



# JUPITER

## LABS

Informe de ejecutivo de **DFIR**

KeepCoding

Profesor: Sergio Sánchez

Realizado por: Mónica Durán Alfonso

Email: [monicadual1915@gmail.com](mailto:monicadual1915@gmail.com)

Linkedin: Mónica Durán

Diciembre 2024

# ÍNDICE

## 1.CTF

## 2.METADATOS

### 2.1. Foto original

### 2.2.Email

### 2.3.Telegram

### 2.4.WhatsApp

## 3.ADQUISICIÓN DE MEMORIA RAM

# 1.CTF

## PREGUNTA 1

### Hash del fichero

Como analistas de la máquina, lo primero que debemos obtener es el hash sha-256 de la evidencia.

-Para obtener el hash del fichero abrimos una PowerShell y lanzamos el comando GET-FILEHASH desde el path donde se encuentra nuestra imagen de disco y obtenemos el hash:

```
PS D:\VIRTUALMACHINES\VM2> Get-FileHash '.\Win10_PC001.vmdk'
```

Algorithm	Hash	Path
SHA256	4446E9C42345A32FA78A8CE20834FAA047A3B161EBA986F894D2230FCF6B0CBE	D:\VIRTUALMACHINES\VM2\Win10_...

```
PS D:\VIRTUALMACHINES\VM2> |
```

Imagen 1. Hash del fichero.

## PREGUNTA 2

### Nombre de la máquina

Para obtener el nombre de la máquina hemos recurrido a la herramienta **FTK** para visualizar los registros navegando a través de los diferentes directorios en busca del archivo **System**.

E:\Windows\System32\config\SYSTEM

Para poder extraer la información solicitada hemos utilizado la herramienta **RegRipper**, en el **campo Hive file** le hemos indicado el path dónde se encuentra el archivo **System** y en el campo **report file** le indicamos la ruta donde queremos que nos los guarde y una vez listo clicamos en **RIP!** y nos genera un **documento.txt** para poder visualizarlos y buscar el nombre de la máquina, una vez allí sólo nos queda filtrar por **ComputerName** y nos lleva hasta el nombre.

-----  
compname v.20090727

(System) Gets ComputerName and Hostname values from System hive

ComputerName = PEGASUS01

TCP/IP Hostname = PEGASUS01

-----  
cred v.20200427

(system) Checks for UseLogonCredential value

UseLogonCredential value not found.  
-----

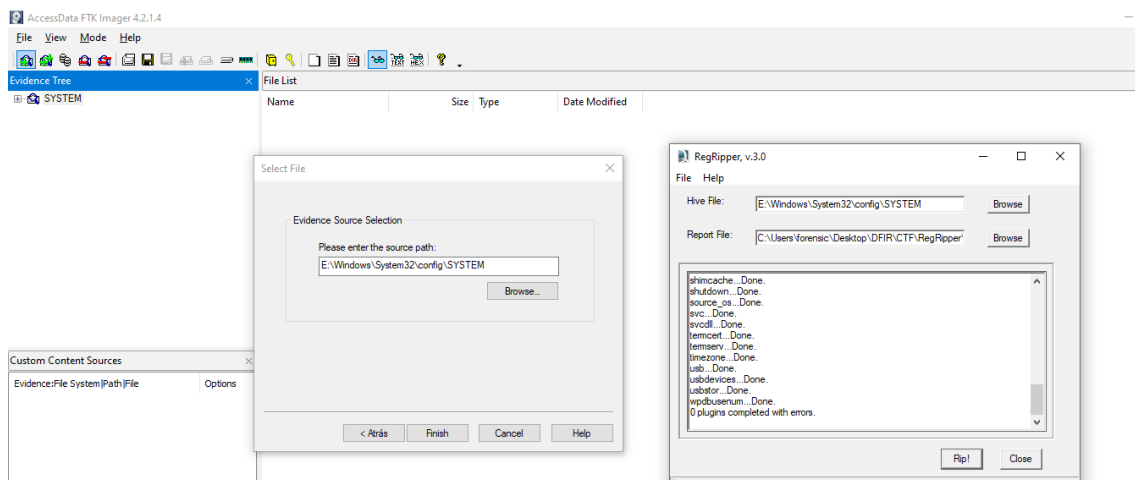


Imagen 2 Nombre de la máquina.

# PREGUNTA 3

## Ficheros maliciosos

¿En qué carpeta (solamente el nombre de la carpeta) se encuentran dichos ficheros?

Procedemos a realizar una búsqueda de la carpeta a través de la herramienta **Chainsaw** junto con la ruta donde tenemos guardadas las evidencias C:\Users\forensic\Desktop\DFIR\Eventos y nos reporta la información de la carpeta que necesitamos que es la de **\tmp**.

C:\Herramientas\01\_Artefactos\Eventos\chainsaw\chainsaw.exe hunt C:\Users\forensic\Desktop\DFIR\Eventos

CHAINSAW

By F-Secure Countercept (@FranticTyping, @AlexKornitzer)

[+] Found 142 EVTX files  
[!] Continuing without detection rules, no path provided  
[+] Hunting: [-----] 142/142 -

[+] Detection: (Built-in Logic) - Windows Defender Detections

system_time	id	computer	threat_name	threat_file	user
2022-05-08 19:04:52	1116	"PEGASUS01"	"Trojan:BAT/VigorF.A"	"file: C:\Users\IEUser\AppData\Local\Temp\APTSimulator\test-sets\command-and-control\wmi-backdoor-c2.bat"	"PEGASUS01\IEUser"
2022-05-08 19:04:53	1116	"PEGASUS01"	"Trojan:Win32/Powersploit!ml"	"file: C:\Users\IEUser\AppData\Local\Temp\APTSimulator\test-sets\credential-access\mimikatz-1.bat"	"PEGASUS01\IEUser"
2022-05-08 19:04:56	1116	"PEGASUS01"	"Trojan:BAT/VigorF.A"	"file: C:\Users\IEUser\AppData\Local\Temp\APTSimulator\test-sets\command-and-control\wmi-backdoor-c2.bat; file: C:\Users\IEUser\AppData\Local\Temp\dist\APTSimulator\test-sets\command-and-control\wmi-backdoor-c2.bat"	"PEGASUS01\IEUser"
2022-05-08 19:04:56	1116	"PEGASUS01"	"Trojan:Win32/Powersploit!ml"	"file: C:\Users\IEUser\AppData\Local\Temp\APTSimulator\test-sets\credential-access\mimikatz-1.bat; file: C:\Users\IEUser\AppData\Local\Temp\dist\APTSimulator\test-sets\credential-access\mimikatz-1.bat"	"PEGASUS01\IEUser"
2022-05-08 19:06:33	1116	"PEGASUS01"	"Backdoor:PowerShell/Powercat.A"	"file: C:\TMP\nc.ps1"	"PEGASUS01\IEUser"
2022-05-08 19:06:43	1116	"PEGASUS01"	"HackTool:Win32/DumpLsass.E"	"CmdLine: C:\Users\Public\procdump64.exe -accepteula -ma lsass.exe C:\TMP\somethingwindows.dmp"	"NT AUTHORITY\SYSTEM"
2022-05-08 19:07:02	1116	"PEGASUS01"	"SettingsModifier:Win32/PossibleHostsFileHijack"	"file: C:\Windows\System32\drivers\etc\hosts"	"PEGASUS01\IEUser"
2022-05-08 19:07:02	1116	"PEGASUS01"	"SettingsModifier:Win32/PossibleHostsFileHijack"	"file: C:\Windows\System32\drivers\etc\hosts"	"PEGASUS01\IEUser"
2022-05-08 19:07:02	1116	"PEGASUS01"	"SettingsModifier:Win32/PossibleHostsFileHijack"	"file: C:\Windows\System32\drivers\etc\hosts"	"PEGASUS01\IEUser"

Imagen 3 Carpeta fichero malicioso Imagen 4 nombre del fichero RDP 1

## PREGUNTA 4

Escriba el nombre del fichero .exe de un programa de control remoto que se ha descargado el usuario.

A través de la herramienta **FTK** desplegamos el panel y en la carpeta **IEUser<Downloads<TeamViewer\_Setup\_x64.exe**.

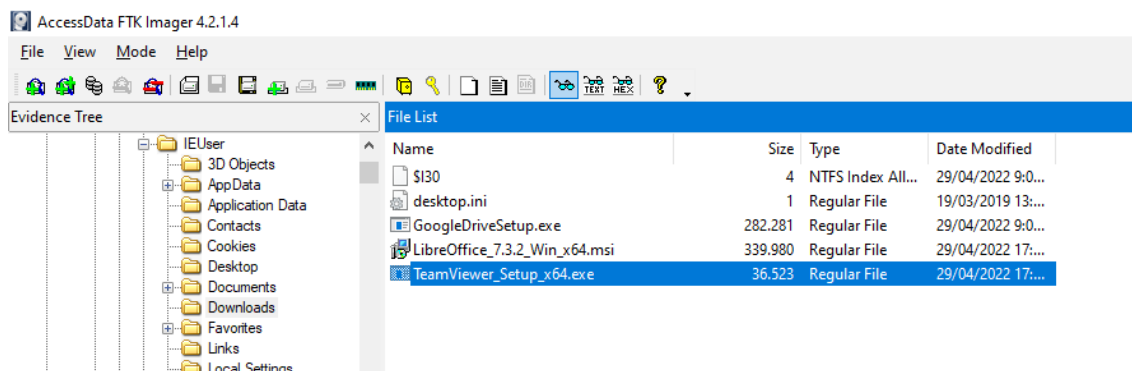


Imagen 4 nombre del fichero RDP.

# PREGUNTA 4.1

Fecha de descarga del software control remoto

Para poder saber cuándo fue descargado podemos exportar dicho archivo a nuestra carpeta de evidencias para poder ver en<TeamViewer\_Setup\_x64.exe<Propiedades y nos aparece la fecha de creación.

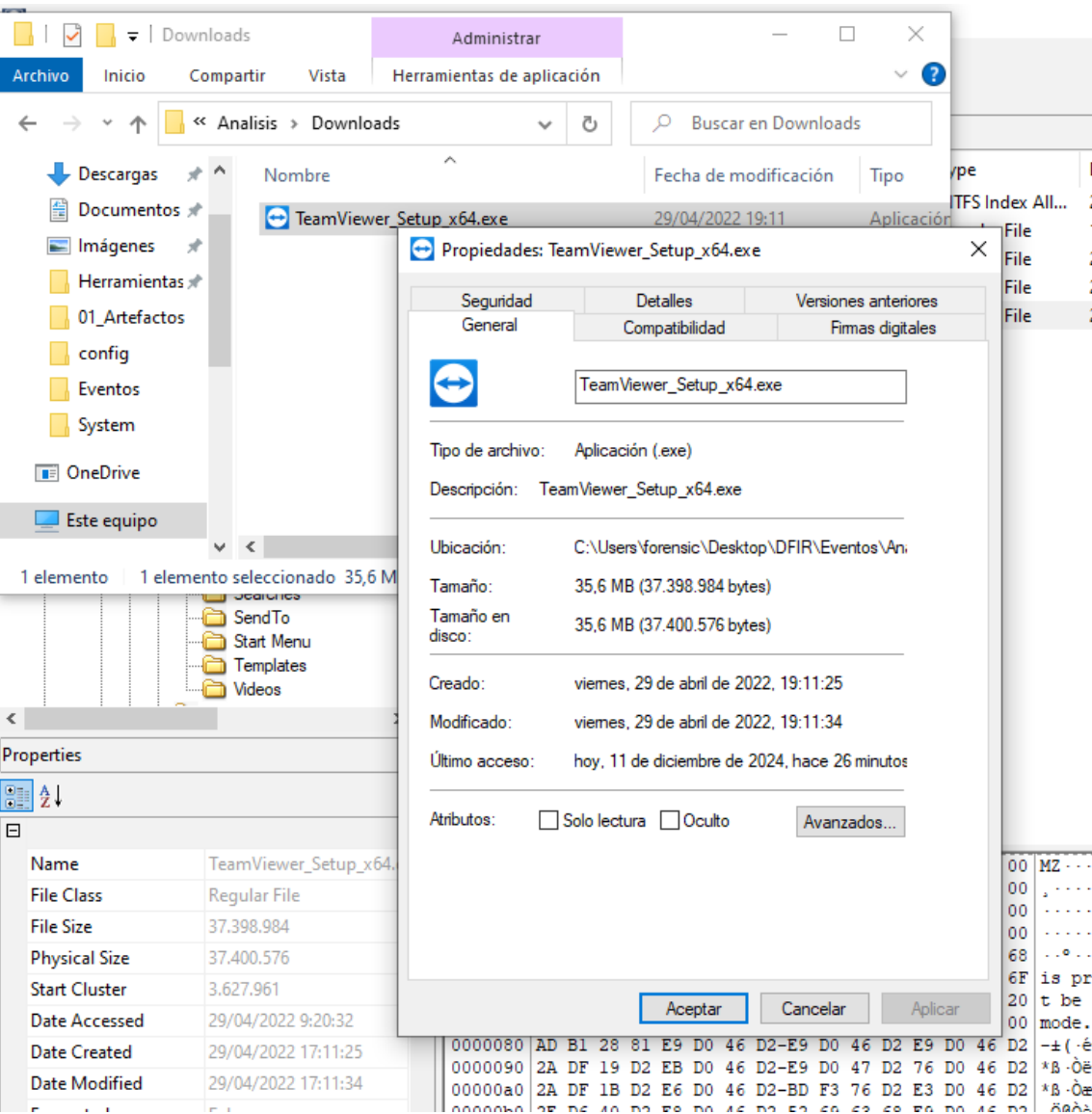


Imagen 5 Fecha de descarga del software.



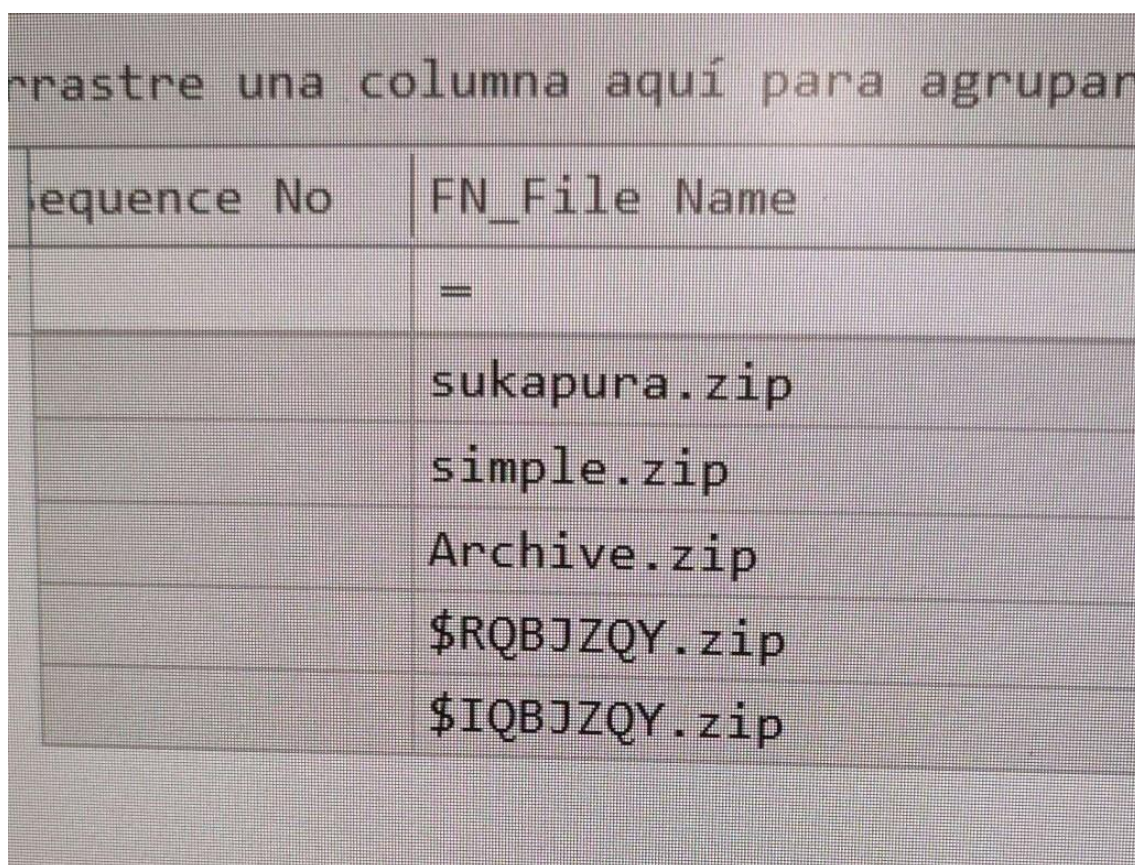
## PREGUNTA 5

### Ficheros eliminados

Se sospecha que existe un fichero .zip eliminado.

Podría indicar el nombre: **cosas.zip**

Lo hemos podido localizar con la ejecución de la herramienta RBCmd.exe de Eric Zimmerman y para ello hemos exportado de nuestra imagen forense los ficheros que aparentemente eran sospechosos de la carpeta **\$Recycle.Bin<S-1-5-21-321011808...<\$IQBJZQY/\$RQBJZQY** y hemos realizado el análisis con dicha herramienta y cuando hemos visualizado el fichero obtenido en **Timeline Explorer** hemos podido ver en nombre de la carpeta en texto en claro.



Sequence No	FN_File Name
	=
	sukapura.zip
	simple.zip
	Archive.zip
	\$RQBJZQY.zip
	\$IQBJZQY.zip

Imagen 6 Ficheros.zip sospechosos.



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Versión 10.0.19044.2846]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\forensic\Downloads\RBCmd>RBCmd.exe -d C:\Users\forensic\Desktop\Papelera --csv C:\Users\forensic\Desktop\Papelera --csvf zip.csv
RBCmd version 1.5.0.0

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

Command line: -d C:\Users\forensic\Desktop\Papelera --csv C:\Users\forensic\Desktop\Papelera --csvf zip.csv
Warning: Administrator privileges not found!

Looking for files in C:\Users\forensic\Desktop\Papelera
Found 6 files. Processing...

Source file: C:\Users\forensic\Desktop\Papelera\IQ8JZQY.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

Source file: C:\Users\forensic\Desktop\Papelera\S-1-5-21-321011808-3761883066-353627080-1000\IQQTUUV.pdf
Version: 2 (Windows 10/11)
File size: 219.389 (214,2KB)
File name: C:\Users\IEUser\Documents\02_AnejoII_EstrucyContTFG_a.pdf
Deleted on: 2022-05-08 20:54:10

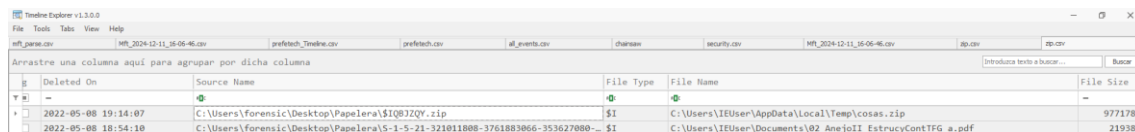
Unknown header 0x49! Send file to saericzimmerman@gmail.com so support can be added

Source file: C:\Users\forensic\Desktop\Papelera\S-1-5-21-321011808-3761883066-353627080-1000\IQ8JZQY.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

Source file: C:\Users\forensic\Desktop\Papelera\S-1-5-21-321011808-3761883066-353627080-1000\IV26VP8.pdf
Version: 2 (Windows 10/11)
File size: 50.673 (49,5KB)
File name: C:\Users\IEUser\Documents\CONFIDENTIAL document list.pdf
Deleted on: 2022-05-08 20:54:10

Source file: C:\Users\forensic\Desktop\Papelera\S-1-5-21-321011808-3761883066-353627080-1000\IVI3X9X.doc
Version: 2 (Windows 10/11)
File size: 0 (0B)
File name: C:\Users\IEUser\Documents\Documento Seguridad HipoSEMG.doc
Deleted on: 2022-05-08 20:54:10
```

Imagen 6.1 Ejecución del comando.



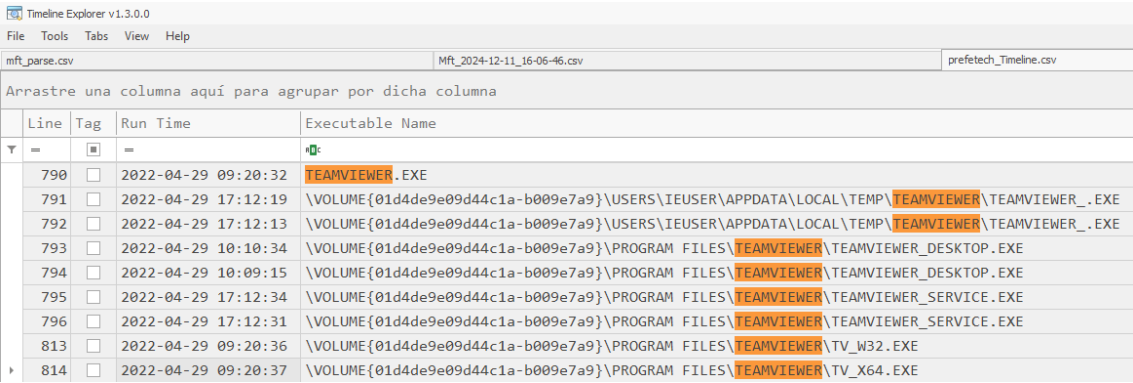
	Deleted On	Source Name	File Type	File Name	File Size
+	2022-05-08 19:14:07	C:\Users\forensic\Desktop\Papelera\IQ8JZQY.zip	\$I	C:\Users\IEUser\AppData\Local\Temp\cosas.zip	9771788
-	2022-05-08 18:54:10	C:\Users\forensic\Desktop\Papelera\S-1-5-21-321011808-3761883066-353627080-1000\IQQTUUV.pdf	\$I	C:\Users\IEUser\Documents\02_AnejoII_EstrucyContTFG_a.pdf	219389

Imagen 6.2 Fichero eliminado en texto en claro.

# PREGUNTA 6

## Fecha de ejecución del programa de control remoto

Para poder visualizar la fecha del programa TeamViewer hemos tomado una copia de la evidencia de los ficheros alojados dentro de **Windows<Prefetch** y ejecutamos la herramienta **PECmd.exe de Zimmerman Tools**, pasamos a guardar los resultados en una carpeta para luego poder analizarnos con el **Timeline Explorer** y en la columna **Run Time** podemos ver cuándo fue la ejecución de dicho archivo.



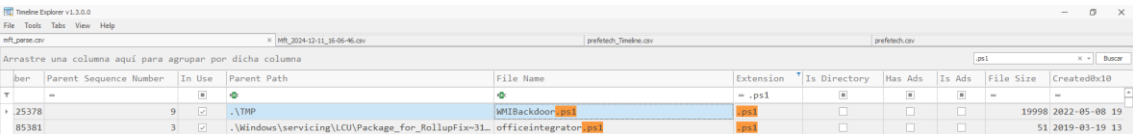
Line	Tag	Run Time	Executable Name
790		2022-04-29 09:20:32	TEAMVIEWER.EXE
791		2022-04-29 17:12:19	\VOLUME{01d4de9e09d44c1a-b009e7a9}\USERS\IEUSER\APPDATA\LOCAL\TEMP\TEAMVIEWER\TEAMVIEWER_.EXE
792		2022-04-29 17:12:13	\VOLUME{01d4de9e09d44c1a-b009e7a9}\USERS\IEUSER\APPDATA\LOCAL\TEMP\TEAMVIEWER\TEAMVIEWER_.EXE
793		2022-04-29 10:10:34	\VOLUME{01d4de9e09d44c1a-b009e7a9}\PROGRAM FILES\TEAMVIEWER\TEAMVIEWER_DESKTOP.EXE
794		2022-04-29 10:09:15	\VOLUME{01d4de9e09d44c1a-b009e7a9}\PROGRAM FILES\TEAMVIEWER\TEAMVIEWER_DESKTOP.EXE
795		2022-04-29 17:12:34	\VOLUME{01d4de9e09d44c1a-b009e7a9}\PROGRAM FILES\TEAMVIEWER\TEAMVIEWER_SERVICE.EXE
796		2022-04-29 17:12:31	\VOLUME{01d4de9e09d44c1a-b009e7a9}\PROGRAM FILES\TEAMVIEWER\TEAMVIEWER_SERVICE.EXE
813		2022-04-29 09:20:36	\VOLUME{01d4de9e09d44c1a-b009e7a9}\PROGRAM FILES\TEAMVIEWER\TV_W32.EXE
814		2022-04-29 09:20:37	\VOLUME{01d4de9e09d44c1a-b009e7a9}\PROGRAM FILES\TEAMVIEWER\TV_X64.EXE

Imagen 7 Ejecución del RDP

# PREGUNTA 7

## Powershell maliciosa

Para poder llegar al script lo único que hemos tenido que hacer es buscar en **Timeline Explorer** los resultados obtenidos de las herramientas de **MFT** y filtrar por **.ps1** y el primer archivo al ver el nombre **WMIBackdoor.ps1** ya nos da pista de que puede ser ese.



Index	Parent Sequence Number	In Use	Parent Path	File Name	Extension	Is Directory	Has Ads	Is Ads	File Size	Created@x10
25378	9		.\TMP	WMIBackdoor.ps1	.ps1				19998	2022-05-08 19
85381	3		.\Windows\servicing\LCU\Package_for_RollupFix-31...officeintegrator	ps1	.ps1				51	2019-03-19 13

Imagen 8 Powershell maliciosa

# PREGUNTA 8

## Contraseñas débiles

Para conocer la contraseña del usuario **IEUser** hemos seleccionado los archivos de registro **NTUSER.DAT,DEFAULT,SAM,SECURITY,SOFTWARE Y SYSTEM** y los guardamos en una carpeta para su posterior análisis con la herramienta **mimikatz**,con ella obtenemos una serie de hashes de las contraseñas de los usuarios y solo nos queda seleccionar el de nuestro usuario objetivo e insertarlo en **CRACKSTATION** para que nos reporte la contraseña en texto plano.

```
Credentials
des_cbc_md5      : 1ce9546ebf6e5e45

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

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

Imagen 9 Hash de la contraseña débil.

Enter up to 20 non-salted hashes, one per line:

2d20d252a479f485cdf5e171d93985bf

No soy un robot

reCAPTCHA

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	qerty

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

[Download CrackStation's Wordlist](#)

Imagen 10 Texto en claro de la contraseña débil.

## PREGUNTA 9

### Conexión programa control remoto.

Accedemos a la carpeta **TeamViewer** y dentro de ella observamos un archivo con un nombre muy curioso **connections\_incoming.txt** si le clicamos nos aparece los datos de la **ID** del programa de control remoto.

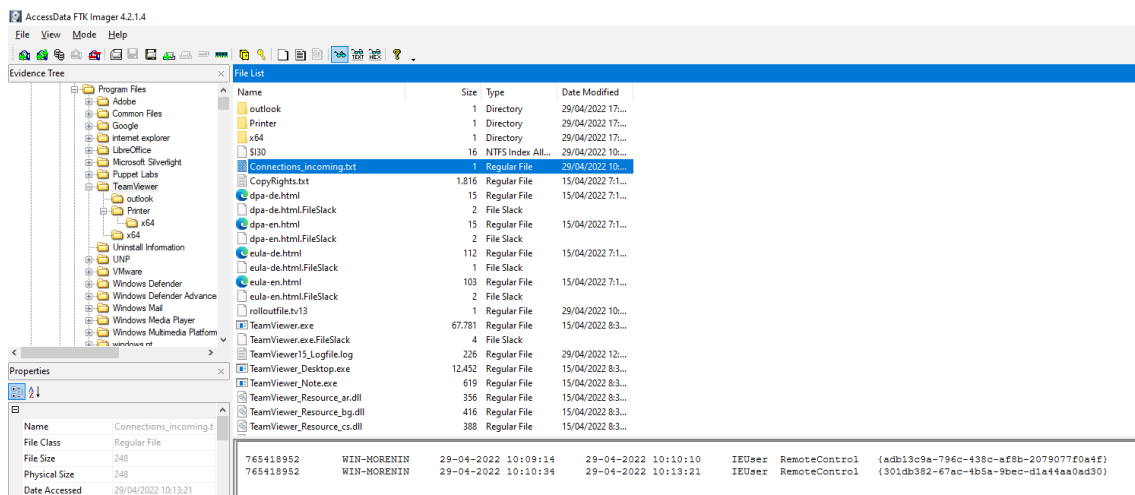


Imagen 11 Conexión RDP

## PREGUNTA 10

### Conexión RDP

Accedemos a la carpeta de **Windows\System32\winevt\Logs** y exportamos los archivos a una carpeta de **Evidencias/Logs** para su posterior análisis con la herramienta de **Zimmerman EvtxECmd** y con el archivo que nos reporta lo pasamos a analizar con **Timeline Explorer** y filtramos la búsqueda para que nos acote los resultados y después de un arduo trabajo de investigación con la prueba de varios identificadores de eventos obtenemos el ansiado resultado.

credentials	WORKGROUP\PEGASUS01\$	127.0.0.1:0	Target: PEGASUS01\IEUser
credentials	PEGASUS01\IEUser	192.168.183.134:445	Target: PEGASUS01\user1
credentials	PEGASUS01\IEUser	192.168.183.134:445	Target: PEGASUS01\user1
credentials	WORKGROUP\PEGASUS01\$	.	Target: Fast-Device-BackUP\MDP 0

Imagen 12 IP y puerto de conexión

## PREGUNTA 11

### **Puerto de conexión máquina atacante:**

Del mismo modo que en la pregunta anterior podemos observar el puerto por el que el atacante se ha conectado por RDP que en este caso es el **445**.

## 2.EXTRACCIÓN DE METADATOS



*Imagen 13 Foto inicial*

```

Megapixels          : 1.0
C:\Users\forensic\Downloads\exiftool-13.07_64\exiftool.exe "C:\Users\forensic\Pictures\Saved Pictures\Foto Monica.jpg"
ExifTool Version Number      : 13.07
File Name                   : Foto Monica.jpg
Directory                  : C:\Users\forensic\Pictures\Saved Pictures
File Size                   : 541 kB
Zone Identifier             : Exists
File Modification Date/Time  : 2024:12:15 13:36:38+01:00
File Access Date/Time       : 2024:12:15 13:44:46+01:00
File Creation Date/Time     : 2024:12:15 13:36:37+01:00
File Permissions            : -rw-rw-rw-
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
JFIF Version                : 1.01
Resolution Unit             : inches
X Resolution                : 96
Y Resolution                : 96
Exif Byte Order              : Big-endian (Motorola, MM)
Date/Time Original          : 2024:05:29 11:40:01
Create Date                  : 2024:05:29 11:40:01
Light Source                 : Unknown
Sub Sec Time Original        : 00
Sub Sec Time Digitized      : 00
GPS Latitude Ref             : North
GPS Longitude Ref           : Unknown (N)
Padding                      : (Binary data 268 bytes, use -b option to extract)
About                        : uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b
Image Width                 : 1440
Image Height                : 1839
Encoding Process             : Baseline DCT, Huffman coding
Bits Per Sample              : 8
Color Components             : 3
Y Cb Cr Sub Sampling        : YCbCr4:2:0 (2 2)
Image Size                  : 1440x1839
Megapixels                  : 2.6
Create Date                  : 2024:05:29 11:40:01.00
Date/Time Original          : 2024:05:29 11:40:01.00
C:\Users\forensic\Downloads\exiftool-13.07_64\exiftool-13.07_64>

```

Imagen 14 Metadatos foto original

## METADATOS WHATSAPP

```

C:\Windows\System32\cmd.exe
C:\Users\forensic\Downloads\exiftool-13.07_64\exiftool-13.07_64\exiftool.exe "C:\Users\forensic\Pictures\Saved Pictures\WhatsAppDescar.jpeg"
ExifTool Version Number      : 13.07
File Name                   : WhatsAppDescar.jpeg
Directory                  : C:\Users\forensic\Pictures\Saved Pictures
File Size                   : 301 kB
Zone Identifier             : Exists
File Modification Date/Time  : 2024:12:15 13:42:01+01:00
File Access Date/Time       : 2024:12:15 13:49:42+01:00
File Creation Date/Time     : 2024:12:15 13:41:23+01:00
File Permissions            : -rw-rw-rw-
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
JFIF Version                : 1.01
Resolution Unit             : None
X Resolution                : 1
Y Resolution                : 1
Image Width                 : 1440
Image Height                : 1839
Encoding Process             : Progressive DCT, Huffman coding
Bits Per Sample              : 8
Color Components             : 3
Y Cb Cr Sub Sampling        : YCbCr4:2:0 (2 2)
Image Size                  : 1440x1839
Megapixels                  : 2.6
C:\Users\forensic\Downloads\exiftool-13.07_64\exiftool-13.07_64>

```

Imagen 15 Metadatos WhatsApp

# METADATOS EMAIL

```
C:\Users\forensic\Downloads\exiftool-13.07_64\exiftool-13.07_64>exiftool.exe "C:\Users\forensic\Pictures\Saved Pictures\Email2.jpg"
ExifTool Version Number      : 13.07
File Name                    : Email2.jpg
Directory                   : C:\Users\forensic\Pictures\Saved Pictures
File Size                    : 541 kB
Zone Identifier              : Exists
File Modification Date/Time   : 2024:12:15 13:47:20+01:00
File Access Date/Time        : 2024:12:15 13:50:13+01:00
File Creation Date/Time      : 2024:12:15 13:47:19+01:00
File Permissions             : -rw-rw-rw-
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
JFIF Version                 : 1.01
Resolution Unit              : inches
X Resolution                 : 96
Y Resolution                 : 96
Exif Byte Order              : Big-endian (Motorola, MM)
Date/Time Original           : 2024:05:29 11:40:01
Create Date                  : 2024:05:29 11:40:01
Light Source                 : Unknown
Sub Sec Time Original        : 00
Sub Sec Time Digitized       : 00
GPS Latitude Ref             : North
GPS Longitude Ref           : Unknown (N)
Padding                      : (Binary data 268 bytes, use -b option to extract)
About                        : uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b
Image Width                  : 1440
Image Height                 : 1839
Encoding Process             : Baseline DCT, Huffman coding
Bits Per Sample              : 8
Color Components              : 3
Y Cb Cr Sub Sampling         : YCbCr4:2:0 (2 2)
Image Size                   : 1440x1839
Megapixels                   : 2.6
Create Date                  : 2024:05:29 11:40:01.00
Date/Time Original           : 2024:05:29 11:40:01.00

C:\Users\forensic\Downloads\exiftool-13.07_64\exiftool-13.07_64>
```

Imagen 16 Metadatos de Email.

# METADATOS TELEGRAM

```
C:\Users\forensic\Downloads\exiftool-13.07_64\exiftool-13.07_64>exiftool.exe "C:\Users\forensic\Pictures\Saved Pictures\TelegramDesca.jpg"
ExifTool Version Number      : 13.07
File Name                    : TelegramDesca.jpg
Directory                   : C:\Users\forensic\Pictures\Saved Pictures
File Size                    : 223 kB
Zone Identifier              : Exists
File Modification Date/Time   : 2024:12:15 13:42:47+01:00
File Access Date/Time        : 2024:12:15 13:48:51+01:00
File Creation Date/Time      : 2024:12:15 13:42:46+01:00
File Permissions             : -rw-rw-rw-
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
JFIF Version                 : 1.01
Resolution Unit              : inches
X Resolution                 : 72
Y Resolution                 : 72
Profile CMY Type             :
Profile Version              : 4.3.0
Profile Class                : Display Device Profile
Color Space Data             : RGB
Profile Connection Space     : XYZ
Profile Date Time            : 2016:01:01 00:00:00
Profile File Signature       : acsp
Primary Platform             : Unknown ( )
CMY Flags                    : Not Embedded, Independent
Device Manufacturer          :
Device Model                 :
Device Attributes            : Reflective, Glossy, Positive, Color
Rendering Intent             : Media-Relative Colorimetric
Connection Space Illuminant  : 0.9642 1 0.82491
Profile Creator              :
Profile ID                   : 0
Profile Description           : sRGB
Red Matrix Column            : 0.43607 0.22249 0.01392
Green Matrix Column          : 0.38515 0.71687 0.09708
Blue Matrix Column           : 0.14307 0.06061 0.7141
Media White Point            : 0.9642 1 0.82491
Red Tone Reproduction Curve  : (Binary data 40 bytes, use -b option to extract)
Green Tone Reproduction Curve : (Binary data 40 bytes, use -b option to extract)
Blue Tone Reproduction Curve : (Binary data 40 bytes, use -b option to extract)
Profile Copyright            : Google Inc. 2016
Image Width                  : 1002
Image Height                 : 1280
Encoding Process             : Progressive DCT, Huffman coding
Bits Per Sample              : 8
Color Components              : 3
Y Cb Cr Sub Sampling         : YCbCr4:2:0 (2 2)
Image Size                   : 1002x1280
Megapixels                   : 1.3

C:\Users\forensic\Downloads\exiftool-13.07_64\exiftool-13.07_64>
```

Imagen 16 Metadatos Telegram.



## Tabla comparativa de los Metadatos

Categoría	Foto Monica	Email2.jpg	TelegramDesca.jpg	WhatsAppDescar.jp
Nombre	Foto Monica.jpg	Email2.jpg	TelegramDesca.jpg	WhatsAppDescar.jp
Directorio	C:/Users/...	C:/Users/...	C:/Users/...	C:/Users/...
Tamaño	541 kB	541 kB	223 kB	301 kB
Modificación	2024:12:15 13:36	2024:12:15 13:47	2024:12:15 13:42	2024:12:15 13:42
Acceso	2024:12:15 13:44	2024:12:15 13:50	2024:12:15 13:48	2024:12:15 13:49
Creación	2024:12:15 13:36	2024:12:15 13:47	2024:12:15 13:42	2024:12:15 13:41
Permisos	-rw-rw-rw-	-rw-rw-rw-	-rw-rw-rw-	-rw-rw-rw-
Tipo	JPEG	JPEG	JPEG	JPEG
Tipo MIME	image/jpeg	image/jpeg	image/jpeg	image/jpeg
Resolución Unidad	inches	inches	inches	None

<b>Resolución X</b>	96	96	72	1
<b>Resolución Y</b>	96	96	72	1
<b>Original</b>	2024:05:29 11:40	2024:05:29 11:40	No especificado	No especificado
<b>Creación Fecha</b>	2024:05:29 11:40	2024:05:29 11:40	No especificado	No especificado
<b>Ancho</b>	1440	1440	1002	1440
<b>Altura</b>	1839	1839	1280	1839
<b>Megapíxeles</b>	2.6	2.6	1.3	2.6
<b>Color Components</b>	3	3	3	3
<b>Encoding Process</b>	Baseline DCT	Baseline DCT	Progressive DCT	Progressive DCT
<b>Bits per Sample</b>	8	8	8	8
<b>Comentarios</b>	No especificado	No especificado	Google Inc. 2016	No especificado
<b>Padding</b>	Binary data 268	Binary data 268	No especificado	No especificado
<b>GPS Latitud</b>	North	North	No especificado	No especificado
<b>GPS Longitud</b>	Unknown (N)	Unknown (N)	No especificado	No especificado

Imagen 17 Comparativa de Metadatos

En la tabla comparativa se muestra los datos entre los diferentes tipos de Apps de envío y podemos resaltar:

\* Resolución: "Foto Mónica" y "Email2.jpg" tienen resoluciones de 96 dpi, mientras que "TelegramDesca.jpg" tiene 72 dpi y "WhatsAppDescar.jpeg" 1 dpi.

\* Tamaño **de archivo**: "Foto Mónica" y "Email2.jpg" son 541 kB cada uno, "TelegramDesca.jpg" es 223 kB y "WhatsAppDescar.jpeg" es 301 kB.

\* Fechas **de modificación**: Las fechas varían, pero todas las imágenes fueron modificadas y creadas el 15 de diciembre de 2024.

\* Componentes **de color y bits por muestra**: Todos los archivos tienen 3 componentes de color y 8 bits por muestra.

### 3. Memoria Ram

Procedemos a descargar la herramienta **Winpmeme** y se ejecuta con permisos de administrador, nos generará un fichero del tamaño de nuestra memoria, le indicamos el nombre del fichero que queremos generar y lo guardamos en la carpeta creada para ello:

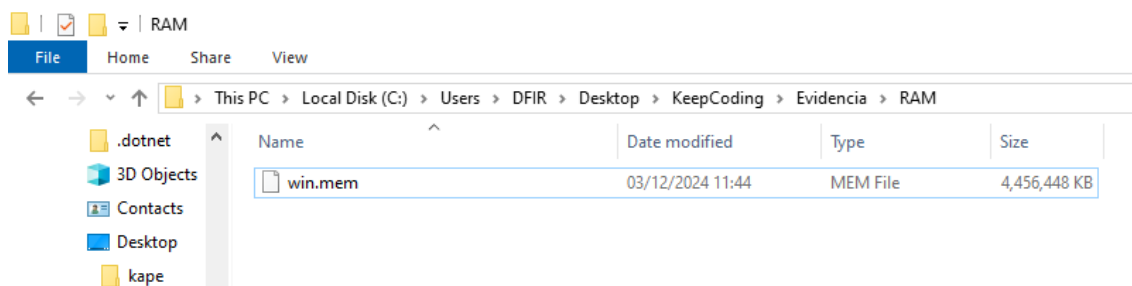


Imagen 18 Fichero Memoria Ram

Ahora para poder analizar dicha memoria nos podemos descargar el software **Volatility versión 3**, para ejecutarlo lo hacemos desde dónde tenemos descargado el software mediante una **cmd** y lo iniciamos con el comando **python vol.py -f + path** donde se encuentra nuestro archivo de la adquisición de la **RAM** y

procedemos a elegir el plugin deseado, para consultarlos se puede lanzar el comando de **python vol.py -h.**

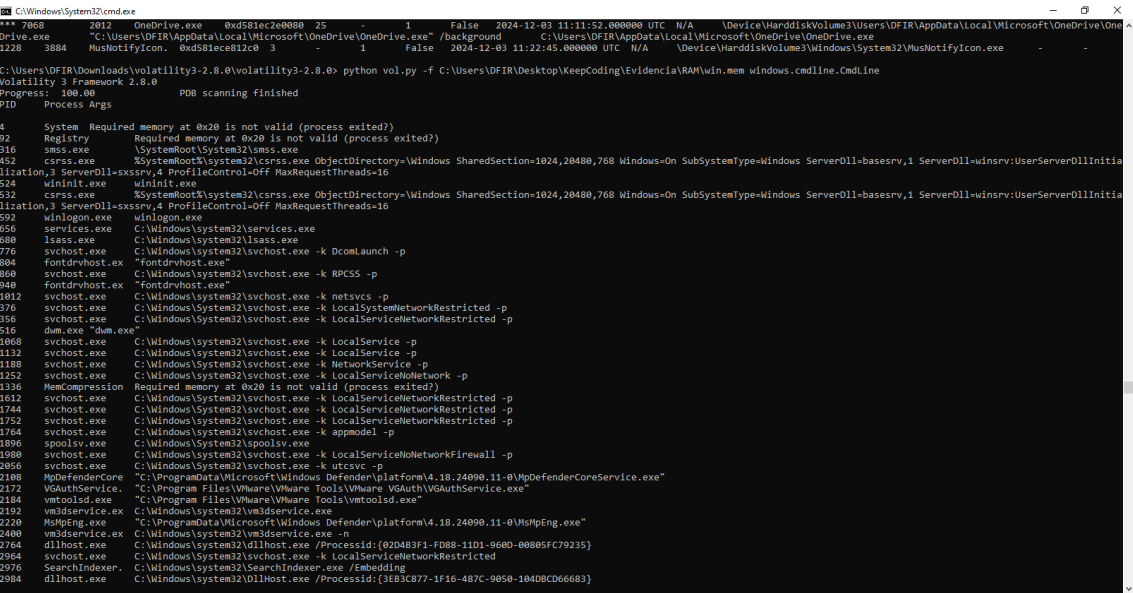


Imagen 19 InFo de plugins

Con el plugin **Windows.info** nos reporta la información que ha obtenido de la tabla de símbolos de nuestra memoria **RAM**.

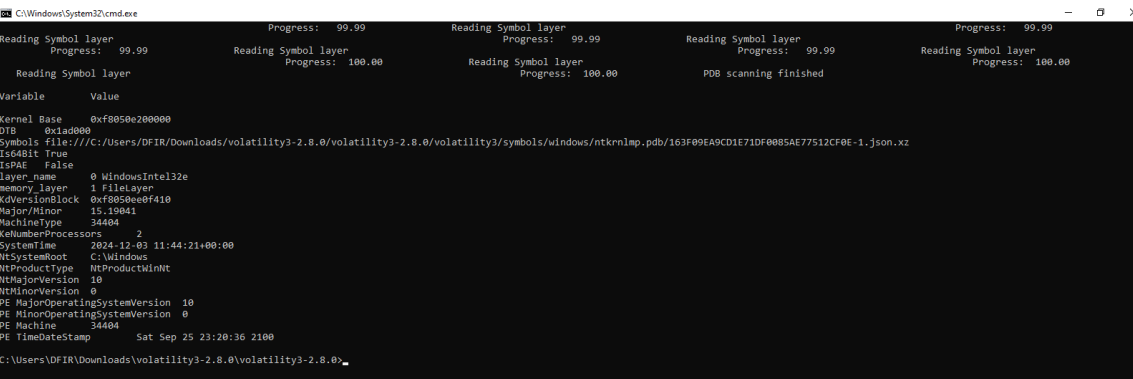


Imagen 20 Información de la memoria Ram de Windows

Otro plugin interesante es el de listado de procesos que se están ejecutando en la maquina en el momento de la adquisición **Windows.pslist.Pslist.**

C:\Windows\System32\cmd.exe

PE MinorOperatingSystemVersion 0  
PE Machine 54404  
PE TimeDateStamp Sat Sep 25 23:20:36 2100

C:\Users\DFIR\Downloads\volatility3-2.8.0\volatility3-2.8.0> python vol.py -f C:\Users\DFIR\Desktop\KeepCoding\Evidencia\RAM\win.mem windows.pslist

Volatility 3 Framework 2.8.0  
Progress: 100.00 PDB scanning finished

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	File output
4	0	System	0xd581e5a0a000	121	-	N/A	False	2024-12-03 11:10:47.000000 UTC	N/A	Disabled
92	4	Registry	0xd581e5a0b000	4	-	N/A	False	2024-12-03 11:10:42.000000 UTC	N/A	Disabled
516	4	smss.exe	0xd581e707a000	2	-	N/A	False	2024-12-03 11:10:47.000000 UTC	N/A	Disabled
452	444	csrss.exe	0xd581e9232300	11	-	0	False	2024-12-03 11:10:54.000000 UTC	N/A	Disabled
524	444	wininit.exe	0xd581e9105240	1	-	0	False	2024-12-03 11:10:55.000000 UTC	N/A	Disabled
532	516	csrss.exe	0xd581e9411240	13	-	1	False	2024-12-03 11:10:55.000000 UTC	N/A	Disabled
592	516	winlogon.exe	0xd581e9100300	5	-	1	False	2024-12-03 11:10:55.000000 UTC	N/A	Disabled
656	524	services.exe	0xd581e9cb30c0	8	-	0	False	2024-12-03 11:10:55.000000 UTC	N/A	Disabled
880	524	lsass.exe	0xd581e9cc2000	9	-	0	False	2024-12-03 11:10:55.000000 UTC	N/A	Disabled
776	656	svchost.exe	0xd581e9cc4200	18	-	0	False	2024-12-03 11:10:55.000000 UTC	N/A	Disabled
804	524	fontdrvhost.exe	0xd581e9d09180	5	-	0	False	2024-12-03 11:10:55.000000 UTC	N/A	Disabled
860	656	svchost.exe	0xd581e9dc0800	11	-	0	False	2024-12-03 11:10:55.000000 UTC	N/A	Disabled
940	592	fontdrvhost.exe	0xd581ea410100	5	-	1	False	2024-12-03 11:10:57.000000 UTC	N/A	Disabled
1012	656	svchost.exe	0xd581ea415200	66	-	0	False	2024-12-03 11:10:58.000000 UTC	N/A	Disabled
376	656	svchost.exe	0xd581ea446200	20	-	0	False	2024-12-03 11:10:58.000000 UTC	N/A	Disabled
1356	656	svchost.exe	0xd581ea4d3100	15	-	0	False	2024-12-03 11:10:58.000000 UTC	N/A	Disabled
516	592	dmv.exe	0xd581ea460000	10	-	1	False	2024-12-03 11:10:58.000000 UTC	N/A	Disabled
1068	656	svchost.exe	0xd581ea4b4300	19	-	0	False	2024-12-03 11:10:58.000000 UTC	N/A	Disabled
1132	656	svchost.exe	0xd581ea50c300	2	-	0	False	2024-12-03 11:10:58.000000 UTC	N/A	Disabled
1188	656	svchost.exe	0xd581ea570a00	15	-	0	False	2024-12-03 11:10:58.000000 UTC	N/A	Disabled
1252	656	svchost.exe	0xd581ea5c7000	15	-	0	False	2024-12-03 11:10:58.000000 UTC	N/A	Disabled
1336	4	MemCompression	0xd581ea530040	90	-	N/A	False	2024-12-03 11:10:58.000000 UTC	N/A	Disabled
1612	656	svchost.exe	0xd581ea63c100	12	-	0	False	2024-12-03 11:10:58.000000 UTC	N/A	Disabled
1744	656	svchost.exe	0xd581ea6d1000	3	-	0	False	2024-12-03 11:10:58.000000 UTC	N/A	Disabled
1752	656	svchost.exe	0xd581ea6d2000	7	-	0	False	2024-12-03 11:10:58.000000 UTC	N/A	Disabled
1764	656	svchost.exe	0xd581ea6e0000	7	-	0	False	2024-12-03 11:10:58.000000 UTC	N/A	Disabled
1896	656	spoolsv.exe	0xd581ea6bf000	7	-	0	False	2024-12-03 11:10:58.000000 UTC	N/A	Disabled
1980	656	svchost.exe	0xd581ea754300	12	-	0	False	2024-12-03 11:10:58.000000 UTC	N/A	Disabled
2056	656	svchost.exe	0xd581ea7d0700	14	-	0	False	2024-12-03 11:10:59.000000 UTC	N/A	Disabled
2108	656	WdFilterService.exe	0xd581ea822000	8	-	0	False	2024-12-03 11:10:59.000000 UTC	N/A	Disabled
2172	656	WdAuthService.exe	0xd581ea826340	2	-	0	False	2024-12-03 11:10:59.000000 UTC	N/A	Disabled
2184	656	vmtoolsd.exe	0xd581ea8292c0	12	-	0	False	2024-12-03 11:10:59.000000 UTC	N/A	Disabled
2192	656	vmtoolsd.exe	0xd581ea829200	3	-	0	False	2024-12-03 11:10:59.000000 UTC	N/A	Disabled
2220	656	MsMpEng.exe	0xd581ea82d000	24	-	0	False	2024-12-03 11:10:59.000000 UTC	N/A	Disabled
2400	2192	vmtoolsd.exe	0xd581ea906200	4	-	1	False	2024-12-03 11:10:59.000000 UTC	N/A	Disabled
2760	656	dllhost.exe	0xd581ea9bc1c0	12	-	0	False	2024-12-03 11:11:00.000000 UTC	N/A	Disabled
2864	656	svchost.exe	0xd581ea9c4300	5	-	0	False	2024-12-03 11:11:01.000000 UTC	N/A	Disabled
2976	656	SearchIndexer.exe	0xd581ea9c7f0c	18	-	0	False	2024-12-03 11:11:01.000000 UTC	N/A	Disabled
2984	776	dllhost.exe	0xd581ea9c0000	4	-	0	False	2024-12-03 11:11:01.000000 UTC	N/A	Disabled
1564	776	WmiPrvSE.exe	0xd581ea9c2c00	12	-	0	False	2024-12-03 11:11:01.000000 UTC	N/A	Disabled
3632	2056	AggregatorHost.exe	0xd581ea9f660c	1	-	0	False	2024-12-03 11:11:03.000000 UTC	N/A	Disabled

Imagen 21 Plugin de listado de procesos

Otro proceso relevante sería **windows.pstree.Pstree** que nos crea un árbol del proceso “Padre” y los procesos “hijos” y nos ayuda a trazar el histórico de ese proceso desde su inicio de ejecución hasta su finalización en el momento de la adquisición.

C:\Windows\System32\cmd.exe

1804 8372 winpmc\_mini\_x 0xd581e70a0000 3 - 1 False 2024-12-03 11:44:21.000000 UTC N/A Disabled

C:\Users\DFIR\Downloads\volatility3-2.8.0\volatility3-2.8.0> python vol.py -f C:\Users\DFIR\Desktop\KeepCoding\Evidencia\RAM\win.mem windows.pstree.Pstree

Volatility 3 Framework 2.8.0  
Progress: 100.00 PDB scanning finished

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	Audit	Cmd	Path
4	0	System	0xd581e5a0a000	121	-	N/A	False	2024-12-03 11:10:47.000000 UTC	N/A	-	-	-
* 1336	4	MemCompression	0xd581e5300040	90	-	N/A	False	2024-12-03 11:10:58.000000 UTC	N/A	-	MemCompression	-
* 92	4	Registry	0xd581e5a0b000	4	-	N/A	False	2024-12-03 11:10:42.000000 UTC	N/A	-	Registry	-
* 516	4	smss.exe	0xd581e707a000	2	-	N/A	False	2024-12-03 11:10:47.000000 UTC	N/A	-	-	-
ss.exe	SystemRoot\System32\smss.exe									-	-	\Device\HarddiskVolume3\Windows\System32\smss.exe
452	444	csrss.exe	0xd581e9232300	11	-	0	False	2024-12-03 11:10:54.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\csrss.exe
524	444	wininit.exe	0xd581e9105240	1	-	0	False	2024-12-03 11:10:55.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\wininit.exe
656	524	services.exe	0xd581e9cb30c0	8	-	0	False	2024-12-03 11:10:55.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\services.exe
880	524	lsass.exe	0xd581e9cc2000	9	-	0	False	2024-12-03 11:10:55.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\lsass.exe
776	656	svchost.exe	0xd581e9cc4200	18	-	0	False	2024-12-03 11:10:55.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\svchost.exe
804	524	fontdrvhost.exe	0xd581e9d09180	5	-	0	False	2024-12-03 11:10:55.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\fontdrvhost.exe
860	656	svchost.exe	0xd581e9dc0800	11	-	0	False	2024-12-03 11:10:55.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\svchost.exe
940	592	fontdrvhost.exe	0xd581ea410100	5	-	1	False	2024-12-03 11:10:57.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\fontdrvhost.exe
1012	656	svchost.exe	0xd581ea415200	66	-	0	False	2024-12-03 11:10:58.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\svchost.exe
376	656	svchost.exe	0xd581ea446200	20	-	0	False	2024-12-03 11:10:58.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\svchost.exe
1356	656	svchost.exe	0xd581ea4d3100	15	-	0	False	2024-12-03 11:10:58.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\svchost.exe
516	592	dmv.exe	0xd581ea460000	10	-	1	False	2024-12-03 11:10:58.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\dmv.exe
1068	656	svchost.exe	0xd581ea4b4300	19	-	0	False	2024-12-03 11:10:58.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\svchost.exe
1132	656	svchost.exe	0xd581ea50c300	2	-	0	False	2024-12-03 11:10:58.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\svchost.exe
1188	656	svchost.exe	0xd581ea570a00	15	-	0	False	2024-12-03 11:10:58.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\svchost.exe
1252	656	svchost.exe	0xd581ea5c7000	15	-	0	False	2024-12-03 11:10:58.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\svchost.exe
1336	4	MemCompression	0xd581ea530040	90	-	N/A	False	2024-12-03 11:10:58.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\MemCompression.exe
1612	656	svchost.exe	0xd581ea63c100	12	-	0	False	2024-12-03 11:10:58.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\svchost.exe
1744	656	svchost.exe	0xd581ea6d1000	3	-	0	False	2024-12-03 11:10:58.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\svchost.exe
1752	656	svchost.exe	0xd581ea6d2000	7	-	0	False	2024-12-03 11:10:58.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\svchost.exe
1764	656	svchost.exe	0xd581ea6e0000	7	-	0	False	2024-12-03 11:10:58.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\svchost.exe
1896	656	spoolsv.exe	0xd581ea6bf000	7	-	0	False	2024-12-03 11:10:58.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\spoolsv.exe
1980	656	svchost.exe	0xd581ea754300	12	-	0	False	2024-12-03 11:10:58.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\svchost.exe
2056	656	svchost.exe	0xd581ea7d0700	14	-	0	False	2024-12-03 11:10:59.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\svchost.exe
2108	656	WdFilterService.exe	0xd581ea822000	8	-	0	False	2024-12-03 11:10:59.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\WdFilterService.exe
2172	656	WdAuthService.exe	0xd581ea826340	2	-	0	False	2024-12-03 11:10:59.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\WdAuthService.exe
2184	656	vmtoolsd.exe	0xd581ea8292c0	12	-	0	False	2024-12-03 11:10:59.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\vmtoolsd.exe
2192	656	vmtoolsd.exe	0xd581ea829200	3	-	0	False	2024-12-03 11:10:59.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\vmtoolsd.exe
2220	656	MsMpEng.exe	0xd581ea82d000	24	-	0	False	2024-12-03 11:10:59.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\MsMpEng.exe
2400	2192	vmtoolsd.exe	0xd581ea906200	4	-	1	False	2024-12-03 11:10:59.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\vmtoolsd.exe
2760	656	dllhost.exe	0xd581ea9bc1c0	12	-	0	False	2024-12-03 11:11:00.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\dllhost.exe
2864	656	svchost.exe	0xd581ea9c4300	5	-	0	False	2024-12-03 11:11:01.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\svchost.exe
2976	656	SearchIndexer.exe	0xd581ea9c7f0c	18	-	0	False	2024-12-03 11:11:01.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\SearchIndexer.exe
2984	776	dllhost.exe	0xd581ea9c0000	4	-	0	False	2024-12-03 11:11:01.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\dllhost.exe
1564	776	WmiPrvSE.exe	0xd581ea9c2c00	12	-	0	False	2024-12-03 11:11:01.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\WmiPrvSE.exe
3632	2056	AggregatorHost.exe	0xd581ea9f660c	1	-	0	False	2024-12-03 11:11:03.000000 UTC	N/A	-	-	\Device\HarddiskVolume3\Windows\System32\AggregatorHost.exe

Imagen 22 Plugin de procesos en árbol

Y para finalizar tenemos el **windows.cmdline.Cmdline** en el podemos encontradas las ejecuciones realizadas a través de la consola de comandos, es importante ya que indica el proceso en el que el analista se ha conectado para poder realizar la adquisición de la memoria y se debe de documentar en el informe.

```
C:\Windows\System32\cmd.exe
6948 msedge.exe "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type-renderer --string-annotations-is-enterprise-managed-no --disable-gpu-compositing --video-capture-use-gpu-
memory-buffer --lang-en-GB --js-flags --ms-user-locale --device-scale-factor-1 --num-raster-threads-1 --renderer-client-id-32 --time-ticks-at-unix-epoch-1733224242327563 --launch-time-ticks-1057689
610 --field-trial-handle-6204,i,10625273453547775671,2637979996585203132,262144 --variations-seed-version --mojo-platform-channel-handle-6244 /prefetch:1
8188 msedge.exe "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type-renderer --string-annotations-is-enterprise-managed-no --disable-gpu-compositing --video-capture-use-gpu-
memory-buffer --lang-en-GB --js-flags --ms-user-locale --device-scale-factor-1 --num-raster-threads-1 --renderer-client-id-40 --time-ticks-at-unix-epoch-1733224242327563 --launch-time-ticks-1059255
671 --field-trial-handle-6396,i,10625273453547775671,2637979996585203132,262144 --variations-seed-version --mojo-platform-channel-handle-6468 /prefetch:1
8484 msedge.exe "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type-renderer --string-annotations-is-enterprise-managed-no --disable-gpu-compositing --video-capture-use-gpu-
memory-buffer --lang-en-GB --js-flags --ms-user-locale --device-scale-factor-1 --num-raster-threads-1 --renderer-client-id-31 --time-ticks-at-unix-epoch-1733224242327563 --launch-time-ticks-1062893
081 --field-trial-handle-6928,i,10625273453547775671,2637979996585203132,262144 --variations-seed-version --mojo-platform-channel-handle-9296 /prefetch:1
5132 msedge.exe "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type-renderer --string-annotations-is-enterprise-managed-no --disable-gpu-compositing --video-capture-use-gpu-
memory-buffer --lang-en-GB --js-flags --ms-user-locale --device-scale-factor-1 --num-raster-threads-1 --renderer-client-id-30 --time-ticks-at-unix-epoch-1733224242327563 --launch-time-ticks-1064837
164 --field-trial-handle-8996,i,10625273453547775671,2637979996585203132,262144 --variations-seed-version --mojo-platform-channel-handle-9368 /prefetch:1
5444 msedge.exe "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type-renderer --string-annotations-is-enterprise-managed-no --disable-gpu-compositing --video-capture-use-gpu-
memory-buffer --lang-en-GB --js-flags --ms-user-locale --device-scale-factor-1 --num-raster-threads-1 --renderer-client-id-49 --time-ticks-at-unix-epoch-1733224242327563 --launch-time-ticks-1067034
764 --field-trial-handle-8936,i,10625273453547775671,2637979996585203132,262144 --variations-seed-version --mojo-platform-channel-handle-8908 /prefetch:1
8086 msedge.exe "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type-renderer --string-annotations-is-enterprise-managed-no --disable-gpu-compositing --video-capture-use-gpu-
memory-buffer --lang-en-GB --js-flags --ms-user-locale --device-scale-factor-1 --num-raster-threads-1 --renderer-client-id-33 --time-ticks-at-unix-epoch-1733224242327563 --launch-time-ticks-1068421
854 --field-trial-handle-6940,i,10625273453547775671,2637979996585203132,262144 --variations-seed-version --mojo-platform-channel-handle-9376 /prefetch:1
2796 msedge.exe "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type-utility --utility-sub-type-edge_search_indexer.mojom.SearchIndexerInterfaceBroker --lang-en-GB --service-
index-type-search_indexer --message-loop-type-ui --string-annotations-is-enterprise-managed-no --field-trial-handle-8444,i,10625273453547775671,2637979996585203132,262144 --variations-seed-version
--mojo-platform-channel-handle-8432 /prefetch:8
1176 taskhostw.exe taskhostw.exe
5176 FileCobuth.exe "C:\Users\UDIR\AppData\Local\Microsoft\OneDrive\124.221.1183.8809\FileCobuth.exe" --Embedding
7556 dl1host.exe "C:\Windows\System32\DllHost.exe /Processid:{9730d807-5620-4489-B708-5A0F49CCDF3F}"
9588 msedge.exe "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type-renderer --string-annotations-is-enterprise-managed-no --disable-gpu-compositing --video-capture-use-gpu-
memory-buffer --lang-en-GB --js-flags --ms-user-locale --device-scale-factor-1 --num-raster-threads-1 --renderer-client-id-56 --time-ticks-at-unix-epoch-1733224242327563 --launch-time-ticks-1382855
741 --field-trial-handle-6556,i,10625273453547775671,2637979996585203132,262144 --variations-seed-version --mojo-platform-channel-handle-6088 /prefetch:1
4348 svchost.exe "C:\Windows\System32\svchost.exe -k wsappx -p"
8372 cmd.exe "C:\Windows\System32\cmd.exe"
8388 conhost.exe "C:\Windows\System32\conhost.exe 0x4"
5668 backgroundTask Process 5668: Required memory at 0x7890b464020 is not valid (incomplete layer memory_layer?)
8296 audiodg.exe "C:\Windows\System32\AUDIODG.EXE 0x30c"
8184 winpmem_mini_x winpmem_mini_x04_rc2.exe C:\Users\UDIR\Desktop\KeepCoding\Evidencia\RAM\win.mem

C:\Users\UDIR\Downloads\volatility3-2.8.0\volatility3-2.8.0_
```

Imagen 23 Plugin de CMD

La adquisición de la memoria RAM para un informe forense es crucial porque permite capturar datos volátiles que no se encuentran en el disco duro, como procesos en ejecución, conexiones activas y contenido de la memoria que puede ser relevante para la investigación. Este proceso, conocido como "adquisición en caliente", debe realizarse mientras el ordenador está encendido<sup>1</sup>. Herramientas como **FTK Imager** y **Dumplt** son comúnmente utilizadas para volcar la memoria RAM. Una vez adquirida, la integridad de los datos se verifica mediante el cálculo de hashes, y posteriormente se analizan con herramientas como **Volatility** para extraer información relevante como por ejemplo los procesos de ejecución, conexiones activas, procesos de la memoria, historial de usuario, claves criptográficas...

La memoria Ram nos genera multitud de información valiosa para nuestro análisis forense, como por ejemplo el dump del proceso, variables de entorno, etc..

