

## **Lab 1.7 Application Execution Analysis**

**Teoria**

**Y**

**Pratica**



**NTUSER.DAT, SYSTEM, and Prefetch**

## Background/Desktop Activity Moderator



Program execution

Propósito
<ul style="list-style-type: none"><li>• Background Activity Moderator (BAM)</li><li>• Desktop Activity Moderator (DAM)</li><li>• Utilizado para la regulación de aplicaciones en "Connected Standby" para ahorrar energía de la batería.</li></ul>
Localización
<ul style="list-style-type: none"><li>•SYSTEM\CurrentControlSet\Services\bam\UserSettings\{SID}</li><li>•SYSTEM\CurrentControlSet\Services\dam\UserSettings\{SID}</li></ul>

Entre los artefactos más recientes que se han descubierto se encuentran las claves BAM.

BAM es un acrónimo de Background Activity Moderator. La segunda clave, casi idéntica a la primera, es la clave DAM, que está relacionada con el Desktop Activity Moderator. Las claves son bastante directas en el sentido de que registran la ruta del ejecutable y la última **fecha/hora de ejecución**.

**El DAM** está presente en sistemas que tienen **Connected Standby**. **Connected Standby** se utiliza cuando Windows está aún encendido, pero la pantalla está apagada. Es similar a cuando un usuario presiona el botón de encendido en un smartphone, pero el teléfono sigue técnicamente encendido. El DAM ayuda suspendiendo y ralentizando el acceso a las aplicaciones de escritorio para que la vida útil de la batería pueda extenderse más, pero los procesos en un sistema aún pueden funcionar y mantener sus capacidades.

**El Background Activity Moderator** es un servicio de controlador de modo kernel que apareció inicialmente en Win10 versión 1709. Hay muy poca información publicada en los sitios web de Microsoft sobre él y cómo se relaciona directamente con el DAM. Sin embargo, ambas claves parecen tener información similar en ellas. La única información encontrada sobre el BAM puede detallarse en los blogs iniciales de DFIR que publicaron detalles sobre los artefactos de ejecución que rastrearon.

+ Info:

[BAM](#)

[BAM KEY](#)

[Desktop Activity Moderator](#)

5-1-5-21-3047407172-2892838466-1416134151-1001					
S-1-5-90-0-1					
BasicDisplay			Device\HarddiskVolume3\Program Files (x86)\CodeMeter\Runtime\bin\CodeMeterCC.exe		2018-03-16 12:33:55
BasicRender			Device\HarddiskVolume3\Program Files (x86)\Egnyte Connect\EgnyteDrive.exe		2018-03-16 12:33:56
BattC			Device\HarddiskVolume3\Program Files (x86)\Google\Drive\googledrivesync.exe		2018-03-16 12:33:57
bomfh2			Device\HarddiskVolume3\Windows\System32\cmd.exe		2018-03-16 12:34:04
BDESVC			Device\HarddiskVolume3\Program Files\Microsoft Office\root\Office16\ONENOTE.EXE		2018-03-16 12:34:08
Beep			Microsoft.SkypeApp\jzlf8qxf38zg5c		2018-03-16 12:34:36
BFE			Device\HarddiskVolume3\Windows\System32\ApplicationFrameHost.exe		2018-03-16 12:35:01
BITS			Microsoft.ZuneVideo_Bwekyb3d8bbwe		2018-03-16 12:35:10
Bonjour Service			Microsoft.WindowsCalculator_Bwekyb3d8bbwe		2018-03-16 12:35:16
browser			Microsoft.Windows.Photos_Bwekyb3d8bbwe		2018-03-16 12:35:22
			Device\HarddiskVolume3\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe		2018-03-16 12:45:20
CryptSvc	11		Device\HarddiskVolume8\Windows\System32\cmd.exe		2017-03-18 21:34:50
CSC	9		Device\HarddiskVolume8\Program Files (x86)\Steam\Steam.exe		2017-03-18 21:34:55
CscService	12		Device\HarddiskVolume8\Program Files (x86)\TechSmith\Snagit 13\Snagit32.exe		2017-03-18 21:34:51
dam	7		Device\HarddiskVolume8\Program Files\GPSoftware\Directory Opus\dopus.exe		2017-03-18 21:34:50
UserSettings	0		Device\HarddiskVolume2\cmd\vendor\conemu-maximus5\ConEmu64.exe		2017-03-17 18:49:40
S-1-5-18	6		Device\HarddiskVolume8\Program Files (x86)\Jabra\Direct\JabraDirect.exe		2017-03-18 21:34:50
S-1-5-21-238543598-4054144643-4261915534-1114	114		Device\HarddiskVolume8\Users\eric\AppData\Local\slack\app-2.5.1\slack.exe		2017-03-12 19:17:14

Este es un ejemplo de extracción de la clave del registro para los artefactos BAM/DAM. Puedes identificar la ruta completa de un programa y la última vez que se ejecutó. Puedes ver programas

comunes como OneNote, el símbolo del sistema, y muchas aplicaciones de Microsoft también, como Fotos de Windows, ZuneVideo, y Calculadora.

## Last Commands Executed



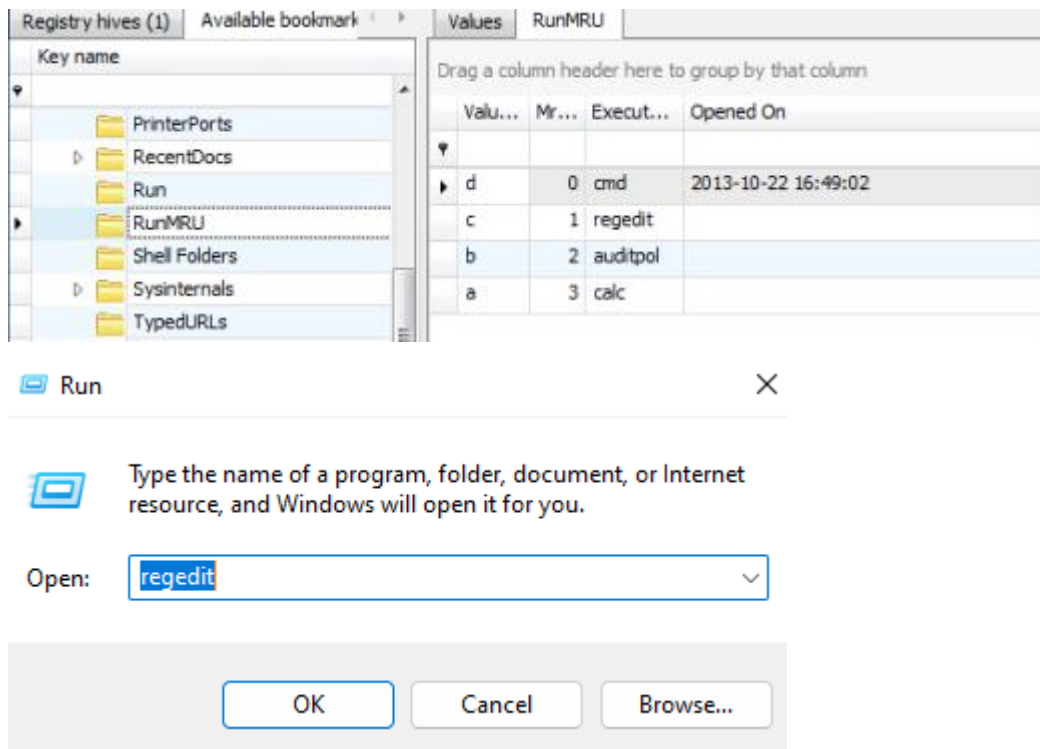
### Program Execution

Localización:

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

- MRUList
  - Orden en el que se ejecutaron los comandos
- Comandos
  - Comandos escritos RUN box de XP/Vista/Win7/8
  - Invocados típicamente mediante las teclas WINDOWS+R





Este es un ejemplo de dónde puedes encontrar el "Último Comando Ejecutado" en el sistema Windows:

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

Cada vez que alguien ejecuta un comando desde Inicio -> Ejecutar (RUN), se registrará la entrada para el comando que ejecutaron. Esta clave listará los comandos ejecutados desde Inicio -> Ejecutar desde la barra de Windows en el escritorio.

El orden en el que se ejecutan los comandos se enumera en el valor de la lista RunMRU. **Las letras representan el orden en el que se ejecutaron los comandos.**

## GUI Program Execution: UserAssist Key



Localización:

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

### **GUIDs for XP/VISTA:**

- 5e6ab780...** -> Internet Toolbar
- 75048700...** -> Active Desktop

### **GUIDs for Win7 and Higher**

- CEBFF5CD-ACE2-4F4F-9178-9926F41749EA**-> Executable File Execution

•**F4E57C4B-2036-45F0-A9AB-443BCFE33D9F** -> Shortcut File Execution

Si nuestro sospechoso ejecutó un programa, ¿podemos saber cuándo fue la última vez que se ejecutó? ¿Podemos saber cuántas veces se ejecutó un programa en el sistema? Las claves USERASSIST en el HIVE del registro NTUSER.dat del sospechoso nos ayudaran aquí.

Las aplicaciones GUI también dejan huellas específicas de las actividades de un usuario en el HIVE NTUSER.DAT.

Las claves que examinaremos en general son las claves USERASSIST, que pueden mostrar la última vez que se ejecutó un programa y la cantidad de veces que se ejecutó.

El análisis adecuado de la clave **UserAssist** nos permitirá determinar lo siguiente para cada programa GUI lanzado en Windows Explorer:

- **Última hora de ejecución (UTC)**
- **Cantidad de ejecuciones**
- **Nombre de la aplicación GUI**
- **Tiempo de enfoque: tiempo total que una aplicación tiene el enfoque, expresado en milisegundos**
- **Cantidad de enfoques: número total de veces que una aplicación volvió a enfocarse en el Explorador (se movió el mouse sobre la aplicación y se hizo clic)**

Una de las cosas más interesantes de un sistema Windows es la gran cantidad de datos que se recopilan. Algunos de estos se encuentran en el registro del usuario. Si resulta que estás conectado como el usuario que está bajo investigación, puedes ejecutar un programa (como UserAssistView de NirSoft

[http://www.nirsoft.net/utils/userassist\\_view.html](http://www.nirsoft.net/utils/userassist_view.html) ) que examinará el archivo de registro de ese usuario bajo

Software\Microsoft\Windows\Currentversion\Explorer\UserAssist\{GUID}\Count. El GUID (Identificador Único Global) apunta al tipo de aplicación que se está utilizando.

Por otra parte, tenemos:



Windows XP UserAssist value names:

Todos los valores empiezan **UEME\_.** , **seguido de:**

- **RUNPATH:** Path absoluto de un ejecutable
- **RUNCPL:** Ejecutado desde el applet de control panel
- **RUNPIDL:** shortcut o LNK FILE
- **UIQCUT:** Conteo del programa lanzado desde Quick Launch
- **UITOOLBA:** Mantiene entradas de los clicks via Windows Explorer Toolbar

Por otra parte : **Win7-Win10 UserAssist Name Values**

ProgramFilesX64	• 6D809377-6AF0-444B-8957-A3773F02200E
ProgramFilesX86	• 7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E
System	• 1AC14E77-02E7-4E5D-B744-2EB1AE5198B7
SystemX86	• D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27
Desktop	• B4BFCC3A-DB2C-424C-B029-7FE99A87C641
Documents	• FDD39AD0-238F-46AF-ADB4-6C85480369C7
Downloads	• 374DE290-123F-4565-9164-39C4925E467B
UserProfiles	• 0762D272-C50A-4BB0-A382-697DCD729B80

Gracias al fantástico trabajo e investigación de Didier Stevens, sabemos que el cambio más crítico es que las claves del registro UserAssist para Windows 7 ya no tienen un valor UEME antepuesto. Incluso Windows Vista seguía el formato UEME original de WinXP.

En Windows 7 y versiones posteriores, **la decodificación del cifrado ROT13 no resulta en una ruta completa, pero generalmente muestra el ejecutable o el archivo LNK además de un GUID.** Los GUID te indicarán la ubicación de la ruta para el archivo ejecutable. Muchos de los GUID son ampliamente conocidos y pueden ser traducidos o buscados fácilmente a través de búsquedas en internet. También hay un excelente sitio web de Microsoft que lista la mayoría de estas ubicaciones.

En otros casos, en Windows 7 y versiones posteriores, mostrará la ruta completa del archivo ejecutable además del ejecutable en ubicaciones donde una ruta de carpeta no esté definida por una entrada de GUID. Debido al fantástico trabajo e investigación de Didier Stevens, sabemos que el cambio más crítico es que las claves

del registro UserAssist para Windows 7 **ya no tienen un valor UEME antepuesto para aplicaciones.**

**El RUNPATH** es la ruta absoluta de un ejecutable. Es probable que el usuario haya hecho doble clic en el ejecutable a través de la interfaz de Windows Explorer.

**El RUNCPL** es el lanzamiento de un applet del Panel de Control. Esto es interesante si ves a algún usuario cambiando valores de seguridad o configuraciones de usuario en el sistema.

**El RUNPIDL** es un puntero al archivo real, como un acceso directo desde un archivo LNK.

**El UIQCUT** cuenta el programa lanzado a través del acceso directo del menú de inicio rápido.

**El UISCUT** cuenta el programa lanzado a través del acceso directo del escritorio.

La entrada **UITOOLBAR** guarda datos sobre clics a través de la barra de herramientas del Explorador de Windows.

+ Info :

[Into The Boxes](#)

[Known Folder GUIDs for File Dialog Custom Places](#)

[CLSID List](#)

[CLSID Key \(GUID\) Shortcuts List for Windows 7](#)

## Windows Prefetch



### Program Execution

Prefetch XP/Vista/Win7/Win8/Win10
<ul style="list-style-type: none"><li>• Aumenta el rendimiento del sistema al precargar páginas de código.</li><li>• El administrador de caché supervisa todos los archivos y directorios y los asigna en un archivo .pf.</li><li>• Se utiliza para mostrar la ejecución de aplicaciones (qué y cuándo).</li><li>• Desactivado en sistemas con unidad de estado sólido (SSD), de lo contrario, activado de forma predeterminada.</li></ul>
C:\Windows\Prefetch
<ul style="list-style-type: none"><li>• Limitado a 128 archivos en XP y Vista/Win7.</li><li>• Limitado a 1024 archivos para Win8/Win10.</li><li>• (nombre del ejecutable)-(hash).pf</li><li>• A partir de Win10, los archivos de Prefetch están comprimidos.</li></ul>

- El hash se calcula en función de la ruta <dir> del ejecutable y las opciones de línea de comandos de ciertos programas (por ejemplo, svchost.exe).

#### **c:\Windows\Prefetch\Layout.ini**

El archivo layout.ini contiene los nombres de ruta originales de los archivos ubicados en el Prefetch.

- El Desfragmentador de disco utiliza layout.ini para reubicar todos los directorios y archivos en un área contigua del disco.

Cuando el sistema operativo utiliza Prefetch, cargará en memoria fragmentos de datos, archivos y código antes de que la información sea necesaria.

El directorio de Prefetch va almacenando datos una vez que se ejecuta una aplicación, por lo que podría ser una buena idea obtener manualmente el contenido del directorio de Prefetch antes de realizar cualquier respuesta a incidentes en una máquina, ya que el contenido de este directorio podría considerarse bastante volátil. El administrador de caché supervisa todos los archivos y directorios referenciados para cada aplicación o proceso y los asigna a un archivo .pf. **El directorio de Prefetch estará limitado a 128 archivos. En Windows 8 y Windows 10, puede haber hasta 1024 archivos en la carpeta Prefetch. A partir de Windows 10, los archivos de Prefetch están comprimidos.**

Para deshabilitar Prefetch:

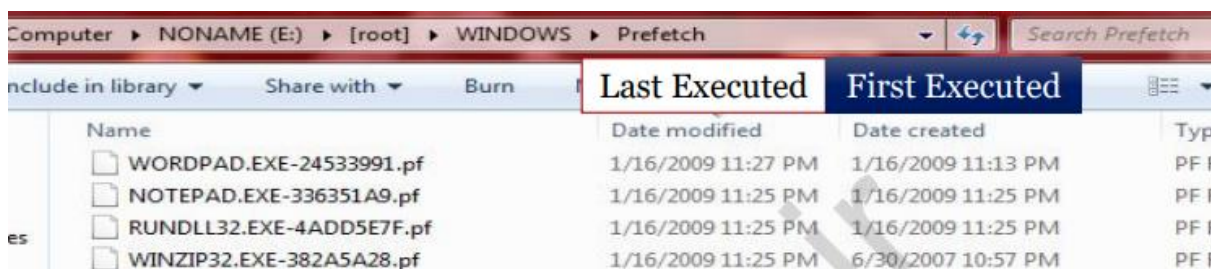
Update the EnablePrefetcher registry key in your run-time image:

- Key:  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters
- Name: EnablePrefetcher
- Type: REG\_DWORD
- Value: 0

Para habilitar Prefetcher key debe tener uno de los siguientes valores:

- 0 = Disabled
- 1 = Application launch prefetching enabled
- 2 = Boot prefetching enabled
- 3 = Application launch and boot enabled To disable Prefetch, set the value to 0

Prefetch Analysis – First/Last Execution	
Date/Time .exe was first executed*	
<ul style="list-style-type: none"> <li>• Creacion de datos .pf file (~-10 seconds)</li> </ul>	
Date/Time .exe last executed	
<ul style="list-style-type: none"> <li>• La hora exacta se almacena en el archivo .pf para el momento exacto.</li> <li>• Windows 8 y Windows 10 almacenan las últimas 8 veces ejecutadas incrustadas en cada archivo .pf.</li> <li>• Fecha de la última modificación del archivo .pf ((~-10 seconds).</li> </ul>	



Name	Date modified	Date created	Type
WORDPAD.EXE-24533991.pf	1/16/2009 11:27 PM	1/16/2009 11:13 PM	PF I
NOTEPAD.EXE-336351A9.pf	1/16/2009 11:25 PM	1/16/2009 11:25 PM	PF I
RUNDLL32.EXE-4ADD5E7F.pf	1/16/2009 11:25 PM	1/16/2009 11:25 PM	PF I
WINZIP32.EXE-382A5A28.pf	1/16/2009 11:25 PM	6/30/2007 10:57 PM	PF I

## PECmd.exe – Análisis de archivos Prefetch

```
C:\> PECmd.exe -f SDELETE.EXE-2288BD2E.PF (SINGLE .PF PARSING)
```

```
C:\> PECmd.exe -d "E:\C\Windows\Prefetch" --csv "G:\cases" -q (DIR PARSING)
```

```
PECmd.exe -d "<dir of PF files>" --csv "<dir>" -q
-d "<dir of PF files>" = Dir to recursively process
-f "<filename>" = File to process
-q = Quiet Output; use w/ --csv
-k = Comma Separated Keywords
--csv "<dir>" = Dir to save CSV (tab separated)
--html "<dir>" = Dir to save html
```



Similar al resto de las herramientas de Eric Zimmerman, PECmd.exe tiene muchas opciones similares. Necesitamos especificar -f o -d. Esto demostrará el procesamiento de un solo archivo de prefetch, ya que la opción -d básicamente hace lo mismo para todos los archivos de prefetch (\*.pf) encontrados en el directorio dado. Además, la opción -d procesa directorios de forma recursiva.

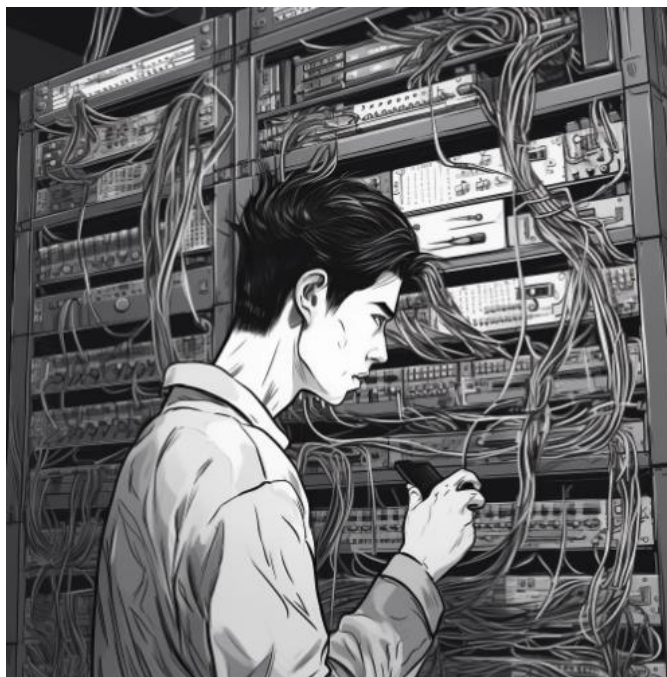
A continuación, veamos cómo puedes aumentar las palabras clave integradas. La Flag -k te permite proporcionar una lista separada por comas de los valores que deseas resaltar en los nombres de archivo y/o directorios. Asegúrate de rodear la lista con comillas dobles.

La API de Windows contiene soporte para descomprimir archivos de prefetch de Windows 10 a partir de Windows 8. Dado que Eric se basa en la API de Windows para descomprimir archivos de prefetch creados en Windows 10, debes ejecutar PECmd.exe en al menos Windows 8 para procesar archivos de Windows 10.

Processing OSCMPGPK.EXE-D0CC0901.pf	
Created on: 2012-04-03 21:18:21 +00:00	
Modified on: 2012-04-03 21:18:21 +00:00	
Last accessed on: 2012-04-03 21:18:21 +00:00	
Executable name: OSCMPGPK.EXE	
Hash: D0CC0901	
File size (bytes): 7,052	
Version: Windows Vista or Windows 7	
Run count: 1	
Last run: 2012-04-03 21:18:21 +00:00	
Volume information:	
#0: Name: \DEVICE\HARDDISKVOLUME1 Serial: AC036525 Created: 2012-04-03 21:18:21 +00:00	
Directories referenced: 3	
#0: \DEVICE\HARDDISKVOLUME1\WINDOWS	
#1: \DEVICE\HARDDISKVOLUME1\WINDOWS\APPPATCH	
#2: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32	
Files referenced: 13	
#0: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\NTDLL.DLL	10/22/2013 16:25:23 c:\WINDOWS\SYSTEM32\DLLHOST.EXE
#1: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\KERNEL32.DLL	10/22/2013 16:25:24 c:\WINDOWS\SYSTEM32\ATBROKER.EXE
#2: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\APITSETSCHEMA.DLL	10/22/2013 16:25:24 c:\WINDOWS\SYSTEM32\RDPClip.EXE
#3: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\KERNELBASE.DLL	10/22/2013 16:33:34 c:\WINDOWS\SYSTEM32\WERFAULT.EXE
#4: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\LOCALS.HLS	10/22/2013 16:33:34 c:\WINDOWS\SYSTEM32\SVCHOST.EXE
#5: \DEVICE\HARDDISKVOLUME1\WINDOWS\OSCMGPK.EXE	10/22/2013 16:33:37 c:\PROGRAM FILES\MICROSOFT OFFICE 15\ROOT\OFFICE15\EXCEL.EXE
#6: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\ADVAPI32.DLL	10/22/2013 16:34:04 c:\WINDOWS\SYSTEM32\TASKMGR.EXE
#7: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\VSVCRT.DLL	10/22/2013 16:34:16 c:\WINDOWS\SYSTEM32\WERMGR.EXE
#8: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\SECCHOST.DLL	10/22/2013 16:34:16 c:\WINDOWS\SYSTEM32\WERMGR.EXE
#9: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\RPCRT4.DLL	10/22/2013 16:34:23 c:\USERS\DONALD\DOWNLOADS\SDELETE.EXE
#10: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\APPHelp.DLL	10/22/2013 16:34:32 c:\USERS\DONALD\DOWNLOADS\SDELETE.EXE
#11: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\RUNDLL32.EXE	10/22/2013 16:34:42 c:\USERS\DONALD\DOWNLOADS\SDELETE.EXE
#12: \DEVICE\HARDDISKVOLUME1\WINDOWS\APPPATCH\SYSMAN.SOB	10/22/2013 16:34:51 c:\USERS\DONALD\DOWNLOADS\SDELETE.EXE
	10/22/2013 16:35:02 c:\USERS\DONALD\DOWNLOADS\SDELETE.EXE
	10/22/2013 16:35:10 c:\USERS\DONALD\DOWNLOADS\SDELETE.EXE
	10/22/2013 16:35:19 c:\USERS\DONALD\DOWNLOADS\SDELETE.EXE
	10/22/2013 16:38:05 c:\PROGRAM FILES\WINDOWS DEFENDER\M...
	10/22/2013 16:38:06 c:\WINDOWS\SYSTEM32\TS_THEME.EXE
	10/22/2013 16:38:09 c:\WINDOWS\SYSTEM32\ATBROKER.EXE
	10/22/2013 16:38:09 c:\WINDOWS\SYSTEM32\RDPClip.EXE

PECMD -d (dir parsing mode) creates a timeline (TSV) file similar to this output

## Lab 1.7 Application Execution Analysis



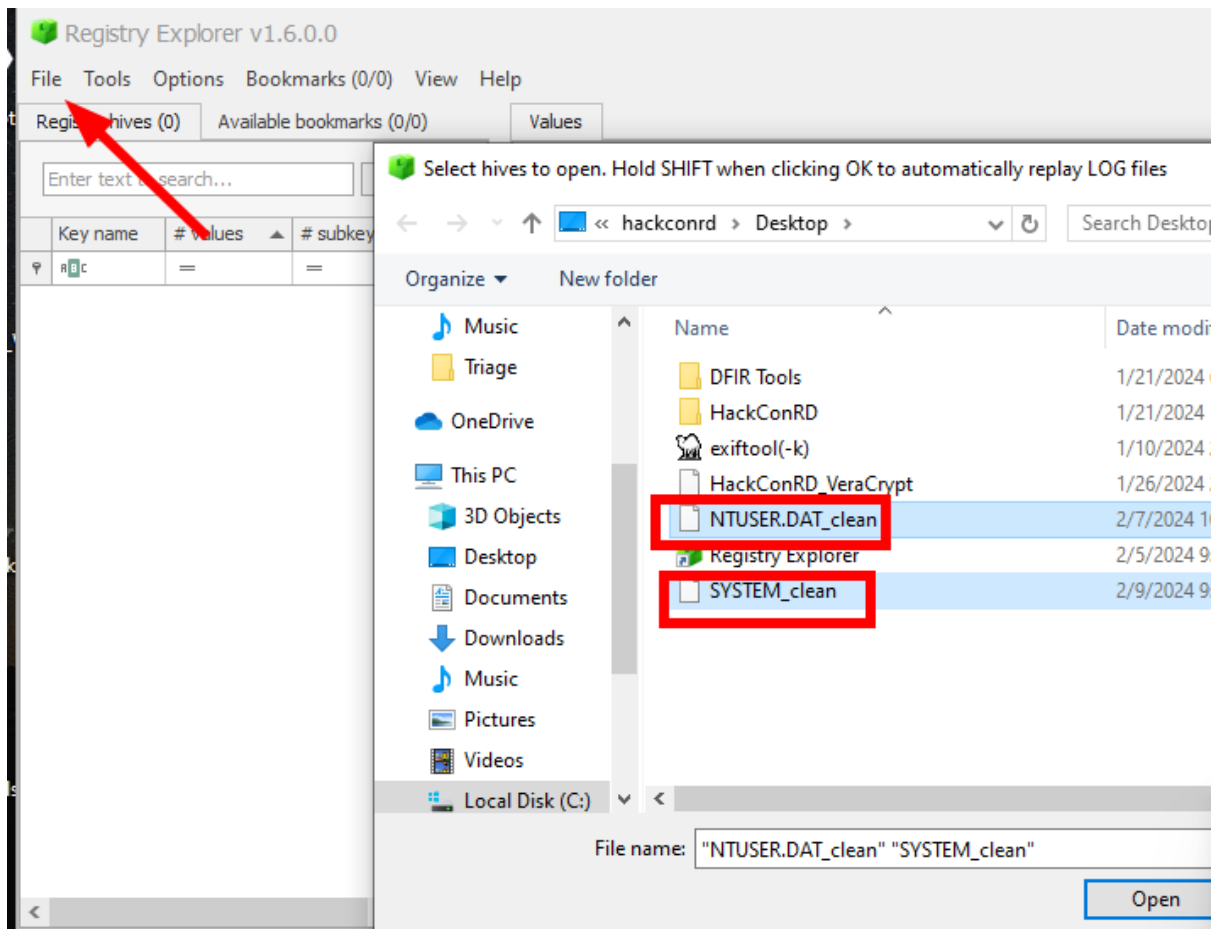
### Objetivos:

La ejecución de aplicaciones es una de las categorías de artefactos más importantes que utilizamos para comprender lo que sucedió en una computadora. Auditar qué aplicaciones estaban presentes y en funcionamiento puede proporcionar una gran perspectiva sobre las actividades del usuario, el tipo de datos que esperar en el sistema, y explicar anomalías que podrían ser causadas por malware o herramientas anti-forenses. Afortunadamente, esta categoría contiene una gran cantidad de artefactos diferentes que pueden demostrar la ejecución de aplicaciones. En este ejercicio exploraremos tres artefactos muy importantes: BAM, UserAssist y Prefetch.

- Exploraremos la clave del registro BAM de Windows 10.
- Decodificaremos los datos ocultos presentes en la clave UserAssist de NTUSER.DAT.
- Examinaremos la gran cantidad de información de ejecución de aplicaciones presente en los archivos de Prefetch de Windows.

- Utilizaremos los metadatos de ejecución de aplicaciones para determinar los tiempos de ejecución y el número de ejecuciones de las aplicaciones.

Al igual que ejercicios anteriores, montamos nuestra imagen (Triage Evidence) y usamos los registros clean de SYSTEM y NTUSER



## BAM!

BAM es un acrónimo Background Activity Moderator, y la clave del registro correspondiente mantiene una lista simple de aplicaciones ejecutadas y su último tiempo de ejecución. Los datos se almacenan por usuario a través de subclaves nombradas para cada identificador de seguridad de cuenta / identificador relativo (SID/RID).

Recuerda que la cuenta fredr tiene un RID de 1002 (según nuestro análisis previo del registro SAM). Por lo tanto, querremos investigar la siguiente clave en el registro SYSTEM:

BAM Key:

**SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-528816539-567677750-276746561-1002**

Ordene el contenido de la clave por Tiempo de Ejecución y revise las aplicaciones ejecutadas el 14 de noviembre de 2020 (UTC), el día del incidente en la residencia del Sr. Rocba. Si no está acostumbrado a mirar los nombres de las aplicaciones de Windows, puede haber muchas de las que no está al tanto. Enumere algunas que podrían ser particularmente interesantes para nuestra investigación.

1. regedit (Editor del Registro) es una herramienta administrativa legítima de Windows, pero parece extraño que se acceda a ella durante un tiempo de otra actividad sospechosa. Regedit se puede utilizar para agregar o eliminar elementos del registro.
2. mstsc es el Cliente de Servicios de Terminal de Microsoft. Esta herramienta se utilizaría para iniciar una sesión de RDP saliente hacia otro sistema. Podría ser una pista de acciones tomadas durante ese período de tiempo conocido como interesante, pero la información como los registros de eventos contaría una historia más completa.
3. Hay muchas más posibles "descubrimientos" en esta lista. Como ejemplo, parece que se accedió a varios navegadores. Deberíamos agregar la forense de bases de datos del navegador a nuestra lista de tareas pendientes para quizás obtener más contexto sobre cómo se usaron los navegadores durante este período de tiempo.
4. En general, los artefactos de ejecución de aplicaciones a menudo nos permiten armar rápidamente una lista de tareas de aplicaciones (y sus artefactos correspondientes) para investigar más a fondo.

Program	Execution Time
Rc	=
91750D7E.Slack_8she8kybcnzg4	2020-11-14 19:45:11
\Device\HarddiskVolume3\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	2020-11-14 14:16:59
\Device\HarddiskVolume3\Program Files\Google\Chrome\Application\chrome.exe	2020-11-14 14:16:01
\Device\HarddiskVolume3\Program Files\Mozilla Firefox\firefox.exe	2020-11-14 14:14:57
\Device\HarddiskVolume3\Windows\System32\cmd.exe	2020-11-14 14:12:34
\Device\HarddiskVolume3\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE	2020-11-14 14:11:49
\Device\HarddiskVolume3\Program Files\Google\Drive File Stream\43.0.8.0\GoogleDriveFS.exe	2020-11-14 14:10:59
\Device\HarddiskVolume3\Program Files\Google\Drive\googledrivesync.exe	2020-11-14 14:07:46
\Device\HarddiskVolume3\Users\fredr\AppData\Local\Temp\~nsu.tmp\Au_.exe	2020-11-14 13:50:47
\Device\HarddiskVolume3\Windows\System32\SystemPropertiesProtection.exe	2020-11-14 13:49:44
\Device\HarddiskVolume3\Users\fredr\AppData\Local\Microsoft\OneDrive\OneDrive.exe	2020-11-14 13:01:52
\Device\HarddiskVolume3\Windows\System32\mstsc.exe	2020-11-14 05:10:44
\Device\HarddiskVolume3\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe	2020-11-14 04:49:49
\Device\HarddiskVolume3\Windows\regedit.exe	2020-11-14 04:43:36
\Device\HarddiskVolume3\Program Files\Microsoft Office\root\Office16\WINWORD.EXE	2020-11-14 04:29:57
Total rows: 52	

## UserAssist

UserAssist ha sido durante mucho tiempo un valioso artefacto de Windows para proporcionar una profunda comprensión del uso de aplicaciones. Debido a que está presente en el hive NTUSER.DAT, toda la actividad está directamente relacionada con la cuenta que posee ese NTUSER.DAT. Si bien UserAssist generalmente solo rastrea aplicaciones basadas en GUI, proporciona una gran cantidad de información de uso difícil de obtener en otros lugares.

Los datos de UserAssist se almacenan nativamente en un formato codificado (ROT-13), por lo que tenemos la suerte de contar con un complemento dentro de Registry Explorer para simplificar el análisis.

Abra la siguiente clave:

**NTUSER.DAT\Software\Microsoft\Windows\Currentversion\Explorer\UserAssist\ .**



Observemos una serie de subclaves en formato de Identificador Único Global (GUID). Cada GUID representa una forma diferente en que la ejecución de la aplicación puede ser rastreada por el sistema operativo (ya sea que algo se haya abierto mediante un acceso directo, a través del menú de inicio, a través de la interfaz "tiled" de la Aplicación Universal de Windows, etc.).

▲	UserAssist	0
▶	{9E04CAB2-CC14-11DF-BB...	1
▶	{A3D53349-6E61-4557-8F...	1
▶	{B267E3AD-A825-4A09-82...	1
▶	{BCB48336-4DDD-48FF-BB...	1
▶	{CAA59E3C-4792-41A5-99...	1
▶	{CEBFF5CD-ACE2-4F4F-91...	1
▶	{F2A1CB5A-E3CC-4A2E-AF...	1
▶	{F4E57C4B-2036-45F0-A9...	1
▶	{FA99DFC7-6AC2-453A-A5...	1

Los dos GUID más comúnmente utilizados en UserAssist son:

- **CEBFF5CD-ACE2-4F4F-9178-9926F41749EA** -> Ejecución de Archivos Ejecutables

- **F4E57C4B-2036-45F0-A9AB-443BCFE33D9F** -> Ejecución de Archivos de Acceso Directo

1. Comenzemos con el GUID que comienza con F4E57 y hagamos clic en la subclave llamada "Count" para activar el complemento de Registry Explorer.



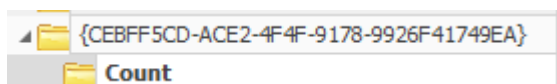
2. Ordena la salida por Nombre del Programa. ¿Qué elementos están anclados en la barra de tareas del usuario? (Pista: Busca {User Pinned}.)

1. **File Explorer**
2. **Google Chrome**
3. **Microsoft Edge**
4. **Outlook**

Saber qué aplicaciones fueron ancladas por un usuario nos da una mejor idea del comportamiento del usuario y dónde deberíamos buscar artefactos forenses adicionales.

{User Pinned}\TaskBar\File Explorer.Ink	14
{User Pinned}\TaskBar\Google Chrome.Ink	4
{User Pinned}\TaskBar\Microsoft Edge.Ink	1
{User Pinned}\TaskBar\Outlook.Ink	3

Ahora pasamos al GUID de UserAssist que comienza con **CEBFF** y haz clic en su subclave llamada "Count" para activar el complemento de Registry Explorer.



Ordena la salida por "Last Executed" y registra las aplicaciones interesantes que ocurrieron el 14 de noviembre de 2020.

Una vez más, no hay respuestas correctas o incorrectas para esta pregunta. ¡Pero elementos como DropboxUninstaller, Outlook, RemoteDesktop y regedit parecen muy interesantes!

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
Microsoft.Office.OUTLOOK.EXE. 15	4	17	0d, 0h, 10m, 58s	2020-11-14 14:09:15
{ProgramFilesX86}\Dropbox\Client\DropboxUninstaller.exe	1	0	0d, 0h, 00m, 00s	2020-11-14 13:50:02
windows.immersivecontrolpanel_cw5n1h2bxeye\microsoft.windows.immersivecontrolpanel	1	18	0d, 0h, 05m, 24s	2020-11-14 13:49:51
Microsoft.Windows.Photos_8wekyb3d8bbwe!App	15	6	0d, 0h, 02m, 29s	2020-11-14 13:04:31
{System}\cmd.exe	1	15	0d, 0h, 06m, 42s	2020-11-14 12:43:01
Chrome	4	13	0d, 0h, 05m, 00s	2020-11-14 12:34:21
Microsoft.Windows.RemoteDesktop	2	3	0d, 0h, 09m, 20s	2020-11-14 05:05:33
{ProgramFilesX86}\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe	6	5	0d, 0h, 01m, 33s	2020-11-14 04:49:43
308046B0AF4A39CB	1	8	0d, 0h, 01m, 00s	2020-11-14 04:47:10
{Windows}\regedit.exe	1	2	0d, 0h, 03m, 39s	2020-11-14 04:39:15
Microsoft.ZuneVideo_8wekyb3d8bbwe!Microsoft.ZuneVideo	2	1	0d, 0h, 00m, 03s	2020-11-14 04:36:56
Microsoft.Office.WINWORD.EXE. 15	14	16	0d, 0h, 02m, 56s	2020-11-14 04:29:49
Microsoft.Office.EXCEL.EXE. 15	5	7	0d, 0h, 00m, 55s	2020-11-14 04:28:05
Microsoft.Office.POWERPNT.EXE. 15	3	4	0d, 0h, 03m, 15s	2020-11-14 04:23:04
Microsoft.XboxGamingOverlay_8wekyb3d8bbwe!App	9	0	0d, 0h, 00m, 00s	2020-11-13 22:09:17

Ordena la salida por **Focus Count**. Este valor representa el número de veces que la aplicación fue la ventana principal para el usuario. Los elementos con un conteo de enfoque más alto a menudo representan aplicaciones más comúnmente utilizadas. ¿Qué aplicación de usuario tiene el conteo de enfoque más alto?

Program Name	Run Counter	Focus Count	Foc
UEME_CTLSESSION	85	390	0d,
Microsoft.Windows.Explorer	15	114	0d,
Chrome.UserData.Profile1	0	28	0d,
Microsoft.Windows.Common-UI	1	20	0d,
windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel	1	18	0d,
Microsoft.Office.OUTLOOK.EXE.15	4	17	0d,
Microsoft.Office.WINWORD.EXE.15	14	16	0d,

Ahora vamos a profundizar en una de las entradas. Examinemos detenidamente la entrada {Windows}\regedit.exe y responde a las siguientes preguntas:

**¿Número de ejecuciones?** Regedit.exe se ejecutó 1 vez.

**¿Última hora de ejecución?** 2020-11-14 04:39:15

**¿Cuántas veces estuvo en foco? Y ¿Cuál fue el tiempo total de enfoque?**

Estuvo en primer plano (en foco) del usuario 2 veces, durante un total de 3 minutos y 39 segundos.

{Windows}\regedit.exe	1	2	0d, 0h, 03m, 39s	2020-11-14 04:39:15
-----------------------	---	---	------------------	---------------------

Ahora tenemos información muy detallada sobre la ejecución de regedit.exe. Si creemos que regedit pudo haber sido utilizado para modificar el registro, podemos utilizar esta información para ver qué se escribió "últimamente" alrededor de este período de tiempo.

Usa Ctrl-F (o Tools -> Find) para abrir el diálogo de búsqueda de Registry Explorer. Bajo Marca de tiempo de última escritura, selecciona Entre y utiliza 2020-11-14 04:39:00 y 2020-11-14 04:45:00 como el período de tiempo a buscar (la última hora de ejecución más algún tiempo de enfoque - no es una ciencia exacta, pero es un buen punto de partida). Haz clic en Buscar.

Last write timestamp

Earliest (UTC) 2020-11-14 04:39:00

Latest (UTC) 2020-11-14 04:45:00

☐ Before ☒ Between ☐ After

Search

NOTE: Unassociated deleted records are not searched in this version

Last write timestamp

Earliest (UTC) 2020-11-14 04:39:00

Latest (UTC) 2020-11-14 04:45:00

☐ Before ☒ Between ☐ After

Search

NOTE: Unassociated deleted records are not searched in this version

How in the Results grid to select the search hit in the main window)

Last Write Time	Key Path
=	REG
2020-11-14 04:43:36	SOFTWARE\Microsoft\Windows\CurrentVersion\Applets
2020-11-14 04:43:36	SOFTWARE\Microsoft\Windows\CurrentVersion\Applets\Regedit
2020-11-14 04:43:37	SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths

¿Has notado que la última vez que se escribió en **SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Typed Paths** está dentro de esta ventana de tiempo? ¿Quizás fue manipulado de alguna manera?

Haz doble clic en el resultado de

**SOFTWARE\Microsoft\Windows\CurrentVersion\Applets\Regedit.**

Esto debería llevarte a esa clave en RegistryExplorer. ¿A qué ubicación del registro hace referencia el valor LastKey?

El valor LastKey para

SOFTWARE\Microsoft\Windows\CurrentVersion\Applets\Regedit indica que Regedit fue utilizado por última vez para interrogar la clave OpenSavePidlMRU en busca de extensiones "PNG". Si bien esto no prueba ninguna manipulación, nos da una idea de que tal vez Regedit se utilizó para acceder a esta clave (además de la clave TypedPaths). También podríamos buscar claves eliminadas en estas ubicaciones, pero lamentablemente no hay ninguna en nuestra evidencia.

Type viewer	Slack viewer   Binary viewer
Value name	LastKey
Value type	RegSz
Value	Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\PNG

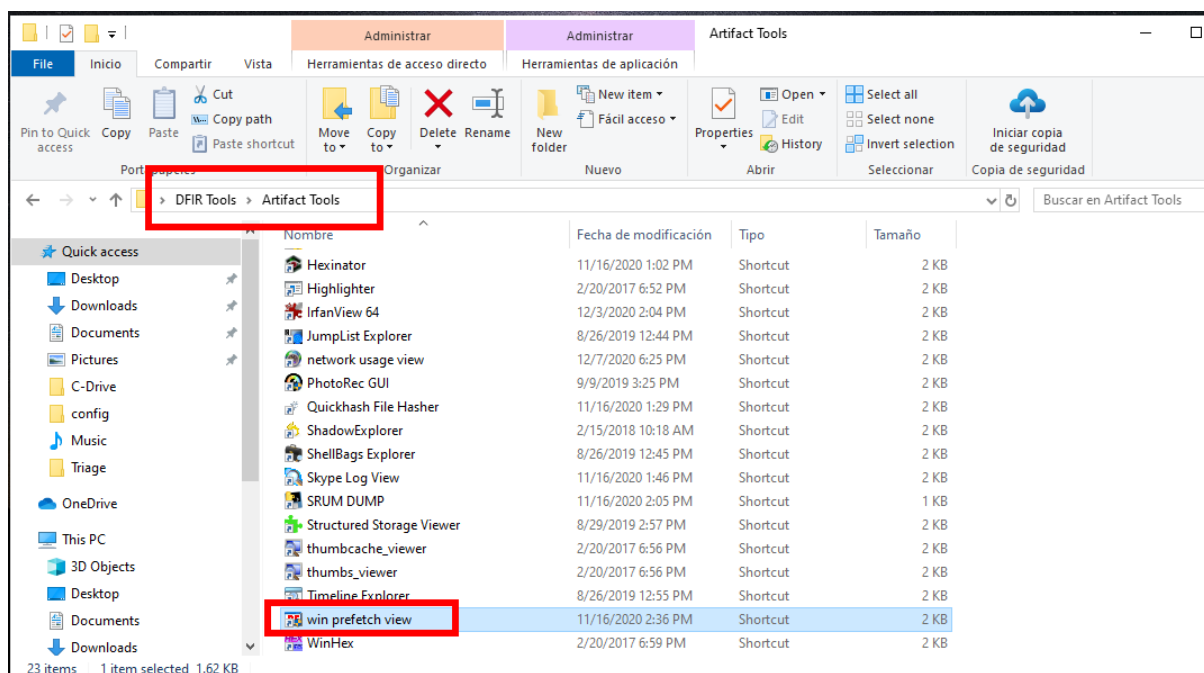
Esta técnica de buscar periodos de tiempo muy específicos dentro del registro es muy poderosa y a veces puede ayudar a responder preguntas interesantes.

## Investigating Prefetch

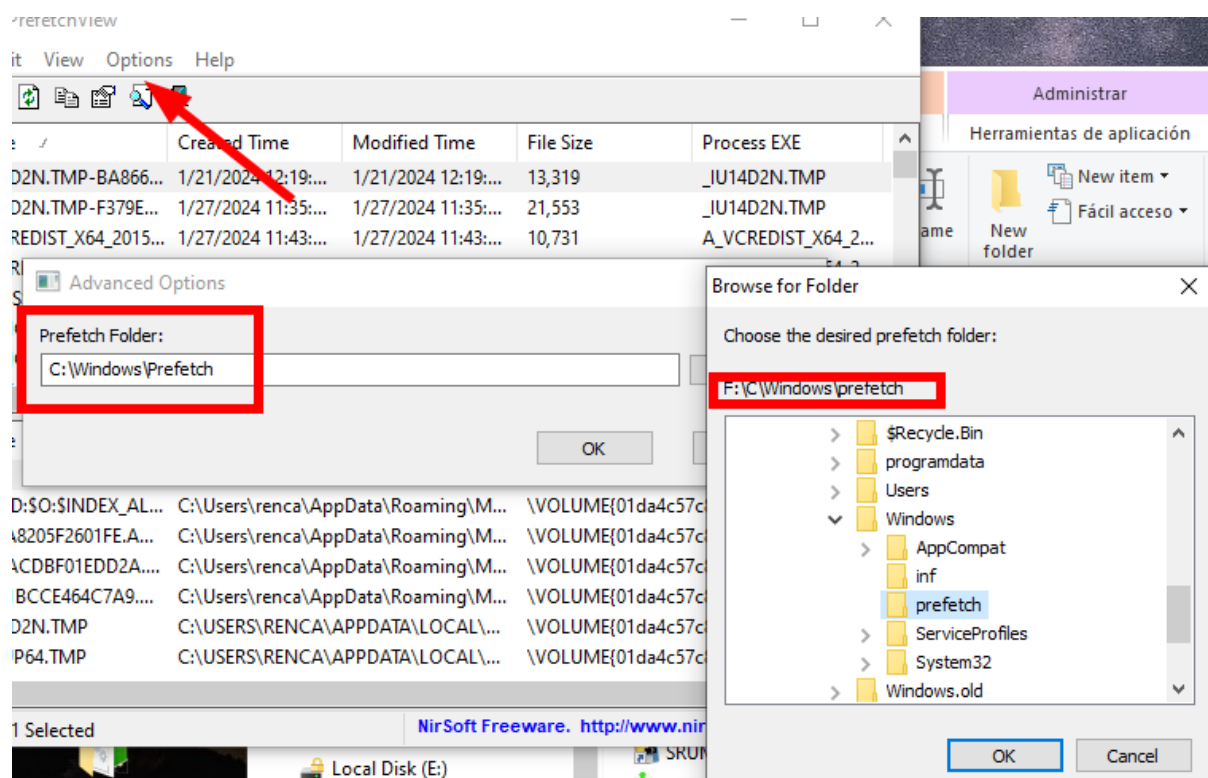
Ahora nos alejamos del registro de Windows hacia la sorprendentemente útil carpeta Prefetch. Prefetch sigue las aplicaciones ejecutadas tanto desde la interfaz gráfica como desde la línea de comandos, a menudo siendo aún más completo que otros artefactos de ejecución de aplicaciones (y ofreciendo una ventaja contra los atacantes que utilizan la línea de comandos en un intento de dejar menos artefactos).

En el desktop tenemos DFIR TOOLS y dentro de la carpeta Artifact Tools





Win Prefetch View se abre por defecto con el Prefetch del sistema en vivo, lo cual no es interesante para nosotros (pero a veces es útil cuando se practica o se realizan pruebas). Selecciona Opciones -> Opciones avanzadas y luego navega hasta la carpeta Prefetch de nuestra imagen de triaje montada: F:\C\Windows\Prefetch. Haz clic en Aceptar.



Realiza una revisión superficial de los archivos prefetch disponibles y luego encuentra BITLOCKERWIZARD.EXE-BC98F555.pf. Responde a las siguientes preguntas:

¿Número de ejecuciones? **3 veces**

¿Última hora de ejecución? **Ultima vez ejecutado 11/10/2020 14:21:56 UTC**

BACKGROUNDTRANSFERHOST.EXE-4ECE3B25.pf	4	11/14/2020 3:03:33 PM, 11/14/2020 3:03:33 PM, 11/14/2020 3:03:33 PM
BDEUI.SRV.EXE-7BC33651.pf	1	11/15/2020 10:43:35 PM
RDFUNLOCK.EXE-A677ADE8.pf	3	11/13/2020 11:45:04 PM, 11/10/2020 10:11:48 AM, 11/10/2020 8:53:13 AM
<b>BITLOCKERWIZARD.EXE-BC98F555.pf</b>	<b>3</b>	<b>11/10/2020 10:21:56 AM, 11/10/2020 8:53:13 AM, 11/10/2020 8:53:13 AM</b>
CHROME.EXE-AED7BA3C.pf	4	11/14/2020 8:34:21 AM, 11/14/2020 1:10:53 AM, 11/14/2020 1:10:53 AM, 11/14/2020 1:10:53 AM

Recuerdas una de las clave de recuperación de Bitlocker presente en la **clave RecentDocs** de **NTUSER.DAT**. Si revisamos la salida a continuación y observamos cómo estos dos elementos encajan temporalmente. Ahora tenemos evidencia no solo de que se abrió un archivo de clave, sino también de que probablemente se utilizó con la aplicación Bitlocker.

Extension	Value...	Target Name	Lnk Name	Mru ...	Opened	Extension Last Opened
RecentDocs	33	Key	Key.lnk	77		
RecentDocs	25	BitLocker Recovery Key 1694D560-A615-4ABB-B721-E7 C3E884F8BD.TXT	BitLocker Recovery Key 1694D560-A615-4ABB-B721-E7 7C3E884F8BD.lnk	78		2020-11-10 14:23:01
RecentDocs	91	Google Drive File Stream (G:)	Google Drive File Stream (G).lnk	79		

Encuentra TSTHEME.EXE-01D23267.pf en tu herramienta WinPrefetchView y perfila su ejecución. TSTHEME es una aplicación interesante ya que se ejecuta en el sistema durante las sesiones de protocolo de escritorio remoto (RDP) entrantes. Es un buen indicador de RDP entrante a una computadora.

¿Numero de ejecuciones? 4 veces, todas el 11/14/2020 :

11/14/2020 14:17:14, 11/14/2020 12:52:03, 11/14/2020 12:51:45, 11/14/2020 05:15:53 UTC

TRUSTEDINSTALLER.EXE-766EFF52.pf	86	11/15/2020 10:37:35 PM, 11/15/2020 10:37:35 PM, 11/15/2020 10:37:35 PM, 11/15/2020 10:37:35 PM
<b>TSTHEME.EXE-01D23267.pf</b>	<b>4</b>	<b>11/14/2020 10:17:14 AM, 11/14/2020 12:52:03 PM, 11/14/2020 12:51:45 PM, 11/14/2020 05:15:53 AM</b>
UPDATER.EXE-88336796.pf	1	11/14/2020 12:47:15 AM

Encuentra MSTSC.EXE-2A83B7D7.pf en tu herramienta WinPrefetchView y perfila su ejecución. MSTSC.exe se utiliza para establecer conexiones salientes de RDP desde un sistema

(básicamente lo contrario de TSTHEME.exe). Perfila el uso de MSTSC.exe en este sistema:

**¿Número de ejecuciones?** Dos ejecuciones, ambas el 11/14/2020  
: 11/14/2020 05:05:33, 11/14/2020 05:00:37 UTC

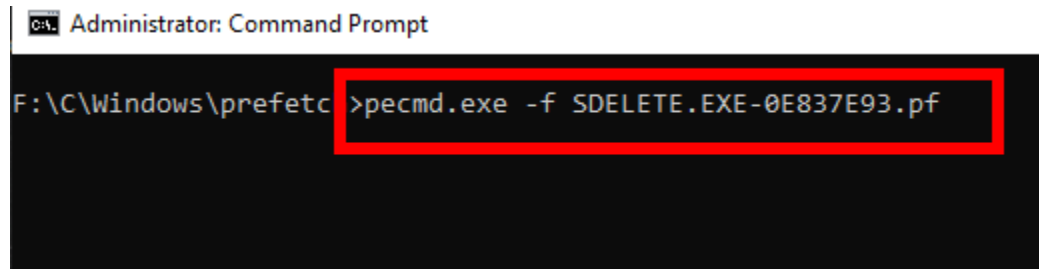
MSIEXEC.EXE-8FFB1633.pf	4	11/14/2020 10:19:43 AM, 11/14/2020 10:18:38 AM, 11/14/2020 10:18:32 AM, 11/14/2020 10:18:27 AM
MSIEXEC.EXE-8BDFC8F7.pf	2	11/14/2020 10:18:11 AM, 11/14/2020 10:18:06 AM
MSTSC.EXE-2A83B7D7.pf	2	11/14/2020 1:05:33 AM, 11/14/2020 1:00:37 AM
NETSH.EXE-8174DA63.pf	1	11/14/2020 9:50:18 AM
...	...	...

Estos son hallazgos muy interesantes durante un momento de interés para nuestra investigación.

## Prefetch Parsing with PECmd

Ahora practicaremos con la herramienta de análisis de prefetch PECmd de Eric Zimmerman. Esta es una herramienta basada en línea de comandos que permite el análisis rápido y exhaustivo de grandes cantidades de archivos Prefetch.

Abre un Símbolo del sistema de administrador encontrando el icono en el lado izquierdo de tu escritorio.



```
Administrator: Command Prompt
F:\C\Windows\prefetc >pecmd.exe -f SDELETE.EXE-0E837E93.pf
```

Revisa la salida de PECmd para SDELETE.EXE-0E837E93 y responde las siguientes preguntas.

**¿Número de ejecuciones?**

**¿Cuál es la fecha de todas las ejecuciones?**

**¿Ves alguna información en la salida que pueda indicar quién ejecutó la herramienta y para qué se usó para borrar?**

- SDELETE se ejecutó cinco veces en este sistema.
- Todas sus ejecuciones tuvieron lugar el 2020-11-14.
- La sección de Archivos Referenciados muestra una referencia a SDELETE.EXE en la carpeta \USERS\FREDR\DOWNLOADS.
- La sección de Archivos Referenciados también muestra varios archivos de usuario "modificados" por la aplicación dentro de diez segundos de ejecución (para una herramienta como sdelete, esto probablemente significa que esos archivos fueron borrados):

\USERS\FREDR\ONEDRIVE\EARTHFORCE SA-26 THUNDERBOLT  
STAR FURY.DOCX

\USERS\FREDR\ONEDRIVE\EARTH\_SA-26\_THUNDERBOLT.JPG

\USERS\FREDR\ONEDRIVE\ADAMANTIUM-BACKGROUND.DOCX

\USERS\FREDR\ONEDRIVE\BUSINESS\_PLAN\_MAIL\_ORDER\_PHARMACY2.DOC  
X

\USERS\FREDR\ONEDRIVE\BUSINESS\_PLAN\_MAIL\_ORDER\_PHARMACY.DOCX

\USERS\FREDR\ONEDRIVE\NOKIA STRATEGY.DOCX

\USERS\FREDR\ONEDRIVE\SUCCESS-TEST-PLAN-VIBRANIUM-ALLOY-  
RESULTS.DOCX

\USERS\FREDR\ONEDRIVE\THE SHIELD BACKGROUND AND ONGOING RESEARCH.DOCX

```
Keywords: temp, tmp

Processing 'SDELETE.EXE-0E837E93.pf'

Created on: 2020-11-14 13:44:54
Modified on: 2020-11-14 13:47:10
Last accessed on: 2024-02-09 16:27:25

Executable name: SDELETE.EXE
Hash: E837E93
File size (bytes): 25,940
Version: Windows 10

Run count: 5
Last run: 2020-11-14 13:47:10
Other run times: 2020-11-14 13:46:58, 2020-11-14 13:45:45, 2020-11-14 13:45:04, 2020-11-14 13:44:52

Volume information:

#0: Name: \VOLUME{01d16533fdf69e51-e0fe3288} Serial: E0FE3288 Created: 2016-02-12 01:23:34 Directories: 11

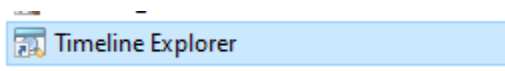
0F6D3-FD0E-4BCD-A4CD-7A580784F070
32: \VOLUME{01d16533fdf69e51-e0fe3288}\WINDOWS\SYSTEM32\CRYPTBASE.DLL
33: \VOLUME{01d16533fdf69e51-e0fe3288}\$MFT
34: \VOLUME{01d16533fdf69e51-e0fe3288}\USERS\FREDR\DOWNLOADS\SDELETE\EULA.TXT
35: \VOLUME{01d16533fdf69e51-e0fe3288}\USERS\FREDR\DOWNLOADS\SDELETE\SDELETE.EXE
36: \VOLUME{01d16533fdf69e51-e0fe3288}\USERS\FREDR\ONEDRIVE\DESKTOP\EARTHFORGE_SA-26_THUNDERBOLT_STAR_FURY.DOCX
37: \VOLUME{01d16533fdf69e51-e0fe3288}\USERS\FREDR\ONEDRIVE\DESKTOP\EARTH_SA-26_THUNDERBOLT.JPG
38: \VOLUME{01d16533fdf69e51-e0fe3288}\WINDOWS\SYSTEM32\APPHelp.DLL
39: \VOLUME{01d16533fdf69e51-e0fe3288}\WINDOWS\APPPATCH\SYSMAIN.SDB
40: \VOLUME{01d16533fdf69e51-e0fe3288}\USERS\FREDR\ONEDRIVE\ADAMANTIUM-BACKGROUND.DOCX
41: \VOLUME{01d16533fdf69e51-e0fe3288}\USERS\FREDR\ONEDRIVE\BUSINESS_PLAN_MAIL_ORDER_PHARMACY2.DOCX
42: \VOLUME{01d16533fdf69e51-e0fe3288}\USERS\FREDR\ONEDRIVE\BUSINESS_PLAN_MAIL_ORDER_PHARMACY.DOCX
43: \VOLUME{01d16533fdf69e51-e0fe3288}\USERS\FREDR\ONEDRIVE\NOKIA_STRATEGY.DOCX
44: \VOLUME{01d16533fdf69e51-e0fe3288}\USERS\FREDR\ONEDRIVE\SUCCESS-TEST-PLAN-VIBRANIUM-ALLOY-RESULTS.DOCX
45: \VOLUME{01d16533fdf69e51-e0fe3288}\USERS\FREDR\ONEDRIVE\THE SHIELD BACKGROUND AND ONGOING RESEARCH.DOCX
```

Para finalizar esta sección, ejecuta PECmd contra cada archivo Prefetch adquirido del sistema. Para ello, utilizarás la opción -d para señalar al directorio Prefetch, la opción -q para el modo silencioso (menos salida) y --csv para la ubicación de la salida en formato CSV:

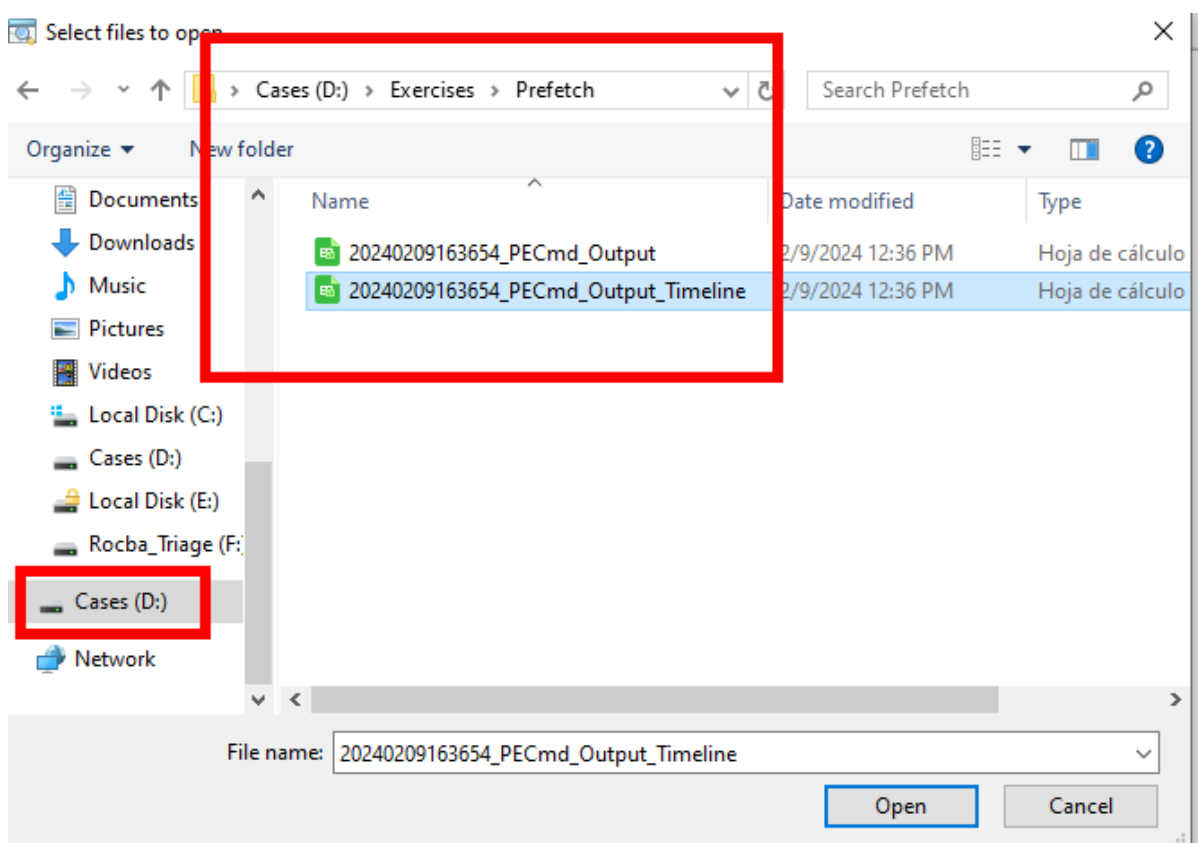
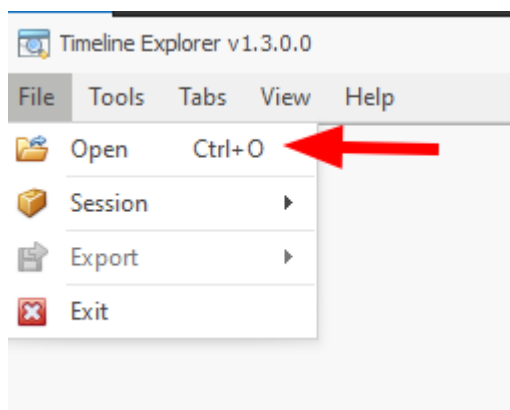
pecmd.exe -d F:\C\Windows\prefetch -q --csv D:\Exercises\Prefetch

```
CSV output will be saved to 'D:\Exercises\Prefetch\20240209163654_PECmd_Output.csv'
CSV time line output will be saved to 'D:\Exercises\Prefetch\20240209163654_PECmd_Output_Timeline.csv'
```

En la misma carpeta de WinPrefech Viewer (DFIR TOOLS --> Artifact Tools) abrimos Timeline Explorer







Ordena la salida por la columna "Run Time" y revisa la salida de la línea de tiempo de PECmd. Este archivo tiene cada ejecución registrada por Prefetch en orden cronológico. Puede ser muy útil para ver las relaciones entre diferentes herramientas y para perfilar las acciones del usuario en un sistema. Filtra la columna "Nombre del ejecutable" para sdelete.

Enumera las ubicaciones desde las que se ejecutó sdelete:

**¿Cuál es el período de tiempo total de la actividad conocida de sdelete en este sistema?**

SDELETE se ejecutó cinco veces desde Windows\System32 y dos veces desde Users\fredr\Downloads\sdelete. Todas las ejecuciones

conocidas de sdelete en este sistema ocurrieron dentro de un período de tiempo de cinco minutos:

2020-11-14 13:42:30 - 13:47:10 UTC.

Line	Tag	Run Time	Executable Name
Y =	<input type="checkbox"/>	=	sdelete
584	<input type="checkbox"/>	2020-11-14 13:42:30	\VOLUME{01d16533fdf69e51-e0fe3288}\USERS\FREDR\DOWNLOADS\SDELETE\SDELETE.EXE
583	<input type="checkbox"/>	2020-11-14 13:42:38	\VOLUME{01d16533fdf69e51-e0fe3288}\USERS\FREDR\DOWNLOADS\SDELETE\SDELETE.EXE
582	<input type="checkbox"/>	2020-11-14 13:44:52	\VOLUME{01d16533fdf69e51-e0fe3288}\WINDOWS\SYSTEM32\SDELETE.EXE
581	<input type="checkbox"/>	2020-11-14 13:45:04	\VOLUME{01d16533fdf69e51-e0fe3288}\WINDOWS\SYSTEM32\SDELETE.EXE
580	<input type="checkbox"/>	2020-11-14 13:45:45	\VOLUME{01d16533fdf69e51-e0fe3288}\WINDOWS\SYSTEM32\SDELETE.EXE
579	<input type="checkbox"/>	2020-11-14 13:46:58	\VOLUME{01d16533fdf69e51-e0fe3288}\WINDOWS\SYSTEM32\SDELETE.EXE
578	<input type="checkbox"/>	2020-11-14 13:47:10	\VOLUME{01d16533fdf69e51-e0fe3288}\WINDOWS\SYSTEM32\SDELETE.EXE

## Hasta ahora tenemos:

Encontramos evidencia de ejecución para varias aplicaciones relevantes para nuestra investigación, todas ejecutadas el día del allanamiento de la residencia del Sr. Rocba, el 14 de noviembre de 2020 (UTC):

- regedit (Editor del Registro)
- mstsc (Cliente de Servicios de Terminal de Microsoft)
- RemoteDesktop y Tstheme (Acceso Remoto)
- Google Chrome (Navegador Web)
- Microsoft Edge (Navegador Web)
- Microsoft Outlook (Cliente de Correo Electrónico)
- DropboxUninstaller (Almacenamiento en la Nube)

Basándonos en las marcas de tiempo de última escritura, parece que regedit fue utilizado para interactuar con OpenSavePidlMRU y la clave TypedPaths.

La herramienta de borrado de archivos sdelete se ejecutó un total de siete veces desde dos ubicaciones diferentes dentro de un período de cinco minutos, comenzando el 14 de noviembre de 2020 a las 13:42:30 UTC.