

---

*IES Zaidín-Vergeles*

*Análisis Forense en Windows. Los artefactos.*

*25 de febrero de 2021*



---

## Tabla de contenidos

---

<b>1. Introducción</b>	<b>1</b>
<b>2. Los Prefetch</b>	<b>3</b>
2.1. SuperFetch . . . . .	4
<b>3. Los Logs</b>	<b>5</b>
<b>4. Ficheros de Hibernación</b>	<b>11</b>
<b>5. Volume Shadow Copy</b>	<b>13</b>
<b>6. Registro del Sistema</b>	<b>15</b>
6.1. Cómo se guardan los datos . . . . .	16
6.1.1. Editor del registro . . . . .	17
6.2. Los subárboles . . . . .	17
6.3. Las Listas MRU . . . . .	18
<b>7. Eventos EVTX</b>	<b>21</b>
7.1. Definición de eventos EVTX . . . . .	22
<b>8. Herramientas</b>	<b>25</b>
8.1. Log Parser . . . . .	25
<b>9. LNK Shortcuts</b>	<b>27</b>
<b>10. Otras evidencias</b>	<b>29</b>
10.1. Navegación . . . . .	29
10.2. Papelera de reciclaje . . . . .	30
10.3. Los metadatos . . . . .	31
10.4. Datos de red . . . . .	32
<b>11. Conclusiones</b>	<b>33</b>



# CAPÍTULO 1

---

## Introducción

---

Los artefactos en Windows son cruciales ya que aportan muchísima información para los análisis forenses. En el presente capítulo se muestran distintos tipos de artefactos y se indica dónde encontrarlos: el registro del sistema (Hives), los prefetch, los distintos logs (entre ellos los logs de instalación de Windows), los ficheros de hibernación y los eventos.

Existen además otras evidencias importantes como la navegación, la papelera de reciclaje, los metadatos, datos de red y otras fuentes de información.



# CAPÍTULO 2

---

## Los Prefetch

---

Esta característica de «precarga» mejora el rendimiento del sistema de forma clara y comenzó a implementarse en la versión XP y se ha mantenido hasta la versión actual de Windows 10 (Windows\Prefetch). Cuando se enciende un sistema Windows, el sistema operativo realiza un seguimiento del inicio y de los programas que se abren habitualmente. Windows guarda esta información en un conjunto de archivos en la carpeta Prefetch. Estos archivos son pequeños, pero facilitan que el inicio del sistema se haga más rápido ya que el sistema operativo accede a ellos para conseguirlo. Se dice que Windows realiza «prefetching» al arrancar o al lanzar aplicaciones.

Existen distintos programas que nos permiten ver el contenido de los prefetch (ficheros .pf), un ejemplo es «WinPrefetch View» de Nirsoft.

Los ficheros .pf se encuentran en «%WINDIR%\prefetch», por cada programa ejecutado se crea un nuevo prefetch que contiene información sobre el programa, como son el path, la fecha y hora de modificación creación y última vez que se ejecutó, así como una lista de las dependencias cargadas por la aplicación en los primeros 30 segundos de su ejecución.

El archivo “pf” también registra información sobre el disco, el GUID y la marca de tiempo de creación de la unidad. Esta información se almacena para todos los volúmenes y es útil para encontrar GUIDS de unidades externas. En algunas pericias es interesante este dato y se puede comparar con las unidades externas utilizadas para poner en marcha las aplicaciones o para descubrir los archivos que han sido abiertos desde el propio dispositivo o disco duro externo y puede ser importante reflejar esto en el análisis pericial.

El funcionamiento básicamente consiste en que «windows cache manager» monitoriza los 10 primeros segundos de la ejecución de cualquier programa almacenando las páginas de memoria que son accedidas con más frecuencia, este proceso se realiza a través de «svchost» y esto se vuelve en un fichero prefetch cuyo nombre tendrá la nomenclatura «programa.extension-HASH.pf».

## 2.1 SuperFetch

SuperFetch es una mejora que empieza en Windows Vista. Incrementa aún más el rendimiento ya que se crea una cache de ficheros a los que cada aplicación accede más frecuentemente. La siguiente mejora vino con Windows 7 donde en función del rendimiento del disco se habilita o deshabilita esta característica. En Windows 7 esta información se guarda en el registro de Windows: HKEY LOCAL MACHINE\SYSTEM\CurrentControlSet\services\sysmain.

SuperFetch no reemplaza al servicio de Prefetch y debido a su efectividad sigue existiendo en Windows 8 y Windows 10. Se guarda la información en bases de datos con nombres “AG\*.db” que también están en la carpeta “%WINDIR%\prefetch”. Este servicio está diseñado para anticipar cuales son las aplicaciones que se ejecutan frecuentemente tras una actividad de hibernación, reposo, cuales son las aplicaciones que cambio de usuario, etc. e el sistema detecte que se encuentra instalado en un SSD el Superfetch desactiva el En caso de que el sistema detecte Ready Boot», «ReadyBoost» y a sí mismo.

The screenshot shows the 'SuperFetch Tree' application window. At the top, there are two tabs: 'Discover and Parse DB Files' (which is selected) and 'Include File Record Detail Dump'. Below the tabs, a section titled 'SuperFetch Discovered Database Files' displays a table of 8 database files:

Name	Comp	Magic	Type	#Files
1 C:\Windows\Prefetch\AgAppLaunch.db	Unk=5			
2 C:\Windows\Prefetch\AgCx_SC4.db	Xpress	0xE	0xB	1330
3 C:\Windows\Prefetch\AgGIFaultHistory.db	Xpress	0xE	0x1	3706
4 C:\Windows\Prefetch\AgGIFgAppHistory.db	Xpress	0xE	0x1	7463
5 C:\Windows\Prefetch\AgGlobalHistory.db	Xpress	0xE	0x1	10130
6 C:\Windows\Prefetch\AgGLUAD_P_S-1-5-21-4251235867-3156790139-409...	Xpress	0xE	0xB	3072
7 C:\Windows\Prefetch\AgGLUAD_S-1-5-21-4251235867-3156790139-409...	Xpress	0xE	0x1	8192
8 C:\Windows\Prefetch\AgRobust.db	None	0xE	0xE	339

Below this, another section titled 'File structure from databases with mapping keys to SuperFetch Database Files' shows a tree view of hard disk volumes and their contents, with mapping keys (1-8) indicated by colored numbers (green, blue, yellow, red) next to the file paths.

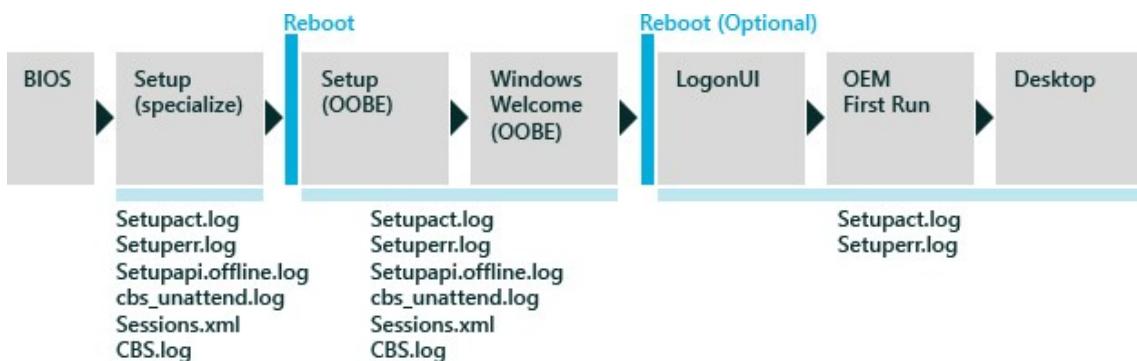
# CAPÍTULO 3

## Los Logs

Un log es un registro de eventos durante un rango de tiempo en particular. Se utiliza para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o para una aplicación concreta.

Para un perito, un log es una evidencia digital valiosísima, la mayoría de los Logs son almacenados en un formato estándar, el cual es un conjunto de caracteres para dispositivos comunes y aplicaciones. Los de los logs que se pueden encontrar en la carpeta del sistema.

En la siguiente imagen, proporcionada por Microsoft en su página oficial se pueden ver los distintos ficheros de log creados durante la sesión de Windows PE:



Se muestra a continuación un listado de los logs más importantes del sistema:

Tabla 1: LOGs del sistema

RUTA	CARACTERÍSTICA
%WINDIR%\setupact.log	Contiene información acerca de las acciones de instalación durante la misma. EVIDENCIAS: Podemos ver fechas de instalación, propiedades de programas instalados, rutas de acceso, copias legales, discos de instalación...
%WINDIR%\setuperr.log	Contiene información acerca de los errores de instalación durante la misma. EVIDENCIAS: Fallos de programas, rutas de red inaccesibles, rutas a volcados de memoria...
%WINDIR%\WindowsUpdate.log	Registra toda la información de transacción sobre la actualización del sistema y aplicaciones. EVIDENCIAS: Tipos de hotfix instalados, fechas de instalación, elementos por actualizar...
%WINDIR%\Debug\mrt.log	Resultados del programa de eliminación de software malintencionado de Windows. EVIDENCIAS: Fechas, Versión del motor, firmas y resumen de actividad.
%WINDIR%\security\logs\	
scecomp.old	Componentes de Windows que no han podido ser instalados. EVIDENCIAS: DLL's no registradas, fechas, intentos de escritura,rutas de acceso...
%WINDIR%\SoftwareDistribution\	

continué en la próxima página

Tabla 1 – proviene de la página anterior

RUTA	CARACTERÍSTICA
ReportingEvents.log	Contiene eventos relacionados con la actualización. EVIDENCIAS: Agentes de instalación, descargas incompletas o finalizadas, fechas, tipos de paquetes, rutas...
%WINDIR%\Logs\CMS\CMS.log	Ficheros pertenecientes a “Windows Resource Protection” y que no se han podido restaurar. EVIDENCIAS: Proveedor de almacenamiento, PID de procesos, fechas, rutas...
%AppData%\Local\Microsoft\	
Websetup (Windows 8)	Contiene detalles de la fase de instalación web de Windows 8 EVIDENCIAS: URLs de acceso, fases de instalación, fechas de creación, paquetes de programas...
%AppData%\setupapi.log	Contiene información de unidades, services pack y hotfixes. EVIDENCIAS: Unidades locales y extraibles, programas de instalación, programas instalados, actualizaciones de seguridad, reconocimiento de dispositivos conectados...
%SYSTEMROOT%\Windows.BT\Sources\Panther\log.xml %WINDIR%\PANTHER\log.xml	Contiene información de acciones, errores y estructuras de SID cuando se actualiza desde una versión anterior de windows. EVIDENCIAS: Fechas, rutas, errores, medio de instalación, dispositivos, versiones, reinicio, dispositivos PnP...

continué en la próxima página

Tabla 1 – proviene de la página anterior

RUTA	CARACTERÍSTICA
%WINDIR%\INF\setupapi.dev.log	Contiene información de unidades Plug and Play y la instalación de drivers. EVIDENCIAS: Versión de SO, Kernel, Service Pack, arquitectura, modo de inicio, fechas, rutas, lista de drivers, dispositivos conectados, dispositivos iniciados o parados...
%WINDIR%\INF\setupapi.app.log	Contiene información del registro de instalación de las aplicaciones. EVIDENCIAS: Fechas, rutas, sistema operativo, versiones, ficheros, firma digital, dispositivos...
%WINDIR%\Performance\	
Winsat\	
winsat.log	Contiene trazas de utilización de la aplicación WINSAT que miden el rendimiento del sistema. EVIDENCIA: Fechas, valores sobre la tarjeta gráfica, CPU, velocidades, puertos USB...
*.INI	Contiene configuraciones de programas EVIDENCIA: Rutas, secciones, parámetros de usuarios...
%WINDIR%\Memory.dmp	Contiene información sobre los volcados de memoria. EVIDENCIA: Rutas, programas, accesos, direcciones de memoria, listado de usuarios, contraseñas, conexiones...

continué en la próxima página

Tabla 1 – proviene de la página anterior

RUTA	CARACTERÍSTICA
EL.CFG Pid.txt	Estos archivos se usan para automatizar la página de entrada de la clave de producto en el programa de instalación de Windows. EVIDENCIA: Contiene el código de producto y la versión instalada
%WINDIR%\System32\config %WINDIR%\ System32\winevt\Logs	Contiene los logs de Windows accesibles desde el visor de eventos. EVIDENCIAS: Casi todas. Entradas, fechas, accesos, permisos, programas, usuario, etc...
%PROGRAMDATA%\Microsoft\Microsoft Antimalware\Support %PROGRAMDATA%\Microsoft\Microsoft Security Client\Support	Logs del motor de anti-malware EVIDENCIAS: Fechas, versión del motor, programas analizados, actividad del malware...



# CAPÍTULO 4

## Ficheros de Hibernación

El fichero llamado hiberfil.sys, cuyo tamaño total es siempre equivalente a la cantidad de RAM de la máquina, guarda el estado de la máquina dentro del proceso de hibernación. La hibernación sería posible si todo el hardware de la máquina cumple con los requisitos ACPI y Plug-and-Play. Este fichero no es más que una imagen de la memoria de la máquina comprimida con un algoritmo que hace necesaria la utilización de herramientas específicas, por ejemplo, el WindowsMemory Toolkit de Moonsols (actualmente Comae). En este conjunto de herramientas se encuentra hibr2bin que es capaz de mostrar los datos.

```
Microsoft Windows [Version 10.0.17763.310]
(c) 2018 Microsoft Corporation. All rights reserved.

D:\Comae-Toolkit\3.0.20190124\x64\hbr2bin>
Hbr2Bin 3.0.20190124-x64\hbr2bin
Copyright (C) 2017, Matthieu Sulice <http://www.msuiche.net>
Copyright (C) 2012 - 2014, MoonSols Limited <http://www.moonsols.com>
Copyright (C) 2015 - 2017, Comae Technologies FZE <http://www.comae.io>
Copyright (C) 2017 - 2018, Comae Technologies DMCC <http://www.comae.io>

Usage: Hbr2Bin [Options] /INPUT <FILENAME> /OUTPUT <FILENAME>

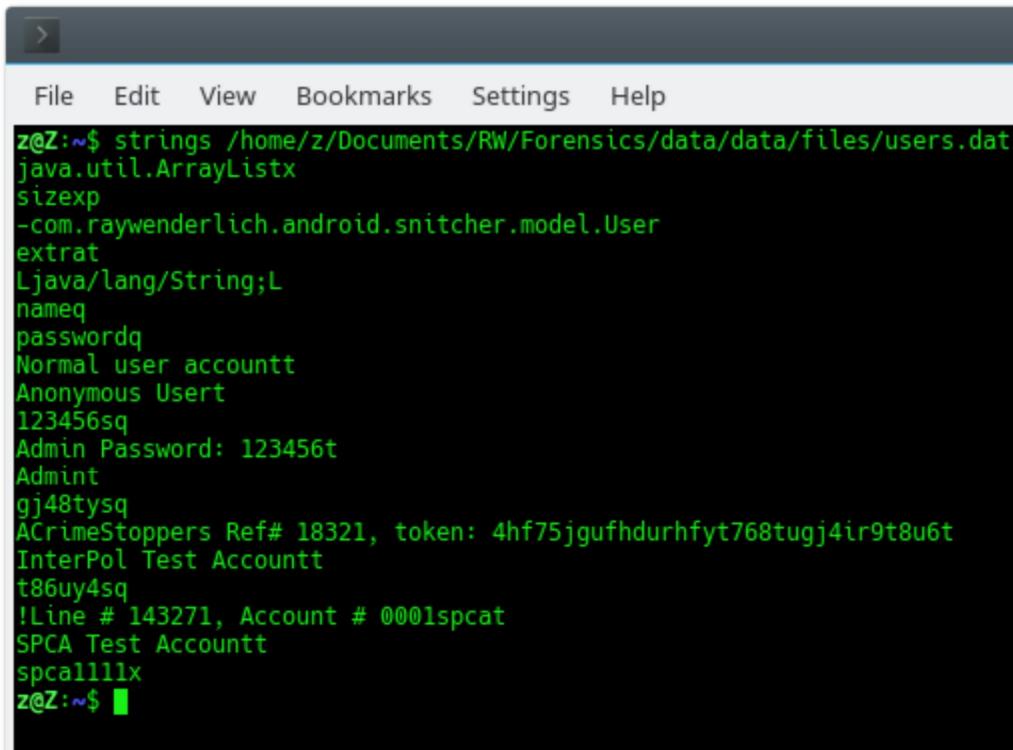
Description:
Enables users to uncompress Windows hibernation file.

Options:
/PPLATFORM /P           Select platform (X64 or X86)
/MINOR /V                Select major version (e.g. 6 for NT 6.1)
/MINOR /M                Select minor version (e.g. 1 for NT 6.1)
/OFFSET /L               Data offset in hexadecimal (optional)
/INPUT /I                Input hiberfil.sys file.
/OUTPUT /O               Output hiberfil.sys file.

Versions:
/MINOR 1                Windows XP
/MINOR 5 /MINOR 2        Windows XP x64, Windows 2003 R2
/MINOR 6 /MINOR 0        Windows Vista, Windows Server 2008
/MINOR 6 /MINOR 1        Windows 7, Windows Server 2008 R2
/MINOR 6 /MINOR 2        Windows 8, Windows Server 2012
/MINOR 6 /MINOR 3        Windows 8.1, Windows Server 2012 R2
/MINOR 10 /MINOR 0       Windows 10, Windows Server 2016

Examples:
Uncompress a Windows 7 (NT 6.1) x64 hibernation file:
Hbr2Bin /PLATFORM X64 /MAJOR 6 /MINOR 1 /INPUT hiberfil.sys /OUTPUT uncompressed.bin
```

También es posible convertir ficheros de hibernación a una imagen cruda empleando el framework Volatility. Posee un módulo que permite generar una imagen legible a partir del fichero de hibernación. Una vez obtenida una imagen lineal, es muy sencillo analizar los contenidos. Otra herramienta útil es Strings que permite buscar cadenas de texto en el contenido del fichero de hibernación, se puede utilizar para hacer una evaluación rápida de los contenidos del fichero, si tener que generar una imagen legible. Estos son algunos ejemplos de los contenidos de un fichero de hibernación: Algunos usuarios y servicios de red:



The screenshot shows a terminal window with a dark background and light-colored text. At the top, there's a menu bar with options: File, Edit, View, Bookmarks, Settings, and Help. Below the menu, the terminal prompt is "z@Z:~\$". The user has run the command "strings /home/z/Documents/RW/Forensics/data/data/files/users.dat". The output of this command is displayed in green text. It includes several Java class names and methods, such as "java.util.ArrayList", "sizeexp", and "com.raywenderlich.android.snitcher.model.User". There are also several password entries, including "123456sq", "Admin Password: 123456t", and "gj48tysq". Other lines include "ACrimeStoppers Ref# 18321, token: 4hf75jgufhdurhfyt768tugj4ir9t8u6t", "InterPol Test Accountt", "t86uy4sq", "!Line # 143271, Account # 0001spcat", "SPCA Test Accountt", and "spcall11x". The terminal ends with the prompt "z@Z:~\$".

# CAPÍTULO 5

---

## Volume Shadow Copy

---

El Shadow Copy también se denomina Volume Snapshot Service, Volume Shadow Copy Service o VSS, es una tecnología incluida en Microsoft Windows que permite hacer backups automáticamente o manualmente de ficheros o volúmenes, incluso cuando estos están en uso. El VSS opera a nivel del sistema de archivos.

Funciona como un servicio de Windows llamado “Volume Shadow Copy service». El software VSS se incluye como parte del sistema operativo para ser utilizado por las aplicaciones de Windows. Esta tecnología necesita que el sistema de archivos sea NTFS para poder crear y almacenar las copias que pueden ser creadas en local y en dispositivos externos, bien en dispositivos en red o dispositivos locales.

Las instantáneas tienen dos propósitos principales: permiten la creación de copias de seguridad consistentes de un volumen, lo que garantiza que los contenidos no pueden cambiar mientras se realiza la copia de seguridad y evitan problemas con el bloqueo de archivos. Al crear una copia de sólo lectura del volumen, los programas de copia de seguridad son capaces de acceder a todos los archivos sin interferir con otros programas de escritura a los mismos archivos.

El proceso de copia de datos puede ser gestionado por el sistema de archivos o por hardware especializado; en este último caso un proveedor de hardware VSS provee abstracción a la funcionalidad del sistema operativo. Las aplicaciones pueden proporcionar apoyo específico a través de los gestores VSS que controlan cómo los datos se establecen en un estado coherente al comienzo de una operación de VSS y mantienen la consistencia durante todo el proceso, entre otras funciones.

A través de la integración entre el Volume Shadow Copy Service, proveedores de hardware o software VSS, gestores de nivel de aplicación y las aplicaciones de copia de seguridad, VSS permite backups totales que son snapshots coherentes sin la herramienta de copia de seguridad propia.

En ocasiones es útil recurrir al VSS ya que en sistemas con Windows Server o Hyper-V, por ejemplo, este servicio crea una copia de seguridad completa a modo de snapshot, lo cual permite analizar el/los huéspedes en un estado anterior que puede ser útil a la hora

de determinar un suceso independiente de las aplicaciones.

El resultado final es similar a un sistema de archivos con control de versiones, permitiendo cualquier archivo se pueda recuperar tal como existía en el momento de alguno de los snapshots

# CAPÍTULO 6

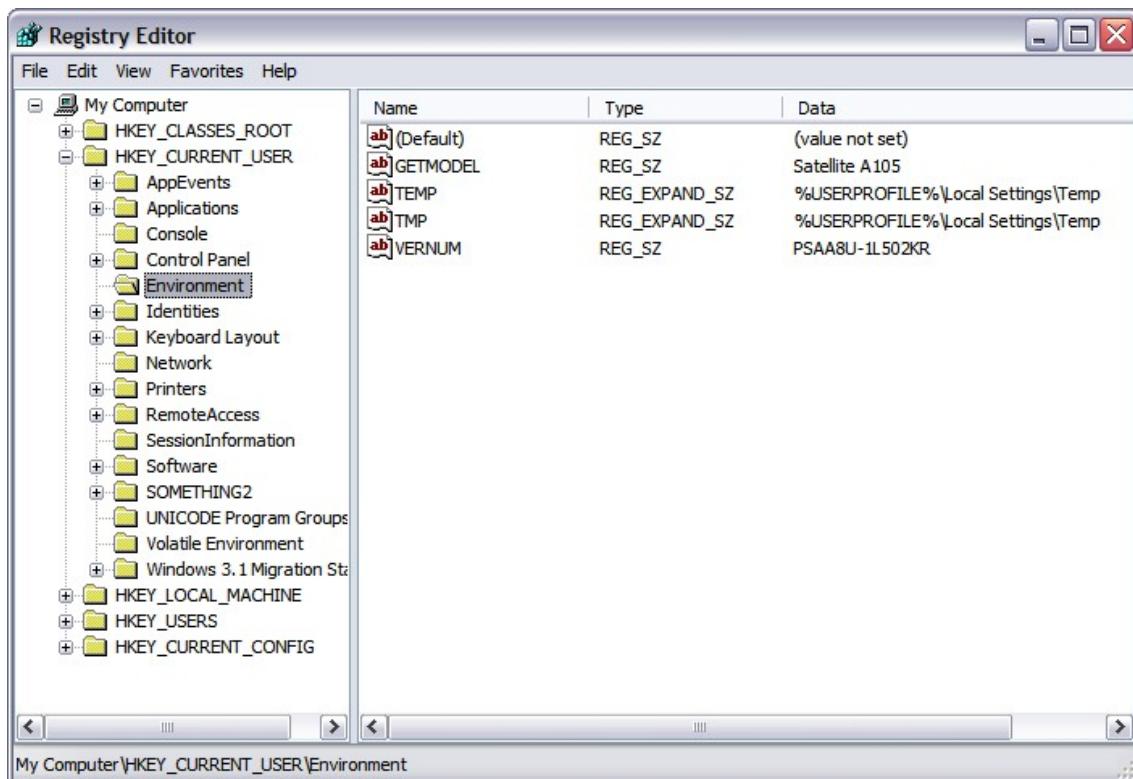
---

## Registro del Sistema

---

El registro de Windows es una base de datos jerárquica que almacena los ajustes de configuración y opciones en los sistemas operativos Microsoft Windows. Contiene la configuración de la componentes de bajo nivel del sistema operativo, así como de las aplicaciones que hay funcionan en la plataforma. Hacen uso del registro: el kernel, los drivers, los servicios, la SAM (administrador de cuentas de seguridad), la GUI y las aplicaciones de terceros. El registro también proporciona acceso a los controladores para generar un perfil del rendimiento del sistema.

En las primeras versiones de Windows, el registro almacena información sobre configuración de algunos componentes. Posteriormente, a partir de la versión 95 y NT, el registro era de ayum para poder ordenar toda la cantidad de ficheros INI que utilizaba cada programa. Estos ficheros se utilizaban para almacenar los ajustes de configuración.



Cuando se trata con aplicaciones portables, los datos de configuración están ubicados en el directorio donde se ejecuta la aplicación.

Es decir, si buscamos información sobre configuraciones, programas ejecutados en el arranque propiedades de los usuarios debemos acudir al registro.

## 6.1 Cómo se guardan los datos

El registro mantiene dos elementos básicos: claves y valores. Se pueden considerar las claves registro como contenedores similares a carpetas: además de los valores, cada clave puede contener subclaves, que a su vez pueden contener más subclaves, y así sucesivamente. Las claves se referencian con una sintaxis parecida a los nombres de las rutas de Windows

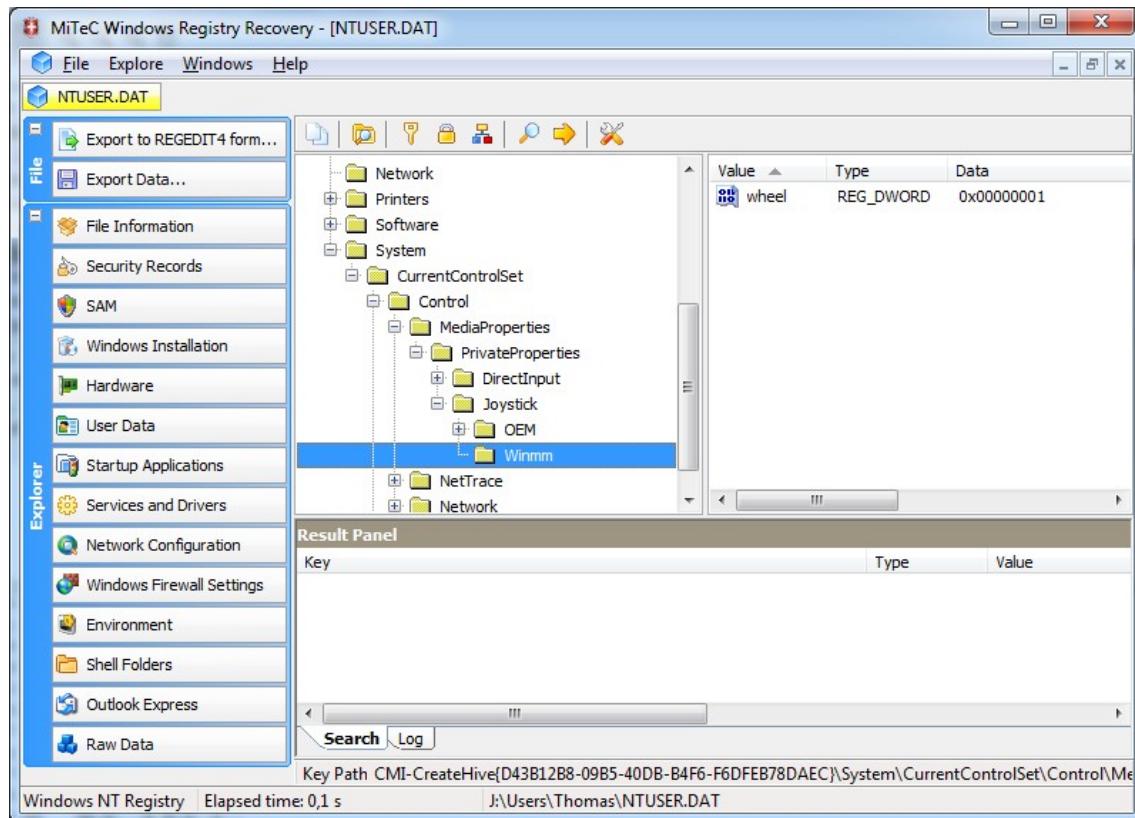
Ejemplo: HKEY\_LOCAL\_MACHINE\Software\Microsoft Windows se refiere a la subclave «Windows» de la subclave «Microsoft» de la subclave «Software» de la clave raíz HKEY\_LOCAL\_MACHINE. Por tanto, tenemos una estructura en árbol con subárboles en las que tendremos una entrada final que nos lleva a un valor.

Microsoft, proporciona una herramienta de forma nativa en sus sistemas operativos para visualizar y modificar estos datos, el «Regedit» (C:\Windows\regedit.exe)

### 6.1.1 Editor del registro

Existen otras herramientas como el «Windows Registry Recovery (WRR) de MiTeC (<http://www.mitec.cz/wrr.html>)

Windows Registry Recovery con la hive system:



## 6.2 Los subárboles

Hay siete claves raíces predefinidas, las cuales tradicionalmente se nombran según su identificador constante definido en la API de Win32, por sus abreviaturas correspondientes (dependiendo de las aplicaciones).

1. HKEY CLASSES ROOT, abreviado como HKCR, contiene información sobre aplicaciones registradas, como asociaciones de archivos e Id. de clase de objetos OLE, ligándolos a las aplicaciones utilizadas para identificar estos elementos.

En Windows 2000 y versiones superiores, HKCR es una compilación de HKCU Software Classes basada en el usuario y de HKLM\Software\Classes basada en el equipo. Si un valor dado existe en las dos subclaves anteriores, la contenida en HKCU\Software Classes prevalece.

El diseño permite el registro de objetos COM específico del equipo o del usuario. El subárbol de clases específico del usuario, a diferencia del subárbol HKCU, no forma parte del perfil de usuario móvil.

2. HKEY\_CURRENT\_USER (HKCU), abreviado como HKCU, almacena configuraciones específicas del usuario con sesión iniciada, La clave HKEY CURRENT

USER es un enlace a la subclave de HKEY\_USERS correspondiente al usuario; se puede acceder a la misma información en ambas ubicaciones

En los sistemas NT de Windows la configuración de cada usuario se almacena en sus propios archivos llamados NTUSER.DAT y USRCLASS.DAT dentro de su carpeta de usuario «\users\%USER%» en Documents and Settings %USER% en Windows XP. Las configuraciones contenidas en este subárbol siguen de equipo en equipo a los usuarios con perfil móvil.

3. HKEY\_LOCAL\_MACHINE (HKLM), abreviado como HKLM, almacena configuración específica del equipo local. Las claves ubicadas como HKLM realmente no se almacena en el disco, sino que el núcleo del sistema la mantiene en la memoria para asignar allí las demás subclaves.
4. HKEY\_USERS (HKU), abreviado como HKU, contiene subclaves correspondientes a las claves HKEY\_CURRENT\_USER de cada perfil de usuario cargado activamente en el equipo, aunque normalmente sólo se cargan los subárboles de usuario correspondientes a los usuarios con sesión iniciada en esos momentos
5. HKEY\_CURRENT\_CONFIG, contiene información acerca del perfil de hardware que utiliza el equipo local cuando se inicia el sistema
6. HKEY\_PERFORMANCE\_DATA, esta clave proporciona información del tiempo de ejecución mediante datos de rendimiento proporcionados por el propio núcleo NT o por controladores del sistema, programas y servicios en funcionamiento que proporcionen datos de rendimiento.

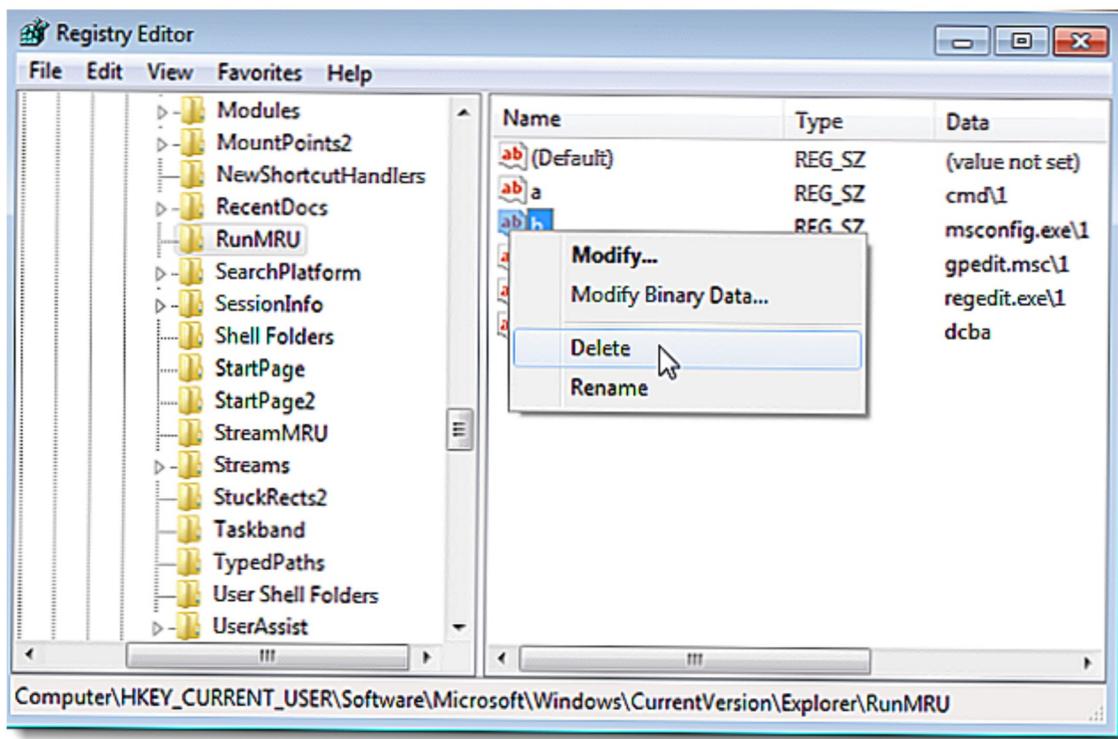
Esta clave no se almacena en ningún subárbol y no aparece en el Editor de registro, pero es visible a través de las funciones de registro en el API de Windows, en una vista simplificada a través de la pestaña Rendimiento del Administrador de tareas (únicamente para algunos datos de rendimiento del sistema local) o a través de paneles de control más avanzados (como el Monitor de rendimientos o el Analizador de rendimientos, los cuales permiten recoger y registrar esta información, incluyendo la de sistemas remotos).

7. HKEY\_DYN\_DATA, esta clave se usa sólo en Windows 95, Windows 98 y Windows Me. Contiene información sobre dispositivos de hardware, incluyendo estadísticas de rendimiento de Plug and Play y de red. La información contenida en este subárbol tampoco se almacena en el disco duro. La información sobre Plug and Play se recoge y configura en el inicio, y se almacena en la memoria,

### 6.3 Las Listas MRU

Las listas MRU contienen los datos más comunes «most recently used», son entradas creadas debido a acciones específicas del usuario. Hay varias listas MRU localizadas en varias claves de registro. El registro mantiene estas listas por si el usuario vuelve a determinados ítems en el futuro. Es similar a cómo el historial y las cookies actúan en un navegador. Un ejemplo es la clave «RunMRU». Cuando un usuario teclea un comando en la caja de ejecución a través del menú Inicio, esa entrada Explorer se encuentra en HKCU\Software\Microsoft\Windows\Current Version\RUNMRU:

El valor de la clave “MRUList» proporciona el orden en el que se deben leer los datos siendo la primera letra de la izquierda la acción más reciente, es útil si se desea comprobar las ejecuciones realizadas y su orden. En la imagen anterior se puede comprobar que el último comando ejecutado fue «notepad».



La clave UserAssist en la ruta HCU\Software\Microsoft\Windows\CurrentVersion Explorer UserAssist, contiene varias subclaves y proporciona un listado con la última fecha de ejecución y el conteo de ejecuciones de cada programa que se ha ejecutado en el sistema.

Otra clave interesante es la que refleja las redes wifi a las que se ha conectado el sistema con su SSID y se guarda en HKLM\SOFTWARE\ Microsoft\WZCSVC\Parameters\Interfaces key.

También es muy útil comprobar los dispositivos USB conectados en la clave HKLM\SYSTEM\ControlSet00x\Enum\USBSTOR donde se puede encontrar el device ID del dispositivo conectado. Los dispositivos montados también pueden darnos información interesante, la clave HKLM\SYSTEM\MountedDevices guarda una base de datos de los volúmenes montados con sistema de ficheros NTFS.



# CAPÍTULO 7

---

## Eventos EVTX

---

Como se ha mostrado, los registros de eventos son archivos especiales que registran los eventos importantes que tienen lugar en el equipo, como, por ejemplo, cuando un usuario inicia sesión en el equipo o cuando se produce un error en un programa. Siempre que se producen este tipo de eventos, Windows los va incluyendo en un registro que se puede leer mediante el Visor de eventos. Para los usuarios avanzados, la información de los registros de eventos puede ser útil para solucionar problemas con Windows y otros programas.

En el visor de eventos, la información se organiza en diversos registros. Estos incluyen:

- **Eventos de aplicaciones (programas).** Cada evento se clasifica como error, advertencia o información, dependiendo de su gravedad. Un error es un problema importante como una pérdida de datos. Una advertencia es un evento que no es importante necesariamente, pero puede indicar la posibilidad de problemas en el futuro. Un evento de información describe la operación correcta de un programa, un controlador o un servicio
- **Eventos relacionados con la seguridad.** Estos eventos se conocen como auditorías y se describen como correctos o con error, dependiendo del evento como, por ejemplo, si un usuario consigue iniciar una sesión en Windows correctamente.
- **Eventos de configuración.** Los equipos que se han configurado como controladores de dominio dispondrán de más registros aquí.
- **Eventos del sistema.** Los eventos del sistema los registran Windows y los servicios del sistema de Windows, y se pueden clasificar como error, advertencia o información.
- **Eventos reenviados.** Estos eventos se reenvían a este registro desde otros equipos

Los registros de aplicaciones y servicios pueden variar. Incluyen registros independientes para los programas que se ejecutan en el equipo, así como registros más detallados relacionados con servicios específicos de Windows

EVTX es un nuevo formato de registro de Microsoft ha implementado en Vista y Server 2008 o superiores. La principal razón para rehacer el formato de registro EVT anterior

es que ha habido muy pocas actualizaciones desde Windows NT 4.0 para dar cabida al creciente nivel de complejidad que se requiere en la actualidad. EVTX incluye nuevas características y propiedades de evento, el uso de canales para publicar eventos, un formato Extensible Markup Language (XML), un nuevo Visor de eventos y Servicio de registro de eventos.

## 7.1 Definición de eventos EVTX

EVTX incluye nuevas propiedades que componen cada evento que es publicado. Una de las nuevas propiedades introducidas en EVT es el campo «Keyword». Este almacena valores que en el formato EVT se almacenaban en «Type». En el formato EVT, el campo «Type» almacena la gravedad y las palabras clave para cada evento. En EVT, el campo «Level» se utiliza para almacenar la severidad del evento en lugar de «Type». Aunque no es una nueva propiedad, muchos valores de «Event ID» cambiaron significativamente en EVT. El suceso es un identificador único que se asigna para cada tipo de evento y es la forma más común para hacer referencia a un evento único, EVTEventId = EVTEventId 4096. La siguiente tabla es una lista de la mayoría de las propiedades de evento comunes:

### Ver también:

[https://www.sans.org/reading-room/whitepapers/logging/  
evt-windows-event-logging-32949](https://www.sans.org/reading-room/whitepapers/logging/evt-windows-event-logging-32949)

Uno de los cambios más notables en la aplicación EVT es el uso de canales para almacenar los eventos. El Kit de Desarrollo de Software del registro de eventos de Windows define canales como corrientes de eventos que son utilizados por el sistema operativo y aplicaciones para publicar eventos a un registro. Los principales canales que están incluidos en versiones superiores a Vista y Server 2008 se dividen en dos grupos:

El primer grupo se llama Registros de Windows y esto incluye la Aplicación, Seguridad y canales del sistema. También incluye dos nuevos canales que reciben el nombre de Setup y ForwardedEvents. Windows y de Log Pars adopción de coinciden p El segundo grupo se llama Application y Services Logs. Este grupo contiene muchos canales que publican eventos desde una sola aplicación o componente. La configuración de la suscripción se guarda en una clave del registro “HKEY LOCAL MACHINE\SOFTWARE\Microsoft\Windows\Current Version\EventCollector\Subscriptions». Los ajustes en la clave de registro se pueden ver mediante “wecutil gs» y modificar mediante «wecutil ss» con los parámetros adecuados. La siguiente figura muestra la salida de «gs wecutil» para una suscripción Microsoft consulta a Registr el o como así llamada Test.

```
C:\Users\Administrator>
C:\Users\Administrator>wecutil gs Test
Subscription Id: Test
SubscriptionType: CollectorInitiated
Description:
Enabled: true
Uri: http://schemas.microsoft.com/wbem/wsman/1/windows/EventLog
ConfigurationMode: MinLatency
DeliveryMode: Push
DeliveryMaxLatencyTime: 30000
HeartbeatInterval: 3600000
Query: <QueryList><Query Id="0"><Select Path="Application">*[System[<Level=1 or
Level=2 or Level=3 or Level=4 or Level=0 or Level=5]]</Select><Select Path="Se
curity">*[System[<Level=1 or Level=2 or Level=3 or Level=4 or Level=0 or Level=
5]]</Select><Select Path="System">*[System[<Level=1 or Level=2 or Level=3 or L
evel=4 or Level=0 or Level=5]]</Select></Query></QueryList>
ReadExistingEvents: false
TransportName: HTTP
ContentFormat: RenderedText
Locale: en-US
LogFile: ForwardedEvents
PublisherName: microsoft-windows-eventcollector
CredentialsType: Default
CommonUserName: GCIA\administrator
CommonUserPassword: *
EventSource[0]:
    Address: server1.gcia.gold
    Enabled: true
C:\Users\Administrator>
```

El comando «wecutil» contiene muchas opciones de configuración que no se muestran en el asistente de suscripción. Una de ellas permite el ajuste de los intervalos de latencia, cuando el valor de “Configuration Mode» se establece en Personalizado. El “wecutil» tiene muchas opciones adicionales que se pueden usar para configurar y solucionar problemas de una suscripción. La mejor documentación sobre la utilidad se puede encontrar utilizando la ayuda que se muestra mediante la ejecución de “wecutil /?” en la línea de comandos.



# CAPÍTULO 8

---

## Herramientas

---

### 8.1 Log Parser

LogParser es una utilidad de CLI que fue inicialmente escrita por Gabriele Giuseppini, para automatizar tests para el Log de IIS. Estaba diseñado para usarlo con los sistemas operativos Windows y fue incluido con el IIS 6.0 Resource Kit Tools. El comportamiento predeterminado de Log Parser, es que trabaja como una “canalización de procesamiento de datos», mediante la adopción de una expresión de SQL en la línea de comandos, y mostrando las líneas contenidas que coinciden para la expresión SQL.

Microsoft define LogParser como una herramienta eficaz y versátil que ofrece acceso universal de consulta a datos basados en texto tales como archivos de registro, archivos XML y archivos CSV, así como orígenes de datos clave en el sistema operativo Windows tal como el Registro de eventos, el Registro, el sistema de archivos y Active Directory. Se le dice a Log Parser qué información se necesita y cómo se desea procesarla. El formato de los resultados de su consulta se puede personalizar en un resultado basado en texto o bien se pueden traspasar a destinos más especializados como SQL, SYSLOG o un gráfico.

Formatos de entrada admitidos:

- **XML:** lee archivos XML (requiere Microsoft XML Parser (MSXML))
- **TSV:** lee archivos de texto con valores separados por fichas y espacios
- **ADS:** lee información desde objetos de Active Directory
- **REG:** lee información desde el Registro de Windows
- **NETMON:** hace posible analizar archivos de captura NetMon .cap
- **ETW:** lee archivos de registro de Seguimiento de eventos para Windows y sesiones en - - directo



# CAPÍTULO 9

## LNK Shortcuts

Los accesos directos contienen la información para redireccionar a otro fichero. Es decir, contiene información de esa ubicación. Son editables mediante el explorador de Windows y es posible tener varios accesos o rutas hacia el mismo archivo (desde Windows Vista). Los accesos LNK son links a otros archivos ejecutables y contienen la información de la ruta a dicho archivo ocultando la extensión. Estos ficheros se pueden encontrar en la ruta «\ProgramData\Microsoft\Windows\Start\Menu\Programs».

En la figura siguiente se muestra un ejemplo, utilizando el programa LinkParser de 4Discovery y definiendo el acceso a la ruta descrita.

El formato se ha mantenido desde Windows 8.1 hasta Windows 10. Los campos más útiles son el Hostname, MAC Address, Volume ID, Owner SID, MAC Times. Se puede utilizar una herramienta como LinkParser v1.3.

Es importante destacar que las aplicaciones modernas no aparecen en esta carpeta, solo los accesos directos de las aplicaciones de escritorio y de la Windows Store.Ink y el Immersive Control Panel.Ink aparecen aquí.

FileModifiedDate	FileAccessDate	FileCreationDate	FileLinkFileName	FileLinkFilePath	FileMD5	LinkModifiedDate
8/14/2017 8:06 AM	11/7/2017 8:40 AM	11/7/2017 8:40 AM	foobar2000.lnk	C:\Users\elena\Desktop\	A99752CD482572E6...	7/10/2017 5:24 AM
10/31/2017 6:04 AM	11/7/2017 8:40 AM	11/7/2017 8:40 AM	GameMaker Studio 2.l...	C:\Users\elena\Desktop\	9FD6E5282E4DDE8F...	10/4/2017 8:35 AM
11/21/2016 8:15 AM	11/7/2017 8:40 AM	11/7/2017 8:40 AM	ILSpy.lnk	C:\Users\elena\Desktop\	A2B91C2EA9FB964C...	11/21/2016 7:54 AM
2/21/2017 10:53 AM	11/7/2017 8:41 AM	11/7/2017 8:41 AM	Minecraft.lnk	C:\Users\elena\Desktop\	99BC36384E5DFEA3...	1/22/2015 12:36 AM
2/22/2017 9:41 AM	11/7/2017 8:41 AM	11/7/2017 8:41 AM	Mozilla Firefox.lnk	C:\Users\elena\Desktop\	59AF977D8377B944C...	1/25/2017 7:13 PM
3/16/2017 7:04 AM	11/7/2017 8:41 AM	11/7/2017 8:41 AM	Oracle VM VirtualBox.l...	C:\Users\elena\Desktop\	A2BD38A402098E45...	3/15/2017 2:17 PM
7/14/2017 10:32 AM	11/7/2017 8:41 AM	11/7/2017 8:41 AM	Stronghold Kingdoms.l...	C:\Users\elena\Desktop\	C24E27C8584A39F41...	7/4/2013 12:30 PM
11/18/2016 1:19 PM	11/7/2017 8:41 AM	11/7/2017 8:41 AM	Thunderbird.lnk	C:\Users\elena\Desktop\	326DAD7BCF45208A...	10/4/2016 5:58 PM
7/24/2017 4:13 AM	11/7/2017 8:40 AM	11/7/2017 8:40 AM	watcher.lnk	C:\Users\elena\Desktop\	D5BC0A8751B73A49...	8/25/2014 4:45 PM



# CAPÍTULO 10

---

## Otras evidencias

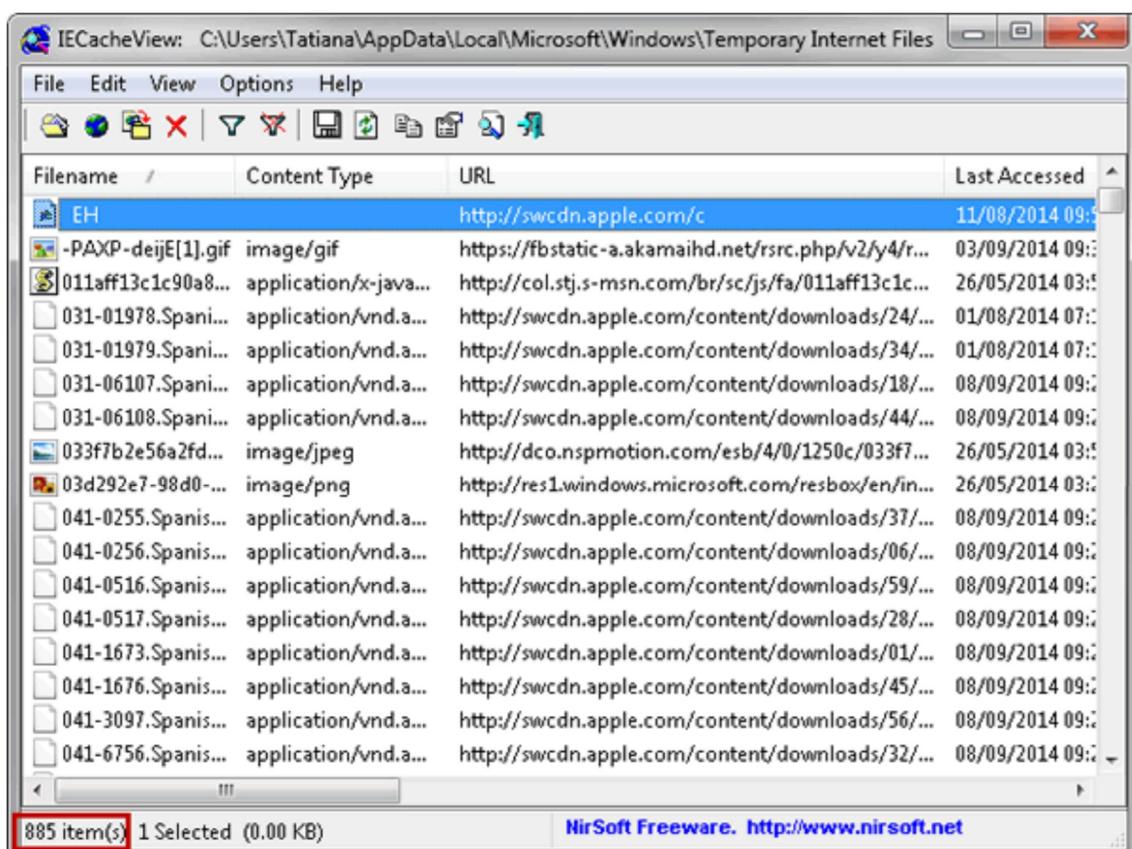
---

### *10.1 Navegación*

Dentro de los navegadores se pueden obtener evidencias importantes como, por ejemplo, el de navegación aporta datos acerca de las páginas web visitadas.

Herramientas muy útiles para poder obtener la información de los navegadores, todas desarrolladas por NirSoft:

- **BrowsingHistoryView:** Herramienta que permite leer datos de historial de cuatro navegadores (Internet Explorer, Mozilla Firefox, Google Chrome y Safari) y que devuelve como resultado una tabla organizada con la URL Visitada, Título, Tiempo de Visita, Contador de Visitas, navegador Web y perfiles de usuario.
- **ChromeCacheView:** Herramienta que permite leer la carpeta de cache de Google Chrome navegador Web y muestra una lista de los archivos almacenados en la memoria cache.
- **IECacheView:** Herramienta que lee la carpeta de cache de Internet Explorer navegador Web y muestra una lista de los archivos almacenados en la memoria cache. La siguiente imagen es un ejemplo de parte de los datos que se pueden ver:



- **MozillaCacheView:** permite leer la carpeta de caché de los navegadores web Firefox / Mozilla /Netscape, y muestra la lista de todos los archivos almacenados en la memoria caché.
- **MyLastSearch:** esta herramienta examina los archivos de caché y el historial de su navegador de Internet, y localizar todas las consultas de búsqueda que se han realizado con los motores de búsqueda más populares y con los sitios de redes sociales habituales como son Twitter o Facebook.
- **MozillaCookiesView:** permite tener una alternativa a la norma Cookie Manager proporcionada por Netscape y Mozilla.
- **OperaCacheView:** esta herramienta permite leer la carpeta de caché de Opera, y muestra la lista de todos los archivos almacenados en la memoria caché.

## 10.2 Papelera de reciclaje

La empresa Microsoft fue quien introdujo la papelera de reciclaje y le dio su mala fama de archivador.

Sirve para controlar la eliminación de los archivos de los discos duros y poder trabajar con las opciones que nos sirven de reciclaje desde Windows 95 en adelante con la intención de mantener los archivos que habían sido borrados, ya sea de forma accidental o intencional, dando la posibilidad a los usuarios de este sistema de revisar su contenido antes de eliminarlo definitivamente; función que en versiones anteriores de Windows y MS-DOS hacia el comando «undelete» siendo esta la única manera de recuperar los archivos bo-

rrados accidentalmente. Además de guardar los archivos en sí, una papelera de reciclaje almacena información de la fecha, hora y la ubicación donde estaban originalmente.

Antes de Windows Vista, la papelera de reciclaje almacena de manera predeterminada un 10 % del volumen total del disco. Por ejemplo, en un disco duro con 20 GB, la papelera de reciclaje almacenará hasta 2 GB. Si esta llega al máximo de su capacidad, entonces los archivos con mayor antigüedad serán eliminados definitivamente sin ser previamente almacenado en esta. En versiones de Windows anteriores a Vista, la papelera de reciclaje tiene una extensión máxima de 3.99 GB, mientras que, en la última versión del sistema operativo, el máximo es el 10 % de la capacidad de la partición del disco, o bien de 4 GB más el 5 % de la capacidad de la partición de disco, en caso de ser este inferior a 40 GB

El directorio real donde se almacenan los archivos que están en la Papelera de reciclaje varía de acuerdo al Sistema operativo o al sistema de archivos que tenga la partición. Así, en el sistema de archivos FAT (usado típicamente en sistemas Windows 9x), el directorio se ubica en X RECYLED (siendo X una letra de la unidad cualquiera), mientras que en el sistema de archivos NTFS y en Windows NT/2000/XP esta se encuentra en X:\$RECYCLER (siendo X una letra de la unidad cualquiera), con excepción de Windows Vista y Windows 7, en los cuales se guardan los archivos en el directorio X:\$Recycle Bin.

Cuando se accede a la Papelera de reciclaje a través del Escritorio, esta muestra diferentes opciones e información que, accediendo con el Explorador de Windows al directorio real no son mostradas; además, si los archivos están guardados en un volumen con el sistema de archivos NTFS, un usuario no puede eliminar archivos en la Papelera de reciclaje de otro, esto porque dentro del directorio X:\$RECYLED o X:\$Recycle.Bin existe un subdirectorío propio para cada usuario del equipo. Cabe mencionar que este directorio presenta atributos de «oculto» y de «sistema», ya que esta carpeta es indispensable para el buen funcionamiento del sistema operativo.

En resumen, la carpeta de la papelera está oculta por defecto, hay una carpeta por usuario y solo ese mismo usuario puede acceder a ella (en un sistema encendido). Cuando se accede a la máquina apagada o a una imagen de la misma, se puede acceder a todas las carpetas de los usuarios. Como cuando se elimina un archivo, no se elimina realmente del disco duro, simplemente se marca su espacio asignado como libre en la MFT pero la información sigue existiendo, hasta que el espacio de memoria no se sobrescribe, es posible recuperar el contenido del fichero.

### *10.3 Los metadatos*

Los documentos suelen almacenar información adicional en el propio fichero que puede contener el usuario que lo ha creado, su fecha de creación, la fecha de modificación, y el software que fue utilizado.

Existen muchas herramientas para poder ver estos metadatos. En Windows podemos utilizar la Foca Free, para Linux o Windows existe Exiftool. Los frameworks de los que ya hemos hablado como OSForensics o FTK Imager nos permiten también ver esta información.

## *10.4 Datos de red*

En este caso se trata de los datos contenidos en los logs de IDS/IPS, logs de firewall, logs de VPN radius, Logs de servidor DHCP y logs de otras aplicaciones que puedan estar relacionadas (ftp, www, bbdd).

En algunos casos es necesario recoger durante unos días la actividad de la red a peritar para detectar posible actividad ilícita.

Para registrar el tráfico desde hacia el sistema analizado se puede utilizar un sniffer, si esto no es posible, hacer un “mirror del puerto del switch, o como última opción, utilizar un hub o usar ip-spoofing para redirigir el tráfico hacia el sniffer (ethereal).

# CAPÍTULO 11

---

## Conclusiones

---

Las caches de los navegadores arrojan mucha luz sobre el comportamiento de un usuario en internet. En alguna ocasión pude apoyar este estudio con los logs de un Squid Proxy que recogía todas las peticiones por IP de los trabajadores de una empresa. Esto hizo que, al recoger los datos de navegación de un trabajador de la misma, el volumen de datos fue tal que el fichero Excel donde exporte esa información tardaba muchísimo tiempo en poder abrirse. En este caso el procesamiento de los datos lo represente con gráficas hechas en Matlab para que fuese fácilmente entendible el informe pericial.