Informática Forense

Hernán Herrera - Sebastián Gómez

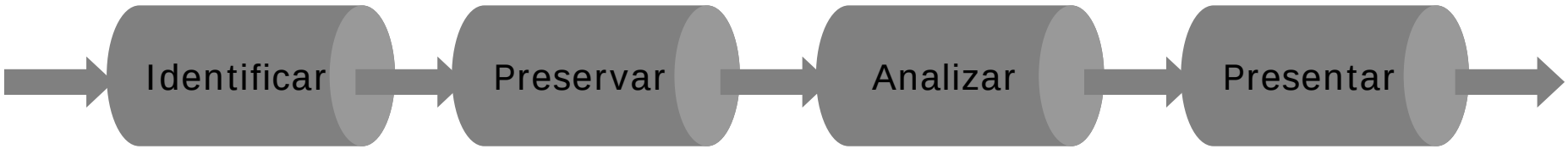
Jornadas de Seguridad Informática
Noviembre 2009

Contenidos

- Definición de informática forense
- Organización interna del Laboratorio
- Software forense
- Hardware forense
- El paradigma de la virtualización aplicado a la informática forense

Definición de informática forense

"Es el proceso de identificar, preservar, analizar y presentar evidencia digital, de manera que esta sea legalmente aceptable"



Identificación de la evidencia digital

En una investigación que involucra información en formato digital, se debe:

- ✓ Identificar las fuentes potenciales de evidencia digital
- ✓ Determinar qué elementos se pueden secuestrar y cuáles no
- ✓ Si se trata de un escenario complejo:
  - Tomar fotografías del entorno investigado
  - Documentar las diferentes configuraciones de los equipos, topologías de red y conexiones a Internet

Preservación de la evidencia digital

Al trabajar con evidencia digital deben extremarse los recaudos a fin de evitar la contaminación de la prueba, considerando su fragilidad y volatilidad

- ✓ Mantenimiento de la Cadena de Custodia
  - Registro de todas la operaciones que se realizan sobre la evidencia digital
  - Resguardo de los elementos secuestrados utilizando etiquetas de seguridad
- ✓ Preservación de los elementos secuestrados de las altas temperaturas, campos magnéticos y golpes
  - Los elementos de prueba originales deben ser conservados hasta la finalización del proceso judicial
- ✓ Obtención de imágenes forenses de los elementos secuestrados
  - Por cuestiones de tiempo y otros aspectos técnicos, esta tarea se realiza una vez que ha sido secuestrado el elemento probatorio original
  - En caso de que la creación de una imagen forense no sea posible, el acceso a los dispositivos originales se realiza mediante mecanismos de protección contra escritura
- ✓ Autenticación de la evidencia original
  - Generación de valores hash –MD5 o SHA-1- a partir de los datos contenidos en los diferentes dispositivos secuestrados

Análisis de la evidencia digital

Involucra aquellas tareas orientadas a localizar y extraer evidencia digital relevante para la investigación

Mediante la aplicación de diversas técnicas y herramientas forenses se intenta dar respuesta a los puntos de pericia solicitados

- ✓ El análisis de datos requiere un trabajo interdisciplinario entre el perito y el operador judicial –juez, fiscal- que lleve la causa

- ✓ Tareas que se llevan a cabo dependiendo del tipo de investigación
  - Búsqueda de palabras claves o documentos en todo el espacio de almacenamiento del dispositivo investigado
  - Determinar si ciertas aplicaciones fueron utilizadas por un determinado usuario
  - Determinar qué tipo de actividad tenía el usuario en la Web, análisis del historial de navegación, análisis de correo electrónico, etc

Presentación de la evidencia digital

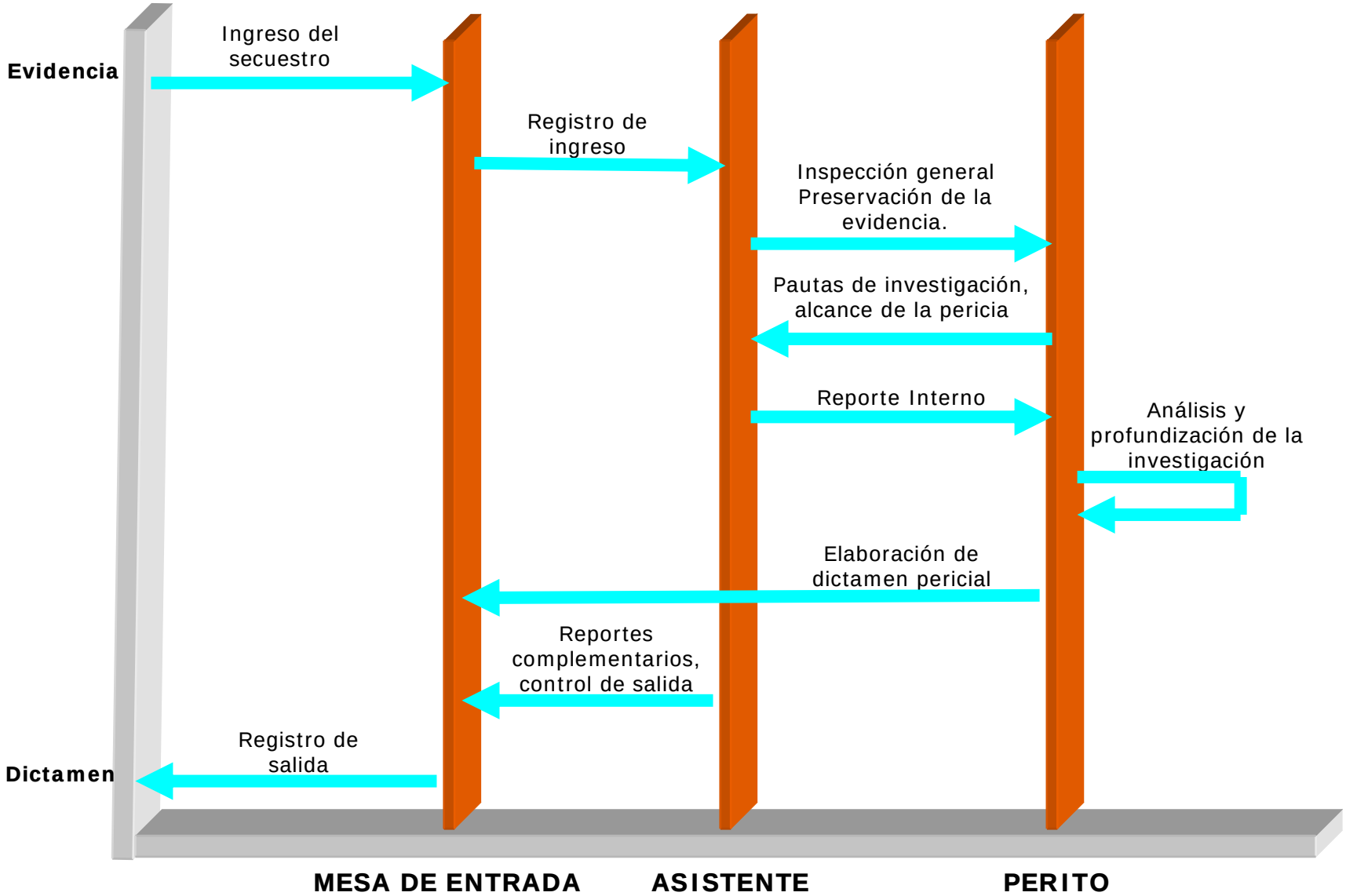
Consiste en la elaboración del dictamen pericial con los resultados obtenidos en las etapas anteriores

- ✓ La eficacia probatoria de los dictámenes informáticos radica fundamentalmente en la continuidad en el aseguramiento de la prueba desde el momento de su secuestro

- ✓ El dictamen debe ser objetivo y preciso, conteniendo suficientes elementos para repetir el proceso en caso de ser necesario (por ejemplo en un juicio oral)

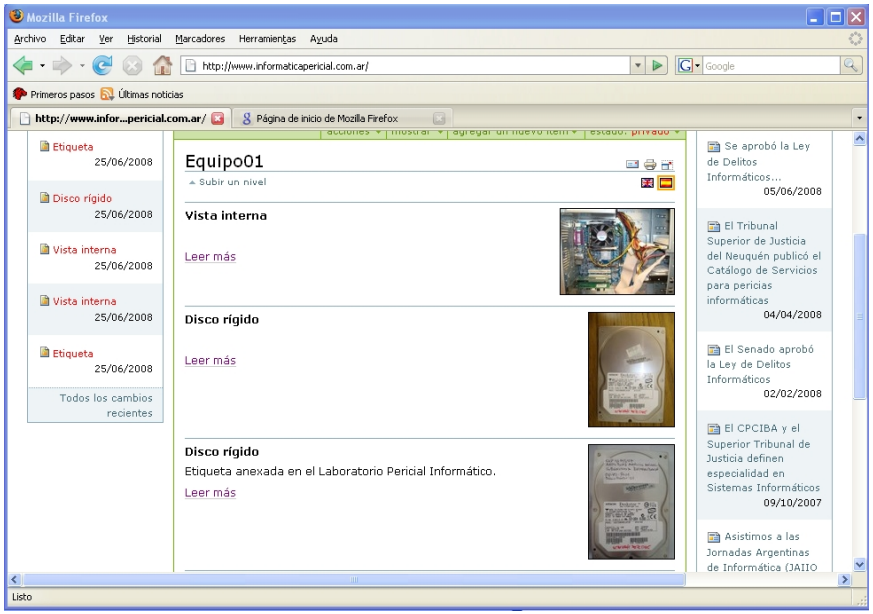
Organización interna del Laboratorio

Workflow del Laboratorio Pericial Informático

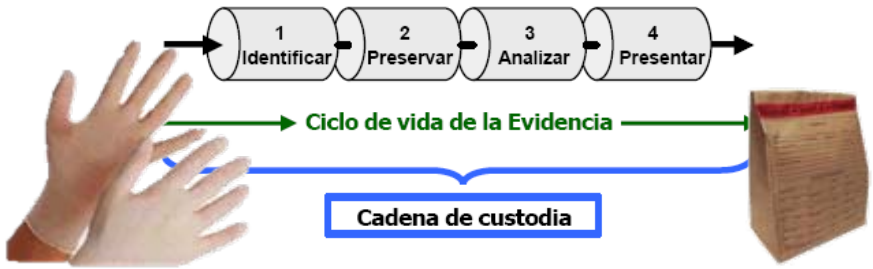


Ingreso del secuestro

- Registro de fotografías digitales en el CMS



- Verificación de la cadena de custodia

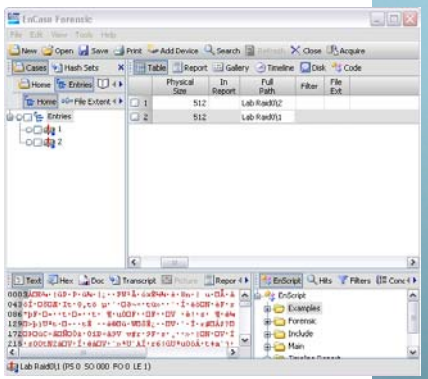


Preservación

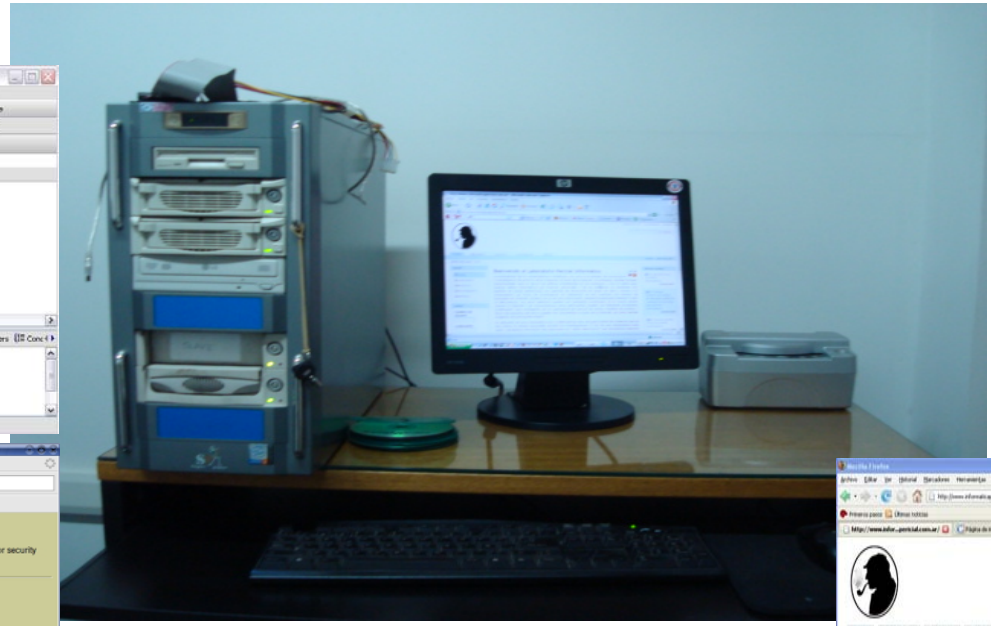
Equipos Informáticos

Telefonía Celular

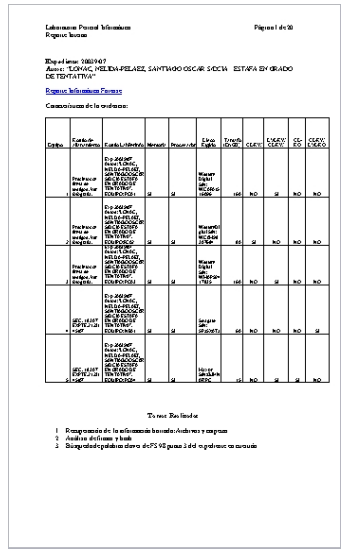
Análisis



Utilización de software forense



Puesto de trabajo forense



Confección de reporte interno

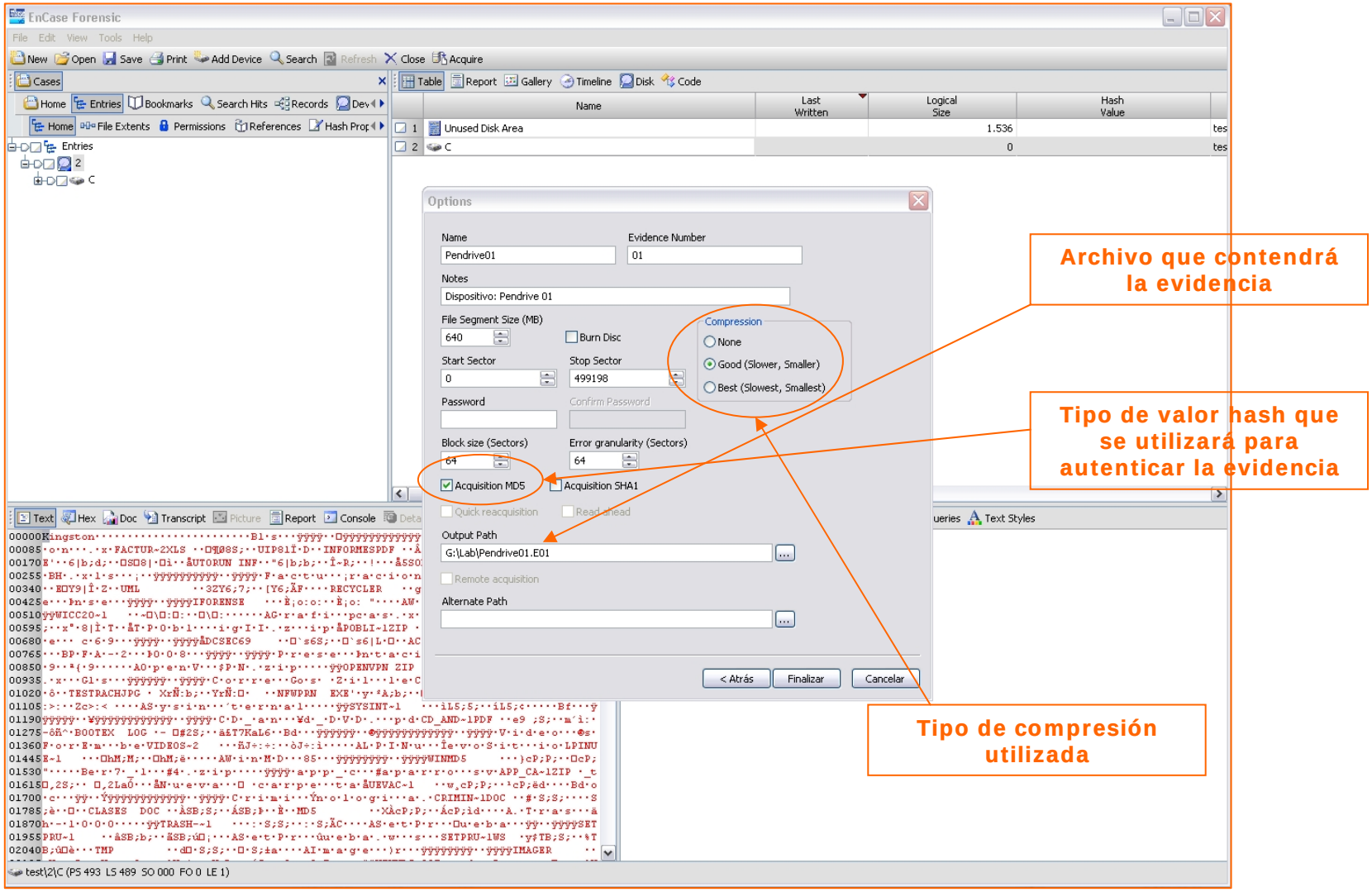
Registro de casuística en el CMS

Presentación y envío

Uso de etiquetas de seguridad → Evidencia Procesada → Registro fotográfico → Dictamen

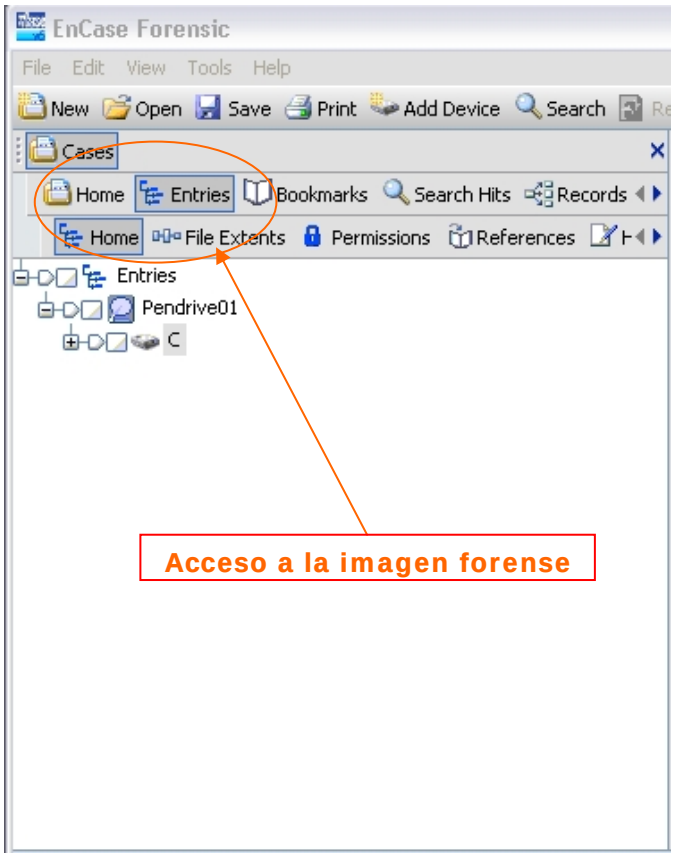
Software forense

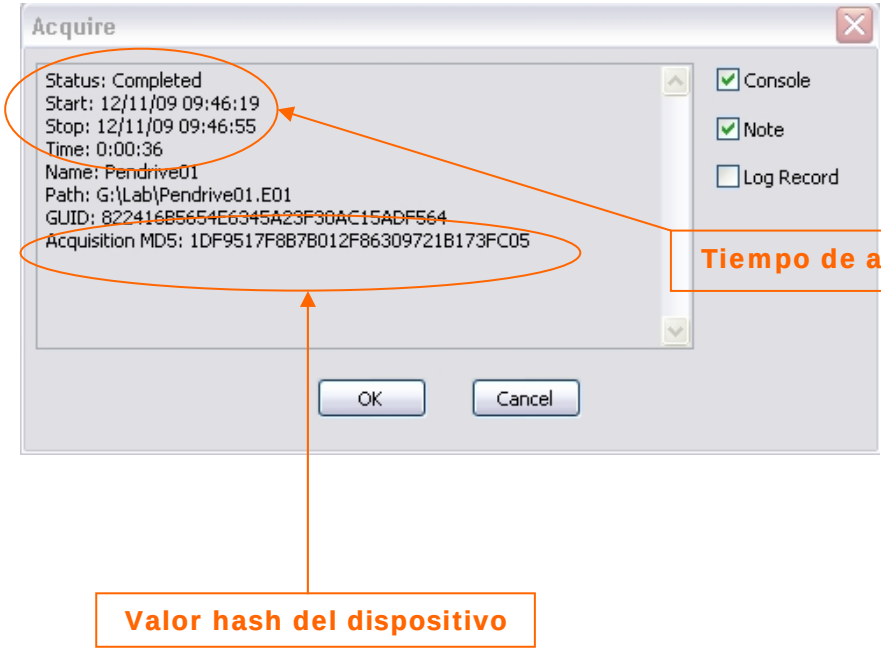
Generación de una imagen forense para practicar la pericia informática



Software forense

Generación de una imagen forense para practicar la pericia informática

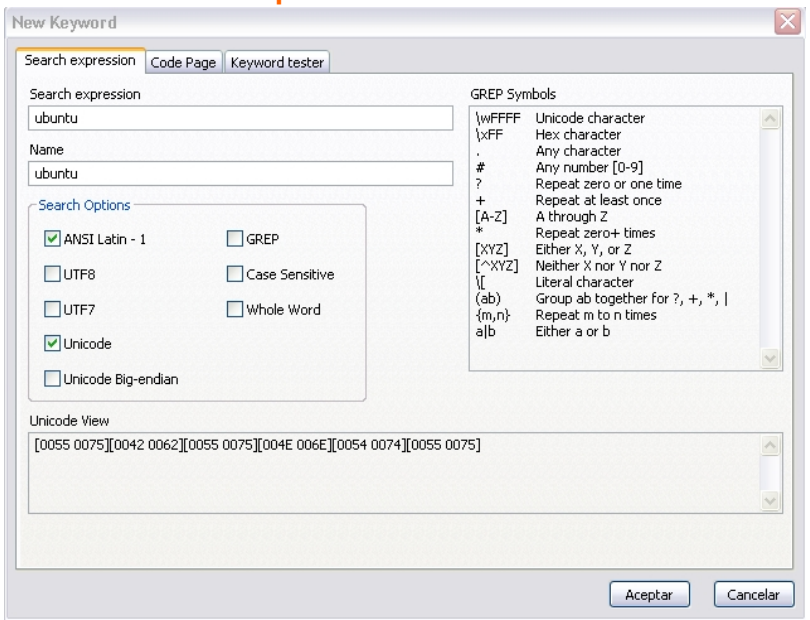




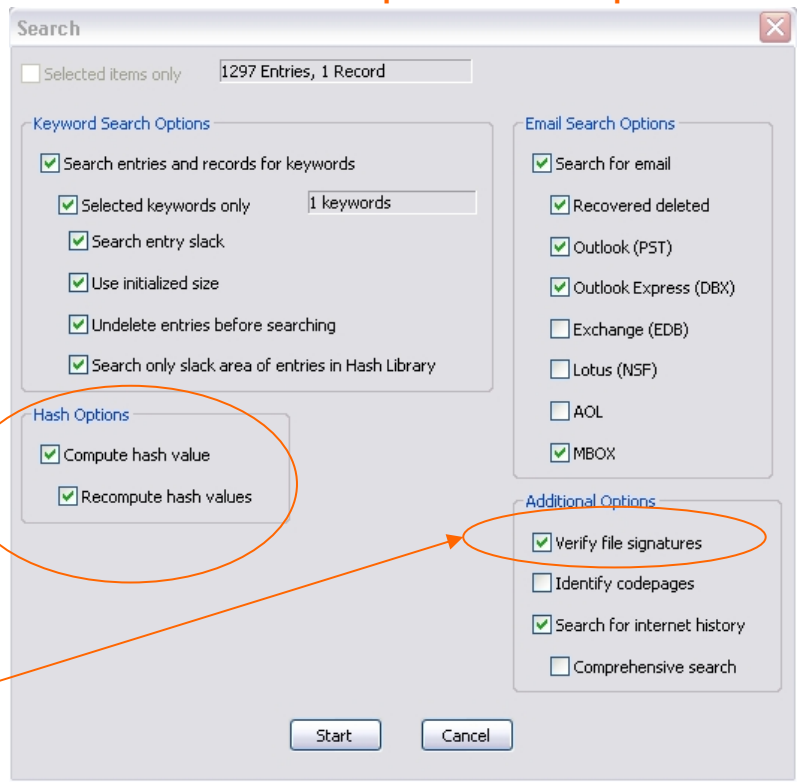
Software forense

Búsqueda de palabras claves

Paso 1: Definir la palabra clave



Paso 2: Determinar las opciones de búsqueda



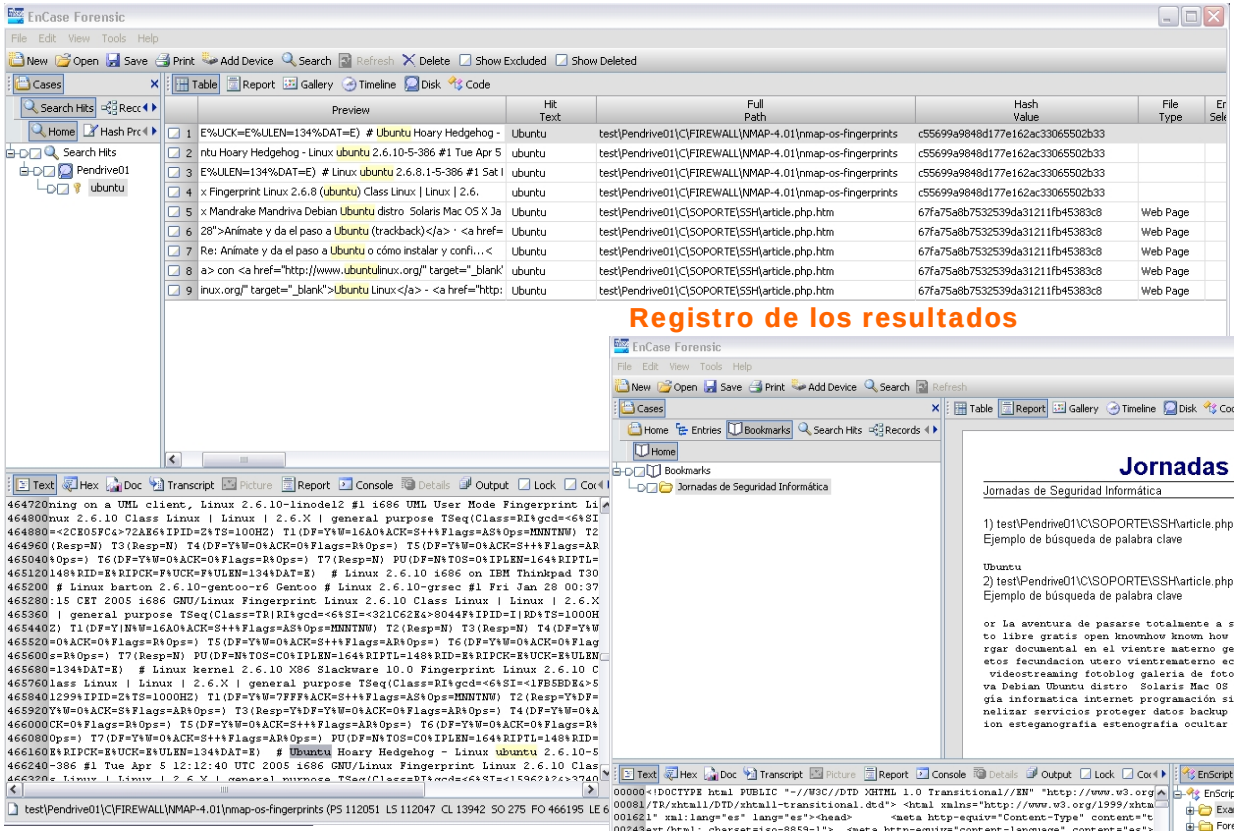
Análisis Hash Set
(National Software Reference Library)

Análisis de firmas

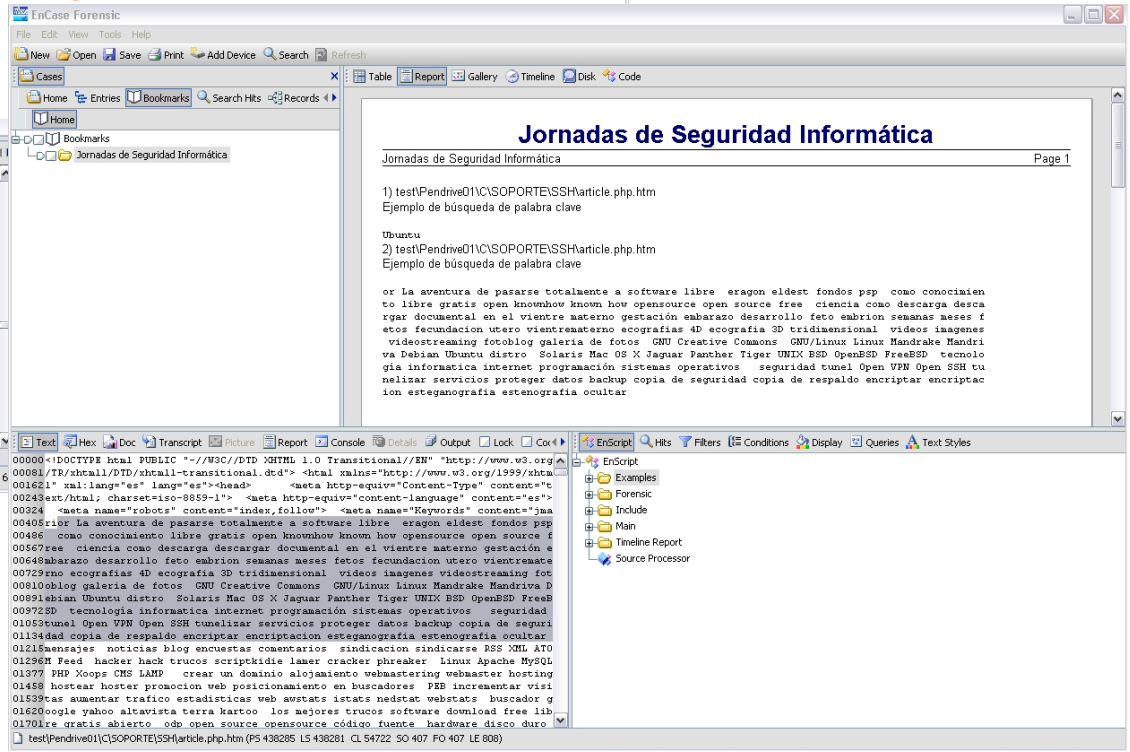
Software forense

Registro de la evidencia digital relevante para la investigación

Resultado de la búsqueda



Registro de los resultados



Hardware Forense

Write Blocker - USB

Write Blocker – Discos Rígidos

Telefonía Celular - Kit de adquisición

Toolkit de allanamiento

Hardware Forense

Destructora de CD

Etiquetas de seguridad

Rotuladora

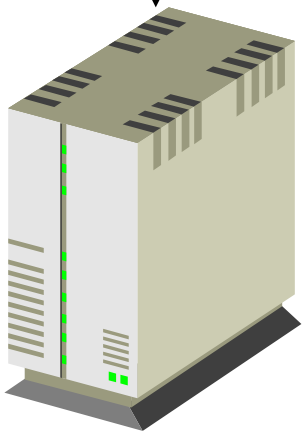
Herramientas para apertura de equipamiento

Hardware Forense

Servidores Blade

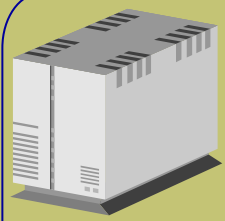
El paradigma de la virtualización

Perito Informático



Aplicaciones

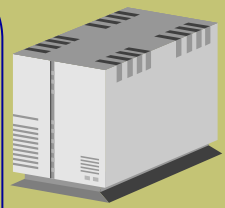
- **Encase**
- **FTK Imager**
- **Otras herramientas forenses**
- **Aplicaciones de ofimática**



- Autopsy
- AIR

Máquina Virtual Linux

- Vmware Server

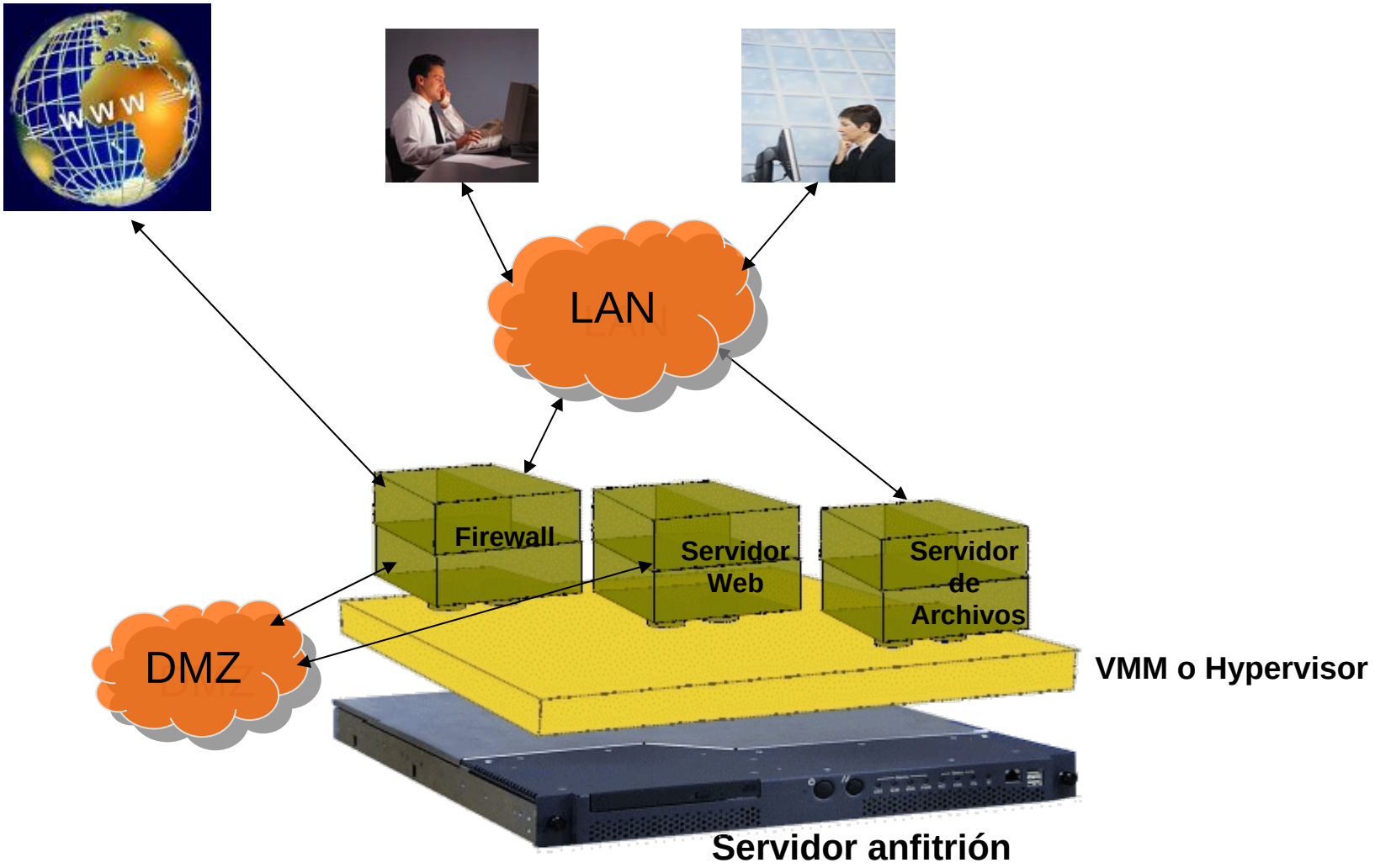


- Evidencia Digital

Máquina Virtual S.O. ...

Ventajas: Mayor disponibilidad de aplicaciones forenses para la investigación, facilidades para la inspección de evidencia digital

Virtualización de la infraestructura de servicios



Ventajas: Optimización de recursos tecnológicos, reducción de espacio físico, simplicidad de administración, mejor tolerancia a fallos

Muchas gracias por la atención

Para mayor información consulte

www.informaticapericial.com.ar