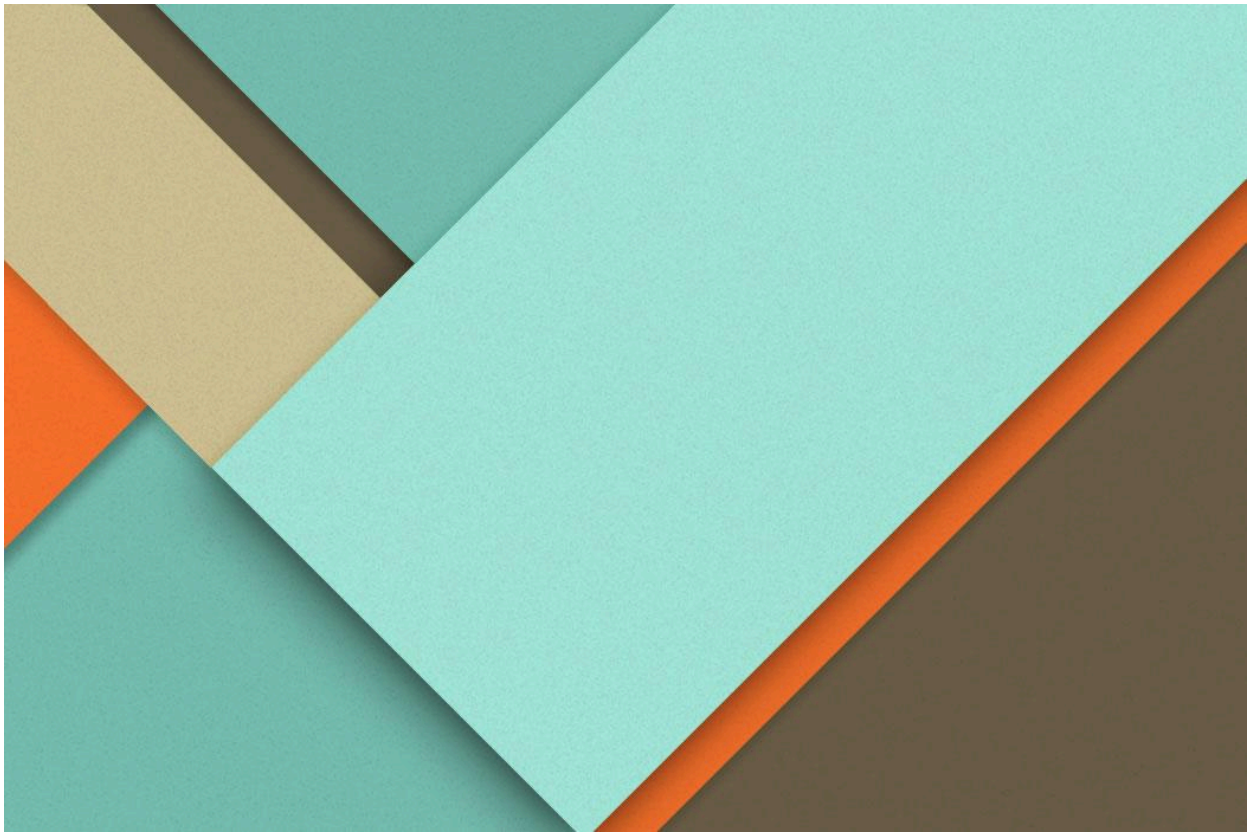


Análisis Post-mortem, los artefactos Windows

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

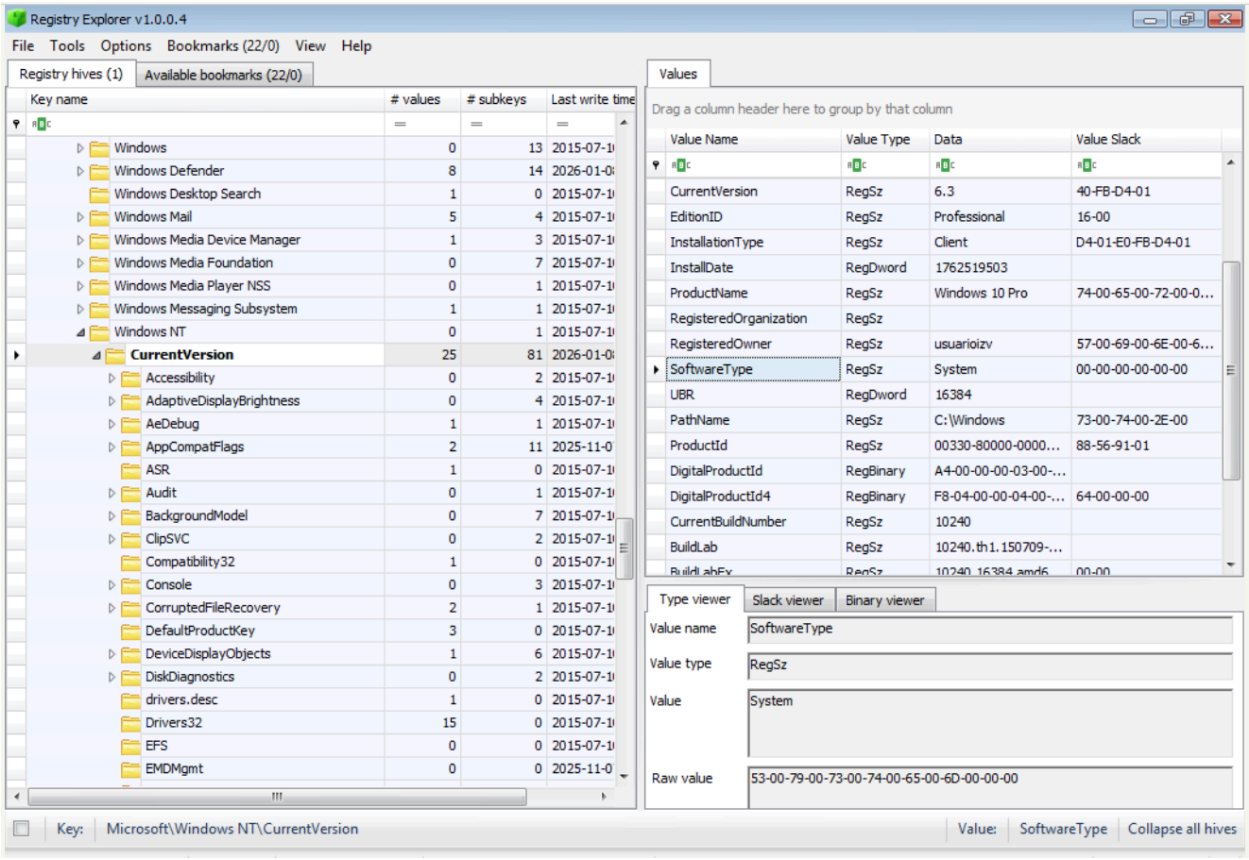
- ☐ **Imagen y montaje:** FTK Imager
- ☐ **Registro:** Registry Explorer
- ☐ **Prefetch:** PECmd (de Eric Zimmerman).
- ☐ **Logs de Eventos:** Event-Log de Windows.
- ☐ **Accesos directos (LNK):** LinkParser.
- ☐ **Jumplists:** JumpListExplorer.
- ☐ **Shellbags (Navegación de carpetas):** Shellbag Explorer.
- ☐ **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.



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
(default)	RegSz	mnmsrvc	02-00-78-00
ComputerName	RegSz	DESKTOP-R9QG4O4	00-00-00-00

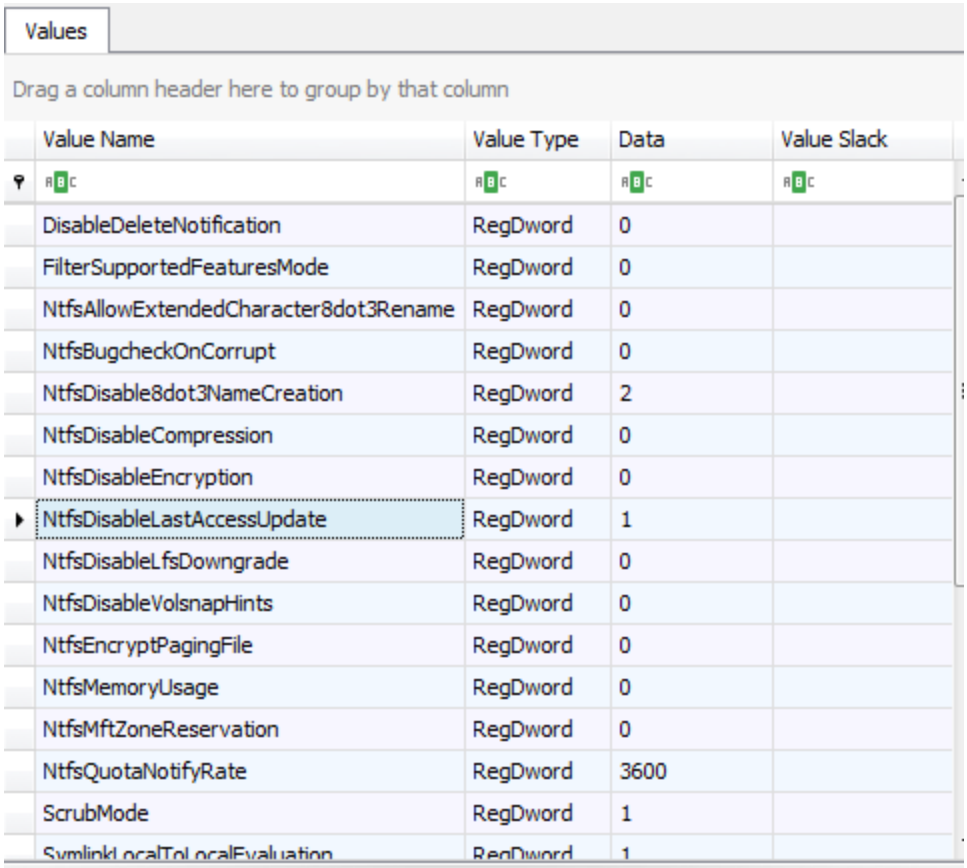
System\ControlSet001\Control\TimeZoneInformation, se observa que el equipo está configurado en la zona horaria **Romance Standard Time** (Hora estándar romance).

Value Name	Value Data	Value Data Raw
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	00-00-03-00-05-00-02-00-00-00-00-00-00-00-00-00
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-00-05-00-03-00-00-00-00-00-00-00-00-00
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.



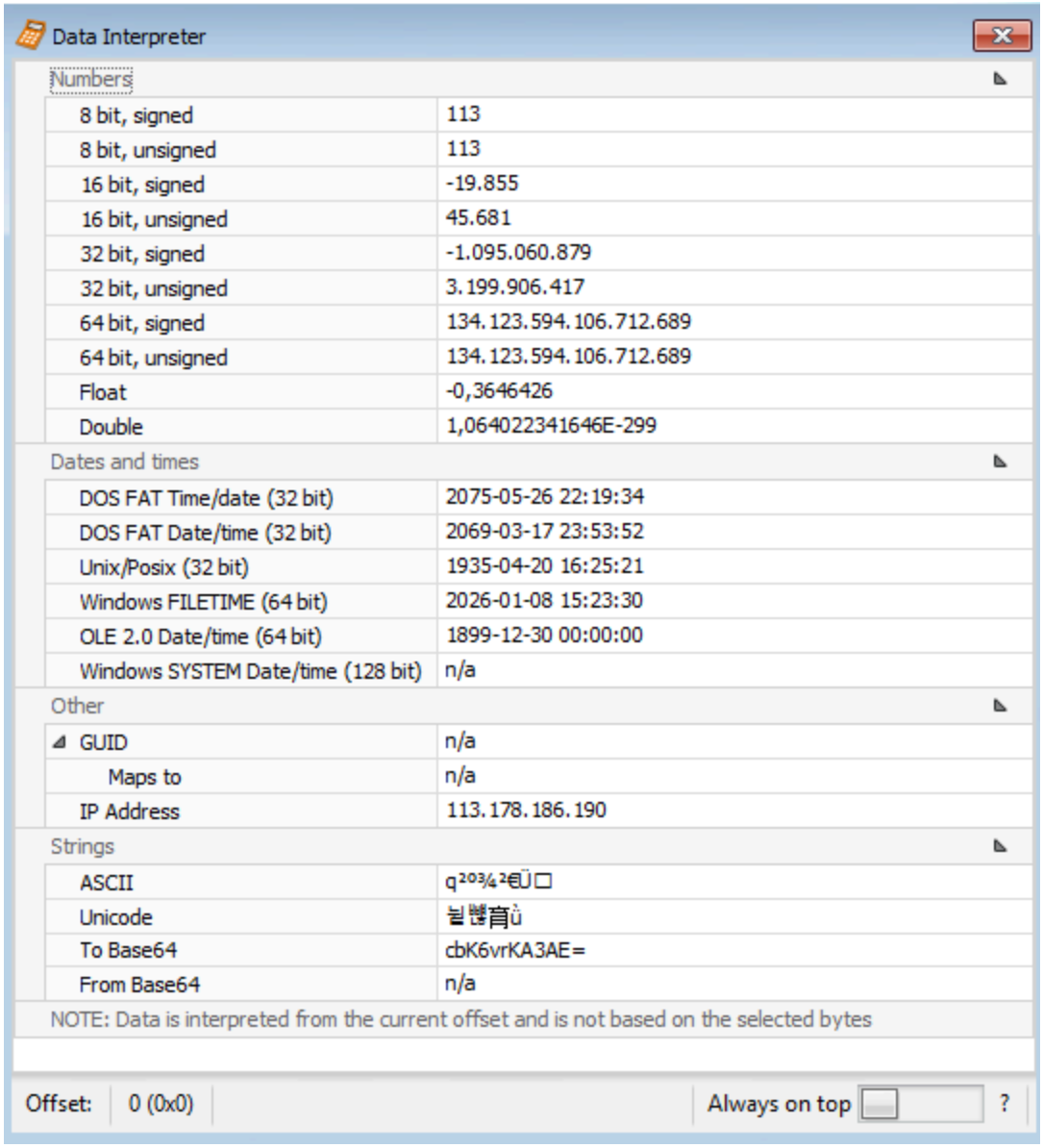
Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack
DisableDeleteNotification	RegDword	0	
FilterSupportedFeaturesMode	RegDword	0	
NtfsAllowExtendedCharacter8dot3Rename	RegDword	0	
NtfsBugcheckOnCorrupt	RegDword	0	
NtfsDisable8dot3NameCreation	RegDword	2	
NtfsDisableCompression	RegDword	0	
NtfsDisableEncryption	RegDword	0	
NtfsDisableLastAccessUpdate	RegDword	1	
NtfsDisableLfsDowngrade	RegDword	0	
NtfsDisableVolsnapHints	RegDword	0	
NtfsEncryptPagingFile	RegDword	0	
NtfsMemoryUsage	RegDword	0	
NtfsMftZoneReservation	RegDword	0	
NtfsQuotaNotifyRate	RegDword	3600	
ScrubMode	RegDword	1	
SymlinkLocalToLocalEvaluation	RegDword	1	

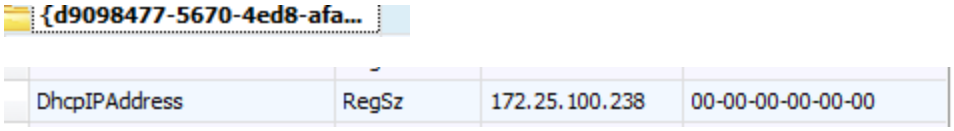
3. Hora de apagado

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).



4. Interfaces de red

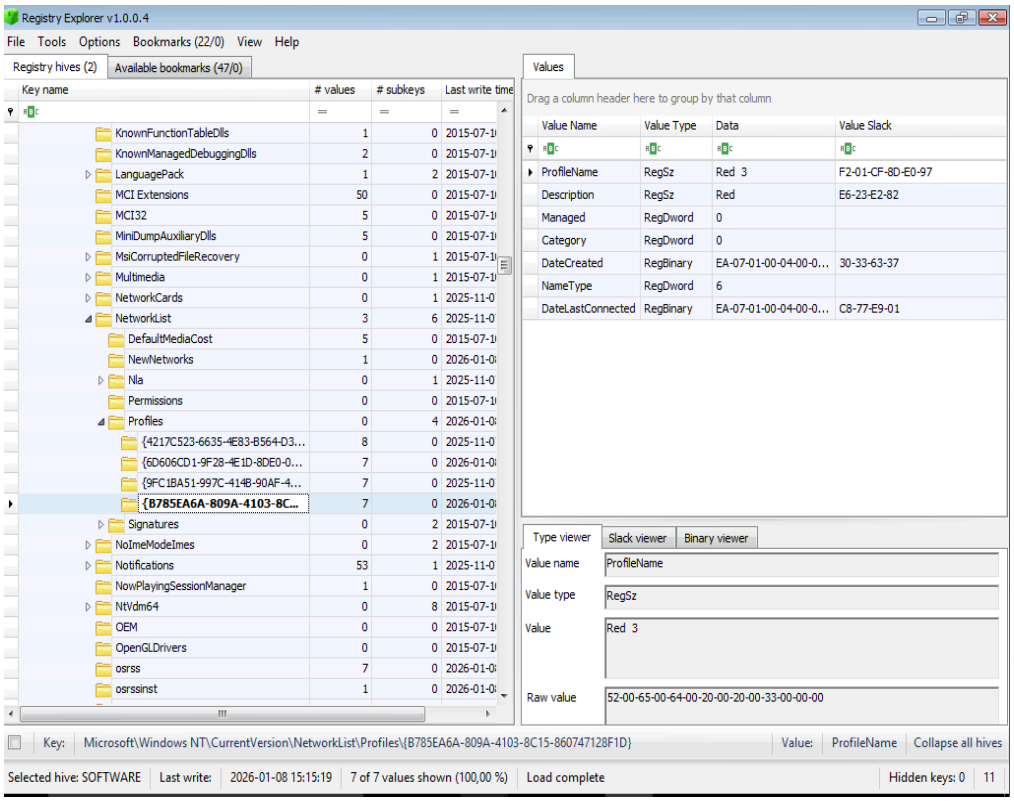
Se han analizado las interfaces de red configuradas en el equipo a través de la ruta System\ControlSet001\Services\Tcpip\Parameters\Interfaces .Se ha identificado una interfaz activa con GUID {d9098477-5670-4ed8-afa9-36cad4b49736}. Esta interfaz tenía asignada la dirección IPv4 **172.25.100.238**, lo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



5. Histórico de redes

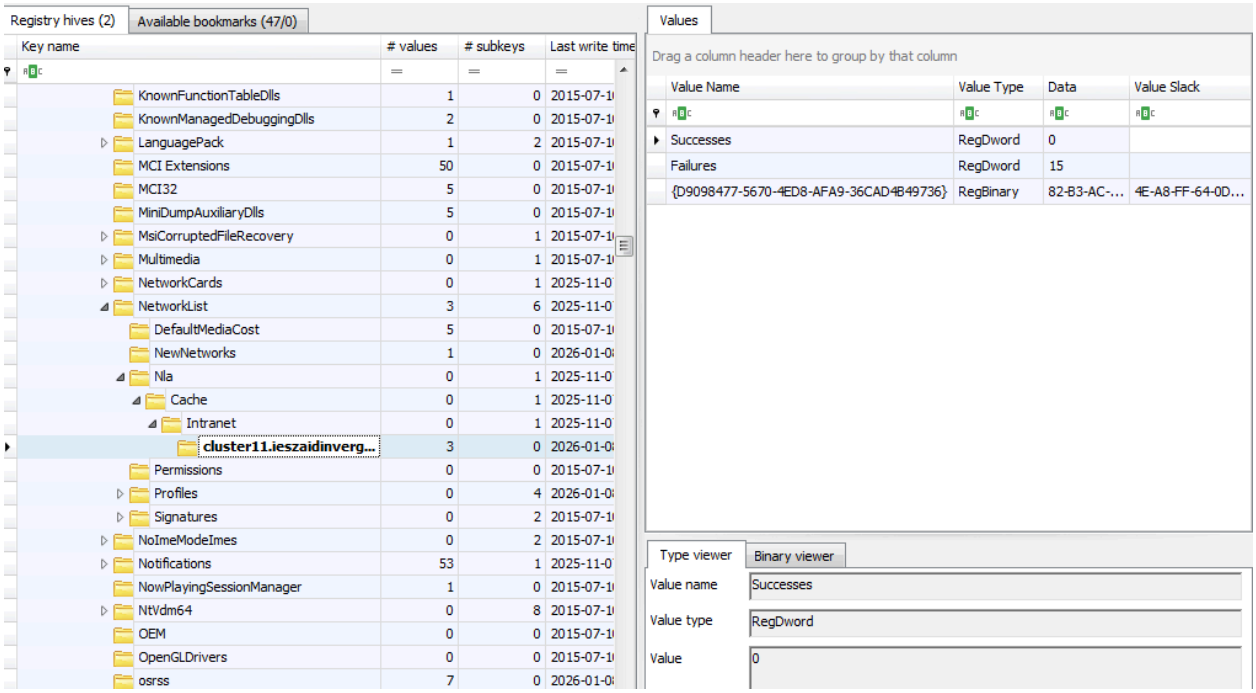
   a. Software\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles

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.



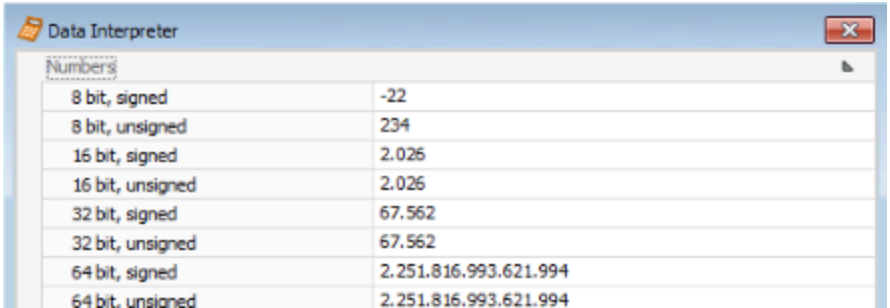
b. Software\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Cache

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).



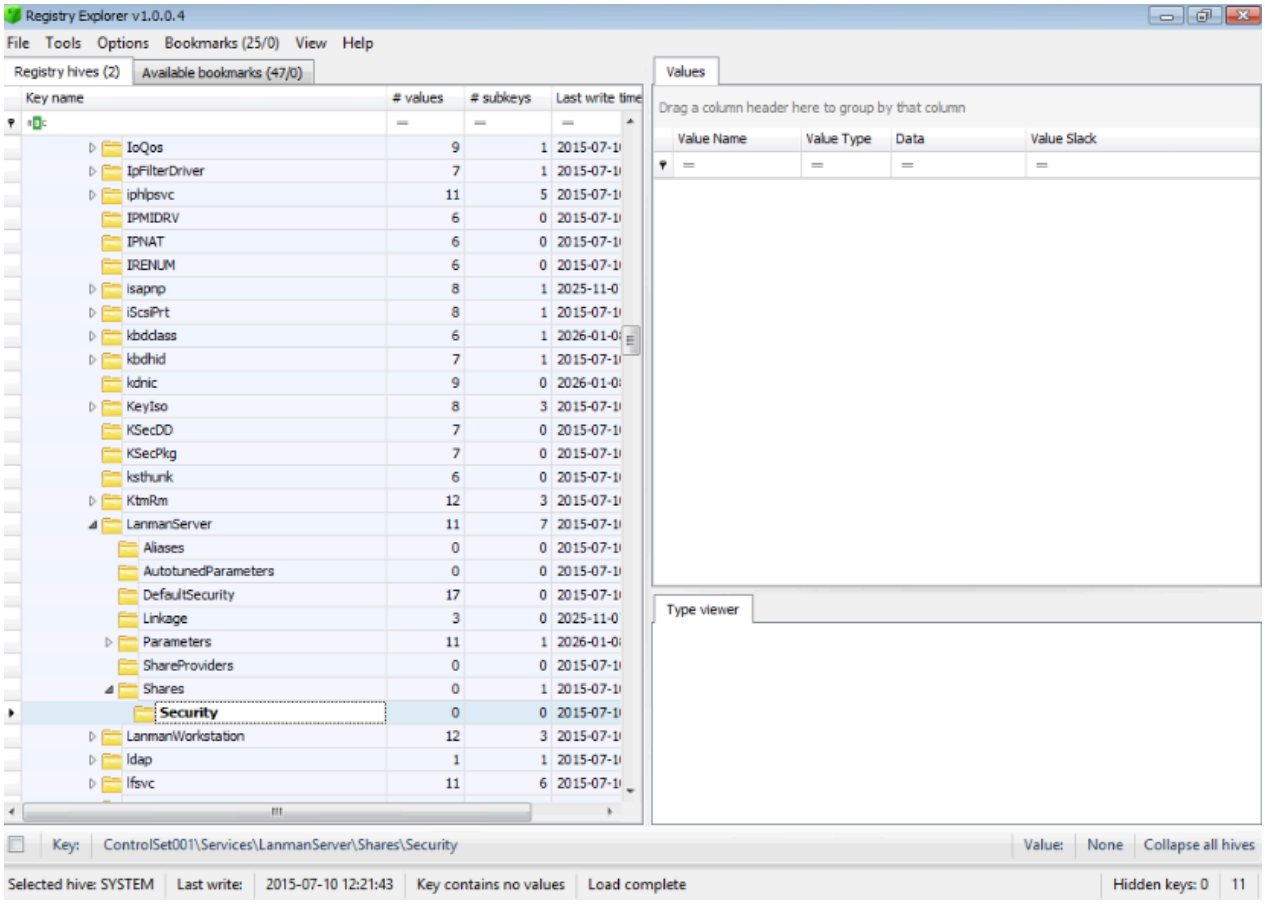
6. Cuándo se conectó a una red

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**.



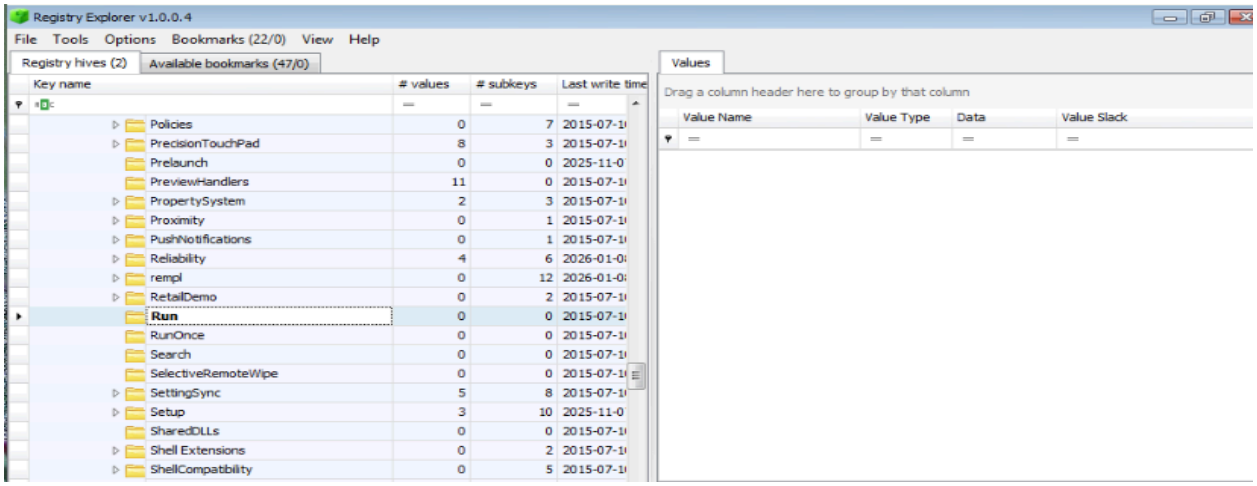
7. Carpetas compartidas

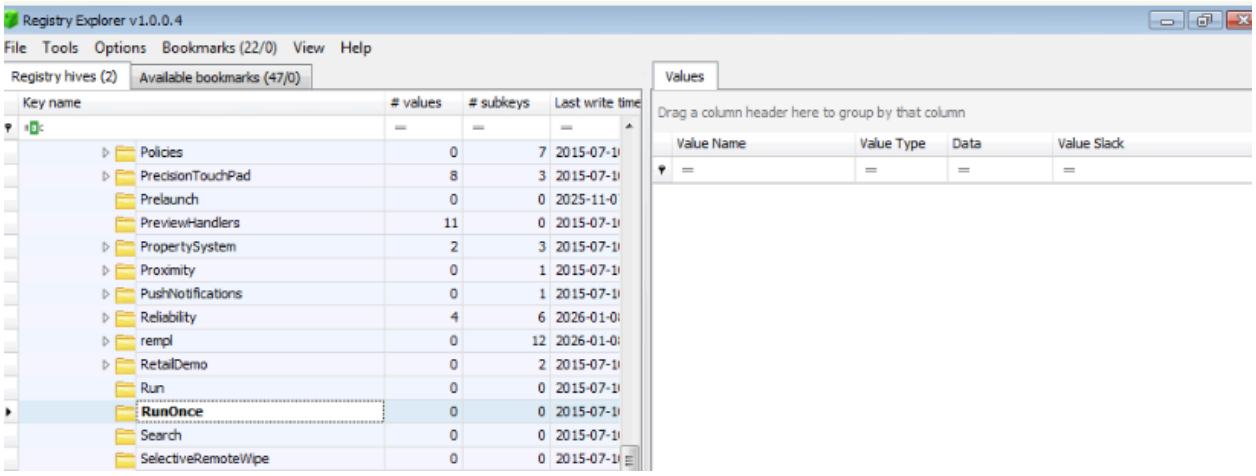
Se ha examinado la clave del registro System\ControlSet001\Services\lanmanserver\Shares en el archivo **SYSTEM** para identificar recursos compartidos en red. La clave no contiene valores asociados a rutas de directorios (aparece vacía de recursos definidos por el usuario, mostrando únicamente la subclave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



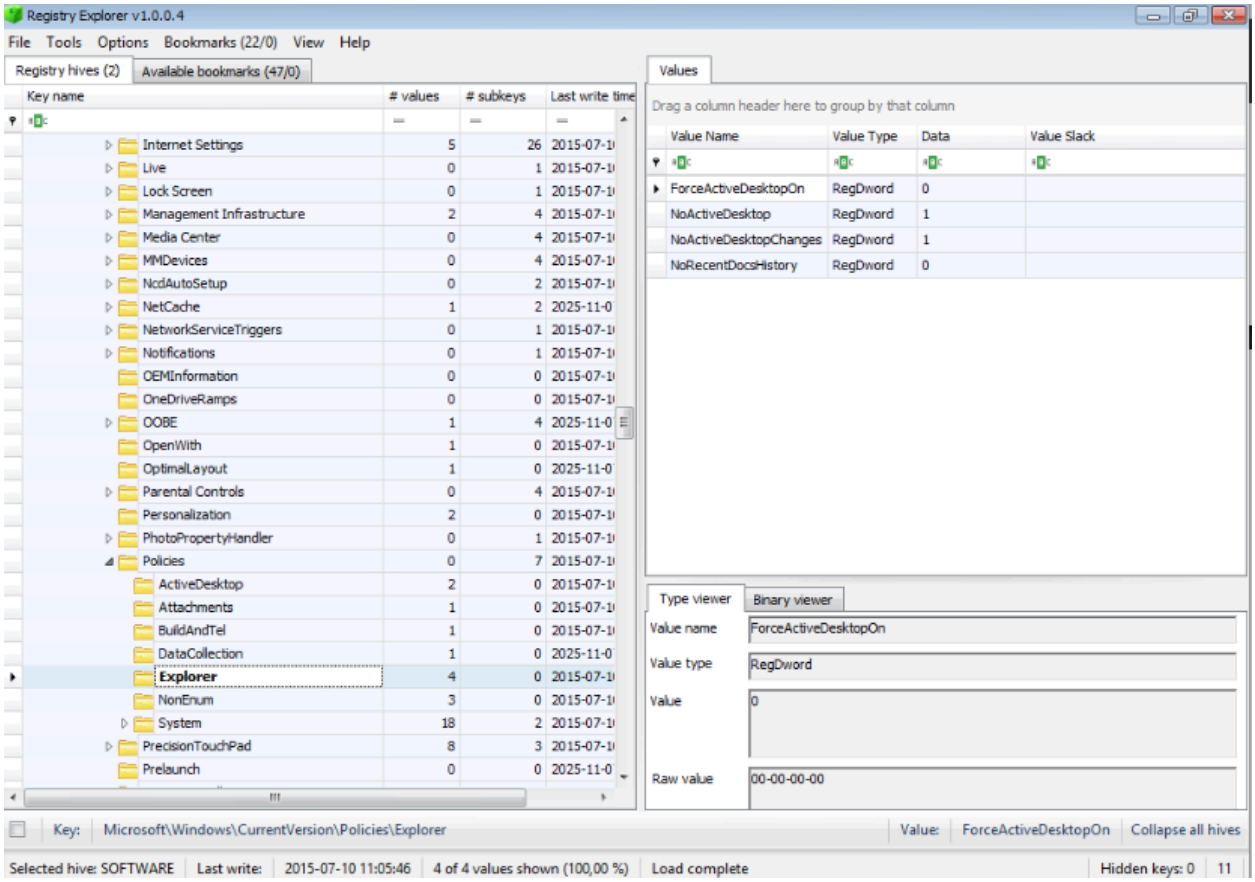
8. Programas de inicio

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.



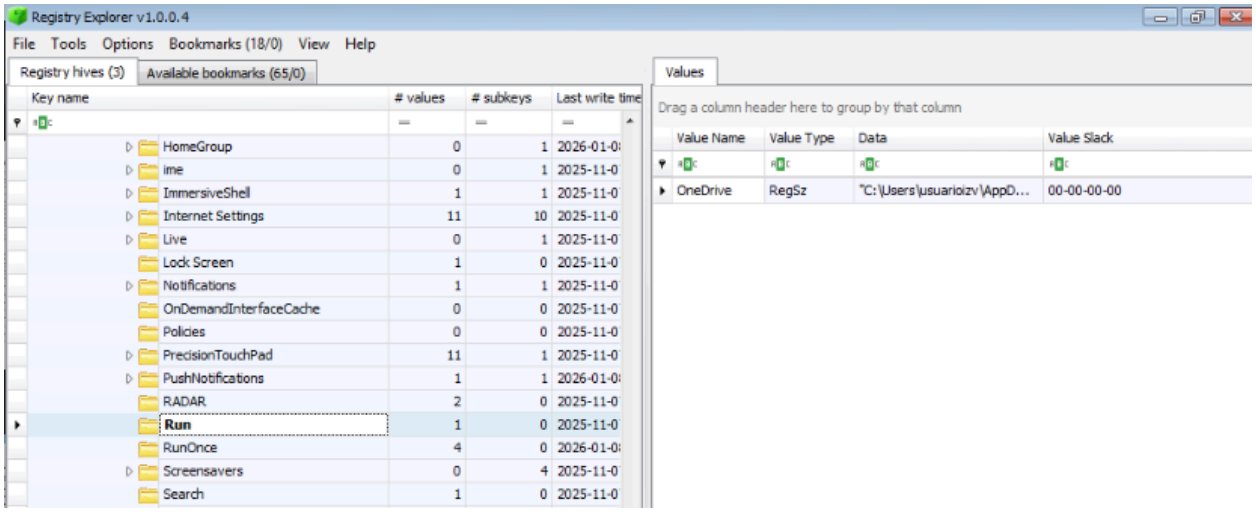


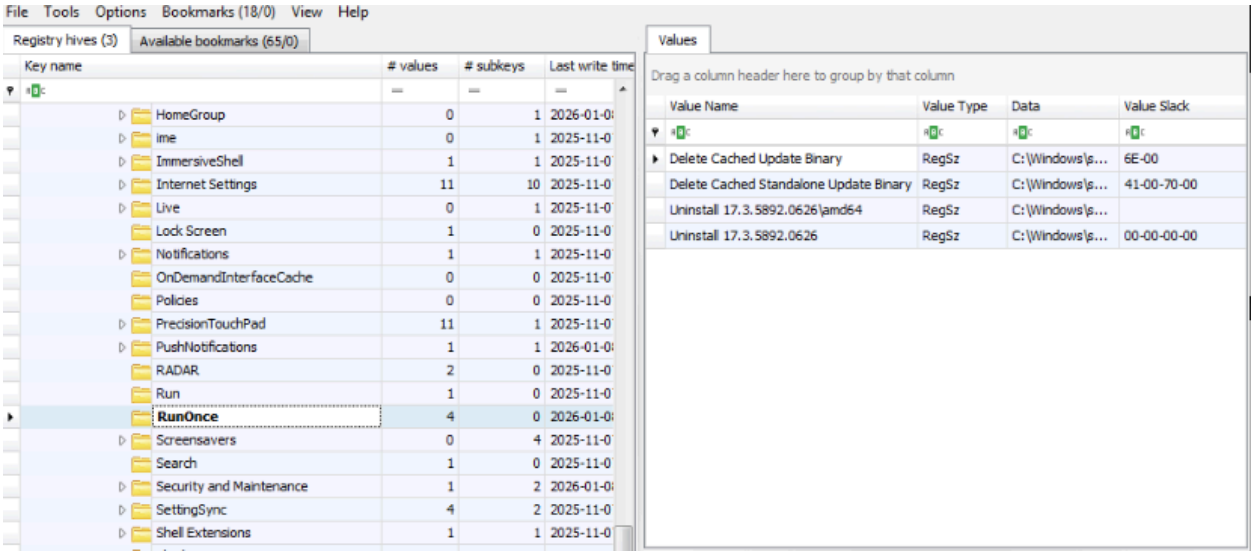
En la ruta Software\Microsoft\Windows\CurrentVersion\Policies\Explorer, se observan configuraciones relacionadas con el **Active Desktop** (ForceActiveDesktopOn, NoActiveDesktop), pero no se detecta la subclave Run que suele utilizarse para ocultar persistencia maliciosa.



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

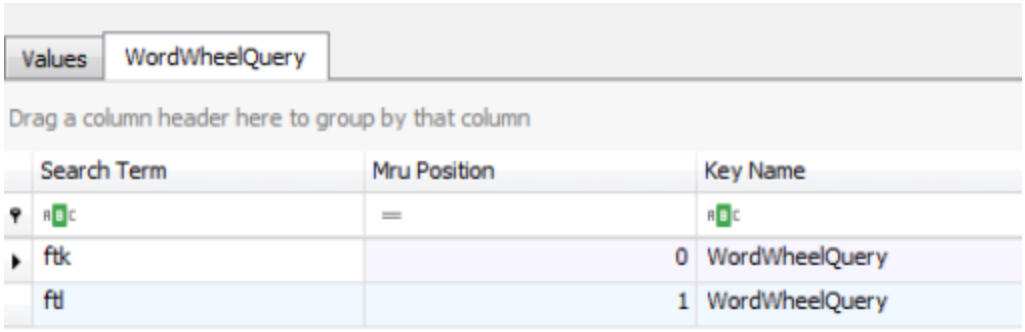
- **Run:** Se ha identificado la ejecución automática de **OneDrive** ("C:\Users\usuarioizv\AppData\..."). Es una entrada legítima y esperada en Windows 10.
- **RunOnce:** Se han encontrado varias entradas pendientes de ejecución (Delete Cached Update Binary, Uninstall...). Estas corresponden a tareas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


Registry Explorer v1.0.0.4
File Tools Options Bookmarks (18/0) View Help
Registry hives (3) Available bookmarks (65/0)
Key name # values # subkeys Last write time
HomeGroup 0 1 2026-01-0
ime 0 1 2025-11-0
ImmersiveShell 1 1 2025-11-0
Internet Settings 11 10 2025-11-0
Live 0 1 2025-11-0
Lock Screen 1 0 2025-11-0
Notifications 1 1 2025-11-0
OnDemandInterfaceCache 0 0 2025-11-0
Policies 0 0 2025-11-0
PrecisionTouchPad 11 1 2025-11-0
PushNotifications 1 1 2026-01-0
RADAR 2 0 2025-11-0
Run 1 0 2025-11-0
RunOnce 4 0 2026-01-0
Screensavers 0 4 2025-11-0
Search 1 0 2025-11-0
Values
Drag a column header here to group by that column
Value Name Value Type Data Value Slack
OneDrive RegSz "C:\Users\usuarioizv\AppD... 00-00-00-00


File Tools Options Bookmarks (18/0) View Help
Registry hives (3) Available bookmarks (65/0)
Key name # values # subkeys Last write time
HomeGroup 0 1 2026-01-0
ime 0 1 2025-11-0
ImmersiveShell 1 1 2025-11-0
Internet Settings 11 10 2025-11-0
Live 0 1 2025-11-0
Lock Screen 1 0 2025-11-0
Notifications 1 1 2025-11-0
OnDemandInterfaceCache 0 0 2025-11-0
Policies 0 0 2025-11-0
PrecisionTouchPad 11 1 2025-11-0
PushNotifications 1 1 2026-01-0
RADAR 2 0 2025-11-0
Run 1 0 2025-11-0
RunOnce 4 0 2026-01-0
Screensavers 0 4 2025-11-0
Search 1 0 2025-11-0
Security and Maintenance 1 2 2026-01-0
SettingSync 4 2 2025-11-0
Shell Extensions 1 1 2025-11-0
Values
Drag a column header here to group by that column
Value Name Value Type Data Value Slack
Delete Cached Update Binary RegSz C:\Windows\s... 6E-00
Delete Cached Standalone Update Binary RegSz C:\Windows\s... 41-00-70-00
Uninstall 17.3.5892.0626\amd64 RegSz C:\Windows\s...
Uninstall 17.3.5892.0626 RegSz C:\Windows\s... 00-00-00-00

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.



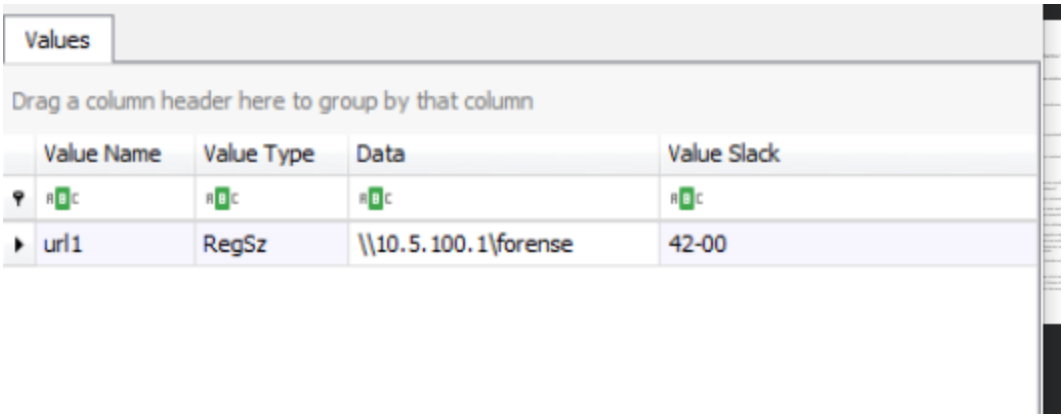
10. Rutas en Inicio o Explorer

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.

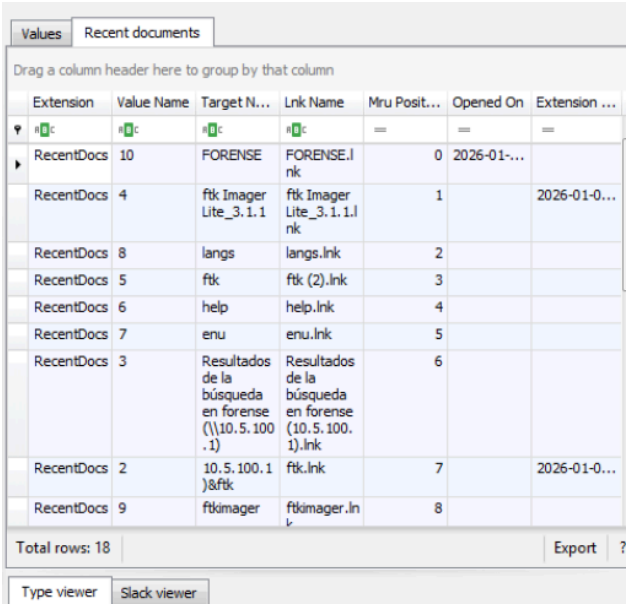
- **Hallazgo:** Esto indica que el usuario accedió conscientemente a un recurso compartido en red (SMB) ubicado en la dirección IP 10.5.100.1 dentro de una carpeta llamada forense.

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



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.



12. Documentos ofimáticos recientes

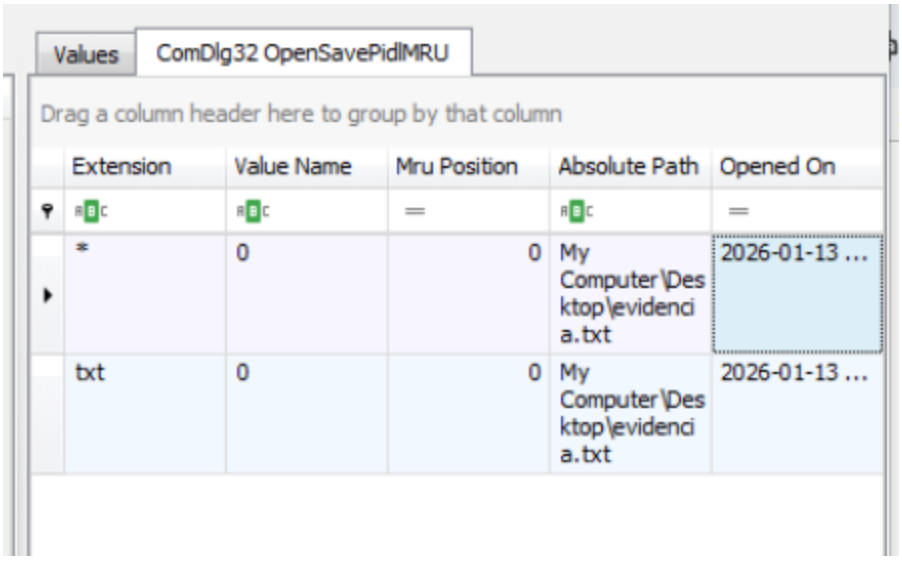
Mi máquina virtual no tiene instalado el Office365.

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

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

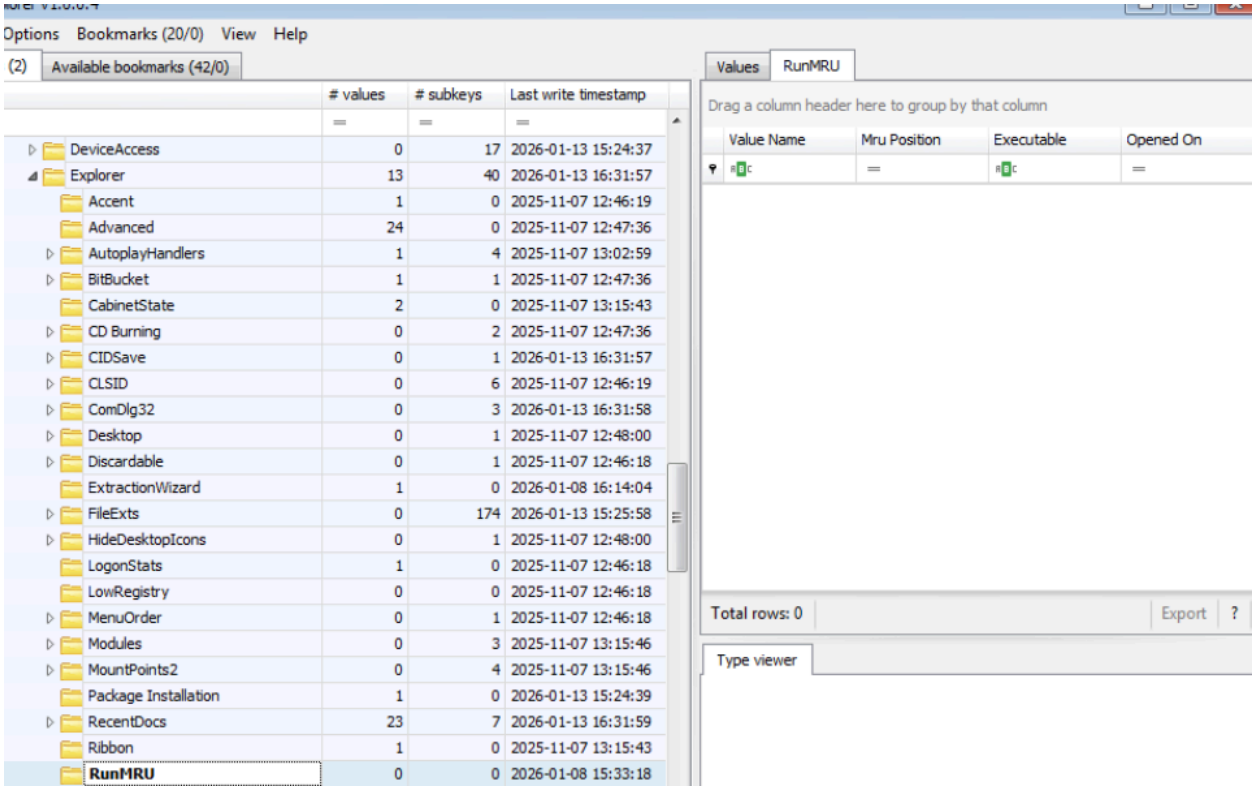
Se ha analizado la clave OpenSavePidlMRU dentro del archivo **NTUSER.DAT**. Esta clave es crítica porque almacena el historial de archivos que han sido manipulados explícitamente a través de las ventanas de diálogo comunes de Windows ("Abrir" o "Guardar como").

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.



14. Últimos comandos ejecutados

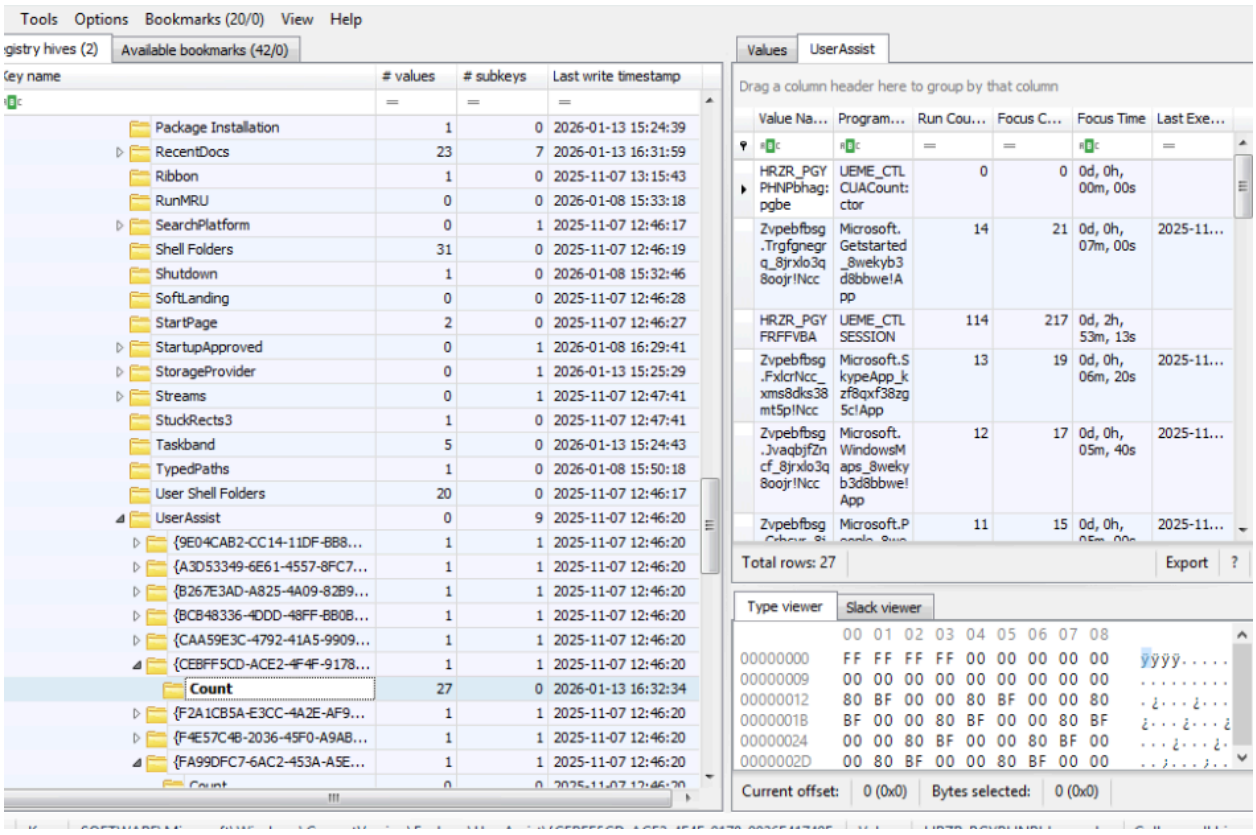
Aunque se ha utilizado la consola de comandos (CMD) para ejecutar herramientas como FTK Imager, la clave RunMRU aparece vacía. Esto indica forensemente que el usuario no lanzó la consola a través del cuadro de diálogo 'Ejecutar' (Win+R), sino probablemente desde el Menú Inicio o un acceso directo. Los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



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.



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)

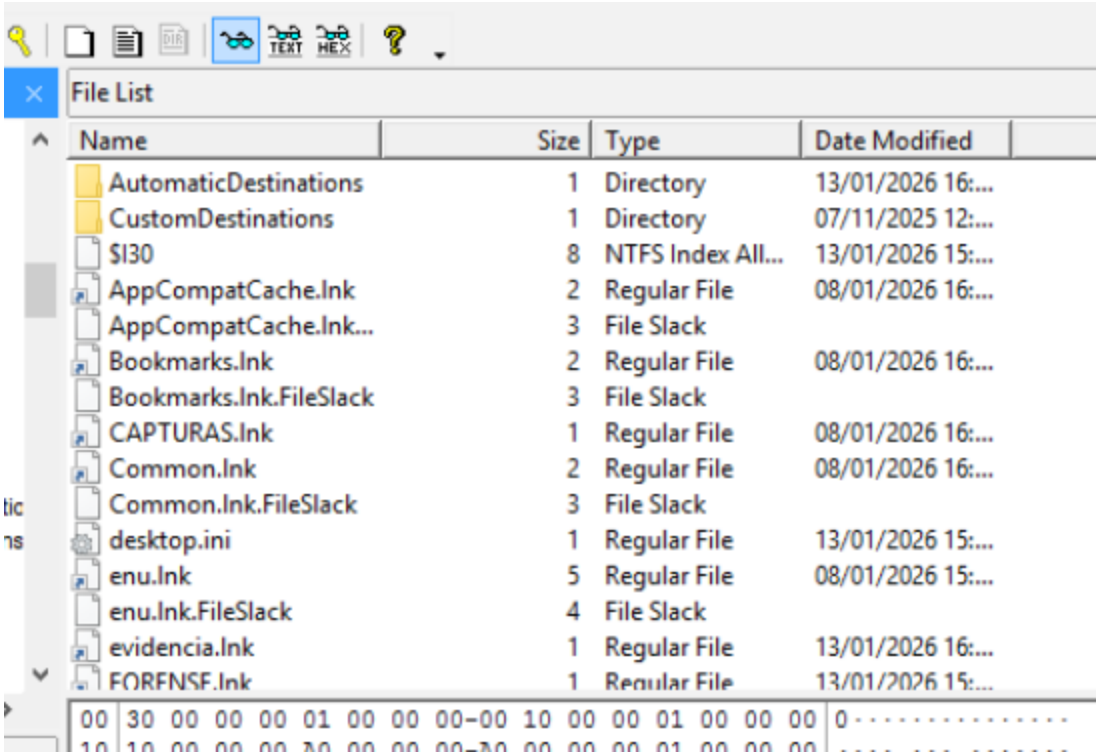
Software\Microsoft\Windows\Current Version\Search\RecentApps

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:

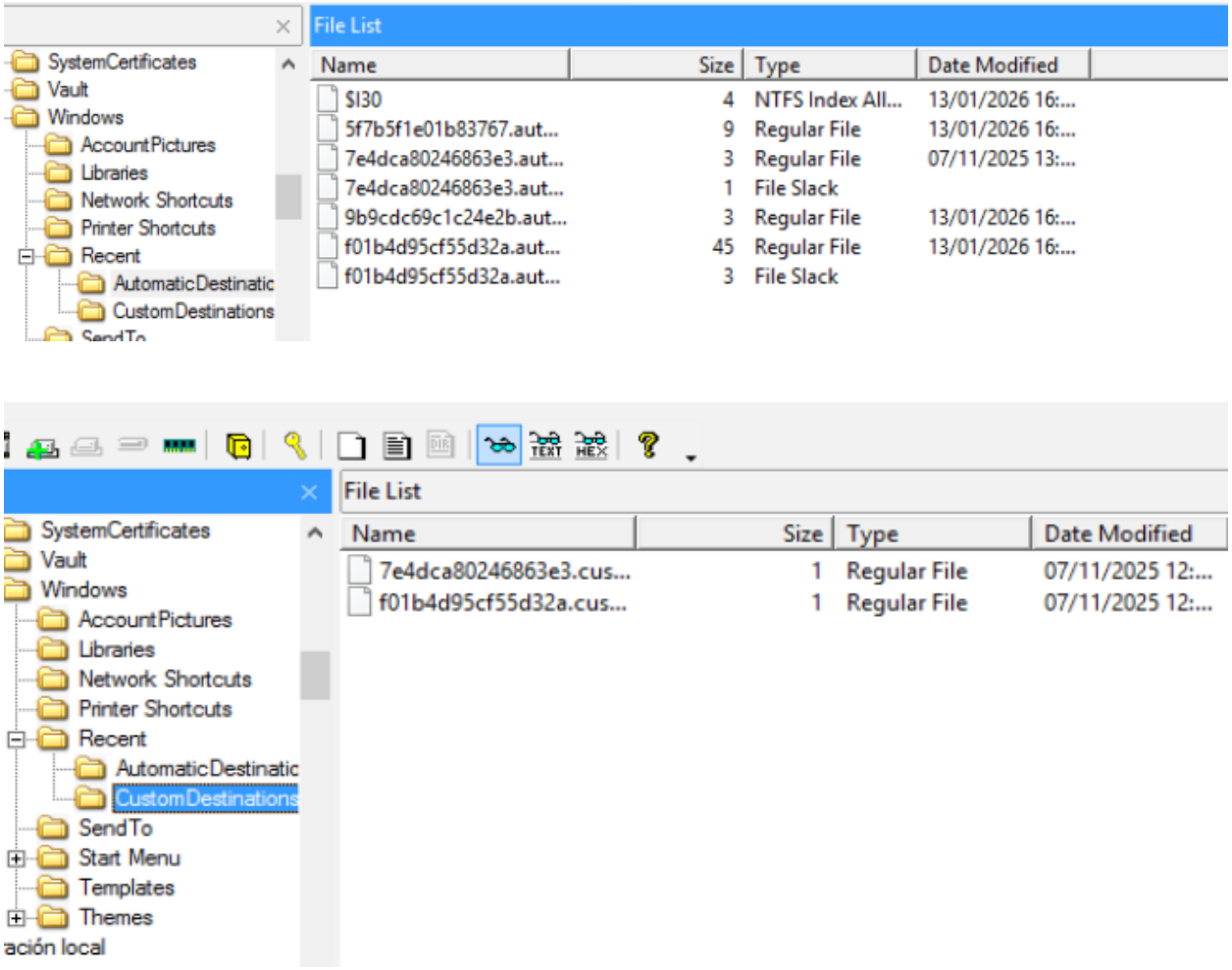
- **evidencia.lnk:** Confirma forensemente que el archivo de texto creado anteriormente en el Escritorio fue abierto recientemente.
- **FORENSE.lnk:** Ratifica la interacción persistente con el directorio compartido en red.
- **CAPTURAS.lnk:** Indica que el usuario ha estado accediendo a una carpeta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



19. Automatic & Custom destinations (JumpListExplorer)

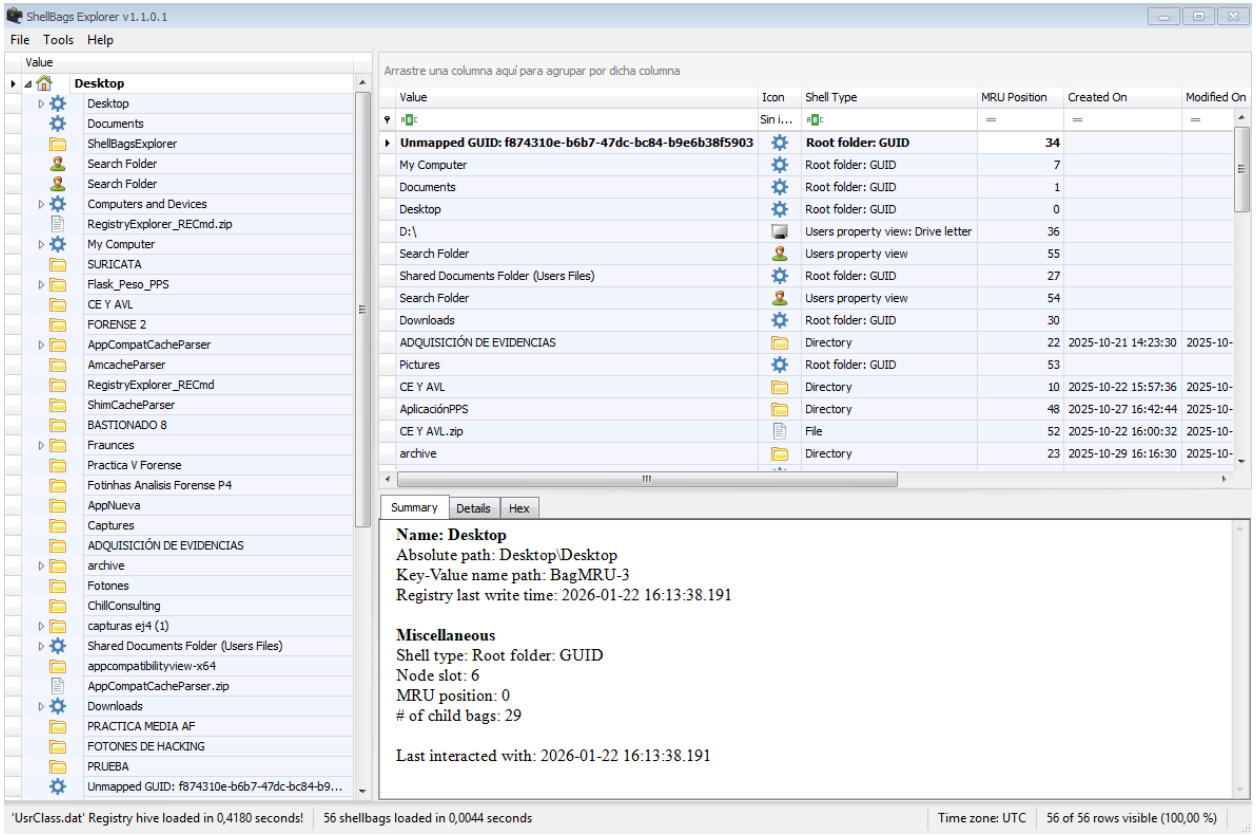
Se han extraído evidencias de las **Jump Lists** de Windows. Estos artefactos son listas de "destinos frecuentes" o "recientes" asociadas a aplicaciones específicas de la barra de tareas.

- **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.



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 extrajeron y aplicaron forensemente los archivos de transacción (.LOG1 y .LOG2), logrando reconstruir la integridad de la base de datos para su análisis.

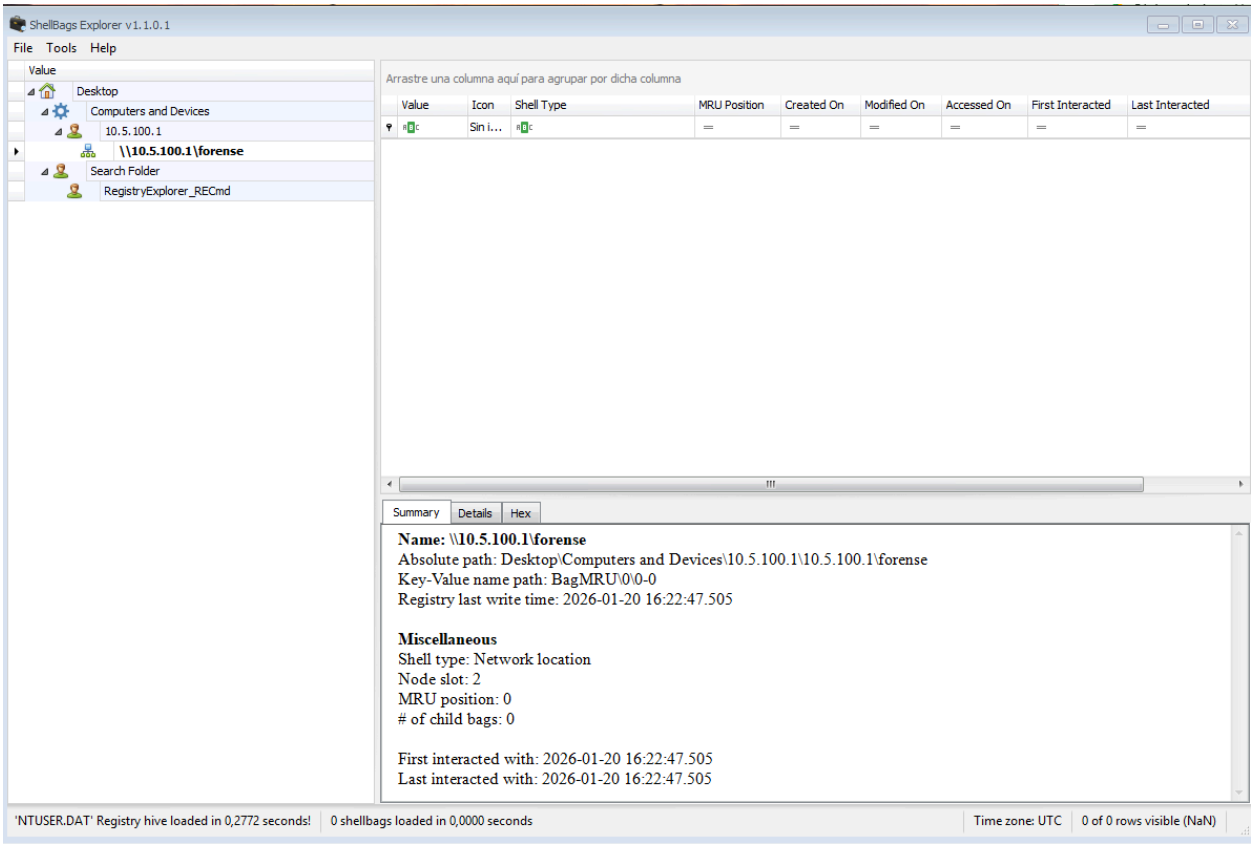


1. Reconstrucción de Rutas (BagMRU): Como se observa en la captura superior, la herramienta ha permitido visualizar la estructura jerárquica de carpetas (BagMRU). Esto confirma las rutas exactas por las que navegó el usuario, identificando accesos directos a directorios críticos como **Descargas** y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

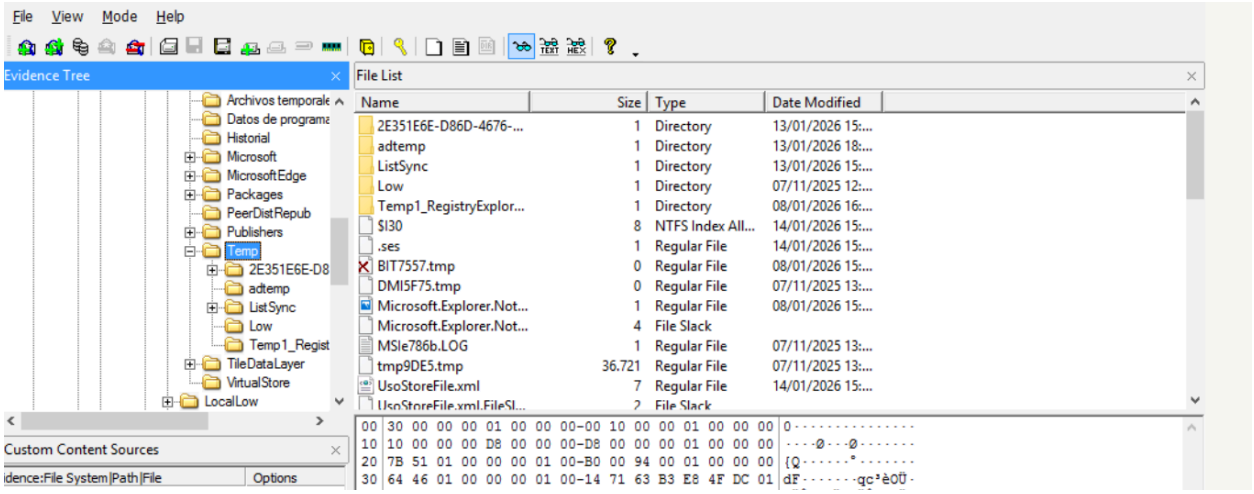
- **Interacción Reciente:** La columna *Last Interacted* (visible en la imagen) registra la fecha y hora exacta en la que el usuario abrió la carpeta. Esto sitúa al usuario visualizando estos archivos en el momento del incidente.

- **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.



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 forensemente 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

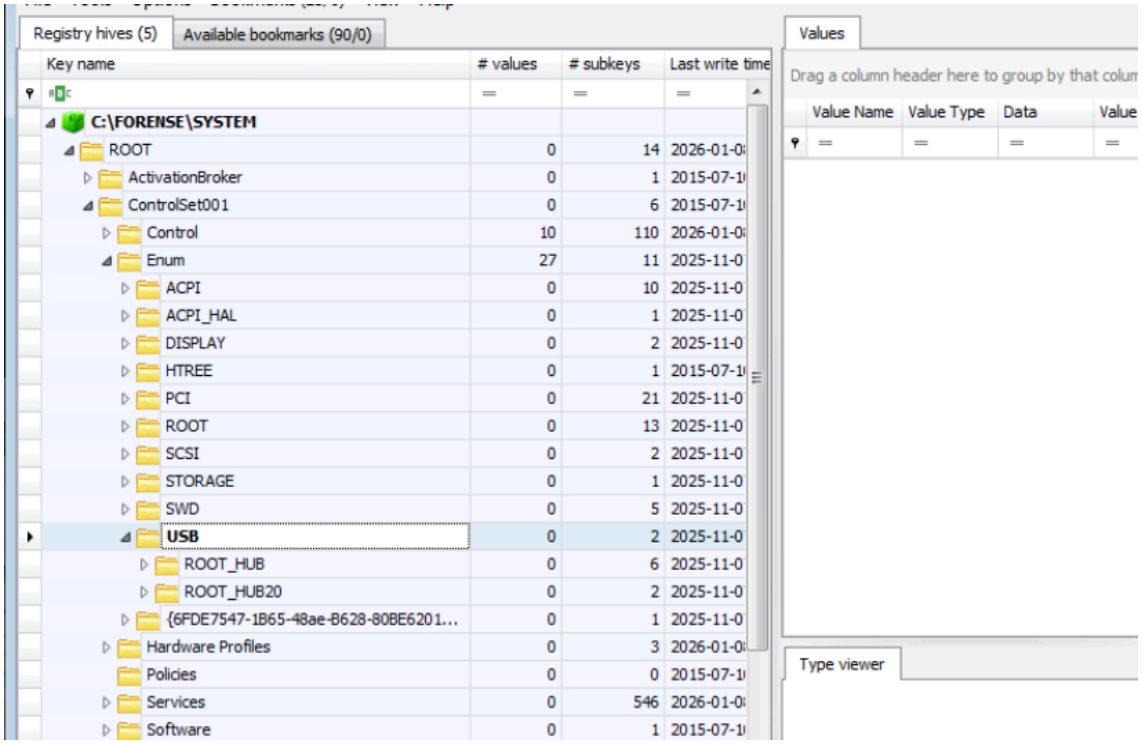
Claves analizadas:

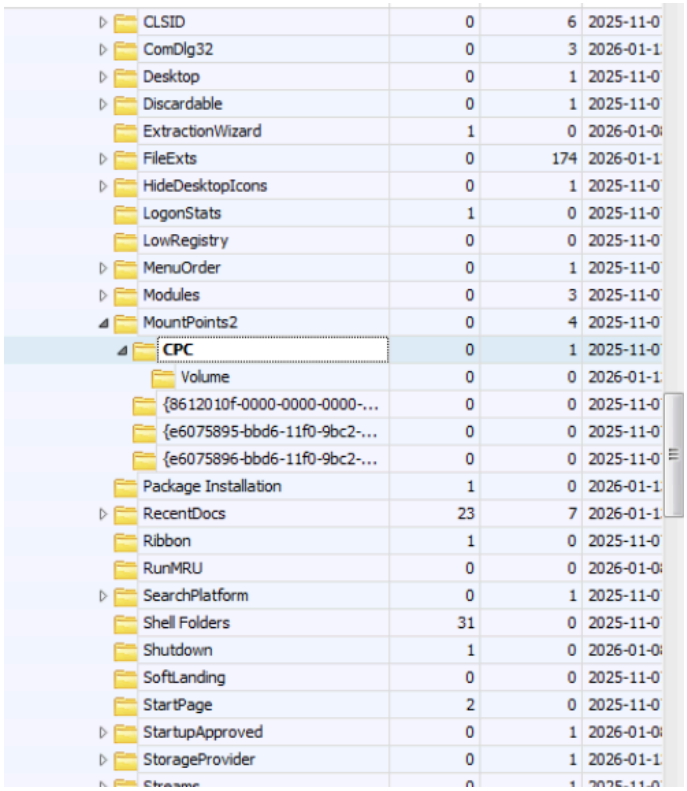
- SOFTWARE\Microsoft\Windows Portable Devices\Devices
- NTUSER.DAT\...\MountPoints2
- Software\Microsoft\Windows NT\CurrentVersion\EMDMgmt
- System\ControlSet001\Enum\USBSTOR

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.

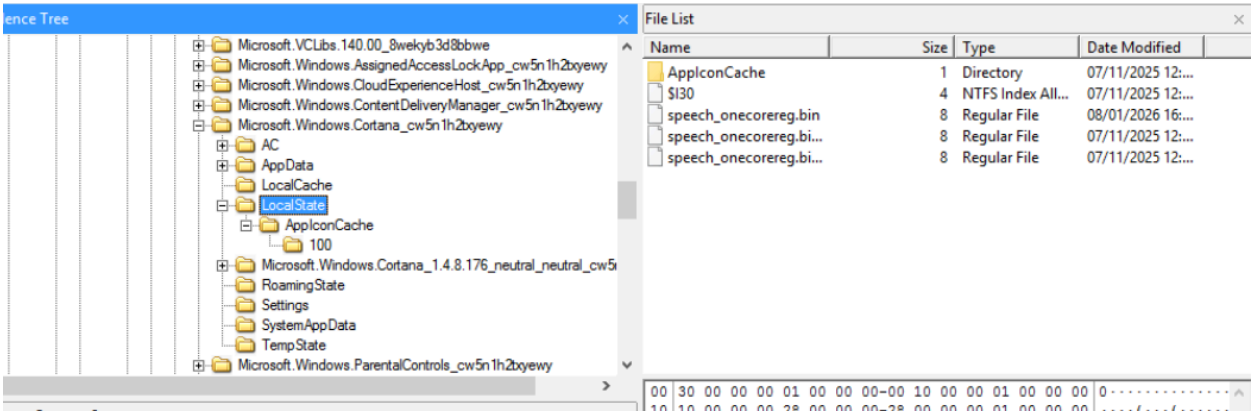

Registry hives (5)
Available bookmarks (90/0)
Key name
values
subkeys
Last write time
C:\FORENSE\SYSTEM
ROOT
ActivationBroker
ControlSet001
Control
Enum
ACPI
ACPI_HAL
DISPLAY
HTREE
PCI
ROOT
SCSI
STORAGE
SWD
USB
ROOT_HUB
ROOT_HUB20
{6FDE7547-1B65-48ae-B628-80BE6201...
Hardware Profiles
Policies
Services
Software
Values
Drag a column header here to group by that colum
Value Name
Value Type
Data
Value
Type viewer


CLSID
ComDlg32
Desktop
Discardable
ExtractionWizard
FileExts
HideDesktopIcons
LogonStats
LowRegistry
MenuOrder
Modules
MountPoints2
CPC
Volume
{8612010f-0000-0000-0000-...
{e6075895-bbd6-11f0-9bc2-...
{e6075896-bbd6-11f0-9bc2-...
Package Installation
RecentDocs
Ribbon
RunMRU
SearchPlatform
Shell Folders
Shutdown
SoftLanding
StartPage
StartupApproved
StorageProvider

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

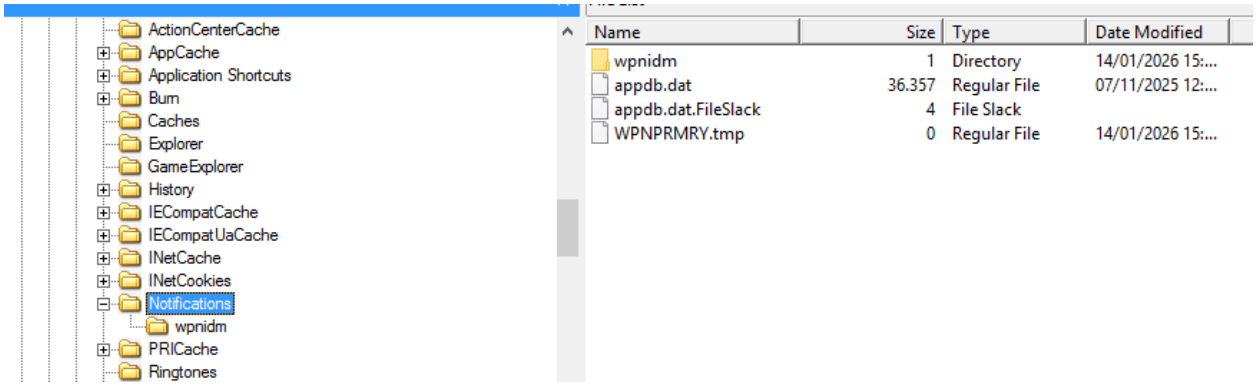
Tras analizar C:\Users\usuarioizv_...\LocalState\ESEDatabase_CortanaCoreInstance,se ha procedido a la búsqueda del archivo CortanaCoreDb.dat en el directorio de paquetes de la aplicación. La ausencia de este artefacto indica que el servicio de Cortana no ha sido activado plenamente o que el usuario no 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.



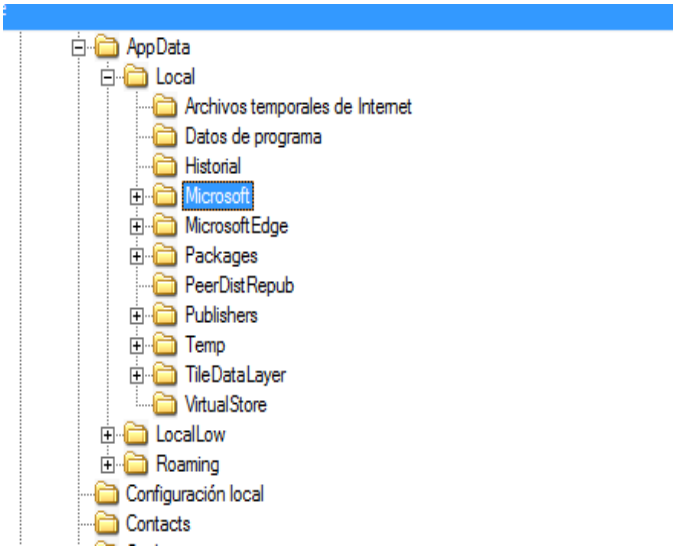
24. Notificaciones de Windows (sqlite studio)

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.



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.

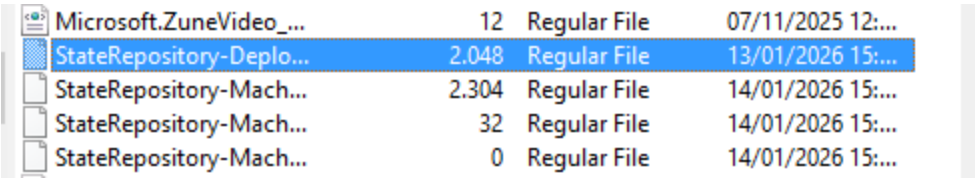


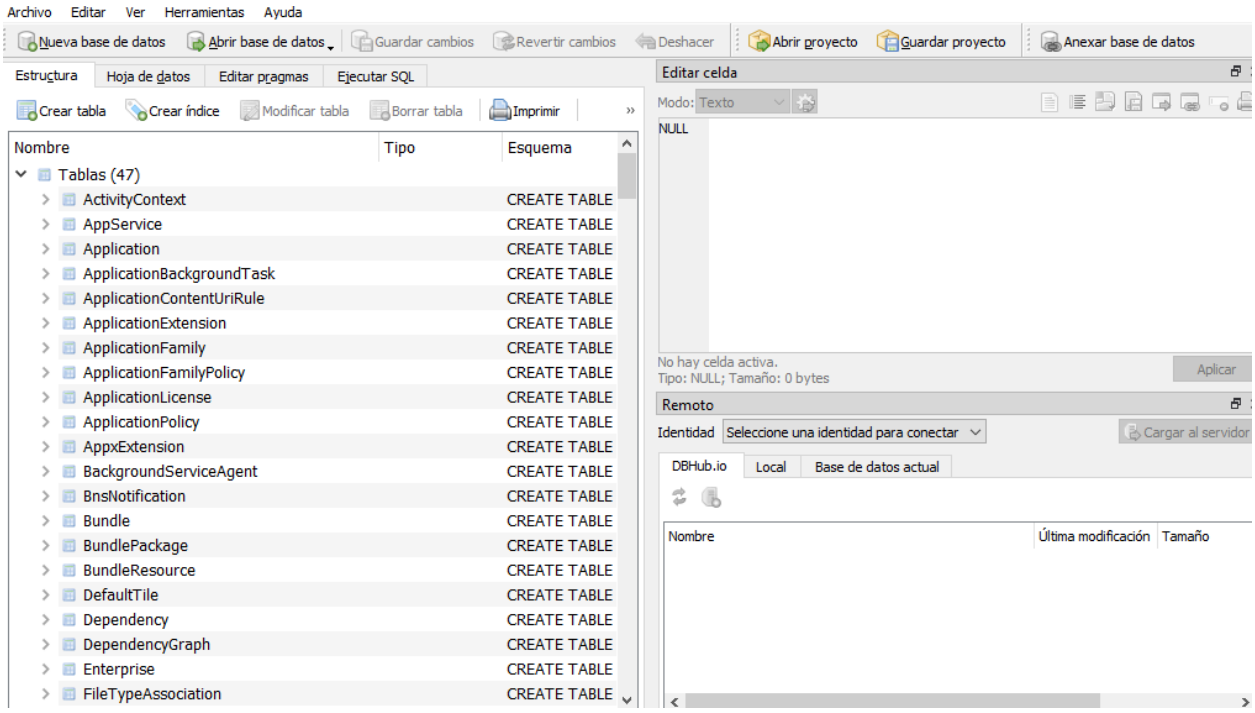
26. Windows Store (**DB Browser for SQLite**)

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.



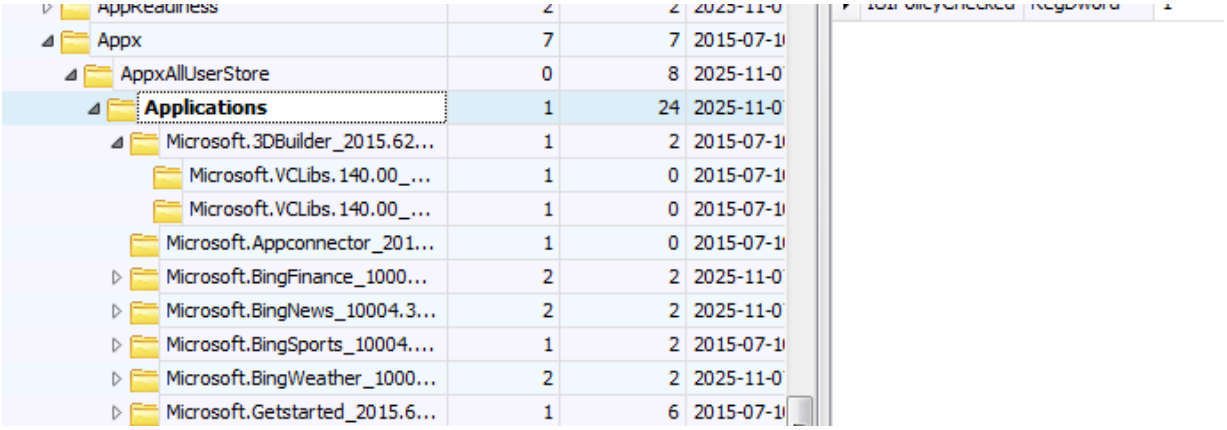


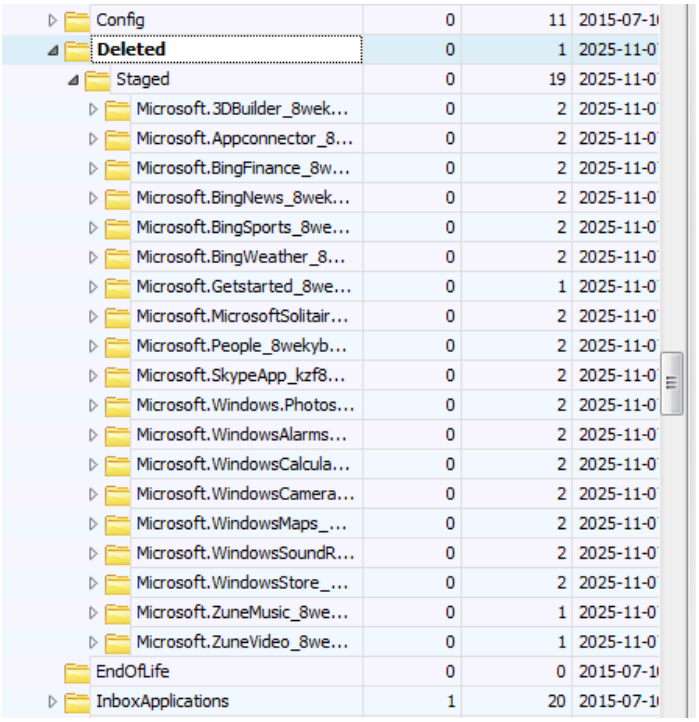
Se ha examinado el registro para auditar el ciclo de vida de las aplicaciones en el equipo:

- **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.



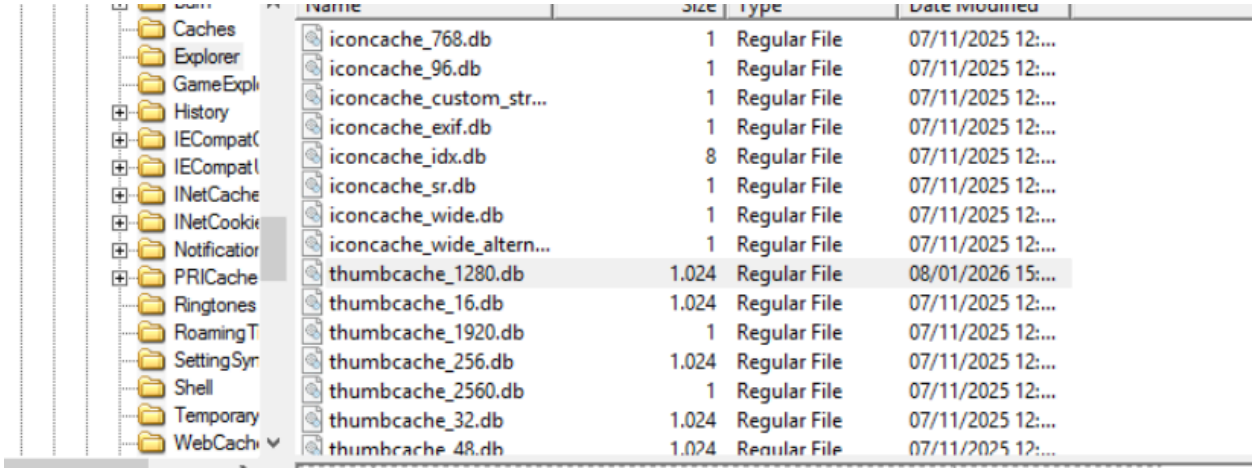


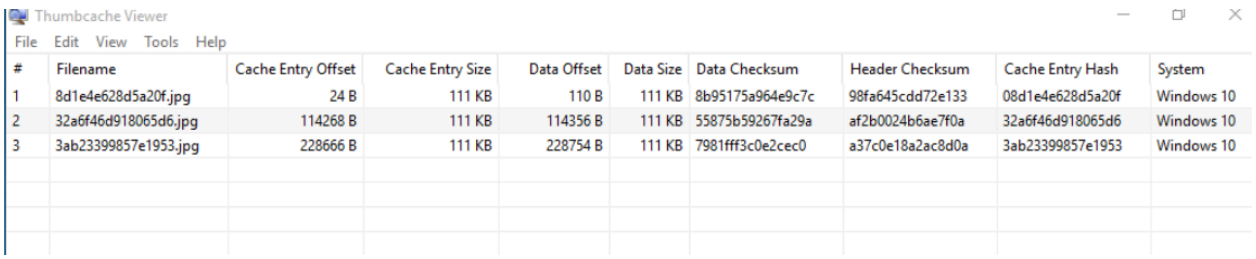
27. Thumbnails (thumbviewer) & Thumbcaché (thumbcacheviewer) Ficheros “thumbs.db”

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.





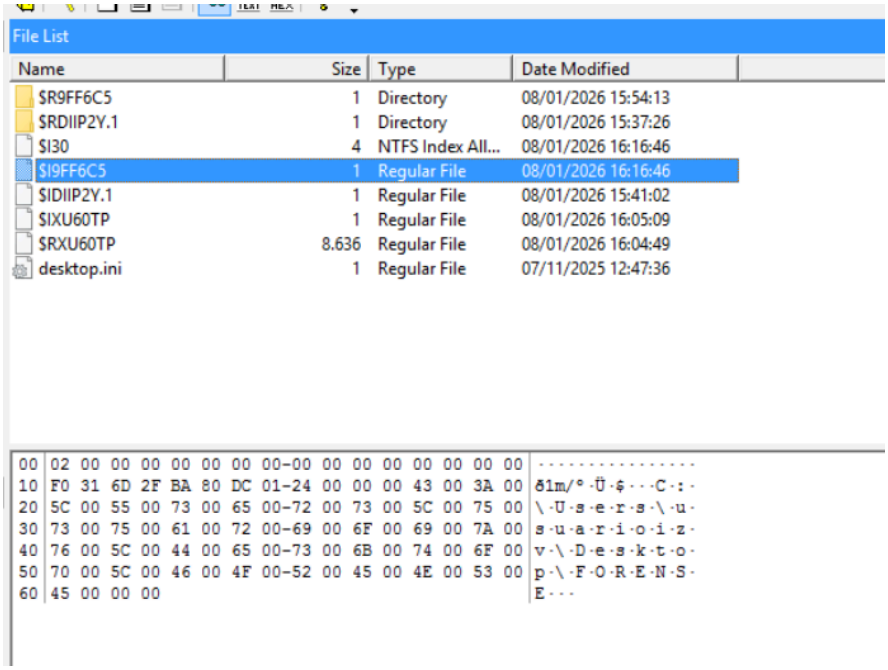
28. Papelera de reciclaje(rifiuti)

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



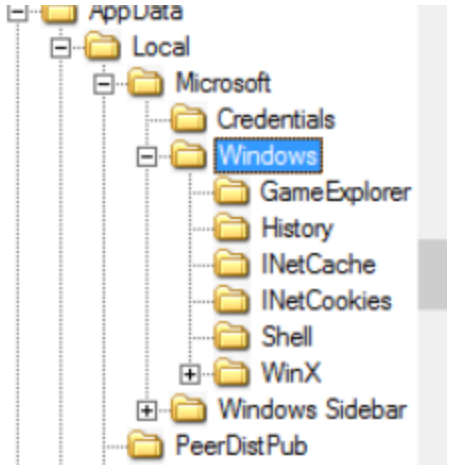
```
C:\Users\usuarioizv\Desktop\rifiuti2-0.6.1-win\x64>"rifiuti-vista.exe" $I9FF6C5
Recycle bin path: '$I9FF6C5'
Version: 2

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

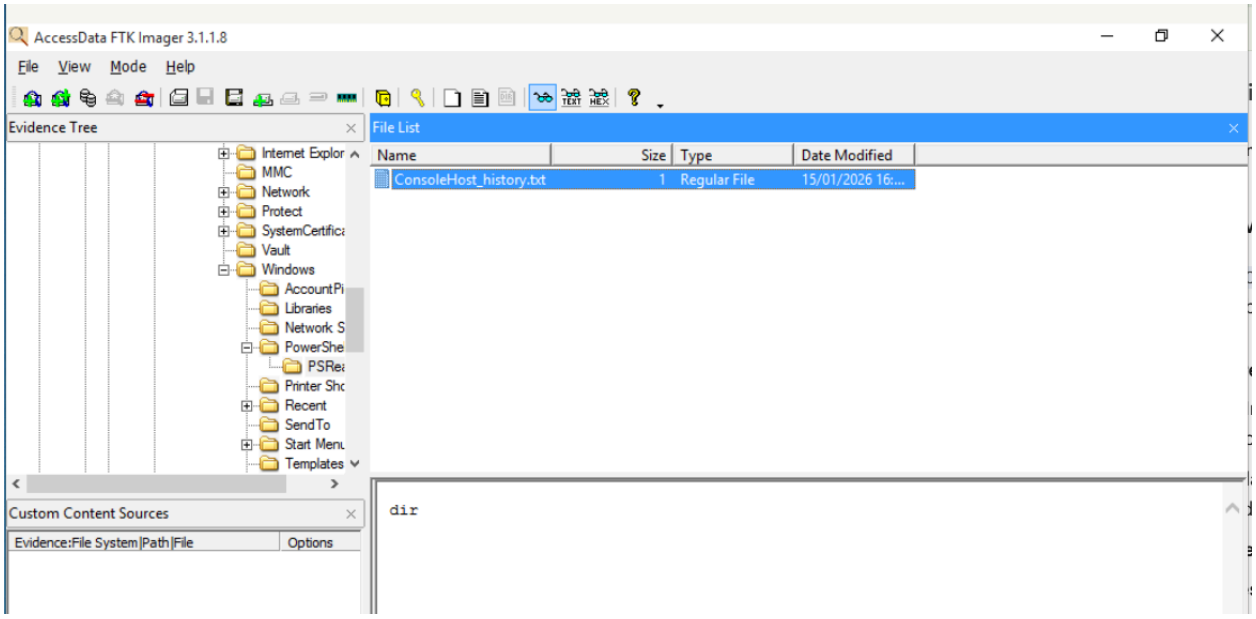
30. IP Pública (ETLParser)

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.



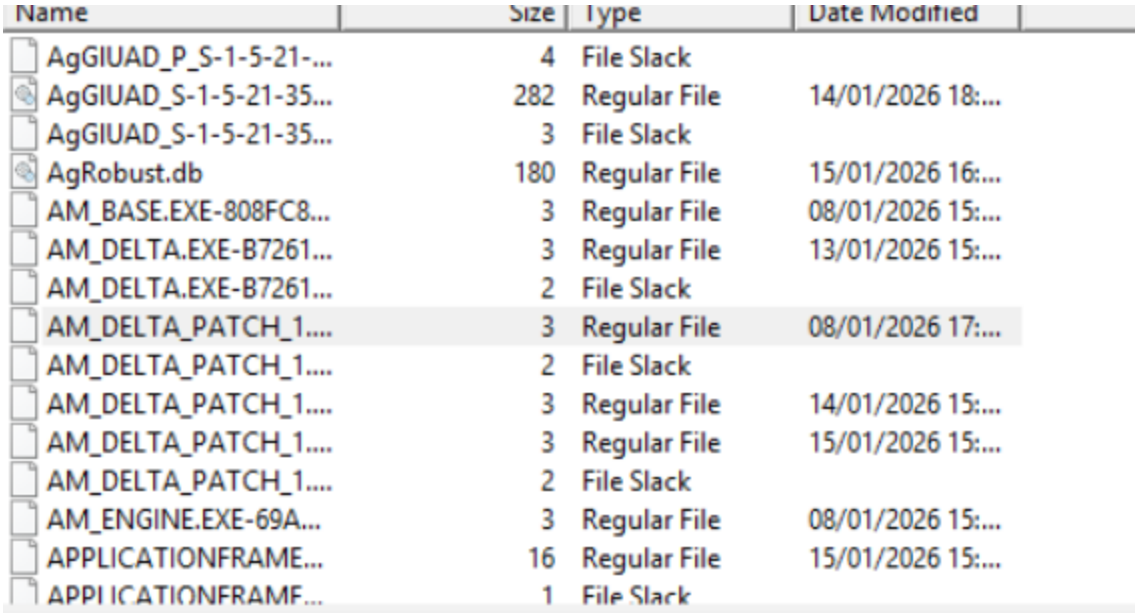
32. Windows PREFETCH (PECmd)

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:...
APPLICATIONFRAME...	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\DOWNLOAD\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\MSVCRT.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)

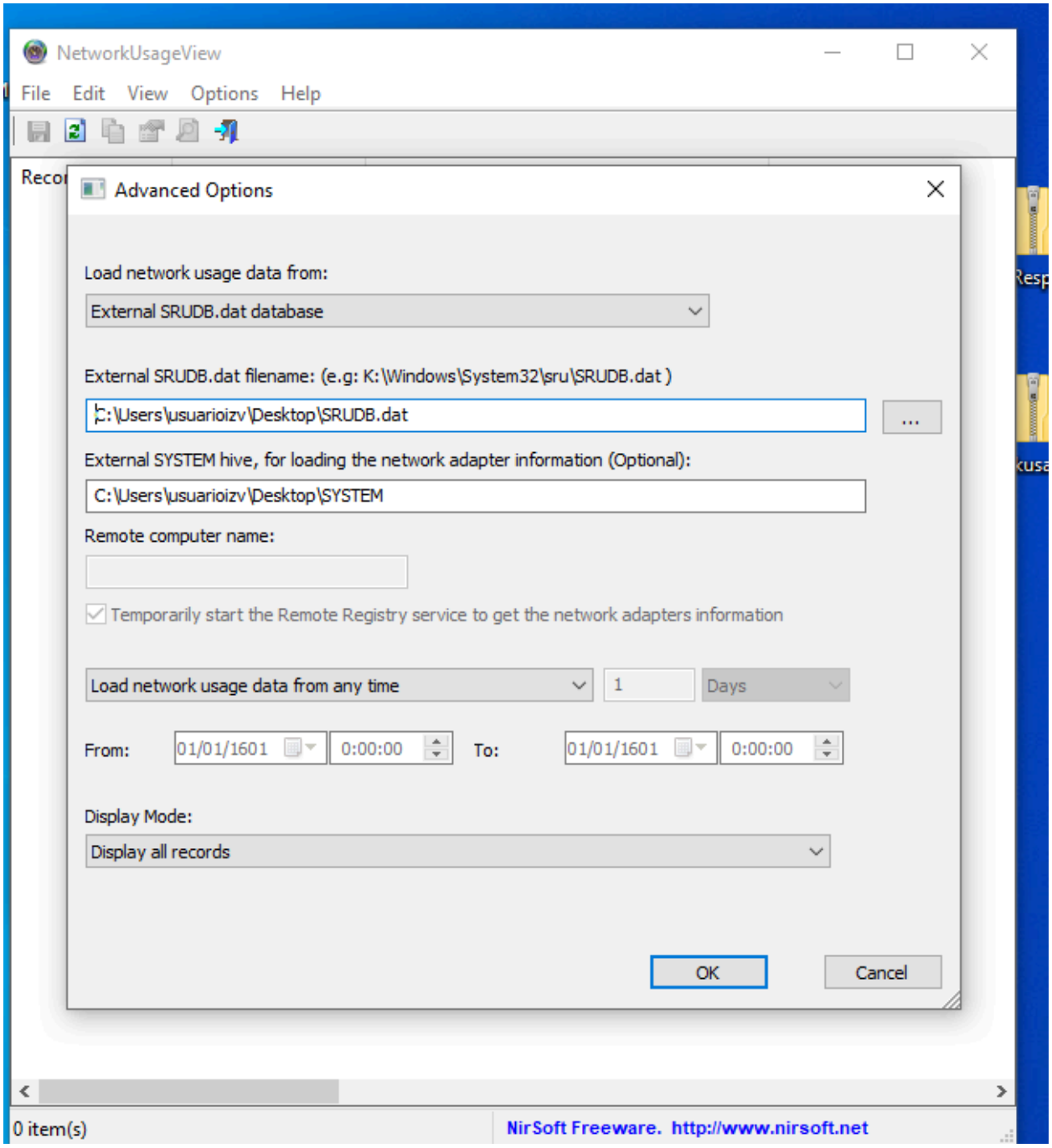
Se ha verificado la existencia de las bases de datos en la ruta C:\Windows\Prefetch\Ag*.db AgAppLaunch.db AgGlGlobalHistory.db mediante la ejecución de **CrowdResponse** y el comando @DirList para validar la capacidad de recolección de artefactos en el entorno. La salida XML confirma la estructura de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

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.

1. **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.
2. **Resultado de la Herramienta:** La ejecución de NetworkUsageView con la configuración correcta devuelve **0 registros**.

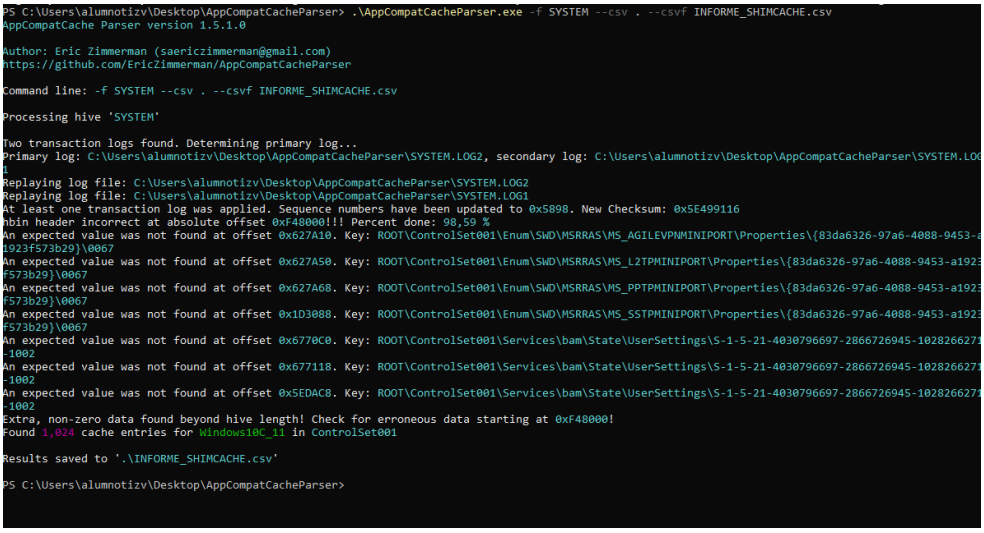
Se determina que el servicio SRUM fue reiniciado o no llegó a escribir datos de tráfico de red en el disco antes de la captura de la imagen. La evidencia confirma la ausencia de historial recuperable en este artefacto específico.



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:

1. **Software de Anonymización/VPN:** Se ha detectado la presencia de **wireguard-installer.exe** en el escritorio del usuario alumnomizv (Fecha modif: 19/01/2026). Este hallazgo es relevante forensemene ya que el uso de VPNs no autorizadas puede indicar intentos de evasión de controles de red o exfiltración de datos.
2. **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).



```
1,35,C:\Program Files (x86)\Microsoft\EdgeUpdate\Install\{D2C3ECF0-C1F9-4756-B29A-77F9F832D992}\MicrosoftEdge_X64_144.0.3719.82_143.0.3650.139.exe,2026-01-19 07:27:10,No,False,SYSTEM
1,36,C:\WINDOWS\System32\DriverStore\FileRepository\nvak.inf_amd64_a1ae244dd2e4b40a\dbInstaller.exe,2021-02-04 19:46:04,Yes,False,SYSTEM
1,37,C:\WINDOWS\System32\DriverStore\FileRepository\nvak.inf_amd64_a1ae244dd2e4b40a\Display.NvContainer\NVDisplay.Container.exe,2021-02-04 19:51:28,No,False,SYSTEM
1,38,C:\Users\ALUMNO~1\AppData\Local\Temp\is-26ONH.tmp\CodeSetup-stable-585eba7c0c34fd6b30faac7c62a42050bfbc0086.tmp,2026-01-16 12:54:38,No,False,SYSTEM
1,39,C:\Users\alumnomizv\AppData\Local\Temp\is-26ONH.tmp\CodeSetup-stable-585eba7c0c34fd6b30faac7c62a42050bfbc0086.tmp,2026-01-16 12:54:38,Yes,False,SYSTEM
1,40,C:\Users\ALUMNO~1\AppData\Local\Temp\vscode-stable-user-x64\CodeSetup-stable-585eba7c0c34fd6b30faac7c62a42050bfbc0086.exe,2026-01-16 12:54:36,No,False,SYSTEM
1,41,C:\Users\alumnomizv\AppData\Local\Temp\vscode-stable-user-x64\CodeSetup-stable-585eba7c0c34fd6b30faac7c62a42050bfbc0086.exe,2026-01-16 12:54:36,Yes,False,SYSTEM
1,42,C:\Program Files\PDFgear\unins000.exe,2025-09-22 07:28:57,No,False,SYSTEM
1,43,C:\Program Files\BraveSoftware\Brave-Browser\Application\144.1.86.139\elevation_service.exe,2026-01-15 06:45:32,No,False,SYSTEM
1,44,C:\Program Files\BraveSoftware\Brave-Browser\Application\144.1.86.139\Installer\setup.exe,2026-01-16 08:37:58,No,False,SYSTEM
1,45,000000090001622100450000000a000065f400008664Microsoft.Copilot8wekyb3d8bbwe,,No,False,SYSTEM
1,46,C:\WINDOWS\system32\srtasks.exe,2024-04-01 07:22:17,No,False,SYSTEM
1,47,000000001b5802e804ea0000000c0000000000008664Microsoft.WindowsAppRuntime.1.78wekyb3d8bbwe,,No,False,SYSTEM
1,48,000000091b5802e804ea0000000c0000000000008664Microsoft.WindowsAppRuntime.1.78wekyb3d8bbwe,,No,False,SYSTEM
1,49,C:\Program Files (x86)\BraveSoftware\Update\Install\{15ECB03F-392F-4DA9-9331-8FDA494D9B63}\CR_F8364.tmp\setup.exe,2026-01-16 08:37:58,No,False,SYSTEM
1,50,C:\Program Files (x86)\BraveSoftware\Update\Install\{15ECB03F-392F-4DA9-9331-8FDA494D9B63}\brave_installer-x64.exe,2026-01-16 08:37:54,No,False,SYSTEM
1,51,C:\WINDOWS\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.443.689.0.exe,2026-01-16 08:36:54,No,False,SYSTEM
1,52,C:\WINDOWS\system32\lpremove.exe,2025-12-10 07:49:59,No,False,SYSTEM
1,53,C:\WINDOWS\system32\DrvInst.exe,2025-12-10 07:49:22,No,False,SYSTEM
1,54,C:\WINDOWS\system32\MpSigStub.exe,2025-09-09 10:17:51,No,False,SYSTEM
1,55,C:\WINDOWS\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.443.669.0.exe,2026-01-15 15:11:40,No,False,SYSTEM
1,56,000000090001000600e0000000000000000000008664Microsoft.WidgetsPlatformRuntime8wekyb3d8bbwe,,No,False,SYSTEM
1,57,C:\Program Files\WindowsApps\Microsoft.WidgetsPlatformRuntime_1.6.14.0_x64__8wekyb3d8bbwe\WidgetService\WidgetService.exe,2025-09-09 10:17:36,No,False,SYSTEM
1,58,000000090001000600e0000000a0000585d00008664Microsoft.WidgetsPlatformRuntime8wekyb3d8bbwe,,No,False,SYSTEM
1,59,C:\Program Files\Mozilla Firefox\default-browser-agent.exe,2026-01-14 15:11:29,No,False,SYSTEM
1,60,00000009000b09ce000e0000000a000066720000 8664Microsoft.WindowsNotepad8wekyb3d8bbwe,,No,False,SYSTEM
1,61,000000001f4002db05fc0000000c0000000000008664Microsoft.WindowsAppRuntime.1.88wekyb3d8bbwe,,No,False,SYSTEM
1,62,000000091f4002db05fc0000000c0000000000008664Microsoft.WindowsAppRuntime.1.88wekyb3d8bbwe,,No,False,SYSTEM
1,63,0000000b629604b4000100000000000000000008664Microsoft.OneDriveSync8wekyb3d8bbwe,,No,False,SYSTEM
1,64,0000000b629604b400010000000a00004a6400008664Microsoft.OneDriveSync8wekyb3d8bbwe,,No,False,SYSTEM
1,65,C:\Users\alumnotizv\HealthyApp\frontend\node_modules\@esbuild\win32-x64\esbuild.exe,2026-01-14 17:18:36,Yes,False,SYSTEM
1,66,C:\WINDOWS\system32\chcp.com,2024-04-01 07:22:16,No,False,SYSTEM
1,67,C:\Program Files\Git\usr\bin\uname.exe,2025-10-17 11:22:02,No,False,SYSTEM
1,68,C:\Program Files\Git\usr\bin\dirname.exe,2025-10-17 11:20:46,No,False,SYSTEM
1,69,C:\Program Files\Git\usr\bin\env.exe,2025-10-17 11:21:58,No,False,SYSTEM
1,70,C:\WINDOWS\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.443.666.0.exe,2026-01-14 15:14:47,No,False,SYSTEM
1,71,C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe,2026-01-13 15:17:54,No,False,SYSTEM
```

36. AmCache (AmCacheParser)

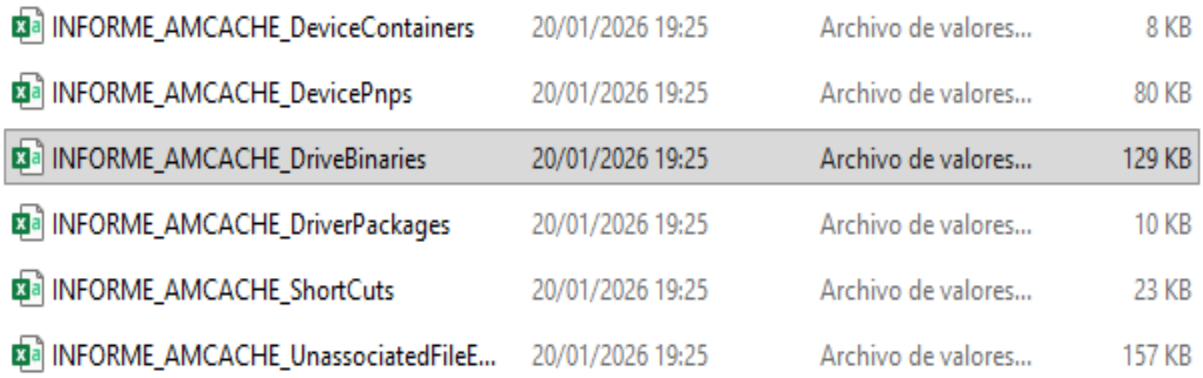
Para el análisis de este artefacto, se extrajo el archivo C:\Windows\AppCompat\Programas\Amcache.hve. Siguiendo el protocolo establecido tras la incidencia con la ShimCache, se extrajeron preventivamente los archivos de transacción (Amcache.hve.LOG1 y .LOG2) para evitar errores de inconsistencia ("Dirty 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
hbin 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
hbin 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\InventoryApplicationFile\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\InventoryApplicationFile\brave.exe|8c8c518236b6c059

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

Key flags: HasActiveParent

NK Record: Size: 0x70
Relative Offset: 0x10F10
Absolute Offset: 0x11F10
Signature: nk
Flags: CompressedName

Name: brave.exe|8c8c518236b6c059
```

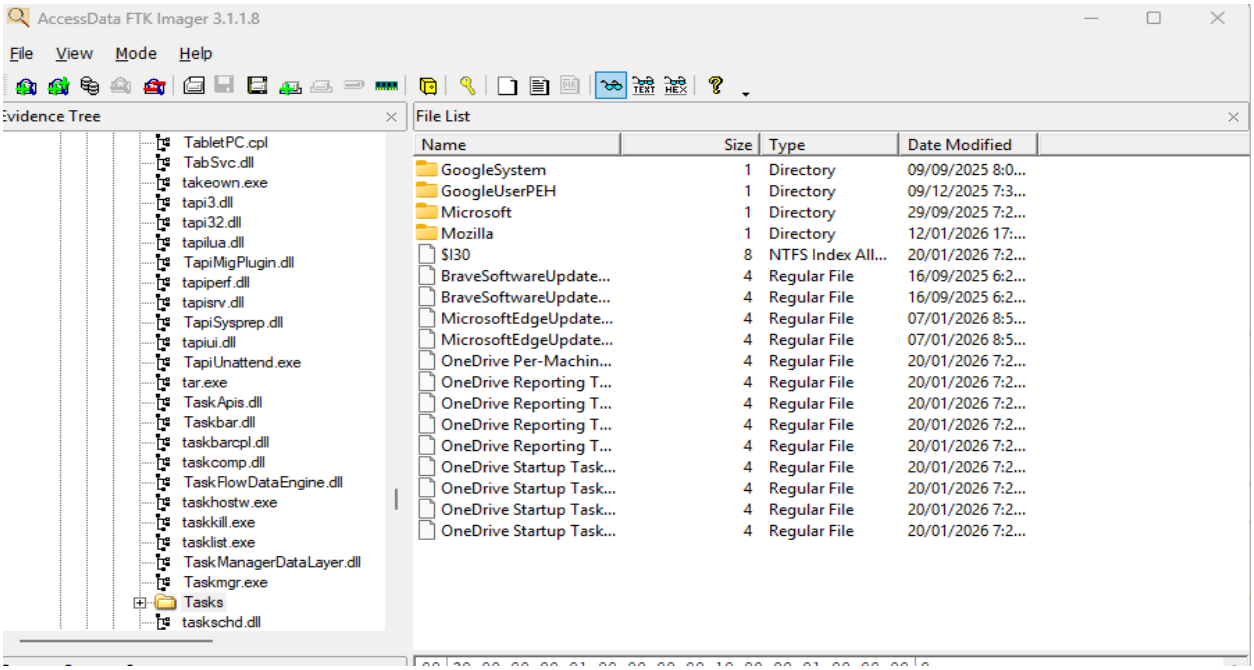


37. Tareas programadas

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:

1. **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".
2. **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.

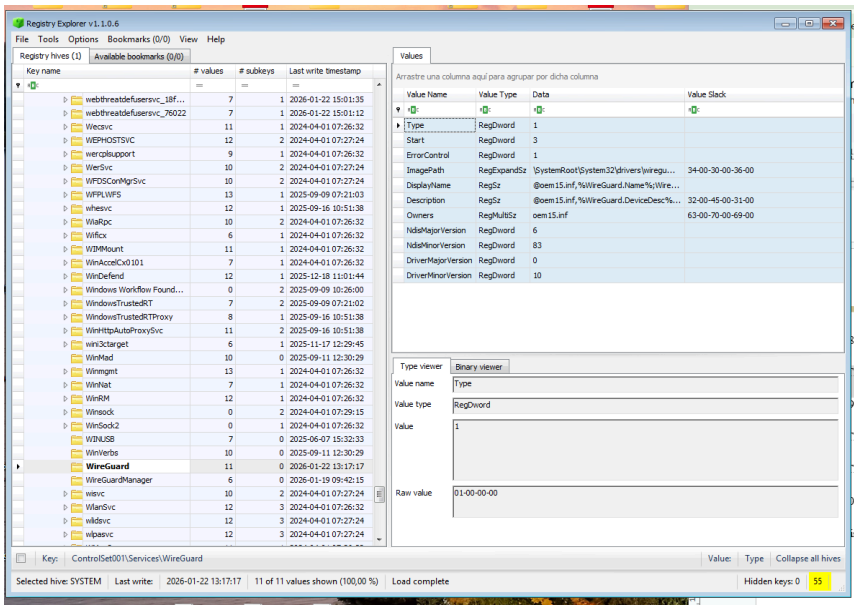
No se han hallado tareas programadas anómalas en la raíz del directorio que indique un intento de persistencia activo por parte de binarios desconocidos en el momento de la adquisición.



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.



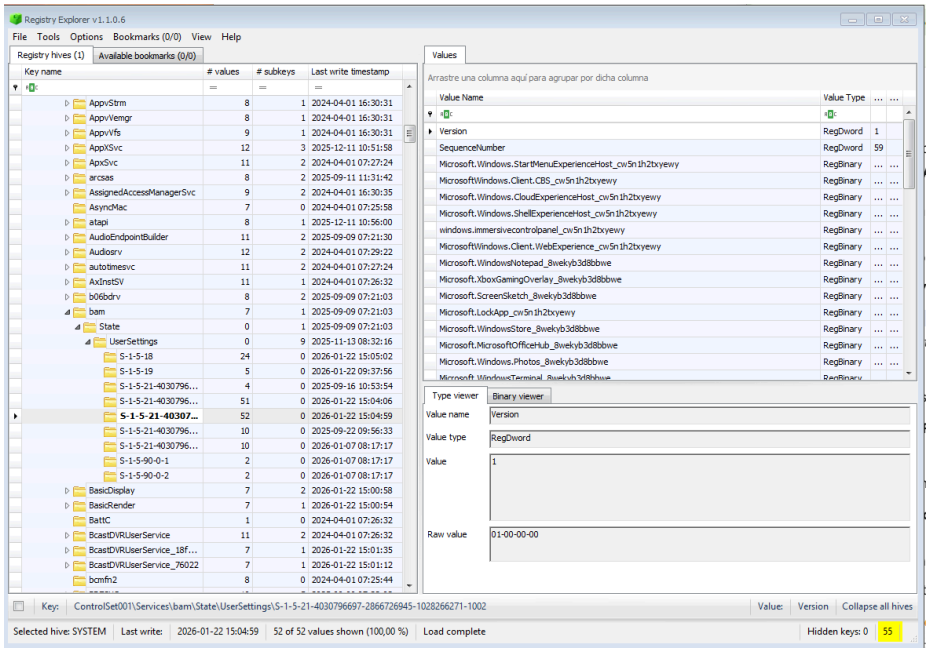
39. BAM (DCode)

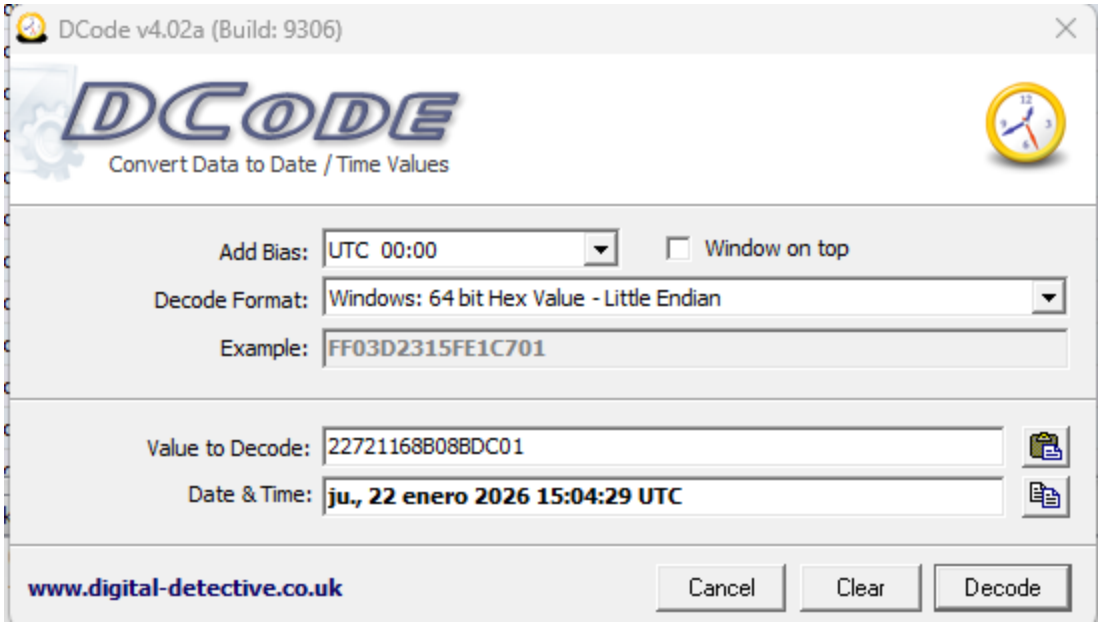
Para garantizar la exactitud de la evidencia y no depender exclusivamente de parsers automáticos, se ha procedido a la decodificación manual del valor RegBinary.

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 (Little Endian)**.

La decodificación ha revelado la fecha exacta de última ejecución:

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





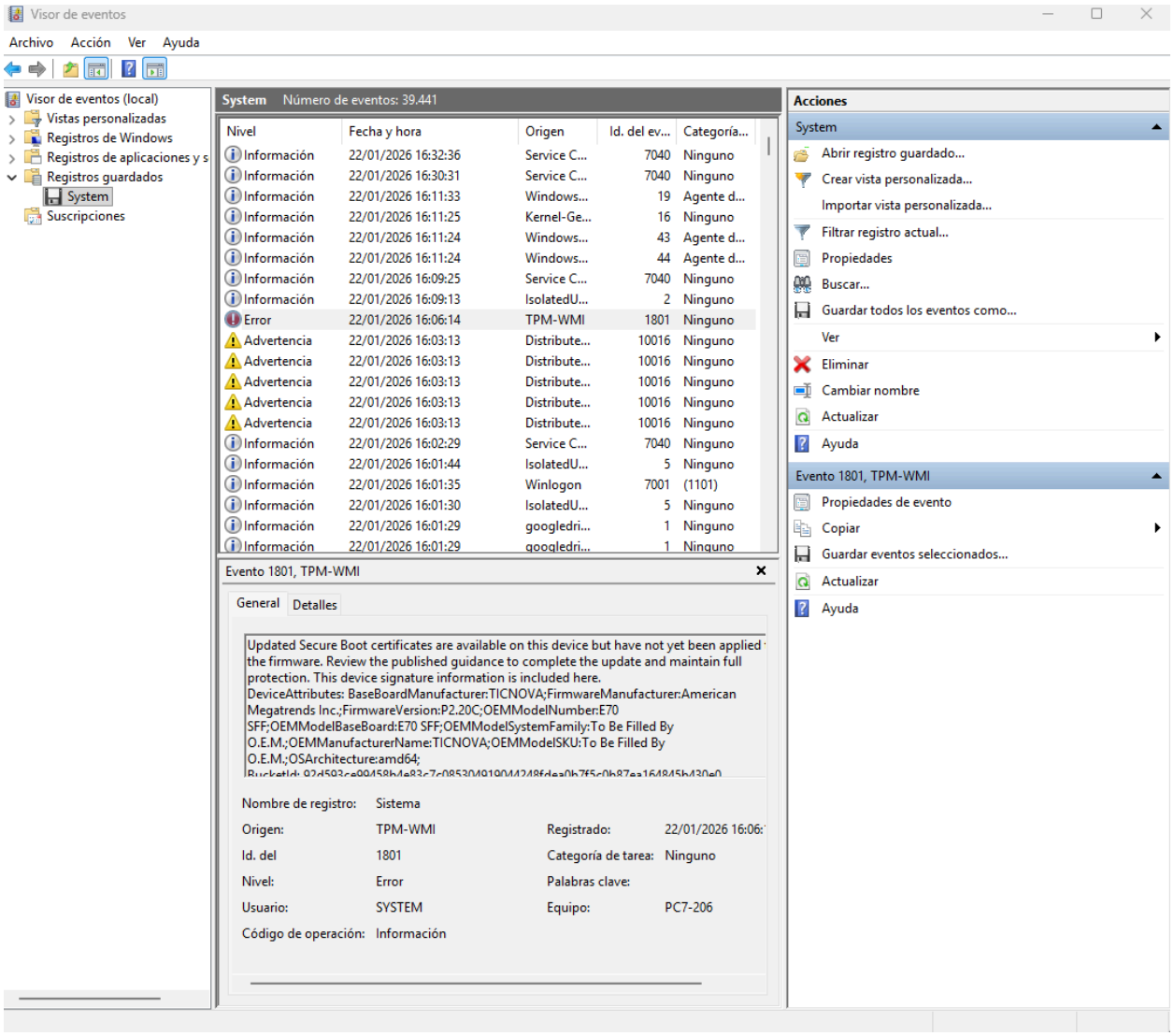
40. Eventos (Event-Log Explorer)

El archivo System.evtxfue 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)


Visor de eventos
Archivo Acción Ver Ayuda
Visor de eventos (local)
Vistas personalizadas
Registros de Windows
Registros de aplicaciones y s
Registros guardados
System
Suscripciones
System Número de eventos: 39.441
Nivel Fecha y hora Origen Id. del ev... Categoría...
Información 22/01/2026 16:32:36 Service C... 7040 Ninguno
Información 22/01/2026 16:30:31 Service C... 7040 Ninguno
Información 22/01/2026 16:11:33 Windows... 19 Agente d...
Información 22/01/2026 16:11:25 Kernel-Ge... 16 Ninguno
Información 22/01/2026 16:11:24 Windows... 43 Agente d...
Información 22/01/2026 16:11:24 Windows... 44 Agente d...
Información 22/01/2026 16:09:25 Service C... 7040 Ninguno
Información 22/01/2026 16:09:13 IsolatedU... 2 Ninguno
Error 22/01/2026 16:06:14 TPM-WMI 1801 Ninguno
Advertencia 22/01/2026 16:03:13 Distribute... 10016 Ninguno
Advertencia 22/01/2026 16:03:13 Distribute... 10016 Ninguno
Advertencia 22/01/2026 16:03:13 Distribute... 10016 Ninguno
Advertencia 22/01/2026 16:03:13 Distribute... 10016 Ninguno
Advertencia 22/01/2026 16:03:13 Distribute... 10016 Ninguno
Información 22/01/2026 16:02:29 Service C... 7040 Ninguno
Información 22/01/2026 16:01:44 IsolatedU... 5 Ninguno
Información 22/01/2026 16:01:35 Winlogon 7001 (1101)
Información 22/01/2026 16:01:30 IsolatedU... 5 Ninguno
Información 22/01/2026 16:01:29 googledri... 1 Ninguno
Información 22/01/2026 16:01:29 googledri... 1 Ninguno
Evento 1801, TPM-WMI
General Detalles
Updated Secure Boot certificates are available on this device but have not yet been applied
the firmware. Review the published guidance to complete the update and maintain full
protection. This device signature information is included here.
DeviceAttributes: BaseBoardManufacturer:TICNOVA;FirmwareManufacturer:American
Megatrends Inc.;FirmwareVersion:P2.20C;OEMModelNumber:E70
SFF;OEMModelBaseBoard:E70 SFF;OEMModelSystemFamily:To Be Filled By
O.E.M.;OEMManufacturerName:TICNOVA;OEMModelSKU:To Be Filled By
O.E.M.;OSArchitecture:amd64;
Nombre de registro: Sistema
Origen: TPM-WMI
Registrado: 22/01/2026 16:06:
Id. del 1801
Categoría de tarea: Ninguno
Nivel: Error
Palabras clave:
Usuario: SYSTEM
Equipo: PC7-206
Código de operación: Información
Acciones
System
Abrir registro guardado...
Crear vista personalizada...
Importar vista personalizada...
Filtrar registro actual...
Propiedades
Buscar...
Guardar todos los eventos como...
Ver
Eliminar
Cambiar nombre
Actualizar
Ayuda
Evento 1801, TPM-WMI
Propiedades de evento
Copiar
Guardar eventos seleccionados...
Actualizar
Ayuda