

# **KeepCoding Bootcamp Ciberseguridad | Edición IX**

## **Módulo DFIR**

### **Informe de Práctica Final**

**Auditor: Oscar Uriel Tobar Rios**

**Fecha del Informe: 12/04/2025**

## Contenido

1	Challenges .....	4
2	Forensic .....	4
2.1	Hash del Fichero .....	4
2.1.1	Solución.....	4
2.2	Nombre de la Maquina .....	5
2.2.1	Solución.....	5
2.3	Ficheros Maliciosos.....	5
2.3.1	Solución.....	6
2.4	Descarga fichero de control remoto .....	12
2.4.1	Solución.....	12
2.5	Fecha de ejecución programa .....	13
2.5.1	Solución.....	13
2.6	Ficheros Eliminados .....	14
2.6.1	Solución.....	14
2.7	Contraseñas Débiles .....	15
2.7.1	Solución.....	16
2.8	Conexión RDP .....	19
2.8.1	Solución.....	19
3	RAM .....	20
3.1	Winpmem .....	20
3.1.1	Solución.....	20
3.2	Proceso Malicioso .....	23
3.2.1	Solución.....	23
3.3	Proceso hijo .....	25
3.3.1	Solución.....	25
3.4	Líneas de comandos .....	25
3.5	IP del C2C .....	28
3.5.1	Solución.....	28
4	Practica Metadatos.....	29
4.1	Solución .....	29
4.1.1	WhatsApp .....	30
4.1.2	Email .....	31

4.1.3	Microsoft Team.....	32
4.1.4	Telegram .....	33

# 1 Challenges

Que ejecutaron los siguientes challenges para el usuario Otoibar1 correo otobar@hotmail.com

**Ram**

Challenge	Status	Score
Proceso malicioso	✓	15
Proceso hijo	✓	15
IP del C2C	✓	20
Hash del archivo		25
Fecha de ejecución		30
Offset del proceso		40

**Forensic**

Challenge	Status	Score
Hash del fichero	✓	10
Nombre de la máquina	✓	10
Fecha descarga software control remoto	✓	10
Ficheros maliciosos	✓	15
Descarga fichero de control remoto	✓	15
Ficheros eliminados	✓	15
Puerto de conexión máquina a máquina	✓	15
Fecha de ejecución programa control remoto	✓	20
Powershell maliciosa	✓	25
Contraseñas débiles	✓	25
Conexión programa control remoto		30
Conexión RDP	✓	30

Activar Windows  
Ve a Configuración pa

## 2 Forensic

### 2.1 Hash del Fichero

Como analistas de la máquina, lo primero que debemos obtener es el hash sha-256 de la evidencia. Recordatorio: Estamos trabajando con una imagen, el archivo que os habéis descargado es un disco duro virtual pero lo tenéis que tratar como si de una imagen forense se tratase, no como un disco duro de una máquina virtual.

#### 2.1.1 Solución

En Windows abro el PowerShell

Ahí Escribe Get-FileHash seguido de un espacio y luego el path de la imagen

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

PS C:\Users\PC> Get-FileHash C:\Users\PC\Downloads\Win10_PC001.vmdk

Algorithm      Hash
-----
SHA256         4446E9C42345A32FA78A8CE20834FAA047A3B161EBA986F894D2230FCF680CBE
Path
-----
C:\Users\PC\Downloads\Win10_P...

PS C:\Users\PC>
```

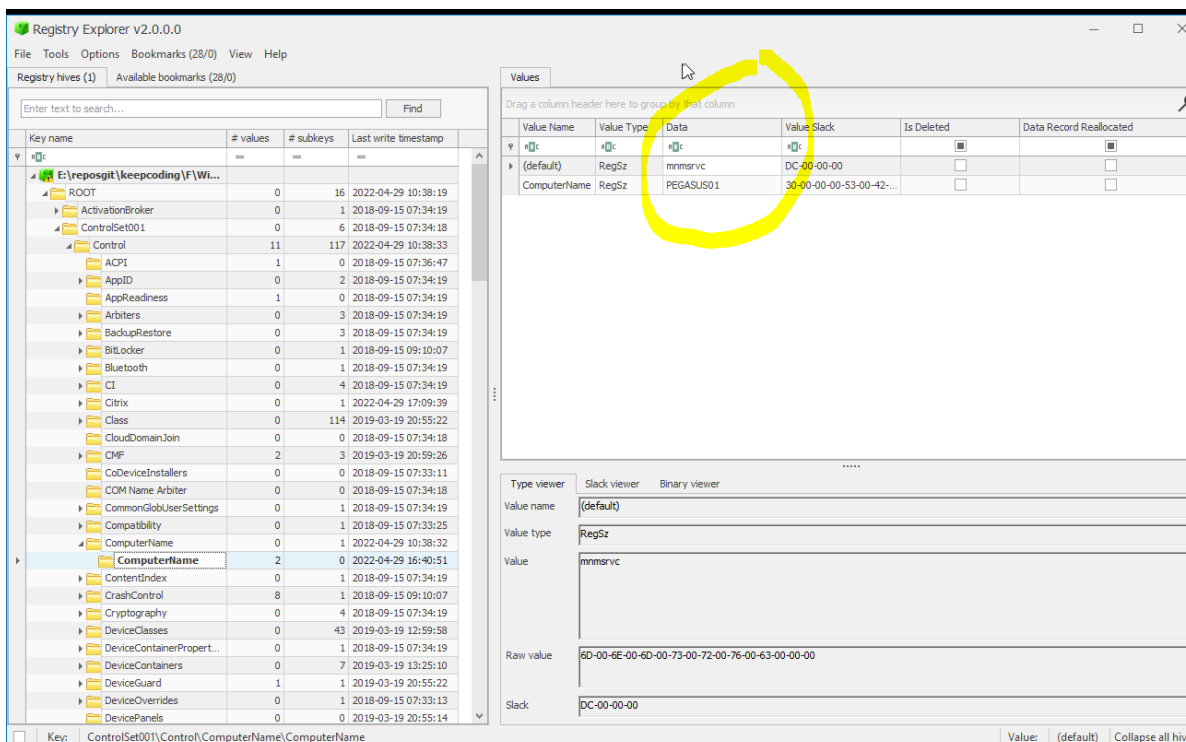
## 2.2 Nombre de la Maquina

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

### 2.2.1 Solución

El uso de Usando Windows Registry Recovery (WRR) no funciono forme generaba error de pantalla azul. Por lo tanto se uso el Registry Explorer, donde se cargo el archivo SYSTEM de F:\windows\System32\config.

A continuación esta la imagen donde se encontró el nombre del equipo:

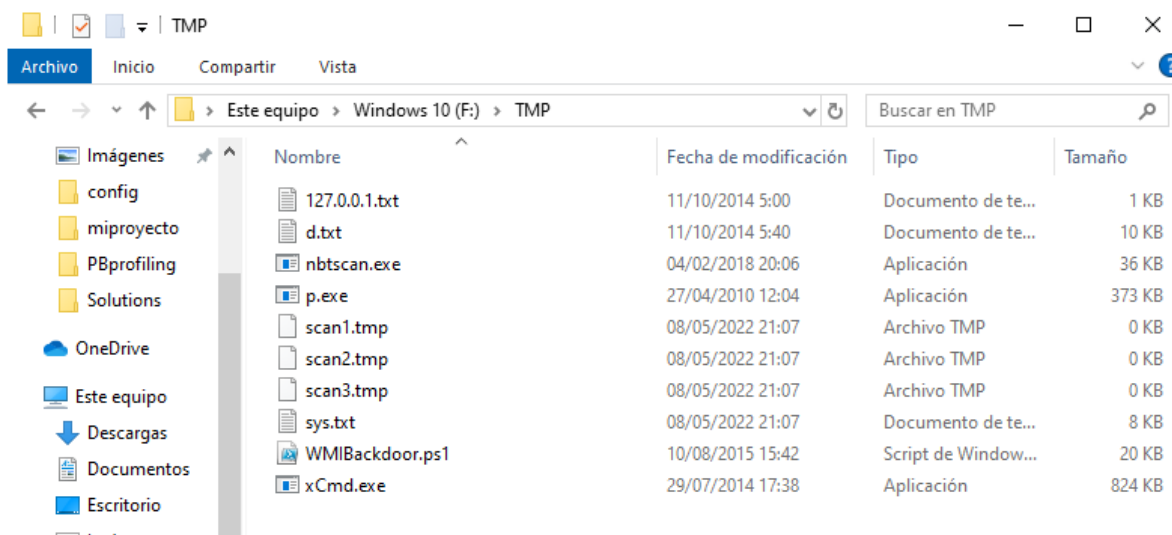


## 2.3 Ficheros Maliciosos

En la máquina se han encontrado varios ficheros maliciosos.

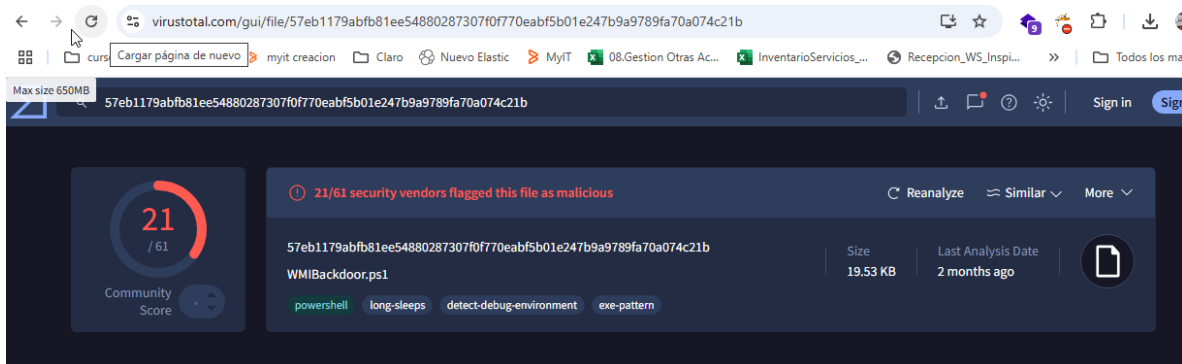
En que carpeta (solamente el nombre de la carpeta) se encuentran dichos ficheros?

## 2.3.1 Solución



### 2.3.1.1 Archivo WMIBackDoor.ps1

El archivo TMP\WMIBackDoor.ps1 se reviso en Visustotal.com y se encontró que es un archivo malicioso



Popular threat label ⓘ trojan.genericfca/powershell		Threat categories	trojan	hacktool	Family labels	genericfca	powershell	nexttronsystems
Security vendors' analysis ⓘ					Do you want to automate checks?			
AliCloud	ⓘ	Trojan:Win/Agent.F#	ALYac	ⓘ	Trojan.GenericFCA-Agent.125393			
Arcabit	ⓘ	Trojan.GenericFCA.Agent.D1E9D1	BitDefender	ⓘ	Trojan.GenericFCA-Agent.125393			
CTX	ⓘ	Powershell.trojan.genericfca	Emsisoft	ⓘ	Trojan.GenericFCA-Agent.125393 (B)			
eScan	ⓘ	Trojan.GenericFCA.Agent.125393	ESET-NOD32	ⓘ	PowerShell/Agent.FF			
GData	ⓘ	PowerShell.Trojan.WMIBackdoor.B	Google	ⓘ	Detected			
Ikarus	ⓘ	Trojan.PowerShell.Agent	Lionic	ⓘ	Trojan.Script.GenericFCA.4lc			
QuickHeal	ⓘ	Autoruninf.Trojan.A13522433	Rising	ⓘ	Trojan.Agent!B.B1E (TOPIS:E0:FMeizg.JP...			
Skyhigh (SWG)	ⓘ	Artemis!Trojan	Symantec	ⓘ	Hacktool			

Skyhigh (SWG)	ⓘ	Artemis!Trojan	Symantec	ⓘ	Hacktool			
Trellix (HX)	ⓘ	Trojan.GenericFCA.Agent.125393	TrendMicro	ⓘ	HackTool.PS1.NextronSystems.A			
TrendMicro-HouseCall	ⓘ	HackTool.PS1.NextronSystems.A	Varist	ⓘ	ABTrojan.UTVY-			
VIPRE	ⓘ	Trojan.GenericFCA.Agent.125393	Acronis (Static ML)	✓	Undetected			
AhnLab-V3	✓	Undetected	Antiy-AVL	✓	Undetected			
Avast	✓	Undetected	AVG	✓	Undetected			
Avira (no cloud)	✓	Undetected	Baidu	✓	Undetected			
Bkav Pro	✓	Undetected	ClamAV	✓	Undetected			
CMC	✓	Undetected	CrowdStrike Falcon	✓	Undetected			
Cynet	✓	Undetected	DrWeb	✓	Undetected			
Fortinet	✓	Undetected	Gridinsoft (no cloud)	✓	Undetected			
Huorong	✓	Undetected	Jiangmin	✓	Undetected			

### 2.3.1.2 Archivo xCmd.exe

El archivo TMP\cCmd.exe se revisó en Visustotal.com y se encontró que es un archivo malicioso

60

/ 73

Community Score

60/73 security vendors flagged this file as malicious

Reanalyze Similar More

6c8eea3ba31463a04d041f4c9ff50b50d9b5945d3306fee35fb4b5bfd292692b

Size 824.00 KB

Last Analysis Date 9 days ago

EXE

xCmd.exe

peexe idle detect-debug-environment themida spreader

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 4

Security vendors' analysis ⓘ		Do you want to automate checks?	
AhnLab-V3	ⓘ Trojan/Win32.Agent.C2624349	Alibaba	ⓘ Backdoor.Win32/DarkKomet.b59473fc
AliCloud	ⓘ Trojan:Win/Cryptor.Gen	ALYac	ⓘ Trojan.GenericKD.43493830
Antiy-AVL	ⓘ RiskWare[Packed]/Win32.Themida.a	Arcabit	ⓘ Trojan.Generic.D297A9C6
Avast	ⓘ Win32:Malware-gen	AVG	ⓘ Win32:Malware-gen
Avira (no cloud)	ⓘ TR/Crypt.TPM.Gen	BitDefender	ⓘ Trojan.GenericKD.43493830
Bkav Pro	ⓘ W32.AIDetectMalware	CrowdStrike Falcon	ⓘ Win/malicious_confidence_100% (W)
CTX	ⓘ Exe.trojan.darkkomet	Cylance	ⓘ Unsafe
Cynet	ⓘ Malicious (score: 100)	DeepInstinct	ⓘ MALICIOUS
DrWeb	ⓘ ToolxCmd	Elastic	ⓘ Malicious (high Confidence)

Emsisoft	ⓘ Trojan.GenericKD.43493830 (B)	eScan	ⓘ Trojan.GenericKD.43493830
ESET-NOD32	ⓘ A Variant Of Win32/Packed.Themida.EGF	Fortinet	ⓘ PossibleThreat
GData	ⓘ Trojan.GenericKD.43493830	Google	ⓘ Detected
Gridinsoft (no cloud)	ⓘ Trojan.HeurI.030100A1	Ikarus	ⓘ Trojan.Win32.Themida
Jiangmin	ⓘ Backdoor.DarkKomet.jzg	K7AntiVirus	ⓘ Trojan ( 0055e39b1 )
K7GW	ⓘ Trojan ( 0055e39b1 )	Kaspersky	ⓘ Backdoor.Win32.DarkKomet.Idrt
Kingsoft	ⓘ Malware.kb.a.743	Malwarebytes	ⓘ Malware.Heuristic.2025
MaxSecure	ⓘ Trojan.Malware.7164915.susgen	McAfee Scanner	ⓘ Ttl6C8EEA3BA314
Microsoft	ⓘ Trojan:MSIL/Cryptor	NANO-Antivirus	ⓘ Trojan.Win32.TPM.dhkiyd
Palo Alto Networks	ⓘ Generic.ml	Panda	ⓘ Trj/CLA
QuickHeal	ⓘ Trojan.Ghanarava.1730867000474196	Rising	ⓘ Backdoor.DarkKometI8.13E (CLOUD)

Palo Alto Networks	ⓘ Generic.ml	Panda	ⓘ Trj/CLA
QuickHeal	ⓘ Trojan.Ghanarava.1730867000474196	Rising	ⓘ Backdoor.DarkKometI8.13E (CLOUD)
Sangfor Engine Zero	ⓘ Backdoor.Win32.DarkKomet.Vyor	SecureAge	ⓘ Malicious
SentinelOne (Static ML)	ⓘ Static AI - Malicious PE	Skyhigh (SWG)	ⓘ ArtemisITrojan
Sophos	ⓘ Mal/Generic-S	Symantec	ⓘ ML.Attribute.HighConfidence
Tencent	ⓘ Malware.Win32.Gencirc.13bdd23d	Trapmine	ⓘ Malicious.high.ml.score
Trellix (ENS)	ⓘ ArtemisI27AEE7F36B40	Trellix (HX)	ⓘ Generic.mg.27aee7f36b4099e8
TrendMicro	ⓘ TROJ_GEN.R002C0DG821	TrendMicro-HouseCall	ⓘ TROJ_GEN.R002C0DG821
Varist	ⓘ W32/ABRisk.IRHP-4556	VBA32	ⓘ TScope.Malware-Cryptor.SB
VIPRE	ⓘ Trojan.GenericKD.43493830	WithSecure	ⓘ Trojan.TR/Crypt.TPM.Gen
Xcitiium	ⓘ TrojWare.Win32.Agent.COC@52vn2u	Yandex	ⓘ Riskware.ThemidaLeZrdbxJrqU0
Zillya	ⓘ Backdoor.DarkKomet.Win32.46167	Zoner	ⓘ Probably Heur.ExeHeaderL
Acronis (Static ML)	✔ Undetected	Baidu	✔ Undetected

DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 4

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic properties

MD5	27aee7f36b4099e8db3e3d3898474196
SHA-1	c26dc6e4ef77cafafa154fa9529c4ce79a8fc78b
SHA-256	6c8eea3ba31463a04d041f4c9ff50b50d9b5945d3306fee35fb4b5b5d292692b
Vhash	08506fd6d1f1f7f11z1z1z
Authentihash	e487980eab13ec926c2461180f658a84ed3d8c029c23b4f51ce27ebc821f6b
Imphash	baa93d47220682c04d92f7797d9224ce
Rich PE header hash	67ebd3a6a3d5f08d768b1be8314d3715
SSDEEP	24576:qsaXJShxiutr0C3dYlx7/aTjklClmS2m6hEQP:qsaXkhDtbtcx7SUIlClF76hEQ
TLSH	T19B05232B8B7E408DF08F5BF39B059BCFFA15480E41BF9948583DB46FE0253D8426A959
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (console) Intel 80386, for MS Windows
TrID	Win32 Dynamic Link Library (generic) (27.1%)   Win16 NE executable (generic) (20.8%)   Win32 Executable (generic) (18.6%)   Windows Icons Li...
DetectItEasy	PE32   Protector: Themida/Winlicense (2.X)   Compiler: Microsoft Visual C/C++ (12.00.8799) [C++]   Linker: Microsoft Linker (6.00.8797)   Tool: ...
Magika	PEBIN
File size	824.00 KB (843776 bytes)

### 2.3.1.3 Archivo nbtsan.exe

El archivo TMP\nbtsan.exe se revisó en Visustotal.com y se encontró que es un archivo malicioso

37

/ 72

Community Score

-89

37/72 security vendors flagged this file as malicious

Reanalyze
Similar
More

c9d5dc956841e000bfd8762e2f0b48b66c79b79500e894b4efa7fb9ba17e4e9e

Size
Last Analysis Date

36.00 KB
1 day ago

EXE

peexe armadillo idle checks-user-input via-tor detect-debug-environment

DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 30+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic properties

MD5	f01a9a2d1e31332ed36c1a4d2839f412
SHA-1	90da10004c8f6afdaa2cf18922670a745564f45
SHA-256	c9d5dc956841e000bfd8762e2f0b48b66c79b79500e894b4efa7fb9ba17e4e9e
Vhash	034036551d1bz22e=z
Authentihash	0dfaabf2239d6523d1c8545bd9850ac5c4ef349fa46cfb8ba9bc929d4f583e4a
Imphash	2fa43c5392ec7923ababced078c2f98d
Rich PE header hash	646371930ed0f882699ba56d2e671296
SSDEEP	384:xl+ZbDOfdyXM5cel8cmoGfOyGPkof7DPzwVkgT+Kfab6BCXS2brlszQ:T+4f9l8YCGPkm7GYkEb4CXSwX
TLSH	T146F2E8157581802DE01103B2917249767AF75AA1238041CFBFD93AA59BF86C3B6FCE4F
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (console) Intel 80386, for MS Windows
TrID	Microsoft Visual C++ compiled executable (generic) (32.2%)   Win64 Executable (generic) (20.5%)   Win32 Dynamic Link Library (generic) (12.8%) ...
DetectItEasy	PE32   Compiler: EP:Microsoft Visual C/C++ (6.0 (1720-9782)) [EXE32]   Compiler: Microsoft Visual C/C++ (12.00.8168) [C]   Linker: Microsoft Link...
Magika	PEBIN
File size	36.00 KB (36864 bytes)
PEID packer	Microsoft Visual C++

AhnLab-V3	! HackTool/Win_Scanner.C5220929	AliCloud	! Hacktool:Win/NetTool.Nbtscan
ALYac	! Trojan.Agent.36864N	Antiy-AVL	! RiskWare/Win32.APT28
Arcabit	! Application.NbtScan.A	BitDefender	! Application.NbtScan.A
Bkav Pro	! W32.FAMVT.APTIxAF.Trojan	CrowdStrike Falcon	! Win/grayware_confidence_100% (W)
CTX	! Exe.trojan.nbtscan	DeepInstinct	! MALICIOUS
DrWeb	! Program.NbtScan.1	Elastic	! Malicious (high Confidence)
eScan	! Application.NbtScan.A	ESET-NOD32	! A Variant Of Win32/NetTool.Nbtscan.B P...

Fortinet	! Riskware/Nbtscan	GData	! Application.NbtScan.A
Google	! Detected	Huorong	! HackTool/Scanner.g
Kaspersky	! Not-a-virus:HEUR:NetTool.Win32.NbtSca...	Lionic	! Riskware.Win32.NbtScan.11c
MaxSecure	! Trojan.Malware.331971382.susgen	McAfee Scanner	! TILC9D5DC956841
Microsoft	! HackTool:Win32/Malgent!MSR	Palo Alto Networks	! Generic.ml
QuickHeal	! Trojan.AgentCIR	Rising	! Hacktool.NbtScan!8.1983C (CLOUD)
Skyhigh (SWG)	! Nbtscan	TACHYON	! Trojan/W32.Agent.36864.DND
Tencent	! Win32.Trojan.Qwer.Gwuz	Trellix (ENS)	! Nbtscan
TrendMicro	! HackTool.Win32.NBTSCAN.REDT	TrendMicro-HouseCall	! HackTool.Win32.NBTSCAN.REDT
Varist	! W32/Tool.XMUR-5657	VIPRE	! Application.NbtScan.A
ViriT	! Trojan.Win32.Generic.BKU	ViRobot	! NetTool.Agent.36864

Tencent	! Win32.Trojan.Qwer.Gwuz	Trellix (ENS)	! Nbtscan
TrendMicro	! HackTool.Win32.NBTSCAN.REDT	TrendMicro-HouseCall	! HackTool.Win32.NBTSCAN.REDT
Varist	! W32/Tool.XMUR-5657	VIPRE	! Application.NbtScan.A
ViriT	! Trojan.Win32.Generic.BKU	ViRobot	! NetTool.Agent.36864
Xcitium	! ApplicUnwnt@#1k2cns0y8hfh	Acronis (Static ML)	✓ Undetected
Alibaba	✓ Undetected	Avast	✓ Undetected
AVG	✓ Undetected	Avira (no cloud)	✓ Undetected
Baidu	✓ Undetected	ClamAV	✓ Undetected
CMC	✓ Undetected	Cylance	✓ Undetected
Cynet	✓ Undetected	Emsisoft	✓ Undetected
Gridinsoft (no cloud)	✓ Undetected	Ikarus	✓ Undetected
Jiangmin	✓ Undetected	K7AntiVirus	✓ Undetected
K7GW	✓ Undetected	Kinesoft	✓ Undetected

#### 2.3.1.4 Otros archivos

Después de analizar los logs del sistema en E:\reposgit\keepcooding\F\Windows\System32\winevt\logs con el programa HAYABUSA que encontralos los siguientes programas

<https://github.com/oscartobar/practicaskkeepcoding/blob/main/DFIR/analysis2>

```
Símbolo del sistema
- Sai Ou Shitsu Ba - The old man lost his horse. (A blessing in disguise.)

E:\hayabusa-3.2.0-win-x64>hayabusa-3.2.0-win-x64.exe csv-timeline -d E:\reposgit\keepcoding\F\Windows\System32\winevt\logs -o E:\reposgit\keepcoding\analysis2

HAYABUSA
by Yamato Security

Taking threat detection to the next level~

Start time: 2025/04/10 23:43
Total event log files: 105
Total file size: 63.2 MB

Scan wizard:
Which set of detection rules would you like to load? · 2. Core+ (3,761 rules) ( status: test, stable | level: medium, high, critical )
Include sysmon rules? (1,865 rules) · yes

Loading detection rules. Please wait.

Excluded rules: 866
Noisy rules: 12 (Disabled)
```

```
Loading detection rules. Please wait.

Excluded rules: 866
Noisy rules: 12 (Disabled)

Stable rules: 147 (3.91%)
Test rules: 3,610 (96.09%)

Correlation rules: 3 (0.08%)
Correlation referenced rules: 3 (0.08%)

Expand rules: 10 (0.27%)
Enabled expand rules: 0 (0.00%)

Hayabusa rules: 66
Sigma rules: 3,691
Total detection rules: 3,757

Creating the channel filter. Please wait.

Evtx files loaded after channel filter: 18
Detection rules enabled after channel filter: 1,859

Output profile: standard

Scanning in progress. Please wait.

[00:00:02] 18 / 18 [=====] 100%
```

```

Results Summary:

Events with hits / Total events: 119 / 21,032 (Data reduction: 20,913 events (99.43%))

Total | Unique detections: 150 | 31
Total | Unique emergency detections: 0 (0.00%) | 0 (0.00%)
Total | Unique critical detections: 14 (9.33%) | 3 (0.00%)
Total | Unique high detections: 30 (20.00%) | 8 (0.00%)
Total | Unique medium detections: 106 (70.67%) | 20 (64.52%)
Total | Unique low detections: 0 (0.00%) | 0 (25.81%)
Total | Unique informational detections: 0 (0.00%) | 0 (9.68%)

First Timestamp: 2019-03-19 13:59:29.535 +01:00
Last Timestamp: 2022-05-08 21:11:47.607 +02:00

Dates with most total detections:
emergency: n/a, critical: 2022-05-08 (14), high: 2022-05-08 (25), medium: 2019-03-19 (91), low: n/a, informational: n/a

Top 5 computers with most unique detections:
emergency: n/a
critical: PEGASUS01 (3)
high: PEGASUS01 (7), MSEDGEWIN10 (3)
medium: MSEDGEWIN10 (16), PEGASUS01 (6)
low: n/a
informational: n/a

```

## 2.4 Descarga fichero de control remoto

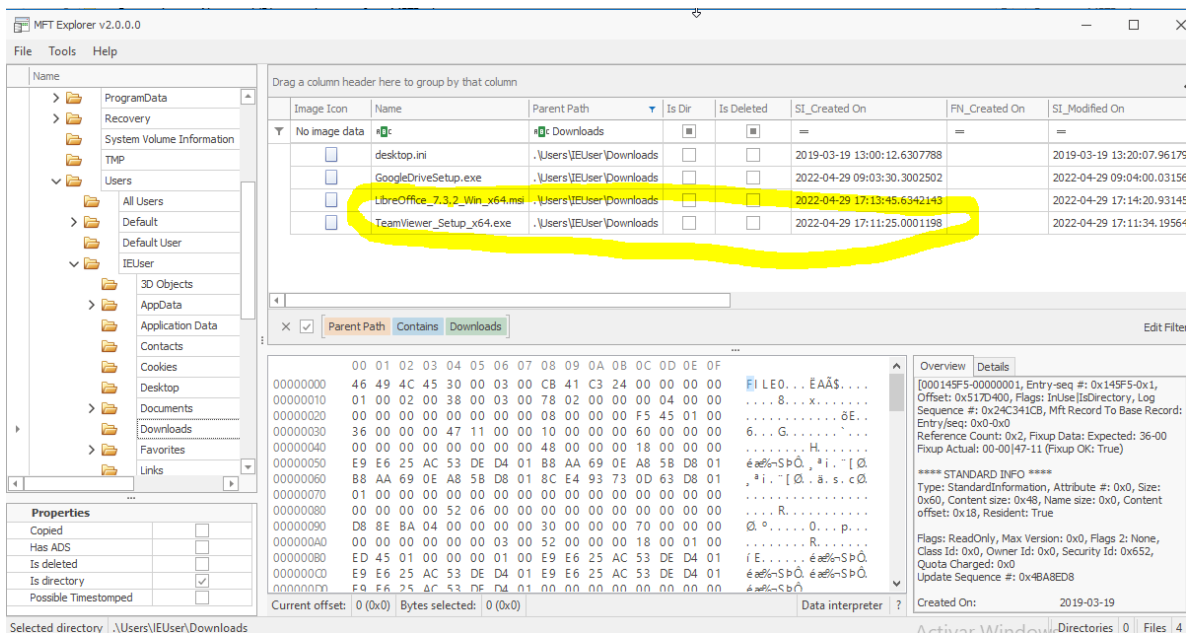
Escriba el nombre del fichero .exe de un programa de control remoto que se ha descargado el usuario

### 2.4.1 Solución

Usando el MFT del archivo se cargo en el MFT Explorer v2.0.0.0 y se buscaron los archivos de nombre Downloads. Aunque se busco en la carpeta Users en los usuarios Default no se encontramos archivos, en Public solo se encontró este archivo

The screenshot shows the MFT Explorer v2.0.0.0 application. The left pane displays a file tree with 'Public' expanded, showing 'Downloads'. The main pane shows a table with columns: Image Icon, Name, Parent Path, Is Dir, Is Deleted, SI\_Created On, FN\_Created On, SI\_Modified On, and FN\_Modified. A single entry is visible: 'desktop.ini' with parent path '.\Users\Public\Downloads'. The right pane shows the MFT record details for the selected file, including hex data, ASCII representation, and a summary of file attributes like Type, Size, and Flags.

Pero solo la carpeta IEUser tuvo archivos ejecutables. El archivo que de bajo fue TeamViewer\_Setup\_X64.exe en .\Users\IEUser\Downloads el día 29/04/2022 a las 17:11/25.0001198

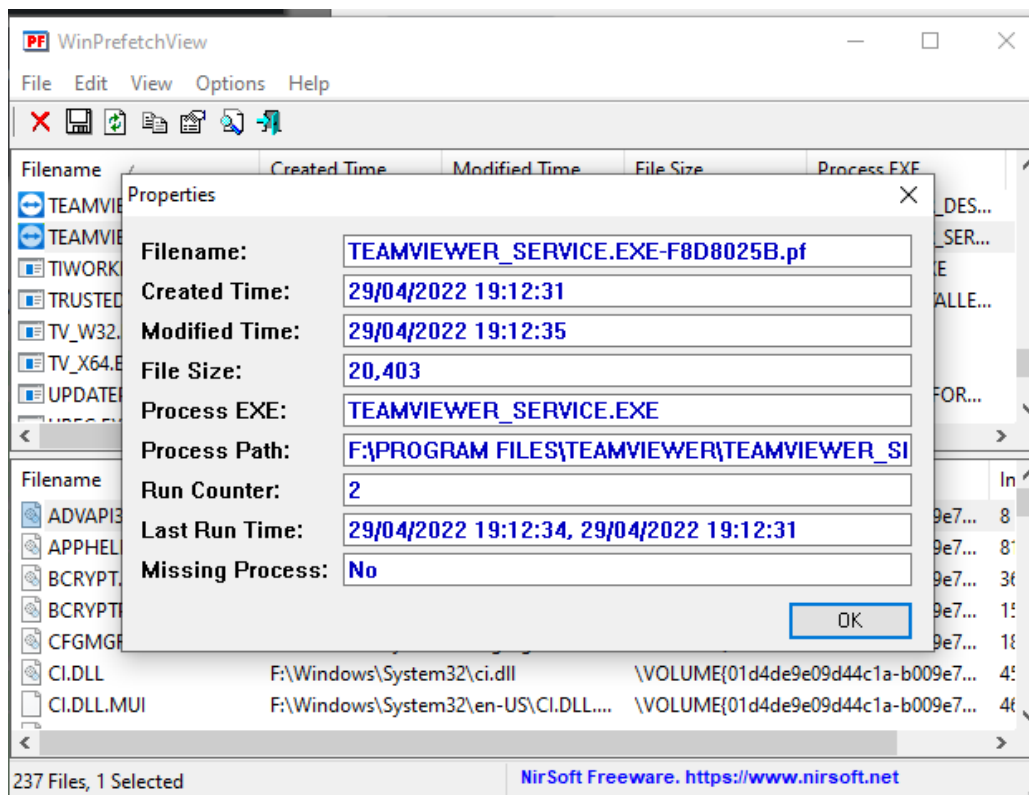


## 2.5 Fecha de ejecución programa

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

### 2.5.1 Solución

Se ejecuto el 29/04/2022



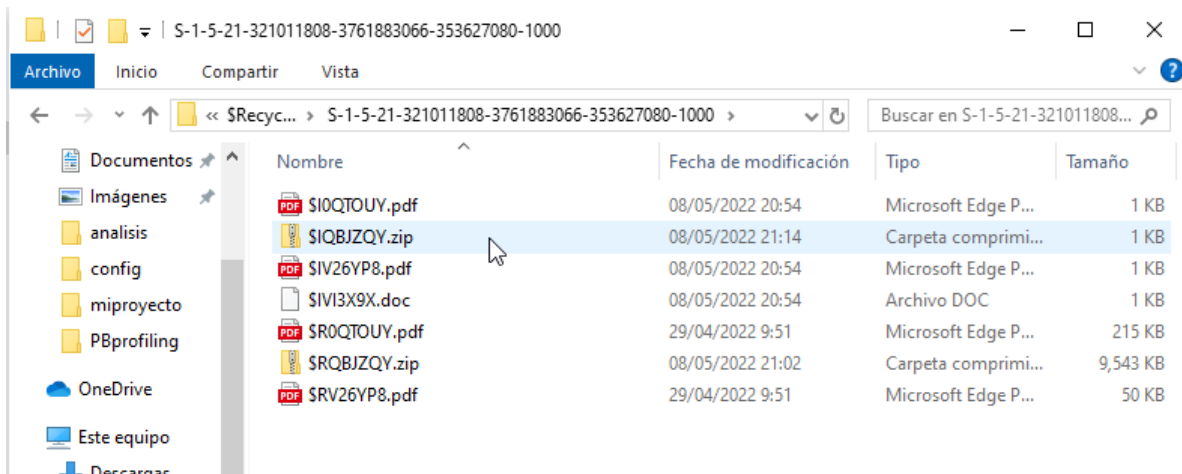
## 2.6 Ficheros Eliminados

Se sospecha que existe un fichero .zip eliminado.

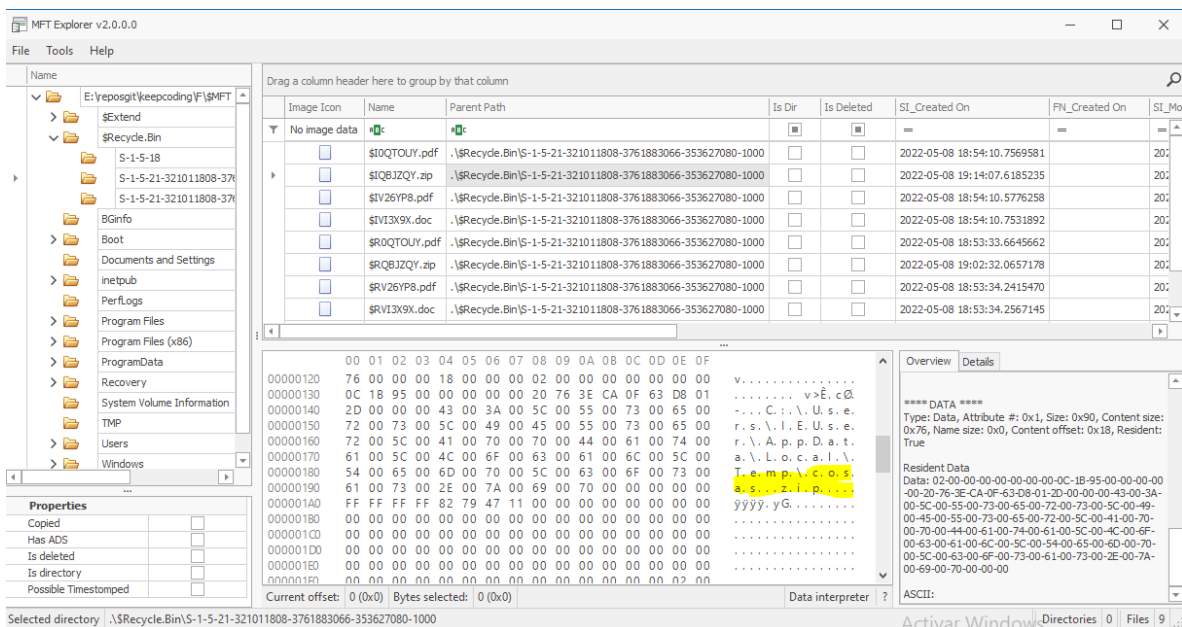
Podría indicar el nombre

### 2.6.1 Solución

En la carpeta \$Recible.Bin se encontraron 2 archivos uno el \$IQBJQY.zip y luego se copio el \$RQBJZQY.zip



. luego de analizar el archivo iniciar se encontró que el nombre del archivo eliminado era cosas.zip



## 2.7 Contraseñas Débiles

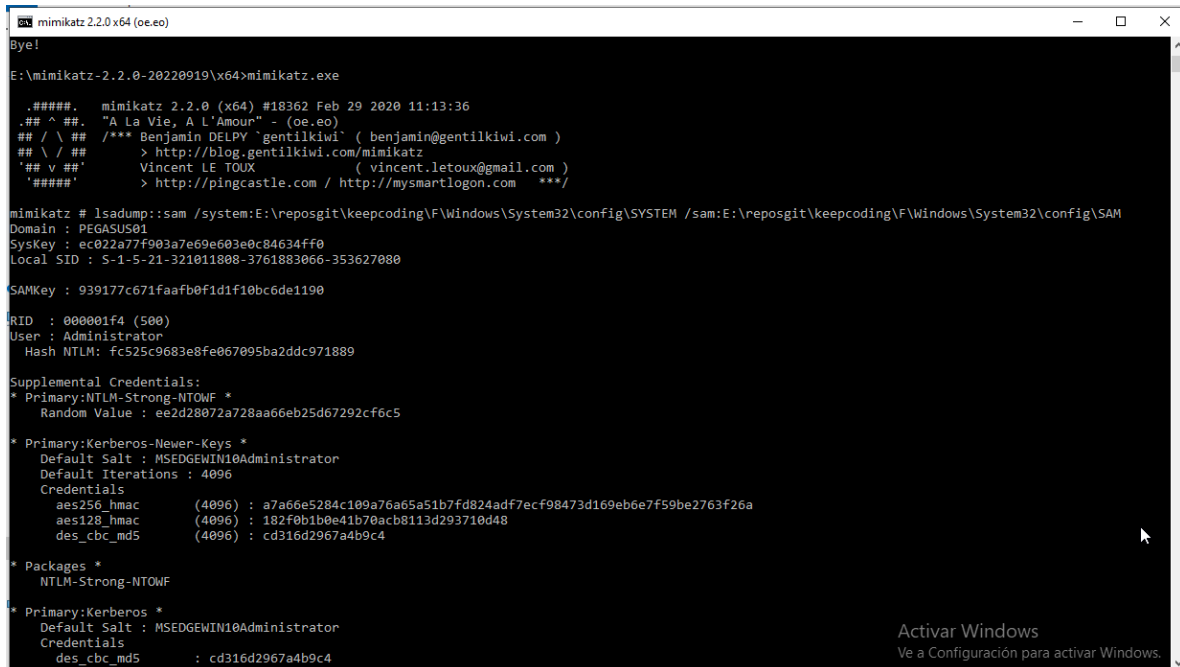
Existen sospechas de que la contraseña del usuario IEUser es una contraseña débil, lo que ha permitido al atacante acceder a ella.

Podrían indicar la contraseña del usuario.

## 2.7.1 Solución

Se utilizó el mimikatz en <https://github.com/ParrotSec/mimikatz/tree/master/x64>

con este programa se ejecuto asi:



```
mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /** Benjamin DELPY "gentilkiwi" ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
## v ## Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ****

mimikatz # lsadump::sam /system:E:\reposgit\keepcoding\F\Windows\System32\config\SYSTEM /sam:E:\reposgit\keepcoding\F\Windows\System32\config\SAM
Domain : PEGASUS81
SysKey : ec022a77f903a7e69e603e0c04634ff0
Local SID : S-1-5-21-321011808-3761883066-353627080

SAMKey : 939177c671faafb0fd1d1f10bc6de1190

RID : 000001f4 (500)
User : Administrator
Hash NTLM: fc525c9683e8fe067095ba2ddc971889

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
Random Value : ee2d28072a728aa66eb25d67292cf6c5

* Primary:Kerberos-Newer-Keys *
Default Salt : MSEDGEWIN10Administrator
Default Iterations : 4096
Credentials
aes256_hmac (4096) : a7a66e5284c109a76a65a51b7fd824adf7ecf98473d169eb6e7f59be2763f26a
aes128_hmac (4096) : 182f0b1b0e41b70acb8113d293710d48
des_cbc_md5 (4096) : cd316d2967a4b9c4

* Packages *
NTLM-Strong-NTOWF

* Primary:Kerberos *
Default Salt : MSEDGEWIN10Administrator
Credentials
des_cbc_md5 : cd316d2967a4b9c4
```

```
RID : 000001f5 (501)
User : Guest

RID : 000001f7 (503)
User : DefaultAccount

RID : 000001f8 (504)
User : WDAGUtilityAccount
Hash NTLM: 20ff0389f84bdbf9ce6fc36af6993b63

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
  Random Value : ac3c2a55378d84eded3472f0b728b7bd

* Primary:Kerberos-Newer-Keys *
  Default Salt : WDAGUtilityAccount
  Default Iterations : 4096
  Credentials
    aes256_hmac      (4096) : fb60f0d32a8abb7dd991ae530844c927fb25380fffeb119ccd0971c5be8df321
    aes128_hmac      (4096) : e4617e2dd5e029348f552ece98695ddb
    des_cbc_md5      (4096) : 1ce9546ebf6e5e45

* Packages *
  NTLM-Strong-NTOWF

* 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 *
```

```
mimikatz 2.2.0 x64 (oe.eo)
Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
  Random Value : c6a807d33d3772144ce3407a8a73f9ef

* Primary:Kerberos-Newer-Keys *
  Default Salt : MSEDGWIN10IEUser
  Default Iterations : 4096
  Credentials
    aes256_hmac      (4096) : 72cc752f2addce7556960ad819259738c4fd86e7130cee6b06aca1137ad1e6cb
    aes128_hmac      (4096) : 7d83280d0766f4ad6510460fbd975fbc
    des_cbc_md5      (4096) : ecd9340ddff7406b
  OldCredentials
    aes256_hmac      (4096) : b55700a5a2002a8a290a8f3554838fd420bcb7877b8f59ed75fd7af6b98ba53c
    aes128_hmac      (4096) : 64be48ded076d1592ae6df8708266f64
    des_cbc_md5      (4096) : a4ce3d75831f988c

* Packages *
  NTLM-Strong-NTOWF

* Primary:Kerberos *
  Default Salt : MSEDGWIN10IEUser
  Credentials
    des_cbc_md5      : ecd9340ddff7406b
  OldCredentials
    des_cbc_md5      : a4ce3d75831f988c

RID : 000003ea (1002)
User : sshd
Hash NTLM: 42760776cade85fd98103a0f44437800

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
  Random Value : 59027b35c620e96f83d319ebd31577be

* Primary:Kerberos-Newer-Keys *
  Default Salt : MSEDGWIN10sshd
  Default Iterations : 4096
  Credentials
    aes256_hmac      (4096) : 9c6818e8b29d2a66b5b66321b95faedfd793908ae666cc254aaca8d9cdd0c3
    aes128_hmac      (4096) : 8e4a19ecfa0cfff16aadf1491aa848d3
    des_cbc_md5      (4096) : 64d51f51efad018a

* Packages *
  NTLM-Strong-NTOWF

* Primary:Kerberos *
  Default Salt : MSEDGWIN10sshd
  Credentials
    des_cbc_md5      : 64d51f51efad018a

mimikatz #
```

Se encontraron los siguientes usuarios con contraseña debil

User: Administrator

Clave: PasswOrd!

The screenshot shows the CrackStation website interface. At the top, there's a navigation bar with the site name and links to Defuse.ca and Twitter. Below this, the main heading is "Free Password Hash Cracker". A text input field contains the hash "fc525c9683e8fe067095ba2ddc971889". To the right of the input field is a reCAPTCHA "I'm not a robot" checkbox and a "Crack Hashes" button. Below the input field, a list of supported hash types is shown: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), and QubesV3.1BackupDefaults. Below this, a table displays the results of the hash cracking process.

Hash	Type	Result
fc525c9683e8fe067095ba2ddc971889	NTLM	PasswOrd!

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

Usuario: IEUser

Clave: qwerty

This screenshot shows the CrackStation website interface with a different hash. The text input field contains the hash "2d20d252a479f485cdf5e171d93985bf". The reCAPTCHA and "Crack Hashes" button are visible. The supported hash types list is the same as in the previous screenshot. The results table shows a successful match for the NTLM hash.

Hash	Type	Result
2d20d252a479f485cdf5e171d93985bf	NTLM	qwerty

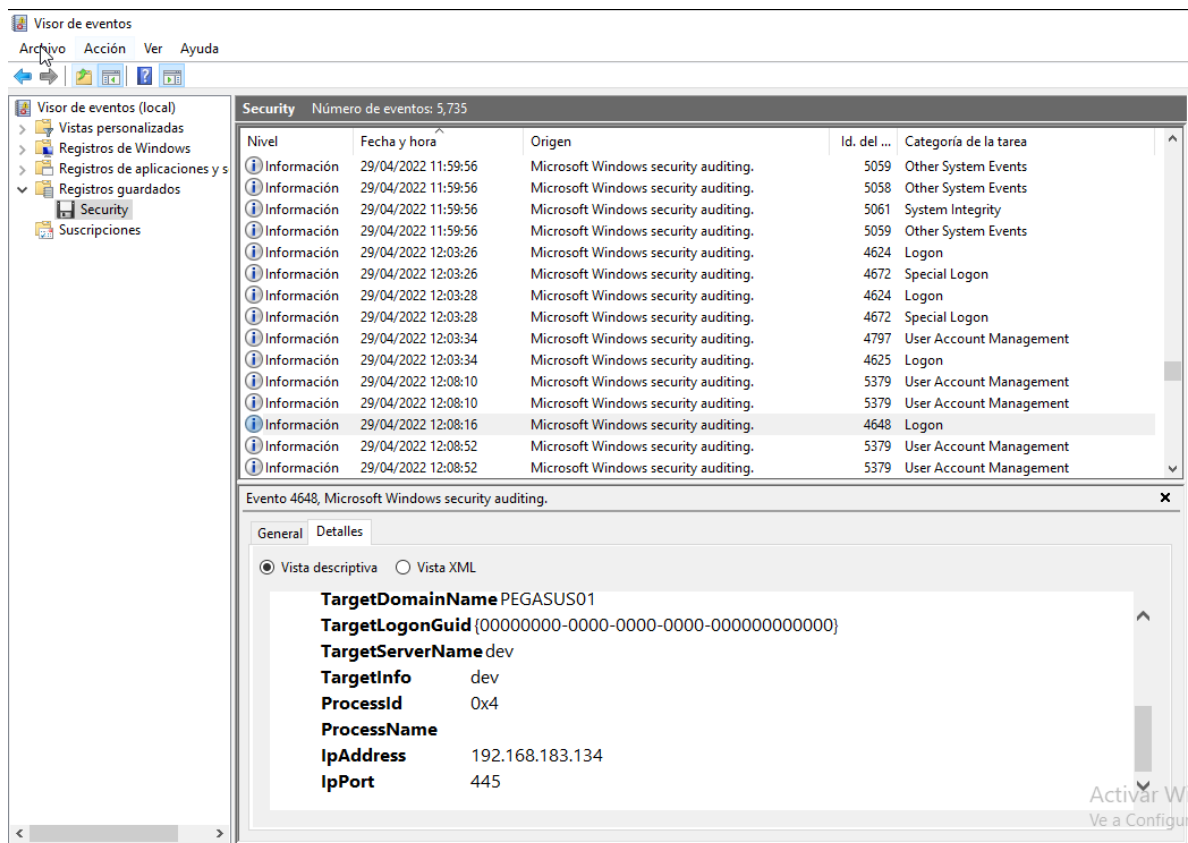
Color Codes: **Green** Exact match, **Yellow** Partial match, **Red** Not found.

## 2.8 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

### 2.8.1 Solución

Al consultar en el evento de Secutity (Windows/system32/winevt/logs) se encontró la ip



### 3 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.

#### 3.1 Winpmem

##### 3.1.1 Solución

Usando el sistema [winpmem\\_mini\\_x64\\_rc2.exe](#) si tomo la memoria ram del equipo Windows así:

```
E:\tools>winpmem_mini_x64_rc2.exe memoriaram.mem
WinPmem64
Extracting driver to C:\Users\PC\AppData\Local\Temp\pmeC25F.tmp
Driver Unloaded.
Loaded Driver C:\Users\PC\AppData\Local\Temp\pmeC25F.tmp.
Deleting C:\Users\PC\AppData\Local\Temp\pmeC25F.tmp
The system time is: 10:33:26
Will generate a RAW image
- buffer_size_: 0x1000
CR3: 0x00001AA002
4 memory ranges:
Start 0x00001000 - Length 0x0009E000
Start 0x00100000 - Length 0x00002000
Start 0x00103000 - Length 0xBFEF6000
Start 0x100000000 - Length 0xF40000000
max_physical_memory_ 0x1040000000
Acquisition mode PTE Remapping
Padding from 0x00000000 to 0x00001000
pad
- length: 0x1000
```

```

00% 0x00001000 .
Padding from 0x0009F000 to 0x00100000
pad
- length: 0x61000
→
00% 0x0009F000 .
copy_memory
- start: 0x100000
- end: 0x102000

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

00% 0x00102000 .
copy_memory
- start: 0x103000
- end: 0xbfff9000

00% 0x00103000 .....
01% 0x32103000 .....
02% 0x64103000 .....
03% 0x96103000 .....
Padding from 0xBFFF9000 to 0x100000000
pad
- length: 0x40007000

04% 0xBFFF9000 .....
04% 0xBFFF9000 .....
copy_memory
- start: 0x100000000
- end: 0x1040000000

06% 0x100000000 .....
07% 0x132000000 .....
08% 0x164000000 .....
09% 0x196000000 .....
10% 0x1C8000000 .....
12% 0x1FA000000 .....
13% 0x22C000000 .....
14% 0x25E000000 .....
15% 0x290000000 .....

```

El archivo se genero fue este

```

12/04/2025 12:32 <DIR> .
12/04/2025 12:32 <DIR> ..
04/04/2025 02:04 3,620 !!!RemoteFileDetails.csv
26/03/2025 17:32 28,029 Get-ZimmermanTools.ps1
12/04/2025 12:40 41,842,376,704 memoriaram.mem
04/04/2025 02:04 <DIR> net6
12/04/2025 06:38 527,640 winpmem_mini_x64_rc2.exe
4 archivos 41,842,935,993 bytes
3 dirs 6,914,048 bytes libres

E:\tools>

```

Sin embargo para el ejercicio de los comandos se utilizó en archivo **20230810.mem** que fue entregado en la evidencia memoria RAM ( ctf.sancastekk.me), pues es mas pequeño que el proceso genenado (**memoriaram.mem**)rm

## 3.2 Proceso Malicioso

Identificar el proceso malicioso y confirmar el id de proceso del proceso malicioso.

### 3.2.1 Solución

Se ejecuto volatility 3 con el comando

Python vol.py -f "c:\volatility\20230810.mem" windows.malfind.Malfind

Con el fin de buscar el código inyectado o encondido en la memoria

Se encontró que el PID 6812 svchost.exe es un proceso malicioso

```
C:\volatility\volatility3>python vol.py -f "C:\volatility\20230810.mem" windows.malfind.Malfind
Volatility 3 Framework 2.26.1
Progress: 100.00 PDB scanning finished
PID Process Start VPN End VPN Tag Protection CommitCharge PrivateMemory File output Notes
Hexdump Disasm
8828 smartscreen.ex 0x25813f90000 0x25813faffff VadS PAGE_EXECUTE_READWRITE 1 1 Disabled
N/A
48 89 54 24 10 48 89 4c 24 08 4c 89 44 24 18 4c H.T$.H.L$.L.D$.L
89 4c 24 20 48 8b 41 28 48 8b 48 08 48 8b 51 50 .L$ H.A(H.H.H.QP
48 83 e2 f8 48 8b ca 48 b8 60 00 f9 13 58 02 00 H...H..H..X..
00 48 2b c8 48 81 f9 70 0f 00 00 76 09 48 c7 c1 .H+.H..p...v.H..
89 4c 24 20 48 8b 41 28 48 8b 48 08 48 8b 51 50 48 83 e2 f8 48 8b ca 48 b8 60 00 f9 13 58 02 00 00 48 2b c8 48 81 f9 70
0f 00 00 76 09 48 c7 c1
8828 smartscreen.ex 0x25814410000 0x25814473fff VadS PAGE_EXECUTE_READWRITE 1 1 Disabled
N/A
e9 fb ff 08 00 00 00 00 00 cc cc cc cc cc cc cc .....
e9 eb 03 09 00 00 00 00 00 00 cc cc cc cc cc cc cc .....
e9 db 1f 09 00 00 00 00 00 00 cc cc cc cc cc cc cc .....
cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc .....
e9 eb 03 09 00 00 00 00 00 00 cc cc cc cc cc cc cc e9 db 1f 09 00 00 00 00 00 cc cc cc cc cc cc cc cc cc cc
cc cc cc cc cc cc cc cc cc
3136 MsMpEng.exe 0x2bb32980000 0x2bb32980fff VadS PAGE_EXECUTE_READWRITE 1 1 Disabled
Function prologue
55 48 8d 2c 24 48 83 ec 20 48 8b 01 48 8b 49 08 UH.,$.H.. H..H.I.
ff d0 48 8d 65 00 5d c3 cc cc cc cc cc cc cc ..H.e.].....
cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc .....
```



## 3.3 Proceso hijo

El equipo del SOC cree que el proceso malicioso puede generar otro proceso que permita al actor de la amenaza ejecutar comandos. ¿Cuál es el ID de ese proceso hijo?

### 3.3.1 Solución

Usando el pstree se busco el proceso hijo del proceso 6812 y se encontro el el proceso hijo es el 4364

Python vol.py -f "c:\volatility\20230810.mem" windows.pstree

```
*** 2776 7436 RamCapture64.e 0x9e8b8aa66080 5 - 1 False 2023-08-10 11:31:52.000000 UTC N/A \Device\HarddiskVolume3\Users\simon.stark\
**** 9816 2776 conhost.exe 0x9e8b91cda080 6 - 1 False 2023-08-10 11:31:52.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\conhc
*** 6812 7436 svchost.exe 0x9e8b87762080 3 - 1 False 2023-08-10 11:30:03.000000 UTC N/A \Device\HarddiskVolume3\Users\simon.stark\Down
**** 4364 6812 cmd.exe 0x9e8b8b6ef080 1 - 1 False 2023-08-10 11:30:57.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\cmd.exe
***** 9204 4364 conhost.exe 0x9e8b89ec7080 3 - 1 False 2023-08-10 11:30:57.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\conhc
* 956 744 fontdrvhost.ex 0x9e8b89530180 5 - 1 False 2023-08-10 11:13:43.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\fontdrvhc
10044 9952 OneDrive.exe 0x9e8b90507080 0 - 1 True 2023-08-10 11:15:31.000000 UTC 2023-08-10 11:15:37.000000 UTC \Device\HarddiskVc
```

## 3.4 Líneas de comandos

Se ejecuto volatility 3 con el comando

Python vol.py -f "c:\volatility\20230810.mem" windows.cmdline.CmdLine

Y se encontró en la memoria

```
Simbolo del sistema
12 archivos      27,632 bytes
7 dirs  34,097,954,816 bytes libres

C:\volatility\volatility3>python vol.py -f "C:\volatility\20230810.mem" windows.cmdline.CmdLine
Volatility 3 Framework 2.26.1
Progress: 100.00      PDB scanning finished
PID      Process Args
4         System -
140       Registry -
436       smss.exe \SystemRoot\System32\smss.exe
564       csrss.exe %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On
SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileCont
rol=Off MaxRequestThreads=16
544       csrss.exe %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On
SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileCont
rol=Off MaxRequestThreads=16
556       wininit.exe wininit.exe
744       winlogon.exe winlogon.exe
788       services.exe C:\WINDOWS\system32\services.exe
808       lsass.exe C:\WINDOWS\system32\lsass.exe
928       svchost.exe C:\WINDOWS\system32\svchost.exe -k DcomLaunch -p
956       fontdrvhost.ex "fontdrvhost.exe"
964       fontdrvhost.ex "fontdrvhost.exe"
512       svchost.exe C:\WINDOWS\system32\svchost.exe -k RPCSS -p
864       svchost.exe C:\WINDOWS\system32\svchost.exe -k DcomLaunch -p -s LSM
1048      dwm.exe "dwm.exe"
1148      svchost.exe C:\WINDOWS\System32\svchost.exe -k NetworkService -s TermService
1272      svchost.exe C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
1280      svchost.exe C:\WINDOWS\System32\svchost.exe -k LocalService -s W32Time
1288      svchost.exe C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts
1296      svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalService -p -s nsi
1304      svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc
1432      svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp
1472      svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog
1500      svchost.exe C:\WINDOWS\system32\svchost.exe -k NetworkService -p -s Dnscache
1580      svchost.exe C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s Schedule
1588      svchost.exe C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s ProfSvc
1712      svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalServiceNoNetwork -p
1748      svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalServiceNoNetworkFirewall -p
1756      svchost.exe C:\WINDOWS\System32\svchost.exe -k NetworkService -p -s NlaSvc
1828      svchost.exe C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s UserManager
1980      svchost.exe C:\WINDOWS\System32\svchost.exe -k netsvcs -p -s Themes
```

```

C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s Themes
C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s SysMain
C:\WINDOWS\system32\svchost.exe -k LocalService -p -s EventSystem
C:\WINDOWS\system32\svchost.exe -k LocalService -p -s netprofm
C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s WinHttpAutoProxySvc
C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s SENS
MemCompression -
C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s Winmgmt
C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s AudioEndpointBuilder
C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s UmRdpService
C:\WINDOWS\system32\svchost.exe -k NetSvc -p -s iphlpsvc
C:\WINDOWS\system32\svchost.exe -k netsvcs -s CertPropSvc
C:\WINDOWS\system32\svchost.exe -k LocalService -p -s DispBrokerDesktopSvc
C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p
C:\WINDOWS\system32\svchost.exe -k NetworkService -p -s LanmanWorkstation
C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s SessionEnv
C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p
C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p
C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s ShellHWDetection
C:\WINDOWS\system32\svchost.exe -k appmodel -p -s StateRepository
spoolsv.exe C:\WINDOWS\system32\spoolsv.exe
C:\WINDOWS\system32\svchost.exe -k utcsvc -p
C:\WINDOWS\system32\svchost.exe -k NetworkService -p -s CryptSvc
C:\WINDOWS\system32\svchost.exe -k LocalService -p -s SstpSvc
C:\WINDOWS\system32\svchost.exe -k LocalServiceNoNetwork -p -s DPS
C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s TrkWks
C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s WpnService
"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"
C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s LanmanServer
vmtoolsd.exe C:\WINDOWS\system32\svchost.exe -k netsvcs
Sysmon64.exe C:\WINDOWS\system32\svchost.exe -k netsvcs
VGAAuthService.exe "C:\Program Files\VMware\VMware Tools\VMware VGAAuth\VGAAuthService.exe"
vm3dservice.exe C:\WINDOWS\system32\vm3dservice.exe
svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalService -p -s WdiServiceHost
svchost.exe C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s LanmanServer
vm3dservice.exe vm3dservice.exe -n
svchost.exe C:\WINDOWS\system32\svchost.exe -k netsvcs
unsecapp.exe C:\WINDOWS\system32\wbem\unsecapp.exe -Embedding
WmiPrvSE.exe C:\WINDOWS\system32\wbem\wmiprvse.exe
dllhost.exe C:\WINDOWS\system32\dllhost.exe /Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235}
svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalService -p -s fdPHost
svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalServiceAndNoImpersonation -p -s FDResPub
msdtc.exe C:\WINDOWS\system32\msdtc.exe
svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalServiceAndNoImpersonation -p -s SSDPSRV
svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s WdiSystemHost

```

```

4160  svchost.exe      C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s WdiSystemHost
1792  svchost.exe      C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted -s RmSvc
5292  WmiPrvSE.exe     C:\WINDOWS\system32\wbem\wmiPrvse.exe
5452  svchost.exe      C:\WINDOWS\system32\svchost.exe -k wsappx -p -s AppXSvc
5796  svchost.exe      C:\WINDOWS\System32\svchost.exe -k LocalService -p -s LicenseManager
5972  svchost.exe      C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s wuauserv
6136  svchost.exe      C:\WINDOWS\System32\svchost.exe -k NetworkService -p -s DoSvc
5628  svchost.exe      C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s StorSvc
7008  svchost.exe      C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s TokenBroker
7072  svchost.exe      C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s UsoSvc
7128  MoUsCoreWorke   C:\Windows\System32\mousocoreworker.exe -Embedding
4272  sihost.exe       C:\WINDOWS\system32\svchost.exe -k UnistackSvcGroup -s CDPUserSvc
4992  svchost.exe      C:\WINDOWS\system32\svchost.exe -k UnistackSvcGroup -s WpnUserService
4372  svchost.exe      C:\WINDOWS\system32\svchost.exe -k UnistackSvcGroup -s WpnUserService
6324  taskhostw.exe    taskhostw.exe {222A245B-E637-4AE9-A93F-A59CA119A75E}
6692  svchost.exe      C:\WINDOWS\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s TabletInputService
6768  ctfmon.exe       "ctfmon.exe"
7400  userinit.exe     -
7436  explorer.exe     C:\WINDOWS\Explorer.EXE
8116  svchost.exe      C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s PcaSvc
7236  svchost.exe      C:\WINDOWS\system32\svchost.exe -k ClipboardSvcGroup -p -s cbdhsvc
7704  StartMenuExper  "C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperien
ceHost.exe" -ServerName:App.AppXywbbrabmsek0gm3tkwpr5kwzbs55tkqay.mca
652  svchost.exe      C:\WINDOWS\System32\svchost.exe -k netsvcs -p
4380  RuntimeBroker.   C:\Windows\System32\RuntimeBroker.exe -Embedding
8224  SearchApp.exe    "C:\WINDOWS\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe" -ServerName:Cortana
UI.AppX8z9r6jm96hw4bsbneegw0kyxx296wr9t.mca
8488  RuntimeBroker.   C:\Windows\System32\RuntimeBroker.exe -Embedding
8680  SearchIndexer.   C:\WINDOWS\system32\SearchIndexer.exe /Embedding
8828  smartscreen.ex   C:\Windows\System32\smartscreen.exe -Embedding
7756  RuntimeBroker.   C:\Windows\System32\RuntimeBroker.exe -Embedding
4200  svchost.exe      -
4664  dllhost.exe      C:\WINDOWS\system32\DllHost.exe /Processid:{973D20D7-562D-44B9-B70B-5A0F49CCDF3F}
9580  SecurityHealth   "C:\Windows\System32\SecurityHealthSystray.exe"
9612  SecurityHealth   C:\WINDOWS\system32\SecurityHealthService.exe
9712  vmtoolsd.exe     "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr
1564  svchost.exe      C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s lfsvc
10044  OneDrive.exe     -
10176  SgrmBroker.exe   C:\WINDOWS\system32\SgrmBroker.exe
1396  uhssvc.exe       "C:\Program Files\Microsoft Update Health Tools\uhssvc.exe"
10072  svchost.exe      C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s wscntvr
7416  svchost.exe      C:\WINDOWS\system32\svchost.exe -k UnistackSvcGroup
3024  TextInputHost.   "C:\WINDOWS\SystemApps\Microsoft.Windows.Client.CBS_cw5n1h2txyewy\TextInputHost.exe" -ServerName:

```

## 3.5 IP del C2C

El responsable del SOC ha desplegado un equipo de caza de amenazas para realizar un barrido del entorno en busca de cualquier indicador de compromiso. Sería de gran ayuda para el equipo si pudiera confirmar la dirección IP y los puertos de C2 para que nuestro equipo pueda utilizarlos en su barrido. Flag: XXX.XXX.XXX.XXX:Puerto

### 3.5.1 Solución

Se ejecuto volatility 3 con el comando

Python vol.py -f "c:\volatility\20230810.mem" windows.netstat.NetStat

Y se encontró el la ip y el puerto son

**13.127.155.166:8888**



```

D:\descargas\exiftool-13.27_64\exiftool-13.27_64>tool.exe -s redes_sociales.png
ExifToolVersion      : 13.27
FileName             : redes_sociales.png
Directory            : .
FileSize             : 2.1 MB
FileModifyDate       : 2025:04:07 10:02:31-05:00
FileAccessDate       : 2025:04:12 13:28:35-05:00
FileCreateDate       : 2025:04:12 13:28:23-05:00
FilePermissions      : -rw-rw-rw-
FileType             : PNG
FileTypeExtension    : png
MIMEType             : image/png
ImageWidth           : 957
ImageHeight          : 1429
BitDepth             : 8
ColorType            : RGB with Alpha
Compression          : Deflate/Inflate
Filter               : Adaptive
Interlace            : Noninterlaced
sRGBRendering        : Perceptual
Gamma                : 2.2
PixelsPerUnitX       : 3778
PixelsPerUnitY       : 3778
PixelUnits           : meters
ImageSize            : 957x1429
Megapixels           : 1.4
D:\descargas\exiftool-13.27_64\exiftool-13.27_64>

```

#### 4.1.1 WhatsApp

La siguientes e la misma Imagen enviada (redes\_sociales.png), luego se descargo la imagen generada en Whastapp, llamada WhatsApp Image 2025-04-12 at 1.30.42 PM.jpeg

```

D:\descargas\exiftool-13.27_64\exiftool-13.27_64>tool.exe -s "WhatsApp Image 2025-04-12 at 1.30.42 PM.jpeg"
ExifToolVersion      : 13.27
FileName              : WhatsApp Image 2025-04-12 at 1.30.42 PM.jpeg
Directory             : .
FileSize              : 481 kB
ZoneIdentifier        : Exists
FileModifyDate        : 2025:04:12 13:30:49-05:00
FileAccessDate        : 2025:04:12 13:32:32-05:00
FileCreateDate        : 2025:04:12 13:30:49-05:00
FilePermissions       : -rw-rw-rw-
FileType              : JPEG
FileTypeExtension     : jpg
MIMEType              : image/jpeg
JFIFVersion           : 1.01
ResolutionUnit        : None
XResolution           : 1
YResolution           : 1
ProfileCMType         : 
ProfileVersion        : 4.3.0
ProfileClass          : Display Device Profile
ColorSpaceData        : RGB
ProfileConnectionSpace : XYZ
ProfileDateTime       : 2016:01:01 00:00:00
ProfileFileSignature  : acsp
PrimaryPlatform       : Unknown ( )
CMMFlags              : Not Embedded, Independent
DeviceManufacturer    : 
DeviceModel           : 
DeviceAttributes      : Reflective, Glossy, Positive, Color
RenderingIntent       : Media-Relative Colorimetric
ConnectionSpaceIlluminant : 0.9642 1 0.82491
ProfileCreator        : 
ProfileID              : 0
ProfileDescription     : sRGB
RedMatrixColumn       : 0.43607 0.22249 0.01392
GreenMatrixColumn     : 0.38515 0.71687 0.09708
BlueMatrixColumn      : 0.14307 0.06061 0.7141
MediaWhitePoint       : 0.9642 1 0.82491
RedTRC                : (Binary data 40 bytes, use -b option to extract)
GreenTRC              : (Binary data 40 bytes, use -b option to extract)
BlueTRC               : (Binary data 40 bytes, use -b option to extract)
ProfileCopyright       : Google Inc. 2016

```

```

ProfileCopyright      : Google Inc. 2016
ImageWidth            : 957
ImageHeight           : 1429
EncodingProcess        : Baseline DCT, Huffman coding
BitsPerSample         : 8
ColorComponents        : 3
YCbCrSubSampling      : YCbCr4:2:0 (2 2)
ImageSize             : 957x1429
Megapixels            : 1.4

D:\descargas\exiftool-13.27_64\exiftool-13.27_64>

```

#### 4.1.2 Email

La siguientes e la misma Imagen enviada (redes\_sociales.png), luego se descargo la imagen generada en email de micosoft OutLook, llamada WhatsApp Image 2025-04-12 at 1.30.42 PM.jpeg

```

D:\descargas\exiftool-13.27_64\exiftool-13.27_64>tool.exe -s "d:\descargas\redes_sociales.png"
ExifToolVersion      : 13.27
FileName              : redes_sociales.png
Directory             : d:\descargas
FileSize              : 2.1 MB
ZoneIdentifier        : Exists
FileModifyDate        : 2025:04:12 13:40:39-05:00
FileAccessDate        : 2025:04:12 13:41:40-05:00
FileCreateDate        : 2025:04:12 13:40:38-05:00
FilePermissions       : -rw-rw-rw-
FileType              : PNG
FileTypeExtension     : png
MIMEType              : image/png
ImageWidth            : 957
ImageHeight           : 1429
BitDepth              : 8
ColorType              : RGB with Alpha
Compression            : Deflate/Inflate
Filter                : Adaptive
Interlace              : Noninterlaced
SRGBRendering         : Perceptual
Gamma                 : 2.2
PixelsPerUnitX        : 3778
PixelsPerUnitY        : 3778
PixelUnits             : meters
ImageSize             : 957x1429
Megapixels            : 1.4

D:\descargas\exiftool-13.27_64\exiftool-13.27_64>

```

### 4.1.3 Microsoft Team

La siguientes e la misma Imagen enviada (redes\_sociales.png), luego se descargo la imagen generada en Microsoft Team, llamada tmp\_b3524214-b92d-4bae-9c74-afc807956b62.jpeg

```

D:\descargas\exiftool-13.27_64\exiftool-13.27_64>tool.exe -s "d:\descargas\tmp_b3524214-b92d-4bae-9c74-afc807956b62.jpeg"
ExifToolVersion      : 13.27
FileName              : tmp_b3524214-b92d-4bae-9c74-afc807956b62.jpeg
Directory             : d:\descargas
FileSize              : 263 kB
FileModifyDate        : 2025:04:12 14:27:43-05:00
FileAccessDate        : 2025:04:12 14:29:48-05:00
FileCreateDate        : 2025:04:12 14:28:17-05:00
FilePermissions       : -rw-rw-rw-
FileType              : JPEG
FileTypeExtension     : jpg
MIMEType              : image/jpeg
JFIFVersion           : 1.01
ResolutionUnit        : None
XResolution            : 1
YResolution            : 1
ProfileCMType         : 
ProfileVersion        : 4.3.0
ProfileClass           : Display Device Profile
ColorSpaceData         : RGB
ProfileConnectionSpace : XYZ
ProfileDateTime        : 0000:00:00 00:00:00
ProfileFileSignature   : acsp
PrimaryPlatform        : Unknown ()
CMFlags                : Not Embedded, Independent
DeviceManufacturer     : 
DeviceModel            : 
DeviceAttributes       : Reflective, Glossy, Positive, Color
RenderingIntent        : Media-Relative Colorimetric
ConnectionSpaceIlluminant : 0.9642 1 0.82491
ProfileCreator         : 
ProfileID              : 0
ProfileDescription     : sRGB
RedMatrixColumn        : 0.43607 0.22249 0.01392
GreenMatrixColumn      : 0.38515 0.71687 0.09708
BlueMatrixColumn       : 0.14307 0.06061 0.71411
RedTRC                 : (Binary data 40 bytes, use -b option to extract)
GreenTRC               : (Binary data 40 bytes, use -b option to extract)
BlueTRC                : (Binary data 40 bytes, use -b option to extract)

```

```

RedTRC          : (Binary data 40 bytes, use -b option to extract)
GreenTRC        : (Binary data 40 bytes, use -b option to extract)
BlueTRC         : (Binary data 40 bytes, use -b option to extract)
MediaWhitePoint  : 0.9642 1 0.82491
ProfileCopyright : Google Inc. 2016
ImageWidth      : 957
ImageHeight     : 1429
EncodingProcess  : Baseline DCT, Huffman coding
BitsPerSample    : 8
ColorComponents  : 3
YCbCrSubSampling : YCbCr4:2:0 (2 2)
ImageSize       : 957x1429
Megapixels      : 1.4

D:\descargas\exiftool-13.27_64\exiftool-13.27_64>

```

#### 4.1.4 Telegram

La siguientes e la misma Imagen enviada (redes\_sociales.png), luego se descargo la imagen generada en telegram llamada , llamada 1\_5177145040203416869.png

```

D:\descargas\exiftool-13.27_64\exiftool-13.27_64>tool.exe -s "d:\descargas\1_5177145040203416869.png"
ExifToolVersion      : 13.27
FileName             : 1_5177145040203416869.png
Directory            : d:\descargas
FileSize             : 2.1 MB
FileModifyDate       : 2025:04:12 14:17:57-05:00
FileAccessDate       : 2025:04:12 14:21:07-05:00
FileCreateDate       : 2025:04:12 14:20:48-05:00
FilePermissions      : -rw-rw-rw-
FileType             : PNG
FileTypeExtension    : png
MimeType             : image/png
ImageWidth           : 957
ImageHeight          : 1429
BitDepth             : 8
ColorType            : RGB with Alpha
Compression          : Deflate/Inflate
Filter               : Adaptive
Interlace            : Noninterlaced
SRGBRendering        : Perceptual
Gamma               : 2.2
PixelsPerUnitX       : 3778
PixelsPerUnitY       : 3778
PixelUnits           : meters
ImageSize            : 957x1429
Megapixels           : 1.4

D:\descargas\exiftool-13.27_64\exiftool-13.27_64>

```