Digital Forensics and Incident Response
Monica Licea Castro
Rabrial03@gmail.com

Práctica de DFIR en Windows.

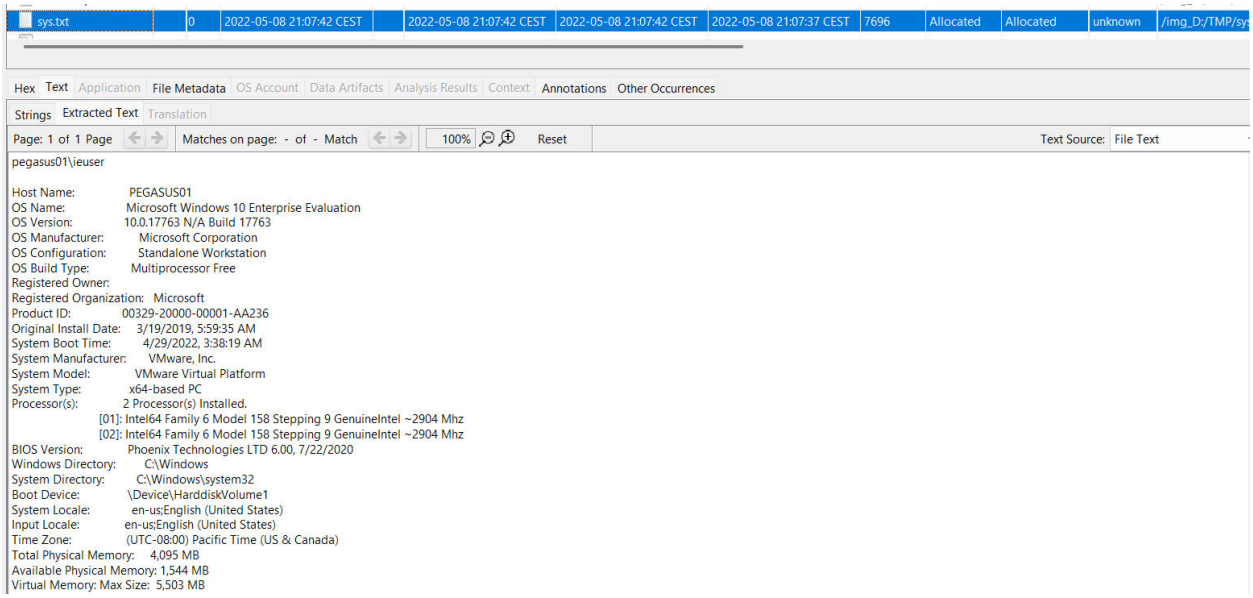
Introducción
Durante esta práctica de laboratorio de DFIR (Digital Forensics and Incident Response), se trabajó con una imagen de máquina virtual con sistema operativo Windows 10, orientada al análisis forense digital. El objetivo principal fue adquirir y analizar evidencia digital para resolver una serie de retos tipo CTF (Capture the Flag), cada uno representando escenarios realistas de incidentes de seguridad.

Inicié el análisis de la máquina con sistema operativo Windows 10 utilizando diversas herramientas presentadas a lo largo del curso. Ante la sospecha de que el usuario del equipo pudiera estar extrayendo información confidencial de la empresa, y tras recibir una alerta del equipo de monitorización sobre comportamientos anómalos en el sistema, se nos encomendó realizar un análisis forense con el fin de identificar posibles indicios y evidencias que confirmen o descarten dichas sospechas.

A continuación, se detallan las herramientas empleadas y las opciones seleccionadas en cada caso para alcanzar los resultados esperados. En varias ocasiones se utilizaron múltiples herramientas —hasta tres o cuatro— que arrojaron los mismos hallazgos; sin embargo, en este informe se presentarán únicamente los resultados obtenidos con una de ellas, con el objetivo de simplificar la exposición sin comprometer la calidad del análisis.

- FTK Imager
- Registry Explorer/ MFTExplorer
- MFTECmd
- Anaconda / Impacket
- Hashcat
- John The Ripper
- Autopsy

Tras registrarme en el sitio ctf.sancastell.me, se habilitó la opción para descargar la máquina a analizar [Win10_PC001.mvdk], en la cual encontré una serie de desafíos que debía resolver. A continuación, se detallan los retos, junto con las capturas de pantalla y el flag correspondiente de cada uno. Es importante destacar que, en muchos casos, es posible obtener el resultado utilizando diferentes herramientas y, en algunas ocasiones, en distintas ubicaciones dentro de la imagen de la máquina virtual. Como primer dato, se presenta la información general de la máquina Windows 10 que se va a analizar.



Hash del fichero

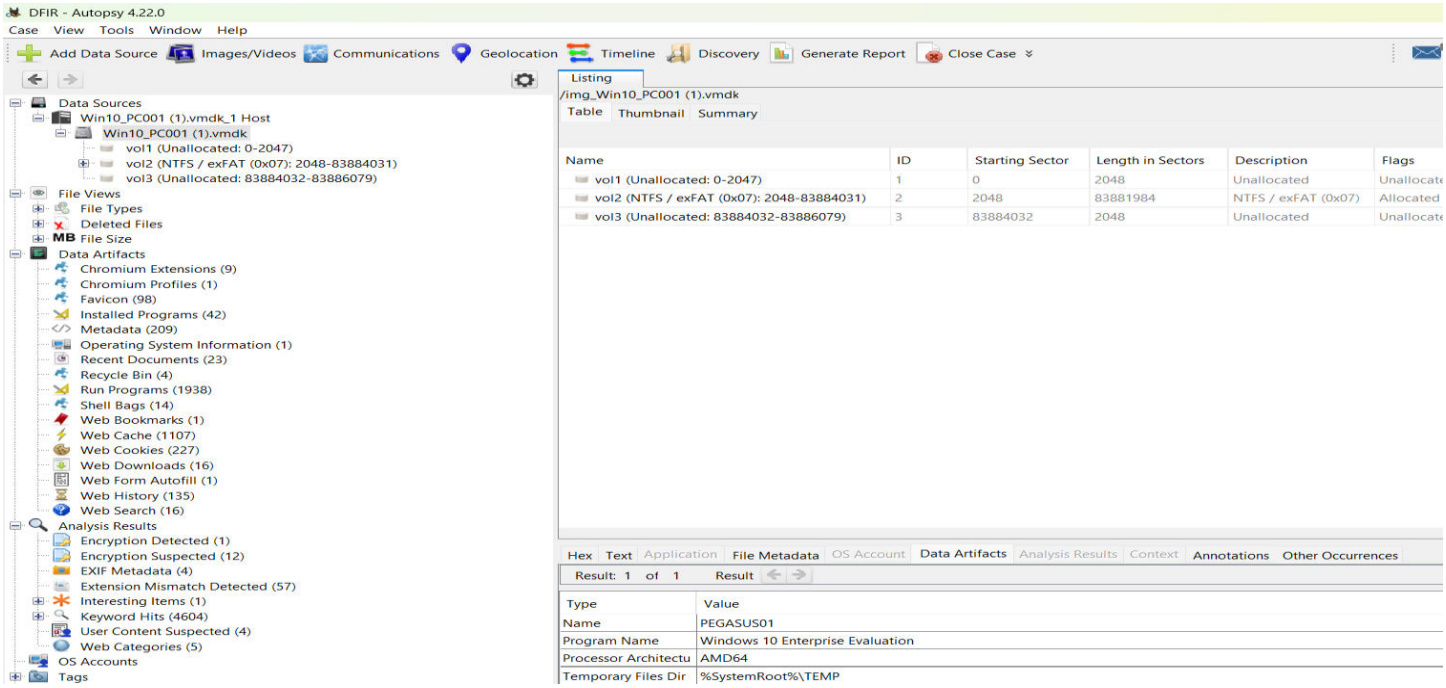
Como analista de la máquina, lo primero que realicé fue obtener el hash sha-256 de la evidencia. Este paso fue crucial y debía ejecutarse inmediatamente después de descargar la imagen, ya que, de no hacerlo, el hash sha-256 cambiaría, lo que dificultaría la obtención del mismo resultado y obligaría a descargar nuevamente la imagen de la máquina.

```
PS C:\Users\rabri> Get-FileHash -Path "C:\Users\rabri\Downloads\Win10_PC001.vmdk" -Algorithm SHA256

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          4446E9C42345A32FA78A8CE20834FAA047A3B161EBA986F894D2230FCF6B0CBE       C:\Users\rabri\Downloads\Win1...
```

4446E9C42345A32FA78A8CE20834FAA047A3B161EBA986F894D2230FCF6B0CBE

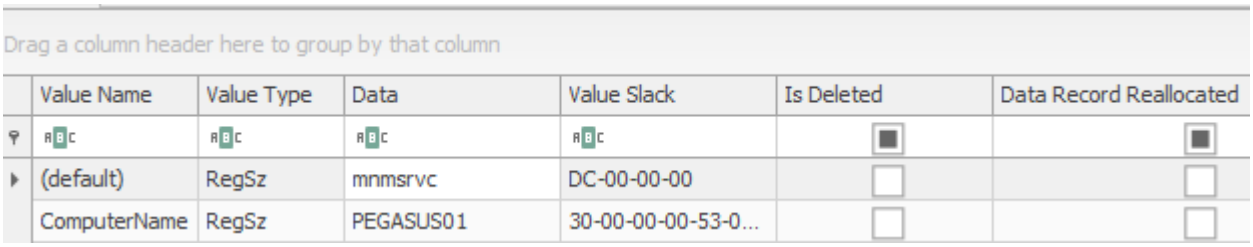
Nombre de la máquina

A continuación, se describen los pasos que seguí para obtener el nombre de la máquina en la que realicé el análisis. Se presenta una variante utilizando la herramienta Autopsy, donde el nombre aparece en la parte inferior derecha del siguiente screenshot:



Una segunda variante consistió en utilizar la herramienta Registry Explorer en modo “run as administrator” para obtener acceso al subdirectorio SYSTEM. En Registry Explorer, seleccioné la opción "Load Hive" y elegí el archivo:

D:\Windows\System32\config\SYSTEM
Siguiendo la siguiente ruta fui directo al nombre del archivo que es la columna **Data**
SYSTEM
└── CurrentControlSet
  └── Control
    └── ComputerName
      └── ComputerName

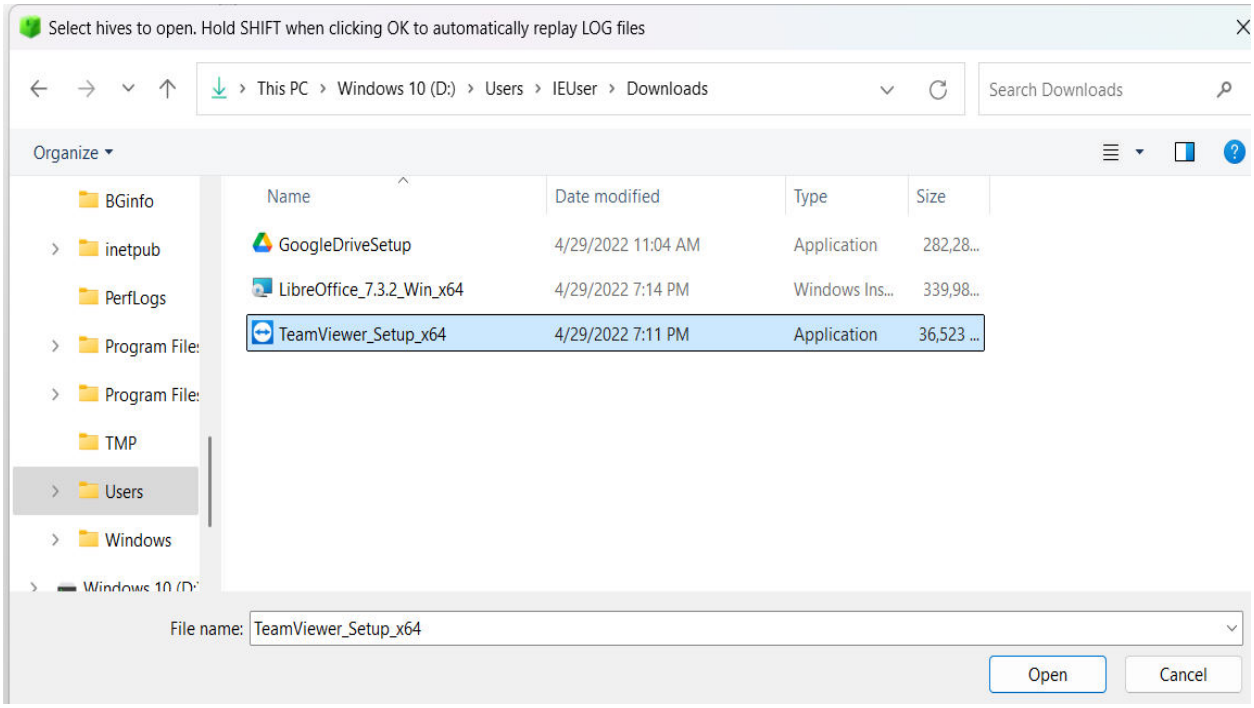


Nombre de la maquina: **PEGASUS01**

Descarga fichero de control remoto

Antes de buscar este archivo, realicé una investigación exhaustiva de todos los ficheros maliciosos, incluidos aquellos que, aunque aparentemente inofensivos, estaban ubicados en lugares muy sospechosos. Fue este archivo en particular el que me llamó la atención. Se me pidió localizar el nombre del archivo .exe de un programa de control remoto que el usuario descargó en la carpeta. A continuación, se muestra la ruta y el screenshot correspondiente, tal como aparece en el siguiente screenshot utilizando la herramienta Registry Explorer.

D:/Users//IEUser/Downloads/



Nombre del Archivo: **TeamViewer_Setup_x64**

Fecha descarga software control remoto

Al verificar la información mostrada anteriormente, podemos observar la fecha en que el usuario descargó el ejecutable de control remoto "TeamViewer_Setup_x64.exe".

Formato de fecha: aaaa-mm-dd (EX: 2020-12-01) → **2022-04-29**

Ficheros maliciosos

En la máquina se han encontrado varios ficheros maliciosos.

Claro, la oración corregida sería:

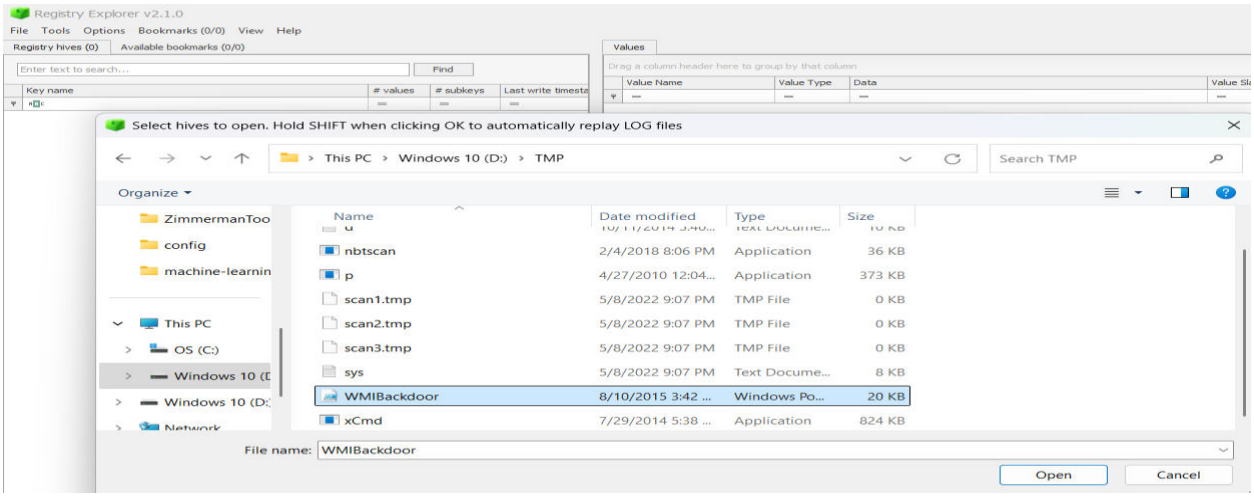
¿En qué carpeta (solo el nombre de la carpeta) se encuentran esos archivos?

Nombre de la carpeta: **TEMP**

A continuación, presento un resumen breve de las acciones realizadas para obtener la respuesta anterior y algo más. Utilizando la herramienta Registry Explorer y con el hive cargado, opté por buscar programas con nombres sospechosos o ubicados en carpetas inusuales, tales como:

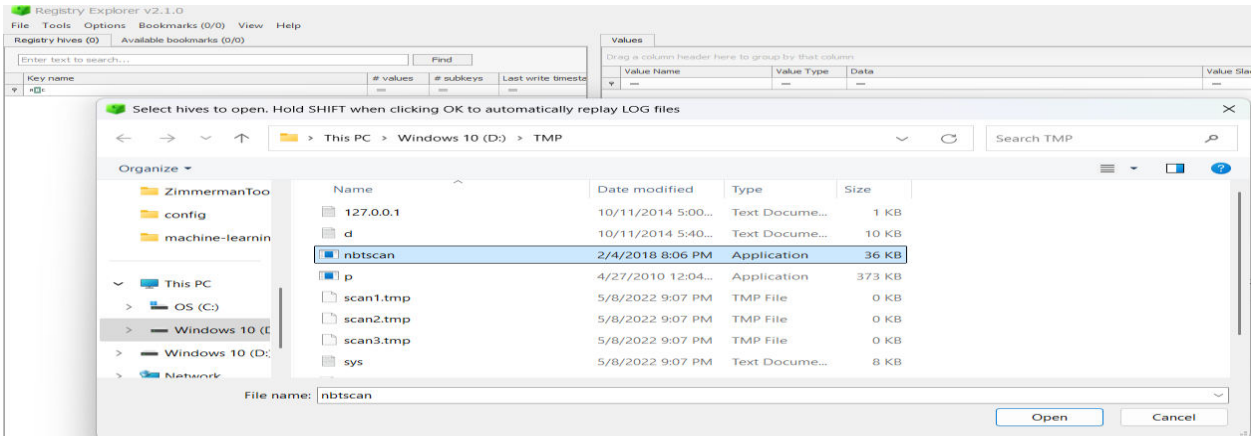
D:\Users\Public\
D:\Windows\Temp\
D:\Users\Usuario\AppData\

Uno de los hallazgos localizados en d:\TMP



El archivo wbmibackdoor Windows PowerShell Script (.ps1) de 20 KB es sumamente sospechoso. Un script de PowerShell (.ps1) llamado wbmibackdoor.ps1 ubicado en la carpeta TMP es una clara señal de actividad maliciosa. El nombre "backdoor" indica que podría tratarse de un script diseñado para acceso remoto o persistencia en el sistema.
¿Qué implica este hallazgo? PowerShell es una herramienta frecuentemente empleada por atacantes, ya que permite ejecutar comandos sin dejar rastros detectables en disco. El nombre "wbmibackdoor" sugiere el uso de WMI (Windows Management Instrumentation), lo que podría señalar un método de persistencia o ejecución remota. El tamaño de 20 KB indica que el archivo contiene un código extenso, probablemente para ejecutar comandos en segundo plano.

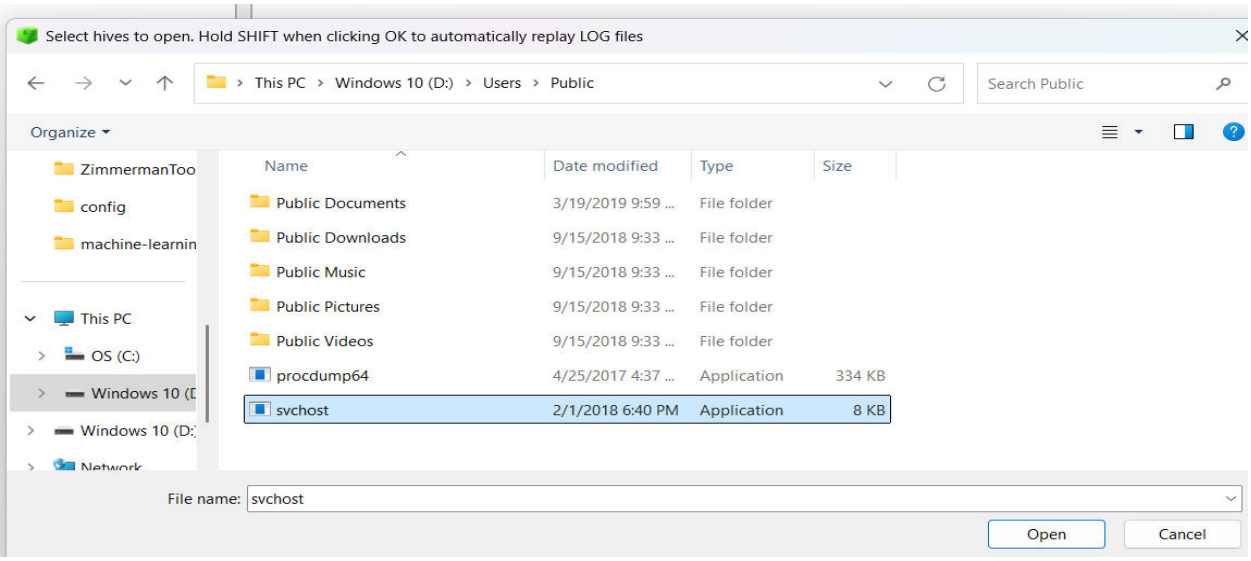
Otro archivo peligroso en D:\TMP\



¡NTBSCAN en D:\TMP\ es claramente malicioso! Mi antivirus lo detectó por casualidad, lo que confirma que este archivo es sospechoso. El nombre "NTBSCAN" sugiere que podría ser un escáner de red, posiblemente utilizado por un atacante para mapear dispositivos en la red y encontrar vulnerabilidades.

¿Por qué es peligroso? “NTBSCAN” tiene un nombre similar a herramientas como NBTScan, que se usan para escanear redes NetBIOS (nombre de equipos en una red Windows). El archivo se encuentra en **D:\TMP**, una carpeta temporal donde los atacantes suelen dejar el malware antes de ejecutarlo o eliminarlo. El antivirus lo marcó como malware, lo que indica que probablemente tiene una firma reconocida de una herramienta maliciosa. El nombre "very funny" parece un intento de engañar al usuario, una táctica común utilizada por el malware.

Otro posible archivo malicioso [svchost].

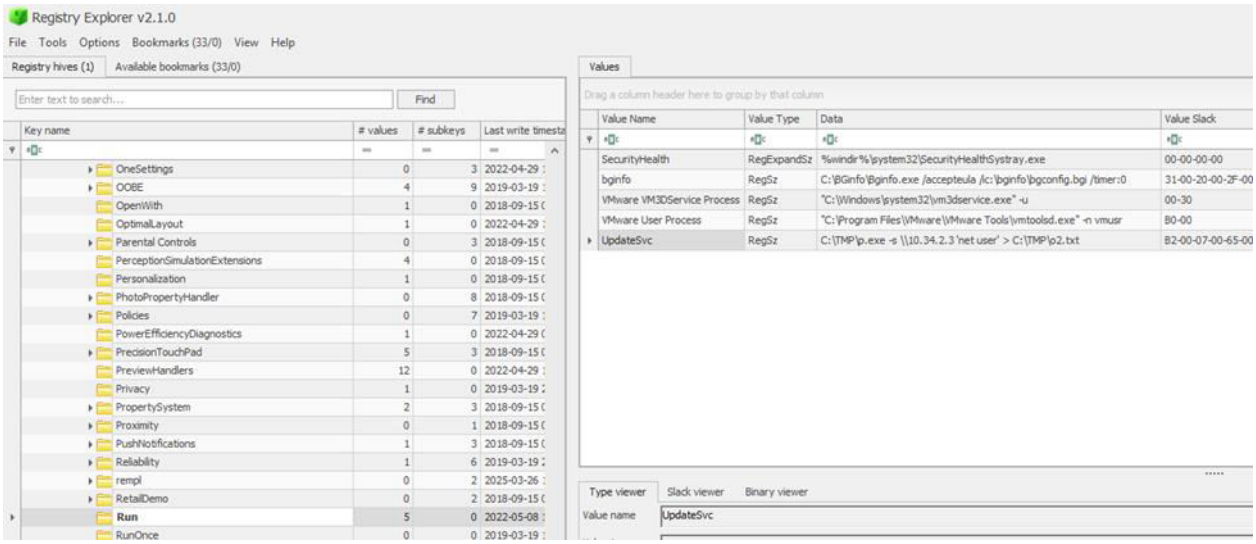


El archivo svhost.exe en *D:\Users\Public* es altamente sospechoso. El archivo legítimo del sistema se llama svchost.exe y siempre se encuentra en la siguiente ubicación:

C:\Windows\System32\svchost.exe.

Este tipo de archivo, ubicado en una carpeta de acceso público, es típicamente donde los atacantes dejan malware para facilitar su ejecución. Además, el tamaño de 8 KB sugiere que podría ser un dropper.

Otro posible archivo malicioso [UpdateSvc]



Análisis de la clave sospechosa:
C:\TMP\p.exe -s \\10.34.2.3 'net user' > C:\TMP\o2.txt
Razones por las que es sospechoso:

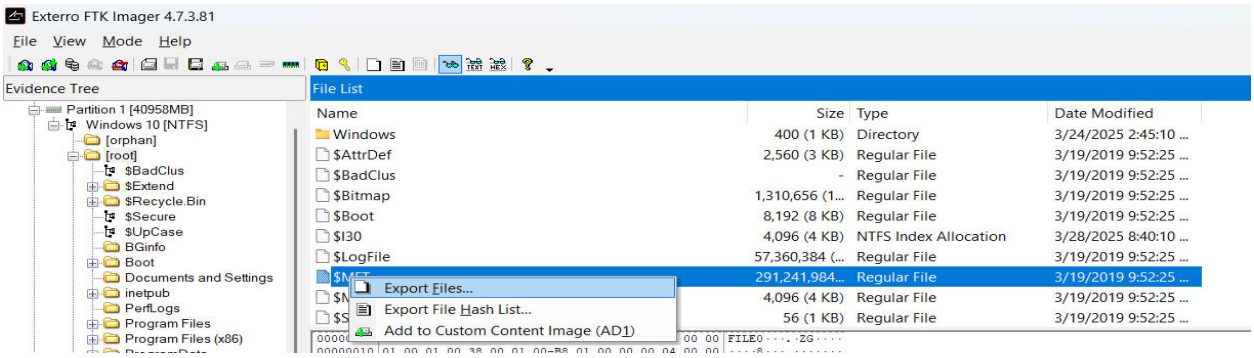
1. Ejecutable en una carpeta sospechosa (C:\TMP\p.exe):
   - C:\TMP\ no es una ubicación estándar para archivos de sistema.
   - Un archivo ejecutable (p.exe) en esta carpeta es sospechoso.

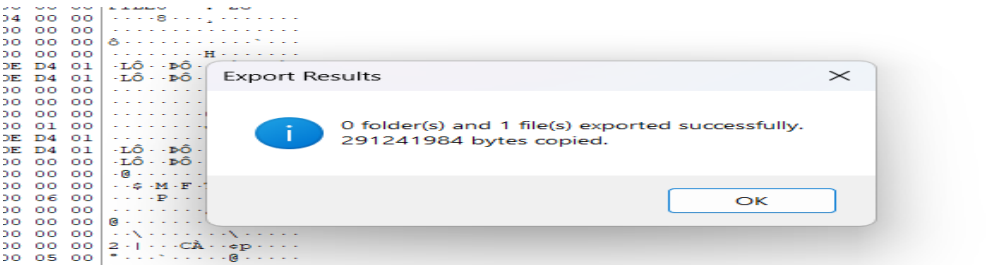
2. Uso de un comando remoto (-s \\10.34.2.3 'net user'):
   - Se está ejecutando p.exe con parámetros que incluyen -s, lo que sugiere una acción automatizada o remota.
   - \\10.34.2.3 indica una posible conexión a otra máquina en la red.
3. Comando 'net user' redirigido a un archivo (> C:\TMP\o2.txt):

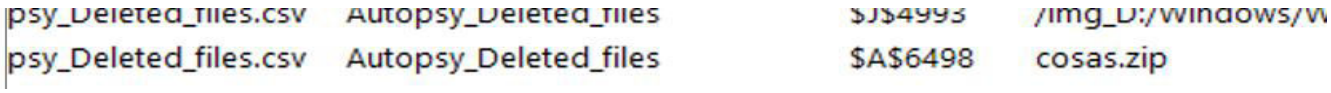
- net user se usa para listar cuentas de usuario en el sistema.
- La salida del comando se guarda en o2.txt, lo que puede indicar recolección de credenciales o información del sistema.

Ficheros eliminados

Se sospecha que existió un archivo .zip eliminado. Logré encontrar el nombre de este archivo por dos métodos diferentes: directamente en **Autopsy** y exportando el archivo **$MFT** utilizando **FTKImager** y la herramienta **MFTECmd** de Eric Zimmerman para abrirlo en Microsoft Excel y realizar la búsqueda de archivos .zip. Su nombre peculiar fue la pista que me llevó a decidir que este debía ser el **Flag** de este reto de CTF.



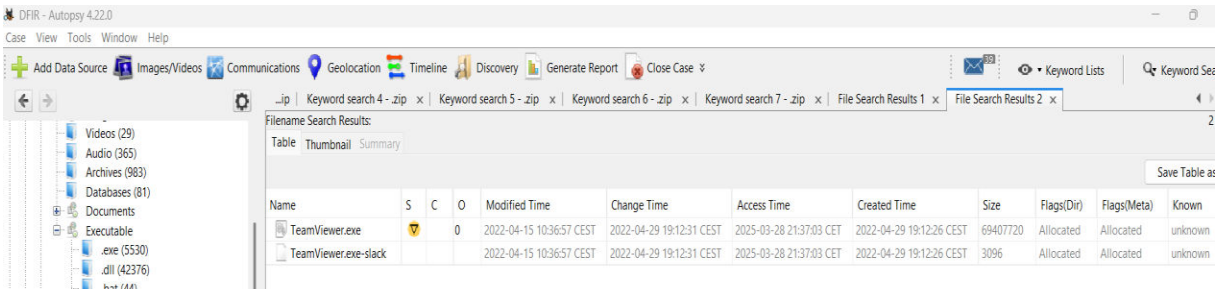




Fecha de ejecución programa de control remoto

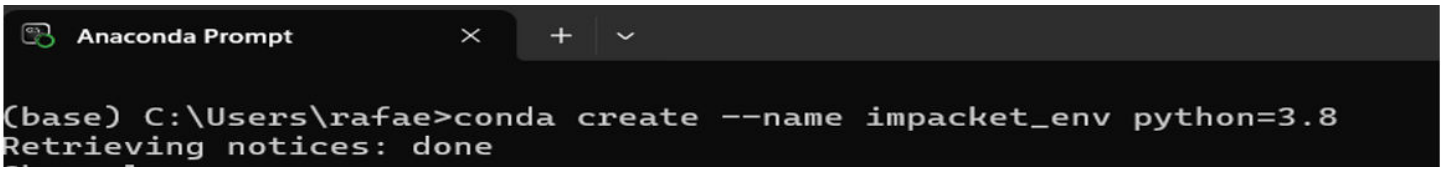
Sabemos que se ha ejecutado el programa Team Viewer en el equipo, ¿podrían indicar la fecha en la que se ejecutó? Formato: dd/mm/yyyy

Fecha: **29/04/2022** Change time [Aparece en el siguiente Screenshot]

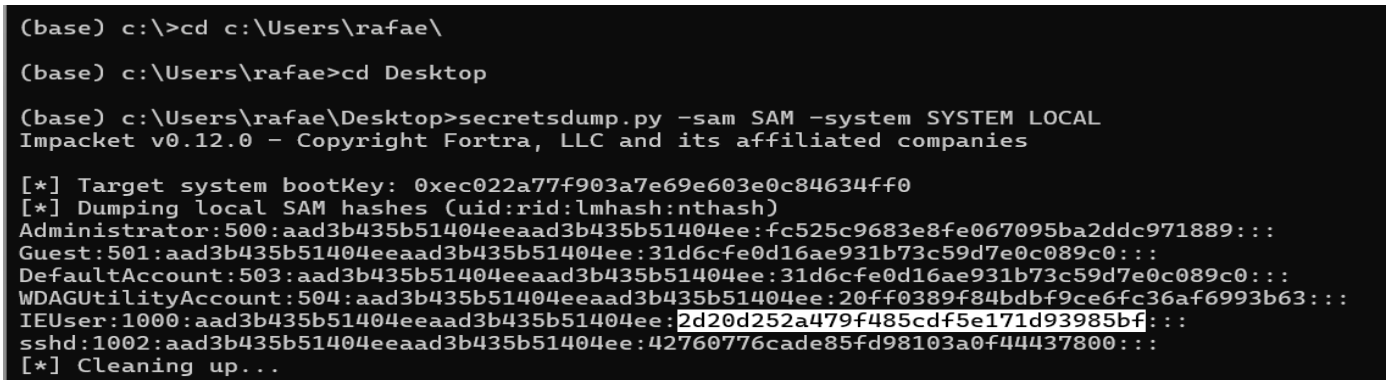


Contraseñas débiles

Existen sospechas de que la contraseña del usuario **IEUser** es débil, lo que permitió al atacante acceder a ella. Intenté utilizar la herramienta **Mimikatz** para obtener esta contraseña, pero decidí usar mi host para esta práctica y me resultó demasiado laborioso instalar Mimikatz debido a los múltiples antivirus que tengo en mi host. Por lo tanto, decidí posponer la instalación para otro momento. En su lugar, opté por seguir otro enfoque, y a continuación detallo cada uno de los pasos que seguí.
El primer paso fue crear un entorno dentro de **Anaconda** para **Impacket**.



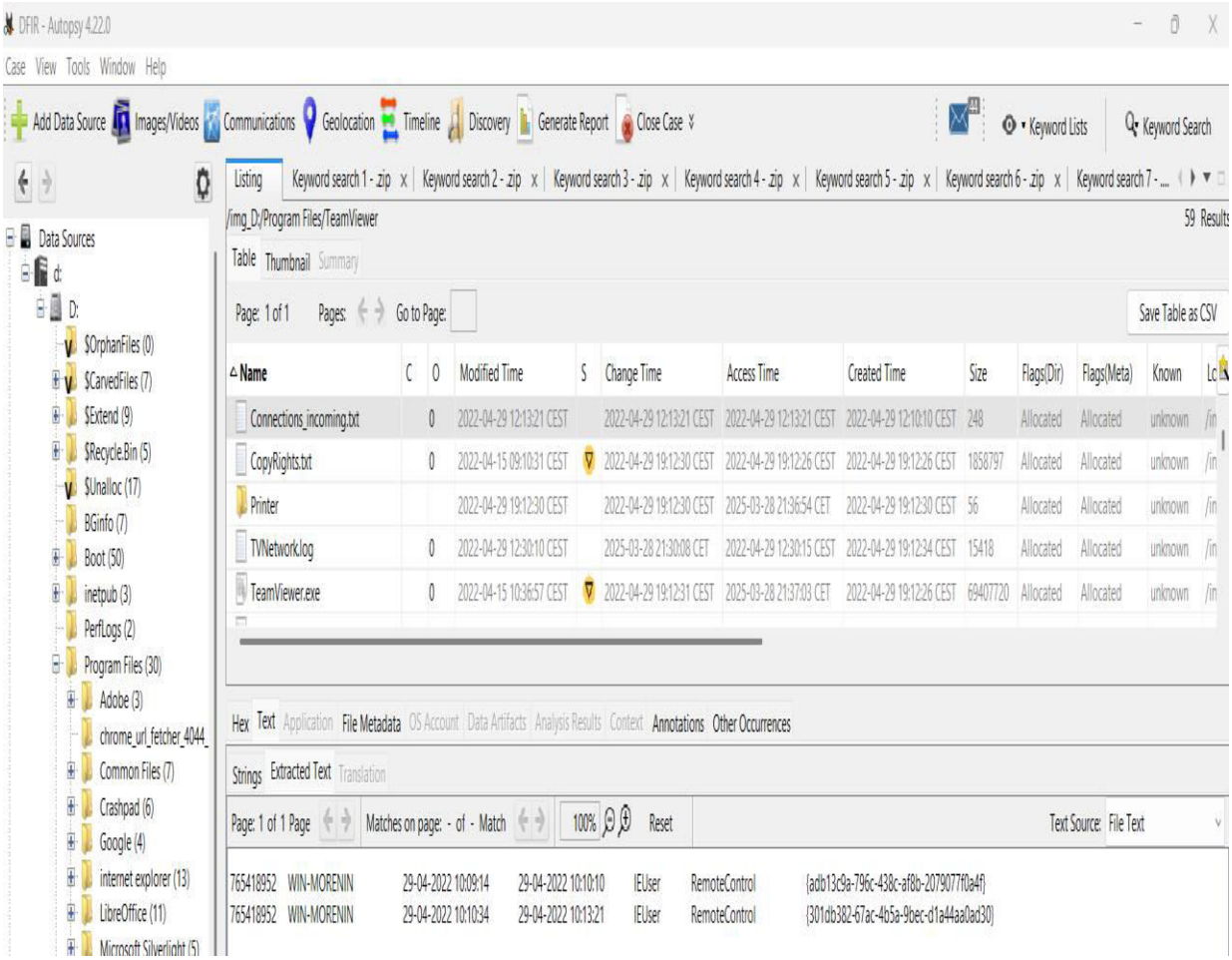
Utilizando el comando secretsdump.py, como se muestra a continuación, obtuve los hashes y seleccioné el necesario para la ejecución con John The Ripper. El hash que aparece resaltado a continuación es el relacionado con la contraseña que quería recuperar.



En el siguiente screenshot aparece la contraseña que buscaba: **qwerty**.

Conexión programa control remoto

Existe la sospecha de que el atacante se haya conectado al equipo mediante un programa de control remoto. ¿Podrían decir cuál es el ID desde el que se conecta el atacante? Para localizar este ID, utilicé Autopsy, y el screenshot donde aparece este ID se muestra a continuación. ID = 765418952



Conexión RDP

Se ha detectado actividad sospechosa en la red. ¿Podrían indicarme la IP desde la que se ha conectado a la máquina por RDP?

Después de encontrar que un equipo se había conectado mediante un programa de control remoto y de localizar el ID desde el que el atacante se conectó, también pude obtener la fecha y la hora exacta de estas dos conexiones. En la misma página de información proporcionada por **Autopsy**, rastreé el momento exacto con una precisión de aproximadamente dos minutos entre ambos eventos.

La IP utilizada fue: 192.168.183.134.
5302,5302,2022-04-29 10:08:16.2309769,4648,LogAlways,Microsoft-Windows-Security-Auditing,Security,640,4384,PEGASUS01,66,A logon was attempted using explicit credentials,PEGASUS01\IEUser,192.168.183.134:445,Target: PEGASUS01\user1.

A continuación, detallo los pasos realizados para obtener la IP. Utilicé la herramienta de Zimmerman EvtxECmd.

```
C:\Users\rafae\Downloads\EvtxECmd\EvtxeCmd>.\EvtxECmd.exe -f "C:\Users\rafae\Documents\Security.evtx" --csv "C:\Users\ra
fae\Documents\evtx_output" --csvf salida_seguridad.csv --inc 4624,4648,4672
EvtxECmd version 1.5.2.0

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


```
C:\Users\rafae\Downloads\EvtxECmd\EvtxeCmd>.\EvtxECmd.exe -f "C:\Users\rafae\Documents\Security.evtx" --csv "C:\Users\ra
fae\Documents\evtx_output" --csvf salida_seguridad.csv --inc 4624,4648,4672
EvtxECmd version 1.5.2.0
```

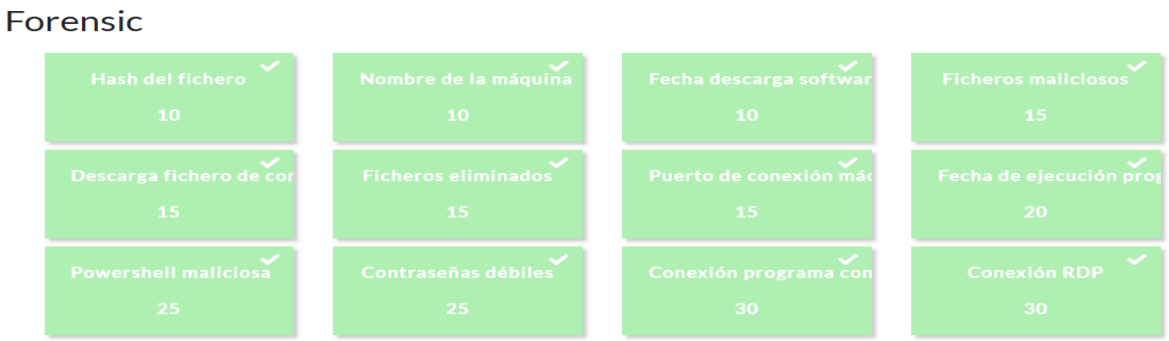

```
CSV output will be saved to C:\Users\rafae\Documents\evtx_output\salida_seguridad.csv

Maps loaded: 453
```

Una vez descargada la información en Microsoft Excel procedí a su búsqueda teniendo en cuenta que este evento estaba relacionado con ,PEGASUS01\IEUser, la fecha 2022-04-29 10:08:16 que aparece vinculada a los eventos donde obtuve el ID de este acceso remoto.

Puerto de conexión máquina atacante

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

El puerto de conexión de es el **445** que aparece en la información descargada en el archivo salida_seguridad.csv y copia de esto aparece mostrada anteriormente.

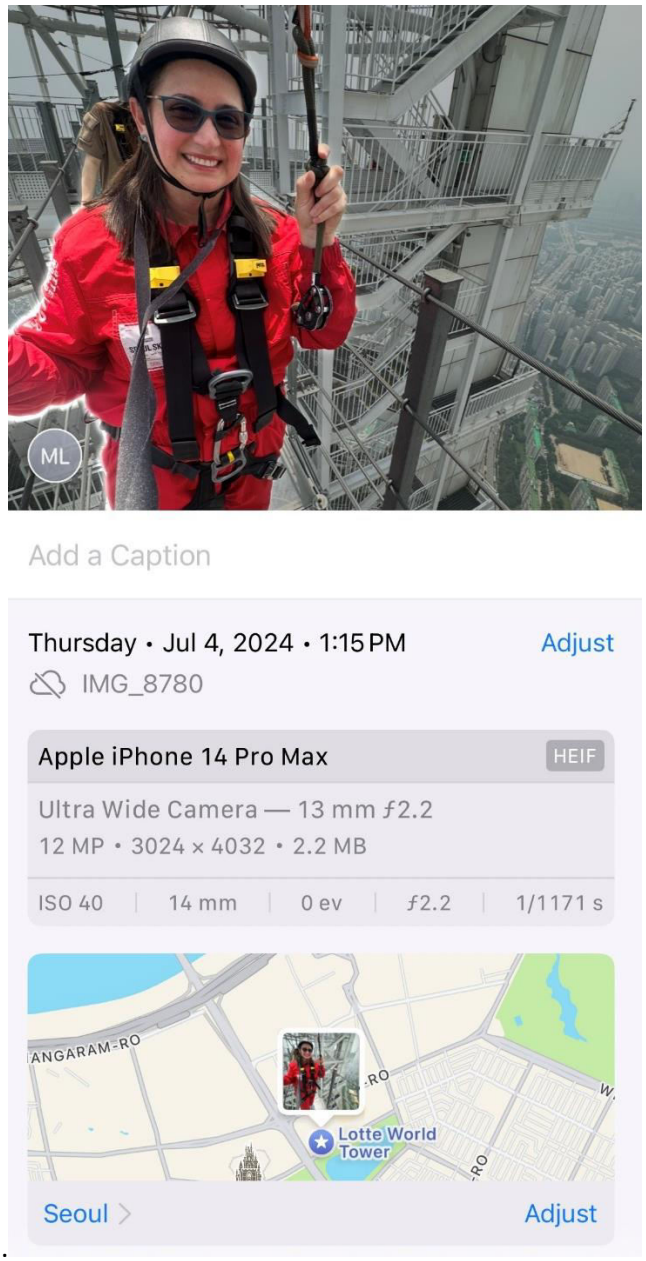


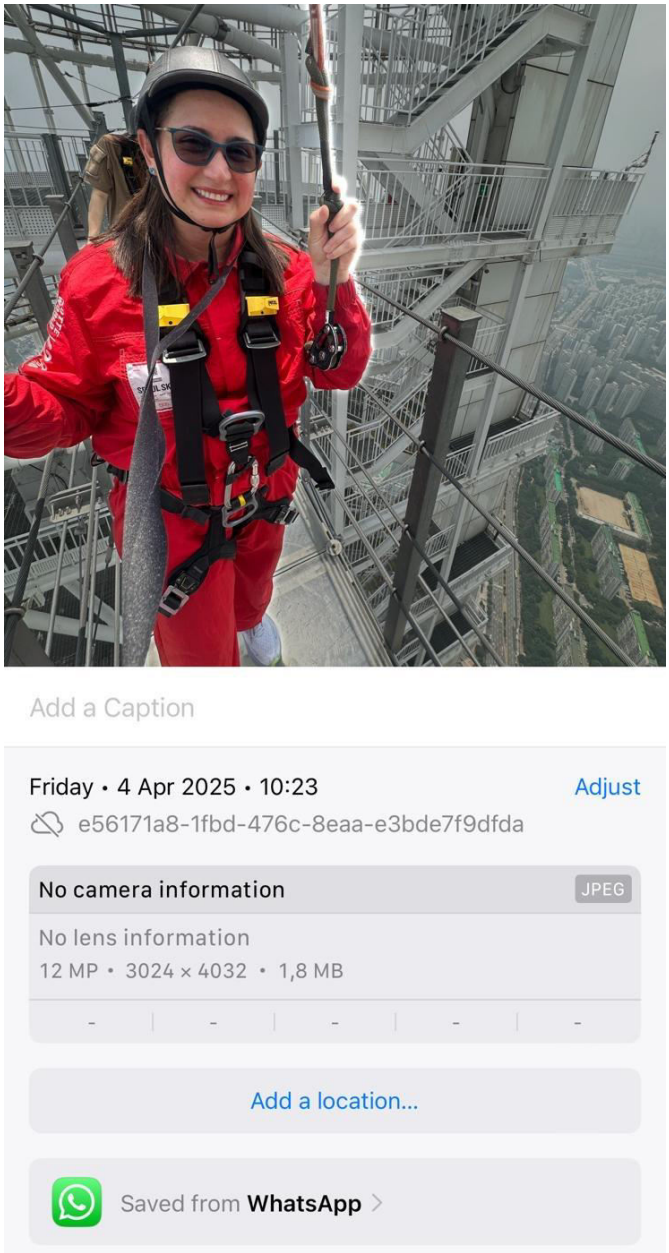
METADATOS DE FOTO ENVIADA POR EMAIL Y APLICACIONES DE MENSAJERIA INSTANTANEA

Foto original

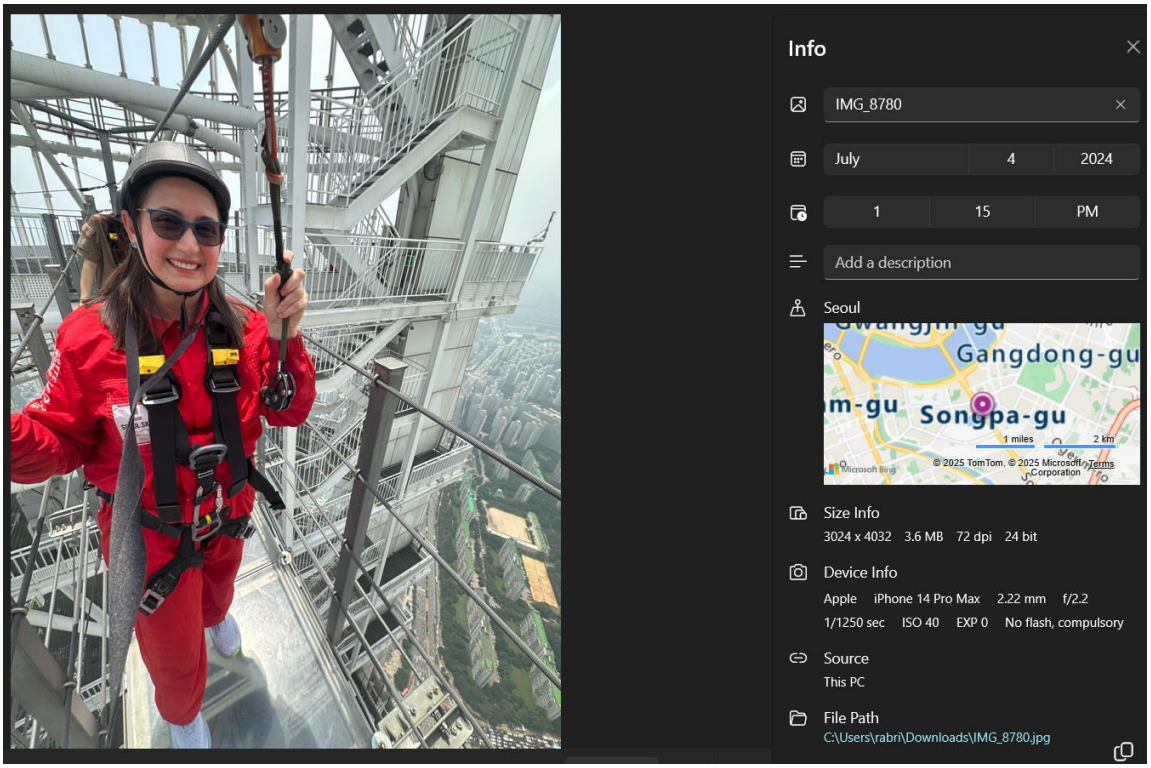
(Fun fact: En Seúl, Corea del Sur a 555 metros de altura en el puente Sky Bridge de la Torre Lotte World)

A la izquierda: Foto original con todos los metadatos
A la derecha: La misma foto enviada por WhatsApp con muy poca información de metadatos originales: información del tamaño original de la foto, pero comprimida y sin información sobre la locación, cambia el formato de la imagen.

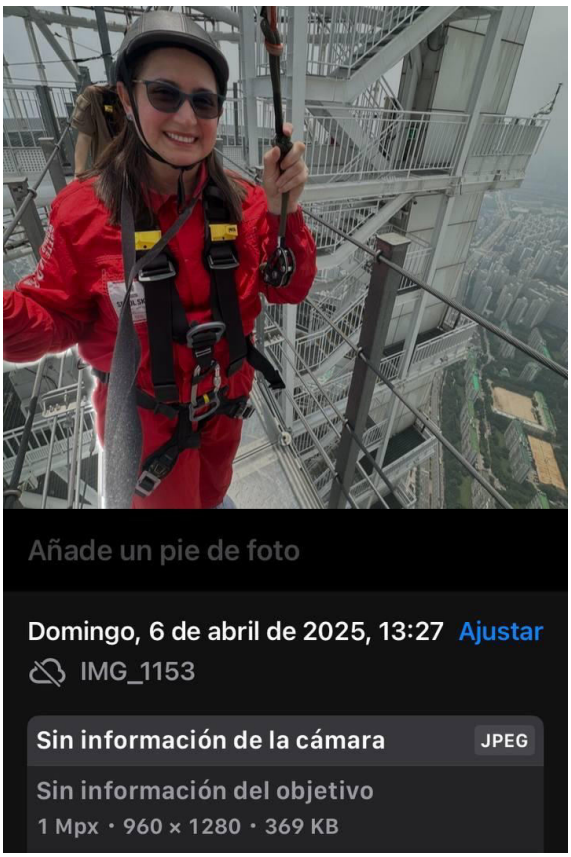




La misma foto enviada por correo electrónico retiene algunos metadatos como el tamaño, el lugar, la fecha, hora, pero no todos, por ejemplo, el dispositivo usado, lente, etc.



La misma foto enviada por Telegram, como se puede observar, acabó con la calidad de la foto y al parecer borró los metadatos.



Conclusiones

El enfoque adoptado fue práctico y orientado a la resolución de desafíos mediante la aplicación de técnicas reales de investigación digital. Cada reto requirió identificar y extraer evidencia concreta desde distintos artefactos del sistema como archivos del sistema, entradas del registro, logs de eventos, metadatos y capturas de red, aplicando principios fundamentales de preservación de evidencia, análisis y documentación.

Esta experiencia permitió afianzar conocimientos en investigación de incidentes y análisis forense digital, con una visión integral de los procesos involucrados en un entorno Windows, desde la recolección inicial de evidencias hasta la resolución de cada reto planteado.

Fin del Informe de DFIR