|  |  |
| --- | --- |
| **Análisis forense de un ordenador.** | |
|  | |
| Shape, rectangle  Description automatically generated | **José Enrique Rodríguez González.**  M1.881 - TFM - Análisis forense  **Nombre Tutor/a de TF**  Dña. Elena Botana de Castro.  **Profesor/a responsable de la asignatura**  D. Jordi Serra Ruiz.  **Fecha Entrega:** Enero de 2024 |

  
Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-SinObraDerivada [3.0 España de Creative Commons](http://creativecommons.org/licenses/by-nc-nd/3.0/es/)

**FICHA DEL TRABAJO FINAL**

|  |  |
| --- | --- |
| **Título del trabajo:** | *Análisis forense de un ordenador.* |
| **Nombre del autor:** | *José Enrique Rodríguez González.* |
| **Nombre del consultor/a:** | *Dña. Elena Botana de Castro.* |
| **Nombre del PRA:** | *D. Jordi Serra Ruiz.* |
| **Fecha de entrega (mm/aaaa):** | *01/2024* |
| **Titulación o programa:** | Master Universitario de Ciberseguridad y privacidad. |
| **Área del Trabajo Final:** | *Análisis forense.* |
| **Idioma del trabajo:** | *Castellano.* |
| Palabras clave | *Máximo 3 palabras clave, validadas por el tutor/a del TF* |
| **Resumen del Trabajo** | |
| El objetivo del presente Trabajo de Fin de Máster es realizar un análisis forense de un ordenador del que se sospecha de que han accedido a los sistemas de forma ilícita. Se comprobará si realmente han accedido, así como el método que han utilizado. Por otro lado, se elaborará un informe con las consecuencias que se derivan del dicho acceso además se comprobará si ha habido extracción de información alguna.  Por último, y no menos importante, para el presente trabajo se tendrán en cuenta los estándares que existen en la actualidad, como pueden ser la norma ISO 27037, la RFC 3227 o las normas de la Asociación Española de Normalización UNE 71505 y UNE 71506. | |
| **Abstract** | |
| The objective of this Master's Thesis is to carry out a forensic analysis of a computer that is suspected of having accessed the systems illicitly. It will be checked whether they have really accessed, as well as the method they have used. On the other hand, a report will be prepared with the consequences that arise from said access, and it will also be verified if there has been any extraction of information.  Lastly, and not least, for this work, the standards that currently exist will be considered, such as the ISO 27037 standard, the RFC 3227 or the standards of the Spanish Association for Standardization UNE 71505 and UNE 71506. | |

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 qué estos tres años que llevo realizando este master y han conocido todos los derroteros que me ha llevado este camino.

Índice

[1. Plan de trabajo 1](#_Toc154822693)

[1.1. Problema por resolver. 1](#_Toc154822694)

[1.2. Objetivos. 1](#_Toc154822695)

[1.3. Metodologías. 4](#_Toc154822696)

[1.1. Objetivos 17](#_Toc154822697)

[1.2. Descripción del entorno de trabajo 17](#_Toc154822698)

[1.3. Listado de tareas 17](#_Toc154822699)

[1.4. Planificación temporal de las tareas 17](#_Toc154822700)

[1.5. Revisión del estado del arte de la informática forense 18](#_Toc154822701)

[2. Extremos del análisis y previsión de pruebas técnicas 19](#_Toc154822702)

[2.1. Propuesta de extremos 19](#_Toc154822704)

[2.2. Previsión de pruebas técnicas 19](#_Toc154822705)

[3. Análisis de la memoria RAM 20](#_Toc154822706)

[4. Análisis del disco duro 21](#_Toc154822707)

[5. Resumen ejecutivo 22](#_Toc154822708)

[6. Informe pericial 23](#_Toc154822709)

[7. Conclusiones 24](#_Toc154822710)

[8. Referencias bibliográficas 25](#_Toc154822711)

[9. Anexos 26](#_Toc154822712)

Lista de figuras

[Figura 1 4](#_Toc112788354)

# 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.

## 1.1. Problema por 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 Trabajo de Final de Máster (en adelante 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.

## 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.
   1. Realizar una recuperación parcial o total de la información borrada existente en los dispositivos susceptibles de ser analizados (carving).
   2. 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.
   3. Relativo al análisis del Disco Duro.
      1. Comprobar la integridad del disco duro.
      2. Determinar la siguiente información del disco duro.
         1. Sistema y versión del sistema operativo instalado.
         2. Nombre del propietario y relación de software instalado.
         3. "Product ID" y "Product Key" asociadas al sistema.
         4. Fecha y hora de instalación del sistema operativo.
      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 algún fichero ejecutable que pueda resultar de interés para la investigación, además, analizar la relación con alguna evidencia anterior.
      7. Determinar el contenido del fichero log de un conocido programa de comunicación si es necesario y relacionarlo con el caso investigado.
      8. Realizar un análisis de la navegación web.
      9. Visualización de los enlaces de los archivos y de los archivos accedidos recientemente.
      10. Estudio de los metadatos de los archivos, si se considera que pueden ser relevantes para el caso.
      11. Estudio de las bases de datos instaladas y las aplicaciones que permiten su gestión.
      12. Estudio de los programas de cifrado, particiones cifradas.
      13. Análisis de los clientes de correo electrónico y del webmail.
   4. 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, elaborarlo teniendo en cuenta los siguientes apartados.
   1. Claridad en la comunicación, proporcionando información de forma clara y concisa y, por otro lado, utilizar un lenguaje accesible para los no expertos en el área.
   2. Presentar el contexto u antecedentes, describiendo el motivo y las circunstancias del análisis forense y Proporcionar una breve descripción del incidente o situación bajo investigación.
   3. Redactar un resumen ejecutivo con los hallazgos clave y las recomendaciones.
   4. Describir la metodología utilizada durante el análisis forense.
   5. Explicar las herramientas y técnicas de análisis implementadas.
   6. Proporcionar una línea de tiempo detallada de los eventos y acciones tomadas.
   7. Incluir evidencia técnica relevante, como registros de logs, archivos.
   8. Evaluar y describir el impacto del incidente en la organización o individuos afectados.
   9. Proveer conclusiones basadas en los hallazgos del análisis forense.
   10. Proporcionar recomendaciones para la acción futura, basadas en los hallazgos y conclusiones.
3. Elaborar un informe pericial teniendo en cuenta los siguientes apartados.
   1. Mantener una postura objetiva e imparcial en todo momento.
   2. Garantizar que el análisis y las conclusiones estén fundamentados en evidencias tangibles y replicables.
   3. Mantener la cadena de custodia y la integridad de las pruebas durante todo el proceso.
   4. Redactar el informe de manera clara, precisa y entendible para personas sin conocimientos técnicos específicos.
   5. Detallar las herramientas, técnicas y procedimientos utilizados en el análisis forense.
   6. Justificar la elección de la metodología y herramientas utilizadas.
   7. Presentar de forma clara y precisa los hallazgos resultantes del análisis forense. Los cuáles será
   8. Interpretar las evidencias de manera fundamentada y ligada a las normativas y principios de la ciencia forense digital.
   9. Derivar conclusiones basadas exclusivamente en las evidencias y hallazgos del análisis.
   10. Ofrecer una opinión pericial en base a los hallazgos, respetando los límites de la prueba pericial y los datos disponibles.
   11. Discutir las implicaciones legales de los hallazgos y su posible impacto en el caso.
   12. 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.
   1. Basarse en ideas fuerza que han aparecido durante todo el TFM.
   2. 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 Reagan.

## 1.3. Metodologías.

Introducción.

En esta sección se procederá a realizar un repaso general de algunas de las normativas y estándares.

Primero abordaremos un pequeño estudio relativo a las normas ISO 27037 e ISO 30131, posteriormente abordaremos la normativa RFC 3227 para finalmente comentar un resumen de las normas UNE 71505 y UNE 71506.

Por último, pero no menos importante, trataré unas conclusiones sobre esta sección.

Normas ISO 27037 e ISO 30121.

Dentro de la seguridad informática cabe destacar una normativa ampliamente conocida, es la familia ISO 27000. Esta serie de normas son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

Esta serie contiene diversas normas todas relacionadas con las mejores prácticas recomendadas en Seguridad de la Información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI).

Concretamente, existe una norma dedicada en exclusiva al análisis forense, se trata de la ISO 27037 Directrices para la identificación, recolección, adquisición y preservación de la prueba digital.

Esta norma ofrece orientación para tratar situaciones frecuentes durante todo el proceso de tratamiento de las pruebas digitales. Además, define dos roles especialistas:

* DEFR **(Digital Evidence First Responders)**: Expertos en primera intervención de evidencias electrónicas.
* DES **(Digital Evidence Specialists)**: Experto en gestión de evidencias electrónicas.

ISO 27037 proporciona orientación para los siguientes dispositivos y circunstancias:

* Medios de almacenamiento digitales utilizados en equipos varios como por ejemplo discos duros, disquetes, discos magneto-ópticos y ópticos y otros similares.
* Teléfonos móviles, PDA's, tarjetas de memoria.
* Sistemas de navegación móvil (GPS).
* Cámaras de video y cámaras digitales (incluyendo circuitos cerrados de televisión).
* Ordenadores estándares con conexiones a redes.
* Redes basadas en protocolos TCP/IP y otros protocolos digitales.
* Otros dispositivos con funcionalidades similares a las descritas anteriormente.

Resumiendo, se puede destacar que esta norma ofrece orientación sobre el manejo de las pruebas digitales. Siguiendo las directrices de esta norma se asegura que la evidencia digital potencial se recoge de manera válida a efectos legales para facilitar su aportación en juicios y procesos legales. Además, cabe destacar que cubre una amplia gama de tipos de dispositivos y situaciones, por lo que la orientación dentro de la norma es ampliamente aplicable.

Se dispone de una copia de la ISO 27037 en inglés.

La ISO/IEC 30121 es la norma internacional para el análisis forense digital. Define los requisitos mínimos que todas las organizaciones deben cumplir para estar preparados ante un análisis forense digital. La primera edición de la norma se publicó en 2015. Desde entonces, se han realizado varias actualizaciones importantes para reflejar las

nuevas tecnologías y la evolución de los procedimientos de investigación criminal. Ha sido adoptada por muchas organizaciones de todo el mundo como base de las mejores prácticas para el manejo de las pruebas digitales, maximizando la disponibilidad y acceso a esta.

La ISO/IEC 30121 se creó para garantizar que las pruebas digitales se traten de forma coherente en las distintas organizaciones y para ayudar a garantizar que las pruebas digitales puedan utilizarse como prueba en los procedimientos judiciales.

Norma RFC 3227.

Otra norma destacable para mencionar es la RFC 3227. Este documento publicado por la Internet Engineering Task Force (IETF) recoge directrices para recopilar y almacenar evidencias sin ponerlas en riesgo.

En cuanto a los principios para la recolección de evidencias destacan básicamente tres, el orden de volatilidad de los datos, las acciones que deben evitarse y las consideraciones sobre la privacidad.

Sobre el procedimiento de almacenamiento tiene en cuenta la cadena de custodia de las pruebas recogidas anteriormente y dónde y cómo se deben almacenar estas para que estén a buen recaudo.

Para acabar detalla qué tipo de herramientas son las más útiles y qué características deben tener para evitar conflictos, haciendo hincapié en que las herramientas deben alterar lo menos posible el escenario. Según este documento el kit de análisis debe incluir las siguientes herramientas:

* Programas para listar y examinar procesos.
* Programas para examinar el estado del sistema.
* Programas para realizar copias bit a bit.

Todas estas recomendaciones tienen como epicentro el principio de intercambio de Locard, que señala que: "siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto".

Se dispone de una copia de la RFC 3227 en español.

Normas UNE 71505 y UNE 71506.

Las normas UNE son normas técnicas desarrolladas por el organismo español de normalización, la Asociación Española de Normalización (UNE). "UNE" es el acrónimo de "Una Norma Española". Estas normas establecen especificaciones técnicas, criterios y directrices que deben seguirse en la fabricación, diseño, instalación, uso o mantenimiento de productos, sistemas o servicios en España.

Estas normas que tratamos en el presente trabajo tienen como finalidad dar una metodología para la preservación, adquisición, documentación, análisis y presentación de pruebas digitales.

Según la asociación esta norma debe dar respuesta a las infracciones legales e incidentes informáticos en las distintas empresas y entidades. Con la obtención de dichas pruebas digitales, que serán más robustas y fiables siguiendo la normativa, se podrá discernir si su causa tiene como origen un carácter intencional o negligente.

Estas normativas se aplican a cualquier organización con independencia de su actividad o tamaño, así como a cualquier profesional competente en este ámbito. Se dirige especialmente a incidentes y seguridad, así como al personal técnico que trabaje en laboratorios o entornos de análisis forense de evidencias electrónicas.

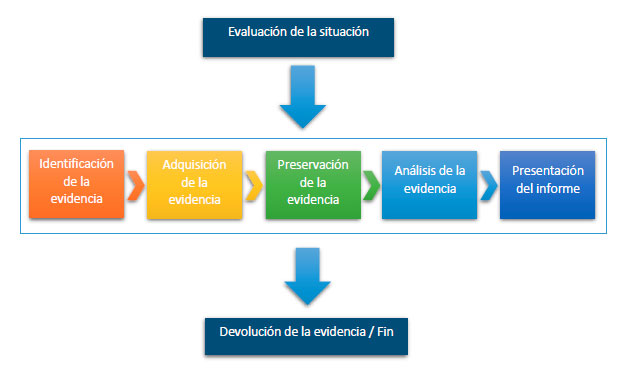
Se dispone de una copia de la norma UNE 71505 en el siguiente repositorio de la referencia que a continuación se detalla.

Conclusiones relativo a las metodologías.

Tras analizar los distintos apartados de esta sección y otras fuentes que se indicarán al final de la sección, se puede llegar a la conclusión de que el análisis forense informático recoge de la misma manera la metodología forense per se, siguiendo la siguiente estructura.

Aunque no existe una metodología que sea única y universal en el análisis forense, a tenor de la documentación consultada y tomando en consideración la normativa legal y los estándares vigentes a nivel internacional, sí que se puede decir que existen una serie de fases o puntos importantes que se tienen que tomar en consideración para que el análisis forense sea adecuado y sirva como elemento probatorio ante un incidente.

Todas estas recomendaciones, recogidas en distintas documentaciones (ver bibliografía), establecen una estructura lógica que permiten garantizar el proceso y que, en el ámbito civil, se compone básicamente de las siguientes fases:



Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamenteImagen que contiene Tabla

Descripción generada automáticamenteInterfaz de usuario gráfica, Aplicación

Descripción generada automáticamenteEn cada una de las fases indicadas en la imagen anterior podemos destacar las siguientes tareas.

**PLANTEAMIENTO DEL PROBLEMA.**

El Trabajo de Fin de Máster (TFM) se centra en un caso donde el jefe de una empresa sospecha, sin pruebas, del acceso ilícito a su sistema, requiriendo así una investigación inicial.

Se explora el aspecto legal y la posibilidad de contaminación de pruebas en relación con un presunto delito contemplado en el código penal.

En tales situaciones, las Fuerzas y Cuerpos de Seguridad del Estado, bajo la autorización de un juzgado de instrucción, son los responsables de llevar a cabo el análisis forense del hecho sospechado.

**IDENTIFICACIÓN.**

En el caso del presente TFM, en el enunciado hemos recibido y el material didáctico que se adjunta, se han realizado previa y satisfactoriamente todos los pasos de esta metodología.

Cabe destacar en una de las tareas dedicadas a la identificación, nos encontramos con la tarea de asegurar la escena, es recomendable realizar las siguientes acciones:

1. Tomar fotografías del entorno del equipo para documentar el estado original de la escena y delimitar el área a investigar, evitando el acceso de personal no autorizado.
2. Proteger las huellas dactilares en los equipos, usando guantes de látex o similares, para facilitar la labor de otros cuerpos de policía e investigadores. Se menciona el principio de intercambio de Locard.
3. Registrar la hora y fecha de los equipos implicados, que pueden diferir de la hora real. Es crucial documentar cualquier discrepancia para la investigación y la creación de una línea temporal de los eventos.
4. Observar y grabar cualquier proceso en pantalla que pueda ofrecer información relevante, así como evaluar las entradas y salidas de los equipos y otros periféricos como impresoras, teléfonos IP y escáneres, para obtener pistas adicionales.

**ADQUISICIÓN.**

Antes de recoger evidencias, es importante establecer su orden de prioridad basado en la volatilidad de los datos. Esto implica identificar qué datos son más propensos a cambiar o desaparecer y recolectarlos primero.

Entendemos por volatilidad de los datos el período de tiempo en el que estarán accesibles en el equipo. Por lo tanto, se deberán recolectar previamente aquellas pruebas más volátiles. Según la RFC 3227, el que se presenta a continuación, es un posible orden de volatilidad de mayor a menor:

Tabla

Descripción generada automáticamente con confianza media

Como ya se ha indicado previamente, para procedimientos penales, es necesario que una autoridad legal (como un secretario judicial o un notario) supervise la recogida de evidencias.

La última tarea de esta fase es la recogida de evidencias, la recolección de evidencias implica hacer una copia bit a bit de los discos que se van a analizar. Esta copia debe ser exacta y abarcar todos los archivos del disco, incluyendo archivos temporales, ocultos, de configuración, eliminados, pero no sobrescritos, y la información de las partes del disco no asignadas.

La copia se debe realizar en un soporte limpio, previamente borrado de manera segura para evitar la contaminación con otros casos.

**PRESERVACIÓN.**

Esta acción, se ha realizado al igual que las anteriores, ha sido realizada de manera previa a la elaboración del TFM, para ello se deben tener en cuenta las siguientes consideraciones.

Una vez realizada la copia se debe verificar la integridad de esta. Para ello se calcula el hash o CRC de la copia, normalmente los equipos destinados al clonado de discos ya incorporan esa característica. Así con el hash del disco original y el de la copia se puede certificar que ambos son idénticos a todos los niveles y ante un juez, por ejemplo, quedará probado que no se ha manipulado de ningún modo. Con este procedimiento también nos aseguraremos de que no se han producido errores en la copia.

Con la primera copia realizada y comprobada procedemos a realizar una segunda copia sobre la primera. En este caso también se comprobará que el contenido es idéntico mediante el mismo proceso descrito anteriormente. Teniendo ambas copias entregaremos la primera al secretario judicial o notario responsable del caso y nos quedaremos con la segunda para poder trabajar. La segunda copia será nuestra copia de respaldo en todo momento en el laboratorio y no será para trabajar directamente con ella en ningún caso. Para realizar el análisis se deberá realizar una tercera copia, comprobar su integridad y trabajar sobre ella, de tal modo que en caso de cualquier desastre o alteración de los datos siempre tengamos la segunda copia exacta al original de donde poder volver a realizar otra copia para analizar.

Una mala preservación de las evidencias, un mal uso o una mala manipulación pueden invalidar toda la investigación que se lleva a cabo delante de un tribunal, este es un factor muy importante que se va repitiendo a lo largo de toda la metodología.

La cadena de custodia es el procedimiento controlado aplicable a las evidencias relacionadas con el suceso, desde el momento en que se encuentran en la escena hasta su análisis en el laboratorio. La finalidad de la cadena de custodia es evitar cualquier tipo de manipulación y tener un control absoluto sobre todos los elementos incautados, quién los ha manipulado, cómo lo ha realizado, porqué los ha manipulado, para qué lo ha hecho y cuándo ha tenido lugar dicha manipulación.

Es importante realizar todas las anotaciones descritas en la fase de identificación de las evidencias para que esta fase sea aún más sólida. Con todos los elementos documentados será mucho más fácil tener un control de todas las evidencias que disponemos y poder realizar una traza de todas las pruebas adquiridas.

Además, se tendrá en cuenta de proteger los bienes para el transporte desde el lugar de los hechos hasta el laboratorio con los medios necesarios para evitar golpes o proteger de caídas fortuitas.

La documentación de la cadena de custodia deberá contener también todos los lugares por donde ha pasado la evidencia y quién ha realizado su transporte y su acceso.

En nuestro caso, cabe destacar que, una vez iniciado el análisis de la memoria, esta no debe de modificarse ni contaminarse, en caso de ello el Hash de las evidencias cambiaría, por lo que la evidencia ha quedado contaminada. Hay que hacer estas acciones teniendo presente al secretario judicial, para que esa copia quede registrada si es necesario y que no ha habido más alteraciones al respecto, ese cambio de hash será notificado y adjuntado en el proceso de instrucción, haciéndose también nuevas copias de este nuevo "snapshot" de la prueba.

**ANÁLISIS.**

La fase de análisis, ***en la cual iniciamos la elaboración del presente TFM***, no termina hasta que no se puede determinar qué o quién causó el incidente, cómo lo hizo, qué afectación ha tenido en el sistema, etc. Es decir, es el núcleo duro de la investigación y tiene que concluir con el máximo de información posible para poder elaborar unos informes con todo el suceso bien documentado.

Antes de empezar el análisis, es importante recordar unas premisas básicas que todo investigador debe tener presente en el momento de enfrontarse al incidente. Como ya se ha explicado nunca se debe trabajar con datos originales y se debe respetar cada una de las leyes vigentes en la jurisdicción donde se lleve a cabo la investigación. Los resultados que se obtengan de todo el proceso han de ser verificables y reproducibles, Es importante también disponer de una documentación adicional con información de diversa índole, por ejemplo:

* Sistema operativo del sistema.
* Programas instalados en el equipo.
* Hardware, accesorios y periféricos que forman parte del sistema.
* Datos relativos a la conectividad del equipo:
  + Si dispone de firewall, ya sea físico o lógico.
  + Si el equipo se encuentra en zonas de red especiales, por ejemplo, DMZ.
  + Si tiene conexión a Internet o utiliza proxies.
* Datos generales de configuración que puedan ser de interés para el investigador
* para ayudar en la tarea.

Cabe recordar que no existe ningún proceso estándar. Cada investigación es única y debe ser tratada individualmente. Las diferencias pueden incluir el sistema operativo del equipo (Windows o Linux), el tipo de incidente (como intrusión en correo electrónico o ataque de denegación de servicio), y la naturaleza del malware.

En todo caso, se pueden destacar varios pasos, que habrá que adaptar en cada caso:

* Preparar un entorno de trabajo adaptado a las necesidades del incidente.
* Reconstruir una línea temporal con los hechos sucedidos.
* Determinar qué procedimiento se llevó a cabo por parte del atacante.
* Identificar el autor o autores de los hechos.
* Evaluar el impacto causado y si es posible la recuperación del sistema.

Antes de empezar el análisis propiamente, se debe preparar un entorno para dicho análisis. Es el momento de decidir si se va a hacer un análisis en caliente o en frío.

En caso de un análisis en caliente se hará la investigación sobre los discos originales, lo que conlleva ciertos riesgos. Hay que tomar la precaución de poner el disco en modo sólo lectura, esta opción sólo está disponible en sistemas operativos Linux, pero no en Windows. Si se opta por esta opción hay que operar con sumo cuidado pues cualquier error puede ser fatal y dar al traste con todo el proceso, invalidando las pruebas.

Si se opta por un análisis en frío, lo más sencillo es preparar una máquina virtual (en adelante VM) con el mismo sistema operativo del equipo afectado y montar una imagen del disco. Para ello, previamente habremos creado la imagen a partir de las copias que se hicieron para el análisis. En este caso podremos trabajar con la imagen, ejecutar archivos y realizar otras tareas sin tanto cuidado, pues siempre cabe la opción de volver a montar la imagen desde cero en caso de problemas.

La opción del análisis en frío, ***La cual será el caso que nos atañe el presente TFM, ya que de este modo es como se realizará el análisis***, resulta muy atractiva pues en caso de malwares se podrán ejecutar sin miedo, reproducir lo que ocurre y desmontar la imagen sin que la copia original resulte afectada. De este modo tal vez se pueda ir un poco más allá en la investigación y ser

un poco más agresivo.

Existen varios programas gratuitos para crear y gestionar VM's por ejemplo,

Oracle VM VirtualBox, que ofrecen muy buenas prestaciones.

Para la tarea de construir una cadena de acontecimientos y hacer una línea temporal cabe destacar lo siguiente.

Para crear la línea temporal, lo más sencillo es referirnos a los tiempos MACD de los archivos, es decir, las fechas de modificación, acceso, cambio y borrado, en los casos que aplique. Es importante, como ya se ha indicado en alguna ocasión tener en cuenta los husos horarios y que la fecha y hora del sistema no tienen por qué coincidir con los reales. Este dato es muy importante para poder dar crédito a las pruebas y a la investigación en general.

Para empezar, lo mejor es determinar la fecha de instalación del sistema operativo, para ello se puede buscar en los datos de registro. Además, la mayoría de los ficheros del sistema compartirán esa fecha. A partir de aquí puede ser interesante ver qué usuarios se crearon al principio, para ver si hay discrepancias o usuarios fuera de lo común en últimos instantes del equipo. Para ver esta información también es útil acudir al registro del sistema operativo.

Teniendo ya los datos iniciales del sistema, ahora se puede buscar más información en los ficheros que se ven "a simple vista". Lo importante es localizar que programas fueron los últimos en ser instalados y qué cambios repercutieron en el sistema. Lo más habitual es que estos programas no se instalen en los lugares habituales, sino que se localicen en rutas poco habituales, por ejemplo, en archivos temporales o mezclados con los archivos y librerías del sistema operativo. Aquí se puede ir creando la línea temporal con esos datos.

Alternativamente es útil pensar que no todos los archivos están a la vista. Se puede encontrar información en archivos normales, pero también en temporales, ocultos, borrados o usando técnicas como la esteganografía, no se puede obviar ninguna posibilidad.

Habitualmente los sistemas operativos ofrecen la opción de visualizar los archivos ocultos y también las extensiones. Es útil activar estas opciones para detectar posibles elementos ocultos y extensiones poco habituales que nos resulten extrañas.

Para los archivos borrados se utilizarán programas especiales capaces de recuperar aquellos datos que se hayan eliminado del disco, pero sobre los cuales aún no se haya sobrescrito nada. Es posible que el atacante elimine archivos o registros varios en afán de esconder lo que ha ocurrido, si estos no han sido sobrescritos se podrán recuperar y se podrán situar en la línea temporal relacionándolos con el conjunto de sucesos. Para recuperar información oculta mediante esteganografía también se deberán usar programas concretos. Es posible que el atacante ocultara información sobre otros archivos, tales como imágenes o audio para enviarlos posteriormente o tenerlos almacenados sin llamar la atención. Habitualmente hallaremos más información en ubicaciones ocultas que en los lugares más habituales.

Con todos estos datos se debería poder crear un esbozo de los puntos clave en el tiempo tales como la instalación del sistema, el borrado de determinados archivos, la instalación de los últimos programas, etcétera.

El siguiente paso del análisis es determinar el ***cómo se actuó***. Para determinar cómo se actuó es importante llevar a cabo una investigación sobre la memoria del equipo. Es interesante realizar un volcado de memoria para la obtención de cierta información. Con programas destinados a tal fin podremos ver que procesos se están ejecutando en el momento concreto y también aquellos que hayan sido ocultados para no levantar sospechas. Con esta información podremos saber qué ejecutables inician los procesos en ejecución y qué librerías se ven involucradas. Llegados aquí se puede realizar volcados de los ejecutables y de dichas librerías para poder analizar si contienen cadenas sospechosas o si, por lo contrario, son archivos legítimos. Sabiendo los procesos que se ejecutan y su naturaleza podemos obtener pistas de cómo se actuó para comprometer el equipo.

A menudo nos deberemos fijar en procesos en ejecución aparentemente inofensivos, habituales y legítimos en los sistemas operativos. No es extraño que determinados procesos con fines malintencionados se camuflen con procesos legítimos. Para ello deberemos observar que muchas veces estos se encuentran sin un proceso padre, cuando lo más habitual es que dependan de otros. En otras ocasiones simplemente se camuflan con nombres muy parecidos a otros para pasar desapercibidos.

Ciertos programas también nos darán información sobre las cadenas del ejecutable en cuestión. Con ellas podremos ver si mutan su contenido cuando se ejecutan en memoria y cuál es su contenido. En ocasiones, cierta información de las cadenas nos puede dar pistas muy valiosas, como, por ejemplo, cadenas dónde encontrar logs, o enlaces a direcciones de Internet. También nos puede dar pistas sobre el tipo de malware al que nos enfrentamos. Si por ejemplo encontramos cadenas con alfabetos o teclas concretas del teclado, es probable que nos encontremos ante un keylogger.

Finalmente, otra práctica interesante para determinar cómo se actuó es leer la secuencia de comandos escrita por consola. Para ello procederemos con el volcado de memoria y podremos obtener dicha información. De este modo podremos leer que comandos se hicieron por consola y sabremos si se ejecutó algún proceso de este modo. Debemos excluir nuestras propias instrucciones pues seguramente aparecerán los comandos del volcado de memoria que se hicieron en su momento. Relativo a esta práctica, personalmente es la primera que se debería de realizar en un análisis forense, de ahí también poder corroborar que es lo que pueda decir el usuario en una posible entrevista, que en este caso no va a ser posible.

Para la tarea de identificación de autores, cabe destacar que, para poder realizar una identificación del autor o autores del incidente, otra información importante que nos puede dar el volcado de memoria son las conexiones de red abiertas y las que están preparadas para enviar o recibir datos. Con esto podremos relacionar el posible origen del ataque buscando datos como la dirección IP en Internet.

Hay que actuar con prudencia puesto que en ocasiones se utilizan técnicas para distribuir los ataques o falsear la dirección IP. Hay que ser crítico con la información que se obtiene y contrastarla correctamente. No siempre se obtendrá la respuesta al primer intento y posiblemente en ocasiones sea muy difícil averiguar el origen de un incidente.

Es interesante recapacitar en los distintos perfiles de atacantes que se pueden dar hoy día en este ámbito para intentar mimetizarse y entender quién pudo ser el autor.

Por un lado, podemos encontrar organizaciones y criminales que actúan por motivaciones económicas. Su finalidad es robar cierta información, ya sea empresarial o personal, para una vez obtenida venderla o sacar un rendimiento oneroso de la información.

Por otro lado, está quién sólo busca acceder a sistemas por mero prestigio y reconocimiento en su ambiente cibernético. Accediendo a sistemas mal configurados y publicando datos que prueben su fechoría incrementará su notoriedad y se dará a conocer más en las redes.

En este punto es importante analizar dos vertientes. En caso de que se esté realizando un peritaje con fines inculpatorios, o sea, judiciales, se deberá intentar resolver quién es el autor o al menos aportar pistas fiables para que otros investigadores puedan llevar a cabo otras investigaciones de otros ámbitos.

En cambio, si es con fines correctivos lo más interesante seguramente será obviar esta fase y proceder con el estudio del impacto causado y estudiar las mejoras que se pueden implantar para evitar episodios similares.

Para establecer el impacto causado, cabe destacar que se puede calcular en base a distintos factores y no hay un método único para su cálculo, ni una fórmula que nos dé un importe económico. Aun así, para estos cálculos puede servir ayudarse de métodos como BIA (Business Impact Analysis) que determinan el impacto de ciertos eventos ayudando a valorar los daños económicamente.

A la larga cualquier incidente ocurrido devengará en unos gastos económicos que habrá que cuantificar en función de los ítems afectados tras el suceso. En ocasiones el coste económico resultará de tener que reemplazar una máquina o dispositivo que ha quedado inservible tras un ataque o bien las horas de empleado de tener que reinstalar el sistema. En este caso, el cálculo no supone mayor dificultad y se resuelve fácilmente.

En otras ocasiones, por ejemplo, los daños pueden deberse al robo de una información de secreto industrial en el que habrá que cuantificar no sólo qué supone reponer el sistema sino, a la larga, en qué se verá afectada la empresa. Los datos robados pueden ser para publicar cierta información sobre la empresa y poner en la opinión pública datos con intenciones de crear mala imagen, lo cual supone un daño incalculable y muy elevado para la empresa.

El impacto no sólo se puede calcular en base económica. Como ya se ha comentado al inicio de esta sección también existen otros factores, es el caso del tiempo de inactividad. Si el incidente ha supuesto paralizar la producción de una planta automatizada de fabricación esto supone muchas horas en que la producción es nula, por lo tanto, no se trabajará. Evidentemente, a la larga también supondrá un problema económico pues no se podrán servir los pedidos pendientes de los clientes. Si la paralización afecta a una oficina, tal vez no se pare la producción de bienes, pero sí el trabajo de los empleados que verán retrasado todo su trabajo.

**PRESENTACIÓN.**

La última fase de un análisis forense queda para redactar los informes que documenten los antecedentes del evento, todo el trabajo realizado, el método seguido y las conclusiones e impacto que se ha derivado de todo el incidente.

Para ello se redactarán dos informes, a saber, el informe técnico y el ejecutivo. En esencia en ambos informes se explican los mismos hechos, pero varía su enfoque y el grado de detalle con que se expone el asunto.

- En el informe ejecutivo se usará un lenguaje claro y sin tecnicismos, se debe evitar usar terminología propia de la ciencia e ingeniería y expresiones confusas para gente no ducha en el tema. Hay que pensar que el público lector de estos informes serán jueces y gerentes que seguramente estén poco relacionados con el tema y además tengan poco tiempo para dedicarle. Se les debe facilitar la tarea al máximo.

En el informe técnico, por el contrario, el público final será técnico y con conocimientos de la materia que se expone. Aquí se detallarán todos los procesos, los programas utilizados, las técnicas, etcétera. Debemos crear un documento que pueda servir de guía para repetir todo el proceso que se ha realizado en caso necesario.

Relativo al informe ejecutivo, cabe destacar que será un resumen de toda la tarea que se ha llevado a cabo con las evidencias digitales. Aunque será un documento de poca extensión, al menos comparado con el informe técnico, éste debería contener al menos los siguientes apartados:

1. Motivos de la intrusión.
   1. ¿Por qué se ha producido el incidente?
   2. ¿Qué finalidad tenía el atacante?
2. Desarrollo de la intrusión.
   1. ¿Cómo lo ha logrado?
   2. ¿Qué ha realizado en los sistemas?
3. Resultados del análisis.
   1. ¿Qué ha pasado?
   2. ¿Qué daños se han producido o se prevén que se producirán?
   3. ¿Es denunciable?
   4. ¿Quién es el autor o autores?
4. Recomendaciones.
   1. ¿Qué pasos dar a continuación?
   2. ¿Cómo protegerse para no repetir los hechos?

El informe técnico será más largo que el anterior y contendrá mucho más detalle. Se hará una exposición muy detallada de todo el análisis con profundidad en la tecnología usada y los hallazgos. En este caso se deberá redactar, al menos:

1. Antecedentes del incidente.
   1. Puesta en situación de cómo se encontraba la situación con anterioridad al incidente.
2. Recolección de datos.
   1. ¿Cómo se ha llevado a cabo el proceso?
   2. ¿Qué se ha recolectado?
3. Descripción de la evidencia.
   1. Detalles técnicos de las evidencias recolectadas, su estado, su contenido,
4. Entorno de trabajo del análisis.
   1. ¿Qué herramientas se han usado?
   2. ¿Cómo se han usado?
5. Análisis de las evidencias.
   1. Se deberá informar del sistema analizado aportando datos como las características del sistema operativo, las aplicaciones instaladas en el equipo y los servicios en ejecución.
6. Descripción de los resultados.
   1. ¿Qué herramientas ha usado el atacante?
   2. ¿Qué alcance ha tenido el incidente?
   3. Determinar el origen de este y como se ha encontrado.
7. Dar la línea temporal de los hechos ocurridos con todo detalle.
8. Redactar unas conclusiones con las valoraciones que se crean oportunas a la vista de todo el análisis realizado.
9. Dar unas recomendaciones sobre cómo proteger los equipos para no repetir el incidente o sobre cómo actuar legalmente contra el autor.

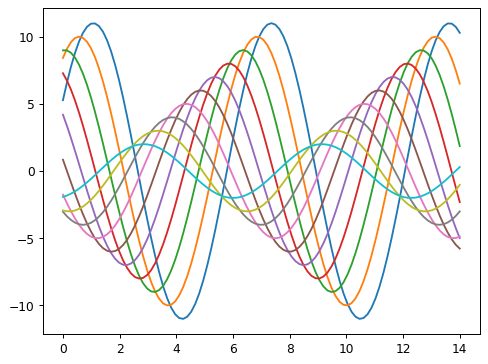


Figura 1: Este es un ejemplo de figura.

## Objetivos

## Descripción del entorno de trabajo

## Listado de tareas

## Planificación temporal de las tareas

## Revisión del estado del arte de la informática forense

# Extremos del análisis y previsión de pruebas técnicas



## Propuesta de extremos

## Previsión de pruebas técnicas

# Análisis de la memoria RAM

# Análisis del disco duro

# Resumen ejecutivo

# Informe pericial

# Conclusiones

# Referencias bibliográficas

# Anexos