[AF] Análisis forense en sistemas Windows

Artefactos

Un aterfacto se refiere a cualquier objeto, dato o elemento almacenado en un sistema que pueda proporcionar información valiosa a una investigación. Hay 2 tipos:

- de aplicación
- de sistema operativo

Logs

Los archivos de registro o logs son artefactos interesantes en cualquier SO.

Registro de eventos

Sirve para obtener inicios de sesión, camibos de configuración, fechas, etc... Antiguamente se guardaban en %SystemRoot%\System32\config en formato .evt y actualmente van en %SystemRoot%\System32\winevt\Logs en formato evtx

NOTA: %WinDir% lleva al directorio de instalación de windows(legacy) y %SystemRoot% hace lo mismo, pero se usa en la actualidad, se recomienda usar el segundo.

Registros de aplicaciones

Pueden estar en varios sitios:

- Carpeta de instalación de la aplicación
- %AppData%: Ajustes de aplicación de un usuario
- %ProgramData%: Ajustes de aplicación comunes de todos los usuarios

Registros sobre la instalación

- %SystemRoot%\setupact.log: Información de las acciones de instalación
- %SystemRoot%\setuperr.log: Información sobre errores de instalación
- %SystemRoot%\WindowsUpdate.log: Registra información sobre actualización del sistema y aplicaciones
- %SystemRoot%\Debug\mrt.log: Resultados de la herramienta de eliminación de software malintencionado de windows (MSRT)
- %SystemRoot%\INF\setupapi.dev.log: Información de cada vez que se ha instalado un dispositivo nuevo
- %SystemRoot%\INF\setupapi.app.log: Instalación de componentes o aplicaciones
- %SystemRoot%\INF\setupapi.setup.log
- %SystemRoot%\INF\setupapi.offline.log

- %SystemRoot%\PANTHER*.log,xml: Info de errores cuando se actualiza desde otra versión

Y muchos más que están en las traspas

Papelera de Reciclaje

Almacena información de interés como archivos borrados e información sobre la fecha, hora y ubicación de los que fueron eliminados. La ruta de la papelera es C:\RECYCLED (Win 9x), C:\RECYCLER (W2000 hasta Svr2003) y C\$Recycle.bin (Vista en adelante). puede ser consultada con comandos de powershell. Dentro de la papelera hay 2 tipos de archivos

- comienzan con $I: Nombre, ruta original y algunos datos del archivo
- Comienzan por $R: Interior del archivo original

Registro de Windows

Es una base de datos jerárquica que contiene información del sistema operativo, hardware, aplicaciones, usuarios... Es muy importante desde un punto de vista forense por ello, guarda:

- Frecuencia y tiempo de uso de las aplicaciones
- Dispositivos conectados
- Asociaciones de tipos de archivos a programas

Una de las rutas más importantes es:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersión\Explorer\UserAssist
```

Que está codificada, pero puede ser vista por software de nirsoft. Por otro lado, podemos ver las asociaciones de archivos en:

```
\HKEY_CLASSES_ROOT\.pdf
```

En este caso nos daría Acrobat.Document.2020

HKEYS

El registro de windows se divide en varias secciones principales llamadas HKEYS (handle to Registry Key):

- HKEY_CLASSES_ROOT (HKCR): Información sobre tipos de archivos, extensiones, asociaciones de programas...
- HKEY_CURRENT_USER (HKCU): Almacena Configuraciones específicas del ususario
- HKEY_LOCAL_MACHINE (HKLM): Guarda configuración y datos relacionados con el Hardware, Software y controladores del sistema.
- HKEY_USERS (HKU): Almacena configuraciones de todos los usuarios en el sistema.
- HKEY_CURRENT_CONFIG (HKCC): Contiene información sobre el perfil de hardware activo.

Hives

El registro se agrupa en secciones lógicas llamadas Hives. Cada Hive se respalda en archivos auxiliares en disco, llamados Hive Files. Esta información se carga al registro en el arranque del sistema. Son esenciales para recuperar un sistema en caso de corrupción o pérdida de datos en el registro. Son muy importantes para obtener información desde el punto de vista forense. Se encuentran ubicados en la siguiente ruta:

```
%SystemRoot%\System32\config #Todo menos HKEY_CURRENT_USER
%SystemProfile% #Aquí se encuentra HKEY_CURRENT USER
```

Los hive files más importantes son:

- SAM:
  - Contiene las contraseñas de los usuarios y sus nombres
  - %SystemRoot\System32\Config\SAM, {SAM.LOG, SAM.SAV}
- SECURITY
  - Contiene información de control de acceso y bloqueo de cuentas
  - %SystemRoot\System32\Config\SECURITY {SECURITY.LOG, SECURITY.SAV}
- SOFTWARE
  - Contiene información de las aplicaciones
  - %SystemRoot\System32\Config\SOFTWARE {SOFTWARE.LOG, SOFTWARE.SAV}
- SYSTEM
  - Se necesita en conjunto con el SAM para poder obtener las contraseñas de los usuarios.
  - %SystemRoot\System32\Config\SYSTEM {SYSTEM.LOG, SYSTEM.SAV, SYSTEM.ALT}
- DEFAULT
  - Contiene información de la configuración del usuario
  - %SystemRoot\System32\Config\DEFAULT
- NTUSER.DAT
  - Contienen información propia del usuario como preferencias
  - %UserProfile%\NTUSER.DAT {.DAT .log .BAK}
- UsrClass.dat
  - Como el NTUSER.DAT pero en sistemas más modernos
  - %UserProfile%\AppDAta\Local\Microsoft\Windows\Usr.dat {.log}

Dentro de estos archivos puede haber otros archivos relacionados:

- .LOG: Archivo transaccional, guarda cosas que aún no se han guardado en el registro
- .SAV: Copia del archivo
- .ALT: Copia de seguridad alternativa

Listas MRU

Most Recently Used, son listas que almacenan infomación de los elementos usados más recientemente por el sistema operativo y aplicaciones. Esto se almacena para mejorar la eficiencia, no es de origen forense, pero nos permite ver que se ha hecho en un momento específico, como si se ha accedido a un archivo o si se han borrado cosas. Las MRU se pueden consultar en el regedit en:

```
HKEY_CURRENT_USER/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/ComDig3
```

```
2/OpenSavePidlMRU #Programas ejecutados recientemente
HKEY_CURRENT_USER/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/RunMRU
#Comandos ejecutados recientemente
```

ShellBags

Lugares donde el SO guarda información relacionada con las preferencias de visualización de archivos en Windows Explorer. Se generan automáticamente cuando un usuario abre una carpeta. Guardan información aunque las carpetas ya no existan. También guardan las fechas y horas, de forma que se puede reconstruir una cronología con esta información. Se encuentran en:

```
HKEY_CURRENT_USER/SOFTWARE/Microsoft/Windows/Shell/Bags #Info de como el
usuario ha personalizado la vista
HKEY_CURRENT_USER/SOFTWARE/Microsoft/Windows/Shell/BagMRU #ntuser.dat,
contiene el historial de carpetas visitadas por un usuario.
#Lo mimso pero para dominio:
HKEY_CURRENT_USER/SOFTWARE/Microsoft/Windows/ShellNoRoam/Bags
HKEY_CURRENT_USER/SOFTWARE/Microsoft/Windows/ShellNoRoam/BagMRU
```

Herramientas

- MiTec Windows Registry Recovery: Herramienta que permite cargar archivos de registro de un backup o de un hive file. Nos facilita la visualización de esta información.
- ShellBags Recovery

Prefetch y Superfetch

Son tecnologías de windows orientadas a la eficiencia del sistema, siendo **prefetch** la más antigua (Win XP), busca mejorar el rendimiento y eficiencia de la carga de aplicaciones. Cuando arranca una aplicación hace un seguimiento de que archivos carga una aplicación y los guarda para acelerar futuras ejecuciones. Los datos de Prefetch se pueden encontrar en:

```
HKEY_LOCAL_MACHINES/SYSTEM/CurrentControlSet/Control/session manager/ Memory
Management/PrefetchParameters #Si está habilitado o deshabilitado
%SystemRoot%/Prefetch #datos del prefetch
```

Para leer los contenidos de los prefetch se recomienda **Windows File Analyzer** o **WinPrefetchView**

Superfetch aparece en Windows Vista para monitorizar de forma contínua el uso de los programas y como usan estos la RAM con el objetivo de optimizar el rendimiento del sistema. A partir de Windows 10 se llama SysMain. Sus datos se pueden encontrar en:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sysmain
%SystemRoot%\prefetch
```

Sistemas de Ficheros

La jerarquía de almacenamiento es 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 el disco a los archivos en cluster completos. Generalmente se usan dos sitemas de archivos: FAT y NTFS. Cada uno de estos sistemas de archivos tienen diferentes parámetros que se definen en el encabezado del sistema de archivos. Cuando se borra un archivo quedan huecos en los sectores llamados Slack Space donde pueden quedar restos de los archivos que a veces se pueden recuperar mediante carving.

Sistema FAT

File Allocation Table, desarrollado en 1977 por Microsoft. Componentes clave:

- Sector de arranque
  - BIOS Parameter Block (BPB): proporciona detalles para acceder al volúmen, como el tamaño del cluster que puede ir de un sector de 512Bytes hasta 128 Sectores de 65.536 Bytes
  - información sobre el sistema de archivos
  - Ubicación del inicio del volúmen
- Tabla de Asignación de Archivos (FAT): Actúa como mapa del dispositivo de almacenamoento, cada entrada FAT se corresponde a un cluster en el disco, que indican si están:
  - Libre (Unallocated)
  - Asignados (Allocated)
  - Fin de archivo (EOF)
  - Defectuoso
- Región del directorio Raíz: Se ubica inmediatamente después de la región FAT
  - Tiene tamaño fijo
  - Contiene entradas para archivos y subdirectorios
  - En FAT32 el directorio raíz se almacena en la región de datos, permitiendo expandirla cuando sea necesario.
- Región de datos

Desde el punto de vista forense:

- Comportamiento de eliminación de archivos:
  - Al eliminar un archivo, el primer carácter de entrada de este pasa a ser 0xE5
  - El resto del archivo permanece intacto hasta que se sobreescriba la zona.
- Espacio Resiudal (Slack Space). Es lo que queda entre donde estaba el archivo y el resto del clúster. Si en un cluster caben 10 cosas y se quieren almacenar 11 cosas, se usan 2 clusters, quedando 9 secciones del segundo cluster libres
- Timestamp: Las fechas no son muy precisas, lo que es un problema para reconstruir la línea de tiempo y no se guarda la zona horaria.
- Almacenamiento del nombre de archivos: Los guarda en formato 8.3 (8 caracteres y extensión de 3 caracteres)
  - Fat guarda como 2 veces, guarda una vez el nombre del archivo, por ejemplo, para InformeConfidencial.docx guarda un archivo INFORM~1.DOC y el nombre en otros archivos a parte.
- Recuperación de entradas FAT: Suele haber un FAT1 y un FAT2, reflejándose los cambios en

FAT1 en FAT2 con mirroring

NTFS

New Technology File System, aparece con Windows NT 3.1 para optimizar el almacenaje en discos duros, mientras que FAT era para disquettes. NTFS guarda la información en unos archivos especiales que empiezan por $:

- Sector de Arranque de Partición (PBS): Ubicado al inicio del volúmen NTFS y almacenado en $$Boot
- MFT (Master File Table): El archivo $MFT reside en la zona MFT del área de datos y actua como la base de datos central de NTFS, registrando información de cada archivo y dato del volúmen.
- Eliminación Lógica: cuando se elimina un archivo, se marca esa zona como no usada en la MFT, siguiendo esos datos ahí.
- Slack Space: Similar al de FAT, pero en menor medida ya que los archivos pequeños pueden ser almacenados directamente en la MFT sin usar el cluster.
- Análisis de Volume Shadow Copy (VSC): Función de NTFS que crea copias de archivos o volúmenes.
    - Permite recuperar versiones anteriores de archivos, incluyendo eliminados y modificados.