[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:

```
HKEY_CURRENT_USER/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/ComDig32/OpenSavePidlMRU #Programas ejecutados recientemente
HKEY_CURRENT_USER/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/RunMRU #Comandos ejecutados recientemente
```

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

Permanent link:
http://www.knoppia.net/doku.php?id=master_cs:analisis_forense:windows&rev=1741197306

Last update: **2025/03/05 17:55**