Digital Forensics

Proceso

1. Identification
2. Preservation
3. Collection
4. Analysis
5. Reporting

Data Representation
- Binary
- Base64
- Hexadecimal
- Octal
- ASCII

Conceptos

Disks
- Hard Disk Basics
  - Platter/Disk
  - Sectors — subdivisión de una pista en un disco magnético u óptico
  - Clusters — es un grupo de sectores dentro de un disco y es la agrupación por lo que se organizan los archivos del disco
  - Slack Space
- Solid State Disk Drive Basics
  - Garbage Collection — recolección de basura es un process utilizado por las unidades de estado sólido para optimizar el espacio y mejorar la eficiencia
  - Trim — los datos eliminados serán borrados definitivamente
  - Wear Leveling — La nivelación del desgaste es una técnica que algunos SSD utilizan para aumentar la vida útil de la memoria mediante un enfoque muy sencillo: distribuir uniformemente la escritura en todos los bloques de un SSD para que se desgasten de forma uniforme

File Systems — Los sistema de archivos es un conjunto de tipos de datos que se emplea para:
- Almacenamiento de datos
- La categorización jerárquica
- La gestión de datos
- La navegación de archivos
- Acceder a los datos
- Recuperación de datos

- FAT16
- FAT32
- NTFS
- EXT3/EXT4

Analizar — FTK Imager

Memory — se almacena información/datos de forma inmediata

Pagefile (Windows) — se almacenan datos cuando la memoria está llena, datos que el sistema no está usando activamente. También como backup en caso de caida

Swapfile (Linux) — usa una partición para almacenar datos que no caben en memoria
```
#free -h
#swapon --show
```

Hibernation File (Windows) — todos los datos de memoria se copian al fichero hiberfil.sys

Digital Evidence and Handling

Digital Evidence Collection
- FTK Imager
  - Dumping Memory
  - Hard Drive Imaging
- Live Acquisition — KAPE

Manipulación
- No alterar pruebas originales
- Asegurarse de utilizar bloqueadores de escritura
- Cada acción que se realiza debe documentarse de una forma u otra

- E-mails
- Digital Photographs
- Logs
- Files
- Messages
- Browser History
- Backups
- Video/audio files

Order of Volatility

1. Registers & Cache
2. Memory
3. Disk
4. Remote Logging and Monitoring Data
5. Physical Configuration, Network Topology, Archival Media

Metadata and File Carving

```
- METADATA
Windows:
Propiedades del archivo

Linux:
#ls -lisap <file>
#stat <file>
#exiftool
```

```
- FILE CARVING
#/etc/scalpel/scalpel.conf
#scalpel -b -o <output> <disk image file>
```

Windows Investigations

Artefactos
- LNK Files — Windows File Analyzer
  ```
  Enlaza un archivo con otro.

  Ruta: C:\Users\$USER$\AppData\Roaming\Microsoft\Windows\Recent
  ```
- Prefetch Files — Prefetch Explorer Command Line — PECmd.exe -k "palabra_buscar" -d "C:\Users\PATH\TOOOS\Prefetch\"
  ```
  Proporciona información sobre programas: ruta, cuándo se ejecutó, cuándo se creó, etc

  Ruta: C:\Windows\Prefetch
  ```
- Jump List Files — JumpList Explorer
  ```
  automaticDestination-ms y customDestination-ms.
  Estos archivos contienen información sobre las aplicaciones que se fijan en la barra de tareas,
  como la ruta del archivo, las marcas de tiempo y los identificadores de la aplicación (AppID)

  Ruta: C:\Users\$ USERNAME%\AppData\ Roaming\Microsoft\Windows\Recent\AutomaticDestinations
  C:\Users\%USERNAME%\AppData\ Roaming\Microsoft\Windows\Recent\CustomDestination
  ```
- Browsers
  - Cookies
  - Favorites
  - Downloaded Files
  - URLs Visited
  - Searches
  - Cached Webpage
  - Cached Images

  Acquisition via
  - KAPE
  - Browser History Viewer
  - Browser History Capturer

Operating System
- Logon Events
  - Event ID 4624 (Successful Logon) — Logon Type
    - 2 - Interactive (interactively logged on, meaning a physical logon to the device)
    - 3 - Network (accessed system via network)
    - 4 - Batch (started as an automated batch job)
    - 5 - Service (a Windows service started by service controller)
    - 6 - Proxy (proxy logon; not used in Windows NT or Windows 2000)
    - 7 - Unlock (unlock workstation - think Interactive logon, but unlocking to resume a previous session)
    - 8 - NetworkCleartext (network logon with cleartext credentials)
    - 9 - NewCredentials (used by RunAs when the /netonly option is used)
  - Event ID 4672 (Special Logon) — Cuando un usuario con permisos de administrador se loga en el sistema — Trazear por el "Logon ID"
  - Event ID 4625 (Failed Logon)

NETLOGON LOGONERR CODE	DESCRIPTION
0xC0000064	The specified user does not exist
0xC000006A	The value provided as the current password is not correct
0xC000006C	Password policy not met
0xC000006D	The attempted logon is invalid due to a bad user name
0xC000006E	User account restriction has prevented successful login
0xC000006F	The user account has time restrictions and may not be logged onto at this time
0xC0000070	The user is restricted and may not log on from the source workstation
0xC0000071	The user account's password has expired
0xC0000072	The user account is currently disabled
0xC000009A	Insufficient system resources
0xC0000193	The user's account has expired
0xC000020A	User must change his password before he logs on the first time
0xC0000234	The user account has been automatically locked

  - Event ID 4634 (Logoff)
- RDP Usage
- Cookies
- Recycle Bin

Linux Investigations

Artefacts

Passwd and Shadow — Cracking Passwords
```
# unshadow passwd shadow > Crack/HV
# john CrackMe --wordlist=rockyou.txt
```

Avalib — Lista de software instalado
```
# /var/lib/dpkg/status
or
# cat status | grep Package > packages.txt
```

Avalog
- Operating System Logs
  - /var/log/auth.log – Contains system authorization information, including user logins
  - /var/log/dpkg.log – Contains information that is logged when a package is installed or removed using the 'dpkg' command
  - /var/log/btmp – This file contains information about failed login attempts
  - /var/log/cron – Whenever the cron daemon starts a cron job, it logs the information about the cron job in this file
  - /var/log/secure – Contains information related to authentication and authorization privileges. For example, sshd (the daemon used for the SSH service) logs all the messages here, including unsuccessful login attempts
  - /var/log/faillog – Contains user failed login attempts
- Web Server Logs — /var/log/apache2/access.log

User Files
- Bash History
  ```
  bash_history > en Home
  # ls -a
  ```
- Hidden Files
- Clear Files — cualquier archivo que sea accesible a través de medios estándar
- Steganography
  - Ocultar ZIPs en imágenes
    ```
    # cat imagen.jpg secretmessage.zip > imagen2.jpg
    ```
  - Ocultar/extraer mensajes en imágenes
    ```
    # steghide embed -cf imagen.jpg -ef secretmessage
    # steghide extract -sf imagen.jpg
    ```
  - Ocultar strings en metadatos
    ```
    # exiftool -Comment="Comentario1" imagen.jpg
    ```

Analysis

Memory Analysis — Volatility

Command Line
- Lista de todos los procesos ejecutados
- Lista de conexiones activas y cerradas
- Vista de historial de Internet (IE)
- Identifica archivos en el sistema y recuperarlos del volcado de memoria
- Lee el contenido de los documentos de bloc de notas
- Recupera los comandos introducidos en el símbolo del sistema de Windows (CMD)
- Escanea la presencia de malware utilizando las reglas de YARA
- Recupera capturas de pantalla y contenidos del portapapeles
- Recupera contraseñas con hash
- Recupera claves y certificados SSL

```
# volatility -f memdump.mem imageinfo // Toma la imagen de memoria "memdump.mem" y determina el perfil sugerido para el análisis. El perfil es el sistema operativo, la versión y la arquitectura.

# volatility -f memdump.mem --profile=PROFILE pslist // Toma la imagen de memoria, proporciona el perfil, y luego utiliza el plugin pslist para imprimir una lista de procesos en la terminal.

# volatility -f memdump.mem --profile=PROFILE pstree // Utiliza el plugin pstree para imprimir un árbol de procesos en la terminal.

# volatility -f memdump.mem --profile=PROFILE psscan // Utilice el plugin psscan para imprimir todos los procesos disponibles, incluyendo los ocultos que suelen ser utilizados por el malware.

# volatility -f memdump.mem --profile=PROFILE psxview // Utilice el plugin psxview para imprimir los procesos esperados y ocultos. Es una combinación de los plugins pslist y psscan.

# volatility -f memdump.mem --profile=PROFILE netscan // Utilice el plugin netscan para identificar cualquier conexión de red activa o cerrada.

# volatility -f memdump.mem --profile=PROFILE timeliner // Utilice el plugin timeliner para crear una línea de tiempo de los eventos de la imagen de memoria.

# volatility -f memdump.mem --profile=PROFILE iehistory // Utiliza el plugin iehistory para extraer el historial de navegación de Internet.

# volatility -f memdump.mem --profile=PROFILE filescan // Utiliza el plugin filescan para identificar cualquier archivo en el sistema desde la imagen de memoria.

# volatility -f memdump.mem --profile=PROFILE dumpfiles -n --dump-dir=. // Utiliza el plugin dumpfiles para recuperar archivos de la imagen de memoria.

# volatility -f memdump.mem --profile=PROFILE cmdlist // Mostrar los argumentos de la línea de comandos del proceso.

# volatility -f memdump.mem --profile=PROFILE procdump -p NUMERO --dump-dir \PATH\ // Dump del .exe y dlls del proceso en el directorio actual
```

Disk Analysis — Autopsy
- Búsqueda por palabras clave
- Análisis de la línea de tiempo
- Análisis de archivos LNK
- Análisis de correo electrónico
- Clasificación por tipo de archivo
- Reproducción de medios
- Visor de miniaturas
- Análisis robusto del sistema de archivos
- Filtrado de conjuntos Hash
- Extracción de cadenas Unicode
- Detección de tipos de archivos basada en firmas y detección de desajustes en las extensiones