

Análisis Forense

ÍNDICE

■ **Parte teórica**

- ***Análisis Forense***
- ***Respuesta a Incidentes***
- ***Motivación***
- ***Evidencias***
- ***El Proceso Forense***

■ **Parte Práctica**

- ***Herramientas***
- ***Análisis de un caso REAL***

Análisis Forense

- Definición de Análisis Forense
 - Respuesta a Incidentes

- Sinónimos: Cyberforensics, Forensic Analysis, Forensics, Computer Forensics, and Digital Forensics

- DFRWS 2001: **Digital Forensic Science**

*The use of scientifically derived and proven methods toward the **preservation, collection, validation, identification, analysis, interpretation, documentation and presentation** of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations*

Respuesta a Incidentes

■ La Respuesta a Incidentes

- Empecemos por el principio....¿Qué es un **Incidente**?

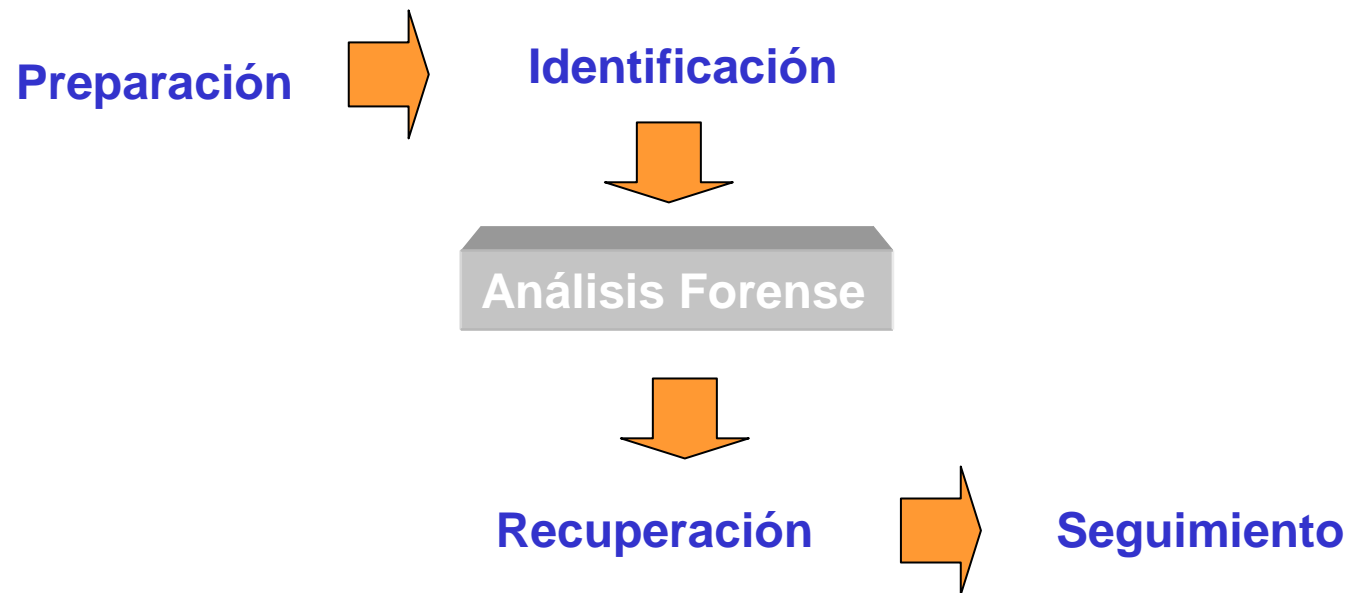
■ Algunos tipos de incidentes:

- Compromisos de integridad
- Uso no autorizado
- Denegación de servicio
- Daños
- Intrusiones



Respuesta a Incidentes

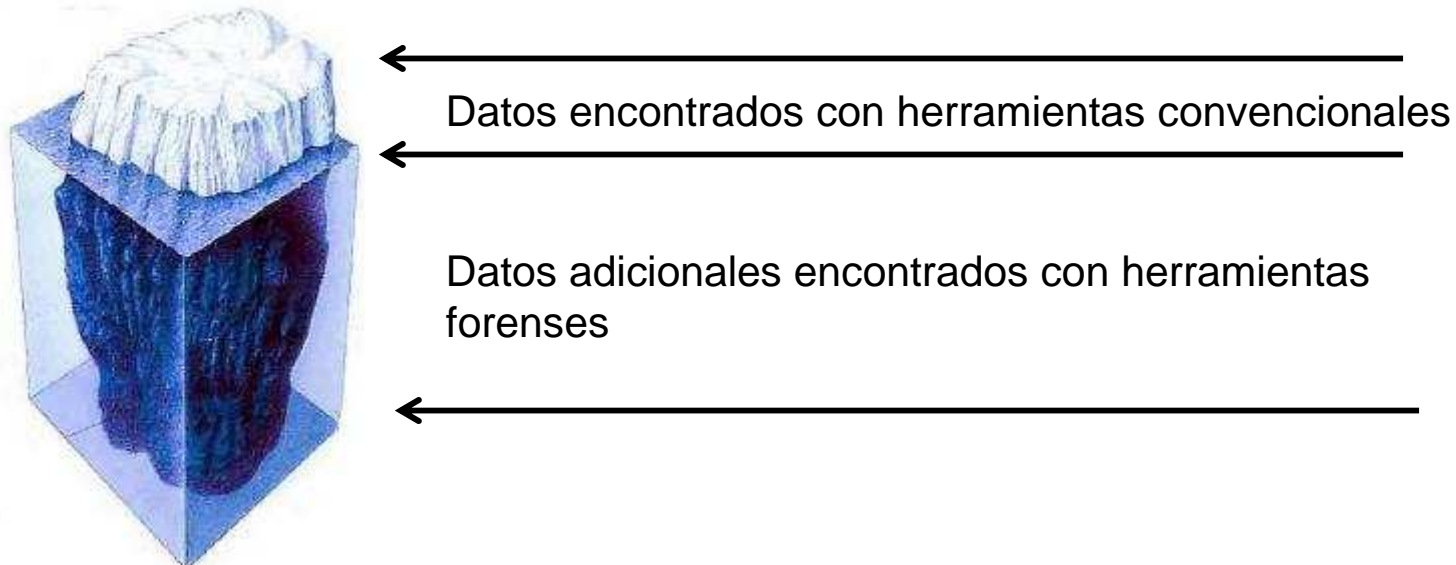
■ El proceso :



Necesidad de Métodos Forenses

■ ¿Por qué es necesario?

- Los datos digitales son **frágiles, volátiles, complejos** de interpretar y deben ser **preservados y autenticados** adecuadamente.
- Deterioro de las evidencias.
- Cambio de perfil del ***ciberdelincuente***.
- El “iceberg de datos”:



Objetivos de la investigación forense

■ Objetivos Generales

- Confirmar el incidente ocurrido.
- Llevar a cabo una investigación estructura del incidente.
- Preservar y asegurar las evidencias digitales y validarlas para un posible proceso judicial.
- Asegurar la continuidad de negocio. Minimizar costes de interrupción de servicio.
- Entender, corregir y proteger de futuros compromisos

Evidencia Digital vs Prueba Electrónica

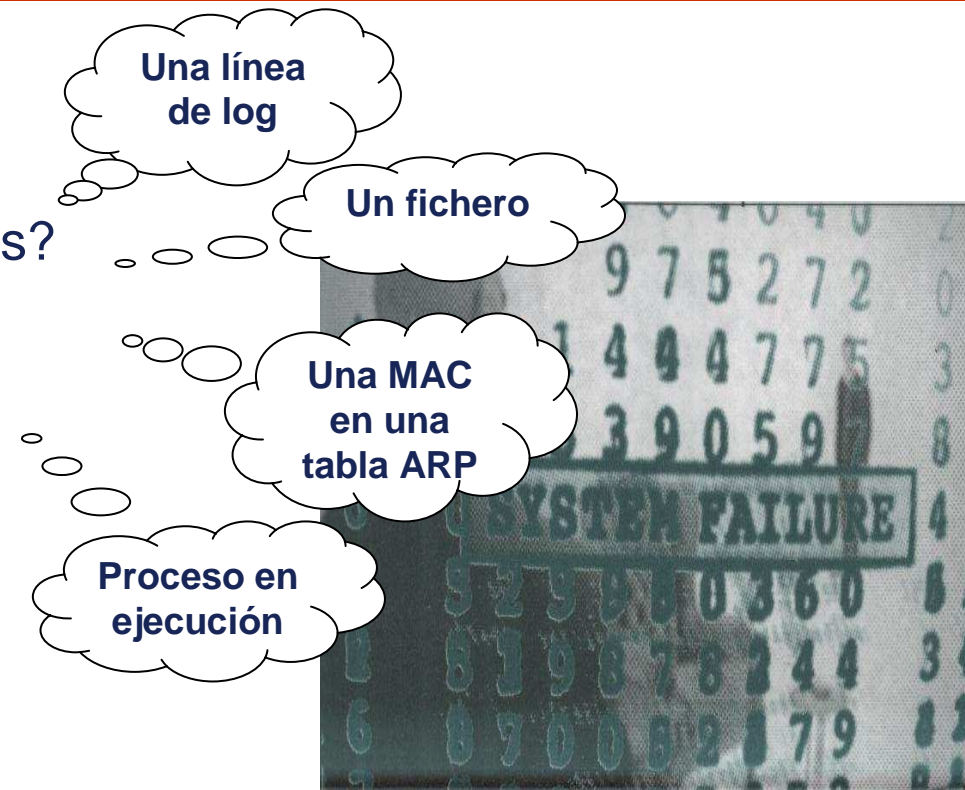
■ La evidencia digital. Que es?

- No son más que datos

■ Donde encontrarlas ??

■ La prueba digital

- Datos = Prueba? **NO**

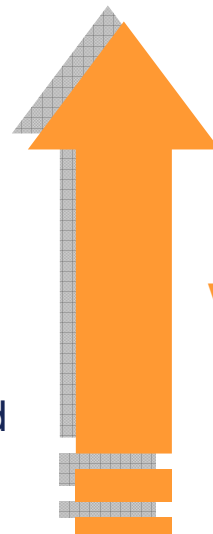


Información almacenada o transmitida en formato digital
aceptada en un proceso judicial

Tipos de Evidencias

■ Tipos de Evidencias

- Testimonio Humano
- Evidencias Físicas
- Evidencias de Red
- Evidencias de Host
 - Memoria
 - Conexiones de Red
 - Procesos
 - Usuarios conectados
 - Configuraciones de red
 - Discos



Volatilidad

El proceso Forense

■ El proceso Forense



Recolección de Evidencias

■ Primera Fase: Llegamos al lugar del incidente.

- Preservar la escena del crimen.
 - De personas: Evitar que acciones de terceros contaminen o destruyan pruebas
- Recoger evidencias físicas
 - Descripción del hardware
 - Descripción de los dispositivos externos
 - Topologías de red
 - Fotografiar el sistema
- Recoger evidencias humanas
 - Testimonio del administrador: ¿Qué ha tocado?

Recolección de Evidencias

■ Recoger evidencias del host.

No se puede obtener el estado de un sistema sin alterarlo

- Tratar de obtener la mayor información posible con el mínimo impacto
- El dilema: ¿apagamos el sistema, o antes interactuamos con él?

Análisis en frío VS Análisis en caliente

■ Análisis en Frío

- Evitamos un mayor impacto en la máquina.
- Solo podemos acceder a la información no volátil.
- ¿Cómo apago el sistema comprometido?

■ Análisis *On-line*

- Podemos recoger mucha más información.
- Técnicas avanzadas solo detectables en memoria.
- Fácil contaminación del sistema. Juicio?
 - login, procesos, binarios contaminados, etc...
- Respuesta del intruso. **Sistema Peligroso!!**
- Información no fiable.

Recolección de Evidencias

■ Recolección de evidencias en caliente

Muy fácil contaminar las evidencias!!

- No utilizar las herramientas del sistema. Podrían haber sido alteradas
- No ser intrusivo:
 - Ejecutar lo estrictamente necesario.
 - No alterar el contenido del disco
 - No instalar programas, ni volcar salida de programas a disco duro.
 - Utilizar medios externos para almacenar los datos o enviarlos vía red.
- Recoger por orden de volatilidad
- Documentación
- Modificación y Sobreescritura en discos

Recolección de Evidencias

■ Preparación del Toolkit

- Herramientas limpias
- Compiladas estáticamente
- Ejemplos: nc,netsatst,memdump, dd , pcat, etc...

■ Interactuar con el entorno

- Análisis del tráfico del red

■ Procedimiento:

- *csi# nc -l -p 8888 > date_compromised*
- *victima# /mnt/cdrom/date | /mnt/cdrom/nc 192.168.1.100 8888 -w 3*

Recolección de Evidencias

■ Estudio previo del Impacto

- Comando mount

Fichero	Modificado
/etc/ld.so.cache	atime
/lib/tls/libc.so.6	atime
/usr/lib/locale/locale-archive	atime
/etc/fstab	atime
/etc/mtab	Atime, mtime, ctime
/dev/cdrom	atime
/bin/mount	atime

Recolección de Evidencias

■ Evidencias a recoger

- **Memoria**
- Tablas caché: arp, rutas, etc..
- Conexiones de red
- Procesos
- Módulos del kernel
- Información del sistema
- Fecha



Recolección de Evidencias

■ **Recolección de evidencias en frío**

- Extracción de discos
- Copiado de disco. bit-por-bit

■ **Recolección de evidencias de red**

- IDS
- Firewall
- Herramientas de monitorización

■ **La entrega de los medios**

- Documento firmado por el perito/notario y la empresa.

Recolección de Evidencias

■ Reglas Básicas:

- Sumas de comprobación
- Documentación de TODO
- Cadena de Custodia
- Consideraciones de transporte y almacenamiento
- Puede no ser suficiente
 - Perito judicial o Notario



Análisis de Evidencias

■ Segunda Fase: Empezamos el análisis

■ Consideraciones:

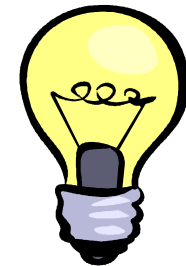
- **NUNCA** trabajar con datos, evidencias, dispositivos, etc..
ORIGINALES
- Respetar la legislación y las políticas de la Organización
- Documentación
- Resultados Verificables y Reproducibles
- No existe un procedimiento estándar.

Análisis de Evidencias

■ Preparación del entorno forense

- Laboratorio forense. **¿Utópico?**
- El Sistema de análisis
 - Entorno limpio
 - Aislado de la red
 - Herramientas limpias y esterilizadas
- Sistema de Simulación
- Sistema de Pruebas en caliente

Vmware



Análisis de las Evidencias

■ Objetivo de Análisis

- Quién? Como? Con que? Porqué? Cuando? Etc...

■ Reconstrucción temporal de los hechos: Timeline

- Correlación de eventos. De donde ?

■ Análisis del sistema de ficheros

- Análisis de los ficheros corrientes del sistema
 - Comprobación de integridad de los binarios del sistema.
 - **ROOTKITS y Virus???**
- Archivos temporales.
- Archivos o directorios “ocultos”
 - Nombres camuflados
- Archivos borrados
- Slack space
- Partición swap
- Esteganografía, cifrado, etc...



Fin Parte Teórica

CONFIDENCIALIDAD Y RESTRICCIONES DE USO

Toda la información contenida en el presente documento, sea de naturaleza técnica, comercial, financiera o de cualquier otro tipo, es propiedad de TISSAT y considerada como "Información estrictamente confidencial", por lo que no se revelará a terceras partes quedando prohibida su reproducción, total o parcial, por cualquier medio sin el previo consentimiento expreso de TISSAT.

Roberto Gutiérrez

Ángel Alonso Párrizas