Confidential Security

DFIR

Confidencial

Nombre del auditor: Kacper Mariusz Koper Mielczarek

Fecha: 06/04/2025

Índice

Introducción

En este proyecto vamos a realizar un análisis Forensic a una base de datos externa. Lo que se va a realizar es primero la importación de la base de datos a nuestro equipo, después realizaremos la copia de seguridad correspondiente y, por último, vamos a utilizar una serie de herramientas para contestar todas las preguntas del challenges http://ctf.sancastell.me/challenges.

En última estancia se realizará una breve conclusión de los resultados del análisis forense.

1. Hash del fichero

Para averiguar el hash de la evidencia usaremos un comando en la terminal de PowerShell en Windows:

Get-FileHash "C:\Users\PC\Desktop\Win10_PC001.vmdk" -Algorithm SHA256

Este comando nos ha proporcionado el siguiente hash SHA256 del archivo Win10_PC001.vmdk.

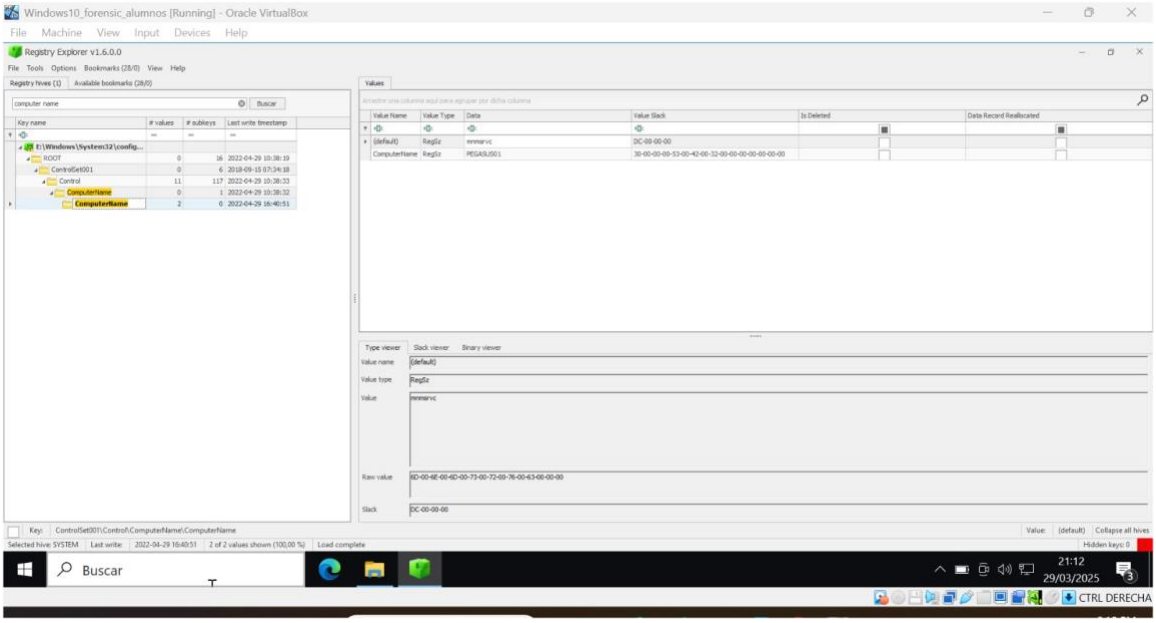
4446E9C42345A32FA78A8CE20834FAA047A3B161EBA986F894D2230FCF6B0CBE

Lo importante de esta parte ha sido calcular el hash justo después de descargar la imagen, ya que si la tocabas el hash se modificaba.

2. Nombre de la máquina

Para conseguir el nombre de la máquina debemos utilizar la herramienta **Registry Explorer**.

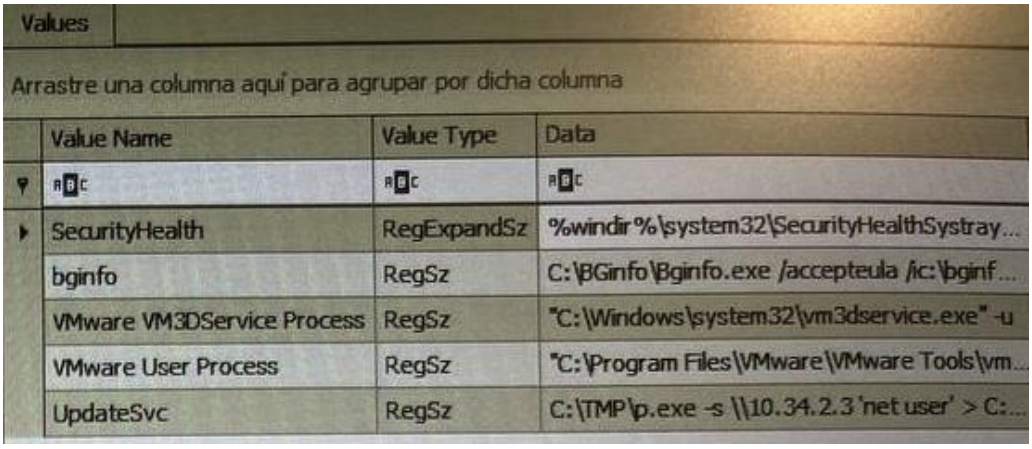
El nombre de la máquina es **PEGASUS01**.



3. Ficheros maliciosos (Malware del atacante)

Para buscar una carpeta que contenga archivos maliciosos volveremos a acudir a la herramienta **Registry Explorer** y nos pondremos a buscar por los diferentes directorios. Al mirar en la carpeta RUN, nos podremos encontrar con un ejecutable sospechoso.

La carpeta del malware es **TMP**.



Values

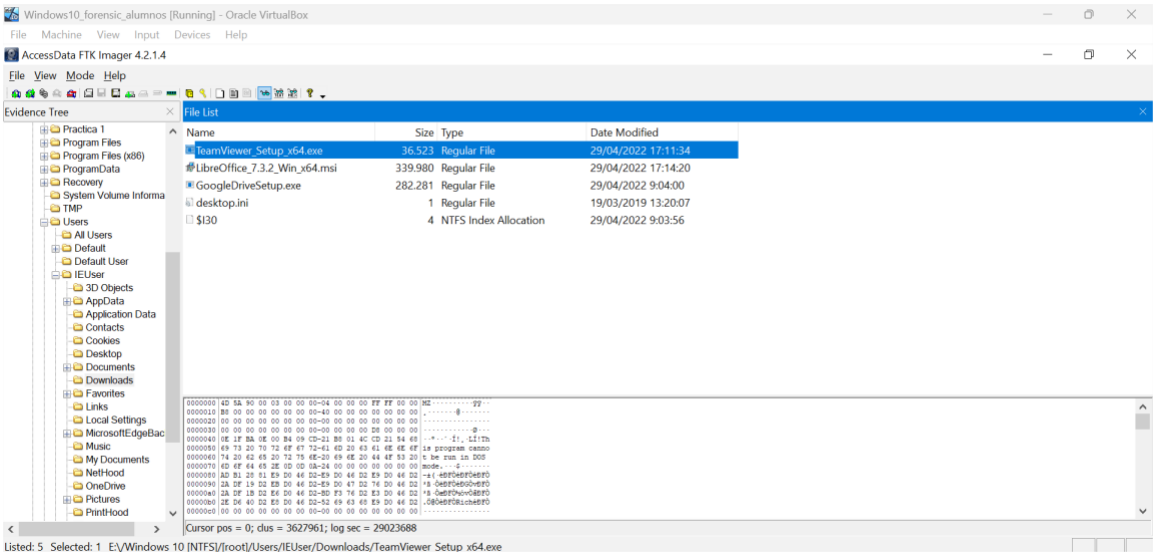
Arrastre una columna aquí para agrupar por dicha columna

Value Name	Value Type	Data
SecurityHealth	RegExpandSz	%windir%\system32\SecurityHealthSystray...
bginfo	RegSz	C:\BGinfo\Bginfo.exe /accepteula /ic:\bginf...
VMware VM3DService Process	RegSz	"C:\Windows\system32\vm3dservice.exe" -u
VMware User Process	RegSz	"C:\Program Files\VMware\VMware Tools\vm...
UpdateSvc	RegSz	C:\TMP\p.exe -s \\10.34.2.3 'net user' > C:...

4. Descarga de fichero de control remoto

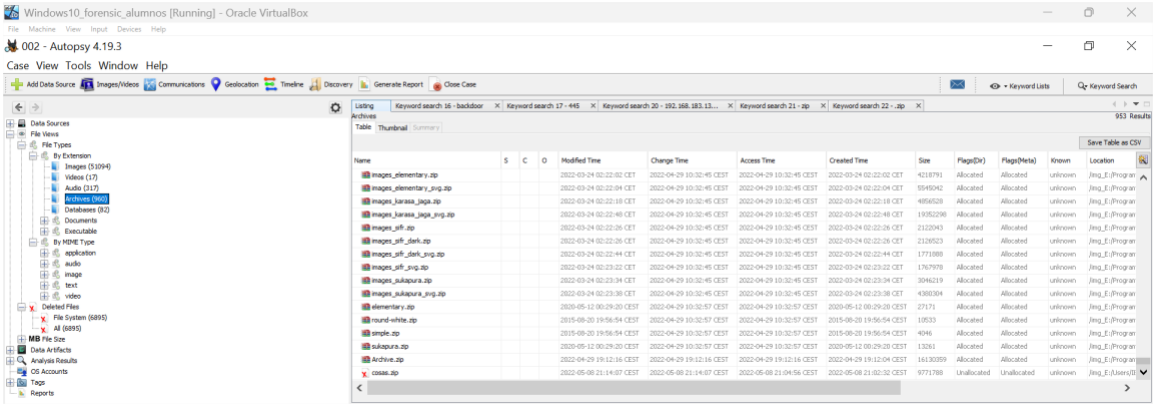
El fichero descargado por el usuario para obtener el control remoto es TeamViewer_Setup_x64.exe.

Lo hemos conseguido gracias a la herramienta **Access Data FTK Imager**.



5. Ficheros eliminados

El fichero que se ha eliminado fue cosas.zip, y fue encontrado gracias a la herramienta de **Autopsy**.



6. Contraseña débil

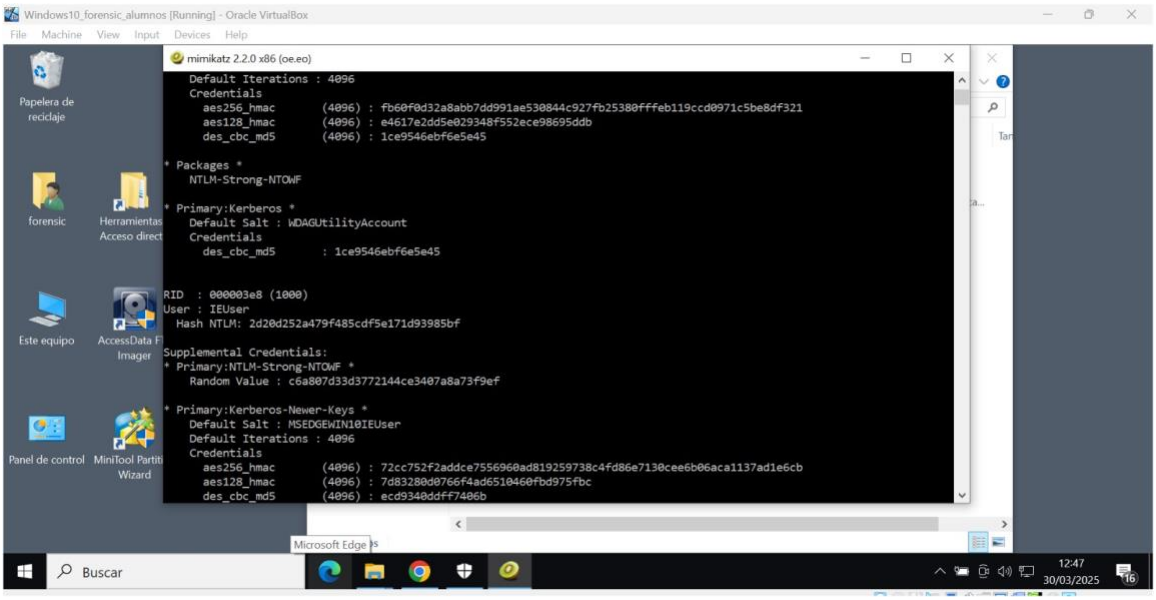
Para conocer la contraseña del usuario IEUser vamos a utilizar la herramienta de **mimikatz.** Con ello podremos sonsacar todos los usuarios de la base de datos con sus correspondientes contraseñas en hash. Cuando obtengamos dicho hash, debemos crackearlo. Por lo tanto, utilizaremos la página web crackstation.net.

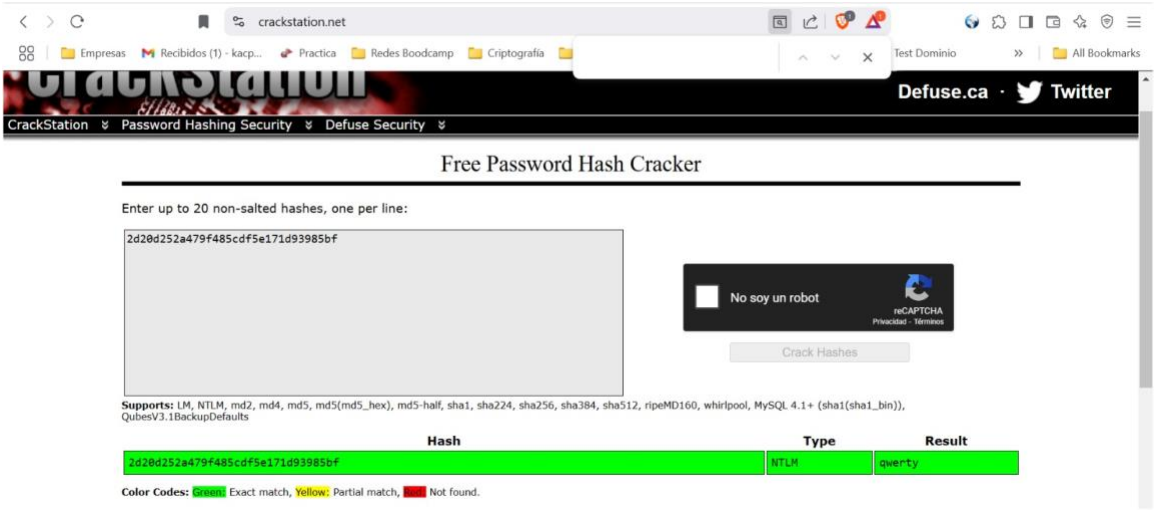
La contraseña que sale es: qwerty

Todo esto es posible porque el hash es un md5, que se considera un hash vulnerable por colisiones.

Para ello debemos utilizar el comando:

lsadump::sam /system:E:\Windows\System32\config\SYSTEM /sam:E:\Windows\System32\config\SAM

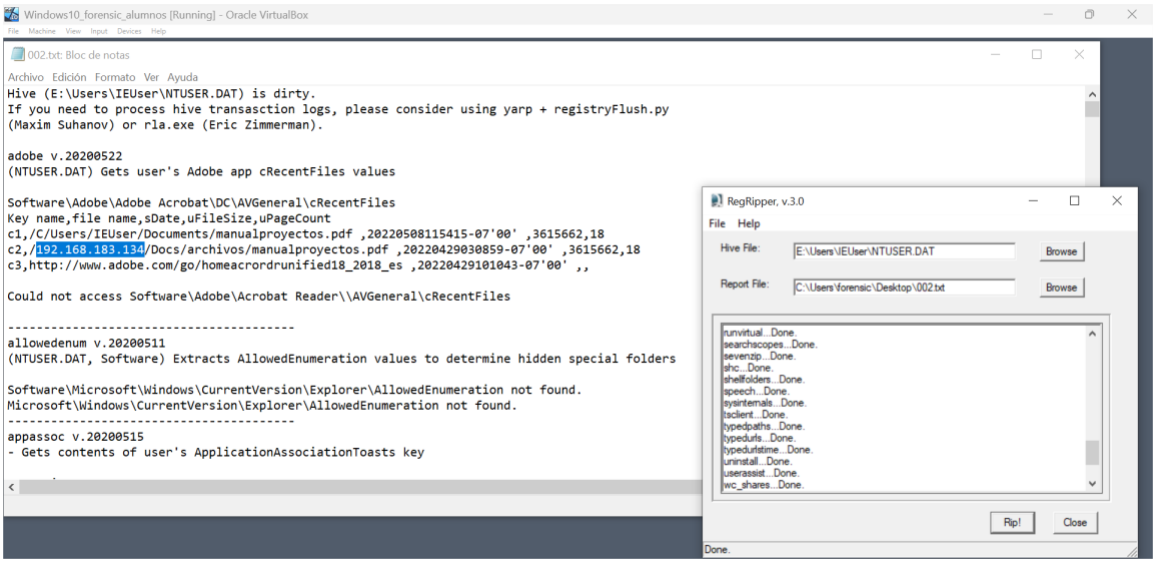




7. Conexión RDP

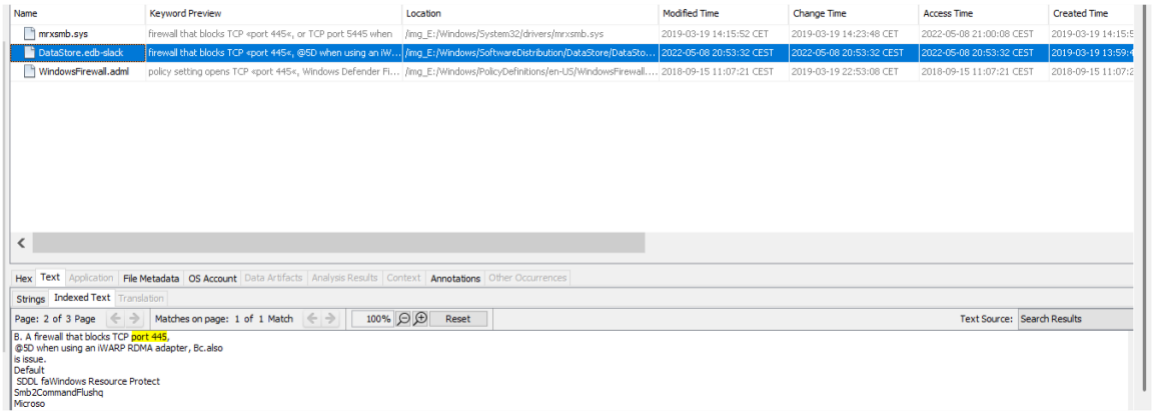
Hemos podido averiguar que la IP sospechosa que se ha detectado es 192.168.183.134, que es la IP desde la que se ha conectado el sospechoso.

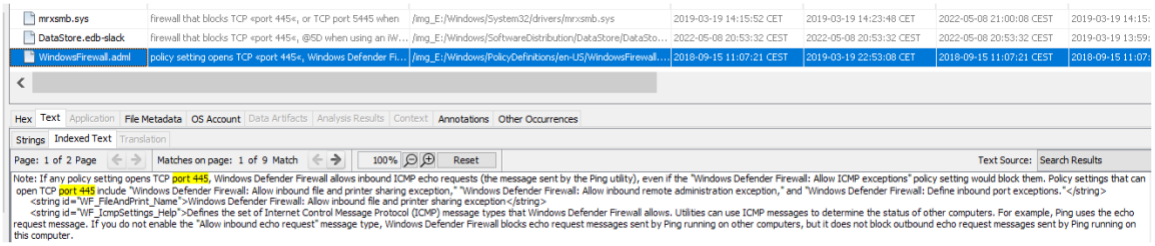
Esto lo hemos descubierto gracias a la herramienta **RegRipper**.



8. Puerto de conexión máquina atacante

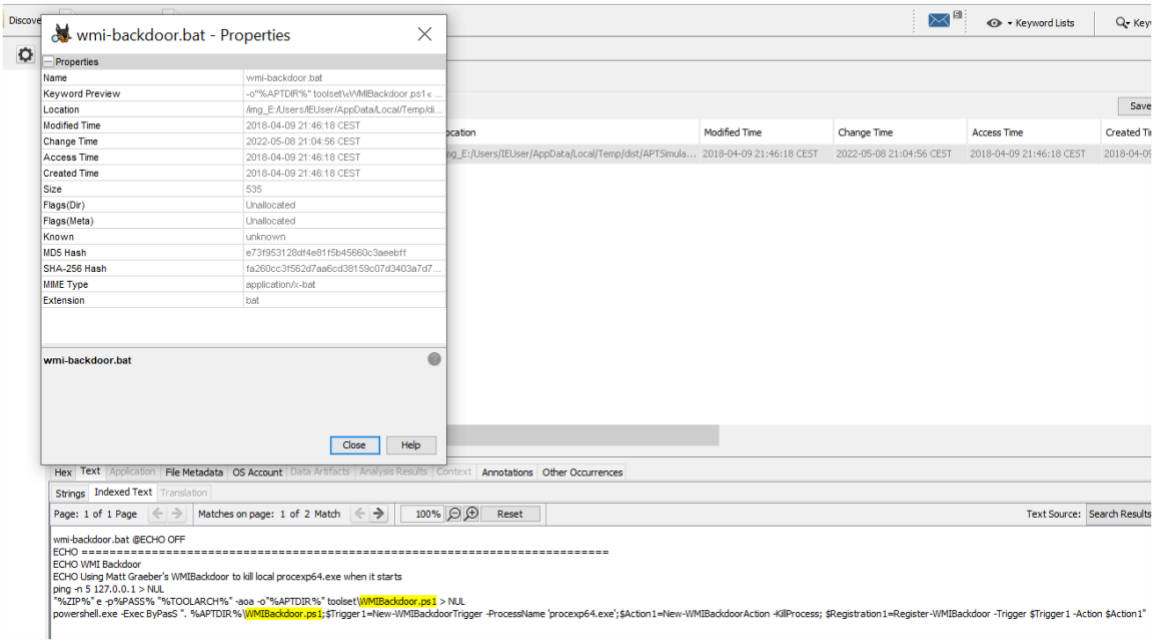
El puerto de conexión de la máquina atacante fue el puerto 445.





9. Powershell maliciosa

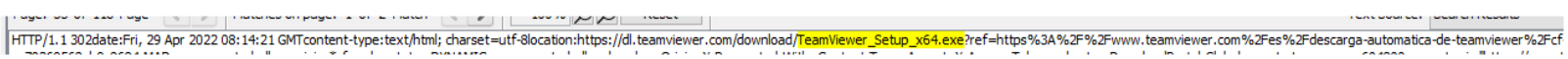
El script de la powershell es WMIBackdoor.ps1.



10. Fecha descarga software control remote

El software de control remoto fue descargado en la fecha 2022-04-29.

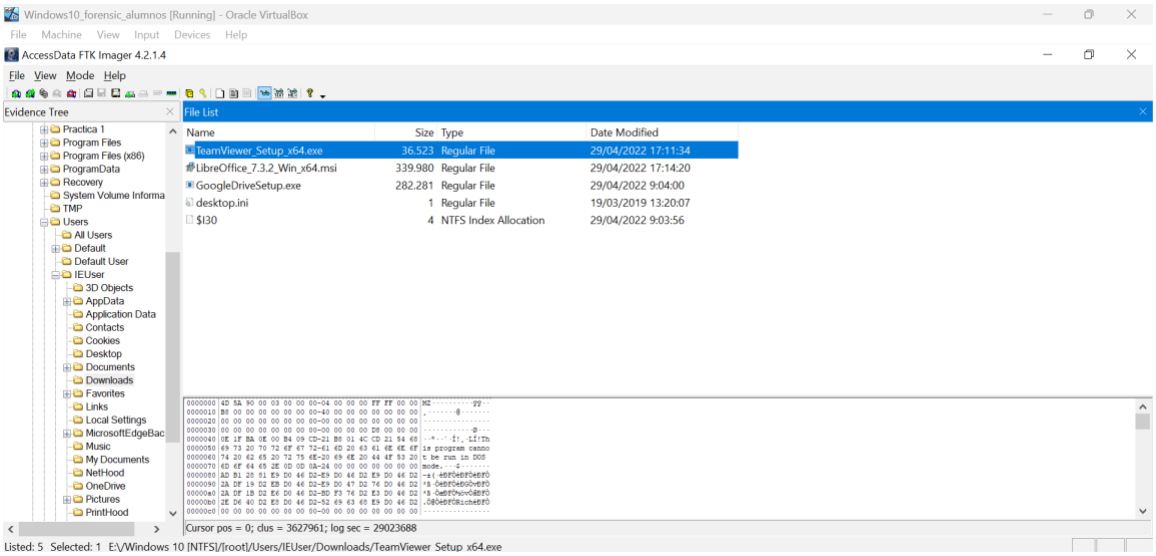
Esto lo sabemos porque realizamos una búsqueda exhaustiva con la herramienta **Autopsy**.



11. Fecha de ejecución programa de control remoto

La fecha de ejecución del programa de control remoto es el 29/04/2022.

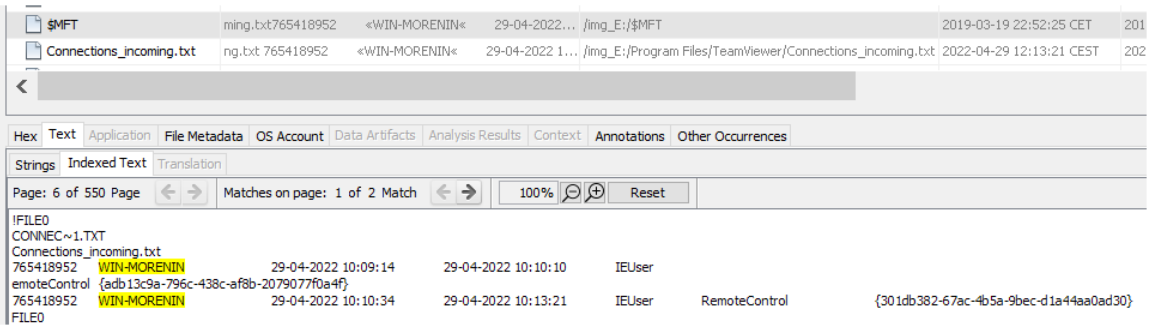
Lo hemos conseguido gracias a la herramienta **Access Data FTK Imager**.



12. Conexión programa control remote

El ID desde el que se conecta el atacante es 765418952.

Lo sabemos porque le hemos seguido el rastro con la herramienta **Autopsy**.



13.Metadatos

Los metadatos que hemos analizado se realizaron con una imagen de un gato.

La imagen original la vamos a pasar por diferentes herramientas para observar el cambio de los metadatos en ella:

1. **I Love IMG (https://www.iloveimg.com/es):** Esta primera conversión no modifico ningún metadato, solamente se añadieron metadatos con referencia del proceso que sufrió la imagen. (Imagen1).
2. **WhatsApp:** Al enviar la imagen original por WhatsApp y volverla a descargar podemos observar que gran parte de los metadatos han sido eliminados por la app. Por ejemplo, ya no podemos saber con qué dispositivo se tomó la foto. Además, se cambió el formato de la propia fotografía. (Imagen2).
3. **Mail:** Esta vez los metadatos sí que muestran los datos del dispositivo con el que se realizó la fotografía. También muestra la evidencia de que la imagen fue descargada por correo, en concreto Gmail. (Imagen3).
4. **Telegram:** Al pasar la imagen por Telegram los metadatos se han simplificado bastante. Podemos observar datos como que el archivo 4.jpeg es una imagen en formato JPEG con un tamaño de aproximadamente 152 KB y una resolución de 960 x 1280 píxeles (orientación vertical). Fue creado y modificado el 5 de abril de 2025 a las 14:15:51 (UTC) y se añadió al sistema pocos segundos después. Utiliza un espacio de color RGB con 24 bits por muestra, sin canal alfa, y está codificado en el perfil de color sRGB IEC61966-2.1. (Imagen4).
   Pero no nos proporciona ningún tipo de dato sensible.
5. **Discord:** Al pasar la imagen por Discord nos devuelven los metadatos una ruta de Discord donde se pueden trazar la ruta de origen. (Imagen5).

Los metadatos fueron hallados con el comando “mdls <nombre_imagen>”.

Confidential Security

Última Página