



Curso de Ciberseguridad

Análisis Forense en Windows

Análisis Forense Informático



Cortana	4
Notificaciones en Windows 10	6
Timeline	8
Windows Store	10
Thumbnails	14
Thumbcache	15
Papelera de Reciclaje	16
OfficeFileCache	21
OfficeBackstage	22
IP Publica	22
Histórico de Ejecución de Powershell	23
Historial del portapapeles	24
Ejecución de programas	25
Windows Prefetch	25
SuperFetch	27
SRUM	28
AppCompatCache (ShimCache)	31
Amcache.hve	33
RecentFileCache	34
Tareas Programadas	36
Servicios	37
BAM	38
Eventos de Windows	40
Eventos de Seguridad	43
Eventos de Seguridad relacionados con la autenticación del usuario	44
Visión de eventos de Windows	49
Recuperación de eventos borrados en Windows	50
Análisis de casuísticas más comunes en cuanto a seguridad en Eventos.	53
BruteForce Attack	53
Remote Desktop Protocol	54
RDP: Conexión Satisfactoria	54
RDP: Conexión No satisfactoria	58
RDP: Conexión LogOFF	59
RDP: Reconexión	59
RDP: Sesión desconectada	59



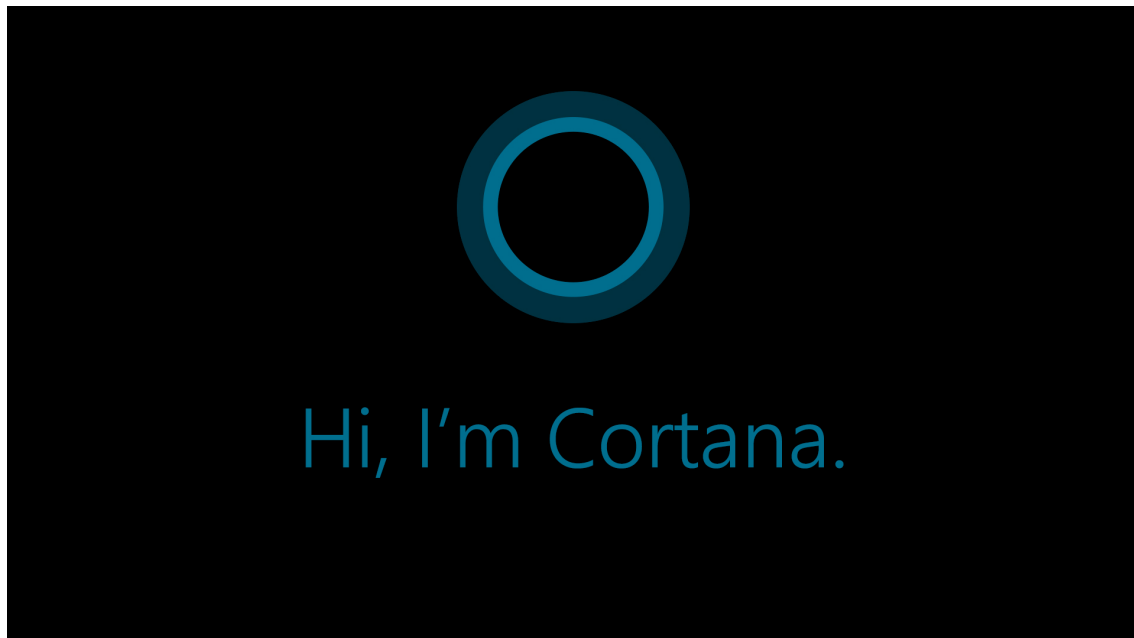
Cambio de Hora	60
Dispositivos USB	60
Apagado/arranque del Sistema	65
Vaciado de Logs	67
Eventos relacionados con la RED	68

QUANTIKA¹⁴



CORTANA

Windows 10 trae una nueva característica, el asistente personal Cortana, el cual expande la búsqueda que había sido introducida en Windows 8.



Cortana puede:

- ◆ Buscar ficheros locales, en el Windows Store.
- ◆ Puede establecer recordatorios
- ◆ Puede iniciar contactos para escribir un email

Las bases de datos de Cortana en SQLITE

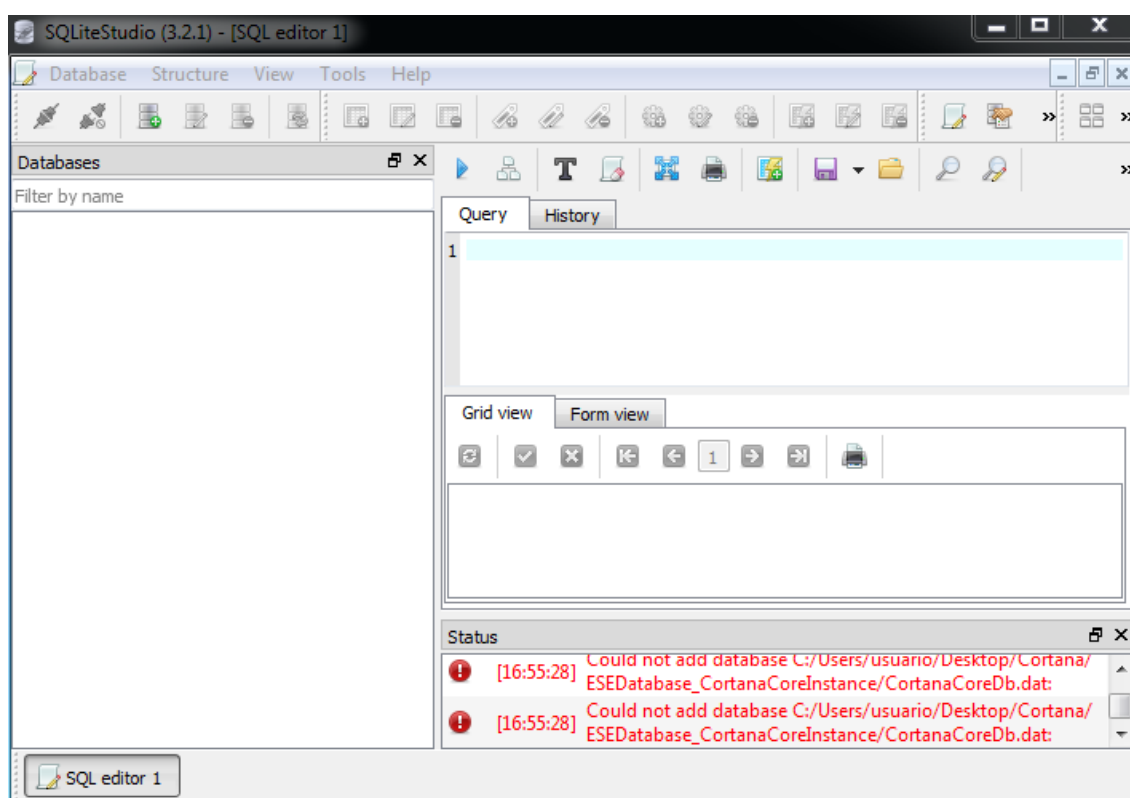
- ◆ `\Users\user_name\AppData\Local\Packages\Microsoft.Windows.Cortana_xxxx\LocalState\ESDatabase_CortanaCoreInstance\CortanaCireDb.dat`

Esta base de datos desaparece desde la compilación de Windows 10.0.17763.55

Tablas interesantes dentro de la base de datos:

- ◆ Location triggers
 - Latitude/Longitude and y nombre del lugar de búsqueda
- ◆ Geofences
 - Latitud/Longitud para los reminders
- ◆ Reminders
 - Creación y finalización en formato UNIX time.

Para poder abrir este tipo de base de datos, utilizaremos la herramienta SQLiteStudio.

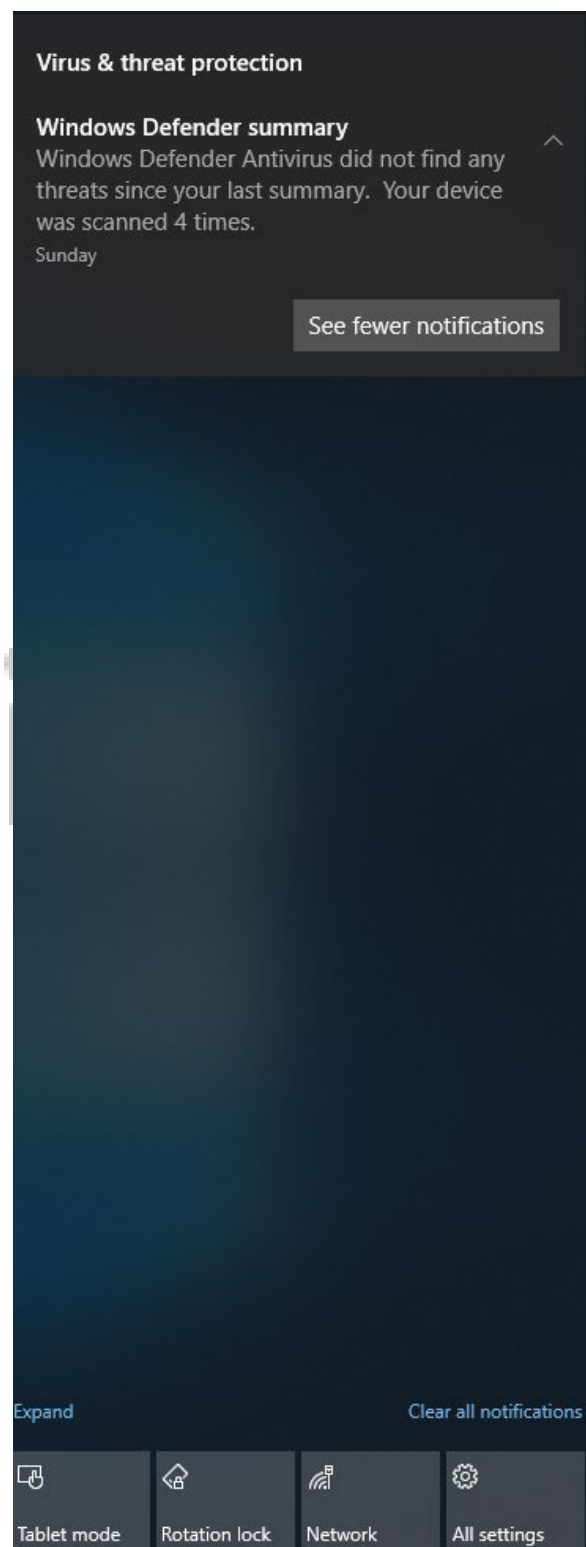


Para ello, solamente deberíamos añadir la base de datos a la aplicación e ir seleccionando tabla, por tabla para viendo la información.



NOTIFICACIONES EN WINDOWS 10

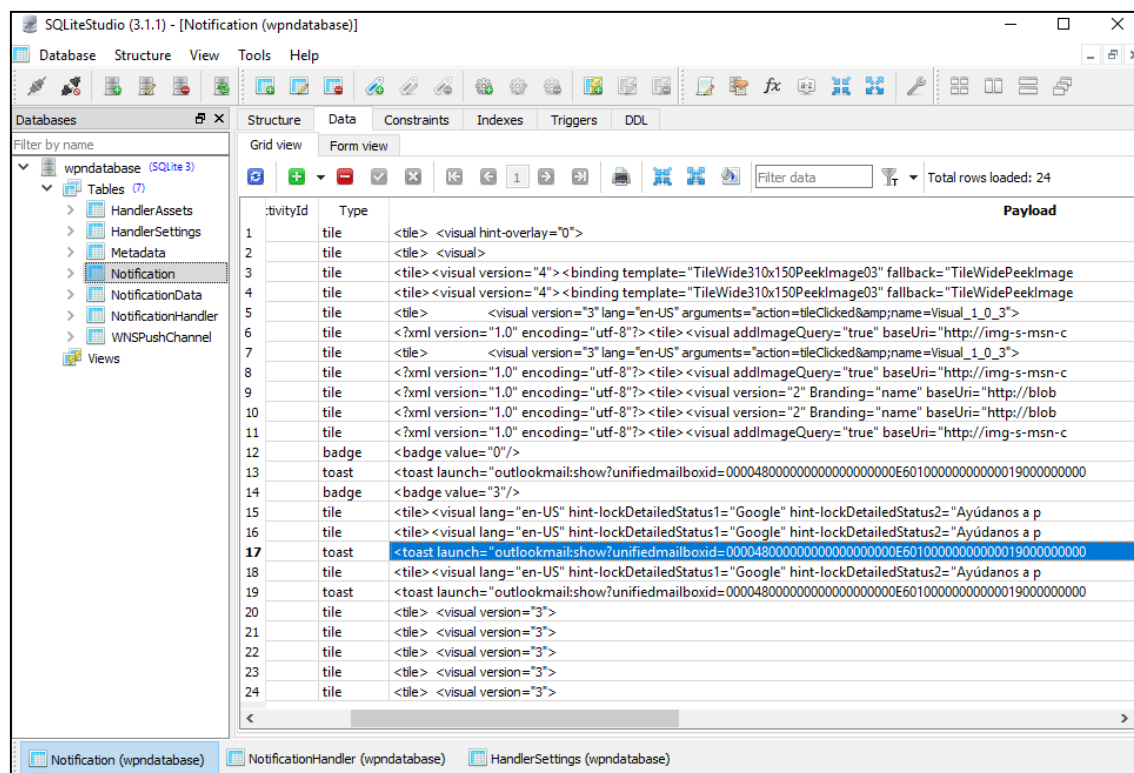
Las notificaciones de Windows 10, se utilizan para que las aplicaciones muestren un mensaje de alerta en la parte derecha de la pantalla. Es posible que los usuarios puedan configurar las notificaciones para recordatorios propios de tareas, tales como eventos y alertas de correo electrónico. Estas notificaciones también se le llaman Notificaciones Toast.



Ruta: \Users\user_name\AppData\Local\Microsoft\Windows\Notifications\

- ◆ appdb.dat -> base de datos SQLite antes del Aniversario de Windows
- ◆ wpndatabase.db -> base de datos SQLite después del Aniversario de Windows

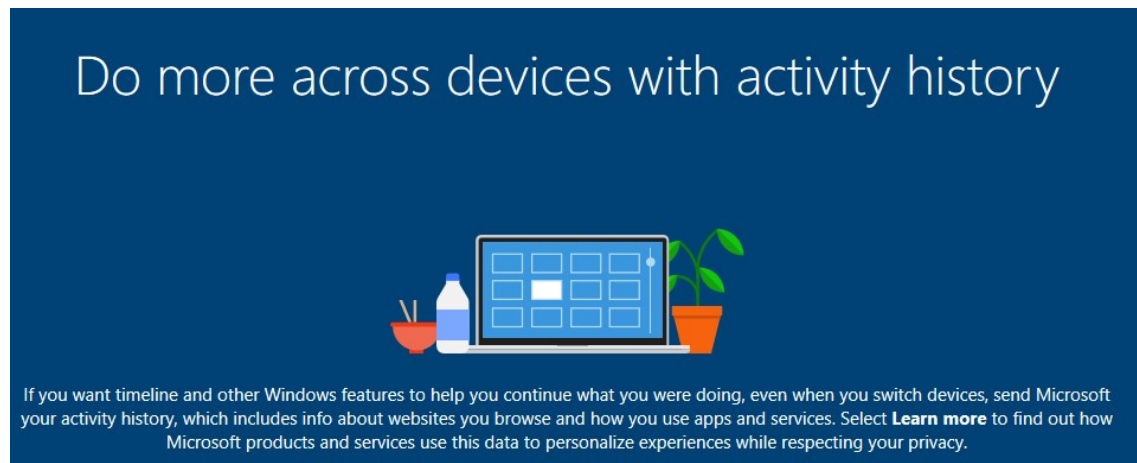
Captura de pantalla de la base de datos wpndatabase.db



*Ver Vídeo: 001/MÓD.4 -Notificaciones Windows

TIMELINE

En abril de 2018 – Windows 10, Microsoft lanzo una actualización que incluía una nueva característica llamada “Timeline”. Esta línea de tiempo o Timeline nos proporciona una cronología tanto de páginas web visitadas, documentos que hayan sido editados, imágenes o aplicaciones que hayan sido ejecutadas.



Esta opción puede ser deshabilitada cuando el administrador instala el sistema operativo, pero es un artefacto que siempre deberemos de comprobar si existe o no.

Para poder analizar la base de datos que contiene el Timeline, debemos extraerla de la siguiente ruta:

`\Users\<profile>\AppData\Local\ConnectedDevicesPlatform\<profile>\ActivitiesCache.db`

Se puede encontrar más información del funcionamiento de del Timeline aquí:

<https://kacos2000.github.io/WindowsTimeline/WindowsTimeline.pdf>

Una vez extraída la base de datos podremos abrirla directamente con SQLite Studio para ver las tablas, o utilizar la herramienta WxTCmd:

```
WxTCmd version 0.3.1.0
Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/WxTCmd

  f      File to process. Required
  csv    Directory to save CSV formatted results to. Be sure to include the full path in double quotes
  dt      The custom date/time format to use when displaying timestamps. See https://goo.gl/CNVq0k for options. Default is: yyyy-MM-dd HH:mm:ss
  cs      When true, use comma instead of tab for field separator. Default is true

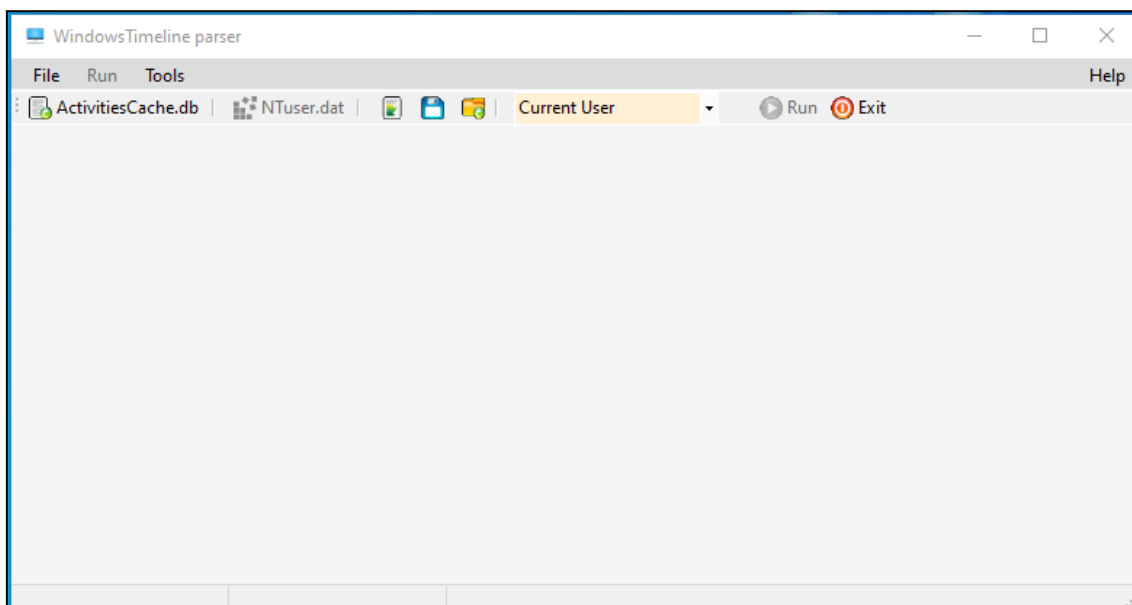
Examples: WxTCmd.exe -f "C:\Users\eric\AppData\Local\ConnectedDevicesPlatform\L.eric\ActivitiesCache.db" --csv c:\temp
          Database files are typically found at 'C:\Users\<profile>\AppData\Local\ConnectedDevicesPlatform\L.<profile>\ActivitiesCache.db'

          Short options (single letter) are prefixed with a single dash. Long commands are prefixed with two dashes
-f is required. Exiting
C:\Digital Forensics\Applications\WxTCmd>
```

Dicha herramienta nos genera dos ficheros, que podremos visualizarlos con la herramienta Timeline Explorer.

**Ver Video: 002 /MÓD4 – Timeline en Windows 10*

Otra herramienta que dispone de interfaz grafico y que puede interpretar de manera más fácil la línea de tiempo en Windows es [Windows TimeLine Parser](#) :

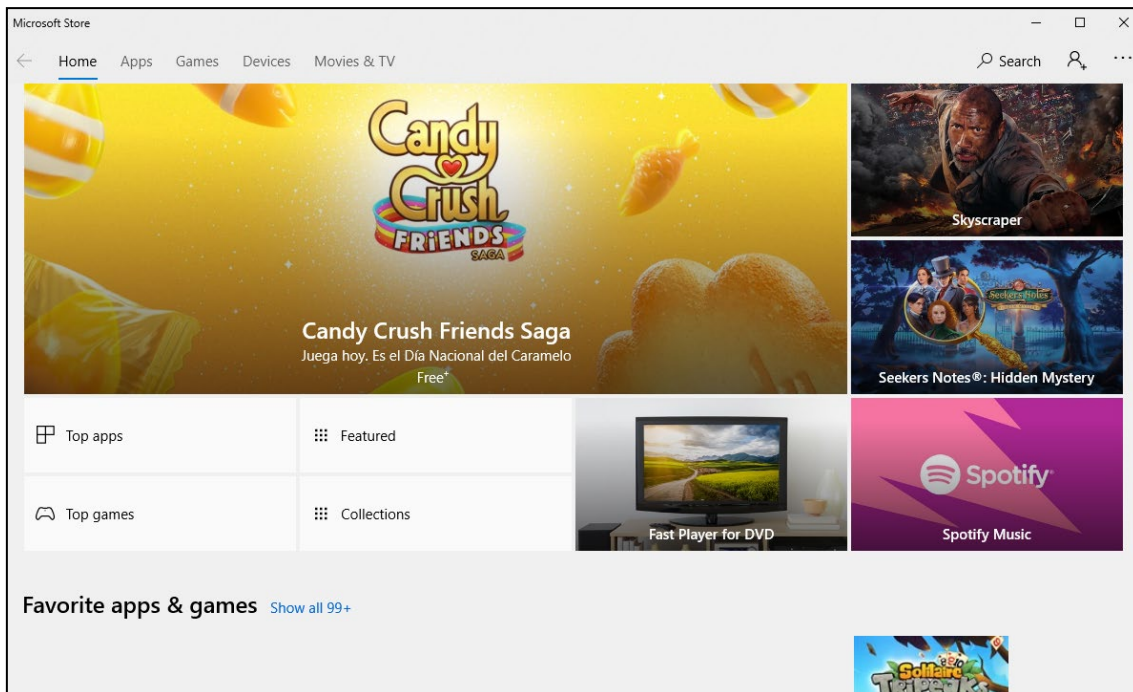


**Ver Video: 003 /MÓD4 – WindowsTimelineParser*



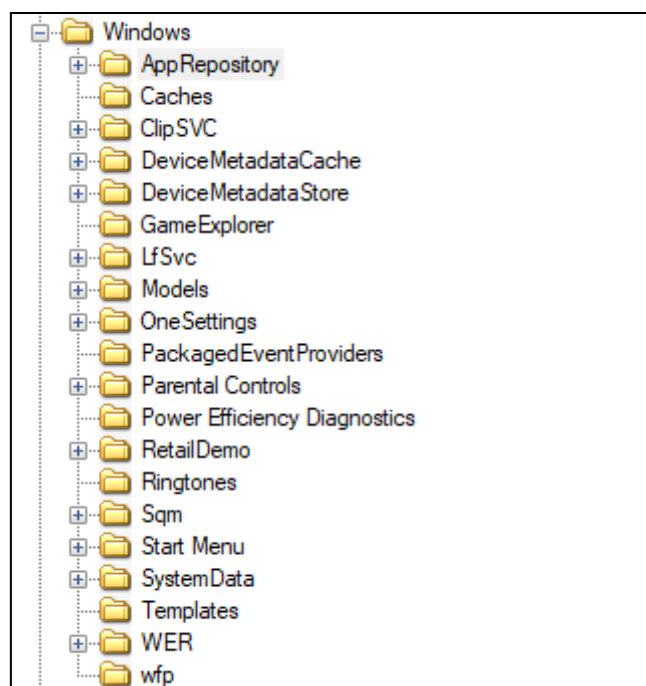
WINDOWS STORE

Hoy en día Windows 10 dispone de un repositorio de aplicaciones que pueden ser descargadas de manera segura. Este tipo de artefacto forense puede indicarnos que aplicaciones fueron instaladas y en que momento.

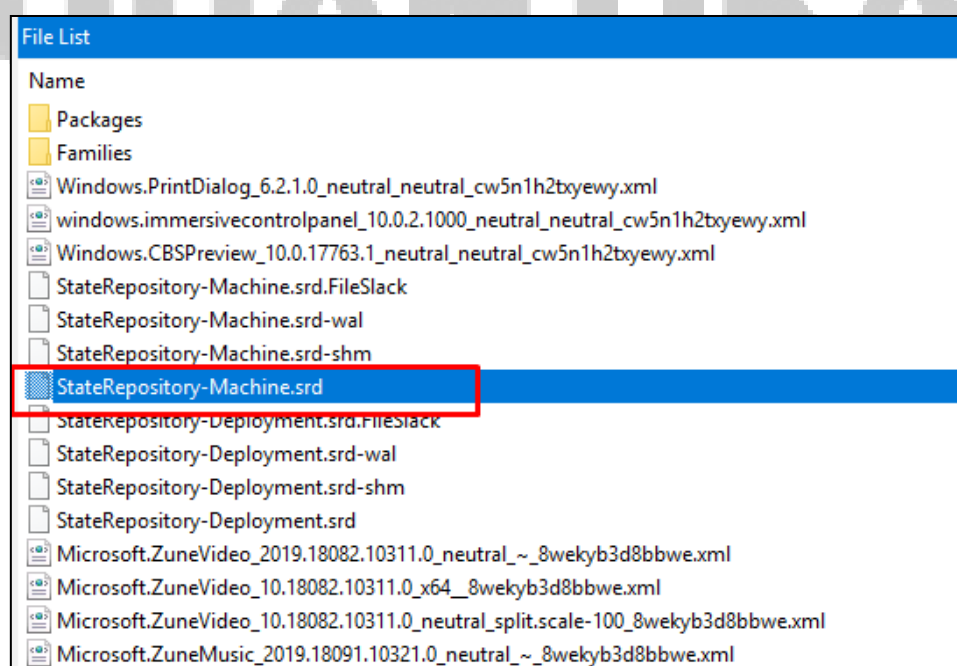


Las aplicaciones instaladas se encuentran en la siguiente ruta del sistema de archivos:

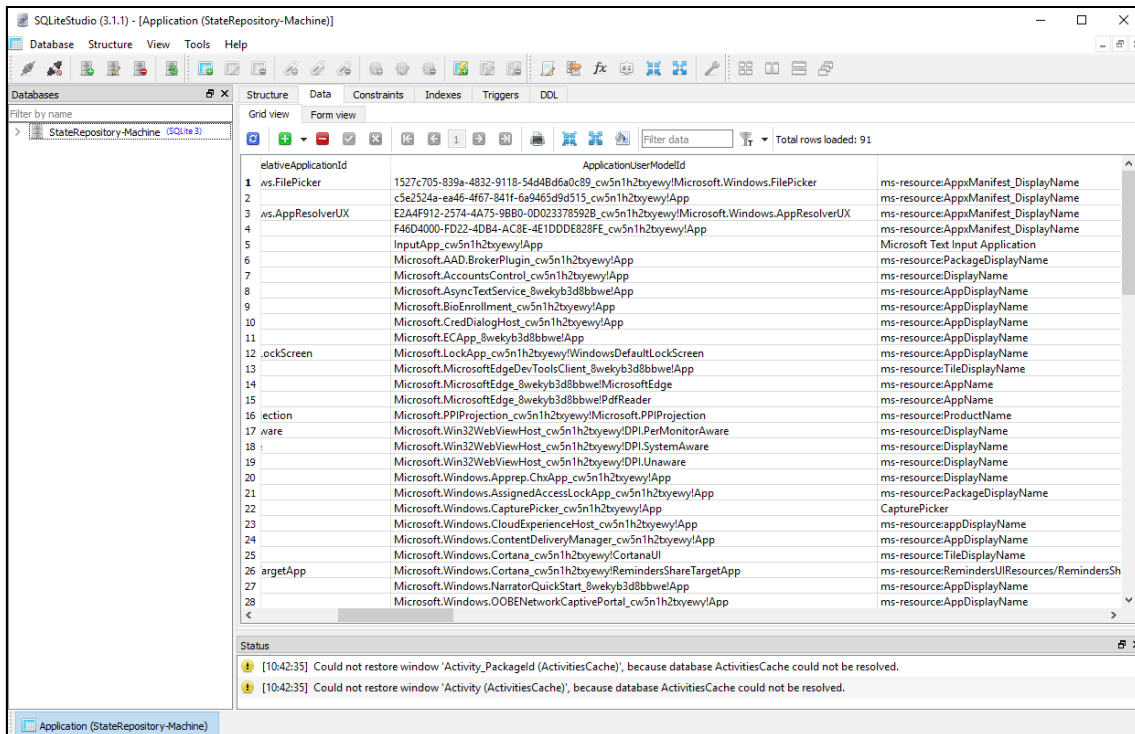
\ProgramData\Microsoft\Windows\AppRepository



Esta carpeta mantiene un log de cada una de las aplicaciones que es actualmente instaladas en el sistema. Las aplicaciones instaladas se pueden localizar en la base de datos **StateRepository-Deployment.srd**



Aunque hay varias tablas dentro de esta base de datos, incluyendo información sobre las aplicaciones, nos centraremos en una tabla en particular "Application". Gracias a esta tabla, la información contenida puede verse en un visor SQLite.



Las columnas más importantes son:

- ◆ Application ID
- ◆ PackageNumber
- ◆ Display Name

Esta tabla contiene aplicaciones instaladas por el usuario y aplicaciones preinstaladas. Que se hayan desinstalado aplicaciones, se puede detectar mediante la detección de los números relativos en ApplicationID:

119	1	0	277	0	1	0	0	Microsoft.XboxIdentityProvider	Microsoft.XboxIdentityProvider_8wekyb3d8bbwe!Microsoft.XboxIdentityProvider
120	1	0	279	0	1	0	0	App	Microsoft.MicrosoftSolitaireCollection_8wekyb3d8bbwe!App
121	1	0	281	0	1	0	0	App	Microsoft.BingWeather_8wekyb3d8bbwe!App
122	1	0	284	0	1	0	0	App	Microsoft.XboxSpeechToTextOverlay_8wekyb3d8bbwe!App
123	1	0	287	0	1	0	0	App	Microsoft.Print3D_8wekyb3d8bbwe!App
124	1	0	289	0	1	0	0	Microsoft.Xbox.TCUI	Microsoft.Xbox.TCUI_8wekyb3d8bbwe!Microsoft.Xbox.TCUI
126	1	0	294	0	1	0	0	App	Microsoft.Getstarted_8wekyb3d8bbwe!App
129	1	0	302	0	1	0	0	App	Microsoft.OneConnect_8wekyb3d8bbwe!App
133	1	0	314	0	1	1	0	App	Microsoft.WindowsSoundRecorder_8wekyb3d8bbwe!App

En la imagen anterior se puede observar distintos saltos (números relativos) entre el 124 y 126; 126 y 129. Y también desde el 129 hasta el 133.

También podemos localizar aplicaciones mediante el Windows Store en el registro Software:

Aplicaciones Instaladas

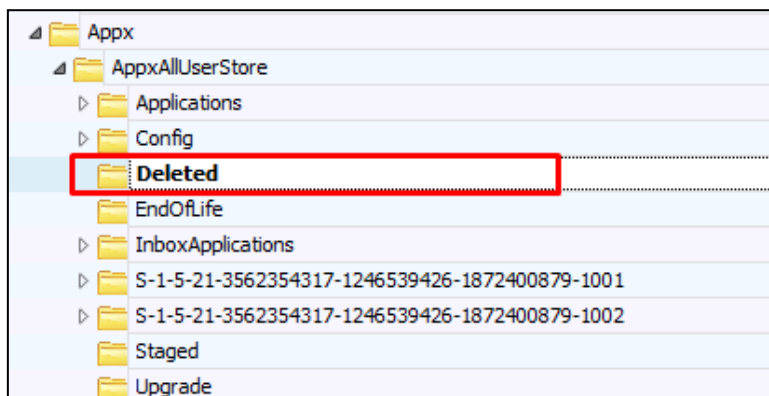
- Software\Microsoft\Windows\CurrentVersion\Appx\AppxAllUserStore\Applications\

AppxAllUserStore
Applications
Microsoft.BingWeather_4.26.12153.0_neutral~_8wekyb3d8bbwe
Microsoft.DesktopAppInstaller_2018.720.2137.0_neutral~_8wekyb3d8bbwe
Microsoft.GetHelp_10.1706.12332.0_neutral~_8wekyb3d8bbwe
Microsoft.Getstarted_6.14.12121.1000_neutral~_8wekyb3d8bbwe
Microsoft.HEIFImageExtension_1.0.11792.0_x64~_8wekyb3d8bbwe
Microsoft.Messaging_2018.727.1430.0_neutral~_8wekyb3d8bbwe
Microsoft.Microsoft3DViewer_5.1807.6012.1000_neutral~_8wekyb3d8bbwe
Microsoft.MicrosoftOfficeHub_2018.614.804.1000_neutral~_8wekyb3d8bbwe
Microsoft.MicrosoftSolitaireCollection_4.2.8172.0_neutral~_8wekyb3d8bbwe
Microsoft.MicrosoftStickyNotes_3.0.118.0_neutral~_8wekyb3d8bbwe
Microsoft.MixedReality.Portal_2000.18090.1131.0_neutral~_8wekyb3d8bbwe
Microsoft.MSPaint_5.1809.1017.0_neutral~_8wekyb3d8bbwe
Microsoft.Office.OneNote_16001.10827.20152.0_neutral~_8wekyb3d8bbwe
Microsoft.OneConnect_5.1807.1991.0_neutral~_8wekyb3d8bbwe
Microsoft.People_2018.905.522.0_neutral~_8wekyb3d8bbwe
Microsoft.Print3D_3.1.2612.0_neutral~_8wekyb3d8bbwe
Microsoft.ScreenSketch_2018.731.48.0_neutral~_8wekyb3d8bbwe
Microsoft.SkypeApp_14.30.73.0_neutral~_kzf8qxf38zq5c

QUANTIKA¹⁴

Aplicaciones borradas

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



El funcionamiento de este Windows Store se puede localizar en los eventos del sistema, sobre todo para identificar errores de funcionamiento:

`\Windows\System32\winevt\Logs\Microsoft-Windows-Store%4Operational.evtx`

THUMBNAILS

Cuando un usuario previsualiza una carpeta de tal manera que la organiza mediante thumbnails, se crea un fichero oculto "thumbs.db", que almacena la preview de imágenes que hay en la carpeta, incluso si las imágenes fueron borradas.

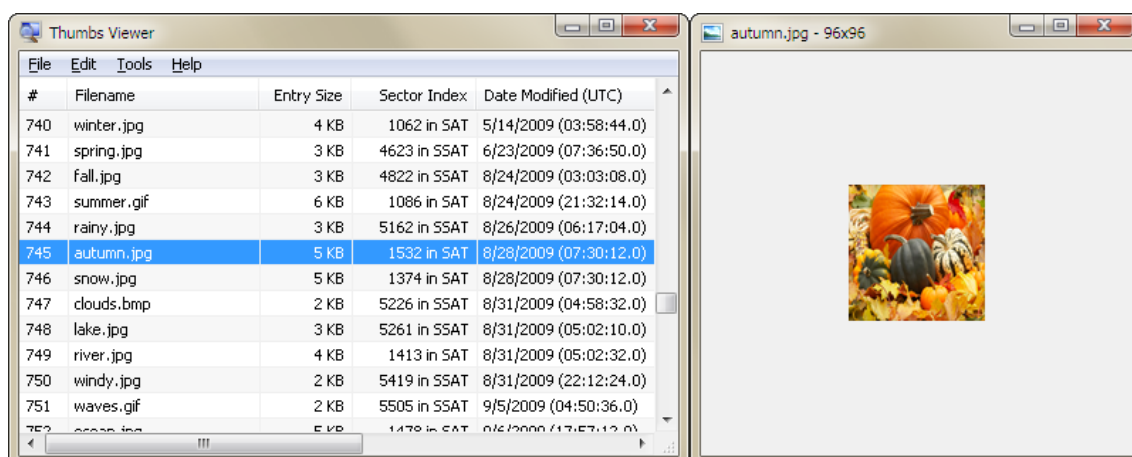
Thumbs.db

- ◆ WinXP/Win8-8.1 -> Creado automáticamente
- ◆ Win7/Win10 -> Automática creado si es accedido vía UNC Path -> \\ruta\ruta\

¿Qué hay en el Thumbs.db?

- ◆ Imagen pequeña de la imagen original incluso si es borrada
- ◆ Última fecha de modificación -> Windows XP
- ◆ Nombre original -> Windows XP

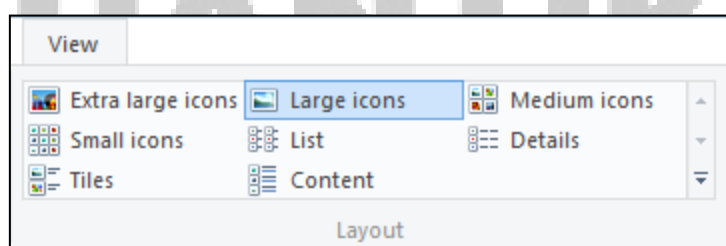
Herramienta que analiza el fichero Thumbs.db: Thumbsviewer



<http://thumbsviewer.github.io/>

THUMBCACHE

El Thumcache, es la evolución del thumbs.db. Su funcionamiento es el mismo.



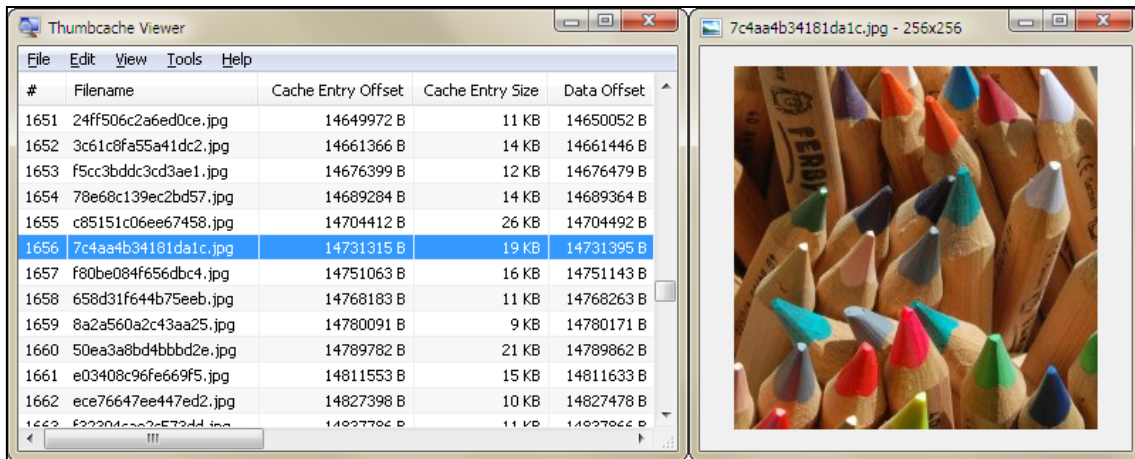
Ruta: **C:\Users\<username>\AppData\Local\Microsoft\Windows\Explorer**

- ◆ Solo Thumbnails
- ◆ Localización de donde estuvo ese thumbnails
- ◆ Solo para Windows 7 / 8 / 10

En la carpeta anterior, se encuentran los vistas preliminares de las imágenes en función del tamaño. De esta manera se adapta a los requisitos del usuario.

- ◆ Thumbcache_32.db -> small
- ◆ Thumbcache_96.db -> medium
- ◆ Thumbcache_256.db -> large
- ◆ Thumbcache_1024.db -> extra large

Herramienta ThumbCache Viewer



<https://thumbcacheviewer.github.io/>

PAPELERA DE RECICLAJE

Carpeta oculta del sistema que contiene un subdirectorio con el SID del usuario. EL SID del usuario lo podemos obtener el fichero SAM.

RECYCLER -> 2000/NT/XP/2003

- ◆ Archivo oculto llamado INFO2
- ◆ Contiene la fecha de borrado y el nombre del archivo original

\$Recycle.bin -> Vista/Win7/Win8/Win10

- ◆ El archivo es ASCII y UNICODE
- ◆ La fecha del borrado y el nombre del fichero original borrado están en ficheros distintos
- ◆ \$I -> Información del fichero (fecha de borrado)
- ◆ \$R -> el contenido del fichero

Solo los ficheros que son borrados desde el Explorer de Windows van a esta localización.

No es un borrado como tal, ya que los ficheros se encuentran disponibles.

Si el usuario realiza SHIFT + borrado el fichero no pasa por la papelera de reciclaje

A nivel del sistema de archivos, el fichero original es movido a la papelera de reciclaje y renombrado con \$R{nombre} y se crea un fichero con \$I{nombre} que contiene la fecha del "borrado". El borrado real, se procederá de verdad cuando la papelera se haya vaciado.

Herramienta para procesar la papelera: Rifiuti

[illegible]

Dos versiones de la herramienta en función del sistema operativo:

Program	Recycle bin from OS	Purpose
rifiuti-vista	Vista or above	Scans \\${Recycle.bin} style folder
rifiuti	Windows 95 to XP/2003	Reads INFO or INFO2 file in \RECYCLED or \RECYCLER folder

***Ver Video: 004/MÓD. 4 – Rifitui**

En Windows 10, existe una opción llamada “Sensor de Almacenamiento” que permite al sistema operativo eliminar los ficheros por él mismo.

Almacenamiento

Sensor de almacenamiento puede liberar espacio automáticamente si se eliminan los archivos que no se necesitan, como los archivos temporales y el contenido de la papelera de reciclaje.






☒ Activado

[Configurar Sensor de almacenamiento o ejecutarlo ahora](#)

Windows (C:) - 953 GB

754 GB usados 199 GB libre

Así es como se usa tu almacenamiento y cómo puedes liberar espacio.

	Otros 266 GB Administrar otras carpetas grandes
	Escritorio 245 GB Administrar la carpeta Escritorio
	Documentos 117 GB Administrar la carpeta Documentos
	Aplicaciones y características 48,8 GB Desinstalar aplicaciones y características no usadas o no deseadas
	Archivos temporales 13,0 GB Elegir los archivos temporales que se van a quitar

[Mostrar más categorías](#)

Este sensor de almacenamiento se puede configurar desde el panel de control, así como establecer cuando debe vaciarse de manera automática la papelera de reciclaje.



Configurar Sensor de almacenamiento o ejecutarlo ahora

Sensor de almacenamiento

☒ Activado

Sensor de almacenamiento se ejecuta cuando queda poco espacio en disco. Limpiamos espacio suficiente para ayudar a que el sistema se ejecute de forma óptima. El mes pasado, limpiamos 3,35 GB de espacio en disco.

Ejecutar Sensor de almacenamiento

Cuando haya poco espacio libre en el disco ▾

Archivos temporales

☒ Elimina los archivos temporales que mis aplicaciones no usan.

Eliminar archivos de la papelera de reciclaje si llevan en esta más de:

30 días ▾

Eliminar archivos de la carpeta Descargas si no se han abierto durante más de:

Nunca ▾

Liberar espacio ahora

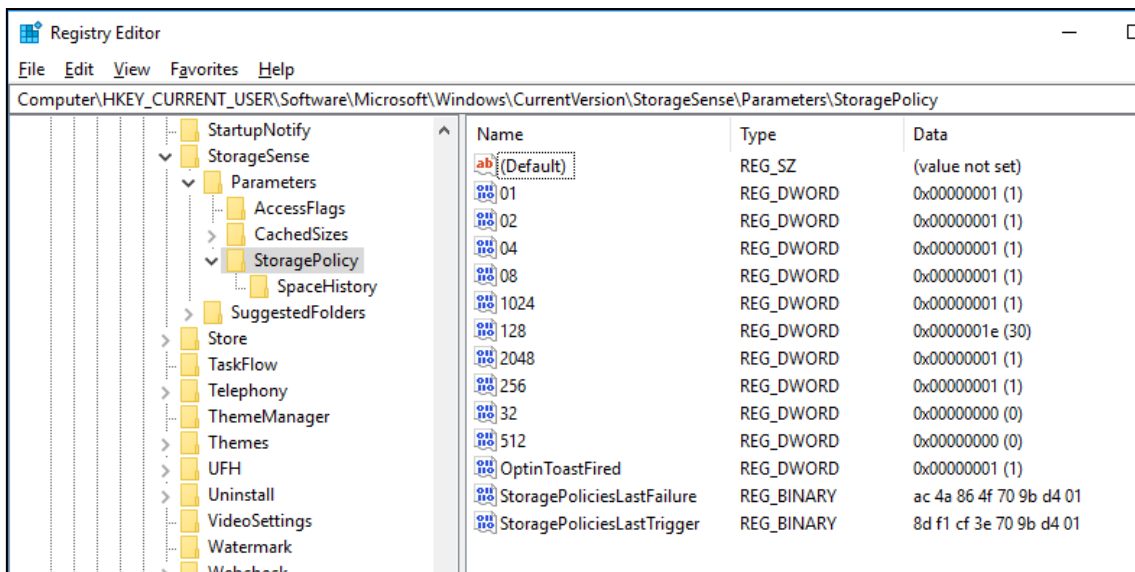
Si te queda poco espacio, podemos intentar limpiar archivos con la configuración de esta página.

Limpiar ahora

La configuración este sensor de almacenamiento la podemos encontrar en el NTUSER.DAT en la siguiente ruta:

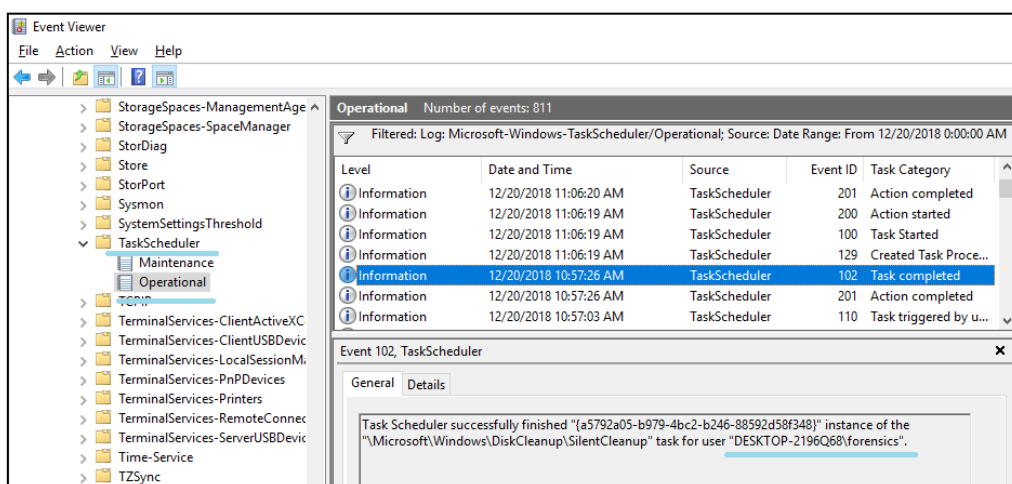
◆ **Software\Microsoft\Windows\CurrentVersion\StorageSense\Parameters\StoragePolicy**

Para analizar el registro podremos utilizar cualquier herramienta de las anteriores vistas, sin embargo para presentar analizar el funcionamiento del sensor, vamos utilizar la herramienta Regedit sobre una maquina encendida:



- ◆ 01 ⇒ Si el campo DATA esta a 1, significa que el sensor esta activado.
- ◆ 256 ⇒ El campo DATA tiene un valor de 30, indica que si los ficheros llevan más de 30 días en la papelera serán borrados.
- ◆ 2048 ⇒ El campo DATA tiene un valor de 1, indica la frecuencia con la que se ejecuta el sensor de almacenamiento para detectar poco espacio y hacer las acciones oportunas. Si tuviese un valor de 7, indicaría 7 días y si tuviese un valor de cero, indicaría que solo se ejecutaría cuando hubiese poco espacio en el disco.
- ◆ 04 ⇒ El campo DATA tiene un valor de 1, indica que borrará los archivos temporales que las aplicaciones no usan.
- ◆ 512 ⇒ El campo DATA tiene un valor de 0, indica que NO borrará los archivos de la carpeta Descargas. Si tuviese valor de 1, 14, 30 o 60, seran los días.

Aunque los eventos de Windows los veremos más adelante, se debe tener en cuenta que estas tareas de limpieza, como bien dice su nombre, generan tareas que serán monitorizadas en los Eventos de las Tareas, tal y como aparece en la siguiente imagen.





OFFICEFILECACHE

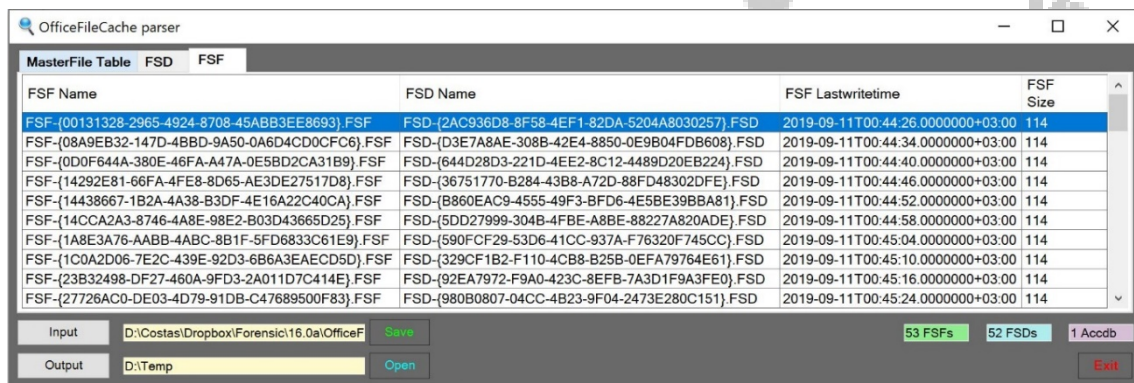
Microsoft Office Document Cache es un artefacto forense cuyo propósito es ser un almacén intermedio para guardar los documentos y todas las modificaciones que se produzcan cuando estamos en la situación de que finalmente van a ser guardados en OneDrive o SharePoint. Para los investigadores, este artefacto es útil porque contiene a menudo solo las múltiples versiones de los documentos office, sino documentos enteros que es posible que no existan en ningún otro sitio.

Este tipo de contenedor será conocido como ODC y cada usuario de Windows dispone de uno en la siguiente ruta:

◆ `\Users\(\Username)\AppData\Local\Microsoft\Office\(\Office Version)\OfficeFileCache`

Dentro de este path encontramos los ficheros FSD, que corresponderán con los documentos en cuestión.

Bajo ciertas circunstancias, estos ficheros FSD también se copian cuando se realice una shadow copy, por lo que podríamos recuperar hasta ficheros borrados, tanto del sistema de archivos como de la shadow copy.

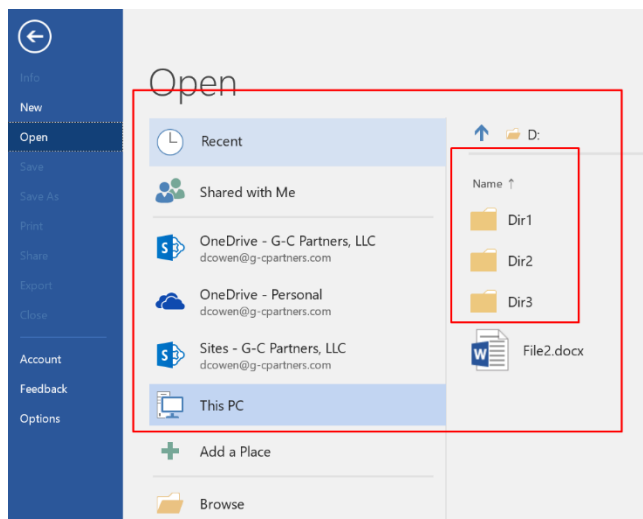


Más información de la herramienta para poder analizar este tipo de artefacto aquí:

<https://github.com/kacos2000/OtherStuff/blob/master/OfficeFileCache/Readme.md>

OFFICEBACKSTAGE

Otro artefacto relacionado con Office es el BackStage. Este artefacto permite reconstruir cual son las unidades de almacenamiento que hay cuando se abre un documento Office:



El artefacto se encuentra en la siguiente ruta:

- \\Users}\\AppData\\Local\\Microsoft\\Office\\16.0\\BackstageinAppNavCache

Para analizarlo es necesario disponer del intérprete de Python y de ejecutar los scripts que se pueden localizar en el siguiente enlace:

<https://github.com/ArsenalRecon/BackstageParser>

IP PUBLICA

En Windows 10 podremos encontrar que IP pública disponía el equipo que estemos analizando, y el momento exacto. Para ello deberemos analizar los Event Trace Log (ETL), en concreto los del tipo “Delivery Optimization Service”

En Windows podremos encontrar los ficheros ETL en la siguiente carpeta con este formato:

- C:\\Windows\\ServiceProfiles\\NetworkService\\AppData\\Local\\Microsoft\\Windows\\DeliveryOptimization\\Logs\\dosvc.20181111_180339_399.etl

Como Podemos apreciar el propio fichero ETL, nos va indicar el momento exacto que se registró la IP pública. Para parsear los ficheros ETL, utilizaremos la herramienta:



<https://github.com/forensiclunch/ETLParser>

```
ETL Parser v0.3, Runtime: 11/06/2020 19:08:57 UTC
=====
Parsing files.....

[BEGIN_PARSE] 11/06/2020 19:08:57 UTC File 1 of 10. Started parsing domgmt.20181003_172143_328.etl.
[PARSE_FINISHED] 11/06/2020 19:08:57 UTC 5 events parsed.

[BEGIN_PARSE] 11/06/2020 19:08:57 UTC File 2 of 10. Started parsing domgmt.20181008_073921_037.etl.
[PARSE_FINISHED] 11/06/2020 19:08:57 UTC 5 events parsed.
```

Una vez parseados nos generará un fichero CSV y deberemos de buscar la palabra “ExternalIpAddress”:

```
'msg: GEO: Refreshing configs: https://geo-prod.do.dsp.mp.microsoft.com/geo/?doClientVersion=10.0.17763.1&pro
'msg: Connecting to the following host: geo-prod.do.dsp.mp.microsoft.com', 'func: CWinHttpAgent::DoConnect',
'msg: GEO: response: {"ExternalIpAddress": "217.182.232.207", "CountryCode": "GB", "KeyValue_EndpointFullUri": "htt
'msg: Version: 2A3C4F2EE266A5EFD325A0562F5847A53270FAE5AC4094D93D9BD412689920F4 is new for type: 1', 'func: CC
'msg: KV: Refreshing configs: https://kv01-prod.do.dsp.mp.microsoft.com/all?doClientVersion=10.0.17763.1&count
```

**Ver Video: 005/MÓD. 4 – ETLPARSER*

HISTÓRICO DE EJECUCIÓN DE POWERSHELL

PowerShell es una interfaz de consola (CLI) con posibilidad de escritura y unión de comandos por medio de instrucciones (scripts en inglés).

```
Windows PowerShell
PS C:\Users> powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

PS C:\Users>
```

Powershell no solo permite interactuar con el sistema operativo, sino también con programas de Microsoft como SQL Server, Exchange o IIS. La principal utilidad de Powershell es permitir automatizar tareas administrativas al usuario. De cara a una investigación forense podríamos obtener los últimos comandos que han sido ejecutados desde la interfaz de Powershell.

En Windows 10 con la versión 3 de Powershell, se pueden recuperar los últimos comandos ejecutados incluso, tras reiniciar el sistema operativo. El fichero que contiene todos los comandos lo podemos localizar aquí:

- \\Users}\\%AppData%\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt

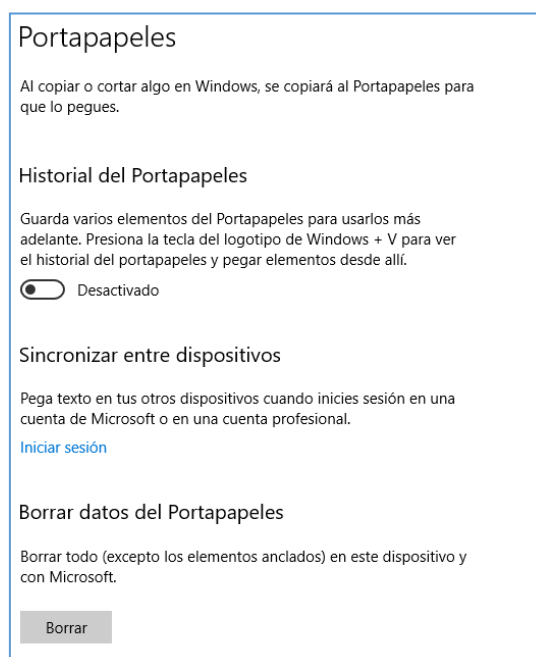
El fichero ConsoleHost_History.txt tendrá los comandos lanzados:

```

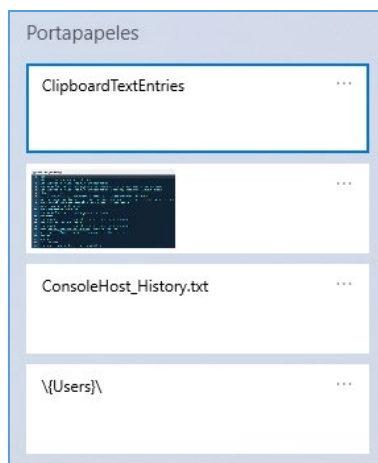
1  dir
2  dir -r | select string "pictures"
3  Get-WmiObject -Class Win32_ComputerSystem
4  Get-WmiObject -Class Win32_ComputerSystem -Property UserName -ComputerName
5  Get-WmiObject -Class Win32_ComputerSystem -Property UserName -ComputerName .
6  find /i "notes"
7  GET-WMIOBJECT win32_diskdrive | Where { $_.InterfaceType -eq 'USB' }
8  gwmi win32_diskdrive | ?{$_interfaceType -eq "USB"} | %{gwmi -Query "ASSOCIATORS
9  wmic logicaldisk get deviceid, volumename, description
10 wmic bios get serialnumber
11 wmic csproduct get name
12 Get-WmiObject -Class Win32_ComputerSystem
13 diskpart
  
```

HISTORIAL DEL PORTAPAPELES

El Historial del Portapapeles fue introducido con la versión 1809 de Windows 10. Al reiniciar el sistema operativo, se eliminan automáticamente los elementos no anclados, es decir, el usuario cuando copia y pega, puede indicar que quiere anclar. Este historial del portapapeles, se pueden encontrar también en memoria, asociados al proceso svchost.exe. En resumen, este artefacto forense, permite almacenar, texto, hipervínculos y gráficos. Esta opción no viene por defecto activada como vemos en la siguiente imagen:



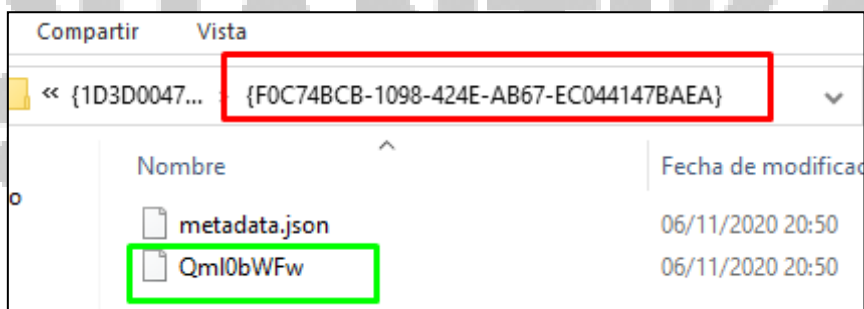
Si hacemos WIN+V podremos ver el portapapeles de nuestro Win10:



Forensicamente hablando, a menos que el usuario ancle el objeto del portapelesse podría encontrar evidencia del mismo, pero esta cifrado. Hoy en día, no se sabe de qué manera está cifrado el fichero.

- %AppData%\Local\Microsoft\Windows\Clipboard

Dentro encontraremos la carpeta HistoryData y Pinned. En Pinned se crea fichero JSON con metadatos de las subcarpetas (GUID, timestamp, source, cloud_id). En la siguiente imagen, podemos distinguir en verde el objeto en cuestión cifrado.



EJECUCIÓN DE PROGRAMAS

En esta sección vamos a ver todos los artefactos forenses que indiquen la ejecución de un programa o proceso.

WINDOWS PREFETCH



La misión de Windows Prefetch es incrementar el rendimiento del sistema con una precarga del ejecutable. El cache mánager monitoriza todos los ficheros y directorios y los mapea contra el fichero .pf (el fichero .pf será el artefacto forense que analizaremos)

- ◆ Deshabilitado en sistemas con disco SSD
- ◆ Muestra cómo y cuándo un binario se ejecutó

Ruta: C:\Windows\Prefetch

- ◆ Limitado a 128 ficheros en XP/VISTA/WIN7
- ◆ Limitado a 1024 ficheros en Win8/Win10
 - {Nombre_ejecutable}-{hash}.pf
 - Windows 10 los prefetch vienen comprimidos
 - El hash está basado en el path del ejecutable y los argumentos que reciben

Ruta: C:\Windows\Prefetch\Layout.ini

- El fichero layout.ini contiene los nombres de los directorios de los ficheros que están en el Prefetch
- El desfragmentador de disco utiliza el layout.ini para realojar todos los directorios y ficheros a un área contigua del disco.

¿Qué indica este artefacto forense?

- ◆ Número de ejecuciones (hasta 8 veces puede registrar)
- ◆ Fechas de las ejecuciones (UTC)
- ◆ El propio fichero, ya indica la ejecución del programa
- ◆ Ficheros abiertos por el programa

Herramienta para analizar los Prefetch: **PeCMD**

```
C:\Digital Forensics\Applications\PEcmd>PEcmd.exe -d "C:\Users\student\Desktop\Prefetch\Prefetch" --html "C:\Users\student\Desktop\Prefetch" -q
PEcmd version 1.2.0.0

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

Command line: -d C:\Users\student\Desktop\Prefetch\Prefetch --html C:\Users\student\Desktop\Prefetch -q
Warning: Administrator privileges not found!

Keywords: temp, tmp

Looking for prefetch files in 'C:\Users\student\Desktop\Prefetch\Prefetch'

Found 371 Prefetch files

----- Processed 'C:\Users\student\Desktop\Prefetch\Prefetch\69.0.3497.100_CHROME_INSTALL-3B1B2BF0.pf' in 0.0268161
0 seconds
----- Processed 'C:\Users\student\Desktop\Prefetch\Prefetch\8E96C6A6-3FFB-4945-A837-BDB2E-D96E0182.pf' in 0.0012659
0 seconds
----- Processed 'C:\Users\student\Desktop\Prefetch\Prefetch\ACRORD32.EXE-ACF2947D.pf' in 0.00254860 seconds -----
---
```

Resultado de ejecutar PeCMD

```

C:\Users\student\Desktop\Prefetch\Prefetch\ACRORD32.EXE-ACF2947D.pf
Source Created: 2018-10-03 18:52:46
Source Modified: 2018-10-03 20:11:06
Source Accessed: 2018-10-17 01:25:48
Last Run: 2018-10-03 20:11:00
Previous Run 0: 2018-10-03 20:11:00
Previous Run 1: 2018-10-03 18:54:13
Previous Run 2: 2018-10-03 18:52:36
Executable Name: ACRORD32.EXE
Run Count: 4
Size: 43486
Hash: ACF2947D
Version: Windows 10
Volume 0 Name: \VOLUME{01d45b901e9ea160-8a1ed5ac}
Volume 0 Serial: 8A1ED5AC
Volume 0 Created: 2018-10-04 03:12:44
Directories: \VOLUME{01d45b901e9ea160-8a1ed5ac}\PROGRAM FILES (X86),
\VOLUME{01d45b901e9ea160-8a1ed5ac}\PROGRAM FILES (X86)\ADOBE\ACROB
READER DC\READER, \VOLUME{01d45b901e9ea160-8a1ed5ac}\WINDOWS, \VO
8a1ed5ac}\WINDOWS\GLOBALIZATION, \VOLUME{01d45b901e9ea160-8a1ed5ac}
8a1ed5ac}\WINDOWS\REGISTRATION, \VOLUME{01d45b901e9ea160-8a1ed5ac}
\VOLUME{01d45b901e9ea160-8a1ed5ac}\WINDOWS\SYSWOW64, \VOLUME{01d
CONTROLS_6595B64144CCF1DF_6.0.17763.1_NONE_37ED96E613BCB533, \VOL
8a1ed5ac}\PROGRAMDATA\MICROSOFT, \VOLUME{01d45b901e9ea160-8a1ed5ac}
8a1ed5ac}\PROGRAMDATA\MICROSOFT\WINDOWS\CACHES

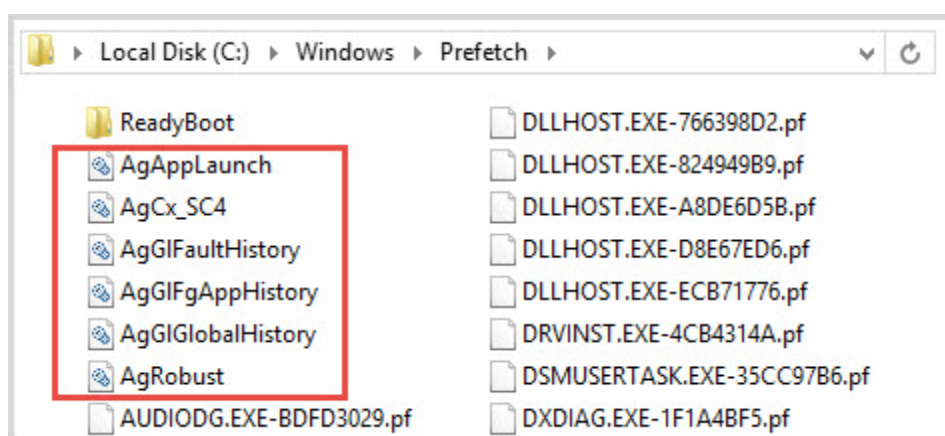
```

*Ver Video 006/MÓD. 4 - Prefetch

SUPERFETCH

Superfetch consiste en una serie de bases de datos localizados en la carpeta

C:\Windows\Prefetch\Ag*.db, que tienen como misión optimizar el uso de memoria. **No reemplaza al servicio Prefetch**



¿Qué podemos obtener?

- ◆ Nombre de la aplicación

- ◆ Número de ejecuciones
- ◆ Ficheros necesarios que son utilizados por el binario.
- ◆ Volumen accedido
- ◆ Path completo
- ◆ TimeFrames
- ◆ Timestamp

Herramienta para analizar el Superfetch: **CrowdResponse**

```

Administrator: Command Prompt
D:\CrowdResponse>CrowdResponse.exe @superfetch /?
@SuperFetch - Windows SuperFetch file processor.

Syntax:
@SuperFetch [-36s] [<dir>]

-3          - Treat files in <dir> as if they came from a 32 bit OS
-6          - Treat files in <dir> as if they came from a 64 bit OS
-s          - Recursive processing of <dir>
<dir>       - Optional directory of Superfetch db files to process

Environment variables are automatically expanded in <dir>.
Be sure to enclose paths that contain spaces within double quotes.
D:\CrowdResponse>CrowdResponse.exe @superfetch > host.superfetch.xml
  
```

<https://www.crowdstrike.com/resources/community-tools/crowdresponse/>

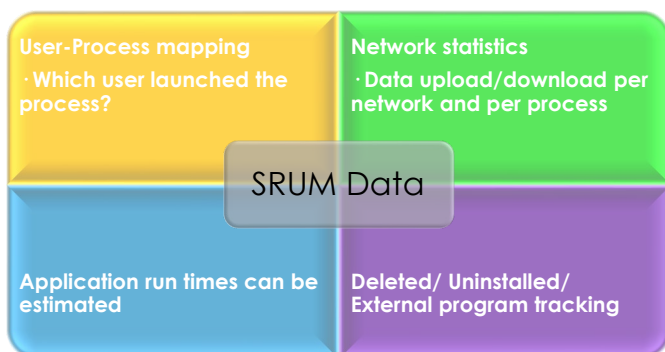
SRUM

System Resource Usage Monitor (SRUM) es un artefacto forense que está destinado a monitorizar los recursos que consume un proceso.

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

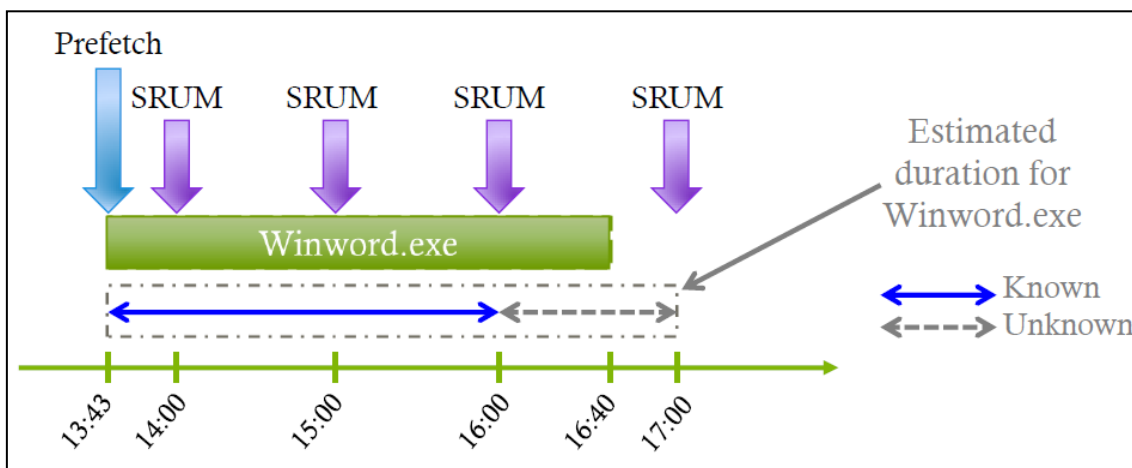
- ◆ A partir de Windows 8
- ◆ Es una Base de datos en formato ESE

Se ha llegado a identificar hasta 60 días de monitorización y nos puede indicar:



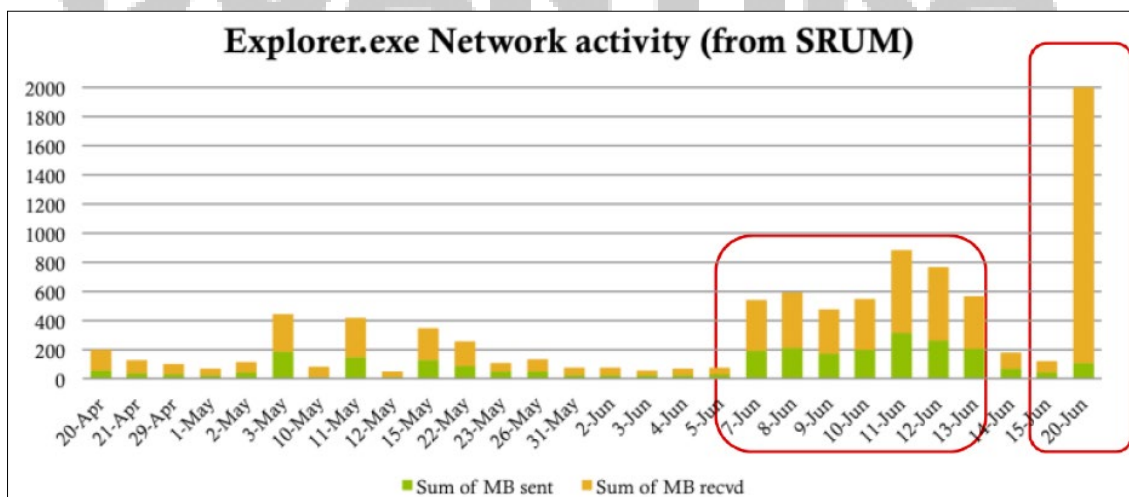
- ◆ AppID y Path
- ◆ Usuario que ejecuta
- ◆ Bytes enviados
- ◆ Bytes recibidos
- ◆ Interfaz de red
- ◆ Tiempo de conexión
- ◆ Tiempo de duración

El Prefetch indica el arranque de un proceso, pero no la duración:



Ejemplo del proceso: **Explorer.exe**

La actividad es actualizada cada 60 min en la base de datos o durante un apagado correcto



Si realizamos un apagado incorrecto hay que reparar la base de datos ESE mediante el comando: **esentul /mh SRUDB.dat**

Herramienta que nos permite analizar el fichero **SRUDB.dat**

SRUM DUMP

```

C:\Binarios\srum-dump-master>srum_dump.exe -h
usage: srum_dump.exe [-h] [--SRUM_INFILE SRUM_INFILE]
                    [--XLSX_OUTFILE XLSX_OUTFILE]
                    [--XLSX_TEMPLATE XLSX_TEMPLATE] [--REG_HIVE REGHIVE]
                    [--quiet]

Given an SRUM database it will create an XLS spreadsheet with analysis of the
data in the database.

optional arguments:
  -h, --help                show this help message and exit
  --SRUM_INFILE SRUM_INFILE, -i SRUM_INFILE
                          Specify the ESE (.dat) file to analyze. Provide a
                          valid path to the file.
  --XLSX_OUTFILE XLSX_OUTFILE, -o XLSX_OUTFILE
                          Full path to the XLS file that will be created.
  --XLSX_TEMPLATE XLSX_TEMPLATE, -t XLSX_TEMPLATE
                          The Excel Template that specifies what data to extract
                          from the srum database. You can create templates with
                          ese_template.py.
  --REG_HIVE REGHIVE, -r REGHIVE
                          If a registry hive is provided then the names of the
                          network profiles will be resolved.
  --quiet, -q              Supress unneeded output messages.

```

**Ver Video:007/MÓD. 4 - SRUM*

Lo resultados de ejecutar la herramienta SRUM DUMP, donde se identifica el proceso junto con su timestams y los bytes que ha enviado y recibido:

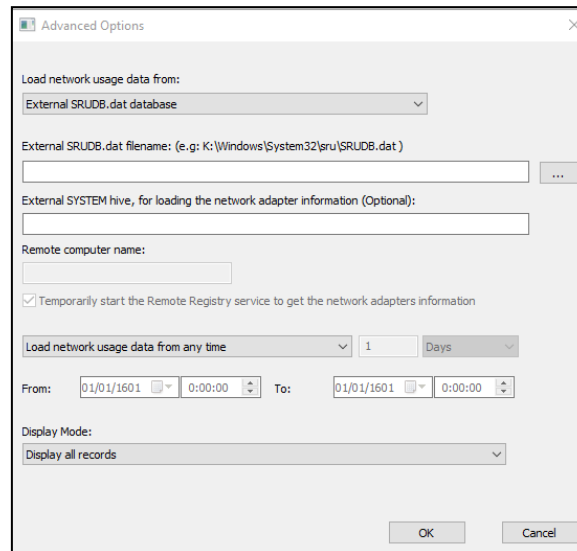
SRUM ENTRY CREATION	Application
2018-10-03 19:07:00	\device\harddiskvolume2\program files\ccleaner\ccleaner64.exe
2018-10-03 20:22:00	\device\harddiskvolume2\program files\ccleaner\ccleaner64.exe
2018-10-03 20:22:00	\device\harddiskvolume2\program files\ccleaner\ccleaner64.exe
2018-10-03 21:25:00	\device\harddiskvolume2\program files\ccleaner\ccleaner64.exe
2018-10-03 21:25:00	\device\harddiskvolume2\program files\ccleaner\ccleaner64.exe
2018-10-08 07:43:00	\device\harddiskvolume2\program files\ccleaner\ccleaner64.exe
2018-10-08 07:43:00	\device\harddiskvolume2\program files\ccleaner\ccleaner64.exe

Bytes Sent	Bytes Received
8385	36636
2529	7500
1287	4637
3709	9251
1287	3432
3364	15885
1341	6047

Otra herramienta que podemos utilizar y de manera gráfica y fácil para analizar el fichero SRUDB.dat es de Nirsoft:

https://www.nirsoft.net/utils/network_usage_view.html

El funcionamiento de esta herramienta es como siempre, es decir, permite analizar la maquina donde se ejecuta o también permite analizar una maquina externa, indicando el fichero SRUDB.dat. Para ello se debe ir a : Options -> Advaced Options y seleccionar el **SRUDB.dat** y el registro **SYSTEM**



Una vez cargado ambos ficheros, ya se puede identificar que proceso envió tantos bytes, mediante que interfaz y cual usuario ejecuto dicho proceso (SID).

Record ID	Timestamp	App Name	App Description	App ID	User Name	User SID	Network Adapter	Bytes Sent
1547	04/11/2020 21:38:00	LicenseManager	Servicio de administrador de licencias de W...	278	NT AUTHORITY\Servicio de red	S-1-5-20	Intel(R) 82574L Gigabit Netwo...	3.337
1548	04/11/2020 21:38:00	wildsv	Ayudante para el inicio de sesión de cuenta...	275	NT AUTHORITY\SERVICIO LO...	S-1-5-19	Intel(R) 82574L Gigabit Netwo...	6.270
1549	04/11/2020 21:38:00	DiagTrack	Experiencias del usuario y telemetría asocia...	274	DESKTOP-0C10CSN\usuario	S-1-5-21-1904304340-2315757...	Intel(R) 82574L Gigabit Netwo...	185.411
1550	04/11/2020 21:38:00	WpnUserService_b11a4	Windows Update	2546	DESKTOP-0C10CSN\usuario	S-1-5-21-1904304340-2315757...	Intel(R) 82574L Gigabit Netwo...	1.876
1551	04/11/2020 21:38:00	wuauclt	Windows Update	279	NT AUTHORITY\SYSTEM	S-1-5-18	Intel(R) 82574L Gigabit Netwo...	23.074
1552	04/11/2020 21:38:00	WinDefend	Servicio de Antivirus de Windows Defender	464	NT AUTHORITY\SYSTEM	S-1-5-18	Intel(R) 82574L Gigabit Netwo...	9.477
1553	04/11/2020 21:38:00	wildsv	Ayudante para el inicio de sesión de cuenta...	275	NT AUTHORITY\SYSTEM	S-1-5-18	Intel(R) 82574L Gigabit Netwo...	36.784
1554	04/11/2020 21:38:00	wildsv	Ayudante para el inicio de sesión de cuenta...	275	NT AUTHORITY\Servicio de red	S-1-5-20	Intel(R) 82574L Gigabit Netwo...	13.470
1555	04/11/2020 21:38:00	WaaSMedicSvc	Windows Update Medic Service	1093	NT AUTHORITY\SYSTEM	S-1-5-18	Intel(R) 82574L Gigabit Netwo...	6.395
1556	04/11/2020 21:38:00	Dnscache	Cliente DNS	84	NT AUTHORITY\Servicio de red	S-1-5-20	Intel(R) 82574L Gigabit Netwo...	14.942
1557	04/11/2020 21:38:00	Spooler	Cola de impresión	280	NT AUTHORITY\SYSTEM	S-1-5-18	Intel(R) 82574L Gigabit Netwo...	1.946.294
1558	04/11/2020 21:38:00	CryptSvc	Servicios de cifrado	281	NT AUTHORITY\SYSTEM	S-1-5-18	Intel(R) 82574L Gigabit Netwo...	552
1559	04/11/2020 21:38:00	CryptSvc	Servicios de cifrado	281	DESKTOP-0C10CSN\usuario	S-1-5-21-1904304340-2315757...	Intel(R) 82574L Gigabit Netwo...	1.831
1560	04/11/2020 21:38:00	BITS	Servicio de transferencia inteligente en seg...	282	NT AUTHORITY\SERVICIO LO...	S-1-5-19	Intel(R) 82574L Gigabit Netwo...	2.045
1561	04/11/2020 21:38:00	Dhcp	Cliente DHCP	288	NT AUTHORITY\SERVICIO LO...	S-1-5-19	Intel(R) 82574L Gigabit Netwo...	1.859
1563	04/11/2020 21:38:00	C:\program files (x86)\...	Microsoft Edge Update	1375	DESKTOP-0C10CSN\usuario	S-1-5-21-1904304340-2315757...	Intel(R) 82574L Gigabit Netwo...	5.943

APPCOMPATCACHE (SHIMCACHE)

Se encarga de chequear la compatibilidad de la aplicación dentro del sistema operativo. Verifica si la aplicación necesita aplicarse ciertas propiedades en el actual sistema operativo o funcionar viejos sistemas operativos.

Appcompatcache monitorizará del ejecutable:



- ◆ Fecha de última modificación: \$STANDARD_INFORMATION
- ◆ Path donde se encuentra
- ◆ Y si fue ejecutado

Si la aplicación sufre una modificación o actualización, será nuevamente actualizada.

Ruta:

- ◆ **SYSTEM\CurrentControlSet\Control\SessionManager\AppcompatCache** -> XP -> 96 entradas
- ◆ **SYSTEM\CurrentControlSet\Control\SessionManager\AppcompatCache\AppCompatCache** -> Server 2003 (512 entradas) y 2008/2012/2016 – Win7/Win8/Win10 (1024 entradas)

Cuando se modifican las propiedades de una aplicación, se crean entradas en el registro. Todo programa (.exe, .bat, .dll) es chequeado con la base de datos para buscar una compatibilidad. Este es el artefacto forense que encontramos.

Solo se actualiza cuando el sistema es apagado y no antes.

- ◆ Eventos más recientes están al principio
- ◆ Nuevos eventos se escriben al ser apagado.

¿Qué podemos evidenciar con el ShimCache y en qué sistema operativo?

Sistema Operativo	Directorio	Ultima fecha de modificación	Tamaño	Ultima ejecución
WinXP	SI	SI	SI	
2003 / XP 64bit	SI	SI	SI	
Win7/8/10/ 2008/2012/2016	SI	SI	SI	

La Herramienta que permite analiza el AppCompatCache de Eric Zimmerman:

AppCompatCache (ShimCache) Parser

```
C:\Binarios\AppCompatCacheParser>AppCompatCacheParser.exe -f "C:\Users\user\Desktop\evidencia\SYSTEM" --csv "C:\Users\user\Desktop\salida"
AppCompatCache Parser version 1.0.0.1

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

Command line: -f C:\Users\user\Desktop\evidencia\SYSTEM --csv C:\Users\user\Desktop\salida

Warning: Administrator privileges not found!

Processing hive 'C:\Users\user\Desktop\evidencia\SYSTEM'

Header length is smaller than the size of the file.
hbin header incorrect at absolute offset 0x9D9000!!! Percent done: 98.48%
Initial processing complete. Building tree...
Found root node! Getting subkeys...
Hive processing complete!
Flushing record lists...
Found 252 cache entries for Windows10 in ControlSet001

Results saved to 'C:\Users\user\Desktop\salida\Windows10_SYSTEM_AppCompatCache.csv'

C:\Binarios\AppCompatCacheParser>
```


**Ver video:008/MÓD. 4 - Shimcache*

Resultado de ejecutar AppCompatCache y analizar el fichero CSV en TimelineExplorer:

Timeline Explorer v0.8.7.0

File Tools Help

Windows10Creators_SYSTEM_AppCompatCache.csv

Find: Enter value to find... 0 of 0 First scrollable column: Select a column to pin

Power filter: Enter filter criteria...

Drag a column header here to group by that column

Line	Tag	Path	Last Modified Tim...	Control...	Cache Enti
1		C:\Program Files\WindowsApps\Microsoft.WindowsStore_11809.1001...	2018-10-08 07:42:55	1	
2		C:\Program Files\WindowsApps\Microsoft.BingWeather_4.26.12153...	2018-10-03 18:18:14	1	
3		C:\Users\pedro\AppData\Local\Microsoft\OneDrive\18.143.0717.00...	2018-10-08 07:39:56	1	
4		00000009 3e812a4b4eb80000 000a00003f3e0000 8664 Microsoft.Offi...	1601-01-01 00:00:00	1	
5		00000009 2e2103e900080000 000a000045550000 8664 Microsoft.Wind...	1601-01-01 00:00:00	1	
6		C:\Users\pedro\AppData\Local\Microsoft\OneDrive\Update\OneDriv...	2018-10-08 07:42:30	1	
7		C:\Users\pedro\AppData\Local\Microsoft\OneDrive\OneDrive.exe	2018-10-08 07:40:58	1	
8		C:\Users\pedro\AppData\Local\Microsoft\OneDrive\18.143.0717.00...	2018-10-08 07:40:35	1	
9		C:\Windows\system32\MusNotificationUx.exe	2018-09-15 07:28:39	1	
10		C:\Windows\system32\MusNotifyIcon.exe	2018-09-15 07:28:39	1	
11		C:\Windows\syswow64\WindowsPowerShell\v1.0\PowerShell_ISE.exe	2018-09-15 07:29:47	1	

AMCACHE.HVE

Artefacto forense que indica ejecución, que es un registro en sí mismo con la siguiente ruta:

C:\Windows\AppCompat\Programas\Amcache.hve (Windows 7/8/8.1/10 y 2012/2016)

- ◆ Keys: Amcache.hve\Root\File\{Volume GUID}\##### -> Para el Formato Antiguo
- ◆ Hay una entrada por cada ejecución, información del directorio, fecha última modificación \$StandardInfo y el volumen desde el que ejecutó (GUID de volumen)
- ◆ La primera vez que se ejecutó: última modificación de la clave de registro
- ◆ El SHA1 del ejecutable también está en el registro

Es el único artefacto forense que evidencia el **HASH SHA1** del binario que ha sido ejecutado, por lo que este artefacto es muy importante a la hora de localizar malware conocido.

Lo analizamos con la Herramienta **AmcacheParser**



```

Command Prompt
AmCacheParser version 1.1.0.0

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

Command line: -f C:\Users\student\Desktop\AmCache\AmCache.hve --csv C:\Users\student\Desktop\AmCache

Header length is smaller than the size of the file.
Found hbin with size 0 at absolute offset 0x137000
Initial processing complete. Building tree...
Found root node! Getting subkeys...
Live processing complete!
Flushing record lists...
Unknown value name when processing FileEntry at path '{11517B7C-E79D-4e20-961B-75A811715ADD}\Root\InventoryApplicationFi
e\64bitmapibroker.[f698d51836c897bd]': Usn
Unknown value name when processing FileEntry at path '{11517B7C-E79D-4e20-961B-75A811715ADD}\Root\InventoryApplicationFi
e\7za.exe|8bb9037766cd3eef': Usn
Unknown value name when processing FileEntry at path '{11517B7C-E79D-4e20-961B-75A811715ADD}\Root\InventoryApplicationFi
e\accicons.exe|54c3db057dd55d6d': Usn

```

**Ver Video: 009/MÓD. 4 - Amcache*

Resultado de la ejecución AmCacheParser:

C	D	E	
2018-10-03 18:12:59	a32a03532a2ac2ca9c9f67ff4e7fb45680985df9	True	c:\windows\system32\conhost.exe
2018-10-03 18:12:59	e6314bc8ab096923cb69a1359c84db4743bf4e1	True	c:\windows\system32\consent.exe
2018-10-03 18:12:59	d0e857d149a8a888276eee92839812ae5b657f1c	True	c:\windows\system32\credentialuibroker.exe
2018-10-03 18:12:59	779b8afc3fa2528b090f400ef3d592e0e2775955	True	c:\windows\system32\csrss.exe
2018-10-03 18:12:59	65597164f3bfc193eac140a8bca7eaa3fce8a92c	True	c:\windows\system32\ctfmon.exe
2018-10-03 20:51:07	a79f6bbe4995cb48771445270997cef0a0a6125b	True	c:\windows\system32\dataexchangehost.exe
2018-10-03 18:12:59	64cd6dc111ba59b11923e2ec26825c75ee6ab7aa	True	c:\windows\system32\devicecensus.exe
2015-10-03 21:04:48	dce2af90e45fb9fc05ecbc9beddee53fb66f3c6d	True	c:\windows\system32\dlhhost.exe
2018-10-03 18:12:59	d3a77e94d08f2eb9a8276f32ca16f65d1ce8b524	False	c:\program files (x86)\dropbox\update\dropboxupdate.exe
2018-10-03 18:12:59	d3a77e94d08f2eb9a8276f32ca16f65d1ce8b524	False	c:\users\ismis\appdata\local\temp\gum343f.tmp\dropboxupdate.exe
2018-10-03 18:12:59	0ac5eabb21c3c873b1ca249a7cb6e099e1431ae	True	c:\windows\system32\drvinst.exe
2018-10-03 18:12:59	a2198b6d266720e3139554c2781e0f4586d29f80	True	c:\windows\system32\dwms.exe
2018-10-03 18:12:59	59ab8548708342c77c51f70e0ec5ced0a88dc4701	True	c:\windows\explorer.exe
2018-10-03 18:12:59	11110a2d3605e8391059aef08b25b94620d5d55e	False	c:\users\ismis\downloads\firefox_installer.exe

RECENTFILECACHE

Este artefacto solo se encuentra en Windows 7 y en la siguiente ruta:

- C:\Windows\AppCompat\Programs\RecentFileCache.bcf

Contiene la ejecución de binarios más reciente en el sistema Windows 7.

Para ver de manera más detallada como se crea este artefacto forense:

<http://journeyintoir.blogspot.com/2013/12/revealing-recentfilecachebcf-file.html>

Para analizar este artefacto utilizaremos la herramienta **RecentFileCacheParse**:



```
RecentFileCacheParser version 0.5.0.0
Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/RecentFileCacheParser

    f      File to process. Required
    q      Only show the filename being processed vs all output. Useful to speed up exporting to json and/or csv

    csv     Directory to save CSV (tab separated) formatted results to. Be sure to include the full path in
double quotes
    json    Directory to save json representation to. Use --pretty for a more human readable layout
    pretty  When exporting to json, use a more human readable layout

Examples: RecentFileCacheParser.exe -f "C:\Temp\RecentFileCache.bcf" --csv "c:\temp"
RecentFileCacheParser.exe -f "C:\Temp\RecentFileCache.bcf" --json "D:\jsonOutput" --jsonpretty

Short options (single letter) are prefixed with a single dash. Long commands are prefixed with two dashes
```

Como siempre, deberemos extraer previamente el artefacto forense mediante Access Data FTK de la ruta anteriormente indicada para que esta herramienta sea capaz de interpretar y analizar. Abrimos un CMD para ejecutar la herramienta e indicarle donde se encuentra el artefacto extraído:

```
C:\Digital Forensics\Applications\RecentFileCacheParser>RecentFileCacheParser.exe -f "C:\Users\student\Desktop\New folder\RecentFileCache.bcf" --csv "C:\Users\student\Desktop\New folder\"
RecentFileCacheParser version 0.5.0.0
Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/RecentFileCacheParser

Command line: -f C:\Users\student\Desktop\New folder\RecentFileCache.bcf --csv C:\Users\student\Desktop\New folder"

Processing 'C:\Users\student\Desktop\New folder\RecentFileCache.bcf'

Source file: C:\Users\student\Desktop\New folder\RecentFileCache.bcf
Source created: 2018-11-12 15:57:17
Source modified: 2018-11-12 12:58:47
Source accessed: 2018-11-12 16:06:22

File names
d:\windows\system32\svchost.exe
d:\windows\servicing\trustedinstaller.exe
d:\windows\system32\lsass.exe
d:\windows\system32\lsmd.exe
d:\windows\system32\oobe\windeploy.exe
d:\windows\system32\spssvc.exe
d:\windows\system32\winsat.exe
```

Finalmente abrimos el fichero CSV generado. Hay que tener cuidado que la extensión es un TSV, es decir un fichero generado por tabulaciones.

Name	Date modified
20181112170624_RecentFileCacheParser_Output.tsv	11/12/2018 5:06 PM
RecentFileCache.bcf	11/12/2018 1:58 PM

Lo abrimos con OpenOffice, cambiándole la extensión a "CSV".

A	B	C	D	
SourceFile	SourceCreated	SourceModified	SourceAccessed	Filename
C:\Users\student\Desktop\New folder\RecentFileCache.bcf	2018-11-12 15:57:17	2018-11-12 12:58:47	2018-11-12 16:06:22	d:\windows\system32\svchost.exe
C:\Users\student\Desktop\New folder\RecentFileCache.bcf	2018-11-12 15:57:17	2018-11-12 12:58:47	2018-11-12 16:06:22	d:\windows\servicing\trustedinstaller.exe
C:\Users\student\Desktop\New folder\RecentFileCache.bcf	2018-11-12 15:57:17	2018-11-12 12:58:47	2018-11-12 16:06:22	d:\windows\system32\lsass.exe
C:\Users\student\Desktop\New folder\RecentFileCache.bcf	2018-11-12 15:57:17	2018-11-12 12:58:47	2018-11-12 16:06:22	d:\windows\system32\lsim.exe
C:\Users\student\Desktop\New folder\RecentFileCache.bcf	2018-11-12 15:57:17	2018-11-12 12:58:47	2018-11-12 16:06:22	d:\windows\system32\oobe\windeploy.exe
C:\Users\student\Desktop\New folder\RecentFileCache.bcf	2018-11-12 15:57:17	2018-11-12 12:58:47	2018-11-12 16:06:22	d:\windows\system32\spssvc.exe
C:\Users\student\Desktop\New folder\RecentFileCache.bcf	2018-11-12 15:57:17	2018-11-12 12:58:47	2018-11-12 16:06:22	d:\windows\system32\winsat.exe
C:\Users\student\Desktop\New folder\RecentFileCache.bcf	2018-11-12 15:57:17	2018-11-12 12:58:47	2018-11-12 16:06:22	d:\windows\system32\rundll32.exe
C:\Users\student\Desktop\New folder\RecentFileCache.bcf	2018-11-12 15:57:17	2018-11-12 12:58:47	2018-11-12 16:06:22	d:\windows\system32\vmcbuilder.exe
C:\Users\student\Desktop\New folder\RecentFileCache.bcf	2018-11-12 15:57:17	2018-11-12 12:58:47	2018-11-12 16:06:22	d:\windows\system32\logonui.exe
C:\Users\student\Desktop\New folder\RecentFileCache.bcf	2018-11-12 15:57:17	2018-11-12 12:58:47	2018-11-12 16:06:22	d:\windows\system32\dlhhost.exe
C:\Users\student\Desktop\New folder\RecentFileCache.bcf	2018-11-12 15:57:17	2018-11-12 12:58:47	2018-11-12 16:06:22	d:\windows\system32\taskhost.exe
C:\Users\student\Desktop\New folder\RecentFileCache.bcf	2018-11-12 15:57:17	2018-11-12 12:58:47	2018-11-12 16:06:22	d:\windows\system32\userinit.exe
C:\Users\student\Desktop\New folder\RecentFileCache.bcf	2018-11-12 15:57:17	2018-11-12 12:58:47	2018-11-12 16:06:22	d:\windows\system32\dwrm.exe
C:\Users\student\Desktop\New folder\RecentFileCache.bcf	2018-11-12 15:57:17	2018-11-12 12:58:47	2018-11-12 16:06:22	d:\windows\explorer.exe
C:\Users\student\Desktop\New folder\RecentFileCache.bcf	2018-11-12 15:57:17	2018-11-12 12:58:47	2018-11-12 16:06:22	d:\windows\system32\runonce.exe
C:\Users\student\Desktop\New folder\RecentFileCache.bcf	2018-11-12 15:57:17	2018-11-12 12:58:47	2018-11-12 16:06:22	d:\windows\system32\drivinst.exe
C:\Users\student\Desktop\New folder\RecentFileCache.bcf	2018-11-12 15:57:17	2018-11-12 12:58:47	2018-11-12 16:06:22	d:\windows\system32\cmd.exe
C:\Users\student\Desktop\New folder\RecentFileCache.bcf	2018-11-12 15:57:17	2018-11-12 12:58:47	2018-11-12 16:06:22	d:\windows\system32\cscrip.exe
C:\Users\student\Desktop\New folder\RecentFileCache.bcf	2018-11-12 15:57:17	2018-11-12 12:58:47	2018-11-12 16:06:22	d:\windows\syswow64\ie4uinit.exe
C:\Users\student\Desktop\New folder\RecentFileCache.bcf	2018-11-12 15:57:17	2018-11-12 12:58:47	2018-11-12 16:06:22	d:\windows\system32\wbem\wmiiprse.exe
C:\Users\student\Desktop\New folder\RecentFileCache.bcf	2018-11-12 15:57:17	2018-11-12 12:58:47	2018-11-12 16:06:22	d:\windows\syswow64\rundll32.exe
C:\Users\student\Desktop\New folder\RecentFileCache.bcf	2018-11-12 15:57:17	2018-11-12 12:58:47	2018-11-12 16:06:22	d:\windows\system32\regsvr32.exe
C:\Users\student\Desktop\New folder\RecentFileCache.bcf	2018-11-12 15:57:17	2018-11-12 12:58:47	2018-11-12 16:06:22	d:\program files\windows mail\winmail.exe
C:\Users\student\Desktop\New folder\RecentFileCache.bcf	2018-11-12 15:57:17	2018-11-12 12:58:47	2018-11-12 16:06:22	d:\program files\windows mail\winmail.exe
C:\Users\student\Desktop\New folder\RecentFileCache.bcf	2018-11-12 15:57:17	2018-11-12 12:58:47	2018-11-12 16:06:22	d:\windows\system32\unregmp2.exe

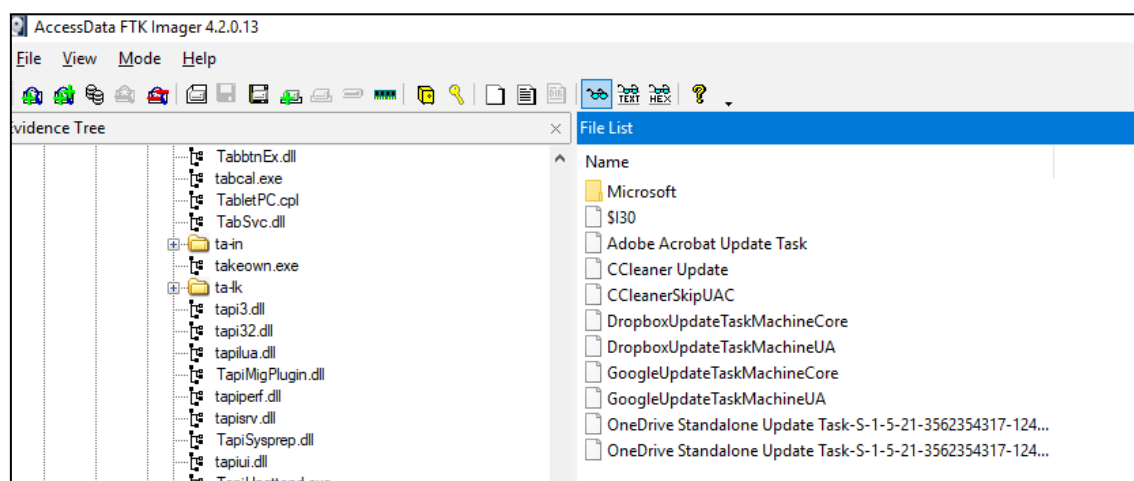
Finalmente disponemos una tabla con la ejecución de los binarios.

TAREAS PROGRAMADAS

Las tareas programadas son utilizadas por el sistema operativo para realizar tareas de actualización o mantenimiento.

Un malware o backdoor puede utilizar las tareas programadas como mecanismo de persistencia. Pero también se puede utilizar este artefacto para evidenciar una ejecución.

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



Podemos extraerlas con Arsenal Image Mounter las tareas para analizarlas. Aunque no tengan extensión, una vez extraídas se puede abrir con el Notepad y verlas como un fichero XML:

```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.6" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <Author>Piriform Ltd</Author>
    <URI>\CCleanerSkipUAC</URI>
  </RegistrationInfo>
  <Triggers />
  <Principals>
    <Principal id="Author">
      <RunLevel>HighestAvailable</RunLevel>
      <UserId>DESKTOP-9D0L8DV\ismis</UserId>
      <LogonType>InteractiveToken</LogonType>
    </Principal>
  </Principals>
  <Settings>
    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>
    <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>
    <AllowHardTerminate>true</AllowHardTerminate>
    <StartWhenAvailable>false</StartWhenAvailable>
    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
    <IdleSettings>
      <StopOnIdleEnd>true</StopOnIdleEnd>
      <RestartOnIdle>false</RestartOnIdle>
    </IdleSettings>
    <AllowStartOnDemand>true</AllowStartOnDemand>
    <Enabled>true</Enabled>
    <Hidden>false</Hidden>
    <RunOnlyIfIdle>false</RunOnlyIfIdle>
    <WakeToRun>false</WakeToRun>
    <ExecutionTimeLimit>P3D</ExecutionTimeLimit>
    <Priority>4</Priority>
  </Settings>
  <Actions Context="Author">
    <Exec>
      <Command>"C:\Program Files\CCleaner\CCleaner.exe"</Command>
      <Arguments>$(Arg0) </Arguments>
    </Exec>
  </Actions>
</Task>
```

La fecha de cuando se añadió, la podemos sacar de las propiedades de los sistemas de archivos, gracias a FTK Imager:

Name	CCleaner Update
File Class	Regular File
File Size	3,936
Physical Size	4,096
Start Cluster	4,283,216
Date Accessed	10/3/2018 7:05:20 PM
Date Created	10/3/2018 7:05:20 PM
Date Modified	10/3/2018 7:05:20 PM
Encrypted	False
Compressed	False
Actual File	True
Start Sector	35,392,128

SERVICIOS

- Ruta: **SYSTEM\ControlSet001\Services**

Lo analizamos con Registry Explorer

Name	Description	Display Name	Start Mode	Service Type	Name Key Last Write	Parameters Key Last ...	Group	Image Path
dbupdate	Keeps your Dropbox software up to date. If this service is disabled or stopped, your Dropbox software will not be kept up to date, meaning security vulnerabilities that may arise cannot be fixed and features may not work. This service uninstalls itself when there is no Dropbox software using it.	Dropbox Update Service (dbupdate)	Manual	Win32OwnProcess	2018-10-03 17:49:12			"C:\Program Files (x86)\Dropbox\Update\DropboxUpdate.exe" /medsvc

Campos por destacar:

- ◆ Display Name: nombre del servicio
- ◆ Start mode: el tipo de arranque
- ◆ Image Path: ejecutable con los argumentos que recibe
- ◆ Name Key Last Write: última vez que se actualizo la clave del registro
- ◆ Parameters Key Last Write: última vez que se cambiaron los parámetros

BAM

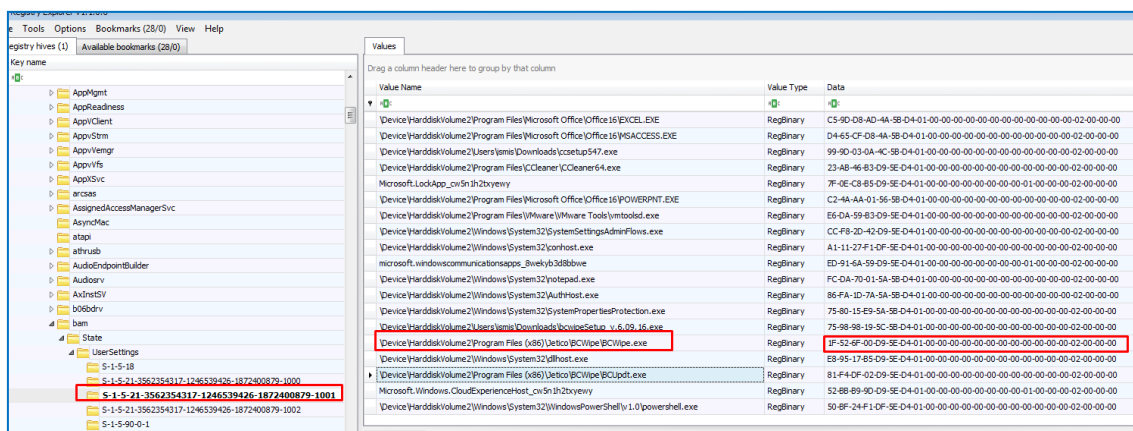
El BAM es un servicio de Windows que se encarga de controlar la actividad de las aplicaciones cuando están en background.

Para las compilaciones más viejas de Windows 10 se puede encontrar en SYSTEM en la siguiente ruta:

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

Para las compilaciones más nuevas de Windows 10 se puede encontrar en SYSTEM en la siguiente ruta:

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

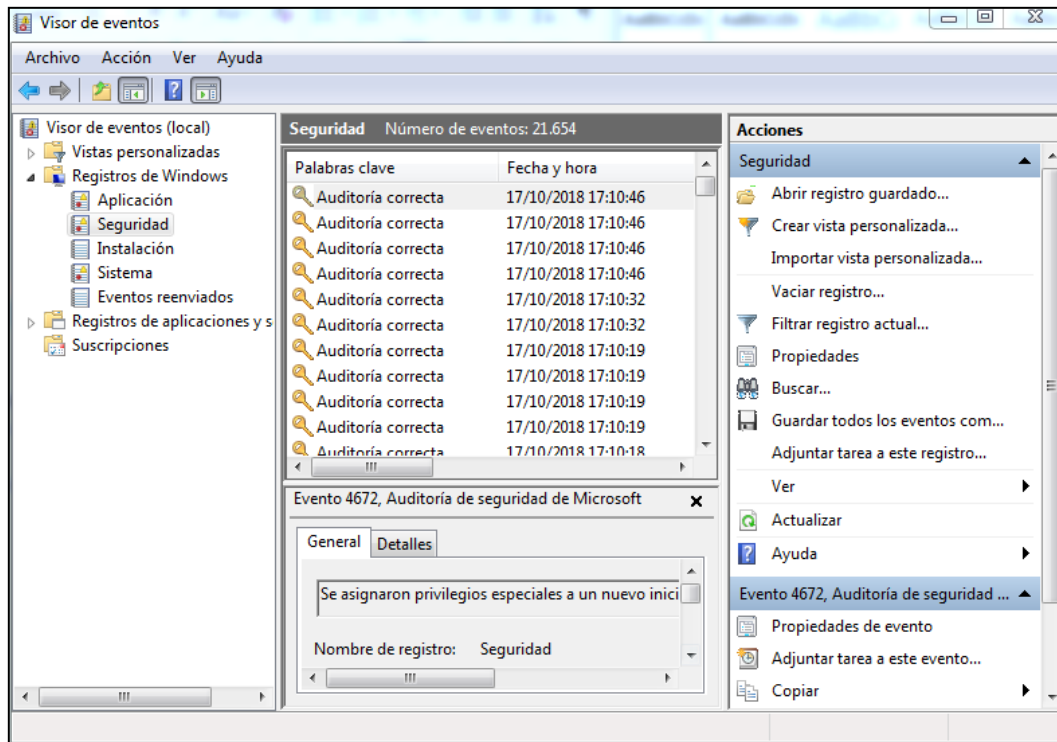




EVENTOS DE WINDOWS

El registro de eventos de Windows proporciona una gran cantidad de información la cual puede ayudar a un investigador a juntar las piezas relevantes sobre las acciones ocurridas en el sistema.

Los eventos son recolectados y almacenados por el Servicio de Registro de Eventos. De manera similar a otros artefactos forenses, es provechoso realizar el ejercicio mental de determinar cuáles preguntas pueden responder los datos del registro de eventos.



¿Qué podemos obtener de los eventos de Windows?

1. ¿Qué ocurrió? (Identificador del Evento, Categorías del Evento, Descripción)

Los registros de eventos pueden ser complicados para un usuario normal, pero están diseñados para proporcionar información muy específica sobre las actividades ocurridas en el sistema.

2. ¿Cuál fue el día y la hora? (Marcas de Tiempo)

Las marcas de tiempo son una parte clave de los registros de eventos, pues proporcionan un contexto temporal para los eventos. Con sistemas registrando miles de eventos, las marcas de tiempo pueden también ayudar al investigador a acercar su enfoque.

3. ¿Quiénes son los usuarios involucrados? (Cuenta de Usuario, Descripción)

Cualquier cosa hecha dentro de Windows es realizada dentro del contexto de una cuenta. Se puede identificar referencias hacia usuarios específicos, como también a información sobre las actividades del sistema operativo Windows realizadas mediante una cuenta especial como System o NetworkService.

4. ¿Cuáles son los sistemas involucrados? (Nombre del Host, Dirección IP)

En un entorno de red, es muy común encontrar referencias hacia otros sistemas aparte del host, como recursos siendo accedidos remotamente. Originalmente sólo el nombre Netbios era registrado, haciendo el rastreo y la atribución mucho más difícil. En sistemas más recientes, la dirección IP es registrada dentro del registro de eventos (Cuando aplica).

5. ¿Cuáles recursos se accedieron? (Archivos, Carpetas, Impresoras, Servicios)

El Servicio de Registro de Eventos puede ser configurado para almacenar información muy granular relacionada a la utilización de varios objetos del sistema. Con casi todos los recursos considerados como un objeto, esto proporciona una muy poderosa auditoría. Como un ejemplo; puede ayudar a identificar intentos de acceso no autorizado hacia los archivos del sistema.

Los eventos de Windows centralizan el registro logs del sistema e información sobre:

- ◆ Software
- ◆ Hardware
- ◆ Funciones del sistema operativo
- ◆ Seguridad

A nivel del sistema de archivos, los podemos encontrar en las siguientes rutas.

Antes de Windows Vista	Desde Windows Vista
C:\Windows\System32\config	C:\Windows\System32\winevt\Logs

Como podemos observar tenemos dos tipos de eventos:

Event log en formato Binario (antes de Windows Vista)

- ◆ Sistema
- ◆ Aplicación
- ◆ Seguridad
- ◆ Extensión en (.evt)



Event log en formato XML (de Windows Vista en adelante)

- ◆ Sistema
- ◆ Aplicación
- ◆ Seguridad
- ◆ Extension (.evtx)
- ◆ 200 tipos de ficheros más que el formato antiguo
- ◆ Ahora incluyen direcciones IP

Las localizaciones de los ficheros de eventos las podemos localizar en el registro SYSTEM en la siguiente ruta:

HKLM\SYSTEM\CurrentControlSet\Services\EventLog\{Application|System|Security}

Seguridad	Registra los accesos y da información sobre la configuración de seguridad. Eventos basados en auditoria y políticas.
Sistema	Contiene eventos relacionados con los servicios, componentes del sistema, drivers, recursos. Ej: paro de Servicio.
Aplicación	Eventos de aplicación no relacionados con el sistema. Ej: Servidor SQL falla al acceder a la base de datos
Custom	Logs de aplicación customizados

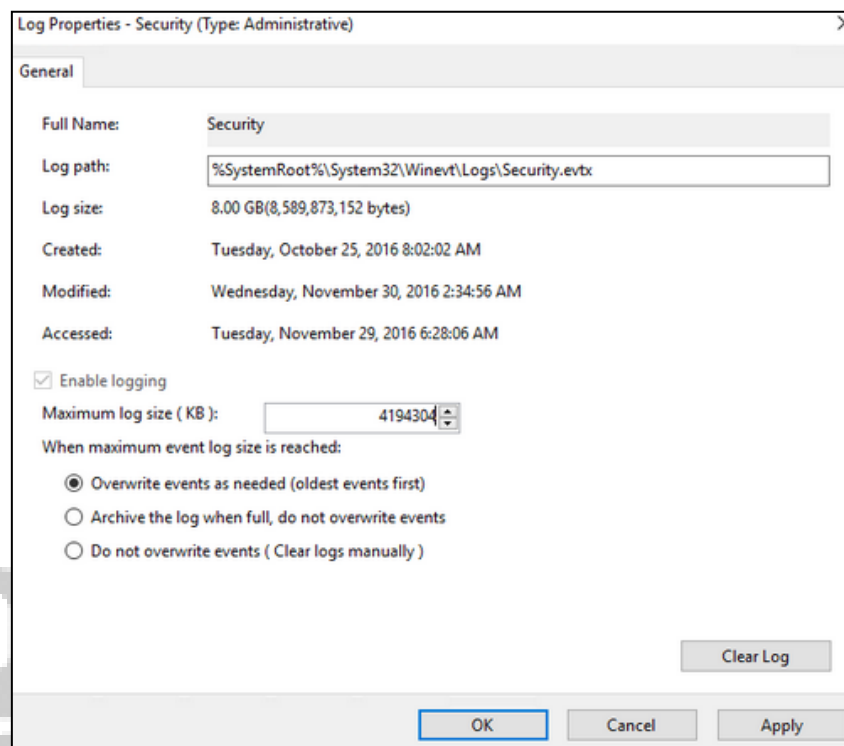
Existen también otros tipos de eventos que no son del sistema operativo Windows, como aplicaciones de terceros, Exchange, Sysmon, SQL Server.

EVENTOS DE SEGURIDAD

Los eventos de seguridad son solo actualizados por el proceso LSASS (Local Security Authority Subsystem Service). Se encuentran en **C:\Windows\System32\winevt\Security.evtx**

Solo con permisos de administrador se pueden ver, exportar o eliminar.

Tienen un tamaño máximo, pero es configurable como vemos a continuación:



Normalmente, el escenario que veremos es que, una vez alcanzado el tamaño asignado, se sobrescribirán los eventos más viejos, es decir un fichero circular.

¿Qué podemos identificar en los eventos de seguridad?

- ◆ Login logoff
- ◆ Conducta del usuario y acciones
- ◆ Acceso a Archivos, Directorios y recursos compartidos
- ◆ Modificaciones de la configuración de seguridad

Los eventos están identificados por ID, y en función de ese identificador podremos identificar que ha ocurrido. En la siguiente web podemos encontrar una descripción exhaustiva de todos los identificadores: <https://www.ultimatewindowssecurity.com>

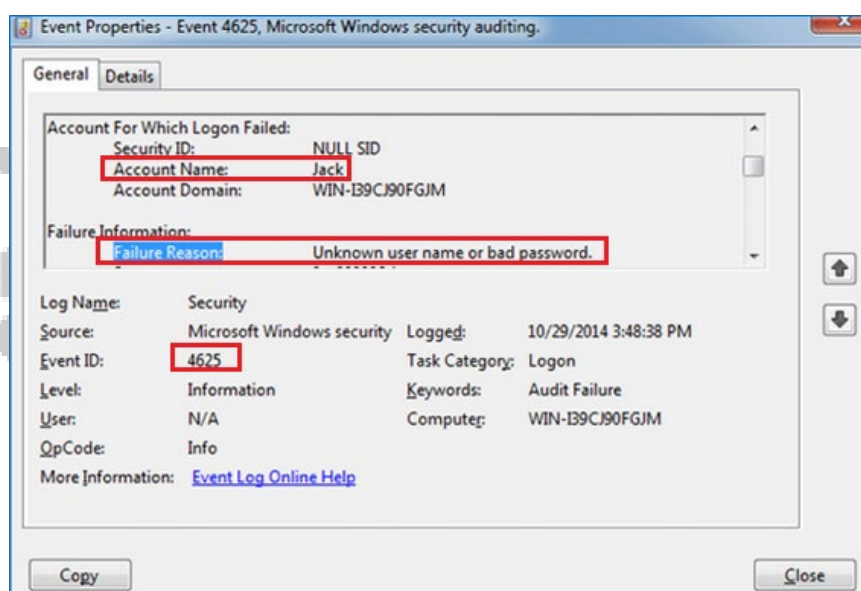
Para el caso de los eventos de Windows Vista y anteriores, se puede encontrar una lista aquí: <https://www.andreafortuna.org/2019/06/12/windows-security-event-logs-my-own-cheatsheet/>

EVENTOS DE SEGURIDAD RELACIONADOS CON LA AUTENTICACIÓN DEL USUARIO

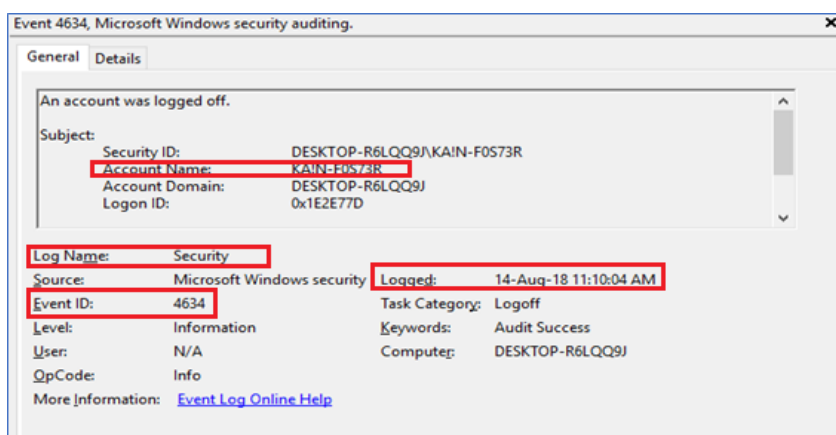
Eventos de relacionados con la autenticación del usuario del sistema Windows:

EventID	Descripción
4624	Evento de autenticación satisfactorio
4625	Evento de fallido de autenticación
4634/4647	Logoff
4672	Logon con permisos de administrador
4776	El controlador de dominio ha intentado validar las credenciales para una cuenta

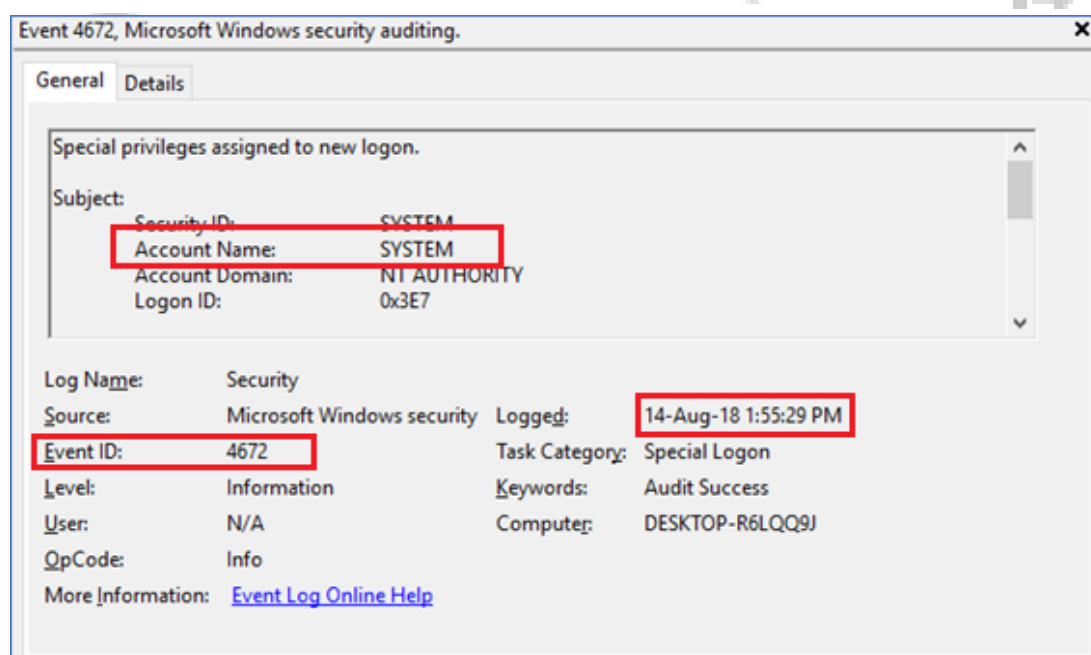
Ejemplo de evento 4625



Ejemplo de evento 4634 Log OFF



Ejemplo de evento 4672 logon especial



Este tipo de evento permite saber cuándo una cuenta con permisos de administrador ha realizado login satisfactorio. Es muy útil para identificar tareas o servicios que utilizan este tipo de credenciales.

Dentro del Evento 4624/4625 encontramos los siguientes subtipos:

- ◆ **TIPO 2** -> Interactive: este tipo de autenticación involucra la utilización del teclado y pantalla del sistema, o la utilización de terceras herramientas remotas como VNC o PSExec -U-
- ◆ **TIPO 3** -> Network: conexión a una carpeta compartida del propio equipo.
- ◆ **TIPO 4** -> Batch: también válido para las tareas programadas, donde los procesos son ejecutados en nombre de otro.
- ◆ **TIPO 5** -> Service: servicios arrancados por el Service Control Manager
- ◆ **TIPO 7** -> Desbloqueo de pantalla con password
- ◆ **TIPO 8** -> Network Cleartext: el usuario se ha autenticado en la maquina desde la red pero sus credenciales no han sido hasheadas. Este tipo de evento suele provenir de la autenticación realizada mediante Internet Information Services (IIS), servidor Web de Microsoft.
- ◆ **TIPO 9** -> NewCredentials: es generado cuando se ejecuta un comando con RunAs desde la CMD o se conecta con una unidad de red, con credenciales distintas a las de la propia sesion.
- ◆ **TIPO 10** -> Remote Interactive: este tipo de autenticación se produce cuando una autenticación se realiza mediante Terminales Services o Remote Desktop Protocol.
- ◆ **TIPO 11** -> CachedInteractive: se autentica con las credenciales últimas cacheadas ya que no se ha sido posible contactar con el controlador de dominio.

Ejemplo de evento 4624 tipo 2:

Evento 4624, Auditoría de seguridad de Microsoft Windows.

General Detalles

Se inició sesión correctamente en una cuenta.

Sujeto:

Id. de seguridad:	SYSTEM
Nombre de cuenta:	LAPTOPS
Dominio de cuenta:	WORKGROUP
Id. de inicio de sesión:	0x3e7

Tipo de inicio de sesión: 2

Nuevo inicio de sesión:

Id. de seguridad:	laptop\usuario
Nombre de cuenta:	usuario
Dominio de cuenta:	laptop
Id. de inicio de sesión:	0x51361
GUID de inicio de sesión:	{00000000-0000-0000-0000-000000000000}

Nombre de registro: Seguridad

Origen: Auditoría de seguridad de Microso Registrado: 11/11/2018 11:51:56

Id. del evento: 4624 Categoría de tarea: Inicio de sesión

Nivel: Información Palabras clave: Auditoría correcta

Usuario: No disponible Equipo: laptop

Código de operación: Información

Más información: [Ayuda Registro de eventos](#)

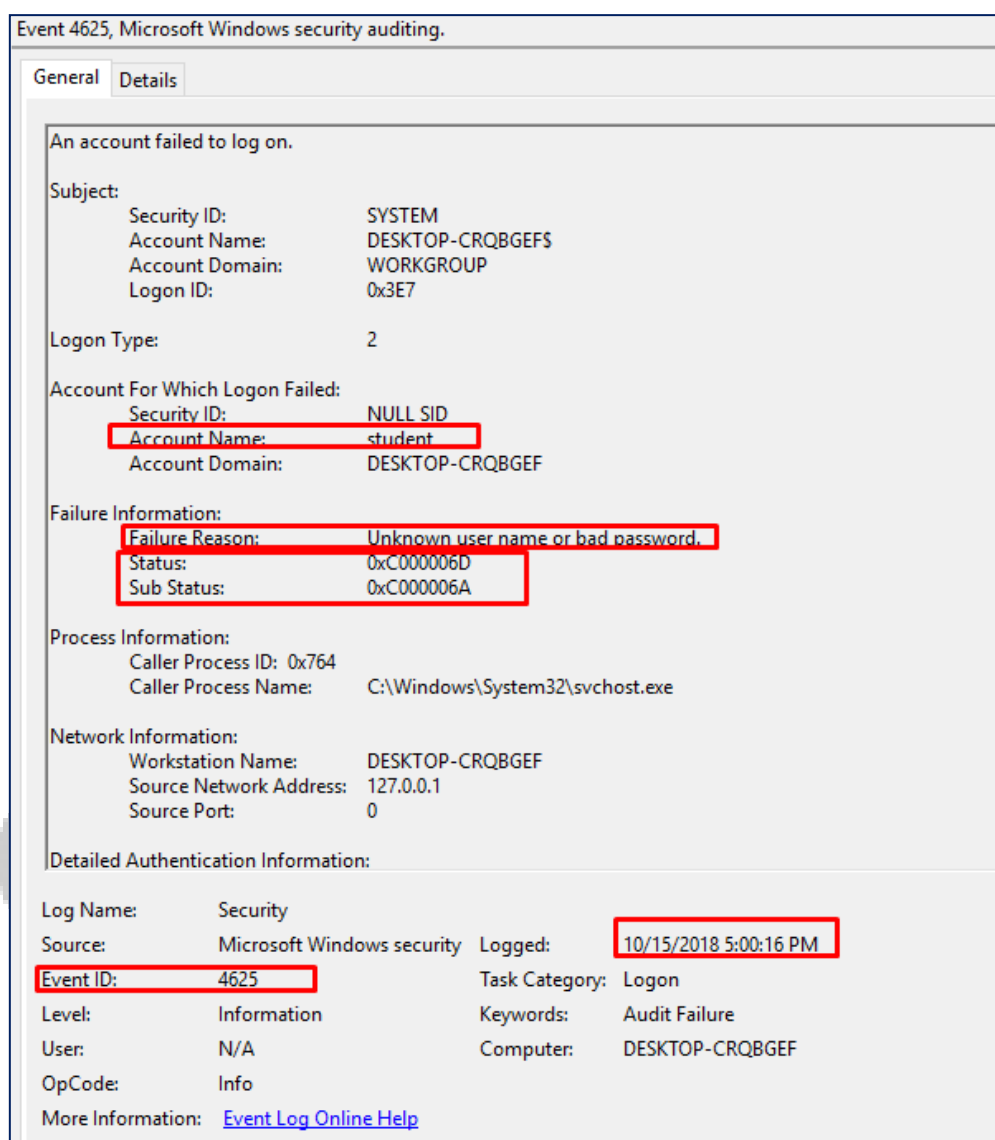


Dentro del evento 4625 se puede indicar el tipo de error al autenticarse mediante los estados y sub-estados:

Status and Sub Status Codes	Description (not checked against "Failure Reason:")
0xC0000064	user name does not exist
0xC000006A	user name is correct but the password is wrong
0xC0000234	user is currently locked out
0xC0000072	account is currently disabled
0xC000006F	user tried to logon outside his day of week or time of day restrictions
0xC0000070	workstation restriction, or Authentication Policy Silo violation (look for event ID 4820 on domain controller)
0xC0000193	account expiration
0xC0000071	expired password
0xC0000133	clocks between DC and other computer too far out of sync
0xC0000224	user is required to change password at next logon
0xC0000225	evidently a bug in Windows and not a risk
0xc000015b	The user has not been granted the requested logon type (aka logon right) at this machine

QUANTIKA¹⁴

Ejemplo de evento 4625 con subestados:

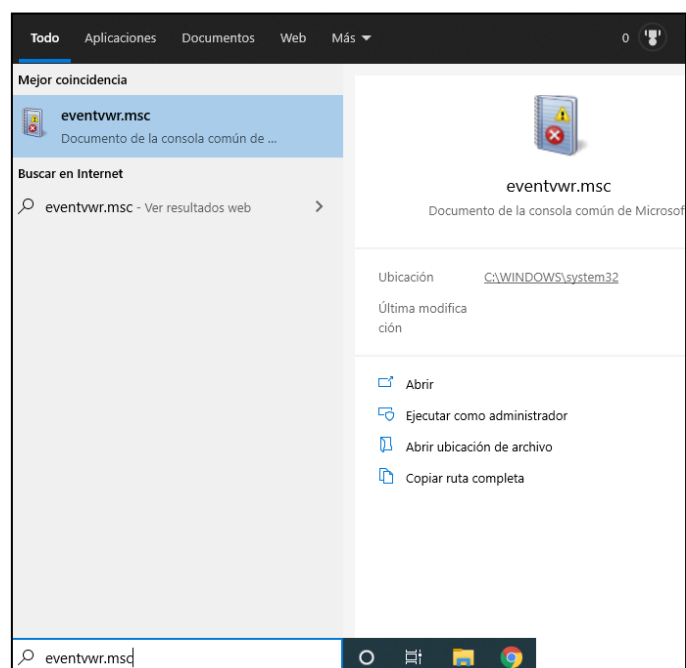


Microsoft-Windows-User profile Service%4 Operational.evtx

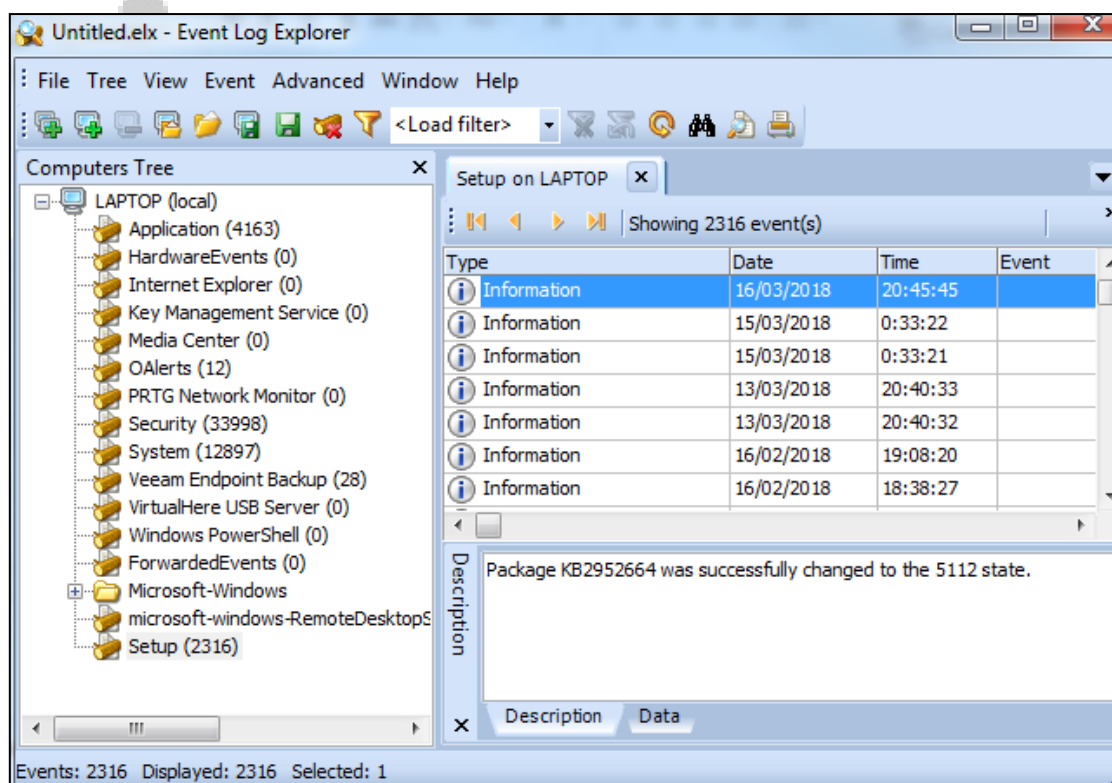
Este tipo de registro de eventos de Windows, se encuentra en el mismo directorio, que el Security.evtx. Cada vez que se inicia sesión, independientemente si es en local o en remoto, se carga el perfil de usuario de este, deja acción de este en Microsoft-Windows-User Profile Service%4Operational.evtx. Es una gran fuente de información, ya que en la mayoría de los casos un atacante suele borrar/vaciar otros eventos de Windows.

VISIÓN DE EVENTOS DE WINDOWS

Los eventos del sistema los podemos visualizar desde la propia gestión de eventos o Event Viewer de Windows (**eventvwr.msc**):

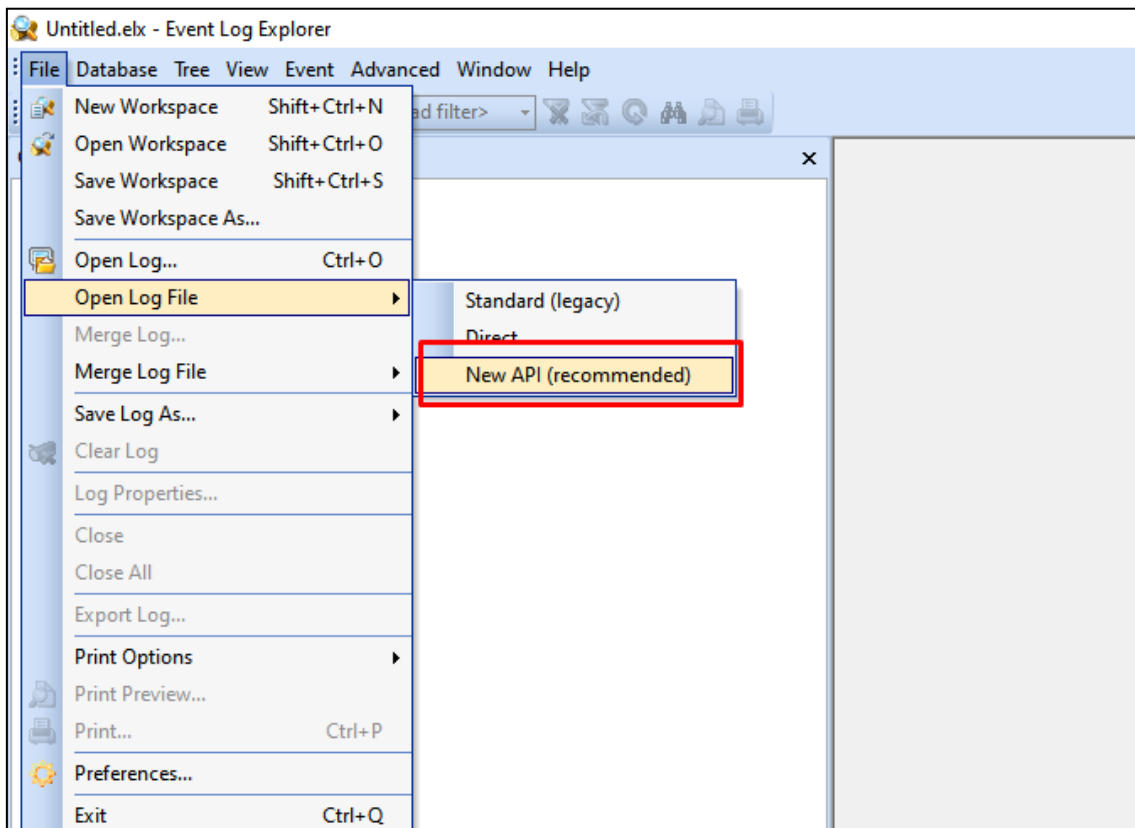


O también podemos utilizar una herramienta que nos permita trabajar tanto de manera live como de manera post-mortem con **Event-Log Explorer**



**Ver Video: 011/MÓD. 4-Eventos del Sistema*

Si en algún momento se identifica algún tipo de error con la apertura de eventos, Event-Log Explorer dispone de una opción para la apertura de eventos: **New API**



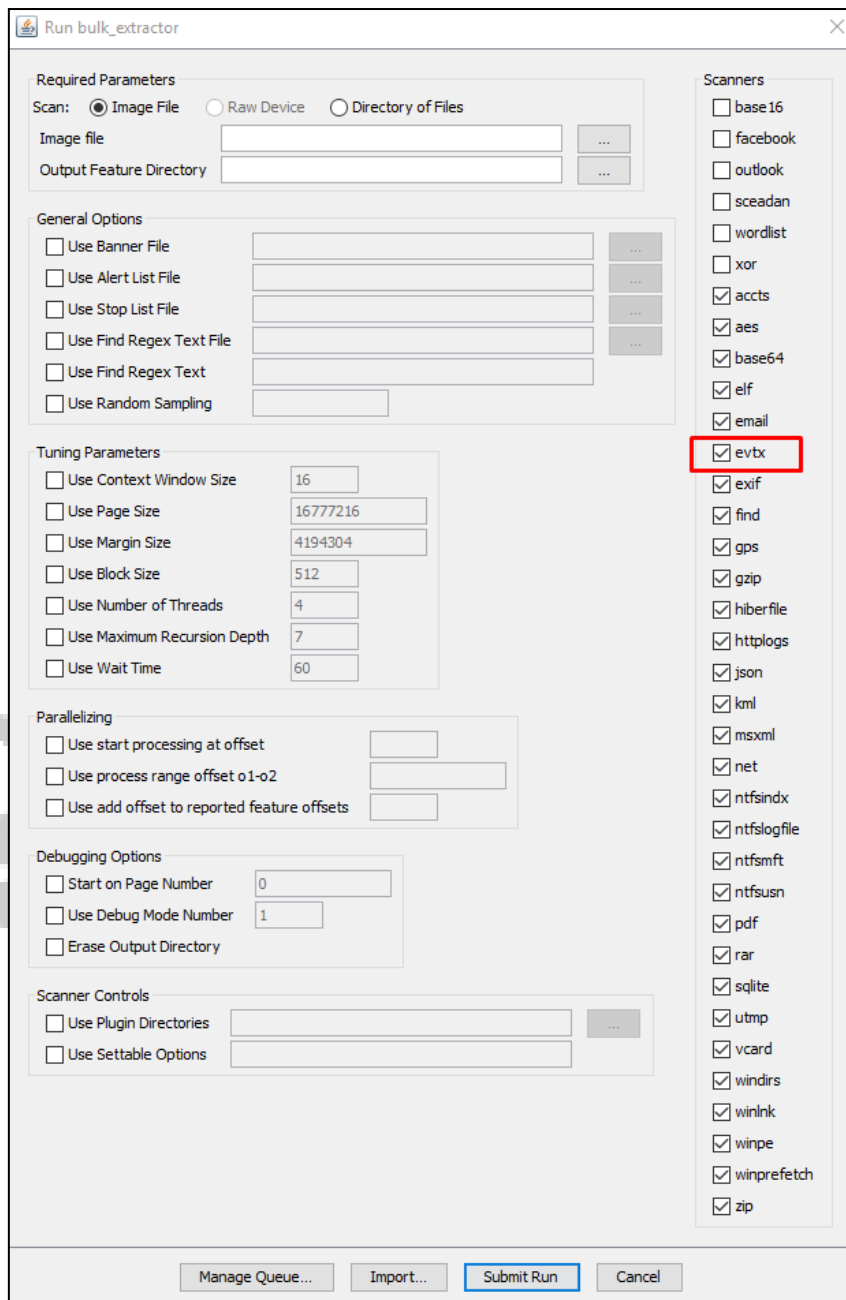
RECUPERACIÓN DE EVENTOS BORRADOS EN WINDOWS

Como hemos visto anteriormente, dependiendo de la configuración que se establezcan en el almacenamiento de los eventos de Windows, es probable que necesitemos realizar una recuperación de los mismos.

Podríamos utilizar técnicas de carving para poder recuperar este tipo de ficheros, pero siempre es muy importante desde que se produce el incidente que la maquina sea apagada/tirada del cable para que la probabilidad de recuperación de este tipo de ficheros aumente tal y como se demuestra en el siguiente enlace.

<https://rawsec.lu/blog/posts/2017/Jun/23/carving-evtx/>

La herramienta que nos va a permitir realizar carving de este tipo de ficheros es **Bulk_Extractor**. Tal y como vimos su funcionamiento en la parte de carving, bastaría con proporcionarle una imagen física o lógica y marcar el escáner como se muestra en la imagen de a continuación:



Otro punto muy importante para tener en cuenta es que cuando se recupera un fichero de eventos, cualquiera que sea, es probable que el fichero este corrupto y no pueda ser abierto.

El visor de eventos de Windows (**eventvwr.msc**) permite abrir este tipo de ficheros para su posterior guardado, de manera que permita ser abierto por una tercera herramienta.

En el caso de que no se puedan abrir los ficheros .evtx recuperados, deberíamos utilizar otra herramienta [Evtx Explorer/EvtxECmd de Eric Zimmerman](#)

```

C:\Windows\System32\cmd.exe

EvtxECmd version 0.6.0.2

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

    d      Directory to process that contains evtx files. This or -f is required
    f      File to process. This or -d is required

    csv     Directory to save CSV formatted results to.
    csvf    File name to save CSV formatted results to. When present, overrides default name
    json    Directory to save JSON formatted results to.
    jsonf   File name to save JSON formatted results to. When present, overrides default name
    xml     Directory to save XML formatted results to.
    xmlf    File name to save XML formatted results to. When present, overrides default name

    dt      The custom date/time format to use when displaying time stamps. Default is: yyyy-MM-dd HH:mm:ss.ffffff
    inc     List of event IDs to process. All others are ignored. Overrides --exc Format is 4624,4625,5410
    exc     List of event IDs to IGNORE. All others are included. Format is 4624,4625,5410
    sd      Start date for including events (UTC). Anything OLDER than this is dropped. Format should match --dt
    ed      End date for including events (UTC). Anything NEWER than this is dropped. Format should match --dt
    fj      When true, export all available data when using --json. Default is FALSE.
    pj      When true, include event 'payload' as json. Default is TRUE.
    tdt     The number of seconds to use for time discrepancy detection. Default is 1 second
    met     When true, show metrics about processed event log. Default is TRUE.

    maps    The path where event maps are located. Defaults to 'Maps' folder where program was executed

    vss     Process all Volume Shadow Copies that exist on drive specified by -f or -d . Default is FALSE
    dedupe  Deduplicate -f or -d & VSCs based on SHA-1. First file found wins. Default is TRUE

    sync    If true, the latest maps from https://github.com/EricZimmerman/evtx/tree/master/evtx/Maps are downloaded and
    updated. Default is FALSE

    debug   Show debug information during processing
    trace   Show trace information during processing

Examples: EvtxECmd.exe -f "C:\Temp\Application.evtx" --csv "c:\temp\out" --csvf MyOutputFile.csv
          EvtxECmd.exe -f "C:\Temp\Application.evtx" --csv "c:\temp\out"
          EvtxECmd.exe -f "C:\Temp\Application.evtx" --json "c:\temp\jsonout"

```

Una prueba de concepto donde se explica el uso de esta herramienta para la recuperación de EVTX borrados, la podemos encontrar aquí: <https://www.kazamiya.net/en/ParseCarvedEVTX>

ANÁLISIS DE CASUÍSTICAS MÁS COMUNES EN CUANTO A SEGURIDAD EN EVENTOS.

A continuación, veremos las situaciones más comunes que podremos identificar mediante eventos del sistema.

BRUTEFORCE ATTACK

Un ataque de fuerza bruta se podrá realizar mediante el intento de autenticación del usuario hasta que consiga acceso al sistema. Veremos muchos eventos 4625 y a continuación un 4624.

The screenshot shows the Windows Security Event Viewer with a list of events filtered to show 679 of 4233 events. The list includes several 'Audit Failure' events (4625) and 'Audit Success' events (4624). The detailed view of event 4625 shows the following information:

- Subject:** Security ID: S-1-0-0, Account Name: -, Account Domain: -, Logon ID: 0x0000000000000000
- Logon Type:** 3
- Account For Which Logon Failed:** Security ID: S-1-0-0, Account Name: anonymous_rdp, Account Domain: laptop
- Failure Information:** Failure Reason: Unknown user name or bad password., Status: 0xC000006D, Sub Status: 0xC0000064
- Process Information:** Caller Process ID: 0x0000000000000000, Caller Process Name: -
- Network Information:** Workstation Name: LAPTOP, Source Network Address: 192.168.192.1, Source Port: 0
- Detailed Authentication Information:** Logon Process: NtLmSsp, Authentication Packages: NTLM, Transited Services: -, Package Name (NTLM only): -, Key Length: 0

The detailed view also includes a description of the event: 'This event is generated when a logon request fails. It is generated on the computer where access was attempted. The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.'

En el
caso
de un

ataque de fuerza bruta donde haya un controlador de dominio involucrado a parte del se identificarán muchos 4625 y 4676 y finalmente un 4624.

REMOTE DESKTOP PROTOCOL

El Remote Desktop Protocol, es el protocolo de Windows para poder conectarse a otra máquina, mediante credenciales, es decir, un escritorio remoto.

En el Security Event Log:

- ◆ Sesión conectada: Event ID 4778 (incluye dirección IP y Hostname)
- ◆ Sesión desconectada: Event ID 4779 (incluye dirección IP y Hostname)
- ◆ Autenticación Satisfactoria Event ID 4624 Tipo (10 y 7 para reconexión)

Logs auxiliares:

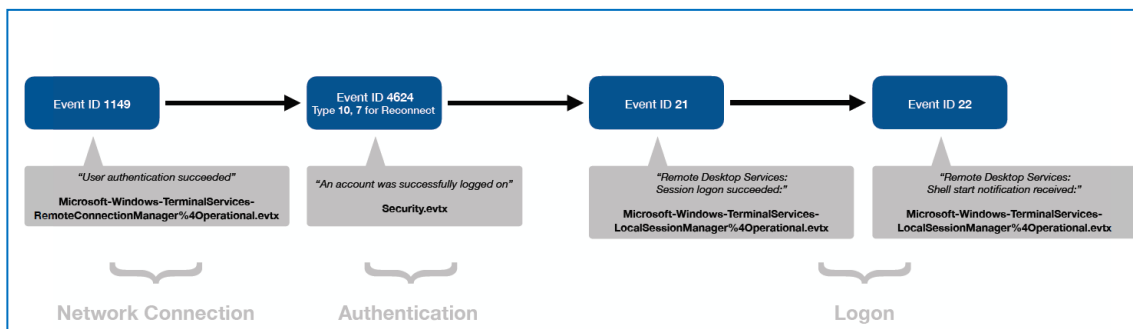
- ◆ Remote Desktop Services – RDPCoreTS (Event ID 131 - Operational)
- ◆ TerminalServices-RemoteConnectionManager%4Operational) (Event ID 1149)
- ◆ Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx (Event ID 21, 22 y 24)

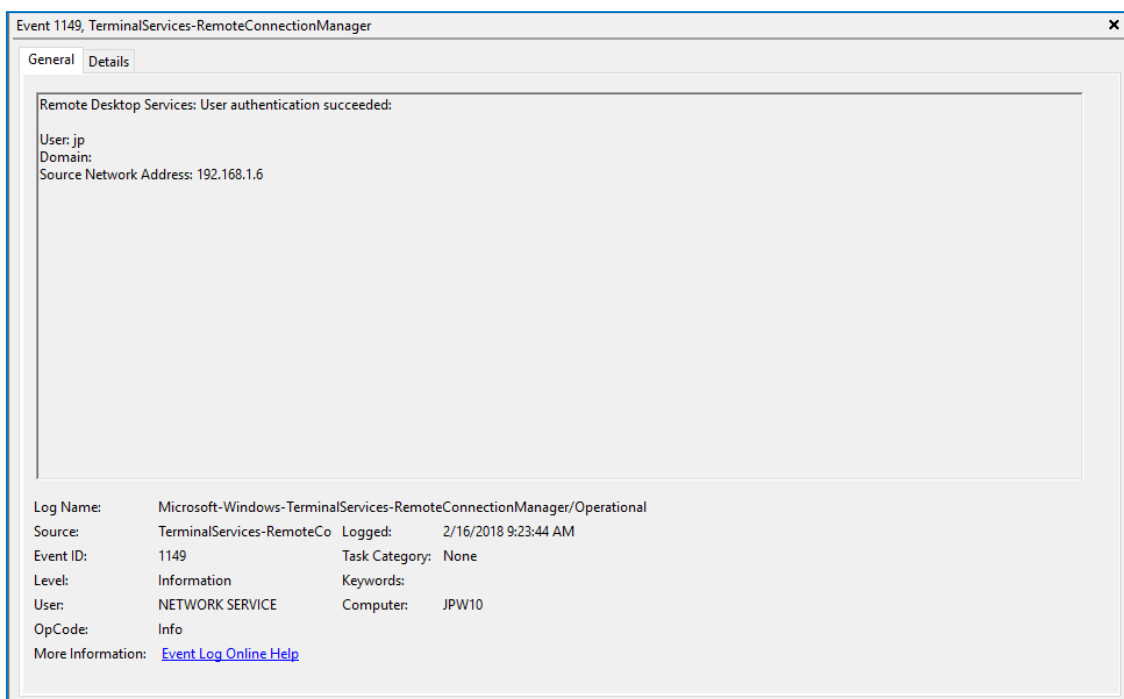
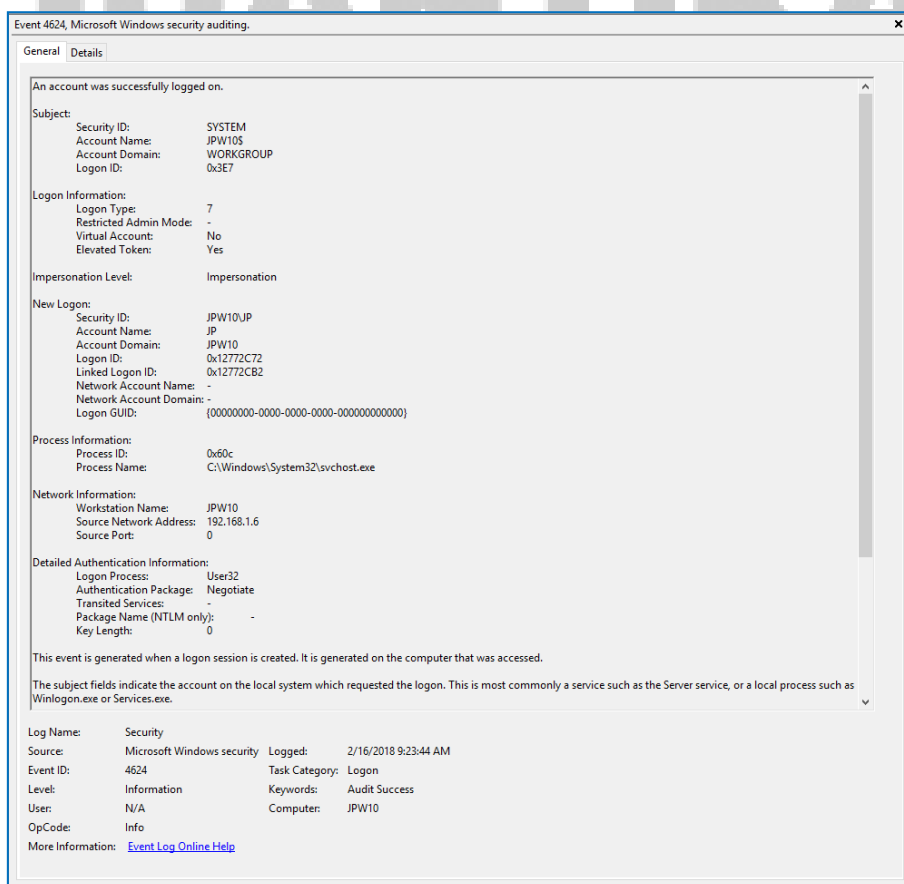
Una explicación más detallada de todo el proceso del escritorio remoto la podemos encontrar aquí:

<https://ponderthebits.com/2018/02/windows-rdp-related-event-logs-identification-tracking-and-investigation/>

RDP: CONEXIÓN SATISFACTORIA

Conexión satisfactoria mediante escritorio remoto



Ejemplo de evento 1149 con IP Origen:**Ejemplo de evento 4624 tipo 7:**

**Ejemplo de evento 21 con IP Origen**

Event 21, TerminalServices-LocalSessionManager

General Details

Remote Desktop Services: Session logon succeeded:

User: JPW10\JP
Session ID: 5
Source Network Address: 192.168.1.20

Log Name: Microsoft-Windows-TerminalServices-LocalSessionManager/Operational
Source: TerminalServices-LocalSessionManager Logged: 8/19/2018 2:12:41 PM
Event ID: 21 Task Category: None
Level: Information Keywords:
User: SYSTEM Computer: JPW10
OpCode: Info
More Information: [Event Log Online Help](#)



Ejemplo de evento 22 con IP Origen:

Event 22, TerminalServices-LocalSessionManager

General Details

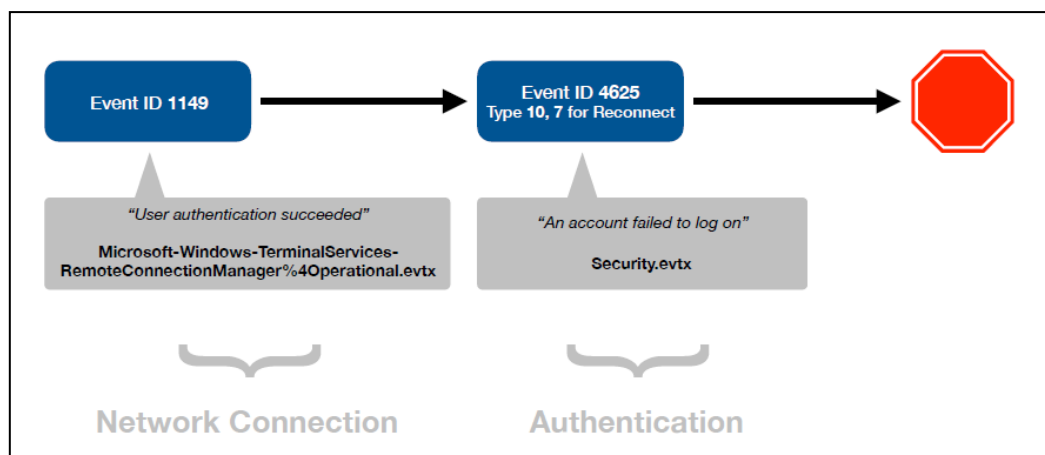
Remote Desktop Services: Shell start notification received:

User: JPW10\JP
Session ID: 5
Source Network Address: 192.168.1.20

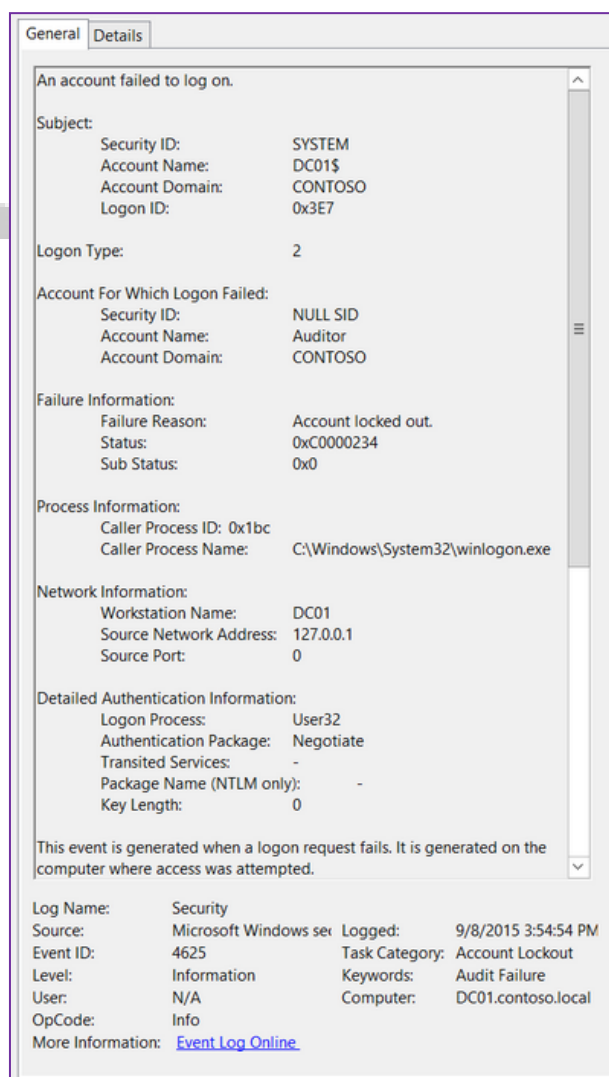
Log Name: Microsoft-Windows-TerminalServices-LocalSessionManager/Operational
Source: TerminalServices-LocalSessionManager Logged: 8/19/2018 2:12:41 PM
Event ID: 22 Task Category: None
Level: Information Keywords:
User: SYSTEM Computer: JPW10
OpCode: Info
More Information: [Event Log Online Help](#)

RDP: CONEXIÓN NO SATISFATORIA

La autenticación no satisfactoria mediante RDP

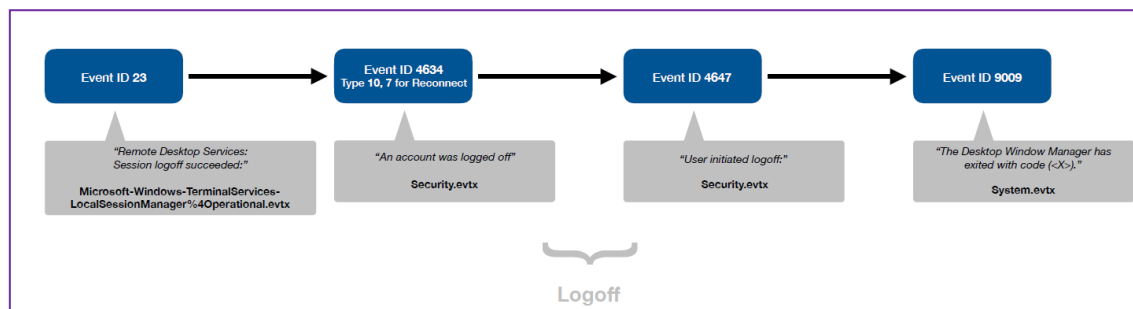


Evento 4625 tipo 2:



RDP: CONEXIÓN LOGOFF

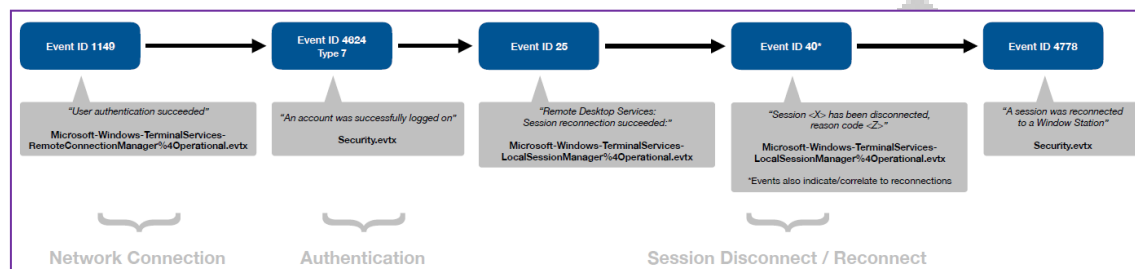
Desconexión de la consola de escritorio remoto mediante logoff solicitado por el usuario.



RDP:

RECONEXIÓN

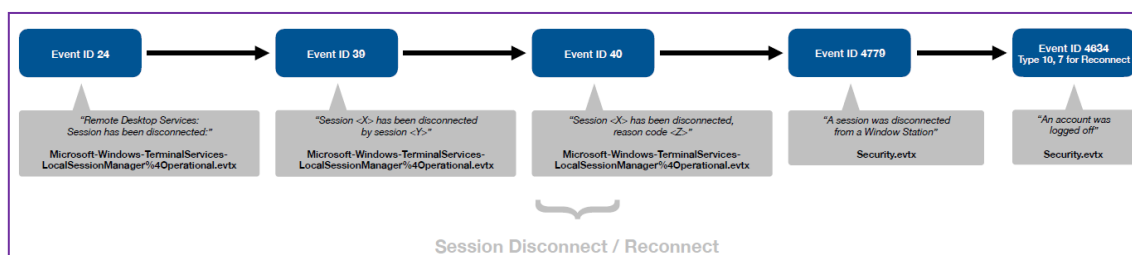
Conexión de nuevo con la consola de escritorio remoto



RDP: SESIÓN DESCONECTADA

Sesión desconectada, cerrando la ventana de escritorio remoto

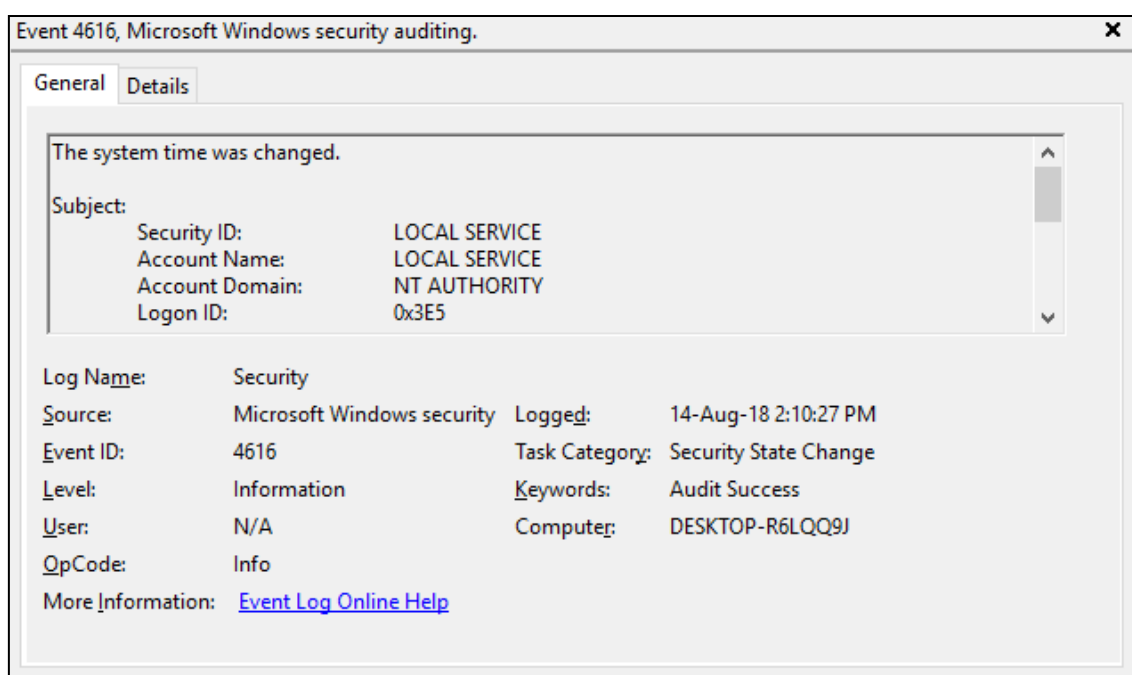
Ilustración 1 - Sesión desconectada por RDP



CAMBIO DE HORA

El cambio de hora de un sistema es una de las peores situaciones que se puede dar para un investigador ya que todos los timestamps quedan modificados:

Al hacer un cambio de hora se produce el Evento 4616 dentro de Security.evtx

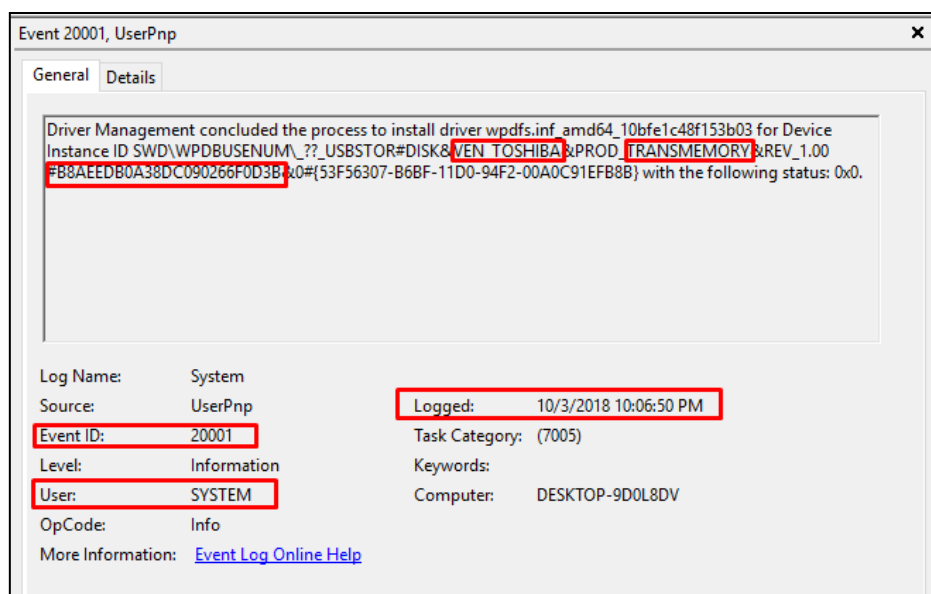


DISPOSITIVOS USB

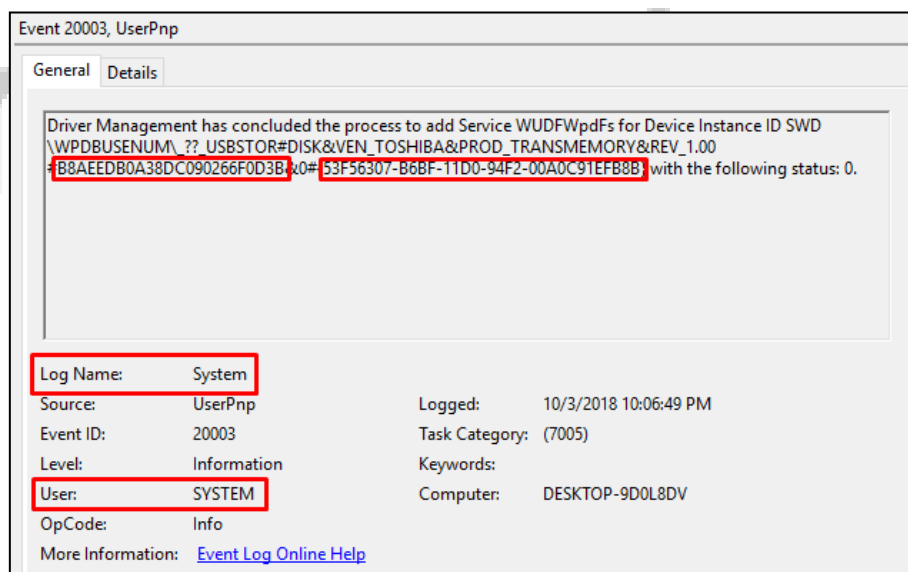
A parte de todos los artefactos que hemos visto anteriormente para la identificación de USBs, también podemos utilizar los **eventos de System.evtx**:

- ◆ 20001 /20003 contiene cuando se insertó por primera vez.
- ◆ 10000 contiene cuando se insertó por primera vez
- ◆ 10100 contiene el log de cuando se actualizó el driver.

Ejemplo de evento 20001

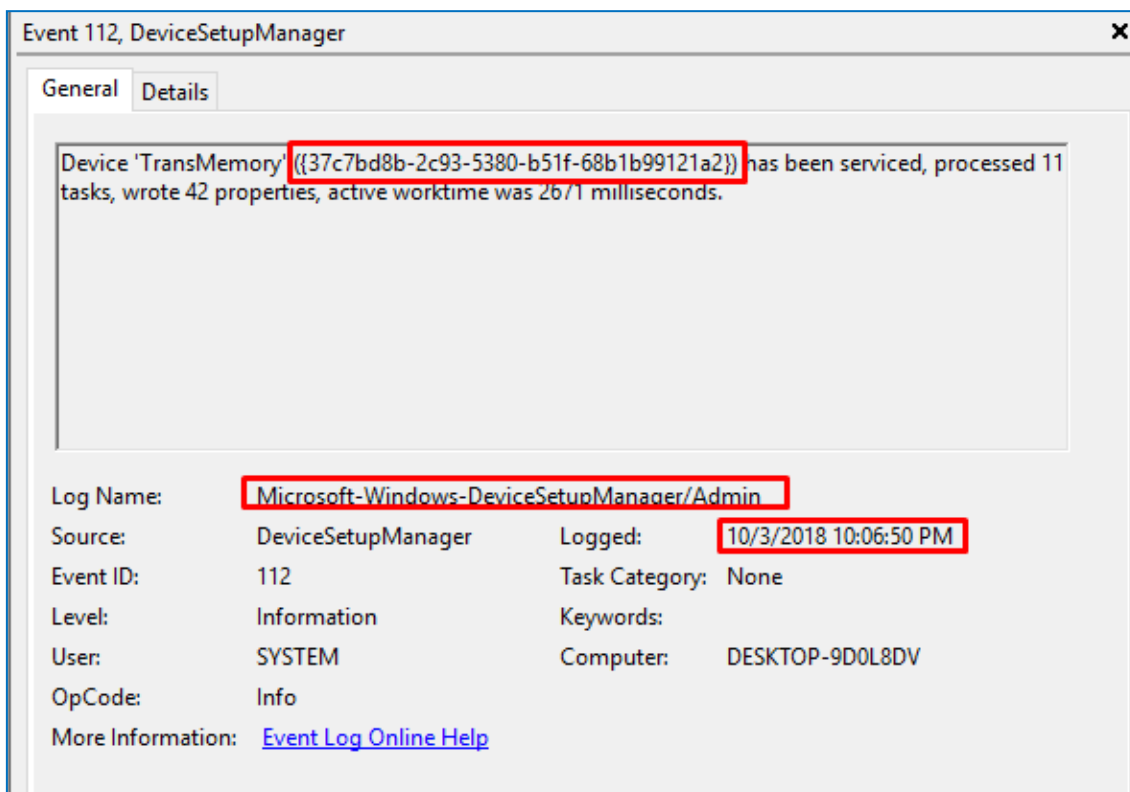


También se puede localizar el número de serie en la anterior captura junto con la marca y modelo, en el evento 20003



Eventos de Microsoft-Windows-DeviceSetupManager%4Admin.evtx

- ◆ Event ID 112: contiene el timestamp de cada dispositivo USB insertado en el sistema. Para correlar, es necesario conocer el ContainerID del USBSTOR key del registro que vimos previamente.

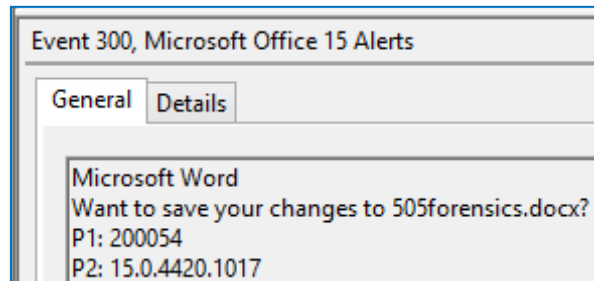


El Container ID concuerda con lo que se vio en la parte de Registro:

DeviceDesc	RegSz	@usbstor.inf,%genericbulkonly.devicedesc%;USB Mass Storage Device
LocationInformation	RegSz	Port_#0001.Hub_#0005
Capabilities	RegDword	148
Address	RegDword	1
ContainerID	RegSz	{37c7bd8b-2c93-5380-b51f-68b1b99121a2}
HardwareID	RegMultiSz	USB\VID_0930&PID_6544&REV_0100 USB\VID_0930&PID_6544
CompatibleIDs	RegMultiSz	USB\Class_08&SubClass_06&Prot_50 USB\Class_08&SubClass_06 USB\Class_08
ClassGUID	RegSz	{36fc9e60-c465-11cf-8056-444553540000}
Service	RegSz	USBSTOR
Driver	RegSz	{36fc9e60-c465-11cf-8056-444553540000}\0009
Mfg	RegSz	@usbstor.inf,%generic.mfg%;Compatible USB storage device
ConfigFlags	RegDword	0

OAlerts.evtx - Microsoft Office 16 Alerts

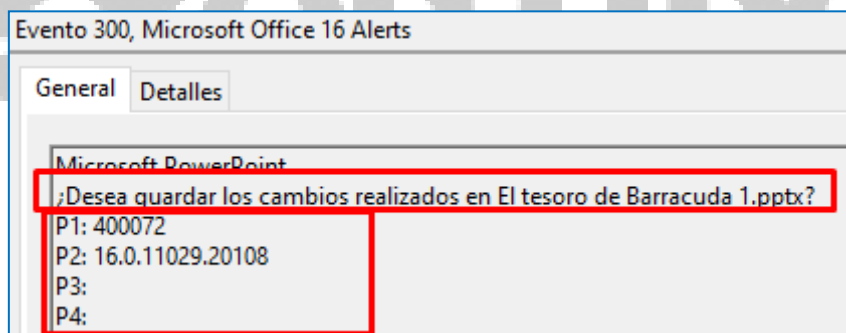
Con el nombre de OAlerts.evtx, permite capturar todas las alertas que se producen con los productos de Microsoft Office durante la interacción que mantiene con el usuario.



El estado del arte respecto a este tipo de eventos, indican que solamente hay un tipo, el evento ID 300. Este tipo de evento puede capturar:

- Borrado de ficheros y mensajes de correo electrónico.
- Guardado de cambios sobre los documentos ofimáticos: cuando el guardado es sobre una ruta externa, indicaría el uso de copiado de información.
- Alertas generadas cuando se habilita contenido externo (muy útil para investigaciones de Phishing)

A parte del mensaje en sí aparecen varios campos con P1, P2, P3 y P4 tal y como se puede identificar en la siguiente imagen:



El campo P1 hace referencia a la aplicación que emite el mensaje:

- Serie 1X - Microsoft Excel
- Serie 2x - Microsoft Word
- Serie 3x - Microsoft Outlook
- Serie 4x - Microsoft PowerPoint
- Serie 5x - Microsoft Access
- Serie 11x - Microsoft Publisher

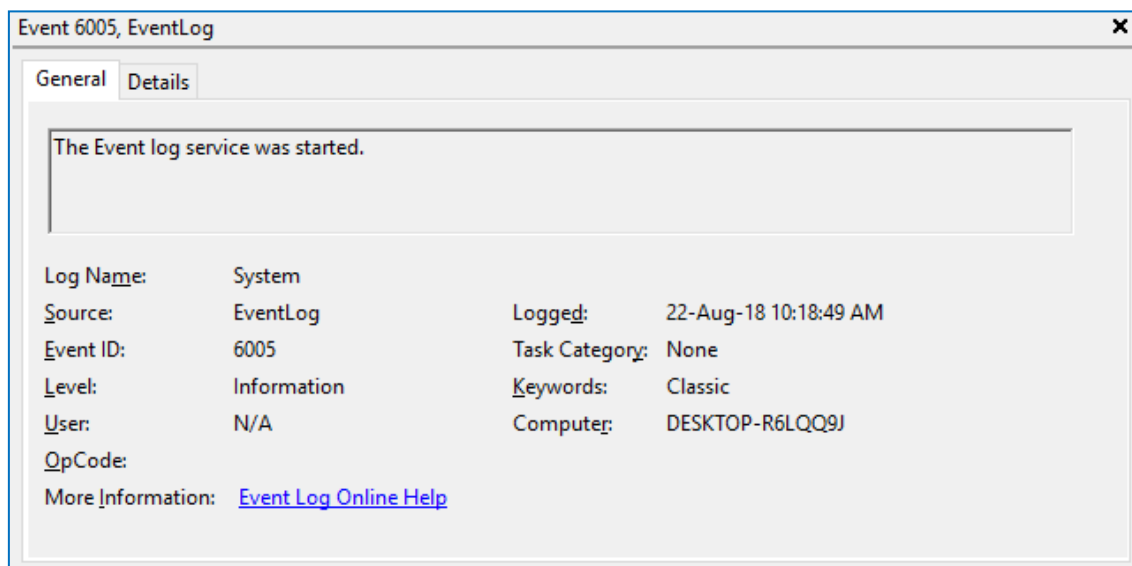
Mientras que el campo P2 hace referencia a la versión de office utilizada.

Un análisis de todos los eventos involucrados en la inserción y extracción de dispositivos USBs los podemos encontrar en el siguiente enlace:

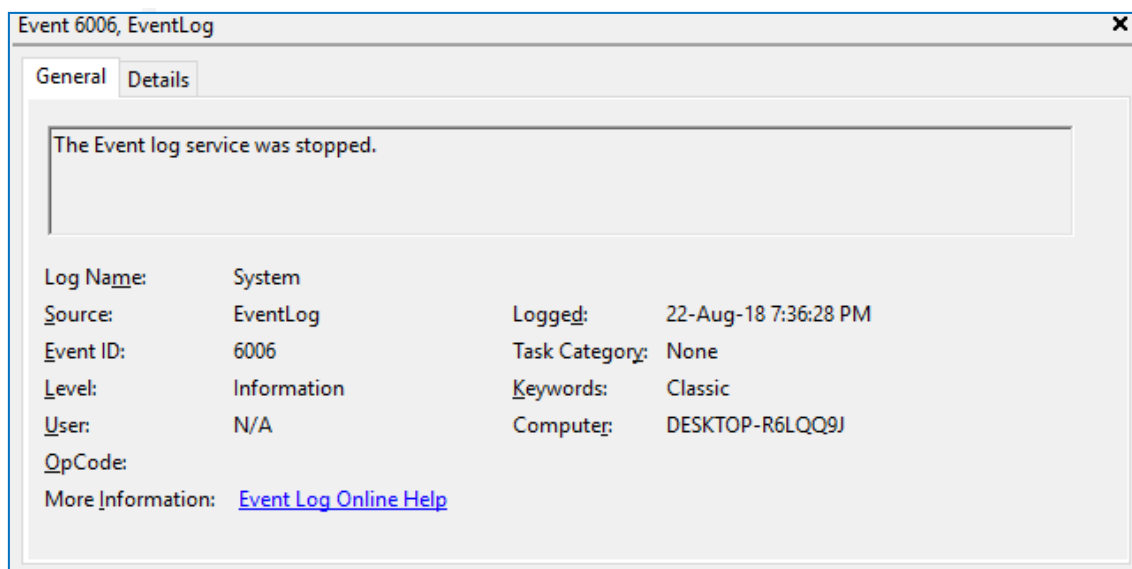
https://forensixchange.com/posts/19_08_03_usb_storage_forensics_1/

APAGADO/ARRANQUE DEL SISTEMA

Identificación del arranque del Sistema mediante el arranque del servicio “Event Log” en el evento 6005

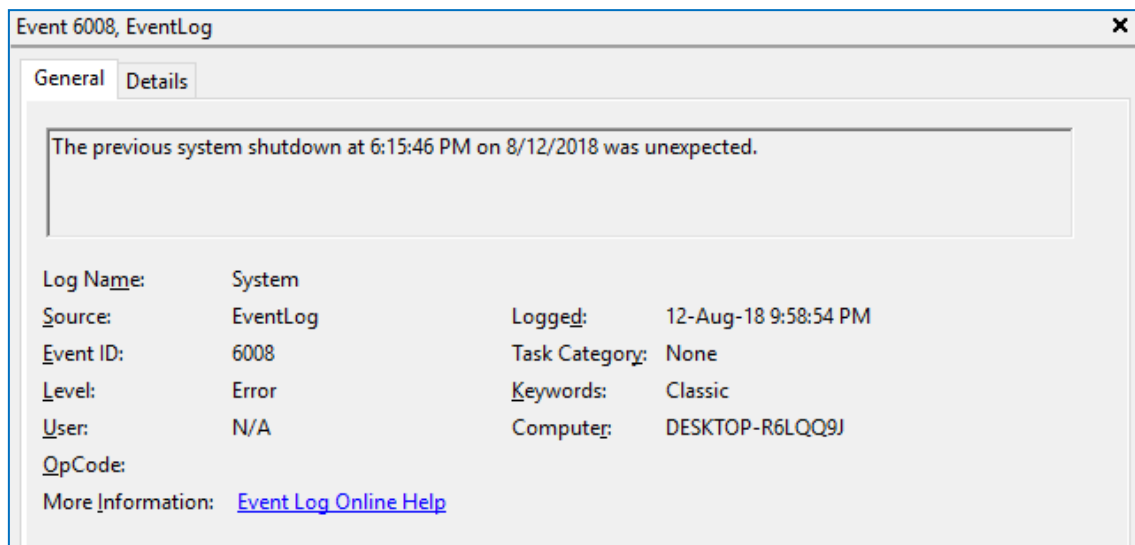


Identificación del apagado del sistema mediante la parada del servicio “Event Log” mediante el evento 6006

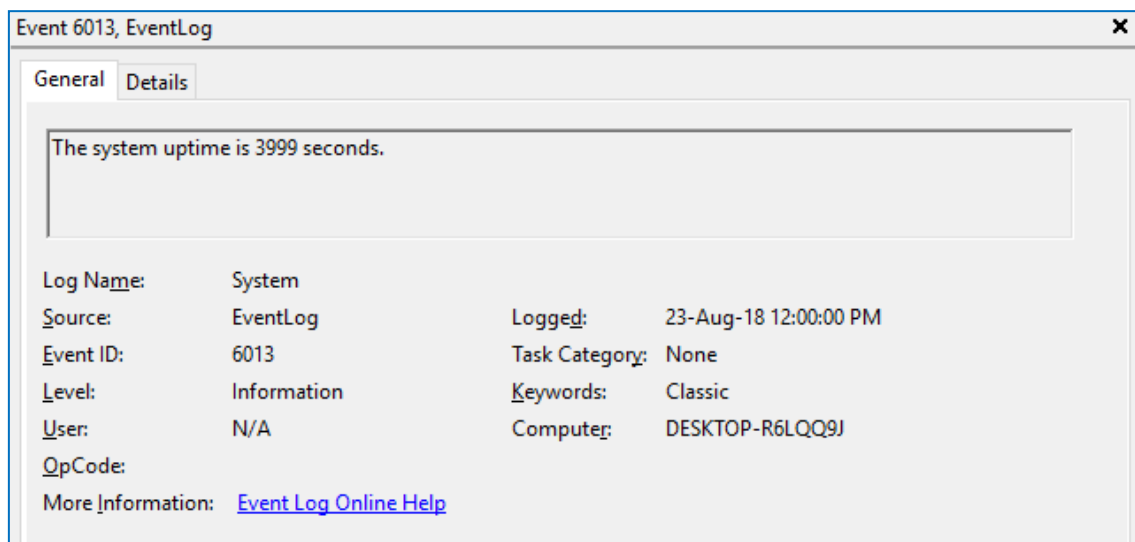




Identificación de un apagado inesperado mediante el evento 6008:

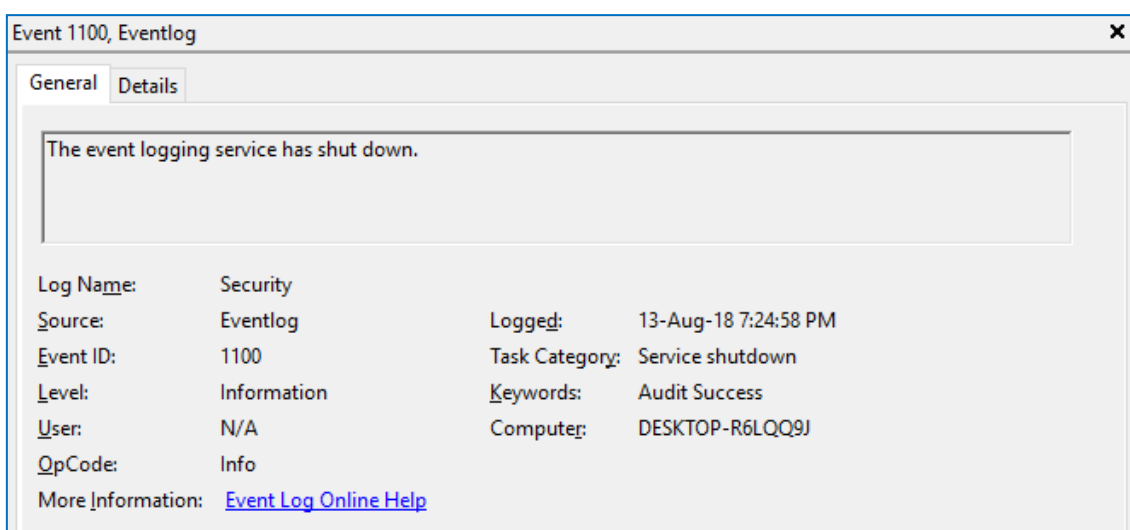


Identificación del tiempo que lleva encendido del sistema:





Apagado del servicio “Event Log” mediante el evento id 1100 en Security



VACIADO DE LOGS

Vaciado del fichero Security.evtx, identificado mediante el evento id 1102

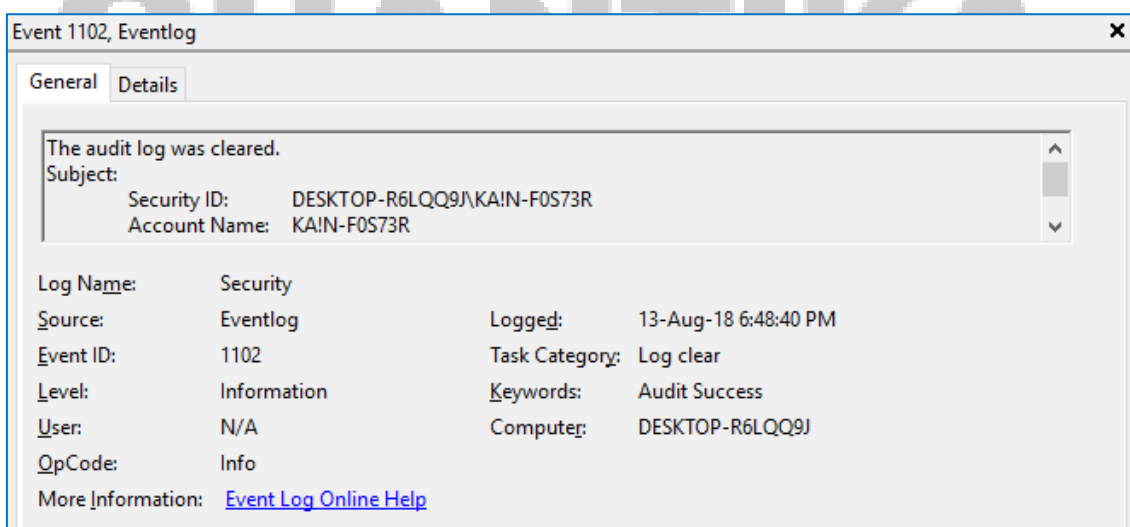


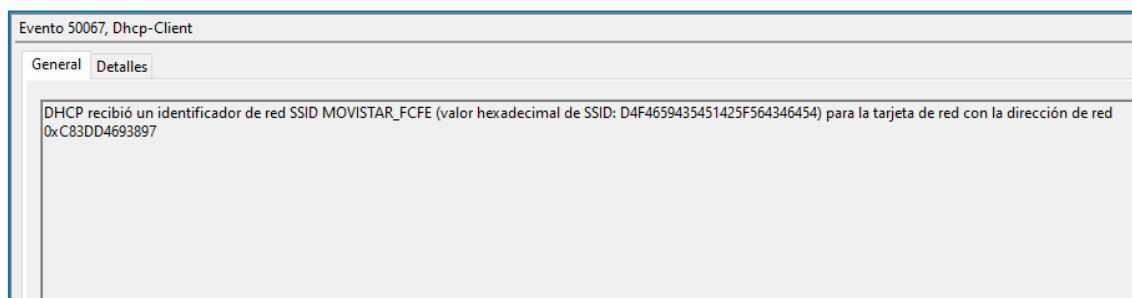
Ilustración 2 - Event ID 1102 de Security

Para más información de eventos de Windows se puede utilizar la siguiente página:

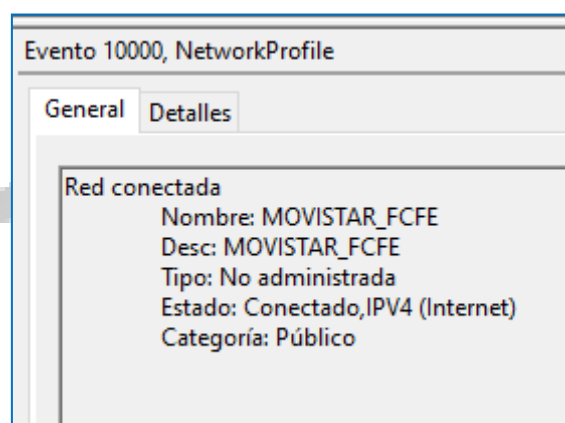
<https://www.ultimatewindowssecurity.com>

EVENTOS RELACIONADOS CON LA RED

Microsoft-Windows-Dhcp-Client%4Admin.evtx contiene los SSID de las redes WiFi a las que se ha conectado el equipo Windows:



Microsoft-Windows-NetworkProfile%4Operational.evtx contiene los eventos relacionados con las conexiones de los perfiles de RED, ya sea WiFi, un dispositivo 4g/5gb o una red conectada, mediante el **event id 10000**:



O una red desconectada con el **event id 10001**:

