POLICIA FEDERAL ARGENTINA

DIVISION SEGURIDAD INFORMATICA FEDERAL

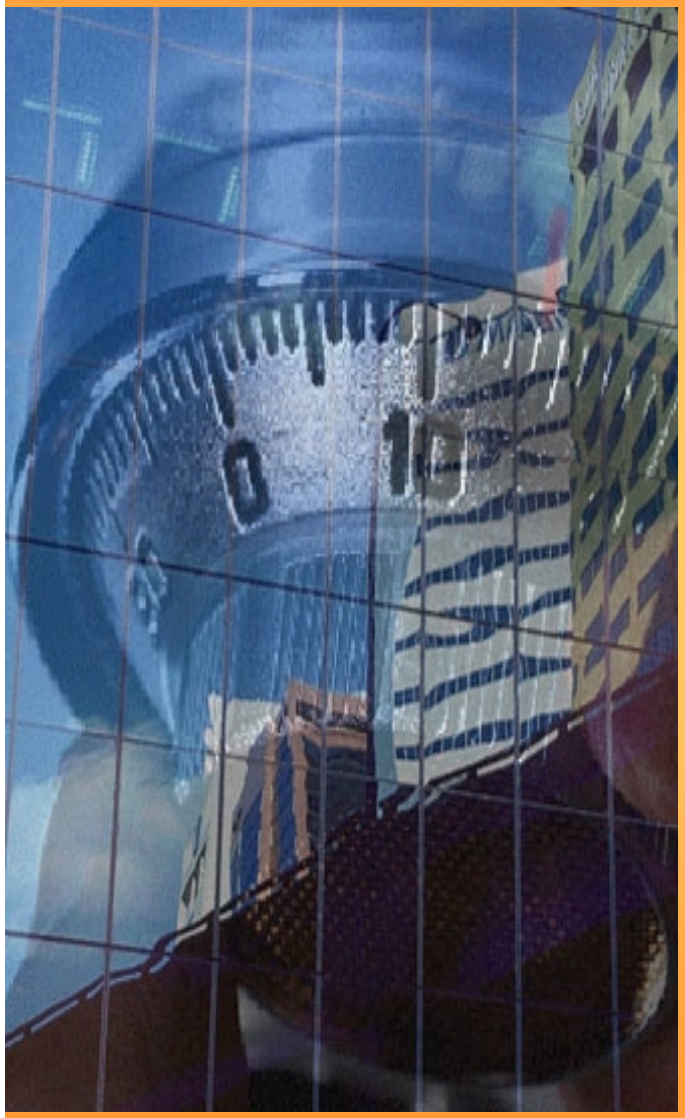
ANALISIS FORENSE DE COMPUTADORAS

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.**

Al Servicio de la Comunidad



Analizando los despojos de un incidente de Seguridad informática.

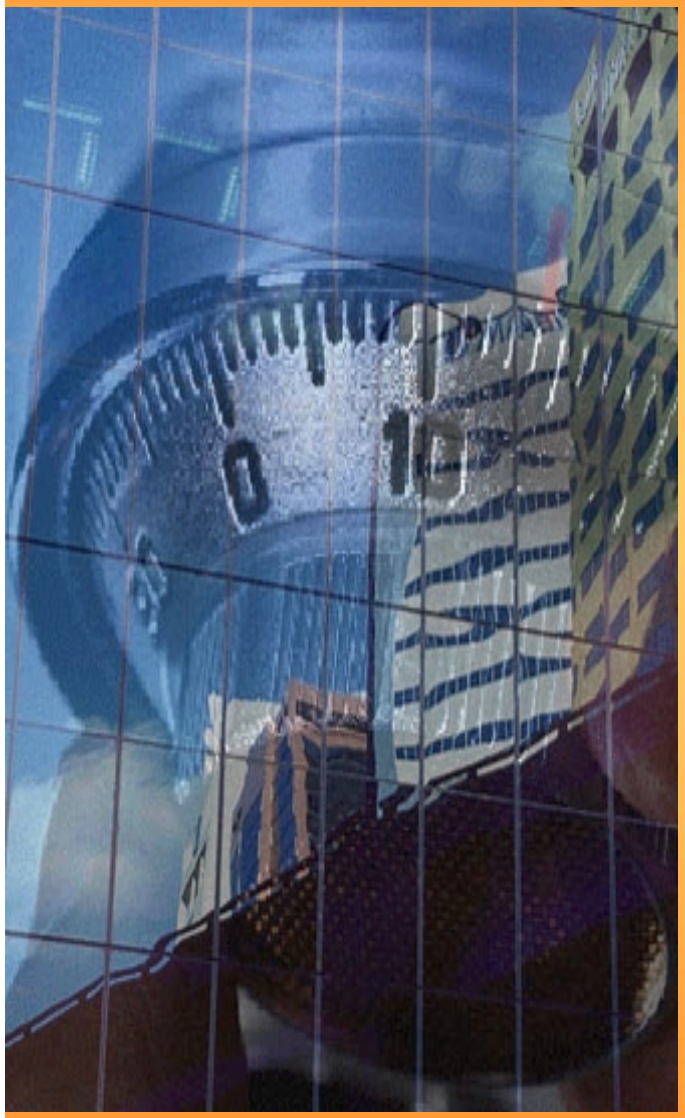
Que queremos decir con un incidente de seguridad.

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.

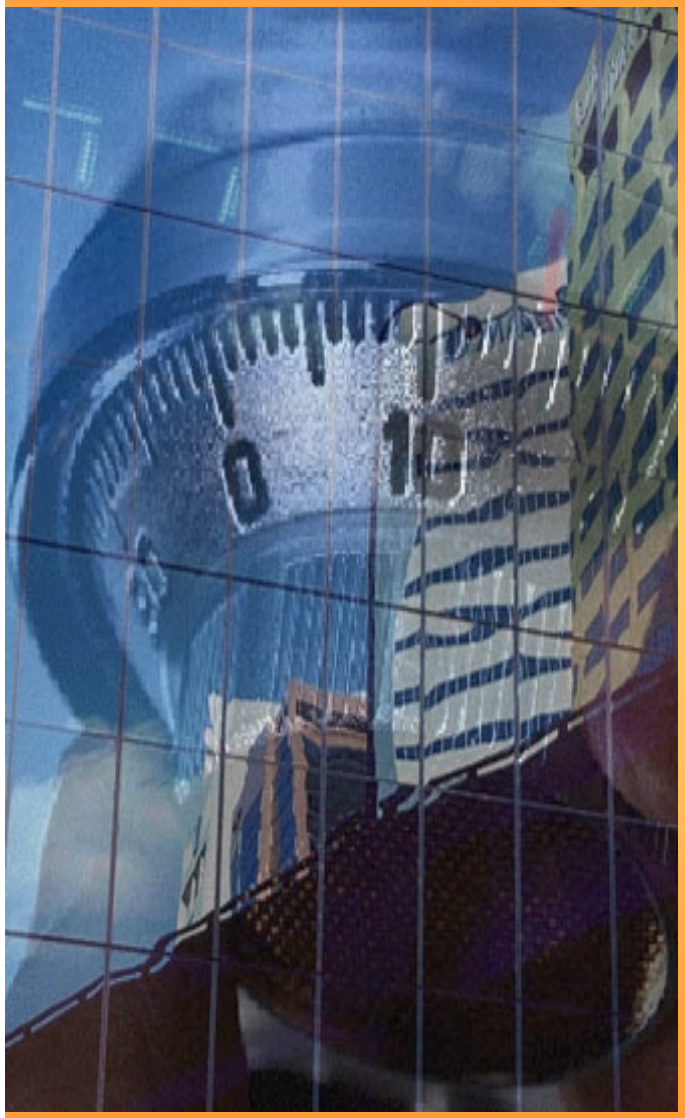
- Procesando datos forenses.

  Recolección.

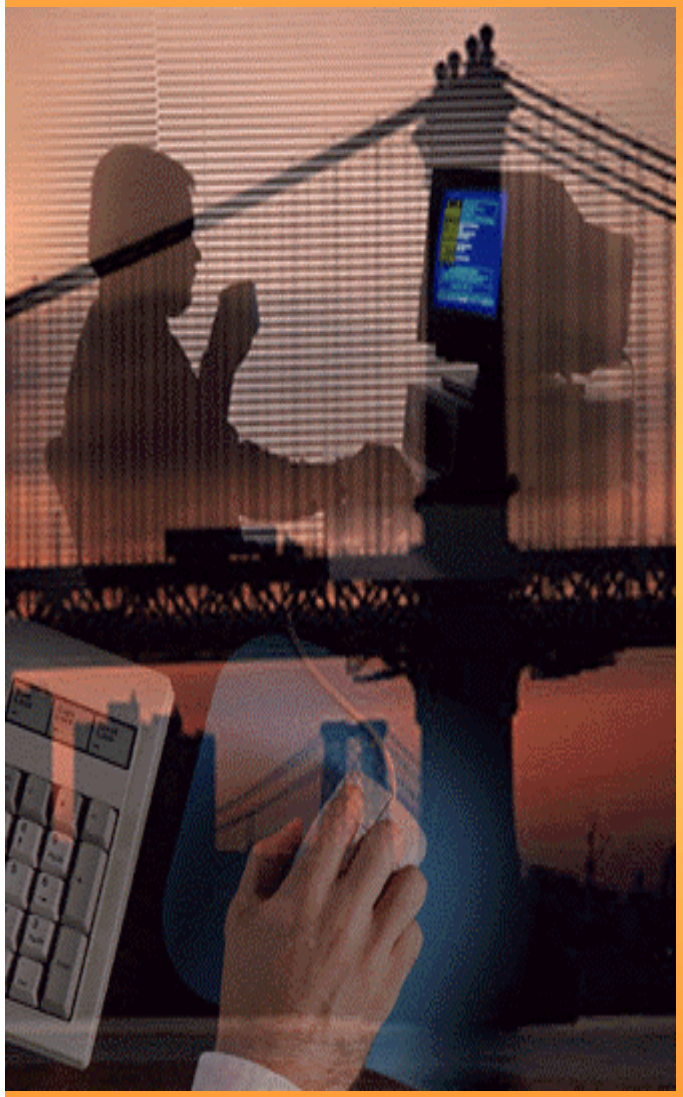
- Técnicas de recolección.

- Herramientas y Técnicas de análisis.

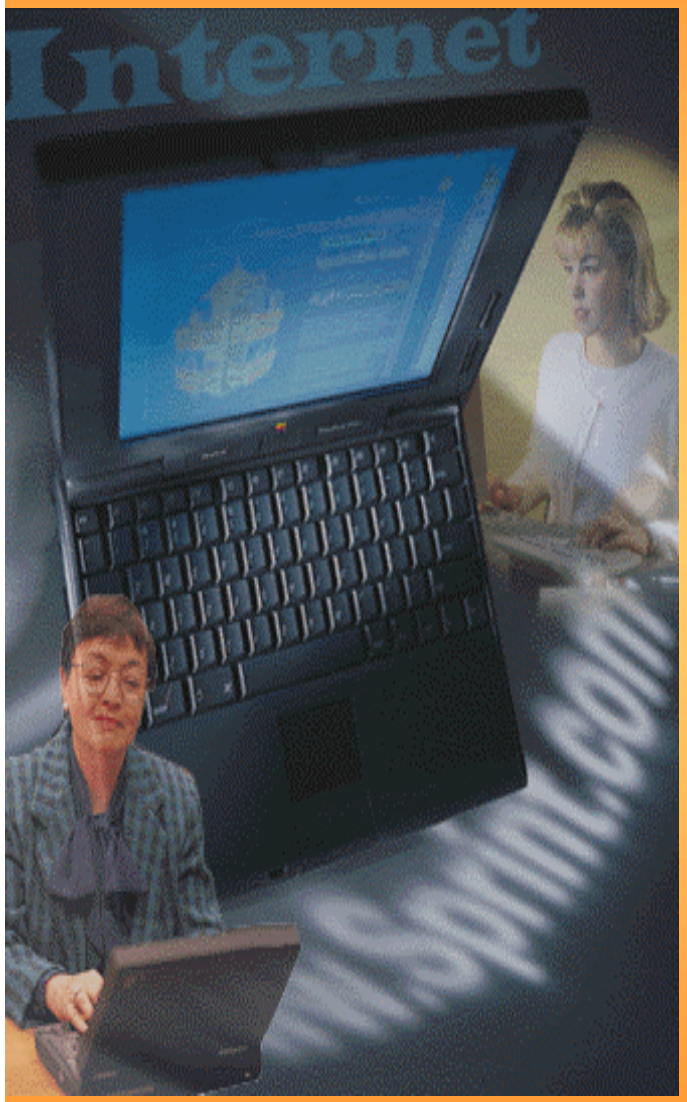
- Encadenamiento



- **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.**

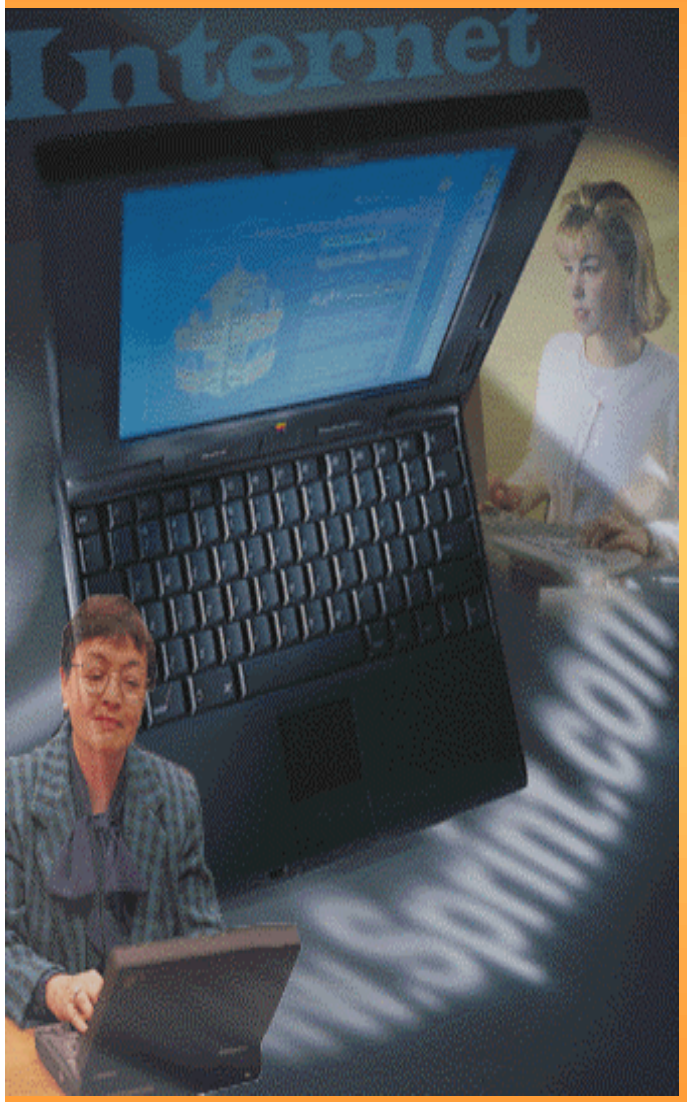


- Iniciando la Investigación.
- Analizando el incidente.
- Analizando la evidencia y preparando su presentación.
- Asegurando o preservando la escena virtual del crimen.
- Mantener a todo el mundo alejado de la computadora investigada.
- Recolectando y preservando evidencia.

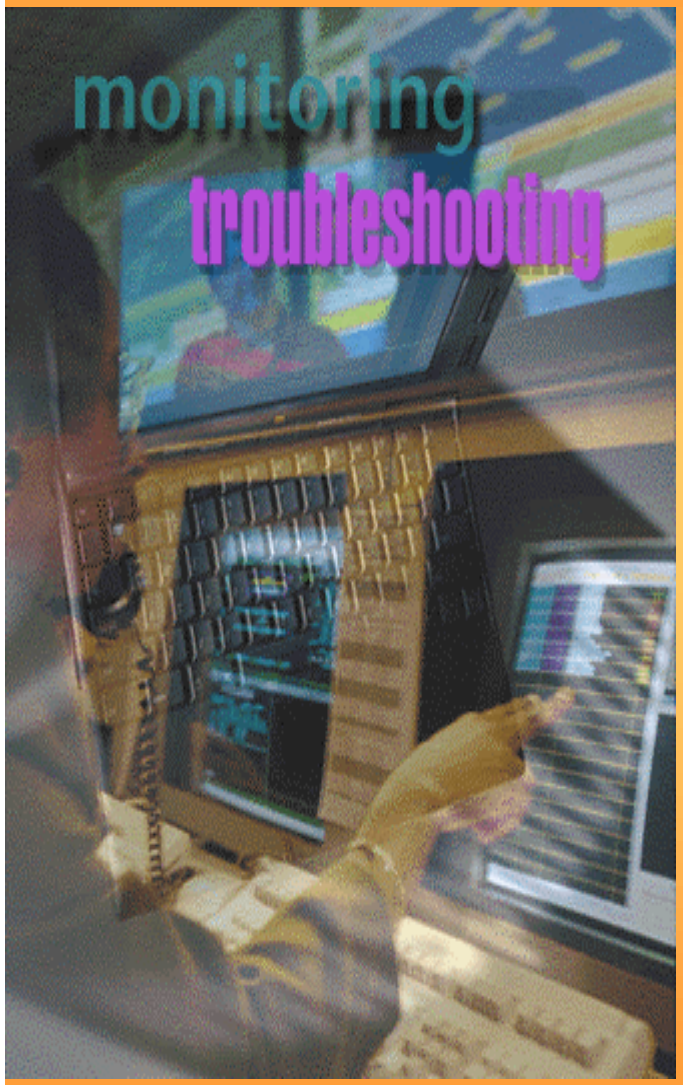


- Determinando si ha tenido lugar un delito.
- Creer en nuestros indicadores.
- Usando herramientas para verificar que ha ocurrido un delito.
- Recuperando datos de discos dañados
- Recuperando Passwords
- Recuperación de Passwords física.
- Cracking de Passwords.

Al Servicio de la Comunidad

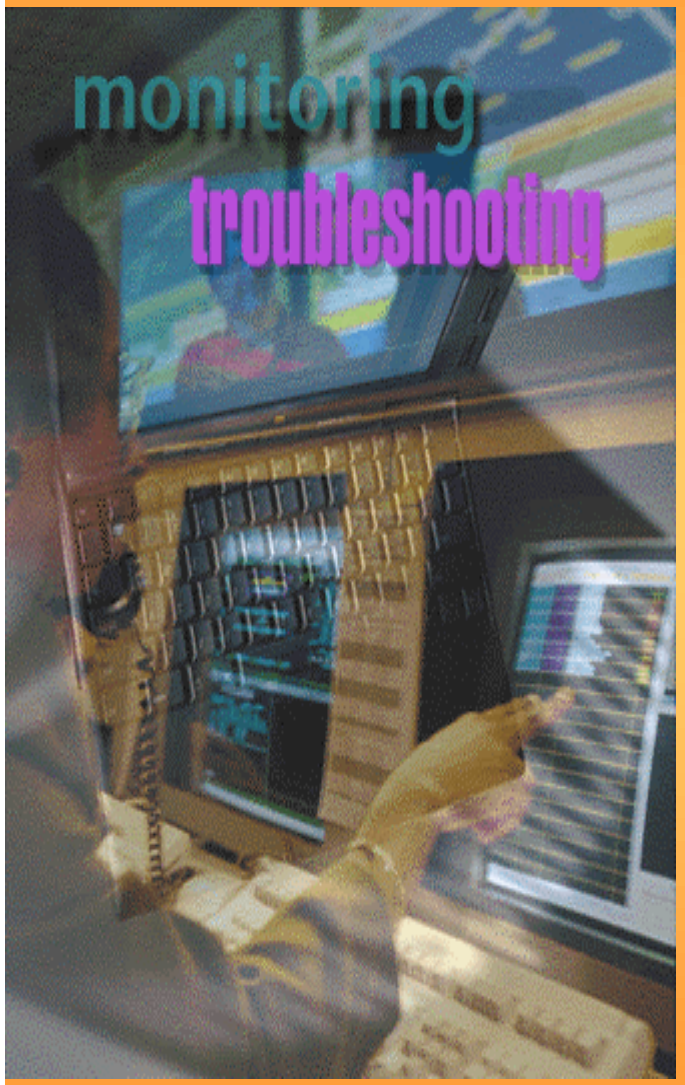


- **Infiriendo.**
- **Examinando LOGS.**
- **Las herramientas.**

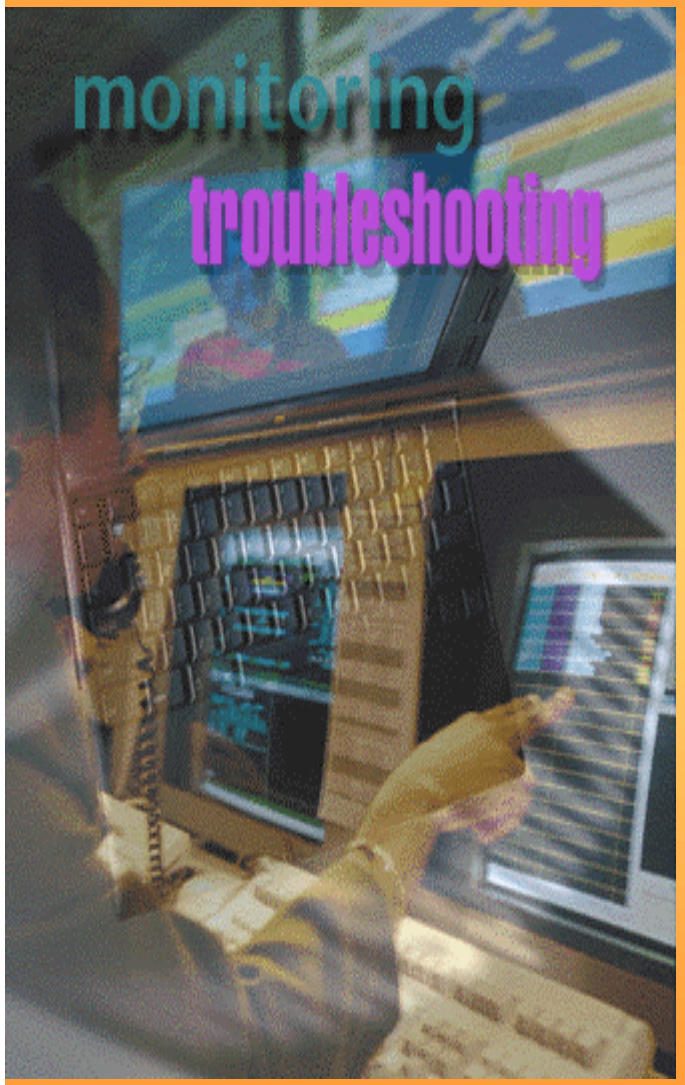


- **Preservando Evidencia.**
- **Conceptos Básicos.**
- **Recolección de evidencia sin perdida de tiempo y cadena de custodia.**
- **Marcando evidencia con un Hash MD-5 y encriptación con PGP.**
- **CRCMD5**
- **Sellando evidencia.**
- **Resumen.**

Al Servicio de la Comunidad

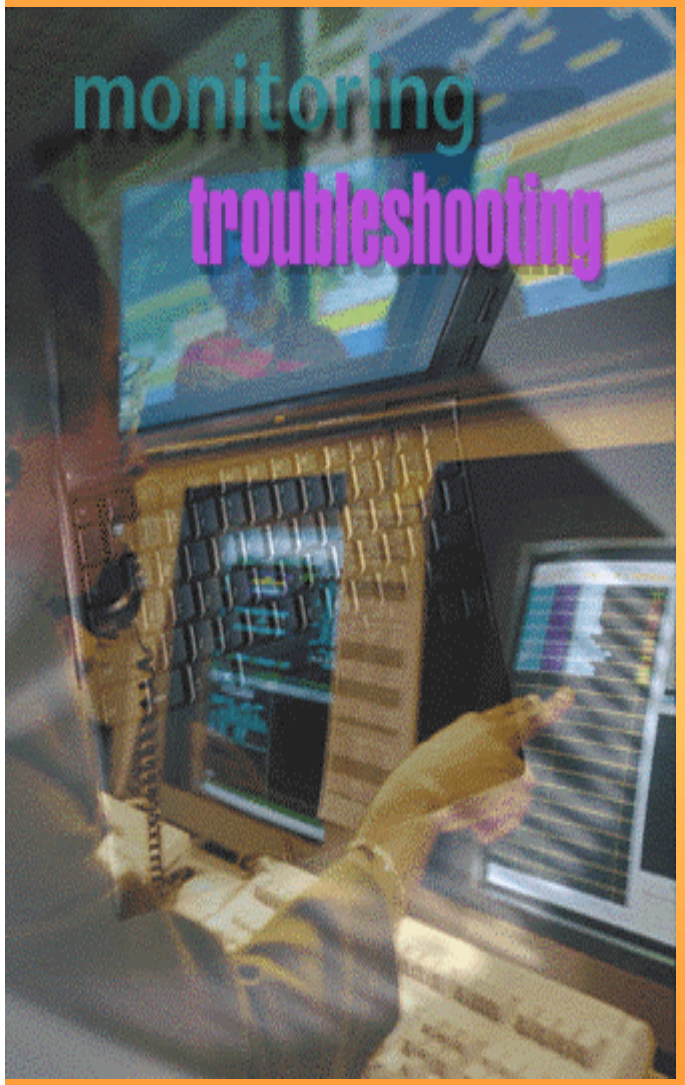


- **Recolectando evidencia.**
- **Primeros pasos.**
- **Usando herramientas para tomar una imagen espejo de un disco.**
- **Tomando un inventario de un disco rígido usando Filelist.**
- **Buscando información oculta.**
- **El filtro inteligente Filter_1 V.4.1**
- **IP filter V.2.2**



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

Al Servicio de la Comunidad



- **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

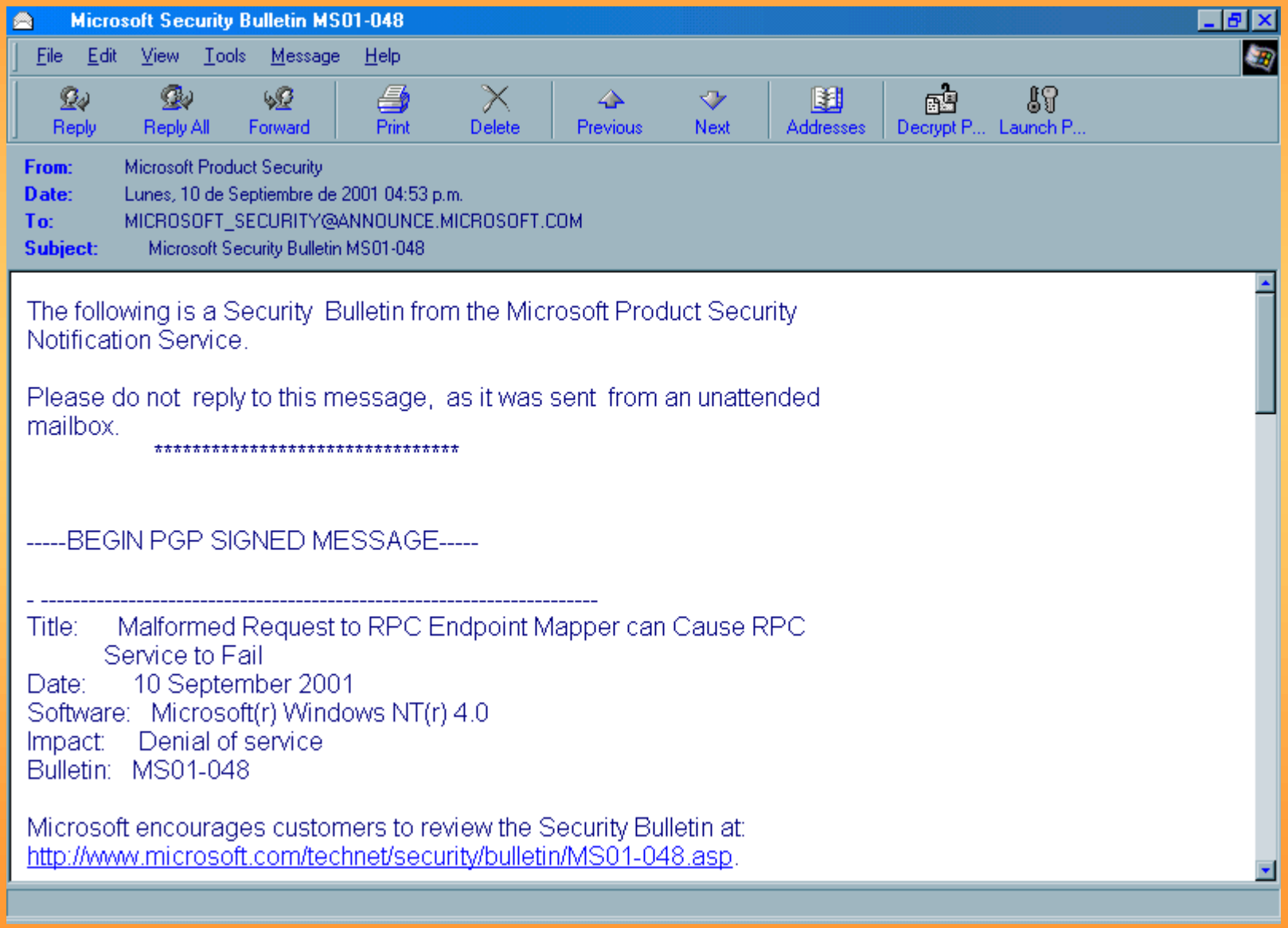
- Dirección IP Remitente
- E-Mail del emisor
- ID usuario
- Día, hora y zona horaria
- Petición realizada
- Códigos de sistema

•Análisis de LOGS - Logs de Aplicaciones.

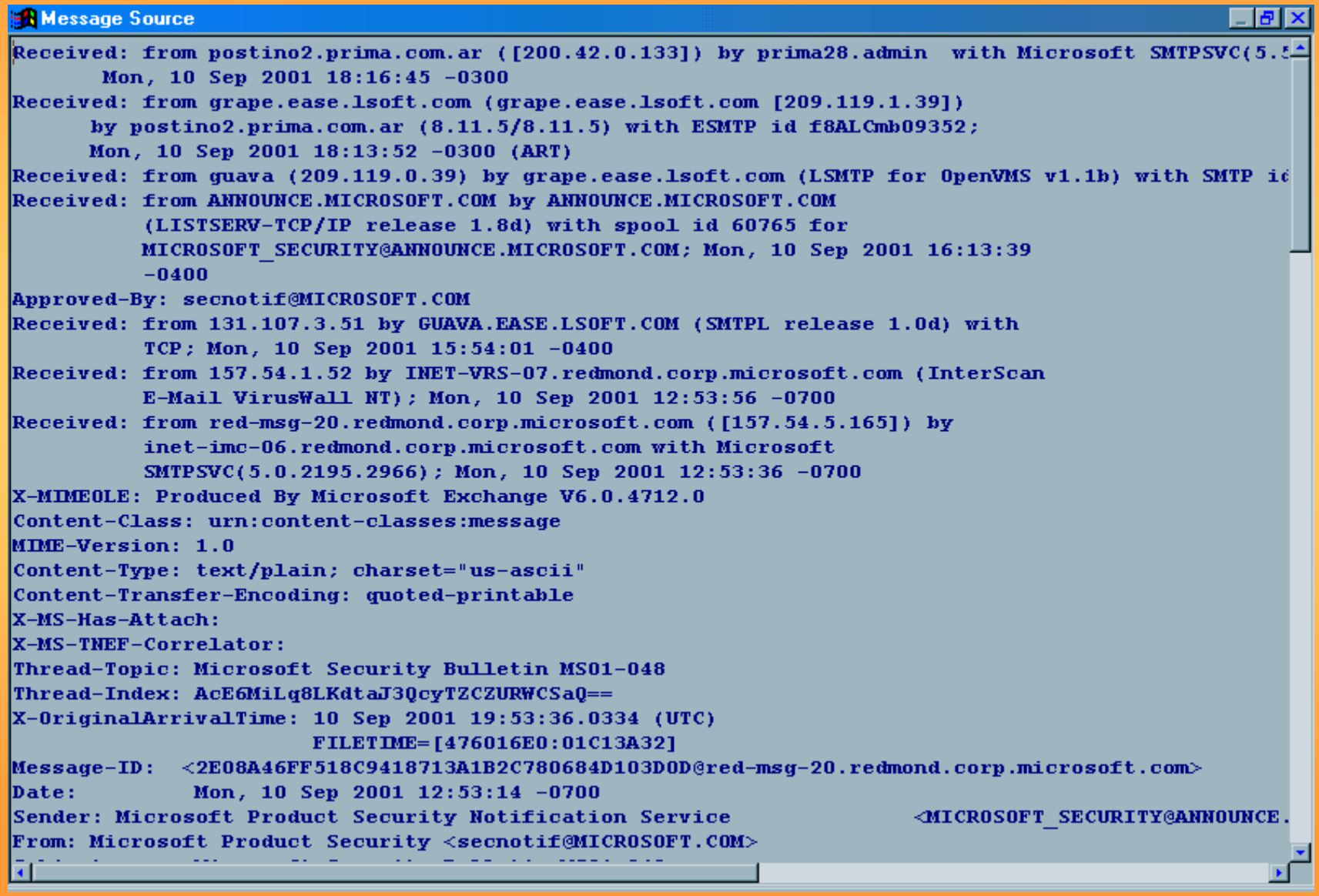
Mensajes de Correo Electrónico

- 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.**



- **Logs de aplicaciones - Mensajes de email.**

Message Source

```
Received: (from cisiar@localhost)
      by w1418.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 w1418.hostcentric.net (8.10.1/8.9.0) with ESMTP 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 QQlgyf21204
      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: <GKEALPJLNGNNMBCGIOMOCEBMCAAA.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 IMO, 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: T1h!!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

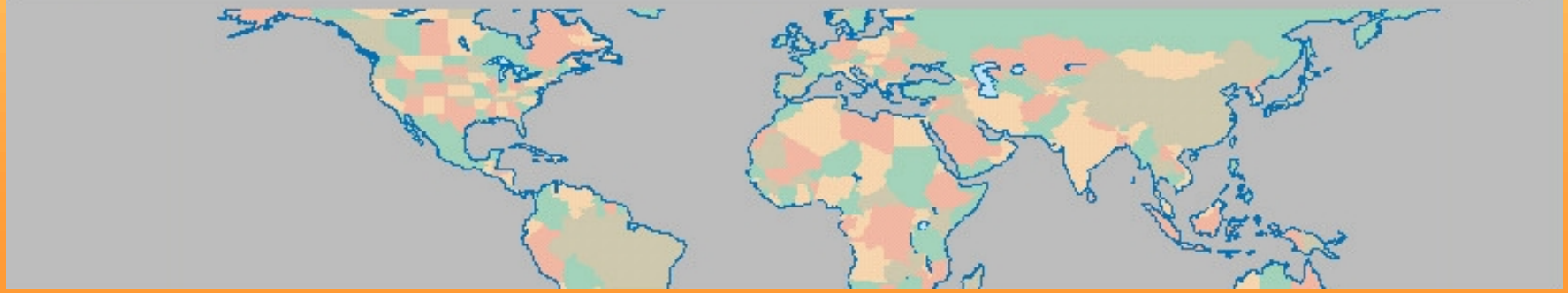
•Herramientas - Visual Route.

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.	0 6056
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.

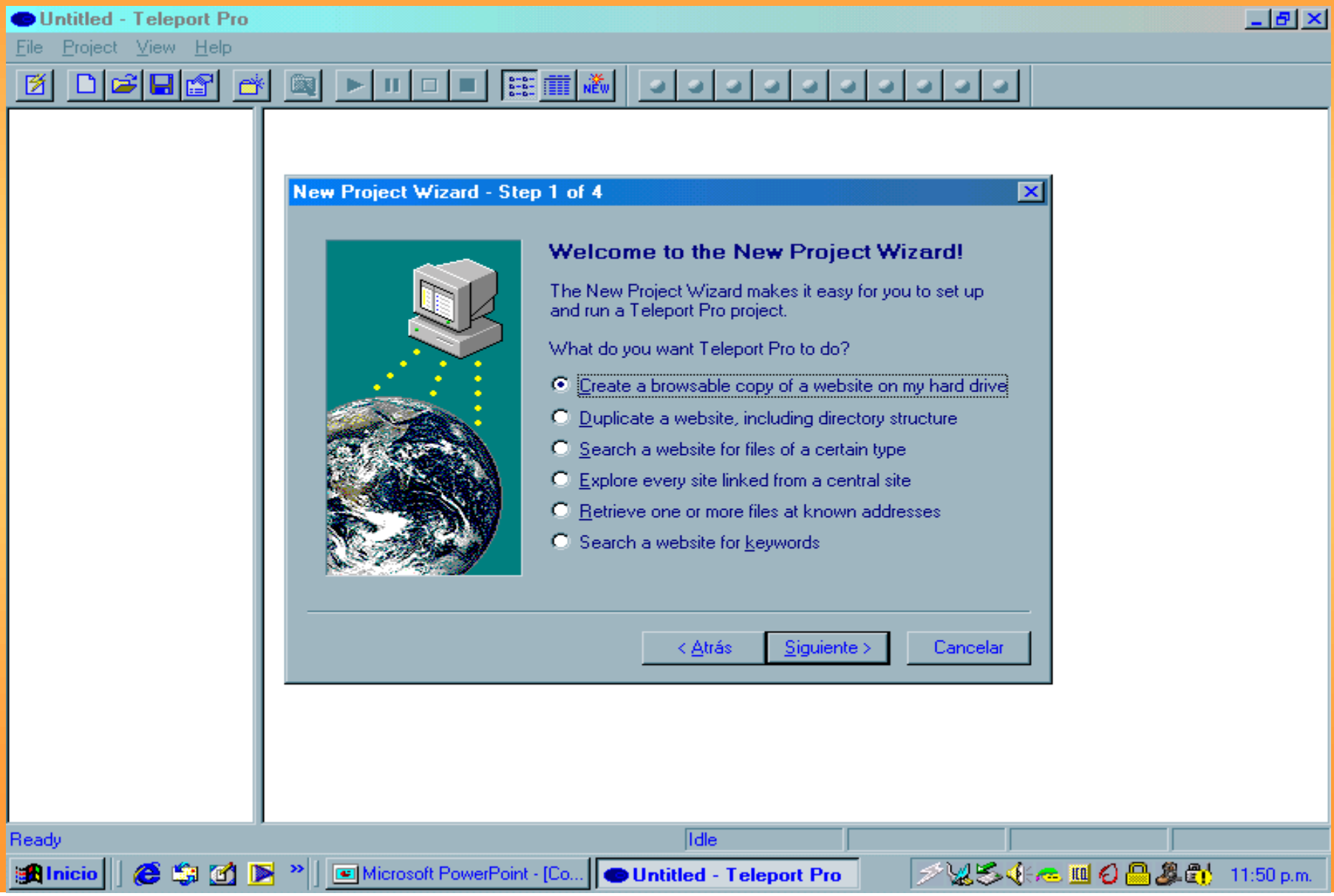
Report for centauro.interar.com.ar [200.47.136.248]

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.

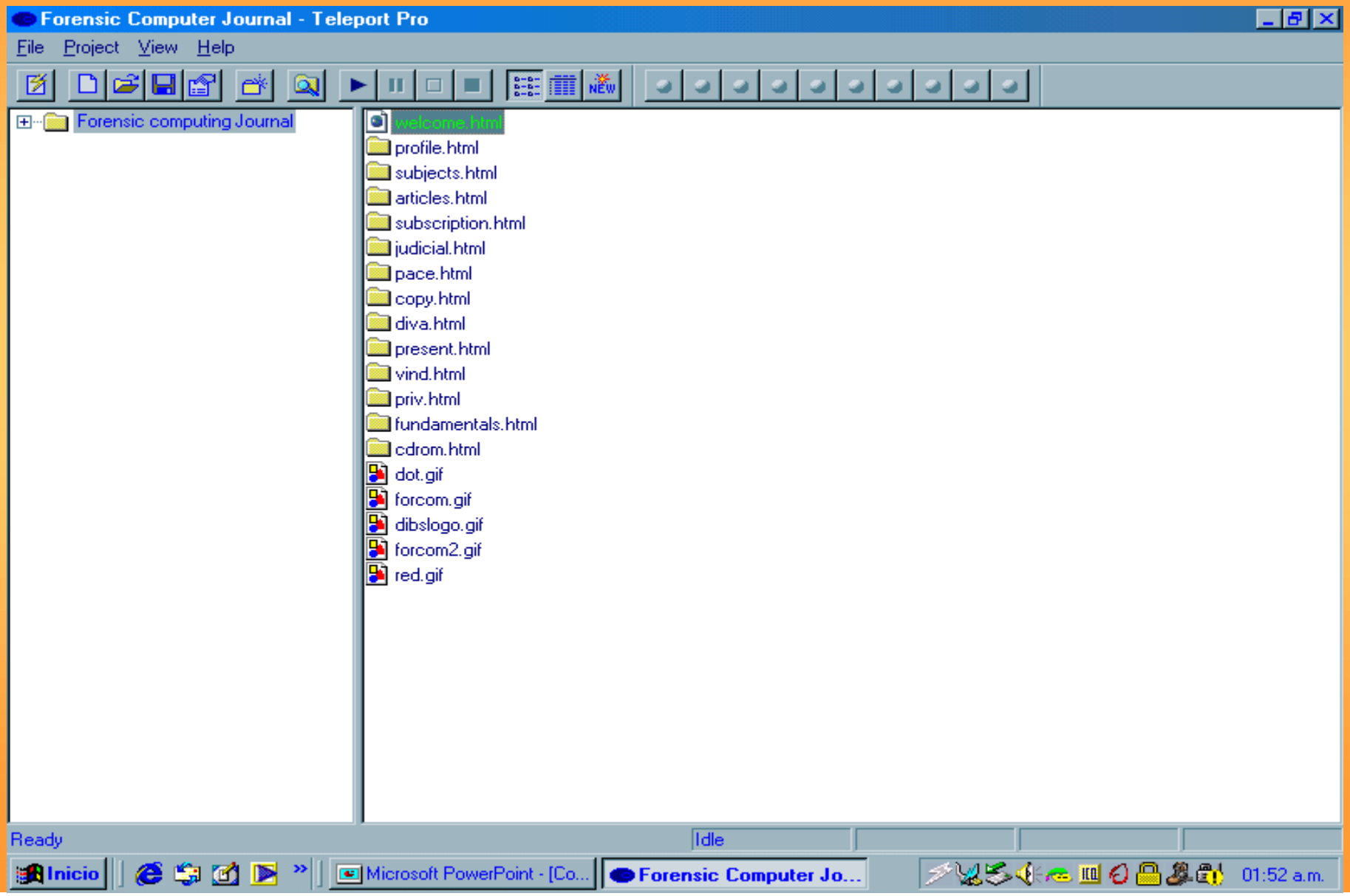
Hop	IP Address	Node Name	Location	Network	Graph
0	200.61.130.236	host236.200.61.130.ifxnw.com.ar	*	IFX Networks Argentina S.R.L.	0 344
1	200.61.128.23	host23.200.61.128.ifxnw.com.ar	Buenos Aires, Argentina	IFX Networks Argentina S.R.L.	
2	200.61.128.1	host1.200.61.128.ifxnw.com.ar	Buenos Aires, Argentina	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.

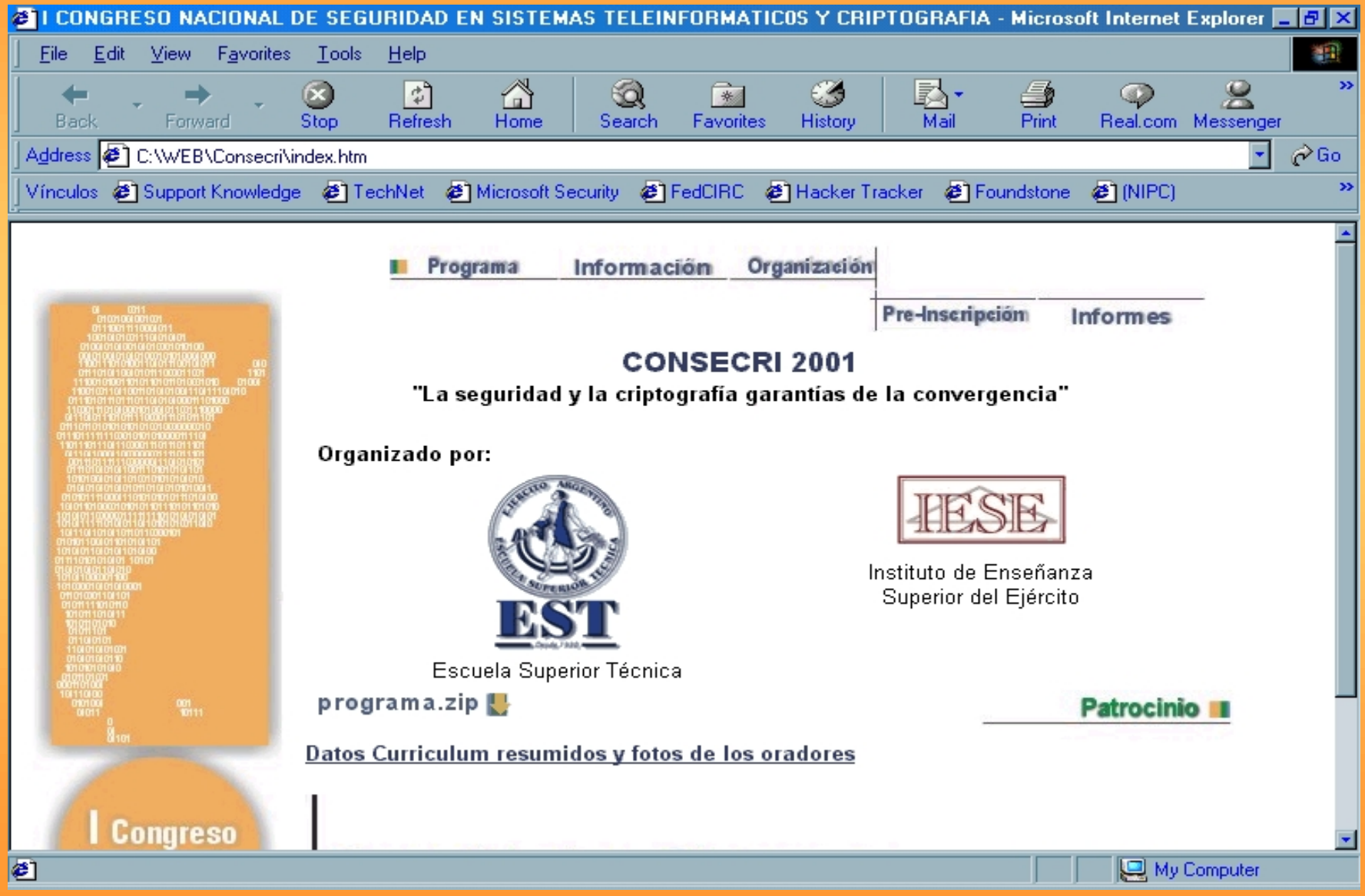


•Herramientas - Teleport Pro.

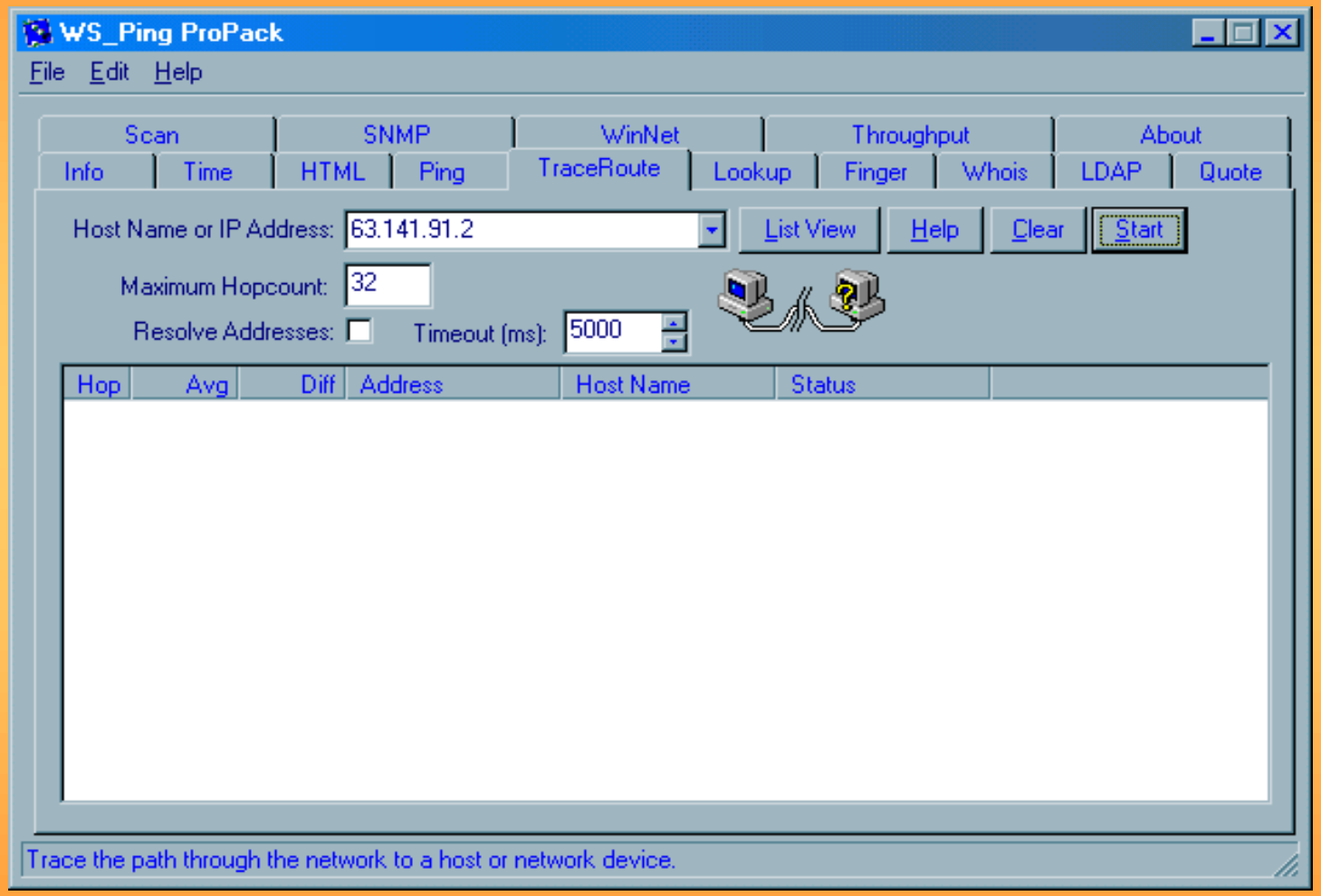


•Herramientas - Teleport Pro. + I.E. 5.5

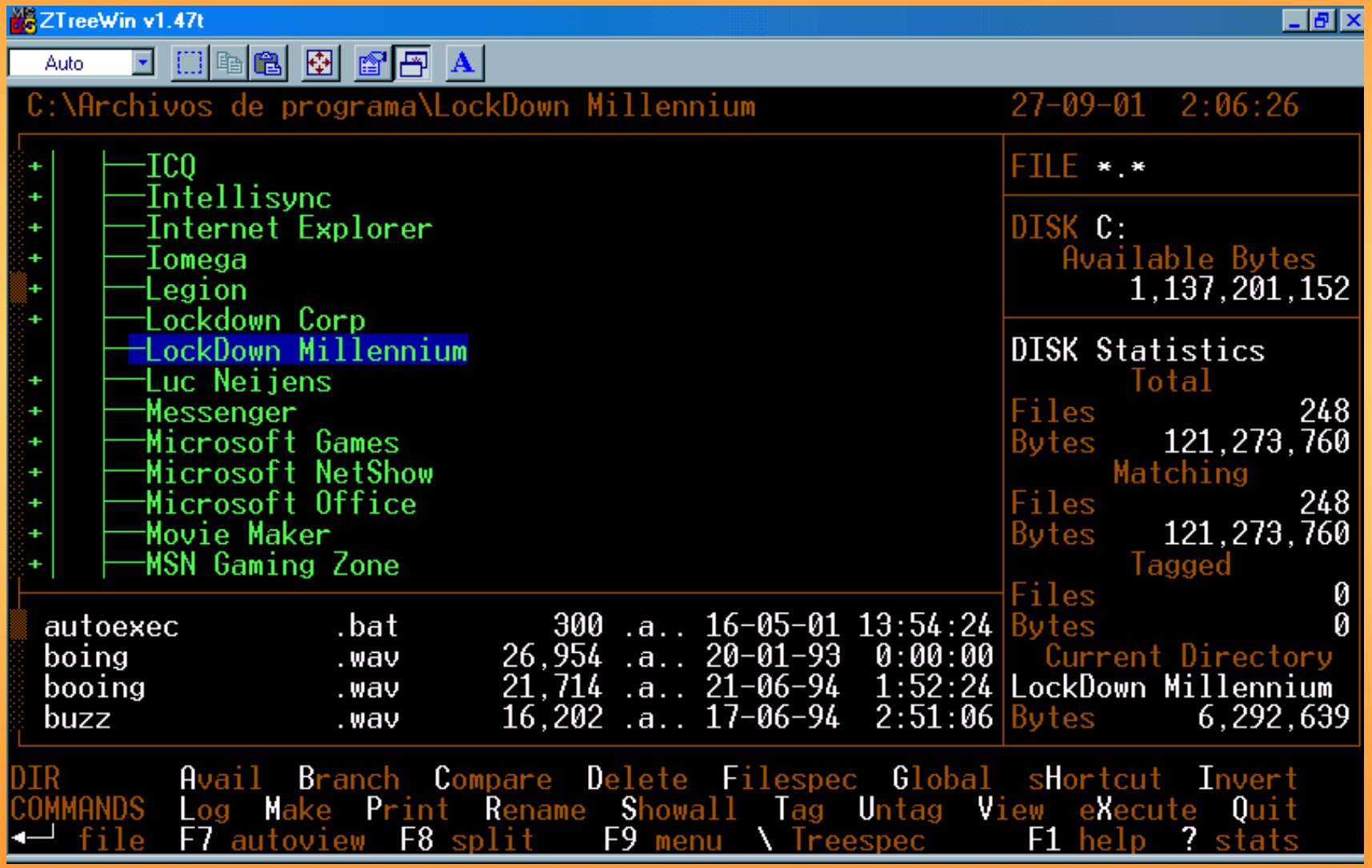
•Herramientas - Teleport Pro. + I.E. 5.5



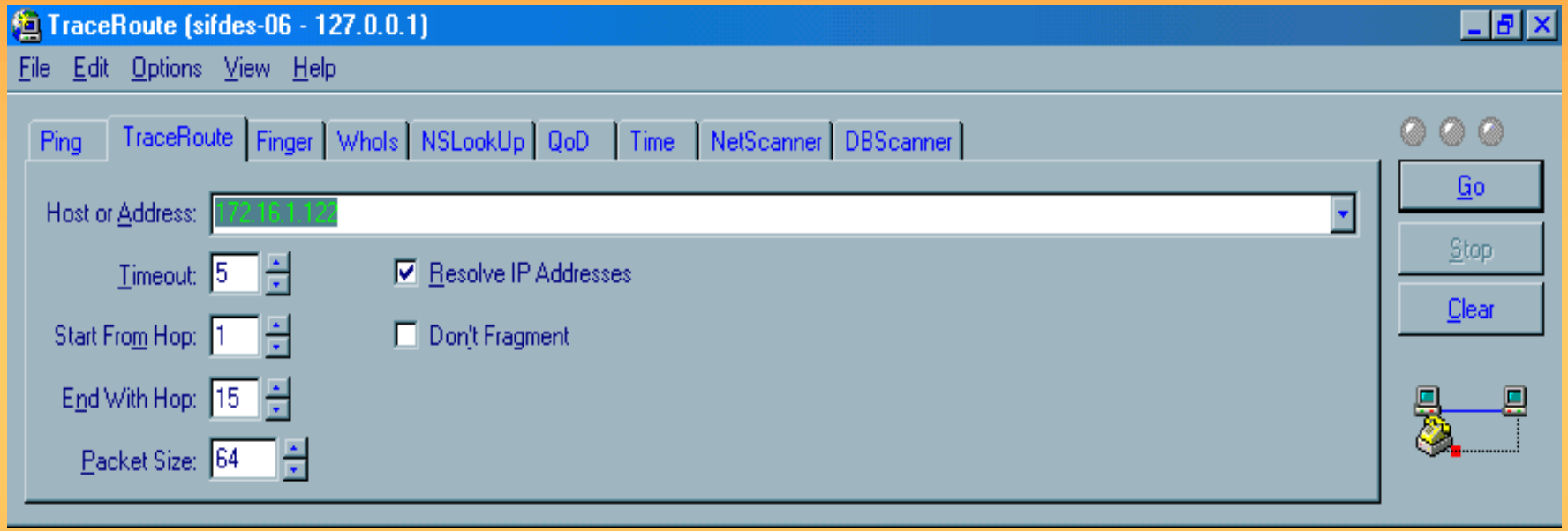
- **Herramientas - WS_Ping ProPack.**



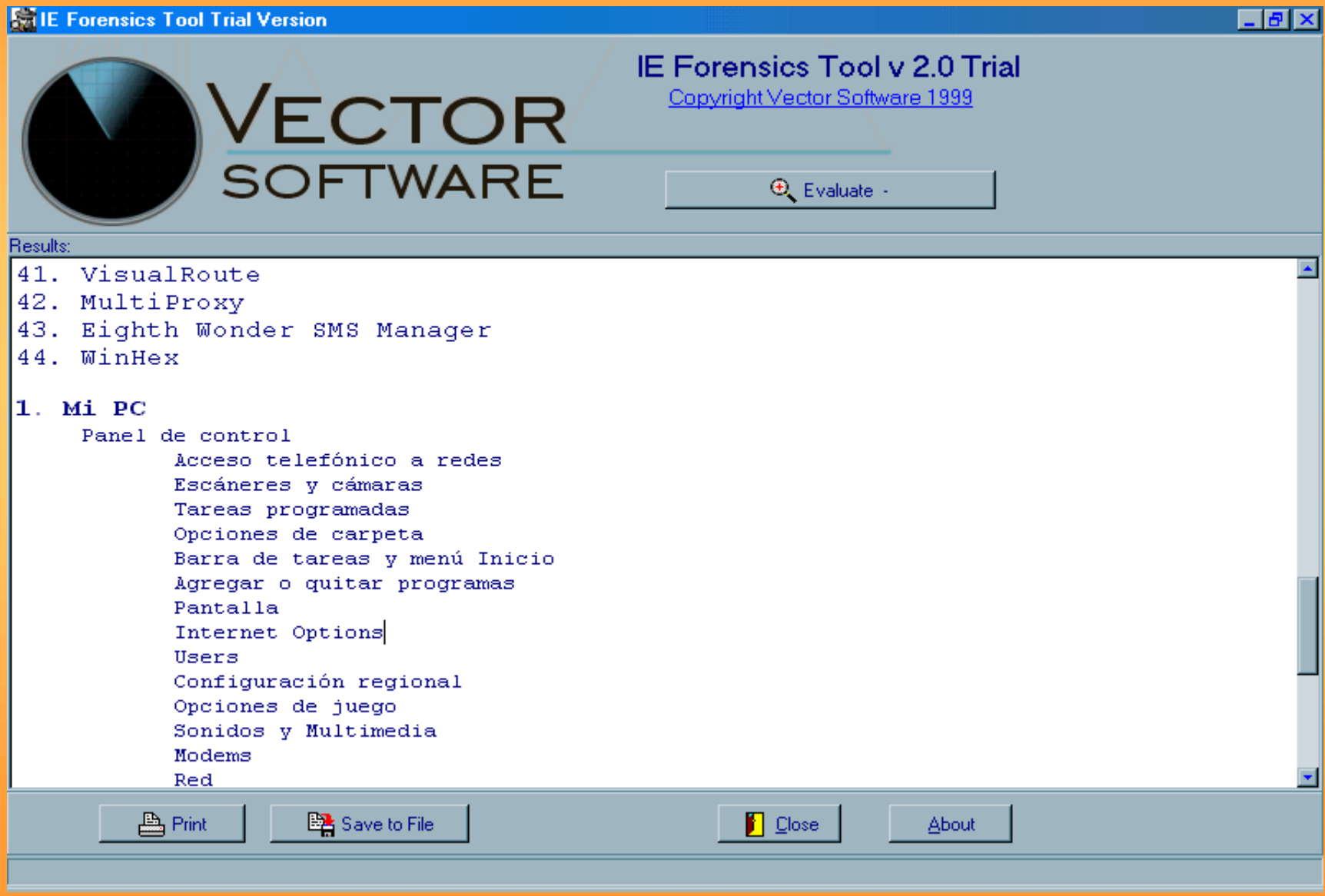
•Herramientas - ZTreeWin v1.47



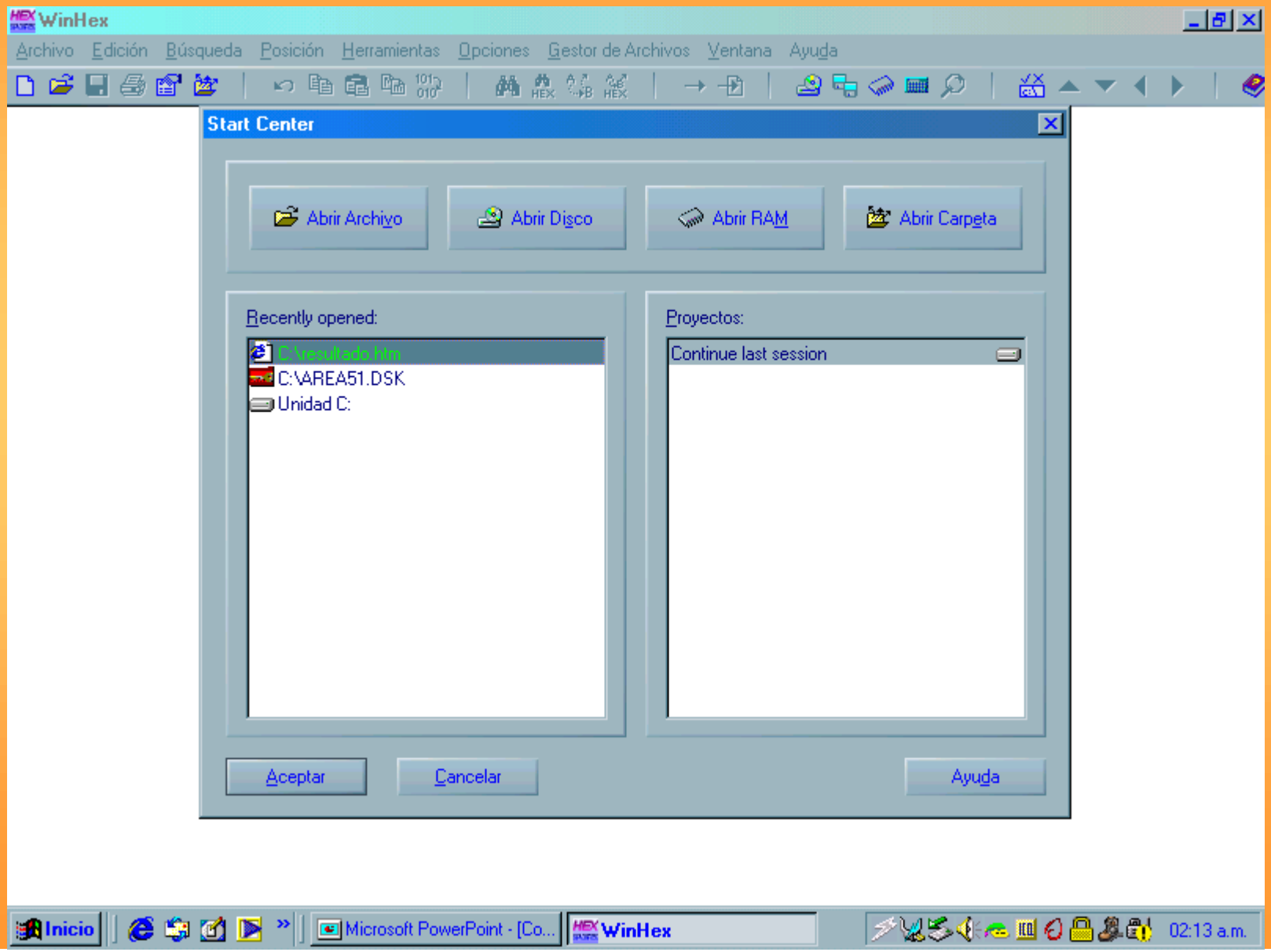
•Herramientas - CyberKit



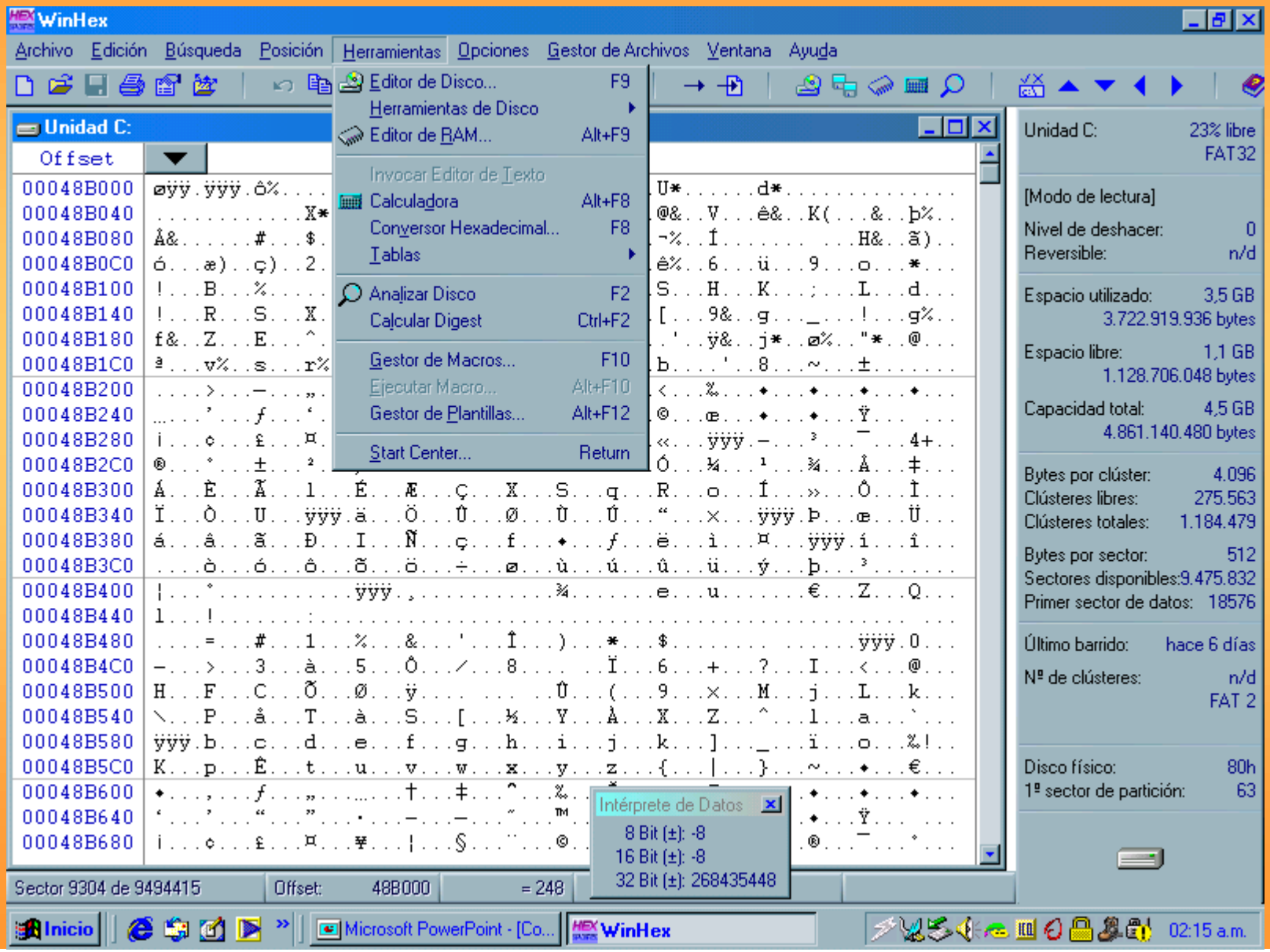
•Herramientas - IE Forensic Tool v2.0



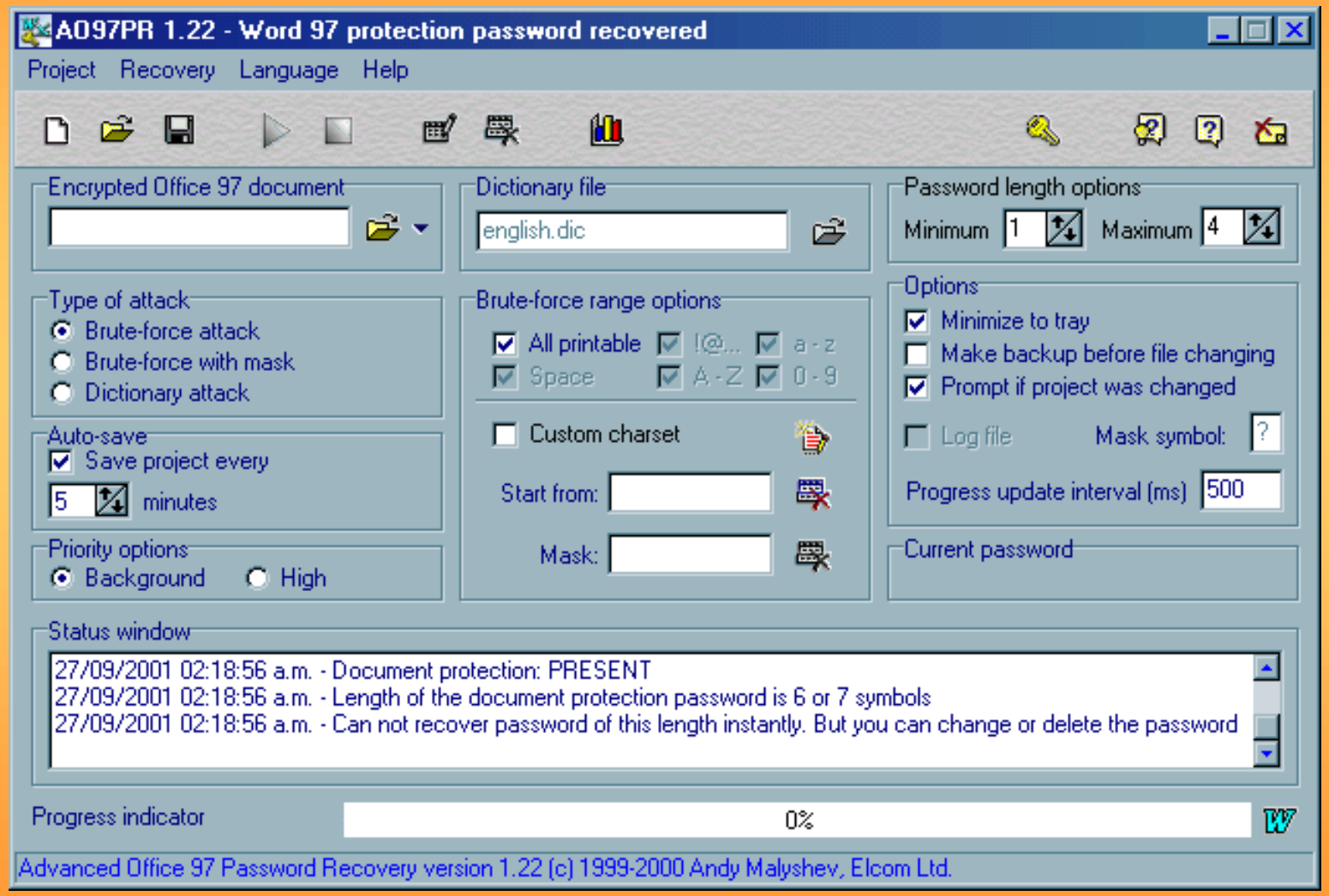
•Herramientas - WinHex



•Herramientas - WinHex



•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

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?peru.html Go

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

DAP Options Software D/L 0 files

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

Internet

•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