

PRÁCTICA 1: Análisis Post-mortem, los artefactos Windows

Objetivos principales de la práctica:

- **Analizar las evidencias que proporcionan los diferentes artefactos en los sistemas operativos Windows.**

PARTE A

Dale una lectura de repaso al tema 4 y contesta a las siguientes cuestiones:

1. Con respecto a los “prefetch”:
 - a. ¿Qué son?
 - b. ¿Qué extensión tienen los ficheros?
 - c. ¿En qué directorio los podemos encontrar?
 - d. ¿Qué información forense guardan que pueda ser importante para una investigación?
2. En cuanto a los “LOGs”
 - a. ¿Cuáles piensas que son los más importantes por el contenido que guardan?
 - b. ¿Dónde los podemos encontrar?
3. En cuanto al fichero de hibernación “hiberfil.sys”
 - a. ¿Dónde lo podemos encontrar?
 - b. ¿Qué herramienta podemos utilizar para decodificar su contenido?
 - c. ¿Piensas que es importante la información que contiene?
4. Con respecto a las instantáneas, puntos de restauración y/o volume shadow copies service (VSS):
 - a. ¿Qué sistema de archivos necesitamos para poder usar esta tecnología?
 - b. ¿Viene activada por defecto o la tiene que activar el usuario?
 - c. ¿Cada cuánto tiempo se realizan?
 - d. Piensa en un par de escenarios donde puedan ser de utilidad
5. Contesta a las siguientes cuestiones relacionadas con el registro de Windows:
 - a. Investiga cómo importar y exportar claves de registro en entornos CLI y GUI.
 - b. Enumera las claves que, desde un punto de vista forense, son interesantes exportar y analizar explicando qué información revelan.
6. ¿Qué tipos de eventos nos pueden interesar inspeccionar desde un punto de vista forense? Pon un par de ejemplos.
7. Investiga sobre qué herramientas software podemos utilizar a la hora de trabajar sobre los artefactos estudiados en el tema: prefetch, logs, fichero de hibernación, volume shadow copies service, registro del sistema, gestión de eventos, enlaces, cachés e historial de navegación y papelera de reciclaje.

PARTE B

La práctica consiste en extraer todas las evidencias posibles de un sistema operativo Windows haciendo búsquedas dirigidas a los diferentes artefactos de los que hace uso.

Aunque en la práctica real se haría en base a una imagen de un sistema operativo, en la presente práctica se recomienda, por agilidad, usar el sistema operativo que esté usando el alumnado en su equipo.

Software a utilizar:

- A. Windows 10 (32 o 64 bits)
- B. FTK Imager FTK Imager
- C. Arsenal Image Mounter
- D. Registry Explorer
- E. Reg Ripper
- F. WRR
- G. LinkParser
- H. JumpListExplorer
- I. ShellbagExplorer
- J. USB Detective

Se pide:

1. Utilizar FTK Imager para extraer de tu equipo y/o imagen montada los ficheros adecuados donde analizar las evidencias.
2. Repasar, uno por uno, los diferentes artefactos Windows que se listan a continuación e ir comentando con descripciones y/o capturas de pantalla la información que se va obteniendo. Obviamente para cada artefacto será necesario extraer con (1) la evidencia que recoge este tipo de información, como por ejemplo el registro de windows (C:\windows\system32\config SYTEM, SOFTWARE, SAM, etc)

- **Versión del sistema, nombre de la máquina y zona horaria.**

Software\Microsoft\Windows NT\CurrentVersion

- **Fecha de último acceso**

System\ControlSet001\Control\Filesystem

- **Hora de apagado**

System\ControlSet001\Control\Windows

- **Interfaces de red**

System\ControlSet001\Services\Tcpip\Parameters\Interfaces\{GUID_INTERFACE}

- **Histórico de redes**

Software\Microsoft\Windows NT\CurrentVersion\NetworkList\
Software\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Cache

- **Cuándo se conectó a una red**

Software\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles

- **Carpetas compartidas**

System\ControlSet001\Services\lanmanserver\Shares\

- **Programas de inicio**

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\RunOnce
Software\Microsoft\Windows\CurrentVersion\Runonce
Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
Software\Microsoft\Windows\CurrentVersion\Run

- **Búsquedas en la barra de búsqueda**

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery

- **Rutas en Inicio o Explorer**

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths

- **Documentos recientes**

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

- **Documentos ofimáticos recientes**

NTUSER.DAT\Software\Microsoft\Office\{Version}\{Excel|Word}\UserMRU

- **Posición de lectura sobre el último documento abierto**

NTUSER.DAT\Software\Microsoft\Office\Word\Reading Locations\Document X.

- **Ficheros ofimáticos autoguardados**

C:\Usuarios\AppData\Roaming\Microsoft\{Excel|Word|Powerpoint}\

- **OpenSaveMRU: Ficheros que han sido abiertos o guardados dentro de una ventana Windows.**

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaved
PidlMRU

- **Últimos comandos ejecutados**

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\Policies\RunMRU

- **UserAssistKey: Programas ejecutados desde el Escritorio**

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{GUID}\Cou
nt

- **Eventos asociados a la barra de tareas**

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\FeatureUsage

- **Aplicaciones recientes**

Software\Microsoft\Windows\Current Version\Search\RecentApps

- **Documentos recientes (LinkParses o LeCMD)**

C:\Users\\AppData\Roaming\Microsoft\Windows\Recent

- **Automatic & Custom destinations (JumpListExplorer)**

C:\Users\\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations
C:\Users\\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations

- **Shellbags: Acceso y tiempos MAC a directorios (ShellbagExplorer)**

USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags
USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU Desktop
NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU

- **Dispositivos MTP**

C:\users\Appdata\Local\Temp\WPDNSE\{GUID}

- **Almacenamiento USB. Identificadores de fabricante(VID) y de producto (PID)**

SYSTEM\ControlSet001\Enum\USBSTOR

- **Nombres de volúmenes USB**

SOFTWARE\Microsoft\Windows Portable Devices\Devices

- **Localizar el usuario que ha utilizado el USB**

System\MountedDevices

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\Mountpoints2

- **Número de serie de volumen lógico**

Software\Microsoft\Windows NT\CurrentVersion\EMDMgmt

- **Primera y última vez que se conectó el dispositivo**

System\ControlSet001\Enum\USBSTOR\{VEN_PROD_VERSION}\{USB
serial}\Properties\{83da6326- 97a6-4088-9453-a1923f573b29}\
C:\Windows\inf\setupapi.dev.log

- **Base de datos Cortana, si existiese, en versiones anteriores a Windows 10.0.17763.55 (Sqlite studio)**

\Users\user_name\AppData\Local\Packages\Microsoft.Windows.Cortana_xxxx\LocalState\ESDatabase_CortanaCoreInstance\CortanaCireDb.dat

- **Notificaciones de Windows (sqlite studio)**

\Users\{user_name}\AppData\Local\Microsoft\Windows\Notifications\wpndatabase.db

- **Timeline (Windows TimelineParser)**

\Users\{user_name}\AppData\Local\ConnectedDevicesPlatform\ActivitiesCache.db

- **Windows Store (SQLite Studio)**

\Users\{user_name}\ProgramData\Microsoft\Windows\AppRepository\StateRepositoryDeployment.srd

Software\Microsoft\Windows\CurrentVersion\Appx\AppxAllUserStore\Applications\
Software\Microsoft\Windows\CurrentVersion\Appx\AppxAllUserStore\Deleted\

- **Thumbnails (thumbviewer) & Thumbcaché (thumbcacheviewer)**

Ficheros "thumbs.db"

C:\Users\\AppData\Local\Microsoft\Windows\Explorer

- **Papelera de reciclaje**

Contenido de carpeta "\$Recycle.bin" (Rifiuti)

- **OfficeFileCache (OfficeFileCacheParser)**

\Users\(\Username)\AppData\Local\Microsoft\Office\(\Office Version)\OfficeFileCache

- **OfficeBacktage (OfficeBackstageParser)**

\{Users}\AppData\Local\Microsoft\Office\16.0\BackstageinAppNavCache

- **IP Pública (ETLParser)**

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Logs\

- **Histórico de PowerShell**

\{Users}\%AppData%\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt

- **Windows PREFETCH (LeCMD)**

C:\Windows\Prefetch

- **Windows SuperFetch (Crowndresponse)**

C:\Windows\Prefetch\Ag*.db

- **SRUM (SRUM DUMP y NetworkUsageView)**

C:\Windows\System32\sru\SRUDB.dat

- **ShimCache (ShimCacheParser)**

SYSTEM\CurrentControlSet\Control\SessionManager\AppcompatCache\AppCompatCache

- **AmCache (AmCacheParser)**

C:\Windows\AppCompat\Programas\Amcache.hve

- **Tareas programadas**

C:\Windows\Tasks o C:\Windows\System32\Tasks

- **Servicios (Registry Explorer)**

SYSTEM\ControlSet001\Services

- **BAM (DCode)**

SYSTEM\CurrentControlSet\Services\bam\UserSettings\{SID}

SYSTEM\CurrentControlSet\Services\bam\state\UserSettings\{SID}

- **Eventos (Event-Log Explorer)**

C:\Windows\system32\winevt\Logs