



Análisis Forense

Seminarios Técnicos Avanzados
Microsoft Technet – Madrid, 11 de Julio del 2006

José Luis Rivas López

TEAXUL
jlrivas@teaxul.com

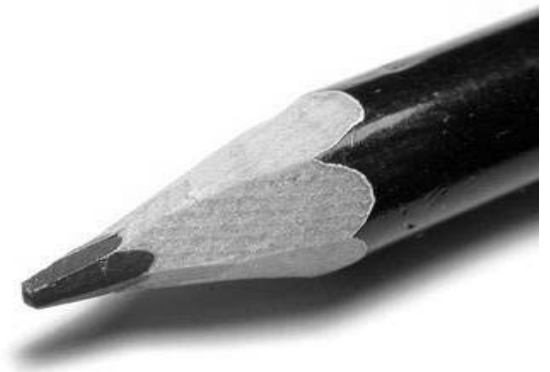
Carlos Frago Mariscal

CESCA / JSS
cfrago@cesca.es - carlos@jessland.net

Agenda

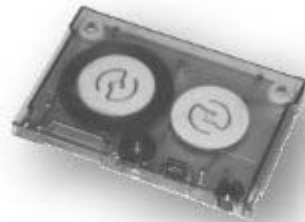


- Introducción
- Metodología y procedimientos
- Herramientas
- Caso de estudio
- Reto de análisis forense



¿ Que és un Análisis Forense ?

- “Obtención y análisis de datos empleando métodos que distorsionen lo menos posible la información con el objetivo de **reconstruir todos los datos y/o los eventos que ocurrieron sobre un sistema en el pasado**”
 - Dan Farmer y Wietse Venema, 1999



En busca de respuestas...

- ¿ Qué sucedió ?
- ¿ Donde ?
- ¿ Cuándo ?
- ¿ Por qué ?
- ¿ Quién ?
- ¿ Cómo ?



Algunos conceptos

- **Evidencia**
- **Cadena de custodia**
- Archivo de hallazgos
- Línea de tiempo
- Imágenes
- Comprobación de integridad
 - Hash



¿ Preservar o salvar ?



Se busca “vivo o muerto”

- Sistema “vivo”
 - Memoria
 - Flujos de red
 - Procesos
 - Ficheros
- Sistema “muerto”
 - Almacenamiento
- Información complementaria:
 - Logs (IDS, firewalls, servidores, aplicaciones)



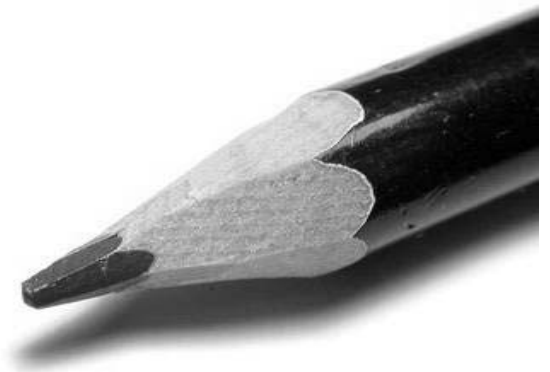
Agenda

Introducción



Metodología y procedimientos

- Herramientas
- Caso de estudio
- Reto de análisis forense



Metodología

- Verificación y descripción del incidente
- Adquisición de evidencias
- Obtención de imágenes de las evidencias
- Análisis inicial
- Creación y análisis de la línea de tiempo
- Análisis específico y recuperación de datos
- Análisis de datos y cadenas
- Generación del informe

Creación del archivo de hallazgos

- Documento que permita llevar un historial de todas las actividades que realicemos durante el proceso del Análisis Forense
- Útil para la reconstrucción del caso un tiempo después de que este haya sido realizado

Recepción de la Imagen de datos

- Consiste en la recepción de las imágenes de datos a investigar.
- Clonación de las imágenes.
- Habrá que verificarlos con MD5 y compararlo con lo de la fuente original.

NOTA: Hay que garantizar siempre que la imagen suministrada no sufra ningún tipo de alteración, con el fin de conservación de la cadena de custodia y así poder mantener la validez jurídica de la evidencia.

Identificación de las particiones

- En esta fase se identificarán las particiones con el sistema de archivos de las particiones actuales o las pasadas.
- Reconocimiento de las características especiales de la organización de la información y se puede definir la estrategia de recuperación de archivos adecuada.

Identificación SO y aplicaciones

- En esta fase se identificarán los sistemas operativos instalados, las aplicaciones utilizadas, antivirus, etc.

Revisión de código malicioso

- Revisar con un antivirus actualizado si tiene algún tipo de *malware*: virus, troyanos, etc.

Recuperación archivos

- Recuperación de los archivos borrados y la información escondida examinando para esta última el slack space:
 - campos reservados en el sistema de archivos
 - espacios etiquetados como dañados por el sistema de archivos

Primera Clasificación de Archivos

- Archivos “buenos” conocidos. Aquellos que su extensión corresponden con su contenido.
- Archivos “buenos” modificados. Aquellos cuya versión original ha sido modificada.
- Archivos “malos”. Aquellos que representan algún tipo de riesgo para el sistema (troyanos, backdoors, etc.)
- Archivos extensión modificada. La extensión no corresponde con su contenido.

Segunda Clasificación de archivos

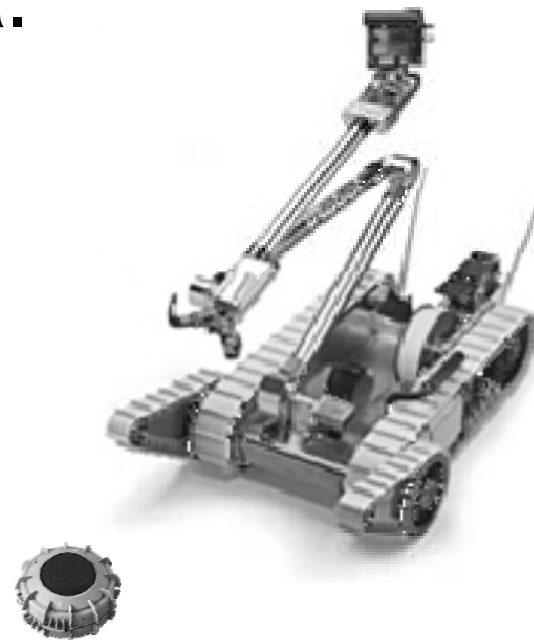
- Se clasifica mediante la relación de los archivos con los usuarios involucrados en la investigación y contenido relevante para el caso.

Analizar los archivos

- Este proceso cesa cuando el investigador, a partir de su criterio y experiencia, considera suficiente la evidencia recolectada para resolver el caso, o por que se agotan los datos para analizar.

Análisis de artefactos

- Consiste en realizar un análisis minucioso de posibles contenidos “conflictivos” identificados en el sistema.
- Tipos de análisis:
 - Comportamiento
 - Código o contenido



Línea de tiempo

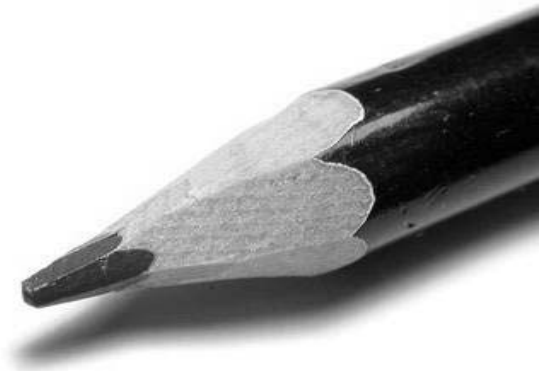
- Esta fase consiste en realizar la reconstrucción de los hechos a partir de los atributos de tiempo de los archivos, lo que permite correlacionarlos enriqueciendo la evidencia.

Informe

- En esta fase elaboramos la realización del informe con los hallazgos, que contiene una descripción detallada de los hallazgos relevantes al caso y la forma como fueron encontrados.
 - Descripción del caso
 - Sistema atacado
 - Valoración de daños
 - Descripción del ataque
 - Anexos

Agenda

- Introducción
- Metodología y procedimientos
- Herramientas
- Caso de estudio
- Reto de análisis forense



Herramientas

- Aplicaciones comerciales:
 - Encase
- Aplicaciones opensource:
 - Sleuthkit, Autopsy, Helix, Fire, etc.
- La herramienta más importante es:



Agenda

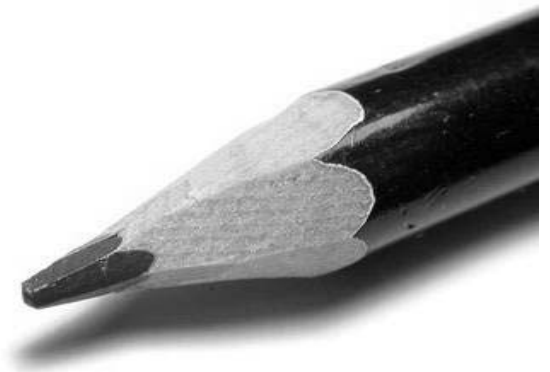
- Introducción
- Metodología y procedimientos

Herramientas



Caso de estudio

- Reto de análisis forense



Agenda

- Introducción
- Metodología y procedimientos
- Herramientas

Caso de estudio



Reto de análisis forense



III Reto de Análisis Forense

- SSOO Win2003 server en partición de 5 GB
- Direccionamiento IP privado (no homologado)
- Buen nivel de parcheado, excepto 3 o 4, uno de ellos el de WMF y alguno de IE.
- Standalone
- Apache+PHP+MySQL
- PostgreSQL
- DNS
- Compartición de archivos
- 2 cuentas de administración y 5 de usuarios sin privilegios
- WebERP

Descarga y comprobación imagen

- Bajar la imagen
- Descomprimirla
- Hacer el md5 comprobando la integridad
> *md5sum.exe windows2003.img*

Montaje de la imagen

- Para montar la imagen utilizamos Filedisk por ser licencia GPL

> *filedisk /mount 0 d:\windows2003.img /ro z:*

Recogida de datos

- Recogida de datos del sistema en:

%systemroot%\system32\config

- con los siguientes nombres:

SECURITY, SOFTWARE, SYSTEM, SAM DEFAULT

Inicios de sesión

- INICIOS DE SESION*

*Fuente: Microsoft technet

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/e104c96f-e243-41c5-aaea-d046555a079d.mspx?mfr=true>

Logs

- LOGS (%systemroot%\system32\config
 - SysEvent.Evt
 - SecEvent.Evt
 - AppEvent.Evt
- Aplicación: Visor de sucesos (eventvwr.msc)

Perfil de usuario

- Registro del perfil de usuario:

Documents and Settings\<<nombre usuario>>\NTuser.dat

- Dicho fichero se carga la sección HKEY_CURRENT_USER del Registro y cuando se inicia sesión y cuando cierra se actualiza.

Histórico de navegación






- Internet Explorer

- \Documents and Settings\\Local Settings\Temporary Internet Files\Content.IE5\
– \Documents and Settings\\Cookies\
– \Documents and Settings\\Local Settings\History\History.IE5\

pasco -d -t index.dat > index.txt

Referencias

CRIME
SCENE - DO NOT CROSS

- “Helix Live CD”, e-fense
 URL: <http://www.e-fense.com/helix/>
- “Computer Forensics Resources”, Forensics.NL
 URL: <http://www.forensics.nl/toolkits>
- “JISK - Forensics”, Jessland Security Services
 URL: <http://www.jessland.net>
- “GNU Utilities for Win32”, Sourceforge Project
 URL: <http://unxutils.sourceforge.net/>
- “Forensics Acquisition Utilities”, George M.Garner Jr.
 URL: <http://unxutils.sourceforge.net/>
- “Windows Forensic Toolchest”, Fool Moon Software & Security
 URL:

