

# III Bootcamp Full Stack Cibersecurity

## Módulo 8 - Digital Forensics and Incident Response



### Caso Práctico

**Marcos Alonso González**

[alonsogonzalezmarcos@gmail.com](mailto:alonsogonzalezmarcos@gmail.com)

<https://github.com/magalorn>

22 de mayo de 2022

# Índice

|  |           |
|--|-----------|
| <b>Primera parte</b>                     | <b>4</b>  |
| <b>Planteamiento del caso práctico 1</b> | <b>4</b>  |
| <b>1. Identificación de la máquina</b>   | <b>5</b>  |
| 1.1. Proceso de adquisición              | 5         |
| <b>2. Análisis de artefactos</b>         | <b>7</b>  |
| 2. 1. MFT                                | 7         |
| 2.2. LogFile                             | 13        |
| 2.3. Registros                           | 14        |
| 2.4. Passwords                           | 21        |
| 2.5. Archivos LNK y JumpList             | 23        |
| 2.6. Shellbags                           | 25        |
| 2.6. USB y Prefetch                      | 27        |
| 2.7. Eventos                             | 30        |
| <b>3. Análisis de volumen</b>            | <b>36</b> |
| 3.1. Bulk                                | 36        |
| 3.2. Loki                                | 37        |
| 3.3. Autopsy                             | 39        |
| <b>4. Resumen ejecutivo</b>              | <b>40</b> |
| <b>Segunda parte</b>                     | <b>42</b> |
| <b>Planteamiento del caso práctico 2</b> | <b>42</b> |
| <b>1. Metadatos</b>                      | <b>43</b> |
| Imagen original                          | 44        |
| Imagen por Airdrop                       | 45        |
| Imagen por correo electrónico Gmail      | 47        |
| Imagen por Discord                       | 47        |
| Imagen por Slack                         | 48        |
| Imagen por Telegram                      | 49        |
| Imagen por Whatsapp                      | 49        |
| Conclusiones                             | 50        |



# Primera parte

## Planteamiento del caso práctico 1

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.

Las principales respuestas que debemos darnos son las siguientes:

- Nombre de la máquina y modelo
- ¿Podemos saber el password del usuario?
- Usuarios de la máquina
- Archivos descargados y eliminados
- Carpetas accedidas recientemente
- Usb conectados a la máquina.
- Logon / logoff del sistema.
- Tiene algún servicio de almacenamiento el cloud
- Se han producido accesos de forma remota a la máquina
- Es posible que se haya accedido a documentación de otros equipos ?
- ¿Existe algún proceso sospechoso en la máquina ?

# 1. Identificación de la máquina

Para éste caso práctico vamos a **analizar la imagen de disco con nombre de archivo Win10\_PC001**.

## 1.1. Proceso de adquisición

Para este proceso se va a utilizar la distribución Tsurugi Linux.

La adquisición de la evidencia, en este caso de la imagen de la máquina denominada **Win10\_PC001**, consiste en realizar una copia exacta del dispositivo que tiene que analizar. Hay tres tipos de adquisición: lógica, física y del sistema de archivos.

Para nuestro caso vamos a realizar una adquisición física mediante software. De esta manera dispondremos de una copia idéntica a la original a nivel de byte que contiene la información exacta de la muestra original, incluido los mismos espacios libres en memoria, ficheros de registro, logs, etc.

Para la adquisición se va a utilizar el software [Guymager](#) y se realiza siguiendo estos pasos:

1. Lanzar en la terminal `sudo guymager`
2. En el menu principal de la interfaz de [Guymager](#) -> seleccionar disco a adquirir -> Clic derecho “Adquirir imagen” -> Seleccionar una de las 2 primeras opciones (Linux dd raw image o Expert Witness Format) El 2<sup>a</sup> comprime la imagen, el primero no
3. La adquisición se puede dividir en varias partes, seleccionando en “Split size”, para aquellos discos de gran tamaño.
4. Se rellenan los datos de Case number, examinar, etc. -> Se selecciona el destino de guardado.
5. Rellenar los campos “Image filename” e “info filename” normalmente con el mismo nombre.
6. Hashes -> normalmente seleccionar MD5 y SHA-1 (MD5 solo no porque tiene colisión y no sería válido en un juicio)

7. Se aconseja hacer 2 copias de la adquisición en 2 dispositivos diferentes (una para trabajar con ella y otra para almacenar como la original).
8. En el fichero .info tendremos la información que necesitamos para etiquetar la evidencia.
9. Se adjunta dicho fichero a este informe.

## Datos de la adquisición

**Linux device:** /dev/sdb

**Device size:** 42949672960 (42.9GB)

**Format:** Expert Witness Format, sub-format Guymager - file extension is .Exx

### Image meta data

**Case number:** 001

**Evidence number:** 001

**Examiner:** Marcos Alonso

**Description:** Win10\_PC001

**Notes:** 01000000000000000000000000000001

**Image path and file name:** /home/tsurugi/Desktop/evidence\_test\_001/

Win10\_PC001.Exx

**Info path and file name:** /home/tsurugi/Desktop/evidence\_test\_001/Win10\_PC001.info

**Hash calculation:** MD5 and SHA-1

**Source verification:** off

**Image verification:** on

No bad sectors encountered during acquisition.

**State:** Finished successfully

**MD5 hash:** 23b19aa285bab15522883384debefcbc

**MD5 hash verified source:** --

**MD5 hash verified image:** 23b19aa285bab15522883384debefcbc

**SHA1 hash:** e7ae45de70e5db9183a5ea539689b336abf56969

**SHA1 hash verified source:** --

**SHA1 hash verified image:** e7ae45de70e5db9183a5ea539689b336abf56969

**SHA256 hash:** --

**SHA256 hash verified source:** --

**SHA256 hash verified image:** --

Image verification OK. The image contains exactly the data that was written.

**Acquisition started :** 2022-05-11 04:21:25 (ISO format YYYY-MM-DD HH:MM:SS)

**Verification started:** 2022-05-11 04:40:51

**Ended:** 2022-05-11 04:51:03 (0 hours, 29 minutes and 38 seconds)

**Acquisition speed:** 35.13 MByte/s (0 hours, 19 minutes and 26 seconds)

**Verification speed:** 66.93 MByte/s (0 hours, 10 minutes and 12 seconds)

## 2. Análisis de artefactos

Para el análisis de los artefactos vamos a utilizar, en su mayoría, herramientas de la máquina Windows10 Forensic, una distribución con multitud de herramientas de análisis forense ya instaladas. También se ha utilizado alguna herramienta instalada en Tsurugi Linux.

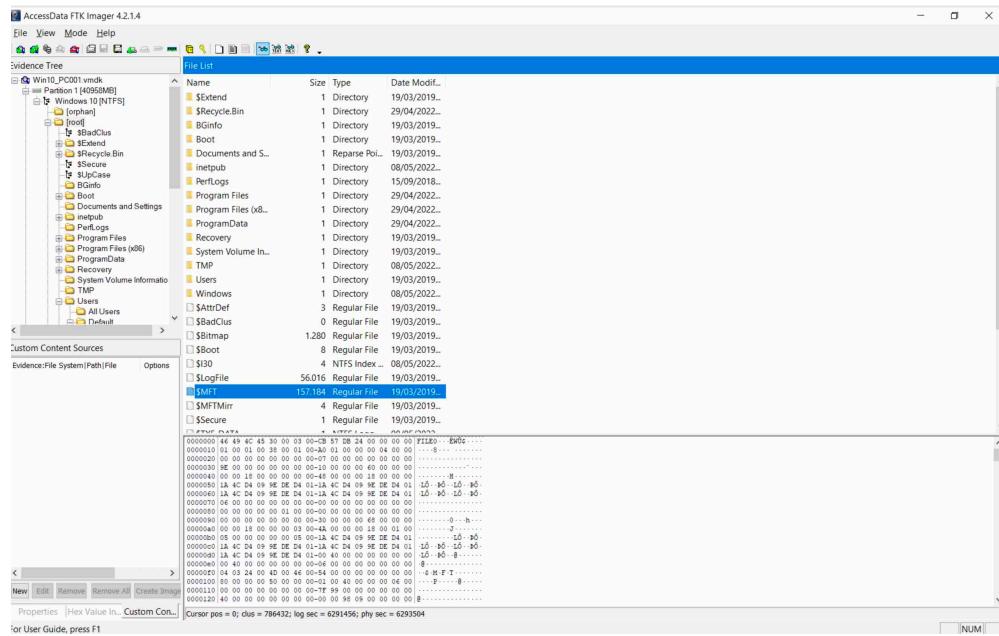
Utilizamos el software [Access Data FTK Imager](#) para poder adquirir la imagen de disco.

Abrimos el programa y seleccionamos File/Add evidence item/Image File y seleccionamos el disco a adquirir/analizar.

A continuación se puede visualizar y navegar por el sistema de archivos de la imagen gracias a la interfaz gráfica de [Access Data FTK Imager](#).

### 2. 1. MFT

En el directorio [root] se puede localizar el archivo en el que vamos a centrar ahora el análisis, el \$MFT.



Este archivo almacena la **MFT (Master File Table)**, una tabla que muestra un registro de todo lo que ha ocurrido con el sistema de ficheros del que consta la imagen de disco.

**Access Data FTK Imager** permite además con su visor hexadecimal el contenido de los ficheros sin tener que abrirlo.

Se encuentran en la carpeta root\TMP los ejecutables:

- p.exe
- nbtscan.exe
- xCmd.exe
- WMIBackdoor.ps1

Se adjuntan a este informe estos archivos en la carpeta comprimida con nombre “malware-TMP”

8. Con un análisis realizado desde [Virus Total](#) sobre este encontramos lo siguiente:

- p.exe Este no es en sí mismo un archivo malicioso. Sin embargo, los actores de amenazas pueden utilizarlo con fines maliciosos, como en la campaña de ransomware Petya/Goldeneye.

## - nbtscan.exe

**Detection**

① 29 security vendors and no sandboxes flagged this file as malicious

c9d5dc956841e000bfd8762e2f0b48b66c79b79500e894b4efa7fb9ba17e4e9e  
nbtscan-1.0.35.exe

Community Score: 29 / 66

File type: EXE

Size: 36.00 KB | 2022-05-13 00:42:39 UTC | 4 hours ago

[Explore in VirusTotal Graph](#)

| DETECTION                           | DETAILS                    | RELATIONS  | BEHAVIOR                                    | COMMUNITY |
|-------------------------------------|----------------------------|------------|---|-----------|
| <b>Security Vendors' Analysis</b> ① |                            |            |   |           |
| Ad-Aware                            | ① Application NbtScan A    | ALYac      | ① Trojan.Agent.36864N                       |           |
| Avast                               | ① FileRepMalware [PUP]     | AVG        | ① FileRepMalware [PUP]                      |           |
| BitDefender                         | ① Application NbtScan.A    | Bkav Pro   | ① W32.Common.2F1TC3E5                       |           |
| Comodo                              | ① AppliUnwnt@#1k2cnsoy0hfh | Cyren      | ① W32.Tool.XMUR-5657                        |           |
| DrWeb                               | ① Program NbtScan.1        | Elastic    | ① Malicious (high Confidence)               |           |
| eScan                               | ① Application NbtScan A    | ESET-NOD32 | ① A Variant Of Win32/NetTool.Nbtscan.B P... |           |
| Fortinet                            | ① Riskware/Nbtscan         | GData      | ① Application NbtScan A                     |           |

**Basic Properties** ①

|                     |  |
|---------------------|--|
| MD5                 | f01a9a2d1e31332ed36c1a4d2839f412   |
| SHA-1               | 90da004c8ffafada2cf18922670a745564f45  |
| SHA-256             | c9d5dc956841e000bfd8762e2f0b48b66c79b79500e894b4efa7fb9ba17e4e9e                     |
| Vhash               | 034036551d1bz2ze=z   |
| Authentihash        | 0dfabaf2239d6523dtc8545bd9850ac5c4ef349fa46cfb8a9bc929d4f583e4a                      |
| ImpHash             | 2fa43c5392ec7923babced078c298d   |
| Rich PE header hash | 646371930ed0f8b2699ba56d2e671296   |
| SSDeep              | 384 x1+ZbDD0fdyxM5cel8cmoGfOyGPko7DPzwVkgI+kFab6BCXS2brlszQ T+4f9l8YCGPk7GYkEb4CXSwX |
| TLSH                | T146F2E8157581802DE01103B2917249767AF75AA1238041CFBF93AA59BF86C3B6FCE4F              |
| File type           | Win32 EXE  |
| Magic               | PE32 executable for MS Windows (console) Intel 80386 32-bit                          |
| TrID                | Microsoft Visual C++ compiled executable (generic) (33.5%)                           |
| TrID                | Win64 Executable (generic) (21.3%)   |
| TrID                | Win32 Dynamic Link Library (generic) (13.3%)   |
| TrID                | Win16 NE executable (generic) (10.2%)  |
| TrID                | Win32 Executable (generic) (9.1%)  |
| File size           | 36.00 KB (36864 bytes)   |
| PEiD packer         | Microsoft Visual C++   |

**Execution Parents** ①

| Scanned    | Detections | Type      | Name   |
|------------|------------|-----------|--|
| 2021-03-08 | 55 / 70    | Win32 EXE | virussign.com_457162dd4303d9a2cd0ce994e832a6e0.vir |
| 2020-04-28 | 39 / 53    | ZIP       | all.zip  |
| 2019-11-07 | 16 / 71    | Win32 EXE | IPS_Injector.exe                                   |
| 2022-05-04 | 34 / 68    | Win32 EXE | 943499   |
| 2022-02-16 | 31 / 69    | Win32 EXE | lantopolog232_setup(20).exe                        |
| 2021-03-03 | 59 / 66    | Win32 EXE | nbtscan.exe  |
| 2022-05-06 | 22 / 51    | Win32 EXE | b  |
| 2021-09-21 | 17 / 69    | Win32 EXE | ComputerInfo.exe                                   |
| 2022-05-07 | 33 / 69    | Win32 EXE | lantopolog232_setup.exe                            |
| 2019-11-07 | 33 / 69    | Win32 EXE | 7ZSfxNew   |
| 2019-11-07 | 43 / 72    | Win32 EXE | vt-upload-yMeGr                                    |
| 2020-10-27 | 52 / 66    | ZIP       | Cobalt-Strike-Aggressor-Scripts-master.zip         |
| 2021-02-22 | 33 / 62    | ZIP       | INFECTED.zip                                       |

**PE Resource Parents** ①

| Scanned    | Detections | Type      | Name        |
|------------|------------|-----------|-------------|
| 2021-03-03 | 59 / 66    | Win32 EXE | nbtscan.exe |

**Dropped Files** ①

| Scanned    | Detections | Type | Name  |
|------------|------------|------|---|
| 2021-05-07 | 2 / 58     | Text | ConDrv  |
| 2021-05-10 | 1 / 57     | Text | ConDrv  |
| ?          | ?          | file | 0D7C290D7AE64D629168B7D2439BC319ED6456D909BD483CEDB1FCB69E2071E |

## - xCmd.exe

Σ 6c8eea3ba31463a04d041f4c9ff50b50d9b5945d3306fee35fb4b5bfd292692b

55 /70 ① 55 security vendors and 1 sandbox flagged this file as malicious

6c8eea3ba31463a04d041f4c9ff50b50d9b5945d3306fee35fb4b5bfd292692b  
xCmd.exe detect-debug-environment peexe

824.00 KB | 2022-02-09 11:58:55 UTC | 3 months ago | EXE

**DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY**

**Security Vendors' Analysis**

| Vendor           | Detection                          | Tool               | Description                         |
|------------------|------------------------------------|--------------------|-------------------------------------|
| Ad-Aware         | ① Trojan.GenericKD.43493830        | AhnLab-V3          | ① Trojan/Win32.Agent.C2624349       |
| Ali巴巴            | ① Backdoor.Win32.DarkKomet.b59473C | ALYac              | ① Trojan.GenericKD.43493830         |
| Anti-AVL         | ① Trojan/Generic.ASMalwS.3104EDF   | Arcabit            | ① Trojan.Generic.D297A9C6           |
| Avast            | ① Win32.Malware-gen                | AVG                | ① Win32.Malware-gen                 |
| Avira (no cloud) | ① TR/Crypt.TPM.Gen                 | BitDefender        | ① Trojan.GenericKD.43493830         |
| BitDefenderTheta | ① Gen NN ZexafF34212.Zy0aaiLRHGpi  | Bkav Pro           | ① W32.AIDetect.malware1             |
| Comodo           | ① TroyWare.Win32.Agent.COC@52vn2u  | CrowdStrike Falcon | ① Win/malicious_confidence_100% (W) |
| Cybereason       | ① Malicious.36b409                 | Cylance            | ① Unsafe                            |
| Cynet            | ① Malicious (score: 100)           | DrWeb              | ① Tool.xCmd                         |

Σ 6c8eea3ba31463a04d041f4c9ff50b50d9b5945d3306fee35fb4b5bfd292692b

55 /70 ① 55 security vendors and 1 sandbox flagged this file as malicious

6c8eea3ba31463a04d041f4c9ff50b50d9b5945d3306fee35fb4b5bfd292692b  
xCmd.exe detect-debug-environment peexe

824.00 KB | 2022-02-09 11:58:55 UTC | 3 months ago

**DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY**

**Basic Properties**

|                     |  |
|---------------------|--|
| MD5                 | 27aee7f36b4099e8db3e3d3898474196   |
| SHA-1               | c26dc6e4ef77cafafa154fa9529c4ce79a8fc78b                                 |
| SHA-256             | 6c8eea3ba31463a04d041f4c9ff50b50d9b5945d3306fee35fb4b5bfd292692b         |
| Vhash               | 08506f6d6d11f7f11z17z1l2   |
| Authentihash        | e487980ea13ec926c2461180f668a84ed3d8cff029c23b4f51ce27ebc821f6b          |
| Imphash             | baa93d47220682c04d92f7797d9224ce   |
| Rich PE header hash | 67ebd3a6a3d5f08d768b1be8314d3715   |
| SSDEEP              | 24576:+qsaXJShxufrtC3dYx//aTjkIIChmS2m6hEQP:+qsaXkhDibtxzSUIICf76hEQ     |
| TLSH                | T19B05232B8B7E408DF08F5BF39B059BCFFA15480E41BF9948583DB46FE0253D8426A959 |
| File type           | Win32 EXE  |
| Magic               | PE32 executable for MS Windows (console) Intel 80386 32-bit              |
| TrID                | Win32 Dynamic Link Library (generic) (29.6%)                             |
| TrID                | Win16 NE executable (generic) (22.7%)                                    |
| TrID                | Win32 Executable (generic) (20.3%)                                       |
| TrID                | OS/2 Executable (generic) (9.1%)   |
| File size           | 824.00 KB (843776 bytes)   |

## - WMBackdoor.ps1

9. Se exporta el fichero \$MFT y lo guardamos en local

Ahora vamos a usar [Kape](#) para analizar algunos archivos de interés de la imagen del disco. Este proceso es conocido como triage.

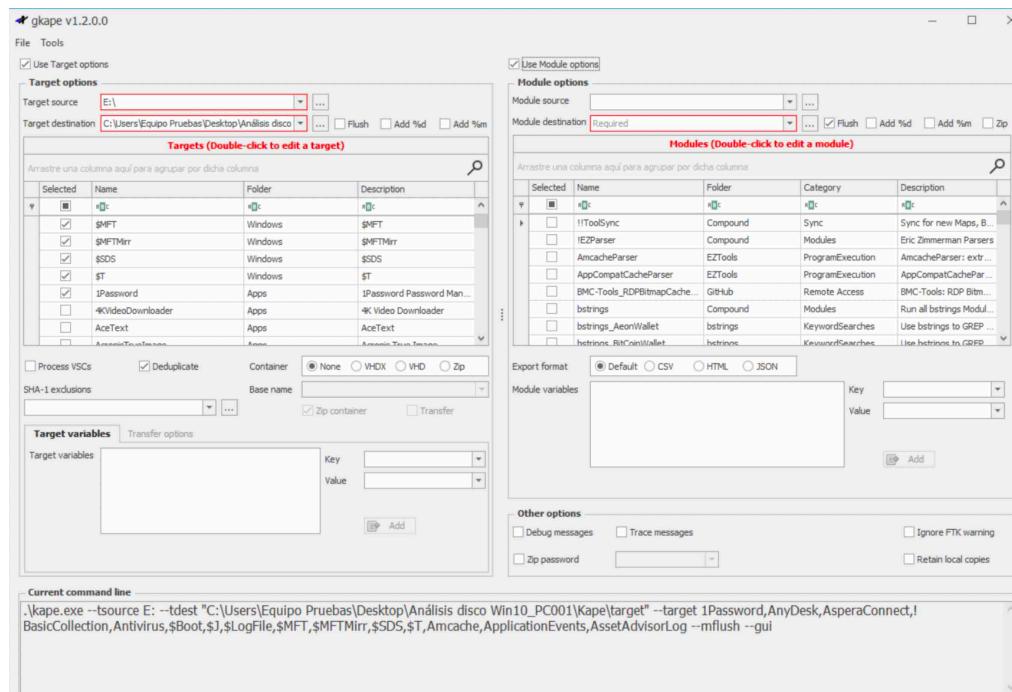
Primero, hay que montar la imagen del disco con el software Arsenal Image Mounter, ya que Kape no funciona para imágenes.

Abrimos la GUI de [Kape](#) con el fichero gkape, y en la sección “Target options” seleccionamos los módulos que queremos pasarle para la extracción de ficheros del disco relacionados con los módulos que le hemos asado y guardamos los resultados en un .zip.

Adicionalmente, se puede copiar la linea de comando que aparece en la ventana inferior de la interfaz gráfica, ya que puede usarse, por ejemplo, para extraer los ficheros que nos interesen de la imagen de disco con [Kape](#) en remoto, mediante SFTP o servicios en la nube como Azure.

Para finalizar, se pulsa “Execute” y nos guarda los ficheros extraídos en la carpeta indicada.

**Importante:** Desmarcar la opción “Flush” junto al campo “Target Destination”, ya que elimina lo que hay guardado en su caso.



Seguidamente hay que hacer el procesamiento de los archivos extraídos, ejecutándolos con la sección “Module options”.

El primer paso es seleccionar el directorio donde están los artefactos que queremos analizar, en este caso en “target”. Para el destino de los análisis, creamos una carpeta para guardarlos, en este caso “modules”.

Se desactiva también el flush y se seleccionan las herramientas que se quieren ejecutar, en relación con cada fichero que hemos extraído anteriormente.

Se adjuntan a este informe los ficheros de la imagen extraídos mediante [Kape](#).

Llegados a este punto, es importante utilizar herramientas como [MFTEmcmd.exe](#), que nos va a permitir parsear la MFT para así poder interpretarla. Se utiliza con comandos. Nos ubicamos en la carpeta donde está el ejecutable MFTEmcmd.exe y lo lanzamos con

```
MFTEmcmd.exe -f <path donde está el archivo MFT> --csv <path para guardar output> --csvf <nombre del fichero>
```

A continuación puede utilizarse la herramienta [Timeline Explorer](#), Util para leer el archivo .csv que se ha generado con MTFECmd, ya que lo saca en forma de fichero excel y se puede filtrar por columnas para que o ordene por los valores que nos interesan visualizar, por ejemplo para ver los ficheros con extensión .exe en una determinada fecha. Así, se obtiene la siguiente información respecto a ficheros .bat

| Line  | Tag              | Entry Number | Seq.             | Parent ... | Paren... | In Use | Parent Path                               | File Name                    |
|-------|------------------|--------------|------------------|------------|----------|--------|---|------------------------------|
| ▼     | =                | =            | =                | =          | =        | =      | █   | █                            |
| ▼     | Last Access0x10: | 01/01/2019   | (Recuento=2)     |            |          |        |   |                              |
| ▼     | Extension:       | .bat         | (Recuento=2)     |            |          |        |   |                              |
| 18... | □                | 156902       | 3                | 156898     | 2        | □      | .\Users\IEUser\AppData\Local\Temp\dist... | js-dropper.bat               |
| 18... | □                | 156918       | 3                | 156912     | 2        | □      | .\Users\IEUser\AppData\Local\Temp\dist... | userinit-mpr-logonscript.bat |
| ▼     | Last Access0x10: | 29/10/2018   | (Recuento=1399)  |            |          |        |   |                              |
| ▼     | Last Access0x10: | 15/09/2018   | (Recuento=25446) |            |          |        |   |                              |
| ▼     | Last Access0x10: | 09/04/2018   | (Recuento=12)    |            |          |        |   |                              |
| ▼     | Extension:       | .bat         | (Recuento=12)    |            |          |        |   |                              |
| 18... | □                | 156885       | 3                | 156884     | 2        | □      | .\Users\IEUser\AppData\Local\Temp\dist... | collect-local-files.bat      |
| 18... | □                | 156890       | 3                | 156886     | 2        | □      | .\Users\IEUser\AppData\Local\Temp\dist... | netcat-back-connect.bat      |
| 18... | □                | 156894       | 3                | 156893     | 2        | □      | .\Users\IEUser\AppData\Local\Temp\dist... | lsass-dump.bat               |
| 18... | □                | 156900       | 3                | 156898     | 2        | □      | .\Users\IEUser\AppData\Local\Temp\dist... | fake-system-file.bat         |
| 18... | □                | 156903       | 3                | 156898     | 2        | □      | .\Users\IEUser\AppData\Local\Temp\dist... | obfuscation1.bat             |
| 18... | □                | 156905       | 3                | 156904     | 2        | □      | .\Users\IEUser\AppData\Local\Temp\dist... | nbtscan.bat                  |
| 18... | □                | 156908       | 3                | 156907     | 2        | □      | .\Users\IEUser\AppData\Local\Temp\dist... | psexec.bat                   |
| 18... | □                | 156909       | 3                | 156907     | 2        | □      | .\Users\IEUser\AppData\Local\Temp\dist... | remote-exe-tools.bat         |
| 18... | □                | 156915       | 3                | 156912     | 2        | □      | .\Users\IEUser\AppData\Local\Temp\dist... | schtasks-xml.bat             |
| 18... | □                | 156917       | 3                | 156912     | 2        | □      | .\Users\IEUser\AppData\Local\Temp\dist... | sticky-key-backdoor.bat      |
| 18... | □                | 156919       | 3                | 156912     | 2        | □      | .\Users\IEUser\AppData\Local\Temp\dist... | web-shells.bat               |
| 18... | □                | 156920       | 3                | 156912     | 2        | □      | .\Users\IEUser\AppData\Local\Temp\dist... | wmi-backdoor.bat             |

| Line  | Tag | Entry Number | Seq. | Parent ... | Paren... | In Use | Parent Path                               | File Name                      | I |
|---|-----|--------------|------|------------|----------|--------|---|--------------------------------|---|
| Y   | -   | -            | -    | -          | -        | -      | -   | IEUser                         |   |
| <b>▼ Last Access@0x10: 02/03/2018 (Recuento=10)</b> |     |              |      |            |          |        |   |                                |   |
| <b>▼ Extension: .bat (Recuento=10)</b>              |     |              |      |            |          |        |   |                                |   |
| 18...   | □   | 156887       | 3    | 156886     | 2        | □      | .\Users\IEUser\AppData\Local\Temp\dist... | c2-connect.bat                 |   |
| 18...   | □   | 156888       | 3    | 156886     | 2        | □      | .\Users\IEUser\AppData\Local\Temp\dist... | dns-cache-1.bat                |   |
| 18...   | □   | 156889       | 3    | 156886     | 2        | □      | .\Users\IEUser\AppData\Local\Temp\dist... | malicious-user-agents.bat      |   |
| 18...   | □   | 156897       | 3    | 156893     | 2        | □      | .\Users\IEUser\AppData\Local\Temp\dist... | wce-1.bat                      |   |
| 18...   | □   | 156899       | 3    | 156898     | 2        | □      | .\Users\IEUser\AppData\Local\Temp\dist... | active-guest-account-admin.bat |   |
| 18...   | □   | 156901       | 3    | 156898     | 2        | □      | .\Users\IEUser\AppData\Local\Temp\dist... | hosts-manipulation.bat         |   |
| 18...   | □   | 156906       | 3    | 156904     | 2        | □      | .\Users\IEUser\AppData\Local\Temp\dist... | recon-cmd-activity.bat         |   |
| 18...   | □   | 156913       | 3    | 156912     | 2        | □      | .\Users\IEUser\AppData\Local\Temp\dist... | at-jobs.bat                    |   |
| 18...   | □   | 156914       | 3    | 156912     | 2        | □      | .\Users\IEUser\AppData\Local\Temp\dist... | run-key.bat                    |   |
| 18...   | □   | 156916       | 3    | 156912     | 2        | □      | .\Users\IEUser\AppData\Local\Temp\dist... | schtasks.bat                   |   |
| <b>▼ Last Access@0x10: 05/02/2018 (Recuento=2)</b>  |     |              |      |            |          |        |   |                                |   |
| <b>▼ Extension: .bat (Recuento=2)</b>               |     |              |      |            |          |        |   |                                |   |
| 18...   | □   | 156911       | 3    | 156910     | 2        | □      | .\Users\IEUser\AppData\Local\Temp\dist... | lateral-movement.bat           |   |
| 18...   | □   | 156922       | 3    | 156921     | 2        | □      | .\Users\IEUser\AppData\Local\Temp\dist... | privilege-escalation.bat       |   |

**Timeline Explorer** permite por tanto hacer seguimiento de un fichero para ver que ha ocurrido con él a lo largo del tiempo, cuando se ha creado, ejecutado, modificado, etc. y también para ver que ha ocurrido en el sistema en una determinada fecha, que ficheros se han borrado, creado, etc.

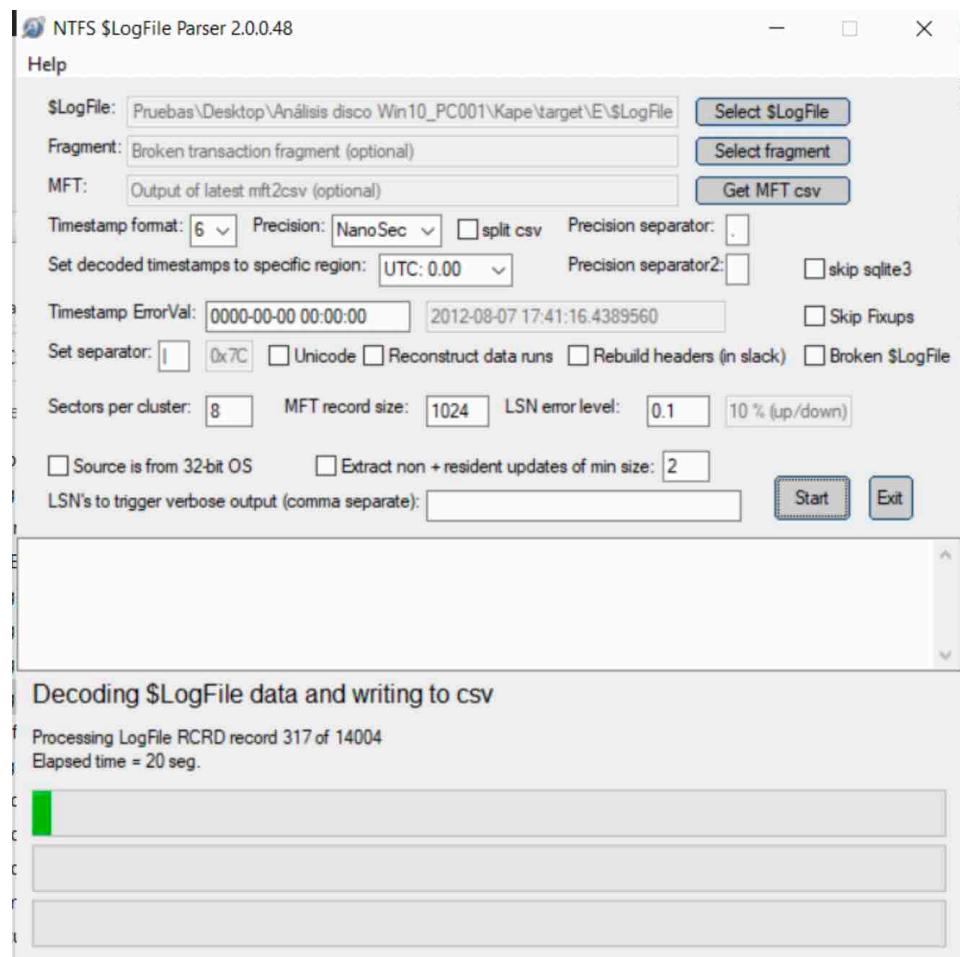
## 2.2.LogFile

Hay otro fichero que es importante también analizar, el **\$LogFile**. Este contiene información que permite al sistema de archivos (NTFS, New Technology File System) retornar a estados anteriores, ya que contiene información de las transacciones que se producen con los archivos: creación, renombrado, borrado, modificación, copia, etc.

Para su interpretación, se va a usar el software [LogFileParser](#), de uso sencillo, solo introducir el fichero \$LogFile que hemos extraído de la imagen del disco Win10\_PC001 y pulsar Start.

Se generan varios archivos .csv que contienen diferentes registros de logs que pueden ser leídos con **Timeline Explorer**, si bien para su interpretación requieren de un análisis exhaustivo.

Se adjuntan a este informe los ficheros .csv obtenidos.



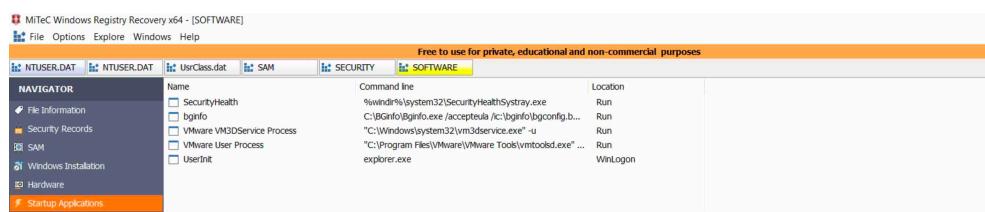
## 2.3. Registros

Vamos ahora a analizar los siguientes registros:

- DEFAULT -> HKEY\_LOCAL\_MACHINE
- NTUSER.DAT -> HKEY\_LOCAL\_MACHINE
- SAM -> HKEY\_LOCAL\_MACHINE
- SECURITY-> HKEY\_LOCAL\_MACHINE
- SYSTEM -> HKEY\_LOCAL\_MACHINE
- SOFTWARE -> HKEY\_LOCAL\_MACHINE

Se pueden utilizar tres herramientas para analizar los registros del disco, todas disponen de interfaz gráfica: son [Registry Explorer](#), [RegRipper](#) y [Windows Registry Recovery](#).

Se ha obtenido cuales son las startup applications del usuario **IEUUser** con [Windows Registry Recovery](#).



Utilizando [RegRipper](#) podemos extraer la información interpretada en un .txt y ver entre otras cosas cuales han sido los **comandos que se han utilizado recientemente** por el usuario, en la sección **Most Recently Used (MRU)**, que se encuentra en NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDIMRU, en este caso son los siguientes:

```

C:\Users\Equipo Pruebas\Desktop\Análisis disco Win10_PC001\Evidence Analysis\ntuserdat_RegRipper.txt - Notepad++
Archivo Editar Buscar Vista Codificación Lenguaje Configuración Herramientas Macro Ejecutar Plugins Ventana ?
ntuserdat_RegRipper.txt

770 - Gets contents of user's RecentApps key
771
772 Software\Microsoft\Windows\CurrentVersion\Search\RecentApps not found.
773 -----
774 recentdocs v.20200427
775 (NTUSER.DAT) Gets contents of user's RecentDocs key
776
777 RecentDocs
778 **All values printed in MRUList\MRUListEx order.
779 Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
780 LastWrite Time: 2022-05-08 18:53:38Z
781     10 = manualproyectos.pdf
782         1 = My Drive
783         2 = GINF-G-006 Guia para una Contraseña Segura.doc
784         0 = Documento Seguridad HipoSEMG.doc
785         11 = archivos
786         9 = Network and Internet
787         6 = :::{8E908FC9-BECC-40F6-915B-F4CA0E70D03D}
788         8 = The Internet
789         7 = network/
790         5 = 192.168.183.134/
791         4 = instagram-posts-collection-qr-code-scanning-with-smartphone
792         3 = 4953651.jpg
793
794 Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.134/
795 LastWrite Time 2022-04-29 09:52:32Z
796 MRUListEx = 0
797     0 = 192.168.183.134/
798
799 Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.doc
800 LastWrite Time 2022-04-29 10:30:10Z
801 MRUListEx = 1,0
802     1 = GINF-G-006 Guia para una Contraseña Segura.doc
803     0 = Documento Seguridad HipoSEMG.doc

804
805 Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.jpg
806 LastWrite Time 2022-04-29 09:21:16Z
807 MRUListEx = 0
808     0 = 4953651.jpg
809
810 Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.pdf
811 LastWrite Time 2022-05-08 18:53:38Z
812 MRUListEx = 0
813     0 = manualproyectos.pdf
814
815 Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder
816 LastWrite Time 2022-04-29 10:30:10Z
817 MRUListEx = 0,4,3,2,1
818     0 = My Drive
819     4 = archivos
820     3 = Network and Internet
821     2 = The Internet
822     1 = instagram-posts-collection-qr-code-scanning-with-smartphone
823
824 -----

```

Se ha podido extraer de NTUSER.DAT **la primera vez que se ha hecho logon en el sistema:**

**613 FirstLogonTime: Tue Mar 19 13:00:06 2019**

E igualmente se han comprobado los programas que se han añadido al **autoarranque** del sistema y en la fecha que se ha realizado.

```

325 run v.20200511
326 (Software, NTUSER.DAT) [Autostart] Get autostart key contents from Software hive
327
328 Software\Microsoft\Windows\CurrentVersion\Run
329 LastWrite Time 2022-04-29 09:58Z
330     OneDrive - "C:\Users\IEUser\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background
331     GoogleDriveFS - "C:\program Files\Google\Drive File Stream\57.0.5.0\GoogleDriveFS.exe" --startup_mode
332

```

Esto es importante averiguarlo porque gracias a este registro puede observarse si se ha implantado algún malware y ha creado persistencia, por ejemplo, a través de un Command and Control. Con el análisis en [Hybrid Analysis](#) vemos en una de las firmas que es habitual que este malware cree acceso remoto en el registro HKLM\SYSTEM\CONTROLSET001\CONTROL\TERMINAL SERVER por lo que es posible que utilice el C2 para la persistencia.

The screenshot shows the Hybrid Analysis interface with the following details:

- Suspicious Indicators:** 7
- Installation/Persistence:**
  - Contains ability to download files from the internet
  - Monitors specific registry key for changes
- Network Related:**
  - Found potential IP address in binary/memory
- Pattern Matching:**
  - Contains ability to download files from the internet
- Remote Access Related:**
  - Reads terminal service related keys (often RDP related)
    - details "nbtscan.exe" (Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\TERMINAL SERVER"; Key: "TSUSERENABLED")
    - source Registry Access
    - relevance 10/10
    - ATT&CK ID T1076 ([Show technique in the MITRE ATT&CK™ matrix](#))
- Unusual Characteristics:**
  - Imports suspicious APIs
  - Installs hooks/patches the running process

Para analizar esto podemos recurrir al parseo del registro SYSTEM, donde ubicamos la ruta ControlSet001\Control\Terminal Server y podríamos averiguar si se ha producido conexión remota. Por otro lado, al extraer ficheros con [Kape](#), se observa que en E:\ProgramFiles/TeamViewer/Conectionsincoming, hay dos logs remotos de la máquina [WIN-MORENIN](#) con IEUser con fecha 29-04-22, lo que puede ser uno de los vectores de ataque.

```

7496 Certificate value not found.
7497 -----
7498 ControlSet001\Control\Terminal Server
7499 LastWrite Time 2022-04-29 10:38:33Z
7500
7501 ProductVersion = 5.1
7502
7503 fDenyTSConnections = 1
7504 1 = connections denied
7505
7506
7507
7508
7509 TSUserEnabled = 0
7510 1 = All users logging in are automatically part of the
7511 built-in Terminal Server User group. 0 = No one is a
7512 member of the built-in group.
7513 Ref: http://support.microsoft.com/kb/238965
7514
7515 fSingleSessionPerUser = 1
7516
7517 AutoStart Locations
7518 Wds\rdpwd key
7519   StartupPrograms: rdpclip
7520 Analysis Tip: This value usually contains 'rdpclip'; any additional entries
7521 should be investigated.
7522
7523 WinStations\RDP-Tcp key
7524   InitialProgram: {blank}
7525 Analysis Tip: Maybe be empty; appears as '{blank}'
7526 WinStations\RDP-Tcp key
7527   SecurityLayer: 2
7528 Analysis Tip: Maybe be empty; appears as '{blank}'
7529 SysProcs key values
7530 LastWrite: 2018-09-15 07:34:18Z
7531   clipsrv.exe - 0
7532   conime.exe - 0
7533   ctfmon.exe - 0
7534   dwm.exe - 0
7535   imepadsv.exe - 0
7536   lmsvcs.exe - 0

```

También con [RegRipper](#) analizando el registro SAM podemos localizar el **nombre de todos los usuarios de la máquina**, que son los siguientes:

[Administrator \[500\]](#)

[Guest \[501\]](#)

[DefaultAccount \[503\]](#)

[WDAGUtilityAccount \[504\]](#)

[IEUser \[1000\]](#)

[sshd \[1002\]](#)

Se puede observar que el único usuario que ha hecho intentos de logins en la imagen, hasta un total de 18, con intentos de meter password fallidos con fecha 29/04/2022 ha sido el usuario **IEUser**, por lo que esto da una pista para centrar la investigación en este usuario. Se observa que la última vez que se ha logueado en el sistema este usuario ha sido el 08/05/2022.

```

69 Username      : IEUser [1000]
70 Full Name     : IEUser
71 User Comment   : IEUser
72 Account Type   :
73 Account Created : 2019-03-19 20:57:23Z
74 Name          :
75 Last Login Date : 2022-05-08 18:52:36Z
76 Pwd Reset Date : 2022-04-29 16:41:59Z
77 Pwd Fail Date  : 2022-04-29 10:38:41Z
78 Login Count    : 18
79 Embedded RID   : 1000
80      --> Password does not expire
81      --> Normal user account
82
83 Username      : sshd [1002]
84 Full Name     : sshd
85 User Comment   :
86 Account Type   :
87 Account Created : 2019-03-19 13:23:55Z
88 Name          :
89 Last Login Date : Never
90 Pwd Reset Date : 2019-03-19 13:23:55Z
91 Pwd Fail Date  : Never
92 Login Count    : 0
93 Embedded RID   : 1002
94      --> Password does not expire
95      --> Normal user account
96

```

Gracias a [Access Data FTK Imager](#) conseguimos averiguar cuales han sido los **ficheros descargados por IEUser**:

| Name                          | Size    | Type          | Date Modif... |
|-------------------------------|---------|---------------|---------------|
| \$130                         | 4       | NTFS Index... | 29/04/2022... |
| desktop.ini                   | 1       | Regular File  | 19/03/2019... |
| GoogleDriveSetup.exe          | 282.281 | Regular File  | 29/04/2022... |
| LibreOffice_7.3.2_Win_x64.msi | 339.980 | Regular File  | 29/04/2022... |
| TeamViewer_Setup_x64.exe      | 36.523  | Regular File  | 29/04/2022... |

El registro SAM también nos permite ver los grupos creados y los usuarios que pertenecen a ellos. Se incluyen aquí los que cuentan con algún usuario por ser lo más relevantes, ya que hay muchos grupos creados que no cuentan con ninguno.

```

105 Group Name      : Guests [1]
106 LastWrite       : 2019-03-19 20:55:22Z
107 Group Comment   : Guests have the same access as members of the Users group by default, except for the Guest account
108 Users :
109     S-1-5-21-321011808-3761883066-353627080-501
110

131 Group Name      : IIS_IUSRS [1]
132 LastWrite       : 2019-03-19 20:55:22Z
133 Group Comment   : Built-in group used by Internet Information Services.
134 Users :
135     S-1-5-17

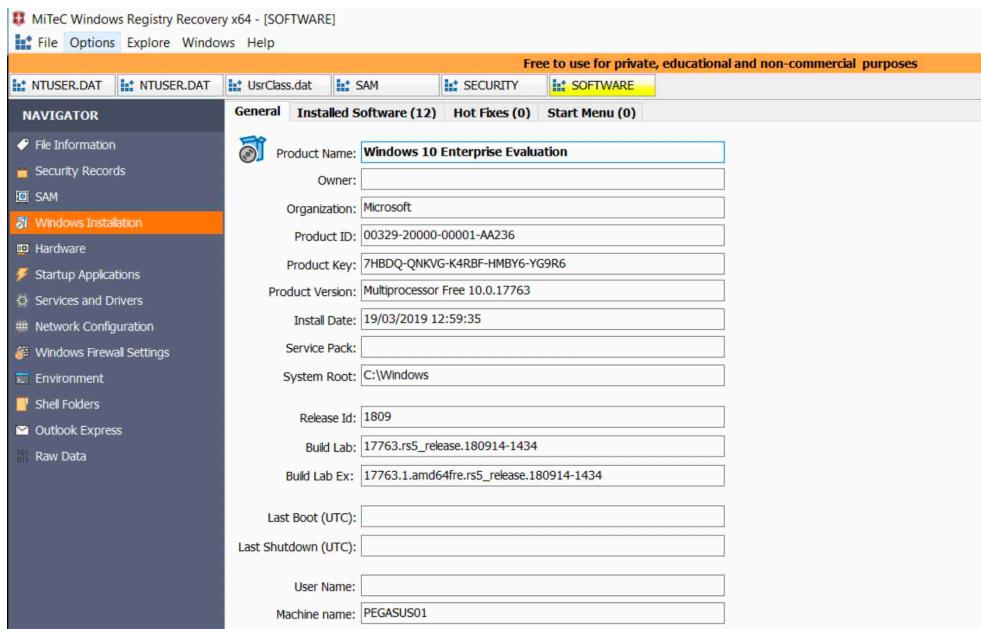
155 Group Name      : System Managed Accounts Group [1]
156 LastWrite       : 2019-03-19 20:55:22Z
157 Group Comment   : Members of this group are managed by the system.
158 Users :
159     S-1-5-21-321011808-3761883066-353627080-503

166 Group Name      : Administrators [3]
167 LastWrite       : 2022-05-08 19:06:51Z
168 Group Comment   : Administrators have complete and unrestricted access to the computer/domain
169 Users :
170     S-1-5-21-321011808-3761883066-353627080-501
171     S-1-5-21-321011808-3761883066-353627080-1000
172     S-1-5-21-321011808-3761883066-353627080-500
173

```

Cómo se puede observar, en el grupo de Administradores se encuentra el usuario con ID 1000, que corresponde a **IUser**, lo que puede indicar que este ha sido el usuario utilizado para elevar privilegios y poder realizar acciones maliciosas en el sistema.

Con el registro SOFTWARE podemos conseguir el **tipo de máquina al que pertenece la imagen y el nombre de la misma**, que en este caso es un **Windows 10 Enterprise Evaluation**, la versión del SO es **10.0.17763 N/A Build 17763** de arquitectura **X64-based PC**, creado con VMWare con el nombre **PEGASUS01**



Además, se puede hallar información más ampliada del sistema gracias a que se descubre un fichero de nombre sys.txt (que se adjunta a este informe) en el directorio.

También en el archivo adjunto 127.0.0.1.txt localizado en el mismo directorio y también adjunto, se localizan los usuarios utilizados por [APT Simulator](#), un Batch Script de Windows que utiliza un conjunto de herramientas y archivos de salida para hacer que un sistema parezca comprometido.

También con este mismo registro podemos averiguar el software que tiene instalado la máquina de la imagen analizada:

| General                     | Installed Software (12) | Hot Fixes (0) | Start Menu (0) |
|-----------------------------|-------------------------|---------------|----------------|
| <b>NAVIGATOR</b>            |                         |               |                |
| File Information            |                         |               |                |
| Security Records            |                         |               |                |
| SAM                         |                         |               |                |
| <b>Windows Installation</b> |                         |               |                |
| Hardware                    |                         |               |                |
| Startup Applications        |                         |               |                |
| Services and Drivers        |                         |               |                |
| Network Configuration       |                         |               |                |
| Windows Firewall Settings   |                         |               |                |
| Environment                 |                         |               |                |
| Shell Folders               |                         |               |                |

## 2.4. Passwords

Para intentar hallar la **contraseña de los usuarios de PEGASUS01** puede utilizarse [mimikatz.exe](#). Se lanza el comando de ejecución sobre los registros analizados anteriormente:

```
lsadump::sam /system:C:\SYSTEM /sam:C:\SAM /software:C:\SOFTWARE
```

```
mimikatz 2.2.0 x64 (oe.eo)
# lsadump::sam /system:C:\SYSTEM /sam:C:\SAM /software:\SOFTWARE
Domain : PEGASUS01
SysKey : ec022a7f903a7e69e03e0c84634ff0
Local SID : S-1-5-21-321011808-376183066-353627080
SAMKey : 939177c671faafb0f1d1f10bc6de1190

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) : 182f0bb1b0e1b1b70acb8113d293710d48
        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: 20ff0389f84bd9f9ce6fc36af6993b63

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : ac32ca55378d84ed6d3472f0b728b7bd

* Primary:Kerberos-Newer-Keys *
    Default Salt : WDAGUtilityAccount
    Default Iterations : 4096
    Credentials
        aes256_hmac      (4096) : fb60f0d32a8abb7dd991ae530844c927fb25380ffffeb119cc0d0971c5be8df321
        aes128_hmac      (4096) : e4617e2dd5e029348f552ece98695ddb

[?] Seleccionar mimikatz 2.2.0 x64 (oe.eo)
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 : IIEUser
Hash NTLM: 2d20d252a479f485cdf5e171d93985bf

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : c6807d33d3772144ce3407a8a73f9ef

* Primary:Kerberos-Newer-Keys *
    Default Salt : MSEDGEWIN10IIEUser
    Default Iterations : 4096
    Credentials
        aes256_hmac      (4096) : 72cc752f2addce7556960ad819259738c4fd86e7130cee6b06aca1137ad1e6cb
        aes128_hmac      (4096) : 7d83280d0766f4ad6510460fb975fb
        des_cbc_md5       (4096) : ecd9340ddf7406b
    OldCredentials
        aes256_hmac      (4096) : b55700a5a2002a8a290a8f3554838fd420cb7877b8f59ed75fd7af6b98ba53c
        aes128_hmac      (4096) : 64be48ded076d1592ae6df8708266f64
        des_cbc_md5       (4096) : a4ce3d75831f988c

* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : MSEDGEWIN10IIEUser
    Credentials
        des_cbc_md5       : ecd9340ddf7406b
    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 *

Primary:Kerberos-Newer-Keys *
Default Salt : MSEDGEWIN10sshd
Default Iterations : 4096
Credentials
    aes256_hmac      (4096) : 9c6818e8b29d2a66b5b66321b95faef7d93908ae666cc254aacaae8d9cdd0c3
    aes128_hmac      (4096) : 8e4a19ecfa0cff16aadf1491aa848d3
    des_cbc_md5       (4096) : 64d51f51efad018a

Packages *
    NTLM-Strong-NTOWF

Primary:Kerberos *
Default Salt : MSEDGEWIN10sshd
Credentials
    des_cbc_md5       : 64d51f51efad018a
```

Se obtienen los hashes de algunos usuarios de la máquina. Con una [herramienta online de crackeo de hashes](#), pueden hallarse las contraseñas de los siguientes usuarios:

IEUser -> qwerty

Administrator -> Passw0rd!

| Hash                             | Type | Result |
|----------------------------------|------|--------|
| 2d20d252a479f485cdf5e171d93985bf | NTLM | qwerty |

## 2.5. Archivos LNK y JumpList

Los **LNK** son archivos que se crean cada vez que se abre un fichero en local o en remoto, y permanecen aunque el archivo a partir del cual se crearon se haya eliminado de la máquina o almacenado en otro dispositivo.

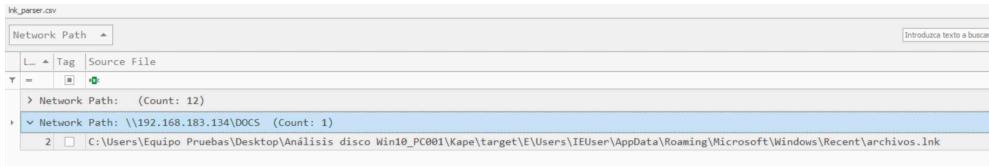
En Windows 10, como es el caso de [PEGASUS01](#) pueden localizarse estos LNK en C:\\Users\\<username>\\AppData\\Roaming\\Microsoft\\Windows\\Recent

Una vez localizados, usamos la herramienta [LECcmd.exe](#) desde la consola, ubicándose en la carpeta donde está almacenada, se lanza el comando

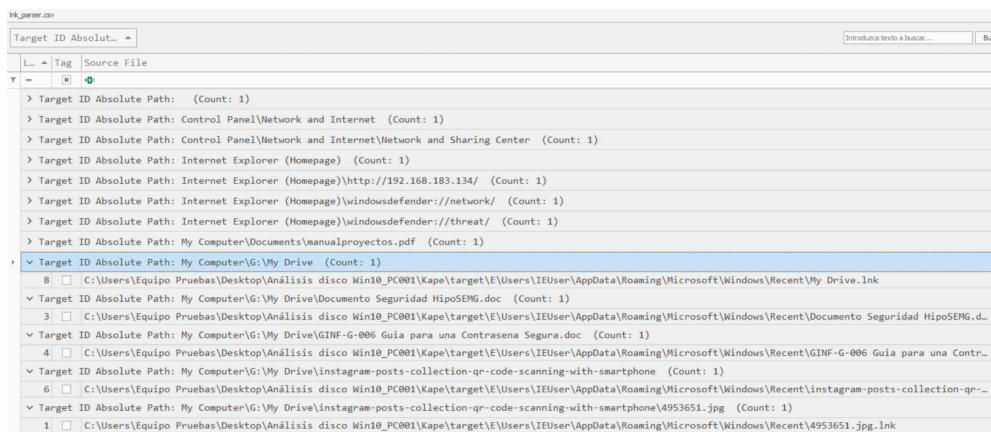
```
LECcmd.exe -d <"path donde está la carpeta Recent"> --all --csv
<"path para guardar output"> --csvf <nombre del fichero>
```

Gracias al paseo de los datos de estos archivos .LNK vamos a poder ver con [Timeline Explorer](#) información de interés para el análisis.

Por un lado, se puede saber que el usuario **IEUser se ha conectado a otra máquina remota** con IP 192.168.183.134, y ha accedido a un directorio llamado DOCS de la misma.



También se puede ver que IEUser ha accedido a documentación de otro volumen de nombre G:/MyDrive y que **cuenta con acceso a un servicio de almacenamiento en la nube**, en concreto de Google Drive y que ha abierto o descargado ficheros de estas ubicaciones en la máquina analizada.



Los archivos **JumpList** contienen enlaces a los archivos recientes del sistema (los últimos que se han abierto o modificado). Hay de dos tipos: Automatics y Custom. Se almacenan en sus carpetas correspondientes en el mismo directorio donde encontramos los archivos LNK.

Para interpretarlos puede utilizarse la herramienta [JLECmd.exe](#), con el mismo procedimiento que [LECmd.exe](#), desde la terminal y con el comando

```
LECmd.exe -d <"path donde está la carpeta Recent"> --all --csv <"path para guardar output"> --csvf <nombre del fichero>
```

Una vez parseados los ficheros `Automatics_Destinations` y `Custom_Destinations`, leyendo el primero con [Timeline Explorer](#) confirmamos que el volumen G:/My Drive pertenece a Google Drive y podemos leer los archivos que se han abierto en la máquina a través de este servicio y hasta en cuantas ocasiones.

| App Id                                  | Description | Last Modified   | Interac...          | Path   |                     |
|---|-------------|---|---------------------|--|---------------------|
| Windows Explorer Windows 8.1            | 4 .. 4      | 1601-01-01 00:00:..   | 0                   | G:\  |                     |
| <hr/>                                   |             |   |                     |  |                     |
| Windows Explorer Windows 8.1            | 4 .. 1      | 2022-05-08 18:53:..   | 5                   | G:\My Drive  |                     |
| Quick Access                            | 4 5 2       | 2022-04-29 10:30:..   | 2                   | G:\My Drive\Documento Seguridad Hiposemg.doc                                       |                     |
| LibreOffice 5.1.0.3 Writer              | 4 2 1       | 2022-04-29 09:20:..   | 1                   | G:\My Drive\Documento Seguridad Hiposemg.doc                                       |                     |
| Quick Access                            | 4 5 1       | 2022-04-29 10:30:..   | 2                   | G:\My Drive\GINF-G-006 Guia para una Contraseña Segura.doc                         |                     |
| LibreOffice 5.1.0.3 Writer              | 4 2 0       | 2022-04-29 09:21:..   | 1                   | G:\My Drive\GINF-G-006 Guia para una Contraseña Segura.doc                         |                     |
| Windows Explorer Windows 8.1            | 4 .. 3      | 2022-04-29 09:21:..   | 1                   | G:\My Drive\Instagram-posts-collection-qrcode-scanning-with-smartphone             |                     |
| Quick Access                            | 4 5 4       | 2022-04-29 09:21:..   | 1                   | G:\My Drive\Instagram-posts-collection-qrcode-scanning-with-smartphone\4953651.jpg |                     |
| Photos Microsoft 16.526.11220...        | 4 1 0       | 2022-04-29 09:21:..   | 1                   | G:\My Drive\Instagram-posts-collection-qrcode-scanning-with-smartphone\4953651.jpg |                     |
| <hr/>                                   |             |   |                     |  |                     |
| Line                                    | Tag         | Source File   | Source Created      | Source Modified  | Source Accessed     |
| =                                       | [#] [F]     |   | =                   | =  | =                   |
| > Volume Label: (Count: 7)              |             |   |                     |  |                     |
| ▼ Volume Label: Google Drive (Count: 9) |             |   |                     |  |                     |
| 14                                      | □           | C:\Users\Equipo Pruebas\Desktop\Análisis disco Win10_PCO01\Kape\target\E\Users... | 2019-03-19 13:00:17 | 2022-05-08 18:53:37  | 2022-05-17 06:19:00 |
| 16                                      | □           | C:\Users\Equipo Pruebas\Desktop\Análisis disco Win10_PCO01\Kape\target\E\Users... | 2019-03-19 13:00:17 | 2022-05-08 18:53:37  | 2022-05-17 06:19:00 |
| 17                                      | □           | C:\Users\Equipo Pruebas\Desktop\Análisis disco Win10_PCO01\Kape\target\E\Users... | 2019-03-19 13:00:17 | 2022-05-08 18:53:37  | 2022-05-17 06:19:00 |
| 4                                       | □           | C:\Users\Equipo Pruebas\Desktop\Análisis disco Win10_PCO01\Kape\target\E\Users... | 2019-03-19 13:00:19 | 2022-05-08 18:53:38  | 2022-05-17 06:18:59 |
| 5                                       | □           | C:\Users\Equipo Pruebas\Desktop\Análisis disco Win10_PCO01\Kape\target\E\Users... | 2019-03-19 13:00:19 | 2022-05-08 18:53:38  | 2022-05-17 06:18:59 |
| 7                                       | □           | C:\Users\Equipo Pruebas\Desktop\Análisis disco Win10_PCO01\Kape\target\E\Users... | 2019-03-19 13:00:19 | 2022-05-08 18:53:38  | 2022-05-17 06:18:59 |
| 11                                      | □           | C:\Users\Equipo Pruebas\Desktop\Análisis disco Win10_PCO01\Kape\target\E\Users... | 2022-04-29 09:20:19 | 2022-04-29 09:21:04  | 2022-05-17 06:19:00 |
| 12                                      | □           | C:\Users\Equipo Pruebas\Desktop\Análisis disco Win10_PCO01\Kape\target\E\Users... | 2022-04-29 09:20:19 | 2022-04-29 09:21:04  | 2022-05-17 06:19:00 |
| 10                                      | □           | C:\Users\Equipo Pruebas\Desktop\Análisis disco Win10_PCO01\Kape\target\E\Users... | 2022-04-29 09:21:16 | 2022-04-29 09:21:20  | 2022-05-17 06:19:00 |
| > Volume Label: Windows 10 (Count: 8)   |             |   |                     |  |                     |

Por tanto, el siguiente paso podría ser investigar estos ficheros, ya que son indicativo de que pudieran pertenecer a la compañía y estar siendo extraídos de la máquina por parte del usuario IEUser.

## 2.6. Shellbags

Son entradas de registro almacenadas por Windows Explorer que permiten conocer los directorios a los que se ha accedido recientemente, tanto desde local como desde remoto o dispositivos extraibles. Se encuentran dentro de las claves de registro de `UsrClass.DAT` y `NTUSER.DAT`.

Para acceder a ellas se puede utilizar la herramienta [SBECmd.exe](#), ubicándose en el terminal en el directorio donde se encuentra la herramienta y lanzando el comando:

```
SBECmd.exe -d <"path donde está el registro USRCLASS.DAT"> --csv
<"path para guardar output"> --csvf <nombre del fichero>
```

Comprobamos el fichero parseado de `UsrClass.DAT` con **Timeline Explorer**. Se puede ver los **directorios a los que se ha accedido recientemente** en o desde el equipo.

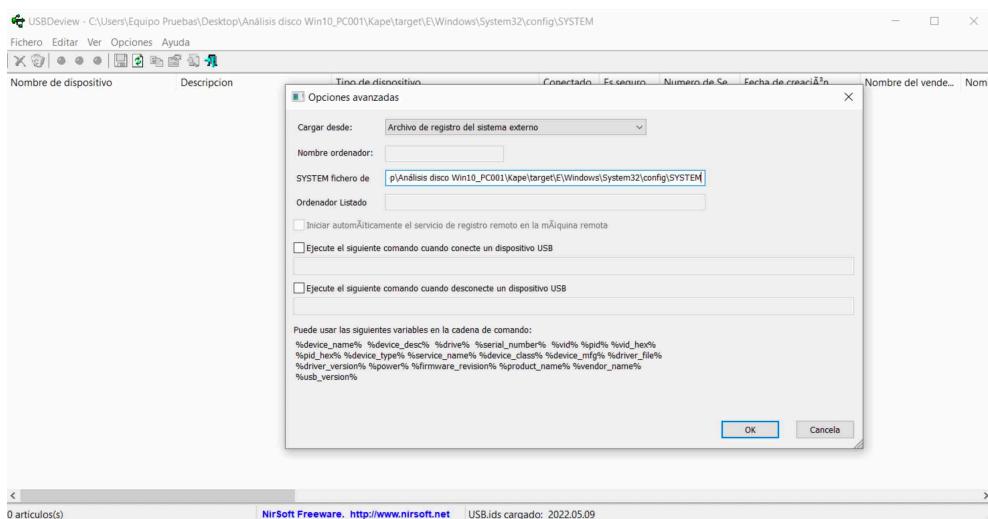
| Absolute Path   | Shell Type                    |
|---|-------------------------------|
| Desktop\Home Folder   | Root folder: GUID             |
| Desktop\My Computer   | Root folder: GUID             |
| Desktop\Control Panel   | Root folder: GUID             |
| Desktop\Computers and Devices   | Root folder: GUID             |
| Desktop\Shared Documents Folder (Users Files)   | Root folder: GUID             |
| Desktop\My Computer\G:  | Drive letter                  |
| Desktop\My Computer\Documents   | Root folder: GUID             |
| Desktop\My Computer\C:  | Drive letter                  |
| Desktop\My Computer\G:\My Drive   | Directory                     |
| Desktop\My Computer\G:\My Drive\instagram-posts-collection-qr-code-scanning-with-smartphone     | Directory                     |
| Desktop\My Computer\C:\Users  | Directory                     |
| Desktop\My Computer\C:\Users\IEUser   | Directory                     |
| Desktop\My Computer\C:\Users\IEUser\AppData   | Directory                     |
| Desktop\My Computer\C:\Users\IEUser\AppData\Local   | Directory                     |
| Desktop\My Computer\C:\Users\IEUser\AppData\Local\Temp  | Directory                     |
| Desktop\My Computer\C:\Users\IEUser\AppData\Local\TeamViewer                                    | Directory                     |
| Desktop\My Computer\C:\Users\IEUser\AppData\Local\Temp\APTSimulator                             | Directory                     |
| Desktop\Control Panel\Network and Internet  | Control Panel Category        |
| Desktop\Control Panel\Network and Internet\Network and Sharing Center                           | GUID: Control panel           |
| Desktop\Control Panel\Network and Internet\Network and Sharing Center\Advanced sharing settings | Variable: Users property view |
| Desktop\Computers and Devices\192.168.183.134   | Variable: Users property view |
| Desktop\Computers and Devices\192.168.183.134\192.168.183.134\Docs                              | Network location              |
| Desktop\Computers and Devices\192.168.183.134\192.168.183.134\Docs\archivos                     | Directory                     |
| Desktop\Shared Documents Folder (Users Files)\AppData   | Users Files Folder            |
| Desktop\Shared Documents Folder (Users Files)\AppData\Local                                     | Directory                     |
| Desktop\Shared Documents Folder (Users Files)\AppData\Local\Temp                                | Directory                     |
| Desktop\Shared Documents Folder (Users Files)\AppData\Local\Temp\APTSimulator                   | Directory                     |
| Desktop\Shared Documents Folder (Users Files)\AppData\Local\Temp\dist                           | Directory                     |
| Desktop\Shared Documents Folder (Users Files)\AppData\Local\Temp\dist\APTSimulator              | Directory                     |

Siguiendo el mismo procedimiento con el fichero pareado de `NTUSER.DAT`, vemos los accesos a directorios remotos, a la IP 192.169.183.134 descubierta anteriormente, en concreto a una carpeta llamada “archivos” un indicativo más de fuga de información.

| Line  | Tag | Absolute Path   | Shell Type                    | Value         |
|---|-----|---|-------------------------------|---------------|
| =   | █   | Desktop\Computers and Devices   | Root folder: GUID             | Computers an  |
| <b>▼ Last Interacted: 29/04/2022 (Count: 4)</b> |     |   |                               |               |
| 1   | □   | Desktop\Computers and Devices   | Root folder: GUID             | Computers an  |
| 2   | □   | Desktop\Computers and Devices\192.168.183.134                               | Variable: Users property view | 192.168.183.  |
| 3   | □   | Desktop\Computers and Devices\192.168.183.134\192.168.183.134\Docs          | Network location              | \\\192.168.18 |
| 4   | □   | Desktop\Computers and Devices\192.168.183.134\192.168.183.134\Docs\archivos | Directory                     | archivos      |

## 2.6. USB y Prefetch

Se pueden comprobar los dispositivos **USB** que han estado conectados a la máquina **PEGASUS01** con la herramienta [USBDevview](#). En AdvancedOptions seleccionamos “Cargar desde archivos de registro del sistema externo” y el archivo de registro SYSTEM de la imagen de **PEGASUS01**. En esta ocasión comprobamos que no se ha conectado ningún USB a esta máquina:



El directorio **Prefetch** de Windows nos muestra los últimos 1024 ejecutables (en el caso de Windows10) que se han ejecutado en el sistema. Repasando los prefetch de **PEGASUS01** comprobamos que el malware **nbtscan.exe** que habíamos localizado anteriormente analizando la MFT se ha ejecutado en el sistema con fecha 09/05/2022.

| Nombre                                   | Fecha de modificación | Tipo       | Tamaño |
|--|-----------------------|------------|--------|
| MICROSOFTEDGE.EXE-0F2B3493(pf)           | 29/04/2022 12:00      | Archivo PF | 39 KB  |
| MICROSOFTEDGECP.EXE-1FF23A10(pf)         | 29/04/2022 12:47      | Archivo PF | 53 KB  |
| MICROSOFTEDGES.EXE-DC6B79BA(pf)          | 29/04/2022 12:00      | Archivo PF | 10 KB  |
| MOBSYNC.EXE-D8BC6ED2(pf)                 | 29/04/2022 12:47      | Archivo PF | 8 KB   |
| MPCMDRUN.EXE-0F43B2C5(pf)                | 08/05/2022 21:10      | Archivo PF | 9 KB   |
| MPCMDRUN.EXE-FBB0D987(pf)                | 29/04/2022 18:53      | Archivo PF | 7 KB   |
| MPSIGSTUB.EXE-7C60A359(pf)               | 08/05/2022 20:54      | Archivo PF | 44 KB  |
| MPSIGSTUB.EXE-D67988B1(pf)               | 29/04/2022 18:41      | Archivo PF | 5 KB   |
| MSCORSVW.EXE-98F0699A(pf)                | 29/04/2022 18:33      | Archivo PF | 24 KB  |
| MSIEXEC.EXE-B5FAFA339(pf)                | 29/04/2022 10:31      | Archivo PF | 31 KB  |
| MSIEXEC.EXE-F3744DFD(pf)                 | 29/04/2022 19:09      | Archivo PF | 11 KB  |
| MUSNOTIFYICON.EXE-A201B346(pf)           | 08/05/2022 20:58      | Archivo PF | 7 KB   |
| NBTSCAN.EXE-9C28C0E8(pf)                 | 08/05/2022 21:07      | Archivo PF | 3 KB   |
| NET.EXE-1FD3A2F6(pf)                     | 08/05/2022 21:07      | Archivo PF | 3 KB   |
| NET1.EXE-B8A247B(pf)                     | 08/05/2022 21:07      | Archivo PF | 3 KB   |
| NGEN.EXE-8F1D81334(pf)                   | 29/04/2022 10:25      | Archivo PF | 5 KB   |
| NGEN.EXE-E9662EB6(pf)                    | 29/04/2022 10:25      | Archivo PF | 6 KB   |
| NGENTASK.EXE-90AAC3ED(pf)                | 29/04/2022 10:25      | Archivo PF | 15 KB  |
| NGENTASK.EXE-F262E2AB(pf)                | 29/04/2022 10:25      | Archivo PF | 13 KB  |
| NOTEPAD.EXE-EB1B961A(pf)                 | 08/05/2022 21:10      | Archivo PF | 10 KB  |
| NSLOOKUP.EXE-0E49F32A(pf)                | 08/05/2022 21:06      | Archivo PF | 4 KB   |
| ONEDRIVE.EXE-33D53679(pf)                | 08/05/2022 20:54      | Archivo PF | 100 KB |
| ONEDRIVESETUP.EXE-07609C61(pf)           | 08/05/2022 20:53      | Archivo PF | 13 KB  |
| OPENWITH.EXE-2DD6FAA1(pf)                | 08/05/2022 21:10      | Archivo PF | 27 KB  |
| P.EXE-7A85E64B(pf)                       | 08/05/2022 21:07      | Archivo PF | 6 KB   |
| PING.EXE-B29F6629(pf)                    | 08/05/2022 21:06      | Archivo PF | 3 KB   |
| POWERSHELLEXE-59FC8F3D(pf)               | 08/05/2022 21:09      | Archivo PF | 51 KB  |
| PSEXEVSC.EXE-51BA46F2(pf)                | 08/05/2022 21:07      | Archivo PF | 5 KB   |
| READERDC64_ES_XA_CRD_SEC_INST-F62...(pf) | 29/04/2022 19:07      | Archivo PF | 13 KB  |
| REG.EXE-26976709(pf)                     | 08/05/2022 21:09      | Archivo PF | 4 KB   |
| REGEDIT.EXE-4748FE01(pf)                 | 29/04/2022 12:06      | Archivo PF | 9 KB   |
| REGSVR32.EXE-55A4EE79(pf)                | 29/04/2022 10:33      | Archivo PF | 9 KB   |
| RUBY.EXE-4684BBC3(pf)                    | 08/05/2022 21:01      | Archivo PF | 37 KB  |

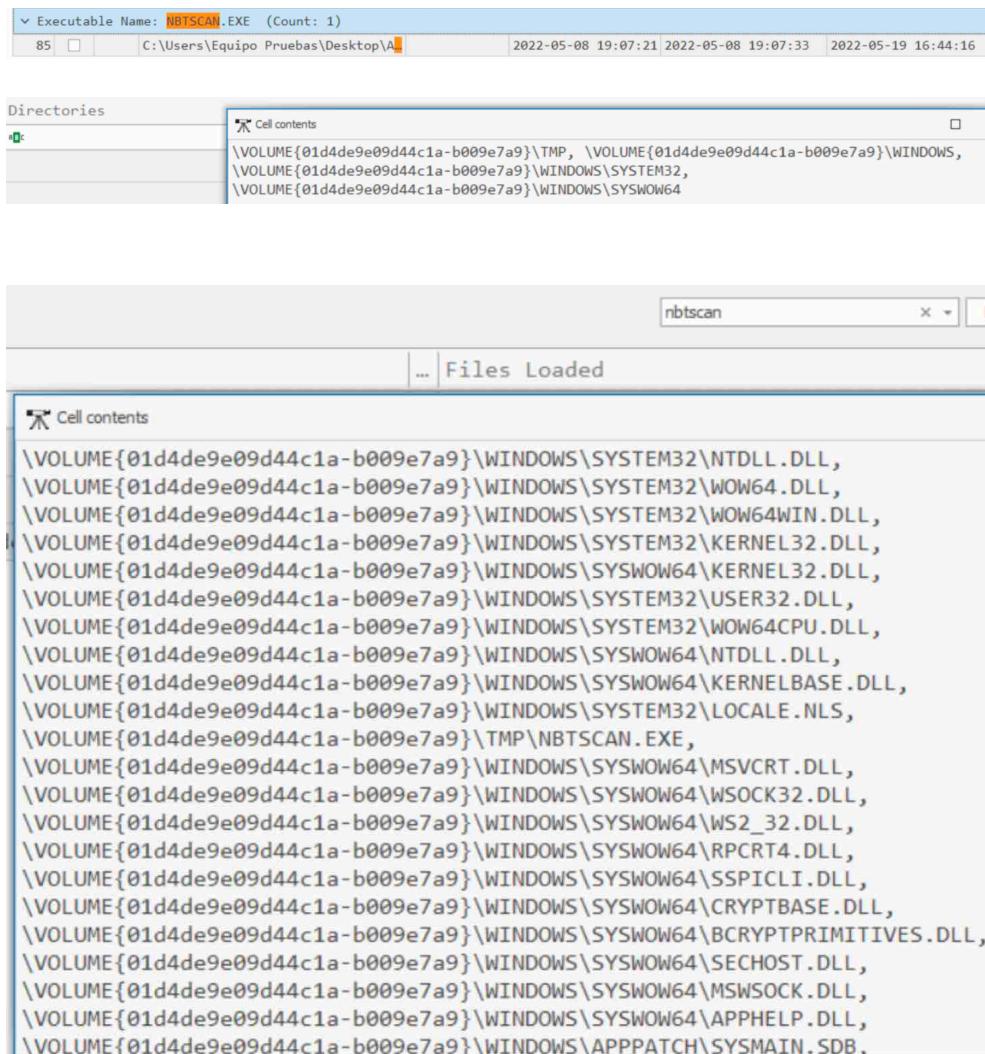
Gracias a la herramienta [PECmd.exe](#) podemos analizar estos ficheros .pf (prefetch). Para lanzarla, es igual que el resto de herramientas de E. Zimmerman que se han utilizado con anterioridad:

```
PECmd.exe -d <"path donde está el registro USRCLASS.DAT"> --csv  
<"path para guardar output"> --csvf <nombre del fichero>
```

Como las veces anteriores, interpretamos el output con [Timeline Explorer](#) y nos fijamos en el ejecutable `nbtscan.exe`

| Line | Tag        | Note          | Source                              | Filename            | Source              | Created | Source | Modified | Run C... | Previous            | Run#                | Previous            | Run1 | Last Run |
|------|------------|---------------|-------------------------------------|---------------------|---------------------|---------|--------|----------|----------|---------------------|---------------------|---------------------|------|----------|
| -    | -          | -             | -                                   | -                   | -                   | -       | -      | -        | -        | -                   | -                   | -                   | -    | -        |
| >    | Executable | Name:         | MICROSOFTEDGEH.EXE                  | (Count: 1)          |                     |         |        |          |          |                     |                     |                     |      |          |
| >    | Executable | Name:         | MOBSYNC.EXE                         | (Count: 1)          |                     |         |        |          |          |                     |                     |                     |      |          |
| >    | Executable | Name:         | MPCMDRUN.EXE                        | (Count: 2)          |                     |         |        |          |          |                     |                     |                     |      |          |
| >    | Executable | Name:         | MPSIGSTUB.EXE                       | (Count: 2)          |                     |         |        |          |          |                     |                     |                     |      |          |
| >    | Executable | Name:         | MSCORSWL.EXE                        | (Count: 1)          |                     |         |        |          |          |                     |                     |                     |      |          |
| >    | Executable | Name:         | MSIEXEC.EXE                         | (Count: 2)          |                     |         |        |          |          |                     |                     |                     |      |          |
| >    | Executable | Name:         | MUSNOTIFICON.EXE                    | (Count: 1)          |                     |         |        |          |          |                     |                     |                     |      |          |
| >    | Executable | Name:         | NBTSCAN.EXE                         | (Count: 1)          |                     |         |        |          |          |                     |                     |                     |      |          |
|      |            | VolumeSerial: | (Count: 1)                          |                     |                     |         |        |          |          |                     |                     |                     |      |          |
| -    | -          | -             | C:\Users\Equipo_Pruuebas\Desktop\A_ | 2022-05-08 19:07:21 | 2022-05-08 19:07:33 |         |        |          | 3        | 2022-05-08 19:07:21 | 2022-05-08 19:07:15 | 2022-05-08 19:07:27 |      |          |

Entre otras cosas podemos ver la fecha de creación y ejecución del ejecutable en la máquina, los directorios a los que su proceso llama y los ficheros que ha cargado al ejecutarse. Se comprueba que el malware está llamando, entre otros al directorio System32, o que la mayoría de archivos que carga son librerías .dll lo que es indicio de que trata de modificar el sistema.



The screenshot shows two windows from the Volatility Framework. The top window is a table with the following columns: Executable Name, Count, File Path, Creation Time, Last Modified, and Last Accessed. It lists one entry: NBTSCAN.EXE (Count: 1) at C:\Users\Equipo Pruebas\Desktop\A with creation time 2022-05-08 19:07:21, last modified 2022-05-08 19:07:33, and last accessed 2022-05-19 16:44:16. The bottom window is a list of file paths under the heading 'Cell contents' for the executable. The paths listed are:

```

\\VOLUME{01d4de9e09d44c1a-b009e7a9}\TMP, \\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS,
\\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SYSTEM32,
\\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SYSWOW64

```

Below this, another list of file paths is shown under the heading 'Cell contents' for the executable, with many entries starting with '\\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SYSTEM32\' followed by various DLL files like NTDLL.DLL, KERNEL32.DLL, USER32.DLL, etc.

## 2.7. Eventos

Los eventos del sistema se encuentran en /WindowsSystem32/Winevt/Log  
En este caso vamos a centrarnos en analizar los eventos de Security, ya que nos interesa conocer para esta práctica cuales han sido los **logon/logoff del sistema**, las veces que los usuarios se han logueado y deslogueado.

También revisaremos algunos ficheros Operational, ya que también interesa confirmar a través de los eventos registrados, las conexiones remotas que se han producido en la máquina.

Para ello utilizamos una nueva herramienta de E.Zimmerman, en este caso [EvtxCmd.exe](#). Se lanza desde el terminal, ubicándonos previamente en el directorio donde está la herramienta:

```
EvtxECmd.exe -f <"path donde está el evento Security.evtx"> --csv
<"path para guardar output"> --csvf <nombre del fichero> --inc
<identificadores de eventos>
```

En este caso, incluimos después de la flag –inc se han incluido los siguientes los eventos, ya que se ha considerado que son interesantes para obtener información sobre si la máquina ha sido atacada.

| Id. de evento de Windows actual | Importancia crítica potencial | Resumen del evento                                     |
|---------------------------------|-------------------------------|--|
| 625                             | Bajo                          | Tipo de cuenta de usuario cambiado                     |
| 4616                            | Bajo                          | Se cambió la hora del sistema.                         |
| 4624                            | Bajo                          | Se inició sesión correctamente en una cuenta.          |
| 4625                            | Bajo                          | No se pudo iniciar sesión en una cuenta.               |
| 4634                            | Bajo                          | Se cerró sesión en una cuenta.                         |
| 4647                            | Bajo                          | Cierre de sesión iniciada por el usuario.              |
| 4648                            | Bajo                          | Se intentó iniciar sesión con credenciales explícitas. |
| 4673                            | Bajo                          | Se llamó a un servicio con privilegios.                |
| 4674                            | Bajo                          | Se intentó una operación en un objeto con privilegios. |
| 4688                            | Bajo                          | Se ha creado un nuevo proceso.                         |

|      |       |  |
|------|-------|--|
| 4689 | Bajo  | Un proceso ha terminado.   |
| 4692 | Media | Se intentó hacer una copia de seguridad de la clave maestra de protección de datos   |
| 4693 | Media | Se intentó recuperar la clave maestra de protección de datos   |
| 4697 | Bajo  | Intento de instalar un servicio  |
| 4698 | Bajo  | Se creó una tarea programada.  |
| 4699 | Bajo  | Se eliminó una tarea programada.   |
| 4700 | Bajo  | Se habilitó una tarea programada.  |
| 4701 | Bajo  | Se deshabilitó una tarea programada.   |
| 4702 | Bajo  | Se actualizó una tarea programada.   |
| 4710 | Bajo  | Se deshabilitaron los Servicios IPsec.   |
| 4720 | Bajo  | Se creó una cuenta de usuario.   |
| 4722 | Bajo  | Se habilitó una cuenta de usuario.   |
| 4723 | Bajo  | Se ha realizado un intento de cambiar la contraseña de una cuenta.   |
| 4724 | Media | Se ha realizado un intento de restablecer la contraseña de una cuenta.   |
| 4738 | Bajo  | Se cambió una cuenta de usuario.   |
| 4740 | Bajo  | Se bloqueó una cuenta de usuario.  |
| 4767 | Bajo  | Se desbloqueó una cuenta de usuario.   |
| 4772 | Bajo  | Error de solicitud de vale de autenticación de Kerberos.   |
| 4781 | Bajo  | Se cambió el nombre de una cuenta  |
| 4793 | Bajo  | Se ha llamado a la API de comprobación de directiva de contraseñas   |
| 4950 | Bajo  | Se cambió una configuración del Firewall de Windows.   |
| 4963 | Media | IPsec descartó un paquete de texto no cifrado entrante que debería estar protegido. Esto suele deberse a que el equipo remoto cambió su directiva IPsec sin informar a este equipo. También podría ser un intento de ataque de suplantación. |
| 5025 | Bajo  | El servicio de Firewall de Windows se ha detenido.   |
| 5049 | Bajo  | Se eliminó una asociación de seguridad de IPsec.   |
| 5050 | Bajo  | Intento de deshabilitar mediante programación el firewall Windows mediante una llamada a InetFwProfile.FirewallEnabled(False)  |
| 5140 | Bajo  | Se tuvo acceso a un objeto de recurso compartido de red  |
| 5376 | Media | Se hizo una copia de seguridad de las credenciales del Administrador de credenciales.  |

|      |       |  |
|------|-------|--|
| 5377 | Media | Se restauraron las credenciales del Administrador de credenciales desde una copia de seguridad.  |
| 5479 | Bajo  | Los servicios IPsec se cerraron correctamente. El cierre de los servicios IPsec puede suponer un mayor riesgo de ataque a la red para el equipo o exponerlo a posibles riesgos de seguridad. |
| 5712 | Bajo  | Se intentó una llamada a procedimiento remoto (RPC).   |
| 6272 | Bajo  | El Servidor de directivas de redes concedió acceso a un usuario.   |

Dado que hemos identificado al usuario IEUser como la cuenta desde que se está produciendo fuga de información y posibles ataques a la máquina mediante la introducción de malware, se expone aquí la información de los logon/logoff del usuario y otra relevante. De todos los eventos lanzados, en la siguiente captura de pantalla se listan aquellos de los que [EvttxECmd.exe](#) ha conseguido extraer información. Se adjunta a este informe el fichero con la información de los eventos.

```

Event log details
Flags: IsDirty
Chunk count: 68
Stored/Calculated CRC: B623391C/B623391C
Earliest timestamp: 2019-03-19 12:59:29.4501356
Latest timestamp: 2022-05-08 19:11:05.0092294
Total event log records found: 5.735

Records included: 1.204 Errors: 0 Events dropped: 4.531

Metrics (including dropped events)
Event ID      Count
4616          10
4624          852
4625           7
4634           12
4647           14
4648           73
4688          177
4720           4
4722           4
4723           1
4724           5
4738          25
4781          20

Processed 1 file in 8,1950 seconds

```

El evento 4624 muestra los logs exitosos de IEUser, el evento 4625 los intentos de login fallidos. En este caso solo hay un intento de login fallido. Observar muchas entradas en este evento en poco margen de tiempo puede ser indicativo de intentos de login por ataque de fuerza bruta.

| Event Id   | User Name   |           |        |              |                 |                 |
|--|---|-----------|--------|--------------|-----------------|-----------------|
| Line   | Tag   | Record... | Eve... | Time Created | Map Description | Executable Info |
| =  | =   | =         | =      | =            | [green]         | [green]         |
| > Event Id: 4616 (Count: 10)                           |   |           |        |              |                 |                 |
| > Event Id: 4624 (Count: 852)                          |   |           |        |              |                 |                 |
| > User Name: -\-\ (Count: 16)                          |   |           |        |              |                 |                 |
| > User Name: \MINWINPC\\$ (Count: 37)                  |   |           |        |              |                 |                 |
| > User Name: MSEDEWIN10\IEUser (Count: 2)              |   |           |        |              |                 |                 |
| 852 [ ] 4288 4288 2022-04-29 16:41:41 Successful logon | C:\Windows\ImmersiveControlPanel\SystemSettings.exe |           |        |              |                 |                 |
| 853 [ ] 4289 4289 2022-04-29 16:41:41 Successful logon | C:\Windows\ImmersiveControlPanel\SystemSettings.exe |           |        |              |                 |                 |
| > User Name: WORKGROUP\MSEDEWIN10\\$ (Count: 524)      |   |           |        |              |                 |                 |
| > User Name: WORKGROUP\PEGASUS01\\$ (Count: 273)       |   |           |        |              |                 |                 |
| > Event Id: 4625 (Count: 7)                            |   |           |        |              |                 |                 |
| > User Name: PEGASUS01\IEUser (Count: 1)               |   |           |        |              |                 |                 |
| 10... [ ] 5299 5299 2022-04-29 10:03:34 Failed logon   | C:\Windows\explorer.exe                             |           |        |              |                 |                 |
| > User Name: WORKGROUP\MSEDEWIN10\\$ (Count: 3)        |   |           |        |              |                 |                 |
| > User Name: WORKGROUP\PEGASUS01\\$ (Count: 3)         |   |           |        |              |                 |                 |

Con el evento 4647 se puede ver las veces que IEUser ha hecho logoff por él mismo, y con el 4648 se puede comprobar cuándo ha intentado hacer login usando credenciales explícitas. Además, podemos comprobar que ha utilizado ese login para conectarse al equipo remoto 192.168.183.134:445, IP ya detectada con anterioridad.

| Event Id   | User Name           |           |        |              |                 |             | Introduzca texto a buscar... |
|--|---------------------|-----------|--------|--------------|-----------------|-------------|------------------------------|
| Line   | Tag                 | Record... | Eve... | Time Created | Map Description | Remote Host |                              |
| =  | =                   | =         | =      | =            | [green]         |             |                              |
| > User Name: Target: MSEDEWIN10\IEUser (Count: 11)                                       |                     |           |        |              |                 |             |                              |
| 190 [ ] 529 529 2019-03-19 13:00:54 User initiated logoff                                |                     |           |        |              |                 |             |                              |
| 256 [ ] 786 786 2019-03-19 13:06:33 User initiated logoff                                |                     |           |        |              |                 |             |                              |
| 315 [ ] 1160 1160 2019-03-19 13:09:15 User initiated logoff                              |                     |           |        |              |                 |             |                              |
| 364 [ ] 1268 1268 2019-03-19 13:10:06 User initiated logoff                              |                     |           |        |              |                 |             |                              |
| 413 [ ] 1378 1378 2019-03-19 13:10:57 User initiated logoff                              |                     |           |        |              |                 |             |                              |
| 462 [ ] 1487 1487 2019-03-19 13:11:50 User initiated logoff                              |                     |           |        |              |                 |             |                              |
| 529 [ ] 1706 1706 2019-03-19 13:18:55 User initiated logoff                              |                     |           |        |              |                 |             |                              |
| 585 [ ] 3336 3336 2019-03-19 13:20:51 User initiated logoff                              |                     |           |        |              |                 |             |                              |
| 638 [ ] 3450 3450 2019-03-19 13:22:20 User initiated logoff                              |                     |           |        |              |                 |             |                              |
| 717 [ ] 3649 3649 2019-03-19 13:29:56 User initiated logoff                              |                     |           |        |              |                 |             |                              |
| 864 [ ] 4317 4317 2022-04-29 16:42:09 User initiated logoff                              |                     |           |        |              |                 |             |                              |
| > User Name: Target: PEGASUS01\IEUser (Count: 2)   |                     |           |        |              |                 |             |                              |
| > Event Id: 4648 (Count: 73)   |                     |           |        |              |                 |             |                              |
| > User Name: \MINWINPC\\$ (Count: 3)   |                     |           |        |              |                 |             |                              |
| > User Name: PEGASUS01\IEUser (Count: 2)   |                     |           |        |              |                 |             |                              |
| 10... [ ] 5302 5302 2022-04-29 10:08:16 A logon was attempted using explicit credentials | 192.168.183.134:445 |           |        |              |                 |             |                              |
| 10... [ ] 5319 5319 2022-04-29 10:13:22 A logon was attempted using explicit credentials | 192.168.183.134:445 |           |        |              |                 |             |                              |

Finalmente, gracias al evento 4723 podemos comprobar las veces que IEUser ha intentado cambiar la contraseña de una cuenta de usuario y a través del 4724, se ven los intentos de reseteo de contraseñas en la máquina, que en este caso no son relevantes ya que son de fecha anterior (19-03-2019) al supuesto incidente de fuga de información e introducción de malware en la máquina (29-04-2022)

|  |  |
|--|--|
| ▼ Event Id: 4722 (Count: 4)  |  |
| ▼ User Name: PEGASUS01\IEUser (S-1-5-21-321011808-3761883066-353627080-1000) (Count: 1)                        |  |
| 11... <input type="checkbox"/> 5708 5708 2022-05-08 19:06:49 A user account was enabled                        |  |
| ► User Name: WORKGROUP\MSEDEWIN10\$ (S-1-5-18) (Count: 3)  |  |
| ▼ Event Id: 4723 (Count: 1)  |  |
| ▼ User Name: MSEDEWIN10\IEUser (S-1-5-21-321011808-3761883066-353627080-1000) (Count: 1)                       |  |
| 856 <input type="checkbox"/> 4293 4293 2022-04-29 16:41:59 An attempt was made to change an account's password |  |
| ▼ Event Id: 4724 (Count: 5)  |  |
| ▼ User Name: WORKGROUP\MSEDEWIN10\$ (S-1-5-18) (Count: 5)  |  |
| 92 <input type="checkbox"/> 203 203 2019-03-19 20:57:23 An attempt was made to reset an account's password     |  |
| 94 <input type="checkbox"/> 209 209 2019-03-19 20:57:23 An attempt was made to reset an account's password     |  |
| 106 <input type="checkbox"/> 230 230 2019-03-19 20:59:25 An attempt was made to reset an account's password    |  |
| 108 <input type="checkbox"/> 232 232 2019-03-19 20:59:25 An attempt was made to reset an account's password    |  |
| 695 <input type="checkbox"/> 3590 3590 2019-03-19 13:23:55 An attempt was made to reset an account's password  |  |

Para comprobar si hay eventos registrados de conexión remota, se la lanza también [EvtxECmd.exe](#) sobre el registro OpenSSH\_%40operational.evtx y sobre Microsoft-Windows-TerminalServices-LocalSessionManager%40operational.evtx los eventos 1149 (User authentication succeeded) y 21 (Remote Desktop Service).

Mientras que con el primero no se obtiene información, con el segundo se observan 3 conexiones remotas con fecha 29/04/2022 por parte de IEUser.

Otra herramienta que permite analizar los **eventos**, esta vez en Tsurugi Linux, es [Chainsaw](#). Este software interpreta comportamientos registrados en los eventos y muestra por sí mismo los que pueden parecer sospechosos. El funcionamiento es simple, es suficiente con lanzar el comando:

```
chainsaw hunt <path donde están guardados los eventos> -csv
```

En este caso comprobamos que **Chainsaw** identifica varios eventos donde IEUser ha introducido ficheros en la máquina identificados como troyanos, ha creado una

backdoor.ps1 (ids 1116, detecciones de Windows Defender) o ha intentado acceder a una cuenta de usuario mediante fuerza bruta (id 4625). Se adjunta un reporte completo a esta informe de los eventos interpretados por esta herramienta.

```
tsurugi@lab-5:~$ chainsaw hunt /home/tsurugi/Desktop/evidence_test_001/logs
```

The screenshot shows the Chainsaw interface with several tabs open:

- Event Log**: Shows a table of events with columns: system\_time, id, computer, threat\_name, threat\_file, user. The table lists various detections such as "Trojan:BAT/Vigorf.A", "Trojan:Win32/Powersploit!ml", and "Backdoor:PowerShell/Powercat.A".
- File Analysis**: Shows a table of files with columns: name, type, owner. It includes entries like "file: C:\Users\IEUser\AppData\Local\Temp\APTSimulator\test-sets\command-and-control\wmi-backdoor-c2.bat" and "file: C:\Users\IEUser\AppData\Local\Temp\APTSimulator\test-sets\credential-access\minikatz-1.bat".
- User Activity**: Shows a table of user logins with columns: system\_time, id, computer, target\_username, user\_sid. It includes entries like "S-1-5-21-321011808-3761883066-353627080-1002" and "S-1-5-21-321011808-3761883066-353627080-504".
- Group Membership**: Shows a table of group memberships with columns: system\_time, id, computer, target\_group. It includes entries like "Administrators" and "Power Users".
- Account Brute Forcing**: Shows a table of failed login attempts with columns: id, username, failed\_login\_count. It includes an entry for "4625" with "IEUser" and a count of 6.

At the bottom, it says "[+] 29 Detections found".

### **3. Análisis de volumen**

### 3.1. Bulk

Esta herramienta escanea la imagen de disco y saca todas las strings que encuentra clasificándolas en categorías como dominios, emails, números de teléfono, etc. incluso imágenes o zips.

Para lanzar Bulk se ha utilizado Tsurugi y este comando

```
bulk_extractor -o <path_output> <path_imagen>
```

```
tsurugi@lab-5: bulk_extractor -o /home/tsurugi/Desktop/evidence_test_001/ /home/tsurugi/Desktop/evidence_test_001/evidence_copy_001/Win10_PCO01.E01
mkdvr: "/home/tsurugi/Desktop/evidence_test_001/"
Opening /home/tsurugi/Desktop/evidence_test_001/evidence_copy_001/Win10_PCO01.E01
bulk_extractor version: 2.0.6-dev
Input file: "/home/tsurugi/Desktop/evidence_test_001/evidence_copy_001/Win10_PCO01.E01"
Output directory: "/home/tsurugi/Desktop/evidence_test_001/"
Disk Size: 4294967296
Scanners: aes base64 elf evtx exif facebook fndt gzip httplogs json kml msxml net ntfsindex ntfslogfile ntfsfmt ntfsusn pdf rar sqlite utmp vcard windln
Inpe wmprefetch zip accts email gps
Threads: 2
going multi-threaded...( 2 )
bulk_extractor Sat May 21 01:20:26 2022
available_memory: 1633689600
bytes queued: 16777216
depth0_sbufs_queued: 1
elapsed_time: 0:49:18
estimated_time_completion: 2022-05-21 01:20:26
estimated_time_remaining: 0:00:00
fraction_read: 100.000000 %
max_offset: 42932895744
sbufs_created: 166949848
sbufs_queued: 1
sbufs_remaining: 1
tasks_queued: 0
thread-1: IDLE
thread-2: 42932895744: email (16777216 bytes)
thread_count: 2
=====
Average consumer time spent waiting: 0 sec.
Phase 2: Shutting down scanners
All Threads Flinshed!
Elapsed time: 1.016e+04 sec.
Total MB processed: 42949
Overall performance: 4.228 <= MBytes/sec 2.114 ( MBytes/sec/thread )
sbufs created: 166950095
sbufs unaccounted: 0 ( should be 0 )
Total email features found: 8603
```

Se consigue una gran cantidad de información de diferentes categorías de strings. En este caso, vamos a centrarnos en el archivo domains.txt, para comprobar que también Bulk ha detectado la IP remota maliciosa a la que se conecta IEUser para sacar información de la máquina.

También es interesante observar el fichero url\_searches.txt, que muestra las búsquedas que se han hecho en navegadores, entre otras “antiforensic”, “como borrar datos del equipo”, o “limpiar registros del equipo”.

```

sqlite_carved.txt ✘ url_searches.txt ✘
1 # BANNER FILE NOT PROVIDED (-b option)
2 # BULK EXTRACTOR-Version: 2.0.0-dev
3 # Feature-Recorder: url
4 # Filename: /home/tsurugi/Desktop/evidence test 001/evidence copy 001/Win10 PC001.E
5 # Histogram-File-Version: 1.1
6 n=40 search?q=antiforensid (utf16=9)
7 n=39 search?q=como+borrar+datos+del+equipo (utf16=9)
8 n=26 search?q=chrome (utf16=15)
9 n=25 search?q=limpiar+registros+del+equipo (utf16=4)
10 n=24 search?q=libre+office (utf16=2)
11 n=19 search?q=teamviewer (utf16=2)
12 n=17 search?q=adobe+reader (utf16=2)
13 n=6 search?q=banyak+islands
14 n=4 search?q=snowdonia+national+park+wales
15 n=3 search/repositories?q=mainrepositorytogetavailablechansec: (utf16=3)
16 n=2 search.aspx?q=%shttp://www.yodao.com/search?ue=utf8&q=%shttp://yc.book.sohu.com
17 n=2 search?client=chrome-omni&gs ri=chrome-ext-ansg&xssi=t&q=l
18 n=2 search?client=chrome-omni&gs ri=chrome-ext-ansg&xssi=t&q=li
19 n=2 search?q=Hitachi+Seaside+Park
20 n=2 search?q=ponyfill. (utf16=1)
21 n=2 search?q=snowdonia+landscane

```

Sería interesante revisar todos los archivos de strings extraídos para realizar un análisis aun más exhaustivo del contenido del disco.

### 3.2. Loki

La herramienta [Loki](#) nos permite hacer un escaneo de un volumen para detectar a través del match con reglas Yara si contiene malware.

Ubicándose en la terminal en el directorio del programa, se lanza el siguiente comando para actualizar las reglas en primer lugar

`loki-upgrader.exe`

Después se realiza el escaneo del volumen con

`loki -p <volumen> --noprocscan --intense`

El output muestra que ha identificado los malware ya conocidos: `xCmd.exe` y `ntbscan.exe`. Además también alerta un match sobre `p.exe`, por lo que puede ser que haya injectado algún proceso malicioso sobre este ejecutable, ya que como se ha

mencionado al principio del informe, aunque no es en sí un archivo malicioso, puede usarse con esos fines.

```

20220520T05:30:17Z WINFORENSIC10 LOKI: Alert: MODULE: FileScan MESSAGE: FILE: E:\TMP\nbtscan.exe SCORE: 160 TYPE: EXE SIZE: 36864 FIRST_BYTES: 4d5a900003000000400000ffff0000b8000000 / <filter object at 0x053CCC58> MD5: f01a9a2d1e31332ed36c1a4d2839f412 SHA1: 90da10004c8f6fafdaa2cf18922670a745564f45 SHA256: c9d5dc956841e000bfd8762e2f0b48b66c79b79500e894b4efa7fb9ba17e4e9e CREATED: Sun May 8 21:07:15 2022 MODIFIED: Sun Feb 4 20:06:06 2018 ACCESSED: Fri May 20 07:30:17 2022 REASON_1: File Name IOC matched PATTERN: \\nbtscan\\.exe SUBSCORE: 60 DESC: Known Bad / Dual use classicsREASON_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-sharepoint-servers/

```

```

20220520T05:30:17Z WINFORENSIC10 LOKI: Alert: MODULE: FileScan MESSAGE: FILE: E:\TMP\p.exe SCORE: 105 TYPE: EXE SIZE: 381816 FIRST_BYTES: 4d5a900003000000400000ffff0000b8000000 / <filter object at 0x053CA748> MD5: aeee996fd3484f28e5cd85fe26b6bdcd SHA1: cd23b7c9e0edef184930bc8e0ca2264f0608bcb3 SHA256: f8dbabdfa03068130c277ce49c60e35c029ff29d9e3c74c362521f3fb02670d5 CREATED: Sun May 8 21:07:46 2022 MODIFIED: Tue Apr 27 12:04:06 2010 ACCESSED: Fri May 20 07:30:17 2022 REASON_1: File Name IOC matched PATTERN: \\[a-zA-Z]\\.exe$ SUBSCORE: 45 DESC: Typical Malware NameREASON_2: Yara Rule MATCH: APT_Cloaked_PsExec SUBSCORE: 60 DESCRIPTION: Looks like a cloaked PsExec. May be APT group activity. REF: - AUTHOR: Florian Roth MATCHES: Str1: psexesvc.exe Str2: Sysinternals PsExec

```

```

20220520T05:30:17Z WINFORENSIC10 LOKI: Warning: MODULE: FileScan MESSAGE: FILE: E:\TMP\xCmd.exe SCORE: 60 TYPE: EXE SIZE: 843776 FIRST_BYTES: 4d5a900003000000400000ffff0000b8000000 / <filter object at 0x053C8328> MD5: 27aaee7f36b4099e8db3e3d3898474196 SHA1: c26dc6e4ef77cafafa154fa9529c4ce79a8fc78b SHA256: 6c8eea3ba31463a04d041f4c9ff50b50d9b5945d3306fee35fb4b5bfd292692b CREATED: Sun May 8 21:09:17 2022 MODIFIED: Tue Jul 29 17:38:13 2014 ACCESSED: Fri May 20 07:30:17 2022 REASON_1: Yara Rule MATCH: XOR_4byte_Key SUBSCORE: 60 DESCRIPTION: Detects an executable encrypted with a 4 byte XOR (also used for Derusbi Trojan) REF: http://blog.airbuscybersecurity.com/post/2015/11/Newcomers-in-the-Derusbi-family AUTHOR: Florian Roth MATCHES: Str1: 85c9740a3106011e83c60449ebf2

```

Se detectan además dos procesos que tambien matchean con reglas Yara, por lo que se deduce que han sido infectados por alguno de los malware. Estos procesos son:

- procdumpx64.exe, utilizado para generar volcados de memoria ( sospechoso, ya que estamos analizando una posible fuga de información de la empresa a través de esta máquina) y,
- svchost.exe, usado para descargar servicios necesarios del sistema operativo que se cargan al arrancar el sistema (el malware podría estar infectando este proceso para generar persistencia)

```

20220520T05:30:18Z WINFORENSIC10 LOKI: Alert: MODULE: FileScan MESSAGE: FILE: E:\Users\Public\procdump64.exe SCORE: 105 TYPE: EXE SIZE: 341672 FIRST_BYTES: 4d5a9000030000004000000fffff0000b8000000 / <filter object at 0x053C8CB8> MD5: a92669ec8852230a10256ac23bbf4489 SHA1: 4bed038c66e7fdbbf0365669923a73fbc9bb8f4 SHA256: 16f413862efda3aba631d8a7ae2bfff6d84acd9f454a7adaa518c7a8a6f375a5 CREATED: Sun May 8 21:06:42 2022 MODIFIED: Tue Apr 25 04:37:46 2017 ACCESSED: Fri May 20 07:30:18 2022 REASON_1: File Name IOC matched PATTERN: \\(Users|Documents and Settings)\\[\\\\]{1}

20220520T05:30:18Z WINFORENSIC10 LOKI: Alert: MODULE: FileScan MESSAGE: FILE: E:\Users\Public\svchost.exe SCORE: 220 TYPE: EXE SIZE: 8192 FIRST_BYTES: 4d5a9000030000004000000fffff0000b8000000 / <filter object at 0x053C36A0> MD5: 4635935fc972c582632bf45c26bfcb0e SHA1: 7c5329229042535fe56e74f1f246c6da8cea3be8 SHA256: abd4af71b3c2bd3f741bbe3cec52c4fa63ac78d353101d2e7dc4de2725d1ca1 CREATED: Sun May 8 21:06:55 2022 MODIFIED: Thu Feb 1 18:40:34 2018 ACCESSED: Fri May 20 07:30:18 2022 REASON_1: File Name IOC matched PATTERN: \\(Users|Documents and Settings)\\[\\\\]{1}

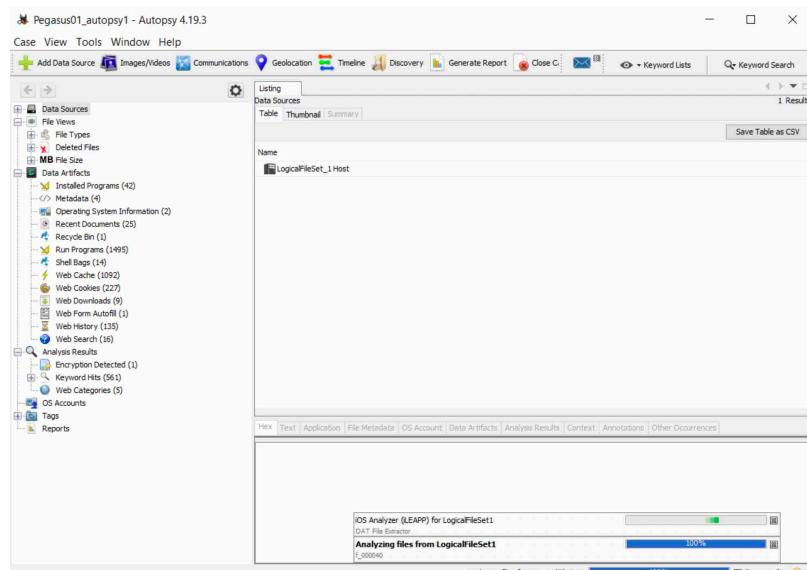
```

### 3.3. Autopsy

Esta herramienta realiza un escaneo entero del equipo o de los archivos seleccionados, según la opción que se prefiera. En este caso se ha realizado un escaneo sobre el archivo lógico obtenido de la imagen de disco obtenida con Kape.

[Autopsy](#) categoriza toda la información a través de una GUI muy útil e intuitiva, y es posible crear un reporte de toda la información extraída y descargarlo (se adjunta el reporte a este informe)

Si bien es una herramienta muy potente, debe servir de complemento a las herramientas anteriormente descritas y utilizadas, ya que estas realizando un análisis más exhaustivo y obtienen información que en algunos casos no es detectada por [Autopsy](#).



## 4. Resumen ejecutivo

Este informe contiene el análisis forense de una imagen de disco de una máquina Windows 10 denominada PEGASUS01, perteneciente a una empresa.

El análisis realizado trata de averiguar principalmente el estado de la máquina ante posibles sospechas de fuga de información de la empresa realizadas por parte de un usuario del sistema.

Después de analizar la máquina con diferentes herramientas de análisis forense desplegadas en sistemas Linux y Windows, se han observado indicios de que el usuario IEUser cuenta con privilegios de administrador y se ha conectado con la IP Remota 192.168.183.134 por el puerto 445.

Este usuario fue creado con fecha 19/03/2019 en la máquina MSEDGEWIN10 y se le asignó el ID 1000. Fue añadido desde el principio al grupo “Administrators”.

Con fecha 29/04/2022 se detectan varios intentos de introducir contraseña fallidos y reseteo de la contraseña por parte de IEUser, por lo que esto da una pista para centrar la investigación en este usuario.

Por la información obtenida, se sabe que se ha producido conexión remota con la IP señalada con fecha 29/04/2022 y que IEUser ha descargado algunos archivos de un directorio llamado DOCS de dicha IP remota a través del volumen G:\My Drive (vinculado a Google Drive), y que es probable que también haya utilizado esta conexión para extraer información de la máquina con dirección a esa IP.

Por la información obtenida, se sabe que esta conexión se ha producido con fecha 29/04/2022 y que IEUser ha descargado algunos archivos de un directorio llamado DOCS del archivo remoto, y que es probable que también haya utilizado esta conexión para extraer información de la máquina con dirección a esa IP.

También con fecha 29/04/2022 se modifica el nombre de la máquina pasando a llamarse PEGASUS01. También se ha observado en el registro de SOFTWARE que se ha instalado y ejecutado con esta fecha el software de acceso remoto TeamViewer, lo que puede ser un indicio más de otro vector de intrusión en la máquina.

Se observa que la última vez que se ha logueado en el sistema IEUser ha sido el 08/05/2022. En esa misma fecha se detecta que se han introducido las muestras de malware halladas en la máquina.

## Segunda parte

### Planteamiento del caso práctico 2

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.

## 1. Metadatos

Para la realización de este caso práctico se ha utilizado la herramienta Exiftool en una distribución Kali Linux 2022.1.

Exiftool permite mediante linea de comando sacar los metadatos de imágenes de diferentes formatos e incluso modificar los mismos.

En este ejercicio se van a comprobar cuáles son los cambios que se producen en los metadatos mostrados en función del canal de envío que se utilice. Es conocido que algunas aplicaciones eliminan metadatos de la imagen original por cuestiones de privacidad.

En este caso se han utilizado las siguientes aplicaciones para este caso práctico:

- Airdrop
- Correo electrónico
- Discord
- Slack
- Telegram
- Whatsapp

El uso es sencillo. Abrimos un terminal, nos ubicamos en el directorio que contiene las imágenes y lanzamos el comando

`exiftool -Sort <nombre del archivo>`

A continuación se muestran los resultados. En primer lugar se muestra captura de pantalla de la imagen original y seguidamente la imagen pasada por cada una de las aplicaciones señaladas.

## Imagen original

```
[kali㉿kali] -[~/Desktop]
└─$ exiftool -Sort metadatos_original.jpg
Acceleration Vector          : -0.1022900119 -0.3167135716 -0.9611587519
Aperture                     : 1.8
Aperture Value               : 1.8
Average Frame Rate           : 0
Bit Depth Chroma             : 8
Bit Depth Luma                : 8
Blue Matrix Column            : 0.1571 0.06657 0.78407
Blue Tone Reproduction Curve : (Binary data 32 bytes, use -b option to extract)
Brightness Value              : 3.138795192
CMM Flags                     : Not Embedded, Independent
Camera Model Name             : iPhone SE (2nd generation)
Chroma Format                 : 4:2:0
Chromatic Adaptation          : 1.04788 0.02292 -0.0502 0.02959 0.99048 -0.01706 -0.00923 0.01508 0.75168
Circle Of Confusion           : 0.004 mm
Color Space                   : Uncalibrated
Color Space Data              : RGB
Compatible Brands              : mifi, MiPr, miaf, MiHB, heic
Composite Image                : General Composite Image
Connection Space Illuminant   : 0.9642 1 0.82491
Constant Frame Rate           : Unknown
Constraint Indicator Flags    : 176 0 0 0 0
Create Date                   : 2022-04-23 12:34:54.946+02:00
Create Date                    : 2022-04-23 12:34:54
Creator Tool                  : 15.3.1
Date Created                  : 2022-04-23 12:34:54
Date/Time Original            : 2022-04-23 12:34:54.946+02:00
Date/Time Original            : 2022-04-23 12:34:54
Device Attributes              : Reflective, Glossy, Positive, Color
Device Manufacturer            : Apple Computer Inc.
Device Model                  :
Directory                     : .
Exif Byte Order                : Big-endian (Motorola, MM)
Exif Image Height              : 3024
Exif Image Width               : 4032
Exif Version                  : 0232
ExifTool Version Number        : 12.39
Exposure Compensation          : 0
Exposure Mode                  : Auto
Exposure Program                : Program AE
Exposure Time                 : 1/50
F Number                      : 1.8
Field Of View                  : 65.5 deg
File Access Date/Time          : 2022-05-22 03:28:34-04:00
File Inode Change Date/Time    : 2022-05-22 03:28:34-04:00
File Modification Date/Time    : 2022-05-22 03:27:25-04:00
File Name                      : metadatos_original.jpg
File Permissions                : -rw-r--r--
File Size                      : 1991 Kib
File Type                      : HEIC
File Type Extension            : heic
Flash                          : Off, Did not fire
Focal Length                   : 4.0 mm
Focal Length                   : 4.0 mm (35 mm equivalent: 28.0 mm)
Focal Length In 35mm Format    : 28 mm
Gen Profile Compatibility Flags : Main Still Picture, Main 10, Main
General Level IDC              : 90 (Level 3.0)
General Profile IDC            : Main Still Picture
General Profile Space          : Conforming
General Tier Flag              : Main Tier
Green Matrix Column             : 0.29198 0.69225 0.04189
Green Tone Reproduction Curve  : (Binary data 32 bytes, use -b option to extract)
HEVC Configuration Version     : 1
Handler Type                  : Picture
Host Computer                  : iPhone SE (2nd generation)
Hyperfocal Distance            : 2.07 m
ISO                            : 100
Image Height                   : 3024
Image Pixel Depth              : 8 8 8
Image Size                     : 4032x3024
Image Spatial Extent           : 4032x3024
Image Width                     : 4032
Lens ID                        : iPhone SE (2nd generation) back camera 3.99mm f/1.8
Lens Info                      : 3.99mm f/1.8
Lens Make                       : Apple
Lens Model                      : iPhone SE (2nd generation) back camera 3.99mm f/1.8
Light Value                     : 7.3
MIME Type                      : image/heic
Major Brand                    : High Efficiency Image Format HEVC still image (.HEIC)
Make                           : Apple
Media Data Offset               : 3503
Media Data Size                 : 2035642
Media White Point               : 0.95045 1 1.08905
Megapixels                      : 12.2
Meta Image Size                 : 4032x3024
Metering Mode                  : Multi-segment
Min Spatial Segmentation IDC    : 0
Minor Version                  : 0.0.0
Modify Date                     : 2022-04-23 12:34:54+02:00
Modify Date                     : 2022-04-23 12:34:54
Num Temporal Layers             : 1
Offset Time                     : +02:00
Offset Time Digitized          : +02:00
Offset Time Original            : +02:00
Orientation                     : Rotate 90 CW
Parallelism Type                : 0
Primary Item Reference          : 49
Primary Platform                : Apple Computer Inc.
Profile CMM Type                : Apple Computer Inc.
Profile Class                  : Display Device Profile
Profile Connection Space         : XYZ
Profile Copyright               : Copyright Apple Inc., 2017
Profile Creator                 : Apple Computer Inc.
Profile Date Time                : 2017-07-07 13:22:32
Profile Description              : Display P3
```

```
(kali㉿kali)-[~/Desktop]
└─$ exiftool -Sort Metadatos airdrop.jpg
Acceleration Vector      : -0.1022900119 -0.3167135716 -0.9611587519
Aperture                 : 1.8
Aperture Value           : 1.8
Average Frame Rate       : 0
Bit Depth Chroma         : 8
Bit Depth Luma            : 8
Blue Matrix Column        : 0.1571 0.06657 0.78407
Blue Tone Reproduction Curve : (binary data 32 bytes, use -b option to extract)
Brightness Value          : 3.138795192
CMM Flags                : Not Embedded, Independent
Camera Model Name         : iPhone SE (2nd generation)
Chroma Format             : 4:2:0
Chromatic Adaptation     : 1.04788 0.02292 -0.0502 0.02959 0.99048 -0.01706 -0.00923 0.01508 0.75168
Circle Of Confusion       : 0.004 mm
Color Space                : Uncalibrated
Color Space Data           : RGB
Compatible Brands          : mif1, MiPr, miaf, MiHB, heic
Composite Image            : General Composite Image
Connection Space Illuminant : 0.9642 1 0.82491
Constant Frame Rate        : Unknown
Constraint Indicator Flags : 176 0 0 0 0
Create Date                : 2022:04:23 12:34:54.946+02:00
Create Date                : 2022:04:23 12:34:54
Creator Tool               : 15.3.1
Date Created                : 2022:04:23 12:34:54
Date/Time Original          : 2022:04:23 12:34:54
Device Attributes           : Reflective, Glossy, Positive, Color
Device Manufacturer         : Apple Computer Inc.
Device Model                :
Directory                  :
Exif Byte Order             : Big-endian (Motorola, MM)
Exif Image Height            : 3024
Exif Image Width             : 4032
Exif Version                : 0232
ExifTool Version Number      : 12.39
Exposure Compensation        : 0
Exposure Mode                : Auto
Exposure Program              : Program AE
Exposure Time                : 1/50
F Number                   : 1.8
Field Of View                : 65.5 deg
File Access Date/Time        : 2022:05:22 03:18:46-04:00
File Inode Change Date/Time   : 2022:05:22 03:18:46-04:00
File Modification Date/Time    : 2022:04:23 06:34:55-04:00
File Name                   : Metadatos_airdrop.jpg
File Permissions              : -rw-r--r--
File Size                   : 1991 Kib
File Type                   : HEIC
File Type Extension          : heic
Flash                      : Off, Did not fire
```

## Imagen por Airdrop

```
(kali㉿kali)-[~/Desktop]
└─$ exiftool -Sort Metadatos airdrop.jpg
Acceleration Vector      : -0.1022900119 -0.3167135716 -0.9611587519
Aperture                 : 1.8
Aperture Value           : 1.8
Average Frame Rate       : 0
Bit Depth Chroma         : 8
Bit Depth Luma            : 8
Blue Matrix Column        : 0.1571 0.06657 0.78407
Blue Tone Reproduction Curve : (binary data 32 bytes, use -b option to extract)
Brightness Value          : 3.138795192
CMM Flags                : Not Embedded, Independent
Camera Model Name         : iPhone SE (2nd generation)
Chroma Format             : 4:2:0
Chromatic Adaptation     : 1.04788 0.02292 -0.0502 0.02959 0.99048 -0.01706 -0.00923 0.01508 0.75168
Circle Of Confusion       : 0.004 mm
Color Space                : Uncalibrated
Color Space Data           : RGB
Compatible Brands          : mif1, MiPr, miaf, MiHB, heic
Composite Image            : General Composite Image
Connection Space Illuminant : 0.9642 1 0.82491
Constant Frame Rate        : Unknown
Constraint Indicator Flags : 176 0 0 0 0
Create Date                : 2022:04:23 12:34:54.946+02:00
Create Date                : 2022:04:23 12:34:54
Creator Tool               : 15.3.1
Date Created                : 2022:04:23 12:34:54
Date/Time Original          : 2022:04:23 12:34:54
Device Attributes           : Reflective, Glossy, Positive, Color
Device Manufacturer         : Apple Computer Inc.
Device Model                :
Directory                  :
Exif Byte Order             : Big-endian (Motorola, MM)
Exif Image Height            : 3024
Exif Image Width             : 4032
Exif Version                : 0232
ExifTool Version Number      : 12.39
Exposure Compensation        : 0
Exposure Mode                : Auto
Exposure Program              : Program AE
Exposure Time                : 1/50
F Number                   : 1.8
Field Of View                : 65.5 deg
File Access Date/Time        : 2022:05:22 03:18:46-04:00
File Inode Change Date/Time   : 2022:05:22 03:18:46-04:00
File Modification Date/Time    : 2022:04:23 06:34:55-04:00
File Name                   : Metadatos_airdrop.jpg
File Permissions              : -rw-r--r--
File Size                   : 1991 Kib
File Type                   : HEIC
File Type Extension          : heic
Flash                      : Off, Did not fire
```

```
Focal Length           : 4.0 mm
Focal Length          : 4.0 mm (35 mm equivalent: 28.0 mm)
Focal Length In 35mm Format : 28 mm
Gen Profile Compatibility Flags : Main Still Picture, Main 10, Main
General Level IDC    : 90 (Level 3.0)
General Profile IDC   : Main Still Picture
General Profile Space : Conforming
General Tier Flag     : Main Tier
Green Matrix Column    : 0.29198 0.69225 0.04189
Green Tone Reproduction Curve : (Binary data 32 bytes, use -b option to extract)
HEVC Configuration Version : 1
Handler Type          : Picture
Host Computer          : iPhone SE (2nd generation)
Hyperfocal Distance    : 2.07 m
ISO                   : 100
Image Height          : 3024
Image Pixel Depth     : 8 8 8
Image Size             : 4032x3024
Image Spatial Extent  : 4032x3024
Image Width            : 4032
Lens ID               : iPhone SE (2nd generation) back camera 3.99mm f/1.8
Lens Info              : 3.99mm f/1.8
Lens Make              : Apple
Lens Model              : iPhone SE (2nd generation) back camera 3.99mm f/1.8
Light Value            : 7.3
MIME Type              : image/heic
Major Brand            : High Efficiency Image Format HEVC still image (.HEIC)
Make                  : Apple
Media Data Offset      : 3503
Media Data Size        : 2035642
Media White Point      : 0.95045 1 1.08905
Megapixels             : 12.2
Meta Image Size        : 4032x3024
Metering Mode          : Multi-segment
Min Spatial Segmentation IDC : 0
Minor Version          : 0.0.0
Modify Date            : 2022-04-23 12:34:54+02:00
Modify Date            : 2022-04-23 12:34:54
Num Temporal Layers   : 1
Offset Time            : +02:00
Offset Time Digitized : +02:00
Offset Time Original  : +02:00
Orientation            : Rotate 90 CW
Parallelism Type       : 0
Primary Item Reference : 49
Primary Platform        : Apple Computer Inc.
Profile CMM Type       : Apple Computer Inc.
Profile Class          : Display Device Profile
Profile Connection Space : XYZ
Profile Copyright       : Copyright Apple Inc., 2017
Profile Creator          : Apple Computer Inc.
Profile Date Time       : 2017-07-07 13:22:32
Profile Description      : Display P3
Profile File Signature  : acsp
Profile ID              : cala9582257f104d389913d5diea1582
Profile Version          : 4.0.0
Red Matrix Column       : 0.51512 0.2412 -0.00105
Red Tone Reproduction Curve : (Binary data 32 bytes, use -b option to extract)
Region Applied To Dimensions H : 3024
Region Applied To Dimensions Unit: pixel
Region Applied To Dimensions W : 4224
Region Area H            : 0.068000000000000006
Region Area Unit          : normalized
Region Area W            : 0.050285714285714267
Region Area X            : 0.5073333333333333
Region Area Y            : 0.6330000000000001
Region Extensions Angle Info Roll: 270
Region Extensions Angle Info Yaw: 0
Region Extensions Confidence Level: 706
Region Extensions Face ID : 2
Region Type              : Face
Rendering Intent          : Perceptual
Resolution Unit           : inches
Rotation                 : 270
Run Time Epoch            : 0
Run Time Flags             : Valid
Run Time Scale             : 1000000000
Run Time Since Power Up  : 14:34:20
Run Time Value             : 52459533008833
Scale Factor To 35 mm Equivalent: 7.0
Scene Type                : Directly photographed
Sensing Method             : One-chip color area
Shutter Speed              : 1/50
Shutter Speed Value        : 1/50
Software                  : 15.3.1
Sub Sec Time Digitized   : 946
Sub Sec Time Original     : 946
Subject Area                : 2042 1910 198 199
Temporal ID Nested         : No
White Balance              : Auto
X Resolution                : 72
XMP Toolkit                 : XMP Core 6.0.0
Y Resolution                : 72
```

## Imagen por correo electrónico Gmail

```
exiftool -Sort metadatos_mail.jpg
Bits Per Sample : 8
Color Components : 3
Color Space : sRGB
Directory :
Encoding Process : Baseline DCT, Huffman coding
Exif Byte Order : Big-endian (Motorola, MM)
Exif Image Height : 240
Exif Image Width : 320
ExifTool Version Number : 12.39
File Access Date/Time : 2022:05:22 12:29:46-04:00
File Inode Change Date/Time : 2022:05:22 12:29:46-04:00
File Modification Date/Time : 2022:05:22 12:29:17-04:00
File Name : metadatos_mail.jpg
File Permissions : -rw-r--r--
File Size : 23 Kib
File Type : JPEG
File Type Extension : jpg
Image Height : 240
Image Size : 320x240
Image Width : 320
JFIF Version : 1.01
MIME Type : image/jpeg
Megapixels : 0.077
Orientation : Rotate 90 CW
Resolution Unit : None
X Resolution : 72
YCbCr Sub Sampling : YCbCr4:2:0 (2 2)
Y Resolution : 72
```

## Imagen por Discord

```
(kali㉿kali)-[~/Desktop]
└─$ exiftool -Sort metadatos_discord.jpg
Bits Per Sample : 8
Blue Matrix Column : 0.1571 0.06657 0.78407
Blue Tone Reproduction Curve : (Binary data 32 bytes, use -b option to extract)
CMM Flags : Not Embedded, Independent
Chromatic Adaptation : 1.04788 0.02292 -0.0502 0.02959 0.99048 -0.01706 -0.00923 0.01508 0.75168
Color Components :
Color Space Data :
Connection Space Illuminant : 0.9642 1 0.82491
Create Date : 2022:04:23 12:34:54
Creator Tool : 15.3.1
Date Created : 2022:04:23 12:34:54
Device Attributes : Reflective, Glossy, Positive, Color
Device Manufacturer : Apple Computer Inc.
Device Model :
Directory :
Encoding Process : Baseline DCT, Huffman coding
Exif Byte Order : Big-endian (Motorola, MM)
ExifTool Version Number : 12.39
File Access Date/Time : 2022:05:22 12:34:49-04:00
File Inode Change Date/Time : 2022:05:22 12:34:49-04:00
File Modification Date/Time : 2022:05:22 12:33:55-04:00
File Name : metadatos_discord.jpg
File Permissions : -rw-r--r--
File Size : 2.3 Mib
File Type : JPEG
File Type Extension : jpg
Green Matrix Column : 0.29198 0.69225 0.04189
Green Tone Reproduction Curve : (Binary data 32 bytes, use -b option to extract)
Image Height : 3024
Image Size : 4032x3024
Image Width : 4032
MIME Type : image/jpeg
Media White Point : 0.95045 1 1.08905
Megapixels : 12.2
Modify Date :
Orientation :
Primary Platform : Apple Computer Inc.
Profile CMM Type : Apple Computer Inc.
Profile Class : Apple Computer Inc.
Profile Connection Space : Display Device Profile
Profile Copyright : Copyright Apple Inc., 2017
Profile Creator : Apple Computer Inc.
Profile Date Time : 2017:07:07 13:22:32
Profile Description : Display P3
Profile File Signature : acsp
Profile ID : cala9582257f104d389913d5d1ea1582
Profile Version : 4.0.0
Red Matrix Column : 0.51912 0.2412 -0.00105
Red Tone Reproduction Curve : (Binary data 32 bytes, use -b option to extract)
Region Applied To Dimensions H : 3024
Region Applied To Dimensions Unit: pixel
Region Applied To Dimensions W : 4224
Region Area H : 0.0680000000000006
Region Area Unit : normalized
Region Area W : 0.050285714285714267
Region Area X : 0.5073333333333333
Region Area Y : 0.6330000000000001
Region Extensions Angle Info Roll: 270
Region Extensions Angle Info Yaw: 0
Region Extensions Confidence Level: 706
Region Extensions Face ID : 2
Region Type : Face
Rendering Intent : Perceptual
XMP Toolkit : XMP Core 6.0.0
YCbCr Sub Sampling : YCbCr4:2:0 (2 2)
```

## Imagen por Slack

```
(kali㉿kali)-[~/Desktop]
└─$ exiftool -Sort metadatos slack.jpg
Application Record Version : 2
Bits Per Sample : 8
Blue Matrix Column : 0.1571 0.06657 0.78407
Blue Tone Reproduction Curve : (Binary data 32 bytes, use -b option to extract)
CMM Flags : Not Embedded, Independent
Chromatic Adaptation : 1.04788 0.02292 -0.0502 0.02959 0.99048 -0.01706 -0.00923 0.01508 0.75168
Coder Character Set : UTF8
Color Components : 3
Color Space Data : RGB
Connection Space Illuminant : 0.9642 1 0.82491
Create Date : 2022:04:23 12:34:54
Creator Tool : 15.3.1
Current IPTC Digest : 2907542abd45c577877c918232ac01ad
Date Created : 2022:04:23 12:34:54
Date/Time Created : 2022:04:23 12:34:54
Date/Time Original : 2022:04:23 12:34:54
Device Attributes : Reflective, Glossy, Positive, Color
Device Manufacturer : Apple Computer Inc.
Device Model : 
Digital Creation Date : 2022:04:23
Digital Creation Date/Time : 2022:04:23 12:34:54
Digital Creation Time : 12:34:54
Directory : 
Encoding Process : Baseline DCT, Huffman coding
ExifTool Version Number : 12.39
File Access Date/Time : 2022:05:22 03:49:31-04:00
File Inode Change Date/Time : 2022:05:22 03:49:31-04:00
File Modification Date/Time : 2022:05:22 03:48:51-04:00
File Name : metadatos_slack.jpg
File Permissions : -rw-r--r--
File Size : 2.4 MiB
File Type : JPEG
File Type Extension : jpg
File Type Extension : 0.29198 0.69225 0.04189
Green Matrix Column : (Binary data 32 bytes, use -b option to extract)
Green Tone Reproduction Curve : 2907542abd45c577877c918232ac01ad
IPTC Digest : 
Image Height : 4032
Image Size : 3024x4032
Image Width : 3024
JFIF Version : 1.01
MIME Type : image/jpeg
Media White Point : 0.95045 1 1.08905
Megapixels : 12.2
Modify Date : 2022:04:23 12:34:54
Primary Platform : Apple Computer Inc.
Profile CMM Type : Apple Computer Inc.
Profile Class : Display Device Profile
Profile Connection Space : XYZ
Profile Copyright : Copyright Apple Inc., 2017
Profile Creator : Apple Computer Inc.
Profile Date Time : 2017:07:07 13:22:32
Profile Description : Display P3
Profile File Signature : acsp
Profile ID : cala9582257f104d389913d5d1ea1582
Profile Version : 4.0.0
Red Matrix Column : 0.51512 0.2412 -0.00105
Red Tone Reproduction Curve : (Binary data 32 bytes, use -b option to extract)
Region Applied To Dimensions H : 3024
Region Applied To Dimensions Unit: pixel
Region Applied To Dimensions W : 4224
Region Area H : 0.0680000000000006
Region Area Unit : normalized
Region Area W : 0.050285714285714267
Region Area X : 0.5073333333333333
Region Area Y : 0.6330000000000001
Region Extensions Angle Info Roll: 270
Region Extensions Angle Info Yaw: 0
Region Extensions Confidence Level: 706
Region Extensions Face ID : 2
Region Type : Face
Rendering Intent : Perceptual
Resolution Unit : inches
Time Created : 12:34:54
X Resolution : 72
XMP Toolkit : XMP Core 6.0.0
YCbCr Sub Sampling : YCbCr4:2:0 (2 2)
Y Resolution : 72
```

## Imagen por Telegram

```
(kali㉿kali)-[~/Desktop]
└─$ exiftool -Sort metadatos telegram.jpg
Bits Per Sample : 8
Color Components : 3
Color Space : sRGB
Components Configuration : Y, Cb, Cr, -
Compression : JPEG (old-style)
Create Date : 2022:05:22 09:42:31.914+02:00
Create Date : 2022:05:22 09:42:31
Create Date : 2022:05:22 09:42:31
Date/Time Original : 2022:05:22 09:42:31.914+02:00
Date/Time Original : 2022:05:22 09:42:31.914+02:00
Directory :
Encoding Process : Progressive DCT, Huffman coding
Exif Byte Order : Big-endian (Motorola, MM)
Exif Image Height : 1280
Exif Image Width : 960
Exif Version : 0221
ExifTool Version Number : 12.39
File Access Date/Time : 2022:05:22 03:44:29-04:00
File Inode Change Date/Time : 2022:05:22 03:44:29-04:00
File Modification Date/Time : 2022:05:22 03:44:18-04:00
File Name : metadatos_telegram.jpg
File Permissions : -rw-r--r--
File Size : 114 KiB
File Type : JPEG
File Type Extension : jpg
Flashpix Version : 0100
Image Height : 1280
Image Size : 960x1280
Image Width : 960
MIME Type : image/jpeg
Megapixels : 1.2
Modify Date : 2022:05:22 09:42:31.914+02:00
Modify Date : 2022:05:22 09:42:31
Offset Time : +02:00
Offset Time Digitized : +02:00
Offset Time Original : +02:00
Resolution Unit : inches
Scene Capture Type : Standard
Sub Sec Time : 914
Sub Sec Time Digitized : 914
Sub Sec Time Original : 914
Thumbnail Image : (Binary data 9775 bytes, use -b option to extract)
Thumbnail Length : 9775
Thumbnail Offset : 478
X Resolution : 72
YCbCr Positioning : Centered
YCbCr Sub Sampling : YCbCr4:2:0 (2 2)
Y Resolution : 72
```

## Imagen por Whatsapp

```
(kali㉿kali)-[~/Desktop]
└─$ exiftool -Sort metadatos whatsapp.jpg
Bits Per Sample : 8
Color Components : 3
Directory :
Encoding Process : Progressive DCT, Huffman coding
ExifTool Version Number : 12.39
File Access Date/Time : 2022:05:22 12:19:30-04:00
File Inode Change Date/Time : 2022:05:22 12:19:30-04:00
File Modification Date/Time : 2022:05:22 07:42:49-04:00
File Name : metadatos_whatsapp.jpg
File Permissions : -rw-r--r--
File Size : 156 KiB
File Type : JPEG
File Type Extension : jpg
Image Height : 1600
Image Size : 1200x1600
Image Width : 1200
JFIF Version : 1.01
MIME Type : image/jpeg
Megapixels : 1.9
Resolution Unit : None
X Resolution : 1
YCbCr Sub Sampling : YCbCr4:2:0 (2 2)
Y Resolution : 1
```

## Conclusiones

Como puede observarse, el envío por las aplicaciones de mensajería instantánea Telegram y Whatsapp, y el envío por correo electrónico son los que alteran en mayor medida los metadatos de la imagen original, eliminando gran parte de ellos.

Por ejemplo, en los 3 casos se elimina de los metadatos el dispositivo con el que se ha tomado la imagen. También el correo electrónico y Whatsapp eliminan la fecha en la que se ha creado la imagen.

La única aplicación que mantiene los metadatos tal cual son en la imagen original es Airdrop.

Discord y Slack mantienen bastantes datos, aunque también eliminan algunos relevantes como el dispositivo que ha hecho la fotografía.