Practica Análisis Forense

De

Daniel Shved

OBJETIVOS:

- Resolver el CTF y explicar como se ha hecho
- Prueba de metadatos en diferentes vias
- Sacar Memoria Ram de un Windows 10

HERRAMIENTAS USADAS PARA EL TRABAJO:

- FTK Imager.
- Arsenal Image Mounter
- Time Line Explorer
- MFTECmd
- MFTExplorer
- LogFileParser
- UsnJrnl2Csv
- RegistryExplorer
- WRR64.exe
- WPR(Passcape)
- Crackstation.net
- EvtxECmd
- Hayabusa
- Chainsaw
- Hashmyfiles

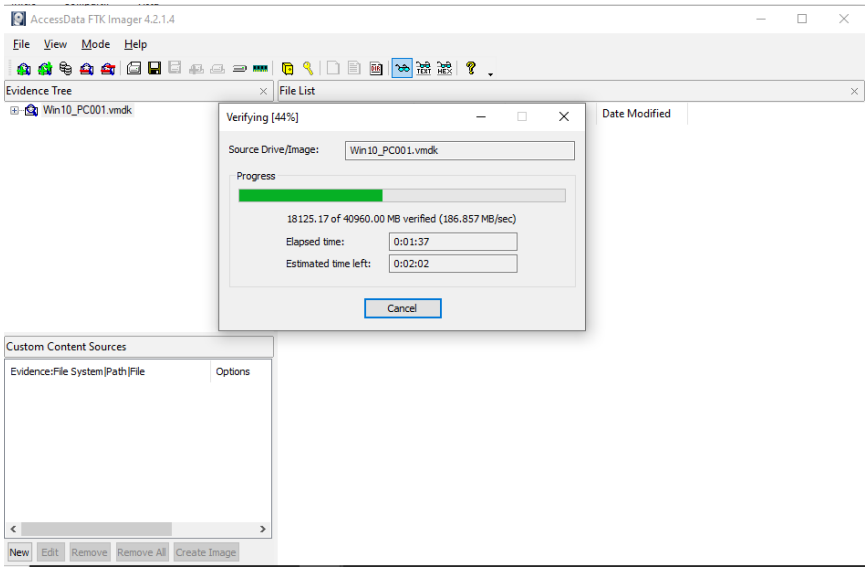
- Exiftool

- Winpmem
- Volatility

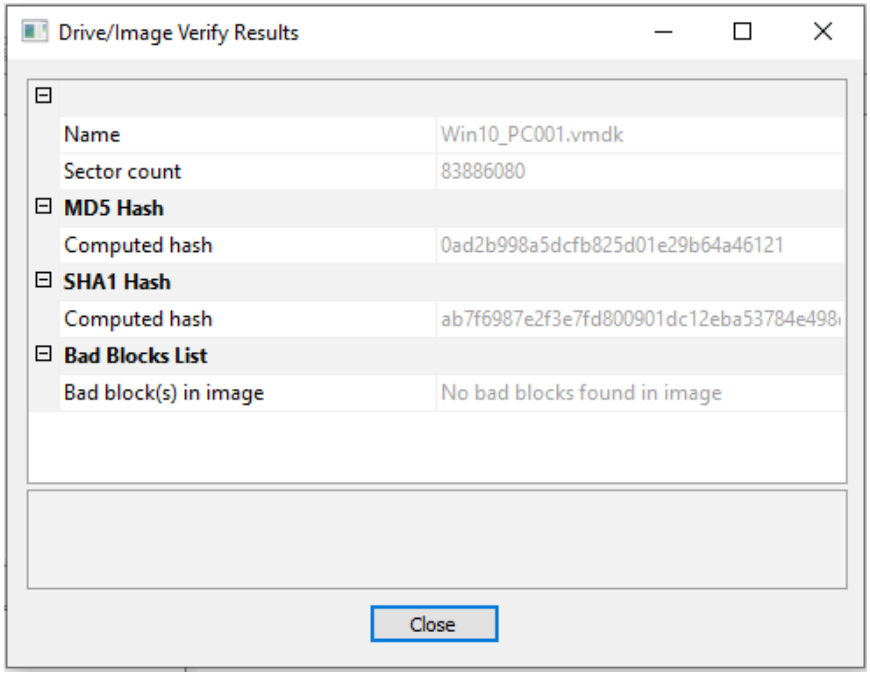
Saca el hash de la evidencia:

He sacado el hash con dos herramientas y con Certutil de Windows y no me coincide con el ctf. Expongo los resultados de todas formas:

Primero use el ftk imager.



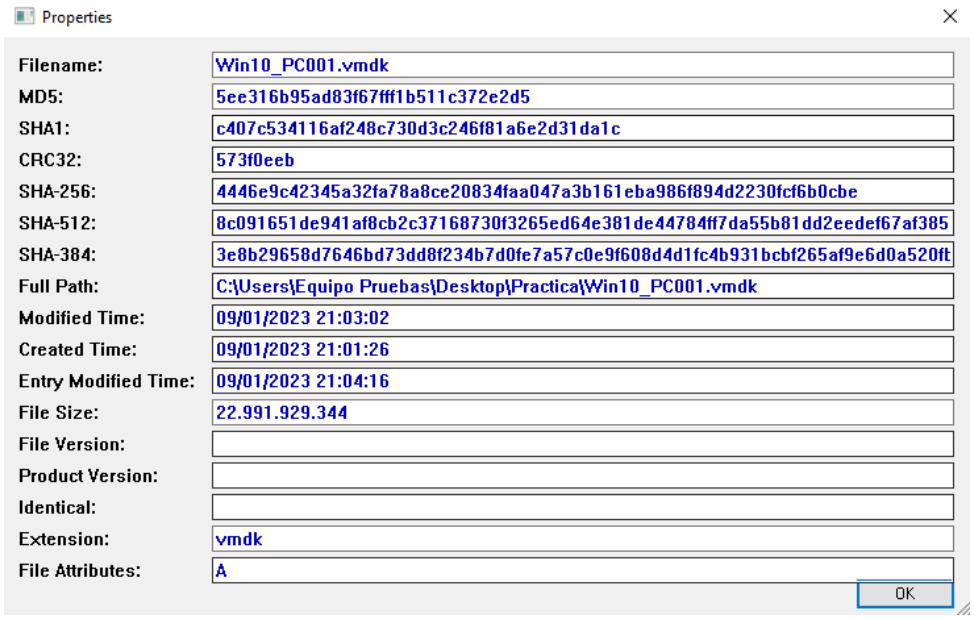
Me di cuenta de que no tiene sha-256:



Use certutil con el siguiente hash sha-256:
4446e9c42345a32fa78a8ce20834faa047a3b161eba986f894d2230fcf6b0cbe

```
PS D:\> cd Descargas
PS D:\Descargas> certUtil -hashfile .\Win10_PC001.vmdk SHA256
SHA256 hash de .\Win10_PC001.vmdk:
4446e9c42345a32fa78a8ce20834faa047a3b161eba986f894d2230fcf6b0cbe
CertUtil: -hashfile comando completado correctamente.
PS D:\Descargas>
```

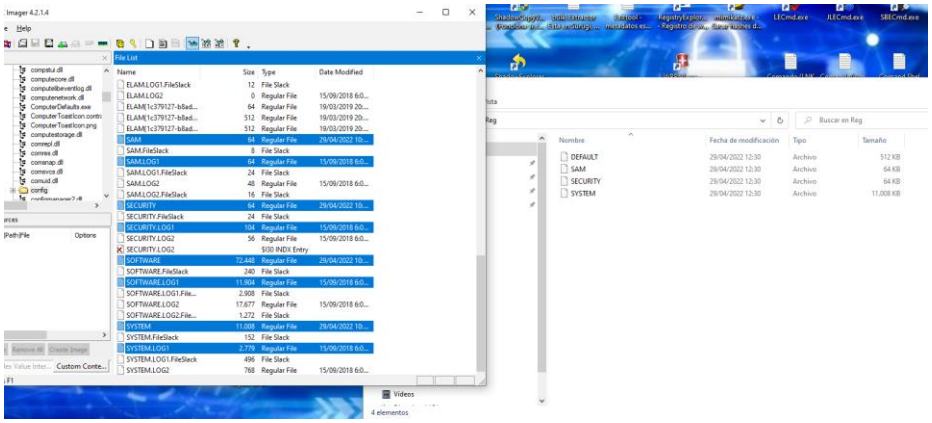
HashMyFiles:



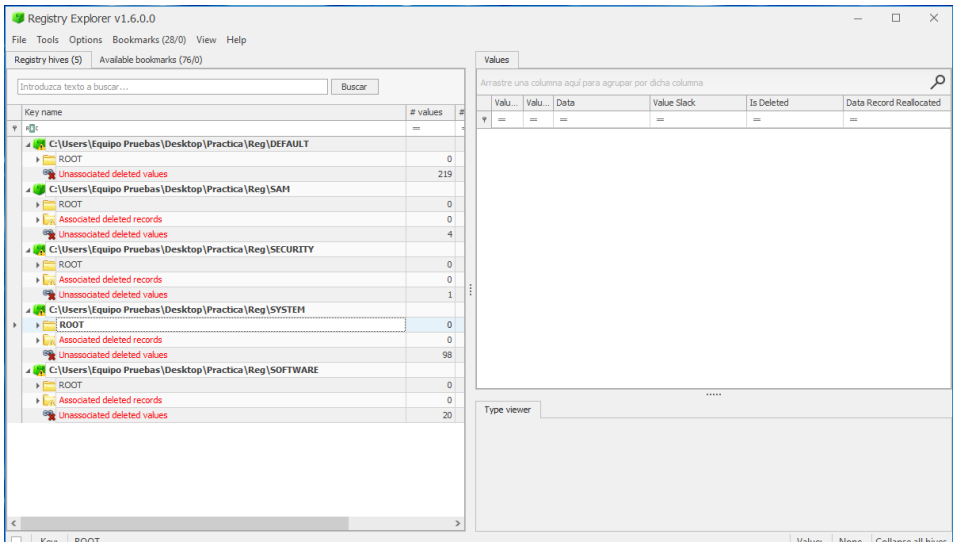
Saca el Nombre Del Equipo:

Investigue un poco y resulta que el nombre del equipo esta en el registro de Windows en la dirección: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ComputerName\ActiveComputerName => ComputerName

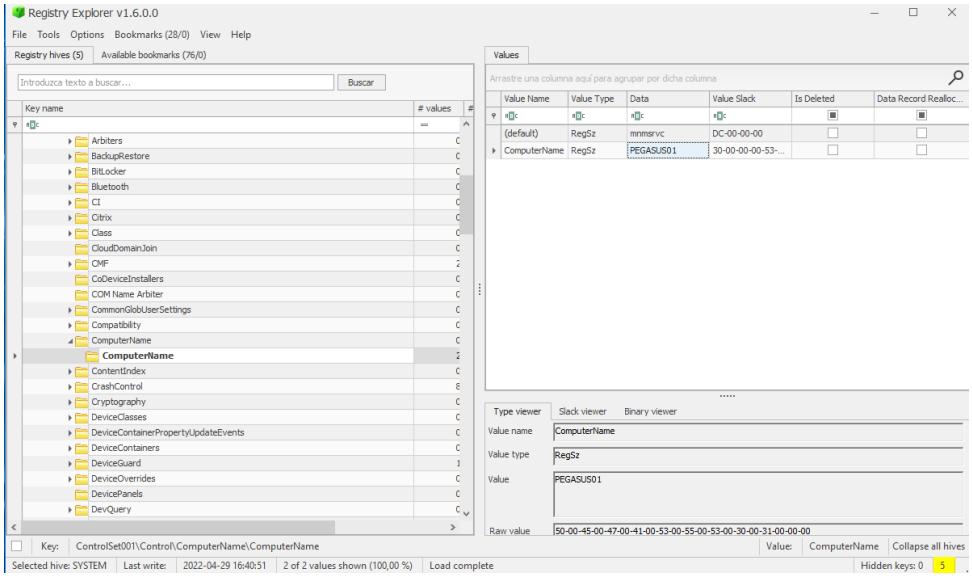
Asi que exporte con ftk imager Sam Security Log System Software y sus respectivos log1 en la dirección Root/windows/System32/Config.



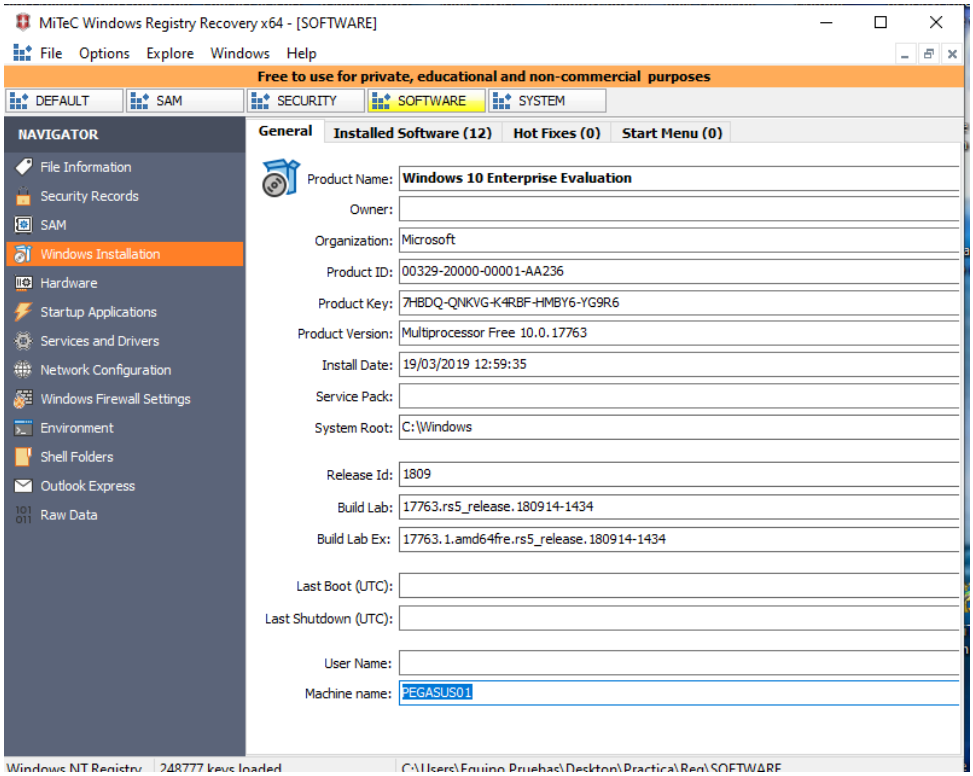
Lo cargue en Registry Explorer:



En la dirección antes mencionada encontramos que el nombre del equipo es PEGASUS01

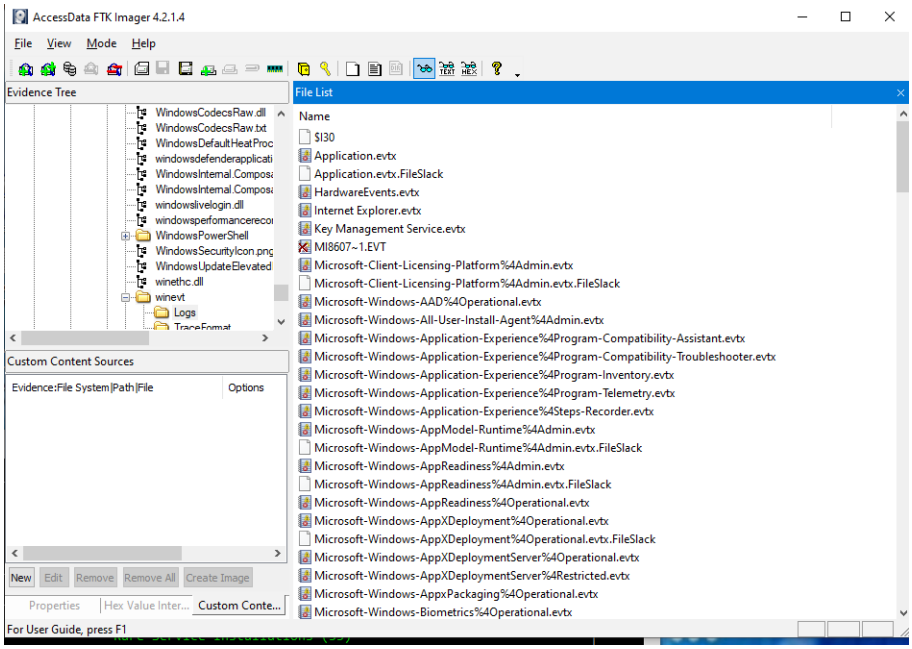


Mas tarde encontré la misma info aquí también y en muchas otras fuentes.



Encuentra la carpeta contenedora del malware:

Saque los Logs de root/windows/%System32%/winevt/Log con FTK



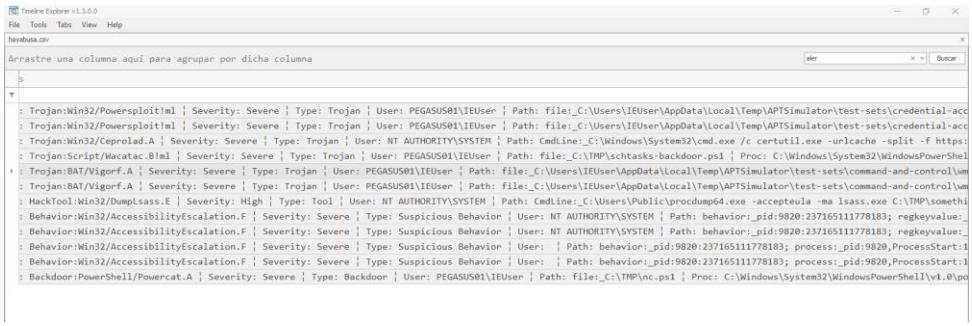
Ejecute hayabusa:

```
C:\Users\Equipo Pruebas\Desktop\Practica>"C:\Herramientas\Hayabusa\hayabusa-1.8.1-win-x64.exe" -d "C:\Users\Equipo Prueb
as\Desktop\Practica\Logs" --European-time -q -o "C:\Users\Equipo Pruebas\Desktop\Practica\hayabusa.csv" -V -U
Start time: 2023/01/09 22:36

Analyzing event files: 142
Total file size: 65.8 MB

Loading detections rules. Please wait.
```

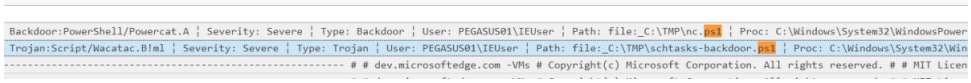
Resultados:

```
Events with hits / Total events: 742 / 48,549 (Data reduction: 47,807 events (98.47%))

Total | Unique detections: 818 | 48
Total | Unique critical detections: 11 (1.34%) | 1 (2.08%)
Total | Unique high detections: 6 (0.73%) | 4 (8.33%)
Total | Unique medium detections: 83 (10.15%) | 9 (18.75%)
Total | Unique low detections: 150 (18.34%) | 17 (35.42%)
Total | Unique informational detections: 568 (69.44%) | 17 (35.42%)

Dates with most total detections:
critical: 08-05-2022 (11), high: 08-05-2022 (3), medium: 19-03-2019 (75), low: 29-04-2022 (85), informational: 19-03-2019 (310)

Top 5 computers with most unique detections:
critical: PEGASUS01 (1)
high: PEGASUS01 (3), MSEDGEWIN10 (2)
medium: MSEDGEWIN10 (9), PEGASUS01 (2)
low: MSEDGEWIN10 (13), PEGASUS01 (6), IEUSER-F7QC4SB2 (2)
informational: MSEDGEWIN10 (17), PEGASUS01 (14), IEUSER-F7QC4SB2 (6)

Top critical alerts:                          Top high alerts:
Defender Alert (Severe) (11)                  User Added To Local Admin Grp (3)
n/a                                           Suspicious PowerShell Invocations - Specific (1)
n/a                                           PSExec Lateral Movement (1)
n/a                                           Defender Alert (High) (1)
n/a                                           n/a

Top medium alerts:                            Top low alerts:
Potentially Malicious PwSh (51)               Modified Rule in Windows Firewall with Advanced Security (68)
WMI Persistence (11)                          Rare Service Installations (35)
MSI Installation From Suspicious Locations (8) Suspicious PowerShell Get Current User (7)
Suspicious PowerShell WindowStyle Option (7)  Suspicious Process Discovery With Get-Process (6)
Windows PowerShell Web Request (2)            Service Crashed (6)

Top informational alerts:
Proc Exec (177)                               Explicit Logon (23)
WMI Provider Started (108)                    Logon (Type 2 Interactive) *Creds in memory* (21)
Bits Job Created (72)                         Logon (Type 0 System) (16)
Svc Installed (35)                            Event Log Svc Started (16)
Admin Logon (23)                              Event Log Svc Stopped (15)
```

En time line explorer vi varios malware en varias carpetas:

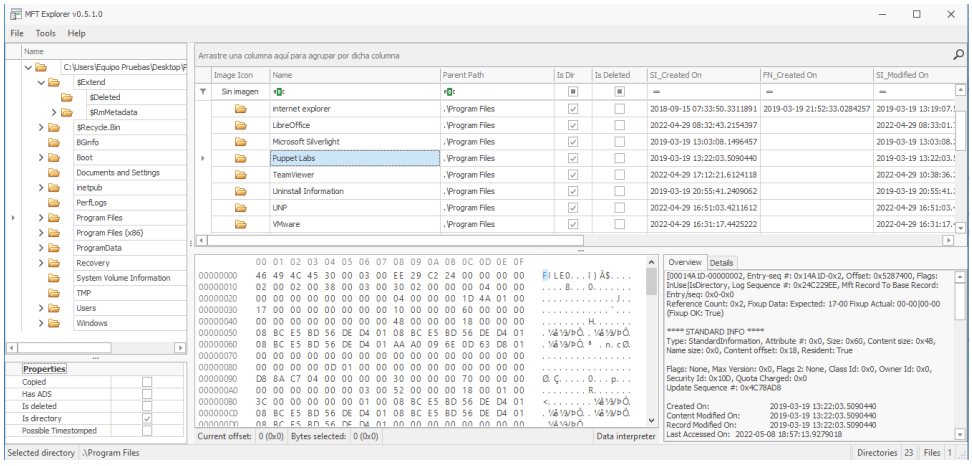


Con la pista de que es un .ps1 encontre la carpeta TMP:

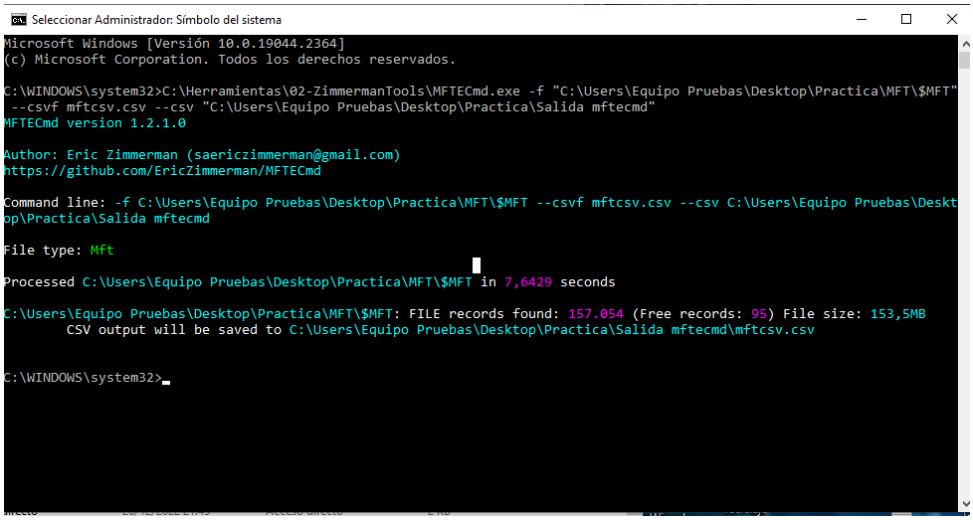


Saca el instalador del Fichero de control Remoto:

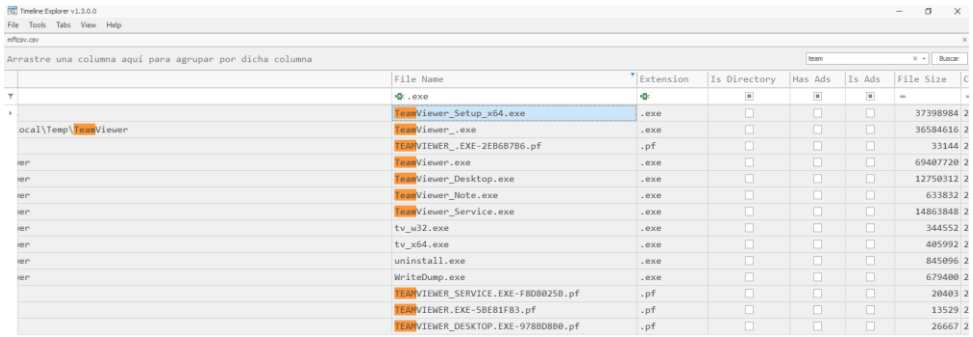
En root sacamos el artefacto $mft y desde mftexplorer sospecho de PuppetLabs y de TeamViewer



Usamos mftcmd.exe para sacar mas información:



En el output en team viewer ponemos .exe en file name y en búsquedas vamos poniendo palabras relacionadas con team viewer y puppetlabs. Vamos mirando los .exe uno a uno hasta que da positivo el setup TeamViewer_Setup_x64.exe



File Name	Extension	Is Directory	Has Ads	Is Ads	File Size
.exe	.exe				=
TeamViewer_Setup_x64.exe	.exe				37398984
TeamViewer_.exe	.exe				36584616
TEAMVIEWER_.EXE-2EB6B7B6.pf	.pf				33144
TeamViewer.exe	.exe				69407720
TeamViewer_Desktop.exe	.exe				12750312
TeamViewer_Note.exe	.exe				633832
TeamViewer_Service.exe	.exe				14863848
tv_w32.exe	.exe				344552
tv_x64.exe	.exe				405992
uninstall.exe	.exe				845096
WriteDump.exe	.exe				679400
TEAMVIEWER_SERVICE.EXE-F8D8025B.pf	.pf				20403
TEAMVIEWER.EXE-5BE81F83.pf	.pf				13529
TEAMVIEWER_DESKTOP.EXE-978BD8B0.pf	.pf				26667

Saca las fechas de ejecución del Programa de control Remoto

En la misma tabla mas adelante están las fechas de ejecución:

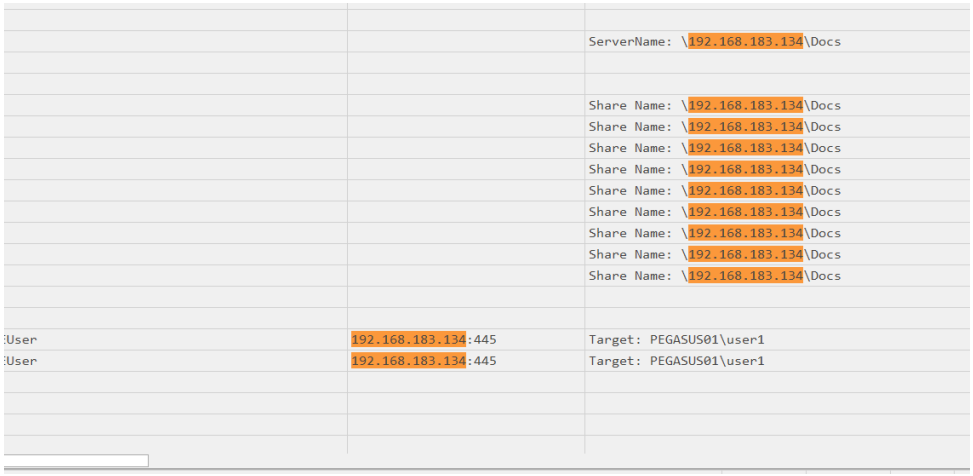
File Name	Extension	Is Directory	Has Ads	Is Ads	File Size	Created0x10
.exe	.exe				=	=
TeamViewer_Setup_x64.exe	.exe				37398984	2022-04-29 17:11:25
TeamViewer_.exe	.exe				36584616	2022-04-15 08:39:20
TEAMVIEWER_.EXE-2EB6B7B6.pf	.pf				33144	2022-04-29 17:12:22
TeamViewer.exe	.exe				69407720	2022-04-29 17:12:26
TeamViewer_Desktop.exe	.exe				12750312	2022-04-29 17:12:28
TeamViewer_Note.exe	.exe				633832	2022-04-29 17:12:28
TeamViewer_Service.exe	.exe				14863848	2022-04-29 17:12:28
tv_w32.exe	.exe				344552	2022-04-29 17:12:28
tv_x64.exe	.exe				405992	2022-04-29 17:12:28
uninstall.exe	.exe				845096	2022-04-29 17:12:28
WriteDump.exe	.exe				679400	2022-04-29 17:12:28
TEAMVIEWER_SERVICE.EXE-F8D8025B.pf	.pf				20403	2022-04-29 17:12:31
TEAMVIEWER.EXE-5BE81F83.pf	.pf				13529	2022-04-29 09:20:34
TEAMVIEWER_DESKTOP.EXE-978BD8B0.pf	.pf				26667	2022-04-29 10:09:25

Sospechamos que un atacante se ha conectado al ordenador con RDP, saca su IP:

Usando el parseado del programa evtxcmd del artefacto log, usamos el evento 1149 correspondiente a la conexión remota rdp. Probe varios eventos relacionados con conexiones remotas.

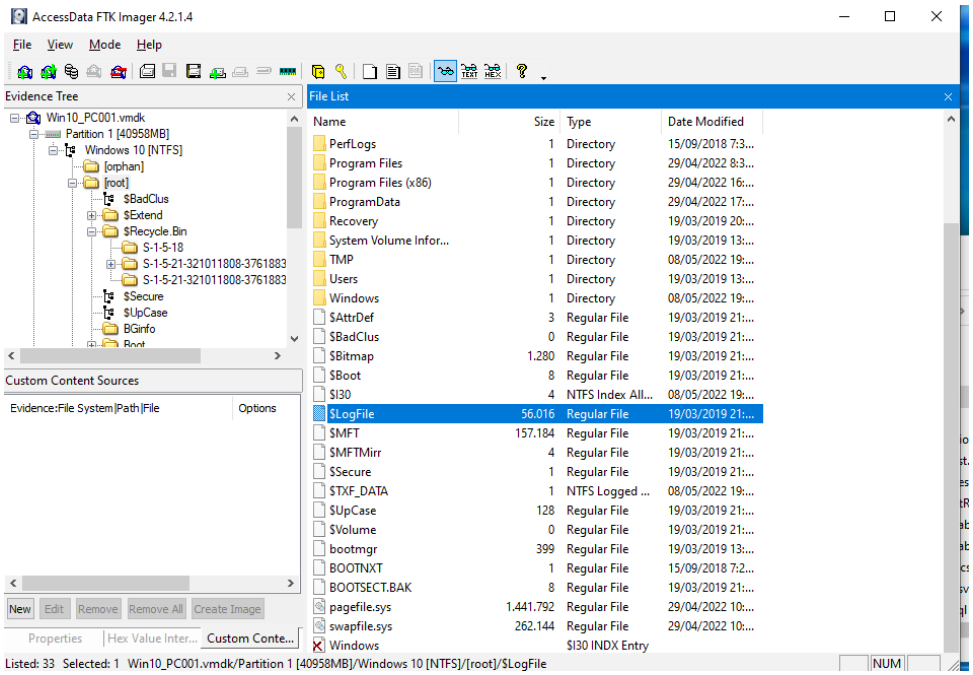
Encontramos tras ir viendo registro por registro una conexión desde la ip 192.168.183.134

Investigando un poco mas parece ser que se conecta desde dicha ip puerto 445:

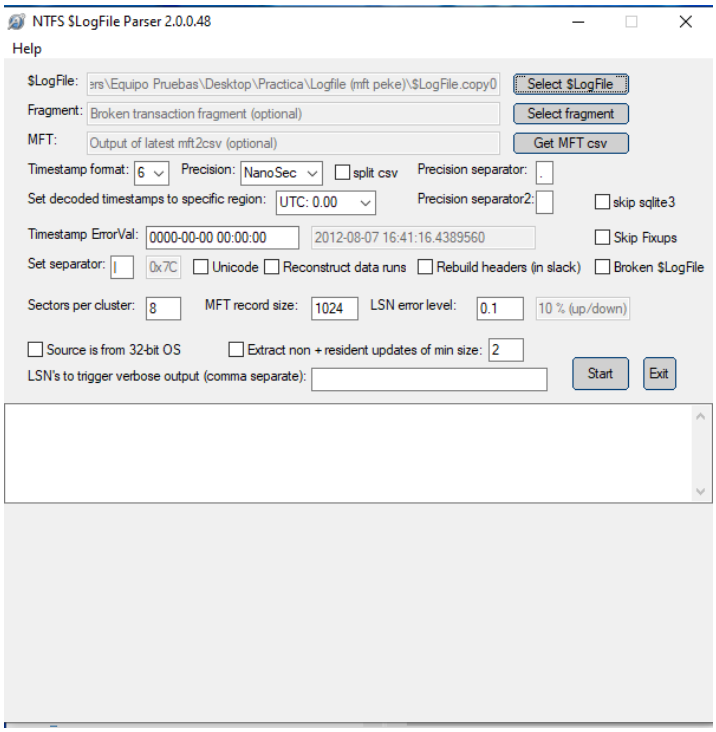


Que fichero .zip ha sido eliminado:

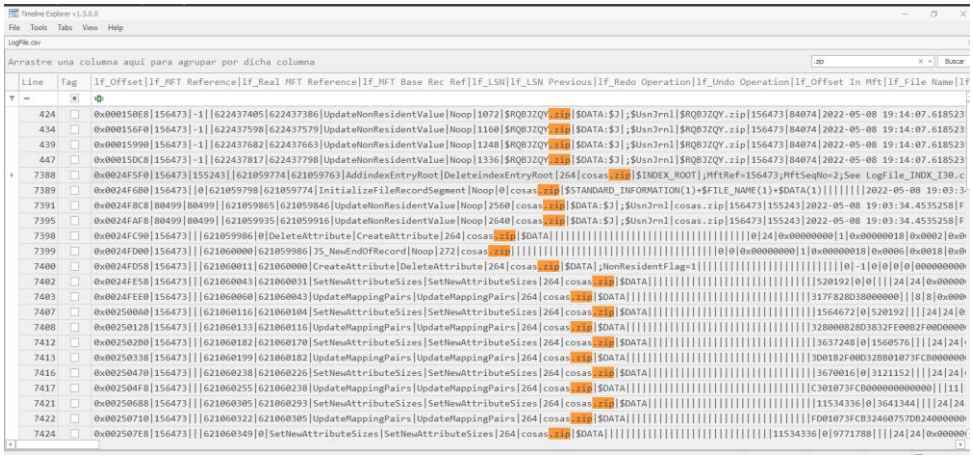
Con ftk sacamos $logfile que esta en root, junto a la $mft:



Lo parseamos con LogFileParser64

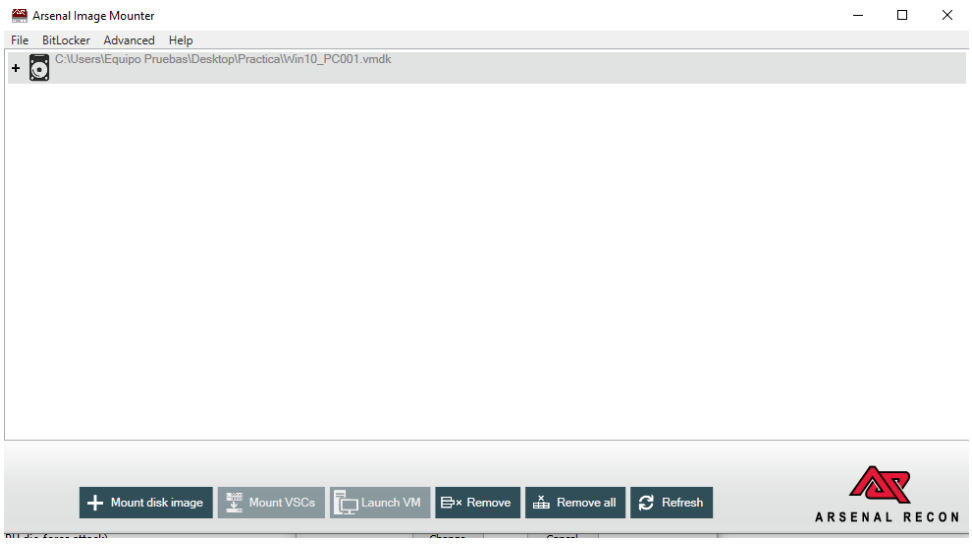


Al abrirlo buscar por .zip vemos multiples registros de que se ah borrado “cosas.zip”

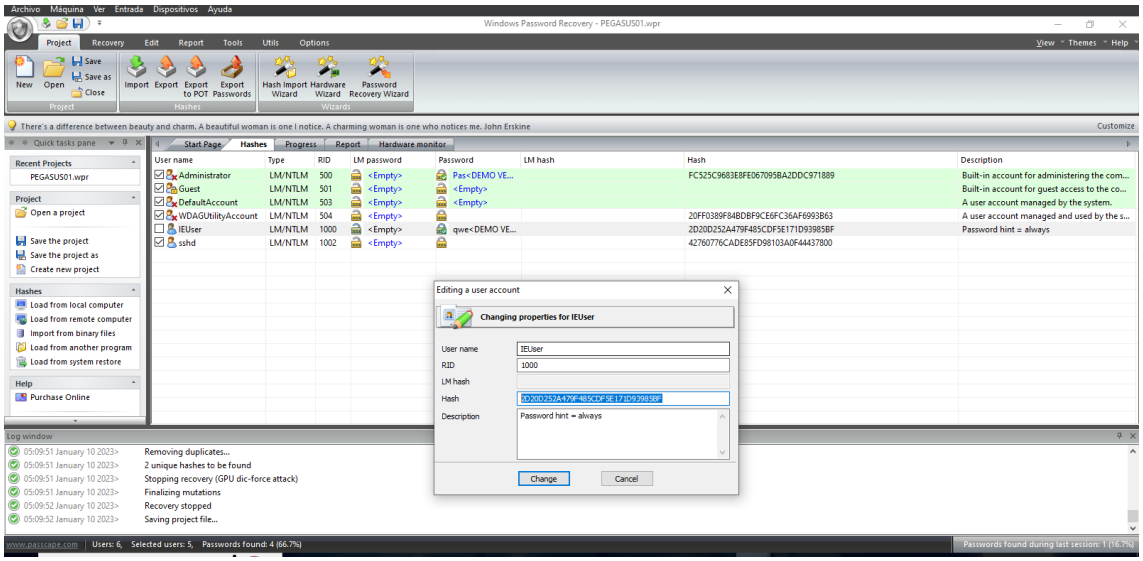


Saca la contraseña del usuario IEUSER del sistema:

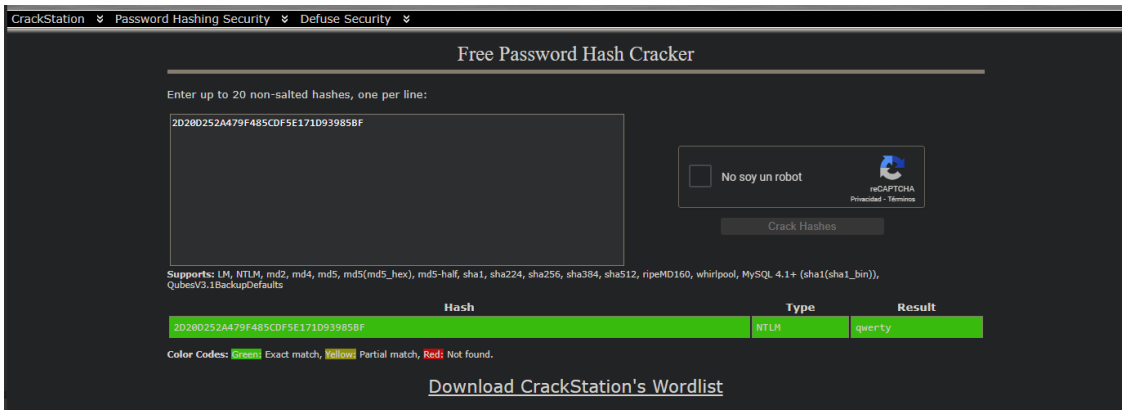
Montamos disco con arsenal en e :



Instalamos lanzamos y sacamos hashes con Windows passcape



En crackstation.net vemos que la contraseña de ieuser es qwerty



Y la contraseña del administrador es Passw0rd!

Encuentra un script malicioso de powershell:

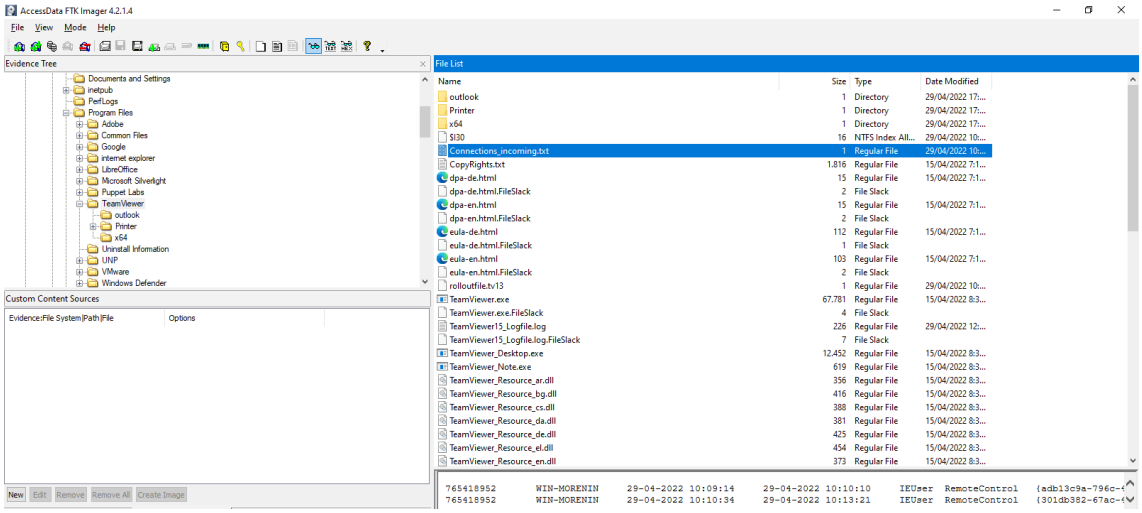
Sospeche atraves de hayabusa, erróneamente, de estos dos:

```
rity: Severe ¦ Type: Backdoor ¦ User: PEGASUS01\IEUser ¦ Path: file:_C:\TMP\nc.ps1 ¦ Proc: C:\Windows\System
: Severe ¦ Type: Trojan ¦ User: PEGASUS01\IEUser ¦ Path: file:_C:\TMP\schtasks-backdoor.ps1 ¦ Proc: C:\Windo
------------------- # # dev.microsoftedge.com -VMs # Copyright(c) Microsoft Corporation. All rights reserved.
------------------- # # dev.microsoftedge.com -VMs # Copyright(c) Microsoft Corporation. All rights reserved.
------------------- # # dev.microsoftedge.com -VMs # Copyright(c) Microsoft Corporation. All rights reserved.
------------------- # # dev.microsoftedge.com -VMs # Copyright(c) Microsoft Corporation. All rights reserved.
------------------- # # dev.microsoftedge.com -VMs # Copyright(c) Microsoft Corporation. All rights reserved.
```

La respuesta es WMBackdoor.ps1 que esta en la carpeta TMP. Se puede ver una vez extraida.

ID de TeamViewer del atacante:

Exportamos carpeta de conexiones de teamviewer atraves de ftk.

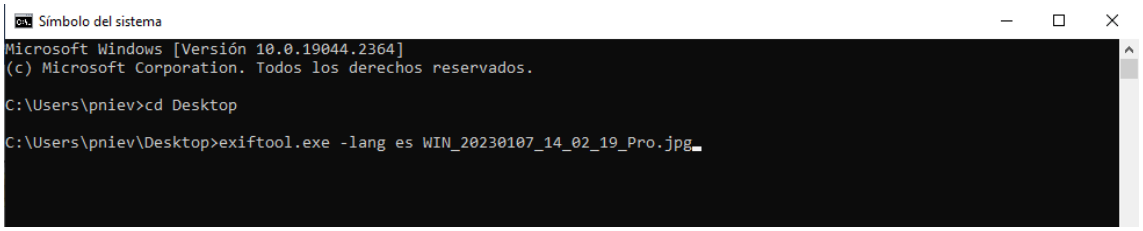


Abrimos y esta el id: 765418952

```
Archivo  Edición  Formato  Ver  Ayuda

765418952       WIN-MORENIN     29-04-2022 10:09:14     29-04-2022 10:10:10     IEUser  RemoteControl   {adb13c9a-796c-438c-af8b-2079077f0a4f}
765418952       WIN-MORENIN     29-04-2022 10:10:34     29-04-2022 10:13:21     IEUser  RemoteControl   {301db382-67ac-4b5a-9bec-d1a44aa0ad30}
```

PRUEBA METADATOS:

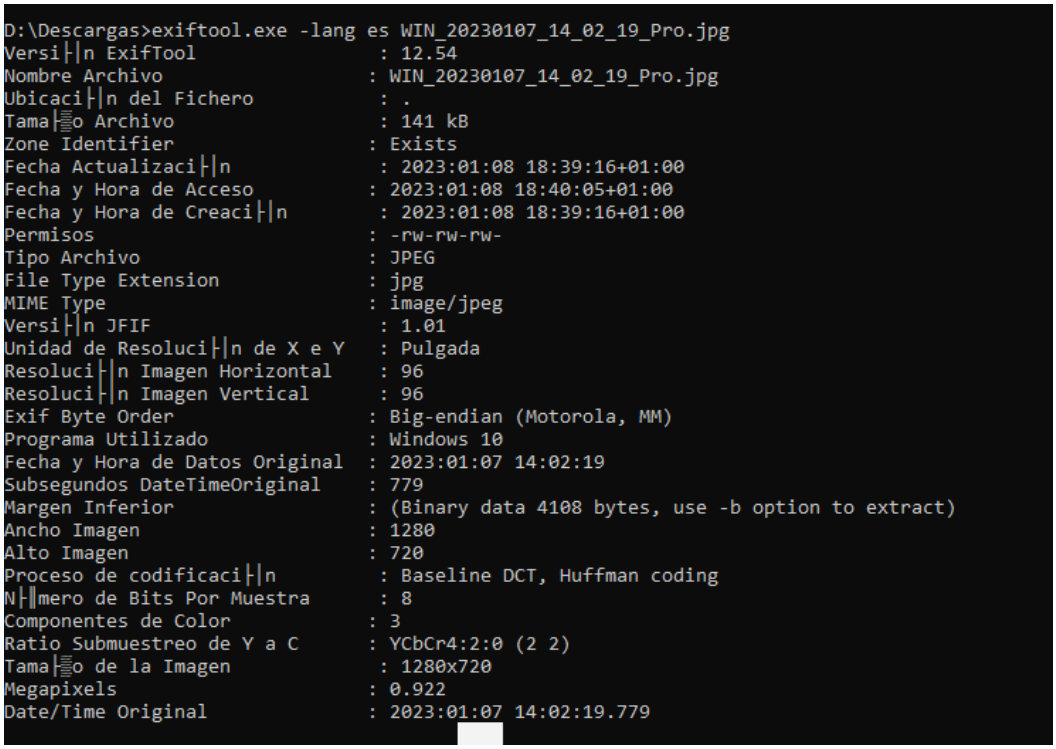
Tomamos foto desde un portátil y vemos su metadatos con exiftool



Estos son sus metadatos originales:

```
C:\Users\pniev\Desktop>exiftool.exe -lang es WIN_20230107_14_02_19_Pro.jpg
Versi├│n ExifTool                : 12.54
Nombre Archivo                  : WIN_20230107_14_02_19_Pro.jpg
Ubicaci├│n del Fichero           : .
Tama├▒o Archivo                 : 141 kB
Zone Identifier                 : Exists
Fecha Actualizaci├│n             : 2023:01:07 14:02:20+01:00
Fecha y Hora de Acceso          : 2023:01:07 14:05:45+01:00
Fecha y Hora de Creaci├│n        : 2023:01:07 14:02:20+01:00
Permisos                        : -rw-rw-rw-
Tipo Archivo                    : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Versi├│n JFIF                    : 1.01
Unidad de Resoluci├│n de X e Y   : Pulgada
Resoluci├│n Imagen Horizontal    : 96
Resoluci├│n Imagen Vertical      : 96
Exif Byte Order                 : Big-endian (Motorola, MM)
Programa Utilizado              : Windows 10
Fecha y Hora de Datos Original  : 2023:01:07 14:02:19
Subsegundos DateTimeOriginal    : 779
Margen Inferior                 : (Binary data 4108 bytes, use -b option to extract)
Ancho Imagen                    : 1280
Alto Imagen                     : 720
Proceso de codificaci├│n         : Baseline DCT, Huffman coding
N├║mero de Bits Por Muestra      : 8
Componentes de Color            : 3
Ratio Submuestreo de Y a C      : YCbCr4:2:0 (2 2)
Tama├▒o de la Imagen             : 1280x720
Megapixels                      : 0.922
Date/Time Original              : 2023:01:07 14:02:19.779

C:\Users\pniev\Desktop>
```

Al enviar la fotografía por mail y ver sus metadatos vemos que se conservan todos. Se actualiza la fecha de de actualización, fecha y hora de acceso y fecha y hora de creación por alguna razón. Por lo demás es igual. Destaca que se mantiene la "date time original"



Whatsap: se modifican la fecha de actualización aceso y creación desparece date time original y el nombre del archivo. Se reduce el tamaño, desaparece subsegundos date time original , margen inferior y fecha y hora de datos original.Desaparece Exif byte order (Motorola MM) y Programa utilizado (Windows 10). Se puede decir que pierde gran parte de los metadatos

```
D:\Descargas>exiftool.exe -lang es "WhatsApp Image 2023-01-07 at 17.15.54.jpeg"
Versi├│n ExifTool                 : 12.54
Nombre Archivo                  : WhatsApp Image 2023-01-07 at 17.15.54.jpeg
Ubicaci├│n del Fichero           : .
Tama├▒o Archivo                  : 129 kB
Zone Identifier                 : Exists
Fecha Actualizaci├│n              : 2023:01:08 18:41:51+01:00
Fecha y Hora de Acceso          : 2023:01:08 18:42:16+01:00
Fecha y Hora de Creaci├│n         : 2023:01:08 18:41:51+01:00
Permisos                        : -rw-rw-rw-
Tipo Archivo                    : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Versi├│n JFIF                    : 1.01
Unidad de Resoluci├│n de X e Y   : Pulgada
Resoluci├│n Imagen Horizontal    : 96
Resoluci├│n Imagen Vertical      : 96
Ancho Imagen                    : 1280
Alto Imagen                     : 720
Proceso de codificaci├│n         : Baseline DCT, Huffman coding
N├║mero de Bits Por Muestra      : 8
Componentes de Color            : 3
Ratio Submuestreo de Y a C      : YCbCr4:2:0 (2 2)
Tama├▒o de la Imagen             : 1280x720
Megapixels                      : 0.922
```

Telegram: es idéntico a whatsapp, se pierden gran parte de los metadatos

```
D:\Descargas>exiftool.exe -lang es photo_5893112382346084192_y.jpg
Versi├│n ExifTool                 : 12.54
Nombre Archivo                  : photo_5893112382346084192_y.jpg
Ubicaci├│n del Fichero           : .
Tama├▒o Archivo                  : 111 kB
Zone Identifier                 : Exists
Fecha Actualizaci├│n              : 2023:01:08 18:45:23+01:00
Fecha y Hora de Acceso          : 2023:01:08 18:45:42+01:00
Fecha y Hora de Creaci├│n         : 2023:01:08 18:45:23+01:00
Permisos                        : -rw-rw-rw-
Tipo Archivo                    : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Versi├│n JFIF                    : 1.01
Unidad de Resoluci├│n de X e Y   : Pulgada
Resoluci├│n Imagen Horizontal    : 96
Resoluci├│n Imagen Vertical      : 96
Ancho Imagen                    : 1280
Alto Imagen                     : 720
Proceso de codificaci├│n         : Progressive DCT, Huffman coding
N├║mero de Bits Por Muestra      : 8
Componentes de Color            : 3
Ratio Submuestreo de Y a C      : YCbCr4:2:0 (2 2)
Tama├▒o de la Imagen             : 1280x720
Megapixels                      : 0.922
```

ADQUISICION DE MEMORIA RAM

Descargamos winpmem, ejecutamos cmd en modo administrador y ejecutamos siguiente comando. De esta manera extraemos la memoria ram Para la practica use mi Windows original para echar un vistazo a los procesos de mi ram.

```
C:\>D:

D:\Descargas>winpmem_mini_x64_rc2.exe xd.mem
WinPmem64
Extracting driver to C:\Users\DAS\AppData\Local\Temp\pme872B.tmp
Driver Unloaded.
Loaded Driver C:\Users\DAS\AppData\Local\Temp\pme872B.tmp.
Deleting C:\Users\DAS\AppData\Local\Temp\pme872B.tmp
The system time is: 19:44:41
Will generate a RAW image
 - buffer_size_: 0x1000
CR3: 0x00001AD000
 4 memory ranges:
Start 0x00001000 - Length 0x0009E000
Start 0x00100000 - Length 0x64225000
Start 0x67EFF000 - Length 0x00001000
Start 0x100000000 - Length 0x38B800000
max_physical_memory_ 0x48b800000
Acquitision mode PTE Remapping
Padding from 0x00000000 to 0x00001000
pad
 - length: 0x1000

00% 0x00000000 .
copy_memory
 - start: 0x1000
 - end: 0x9f000

00% 0x00001000 .
Padding from 0x0009F000 to 0x00100000
pad
 - length: 0x61000

00% 0x0009F000 .
copy_memory
 - start: 0x100000
 - end: 0x64325000
```

```
00% 0x00100000 ..................................................
04% 0x32100000 ..................................................
08% 0x64100000 .
Padding from 0x64325000 to 0x67EFF000
pad
 - length: 0x3bda000

08% 0x64325000 ....
copy_memory
 - start: 0x67eff000
 - end: 0x67f00000

08% 0x67EFF000 .
Padding from 0x67F00000 to 0x100000000
pad
 - length: 0x98100000

08% 0x67F00000 ..................................................
08% 0x67F00000 ..................................................
08% 0x67F00000 ..................................................
08% 0x67F00000 ...
copy_memory
 - start: 0x100000000
 - end: 0x48b800000

22% 0x100000000 ..................................................
26% 0x132000000 ..................................................
30% 0x164000000 ..................................................
34% 0x196000000 ..................................................
39% 0x1C8000000 ..................................................
43% 0x1FA000000 ..................................................
47% 0x22C000000 ..................................................
52% 0x25E000000 ..................................................
56% 0x290000000 ..................................................
60% 0x2C2000000 ..................................................
64% 0x2F4000000 ..................................................
69% 0x326000000 ..................................................
73% 0x358000000 ..................................................
77% 0x38A000000 ..................................................
82% 0x3BC000000 ..................................................
86% 0x3EE000000 ..................................................
90% 0x420000000 ..................................................
95% 0x452000000 ..................................................
99% 0x484000000 ........
The system time is: 19:44:53
Driver Unloaded.
```

Instalamos Python3, lanzamos: vol.py C:\Users\Equipo Pruebas\Desktop windows.plist

Lanzamos volitility con vol.py -f "C:\Users\Equipo Pruebas\Desktop\xd.mem" windows.psscan para ver los procesos evidentes y ocultos, por curiosidad a ver si veo algo raro en mi Windows, malware o procesos ocultos:

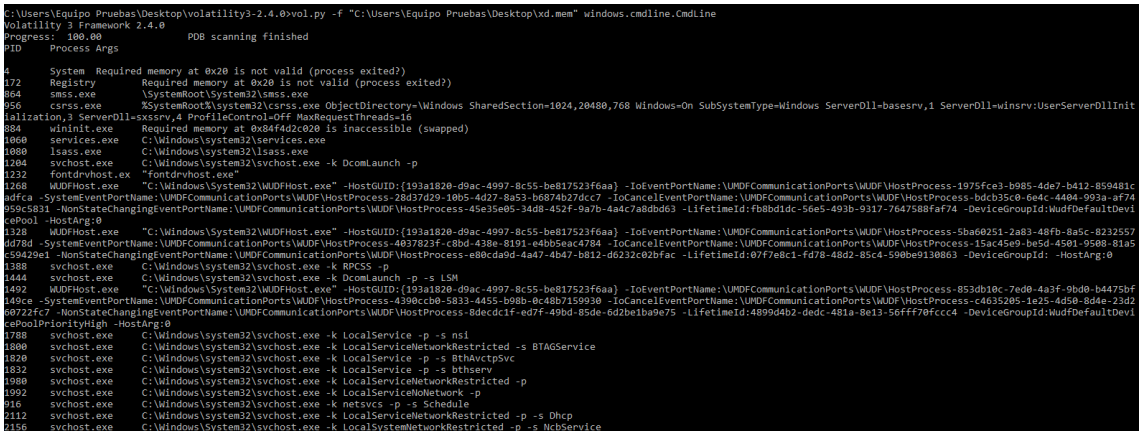
```
C:\Users\Equipo Pruebas\Desktop\volatility3-2.4.0>vol.py -f "C:\Users\Equipo Pruebas\Desktop\xd.mem" windows.psscan
Volatility 3 Framework 2.4.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0xd288846d90c0  290     -       N/A     False   2023-01-05 19:58:31.000000      N/A     Disabled
172     4       Registry        0xd2888477a040  4       -       N/A     False   2023-01-05 19:58:22.000000      N/A     Disabled
10376   1060    svchost.exe     0xd28889cd0080  0       -       2       False   2023-01-07 19:13:16.000000      2023-01-08 02:12:04.000000      Disabled
5848    17312   Spotify.exe     0xd28889f42080  16      -       3       True    2023-01-08 14:31:23.000000      N/A     Disabled
11920   916     asus_framework  0xd28889fca300  12      -       3       True    2023-01-08 14:27:50.000000      N/A     Disabled
11064   17704   chrome.exe      0xd288a3091080  0       -       2       False   2023-01-07 19:13:24.000000      2023-01-08 02:11:57.000000      Disabled
13292   5368    rundll32.exe    0xd288a3099080  0       -       2       False   2023-01-07 19:13:24.000000      2023-01-07 19:13:24.000000      Disabled
2448    916     AcPowerNotific  0xd288a30b2300  9       -       3       True    2023-01-08 14:27:50.000000      N/A     Disabled
17528   17704   chrome.exe      0xd288a30b9080  0       -       2       False   2023-01-07 19:13:25.000000      2023-01-08 02:11:57.000000      Disabled
11784   1204    ScreenClipping  0xd288a424d080  0       -       3       False   2023-01-08 17:35:57.000000      2023-01-08 17:36:00.000000      Disabled
1968    1204    RuntimeBroker.  0xd288a4275080  0       -       3       False   2023-01-08 17:27:25.000000      2023-01-08 17:28:07.000000      Disabled
13980   1060    svchost.exe     0xd288a42b5080  3       -       3       False   2023-01-08 17:28:50.000000      N/A     Disabled
12972   18032   chrome.exe      0xd288a42c9080  17      -       3       False   2023-01-08 18:30:57.000000      N/A     Disabled
4092    1204    smartscreen.ex  0xd288a4306080  0       -       3       False   2023-01-08 17:27:40.000000      2023-01-08 17:33:05.000000      Disabled
13872   18032   chrome.exe      0xd288a4331080  19      -       3       False   2023-01-08 18:41:51.000000      N/A     Disabled
18852   18032   chrome.exe      0xd288a4364080  17      -       3       False   2023-01-08 17:20:33.000000      N/A     Disabled
18896   5808    ONENOTEM.EXE    0xd288a4380080  2       -       3       False   2023-01-08 17:28:16.000000      N/A     Disabled
18692   18032   chrome.exe      0xd288a43a8080  21      -       3       False   2023-01-08 17:24:25.000000      N/A     Disabled
14720   1204    RuntimeBroker.  0xd288a4520080  6       -       3       False   2023-01-08 14:27:53.000000      N/A     Disabled
4720    1060    SgrmBroker.exe  0xd288a4b74080  6       -       0       False   2023-01-05 20:00:37.000000      N/A     Disabled
10964   1060    svchost.exe     0xd288a4bf0080  3       -       0       False   2023-01-05 20:00:37.000000      N/A     Disabled
10844   1060    svchost.exe     0xd288a4f76080  7       -       0       False   2023-01-05 20:00:37.000000      N/A     Disabled
864     4       smss.exe        0xd288a552a040  2       -       N/A     False   2023-01-05 19:58:31.000000      N/A     Disabled
1268    1060    WUDFHost.exe    0xd288a56e8140  5       -       0       False   2023-01-05 19:58:33.000000      N/A     Disabled
956     944     csrss.exe       0xd288a56f4140  14      -       0       False   2023-01-05 19:58:31.000000      N/A     Disabled
884     944     wininit.exe     0xd288a8a0f1c0  1       -       0       False   2023-01-05 19:58:33.000000      N/A     Disabled
1080    884     lsass.exe       0xd288a8b80080  10      -       0       False   2023-01-05 19:58:33.000000      N/A     Disabled
1060    884     services.exe    0xd288a8b850c0  7       -       0       False   2023-01-05 19:58:33.000000      N/A     Disabled
1204    1060    svchost.exe     0xd288a8be2080  12      -       0       False   2023-01-05 19:58:33.000000      N/A     Disabled
1232    884     fontdrvhost.ex  0xd288a8be3080  5       -       0       False   2023-01-05 19:58:33.000000      N/A     Disabled
1388    1060    svchost.exe     0xd288a8c38240  11      -       0       False   2023-01-05 19:58:34.000000      N/A     Disabled
1492    1060    WUDFHost.exe    0xd288a8c96080  5       -       0       False   2023-01-05 19:58:34.000000      N/A     Disabled
1444    1060    svchost.exe     0xd288a8cb1080  3       -       0       False   2023-01-05 19:58:34.000000      N/A     Disabled
1328    1060    WUDFHost.exe    0xd288a8cc4080  15      -       0       False   2023-01-05 19:58:34.000000      N/A     Disabled
2180    1060    svchost.exe     0xd288a8db90c0  1       -       0       False   2023-01-05 19:58:35.000000      N/A     Disabled
12740   3080    NVDisplay.Cont  0xd288a8dd70c0  35      -       3       False   2023-01-08 02:12:07.000000      N/A     Disabled
1820    1060    svchost.exe     0xd288a8e4d080  2       -       0       False   2023-01-05 19:58:35.000000      N/A     Disabled
1788    1060    svchost.exe     0xd288a8e4e080  4       -       0       False   2023-01-05 19:58:35.000000      N/A     Disabled
```

Adjunto también salida: “Salida Volatility psscan.txt”

Hives: vol.py -f "C:\Users\Equipo Pruebas\Desktop\xd.mem" windows.registry.hivescan

```
C:\Users\Equipo Pruebas\Desktop\volatility3-2.4.0>vol.py -f "C:\Users\Equipo Pruebas\Desktop\xd.mem" windows.registry.hivescan
Volatility 3 Framework 2.4.0
Progress:  100.00               PDB scanning finished
Offset

0xbe0743cfb000
0xbe0738890000
0xbe0737b03000
0xbe0743096000
0xbe072f75c000
0xbe074aec2000
0xbe074a76f000
0xbe073954b000
0xbe073fa1d000
0xbe0734c40000
0xbe0741fd1000
0xbe073782c000
0xbe0743bda000
0xbe074eed3000
0xbe072f67f000
0xbe073a291000
0xbe0735d14000
0xbe073874a000
0xbe0734bba000
0xbe073e45b000
0xbe07329ea000
0xbe0738872000
0xbe0743996000
0xbe072ffde000
0xbe073dc9f000
0xbe074a067000
0xbe0735245000
0xbe072f681000
0xbe073a8b8000
0xbe073de6c000
0xbe0738cee000
0xbe0738751000
0xbe0734ef3000
0xbe073cf72000
0xbe0738a6b000
0xbe07579c6000
0xbe0737c82000
0xbe0734c4e000
```

Historial cmd: vol.py -f "C:\Users\Equipo Pruebas\Desktop\xd.mem" windows.cmdline.CmdLine >> "C:\Users\Equipo Pruebas\Desktop\salida_cmd.txt"



```
C:\Users\Equipo Pruebas\Desktop\volatility3-2.4.0>vol.py -f "C:\Users\Equipo Pruebas\Desktop\xd.mem" windows.cmdline.CmdLine
Volatility 3 Framework 2.4.0
Progress:  100.00               PDB scanning finished
PID     Process Args

4       System  Required memory at 0x20 is not valid (process exited?)
172     Registry        Required memory at 0x20 is not valid (process exited?)
864     smss.exe        \SystemRoot\System32\smss.exe
956     csrss.exe       %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInit
ialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
884     wininit.exe     Required memory at 0x84f4d2c020 is inaccessible (swapped)
1060    services.exe    C:\Windows\system32\services.exe
1080    lsass.exe       C:\Windows\system32\lsass.exe
1204    svchost.exe     C:\Windows\system32\svchost.exe -k DcomLaunch -p
1232    fontdrvhost.ex  "fontdrvhost.exe"
1268    WUDFHost.exe    "C:\Windows\System32\WUDFHost.exe" -HostGUID:{193a1820-d9ac-4997-8c55-be817523f6aa} -IoEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-1975fce3-b985-4de7-b412-859481c
adfca -SystemEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-28d37d29-10b5-4d27-8a53-b6874b27dcc7 -IoCancelEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-bdcb35c0-6e4c-4404-993a-af74
959c5831 -NonStateChangingEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-45e35e05-34d8-452f-9a7b-4a4c7a8dbd63 -LifetimeId:fb8bd1dc-56e5-493b-9317-7647588faf74 -DeviceGroupId:WudfDefaultDevi
cePool -HostArg:0
1328    WUDFHost.exe    "C:\Windows\System32\WUDFHost.exe" -HostGUID:{193a1820-d9ac-4997-8c55-be817523f6aa} -IoEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-5ba60251-2a83-48fb-8a5c-8232557
dd78d -SystemEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-4037823f-c8bd-438e-8191-e4bb5eac4784 -IoCancelEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-15ac45e9-be5d-4501-9508-81a5
c59429e1 -NonStateChangingEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-e80cda9d-4a47-4b47-b812-d6232c02bfac -LifetimeId:07f7e8c1-fd78-48d2-85c4-590be9130863 -DeviceGroupId: -HostArg:0
1388    svchost.exe     C:\Windows\system32\svchost.exe -k RPCSS -p
1444    svchost.exe     C:\Windows\system32\svchost.exe -k DcomLaunch -p -s LSM
1492    WUDFHost.exe    "C:\Windows\System32\WUDFHost.exe" -HostGUID:{193a1820-d9ac-4997-8c55-be817523f6aa} -IoEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-853db10c-7ed0-4a3f-9bd0-b4475bf
149ce -SystemEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-4390ccb0-5833-4455-b98b-0c48b7159930 -IoCancelEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-c4635205-1e25-4d50-8d4e-23d2
60722fc7 -NonStateChangingEventPortName:\UMDFCommunicationPorts\WUDF\HostProcess-8decdc1f-ed7f-49bd-85de-6d2be1ba9e75 -LifetimeId:4899d4b2-dedc-481a-8e13-56fff70fccc4 -DeviceGroupId:WudfDefaultDevi
cePoolPriorityHigh -HostArg:0
1788    svchost.exe     C:\Windows\system32\svchost.exe -k LocalService -p -s nsi
1800    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -s BTAGService
1820    svchost.exe     C:\Windows\system32\svchost.exe -k LocalService -p -s BthAvctpSvc
1832    svchost.exe     C:\Windows\system32\svchost.exe -k LocalService -p -s bthserv
1980    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p
1992    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork -p
916     svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule
2112    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp
2156    svchost.exe     C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
```

Adjunto salida: “Salida Volatility psscan.txt”