

POLICIA FEDERAL ARGENTINA



DIVISION SEGURIDAD
INFORMATICA FEDERAL

ANALISIS
FORENSE
DE
COMPUTADORAS

Por Carlos Alberto Zoratto Jefe de Operaciones y Pericias



National Infrastructure Protection Center



- Analizando los restos de un incidente de seguridad con computadoras.
- Comenzando la Investigación.
- Determinando si se ha cometido un delito informatico.
- Conduciendo la investigación cuando un delito esta en progreso.
- Preservando la evidencia.
- Recolectando evidencia.
- Manejando disquetes.



Analizando los despojos de un incidente de Seguridad informática.

Que queremos decir con un incidente de seguridad.

Nunca recibimos los llamados a tiempo.

Análisis forense de Computadora - Delitos de computadora desde la computadora.

Ramas de la ciencia forense.

Breve tutorial de DOS - Espacio Slack.



- Espacio no asignado.

Archivos Swap y caches de buscadores Web de Windows.

- Procesando datos forenses.

Recolección.

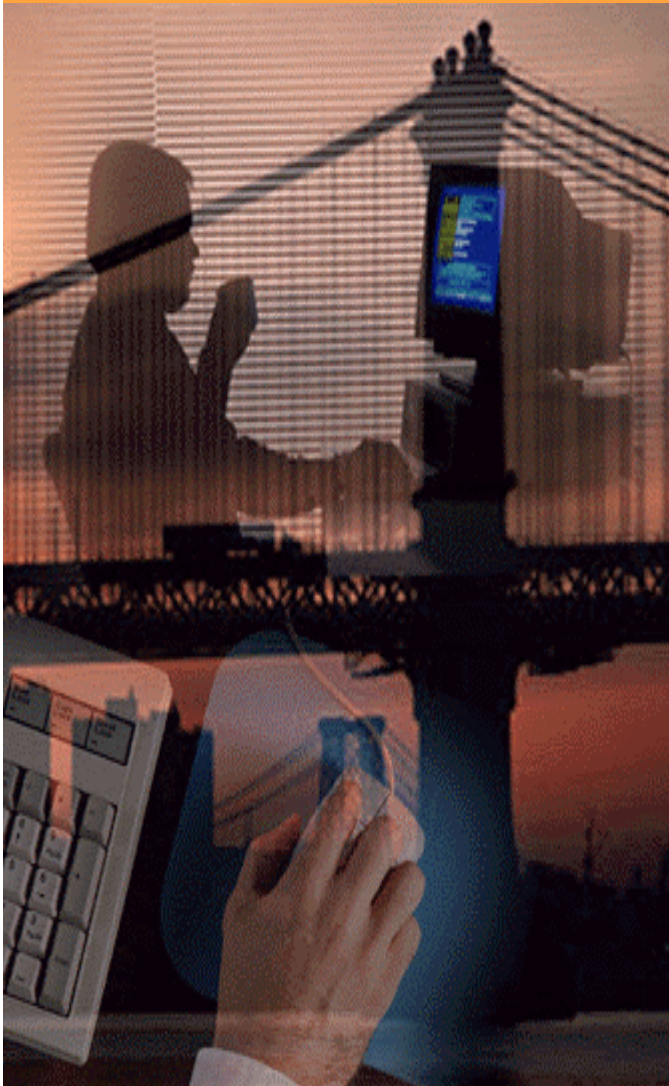
- Técnicas de recolección.

•Herramientas y Técnicas de análisis.

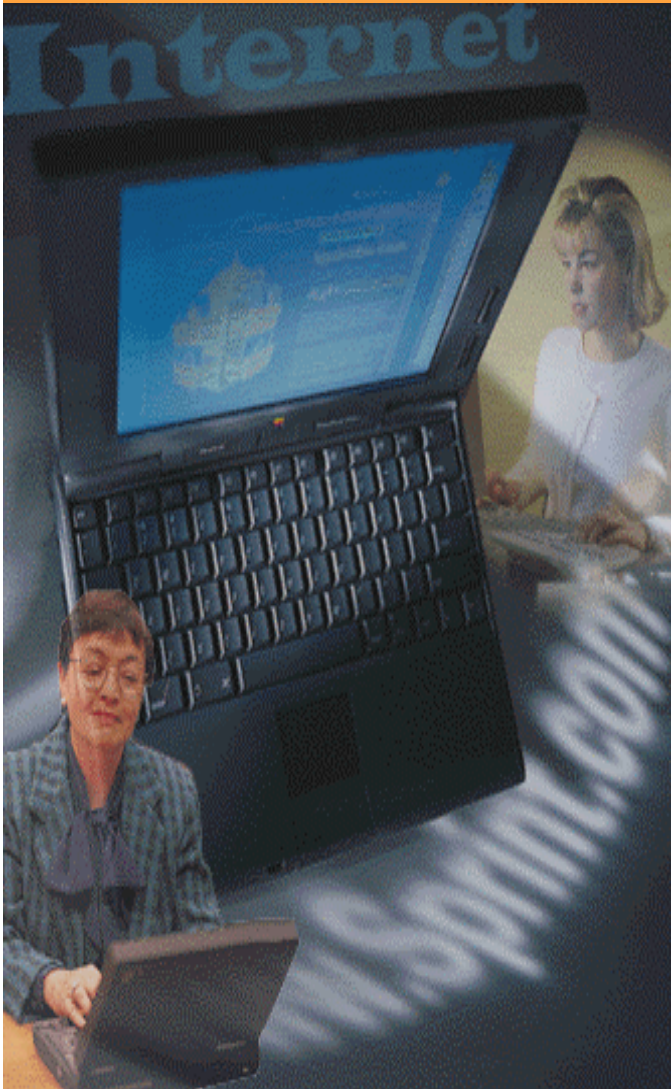
- Encadenamiento



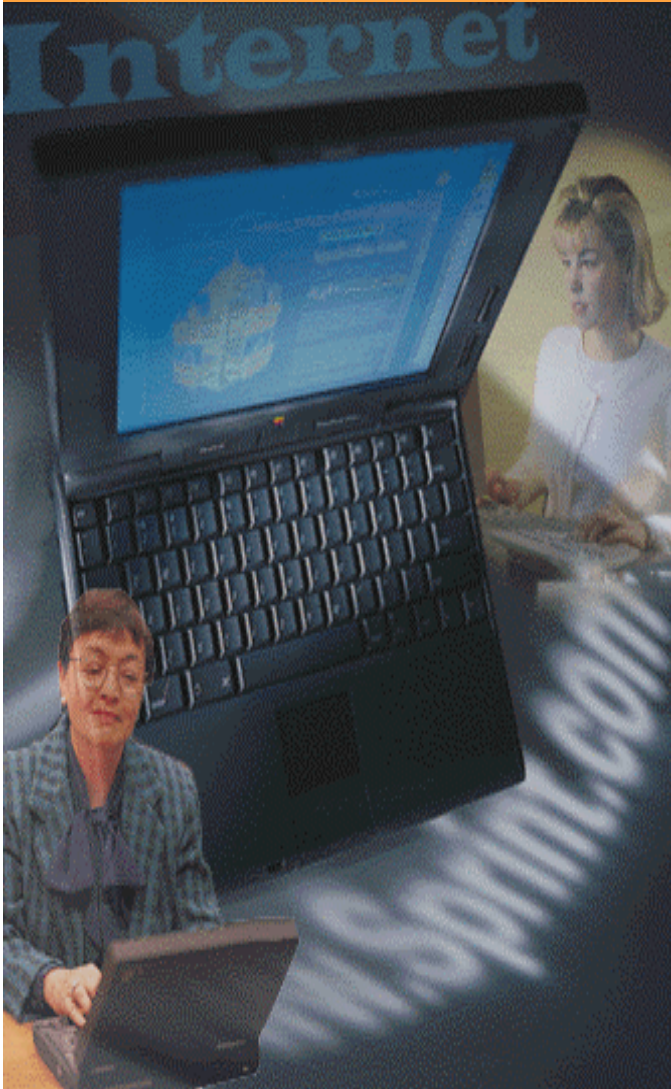
- Análisis Forense Cibernético
- Delitos involucrando redes.
- Análisis Forense de Software.
- Las limitaciones de los LOGS de sistemas.
- Los LOGS pueden contar el cuento.
- Análisis múltiples de LOGS.



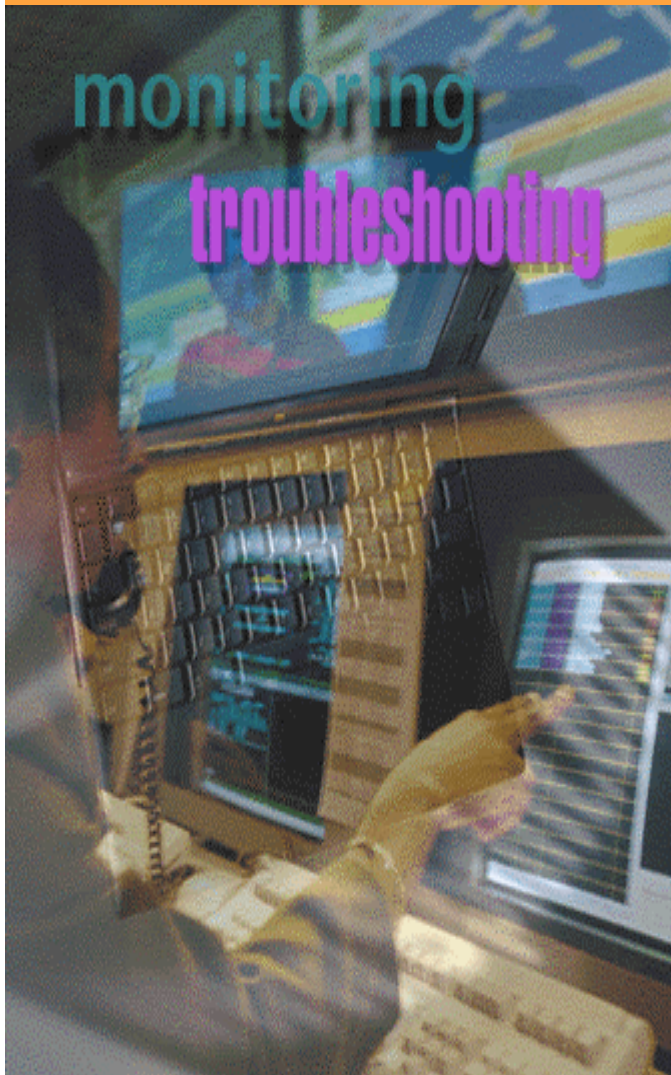
- **Iniciando la Investigación.**
- **Analizando el incidente.**
- **Analizando la evidencia y preparando su presentación.**
- **Asegurando o preservando la escena virtual del crimen.**
- **Mantener a todo el mundo alejado de la computadora investigada.**
- **Recolectando y preservando evidencia.**



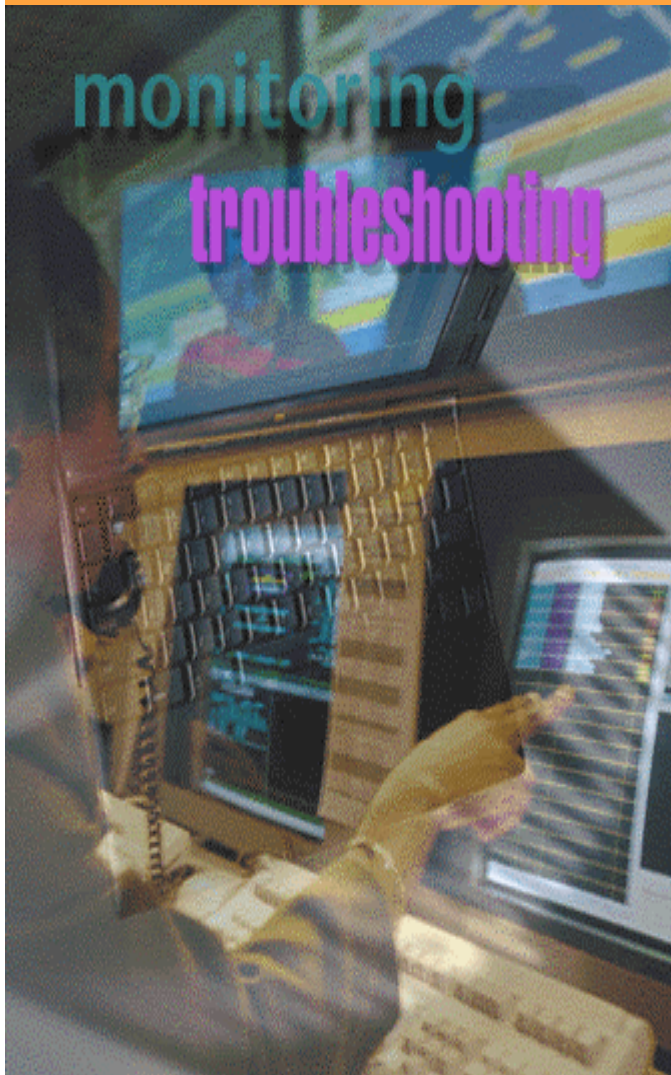
- Determinando si ha tenido lugar un delito.
- Creer en nuestros indicadores.
- Usando herramientas para verificar que ha ocurrido un delito.
- Recuperando datos de discos dañados
- Recuperando Passwords
- Recuperación de Passwords física.
- Cracking de Passwords.



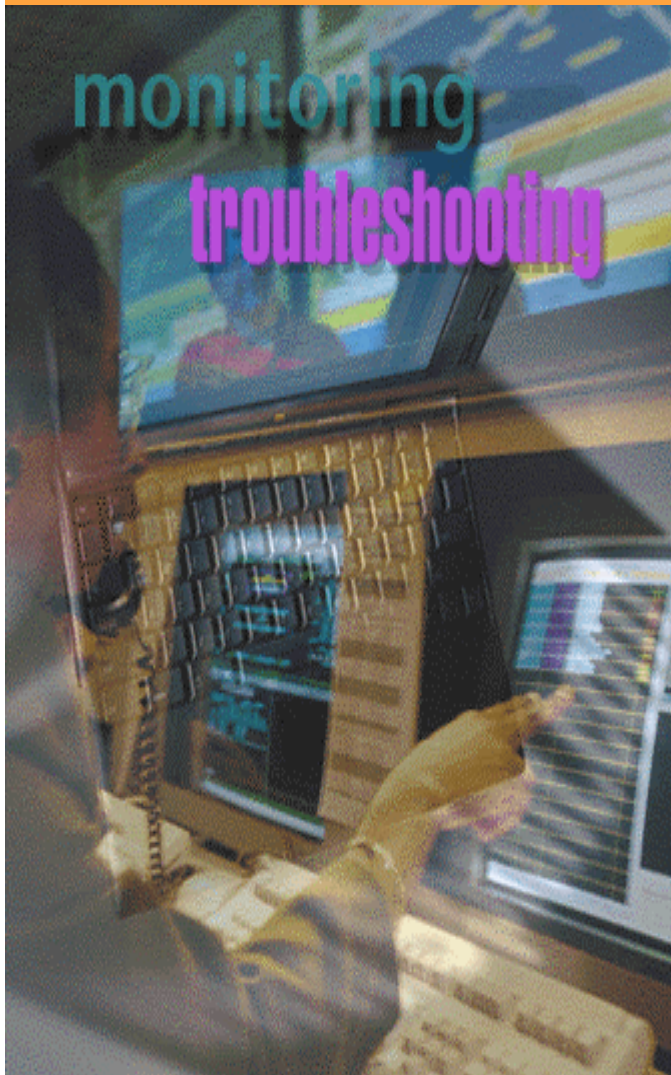
- Infiriendo.
- Examinando LOGS.
- Las herramientas.



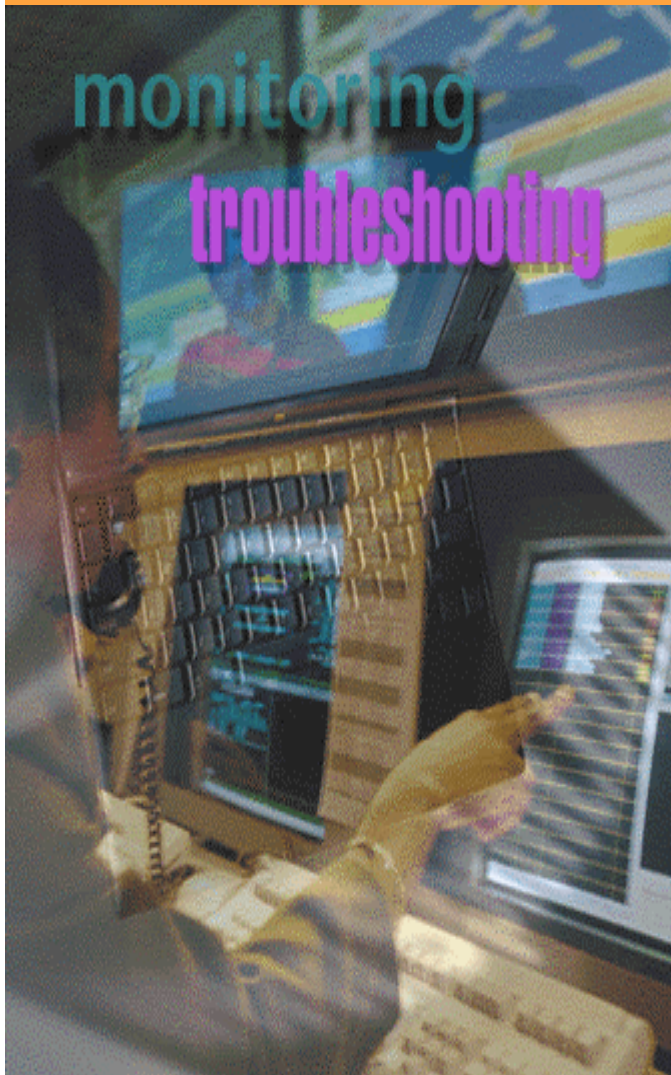
- Preservando Evidencia.
- Conceptos Básicos.
- Recolección de evidencia sin perdida de tiempo y cadena de custodia.
- Marcando evidencia con un Hash MD-5 y encriptación con PGP.
- CRCMD5
- Sellando evidencia.
- Resumen.



- Recolectando evidencia.
- Primeros pasos.
- Usando herramientas para tomar una imagen espejo de un disco.
- Tomando un inventario de un disco rígido usando Filelist.
- Buscando información oculta.
- El filtro inteligente Filter_1 V.4.1
- IP filter V.2.2



- Getslack
- Getfree
- TextSearch Plus V.2.04
- Usando Utilitarios de Norton
- Manejando Disquetes
- Copiando disquetes a un disco de trabajo.



- Análisis de LOGS
- LOGS genéricos.
- LOGS de aplicaciones.
- LOGS de captura.
- Relaciones entre LOGS.
- Problemas diversos en LOGS.
- Herramientas.

•Análisis de LOGS - Contenidos de los archivos.

Datos identificativos

Identificación del origen

Acción efectuada

Ocasionalmente, contenido de la acción

Estructuración de la información

Localización en el tiempo (día, zona horaria, etc..)

Origen (dirección IP y datos adicionales de identificación)

Identificación del tipo de transacción realizada

Opcionalmente, contenido de la transacción.

•Análisis de LOGS - Archivos de sucesos.

Ambito General

Recibo de cajero automático.
Factura telefónica.

Ambito Informático

Cabeceras de un correo electrónico.
Archivos de registro de servidores Web, e-mail, etc..

•Análisis de LOGS - Tipos de Logs genéricos.

Logs de sistema

- Windows NT/2000 (visor de sucesos o Event Viewer)
- Registro de Windows y archivos .INI (información de aplicaciones y/o contraseñas).
- Sistemas Unix (ficheros wtmp).

Logs de aplicación

- Servidores Web, E-mail, Radius, etc..

Logs de captura

- Logs de software para captura de datos.

•Análisis de LOGS - Tipos de sistema.

Registro de Windows y archivos .INI

- Información sobre software instalado en el PC
- fecha de instalación de dicho software.
- Datos de la instalación.
- Obtención de contraseñas.
- Aplicaciones ocultas realizadas en la computadora.

•Análisis de LOGS - Tipos de sistema.

Registro de Windows y archivos .INI

- Información sobre software instalado en el PC
- fecha de instalación de dicho software.
- Datos de la instalación.
- Obtención de contraseñas.
- Aplicaciones ocultas realizadas en la computadora.

•Análisis de LOGS - Tipos de sistema.

Visor de sucesos (event viewer)

- Avisos del sistema
- Información genérica.
 - Aplicación
 - Seguridad
 - Sistema
 - Aplicaciones específicas

•Análisis de LOGS - Logs de Aplicaciones.

Servidores WEB y FTP

- Dirección IP
- Usuario.
- Día, hora y zona horaria
- Petición realizada
- Códigos de sistema
- Datos adicionales

•Análisis de LOGS - Logs de Aplicaciones.

Servidores E-Mail

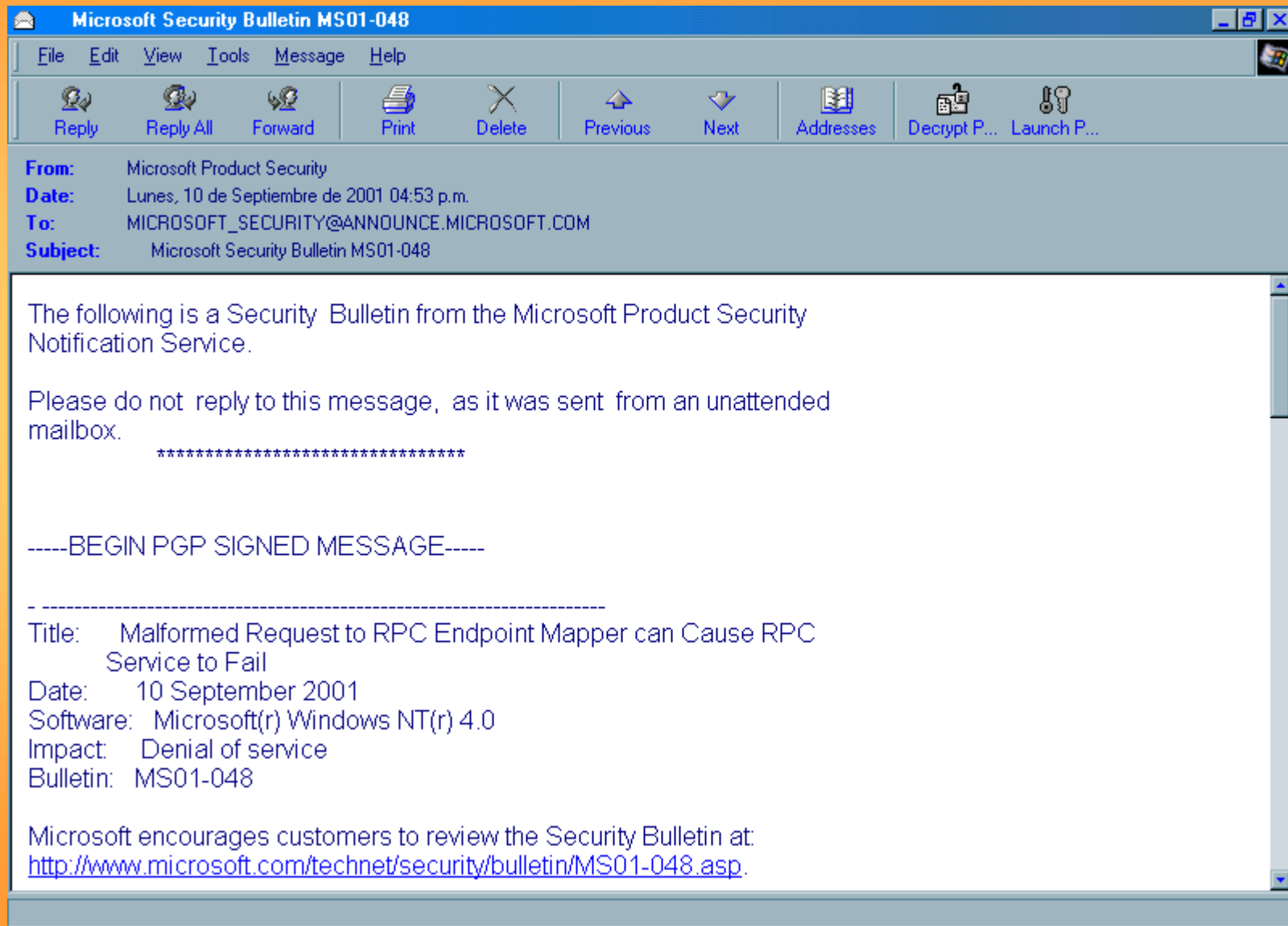
- Dirección IP Remitente
- E-Mail del emisor
- ID usuario
- Día, hora y zona horaria
- Petición realizada
- Códigos de sistema

•Análisis de LOGS - Logs de Aplicaciones.

Mensajes de Correo Electrónico

- Servidores intermedios
- Día, hora y zona horaria
- IP emisor
- Códigos de sistema
- Datos adicionales

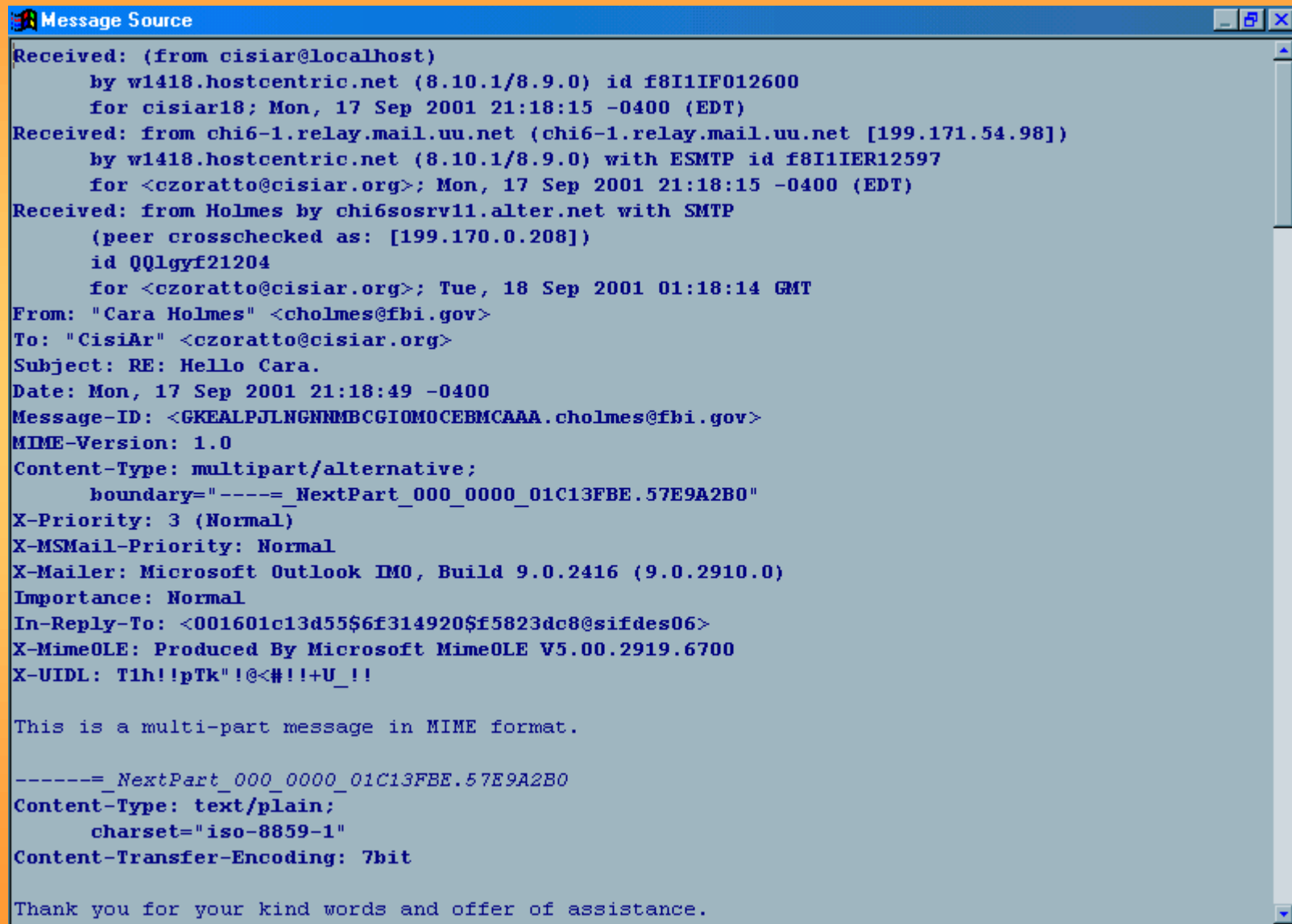
- Logs de aplicaciones - Mensajes de email.



- Logs de aplicaciones - Mensajes de email.

```
Message Source
Received: from postino2.prima.com.ar ([200.42.0.133]) by prima28.admin with Microsoft SMTPSVC(5.5.2)
    Mon, 10 Sep 2001 18:16:45 -0300
Received: from grape.ease.lsoft.com (grape.ease.lsoft.com [209.119.1.39])
    by postino2.prima.com.ar (8.11.5/8.11.5) with ESMTMP id f8ALCmb09352;
    Mon, 10 Sep 2001 18:13:52 -0300 (ART)
Received: from guava (209.119.0.39) by grape.ease.lsoft.com (LSMTMP for OpenVMS v1.1b) with SMTP id 1000000000
Received: from ANNOUNCE.MICROSOFT.COM by ANNOUNCE.MICROSOFT.COM
    (LISTSERV-TCP/IP release 1.8d) with spool id 60765 for
    MICROSOFT_SECURITY@ANNOUNCE.MICROSOFT.COM; Mon, 10 Sep 2001 16:13:39
    -0400
Approved-By: secnotif@MICROSOFT.COM
Received: from 131.107.3.51 by GUAVA.EASE.LSOFT.COM (SMTP release 1.0d) with
    TCP; Mon, 10 Sep 2001 15:54:01 -0400
Received: from 157.54.1.52 by INET-VRS-07.redmond.corp.microsoft.com (InterScan
    E-Mail VirusWall NT); Mon, 10 Sep 2001 12:53:56 -0700
Received: from red-msg-20.redmond.corp.microsoft.com ([157.54.5.165]) by
    inet-ime-06.redmond.corp.microsoft.com with Microsoft
    SMTPSVC(5.0.2195.2966); Mon, 10 Sep 2001 12:53:36 -0700
X-MIMEOLE: Produced By Microsoft Exchange V6.0.4712.0
Content-Class: urn:content-classes:message
MIME-Version: 1.0
Content-Type: text/plain; charset="us-ascii"
Content-Transfer-Encoding: quoted-printable
X-MS-Has-Attach:
X-MS-TNEF-Correlator:
Thread-Topic: Microsoft Security Bulletin MS01-048
Thread-Index: AcE6MiLq8LKdtaJ3QcyTZCZURWCSaQ==
X-OriginalArrivalTime: 10 Sep 2001 19:53:36.0334 (UTC)
    FILETIME=[476016E0:01C13A32]
Message-ID: <2E08A46FF518C9418713A1B2C780684D103D0D@red-msg-20.redmond.corp.microsoft.com>
Date: Mon, 10 Sep 2001 12:53:14 -0700
Sender: Microsoft Product Security Notification Service <MICROSOFT_SECURITY@ANNOUNCE.MICROSOFT.COM>
From: Microsoft Product Security <secnotif@MICROSOFT.COM>
```

- Logs de aplicaciones - Mensajes de email.



```
Message Source
Received: (from cisiar@localhost)
  by wl418.hostcentric.net (8.10.1/8.9.0) id f8I1IF012600
  for cisiar18; Mon, 17 Sep 2001 21:18:15 -0400 (EDT)
Received: from chi6-1.relay.mail.uu.net (chi6-1.relay.mail.uu.net [199.171.54.98])
  by wl418.hostcentric.net (8.10.1/8.9.0) with ESMTMP id f8I1IER12597
  for <czoratto@cisiar.org>; Mon, 17 Sep 2001 21:18:15 -0400 (EDT)
Received: from Holmes by chi6sosrv11.alter.net with SMTP
  (peer crosschecked as: [199.170.0.208])
  id QQ1gyf21204
  for <czoratto@cisiar.org>; Tue, 18 Sep 2001 01:18:14 GMT
From: "Cara Holmes" <cholmes@fbi.gov>
To: "CisiAr" <czoratto@cisiar.org>
Subject: RE: Hello Cara.
Date: Mon, 17 Sep 2001 21:18:49 -0400
Message-ID: <GKEALPJLNGNMBBCGIOMOCEBMCAAA.cholmes@fbi.gov>
MIME-Version: 1.0
Content-Type: multipart/alternative;
  boundary="-----_NextPart_000_0000_01C13FBE.57E9A2B0"
X-Priority: 3 (Normal)
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook IM0, Build 9.0.2416 (9.0.2910.0)
Importance: Normal
In-Reply-To: <001601c13d55$6f314920$f5823dc8@sifdes06>
X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2919.6700
X-UIDL: Tih!!pTk"!@<#!!+U_!!

This is a multi-part message in MIME format.

-----=_NextPart_000_0000_01C13FBE.57E9A2B0
Content-Type: text/plain;
  charset="iso-8859-1"
Content-Transfer-Encoding: 7bit

Thank you for your kind words and offer of assistance.
```

•Análisis de LOGS - Relaciones entre Logs.

Necesarias para la identificación con garantías

- Extracción de información cruzada
- Códigos de señalización permiten el seguimiento de datos en logs de diferentes sistemas.
- Ayudan a confirmar la autenticidad de la información obtenida en otros logs

•Análisis de LOGS - Problemas comunes entre Logs.

Problemas inherentes a logs

- Errores de interpretación debido a zonas horarias
- Errores de interpretación debidos a diferencias de reloj entre servidores
- Problemas de localización de registros debidos al volumen de información a gestionar
- Errores de integridad en los archivos que hacen dudar de su credibilidad

•Herramientas - Visual Route.

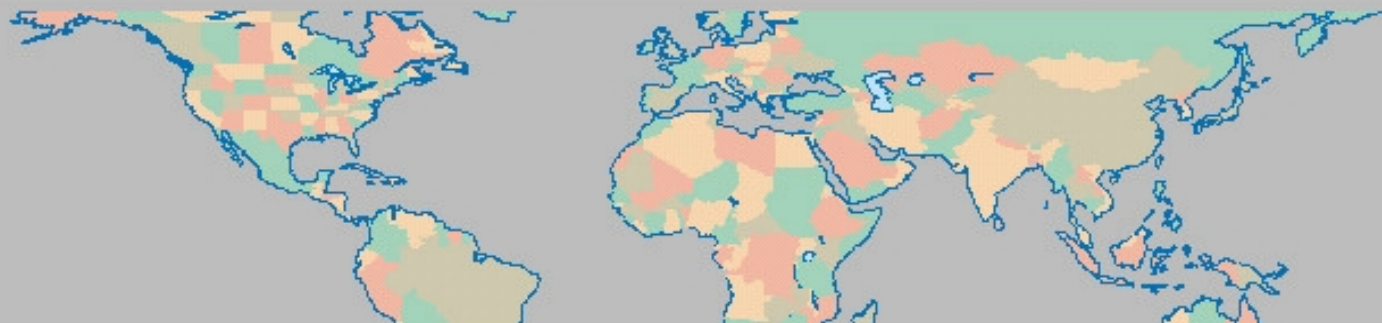
Report for 64.76.24.176

Analysis: IP packets are being lost past network "FRANQUICIAS" at hop 12. There is insufficient cached information to determine the next network at hop 13. Connections to HTTP port 80 are being rejected. Node 64.76.24.130 at hop 12 in network "FRANQUICIAS" reports "The destination host is unreachable".

Hop	IP Address	Node Name	Location	Network	Graph
0	200.61.129.147	host147.200.61.129.ifxnw.com.ar	*	IFX Networks Argentina S.R.L.	
1	200.61.128.23	host23.200.61.128.ifxnw.com.ar	Buenos Aires, Argentina	IFX Networks Argentina S.R.L.	
2	200.61.128.1	host1.200.61.128.ifxnw.com.ar	Buenos Aires, Argentina	IFX Networks Argentina S.R.L.	
3	200.61.160.66	line160-66.iplan.com.ar	Buenos Aires, Argentina	NSS, S.A.	
4	200.61.173.2	line160-2.iplan.com.ar	Buenos Aires, Argentina	NSS, S.A.	
5	200.41.38.137	-	(Argentina)	esmeraldadialup	
6	200.55.0.9	-	Buenos Aires, Argentina	Impsat Argentina	
7	200.41.25.230	rcorelma1-rcoreats1.impsat.net.ar	Buenos Aires, Argentina	Impsat S.A.	
8	200.41.25.233	rcoretlp1.impsat.net.ar	Buenos Aires, Argentina	Impsat S.A.	
9	200.0.194.83	rgf6.impsat.net.ar	(Argentina)	IMPSAT ARGENTINA	
10	200.41.25.94	rpil1.impsat.net.ar	Buenos Aires, Argentina	Impsat S.A.	
11	64.76.24.130	tntpil1.impsat.net.ar	(Argentina)	FRANQUICIAS	
12	64.76.24.130	tntpil1.impsat.net.ar	(Argentina)	FRANQUICIAS	
...					
?	64.76.24.176	64-76-24-176-tntpil1.impsat.net.ar	(Argentina)	FRANQUICIAS	

VisualRoute Report for 64.76.24.176 produced at 19:03 on 30 de julio de 2001.

64.76.24.176 is not accepting ICMP packets. Roundtrip time to 64.76.24.130 average = 4276ms min = 1497ms max = 6056ms



•Herramientas - Visual Route.

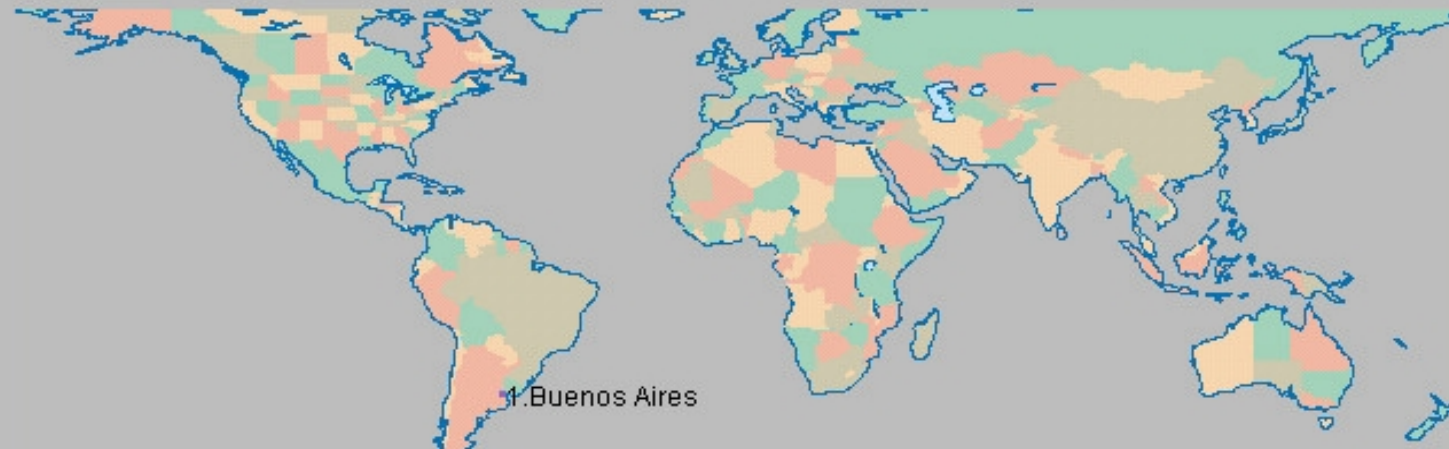
Report for centauro.interar.com.ar [200.47.136.248]

Analysis: Node 'centauro.interar.com.ar' was found in 11 hops (TTL=245). But, problems starting at hop 4 in network "NSS, S.A." are causing IP packets to be dropped. Connections to HTTP port 80 are being rejected.

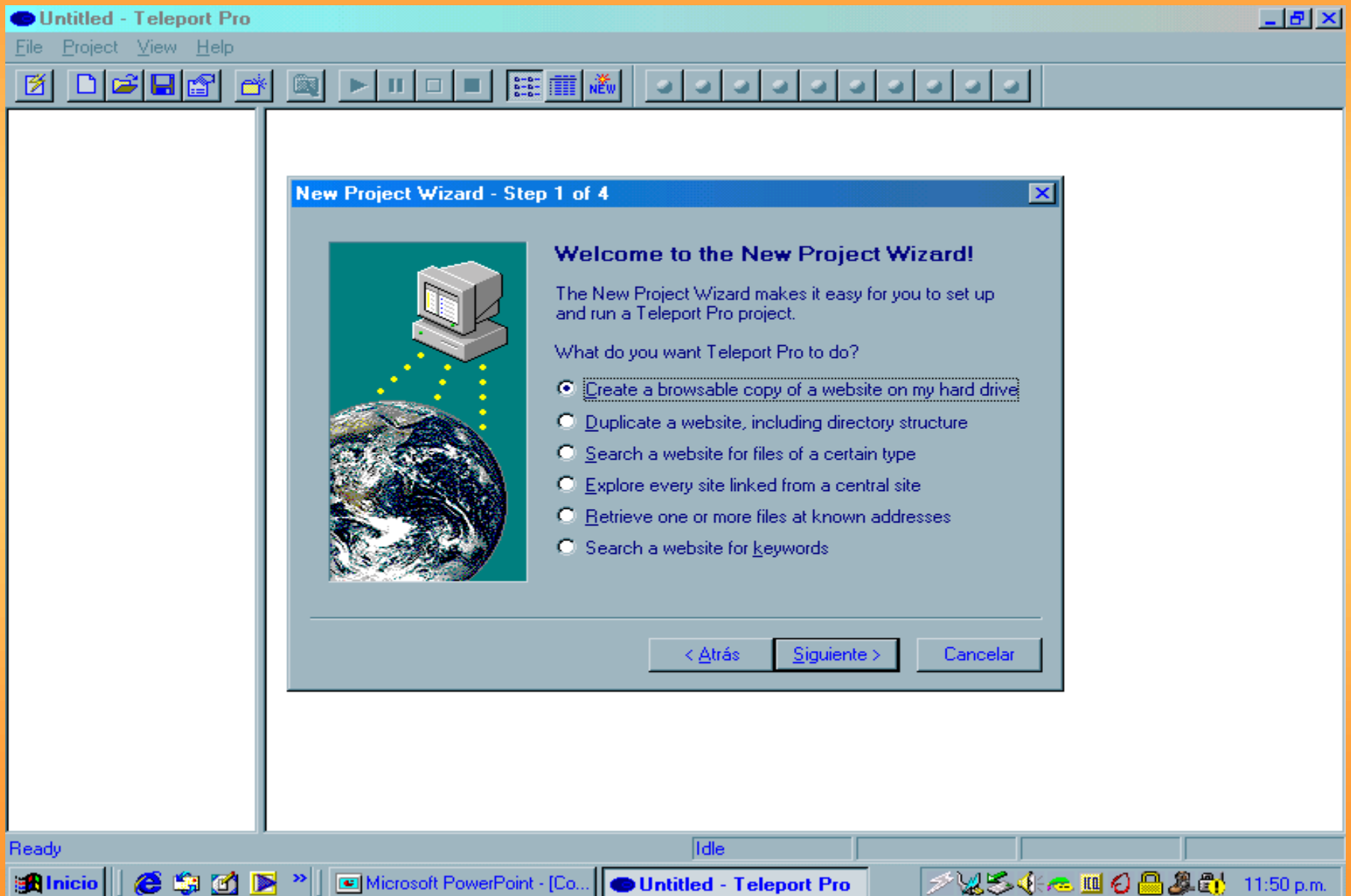
Hop	IP Address	Node Name	Location	Network	Graph
0	200.61.130.236	host236.200.61.130.ifxnw.com.ar	*	IFX Networks Argentina S.R.L.	
1	200.61.128.23	host23.200.61.128.ifxnw.com.ar	Buenos Aires, Argentina	IFX Networks Argentina S.R.L.	
2	200.61.128.1	host1.200.61.128.ifxnw.com.ar	Buenos Aires, Argentina	IFX Networks Argentina S.R.L.	
3	200.61.160.66	line160-66.iplan.com.ar	Buenos Aires, Argentina	NSS, S.A.	
4	200.61.173.2	line160-2.iplan.com.ar	Buenos Aires, Argentina	NSS, S.A.	
5	200.47.11.62	line62.comsat.net.ar	(Argentina)	Comsat Argentina S.A.	
6	200.47.149.221	line221.comsat.net.ar	(Argentina)	Comsat Argentina S.A.	
7	200.47.162.101	STM1.N4-N3.comsat.net.ar	(Argentina)	Comsat Argentina S.A.	
8	200.47.128.90	line90.comsat.net.ar	(Argentina)	Comsat Argentina S.A.	
9	200.47.5.52	router-nap-lp-pil.interar.net	(Argentina)	Comsat Argentina S.A.	
10					
11	200.47.136.248	centauro.interar.com.ar	(Argentina)	Comsat Argentina S.A.	

VisualRoute Report for centauro.interar.com.ar produced at 18:31 on 30 de julio de 2001.

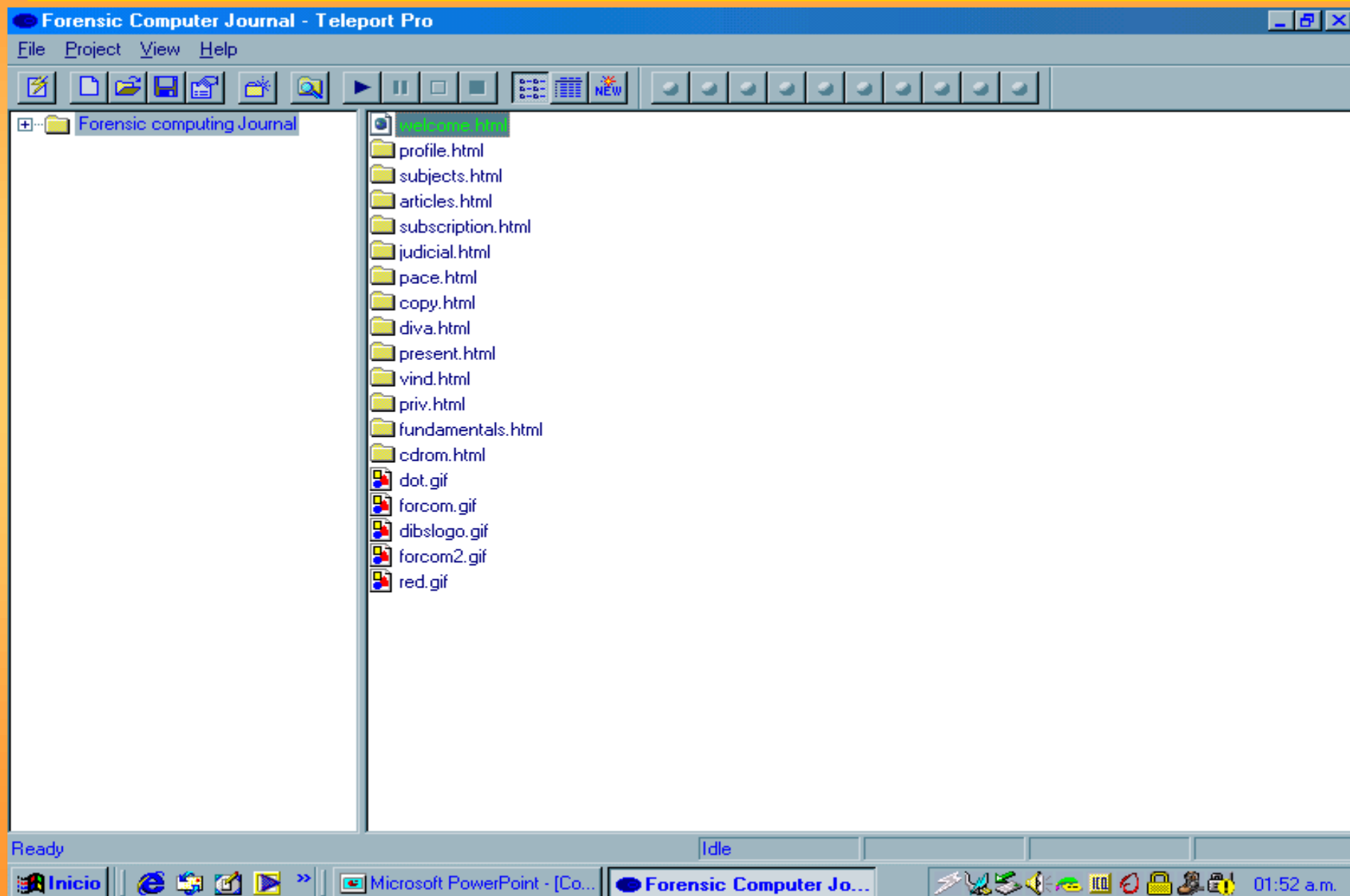
Roundtrip time to centauro.interar.com.ar (200.47.136.248) average = 197ms min = 151ms max = 330ms



•Herramientas - Teleport Pro.



•Herramientas - Teleport Pro.



•Herramientas - Teleport Pro. + I.E. 5.5



The screenshot shows a Microsoft Internet Explorer 5.5 window titled "Forensic Computing - Journal - Authoritative Comment - Microsoft Internet Explorer". The address bar shows the local file path "C:\WEB\Forensic Computer Journal\welcome.html". The browser's menu bar includes File, Edit, View, Favorites, Tools, and Help. The toolbar contains buttons for Back, Forward, Stop, Refresh, Home, Search, Favorites, History, Mail, Print, Real.com, and Messenger. Below the toolbar, there are links for Support Knowledge, TechNet, Microsoft Security, FedCIRC, Hacker Tracker, Foundstone, and (NIPC).

The main content area displays the logo for the *International Journal of FORENSIC COMPUTING™*, which features a globe graphic. To the right of the logo, a paragraph of text reads: "The International Journal of Forensic Computing™ addresses all aspects of computer evidence and computer investigations. It provides its readership with the investigative strategy necessary to conduct computer investigations and the tactics, techniques and tools available to the investigator. The Journal is an invaluable source of information to auditors, technicians, security managers and lawyers who regularly encounter computer systems upon which potential evidence may reside."

Below the logo, there are five red underlined links: [ABOUT THE JOURNAL](#), [SUBJECTS COVERED](#), [ARTICLES](#), [SUBSCRIPTION DETAIL](#), and [E-MAIL US](#).

At the bottom of the page, another paragraph of text begins: "In addition to publishing commissioned articles and case studies written by respected and highly experienced computer investigators and forensic practitioners, The International Journal of Forensic Computing™ also keeps its".

The status bar at the bottom of the browser window shows "Done" and "My Computer".

•Herramientas - Teleport Pro. + I.E. 5.5

Microsoft Internet Explorer - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail Print Real.com Messenger

Address C:\WEB\Consecri\index.htm

Vínculos Support Knowledge TechNet Microsoft Security FedCIRC Hacker Tracker Foundstone (NIPC)


Programa Información Organización

Pre-Inscripción Informes


CONSECRI 2001

"La seguridad y la criptografía garantías de la convergencia"

Organizado por:



Escuela Superior Técnica



Instituto de Enseñanza Superior del Ejército

programa.zip

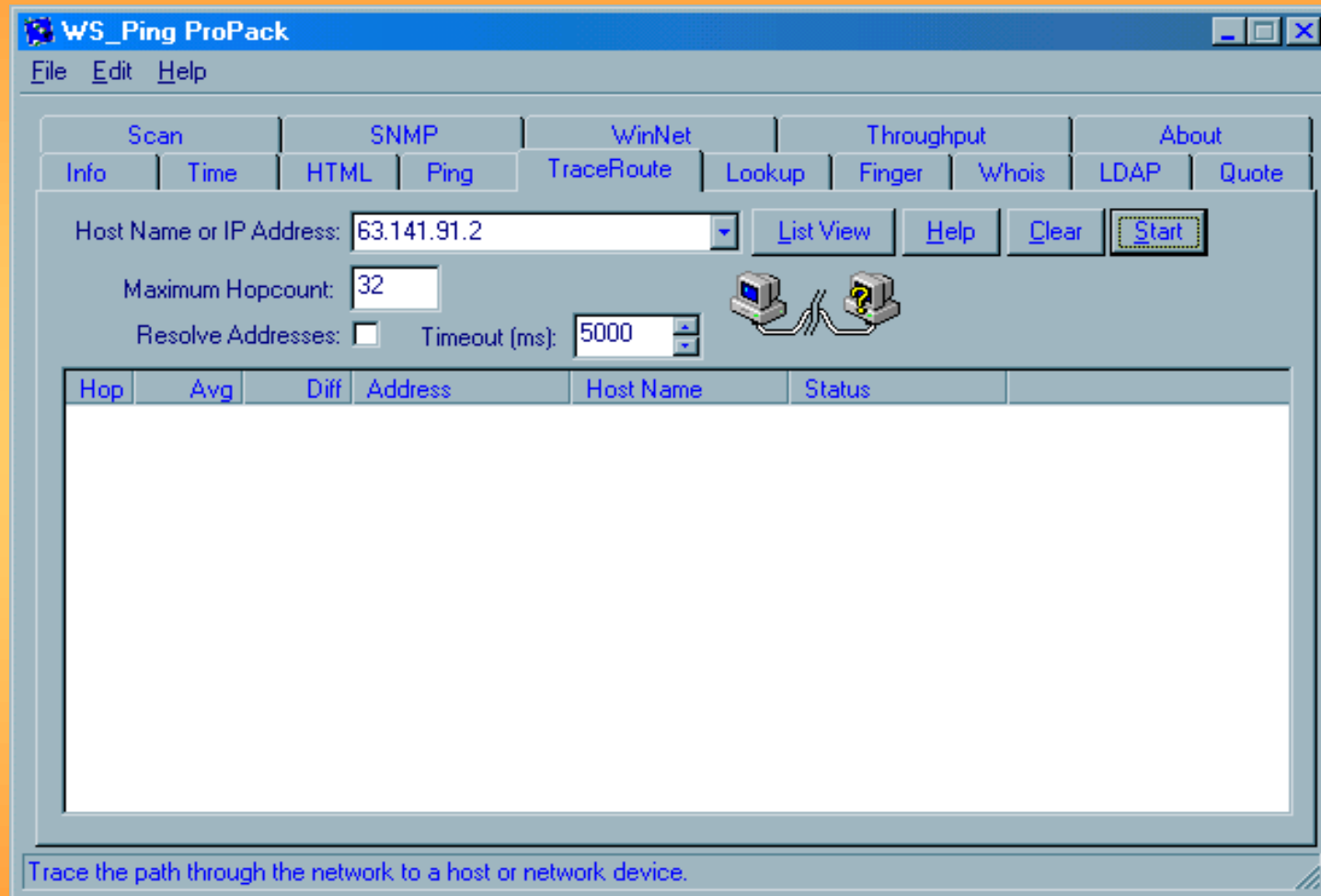
Patrocinio

Datos Curriculum resumidos y fotos de los oradores

1 Congreso

My Computer

•Herramientas - WS_Ping ProPack.



• Herramientas - ZTreeWin v1.47

ZTreeWin v1.47t

Auto

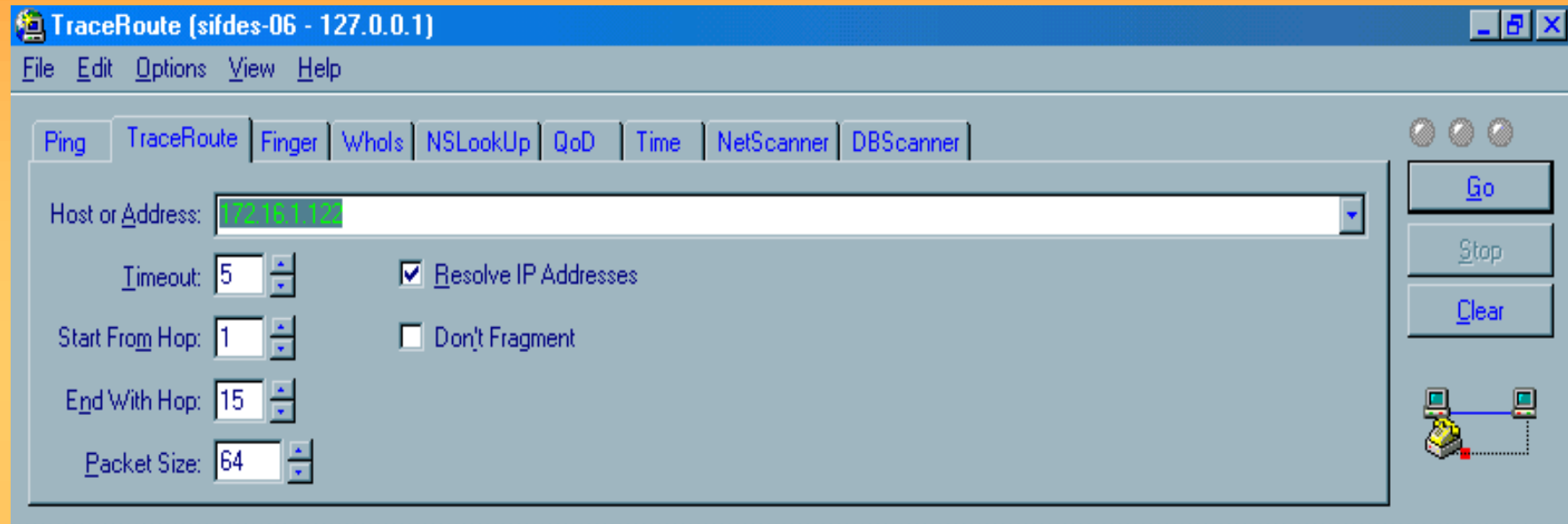
C:\Archivos de programa\LockDown Millennium 27-09-01 2:06:26

<ul style="list-style-type: none"> + — ICQ + — Intellisync + — Internet Explorer + — Iomega + — Legion + — Lockdown Corp + — LockDown Millennium + — Luc Neijens + — Messenger + — Microsoft Games + — Microsoft NetShow + — Microsoft Office + — Movie Maker + — MSN Gaming Zone 	<pre> FILE *.* ----- DISK C: Available Bytes 1,137,201,152 DISK Statistics Total Files 248 Bytes 121,273,760 Matching Files 248 Bytes 121,273,760 Tagged Files 0 Bytes 0 Current Directory LockDown Millennium Bytes 6,292,639 </pre>
--	---

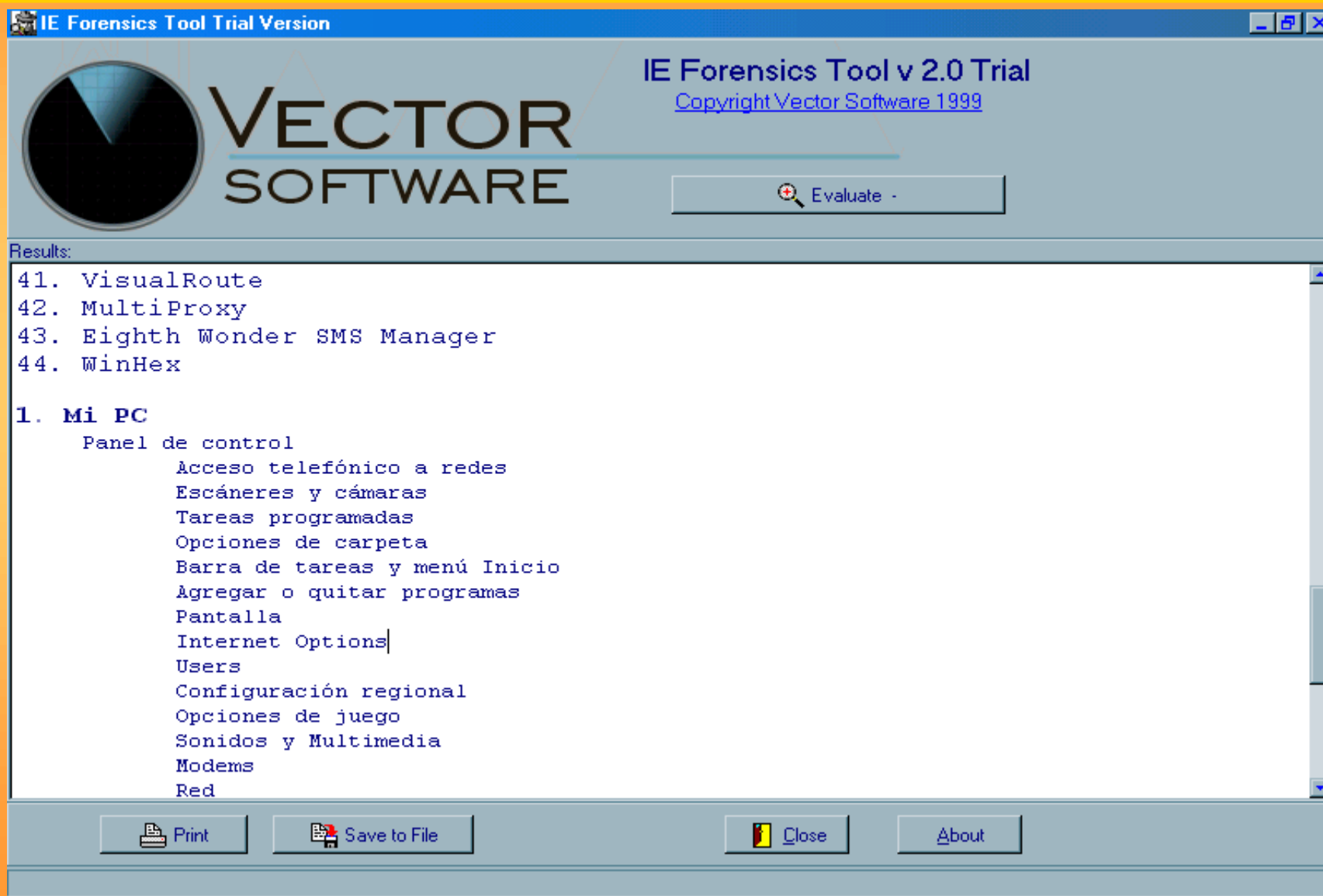
autoexec	.bat	300	.a..	16-05-01	13:54:24
boing	.wav	26,954	.a..	20-01-93	0:00:00
booning	.wav	21,714	.a..	21-06-94	1:52:24
buzz	.wav	16,202	.a..	17-06-94	2:51:06

DIR Avail Branch Compare Delete Filespec Global sHortcut Invert
 COMMANDS Log Make Print Rename Showall Tag Untag View eXecute Quit
 ← file F7 autoview F8 split F9 menu \ Treespec F1 help ? stats

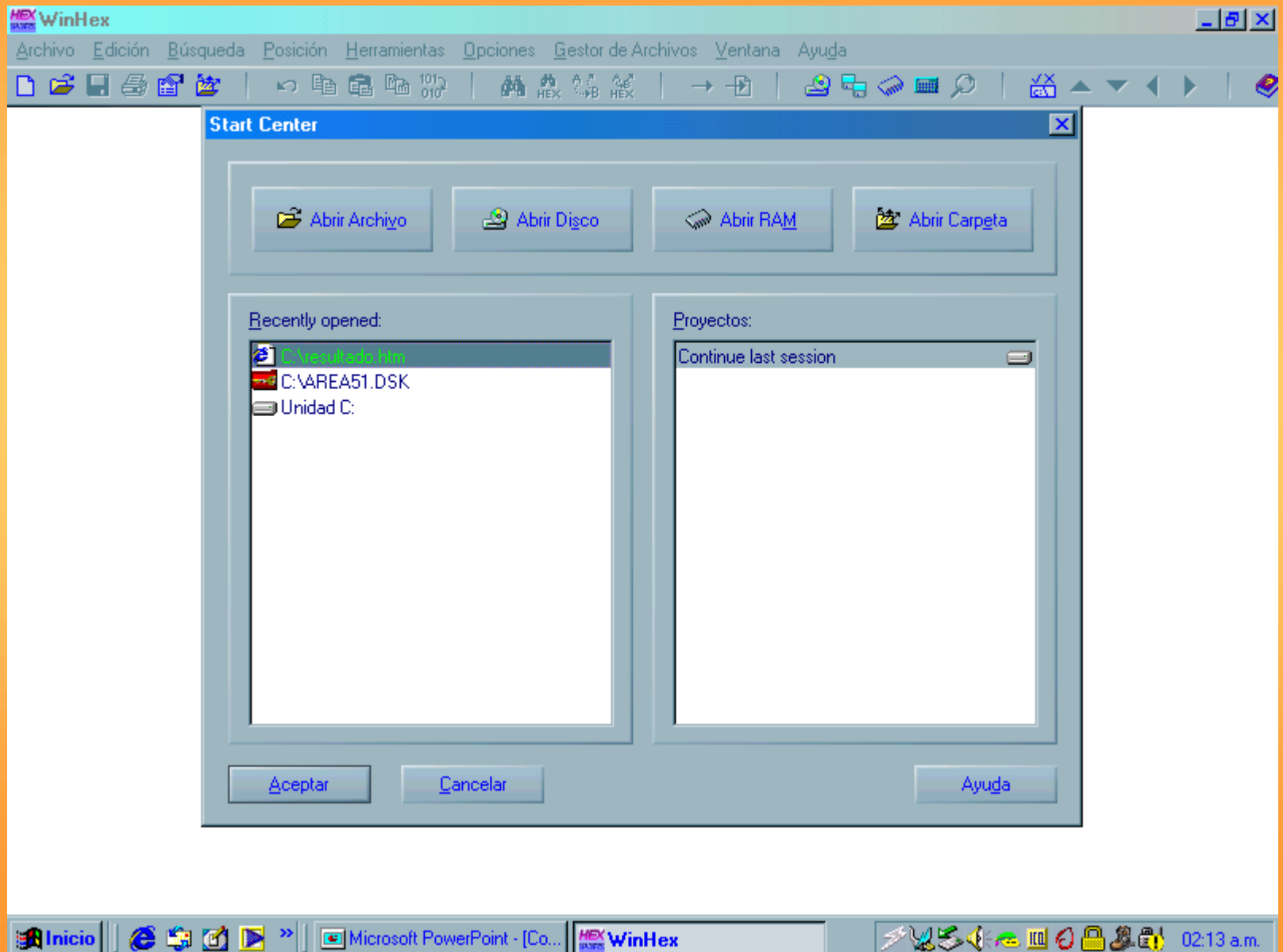
•Herramientas - CyberKit



•Herramientas - IE Forensic Tool v2.0



• Herramientas - WinHex



Herramientas - WinHex

The screenshot displays the WinHex application interface. The main window shows a hex editor for 'Unidad C:' with a list of offsets and their corresponding hexadecimal and ASCII values. A menu is open over the 'Herramientas' (Tools) section, listing various utilities like 'Editor de Disco...', 'Calculadora', and 'Analizar Disco'. A small 'Intérprete de Datos' (Data Interpreter) window is also visible, showing bit-level interpretations for the selected data.

Offset	Hex	ASCII
00048B000	øÿÿ . ÿÿÿ . ô%	
00048B040		X*
00048B080	Å& # . . . \$.	
00048B0C0	ó . . . (æ) . . ç) . . 2 .	
00048B100	! . . B . . %	
00048B140	! . . R . . S . . X .	
00048B180	f& . . Z . . E . . ^ .	
00048B1C0	à . . v% . . s . . r%	
00048B200	. . . > . . - . . " . .	
00048B240 ' . . f	
00048B280	i . . c . . é . . ¤ . .	
00048B2C0	© . . ° . . ± . . ² . .	
00048B300	Á . . È . . Æ . . 1 . . É . . Æ . . Ç . . X . . S . . ç . . R . . o . . Í . . » . . Ô . . Î . .	
00048B340	Ï . . Ò . . U . . ÿÿÿ ä . . Ö . . Û . . Ø . . Û . . Û . . " . . × . . ÿÿÿ Þ . . œ . . Û . .	
00048B380	á . . á . . ß . . Ð . . I . . Ñ . . ç . . f . . + . . f . . è . . i . . ¤ . . ÿÿÿ í . . í . .	
00048B3C0	. . . ò . . ó . . ô . . õ . . ÷ . . ø . . ù . . ú . . û . . ü . . ý . . þ . . ³ . .	
00048B400	. . ° ÿÿÿ ¤ e . . u € . . Z . . Q . .	
00048B440	l . . !	
00048B480	. . . = . . # . . 1 . . % . . & . . ' . . Î . .) . . * . . \$ ÿÿÿ 0 . .	
00048B4C0	- . . > . . 3 . . à . . 5 . . Ô . . / . . 8 Ï . . 6 . . + . . ? . . I . . < . . @ . .	
00048B500	H . . F . . C . . Ö . . Ø . . ý Û . . (. . 9 . . × . . M . . j . . I . . k . .	
00048B540	\ . . P . . å . . T . . à . . S . . [. . ¼ . . Y . . Å . . X . . Z . . ^ . . l . . a . . ` . .	
00048B580	ÿÿÿ b . . c . . d . . e . . f . . g . . h . . i . . j . . k . .] . . _ . . i . . o . . %! . .	
00048B5C0	K . . p . . Ê . . t . . u . . v . . w . . x . . y . . z . . { } . . ~ . . + . . € . .	
00048B600	+ f † . . ‡ . . ^ . . % . .	
00048B640	' . . ' . . " . . " - . . - . . ~ . . ™ . .	
00048B680	i . . c . . é . . ¤ . . ¤ \$ © . .	

Intérprete de Datos

- 8 Bit (±): -8
- 16 Bit (±): -8
- 32 Bit (±): 268435448

Unidad C: 23% libre FAT32

[Modo de lectura]

Nivel de deshacer: 0
Reversible: n/d

Espacio utilizado: 3.5 GB
3.722.919.936 bytes

Espacio libre: 1.1 GB
1.128.706.048 bytes

Capacidad total: 4.5 GB
4.861.140.480 bytes

Bytes por clúster: 4.096
Clústeres libres: 275.563
Clústeres totales: 1.184.479

Bytes por sector: 512
Sectores disponibles: 9.475.832
Primer sector de datos: 18576

Último barrido: hace 6 días

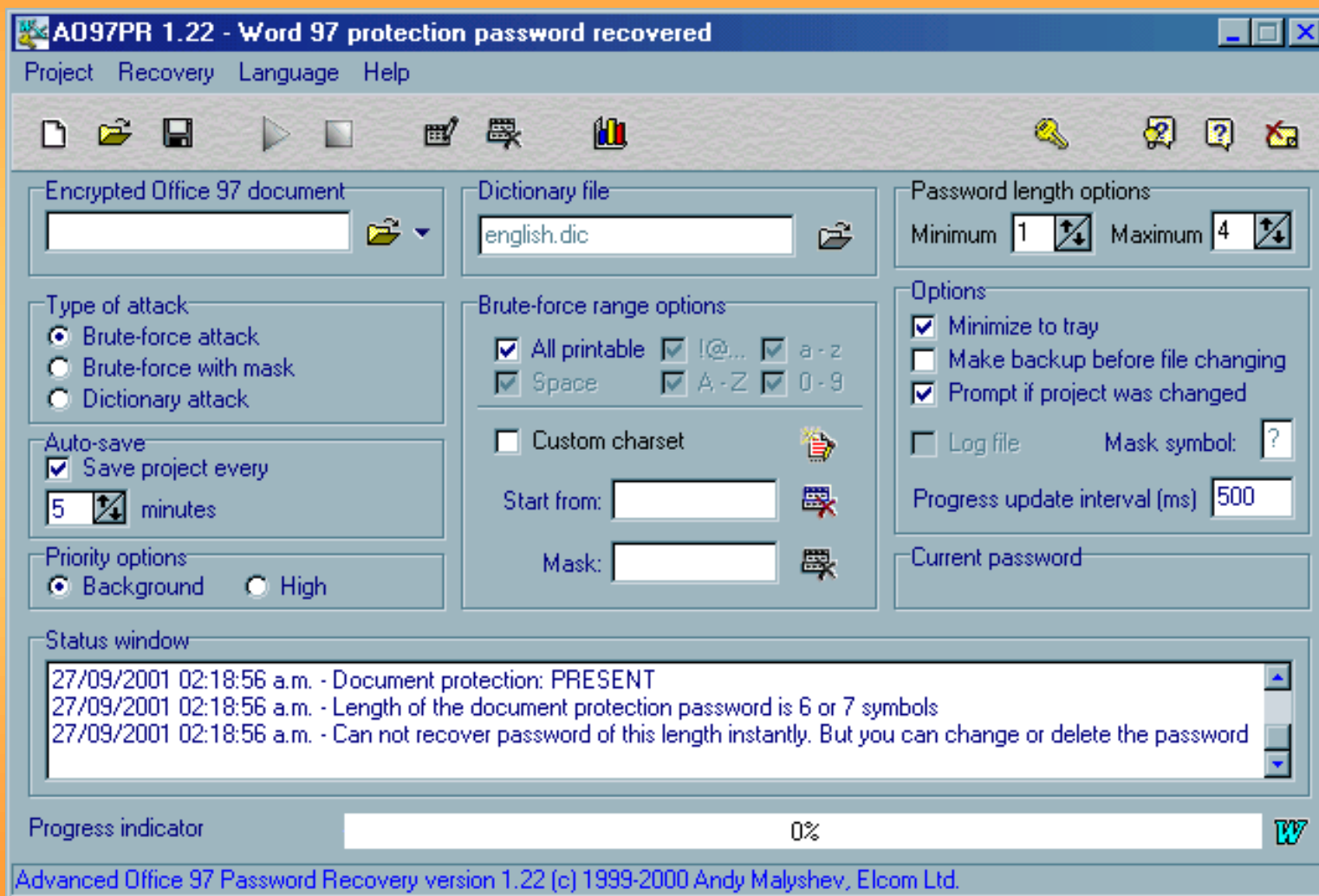
Nº de clústeres: n/d
FAT 2

Disco físico: 80h
1º sector de partición: 63

Sector 9304 de 9494415 Offset: 48B000 = 248

Microsoft PowerPoint - [Co... WinHex 02:15 a.m.

•Herramientas - Advanced Office Password Recovery



• Herramientas - Equipamiento forense


Acrobat Reader - [Raid Flyer with Price.pdf]

Archivo Edición Documento Ver Ventana Ayuda

DIBS[®] RAID

Rapid Action Imaging Device

DIBS[®] Rapid Action Imaging Device is a tough yet lightweight unit designed to enable a forensically sound copy to be made from a suspect hard drive directly onto a second hard drive. The copy can then be examined for the presence of evidential material without risk of damaging the original. The unit is ideal for making fast copies for initial analysis and assessment of evidence.



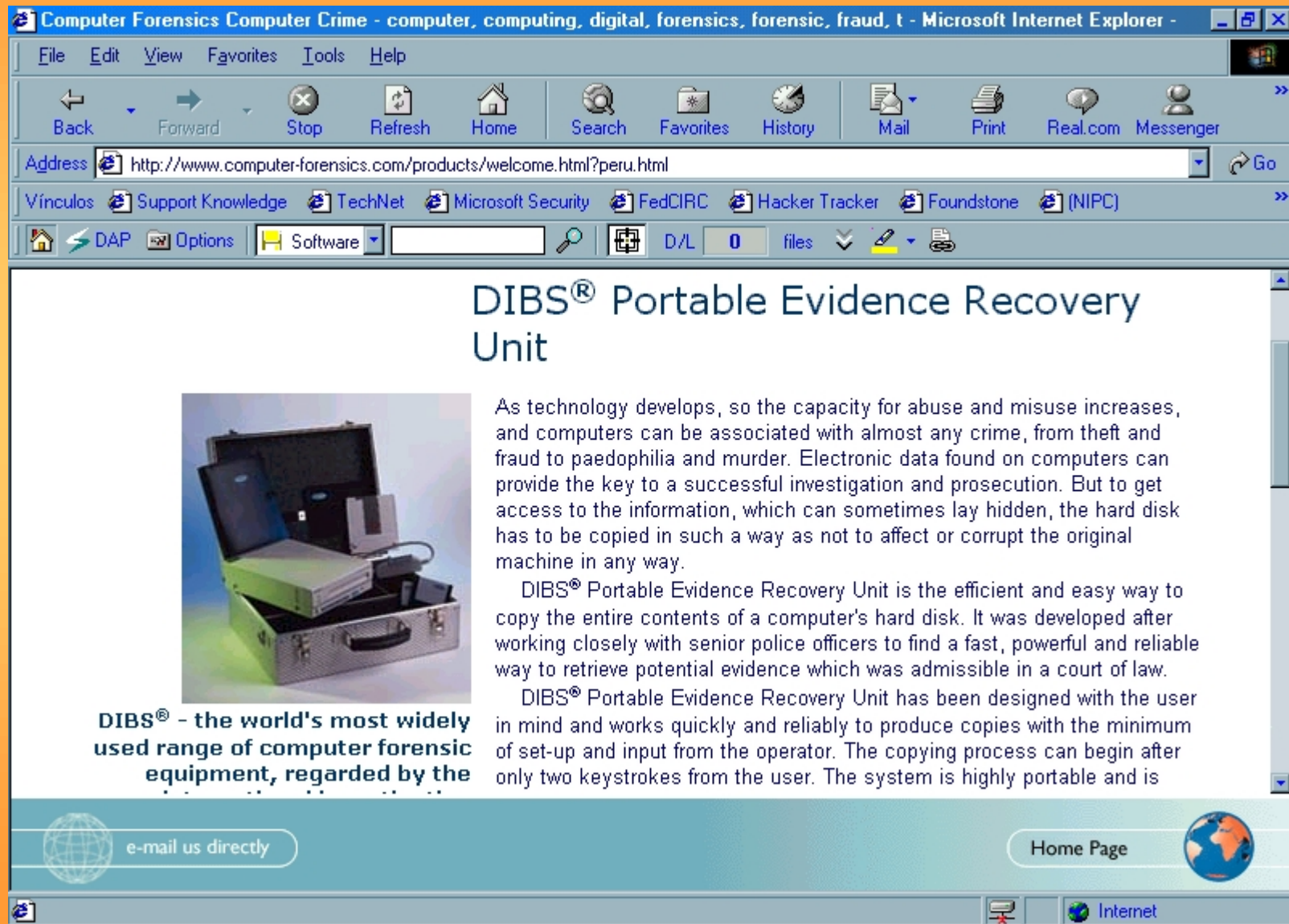
The Advantages of Using DIBS[®] RAID

- Provides fast and exact bitstream copying of

Forensically Sound Rapid Copying at Speeds of up to *1 GB per minute.**


125% 1 de 1 215.9 x 279.4 mm

•Herramientas - Equipamiento forense



The screenshot shows a Microsoft Internet Explorer browser window. The title bar reads "Computer Forensics Computer Crime - computer, computing, digital, forensics, forensic, fraud, t - Microsoft Internet Explorer". The address bar contains the URL "http://www.computer-forensics.com/products/welcome.html?peru.html". The browser's menu bar includes File, Edit, View, Favorites, Tools, and Help. The toolbar contains icons for Back, Forward, Stop, Refresh, Home, Search, Favorites, History, Mail, Print, Real.com, and Messenger. The address bar also shows "Vínculos" and a list of links: Support Knowledge, TechNet, Microsoft Security, FedCIRC, Hacker Tracker, Foundstone, and (NIPC). The browser's status bar at the bottom shows "Internet".

DIBS® Portable Evidence Recovery Unit



DIBS® - the world's most widely used range of computer forensic equipment, regarded by the

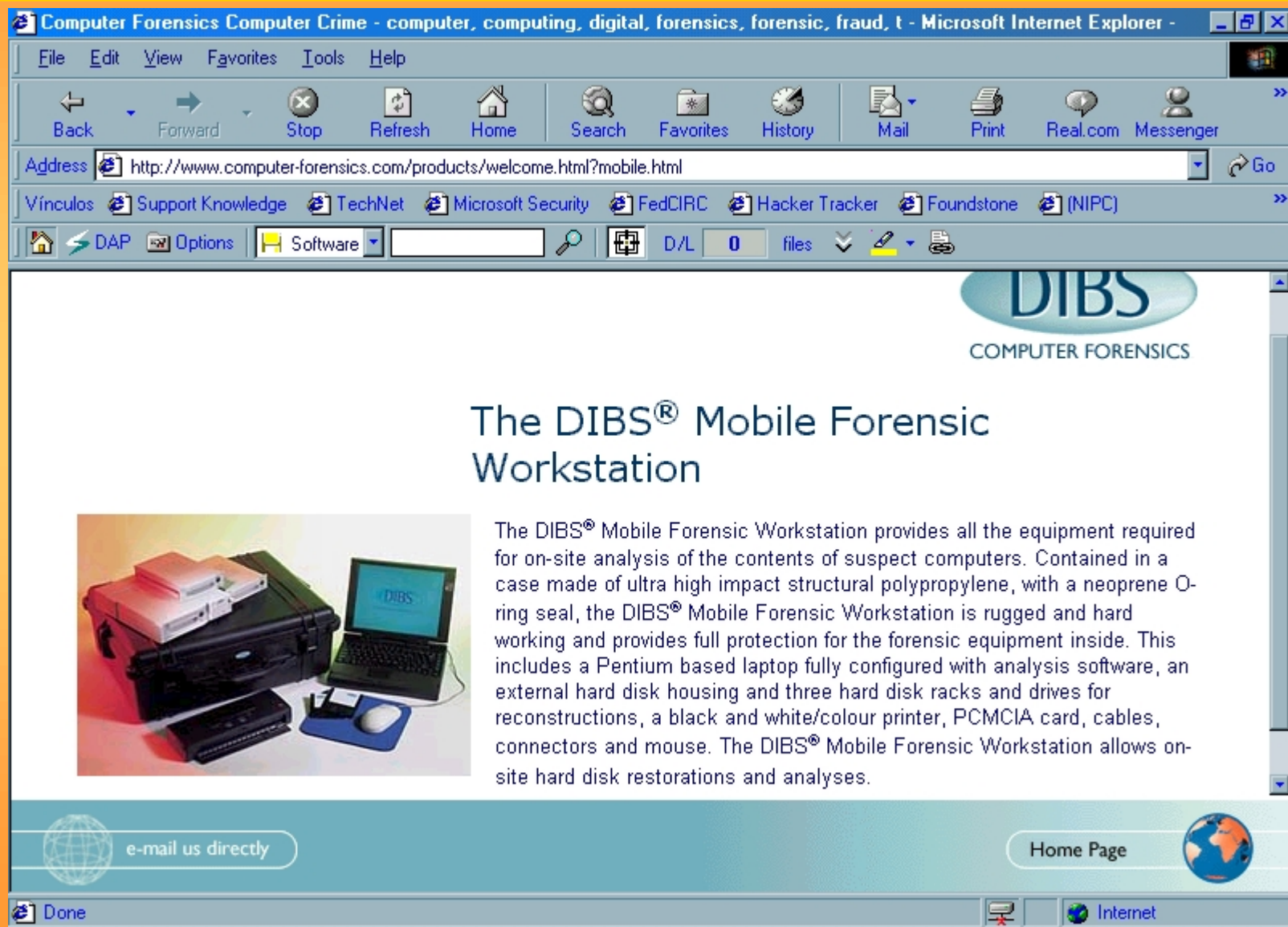
As technology develops, so the capacity for abuse and misuse increases, and computers can be associated with almost any crime, from theft and fraud to paedophilia and murder. Electronic data found on computers can provide the key to a successful investigation and prosecution. But to get access to the information, which can sometimes lay hidden, the hard disk has to be copied in such a way as not to affect or corrupt the original machine in any way.

DIBS® Portable Evidence Recovery Unit is the efficient and easy way to copy the entire contents of a computer's hard disk. It was developed after working closely with senior police officers to find a fast, powerful and reliable way to retrieve potential evidence which was admissible in a court of law.

DIBS® Portable Evidence Recovery Unit has been designed with the user in mind and works quickly and reliably to produce copies with the minimum of set-up and input from the operator. The copying process can begin after only two keystrokes from the user. The system is highly portable and is

e-mail us directly [Home Page](#)

•Herramientas - Equipamiento forense



Computer Forensics Computer Crime - computer, computing, digital, forensics, forensic, fraud, t - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail Print Real.com Messenger


Address <http://www.computer-forensics.com/products/welcome.html?mobile.html> Go

Vínculos [Support Knowledge](#) [TechNet](#) [Microsoft Security](#) [FedCIRC](#) [Hacker Tracker](#) [Foundstone](#) [\(NIPC\)](#)

DAP Options Software D/L 0 files

DIBS
COMPUTER FORENSICS

The DIBS® Mobile Forensic Workstation



The DIBS® Mobile Forensic Workstation provides all the equipment required for on-site analysis of the contents of suspect computers. Contained in a case made of ultra high impact structural polypropylene, with a neoprene O-ring seal, the DIBS® Mobile Forensic Workstation is rugged and hard working and provides full protection for the forensic equipment inside. This includes a Pentium based laptop fully configured with analysis software, an external hard disk housing and three hard disk racks and drives for reconstructions, a black and white/colour printer, PCMCIA card, cables, connectors and mouse. The DIBS® Mobile Forensic Workstation allows on-site hard disk restorations and analyses.

e-mail us directly Home Page

Done Internet


- Herramientas - Equipamiento forense



• Herramientas - Boletín electrónico del FBI

Acrobat Reader - [2001-14.pdf]

Archivo Edición Documento Ver Ventana Ayuda



**National Infrastructure Protection Center
CyberNotes**

Issue #2001-14 July 16, 2001

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malware scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at <http://www.nipc.gov>.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between June 21 and July 12, 2001. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized the vulnerability or an exploit script is known to exist. Software versions are identified if known. This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site. Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in this update will appear in italicized colored text. Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
AcLogic	Windows 35/38/486/NT 3.5/5.0/4.0/2000	Client 1P 0.98b	A buffer overflow vulnerability exists when the HTTP command is not followed by a very long string of characters, which could let a remote malicious user execute arbitrary code or gain SYSTEM privileges.	No workaround or patch available at time of publishing.	Client 1P's HTTP Command Buffer Overflow	High	Bug discussed in newsgroups and websites.

* Rating: July 4, 2001.

NIPC CyberNotes #2001-14 Page 1 of 23 07/16/2001

60% 1 de 23 215.9 x 279.4 mm