

Practica DFIR



KEEPCODING

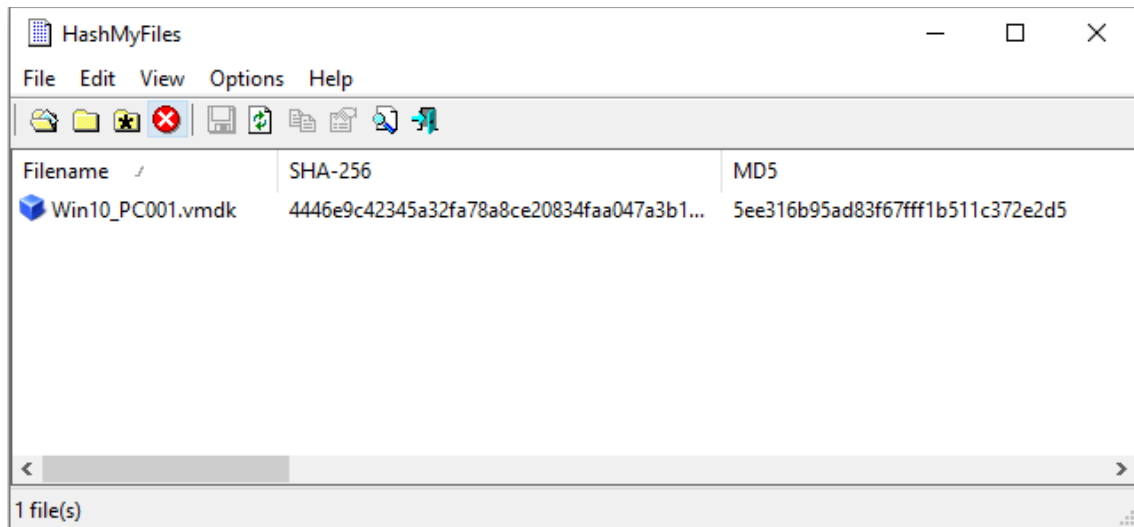
ÍNDICE

1. Practica Windows (Retos CTF)	3
2. Practica memoria RAM	16
3. Practica metadatos	20

1. Practica Windows (Retos CTF)

Hash del fichero - Extracción del hash SHA256 de la evidencia

Utilizo la herramienta HashMyfiles para la obtención del SHA-256 de la maquina con las evidencias



Hash SHA256: **4446e9c42345a32fa78a8ce20834faa047a3b161eba986f894d2230fcf6b0cbe**

Nombre de la máquina - Obtención del hostname

Extraigo el fichero SYSTEM el cual contiene el valor del hostname en la clave ComputerName

Ruta de la clave: *ControlSet001\Control\ComputerName\ComputerName*

PD: A tener en cuenta que la carpeta ControlSet001 se denomina así porque se está leyendo del fichero extraído (en frío), si se estuviera viendo desde la máquina encendida sería ControlSet

Con el uso de la herramienta WRR, nos movemos hacia la clave de registro que contiene el valor de la clave con el hostname: PEGASUS01

También se puede obtener con registry explorer o en logs del sistema

MiTeC Windows Registry Recovery - [SYSTEM]

File Options Explore Windows Help

Free to use for private, educational and non-commercial purposes

SYSTEM

NAVIGATOR

- File Information
- Security Records
- SAM
- Windows Installation
- Hardware
- Startup Applications
- Services and Drivers
- Network Configuration
- Windows Firewall Settings
- Environment
- Shell Folders
- Outlook Express
- Raw Data

CloudDomainJoin

CMF

CoDeviceInstallers

COM Name Arbiter

CommonGlobUserSettings

Compatibility

ComputerName

ComputerName

ContentIndex

CrashControl

Cryptography

DeviceClasses

DeviceContainerPropertyUpdateEvents

DeviceContainers

DeviceGuard

DeviceOverrides

DevicePanels

Value	Type	Data
(default)	REG_SZ	mmmsvc
ComputerName	REG_SZ	PEGASUS01

Result Panel

Key	Type	Value	Data
-----	------	-------	------

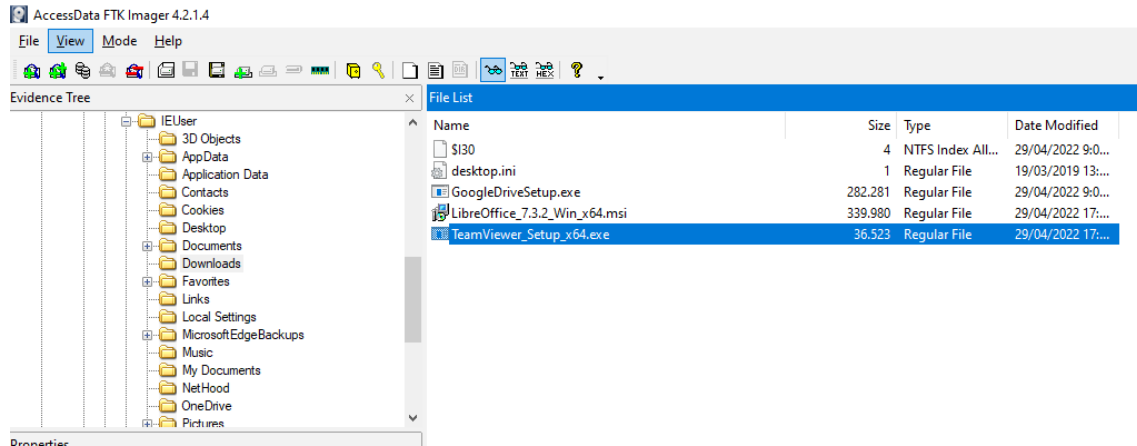
Search Log

0 keys / 2 values

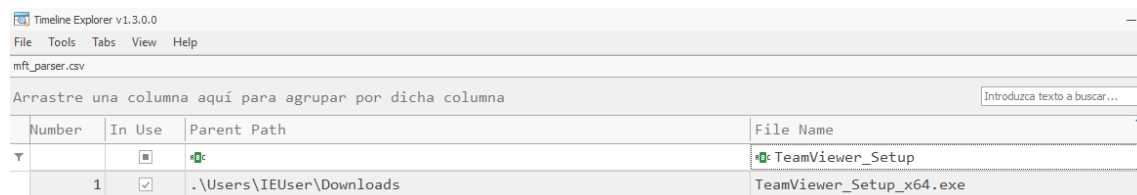
Key Path ROOT\ControlSet001\Control\ComputerName\ComputerName

Fecha de descarga software

Encuentro en descargas un programa remoto: TeamViewer_Setup_x64.exe con fecha **29/04/2022**



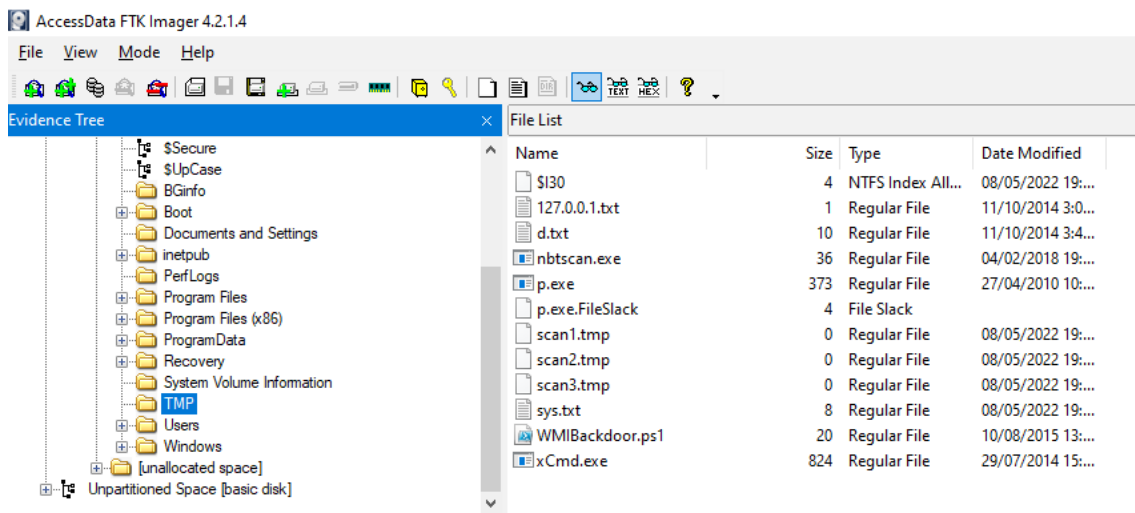
Extrayendo el \$MFT con FTK Imager y parseandolo con MFTECmd, con Timeline explorer también se puede encontrar



Ficheros maliciosos – ¿Dónde se encuentran?

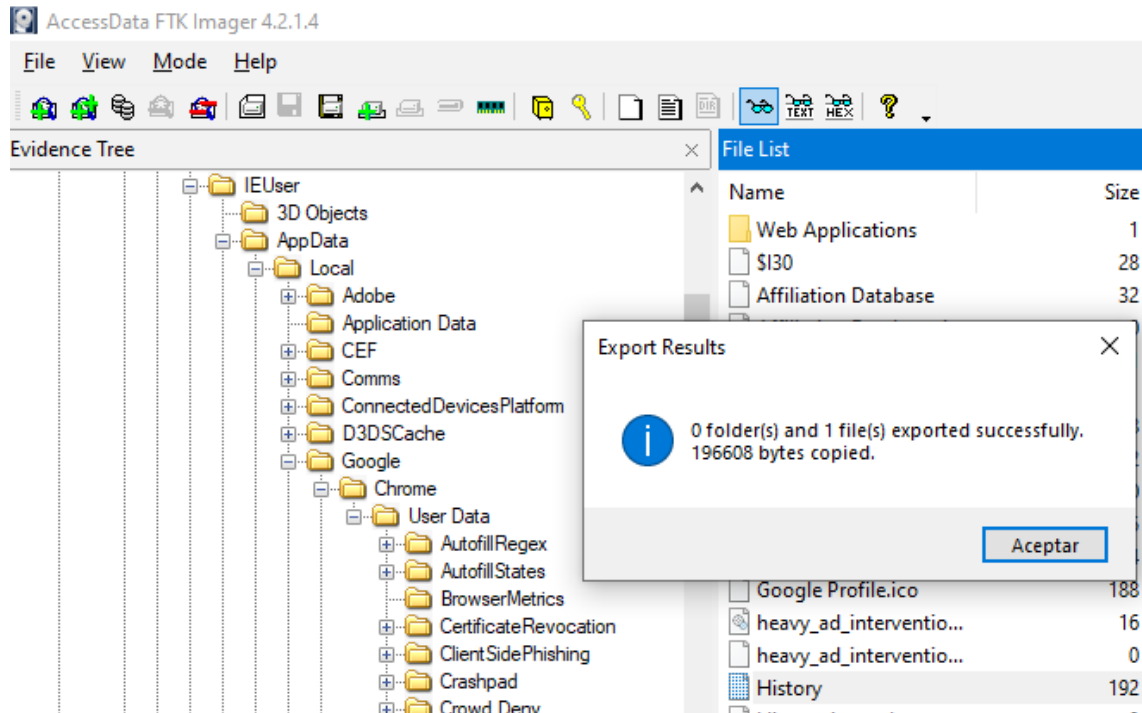
Con AccessData FTK Imager encuentro una carpeta llamada **TMP** la cual se encuentran archivos sospechosos denominados “WMIBackdoor.ps1”, “p.exe”, “xCmd.exe”

Es de suponer por tanto que usaron esta carpeta para descarga/uso y ejecución de herramientas y comandos, también se puede ver cómo hay archivos como scan1.tmp, scan2.tmp, scan3.tmp que dan a entender que el atacante hizo un escáner (sin conocer de que tipo)



Descarga fichero de control remoto

Extraemos el fichero History de Chrome con AccessData FTK Imager



Encontramos en el histórico de descarga de Chrome el programa remoto **TeamViewer_Setup_X64.exe**

DB Browser for SQLite - C:\Users\forensic\Desktop\Practical\Analysis\History\Chrome\History

Archivo Editar Ver Herramientas Ayuda

Nueva base de datos Abrir base de datos Guardar cambios Deshacer cambios Abrir proyecto Guardar proyecto Anexar base de datos Cerrar base de datos

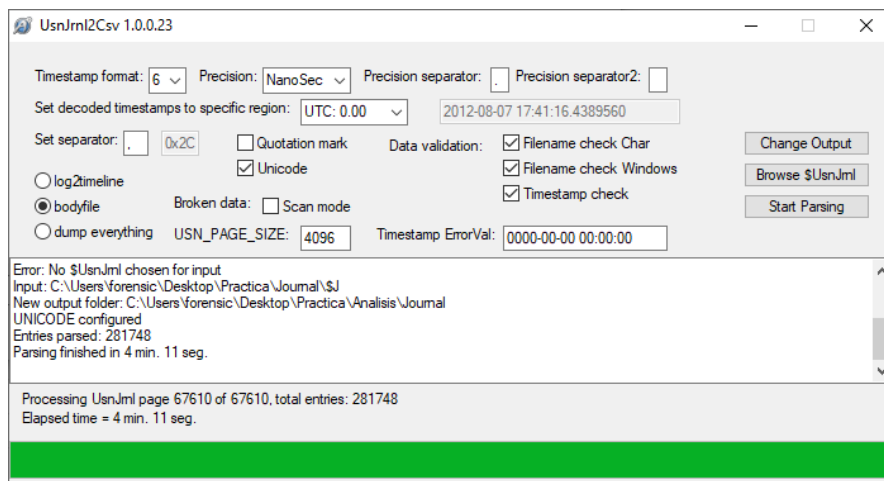
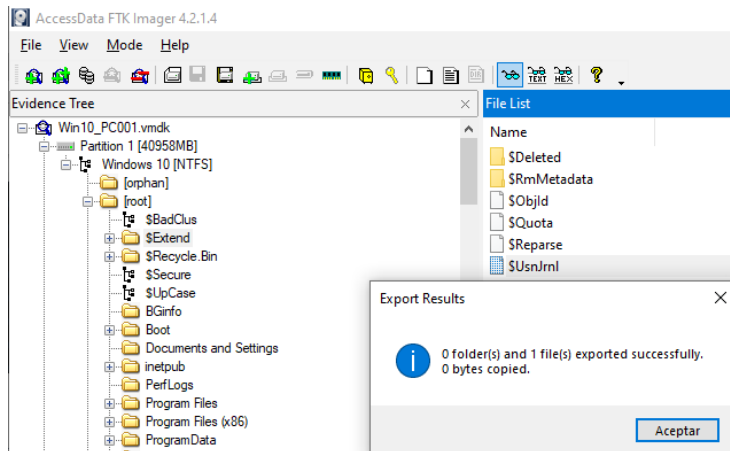
Estructura Hoja de datos Editar pragmas Ejecutar SQL

Tabla: downloads

	id	guid	current_path	target_path	last_modified
	Filtro	Filtro	Filtro	Filtro	Filtro
1	3	10c95149-34bc-48cc-aaa3-0e9307cd71c6	C:\Users\IEUser\Downloads\readerdc64_es_xa_crd_sec_install.exe	C:\Users\IEUser\Downloads\readerdc64_es_xa_crd_sec_install.exe	
2	4	584ddb68-f550-4bc3-bc18-3ce6dafb843c	C:\Users\IEUser\Downloads\TeamViewer_Setup_x64.exe	C:\Users\IEUser\Downloads\TeamViewer_Setup_x64.exe	Tue, 26 Apr 2022 10:23:17 GMT
3	5	49317fe0-1de8-43ad-8933-4d57204042c8	C:\Users\IEUser\Downloads\LibreOffice_7.3.2_Win_x64.msi	C:\Users\IEUser\Downloads\LibreOffice_7.3.2_Win_x64.msi	Thu, 24 Mar 2022 13:13:57 GMT
4	6	40fb84f8-a254-4173-8588-586163b36459	C:\Users\IEUser\Downloads\GoogleDriveSetup.exe	C:\Users\IEUser\Downloads\GoogleDriveSetup.exe	Thu, 14 Apr 2022 19:58:27 GMT

Ficheros eliminados – Extracción y obtención

Extraigo fichero \$UsnJrnl que es el que guarda las operaciones que se han hecho en los ficheros



Timeline Explorer v1.3.0.0

File Tools Tabs View Help

mft_parser.csv UsnJrnl_2024-04-24_22-27-55.csv

Arrastre una columna aquí para agrupar por dicha columna

	Parent Entry Number	Parent Sequence Number	In Use	Parent Path	File Name
2	23204	2	<input checked="" type="checkbox"/>	.\Program Files\WindowsApps\Microsoft.Microsoft3...	Archive.zip
8	84074	1	<input checked="" type="checkbox"/>	.\\$Recycle.Bin\S-1-5-21-321011808-3761883066-353...	\$IQBJZQY.zip

Observo que en \$Recycle.Bin hay un fichero denominado \$IQBJZQY.zip

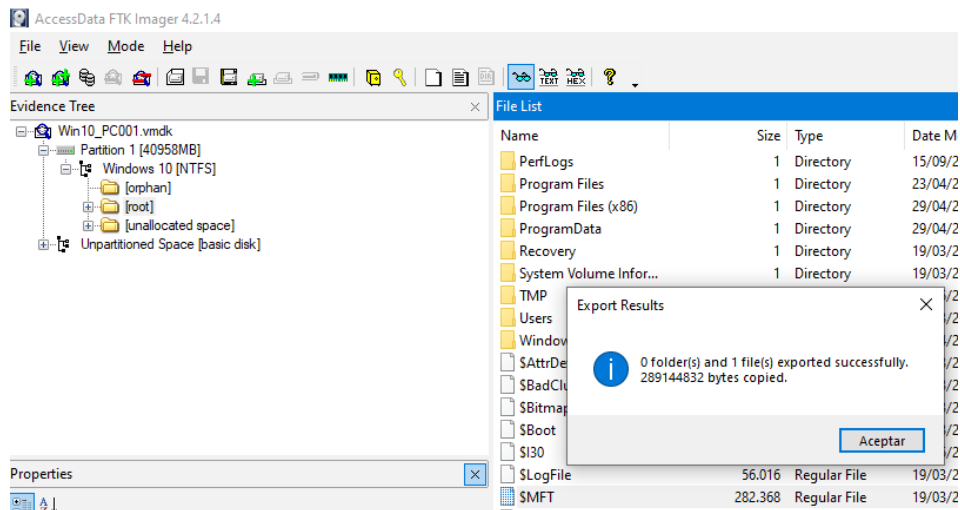
Parseamos con RBCmd para saber cuál es el nombre del fichero real eliminado y obtenemos: **cosas.zip**



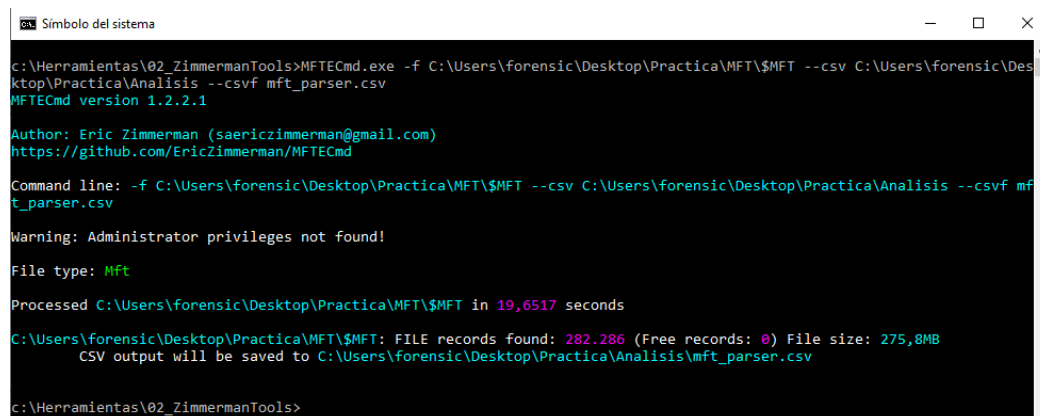
```
Símbolo del sistema
C:\Herramientas\02_ZimmermanTools>RBCmd.exe -f "C:\Users\forensic\Desktop\Practica\Fichero_eliminado\IQBJZQY.zip" --csv
"C:\Users\forensic\Desktop\Practica\Fichero_eliminado\output"
RBCmd version 1.5.0.0
Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/RBCmd
Command line: -f C:\Users\forensic\Desktop\Practica\Fichero_eliminado\IQBJZQY.zip --csv C:\Users\forensic\Desktop\Practica\Fichero_eliminado\output
Warning: Administrator privileges not found!
Found 1 files. Processing...
Source file: C:\Users\forensic\Desktop\Practica\Fichero_eliminado\IQBJZQY.zip
Version: 2 (Windows 10/11)
File size: 9.771.788 (9,3MB)
File name: C:\Users\IEUser\AppData\Local\Temp\cosas.zip
Deleted on: 2022-05-08 21:14:07
Processed 1 out of 1 files in 0,0407 seconds
CSV output will be saved to C:\Users\forensic\Desktop\Practica\Fichero_eliminado\output\20240424224427_RBCmd_Output.csv
C:\Herramientas\02_ZimmermanTools>
```

Fecha ejecución programa remoto

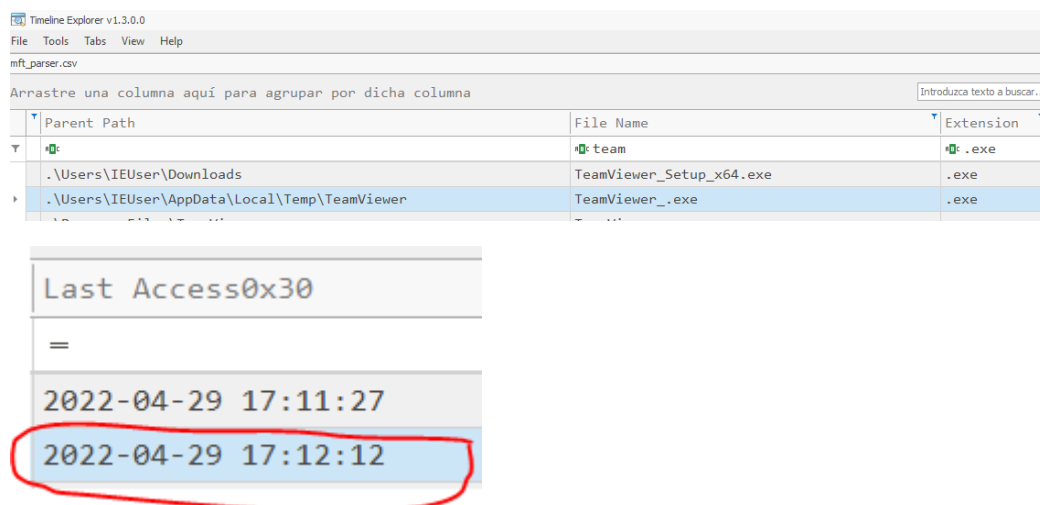
Extraemos el fichero \$MFT con Access FK Imager



Con MFTEcmd genero un fichero CSV (mft_parser.csv)




El cual podre visualizar con Timeline Explorer



Fecha ejecución: **2022-04-29**

Powershell maliciosa - Búsqueda

Con el \$MFT extraído y parseado anteriormente, haciendo una búsqueda con Timeline explorer encontramos un fichero denominado **WMIBackdoor.ps1**, con el propio nombre de Backdoor ya deducimos que es malicioso

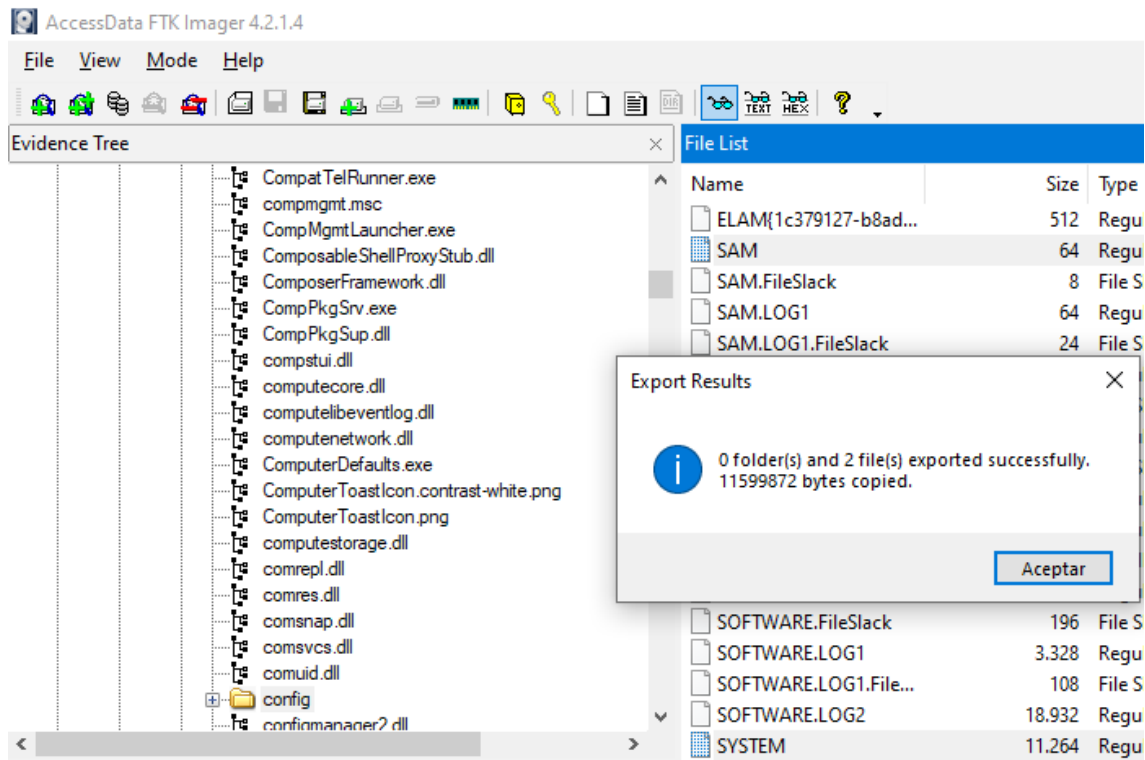


The screenshot shows the Timeline Explorer v1.3.0.0 interface. The menu bar includes File, Tools, Tabs, View, and Help. The main window displays a table with columns: In Use, Parent Path, File Name, and Extension. A single row is visible, representing a file named WMIBackdoor.ps1 located in the .\TMP directory. The file is marked as 'In Use' with a green icon and a checkmark.

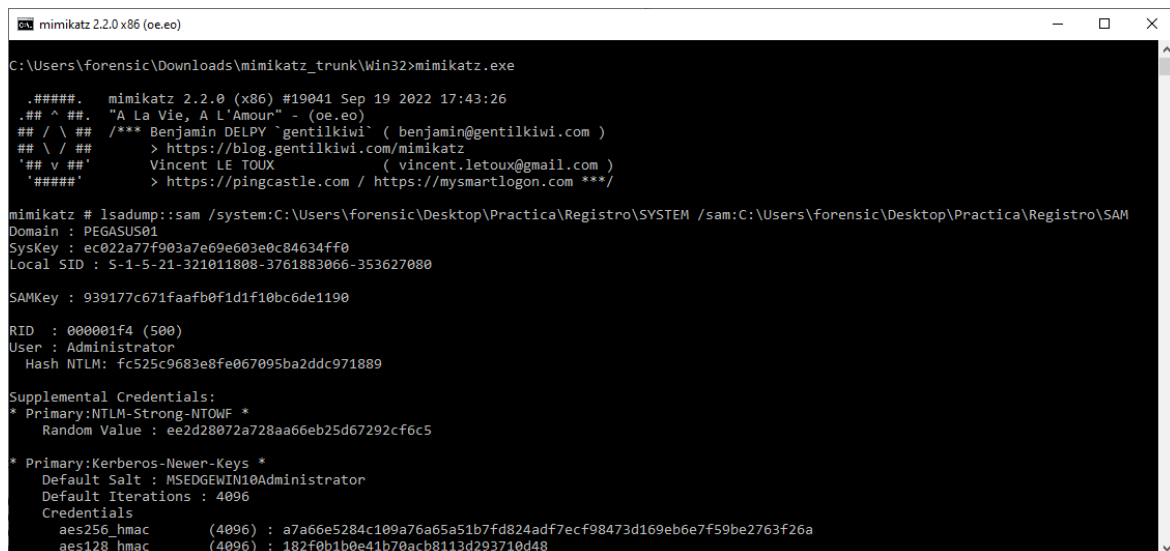
In Use	Parent Path	File Name	Extension
<input checked="" type="checkbox"/>	.\TMP	WMIBackdoor.ps1	.ps1

Contraseñas débiles

Extraemos el fichero SAM y SYSTEM que contiene los hashes



Con mimikatz hacemos un dump para conocer los hashes



Encuentro la cuenta de usuario IEUser

```
RID : 000003e8 (1000)
User : IEUser
Hash NTLM: 2d20d252a479f485cdf5e171d93985bf

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
Random Value : c6a807d33d3772144ce3407a8a73f9ef
```

Hash: 2d20d252a479f485cdf5e171d93985bf

En <https://crackstation.net/> ponemos el hash para romperlo

2d20d252a479f485cdf5e171d93985bf

No soy un robot

reCAPTCHA

Privacidad - Términos

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
2d20d252a479f485cdf5e171d93985bf	NTLM	qwerty

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

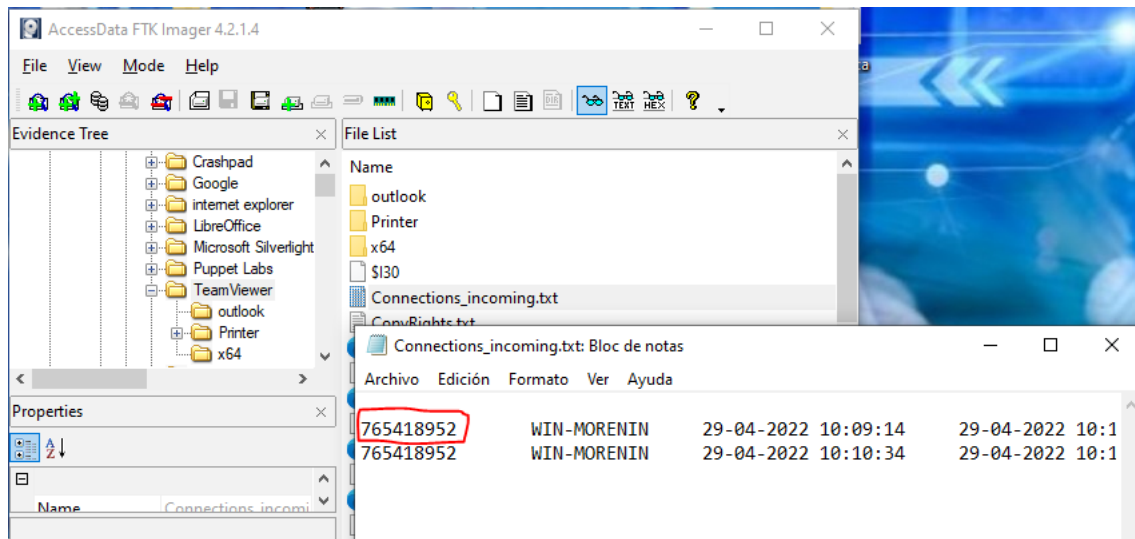
Contraseña débil: **qwerty**

Conexión programa control remoto

Revisamos la carpeta donde se aloja Teamviewer y extraer el log del teamviewer que contiene su ID

Ruta archivo: C:\Program Files\Teamviewer\Connections_incoming.txt

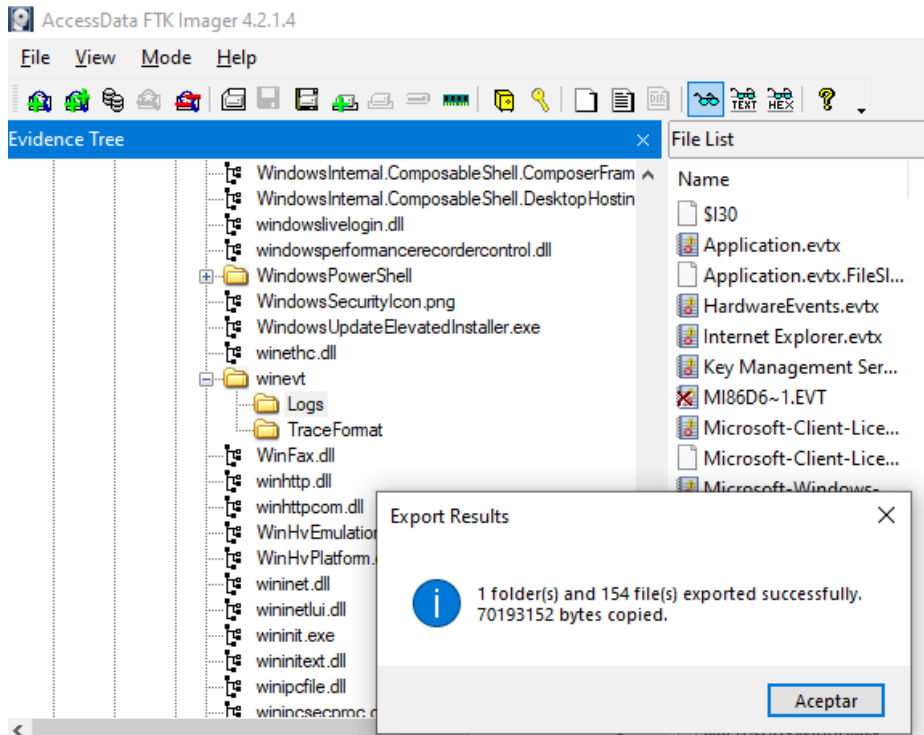
El fichero esta en texto plano, por tanto se puede leer sin problema



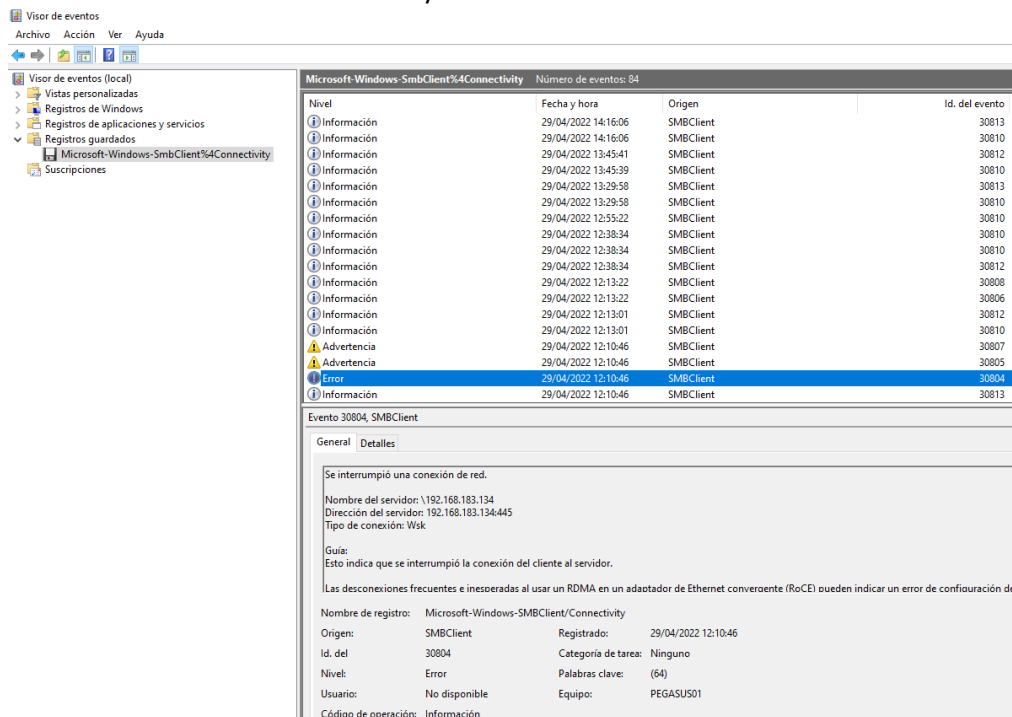
ID: 765418952

Conexión RDP (IP) y puerto conexión maquina atacante

Con AccessData FTK Imager extraigo la carpeta de Logs de: C:\Windows\System32\winevt\Logs



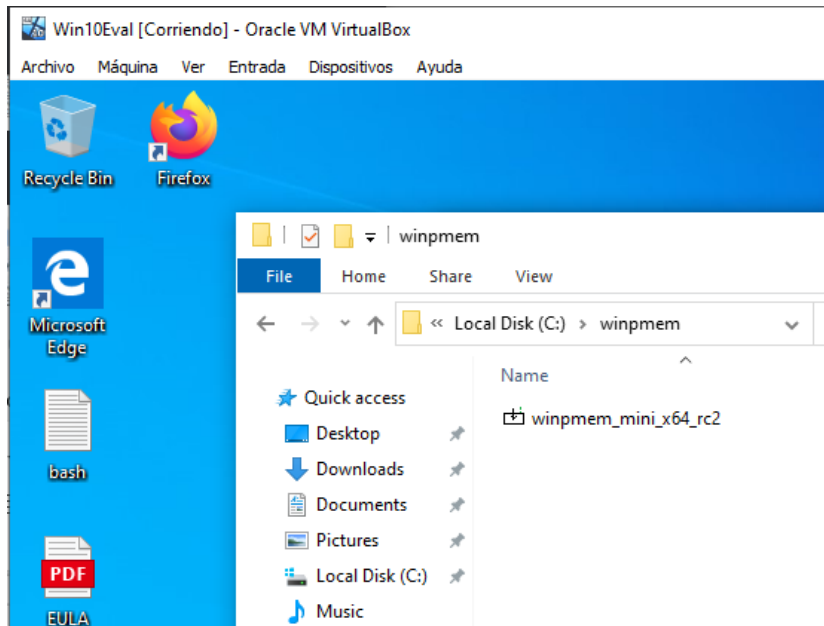
Buscando y revisando con el visor de eventos, encuentro en los logs de eventos Microsoft-Windows-SmbClient%4Connectivity.evtx un error:



Puedo determinar que dicho error es una conexión que hace el atacante con IP **192.168.183.134** y en el puerto **445**

2. Practica RAM

Para la adquisición de la ram usare un maquina W10 que tengo virtualizada:



Me descargo winpmem de <https://github.com/Velocidex/WinPmem/releases>

Hago un dump de la memoria con winpmem

```
Administrator: Command Prompt
C:\winpmem>winpmem_mini_x64_rc2.exe dump_ram_practica.mem_
```

```
Administrator: Command Prompt - winpmem_mini_x64_rc2.exe dump_ram_practica.mem
pad
- length: 0x1000
00% 0x00000000 .
copy_memory
- start: 0x1000
- end: 0x9f000
00% 0x0001000 .
Padding from 0x0009f000 to 0x00100000
pad
- length: 0x61000
00% 0x0009f000 .
copy_memory
- start: 0x100000
- end: 0x102000
00% 0x00100000 .
Padding from 0x00102000 to 0x00103000
pad
- length: 0x1000
00% 0x00102000 .
copy_memory
- start: 0x103000
- end: 0x7fff0000
00% 0x00103000 .....
39% 0x32103000 .....
```



```

C:\> Select Administrator: Command Prompt

- start: 0x1000
- end: 0x9f000

00% 0x00001000 .
Padding from 0x0009f000 to 0x00100000
pad
- length: 0x61000

00% 0x0009f000 .
copy_memory
- start: 0x100000
- end: 0x102000

00% 0x00100000 .
Padding from 0x00102000 to 0x00103000
pad
- length: 0x1000

00% 0x00102000 .
copy_memory
- start: 0x103000
- end: 0x7fff0000

00% 0x00103000 .....
39% 0x32103000 .....
78% 0x64103000 .....
The system time is: 20:13:43
Driver Unloaded.

C:\winpmem>

```

Para el uso de volatility usare la maquina virtual de W10 forensic, instalo Python

```

C:\Users\forensic>python --version
Python 3.12.3

C:\Users\forensic>cd C:\Herramientas\01_Artefactos\RAM\volatility3-2.5.2

C:\Herramientas\01_Artefactos\RAM\volatility3-2.5.2>pip3 install -r requirements-minimal.txt
Collecting pefile==2023.2.7 (from -r requirements-minimal.txt (line 2))
  Downloading pefile-2023.2.7-py3-none-any.whl.metadata (1.4 kB)
  Downloading pefile-2023.2.7-py3-none-any.whl (71 kB)
----- 71.8/71.8 kB 436.5 kB/s eta 0:00:00
Installing collected packages: pefile
Successfully installed pefile-2023.2.7

C:\Herramientas\01_Artefactos\RAM\volatility3-2.5.2>

```

y descargo volatility de:

<https://github.com/volatilityfoundation/volatility3/archive/refs/tags/v2.5.2.zip>

Con el dump de memoria utilizo volatility para extraer información

Con el comando Windows.cmdline.CmdLine, me lista los comandos que se han ejecutado en memoria

```

Simbolo del sistema - python vol.py -f C:\Users\forensic\Desktop\Practica\Analisis\RAM\dump_ram_practica.mem windows.cmdline.CmdLine

C:\Herramientas\01_Artefactos\RAM\volatility3-2.5.2>python vol.py -f C:\Users\forensic\Desktop\Practica\Analisis\RAM\dump_ram_practica.mem windows.cmdline.CmdLine
Volatility 3 Framework 2.5.2
Progress: 8.59 Scanning memory_layer using BytesScanner

```

```

Seleccionar Símbolo del sistema

7892 firefox.exe "C:\Program Files (x86)\Mozilla Firefox\Firefox.exe" -contentproc --channel=4084 -parentBuildID 20240425211020 -prefsHandle 4076 -prefMapHandle 4072 -prefsLen 23586 -p
refMapSize 245987 -appDir "C:\Program Files (x86)\Mozilla Firefox\browser" - {8f578418-5e4b-4055-8646-f688102ba47a} 5380 "\\.\pipe\gecko-crash-server-pipe.5380" rdd
5516 firefox.exe "C:\Program Files (x86)\Mozilla Firefox\Firefox.exe" -contentproc --channel=4316 -childID 3 -isForBrowser -prefsHandle 4296 -prefMapHandle 4292 -prefsLen 22849 -prefMa
pSize 245987 -jsInitHandle 1260 -jsInitLen 234952 -parentBuildID 20240425211020 -win32LockedDown -appDir "C:\Program Files (x86)\Mozilla Firefox\browser" - {5ffbfed1-4a2f-4e2a-acf1-176c980b
2a7} 5380 "\\.\pipe\gecko-crash-server-pipe.5380" tab
5384 firefox.exe Required memory at 0x4c0020 is inaccessible (swapped)
7732 firefox.exe Required memory at 0x4c1020 is inaccessible (swapped)
7296 firefox.exe Required memory at 0x431020 is inaccessible (swapped)
1468 firefox.exe Required memory at 0x492100 is inaccessible (swapped)
924 firefox.exe Required memory at 0x4de020 is inaccessible (swapped)
5812 WindowsInterna "C:\Windows\SystemApps\InputApp_cw5n1h2xyewy\WindowsInternal.ComposableShell.Experiences.TextInput.InputApp.exe" -ServerName:App.AppXgta193nsrpf7mheremt3yyfa1g555vc.
mca
5176 firefox.exe Required memory at 0x479e020 is inaccessible (swapped)
84 taskhostw.exe taskhostw.exe
3112 rdpLeakdiag.ex Required memory at 0x7bc020 is inaccessible (swapped)
2096 audiodg.exe C:\Windows\System32\AUDIOCG.EXE 0x3e4
6064 cmd.exe "C:\Windows\System32\cmd.exe"
7896 conhost.exe \?A\C:\Windows\System32\conhost.exe 0x4
7144 WMIProcV.exe C:\Windows\System32\Wbem\WMIProcV.exe
4852 SystemSettings Required memory at 0xfdfc9000 is inaccessible (swapped)
2488 TrustedInstall C:\Windows\servicing\TrustedInstaller.exe
1148 TiWorker.exe C:\Windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.18362.710_none_5f52d84058d0677f\TiWorker.exe -Embedding
7680 dlhst.exe C:\Windows\System32\OllHost.exe /ProcessId {3E3C877-1F16-487C-9050-10408C066683}
7972 svchost.exe C:\Windows\System32\svchost.exe -k NetworkService -p
1164 SearchProtocol "C:\Windows\System32\SearchProtocolHost.exe" Global\UsGthrFltPipeMsGthrPipe7 Global\UsGthrCtrlFltPipeMsGthrPipe7 1 -2147483646 "Software\Microsoft\Windows Search" -
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT; MS Search 4.0 Robot) "C:\ProgramData\Microsoft\Search\Data\Temp\usgthrsvc" "DownLevelDaemon"
7056 SearchFilter "C:\Windows\System32\SearchFilterHost.exe" 0 776 780 8192 764
8136 backgroundTask "C:\Windows\System32\BackgroundTaskHost.exe" -ServerName:x27e26f40ye01y48a6yb130ydf2038991ax.AppX09jg2m3yagbcrg7v3ym4r2ykqy91j5x.mca
6352 SkypeApp.exe "C:\Program Files\WindowsApps\Microsoft.SkypeApp_14.35.152.0_x64_kzfbqxf38zgc5\SkyypeApp.exe" -ServerName:App.AppXfn3yxqvgaw9fpmhny90fr3y01dit5b.mca
6564 HxTsr.exe "C:\Program Files\WindowsApps\Microsoft.WindowsCommunicationsapps_16005.11029.20108.0_x64_gwekyb3d8bbwe\HxTsr.exe" -ServerName:Hx.IPC.Server
568 backgroundTask Required memory at 0x19e0603640 is inaccessible (swapped)
4176 RuntimeBroker.exe -Embedding
6056 winmem_mini_x winmem_mini_x64_rc2.exe dump_ram_practica.mem

```

Comando para listar procesos (Windows.pstree)

```

Simbolo del sistema

C:\Herramientas\01_Artefactos\RAM\volatility3-2.5.2>python vol.py -f C:\Users\forensic\Desktop\Practica\Analisis\RAM\dump_ram_prac
tica.mem windows.pstree
Volatility 3 Framework 2.5.2
Progress: 100.00 PDB scanning finished
PID PPID ImageFileName Offset(V) Threads Handles SessionId Wow64 CreateTime ExitTime
4 0 System 0xae03d27c040 118 - N/A False 2024-04-30 19:44:02.000000 N/A
* 1544 4 MemCompression 0xae03d8074840 110 - N/A False 2024-04-30 19:44:12.000000 N/A
* 68 4 Registry 0xae03d2b96040 4 - N/A False 2024-04-30 19:43:59.000000 N/A
* 308 4 smss.exe 0xae03d4195040 2 - N/A False 2024-04-30 19:44:02.000000 N/A
468 460 csrss.exe 0xae03d6671140 12 - 1 False 2024-04-30 19:44:07.000000 N/A
520 460 winlogon.exe 0xae03d4f45080 7 - 1 False 2024-04-30 19:44:07.000000 N/A
* 712 520 fontdrvhost.ex 0xae03d4feb280 5 - 1 False 2024-04-30 19:44:08.000000 N/A
* 884 520 dwm.exe 0xae03d67e4100 15 - 1 False 2024-04-30 19:44:09.000000 N/A
* 3668 520 userinit.exe 0xae03d8c2b4c0 0 - 1 False 2024-04-30 19:44:35.000000 2024-04-30 19:45:0
1.000000
* 3680 3668 explorer.exe 0xae03d8c2e4c0 81 - 1 False 2024-04-30 19:44:35.000000 N/A
*** 3536 3680 Taskmgr.exe 0xae03d9f2e080 0 - 1 False 2024-04-30 19:45:36.000000 2024-04-30
19:46:32.000000
*** 6064 3680 cmd.exe 0xae03d99fc080 1 - 1 False 2024-04-30 20:05:47.000000 N/A
*** 7896 6064 conhost.exe 0xae03d6fb0800 4 - 1 False 2024-04-30 20:05:48.000000 N/A
*** 6056 6064 winmem_mini_x 0xae03d96b8080 2 - 1 False 2024-04-30 20:13:23.000000 N/A
*** 2260 3680 OneDrive.exe 0xae03d98ed080 0 - 1 True 2024-04-30 19:45:23.000000 2024-04-30
19:50:01.000000
*** 6776 2260 OneDriveSetup. 0xae03d8e7a080 0 - 1 True 2024-04-30 19:46:08.000000 2024-04-30
19:50:14.000000
**** 6848 6776 OneDriveSetup. 0xae03d89330c0 0 - 1 True 2024-04-30 19:46:10.000000 2024-04-30
19:50:14.000000
***** 896 6848 OneDrive.exe 0xae03d9d75080 26 - 1 True 2024-04-30 19:50:06.000000 N/A
*** 916 3680 SecurityHealth 0xae03d8e2f440 0 - 1 False 2024-04-30 19:45:20.000000 2024-04-30 19:45:2
1.000000
*** 5428 3680 VBoxTray.exe 0xae03d915a4c0 0 - 1 False 2024-04-30 19:45:21.000000 2024-04-30
19:46:26.000000
*** 5724 3680 vm3dservice.ex 0xae03d8e76080 1 - 1 False 2024-04-30 19:45:22.000000 N/A
6812 1868 firefox.exe 0xae03db4d9080 0 - 1 True 2024-04-30 20:00:02.000000 2024-04-30 20:00:3
7.000000

```

Comando para obtener los hashes (windows.hashdump)

```

Simbolo del sistema

C:\Herramientas\01_Artefactos\RAM\volatility3-2.5.2>python vol.py -f C:\Users\forensic\Desktop\Practica\Analisis\RAM\dump_ram_prac
tica.mem windows.hashdump
Volatility 3 Framework 2.5.2
Progress: 100.00 PDB scanning finished
User rid lmhash nthash
Administrator 500 aad3b435b51404eeaad3b435b51404ee 31d6cfe0d16ae931b73c59d7e0c089c0
Guest 501 aad3b435b51404eeaad3b435b51404ee 31d6cfe0d16ae931b73c59d7e0c089c0
DefaultAccount 503 aad3b435b51404eeaad3b435b51404ee 31d6cfe0d16ae931b73c59d7e0c089c0
WDAGUtilityAccount 504 aad3b435b51404eeaad3b435b51404ee 7485b1724974efb42754a55270d13ee6
User 1001 aad3b435b51404eeaad3b435b51404ee 31d6cfe0d16ae931b73c59d7e0c089c0
C:\Herramientas\01_Artefactos\RAM\volatility3-2.5.2>

```

Comando para listar los servicios (windows.svcscan.SvcScan)

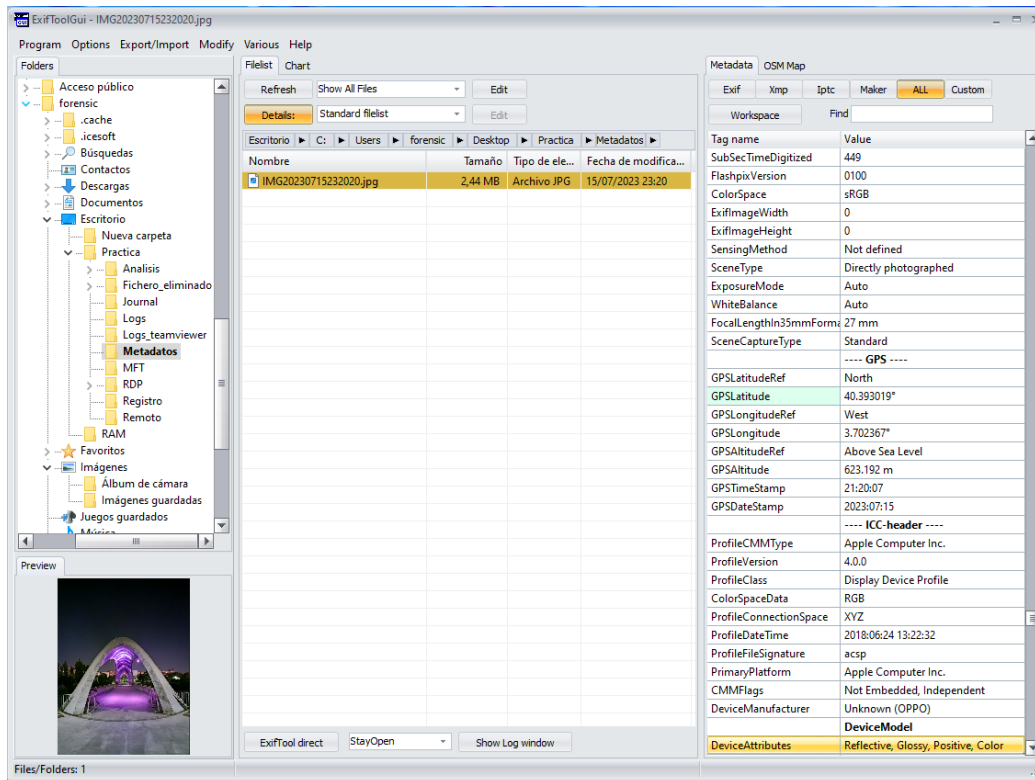
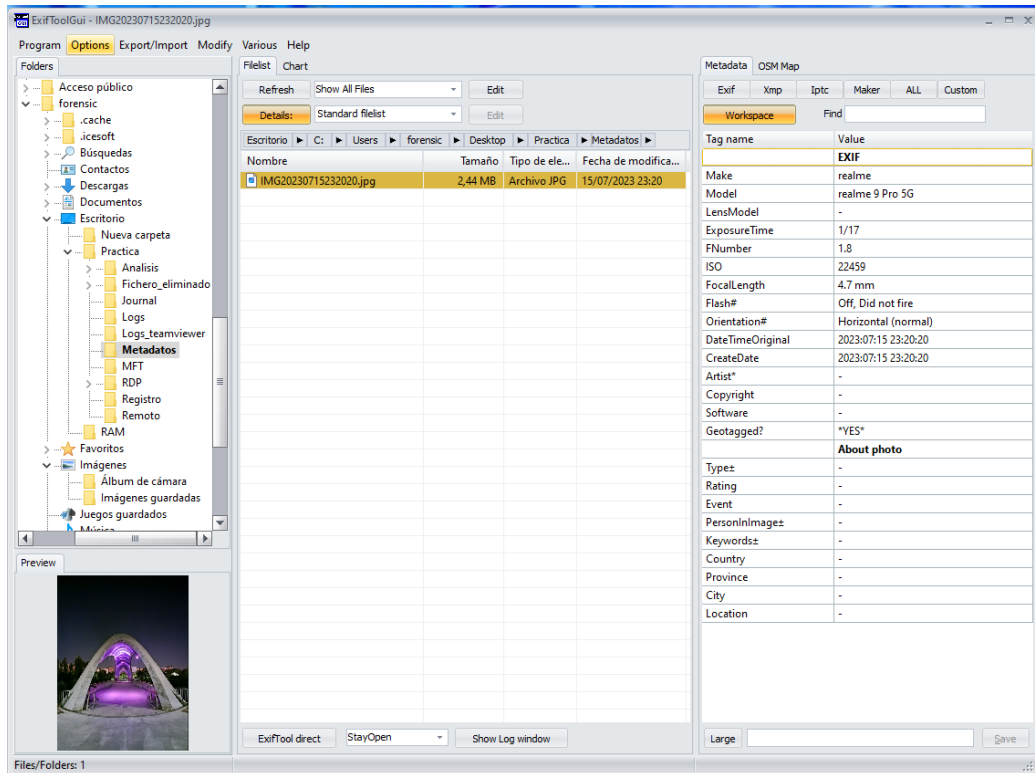
```

C:\Herramientas\01_Artefactos\RAM\volatility3-2.5.2>python vol.py -f C:\Users\forensic\Desktop\Practica\Analisis\RAM\dump_ram_prac
tica.mem windows.svcscan.SvcScan
Volatility 3 Framework 2.5.2
Progress: 100.00
PDB scanning finished
Offset Order PID Start State Type Name Display Binary
0x19d82664040 430 - SERVICE_AUTO_START SERVICE_RUNNING SERVICE_WIN32_OWN_PROCESS sppsvc Software Protectio
0x19d82664050 429 - SERVICE_AUTO_START SERVICE_RUNNING SERVICE_WIN32_OWN_PROCESS|SERVICE_INTERACTIVE_PROCESS Sp
ooler Print Spooler
0x19d82665bf0 428 N/A SERVICE_DEMAND_START SERVICE_STOPPED SERVICE_WIN32_OWN_PROCESS spectrum Windows Pe
rception Service
0x19d82664a10 427 N/A SERVICE_DEMAND_START SERVICE_STOPPED SERVICE_KERNEL_DRIVER SpbCx - N/A
0x19d82667750 426 N/A SERVICE_DEMAND_START SERVICE_STOPPED SERVICE_KERNEL_DRIVER SpatialGraphFilter - N/
0x19d82668650 425 N/A SERVICE_BOOT_START SERVICE_RUNNING SERVICE_KERNEL_DRIVER spaceport Storage Spaces Dri
ver
0x19d82667150 424 N/A SERVICE_DEMAND_START SERVICE_STOPPED SERVICE_WIN32_OWN_PROCESS SNMPTRAP SNMP Trap
N/A
0x19d82665d90 423 N/A SERVICE_DEMAND_START SERVICE_STOPPED SERVICE_WIN32_SHARE_PROCESS SmsRouter Microsoft
Windows SMS Router Service.
0x19d82665090 422 N/A SERVICE_DEMAND_START SERVICE_STOPPED SERVICE_WIN32_OWN_PROCESS smphost Microsoft Storage
Spaces SMP
0x19d82664390 421 N/A SERVICE_DEMAND_START SERVICE_STOPPED SERVICE_FILE_SYSTEM_DRIVER smbdirect smbdirect
N/A
0x19d82668450 420 N/A SERVICE_DEMAND_START SERVICE_STOPPED SERVICE_KERNEL_DRIVER SmartSAMD SmartSAMD N/
A
0x19d82668350 419 N/A SERVICE_DEMAND_START SERVICE_STOPPED SERVICE_KERNEL_DRIVER SiSRaid4 SiSRaid4 N/
A
0x19d82668250 418 N/A SERVICE_DEMAND_START SERVICE_STOPPED SERVICE_KERNEL_DRIVER SiSRaid2 SiSRaid2 N/
A
0x19d82667f50 417 N/A SERVICE_DISABLED SERVICE_STOPPED SERVICE_WIN32_SHARE_PROCESS shpamsvc Shared PC
Account Manager N/A
0x19d82664870 416 - SERVICE_AUTO_START SERVICE_RUNNING SERVICE_WIN32_SHARE_PROCESS ShellHWDetection Sh
ell Hardware Detection
0x19d826646d0 415 N/A SERVICE_DEMAND_START SERVICE_STOPPED SERVICE_WIN32_SHARE_PROCESS SharedRealitySvc Sp

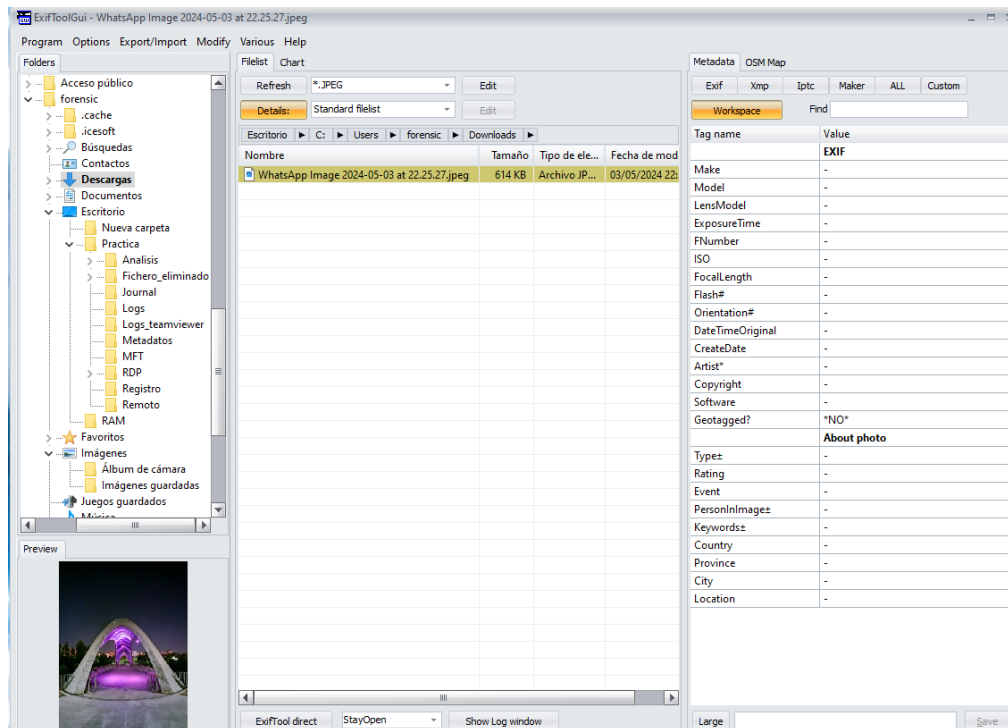
```

3. Practica metadatos

Selecciono una imagen hecha con el móvil, esta sin modificar

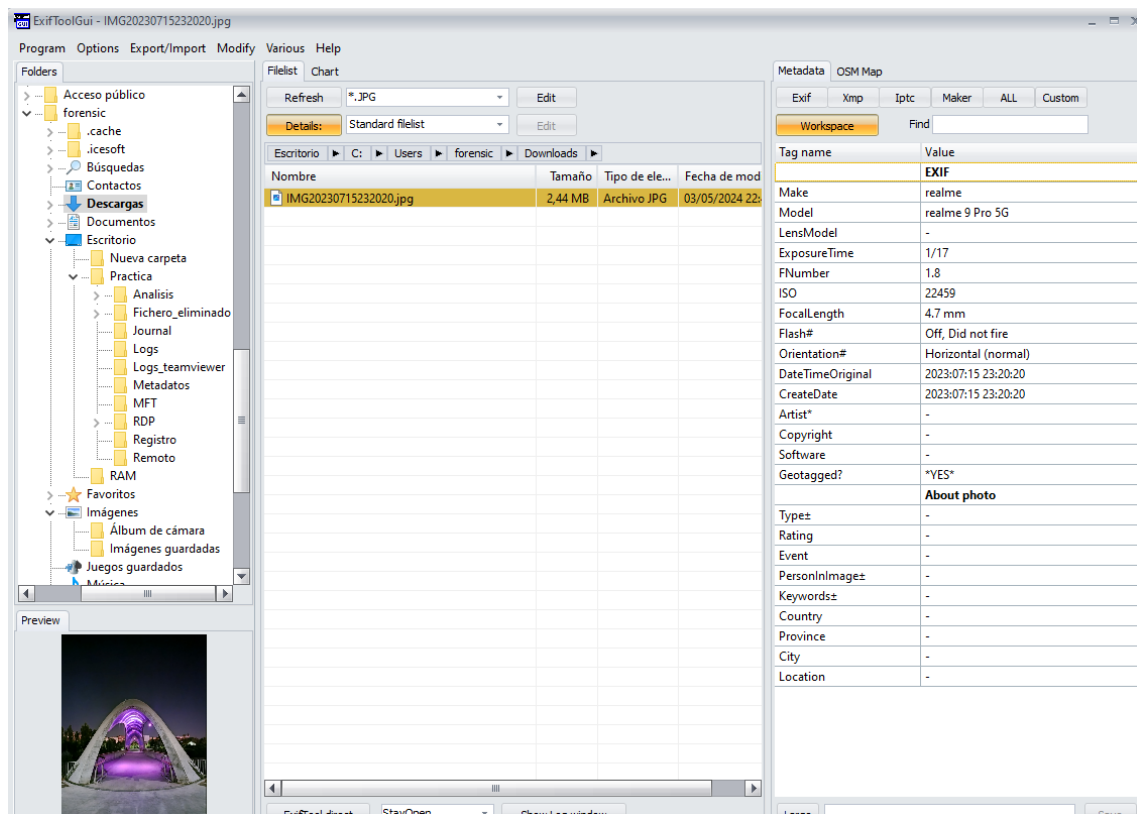


Metadatos de imagen enviada por Whatsapp y descargada

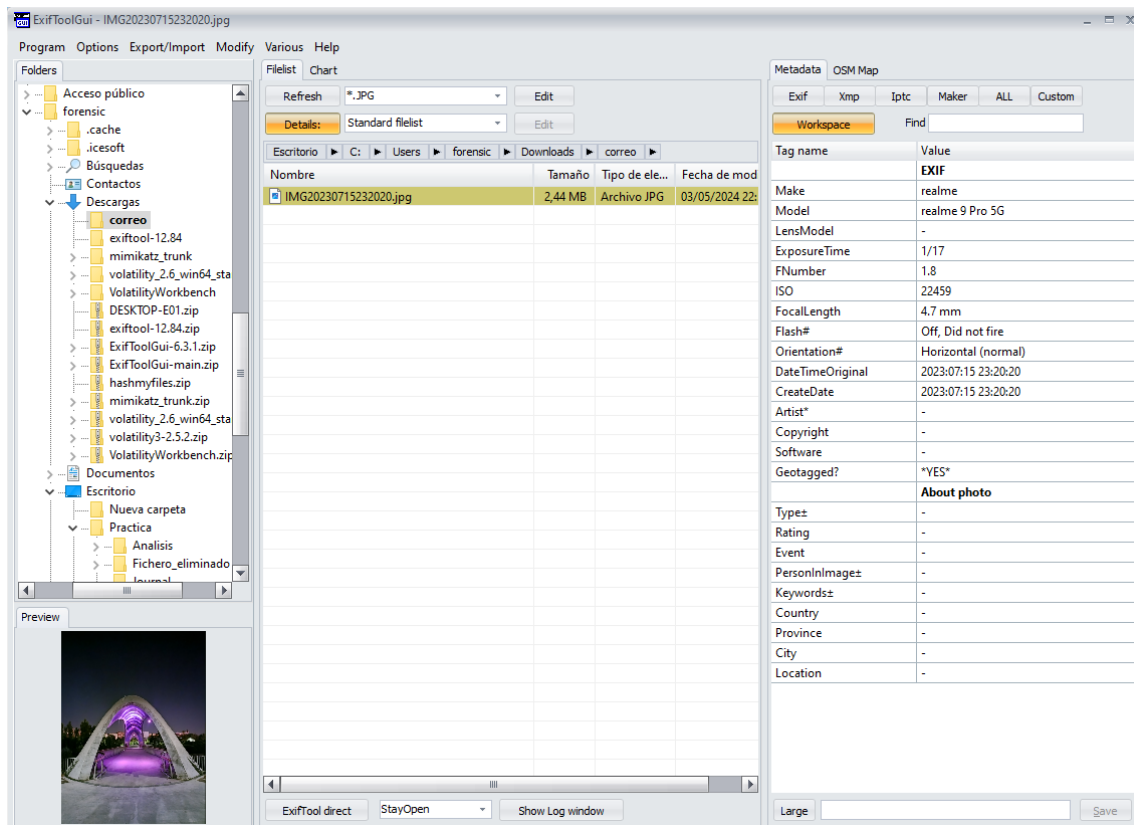


Metadatos en Telegram

Con Telegram se puede observar que si guarda los metadatos y mantiene mismo nombre, al descargar la imagen compruebo que se conserva igual que la imagen original:



Metadatos de imagen enviada y descargada por correo



Se puede observar que mantiene el mismo nombre y los metadatos que la imagen original

Como conclusión en el único servicio/programa que elimina los metadatos es Whatsapp, así que da a pensar para cuando quieres enviar imágenes y que no sepan de que móvil o dispositivo has utilizado, así como la relocalización (que se puede desactivar al tomar foto desde móvil)