

Análisis Post-mortem, los artefactos Windows

08/01/2025

—

Ramón Javier Romero Montilla
Análisis Forense
Granada

BLOQUE A.

1. Con respecto a los "prefetch"

a. ¿Qué son?

Son artefactos generados por el Administrador de Memoria de Windows. Su función principal es monitorear los primeros 10 segundos de la ejecución de una aplicación para optimizar su carga en futuros inicios. Para nosotros, los forenses, son oro puro porque demuestran ejecución de programas.

b. ¿Qué extensión tienen los ficheros?

Tienen la extensión .pf.

c. ¿En qué directorio los podemos encontrar?

Se almacenan en C:\Windows\Prefetch.

d. ¿Qué información forense guardan?

Guardan el nombre del ejecutable, el *hash*, la ruta completa desde donde se ejecutó, la fecha y hora de la última ejecución y, muy importante, un contador de cuántas veces se ha ejecutado ese programa. Además, lista los archivos y directorios que el programa tocó durante su arranque.

2. En cuanto a los "LOGS" (Registros de eventos)

a. ¿Cuáles son los más importantes?

Aunque hay muchos, los "Tres Grandes" son:

- Seguridad (Security):** Registra intentos de inicio de sesión (exitosos y fallidos, clave para ver intrusiones), uso de privilegios y auditoría de recursos.

- 
- Sistema (System):** Muestra eventos de componentes de Windows, como servicios que se inician o detienen (persistencia de malware), carga de drivers y conexión de dispositivos USB.
 - Aplicación (Application):** Errores o advertencias generados por programas instalados.

b. ¿Dónde los podemos encontrar?

Físicamente están en C:\Windows\system32\winevt\Logs, con extensión .evtx en sistemas modernos.

3. En cuanto al fichero de hibernación "hiberfil.sys"

a. ¿Dónde lo podemos encontrar?

Se encuentra en la raíz de la unidad del sistema, típicamente C:\hiberfil.sys. Es un archivo oculto y de sistema.

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

La herramienta reina aquí es **Volatility**, que permite convertir el fichero de hibernación a una imagen "raw" (imagecopy) para analizarla como si fuera un volcado de RAM. También se menciona **Arsenal Image Mounter** en tu práctica para montar imágenes y acceder a estos ficheros.

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

Es crítica. El hiberfil.sys es básicamente una copia comprimida de la memoria RAM en el momento en que el equipo hibernó. Aquí puedes encontrar contraseñas en texto claro, claves de cifrado, conexiones de red abiertas, procesos en ejecución y fragmentos de documentos no guardados que no estarían en el disco duro normal.

4. Con respecto a las instantáneas (VSS)

a. ¿Qué sistema de archivos necesitamos?

Necesitamos el sistema de archivos **NTFS**, ya que es una característica intrínseca de su estructura.

b. ¿Viene activada por defecto?

Sí, en Windows 10 y posteriores suele venir activada por defecto para la unidad del sistema (C:) como parte de la "Protección del sistema".

c. ¿Cada cuánto tiempo se realizan?

Se crean automáticamente cuando se instala software crítico, actualizaciones de Windows, o drivers firmados. También se pueden programar (típicamente cada 24 horas o semanalmente) o crear manualmente por el usuario.

d. Escenarios de utilidad:

- Recuperación de Ransomware:** Si el malware no borró las VSS, puedes restaurar archivos a su estado previo al cifrado.
- Historial de usuario:** Ver un archivo que el sospechoso borró hace días; si existe un VSS de esa fecha, el archivo sigue ahí.

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

a. Importar y exportar claves:

- GUI (Gráfico):** Usando regedit.exe. Seleccionas la clave, vas a "Archivo" > "Exportar" para guardar como .reg o colmenas (hives). Para importar, "Archivo" > "Importar".
- CLI (Comandos):** Usando el comando reg.
 - Exportar: reg export <Clave> <Archivo.reg>

- Importar: reg import <Archivo.reg>.

b. Claves interesantes para forense

- Persistencia** (Run/RunOnce):
Software\Microsoft\Windows\CurrentVersion\Run. Revela qué programas se inician automáticamente con Windows (típico de malware).
- Historial USB (USBSTOR):** SYSTEM\ControlSet001\Enum\USBSTOR.
Muestra todos los dispositivos USB que se han conectado históricamente, con marca y número de serie.
- Redes conocidas (NetworkList):** Software\Microsoft\Windows NT\CurrentVersion\NetworkList. Indica a qué redes wifi o cableadas se conectó el equipo y cuándo.
- Ejecución de programas (UserAssist):** NTUSER.DAT\...\UserAssist. Guarda contadores cifrados (ROT13) de programas ejecutados desde el explorador.
- Shellbags:** USRCLASS.DAT\...\Shell\Bags. Rastrean qué carpetas abrió el usuario y su posición, incluso si la carpeta ya fue borrada.

6. Eventos de interés forense

- Inicios de sesión (Logon/Logoff):** Event ID 4624 (éxito) y 4625 (fallo). Muchas fallas seguidas indican fuerza bruta.
- Conexión de dispositivos externos:** Para ver si alguien robó datos con un USB (Eventos en Microsoft-Windows-DriverFrameworks-UserMode).
- Manipulación del reloj:** Event ID 4616. Si el sospechoso cambió la hora para ocultar la línea temporal del delito.
- Borrado de logs:** Event ID 1102. Si aparece esto, alguien intentó "limpiar la escena del crimen".

7. Herramientas software para utilizar

- Imagen y montaje:** FTK Imager
- Registro:** Registry Explorer
- Prefetch:** PEcmd (de Eric Zimmerman).
- Logs de Eventos:** Event-Log de Windows.
- Accesos directos (LNK):** LinkParser.
- Jumplists:** JumpListExplorer.
- Shellbags (Navegación de carpetas):** Shellbag Explorer.
- USB:** USB Detective.
- Historial de navegación/Papelera:** Rifiuti

PARTE B

1. Versión del sistema, nombre de la máquina y zona horaria.

Analizando la clave Software\Microsoft\Windows NT\CurrentVersion dentro del archivo *hive SOFTWARE*, se ha extraído la siguiente información básica del sistema operativo:

- **Nombre del sistema:** Windows 10 Pro.
- **Propietario registrado (*RegisteredOwner*):** usuarioizv.
- **Versión de compilación (*CurrentBuildNumber*):** 10240.

Value Name	Value Type	Data	Value Slack
CurrentVersion	RegSz	6.3	40-FB-D4-01
EditionID	RegSz	Professional	16-00
InstallationType	RegSz	Client	D4-01-E0-FB-D4-01
InstallDate	RegDword	1762519503	
ProductName	RegSz	Windows 10 Pro	74-00-65-00-72-00-0...
RegisteredOrganization	RegSz		
RegisteredOwner	RegSz	usuarioizv	57-00-69-00-6E-00-6...
SoftwareType	RegSz	System	00-00-00-00-00-00
UBR	RegDword	16384	
PathName	RegSz	C:\Windows	73-00-74-00-2E-00
ProductID	RegSz	00330-80000-0000...	88-56-91-01
DigitalProductId	RegBinary	A4-00-00-00-03-00...	
DigitalProductId4	RegBinary	F8-04-00-00-04-00...	64-00-00-00
CurrentBuildNumber	RegSz	10240	
BuildLab	RegSz	10240.th1.150709-...	
BuildLabFw	RegSz	10240_16384_amd64	nn-nn

Analizando System\ControlSet001\Control\ComputerName\ComputerName, se ha identificado que el nombre de red asignado al equipo es **DESKTOP-R9QG4O4**.

Value Name	Value Type	Data	Value Slack
R9C	RegSz	R9C	R9C
(default)	RegSz	mnnmsrvc	02-00-78-00
ComputerName	RegSz	DESKTOP-R9QG4O4	00-00-00-00

System\ControlSet001\Control\TimeZoneInformation, se observa que el equipo está configurado en la zona horaria **Romance Standard Time** (Hora estándar romance).

	Value Name	Value Data	Value Data Raw
	R9C	R9C	R9C
▶	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	00-00-03-00-05-00-02-00-00 0-00-00-00-00-00-00
	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	00-00-0A-00-05-00-03-00-00 0-00-00-00-00-00-00
	TimeZoneKeyName	Romance Standard Time	Romance Standard Time
	ActiveTimeBias	-60	4294967236

2. Fecha de último acceso

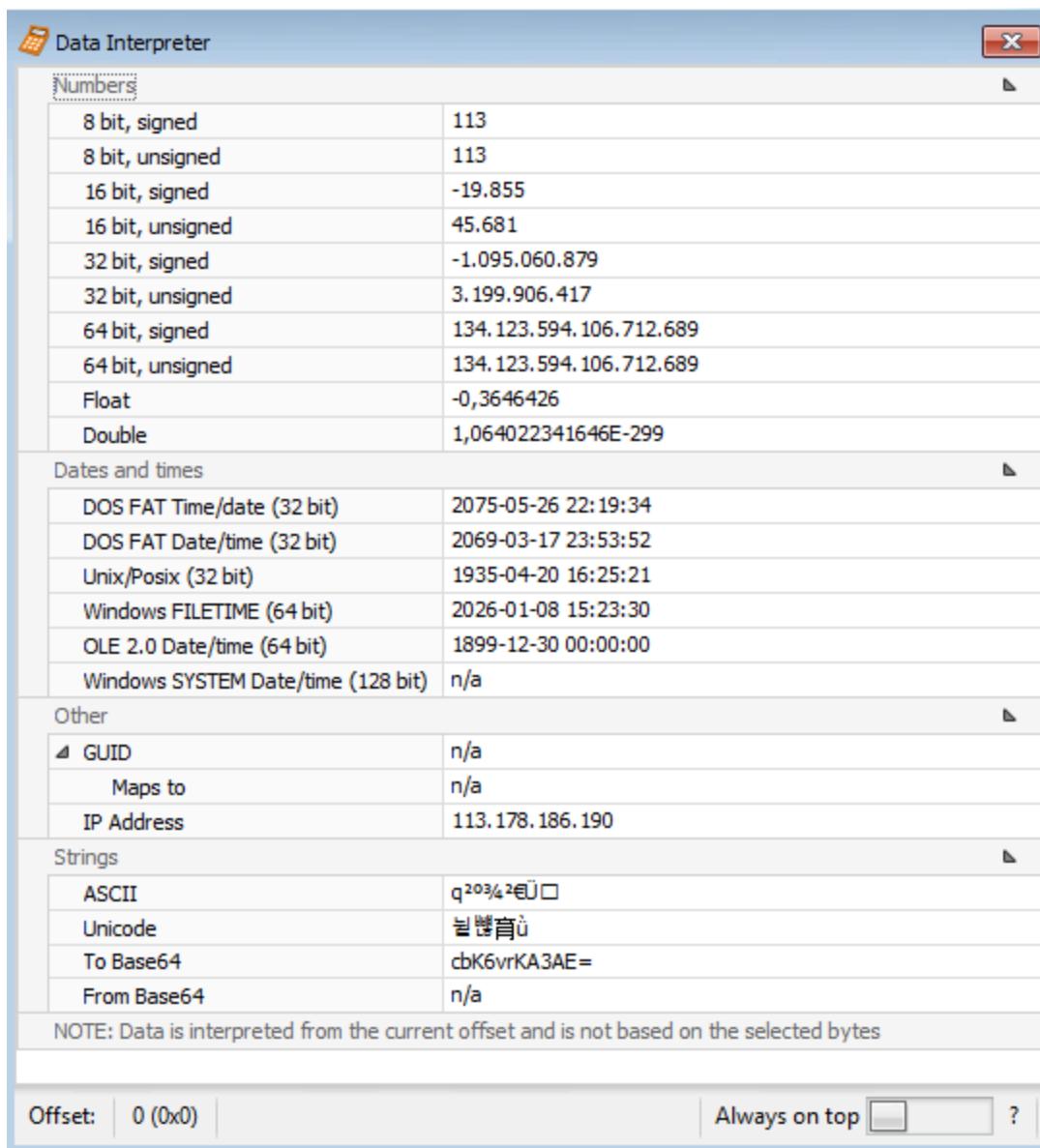
Se ha examinado la configuración del sistema de archivos en la ruta System\ControlSet001\Control\Filesystem del archivo **SYSTEM**. El parámetro NtfsDisableLastAccessUpdate tiene el valor 1. Esto indica que la actualización de la fecha de "último acceso" está **desactivada**. Por lo tanto, las marcas de tiempo de acceso en los ficheros no

son fiables para determinar cuándo fueron abiertos por última vez, ya que el sistema no registra estos eventos para optimizar el rendimiento.

Values			
Drag a column header here to group by that column			
Value Name	Value Type	Data	Value Slack
R B C	RegDword	R B C	R B C
DisableDeleteNotification	RegDword	0	
FilterSupportedFeaturesMode	RegDword	0	
NtfsAllowExtendedCharacter8dot3Rename	RegDword	0	
NtfsBugcheckOnCorrupt	RegDword	0	
NtfsDisable8dot3NameCreation	RegDword	2	
NtfsDisableCompression	RegDword	0	
NtfsDisableEncryption	RegDword	0	
► NtfsDisableLastAccessUpdate	RegDword	1	
NtfsDisableLsDowngrade	RegDword	0	
NtfsDisableVolsnapHints	RegDword	0	
NtfsEncryptPagingFile	RegDword	0	
NtfsMemoryUsage	RegDword	0	
NtfsMftZoneReservation	RegDword	0	
NtfsQuotaNotifyRate	RegDword	3600	
ScrubMode	RegDword	1	
SymlinkLocalToLocalEvaluation	RegDword	1	

3. Hora de apagado

Consultando la ruta System\ControlSet001\Control\Windows en el archivo **SYSTEM**, se ha localizado el valor binario ShutdownTime. Tras decodificar el valor hexadecimal, se determina que la fecha y hora del último apagado controlado del sistema fue el **08/01/2026 a las 15:23:30** (en UTC en hora local serían +1).



The screenshot shows the Data Interpreter tool interface with several sections of data:

- Numbers** section:

8 bit, signed	113
8 bit, unsigned	113
16 bit, signed	-19.855
16 bit, unsigned	45.681
32 bit, signed	-1.095.060.879
32 bit, unsigned	3.199.906.417
64 bit, signed	134.123.594.106.712.689
64 bit, unsigned	134.123.594.106.712.689
Float	-0,3646426
Double	1,064022341646E-299
- Dates and times** section:

DOS FAT Time/date (32 bit)	2075-05-26 22:19:34
DOS FAT Date/time (32 bit)	2069-03-17 23:53:52
Unix/Posix (32 bit)	1935-04-20 16:25:21
Windows FILETIME (64 bit)	2026-01-08 15:23:30
OLE 2.0 Date/time (64 bit)	1899-12-30 00:00:00
Windows SYSTEM Date/time (128 bit)	n/a
- Other** section:

GUID	n/a
Maps to	n/a
IP Address	113.178.186.190
- Strings** section:

ASCII	q20342€Ü□
Unicode	novità
To Base64	cbK6vrKA3AE=
From Base64	n/a

NOTE: Data is interpreted from the current offset and is not based on the selected bytes

Offset: 0 (0x0) Always on top ?

4. Interfaces de red

Se han analizado las interfaces de red configuradas en el equipo a través de la ruta System\ControlSet001\Services\Tcpip\Parameters\Interfaces . Se ha identificado una interfaz activa con GUID {d9098477-5670-4ed8-afa9-36cad4b49736}. Esta interfaz tenía asignada la dirección IPv4 **172.25.100.238**, lo que confirma la conectividad del equipo dentro de ese rango de red.

DhcpIPAddress	RegSz	172.25.100.238	00-00-00-00-00-00
---------------	-------	----------------	-------------------

5. Histórico de redes

a. Software\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles

Mediante el análisis de la clave Software\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles , se ha recuperado el historial de redes a las que se ha conectado la máquina. Se encontraron perfiles de conexión correspondientes a los nombres: **Red**, **Red 2**, **Red 3** y **Red 4**. Esto sugiere múltiples conexiones o reconfiguraciones de la interfaz de red en el entorno virtualizado.

Value Name	Type	Data	Value Slack
ProfileName	RegSz	Red 3	F2-01-CF-8D-E0-97
Description	RegSz	Red	E6-23-E2-82
Managed	RegDword	0	
Category	RegDword	0	
DateCreated	RegBinary	EA-07-01-00-04-00-0...	30-33-63-37
NameType	RegDword	6	
DateLastConnected	RegBinary	EA-07-01-00-04-00-0...	C8-77-E9-01

b. Software\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Cache

Adicionalmente, se ha examinado la clave Software\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Cache\Intranet dentro del archivo **SOFTWARE**. Se ha localizado una subclave con el nombre **cluster11.ieszaidinverg...** (el nombre completo aparece truncado en la vista de árbol, pero hace referencia al dominio local).

Value Name	Value Type	Data	Value Slack
Successes	RegDword	0	
Failures	RegDword	15	
{D9098477-5670-4ED8-AFA9-36CAD4B49736}	RegBinary	82-B3-AC-... 4E-A8-FF-64-0D...	

6. Cuándo se conectó a una red

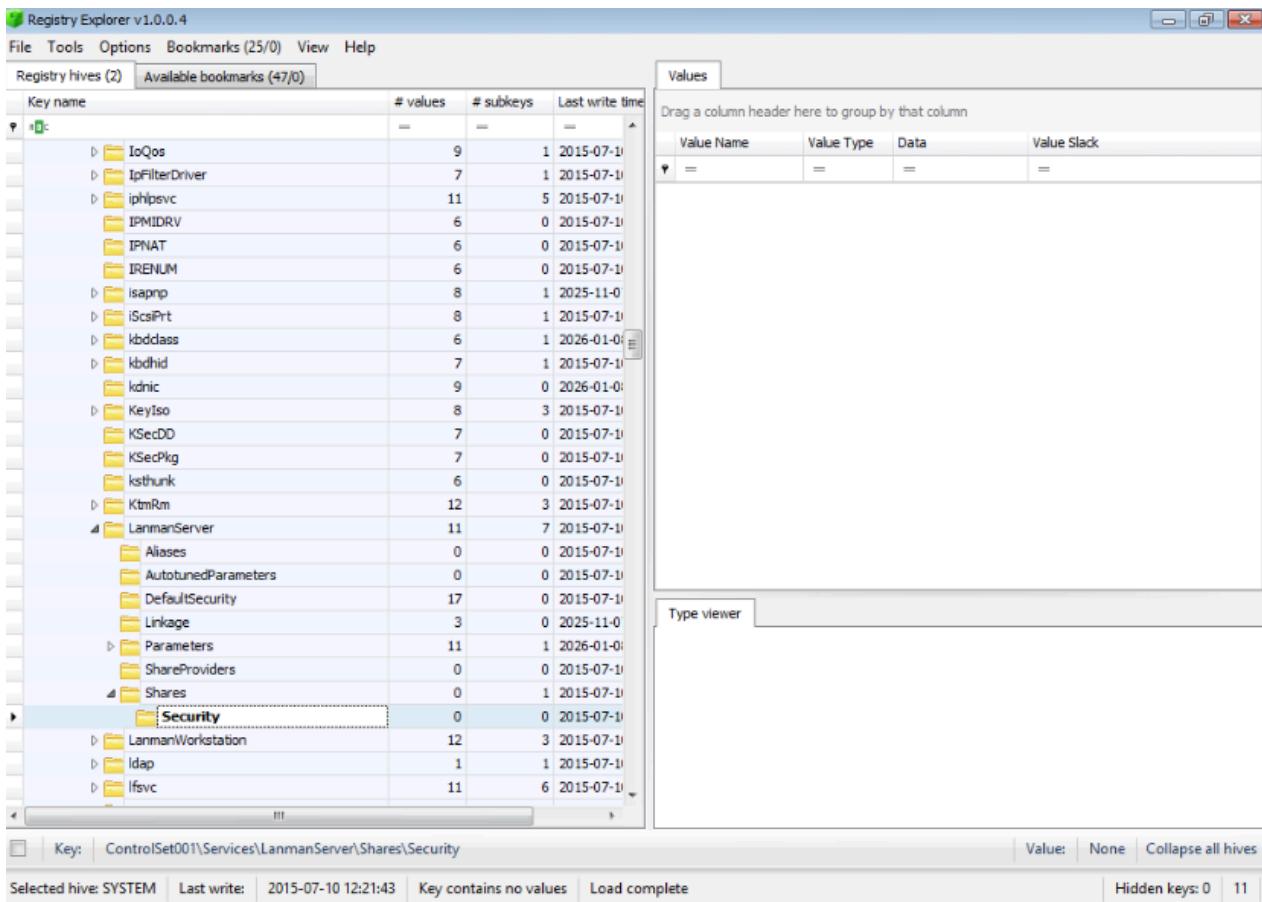
Analizando la clave Software\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles se ha analizado el valor de tiempo de la última conexión (*DateLastConnected* o *DateCreated*) en el perfil más reciente. Mediante la decodificación del valor de 128 bits, se ha establecido que la última conexión a la red se produjo el **08/01/2026 a las 16:24:03**.

Type	Value	Unit
8 bit, signed	-22	
8 bit, unsigned	234	
16 bit, signed	2.026	
16 bit, unsigned	2.026	
32 bit, signed	67.562	
32 bit, unsigned	67.562	
64 bit, signed	2.251.816.993.621.994	
64 bit, unsigned	2.251.816.993.621.994	



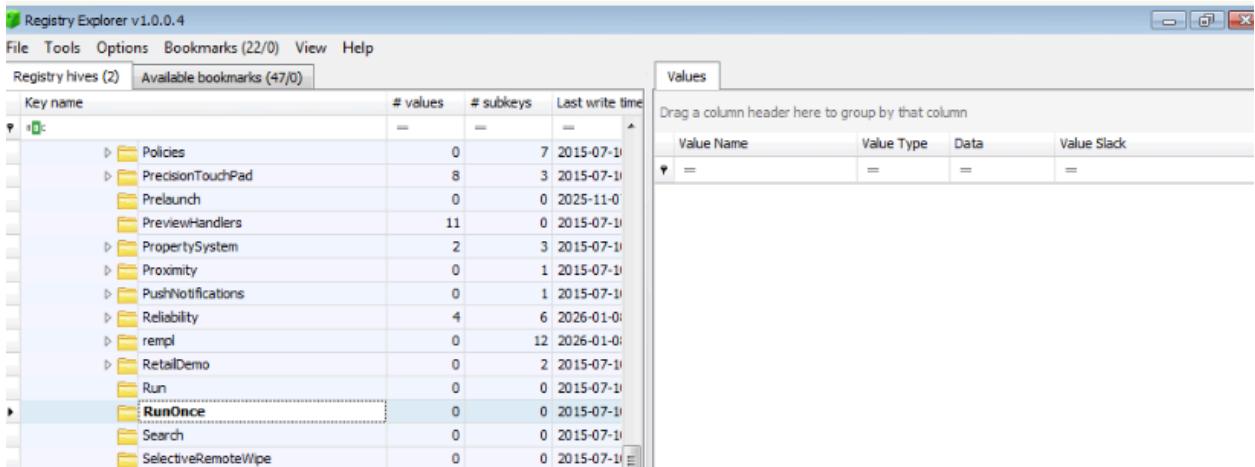
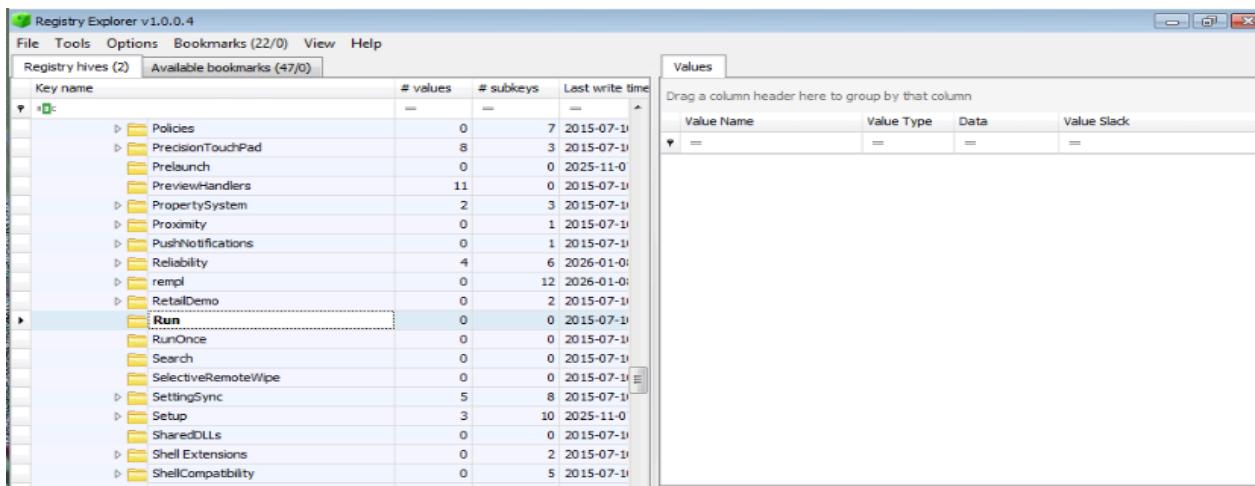
7. Carpetas compartidas

Se ha examinado la clave del registro System\ControlSet001\Services\lanmanserver\Shares en el archivo **SYSTEM** para identificar recursos compartidos en red. La clave no contiene valores asociados a rutas de directorios (aparece vacía de recursos definidos por el usuario, mostrando únicamente la subclave de seguridad por defecto).

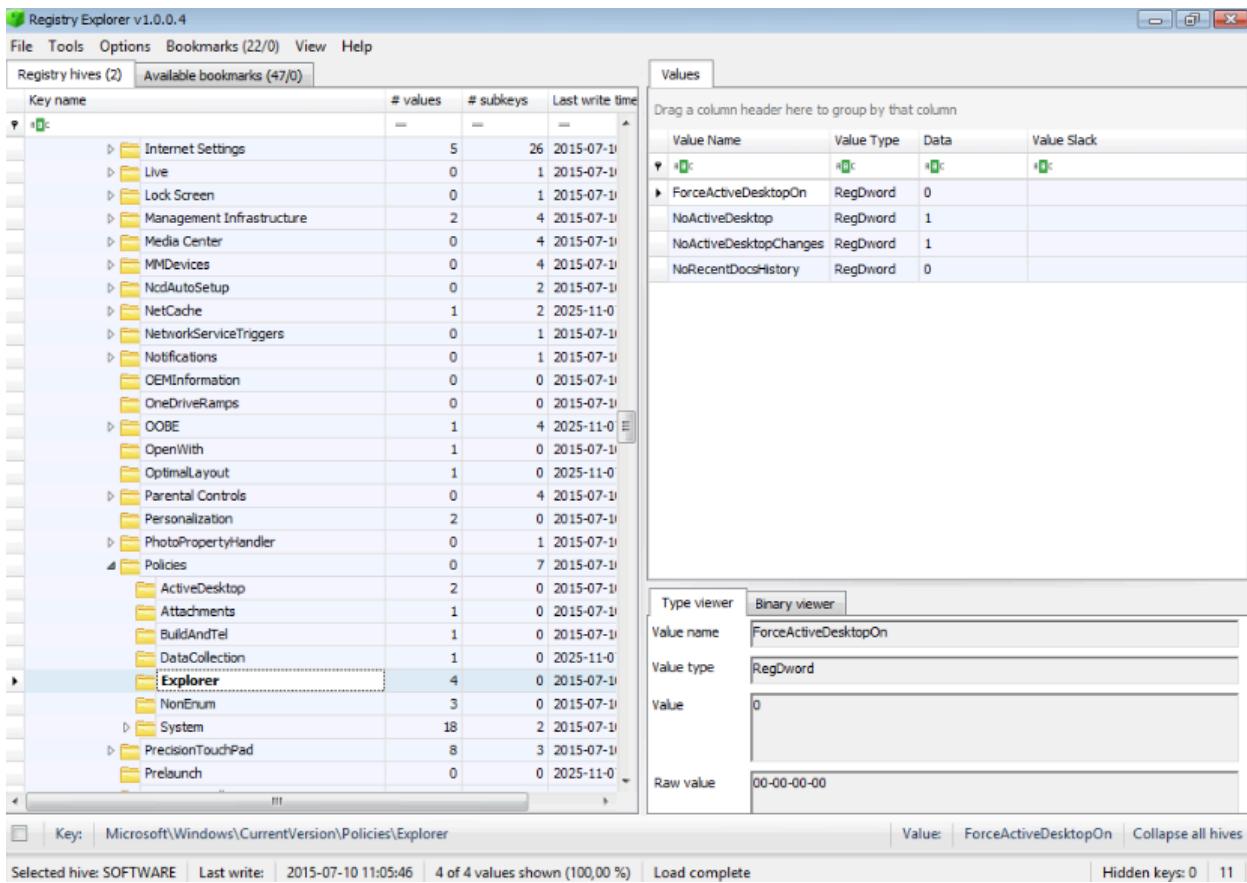


8. Programas de inicio

Software\Microsoft\Windows\CurrentVersion\Run y RunOnce (sistema), no se han encontrado valores configurados. Las capturas muestran las claves vacías, lo cual indica que no hay software de terceros o malware forzando su arranque global en esta máquina.

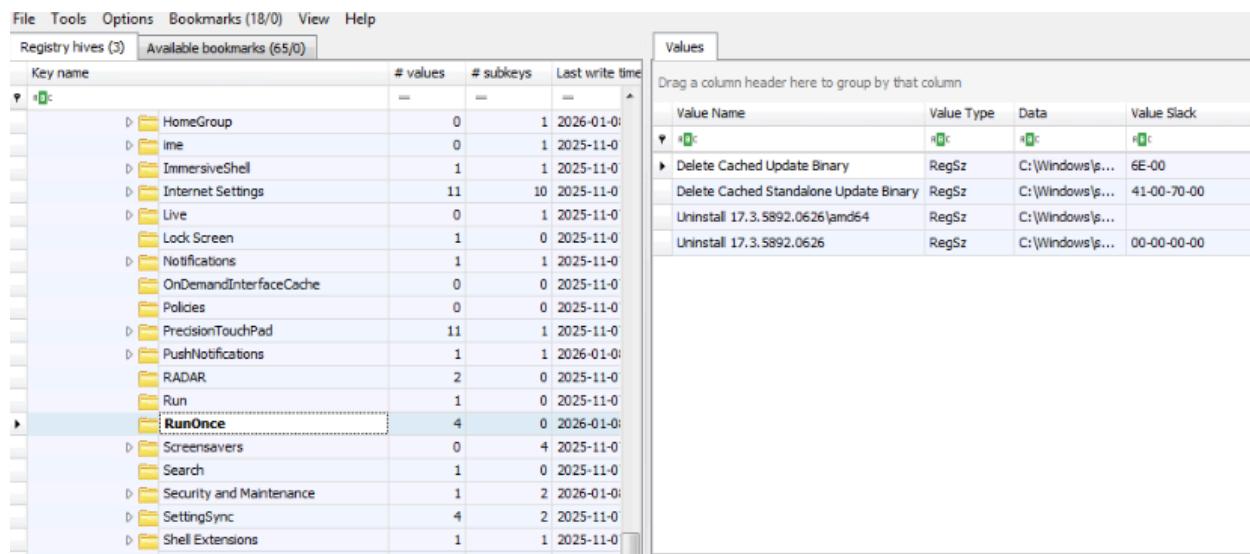
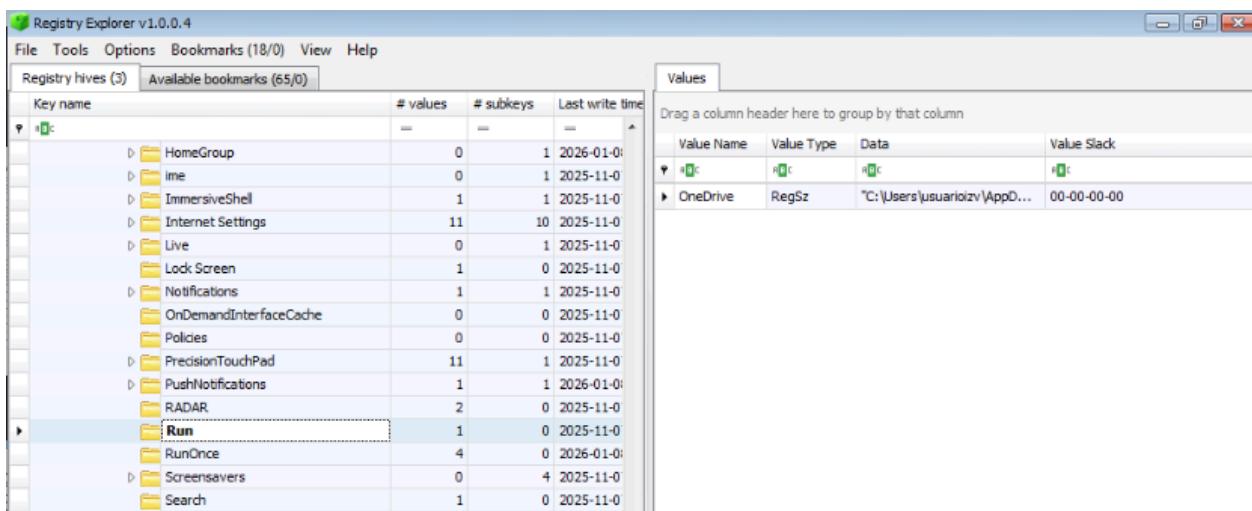


En la ruta Software\Microsoft\Windows\CurrentVersion\Policies\Explorer, se observan configuraciones relacionadas con el **Active Desktop** (ForceActiveDesktopOn, NoActiveDesktop), pero no se detecta la subclave Run que suele utilizarse para ocultar persistencia maliciosa.



Al analizar NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion Run y RunOnce del usuario *usuarioizv*:

- Run:** Se ha identificado la ejecución automática de **OneDrive** ("C:\Users\usuarioizv\AppData\..."). Es una entrada legítima y esperada en Windows 10.
- RunOnce:** Se han encontrado varias entradas pendientes de ejecución (Delete Cached Update Binary, Uninstall...). Estas corresponden a tareas de limpieza post-actualización de OneDrive o del sistema, y no representan una amenaza.



9. Búsquedas en la barra de búsqueda

Tras examinar la clave WordWheelQuery en el archivo **NTUSER.DAT**, se han recuperado evidencias de interacción del usuario con la barra de búsqueda del Explorador de Windows. Se han identificado los términos "**ftk**" y "**ftl**". La presencia de estos términos confirma que el usuario estaba intentando localizar manualmente software o archivos que comenzaban por esas letras (coincidente con herramientas forenses como FTK Imager) en el momento de la investigación.

The screenshot shows a Windows Registry table titled "WordWheelQuery". The table has three columns: "Search Term", "Mru Position", and "Key Name". There are four entries:

Search Term	Mru Position	Key Name
RBC	=	RBC
ftk	0	WordWheelQuery
ftl	1	WordWheelQuery

10. Rutas en Inicio o Explorer

Se ha examinado la clave TypedPaths dentro del archivo **NTUSER.DAT**. Esta clave almacena el historial de rutas que el usuario ha introducido manualmente en la barra de direcciones del Explorador de Windows.

En la evidencia recolectada se observa el valor url1 con el contenido \\10.5.100.1\forense.

- **Hallazgo:** Esto indica que el usuario accedió conscientemente a un recurso compartido en red (SMB) ubicado en la dirección IP 10.5.100.1 dentro de una carpeta llamada forense.

- **Importancia forense:** Demuestra que el usuario conocía la ubicación exacta del servidor y el nombre del recurso compartido, descartando un acceso accidental.

Values			
Drag a column header here to group by that column			
Value Name	Value Type	Data	Value Slack
url1	RegSz	\\\10.5.100.1\forense	42-00

11. Documentos recientes

El análisis de la clave RecentDocs en NTUSER.DAT confirma que el usuario interactuó activamente con el recurso de red \\10.5.100.1, llegando a realizar búsquedas específicas dentro de la carpeta compartida "forense". Asimismo, se evidencia la ejecución y navegación por los directorios de la herramienta "FTK Imager Lite", lo cual corrobora las búsquedas de términos detectadas anteriormente, junto con el acceso al panel de "Sistema y seguridad", demostrando un uso técnico e intencional del equipo.

Recent documents							
Extension	Value Name	Target N...	Lnk Name	Mrw Posit...	Opened On	Extension ...	
.nc	.nc	.nc	.nc	=	=	=	
RecentDocs	10	FORENSE	FORENSE.lnk	0	2026-01-...		
RecentDocs	4	ftk Imager Lite_3.1.1.lnk	ftk Imager Lite_3.1.1.lnk	1	2026-01-0...		
RecentDocs	8	langs	langs.lnk	2			
RecentDocs	5	ftk	ftk (2).lnk	3			
RecentDocs	6	help	help.lnk	4			
RecentDocs	7	enu	enu.lnk	5			
RecentDocs	3	Resultados de la búsqueda en forense (\\\10.5.100.1)	Resultados de la búsqueda en forense (\\\10.5.100.1).lnk	6			
RecentDocs	2	10.5.100.1)&ftk	ftk.lnk	7	2026-01-0...		
RecentDocs	9	ftkimager	ftkimager.lnk	8			

Total rows: 18

Type viewer Slack viewer

12. Documentos ofimáticos recientes

Mi máquina virtual no tiene instalado el Office365.

- NTUSER.DAT\Software\Microsoft\Office\{Version}\{Excel|Word}\UserMRU
- NTUSER.DAT\Software\Microsoft\Office\Word\Reading Locations\Document X.
- C:\Usuarios\Roaming\Microsoft\{Excel|Word|Powerpoint}\

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

Se ha analizado la clave OpenSavePidlMRU dentro del archivo **NTUSER.DAT**. Esta clave es crítica porque almacena el historial de archivos que han sido manipulados explícitamente a través de las ventanas de diálogo comunes de Windows ("Abrir" o "Guardar como").

En la evidencia recolectada, se identifica la entrada evidencia.txt ubicada en el Escritorio (Desktop), con fecha de acceso reciente. Esto confirma que el usuario no solo accedió al archivo, sino que interactuó con la interfaz de guardado, seleccionando manualmente la ruta de destino y el nombre del fichero.

ComDlg32 OpenSavePidlMRU				
Extension	Value Name	Mru Position	Absolute Path	Opened On
*	0	0	My Computer\Desktop\ evidencia.txt	2026-01-13 ...
txt	0	0	My Computer\Desktop\ evidencia.txt	2026-01-13 ...

14. Últimos comandos ejecutados

Aunque se ha utilizado la consola de comandos (CMD) para ejecutar herramientas como FTK Imager, la clave RunMRU aparece vacía. Esto indica forensemente que el usuario no lanzó la consola a través del cuadro de diálogo 'Ejecutar' (Win+R), sino probablemente desde el Menú Inicio o un acceso directo. Los comandos internos de la consola no dejan traza en esta clave de registro.

The screenshot shows the RegEx viewer interface. On the left, there is a tree view of available bookmarks, including DeviceAccess, Explorer, AutoplayHandlers, BitBucket, CabinetState, CD Burning, CIDSave, CLSID, ComDlg32, Desktop, Discardable, ExtractionWizard, FileExts, HideDesktopIcons, LogonStats, LowRegistry, MenuOrder, Modules, MountPoints2, Package Installation, RecentDocs, Ribbon, and RunMRU. The RunMRU node is highlighted. On the right, there are two tabs: 'Values' and 'RunMRU'. The 'RunMRU' tab is selected and displays a table with four columns: Value Name, Mru Position, Executable, and Opened On. The table has one row with values: Value Name is 'RunMRU', Mru Position is '=', Executable is 'n/a', and Opened On is '='. Below the table, it says 'Total rows: 0' and there is a 'Type viewer' button.

Value Name	Mru Position	Executable	Opened On
RunMRU	=	n/a	=

En cuanto a Policies\RunMRU no se adjunta captura debido a la inexistencia de la clave.

15. UserAssistKey: Programas ejecutados desde el Escritorio

En la captura se observan los nombres de los ejecutables ofuscados mediante el algoritmo **ROT13**. La columna "Run Counter" revela el número exacto de veces que el usuario ha ejecutado cada aplicación, y "Last Executed" indica la fecha y hora de la última vez que se lanzó. Esto permite establecer un perfil de uso habitual y demostrar la interacción directa del usuario con programas específicos.

Available bookmarks (42/0)						
Key name	# values	# subkeys	Last write timestamp	Values UserAssist		
Package Installation	1	0	2025-01-13 15:24:39			
RecentDocs	23	7	2025-01-13 16:31:59			
Ribbon	1	0	2025-11-07 13:15:43			
RunMRU	0	0	2025-01-08 15:33:18			
SearchPlatform	0	1	2025-11-07 12:46:17			
Shell Folders	31	0	2025-11-07 12:46:19			
Shutdown	1	0	2025-01-08 15:32:46			
SoftLanding	0	0	2025-11-07 12:46:28			
StartPage	2	0	2025-11-07 12:46:27			
StartupApproved	0	1	2025-01-08 16:29:41			
StorageProvider	0	1	2025-01-13 15:25:29			
Streams	0	1	2025-11-07 12:47:41			
StuckRects3	1	0	2025-11-07 12:47:41			
Taskband	5	0	2025-01-13 15:24:43			
TypedPaths	1	0	2025-01-08 15:50:18			
User Shell Folders	20	0	2025-11-07 12:46:17			
UserAssist	0	9	2025-11-07 12:46:20			
{9E04CAB2-CC14-11DF-BB8...	1	1	2025-11-07 12:46:20			
{A3D53349-6E61-4557-8FC7...	1	1	2025-11-07 12:46:20			
{B267E3AD-A825-4A09-82B9...	1	1	2025-11-07 12:46:20			
{BCB48336-4DD0-48FF-BB0B...	1	1	2025-11-07 12:46:20			
{CAA59E3C-4792-41A5-9909...	1	1	2025-11-07 12:46:20			
{CEBF5CD-ACE2-4F4F-9178...	1	1	2025-11-07 12:46:20			
Count	27	0	2025-01-13 16:32:34			
{F2A1CB5A-E3CC-4A2E-AF9...	1	1	2025-11-07 12:46:20			
{F4E57C4B-2036-45F0-A9AB...	1	1	2025-11-07 12:46:20			
{FA99DFC7-6AC2-453A-A5E...	1	1	2025-11-07 12:46:20			
Count	0	0	2025-11-07 12:46:20			

P:\Hfref\hf hnevbmvi Qrfqbc\Er tvfgelRkcy bere_ERPz q_1004\Er vfgelRkcyb ere.rkr	C:\Users\us uariozv\Des ktop\Re gistryExpl orer_RECm d_1004\Reg istryExplor er.exe	2	17	0d, 1h, 29m, 49s	2026-01..
►					

16. Eventos asociados a la barra de tareas

Mi máquina virtual no tiene eventos asociados a la barra de tareas.

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

17. Aplicaciones recientes

En mi máquina virtual la carpeta Search está vacía. Por lo que el sistema no está registrando el historial de aplicaciones lanzadas a través de la barra de búsqueda (Cortana/Search)

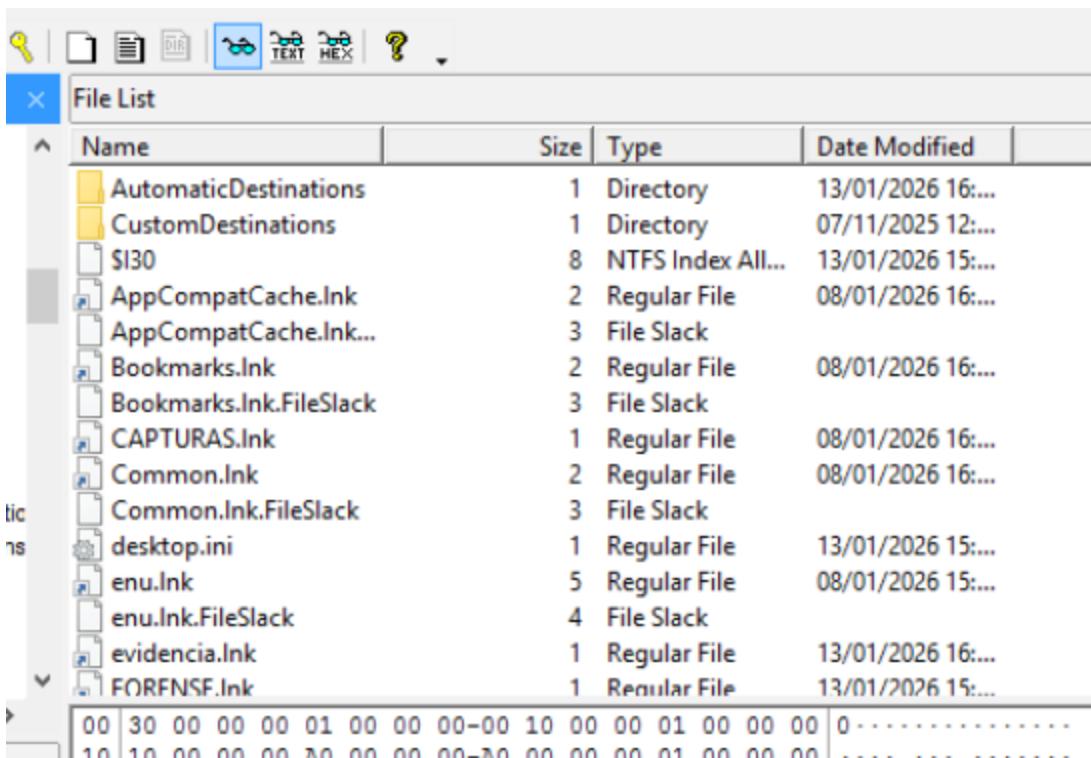
Software\Microsoft\Windows\Current Version\Search\RecentApps

18. Documentos recientes (LinkParses o LeCMD)

Se ha examinado el directorio Recent del sistema de archivos mediante FTK Imager. Este directorio contiene ficheros de enlace (.lnk) que Windows genera automáticamente cada vez que el usuario abre un archivo o directorio.

Hallazgos clave en la evidencia:

- **evidencia.lnk:** Confirma forensemente que el archivo de texto creado anteriormente en el Escritorio fue abierto recientemente.
- **FORENSE.lnk:** Ratifica la interacción persistente con el directorio compartido en red.
- **CAPTURAS.lnk:** Indica que el usuario ha estado accediendo a una carpeta de imágenes o capturas, probablemente relacionada con la documentación de sus actividades.



The screenshot shows a software interface titled "File List". The table has columns for Name, Size, Type, and Date Modified. The data is as follows:

Name	Size	Type	Date Modified
AutomaticDestinations	1	Directory	13/01/2026 16:...
CustomDestinations	1	Directory	07/11/2025 12:...
SI30	8	NTFS Index All...	13/01/2026 15:...
AppCompatCache.lnk	2	Regular File	08/01/2026 16:...
AppCompatCache.lnk...	3	File Slack	
Bookmarks.lnk	2	Regular File	08/01/2026 16:...
Bookmarks.lnk.FileSlack	3	File Slack	
CAPTURAS.lnk	1	Regular File	08/01/2026 16:...
Common.lnk	2	Regular File	08/01/2026 16:...
Common.lnk.FileSlack	3	File Slack	
desktop.ini	1	Regular File	13/01/2026 15:...
enu.lnk	5	Regular File	08/01/2026 15:...
enu.lnk.FileSlack	4	File Slack	
evidencia.lnk	1	Regular File	13/01/2026 16:...
FORFNSF.lnk	1	Regular File	13/01/2026 15:...

Below the table, there is a hex dump of the file data.

19. Automatic & Custom destinations (JumpListExplorer)

Se han extraído evidencias de las **Jump Lists** de Windows. Estos artefactos son listas de "destinos frecuentes" o "recientes" asociadas a aplicaciones específicas de la barra de tareas.

- **AutomaticDestinations:** Contiene archivos con extensión .automaticDestinations-ms. Los nombres de archivo (como 5f7b5f1e01b83767) son identificadores hexadecimales (AppIDs) únicos para cada programa (ej: Explorador de Archivos, navegadores). Su análisis permite reconstruir qué documentos específicos abrió el usuario con cada aplicación y en qué orden.
- **CustomDestinations:** Contiene archivos .customDestinations-ms. Estos ficheros registran los elementos que el usuario ha "anclado" manualmente a la Jump List o categorías personalizadas por la aplicación, demostrando archivos de alta relevancia para el usuario.

The screenshot displays two separate windows of the Shellbag Explorer tool. Both windows have a title bar 'File List' and a toolbar with various icons.

Top Window (Recent Shellbag):

- Left pane: Shows the Windows shellbag structure with 'Recent' expanded, revealing 'AutomaticDestinatic' and 'CustomDestinations' sub-folders.
- Right pane: A table titled 'File List' with columns: Name, Size, Type, Date Modified. It lists several files:

Name	Size	Type	Date Modified
\$I30	4	NTFS Index All...	13/01/2026 16:...
5f7b5f1e01b83767.aut...	9	Regular File	13/01/2026 16:...
7e4dca80246863e3.aut...	3	Regular File	07/11/2025 13:...
7e4dca80246863e3.aut...	1	File Slack	
9b9cdc69c1c24e2b.aut...	3	Regular File	13/01/2026 16:...
f01b4d95cf55d32a.aut...	45	Regular File	13/01/2026 16:...
f01b4d95cf55d32a.aut...	3	File Slack	

Bottom Window (CustomDestinations Shellbag):

- Left pane: Shows the Windows shellbag structure with 'CustomDestinations' selected.
- Right pane: A table titled 'File List' with columns: Name, Size, Type, Date Modified. It lists two files:

Name	Size	Type	Date Modified
7e4dca80246863e3.cus...	1	Regular File	07/11/2025 12:...
f01b4d95cf55d32a.cus...	1	Regular File	07/11/2025 12:...

20. Shellbags: Acceso y tiempos MAC a directorios (ShellbagExplorer)

Se ha procedido al análisis de los artefactos *Shellbags*, esenciales para reconstruir el historial de navegación del usuario a través del Explorador de Archivos. Durante la extracción, se detectó que el archivo USRCLASS.DAT se encontraba en estado inconsistente (**Dirty Hive**), lo que impedía su lectura directa. Para subsanarlo, se trajeron y aplicaron forensemente los archivos de transacción (.LOG1 y .LOG2), logrando reconstruir la integridad de la base de datos para su análisis.

The screenshot shows the ShellBags Explorer interface. On the left is a tree view of desktop items, including 'Desktop', 'Documents', 'Search Folder', 'Computers and Devices', 'RegistryExplorer_RECcmd.zip', 'My Computer', 'SURICATA', 'Flask_Peso_PPS', 'CE Y AVL', 'FORENSE 2', 'AppCompatCacheParser', 'AmcacheParser', 'RegistryExplorer_RECcmd', 'ShimCacheParser', 'BASTIONADO 8', 'Frances', 'Practica V Forense', 'Fotinhas Analisis Forense P4', 'AppNueva', 'Captures', 'ADQUISICIÓN DE EVIDENCIAS', 'archive', 'Fotos', 'ChillConsulting', 'capturas ej4 (1)', 'Shared Documents Folder (Users Files)', 'appcompatibilityview-x64', 'AppCompatCacheParser.zip', 'Downloads', 'PRACTICA MEDIA AF', 'FOTONES DE HACKING', and 'PRUEBA'. On the right is a detailed table of shell bags:

Value	Icon	Shell Type	MRU Position	Created On	Modified On
Desktop	Sin i...	Root folder: GUID	=	=	=
Documents	Root folder: GUID	Root folder: GUID	7		
Search Folder	Root folder: GUID	Root folder: GUID	1		
Computers and Devices	Root folder: GUID	Root folder: GUID	0		
RegistryExplorer_RECcmd.zip	Users property view: Drive letter	Users property view	36		
My Computer	Users property view	Users property view	55		
SURICATA	Root folder: GUID	Root folder: GUID	27		
Flask_Peso_PPS	Root folder: GUID	Root folder: GUID	54		
CE Y AVL	Root folder: GUID	Root folder: GUID	30		
FORENSE 2	Directory	Directory	22	2025-10-21 14:23:30	2025-10-
AppCompatCacheParser	Root folder: GUID	Root folder: GUID	53		
AmcacheParser	Root folder: GUID	Root folder: GUID	10	2025-10-22 15:57:36	2025-10-
RegistryExplorer_RECcmd	Root folder: GUID	Root folder: GUID	48	2025-10-27 16:42:44	2025-10-
ShimCacheParser	File	File	52	2025-10-22 16:00:32	2025-10-
BASTIONADO 8	archive	Directory	23	2025-10-29 16:16:30	2025-10-
Frances					
Practica V Forense					
Fotinhas Analisis Forense P4					
AppNueva					
Captures					
ADQUISICIÓN DE EVIDENCIAS					
archive					
Fotos					
ChillConsulting					
capturas ej4 (1)					
Shared Documents Folder (Users Files)					
appcompatibilityview-x64					
AppCompatCacheParser.zip					
Downloads					
PRACTICA MEDIA AF					
FOTONES DE HACKING					
PRUEBA					
Unmapped GUID: f874310e-b6b7-47dc-bc84-b9...					

Below the table, there is a summary section with details about the selected item ('Desktop'):

- Name: Desktop
- Absolute path: Desktop\Desktop
- Key-Value name path: BagMRU-3
- Registry last write time: 2026-01-22 16:13:38.191
- Miscellaneous
- Shell type: Root folder: GUID
- Node slot: 6
- MRU position: 0
- # of child bags: 29
- Last interacted with: 2026-01-22 16:13:38.191

At the bottom, status messages indicate: 'UsrClass.dat' Registry hive loaded in 0,4180 seconds! | 56 shellbags loaded in 0,0044 seconds | Time zone: UTC | 56 of 56 rows visible (100,00 %)

1. Reconstrucción de Rutas (BagMRU): Como se observa en la captura superior, la herramienta ha permitido visualizar la estructura jerárquica de carpetas (BagMRU). Esto confirma las rutas exactas por las que navegó el usuario, identificando accesos directos a directorios críticos como **Descargas** y **Escritorio**, ubicaciones clave en esta investigación.

2. Confirmación de Interacción Humana (Bags): El análisis de los valores *Bags* aporta pruebas concluyentes de actividad consciente por parte del usuario:

- **Interacción Reciente:** La columna *Last Interacted* (visible en la imagen) registra la fecha y hora exacta en la que el usuario abrió la carpeta. Esto sitúa al usuario visualizando estos archivos en el momento del incidente.

- **Preferencias de Vista:** Los parámetros configurados, como LogicalViewMode o IconSize, demuestran que el contenido fue visualizado gráficamente (iconos, lista, detalles), lo que descarta accesos automatizados y confirma la navegación manual.

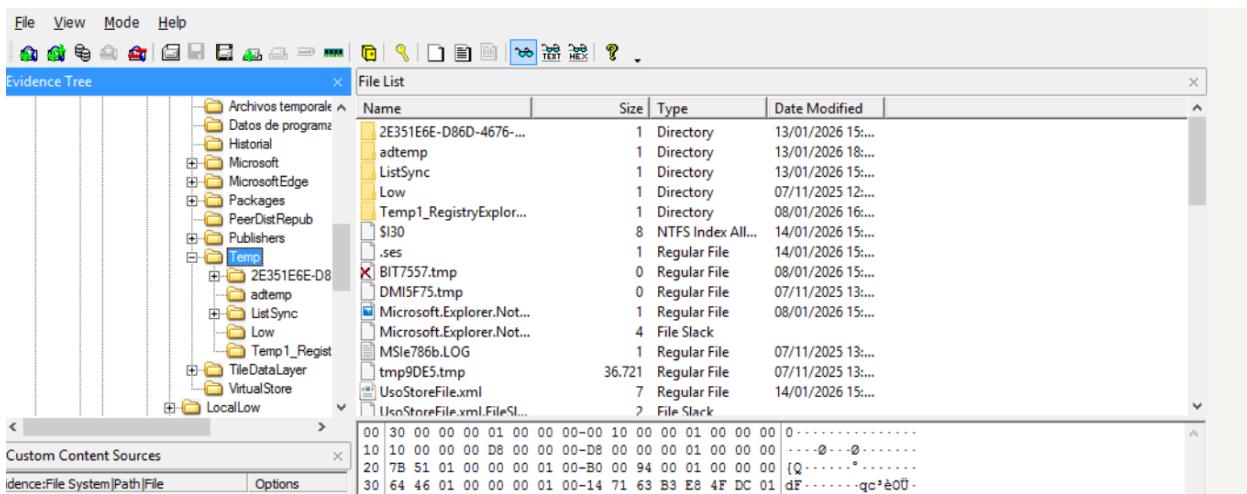
The screenshot shows the ShellBags Explorer interface. On the left, a tree view displays the registry structure under 'Value'. The root node is 'Desktop', which contains 'Computers and Devices', '10.5.100.1', and a 'Search Folder' named '\10.5.100.1\forenses'. Below '10.5.100.1' is a 'RegistryExplorer_RECm' entry. The main pane is a grid table with columns: Value, Icon, Shell Type, MRU Position, Created On, Modified On, Accessed On, First Interacted, and Last Interacted. A single row is visible in the grid, corresponding to the '\10.5.100.1\forenses' entry. The bottom pane is a details view for the selected entry. It shows the following information:
Name: \10.5.100.1\forenses
Absolute path: Desktop\Computers and Devices\10.5.100.1\10.5.100.1\forenses
Key-Value name path: BagMRU\0\0-0
Registry last write time: 2026-01-20 16:22:47.505

Miscellaneous
Shell type: Network location
Node slot: 2
MRU position: 0
of child bags: 0

First interacted with: 2026-01-20 16:22:47.505
Last interacted with: 2026-01-20 16:22:47.505

21. Dispositivos MTP

Tras analizar C:\Users\usuarioizv\AppData\Local\Temp se ha procedido a la búsqueda de evidencias relacionadas con dispositivos portátiles (Windows Portable Devices). La ausencia del subdirectorio WPDNSE en la carpeta temporal del usuario indica forenseamente que **no se han conectado dispositivos MTP** (como teléfonos inteligentes Android/iOS o cámaras digitales) configurados para la transferencia de archivos multimedia en esta sesión de usuario.



22. Volúmenes USB

Claves analizadas:

- SOFTWARE\Microsoft\Windows Portable Devices\Devices
- NTUSER.DAT\...\MountPoints2
- Software\Microsoft\Windows NT\CurrentVersion\EMDMgmt
- System\ControlSet001\Enum\USBSTOR

Se ha verificado la ausencia de subclaves y valores asociados a dispositivos de almacenamiento externo en las rutas indicadas.

- **USBSTOR y Properties:** No existen registros de identificadores de fabricante (VID) ni de producto (PID) correspondientes a memorias USB.
- **EMDMgmt:** No hay rastro de dispositivos utilizados para ReadyBoost.
- **MountPoints2:** No se identifican puntos de montaje asociados a letras de unidad extraíbles (E:, F:, etc.).

El sistema no presenta evidencia técnica de haber interactuado con dispositivos de almacenamiento físico externo (USB/HDD/SSD) durante la sesión del usuario analizado.

Registry hives (5) Available bookmarks (90/0)

Key name	# values	# subkeys	Last write time
ROOT	0	14	2026-01-01 00:00:00
ActivationBroker	0	1	2015-07-10 18:00:00
ControlSet001	0	6	2015-07-10 18:00:00
Control	10	110	2026-01-01 00:00:00
Enum	27	11	2025-11-01 18:00:00
ACPI	0	10	2025-11-01 18:00:00
ACPI_HAL	0	1	2025-11-01 18:00:00
DISPLAY	0	2	2025-11-01 18:00:00
HTREE	0	1	2015-07-10 18:00:00
PCI	0	21	2025-11-01 18:00:00
ROOT	0	13	2025-11-01 18:00:00
SCSI	0	2	2025-11-01 18:00:00
STORAGE	0	1	2025-11-01 18:00:00
SWD	0	5	2025-11-01 18:00:00
USB	0	2	2025-11-01 18:00:00
ROOT_HUB	0	6	2025-11-01 18:00:00
ROOT_HUB20	0	2	2025-11-01 18:00:00
{6FDE7547-1B65-48ae-B628-80BE6201...	0	1	2025-11-01 18:00:00
Hardware Profiles	0	3	2026-01-01 00:00:00
Policies	0	0	2015-07-10 18:00:00
Services	0	546	2026-01-01 00:00:00
Software	0	1	2015-07-10 18:00:00

Values			
Value Name	Value Type	Data	Value
=	=	=	=

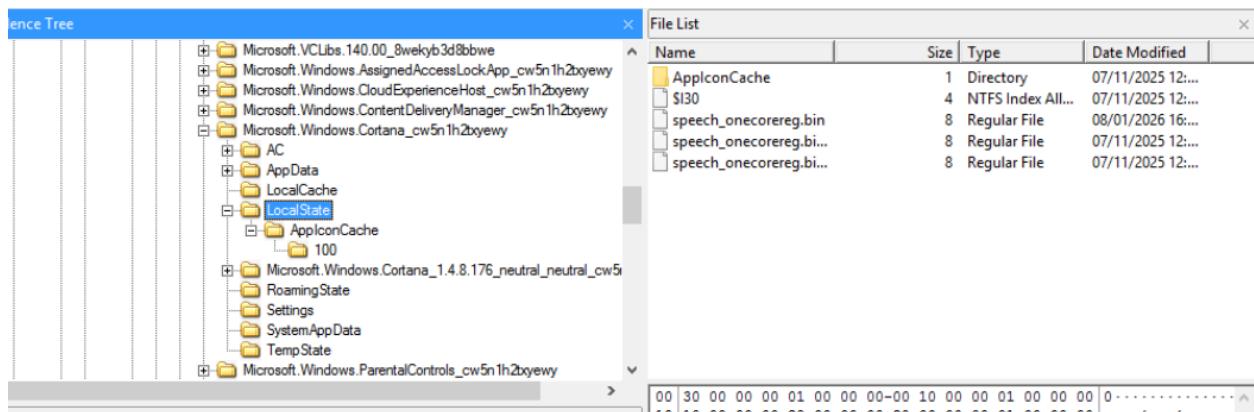
Type viewer

CLSID	0	6	2025-11-01 18:00:00
ComDig32	0	3	2026-01-01 00:00:00
Desktop	0	1	2025-11-01 18:00:00
Discardable	0	1	2025-11-01 18:00:00
ExtractionWizard	1	0	2026-01-01 00:00:00
FileExts	0	174	2026-01-01 00:00:00
HideDesktopIcons	0	1	2025-11-01 18:00:00
LogonStats	1	0	2025-11-01 18:00:00
LowRegistry	0	0	2025-11-01 18:00:00
MenuOrder	0	1	2025-11-01 18:00:00
Modules	0	3	2025-11-01 18:00:00
MountPoints2	0	4	2025-11-01 18:00:00
CPC	0	1	2025-11-01 18:00:00
Volume	0	0	2026-01-01 00:00:00
{8612010f-0000-0000-0000-000000000000	0	0	2025-11-01 18:00:00
{e6075895-bbd6-11f0-9bc2-000000000000	0	0	2025-11-01 18:00:00
{e6075896-bbd6-11f0-9bc2-000000000000	0	0	2025-11-01 18:00:00
Package Installation	1	0	2026-01-01 00:00:00
RecentDocs	23	7	2026-01-01 00:00:00
Ribbon	1	0	2025-11-01 18:00:00
RunMRU	0	0	2026-01-01 00:00:00
SearchPlatform	0	1	2025-11-01 18:00:00
Shell Folders	31	0	2025-11-01 18:00:00
Shutdown	1	0	2026-01-01 00:00:00
SoftLanding	0	0	2025-11-01 18:00:00
StartPage	2	0	2025-11-01 18:00:00
StartupApproved	0	1	2026-01-01 00:00:00
StorageProvider	0	1	2026-01-01 00:00:00
Chromosome	0	1	2025-11-01 18:00:00

23. Base de datos Cortana, si existiese, en versiones anteriores a Windows 10.0.17763.55 (Sqlite studio)

Tras analizar C:\Users\usuarioizv_...\LocalState\ESEDatabase_CortanaCoreInstance, se ha procedido a la búsqueda del archivo CortanaCoreDb.dat en el directorio de paquetes de la aplicación. La ausencia de este artefacto indica que el servicio de Cortana no ha sido activado plenamente o que el usuario no ha iniciado sesión con una cuenta de Microsoft para habilitar el historial en la nube y local. Por tanto, no existe registro de consultas de voz o texto recuperable en este dispositivo.

Si se hubiera localizado, el archivo CortanaCoreDb.dat (base de datos ESE) podría analizarlo con herramientas como **ESEDatabaseView** para extraer la tabla de actividad. Esto permitiría recuperar evidencias críticas como las **palabras clave buscadas** (*Query Keywords*), la fecha y hora exacta de las consultas y los **enlaces o aplicaciones ejecutadas** (*LaunchUri*) a raíz de dichas búsquedas.



24. Notificaciones de Windows (sqlite studio)

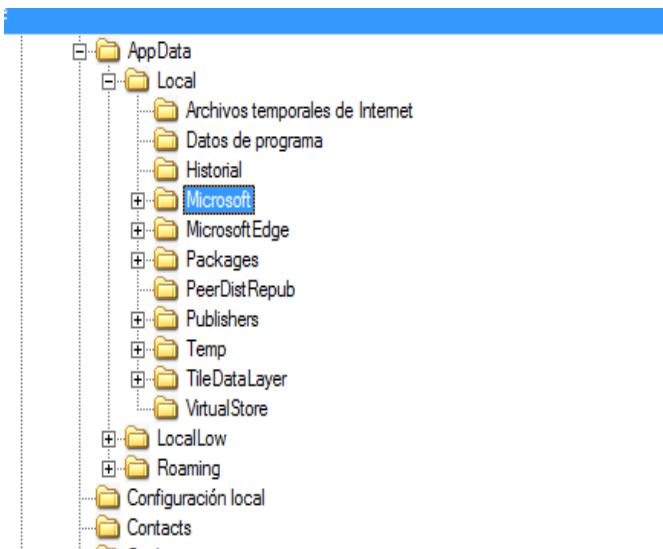
Se ha examinado el directorio de notificaciones del sistema (`C:\Users\usuarioizv\AppData\Local\Microsoft\Windows\Notifications`). Se constata la **ausencia del archivo wpndatabase.db** (base de datos SQLite principal de notificaciones). Solo se encuentran archivos de configuración y estado (`appdb.dat`), lo que indica forensemente que el sistema no ha recibido ni procesado notificaciones "Toast" (alertas de usuario) durante esta sesión. Por tanto, no es posible recuperar historial de mensajes o alertas del centro de actividades.

The screenshot shows the SQLite Studio interface with a file browser on the left and a table viewer on the right. The file browser displays a tree view of the Windows Notifications folder structure. The table viewer shows the following data:

Name	Type	Date Modified
wpnidm	Directory	14/01/2026 15:...
appdb.dat	Regular File	07/11/2025 12:...
appdb.dat.FileSlack	File Slack	4
WPNPROMRY.tmp	Regular File	14/01/2026 15:...

25. Timeline (Windows TimelineParser)

Tras intentar analizar la clave `C:\Users\usuarioizv\AppData\Local\ConnectedDevicesPlatform` nos hemos dado cuenta que también la funcionalidad "Windows Timeline" fue introducida en Windows 10 versión 1803. Dado que el sistema opera sobre la compilación **10240**, esta característica no está implementada en el sistema operativo. **Conclusión:** No existen artefactos de línea de tiempo (ActivitiesCache) que permitan reconstruir la continuidad de actividades del usuario, ya que el servicio Connected Devices Platform no está presente en esta versión antigua de Windows.



26. Windows Store (**DB Browser for SQLite**)

Analizando el AppRepository\StateRepository-Machine.srdSe ha procedido a la extracción y análisis forense de la base de datos StateRepository-Machine.srd utilizando la herramienta **DB Browser for SQLite**. El examen de la estructura interna revela 47 tablas de sistema, destacando:

- **Application:** Contiene el inventario detallado de aplicaciones instaladas.
- **Package:** Almacena la información de los paquetes de instalación y sus versiones.
- **User:** Vincula cada aplicación con el SID del usuario que la instaló.

Este artefacto permite cruzar la información obtenida del Registro de Windows para verificar la integridad del software instalado y detectar aplicaciones que pudieran estar ocultas a nivel de interfaz gráfica pero presentes en la base de datos del repositorio.

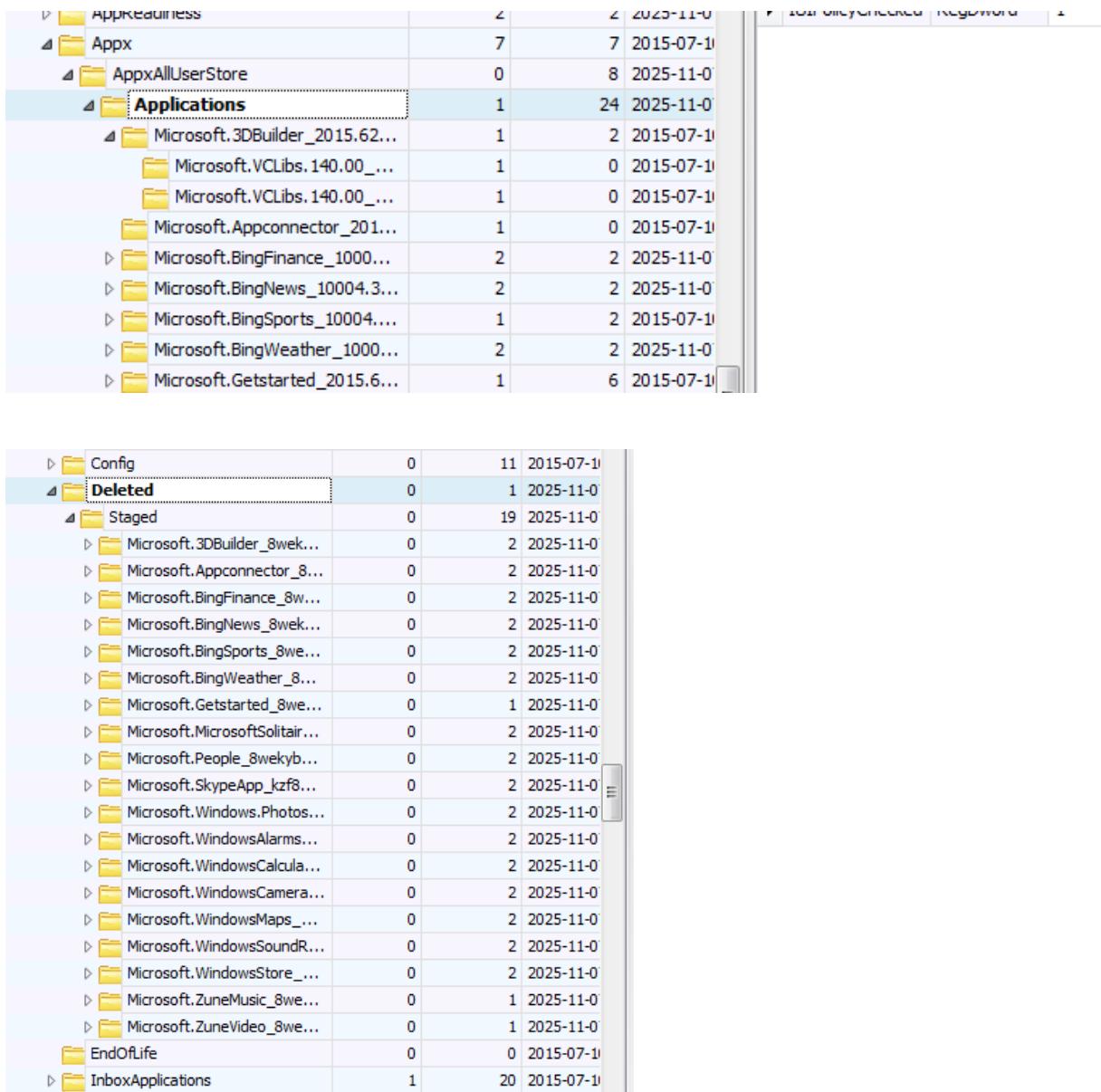
The screenshot displays a forensic analysis interface. At the top, there is a file list showing several files, including 'Microsoft.ZuneVideo_...' (Regular File, 12 bytes, 07/11/2025), 'StateRepository-Deplo...' (Regular File, 2.048 bytes, 13/01/2026), and several entries for 'StateRepository-Mach...' (Regular Files, sizes 2.304, 32, and 0 bytes, all dated 14/01/2026). Below this is a menu bar with Archivo, Editar, Ver, Herramientas, Ayuda, and various toolbar icons. The main area shows a database structure with a tree view of tables (47 total) under 'Estructura'. A table structure is shown for 'Tablas (47)' with columns Nombre, Tipo, and Esquema, all showing 'CREATE TABLE' for each entry. To the right, there is a 'Hoja de datos' (Data Grid) window titled 'Editar celda' (Edit cell) with a single cell containing 'NULL'. Below it, a message says 'No hay celda activa. Tipo: NULL; Tamaño: 0 bytes' and has an 'Aplicar' (Apply) button. Further down, there is a 'Remoto' (Remote) section with 'Identidad' (Identity) set to 'Selección una identidad para conectar' (Select a connection identity) and buttons for 'Cargar al servidor' (Load to server) and 'DBHub.io', 'Local', and 'Base de datos actual' (Current database). At the bottom, there is a table with columns Nombre, Última modificación (Last modification), and Tamaño (Size).

Se ha examinado el registro para auditar el ciclo de vida de las aplicaciones en el equipo:

- **Aplicaciones Activas (Applications):** La captura muestra el software UWP que reside actualmente en el sistema, como 3DBuilder y BingFinance.
- **Aplicaciones Eliminadas (Deleted):** Se ha localizado un historial extenso bajo la subclave Deleted (y Staged). Este hallazgo evidencia que aplicaciones como **Skype**, **ZuneVideo** o **BingSports** estuvieron presentes en el sistema anteriormente y fueron desinstaladas o desprovisionadas.

Se observa también la presencia simultánea de ciertas aplicaciones (ej. BingFinance) en ambas ramas. Esto se debe al **historial de actualizaciones del sistema**: las entradas en Deleted corresponden a versiones antiguas o paquetes base que fueron reemplazados por las versiones

más recientes listadas en Applications. Esto confirma no solo la instalación, sino el mantenimiento y actualización activa del software en el equipo.



The screenshot shows two windows side-by-side displaying registry keys from a dump. The left window shows the `AppxAllUserStore\Deleted\Staged` key, which contains numerous entries for Microsoft applications. The right window shows the `AppxAllUserStore\Deleted\Deleted` key, which is currently empty. Both windows have columns for name, value, and timestamp.

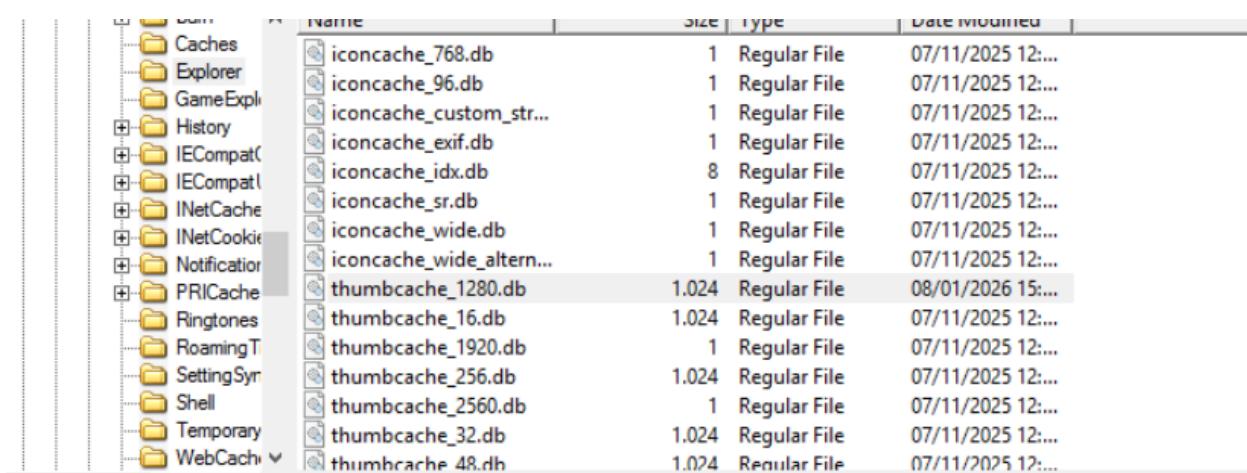
Name	Type	Value	Timestamp
Microsoft.3DBuilder_8wek...	File	0	2025-11-0
Microsoft.Appconnector_8...	File	0	2025-11-0
Microsoft.BingFinance_8w...	File	0	2025-11-0
Microsoft.BingNews_8wek...	File	0	2025-11-0
Microsoft.BingSports_8we...	File	0	2025-11-0
Microsoft.BingWeather_8...	File	0	2025-11-0
Microsoft.Getstarted_8we...	File	0	2025-11-0
Microsoft.MicrosoftSolitair...	File	0	2025-11-0
Microsoft.People_8wekyb...	File	0	2025-11-0
Microsoft.SkypeApp_kzf8...	File	0	2025-11-0
Microsoft.Windows.Photos...	File	0	2025-11-0
Microsoft.WindowsAlarms...	File	0	2025-11-0
Microsoft.WindowsCalcula...	File	0	2025-11-0
Microsoft.WindowsCamera...	File	0	2025-11-0
Microsoft.WindowsMaps_...	File	0	2025-11-0
Microsoft.WindowsSoundR...	File	0	2025-11-0
Microsoft.WindowsStore_...	File	0	2025-11-0
Microsoft.ZuneMusic_8we...	File	0	2025-11-0
Microsoft.ZuneVideo_8we...	File	0	2025-11-0
EndOfLife	File	0	2015-07-1
InboxApplications	File	1	2015-07-1

27. Thumbnails (thumbviewer) & Thumbcaché (thumbcacheviewer) Ficheros “thumbs.db”

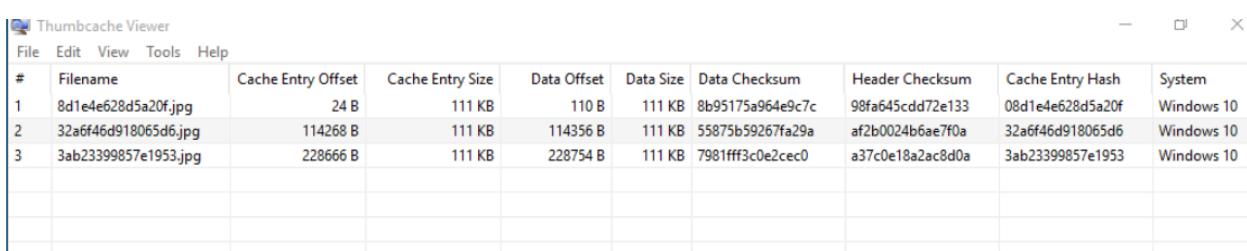
Se han localizado los ficheros de base de datos thumbcache_*.db en el directorio de caché del C:\Users\usuarioizv\AppData\Local\Microsoft\Windows\Explorer.

Mediante la herramienta **Thumbcache Viewer**, se ha procedido a la extracción del contenido de estas bases de datos. Como se observa en la captura de análisis, se han recuperado **3 registros de imágenes** (archivos JPG) que el usuario visualizó en el sistema.

La recuperación exitosa de estas miniaturas demuestra que el usuario tuvo acceso y visualizó dichos archivos gráficos. Estos artefactos persisten independientemente de si los archivos originales han sido borrados de la papelera de reciclaje, sirviendo como evidencia gráfica de la actividad del usuario.



	Name	Size	Type	Date Modified
	iconcache_768.db	1	Regular File	07/11/2025 12:...
	iconcache_96.db	1	Regular File	07/11/2025 12:...
	iconcache_custom_str...	1	Regular File	07/11/2025 12:...
	iconcache_exif.db	1	Regular File	07/11/2025 12:...
	iconcache_idx.db	8	Regular File	07/11/2025 12:...
	iconcache_sr.db	1	Regular File	07/11/2025 12:...
	iconcache_wide.db	1	Regular File	07/11/2025 12:...
	iconcache_wide_altern...	1	Regular File	07/11/2025 12:...
	thumbcache_1280.db	1.024	Regular File	08/01/2026 15:...
	thumbcache_16.db	1.024	Regular File	07/11/2025 12:...
	thumbcache_1920.db	1	Regular File	07/11/2025 12:...
	thumbcache_256.db	1.024	Regular File	07/11/2025 12:...
	thumbcache_2560.db	1	Regular File	07/11/2025 12:...
	thumbcache_32.db	1.024	Regular File	07/11/2025 12:...
	thumbcache_48.rlh	1.024	Regular File	07/11/2025 12:...



#	Filename	Cache Entry Offset	Cache Entry Size	Data Offset	Data Size	Data Checksum	Header Checksum	Cache Entry Hash	System
1	8d1e4e628d5a20f.jpg	24 B	111 KB	110 B	111 KB	8b95175a964e9c7c	98fa645cdd72e133	08d1e4e628d5a20f	Windows 10
2	32a6f46d918065d6.jpg	114268 B	111 KB	114356 B	111 KB	55875b59267fa29a	af2b0024b6ae7f0a	32a6f46d918065d6	Windows 10
3	3ab23399857e1953.jpg	228666 B	111 KB	228754 B	111 KB	7981fff3c0e2cec0	a37c0e18a2ac8d0a	3ab23399857e1953	Windows 10

28. Papelera de reciclaje(rifiuti)

Se ha examinado el directorio oculto C:\\$Recycle.Bin correspondiente al identificador de seguridad (SID) del usuario. El análisis revela la existencia de archivos eliminados que aún residen en el disco, identificados por la nomenclatura estándar de Windows:

- **Archivos de Metadatos (\$I):** Ficheros de índice que contienen la fecha exacta del borrado y la ruta original.
 - **Archivos de Datos (\$R):** Ficheros que contienen los datos íntegros recuperables (contenido real).

Para corroborar los hallazgos, se procesó el archivo de índice **\$I9FF6C5** utilizando la herramienta específica **rifiuti-vista.exe**. La ejecución arrojó los siguientes metadatos decodificados:

- **Ruta Original:** C:\Users\usuarioizv\Desktop\FORENSE
 - **Fecha de Borrado:** 08/01/2026 a las 16:16:46

Name	Size	Type	Date Modified
\$R9FF6C5	1	Directory	08/01/2026 15:54:13
SRDIIP2Y.1	1	Directory	08/01/2026 15:37:26
\$I30	4	NTFS Index All...	08/01/2026 16:16:46
\$I9FF6C5	1	Regular File	08/01/2026 16:16:46
SDIIP2Y.1	1	Regular File	08/01/2026 15:41:02
SIXU60TP	1	Regular File	08/01/2026 16:05:09
SRXU60TP	8.636	Regular File	08/01/2026 16:04:49
desktop.ini	1	Regular File	07/11/2025 12:47:36

00	02 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00
10	E0 31 6D 2F BA 80 DC 01-24 00 00 00 43 00 3A 00	δim/°-Ü-\$...C::-
20	5C 00 55 00 73 00 65 00-72 00 73 00 5C 00 75 00	\U-s-e-r-s\.\u-
30	73 00 75 00 61 00 72 00-69 00 6F 00 69 00 7A 00	s-u-a-r-i-o-i-z-
40	76 00 5C 00 44 00 65 00-73 00 6B 00 74 00 6F 00	v\.\D-e-s-k-t-o-
50	70 00 5C 00 46 00 4F 00-52 00 45 00 4E 00 53 00	p\.\F-O-R-E-N-S-
60	45 00 00 00	E...

```
C:\Users\usuarioizv\Desktop\rifiuti2-0.6.1-win\x64>"rifiuti-vista.exe" $I9FF6C5
Recycle bin path: '$I9FF6C5'
Version: 2

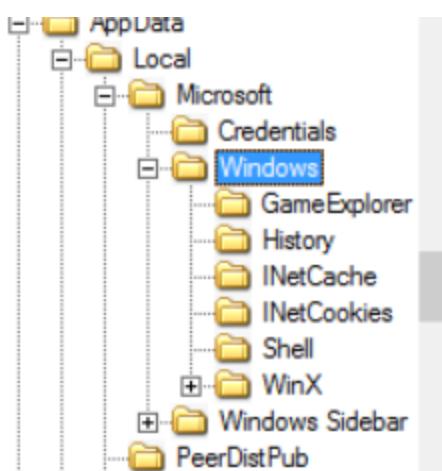
Index Deleted Time      Size     Path
$I9FF6C5           2026-01-08 16:16:46      0       C:\Users\usuarioizv\Desktop\FORENSE
```

29. OfficeFileCache

Al no tener instalado Office365 no se encuentran las claves de las rutas C:\Users\...\Office C:\Users\Office\16.0\BackstageInAppNavCach

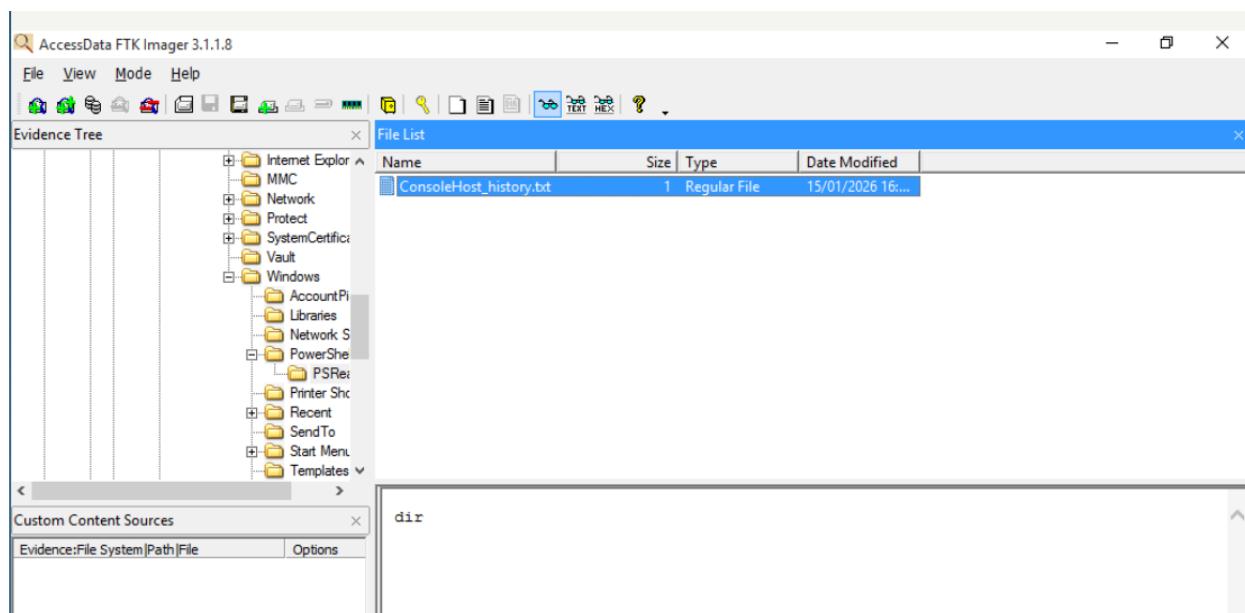
30. IP Pública (ETLParser)

Se ha navegado hasta la ruta del perfil de servicio de red C:\Windows\ServiceProfiles\...\DeliveryOptimization para localizar los registros del servicio de Optimización de Entrega. Como se evidencia en la captura, el directorio **DeliveryOptimization** no se encuentra presente en la estructura de archivos del sistema.



31. Histórico de PowerShell

Analizando C:\Users\usuarioizv...\PowerShell\PSReadLine\ConsoleHost_history.txt el historial de la consola de administración PowerShell mediante el archivo ConsoleHost_history.txt. El análisis del contenido en texto plano revela la ejecución del comando **dir** para listar el contenido de directorios.



32. Windows PREFETCH (PECmd)

Aunque la guía de referencia sugiere el uso de LECmd (herramienta diseñada para accesos directos LNK), para el análisis de artefactos Prefetch (.pf) se ha utilizado la herramienta correcta: **PECmd** de Eric Zimmerman.

1. **Identificación:** Se ha localizado el directorio Prefetch conteniendo los rastros de ejecución de aplicaciones.
2. **Extracción de Metadatos:** Se ha procesado el archivo AM_DELTA_PATCH...pf mediante la consola de comandos para verificar su actividad.

Como se observa en la captura de la terminal, la herramienta ha recuperado datos críticos que no son visibles en el explorador de archivos:

- **Run Count (Conteo de ejecución):** 1 (El programa se ejecutó una única vez).
- **Last Run (Última ejecución):** 08/01/2026 a las 17:24:42.
- **Files Referenced:** Se listan las librerías cargadas (DLLs) y rutas accedidas durante la ejecución, confirmando que el programa interactuó con el sistema de archivos (SYSTEM32, DRIVERS).

Name	Size	Type	Date Modified
AgGIUAD_P_S-1-5-21-...	4	File Slack	
AgGIUAD_S-1-5-21-35...	282	Regular File	14/01/2026 18:...
AgGIUAD_S-1-5-21-35...	3	File Slack	
AgRobust.db	180	Regular File	15/01/2026 16:...
AM_BASE.EXE-808FC8...	3	Regular File	08/01/2026 15:...
AM_DELTA.EXE-B7261...	3	Regular File	13/01/2026 15:...
AM_DELTA.EXE-B7261...	2	File Slack	
AM_DELTA_PATCH_1....	3	Regular File	08/01/2026 17:...
AM_DELTA_PATCH_1....	2	File Slack	
AM_DELTA_PATCH_1....	3	Regular File	14/01/2026 15:...
AM_DELTA_PATCH_1....	3	Regular File	15/01/2026 15:...
AM_DELTA_PATCH_1....	2	File Slack	
AM_ENGINE.EXE-69A...	3	Regular File	08/01/2026 15:...
APPLICATIONFRAME...	16	Regular File	15/01/2026 15:...
APPLICATIONFRAMF...	1	File Slack	

```
Run count: 1
Last run: 2026-01-08 17:24:42

Volume information:

#0: Name: \VOLUME{01dc4fe32f3b813c-ee2f66ab} Serial: EE2F66AB Created: 2025-11-07 12:36:48 Directories: 8 File references: 23

Directories referenced: 8

0: \VOLUME{01dc4fe32f3b813c-ee2f66ab}\WINDOWS
1: \VOLUME{01dc4fe32f3b813c-ee2f66ab}\WINDOWS\GLOBALIZATION
2: \VOLUME{01dc4fe32f3b813c-ee2f66ab}\WINDOWS\GLOBALIZATION\SORTING
3: \VOLUME{01dc4fe32f3b813c-ee2f66ab}\WINDOWS\SOFTWAREDISTRIBUTION
4: \VOLUME{01dc4fe32f3b813c-ee2f66ab}\WINDOWS\SOFTWAREDISTRIBUTION\DOWNLOAD
5: \VOLUME{01dc4fe32f3b813c-ee2f66ab}\WINDOWS\SOFTWAREDISTRIBUTION\DOWNLOAD\INSTALL
6: \VOLUME{01dc4fe32f3b813c-ee2f66ab}\WINDOWS\SYSTEM32
7: \VOLUME{01dc4fe32f3b813c-ee2f66ab}\WINDOWS\SYSTEM32\DRIVERS

Files referenced: 15

00: \VOLUME{01dc4fe32f3b813c-ee2f66ab}\WINDOWS\SYSTEM32\NTDLL.DLL
01: \VOLUME{01dc4fe32f3b813c-ee2f66ab}\WINDOWS\SOFTWAREDISTRIBUTION\INSTALL\AM_DELTA_PATCH_1.443.561.0.EXE
02: \VOLUME{01dc4fe32f3b813c-ee2f66ab}\WINDOWS\SYSTEM32\KERNEL32.DLL
03: \VOLUME{01dc4fe32f3b813c-ee2f66ab}\WINDOWS\SYSTEM32\KERNELBASE.DLL
04: \VOLUME{01dc4fe32f3b813c-ee2f66ab}\WINDOWS\SYSTEM32\LOCALE.NLS
05: \VOLUME{01dc4fe32f3b813c-ee2f66ab}\WINDOWS\SYSTEM32\ADVAPI32.DLL
06: \VOLUME{01dc4fe32f3b813c-ee2f66ab}\WINDOWS\SYSTEM32\MSVCR7.DLL
07: \VOLUME{01dc4fe32f3b813c-ee2f66ab}\WINDOWS\SYSTEM32\SECHOST.DLL
08: \VOLUME{01dc4fe32f3b813c-ee2f66ab}\WINDOWS\SYSTEM32\RPCRT4.DLL
09: \VOLUME{01dc4fe32f3b813c-ee2f66ab}\WINDOWS\SYSTEM32\VERSION.DLL
10: \VOLUME{01dc4fe32f3b813c-ee2f66ab}\WINDOWS\SYSTEM32\BCRYPTPRIMITIVES.DLL
11: \VOLUME{01dc4fe32f3b813c-ee2f66ab}\WINDOWS\GLOBALIZATION\SORTING\SORTDEFAULT.NLS
12: \VOLUME{01dc4fe32f3b813c-ee2f66ab}\WINDOWS\SYSTEM32\WUAUCLT.EXE
13: \VOLUME{01dc4fe32f3b813c-ee2f66ab}\WINDOWS\SYSTEM32\MPSIGSTUB.EXE
14: \VOLUME{01dc4fe32f3b813c-ee2f66ab}\WINDOWS\SYSTEM32\DRIVERS\NPSVCTRIG.SYS
```

33. Windows SuperFetch (Crowndresponse)

Se ha verificado la existencia de las bases de datos en la ruta C:\Windows\Prefetch\Ag*.db [AgAppLaunch.db](#) AgGlGlobalHistory.db mediante la ejecución de **CrowdResponse** y el comando @DirList para validar la capacidad de recolección de artefactos en el entorno. La salida XML confirma la estructura de datos que genera la herramienta al localizar estos ficheros.

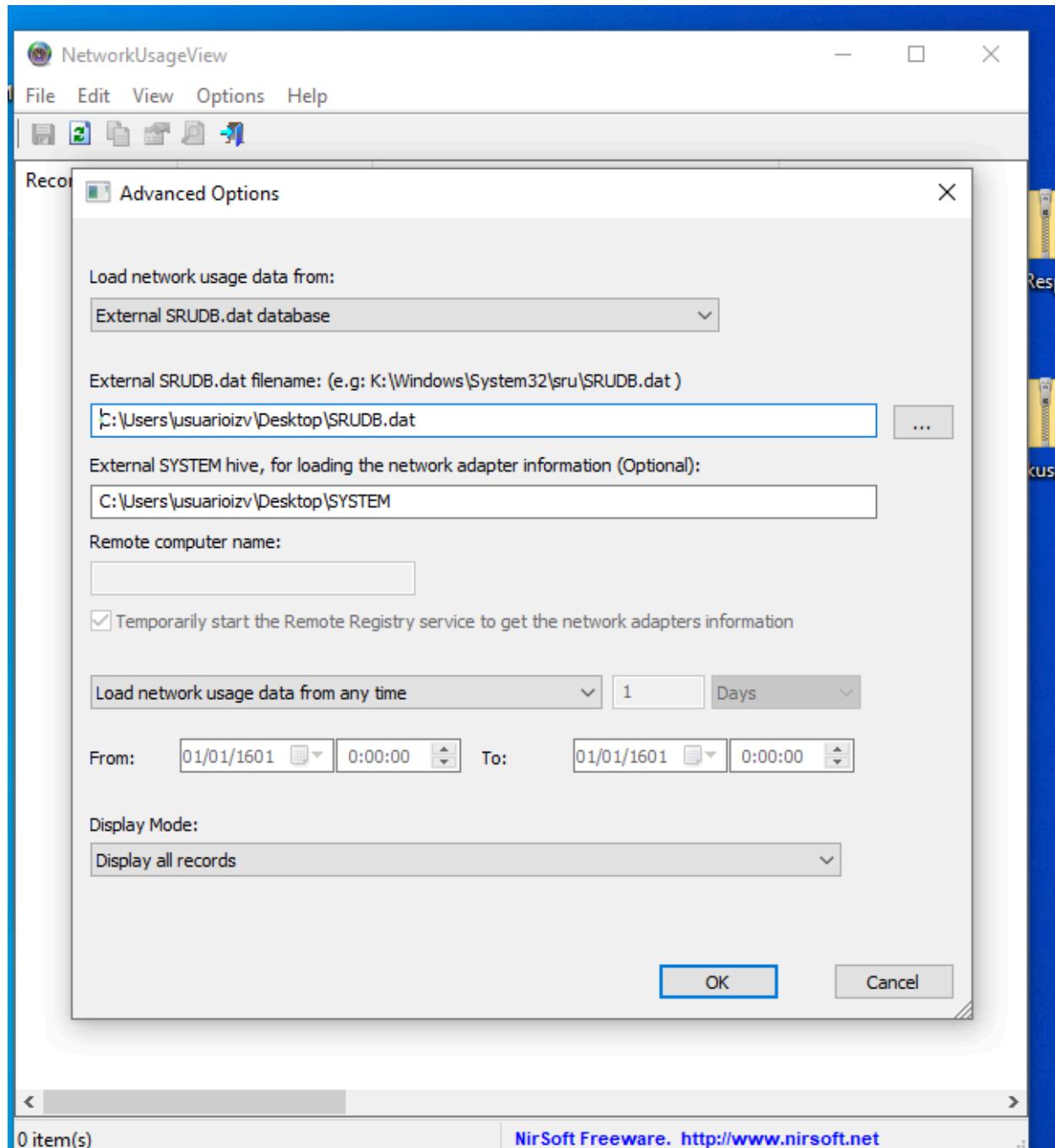
```
C:\Users\usuarioizv\Desktop\CrowdResponse\CrowdResponse>"CrowdResponse.exe" @DirList "C:\Windows\Prefetch" -f "Ag*.db"
<?xml version="1.0" encoding="utf-8"?>
<system>
<timestamp_utc>2026-01-15T17:18:16Z</timestamp_utc>
<timestamp_local>2026-01-15T18:18:16Z</timestamp_local>
<timezone>Hora est&#225;ndar romance</timezone>
<ipv4>172.25.100.238</ipv4>
<macv4>BC-24-11-39-C7-C7</macv4>
<ipv6>fe80::f1ca:4e60:8a68:b1dc</ipv6>
<macv6>BC-24-11-39-C7-C7</macv6>
<netbios>DESKTOP-R9QG404</netbios>
<domain>WORKGROUP</domain>
<dns>DESKTOP-R9QG404</dns>
<os>Windows 10 Pro</os>
<osinstall>2025-11-07T12:45:03Z</osinstall>
<csid>NoCSID</csid>
<agid>NoAGID</agid>
<iswow64process>FALSE</iswow64process>
<is64bitOS>TRUE</is64bitOS>
<isAdmin>TRUE</isAdmin>
<output>console</output>
<version>1.0.6.0</version>
<tools>
```

34. SRUM (SRUM DUMP y NetworkUsageView)

Se ha analizado el archivo C:\Windows\System32\sru\SRUDB.dat utilizando la herramienta especializada **NetworkUsageView**, cargando correctamente los hives de registro auxiliares.

- Tamaño del Artefacto:** El fichero presenta un tamaño de **960 KB**. En bases de datos ESE (Extensible Storage Engine), este tamaño corresponde a la estructura inicial reservada por el sistema sin contenido de usuario significativo. Una base de datos con actividad real de 30 días superaría habitualmente los 10-20 MB.
- Resultado de la Herramienta:** La ejecución de NetworkUsageView con la configuración correcta devuelve **0 registros**.

Se determina que el servicio SRUM fue reiniciado o no llegó a escribir datos de tráfico de red en el disco antes de la captura de la imagen. La evidencia confirma la ausencia de historial recuperable en este artefacto específico.



35. ShimCache (AppCompatCacheParser)

Se ha procesado el hive SYSTEM mediante la herramienta **AppCompatCacheParser**. Debido a que el archivo original se encontraba en estado inconsistente (*Dirty Hive*), fue necesario inyectar los archivos de transacción (SYSTEM.LOG1 y SYSTEM.LOG2) recuperados manualmente para reconstruir la integridad del registro y permitir la extracción del CSV. El análisis del artefacto ShimCache ha revelado la existencia histórica de ejecutables clave, independientemente de si siguen presentes en el disco:

- Software de Anonymización/VPN:** Se ha detectado la presencia de **wireguard-installer.exe** en el escritorio del usuario alumnotizv (Fecha modif: 19/01/2026). Este hallazgo es relevante forensemente ya que el uso de VPNs no autorizadas puede indicar intentos de evasión de controles de red o exfiltración de datos.
- Ejecución desde Directorios Temporales:** Se observa una alta actividad de ejecución de binarios desde rutas volátiles (AppData\Local\Temp), patrón común tanto en instaladores legítimos (como se observa con *CodeSetup*) como en fases iniciales de compromiso por malware (droppers).

```
PS C:\Users\alumnotizv\Desktop\AppCompatCacheParser> ./AppCompatCacheParser.exe -f SYSTEM --csv . --csvf INFORME_SHIMCACHE.csv
AppCompat Cache Parser version 1.3.1.0
Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/AppCompatCacheParser
Command line: -f SYSTEM --csv . --csvf INFORME_SHIMCACHE.csv
Processing hive 'SYSTEM'
Two transaction logs found. Determining primary log...
Primary log: C:\Users\alumnotizv\Desktop\AppCompatCacheParser\SYSTEM.LOG2, secondary log: C:\Users\alumnotizv\Desktop\AppCompatCacheParser\SYSTEM.LOG1
Replaying log file: C:\Users\alumnotizv\Desktop\AppCompatCacheParser\SYSTEM.LOG2
Replaying log file: C:\Users\alumnotizv\Desktop\AppCompatCacheParser\SYSTEM.LOG1
At least one transaction log was applied. Sequence numbers have been added to 0x5898. New Checksum: 0xE499116
An bin header incorrect at absolute offset 0xF48000!!! Percent done: 98,59 %
An expected value was not found at offset 0x027A10. Key: ROOT\ControlSet001\Enum\SWD\MSRRAS\MS_AGILEVPNMINIPORT\Properties\{83da6326-97a6-4088-9453-a1923f573b29}\0067
An expected value was not found at offset 0x627A50. Key: ROOT\ControlSet001\Enum\SWD\MSRRAS\MS_L2TPMINIPORT\Properties\{83da6326-97a6-4088-9453-a1923f573b29}\0067
An expected value was not found at offset 0x627A68. Key: ROOT\ControlSet001\Enum\SWD\MSRRAS\MS_PPTPMINIPORT\Properties\{83da6326-97a6-4088-9453-a1923f573b29}\0067
An expected value was not found at offset 0x1D3088. Key: ROOT\ControlSet001\Enum\SWD\MSRRAS\MS_SSTPMINIPORT\Properties\{83da6326-97a6-4088-9453-a1923f573b29}\0067
An expected value was not found at offset 0x677E00. Key: ROOT\ControlSet001\services\bam\state\UserSettings\S-1-5-21-4030796697-2866726945-1028266273\1002
An expected value was not found at offset 0x677118. Key: ROOT\ControlSet001\services\bam\state\UserSettings\S-1-5-21-4030796697-2866726945-1028266273\1002
An expected value was not found at offset 0x5EDAC8. Key: ROOT\ControlSet001\services\bam\state\UserSettings\S-1-5-21-4030796697-2866726945-1028266273\1002
Extra, non-zero data found beyond hive length! Check for erroneous data starting at 0xF48000!
Found 1,024 cache entries for Windows10C_11 in ControlSet001
Results saved to './INFORME_SHIMCACHE.csv'

PS C:\Users\alumnotizv\Desktop\AppCompatCacheParser>
```

36. AmCache (AmCacheParser)

Para el análisis de este artefacto, se extrajo el archivo C:\Windows\AppCompat\Programas\Amcache.hve. Siguiendo el protocolo establecido tras la incidencia con la ShimCache, se trajeron preventivamente los archivos de transacción (Amcache.hve.LOG1 y .LOG2) para evitar errores de inconsistencia ("Dirty Hive"). Posteriormente, se procesaron con **AmCacheParser**, generando reportes detallados de ejecución. El reporte UnassociatedFileEntries.csv ha revelado información crítica que complementa a la ShimCache:

1. **Identificación Univoca (SHA1):** A diferencia de otros artefactos, AmCache ha registrado el hash SHA1 de los ejecutables. Esto permitiría contrastar cualquier binario sospechoso con bases de datos de inteligencia de amenazas (como VirusTotal) para confirmar si es malicioso.
 2. **Registro de Actividad Reciente:** Se ha identificado la ejecución de herramientas administrativas y de instalación recientes, como:

- aspnetcore-runtime-9.0.0-win-x64.exe (Instalación de librerías del sistema).
- AppCompatCacheParser.exe (Herramientas forenses ejecutadas en el sistema).
- cdbxp_setup...exe (Software de grabación CDBurnerXP).

3. Rutas de Ejecución:

Se confirman ejecuciones desde rutas de usuario

(C:\Users\alumnotizv\Downloads\)) y carpetas temporales, lo que permite trazar el origen de los ficheros descargados.

```
PS C:\Users\alumnotizv\Desktop\AmcacheParser> .\AmCacheParser.exe -f Amcache.hve --csv . --csvf INFORME_AMCACHE.csv
AmcacheParser version 1.5.2.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/AmcacheParser

Command line: -f Amcache.hve --csv . --csvf INFORME_AMCACHE.csv

Warning: Administrator privileges not found!

Two transaction logs found. Determining primary log...
Primary log: C:\Users\alumnotizv\Desktop\AmcacheParser\Amcache.hve.LOG2, secondary log: C:\Users\alumnotizv\Desktop\AmcacheParser\Amcache.hve.LOG1
Replaying log file: C:\Users\alumnotizv\Desktop\AmcacheParser\Amcache.hve.LOG2
Replaying log file: C:\Users\alumnotizv\Desktop\AmcacheParser\Amcache.hve.LOG1
At least one transaction log was applied. Sequence numbers have been updated to 0x2AF1. New Checksum: 0x5C5EA0F6
hbini header incorrect at absolute offset 0x3C3000!!! Percent done: 94,04 %
Extra, non-zero data found beyond hive length! Check for erroneous data starting at 0x3C3000!
Two transaction logs found. Determining primary log...
Primary log: C:\Users\alumnotizv\Desktop\AmcacheParser\Amcache.hve.LOG2, secondary log: C:\Users\alumnotizv\Desktop\AmcacheParser\Amcache.hve.LOG1
Replaying log file: C:\Users\alumnotizv\Desktop\AmcacheParser\Amcache.hve.LOG2
Replaying log file: C:\Users\alumnotizv\Desktop\AmcacheParser\Amcache.hve.LOG1
At least one transaction log was applied. Sequence numbers have been updated to 0x2AF1. New Checksum: 0x5C5EA0F6
hbini header incorrect at absolute offset 0x3C3000!!! Percent done: 94,04 %
Extra, non-zero data found beyond hive length! Check for erroneous data starting at 0x3C3000!
Error parsing FileEntry at {11517B7C-E79D-4e20-961B-75A811715ADD}\Root\Inventory\ApplicationFile\brave.exe|8c8c518236b6c059. Error: No se puede reconocer la cadena como valor DateTime válido.
System.FormatException: No se puede reconocer la cadena como valor DateTime válido.
   en Amcache.AmcacheNew..ctor(String hive, Boolean recoverDeleted, Boolean noLogs)
Please send the following text to saericzimmerman@gmail.com
Key data: Key Name: brave.exe|8c8c518236b6c059
Key Path: {11517B7C-E79D-4e20-961B-75A811715ADD}\Root\Inventory\ApplicationFile\brave.exe|8c8c518236b6c059

Last Write Time: 19/01/2026 7:28:19 +00:00
Key Flags: HasActiveParent

NW Record: Size: 0x70
Relative Offset: 0x10F10
Absolute Offset: 0x11F10
Signature: nk
Flags: CompressedName
Name: brave.exe|8c8c518236b6c059
```

 INFORME_AMCACHE_DeviceContainers	20/01/2026 19:25	Archivo de valores...	8 KB
 INFORME_AMCACHE_DevicePnps	20/01/2026 19:25	Archivo de valores...	80 KB
 INFORME_AMCACHE_DriveBinaries	20/01/2026 19:25	Archivo de valores...	129 KB
 INFORME_AMCACHE_DriverPackages	20/01/2026 19:25	Archivo de valores...	10 KB
 INFORME_AMCACHE_ShortCuts	20/01/2026 19:25	Archivo de valores...	23 KB
 INFORME_AMCACHE_UnassociatedFileE...	20/01/2026 19:25	Archivo de valores...	157 KB

37. Tareas programadas

Se ha auditado el directorio de tareas programadas con el objetivo de identificar mecanismos de persistencia (ejecución automática). El análisis se ha centrado en **cruzar los datos** obtenidos anteriormente en la ShimCache y AmCache:

- Búsqueda de Malware/VPN:** Se ha verificado la existencia de tareas asociadas al instalador **wireguard-installer.exe** detectado previamente. La ausencia de una tarea programada con este nombre sugiere que el software podría haber sido instalado sin configurar actualizaciones automáticas o que fue ejecutado en modo "portable/standalone".
- Ruido del Sistema:** Se observan múltiples tareas legítimas de mantenimiento asociadas a MicrosoftEdgeUpdate y OneDrive (visibles en la captura). Estas son tareas estándar en entornos Windows y no se consideran indicadores de compromiso (IOCs) por sí mismas.

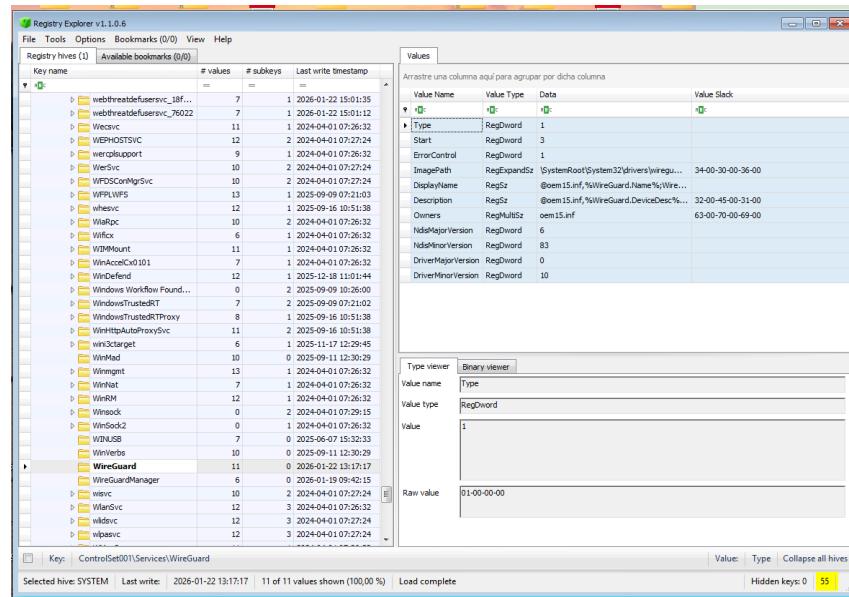
No se han hallado tareas programadas anómalas en la raíz del directorio que indique un intento de persistencia activo por parte de binarios desconocidos en el momento de la adquisición.

Name	Size	Type	Date Modified
GoogleSystem	1	Directory	09/09/2025 8:0...
GoogleUserPEH	1	Directory	09/12/2025 7:3...
Microsoft	1	Directory	29/09/2025 7:2...
Mozilla	1	Directory	12/01/2026 17:...
\$I30	8	NTFS Index All...	20/01/2026 7:2...
BraveSoftwareUpdate...	4	Regular File	16/09/2025 6:2...
BraveSoftwareUpdate...	4	Regular File	16/09/2025 6:2...
MicrosoftEdgeUpdate...	4	Regular File	07/01/2026 8:5...
MicrosoftEdgeUpdate...	4	Regular File	07/01/2026 8:5...
OneDrive Per-Machin...	4	Regular File	20/01/2026 7:2...
OneDrive Reporting T...	4	Regular File	20/01/2026 7:2...
OneDrive Reporting T...	4	Regular File	20/01/2026 7:2...
OneDrive Reporting T...	4	Regular File	20/01/2026 7:2...
OneDrive Reporting T...	4	Regular File	20/01/2026 7:2...
OneDrive Startup Task...	4	Regular File	20/01/2026 7:2...
OneDrive Startup Task...	4	Regular File	20/01/2026 7:2...
OneDrive Startup Task...	4	Regular File	20/01/2026 7:2...
OneDrive Startup Task...	4	Regular File	20/01/2026 7:2...

38. Servicios (Registry Explorer)

Analizando el registro SYSTEM\ControlSet001\Services se han localizado muchas carpetas. En concreto nos hemos centrado en una entrada crítica de los servicios del sistema correspondiente al software de tunelización **WireGuard**.

- **Nombre del Servicio:** WireGuard (Visible en DisplayName).
- **Tipo de Servicio (Type: 1):** Se trata de un **Kernel Driver** (Controlador de modo núcleo). Esto confirma que la instalación se realizó con **privilegios administrativos elevados**, ya que un usuario estándar no tiene permisos para registrar controladores en el sistema.
- **Ruta del Binario (ImagePath):** Apunta a \SystemRoot\System32\drivers\wireguard.sys. El archivo malicioso o de la herramienta reside en el directorio protegido de drivers de Windows.
- **Modo de Inicio (Start: 3):** El valor 3 indica un inicio **Manual** (Demand Start). Esto sugiere que el servicio no arranca automáticamente con el sistema, sino que es invocado bajo demanda cuando la aplicación WireGuard es ejecutada por el usuario o por otro proceso.



39. BAM (DCode)

Para garantizar la exactitud de la evidencia y no depender exclusivamente de parsers automáticos, se ha procedido a la decodificación manual del valor RegBinary.

1. Extracción del Dato: Se localizó la entrada correspondiente al navegador:

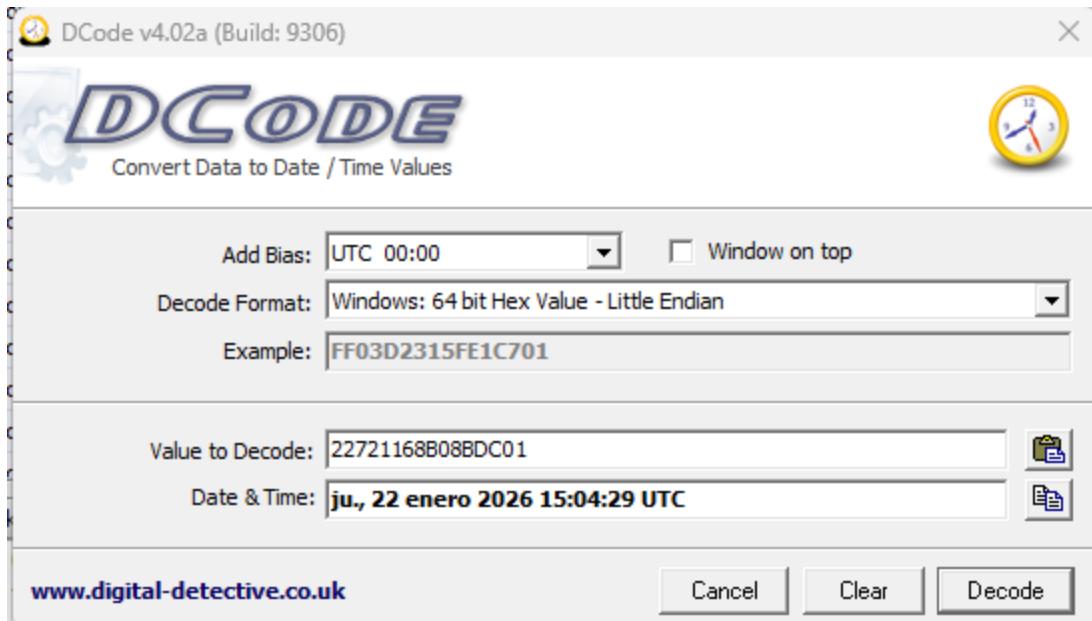
- **Ruta registrada:** \Device\HarddiskVolume3\Program Files\Mozilla Firefox\firefox.exe (Ruta típica de volumen físico).

2. Decodificación (Timestamp): Se extrajo la secuencia hexadecimal cruda y se procesaron los primeros 8 bytes (22 72 11 68 B0 8B DC 01) con la herramienta **DCode**, utilizando el formato estándar de Windows **64-bit Hex Value (LittleEndian)**.

La decodificación ha revelado la fecha exacta de última ejecución:

- **Fecha:** 22 de enero de 2026
- **Hora:** 15:04:29 (UTC+1/Local)

Value Name	Type	Value
Version	RegDword	1
SequenceNumber	RegBinary	59
Microsoft.Windows.StartMenuExperienceHost_cw5n1h2tbyewy	RegBinary	
Microsoft.Windows.Client.CBS_cw5n1h2tbyewy	RegBinary	
Microsoft.Windows.CloudExperienceHost_cw5n1h2tbyewy	RegBinary	
Microsoft.Windows.ShellExperienceHost_cw5n1h2tbyewy	RegBinary	
windows.immersivecontrolpanel_cw5n1h2tbyewy	RegBinary	
Microsoft.Windows.Client.WebExperience_cw5n1h2tbyewy	RegBinary	
Microsoft.Windows.Notepad_cw5kvb3d8bbwe	RegBinary	
Microsoft.XboxGamingOverlay_bvekyb3d8bbwe	RegBinary	
Microsoft.ScreenSketch_bvekyb3d8bbwe	RegBinary	
Microsoft.LockApp_cw5n1h2tbyewy	RegBinary	
Microsoft.WindowsStore_bvekyb3d8bbwe	RegBinary	
Microsoft.MicrosoftOfficeHub_bvekyb3d8bbwe	RegBinary	
Microsoft.WindowsTerminal_bvekyb3d8bbwe	RegBinary	



40. Eventos (Event-Log Explorer)

El archivo System.evtx fue localizado y recuperado de la ruta del sistema: C:\Windows\system32\winevt\Logs. Tras su análisis en el Visor de Eventos, se identificó una entrada crítica de nivel "Error" generada por el módulo TPM-WMI.

Se examinó el Event ID 1801, el cual reporta una discrepancia en los certificados de arranque seguro ("Updated Secure Boot certificates are available...") y expone metadatos identificativos del hardware (Fabricante: TICNOVA, Modelo: E70 SFF).

La marca de tiempo del evento confirma la actividad del sistema operativo en el instante preciso:

- **Fecha:** 22 de enero de 2026
- **Hora:** 16:06:14 (Hora Local)

The screenshot shows the Windows Event Viewer interface. On the left, there's a navigation pane with options like 'Visor de eventos (local)', 'Vistas personalizadas', 'Registros de Windows', 'Registros de aplicaciones y servicios', 'Registros guardados', 'System' (which is selected), and 'Suscripciones'. The main area displays a table of events under the 'System' category. The table has columns for 'Nivel' (Level), 'Fecha y hora' (Date and Time), 'Origen' (Source), 'Id. del evento' (Event ID), and 'Categoría...' (Category...). Most events are 'Información' level, with one 'Error' event (Event ID 1801) highlighted. The details pane on the right shows the properties for this error event, including its source as 'TPM-WMI' and its message: 'Updated Secure Boot certificates are available on this device but have not yet been applied to the firmware. Review the published guidance to complete the update and maintain full protection. This device signature information is included here.' It also lists other event details like 'Nombre de registro: Sistema', 'Origen: TPM-WMI', 'Registrado: 22/01/2026 16:06', etc.