CIBERSEGURIDAD

‘Bootcamp IX’

Informe Práctica Módulo DFIR.

Maximiliano Dariel Altamirano.

Academia KeepCoding.

INDICE

[DESARROLLO 3](#_Toc194871642)

[Práctica Windows 4](#_Toc194871643)

[Forensic 4](#_Toc194871644)

[Hash del fichero 4](#_Toc194871645)

[Nombre de la máquina 4](#_Toc194871646)

[Ficheros maliciosos 5](#_Toc194871647)

[Descarga fichero de control remoto 5](#_Toc194871648)

[Fecha descarga software control remoto 5](#_Toc194871649)

[Ficheros eliminados 6](#_Toc194871650)

[Contraseñas débiles 6](#_Toc194871651)

[Conexión RDP 6](#_Toc194871652)

[Práctica memoria RAM 7](#_Toc194871653)

[Práctica Metadatos 9](#_Toc194871654)

[Conclusiones: 11](#_Toc194871655)

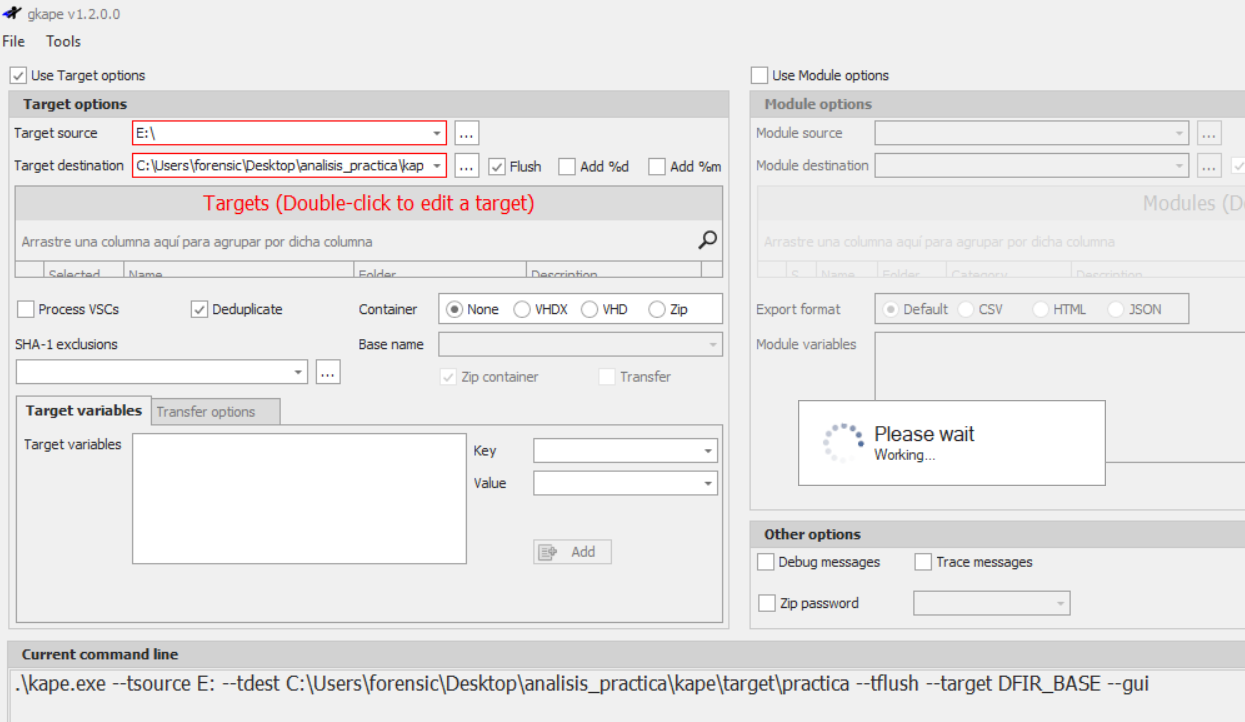
[RESUMEN 12](#_Toc194871656)

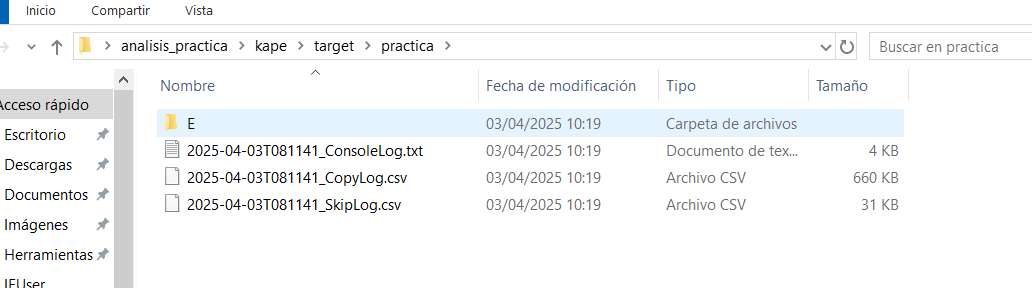
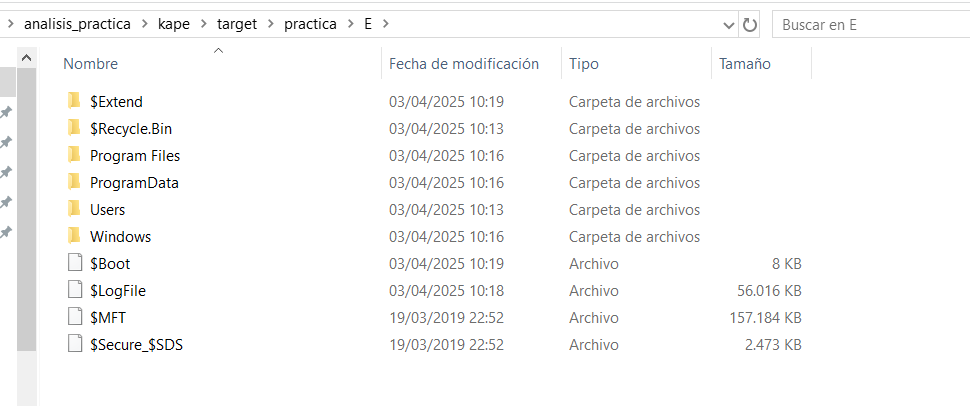
[Objetivo 12](#_Toc194871657)

[Herramientas 12](#_Toc194871658)

# DESARROLLO

Para el análisis de la evidencia vamos a preprocesar los datos y ficheros con la herramienta Kape, utilizando el módulo target predefinido “DFIR\_BASE.tkape”.



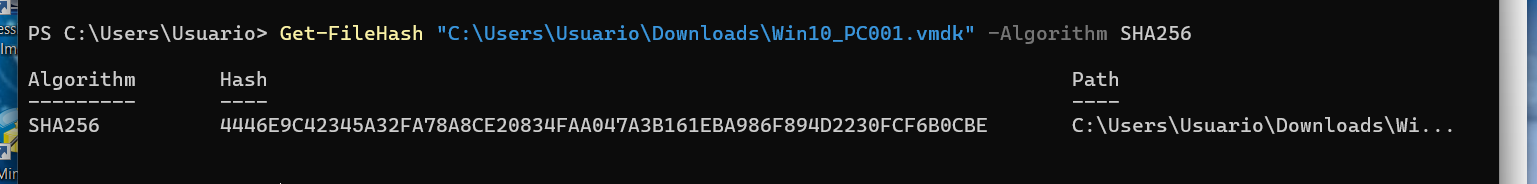
# Práctica Windows

Avanzaremos en los desafíos propuestos en el enlace <http://ctf.sancastell.me/challenges>

## Forensic

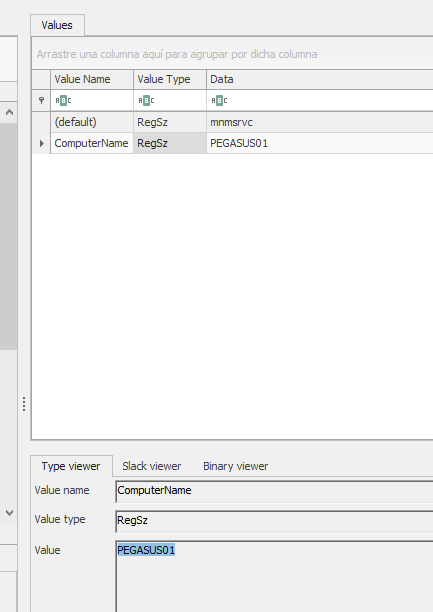
### Hash del fichero

Valimos el hash del fichero con el siguiente comando en la consola de Windows



### Nombre de la máquina

Navegaremos las opciones con la herramienta RegistryExplorer para identificar el nombre de la máquina



### Ficheros maliciosos

Utilizamos el módulo loki.exe para intentar identificar los ficheros maliciosos, obteniendo como ruta crítica E:\Users\Public



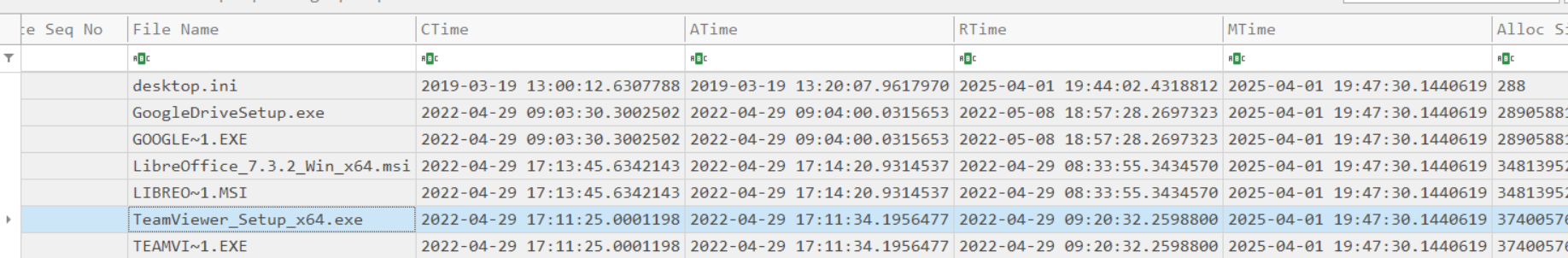
### Descarga fichero de control remoto

Con la herramienta FTK Imager identificamos el archivo .exe de control remoto que ha descargado el usuario.



### Fecha descarga software control remoto

Identificamos con la herramienta Timeline Explorer, procesando con Indx2Csv previamente el fichero $I30 del directorio Descargas del usuario, la fecha en la que hizo la descarga.

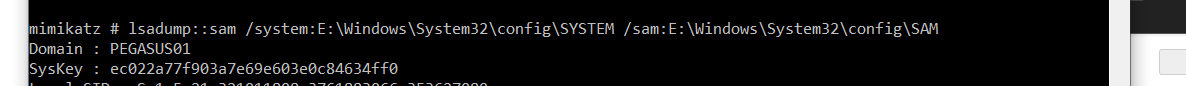


### Ficheros eliminados

Con la herramienta UsnJrnl2Csv64.exe exploramos la información del fichero $J para identificar el fichero .zip eliminado

### Contraseñas débiles

Para descubrir la contraseña, utilizamos el módulo mimikatz, lanzando el siguiente comando:



Obteniendo como resultado el siguiente HASH

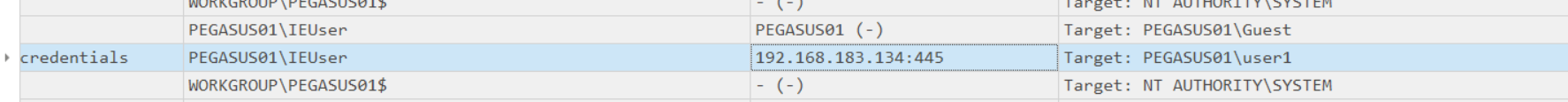


Solo resta romper el hash desde <https://crackstation.net/>



### Conexión RDP

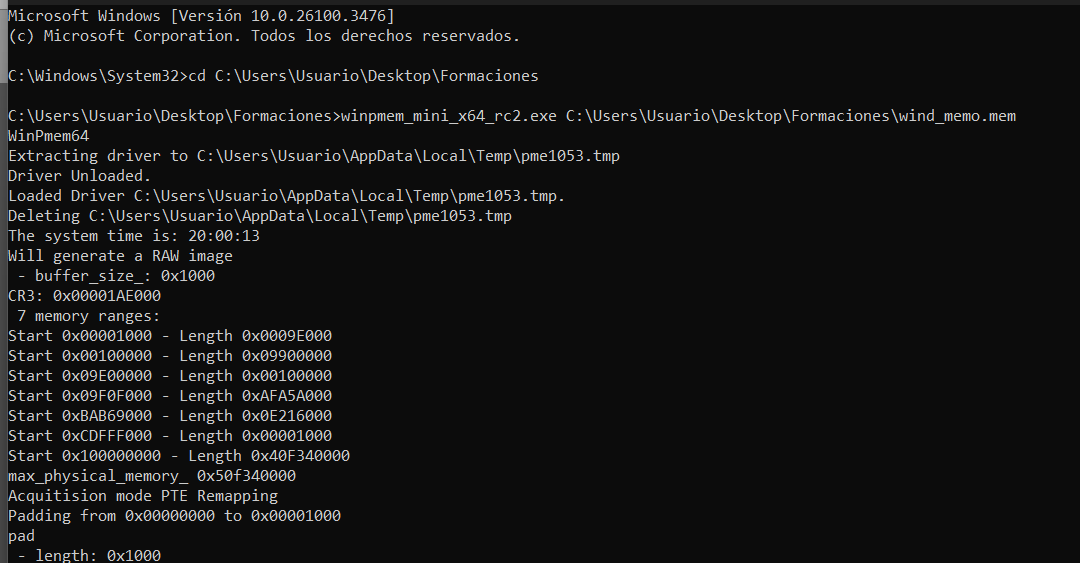
Hemos identificado el IP de conexión por RDP con los datos obtenidos desde los eventos de seguridad de Wind (192.168.183.134:445).



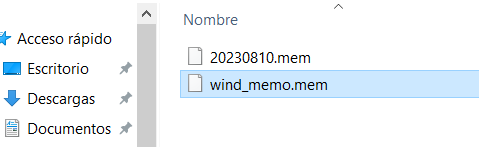
# Práctica memoria RAM

Haremos una adquisición desde nuestra RAM en Windows. Utilizaremos la herramienta *winpmem\_mini\_x64\_rc2.exe*. Lanzaremos desde el CMD como administrador el siguiente comando:

C:\Users\Usuario\Desktop\Formaciones>winpmem\_mini\_x64\_rc2.exe C:\Users\Usuario\Desktop\Formaciones\wind\_memo.mem



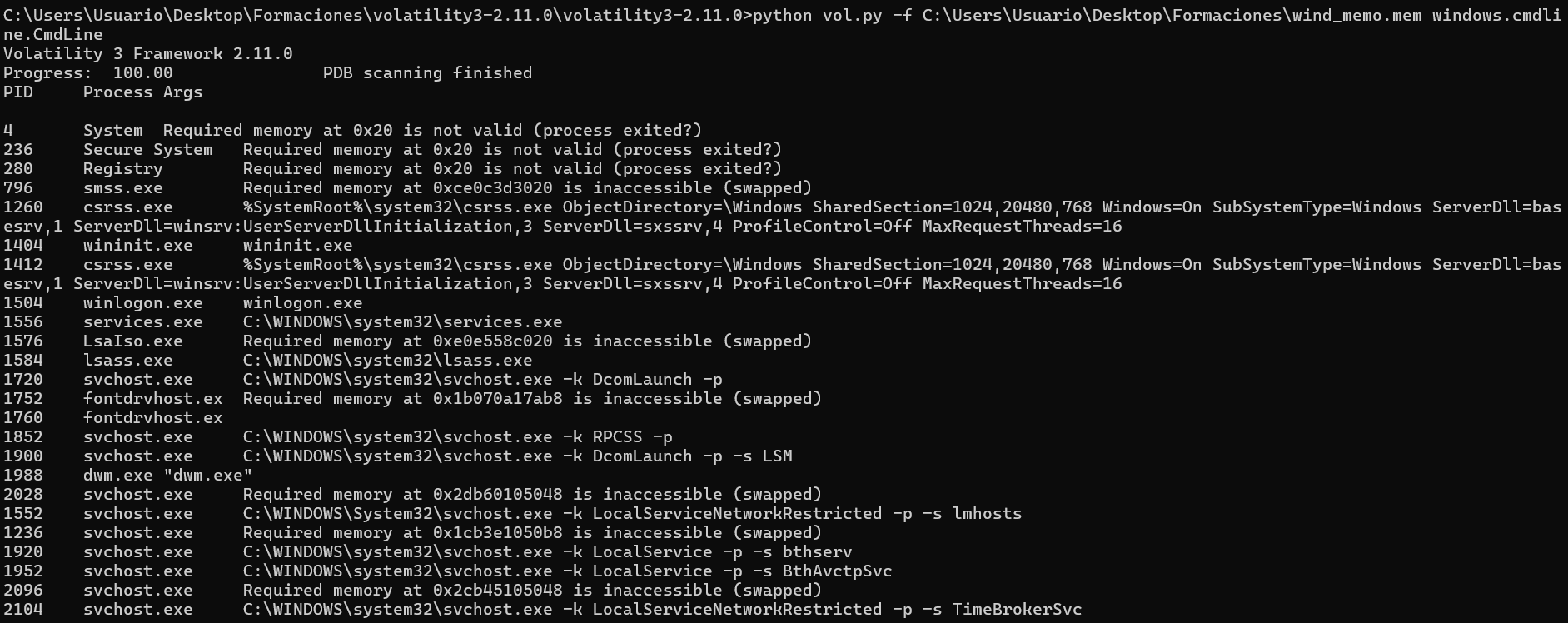
Generando el siguiente fichero(wind\_memo.mem):



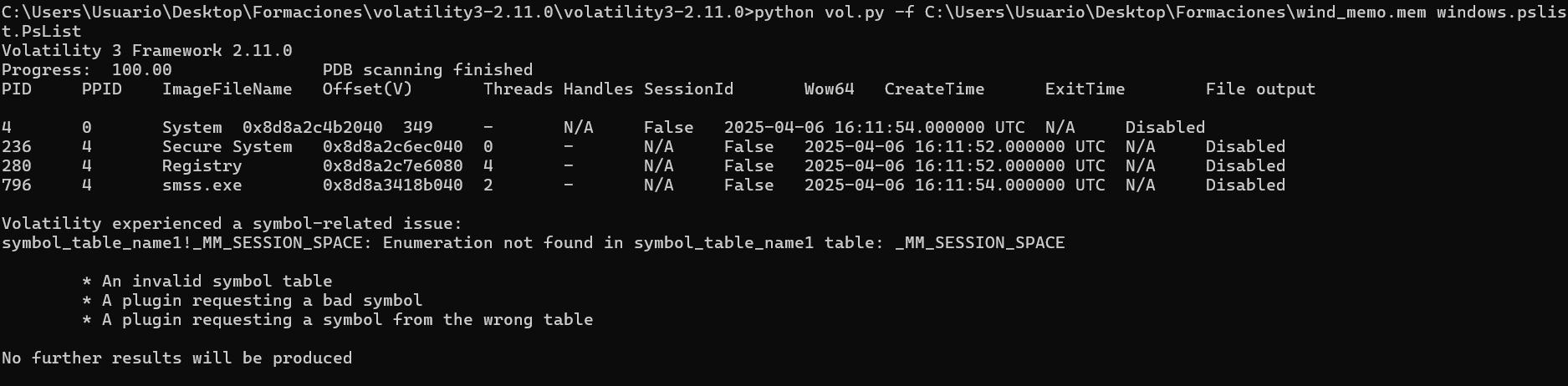
Utilizaremos *Volatility* para interpretar la memoria que hemos generado:

Lanzaremos los comandos más utilizados para el análisis (adquisición de RAM maquina Wind propia):

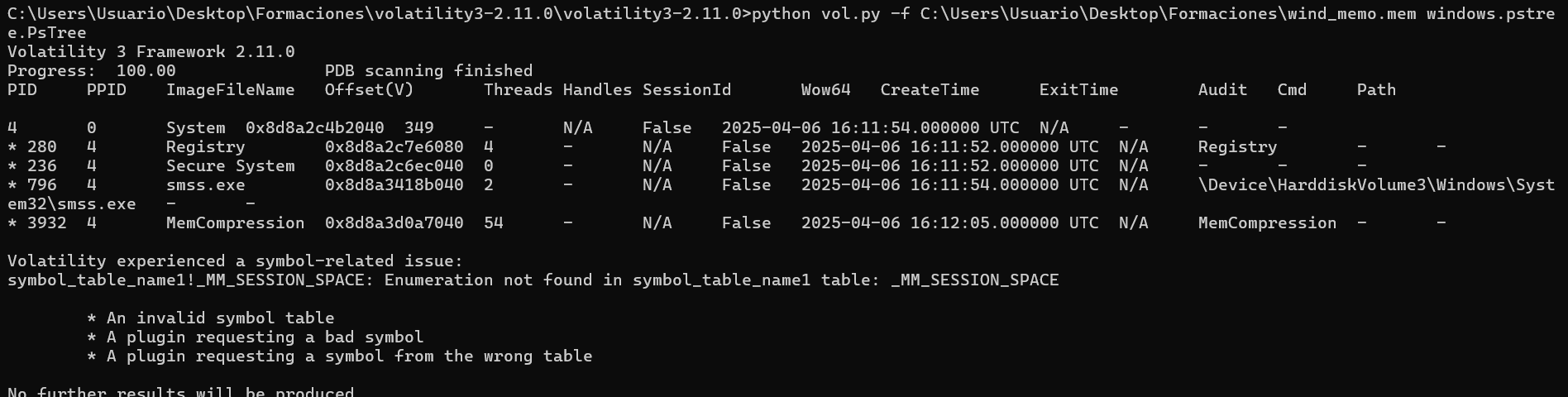
*python vol.py -f C:\Users\Usuario\Desktop\Formaciones\wind\_memo.mem windows.cmdline.CmdLine*

**

*python vol.py -f C:\Users\Usuario\Desktop\Formaciones\wind\_memo.mem windows.pslist.PsList*

**

*python vol.py -f C:\Users\Usuario\Desktop\Formaciones\wind\_memo.mem windows.pstree.PsTree*

**

# Práctica Metadatos

Analizaremos 3 imágenes incluidas en directorio *Imágenes (adjunta en la práctica)* con el módulo *exiftool*.

Para este punto enviaremos la imagen original tomada desde un terminal POCO F5 por dos medios, envío por Gmail y WhatsApp.

Para este punto evidenciamos el análisis de la imagen “original\_1” del directorio “imagen\_1”, obteniendo los siguientes resultados:

|  |  |  |
| --- | --- | --- |
| **======== original\_1.jpg** | **======== gmail\_1.jpg** | **======== wp\_1.jfif** |
| ExifTool Version Number : 13.10 | ExifTool Version Number : 13.10 | ExifTool Version Number : 13.10 |
| File Name : original\_1.jpg | File Name : gmail\_1.jpg | File Name : wp\_1.jfif |
| Directory : . | Directory : . | Directory : . |
| File Size : 3.5 MB | File Size : 3.5 MB | File Size : 373 kB |
| File Modification Date/Time : 2025:04:06 00:02:04+02:00 | File Modification Date/Time : 2025:04:06 00:02:04+02:00 | File Modification Date/Time : 2025:04:06 00:02:05+02:00 |
| File Access Date/Time : 2025:04:06 00:11:14+02:00 | File Access Date/Time : 2025:04:06 00:11:14+02:00 | File Access Date/Time : 2025:04:06 00:18:54+02:00 |
| File Inode Change Date/Time : 2025:04:06 00:08:41+02:00 | File Inode Change Date/Time : 2025:04:06 00:08:41+02:00 | File Inode Change Date/Time : 2025:04:06 00:08:41+02:00 |
| File Permissions : -rw------- | File Permissions : -rw------- | File Permissions : -rw------- |
| File Type : JPEG | File Type : JPEG | File Type : JPEG |
| File Type Extension : jpg | File Type Extension : jpg | File Type Extension : jpg |
| MIME Type : image/jpeg | MIME Type : image/jpeg | MIME Type : image/jpeg |
| Exif Byte Order : Big-endian (Motorola, MM) | Exif Byte Order : Big-endian (Motorola, MM) | JFIF Version : 1.01 |
| Make : Xiaomi | Make : Xiaomi | Resolution Unit : None |
| Orientation : Horizontal (normal) | Orientation : Horizontal (normal) | X Resolution : 1 |
| Modify Date : 2025:03:28 11:35:03 | Modify Date : 2025:03:28 11:35:03 | Y Resolution : 1 |
| Y Resolution : 72 | Y Resolution : 72 | Image Width : 1640 |
| X Resolution : 72 | X Resolution : 72 | Image Height : 1232 |
| Camera Model Name : 23049PCD8G | Camera Model Name : 23049PCD8G | Encoding Process : Progressive DCT, Huffman coding |
| Y Cb Cr Positioning : Centered | Y Cb Cr Positioning : Centered | Bits Per Sample : 8 |
| Exif Version : 0220 | Exif Version : 0220 | Color Components : 3 |
| Aperture Value : 2.2 | Aperture Value : 2.2 | Y Cb Cr Sub Sampling : YCbCr4:2:0 (2 2) |
| Scene Type : Directly photographed | Scene Type : Directly photographed | Image Size : 1640x1232 |
| Mirror : false | Mirror : false | Megapixels : 2.0 |
| Sensor Type : rear | Sensor Type : rear |  |
| Hdr : auto | Hdr : auto |  |
| Op Mode : 36869 | Op Mode : 36869 |  |
| Small Picture : false | Small Picture : false |  |
| AI Scene : 15 | AI Scene : 15 |  |
| Filter Id : 66048 | Filter Id : 66048 |  |
| Zoom Multiple : 0.6000000238418579 | Zoom Multiple : 0.6000000238418579 |  |
| Exposure Compensation : 0 | Exposure Compensation : 0 |  |
| Exposure Program : Program AE | Exposure Program : Program AE |  |
| Color Space : sRGB | Color Space : sRGB |  |
| Max Aperture Value : 2.2 | Max Aperture Value : 2.2 |  |
| Exif Image Height : 2464 | Exif Image Height : 2464 |  |
| Brightness Value : 7.92 | Brightness Value : 7.92 |  |
| Date/Time Original : 2025:03:28 11:35:03 | Date/Time Original : 2025:03:28 11:35:03 |  |
| Flashpix Version : 0100 | Flashpix Version : 0100 |  |
| Sub Sec Time Original : 986 | Sub Sec Time Original : 986 |  |
| White Balance : Auto | White Balance : Auto |  |
| Interoperability Index : R98 - DCF basic file (sRGB) | Interoperability Index : R98 - DCF basic file (sRGB) |  |
| Interoperability Version : 0100 | Interoperability Version : 0100 |  |
| Exposure Mode : Auto | Exposure Mode : Auto |  |
| Exposure Time : 1/753 | Exposure Time : 1/753 |  |
| Offset Time : +01:00 | Offset Time : +01:00 |  |
| Flash : Auto, Did not fire | Flash : Auto, Did not fire |  |
| Sub Sec Time : 986 | Sub Sec Time : 986 |  |
| F Number : 2.2 | F Number : 2.2 |  |
| Exif Image Width : 3280 | Exif Image Width : 3280 |  |
| ISO : 50 | ISO : 50 |  |
| Components Configuration : Y, Cb, Cr, - | Components Configuration : Y, Cb, Cr, - |  |
| Focal Length In 35mm Format : 16 mm | Focal Length In 35mm Format : 16 mm |  |
| Sub Sec Time Digitized : 986 | Sub Sec Time Digitized : 986 |  |
| Create Date : 2025:03:28 11:35:03 | Create Date : 2025:03:28 11:35:03 |  |
| Shutter Speed Value : 1/753 | Shutter Speed Value : 1/753 |  |
| Metering Mode : Center-weighted average | Metering Mode : Center-weighted average |  |
| Focal Length : 1.6 mm | Focal Length : 1.6 mm |  |
| Offset Time Original : +01:00 | Offset Time Original : +01:00 |  |
| Scene Capture Type : Standard | Scene Capture Type : Standard |  |
| Light Source : D65 | Light Source : D65 |  |
| Sensing Method : Not defined | Sensing Method : Not defined |  |
| Resolution Unit : inches | Resolution Unit : inches |  |
| Xiaomi Model : POCO F5 | Xiaomi Model : POCO F5 |  |
| Compression : JPEG (old-style) | Compression : JPEG (old-style) |  |
| Thumbnail Offset : 10716 | Thumbnail Offset : 10716 |  |
| Thumbnail Length : 25060 | Thumbnail Length : 25060 |  |
| Image Width : 3280 | Image Width : 3280 |  |
| Image Height : 2464 | Image Height : 2464 |  |
| Encoding Process : Baseline DCT, Huffman coding | Encoding Process : Baseline DCT, Huffman coding |  |
| Bits Per Sample : 8 | Bits Per Sample : 8 |  |
| Color Components : 3 | Color Components : 3 |  |
| Y Cb Cr Sub Sampling : YCbCr4:2:0 (2 2) | Y Cb Cr Sub Sampling : YCbCr4:2:0 (2 2) |  |
| Aperture : 2.2 | Aperture : 2.2 |  |
| Image Size : 3280x2464 | Image Size : 3280x2464 |  |
| Megapixels : 8.1 | Megapixels : 8.1 |  |
| Scale Factor To 35 mm Equivalent: 9.7 | Scale Factor To 35 mm Equivalent: 9.7 |  |
| Shutter Speed : 1/753 | Shutter Speed : 1/753 |  |
| Create Date : 2025:03:28 11:35:03.986 | Create Date : 2025:03:28 11:35:03.986 |  |
| Date/Time Original : 2025:03:28 11:35:03.986+01:00 | Date/Time Original : 2025:03:28 11:35:03.986+01:00 |  |
| Modify Date : 2025:03:28 11:35:03.986+01:00 | Modify Date : 2025:03:28 11:35:03.986+01:00 |  |
| Thumbnail Image : (Binary data 25060 bytes, use -b option to extract) | Thumbnail Image : (Binary data 25060 bytes, use -b option to extract) |  |
| Circle Of Confusion : 0.003 mm | Circle Of Confusion : 0.003 mm |  |
| Field Of View : 96.7 deg | Field Of View : 96.7 deg |  |
| Focal Length : 1.6 mm (35 mm equivalent: 16.0 mm) | Focal Length : 1.6 mm (35 mm equivalent: 16.0 mm) |  |
| Hyperfocal Distance : 0.40 m | Hyperfocal Distance : 0.40 m |  |
| Light Value : 12.8 | Light Value : 12.8 |  |

### Conclusiones:

Los metadatos originales se respetan en el envío por mail, pero no así en los servicios de mensajería (WhatsApp), ya que en este último perduran solo los indicadores “básicos” como metadatos.

Esto se debe a varios motivos:

Compresión: Algunas aplicaciones reduce el tamaño de las imágenes para ahorrar espacio, eliminando o modificando metadatos como la ubicación o los ajustes de la cámara. En nuestro análisis vemos reducido el tamaño del archivo y la calidad de la imagen en WhatsApp.

Privacidad: Algunas plataformas eliminan metadatos sensibles, como la geolocalización, para proteger la privacidad del usuario.

Optimización: Servicios como Gmail pueden ajustar el formato o la resolución de las imágenes para facilitar su envío y visualización.

Dejamos evidencia en el mismo directorio de 2 imágenes más con resultados similares a este.

# RESUMEN

## Objetivo

El informe pretende dejar en evidencia las herramientas y conocimientos adquiridos en el módulo DFIR, explorando desde una máquina virtual, todas las herramientas revisadas en clases.

## Herramientas

Para el avance de utilizamos las siguientes herramientas:

* Virtual Box – Windows 10
* Virtual Box - Kali