



Artefactos de sistemas Windows

Índice

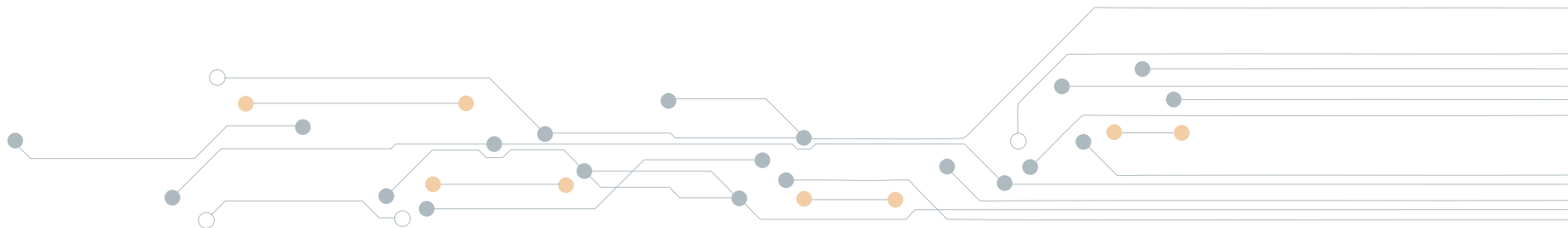


1 Introducción	3
2 Clasificación de los artefactos	4
3 Principales artefactos en el sistema operativo Windows	14

1. Introducción

Una vez se han realizado las copias de las evidencias del sistema objeto del estudio es necesario analizar los datos. Hay que tener presente que los datos importantes que ayudarán a resolver el análisis puede que estén aun en el sistema, puede que hayan sufrido un intento de eliminación o directamente que sólo queden rastros que indiquen la existencia de una acción. Hay que, por ello, intentar recuperar el máximo de información posible empezando por lo más evidente. Lo que se ha intentado eliminar.

Los artefactos son todos los procesos o mecanismos que dejan rastro de la actividad de los usuarios, de las aplicaciones que se manejan, los accesos, las conexiones y servicios, si se ha navegado y por donde, que se ha descargado...



2. Clasificación de los artefactos

Podemos realizar una clasificación por:

Archivos Descargados:

- **Abrir/Guardar archivos recientemente utilizados (MRU):** En términos más simples, esta clave rastrea archivos que se han abierto o guardado en un cuadro de diálogo de shell de Windows. Ésta pasa a ser un gran conjunto de datos, no sólo incluye navegadores como Internet Explorer y Firefox, sino también la mayoría de las aplicaciones más utilizadas.

```
Win7 NTUSER.DAT\Software\Microsoft\Windows\
CurrentVersion\Explorer\ComDlg32\OpenSavePIDMRU
```

- **Adjuntos de Emails:** la industria de correo electrónico estima que el 80% de los datos de correo electrónico se almacenan mediante archivos adjuntos. Las normas de correo electrónico solo permiten texto. Los archivos adjuntos deben codificarse con el formato MIME / base64

```
Win7 %USERPROFILE%\AppData\Local\Microsoft\
```

- **Historial Skype:** el historial de Skype mantiene un registro de las sesiones de chat y los archivos transferidos de una máquina a otra. Esta opción está activada de forma predeterminada en las instalaciones de Skype

```
Win7 C:\Users\<username>\AppData\Roaming\
Skype\<skype-name>
```

- **Index.dat/Places.sqlite:** no está directamente relacionado con "Descarga de archivos". Detalles almacenados para cada cuenta de usuario local. Registra el número de veces visitadas (frecuencia).

```
Win7 %userprofile%\AppData\Local\Microsoft\Windows\
History\Low\History.IE5

Win7 %userprofile%\AppData\Roaming\Mozilla\Firefox\
Profiles\<random text>.default\places.sqlite
```

- **Downloads.sqlite:** Firefox tiene una aplicación integrada de gestión de descargas que mantiene un historial de cada archivo descargado por el usuario. Este artefacto del navegador puede proporcionar información excelente sobre qué sitios ha estado visitando un usuario y qué tipos de archivos han estado descargando de ellos.

```
Win7 %userprofile%\AppData\Roaming\Mozilla\Firefox\
Profiles\<random text>.default\downloads.sqlite
```

Ejecución de programas

- **UserAssist:** los programas basados en GUI lanzados desde el escritorio se rastrean en el lanzador en un sistema Windows.

```
NTUSER.DAT\Software\Microsoft\Windows\Currentversion\
Explorer\UserAssist\{GUID}\Count
```

- **Última visita MRU:** rastrea el ejecutable específico utilizado por una aplicación para abrir los archivos documentados en la clave OpenSaveMRU. Además, cada valor también rastrea la ubicación del directorio del último archivo al que accedió esa aplicación.

```
Win7 NTUSER.DAT\Software\Microsoft\Windows\
CurrentVersion\Explorer\ComDlg32\LastVisitedPidIMRU
```

- **Caché de compatibilidad de aplicaciones:** la base de datos de compatibilidad de aplicaciones de Windows es utilizada por Windows para identificar posibles problemas compatibles de aplicaciones con ejecutables, y rastrea el nombre de archivo de los archivos ejecutables, el tamaño del archivo, la última hora modificada.

```
Win7 SYSTEM\CurrentControlSet\Control\Session
Manager\AppCompatCache
```

- **Win7 Jump Lists:** la barra de tareas de Windows 7 (Jump List) está diseñada para permitir a los usuarios “saltar” o acceder a los elementos que utilizan con frecuencia o que han utilizado recientemente de forma rápida y sencilla. Esta funcionalidad no sólo puede ser archivos de medios recientes, sino también tareas recientes. Los datos almacenados en la carpeta AutomaticDestinations tendrán cada uno un archivo único AppID de la aplicación asociada.

```
Win7 C:\Users\<user>\AppData\Roaming\Microsoft\
Windows\Recent\ AutomaticDestinations
```

- **Prefetch:** aumenta el rendimiento de un sistema mediante la precarga de páginas de códigos de las aplicaciones más utilizadas. Cache Manager supervisa todos los archivos y directorios referenciados para cada aplicación o proceso y los asigna en un archivo .pf. Utilizado para saber que una aplicación fue ejecutada en un sistema. Limitado a 128 archivos en XP y Win7. Su estructura es (Exename) - (hash) .pf

```
Win7 C:\Windows\Prefetch
```

- **Services Events:** analizar registros de servicios sospechosos que se ejecutan en el momento de arranque. Revisión de los servicios iniciados o detenidos en el momento de un compromiso sospechoso.

```
Todos los sucesos hacen referencia al registro del sistema
```

Creación y Apertura de archivos

- **Abrir/Guardar archivos recientemente utilizados (MRU):** en términos más simples, esta clave rastrea archivos que se han abierto o guardado en un cuadro de diálogo de shell de Windows. Ésta pasa a ser un gran conjunto de datos, no sólo incluye navegadores como Internet Explorer y Firefox, sino también la mayoría de las aplicaciones más utilizadas.

```
Win7 NTUSER.DAT\Software\Microsoft\Windows\
CurrentVersion\Explorer\ComDlg32\OpenSavePIDMRU
```

- **Última visita MRU:** rastrea el ejecutable específico utilizado por una aplicación para abrir los archivos documentados en la clave OpenSaveMRU. Además, cada valor también rastrea la ubicación del directorio del último archivo al que accedió esa aplicación.

```
Win7 NTUSER.DAT\Software\Microsoft\Windows\
CurrentVersion\Explorer\ComDlg32\LastVisitedPidMRU
```

- **Archivos recientes:** clave de registro que rastreará los últimos archivos y carpetas abiertos y se utiliza para rellenar datos en menús “recientes” del menú Inicio.

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

- **Archivos recientes de Office:** los programas de MS Office rastrearán su propia lista de archivos recientes para facilitar al usuario recordar el último archivo que estaban editando.

```
NTUSER.DAT\Software\Microsoft\Office\VERSION
```

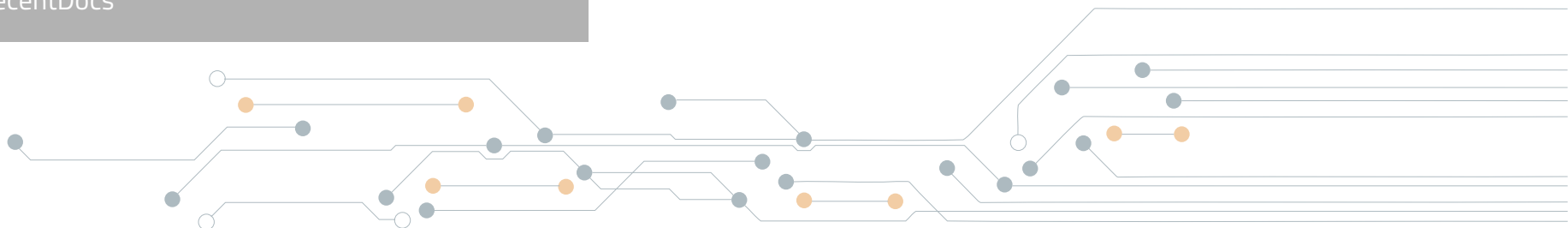
- **Shell Bags:** puede rastrear las preferencias de visualización de ventanas de usuario en el Explorador de Windows. Se puede utilizar para saber si la actividad se ha producido en una carpeta. En algunos casos, también puede ver los archivos de una carpeta específica

```
Win7 USRCLASS.DAT\Local Settings\Software\Microsoft\
Windows\Shell\Bags
```

```
Win7 USRCLASS.DAT\Local Settings\Software\Microsoft\
Windows\Shell\BagMRU
```

```
Win7 NTUSER.DAT\Software\Microsoft\Windows\Shell\
BagMRU
```

```
Win7 NTUSER.DAT\Software\Microsoft\Windows\Shell\
Bags
```



- **Archivos LNK:** archivos de acceso directo creados automáticamente por Windows. Archivos recientes. Abrir archivos de datos locales y remotos y documentos generará un archivo de acceso directo (.lnk)

```
Win7 C:\Users\<user>\AppData\Roaming\Microsoft\
Windows\Recent\
```

```
Win7 C:\Users\<user>\AppData\Roaming\Microsoft\
Office\Recent\
```

- **Win7 Jump Lists:** la barra de tareas de Windows 7 (Jump List) está diseñada para permitir a los usuarios "saltar" o acceder a los elementos que utilizan con frecuencia o que han utilizado recientemente de forma rápida y sencilla. Esta funcionalidad no sólo puede ser archivos de medios recientes, sino también tareas recientes. Los datos almacenados en la carpeta AutomaticDestinations tendrán cada uno un archivo único AppID de la aplicación asociada.

```
Win7 C:\Users\<user>\AppData\Roaming\Microsoft\
Windows\Recent\ AutomaticDestinations
```

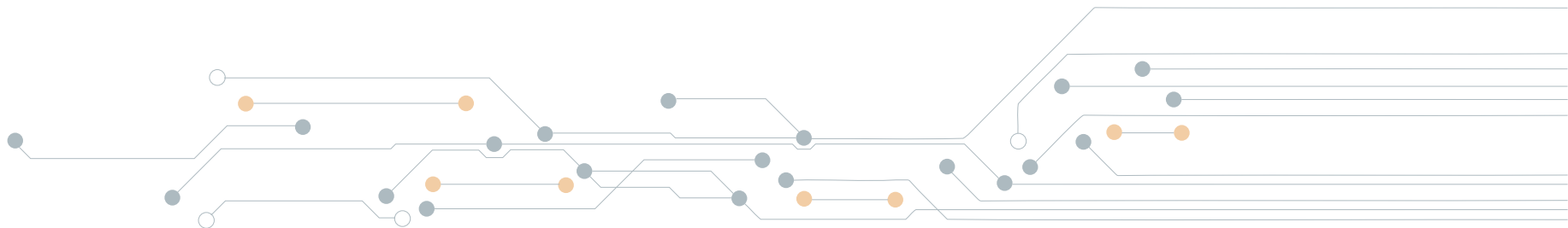
- **Prefetch:** aumenta el rendimiento de un sistema mediante la precarga de páginas de códigos de las aplicaciones más utilizadas. Cache Manager supervisa todos los archivos y directorios referenciados para cada aplicación o proceso y los asigna en un archivo .pf. Utilizado para saber que una aplicación fue ejecutada en un sistema. Limitado a 128 archivos en XP y Win7. Su estructura es (Exename) - (hash) .pf

```
Win7 C:\Windows\Prefetch
```

- **Index.dat (file://):** un hecho poco conocido sobre la historia de IE es que la información almacenada en los archivos de historial no se relaciona sólo con la navegación por Internet. El historial registra también el acceso a archivos locales y remotos (a través de particiones de red), lo que nos da un excelente medio para determinar qué archivos y aplicaciones se acceden al sistema día a día.

```
Win7 %userprofile%\AppData\Local\Microsoft\Windows\
History\History.IE5
```

```
Win7 %userprofile%\AppData\Local\Microsoft\Windows\
History\Low\History.IE5
```



Eliminación de archivos

- **Win7 Search –WordWheelQuery:** palabras clave buscadas desde la barra de menús de inicio en una máquina con Windows 7.

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

- **Última visita MRU:** rastrea el ejecutable específico utilizado por una aplicación para abrir los archivos documentados en la clave OpenSaveMRU. Además, cada valor también rastrea la ubicación del directorio del último archivo al que accedió esa aplicación.

```
Win7 NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidIMRU
```

- **Win7 Thumbnails:** en las versiones de Win7 de Windows, thumbs.db no existe. Los datos ahora se encuentran bajo un único directorio para cada usuario de la máquina que se encuentra en su directorio de datos de aplicación en su directorio personal.

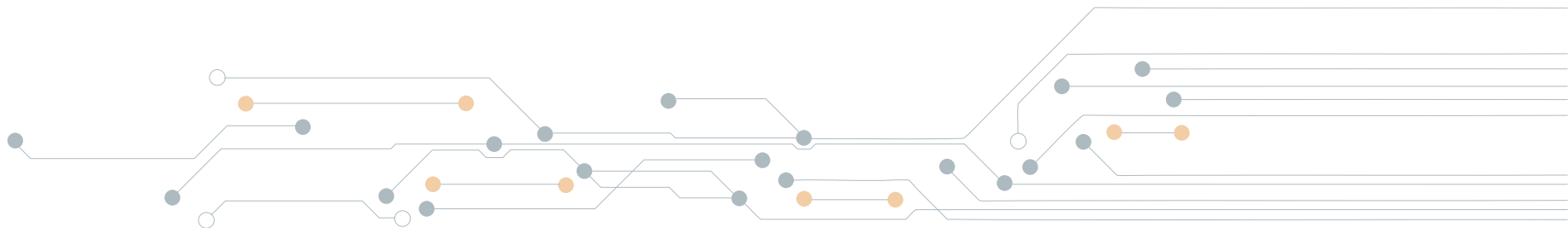
```
C:\Users\<username>\AppData\Local\Microsoft\Windows\Explorer\
```

- **Papelera de reciclaje Win7** la papelera de reciclaje es una ubicación muy importante en un sistema de archivos de Windows para entender. Puede ayudarle cuando realice una investigación forense ya que cada archivo que se elimina de un programa generalmente se coloca primeramente en la papelera de reciclaje.

```
C:\$Recycle.bin
```

- **Index.dat (file://):** un hecho poco conocido sobre la historia de IE es que la información almacenada en los archivos de historial no se relaciona sólo con la navegación por Internet. El historial registra también el acceso a archivos locales y remotos (a través de particiones de red), lo que nos da un excelente medio para determinar qué archivos y aplicaciones se acceden al sistema día a día.

```
INDEX.DAT - file:///C:/directory/filename.ext
```



Localización física

- **Timezone:** identifica la zona horaria actual del sistema.

```
SYSTEM\CurrentControlSet\Control\TimeZoneInformation
```

- **Historial de la red en Win7:** identificar las redes a las que se ha conectado el equipo. Las redes pueden ser inalámbricas o cableadas. Identificar nombre de dominio / nombre de intranet. Identificar SSID. Identificar la dirección MAC de la puerta de enlace.

```
SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged
```

```
SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed
```

```
SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Cache
```

- **Cookies:** las cookies ofrecen información sobre qué sitios web se han visitado y qué actividades pueden haber tenido lugar allí.

```
Win7 %userprofile%\AppData\Roaming\Microsoft\Windows\Cookies
```

```
Win7 %userprofile%\AppData\Roaming\Microsoft\Windows\Cookies\Low
```

- **Términos de búsqueda del navegador:** registra los sitios web visitados por fecha y hora. Detalles almacenados para cada cuenta de usuario local. Registra el número de veces visitadas (frecuencia). También controla el acceso de los archivos del sistema local. Esto también incluirá la historia del sitio web de términos de búsqueda en los motores de búsqueda.

```
Win7 %userprofile%\AppData\Local\Microsoft\Windows\History\History.IE5
```

```
Win7 %userprofile%\AppData\Local\Microsoft\Windows\History\Low\History.IE5
```

```
Win7 %userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\<random text>.default\places.sqlite
```



USB & Dispositivos

- **Identificación Clave:** rastrea dispositivos USB conectados a una máquina.

```
SYSTEM\CurrentControlSet\Enum\USBSTOR
SYSTEM\CurrentControlSet\Enum\USB
```

- **Primera/Última utilización:** determine el uso temporal de dispositivos USB específicos conectados a una máquina Windows.

```
Win7 C:\Windows\inf\setupapi.dev.log
```

- **Usuario:** buscar usuario que utilizó el dispositivo USB único

```
SYSTEM\MountedDevices
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\
Explorer\MountPoints2
```

- **Número de serie del volumen:** descubra el número de serie de volumen de la partición de sistema de archivos en el USB (NOTA: Este no es el número de serie único USB, que se crea cuando se inicializa un sistema de archivos).

```
SOFTWARE\Microsoft\Windows NT\CurrentVersion\
ENDMgmt
```

- **Letra de unidad y nombre de volumen:** descubra la letra de unidad del dispositivo USB cuando se conectó en la máquina.

```
SOFTWARE\Microsoft\Windows Portable Devices\Devices
SYSTEM\MountedDevices
```

- **Archivos LNK:** archivos de acceso directo creados automáticamente por Windows. Archivos recientes. Abrir archivos de datos locales y remotos y documentos generará un archivo de acceso directo (.lnk)

```
Win7 C:\Users\<user>\AppData\Roaming\Microsoft\
Windows\Recent\
Win7 C:\Users\<user>\AppData\Roaming\Microsoft\
Office\Recent\
```

- **Plug&Play Event Log:** cuando se intenta instalar un controlador Plug and Play, el servicio registrará un evento ID 20001 y proporcionará un estado dentro del evento. Es importante señalar que este evento se disparará para cualquier dispositivo compatible con Plug and Play, incluyendo, pero no limitado a dispositivos USB, Firewire y PCMCIA.

```
Win7 %system root%\System32\winevt\logs\System.evtx
```

Uso de Cuentas

- **Último login:** enumera las cuentas locales del sistema y sus identificadores de seguridad equivalentes.

```
C:\windows\system32\config\SAM  
SAM\Domains\Account\Users
```

- **Último cambio de la contraseña:** lista la última vez que se ha cambiado la contraseña de un usuario específico.

```
C:\windows\system32\config\SAM  
SAM\Domains\Account\Users
```

- **Inicios de sesión válidos o erróneos:** determine qué cuentas se han utilizado para intentos de inicio de sesión. Controle el uso de cuentas de cuentas comprometidas conocidas.

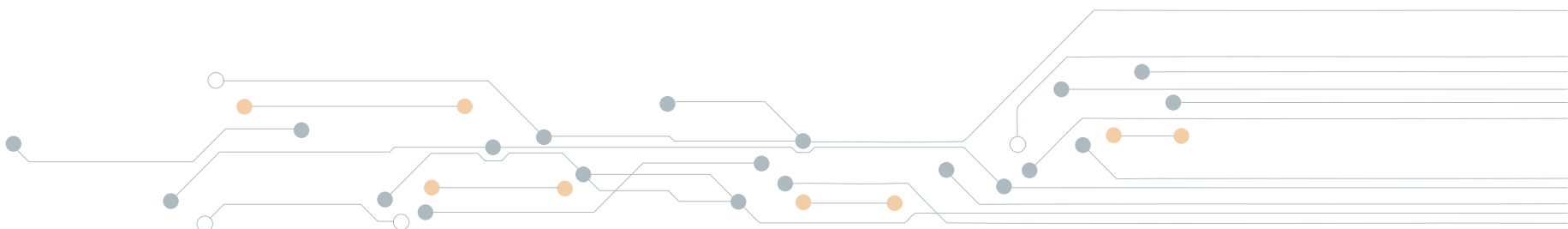
```
Win7 %system root%\System32\winevt\logs\Security.evtx
```

- **Tipos de inicio de sesión:** puede darnos información muy específica sobre la naturaleza de las autorizaciones de cuenta en un sistema si sabemos dónde buscar y cómo descifrar los datos que encontramos. Además de indicarnos la fecha, la hora, el nombre de usuario, el nombre de host y el estado de éxito / fallo de un inicio de sesión, también podemos determinar exactamente qué significa que se intentó iniciar sesión.

```
Win7 Event ID 4624
```

- **Uso de RDP:** realiza el seguimiento de los inicios de sesión de Protocolo de Escritorio Remoto en las máquinas de destino.

```
Win7 %system root%\System32\winevt\logs\Security.evtx
```



Uso de Navegadores

- **Historial:** registra los sitios web visitados por fecha y hora. Detalles almacenados para cada cuenta de usuario local. Registra el número de veces visitadas (frecuencia). También controla el acceso de los archivos del sistema local.

```
Win7 %userprofile%\AppData\Local\Microsoft\Windows\History\History.IE5
```

```
Win7 %userprofile%\AppData\Local\Microsoft\Windows\History\Low\History.IE5
```

```
Win7 %userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\<random text>.default\places.sqlite
```

- **Cookies:** las cookies ofrecen información sobre qué sitios web se han visitado y qué actividades pueden haber tenido lugar allí.

```
Win7 %userprofile%\AppData\Roaming\Microsoft\Windows\Cookies
```

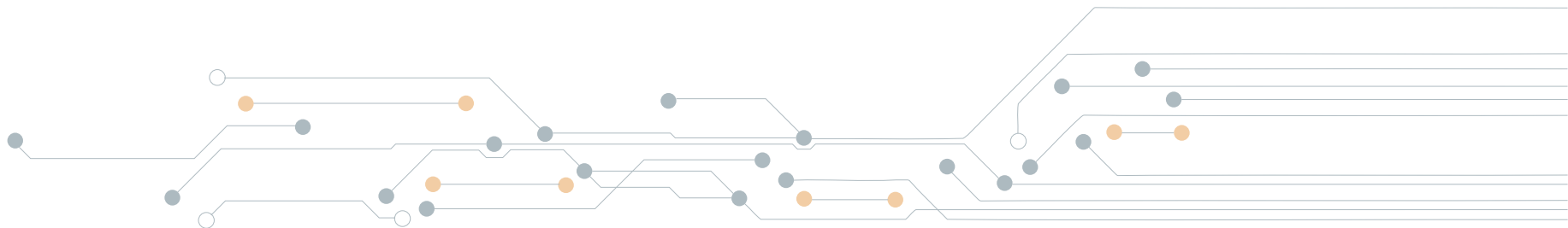
```
Win7 %userprofile%\AppData\Roaming\Microsoft\Windows\Cookies\Low
```

- **Cache:** el caché es donde los componentes de la página web se pueden almacenar localmente para acelerar las visitas posteriores. Le da al investigador una “instantánea en el tiempo” de lo que un usuario estaba viendo en línea. Identifica los sitios web visitados. Proporciona los archivos reales que el usuario vio en un sitio web determinado. Los archivos en caché están vinculados a una cuenta de usuario local específica. Las marcas de tiempo muestran cuándo se guardó y guardó por última vez el sitio:

```
Win7 %userprofile%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5
```

```
Win7 %userprofile%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5
```

```
Win7 %userprofile%\AppData\Local\Mozilla\Firefox\Profiles\<random text>.default\Cache
```



- **Restaurar sesión:** recuperación automática de fallos incorporada en el navegador.

```
Win7 %userprofile%/AppData/Local/Microsoft/  
InternetExplorer/Recovery
```

```
Win7 %userprofile%\AppData\Roaming\Mozilla\Firefox\  
Profiles\<random text>.default\sessionstore.js
```

- **Flash & Super Cookies:** los Objetos Almacenados Locales (LSOs), o Flash Cookies, se han convertido en omnipresentes en la mayoría de los sistemas debido a la penetración extremadamente alta de las aplicaciones Flash a través de Internet. Los LSO permiten que una aplicación web almacene información que posteriormente pueda tener acceso la misma aplicación (o dominio). Tienden a ser mucho más persistentes, ya que no caducan y no hay mecanismo incorporado en el navegador para eliminarlos. De hecho, muchos sitios han comenzado a usar LSOs para sus mecanismos de seguimiento, ya que rara vez se eliminan como las cookies tradicionales.

```
Win7 %APPDATA%\Roaming\Macromedia\Flash Player\
```

```
Win7 %APPDATA%\Roaming\Macromedia\Flash  
Player\#SharedObjects\<random profile id>
```

```
Win7 %APPDATA%\Roaming\Macromedia\Flash Player\  
macromedia.com\support\flashplayer\sys
```



3. Principales artefactos en el sistema operativo Windows

A continuación, entraremos en detalle algunos de los principales artefactos que podemos encontrarnos en el sistema operativo Windows.

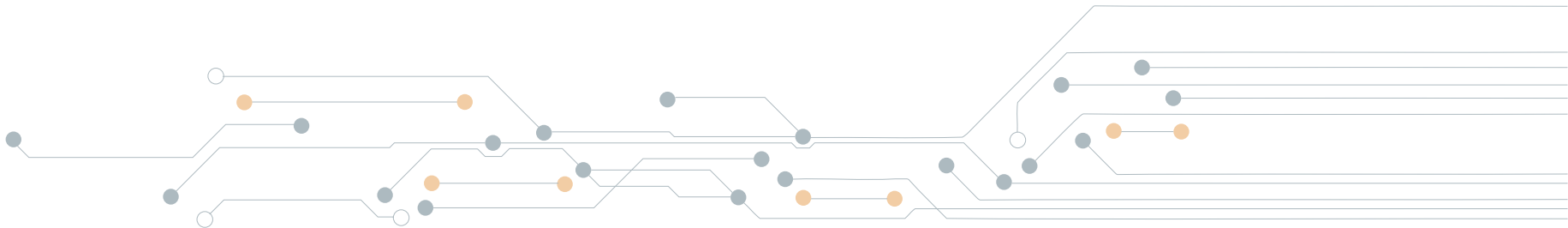
El registro de Windows

El registro de Windows es una gran base de datos con información exhaustiva relacionada con la multitud de elementos que componen un sistema Microsoft Windows. Entre otras muchas categorías será posible localizar información respecto de:

- Sistema Operativo
- Aplicaciones del sistema
- Aplicaciones nativas
- Aplicaciones de terceros instaladas
- Configuraciones de máquina y usuario

Esta información se almacena en diferentes archivos dependiendo de la versión del sistema operativo al que pertenezca el registro y el tipo de información del que se esté almacenando la configuración.

En principio la información almacenada en esta base de datos puede parecer complicada pero su funcionamiento no es tan complejo. Representa una valiosa fuente de información en el que se encuentran las configuraciones de usuarios, de aplicaciones, las acciones efectuadas por el usuario, y cómo las ha realizado, junto a otros múltiples datos funcionales.

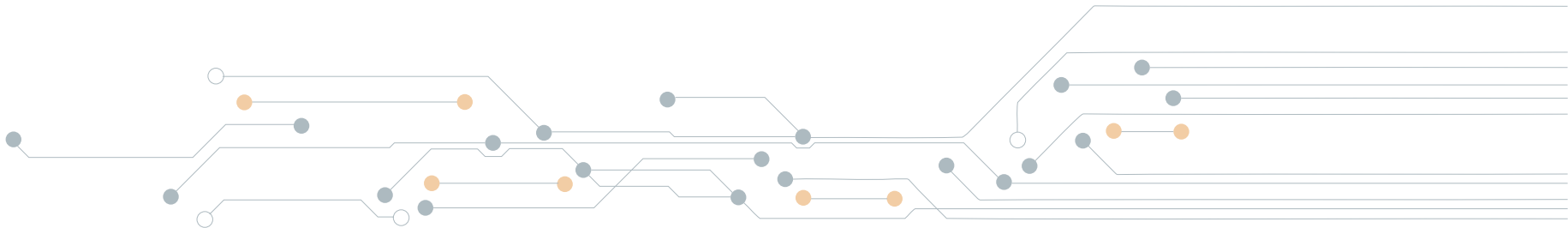


Estos ficheros se conforman un grupo lógico de claves, subclaves y valores, todos ellos fundamentales para el funcionamiento del sistema. Microsoft denomina a estos ficheros Registry Hives y, desde que se enciende el sistema operativo hasta que se apaga, se encuentran en continuo uso.

- **HKEY_CLASSES_ROOT:** garantiza que cuando abra un archivo con el Explorador de Windows se abrirá el programa correcto.
- **HKEY_CURRENT_USER:** configuración del usuario que ha iniciado sesión.
- **HKEY_LOCAL_MACHINE:** Información de configuración específica del equipo (para cualquier usuario).
- **HKEY_USERS:** Perfiles de usuario cargados activamente en el equipo.
- **HKEY_CURRENT_CONFIG:** Información acerca del perfil de hardware que utiliza el equipo local cuando se inicia el sistema.

Así mismo, existen una serie de ficheros que pueden ser recopilados y que sirven de respaldo para las claves de registro.

- **HKEY_LOCAL_MACHINE\SAM:** Sam, Sam.log, Sam.sav
- **HKEY_LOCAL_MACHINE\Security:** Security, Security.log, Security.sav
- **HKEY_LOCAL_MACHINE\Software:** Software, Software.log, Software.sav
- **HKEY_LOCAL_MACHINE\System:** System, System.alt, System.log, System.sav
- **HKEY_CURRENT_CONFIG:** System, System.alt, System.log, System.sav, Ntuser.dat, Ntuser.dat.log
- **HKEY_USERS\DEFAULT:** Default, Default.log, Default.sav



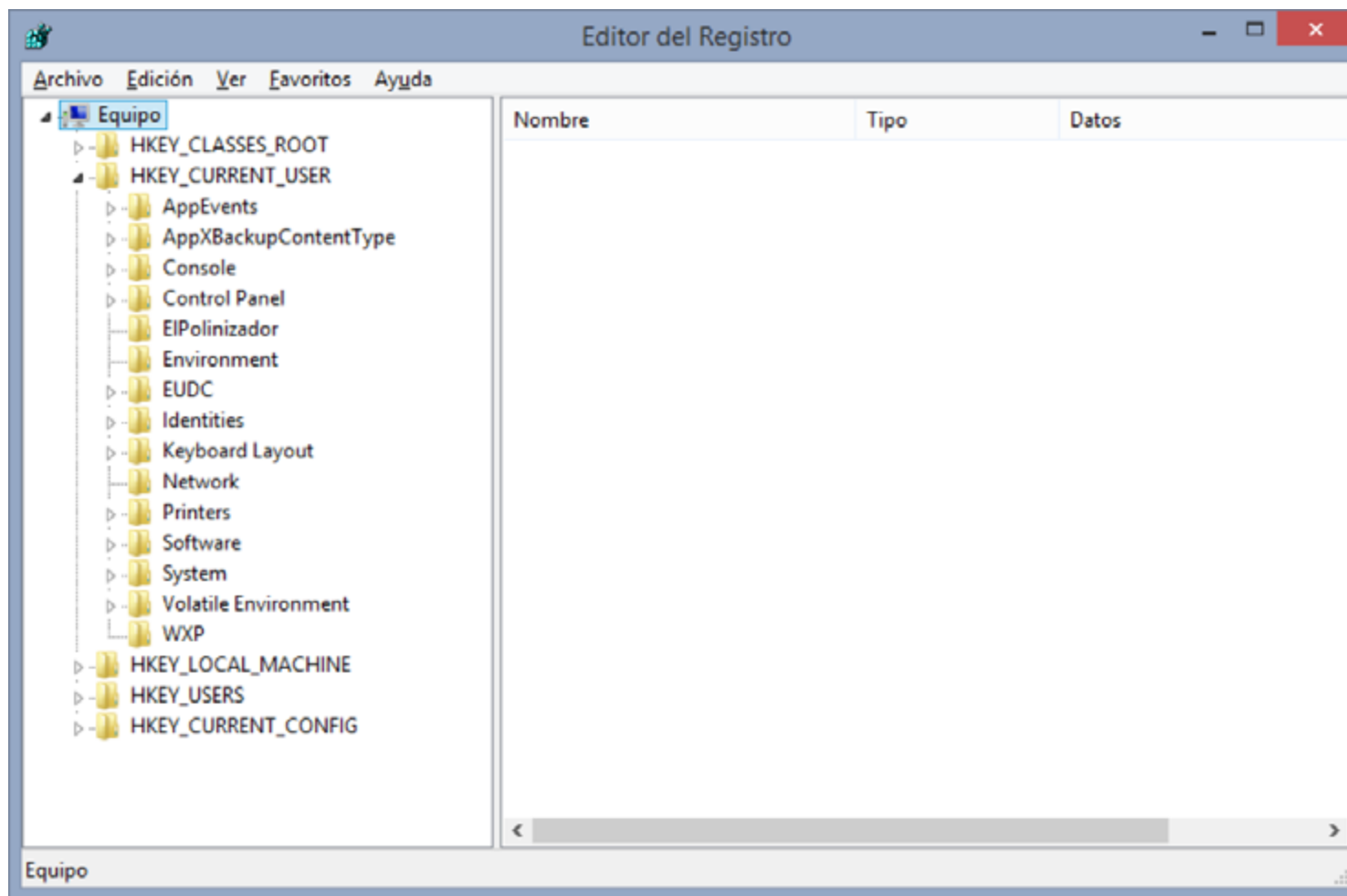
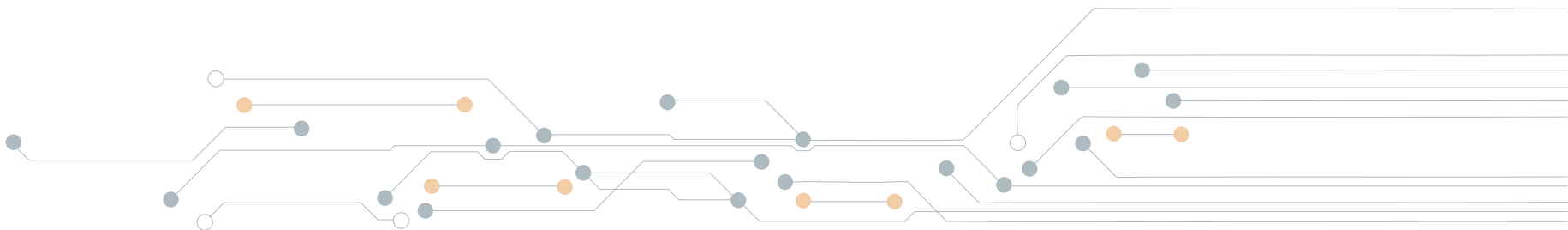


Imagen 54 Editor del Registro de Windows



Una vez que se conoce cómo se almacena toda esta información en el registro será más fácil para el analista obtener y explotar los datos obtenidos en él. Un análisis del mismo se puede realizar tanto de forma online como offline.

- **Análisis Online:** el registro se puede analizar de forma online sin ningún problema, obteniendo información respecto del estado actual del sistema en tiempo real. Existen muchas posibilidades y metodologías para hacerlo, ya sea a través de la extracción de datos, exportación de claves para su posterior análisis o comparación de ficheros. Existe un gran número de claves de registro que guardan información muy valiosa del sistema operativo y de los usuarios que hacen uso de él.
- **Análisis Offline:** hay que tener presente que si el sistema está infectado con algún malware que utilice tecnologías rootkit de ocultación puede hacer que se obtenga información falseada. Es por tanto necesario realizar un análisis offline del registro.

Para un correcto análisis offline del registro completo se han de realizar copias de todas las ubicaciones en donde se pueden encontrar las bases de datos que conforman el mismo.

Hay diversas herramientas para realizar copias y analizar el registro de Windows. Destacaremos RegRipper ya que es una de las más completas para analizar de manera offline. Esta herramienta es rápida y escalable, gracias a su estructura de plugins. No es un visor de registro, sino que parsea claves importantes del registro buscando información en base a patrones de búsqueda. Una vez iniciada la herramienta, y en función de los datos que se deseen parsear, RegRipper utilizará una serie de plugins para extraer esa información e introducirla en un archivo log, el cuál mostrará información acerca de los datos extraídos, separados por claves y aportando información adicional, como puede ser la última vez que se escribió en esa clave.



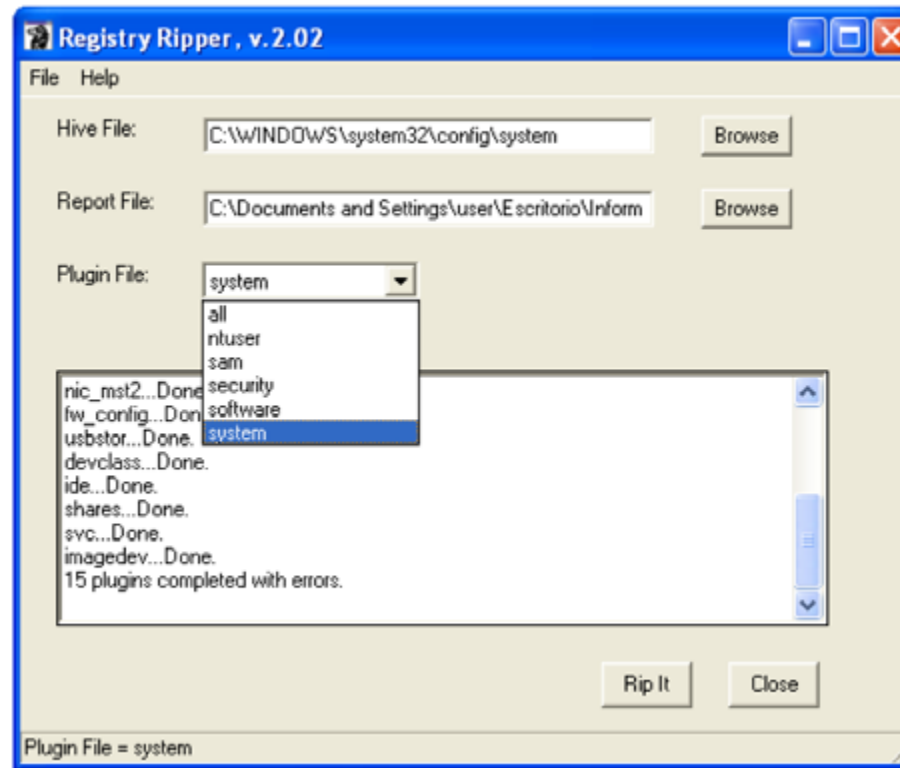
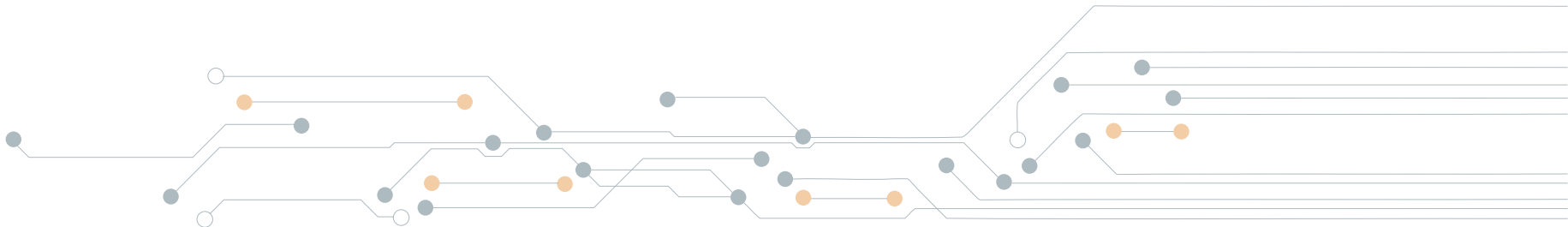


Imagen 55 RegRipper

También podemos comprobar de una forma visual el registro a través de la herramienta Windows Registry Recovery, facilitado la extracción de información rápidamente y de una forma muy cómoda.



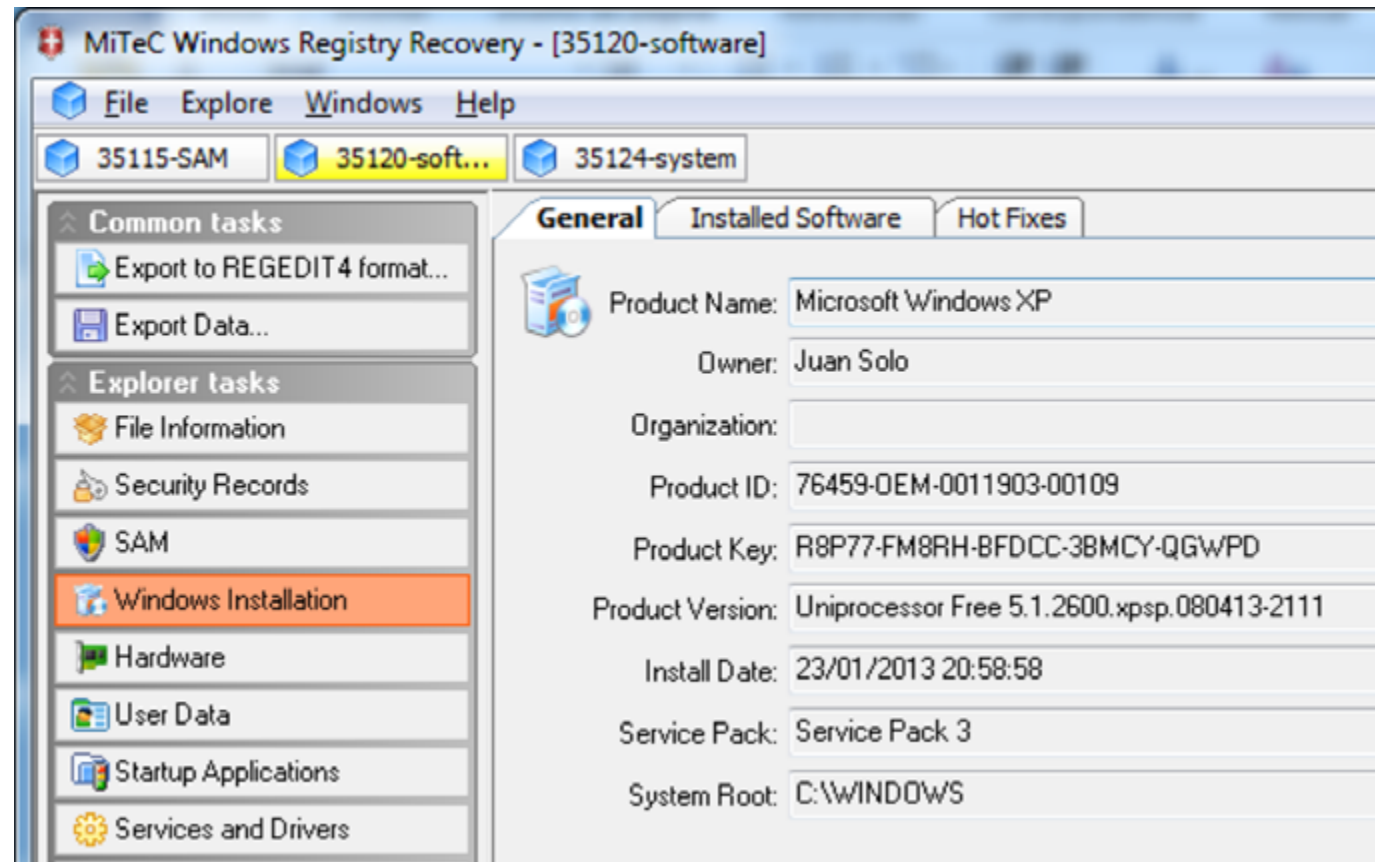
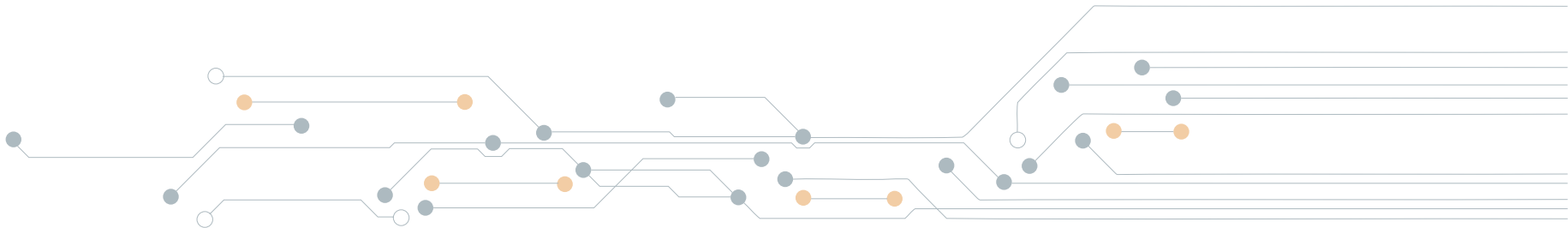


Imagen 56 Windows Registry Recovery



Visor de eventos

Es una de las herramientas de diagnóstico más fundamentales de Microsoft Windows ya que permite de un modo sencillo conocer los errores o alertas que se han producido y obtener los datos para averiguar la causa que lo ha provocado.

Permite trazar líneas de tiempo y analizar los eventos que han ido ocurriendo en el sistema, para poder resolver un incidente relacionado con la detección de vulnerabilidades, fallos en el sistema, ...

La información está organizada de una manera poco amigable, pero con un poco de práctica se puede entender y comprender fácilmente la información.

El visor de eventos se carga con el comando *eventvwr.msc* y recomendable realizarlo con privilegios de Administrador, ya que nos permitirá tener un mayor control sobre los logs del sistema. Al iniciar el visor de eventos nos aparece una pantalla como la siguiente, en la que se puede observar en la columna izquierda las dos categorías principales como son el Registro de Windows y el Registro de aplicaciones.



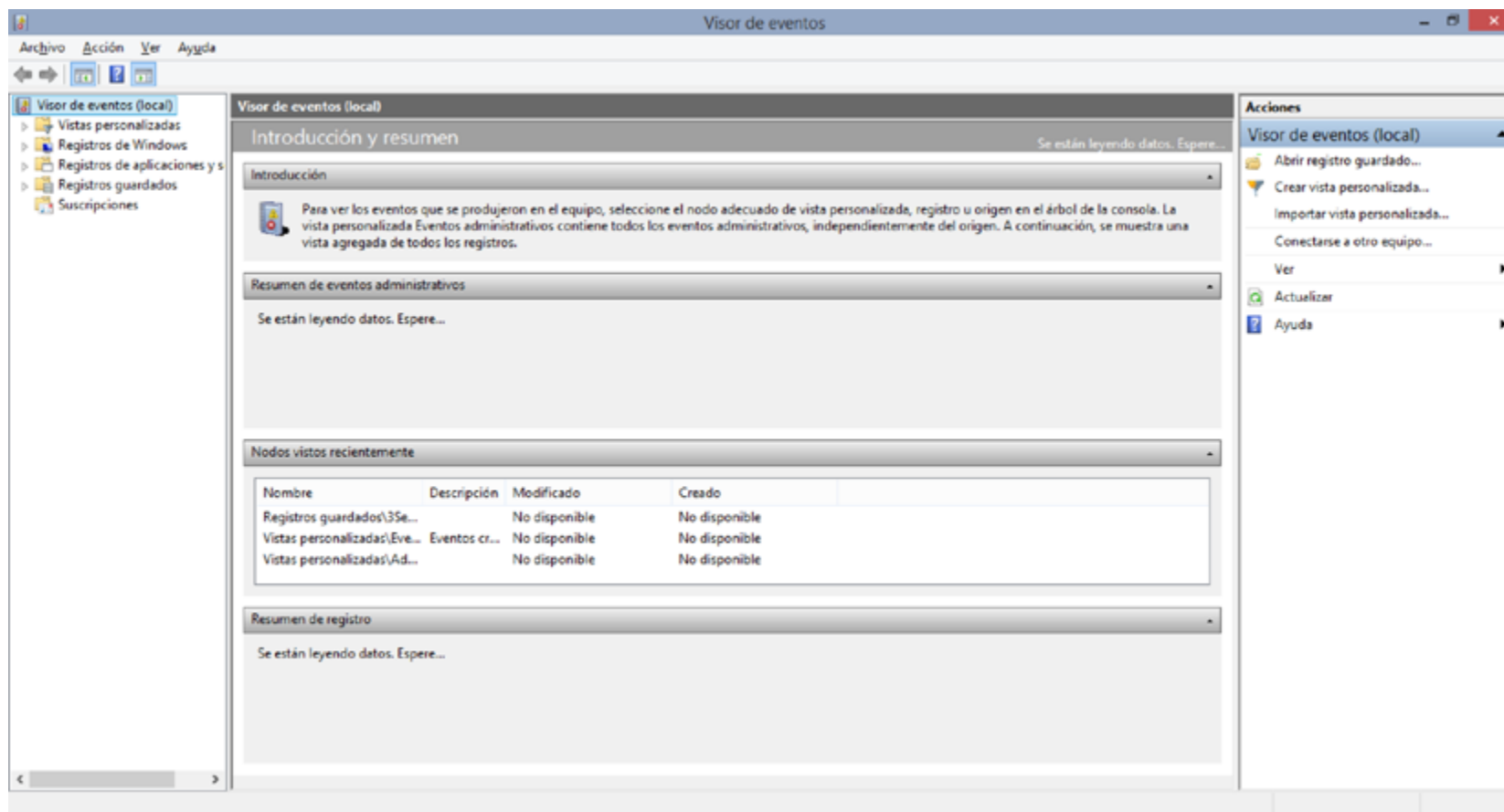
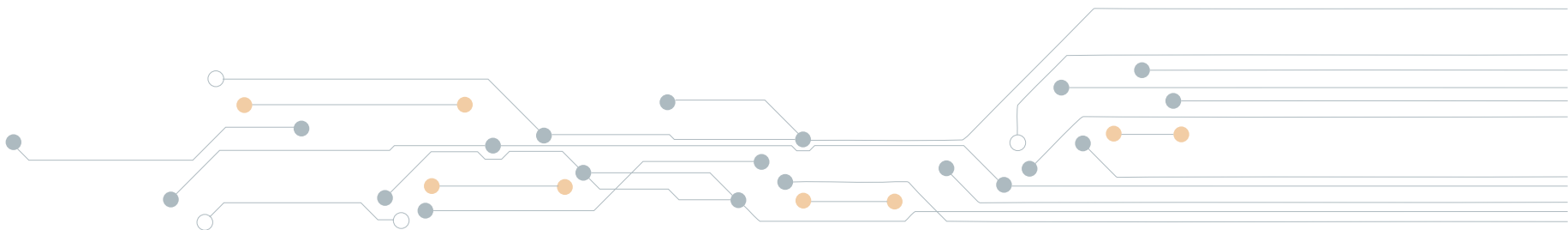


Imagen 57 Visor de eventos



Registros de Windows: en esta categoría se almacenan una gran cantidad de registros a nivel del sistema operativo, que se subdividen

en cinco subcategorías: Aplicación, Instalación, Seguridad, Sistema y Eventos reenviados.

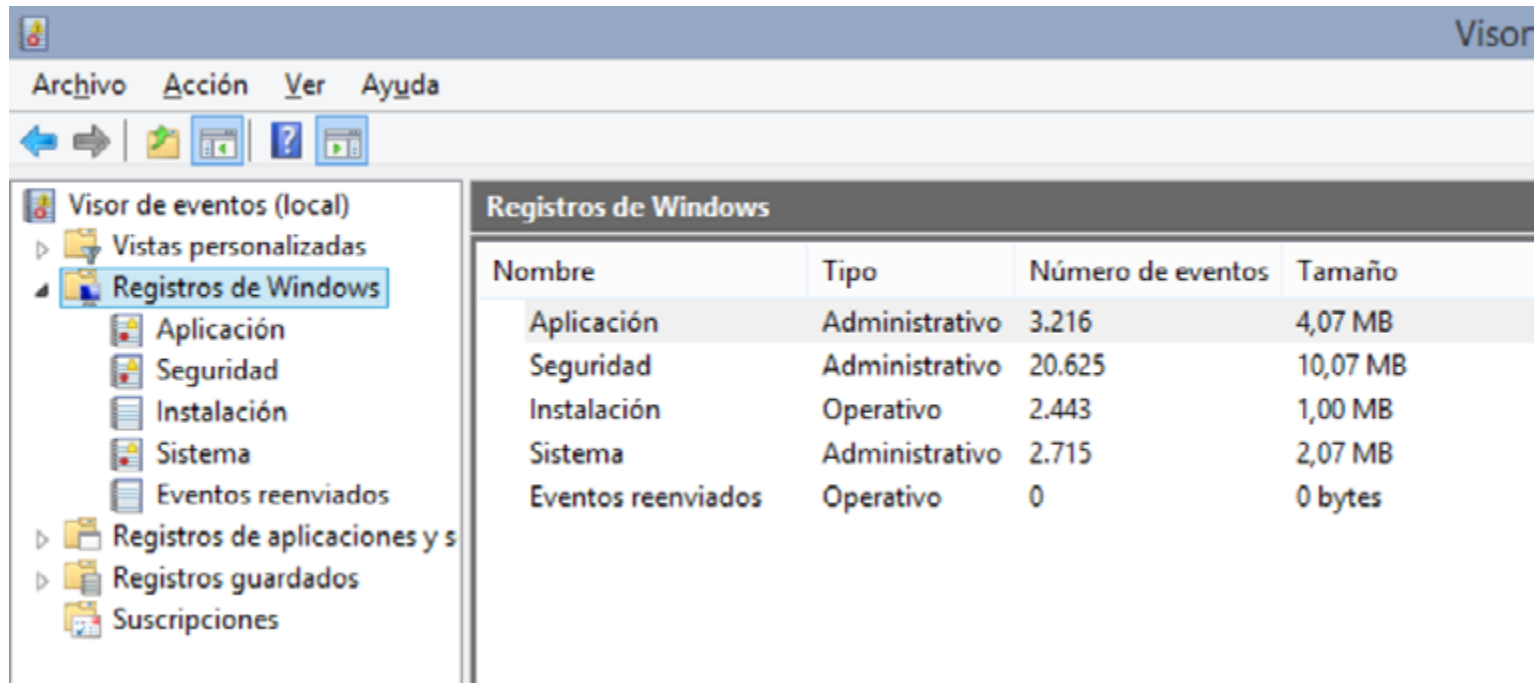
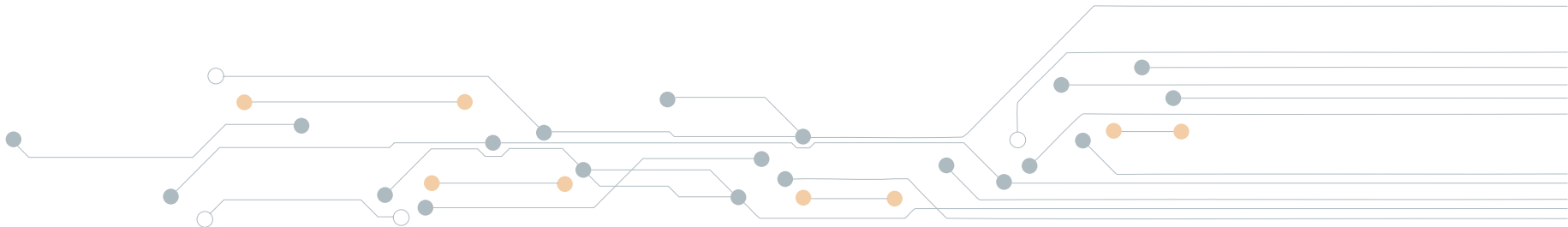


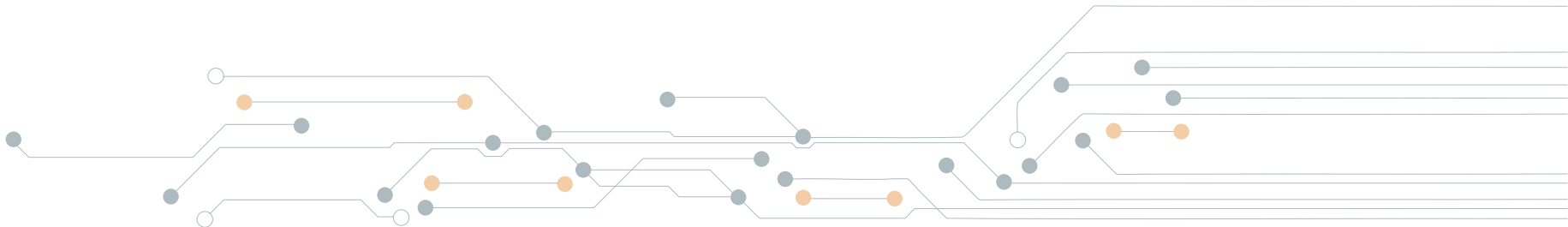
Imagen 58 Visor de eventos - Registros de Windows

Los eventos están clasificados por un identificador que determina el tipo de evento y a que está asociado. A continuación, se muestra un listado con los eventos principales.



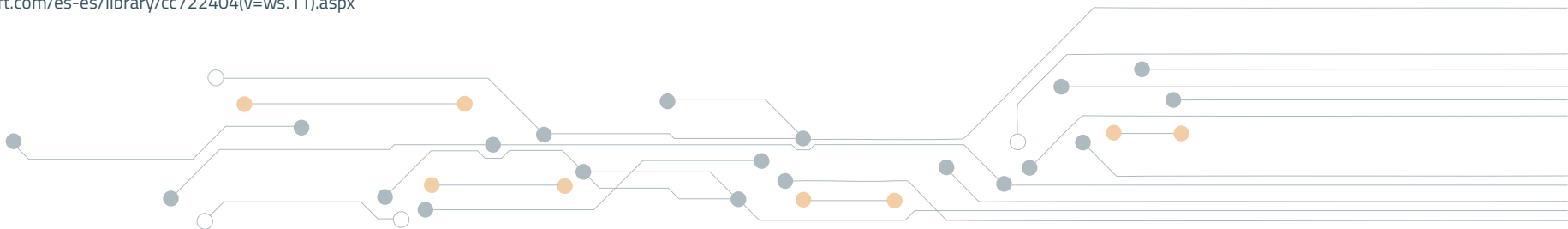
Event ID	Descripción
4624	Acceso exitoso
4625	Error de sesión
4672	Administración de cuentas de sesión
4647	Cierre de sesión exitoso
4634	Cierre de sesión exitoso
4771	Error en la pre- autenticación a través de dominio
4768	Controlador de dominio emitió TGT(Ticket Granting Ticket)
4776	Inicio de sesión fallido o exitoso a través de dominio
7034	Servicio caído de forma inesperada
7035	El Servicio envía una señal de arranque o apagado
7036	Detenimiento o Inicio de Servicio
7040	El Tipo de inicio del servicio ha cambiado
5140	Asignación de recurso compartido en la red
4778	Iniciación de sesión RDP
4779	Finalización de la sesión RDP
106	Tarea programada
200	Tarea ejecutada
201	Tarea terminada
141	Tarea Eliminada

Imagen 59 Lista de ID de eventos



- **Registro de la aplicación¹:** el registro de aplicación contiene los eventos registrados por aplicaciones o programas. Por ejemplo, un programa de base de datos podría registrar un error de archivo en el registro de la aplicación. Los programadores deciden qué eventos se deben registrar.
- **Registro de seguridad:** el registro de seguridad guarda eventos como intentos de inicio de sesión válidos y no válidos, además de eventos relacionados con el uso de recursos, como la creación, apertura o eliminación de archivos u otros objetos. Los administradores pueden especificar los eventos que se incluirán en el registro de seguridad. Por ejemplo, si habilitó la auditoría de inicio de sesión, se incluirán en el registro de seguridad los intentos de inicio de sesión en el sistema.
- **Registro de instalación:** el registro de instalación incluye los eventos relacionados con la instalación de la aplicación.
- **Registro del sistema:** el registro del sistema contiene eventos registrados por componentes del sistema Windows. Por ejemplo, el error al cargar un controlador u otro componente del sistema durante el inicio queda registrado en el registro del sistema. Los tipos de eventos registrados por los componentes del sistema están predeterminados por Windows.
- **Registro de eventos reenviados:** el registro de eventos reenviados se usa para almacenar eventos recopilados de equipos remotos. Para recopilar eventos de equipos remotos, debe crear una suscripción de evento. Para obtener información acerca de las suscripciones, consulte Suscripciones a eventos.

¹ [https://technet.microsoft.com/es-es/library/cc722404\(v=ws.11\).aspx](https://technet.microsoft.com/es-es/library/cc722404(v=ws.11).aspx)



Registros de aplicaciones y servicios: muestra los eventos de una aplicación o componente en concreto que no tenga impacto sobre el todo el sistema.

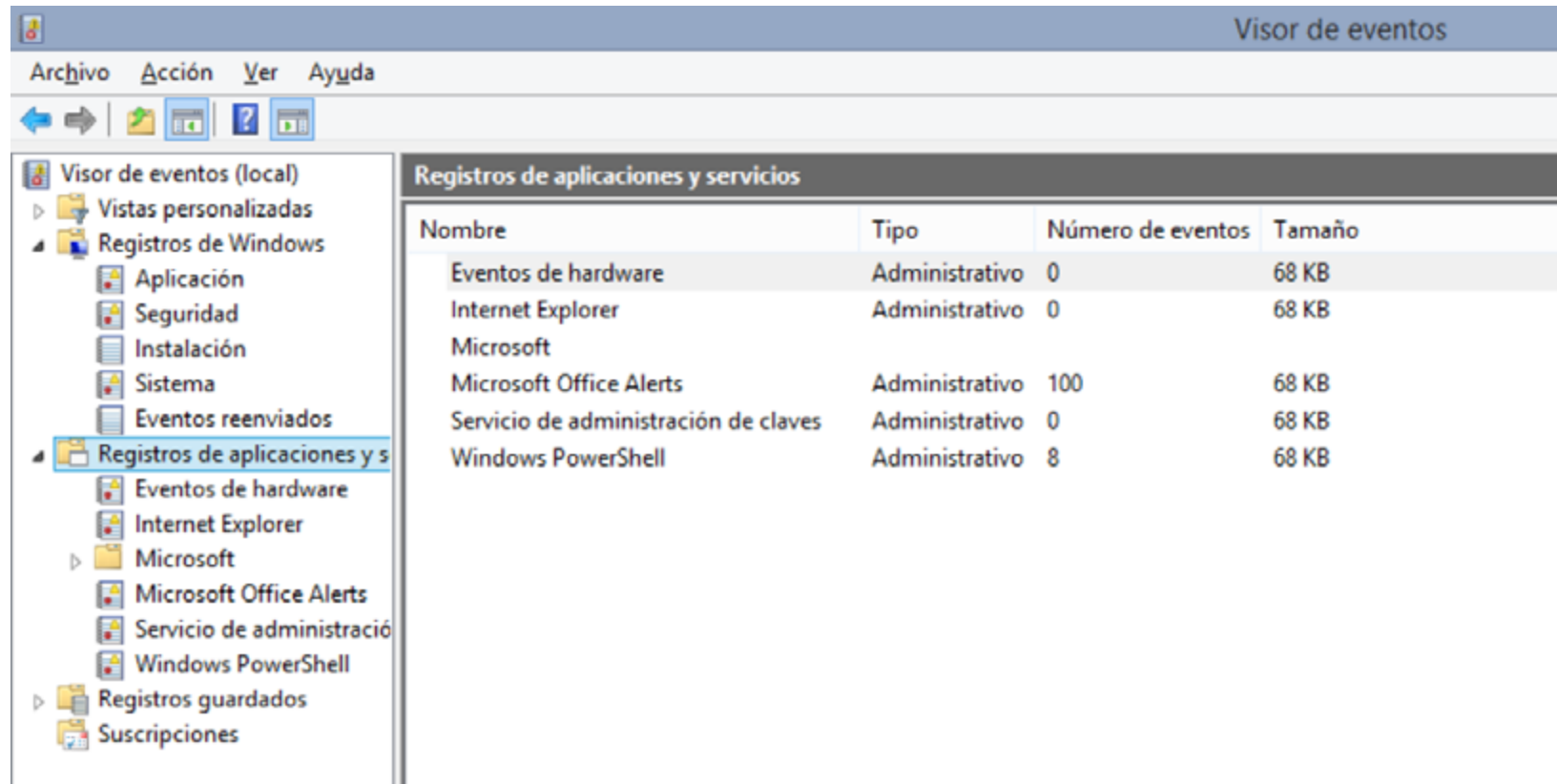
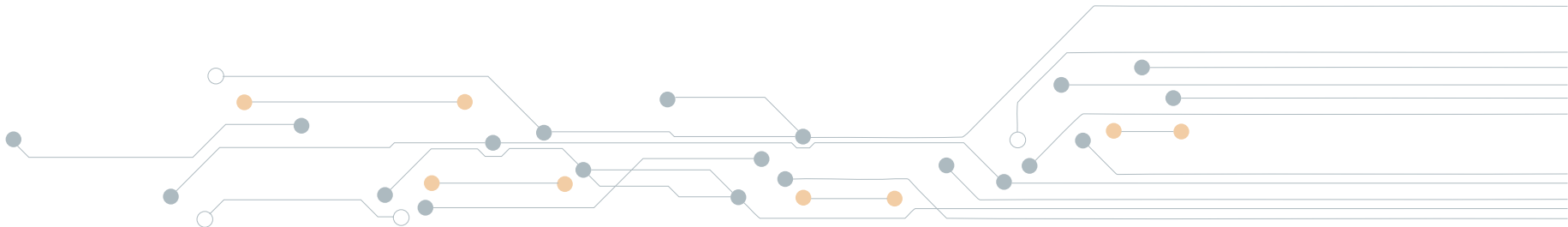


Imagen 60 Visor de eventos - Registros de aplicaciones y servicios



Esta categoría de registros incluye cuatro subtipos: registros de administración, operativos, analíticos y de depuración. Los eventos de los registros de administración son de particular interés para los profesionales de TI que usan el visor de eventos para solucionar problemas. Los eventos de los registros de administración deben proporcionar una orientación sobre cómo responder. Los eventos del registro operativo también resultan útiles para los profesionales de TI, pero suelen ser más difíciles de interpretar. Los registros de administración y depuración no son tan fáciles de usar. Los registros analíticos almacenan eventos que realizan el seguimiento de un problema y, a menudo, hay un gran volumen de eventos registrados. Los registros analíticos y de depuración están ocultos y deshabilitados de manera predeterminada.

En un sistema, el número de logs que almacena puede ser inmenso, por lo que consultar individualmente uno por uno puede ser una tarea ardua. Para ello se pueden utilizar los filtros o la búsqueda de registros, sobre todo, para facilitar y delimitar el tipo de información que queremos.

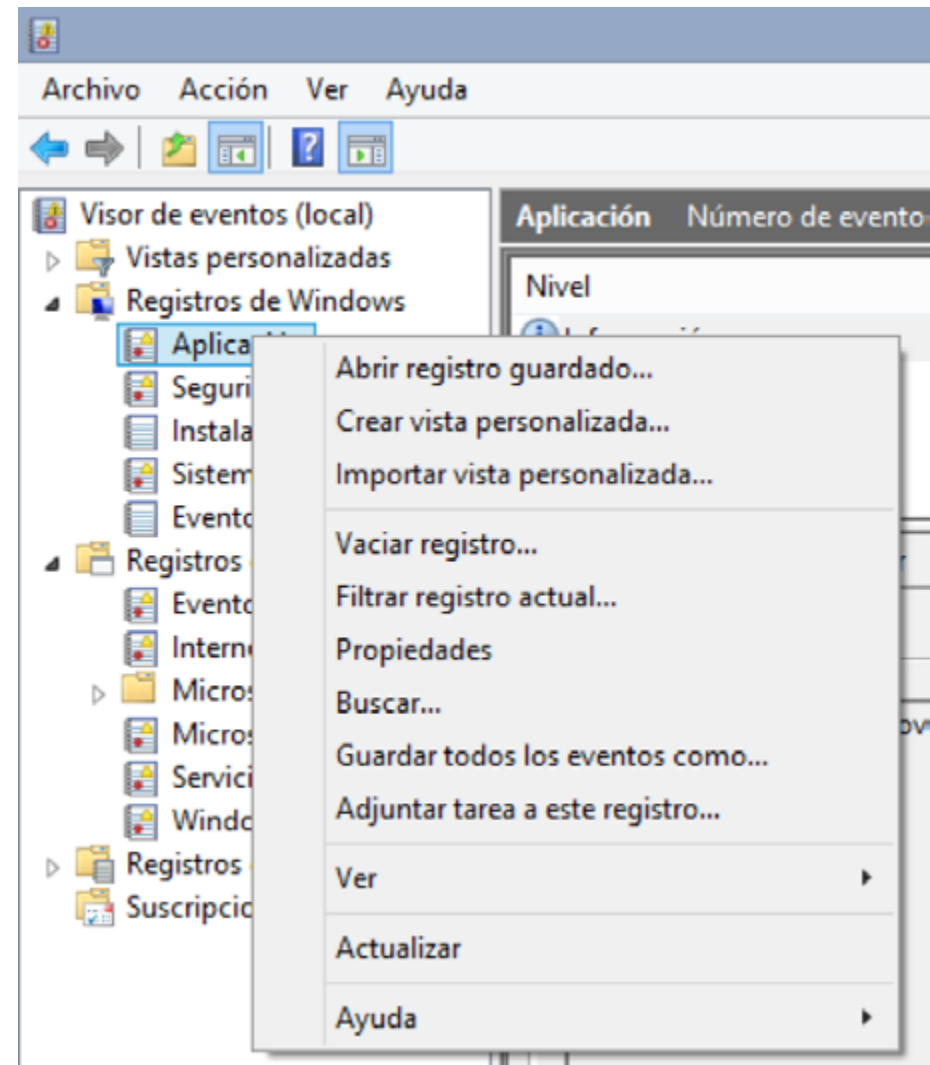
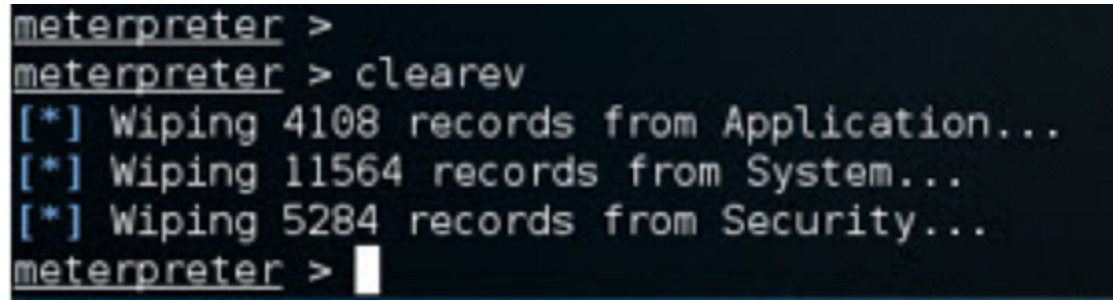


Imagen 61 Visor de eventos - Filtro y búsqueda

Hay que ir con cuidado ya que existen técnicas antiforenses que lo que permiten es borrar el registro de manera remota o local, eliminando cualquier huella que haya dejado un atacante.



```
meterpreter >  
meterpreter > clearev  
[*] Wiping 4108 records from Application...  
[*] Wiping 11564 records from System...  
[*] Wiping 5284 records from Security...  
meterpreter >
```

Imagen 62 Borrado de eventos

También hay que tener cuidado con no contaminar la escena ya que estas herramientas lo que hacen es, como comentábamos, registrar todo lo que sucede en el sistema, incluso si hemos accedido al visor, o a cualquier otro componente. Esto, podría acarrear que un caso se anulara ante un juez, para ello, deberíamos utilizar otra clase de herramientas externas como Helix, Deft,...

Prefetch

Todo lo que ocurre desde que arrancamos el ordenador queda almacenado en un conjunto de archivos dentro de la carpeta Prefetch, de modo que a la próxima vez que se arranque el ordenador el sistema accederá a dicha carpeta para acelerar la carga del sistema. Por tanto, funciona como una cache de archivos y aplicaciones. Dicha carpeta sería interesante no borrar, ya que la próxima vez que arrancase el ordenador tardaría más de lo normal.

Además, en dicha carpeta se almacenan la fecha de la última ejecución de un programa y el número de veces que se ha ejecutado, en archivos con extensión pf. Este archivo registra también la

información sobre el disco, el número de serie e información extra muy interesante para los casos de forense. Por tanto, cualquier aplicación que se haya ejecutado deja huella en el sistema.

Durante los primeros segundos de la ejecución de un programa, ésta es monitorizada por el "Windows cache manager" y la consecuencia conlleva que se escriba en un fichero pf toda la información anterior. El nombre tiene la estructura programa-HASH.pf Siendo el HASH un número de 32 bits en hexadecimal calculado a partir de la ruta completa del programa.

La clave del registro, como hemos visto anteriormente en el listado de artefactos está en HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters

Hay disponibles varias herramientas para el manejo de archivos pf, pero podemos destacar WinPrefetchView² ya que nos permite visualizar de modo legible la información de estos ficheros y es muy útil en un análisis forense en busca de evidencias, instalación de aplicaciones, detectar intrusiones de algún tipo de malware.

² http://www.nirsoft.net/utils/win_prefetch_view.html

WinPrefetchView

File Edit View Options Help

Filename	Created Time	Modified Time	File Size	Process EXE	Process Path	Run Counter	Last Run Time	Missing Pr...
3.4.9_42973.EXE-19A7...	06/12/2016 13:02...	06/12/2016 13:02...	77.530			1	06/12/2016 13:02:33	No
ADDINUTILE.EXE-E4104...	09/12/2016 17:40...	09/12/2016 17:40...	72.254	ADDINUTILE.EXE	C:\Windows\MICROSOFT.NET\FRAMEWO...	2	09/12/2016 17:40:41, 09/12/2016 17:40:40	No
AM_DELTA.EXE-B7261...	09/12/2016 8:11:32	09/12/2016 8:11:32	56.216	AM_DELTA.EXE	C:\WINDOWS\SOFTWAREDISTRIBUTION\...	1	09/12/2016 8:11:22	Yes
AM_DELTA_PATCH_1...	07/12/2016 5:38:52	07/12/2016 5:38:52	18.448			1	07/12/2016 5:38:42	No
AM_DELTA_PATCH_1...	08/12/2016 4:33:25	08/12/2016 4:33:25	15.468	AM_DELTA_PATC...	C:\WINDOWS\SOFTWAREDISTRIBUTION\...	1	08/12/2016 4:33:15	Yes
AM_DELTA_PATCH_1...	10/12/2016 8:27:38	10/12/2016 8:27:38	16.314			1	10/12/2016 8:27:28	No
APP.HASHCATGUI.EX...	31/10/2016 12:40...	31/10/2016 12:40...	101.916				31/10/2016 12:40:08	Yes
APP.HASHCATGUI.EX...	31/10/2016 12:44...	31/10/2016 12:44...	96.892				31/10/2016 12:44:09	Yes
BACKGROUNDTRANS...	07/12/2016 13:11...	08/12/2016 9:15:50	33.528				08/12/2016 9:15:41, 07/12/2016 13:11:45	No
BURPSUITE_FREE_WIN...	24/11/2016 9:19:55	24/11/2016 9:19:55	58.742				24/11/2016 9:19:54	No
CALC.EXE-77FDF17F.pf	11/11/2016 17:35...	07/12/2016 9:15:58	31.592				07/12/2016 9:15:48, 07/12/2016 9:14:18, 28/11/2016	No
CHROME.EXE-D999B1...	11/11/2016 16:25...	10/12/2016 23:02...	21.490				10/12/2016 23:02:26, 10/12/2016 22:49:19, 1...	No
CHROME.EXE-D999B1...	10/11/2016 21:15...	10/12/2016 23:02...	42.364				10/12/2016 23:02:26, 10/12/2016 22:48:07, 1...	No
CHROME.EXE-D999B1...	08/12/2016 7:11:14	08/12/2016 9:28:04	81.702				08/12/2016 9:27:54, 08/12/2016 7:21:19, 08/11/2016	No
CHROME.EXE-D999B1...	10/11/2016 21:18...	10/12/2016 23:02...	21.438				10/12/2016 23:02:26, 10/12/2016 22:49:19, 1...	No

Properties

Filename: CALC.EXE-77FDF17F.pf

Created Time: 11/11/2016 17:35:59

Modified Time: 07/12/2016 9:15:58

File Size: 31.592

Process EXE: CALC.EXE

Process Path: C:\Windows\System32\calc.exe

Run Counter: 9

Last Run Time: 07/12/2016 9:15:48, 07/12/2016 9:14:18, 28/11/2016

Missing Process: No

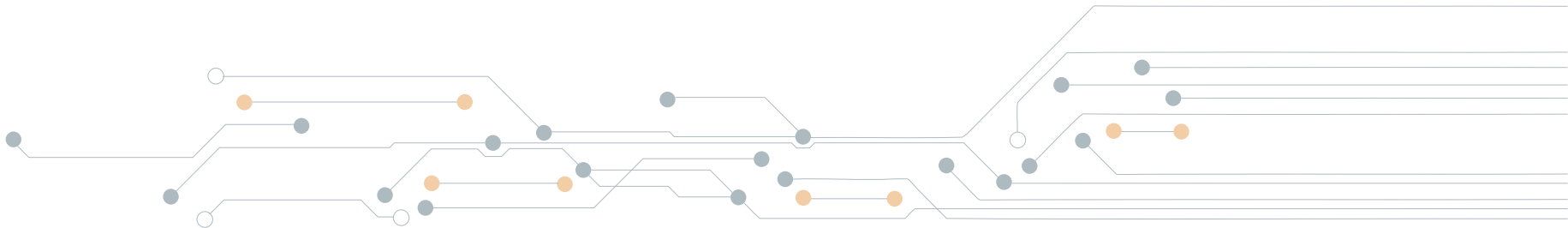
OK

Filename	Full Path	Device
SMFT	C:\Windows\System32\SHCore.dll	\DEVICE\HARDISKVOLUME2\WIND...
ADVAPI32.DLL	C:\Windows\System32\advapi32.dll	\DEVICE\HARDISKVOLUME2\WIND...
BCRYPTPRIMITIVES.DLL	C:\Windows\System32\BCRYPTPRIMI...	\DEVICE\HARDISKVOLUME2\WIND...
CALC.EXE	C:\Windows\System32\calc.exe	\DEVICE\HARDISKVOLUME2\WIND...
CALC.EXE.MUI	C:\Windows\System32\es-ES\CALC.E...	\DEVICE\HARDISKVOLUME2\WIND...
CFGMR32.DLL	C:\Windows\System32\cfgmgr32.dll	\DEVICE\HARDISKVOLUME2\WIND...
CLBCATQ.DLL	C:\Windows\System32\clbcatq.dll	\DEVICE\HARDISKVOLUME2\WIND...
COM-PATERVA-MAL...	C:\PROGRAM FILES (X86)\Paterna\M...	\DEVICE\HARDISKVOLUME2\PROG...
COMBASE.DLL	C:\Windows\System32\combase.dll	\DEVICE\HARDISKVOLUME2\WIND...
COMCTL32.DLL	C:\Windows\WinSxS\AMD64_MICRO...	\DEVICE\HARDISKVOLUME2\WIND...
CRYPTBASE.DLL	C:\Windows\System32\CRYPTBASE.D...	\DEVICE\HARDISKVOLUME2\WIND...
DEVOBJ.DLL	C:\Windows\System32\devobj.dll	\DEVICE\HARDISKVOLUME2\WIND...
DWMAPI.DLL	C:\Windows\System32\dwmapi.dll	\DEVICE\HARDISKVOLUME2\WIND...
GDI32.DLL	C:\Windows\System32\gdi32.dll	\DEVICE\HARDISKVOLUME2\WIND...
GDIPLUS.DLL	C:\Windows\WinSxS\AMD64_MICRO...	\DEVICE\HARDISKVOLUME2\WIND...

206 Files, 1 Selected

NirSoft Freeware. <http://www.nirsoft.net>

Imagen 63 WinPrefetchView



Telefonica EDUCACIÓN DIGITAL