



CHARLA MAGISTRAL · TRACK DE IA

Forensic con IA en 2026

● **Manuel Moreno** · CEO · GLOBALSECURE



IA LATAM · Comunidad

Congreso AI LATAM



Manuel Moreno Leiva
CEO & Incident Commander

- 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



Servicios Avanzados

CiberSeguridad Ofensiva

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

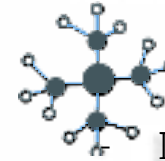


NUESTRA OFERTA DE VALOR



CiberSeguridad Defensiva

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



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



BlueTeam Service

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





CHARLA MAGISTRAL · TRACK DE IA

Forensic con IA en 2026

● **Manuel Moreno** · CEO · GLOBALSECURE



IA LATAM · Comunidad

Congreso AI LATAM

¿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.

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 artefactos colectados (Disco, Memoria, Archivos sospechosos)

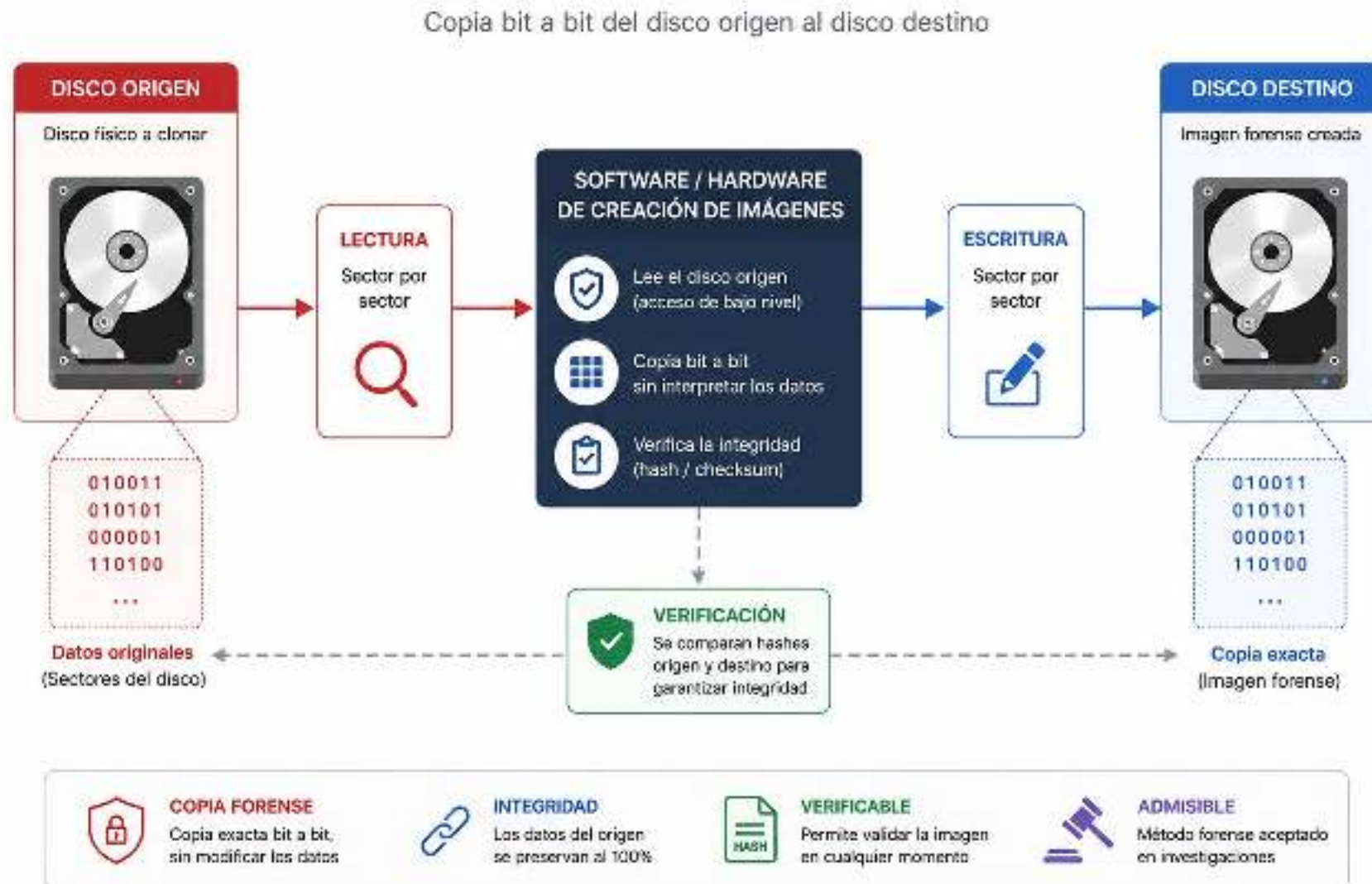
La regla del Forense es:

si esta prendido... **déjalo Prendido**

si esta apagado ... **déjalo apagado** (pero no tenemos RAM ☹)

Qué es la creación de imágenes forenses

Preciso, verificable, reproducible.



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

¿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.

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.

Base de conocimiento

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

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

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 áreas más operativas, colaborando y guiando cada etapa del proceso. Algunas de las responsabilidades de este rol son:

- Definición de la estrategia en el incidente
- Asignación de los distintos roles del equipo
- Definición clave de las evidencias y procesos de triage a realizar en las primeras máquinas.
- Análisis de riesgos para la vuelta a operaciones de forma segura
- Orquestación de los trabajos críticos 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

First Responders

Es un rol clave para el inicio del proceso de respuesta ante incidentes. Es el encargado en activar el proceso o protocolo de respuesta ante incidentes, quien genera las primera notificaciones y quien colecta las primeras evidencias iniciales del incidente. Algunas 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 algún proceso de restauración por parte de tecnología.
- Consultar las consolas de SIEM, EDR, xDR

• Archivos (sin archivos en disco)
• Aplicaciones en tiempo real (funciones, comandos, credenciales en uso)
• Evidencia que no queda registrada en los logs
• Evidencia que no queda registrada en el disco

¿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

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!

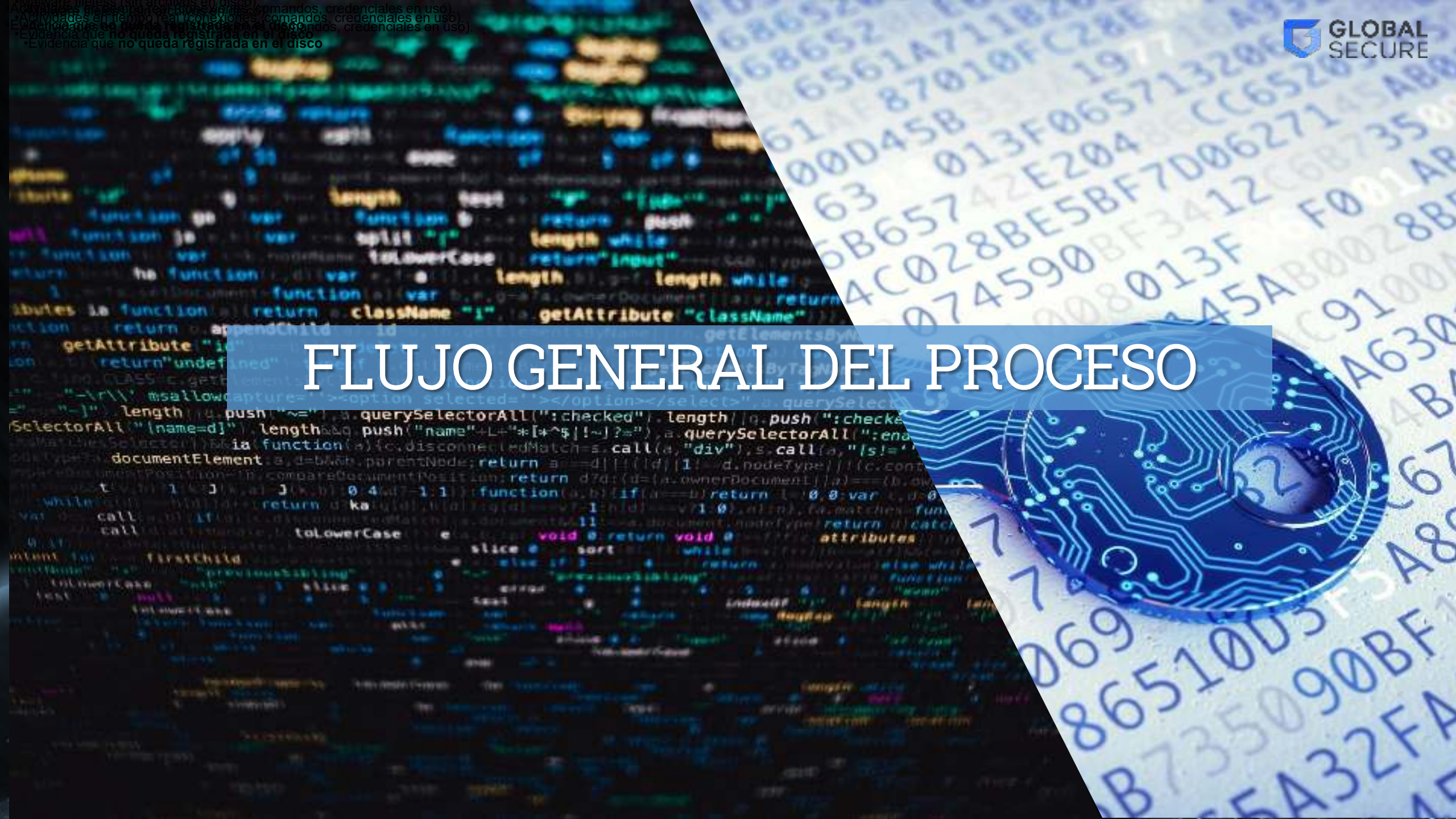
- Don'ts of Incident Response
 - Do Not Turn Off The System
 - Do Not Immediately Disconnect From Network
 - Do Not Run Anti-Virus Programs
 - Changes last-access time of virtually every file
 - Forces system log rotation
 - Do Not Run Registry Or File Cleaner Programs
 - Do Not Install Or Run Any Additional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

-Archivos (sin archivos en disco)
 -Comandos, credenciales en uso)
 -Evidencia que no queda registrada en el disco
 -Comandos, credenciales en uso)
 -Evidencia que no queda registrada en el disco

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

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?

• Archivos (sin archivos en disco)
• Aplicaciones en tiempo real (comandos, credenciales en uso)
• Evidencia que no queda registrada en los logs
• Evidencia que no queda registrada en el disco

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.
- filesan, dumpfiles → recuperación de archivos desde memoria.

Volatility framework 2

```
root@ZeusOS:~# volatility -f DMZ-Server1x64.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO      : volatility.debug      : Determining profile based on KDBG search...
           Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64,
Win7SP1x64_24000, Win7SP1x64_23418
           AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
           AS Layer2 : FileAddressSpace (/root/DMZ-Server1x64.vmem)
           PAE type  : No PAE
           DTB       : 0x187000L
           KDBG      : 0xf800019fa070L
           Number of Processors : 2
           Image Type (Service Pack) : 0
           KPCR for CPU 0 : 0xffffffff800019fbd00L
           KPCR for CPU 1 : 0xffffffff880009bf000L
           KUSER_SHARED_DATA : 0xffffffff78000000000L
           Image date and time : 2018-07-24 05:25:07 UTC+0000
           Image local date and time : 2018-07-24 02:25:07 -0300
root@ZeusOS:~#
```

Volatility framework 2

```

root@ZeusOS:~# volatility -f DMZ-Server1x64.vmem --profile=Win2008R2SP1x64 netscan
Volatility Foundation Volatility Framework 2.6
Offset(P)      Proto  Local Address      Foreign Address    State      Pid      Owner      Created
0xb96d380      UDPv4  0.0.0.0:0          *:.*               *          268      powershell.exe 2018-07-24 03:44:13 UTC+0000
0xe594160      TCPv4  172.16.59.100:49587 52.38.51.83:80     CLOSED     1260     powershell.exe 2018-07-24 03:44:16 UTC+0000
0xf2a1ec0      UDPv4  0.0.0.0:0          *:.*               *          268      powershell.exe 2018-07-24 03:44:16 UTC+0000
0xf2a1ec0      UDPv6  :::0              *:.*               *          268      powershell.exe 2018-07-24 03:44:16 UTC+0000
0x1023b7d0     UDPv4  0.0.0.0:0          *:.*               *          268      powershell.exe 2018-07-24 03:44:13 UTC+0000
0x1023b7d0     UDPv6  :::0              *:.*               *          268      powershell.exe 2018-07-24 03:44:13 UTC+0000
0x1ca41010     TCPv4  172.16.59.100:3389 172.16.59.137:50148 ESTABLISHED 2416     svchost.exe
0x22013010     TCPv6  -:0               d868:770d:80fa:ffff:d868:770d:80fa:ffff:0 CLOSED     268      powershell.exe
0x32864780     TCPv6  -:0               68b0:750d:80fa:ffff:68b0:750d:80fa:ffff:0 CLOSED     268      powershell.exe
0x32864cf0     TCPv6  -:0               68b0:750d:80fa:ffff:68b0:750d:80fa:ffff:0 CLOSED     1260     powershell.exe
0x3e2513d0     UDPv6  ac10:3b64::c811:4e0d:80fa:ffff:1812 *:.*          844      svchost.exe 2018-07-24 03:17:20 UTC+0
000
0x3e25fec0     UDPv6  ac10:3b64::c811:4e0d:80fa:ffff:1813 *:.*          844      svchost.exe 2018-07-24 03:17:20 UTC+0
000
0x3e2d3270     UDPv6  fe80::f1c9:fee5:7373:a70:1813 *:.*          844      svchost.exe 2018-07-24 03:17:20 UTC+0000
0x3e2f2010     UDPv4  0.0.0.0:3702      *:.*               *          900      svchost.exe 2018-07-24 05:15:38 UTC+0000
0x3e3d1ec0     UDPv4  0.0.0.0:5353      *:.*               *          3512     chrome.exe 2018-07-24 03:37:32 UTC+0000
0x3e3d2940     UDPv4  0.0.0.0:5353      *:.*               *          3512     chrome.exe 2018-07-24 03:37:32 UTC+0000
0x3e3d2940     UDPv6  :::5353           *:.*               *          3512     chrome.exe 2018-07-24 03:37:32 UTC+0000
0x3e3d4440     UDPv4  0.0.0.0:0         *:.*               *          1260     powershell.exe 2018-07-24 03:45:20 UTC+0000
0x3e438ac0     UDPv4  172.16.59.100:138 *:.*               *          4        System     2018-07-24 03:15:16 UTC+0000
0x3e43a9c0     UDPv4  172.16.59.100:137 *:.*               *          4        System     2018-07-24 03:15:16 UTC+0000
0x3e4585d0     UDPv4  0.0.0.0:0         *:.*               *          996      svchost.exe 2018-07-24 03:15:16 UTC+0000
0x3e4585d0     UDPv6  :::0              *:.*               *          996      svchost.exe 2018-07-24 03:15:16 UTC+0000
0x3e496870     UDPv4  0.0.0.0:59286     *:.*               *          900      svchost.exe 2018-07-24 05:15:38 UTC+0000
0x3e496870     UDPv6  :::59286          *:.*               *          900      svchost.exe 2018-07-24 05:15:38 UTC+0000
0x3e4da010     UDPv4  0.0.0.0:0         *:.*               *          268      powershell.exe 2018-07-24 03:44:16 UTC+0000
0x3e4e4b30     UDPv4  0.0.0.0:0         *:.*               *          2448     svchost.exe 2018-07-24 03:15:17 UTC+0000
0x3e4e6ec0     UDPv4  0.0.0.0:0         *:.*               *          2448     svchost.exe 2018-07-24 03:15:17 UTC+0000
0x3e4e6ec0     UDPv6  :::0              *:.*               *          2448     svchost.exe 2018-07-24 03:15:17 UTC+0000
0x3e50dec0     UDPv4  0.0.0.0:3702      *:.*               *          900      svchost.exe 2018-07-24 05:15:38 UTC+0000
0x3e50dec0     UDPv6  :::3702           *:.*               *          900      svchost.exe 2018-07-24 05:15:38 UTC+0000
0x3e56e5d0     UDPv4  0.0.0.0:3702      *:.*               *          900      svchost.exe 2018-07-24 05:15:38 UTC+0000
0x3e56e5d0     UDPv6  :::3702           *:.*               *          900      svchost.exe 2018-07-24 05:15:38 UTC+0000
0x3e583010     UDPv6  fe80::f1c9:fee5:7373:a70:1812 *:.*          844      svchost.exe 2018-07-24 03:17:20 UTC+0000
0x3e676010     UDPv4  0.0.0.0:500       *:.*               *          844      svchost.exe 2018-07-24 03:15:15 UTC+0000

```


Volatility framework 2

```
root@ZeusOS:~# volatility -f DMZ-Server1x64.vmem --profile=Win2008R2SP1x64 consoles
Volatility Foundation Volatility Framework 2.6
*****
ConsoleProcess: conhost.exe Pid: 1836
Console: 0xff9f6200 CommandHistorySize: 50
HistoryBufferCount: 2 HistoryBufferMax: 4
OriginalTitle: Símbolo del sistema
Title: Símbolo del sistema
-----
CommandHistory: 0x32f780 Application: ipconfig.exe Flags:
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x0
-----
CommandHistory: 0x32df50 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 1 LastAdded: 0 LastDisplayed: 0
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0xc
Cmd #0 at 0x32d4f0: ipconfig
-----
Screen 0x311d90 X:80 Y:300
Dump:
Microsoft Windows [Versi7n 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\globalsecure>ipconfig

Configuraci7n IP de Windows

Adaptador de Ethernet Conexi7n de 7rea local:

    Sufijo DNS espec7fico para la conexi7n. . . : 
    V7nculo: direcci7n IPv6 local. . . . . : fe80::f1c9:fee5:7373:a70%11
    Direcci7n IPv4. . . . . : 172.16.59.100
    M7scara de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada. . . . . : 172.16.59.2

Adaptador de t7nel isatap.{2A122CE8-549C-4265-9E11-15EBEA9EB7A9}:
```

Volatility framework 2

```
root@ZeusOS:~# volatility -f DMZ-Server1x64.vmem --profile=Win2008R2SP1x64 hashdump
Volatility Foundation Volatility Framework 2.6
Administrador:500:aad3b435b51404eeaad3b435b51404ee:bbb31423e81312f30d59736544bf357a:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
globalsecure:1000:aad3b435b51404eeaad3b435b51404ee:347eaa86145c261ff20b477b75fbedc6:::
gppt:1006:aad3b435b51404eeaad3b435b51404ee:cbe177e76e4b8611cecf0fc71ebb536d:::
Gerencia:1007:aad3b435b51404eeaad3b435b51404ee:8e7d3c273c02e09ad194cb01e2988525:::
root@ZeusOS:~#
```

Volatility framework 2

```

/bin/bash
root@Zeus05:~# volatility -f DMZ-Server1x64.vmem --profile-Win2008R2SP1x64 mftparser
Volatility Foundation Volatility Framework 2.6
Scanning for MFT entries and building directory, this can take a while
*****
MFT entry found at offset 0xa000
Attribute: In Use & File
Record Number: 0
Link count: 1

$STANDARD_INFORMATION
Creation              Modified              MFT Altered              Access Date              Type
-----
2015-03-20 23:16:09 UTC+0000 2015-03-20 23:16:09 UTC+0000 2015-03-20 23:16:09 UTC+0000 2015-03-20 23:16:09 UTC+0000 Hidden & System

$FILE_NAME
Creation              Modified              MFT Altered              Access Date              Name/Path
-----
2015-03-20 23:16:09 UTC+0000 2015-03-20 23:16:09 UTC+0000 2015-03-20 23:16:09 UTC+0000 2015-03-20 23:16:09 UTC+0000 $MFT

$DATA

$OBJECT_ID
Object ID: 40000000-0000-0000-0000-d40900000000
Birth Volume ID: 0000d409-0000-0000-0000-d40900000000
Birth Object ID: 33409d00-0000-0c00-b000-000060000000
Birth Domain ID: 01004000-0000-0500-0000-000000000000

*****
MFT entry found at offset 0xa000
Attribute: In Use & Directory
Record Number: 5
Link count: 1

$STANDARD_INFORMATION
Creation              Modified              MFT Altered              Access Date              Type
-----

```


Volatility framework 2

```

/bin/bash
/bin/bash 151x39
root@ZeusOS:~# volatility -f DMZ-Server1x64.vmem --profile=Win2008R2SP1x64 mftparser| grep cmd.exe
Volatility Foundation Volatility Framework 2.6
2015-03-20 23:18:38 UTC+0000 2015-03-20 23:18:38 UTC+0000 2015-03-20 23:18:38 UTC+0000 2015-03-20 23:18:38 UTC+0000 cmd.exe
2015-03-20 23:18:38 UTC+0000 2015-03-20 23:18:38 UTC+0000 2015-03-20 23:18:38 UTC+0000 2015-03-20 23:18:38 UTC+0000 Windows\System32\cmd.exe
root@ZeusOS:~# volatility -f DMZ-Server1x64.vmem --profile=Win2008R2SP1x64 mftparser| grep powershell
Volatility Foundation Volatility Framework 2.6
2015-03-20 23:22:11 UTC+0000 2015-03-20 23:22:11 UTC+0000 2015-03-20 23:22:11 UTC+0000 2015-03-20 23:22:11 UTC+0000 Windows\winsxs\Manifests\amd6
4_microsoft-windows-iis-powershellprovider_31bf3856ad364e35_6.1.7600.16385_none_f7454d6160c30219.manifest
2015-03-20 23:22:13 UTC+0000 2015-03-20 23:22:13 UTC+0000 2015-03-20 23:22:13 UTC+0000 2015-03-20 23:22:13 UTC+0000 Windows\winsxs\Manifests\amd6
4_microsoft.windows.s...powershell-nonmsil_31bf3856ad364e35_6.1.7600.16385_none_fb6a600eef820683.manifest
2015-03-20 23:22:28 UTC+0000 2015-03-20 23:22:28 UTC+0000 2015-03-20 23:22:28 UTC+0000 2015-03-20 23:22:28 UTC+0000 powershell_ise.resources.dll
2015-03-20 23:22:28 UTC+0000 2015-03-20 23:22:28 UTC+0000 2015-03-20 23:22:28 UTC+0000 2015-03-20 23:22:28 UTC+0000 powershell_ise.exe
root@ZeusOS:~#

```

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.

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

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

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

Tipo	Imagen - nombre de la ubicación	Número de evidencia
------	---------------------------------	---------------------

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

COMPUTADORA SELECCIONAR FUENTE DE EVIDENCIA



WINDOWS



MAC



LINUX



CHROMEBOOK

Herramientas Profesionales

FUENTES DE EVIDENCIA

DETALLES DEL CASO

FUENTES DE EVIDENCIA

DETALLES DEL PROCESAMIENTO

- Buscar archivos y copias de seguridad móviles Act
- Decodifique el cifrado basado en archivos
- Añadir palabras clave para buscar
- Extraer texto de archivos (OCR)
- Calcular los hashes y encontrar coincidencias Act
- 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

SELECCIONAR FUENTE DE EVIDENCIA



UNIDAD



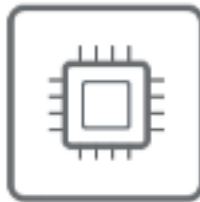
IMAGEN



ARCHIVOS Y CARPETAS



COPIA DE VOLÚMENES DE REDUNDANCIA



MEMORIA



SMFT

Herramientas Profesionales

FUENTES DE EVIDENCIA

DETALLES DEL CASO

FUENTES DE EVIDENCIA

DETALLES DEL PROCESAMIENTO

- Buscar archivos y copias de seguridad móviles Acción
- Decodifique el cifrado basado en archivos
- Añadir palabras clave para buscar
- Extraer texto de archivos (OCR)
- Calcular los hashes y encontrar coincidencias Acción
- 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

Herramientas Profesionales

FUENTES DE EVIDENCIA

DETALLES DEL CASO

FUENTES DE EVIDENCIA

DETALLES DEL PROCESAMIENTO

Buscar archivos y copias de seguridad móviles Ac

Decodifique el cifrado basado en archivos

Añadir palabras clave para buscar

Extraer texto de archivos (OCR)

Calcular los hashes y encontrar coincidencias Ac

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

SELECCIONAR UN PERFIL

Para procesar una imagen de memoria, debe proporcionar el perfil de imagen correcto, en función del número de compilación del sistema operativo.

AXIOM Process puede proporcionar una lista de perfiles de imagen de memoria recomendados, lo que puede tardar un tiempo. También puede seleccionar un perfil manualmente.

☐ Quiero que AXIOM Process proporcione una lista de perfiles de imagen recomendados.

☒ Quiero seleccionar el perfil de imagen yo mismo.

Seleccionar un perfil de imagen. Opcionalmente, también puede proporcionar la dirección de Kernel Debug (KDBG) del perfil para un análisis de memoria más rápido. En Windows 8 +, Volatility informa esta dirección como "KdCopyDataBlock (V)" y, en versiones anteriores de Windows, como "Offset (V)".

Perfil de la imagen Win10x64 19041

Dirección KDBG

Herramientas Profesionales

SELECCIONAR ARTEFACTOS PARA INCLUIRLOS EN EL CASO

DETALLES DEL CASO

FUENTES DE EVIDENCIA

DETALLES DEL PROCESAMIENTO

DETALLES DEL ARTEFACTO

ANALIZAR EVIDENCIA

Buscar archivos y copia de seguridad móviles. An

Demolir el estado basado en archivos

Añadir palabras clave para buscar

Eliminar todos los archivos (OCR)

Calcular los hashes y eliminar redundantes. An

Analizar chats con Magnet.AI

Analizar imágenes con Magnet.AI

Elige qué imágenes ver. VRS

Encuentra más artefactos

Artefactos móviles

Artefactos en la nube

Artefactos informáticos 226

Artefactos de red

Analizar y procesar artefactos

Comando privilegiado

filtro de rango de fechas

ARTEFACTOS INFORMÁTICOS

BORRAR TODO

SISTEMA OPERATIVO

VER TODO

☒ AVANZAMIENTO EN LA NUBE (0 de 0)

☒ ARTEFACTOS PERSONALIZADOS (4 de 5)

☒ ARTEFACTOS VOLÁTILES (1 de 1)

☒ CERRADO Y CREDENCIALES (5 de 4)

☒ COMUNICACIÓN (15 de 20)

☒ CORREO ELECTRÓNICO Y CALENDARIO (13 de 14)

☒ DISPOSITIVOS CONECTADOS (7 de 3)

☒ DOCUMENTOS (15 de 15)

☒ FUENTES ADICIONALES (5 de 4)

☒ HARDWARE (12 de 12)

☒ MEMORIA (21 de 22)

☒ MUNDO A MUNDO (8 de 11)

☒ REDES SOCIALES (5 de 5)

☒ SISTEMA OPERATIVO (68 de 73)

☒ UBICACIÓN Y VIAJES (1 de 1)

☒ USO DE LA APLICACIÓN (8 de 9)

☒ WEB RELACIONADA (11 de 10)

☒ Auténtico. Sistema operativo

☒ Archivos en la nube. Sistema operativo

☒ Banners de inicio de sesión de Windows. Sistema operativo

☐ Paquetes de Windows. Sistema operativo

☒ Cuentas de Apple. Sistema operativo

☒ Cuentas de Android. Sistema operativo

☒ Elementos de escritorio. Sistema operativo

☐ Eventos del sistema de archivos. Sistema operativo

☒ Información del sistema de archivos (APFS). Sistema operativo

☒ Archivos. Sistema operativo

☒ Archivos LNK. Sistema operativo

☒ Bases de datos. Sistema operativo

☒ Bases de datos de publicación. Sistema operativo

☒ Cuentas de Apple. Sistema operativo

☒ Cuentas de Apple. Sistema operativo

☒ Elementos de escritorio. Sistema operativo

☒ Información de inicio de sesión. Sistema operativo

☒ Información del sistema de archivos (APFS). Sistema operativo

☒ Archivos de bloqueo previa. Sistema operativo

☒ Archivos del sistema. Sistema operativo

☒ Bases de datos de usuarios. Sistema operativo

☒ Cuentas de Apple. Sistema operativo

☒ Elementos del Outlook. Sistema operativo

☒ Información de red compartida. Sistema operativo

☒ Información del sistema operativo. Sistema operativo

☒ Archivos de bloqueo previa. Sistema operativo

☒ Archivos de bloqueo de registros. Sistema operativo

☒ Bases de datos. Sistema operativo

☒ Cuentas de Apple. Sistema operativo

☒ Cuentas de usuario. Sistema operativo

☒ iOS Store. Sistema operativo

☒ Pantallas de inicio de sesión. Sistema operativo

☒ Información de zona horaria. Sistema operativo

☒ Información del volumen. Sistema operativo

Buscar en artefactos...

PERFIL: Todos los artefactos

Opciones de perfil

ATRÁS

IR A ANALIZAR Y EXTRAER ARTEFACTOS

ANALIZAR IMÁGENES CON MAGNET.AI

DETALLES DEL CASO

FUENTES DE EVIDENCIA

DETALLES DEL PROCESAMIENTO

DETALLES DEL ARTEFACTO

ANALIZAR EVIDENCIA

Buscar archivos y copias de seguridad móviles Act

Decodifique el cifrado basado en archivos

Añadir palabras clave para buscar

Extraer texto de archivos (OCR)

Calcular los hashes y encontrar coincidencias Act

Analizar chats con Magnet.AI

Analizar imágenes con Magnet.AI

Búsqueda con reglas YARA

Encontrar más artefactos

Artefactos móviles

Artefactos en la nube

Artefactos informáticos 226 c

Artefactos del vehículo

Analizar y extraer artefactos

Contenido privilegiado

Filtro de rango de fechas

Cuando analice imágenes con Magnet.AI, AXIOM Examine puede ayudarlo a encontrar imágenes que sean relevantes para su investigación. Magnet.AI procesará todos los archivos de imágenes y elementos que contengan imágenes (por ejemplo, una imagen incrustada en un archivo .docs).

CREAR UNA COMPARACIÓN DE IMÁGENES

En AXIOM Examine, puede encontrar imágenes que son similares a una imagen de referencia de su caso, o puede importar una imagen externa para encontrar imágenes similares.

☐ Crear una comparación de imágenes para permitir encontrar imágenes similares en AXIOM Examine

CATEGORIZAR IMÁGENES CON MAGNET.AI

Puede habilitar las categorías de imágenes para que Magnet.AI las clasifique y etiquete automáticamente en AXIOM Examine.

Las muestras de cuadros de alta resolución opcionales de videos están actualmente [desactivadas](#) [EDITAR](#)

☒ indica categorías que requieren más tiempo de procesamiento.

Habilitado	Categoría	Etiqueta
☐	Capturas de pantalla	
☐	Desnudez (Predeterminado)	
☐	Documentos	
☐	Documentos de identificación	
☐	Drogas	
☐	Edificios (exterior)	
☐	☒ Escritura	
☐	Facturas/recibos	
☐	Ícono	
☐	☒ Rostros humanos	
☐	Vehículos (automóviles/camiones/f	

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

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.Awful.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	Magnet Forensics	15/12/2024 20:11:27	
☐	Win32.Virus.Cmavg.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.Elrod.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	Magnet Forensics	15/12/2024 20:11:27	
☐	Win32.Virus.Green.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.Neqb.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.HemmeticWiper.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	Magnet Forensics	15/12/2024 20:11:27	
☐	Win32.Trojan.IvanWiper.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.Aps...	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	Magnet Forensics	15/12/2024 20:11:26	

ETIQUETAS. PERFILES Y CATEGORÍAS DE MEDIOS

Herramientas Profesionales

Filtros

Fuentes

Artefactos

Tipos de contenido

Perfiles y temas

Etiquetas y categorías

Perfiles

Recursos parciales

Historial de actividades

Tiempo de procesamiento

Categorización de medios

Artefactos multimedia (ML)

Artefactos

EVIDENCIA (60)

Vista de la columna

TODA LA EVIDENCIA 678.137

REFINED RESULTS 2.935

Classified URLs 34

Cloud Services URLs 51

Facebook URLs 70

Google Maps Queries 28

Google Searches 1.476

Identifiers - Device 505

Identifiers - People 131

Locally Attached Files and Folders 487

Malware/Phishing URLs 11

Harvest 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

Site Name	URL	Date/Time	Artifact
Videos de sexo porno gratuitos - RedTube - XXXMo...	https://es.redtube.com/	30-07-2023 16:46	WebKit Browse
Videos porno de Salvajes Transgender: Cogiendo R...	https://es.redtube.com/redtube/transgender	19-07-2023 16:11:16	WebKit Browse
Categorías de video - RedTube	https://es.redtube.com/categories	30-07-2023 16:48:17	WebKit Browse
Free Porn, Sex Videos - HD Porno - XXX Porn Tube - ...	https://es.redtube.com/?page=4	10-07-2023 20:39:11	WebKit Browse
Free Porn, Sex Videos - HD Porno - XXX Porn Tube - ...	https://es.redtube.com/?page=5	30-07-2023 20:38:59	WebKit Browse
Big Tittle Redhead Cougar - RedTube	https://es.redtube.com/102274021	10-07-2023 20:44:35	WebKit Browse
Roxy Sweetheart takes a load of cum in her mouth - ...	https://es.redtube.com/102258671	30-07-2023 20:47:06	WebKit Browse
Free Porn, Sex Videos - HD Porno - XXX Porn Tube - ...	https://es.redtube.com/?page=2	10-07-2023 20:39:27	WebKit Browse
Pretty Ebony African Masseuse Sucking and Fucking...	https://es.redtube.com/102350251	30-07-2023 20:38:54	WebKit Browse
Free Porn, Sex Videos - HD Porno - XXX Porn Tube - ...	https://es.redtube.com/?page=3	10-07-2023 20:37:24	WebKit Browse
Los Videos Porno de Moda - Child's - RedTube	https://es.redtube.com/hot90c-d	30-07-2023 15:38:04	WebKit Browse
Porn Videos Watched History Redtube	https://es.redtube.com/recently_viewed/history	10-07-2023 15:38:24	WebKit Browse
cute shemales one lucky guy - RedTube	https://es.redtube.com/10415591	30-07-2023 15:38:07	WebKit Browse
Transgender Girl Has Swingers Anal Sex - RedTube	https://es.redtube.com/43471091	10-07-2023 15:39:52	WebKit Browse
Hot Trans In Pantyhose Gets Her Sweet Ass Fucked - ...	https://es.redtube.com/48282821	30-07-2023 15:48:57	WebKit Browse
DEVILSTGRLS (1 foto a pelo el bestie trans de su es...	https://es.redtube.com/43242191	10-07-2023 15:50:31	WebKit Browse
Rale Trans Babe Victoria Carvalho Rammed Good By...	https://es.redtube.com/48425331	30-07-2023 15:53:29	WebKit Browse
GenderXtreme - Cute animadora trans colada claved...	https://es.redtube.com/43237221	10-07-2023 16:09:10	WebKit Browse
STELLA COX HAS HOT DOUBLE PENETRATION SEX...	https://es.redtube.com/premium/1928651113from-...	30-07-2023 16:08:06	WebKit Browse
Trans Hischer Fucked Hardcore - RedTube	https://es.redtube.com/43293001	10-07-2023 16:09:50	WebKit Browse
Emma Rose Uses Alluring Cock To Tempt Handyman...	https://es.redtube.com/48275831	30-07-2023 16:08:27	WebKit Browse
Peruana callejera es pillada por noble joven de provi...	https://es.redtube.com/412393001	10-07-2023 16:21:13	WebKit Browse
Esta Venezolana Estaba Tan Caliente Que Me Pidió...	https://es.redtube.com/40485701	30-07-2023 16:25:13	WebKit Browse
Empleada venezolana de nalgas enormes - RedTube	https://es.redtube.com/42562971	10-07-2023 16:40:16	WebKit Browse
ME CORRÍ DENTRO DE UNA LATINA CALIENTE - Ro...	https://es.redtube.com/40745141	30-07-2023 16:40:08	WebKit Browse
NOVIA ARGENTINA LE ACABÓ EN LA CARA PORO N...	https://es.redtube.com/15301501	10-07-2023 16:40:00	WebKit Browse
Tinder no faltó y me trae a una zona que le encanta...	https://es.redtube.com/40822391	30-07-2023 16:40:01	WebKit Browse
A Tight Cressie, Juicy Ass & Big Natural Tits - Aria Ka...	https://es.redtube.com/premium/435195631	10-07-2023 16:35:56	WebKit Browse
Refrescos vendidos de noche colados en las calles de...	https://es.redtube.com/427081801	10-07-2023 16:39:48	WebKit Browse

Peruana callejera es pillada por noble...

yDMZ-RAM.raw

DETALLES

INFORMACIÓN DEL ARTEFACTO

Site Name

URL

Date/Time

Tipo

ID del elemento

Artefacto original

Fuente

Método de recuperación

Fuente binaria

Ubicación

Número de evidencia

Peruana callejera es pillada por noble joven de provincia - RedTube

https://es.redtube.com/41239381

30-07-2023 16:23:13

Pornography URLs

67904

WebKit Browser Web History (Carved)

GatewayDMZ-RAM.raw

Método de recuperación

Fuente binaria

File Offset 52640139479

GatewayDMZ-RAM.raw

ETIQUETAS, PERFILES Y CATEGORÍAS DE MEDIOS

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

Herramientas Profesionales



03-09-1969 5:09:22 - 02-12-2035 19:35:35

IR A LA FECHA

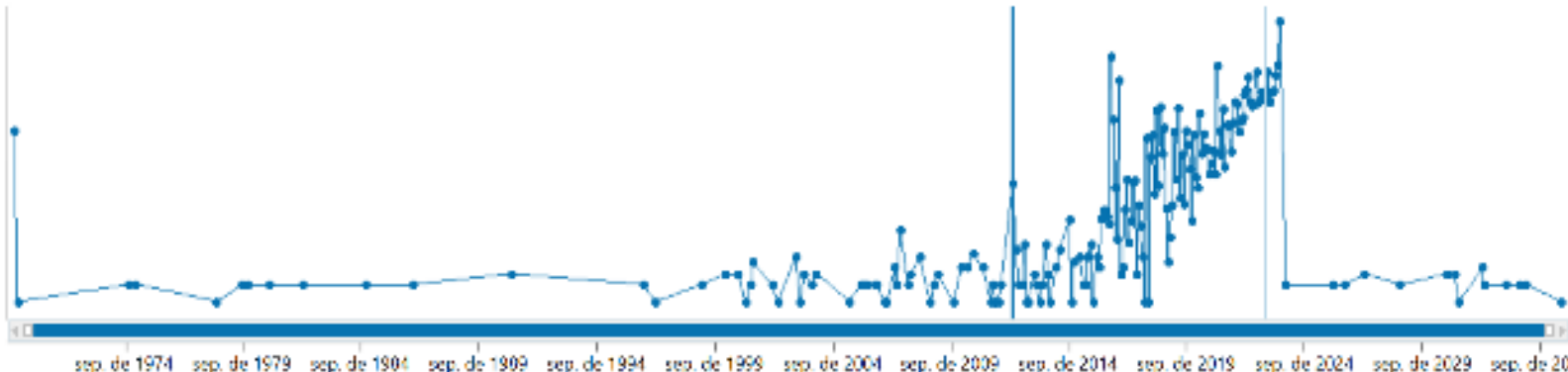


ZOOM



— AÑOS +

PÁGINA



\\192.168.1.186\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/carpetas	Operating System	LNK Files	Linked Path
22-05-2012 0:00:00	Start Date/Time	Evento del usuario	Memory	Timeline (timeline)	Start Date/Time - UTC (yyyy-mm-dd)
22-05-2012 0:00:00	Start Date/Time	Evento del usuario	Memory	Timeline (timeline)	Start Date/Time - UTC (yyyy-mm-dd)
22-05-2012 0:00:00	Start Date/Time	Evento del usuario	Memory	Timeline (timeline)	Start Date/Time - UTC (yyyy-mm-dd)
22-05-2012 0:00:00	Start Date/Time	Evento del usuario	Memory	Timeline (timeline)	Start Date/Time - UTC (yyyy-mm-dd)
22-05-2012 0:00:00	Start Date/Time	Evento del usuario	Memory	Timeline (timeline)	Start Date/Time - UTC (yyyy-mm-dd)
22-05-2012 0:00:00	Start Date/Time	Evento del usuario	Memory	Timeline (timeline)	Start Date/Time - UTC (yyyy-mm-dd)
22-05-2012 0:00:00	Start Date/Time	Evento del usuario	Memory	Timeline (timeline)	Start Date/Time - UTC (yyyy-mm-dd)
22-05-2012 0:00:00	Start Date/Time	Evento del usuario	Memory	Timeline (timeline)	Start Date/Time - UTC (yyyy-mm-dd)
22-05-2012 0:00:00	Start Date/Time	Evento del usuario	Memory	Timeline (timeline)	Start Date/Time - UTC (yyyy-mm-dd)

\\192.168.1.186\Traspaso\CorreoSaliente...

GatewayDMZ-RAM.raw

DETALLES

INFORMACIÓN DEL ARTEFACTO

Linked Path	\\192.168.1.186\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	00:50:56:80:00:00
Target File Size (Bytes)	148
Tipo	LNK Files
ID del elemento	34966

INFORMACIÓN DE EVIDENCIA

Fuente	GatewayDMZ-RAM.raw
Método de recuperación	Moldeado
Fuente barrida	
Ubicación	File Offset 26819206464

ETIQUETAS, PERFILES Y CATEGORÍAS DE MEDIOS

01

— SECCIÓN

Presentación del Caso

Analisis Forense a un servidor atacado.



A photograph of Mike Tyson in a boxing ring, wearing red gloves and black trunks with an American flag patch. He is in a fighting stance, looking down at his opponent who is on the ground. The background is dark with some lights.

Ransomware Gang

**"EVERYONE HAS
A PLAN 'TILL THEY
GET PUNCHED
IN THE MOUTH."**

MIKE TYSON



Servidor Comprometido

Servidor Oracle 7.9 con 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”

Obtener la memoria para su análisis

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).

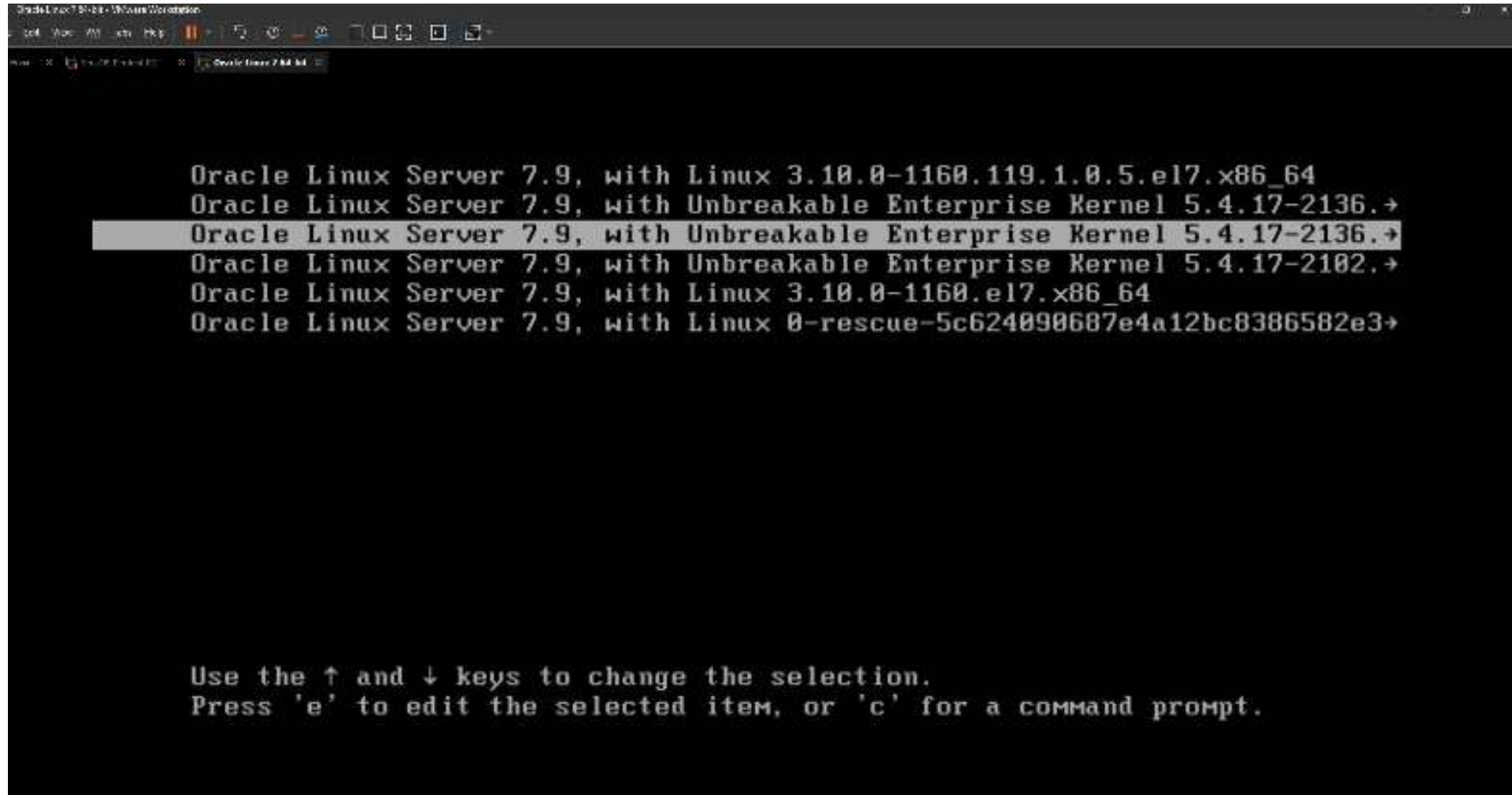
Pasos para crear una replica de un server comprometido

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!

Monte un servidor replica del Kernel



Correr Volatility no daba respuesta

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

```
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>
```



Strings...

Si no existe forma de procesar con Volatility 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/ssh/
/etc/selinux/targeted/active/modules/100/ssh/
- Label .ssh under amanda
- corenet_tcp_bind_all_unreserved_ports(sshd_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
```

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



PDF
(Documento)

Magic Number (Hex)

25	50	44	46
----	----	----	----

ASCII

%PDF



PNG
(Imagen)

Magic Number (Hex)

89	50	4E	67	0D	0A	1A	0A
----	----	----	----	----	----	----	----

ASCII

.PNG....



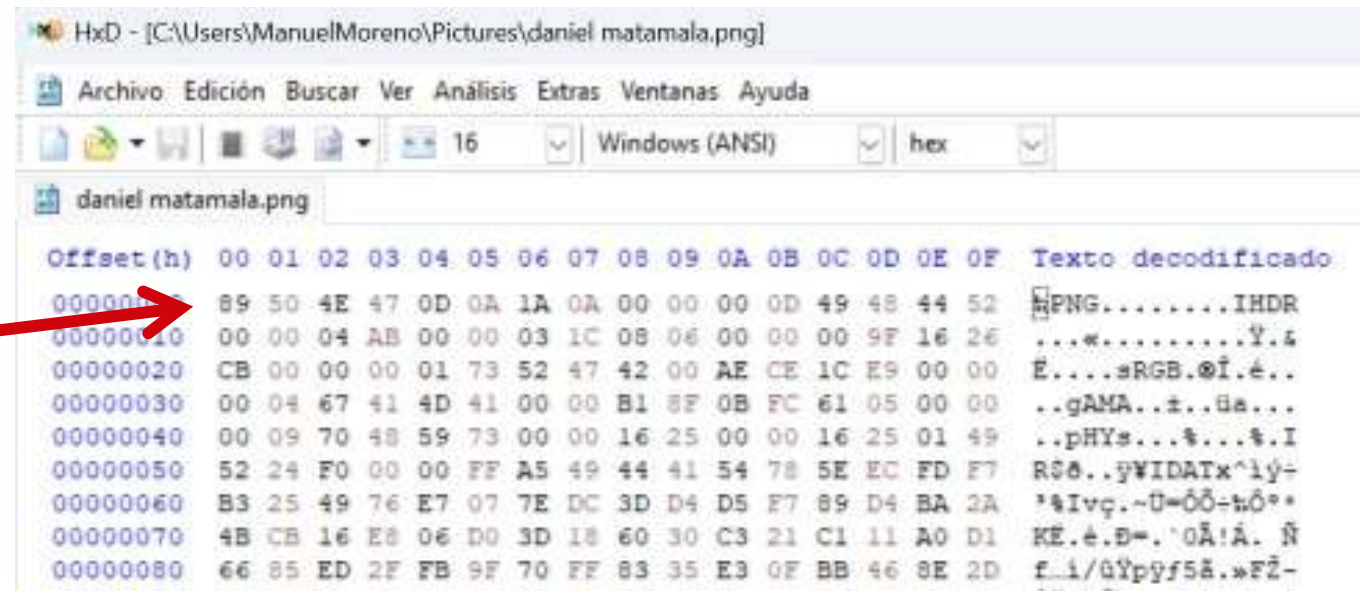
ZIP
(Archivo comprimido)

Magic Number (Hex)

50	4B	03	04
----	----	----	----

ASCII

PK..



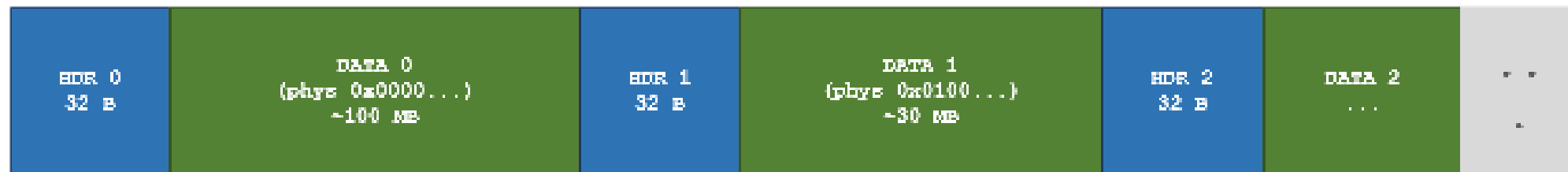
Formato LiME: Estructura Normal

Como Volatility 3 espera encontrar el dump en disco

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

0x40504050 "LiME"	Magic 4 bytes	Version 4 bytes	Phys_Start 8 bytes	Phys_End 8 bytes	Reserved 8 bytes
----------------------	------------------	--------------------	-----------------------	---------------------	---------------------

Cadena de segmentos en el archivo .lime:



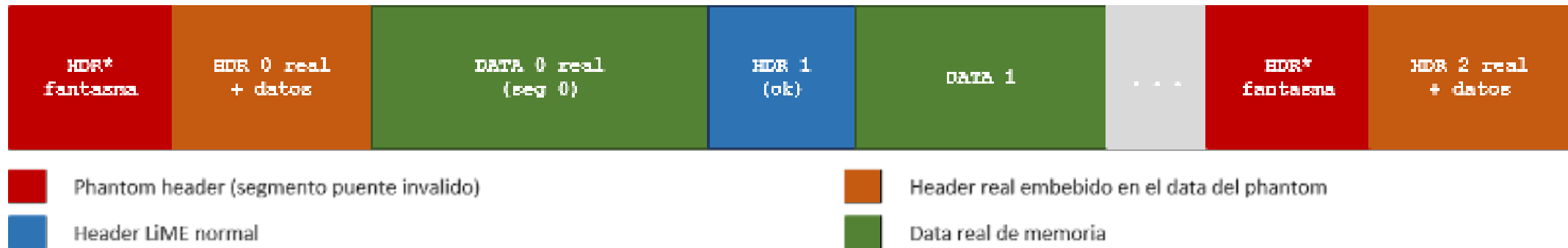
Volatility lee HDR 0 -> calcula `next_offset = 32 + seg_len` -> salta a esa posición -> verifica HDR 1 válido -> continua

Resultado esperado con dump estándar:

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

El Problema: Phantom Headers

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



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 + 12 + seg_len + basura -> salta a una posición 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.

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	2º 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.

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)

Escanear 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

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)
    if 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

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.

Volatility 3 working!

```
PS C:\Users\ManuelMoreno\Documents\DEV\Memory-Forensic\volatility3-2.28.8\volatility3-2.28.8> python.exe .\vol.py -f C:\Users\ManuelMoreno\Documents\DEV\Memory-Forensic\memdump-2026-04-23.lime linux.pslist
Volatility 3 Framework 2.28.8
Progress: 100.0%
OFFSET (V)  PID  TID  PPID  COMM  UID  GID  EUID  EGID  CREATION TIME  File output
0x05b9c740dd80  1    1    0    systemd  0    0    0    0    2026-03-23 04:56:35.221086 UTC Disabled
0x05b9c74e8080  2    2    0    kthreadd  0    0    0    0    2026-03-23 04:56:35.221980 UTC Disabled
0x05b9c74e9f80  3    3    2    rcu_gp  0    0    0    0    2026-03-23 04:56:35.221086 UTC Disabled
0x05b9c74eb080  4    4    2    rcu_par_gp  0    0    0    0    2026-03-23 04:56:35.221980 UTC Disabled
0x05b9c6c1bc80  6    6    2    kworker/8:8H  0    0    0    0    2026-03-23 04:56:35.221086 UTC Disabled
0x05b9c6c18080  8    8    2    kworker/8:1H  0    0    0    0    2026-03-23 04:56:35.221980 UTC Disabled
0x05b9c6c38080  9    9    2    mn_percpu_wq  0    0    0    0    2026-03-23 04:56:35.221086 UTC Disabled
0x05b9c6c39f80  10   10   2    ksoftirqd/0  0    0    0    0    2026-03-23 04:56:35.221980 UTC Disabled
0x05b9c6c3bc80  11   11   2    rcu_sched  0    0    0    0    2026-03-23 04:56:35.221086 UTC Disabled
0x05b9c6c3dd80  12   12   2    migration/0  0    0    0    0    2026-03-23 04:56:35.221980 UTC Disabled
0x05b9c6eb9f80  14   14   2    cpuhp/0  0    0    0    0    2026-03-23 04:56:35.223086 UTC Disabled
0x05b9c6ebb080  15   15   2    cpuhp/1  0    0    0    0    2026-03-23 04:56:35.223980 UTC Disabled
0x05b9c6ebdd80  16   16   2    migration/1  0    0    0    0    2026-03-23 04:56:35.223086 UTC Disabled
0x05b9c6eb8080  17   17   2    ksoftirqd/1  0    0    0    0    2026-03-23 04:56:35.223980 UTC Disabled
0x05b9c6e08080  19   19   2    kworker/1:8H  0    0    0    0    2026-03-23 04:56:35.223086 UTC Disabled
0x05b9c6ee1f80  20   20   2    cpuhp/2  0    0    0    0    2026-03-23 04:56:35.208980 UTC Disabled
0x05b9c6e03080  21   21   2    migration/2  0    0    0    0    2026-03-23 04:56:35.268086 UTC Disabled
0x05b9c6f2dd80  22   22   2    ksoftirqd/2  0    0    0    0    2026-03-23 04:56:35.208980 UTC Disabled
0x05b9c6f20f80  24   24   2    kworker/2:8H  0    0    0    0    2026-03-23 04:56:35.268086 UTC Disabled
0x05b9c6f2be80  25   25   2    cpuhp/3  0    0    0    0    2026-03-23 04:56:35.288980 UTC Disabled
0x05b9c6f68080  26   26   2    migration/3  0    0    0    0    2026-03-23 04:56:35.288086 UTC Disabled
0x05b9c6f09f80  27   27   2    ksoftirqd/3  0    0    0    0    2026-03-23 04:56:35.288980 UTC Disabled
0x05b9c6f6dd80  29   29   2    kworker/3:8H  0    0    0    0    2026-03-23 04:56:35.288086 UTC Disabled
0x05b9c6fa9f80  30   30   2    cpuhp/4  0    0    0    0    2026-03-23 04:56:35.292980 UTC Disabled
0x05b9c6fab080  31   31   2    migration/4  0    0    0    0    2026-03-23 04:56:35.292086 UTC Disabled
0x05b9c6fadd80  32   32   2    ksoftirqd/4  0    0    0    0    2026-03-23 04:56:35.292980 UTC Disabled
0x05b9c6fd3080  34   34   2    kworker/4:8H  0    0    0    0    2026-03-23 04:56:35.292086 UTC Disabled
0x05b9c6fd5d80  35   35   2    cpuhp/5  0    0    0    0    2026-03-23 04:56:35.338980 UTC Disabled
0x05b9c6fd8080  36   36   2    migration/5  0    0    0    0    2026-03-23 04:56:35.338086 UTC Disabled
0x05b9c6fd1f80  37   37   2    ksoftirqd/5  0    0    0    0    2026-03-23 04:56:35.338980 UTC Disabled
0x05b9c680dd80  39   39   2    kworker/5:8H  0    0    0    0    2026-03-23 04:56:35.338086 UTC Disabled
```

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>

Como funciona el agente



”

DEMO TIME!!!!





¡Gracias!

¿Conversamos? Espacio para preguntas.

manuel.moreno@globalsecure.cl [@manu0x01 \(Linkedin\)](#) +5699 300 3432

