Turbo_Resumen_Express.txt

la informatica forense es el proceso de identificar, preservar, analizar y presentar evidencias de una forma legar y aceptable aplicando técnicas científicas y analíticas especializadas a la infraestructura tecnológica.
Principio de locardx: siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto

Funciones o ambito de actuacion
recopilación y preservacion de pruebas digitales
Analissi de pruiebas
Recuperacion de datos
investigacion de incidentes de seguridad
analisis de redes y cominicaciones
creacion de informes y testimonio en tribunales
asesoria y capacitacion
investigacion y desarrollo

Guias para el proceso de investifgdacion forense

Estandares:
AENOR e IOS/IEC

Familia 71505:
-1 Vocabulario y principios generales
-2 Buenas prácticas
-3 Formatos y mecanismos técnicos

UNE 71506: Metodología para el análisis forense de las evidencias
- Preservación
- Adquisición
- Docimentación
- Anbalisis
- Presentacion

UNE 1927010: Criterios generales para elaboración de informes

ISO 27037 Guias para identificación, recolección, adquisición y preservacion de evidencias digitales
ISO 27042: Guias para el analisis e interpretación de evidencias

Proceso de investigación forense (Preparación, identificacion, adquisición, preservacion, analissi y presentacion PIAPAP)
1. Preparación del caso
Es importante hacer una preparación previa para poder adquirir las evidencias correctamente y que todo sea correcto legalmente: contar con los permisos, autorización y contrato

Aseguirar la escena para evitar modificación o destrucción de las evidencias digitales

2. Identificación
Consiste en detectar y localziar fuentes de evidencia digital
Se debe determinar la fuente de los datos, ubnicación y relación con el incidente investigado
Incluye la evaluación preliminar de los dispositivos y mdedios de almacenamiento apra evitar alteraciones
Revisar entorno legal que protege el bien
INICIO de cadena de custodia

2.1 Revisión de enterono legarl que protege el bien
Analizar normativas y regulaciones aplicables a la evidencia digital y al bien protegido, asegurando que la recolección, adquisición y análisis de los datos se realicend e manera legarl y sean adminisibles en un proceso judicial

2.2 Cadena de custodia
Procedimiento mediante el cual se garantiza la autenticidad de la prueba digital desde su obtención hasta que se aporta como hecho porbatorio a un procedimiento judicial.

Es fundamental mantener la cadenad e custodia para garantizar que la evedencia digital sea adminisble en un tribunal.
Para garantizar la cadena de custiodia se debe documentar detalles de:
- descubrimiento y recolección de la evidencia
- Manejo de la evidencia
- Quien custodió la evidencia
- Cambios de custodia

3. Adquisición

Recopilación de pruebas digitales de dispositivos electrónicos usando técnicas y herramientas especializadas para garantizar la integridad y autenticidad de los datos
Debe documentarse para garantizar la cadena de custodia.
La adquisición se debe hacer por orden de volatilidad, comenzando por registros y cache, pasando a ram, archivos temporales, disco....

Hay 2 modos de adquisición:
- Live: compleja, se hace volcado de RAM y se tira del cable
- DEAD: más siple, se tira del cable a machete

Clonado: consiste en realizar una copia exacta bit a bit de un disco, incluyendo errores osectores defectuosos.
Objetivos: Disponer de una copia sobre la que realizar el analisis sin alterar la prueba.
HHerramientas: dd, dcfldd, dc3dd, FTK Imager
OJO: NO SE DEBE MONTAR NUNCA EL DISCO

clonado dd: DD if=/dev/sda of=/dev/sdb bs=1M

Integridad: es preciso asegurar que los datos clonados son una copia original, para ello se usan funciones hash SHA-2 o SHA-3, aunque en caso de no disponer de estas se pueden combinar MD5 y SHA-1
Si se hace clonado con dc3dd se puede comprobar al vuelo: dc3dd if=/dev/sdb of/imagen5.img hash=md5,sha256

4. Preservación

Adecuado tratamiento y documentación de las evidencias garantizando la cadena de custodia. se deben documentar los procedimientos

5. Analisis+
Examinar los datos recopilados
Autopsy, creado por brian portaaviones, open source,, permite trabajo en equipo y es multiplataforma

Volatility: Analisis forense de memoria, tiene 2 versiones

6. Presentación de los resultados
recopilar y documentar toda la onfo obtenida para genrar un informe pericial.

El perito informatico es un experto en tecnologías de la información y sistremas informáticos
El perito forense es un experto en ciencias forenses
El perito informatico forense es un experto en informatica forense especializado en la identificación, preservación, análisis y presentación de pruebas digitales en investigaciones y casos legales.

El perito judicial es unn profesional adotado de conocimientos especializados y reconocidos a través de sus estudios superiores que suministra información u opinión fundada a los tribunales de justicia sobre los puntos litigiosos que son materia de siu dicatamen

Perito de oficio: elegido por juez o tribunal
Perito de parte: Elegido por una de las partes y luego aceptado por juez o fiscal

código deontológico
Es un código de ética profesional que recoge un concepto de criterios, normas y valores que redacta y aceptan los profesionales de una actividad

Responsabilidades: Civilm penal, disciplinaria y provesional

Cuerpo oficial de Peritos colegiados (COP, conjunto de peritos colegiados.

Normativas en españa
LOPDGDD
Codigo Pejal
Ley de enjuiciamiento civil
Ley de enjuiciamiento Criminal
Ley de Servicios de la Sociedad de la informacióny comercio electrónico
Ley orgánica de protección de la seguridad ciudadana
Ley de conservación de datos

LOPDGDD: Regula la protección de datos personales en españay garantiza los derechos diitales de los ciudadanos. Está en consonancia con el GDPR que establece los requisitos estruicvtos en relaci

El codigo penal español contiene disposiciones para delitos informaticos

La ley de enjuiciamiento civil regula los procedimientos y procesos en casos civiles en españa

---

Analisis forense en windows

Un artefacto se refiere a cualquier objeto, dato o elemento almacenado en un sistema informático que pueda proporcionar información valiosa para una investigación. Hay 2 tipos:
- de aplicación
- de sistema operativo

Archivos de registro o logs
son artefactos interesantes en cualquier OS
Contienen información de eventos específicos, apps y servicios

Event logs: registros que se pueden encontrar en el event viewer o eventvwr.msc y están organizados en diferentes categorías como aplicación, seguridad configuración y sistema. Aqui se peuden ver inicios de sesión,

cambios de configuracion, fechas de acceso, permisos....
Los event losgs se pueden encontrar en %systemRoot%/System32/config o %SystemRoot%/system32/winevt/Logs dependiendo de si es previo o posterior a vista

Registros de aplicaciones
Muchas apps generan sus propios registros, se pueden encontrar en %APPData% para ususarios específicos o en %ProgramData% para todo el equipo

Registros sobre la instalación

Mirando en la raiz del sistema pueden ser:
- setupact.log: acciones de instalación
- setuperr.log errores de instalación
- WindowsUpdate.log: Actualizaciones del sistema y apolicaciones
- Debug/mrt.log Resultados de la erramienta de eliminación de malware de windows.
- Security/logs/scecomp.old: Componentes de windows que no se pudieron instalar
- /softwareDistribution/reportingEvents.log: Contiene eventos relacionados con la actualización
- /Logs/CBS/CBS.log: Almacena info relacionadas con el component based servicing, que se usa para administrar actualizaciones del sistema
- /inf/setupapi.dev.log: detecciones de nuevo dispositivo o actualización de driver existente
- /inf/setupapi.app.log: Instalación de componentes o aplicaciones
- /inf/setupapi.setup.log: Operaciones de instalación o config de windows
- /inf/setupapi.offline.log: Procesos o reparaciones realizados en modo fuera de linea
- /PANTHER*.log,xml: Información de acciones, errores cuando se actualiza desde una versión anterior de windows.
- /Performance/Winsat/winsat.log: Trazas de utilización de Windows System Assessment tool (WINSAT)

Papelera de reciclaje

Puede contener archivos borrados así como la fecha, hora y ubicación de la que fueron borrados
- En Windows 95 se encuentra en C:/RECYCLED
- En Sistemas NT pre VISTA en C:/RECYCLER
- en sistemas Post Vista en C:/$Recycle.Bin

En el interior de la carpeta de cada usuario hay 2 tipos de archivos:
- $I: Contienen el nombre,ruta y algunos datos del archivo
- $R: Contienen el contenido del arcivo original

Registro de Windows (Windows Registry)

Base de datos jerárquica que contiene info y conffig del SO y el HW, además de apps instaladas y preferencias de usuarios.
- Frecuencia y tiempo de uso de apps: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist, Se peude visualizar con USERAssistView
- Dispositivos USB conectados: HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Enum/USBStor
- Asociaciones de tipos de archivos y programas predeterminados: HKEY_CLASSES_ROOT/.<extension>

HKEYs

El registro de Windows se divide en varias secciones principales llamadas HKEYs (Handle to Registry Key)_
- HKEY_CLASSES_ROOT (HKCR): Info sobre tipos de archivos, extensines, asociaciones....
- HKEY_CURRENT_USER (HKCU): Info sobre configuraciones y preferencias de un usuario en la sesión actual.
- HKEY_LOCAL_MACHINE (HKLM): Guarda configuraciones y datos relacionados con Hardware, software y controladores del sistema
- HKEY_USERS (HKU): Almacena configuraciones y preferencias de todos los usuarios del sistema
- HKEY_CURRENT_CONFIG (HKCC): Contiene info sobre el perfil de hardware activo

Hives

El registro se agrupa en secciones lógicas conocidas como Hives, que son un grupo de claves, subclaves y valores relacionados con una parte específica del SO o las configs del usuario
Permiten organizar y estructurar la infod el registro, facilitando su administración y mantenimiento. Cada Hive se respalda en Hive Files que contienen copias de seguridad de sus datos.
- Los hives de respaldo para todos los hives (Salvo HKEY_CURRENT_USER) están en %SystemRoot%/System32/config.
- Los hives de respaldo para HKEY_CURRENT_USER estan en %UserProfile%

Algunos Hive files importantes son los siguientes:
- %SystemRoot%/System32/config/SAM: HKEY_LOCAL_MACHINE/SAM, archivos de Security Accounts Manager, contiene info de cuentas de usuario y sus contraselas hasheadas
- %SystemRoot%/System32/config/SECURITY: HKEY_LOCAL_MACHINE/SECURITY: Configuraciones de políticas de contraseña, bloqueo de cuentas, privilegios y control de acceso
- %SystemRoot%/System32/config/SOFTWARE: HKEY_LOCAL_MACHINE/SOFTWARE: Detalles sobre las aplicaciones instaladas
- %SystemRoot%/System32/config/SYSTEM: HKEY_LOCAL_MACHINE/SYSTEM: Detalles sobre el hardware de sistema, contiene también la clave de cifrado de las

contraseñas almacenadas en SAM
- %SystemRoot%/System32/config/DEFAULT: HKEY_USERS/DEFAULT: Contiene la configuracion de usuario predeterminada
- %UserProfile%/NTUSER.DAT: HKEY_USERS/<USER_ID>: Preferencias específicas del usuario.
- %UserProfile%/AppData/Local/Microsoft/Windows/UsrClass.dat: HKEY_CURRENT_USER\Software\Classes: Contiene información de las preferencias específicas del usuario

Listas MRU

Listas de lo utilizado de forma reciente (Most Recently Used), alamacenan info sobre los elementos utilizados más recientes en el sistema o aplicaciones específicas.
En el registro de Windows se pueden encontar en:
- HKEY_CURRENT_USER/Software/microsoft/Windows/CurrentVersion/Explorer/ComDlg32/OpenSavePid1MRU: Info sobre los archivos abiertos o guardados recientemente a través de cuadros de diálogo de Windows.
- HKEY_CURRENT_USER/Software/microsoft/Windows/CurrentVersion/Explorer/RunMRU: Comandos ejecutados en la ventana Windows + R. Se almacenan en orden de comando ejecutado

ShellBags

Donde el SO almacena la info relacionada con las preferencias de visualización de contenidos del Explorador de Windows. Se generan cuando un usuario abre una carpeta y personaliza la vista de dicha carpeta. Solo se guarda si se han abierto los contenidos al menos una vez
Pueden proprocionar información sobre las carpetas a las que el usuario ha accedido aunque ya no existan, además de marcas de tiempo.
Sen sistemas Post Windows Vista se pueden encontrar en HKEY_CURRENT_USER\Software\Microsoft\Windows\:
- Shell/Bags
- Shell/BagMRU
- ShellNoRoam/Bags
- ShellNoRoam/BagMRU
y en HKEY_CURRENT_USERS/Sotftware/Classes/local Settings/Software/microsoft/Windows/shell:
- BagMRU
- Bags

Shell y ShellNoRoam son iguales, diferenciándose en que las segundas

```
contienen config y preferencias del shell de windows no itinerantes.
Hay 2 tipos de ShellBags:
- Bags: Contienen info de las shellbags como la personalización de vista del
usuario
- BagMRU: Contiene info sobre el historial de carpetas visitadas por el
usuario




Herramientas


MiTecWindows Registry Revovery:
- Funciona en sistemas desde windows 95 hasta windows 10
- Sirve para realizar copias de seguridad con el registro.
- Uso gratuito para fines privados/educativos/no comerciales

ShellBags Explorer (SBE)







Prefetch

Es un componente de windows desde Win XP. Se usa para mejorar el
rendimniento y eficiencia de carga de aplicaciones. Realiza un seguimiento
de las apps y archivos usados conf recuencia y almacena info sobre como se
cargan el sistema
Para cada aplicación o proceso sometido a prefetching se genera un fichero
.pf con las referencias a los ficheros y directorios usuados en la carga de
la app
El fichero tendrá una huella temporal de la última ejecución de la
aplicación o proceso seleccionado.
Nos permite componer una línea temporal de eventos mediante el uso de sus
contenidos.
Prefetch se enceuntra en;
- HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Control/session Manager/Memory
Management/PrefetchParameters: 0 para deshabilitado, 1 para solo apps, 2
para solo arranque y 3 para aplicaciones y arranque
- %SYSTEMRoot/Prefetch: Aquí se encuentran los .pf, se recomienda obtenerlos
lo antes posible debido a su elevado nivel de volatilidad.
También se pueden analizar los contenidos de los archivos .pf con:
- prefetch Explorer Command Line
- Windows File Analyzer
- WinPrefetchView
```

SuperFetch

Aparece en Windows Vista. Monitoriza de forma continua el uso de los programas para la optimización de la asignación de memoria y precargado en RAM de elementos que se usan con mayor frecuencia según el patrón de uso del usuario.
A partir de Win 10 cambia su nombre por SysMain. Se pueden encontrar us archivos en:
- HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/sysmain: Configuración
- %SystemRoot%/Prefetch: Ficheros de base de datos de tipo Ag<nombre>.db

Sistemas de ficheros en Windows
Jerarquía de almacenamiento Bit > Byte > Sector > Cluster
El tamaño de los sectores y clusters se define en el encabezado del sistema de archivos, Los sistemas de archivos asignan espacio en disco a los archivos en clusters completos.

Partición: División de bajo nivel de un disco físico en regiones separadas y contiguas, define áreas específicas del disco pero no incluye sistema de archivos. Es una división lógica, mientras que un volúmen es una unidad formateada y lista para su uso
Volúmen: Área de almacenamiento formateada con un sistema de archivos y lista para guardar datos.

Sistemas de archivos FAT
File Allocation Table, tiene los siguientes comonentes clave:
- Sector de arranque: En el inicio del volumen, contiene info esencial sobre el sistema de arvhibos, incluye Bios Parameter Block (BPB) que da detalles necesarios para acceder correctamente al volúmen.
- Tabla de Asignación de Archivos (FAT): Actua como mapa del dispositivo, indicando si una zona está libre, asignada, es el fin de un archivo o es defectuosa.
- Región del directorio raiz: En Fat12 y Fat16 se ubica justo después de la región fat, tiene tamaño fijo, contiene entradas para archivos y subdirectorios. En FAT32 se almacena en la región de datos, permitiendo que se expanda
- Región de datos: Mayor parte del volúmen, está dividida en clusters que almacenan datos reales de archivos y directorios.

Forense en FAT
- Comprotamiento de eliminación de archivos: Al eliminar un archivo, el primer carácter de su entrada se reemplaza por 0xE5, permaneciendo el resto

del archivo intacto
- Retos de fragmentación: Fat tiende a la fragmentación, por lo que los datos de un archivo se dispersan en clusters no contiguos.
- Espacio residual: Debido a los tamaños fijos de los clusters, los archivos pequieños puieden no ocupar todo el espacio asignado, dejando sectores residuales que pueden contener restos de archivos eliminados
- Artefactos de timestamp: Fat registra las fechas de creación, modificación y acceso con precisión limitada. Los timestamps no incluyen info de la zona horaria.
- Almacenamiento de nombres de archivos: Los nombres largos se almacenan mediante entradas de directorio especiales, generando artefactos.
- Recuperación de entradas FAT: Para proteger contra la corrupción los datos se almacenan dos fats, siendo uno el principal y el otro actuando como copia de seguridad.

Sistemas de archivos NTFS
New Technology File System. Reemplaza a Fat, está optimizado para discos duros y soporta volúmenes y archivos de mayor tamaño. NTFS utiliza archivos especiales cuyos nombres empiezan con el caracter del dolar.

NTFS tiene los siguientes componentes clave:
- Sector de arranque de partición (PBS): Ubicado al principiop del volúmen NTFS y almacenado en el registro $Boot. Contiene info esencial para inicial el SO y detelles sobre el sistema de arcjivos como el BPB.
- Área de datos: Es la región del volúmen donde se almacenan los archivos de usuario y los directorios, se gestiona con clusters y se controla su asignación con el archivo $Bitmap
- Mater File Table (MFT): Reside en la zona MFT del área de datos y actua como la base de datos central de NTFS.

Forense NTFS:
- Eliminación Lógica: Al eliminar un archivo, la entrada se marca como no usada, pero permanece intacta. Los clústeres de datos no se borra inmediatamente, por lo que pueden ser recuperados
- Slack Space: Puden quedar restos del archivo en el slack space si un archivo nuevo no llena complemtamente el cluster.
- Análisis de Volumne Shadow Copy (VSC): Función de NTFS que crea copias instantaneas de archivos o volúmenes incluso en uso. Permite recueprar versiones anteriores de archivos.

```
Forense en WhatsApp

Directorios

Whatsapp emplea varios directorios para almacenar sus datos:
- Externo (Público): /android/media/com.whatsapp/WhatsApp, /WhatsApp,
/sdcard/WhatsApp/
  * Cualquier usuario puede acceder: el ADB puede acceder si el debugging
USB está activado en el dispositivo
- Interno (Privado). /data/data/com.whatsapp/, /data/app/com.whatsapp-2.apk
  * Hay que ser root para acceder
Ficheros importantes:
- Clave de cifrado: /data/data/com.whatsapp/files -> key
- BBDD Contactos: /data/data/com.whatsapp/databases -> wa.db (SQLite v.3)
- BBDD chats: /data/data/com.whatsapp/databases ->msgstore.db (SQLite v.3)
- Backups de BBDD chats (AES 256): /mnt/sdcard/Whatsapp/Databases ->
msgstore.db.cryptXX, msgstore-<fecha>.cryptXX



Chats cifrados
La BBDD de chats está en la zona privada, mientras que los backups cifrados
están en la pública, en /WhatsApp/databases/msgstore.db.cryptXX.
Puede ser extraida con DADB pull (adb.exe pull
/storage/self/primary/WhatsApp/Databases <Ruta de guardado>)
Para descifrar las bases de datos se necesita la clave almacenada en el
archivo key dentro de /data/data/com.whatsapp/files, ubicación para la que
es
necesario ser root para acceder.

Como obtener la Key sin ser Root
Para acceder a la Key sin ser root tan solo es necesario hacer downgrade de
la APK de Whatsapp siguiendo el siguiente procedimiento:
1. Borrar la apk de whatsapp
2. Instalar una versión aintigua que sea vulnerable
3. Acceder al contenido del fichero key
4. Reinstalar la versión de WhatsApp que se tenía de base









Forense Telegram

Directorios

Telegram usa varios directorios para almacenar sus datos:
- Externo: /Android/media/org.telegram.messenger/Telegram, /Telegram,
/sdcard/Telegram/, Cualquier usuario puede acceder mediante el uso de ADB
```

```
- Interno: /data/data/org.telegram.messenger/,
/data/app/org/telegram.messenger.apk, se necesita root para acceder

Ficheros:
- BBDD chats:
  * /data/data/org.telegram.messenger/files -> cache4.db (SQLite v.3)
  * /data/data/org.telegram.messenger/files/account1 -> cache4.db (SQLite
v.3)
  * /data/data/org.telegram.messenger/files/account2 -> cache4.db (SQLite
v.3)
  * /data/data/org.telegram.messenger/files/account3 -> cache4.db (SQLite
v.3)
- BBDD de rutas a ficheros cacheados:
/data/data/org.telegram.messenger/files -> file_to_path.db
- Ajustes y preferencias: /data/data/org.telegram.messenger/shared_prefs



Chats inaccesibles
La BBDD de chats está en una zona privada y no hay backups locales como en
whatsapp





--------------------------------------------------------------------------
--------------------------------------------------------------------------
----------------------



Autopsy

Plataforma de analisis forense digital de dispositivos de almacenamiento con
GUI extensible basada en módulos. Tiene 2 modos de funcionamiento
- Single User: En una sola máquina con un usuario analizando las evidencias
localmente, tiene un consumo de recuros alto
- Multi User Cluster: Distribución de procesamiento forense entre varios
nodos en un clúster, permitiendo colaboración y mayor capacidad de análisis

Típos de Módulos de Autopsy:
- Módulos de Ingesta: Se ejecutan durante el análisis para extraer, analizar
y categorizar los datos forenses.
- Módulos de Reporte: es encargan de generar los informes sobre los
hallazgos obtenidos durante el análisis.
- Módulos de visualización de contenido: Facilitan la inspección de archivos
individuales dentro de la interfaz de autopsy.
- Modulos de visualización de resultados: Permiten al analista explorar y
organizar los resultados obtenidos. Se centran en la presentación de datos
```

procesados.

Tipos de Ingest módules:
- Picture Analyzer: Analiza imágenes
- GPX Analyzer: Extrae y analiza datos deg eolocalización
- Android Analyzer: Profundiza en datos forenses de dispositivos android
- IOS Analyzer: Analiza dispositivos IOS
- DJI Drone analyzer: Extrae y analiza datos forenses de drones DJI
- Embedded File Extractor: Extrae archivos incrustados dentro de otros documentos
- PhotoRec Carver: Recupera archivos eliminados del espacio sin asignar del disco mediante técnicas de carving
- Virtual Machine Extractor: detecta y extrae archivos de máquinas virtuales.
- Hash Lookup: Compara archivos con BBDD de hashes conocidos para detectar archivos maliciosos o verificar integridad
- File Type identification: Determina el tipo de archivo basado en su estructura
- Extension Mismatch Detector: Detecta discrepancias entre la extensi´no del archivo y su formato real
- Data Source Integrity: Verigica la integrida de los datos en la imagen forense
- Recent Activity: Extrae la actividad reciente del Usuario
- Keyword Search: Permite buscar palabras claves entre distintos archivos y artefactos
- Email parser: Procesa correos electrónicos en diversos formatos
- Plaso: procesa logs y reconstruye la cronología de eventos
- Cyber Triage Malware Scanner: Escanea u busca malware
- YARA analyzer: Usa reglas YARA para detectar archivos sospechosos
- Encryption detection: Detecta la presencia de archivos cifrados
- Interesting Files Identifier: Señala archivos relevantes basados en reglas predefinidas

---

Volatility

Es un framework forense de memoria RAM de código abierto. Se puede usar para el análisis y extracción de datos volátiles de sistemas en ejecución.
Permite:
- Analizar dumps de memoria
- Identificar procesos, conexiones de red y módulos cargados
- Detectar malware en memoria.

Versiones de Volatility:

```
- Volatility2:
  * Descontinuado
  * Basado en Perfiles estáticos
  * Plugins asociados a perfiles de memoria concretos

- Volatility3:
  * Los perfiles de memoria funcionan de forma dinámica
  * Los plugins se basan en el modelo de objeto



Perfiles de Memoria y Symbol Tables
- Perfiles de memoria (Volatility2)
  * Permiten intempretar correctamente la estructura interna de un volcado
de memoria
  * Así se pueden identificar procesos, módulos, conexiones y otros datos
del SO
  * Puede ser válido para más de una versión de un SO.

- Symbol Tables (Volatility 3)
  * Se encargan de representar las estructuras de memoria del SO


Comandos importantes de volatility2:
- imageinfo: Permite ver datos del volcado de memoria y sugiere que perfiles
podemos usar -> volatility2 -f /eivdencia.raw imageinfo
- pslist: permite ver los procesos en ejecución -> volatility2 -f
/evidencia.raw --profile=<perfil> pslist
- netscan: Detecta las conexiones activas -> volatility2 -f /evidencia.raw -
-profile=<perfil> netscan
- cmdscan: Extrae el historial de comandos -> volatility2 -f /evidencia.raw
--profile=<perfil> cmdscan
- filescan: Lista los archivos cargados en memoria -> volatility2 -f
/evidencia.raw --profile=<perfil> filescan
- dumpfiles: Permite extraer ficheros de la memoria -> volatility2 -f
/evidencia.raw --profile=<perfil> dumpfiles -Q <Dirección de Memoria> -D
<Destino para guardar archivo>
- clipboard: Muestra los contenidos del portapapeles -> volatility2 -f
/evidencia.raw --profile=<perfil> clipboard
- procdump: Extrae la memoria correspondiente a un proceso -> volatility2 -f
/evidencia.raw --profile=<perfil> procdump -p <ID del Proceos> -D <Destino
para guardar el archivo>
- hivelist: Lista los gives del registro cargados en memoria -> volatility2
-f /evidencia.raw --profile=<perfil> hivelist
- hivedump: Muestra las subclaves de un hive -> volatility2 -f
/evidencia.raw --profile=<perfil> hivedump -o <Direccion de memoria>
- hashdump: Extrae los hashes de contraseñas de los usuarios -> volatility2
-f /evidencia.raw --profile=<perfil> hashdump


Comandos importantes volatility3:
```

```
- windows.info.Info: Muestra información sobre el volcado (Similar a
imageinfo) -> volatility3 windows.info.Info
- Windows.pslist: lista los procesos en ejecución -> volatility3
windows.pslist
- windows.netscan: Detecta las conexiones activas -> volatility3
windows.netscan
- windows.cmdscan: Extrae el historial de cmoandos -> volatility3
windows.cmdscan
- windows.filescan: Lista los archivos cargados en memoria -> -> volatility3
windows.filescan
- windows.dumpfiles: Extrae un fichero concreto de memoria o de un proceso
  * volatility3 windows.dumpfiles --virtaddr <dirección de memoria>
  * volatility3 windows.dumpfiles --pid <ID de proceso>
- windows.registry.hivelist: Lista los hives de registro cargados en memoria
-> volatility3 windows.registry.hivelist
- windows.hashdump: extrae los hashes de las contraseñas de los usuarios ->
volatility3 windows.hashdump
```

From:
https://www.knoppia.net/ - **Knoppia**

Permanent link:
https://www.knoppia.net/doku.php?id=master_cs:analisis_forense:restxt

Last update: **2025/07/01 13:33**