

# EQUIPO FORENSE

# ORACLE



PROYECTO:

Confianza23

# ÍNDICE

<b>RECURSOS.....</b>	<b>3</b>
<b>ESTRUCTURA.....</b>	<b>6</b>
<b>DÍA 1.....</b>	<b>9</b>
1. Investigación y documentación de los fundamentos del análisis forense digital.....	9
2. Identificación de las leyes y normativas relevantes (RGPD, etc.).....	10
3. Elaboración de un plan de proyecto detallado, incluyendo objetivos, alcance y metodología.....	10
4. Preparación del entorno de laboratorio virtualizado con Windows Server 2012, Oracle 12c y Kaspersky.....	12
<b>DÍA 2.....</b>	<b>14</b>
1. Investigación y documentación de las herramientas forenses necesarias (Autopsy, Volatility, etc.)....	14
2. Creación de una lista de verificación para la adquisición y preservación de evidencia digital.....	18
<b>DÍA 3.....</b>	<b>20</b>
1. Adquisición de imágenes forenses de los discos duros del servidor utilizando.....	20
2. Cálculo de hashes (MD5, SHA-1) para verificar la integridad de las imágenes.....	22
<b>DÍA 4.....</b>	<b>23</b>
1. Adquisición de la memoria RAM del servidor.....	23
2. Análisis inicial de la memoria RAM con herramientas como Volatility.....	25
<b>DÍA 5.....</b>	<b>27</b>
1. Análisis del sistema de archivos con Autopsy, identificando archivos eliminados, modificados o sospechosos.....	27
2. Recuperación de archivos eliminados y análisis de sus metadatos.....	29
3. Análisis de Registros de Eventos en Windows.....	30
<b>DÍA 6.....</b>	<b>32</b>
1. Análisis de los registros de la base de datos Oracle 12c para identificar accesos no autorizados o modificaciones de datos.....	32
2. Análisis de los registros del antivirus Kaspersky Endpoint Security para identificar detecciones de malware o intrusiones.....	34
3. Análisis de los logs de acceso del sistema operativo, para poder determinar si ha habido usuarios que han accedido de forma remota al sistema.....	35
<b>DÍA 7.....</b>	<b>36</b>
1. Análisis de la línea de tiempo para reconstruir la secuencia de eventos.....	36
2. Correlación de los hallazgos de diferentes fuentes de evidencia.....	37
3. Investigación de los procesos activos del sistema, para poder determinar si existe algún proceso malicioso activo.....	37
<b>DÍA 8.....</b>	<b>39</b>
1. Análisis de la red, para la detección de posibles conexiones no autorizadas.....	39

2. Análisis de las posibles vulnerabilidades del sistema operativo y de la base de datos.....	41
3. Análisis de los usuarios y grupos del sistema operativo y de la base de datos, para poder determinar si existe alguna cuenta de usuario no autorizada.....	42

# RECURSOS

- ❖ Hypervisor VirtualBox 7.1.6 o VMware Workstation Player 17 para desplegar el sistema operativo y la base de datos.
  - ★ <https://www.virtualbox.org/wiki/Downloads>
  - ★ <https://blogs.vmware.com/workstation/2024/05/vmware-workstation-pro-now-available-free-for-personal-use.html>
- ❖ Licencia de Windows 2012 Server (o evaluación)
  - ★ <https://www.microsoft.com/es-es/evalcenter/download-windows-server-2012-r2>
- ❖ Oracle 12c 32 bits
  - ★ <https://docs.oracle.com/en/database/oracle/oracle-database/12.2/index.html>
  - ★ <https://oracledba.net/client/installation/windows/7/oracle/12.1/>
  - ★ <https://www.oracle.com/es/database/technologies/instant-client/microsoft-windows-32-downloads.html>
  - ★ [https://www.oracle.com/es/database/technologies/oracle-database-software-downloads.html#db\\_ee](https://www.oracle.com/es/database/technologies/oracle-database-software-downloads.html#db_ee)
- ❖ Kaspersky Endpoint Security v12.3.0.493
  - ★ <https://support.kaspersky.com/help/KESWin/12.3/es-ES/256811.htm>
- ❖ Autopsy
  - ★ <https://www.autopsy.com/download/>

- ❖ Volatility
  - ★ <https://github.com/volatilityfoundation/volatility>
- ❖ Wireshark
  - ★ <https://www.wireshark.org/download.html>
- ❖ Nmap.
  - ★ <https://nmap.org/>
- ❖ Herramientas de análisis de registros de eventos de Windows.
  - ★ <https://learn.microsoft.com/es-es/windows/win32/etw/event-tracing-tools>
  - ★ <https://learn.microsoft.com/es-es/defender-endpoint/event-error-codes>
- ❖ Herramientas de análisis de registros de auditoría de Oracle: Oracle Database proporciona capacidades de auditoría que registran las actividades realizadas en la base de datos. El análisis de estos registros es crucial para el análisis forense.
  - ★ <https://docs.oracle.com/es-ww/iaas/logging-analytics/doc/oracle-database-audit-analysis.html>
- ❖ Herramientas de análisis de registros de Kaspersky.
  - ★ <https://support.kaspersky.com/KESWIN/12.1/es-ES/199173.htm>
- ❖ Oracle SQL Developer
  - ★ <https://www.oracle.com/database/sqldeveloper/>
    - Esta es una herramienta gratuita proporcionada por Oracle. Es un entorno de desarrollo integrado (IDE) que facilita el desarrollo y la administración de bases de datos Oracle. Permite ejecutar consultas SQL, explorar

esquemas de bases de datos y analizar datos. Es muy útil para examinar el contenido de las tablas de la base de datos y realizar búsquedas de datos específicos.

**NOTA:** HeidiSQL no está soportada para Oracle pero otros entornos sí lo están como por ejemplo TOAD for Oracle (Quest software), SquirrelSQL, Apache OpenOffice Base, etc.

SQLcl (SQL Developer Command Line):

- ❖ También de Oracle, es una interfaz de línea de comandos moderna para Oracle Database. Permite ejecutar scripts SQL y realizar tareas de administración de bases de datos desde la línea de comandos. Puede ser útil para automatizar tareas de análisis y extracción de datos.

★ <https://docs.oracle.com/en/database/oracle/sql-developer-command-line/22.2/sqcup-working-sqlcl.html>

- ❖ ***Oracle Instant Client:***

- ❖ Proporciona las bibliotecas necesarias para que las aplicaciones se conecten a bases de datos Oracle. Aunque no es una herramienta de análisis en sí misma, es un componente esencial para que otras herramientas puedan conectarse a la base de datos. Este paquete proporciona SQL plus, que es una herramienta muy útil para la realización de consultas SQL.

★ <https://www.oracle.com/database/technologies/instant-client/downloads.html>

- ❖ Para poder realizar un análisis de los logs de auditoría, se podrán utilizar herramientas de análisis de ficheros de texto, como por ejemplo, notepad ++, o herramientas de análisis de logs como logparser de Microsoft.

★ <https://techcommunity.microsoft.com/blog/exchange/introducing-log-parser-studio/601131>

# ESTRUCTURA

## *Fase 1: Planificación y Preparación (Jornadas 1-2)*

- **Día 1:**
  - o Investigación y documentación de los fundamentos del análisis forense digital.
  - o Identificación de las leyes y normativas relevantes (RGPD, etc.).
  - o Elaboración de un plan de proyecto detallado, incluyendo objetivos, alcance y metodología.
  - o Preparación del entorno de laboratorio virtualizado con Windows Server 2012, Oracle 12c y Kaspersky.
- **Día 2:**
  - o Investigación y documentación de las herramientas forenses necesarias (Autopsy, Volatility, etc.).
  - o Creación de una lista de verificación para la adquisición y preservación de evidencia digital.
  - o Configuración de las herramientas forenses en el entorno de laboratorio.
  - o Creación de un documento donde se indiquen todos los pasos a seguir para la creación de copias forenses de los discos duros virtuales y de la memoria RAM del sistema.

***Fase 2: Adquisición y Preservación de Evidencia (Jornadas 3-4)***

· **Día 3:**

- o Adquisición de imágenes forenses de los discos duros del servidor utilizando
- o Cálculo de hashes (MD5, SHA-1) para verificar la integridad de las imágenes.
- o Documentación detallada del proceso de adquisición y verificación.

· **Día 4:**

- o Adquisición de la memoria RAM del servidor.
- o Análisis inicial de la memoria RAM con herramientas como Volatility.
- o Documentación de los hallazgos iniciales en la memoria RAM.

***Fase 3: Análisis Forense (Jornadas 5-8)***

· **Día 5:**

- o Análisis del sistema de archivos con Autopsy, identificando archivos eliminados, modificados o sospechosos.
- o Recuperación de archivos eliminados y análisis de sus metadatos.
- o Análisis de los registros de eventos de Windows para identificar actividades sospechosas.

· **Día 6:**

- o Análisis de los registros de la base de datos Oracle 12c para identificar accesos no autorizados o modificaciones de datos.
- o Análisis de los registros del antivirus Kaspersky Endpoint Security para identificar detecciones de malware o intrusiones.

- o Análisis de los logs de acceso del sistema operativo, para poder determinar si a habido usuarios que han accedido de forma remota al sistema.

**Día 7:**

- o Análisis de la línea de tiempo para reconstruir la secuencia de eventos.
- o Correlación de los hallazgos de diferentes fuentes de evidencia.
- o Investigación de los procesos activos del sistema, para poder determinar si existe algún proceso malicioso activo.

**Día 8:**

- o Análisis de la red, para la detección de posibles conexiones no autorizadas.
- o Análisis de las posibles vulnerabilidades del sistema operativo y de la base de datos.
- o Análisis de los usuarios y grupos del sistema operativo y de la base de datos, para poder determinar si existe alguna cuenta de usuario no autorizada.

***Fase 4: Elaboración del Informe (Jornadas 9-10)***

**Día 9:**

- o Redacción del informe forense, incluyendo una descripción detallada de la metodología, los hallazgos y las conclusiones.
- o Elaboración de un resumen ejecutivo con los puntos clave del informe.

**Día 10:**

- o Revisión y corrección del informe forense.
- o Preparación de una presentación para comunicar los hallazgos.
- o Creación de un documento anexo donde se indiquen todas las herramientas utilizadas, con su correspondiente versión.

# **DÍA 1**

## ***1. Investigación y documentación de los fundamentos del análisis forense digital.***

El análisis forense digital es el proceso de identificar, preservar, analizar y presentar evidencia digital de manera que sea admisible en un tribunal.

### **Fundamentos del Análisis Forense Digital:**

#### **1. Principios Básicos**

- ❖ Integridad de la evidencia: Se debe garantizar que los datos originales no sean alterados.
- ❖ Cadena de custodia: Registro documentado de la manipulación de la evidencia.
- ❖ Reproducibilidad: Los procedimientos utilizados deben permitir la replicación de los resultados.
- ❖ Legalidad: Todas las acciones deben estar en conformidad con las leyes vigentes.

#### **2. Fases del Análisis Forense Digital**

- ❖ Identificación: Determinar la ubicación y el tipo de evidencia digital.
- ❖ Adquisición: Extracción segura de la información.
- ❖ Preservación: Garantizar que la evidencia no sea alterada.
- ❖ Análisis: Evaluación de los datos utilizando herramientas especializadas.
- ❖ Documentación y reporte: Registro detallado de hallazgos y conclusiones.
- ❖ Presentación: Uso de la evidencia en procedimientos legales o judiciales.

#### **3. Herramientas Utilizadas en el Análisis Forense Digital**

- ❖ Software de adquisición de datos: FTK Imager, EnCase, Autopsy.
- ❖ Ánalisis de discos duros: The Sleuth Kit, X-Ways Forensics.
- ❖ Ánalisis de redes: Wireshark, NetworkMiner.
- ❖ Recuperación de datos eliminados: Recuva, R-Studio.

#### **4. Documentación en el Análisis Forense Digital**

La documentación es fundamental para mantener la validez de la investigación y asegurar que los hallazgos puedan ser utilizados en un juicio. Esta debe incluir:

- ❖ Descripción del caso y objetivos de la investigación.
- ❖ Registro de la cadena de custodia.
- ❖ Metodología utilizada.
- ❖ Resultados obtenidos y su interpretación.
- ❖ Conclusiones y recomendaciones.

## *2. Identificación de las leyes y normativas relevantes (RGPD, etc.).*

- ❖ **Reglamento General de Protección de Datos (RGPD – UE 2016/679):**  
Establece principios y obligaciones en el tratamiento de datos personales en la Unión Europea.
- ❖ **Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD – España):**  
Complementa el RGPD y define directrices específicas para la protección de datos en España.
- ❖ **Convención de Budapest sobre Ciberdelincuencia:**  
Marco internacional para la cooperación en la investigación de delitos informáticos.
- ❖ **Normas ISO/IEC:**
  - ISO/IEC 27037: Directrices para la identificación, recopilación y preservación de evidencias digitales.
  - ISO/IEC 27042 y 27050: Orientaciones para el análisis y presentación de evidencia.
- ❖ **NIST 800-86:**  
Guía para la realización de análisis forense digital en sistemas informáticos.
- ❖ **Directiva NIS2 (UE):**  
Define requisitos de seguridad para la protección de infraestructuras críticas.

## *3. Elaboración de un plan de proyecto detallado, incluyendo objetivos, alcance y metodología.*

### **Objetivos del Proyecto**

- ❖ **Objetivo General:**  
Desarrollar e implementar una metodología forense especializada en entornos Oracle que permita identificar, recolectar y analizar evidencia digital de manera precisa y conforme a las normativas vigentes.
- ❖ **Objetivos Específicos:**
  - Aplicar protocolos que aseguren la integridad y autenticidad de la evidencia.
  - Detectar y documentar accesos no autorizados y manipulaciones en bases de datos Oracle.
  - Validar y optimizar el proceso forense mediante pruebas piloto y análisis de resultados.

## Alcance del Proyecto

### ❖ Aplicación:

Realizar análisis forense en bases de datos Oracle 12c, con especial énfasis en logs de transacciones, auditorías de acceso y configuraciones de seguridad.

### ❖ Entregables:

- Informes técnicos detallados sobre incidentes y vulnerabilidades detectadas.
- Documentación completa de la cadena de custodia y del análisis realizado.
- Protocolos y procedimientos para la extracción y análisis de evidencia digital.

### ❖ Limitaciones:

- Enfoque centrado en entornos Oracle, excluyendo otros sistemas.
- Dependencia de herramientas y recursos específicos para la recolección y análisis forense.

## Metodología a Seguir

### ❖ Fase 1: Investigación y Documentación Inicial

Revisión bibliográfica y análisis de casos de estudio en análisis forense digital, compilación de normativas y estándares.

### ❖ Fase 2: Planificación y Diseño

Definición de objetivos, alcance, recursos y cronograma; diseño de protocolos específicos para la captura y preservación de evidencia en entornos Oracle.

### ❖ Fase 3: Implementación

Configuración de herramientas forenses especializadas y realización de pruebas piloto en entornos controlados, asegurando la extracción de evidencia sin alteraciones.

### ❖ Fase 4: Análisis y Validación

Examen detallado de logs, registros de transacciones y auditorías para identificar accesos no autorizados y manipulaciones, correlacionando eventos mediante técnicas de ciberinteligencia.

### ❖ Fase 5: Documentación y Capacitación

Elaboración de informes técnicos y manuales de uso, y organización de sesiones de capacitación para el equipo involucrado.

### ❖ Gestión del Proyecto:

Uso de metodologías ágiles (por ejemplo, SCRUM) para iteraciones y ajustes continuos, con reuniones periódicas de seguimiento y revisión.

## **4. Preparación del entorno de laboratorio virtualizado con Windows Server 2012, Oracle 12c y Kaspersky.**

### **Configuración del Entorno**

- ❖ **Sistema Operativo:**
  - Windows Server 2012 (o versión equivalente compatible con Oracle).
- ❖ **Base de Datos:**
  - Oracle 12c
- ❖ **Instalación y Requisitos Previos:**
  - Verificar que el hardware y el sistema operativo cumplen con los requisitos mínimos establecidos por Oracle 12c.
  - Aplicar los parches y actualizaciones recomendados.
- ❖ **Configuración Inicial:**
  - Realizar una instalación limpia siguiendo las mejores prácticas.
  - Configurar parámetros iniciales (memoria SGA y PGA, número de procesos, tamaños de archivo, etc.).
- ❖ **Parámetros de Seguridad:**
  - **Autenticación y Control de Acceso:**  
Configurar contraseñas complejas, integración con servicios externos (LDAP, Kerberos) e implementar Oracle Database Vault.
  - **Encriptación:**  
Activar Transparent Data Encryption (TDE) y configurar Oracle Net Services para encriptar comunicaciones.
  - **Auditoría y Monitoreo:**  
Habilitar funciones de auditoría y establecer alertas para detectar comportamientos inusuales.
  - **Hardening:**  
Deshabilitar servicios y cuentas innecesarias, aplicar actualizaciones periódicas.
  - **Software de Seguridad:**  
Implementar soluciones (por ejemplo, Kaspersky) para monitorización en tiempo real y protección contra accesos no autorizados.
- ❖ **Plataforma de Virtualización:**  
Utilizar VMware o VirtualBox para la creación y gestión de entornos de prueba, facilitando la replicación de escenarios y restauración mediante snapshots.

## Pasos de Configuración

### ❖ Instalación y Configuración de Windows Server 2012:

- Crear la máquina virtual, asignando recursos (CPU, RAM, almacenamiento) y configurando la red.
- Instalar Windows Server 2012 siguiendo el asistente de instalación y realizar la configuración post-instalación (red, actualizaciones, seguridad).

### ❖ Implementación de Oracle 12c:

- Instalar Oracle 12c asegurando la activación de auditorías y logs de transacciones.
- Ajustar el software de seguridad para monitorización continua y crear snapshots para facilitar análisis y recuperación.

## **DÍA 2**

### ***1. Investigación y documentación de las herramientas forenses necesarias (Autopsy, Volatility, etc.).***

#### **❖ Kaspersky Endpoint Security v12.3.0.493:**

- Descripción: Protección avanzada contra malware, ransomware y ataques dirigidos.
- Uso: Revisión de registros de amenazas y análisis de modificaciones no autorizadas.
- Proceso de Instalación:
  - Descargar desde el sitio oficial.
  - Ejecutar instalador con privilegios de administrador, seleccionar el tipo de instalación (rápida o personalizada), configurar protección en tiempo real y reiniciar si es requerido.

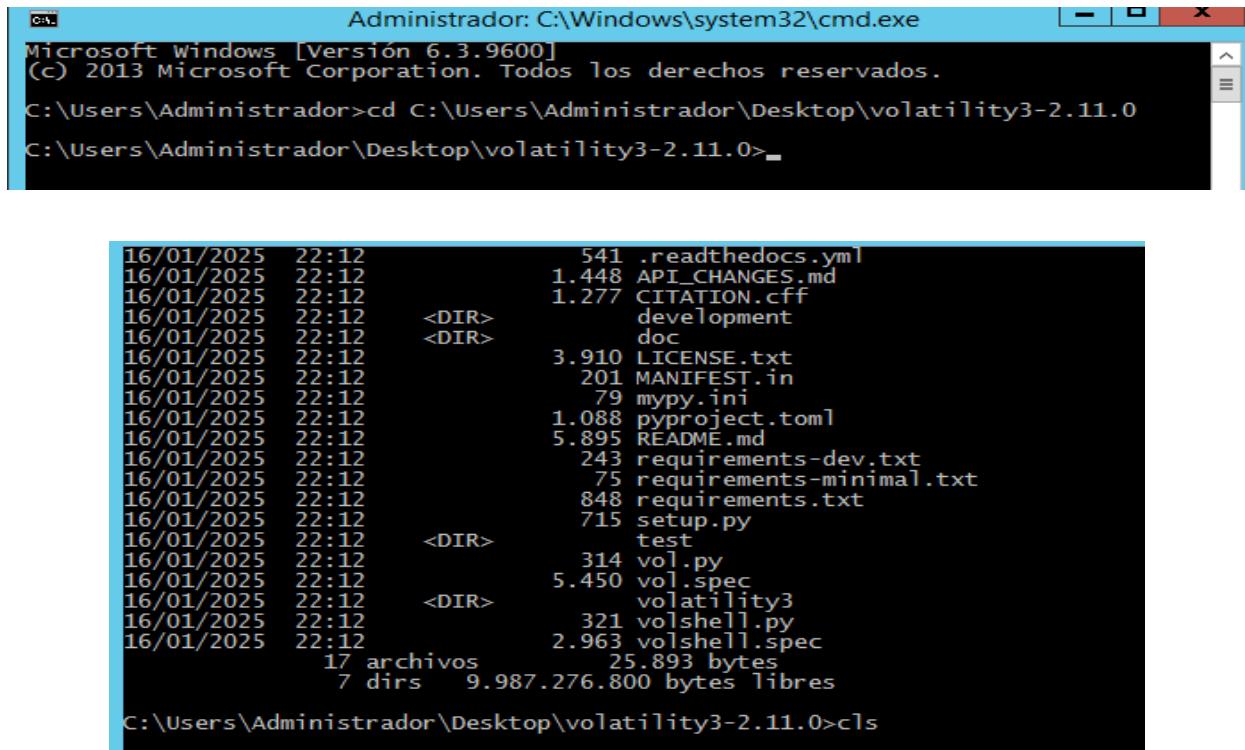
#### **❖ Autopsy:**

- Descripción: Plataforma de código abierto para análisis forense de discos y sistemas de archivos.
- Uso: Examen de discos, recuperación de archivos eliminados y extracción de metadatos.
- Proceso de Instalación:
  - Descargar desde [autopsy.com](http://autopsy.com).
  - Ejecutar instalador (con permisos de administrador) e instalar dependencias (JRE).

#### **❖ Volatility 3:**

- Descripción: Herramienta para análisis de memoria RAM.
- Proceso de Instalación:
  - Descargar desde [volatilityfoundation.org](http://volatilityfoundation.org).
    - <https://github.com/volatilityfoundation/volatility3>
    - <https://downloads.volatilityfoundation.org/volatility3/symbols/windows.zip>
  - Instalar Python 3 y configurar variables de entorno.
  - Descargamos los ficheros en nuestra máquina desde los enlaces arriba marcados. Desde la página oficial de volatility nos llevará hasta un

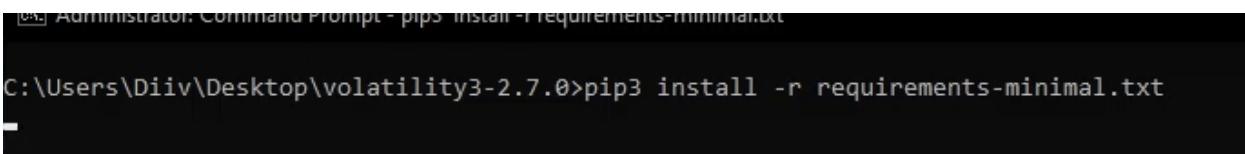
directorio en GitHub, donde tendremos que descargar los ficheros de la aplicación software. Antes de su instalación debemos tener instalado Python. Abrimos el cmd como administrador y copiamos la ruta del directorio descargado de volatility 3.



```
Administrador: C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.3.9600]
(c) 2013 Microsoft Corporation. Todos los derechos reservados.

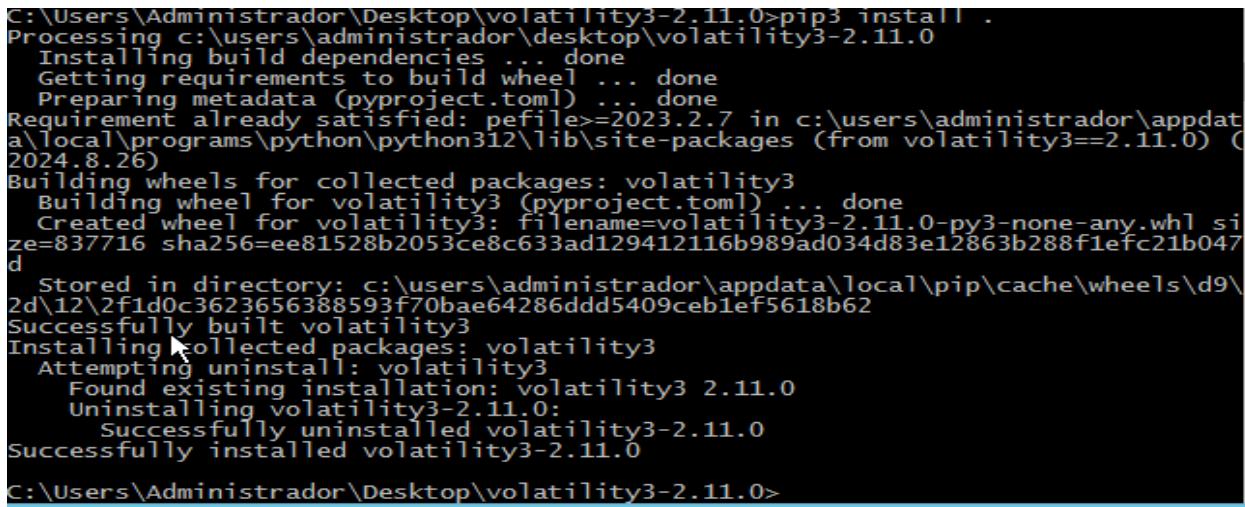
C:\Users\Administrador>cd C:\Users\Administrador\Desktop\volatility3-2.11.0
C:\Users\Administrador\Desktop\volatility3-2.11.0>_

16/01/2025 22:12      541 .readthedocs.yml
16/01/2025 22:12      1.448 API_CHANGES.md
16/01/2025 22:12      1.277 CITATION.cff
16/01/2025 22:12      development
16/01/2025 22:12      doc
16/01/2025 22:12      3.910 LICENSE.txt
16/01/2025 22:12      201 MANIFEST.in
16/01/2025 22:12      79 mypy.ini
16/01/2025 22:12      1.088 pyproject.toml
16/01/2025 22:12      5.895 README.md
16/01/2025 22:12      243 requirements-dev.txt
16/01/2025 22:12      75 requirements-minimal.txt
16/01/2025 22:12      848 requirements.txt
16/01/2025 22:12      715 setup.py
16/01/2025 22:12      test
16/01/2025 22:12      314 vol.py
16/01/2025 22:12      5.450 vol.spec
16/01/2025 22:12      volatility3
16/01/2025 22:12      321 volshell.py
16/01/2025 22:12      2.963 volshell.spec
16/01/2025 22:12      17 archivos      25.893 bytes
                           7 dirs        9.987.276.800 bytes libres
C:\Users\Administrador\Desktop\volatility3-2.11.0>cls
```



```
Administrator: Command Prompt - pip3 install -r requirements-minimal.txt

C:\Users\Diiv\Desktop\volatility3-2.7.0>pip3 install -r requirements-minimal.txt
```



```
C:\Users\Administrador\Desktop\volatility3-2.11.0>pip3 install .
Processing c:\users\administrador\desktop\volatility3-2.11.0
Installing build dependencies ... done
Getting requirements to build wheel ... done
Preparing metadata (pyproject.toml) ... done
Requirement already satisfied: pefile>=2023.2.7 in c:\users\administrador\appdata\local\programs\python\python312\lib\site-packages (from volatility3==2.11.0) (2024.8.26)
Building wheels for collected packages: volatility3
  Building wheel for volatility3 (pyproject.toml) ... done
    Created wheel for volatility3: filename=volatility3-2.11.0-py3-none-any.whl size=837716 sha256=ee81528b2053ce8c633ad129412116b989ad034d83e12863b288f1efc21b047d
    Stored in directory: c:\users\administrador\appdata\local\pip\cache\wheels\d9\2d\12\2f1d0c3623656388593f70bae64286ddd5409ceb1ef5618b62
Successfully built volatility3
Installing collected packages: volatility3
  Attempting uninstall: volatility3
    Found existing installation: volatility3 2.11.0
    Uninstalling volatility3-2.11.0:
      Successfully uninstalled volatility3-2.11.0
Successfully installed volatility3-2.11.0
C:\Users\Administrador\Desktop\volatility3-2.11.0>
```

```
C:\Users\Diiv\Desktop\volatility3-2.7.0>pip3 install .
Processing c:\users\diiv\desktop\volatility3-2.7.0
  Installing build dependencies ... done
    Getting requirements to build wheel ... done
    Preparing metadata (pyproject.toml) ... done
Requirement already satisfied: pefile>=2023.2.7 in c:\program files\python31
Building wheels for collected packages: volatility3
  Building wheel for volatility3 (pyproject.toml) ... done
  Created wheel for volatility3: filename=volatility3-2.7.0-py3-none-any.whl
bb625a809356
  Stored in directory: c:\users\diiv\appdata\local\pip\cache\wheels\23\8f\1d
Successfully built volatility3
Installing collected packages: volatility3
Successfully installed volatility3-2.7.0

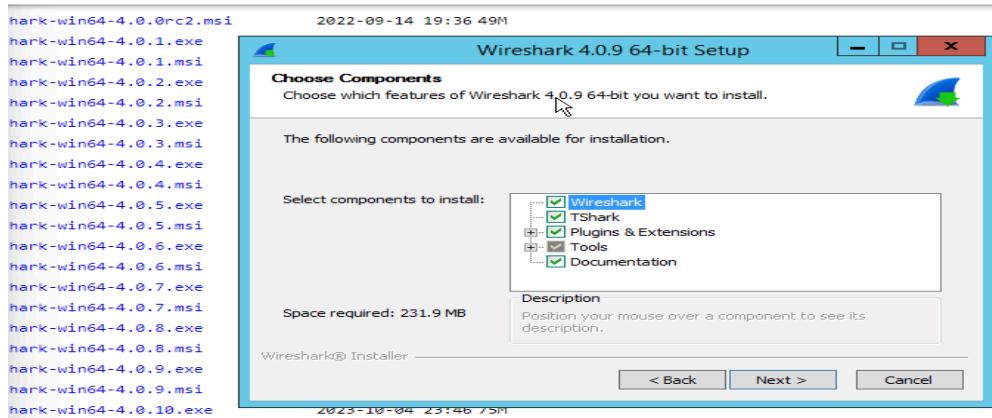
C:\Users\Diiv\Desktop\volatility3-2.7.0>pip3 install -r requirements.txt
```

❖ **Wireshark:**

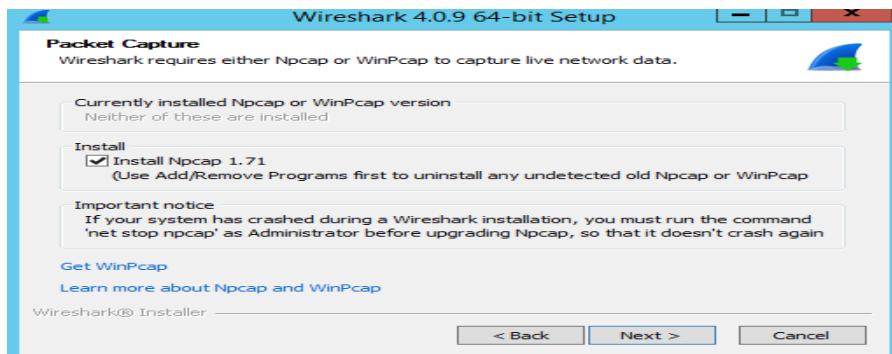
➤ Descripción: Analizador de protocolos de red para captura y análisis de tráfico.

➤ Proceso de Instalación:

- Descargar desde [wireshark.org](https://www.wireshark.org).
- Descargamos la versión 4.0.exe para una instalación más rápida y sencilla.

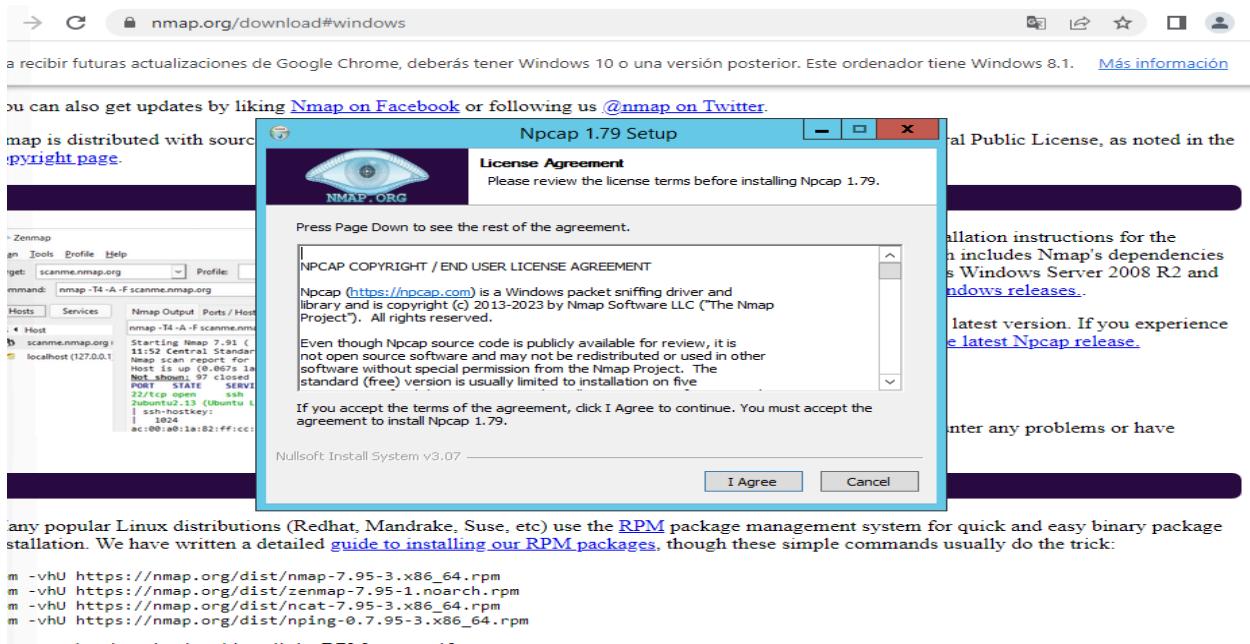


- Ejecutar el instalador, instalar componentes necesarios (WinPcap o Npcap) y reiniciar si es necesario.



❖ **Nmap:**

- Descripción: Herramienta de escaneo de redes para detectar dispositivos y evaluar vulnerabilidades.
- Proceso de Instalación:
  - Descargar desde [nmap.org](https://nmap.org) y ejecutar el instalador.



❖ **Análisis de Registros de Eventos de Windows:**

- Herramientas: Event Viewer (integrado) y Logparser de Microsoft.

❖ **Oracle SQL Developer:**

- Proceso de Instalación:

- Descargar el ZIP desde el sitio de Oracle, extraerlo y ejecutar sqldeveloper.exe.

❖ **Herramientas de Análisis de Archivos de Texto y Logs**

- Ejemplos: Notepad++, Logparser.

## *2. Creación de una lista de verificación para la adquisición y preservación de evidencia digital.*

### ❖ Preparación Inicial:

- Definir objetivos (análisis de malware, fraude, acceso no autorizado, etc.).
- Identificar dispositivos de almacenamiento y sistemas operativos.
- Verificar compatibilidad con herramientas (Autopsy, FTK Imager, EnCase, etc.).
- Asegurar medios de almacenamiento adecuados y deshabilitar conexiones que puedan alterar la evidencia.

### ❖ Preservación y Adquisición en Vivo:

- Registrar configuración de red (ipconfig, netstat, arp).
- Documentar procesos en ejecución (tasklist, wmic).
- Extraer claves de registro y volcar la memoria RAM utilizando herramientas especializadas.

### ❖ Generación y Verificación de Hashes:

- Utilizar herramientas como md5deep, sha256sum o Get-FileHash.
- Documentar y comparar los hashes antes y después de la adquisición.

### ❖ Adquisición de Evidencia Digital:

- Discos Duros: Crear imágenes forenses bit a bit (dd, FTK Imager, Guymager) en formatos E01, DD o AFF.
- Memoria RAM: Extraer mediante Volatility, Rekall o Belkasoft RAM Capturer y generar hash de integridad.
- Archivos y Sistemas de Archivos: Recuperar archivos eliminados y analizar metadatos.
- Registros de Eventos y Logs: Copiar logs de Oracle 12c, Kaspersky y Windows.

### ❖ Documentación de la Cadena de Custodia:

- Registrar fecha, hora, responsable, descripción del hardware/software y ubicación de la evidencia.
- Utilizar formularios estandarizados.

### ❖ Almacenamiento Seguro:

- Cifrar copias con VeraCrypt o BitLocker, guardar en medios de solo lectura y verificar integridad periódicamente.

### ❖ Validación Final:

- Comparar resultados de la adquisición con los registros originales y documentar cualquier inconsistencia.

### ❖ Configuración de Herramientas en el Entorno de Laboratorio:

- Instalar y configurar herramientas (Autopsy, FTK Imager, Volatility, Wireshark) y validar su funcionalidad.
- Configurar Kaspersky en modo pasivo y controles de acceso.

❖ **Procedimiento para la Creación de Copias Forenses:**

- Recolección de información preliminar (identificar discos virtuales, registrar configuraciones, generar hashes).
- Creación de copias forenses mediante herramientas como FTK Imager o dd, verificando integridad mediante hashes.
- Extracción de memoria RAM con herramientas especializadas y documentación detallada.
- Almacenamiento seguro y mantenimiento de la cadena de custodia.

## **DÍA 3**

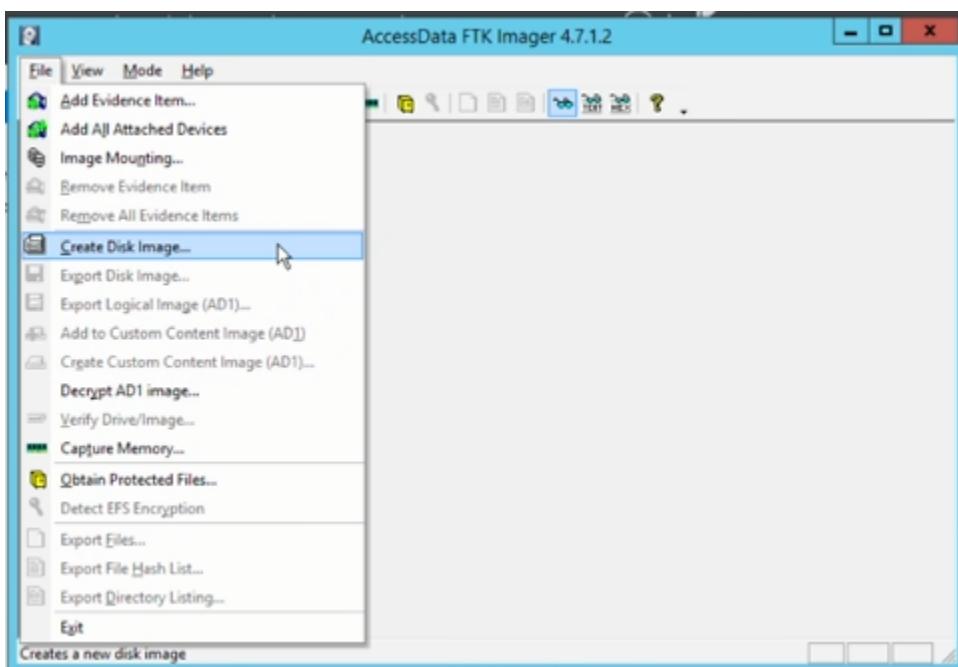
### **1. Adquisición de imágenes forenses de los discos duros del servidor utilizando**

#### **❖ Proceso de adquisición con FTK imager:**

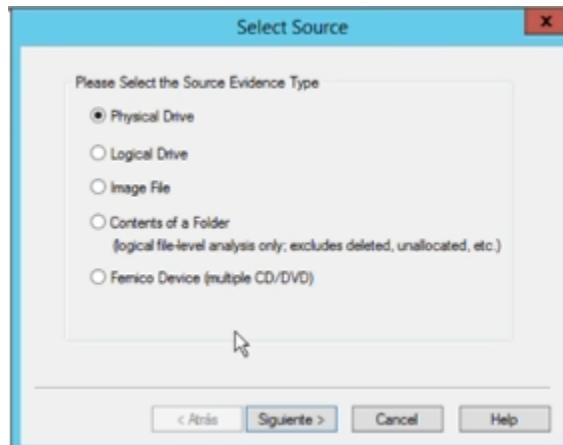
- Descargar FTK Imager
- Ejecutar FTK Imager como administrador.
- Ir a File > Create Disk Image.
- Seleccionar la fuente (Physical Drive o Logical Drive según corresponda).
- Elegir el formato de la imagen (E01 para compresión y metadatos o RAW para una copia exacta).
- Seleccionar la ubicación del destino y asignar un nombre a la imagen.
- Habilitar la opción de calcular hash MD5/SHA-1 durante la adquisición.
- Iniciar el proceso y esperar a que finalice.
- Verificar la integridad de la imagen comparando el hash generado con el original.

#### **❖ Visualización:**

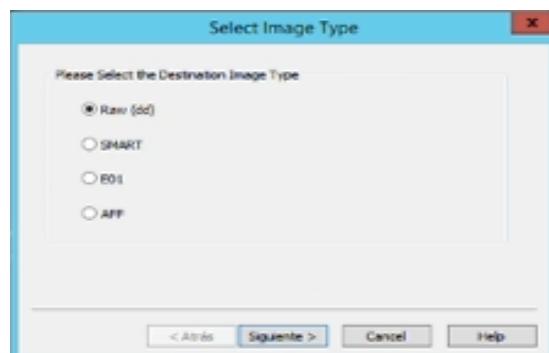
- Ejecutar FTK Imager como Administrador
- Ir File → Create Disk



- Selecciona Fuente Physical Drive



- Elegir el destino (En este Caso Unidad E:)
- Raw (dd) → Formato estándar Forense



- Iniciar Proceso
- Nombre del Archivo: disck\_image
  - Hora: 11:20

## *2. Cálculo de hashes (MD5, SHA-1) para verificar la integridad de las imágenes.*

### ❖ Automático FTK IMAGER

Drive/Image Verify Results	
<input type="checkbox"/>	
Name	disk_image.E01
Sector count	104857600
<input type="checkbox"/> MD5 Hash	
Computed hash	2a52f2efbd656a4f55e5097f3a57695c
Stored verification hash	2a52f2efbd656a4f55e5097f3a57695c
Report Hash	2a52f2efbd656a4f55e5097f3a57695c
Verify result	Match
<input type="checkbox"/> SHA1 Hash	
Computed hash	6dd756ed0ea22327ef5cc7ab8436eca2ce2d
Stored verification hash	6dd756ed0ea22327ef5cc7ab8436eca2ce2d

### ❖ Manualmente utilizando HashCalc o CertUtil de Windows:

- CertUtil -hashfile imagen.E01 MD5
- CertUtil -hashfile imagen.E01 SHA1

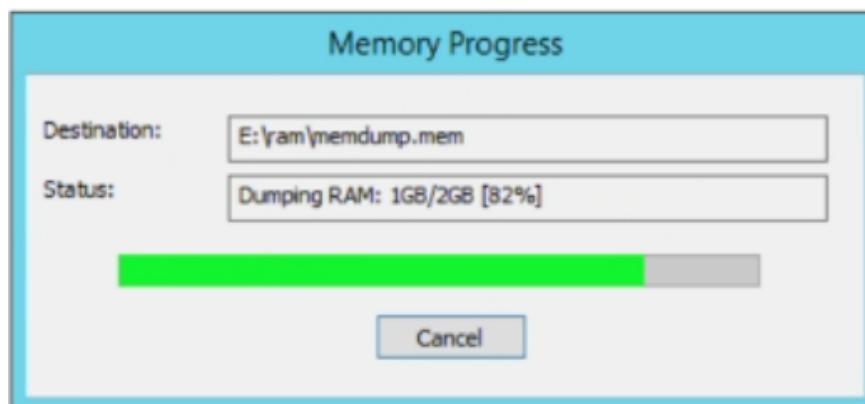
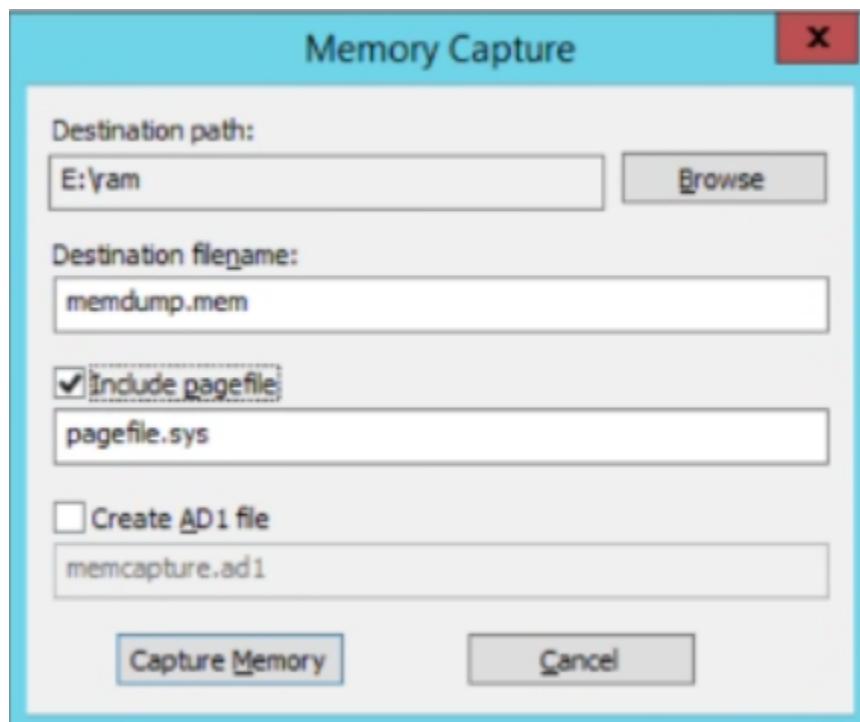
# DÍA 4

## *1. Adquisición de la memoria RAM del servidor.*

### ❖ *Adquisición con FTK Imager*

#### ➤ *Captura de memoria RAM*

- Ejecutar FTK imager como administrador
- Ve a File → Capture Memory.
- Selecciona la unidad donde guardarás la imagen (preferiblemente un disco externo).
- Guarda el archivo como .mem (ej: servidor\_memoria.mem).



❖ **Verificación**

- Guarda el hash generado como archivo de texto

The screenshot shows a Windows Notepad window with the title bar "memcapture.ad1: Bloc de notas". The menu bar includes "Archivo", "Edición", "Formato", "Ver", and "Ayuda". Below the menu is the text "Created By AccessData® FTK® Imager 4.7.1.2". The main content area contains the following text:

```
Case Information:  
Case Number:  
Evidence Number:  
Unique Description:  
Examiner:  
Notes:  
-----  
Information for E:\ram\memcapture.ad1:  
[Computed Hashes]  
MD5 checksum: 7439b97d09825f26144a82516d208140  
SHA1 checksum: 47f9a272ed95975da2582f4879ad415fd91f406c  
Image information:  
Acquisition started: Wed Mar 26 10:10:26 2025  
Acquisition finished: Wed Mar 26 10:11:38 2025  
Segment list:  
E:\ram\memcapture.ad1
```

## 2. Análisis inicial de la memoria RAM con herramientas como Volatility.

### ❖ Acciones iniciales en el análisis con Volatility:

- Determinar el perfil del sistema (SO, arquitectura, versión):
  - **volatility -f memoria.dmp imageinfo**
- Extraer procesos en ejecución:
  - **volatility -f memoria.dmp --profile=Win12x64 pslist**
- Identificar conexiones de red activas:
  - **volatility -f memoria.dmp --profile=Win12x64 netscan**
- Analizar archivos y comandos ejecutados recientemente:
  - **volatility -f memoria.dmp --profile=Win12x64 cmdscan**
- Buscar posibles indicadores de compromiso (IoCs) relacionados con malware o actividad sospechosa.

### ❖ Análisis con Volatility

Para obtener información del sistema desde la memoria capturada:

```
python vol.py -f memoria.mem windows.info
```

Variable	Value
Kernel Base	0xf80008819000
DTB	0x1aa000
Symbols file	:///C:/Users/Administrador/Desktop/volatility3-2.11.0/volatility3/symbols/windows/ntkrnlmp.pdb/DD04953A2DB5491C9C9671371779ECDB-1.json.xz
Is64Bit	True
IsPAE	False
Layer_name	0 WindowsIntel32e
Memory_layer	1 FileLayer
KdVersionBlock	0xf80008aabe50
Major/Minor	15.9600
MachineType	34404
KeNumberProcessors	2
SystemTime	2025-04-01 18:51:55+00:00
NtSystemRoot	C:\Windows
NtProductType	NtProductServer
NtMajorVersion	6
NtMinorVersion	3
PE MajorOperatingSystemVersion	6
PE MinorOperatingSystemVersion	3
PE Machine	34404
PE TimeStamp	Fri Jan 6 03:03:12 2023

Análisis de la Memoria RAM

- Para listar los procesos en ejecución en el momento de la captura:

```
python vol.py -f memoria.mem windows.pslist
```

PE TimeDateStamp	Fri Jan 6 03:03:12 2023						
C:\Users\Administrador\Desktop\volatility3-2.11.0>python vol.py -f memoria.mem windows.pslist							
Volatility 3 Framework 2.11.0							
Progress: 100.00	PDB scanning finished						
PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	
Wow64	CreateTime	ExitTime	File output				
4	0	System	0xe001b20308c0	107	-	N/A	False
01	16:58:12.000000 UTC	N/A	Disabled				
312	4	smss.exe	0xe001b262b7c0	2	-	N/A	False
2025-04-01	16:58:12.000000 UTC	N/A	Disabled				
416	404	csrss.exe	0xe001b2be8080	9	-	0	False
2025-04-01	16:58:17.000000 UTC	N/A	Disabled				
480	404	wininit.exe	0xe001b20b18c0	1	-	0	False
2025-04-01	16:58:18.000000 UTC	N/A	Disabled				
488	472	csrss.exe	0xe001b20a8080	10	-	1	False
2025-04-01	16:58:18.000000 UTC	N/A	Disabled				
516	472	winlogon.exe	0xe001b209f080	2	-	1	False
2025-04-01	16:58:18.000000 UTC	N/A	Disabled				
576	480	services.exe	0xe001b3302600	3	-	0	False
2025-04-01	16:58:18.000000 UTC	N/A	Disabled				
584	480	lsass.exe	0xe001b32b87c0	5	-	0	False
2025-04-01	16:58:18.000000 UTC	N/A	Disabled				

- Para verificar conexiones de red activas:

```
python vol.py -f memoria.mem windows.netscan
```

- Para buscar malware en la memoria

```
python vol.py -f memoria.mem windows.malfind
```

Administrator: C:\Windows\system32\cmd.exe							
C:\Users\Administrador\Desktop\volatility3-2.11.0>python vol.py -f memoria.mem windows.malfind							
Volatility 3 Framework 2.11.0							
Progress: 100.00 PDB scanning finished							
PID Process Start VPN End VPN Tag Protection CommitCharge							
PrivateMemory File output Notes Hexdump Disasm							
WARNING volatility3.plugins.windows.malfind: [proc_id 584] Found suspicious DIRTY + PAGE_EXECUTE page at 0x7ffc6ca51000							
584	lsass.exe	0x7ffc6ca50000	0x7ffc6ca5ffff	Vads	PAGE_EXECUTE		
16	1	Disabled	N/A				
ff	25	00 00 00 00 60 5f 87 6c fc 7f 00 00 cc 4c %. . . . . L					
8b	d1 b8 87 00 00 00 ff 25 00 00 00 00 68 0a 93 . . . . % . . h .						
6c	fc 7f 00 00 cc 00 00 ff 25 00 00 00 00 80 5f i . . . . % . . .						
87	6c fc 7f 00 00 cc 4c 8b d1 b8 0e 00 00 00 ff . i . . . L . . . .						
00	00 00 60 5f 87 6c fc 7f 00 00 cc 4c 8b d1 b8 87 00 00 00 ff 25 00 00 00 00 6						
8	0a 93 6c fc 7f 00 00 cc 00 00 ff 25 00 00 00 00 80 5f 87 6c fc 7f 00 00 cc 4c						
8b	d1 b8 0e 00 00 00 ff						
1132	avp.exe	0xde40000	0xe03ffff	Vads	PAGE_EXECUTE_READWRITE		
512	1	Disabled	N/A				
53	48 42 32 e8 ff 00 00 00 00 00 10 00 00 e5 0d SHB2 . . . . .						
00	00 00 00 00 00 00 00 00 8c 86 ff c2 42 02 20 63 . . . . . B . c						
8b	53 30 83 3a 00 75 06 c7 02 01 00 00 00 8b bb . S0 . . u . . .						
b8	00 00 00 8b b3 bc 00 00 00 8b ef 8b d6 83 c5 . . . . . . . . .						
32	e8 ff 00 00 00 00 00 10 00 00 e5 0d 00 00 00 00 00 00 00 00 8c 86 ff c2 42 0						

# DÍA 5

## *1. Análisis del sistema de archivos con Autopsy, identificando archivos eliminados, modificados o sospechosos.*



### ❖ Identificación de archivos eliminados

Ubicación en Autopsy:

- Navega a Data Sources > Selecciona tu fuente de datos (ej: disco duro o imagen forense).

The screenshot shows the "CREATE A NEW CASE" dialog box. At the top, the title "CREATE A NEW CASE" is displayed. The form contains three sections: 1. Case Name: A text input field with the placeholder "I". 2. Description: A text input field with the placeholder "...". 3. Investigator Names: A section with two columns of five input fields each, labeled "a.", "c.", "e.", "g.", "i." in the first column and "b.", "d.", "f.", "h.", "j." in the second column. At the bottom of the dialog box, there are three buttons: "NEW CASE", "CANCEL", and "HELP".

➤ Dirígete a File Analysis > Deleted Files.

All Deleted Files									
Type	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SEE	UID	GID	META
dir / in									None

Acciones:

- Revisa la lista de archivos marcados como "deleted". Autopsy los identifica automáticamente.
- Filtra por extensiones sospechosas.
- Usa la columna "Modified Time" para detectar archivos eliminados cerca de la fecha del incidente.

#### ❖ Archivos modificados o sospechosos

File Type Sorting: En File Analysis se muestran las características de los datos analizados (Tamaño, Acceso...)

DEL	Type	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID	GID	META
<b>Error Parsing File (Invalid Characters?):</b> V/V 256: \$OrphanFiles 0000-00-00 00:00:00 (UTC)										
0: 0	r / r	\$AllRef	2025-03-21 06:46:36 (EDT)	2025-03-21 06:46:36 (EDT)	2025-03-21 06:46:36 (EDT)	2025-03-21 06:46:36 (EDT)	2560	48	0	4-128-4
1: 0	r / r	\$BadClus	2025-03-21 06:46:36 (EDT)	2025-03-21 06:46:36 (EDT)	2025-03-21 06:46:36 (EDT)	2025-03-21 06:46:36 (EDT)	0	0	0	8-128-2
2: 0	r / r	\$BadClus:\$Bad	2025-03-21 06:46:36 (EDT)	2025-03-21 06:46:36 (EDT)	2025-03-21 06:46:36 (EDT)	2025-03-21 06:46:36 (EDT)	366997504	0	0	8-128-1
3: 0	r / r	\$BLIngr	2025-03-21 06:46:36 (EDT)	2025-03-21 06:46:36 (EDT)	2025-03-21 06:46:36 (EDT)	2025-03-21 06:46:36 (EDT)	11200	0	0	6-128-4
4: 0	r / r	\$boot	2025-03-21 06:46:36 (EDT)	2025-03-21 06:46:36 (EDT)	2025-03-21 06:46:36 (EDT)	2025-03-21 06:46:36 (EDT)	8192	48	0	7-128-1

- #### ❖ Keyword Search: Usa términos como password, confidential, o palabras relacionadas con el caso (admin).

FILE ANALYSIS	
<b>Searching for ASCII: Done</b> Saving: Done 1719 hits- <a href="#">link to results</a>	
<b>Searching for Unicode: Done</b> Saving: Done 544 hits- <a href="#">link to results</a>	
<b>New Search</b>	
<b>1719 occurrences of password were found</b> Search Options: ASCII Case Sensitive  There were more than 1000 hits. Please revise the search to a manageable amount.  The 1719 hits can be found in: /var/lib/autopsy/Analisis_Servidor_2024/host1/output/disk_image.E01-disk-1.srch	
<b>544 occurrences of password were found</b> Search Options: Unicode Case Sensitive  Unit 12752 (Hex - Ascii) 1: 128 ( the password to u) 2: 216 (rect password; ple) 3: 270 ( the password agai) 4: 326 (many password entr)  Unit 12758 (Hex - Ascii) 5: 348 ( the password as y)  Unit 12759 (Hex - Ascii) 6: 62 ( the password as y)	

FILE ANALYSIS	
<b>Searching for ASCII: Done</b> Saving: Done 2089 hits- <a href="#">link to results</a>	
<b>Searching for Unicode: Done</b> Saving: Done 1309 hits- <a href="#">link to results</a>	
<b>New Search</b>	
<b>2089 occurrences of admin were found</b> Search Options: ASCII Case Sensitive  There were more than 1000 hits. Please revise the search to a manageable amount.  The 2089 hits can be found in: /var/lib/autopsy/Analisis_Servidor_2024/host1/output/disk_image.E01-disk-3.srch	
<b>1309 occurrences of admin were found</b> Search Options: Unicode Case Sensitive  There were more than 1000 hits. Please revise the search to a manageable amount.  The 1309 hits can be found in: /var/lib/autopsy/Analisis_Servidor_2024/host1/output/disk_image.E01-disk-4.srch	

## **2. Recuperación de archivos eliminados y análisis de sus metadatos.**

### **❖ Recuperación**

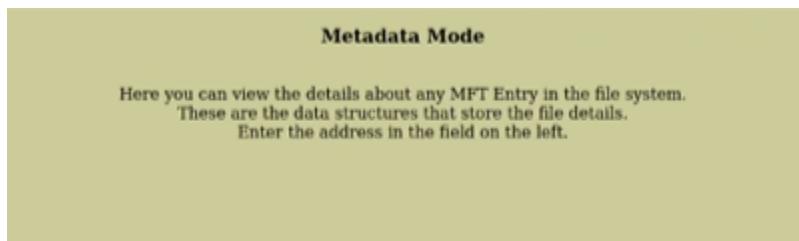
#### **➤ Recuperar archivos eliminados en Autopsy**

- Abrir Autopsy y cargar el caso en el que se está trabajando.
- En Deleted Files, selecciona el archivo de interés.
- Haz clic derecho > Export File para recuperarlo (si el espacio no ha sido sobrescrito).
- Verifica la integridad con Hash (MD5/SHA-1) antes y después de la recuperación.
- Guardar los archivos recuperados en una carpeta segura para analizarlos más tarde.

### **❖ Metadatos**

#### **➤ Propiedades básicas:**

- Nombre, tamaño, fechas (Created, Modified, Accessed).
- Ubicación original (ej: C:\Users\Usuario\Downloads).
- EXIF Data (para imágenes/PDFs):
- Revisa la pestaña Metadata en Autopsy.



#### **➤ Metadatos de sistema:**

- En File System Metadata, busca entradas en la MFT (Master File Table) para reconstruir la historia del archivo.

MFT Entry Number:

VIEW

ALLOCATION LIST

Pointed to by file:  
C:\\$volume

File Type:  
empty

MD5 of content:  
d41d8cd98f0b0b284e9809998ecfb427e -

SHA-1 of content:  
da39a3ee5e6bb4b8225bfef9560199af08979 -

Details:

MFT Entry Header Values:  
Entry: 3 Sequence: 3  
LogFile Sequence Number: 1056791  
Allocation File  
Links: 1

STANDARD INFORMATION Attribute Values:  
Flags: Hidden, System  
Owner ID: 0  
Security ID: 257 (S-1-5-18)  
Create Time: 2025-03-21 06:46:36.478824000 (EDT)  
File Modified: 2025-03-21 06:46:36.478824000 (EDT)  
MFT Modified: 2025-03-21 06:46:36.478824000 (EDT)  
Accessed: 2025-03-21 06:46:36.478824000 (EDT)

FILE NAME Attribute Values:  
File Name: \$Volume  
Parent MFT Entry: 5 Sequence: 5  
Allocated Size: 0  
Create Time: 2025-03-21 06:46:36.478824000 (EDT)  
File Modified: 2025-03-21 06:46:36.478824000 (EDT)

❖ **Análisis de Registros de Eventos de Windows**

- Ubicación de los logs en Autopsy:
- Logs críticos:
  - Security.evtx: Intentos de inicio de sesión, cambios de permisos.
  - System.evtx: Errores de hardware/drivers.
  - Application.evtx: Eventos de aplicaciones.

❖ **Búsqueda de actividades sospechosas**

- Filtros recomendados:
  - Event ID 4624/4625: Inicios de sesión exitosos/fallidos (busca IPs o usuarios desconocidos).
  - Event ID 4688: Creación de procesos (ej: ejecución de powershell.exe o cmd.exe con parámetros sospechosos).
  - Event ID 4104: Ejecución de scripts PowerShell (verifica comandos inusuales).
  - Event ID 7045: Servicios instalados por usuarios no administrativos.
  - Event ID 1102: Borrado de registros de eventos (indicador de intento de ocultación).

❖ **Correlación temporal**

- Cruza los horarios de los eventos con:
- Modificaciones de archivos.
- Accesos a carpetas sensibles (ej: C:\Windows\System32).
- Conexiones de red registradas en otros logs.

### **3. Análisis de Registros de Eventos en Windows**

Windows guarda un historial de todo lo que ocurre en el sistema a través de los registros de eventos. Esto permite identificar actividad sospechosa, como intentos de inicio de sesión fallidos, uso de permisos de administrador y la eliminación de registros para ocultar evidencias.

❖ **Abrir el Visor de Eventos en Windows**

- Presionar Windows + R, escribir eventvwr y presionar Enter.
- En el panel izquierdo, ir a Registros de Windows > Seguridad.
- Aquí se encuentran los eventos relacionados con la seguridad del sistema.

❖ **Buscar eventos importantes**

Dentro del Visor de Eventos, hay ciertos registros clave que pueden indicar actividad sospechosa:

- [4624](#): Inicio de sesión exitoso.
- [4625](#): Intento de inicio de sesión fallido.
- [4672](#): Uso de privilegios de administrador.
- [1102](#): Eliminación de registros de eventos (posible intento de ocultar actividad).

Para buscar un evento específico:

- En la parte derecha de la ventana, hacer clic en Filtrar registro actual.
- En "Identificadores de eventos", escribir el número del evento a buscar (por ejemplo, 4625).
- Presionar Aceptar y revisar los resultados.

#### ❖ **Anализar los registros con LogParser**

LogParser es una herramienta que permite analizar los registros de eventos usando comandos.

- Descargar e instalar LogParser de la página oficial de Microsoft.
- Abrir Símbolo del sistema (cmd).
- Usar el siguiente comando para ver intentos de inicio de sesión y otras actividades relevantes:

```
logparser "SELECT * FROM Security WHERE EventID IN (4624,4625,4672,1102)" -i:EVT
```

#### ❖ **Usar EvtxExplorer para un análisis más avanzado**

Si se necesita una visualización más detallada, EvtxExplorer es una herramienta útil para examinar los registros de eventos.

- Descargar e instalar EvtxExplorer.
- Abrir los archivos de registro (.evtx) del sistema.
- Buscar eventos sospechosos con filtros avanzados.

# DÍA 6

## *1. Análisis de los registros de la base de datos Oracle 12c para identificar accesos no autorizados o modificaciones de datos.*

### ❖ Identificar conexiones sospechosas

➤ Conéctate como sysdba:

- sqlplus / as sysdba
- Consulta accesos recientes:
- SELECT username, osuser, machine, program, logon\_time
- FROM v\$session
- WHERE username IS NOT NULL
- ORDER BY logon\_time DESC;
- Busca: IPs desconocidas, programas no autorizados (ej: sqlmap).

```
Administrator: C:\Windows\system32\cmd.exe - sqlplus / as sysdba

SQL> SELECT username, osuser, machine, program, logon_time
  2  FROM v$session
  3  WHERE username IS NOT NULL
  4  ORDER BY logon_time DESC;

USERNAME
OSUSER
MACHINE
PROGRAM
LOGON_TI
SYS
WIN-LG8U31EC0BA\Administrador
WORKGROUP\WIN-LG8U31EC0BA
sqlplus.exe
28/03/25

SQL>
```

➤ Auditar consultas SQL inusuales

- SELECT sql\_text, executions, last\_load\_time
- FROM v\$sql
- WHERE LOWER(sql\_text) LIKE '%delete%' OR LOWER(sql\_text)  
LIKE '%update%'
- ORDER BY last\_load\_time DESC;

```
EXECUTIONS
LAST_LOAD_TIME
= equality_preds + decode(bitand(:flag,1),0,0,1), equijoin_preds = equ
ijoin_preds + decode(bitand(:flag,2),0,0,1), nonequijoin_preds = nonequijo
n_preds + decode(bitand(:flag,4),0,0,1), range_preds = range_preds
+ decode(bitand(:flag,8),0,0,1), like_preds = like_preds + deco
de(bitand(:flag,16),0,0,1), null_preds = null_preds + decode(bit
and(:flag,32),0,0,1), flags      ↵ = :flag, timestamp = :time where ob
j# = :objn and intcol# = :coln
SQL_TEXT

EXECUTIONS
LAST_LOAD_TIME
601
2025-03-28/12:02:13
select /* KSXM:LOAD_DML_INF *//*+ leading(o) index(m) use_nl(m) */      nv
l(m.inserts, 0) ins, nvl(m.updates, 0) upd, nvl(m.deletes, 0) del,          nvl(
m.drop_segments, 0) dropseg, nvl(m.flags, 0) flags,                      nvl(ro
wcnt, 0) rowcnt, o.pobjn pobjn                                         from
SQL_TEXT

EXECUTIONS
LAST_LOAD_TIME
<select :o
bijn objn, 0 pobjn, rowcnt
from tab$ t
where t.obj#
union all
select :objn objn
from tabpart$ tp
where tp.obj# = :objn
SQL_TEXT
```

## *2. Análisis de los registros del antivirus Kaspersky Endpoint Security para identificar detecciones de malware o intrusiones.*

### ❖ Elementos clave a revisar:

#### ➢ **Registros de detección de malware:**

- Nombre del archivo infectado, tipo de malware (ej. Trojan.Win32, Ransomware).
- Rutas de archivos bloqueados o puestos en cuarentena.
- Severidad (Critical, High).

### ❖ Eventos de protección en tiempo real:

- Bloqueo de exploits (ej. CVE-2023-XXXX).
- Alertas de ataques en la red (ej. Intrusion.Generic).

#### ➢ **Alertas del módulo Anti-Phishing o Firewall:**

- Conexiones bloqueadas a dominios maliciosos.

Fecha del evento	Evento	Componente	Aplicación
■ Hoy, 28/03/2025 12:23:57	La tarea no se puede llevar a cabo	Comprobación de integridad de la aplicación	Kaspersky Endpoint Security
■ Hoy, 28/03/2025 12:23:57	La tarea no se puede llevar a cabo	Comprobación de integridad de la aplicación	Kaspersky Endpoint Security
■ Hoy, 28/03/2025 12:23:57	La tarea no se puede llevar a cabo	Comprobación de integridad de la aplicación	Kaspersky Endpoint Security
■ Hoy, 28/03/2025 12:23:57	La tarea no se puede llevar a cabo	Comprobación de integridad de la aplicación	Kaspersky Endpoint Security
■ Hoy, 28/03/2025 12:23:57	La tarea no se puede llevar a cabo	Comprobación de integridad de la aplicación	Kaspersky Endpoint Security
■ Hoy, 28/03/2025 12:23:57	La tarea no se puede llevar a cabo	Comprobación de integridad de la aplicación	Kaspersky Endpoint Security
■ Hoy, 28/03/2025 12:23:57	La tarea no se puede llevar a cabo	Comprobación de integridad de la aplicación	Kaspersky Endpoint Security
■ Hoy, 28/03/2025 12:23:57	La tarea no se puede llevar a cabo	Comprobación de integridad de la aplicación	Kaspersky Endpoint Security
■ Hoy, 28/03/2025 12:23:57	La tarea no se puede llevar a cabo	Comprobación de integridad de la aplicación	Kaspersky Endpoint Security
■ Hoy, 28/03/2025 12:23:57	La tarea no se puede llevar a cabo	Comprobación de integridad de la aplicación	Kaspersky Endpoint Security
■ Hoy, 28/03/2025 12:23:57	La tarea no se puede llevar a cabo	Comprobación de integridad de la aplicación	Kaspersky Endpoint Security
■ Hoy, 28/03/2025 12:23:57	La tarea no se puede llevar a cabo	Comprobación de integridad de la aplicación	Kaspersky Endpoint Security
■ Hoy, 28/03/2025 12:23:57	La tarea no se puede llevar a cabo	Comprobación de integridad de la aplicación	Kaspersky Endpoint Security
■ Hoy, 28/03/2025 12:23:57	La tarea no se puede llevar a cabo	Comprobación de integridad de la aplicación	Kaspersky Endpoint Security
■ Hoy, 28/03/2025 12:19:30	Tarea terminada	Actualización	Kaspersky Endpoint Security
■ Hoy, 28/03/2025 12:19:25	La tarea no se puede llevar a cabo	Actualización	Kaspersky Endpoint Security
■ Hoy, 28/03/2025 12:18:46	Tarea iniciada	Actualización	Kaspersky Endpoint Security

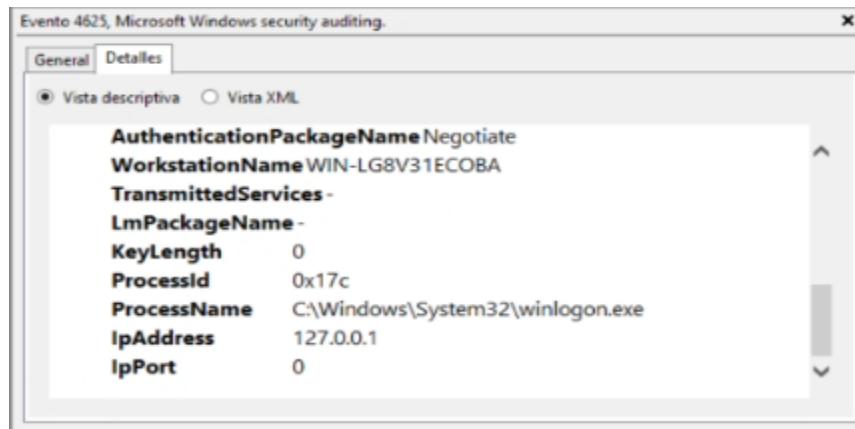
### *3. Análisis de los logs de acceso del sistema operativo, para poder determinar si ha habido usuarios que han accedido de forma remota al sistema.*

#### ❖ Elementos clave según el SO:

- Eventos de inicio de sesión (Visor de Eventos > Registros de Windows > Seguridad):
- Evento 4624 (éxito) y 4625 (fallo).

	Auditoria correcta	21/03/2025 11:48:53	Microsoft Win...	4624	Inicio de sesión
	Error de auditoría	25/03/2025 11:11:08	Microsoft Win...	4625	Inicio de sesión

- Campo Dirección IP de origen en eventos de tipo 10 (Logon Type 10: RemoteInteractive).



- Conexiones RDP: Revisar registros en Windows PowerShell:

```
PowerShell
Get-WinEvent -LogName
'Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operati
onal' | Where-Object {$_._ID -eq 1149}
```

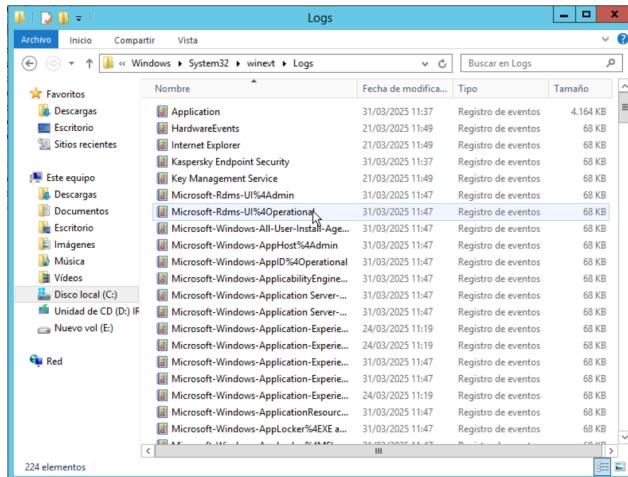
```
Administrator: Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. Todos los derechos reservados.
PS C:\Users\Administrador> Get-WinEvent -LogName 'Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational'
' | Where-Object {$_._ID -eq 1149}
```

# DÍA 7

## *1. Análisis de la línea de tiempo para reconstruir la secuencia de eventos.*

### ❖ Recopilar Registros de Eventos:

- Acceder al Visor de Eventos (eventvwr.msc).
- Exportar registros clave:
  - Seguridad (Eventos de inicio de sesión, acceso a recursos).
  - Sistema (Errores del sistema, servicios).
  - Aplicación (Registros de aplicaciones y servicios).
- Ubicación física: C:\Windows\System32\winevt\Logs\.



### ❖ Generar una Línea de Tiempo:

- FTK Imager (Exportar registros).

### ❖ Analizar Eventos Clave:

- Filtrar por:
  - ID 4624: Inicio de sesión exitoso.
  - ID 4688: Creación de procesos.
  - ID 7045: Servicios instalados.

## **2. Correlación de los hallazgos de diferentes fuentes de evidencia.**

### **❖ Integrar Fuentes de Datos:**

- Firewall/IDS: Exportar logs de conexiones bloqueadas.
- Capturas de Red (Wireshark): Filtrar por tráfico anómalo (Ej: conexiones a IPs maliciosas).
- Antivirus: Revisar alertas de detección (archivos/quarantine).

## **3. Investigación de los procesos activos del sistema, para poder determinar si existe algún proceso malicioso activo**

### **❖ Listar Procesos Activos:**

- PowerShell:

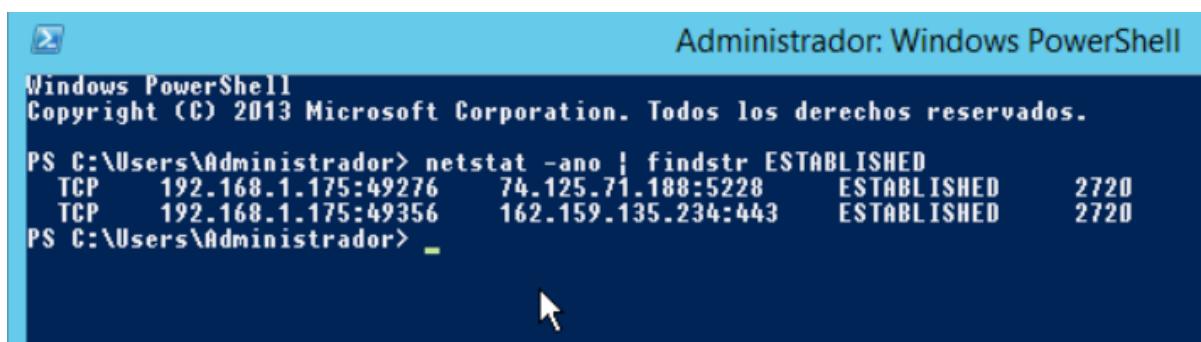
```
powershell
```

```
Get-Process | Select-Object Id, ProcessName, Path, CPU | Export-Csv procesos.csv
```

### **❖ Analizar Conexiones de Red:**

```
powershell
```

```
netstat -ano | findstr ESTABLISHED
```



```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. Todos los derechos reservados.

PS C:\Users\Administrador> netstat -ano | findstr ESTABLISHED
TCP    192.168.1.175:49276    74.125.71.188:5228    ESTABLISHED      2720
TCP    192.168.1.175:49356    162.159.135.234:443   ESTABLISHED      2720
PS C:\Users\Administrador>
```

### **❖ Análisis de Memoria (Opcional):**

- Usar Volatility:

```
bash
```

```
volatility -f memory.dump windows.pslist.PsList
```

PDB scanning finished												
PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	File output		
4	0	System	0xe0009ce6b900	70	-	N/A	False	2025-03-26 09:00:25.000000 UTC	N/A	Disabled		
196	4	sess.exe	0xe0009d478900	2	-	N/A	False	2025-03-26 09:00:25.000000 UTC	N/A	Disabled		
284	276	csrss.exe	0xe0009dad2900	8	-	0	False	2025-03-26 09:00:26.000000 UTC	N/A	Disabled		
348	340	csrss.exe	0xe0009cef5540	9	-	1	False	2025-03-26 09:00:27.000000 UTC	N/A	Disabled		
376	276	wininit.exe	0xe0009cef080	1	-	0	False	2025-03-26 09:00:27.000000 UTC	N/A	Disabled		
384	340	winlogon.exe	0xe0009db30900	2	-	1	False	2025-03-26 09:00:27.000000 UTC	N/A	Disabled		
448	376	services.exe	0xe0009ceb9240	4	-	0	False	2025-03-26 09:00:27.000000 UTC	N/A	Disabled		
456	376	lsass.exe	0xe0009db7d080	6	-	0	False	2025-03-26 09:00:27.000000 UTC	N/A	Disabled		
512	448	svchost.exe	0xe0009dd32900	9	-	0	False	2025-03-26 09:00:28.000000 UTC	N/A	Disabled		
540	448	svchost.exe	0xe0009dd3a900	10	-	0	False	2025-03-26 09:00:28.000000 UTC	N/A	Disabled		
540	384	dwm.exe	0xe0009dd88080	8	-	1	False	2025-03-26 09:00:28.000000 UTC	N/A	Disabled		
556	448	svchost.exe	0xe0009dd83900	12	-	0	False	2025-03-26 09:00:28.000000 UTC	N/A	Disabled		
712	448	svchost.exe	0xe0009dd81900	34	-	0	False	2025-03-26 09:00:28.000000 UTC	N/A	Disabled		
772	448	svchost.exe	0xe0009cccd540	16	-	0	False	2025-03-26 09:00:28.000000 UTC	N/A	Disabled		
852	448	svchost.exe	0xe0009dd7080	16	-	0	False	2025-03-26 09:00:28.000000 UTC	N/A	Disabled		
992	448	svchost.exe	0xe0009de68900	19	-	0	False	2025-03-26 09:00:29.000000 UTC	N/A	Disabled		
492	448	spoolsv.exe	0xe0009dea900	8	-	0	False	2025-03-26 09:00:29.000000 UTC	N/A	Disabled		
784	448	svchost.exe	0xe0009df163c0	10	-	0	False	2025-03-26 09:00:29.000000 UTC	N/A	Disabled		
916	448	wlms.exe	0xe0009df21980	2	-	0	False	2025-03-26 09:00:29.000000 UTC	N/A	Disabled		
1416	712	taskhostex.exe	0xe0009e0f440	7	-	1	False	2025-03-26 09:00:50.000000 UTC	N/A	Disabled		
1468	1460	explorer.exe	0xe0009dd75900	50	-	1	False	2025-03-26 09:00:50.000000 UTC	N/A	Disabled		
1852	1432	ServerManager	0xe0009e01a900	9	-	1	False	2025-03-26 09:00:51.000000 UTC	N/A	Disabled		
1896	1468	FTK Imager.exe	0xe0009e016900	16	-	1	False	2025-03-26 09:00:53.000000 UTC	N/A	Disabled		
1964	1424	GoogleCrashMan	0xe0009e014900	4	-	0	True	2025-03-26 09:00:55.000000 UTC	N/A	Disabled		
1972	1424	GoogleCrashMan	0xe0009e1af900	4	-	0	False	2025-03-26 09:00:55.000000 UTC	N/A	Disabled		
1780	1468	chrome.exe	0xe0009d1c8900	24	-	1	False	2025-03-26 09:02:03.000000 UTC	N/A	Disabled		
1784	1780	chrome.exe	0xe0009db39080	7	-	1	False	2025-03-26 09:02:03.000000 UTC	N/A	Disabled		
1220	1780	chrome.exe	0xe0009d1ff3c0	10	-	1	False	2025-03-26 09:02:04.000000 UTC	N/A	Disabled		
1376	1780	chrome.exe	0xe0009df3c200	13	-	1	False	2025-03-26 09:02:04.000000 UTC	N/A	Disabled		
1252	1780	chrome.exe	0xe0009e2c5900	7	-	1	False	2025-03-26 09:02:04.000000 UTC	N/A	Disabled		
2392	1780	chrome.exe	0xe0009e01c900	14	-	1	False	2025-03-26 09:02:25.000000 UTC	N/A	Disabled		
2612	448	msdtc.exe	0xe0009e437900	9	-	0	False	2025-03-26 09:02:30.000000 UTC	N/A	Disabled		
2748	1780	chrome.exe	0xe0009e44c900	14	-	1	False	2025-03-26 09:02:31.000000 UTC	N/A	Disabled		
2924	1780	chrome.exe	0xe0009efafa900	11	-	1	False	2025-03-26 09:02:40.000000 UTC	N/A	Disabled		
2068	512	WmiPrvSE.exe	0xe0009e52c900	4	-	0	False	2025-03-26 09:04:29.000000 UTC	N/A	Disabled		
1588	512	WmiPrvSE.exe	0xe0009e457080	9	-	0	False	2025-03-26 09:09:55.000000 UTC	N/A	Disabled		
56	1896	ADIso.exe	0xe0009dc5e7c0	9	-	1	True	2025-03-26 09:09:56.000000 UTC	N/A	Disabled		
2004	56	conhost.exe	0xe0009e242240	1	-	1	False	2025-03-26 09:09:56.000000 UTC	N/A	Disabled		

# DÍA 8

## *1. Análisis de la red, para la detección de posibles conexiones no autorizadas.*

### ❖ Monitoreo de tráfico:

- Utilizar herramientas como Wireshark, tcpdump o Zeek para analizar patrones de tráfico inusuales (picos fuera de horario, protocolos no estándar).
- Buscar conexiones a direcciones IP externas sospechosas (por ejemplo, países de alto riesgo).

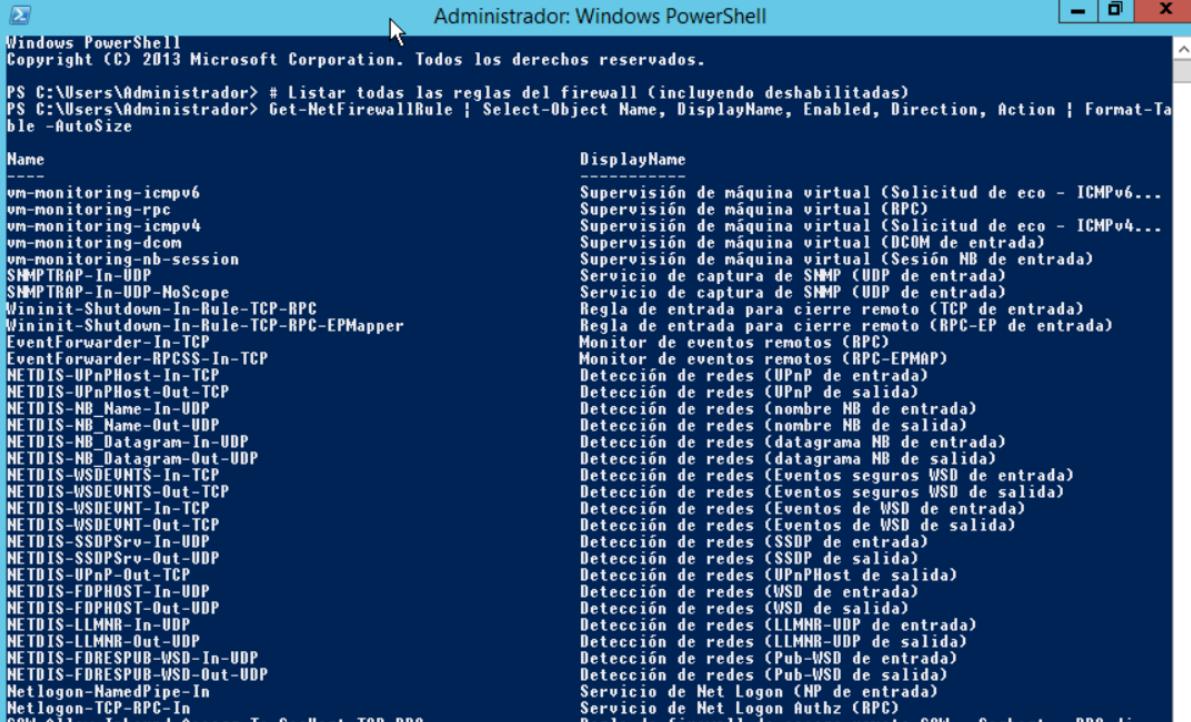
Proto	Dirección local	Dirección remota	Estado	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	632
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:5985	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:47001	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING	440
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING	752
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING	828
TCP	0.0.0.0:49155	0.0.0.0:0	LISTENING	616
TCP	0.0.0.0:49157	0.0.0.0:0	LISTENING	548
TCP	0.0.0.0:49172	0.0.0.0:0	LISTENING	1096
TCP	0.0.0.0:49182	0.0.0.0:0	LISTENING	540
TCP	127.0.0.1:49158	0.0.0.0:0	LISTENING	1044
TCP	192.168.1.175:139	0.0.0.0:0	LISTENING	4
TCP	192.168.1.175:49191	74.125.206.84:443	TIME_WAIT	0
TCP	192.168.1.175:49192	142.250.184.161:443	TIME_WAIT	0
TCP	192.168.1.175:49193	216.58.209.67:443	TIME_WAIT	0
TCP	192.168.1.175:49194	142.250.201.74:443	TIME_WAIT	0
TCP	192.168.1.175:49195	142.250.200.110:443	TIME_WAIT	0

### ❖ Escaneo de puertos y servicios:

- Ejecutar nmap o Masscan para detectar puertos abiertos no autorizados (ej. puerto 22/SSH expuesto públicamente sin necesidad).
- Verificar servicios innecesarios (ej. Telnet, FTP sin cifrar).

❖ **Firewall y reglas de red:**

- Revisar reglas de firewall (iptables, Windows Firewall, o soluciones empresariales) para asegurar que solo se permiten conexiones autorizadas.
- Eliminar reglas ambiguas o demasiado permisivas (ej. ALLOW ANY:ANY).



Windows PowerShell  
Copyright (C) 2013 Microsoft Corporation. Todos los derechos reservados.  
PS C:\Users\Administrador> # Listar todas las reglas del firewall (incluyendo deshabilitadas)  
PS C:\Users\Administrador> Get-NetFirewallRule | Select-Object Name, DisplayName, Enabled, Direction, Action | Format-Table -AutoSize

Name	DisplayName
vm-monitoring-icmpv6	Supervisión de máquina virtual (Solicitud de eco - ICMPv6...)
vm-monitoring-rpc	Supervisión de máquina virtual (RPC)
vm-monitoring-icmpv4	Supervisión de máquina virtual (Solicitud de eco - ICMPv4...)
vm-monitoring-dcom	Supervisión de máquina virtual (DCOM de entrada)
vm-monitoring-nb-session	Supervisión de máquina virtual (Sesión NB de entrada)
SNMPTRAP-In-UDP	Servicio de captura de SNMP (UDP de entrada)
SNMPTRAP-In-UDP-NoScope	Servicio de captura de SNMP (UDP de entrada)
Vininit-Shutdown-In-Rule-TCP-RPC	Regla de entrada para cierre remoto (TCP de entrada)
Vininit-Shutdown-In-Rule-TCP-RPC-EPMapper	Regla de entrada para cierre remoto (RPC-EP de entrada)
EventForwarder-In-TCP	Monitor de eventos remotos (RPC)
EventForwarder-RPCSS-In-TCP	Monitor de eventos remotos (RPC-EPMAP)
NETDIS-UPnPhost-In-TCP	Detección de redes (UPnP de entrada)
NETDIS-UPnPhost-Out-TCP	Detección de redes (UPnP de salida)
NETDIS-NB_Name-In-UDP	Detección de redes (nombre NB de entrada)
NETDIS-NB_Name-Out-UDP	Detección de redes (nombre NB de salida)
NETDIS-NB_Datagram-In-UDP	Detección de redes (datagrama NB de entrada)
NETDIS-NB_Datagram-Out-UDP	Detección de redes (datagrama NB de salida)
NETDIS-WSDEVENTS-In-TCP	Detección de redes (Eventos seguros WSD de entrada)
NETDIS-WSDEVENTS-Out-TCP	Detección de redes (Eventos seguros WSD de salida)
NETDIS-WSDEVENT-In-TCP	Detección de redes (Eventos de WSD de entrada)
NETDIS-WSDEVENT-Out-TCP	Detección de redes (Eventos de WSD de salida)
NETDIS-SSDPDrv-In-UDP	Detección de redes (SSDP de entrada)
NETDIS-SSDPDrv-Out-UDP	Detección de redes (SSDP de salida)
NETDIS-UPnP-Out-TCP	Detección de redes (UPnPHost de salida)
NETDIS-FDPPHOST-In-UDP	Detección de redes (WSD de entrada)
NETDIS-FDPPHOST-Out-UDP	Detección de redes (WSD de salida)
NETDIS-LLMNR-In-UDP	Detección de redes (LLMNR-UDP de entrada)
NETDIS-LLMNR-Out-UDP	Detección de redes (LLMNR-UDP de salida)
NETDIS-FDRESPUB-WSD-In-UDP	Detección de redes (Pub-WSD de entrada)
NETDIS-FDRESPUB-WSD-Out-UDP	Detección de redes (Pub-WSD de salida)
Netlogon-Namedpipe-In	Servicio de Net Logon (NP de entrada)
Netlogon-TCP-RPC-In	Servicio de Net Logon Authz (RPC)

❖ **Análisis de logs:**

- Revisar logs de dispositivos de red (routers, switches) y servidores para identificar intentos de acceso fallidos o repetidos.
- Buscar eventos como "Failed login" o "Connection refused".

❖ **Segmentación de red:**

- Validar que la red está segmentada (ej. VLANs para áreas críticas como bases de datos) para limitar el movimiento lateral de atacantes.

❖ **Detección de intrusos:**

- Implementar un IDS/IPS (Snort, Suricata) para alertar sobre actividades sospechosas (ej. escaneo de puertos, tráfico malicioso).

## *2. Análisis de las posibles vulnerabilidades del sistema operativo y de la base de datos.*

### ❖ Actualizaciones y parches:

- Verificar si el SO está actualizado (ej. yum check-update en Linux, Windows Update).
- Identificar vulnerabilidades críticas no parcheadas (ej. CVE relacionadas con RCE o escalación de privilegios).

HotFixID	InstalledOn
KB2938772	
KB2939471	
KB2949621	
KB2919355	
KB2919442	
KB2937220	

### ❖ Configuraciones inseguras:

- Revisar permisos de archivos críticos (ej. /etc/passwd, /etc/shadow en Linux).
- Deshabilitar servicios innecesarios (ej. SMBv1 en Windows, servicios legacy en Linux).
- Asegurar que el SELinux/AppArmor (Linux) o el Windows Defender estén habilitados.

```
Administrator: Windows PowerShell
BUILTIN\Administradores:(I)(F)
C:\Windows\System32\config\BBI.LOG1 NT AUTHORITY\SYSTEM:(I)(F)
BUILTIN\Administradores:(I)(F)
C:\Windows\System32\config\BBI.LOG2 NT AUTHORITY\SYSTEM:(I)(F)
BUILTIN\Administradores:(I)(F)
C:\Windows\System32\config\BBI{42b8217e-0b2e-11e3-93f4-90b11c2eb9f2}.TM.bif NT AUTHORITY\SYSTEM:(I)(F)
BUILTIN\Administradores:(I)(F)
C:\Windows\System32\config\BBI{42b8217e-0b2e-11e3-93f4-90b11c2eb9f2}.TMContainer00000000000000000000000000000001.retrans-ms NT AUTHORITY\SYSTEM:(I)(F)
BUILTIN\Administradores:(I)(F)
C:\Windows\System32\config\BBI{42b8217e-0b2e-11e3-93f4-90b11c2eb9f2}.TMContainer00000000000000000000000000000002.retrans-ms NT AUTHORITY\SYSTEM:(I)(F)
BUILTIN\Administradores:(I)(F)
C:\Windows\System32\config\BCD-Template NT AUTHORITY\SYSTEM:(I)(F)
BUILTIN\Administradores:(I)(F)
C:\Windows\System32\config\BCD-Template.LOG NT AUTHORITY\SYSTEM:(I)(F)
BUILTIN\Administradores:(I)(F)
C:\Windows\System32\config\BCD-Template.LOG1 NT AUTHORITY\SYSTEM:(I)(F)
BUILTIN\Administradores:(I)(F)
C:\Windows\System32\config\BCD-Template.LOG2 NT AUTHORITY\SYSTEM:(I)(F)
BUILTIN\Administradores:(I)(F)
```

- ❖ **Benchmarks de seguridad:**
  - Usar herramientas como CIS-CAT o Lynis (Linux) para validar el cumplimiento de estándares de seguridad.
- ❖ **Base de Datos (BD):**
  - **Configuraciones críticas:**
    - Validar que no se usan credenciales por defecto (ej. usuario sa en SQL Server con contraseña vacía).
    - Asegurar cifrado en tránsito (TLS/SSL) y en reposo (TDE, Transparent Data Encryption).
    - Restringir accesos remotos innecesarios (ej. MySQL sin bind a 0.0.0.0).
  - **Vulnerabilidades conocidas:**
    - Revisar parches para la versión específica de la BD (ej. Oracle Critical Patch Updates).
  - **Auditoría de consultas:**
    - Habilitar logs de auditoría para registrar consultas privilegiadas o accesos a datos sensibles.

### ***3. Análisis de los usuarios y grupos del sistema operativo y de la base de datos, para poder determinar si existe alguna cuenta de usuario no autorizada.***

- ❖ **Usuarios locales y grupos:**
  - En Windows: Usar net user y net localgroup para listar usuarios y grupos administrativos.
  - Buscar cuentas inactivas (ej. última conexión hace más de 90 días) o con UID/GID incongruente.
- ❖ **Privilegios:**
  - Verificar usuarios con acceso en el grupo "Administradores" (Windows).
  - Eliminar privilegios innecesarios (principio de mínimo privilegio).
- ❖ **Autenticación externa:**
  - Revisar integración con LDAP/Active Directory para detectar cuentas huérfanas o no sincronizadas.