

## Practica 1

# Análisis Post-mortem, los artefactos Windows

### Parte A:

#### 1. Con respecto a los “prefetch”:

a) ¿Qué son?

Los archivos **prefetch** son **archivos binarios** que contienen información sobre las aplicaciones y archivos utilizados con frecuencia durante el arranque del sistema operativo. Estos archivos ayudan al sistema operativo a **acelerar la carga** de programas al predecir cuales se utilizaran y cargandolos en la memoria antes de que el usuario los solicite.

b) ¿Qué extensión tienen los ficheros?

Los archivos **prefetch** en sistemas operativos Windows tienen la extensión **".pf"**. Por ejemplo, un archivo prefetch para una aplicación llamada "example.exe" se llamará "example.exe.pf".

c) ¿En qué directorio los podemos encontrar?

Los archivos **prefetch** se almacenan en el directorio **"%SystemRoot%\Prefetch"**. Normalmente, el directorio de prefetch está en la raíz del sistema operativo, donde **"%SystemRoot%"** representa la carpeta de instalación de Windows, como **"C:\Windows\Prefetch"**.

d) ¿Qué información forense guardan que pueda ser importante para una investigación?

Los archivos **prefetch** en Windows guardan información sobre las aplicaciones utilizadas, su fecha y hora de ejecución, y la frecuencia de uso. Son útiles en investigaciones forenses para entender la actividad del sistema y detectar posibles actividades maliciosas. Sin embargo, la información puede ser borrada o manipulada, por lo que debe considerarse como una fuente potencial en lugar de pruebas definitivas.

## 2. En cuanto a los “LOGs”:

a) ¿Cuáles piensas que son los más importantes por el contenido que guardan?

Los **logs** más importantes dependen del contexto y del propósito de la investigación. Sin embargo, en general, los **logs de seguridad** (como los registros de eventos del sistema y del servidor) son críticos, ya que registran información sobre accesos, cambios en el sistema y posibles incidentes de seguridad.

b) ¿Dónde los podemos encontrar?

Los **logs** se encuentran en diferentes ubicaciones según el sistema operativo y la aplicación. En sistemas Windows, los logs pueden estar en el **Visor de eventos (Event Viewer)**, mientras que en sistemas basados en Unix/Linux, los logs suelen almacenarse en directorios como **"/var/log"**. Las aplicaciones específicas también pueden generar sus propios logs en ubicaciones designadas. La identificación precisa de los logs relevantes dependerá del entorno y de los eventos que se estén investigando.

## 3. En cuanto al fichero de hibernación “hiberfil.sys”:

a) ¿Dónde lo podemos encontrar?

El archivo de hibernación **"hiberfil.sys"** se encuentra típicamente en la raíz del directorio del sistema operativo. Por ejemplo, en sistemas Windows, podría ubicarse en la misma carpeta que el sistema operativo, como **"C:\hiberfil.sys"**.

b) ¿Qué herramienta podemos utilizar para decodificar su contenido?

Para analizar el contenido del archivo de **hibernación**, se pueden utilizar herramientas forenses especializadas, como **Volatility Framework**. Volatility es una herramienta que puede extraer información del archivo de hibernación y analizarla para obtener detalles sobre los procesos en ejecución, la memoria del sistema, y otros datos relevantes.

c) ¿Piensas que es importante la información que contiene?

Sí, la información en el archivo de **hibernación** puede ser valiosa en una investigación forense. Contiene una instantánea de la memoria del sistema en el momento en que se activó la hibernación. Esto puede incluir datos sobre procesos en ejecución, conexiones de red, y otros detalles del estado del sistema en ese momento.

#### 4. Con respecto a las instantáneas, puntos de restauración y/o volume shadow copies service (VSS):

- a) ¿Qué sistema de archivos necesitamos para poder usar esta tecnología?

La tecnología de **instantáneas, puntos de restauración y VSS** está diseñada para funcionar con sistemas de archivos **NTFS (New Technology File System)**, que es el sistema de archivos utilizado comúnmente en sistemas operativos Windows.

- b) ¿Viene activada por defecto o la tiene que activar el usuario?

En sistemas operativos Windows, la función de **instantáneas y VSS** generalmente está activada por defecto. Sin embargo, los usuarios pueden ajustar la configuración y la frecuencia de las instantáneas a través de las opciones del sistema o herramientas específicas.

- c) ¿Cada cuánto tiempo se realizan?

La **frecuencia de las instantáneas y la creación de puntos de restauración** depende de la configuración del sistema y de las políticas del usuario. Pueden realizarse de forma programada, como parte de la configuración del sistema o cuando se instalan actualizaciones importantes del sistema.

- d) Piensa en un par de escenarios donde puedan ser de utilidad

- **Recuperación de datos:** En caso de pérdida o corrupción accidental de archivos, las instantáneas permiten a los usuarios restaurar el sistema a un estado anterior y recuperar los datos.
- **Actualizaciones del sistema:** Antes de realizar cambios significativos en el sistema, como la instalación de software o actualizaciones del sistema operativo, se pueden crear instantáneas para facilitar la restauración en caso de problemas.

#### 5. Contesta a las siguientes cuestiones relacionadas con el registro de Windows:

- a) Investiga cómo importar y exportar claves de registro en entornos CLI y GUI.

Para **exportar e importar claves del registro** en la línea de comandos en Windows, puedes utilizar la herramienta '**reg**'. Aquí hay ejemplos básicos:

- Exportar una clave:

*reg export <ruta de la clave> <nombre del archivo.reg>*

- Importar una clave:

*reg import <nombre del archivo.reg>*

Para realizar estas operaciones en el entorno gráfico, puedes utilizar el Editor del Registro (regedit):

- Para **exportar**, selecciona la clave, haz clic derecho y elige "Exportar".
  - Para **importar**, haz clic derecho en el archivo .reg y selecciona "Merge".
- b) Enumera las claves que, desde un punto de vista forense, son interesantes exportar y analizar explicando qué información revelan.
1. **HKEY\_LOCAL\_MACHINE\SOFTWARE**: Información de Software Instalado: Revela detalles sobre las aplicaciones instaladas, versiones y configuraciones.
  2. **HKEY\_CURRENT\_USER\Software**: Configuración de Usuario: Contiene configuraciones específicas del usuario y datos de aplicaciones.
  3. **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment**: Variables de Entorno: Muestra las variables de entorno del sistema, que pueden ser críticas para el funcionamiento de las aplicaciones.
  4. **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall**: Información de Desinstalación: Ofrece detalles sobre programas instalados, incluyendo desinstaladores y rutas de instalación.
  5. **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services**: Configuración de Servicios: Contiene información sobre los servicios del sistema, sus configuraciones y estados.
  6. **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders**: Proveedores de Seguridad: Contiene información sobre proveedores de seguridad utilizados en el sistema.
  7. **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enum**: Información sobre Hardware: Ofrece detalles sobre hardware conectado al sistema, útil para el análisis de dispositivos.
  8. **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**: Programas que se ejecutan en el inicio: Lista las aplicaciones que se ejecutan automáticamente al inicio del sistema.
  9. **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Windows**: Configuración del Sistema Operativo: Contiene información sobre la versión del sistema operativo, controladores y configuración del sistema.

## 6. ¿Qué tipos de eventos nos pueden interesar inspeccionar desde un punto de vista forense? Pon un par de ejemplos.

### 1. Eventos de Seguridad (Security Events):

- **Ejemplo:** Evento de inicio de sesión fallido.
- **Importancia Forense:** Puede indicar intentos de acceso no autorizados y proporcionar información sobre posibles ataques o actividades maliciosas en el sistema.

### 2. Eventos del Sistema (System Events):

- **Ejemplo:** Evento de cambio en la configuración del sistema.
- **Importancia Forense:** Permite rastrear alteraciones en la configuración del sistema, lo que puede ser crucial para identificar cambios no autorizados o actividades sospechosas.

### 3. Eventos de Registro (Registry Events):

- **Ejemplo:** Registro de cambios en claves críticas del registro.
- **Importancia Forense:** Proporciona información sobre modificaciones en la configuración del sistema, instalación o desinstalación de software, y puede ayudar a rastrear acciones realizadas por usuarios o malware.

### 4. Eventos de Red (Network Events):

- **Ejemplo:** Registro de conexiones de red inusuales.
- **Importancia Forense:** Ayuda a identificar patrones de tráfico sospechoso, intrusiones o intentos de comunicación no autorizados.

### 5. Eventos de Archivos (File Events):

- **Ejemplo:** Registro de cambios en archivos del sistema.
- **Importancia Forense:** Permite rastrear modificaciones en archivos críticos, identificar acciones de malware o manipulaciones no autorizadas.

### 6. Eventos de Aplicaciones (Application Events):

- **Ejemplo:** Registro de errores o comportamientos inusuales de aplicaciones.
- **Importancia Forense:** Puede indicar posibles problemas de seguridad, fallas del sistema o actividades anómalas en aplicaciones específicas.

### 7. Eventos de Auditoría (Audit Events):

- **Ejemplo:** Registro de acciones realizadas por usuarios privilegiados.
- **Importancia Forense:** Permite monitorear las acciones de usuarios con privilegios elevados, identificar cambios en permisos y evaluar la conformidad con las políticas de seguridad.

## **7. Investiga sobre qué herramientas software podemos utilizar a la hora de trabajar sobre los artefactos estudiados en el tema: prefetch, logs, fichero de hibernación, volume shadow copies service, registro del sistema, gestión de eventos, enlaces, cachés e historial de navegación y papelera de reciclaje.**

### **1. Autopsy:**

- Características:
  - Análisis forense de discos duros.
  - Soporte para artefactos del sistema operativo Windows.
  - Visualización de eventos, registros y otros artefactos.

### **2. EnCase:**

- Características:
  - Análisis forense de discos y sistemas.
  - Herramientas específicas para la recuperación de datos y análisis de registros.

### **3. AccessData FTK (Forensic Toolkit):**

- Características:
  - Herramienta integral de análisis forense.
  - Admite la recuperación y análisis de varios artefactos del sistema.

### **4. Volatility Framework:**

- Características:
  - Enfoque en el análisis de memoria.
  - Especializado en el análisis de sistemas basados en Windows.

### **5. Sysinternals Suite:**

- Características:
  - Conjunto de herramientas de Sysinternals para la administración y resolución de problemas de sistemas Windows.
  - Incluye herramientas como Process Explorer y Autoruns.

### **6. RegRipper:**

- Características:
  - Herramienta específica para analizar el registro del sistema Windows.
  - Facilita la extracción y presentación de información relevante.



## 7. LogParser:

- Características:
  - Herramienta de línea de comandos para analizar logs.
  - Permite consultar y extraer información de diversos registros, incluyendo logs de eventos.

## 8. Wireshark:

- Características:
  - Herramienta de análisis de tráfico de red.
  - Útil para el análisis de eventos de red y la identificación de patrones inusuales.

## 9. Recuva:

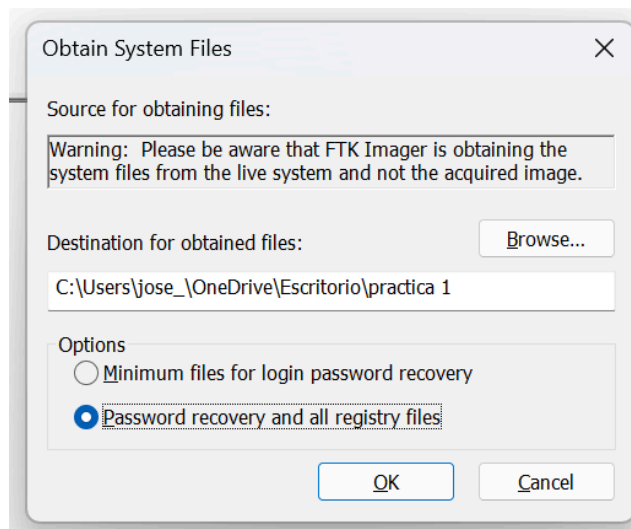
- Características:
  - Software de recuperación de datos.
  - Útil para la recuperación de archivos eliminados, incluyendo aquellos de la papelera de reciclaje.

## 10. Browser History Viewer:

- Características:
  - Herramienta para visualizar el historial de navegación de varios navegadores.
  - Permite analizar los sitios web visitados y las actividades de navegación.

## Parte B:

Para obtener los registros de Windows y otros datos relevantes, utilizaremos **FTK Imager**. Simplemente selecciona '**File > Obtain protected files**',. Una vez en la ventana emergente, elige el directorio donde deseas almacenar la información y selecciona la opción '**Password recovery and all registry files**'.



Así, los registros de Windows quedarán almacenados en nuestro directorio seleccionado.

Sincronizando > Jose - Personal > Escritorio > practica 1 >					
Ordenar Ver ...					
Nombre	Estado	Fecha de modificación	Tipo	Tamaño	
Users	✓	28/02/2024 15:25	Carpeta de archivos		
default	✓	27/02/2024 11:58	Archivo	2.560 KB	
SAM	✓	27/02/2024 11:58	Archivo	128 KB	
SECURITY	✓	27/02/2024 11:58	Archivo	64 KB	
software	✓	27/02/2024 11:58	Archivo	111.104 KB	
system	✓	27/02/2024 11:58	Archivo	21.760 KB	
userdiff	✓	28/01/2024 19:50	Archivo	8 KB	

Ahora revisaremos de manera detallada cada uno de los diversos artefactos de Windows que se encuentran enlistados a continuación, proporcionando comentarios descriptivos sobre la información que vamos obteniendo.

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

*Software\Microsoft\Windows NT\CurrentVersion*



InstallDate	RegDword	1706472048	
ProductName	RegSz	Windows 10 Pro	72-00-70-00-72...
ReleaseId	RegSz	2009	00-00
SoftwareType	RegSz	System	00-00-00-00-00...
UBR	RegDword	3155	
PathName	RegSz	C:\Windows	00-00-00-00-00...
PendingInstall	RegDword	0	
ProductId	RegSz	00330-80000-0...	D0-08-97-03
DigitalProductId	RegBinary	A4-00-00-00-03...	
DigitalProductId4	RegBinary	F8-04-00-00-04...	64-33-36-34
RegisteredOrganization	RegSz		
RegisteredOwner	RegSz	jose_016al@ou...	8F-00-10-C9-8F...
InstallTime	RegQword	133509456487...	45-ED-85-8C

Al convertir el valor de **'installTime'** a hexadecimal, podemos introducirlo en la herramienta Dcode para obtener la información de la zona horaria correspondiente

Value Input

Format
Hexadecimal (Big-Endian)

Value
1D49514A427A06AB

Decode

Time Zone

Name
(UTC+01:00) Bruselas, Copenhagen, Madrid, París

No Adjustment
Select

Date Output

Pattern
yyyy'-MM'-'dd HH':'mm':'ss'.ffffff K

Sample
2024-02-28 18:17:33.6306969 +01:00

Default

*System\ControlSet001\Control\ComputerName\ComputerName*

	Value Name	Value Type	Data	Value Slack
🔍	REG_C	REG_C	REG_C	REG_C
▶	(default)	RegSz	mnmsrvc	02-00-B0-00
	ComputerName	RegSz	JOSE	00-00

*System\ControlSet001\Control\TimeZoneInformation*

	Value Name	Value Data	Value Data Raw
🔍	REG_C	REG_C	REG_C
	Bias	-60	4294967236
	DaylightBias	-60	4294967236
	DaylightName	@tzres.dll,-301	@tzres.dll,-301
	DaylightStart	Month 3, week of month 5, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0	00-00-03-00-05-00-02-00-00-00-00-00-00-00-00
	StandardBias	0	0
	StandardName	@tzres.dll,-302	@tzres.dll,-302
	StandardStart	Month 10, week of month 5, day of week 0, Hours:Minutes:Seconds:Milliseconds 3:0:0:0	00-00-0A-00-05-00-03-00-00-00-00-00-00-00
▶	TimeZoneKeyName	Romance Standard Time	Romance Standard Time

En estas claves del registro, puedes encontrar información crítica sobre la configuración del sistema, como la versión del sistema operativo (ProductName), el nombre de la máquina (ComputerName) y la zona horaria (TimeZoneInformation). Estos detalles proporcionan información esencial sobre la configuración general del sistema.

- **Fecha de último acceso**

*System\ControlSet001\Control\FileSystem*

	NtfsQuotaNotifyRate	RegDword	3600
▶	RefsDisableLastAccessUpdate	RegDword	1
	RefsEnableDirCaseSensitivity	RegDword	3

Por defecto Windows no actualiza la fecha de último acceso, lo que impide saber cuando se accedio.

- Hora de apagado

*System\ControlSet001\Control\Windows*

CSDVersion	RegDword	0		
Directory	RegExpandSz	%SystemRoot%	00-00	
ErrorMode	RegDword	0		
FullProcessInformationSID	RegBinary	01-06-00-00-0...	00-00-00-00	
NoInteractiveServices	RegDword	1		
ShellErrorMode	RegDword	1		
SystemDirectory	RegExpandSz	%SystemRoot...		
ShutdownTime	RegBinary	02-8E-B0-D9-6...	24-22-26-00	

En esta clave del registro, se puede encontrar información relacionada con la configuración de Windows, incluida la hora de apagado del sistema. Analizar estos datos puede proporcionar información sobre los patrones de apagado del sistema y eventos relacionados con el ciclo de vida del sistema operativo.

- Interfaces de red

*System\ControlSet001\Services\Tcpip\Parameters\Interfaces\{GUID\_INTERFACE}*

buscar...				Buscar	F11: datos C:\ntls\ntlsdata.dat que para el cifrado, por el modo control de				
	# values	# subkeys	Last write timestamp		Value Name	Value Type	Data	Value Slack	Is
	=	=	=		#c	#c	#c	#c	
{88B74B96-6ED5-4B1F-A783-BED0ED01BC85}	4	0	2024-01-28 18:52:2		EnableDHCP	RegDword	1		
{8B37B34D-3A73-41C7-ABB3-142B52B48DEE}	4	0	2024-01-28 18:52:2		Domain	RegSz			
{91AE59C9-961F-4520-AC7F-42E8BF00A2F0}	4	0	2024-01-28 18:52:2		NameServer	RegSz			
{963899A0-37AD-4ADA-A55A-B4A2D42BA9CE}	4	0	2024-01-28 18:52:2		DhcpIPAddress	RegSz	192.168.1.136		
{99191955-9BE4-441C-9FBA-8CAECD59D69}	4	0	2024-01-28 18:52:2		DhcpSubnetMask	RegSz	255.255.255.0		
{9c566a8d-084b-4892-97a2-d0178e4f...	21	2	2024-02-28 10:01:5		DhcpServer	RegSz	192.168.1.1	20-80-50-01	
{A562DCC5-FA42-496C-9722-ACFC1CB6B894}	4	0	2024-01-28 18:52:2		Lease	RegDword	86400		
{AB1ED5CB-0196-4509-8BC0-B77CDFE435}	4	0	2024-01-28 18:52:2		LeaseObtainedTime	RegDword	1709114517		
{AE9B6102-5F85-44E6-9C19-0588877EBF49}	4	0	2024-01-28 18:52:2		T1	RegDword	1709157717		
{b16e7329-447c-4999-b65a-1ecf22f4b197}	21	0	2024-02-26 22:16:1		T2	RegDword	1709190117		
{B3170C1D-AD1D-4C5E-A7C8-644B86D6D8E}	4	0	2024-01-28 18:52:2		LeaseTerminatesTime	RegDword	1709200917		
{B6DD7910-C529-4AC5-AFAB-07169AF37331}	4	0	2024-01-28 18:52:2		AddressType	RegDword	0		
{baba64c9-7608-4d25-aa58-bc621811d625}	5	0	2024-01-28 18:52:2		IsServerNapAware	RegDword	0		
{8FF723AC-517C-469E-9563-9B27E745C5B5}	4	0	2024-01-28 18:52:2		DhcpConnForceBroadcastFlag	RegDword	0		
{C1472B47-0ACA-4E56-A0CB-C9653C4B59F7}	4	0	2024-01-28 18:52:2		DhcpNetworkHint	RegSz	4494749464...	00-00-00-00-...	
{C7CC45AF-3008-4F9C-80E9-4B7496596F11}	4	0	2024-01-28 18:52:2		DhcpInterfaceOptions	RegBinary	FC-00-00-00...	04-00-00-00	
{D0DE9BD2-C1B7-482C-913D-E9D52A4B7FF9}	4	0	2024-01-28 18:52:2		DhcpNameServer	RegSz	100.100.1.1 ...	72-76-65-72-...	
{D23AEF1F-9037-456F-A5EE-D51BF80E9B2}	4	0	2024-01-28 18:52:2		DhcpDefaultGateway	RegMultiSz	192.168.1.1	52-01	
{D59A4E46-8B47-4D8A-9D8B-6B0C8B2F6D25}	4	0	2024-01-28 18:52:2		DhcpSubnetMaskOpt	RegMultiSz	255.255.255.0	00-00-76-65-...	
{D725DF3-05B3-4A31-A69E-5E342D4C3B0A}	4	0	2024-01-28 18:52:2		DhcpGatewayHardware	RegBinary	C0-A8-01-01...	50-01-38-C2...	
{D7A8F1D7-8180-425D-BB28-C2A705FA54CB}	4	0	2024-01-28 18:52:2		DhcpGatewayHardwareCount	RegDword	1		
{D88B8460-B807-42F0-BFB8-1AFFA34DC428}	4	0	2024-01-28 18:52:2						
{DA12A474-B58E-4821-990A-A5A8647D401F}	4	0	2024-01-28 18:52:2						

En el registro, la ubicación mencionada guarda detalles específicos de las interfaces de red, como direcciones IP y configuraciones. Este registro es esencial para comprender la configuración de red del sistema, siendo valioso en investigaciones forenses relacionadas con actividades de red. La información está organizada por interfaz de red, identificada por un GUID único.

- **Histórico de redes**

*Software\Microsoft\Windows NT\CurrentVersion\NetworkList\*

	# values	# subkeys	Last write timestamp	First Net...	Network ...	Name Type	First Con...	Last Conn...	Managed	DNS Suffix	Gateway ...	Profile GUID
Image File Execution Options	0	56	2024-02-21 11:57:4	VPN 69	VPN 69	WWAN	2023-10-...	2023-10-...	<input type="checkbox"/>	<ninguno>		{0189F82D-8F5-1BFF51C4-0406}
IniFileMapping	0	5	2022-05-07 05:28:0	VPN 63	VPN 63	WWAN	2023-10-...	2023-10-...	<input type="checkbox"/>	<ninguno>		{02185C77-D480-4A1C-9E4F-389BA60CA19C}
KnownFunctionTableDlls	1	0	2024-01-28 18:49:0	VPN 44	VPN 44	WWAN	2023-10-...	2023-10-...	<input type="checkbox"/>	<ninguno>		{08E7344A-8718-4B3D-82FC-A75989FB8323}
KnownManagedDebuggingDlls	2	0	2024-01-28 18:49:0	VPN 73	VPN 73	WWAN	2023-10-...	2023-10-...	<input type="checkbox"/>	<ninguno>		{09067DF5-5D73-45E1-BA11-8D5681044D287}
LanguagePack	1	2	2022-05-07 05:28:0	VPN 12	VPN 12	WWAN	2023-10-...	2023-10-...	<input type="checkbox"/>	<ninguno>		{09392ACB-C8DD-48B6-8118-EDD098BB4133}
LicensingDiag	1	0	2022-05-07 05:28:0	VPN 5	VPN 5	WWAN	2023-10-...	2023-10-...	<input type="checkbox"/>	<ninguno>		{1627694F-760B-4255-8490-61F510EC5FD4}
MCI Extensions	50	0	2022-05-07 05:28:0	VPN 36	VPN 36	WWAN	2023-10-...	2023-10-...	<input type="checkbox"/>	<ninguno>		{1A510FE5-38E4-45AC-9CB9-1489990DDAD1}
MCI32	5	0	2022-05-07 05:28:0	VPN 48	VPN 48	WWAN	2023-10-...	2023-10-...	<input type="checkbox"/>	<ninguno>		{1B3A51EF-08ED-4956-ACE9-88813DF54D1D}
MiniDumpAuxiliaryDlls	5	0	2024-01-28 18:49:0	VPN 51	VPN 51	WWAN	2023-10-...	2023-10-...	<input type="checkbox"/>	<ninguno>		{1CAEAA7D-3380-4309-B806-A4059340...
MsiCorruptedFileRecovery	0	1	2022-05-07 05:28:0									
Multimedia	0	1	2022-05-07 05:28:0									
NaAuth	0	1	2022-05-07 05:28:0									
NetworkCards	0	3	2024-02-08 17:45:0									
<b>NetworkList</b>	<b>3</b>	<b>7</b>	<b>2024-02-27 10:58:3</b>									
NoIcmpModeImes	0	2	2022-05-07 05:28:0									
Notifications	163	1	2024-02-28 10:02:0									
NowPlayingSessionManager	2	0	2024-01-28 18:49:0									
NTVdm64	0	8	2022-05-07 05:28:0									
OEM	0	0	2022-05-07 05:28:0									
OpenGLDrivers	0	0	2022-05-07 05:28:0									
PasswordLess	0	1	2024-01-28 18:52:2									
PeerDist	0	9	2022-05-07 10:28:5									
PeerNet	0	1	2022-05-07 05:28:0									
Perfib	6	3	2024-02-27 11:04:2									
PerfHwIdStorage	0	14	2022-05-07 10:28:5									
Ports	11	0	2024-01-28 18:52:1									

En esta ubicación del registro, se almacena información relacionada con la configuración de red. Puedes encontrar detalles sobre las redes a las que se ha conectado el sistema, su tipo (pública, privada o de trabajo), y otra información relacionada con la conectividad de red.

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

En esta clave específica, llamada "Cache", se guarda información en caché sobre las redes a las que se ha conectado el sistema. Puedes encontrar registros de conexiones pasadas, incluyendo detalles como direcciones IP, nombres de red, y perfiles de seguridad asociados. Este historial es útil para comprender la actividad de red pasada en el sistema.

- **Cuándo se conectó a una red**

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

	Value Name	Value Type	Data	Value Slack	Is Deleted
▼	RegDWord	RegDWord	RegDWord	RegDWord	
▶	ProfileName	RegSz	VPN 69	00-00-00-00-0...	
	Description	RegSz	VPN	00-12-18-00	
	Managed	RegDword	0		
	Category	RegDword	0		
	DateCreated	RegBinary	E7-07-0A-00-...	73-67-43-04	
	NameType	RegDword	23		
	DateLastConnected	RegBinary	E7-07-0A-00-...	08-67-43-04	

Guarda información sobre perfiles de red, incluyendo detalles sobre cuándo se conectó a una red específica. Esta ubicación es útil para rastrear patrones de conexión y establecer la línea de tiempo de actividades de red en el sistema.

- **Carpetas compartidas**

*System\ControlSet001\Services\lanmanserver\Shares\*

	# values	# subkeys	Last write timestamp	Value Name	Value Type	Data	Value Slack	Is Deleted
	=	=	=	▼	=	=	=	=
Linkage	3	0	2024-02-08 20:13:01					
Parameters	9	1	2024-02-27 10:58:41					
ShareProviders	0	0	2024-01-28 19:57:00					
Shares	0	1	2024-01-28 18:52:21					
Security	0	0	2024-01-28 18:52:21					

Guarda información sobre carpetas compartidas en Windows, incluyendo detalles de permisos y configuraciones.

- **Programas de inicio**

*NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run*

Value Name	Value Type	Data	Value Slack
▼	RegDWord	RegDWord	RegDWord
▶	RegSz	%C:\...	00-0...
	RegSz	%C:\...	00-0...
	RegSz	%C:\...	00-0...
	RegSz	C:\...	00-0...

Almacena programas específicos que se ejecutan automáticamente al iniciar sesión para un usuario específico. Estos programas son configurados por el usuario para iniciar junto con su sesión.

*NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\RunOnce*

Contiene programas que se ejecutan solo una vez al iniciar sesión para un usuario en particular. Después de ejecutarse una vez, la entrada se elimina automáticamente.

*Software\Microsoft\Windows\CurrentVersion\Runonce*

Almacena programas que se ejecutan una sola vez durante el inicio del sistema. Estas entradas se eliminan automáticamente después de la ejecución.

*Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run*

	REG	REG	REG	REG
ForceActiveDesktopOn	RegDword	0		
NoActiveDesktop	RegDword	1		
NoActiveDesktopChanges	RegDword	1		
NoDriveTypeAutorun	RegDword	158		

Contiene programas configurados mediante políticas del sistema que se ejecutan al iniciar sesión. Estas políticas son establecidas por administradores y pueden controlar el comportamiento del sistema.

*Software\Microsoft\Windows\CurrentVersion\Run*

	REG	REG	REG	REG
SecurityHealth	RegExpandSz	%windir%\...	00-00-00-00	
RtkAudUService	RegSz	"C:\WINDO...	13-39-25-00	
BraveVpnWireguardService	RegSz	"C:\Progra...	AE-03-61-5...	

Almacena programas que se ejecutan automáticamente al iniciar sesión a nivel del sistema. Estas entradas afectan a todos los usuarios del sistema y son utilizadas para configurar aplicaciones o servicios que deben ejecutarse en cada inicio de sesión.

- **Búsquedas en la barra de búsqueda**

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

Almacena consultas de búsqueda realizadas en la barra de búsqueda de Windows. Esta información puede revelar términos de búsqueda recientes y patrones de búsqueda del usuario.

- **Rutas en Inicio o Explorer**

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

Contiene rutas de archivos o carpetas que el usuario ha escrito o utilizado recientemente en el explorador de archivos. Proporciona información sobre las ubicaciones accedidas con frecuencia.

- **Documentos recientes**

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

	Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On
🔍	REG	REG	REG	REG	=	=
▶	RecentDocs	1	Descargas	Descargas.lnk	0	2024-02-27 1..
	RecentDocs	41	scriptFuerzaBruta - cajero.jmx	scriptFuerzaBruta - cajero.jmx.lnk	1	
	RecentDocs	46	Carpeta-Compartida	Carpeta-Compartida (10).lnk	2	
	RecentDocs	62	1896.dmp	1896.dmp.lnk	3	
	RecentDocs	0	&suppressAnimations=false&showFooter=true&allowPageNavigation=true&edgeGestureOffset=0&inputAnimationSourceId=0&inputAnimationProviderId=0	ms-actioncentercontrolcenter-&suppressAnimations=false&showFooter=true&allowPageNavigation=true&edgeGestureOffset=0&inputAnimationSourceId=0&inputAnimationProviderId=0 (30).lnk	4	
	RecentDocs	28	scriptFuerzaBruta_foro.jmx	scriptFuerzaBruta_foro.jmx.lnk	5	
	RecentDocs	145	cajero	cajero.lnk	6	
	RecentDocs	88	index.php	index.lnk	7	

Guarda accesos recientes a documentos. Ofrece una lista de los archivos más recientes abiertos por el usuario, lo que puede indicar actividades y proyectos recientes.

- Documentos ofimáticos recientes

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

Buscar...				Arrastre una columna aquí para agrupar por dicha columna			
	# values	# subkeys	Last write timestamp	Value Name	Last Opened	Last Closed	File Name
Access	0	1	2024-01-28 19:58:0	FOLDERID_Desktop			C:\Users\jose_\OneDrive\Escri
Common	8	30	2024-02-27 19:02:5	FOLDERID_Desktop			C:\Users\jose_\OneDrive\Escri
Excel	8	7	2024-01-28 19:58:0	FOLDERID_Desktop			C:\Users\jose_\OneDrive\Escri
MAPI	0	0	2024-01-28 19:58:0	Item 1	2024-01-30 21:15:05	2024-01-30 22:45:02	C:\Users\jose_\Downloads\Eje
MS Project	0	1	2024-01-28 19:58:0	Item 2	2024-01-30 15:14:59	2024-01-30 20:30:47	C:\Users\jose_\Downloads\Pr
Outlook	4	8	2024-01-28 19:58:0	Item 3	2024-01-19 16:38:22	2024-01-28 19:58:02	C:\Users\jose_\Downloads\Mo
PowerPoint	2	9	2024-01-28 19:58:0	Item 4	2024-01-19 16:32:36	2024-01-28 19:58:02	C:\Users\jose_\Downloads\Mo
User Settings	0	27	2024-01-28 19:58:0	Item 5	2024-01-18 18:56:43	2024-01-28 19:58:02	C:\Users\jose_\Downloads\Pr
WEF	1	2	2024-01-28 19:58:0	Item 6	2023-11-27 20:04:20		C:\Users\jose_\Downloads\of
Word	2	10	2024-01-30 22:45:0	Item 7	2023-11-27 20:03:06		C:\Users\jose_\Downloads\of
Data	2	0	2024-01-30 22:45:0	Item 8	2023-11-27 19:51:34		C:\Users\jose_\Downloads\of
DocumentTemplateCache	3	2	2024-01-30 22:33:2	Item 9	2023-11-14 09:43:44		D:\Normativa.docx
File MRU	2	0	2024-01-28 19:58:0	Item 10	2023-11-12 20:51:36		C:\Users\jose_\OneDrive\Escri
Options	21	0	2024-01-29 20:23:5				
Place MRU	2	0	2024-01-28 19:58:0				
Reading Locations	0	5	2024-01-29 19:46:1				
Recent Templates	1	2	2024-01-28 19:58:0				
Security	0	2	2024-01-28 19:58:0				
User MRU	1	1	2024-01-28 19:58:0				
LiveId_3DA6B6C9C6B3A2EDA5410D3BDDA...	0	2	2024-01-28 19:58:0				
File MRU	12	0	2024-01-30 21:15:0				
Place MRU	6	0	2024-01-30 21:15:0				

Almacena la lista de documentos ofimáticos recientes abiertos con Microsoft Office. Revela archivos recientes utilizados en aplicaciones específicas de Office.

- Posición de lectura sobre el último documento abierto

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

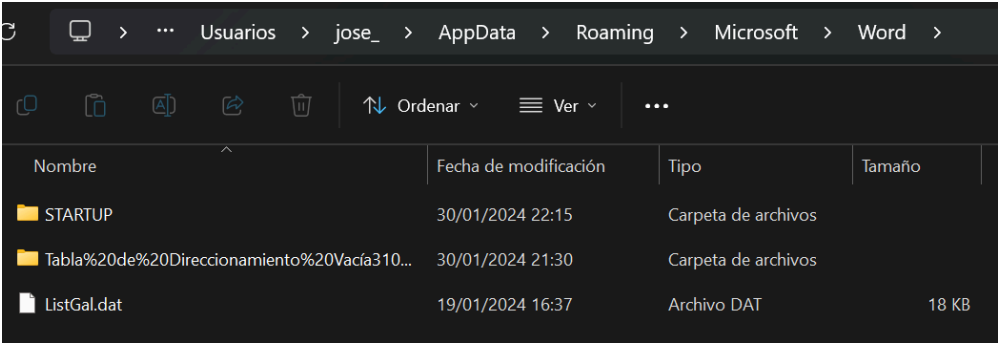
buscar...				Arrastre una columna aquí para agrupar por dicha columna				
	# values	# subkeys	Last write timestamp	Value Name	Value Type	Data	Value Slack	Is Deleted
Access	0	1	2024-01-28 19:58:0	File Path	RegSz	C:\Users\jo...	00-05-12-00...	<input type="checkbox"/>
Common	8	30	2024-02-27 19:02:5	Datetime	RegSz	2024-01-19...	00-00	<input type="checkbox"/>
Excel	8	7	2024-01-28 19:58:0	Position	RegSz	1053908451...	00-00-00-00	<input type="checkbox"/>
MAPI	0	0	2024-01-28 19:58:0					
MS Project	0	1	2024-01-28 19:58:0					
Outlook	4	8	2024-01-28 19:58:0					
PowerPoint	2	9	2024-01-28 19:58:0					
User Settings	0	27	2024-01-28 19:58:0					
WEF	1	2	2024-01-28 19:58:0					
Word	2	10	2024-01-30 22:45:0					
Data	2	0	2024-01-30 22:45:0					
DocumentTemplateCache	3	2	2024-01-30 22:33:2					
File MRU	2	0	2024-01-28 19:58:0					
Options	21	0	2024-01-29 20:23:5					
Place MRU	2	0	2024-01-28 19:58:0					
Reading Locations	0	5	2024-01-29 19:46:1					
Document 0	3	0	2024-01-28 19:58:0					
Document 1	3	0	2024-01-28 19:58:0					
Document 10	3	0	2024-01-28 19:58:0					
Document 11	3	0	2024-01-30 20:30:4					
Document 2	3	0	2024-01-30 22:45:0					

Guarda la posición de lectura (ubicación y formato) del último documento abierto en Microsoft Word. Permite retomar la lectura desde la última posición.



- **Ficheros ofimáticos autoguardados**

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



Contiene archivos autoguardados de las aplicaciones de Microsoft Office (Excel, Word, Powerpoint). Estos archivos sirven como copias de respaldo en caso de cierre inesperado o pérdida de datos.

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

*NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU*

a buscar...				Arrastre una columna aquí para agrupar por dicha columna				
	# values	# subkeys	Last write timestamp	Extension	Value Name	MrU Position	Absolute Path	Opened On
Advanced	36	0	2024-02-28 10:02:0	*	10	0	Downloads\scriptFuerzaBruta - cajero.jmx	2024-02-27 19:16:15
AppContract	0	2	2024-01-28 19:57:4	dmp	0	0	My Computer\Virtual Machines\Carpeta-Compartida\1896.dmp	2024-02-27 18:08:05
AutoplayHandlers	1	5	2024-01-28 19:58:0	htm	0	0	OneDrive\Escritorio\descarga.htm	2024-02-06 17:20:47
BamThrottling	0	0	2024-01-28 20:01:2	iso	2	0	E:\Windows\Windows 10 x32 x64.iso	2024-02-11 22:28:22
BannerStore	0	1	2024-02-28 10:02:3	jmx	0	0	Downloads\scriptFuerzaBruta - cajero.jmx	2024-02-27 19:16:15
BitBucket	1	1	2024-01-28 19:59:1	jpg	4	0	Downloads\descarga.jpg	2024-02-07 18:02:28
CabinetState	2	0	2024-01-28 19:59:1	ova	3	0	OneDrive\Escritorio\Windows 10.ova	2024-02-12 09:26:12
CIDOpen	0	1	2024-01-29 22:51:3	pdf	6	0	Downloads\Practica 1 - Jose Almirón.pdf	2024-02-14 12:55:18
CIDSave	0	1	2024-01-29 16:30:1	pkt	2	0	OneDrive\Escritorio\	2024-02-26 18:31:24
CLSID	0	5	2024-01-28 19:58:0	png	15	0	Downloads\unified.png	2024-02-07 18:10:17
ComDlg32	0	3	2024-01-29 16:30:2	rar	2	0	Downloads\Enrutamiento con VLAN - Jose Almirón.rar	2024-02-26 23:36:05
CIDSizeMRU	13	0	2024-02-28 13:31:0	sql	0	0	Downloads\forum.sql	2024-02-20 13:00:51
LastVisitedPidlMRU	10	0	2024-02-27 19:16:1	txt	0	0	OneDrive\Escritorio\	2024-02-13 18:06:41
OpenSavePidlMRU	0	14	2024-02-27 19:16:1					
Desktop	0	1	2024-01-28 19:58:0					
Discardable	0	1	2024-01-28 20:01:0					
ExtractionWizard	1	0	2024-02-20 16:17:2					
FeatureUsage	1	4	2024-01-28 19:59:2					
FileExts	0	257	2024-02-27 18:08:0					
HideDesktopIcons	0	1	2024-01-28 19:58:0					

Almacena registros de archivos que han sido abiertos o guardados dentro de ventanas de Windows. Proporciona información sobre los archivos utilizados recientemente.

- Últimos comandos ejecutados

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

Value Name	Mru Position	Executable
R[C	=	R[C
b	0	regedit
a	1	cmd
e	2	prefetch
d	3	%temp%
c	4	msinfo32

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

Guarda registros de los últimos comandos ejecutados por el usuario. Puede incluir comandos ejecutados en el Explorador de Windows.

- UserAssistKey: Programas ejecutados desde el Escritorio

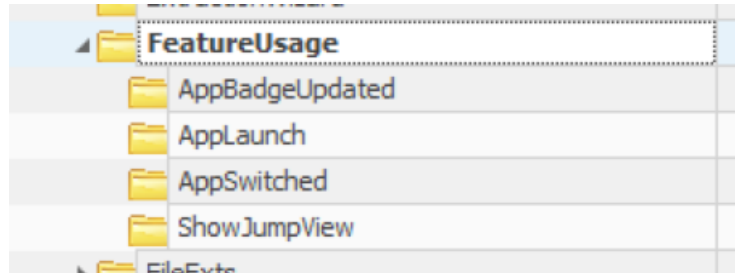
*NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{GUID}\Count*

	# values	# subkeys	Last write timestamp	Program Name	Run Counter	Focus Count	Focus Time	Last Executed
Streams	0	2	2024-02-20 11:27:4	UEME_CTLQUACount:c tor	0	0	0d, 0h, 00m, 00s	
StuckRects3	1	0	2024-01-28 19:59:2	Microsoft.Getstarted_ 8wekyb3d8bbwe!App	0	0	0d, 0h, 00m, 00s	2023-09-04 10:08:09
TabletMode	1	0	2024-01-28 19:57:4	UEME_CTLSESSION	222	1911	1d, 14h, 57m, 33s	
Taskband	5	1	2024-02-05 10:53:3	Microsoft.WindowsFee dbackHub_8wekyb3d8 bbwe!App	0	0	0d, 0h, 00m, 00s	2023-09-04 10:08:09
TypedPaths	0	0	2024-01-28 20:03:1	Microsoft.WindowsMa ps_8wekyb3d8bbwe!A pp	0	0	0d, 0h, 00m, 00s	2023-09-04 10:08:09
User Shell Folders	27	0	2024-01-28 20:01:1	Microsoft.People_8we kyb3d8bbwe!x4c7a3b 7dy2188y46d4ya362y 19ac5a5805e5x	0	0	0d, 0h, 00m, 00s	2023-09-04 10:08:09
User Assist	0	9	2024-01-28 19:57:4	Microsoft.MicrosoftSti ckyNotes_8wekyb3d8 bbwe!App	0	0	0d, 0h, 00m, 00s	2023-09-04 10:08:09
{9E04CAB2-CC14-11Df-8B8C-A2F1DED720...}	1	1	2024-01-28 19:57:4	Microsoft.WindowsCal culator_8wekyb3d8bb we!App	0	0	0d, 0h, 00m, 00s	2023-09-04 10:08:09
Count	1	0	2024-02-15 18:58:1	Microsoft.Paint_8weky b3d8bbwe!App	0	0	0d, 0h, 00m, 00s	2023-09-04 10:08:09
{A3D53349-6E61-4557-8FC7-0028EDCEEB...}	1	1	2024-01-28 19:57:4	Microsoft.WindowsNot epad_8wekyb3d8bbwe !App	17	117	0d, 1h, 10m, 01s	2024-02-26 20:23:44
Count	1	0	2024-02-15 18:58:1	MicrosoftTeams_8wek yb3d8bbwe!MicrosoftT eams	0	0	0d, 0h, 00m, 00s	2023-09-04 10:11:13
{B267E3AD-A825-4A09-82B9-EEC22AA3B8...}	1	1	2024-01-28 19:57:4	MicrosoftWindows.Cle nt.CBS_cw5n1h2txy	0	46	0d, 0h, 07m, 11s	
Count	0	0	2024-01-28 19:57:4					
{BC848336-4DD0-48FF-8B0B-D3190DACB3...}	1	1	2024-01-28 19:57:4					
Count	1	0	2024-02-15 18:58:1					
{CAA59E3C-4792-41A5-9909-6A6A8D3249...}	1	1	2024-01-28 19:57:4					
Count	1	0	2024-02-15 18:58:1					
{CEBFF5CD-ACE2-4F4F-9178-9926F41749...}	1	1	2024-01-28 19:57:4					
Count	240	0	2024-02-28 14:21:5					
{F2A1CB5A-E3CC-4A2E-AF9D-505A7009D...}	1	1	2024-01-28 19:57:4					
{F4E57C4B-2036-45F0-A9AB-443BCFE33D...}	1	1	2024-01-28 19:57:4					
{FA99DFC7-6AC2-453A-A5E2-5E2AFF4507...}	1	1	2024-01-28 19:57:4					
VirtualDesktops	3	1	2024-02-28 10:02:0					
VisualEffects	0	19	2024-01-28 20:01:2					

Almacena información sobre programas ejecutados desde el Escritorio. Proporciona detalles sobre las aplicaciones utilizadas y la frecuencia de ejecución.

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

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



Guarda eventos relacionados con el uso de la barra de tareas, proporcionando información sobre las funciones y características de la interfaz de usuario que han sido utilizadas.

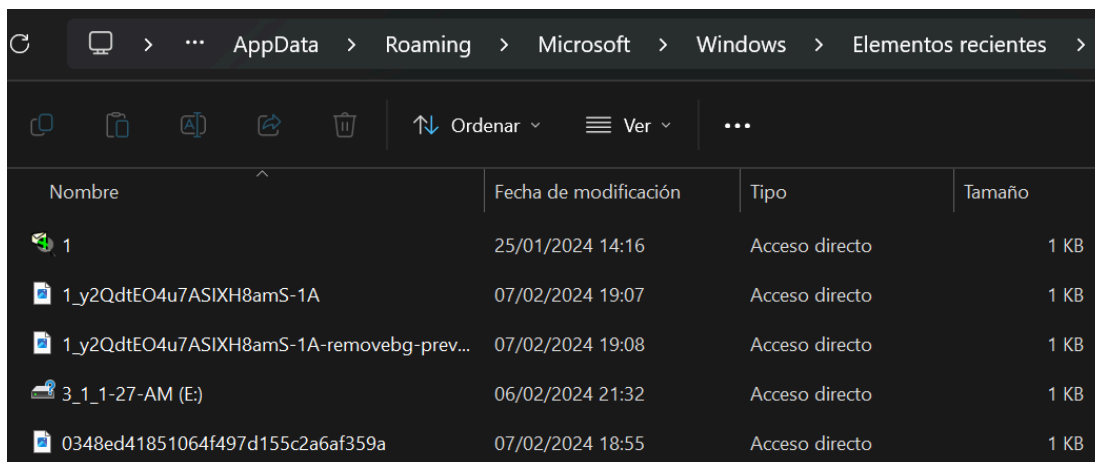
- **Aplicaciones recientes**

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

Almacena información sobre aplicaciones utilizadas recientemente, proporcionando una lista de las aplicaciones abiertas recientemente en el sistema.

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

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



Esta carpeta almacena accesos directos (enlaces) a documentos recientes en el sistema. Estos enlaces pueden ser creados automáticamente por el sistema operativo o por aplicaciones cuando se accede a un archivo. Proporciona una lista fácilmente accesible de documentos, imágenes o aplicaciones a los que el usuario ha accedido recientemente.

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

*C:\Users\...\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations*

*C:\Users\...\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations*

Contienen información sobre destinos automáticos y personalizados en las listas de salto (Jump Lists). Los destinos automáticos se generan automáticamente por el sistema, mientras que los personalizados son configurados por el usuario.

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

*USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags*

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

*NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU*

a texto a buscar...				Buscar
ie	# values	# subkeys	Last write timestan	
ie	==	==	==	^
<ul style="list-style-type: none"> <li>iTunes.ipa</li> <li>JavaPlugin.114012</li> <li>Inkfile</li> <li>Local Settings</li> <li>ImmutableMUICache</li> <li>MrtCache</li> <li>MUICache</li> <li>Software               <ul style="list-style-type: none"> <li>Microsoft                   <ul style="list-style-type: none"> <li>Windows                       <ul style="list-style-type: none"> <li>CurrentVersion</li> <li>Shell                           <ul style="list-style-type: none"> <li>BagMRU</li> <li>Bags</li> <li>MUICache</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> <li>Magnet</li> </ul>	0	2	2024-01-28 19	
	0	1	2024-02-20 15	
	0	1	2024-01-28 19	
	0	4	2024-01-28 20	
	0	1	2024-01-28 20	
	0	91	2024-02-28 10	
	0	1	2024-02-27 10	
	0	1	2024-01-28 19	
	0	1	2024-01-28 19	
	0	2	2024-01-28 19	
	0	5	2024-01-28 20	
	0	3	2024-01-28 20	
	31	28	2024-02-27 19	
	0	477	2024-02-27 12	
	92	0	2024-02-27 10	
	3	2	2024-01-28 19	

Arrastre una columna aquí para agrupar por dicha columna				
Value Name	Value Type	Data	Value Slack	Is Deleted
NodeSlots	RegBinary	02-02-02-02-02-0...		<input type="checkbox"/>
MRUListEx	RegBinary	01-00-00-00-04-0...		<input type="checkbox"/>
0	RegBinary	14-00-1F-40-0E-3...	00-00-00-00-00-00	<input type="checkbox"/>
1	RegBinary	3A-00-1F-00-05-3...		<input type="checkbox"/>
2	RegBinary	3A-00-1F-46-47-1...		<input type="checkbox"/>
3	RegBinary	3A-00-1F-41-66-5...		<input type="checkbox"/>
4	RegBinary	14-00-1F-50-E0-4...	00-00-00-00-00-00	<input type="checkbox"/>
5	RegBinary	14-00-1F-70-68-0...	00-00-00-00-00-00	<input type="checkbox"/>
6	RegBinary	B5-02-1F-00-65-0...	00-00-00-00-00-00	<input type="checkbox"/>
7	RegBinary	DF-02-1F-00-65-0...	00-00-00-00-00-00	<input type="checkbox"/>
8	RegBinary	55-00-1F-00-2F-0...	00-00-00-00-00-00	<input type="checkbox"/>
9	RegBinary	14-00-1F-58-0D-1...	00-00-00-00-00-00	<input type="checkbox"/>
10	RegBinary	92-00-31-00-00-0...		<input type="checkbox"/>
11	RegBinary	84-00-31-00-00-0...	00-00-00-00-00-00	<input type="checkbox"/>
12	RegBinary	7C-00-31-00-00-0...	00-00-00-00-00-00	<input type="checkbox"/>

Almacenan información sobre la ubicación y el tiempo de acceso a carpetas. Los Shellbags registran detalles como la posición y configuración de ventanas en el Explorador de archivos.

- **Dispositivos MTP**

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

Contiene información sobre dispositivos MTP (Protocolo de Transferencia de Medios) conectados al sistema. Puede incluir detalles sobre la interacción con dispositivos multimedia.

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

SYSTEM\ControlSet001\Enum\USBSTOR

me	# values	# subkeys	Last write timestamp	Time...	Manufa...	Title	Version	Disk Id	Serial N...	Device ...	Installed	First In...	Last Co...	Last Rem...
HTREE	0	1	2024-01-28 19	2024-0...	Ven_Gen	Prod_Flas	Rev_8.07	{fcc1ffcd-7b04-11ee-9ce6-e4814550defb}	7B64A9D980	Generic Flash Disk USB Device	2024-0...	2024-0...	2024-0...	2024-02-...
PCI	0	14	2024-01-28 19	2024-0...	Ven_USB	Prod_Flas	Rev_1100	{c486470f-c414-11ee-9d11-983b9f9a9a34}	SCY000000002714380	USB Flash Disk USB Device	2024-0...	2024-0...	2024-0...	2024-02-...
ROOT	0	20	2024-02-04 11	2024-0...	Ven_Ven	Prod_Pro	Rev_2.00	{705018e7-846b-11ee-9ced-adcd9b59ea59}	524656112437034915280	VendorCo ProductC ode USB Device	2024-0...	2024-0...	2024-0...	2024-02-...
SCSI	0	1	2024-01-28 19											
STORAGE	0	2	2024-01-28 20											
SW	0	1	2024-01-28 20											
SWD	0	8	2024-02-03 12											
UEFI	0	1	2024-01-28 19											
USB	0	17	2024-02-08 17											
USBSTOR	0	3	2024-02-06 20											
Disk\Ven_Generic&Prod_Flash_Disk&Rev_8.07	0	1	2024-02-06 16											
7B64A9D980	12	2	2024-02-06 16											
Device Parameters	0	2	2024-02-06 16											
Properties	0	5	2024-02-06 16											
Disk\Ven_USB&Prod_Flash_Disk&Rev_1100	0	1	2024-02-06 20											
Disk\Ven_VendorCo&Prod_ProductCode&Rev_2.00	0	1	2024-02-03 12											
{5d624f94-8850-40c3-a3fa-a4fd2080baf3}	0	1	2024-01-28 19											

Registra información sobre dispositivos de almacenamiento USB, incluyendo identificadores de fabricante (VID) y de producto (PID). Puede ser útil para rastrear la conexión de dispositivos USB al sistema.

- **Nombres de volúmenes USB**

SOFTWARE\Microsoft\Windows Portable Devices\Devices

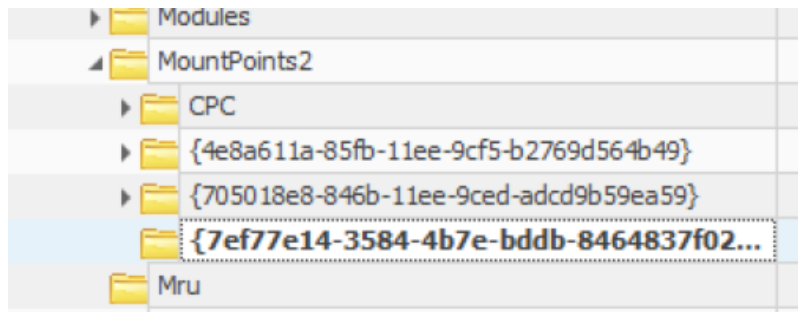
name	# values	# subkeys	Last write timestamp	Value Name	Value Type	Data	Value Slack	Is Delet
Windows NT	0	1	2022-05-07 05	FriendlyName	RegSz	E:\	00-00-00-00	
Windows Photo Viewer	0	1	2022-05-07 10					
Windows Portable Devices	0	2	2022-05-07 10					
Devices	0	8	2024-02-06 20					
SWD#WPDBUSENUM#_??_USBSTOR#DISK&VEN...	1	0	2024-01-28 18					
SWD#WPDBUSENUM#_??_USBSTOR#DISK&VEN_VEND...	1	0	2024-01-28 18					
SWD#WPDBUSENUM#_??_USBSTOR#DISK&VEN_VEND...	1	0	2024-01-28 18					

Almacena información sobre los nombres de volúmenes asignados a dispositivos USB. Proporciona detalles sobre los dispositivos reconocidos como unidades portátiles.

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

System\MountedDevices

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



Proporcionan información sobre los dispositivos montados, incluyendo unidades USB. Puedes rastrear la interacción con USB y la asignación de letras de unidad.

- **Número de serie de volumen lógico**

*Software\Microsoft\Windows NT\CurrentVersion\EMDMgmt*

```
Microsoft Windows [Versión 10.0.22631.3155]
(c) Microsoft Corporation. Todos los derechos reservados.

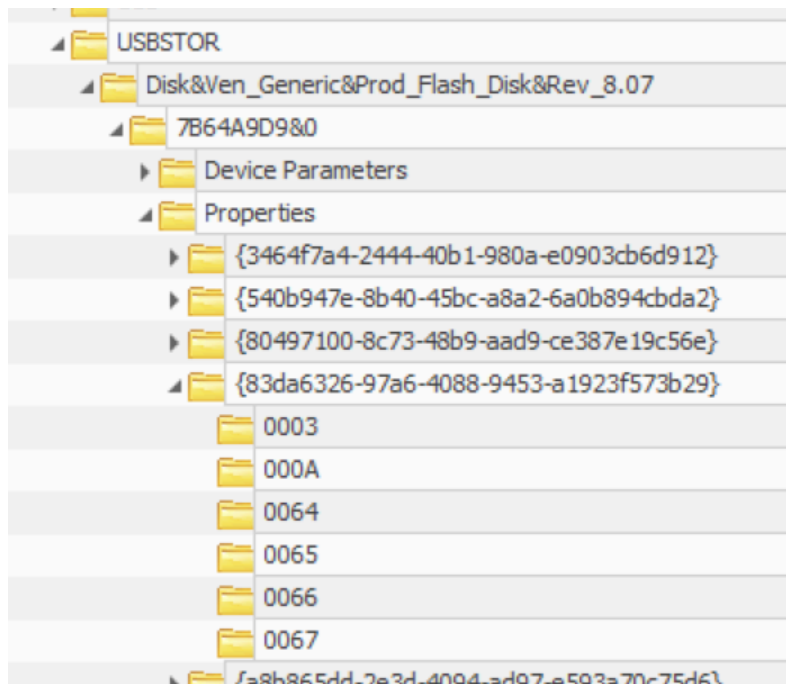
C:\Users\jose_>vol
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: CC77-1A2F

C:\Users\jose_>|
```

Contiene información sobre el número de serie del volumen lógico. Útil para identificar y rastrear dispositivos de almacenamiento.

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

*System\ControlSet001\Enum\USBSTOR\{VEN\_PROD\_VERSION}\{USB  
serial}\Properties\{83da6326- 97a6-4088-9453-a1923f573b29}\*



*C:\Windows\inf\setupapi.dev.log*

Registra la primera y última conexión de un dispositivo USB. La ruta en setupapi.dev.log proporciona detalles adicionales.

- **Base de datos Cortana, si existiese, en versiones anteriores a Windows**

*10.0.17763.55 (Sqlite studio)*

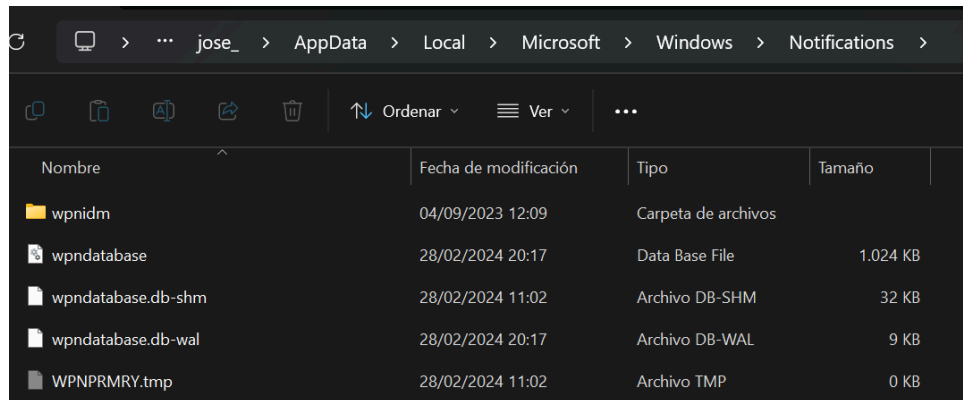
*\Users\user\_name\AppData\Local\Packages\Microsoft.Windows.Cortana\_xxxx\LocalState\E*

*SEDatabase\_CortanaCoreInstance\CortanaCireDb.dat*

Contiene datos de la base de datos Cortana. En versiones anteriores a Windows 10.0.17763.55, se puede examinar con Sqlite Studio para obtener información sobre las actividades de Cortana.

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

*\Users\{user\_name}\AppData\Local\Microsoft\Windows\Notifications\wpndatabase.db*

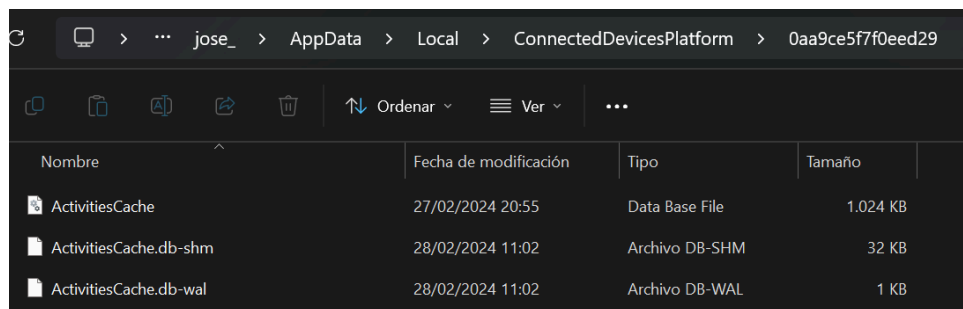


Nombre	Fecha de modificación	Tipo	Tamaño
wpnidm	04/09/2023 12:09	Carpeta de archivos	
wpndatabase	28/02/2024 20:17	Data Base File	1.024 KB
wpndatabase.db-shm	28/02/2024 11:02	Archivo DB-SHM	32 KB
wpndatabase.db-wal	28/02/2024 20:17	Archivo DB-WAL	9 KB
WPNPRMRY.tmp	28/02/2024 11:02	Archivo TMP	0 KB

Contiene datos sobre notificaciones de Windows. Puede examinarse con Sqlite Studio para obtener detalles sobre las notificaciones recibidas.

- **Timeline (Windows TimelineParser)**

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



Nombre	Fecha de modificación	Tipo	Tamaño
ActivitiesCache	27/02/2024 20:55	Data Base File	1.024 KB
ActivitiesCache.db-shm	28/02/2024 11:02	Archivo DB-SHM	32 KB
ActivitiesCache.db-wal	28/02/2024 11:02	Archivo DB-WAL	1 KB

Contiene datos de la línea temporal (Timeline) de Windows. Puede analizarse con Windows TimelineParser para visualizar las actividades del usuario a lo largo del tiempo.

- **Windows Store (SQLite Studio)**

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

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

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

Contiene información sobre las aplicaciones de la Tienda Windows, incluyendo su estado, instalación y desinstalación. Puede analizarse con SQLite Studio.

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



### Ficheros "thumbs.db"

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

Almacenan miniaturas (thumbnails) y caché de miniaturas generadas por el sistema. Los "thumbs.db" son archivos de base de datos que contienen información sobre miniaturas de imágenes.

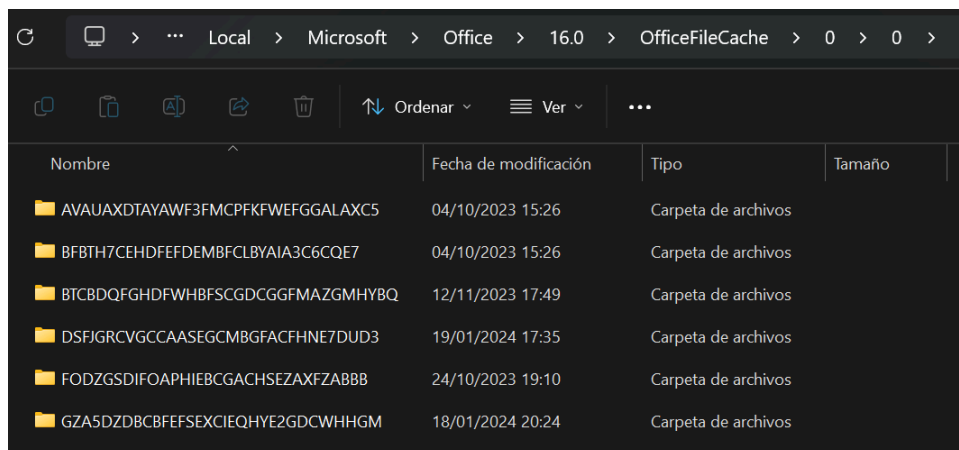
- **Papelera de reciclaje**

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

Contiene archivos eliminados. Puede ser examinado con herramientas como Rifiuti para recuperar información sobre archivos eliminados.

- **OfficeFileCache (OfficeFileCacheParser)**

*\Users\...\AppData\Local\Microsoft\Office\...\OfficeFileCache*



Nombre	Fecha de modificación	Tipo	Tamaño
AVAUAXDTAYAWF3FMC...FWEFGGALAXC5	04/10/2023 15:26	Carpeta de archivos	
BFBTH7CEHDFEFDEMBFCLBYAIA3C6CQE7	04/10/2023 15:26	Carpeta de archivos	
BTCBDQFGHDFWHBFSCGDCGGFMAZGMHYBQ	12/11/2023 17:49	Carpeta de archivos	
DSFJGRCVGCCAASEGCMBGFACFHNE7DUD3	19/01/2024 17:35	Carpeta de archivos	
FODZGSDIFOAPHIEBCGACHSEZAXFZABBB	24/10/2023 19:10	Carpeta de archivos	
GZA5DZDBCBEFSEXCIEQHYE2GDCWHHGM	18/01/2024 20:24	Carpeta de archivos	

Almacena archivos temporales de caché utilizados por Microsoft Office. Puede analizarse con OfficeFileCacheParser.

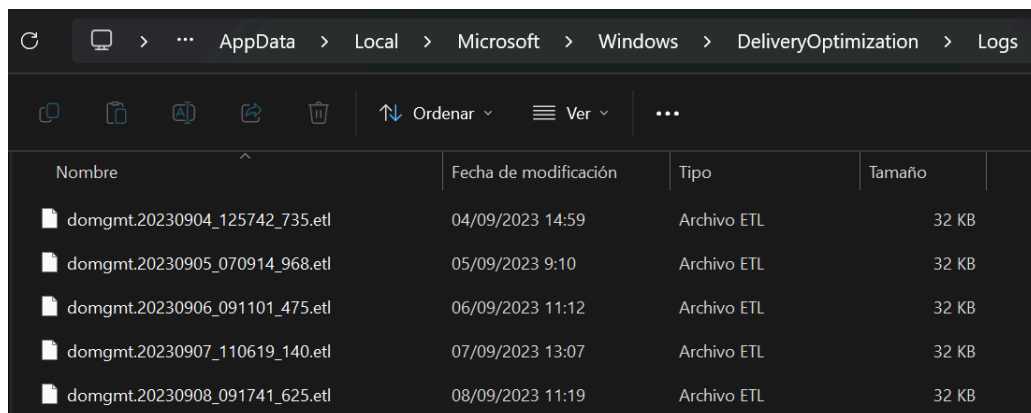
- **OfficeBackstage (OfficeBackstageParser)**

*\Users\...\AppData\Local\Microsoft\Office\16.0\BackstageinAppNavCache*

Contiene información sobre el historial de navegación en el menú Backstage de Microsoft Office. Puede analizarse con OfficeBackstageParser.

- **IP Pública (ETLParser)**

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

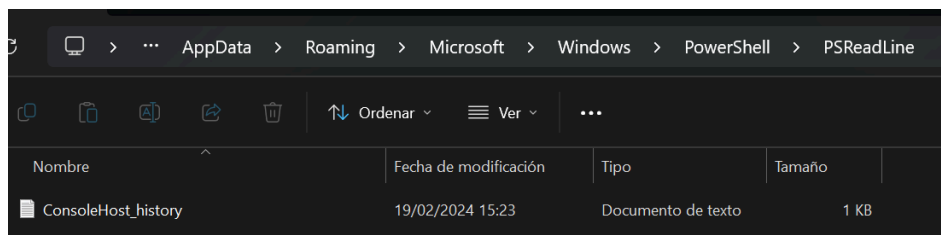


Nombre	Fecha de modificación	Tipo	Tamaño
domgmt.20230904_125742_735.etl	04/09/2023 14:59	Archivo ETL	32 KB
domgmt.20230905_070914_968.etl	05/09/2023 9:10	Archivo ETL	32 KB
domgmt.20230906_091101_475.etl	06/09/2023 11:12	Archivo ETL	32 KB
domgmt.20230907_110619_140.etl	07/09/2023 13:07	Archivo ETL	32 KB
domgmt.20230908_091741_625.etl	08/09/2023 11:19	Archivo ETL	32 KB

Contiene información sobre la IP pública del sistema. Puede ser analizado con ETLParser para extraer datos relevantes.

- **Histórico de PowerShell**

*\{Users}\%AppData%\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost\_history.txt*

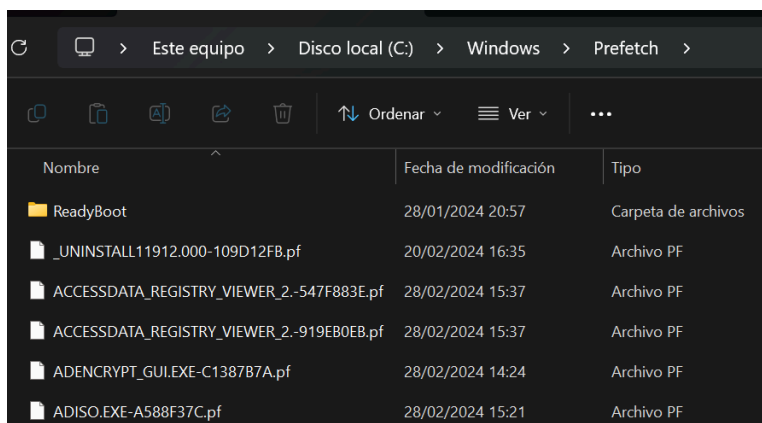


Nombre	Fecha de modificación	Tipo	Tamaño
ConsoleHost_history	19/02/2024 15:23	Documento de texto	1 KB

Guarda un historial de comandos ejecutados en PowerShell. Proporciona información sobre las acciones realizadas mediante PowerShell.

- **Windows PREFETCH (LeCMD)**

*C:\Windows\Prefetch*



Nombre	Fecha de modificación	Tipo
ReadyBoot	28/01/2024 20:57	Carpeta de archivos
_UNINSTALL11912.000-109D12FB.pf	20/02/2024 16:35	Archivo PF
ACCESSDATA_REGISTRY_VIEWER_2.-547F883E.pf	28/02/2024 15:37	Archivo PF
ACCESSDATA_REGISTRY_VIEWER_2.-919EB0EB.pf	28/02/2024 15:37	Archivo PF
ADENCRYPT_GUI.EXE-C1387B7A.pf	28/02/2024 14:24	Archivo PF
ADISO.EXE-A588F37C.pf	28/02/2024 15:21	Archivo PF

Contiene archivos prefetch que registran la ejecución de programas. Puede analizarse con LeCMD para extraer información sobre las aplicaciones utilizadas.

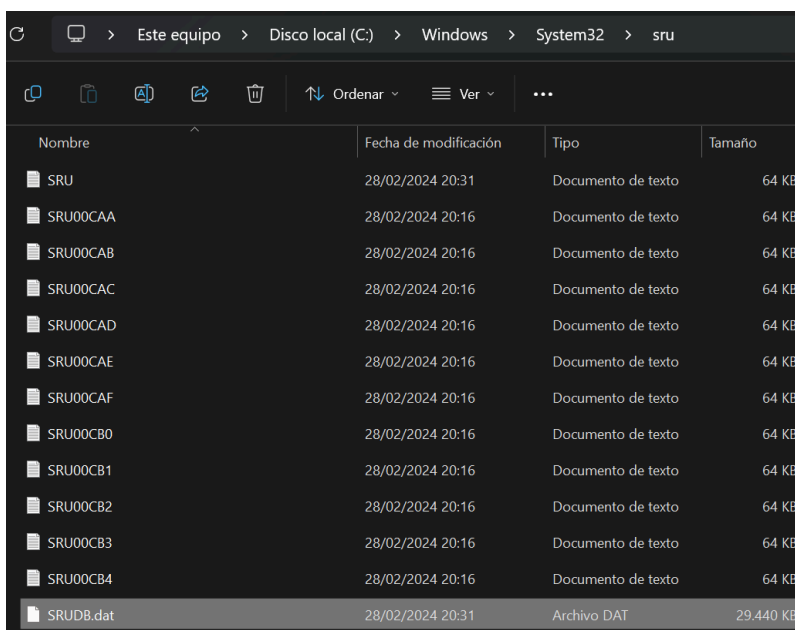
- **Windows SuperFetch (Crowdresponse)**

*C:\Windows\Prefetch\Ag\*.db*

Contiene bases de datos SuperFetch que almacenan información sobre programas utilizados con frecuencia. Puede ser examinado con Crowdresponse.

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

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



Nombre	Fecha de modificación	Tipo	Tamaño
SRU	28/02/2024 20:31	Documento de texto	64 KB
SRU00CAA	28/02/2024 20:16	Documento de texto	64 KB
SRU00CAB	28/02/2024 20:16	Documento de texto	64 KB
SRU00CAC	28/02/2024 20:16	Documento de texto	64 KB
SRU00CAD	28/02/2024 20:16	Documento de texto	64 KB
SRU00CAE	28/02/2024 20:16	Documento de texto	64 KB
SRU00CAF	28/02/2024 20:16	Documento de texto	64 KB
SRU00CB0	28/02/2024 20:16	Documento de texto	64 KB
SRU00CB1	28/02/2024 20:16	Documento de texto	64 KB
SRU00CB2	28/02/2024 20:16	Documento de texto	64 KB
SRU00CB3	28/02/2024 20:16	Documento de texto	64 KB
SRU00CB4	28/02/2024 20:16	Documento de texto	64 KB
SRUDB.dat	28/02/2024 20:31	Archivo DAT	29,440 KB

La base de datos SRUM almacena información sobre el uso de la red por parte de aplicaciones. Puede analizarse con SRUM DUMP y NetworkUsageView.

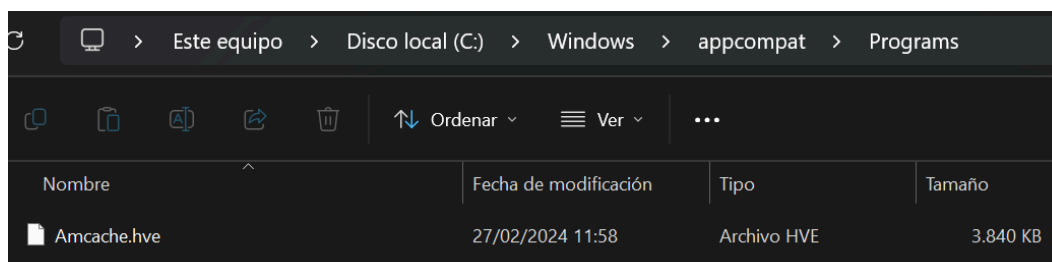
- **ShimCache (ShimCacheParser)**

*SYSTEM\CurrentControlSet\Control\SessionManager\AppcompatCache\AppCompatCache*

Contiene información sobre programas ejecutados y puede ser analizado con ShimCacheParser.

- **AmCache (AmCacheParser)**

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



Almacena información sobre la ejecución de programas. Puede ser analizado con AmCacheParser.

- **Tareas programadas**

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

Contiene las tareas programadas en el sistema. Puede ser analizado para entender la automatización de tareas.

- **Servicios (Registry Explorer)**

*SYSTEM\ControlSet001\Services*

Item	Value 1	Value 2	Date
ROOT	0	17	2024-02-27 10
ActivationBroker	0	1	2022-05-07 05
ControlSet001	0	5	2022-05-07 05
Control	12	133	2024-02-27 10
Enum	38	16	2024-02-08 20
Hardware Profiles	0	2	2024-02-27 10
Policies	0	1	2024-01-28 20
Services	0	789	2024-02-28 10
.NET CLR Data	0	2	2024-02-14 20
.NET CLR Networking	0	2	2024-02-14 20
.NET CLR Networking 4.0.0.0	0	2	2022-05-07 05
.NET Data Provider for Oracle	0	2	2022-05-07 05
.NET Data Provider for SqlServer	0	2	2022-05-07 05
.NET Memory Cache 4.0	0	2	2022-05-07 05
.NETFramework	0	1	2022-05-07 05
1394ohci	6	0	2022-05-07 05
3ware	7	2	2024-01-28 19
AarSvc	12	1	2022-05-07 05

Contiene información sobre los servicios del sistema. Puede ser analizado con Registry Explorer.

- **BAM (DCode)**

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

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

- Contiene información sobre el uso de aplicaciones por parte de usuarios. Puede ser analizado con DCode.

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

*C:\Windows\system32\winevt\Logs*

Nombre	Fecha de modificación	Tipo	Tamaño
Application	27/02/2024 20:11	Registro de eventos	2.116 KB
HardwareEvents	28/01/2024 20:58	Registro de eventos	68 KB
Internet Explorer	28/01/2024 20:58	Registro de eventos	68 KB
Key Management Service	28/01/2024 20:58	Registro de eventos	68 KB
Microsoft-Client-Licensing-Platform%4Admin	27/02/2024 11:59	Registro de eventos	1.028 KB
Microsoft-Windows-AAD%4Operational	02/02/2024 10:50	Registro de eventos	68 KB

Contiene archivos de registro de eventos del sistema. Puede ser analizado con Event-Log Explorer para entender las actividades y eventos del sistema.