsoft en 1992. El formato AVI proviene del contenedor de formato de archivo de intercambio RIFF (Resource Interchange File Format) que almacena el contenido del archivo como una serie de fragmentos; cada fragmento puede incluir uno de información (INFO) para guardar los metadatos, los cuales pueden ser del tipo XMP. El archivo AVI contiene flujos de datos de audio y video comprimido por numerosos códecs, los cuales se identifican utilizando una secuencia fija de cuatro bytes denominado FourCC codes. Este código le informa al programa reproductor del video AVI cuáles son los códecs necesarios para decodificar en forma adecuada el contenido del archivo. Los archivos AVI se pueden analizar de la misma forma que los de audio del tipo WAV. En el sitio del Departamento de Ciencias de la Computación de la Universidad de Florida en EE.UU. de Norteamérica, se encuentran publicados archivos de video del tipo AVI (http://people.sc.fsu.edu/~jburkardt/data/avi/avi.html). En la extracción de datos se utilizará el archivo rbc.avi (una animación del movimiento y deformación de un glóbulo rojo).

a. En la línea de comando ejecutar la herramienta:

$hachoir-metadata rbc.avi

El resultado del comando devuelve información sobre el nombre de la aplicación que creó el archivo, nombre del autor, fecha y hora, y datos relacionados con el archivo de video y audio.

b. En la línea de comando ejecutar la herramienta exiftool.exe, asignarle el archivo de video a analizar y direccionar la salida a un archivo de texto, en el cual se registrará la información extraída del archivo de extensión .AVI.

En Windows:

C:\exiftool>exiftool.exe rbc.avi > metadatosrbc-avi.txt

En Linux:

$exiftool exiftool.exe rbc.avi > metadatosrbc-avi.txt

La información contenida en el archivo de texto metadatos-rbc-avi.txt es la siguiente: ExifTool Version Number: 8.99

File Name: rbc.avi

Directory: .

File Size: 5.9 MB

File Modification Date/Time: 2012:08:19 13:19:23-03:00

File Permissions: r--r--r-File Type: AVI

MIME Type: video/x-msvideo

Frame Rate: 10

Max Data Rate: 817.9 kB/s

Frame Count: 80

Stream Count: 1

Stream Type: Video

Video Codec: 00dc

Video Frame Rate: 10

Video Frame Count: 80

Quality: 0

Sample Size: Variable

Image Width: 791

Image Height: 704

Planes: 1

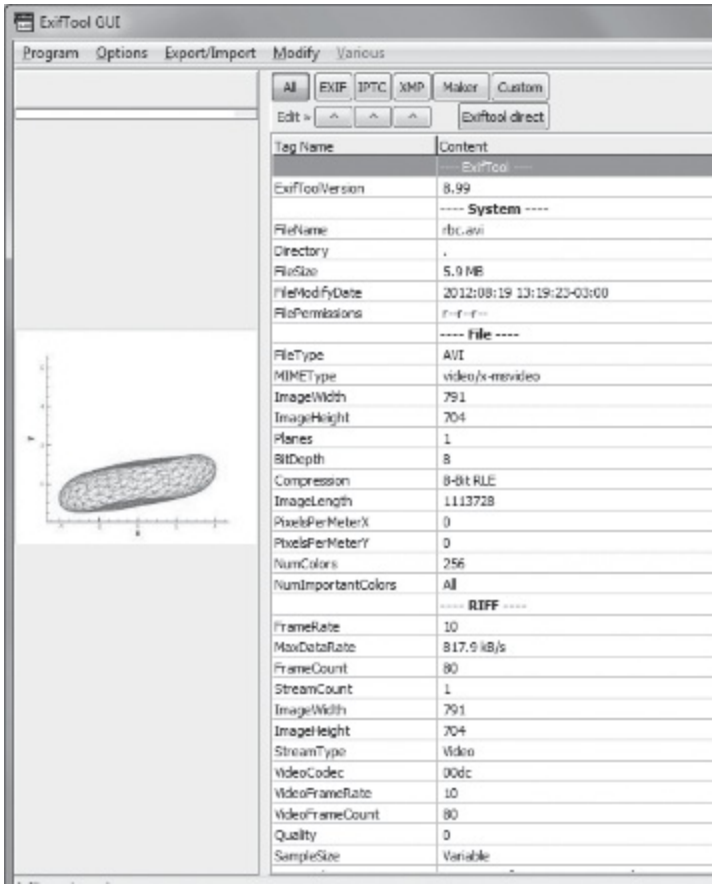
Bit Depth: 8

Compression: 8-Bit RLE

Image Length: 1113728

Pixels Per Meter X: 0
Pixels Per Meter Y: 0
Num Colors: 256
Num Important Colors: All
Duration: 8.00 s
Image Size: 791x704

c. Ejecutar en Windows la interfaz gráfica de la herramienta ExifToolGui y analizar los resultados del metadato extraído:



· MOV, es el formato de la aplicación QuickTime de Apple. Los metadatos de estos archivos de video se pueden extraer con la herramienta qtinfo, que forma parte del paquete de utilidades (quicktime-utils) de la distribución de Linux Ubuntu. En la extracción de datos se utilizará el archivo rbc.mov (una animación del movimiento y deformación de un glóbulo rojo, http://people.sc.fsu.edu/~jburkardt/data/mov/mov.html).

a. En la línea de comando ejecutar la herramienta exiftool.exe, asignarle el archivo de video a analizar y direccionar la salida a un archivo de texto, en el cual se registrará la información extraída del archivo de extensión .MOV.

En Windows:

C:\exiftool>exiftool.exe rbc.mov > metadatosrbc-mov.txt

En Linux:

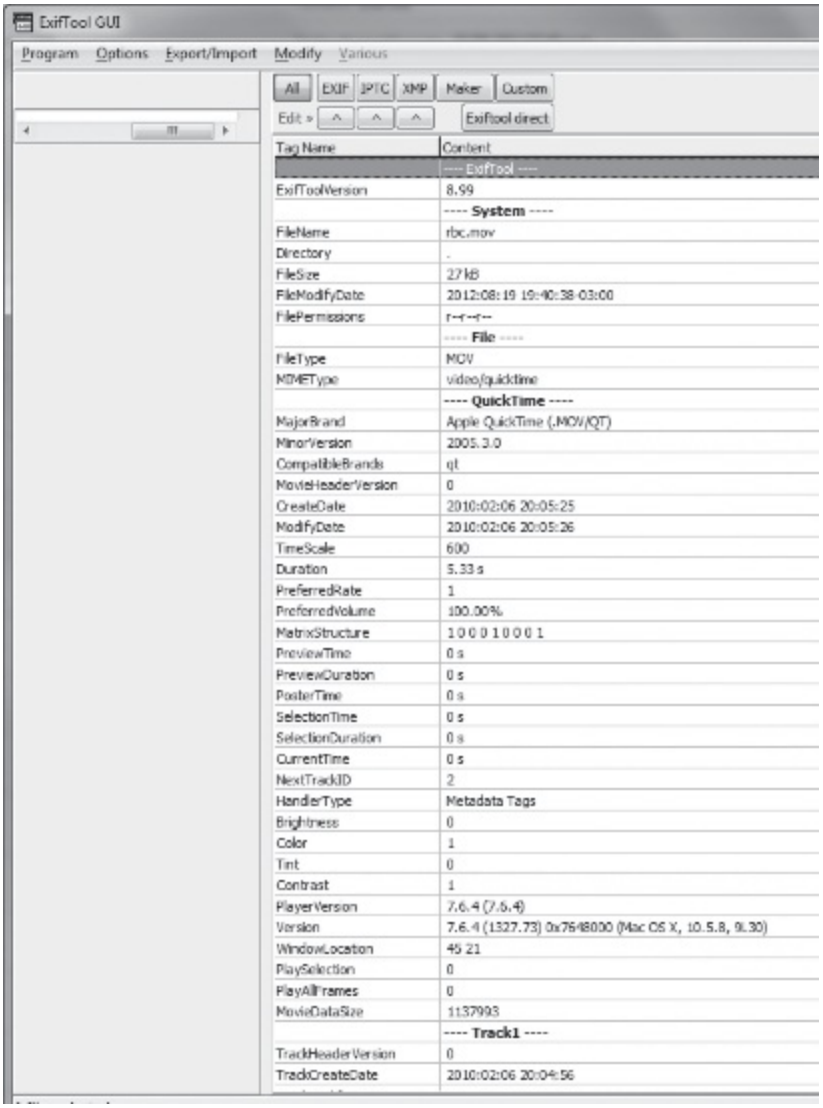
$exiftool exiftool.exe rbc.mov > metadatosrbc-mov.txt

La información contenida en el archivo de texto metadatos-rbc-avi.txt es la siguiente:

ExifTool Version Number: 8.99
File Name: rbc.mov
Directory: .
File Size: 27 kB
File Modification
Date/Time: 2012:08:19 19:40:38-03:00
File Permissions: r--r--r-File
Type: MOV
MIME Type: video/quicktime
Major Brand: Apple QuickTime (.MOV/QT)
Minor Version: 2005.3.0
Compatible Brands: qt
Movie Header Version: 0
Create Date: 2010:02:06 20:05:25
Modify Date: 2010:02:06 20:05:26
Time Scale: 600
Duration: 5.33 s
Preferred Rate: 1
Preferred Volume: 100.00%
Preview Time: 0 s
Preview Duration: 0 s
Poster Time: 0 s
Selection Time: 0 s
Selection Duration: 0 s
Current Time: 0 s
Next Track ID: 2
Track Header Version: 0
Track Create Date: 2010:02:06 20:04:56
Track Modify Date: 2010:02:06 20:05:26
Track ID: 1
Track Duration: 5.33 s Track Layer: 0

Track Volume: 0.00%
Matrix Structure: 1 0 0 0 1 0 0 0 1
Image Width: 580
Image Height: 520
Media Header Version: 0
Media Create Date: 2010:02:06 20:05:25
Media Modify Date: 2010:02:06 20:05:26
Media Time Scale: 600
Media Duration: 5.33 s
Graphics Mode: dither
Copy Op Color: 32768 32768 32768
Handler Class: Data Handler
Handler Vendor ID: Apple
Handler Description: Apple
Alias Data Handler Compressor ID: jpeg
Vendor ID: Apple
Source Image Width: 580
Source Image Height: 520
X Resolution: 72
Y Resolution: 72
Compressor Name: Photo
JPEG Bit Depth: 24
Video Frame Rate: 15
Handler Type: Metadata
Tags Brightness: 0
Color: 1
Tint: 0
Contrast: 1
Player Version: 7.6.4 (7.6.4)
Version: 7.6.4 (1327.73) 0x7648000 (Mac OS X, 10.5.8, 9 L30)
Window Location: 45 21
Play Selection: 0 Play All Frames: 0
Movie Data Size: 1137993
Avg Bitrate: 1.71 Mbps
Image Size: 580x520
Rotation: 0

b. Ejecutar en Windows la interfaz gráfica de la herramienta ExifToolGui y analizar los resultados del metadato extraído:



· MKV, Matroska Multimedia Container (http://www.matroska.org/), es un formato de estándar abierto que puede ser utilizado para audio, video, imágenes y subtítulos de pistas, y en la modalidad de compartir archivos, en particular el sistema de archivos compartidos de videos de animación japonesa (Anime), por la característica de transportar subtítulos. El paquete de herramientas mkvtoolnix (http://www.bunkus.org/videotools/ mkvtoolnix/downloads.html), en la línea de comando permite manejar, extraer e identificar los flujos de datos en el contenedor de MKV y de metadatos. El paquete se encuentra disponible para los sistemas operativos Mac OS X, Unix, Linux y Windows (http://www.bunkus.org/videotools/mkvtoolnix/downloads.html). Otra herramienta de análisis de estos archivos es hachoir-metadata.

En la extracción de datos se utilizarán archivos de prueba publicados en el sitio de Sourceforge, http://sourceforge.net/projects/matroska/files/.

a. En la estación de trabajo de Informática forense instalar según el sistema operativo la herramienta mkvtoolnix.

b. En la línea de comando ejecutar la herramienta mkvinfo.exe, asignarle el archivo de video a analizar y direccionar la salida a un archivo de texto, en el cual se registrará la información extraída del archivo de extensión .MKV.

En Windows:

C:\ mkvtoolnix-0.4.2>mkvinfo.exe -v test7.mkv > metadatos-test7-mkv.txt
En Linux:

$mkvinfo –v test7.mkv > metadatos-test7-mkv.txt

La información contenida en el archivo de texto metadatos-rbc-avi.txt es la siguiente: (MKVInfo) + EBML head

(MKVInfo) + Segment

(MKVInfo) |+ Seek head

(MKVInfo) | + Unknown element: N7libebml9EbmlCrc32E (MKVInfo) | + Seek entry

(MKVInfo) | + Unknown element: N7libebml9EbmlCrc32E (MKVInfo) |+ Segment information

(MKVInfo) | + Unknown element: N7libebml9EbmlCrc32E (MKVInfo) |+ Segment tracks

(MKVInfo) | + Unknown element: N7libebml9EbmlCrc32E (MKVInfo) |+ Tags (skipping all subelements!)

(MKVInfo) |+ EbmlVoid (MKVInfo) |+ EbmlVoid (MKVInfo) |+ EbmlVoid (MKVInfo) |+ EbmlVoid (MKVInfo) |+ EbmlVoid (MKVInfo) |+ EbmlVoid (MKVInfo) |+ EbmlVoid (MKVInfo) |+ EbmlVoid (MKVInfo) |+ EbmlVoid (MKVInfo) |+ EbmlVoid (MKVInfo) |+ EbmlVoid (MKVInfo) |+ EbmlVoid (MKVInfo) |+ EbmlVoid (MKVInfo) |+ EbmlVoid (MKVInfo) |+ EbmlVoid (MKVInfo) |+ EbmlVoid

En Windows:

C:\ mkvtoolnix-0.4.2>mkvinfo.exe -g test7.mkv

En Linux:

$mkvinfo –g test7.mkv

c. En la línea de comando ejecutar la herramienta exiftool.exe, asignarle el archivo de video a analizar y direccionar la salida a un archivo de texto, en el cual se registrará la información extraída del archivo de extensión .MKV.

En Windows:

C:\exiftool>exiftool.exe test7.mkv > metadatos-test7-mkv.txt

En Linux:

$exiftool exiftool.exe test7.mkv > metadatos-test7-mkv.txt

La información contenida en el archivo de texto metadatos-rbc-avi.txt es la siguiente:

ExifTool Version Number: 8.99

File Name: test7.mkv

Directory: .

File Size: 21 MB

File Modification Date/Time: 2010:08:21 19:04:18-03:00

File Permissions: r--r--r-File Type: MKV

MIME Type: video/x-matroska

Doc Type: matroska

Doc Type Version: 2

Doc Type Read Version: 2

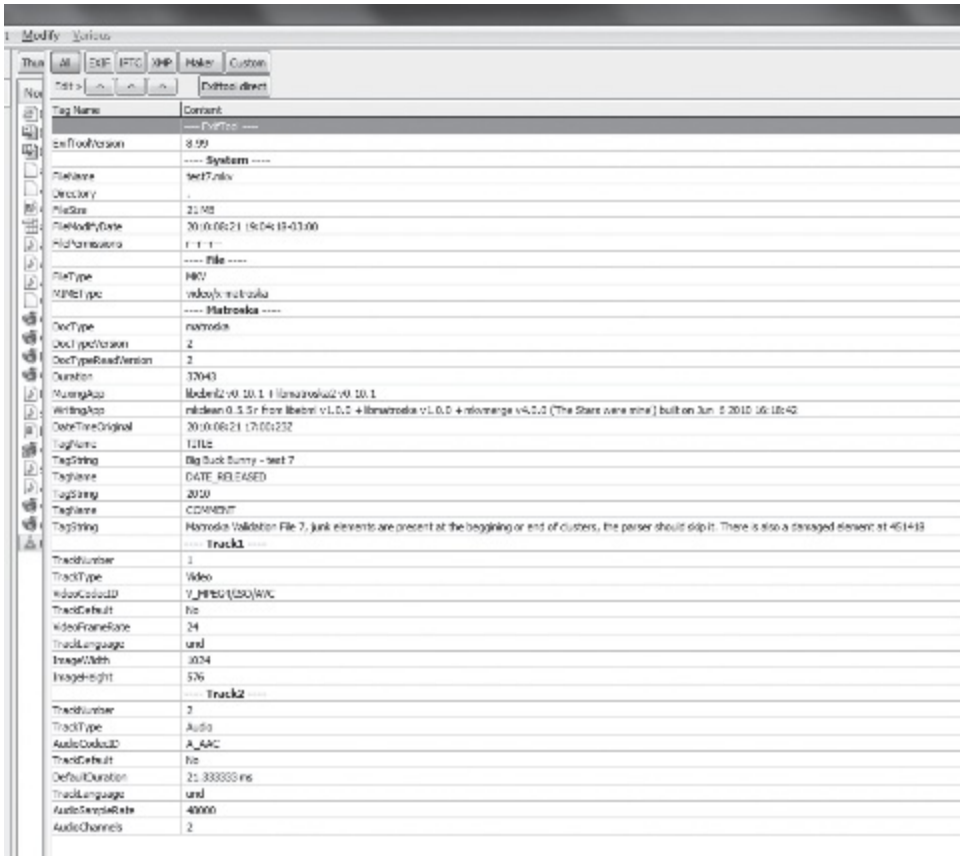
Duration: 37043

Muxing App: libebml2 v0.10.1 + libmatroska2 v0.10.1 Writing App: mkclean 0.5.5 r from libebml v1.0.0 + libmatro

ska v1.0.0 + mkvmerge v4.0.0 (‘The Stars were mine’) built on Jun 6 2010 16:18: 42

Date/Time Original: 2010:08:21 17:00:23Z
Video Codec ID: V_MPEG4/ISO/AVC
Video Frame Rate: 24
Image Width: 1024
Image Height: 576
Track Number: 2
Track Type: Audio
Audio Codec ID: A_AAC
Track Default: No
Default Duration: 21.333333 ms
Track Language: und
Audio Sample Rate: 48000 Audio Channels: 2
Tag Name: COMMENT
Tag String: Matroska Validation File 7, junk elements are present at the beggining or end of clusters, the parser should skip it. There is also a damaged element at 451418 Image Size: 1024x576

d. Ejecutar en Windows la interfaz gráfica de la herramienta ExifToolGui y analizar los resultados del metadato extraído:



· OGG, es un formato de contenedor abierto de libre disponibilidad, creado y mantenido por la fundación Xiph.org, que produce herramientas y multimedia de código abierto. OGG está diseñado para proveer un flujo de datos eficiente y un manejo de multimedia digital de alta calidad. En el sitio http://www.bunkus.org/videotools/ogmtools/index. html, se encuentran herramientas de manejo de archivos OGG de audio y video. En la extracción de metadatos se utilizará un ejemplo publicado en http://commons.wikimedia.org/wiki/File:Xacti-AC8EX-Sample_video-001.ogg.

a. En la línea de comando ejecutar la herramienta exiftool.exe, asignarle el archivo de video a analizar y direccionar la salida a un archivo de texto, en el cual se registrará la información extraída del archivo de extensión .OGG.

En Windows:

C:\exiftool>exiftool.exe Xacti-AC8EX-Sample_video-001.ogg > metadatos-videoogg.txt

En Linux:

$exiftool exiftool.exe Xacti-AC8EX-Sample_video-001.ogg > metadatos-video-ogg.txt La información contenida en el archivo de texto metadatos-rbc-avi.txt es la siguiente: ExifTool Version Number: 8.99

File Name: Xacti-AC8EX-Sample_video-001.ogg

Directory: .

File Size: 4.5 MB

File Modification Date/Time: 2012:08:20 01:47:53-03:00 File Permissions: rw-rw-rwFile Type: OGV

MIME Type: video/x-ogg Theora Version: 3.2.1

Image Width: 720

Image Height: 576

X Offset: 0

Y Offset: 0

Frame Rate: 25

Pixel Aspect Ratio: 1.067 Color Space: Rec. 470BG

Nominal Video Bitrate: Unspecified Quality: 63

Pixel Format: 4:2:0

Vorbis Version: 0

Audio Channels: 2

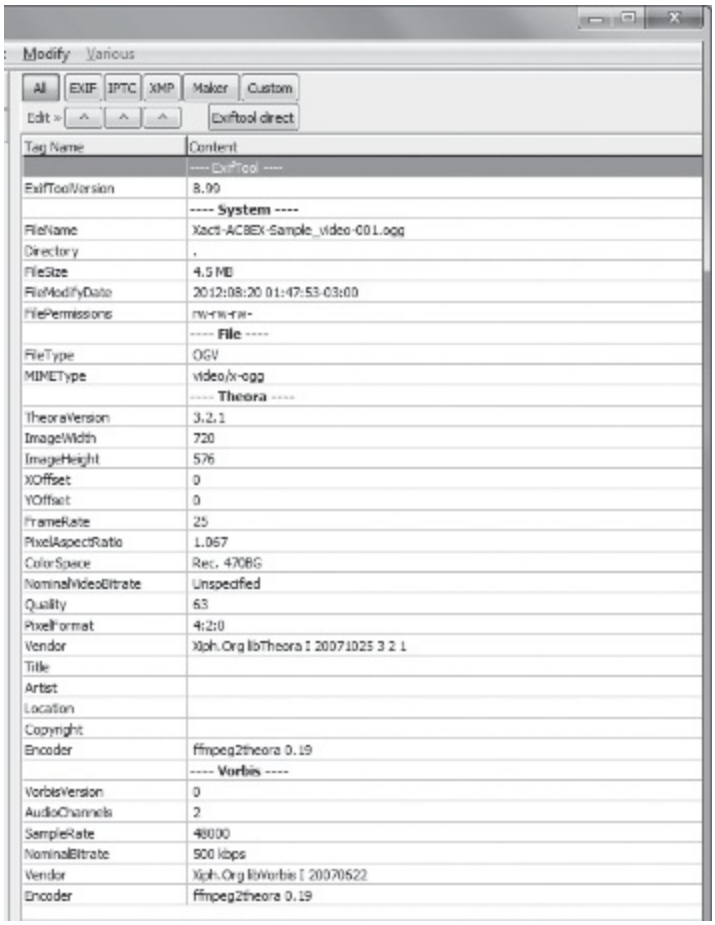
Sample Rate: 48000 Nominal Bitrate: 500 kbps Title:

Artist: Location: Copyright:

Vendor: Xiph.Org libVorbis I 20070622 Encoder: ffmpeg2theora 0.19

Duration: 0:01:15 (approx) Image Size: 720x576

b. Ejecutar en Windows la interfaz gráfica de la herramienta ExifToolGui y analizar los resultados del metadato extraído:



Procedimiento para el análisis del contenido del video forense

El análisis del video forense conforma otras de las especialidades de la Criminalística para la identificación, comparación y evaluación del video.

Las técnicas más comunes para el análisis del video forense son las siguientes:

1. Realizar la digitalización de la cinta del video sin procesar, tal como ha sido filmado, de manera confiable y en modo seguro en una computadora, utilizando programas de edición no lineales o no destructivos, por ejemplo: Lightworks, http://www.lwks.com/, de licencia Freeware, es decir disponible sin costo y de uso ilimitado. En el caso de videos digitales grabados en dispositivos removibles como CD, DVD y Memorias Flash, efectuar la copia de estos en otro dispositivo de almacenamiento.

2. Proteger el video original para evitar daños producidos por factores externos que pueden dañar el dispositivo contenedor o la señal de grabación contenida en el video, tales como roturas de la protección externa, campos magnéticos, descargas eléctricas, entre otros.

3. Efectuar las certificaciones matemáticas (hash) de los archivos digitalizados en el paso 1.

4. Generar dos o más copias del video digitalizado como resguardo ante posibles extravíos o daños.

5. Efectuar la separación de audio y video (demultiplexar) del video original multiplexado del Circuito Cerrado de Televisión.

6. Convertir el video digital del dispositivo de grabación de video en formatos de video digital factibles de utilizar para el análisis forense del mismo.

7. Aplicar técnicas de mejoramiento, aclaración o clarificación tal como la de promedios de cuadros para reducir los errores en ellos (frame averaging).

8. Señalar o marcar datos de interés en el video.

9. Aumentar las áreas del video que resultan de interés.

10. Efectuar mediciones de objetos, personas y de distancias entre puntos observados en el video.

11. Registrar los datos, capturar pantalla y/o imprimir:

a. En el caso de requerir la impresión de las imágenes de interés del video, se debe considerar la relación de aspecto y tamaño; si el sistema de análisis del video sigue los lineamientos establecidos en el estándar de codificación de televisión digital, ITU-601 (http://www.itu.int/dms_pubrec/itu-r/rec/bt/R-REC-BT.601-7-201103-I!!PDF-E.pdf), se deben corregir las imágenes para la transferencia adecuada de los píxeles en la salida impresa.

12. Efectuar la certificación matemática (hash) de los archivos digitalizados de video y comparar los resultados con los obtenidos en el paso 2., con el fin de verificar que no se hayan producido modificaciones en los archivos de video digitalizados al utilizar diversas herramientas para su análisis.

13. Efectuar el resguardo de los datos y de las herramientas utilizadas con sus respectivas certificaciones matemáticas (hash).

Guía para el procedimiento de video de la Agencia Federal de Investigaciones (FBI)

A continuación, se enuncian los lineamientos para el procesamiento de video establecido por la Agencia Federal de Investigaciones de EE.UU. de Norteamérica (Servicios de Laboratorio, Publicaciones de ciencias forenses http://www.fbi.gov/about-us/lab/forensic-sciencecommunications/fsc/oct2003/2003_10_guide02.htm#guidelines). El contenido del documento es el siguiente:

Criterios y Directrices

Definiciones, Recomendaciones y Directrices para el Uso de Procesamiento de Video Forense en el Sistema de Justicia Penal Grupo Científico de Trabajo sobre Tecnologías de la Imagen (SWGIT) Octubre 2003 Volumen 5 Número 4

Versión 1.2 06 2003

Misión | Introducción | Definiciones | Equipos Directrices para Video Processing Procedimientos Operativos Estándar

Pasos para el procesamiento de cintas de video

Misión

La misión de la Subcomisión de video SWGIT forense es proporcionar directrices con respecto a las imágenes de video y su captura, reproducción, transformación, valorización, almacenamiento y salida en un entorno forense.

Introducción

El propósito de este documento es proporcionar definiciones, recomendaciones y directrices para el uso de captura de video y procesamiento con el objetivo de garantizar la exitosa introducción de imágenes de video como prueba en un tribunal de justicia. Esta sección incluye definiciones, el equipo utilizado, las directrices para los procedimientos normalizados de trabajo y los procedimientos generales para el procesamiento de video.

Definiciones

Amplificador de distribución de video: Un dispositivo que se utiliza para dividir las señales de video individuales, mientras aumenta su fuerza para su entrega a los dispositivos de video múltiples.

Análisis de video forense: El examen científico, la comparación y/o evaluación de video en asuntos legales.

Campo: Elemento de una señal de video que contiene líneas horizontales alternativas. En el sistema NTSC de video entrelazada, el patrón de exploración se divide en dos conjuntos (pares e impares) de líneas espaciadas que se muestran secuencialmente. Cada conjunto de líneas se denomina campo, y el conjunto entrelazado de los dos conjuntos de líneas es un marco.

CD / DVD (disco compacto / disco versátil digital): Formatos de disco óptico diseñado para funcionar como medio de almacenamiento de datos.

Desentrelazado: Separar un marco entrelazado en dos campos separados.

Enhancement: Cualquier proceso destinado a mejorar el aspecto visual de una imagen.

Frame (cuadro): Líneas de información espacial de una señal de video. Para el video entrelazado, un cuadro consta de dos campos: uno de las líneas

impares y uno de las líneas pares, que se muestran en secuencia. Para la exploración progresiva (no entrelazada) de video, la trama contiene muestras a partir de un momento, y continuando a través de las líneas sucesivas de la parte inferior del marco.

Interlaced scan: Formato de video de imagen. El fotograma de video se compone de dos campos. El primer campo contiene todas las líneas horizontales impares y el segundo campo todas las líneas pares.

La matriz de conmutación: Un dispositivo utilizado para dirigir la trayectoria de una o más señales en uno o más dispositivos.

Monitor de forma de onda: Un dispositivo electrónico que proporciona una representación gráfica de la fuerza de una señal de video.

Multiplexor / demultiplexor (muxer / demuxer): Un dispositivo que se utiliza para combinar las señales de video múltiples en una sola señal o separar una señal combinada. Estos dispositivos se utilizan con frecuencia en aplicaciones de seguridad y del ámbito legal, además en la visualización de imágenes de múltiples cámaras simultáneamente o en sucesión.

NTSC: National Television Standards Committee.

Procesamiento: Cualquier actividad que transforma una imagen de entrada y/o de la señal en una imagen de salida y/o de la señal.

Producción conmutador: Dispositivo que se utiliza para mezclar las señales de video a partir de dos o más fuentes (por ejemplo: cámaras, videograbadora/jugadores, correctores de base de tiempo, generadores de caracteres) para disoluciones, barridos y otros efectos de transición.

Reproducción: Material grabado visto y oído como se registra, facilitado por la cámara de video, grabadora de cinta de video o cualquier otro dispositivo.

Reproductor de video (VCR): Máquina multifunción diseñada principalmente para la reproducción y grabación de video almacenado en cassettes.

Salida: El medio por el cual se presenta una imagen para su examen u observación.

Tarjeta de captura / retención de cuadro: Una pieza de hardware que convierte una señal de video analógica en datos digitales.

Time-corrector base (TBC, corrector de base de tiempo): Un dispositivo electrónico utilizado para corregir inconsistencias de temporización y estabilizar la reproducción de la señal de video para una calidad óptima. También sincroniza las fuentes de video que permiten la imagen de mezcla.

Time-lapse videograbadora: Un tipo de grabador de video que se puede configurar para grabar de forma continua durante largos períodos, que se logra mediante una cinta que se mueve en pasos y graba un marco o campo a

la vez. Estos dispositivos se utilizan con frecuencia en aplicaciones de seguridad y del ámbito judicial.

Vectorescopio: Un dispositivo electrónico que mide el rendimiento del color de una señal de video.

Video: La representación electrónica de una secuencia de imágenes, que representa ya sea escenas fijas o en movimiento; puede incluir audio.

Videocámara: Una cámara de video autónoma y dispositivo de grabación.

Equipo

El propósito de esta sección es identificar algunos de los equipos utilizados para visualizar, procesar y mejorar las imágenes de video.

Los dispositivos de reproducción deben ser capaces de producir una representación exacta de la imagen grabada. Los dispositivos de reproducción incluyen lo siguiente:

· Grabadoras de cinta de video, incluyendo grabadores de lapsos de tiempo
· Videocámaras
· CD/DVD
· Reproductores de medios digitales
· Monitores

Procesamiento / Mejoramiento

· Multiplexor
· Time-corrector base (corrector de base de tiempo)
· Tarjeta capturadora de video
• Frame grabber u otro dispositivo de captura de imágenes
· Computadora
· Software
• Waveform monitor/vectorscopio (monitor de campos de video)
· Sistema de edición
· Monitoreo
· Matriz de conmutación
· Producción
· Amplificador de distribución

Salida / Almacenamiento

· Monitor
· Impresora
· Videograbadora
· Dispositivos de almacenamiento (por ejemplo, ordenador, CD/DVD,

dispositivos de memoria interna o extraíble de almacenamiento)

Directrices sobre los procedimientos operativos estándar de procesamiento de video Título: Procedimiento de Operación Estándar de Procesamiento de Video

Objetivo: Aplicar las técnicas de tratamientos destinados a mejorar y/o analizar imágenes

de video. Nota: El tratamiento exitoso de imágenes de video se debe hacer con respecto a los cuatro criterios jurídicos: fiabilidad, reproducibilidad, seguridad y descubrimiento.

Equipamiento: La agencia debe abordar los siguientes requisitos mínimos de equipamiento: Hardware

- Dispositivos de reproducción
- Sistemas de procesamiento de imágenes
- Dispositivos de salida
- Almacenamiento/archivo Software
- Gestión de imágenes
- Procesamiento de imágenes

Procedimientos: Las agencias deben establecer procedimientos específicos paso a paso para el procesamiento de video de acuerdo con las directrices del SWGIT y los requisitos de la agencia. Estos procedimientos deben incluir lo siguiente, como mínimo:

- Reproducción
- Procesamiento
- Almacenamiento/archivo
- Gestión de imágenes
- Seguridad
- Salida

Calibración: Si es necesario, los organismos deben desarrollar procedimientos específicos para sus necesidades.

Cálculos: Si es necesario, los organismos deben desarrollar procedimientos específicos para sus necesidades.

Limitaciones: Las agencias deben tener en cuenta el presupuesto, el equipo, la gestión y los requisitos de acreditación de la agencia.

Seguridad: Las agencias deben desarrollar procedimientos específicos para sus necesidades.

Referencias: Documentación específica de la agencia, manuales de los fabricantes y las directrices SWGIT (Scientific Working Group on Imaging Technologies).

Capacitación: Las agencias deben documentar los procedimientos a fin de garantizar una formación suficiente para soportar la competencia y la pericia en la aplicación del procesamiento de video (Véanse las Directrices y Recomendaciones para la Formación en Tecnologías de Imagen en el Sistema de Justicia Penal en www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2002/swgittraining.htm/).

Pasos para el procesamiento de cintas de video

Las agencias deben establecer paso a paso los procedimientos específicos para el procesamiento de video de acuerdo con las directrices y requisitos del grupo de trabajo SWGIT. Estos procedimientos deben incluir como mínimo lo siguiente:

1. Hacer una inspección visual de la cinta y de la caja protectora del cassette:
   a. Asegurarse que la caja protectora esté intacta.
   b. Inspeccionar la cinta en busca de daños (por ejemplo, torsión, separación).
   c. Si se encuentra algún daño, tomar medidas correctivas y documentar.
2. Activar cualquier dispositivo de protección de grabación (por ejemplo, retirar la pestaña, deslizar la perilla de grabación, quitar el botón para grabar).
3. Determinar si la cinta presentada es un original o una copia. Si se trata de un original, ir al paso 4. Si se trata de una copia, ponerse en contacto con el remitente, solicitar la cinta original y terminar el examen de la copia de la cinta. Si la copia es la mejor disponible, continuar con su análisis.
4. Si es posible, determinar la marca, el modelo y la configuración del dispositivo utilizado para grabar el video presentado. Estas configuraciones pueden incluir el formato de grabación y la velocidad.
5. Seleccionar el o los dispositivos de reproducción adecuados para conseguir una calidad óptima de la señal del video.
6. Utilizando los dispositivos y configuraciones seleccionadas, revisar el video presentado para localizar el o los segmentos pertinentes.
7. Determinar la velocidad de reproducción apropiada para el procesamiento del video.
8. Se puede utilizar un corrector de base de tiempo a fin de estabilizar la señal para la reproducción y permitir el ajuste del video, colores, los niveles de negro, u otras señales.
9. A criterio del examinador, puede generarse una copia de trabajo del segmento pertinente utilizando un dispositivo análogo disponible o digital.

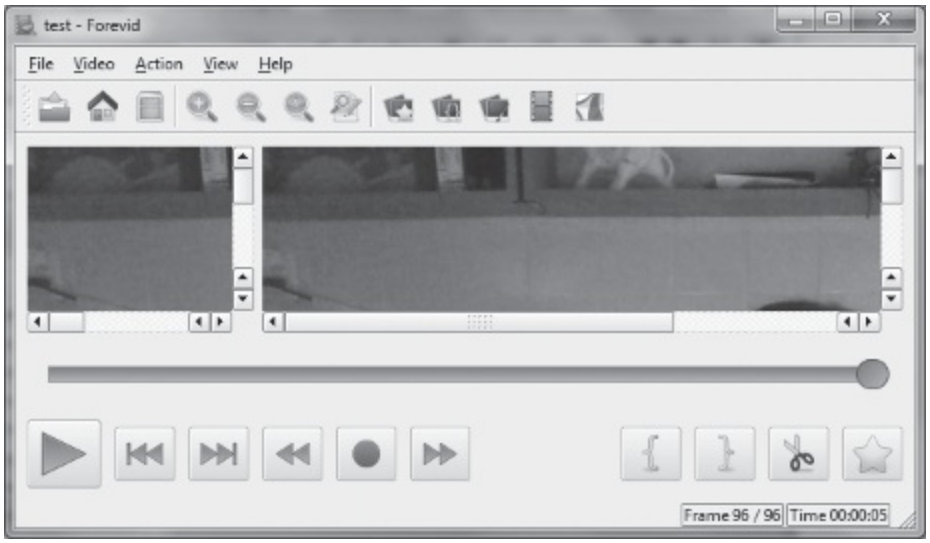
10. Las imágenes pueden ser mejoradas utilizando una serie de operaciones de procesamiento, las que pueden incluir y no están limitadas a la ecualización del histograma, ajustes de múltiples cuadros (imagen sin saltos, frame averaging), ajustes de niveles, de contraste y nitidez (Véanse las Recomendaciones y Directrices para el Uso de Procesamiento Digital de Imágenes en el Sistema de Justicia Penal en http://www.fbi.gov/ about-us/lab/forensic-science-communications/fsc/jan2003/swgitdigital).

11. Una vez que se efectuó el proceso de mejoramiento, la imagen final debe ser enviada al dispositivo apropiado de almacenamiento.

Herramientas para el análisis de video de vigilancia

• Forevid, http://www.forevid.org/, de código abierto, desarrollada por el Laboratorio Forense de la Oficina Nacional de Investigación de Finlandia (Forensic Laboratory of the National Bureau of Investigation, PO Box 285 FI-01370 VANTAA FINLAND, contact@ forevid.org). La herramienta contiene características similares a los programas comerciales y es la primera aplicación de código abierto desarrollada para el análisis de videos de vigilancia. El propósito de este proyecto es ofrecer al ámbito judicial y forense una herramienta de fácil uso. Forevid permite realizar las siguientes tareas:

- Analizar videos marco a marco.
- Ejecutar diferentes tipos de formato de video.
- Documentar y analizar los resultados.
- Aplicar diferentes operaciones al procesamiento del video.



• Amped Five, http://ampedsoftware.com/, un producto comercial, de la empresa Amped Software; verifica patentes de vehículos, caras y genera informes utilizando metodología científica.

• Cognitech, http://www.cognitech.com, comercial, desarrolla hardware y software para la adquisición de video forense.

• Ikena, http://www.motiondsp.com/products/ikena, producto comercial de la empresa MotionDSP, diseñado para acelerar, automatizar y procesar videos para el análisis forense.

• Lightworks, http://www.lwks.com/, de licencia Freeware, es decir disponible sin costo y de uso ilimitado. Editor de video no lineal.

• Ocean Systems dTective, http://www.oceansystems.com/dtective/, comercial de la empresa Ocean Systems; integra varias aplicaciones para el análisis forense de video, audio e imágenes.

• Omnivore, http://www.oceansystems.com/, producto comercial de la empresa Ocean Systems para la recuperación de video.

• Salient Stills VideoFOCUS, http://www.salientstills.com, comercial de la empresa Salient Stills, diseñado para el mejoramiento de videos y para dar apoyo en el marco judicial.

• StarWitness, http://www.starwitness.com/, ofrece una variedad de productos para la recuperación y análisis de video forense, se requiere completar la información de los datos personales para solicitar asesoramiento y capacitación.

Formulario de registro de evidencia de video

Especificaciones de otros equipos						
Marca						
Modelos						
Nro de serie						
vHs (video Home system)						
svHs (super video Home system)						
Otro						
Observaciones						
Especificaciones multiplexor						
Marca						
Modelo						
Nro de serie						
Observaciones						
Modo de grabación (horas)						
2	6	12	24	48	72	Otro
Observaciones						
Especificaciones de la cinta						

Largo (metros)			
Etiqueta			
Tiempo de grabación NTsC (National Television standards Committee)	sP (standard)	LP	EP/sLP
Tiempo de grabación PAL (Phase Alternation by Line)	sP	LP	
Observaciones			

Perito informático forense	Lugar	Fecha
Apellido: Nombre: Legajo Nro: DNI: Dirección de correo electrónico: Teléfono: Celular:	Firma Aclaración:	

138 http://en.wikipedia.org/wiki/Dalvik_(software) junio 2012.

139 http://es.wikipedia.org/wiki/YAFFS junio 2012; http://www.yaffs.net/ junio 2012.

140 Hoog, Andrew, Android Forensics, Investigation, Analysis and Mobile Security for Google Android, Ed. Elsevier-Syngress, EE.UU., 2011.

141 http://www.htc.com/la/ junio 2012.

142 http://en.wikipedia.org/wiki/Droid_Incredible junio 2012.

143 Hoog, Andrew, Android Forensics, Investigation, Analysis and Mobile Security for Google Android, Ed. Elsevier-Syngress, EE.UU., 2011.

144 Arellano, Luis y Darahuge, María Elena, Manual de Informática Forense, Ed. Errepar, Buenos Aires, 2011.

145 Hoog, Andrew, Android Forensics, Investigation, Analysis and Mobile Security for Google Android, Ed. Elsevier-Syngress, EE.UU., 2011.

146 http://developer.android.com/guide/topics/data/backup.html junio 2012.

147 Hoog, Andrew, Android Forensics, Investigation, Analysis and Mobile Security for Google Android, Ed. Elsevier-Syngress, EE.UU., 2011.

148 http://en.wikipedia.org/wiki/Joint_Test_Action_Group junio 2012.

149 Hoog, Andrew, Android Forensics, Investigation, Analysis and Mobile Security for Google Android, Ed. Elsevier-Syngress, EE.UU., 2011.

150 http://modmymobile.com/forums/35-general-en-espanol/520528-guia-como-flashear-tu-motorola-con-rsdlite.html junio 2012.

151 Guía de comandos de fastboot, http://www.htcmania.com/mediawiki/index.php/C%C3%B3mo_utilizar_Fast Boot#Requisitos_para_utilizar_FASTBOOT_en_Windows junio 2012.

152 http://source.android.com/index.html junio 2012.

153 Hoog, Andrew, Android Forensics, Investigation, Analysis and Mobile Security for Google Android, Ed. Elsevier-Syngress, EE.UU., 2011.

154 https://viaforensics.com/android-forensics/afphysical-method.html junio 2012.

155 Arellano, Luis y Darahuge, María Elena, Manual de Informática Forense, Ed. Errepar, Buenos Aires, 2011.

156 http://elinux.org/Android_Logging_System junio 2012.

157 http://thomascannon.net/projects/android-reversing/ junio 2012.

158 Consultar la secuencia de pasos para la creación de la línea de tiempo en YAFFS2: Hoog, Andrew, Android Forensics, Investigation, Analysis and Mobile Security for Google Android, Ed. Elsevier-Syngress, EE.UU., 2011.

159 http://www.rogoyski.com/adam/programs/hexedit/onlinedoc/hexedit.html#SEC9.

160 Hoog, Andrew, Android Forensics, Investigation, Analysis and Mobile Security for Google Android, Ed. Elsevier-Syngress, EE.UU., 2011.

161 *Es el número de bytes que indican el desplazamiento desde el comienzo de una estructura de datos o sector.*

162 Arellano, Luis y Darahuge, María Elena, Manual de Informática Forense, Ed. Errepar, Buenos Aires, 2011.

163 Hoog, Andrew, Android Forensics, Investigation, Analysis and Mobile Security for Google Android, Ed. Elsevier-Syngress, EE.UU., 2011.

164 *http://es.wikipedia.org/wiki/CD-ROM junio 2012.*

165 http://es.wikipedia.org/wiki/DVD junio 2012.

166 http://es.wikipedia.org/wiki/Blu-ray_Disc junio 2012.

167 http://es.wikipedia.org/wiki/Disco_compacto junio 2012.

168 *http://es.wikipedia.org/wiki/Blu-ray_Disc junio 2012.*

169 *Crowley, Paul y Kleiman, Dave, CD and DVD Forensics, Ed. Elsevier-Syngress, EE.UU., 2007.*

170 *Bolígrafos de tinta fluida en contraposición a los bolígrafos de tinta oleosa.*

171 http://www.infinadyne.com/cddvd_inspector.html junio 2012.

172 http://www.forensicimager.com/ junio 2012.

173 Arellano, Luis y Darahuge, María Elena, Manual de Informática Forense, Ed. Errepar, Buenos Aires, 2011.

174 *http://www.infinadyne.com/cddvd_inspector.html junio 2012.*

175 Crowley, Paul y Kleiman, Dave, CD and DVD Forensics, Ed. Elsevier-Syngress, EE.UU., 2007.

176 *Crowley, Paul y Kleiman, Dave, CD and DVD Forensics, Ed. Elsevier-Syngress, EE.UU., 2007.*

177 *http://smithii.com/cdrtools/ junio 2012.*

178 *http://linux.die.net/man/1/genisoimage junio 2012.*

179 *Arellano, Luis y Darahuge, María Elena, Manual de Informática Forense, Ed. Errepar, Buenos Aires, 2011.*

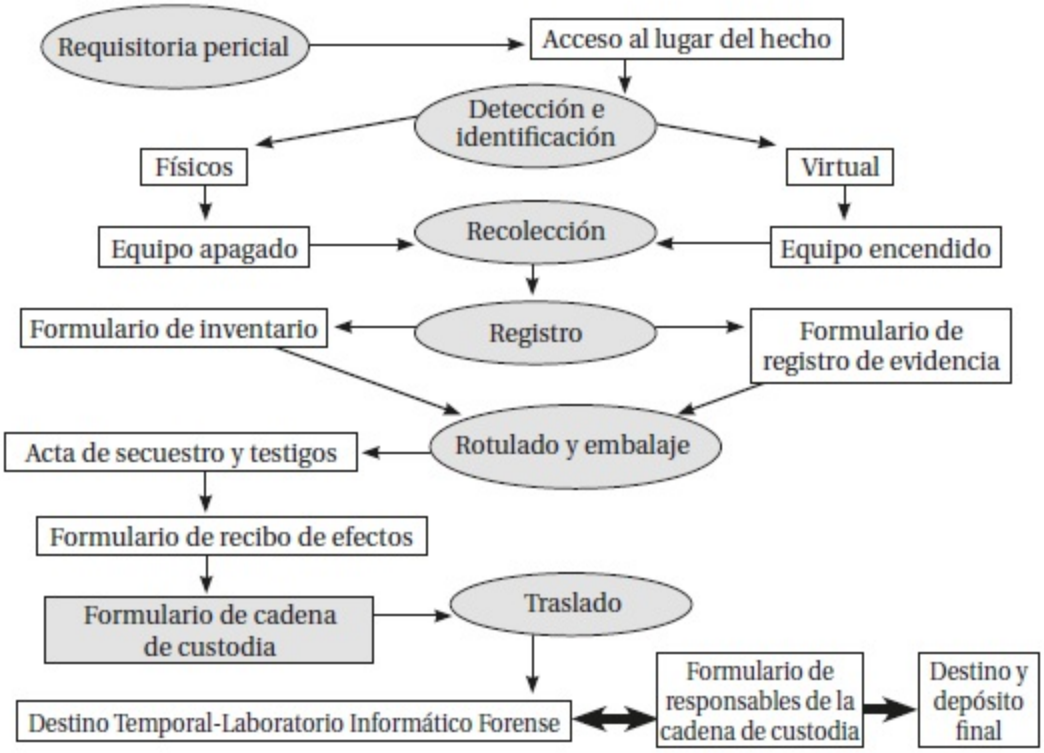
180 *Crowley, Paul y Kleiman, Dave, CD and DVD Forensics, Ed. Elsevier-Syngress, EE.UU., 2007.*

181 *Carrier, Brian, http://www.dfrws.org/2010/proceedings/2010-315.pdf junio 2012.*

182 https://www.tomtom.com/es_es/products/ junio 2012.

183 *http://www.gpsforensics.org/articles/tomtom/basis.html junio 2012.*

ANEXO 1
PROCEDIMIENTO PARA LA CADENA DE CUSTODIA EN LA PERICIA DE INFORMÁTICA FORENSE



Cadena de custodia final

La Informática forense, como especialidad dentro de la Criminalística, debe incluir los requisitos generales establecidos en la Inspección Judicial en Criminalística. En esta especialidad, los elementos dubitados pueden ser del tipo físico o virtual. En el caso de los elementos virtuales, la detección, identificación y recolección deberá efectuarse en tiempo real, es decir, en vivo, con el equipo encendido. La información es un elemento intangible que se encuentra almacenado en dispositivos que pueden ser volátiles o no. Con el fin de determinar la validez de la información contenida en los mencionados dispositivos, será necesario efectuar la correspondiente certificación matemática por medio de un digesto matemático o hash. Esta compro

bación es la que permitirá posteriormente determinar la integridad de la prueba recolectada y su correspondencia con el elemento original.

El objetivo principal es preservar la evidencia, por lo tanto al acceder al lugar del hecho deberá:

- Identificar
- Situar
- Relacionar

A través de un accionar metódico, sistemático y seguro, cuya consigna será:

- Rotular
- Referenciar
- Proteger

En síntesis, se deberá mantener la seguridad, procurar el resguardo legal y aplicar una metodología estricta.

En el lugar del hecho, se deberá seguir una secuencia de pasos expresada en el siguiente procedimiento, que será considerado como la etapa preliminar a la elaboración del formulario de la cadena de custodia (el cual a su vez debe ser considerado como información confidencial, clasificada, y resguardado en un lugar seguro):

- Detección
- Identificación y
- Registro

1. En lo posible se debe identificar la totalidad de los elementos informáticos dubitados – computadoras, red de computadoras, netbook, notebook, celular, iPad, GPS, etc.–. Consultar “Inventario de hardware en la inspección y reconocimiento judicial” y el “Formulario de registro de evidencia”.
2. Colocarse guantes.
3. Fotografiar el lugar del hecho o filmar todos los elementos que se encuentran en el área de inspección, desde la periferia hacia el interior del ambiente a revisar, considerando como destino final al núcleo de procesamiento de información sometido a examen (correspondiente a un centro de cómputos, comunicaciones, gestión de datos, administración informática, hasta una PC aislada, acorde con la magnitud de la tarea encomendada).
4. Fotografiar los elementos informáticos, determinando en cuál de ellos efectuar macro fotografías:
   a. Pantallas del monitor del equipo dubitado.
   b. Vistas frontal, lateral y posterior, según corresponda.
   c. Números de series de los elementos informáticos, etiquetas de garantías.
   d. Periféricos (teclados, mouse, monitor, impresora, agendas PDA, videocámara, video grabadora, pendrive, dispositivos de almacenamiento en

red, unidades de zip o jazz, celulares, iPod, entre otros).

5. Identificar y eventualmente secuestrar el material impreso en la bandeja de la impresora o circundante.

6. Fotografiar los cableados y dispositivos de conectividad, alámbricos e inalámbricos.

7. Modelizar y registrar diagramas de la red y topologías.

8. Inventariar todos los elementos utilizando una planilla de registro del hardware, identificando: tipo, marca, número de serie, registro de garantía, estado (normal, dañado), ob9.

servaciones particulares. Consultar el "Inventario de hardware de la Inspección Judicial y Reconocimiento Judicial" y el "Formulario de registro de evidencia de la computadora".

10. Efectuar un croquis del lugar del hecho, con elementos de dibujo o con apoyo fotográfico informático (cámaras estereométricas y reconstituidores digitales) especificando el acceso al lugar, la ubicación del o los equipos informáticos y de cualquier otro elemento, mobiliario, racks, cableado, existentes en el área a inspeccionar, para luego representarlo con cualquier herramienta de diseño.

11. Recolección de los elementos informáticos dubitados (físicos o virtuales).

12. El perito informático forense deberá recolectar la evidencia procediendo acorde al origen del requerimiento de la pericia informático forense, a saber:

Procedimiento

Por orden judicial, que indique Secuestrar la evidencia para su posterior análisis en el laboratorio, el perito informático forense procederá a:

1. Identificar y registrar la evidencia.
2. Certificarla matemáticamente.
3. Elaborar un acta ante testigos.
4. Iniciar la cadena de custodia.
5. Transportar la evidencia al laboratorio.
6. Efectuar la copia de la evidencia para su posterior análisis en el laboratorio; el perito informático forense procederá a:

a. Certificar matemáticamente la evidencia.

b. Duplicarla digitalmente.

c. Identificar y registrar la evidencia y las copias obtenidas (a veces es necesario hacer entrega de estas copias a pedido de las partes, en general los interesados deben proveer el material informático necesario para efectuar dicha copia, especialmente cuando se trata de prueba documental informática de gran porte: múltiples equipos de computación, discos rígidos, DVD, CD,

etc.). La realización de dichas copias y la entrega a las partes deben ser solicitadas y autorizadas específicamente por el tribunal interventor.

d. Elaborar un acta ante testigos.

e. Realizar las tareas periciales requeridas (tener en cuenta la obligatoriedad de informar a las partes sobre el lugar y momento de realización de dichas actividades, para asegurar la posibilidad de presenciarlas y, por ende, el legítimo derecho de defensa y el debido proceso constitucionalmente protegido).

Por solicitud particular de una persona específica, de una consultora, empresa, institución, organismo u otros profesionales, el perito informático forense procederá a:

1. Concurrir al lugar del hecho con un escribano público.
2. En lo posible, contar con testigos hábiles durante la recolección.
3. Especificar en el acta del escribano la autorización del interesado para ingresar y recolectar la información que se indique. Esta autorización debe ser expresa y manifestada en alta voz a todos los presentes. El perito no puede extender su recolección más allá de lo específicamente autorizado por el dueño de la información.
4. En caso de requerirse la inclusión de elementos de información pública, esta debe ser evidente y no requerir de autorización alguna para su acceso (membresías, identificación de usuario, suscripción, etc.).
5. La información no obrante en la máquina, perteneciente a terceros o a la contraparte, no puede ser accedida y recolectada, sin autorización judicial expresa y con los requisitos formales ya especificados.
6. Identificar y recolectar la información solicitada.
7. Certificar matemáticamente la evidencia ante el escribano público.
8. Duplicar la evidencia ante el escribano y los testigos.
9. Solicitar al escribano que deje constancia en el acta de los motivos del secuestro, de los datos de la o las personas que solicitaron la pericia, el perito, los testigos, y detallar las razones argumentadas y los fines pretendidos con la recolección y preservación efectuada.
10. Solicitar una copia del acta realizada por el escribano y del rese rvorio de información utilizado (DVD, CD).
11. Las copias deben ser identificadas y resguardadas estrictamente[184].
12. Hacer entrega de las copias a los participantes del acto (copia para el escribano, para el perito actuante y tantas como requiera la parte; cada una de ellas debe tener asociado su correspondiente formulario de cadena de custodia, inclusive la que se lleva el perito para su propio archivo personal).

Duplicación y autenticación de la prueba

En ciertas situaciones, el perito informático forense no podrá trasladar el equipamiento que contiene la información dubitada, por lo tanto deberá, en el lugar del hecho, efectuar la duplicación de la información contenida en su repositorio original. Esta tarea se deberá realizar de manera tal que la duplicación o copia generada preserve la validez de su contenido original.

A continuación, se enuncian los pasos para efectuar la autenticación y duplicación de la prueba, el perito informático forense llevará en su maletín los dispositivos de almacenamiento limpios y desinfectados y el dispositivo de arranque (disco rígido externo, CD-ROM, DVD, disquete) o inicio en vivo protegido contra escritura, que contiene el software de base seleccionado para la tarea y el software de autenticación y duplicación.

Las imágenes de los discos se deben realizar bit a bit para capturar en la totalidad del disco rígido los espacios libres, no asignados y los archivos de intercambio, archivos eliminados y ocultos. Acorde a lo expresado por el NIST (National Institute of Standard and Technology), la herramienta utilizada para la generación de la imagen debe reunir ciertas especificaciones, a saber:

1. La herramienta deberá efectuar una imagen bit a bit de un disco original o de una partición en un dispositivo fijo o removible.
2. La herramienta debe asegurar que no alterará el disco original.
3. La herramienta podrá acceder tanto a discos SCSI como IDE.
4. La herramienta deberá verificar la integridad de la imagen de disco generada.
5. La herramienta deberá registrar errores tanto de entrada como de salida e informar si el dispositivo de origen es más grande que el de destino.
6. Se debe utilizar un bloqueador de escritura, preferiblemente por hardware, para asegurar la inalterabilidad del elemento de almacenamiento accedido[185].
7. La documentación de la herramienta deberá ser consistente para cada uno de los procedimientos[186]. Esta imagen del disco se utilizará en la computadora del laboratorio para efectuar el análisis correspondiente.

Operaciones a realizar

1. Apagar el equipo desconectando el cable de alimentación eléctrica.
2. Retirar disquete, pendrive, zip.
3. Descargar la propia electricidad estática, tocando alguna parte metálica y abrir el gabinete.
4. Desconectar la alimentación eléctrica del dispositivo de disco rígido.
5. Desconectar la interfaz o cable de datos; puede ser IDE o SCSI.
6. Ingresar al CMOS (Complementary Metal Oxide Semiconductor) o

Configuración del BIOS (sistema de entrada y salida de la computadora):

a. Encender la computadora.

b. Oprimir el conjunto de teclas que se muestra en el monitor cuando se inicia la computadora para acceder al CMOS.

c. Verificar la fecha y hora del CMOS y registrarla en el formulario de recolección de evidencia y documentar todo tipo de dato que el perito informático forense considere relevante.

d. Modificar la unidad de inicio o arranque del sistema operativo, es decir, seleccionar la unidad de disquete, CD-ROM/DVD o zip.

e. Guardar los cambios al salir.

f. Verificar la existencia de discos CD-ROM o DVD:

i. Abrir la lectora o grabadora de CD-ROM o de DVD y quitar el disco pertinente.

ii. Colocar la unidad de arranque, disquete, CD-ROM/DVD o zip en el dispositivo de hardware pertinente.

g. Verificar el inicio desde la unidad seleccionada.

h. Apagar el equipo.

7. Asegurar el dispositivo de almacenamiento secundario original; generalmente está configurado en el CMOS como master –maestro o primario– con protección de solo lectura, a través de la configuración de los jumpers que indique el fabricante del disco o a través de un hardware bloqueador de lectura.

8. Conectar el cable plano al disco rígido, puede ser IDE o SCSI.

9. Conectar la alimentación eléctrica del dispositivo de disco rígido master –maestro o primario–.

10. Conectar el dispositivo que se utilice como destino para hacer la duplicación del disco rígido dubitado como slave –esclavo o secundario–, ya sea una controladora SCSI, un disco IDE esclavo o una unidad de cinta, o cualquier otro hardware utilizado para la duplicación de tamaño superior al disco original o dubitado. Si el almacenamiento secundario original es demasiado grande o es un arreglo de discos, efectuar la copia en cintas.

11. Verificar que en el dispositivo de arranque seleccionado se encuentren los controladores del hardware para la duplicación, en caso de que sean requeridos.

12. Encender la computadora desde la unidad de arranque configurada en el CMOS.

13. Efectuar la certificación matemática del dispositivo dubitado.

14. Guardar el resultado en un dispositivo de almacenamiento secundario.

15. Registrar el resultado en el formulario de registro de la evidencia.

16. Duplicar el dispositivo de los datos con la herramienta de software y hardware seleccionada.

17. Efectuar, acorde al requerimiento de la pericia, las copias de la evidencia necesarias.

En el caso de realizar dos copias, una se deja en el lugar del hecho, para permitir la continuidad de las actividades, otra copia se utiliza para el análisis en el laboratorio del perito informático forense, y el original se deja en depósito judicial o, si la pericia ha sido solicitada por un particular, se registra ante escribano público y se guarda según lo indicado por el solicitante de la pericia y el escribano público.

18. Efectuar la certificación matemática de la o las copias del dispositivo dubitado.

19. Guardar el resultado generado por las copias duplicadas en un dispositivo de almacenamiento.

20. Registrar el resultado generado por las copias duplicadas en el formulario de recolección de la evidencia.

21. Apagar el equipo.

22. Retirar los tornillos de sujeción del dispositivo de disco rígido.

23. Retirar el disco rígido con cuidado de no dañar el circuito electrónico.

recolección y registro de evidencia virtual

Equipo encendido

En el caso de que se deba acceder a un equipo encendido, se debe considerar la obtención de los datos en tiempo real y de los dispositivos de almacenamiento volátil. Los dispositivos de almacenamiento volátil de datos pierden la información luego de interrumpirse la alimentación eléctrica, es decir, al apagar la computadora la información almacenada se pierde.

Los datos que se encuentran en el almacenamiento volátil muestran la actividad actual del sistema operativo y de las aplicaciones, como por ejemplo: procesos en el estado de ejecución, en el estado de listo o bloqueado, actividad de la impresora (estado, cola de impresión), conexiones de red activas, puertos abiertos (el puerto es una estructura a la cual los procesos pueden enviar mensajes o de la cual pueden extraer mensajes, para comunicarse entre sí, siempre está asociado a un proceso o aplicación, por consiguiente solo puede recibir de un puerto un proceso, recursos compartidos, estado de los dispositivos como discos rígidos, disqueteras, cintas, unidades ópticas).

Los datos volátiles están presentes en los registros de la unidad central de procesamiento del microprocesador, en la memoria caché, en la memoria

RAM o en la memoria virtual.

Procedimiento para el acceso a los dispositivos de almacenamiento volátil

Conjunto de tareas a realizar en el acceso a los dispositivos de almacenamiento volátil:

1. Ejecutar un intérprete de comandos confiable o verificado matemáticamente.
2. Registrar la fecha, hora del sistema, zona horaria.
3. Determinar quién o quiénes se encuentran con una sesión abierta, ya sean usuarios locales o remotos.
4. Registrar los tiempos de creación, modificación y acceso de todos los archivos.
5. Verificar y registrar todos los puertos de comunicación abiertos.
6. Registrar las aplicaciones relacionadas con los puertos abiertos.
7. Registrar todos los procesos activos.
8. Verificar y registrar las conexiones de redes actuales y recientes.
9. Registrar la fecha y hora del sistema.
10. Verificar la integridad de los datos.
11. Documentar todas las tareas y comandos efectuados durante la recolección.
12. Posteriormente, en lo posible, se debe realizar una recolección más detallada de los datos existentes en el almacenamiento volátil, efectuando las siguientes tareas:
    a. Examinar y extraer los registros de eventos.
    b. Examinar la base de datos o los módulos del núcleo del sistema operativo.
    c. Verificar la legitimidad de los comandos del sistema operativo.
    d. Examinar y extraer los archivos de claves del sistema operativo.
    e. Obtener y examinar los archivos de configuración relevantes del sistema operativo.
    f. Obtener y examinar la información contenida en la memoria RAM del sistema.

Procedimiento con el equipo encendido

1. En la computadora, con el equipo encendido, acceder al recurso acorde al orden de volatilidad de la información, con las herramientas forenses almacenadas en disquete o CD-ROM y de acceso de solo lectura.
2. Ejecutar un intérprete de comandos legítimo[187] y certificado.

3. Obtener y transferir el listado de comandos utilizados en la computadora, antes de la recolección de datos.
4. Registrar fecha y hora del sistema.
5. Recolectar, transferir a la estación forense o medio de recolección forense y documentar.
a. Fecha y hora del sistema.
b. Memoria principal.
c. Usuarios conectados al sistema.
d. Registro de modificación, creación y tiempos de acceso de todos los archivos.
e. Listado de puertos abiertos y de aplicaciones escuchando en dichos puertos.
f. Listado de las aplicaciones asociadas con los puertos abiertos.
g. Tabla de procesos activos.
h. Conexiones de red actuales o recientes.
i. Recursos compartidos.
j. Tablas de ruteo.
k. Tabla de ARP.
l. Registros de eventos de seguridad, del sistema, de las aplicaciones, servicios activos.
m. Configuración de las políticas de auditoría del sistema operativo.
n. Estadísticas del núcleo del sistema operativo.
ñ. Archivos de usuarios y contraseñas del sistema operativo.
o. Archivos de configuración relevantes del sistema operativo.
p. Archivos temporales.
q. Enlaces rotos.
r. Archivos de correo electrónico.
s. Archivos de navegación en Internet.
6. Certificación matemática de la integridad de los datos.
7. Listado de los comandos utilizados en la computadora, durante la recolección de datos.
8. Recolectar la topología de la red.
9. Si es factible, apagar el equipo.

Equipo apagado

En el caso de que el perito informático forense efectúe la recolección de la evidencia a partir del equipo apagado, deberá previamente asegurarse de que

el dispositivo de inicio del equipo no se realice a través del disco rígido o dispositivo de almacenamiento secundario dubitado.

Deberá utilizar dispositivos de arranque en el modo solo lectura, con herramientas informáticas forenses para realizar la detección, recolección y registro de indicios probatorios.

Procedimiento para la detección, recolección y registro de indicios probatorios

1. Retirar disquetes, pendrive, zip.
2. Apagar el equipo y desconectar el cable de alimentación eléctrica.
3. Descargar la propia electricidad estática, tocando alguna parte metálica y abrir el gabinete.
4. Abrir el gabinete y desconectar la interfaz o cable de datos; puede ser IDE o SCSI.
5. Desconectar la alimentación eléctrica del dispositivo de disco rígido.
6. Ingresar al CMOS (Complementary Metal Oxide Semiconductor) o Configuración del BIOS (Sistema de entrada y salida de la computadora):
   a. Encender la computadora.
   b. Oprimir el conjunto de teclas que se muestra en el monitor cuando se inicia la computadora para acceder al CMOS.
   c. Verificar la fecha y hora del CMOS, registrarla en el formulario de recolección de evidencia, documentar todo tipo de dato que el perito informático forense considere relevante y documentarlo con fotografía, filmadora o en la lista de control.
   d. Modificar la unidad de inicio o arranque del sistema operativo, es decir, seleccionar la unidad de disquete, CD-ROM/DVD o zip de solo lectura con las herramientas informático forenses.
   e. Guardar los cambios al salir.
7. Colocar la unidad de arranque, disquete, CD-ROM/DVD o zip en el dispositivo de hardware pertinente.
8. Verificar el inicio desde la unidad seleccionada.
9. Apagar el equipo.

Acorde a la decisión del perito informático forense o a lo solicitado en la requisitoria pericial, se podrá realizar el procedimiento de duplicación y autenticación de la prueba, explicado anteriormente, o continuar con la lectura del dispositivo original, configurándolo con los jumpers que el fabricante indique como solo lectura o colocando un dispositivo de hardware de bloqueo de escritura.

1. Conectar el cable plano al disco rígido; puede ser IDE o SCSI.
2. Conectar la alimentación eléctrica del dispositivo de disco rígido.
3. Encender la computadora desde la unidad de arranque configurada en el CMOS.
4. Colocar el dispositivo de almacenamiento forense.
5. Efectuar la certificación matemática del dispositivo dubitado.
6. Guardar el resultado en un dispositivo de almacenamiento forense.
7. Registrar el resultado en el formulario de recolección de la evidencia.
8. Por medio del conjunto de herramientas informático forenses, obtener la siguiente información del disco dubitado, documentarla y almacenarla en dispositivos de almacenamiento forense, para su posterior análisis, ya sea en el lugar del hecho o en el laboratorio:
a. Tipo de sistema operativo.
b. Fecha, hora y zona horaria del sistema operativo.
c. Versión del sistema operativo.
d. Número de particiones.
e. Tipo de particiones.
f. Esquema de la tabla de particiones.
g. Listado de todos los nombre de archivos, fecha y hora.
h. Registro del espacio descuidado o desperdiciado.
i. Incluir el MBR y la tabla de particiones.
j. Incluir la partición de inicio del sistema y los archivos de comandos.
k. Registro del espacio no asignado.
l. Registro del espacio de intercambio.
m. Recuperación de archivos eliminados.
9. Búsqueda de archivos ocultos, con las palabras claves, en:
a. El espacio desperdiciado.
b. El espacio no asignado.
c. El espacio de intercambio.
d. El MBR y tabla de particiones.
10. Listado de todas las aplicaciones existentes en el sistema.
11. Búsqueda de programas ejecutables sospechosos.
12. Identificación de extensiones de archivos sospechosas.
13. Listado de todos los archivos protegidos con claves.
14. Listado del contenido de los archivos de cada usuario en el directorio raíz y, si existen, en los subdirectorios.

15. Verificación del comportamiento del sistema operativo:

a. Integridad de los comandos.

b. Integridad de los módulos.

c. Captura de pantallas.

16. Generar la autenticación matemática de los datos a través del algoritmo de hash al finalizar la detección, recolección y registro.

17. Conservar las copias del software utilizado (debidamente resguardadas y certificadas mediante hash).

18. Apagar o dejar funcionando el equipo, esto dependerá de la requisitoria pericial.

Procedimiento para el resguardo de la prueba y preparación para su traslado

1. Disponer, según sea el caso, las pruebas obtenidas en una zona despejada, para su posterior rotulado y registro.

2. Registrar en el formulario de registro de la evidencia cada uno de los elementos dubitados, acorde a lo especificado en dicho formulario y agregando cualquier otra información que considere pertinente el perito informático forense.

3. Proteger:

a. En bolsas antiestáticas los elementos informáticos de almacenamiento secundario, registrando fecha y hora del secuestro, tipo, nro. de serie del elemento si se puede obtener, capacidad de almacenamiento, apellido, nombre y DNI del perito informático forense, firma del perito informático forense –Rótulos para las evidencias–.

b. En bolsas manufacturadas con filamentos de cobre y níquel para prevenir la interferencia de señales inalámbricas, celulares, GPS, etc.

c. Con plástico y/o con bolsas estériles, cualquier otro elemento que considere relevante el perito informático forense y rotularlos con los datos pertinentes al elemento, apellido, nombre y DNI del perito informático forense, firma del perito informático forense.

4. Elaborar el acta de secuestro acorde al formulario del recibo de efectos.

5. Colocar los elementos identificados y registrados en una caja o recipiente de traslado que asegure la suficiente rigidez, aislamiento térmico, electromagnético y protección para evitar daños accidentales en el traslado de los elementos probatorios.

6. Trasladar, en lo posible, los elementos secuestrados reunidos en un único recipiente, evitando la confusión, separación o pérdida durante su almacenamiento posterior

–Formulario para la cadena de custodia–.

Traslado de la evidencia de Informática forense

El traslado de la evidencia tendrá como destino el Laboratorio de Informática Forense correspondiente al organismo establecido en la requisitoria pericial. La permanencia en este laboratorio puede ser temporal, pero será necesario mantener la cadena de custodia mientras la prueba sea analizada por las entidades involucradas –Formulario de responsables de la cadena de custodia–.

Acorde a la evolución del proceso judicial en el que se encuentra involucrada la prueba de Informática forense, la prueba podrá ser posteriormente entregada y resguardada en un lugar o destino específico para su resguardo y depósito final o definitivo.

Nota: Es sumamente importante considerar que si bien la prueba documental informática constituye una especie del género prueba documental clásica (bibliográfica, foliográfica y pictográfica), de la cual solo difiere en el soporte (papel vs. digital), no significa que por esto escape a las consideraciones generales que le aporta la Criminalística en su sentido más amplio.

Suele ocurrir que, como la realización de la certificación por digesto matemático de los discos secuestrados (hash) in situ es una tarea que insume mucho tiempo, se prefiere secuestrar los equipos, clausurarlos y dejar la tarea de validación y hash para un momento posterior, generalmente en el laboratorio pericial. Sin embargo, se suele preservar la prueba en las mismas condiciones en que fue encontrada en el momento de la recolección. Este criterio hace que al secuestrar equipos informáticos, se mantenga el disco conectado a su fuente de alimentación y a su cable de datos para “no modificar la prueba y preservar las condiciones de secuestro”. Sin embargo, este es un error que pone en serio riesgo la integridad de los datos recolectados en el disco referido. Debemos tener presente que se puede acceder al disco por cualquier puerto (conectores USB, serie, paralelo, de red, inclusive inalámbricos, etc.).

En efecto, si el aislamiento posterior del equipo con las correspondientes fajas de clausura deja resquicios accesibles, cualquier persona de manera intencional o accidental podrá acceder al disco y modificar su contenido. La experiencia indica que muchas veces es posible incluso retirar el disco o acceder a este sin romper las fajas de clausura oportunamente colocadas. De ahí que sea preferible abrir el gabinete y desconectar físicamente el disco (alimentación y datos), hecho que debe ser registrado en el acta de secuestro, lo que lo protegerá de accesos indeseados, hasta el momento de la ruptura

formal de las fajas, para realizar las tareas técnico periciales encomendadas.

Esta acción de apertura debe ser ejecutada con todos los requisitos procesales debidos: acta de apertura, presencia de testigos, comprobación de integridad de las fajas de clausura y desconexión de los discos insertos en el gabinete, todo lo cual debe quedar registrado en un acta de apertura, que constituye la contrapartida del acta de secuestro. Al finalizar la labor pericial, debe desconectarse nuevamente el disco y dejar registro de esta circunstancia en el acta que corresponda (tareas periciales efectuadas, registro, comprobación, etc.). Todos los elementos utilizados, incluyendo las actas y las fajas de clausura retiradas, deben ser preservados y agregados al informe pericial para su revisión oportuna, durante el desarrollo del proceso judicial que diera origen a la tarea detallada.

Haciendo una analogía que tal vez pueda clarificar este punto, cuando se secuestra un arma se privilegia la seguridad por sobre la protección de la prueba, es decir, se descargan y envían proyectiles, vainas y munición intacta por separado, en especial para evitar accidentes, esto en nada afecta a la prueba. La misma atención se debe aplicar a la prueba documental informática resguardada en el disco; se debe privilegiar la protección de los datos por sobre el mantenimiento de las condiciones de recolección a ultranza, basta con aclarar la acción efectuada, para que el juez tenga conocimiento de lo ocurrido y su razón de ser técnica y procesal.

Inventario de hardware en la inspección y reconocimiento judicial

Id	Tipo	Nro. de serie/Marca/Modelo Capacidad/velocidad	Estado	Observaciones
1	Monitor			
2	Teclado			
3	Mouse			
4	Gabinete			
5	Impresora			
6	Unidad de zip			
7	Unidad de jazz			
8	Pendrive			
9	Cámara			
10	Parlantes			
11	Discos externos			
12	Disco rígido			
13	Disquetes			
14	CD-rOM			

15	DvD			
16	Hub			
17	switch			
18	router			
19	Computadora Portátil			
20	Módem			
21	Placa de red			
22	Celular			
23	Teléfono			
24	UPs			
25	IPod			
26	Otros no especificados			

Formulario de registro de evidencia de la computadora

Organismo	Formulario de registro de evidencia de la computadora	IF-Nro.
Caso Nro.	juzgado	Lugar y fecha

Especificaciones de la computadora	
Marca	
Modelo	
Nro. de serie	
Garantía	
Placa Madre Marca/Modelo	
Microprocesador Marca/Modelo/velocidad	
Memoria rAM	
Memoria Caché	

Almacenamiento secundario, fijo y/o removible					
Cantidad	Tipo Disquetera, CD-rOM, DvD, Disco rígido, IDE, sCsI, UsB, Zip,	Marca/ Modelo	velocidad/ Capacidad	Nro. de serie	Hash (si correspo

	jazz, Pendrive				

Accesorios y periféricos				
Cantidad	Tipo Placa de red, módem, cámara, tarjeta de acceso, impresora, etc.	Marca/ Modelo	velocidad/ Capacidad	Nro. de serie

Observaciones		
Perito informático forense	Lugar	Fecha
Apellido: Nombre: Legajo Nro.: DNI:	Firma Aclaración:	

Formulario de registro de evidencia de celulares

Organismo	Formulario de registro de evidencia celulares	IF-Nro.
Caso Nro.	juzgado	Lugar y fecha

Especificaciones del celular	
Marca	
Modelo	
Nro. de serie	
Garantía	
IMEI	
Nro. teléfono	
Proveedor de enlace	
Otro	

Almacenamiento				
Cantidad	Tipo Memoria	Marca/Modelo	velocidad/ Capacidad	Nro. de serie

Accesorios y periféricos				
Cantidad	Tipo	Marca/Modelo	velocidad/ Capacidad	Nro. de serie

Observaciones		
Perito informático forense	Lugar	Fecha
Apellido: Nombre: Legajo Nro.: DNI:	Firma Aclaración:	

Rótulos para las evidencias

Nro.
Caso
Fecha
Tipo
Observaciones
Firma

Formulario – recibo de efectos*

Fecha	Organismo	Caso Nro.
Dirección	Ciudad/Provincia	Teléfono
requiere consentimiento sÍ NO	Firma del responsable del consentimiento	rótulo
Descripción del elemento		
Número Único de Identificación		
Modelo		
P/N		
s/N		
Entrega conforme		Firma
recibe conforme		Firma

*Adjuntar con el formulario de cadena de custodia.

Formulario para la cadena de custodia

Cadena de custodia de la evidencia (seguimiento – trazabilidad)					
Nro. Identificación de Caso:					
Nro. Único de Identificación	Ubicación actual	Fecha	razón de traslado	sitio a donde se traslada	Observaciones
Entregado por:					Firma y Aclaración
recibido por:					Firma y Aclaración
Lugar de depósito final de la evidencia:					Fecha:

Formulario de responsables de la cadena de custodia

Nro. de Identificación Único del Caso:			
responsable	Firma y Aclaración	Fecha	Hora
Entregado por:			
recibido por:			
razón de traslado:			
responsable	Firma y Aclaración	Fecha	Hora
Entregado por:			
recibido por:			
razón de traslado:			
responsable	Firma y Aclaración	Fecha	Hora
Entregado por:			
recibido por:			
razón de traslado:			
responsable	Firma y Aclaración	Fecha	Hora
Entregado por:			
recibido por:			
razón de traslado:			
responsable	Firma y Aclaración	Fecha	Hora
Entregado por:			
recibido por:			
razón de traslado:			
responsable	Firma y Aclaración	Fecha	Hora
Entregado por:			
recibido por:			
razón de traslado:			

Modelo de Acta de inspección o secuestro

En la Ciudad Autónoma de Buenos Aires, a los trece días del mes de junio de 2013, el funcionario que suscribe, Inspector N. T., Jefe de la Unidad de Delitos Informáticos de la Policía Metropolitana, en cumplimiento de la Orden de Allanamiento Nº 132/13, emitida por el Sr. Juez Nacional de Primera Instancia en lo Criminal de Instrucción Dr. P. A., por ante la Secretaría Nº 2, del Dr. A. A. y en relación con los autos caratulados “Andrea Castaneta, s/Infracción a la ley 11.723”, hace constar que en este acto se constituye en el inmueble sito en la calle Virrey Loreto 8.612, piso 35, Dpto. 305, donde en

presencia de los testigos: J. O. F., DNI ..., TE..., Email..., ddo. en Campillay 123, Llavallol, Pcia. de Buenos Aires y C.A., DNI..., TE..., Email..., ddo. en Pedro Luro 451, San Pedro, Pcia. de Buenos Aires y de la titular del inmueble, A. C., DNI ..., y procede al secuestro*188*, a fin de ser trasladado a la Dependencia Policial antes citada, de un equipo de computación, compuesto de un gabinete de color negro, identificado con el Nº de Serie 1234345622-11, cuyo registro fotográfico se acompaña a la presente, un monitor marca View Sonic, de 17 pulgadas, color, Serie 1165654, con su correspondiente teclado marca M Serie 888898889234 y mouse de tres botones, de color negro, marca Logitech, sin número de serie. Que se procedió a la apertura del gabinete precitado y a la desconexión física del cable de alimentación y del cable de datos del disco rígido marca Seagate, Nº 234890765432, con capacidad de 80 Gigabytes, cerrándose nuevamente el gabinete, que fue envuelto en film y precintado con dos franjas de clausura transversales, acorde con la fotografía que se anexa, la que fue firmada por la totalidad de los presentes en el acto. Se inicia en el mismo acto el correspondiente formulario de cadena de custodia, referido con el número UDI-PMCABA 1245/13, el que forma parte integral de la presente, conjuntamente con los referidos registros fotográficos. Se deja constancia de que la mencionada A. C., mostró en todo momento una actitud colaborativa con la comisión policial, facilitando en todo su labor. Terminado el acto y leída que fue la presente en alta voz a los participantes del acto, se ratifican de su contenido, firmando al pie de la presente para constancia de que CERTIFICO.

Modelo de Acta de escribano

ACTA DE CONSTATACIóN: requiere Mario P. ESCRITURA NÚMERO CIENTO DIEZ Y SEIS.

En la Ciudad de Buenos Aires, República Argentina, a los veinticuatro días del mes de junio del año dos mil nueve, ante mí, escribana autorizante, constituida a solicitud del requirente, en la calle Díaz Colodrero 2895, piso 1º de esta ciudad, en donde ante mi COMPARECE: ...., italiano, nacido el 9 de agosto de 1946, divorciado, titular del Documento Nacional de Identidad ..., domiciliado en la calle OT 38, San Isidro, Provincia de Buenos Aires, de tránsito aquí. Persona capaz, mayor de edad y que he individualizado de acuerdo al artículo 1002 inciso c) del Código Civil con el mencionado documento de identidad que en su original tengo a la vista para el presente acto, y que en fotocopia debidamente autenticadas agrego por cabeza de la presente, doy fe, quien manifiesta actuar en nombre y representación de Juan Carlos O., M... O. y Nicolás Dublo, a mérito de Poder General Judicial, otorgado mediante escritura 88 del 21 de mayo de 2009, pasada al folio 236 del presente registro y corriente protocolo, ante el Escribano Osvaldo G. C., al

cual me remito. Y el compareciente en el carácter invocado y acreditado manifestando que dicho poder no le fue revocado, suspendido, ni limitado en forma alguna EXPONE: Que requiere de mí, escribana autorizante, me constituya en su compañía, en la calle DC ..., piso 1º de esta ciudad, a los efectos de proceder a registrar las actividades periciales informático forenses necesarias para resguardar la posterior prueba judicial, que sea requerida, acorde a lo solicitado por el abogado P. Que dichas actividades serán efectuadas técnicamente por el Ingeniero Luis Enrique ARELLANO GONZÁLEZ, y consisten en: 1) la detección de la existencia y desarrollo comercial de la firma, que gira en esta ciudad, bajo la denominación SC.... LIMITADA, que obren en la red de Internet; 2) Copia de seguridad y resguardo de encabezados de los mensajes que obran en las distintas cuentas sometidas a estudio, a saber: m@s.com.ar, e@s.com.ar, a@ fibertel.com.ar, m@hotmail.com, m@fibertel.com.ar. 3) El resguardo en una unidad de almacenamiento óptico (CD) de la totalidad de la prueba identificada, protegida y resguardada, la que se certificará contra modificaciones, mediante la creación de un digesto, empleando dos algoritmos de Hash, independientes, bajo la norma de los protocolos MD5 y SHA1. ACEPTO EL REQUERIMIENTO considerando al requirente con interés legítimo para el presente acto, siendo las 14:50 horas del día de la fecha. Acto seguido dejo constancia que se encuentra presente en el lugar el Ingeniero Luis Enrique ARELLANO GONZÁLEZ, quien se identifica con su Documento Nacional de Identidad, número 10... y exhibe Matrícula Profesional del CONSEJO PROFESIONAL DE INGENIERIA DE TELECOMUNICACIONES, ELECTRóNICA Y COMPUTACIóN Número 5101 y Carnet de Perito de la misma Institución y orden de registro de matrícula. Que en este estado el precitado ingeniero, comienza a realizar las tareas, enumeradas y que consisten en: 1) Se procede a acceder a la cuenta de Outlook Express, designada con la identificación: a@fibertel.com.ar, desde una de las computadoras que se encuentran en la vivienda. Para realizar dicho acceso se cuenta con la autorización de su propietario J...i, quien se encuentra presente, autoriza y facilita el acceso a dicha cuenta. 2) Se procede a efectuar una inspección detallada y específica, para obtener mensajes relacionados con la solicitud del Dr. MP. A partir de dicha inspección, búsqueda y selección, se puede establecer la existencia de DIEZ (10) mensajes procedentes de la cuenta M...Y, correspondiente a la cuenta de correo electrónico: m@s.com.ar. Efectuado el correspondiente despliegue de encabezados de los mensajes detectados y recibidos, se pudo establecer que corresponden al período 1/10/2007, al 24/06/2009, con la opción de mensajes adjuntos. A partir de dicha revisión se obtienen los datos de origen (m@s.com.ar), destino (a@ fibertel.com.ar), archivos adjuntos y hora de transmisión GMT, se resguardan en la carpeta mensajes-y-s. Dichos

mensajes poseen las siguientes características identificativas: 1) viernes 06 de junio de 2..., 0300 PM, con archivo adjunto denominado “o...xls”, de 6,67 kilobytes. 2) Se efectúa un filtrado de los mensajes procedentes de la cuenta de M...Y (m...@fibertel.com.ar) destino (a@fibertel.com.ar), se puede establecer la existencia de 3 (TRES) mensajes, dentro de la carpeta denominada mensajes-y-fibertel. Dichos mensajes poseen las siguientes características identificativas: 1) lunes 13 de octubre de 2... 03:16 p.m., con adjunto ATT00010, TXT de 133 bytes, 2) jueves, 22 de enero de 2009 03:19 p.m... miércoles, 22 de abril de 2009 10:01 a.m. con adjunto obra pendiente.doc de 60,5 Kb. En todos los casos se procede a la captura de las ventanas que contienen los mensajes y los siguientes campos de mensaje: “DE”, “FECHA”, “PARA”, “ASUNTO” y “ADJUNTAR”. A continuación se efectúa la visualización de las propiedades del mensaje, se captura la ficha general, la ficha detalles donde aparece el encabezado de Internet para cada mensaje respectivo. Seguidamente se captura la información correspondiente al origen de mensaje, donde se encuentra el “código fuente del mensaje”. Se procede al resguardo del mensaje en formato digital en una carpeta identificada con el nombre: “mensaje-fechadelmensaje”, se copia el código fuente del mensaje, en un archivo de texto y se resguarda con el nombre “encabezado del mensaje” y la fecha correspondiente. Se procede a resguardar los archivos adjuntos a cada mensaje, en la carpeta respectiva. 3) Se procede a la captura de pantallas y resguardo de encabezados de los mensajes recibidos en la casilla de correo de m...o.22@hotmail. com, dentro de la carpeta denominada mensajes-hotmail, se puede establecer la existencia de 2 (DOS) mensajes. Dichos mensajes poseen las siguientes características identificativas: 1) martes 02 de marzo de 2009 08:18:05 p.m, 2) martes 03 de marzo de 2009 12:04 p.m. 3) Se capturan pantallas de los mensajes procedentes de la cuenta de correo m...@s.com.ar sin archivo adjunto recibidos entre los meses de marzo de 2... y abril de 2009. Se resguarda la información recolectada de los mensajes en el archivo mensajes-recibidos-s.doc. 6) Se efectúa la consulta del registro de dominio de s.com.ar en el sitio web del Centro de Información de Red de Argentina en la dirección url: http://www.nic.ar y posterior captura de pantalla de la página. 7) Se ingresa la dirección http://www.s.com.ar en el navegador de Internet y se accede al sitio y se navega por los enlaces de la página principal y de los vínculos Empresa, Servicios, Asociarse, Formularios y Contacto, se capturan las páginas correspondientes a los distintos enlaces del sitio. 8) Se efectúa la búsqueda en el buscador Google en la dirección http://www.google.com.ar con el siguiente texto ·“s” y se procede a la captura de pantallas de los resultados obtenidos.

9) Se consultan en el sitio http://network-tools.com/ los registros del nombre de dominio (DNS) – s.com.ar y del registro de intercambio de correo (MX)

correspondiente al servidor de correo mail.s.com.ar. Se consulta la dirección ip 200.80.42.119, registro whois y trazado de la ruta a través de la dirección url http://visualroute.visualware.com/, se capturan las respectivas páginas. Se resguarda la información recolectada en el archivo denominado Registros-dominio-s.doc. Al finalizar las tareas, se procedió a efectuar una certificación de contenido de archivos empleando el algoritmo MD5 (Message-Digest Algorithm 5, Algoritmo de Resumen del Mensaje 5) con el siguiente resultado: # MD5 checksums generated by MD5summer (http:// www.md5summer.org); # Generated 24/06/2009 10:07:40 p.m.; 53aa68d4b24712bde51e58cf17 ee7301 *mensajes-recibidos-S.doc; a27f7b668138005e2654e35aba8e4f7f... *Registros-dominios.doc; 8ea57be61258b16 f22ac9168b4f218b6. Se realiza un original y siete copias, el original se adjunta a la presente acta de constatación. Siendo las horas, doy por concluido mi cometido, LEO al requirente y al ingeniero que realiza la labor técnica, quienes se ratifican plenamente de su contenido y en prueba de conformidad, firman por ante mí, de todo lo cual, doy fe. 10)

184 En la práctica diaria solemos recurrir al uso de sobres del tipo de envío por avión, que una vez cerrados y sellados, si son abiertos o perforados, se inflan y muestran de manera evidente la violación soportada. Por otra parte, cuentan con una etiqueta con numeración propia, lo que facilita la identificación y certificación por parte del escribano interventor.

185 Siempre es necesario recurrir a un bloqueador de escritura por hardware, ya que los que operan por software son fácilmente impugnables por la contraparte.

186 Esta característica es una fuente excelente de impugnación para el abogado que la tome en cuenta. En efecto, si el perito trabaja con una herramienta, debe poder explicar con claridad los procedimientos y selecciones efectuados en forma manual, semiautomática o automática, por el programa utilizado. Si no puede hacerlo, entonces la prueba no es válida, ya que implicaría confiar ciegamente en lo que propone un fabricante de software, generalmente extranjero y que no admite el acceso a sus códigos fuentes y a sus estructuras lógicas de recolección de datos, escudado en el secreto comercial. Debemos recordar que estamos entregando elementos probatorios, destinados a brindar soporte a una decisión judicial que seguramente afectará el patrimonio o la libertad de una persona. Por eso, recomendamos a nuestros lectores el uso de herramientas de software libre, cuyo código fuente esté disponible y cuyos algoritmos sean públicos.

187 Siempre debemos utilizar herramientas aprobadas y aceptadas por el diseñador, fabricante o comunidad de respaldo del sistema operativo considerado.

188 En referencia a estos actos se debe tener en cuenta el correcto empleo de los siguientes vocablos:

Expropiar: (paras. de propio)

1. Desposeer legalmente (de una cosa) a su propietario por razón de interés público.

2. tr. Quitar una cosa a su propietario por motivos de utilidad pública y a cambio ofrecerle generalmente una indemnización: “le han expropiado una finca para construir una autopista”.

Confiscar:

1. Atribuir al Fisco (los bienes de una persona).

2. tr. Privar a alguien de sus bienes y aplicarlos a la Hacienda Pública o al Fisco.

3. Apropiarse las autoridades competentes de lo implicado en algún delito: “confiscar mercadería de contrabando”.

4. Apropiarse de algo (por la fuerza, con o sin violencia).

Secuestrar:

1. tr. Detener y retener por la fuerza a una o a varias personas para exigir dinero u otra contraprestación a cambio de su liberación: “amenazaron con asesinar a los secuestrados, si no liberaban a sus compañeros encarcelados”.

2. Tomar el mando de un vehículo o nave por la fuerza, reteniendo a sus pasajeros o a su tripulación, con el fin de obtener un beneficio a cambio de su rescate: “secuestrar un avión”.

3. Ordenar el juez el embargo o retirada de la circulación de una cosa: “secuestrar la edición de un periódico”. Decomisar: tr. Incautarse el Estado como pena de las mercancías procedentes de comercio ilegal o los instrumentos del delito: “se ha decomisado un kilo de heroína”.

Incautar(se) (no existe el verbo incautar): (de in y cautum, multa) Forma pronominal.

1. Dicho de una autoridad judicial o administrativa. Privar a alguien de sus bienes como consecuencia de la relación de estos con un delito, falta o infracción administrativa. Cuando hay condena firme se sustituye por la pena accesoria de comiso.

2. Apoderarse arbitrariamente de algo. Fuente: www.rae.es.

ANEXO 2
ESTRUCTURA DEMOSTRATIVA JUDICIAL

Con el objeto de facilitar al perito la interacción con los operadores del Derecho, se agrega esta síntesis argumental, que pretende actuar como interfaz entre las solicitudes del abogado y las respuestas técnicas del experto convocado. Aunque aparece como un tema destinado principalmente a los profesionales del Derecho, debería ser considerado y empleado por el perito a la hora de construir sus discursos demostrativos, ya que de esta manera se facilita la comprensión por quien debe analizarlos, evaluarlos y decidir sobre su utilidad probatoria (resulta mucho más fácil convencer si hablamos el mismo idioma que nuestro interlocutor).

Para comprender la naturaleza del litigio judicial, es necesario mostrar algunas de sus características básicas:

1. Sin pretensión no hay litigio.
2. La pretensión se genera a partir de la transgresión de una norma jurídica.
3. La resolución de la pretensión consiste siempre en una acción positiva implementada mediante el imperio de la ley (ejecución de sentencia).
4. Quien decide si la pretensión está debidamente fundada es el juez.
5. Para convencer al juez sobre la credibilidad, confiabilidad y ajuste a derecho de la pretensión, es necesario realizar una construcción argumental, lógico-racional, para demostrar:
   a. Los hechos descriptos.
   b. La transgresión a la norma jurídica como consecuencia del punto anterior.
6. Todo hecho puede ser descripto mediante un procedimiento formal:
   a. Determinar el sistema de referencias que lo circunscribe.
   b. Establecer las variables que involucra.
   c. Organizar las variables en una estructura dinámica coherente (guión).
   d. Generar la estructura argumental correspondiente:
      i. Transformar todas las variables en variables binarias puras (proposiciones).
      ii. Transformar las proposiciones en premisas: afirmar o negar las proposiciones mediante argumentos fácticos; este es el momento de utilizar la prueba disponible y establecida en el Código Procesal correspondiente.
      iii. Utilizar las premisas para construir silogismos válidos.
      iv. Integrar los silogismos en un modelo de comportamiento que confluya en

una variable que debe ser lo más similar posible a la pretensión (si hay identidad, la pretensión está probada; si no se logra, cuanto más se aleje de esta identidad, mayor será el grado de libertad disponible por el juez: pasando desde la prueba tasada, a la sana crítica, hasta las libres convicciones).

e. Sobre la estructura lógica argumental anterior, se construye la fundamentación jurídica, la que dependerá no solo de los conocimientos jurídicos del constructor, sino también de su nivel de cultura y de su manejo del idioma nacional (es frecuente observar citas en latín, pero no lo es presenciar una conversación fluida en dicho idioma).

f. Establecida la argumentación, se debe realizar una construcción argumental oral, para los casos que sea necesario. Los buenos actores ensayan las obras antes de presentarse ante el público; los abogados eficientes, efectivos y eficaces deberían hacer lo mismo antes de presentarse en las audiencias orales.

El problema de la prueba

1. En muy escasas ocasiones, generalmente relacionadas con juicios ejecutivos o con aquellas situaciones que se resuelven por mecanismos de prueba tasada, puede ser suficiente con un grupo reducido o único de elementos probatorios.

2. En la generalidad de los casos, al atacar el punto 6. d. ii., del párrafo anterior, se requiere de la coordinación argumental de una serie determinada de elementos probatorios. La primera tarea del abogado litigante debe consistir en coordinar e integrar estos elementos probatorios en la estructura argumental antes descripta.

3. En el sentido de la Informática forense, los elementos probatorios interactúan en el siguiente esquema:

a. Prueba documental:

- Clásica (soporte papel):

i. Bibliográfica (texto), la controversia se resuelve mediante pericias documentológicas y/o caligráficas.

ii. Foliográfica (gráficos), la controversia se resuelve mediante pericias de expertos en la temática (arquitectos, ingenieros, agrimensores, etc.).

iii. Pictográfica (fotografía, cinematografía no digital), la controversia se resuelve mediante pericias de expertos en las distintas ramas involucradas (fotógrafos, cineastas, ingenieros electrónicos, electromecánicos, mecánicos, etc.).

- Informática: Ídem anterior pero en soporte digital (magnético, óptico, etc.), la controversia se resuelve mediante pericias informático forenses (título de grado en Informática, especialización en Seguridad informática o Informática

forense).

b. Prueba de informes: Complementa y certifica a la prueba documental informática recolectada; generalmente, pero no de manera excluyente, se relaciona con proveedores de servicios (por ejemplo, ISP nacionales o extranjeros).

c. Prueba de peritos: En la mayoría de los casos se debe emplear en subsidio, ya que dependerá de la aceptación o no por la contraparte, de la prueba documental informática recolectada y ofrecida en el litigio. La Informática forense es a la Informática, lo que la Medicina legal es a la Medicina. Debe ser realizada por expertos reales y no supuestos en la materia, de la misma forma que una autopsia la instrumenta un médico legista, en este caso es de rigor la participación de profesionales de la Informática, con título de grado y capacitación judicial y criminalística estricta (recordemos que no es lo mismo Informática que Computación o Sistemas de Información, y que nada tiene que ver con la Electrónica, de ahí que se la denomine: “Informática forense” y no Computación forense, Sistemática forense o Electrónica forense).

ANEXO 2
ESTRUCTURA DEMOSTRATIVA JUDICIAL

El problema de la redacción

Aunque debería resultar inconcebible que un profesional que ha pasado aproximadamente un lustro recorriendo los claustros universitarios, ignore las más elementales reglas ortográficas y gramaticales, la experiencia diaria nos enfrenta con demasiada frecuencia a textos que ignoran absolutamente dichos principios. Textos engorrosos, complejos, que aparentan erudición pero que solo intentan cubrir la falta de capacitación profesional o, lo que es peor, la ineptitud intelecto-cognitiva con palabras grandilocuentes, supuestamente técnicas y normalmente vacuas.

De ahí que un profesional que se precie debe tener en cuenta que al exponer los hechos, en realidad está construyendo el modelo teórico sobre el cual fundará su argumentación para convencer al juez acerca de la pertinencia fáctica y legal de su pretensión. En este sentido, dicha exposición debe seguir un estilo literario, normalmente se trata de una narración, en forma de relato unipersonal, el que describirá en primera instancia el sistema de referencias que constituye el soporte de dicho relato.

Un sistema de referencias, en nuestro caso, se compone de un marco referencial (descripción clara y detallada de las circunstancias espacio temporales, donde se desarrollaron los hechos a relatar). Este marco referencial debe contener:

1. La identificación del lugar o los lugares donde sucedieron los acontecimientos (estos lugares pueden ser reales o virtuales, en este último caso en general relacionados con descripciones de un lugar del hecho virtual propio).
2. La cronología de los hechos, mediante un detalle claro y específico sobre la o las fechas en que sucedieron.
3. La identificación y descripción exhaustiva de los protagonistas involucrados en ellos (personas de existencia real o ideal y también personajes de existencia virtual).

Sobre este marco referencial, se construye el relato, de esta manera habremos puesto en situación al lector y le será mucho más sencillo comprender la razón de ser de cada uno de los actos detallados. Aunque es muy raro de ver, esta descripción podría incluir gráficos que simplifiquen la comprensión de lo expuesto. No es necesario ser un perito, ni un experto para

realizar un cursograma sencillo o graficar una situación; un gráfico no es otra cosa que un documento que pretende ayudar y conducir al observador en este caso a través de la trama detallada.

Sintetizando, podemos decir que primero se describe el lugar y la época, y luego el relato cronológico de los hechos, mediante una narración descriptiva, en forma de relato circunstanciado.

Para que esta redacción se constituya en sustento de una posterior defensa oral ante un Tribunal, tal vez pueda ser de interés tener en cuenta algunos elementos que conforman las nuevas formas de comunicación virtual. Al respecto, podemos considerar una clasificación informal, pero muchas veces útil de los distintos estilos al enfrentar una situación de oralidad. No se trata de una clasificación metodológica y/o académica, sino de una visión resumida, desde la práctica, que nos permitirá utilizar una forma de expresión particular, acorde con el entorno (lugar, auditorio, rol que ocupamos) en que debamos exponer, teniendo en cuenta que si bien nuestro discurso se ofrece a todo el auditorio, su principal destinatario es el Tribunal; quienes deben ser convencidos son los jueces y, al igual que en las obras de la Edad Media donde relatores, juglares y bufones actuaban para toda la corte, pero lo que se buscaba era el beneplácito del rey, debemos ponernos en situación, si logramos convencer al juez (evaluador y destinatario del argumento presentado), habremos logrado brindar una defensa técnica eficiente, efectiva y eficaz a nuestro cliente; si no lo logramos, de nada valen las excusas y justificaciones: habremos fracasado. La siguiente clasificación puede resultar de interés para adoptar la actitud adecuada a cada circunstancia fáctica que se nos presente, ninguno de estos estilos es suficiente por sí mismo y deberá integrarse o utilizarse sucesiva y secuencialmente, según nuestras necesidades y planificación previa:

El estilo sobrio: El estilo sobrio rechaza todo tipo de recursos literarios, que sirven solo como ornamentación, y se limita a exponer los conceptos de forma directa y clara. Este estilo es muy frecuente en las obras de carácter didáctico. “El hombre es el único ser que consume sin producir. No da leche, no pone huevos, es demasiado débil para tirar del arado y su velocidad ni siquiera le permite atrapar conejos. Sin embargo, es dueño y señor de todos los animales. Los hace trabajar, les da el mínimo necesario para mantenerlos y lo demás se lo guarda para él” (Revolución en la granja, George Orwell).

El estilo sencillo: Similar al estilo sobrio, el sencillo busca la claridad ante que complicaciones. Admite los adornos y los elementos poéticos, pero rechaza las exageraciones y los recursos rebuscados.

El estilo nítido: El estilo nítido es el que se destaca por la corrección, la elegancia y la propiedad. Admite imágenes y figuras literarias siempre que no

dificulten la comprensión del mensaje.

El estilo elegante: El estilo elegante se caracteriza por otorgar colorido a la obra. Abunda en adornos literarios, figuras poéticas, armonía, etc., pero cuidando el equilibrio de los adornos poéticos. “Para todo trabajo. Para todo trabajo, Señor, fieros y competentes en puntear las reses y en talar quebrachales, repuntar en los montes la cerrazón del alba, regar las hortalizas secas en el verano, desbravar alazanes indomables, apagar la humareda del noroeste triste” (Elvio Romero).

El estilo florido: El estilo florido se caracteriza por el empleo recargado de las imágenes, metáforas y otros recursos poéticos para dar una impresión de vivacidad a la obra y hacerla atractiva, aunque la comprensión exija mayor esfuerzo por parte del receptor. “Silencio de cal y mirto. Malvas en las hierbas finas. La monja borda alhelíes sobre una tela pajiza.Vuelan en la araña gris, siete pájaros del prisma. La iglesia gruñe a lo lejos como un oso panza arriba” (Federico García Lorca).

El estilo pomposo: El estilo pomposo o ampuloso abunda en adornos poéticos al igual que el estilo florido, pero añade una entonación elevada a la expresión del pensamiento y rotundidad al período.

El estilo magnífico: El estilo magnífico se distingue por la sublimidad del pensamiento. Para lograr este efecto, recurre a las figuras poéticas y otros recursos literarios que dan elegancia y colorido a la expresión.

El estilo sublime: La excelencia de los pensamientos, la belleza de las imágenes y el buen empleo de los recursos literarios hacen que el estilo sublime tenga un poder extraordinario que arrebata al lector u oyente.

El estilo jocoso y humorista: El estilo jocoso utiliza los recursos literarios para otorgar un carácter cómico a las producciones. Su finalidad es hacer reír.

El estilo cortado: El nerviosismo es la nota característica del estilo cortado. Está elaborado con oraciones muy breves y no admite adornos ni rodeos innecesarios. Expresa el pensamiento en forma rápida y pasa de unos pensamientos a otros con rapidez.

El estilo vivo: Vivo, como su nombre dice, es el estilo que comunica vivacidad, animación y alegría. Es divertido y busca recrear al lector pero sin ser jocoso.

El estilo enérgico: La fuerza y el vigor de la expresión se destacan en el estilo enérgico. Cada oración y cada pensamiento parece que fuese una frase esculpida en una lápida y para la cual no se admitiría ninguna objeción.

El estilo vehemente: El estilo vehemente concede un predominio al impulso de la pasión e incluso de la violencia. Las palabras y las ideas reflejan ese impulso y se precipitan unas tras otras.

El estilo dramático: Al impulso y a la pasión del estilo vehemente, el dramático añade un concepto de oposición entre varias cosas para mantener una actitud de lucha que hace resaltar la idea central.

ANEXO 3
LA NOTIFICACIÓN

POr COrrEO ELECTrÓNICO (LEy 14.142, PCIA. DE Bs. As.)

La ley 14.142 de la provincia de Buenos Aires, promulgada por Decreto Nº 1065/10 del 8 de julio de 2010, fue publicada en el suplemento del Boletín Oficial 26.403, de fecha 26 de julio de 2010 y entrará en vigencia en el segundo trimestre del año 2011 (artículo 9º de la mencionada ley).

En síntesis y considerando, entre otros, los antecedentes implementados por la provincia de Mendoza*189* y la CABA*190*, realiza las siguientes modificaciones procesales normativas (ver cuadro comparativo al final del anexo):

1. Se sustituyen los artículos 40, 143, 144 y 148 del Código Procesal Civil y Comercial de la Provincia de Buenos Aires y se incorpora el artículo 143 bis.
2. Se modifica el artículo 16 de la Ley 11.653 de Procedimiento Judicial Laboral.
3. Los medios alternativos de notificación por cédula establecidos en la ley se hacen extensivos a los procesos iniciados en el marco de la Ley 24.522 de Concursos y Quiebras y a sus modificatorias.

El correo epistolar y el aviso de retorno

Los profesionales en general se acostumbran a las comodidades que les brinda desde hace tiempo el correo epistolar y en general las emplean de manera automática y sin reflexionar mucho sobre su naturaleza y utilidad. El correo es un servicio disponible, que se usa cuando es necesario y luego se olvida hasta la próxima correspondencia enviada o recibida.

Sin embargo, dentro de la precitada prestación, se pueden distinguir varios elementos esenciales que son necesarios considerar, discriminar y detallar:

1. Servicio de recepción, envío y distribución de correspondencia (cartas, paquetes, etc.) y mensajería (telegramas).
2. Servicios especiales con mecanismos de reducción de tiempos, protección de contenidos y distribución personalizada (carta documento, certificada, expreso, telegramas colacionados).
3. Servicios de identificación de destinatario y recipiente (aviso de retorno para cartas y telegramas).

La carta simple, la carta certificada y la carta expreso no son reconocidas en la legislación provincial como elementos de notificación válidos, aunque

puedan constituirse en elementos probatorios o indicios, acorde con su pertinencia respecto de los hechos controvertidos e investigados. Tampoco lo es el telegrama simple.

Sin embargo, la carta documento con aviso de entrega (el denominado "aviso de retorno") sí es aceptada como medio válido de notificación (artículo 143, inciso 4, del CPCCPBA).

Lo mismo ocurre con el telegrama colacionado con copia certificada y aviso de entrega (ídem, inciso 3).

El correo electrónico y el concepto de No Repudio

El denominado correo electrónico es una prestación digitalizada, con características similares al correo epistolar, descripto en el apartado anterior, pero con algunas características propias que son necesarias destacar:

1. En su forma más difundida, se comporta como un mecanismo de "carta simple". Se coloca un destinatario y se envía el mensaje, con o sin archivos adjuntos. La forma de comprobar su recepción por parte del destinatario depende de que este nos responda acusando recibo. Evidentemente, no puede ser empleado como medio de notificación judicial, ya que no cumple con los requisitos procesales de notificación vigentes.
2. No obstante, algunos prestadores de servicios ofrecen formas de comprobar la recepción del mensaje. En general, si el corresponsal que envía el correo lo solicita (validando una opción al enviar), el servicio le devuelve una confirmación de recepción y/o lectura al recibirlo. Sin embargo, esta opción puede ser perfectamente anulada por el receptor, ya que existen opciones que bloquean las respuestas de forma automática[191]. Este bloqueo puede ser parte del servicio (denegado por el prestador) o voluntario por parte del usuario. En ambos casos, inhabilita el sistema para validar y autenticar la recepción material objetiva del mensaje.
3. Por supuesto, si una entidad oficial ofrece un servicio de correo electrónico, puede disponer de todas las facilidades que pretenda suministrar a sus usuarios. Entre ellas: Prioridad: normal, alta y baja; Confirmación: de lectura, de entrega; Opciones: de firma, avisos de confidencialidad[192].

Sintetizando, podemos comparar el correo epistolar clásico con el correo electrónico y sus respectivos servicios, en el siguiente cuadro:

Cuadro comparativo	
Correo epistolar	Correo electrónico
Carta simple.	Mensaje de correo simple.
Carta certificada.	Confirmación de entrega al destinatario.
Carta documento.	Confirmación de lectura.

Carta expreso.	Prioridad: alta (normal o baja).
Documentos impresos (por ejemplo, copias).	Documentos digitales adjuntos (por ejemplo, copias digitalizadas).
Se puede adjuntar la prueba documental clásica (bibliográfica, foliográfica y/o pictográfica).	Se puede adjuntar la prueba documental clásica e incluir la prueba documental informática.
	Opción de firma electrónica (aceptada entre partes) o digital (certificada).
	Cifrado de datos (confidencialidad absoluta entre corresponsales).
	Opción para avisos de confidencialidad.
	Opciones de no repudio (identificación estricta de corresponsales).

Como restricción, el artículo 2º de la ley 14.142 establece que: "Los medios mencionados en los apartados 1), 3) y 4) no podrán utilizarse en los supuestos de notificaciones previstas en los apartados 1), 10) y 12) del artículo 135" [193]. Y asimismo autoriza: "El Juzgado o Tribunal deberá realizar de oficio, por medio de correo electrónico o por cédula, las notificaciones previstas en los apartados 3), 4) y 11) del artículo 135; la providencia que cita a audiencia preliminar y la que provee a la prueba ofrecida"[194].

La casilla profesional y la casilla personal

En la sociedad actual, los individuos generan múltiples perfiles, en distintos entornos virtuales (Facebook, Messenger, Youtube, etc.). Muchos de ellos contienen información auténtica, veraz y verificable, sin embargo, otros se llenan con información calificada, optimizada o simplemente fraudulenta, con los más variados fines (relacionarse, obtener amistades, aumentar el status quo social, estafar, defraudar, sustituir identidad, pescar víctimas para trata de personas, pornografía y prostitución infantil, etc.).

Esta visión particular del servicio de correo electrónico permite confirmar la inocuidad de las herramientas en cuanto a su sentido ético y legal. El instrumento en sí mismo no participa de los criterios deónticos de la sociedad que lo emplea. Por supuesto, puede generar enormes beneficios o resultar nocivo en múltiples aspectos.

En el mismo sentido, el abogado que ejerce la profesión en forma libre, actuando con y para su matrícula, pretende ser reconocido como tal. Su trabajo, su prosperidad, su bienestar familiar dependen de su perfil y de la aceptación que él tenga dentro de la comunidad jurídica en particular y de la

sociedad en general. Por dicha razón, se generan páginas web que representan al estudio y dentro de ellas se brinda el servicio de correo electrónico, que permite asociar al usuario con el precitado estudio de abogados, de manera directa, al leer la dirección de correo de quien envía el mensaje. Esto constituye un símbolo de pertenencia, de integración, en definitiva, de calidad y compromiso profesional. Sin embargo, puede ser perfectamente apócrifo y contener datos tan falsos como los perfiles de Facebook.

La casilla profesional como dato filiatorio

La sustitución del artículo 40 del CPCCPBA ha generado la constitución de una casilla de correo electrónico para la parte, consistente en una casilla de correo electrónico asignada oficialmente al letrado que lo asista.

En el caso particular de los operadores del Derecho, sería de especial interés que puedan contar con una casilla oficial, asociada a su nombre y datos personales, con el respaldo de una institución que certifique sus datos personales, en particular los respectivos colegios de abogados. En este sentido, la dirección de correo electrónico se constituiría en un auténtico dato filiatorio más, similar a la matrícula profesional. Aunque no toda persona tiene un número de matrícula, el tomo y el folio del abogado representan parte de su identidad y se encuentran profundamente consustanciados con su perfil profesional, de la misma forma que el cargo judicial que en determinado momento ocupa (sigue siendo “el abogado Sosa”, pero mientras ocupe el cargo será “el fiscal Sosa” y hasta simplemente “el fiscal”). Los roles dentro de la sociedad adquieren entidad propia e identifican en plenitud al individuo, al igual que el nombre y apellido o el DNI.

Esta oficialidad, requerida por la ley 14.142, en su artículo 3º, establece un correo oficial (que deberá ser reglamentado), que constituye una herramienta útil para el desempeño de las relaciones jurídicas, en el marco de un proceso judicial, con jurisdicción y competencia en la provincia de Buenos Aires. Es un avance enorme, pero limitado al espacio físico temporal antes citado.

Creemos que este servicio debería ser prestado por cada uno de los colegios de abogados que obran en el país, de esta manera se quitaría trabajo y esfuerzo a un sistema judicial ya sobrecargado de por sí. El colegio de abogados es la entidad que nuclea, reúne, integra, define e identifica a dichos profesionales. Es el responsable de su habilitación, por medio de la matrícula; es quien establece la idoneidad (al menos académica) de quien porta su respectiva credencial, marcando su pertenencia al mundo de los letrados.

Todos los colegios de abogados poseen su respectiva página web y brindan múltiples servicios a sus matriculados (cronogramas de actividades, calendarios judiciales, doctrina, jurisprudencia, legislación y muchos más). El

incluir, como parte de la matrícula, una casilla de correo electrónico propia para cada matriculado (incluida en la matrícula, de la misma forma que lo está la credencial que identifica al profesional) es una tarea sencilla, de bajo costo y que aportaría valor agregado y utilidad práctica al colegio de abogados en cuestión.

Una casilla de correo electrónico como parte integrante del proceso de matriculación, en cada colegio de abogados, permitiría ofrecer los siguientes servicios adicionales:

1. Control de identidad y autenticación: La dirección de correo electrónico aportada por el colegio de abogados se transforma en un dato filiatorio más del profesional que la posee y actúa como un auténtico domicilio electrónico a todos los fines judiciales pertinentes.

2. Servicio de firma electrónica: Es de destacar la diferencia entre la firma digital, con todos los requisitos establecidos por la ley 25.505, y el servicio de firma[195], que en nuestra legislación sería identificado con la firma electrónica. A diario ocurren millones de transacciones en todo el mundo, adquiriendo productos y pagando por ellos, utilizando medios digitales, muchos de ellos han sido firmados por medios digitales y son reconocidos como válidos por sus interlocutores. Este mismo principio se puede aplicar a una firma establecida mediante cualquier mecanismo universalmente reconocido, como por ejemplo el aplicativo PGP (Pretty Good Privacy), y la autoridad que certifica dicha firma puede perfectamente ser el mismo colegio de abogados. La validez de esta firma sería completa, mientras sea aceptada por sus usuarios (particulares y oficiales), aportando un nuevo elemento a la notificación digital y permitiendo deslindar responsabilidades, sea cual fuere el origen o el destino de la notificación, mientras recaiga en el referido entorno judicial de aceptación.

3. Servicio de cifrado digital de mensajes: De la misma forma que puede implementarlo cualquier estudio de abogados, respecto de sus integrantes y su clientela, el servicio de cifrado digital de mensajes es una utilidad que prácticamente viene asociada con la de firma digital. Esto permitiría asegurar la privacidad en los intercambios entre mensajes de profesionales, con sus clientes y con los restantes usuarios del sistema. Este mecanismo debería ser prioritario para proteger los derechos constitucionales involucrados en el intercambio de información por este medio o sus similares, en especial lo determinado en el artículo 18, ya que la correspondencia digital es en esencia asimilable a la correspondencia epistolar y debe gozar de la misma protección jurídica.

4. Servicio de No Repudio (aviso de recepción o de retorno): En este sentido, tiene ventajas sobre los métodos epistolares, ya que posibilita:

a. Establecer con precisión de décimas de segundo el momento en que fue recibido el mensaje en la casilla del destinatario.

b. Con la misma precisión establecer el momento de lectura efectiva del mensaje por parte del titular de la casilla.

c. Identificar el origen del mensaje, y en el caso de ser otro usuario del sistema (es decir, otra casilla facilitada por el mismo colegio de abogados, o por sus similares u otros organismos con los cuales haya establecido relaciones de confianza mutua[196]) establecer su identidad, procedencia, fecha y hora de envío.

En lo referido a la confiabilidad de los datos de la casilla de correo, esta contaría con el respaldo del respectivo colegio de abogados, el que de por sí ya extiende documentos confiables y aceptados a diario en la práctica judicial, como ser el Carné o Cédula Profesional, cuya validez ante los juzgados le otorga primacía sobre los documentos de identidad clásicos. En la práctica, el abogado que concurre por primera vez a un Tribunal, presenta su Carné o Cédula Profesional y no su DNI.

Respecto de los inconvenientes generados ante una posible sustitución de identidad, estos son subsanables mediante la implementación de los mecanismos de seguridad informática necesarios para evitarla. Si son posibles las transacciones interbancarias internacionales y sus hermanas menores, las compras y pagos mediante aplicativos de comercio electrónico, entonces son posibles las notificaciones seguras y por lo tanto confiables[197].

Los servicios disponibles y los servicios necesarios

La nueva ley promulgada en la provincia de Buenos Aires constituye un claro avance en procura de proveer una normativa que se aproxime a las nuevas necesidades y servicios que el desarrollo tecnológico nos aporta diariamente.

Al determinar el uso del mensaje de correo electrónico como herramienta de notificación, equivalente a la conocida cédula, nos aproxima al mundo real de la sociedad en que vivimos.

Los servicios que la ley exige, sin embargo, aparecen como una carga laboral y económica importante, dentro de un sistema judicial apabullado por sus necesidades insatisfechas (personal, tecnología, partidas presupuestarias, decisiones políticas). No obstante, si es aceptada y consensuada la participación de los colegios de abogados en la provisión del servicio de correo electrónico, dicha carga resultaría mucho menos onerosa para las distintas provincias que quisieran adherir al sistema y permitiría disponer de los mismos beneficios en todas las jurisdicciones participantes, con una mayor distribución de cargas y, por supuesto, con menor esfuerzo para el siempre limitado presupuesto público.

En este nuevo entorno teórico, sería posible incorporar paulatinamente más servicios: firma electrónica o digital, cifrado de mensajes, intercambio de documentos entre tribunales y funcionarios, sistemas de consulta on-line, métodos de apoyo a la decisión (soportados en inteligencia artificial e implementados mediante realidad virtual), en definitiva, todos aquellos elementos tecnológicos que una empresa de mediano porte pone a disposición de sus gerentes y, ¿quién no desea los mejores gerentes, para que decidan de forma eficiente, efectiva y eficaz sobre su libertad ambulatoria o su patrimonio? Los servicios están disponibles, solo es cuestión de integrarlos a los organismos pertinentes (como en su momento fueron integrados la imprenta, la máquina de escribir, el telégrafo, el teléfono, el teletipo, el fax y tantos otros).

En general, los cambios tecnológicos generan cambios sociales relacionados en el corto plazo, luego le siguen los litigios (siempre que existan relaciones humanas existen controversias, las que por suerte en nuestro sistema democrático se dirimen ante el sistema judicial vigente), a continuación actúa la jurisprudencia*198* y posteriormente la acción legislativa.

Es cierto que la actividad legislativa, por norma general, siempre reacciona a posteriori del desarrollo social y como respuesta a las situaciones de hecho que estimulan el cambio de reglas jurídicas (manteniendo el orden jurídico, pero modificando el sistema jurídico*199*). Es una constante carrera “desde atrás” y se ve muy distante la posibilidad de un “derecho preventivo”, que pueda anticiparse a los hechos altamente probables que el futuro nos depara. Especialmente por el riesgo de vulnerar garantías y derechos que esa acción “preventiva” pudiera generar. No obstante, una relación de aproximación progresiva, manteniendo siempre “a la vista” los cambios previsibles, hace que la tarea judicial y su aceptación social se mantengan reguladas por relaciones mutuas que aseguren un “lenguaje en común”. Por otra parte, la consulta del ciudadano a la información judicial es una necesidad creciente, que ya ha sido implementada y probada desde hace más de diez años en otros países (por ejemplo, España*200*) con excelentes resultados.

Por último, deseo agregar que sería de interés particular para los clientes de los distintos estudios de abogados el contar con un servicio similar ofrecido por dichos estudios. En efecto, la provisión de un servicio de correo electrónico entre los miembros del estudio y sus clientes, que permita el cifrado y la firma electrónica, constituiría una innovación que permitiría asegurar la confidencialidad de la relación abogado-patrocinado (o representado) y preservar el secreto profesional involucrado en ella, con el consiguiente ahorro procedimental y económico asociado ya descripto en este anexo.

Cuadro comparativo normativo	
Norma vigente	Norma modificada
Código Procesal Civil y Comercial de la Provincia de Buenos Aires	
Artículo 40: Domicilio. Toda persona que litigue por su propio derecho o en representación de tercero, deberá constituir domicilio legal dentro del perímetro de la ciudad que sea asiento del respectivo juzgado o tribunal. Ese requisito se cumplirá en el primer escrito que presente, o audiencia a que concurra, si es esta la primera diligencia en que interviene. En las mismas oportunidades deberá denunciarse el domicilio real de la persona representada. Se diligenciarán en el domicilio legal todas las notificaciones a domicilio que no deban serlo en el	Artículo 40: Domicilio. Toda persona que litigue por su propio derecho o en representación de tercero, deberá constituir domicilio dentro del perímetro de la ciudad que sea asiento del respectivo juzgado o tribunal, juntamente con una casilla de correo electrónico, que será la asignada oficialmente al letrado que lo asista, donde se le cursarán las notificaciones por cédula que no requieran soporte papel y la intervención del Oficial Notificador. Estos requisitos se cumplirán en el primer escrito que presente, o audiencia a que concurra, si es esta la primera diligencia en que interviene. En las mismas oportunidades deberá denunciarse el domicilio real de la persona representada. Se diligenciarán en el domicilio legal todas las notificaciones a domicilio que no deban serlo en el real.

real.	

Cuadro comparativo normativo	
Norma vigente	Norma modificada
Código Procesal Civil y Comercial de la Provincia de Buenos Aires	
Artículo 143: Notificación por telegrama. A solicitud de parte, podrá notificarse por telegrama colacionado o recomendado: 1°) La citación de testigos, peritos o intérpretes. 2°) Las audiencias de conciliación. 3°) La constitución, modificación o levantamiento de medidas precautorias.	Artículo 143: (Texto según ley 14.142) Medios de notificación: En el caso que este Código, en los procesos que regula, establezca la notificación por cédula, ella también podrá realizarse por los siguientes medios: 1. Correo electrónico oficial. 2. Acta Notarial. 3. Telegrama Colacionado con copia certificada y aviso de entrega. 4. Carta Documento con aviso de entrega. Se tendrá por cumplimentada la entrega de copias si se transcribe su contenido. En caso que ello resulte imposible o inconveniente las copias quedarán a disposición del notificado en el juzgado, lo que así se le hará saber. Se tomará como fecha de notificación el día de labrada el acta o entrega del telegrama o carta documento, salvo que hubiera quedado pendiente el retiro de copias, en cuyo caso se computará el día de nota inmediato posterior. Esta última fecha se tomará en cuenta en los supuestos que la notificación fuera por medio de correo electrónico, independientemente que se transcriba o no el contenido de las copias en traslado. Los medios mencionados en los apartados 1), 1. y 4) no podrán utilizarse en los supuestos de notificaciones previstas en los apartados 1), 10) y 12) del artículo 135. El Juzgado o Tribunal deberá realizar de oficio, por medio de correo electrónico o por cédula, las notificaciones previstas en los apartados 3), 2. y 11) del artículo 135; la providencia que cita a audiencia preliminar y la que provee a la prueba ofrecida.

	La elección de los medios enunciados en los apartados 2), 3) y 4) se realizará por los letrados, sin necesidad de manifestación alguna en las actuaciones. Los gastos que arrojen las notificaciones integrarán la condena en costas; con la salvedad de lo dispuesto en el artículo 77. Ante el fracaso de una diligencia de notificación no será necesaria la reiteración de la solicitud de libramiento de una nueva, la que incluso podrá ser intentada por otra vía.

Cuadro comparativo normativo	
Norma vigente	Norma modificada
Código Procesal Civil y Comercial de la Provincia de Buenos Aires	
	Artículo 143 bis: (Artículo incorporado por ley 14.142) Notificación por correo electrónico. El letrado patrocinante o apoderado de la parte que tenga interés en la notificación, el síndico, tutor o curador “ad litem”, en su caso, enviará las notificaciones utilizando el sistema de correo electrónico habilitado al efecto por el Poder Judicial, conforme determine la reglamentación. La oficina de notificaciones encargada de la base de datos del sistema de comunicaciones electrónicas del Poder Judicial emitirá avisos de fecha de emisión y de recepción a las casillas de correo electrónico de las partes y del Tribunal o Juzgado. El envío de un correo electrónico importará la notificación de la parte que lo emita.
Artículo 144: Contenido y emisión del telegrama. La notificación que se practique por telegrama, contendrá las enunciaciones esenciales de la cédula. El telegrama colacionado o recomendado se emitirá en doble ejemplar, uno de los cuales, bajo atestación, entregará el secretario para	Artículo 144: (Texto según ley 14.142) Régimen de la notificación por telegrama o carta documento. Cuando se notifique mediante telegrama certificado con aviso de recepción o carta documento, la fecha de notificación será la de la constancia de la entrega al destinatario. Quien suscriba la notificación deberá agregar a las actuaciones copia de la pieza impuesta y la constancia de entrega.

su envío y el otro, con su firma, se agregará al expediente. La fecha de notificación será la de la constancia de la entrega del telegrama. Los gastos de la notificación por telegrama colacionado no se incluirán en la condena en costas.	

Cuadro comparativo normativo	
Norma vigente	Norma modificada
Código Procesal Civil y Comercial de la Provincia de Buenos Aires	
Artículo 148: Notificación por radiodifusión. En todos los casos en que este Código autoriza la publicación de edictos a pedido del interesado, el juez podrá ordenar que aquellos se anuncien por radiodifusión. Las transmisiones se harán por una emisora oficial y por las que determine la reglamentación de superintendencia y su número coincidirá con el de las publicaciones que este Código prevé en cada caso con respecto a la notificación por edictos. La diligencia se acreditará agregando al expediente certificación emanada de la empresa radiodifusora, en la que constará el texto del anuncio, que deberá ser el mismo que el de los edictos, y los días y horas en que se difundió. La resolución se tendrá por notificada al día siguiente de la última transmisión radiofónica. Respecto de los gastos que irrogare esta forma de notificación, regirá lo dispuesto en el último párrafo del artículo 144.	Artículo 148: (Texto según ley 14.142) Notificación por radiodifusión o televisión. En todos los casos que este Código autoriza la publicación de edictos, a pedido del interesado, el juez o Tribunal podrá ordenar que aquéllos se anuncien por radiodifusión o televisión. Las transmisiones se harán en el modo y por el medio que autorice la reglamentación de la superintendencia, en horario de 8 a 20. La diligencia se acreditará agregando al expediente certificación emanada de la empresa radiodifusora o de televisión, en la que constará el texto del anuncio, que deberá ser el mismo que el de los edictos, y los días y horas en que se difundió. La resolución se tendrá por notificada al día siguiente de la última transmisión radiofónica o televisiva. Respecto de los gastos que irroga

	esta forma de notificación, regirá lo dispuesto en el anteúltimo párrafo del artículo 143.

Ley 11.653: Procedimiento judicial Laboral	
Norma vigente	Norma modificada
Notificaciones. Artículo 16. Las providencias quedarán notificadas por ministerio de la ley, los días martes y viernes o el siguiente hábil si alguno de ello no lo fuere, sin necesidad de nota, certificado u otra diligencia. Se notificarán personalmente o por cédula: a. El traslado de la demanda, de la reconvención y de sus contestaciones. b. La audiencia a que se refiere el artículo 29. c. La declaración de rebeldía. d. La citación al acto previsto en el artículo 25. e. La providencia que declare la cuestión de puro derecho y los traslados a que se refiere el artículo 32, último párrafo. f.) El auto de apertura y recepción de prueba, el de designación de la audiencia de vista de la causa, las cargas procesales que se impongan a las partes y, en su caso, los traslados para alegar por escrito. g. El traslado de los informes y dictámenes periciales, de los autos que ordenen intimaciones y medidas para mejor proveer. h. La sentencia definitiva, juntamente con la liquidación a que se refiere el artículo 48. a. La providencia de “autos” contemplada en el artículo 57, inciso b). b. La denegatoria de los recursos extraordinarios. c. Las que hacen saber medidas cautelares, o su modificación o levantamiento.	Notificaciones. Artículo 16. (Texto según ley 14.142) Las providencias quedarán notificadas por ministerio de la ley, los días martes y viernes o el siguiente hábil si alguno de ellos no lo fuere, sin necesidad de nota, certificado u otra diligencia. Se notificarán personalmente o por cédula: a. El traslado de la demanda, de la reconvención y de sus contestaciones. b. La audiencia a que se refiere el artículo 29. c. La declaración de rebeldía. d. La citación al acto previsto en el artículo 25. e. La providencia que declare la cuestión de puro derecho y los traslados a que se refiere el artículo 32, último párrafo. f.) El auto de apertura y recepción de prueba, el de designación de la audiencia de vista de la causa, las cargas procesales que se impongan a las partes y, en su caso, los traslados para alegar por escrito. g. El traslado de los informes y dictámenes periciales, de

d. Las resoluciones en los incidentes, las interlocutorias con carácter de definitivas y aquellas otras providencias que, en su caso, se indique expresamente. Cuando así se lo disponga por notificarse por carta documento, por telegrama o por acta notarial. Cuando la notificación de un traslado se efectuare mediante acta notarial, carta documento o telegrama, la parte podrá retirar las copias respectivas en el plazo no superior de cinco (5) días que se establezca, por sí misma, por apoderado o por persona simplemente autorizada por escrito, dejándose constancia de ello en los autos, con indicación de la fecha de la entrega y la identidad personal de quien las recibe. El término del traslado comenzará a partir del vencimiento del plazo fijado para el retiro de las copias.	los autos que ordenen intimaciones y medidas para mejor proveer. h. La sentencia definitiva, juntamente con la liquidación a que se refiere el artículo 48. a. La providencia de "autos" contemplada en el artículo 57 inciso b). b. La denegatoria de los recursos extraordinarios. c. Las que hacen saber medidas cautelares, o su modificación o levantamiento. d. Las resoluciones en los incidentes, las interlocutorias con carácter de definitivas y aquellas otras providencias que, en su caso, se indique expresamente. Cuando así se lo disponga podrá notificarse por carta documento, por telegrama, por acta notarial o por correo electrónico. Se tendrá por cumplimentada la entrega de copias si se transcribe su contenido. En caso que ello resulte imposible o inconveniente, las copias quedarán a disposición del notificado en el Tribunal, lo que así se la hará saber. Se tomará

	como fecha de notificación el día de labrada el acta o entrega del telegrama o carta documento, salvo que hubiera quedado pendiente el retiro de copias, en cuyo caso se computará el día de nota inmediato posterior. Esta última fecha se tomará en cuenta en los supuestos que la notificación fuera por medio electrónico, independientemente que se transcriba o no el contenido de las copias en traslado.

189 Ley 7855, modificación de la ley 2269, Código Procesal Civil, sustitución de domicilio legal, casilla de correo electrónico, notificaciones, firmas digitales electrónicas, mail, autoridades certificantes. Mendoza, 6 de mayo de 2008, B.O. 20/06/2008.

190 Resolución Nº 280/ 2009 del Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires, 4 de junio de 2009 (en relación con Resolución N° 832/05 del mismo organismo, sobre firma digital y de acuerdo a lo establecido en la resolución CM 870/06 sobre el uso del Sistema de Gestión JusCABA y del Plan Estratégico de la Dirección de Informática y Tecnología).

191 Este servicio que anula las respuestas tiene su razón de ser. De la misma forma en que se utilizan llamadas telefónicas automáticas –que en el mejor de los casos tienen por objeto realizar encuestas o promocionar bienes y servicios, y en el peor de ellos intentan comprobar los horarios de presencia en los inmuebles para luego concurrir y robar su contenido–, en los mecanismos digitales de comunicación existen riesgos similares (spam, chequeo automático de datos, hurto de información y el peor de todos "robo y sustitución de identidad"). Impedir las respuestas automáticas permite protegernos parcialmente de estos ataques. Esta es la razón de disponer dicha utilidad por parte de los proveedores del servicio (ISP Internet Service Provider), por lo que no resulta conveniente su eliminación, ya que responde a necesidades de seguridad de los usuarios que no pueden ser sustituidas por otros mecanismos.

192 La prioridad resulta de utilidad para los mensajes urgentes, la confirmación asegura la recepción en la casilla de destino del mensaje enviado y su lectura (devuelve fecha y hora de ambos eventos). La opción de firma permite *oficializar el envío, confirmando la relación que se establece entre el usuario y su identidad real (incluyendo cargo y función). Ejemplo:*

Prof. Ing. Luis Enrique Arellano González (Abogado Orientación en Derecho Penal) "Lauda Finem"

La opción de avisos de confidencialidad permite agregar un texto legal deslindando responsabilidad y/o exigiendo privacidad a la comunicación pretendida. Ejemplo:

193 *Artículo 135: "Notificación personal o por cédula. Solo serán notificadas personalmente o por cédula las siguientes resoluciones:*

1) La que dispone el traslado de la demanda, de la reconvención y de los documentos que se acompañen con sus contestaciones.

10) La que dispone la citación de personas extrañas al proceso.

12) Las sentencias definitivas y las interlocutorias con fuerza de tales, con excepción de las que resuelvan negligencias en la producción de la prueba".

194 *Artículo 135: "Notificación personal o por cédula. Solo serán notificadas personalmente o por cédula las siguientes resoluciones:*

3) La que declara la cuestión de puro derecho y la que ordena la apertura a prueba.

4) Las que se dictan entre el llamamiento para la sentencia y ésta.

11) Las que se dicten como consecuencia de un acto procesal realizado con anterioridad al plazo que la ley señala para su cumplimiento".

195 *En este sentido, es necesario destacar que la firma digital es el equivalente, con los requisitos de la referida ley; constituye a la Autoridad Certificante en un auténtico escribano digital, pero que no es la única, ni exclusiva opción posible. Desde el comienzo de Internet, el principal intercambio en la red fue pornográfico, no tengo interés alguno en realizar juicios deónticos al respecto, solo señalo una realidad comprobable por cualquier navegante, medianamente atento a su entorno. En este tipo de intercambio comercial, una serie de prestadores de servicio confirman las transacciones mediante mecanismos de firma digital y resultan plenamente confiables para los interlocutores que realizan la transferencia, basados en la confianza mutua (credibilidad en el certificante). Me pregunto: Si aquellos que intercambian pornografía pueden confiar en sus sistemas de certificación de firma,*

¿por qué los abogados no deberíamos confiar en la firma producida por un colegio de abogados (legítimo y legal), aunque no reúna los requisitos de la ley 25.505?

196 Estas relaciones de confianza se establecen mediante identificaciones y validaciones mutuas, que aseguran la misma fidelidad en los datos y las mismas condiciones de privacidad, entre los distintos organismos involucrados; deben ser abiertas, sinceras y deónticamente confiables entre las partes, para facilitar la integración de sistemas particulares en arquitecturas más complejas, las que perfectamente podrían alcanzar niveles nacionales o regionales, manteniendo la credibilidad y pertinencia de los servicios disponibles. No son raras en la sociedad civil, ya que constituyen la base de los mecanismos digitales de clearing bancario nacionales e internacionales, entre otros similares.

197 Considerando que ningún sistema físico o lógico es absolutamente seguro y fiable. La seguridad y sus

métodos de violación se encuentran enzarzados en una lucha eterna, similar a la que se desarrollaba entre el Presidente del Baltimore Gun-Club Impey Barbicane y el Capitán Nicholl, lo que no impide el uso de herramientas de protección de los activos informáticos, efectivas, eficientes y eficaces, que provean un marco de confiabilidad suficiente, a los efectos legales de la notificación.

198 *En el caso "Bunker Diseños S.A. c/IBM Argentina S.A. s/ordinario", la Cámara Comercial indicó que los correos electrónicos son "un principio de prueba por escrito", aunque no estén firmados digitalmente, considerando que: "no existe impedimento para que se ofrezcan como medio de prueba... Aunque por no estar firmados no alcancen la categoría de documento privado, es admisible su presentación en juicio para probar un contrato siempre que emanen del adversario, hagan verosímil el hecho litigioso y que las restantes pruebas examinadas a la luz de la sana crítica corroboren su autenticidad".*

199 En este sentido, y por razones de afinidad académica, adhiero a la visión que expresaran Carlos Alchourrón y Eugenio Bulygin, en su obra Introducción a la Metodología de las Ciencias Jurídicas y Sociales, editorial Astrea, Buenos Aires (5ta reimpresión, 2006), aunque reconozco que es solo una posición válida entre otras para analizar lógicamente el Derecho, pero tan controversial como cualquiera.

200 "MADRID.La puesta en marcha de un servicio de correo electrónico por parte del Ministerio de Justicia, hace poco más de un año, ha hecho que se duplique el número de consultas que los ciudadanos plantean al departamento que dirige la ministra Margarita Mariscal de Gante. En 1999, su Servicio de Comunicación Ciudadana atendió 4.331 peticiones, frente a las 2.781 recibidas en el 98, lo que supone un incremento del 55,5%. En 1996, ese servicio, entonces recién creado, recibió 2.397 consultas; al año siguiente, 2.852, y 2.781 en el 98. En noviembre del 98 comenzó a funcionar el correo electrónico y, según el Ministerio de Justicia, este ha sido uno de los principales motivos por los que se ha duplicado el número de ciudadanos que han solicitado algún tipo de información. De las 4.331 consultas recibidas y atendidas durante el año pasado, un 60% (2.619) llegaron por correo postal y el resto *(1.712) por correo electrónico. En la mayor parte de las consultas recibidas a través del correo electrónico se solicitaba información general y sobre asuntos jurisdiccionales (27,7%). Un 24,8% de los ciudadanos que se han dirigido al ministerio utilizaron ese medio informático para pedir datos sobre las ofertas de empleo en la Administración de Justicia. Otras consultas recibidas en Justicia a través del correo electrónico, durante el año pasado, se referían a nacionalidad, registros civiles, títulos nobiliarios e indultos (19,8%); jurisprudencia, acción legislativa y bases de datos (10,2%), y objeción de conciencia (6,9%). Otro 10,3% se sirvió de ese método para plantear sus opiniones al equipo de Mariscal".*

Fuente: Diario del Navegante, http://www.elmundo.es/navegante/2000/01/06/justicia.html, jueves 6 de enero de 2000.

ANEXO 4
UNIFORMAR LAS FORMAS Y FORMAR LOS UNIFORMES

La esperanza, el último mal de la Caja de Pandora

El peso del bronce

O'Gorman, Fentanes, Lago, Rosset, Albarracín, nombres que se acumulan y construyen la historia profesional de la Policía Federal Argentina. Tienen elementos en común –que comparten con otros modelos de dicha profesión como Vucetich y tantos otros– entre ellos la dedicación al servicio, las férreas convicciones personales, la insoslayable confianza en la ciencia, pero en particular una infinita curiosidad ante el fenómeno que demuestra la investigación del delito. Esta Criminalística en ciernes, se representa en el Gabinete Scopométrico (con sus instrumentos propios y característicos, como el Scopómetro y el fotocomparador sistema Belaunde), que luego evolucionará hasta estallar en múltiples especialidades (Medicina legal, Balística, Laboratorio químico, Documentología, Rastros, Dactiloscopía, etc.). Especialidades que se caracterizan por una forma estricta de constituirse, se construyen a partir de especialistas que, con o sin título universitario, dedican su vida a investigar el tema que los apasiona: así surgen, entre otros, Molera y Hayet. La historia sigue su curso y la Academia Superior de Estudios Policiales comienza a capacitar al personal de la Fuerza, los idóneos son absorbidos e integrados a los egresados con títulos terciarios o universitarios, la Criminalística se ha profesionalizado, ya no hay lugar para los aficionados.

Sin embargo, aparece la Informática y el consagrado y exitoso modelo anterior desaparece, hay que reaccionar ante el delito informático propio e impropio y no se cuenta con profesionales universitarios especializados en el tema. Hacen falta recursos edilicios, instrumentales, procedimentales y humanos. No hay tiempo para formarlos, se recurre a lo que está disponible en el momento.

Idoneidad: capacitación vs. aceleración

Resulta evidente que para exigir idoneidad, hay que establecer mecanismos de capacitación y evaluación que aseguren al interesado la posibilidad de acceder a dicha idoneidad. El Protomedicato a nivel Río de la Plata fue sucedido por una serie de instituciones que facilitaron la formación de médicos y su empleo por los organismos públicos y privados que brindan atención médica a la población. En Informática forense, no se ha producido un

efecto similar. Las razones de esa falencia son variadas, entre otras: la aceleración tecnológica, que nos invade a diario y que exige respuestas periciales a las preguntas judiciales, preguntas que normalmente resultan ambiguas, tanto para quien las formula, como para quien debería resolverlas. Mientras que un perito en Documentología ha sido formado académicamente en Derecho procesal y Criminalística, sus equivalentes informáticos no poseen ningún tipo de formación similar. En el mejor de los casos, y solo para aquellos que cuentan con un título de grado aproximadamente afín, han recibido cierto barniz de formación legal, normalmente orientado al desarrollo de su actividad profesional, pero que nada les aporte en lo que respecta a la inserción pericial de sus informes técnicos.

Por otra parte, la multiplicidad de títulos y niveles académicos aporta aún más elementos a esta confusión generalizada. Al igual que en las palabras de Discépolo, se mezclan profesionales con título de grado (ingenieros, licenciados), con título terciario (analistas de sistemas, programadores y similares), con título secundario (técnicos en informática egresados de colegios industriales) y otros sin relación alguna con la temática (electrónicos, contadores, administradores de empresa o simples voluntaristas) que ante la indefinición legal abarcativa, se integran al proceso en igualdad de condiciones de credibilidad a los efectos de brindar soporte al proceso judicial y su resultado esperado en la toma de decisión legalmente obligada (sentencia).

Aunque esto parezca un desquicio jurídico, resulta conveniente para muchos de los involucrados. El simple detalle expuesto en el apartado anterior y sumamente resumido nos lleva a la conclusión de que son muchos más los que carecen de soporte académico adecuado para realizar pericias informático forenses, que los que reúnen dichas condiciones. Como todos desean participar del proceso y muy pocos realizar el esfuerzo necesario para obtener la certificación académica correspondiente (título de grado en Informática y especialización en Informática forense), la opinión mayoritaria se inclina por la permanencia de este sistema absolutamente perverso para el apoyo judicial, para el aseguramiento del debido proceso y para los intereses de las partes. A río revuelto, ganancia de pescadores: Los colegios de profesionales están mayoritariamente integrados por profesionales que no se corresponden con el área informática (electrónicos, electro-mecánicos, etc.), por lo que tampoco tienen interés alguno en que se aclare el panorama, se definan las incumbencias y se actúe en consecuencia; algo que ya ha sido claramente definido para un médico legista, resulta impensable para un informático forense.

Es así que las Fuerzas de Seguridad, ante el requerimiento obligado, perentorio e ineludible de realizar pericias informático forenses, aunado al

peso histórico que su prestigio en Criminalística les aporta (Medicina legal, Balística, Documentología, Rastros, Laboratorio químico, Identificación personal, Fotografía pericial, Papiloscopía, Dactiloscopía, Pelmatoscopía y Palametoscopía) tantos resultados han aportado a la investigación judicial en nuestro país. Desde la historia los próceres de la disciplina observan y resguardan la imagen pericial de la institución. Esto deviene en dos hechos enormemente contradictorios: Ante la imposibilidad de disponer de personal capacitado, se recurre al que está disponible, sin pretender título académico afín alguno[201]. Como no se tiene muy claro cuál debe ser la inserción de la nueva área creada, se la hace depender del área de comunicaciones de la Fuerza, aislándola de hecho de su cadena de pertenencia natural: el área criminalística. Esto genera una inmediata pérdida procedimental, que se ve reflejada en las diferencias de presentación entre los informes periciales (formalmen-te estrictos y ya asegurados por decenas de años de interacción con el Poder Judicial) que son sustituidos por informes estructurados según el leal saber y entender de su autor que, como dijimos, no tiene formación pericial, legal, ni criminalística alguna.

A partir de esta situación absolutamente confusa, se hace entrega de un informe al Poder Judicial. El representante de turno de dicho Poder Judicial (tribunal interventor), lo recibe y le otorga la misma credibilidad que a una pericia médico legal, psiquiátrico legal, balística, caligráfica o documentológica. Y lo hace basado en su experiencia y confiabilidad referida a la institución que refrenda el informe, sin detenerse a reflexionar, ni cuestionarse la idoneidad de quien ha realizado la tarea. Acaba de recibir un informe realizado por un funcionario policial, sin título académico afín alguno, refrendado por un Jefe de Área, en idénticas condiciones, independientes de la estructura formal criminalística de la Fuerza y sin supervisión metodológica verificable. Esta credibilidad fundada en la institución y no en la idoneidad de sus profesionales resulta natural a la hora de analizar las otras áreas criminalísticas, no es necesario solicitar un informe para saber que el informe de necropsia lo firma un médico legista, o que el informe balístico lo firma un perito en balística o un licenciado en criminalística; sin embargo, debería ser imprescindible a la hora de aceptar un informe pericial informático forense y los operadores del Derecho que respaldan a las partes deberían exigirlo en forma perentoria, para asegurar la idoneidad de quien lo ha realizado y presentado como prueba ante el sistema jurídico, del que todos dependemos.

Informe estructurado vs. estructura informal

En el Manual de Informática Forense hemos incluido el formato estandarizado del informe pericial. Formato que permite su análisis comparativo desde diferentes disciplinas criminalísticas y su integración en la

toma de decisiones judiciales. Este formato (objeto de la pericia, elementos ofrecidos, operaciones realizadas, conclusiones) no responde a una actitud caprichosa de los autores, sino que ha sido construido, formado, convalidado y establecido de hecho por más de medio siglo de accionar pericial. Constituye una herramienta de análisis y presentación de conclusiones periciales, que aporta a los operadores del Derecho una herramienta de control, supervisión y sobre todo de interpretación multidisciplinaria, facilitando su tarea de inclusión de la prueba indiciaria en sus argumentaciones legales (un lenguaje transdisciplinario en común). De ahí la necesidad de mantener las formas para preservar el fondo jurídicamente pretendido. No es posible, ni necesario, aceptar modificaciones formales en aras de un supuesto cambio tecnológico, este cambio tecnológico genera por supuesto cambios metodológicos y procedimentales, pero nada implica respecto a la presentación ante el Tribunal de los resultados alcanzados. La única razón por la que no es utilizado por muchos de los supuestos expertos en Informática forense, reside en su falta de formación profesional criminalística y legal.

Las contradicciones evidentes

El Presidente del Tribunal Oral observa atentamente al perito, mientras este describe el arma que tiene en sus manos. Le pregunta: "¿Es apta para el disparo?". El perito responde: "Sería necesario probarla, efectuando un disparo". "Bueno –afirma el juez–, vayamos al fondo y hagámoslo". Nos resulta chocante y absurda la situación, ningún juez en sus cabales propondría semejante cosa[202]; sin embargo, es posible que ocurra la siguiente situación, sin que altere nuestra sensibilidad.

En el antes referido Tribunal Oral, se está juzgando a un comerciante por vender computadoras, con el sistema operativo de mayor difusión mundial, sin contar con la licencia correspondiente. A la vista del lego, el acto guarda todos los recaudos establecidos para asegurar el debido proceso judicial y arribar a la sentencia absolutoria o condenatoria que corresponda. Pero a la vista del experto, algunas circunstancias resultan al menos curiosas: La computadora en que se realiza el acta parece no tener ninguna de las etiquetas que certifican la instalación de programas con sus respectivas licencias. El presidente del Tribunal utiliza una computadora móvil (tablet, netbook o similar), en idénticas condiciones. Esta circunstancia se replica en todas y cada una de las máquinas del edificio y del Juzgado de Primera Instancia en que se realizó la instrucción del sumario.

Mientras el acusado escucha la acusación: Vender computadoras con un sistema operativo comercial instalado, sin contar con las licencias de uso correspondiente (un tema de software legal, con muchas más connotaciones comerciales que penales, pero tipificado en una ley penal), uno de los

secretarios del Tribunal escribe en el equipo portátil de su propiedad: ¿Cuenta este equipo con su correspondiente licencia?

Estamos ante un caso de "en casa de herrero, cuchillo de palo". Pensamos que no, estamos ante un hecho que visto desde el más puro y llano sentido común, configura al menos una hipocresía procesal: Se juzga al posible delincuente con herramientas informáticas tan apócrifas, ilegales e ilegítimas como las que fundamentan su procesamiento.

Curiosamente, no se plantea la ya consagrada teoría del fruto del árbol venenoso, tan venenoso que sin él no sería posible procesar al acusado. ¿Error de interpretación? ¿Excusación procedimental? ¿Disculpa por carencia de medios y presupuesto judicial-policial? ¿Usos y costumbres? ¿Caída en desuetudo? Cualquiera de estas excusas puede ser válida para satisfacer la consciencia del transgresor, pero al menos debería ser aplicada democráticamente: Si los funcionarios que procesan, juzgan y sentencian emplean en sus equipos de trabajo y en sus equipos personales software ilegal, ¿con qué entidad deóntica juzgan a los acusados por idéntico delito? Las circunstancias eximentes de culpa ante la comisión de un delito constituyen numerus clausus, y en nuestra formación profesional, no hemos podido hallar hasta el momento una que se adecue a la situación propuesta. "¿Haz lo que yo digo, pero no lo que yo hago?" *203*.

[201] Algunas Fuerzas de Seguridad recurren a supuestos idóneos, por simple conocimiento personal y sin título universitario alguno, lo que sería impensable en el Departamento de Medicina Legal, o a oficiales y suboficiales pertenecientes al escalafón pericial, por su simple pertenencia a este y sin haber realizado capacitación específica alguna. Como máximo han estudiado alguna materia de computación, referida a herramientas de oficina o a brindar soporte pericial (lugar del hecho virtual impropio), planimetría virtual, trayectorias, simulaciones, pero solo como soporte a las otras disciplinas involucradas y sin relación alguna con la problemática pericial informático forense).

[202] *Curiosamente, el hecho referido constituye una anécdota, ocurrida en un Tribunal Oral de una provincia argentina hace ya más de veinte años, en relación con una pericia balística de aptitud y funcionamiento de un revólver 7.5 suizo. Por suerte, gracias a la firme negativa de los restantes integrantes del Tribunal, la experiencia no se llevó a cabo.*

[203] *Derecho de propiedad intelectual: ¿Qué estamos pagando? ¿Es el precio de una idea? ¿Es una compensación por la tarea intelectual realizada? ¿Por qué le debo pagar a Mic... y no a los herederos de Pitágoras? ¿En base a qué razón se fija la duración de este derecho? Si soy dueño de mis ideas, entonces, ¿por qué pueden colgar un cuadro en un museo y no me pagan por cada mirada? ¿O por cada lectura de un artículo? ¿Se vende de contado o en cuotas?*

El hecho cierto de la comisión de un delito por muchos no le quita su calidad delictiva (a pesar de la experiencia diaria del artículo 247, segunda parte, y los supuestos "doctores", que nunca pasaron por un doctorado, ni siquiera con fines informativos); algunos aducen que si la norma es violada constantemente es porque ha caído en desuetudo, como el mencionado artículo según la mayoritaria opinión de los transgresores, que curiosamente pertenecen al Poder Judicial o interactúan con él. Al parecer, siendo el derecho un invento social sin sustento, ni fundamento alguno demostrable, todo vale. La pena de muerte era un elemento conforme a derecho (aún hoy lo es en muchos países), que cayó en desuetudo por falta de voluntarios. La indisolubilidad del matrimonio también. El voto universal, en fin, tantas cosas que en un momento son delictivas y en otro no.

El tema del aborto creo que sigue el mismo camino, aunque tenemos el problema de la reserva a la Convención Internacional de Derecho del Niño, que unida a la nueva legislación civil lleva a dicotomías bastante difíciles de integrar: un embrión en el interior de un frasco es evidentemente un niño, así lo establece la reserva referida "desde la concepción, hasta los 18 años"; nada dice del lugar de producción de dicha concepción (momento en que el espermatozoide y el óvulo se unen, para formar el huevo o cigoto, del que derivará el feto), sea dentro o fuera del seno materno, sigue siendo un niño. Esto elimina de cuajo el aborto, todos podemos entender que si se mata un niño es homicidio y no aborto (esté en una probeta, en el útero materno o fuera de él). Por otra parte, el Código Civil establece que se es persona desde la implantación en el útero materno. Ergo, tenemos niños en las probetas, que no son personas, pero que si son eliminados obligan al autor de dicha eliminación a responder por homicidio. Es claro que el Derecho vigente nos supera al menos intelectualmente.

Aunque casi todo derecho se hace en perjuicio del derecho de otros, el de la

propiedad intelectual tiene ribetes muy particulares. De por sí es discriminatorio, porque solo lo pueden percibir aquellos privilegiados que consiguen un buen CI, o una predisposición al arte, o alguna cosa parecida, que les permita crear y producir obras registrables o atribuibles a una determinada persona. Difícilmente se le pague a un discapacitado intelecto cognitivo, y entonces, ¿qué hizo de malo el discapacitado mental para no poder acceder a esta protección? Su situación es similar a la de quien nace en un entorno socio económico desfavorable, sin embargo este último goza de protección legal. Es un derecho tan elitista como cualquier otro similar. En palabras claras y sencillas, el derecho a la propiedad intelectual hay que respetarlo a ultranza en bien del autor, en cambio no ocurre lo mismo con el derecho a ser llamado doctor porque solo afecta (degrada, denigra) a los auténticos doctores académicamente titulados. No llegamos a discernir con claridad los fundamentos argumentales y legales de esta contradicción normativa.

Nos resulta imposible conciliar la dualidad implícita en llamar “contra legem” a toda modificación en las conductas sociales que resulte contraria a los propios intereses, y “desuetudo” a las que nos favorecen.

La compensación económica (tenga o no razón filosófica cierta de ser) desde antaño ha sido un premio a la labor humana. Esta labor puede ser de todo tipo, es indudable que quien corta leña tiene derecho a que compensen su trabajo, vendiendo el producto más caro que lo que le costaría al comprador si lo corta por sí mismo (Marx y su plusvalía tratan este y otros conceptos, con mucha más propiedad e inteligencia que yo). Podemos entonces hacerlo extensivo también a la creatividad (aunque esta creatividad sirva únicamente para recrear la vista, ya que “no solo de pan vive el hombre” y como dijo MA: “Si no tienen pan que coman tortas”), de ahí que deberíamos reconsiderar nuestra opinión respecto de los tratantes de personas, ya que brindan un servicio insustituible y al parecer (al menos por su difusión universal) imprescindible. Claro: ¿Dónde termina ese derecho de recompensa por la labor realizada? Es evidente que gana mucho más un narcotraficante que una enfermera, aunque esta última tenga que lidiar con los problemas que indirectamente genera el primero.

¿Y el derecho de autor? Bueno, sería una compensación por haber construido una obra, ya sea reordenando ideas anteriores, reformulándolas, en fin, dándole otro sentido a lo ya conocido o contribuyendo a la tendencia humana a contemplar y extasiarse ante la belleza. Vade retro, ratio.

Lo realmente diferente en el derecho de autor es el alcance de la recompensa pretendida. El carpintero que construye la silla la vende y punto, no pretende alquiler por cada vez que alguien se sienta en ella. Lo mismo ocurre con los

bienes inmuebles, los muebles y los servicios. ¿Se imaginan una maestra que le cobre a su alumno, futuro contador, por cada vez que usa una fórmula que le enseñó? Podrán decirme: la maestra no ha creado la fórmula, pero entonces debo decir que el escritor tampoco ha creado las palabras, en el mejor de los casos se ha limitado a ordenarlas de una manera particular e ¿inédita?

Como decíamos, se paga una vez y punto; a otra cosa, hasta el daño moral y las compensaciones económicas asociadas (sustentadas por el Código Civil: el que daña debe pagar) también tienen un monto y finalizan (este monto puede ser abonado en cuotas, pero es cierto y limitado en el tiempo). El derecho de autor es una especie de alquiler vitalicio (inclusive puede trascender la vida del autor) sobre una cosa o idea (no solo el derecho de autor, la patente es algo similar). ¿Por qué este derecho goza de tal privilegio? Bueno, nos parece que simplemente porque conviene a algunos que tienen suficiente poder como para hacerlo cumplir. Pero esta es una condición filosófica básica del derecho, por lo que nada hemos aportado a la discusión planteada.

¿Por qué M no le paga derecho de autor al creador del Código Binario? O a los descendientes de Pascal, o de Descartes, o de Pitágoras. Bueno, simplemente porque es un derecho vitalicio, pero no eterno y en esto difiere de la propiedad como derecho real, que se trasmite de unos a otros pero no caduca mientras el elemento exista. Con la excepción de los pueblos originarios, que nacen con el pecado mortal irreversible, irrecurrible e insubsanable de ser originarios; la casa donde vivo seguro que se encuentra asentada en los predios de caza de algún cacique de la zona, “uno de esos valientes llenos de fama y de gloria y que no dejan memoria, porque nacieron aquí”. Esta última frase, ¿fue plagio?

¿Cuánto debería pagarle a Luis Domínguez, o sus deudos, por haberla usado? Claro que no debo pagar, porque son menos de mil palabras. Sería similar a que me usurpen la casa, pero solo una habitación (uso pero no abuso).

Si fuéramos absolutamente críticos y desconfiados, podríamos decir que el derecho de autor es nada más y nada menos que una forma de recuperar ganancias, con el esfuerzo de otros y a costa de la masa de usuarios.

En cuanto al plagio: ¿El autor ha generado nuevas ideas inéditas y espontáneas? ¿Se ha desarrollado a partir de un huevo interplanetario? ¿Su cultura proviene de Marte? ¿Sus conocimientos del éter? ¿O es una construcción particular generada a partir del desarrollo evolutivo humano? ¿Qué cosa puede atribuirse a sí mismo y que no sea producto de su propio desarrollo personal, basado en conocimientos adquiridos? Los conocimientos se transmiten culturalmente, por medio de la experiencia y la comunicación, pero fundamentalmente por la educación formal e informal y esto ¿no es acaso

plagiar lo creado por otros?

En fin, ¿por qué la propiedad de una cosa se transfiere al contado y por una suma determinada, mientras que el derecho de autor está siempre indeterminado, pero siempre vigente? Esa es la pregunta que brinda sustento a esta disquisición y que suponemos podrán respondernos los avezados operadores del Derecho que tienen mayor idoneidad para opinar al respecto.

Nos parece que la diferencia de opiniones no se basa en una controversia legal y/o tecnológica, sino más bien en el nivel de abstracción de ambos. En lo referente a la posibilidad de ser víctima de esta violación a los derechos de autor, subyace el criterio de propiedad, algo que ha sido impuesto por ciertos modelos políticos, a la fuerza y normalmente por el que más tiene sobre el que tiene la desgracia de nacer pobre (en todo sentido, no solo económico); el derecho de propiedad es un elemento más en la discusión filosófica (al parecer muchas comunidades lo consideran inútil; claro, son comunidades subdesarrolladas, no se pueden comparar con nuestra magnificencia intelectual). Bueno, aceptemos las cosas como son: el derecho de propiedad existe natural y normativamente y cuando garabateamos palabras, miles de veces escritas, y oraciones y textos en iguales condiciones, somos sus propietarios por una especie de derecho divino, no susceptible de reivindicación por venganza privada, pero… cuasi. Aunque en realidad cuando uno escribe un libro, normalmente copia más del noventa por ciento de lo que escribe. Esto parece exagerado pero no lo es, ya que una obra en general no es más que el reordenamiento no solo de letras, palabras y oraciones ya utilizadas con anterioridad por otros autores, sino la más pura recomposición de ideas precedentes con nuevas visiones (la relatividad está implícita en Newton y viceversa, aunque haya logrado cambiar el mundo, lo que fue evidente para habitantes de Hiroshima y Kagasaki en abril de 1945). De ahí que toda obra es en realidad un producto social. Basta con pedir al lector que exprese una palabra que sea pura creación propia, en la que no haya empleado términos existentes con otros sentidos o que no haya copiado del ambiente que lo rodea (nosotros no tenemos ninguna, salvo que aceptemos las voces guturales, ya predicadas por Esther Vilar, como ser “guglo, guglo, gorgorito” o “pintribólico”, sobre las cuales no estamos aún de acuerdo en su significado cabal).

Al parecer, el Derecho ha quedado tan atrás de la realidad social que ha perdido su razón de ser (si es que tiene alguna otra que no sea ejercitar el poder de quien lo posee y controla). Por supuesto, sin exagerar, si nos planteamos por qué los abogados cobran honorarios, suponiendo la ley conocida por todos, no deberían ser necesarios, pero esto suena más a error normativo que a realidad social. Esto último parece falaz, pero… un médico

ejerce la medicina, porque es una ciencia independiente, un ingeniero ídem, un veterinario, un bioquímico, etc., todos tratan sobre saberes ajenos a su propia profesión, investigados, desarrollados e instrumentados utilizando elementos externos a la voluntad del profesional que se beneficia de ellos. ¿Pasa lo mismo con el Derecho? Parece que no, la fuente de producción del Derecho es el legislador, por supuesto, con el auxilio del abogado, luego la ley es aplicada por abogados, impuesta por políticos (en su mayoría de igual profesión) e interpretada por otros del mismo rubro.

¿Se imaginan una medicina donde las reglas para curar al enfermo las puede crear e imponer el médico directamente, sin supervisión estatal alguna?

Cada vez nos convencemos más de que "en este mundo traidor, nada es verdad, ni mentira, todo es según el color del cristal con que se mira" (afirmación seguramente compartida por Nerón y su esmeralda). Es bueno ver el choque de las olas de la juventud, contra las rocas de la visión conservadora (aunque millones de granos de arena nos indiquen, sin lugar a dudas, cómo terminará la cosa).

Nos parece que, en el trasfondo de esta conversación se oculta un duendecillo que persigue a esta utopía no siempre bien intencionada que hemos dado en nominar "Derecho". Pero, aunque al igual que el demiurgo platónico, decide qué elementos hará circular por detrás de los observadores de sombras; su interés no es formar opinión, sino por el contrario deformarla en beneficio propio (esto indica que no es único, sino que va cambiando a medida que son sustituidos los distintos detentadores del poder).

Este duendecillo es narcisista, soberbio, terco, tozudo, obstinado e insoportablemente personalista, por lo que mantiene una férrea posición conservadora. Da la sensación de que el Derecho ha quedado suspendido en una etapa evolutiva apenas posterior a la Edad Media. Este desfasaje entre el Derecho y la realidad social es uno de los componentes principales del problema. De ahí que los administrados en la mayoría de los casos no entiendan el sentido de las leyes y mucho menos de las decisiones judiciales, por lo que deben recurrir a los medios de comunicación masiva que, en lugar de aclarar el problema, simplemente optan por ocultar al duendecillo, con el velo de sus intereses instantáneos y cambiantes.

Se puede apreciar claramente: Cuando Sócrates prefiere la muerte antes que el ostracismo y el destierro, está acatando las leyes de la ciudad, pero no porque fuera un masoquista (como al parecer somos hoy la mayoría de los ciudadanos), sino porque entendía la ley y el contexto de su significado y decidía voluntariamente cumplirla. Hoy la mayoría no entiende la ley (esto incluye a muchos operadores del Derecho, entre ellos los autores) y los pocos que parecen entenderla son los que la generan según sus intereses del

momento.

Desde que el hombre descubrió la posibilidad de iniciar y transportar el fuego hasta la agricultura, pasó más de un millón de años. Luego, solo algunos miles de años más tarde surgió la rueda y el desarrollo tecnológico comenzó a acelerarse. El desarrollo tecnológico no sigue un movimiento rectilíneo uniforme, ni siquiera uniformemente acelerado, es un impulso caótico y explosivo que estalla a nuestro alrededor (la mejor prueba es el abismo generacional pre y postdesarrollo informático, que ha provocado el fenómeno de incomunicación que nos rodea). Por eso, la sociedad, que a pesar de lo que pretendan los generadores de normas, se mueve según la tecnología y no según la conveniencia de legisladores y operadores del Derecho, ignora olímpicamente las viejas normas y se adapta al nuevo proceso de comunicación e integración, dejando de lado a los que no pueden (en general, por haber tenido la desgracia de nacer en un entorno económico social desfavorable) o no quieren (en general, por haber nacido necios) adaptarse al mundo que los rodea.

Hace unos veinte años, desde que se tenía una idea hasta que se la publicaba en una revista especializada, pasaban un par de años, y para que alguien la modificara, otro tanto. Hoy, se tiene la idea, se publica y antes del nuevo amanecer (cualquiera sea la hora en que la publiquemos, ya que siempre está amaneciendo en algún lugar del mundo y la red informática es ubicua), ya ha sido modificada, optimizada y transformada. ¿Qué hacen en respuesta los operadores y generadores de normas, para adecuar el Derecho a este cambio? No tengo idea, al parecer siguen discutiendo sobre la naturaleza jurídica del derecho de autor o sobre las teorías de la pena o sobre la posibilidad de acomodar adaptativamente la realidad a sus normas (léase, por ejemplo: culpa y dolo tradicionales, expandidos a culpa con representación o dolo eventual, algo que solo puede resolverse comprendiendo la intención del delincuente, y que solo puede lograr un tercero iluminado trascendentalmente, en general el juez, no por voluntad, sino por obligación de dictar sentencia, porque creemos que ni el mismo delincuente puede decidirlo y clasificarlo en uno de estos modelos).

Las posturas basadas en la igualdad y la hermandad entre los hombres son difíciles de sostener; de hecho, al mirar a nuestro alrededor solo comprobamos similitudes morfológicas relativas y una enorme diversidad biológica, filosófica, política y social (de hecho y de derecho). Al parecer, cada comunidad (sea lo que sea que esto represente), cada región, cada grupo humano tiene derecho a fijar su propio derecho. El Derecho es solo la imposición de normas, por parte de quien ejerce el poder (sea este grupo mayoritario o no). El Derecho no evoluciona, no podría hacerlo, porque siendo

un invento humano, depende únicamente de la voluntad (el deseo y el poder) del detentador del poder en el espacio/tiempo considerado (sea único o múltiple); lo que cambian son las normas, acorde con dicho detentador.

No estamos en presencia de derechos (que por otro lado no tendrían fundamento alguno, salvo en la voluntad de quien quiere imponerlos), sino de conveniencias particulares (en su mayoría económicas) y esto no es compatible con sustentabilidad normativa alguna (salvo la sustentabilidad de quien ejerce el poder).

Estas distintas posturas, en razón de la globalización en que nos encontramos inmersos, implica la necesidad de compatibilizar los intereses de criterios sociales absolutamente dispares. En el caso que nos ocupa, los intereses comerciales, propios y particulares de una gran empresa multinacional y las necesidades de nuestro pueblo.

Nos parece que el análisis del derecho de propiedad deviene en el fondo en un problema generacional, los viejos modos de pensar deben ser eliminados, en aras de una nueva forma de enfrentar la humana realidad. Creemos que este proceso puede sintetizarse en una frase: Pro bono publico, et pro domo sua: Ubi bene ibi patria, y esta patria no tiene fronteras, ni límites normativos, que no surjan del consenso del grupo humano considerado. Por suerte, y hasta que se descubra la forma de no morir, a los carcamanes cada vez nos queda menos carretel en el hilo y es posible (no sabemos si probable) que la siguiente generación pueda enfrentar estos dilemas con un poco más de claridad y menos de soberbia anquilosada.

ANEXO 5
CONTRADICCIONES JUDICIALES

Muchas veces, en nuestra calidad de peritos en Informática forense, somos convocados a participar de ciertos hechos que consideramos legítimos y legales, pero que ante la revisión del Derecho pueden resultar al menos confusos.

Cuando los operadores del Derecho necesitamos establecer si un delito corresponde al tipo de acción de instancia privada o de acción privada, recurrimos a los artículos 72 y 73 del Código Penal de la Nación Argentina; siendo este listado taxativo, enumerativo y mientras no se modifique la ley penal, numerus clausus, la tarea parece resultar sumamente sencilla. Sin embargo, lo que de derecho parece simple, suele resultar engorroso ante los hechos diarios.

Caso de estudio: Un joven (típico adolescente) se hace presente en un negocio de venta de computadoras. Solicita al vendedor un equipo y le pide que se lo entregue con el sistema operativo instalado (en particular, Windows). El vendedor le dice que debe entonces pagar la licencia de dicho sistema operativo, la que no está incluida en el precio de lista del equipo que solicita. El joven aduce que en realidad solo quiere que se lo instalen para probarlo, ya que luego él en su casa instalará el sistema operativo que más le convenga, que lo tendrá durante las 72 horas de prueba y luego pasará a otro programa similar, desinstalando el que le instale el vendedor. Se hace la compra en estas condiciones, el joven se retira. En la puerta, lo espera un escribano, que labra un acta y poco tiempo después el vendedor es citado en calidad de presunto autor de una violación a los derechos de autor establecidos en la ley 11.723, la que incluye en su artículo primero a los programas de computación.

Desde la Informática forense, la cantidad y calidad de estudios periciales que pueden realizarse en este caso es bastante extensa y no forma parte de estas reflexiones, sino de las previsiones establecidas en el Manual de Informática Forense de nuestra co-autoría. El problema que nos atrae reside en el ejercicio selectivo de la acción penal, por parte de un individuo, generalmente pero no de manera excluyente, en representación de una multinacional del norte y sus consecuencias doctrinarias para nuestro Derecho penal vigente.

Podríamos encuadrar la acción del joven (luego analizaremos la del escribano) en una de estas tres figuras: agente encubierto, agente provocador o partícipe primario en grado de instigador.

1. Suponiendo la calidad de agente encubierto, el cual está normalmente

respaldado por una ley y protegido por una institución[204], las leyes que nos protegen contra el narcoterrorismo en particular y una fuerza de seguridad con respaldo judicial, con seguridad. No es este el caso, no hay ley que establezca la figura y el joven no pertenece a fuerza de seguridad alguna; el joven es empleado de un estudio jurídico que posee cierto grado de representación de la multinacional referida, con amplia presencia comercial en nuestro país. Es evidente que no se trata de un agente encubierto: la respuesta, por lo tanto, es no.

2. En la supuesta calidad de agente provocador, podríamos tratar el ejemplo del funcionario que concurre a un negocio y se retira sin solicitar el cupón de pago (denominado vulgarmente tique de compra) y luego actúa denunciando al comerciante ante la AFIP. No tiene el respaldo de una norma jurídica de fondo, pero es empleado de un organismo oficial (la AFIP) y lo cubre una norma administrativa. Si dicha norma tiene o no el mismo nivel que una ley de fondo, aunque goce de ejecutividad de hecho, es un tema doctrinario a discutir en otro momento. Adoptando la posición de que esto no es real y una norma administrativa generada por un organismo nacional es inferior a una ley de fondo de la Nación (según la estructura piramidal de Kelsen), podemos decir que a este individuo lo ampara la institución pero no lo ampara una ley penal. Por lo tanto, creemos que como figura se le debe aplicar la de agente provocador. Tampoco es el accionar del joven que describimos en nuestro caso de estudio. Es decir, la respuesta también debería ser no.

3. Para la última figura, ¿el joven se encuentra protegido por alguna ley de fondo de la Nación? No. ¿Por algún organismo oficial? No. ¿Por alguna norma interna de algún organismo oficial? Tampoco. ¿El delito se hubiera cometido sin su participación como instigador? No. Por lo tanto, es un partícipe primario en grado de instigador.

4. En el mismo sentido, el escribano que participa y registra el evento, y el experto en Informática forense que lo acompaña están refrendando un acto ilegítimo e ilícito. Presencian un delito y están obligados a denunciarlo, pero no lo hacen, limitando su accionar a la certificación del hecho ocurrido y el material secuestrado. Pensamos que estamos ante un caso típico de incumplimiento de deberes de funcionario público.

Complementariamente, y recurriendo a lo dicho por Mario Daniel Montoya (Informantes y Técnicas de Investigación Encubiertas, Ed. Ad-Hoc, Buenos Aires, 2001, pág. 31), esta conducta encuadra en el aspecto criminológico del accionar subrepticio encubierto al menos en los siguientes supuestos: "...1) generando un mercado para la compra o venta de objetos, sustancias y servicios ilegales, así como el capital necesario para tales actos, 2) creando la idea del delito..., 3) propiciando una inducción..., 5) coaccionando o

intimidando a una persona que de otra forma no estaría predispuesta a cometer una ofensa, 6) generando oportunidades para que los agentes encubiertos o los informantes lleven a cabo acciones ilegales…, 9) utilizando el dinero de los contribuyentes para tentar a la población a cometer ilícitos en lugar de invertirlo en combatir delincuentes…"; sin embargo, no puede excusarse en (ibídem, pág. 42): "Es frecuente que se trate de justificar la conducta del agente provocador apelando al ámbito de la antijuridicidad ya sea en lo que respecta al consentimiento del ofendido, al cumplimiento del deber o al ejercicio legítimo de un derecho, oficio o cargo…"; no es necesario destacar que no se da ninguno de estos supuestos.

Si bien no es de aplicación en nuestro país, bastaría con aplicar el test objetivo de entrapment, de uso frecuente en el país del norte, para comprobar si el accionar del joven de nuestro ejemplo y su co-equiper, el escribano, se encuentra o no dentro de la ley. En obra antes citada, página 97, podemos leer: "Test objetivo. Se centra en la conducta policial e investiga si tal comportamiento induciría a una persona que normalmente evitaría cometer un crimen a ceder a la tentación de perpetrarlo. El test objetivo de entrapment fue presentado por Justice Roberts en su opinión concurrente en 'Sorrell' y fue más tarde vigorosamente apoyado por Frankfurter en 'Sherman'. Dicha teoría se basa en el rechazo de los métodos de investigación usados por los gobernantes para reunir evidencia contra el acusado. El test aludido ha sido aplicado por algunas cortes de primera instancia".

En nuestro caso, consiste simplemente en analizar si la trampa tendida al comerciante ha violado alguno de los siguientes aspectos del precitado test:

· Inducir a comprometerse en actividades ilegales, en particular, las tipificadas por el Derecho penal, iniciándolas, sugiriéndolas o instigándolas.

· Utilizar métodos irrazonables para forzar la comisión del delito (violación de derechos constitucionales, intrusiones excesivas y no ordenadas por la autoridad judicial, inexcusable comisión de crímenes por funcionarios públicos o evitar la denuncia de los ilícitos por parte de estos, inducción al crimen que efectuada a un ciudadano respetuoso de la ley –un pater familiae– lo llevaría a cometer o participar del acto ilegal propuesto).

· Mala fe (actuar solo para obtener la comisión del delito, sin un propósito posterior de evitarlo, omisión de procedimientos razonables por parte de los funcionarios públicos involucrados –como dar a conocer su calidad de tal, por parte del escribano en el momento de actuar, evidenciando mala fe y esperando afuera del comercio sin notificar este entrapment al futuro acusado–, evitar causar un daño sustancial innecesario o activar los mecanismos judiciales penales, con el solo objeto de obtener elementos de coerción para futuras acciones patrimoniales –civiles o comerciales–).

· Provocar daño sustancial (a una persona, en este caso el acusado) excesivo, no autorizado legalmente, no confirmado, supervisado ni controlado por la autoridad judicial correspondiente.

Es evidente que este test debería formar parte de los aspectos a considerar al momento de fundar cualquier sentencia referida al tema en estudio.

reflexión doctrinaria

Pensemos en la siguiente situación, también puramente especulativa e hipotética:

1. Jaime Lavandeira es acusado de infracción a la ley 11.723, mediante el método ya descripto.
2. Se realizan las correspondientes pericias, el fiscal acusa, no se resuelve por ningún medio abreviado y llega el momento de la audiencia oral en el correspondiente TOC.
3. S. Sa. ordena la presencia de los peritos, en una audiencia en común, para contrastar las opiniones divergentes, que surgen de los informes periciales del perito oficial y de la defensa. Se produce una situación incómoda, ya que ni el perito oficial, ni el perito por la parte querellante, poseen título en Informática alguno (uno de ellos posee título en Electrónica, pero no estamos ante "Electrónica forense", sino ante "Informática forense"); no obstante,

S. Sa. convalida la participación de estos "peritos", por no hallarse reglamentada la profesión[205], algo que no ocurriría, por supuesto, en caso de una pericia médico forense. Por extraño que parezca en la misma audiencia y discutiendo temas de Informática forense, puede verse actualmente a profesionales de distintas áreas (contadores, administradores de empresas, ingenieros industriales o electrónicos, analistas de sistemas, técnicos industriales, autodenominados idóneos, etc.), conformando una auténtica parafernalia de individuos, con formaciones de los más diversos niveles (desde ingenieros en informática con seis años de formación, hasta jóvenes provenientes de una escuela secundaria), lo que complica y degrada la discusión científica, tecnológica y técnica que debería servir de sustento y apoyo a la decisión de S. Sa. Algo equivalente a permitir la participación en una audiencia sobre Medicina forense (autopsia o necropsia) –para establecer la hora de muerte del occiso–, de médicos legistas, médicos de otras áreas, auxiliares de medicina varios, veterinarios, enfermeros, electricistas, ascensoristas, conductores de ambulancias y cualquier otro que desee acercarse y aportar su opinión al respecto; lo curioso es que todas estas opiniones tendrán el mismo valor frente a S. Sa., un auténtico "Protomedicato informático"[206].

4. En esta situación, y con esta meridiana claridad intelectual y cognoscitiva,

S. Sa. pregunta a los peritos: ¿De qué manera es posible establecer la existencia de una licencia comercial que habilite el empleo de un sistema operativo, en un equipo determinado? El perito de la querella lo explica y S. Sa. requiere mayor aclaración práctica. En ese momento, el perito de la defensa solicita permiso a S. Sa. para mostrarlo prácticamente en la máquina que emplea el secretario para llevar cuenta en Actas de lo ocurrido durante el debate. Autorizado, se aproxima y determina que dicha máquina no posee licencia alguna. Ante la situación, señala la notebook del fiscal, para mostrar lo mismo y con curiosidad descubre que ni siquiera posee las etiquetas que denotan la legalidad del software instalado en ella (por supuesto, lo mismo hubiera ocurrido con el resto de los equipos de computación obrantes en la sala, desde público y periodistas, hasta los miembros del honorable tribunal, solo que S. Sa. da por finalizado el acto y la audiencia prosigue, con resultado incierto).

¿Qué debería haber hecho S. Sa.? Es un funcionario público, nada más y nada menos que un juez de la Nación, ante la determinación indudable de la comisión de un delito de acción pública, por parte de varias personas de las presentes en la sala de audiencias. Evidentemente, debe hacer extraer testimonio y dar participación al Ministerio Fiscal, para que se investigue a todos y cada uno de los poseedores de las máquinas en clara transgresión con la ley 11.723. Hasta podría darse el caso de tener que incluirse en dicha lista, al comprobar que la tablet (computadora personal portátil, muy en uso en la actualidad) que emplea, aunque comprada legalmente y en un comercio de máximo prestigio nacional, tampoco tiene etiquetas de licencia, ni licencia legítima alguna.

¿Por qué no ocurre esto en la realidad? Simplemente porque en una actitud raramente hipócrita, quienes deben acusar sobre este tema no acusan y, por el contrario, quienes no deberían necesitar hacerlo, lo hacen utilizando medios propios de un estado policial y no de una democracia en pleno Estado de Derecho (instigar el delito, actuar como partícipes primarios involucrando en dicha figura a algunos escribanos que en forma dolosa o culposa participan de este accionar). Todos saben que la mayoría de las instituciones y organismos del país emplea computadoras con “software trucho”[207]; de hecho, la forma en que se introdujo la computación en la función pública fue por este método: La mayoría de los funcionarios de mediana edad actuales se relacionó con la entonces incipiente ofimática laboral a partir del uso habitual de un procesador de textos, llamado “profesional write”, coloquialmente “el PW”, del cual no creo haber visto jamás una licencia, aunque seguramente alguien escribió el código y tenía derecho a las correspondientes regalías. Nuestros organismos oficiales centralizados y descentralizados siguen actuando de igual

manera, en forma total o parcial, dándose situaciones de instituciones que poseen más de diez mil puestos de trabajo y menos de doscientas licencias legalmente adquiridas.

Es suficiente con entrar a una sala de computación de un centro de estudiantes, de alguna universidad que todos amamos, para notar que no tienen etiqueta ni licencia alguna. Por supuesto, sacarlas de funcionamiento implicaría que decenas de miles de nuestros jóvenes dejen de acceder a Internet y puedan consultar su situación como estudiantes, ya que dicha universidad solo admite la inscripción a materias por este método. Se trata de un caso tan paradójico como el de las fotocopias: el estudiante concurre a la fotocopiadora "oficial" para extraer copia de un libro del cual solo hay un par de ejemplares en el país y le dicen que no; entonces se mueve unos metros a su derecha y, en la otra fotocopiadora "semi-oficial", se lo hacen sin inconvenientes. Si hiciéramos una encuesta entre nuestros operadores del Derecho para ver qué proporción de libros utilizaron en sus años de facultad, respecto de igual material fotocopiado (vulgarmente llamado "separata", pero tan "ilegítimo" como las licencias de software que motivan estas disquisiciones), seguramente podríamos establecer un interesante, pero previsible, resultado a favor de la "separata". ¿Se encuentra en este caso en pugna el derecho de estudiar con el derecho de percibir regalías por derecho de autor? ¿Debería privilegiarse el primero sobre el segundo, en aras del crecimiento educativo nacional? ¿Algo similar deberíamos hacer con el uso de "licencias truchas", por parte de los funcionarios que administran la ley, a favor de mantener el orden institucional y el Estado de Derecho, permitiendo la labor judicial, en franca contraposición con el orden normativo de fondo? No estoy en condiciones de resolver estos temas, solo me resulta curioso que sean tan pocos los que "se dan cuenta" y menos aún los que intentan darles solución.

El problema subjetivo

Podríamos suponer que el problema anterior quedaría solucionado simplemente cambiando el modus operandi de quienes pretenden arrogarse la potestad de ejercer la acción penal pública, actuando como auténticos representantes de la ley, con el único respaldo legal de ser parte de un estudio de abogados determinado, que representa los intereses de una multinacional. Supongamos por un momento que el estudio de abogados evite contratar a un joven para que realice la tarea sistemática y reiterada de actuar como instigador del delito de violación de la propiedad intelectual, al concurrir sucesivamente a distintos locales de venta de computadoras con intenciones de adquirir una computadora con sus programas, pero sin las licencias respectivas y hacerlo no para su uso personal o el uso del estudio para el que

trabaja, sino únicamente para registrar el evento y efectuar la correspondiente denuncia al comerciante que fuera involucrado con esta acción positiva e instigadora.

Para evitar esta circunstancia, el estudio recurre a la solución aparentemente menos ilegítima de esperar a la salida de los comercios a los clientes que han adquirido equipos en las condiciones referidas (con programas de base –sistemas operativos– y/o aplicaciones –programas de ofimática– registrados comercialmente, pero instalados sin su correspondiente licencia) y los invita cordialmente a que muestren su adquisición. Supongamos que el cliente accede y este evento se certifica ante el ya referido escribano, continuando con los mecanismos de denuncia ya mencionados.

Aun en este caso, el procedimiento sería más que dudoso desde el punto de vista del resguardo del debido proceso, ya que el cliente que adquirió el equipo con pleno conocimiento sobre la falta de licencias, también actuó como partícipe primario, el delito nunca se habría producido, si él no hubiera concurrido libre y voluntariamente a adquirir un producto, que sabe ilegítimo e ilegal (artículo 45 del Código Penal). Frente a esta circunstancia, al ser invitado a sumarse a la denuncia pretendida por quienes lo interceptaron en la vía pública, sin ninguna potestad policial, ni orden judicial, en realidad ha sido obligado a declarar en su propia contra, sin haberle sido enunciados sus derechos en tiempo y forma. Ante esta manifestación "voluntaria", el tribunal solo podría actuar considerándolo partícipe primario e incluyéndolo entre los acusados.

La situación por supuesto no se asimila a las figuras de "agente encubierto", ni "agente provocador", ya que concurrió en pleno uso de su libertad, de manera dolosa, e instigó a la comisión de un delito de acción pública, lo que no puede ser ignorado por el juez, ni mucho menos por el fiscal que toma conocimiento de los hechos. Luego habría que recibirle declaración indagatoria, y en el supuesto caso de que aceptara declarar, estimar, determinar y establecer en decisión fundada si la declaración prestada "libremente" en el momento de salir del comercio y ser interceptado por los denunciantes y el escribano, sin que se le dieran a conocer sus derechos y posibles responsabilidades penales, es válida y pertinente para la investigación en curso.

La "vulnerabilidad" ante la copia ilegítima (e ilegal)

Si hacemos una revisión comparativa de la cantidad y variedad de software instalado mediante el uso de licencias apócrifas que se observa en el mercado, veremos que predominantemente se observa dicha circunstancia en los productos de una empresa en particular ("M") y especialmente en su sistema operativo ("W") y sus aplicaciones de ofimática ("O"). Pero "M" es una

multinacional que dispone de recursos económicos que superan ampliamente a más de la mitad de los productos brutos de los países que ocupan este planeta. ¿Debemos suponer, entonces, que proteger sus productos es una tarea demasiado difícil o demasiado onerosa? ¿Será posible que la fabricación de una licencia para utilizar al instalar un producto es una tarea tan

simple que, apenas lanzado el producto, ya está disponible en cientos de lugares de Internet? De no ser así, ¿quién pone a disposición de los usuarios estas licencias "truchas"? Licencias que por otro lado serán "truchas" pero funcionan a la perfección y al parecer "M" no se da cuenta de ello. Por otra parte, "M" no se preocupa demasiado por este fenómeno masivo y mundial.

No hay nada más sencillo que conseguir un número de licencia funcional para el último producto de "M", basta con ingresar a Internet, colocar el nombre del producto y la frase "descargar licencia gratis", para que curiosamente obtengamos el elemento buscado al momento. Si quien lo hace por curiosidad trata de hacer lo propio con un producto como "E" (la conocida aplicación de Informática forense), verá que no sucede lo mismo. De hecho, es muy difícil conseguir la aplicación y casi imposible una licencia "trucha" que funcione. Sin embargo, la empresa que produce y distribuye "E" es un pigmeo económico al lado del gigante norteño.

¿Cómo es posible que dicho gigante sea incapaz de proteger sus desarrollos informáticos de la copia ilegítima?

Otras instituciones de similar tamaño que "E", como bancos, financieras, negocios de venta por Internet ("A"), no tienen problemas para asegurar sus productos y validar a los clientes; si esto no fuera así, hace tiempo que habrían sido llevados a la quiebra. ¿Es que tienen personal más capacitado que "M"? ¿Será que "M" contrata personal de seguridad informática sin la aptitud necesaria para asegurar sus productos? En este mundo y momento, mientras se realizan intercambios multimillonarios basados en sistemas de cifrado y validación simples (firma digital, cifrado por clave pública, etc.), los que se usan a cada instante en el comercio interno e internacional (no es necesario señalar que también lo hacen los narcotraficantes, el terrorismo internacional, los tratantes de personas, etc.), parece ser que el único que no puede proteger sus productos es el gigante del norte. ¿Será alguna restricción intelecto-cognitiva que afecta al terreno donde se encuentran sus instalaciones (no puede ser genérica, porque los productos más eficientes, efectivos y eficaces de seguridad informática salen de la misma región geográfica).

Resumiendo: ¿De dónde salen las claves apócrifas que se utilizan para habilitar los productos de "M"? ¿Quién distribuye las copias necesarias para instalarlo? ¿Por qué no es posible asegurar el producto contra las copias ilegales y el desarrollo por terceros de números de licencia válidos? ¿Quién

tiene interés en que el producto se difunda y emplee masivamente (de manera ilegal o ilegítima)? ¿Por qué siempre los productos de “M” han sido los más fáciles de copiar y “hackear”? En Argentina existe un viejo dicho campero que da respuesta a estos interrogantes: “Del mismo cuero salen las lonjas”. Curiosamente, a partir de la situación imperante, el gigante hace ojos ciegos a todo lo que pasa y luego decide contra quién accionar judicialmente. Esta situación en mayor o menor medida se da en todo el mundo, solo que en general es un tema del Derecho comercial, los argentinos nos hemos encargado de que sea además un tema penal (la última ratio al servicio y voluntad de “M”).

Esto se hace evidente a diario, “M” no coloca barreras anticopia; por el contrario, tolera con beneplácito las múltiples páginas que ofrecen descargar el producto o sus licencias simuladas en forma gratuita. Esto le conviene a nivel comercial, la estrategia consiste en permitir que todos lo copien y lo usen y luego decidir a quien le exigen el pago. Ante todo, buscando a aquellos que tienen solvencia para hacerlo y no poseen poder para evitarlo. Entre los incobrables se encuentran nuestras instituciones y organismos de la APN que en general no tienen licencia alguna, pero es raro que SL se presente a la puerta de Tribunales, de un regimiento militar del departamento de policía o de la UBA, a exigir licencias. Esta capacidad para regular y distribuir la acción judicial podría aceptarse desde el punto de vista comercial y, con muchos recaudos, desde el punto de vista civil, pero ¿desde el punto de vista penal? La empresa se encarga de facilitar la copia de su producto, algo similar a lo que ocurriría si dejáramos una billetera, evidentemente repleta de dinero, en el portal de una casa, con la puerta abierta y a unos pocos centímetros de la vereda, sin

persona alguna que la vigile. Aunque es una de las empresas más poderosas del mundo, no gasta dinero en proteger su propiedad intelectual. ¿Es por error? No, es una estrategia comercial que implica: usen “W”, legal o no, legítimo o no –como decimos en Argentina, trucho o no– pero usen “W”, que luego yo me encargo de criminalizar a quien me conviene.

La acción penal en manos del Estado

Desde nuestra primera aproximación al estudio del Derecho, entre otros justificativos, en especial de la razón de ser del Derecho penal, se me explicó que se trataba de una solución de compromiso para evitar la resolución personal de los problemas delictivos, denominada generalmente venganza privada. Algunas películas, como Adiós Hermano Cruel, daban cabal cuenta de este problema medieval. La solución implicaba quitar de manos de los ciudadanos la potestad de cobrar venganza por el daño real o supuesto cometido, ya que además del claro injusto que esto implica, dado que la pena

la fija la víctima, también separaba a las personas, acorde con el poder que tenían para ejercer dicha acción reivindicatoria. Algunas sociedades, como la japonesa, crearon verdaderas instituciones al respecto, entre otras los ninjas. Pero en occidente optamos por el poder en manos del Estado, en el Estado con división de poderes, el poder de ejercer la acción penal en manos del Poder Judicial. Con las excepciones que ya indiqué al comienzo del artículo para los casos de instancia privada y acción privada.

Ahora estamos volviendo a la solución medieval: Quien decide ejercer o no la acción penal de un delito de acción pública es el económicamente damnificado; y a partir del propio impulso de este, al no colocar barrera alguna que defienda su producto de la copia ilegal. Él decide si actúa o no. No conforme con esta potestad, también decide sobre el blanco de la criminalización secundaria, al elegir entre unos y otros a ver a quién le conviene denunciar.

Nuestras instituciones y organismos carecen prácticamente de licencias en sus máquinas. Hasta es probable que la máquina que se emplea en la audiencia oral, donde se procesa al autor del delito, denunciado por el joven de nuestro caso de estudio, carezca de licencia de sistema operativo o de aplicativos. Incluso puede no tenerla la máquina forense donde se realiza la pericia, en el interior de una institución policial o judicial, o las máquinas de la oficina de al lado o la que transporta el funcionario bajo su brazo, cuando traslada los archivos de un lugar a otro (sea personal o institucional dicho equipo). Se recolecta la prueba, se la resguarda, se la traslada, se la analiza y se escribe el informe utilizando máquinas sin licencia o con licencia “trucha”. Luego, lo que es peor, se procesa al acusado y se labra la sentencia con máquinas en iguales condiciones. Hasta puede ocurrir que alguno de los miembros del tribunal asista a la audiencia con equipos personales en igualdad de condiciones, sean estos informáticos o de comunicaciones (en particular, celulares) o esté escuchando música descargada ilegalmente. En fin, al parecer la doctrina del fruto del árbol envenenado no funciona en este caso.

Pero, por sobre todo, se permite que la empresa designe una persona física (nuestro personaje hipotético y su escribano) o jurídica (software legal), para que en su representación ejerza la acción penal, sobre un ciudadano de nuestro país. Si esto no es colonialismo, ¿cómo debemos llamarlo? Si el caso fuera civil y comercial, lo único que ocurriría sería que las regalías se cobrarían y saldrían del país a pesar de los cerberos aduaneros. En realidad, nos afecta patrimonialmente y en forma colectiva a la sociedad. Sin embargo, si alguno de nuestros compatriotas crea un aplicativo y pretende cobrar las regalías en el país del norte, tendrá serias dificultades para lograrlo, es decir que también

nos afecta en forma individual.

Lo expuesto hasta aquí podríamos considerarlo como simplemente anecdótico, ya que solo implica intercambio de dinero y este nunca ha sido el fuerte del Derecho penal, más intere

sado al parecer en los asesinos seriales visibles (existencia de cadáveres) que en los invisibles (vaciamiento de empresas, desvío de fondos, lavado de dinero, etc.). Pero cuando se hace una denuncia penal, estamos hablando de penas restrictivas de la libertad ambulatoria de una persona (no existen las penas privativas de la libertad, ya que implicarían poner al individuo en un estado de coma profundo y me parece que dicha sanción no aparece en nuestra legislación vigente). Es decir, podemos enviar a una persona a la cárcel a cumplir una pena, por decisión exclusiva de una empresa que decidió criminalizarlo, no se sabe bien por qué oscuros deseos o con qué motivo.

Uno de estos motivos podría ser: El dar un ejemplo a los demás y exigir que paguen, constituyendo un leading case que actúe como argumento de persuasión sobre los demás, a los que deja inermes ante una auténtica acción extorsiva, donde el transgresor no recibe el mensaje “pague o lo demandamos y pagará más”, típico del Derecho civil y comercial, sino el mensaje “pague, aunque ningún otro pague, ni siquiera quien lo procesa, porque si no irá preso”. Creemos que lo injusto de la situación se hace evidente por sí mismo.

Como ciudadanos, podemos aceptar que la acción penal le haya sido cedida al Estado. No creemos haberla cedido nosotros, ya que nunca fuimos consultados al respecto, pero habiendo nacido en sociedad, entendemos que es uno de los precios que debemos pagar para gozar de los beneficios generales de la vida en sociedad y particulares del Estado democrático de Derecho. Lo que nos cuesta aceptar es que esa acción penal sea a su vez cedida por el Estado a una persona física o jurídica determinada o determinable, ya que esto en realidad implica volver la situación al estado que imperaba durante la Edad Media. ¿Quién puede acusar de falta de licencia? El que tiene el poder para hacerlo. ¿Y quién lo tiene? La empresa que genera el producto y no lo resguarda en forma alguna por sí misma o por sus representantes. ¿Qué tipo de orden jurídico y en qué sistema jurídico democrático sustenta estos hechos? ¿El sistema judicial que nos debe defender y proteger como ciudadanos no se da cuenta de lo que pasa? En fin, son preguntas para otros operadores del Derecho mucho más capacitados que nosotros, que no deberían hacerse los desentendidos porque hacerlo implica aceptar una modificación sustancial en nuestra forma de ejercer el Derecho penal, eliminando de cuajo el alcance efectivo de los artículos 72 y 73 del Código Penal.

En resumen, el empleo de los medios informáticos para recolectar prueba puede resultar atrapado en este tipo de situaciones caóticas desde el punto de

vista jurídico e indeterminables desde el punto de vista informático forense. La posición del perito en Informática forense puede resultar ambigua, ilegítima o ilegal.

[204] *Ley 24.424, modificatoria de la ley 23.737, Art. 6 – "Incorpórase como artículo 31 bis a la ley 23.737, el siguiente: Artículo 31 bis: Durante el curso de una investigación y a los efectos de comprobar la comisión de algún delito previsto en esta ley o en el artículo 866 del Código Aduanero, de impedir su consumación, de lograr la individualización o detención de los autores, partícipes o encubridores, o para obtener y asegurar los medios de prueba necesarios, el juez por resolución fundada podrá disponer, si las finalidades de la investigación no pudieran ser logradas de otro modo, que agentes de las fuerzas de seguridad en actividad, actuando en forma encubierta: a) Se introduzcan como integrantes de organizaciones delictivas que tengan entre sus fines la comisión de los delitos previstos en esta ley o en el artículo 866 del Código Aduanero, y b) Participen en la realización de alguno de los hechos previstos en esta ley o en el artículo 866 del Código Aduanero. La designación deberá consignar el nombre verdadero del agente y la falsa identidad con la que actuará en el caso, y será reservada fuera de las actuaciones y con la debida seguridad. La información que el agente encubierto vaya logrando, será puesta de inmediato en conocimiento del juez. La designación de un agente encubierto deberá mantenerse en estricto secreto. Cuando fuere absolutamente imprescindible aportar como prueba la información personal del agente encubierto, este declarará como testigo, sin perjuicio de adoptarse, en su caso, las medidas previstas en el artículo 31 quinquies".*

[205] *El juez utiliza la potestad que le otorga el artículo 254 del CPPN: "Calidad habilitante Los peritos deberán tener título de tales en la materia a que pertenezca el punto sobre el que han de expedirse y estar inscriptos en las listas formadas por el órgano judicial competente. Si no estuviere reglamentada la profesión, o no hubiere peritos diplomados o inscriptos, deberá designarse a persona de conocimiento o práctica reconocidos". Esta situación de hecho y de derecho coloca a la Informática forense en una situación similar a la de la Medicina en tiempos del Virreinato y respecto del denominado "Protomedicato". Existía una serie de profesionales de las más diversas especialidades (médicos, cirujanos, barberos, sangradores, curanderos, hechiceros, etc.) que competía por el ejercicio de la Medicina. Al comenzar a reglamentarse esta ciencia, se limitó la participación de los antes detallados y se comenzó a exigir el correspondiente título de grado, se incluyó a posteriori la necesidad de matriculación en el correspondiente Colegio Médico y se finalizó con ese ejemplo de probidad profesional y académica que constituye la Academia Nacional de Medicina. Un caso similar se produjo a mediados de los ochenta del siglo pasado con las carreras denominadas "perito en Documentología" y "perito en Documentoscopía", que surgieron en clara competencia con los ya existentes calígrafos públicos nacionales, para ocupar el rol de "perito calígrafo" ante los estrados judiciales de las distintas jurisdicciones y competencias. Se resolvió manteniendo la vigencia de los "idóneos" y exigiendo la formación profesional en un plazo determinado. En este caso, podría hacerse lo mismo, siendo quid pro quo la Informática forense a la Informática, lo que la Medicina legal a la Medicina, debería exigirse una formación de posgrado habilitante para aquellos informáticos con título de grado que deseen actuar como peritos en Informática forense ante los referidos fueros. Tanto la Medicina legal como la Informática forense pueden ser integradas dentro de las llamadas disciplinas criminalísticas y, por lo tanto, deberían soportar iguales requisitos: Título y matrícula de médico, cinco años de ejercicio de la profesión y diploma de médico legista (posgrado), para la Medicina, que equivalen a título y matrícula de Informática y diploma en Informática forense (posgrado en nivel de especialización). ¿Por qué no toman partido los colegios correspondientes? Porque en la mayoría de los casos integran profesionales de distintas áreas, mientras el colegio de abogados solo recibe abogados y procuradores, diferenciando con claridad sus incumbencias; el mismo juez que permite actuar simultáneamente a un ingeniero en Informática, junto con un administrador de empresas, sería tajante a la hora de excluir a un procurador que pretende asumir las funciones de un abogado. No se trata de una cuestión de "idoneidad", sea lo que fuere que esta palabra signifique en este caso en particular, ya que depende de la visión particular y la experiencia que quien opina tenga sobre la Informática, estoy seguro de que el mejor de los procuradores es más confiable como abogado que el peor de los abogados, pero esto no justifica ni autoriza a este a ejercer la abogacía, algo así opinaba mi madre respecto de los curanderos y los médicos, aunque a la postre siempre recurría al médico. Un mismo colegio de abogados reúne ingenieros en Electrónica, Telecomunicaciones,*

Informática, entre otras especialidades, pero con la especial característica de que la mayoría más absoluta la constituye la suma de los dos primeros, que prefieren actuar como "peritos en Informática", ya que son muy pocas las "pericias electrónicas o de telecomunicaciones", el interés en preservar la situación se demuestra claro y evidente en términos cartesianos. Dichos profesionales aducen que cuando ellos estudiaron no existían los títulos en Informática, sin embargo, dichos títulos ya llevan más de treinta años de vigencia en nuestros claustros universitarios, tiempo más que suficiente para satisfacer el interés formativo de aquellos que no están conformes con la profesión que abrazaron vocacionalmente (Electrónica, Telecomunicaciones, contador, administrador de empresas) y prefieren actuar como informáticos, lo que se logra simplemente cursando una carrera de grado informática en cualquier universidad pública o privada que posea dicha oferta educativa y que debería sin lugar a dudas exigir formación de posgrado para poder actuar como "perito en Informática forense". El auge de los delitos informáticos propios e impropios está llevando a la sociedad en general y al sistema judicial en particular a una interacción cada vez más frecuente con esta problemática. ¿Hasta cuándo nuestros legisladores escaparán al tema? Permitiendo esta mezcolanza insoportable de profesionales, supuestos profesionales e idóneos en un área pericial que resulta imprescindible para brindar soporte a la decisión judicial. Las relaciones comerciales internas, externas, transnacionales, regionales y mundiales se celebran a diario por medios informáticos, lo que conlleva el correspondiente riesgo delictivo. ¿Será necesario esperar tanto tiempo como con el Protomedicato para remediar la situación? La sociedad de principios del siglo XXI no puede permitirse este lujo, o será avasallada por la tecnología y sus usuarios criminales.

206 El Protomedicato era un cuerpo técnico encargado de vigilar el ejercicio del arte de curar, así como de ejercer una función docente y atender a la formación de profesionales. A partir de la segunda mitad del siglo XV, en España hubo un gran adelanto de la ciencia médica; se practicaron autopsias y disección de cadáveres, nuevos estudios e investigaciones de anatomía, terapéutica y cirugía. Los reyes crearon entonces un tribunal llamado "Protomedicato", encargado de vigilar el trabajo de los médicos y de perseguir a los que ejercían indebidamente la Medicina. En América también se crearon Protomedicatos, los de Lima y México datan del siglo XV. En Buenos Aires, había un representante del Protomedicato de Lima; pero cuando Juan José de Vértiz fue virrey del Río de la Plata, trató de crear un tribunal en Buenos Aires, independiente del de Lima, para mejorar el estado lamentable en que se hallaban los servicios médicos, hospitalarios, farmacéuticos, etc. Vértiz creó en forma provisoria el Protomedicato de Buenos Aires. Fue real protomédico el doctor Miguel O'Gorman. Una de sus primeras tareas fue tomar examen de competencia a los médicos que trabajaban dentro de su jurisdicción. Vigiló además los precios de los medicamentos y persiguió a los curanderos, también introdujo la vacuna contra la viruela y la obligación de denunciar enfermedades contagiosas como la lepra, la tuberculosis, etc. Los integrantes del Protomedicato fueron autorizados para organizar la enseñanza de la Medicina y de la Cirugía. Como secretario del Protomedicato se destacó el doctor Cosme Argerich, que reemplazó en la cátedra al doctor Miguel O'Gorman. Funcionó de manera precaria hasta 1798, año en el cual llegó la autorización Real para el Protomedicato, para organizar los estudios médicos; se creó, entonces, en 1801, la primera escuela de Medicina en la Argentina, que funcionó en la intersección de las actuales calles Perú y Alsina, en Buenos Aires, utilizando también las aulas del Colegio de los Jesuitas. El plan de estudios se basaba en el de la Universidad de Edimburgo. El primer protomédico fue Miguel O'Gorman (1749?-1819), de origen irlandés, que había estudiado en París y Reims y revalidado en Madrid, llegando al Río de la Plata en 1776. Dio los primeros cursos del Protomedicato en 1801. También estuvo a cargo de estos cursos Agustín Eusebio Fabre (1729-1820), quien enseñó Cirugía. Lo reemplazó, en 1802, un criollo hijo de un médico catalán, Cosme Mariano Argerich (1756-1820), que además fue secretario del Protomedicato, al suceder a O'Gorman en 1802. También contaba con un tribunal especial para castigar las faltas cometidas por los facultativos y perseguir a los curanderos. Tenía además una función financiera, pues fijaba aranceles para exámenes y visitas de boticas, regulaba multas, administraba y distribuía esos fondos entre sus miembros o los aplicaba a la finalidad que mejor le parecía. Los estudios de Medicina no lograron atraer interesados en la región del Plata. En la camada de 1804, hubo solo cuatro inscriptos; en las de 1807 y 1810, ninguno. En 1812, solo tenía tres estudiantes por graduarse, que practicaban en el ejército. Las aulas del Protomedicato se convirtieron en depósito de material para la guerra. Por otra parte, existía el problema de que muchos estudiantes no daban las últimas materias, pues de hacerlo, al recibirse, estaban obligados a prestar su ayuda en

las guerras de la independencia. En 1821, el Protomedicato fue reemplazado por un Instituto Médico. Al mismo tiempo se creó el Departamento de Medicina de la Universidad de Buenos Aires. Fuente: http://es.wikipedia.org/wiki/Protomedicato_del_R%C3%ADo_de_la_Plata.

207 Trucho: Palabra utilizada en el argot bonaerense para referirse a los elementos falsificados de todo tipo que pululan en las ferias y entre los vendedores ambulantes locales.

ANEXO 6
MODELOS

Modelo de oficio a ISP

OFICIO jUDICIAL

Ciudad Autónoma de Buenos Aires, 13 de junio de 2012

Al Sr. Presidente de Yahoo de Argentina SRL Av. C... Nº xxxx, xdo piso (CP 1428BUC) CABA S / D

Tengo el agrado de dirigirme a usted en los autos caratulados (carátula, Nº expediente) que tramitan por ante (tribunal de radicación de la causa), a cargo de (nombre y apellido del juez), por ante la Secretaría Nº ( ), a cargo de (nombre y apellido del secretario), sito en la calle (domicilio del tribunal de radicación), de esta ciudad, a fin de solicitarle quiera disponer lo necesario para que se proceda a determinar e informar si obran en sus registros de intercambio de mensajes por correo electrónico los que se han podido identificar con los siguientes datos de origen, destino, fecha y hora, obtenidos a partir de sus respectivos encabezados:

1. Received: from fun1079 ([190.246.181.3])

by mx.google.com with ESMTPS id v37sm60498yba.8.2010.10.08.07.52.19 (version=SSLv3 cipher=RC4-MD5);

Fri, 08 Oct 2010 07:53:14 -0700 (PDT)

From: “Daniela” <daniela@foodsland.com.ar> To: estudioconsultas@yahoo.com.ar

2. From: =?iso-8859-1?Q? Estudio_Jur=EDdico_Dres._Leonardi_&_Cabrera?= <estudiocon sultas@yahoo.com.ar>

To: “Daniela” <daniela@foodsland.com.ar>

References: <5B443EFDD1B44D5F96EBD848670F095D@foodsland.local> Subject: Re: pagos

Date: Fri, 8 Oct 2010 14:16:56 -0300

El auto que ordena la medida dice: (transcribir el proveído que ordena el objeto del presente oficio).

Se deja constancia de que se encuentra autorizado para correr con el diligenciamiento del presente oficio el/la Sr./Sra. (nombre y apellido de la persona autorizada a diligenciar el oficio) DNI (indicar tipo y número de documento de la persona autorizada).

Sin otro particular, saludo a Ud. muy Atte.

Modelo de ofrecimiento de prueba documental informática y pericial informático forense en subsidio

OFRECE PRUEBA:

Documental:

Bibliográfica (si la hubiere). Foliográfica (si la hubiere). Pictográfica (si la hubiere). Informática:

Acompaña prueba indiciaria informático forense: Agréguese a los presentes actuados la recolección de prueba documental informática, efectuada con autorización de mi cliente en el equipo portátil de su propiedad, por el ingeniero en informática Luis Enrique Arellano González (MP COPITEC: 5101), certificada por el escribano MLB, la que obra en un CD, en sobre cerrado y con su correspondiente firma electrónica, registrada por medio de un digesto matemático (hash) unívoco para preservar su identidad y asegurar la confiabilidad de esta, acompañada por la correspondiente acta de recolección, resguardo, certificación y cadena de custodia en (xxx) fojas y el correspondiente informe técnico de recolección, resguardo y preservación de prueba documental informática, realizado por el ingeniero Arellano González.

A efectos de resguardar la prueba documental informática recolectada, solicita se la reserve por la Secretaría del Tribunal, en las condiciones en que ha sido entregada, a los efectos periciales que pudieren corresponder y con el objeto de preservar su integridad probatoria y mantener la cadena de custodia que asegura la prueba acompañada. Esta medida es imprescindible en razón de la particular vulnerabilidad de la prueba documental informática a las acciones dolosas, culposas o accidentales que pudieran afectar su integridad y anular su validez y confiabilidad probatoria, requiriendo cuidados análogos a los establecidos en el artículo 139 del Código Procesal Civil y Comercial de la Nación.

En caso de requerimiento de la contraparte para obtener una copia de la prueba recolectada, se hace saber que no es necesario que esta sea retirada de la sede del juzgado depositario, en razón de la particular característica de este tipo de pruebas, denominada Principio de Identidad Atípico: “Un bit es idéntico a otro bit, por lo que la copia digital (bit a bit) de un archivo, genera un nuevo original indistinguible del primero”. Esta circunstancia implica que los resultados obtenidos a partir de cualquier tipo de tarea realizada sobre una copia digital son directamente aplicables a su original, por tratarse en realidad de dos originales idénticos. Lo antedicho permite:

1. Resguardar la prueba recolectada, por Secretaría, de manera permanente y

hasta finalizar los trámites procesales que requieran los autos en trámite judicial.

2. De ser requerido, entregar a la parte que lo solicite una copia digital de la misma a partir del siguiente procedimiento:

a. Apertura del envase contenedor (sobre sellado, lacrado y firmado en la escribanía antes detallada).

b. Procedimientos procesales de rigor:

i. Acta de apertura.

ii. Copia digital del CD contenido en el sobre.

iii. Identificación mediante marcador indeleble del nuevo original resultante del proceso de copia.

ANEXO 6
MODELOS

v. Entrega formal a la parte requirente.

vi. Ensobrado y cierre formal del CD accedido.

vii. Constancia en autos de las tareas realizadas.

viii. Constancia en la cadena de custodia.

3. Requerimientos a la contraparte para realizar la tarea del punto anterior: un CD virgen de solo lectura.

Pericial informático forense:

Desígnese perito único ingeniero en Informática, ante la eventual negativa por la contraparte de la documental informática acompañada, reservándose esta parte la redacción oportuna de los puntos de pericia a requerir acorde con el alcance y términos de dicha negativa.

ANEXO 7
LA YAPA

Hemos hecho nuestro mejor esfuerzo, seguro que no fue suficiente, pero es lo que podemos ofrecer a nuestros estudiantes y a todos los interesados en el tema; esperamos que les sea de utilidad y, como reflexión final, a los peritos les dejamos la siguiente propuesta:

1. Un perito no es un juez: pero debe opinar fundando sus opiniones en la sana crítica y en los elementos tasados (probados científica, tecnológica y técnicamente) y, sobre todo, descartando las libres convicciones.
2. Un perito no es un fiscal: pero debe tener en cuenta especialmente los errores procedimentales que confluyen en la imputación infundada.
3. Un perito no es un policía (o miembro de cualesquiera otras FFSS): pero debe mantener el compromiso y sentido del deber hacia la sociedad que este rol implica.
4. Un perito no es un investigador privado ni público: pero no puede ser un necio que sostiene sus ideas basado en sus propias, únicas e infundadas creencias.
5. Un perito no es un abogado (o cualquier otro operador del Derecho): pero debe preservar a ultranza el mandamiento constitucional del debido proceso.
6. Un perito no es un escribano: pero debe aportar a la certificación de la prueba los elementos técnicos necesarios (firma digital, hash, etc.).
7. Un perito es simplemente: “un testigo experto”, nada más y nada menos.

BIBLIOGRAFÍA

Además de la bibliografía que se detalla a continuación, propia de este volumen, se remite a la presentada en el Manual de Informática Forense, que brinda soporte referencial a esta obra.

· Altheide, Cory y Carvey Harlan, Digital Forensics with open source tools, Ed. ElsevierSyngress, EE.UU., 2011.

· Crowley, Paul y Kleiman, Dave, CD and DVD Forensics, Ed. Elsevier-Syngress, EE.UU., 2007.

· Arellano González, Luis Enrique y Darahuge, María Elena, Manual de Informática Forense, Ed. Errepar, Buenos Aires, 2011.

· Hoog, Andrew, Android Forensics, Investigation, Analysis and Mobile Security for Google Android, Ed. Elsevier-Syngress, EE.UU., 2011.

· Hoog, Andrew y Strzempka, Katie, iPhone and iOS Forensics. Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS devices, Ed. Elsevier-Syngress, EE.UU., 2011.

· Kubasiak, Ryan; Morrissey, Sean y Varsalone, Jesse, Mac OS X, iPod, an iPhone Forensic Analysis DVD Toolkit, Ed. Elsevier-Syngress, EE.UU., 2009.

· Morrissey, Sean, iOS Forensic Analysis, for iPhone, iPad and iPod Touch, Ed. Apress, EE.UU., 2010.

· Zdziarski, Jonathan, Phone Forensics: Recovering Evidence, Personal Data, and Corporate Assets, Ed. O'Reilly, EE.UU., 2008.

Índice