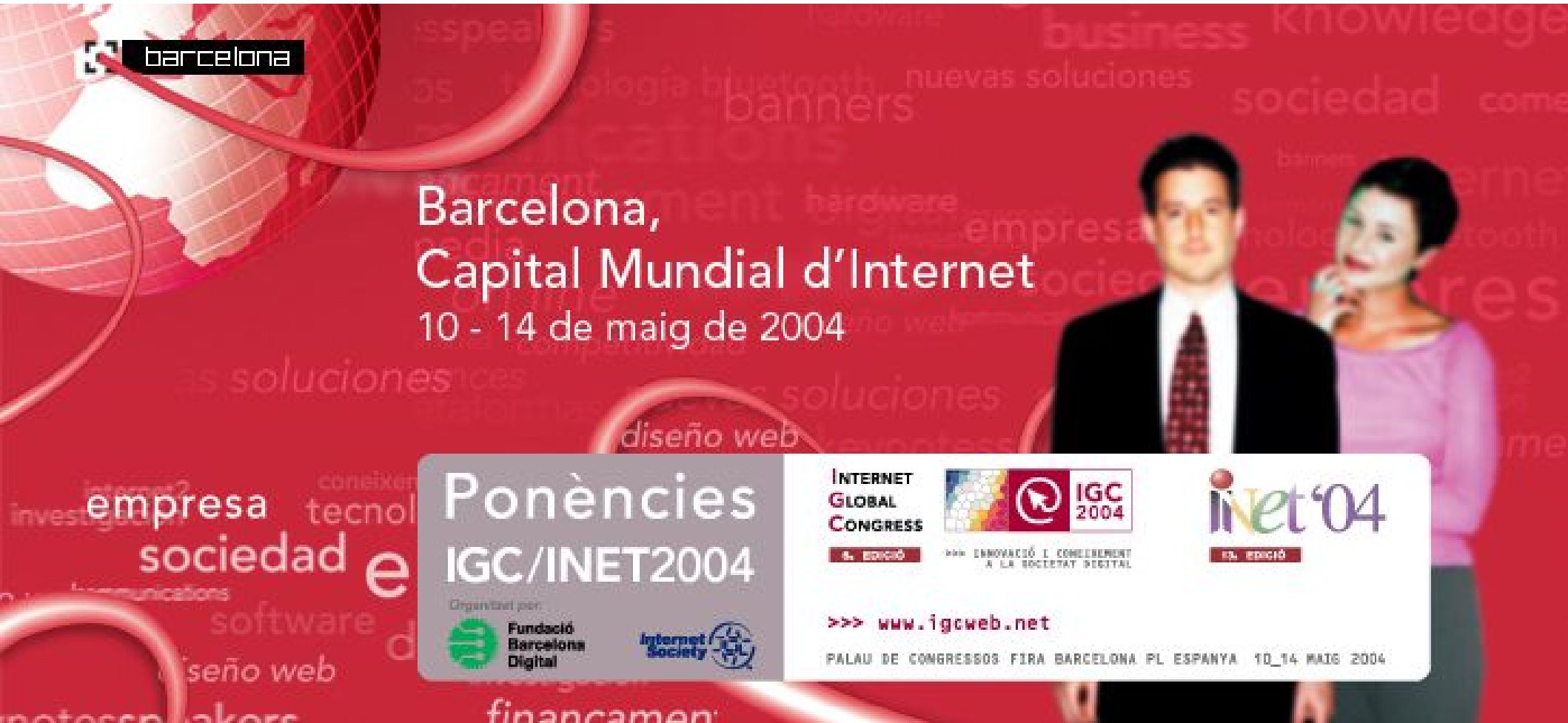
Informática Forense:

“Recuperación de la Evidencia Digital”

Daniel Fernández Bleda
Internet Security Auditors
dfernandez@isecauditors.com
CISSP, OPST/OPSA Trainer
Co-Founder

internet security auditors
www.isecauditors.com



Índice

- ¿Qué es la Informática Forense?
- ¿Qué no es la Informática Forenese?
- ¿Qué es una Evidencia Digital?
- Herramientas de Análisis Forense:
  - Hardware
  - Software
- Problemas actuales en la Informática Forense
- Recolección de Datos
- Cadena de Custodia antes del Análisis
- Ejemplos de Análisis Forense
- El ¿Futuro? de la Informática Forense
- Referencias

¿Qué es la Informática Forense?

- ¿Qué es?

  "La ciencia de la Informática Forense es la ciencia de adquirir, preservar, obtener y presentar datos que hayan sido procesados electrónicamente y almacenados en soportes informáticos."

- ¿Por qué aparece?

  "La ciencia de la Informática Forense fue creada para dirigir las necesidades específicas y articuladas de las fuerzas de la ley para aprovechar al máximo esta forma nueva de evidencia electrónica"

- ¿Cuál es el reto de la Informática Forense?

  "Los soportes informáticos que son examinados y las técnicas disponibles para el investigador son productos resultado de un sector determinado por el mercado privado. Además, en contraste con el análisis forense tradicional, en la I.F. las investigaciones deben llevarse a cabo en prácticamente cualquier situación o dispositivos físico, no sólo en un entorno controlado de laboratorio."

¿Qué no es Informática Forense?

- NO ES el simple hecho de recuperar ficheros eliminados por error de un equipo.

- NO ES el descubrir porque una máquina se ha contaminado por un virus y su eliminación: eso es trabajo de un Antivirus.

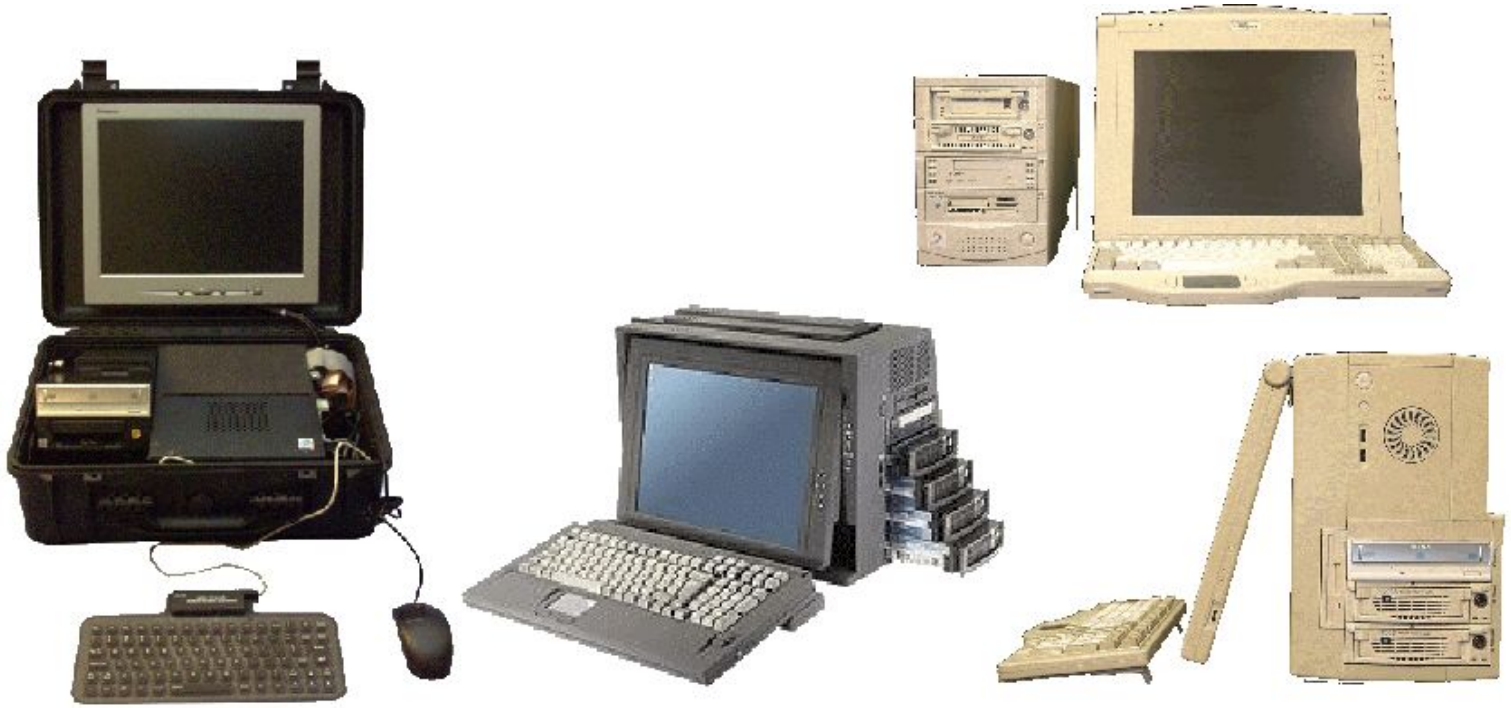
- NO ESTÁ limitada a aquello que podemos encontrar en una sola máquina: la información útil puede estar dispersa en diferentes sistemas.

¿Qué es una Evidencia Digital?

- Información almacenada digitalmente que puede llegar a ser utilizada como prueba en un proceso judicial.
- Para que esto sea viable será necesario seguir unos procedimientos en su recuperación, almacenamiento y análisis.
- Es muy importante seguir una cadena de custodia lo suficientemente robusta y permita asegurar la inmutabilidad de la evidencia digital.

Herramientas de Análisis Forense (I)

- **Equipos Informáticos**: podemos contar con sistemas informáticos especialmente adaptados (o también podemos crear los nuestros) para facilitar la reproducción de todo tipo de soporte electromagnético y óptico. Además deben permitir su transporte para realizar las investigaciones en cualquier lugar.



Herramientas de Análisis Forense (II)

- **Software Comercial**: En los últimos años han aparecido multitud de empresas que ofrecen herramientas comerciales de análisis forense.
- **Software OpenSource**: El auge de la Informática Forense ha hecho que se incremente la cantidad de gente interesada en el tema, y muchas de ellas han creado herramientas Open Source de potencial muy elevado accesibles a cualquiera:
  - **TCT** (**The Coroner's Toolkit**): Suite de herramientas de AF creada por dos de los padres de la AF: Dan Farmer y Wietse Venema.
  - **TSK** / **Autopsy** (**The Sleuth Kit**): Herramientas basadas en TCT
  - **Foremost**: Recuperación de archivos según sus cabeceras y pies.
  - **ODESSA** (**Open Digital Evidence Search and Seizure Architecture**): suite de herramientas para recuperar información en sistemas Windows (papelera de reciclaje, históricos de navegación web, etc.)
  - Y un **interminable** etcétera....

Problemas actuales en la IF

- No existen metodologías estandarizadas para la recuperación de evidencias digitales. Iniciativas como CTOSE van en este camino.
- Se recurre a los expertos forenses mucho tiempo después de producirse los incidentes, con lo que la información que podía ser útil suele perderse o alterarse parcial o totalmente.
- La forma de obtener y almacenar las evidencias digitales está basada en unas “buenas maneras”.
- El Análisis Forense lo llega a realizar personal que no tiene base tecnológica y no conoce profundamente los Sistemas Operativos y dispositivos de donde debe obtener la información.
- A los técnicos que realizan Análisis Forense les es costoso demostrar que los métodos seguidos son válidos a alguien que no tiene una base tecnológica.
- Emplear la I.F. dentro de una empresa puede violar la intimidad o los derechos de los empleados siempre que no se sigan códigos éticos (p.e. $(ISC)^2$, OSSTMM, The Sedona Conference, etc.).

Recolección de datos

- Existen dos tendencias a la hora de realizar análisis en máquinas comprometidas:
  - La primera opta por no realizar ningún tipo de acción sobre la máquina con el objetivo de obtener información del estado actual.
  - La segunda opta por recoger información del estado actual, ya que en caso de no obtenerse en ese precio instante, se perdería.
- Inconvenientes de análisis en caliente: realizar cualquier acción sobre la máquina implica que esa propia acción altera su estado y puede alterar la información, también puede implicar un aviso al atacante y que este elimine sus huellas rápidamente.
- Beneficios del análisis en caliente: la información que podemos obtener del estado de la máquina puede ser muy útil (conexiones, ficheros abiertos, programas en ejecución, estado de la memoria, etc.).

Cadena de Custodia antes del Análisis

- Fotografiar el equipo sin desmontar (apagado con el cartel de número de serie)
- Fotografiar el equipo desmontado (con el cartel visualizando números de serie de hardware)
- Fotografiar la configuración equipo por dentro
- Apuntes en el cuaderno de todos los pasos
- Montar el disco (nodev, noexec, ro)
- Imágenes del disco (3).
- Generación de md5sum del disco de cada una de las particiones.
- Generación de md5sum de cada de las 3 imágenes del disco (tienen coincidir).
- Grabar las 2 imágenes en una cinta magnética (comprobar MD5 tiene que coincidir con la imagen y del disco).
- Etiquetar el HD original y las 2 cintas (etiqueta, iniciales analista, acompañante, MD5)
- Fotografiar el HD original y las 2 cintas juntas (se tiene que ver la fecha, hora y las etiquetas).
- Guardar el HD original y las cintas en una caja fuerte. Entregar las llaves al Cliente o Autoridades.

Ejemplos de Análisis Forense

- El Proyecto Honeynet pretende se un centro de entrenamiento para todos aquellos interesados en el Análisis Forense y la gestión de incidentes en general.
- Honeynet dispone máquinas que simulan estar en producción sobre las que se mantiene monitorización para poder capturar ataques sobre ellas y poder detectar nuevos tipos de ataques o técnicas.
- Además es la mejor manera de "entrenarse" dado que no son ataques simulados, sino, simplemente, controlados.
- Permite obtener práctica para llegar a realizar A.F. en casos como:
  - Recuperación de información de imágenes de disco magnéticos, de discos duros, cintas de backup, chips de memoria, telefónos móviles, etc.
  - Análisis de Intrusiones en sistemas comprometidos.
  - Reconstrucción de intrusiones a partir de logs de IDS.
  - Reconstrucción de intrusiones a partir de logs de Firewalls.
  - Seguimiento de envíos/recepciones de correos electrónicos.

El ¿Futuro? de la Informática Forense

- Los investigadores forenses ya no pueden quedarse limitados a los ordenadores.
- Con el auge de los honeypots y honeynets, los atacantes emplean métodos para ocultar, ofuscar o encriptar la información utilizada en los ataques (exploits, rootkits, etc.) con lo que la reconstrucción de los ataques es más compleja y requiere conocimientos de ingeniería inversa.
- Cada vez más, han ido apareciendo nuevos dispositivos, más complejos y que almacenan información importante:
  - Teléfonos móviles: teléfonos, mensajes, listados de llamadas, etc.
  - PDAs: prácticamente se asemejan más a los ordenadores → la información que almacenan puede ser tan importante como la de estos.
  - Relojes, tarjetas inteligentes, etc...
- Entonces: ¿si en un HD pueden haber datos "eliminados" recuperables y utilizables como evidencia...¿por qué no en una PDA, o en un móvil?
- Mientras que la ciencia forense ha mejorado técnicas para investigar sobre un mismo medio, la informática forense debe adaptarse y mejorar sus técnicas para investigar sobre un medio cambiante día a día.

Referencias

- SANS Institute (SANS InfoSec Reading Room):
  www.sans.org/rr/
- Forensics Science Communications:
  http://www.fbi.gov/hq/lab/fsc/current/index.htm
- Página web de Wietse Venema
  http://www.porcupine.org/
- ActivaLink (página web de Ervin Sarkisov):
  http://www.activalink.net/
- sleuthkit.org (página web de SleuthKit y Autopsy):
  http://www.sleuthkit.org/
- Proyecto Honeynet:
  http://www.honeynet.org/
- Códigos éticos en I.F. y hacking en general:
  http://www.isc2.org/
  http://www.osstmm.org/
  http://www.thesedonaconference.org/

Informática Forense:

“Recuperación de la Evidencia Digital”

Daniel Fernández Bleda
Internet Security Auditors
dfernandez@isecauditors.com
CISSP, OPST/OPSA Trainer
Co-Founder

internet security auditors
www.isecauditors.com

Gracias por su asistencia