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

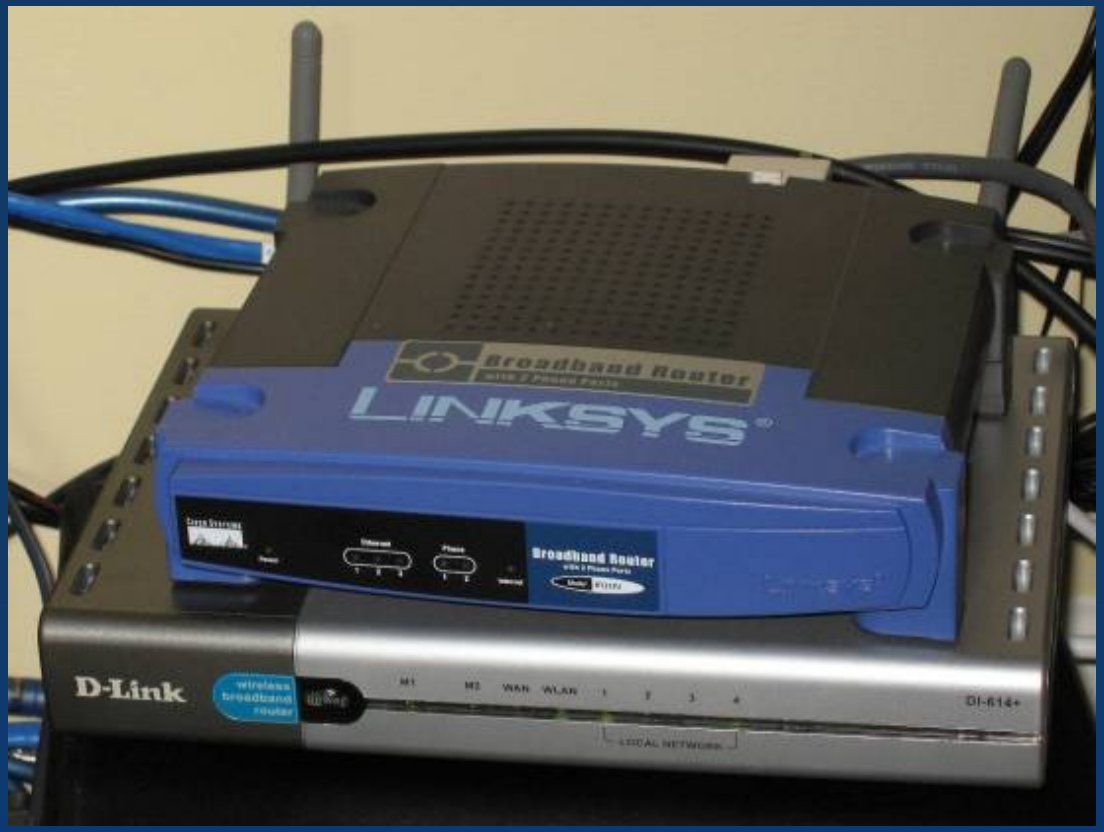
- Computadoras de escritorio (*desktops*) a servidores

Variedad de medios

Variedad de medios

Routers

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

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

Impresoras

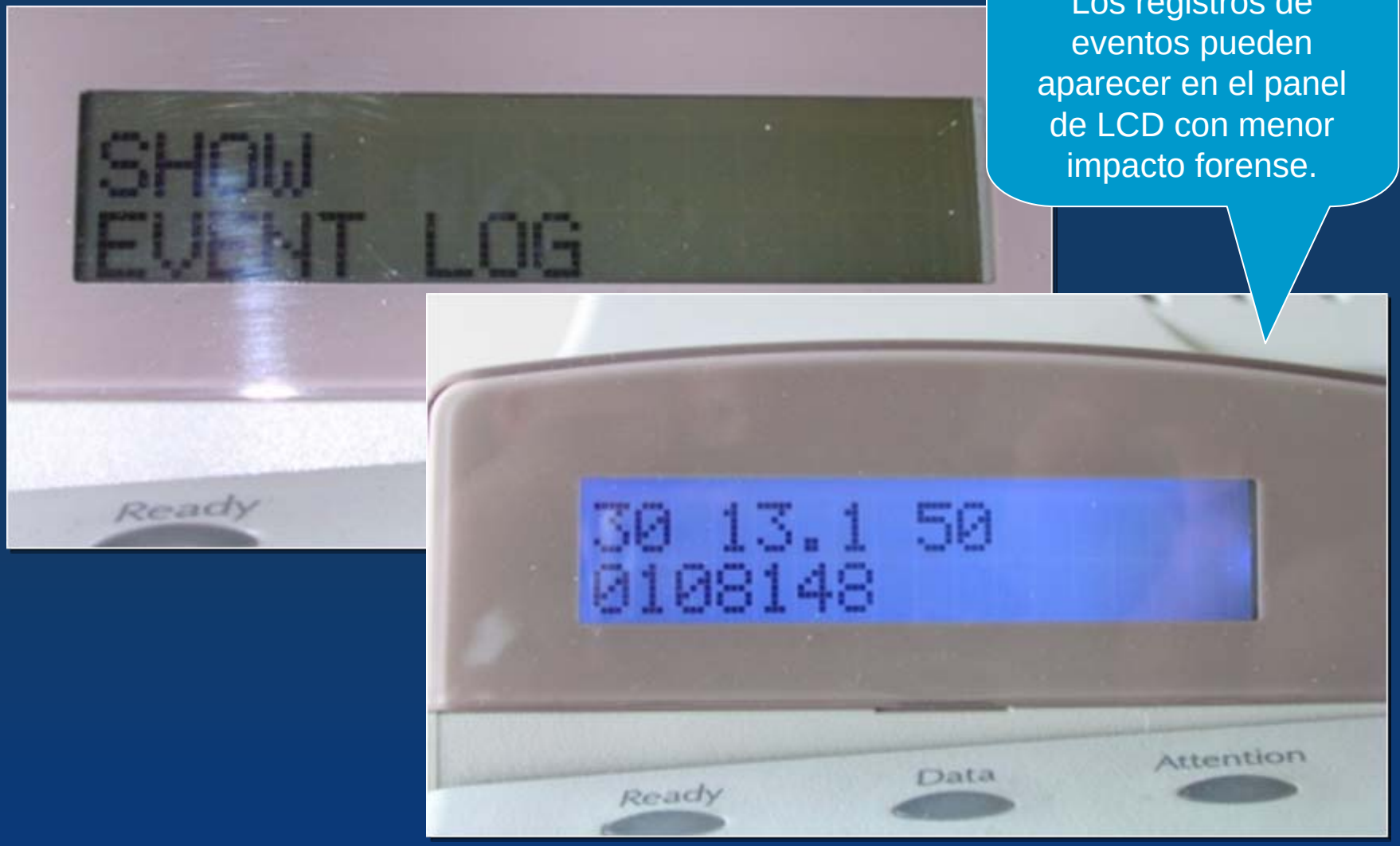
- La mayoría de los investigadores ni siquiera registrará una impresora.
- Las impresoras pueden contener todo tipo de información que a menudo es pasada por alto.
  - ¿La impresora tiene un disco RAM?
  - ¿Tiene un disco duro?
  - ¿Una interfaz web?
  - ¿Registros de eventos?
  - ¿Registros de trabajos?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

Menús del LCD de la impresora

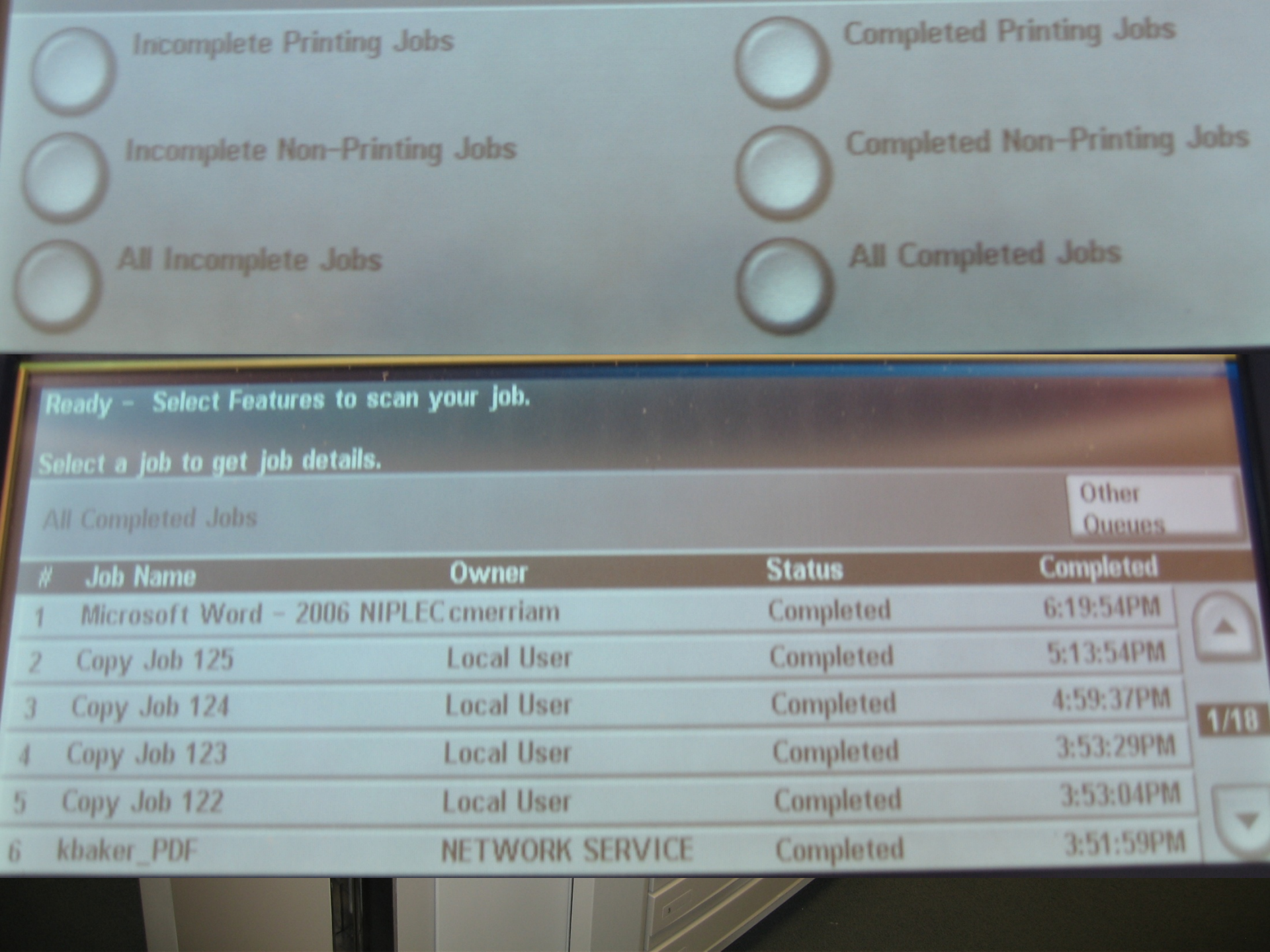
El menú de información de HP es la puerta de entrada a todo tipo de pruebas ocultas…

… como el registro de eventos…

Impresoras



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

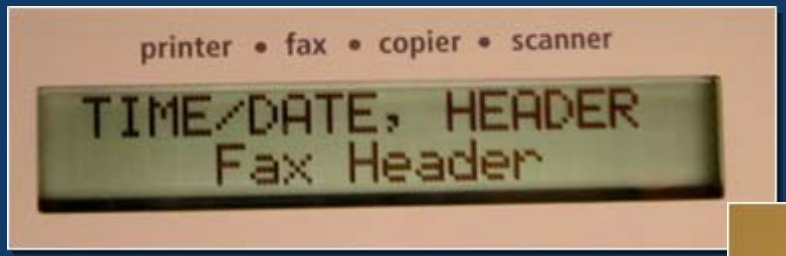

Incomplete Printing Jobs
Completed Printing Jobs
Incomplete Non-Printing Jobs
Completed Non-Printing Jobs
All Incomplete Jobs
All Completed Jobs
Ready - Select Features to scan your job.
Select a job to get job details.
All Completed Jobs
Other Queues
Job Name Owner Status Completed
1 Microsoft Word - 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

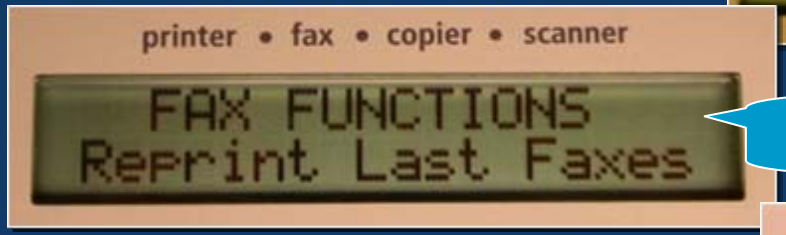
- Los faxes pueden contener:
  - Registros de eventos
  - Registros de fax
  - Guías telefónicas
  - Información sobre el encabezado de los faxes
  - Información de números recientes (rediscado)

- Los dispositivos multifuncionales (fax, impresora, copiadora, etc.) tienen toda esta información y aún más:
  - Trabajos en caché.
  - Registros de eventos
  - Etc.

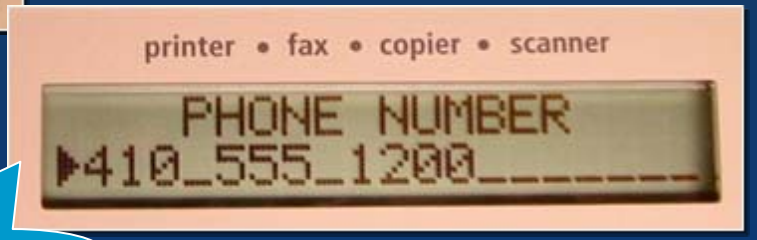
Faxes / Multifuncionales



…encabezado de fax…



..reimprimir los últimos faxes…

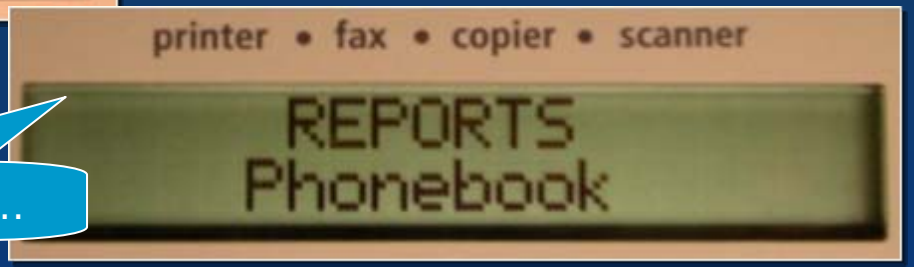


…número de fax local (¡puede ser falso!)

Faxes / Multifuncionales

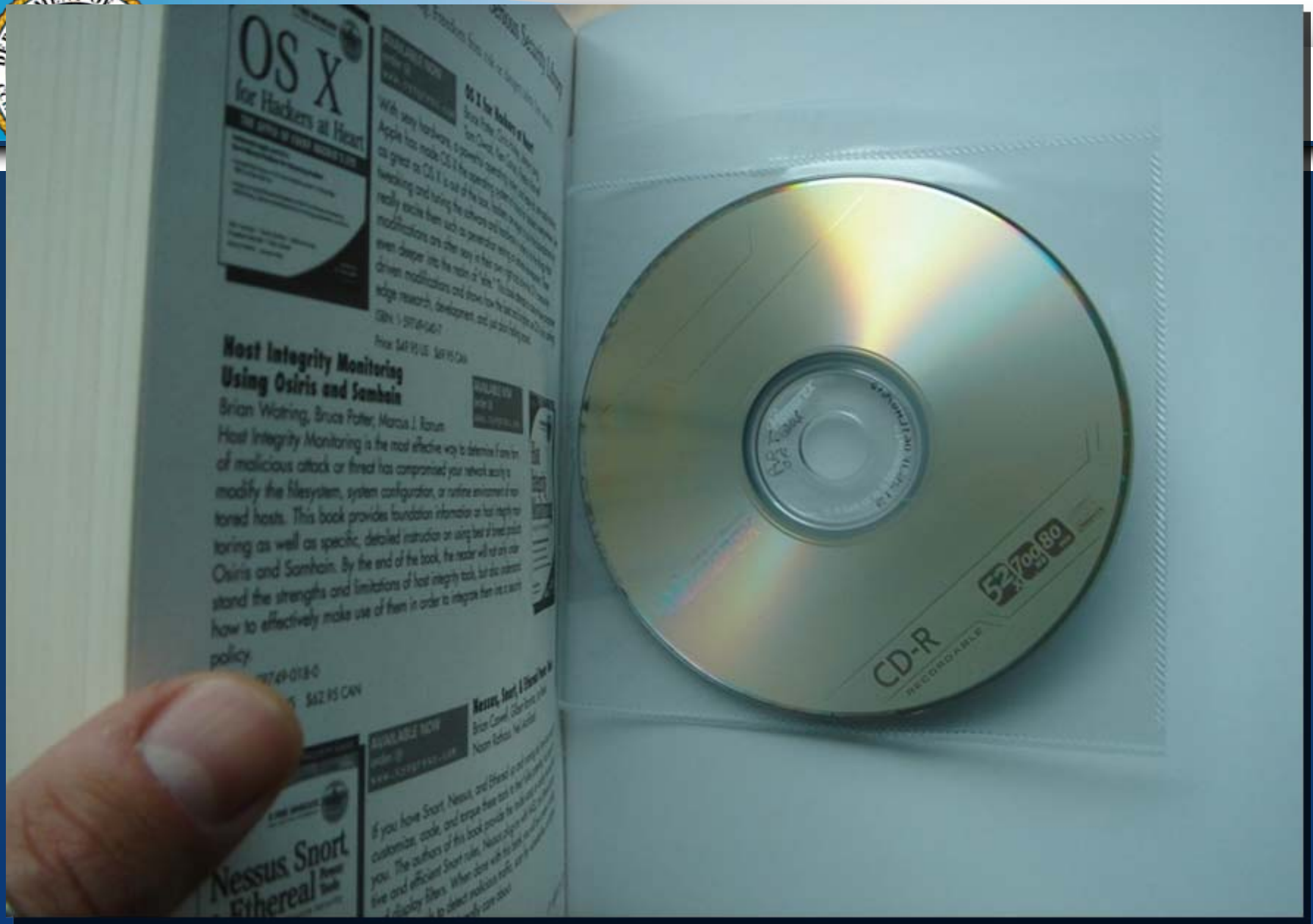
…registros de fax…

…reportes de transmisión…



…directorios telefónicos…

4 FREE E-BOOKLETS
OS X FOR HACKERS
SYNGRESS
HACKING CON GOOGLE
Christopher
Johnny Long Legs
4 FREE E-BOOKLETS
PENTESTER'S
OPEN SOURCE TOOLKIT
SYNGRESS
4 FREE E-BOOKLETS
AGGRESSIVE NETWORK SELF-DEFENSE
SYNGRESS
4 FREE E-BOOKLETS
GOOGLE HACKING
SYNGRESS
4 FREE E-BOOKLETS
GOOGLE HACKING
SYNGRESS
4 FREE E-BOOKLETS
INFOSEC CAREER HACKING
SYNGRESS
STEALING THE NETWORK HOW TO OWN AN IDENTITY
SYNGRESS
GOOGLE HACKING
J. LONG


OS X
for Hackers at Heart
Host Integrity Monitoring
Using Osiris and Samhain
Brian Wotring, Bruce Potter, Marcus J. Ranum
Nessus, Snort, & Ethereal
CD-R
700 MB
80

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