

# Práctica de Análisis Forense

## 1. Hash del Archivo

Como analistas forenses, el primer paso es obtener el hash SHA-256 de la evidencia.

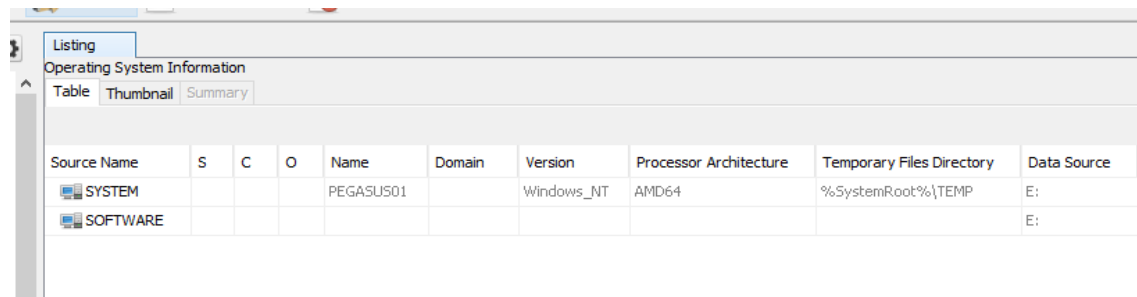


→ Con la Herramienta HashMyFiles le pasamos la evidencia y encontramos el Hash SHA-256 de la máquina

## 2. Nombre de la Máquina

Por favor, indiquen el nombre de la máquina bajo análisis.

Gracias a la Herramienta Autopsy de una forma fácil y sencilla nos otorga la información solicitada:



Aunque otra opción sería acceder al recurso de los registros de windows en:  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\ComputerName\Computer Name

En concreto a través del archivo SYSTEM alojado en Windows -> System32 -> Config ->

**SYSTEM**

### 3. Fecha de Descarga del Software de Control Remoto

¿En qué fecha se descargó el ejecutable de control remoto "TeamViewer\_Setup\_x64.exe"?

Formato de fecha: aaaa-mm-dd (por ejemplo, 2020-12-01)

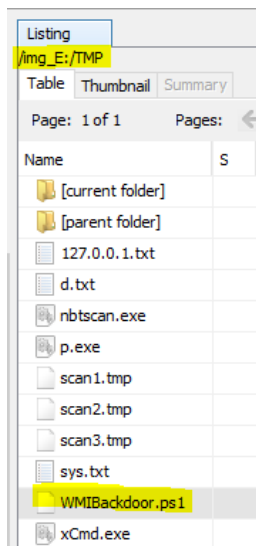


TeamViewer_Setup_x64.exe - Properties	
Properties	
Name	TeamViewer_Setup_x64.exe
S	(No Property Editor)
C	NO_COMMENT
O	0
Modified Time	2022-04-29 19:11:34 CEST
Change Time	2022-04-29 19:12:07 CEST
Access Time	2022-04-29 11:20:32 CEST
Created Time	2022-04-29 19:11:25 CEST

### 4. Ubicación de los Archivos Maliciosos

Se han identificado varios archivos maliciosos en la máquina. ¿En qué carpeta se encuentran estos archivos? (Por favor, proporciona solo el nombre de la carpeta)

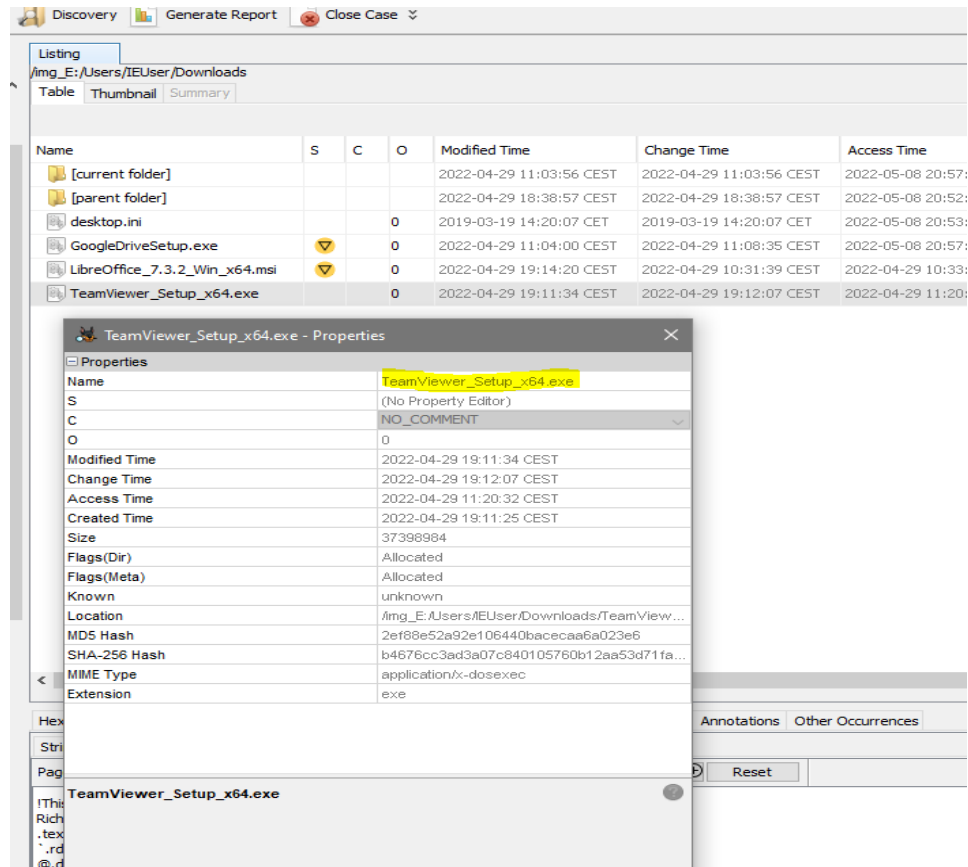
→ La razón por la que esta carpeta es una buena opción es porque los scripts que se ejecutan desde esta ubicación suelen tener privilegios más altos y pueden evadir ciertas medidas de seguridad. Además, los archivos temporales suelen tener menos restricciones de seguridad que otros archivos del sistema, lo que hace que sea más fácil para un atacante ejecutar un script malicioso sin ser detectado.



Listing	
/tmp	
Table	Thumbnail Summary
Page: 1 of 1 Pages: <	
Name	S
[current folder]	
[parent folder]	
127.0.0.1.txt	
d.txt	
nbtscan.exe	
p.exe	
scan1.tmp	
scan2.tmp	
scan3.tmp	
sys.txt	
WMIBackdoor.ps1	
xCmd.exe	

## 5. Nombre del Archivo del Programa de Control Remoto Descargado

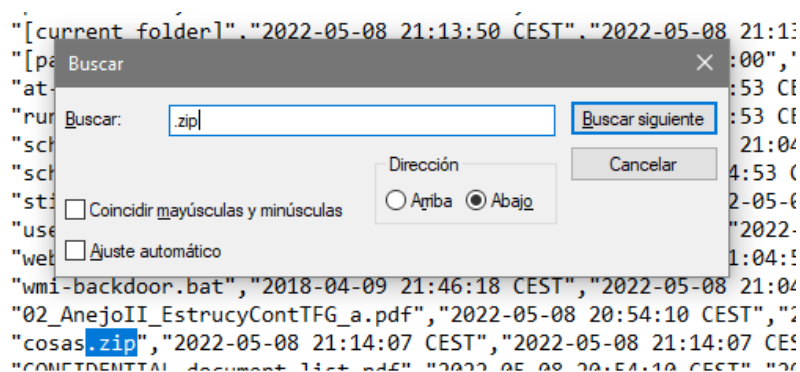
Proporcione el nombre del archivo .exe del programa de control remoto que fue descargado por el usuario.

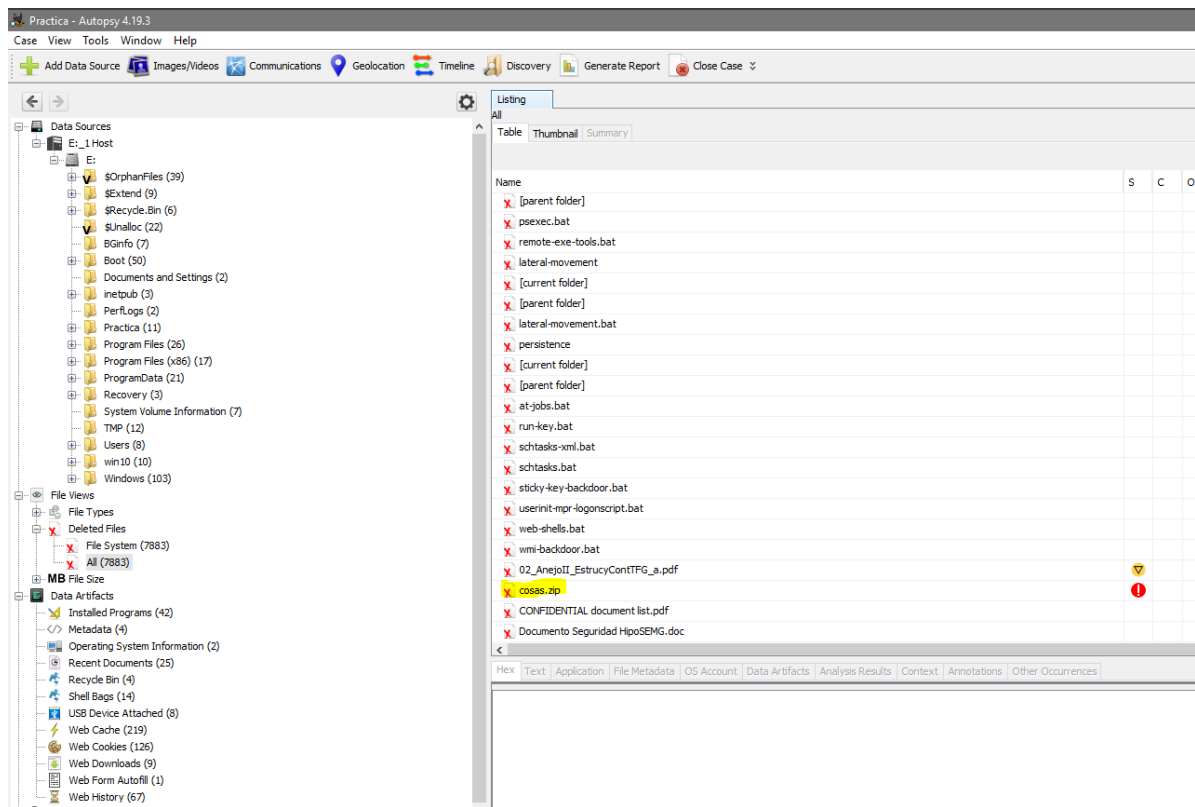


## 6. Archivos Eliminados

Existe la sospecha de que se haya eliminado un archivo .zip. ¿Podrías proporcionar el nombre de dicho archivo?

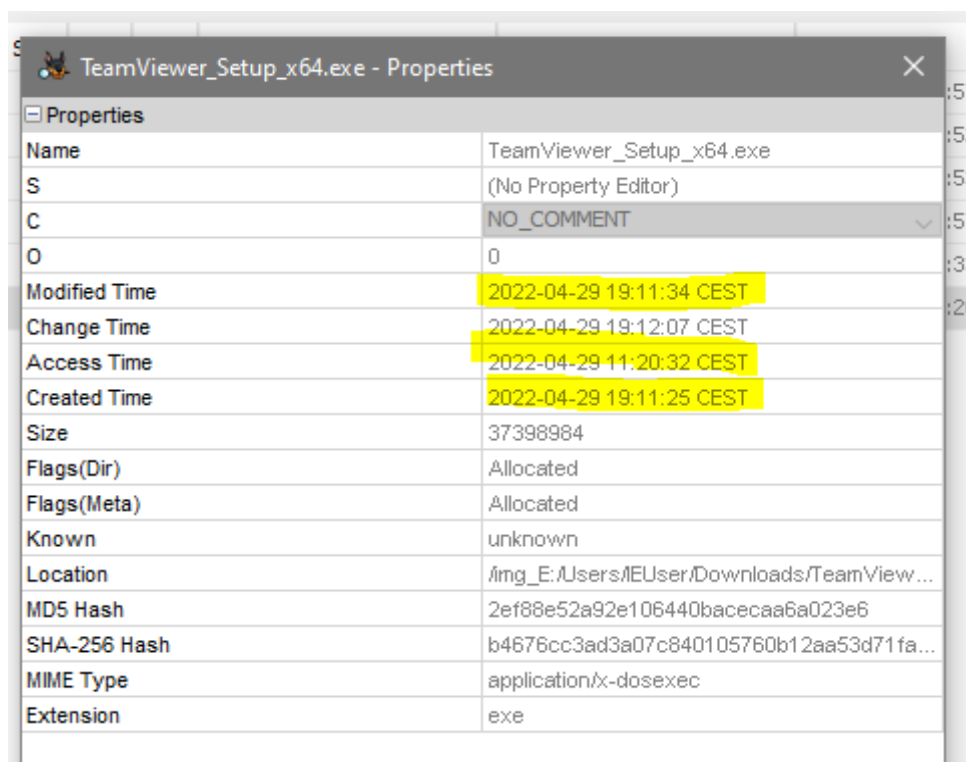
Autopsi nos brinda la opción de mostrar archivos eliminados, así que he exportado el csv, lo he abierto con el bloc de notas y he buscado por .zip





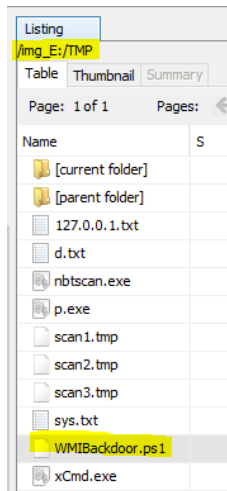
## 7. Fecha de Ejecución del Programa de Control Remoto

Se tiene constancia de que el programa TeamViewer fue ejecutado en el equipo.  
¿Podrían indicar la fecha en que se realizó esta ejecución? (Formato: dd/mm/aaaa)



## 8. Script Malicioso de PowerShell

Se ha identificado un script de PowerShell malicioso con la extensión .ps1 en el sistema. ¿Cuál es el nombre de este script?



No hay que ser un experto para saber que, si tmp es la carpeta por excelencia en Windows para alojar scripts maliciosos, el archivo ps1 que buscamos se encuentre ahí y más llamándose “Puerta trasera”.

## 9. Contraseña Débil

Existen sospechas de que la contraseña del usuario IEUser sea débil, lo que podría haber permitido al atacante acceder a ella. Por favor, proporcione la contraseña del usuario.

→ Usando Mimikatz le pasamos los archivos SYSTEM y SAM usando lsadump. Este nos arroja un hash el cual pasamos por una página web que nos saca la contraseña a partir de este hash: QWERTY

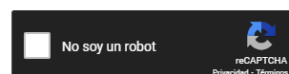
```
mimikatz # lsadump::sam /system:C:/SYSTEM /sam:C:/SAM
Domain : DESKTOP-SDN1RPT
SysKey : 43ab21a5faf16360d499d5c186882fa6
Local SID : S-1-5-21-321011808-3761883066-353627080
```

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

### Free Password Hash Cracker

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

2d20d252a479f485cdf5e171d93985bf



Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, 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

## 10. ID de Conexión del Programa de Control Remoto

Se sospecha que ha habido una conexión al equipo desde un programa de control remoto. ¿Podrían proporcionar el ID desde el que se ha realizado esta conexión?

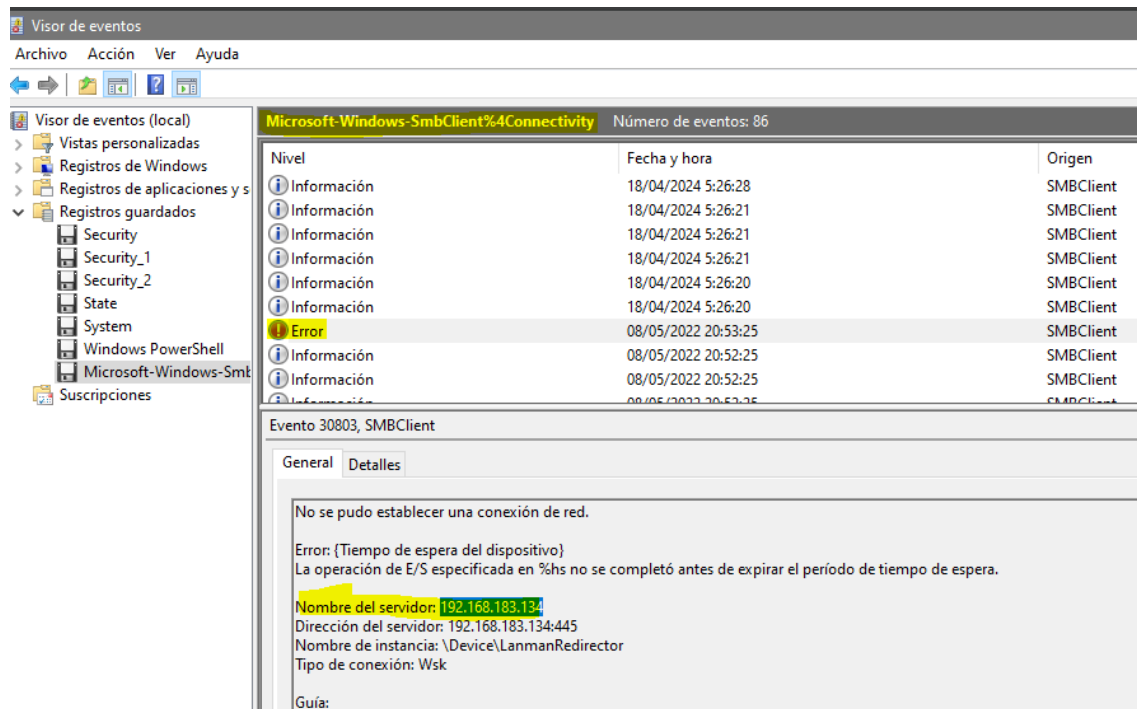
ID	Source	Date/Time	User/Program
765418952	WIN-MORENIN	29-04-2022 10:09:14	IEUser RemoteControl
765418952	WIN-MORENIN	29-04-2022 10:10:34	IEUser RemoteControl
		29-04-2022 10:13:21	IEUser RemoteControl

Dentro de la carpeta donde se aloja TeamViewer podemos encontrar un LOG que nos proporciona los ID de los diferentes equipos desde los que se ha realizado una conexión.

## 11. Conexión RDP

Se ha detectado actividad sospechosa en la red. ¿Podrían proporcionar la dirección IP desde la que se ha realizado la conexión a la máquina a través de RDP?

Name	S	C	O
Microsoft-Windows-Resource-Exhaustion-Resolver%4Operational.evtx			0
Microsoft-Windows-RestartManager%4Operational.evtx			1
Microsoft-Windows-Security-LessPrivilegedAppContainer%4Operational.evtx			0
Microsoft-Windows-Security-Mitigations%4KernelMode.evtx			0
Microsoft-Windows-Security-Mitigations%4UserMode.evtx			1
Microsoft-Windows-Security-SPP-UX-Notifications%4ActionCenter.evtx			0
Microsoft-Windows-SettingSync%4Debug.evtx			0
Microsoft-Windows-SettingSync%4Operational.evtx			0
Microsoft-Windows-Shell-ConnectedAccountState%4ActionCenter.evtx			1
Microsoft-Windows-Shell-Core%4ActionCenter.evtx			1
Microsoft-Windows-Shell-Core%4AppDefaults.evtx			0
Microsoft-Windows-Shell-Core%4LogonTasksChannel.evtx			1
Microsoft-Windows-Shell-Core%4Operational.evtx			0
Microsoft-Windows-ShellCommon-StartLayoutPopulation%4Operational.evtx			0
Microsoft-Windows-SmbClient%4Audit.evtx			1
Microsoft-Windows-SmbClient%4Connectivity.evtx			0
Microsoft-Windows-SMBClient%4Operational.evtx			0
Microsoft-Windows-SmbClient%4Security.evtx			0
Microsoft-Windows-SMBServer%4Audit.evtx			1



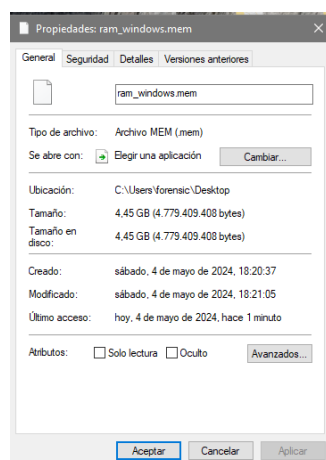
Dado que no encontraba donde se podía alojar el evento de conexiones RDP decidí hacer una búsqueda a través de otros protocolos en busca de actividad extraña, aunque la captura que adjunto no responde del todo a la pregunta, he conseguido encontrar la dirección IP bajo un puerto operando a través del protocolo SMB.

## Práctica memoria Ram

Para este apartado de la práctica, debéis de hacer una adquisición de memoria ram sobre el sistema operativo a vuestra elección.

Se deberán indicar los pasos seguidos para la realización de la adquisición, así como la ejecución de mínimo dos comandos con volatility.

```
C:\Users\forensic\Desktop>winpmem_mini_x64_rc2.exe ram_windows.mem
```



## Ejecución de PSLIST

→ Gracias a PSLIST podemos extraer la información de los procesos que se encontraban en ejecución al capturar la “imagen” de la memoria.

→ Por ejemplo podemos ver la ejecución de un proceso de virtual box para facilitar la comunicación con el anfitrión a través de las guetsAdditions

```
C:\Users\forensic\Downloads\volatility3-2.5.2\volatility3-2.5.2>python vol.py -f C:\Users\forensic\Desktop\mem_ram\ram_windows.mem windows.pslist.PsList
```

Progress: 100.00			PDB scanning finished										
PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	File output			
4	0	System	0x92022f07b080 161	-	N/A	False	2024-04-29 20:12:35.000000	N/A	Disabled				
92	4	Registry	0x92022f1e3040 4	-	N/A	False	2024-04-29 20:12:33.000000	N/A	Disabled				
392	4	smss.exe	0x92022fdcc040 2	-	N/A	False	2024-04-29 20:12:35.000000	N/A	Disabled				
584	488	csrss.exe	0x920230be8080 11	-	0	False	2024-04-29 20:12:42.000000	N/A	Disabled				
580	488	wininit.exe	0x920235b1e080 1	-	0	False	2024-04-29 20:12:42.000000	N/A	Disabled				
592	572	csrss.exe	0x920235b5e0c0 12	-	1	False	2024-04-29 20:12:42.000000	N/A	Disabled				
576	572	winlogon.exe	0x920235b65080 5	-	1	False	2024-04-29 20:12:42.000000	N/A	Disabled				
712	580	services.exe	0x920235b68080 10	-	0	False	2024-04-29 20:12:42.000000	N/A	Disabled				
720	580	lsass.exe	0x920235b6b080 11	-	0	False	2024-04-29 20:12:42.000000	N/A	Disabled				
840	712	svchost.exe	0x920235be1240 21	-	0	False	2024-04-29 20:12:43.000000	N/A	Disabled				
848	580	fontdrvhost.exe	0x920235bec080 5	-	0	False	2024-04-29 20:12:43.000000	N/A	Disabled				
856	676	fontdrvhost.exe	0x920235be1440 5	-	1	False	2024-04-29 20:12:43.000000	N/A	Disabled				
952	712	svchost.exe	0x9202362852c0 15	-	0	False	2024-04-29 20:12:43.000000	N/A	Disabled				
1004	712	svchost.exe	0x9202361ea240 5	-	0	False	2024-04-29 20:12:43.000000	N/A	Disabled				
8	676	dmw.exe	0x92023e0f2080 17	-	1	False	2024-04-29 20:12:44.000000	N/A	Disabled				
828	712	svchost.exe	0x920236288240 0	-	0	False	2024-04-29 20:12:44.000000	2024-04-29 21:16:25.000000					
1040	712	svchost.exe	0x9202362eb2c0 3	-	0	False	2024-04-29 20:12:44.000000	N/A	Disabled				
1096	712	svchost.exe	0x92023c1e3280 2	-	0	False	2024-04-29 20:12:44.000000	N/A	Disabled				
1108	712	svchost.exe	0x92023b0f4380 4	-	0	False	2024-04-29 20:12:44.000000	N/A	Disabled				
1168	712	svchost.exe	0x92023b304380 8	-	0	False	2024-04-29 20:12:44.000000	N/A	Disabled				
1228	712	svchost.exe	0x92023d3d8380 2	-	0	False	2024-04-29 20:12:44.000000	N/A	Disabled				
1276	712	svchost.exe	0x92023d3c20c0 5	-	0	False	2024-04-29 20:12:44.000000	N/A	Disabled				
1328	712	svchost.exe	0x92023e219380 7	-	0	False	2024-04-29 20:12:44.000000	N/A	Disabled				
1340	712	svchost.exe	0x92023e221280 2	-	0	False	2024-04-29 20:12:44.000000	N/A	Disabled				
1456	712	svchost.exe	0x92023c4f12c0 7	-	0	False	2024-04-29 20:12:44.000000	N/A	Disabled				
1484	712	svchost.exe	0x92022f664080 15	-	0	False	2024-04-29 20:12:44.000000	N/A	Disabled				
1600	712	VBoxService.exe	0x92022f079080 11	-	0	False	2024-04-29 20:12:44.000000	N/A	Disabled				
1616	712	svchost.exe	0x92023bbce2c0 9	-	0	False	2024-04-29 20:12:44.000000	N/A	Disabled				
1640	712	svchost.exe	0x92023b3c4080 5	-	0	False	2024-04-29 20:12:44.000000	N/A	Disabled				
1668	712	svchost.exe	0x92023bbd12c0 7	-	0	False	2024-04-29 20:12:44.000000	N/A	Disabled				
1680	712	svchost.exe	0x92023bbc4080 5	-	0	False	2024-04-29 20:12:44.000000	N/A	Disabled				

## Ejecución de PSTREE

→ PSTREE nos ofrece un árbol de los procesos permitiéndonos así ver de una manera más clara como están organizados los procesos en el sistema.

```
C:\Users\forensic\Downloads\volatility3-2.5.2\volatility3-2.5.2>python vol.py -f C:\Users\forensic\Desktop\mem_ram\ram_windows.mem windows.pstree.PsTree
```

Progress: 100.00	PID	PPID	ImageFileName	PDB	scanning finished	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime
4	0		System	0x92022f07b080	161	-	-	N/A	False	2024-04-29 20:12:35.000000	N/A	
* 392	4		smss.exe	0x92022fdcc040	2	-	-	N/A	False	2024-04-29 20:12:35.000000	N/A	N/A
* 1816	4		MemCompression	0x92023e0bf080	22	-	-	N/A	False	2024-04-29 20:12:44.000000	N/A	N/A
* 92	4		Registry	0x92022f1e3040	4	-	-	N/A	False	2024-04-29 20:12:33.000000	N/A	N/A
* 584	488		csrss.exe	0x920230be8080	11	-	-	0	False	2024-04-29 20:12:42.000000	N/A	N/A
* 580	488		wininit.exe	0x920235b1e080	1	-	-	0	False	2024-04-29 20:12:42.000000	N/A	N/A
* 712	580		services.exe	0x920235b68080	10	-	-	0	False	2024-04-29 20:12:42.000000	N/A	N/A
* 1040	712		svchost.exe	0x92023c1eb2c0	3	-	-	0	False	2024-04-29 20:12:44.000000	N/A	N/A
* 8216	712		svchost.exe	0x920230dc2280	10	-	-	0	False	2024-05-02 20:15:41.000000	N/A	N/A
* 2092	712		svchost.exe	0x92023dbf240	9	-	-	0	False	2024-04-29 20:12:44.000000	N/A	N/A
** 4208	2092		sihost.exe	0x92023b461080	13	-	1	False	2024-04-29 20:12:48.000000	N/A	N/A	N/A
** 3116	712		svchost.exe	0x92023e281240	5	-	-	0	False	2024-04-29 20:12:45.000000	N/A	N/A
** 3128	712		svchost.exe	0x92023e282080	12	-	-	0	False	2024-04-29 20:12:45.000000	N/A	N/A
* 1600	712		VBoxService.exe	0x92022f079080	11	-	-	0	False	2024-04-29 20:12:44.000000	N/A	N/A
* 7236	712		svchost.exe	0x92023b1b6080	4	-	-	0	False	2024-04-29 20:27:47.000000	N/A	N/A
* 1096	712		svchost.exe	0x92023c1e3280	2	-	-	0	False	2024-04-29 20:12:44.000000	N/A	N/A
* 1616	712		svchost.exe	0x92023bbce2c0	9	-	-	0	False	2024-04-29 20:12:44.000000	N/A	N/A
* 1108	712		svchost.exe	0x92023b0f4380	4	-	-	0	False	2024-04-29 20:12:44.000000	N/A	N/A
* 3668	712		svchost.exe	0x92023a426380	12	-	-	0	False	2024-04-29 20:12:46.000000	N/A	N/A
* 1640	712		svchost.exe	0x92023bbcf080	5	-	-	0	False	2024-04-29 20:12:44.000000	N/A	N/A
* 6760	712		svchost.exe	0x92023b159340	4	-	-	0	False	2024-04-29 20:14:47.000000	N/A	N/A
* 4724	712		svchost.exe	0x92023c1b5280	4	-	-	0	False	2024-04-29 20:12:48.000000	N/A	N/A
** 4816	4724		ctfmon.exe	0x92023b48d2c0	11	-	1	False	2024-04-29 20:12:49.000000	N/A	N/A	N/A
* 1668	712		svchost.exe	0x92023bbd12c0	7	-	-	0	False	2024-04-29 20:12:44.000000	N/A	N/A
* 3716	712		svchost.exe	0x92023b246380	3	-	-	0	False	2024-04-29 20:12:47.000000	N/A	N/A
* 1168	712		svchost.exe	0x92023b304380	8	-	-	0	False	2024-04-29 20:12:44.000000	N/A	N/A
* 1680	712		svchost.exe	0x92023bbc4080	5	-	-	0	False	2024-04-29 20:12:44.000000	N/A	N/A
* 2196	712		svchost.exe	0x92023b04f240	6	-	-	0	False	2024-04-29 20:12:44.000000	N/A	N/A
* 4252	712		svchost.exe	0x92023b48a340	9	-	1	False	2024-04-29 20:12:48.000000	N/A	N/A	N/A
* 3744	712		svchost.exe	0x92023b2482c0	2	-	-	0	False	2024-04-29 20:12:47.000000	N/A	N/A
* 1704	712		svchost.exe	0x92023bbc6080	4	-	-	0	False	2024-04-29 20:12:44.000000	N/A	N/A

## Ejecución de CMDLINE

→ Con CMDLINE podemos extraer la línea de comandos asociada a cada proceso registrado en la imagen de la memoria.

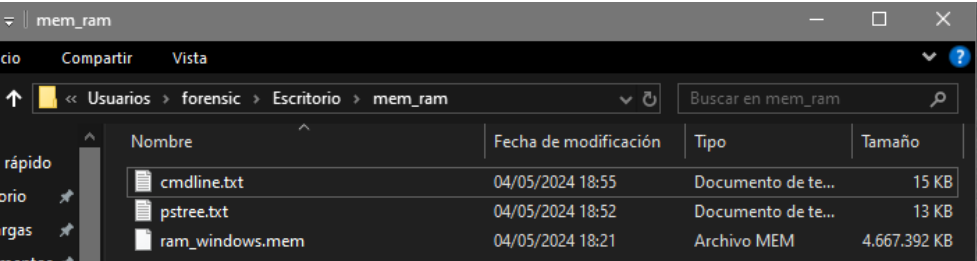
```
C:\Users\forensic\Downloads\volatility3-2.5.2\volatility3-2.5.2>python vol.py -f C:\Users\forensic\Desktop\mem_ram\ram_windows.mem windows.cmdline.CmdLine
```



```
Volatility 3 Framework 2.5.2

PID    Process Args
4      System Required memory at 0x20 is not valid (process exited?)
92     Registry Required memory at 0x20 is not valid (process exited?)
392    smss.exe \SystemRoot\System32\smss.exe
504    csrss.exe \SystemRoot\System32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows-On SubSystemType=Windows ServerDll=base
580    wininit.exe
592    csrss.exe \SystemRoot\System32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows-On SubSystemType=Windows ServerDll=base
676    winlogon.exe
712    services.exe C:\WINDOWS\system32\services.exe
720    lsass.exe C:\WINDOWS\system32\lsass.exe
840    svchost.exe C:\WINDOWS\system32\svchost.exe -k DcomLaunch -p
848    fontdrvhost.exe "fontdrvhost.exe"
856    fontdrvhost.exe C:\WINDOWS\system32\svchost.exe -k RPCSS -p
952    svchost.exe C:\WINDOWS\system32\svchost.exe -k DcomLaunch -p -s LSM
1004   dm.exe "dm.exe"
828    svchost.exe Required memory at 0x5772e0020 is not valid (process exited?)
1040   svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalServiceNetwork -p
1096   svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
1108   svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc
1168   svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog
1208   svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalService -p -s DisplayBrokerDesktopSvc
1276   svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalService -p -s nsi
1328   svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp
1340   svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s DevQueryBroker
1456   svchost.exe C:\WINDOWS\system32\svchost.exe -k NetworkService -p -s RlaSvc
1484   svchost.exe C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s Schedule
1600   VBoxService.exe C:\WINDOWS\system32\VBoxService.exe
1616   svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalService -p -s netprofm
1640   svchost.exe C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s ProfSvc
1668   svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalService -p -s EventSystem
1680   svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s SysMain
1784   svchost.exe C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s Themes
1816   MemCompression Required memory at 0x20 is not valid (process exited?)
1836   svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalService -p
1864   svchost.exe C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s SEHS
1900   svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s AudioEndpointBuilder
1932   svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalService -p -s FontCache
1900   svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p
2092   svchost.exe C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s UserManager
```

Carpeta con los output de un par de plugins de Volatiliti y un registro (.MEM) de la memoria RAM.



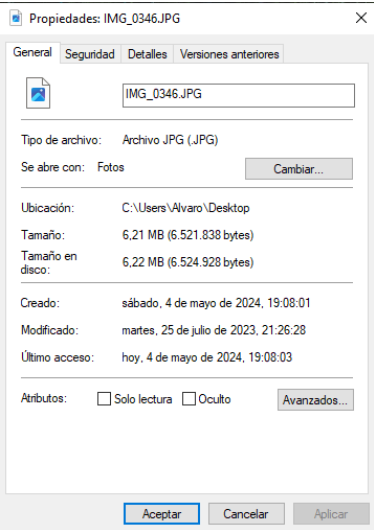
# Práctica Metadatos

La idea de este ejercicio es examinar cómo las plataformas de mensajería quitan una serie de

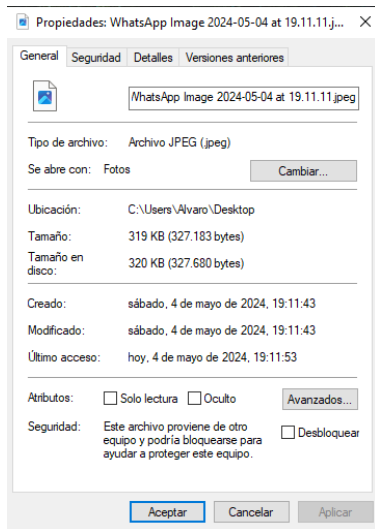
metadatos cuando las enviamos entre unas y otras.

Necesito que hagáis una prueba con una foto vuestra:

1. Miréis los metadatos que tiene inicialmente

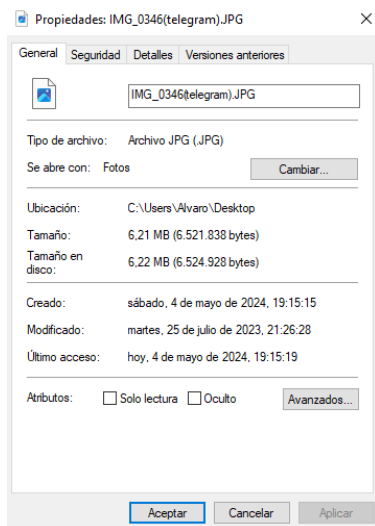


## 2. La envíen por whatsapp y los volváis a mirar



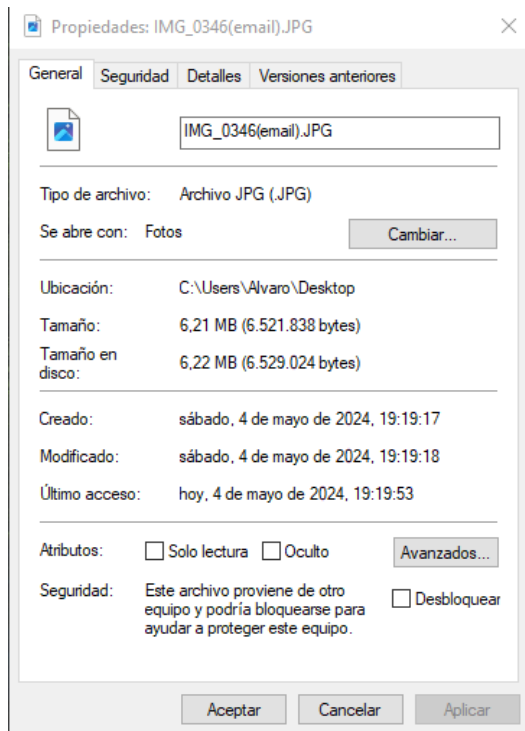
→La fecha de modificación, creación y tamaño han cambiado (Ha cambiado incluso el nombre del archivo).

## 3. La envíen por telegram y lo volváis a comparar



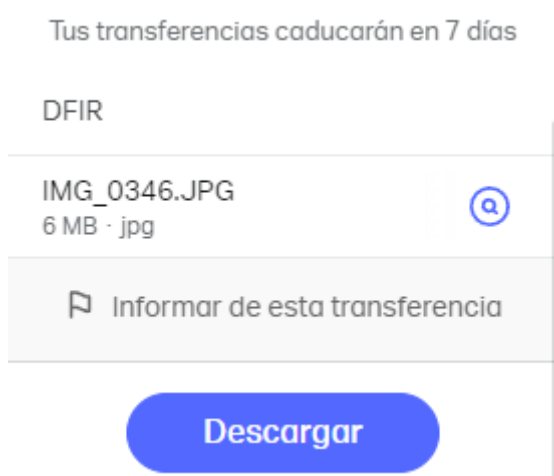
→La fecha de creación se ha modificado, pero tanto la fecha de modificación como el tamaño han permanecido intactos.

## 4. La enviéis por email y la comparáis



→ En este caso ocurre algo parecido que, en WhatsApp, con la diferencia de que mantenemos toda la calidad original del archivo.

## 5.A través de Wetransfer



→ En este caso ocurre exactamente que con el email.

