

Introducción a las investigaciones de delitos informáticos

Laboratorio de Delitos Informáticos
Departamento de Justicia de los
Estados Unidos

Sección de Delitos Informáticos y Propiedad Intelectual



Orden de la presentación

- Introducción
- Tipos de delitos que involucran computadoras
- Dónde encontrar pruebas informáticas
- Preparándose para revisar e incautar computadoras



Introducción

- El laboratorio de delitos informáticos ofrece todo el apoyo técnico necesario para resolver un caso
 - Técnicas forenses informáticas tradicionales
 - Análisis de redes
 - Desarrollo de bases de datos
 - Cualquier otra cosa que sea necesaria



Tipos de delitos que involucran computadores

- Una computadora puede ser utilizado para cometer un delito, o para guardar pruebas sobre un delito
- Pornografía infantil
- *Hacking*
- Casi cualquier otro delito
 - Pandillas: usan computadoras para comunicarse
 - Drogas: usan computadoras para rastrear ventas, negocios
 - Otros



Dónde encontrar pruebas informáticas

Incautar los elementos especificados en la orden de registro.

- Computadoras, portátiles, equipos de redes (concentradores e interruptores [*switches*])
- Periféricos: CD-R's, DVD-R's, cámaras digitales, PDA's
- Medios externos: CD's, discos floppy, discos USB miniatura
- Notas de papel, documentación y manuales, notas Post-It

Llevar un registro del equipo informático y los periféricos antes de removerlos.

- Fotos digitales, diagramas

Fotos digitales de toda la casa, incluyendo las alcobas, los baños, y las zonas exteriores (para comparar luego con las imágenes que puedan llegar a ser recuperadas de la computadora).



Tipos de medios electrónicos

- Computadoras de escritorio (*desktops*) a servidores





Variedad de medios



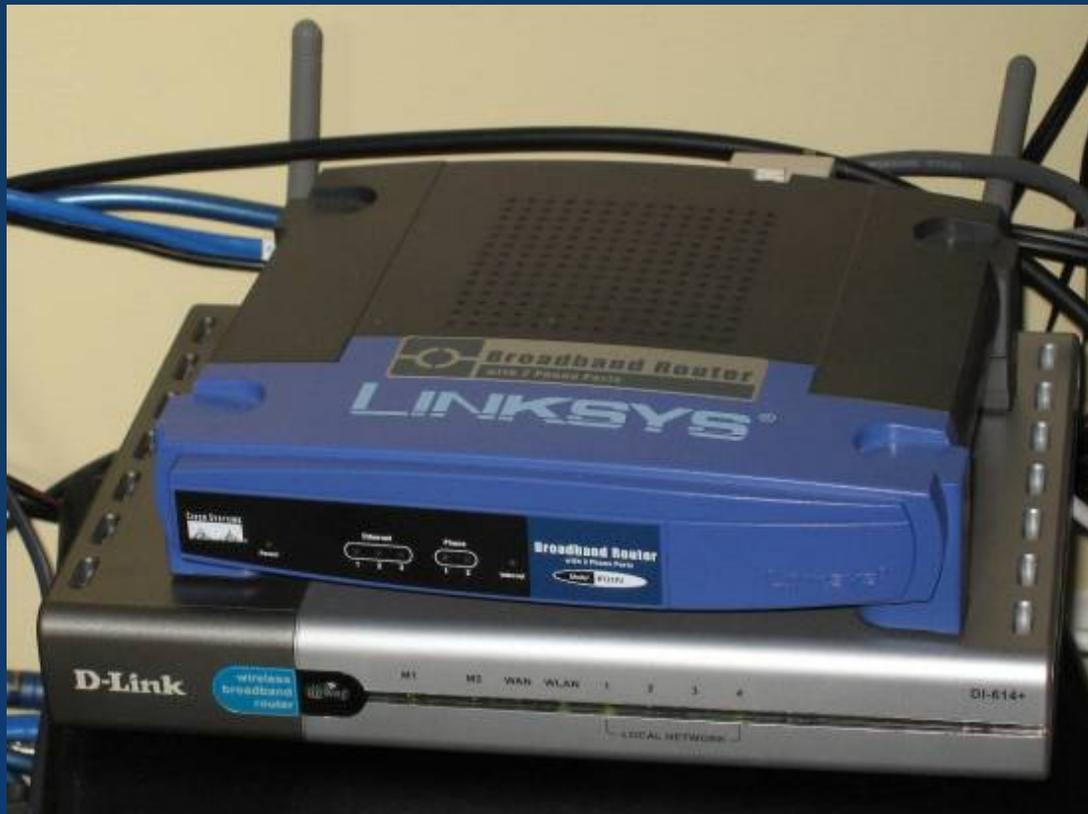


Variedad de medios





Pero esperen: hay más





iPods

- Los iPods se están volviendo muy populares. Están apareciendo por todos lados.
- Son más que reproductores de música: son dispositivos de almacenamiento.





¿Qué hay en esos iPods?

- Música
- Videos
- Listas de contactos
- pr0n
- Calendarios
- pr0n
- Apuntes
- Pr0n
- Cualquier cosa



Teléfonos celulares



Ranura de tarjeta SD

- Los teléfonos celulares pueden contener:
 - Imágenes
 - Información de llamadas
 - Directorios telefónicos
 - Tarjetas SD de teléfono celular





Impresoras

- La mayoría de los investigadores ni siquiera registrará una impresora.
- Las impresoras pueden contener todo tipo de información que a menudo es pasada por alto.
 - ¿La impresora tiene un disco RAM?
 - ¿Tiene un disco duro?
 - ¿Una interfaz web?
 - ¿Registros de eventos?
 - ¿Registros de trabajos?
 - ¿Horarios de trabajos?
 - ¿Hay datos volátiles o no-volátiles?



Menús del LCD de la impresora



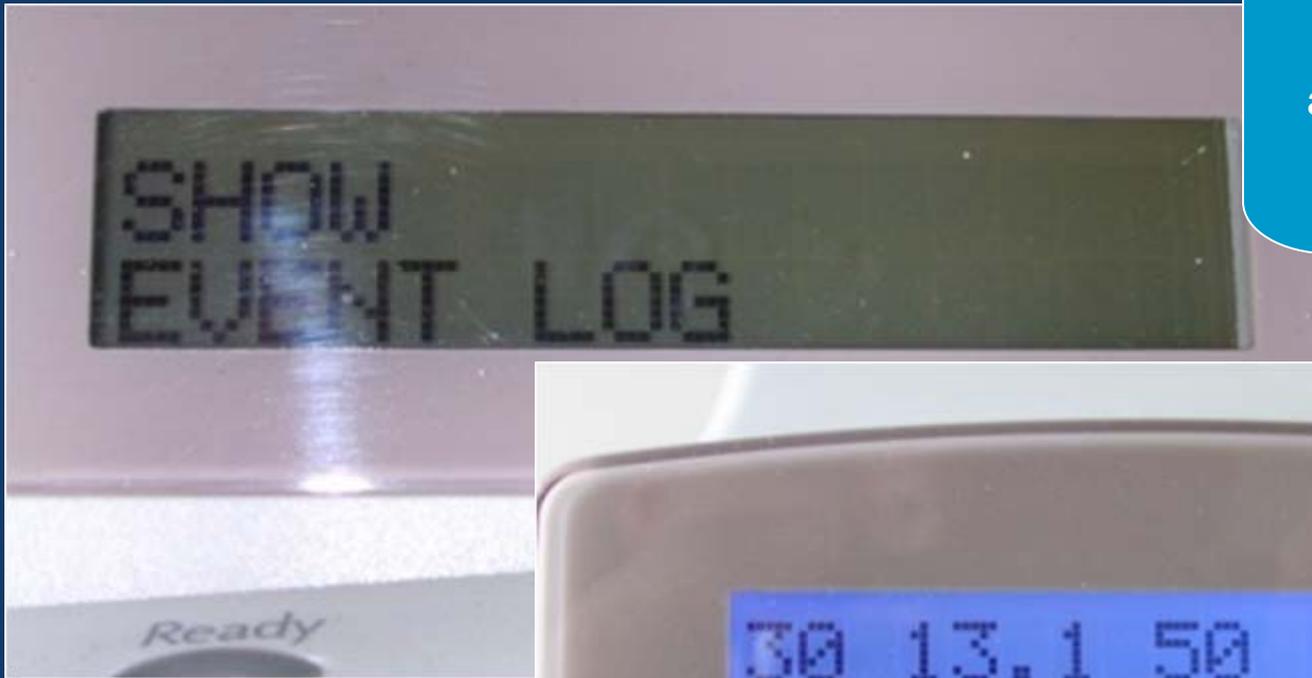
El menú de información de HP es la puerta de entrada a todo tipo de pruebas ocultas...

... como el registro de eventos...

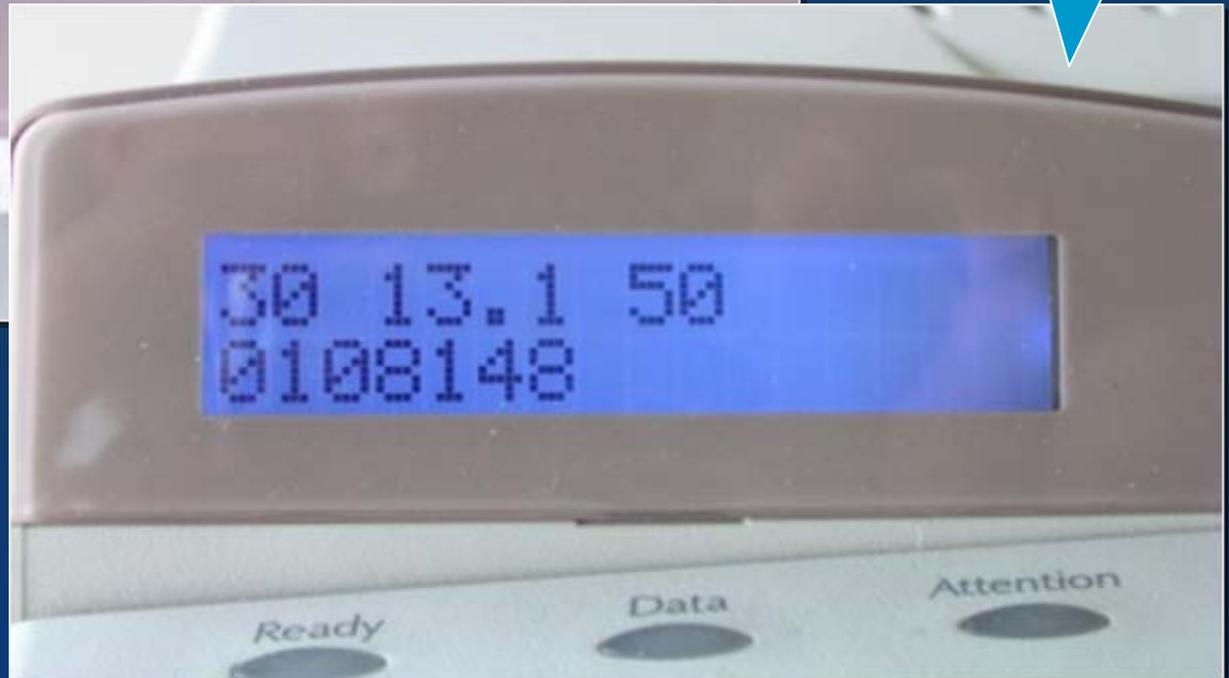




Impresoras



Los registros de eventos pueden aparecer en el panel de LCD con menor impacto forense.



Incomplete Printing Jobs

Completed Printing Jobs

Incomplete Non-Printing Jobs

Completed Non-Printing Jobs

All Incomplete Jobs

All Completed Jobs

Ready - Select Features to scan your job.

Select a job to get job details.

All Completed Jobs

Other Queues

#	Job Name	Owner	Status	Completed
1	Microsoft Word - 2006 NIPLEC	cmerriam	Completed	6:19:54PM
2	Copy Job 125	Local User	Completed	5:13:54PM
3	Copy Job 124	Local User	Completed	4:59:37PM
4	Copy Job 123	Local User	Completed	3:53:29PM
5	Copy Job 122	Local User	Completed	3:53:04PM
6	kbaker_PDF	NETWORK SERVICE	Completed	3:51:59PM



1/18





Faxes

- Los faxes pueden contener:
 - Registros de eventos
 - Registros de fax
 - Guías telefónicas
 - Información sobre el encabezado de los faxes
 - Información de números recientes (rediscado)
- Los dispositivos multifuncionales (fax, impresora, copiadora, etc.) tienen toda esta información y aún más:
 - Trabajos en caché.
 - Registros de eventos
 - Etc.



Faxes / Multifuncionales

printer • fax • copier • scanner

TIME/DATE, HEADER
Fax Header

...encabezado de fax...

printer • fax • copier • scanner

COMPANY NAME
▶KNUTH INDUSTRIES___

printer • fax • copier • scanner

FAX FUNCTIONS
Reprint Last Faxes

..reimprimir los últimos
faxes...

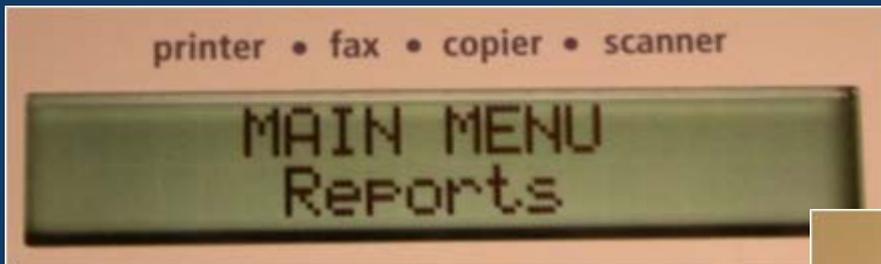
printer • fax • copier • scanner

PHONE NUMBER
▶410_555_1200_____

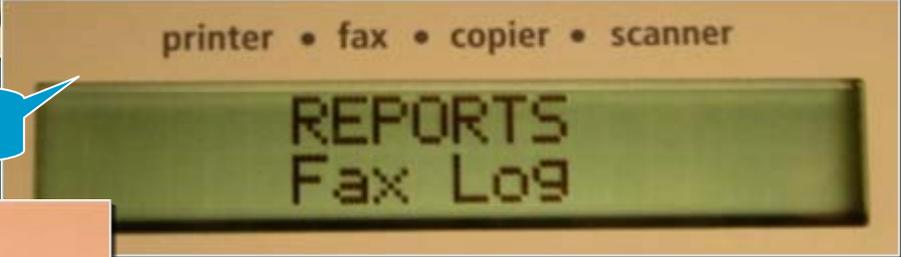
...número de fax local
(¡puede ser falso!)



Faxes / Multifuncionales



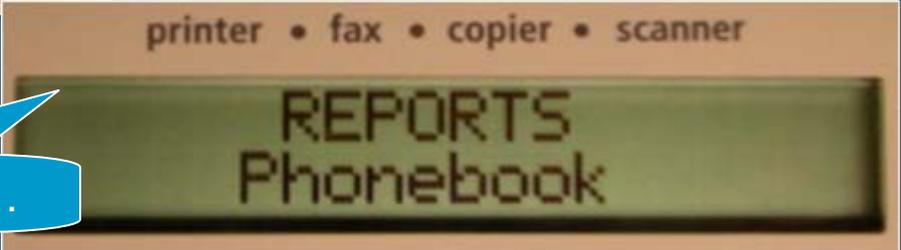
...registros de fax...



...reportes de transmisión...



...directorios telefónicos...



LONG T

GNICKVAH 1TGOOG



STEALING THE NETWORK HOW TO OWN AN IDENTITY

4 FREE E-BOOKLETS

INFOSEC CAREER HACKING

4 FREE E-BOOKLETS

GOOGLE HACKING

4 FREE E-BOOKLETS

GOOGLE HACKING

4 FREE E-BOOKLETS

AGGRESSIVE NETWORK SELF-DEFENSE



PENTESTER'S OPEN SOURCE TOOLKIT

4 FREE E-BOOKLETS

OS X FOR HACKERS



HACKING ON GOOGLE

Christopher Johnny Long Legs



OS X for Hackers at Heart
THE ART OF HACKING MAC OS X

OS X for Hackers at Heart
 Steve Butler, Chris Gammell, and
 Tom Lord
 With easy hardware, a powerful operating system, and a wide range of
 as great as OS X. The operating system is not only secure, but also
 tweaking and tuning the software and hardware. The authors are
 really excited about the software and hardware. The authors are
 modifications are other way in their own right. The authors are
 even deeper into the realm of "hacking". The authors are
 driven, modifications and show how the authors are
 edge research, development, and security. The authors are
 ISBN: 1-57749-046-7
 Price: \$49.95 US, \$69.95 CAN

Host Integrity Monitoring Using Osiris and Samhain

Brian Wotring, Bruce Potter, Marcus J. Ranum
 Host Integrity Monitoring is the most effective way to determine if one
 of malicious attack or threat has compromised your network security
 modify the filesystem, system configuration, or runtime environment of
 torated hosts. This book provides foundation information on host integrit
 toring as well as specific, detailed instruction on using best of breed
 Osiris and Samhain. By the end of the book, the reader will not only
 stand the strengths and limitations of host integrity tools, but also understand
 how to effectively make use of them in order to integrate them into a security
 policy.

ISBN: 1-57749-018-0
 Price: \$42.95 US, \$62.95 CAN

Nessus Snort Ethereal
Power Tools

Nessus, Snort, & Ethereal
 Brian Caswell, Charles
 Neuenhofer, Michael
 If you have Nessus, Snort, and Ethereal you are ready to go. This book
 customize, code, and tune these tools to the maximum. The authors
 you. The authors of this book provide the reader with the most
 five and efficient filters. When done with the book, the reader
 display filters. When done with the book, the reader will be able
 to detect malicious traffic with the maximum accuracy.





Preparándose para revisar e incautar computadoras

- Averiguar qué es probable esperar
 - ¿Cuántas computadoras?
 - ¿Qué tipos de computadoras?
 - ¿Qué tipo de situación de red?
 - ¿Qué otros equipos?
- Prepárese para lo inesperado
 - Puede ser necesario buscar en el lugar
 - Puede ser necesario tomar los equipos y buscar luego



Preparándose para revisar e incautar computadoras

- Peligro generado por la red: es posible entrar a las computadoras y controlarlas a distancia
- Publicidad: las noticias sobre una operación grande viajan a la velocidad de Internet



Contacto

Laboratorio de Delitos Informáticos
Sección de Delitos Informáticos
y Propiedad Intelectual
Departamento de Justicia de los Estados Unidos

- Teléfono: 202-514-1026
- Internet: www.cybercrime.gov