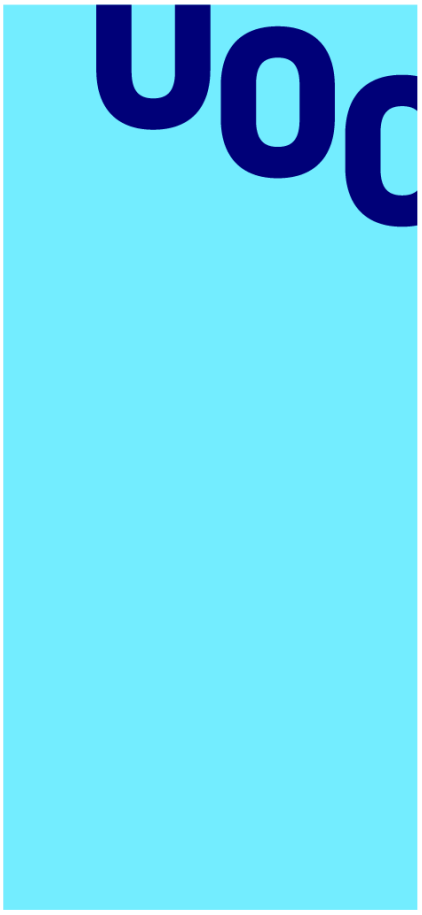
Análisis forense de un ordenador personal



Universitat Oberta de Catalunya

Alumno:
José Enrique Rodríguez González

Master Universitario de Ciberseguridad y privacidad.

M1.881 - TFM - Análisis forense

Tutora de TFM:
Dña. Elena Botana de Castro

Profesor responsable de la asignatura:
D. Jordi Serra Ruiz

Fecha de Entrega:
Enero de 2024

Deuda técnica

Este no es un capitulo al uso del TFM, si no que tratará de llevar un control de las tareas pendientes (Deuda técnica) de todo el TFM.

PEC 1

1. **DEUDA TÉCNICA: Pendiente de Referenciar!!!, enunciado del TFM**
2. **DEUDA TÉCNICA: Pendiente de Referenciar!!!, referenciar de la web de los TFM**
3. **DEUDA TÉCNICA: Buscar presidente de los EE.UU., preguntar a //4lanoga"**

   LA RESPUESTA ES REAGAN
4. **DEUDA TÉCNICA: Listado de aplicaciones a utilizar en la descripción del entorno de trabajo**
5. **DEUDA TÉCNICA: Revisar código LaTeX de Estado del arte**
6. **DEUDA TÉCNICA: plantear posible reducción del estado del arte**
7. **DEUDA TÉCNICA: Referencia a WIKIPEDIA**

Agradecimientos

A mi esposa e hija, acompañantes en todo momento de esta aventura académica.

A mis compañeros de trabajo, Juanma, Luisma y Borja, que saben de que estos tres años que llevo realizando este master y han conocido todos los derroteros que me ha llevado este camino.

Índice general

Capítulo 1

Plan de trabajo.

La situación en la que nos encontramos es un caso práctico laboral, en el que realizamos el papel de CISO.

En este caso, la dirección de la empresa tiene serias sospechas, no probadas, de que han accedido a los sistemas de forma ilícita. Por lo que el gerente de la empresa me solicita, como CISO, que se compruebe si realmente han accedido, así como el método que han utilizado. Por otro lado, solicitan las consecuencias que se derivan del dicho acceso, si ha habido extracción de información alguna.

DEUDA TÉCNICA: Pendiente de Referenciar!!! ENUNCIADO TFM

1.1. Problema a resolver.

Por, lo expuesto en la introducción del capítulo, se coliga que el problema a resolver es la resolución de las cuestiones solicitadas por el Gerente de la empresa.

Una definición idónea que se puede adoptar en el presente TFM es lo indicado en su momento en la propuesta del TFM:

Solventar las necesidades del gerente de la empresa mediante el análisis forense del disco duro y la captura de memoria de un ordenador personal, en un caso real con un sistema virtualizado, vinculado a una presunta conducta delictiva real. Para ello, se utilizarán herramientas específicas para la localización de las evidencias digitales sobre los discos duros y la memoria que puedan demostrar el presunto delito (Encase, Autopsy, Volatility, o cualquier otra herramienta, o conjunto de herramientas con prestaciones equivalentes). Finalmente, las evidencias localizadas deberán recogerse en un informe ejecutivo o pericial, el cual, además de los aspectos técnicos, deberá tener en cuenta aquellos requisitos procesales necesarios para que el análisis pueda tener validez en un proceso judicial.

DEUDA TÉCNICA: Pendiente de Referenciar!!!, referenciar de la web de los TFM

1.2. Objetivos.

Se describe un el siguiente listado de objetivos que se obtienen al analizar el enunciado del TFM:

1. Elaboración del Análisis forense de Disco Duro y RAM.
   - *a*) realizar una recuperación parcial o total de la información borrada existente en los dispositivos susceptibles de ser analizados (carving).
   - *b*) Relativo al análisis de la memoria RAM.
     1) Comprobar la integridad de la memoria RAM.
     2) Comprobar fecha de la captura de la RAM.
     3) Determinar la edición y versión de Windows que tiene instalado el sistema operativo del ordenador sobre el cual se ha efectuado la captura de la memoria RAM.
     4) Buscar los procesos en funcionamiento y localiza aquellos que te parezcan de interés para el análisis forense del ordenador analizado.
     5) Extraer los procesos que consideres sospechosos y analizarlos.
     6) Listar las conexiones de red y analizarlas.
   - *c*) Relativo al analisis del Disco Duro.
     1) Comprobar la integridad del disco duro.
     2) Determinar la siguiente información del disco duro.
        - *a'* Tamaño del disco duro analizado.
        - *b'* Sistema y versión del sistema operativo instalado.
        - *c'* Nombre del propietario y relación de software instalado.
        - *d'* "Product ID" y "Product Key" asociadas al sistema.
        - *e'* Fecha y hora de instalación del sistema operativo.
        - *f'* Determinar marca y modelo (si es posible) del hardware siguiente: CPU, monitor, tarjeta gráfica, tarjeta Ethernet y Wireless.
     3) Determinar qué usuarios tiene definidos el sistema.
     4) Localizar los documentos (archivos PDF, de texto, hojas de cálculo, etc.) que puedan tener relación con alguna conducta presuntamente delictiva.
     5) Localizar los archivos eliminados y determina si hay alguno relevante para la causa investigada.
     6) Localizar los ficheros comprimidos relevantes analizarlos, reventar contraseña si es necesario y analizar su contenido.
     7) Localizar algún fichero ejecutable que pueda resultar de interés para la investigación, ademas, analizar la relación con alguna evidencia anterior.
     8) Determinar el contenido del fichero log de un conocido programa de comunicación si es necesario y relacionarlo con el caso investigado.

9) Realizar un análisis de la navegación web.
10) Estudio de los dispositivos físicos que en algún momento fueron conectados al sistema estudiado: móviles, USBs, impresoras, escáneres, cámaras, tarjetas de memoria.
11) Estudio de la información contenida en los unallocated cluster o en el file slack.
12) Información contenida en los archivos de hibernación, paginación, particiones y archivos de intercambio (swap).
13) Análisis de la cola de impresión.
14) Visualización de los links de los archivos y de los archivos accedidos recientemente.
15) Estudio de los metadatos de los archivos, si se considera que pueden ser relevantes para el caso.
16) Estudio de las aplicaciones de virtualización.
17) Estudio de las bases de datos instaladas y las aplicaciones que permiten su gestión.
18) Estudio de los programas de cifrado, particiones cifradas.
19) Análisis de los clientes de correo electrónico y del webmail.

d) Realizar un estudio de la seguridad.

1) Estudiar si las evidencias analizadas han sido comprometidas.
2) Identificar cualquier aplicación vulnerable, software malicioso, evaluar el daño sufrido, identificar los archivos que han sido comprometidos, así como determinar la vía de acceso al sistema.

2. Relativo al resumen ejecutivo, elaboarlo teniendo en cuenta los siguientes apartados.

a) Claridad en la comunicacion, proporcionando información de forma clara y concisa y, por otro lado, utilizar un lenguaje accesible para los no expertos en el área.

b) Presentar el contexto u antecedentes, describibiendo el motivo y las circunstancias del análisis forense y Proporcionar una breve descripción del incidente o situación bajo investigación.

c) Redactar un resumen ejecutivo con los hallazgos clave y las recomendaciones.

d) Describir la metodología utilizada durante el análisis forense.

e) Explicar las herramientas y técnicas de análisis implementadas.

f) Proporcionar una línea de tiempo detallada de los eventos y acciones tomadas.

g) Detallar los hallazgos significativos del análisis.

h) Incluir evidencia técnica relevante, como registros de logs, archivos, etc

i) Evaluar y describir el impacto del incidente en la organización o individuos afectados.

j) Proveer conclusiones basadas en los hallazgos del análisis forense.

k) Proporcionar recomendaciones para la acción futura, basadas en los hallazgos y conclusiones.

l) Sugerir medidas preventivas y correctivas para evitar incidentes similares en el futuro.

3. Elaborar un informe pericial teniendo en cuenta los siguientes apartados.

a) Mantener una postura objetiva e imparcial en todo momento.

b) Garantizar que el análisis y las conclusiones estén fundamentados en evidencias tangibles y replicables.

c) Mantener la cadena de custodia y la integridad de las pruebas durante todo el proceso.

d) Redactar el informe de manera clara, precisa y entendible para personas sin conocimientos técnicos específicos.

e) Describir detalladamente el caso, partes involucradas, y el objeto del peritaje.

f) Detallar las herramientas, técnicas y procedimientos utilizados en el análisis forense.

g) Justificar la elección de la metodología y herramientas utilizadas.

h) Establecer una línea temporal clara de todas las acciones y procesos llevados a cabo durante la investigación

i) Presentar de forma clara y precisa los hallazgos resultantes del análisis forense. Los cuales será

j) Incluir elementos visuales como gráficos, imágenes o tablas para facilitar la comprensión de los datos.

k) Interpretar las evidencias de manera fundamentada y ligada a las normativas y principios de la ciencia forense digital.

l) Derivar conclusiones basadas exclusivamente en las evidencias y hallazgos del análisis.

m) Ofrecer una opinión pericial en base a los hallazgos, respetando los límites de la experticia y los datos disponibles.

n) Garantizar que toda la información manejada se mantiene confidencial y segura.

ñ) Discutir las implicaciones legales de los hallazgos y su posible impacto en el caso.

o) Estar preparado para ratificar el informe en un tribunal y responder a preguntas relacionadas con el análisis y los hallazgos. Este supuesto, el defensor se intuye que se realizará en la defensa síncrona de la defensa de este TFM.

4. Realizar unas conclusiones acordes a todo el TFM realizado.

a) Basarse en ideas fuerza que han aparecido durante todo el TFM.

b) Tener en cuenta que este apartado es el que finalmente, el gerente de la empresa, como miembro directivo de la misma, usando el método del Presidente **DEUDA TÉCNICA: Buscar presidente de los EEUU, preguntar a //4lanoga"**.

DEUDA TÉCNICA: Pendiente de Referenciar!!! ENUNCIADO TFM

1.3. Descripción del entorno de trabajo.

El entorno de trabajo para un análisis forense enfocado en la exploración de memoria RAM y disco duro exige una meticulosa preparación y adecuación de las herramientas y espacios de trabajo. Las evidencias, provenientes tanto de la RAM como del almacenamiento persistente del ordenador en cuestión, se convierten en el pilar fundamental del análisis, permitiendo la evaluación de procesos en ejecución, archivos almacenados, registros de actividad y cualquier otro elemento que pueda arrojar luz sobre las acciones realizadas en la máquina.

En un segundo plano, pero no menos esencial, se encuentra el portátil personal, que se configura como la estación de trabajo principal para la realización del análisis forense. Este debe estar equipado con un sistema operativo que, comúnmente en el ámbito forense, suele ser alguna distribución de Linux, junto con una serie de herramientas específicas para el análisis forense (como Autopsy o Sleuth Kit). No obstante, la selección y configuración de estas herramientas incurren en una deuda técnica que debe ser minuciosamente administrada, asegurando la pertinencia, licencia y compatibilidad de las mismas.

Relativo al ordenador personal destacar las siguientes aplicaciones que se van a utilizar para la realización del análisis.

DEUDA TÉCNICA: Listado de aplicaciones a utilzar en la descripción del entorno de trabajo

Por otro lado, la documentación y redacción del Trabajo de Fin de Máster (TFM) se consolida mediante el uso del repositorio en GitHub TFM-ANALISIS-FORENSE (https://github.com/jrodg85/TFM-ANALISIS-FORENSE). Este repositorio no solo sirve como medio para documentar y presentar los hallazgos y metodologías empleadas, sino que también se erige como una herramienta para gestionar versiones y cambios a lo largo del desarrollo del trabajo, facilitando la trazabilidad y coherencia del mismo. Se deben establecer estrategias robustas para garantizar la integridad y confidencialidad de la información almacenada, considerando la naturaleza sensible de los datos manejados en la investigación forense.

Finalmente, Internet emerge como un recurso invaluable para la investigación, actualización y comunicación a lo largo del proyecto. Navegar por la red debe ser realizado de forma segura y consciente, protegiendo las comunicaciones y asegurando la integridad de las herramientas y datos descargados.

1.4. Listado de tareas.

En esta seccion se ha elaborado despues de una planificacion del trabajo, el cual se han designado el siguiente listado de tareas a realizar. Gracias a este listado, podemos organizar el cómo vamos a realizar el TFM

Destacar que durante el listado de las tareas, cabe mencionar que habran tareas de grooming o refimamiento, ellas no son utilizadas para reduccion de deuda técnica, el objetivo estas jornadas es reflexionar sobre el contenido del mismo y valorar posibilidad de mejorar la organización del mismo. Estas variaciones, gracias a que se está realizando un control de versiones con git, se podrán ver las evoluciones o cambios del TFM en el mismo.
Durante la elaboracion del reto 1 (PEC 1), se realizarán las siguientes tareas.

1. Lectura enunciado actividad 1.
2. Decision de formato de TFM.
3. Maquetacion de TFM en LaTeX.
4. Elaboración de índice.
5. Refinamiento de TFM 1.
6. Diagrama de Gantt.
7. Problema a resolver.
8. Objetivos.
9. Revisión del estado del arte de la informática forense.
10. efinamiento de TFM 2

Durante la elaboracion del reto 2 (PEC 2), se realizarán las siguientes tareas.

1. Lectura enunciado actividad 2
2. Extremos de análisis y previsión de pruebas: Introducción.
3. Extremos de análisis.
4. Previsión de pruebas.
5. Análisis de la memoria RAM: Introduccion.
6. Acciones previas al análisis de RAM.
7. Busqueda de procesos en funcionamiento.
8. Análisis y extracción de procesos sospechosos.
9. Listado de conexiones de red y conexiones sospechosas.
10. Refinamiento TFM 3.

11. Feedback de la PEC 01.
12. Analisis de disco duro: Introducción.
13. Acciones previas al análisis de disco duro.
14. Datos de interés y usuarios del sistema del disco duro analizado.
15. Análisis de las evidencias del disco duro.
16. Planning relativo al resumen ejecutivo.
17. Planning relativo al informe pericial.
18. Adaptacion al indice a los nuevos cambios en los capitulos 6 y 7.
19. Refinamiento TFM 4.

Durante la elaboracion del reto 3 (PEC 3), se realizarán las siguientes tareas.

1. Lectura enunciado actividad 3.
2. Introduccion Resumen ejecutivo.
3. Analisis Ejecutivo.
4. Conclusión de analisis ejecutivo.
5. Refinamiento TFM 5.
6. Feedback de la PEC 02.
7. Introducción del informe pericial.
8. Cuerpo del informe pericial.
9. Conclusiones del informe pericial.
10. Conclusiones TFM.
11. Revision de terminos abrebiaturas y acrónimos.
12. Revisión de imágenes.
13. Revision de referencias.
14. Refinamiento TFM 6.

Durante la elaboracion del reto 4 (PEC 4), se realizarán las siguientes tareas.

1. Revisión de las anotaciones y consejos de la tutora de TFM 1.
2. Ultimas correcciones Feedback TFM 1.
3. Revisión de las anotaciones y consejos de la tutora de TFM 2.
4. Ultimas correcciones Feedback TFM 2.

La Entrega de videos, presentacion y realización de la defensa del TFM, se consideran que estan fuera de este TFM, ya que a partir de la fecha se considera entregado el presente documento.

1.5. Planificación temporal de las tareas.

Para esta sección, se han elaborado los siguientes diagramas de Gantt relativos a cada uno de los retos a entregrar.
Relativo al reto/PEC 1 se establece el siguiente diagrama.

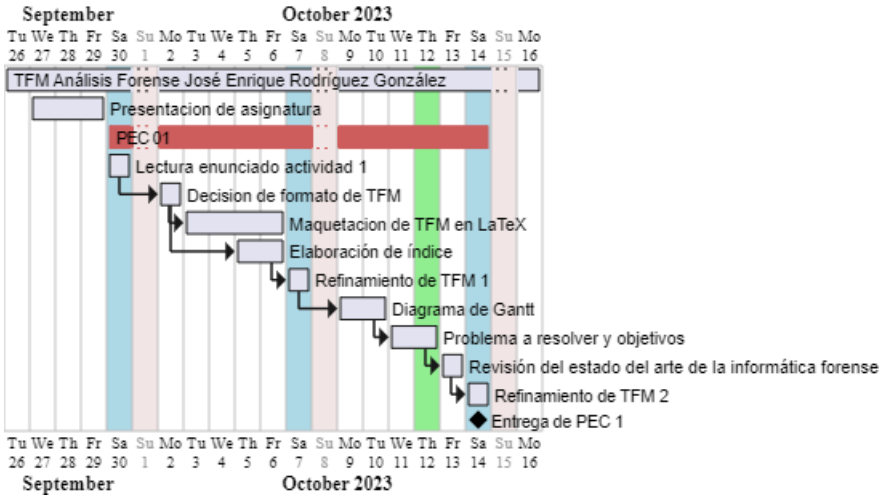


Figura 1.1: Ejemplo de Diagrama de Gantt relativo al reto/PEC 01.

Relativo al reto/PEC 2 se establece el siguiente diagrama.

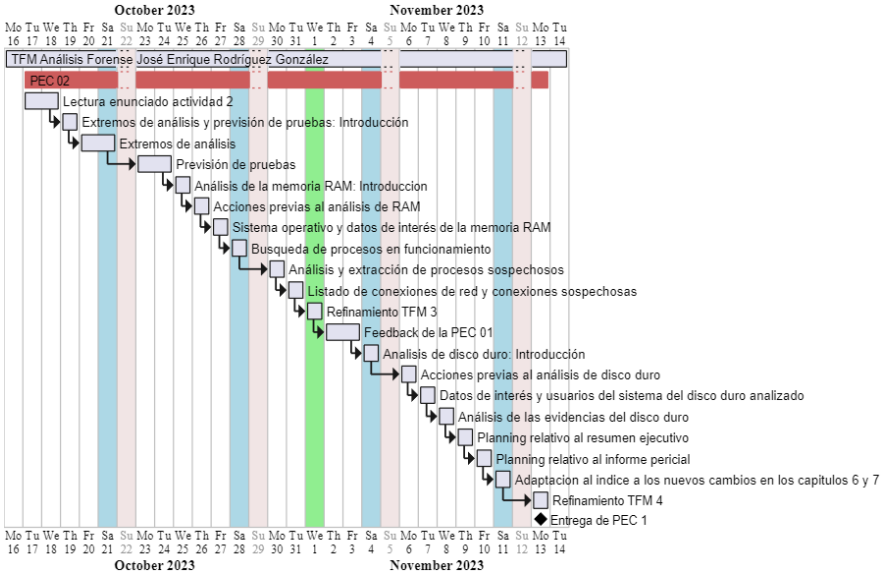


Figura 1.2: Ejemplo de Diagrama de Gantt relativo al reto/PEC 02.

Relativo al reto/PEC 3 se establece el siguiente diagrama.

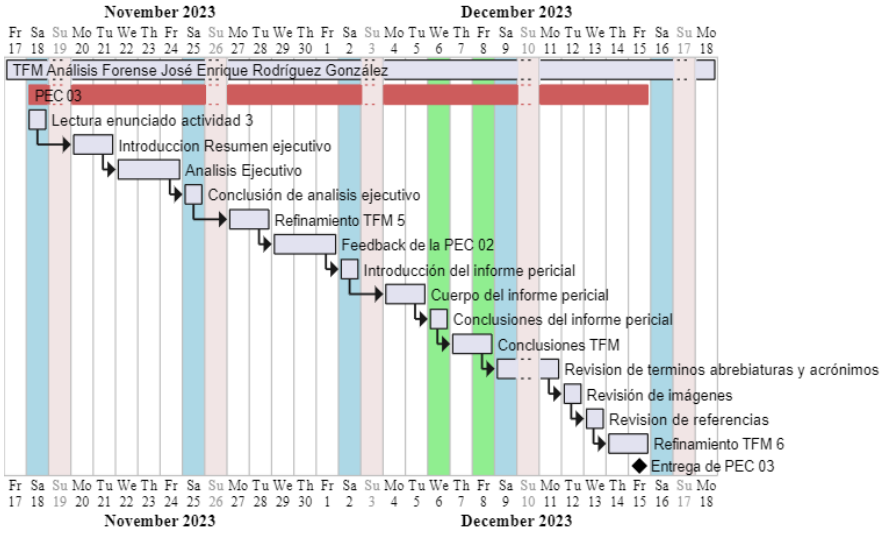


Figura 1.3: Ejemplo de Diagrama de Gantt relativo al reto/PEC 03.

Relativo al reto/PEC 4 se establece el siguiente diagrama.

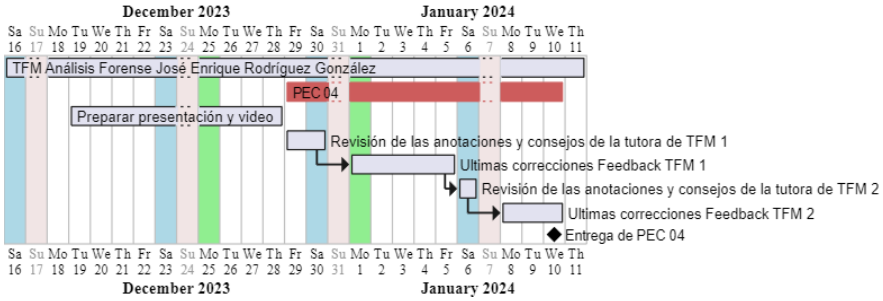


Figura 1.4: Ejemplo de Diagrama de Gantt relativo al reto/PEC 04.

1.6. Revisión del estado del arte de la informática forense.

1.6.1. Introducción

DEUDA TÉCNICA: Revisar código LaTeX de Estado del arte

El análisis forense, también llamado informática forense, computación forense, análisis forense digital o examen forense digital 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.

Esta disciplina no sólo 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 de informática y sistemas para identificar lo que ha ocurrido dentro de cualquier dispositivo electrónico. La formación de un informático forense abarca no sólo el conocimiento del software, sino también de hardware, redes, seguridad, piratería, hackeo y recuperación de información.

La informática forense ayuda a detectar pistas sobre ataques informáticos, robos de información, conversaciones o para recolectar evidencias en correos electrónicos y chats.

La evidencia digital o electrónica es sumamente frágil, de ahí la importancia de mantener su integridad; por ejemplo, el simple hecho de pulsar dos veces en un archivo modificaría la última fecha de acceso del mismo.

Dentro del proceso del análisis forense, un examinador forense digital puede llegar a recuperar información que haya sido borrada desde el sistema operativo. El informático forense debe tener muy presente el principio de intercambio de Locard por su importancia en el análisis criminalístico, así como el estándar de Daubert para hacer admisibles en juicio las pruebas presentadas por el experto forense.

Es muy importante mencionar que la informática o el análisis forense no tiene como objetivo prevenir delitos, por lo que resulta imprescindible tener claros los distintos marcos de actuación de la informática forense, la seguridad informática y la auditoría informática.

1.6.2. Definiciones.

Existen diferentes términos referentes a la ciencia forense en informática. Cada uno de estos términos trata de manera particular o general temas que son de interés para las ciencias forenses.

- **Computación forense (computer forensics):**
    - Disciplina de la ciencia forense que considera los procedimientos en relación con las evidencias para descubrir e interpretar la información

en los medios informáticos con el fin de establecer hipótesis o hechos relacionados con un caso. (Centrada en las consideraciones forenses).

- Disciplina científica que ofrece un análisis de la información que contienen las tecnologías y de los equipos de computación a partir de su compresión.(Centrada en la tecnología).

- **Ciencia forense en las redes (network forensics):**

  - Trata las operaciones de redes de computadores, estableciendo rastros e identificando movimientos y acciones. Es necesario entender los protocolos, configuraciones y la infraestructura de las comunicaciones. A diferencia de la computación forense, es necesario poder establecer relaciones entre eventos diferentes e incluso aleatorios.

- **Ciencia forense digital (digital forensics):**

  - Es una forma de aplicar los conceptos y procedimientos de la criminalística a los medios informáticos o digitales. Su objetivo es apoyar al poder judicial en el contexto de la inseguridad informática es decir, la perpetración de posibles delitos aclarando temas relacionados con incidentes o fraudes.

1.6.3. Objetivos de la informática forense.

La informática forense tiene tres objetivos:
- La compensación de los daños causados por los intrusos o criminales.
- La persecución y procesamiento judicial de los criminales.
- La creación y aplicación de medidas para prevenir casos similares.

Estos objetivos se alcanzan de varias formas, siendo la principal la recopilación de evidencias.

Es importante mencionar que quienes se dedican a la informática forense deben ser profesionales con altos niveles de ética, pues gracias a su trabajo se toman decisiones sobre los hechos y casos analizados.

1.6.4. Evidencia digital.

Los discos duros, las memorias USB y las impresoras (entre otros elementos) se pueden considerar evidencias en un proceso legal, al igual que las huellas digitales o las armas. Las evidencias digitales son las que se extraen de un medio informático.

Características.

Estas evidencias comparten una serie de características que dificultan el ejercicio de la computación forense:

1. Volatilidad.
2. Anonimato.
3. Facilidad de duplicación.
4. Alterabilidad.
5. Facilidad de eliminación.

Categorías.

Estas evidencias se pueden dividir en tres categorías:

1. Registros almacenados en el equipo de tecnología informática (ej. imágenes y correos).

2. Registros generados por equipos de tecnología informática (ej. transacciones, registros en eventos).

3. Registros parcialmente generados y almacenados en los equipos de tecnología informática (ej. consultas en bases de datos).

Dispositivos a analizar.

Cualquier infraestructura informática que tenga una memoria (almacenamiento) es susceptible a los análisis:

- Disco duro de una Computadora o Servidor.
- Documentación referente al caso.
- Tipo de sistema de telecomunicaciones.
- Dirección MAC.
- Inicios de sesiones.
- Información de los cortafuegos.
- IP, redes Proxy. LMhost, host, conexiones cruzadas, pasarelas.
- Software de supervisión y seguridad.
- Credenciales de autentificación.
- Rastreo de paquetes de red.
- Teléfonos móviles o celulares (telefonía móvil)
- Agendas electrónicas (PDA).
- Dispositivos de GPS.
- Impresoras.
- Memorias USB.
- BIOS.

1.6.5. Perspectiva de tres roles.

En el análisis de un caso en el que sea necesario el cómputo forense, hay tres roles principales que son importantes y se deben tener en cuenta: el intruso, el administrador y la infraestructura de la seguridad informática, al igual que el investigador.

Intrusos

El intruso es aquel que ataca un sistema, hace cambios no autorizados, manipula contraseñas o cambia configuraciones, entre otras actividades que ponen a

prueba la seguridad de un sistema. La intención de los intrusos es un punto clave para poder analizar el caso, ya que no se puede comparar un intruso cuya motivación es el dinero con otro cuya motivación es la demostración de sus habilidades. Jeimy J. Cano hace una comparación entre las motivaciones de diferentes tipos de atacantes, basada en el artículo de Steven Furnell, Cybercrime.

En la primera fase (reconocimiento), se busca reconocer y recolectar información. De esta manera, el atacante puede saber cómo puede actuar y los riesgos posibles, para así poder avanzar. En la segunda fase (ataque) se compromete el sistema, avanzando hasta el nivel más alto, teniendo el control del sistema atacado. Esta etapa usualmente se maneja de manera discreta, lo que dificulta la identificación del intruso. Usualmente, la vanidad del intruso y la falta de discreción ayudan al investigador a resolver el caso con mayor facilidad. Finalmente, (en la fase de eliminación) se altera, elimina o desaparece toda la evidencia que pueda comprometer al intruso en algún caso judicial. Del cuidado con el que el atacante proceda en esta fase depende el proceso del informático forense y del caso.

Administradores y la infraestructura de la seguridad informática

El administrador del sistema es el experto encargado de la configuración de este, de la infraestructura informática y de la seguridad del sistema. Estos administradores son los primeros en estar en contacto con la inseguridad de la información, ya sea por un atacante o por una falla interna de los equipos. Al ser los arquitectos de la infraestructura y de la seguridad de la información del sistema, son quienes primero deberían reaccionar ante un ataque. Además, ellos deben proporcionar su conocimiento de la infraestructura del sistema para apoyar el caso y poder resolverlo con mayor facilidad.

Las infraestructuras de seguridad informática (realizadas por el administrador) han avanzado a medida que avanzan las tecnologías. Inicialmente, se utilizaba una infraestructura centralizada en la cual la información se encontraba en un equipo. Por lo tanto, en este caso la seguridad informática se concentraba en el control del acceso a los equipos con la información, al control del lugar en donde se encontraban y en el entrenamiento de quienes estaban encargados de manejar los equipos. Pero con la tecnología fueron cambiando las infraestructuras y las inseguridades cambiaron. Así es como se crearon los proxies, firewall, el sistema de detección de intrusos (IDS) , el sistema de prevención de intrusos (IPS) entre muchas otras herramientas para proveer una mejor seguridad a los sistemas, ya que ahora el acceso no ocurría solo a través de la máquina, sino a través de otras y de la Web.

Por otro lado, es importante hablar de la auditabilidad y trazabilidad, que son propiedades del sistema, relacionados con la infraestructura que son útiles como evidencia para el investigador. La auditabilidad es la capacidad del sistema para registrar los eventos de una acción en particular con el fin de mantener la historia de estos y de realizar un control con mayor facilidad. En cambio, la trazabilidad es la propiedad que tiene un sistema para rastrear o reconstruir relaciones entre diferentes objetos monitorizados.

Es importante resaltar que el administrador debe conocer lo suficiente sobre la infraestructura del sistema para poder colaborar con el caso, ya que su análisis puede facilitar el proceso del investigador forense. Adicionalmente, contar con los

rastros y registro de eventos (Auditoría informática) en los sistemas es crucial para el administrador y su infraestructura, no solo porque genera confianza en sus clientes, sino también porque es una buena práctica en términos de seguridad para toda la empresa.

Investigador

Es un nuevo profesional que actúa como experto, criminalista digital, o informático. Comprende y conoce las nuevas tecnologías de la información. Además, el investigador analiza la inseguridad informática emergente en los sistemas. El perfil del investigador es nuevo y necesario en el contexto abierto informático en el que vivimos. Por lo tanto, es necesario formar personas que puedan trabajar como investigadores en la disciplina emergente de la criminalística digital y el cómputo forense. Estas prácticas emergentes buscan articular las prácticas generales de la criminalística con las evidencias digitales disponibles en una escena del crimen. El trabajo del informático es indagar en las evidencias, analizarlas y evaluarlas para poder decidir cómo estas evidencias pueden ayudar a resolver el caso. Por lo tanto, es ideal que un investigador tenga conocimientos (al menos) sobre las siguientes áreas: justicia criminal, auditoría, administración y operación de tecnologías de Información.

En una investigación informática forense, hay ocho roles principales en un caso: el líder del caso, el propietario del sistema, el asesor legal, el auditor/ingeniero especialista en seguridad de la información, el administrador del sistema, el especialista en informática forense, el analista en informática forense y el fiscal. Usualmente, entre todos estos roles, los informáticos forenses pueden tomar los siguientes cuatro roles:

- Líder del caso: es aquel que planea y organiza todo el proceso de investigación digital. Debe identificar el lugar en donde se realizará la investigación, quienes serán los participantes y el tiempo necesario para esta.

- Auditor/ingeniero especialista en seguridad de la información: conoce el escenario en donde se desarrolla la investigación. Tiene el conocimiento del modelo de seguridad, los usuarios y las acciones que pueden realizar en el respectivo sistema. A partir de sus conocimientos debe entregar información crítica a la investigación.

- Especialista en informática forense: es un criminalista digital que debe identificar los diferentes elementos probatorios informáticos vinculados al caso, determinando la relación entre los elementos y los hechos para descubrir el autor del delito.

- Analista en informática forense: examina en detalle los datos, los elementos informáticos recogidos en la escena del crimen con el fin de extraer toda la información posible y relevante para resolver el caso.

1.6.6. Pasos del proceso del cómputo forense.

A continuación se describe el proceso de análisis forense:

Identificación

Es muy importante conocer los antecedentes a la investigación "HotFix", la situación actual y el proceso que se quiere seguir para poder tomar la mejor decisión con respecto a las búsquedas y las estrategias (debes estar bien programado

y sincronizado con las actividades a realizar, herramientas de extracción de los registros de información a localizar). Incluye muchas veces (en un momento específico observar, analizar e interpretar y aplicar la certeza, esto se llama criterio profesional que origina la investigación) la identificación del bien informático, su uso dentro de la red, el inicio de la cadena de custodia (proceso que verifica la integridad y manejo adecuado de la evidencia), la revisión del entorno legal que protege el bien y del apoyo para la toma de decisión con respecto al siguiente paso una vez revisados los resultados.

Preservación

Este paso incluye la revisión y generación de las imágenes forenses de la evidencia para poder realizar el análisis. Esta duplicación se realiza utilizando tecnología punta para poder mantener la integridad de la evidencia y la cadena de custodia requerida (soportes). Al realizar una imagen forense, nos referimos al proceso que se requiere para generar una copia "bit-a-bit"(copia binaria) de todo el disco duro, el cual permitirá recuperar (en el siguiente paso) toda la información contenida y borrada del disco duro. Para evitar la contaminación del disco duro, normalmente se ocupan bloqueadores de escritura de hardware, los cuales evitan el contacto de lectura con el disco, lo que provocaría una alteración no deseada en los medios.

Análisis

Proceso de aplicar técnicas científicas y analíticas a los medios duplicados por medio del proceso forense para poder encontrar pruebas de ciertas conductas. Se pueden realizar búsquedas de cadenas de caracteres, acciones específicas del o de los usuarios de la máquina como son el uso de dispositivos de USB (marca, modelo), búsqueda de archivos específicos, recuperación e identificación de correos electrónicos, recuperación de los últimos sitios visitados, recuperación de la caché del navegador de Internet, etc.

Presentación

Es la recopilación de toda la información que se obtuvo a partir del análisis para realizar el reporte y la presentación a los abogados, jueces o instancias que soliciten este informe, la generación (si es el caso) de una pericial y de su correcta interpretación sin hacer uso de tecnicismos; se deberá presentar de manera cauta, prudente y discreta al solicitante la documentación, ya que siempre existirán puertas traseras dentro del sistema en observación. Debe ser muy específica la investigación dentro del sistema que se documenta porque se compara y vincula una plataforma de telecomunicación y cómputo forense que están muy estrechamente enlazadas, sin olvidar los medios de almacenamiento magnéticos portables basados en software libre y privativo. La información que se transmite debe manejarse con cuidado, porque el prestigio técnico depende de las plataformas y los sistemas

Para poder realizar con éxito su trabajo, el investigador nunca debe olvidar:

- Ser imparcial. Solamente analizar y reportar lo encontrado.
- Realizar una investigación formal sin conocimiento y experiencia.
- Mantener la cadena de custodia (proceso que verifica la integridad y manejo adecuado de la evidencia).
- Documentar toda actividad realizada.

El especialista debe conocer también sobre:

- Desarrollo de los exploit (vulnerabilidades), esto le permite al informático forense saber qué tipo de programas se pondrán de moda, para generar una base de estudio que le permita observar patrones de comportamiento.

1.6.7. Retos y riesgos en el cómputo forense.

Al estar en un escenario que evoluciona constantemente, cada vez surgen más retos y riesgos en el área de la informática forense. Entre ellos la formación de informáticos forenses, la confiabilidad de las herramientas, la facilidad de la destrucción de las evidencias, las amenazas estratégicas y tácticas que plantea el ciberterrorismo; y las tecnologías emergentes como la nube, las tecnologías móviles, y las redes sociales. Algunos de estos temas se abordarán a continuación:

Formación de informáticos forenses

Los criminales informáticos son una nueva generación de delincuentes, en este contexto, es necesario desarrollar un nuevo tipo de investigadores: los informáticos forenses. En este momento es un desafío encontrar personas que tengan este perfil, ya que no existen suficientes programas que realicen este tipo de formación. Adicionalmente, en este momento, la mayoría de las personas ignoran la importancia de los informáticos forenses porque no son conscientes de la dimensión del cibercrimen. Usualmente se cree que no es algo tan grave y se le da mayor importancia a otro tipo de crímenes.

Por lo tanto, se deben plantear programas e iniciativas para poder realizar esta formación. Según investigaciones e iniciativas ya realizadas, hay cuatro componentes principales que deben estar presentes en un programa de computación forense o forensia digital: contenido multidisciplinario, ejercicios prácticos, profesores de calidad y ejemplos del mundo real (investigación de Taylor Endicott-Popovsky y Phillips, 2007).

- *Contenido multidisciplinario:* técnico en informática, conocimiento de criminalística, seguridad y delitos informáticos, entre otros.
- *Ejercicios prácticos en el laboratorio:* con herramientas tecnológicas forenses, en diferentes niveles de dificultad y variedad de componentes a analizar.
- *Profesores calificados:* con alto conocimiento en el tema.
- *Ejemplos del mundo real:* con el fin de dar mayor profundidad al aprendizaje.

Confiabilidad de las herramientas

Las herramientas existentes disponibles para el cómputo forense presentan otro reto. Las herramientas licenciadas exigen a los investigadores inversiones altas (tanto en hardware, como en software), al adquirirlas y para mantenerlas. Adicionalmente, como las herramientas están avanzando constantemente requieren técnicos y usuarios que estén constantemente aprendiendo las actualizaciones, las modificaciones y los posibles errores. Por otro lado, las herramientas de código abierto son cuestionadas en muchos tribunales por su confiabilidad. Por lo tanto, no se recomiendan a la hora de usarse en una audiencia.

Es por esto que el NIST (National Institute of Standards and Technology de Estados Unidos) ha planteado importantes investigaciones para probar y poner reglas para las herramientas del cómputo forense, en su proyecto NIST Computer Forensic Tool Testing Program. Las pruebas realizadas serán útiles para cumplir las exigencias del test de Daubert standard, prueba que establece la confiabilidad de las herramientas en computación forense

1.6.8. Herramientas de Análisis Forense.

La siguiente tabla compara cuatro herramientas reconocidas internacionalmente al ser muy completas. Luego, se encuentra una lista más completa de herramientas útiles para la labor del investigador.

Cuadro 1.1: Comparativa de herramientas forenses

Herramienta	Licencia	Imagen	Control de Integridad	Administración del caso
Encase	SÍ	SÍ	SÍ	SÍ
Forensic Toolkit	SÍ	SÍ	SÍ	SÍ
Winhex	SÍ	SÍ	SÍ	SÍ
Sleuth Kit	NO	SÍ	SÍ	SÍ

- Air (Forensics Imaging GUI).
- Autopsy (Forensics Browser for Sleuth Kit)Cryptcat (Command Line)Deep Freeze.
- Dcfldd (DD Imaging Tool command line tool and also works with AIR).
- Dumpzilla (Forensics Browser: Firefox, Iceweasel and Seamonkey).
- Encase: `https://www.guidancesoftware.com/encase-forensic?cmpid=nav_r`
- Exif Viewer (Visor de metadatos en imágenes).
- Faces.
- Foremost (Data Carver command line tool).
- Forensik Toolkit: `https://accessdata.com/products-services/forensic-toolkit-ftk`.
- Helix.
- Hetman software (Recuperador de datos borrados por los criminales).
- Hiren´s boot.
- Md5deep (MD5 Hashing Program).
- Metashield Analyser Online (Analizador de metadatos online).
- Mini XP.

- NTFS-Tools.
- Netcat (Command Line).
- Net resident.
- NetFlow.
- Py-Flag (Forensics Browser).
- Qtparted (GUI Partitioning Tool).
- R-Studio Emergency (Bootable Recovery media Maker).
- R-Studio Network Edtion.
- R-Studio RS Agent.
- Regviewer (Windows Registry).
- Sleuth Kit (Forensics Kit. Command Line): `https://www.sleuthkit.org/`.
- Snort.
- Viewer.
- Volatility (Reconstrucción y análisis de memoria RAM).
- X-Ways Forensics.
- X-Ways WinHex `https://www.x-ways.net/winhex/`.
- X-Ways WinTrace.

Herramientas para el análisis de discos duros

- AccessData Forensic ToolKit (FTK).
- Guidance Software EnCase.
- Kit Electrónico de Transferencia de datos.

Herramientas para el análisis de correos electrónicos

- Paraben
- AccessData Forensic ToolKit (FTK)

Herramientas para el análisis de dispositivos móviles

- Cellebrite UFED Touch 2, Physical Analyzer.
- AccessData Mobile Phone Examiner Plus (MPE+)

Herramientas para el análisis de redes

- E-Detective - Decision Computer Group
- SilentRunner - AccessData
- NetworkMiner
- Netwitness Investigator

Herramientas para filtrar y monitorear el tráfico de una red tanto interna como a internet

- Tcpdump
- USBDeview
- SilentRunner - AccessData
- WireShark

Términos importantes

- *Cadena de custodia:* la identidad de personas que manejan la evidencia en el tiempo del suceso y la última revisión del caso. Es la responsabilidad de la persona que maneja la evidencia asegurar que los artículos son registrados y contabilizados durante el tiempo en el cual están en su poder, y que son protegidos, así mismo llevando un registro de los nombres de las personas que manejaron la evidencia o artículos durante el lapso de tiempo y fechas de entrega y recepción.
- *Imagen forense:* técnica llamada también .espejeo"(en inglés "Mirroring"), la cual es una copia binaria de un medio electrónico de almacenamiento. En la imagen quedan grabados los espacios que ocupan los archivos y las áreas borradas incluyendo particiones escondidas.
- *Análisis de archivo:* examina cada archivo digital descubierto y crea una base de datos de información relacionada al archivo (metadatos, etc.), consistente entre otras cosas en la firma del archivo o hash (indica la integridad del archivo).

DEUDA TÉCNICA: Revisar código LaTeX de Estado del arte DEUDA TÉCNICA: plantear posible reducción del estado del arte DEUDA TÉCNICA: Referencia a WIKIPEDIA

Capítulo 2

Extremos del análisis y previsión de pruebas técnicas.

En la era digital actual, la capacidad de llevar a cabo análisis forenses en ordenadores se ha convertido en una competencia crítica dentro del ámbito de la investigación criminal. El análisis forense informático permite a los investigadores descubrir, preservar y analizar datos en dispositivos electrónicos que pueden ser críticos para resolver delitos. Este capítulo se dedica al estudio meticuloso de los métodos y prácticas estándar en la computación forense, con un enfoque específico en la adquisición y análisis de datos de la memoria RAM y discos duros. Se expondrá la metodología utilizada para garantizar la integridad de la evidencia y se ilustrarán los desafíos asociados a la recolección y el análisis de datos digitales.

Con el avance de la tecnología, los investigadores forenses enfrentan la dualidad de oportunidades y desafíos. Por un lado, las herramientas modernas ofrecen capacidades sin precedentes para recuperar y analizar datos; por otro lado, la creciente sofisticación del software y hardware supone nuevos niveles de complejidad y la necesidad de constante actualización en conocimientos y técnicas. Este capítulo también contempla la noción de deuda técnica asociada a la utilización de herramientas y sistemas operativos en la investigación forense, reconociendo la importancia de mantener un enfoque crítico hacia las herramientas utilizadas.

La documentación y control de versiones son aspectos cruciales en cualquier proyecto de investigación y desarrollo, más aún en el ámbito forense digital, donde la transparencia y reproducibilidad son fundamentales. Se detallará el uso del repositorio de Github (https://github.com/jrodg85/TFM-ANALISIS-FORENSE) para la documentación del TFM y el control de versiones aplicado al proceso de análisis forense. Se discutirá la relevancia de la colaboración y el seguimiento preciso de cambios en el código y documentos relacionados con el proyecto.

Finalmente, no se puede ignorar el papel fundamental que juega el acceso a recursos online en la actualización constante y el acceso a información relevante y actualizada en el campo de la forense digital. La Internet es una fuente inagotable de conocimiento, pero también presenta riesgos que deben ser gestionados con prudencia. En resumen, este capítulo traza el panorama del análisis forense en ordenadores, describiendo las herramientas y metodologías utilizadas, así como las mejores prácticas en la documentación y gestión de la información digital en investigaciones forenses.

Esta introducción proporciona una vista general y establece las expectativas para el contenido que seguirá, preparando al lector para los detalles técnicos y metodológicos que se presentarán en el capítulo.

2.1. Propuesta de extremos.

La presente investigación tiene como propósito fundamental el establecimiento de un marco metodológico para el análisis forense de ordenadores, específicamente orientado hacia la identificación, recolección y análisis de evidencias digitales que puedan ser presentadas en un entorno judicial. A continuación, se delinean los extremos de esta propuesta:

Objeto de Estudio:

- La investigación se centrará exclusivamente en el análisis forense del material facilitado para el desarrollo de la asignatura por parte del profesorado de la asignatura.
- Se realizará una breve indicacion sobre la aplicacion utilizada con cada uno de los objetivos del presente TFM.

Alcance metodológico:

- La validación de la integridad de la evidencia se hará mediante el uso de funciones hash estándar.
- Se examinarán las metodologías para el análisis de la memoria volátil y no volátil.

Limitaciones:

- La validación de la integridad de la evidencia se hará mediante el uso de funciones hash estándar.
- Se examinarán las metodologías para el análisis de la memoria volátil y no volátil.

Exclusiones:

- No se utilizará material de analisis que no sea el proporcionado por la asignatura.

2.2. Previsión de pruebas técnicas.

Pruebas técnicas:

- El propósito de estas pruebas técnicas es lo indicado en el apartado de problema a resolver del presente Trabajo de fin de master
  - Solventar las necesidades del gerente de la empresa mediante el análisis forense del disco duro y la captura de memoria de un ordenador personal, en un caso real con un sistema virtualizado.
  - Posible vinculación con una presunta conducta delictiva real.
- Importancia de las pruebas para validar la hipótesis y objetivos de investigación.
  - La posible imputación de los hechos ocurridos y tomar posibles medidas legales contra el autor univoco de la acción detectada.

Marco metodológico de las pruebas:

- Las pruebas que se realizarán serán una investigación y un estudio temporal de los hechos ocurridos dentro del pc.
- Se emplearán herramientas de análisis forense en sus distintos sistemas operativos (Linux/Windows) para su detección.
- se tratará de arrancar el sistema virtualizado para posible carving de la información del disco duro por posible eliminación de pruebas por parte del posible infractor.
- La planificación de las pruebas ha quedado detallado en la sección "planificación temporal de las tareas".

Criterios de éxito de las pruebas:

- Análisis de los incidentes ocurridos con una justificación probatoria del mismo.
- Realización de un análisis de seguridad de las vulnerabilidades detectadas y una via de mitigación de los mismos.

Cronograma de pruebas:

- El cronograma de las pruebas ha quedado detallado en la sección "planificación temporal de las tareas".
- Hitos importante, fechas de entrega de las PEC.

Capítulo 3

Análisis de la memoria RAM.

El análisis forense de la memoria RAM es un componente crítico en la investigación digital, pues permite a los analistas extraer información valiosa que no persiste una vez que el dispositivo se apaga. Esta volatilidad hace que la memoria RAM sea una fuente de evidencia esencial, especialmente en casos donde los procesos activos y la información en tránsito son relevantes para el caso. El presente capítulo detalla un enfoque metodológico estructurado para examinar de manera exhaustiva el contenido de la memoria RAM capturada de un sistema informático, con el objetivo de identificar y analizar aspectos críticos que contribuyan a la investigación.

Las acciones específicas que se abordarán son las siguientes:

1. **Comprobación del MD5:**

   Iniciaremos con la verificación de la integridad del volcado de la memoria RAM mediante el cálculo de su suma de verificación MD5. Este paso es fundamental para asegurar que los datos analizados no han sido alterados desde el momento de su adquisición, garantizando así la cadena de custodia digital.

2. **Búsqueda de Datos de Interés:**

   Seguiremos con la inspección minuciosa del contenido de la memoria para identificar información potencialmente relevante para el caso. Esto incluye, pero no se limita a, datos residuales de aplicaciones, fragmentos de comunicaciones y elementos que puedan ser reconstruidos para obtener evidencia. Servirá para tener una previsión de por donde dirigir el estudio de todo el analisis forense.

3. **Identificación del Sistema Operativo:**

   Aunque ya intuyamos, por el apartado anterior datos básicos del Sistema operativo, es vital determinar la versión y configuración del sistema operativo en uso, ya que esto influirá en la interpretación de los datos y en la selección de las herramientas de análisis adecuadas.

4. **Búsqueda de Procesos en Funcionamiento de Interés:**

   Un punto focal de nuestra investigación será el examen de los procesos activos en el momento de la captura de la memoria. Esta inspección nos

permitirá comprender mejor el estado del sistema antes del apagado o la hibernación.

5. **Análisis y Extracción de Procesos Sospechosos:**

   Finalmente, nos concentraremos en reconstruir y examinar las conexiones de red activas y pasivas. El objetivo es identificar patrones de tráfico inusuales o conexiones que puedan indicar comunicación con servidores de comando y control, exfiltración de datos o cualquier otra actividad que se considere sospechosa.

El resultado de este análisis exhaustivo proporcionará una comprensión detallada de lo que estaba ocurriendo en el sistema en el momento de la captura de la memoria. Esta información es invaluable para formar una imagen completa de los eventos bajo investigación y para establecer hechos concretos que puedan ser presentados como evidencia en un entorno judicial.

3.1. Acciones previas al análisis de la memoria RAM.

3.2. Datos de interés de la captura de la memoria RAM.

3.3. Sistema Operativo de la memoria RAM analizada.

3.4. Busqueda de procesos en funcionamiento de interés para el análisis.

3.5. Análisis y extracción de procesos sospechosos.

3.6. Listado de conexiones de red y conexiones sospechosas.

Capítulo 4

Análisis del disco duro.

4.1. Acciones previas al análisis del disco duro.

4.2. Datos de interés del disco duro.

4.3. Usuarios del sistema.

4.4. Análisis de evidencias del disco duro.

Capítulo 5

Resumen ejecutivo.

Capítulo 6

Informe pericial.

Capítulo 7

Conclusiones.

Capítulo 8

Anexos.

8.1. Glosario de términos y abreviaturas.

CISO

8.2. Imágenes.