CHARLA MAGISTRAL · TRACK DE IA

Forensic con IA en 2026

Manuel Moreno · CEO · GLOBALSECURE

Instructor



- Profesional autodidacta con 20+ años en CiberSeguridad Ofensiva y Defensiva
- Creador de ZeusOS www.zeusos.org
- Creador de las certificaciones G|PPT, G|WPT, G|SIA, G|SPT, G|CFI y G|RIR
- Speaker internacional con ponencias en Ekoparty (Argentina), Ground Zero Summit (India), Microsoft Techdays (Chile), Owasp Latam Tour y otras.

Educación:

- Certified Chief Information Security Officer (CCISO) 2024
- Adversary Tactics – Detection (Blackhat USA 2022)
- Assessing and Exploiting Control Systems (Blackhat USA 2016)
- Practical Hardware Hacking (Ekoparty 2016)
- Dark Side Ops: Custom Penetration Testing (Blackhat USA 2015)
- Alienvault USM for Security Engineers (2016)
- Certificado OPST (OSSTMM Professional Security Tester) ISECOM
- Certificado CEH (Certified Ethical Hacking)
- Certificado CHFI (Computer Hacking Forensic Investigator)
- Certificado ECSP (Certified Secure Programmer)
- Certificado ECSA (Certified Security Analyst)
- Certificado Auditor Líder ISO 27001

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.


YOUR
SERVER IS
MY SERVER









Servicios Avanzados

GLOBAL SECURE

CiberSeguridad Ofensiva

- Penetration Testing
- Análisis de vulnerabilidades
- Web & Mobile App hacking
- Adversary emulation (Mitre) Purple team
- Lógica de fraude
- Industrial control systems Pentest (OT)



Physical Penetration Testing (RedTeam)

- Estudio de campo (seguridad física, ubicación cámaras, guardias, horarios)
- Clonación tarjetas de acceso
- Clonación de credenciales
- Ingeniería social
- Grabación con cámaras ocultas
- Hardware 4G para mantener acceso



GLOBAL SECURE

NUESTRA OFERTA DE VALOR



CiberSeguridad Defensiva

- Incident Response Preparation Service
- Ransomware attack
- Incident Response (DFIR)
- Investigación forense digital
- Investigación Sabotaje Informático
- Peritaje Fraudes BEC
- Servicio data recovery



BlueTeam Service

- Gestión de SIEM & Vulnerabilidades
- Hardening Servidores
- Hardening servicios Cloud
- Auditoria Firewalls/IPS/WAF
- Gestión de contraseñas
- Security Awareness program



Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

CHARLA MAGISTRAL · TRACK DE IA

Forensic con IA en 2026

Manuel Moreno · CEO · GLOBALSECURE

¿Qué es computación forense?

Es la aplicación de técnicas científicas y analíticas especializadas a infraestructuras tecnológicas que permiten identificar, preservar, analizar y presentar datos válidos dentro de un proceso legal.

Dichas técnicas incluyen reconstruir elementos informáticos, examinar datos residuales, autenticar datos y explicar las características técnicas del uso de datos y bienes informáticos.

Como la definición anterior lo indica, esta disciplina no solo hace uso de tecnologías de punta para mantener la integridad de los datos y del procesamiento de los mismos; sino que también requiere de una especialización y conocimientos avanzados en materia de informática y sistemas para poder detectar qué ha sucedido dentro de cualquier dispositivo electrónico.

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Primeros pasos en computación forense

- ASEGURAR LA CADENA DE CUSTODIA
- SACAR FOTOGRAFIAS DEL PROCESO
- OBTENER COPIA EN ORDEN DE VOLATILIDAD…

RAM -> Conexiones de Red-> Procesos en Ejecución > Disco

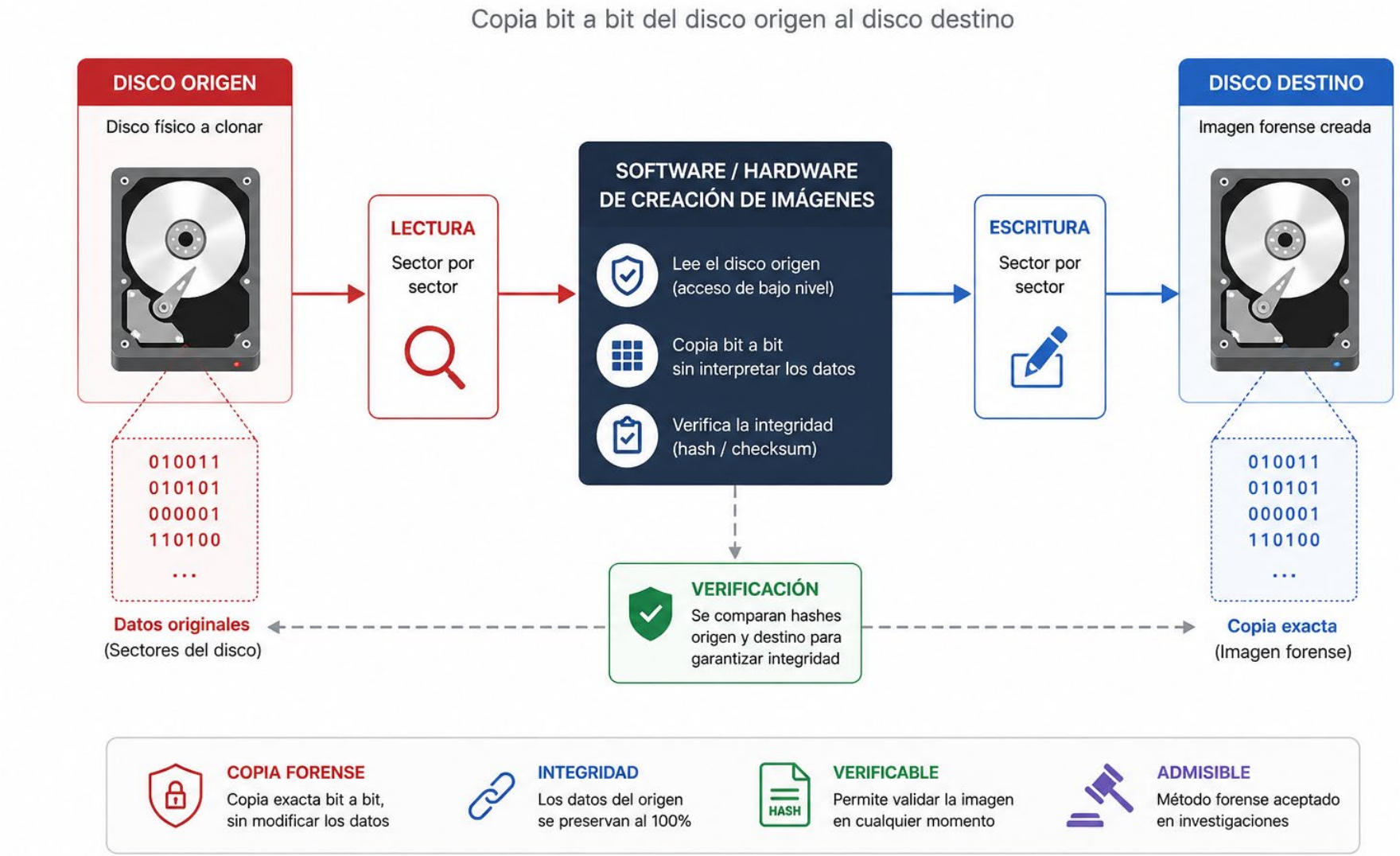
- Usar Bloqueador de Disco para Obtener la copia de Disco **(IMPORTANTE SI DESEAS LLEVAR LA EVIDENCIA A JUICIO)**
- Procesar la Evidencia obteniendo los hashes de los artecfactos colectados (Disco, Memoria, Archivos sospechosos)

La regla del Forense es:
si esta prendido… **déjalo Prendido**
si esta apagado … **déjalo apagado** (pero no tenemos RAM ☹)

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Qué es la creación de imágenes forenses

Preciso, verificable, reproducible.



Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

El valor de la creación de imágenes forenses

- La respuesta al incidente / creación de imágenes forenses es el paso MÁS IMPORTANTE en la investigación electrónica.
- El fracaso en este paso puede invalidar o hacer inadmisible toda la demás información recogida a partir de la prueba digital
- O al menos les puede dar un dolor de cabeza a sus abogados

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

¿Qué es Incident Response?

Incident Response (IR) es el proceso organizado y estructurado para identificar, contener, erradicar y recuperarse de incidentes de ciberseguridad. En el contexto de un curso sobre ransomware, la respuesta a incidentes se centra en minimizar el impacto de estos ataques y restaurar las operaciones normales de la organización lo más rápido posible.

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Elementos claves

Preparación:
Crear y mantener un plan de respuesta a incidentes, con protocolos claros y roles definidos. Incluye capacitación para el equipo y simulacros de ataque (tabletop exercises).

Identificación:
Detectar la presencia de un incidente de ransomware, determinar su alcance y clasificarlo. Esto incluye reconocer signos como archivos encriptados o mensajes de rescate.

Contención:
Implementar acciones inmediatas para limitar la propagación del ransomware. Ejemplo: desconectar sistemas afectados de la red o implementar reglas en el firewall.

Erradicación:
Eliminar completamente el ransomware de los sistemas comprometidos. Esto puede incluir restaurar sistemas desde respaldos seguros o aplicar parches.

Recuperación:
Restaurar las operaciones normales de la organización asegurándose de que los sistemas afectados estén limpios y protegidos contra futuros ataques.

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Base de conocimiento

Un equipo de incident response debe estar conformado por varios profesionales con distintas capacidades para dar velocidad al proceso de respuesta. Alguna de las especialidades que se requieren son:

- Incident Commander
- First Responders
- Forensic Leader
- Sysadmin
- Networking
- Malware reversing & Analysis
- Theat hunting

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Incident Commander

Un Incident Commander es quien lidera el proceso completo del incidente. Desde el contacto con el cliente, la alta dirección, socios o gerencia hasta las areas mas operativas, colaborando y guiando cada etapa del proceso. Alguna de las responsabilidades de este rol son:

- Definición de la estrategia en el incidente
- Asignación de los distintos roles del equipo
- Defición clave de las evidencias y procesos de triage a realizar en las primeras maquinas.
- Analisis de riesgos para la vuelta a operaciones de forma Segura
- Orquestración de los trabajos criticos realizados entre equipos internos, consultores externos y equipo de Incident Response
- Asesorar en el proceso de negociación (en caso que sea necesario pagar)
- Dar visibilidad en aspectos no cubiertos de forma inicial

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

First Responders

Es un rol clave para el inicio del proceso de respuesta ante incidentes. Es el encargado en activar el proceso o protocol de respuesta ante incidents, quien genera las primera notificaciones y quien colecta las primeras evidencias iniciales del incidente. Alguna de las labores que debe realizar este rol son:

- Ejecutar un proceso de TRIAGE en los servidores o estaciones de trabajo sospechosos de un incidente
- Asegurar la evidencia digital para que no sea destruida en algun proceso de restauracion por parte de tecnologia.
- Consultar las consolas de SIEM, EDR, xDR

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

¿POR QUÉ ANALIZAR LA MEMORIA RAM?



¿Por qué Analizar la memoria RAM?

El análisis de memoria (memory forensics) es clave en incident response porque la RAM contiene información volátil que desaparece al apagar un equipo, pero que puede revelar cosas como:

- Procesos maliciosos activos o recién terminados
- Malware fileless (sin archivos en disco)
- Actividades en tiempo real (conexiones, comandos, credenciales en uso)
- Evidencia que no queda registrada en el disco
- Llaves de cifrado de disco

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Mark Your Calendar: APT41 Innovative Tactics

May 28, 2025

Malware Infection Chain

This malware has three distinct modules, deployed in series, each with a distinct function. Each module also implements stealth and evasion techniques, including memory-only payloads, encryption, compression, process hollowing, control flow obfuscation, and leveraging Google Calendar for C2.

1. **PLUSDROP** - DLL to decrypt and execute the next stage in memory.
2. **PLUSINJECT** - Launches and performs process hollowing on a legitimate "svchost.exe" process, injecting the final payload.

- https://cloud.google.com/blog/topics/threat-intelligence/apt41-innovative-tactics

Que Hacer En Caso De Tener Un Incidente!

- Don'ts of Incident Response
  - Do Not Turn Off The System
  - Do Not Immediately Disconnect From Network
  - Do Not Run Anti-Virus Programs
    - Changes last-access time of virtually every file
    - Forces system log rotation
  - Do Not Run Registry Or File Cleaner Programs
  - Do Not Install Or Run Any Additional Tools
- Do's of Incident Response
  - Capture Memory
  - Disk Image

The volatile memory in a system is a gold mine of forensics data, often containing information that cannot be found on the hard drive or anywhere else. Some advanced malware has even evolved to erase any sign of its presence except for the code in memory that it needs to run. For these reasons, those responding to an incident should make every effort to capture a memory image

https://www.cisa.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_AreYouCompromised_S508C.pdf

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

FLUJO GENERAL DEL PROCESO



Orden de volatilidad de la evidencia

Order of Volatility

Order of Volatility	Type of Artifact	Time to Change
Most Volatile	Memory/RAM	Microseconds
Very Volatile	Network State	Milliseconds
Volatile	Running Processes	Seconds
Volatile	Network Traffic	Seconds to Minutes
Non-Volatile	Hard Disk	Minutes
Stable	Floppy Disk/Backup Media etc.	Years

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Proceso de análisis de memoria

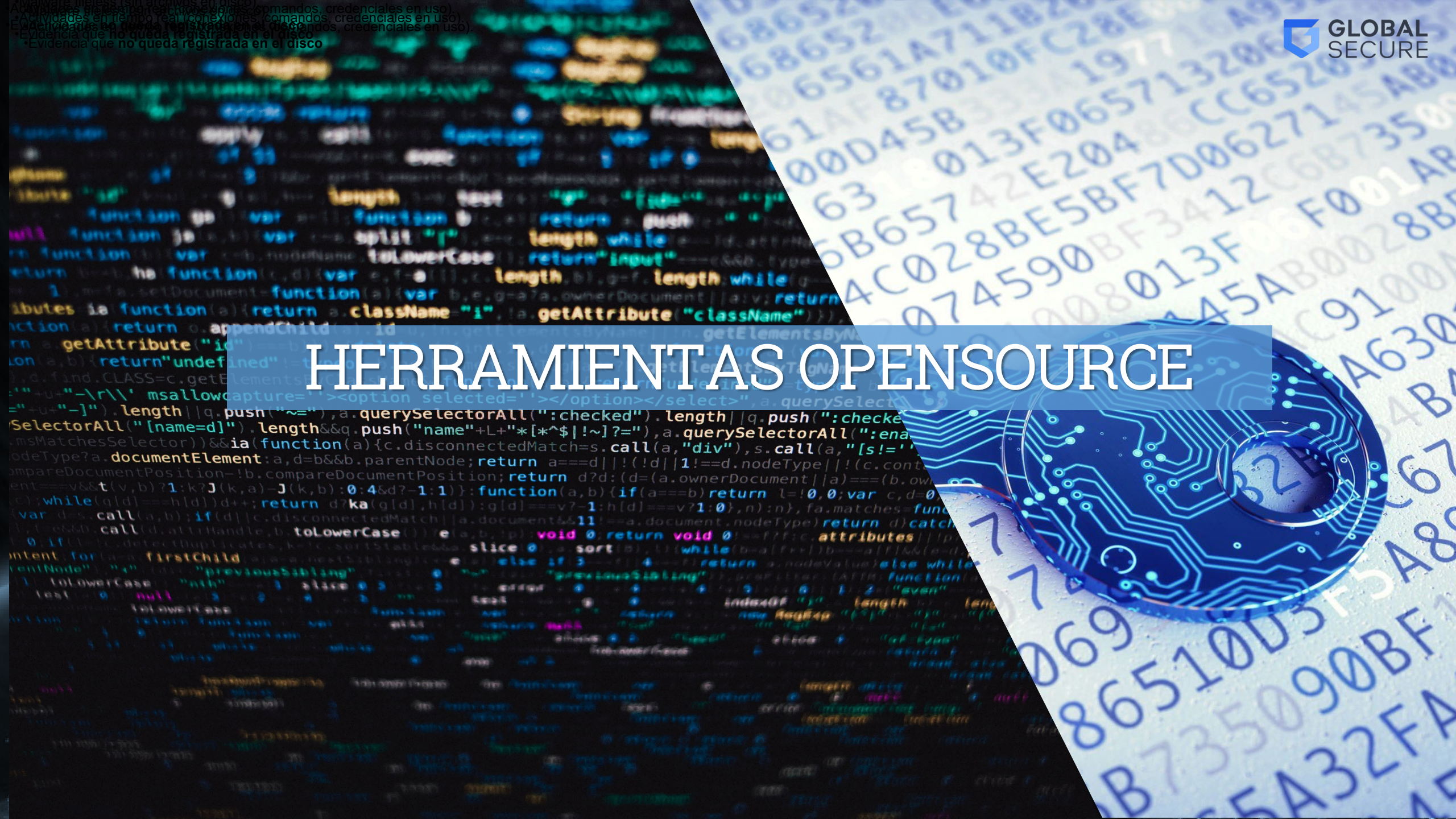
1 - Adquisición de memoria
Herramientas: DumpIt, Magnet RAM Capture, WinPMEM, Belkasoft RAM Capturer.
Se obtiene un dump de memoria (ej. memdump.raw).
Considerar la cadena de custodia y el hash (MD5/SHA256).

2 - Análisis
Se cargan los dumps en frameworks como **Volatility 2/3** o **MemProcFS**. O se usan herramientas comerciales como **Magnet Forensic, Belkasoft BEC o Encase**.
Se exploran procesos, conexiones, artefactos de usuario y actividad del sistema.

3 - Correlación con el incidente
Se cruza la información de RAM con logs, disco y red.
Permite responder preguntas clave: ¿Qué malware corría? ¿Qué hizo? ¿Cómo persistía?

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

HERRAMIENTAS OPENSOURCE



Volatility framework 2

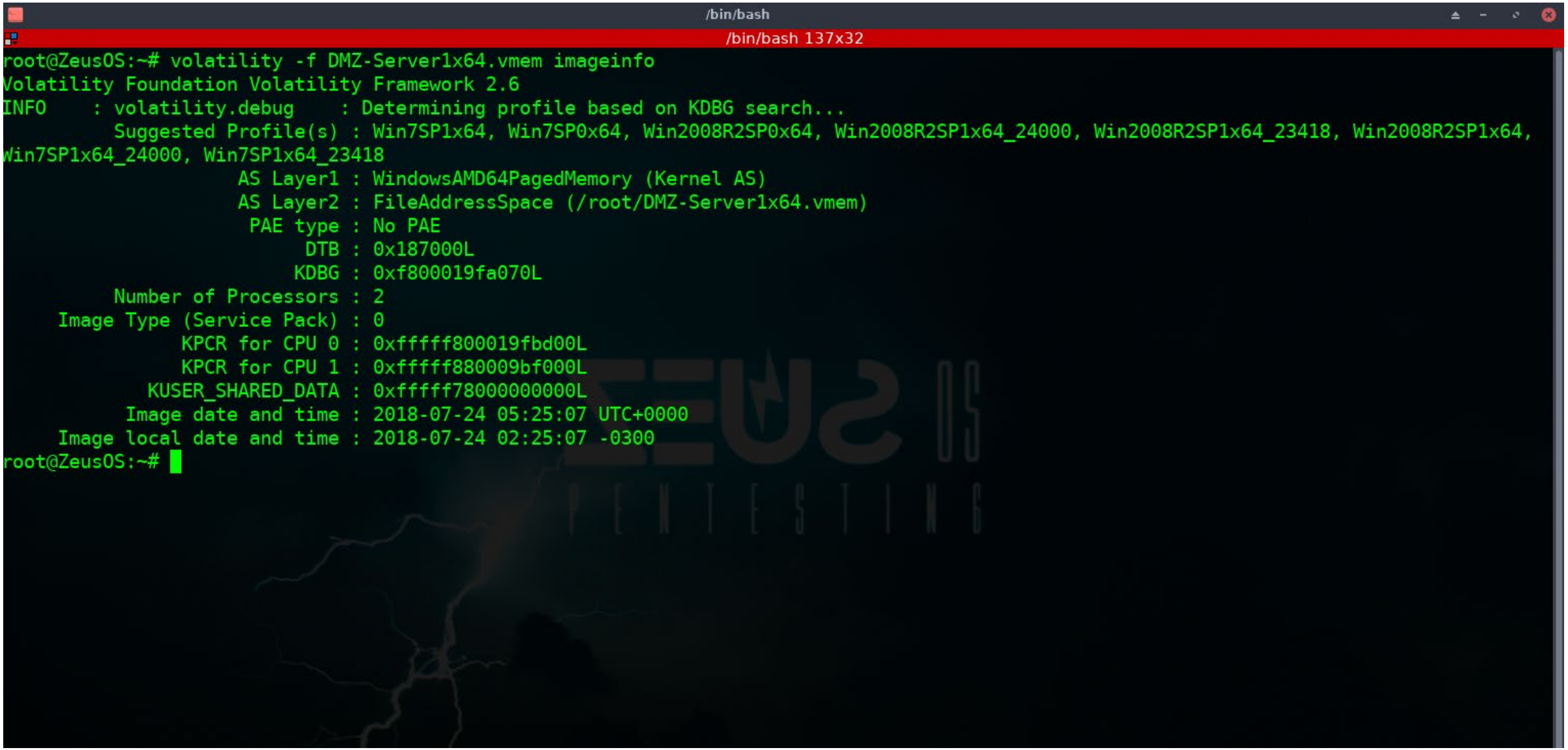
Volatility 2

Más antiguo, basado en **Python 2.7**.
Usa **perfiles** (Windows XP, 7, 10, Linux, etc.).
Plugins muy conocidos:

- pslist, pstree → lista de procesos.
- netscan → conexiones de red.
- malfind → inyecciones de código sospechosas.
- cmdscan, consoles → historial de comandos.
- hivelist, printkey → registros del sistema.
- dlllist, ldrmodules → DLLs cargadas.
- filescan, dumpfiles → recuperación de archivos desde memoria.

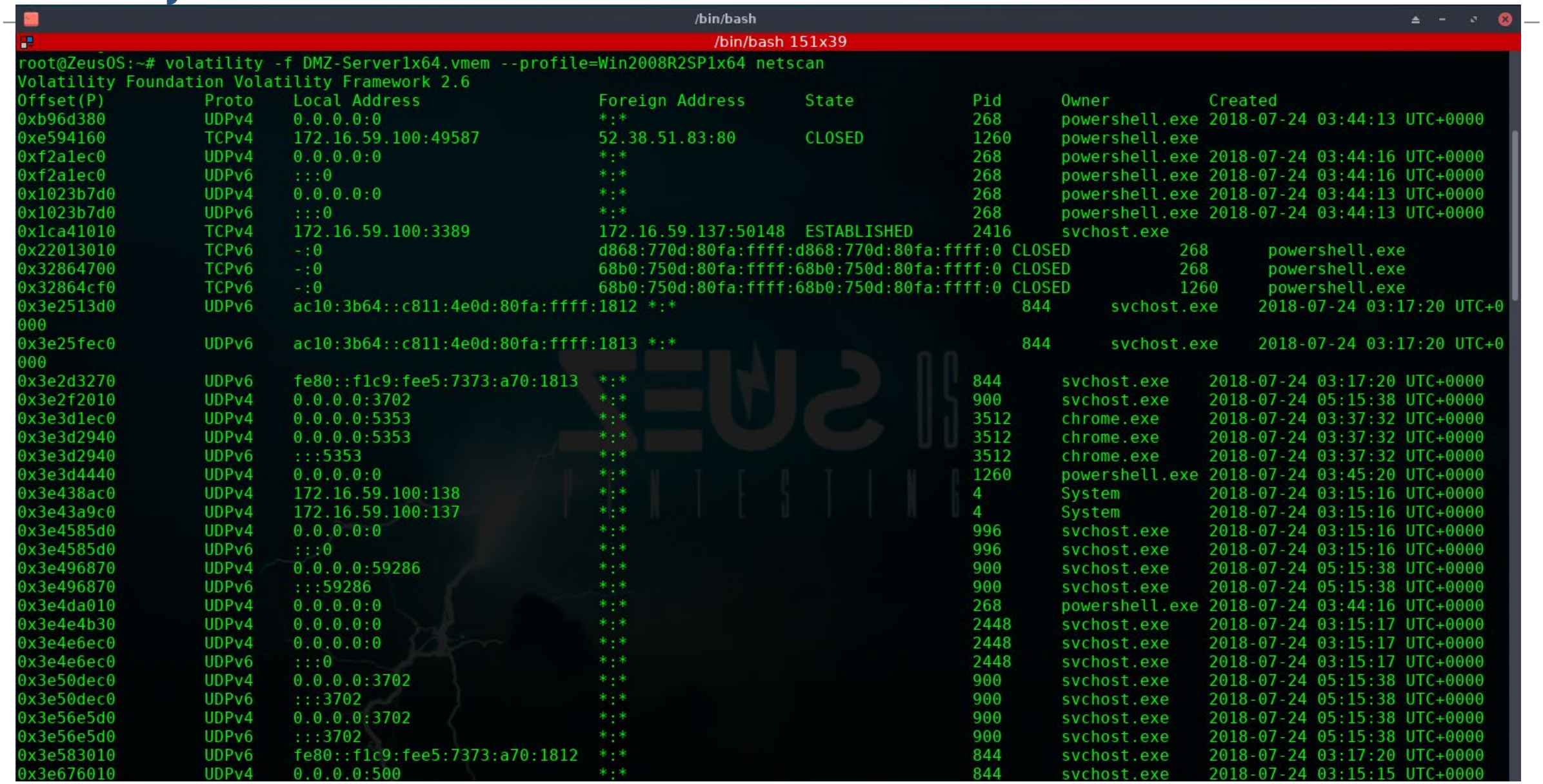
Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Volatility framework 2



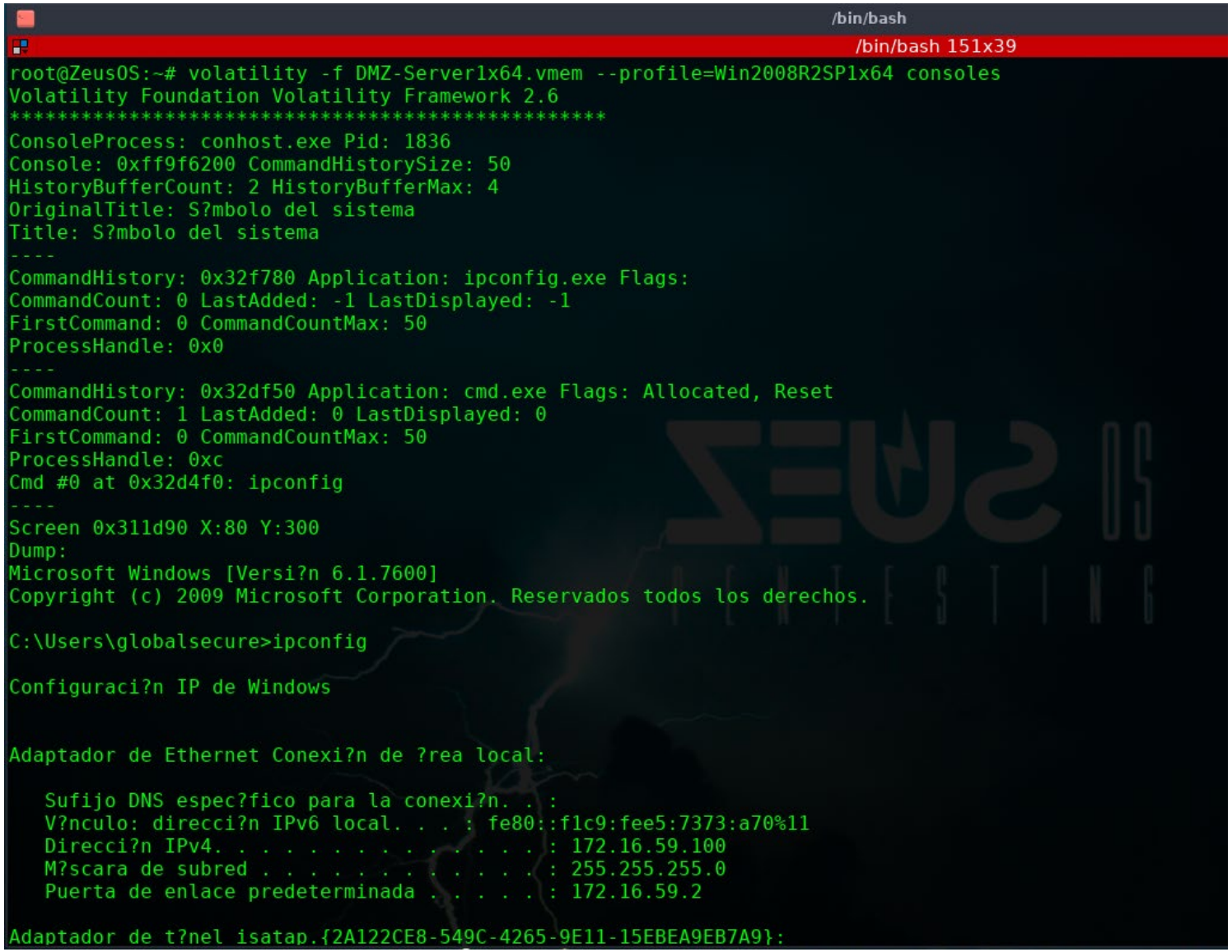
Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Volatility framework 2



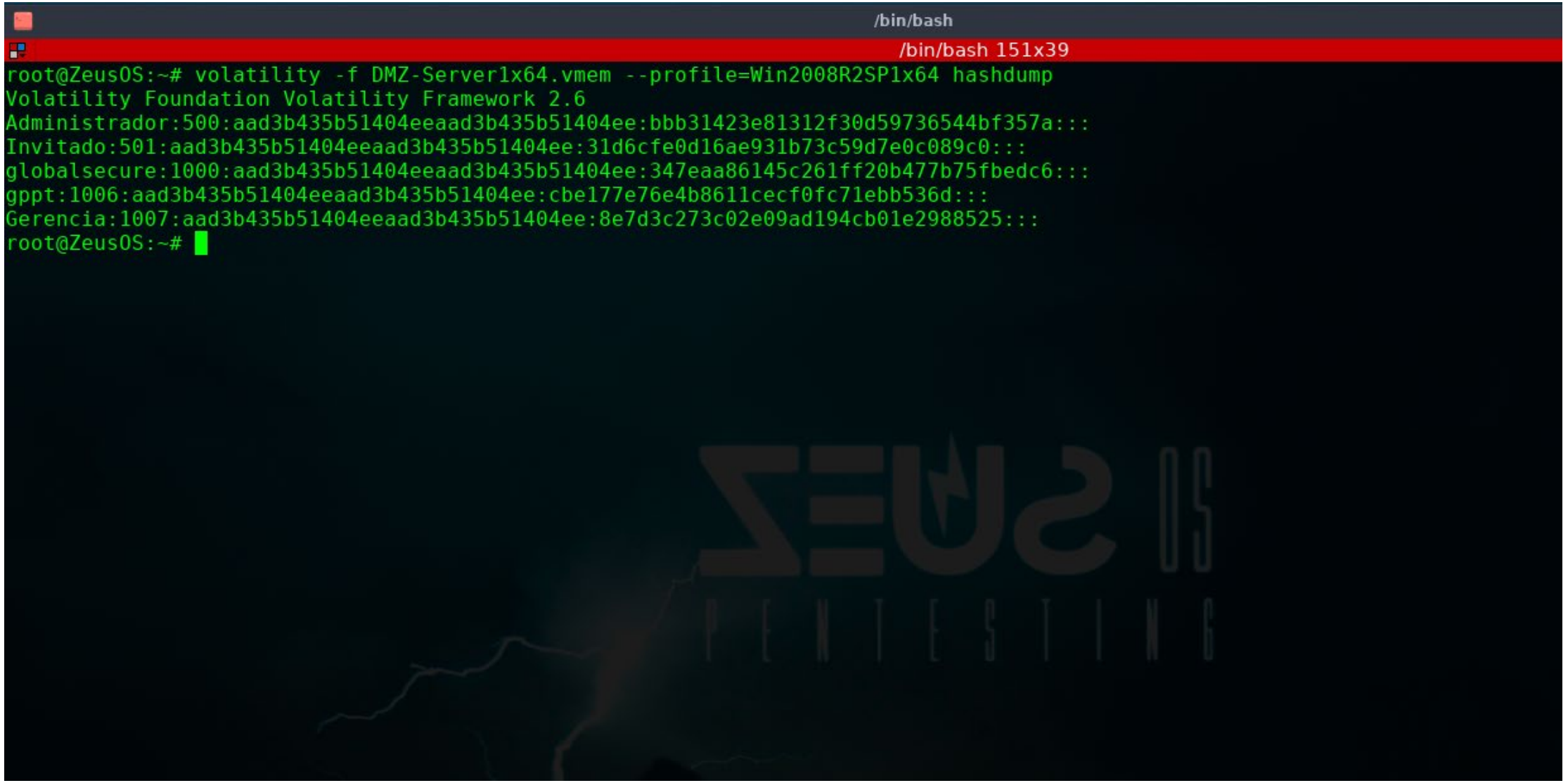
Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Volatility framework 2



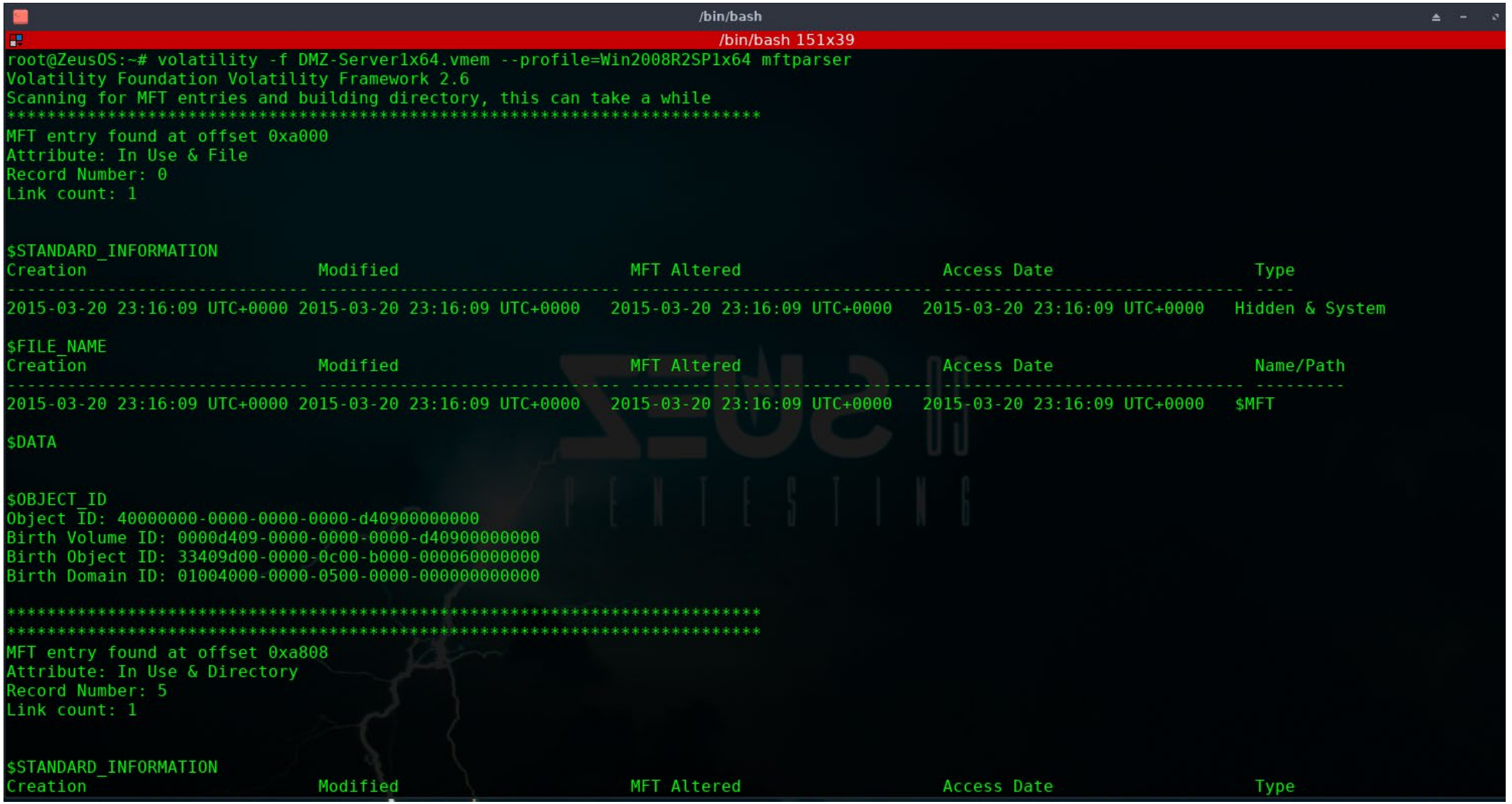
Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Volatility framework 2



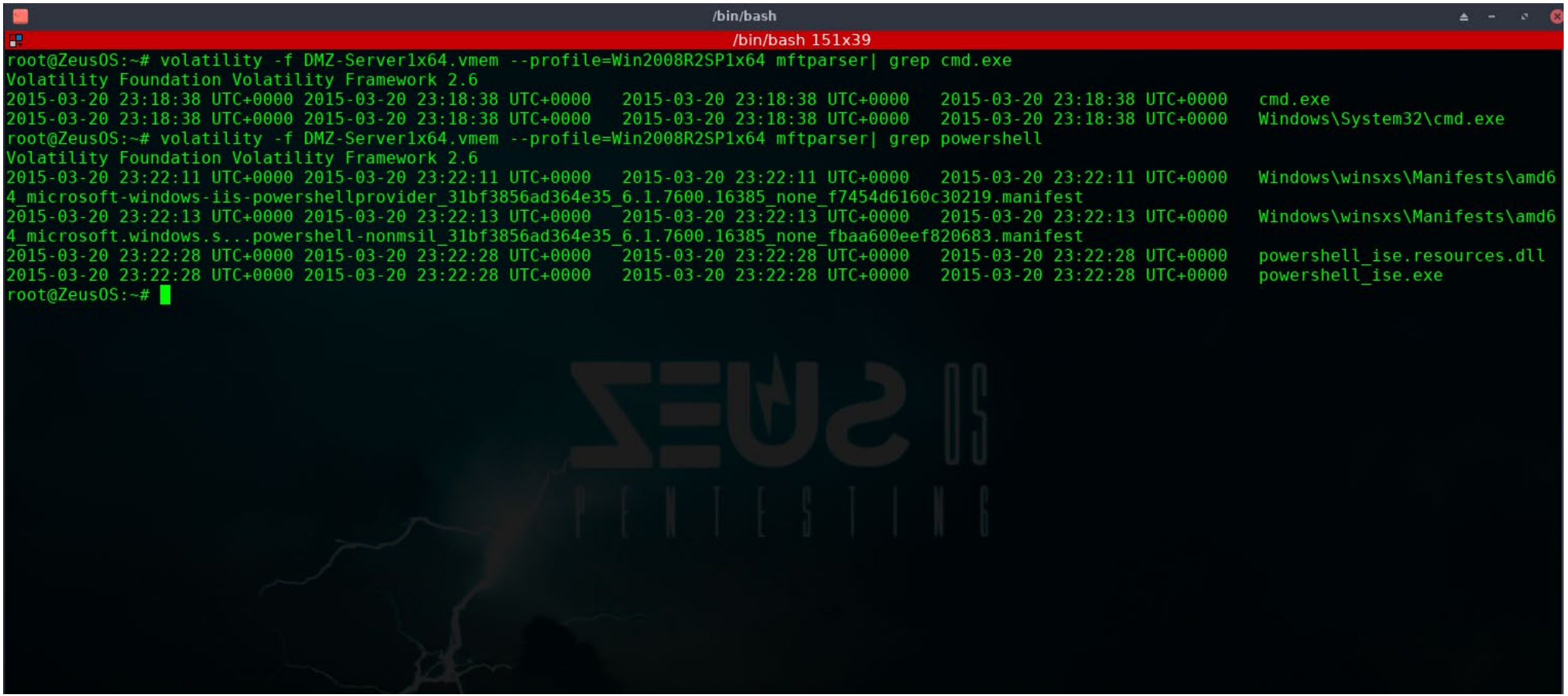
Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Volatility framework 2



Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Volatility framework 2



Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Volatility framework 3

Volatility 3

Reescrito en **Python 3** con arquitectura modular.
No necesita perfiles: detecta la plataforma automáticamente.
Mejor soporte para Windows 10/11 y Linux modernos.

Plugins clave:

- **windows.pslist** → procesos.
- **windows.netscan** → conexiones.
- **windows.cmdline** → comandos usados.
- **windows.malfind** → inyecciones de malware.
- **windows.registry.hivelist** → claves de registro.
- **linux.pslist, linux.bash** → procesos e historial de bash.

Ventaja: más compatible con sistemas actuales y soporta dumps grandes con mejor performance.

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Volatility framework 3

```
$ vol3 -r pretty -f data.lime windows.sessions
| Session ID | Session Type | Process ID |        Process |                    User Name |                  Create Time
* |        N/A |            - |          4 |         System |                            - | 2024-05-28 00:23:09.000000
* |        N/A |            - |        100 |       Registry |                            - | 2024-05-28 00:23:05.000000
* |        N/A |            - |        444 |       smss.exe |                            - | 2024-05-28 00:23:09.000000
* |          0 |            - |        600 |       csrss.exe |                     /SYSTEM | 2024-05-28 00:23:11.000000
* |          0 |            - |        700 |    wininit.exe |                     /SYSTEM | 2024-05-28 00:23:11.000000
* |          0 |            - |        820 |   services.exe |                     /SYSTEM | 2024-05-28 00:23:12.000000
* |          0 |            - |        828 |       lsass.exe |                     /SYSTEM | 2024-05-28 00:23:12.000000
* |          0 |            - |        544 |    svchost.exe |  ACMECORP/EC2AMAZ-DDPQH3R$ | 2024-05-28 00:23:15.000000
* |          0 |            - |        676 |    svchost.exe |  ACMECORP/EC2AMAZ-DDPQH3R$ | 2024-05-28 00:23:15.000000
* |          0 |            - |        416 |    svchost.exe |  ACMECORP/EC2AMAZ-DDPQH3R$ | 2024-05-28 00:23:15.000000
* |          0 |            - |       1112 |    svchost.exe |  ACMECORP/EC2AMAZ-DDPQH3R$ | 2024-05-28 00:23:15.000000
* |          0 |            - |       1204 |    svchost.exe | NT AUTHORITY/LOCAL SERVICE | 2024-05-28 00:23:15.000000
* |          0 |            - |       1212 |    svchost.exe | NT AUTHORITY/LOCAL SERVICE | 2024-05-28 00:23:15.000000
* |          0 |            - |       1220 |    svchost.exe | NT AUTHORITY/LOCAL SERVICE | 2024-05-28 00:23:15.000000
* |          0 |            - |       1232 |    svchost.exe |  ACMECORP/EC2AMAZ-DDPQH3R$ | 2024-05-28 00:23:15.000000
[snip]
* |          2 |            - |       3060 |    rdpclip.exe |     ACMECORP/Administrator | 2024-05-28 00:28:37.000000
* |          2 |            - |       3628 |    svchost.exe |     ACMECORP/Administrator | 2024-05-28 00:28:37.000000
* |          2 |            - |       1940 |    svchost.exe |     ACMECORP/Administrator | 2024-05-28 00:28:37.000000
* |          2 |            - |       1180 |     sihost.exe |     ACMECORP/Administrator | 2024-05-28 00:28:37.000000
```

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Volatility framework 3

Command	Vol2	Vol3
List processes in a table	pslist --profile=PROFILE	windows.pslist
List processes in a tree	pstree --profile=PROFILE	windows.pstree
List process command lines	cmdline --profile=PROFILE	windows.cmdline
List DLLs in a process	dlllist --profile=PROFILE -p PID	windows.dlllist --pid PID
Dump DLL(s)	dlldump [-p PID] [-b BASE] -D DIR	windows.dlllist --dump [--pid PID]
Dump a process	procdump [-p PID] -D DIR	windows.pslist --dump [--pid PID]
Dump process memory	memdump [-p PID] -D DIR	windows.memmap --dump [--pid PID]
Dump a cached file by physical offset	dumpfiles -Q OFFSET -D DIR	windows.dumpfiles --physaddr OFFSET
Scan for MFTs	mftparser	windows.mftscan
List registry hives	hivelist	windows.registry.hivelist
Print registry key	printkey -o OFFSET -K KEY	windows.registry.printkey --offset OFFSET --key KEY

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

HERRAMIENTAS FORENSES PROFESIONALES DE PAGO



Herramientas Profesionales

Foco en productividad, calidad y sobre todo “velocidad”. Utilizadas por el FBI, NSA y la mayoría de las policías a nivel mundial (incluido chile).

En la práctica, Magnet AXIOM + Volatility/MemProcFS sigue siendo la combinación más usada en incident response, porque AXIOM da reportes claros para managers/jueces y Volatility/MemProcFS da el análisis técnico profundo

Algunas opciones son:

Magnet Forensic AXIOM
Belkasoft BEC
Cellebrite Inspector
Encase

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Herramientas Profesionales



Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Herramientas Profesionales



Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Herramientas Profesionales



Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Herramientas Profesionales

FUENTES DE EVIDENCIA

DETALLES DEL CASO

FUENTES DE EVIDENCIA

DETALLES DEL PROCESAMIENTO

- Buscar archivos y copias de seguridad móviles
- Decodifique el cifrado basado en archivos
- Añadir palabras clave para buscar
- Extraer texto de archivos (OCR)
- Calcular los hashes y encontrar coincidencias
- Analizar chats con Magnet.AI
- Analizar imágenes con Magnet.AI
- Búsqueda con reglas YARA
- Encontrar más artefactos

DETALLES DEL ARTEFACTO

- Artefactos móviles
- Artefactos en la nube
- Artefactos informáticos
- Artefactos del vehículo
- Analizar y extraer artefactos
- Contenido privilegiado
- Filtro de rango de fechas

ANALIZAR EVIDENCIA

WINDOWS

SELECCIONE EL COMPLEMENTO DE MEMORIA

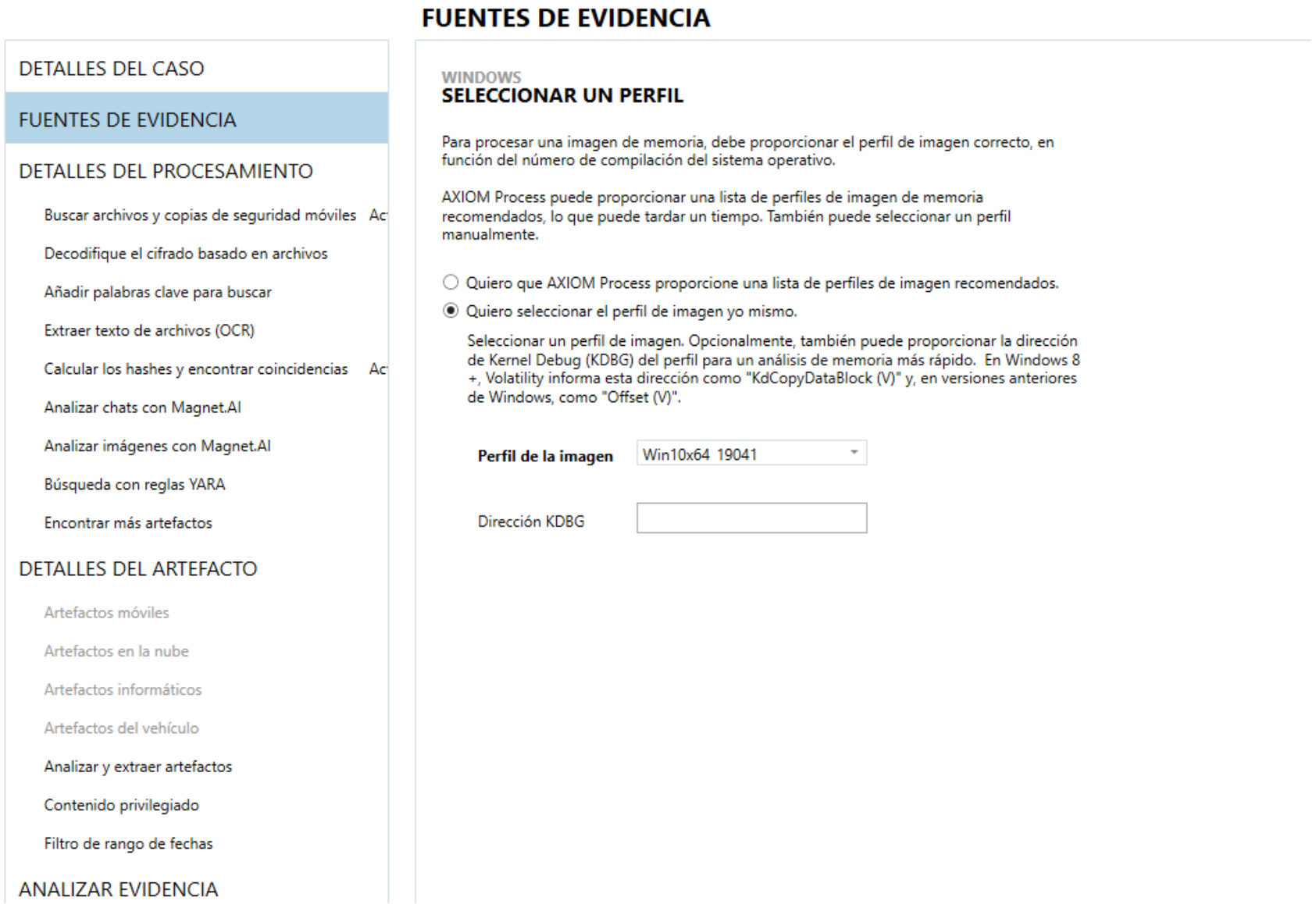
Según la fuente de evidencia, puede usar los complementos de memoria a continuación. Usar diferentes complementos de memoria puede arrojar diferentes resultados. Para obtener más información, consulte el artículo **Seleccionar complemento de memoria con AXIOM Cyber** .



VOLATILITY

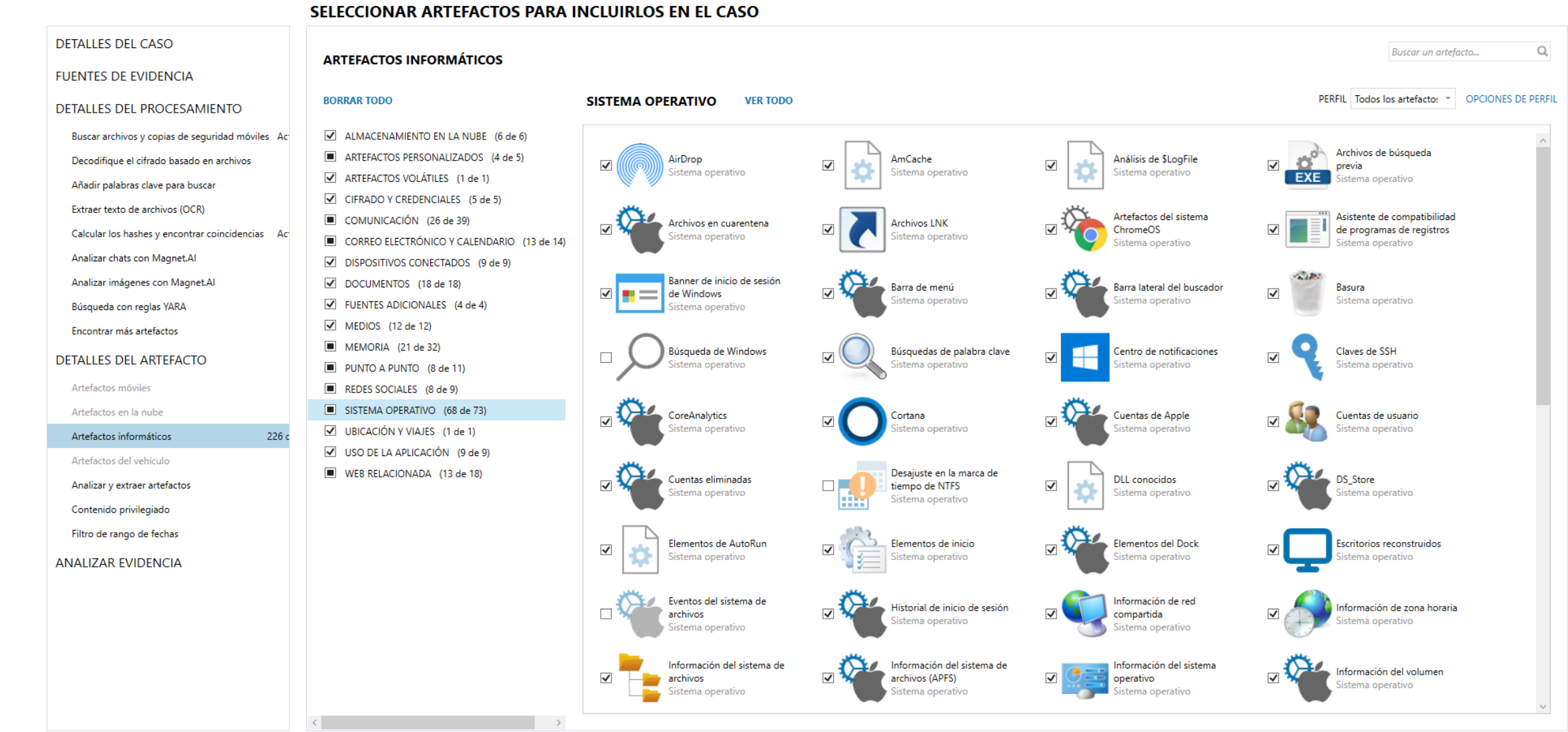
Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Herramientas Profesionales



Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Herramientas Profesionales



Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Herramientas Profesionales



Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Herramientas Profesionales

BÚSQUEDA CON REGLAS YARA

DETALLES DEL CASO

FUENTES DE EVIDENCIA

DETALLES DEL PROCESAMIENTO

- Buscar archivos y copias de seguridad móviles
- Decodifique el cifrado basado en archivos
- Añadir palabras clave para buscar
- Extraer texto de archivos (OCR)
- Calcular los hashes y encontrar coincidencias
- Analizar chats con Magnet.AI
- Analizar imágenes con Magnet.AI
- Búsqueda con reglas YARA
- Encontrar más artefactos

DETALLES DEL ARTEFACTO

- Artefactos móviles
- Artefactos en la nube
- Artefactos informáticos 226
- Artefactos del vehículo
- Analizar y extraer artefactos
- Contenido privilegiado
- Filtro de rango de fechas

ANALIZAR EVIDENCIA

CONJUNTOS DE REGLAS YARA

Utilice las reglas YARA para identificar los archivos coincidentes. Puede importar conjuntos de reglas YARA desde una carpeta que contenga archivos .yar o .yara o puede añadir manualmente conjuntos de reglas YARA.

NOTA: La ejecución de varios conjuntos de reglas YARA a la vez puede aumentar el tiempo de escaneo.

Leyendo conjuntos de reglas YARA de 1 carpetas sincronizadas. EDITAR

Buscar por nombre o ruta de origen...

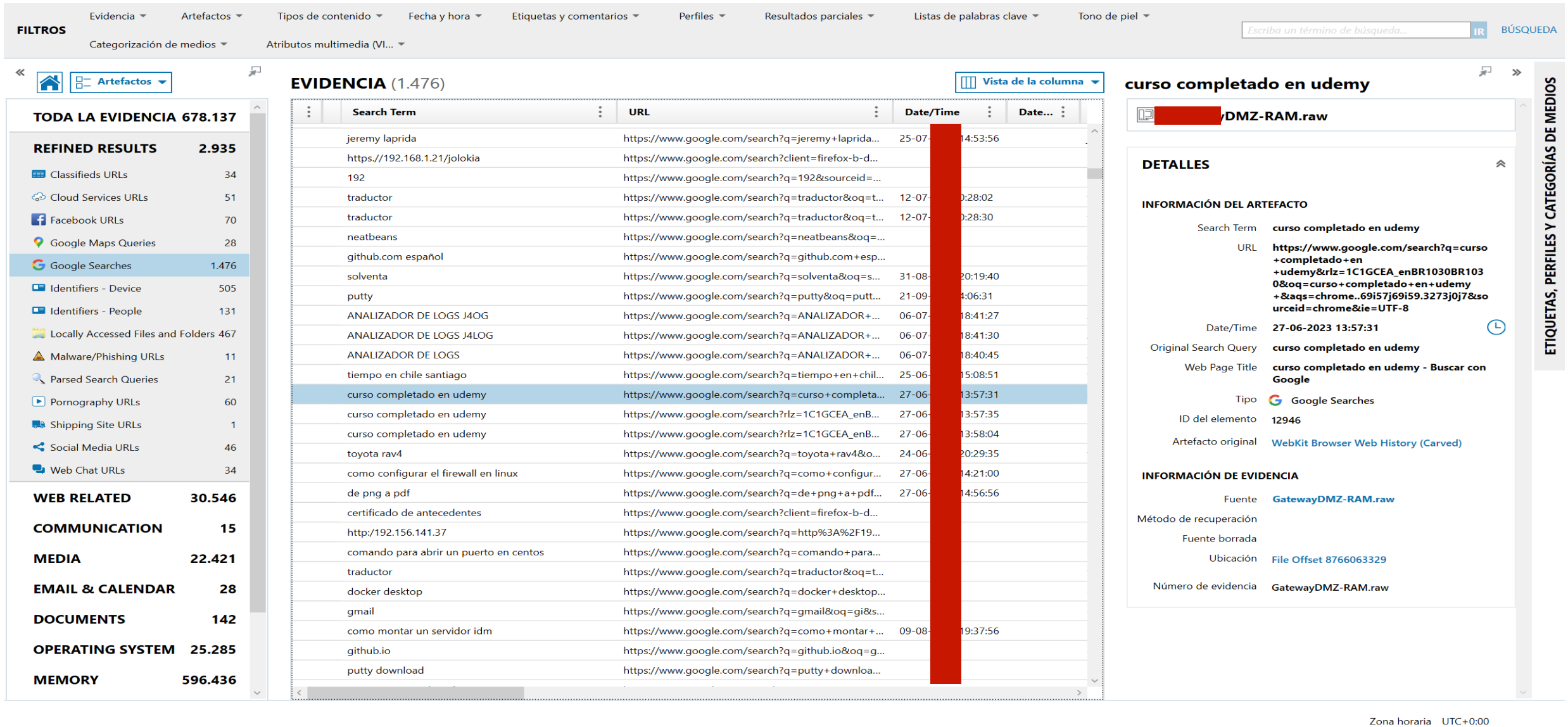
SELECCIONAR TODO AÑADIR UN NUEVO CONJUNTO DE REGLAS ACTUALIZAR

Reglas seleccionadas: 0

Habilita	Nombre del conjunto de reg	Ruta fuente	Fuente	Fecha de creación
☐	Linux.Virus.Vit.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	Magnet Forensics	15/12/2024 20:11:27
☐	Win32.Virus.Awfull.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	Magnet Forensics	15/12/2024 20:11:27
☐	Win32.Virus.Cmay.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	Magnet Forensics	15/12/2024 20:11:27
☐	Win32.Virus.DeadCode.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	Magnet Forensics	15/12/2024 20:11:27
☐	Win32.Virus.Elerad.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	Magnet Forensics	15/12/2024 20:11:27
☐	Win32.Virus.Greenp.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	Magnet Forensics	15/12/2024 20:11:27
☐	Win32.Virus.Mocket.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	Magnet Forensics	15/12/2024 20:11:27
☐	Win32.Virus.Negt.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	Magnet Forensics	15/12/2024 20:11:27
☐	Win32.Trojan.CaddyWiper.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	Magnet Forensics	15/12/2024 20:11:27
☐	Win32.Trojan.Dridex.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	Magnet Forensics	15/12/2024 20:11:27
☐	Win32.Trojan.Emotet.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	Magnet Forensics	15/12/2024 20:11:27
☐	Win32.Trojan.HermeticWiper.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	Magnet Forensics	15/12/2024 20:11:27
☐	Win32.Trojan.IsaacWiper.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	Magnet Forensics	15/12/2024 20:11:27
☐	Win32.Trojan.TrickBot.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	Magnet Forensics	15/12/2024 20:11:27
☐	ByteCode.MSIL.Ransomware.Ap...	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	Magnet Forensics	15/12/2024 20:11:26

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Herramientas Profesionales



Zona horaria UTC+0:00

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Herramientas Profesionales

GLOBAL SECURE

FILTROS | Evidencia | Artefactos | Tipos de contenido | Fecha y hora | Etiquetas y comentarios | Perfiles | Resultados parciales | Listas de palabras clave | Tono de piel | Categorización de medios | Atributos multimedia (VI...

Escriba un término de búsqueda... IR BÚSQUEDA

Artefactos

TODA LA EVIDENCIA 678.137

REFINED RESULTS	**2.935**
Classifieds URLs	34
Cloud Services URLs	51
Facebook URLs	70
Google Maps Queries	28
Google Searches	1.476
Identifiers - Device	505
Identifiers - People	131
Locally Accessed Files and Folders	467
Malware/Phishing URLs	11
Parsed Search Queries	21
Pornography URLs	60
Shipping Site URLs	1
Social Media URLs	46
Web Chat URLs	34
WEB RELATED	**30.546**
COMMUNICATION	**15**
MEDIA	**22.421**
EMAIL & CALENDAR	**28**
DOCUMENTS	**142**
OPERATING SYSTEM	**25.285**
MEMORY	**596.436**

EVIDENCIA (60)

Vista de la columna

Site Name	URL	Date/Time	Artifact
Videos de sexo porno gratuitos - Redtube - XXXMo...	https://es.redtube.com/	30-07-[redacted]20:31:46	WebKit Browse
Videos porno de Salvajes Transexuales: Cogiendo | R...	https://es.redtube.com/redtube/transgender	19-07-[redacted]16:11:46	WebKit Browse
Categorías de vídeo - RedTube	https://es.redtube.com/categories	30-07-[redacted]16:43:17	WebKit Browse
Free Porn, Sex Videos - HD Porno - XXX Porn Tube -...	https://es.redtube.com/?page=4	30-07-[redacted]20:38:11	WebKit Browse
Free Porn, Sex Videos - HD Porno - XXX Porn Tube -...	https://es.redtube.com/?page=5	30-07-[redacted]20:38:59	WebKit Browse
Big Tittie Redhead Cougar - RedTube	https://es.redtube.com/102274021	30-07-[redacted]20:44:35	WebKit Browse
Roxy Sweetheart takes a load of cum in her mouth -...	https://es.redtube.com/102258671	30-07-[redacted]20:47:05	WebKit Browse
Free Porn, Sex Videos - HD Porno - XXX Porn Tube -...	https://es.redtube.com/?page=2	30-07-[redacted]20:35:27	WebKit Browse
Pretty Ebony African Masseuse Sucking and Fucking...	https://es.redtube.com/102350231	30-07-[redacted]20:32:54	WebKit Browse
Free Porn, Sex Videos - HD Porno - XXX Porn Tube -...	https://es.redtube.com/?page=3	30-07-[redacted]20:37:24	WebKit Browse
Los Videos Porno de Moda - Chile's - RedTube	https://es.redtube.com/hot?cc=cl	30-07-[redacted]15:32:04	WebKit Browse
Porn Videos Watched History | Redtube	https://es.redtube.com/recently_viewed/history	30-07-[redacted]15:32:24	WebKit Browse
cute shemales one lucky guy - RedTube	https://es.redtube.com/19413591	30-07-[redacted]15:33:07	WebKit Browse
Transgender Girl Has Swingers Anal Sex - RedTube	https://es.redtube.com/43471091	30-07-[redacted]15:39:52	WebKit Browse
Hot Trans In Pantyhose Gets Her Sweet Ass Fucked -...	https://es.redtube.com/43382921	30-07-[redacted]15:46:37	WebKit Browse
DEVILSTGIRLS Él folló a pelo el bestie trans de su es...	https://es.redtube.com/43242391	30-07-[redacted]15:50:31	WebKit Browse
Pale Trans Babe Victoria Carvalho Rammed Good By...	https://es.redtube.com/43425331	30-07-[redacted]15:55:29	WebKit Browse
GenderXFilms - Cute animadora trans colada clavad...	https://es.redtube.com/43237221	30-07-[redacted]16:08:10	WebKit Browse
STELLA COX HAS HOT DOUBLE PENETRATION SEX...	https://es.redtube.com/premium/192865111?from=...	30-07-[redacted]16:08:05	WebKit Browse
Trans Hitcher Fucked Hardcore - RedTube	https://es.redtube.com/43299801	30-07-[redacted]16:00:58	WebKit Browse
Emma Rose Uses Alluring Cock To Tempt Handyman...	https://es.redtube.com/43278831	30-07-[redacted]16:08:27	WebKit Browse
Peruana callejera es pillada por noble joven de provi...	https://es.redtube.com/41239381	30-07-[redacted]16:23:13	WebKit Browse
Esta Venezolana Estaba Tan Caliente Que Me Pidió...	https://es.redtube.com/40496701	30-07-[redacted]16:23:15	WebKit Browse
Empleada venezolana de nalgas enormes - RedTube	https://es.redtube.com/42562971	30-07-[redacted]16:40:16	WebKit Browse
ME CORRO DENTRO DE UNA LATINA CALIENTE - Re...	https://es.redtube.com/40745141	30-07-[redacted]16:40:08	WebKit Browse
NOVIA ARGENTINA LE ACABO EN LA CARA PERO N...	https://es.redtube.com/15881581	30-07-[redacted]16:40:08	WebKit Browse
Tinder no falla y me trae a una zorra que le encanta...	https://es.redtube.com/40822391	30-07-[redacted]16:40:01	WebKit Browse
A Tight Onesie, Juicy Ass & Big Natural Tits - Aria Ka...	https://es.redtube.com/premium/435199631	30-07-[redacted]16:35:56	WebKit Browse
Pelirroja vendedora de polos pillada en las calles de...	https://es.redtube.com/42792891	30-07-[redacted]16:39:49	WebKit Browse

Peruana callejera es pillada por noble...

[redacted]yDMZ-RAM.raw

DETALLES

INFORMACIÓN DEL ARTEFACTO

Site Name	**Peruana callejera es pillada por noble joven de provincia - RedTube**
URL	**https://es.redtube.com/41239381**
Date/Time	**30-07-2023 16:23:13**
Tipo	**Pornography URLs**
ID del elemento	**67904**
Artefacto original	**WebKit Browser Web History (Carved)**

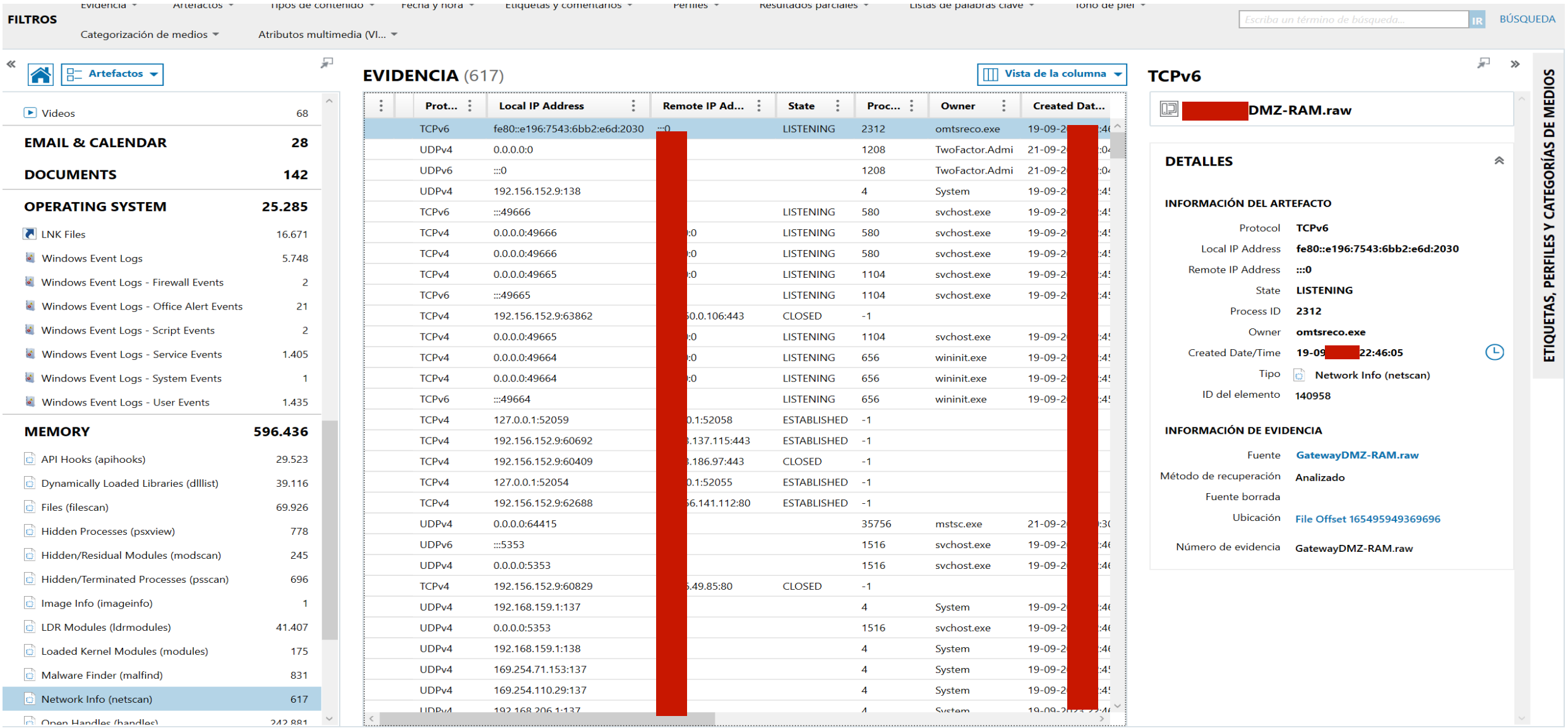
INFORMACIÓN DE EVIDENCIA

Fuente	**GatewayDMZ-RAM.raw**
Método de recuperación	
Fuente borrada	
Ubicación	**File Offset 52648139419**
Número de evidencia	**GatewayDMZ-RAM.raw**

ETIQUETAS, PERFILES Y CATEGORÍAS DE MEDIOS

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Herramientas Profesionales

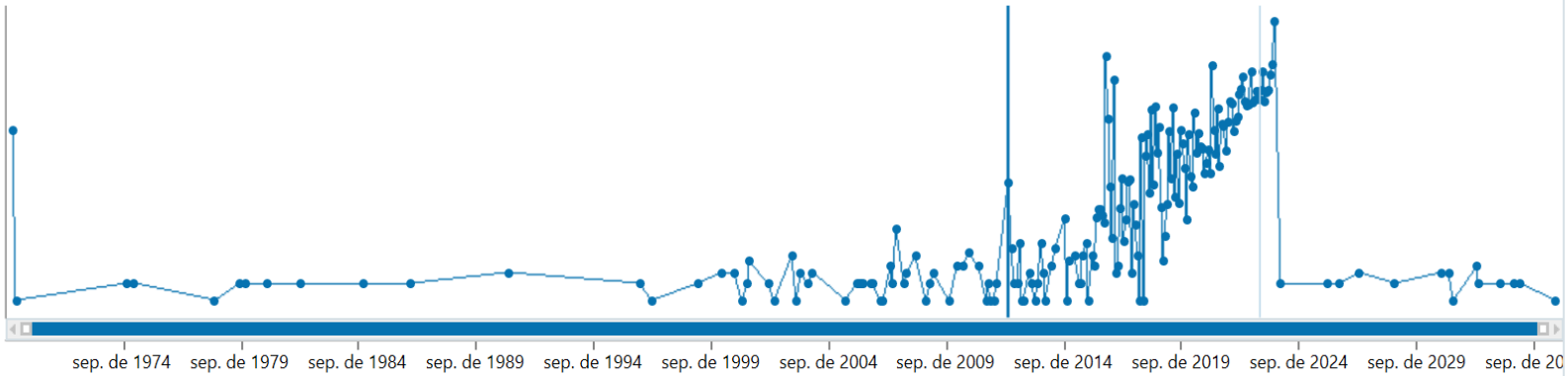


Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Herramientas Profesionales

Línea de tiempo

03-09-1969 5:09:22 - 02-12-2035 19:35:35 IR A LA FECHA ZOOM AÑOS PÁGINA



\\192.[redacted]186\Traspaso\CorreoSaliente\Juan\Control_trx\Apertura2.log < 1 DE 3 MARCAS DE TIEMPO >

Fecha/hora	Atributo de fecha/hora	Categoría de línea...	Categoría	Tipo	Nombre del elemento
17-05-2012 19:04:02	Target File Last Modified Date/Time	Apertura de archivo/carpeta	Operating System	LNK Files	Linked Path
22-05-2012 0:00:08	Start Date/Time	Evento del usuario	Memory	Timeline (timeliner)	Start Date/Time - UTC (yyyy-mm-dd)
22-05-2012 0:00:08	Start Date/Time	Evento del usuario	Memory	Timeline (timeliner)	Start Date/Time - UTC (yyyy-mm-dd)
22-05-2012 0:00:08	Start Date/Time	Evento del usuario	Memory	Timeline (timeliner)	Start Date/Time - UTC (yyyy-mm-dd)
22-05-2012 0:00:08	Start Date/Time	Evento del usuario	Memory	Timeline (timeliner)	Start Date/Time - UTC (yyyy-mm-dd)
22-05-2012 0:00:08	Start Date/Time	Evento del usuario	Memory	Timeline (timeliner)	Start Date/Time - UTC (yyyy-mm-dd)
22-05-2012 0:00:08	Start Date/Time	Evento del usuario	Memory	Timeline (timeliner)	Start Date/Time - UTC (yyyy-mm-dd)
22-05-2012 0:00:08	Start Date/Time	Evento del usuario	Memory	Timeline (timeliner)	Start Date/Time - UTC (yyyy-mm-dd)
22-05-2012 0:00:08	Start Date/Time	Evento del usuario	Memory	Timeline (timeliner)	Start Date/Time - UTC (yyyy-mm-dd)
22-05-2012 0:00:08	Start Date/Time	Evento del usuario	Memory	Timeline (timeliner)	Start Date/Time - UTC (yyyy-mm-dd)

\\[redacted].186\Traspaso\CorreoSaliente...

GatewayDMZ-RAM.raw

DETALLES

INFORMACIÓN DEL ARTEFACTO

Linked Path \\192.[redacted]\Traspaso\CorreoSaliente\Juan\Control_trx\Apertura2.log

Target File Created Date/Time 07-01-2023 11:37:41

Target File Last Modified Date/Time 17-05-2012 19:04:02

Target File Last Accessed Date/Time 07-01-2023 11:37:42

Target Attributes FILE_ATTRIBUTE_ARCHIVE

Show Command SW_SHOWNORMAL

MAC Address 00:50:[redacted]

Target File Size (Bytes) 148

Tipo LNK Files

ID del elemento 34966

INFORMACIÓN DE EVIDENCIA

Fuente [redacted]yDMZ-RAM.raw

Método de recuperación Moldeado

Fuente borrada

Ubicación File Offset 26819206464

[redacted]

ETIQUETAS, PERFILES Y CATEGORÍAS DE MEDIOS

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

01

SECCIÓN

Presentación del Caso

Analisis Forense a un servidor atacado.


Ransomware Gang
"EVERYONE HAS A PLAN 'TILL THEY GET PUNCHED IN THE MOUTH."
MIKE TYSON
Information Security Management
ISO 27001
Certified

Servidor Comprometido

Servidor Oracle 7. 9con kernel UEK

- 192GB de RAM a analizar
- Logs no entregaban toda la historia
- Había espacios donde incluso no había logs!
- Usar Volatility dio error que era indeterminado

- Por privacidad y NDAs no se puede enviar información ni logs ni nada a servidores CLOUD ni de terceros. TODOS DEBE SER PROCESADO “ONPREMISE”

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Obtener la memoria para su analisis

Usar AVML: https://github.com/microsoft/avml

AVML es una herramienta de adquisición de memoria volátil en espacio de usuario X86_64 escrita en Rust , diseñada para implementarse como un binario estático. AVML permite adquirir memoria sin necesidad de conocer de antemano la distribución del sistema operativo o el kernel. No requiere compilación ni análisis de huellas digitales en el sistema de destino.

Características

- Guarde las imágenes grabadas en ubicaciones externas mediante Azure Blob Store o HTTP PUT.
- Compresión opcional a nivel de página mediante Snappy .
- Utiliza el formato **de salida LiME** (cuando no se utiliza compresión).

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Pasos para crear una replica de un server comprometido

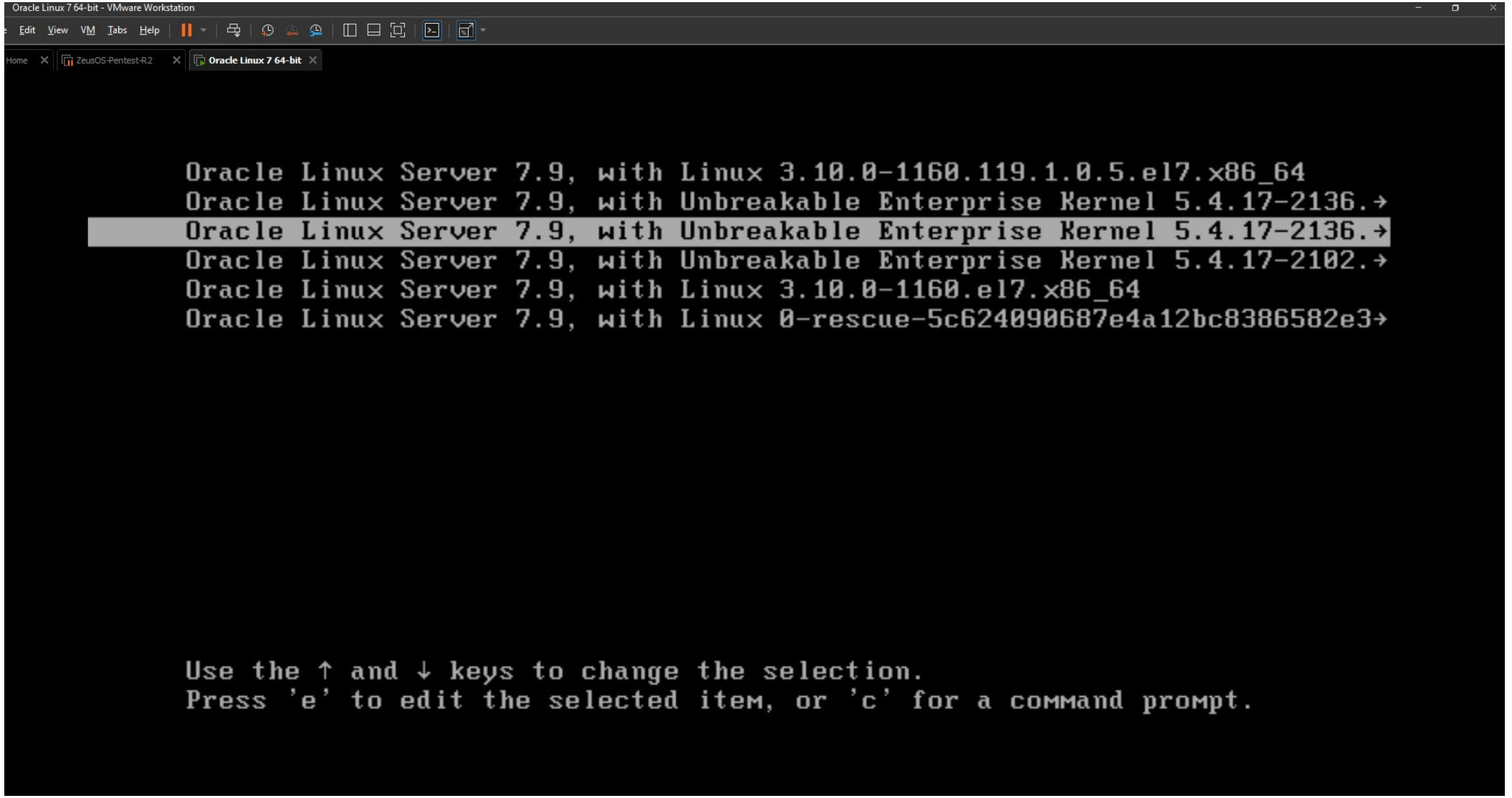
Para analizar una memoria, Volatility necesita crear un perfil (symbols) de Linux que contenga la misma y “exacta” versión del kernel del servidor comprometido. Los pasos son:

- Crear una VM con la misma versión de Linux
- Aplicar la misma versión de kernel (esta parte del trabajo es laborioso y consume tiempo)
- Usar dwar2json para crear el perfil (esto se debe compilar en el servidor “REPLICA”

NUNCA SE TRABAJA SOBRE LA EVIDENCIA.. REGLA DE ORO!

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Monte un servidor replica del Kernel



Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Correr Volatility no daba respuesta

A pesar de tener todo correcto… por algún motivo hasta ese momento desconocido…
no listaba los procesos.

```
C:\Windows\System32\cmd.e

D:\DFIR Tools\Volatility3\volatility3-2.26.2>python vol.py -f "C:\Users\ManuelMoreno\Documents\DEV\Memory-Forensic\memdump-2026-04-23.lime" linux.pslist
Volatility 3 Framework 2.26.2
Progress:  100.00               Stacking attempts finished
OFFSET (V)      PID     TID     PPID    COMM    UID     GID     EUID    EGID    CREATION TIME   File output

D:\DFIR Tools\Volatility3\volatility3-2.26.2>
```



Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Strings...

Si no existe forma de procesar con Volality se puede usar strings, pero al ser un forma sin estructura es literalmente “cazar” con un rifle a 10.000 km de distancia!.

```
┌──(manu0x01㉿Manu0x02)-[/mnt/c/Users/ManuelMoreno/Documents/DEV/Memory-Forensic]
└─$ strings memdump-2026-04-23.lime | grep ssh
MESSAGE=Accepted password for root from 192.168.140.202 port 57402 ssh2
/etc/selinux/targeted/active/modules/100/rssh/
/etc/selinux/targeted/active/modules/100/ssh/
- Label .ssh under amanda
- corenet_tcp_bind_all_unreserved_ports(ssh_t) should be called with the user_tcp_server boolean
- Allow lsmd plugins to connect to http/ssh/http_cache ports by default
- Allow gpg_agent to use ssh-add
- Allow gpg_agent to use ssh-add
MESSAGE=Accepted password for [redacted] from 172.16.215.94 port 52038 ssh2
- Fixes for mls use of ssh
- Revert "Allow sshd setcap capability. This is needed due to latest changes in sshd"
MESSAGE=Accepted password for [redacted] from 172.16.215.94 port 52038 ssh2
MESSAGE=Accepted password for root from 192.168.140.202 port 52123 ssh2
MESSAGE=Accepted password for root from 192.168.140.202 port 58712 ssh2
- ssh into a box with -X -Y requires ssh_use_ptys
- Allow sshd_t sys_admin for use with afs logins
- Allow sshd_t sys_admin for use with afs logins
```

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Magic Numbers

Un magic number es una secuencia específica de bytes al inicio (o, en algunos casos, en otra parte) de un archivo que identifica su formato. Es como una "firma" o "huella digital" del archivo.

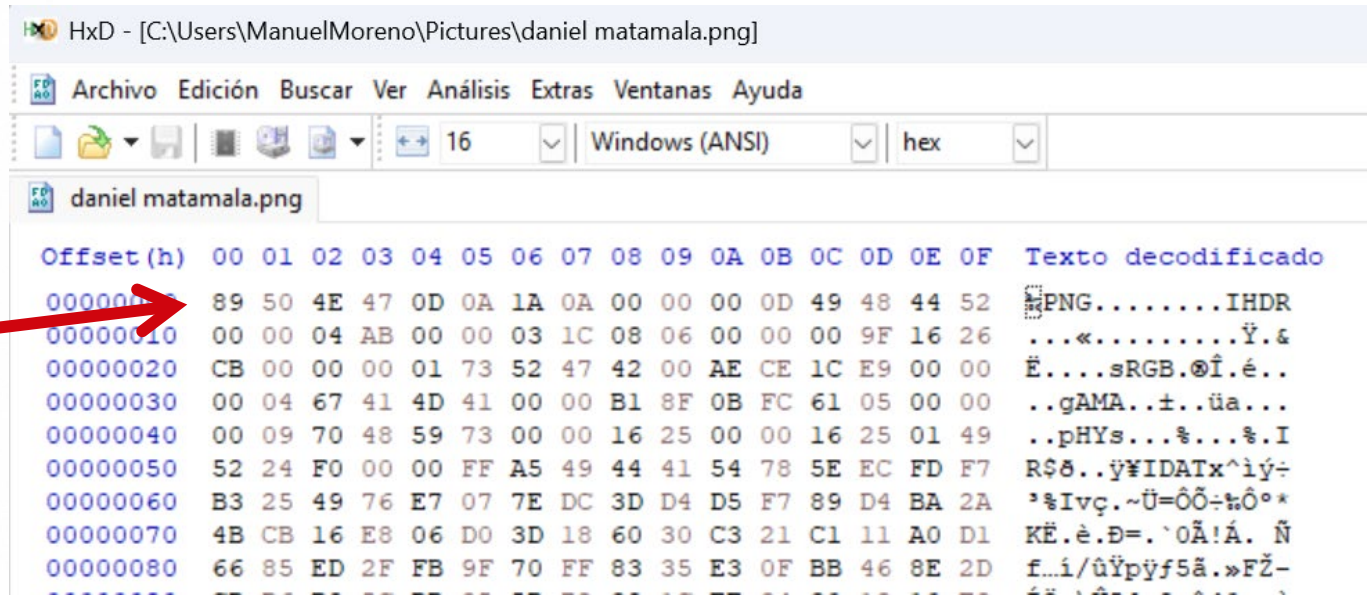
¿Por qué existen? Cuando un programa abre un archivo necesita saber:

- Cómo interpretar los bytes
- Qué estructura interna tiene y qué parser utilizar

En lugar de confiar en el nombre del archivo, revisa los primeros bytes.

Ejemplos de Magic Numbers

	Magic Number (Hex)				ASCII
PDF (Documento)	25	50	44	46	%PDF
PNG (Imagen)	89	50	4E	67	0D	0A	1A	0A	.PNG....
ZIP (Archivo comprimido)	50	4B	03	04	PK..



Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

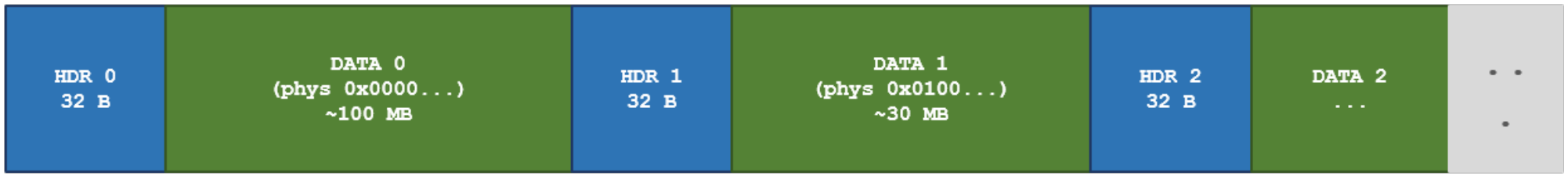
Formato LiME: Estructura Normal

Como Volatility 3 espera encontrar el dump en disco

Estructura del Header LiME (32 bytes, little-endian):



Cadena de segmentos en el archivo .lime:



Volatility lee HDR 0 -> calcula next_offset = 32 + seg_len -> salta a esa posicion -> verifica HDR 1 valido -> continua

Resultado esperado con dump estándar:

- N segmentos físicos correctamente mapeados
- Stack: primary -> LimeLayer -> FileLayer
- Todos los plugins linux.* disponibles para análisis

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

El Problema: Phantom Headers

Estructura anomala del dump **memdump-2026-04-23.lime**



Phantom header (segmento puente invalido)

Header real embebido en el data del phantom

Header LiME normal

Data real de memoria

COMPORTAMIENTO DE VOLATILITY 3 SIN EL FIX:

1. Lee HDR* en offset 0 -> magic 0x4C694D45 valido, version 1 -> acepta el header fantasma
2. Calcula next_offset = 0 + 32 + seg_len_basura -> salta a una posicion arbitraria dentro del dump
3. **En next_offset: NO hay header LiME valido -> LimeFormatException -> DETENCION TOTAL del parser**

X. **Resultado: 0 segmentos mapeados. Volatility no puede leer nada. 191.64 GB de evidencia inaccesibles.**

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Causa Raiz del Phantom Header

¿Por que existen estos segmentos fantasma en el dump?

Como funciona el modulo LiME

1. El modulo kernel LiME itera sobre los rangos de RAM fisica
2. Por cada rango, escribe primero el header LiME y luego los datos
3. En algunas variantes del modulo, el header del SIGUIENTE rango es pre-escrito en los primeros 32 bytes del rango actual
4. Al capturar esa region, esos 32 bytes quedan incluidos en el dump como un segmento puente invalido

Evidencia encontrada en el dump

`Offset 0`	HDR fantasma -> seg_len incoherente
`Offset 32`	HDR real del segmento 0 (valido)
`Offset 2.622.750.940`	2° HDR fantasma
`Offset +32`	HDR real del segmento siguiente

Conclusion: Es un bug de la version del modulo LiME utilizada. Al pre-escribir el header del siguiente segmento dentro de la primera pagina fisica antes de capturarla, esa pagina queda como un "segmento puente" invalido en el dump, rompiendo el parser estandar de Volatility 3.

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Diagnostico: Ingenieria Inversa del Dump

Scripts de análisis escritos para identificar el patrón

inspect_lime.py — Fase 1 (diagnostico)

Hexdump de los primeros 96 bytes del dump y walk estandar LiME v1.

-> Header doble en offsets 0 y 32 -> cadena rota desde el inicio

analyze_lime.py — Fase 1 (diagnostico)

Escaneo completo del archivo (~300 GB) buscando todas las ocurrencias del magic 0x4C694D45 e intentando todas las posiciones como posibles headers reales.

-> 10 posiciones con magic valido · Phantoms confirmados en offsets 0 y 2.622.750.940

test_lime_fix.py — Fase 2 (solucion)

Simulacion del walk iniciando en offset 32 (saltando el primer phantom) para verificar que la cadena real era completamente accesible.

-> 8 segmentos validos · 191.64 GB de RAM correctamente mapeados

test_lime_fix2.py — Fase 2 (solucion)

Prueba del algoritmo de deteccion bidireccional:
(1) cadena rota -> (2) busca header en data_start -> (3) decide phantom vs. fin real.

-> Logica validada · Lista para integrar en lime.py de Volatility 3

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

La Solucion: Modificacion de lime.py (en Volatility)

volatility3/framework/layers/lime.py — funcion _load_segments()

CODIGO ORIGINAL

```
while offset < file_size:

  start, end =
    check_header(offset)
  # Si falla -> BREAK

  seg_len = end - start + 1
  add_segment(...)
  offset += 32 + seg_len


# Sin recuperacion ante
# errores en la cadena
```

->

CODIGO CORREGIDO

```
while offset < file_size:
  start, end =
    check_header(offset)

  next = offset + 32 +
    (end - start + 1)

  try:
    check_header(next)
    add_segment()
    offset = next
  except:  # cadena rota
    data = offset + 32
    try:
      check_header(data)
      offset = data  # phantom!
    except:
      add_segment(); break
```

Propiedades del fix:

- Backward-compatible: dumps LiME estandar funcionan exactamente igual
- Detecta phantom headers en cualquier posicion de la cadena
- Aproximadamente 30 lineas de cambio en total en lime.py

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Resultados: Antes vs. Despues

Impacto concreto del fix sobre el análisis forense del incidente

ANTES (codigo original de Volatility 3)

X Segmentos mapeados: 0

- LimeFormatException al leer el primer header

- Stack de capas: FALLA

- linux.pslist / pstree: ERROR

X 191.64 GB de evidencia forense INACCESIBLES

->

DESPUES (lime.py con deteccion de phantoms)

OK Segmentos mapeados: 8

- Memoria fisica cubierta: 191.64 GB completos

- Stack: primary -> LimeLayer -> FileLayer

- linux.pslist: 504 procesos

OK Analisis forense completo del incidente Oracle 12c

Una modificacion de ~30 lineas en lime.py desbloqueo 191.64 GB de evidencia forense. Diagnostico y fix completados en una sesion de analisis.

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Volatility 3 working!

```
PS C:\Users\ManuelMoreno\Documents\DEV\Memory-Forensic\volatility3-2.28.0\volatility3-2.28.0> python.exe .\vol.py -f C:\Users\ManuelMoreno\Documents\DEV\Memory-Forensic\memdump-2026-04-23.lime linux.pslist
Volatility 3 Framework 2.28.0
Progress:  100.00               Stacking attempts finished
OFFSET (V)      PID     TID     PPID    COMM    UID     GID     EUID    EGID    CREATION TIME   File output

0x95b9c74edd00  1       1       0       systemd 0       0       0       0       2026-03-23 04:56:35.221906 UTC  Disabled
0x95b9c74e8000  2       2       0       kthreadd        0       0       0       0       2026-03-23 04:56:35.221906 UTC  Disabled
0x95b9c74e9f00  3       3       2       rcu_gp  0       0       0       0       2026-03-23 04:56:35.221906 UTC  Disabled
0x95b9c74ebe00  4       4       2       rcu_par_gp      0       0       0       0       2026-03-23 04:56:35.221906 UTC  Disabled
0x95b9c6c1be00  6       6       2       kworker/0:0H    0       0       0       0       2026-03-23 04:56:35.221906 UTC  Disabled
0x95b9c6c18000  8       8       2       kworker/0:1H    0       0       0       0       2026-03-23 04:56:35.221906 UTC  Disabled
0x95b9c6c38000  9       9       2       mm_percpu_wq    0       0       0       0       2026-03-23 04:56:35.221906 UTC  Disabled
0x95b9c6c39f00  10      10      2       ksoftirqd/0     0       0       0       0       2026-03-23 04:56:35.221906 UTC  Disabled
0x95b9c6c3be00  11      11      2       rcu_sched       0       0       0       0       2026-03-23 04:56:35.221906 UTC  Disabled
0x95b9c6c3dd00  12      12      2       migration/0     0       0       0       0       2026-03-23 04:56:35.221906 UTC  Disabled
0x95b9c6eb9f00  14      14      2       cpuhp/0 0       0       0       0       2026-03-23 04:56:35.223906 UTC  Disabled
0x95b9c6ebbe00  15      15      2       cpuhp/1 0       0       0       0       2026-03-23 04:56:35.223906 UTC  Disabled
0x95b9c6ebdd00  16      16      2       migration/1     0       0       0       0       2026-03-23 04:56:35.223906 UTC  Disabled
0x95b9c6eb8000  17      17      2       ksoftirqd/1     0       0       0       0       2026-03-23 04:56:35.223906 UTC  Disabled
0x95b9c6ee0000  19      19      2       kworker/1:0H    0       0       0       0       2026-03-23 04:56:35.223906 UTC  Disabled
0x95b9c6ee1f00  20      20      2       cpuhp/2 0       0       0       0       2026-03-23 04:56:35.268906 UTC  Disabled
0x95b9c6ee3e00  21      21      2       migration/2     0       0       0       0       2026-03-23 04:56:35.268906 UTC  Disabled
0x95b9c6f2dd00  22      22      2       ksoftirqd/2     0       0       0       0       2026-03-23 04:56:35.268906 UTC  Disabled
0x95b9c6f29f00  24      24      2       kworker/2:0H    0       0       0       0       2026-03-23 04:56:35.268906 UTC  Disabled
0x95b9c6f2be00  25      25      2       cpuhp/3 0       0       0       0       2026-03-23 04:56:35.280906 UTC  Disabled
0x95b9c6f68000  26      26      2       migration/3     0       0       0       0       2026-03-23 04:56:35.280906 UTC  Disabled
0x95b9c6f69f00  27      27      2       ksoftirqd/3     0       0       0       0       2026-03-23 04:56:35.280906 UTC  Disabled
0x95b9c6f6dd00  29      29      2       kworker/3:0H    0       0       0       0       2026-03-23 04:56:35.280906 UTC  Disabled
0x95b9c6fa9f00  30      30      2       cpuhp/4 0       0       0       0       2026-03-23 04:56:35.292906 UTC  Disabled
0x95b9c6fabe00  31      31      2       migration/4     0       0       0       0       2026-03-23 04:56:35.292906 UTC  Disabled
0x95b9c6fadd00  32      32      2       ksoftirqd/4     0       0       0       0       2026-03-23 04:56:35.292906 UTC  Disabled
0x95b9c6fd3e00  34      34      2       kworker/4:0H    0       0       0       0       2026-03-23 04:56:35.292906 UTC  Disabled
0x95b9c6fd5d00  35      35      2       cpuhp/5 0       0       0       0       2026-03-23 04:56:35.338906 UTC  Disabled
0x95b9c6fd0000  36      36      2       migration/5     0       0       0       0       2026-03-23 04:56:35.338906 UTC  Disabled
0x95b9c6fd1f00  37      37      2       ksoftirqd/5     0       0       0       0       2026-03-23 04:56:35.338906 UTC  Disabled
0x95b9c680dd00  39      39      2       kworker/5:0H    0       0       0       0       2026-03-23 04:56:35.338906 UTC  Disabled
```

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

02

SECCIÓN

Usando IA Local en DFIR

Analisis Forense a un servidor atacado.

Las consideraciones del uso de IA en DFIR

La información que se maneja en los casos de análisis forense digital son en su amplia mayoría “Investigaciones Privadas” o bajo acuerdos de NDA (contrato de no divulgación), por lo que no se puede usar “ChatGPT” o Claude para decirle algo así como “Analízame estos logs”… pero allí es donde entra la **IA LOCAL**

Se puede usar algún modelo de frontera Cloud para construir las herramientas, **pero la evidencia procesarla con IA LOCAL (OnPremise)** y así evitas enviar datos de tus clientes a un proveedor de IA extranjero.

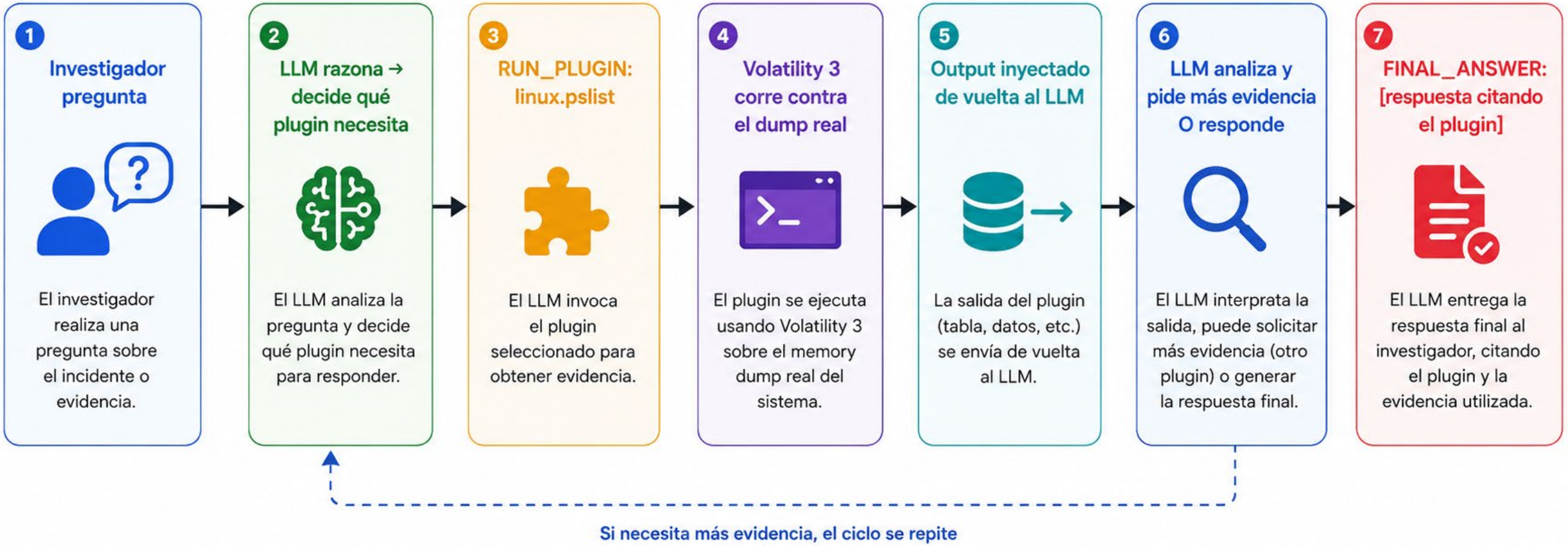
En mi caso estoy usando el modelo QWEN2.5-14b-instruct-1M1m

Pero el modelo se puede ajustar fácilmente si salen nuevos modelos disponibles, lo que permite flexibilidad y rapidez.

https://github.com/GlobalsecureAcademy/Volatility-Local-LLM

Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

Como funciona el agente



Derechos de autor GlobalSecure. Todos los derechos reservados. estrictamente prohibida su reproducción total o parcial.

DEMO TIME!!!!



¡Gracias!

¿Conversamos? Espacio para preguntas.

manuel.moreno@globalsecure.cl **@manu0x01 (Linkedin)** **+5699 300 3432**