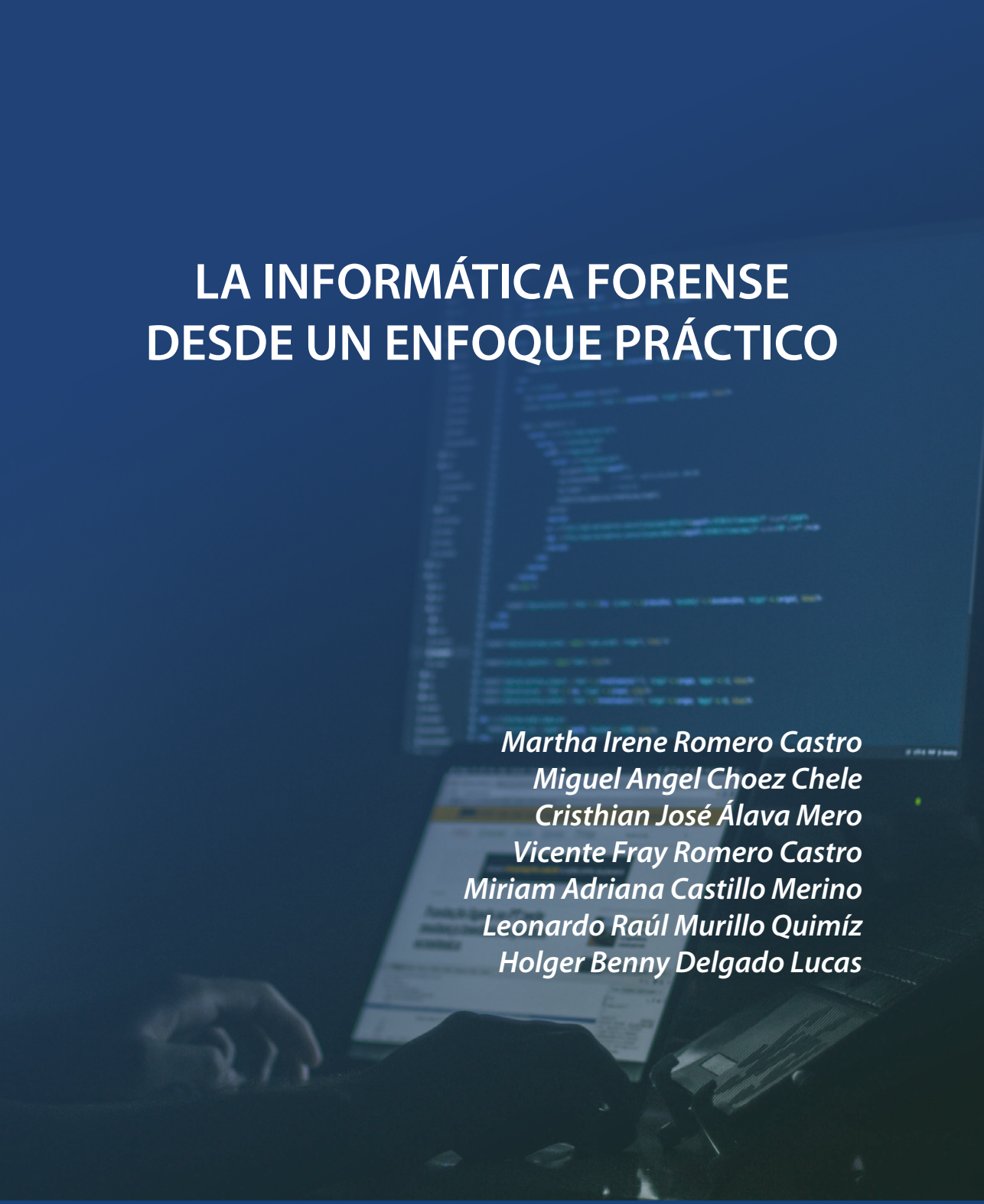
LA INFORMÁTICA FORENSE DESDE UN ENFOQUE PRÁCTICO



Martha Irene Romero Castro
Miguel Angel Choez Chele
Cristhian José Álava Mero
Vicente Fray Romero Castro
Miriam Adriana Castillo Merino
Leonardo Raúl Murillo Quimíz
Holger Benny Delgado Lucas

Ingeniería y Tecnología

3ciencias

LA INFORMÁTICA FORENSE DESDE UN ENFOQUE PRÁCTICO

Martha Irene Romero Castro
Miguel Angel Choez Chele
Cristhian José Álava Mero
Vicente Fray Romero Castro
Miriam Adriana Castillo Merino
Leonardo Raúl Murillo Quimíz
Holger Benny Delgado Lucas

Editorial Área de Innovación y Desarrollo,S.L.

ÁREA DE INNOVACIÓN Y DESARROLLO, S.L.

C/Alzamora, 17- 03802- ALCOY (ALICANTE) info@3ciencias.com

Primera edición: **septiembre 2020**

ISBN: **978-84-122093-0-3**

DOI: **https://doi.org/10.17993/IngyTec.2020.63**

AUTORES

Martha Irene Romero Castro, Magister en Informática Empresarial, Magister en Docencia Universitaria e Investigación Educativa, Especialista en Redes de Comunicación de Datos, Ingeniera en Sistemas, Coordinadora de la Carrera de Ingeniería en Computación y Redes, Docente Titular Principal de la Universidad Estatal del Sur de Manabí.

Miguel Ángel Choez Chele, Licenciado en Análisis de Sistemas por la Universidad Laica Eloy Alfaro de Manabí, Magister en Docencia e Investigación Educativa por la Universidad Técnica de Manabí, Experto en Gestión Organizacional y Liderazgo por la Universidad de Cuenca. Investiga temas relacionados Tecnología de la Información y Comunicación Aplicado en el Ámbito Educativo, Plataformas Educativas E – Learning, Ex Docente de la Universidad Estatal del Sur de Manabí, Actualmente Docente Titular de la Unidad Educativa Eleodoro González Cañarte.

Cristhian José Álava Mero, Ingeniero en Sistemas Informáticos por la Universidad Técnica de Manabí, Magister en Informática Empresarial, Especialista en Redes de Comunicación de Datos, Diploma Superior en Sistemas de Información Empresarial por la Universidad Regional Autónoma de los Andes, Docente de la Carrera de Tecnologías de la Información de la Universidad Estatal del Sur de Manabí. Ecuador.

Vicente Fray Romero Castro, Ingeniero en Sistemas por la Universidad Laica Eloy Alfaro de Manabí, Magister en Sistemas de Información Gerencial por la Escuela Superior Politécnica del Litoral. Investiga temas relacionados a Tecnologías de Desarrollo de Software, Inteligencia de Negocios y metodologías Orientadas a Objetos. Actualmente Docente en la Universidad Estatal del Sur de Manabí.

Miariam Adriana Castillo Merino, Magister en Gerencia Educativa, Ingeniera en Computación y Redes, Docente contratado Carrera Ingeniería Forestal, Tecnología de la Información, Unidad de Nivelación y Admisión, Universidad Estatal del Sur de Manabí, Ecuador.

Leonardo Raúl Murillo Quimiz, Ingeniero en Computación y Redes por la Universidad Estatal del Sur de Manabí, Magister en Educación Informática por la Universidad de Guayaquil. Investiga temas relacionados con redes y telecomunicaciones. Actualmente profesor y coordinador del área de seguimiento a graduados de la Universidad Estatal del Sur de Manabí. Ecuador.

Holger Benny Delgado Lucas, Ingeniero en Sistemas por la Universidad Laica Eloy Alfaro de Manabí, Magister en Docencia Universitaria, por la Universidad Nacional de Loja, Magister en Tecnologías de la Información y Comunicación, por la Universidad Nacional de Piura—Perú, Docente titular principal, Carrera de Ingeniería en Sistemas Computacionales y Tecnologías de la Información, Decano de la Facultad de Ciencias Técnicas en la Universidad Estatal del Sur de Manabí.

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

PRÓLOGO

En los actuales momentos, en la actividad cotidiana y empresarial se cometen muchos delitos desde robos, hasta estafas masivas, en algunos casos con el uso de equipos tecnológicos. Este libro tiene como objetivo principal analizar las diferentes técnicas y métodos para detectar los diferentes delitos informáticos a través de las ciencias forenses basadas en la informática.

El contenido de esta investigación está dirigido a profesionales en informática, de la seguridad, estudiantes y docentes que están inmersos en el mundo de la informática.

El contenido del libro en sus diferentes apartados brinda conocimientos sobre las ciencias forenses, cómo se debe preparar una investigación en informática forense, cómo se debe proceder cuando se presenta un ciberincidente, la forma de conservar y guardar las evidencias recolectadas y las diferentes técnicas para que estas conserven la integridad y no comprometan el resultado de la investigación.

También, se analiza en detalle cómo realizar la investigación forense en unos de los sistemas operativos con más usuarios actualmente como lo es el sistema Windows, se conocerá la estructura básica de los directorios más importantes o especiales para que los peritos sepan donde buscar la información más crítica, se conocerá la forma de recuperar datos del registro de Windows, del registro de eventos, de los diferentes navegadores web y por último, recuperar datos de los diferentes dispositivos móviles presentes en el mercado.

CAPÍTULO I: ENTENDER A LA INFORMÁTICA FORENSE

Este capítulo tiene como objetivo conocer cuáles son los objetivos de la informática forense, los tipos de investigación que se pueden realizar, las buenas prácticas que se deben establecer, conocer cuáles serían las implicaciones legales que conlleva a realizar un peritaje informático mal hecho y estar al tanto de los diferentes estándares de investigación forense.

1.1. Objetivos de la informática forense

El objetivo principal de la informática forense es generar evidencias legales para procedimientos judiciales, las evidencias desde el punto de vista que ocupa, son el conjunto de recursos y datos a los que ha tenido acceso un perito para extraerlos, analizarlos, verificar su autenticidad y poder así responder a las cuestiones técnicas planteadas por la parte que le contrate o por un tribunal. Según Estrada (2010) la informática forense permite dar solución a problemas relacionados con la seguridad de la información, con el objetivo de salvaguardar la información digital, en el caso de haber ocurrido un delito, utilizando como medio a el computador o algún equipo digital.

Fases de peritaje

El proceso general de peritaje consta de al menos tres etapas que se las detallan a continuación:

- Adquisición.
- Análisis.
- Presentación.

Aunque, pueden ser extendidas agrupando las actividades en cinco etapas que se detallan a continuación:

Preparación.- La primera es prepararse para una investigación, que empieza incluso antes de ser contratados o de que ocurra un incidente, ya que la preparación incluye formación, mantenimiento de equipos, recursos, reciclaje, además de preparación específica en función del incidente a atender.

Adquisición.- La segunda fase es la de adquisición de datos, que se realizan bien en la escena del incidente, en el laboratorio, si es allí donde llevan los equipos afectados o involucrados en un incidente.

Análisis.- El análisis de datos es el siguiente paso, consiste en indexar, dar forma y comprender la información pertinente para la investigación de entre todo el conjunto de datos adquiridos en la fase previa.

Identificación de evidencias.- La identificación de evidencias, es la cuarta etapa y consiste en señalar de todo lo adquirido y analizado, que es lo relevante para el caso en el que se trabaja, lo que, en caso de declaración ante un tribunal, se tendría que explicar y defender.

Informe de conclusiones.- Por último, está la generación del informe de conclusiones o informe pericial, en el que se detallan todas las actividades del proceso de investigación y las conclusiones obtenidas respecto a la información disponible y a las preguntas que el contratista formulase.

El trabajo forense o peritaje, tiene que ser de carácter científico, no subjetivo, el perito debe responder a preguntas de tipo técnico planteadas por su contratista, sea una parte involucrada en un incidente o por un tribunal.

El perito no debe valorar, por ejemplo, si la acción de una persona es constitutiva de delito, sino, localizar o verificar las evidencias que permitan a los juristas comprender los aspectos de la tecnología que escapan a su conocimiento y así poder tomar esa decisión de forma razonada.

Al fin y al cabo, la ciencia forense es la aplicación de conocimientos, métodos y técnicas de investigación científica que buscan determinar la veracidad de unos hechos, su origen y su autoría. En informática forense una gran parte del trabajo consiste en verificar la veracidad de la información, ya que las evidencias digitales son fácilmente modificables, incluso pueden ser evidencias totalmente inventadas, confirmada la veracidad objetiva de una evidencia, el trabajo consiste en el cómo y cuándo es posible en el quién y cuándo se habla de quién, se puede referir no sólo a personas, quizá sea a equipos, a cuentas de servicios online, etc., que otros profesionales deberán vincular con una persona física.

1.2. Tipos de investigación de un perito informático

Hay veces en que el trabajo del perito puede parecer una cosa muy simple, pero todos los trabajos son necesarios y todo implica una responsabilidad y una necesidad de hacer bien las tareas.

Dentro de este contexto, este tipo de trabajos va a cubrir tres objetivos que se detallan a continuación:

- Definir el arbitraje.
- Enumerar los tipos de arbitraje.
- Subrayar cuando un perito informático debe aceptar o rechazar su intervención en una actuación judicial.

Se considera a la informática forense como una ciencia que no solo es utilizada para analizar e investigar crímenes tecnológicos, sino también, investiga crímenes en donde se use una computadora que pueda tener alguna evidencia registrada.

Investigaciones privadas

Cuando los peritos informáticos realizan trabajos de tipos privados, aunque no involucren procesos judiciales, deben ajustarse a la legislación vigente y respetar especialmente las leyes referentes a los derechos de las personas, además, deberán respetarse las políticas de la propia empresa que contrate los servicios del perito.

Se trata de investigaciones que no tienen por qué tener finalidad jurídica, pueden tratarse de investigaciones internas de una empresa, respuesta a incidentes, evaluaciones de seguridad y más. Cuando se practican este tipo de servicios hay que tener en cuenta que los solicitantes suelen ser empresas privadas, no se debe bloquear la continuidad del negocio, durante un ataque prima la seguridad y continuidad de la empresa sobre la evidencia legal.

Se trabaja para entidades privadas que quieren obtener información que puede o no llegar a instancias judiciales, es decir, que puede quedar todo en una investigación interna sin pasar a más, llegar a un arbitraje o llegar a una demanda, generalmente de tipo civil, algunos casos con los que puede estar más relacionado el servicio de peritaje privado son:

- Incidentes.
- Sabotaje.
- Espionaje industrial.
- Malversación de recursos de la empresa.
- Disputas laborales y muchos otros.

De privado a público

A veces las investigaciones privadas pueden derivar en procedimientos judiciales, la investigación de, por ejemplo, la actividad de un empleado debe desempeñarse de acuerdo a la legislación laboral y a los derechos de privacidad intrínsecos al trabajador, no sólo, de acuerdo a las políticas de la empresa. El descubrimiento durante una investigación privada de la comisión de un delito, debe derivar automáticamente en la pertinente denuncia ante las autoridades, por ejemplo, si se está investigando una posible fuga de información de una empresa y se encuentra contenido inapropiado por ilegal en un equipo, debe denunciarse ante la policía o un juzgado, así se puede decir que si se trata todos los casos como si fueran a acabar en un tribunal, se podrá garantizar la calidad del trabajo sea cual sea la deriva que tome el caso.

1.3. Buenas prácticas en informática forense

Para aplicar un análisis forense, se lo debe realizar practicando el mismo patrón como si se realizase un experimento de laboratorio en la medicina actual. Cuando se tiene que trabajar con evidencias y verificar que estas no hayan sido comprometidas física o lógicamente, se debe establecer una serie de cuidados y establecer lo que se conoce como cadena de custodia.

Estos mecanismos van a permitir conservar las garantías de confiabilidad de una evidencia, ya que si una evidencia no presenta las seguridades necesarias y sufre cambios del estado original como se la recogió, pondrá en duda las futuras conclusiones que se extraigan de dicha evidencia y así no tendrán la validez suficiente cuando vayan a ser incluidas como parte de un proceso judicial.

La cadena de custodia de una evidencia debe estar formada por varias etapas, bien descritas y con una excelente documentación desde el origen hasta el punto de llegada de dicha evidencia, las cuales se las puede detallar a continuación:

- La identificación, extracción y registro de la evidencia. – La evidencia debe ser bien identificada, indiferente del lugar de donde venga, sea un equipo informático llevado a un laboratorio, una escena de un delito, etc.
- La preservación y almacenamiento de la evidencia. – Se deben aplicar medidas de preservación de una determinada evidencia, garantizando la seguridad y el correcto almacenamiento de la misma.
- Los traslados a los que se vea sometida a la prueba, indicando tiempos, origen y destino para cada desplazamiento, así como, los posibles incidentes que puedan darse durante los mismos.

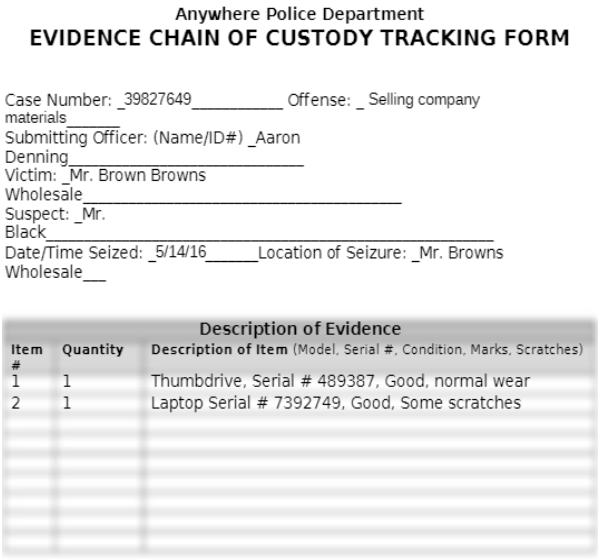
1.3.1. Cadena de custodia

Los traspasos de posesión, qué son los cambios en la titularidad de la responsabilidad de la conservación de una evidencia, por ejemplo, si se entrega una evidencia a un compañero para que haga copias , la almacene o la traslade, dichos traspasos tienen que registrar cuando y donde tuvieron lugar, quién entregaba la evidencia y quién la recibida y el receptor deberá encargarse a partir de ese momento, tanto de la evidencia, como de su cadena de custodia y como no podía ser de otra forma las medidas de custodia y preservación de la evidencia que se apliquen también deben documentarse en la cadena de custodia, al fin y al cabo, la cadena de custodia es un registro cronológico de actividades, incidentes y responsabilidades respecto de cada evidencia.

Cada entrada en el registro, debe indicar quién tiene la evidencia, quién se la entregó cuando se la entregó, cómo y dónde se almacenó y que se hizo con ella, además, puede ser positivo, cuando se trate de evidencias físicas, adjuntar fotografías o incluso videos de los procesos en los que esta información multimedia puede aportar valor, como por ejemplo, durante la adquisición para mostrar el estado de las evidencias y durante los procesos a los que la sometan para demostrar que no varía su estado.

Según Domínguez (2013), una vez asegurada la cadena de custodia, aquí, empieza el trabajo verdadero del perito forense, si la información que se custodia es un disco duro, como regla principal se recomienda nunca trabajar sobre los soportes originales.

Se puede crear un formulario de cadena de custodia, y es que dependiendo de la legislación del país en el que se actúe, o si es un investigador independientes o agentes de las fuerzas de seguridad, es posible que se deba emplear formularios de cadena de custodia con formatos específicos como el que se muestra en la Figura 1.



Anywhere Police Department

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: _39827649_____ Offense: _ Selling company materials_____
Submitting Officer: (Name/ID#) _Aaron Denning_____
Victim: _Mr. Brown Browns Wholesale_____
Suspect: _Mr. Black_____
Date/Time Seized: _5/14/16_____Location of Seizure: _Mr. Browns Wholesale___

Description of Evidence		
Item #	**Quantity**	**Description of Item** (Model, Serial #, Condition, Marks, Scratches)
1	1	Thumbdrive, Serial # 489387, Good, normal wear
2	1	Laptop Serial # 7392749, Good, Some scratches

Figura 1. Ejemplo de formulario de cadena de custodia.
Fuente: recuperado de Course Hero (s.f.) (https://www.coursehero.com/).

Otro ejemplo, es otro formulario empleado por los cuerpos de seguridad de Guanajuato en México y aparte de explicar en qué consiste la cadena de custodia en toda la parte anterior, plantea la plantilla sobre la que se desarrolla esa cadena de custodia.

Se puede crear propios formularios, inspirándose en los que sean legalmente aceptados en el país o estado que se realiza la auditoria, es recomendable y en algunos casos imprescindible, contar con la presencia de un fedatario público que levante acta notarial de las actividades que se practica, sobre todo en cuanto a la adquisición y manipulación inicial de las evidencias, en España, por ejemplo, son fedatarios públicos los notarios y los secretarios judiciales, son las dos profesiones que pueden emitir un documento legal denominado acta, en el que describen todo aquello de lo que son testigos, desde el apagado de un equipo, hasta la ejecución de un comando concreto para generar la imagen de un disco duro y el hash de dicha imagen.

Algo fundamental entre las buenas prácticas en cualquier actividad, es la planificación, es más fácil defender los resultados de un peritaje forense si está perfectamente documentado y se ajusta a una planificación preestablecida que se debe seguir siempre paso a paso, los pasos fundamentales serán la recolección y análisis.

Plan de adquisición

Antes de practicar una adquisición de evidencias, se debe tener un plan tecnológico preestablecido, establecer un método de recolección sistemático y durante el proceso se debe documentar en el acto cada evidencia e iniciar su correspondiente cadena de custodia.

Plan de análisis

Durante la fase de análisis de las evidencias, se debe especificar la tecnología y recursos que se emplean, describir el entorno de trabajo, anotar los procedimientos que se van siguiendo, cuando empiezan y cuánto dura y adjuntar información sobre cualquier colaboración a la que se recurra para resolver la investigación.

1.4. Implicaciones legales de un peritaje mal hecho

El trabajo de un perito es el de asesoramiento técnico en su materia de especialidad, en el tema que ocupa la informática y la información digital en prácticamente todos sus formatos. Cuando un trabajo de investigación es impecable, la persona que investiga es lo único que puede ser atacado, por lo que la reputación es muy importante.

Una buena reputación evita que un trabajo bien hecho pueda ser desprestigiado mediante falacias, la buena reputación cuesta mucho ganarla, con estudio, con certificaciones, con títulos, con cada trabajo, con cada informe y cada cliente satisfecho, pero basta practicar un mal peritaje para perderla.

Si el trabajo no es hablando desde el punto de vista forense, intachable la evidencia aportada puede ser desestimada, lo cual perjudica siempre a una de las partes y además al perito el cual pierde reputación y puede tener que asumir responsabilidades legales.

Adquisición de evidencias

La adquisición de evidencias debe ser siempre de acuerdo a la ley, en investigaciones privadas deben respetarse todas las garantías y derechos de los ciudadanos y de cualesquiera otras condiciones adicionales que estos tengan, como por ejemplo, ser un empleado, un menor, etc., igual que en investigaciones judiciales, por ejemplo, no se puede investigar una computadora o smartphone si no es el propietario quién hace entrega de la misma o sería una violación de la intimidad y del secreto de las comunicaciones.

En investigaciones judiciales no se debe tomar o acceder a nada que no sea proporcionado por las autoridades o adquirido en base a mandamientos judiciales, siempre según la legislación vigente en cada momento y lugar, es decir, se trabaja con lo que aporta el tribunal que es lo que éste ha considerado que debe ser evaluado.

Método científico

Para que una evidencia sea aceptable tanto en casos públicos como privados, esta debe ser reproducible, es decir, otro perito tiene que poder llegar a las mismas conclusiones partiendo de la misma evidencia. La trazabilidad de las evidencias o la cadena de custodia es una herramienta documental que garantiza la conservación de la evidencia, para esto, es importante establecer protocolos sistemáticos de actuación y calcular los hashes de las evidencias digitales, ya que, permiten comprobar que no han sido alteradas.

Por último, es aconsejable que los peritos ya sea por pertenencia a una asociación profesional o por contratación propia, estén respaldados por un seguro de responsabilidad civil que les cubra en el ejercicio de su profesión y si en algún momento el perito duda sobre la legalidad de cualquier actividad, que por iniciativa propia o del cliente fuese a ejecutar, mejor consultar antes con un asesor legal.

1.5. Estándares de investigación forense

Como cualquier otra ciencia, la investigación forense posee estándares establecidos para ejecutar los procesos técnicos que se presenten, estos procesos pueden ser descritos de la siguiente manera:

- Fase de adquisición de las evidencias.
- Fase de autenticación de las evidencias.
- Fase de análisis de las evidencias.

También existen instituciones que tienen establecidas sus reglas y estándares para aplicar una investigación de este tipo como es el caso del departamento de defensa de los Estados Unidos como se describe a continuación:

- Fase para estandarizar formatos de los datos forenses
- Se debe incluir interfaces técnicas
- Se deben aplicar metodologías de conformidad, la cual tiene especial interés en la interoperabilidad con otros organismos.

Digital Forensic Process

El proceso forense digital, establece otra forma de trabajo distinta, la cual divide al proceso del trabajo forense en siete fases, en lugar de las tres antes descrita, además de adquisición, autenticación y análisis, antes se ejecuta identificación, preservación y estrategia de aproximación y después de los tres originales la presentación. Según Astudillo y Morales (2018) Digital Forensic es considerada una plataforma de código abierto dedicada al análisis forense digital y que, al estar bajo código libre, está bajo licencia GPL.

IDIP

El proceso integrado de investigación digital o IDIP por sus siglas en inglés, está basado en investigación de escenas de crimen físicas o los llamados crímenes tradicionales, aquí, se considera a la computadora como una escena del crimen en sí misma y por tanto aplica metodología del mundo físico a la digital en las siguientes etapas:

- Preparación.
- Despliegue.
- Investigación de la escena física.
- Investigación de la escena digital.
- Presentación de las conclusiones.

Otros estándares

Existen otra serie de estándares de aplicación nacional e internacional que pueden ser interesantes, sobre todo porque son estándares de reconocimiento oficial e inspiración para otros marcos de trabajo, aunque hay bastantes más relacionados con este tema, se puede mencionar sólo un par de los que se publican en España:

Primero, se deben evaluar criterios para poder elaborar dictámenes e informes periciales sobre tecnologías de la información y comunicación, que es la norma "**UNE 197010:2015**", luego se tiene la "**UNE 71505:2013**", que se divide en vocabulario y principios generales, buenas prácticas en la gestión de las evidencias electrónicas y formatos y mecanismos técnicos, luego se tiene también la "**UNE 71506:2013**", sobre procesos de análisis forense dentro del ciclo de gestión de evidencias informáticas.

A nivel internacional se puede mencionar, por ejemplo, las guías para identificación, recolección, adquisición y preservación de evidencias digitales en la "**ISO/IEC 27037:2012**" o las guías para el análisis e interpretación de evidencias digitales en la "**ISO/IEC 27042:2015**".

CAPÍTULO II: PREPARACIÓN DE LA INVESTIGACIÓN FORENSE

Este capítulo tiene como objetivo preparar al perito informático para una investigación forense, desde el conocimiento del tipo de hardware y software a utilizar para establecer un análisis, conocer técnicas como el particionado de discos, saber cómo está representada la información y saber cómo analizarla, como es el caso del formato hexadecimal, y conocer en detalles términos como el offset.

2.1. Tipos de hardware para informática forense

Al momento de planificar la adquisición de un determinado hardware para realizar algún trabajo de informática forense, no hay que enforcarse solamente en la seguridad, sino, hay que pensar también en la eficiencia, ya que el proceso puede consumir mucho tiempo y se debe considerar la utilización de un hardware potente para algún tipo de peritaje informático.

Los recursos como la memoria RAM, debe ser considerado importante cuando se considere trabajar con archivos considerados grandes cuando se tengan que cargar en la memoria, los recursos de almacenamiento también deben ser analizados, ya que la velocidad de lectura y escritura en los discos es muy importante para agilizar el trabajo, se recomienda la utilización de discos SSD o de estado sólido para almacenar la información.

Compatibilidad

Revisar la compatibilidad, es otro componente importante que tiene que cumplir el sistema informático, se tienen que ser capaces de operar con distintos sistemas operativos, ya sea para practicar o para trabajar con las evidencias que lleguen o se adquieran o porque la mayor parte del software forense está desarrollado para ejecutarse en plataformas Linux o Windows y además está la conectividad, es decir, la capacidad para poder conectar a la computadora de análisis cualquier dispositivo, disco, terminal, adaptador o lo que corresponda para poder desempeñar el trabajo, ya que nunca se sabe que se puede encontrar en el camino.

Capacidad

La capacidad de una computadora es otro aspecto fundamental y se habla básicamente de tres facetas que se detallan a continuación:

- General, se componen de:
    - La memoria

    - Las bahías y puertos para ampliar y conectar otros elementos al sistema.
    - Espacio de disco para poder trabajar con evidencias de gran tamaño.

- Almacenamiento externo: en ocasiones la capacidad de almacenamiento limitada de un equipo se debe compensar con equipos en red, tipo NAS que den gran capacidad de almacenamiento y gracias a la configuración RAID apropiada, redundancia local contra fallos en los discos.

- Copias de seguridad: se debe tener siempre un sistema de backup redundante con copias locales y deslocalizadas.

Localización

Respecto al lugar de trabajo hay que considerar dos posibilidades, que se trabaje en un laboratorio propio o fuera de él. Cuando se trabaje en movilidad, por ejemplo, cuando se tenga que ir a la localización del incidente a realizar la adquisición de evidencias, se debe dar prioridad a la portabilidad de los equipos y ponerla en una balanza con la potencia de los mismos, además, se debe incluir las herramientas y adaptadores básicos para cualquier tipo de contingencia que se presente. Cuando se prepara material para el laboratorio, el tamaño, consumo o peso serán menos críticos y se buscará la potencia y la eficiencia.

Otros recursos

Otros recursos muy útiles son bolsas antiestáticas para protección de dispositivos electrónicos, cajas o maletas robustas y material de acolchado, jaulas de Faraday para aislar teléfonos móviles dejándolos sin cobertura, cámaras de fotos para registrar el estado de las escenas, conexión de equipos, etc., y otras cosas como iluminación auxiliar, etiquetado y precintos para evidencias y herramientas.

2.2. Software usado para informática forense

Con el software pasa un poco como con el hardware, se tiene que estar preparados para todo lo que se pueda encontrar. Se va a empezar clasificando el software por el tipo de licencia con el que se distribuye como se detalla a continuación:

En la categoría de software con licencia comercial se tiene:

- FTK.
- ProDiscover.
- EnCase.

En la categoría de Open Source se tiene:

- Autopsy.
- Digital Forensics Framework.
- Caine Linux.

Atendiendo a las características del software se lo puede clasificar en:

Suites, que proporciona las herramientas fundamentales para desarrollar todo tipo de proceso de investigación forense, desde la adquisición de datos, hasta la emisión de informes entre ellos se tiene a Encase, FTK, ProDiscover, Autopsy, Digital Forensics Framework.

En utilidades especializadas que se centran en una tarea específica de la investigación, se puede encontrar herramientas más potentes que las incluidas en la Suite, para obtener imágenes de disco, por ejemplo, se tiene a FTK Imager o DiskExplorer y las herramientas dedicadas de generación de imágenes por línea de comando "**dcfldd**" o directamente "**dd**" y para examinar ficheros o imágenes a nivel de bits se puede usar Hex Workshop, por ejemplo.

2.3. Qué es el particionado de discos

En plataformas Linux una partición de disco se representa como un archivo dentro de la estructura de ficheros y en general en prácticamente cualquier sistema, aunque luego eso se enmascara para hacer la interfaz más amigable al usuario. Es importante ver así las particiones porque en muchas ocasiones se deberá conectar discos en computadoras con distribuciones Linux orientadas a la informática forense, ya que permiten controlar con mucho detalle los permisos de lectura y escritura, como, por ejemplo, en la distribución Caine, desarrollada específicamente para trabajos de investigación forense. Según Gallego y Folgado (2011) el disco duro un disco duro está compuesto de cabezales, pistas y cilindros, en donde, cada pista puede ser dividida en segmentos denominada sectores.

Unidad vs partición

En sistemas Linux una unidad de almacenamiento se representa como un archivo, por ejemplo, una unidad sata conectada al sistema estará representada con la ruta **"/dev/sda**", en el sistema de archivos las unidades físicas se representan con las siglas de la unidad y una letra como identificador, por ejemplo, sda, sdb, etc., mientras que las unidades lógicas, las particiones añaden un número al nombre anterior, así se tendría, por ejemplo, dos particiones en el disco "**sda**" que se mostrarían como

sda1 y sda2, por lo tanto, los dispositivos de almacenamiento son el hardware, ya sea, "**hdd**" o "**ssd**", memorias externas, por ejemplo, y las particiones son las representaciones lógicas que distingue el sistema operativo y sobre las que se operan con sus estructuras de ficheros.

En una instalación de Ubuntu Linux, se puede abrir una línea de comandos o terminal y se puede ejecutar el siguiente comando:

- sudo fdisk -l, esta opción mostrará los discos que hay conectado al sistema, como se muestra en la Figura 2.

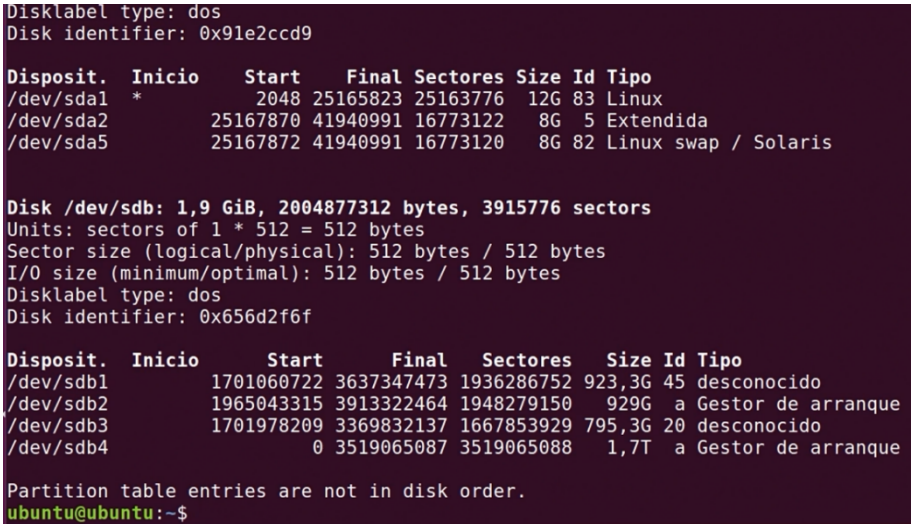


Figura 2. Listado de particiones conectadas en el Sistema Linux Ubuntu.
Fuente: elaboración propia.

En la figura anterior, se visualiza que se tiene dos discos y muestra para cada uno las correspondientes particiones, como se decía se añaden el número, en este caso, el sistema indica dónde empiezan, dónde terminan, el número de sectores, el tamaño, las unidades por sector para que se pueda calcular los distintos tamaños, esta es la funcionalidad del comando "**fdisk**", una de ellas la de listar las unidades hardware conectadas al sistema y las particiones de cada una de esas unidades.

2.4. Información hexadecimal en investigación forense

El sistema decimal utiliza 10 caracteres para representar todos los números, los caracteres que utiliza son los dígitos desde el 0 hasta el 9, el sistema hexadecimal utiliza 16 caracteres desde los 10 dígitos desde el 0 hasta el 9 y las letras desde la letra A hasta la F.

Los números del 0 hasta el 9 son idénticos en el sistema Hexadecimal que, en el decimal, pero el número 10 en el sistema decimal se representa con la letra A en el hexadecimal el número 11 es la B hasta llegar al 16 que sería la letra F. En computación es muy bien conocido que la unidad mínima de medida es el bit, formado por dos dígitos el 0 y el 1, dando lugar al byte que está formado por 8 bits, se puede hacer conversiones entre sistemas del binario a hexadecimal como se muestra en la Figura 3.

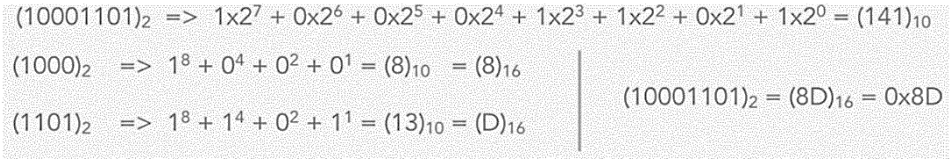


Figura 3. Conversión de un número a hexadecimal.
Fuente: elaboración propia.

En la figura anterior se tiene equivalencias entre sistemas, la letra ”A“ representa al número 10 en formato decimal y la “F” es el número 15, es decir, que el número F son cuatro unos en binario.

En informática la unidad superior al bit, es el byte, que son 8 bits, si un número de una cifra hexadecimal ocupa 4 bits con dos cifras se tiene un byte y por eso se usa la representación hexadecimal. Las herramientas de análisis de datos cuando éstos no son decodificables, los representan en formato hexadecimal, pero también, resulta útil para datos que sí son decodificables en sus correspondientes formatos, además, en ocasiones el análisis hexadecimal es necesario para identificar información oculta o modificada, ya que los datos pueden manipularse a nivel de bit para ocultar o destruir información.

Por eso, un investigador forense debe poder trabajar a nivel binario y por comodidad en hexadecimal, la codificación comparada en base binaria, decimal y hexadecimal sería la siguiente como se muestra a continuación:

“**Para 8 bits de ceros, se tendría 0 en decimal y 0 en hexadecimal, para 8 bits de 1 se tendría 255 en decimal FF en hexadecimal**”

Como se analiza el binario puede ser demasiado largo y el decimal deja sin utilizar los números del 256 al 999, así las ventajas del uso de la representación hexadecimal son:

- Es un 33% más breve que en decimal y
- Un 75% más breve que en binario

- Aprovecha todos los símbolos que hay entre el 0 y el F, lo cual permite un reconocimiento visual de patrones una vez que se lo representa en un editor hexadecimal.

2.5. Qué es el offset

La palabra offset es un término que es muy utilizado en el campo de la informática, se lo puede definir como desplazamiento, es muy importante en el análisis de datos con formato hexadecimal, ya que permite localizar información concreta en un archivo o imagen. El offset determina una posición concreta para localizar la información, que puede ser un archivo, un sector, una partición, etc.

Por ejemplo, se puede analizar en la Figura 4 la representación hexadecimal de una fotografía en formato jpg.

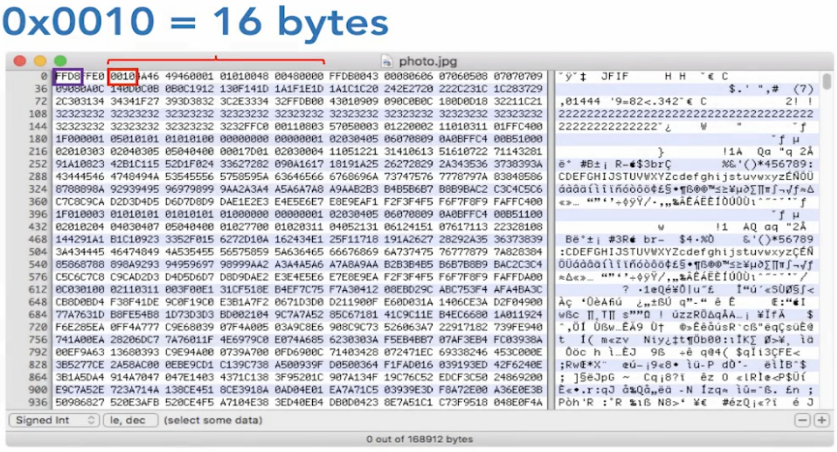


Figura 4. Representación de un archivo de imagen en formato hexadecimal
Fuente: elaboración propia.

En la figura anterior, se visualiza un inicio, formada por una cabecera que inicia en "**FFD8**", después, indica el final del archivo con los bytes "**FFD9**". Cada sector del archivo se inicia generalmente con el byte FF, seguido de otro byte indicativo y a continuación, dos bytes que indican el tamaño del sector, es decir, indican el offset.

Contando desde el primer byte de tamaño hasta el siguiente sector, así en la imagen anterior, el primer sector empieza con F0E0 y tiene un tamaño 0010, qué es 16 convertido a decimal, así que, si se señala 16 bytes incluyendo el tamaño del sector, se ve que efectivamente en ambos lados se tienen cabeceras de sector.

Lo mismo ocurre para el siguiente sector, en esta ocasión encabezado "**FFDE**" y con longitud 43 en hexadecimal, que son 67 bytes de offset desplazándose desde el primer byte que indica el propio offset, el último dato a considerar cuando se habla de numeración hexadecimal es que cuando se la escribe para diferenciarla de la decimal, se antepone el prefijo 0x a las cifras hexadecimales tal y como se muestra en el ejemplo de la Figura 5.

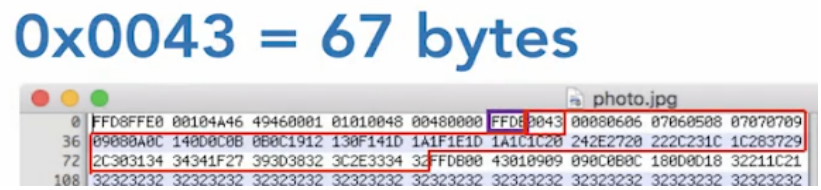


Figura 5. Verificación del offset en un archivo.
Fuente: elaboración propia.

CAPÍTULO III: RESPONDER A UN CIBERINCIDENTE

Este capítulo tratará sobre los diferentes incidentes que puedan producirse en una investigación forense, desde el estado como se encuentran los equipos, cuál es el mecanismo para recuperarse cuando se presenta un desastre, hasta la forma de informar cuando sucede un ciberincidente.

3.1. Detectar incidentes

Las organizaciones deben desarrollar e implementar un plan de respuesta a incidentes, un plan de respuesta a incidentes es algo absolutamente imprescindible para garantizar la continuidad operativa de una organización, si no existe se debe desarrollarlo, se tiene que conocerlo y darlo a conocer al resto del personal. Hay que asignar responsabilidades específicas a tareas concretas dentro de los procesos que se especifiquen el plan y para estar prevenidos, siempre es conveniente, si no, necesario practicar el plan a modo de simulacro, antes de que ocurra un incidente real y se descubra que algún protocolo no está tan bien desarrollado como debería.

3.1.1. Plan de respuestas a incidentes

Se puede plantear una situación para ver qué pasos deben seguirse, por ejemplo, suponer que se identifica la comisión de un posible delito, por ejemplo, un robo de información, lo primero que se debe hacer, es verificar que efectivamente se ha cometido esa falta o delito, o si se trata de un accidente, no es lo mismo que alguien pierda unas notas con información confidencial, que sufrir un robo de información mediante software de espionaje, por ejemplo, si se considera que en efecto hay un incidente grave, se debe bloquear el escenario del crimen, hay que evitar a toda costa la alteración de las evidencias.

3.1.2. Conservación de evidencia

Las acciones deben estar medidas y meditadas y ajustarse al plan que se haya desarrollado, las acciones impulsivas llevan a cometer errores y eso podría causar la destrucción o invalidación de evidencias, así que lo primero, es mantener los equipos en el estado en que se encuentren hasta que se tenga que trabajar con ellos.

La interacción con los equipos puede disparar mecanismos de auto borrado o corrupción de datos, etc., de hecho, lo ideal es que nadie que no forme parte del equipo de respuesta toque ningún equipo potencialmente involucrado en el incidente.

3.1.3. Notificación del incidente

Una vez que la escena del incidente está controlada, hay que decidir si hay que notificar el incidente y a quién, esto dependerá de la regulación que afecte a cada organización, por ejemplo, las consideradas infraestructuras críticas, estarán siempre obligadas a notificar los incidentes de seguridad a las autoridades competentes de su país, probablemente un organismo internacional.

Otro ejemplo se da, en base a las legislaciones de protección de datos de carácter personal, cada vez más países obligan a las organizaciones que gestionan datos a notificar a los propietarios de los mismos, si un incidente ha podido suponer que se hagan públicos o que fuesen robado, la denuncia a las autoridades policiales es recomendable, aunque sea, sólo para que el estado sea consciente de que los ciberdelitos existen.

3.1.4. Evaluación de impacto

A continuación, se debe determinar el nivel apropiado de respuesta, para ello, se evalúa el potencial impacto del incidente en curso y se activa el plan de respuesta conveniente asignando los recursos que sean necesarios para recuperarse del incidente lo antes posible, minimizando ese impacto calculado.

A la hora de evaluar el problema, se debe recopilar cierta información preliminar, se tiene que Identificar y entrevistar testigos tan pronto como sea posible, porque la memoria de las personas es casi más volátil que la RAM del computador y se rompe con facilidad.

En estas entrevistas, se debe incluir tanto a personal con acceso físico a las evidencias, como con acceso telemático, así como, a las personas que trabajen con las primeras, hay que ser amistoso con los compañeros o clientes, se debe identificar, etiquetar y catalogar todos los dispositivos y servicios dentro y fuera de las instalaciones de la organización, involucrados real o potencialmente en el incidente, esto incluye:

- Ordenadores.
- Portátiles.
- Tabletas.
- Smartphones.
- Impresoras y otros dispositivos.

Se registrará datos como números de serie, marca, modelo, conectividad, sistema operativo, cuentas de usuario y contraseñas, proveedores de servicio, etc., con toda esta información se tendrá una foto fija del estado del incidente, sea un incidente fortuito o un delito y de los actores involucrados en el momento en el que se ha descubierto el problema, lo cual permitirá manejar adecuadamente los pasos a seguir a partir de ese punto.

3.2. Equipos encendidos vs. equipos apagados

En el escenario de un incidente se puede encontrar a los equipos encendidos y equipos apagados y en cada caso, hay que operar de manera distinta, lo primero es ser conscientes de dos conceptos que se tiene que asumir desde el principio.

El análisis forense físico no es igual a la digital, cada uno tiene sus condicionantes, en la escena de un delito no se recoge todo lo que hay, lo que se hace es fotografía del estado de la escena para saber cómo está todo y luego se investiga cada evidencia y se va recogiendo de una en una.

Lo mismo hay que hacer con las evidencias digitales, no se agarra todo lo que uno encuentra porque sí, se denomina coloquialmente análisis postmortem al que se practica sobre equipos que se encuentran apagado, tradicionalmente se apagaban los equipos para preservar las evidencias y eliminar riesgo de modificación, pero entonces, se podía perder información volátil.

El objetivo principal de este tipo de análisis es la recuperación de datos de las unidades de memoria como discos duros o memoria USB. Se llama e-Discovery al proceso de capturar y analizar grandes cantidades de datos para descubrir evidencias entre ellos, al ser una forma de adquisición masiva de datos, suele darse en incidentes graves y grandes o relacionados con grandes infraestructuras, puede involucrar decenas o cientos de equipos, sistemas raid, etc., el objetivo no es tanto localizar información oculta, cómo detectar información relevante entre la masa total de datos disponibles, este trabajo puede gestionarse mediante técnicas de Big Data.

El análisis de equipos en vivo es el que se practica cuando se encuentra con una computadora o un servidor encendido, en lugar de apagado. Es típico de respuestas a brechas de seguridad en redes o equipos y busca la captura de datos reales en vivo, tiene ciertas ventajas sobre los escenarios postmortem, como el acceso a disco cifrados, el volcado de memoria RAM, el acceso archivos temporales, etc., el

problema es que suele modificarse la evidencia por la actividad del propio perito, el análisis en vivo no siempre es posible, pero siempre se puede recurrir a analizar otros equipos de la misma infraestructura para comprender cómo interactuar.

3.3. Recuperación de desastres por incidente o ciberdelito

El trabajo de los forenses empieza desde el momento que se detecta un incidente, hasta que esté controlado. Se debe tener una perfecta organización cuando se presente un incidente, para ello, se debe tener lo que se denomina como "plan de respuesta a incidente", que se constituye como la herramienta fundamental cuando se tiene que enfrentar a un problema, y para esto, se tiene que considerar tres elementos:

- El denominado plan de recuperación de desastres.
- Un plan de continuidad del negocio
- La metodología por seguir.

Plan de recuperación

Cuando se planifique un plan de recuperación, no se exige que tengan que ser precisos, a diferencia de los procedimientos concretos, los planes se ejecutarán cuando tenga lugar un incidente, pero los incidentes pueden llegar a ser inimaginables, por este motivo, el plan debe encauzar, pero no constreñirlos, la figura 6 muestra un esquema del plan de recuperación.

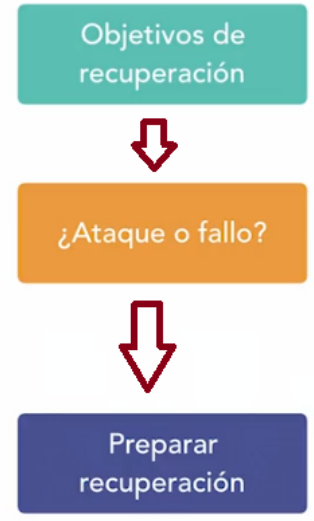


Figura 6. Plan de recuperación ante desastres.
Fuente: elaboración propia.

En la figura anterior, la primera parte del plan debe ser establecer los objetivos de recuperación determinando en el proceso, si el incidente se trata de un ataque o de un fallo, a continuación, se debe preparar la recuperación de la operativa normal y para ello se debe saber cuál es el nivel normal de servicio, calcular cuándo se podrá conseguirlo y establecer el cómo.

En gestión de incidentes, hay dos cosas que se sabe, la primera es, si se ha preparado cómo funciona la infraestructura de la organización y de qué se compone. La segunda certeza es que no se sabe cuándo puede ocurrir un desastre, por este motivo, es conveniente tener siempre a punto un kit de emergencias o maletín de desastres, estas herramientas deben haber sido escogidas en base a lo que se sabe de la infraestructura de la organización y se debe mantenerlos siempre actualizado y a punto, porque no se sabe cuándo se podrá necesitarlo, es aconsejable que la gestión de los recursos de emergencia, forme parte del plan de respuesta a incidentes para tenerlos inventariados y controlados.

3.4. Informar o denunciar ciberincidentes

Por norma general la notificación de un incidente tiene tres fases:

- El reporte inmediato.
- Los reportes adicionales.
- Compartir información.

El reporte inmediato como su propio nombre indica, es el primero que se tiene que ejecutar y debe iniciarse en el mismo momento de descubrir el incidente y actualizarse periódicamente, en primer lugar, está notificación va dirigida al personal interno de la organización, son los gerentes, técnicos y personal cuya actividad se puede ver afectada por el incidente que tenga que intervenir en resolver el incidente, o que tenga que intervenir en la mitigación de las consecuencias del incidente.

El plan de respuesta a incidentes y el de continuidad de negocio, deberían definir quiénes son estas personas y qué información requieren, si se tienen sospechas fiables de que un incidente puede deberse a un ataque o actividad delictiva de cualquier tipo, hay que interponer la debida denuncia y alertar a las autoridades, algunas empresas no denuncian por miedo a daños a su reputación o por miedo a interferencias de las fuerzas y cuerpos de seguridad del estado en el restablecimiento de las operaciones necesarias para dar continuidad al negocio.

La notificación a las fuerzas y cuerpos de seguridad, es más que obligatoria si durante el análisis forense del incidente, se detecta que éste se debe a sistemas de espionaje, ya sea, mediante software o hardware, sin embargo, las organizaciones catalogadas como infraestructuras críticas, tienen la obligación de reportar los incidentes a la autoridad que especifique la normativa de infraestructuras críticas de su país, dicha normativa puede incluso definir plazos máximos de notificación, así como la forma y el contenido de dichas notificaciones.

Los reportes adicionales, son los que no son críticos para la continuidad de negocio, pero no por ello son menos importantes, en algunos casos, son también obligatorios, estos se clasifican en:

- Propietarios de datos personales.
- Víctimas de daños colaterales.
- Otros organismos competentes en materia de seguridad.

Se debe informar a los propietarios de datos personales que puedan haberse visto afectados, si no, por ética profesional al menos porque las leyes de protección de datos de carácter personal de los distintos países suelen requerirlo.

Así lo dicta, por ejemplo, el nuevo reglamento general de protección de datos que es obligatorio a partir de abril de 2018 para toda empresa que presta servicios en los países miembros de la Unión Europea. Cada país, además, puede tener mandamientos específicos a este respecto y establecer la forma y plazos en que dichas notificaciones deben ser realizadas, también, se debe notificar los incidentes en la forma que sea más conveniente a víctimas, como, por ejemplo, empresas que subcontratan servicios a la organización.

Estas víctimas deben ser notificadas dado que el incidente puede afectar al servicio que se les prestan y suponer un incumplimiento del contrato o de los acuerdos de nivel de servicio, sin contar con que datos de los clientes se pueden haber visto comprometidos, estas notificaciones adicionales dependiendo de la regulación del país, pueden conducirse a través de la policía si se ha Interpuesto la pertinente denuncia.

Los incidentes debido a vulnerabilidades detectadas en el hardware o software de la infraestructura de la organización deberían ser notificados también a los organismos competentes, para que se pueda trasladar la notificación a los fabricantes y que desarrollen los parches necesarios.

Si se habla de compartir, no sólo con el fabricante, sino, con otras organizaciones para que puedan evitar incidentes derivados de las mismas vulnerabilidades, por último, se tiene que valorar la opción de compartir la información del incidente de forma pública, especialmente la información técnica. Existen entidades públicas y privadas a las que reportar vulnerabilidades e incidentes de ciberseguridad con el objetivo de cooperar y compartir información, generando un efecto vacuna, de forma que, el primer afectado ayuda a los demás a protegerse.

Además, compartir información enriquece los conocimientos de los responsables y de todas las organizaciones y mejora la seguridad global. Algunos organismos con los que se puede compartir este tipo de incidentes:

- ENISA (Agencia Europea para la seguridad de la red y la información).
- CERT públicos y privados.
- INCIBE.
- Asociación de empresas.

La notificación y en su caso denuncia de incidentes, sienta precedentes tanto a nivel tecnológico como a nivel policial y judicial, permitiendo la adaptación de todos los involucrados a las nuevas circunstancias derivadas de la evolución de las tecnologías de la información.

CAPÍTULO IV: ADQUISICIÓN DE DATOS EN INFORMÁTICA FORENSE

Este capítulo tiene como objetivo demostrar la manera de adquirir los datos para la investigación forense, desde el uso de herramientas open Source, hasta las comerciales, también, se enfocará en realizar copias de imágenes de la información encontrada para que esta no sufra ningún cambio que puedan afectar la investigación, también se podrá obtener información en vivo de todas las evidencias encontradas hasta el análisis del volcado de la memoria con herramientas especializadas en esta.

4.1. Adquisición estática con herramienta Open Source

La adquisición estática de evidencias es la más común que suele darse en informática forense y habitualmente la más sencilla. La adquisición estática consiste en la extracción de datos de fuentes de almacenamiento no volátil, por ejemplo, discos duros, tarjetas SD, memoria USB y cualquier otro soporte de información digital. Se trata de generar una imagen, se dice que estos soportes de almacenamiento contienen información no volátil, porque esta continúa presente en el dispositivo, aunque se lo apague y se le retire el suministro eléctrico, cosa que no pasa, por ejemplo, con la memoria RAM.

Existen múltiples herramientas Open Source disponibles para obtener imágenes de discos o particiones, pero existe un comando llamado "**dd**" en la plataforma Linux y Mac OS. Por ejemplo, en Caine Linux, que es una distribución basada en Ubuntu, pero el comando "**dd**" se lo puede encontrar en todos los sistemas.

Para verificar que unidades hay conectadas a la máquina en el sistema Caine Linux se tiene que abrir una ventana de consola mediante el siguiente comando **"sudo fdisk -l**", como se muestra en la Figura 7.

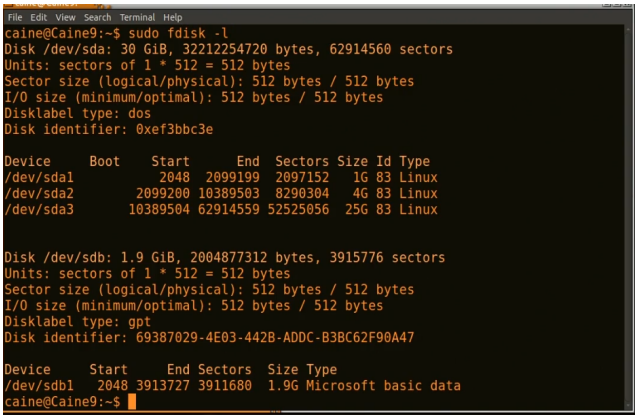


Figura 7. Visualización de discos conectados en Caine Linux.
Fuente: elaboración propia.

En la figura anterior, se puede verificar que salen algunas unidades de disco con varias particiones conectadas como la "**sda**" con 30 gigas y "**sdb**" que es una memora USB conectada de 1.9 gigas.

Para poder hacer una imagen, lo primero que se tiene que hacer es montar esta unidad en modo sólo lectura, se puede tipear el siguiente comando:

- sudo mount-o ro /dev/sdb1

Con este comando la unidad sdb1 ya está montada, si ahora se va, por ejemplo, al explorador de archivos se verifica que se tiene la unidad con todos sus archivos, como se muestra en la Figura 8.

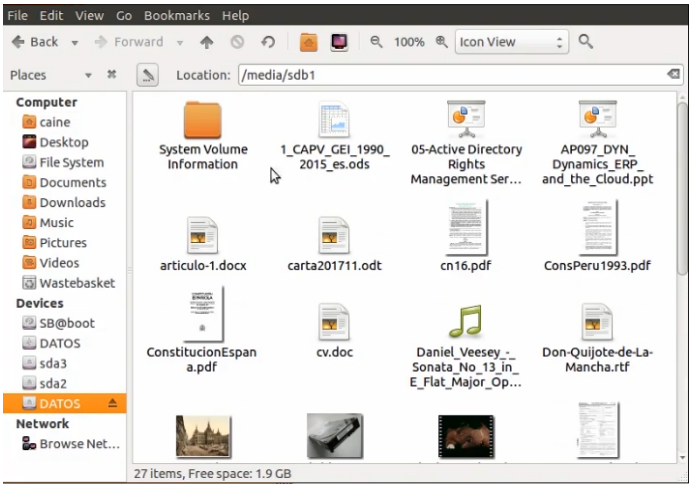


Figura 8. Montaje de una unidad en Caine Linux.
Fuente: elaboración propia.

Si se desea hacer una imagen de esta unidad, se abre la ventana de comandos y se debe ir primero al escritorio, teniendo en cuenta que cuando no se indica el punto de montaje, éste va a ser en la carpeta "media", una vez en la consola se va a ejecutar el comando:

- "sudo dd if=/dev/sdb"

Con el comando anterior, se quiere hacer una copia completa de la unidad, no se indica el número, hay que recordar "sdb" es la unidad y sdb1 es la partición, que en este caso coincide, al comando anterior se le añade un nombre de salida con varios parámetros más como se muestra en la Figura 9.

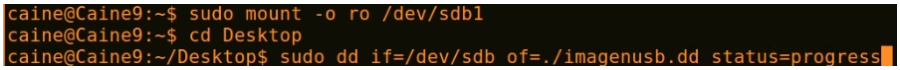


Figura 9. Creación de una copia de una imagen USB en Caine Linux.
Fuente: elaboración propia.

En la figura anterior, se empieza el proceso y se debe dejar que termine, mientras tanto en el escritorio se creará el archivo con el nombre indicado, en este caso, "**imagenusb.dd**".

Todo este proceso también se lo puede realizar en una herramienta grafica que está disponible en Caine Linux, denominada GUYMAGER, cuya interfaz se muestra en la Figura 10.

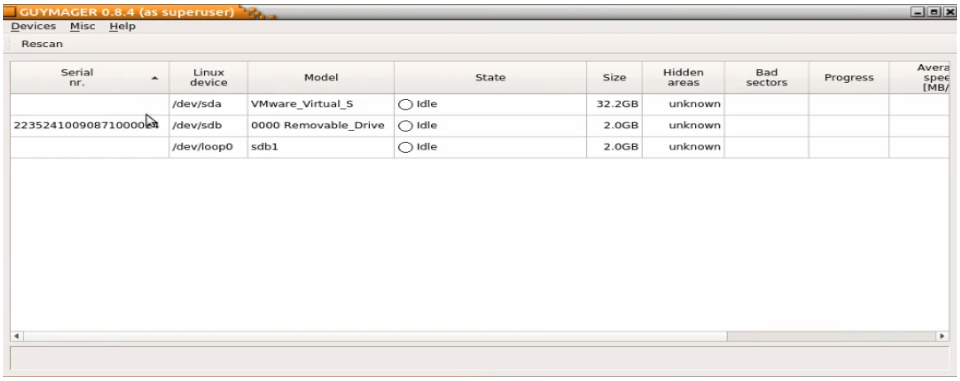


Figura 10. Herramienta de copia de imagen en Caine Linux.
Fuente: elaboración propia.

En la figura anterior, se analiza que aparecen las distintas unidades, se selecciona el dispositivo extraíble que sería "**sdb**" y se indica adquirir imagen como se muestra en la Figura 11.

Figura 11. Adquisición de una imagen en el Programa GUYMAGER.
Fuente: elaboración propia.

Una vez adquirida la imagen aparecerá la pantalla con varias opciones como se muestra en la Figura 12.

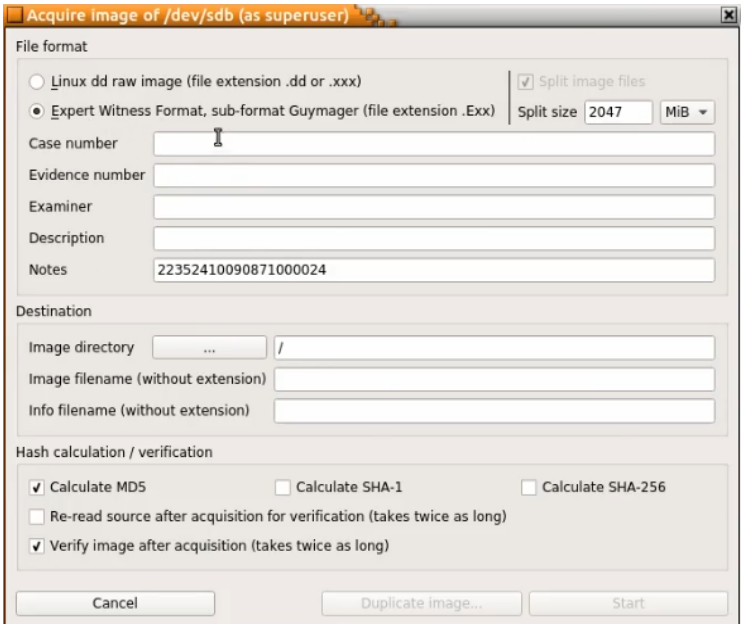


Figura 12. Opciones de la adquisición de imagen en GUYMAGER.
Fuente: elaboración propia.

Para indicar el proceso se deben seleccionar varios parámetros, desde la ubicación donde se almacenará la imagen, hasta el nombre como se muestra en la Figura 13.

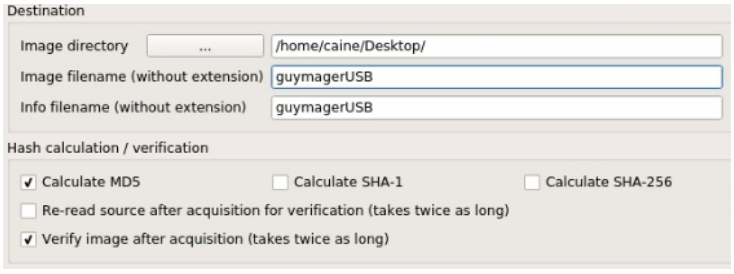


Figura 13. Creación del archivo de imagen en GUYMAGER.
Fuente: elaboración propia.

Este programa genera dos archivos, la copia o la imagen y un archivo de información, el proceso es más rápido, mucho más eficiente que la vez anterior, estas son dos formas en Caine Linux de obtener imágenes, mediante comandos y por una herramienta gráfica.

Otras herramientas disponibles, por ejemplo, son el comando "**dcfldd**" cuyas siglas provienen de "US Department of Computer Forensic Lab dd", la cual es una versión forense de "**dd**", la herramienta que se acaba de utilizar.

También, se tiene el software Clonezilla, de la cual se puede utilizar una versión Live para el arranque de una computadora, extraer imágenes sin iniciar el sistema operativo de la computadora en cuestión.

4.2. Crear una imagen de disco en varios archivos con DD

Suponer que se tiene un disco de gran tamaño del que se necesita extraer una imagen, pero se necesita que no sea de un único archivo, porque luego se va a tener que almacenarla en varios dispositivos, por ejemplo, en varias sedes o lugares.

Si el disco original es superior a 650 megas no se va a poder almacenarlo, entonces se trabajaría de la siguiente manera, primero, se tiene que comprobar que realmente está conectada la memoria USB de la que se quiere extraer la imagen en la computadora, para ello se ejecuta el siguiente comando:

- sudo fdisk-l

Con el comando anterior, se verifica la unidad y su tamaño como se muestra en la Figura 14.

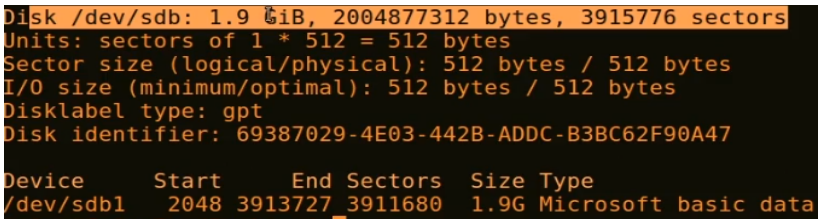


Figura 14. Verificación de unidad en Linux mediante el comando fdisk.
Fuente: elaboración propia.

Aquí, se debe hacer una imagen de la unidad, no de la partición y el comando podría quedar de la siguiente manera:

- sudo dd if=/dev/sdb status=progress I split-b 650m – usb.

Con esto, el comando Split va añadiendo extensiones a los archivos ejecutamos, se ejecuta el comando y se crea la imagen como se muestra en la Figura 15.

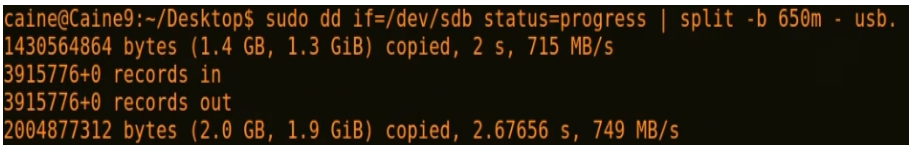


Figura 15. Resultado de la copia de imagen con el comando dd.
Fuente: elaboración propia.

El proceso anterior, se lo podría realizar de una manera más comprensible utilizando el comando "dd" de la siguiente manera:

- sudo dd if=/dev/sdb of=p1 bs=512

El comando anterior, saca la imagen parte por parte, en este caso, sería la primera porción del archivo

También, se debe seleccionar los bits de la unidad de almacenamiento desde el cero, hasta un número determinado, en este caso se quiere que sea de 650 Megas, para esto se una el siguiente parámetro a la línea de comando anterior:

- sudo dd if=/dev/sdb of=p1 bs=512 count=$[1024*1024*650/521] status=progress

Con esto se crea el primer archivo, para obtener la segunda parte del archivo, el tamaño debe ser el mismo que la línea de comando anterior, pero antes se debe realizar una operación:

- echo $[1024*1024*650/512] = 1331200

Este es el tamaño en sectores de uno de los archivos que se acaban de hacer, entonces el segundo archivo tiene que llevar un nombre, en este caso "**p2**" que tendrá el mismo tamaño, pero se tiene que incluir un parámetro que se salte lo que se ha capturado en el primer archivo, el comando quedaría de la siguiente manera:

- sudo dd if=/dev/sdb of=p2 bs=512 count=$[1024*1024*650/521] skip=$[1024*1024*650/521] status=progress.

Con esto ya se tienen dos archivos p1 y p2 del mismo tamaño como se muestra en la Figura 16.

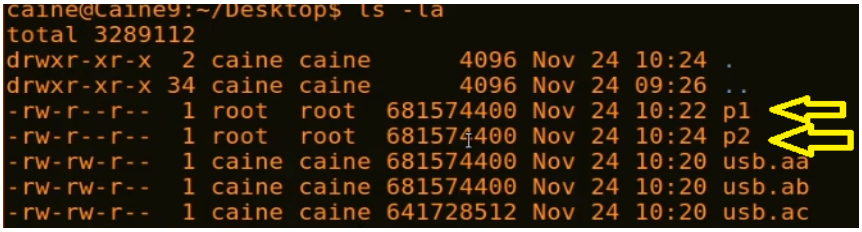


Figura 16. Generación de varios archivos de imágenes con el comando dd.
Fuente: elaboración propia.

Se puede apreciar en la figura anterior, que se han obtenido los dos nombres de ficheros, para poder unirlos en uno solo se puede tipear el siguiente comando:

- cat p1 p2 > partes.dd

El comando anterior concatena los archivos y lo guarda en uno solo, para comprobar que el hash del archivo es el mismo se utiliza el siguiente comando:

- md5sum partes.dd

Con esto, se comprueba que el hash del archivo coincide como se muestra en la Figura 17.

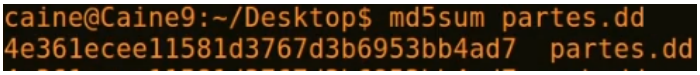


Figura 17. Comprobación del hash del archivo con el comando dd.
Fuente: elaboración propia.

Se ha realizado una copia fraccionada de una imagen de una unidad de disco de dos formas distintas, ensamblado cada una por separado y, aun así, se sigue manteniendo el hash, por lo tanto, la evidencia es completa y es confiable.

4.3. Adquisición estática con dcfldd (DD forense)

Dcfldd es una versión forense de "**dd**" y funciona más o menos igual que la aplicación antes mencionada, pero está desarrollada por el laboratorio de informática forense de los Estados Unidos pensando en su fiabilidad, para instalar esta herramienta se puede ejecutar el siguiente comando.

- sudo apt-get install dcfldd

Para esto se debe abrir una ventana de comando en Caine Linux y ejecutar para proceder a la instalación como se muestra en la Figura 18.

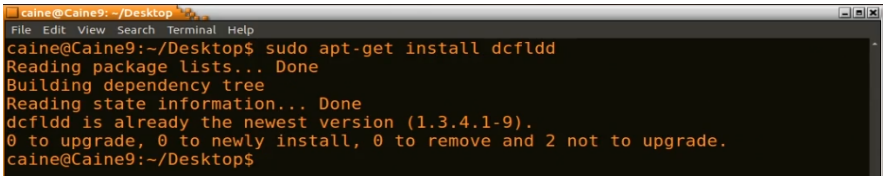


Figura 18. Instalación de la herramienta dcfldd en Caine Linux.
Fuente: elaboración propia.

En el caso de la figura anterior, la herramienta ya está instalada, lo primero como siempre, se tiene que comprobar si la unidad está montada, en este caso, está montada como se muestra en la Figura 19.

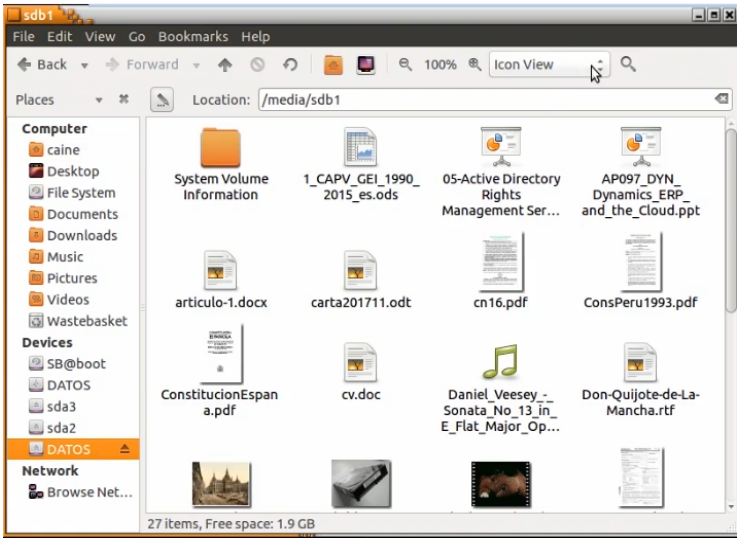


Figura 19. Comprobación de montaje de unidad en Caine Linux.
Fuente: elaboración propia.

En este caso, se puede realizar la copia, para ello se ejecuta el siguiente comando:

- sudo dcfldd if=/dev/sdb of=usbimage.ddf hash=sha256 haslog=usbimage.log

El siguiente comando crea la imagen de la unidad USB y se agrega un nombre como salida de archivo, en este caso, "**usbimage.ddf**", este comando tiene la ventaja que también se pueden enviar como parámetro el cálculo del hash de la imagen USB, el cual puede ser el hash "**sha256**" y que guarde el haslog en "**usbimage.log**", se ejecuta el archivo y se procede a crear la imagen con los parámetros establecidos, creando dos archivos donde almacenará la imagen de la copia y el hash.

En el caso si se abre el archivo del hash se puede verificar el hash creado, que es el sha256 de la unidad de memoria como se muestra en la Figura 20.

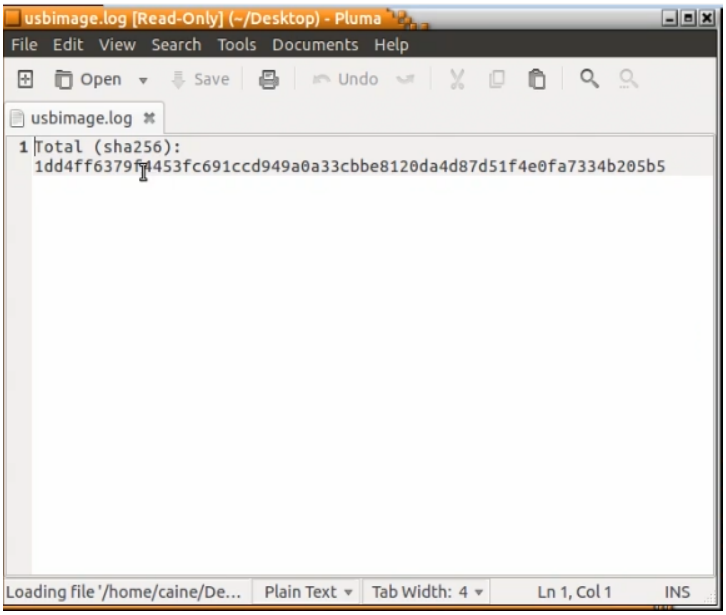


Figura 20. Creación del hash de la imagen con la herramienta dcfldd.
Fuente: elaboración propia.

En resumen, "**dcfldd**" es más fácil y un poco más seguro de usar que "**dd**", si se desea ver todas las opciones del comando se tipea la siguiente sentencia "**dcfldd help**" y se muestra un resumen de todas las opciones disponibles como se muestra en la Figura 21.

```
  \r   Carriage return
  \\   Insert the '\' character
  ##   Insert the '#' character as text, not a variable

BLOCKS and BYTES may be followed by the following multiplicative suffixes:
xM M, c 1, w 2, b 512, kD 1000, k 1024, MD 1,000,000, M 1,048,576,
GD 1,000,000,000, G 1,073,741,824, and so on for T, P, E, Z, Y.
Each KEYWORD may be:

  ascii     from EBCDIC to ASCII
  ebcdic    from ASCII to EBCDIC
  ibm       from ASCII to alternated EBCDIC
  block     pad newline-terminated records with spaces to cbs-size
  unblock   replace trailing spaces in cbs-size records with newline
  lcase     change upper case to lower case
  notrunc   do not truncate the output file
  ucase     change lower case to upper case
  swab      swap every pair of input bytes
  noerror   continue after read errors
  sync      pad every input block with NULs to ibs-size; when used
            with block or unblock, pad with spaces rather than NULs

Report bugs to <nicholasharbour@yahoo.com>.
caine@Caine9:~/Desktop$
```

Figura 21. Listado de todas las opciones de la herramienta dcfldd.
Fuente: elaboración propia.

Esta herramienta contando con el respaldo de sus desarrolladores, puede ser una aplicación más respetable y por lo tanto, confiable en procesos de investigación, sea cual sea la herramienta de obtención de imágenes que se use, se debe en cuenta que el rendimiento, es decir, la velocidad no sólo depende del tamaño de la evidencia, también, influye en la velocidad de lectura del soporte digital y la velocidad de escritura en el disco de destino de la imagen, la más lenta será la que marca el ritmo y luego se tiene la potencia de procesado que afecta en menor medida a la copia y al cálculo de los hashes sobre todo para imágenes de gran tamaño.

4.4. Adquisición estática con una herramienta comercial

En esta sección, se va a realizar la adquisición estática de la imagen de un soporte de almacenamiento, en concreto, de una memoria USB mediante FTK Imager de la empresa AccessData, que es una herramienta gratuita, pero no libre.

Para su descarga se debe ir a la web de AccessData disponible en https://accessdata.com/ y cuya página principal se muestra en la Figura 22.

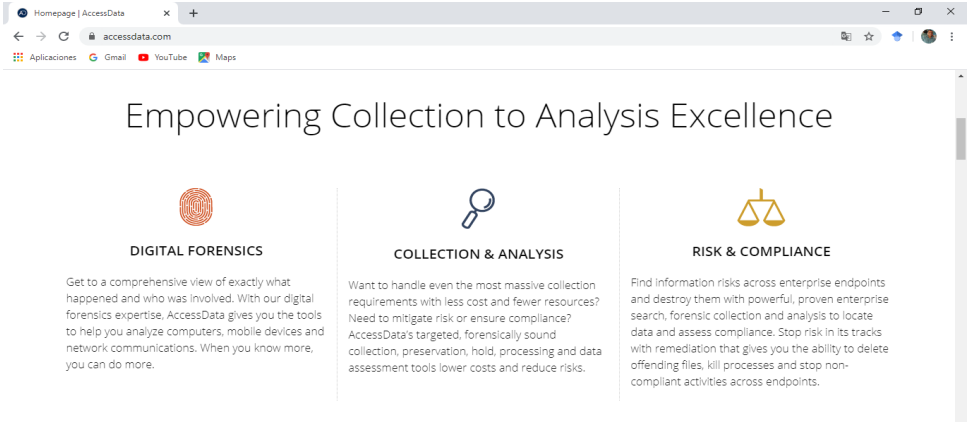


Figura 22. Página de descarga de la herramienta FTK Imager.
Fuente: elaboración propia.

Para descargar el aplicativo se debe ir a la opción de productos o servicios productos, descargar y buscar FTK Imager, se seleccionar la última versión y aquí se da acceso al panel donde se solicita los datos del usuario para enviar el enlace de descarga al correo con que se registra.

Una vez descargada e instalada la herramienta se puede ejecutar y aparecerá la pantalla principal para crear la imagen, para lo cual se tiene que ir a la opción "**File - >Create Disk Image**" y aparecerá una pantalla de opciones como se muestra en la Figura 23.

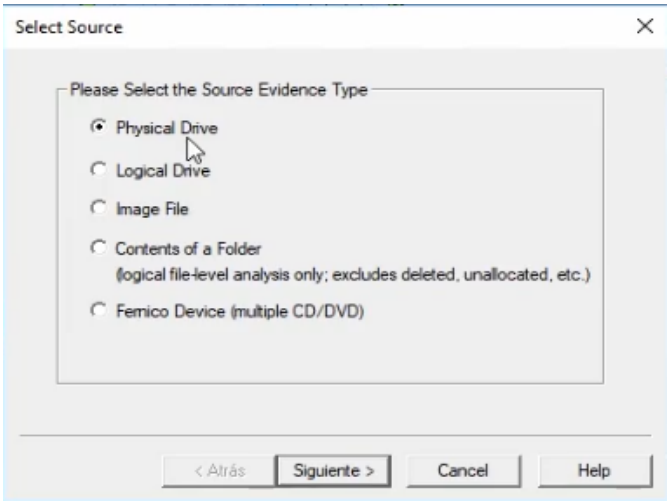


Figura 23. Opciones para la creación de una imagen en FTK Imager.
Fuente: elaboración propia.

Después de seleccionar la primera opción, Physical Drive, aparecerá una pantalla para seleccionar la memoria USB como se muestra en la Figura 24.

Figura 24. Selección de la imagen en FTK Imager.
Fuente: elaboración propia.

Una vez seleccionada la imagen, lo que se tiene que hacer es indicar el destino que va a tener la copia y el tipo de copia que puede ser:

- Raw(dd).
- SMART.
- E01.
- AFF.

Se selecciona la primera opción, es decir una copia en crudo y aparecerá la siguiente pantalla como se muestra en la Figura 25.

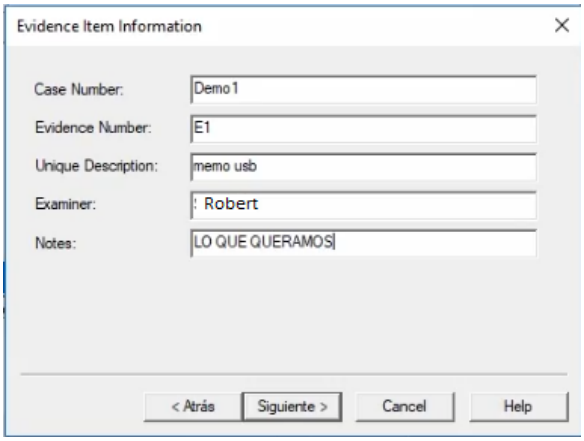


Figura 25. Llenado de datos para la creación de la evidencia en FTK Imager.
Fuente: elaboración propia.

Después de esta pantalla, se da clic en siguiente y se elige en este caso, el escritorio como destino de la copia y el nombre, se puede elegir el tamaño de los archivos si se quiere fragmentar la imagen en trozos más pequeños, la Figura 26 muestra la creación de la imagen.

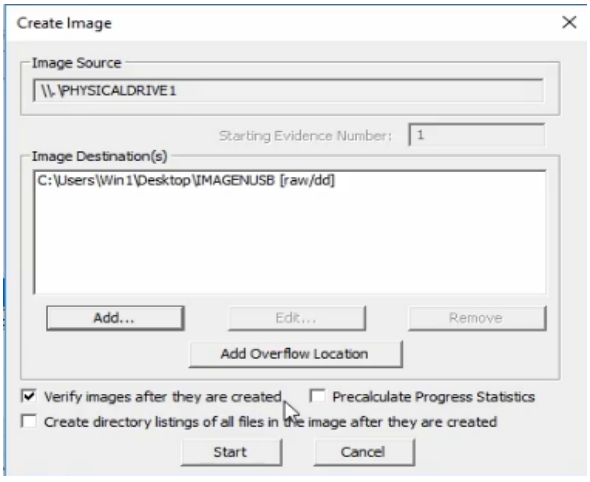


Figura 26. Creación de la imagen con parámetros de salida en FTK Imager.
Fuente: elaboración propia.

Una vez completado el proceso se muestra una ventana con los resultados obtenidos de la creación de la imagen como se muestra en la Figura 27.

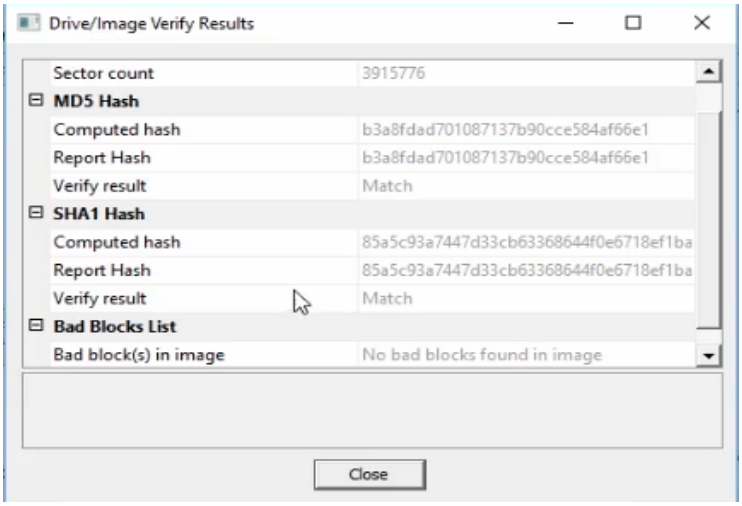


Figura 27. Detalle de los resultados obtenidos en la creación de la imagen de USB.
Fuente: elaboración propia.

La figura anterior, muestra varios parámetros como los hashes original y copia, con esto se obtiene una imagen de disco completa mediante FTK Imager y se ha capturado simultáneamente el hash de la original de la copia, por lo que al verificar que es válido, cualquier análisis que se haga a la copia será como si se lo hiciera al original, pero preservando la integridad de este, hay que tener en cuenta que el original hay que tenerlo conectado a la computadora con un protector contra escritura vía hardware, después el resultado será los archivos con los hashes y el proceso como se muestra en la Figura 28.

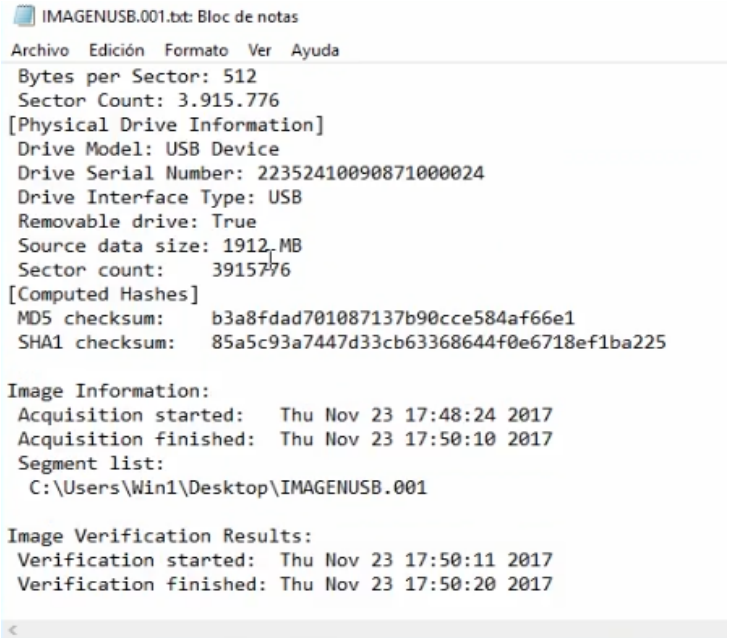


Figura 28. Archivos y hashes de verificación de la imagen creada con FTK Imager.
Fuente: elaboración propia.

Toda la información que se obtiene deberá añadirse a la investigación, para determinar cómo se ha realizado la copia.

4.5. Adquisición en vivo con FTK Imager

En Windows 10, existe la herramienta FTK Imager perteneciente a la empresa **Accesdata**, cuyo objetivo es crear y gestionar imágenes de disco, incluso puede hacer volcado de memoria, para esto se puede abrir la aplicación e ir a la opción "**File->Capture Memory**", una vez seleccionada la opción aparece una pantalla que indica donde se debe almacenar la captura de los datos de la memoria, entre los parámetros a considerar está un archivo denominado "pagefile.sys", denominado memoria virtual que es utilizado para intercambiar datos e información entre el sistema y la memoria RAM, normalmente ocupa un porcentaje del tamaño de esta memoria, por ejemplo, si se tiene una RAM de 4 gigas, se debería tener un pagefile. sys de 16 gigas, la Figura 29 muestra el proceso de captura de memoria.

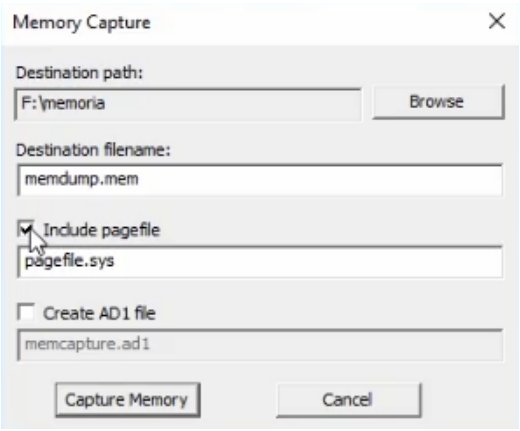


Figura 29. Pantalla de captura de la memoria en FTK Imager.
Fuente: elaboración propia.

En la figura anterior, se visualiza el archivo ad-1, que es un archivo de captura de memoria propietario de AccessData, en este caso, no se los va a solicitar.

A partir de este punto, toca esperar, el resultado de este proceso será un archivo con la extensión ".mem", para ver el resultado del volcado de memoria se puede usar la suite comercial FTK AccessData o aplicaciones de software libre como, por ejemplo, Volatility.

Estas herramientas de análisis indexan automáticamente la información que encuentran para no tener que explorar toda la RAM con un editor hexadecimal, ya que con tantas gigas como se usan actualmente, no se abarcaría el total de la información nunca.

4.6. Análisis de volcado de memoria con Volatility

Volatility es una herramienta Open Source desarrollada por la comunidad y mantenida por Volatility Foundation una organización sin ánimo de lucro cuya, el propósito de esta herramienta es el análisis de los volcados de memoria que se hayan obtenido durante la adquisición en vivo de otras computadoras, esta organización está disponible en internet en la siguiente dirección https://www.volatilityfoundation.org/, cuya página principal se muestra a continuación en la Figura 30.

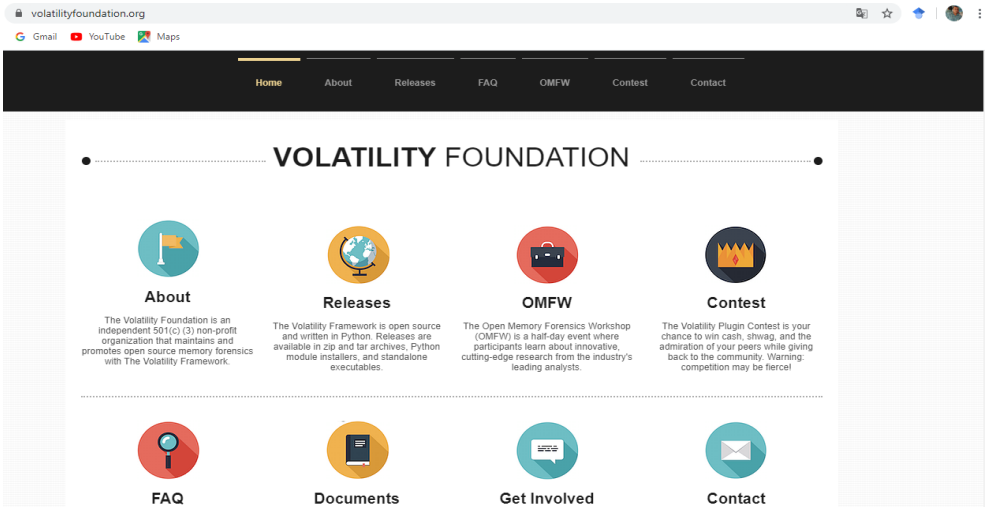


Figura 30. Página principal de Volatility Foundation.
Fuente: recuperado de https://www.volatilityfoundation.org

Para realizar pruebas en vivo, se debe descargar la herramienta en la página de la organización en el vínculo denominado "**Releases**", se selecciona la opción más conveniente de las varias opciones que se muestran en la Figura 31.

Figura 31. Selección de versión de descarga de Volatility.
Fuente: recuperado de https://www.volatilityfoundation.org

En el caso de la figura anterior, se selecciona "**Volatility 2.6 Windows Standalone Executable"**, una vez descargado se lo almacena en una carpeta y se procede a extraer el contenido directamente en el escritorio, se puede cambiar el nombre de la carpeta por comodidad a Volatility y dentro se puede encontrar información sobre los autores, crédito, información legal, licencia y el ejecutable.

En ese programa se puede ver las capturas de memoria, que pueden estar almacenada en la memoria externa, se procede a seleccionar estos archivos y por comodidad se puede trabajar con ellos en el mismo directorio que el programa, para esto se tiene que iniciar el intérprete de comandos en Windows y lo primero que se tiene que hacer es obtener información sobre el tipo de memoria analizada, es decir, no es lo mismo trabajar con una computadora Macintosh, que con una computadora Windows, depende de donde se haya hecho el volcado de memoria, así se deberá procesar la información, además, no sólo importa el tipo o el proveedor, también, la versión del sistema operativo.

Abierta la terminal se procede a ejecutar el comando con los siguientes parámetros:

- Volatility.exe imageinfo-f memdump.mem

Donde "**imageinfo**" le da instrucciones a la aplicación Volatility, que sería el equivalente a los metadatos del volcado de memoria, este proceso tardará más cuanto mayor sea el archivo por analizar, así que puede ser ejecutando.

También, se puede ejecutar Volatility para obtener la información sobre los plugin y demás información que puede proporcionar este programa, en este caso, se obtiene todos los datos como muestra la figura 32.

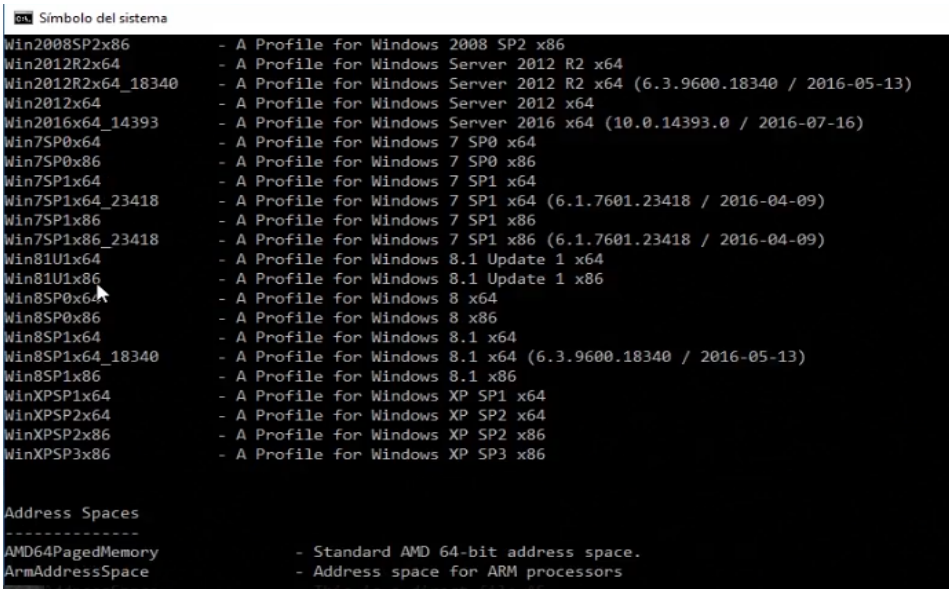


Figura 32. Listado de plugin y opciones de Volatility.
Fuente: elaboración propia.

También, muestra información de los perfiles, es decir, lo que se está tratando de averiguar en el intérprete de comandos. Una vez terminado el proceso, se puede ver los posibles sistemas operativos a los que puede corresponder el volcado de memoria.

A continuación, se puede realizar una búsqueda para ver qué procesos había en ejecución al hacer el volcado de memoria, así que se puede ejecutar Volatility con los siguientes parámetros:

- Volatility.exe-f memdump.mem – profile=Win10x64_14393 pslist

En el comando anterior, se indica el perfil deseado, la solicitud de información y los procesos en ejecución y aparece información sobre todos los procesos que había en ejecución, como se muestra en la Figura 33.

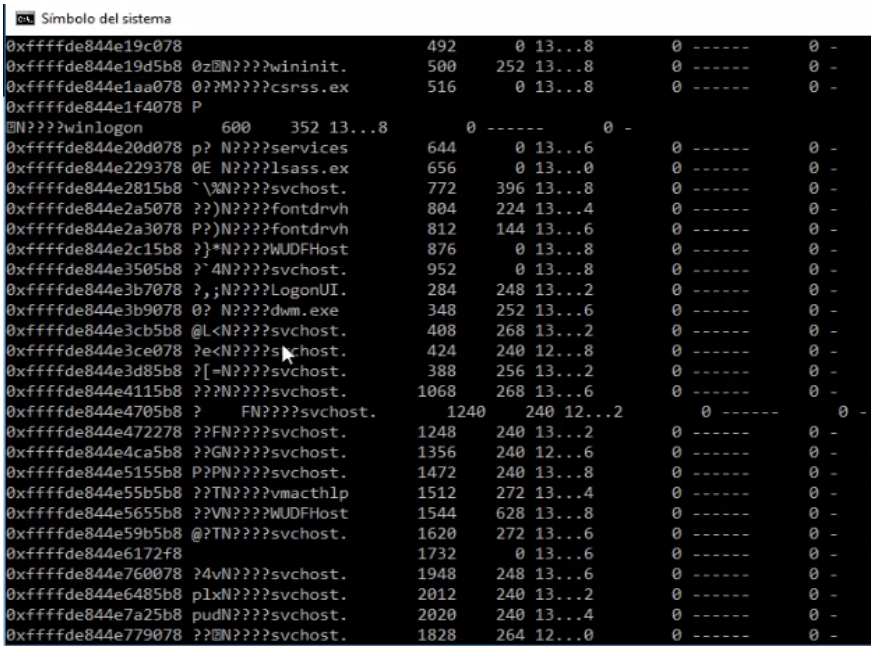


Figura 33. Resultado de búsqueda de los procesos en memoria con Volatility.
Fuente: elaboración propia.

Esto es solo un ejemplo de lo que se puede averiguar de lo que estaba sucediendo en el equipo, otra información importante a la hora de analizar, es que en la primera columna se tiene el offset, es decir donde se ha encontrado en el archivo de memoria la información sobre el proceso en ejecución, al haber ejecutado un programa en la máquina que se está investigando, este va a dejar huellas, además de la búsqueda anterior, con Volatility se puede realizar búsquedas por patrones

y se puede encontrar claves públicas y privadas de certificados SSL, se puede ver el histórico de comandos de la ventana de consola, se puede localizar conexiones abiertas que hubiese durante el volcado de memoria, y también se puede obtener archivos cargados en memoria, también se puede buscar historiales de navegación.

En resumen, Volatility es un buscador en base a patrones conocidos de información específica en volcado de memoria.

CAPÍTULO V: CONSERVACIÓN DE DATOS EN INVESTIGACIÓN FORENSE

Este capítulo trata sobre la forma de como conservar la integridad de la información utilizando varios componentes, como los bloqueadores de escritura, tanto por hardware o software, también, se utilizarán técnicas como la de hashing para verificar la integridad de la evidencia y preservación de la misma.

5.1. Bloqueadores de escritura e integridad de evidencias

La conservación de evidencias es la regla número uno en informática forense, no se debe dañar o permitir que se dañen las evidencias, ni en su estado físico, ni el contenido digital, no se debe modificar la evidencia bajo ninguna circunstancia siempre que pueda evitarse, no se debe perder la evidencia ni física, ni los datos contenidos en el soporte físico. Precisamente para no perderla en el sentido de tenerla siempre controlada, están los protocolos de trabajo y la cadena de custodia.

Para no dañar o modificar una evidencia digital aparte de las precauciones que se deben tomar para la conservación óptima del soporte físico, hay que evitar escribir datos en las memorias o unidades de disco cuando se trabajen con ellas. Al montar una unidad de disco en un sistema operativo casi con toda seguridad la unidad sufrirá la modificación de algún dato por la simple interacción con el sistema, que puede crear archivos temporales, de indexación o de formato de presentación de la información, para evitarlo se debe usar bloqueadores de escritura que son interfaces hardware o software que impiden al sistema escribir en la unidad, permitiendo por el contrario que lean su contenido.

Tipos de bloqueadores

Existen dos tipos fundamentales de bloqueadores de escritura que se detallan a continuación:

- **Bloqueadores de hardware**: Son dispositivos electrónicos que actúan como interfaz entre la computadora y el soporte físico de almacenamiento.
- **Bloqueadores basados en software**: Suelen formar parte de la suite de software forense, aunque también se puede conseguir este efecto mediante la configuración apropiada del sistema operativo.

Invalidación de evidencias

Las evidencias digitales cuya integridad no pueda ser demostrada, y aquellas cuyo daño o modificación este manifiestamente demostrado, podrán ser automáticamente invalidadas, en el primer caso porque no se puede garantizar que no haya sucedido lo segundo y en el segundo caso, el de la modificación patente, porque las conclusiones que extraiga un perito, aunque válidas parten de una fuente de datos que puede haber sido modificada, lo cual invalida los procedimientos derivados de ella.

Más soluciones

Protección física: los bloqueadores de escritura no son las únicas herramientas a disposición para la conservación de la integridad de las evidencias digitales, también se debe aplicar protección física a los soportes de información mediante el almacenamiento en condiciones apropiadas.

Cadena de custodia: implementar una cadena de custodia en la que se registre quién accede a una evidencia, cuándo y para qué.

Cálculo de hashes: calcular y conservar como parte de la cadena de custodia los hashes de la información para poder garantizar su integridad y en caso de violación de la misma, poder comprobar cuando tuvo lugar.

Una vez más se tiene en las manos un soporte de información digital original, si se genera un duplicado o una imagen valiéndose de un bloqueador de escritura para salvaguardar el original, se obtendrán copias con las que se podrá trabajar sin poner en riesgo el mencionado original, además así se puede saber que si el original sufre alguna modificación, se deberá a accesos no autorizados y se podrá tratar de poner remedio al problema de seguridad que ha derivado en esa situación.

Se debe tener siempre en mente el caso particular de los discos SSD, cuya distribución de contenidos puede variar sólo por el hecho de tener suministro eléctrico, por lo que, en estos casos, aunque se use un bloqueador de escritura, el hash del soporte original variará, aunque sí se puede garantizar que no se ha añadido ni borrado ficheros.

5.2. Bloquear escritura por software

Sin utilizar ninguna herramienta específica valiéndose de los recursos nativos de Windows, en este caso Windows 10, se puede bloquear la posibilidad de que el sistema operativo escriba en las memorias USB que se conecten a la computadora, para ello lo primero que se va a ver es cómo funciona correctamente al conectar una memoria USB.

Cuando se ha conectado a la memoria se puede ir al explorador de archivos y se puede ver que se tiene conectada la memoria con un archivo, como muestra la Figura 34.

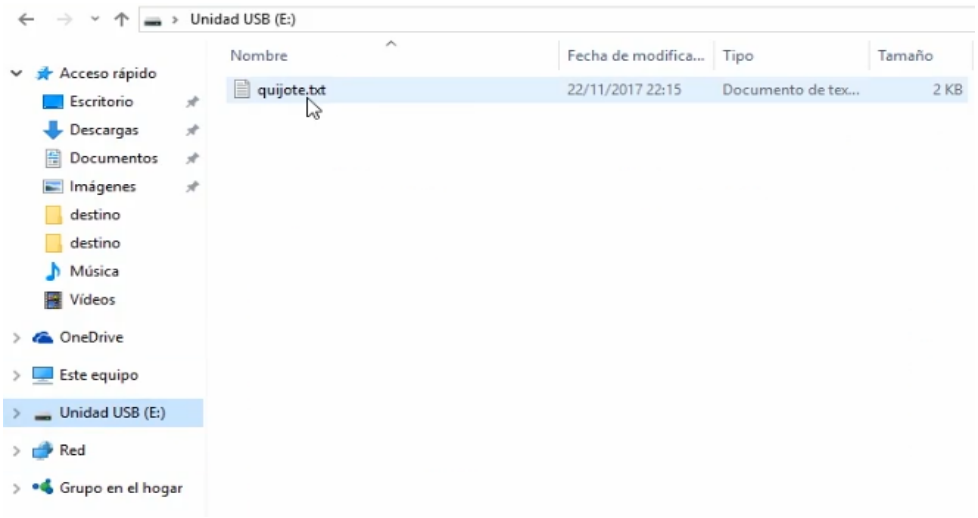


Figura 34. Verificación de archivos en el explorador de Windows.
Fuente: elaboración propia.

La figura anterior, muestra un archivo con extensión "**txt**" denominado quijote.txt, se puede editar el archivo, añadir una línea, se puede guardar, se puede crear un nuevo archivo, un documento de texto con el nombre prueba.txt, se puede abrirlo y escribir algo y guardarlo, así que se ve que el USB funciona con total normalidad.

Se puede expulsar la unidad y se va a abrir el registro de Windows con el comando REGEDIT en la pantalla de búsqueda de Windows como se muestra en la Figura 35.

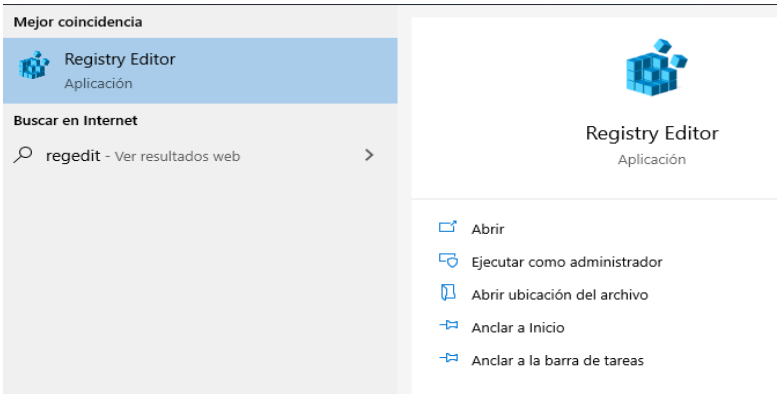


Figura 35. Ejecución del editor del registro de Windows.
Fuente: elaboración propia.

Una vez abierto el programa, lo que se va a hacer es ir al principio y encontrar el registro "**HKEY_LOCAL_MACHINE**" y se selecciona la opción "**SYSTEM**" y se abre "**CurrentControlSet**" y de ahí se abre la opción control, en esta opción se tiene que crear una clave nueva como se muestra en la Figura 36.

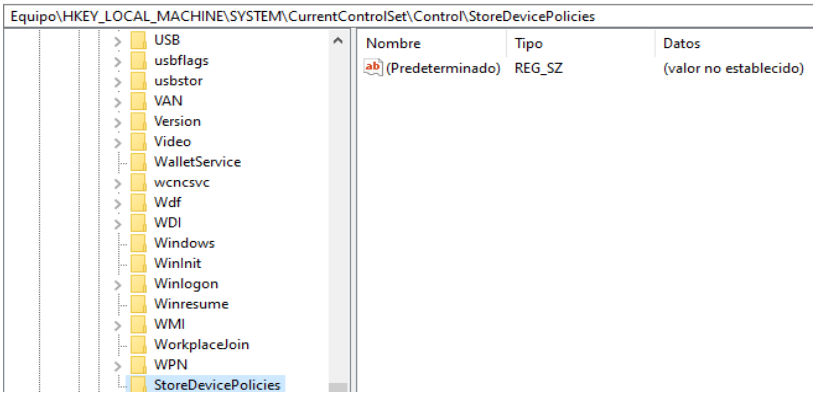


Figura 36. Búsqueda de claves en el registro de Windows.
Fuente: elaboración propia.

La figura anterior, muestra la creación de la clave que se denomina "**StoreDevicePolicies**", una vez creada se tiene que crear un elemento para esta nueva clave que son políticas de dispositivos de almacenamiento como se muestra en la Figura 37.

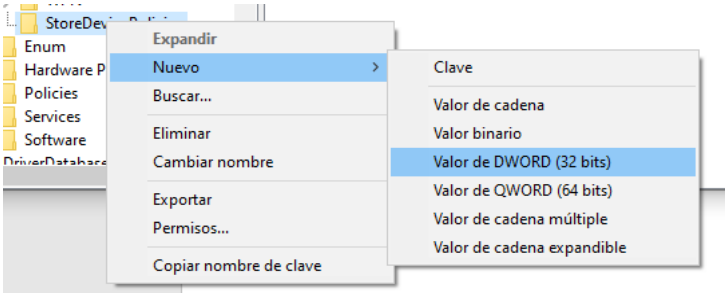


Figura 37. Creación de nueva clave en el registro de Windows.
Fuente: elaboración propia.

Una vez seleccionada la nueva clave se le dará el nombre de "**WriteProctect**" que es protección contra escritura como se muestra en la Figura 38.

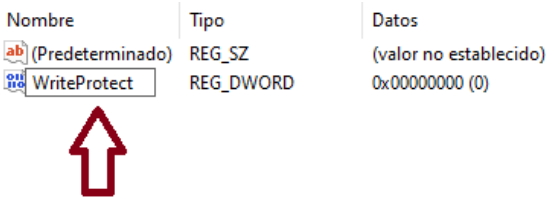


Figura 38. Protección de clave de escritura en el registro de Windows.
Fuente: elaboración propia.

Una vez creada la clave, se puede dar un doble clic sobre la opción y permite editar un valor, en este caso para activar la clave como se muestra en la Figura 39.

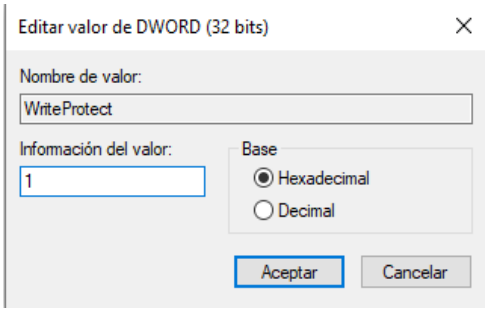


Figura 39. Establecimiento de valores en el registro de Windows.
Fuente: elaboración propia.

Una vez editado, se da clic en aceptar y se cierra el registro y para que todos estos cambios surtan efecto se debe reiniciar el equipo.

Una vez reiniciado el equipo, se puede conectar la llave USB con la memoria, una vez conectada se debe ir al explorador de archivos, se verifica la unidad y se visualiza los archivos, se puede abrir el archivo de prueba que se creó antes y si se desea modificar algún dato del contenido de los mismos se producirá un error como se muestra en la Figura 40.

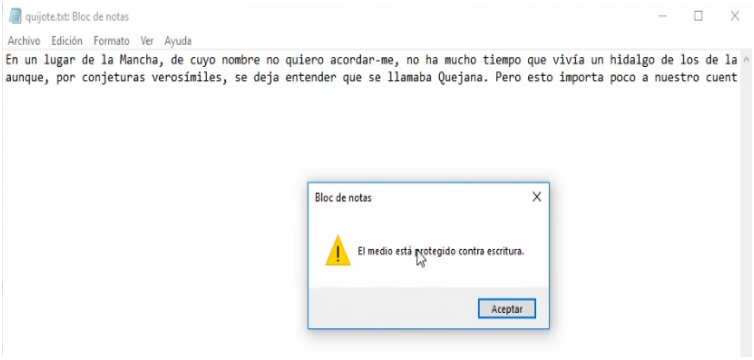


Figura 40. Verificación de la protección contra escritura del archivo.
Fuente: elaboración propia.

El mensaje de error que se muestra indica que no se tiene permisos de escritura, qué es lo que se quiere obtener para prohibir la escritura de los archivos en la llave USB, si se intenta crear un nuevo archivo, no se va a poder ya que la opción de crear archivos nuevos esta desactivada como se muestra en la Figura 41.

Figura 41. Bloqueo contra escritura en la creación de archivos en Windows.
Fuente: elaboración propia.

Esto es lo que se ha quitado al modificar el registro de Windows en "**HKEY_LOCAL_MACHINE**", esta es una forma sencilla de bloquear la escritura en memorias USB, pero no es infalible y depende de la unidad de almacenamiento que se conecte y como la reconozca el sistema operativo, así que para una emergencia es válida, si no, hay que contar siempre con bloqueadores de escritura preferiblemente en Hardware.

5.3. Bloqueadores de escritura por hardware

Cuando se necesita realizar una investigación forense y se necesita salvaguardar la información de una evidencia original y que esta no se altere, existen los llamados bloqueadores por hardware, aunque hay también los de software. Estos dispositivos tienen como objetivo principal ser un intermediario entre el ordenador y la unidad de disco, la finalidad es que solo se pueda leer la información, mas no poder escribir sobre ella, la Figura 42 muestra el funcionamiento de un bloqueador por hardware.

Figura 42. Funcionamiento bloqueador por hardware.
Fuente: elaboración propia.

Existen muchos dispositivos con interfaces sencillas para conectarse al PC, como el conocido puerto USB, por lo general tienen la apariencia de una pequeña caja donde se conectan cables de ambos lados como se muestra en la Figura 43.

Figura 43. Bloqueador de escritura por cable.
Fuente: recuperador de http://www.reydes.com/

Existen distintos modelos dependiendo del tipo de interfaz de la unidad de disco, pero lo normal es que tengan interfaces de varios tipos como:

- IDE.
- SATA.
- USB.
- Lectores de tarjetas.

También, se puede tener incluso encadenamientos que se haga, por ejemplo, conectar un lector de tarjetas estándar USB, al puerto USB GUEST del bloqueador y éste a la computadora.

Otro tipo de dispositivos son las **Docking** *Station*, estos dispositivos tienen el mismo propósito que los modelos de cable USB, pero el formato de hardware permite obtener un espacio de trabajo más ordenado y los discos en una posición más segura.

Hardware profesional

Igual que hay software especializado en análisis forense, también hay hardware especializado y los bloqueadores de escritura no son una excepción. Estos equipos se diseñan con dos ideas fundamentales en mente que se detallan a continuación:

- Minimizar riesgos, es decir evitar que el usuario se confunda.
- Cumplimiento de estandartes legales y profesionales, son más costosos, pero son más fiables y sin lugar a dudas más aceptados a la hora de presentar informes sobre las actividades realizadas con las evidencias adquiridas.

Existen múltiples fabricantes que proporcionan este tipo de tecnología, por ejemplo, Guidance Software disponible en https://www.guidancesoftware.com/ con la línea "Tableau Hardware" y el producto "Forensic Bridges" que muestra varias opciones como se visualiza en la Figura 44.

Figura 44. Bloqueadores de hardware del proveedor Guidance Software.
Fuente: recuperador de https://www.guidancesoftware.com

La figura anterior muestra varias de sus opciones, por ejemplo, el Tableau Forensic USB 3.0 Bridge, qué tiene distintas interfaces de comunicación para conecta la unidad de almacenamiento al PC. También, se tiene otros fabricantes como CRU disponible en la web en la siguiente dirección https://www.cru-inc.com/, con sus

unidades que también tienen un lado para el HOST, es decir, para el PC y otro lado en el otro extremo para no confundirse con el guest, es decir, la unidad de disco que se quiere conectar y proteger contra escritura, la Figura 45 muestra un ejemplo de este bloqueador de hardware.

Figura 45. Bloqueador USB de hardware del proveedor CRU.
Fuente: recuperador de https://www.cru-inc.com/

Existen modelos que incluyen diferentes interfaces o modelos dedicados a una interfaz dedicada, depende del fabricante y del formato del equipo que se pueda adquirir.

Clonadoras

Las clonadoras son los dispositivos más especializados en la categoría de equipos de la que se está analizando, son rápidas y eficientes no requieren de conexión a la computadora para hacer su trabajo, se conectan al disco de origen y al de destino, la clonadora copia el primero en el segundo, e incluso calcula el hash durante el proceso.

A la hora de adquirir este tipo de tecnología debe primar la practicidad y la seguridad, no es prioritario tenerlo todo, sino, tener lo necesario. Es más importante que los procesos sean seguros que la cantidad de cosas que se pueden hacer, el kit de herramientas puede ampliarse progresivamente, por lo que no es necesario comprar un equipo muy costoso que lo haga todo desde el principio.

5.4. Hashing como método de preservación de evidencias

Se puede indicar que el hashing es un instrumento en informática forense que detecta si una copia de la información es idéntica a la original. Las características fundamentales de los algoritmos de hashing aparte de entregar resultados, es que se puede convertir en un proceso irreversible, es decir, que no se pueden obtener los

datos de origen si se parte de los cálculos del hash. Si el archivo origen sufre algún cambio ya sea por accidente o de forma deliberada el hash cambiará totalmente y se sabrá que no es igual al archivo original.

Garantía forense

Si se trabaja siempre con copias cuyo hash equivale al de la evidencia original, se sabrá que los datos son iguales y por tanto los procedimientos son válidos y reproducibles, por lo tanto, cualquier herramienta profesional para informática forense debe poder calcular hashes.

Para comprobar cómo se puede utilizar un verificador de hashes nativo de Windows, se va a utilizar una herramienta nativa de Microsoft que se llama "**File Checksum Integrity Verifier Utility**", la cual está disponible en la web de soporte de Microsoft en la siguiente dirección https://www.microsoft.com/en-us/download/details.aspx?id=11533, como se muestra en la figura 46.

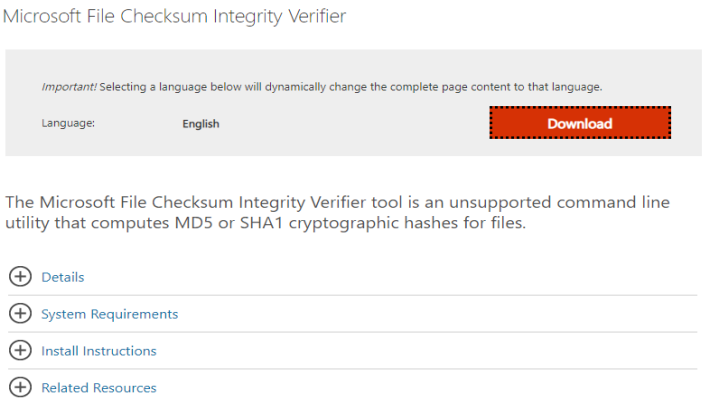


Figura 46. Herramienta de verificación de hashes de Microsoft.
Fuente: recuperado de https://www.microsoft.com/

Una vez descargado el archivo, se lo va a guardar en el disco "C ", y se puede crear una nueva carpeta que se va a llamar FCIV, dentro de esta carpeta se procede a ejecutar el programa para la instalación y para esto pide una ruta de una determinada carpeta donde debe descomprimir los archivos como muestra la Figura 47.

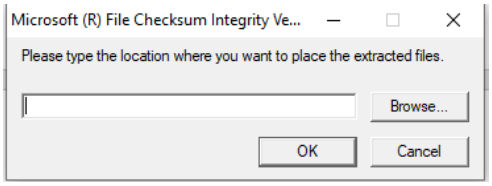


Figura 47. Instalación de la herramienta de verificación de hashes de Microsoft.
Fuente: elaboración propia.

Una vez completado el proceso se tiene un archivo de lectura un archivo de lectura y el "**fciv.exe**", para ejecutarlo se va a hacer la prueba de forma sencilla, copiando un archivo de texto en el mismo directorio, también se puede agregar el programa a las variables de entorno del sistema.

Para abrir el comando, se puede ir a la ventana de consola y abrir la carpeta donde fue copiado y se puede ver las diferentes opciones como se muestra en la Figura 48.

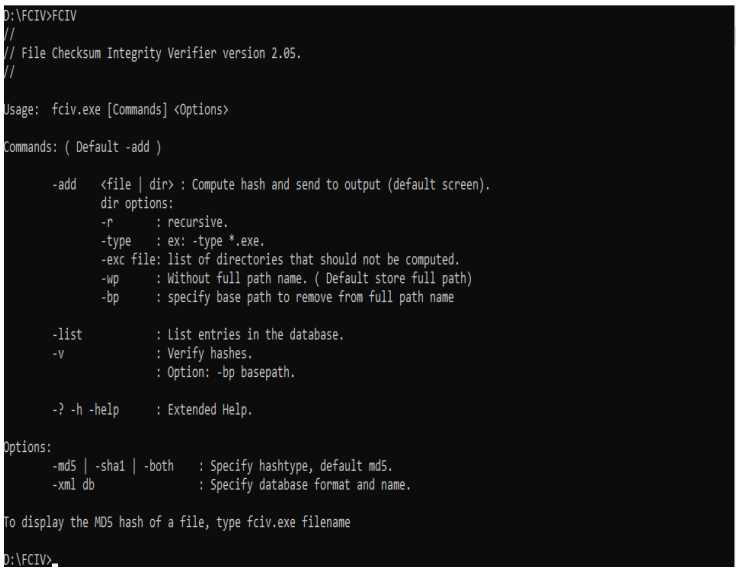


Figura 48. Ejecución del programa Fciv.exe.
Fuente: elaboración propia.

En la figura anterior, se puede ver las distintas opciones, permite hacer búsquedas recursivas calculando hashes, permite verificar le si le indica hacer con lo que comparar, por ejemplo, se puede calcular el hash por ejemplo "**sha1**" del archivo del primer párrafo del archivo prueba.txt con la siguiente línea de comando:

- fciv-sha1 prueba.txt

La línea de comando anterior muestra la versión del programa que se está utilizando y el hash indicado como se muestra en la Figura 49.

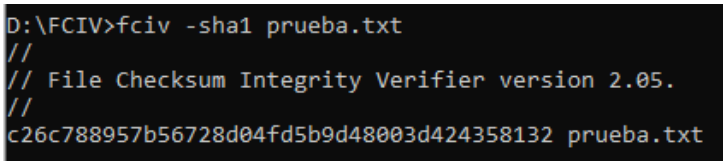


Figura 49. Verificación de la versión del algoritmo del programa Fciv.exe.
Fuente: elaboración propia.

Si se modifica el archivo y se edita algo dentro del mismo, y si se ejecuta nuevamente el comando se verifica que el hash ha cambiado como se muestra en la Figura 50.

Figura 50. Cambio del hash con Fciv.exe.
Fuente: elaboración propia.

Este programa permite verificar si cualquier archivo ha sido alterado, así solo se le ubique un solo carácter en el contenido del mismo.

5.5. Algoritmos de hashing

Existen distintos algoritmos de tipo hash, entre los más conocidos se tienen a los siguientes:

5.5.1. MD5

Según Mena (2009) MD5 es un algoritmo desarrollado en el año 1991 por Ronald Rivest del MIT, este algoritmo ha sido muy popular por su velocidad, pero desde sus comienzos inició con algunos fallos en su diseño.

Este algoritmo funciona formando bloques y encadenando resúmenes, en el mensaje se agrupa en bloques de 512 bits con 16 palabras de 32 bits, para completar el último bloque de 512 bits se aplicará un relleno de un '1' seguido de tantos '0' como **haga falta**, reservando los últimos 64 bits para indicar el tamaño del mensaje o archivo, por ejemplo, la palabra de 32 bits "**Amor**", que en hexadecimal es "**0x416D6F72**" se leerá "**726F6D41**", como se muestra en la Figura 51.

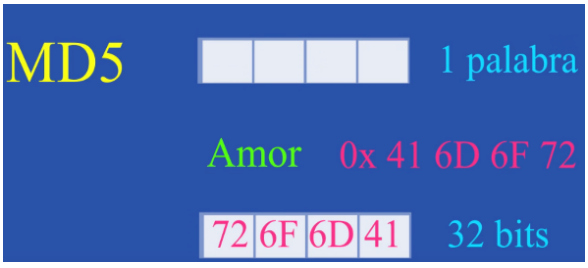


Figura 51. Utilización del algoritmo MD5.
Fuente: elaboración propia.

5.5.2. SHA

Según Yerko (2009), SHA, corresponde a las siglas de Secure Hash Algorithm o algoritmo seguro de hashing, el cual indica que se crea un numero basado en el contenido de un grupo de bits, es un algoritmo más seguro en relación al MD5 que llega hasta los 512 bits. Este algoritmo también tiene vulnerabilidades, uno de ellos es el llamado "ataque de cumpleaños", el cual consiste en una paradoja para encontrar a un par de personas con el mismo día de cumpleaños, la figura 52 muestra el funcionamiento de SHA, al igual que MD5 tiene 512 bits y aplica rellenos para completar el mensaje.

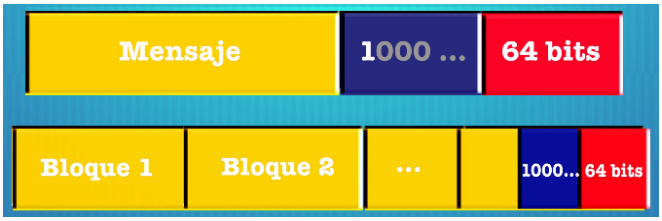


Figura 52. Algoritmo SHA.
Fuente: elaboración propia.

Cuando se elige a un algoritmo, se debe verificar el grado de vulnerabilidad que este va a tener, por lo general determinar el grado de colisiones que estos pueden tener, por ejemplo, una fotografía y una versión modificada de esa misma fotografía generen el mismo hash, esto sería un problema porque no se podría distinguir mediante el hash cual es el original y cuál la copia.

Actualmente se han encontrado colisiones en md5 y sha1, así que siempre es más aconsejable usar algoritmos con resúmenes de mayor longitud, cuanto mayor sea la longitud del hash, menos probabilidades hay de que existan colisiones, pero más cuesta calcularlo y eso se traduce en tiempo que se debe tener ocupado un recurso para calcular ese hash. Cuando es un archivo no es relevante, pero si son miles de archivos o un disco duro completo, entonces puede llevar horas.

Una alternativa que utilizan algunos profesionales es calcular el hash md5 y sha1 de una misma evidencia, ambos son potencialmente débiles, pero es probabilísticamente descartable que ambos algoritmos puedan colisionar con la misma fuente de datos, así que este es un truco que puede usarse si el cálculo de un sha2 o 3 tarda más que la suma del tiempo de calcular md5 y sha1.

5.6. Hashing en herramientas de informática forense

Muchas herramientas de software forenses actuales incluyen funcionalidades de hash, incluso las clonadoras profesionales lo calculan y verifican. El objetivo es validar y verificar las copias de las evidencias, entre estas herramientas se puede encontrar para calcular hashes de imágenes de discos a una de las más usadas Qué es FTK Imager, se trata de una herramienta comercial, aunque de distribución gratuita de la empresa Access Data, pero es muy popular, además de esto existen otras muchas herramientas tanto comerciales, como Open Source, incluso se dispone de herramientas nativas que pueden resolver esta tarea en distintos sistemas operativos.

En Windows se tiene la herramienta PowerShell, ya que originalmente no hay herramientas nativamente instaladas. En PowerShell se tiene el comando "**Get-Filehash**", también existe la herramienta de Microsoft "**File Integrity Check Value**" que se puede descargar de la plataforma de Microsoft.

En Linux se tiene a las herramientas "**md5sum**" o "**sha1sum**" y en MacOS se puede usar comandos "**md5**" o "**shasum**".

En Windows 10 se puede a ir a la web de Access Data, a la zona de descargas y descargar la herramienta FTK Imager, para esto se debe ir al link https://accessdata.com/product-download y proceder a la descarga como muestra la Figura 53.

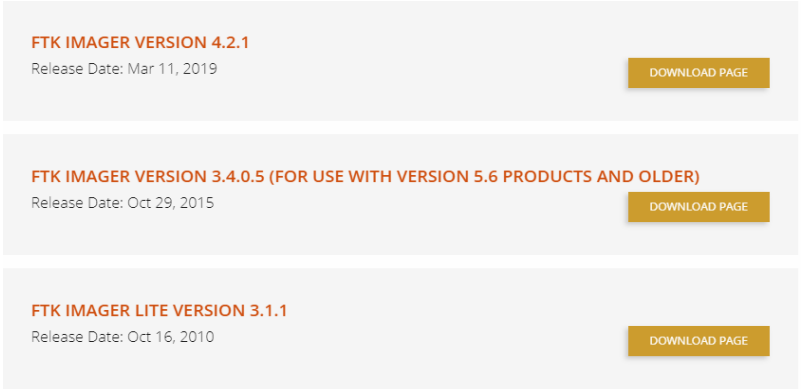


Figura 53. Descarga de la herramienta FTK IMAGER.
Fuente: recuperado de https://accessdata.com/

Una vez descargado el programa se procede a la instalación como se muestra en la Figura 54.

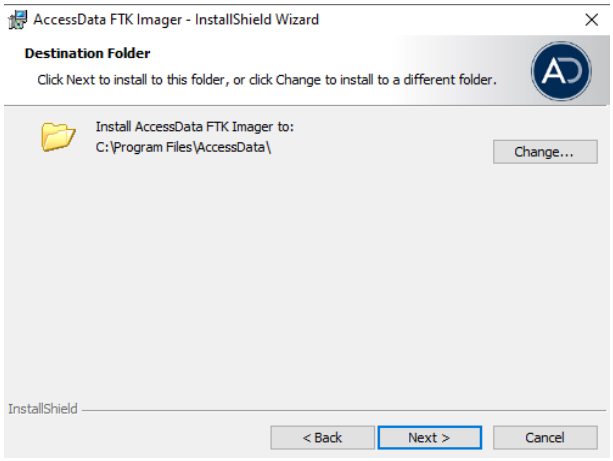


Figura 54. Instalación de FTK Imager en Windows.
Fuente: elaboración propia.

Una vez instalada la herramienta se procede a abrirla y se puede probar el funcionamiento, en el escritorio del PC se tiene la imagen de una memoria USB como se muestra en la Figura 55.

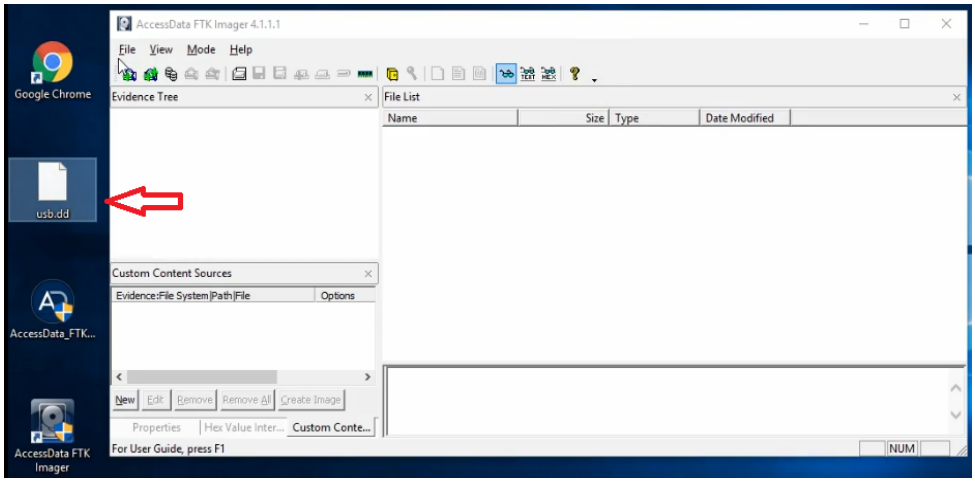


Figura 55. Verificación de los archivos en FTK Imager en Windows.
Fuente: elaboración propia.

Se puede ir a la opción “File”, “Add Evidence Item”, para agregar una imagen, se indica el origen de esa imagen y se termina haciendo clic como se muestra en la Figura 56.

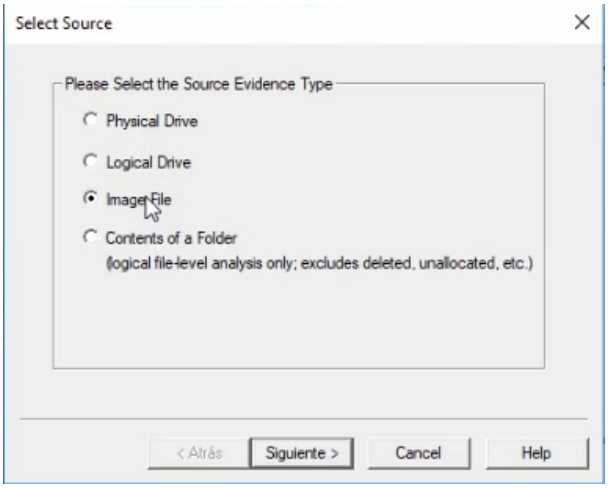


Figura 56. Agregación de una imagen USB en FTK Imager.
Fuente: elaboración propia.

Si se hace clic derecho sobre la imagen, se podrá verificar y calculará el hash como muestra la Figura 57.

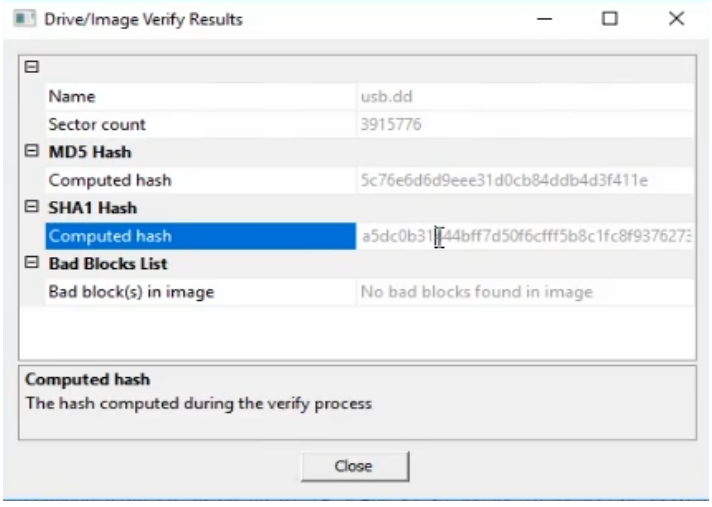


Figura 57. Cálculo del Hash con FTK Imager.
Fuente: elaboración propia.

En el caso de la figura anterior, da como resultado el md5 y sha1 y aquí se visualizan los valores para proceder a cerrar. También, se puede añadir una nueva evidencia, en este caso una evidencia física como una memoria USB conectada al computador y se puede verificar el hash como se muestra en la Figura 58.

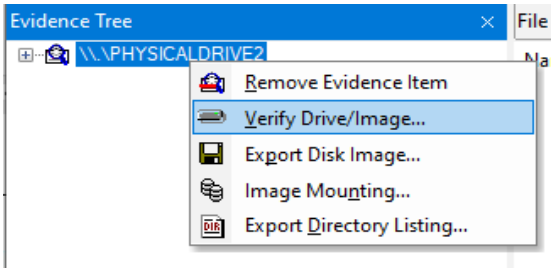


Figura 58. Verificación de un hash en una unidad física.
Fuente: elaboración propia.

Otra opción que se puede utilizar para calcular el hash es PowerShell que es un programa tipo modo consola como se muestra en la Figura 59.

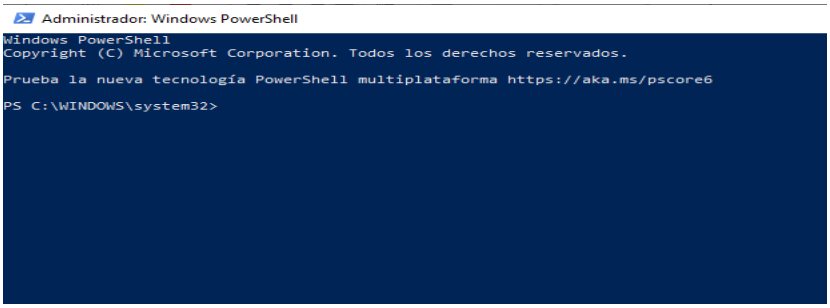


Figura 59. Cálculo de hashes con PowerShell.
Fuente: elaboración propia.

Se puede realizar una verificación de hash de un determinado archivo tipeando un comando y mostrará el resultado con el tipo de algoritmo indicado como se muestra en la Figura 60.

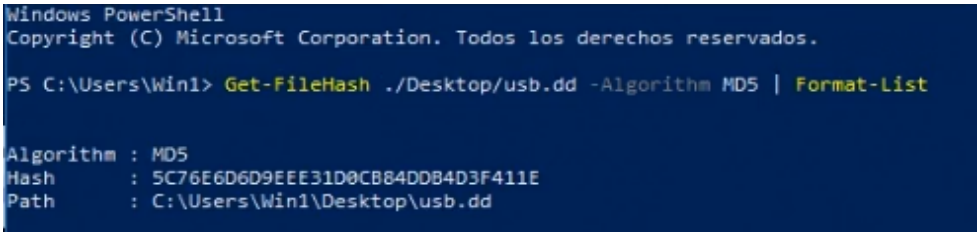


Figura 60. Resultado del cálculo del hash con PowerShell.
Fuente: elaboración propia.

5.7. Entender el montaje de unidades en Linux

Se va a explicar en qué consiste el proceso de montar o desmontar una partición en Linux. Montar o Mount en inglés es el proceso que se realiza para que, al conectar una unidad de almacenamiento a una computadora, el sistema operativo puede reconocer sus particiones y por lo tanto, pueda acceder a leer o escribir archivos.

Desmontar es lo contrario, es desvincular la partición del sistema operativo de forma que no pueda ser leída y escrita. Por lo general los sistemas operativos actuales montan o desmontan automáticamente las particiones de las unidades físicas que se conectan, pero en informática forense eso no es lo más conveniente y por eso se está repasando estos conceptos.

El término de montar se usa principalmente en entornos y UNIX especialmente Linux y en base a la arquitectura Linux, se desarrollará la explicación. El punto de montaje es el directorio de la estructura de archivos del sistema operativo que se asocia a una partición concreta, es decir, que desde el punto de vista del sistema la partición contenida, por ejemplo, en una memoria USB es un directorio, aunque al usuario se le pueda representar de una forma más amigable y accesible.

Cuando se accede a los subdirectorios de ese punto de montaje, se está accediendo a los directorios y archivos contenidos en la partición que se ha montado.

En el sistema operativo Ubuntu, se puede abrir un terminal y después se va a conectar una memoria USB al sistema. Ubuntu es un sistema operativo para usuarios y al conectar la memoria USB directamente se abrirá un explorador de archivos y se monta la unidad como se muestra en la Figura 61.

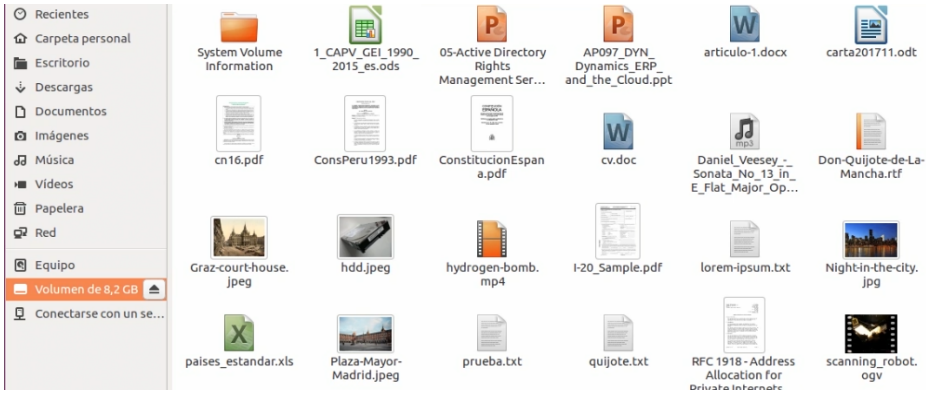


Figura 61. Montaje de unidades USB en Ubuntu.
Fuente: elaboración propia.

Se tiene que ir al terminal y ejecutar El comando "**sudo fdisk -l**" para hacerlo como administrador, con ese comando se va a ver la lista de unidades y se visualiza que se tiene dos grupos como se muestra en la Figura 62.

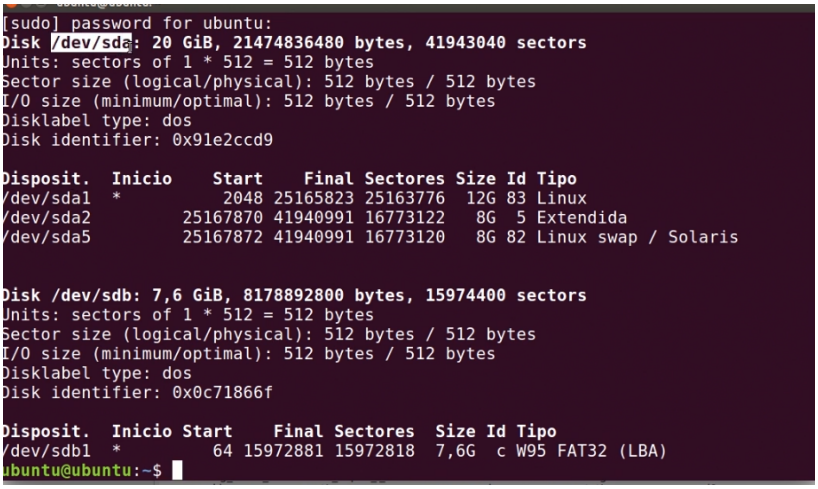


Figura 62. Visualización de unidades de montaje como administrador en Ubuntu.
Fuente: elaboración propia.

En la figura anterior, se visualiza el grupo "/**dev/sda**" que tiene 20 gigas y el grupo "**dev/sdb**" de 7,6 gigas. El primer grupo es el correspondiente al disco sobre el que está instalado el sistema operativo, se tiene la partición extendida y el Swap para intercambio de información y la unidad USB que corresponde sdb que tiene 7,6, si se quiere desmontar esta unidad se ejecuta el comando "**umount/dev/sdbl**", esta es la unidad física que se ha conectado y sdb1 es la partición concreta, en este caso, es un disco que tiene una única partición, se ejecuta el comando y la unidad estará desmontada. Para comprobar que la unidad se desmontó, se vuelve a tipear el comando y saldrá un mensaje indicando que la unidad no existe como se muestra en la Figura 63.

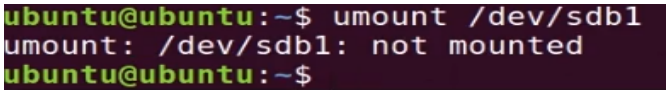


Figura 63. Desmontaje de unidades USB en Ubuntu.
Fuente: elaboración propia.

CAPÍTULO VI: RECOLECCIÓN DE EVIDENCIAS

En este capítulo se analiza la forma de cómo se deben recolectar las evidencias, desde la utilización de diferentes protocolos, la forma de almacenarlas, los diferentes métodos de ocultación de la información, como se debe proceder para recuperar información borrada, recuperar datos de navegación a través de los navegadores web y por último, recuperar información a través de Smartphone.

6.1. Protocolo de recolección de evidencias

La recolección de evidencias es uno de los pasos fundamentales para todo proceso relacionado con una investigación forense, la cual puede ser dividida en 4 componentes principales que son:

- Identificación de las evidencias.
- Aseguramiento de las evidencias, para evitar posibles daños.
- Documentación de las evidencias.
- Control de la evidencia a través de una cadena de custodia.

Existen varias formas para tomar evidencias, uno de estos casos, es cuando se encuentra la computadora apagada, para ello se deben tomar varios procedimientos en cuenta como fotografiar la escena, haciendo constancia de cómo se encontró el equipo, en este caso, apagado. En el caso de estar apagado se deben desconectar los cables de energía y en el caso de equipos portátiles, se procede a retirar la batería, se deben prestar atención a todos los detalles, documentarlas y en el caso de conexiones de red, estas deben ser analizadas, con todo esto, ahora se procede a iniciar el proceso de recolección de las evidencias, empezando por obtener una imagen o clonado de su disco duro, la Figura 64 muestra el flujo del proceso de protocolo para recolectar evidencias

Figura 64. Flujo de los procesos para recolectar evidencias en equipos apagados.
Fuente: elaboración propia.

En una computadora encendida, se fotografía la escena y el equipo, se genera una imagen de la información volátil, incluyendo memoria RAM, archivos temporales, cachés, etc., si se ha aplicado cifrado a los discos, se debe generar imágenes de los mismos antes de apagar o al menos, obtener copia de los archivos, aunque esto no es lo ideal, por último, apagar el equipo y continuar como con un equipo apagado, la Figura 65 muestra el flujo de procesos de un equipo encendido para la recolección de evidencias.

Figura 65. Flujo de los procesos para recolectar evidencias en equipos encendidos.
Fuente: elaboración propia.

Guardar todas las evidencias en bolsas antiestáticas y empaquetarlas de forma segura con su correspondiente numeración, y antes de terminar de empaquetar las evidencias, no olvidar Identificar, documentar y almacenar, manuales, guías notas y demás información que pueda ser relevante respecto a los equipos recolectados, estos pueden ser de utilidad para la fase de análisis de las evidencias.

6.1.1. Orden de volatilidad

Los datos disponibles en una computadora tienen distintos niveles de volatilidad, es decir, cuanto más tiempo pase, más probabilidades hay de que dejen de estar disponibles o de ser útiles, por eso, se extraen en función de la necesidad en un orden concreto de mayor a menor volatilidad.

En primer lugar, está la CPU, la memoria caché y el contenido del registro, a continuación, las tablas de enrutamiento, la cache ARP, la tabla de procesos y las estadísticas del kernel. En tercer lugar, se tiene la memoria RAM, en cuarto los ficheros temporales y el espacio de intercambio. A continuación, los datos almacenados en discos duros, después, los datos almacenados en recursos remotos como servicios en la nube, y, por último, los servicios digitales externos que se encuentren desconectados.

Este orden de volatilidad puede variar en función de distintas tecnologías y con el paso del tiempo, por lo que es interesante mantener una idea general, pero también, adaptarse a las circunstancias, siempre documentando el cómo y el porqué de las decisiones y acciones y obviamente, también el método de adquisición de esa información volátil,

6.2. Almacenamiento de evidencias

El almacenamiento de evidencias digitales, es una tarea no sólo de índole práctica, también de responsabilidad, un investigador forense requiere de gran cantidad de almacenamiento para conservar evidencias de todo tipo durante el tiempo que dure su trabajo y posteriormente hasta que el caso sea cerrado, además, debe proporcionar todas las medidas de seguridad a su alcance para evitar que dicha información sea corrompida o peor filtrada, sobre todo, si se trata de información de otras personas o empresas.

A la hora de trabajar con información almacenada, se debe tomar una serie de precauciones, para empezar, se debe implementar un inventario de todo lo que se tiene almacenado para poder localizarlo fácilmente cuando se lo necesite.

En cuanto a la seguridad física, se debe almacenar las evidencias en lugares de acceso restringido y de ser posible con control ambiental, sobre todo de humedad. Se debe operar con protección contra picos de corriente o cortes de luz, para lo cual, se puede utilizar sistemas de alimentación ininterrumpida, se debe mantener un ambiente limpio y estable y evitar polvo, corrosión, vibraciones, etc.

Los dispositivos de almacenamiento con soporte magnético o electrónico deben embolsarse individualmente con aislamiento antiestático, cuando se trata de trabajar con dispositivos móviles, se debe atender a las características intrínsecas de su tecnología, para empezar, se debe almacenarlos en jaulas de Faraday para bloquear las comunicaciones radioeléctricas, existen bolsas destinadas a este propósito.

Si hay que conservar el dispositivo encendido, se pueden usar packs de baterías para evitar que se descarguen, aunque se debe tener en cuenta que el teléfono registra a esa carga modificando la evidencia, así que, hay que explicar y documentar esta operación, si se usan pack de baterías deben estar dentro de la bolsa de aislamiento, o el cable podría hacer efecto antena e inutilizar el efecto de La jaula de Faraday.

También, se debe proceder salvaguardando la información volátil, antes que nada, además, si el teléfono está desbloqueado se debe mantenerlo así, o intentar conseguir el código de seguridad y, por último, no se debe olvidar que muchos modelos de teléfono pueden tener tarjetas de memoria extraíbles.

La forma en que se protege las evidencias que se recolectan puede definir la fiabilidad que dicha evidencia tenga en una investigación, una protección inadecuada puede invalidar una evidencia.

Por último, se debe mantener cierto control sobre la integridad del almacenamiento de evidencias digitales, en caso de corrupción de datos en un sistema de almacenamiento de evidencias, se tiene que ser capaces de ofrecer ciertas garantías, la corrupción debe estar acotada y no puede afectar a otras evidencias.

El incidente debe ser identificable, es decir, que se tiene que ser capaces de detectarlo y esto se consigue normalmente mediante el cálculo de hashes durante la adquisición y la verificación a posteriori, si no coinciden, la copia a sufrido cambios.

Si una sección de información está corrupta, un sistema de almacenamiento compartimentado permitiría aislar esa parte o fragmento de información garantizando la integridad del resto, cuyo procesador siendo totalmente válido y fiable.

6.3. Copias forenses

Uno de los trabajos más comunes en informática forense, es la generación de evidencias para la resolución de casos, con el objeto de preservar la evidencia original. Pues se recomienda, nunca trabajar con las evidencias originales que pueden ser:

- Discos duros.
- Memorias USB.

En el caso de tomar en vivo evidencias, por ejemplo, volcados de memoria, en estos casos, no queda más alternativa que hacerlo de esta manera, pero lo ideal es respaldar el original y trabajar con los duplicados.

Existen varios mecanismos para generar copias sobre evidencias forenses, que se mencionan a continuación.

Uno de los métodos más utilizados es el clonado de discos, cuyo objetivo es generar una copia en físico de un disco en otro, esta copia es de bit a bit.

En el caso de este tipo de duplicado, la desventaja es que el proceso debe cumplir ciertos requerimientos técnicos como que el disco destino debe tener ciertos parámetros como la escritura con ceros antes de realizar la copia, incluso, aunque sea una unidad recién comprada, porque puede traer datos del fabricante o ser reacondicionado. La segunda condición, es que el disco debe ser preferiblemente de las mismas características que el original, es decir, marca, modelo, capacidad. Esto es lo que ayuda a garantizar que, al copiar todos los bits de la evidencia original en el disco de destino, este será un duplicado perfecto del primero.

El segundo método más eficiente y práctico, es la generación de imágenes, que consiste en generar un archivo que contenga toda la información de la evidencia original bit a bit, la diferencia principal es que al ser un archivo se puede guardarlo en cualquier soporte y sacar tantas copias del mismo como se necesite, incluso se puede pasar de la imagen a un disco si fuese necesario.

La desventaja es que el soporte en que se almacene la imagen tiene que ser de tamaño superior al disco de origen, aunque ya existen formatos de imagen que permiten compresión, e incluso, se puede fraccionar las imágenes en varios archivos.

Para hacer copias forenses, se tiene que seleccionar las herramientas apropiadas teniendo en cuenta que, debe poder hacer copias bit a bit, debe proteger el soporte original contra escritura conservándolo inalterado, debe poder calcular hashes de discos e imágenes para garantizar la integridad de las copias, debe documentar mediante registros los errores de lectura y escritura que puedan suceder durante el proceso de copia y por último, se debe generar un reporte del proceso.

Como se ha indicado, cualquier buena herramienta de clonado o generación de imágenes calculará el hash del disco o imagen para verificar que la copia es perfecta. Se usa el hashing porque modificar un único bit, causará que el nuevo hash sea totalmente distinto al anterior, por lo que se puede detectar fácilmente las modificaciones.

Disponiendo de los algoritmos de hash, lo correcto es calcular el hash del disco original y de las copias, esto permite validar las copias en el momento, de hecho, es común que la generación de la primera imagen o clonado se haga ante notario, para que deje constancia del hash resultante y así poder garantizar a posteriori que cualquier copia que tenga ese mismo hash, es una copia perfecta del original.

6.3.1. Discos SSD

Los discos SSD no funcionan igual que los discos HDD o mecánicos, lo cual conlleva una serie de condicionantes a la hora de hacer copias forenses. Los discos SSD continuamente seleccionan nuevos sectores de escritura, descartan sectores dañados o imprecisos para almacenar un 1 o 0 y por tanto, sólo con tener suministro eléctrico cambian.

Si se calcula varias veces el hash de un disco SSD, normalmente dará varios valores distintos, aunque no se haya modificado, añadido o borrado archivos, por lo tanto, la evidencia original cambia haciendo casi imposible que su clonado genere el mismo hash, por eso, se recurre a la generación de imágenes, en lugar de al clonado, o si se prefiere a un clonado en disco mecánico para que dicha primera copia permanezca inalterable. En los casos en que se trabaje con discos de estado sólido, esa primera copia o clon será la evidencia sobre la que se tendrá que trabajar la que conservará siempre el mismo hash, lo cual no implica que se deba desatenderse del soporte físico original, el cual se debe conservar puesto que es la evidencia física original.

6.4. Métodos de ocultación de información

Como métodos de ocultación de información, se puede analizar un par de ejemplos de técnicas que pueden usar personas o aplicaciones maliciosas para ocultar información, esta ocultación puede ser por motivos de seguridad para evitar el filtrar información de forma sigilosa o para cualquier otra cosa, buena o mala que se pueda ocurrir.

La técnica fundamental es el cifrado, también conocido como encriptación, consiste en transformar información mediante un algoritmo y una clave, para que el resultado sea incomprensible para quien accede a él, muchas empresas y sobre todo instituciones gubernamentales de muchos países hacen obligatorio el uso de cifrado en sus equipos.

6.4.1. Herramientas de cifrado

La mayor parte de los sistemas operativos incluyen herramientas de cifrado, en Windows se tiene BitLocker, en MacOS FileVault y en Linux se puede elegir cifrar los directorios de usuario durante el proceso de instalación del sistema. Pero existen muchas otras herramientas libres y comerciales que se pueden utilizar para cifrar discos, memorias, archivos concretos y lo que se ocurra.

Otro modelo de ocultación de información es la estenografía, proviene del griego esteranos, que significa oculto y grafía que proviene del latín y puede traducirse como escritura o campo de estudio, por lo tanto, la esteganografía consiste en escribir mensajes ocultos, técnicamente en ocultar información dentro de otros conjuntos de información, de forma, que pase desapercibida.

Se podría decir que es algo así como un camuflaje, en esteganografía se tienen dos elementos claven que son:

- El contenedor.
- El contenido.

El contenedor es la información abierta, la que se puede llamar normal y que se usará para camuflar otra información, esa otra información, la que se quiere mantener oculta es el contenido, la idea es que sí se transmite el mensaje contenedor y éste es capturado, el contenido siga oculto a los ojos de quien lo haya interceptado.

Los contenedores más habituales son archivos fotográficos, de audio o de video, porque se trata de información multimedia bastante variable y difícilmente procesable si se observa la información con editores de texto o hexadecimales. Si se intentase ocultar la información en archivos de texto, hojas de cálculo o similar, la modificación del contenedor sería bastante evidente y podría inducir a pensar que hay algo oculto, aunque hay soluciones muy imaginativas como incluir espacios y tabulaciones al final de párrafos, información que no corrompe el archivo ni es visible con el editor convencional.

Existen múltiples aplicaciones para diferentes sistemas operativos destacando, por ejemplo, Openpuff en Windows 10, cuya interfaz principal se muestra en la Figura 66.

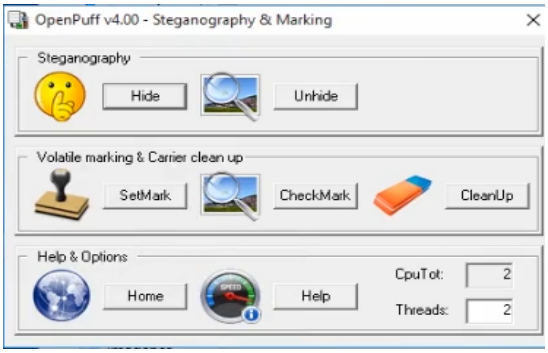


Figura 66. Interfaz principal del programa OpenPuff.
Fuente: elaboración propia.

Se puede agregar un archivo con información que se quiere ocultar, por ejemplo, si se trata sólo del primer párrafo el cual se puede verlo representado en la Figura 67.

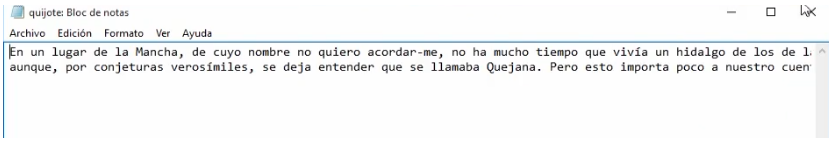


Figura 67. Archivo de muestra para ocultar la información.
Fuente: elaboración propia.

Para hacer las veces de contenedor se puede utilizar una fotografía para ocultar la información del archivo que se seleccione, en este caso, se llama Quijote.txt, abierta la aplicación se puede seleccionar la opción de ocultar o Hide, como se muestra en la Figura 68.

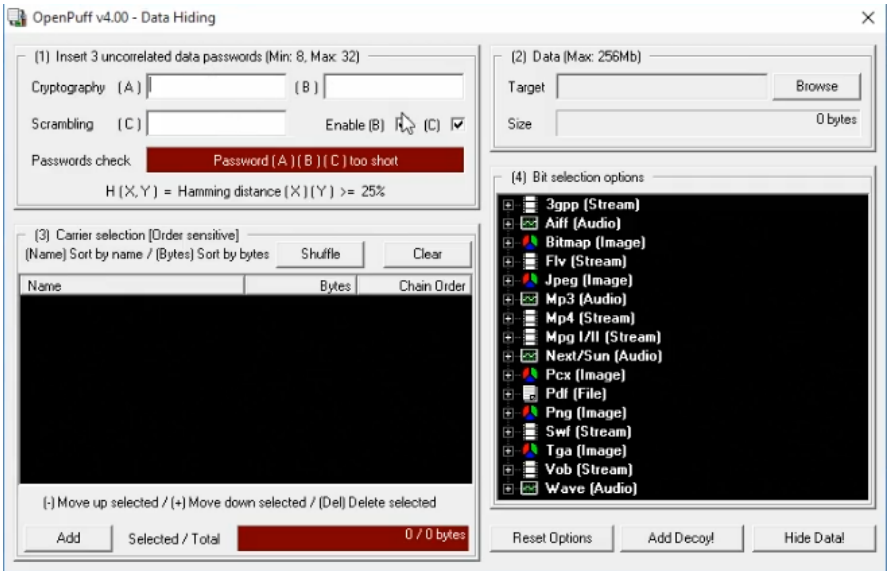


Figura 68. Opción de ocultar la información en OpenPuff.
Fuente: elaboración propia.

Se tiene que indicar una contraseña para cada nivel, si se quiere aplicar los tres niveles de cifrado aparte de la esteganografía que ofrece la aplicación, entonces, se indica la contraseña y esteganografía, después, se selecciona la información que se quiere ocultar, qué es el archivo del Quijote.txt y la fotografía en la que se quiere ocultarla, el método de estenografía será para un archivo jpg o png, se selecciona esta opción y se indica que oculte la información.

Se pude guardarla en cualquier parte, por ejemplo, en el escritorio en la carpeta destino, se acepta y cuando termina el proceso se muestra el resumen como se muestra en la Figura 69.

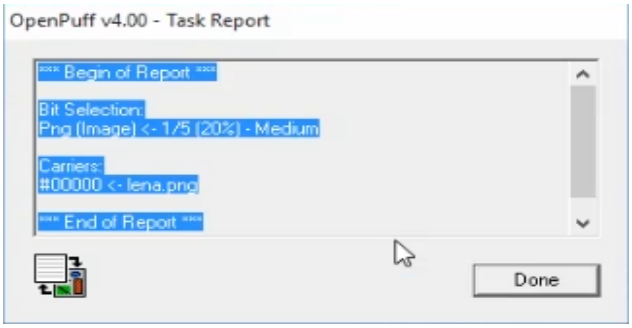


Figura 69. Resultado de ocultar la información en OpenPuff.
Fuente: elaboración propia.

Como resultado en la carpeta de destino, se tiene la fotografía y se procede a cambiarle el nombre para diferenciarla de la original.

Si se desea ver el contenido de la información oculta, se puede volver a la aplicación OpenPuff y se puede realizar el proceso inverso, es decir, extraer el contenido que hay en la fotografía, para ellos se da clic en el botón Unhide de la aplicación como se muestra en la Figura 70.

Figura 70. Resultado inverso para mostrar la información en OpenPuff.
Fuente: elaboración propia.

La fotografía es el contenedor, se selecciona la misma en la carpeta, se le indica la contraseña y esteganografía y a la misma carpeta destino se puede guardar el contenido, una vez completado el proceso, muestra el resumen del proceso y si visualiza al directorio, se tiene nuevo el archivo del Quijote.txt, que se puede abrir Word y se puede constatar que no se ha perdido nada de información como muestra la Figura 71.

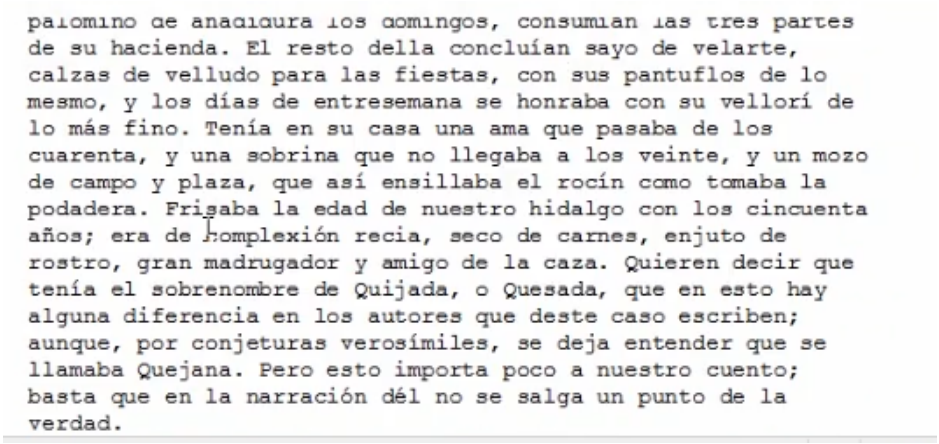


Figura 71. Verificación de la información ocultada en OpenPuff.
Fuente: elaboración propia.

6.5. Recuperar información borrada

Los procesos de recuperación de archivos borrados se realizan en base al tipo de archivo, mediante una técnica conocida como Carving. Los sistemas de almacenamiento de archivo de antiguas versiones de Windows eran FAT o File Allocation Table, al borrar un archivo el índice de FAT marca como disponibles los clústeres de memoria donde se aloja el archivo, pudiendo sobrescribirse, pero no los borra por defecto.

Lo que permite a un software de recuperación es localizar clúster que hayan sido marcados como liberados, pero que aún no se hayan sobrescrito, y así, poder reconstruir ficheros.

Para hacer búsquedas en estos sistemas, se establecen dos premisas del propio protocolo FAT que son:

- El tamaño de los clústeres es fijo.
- Nunca hay más de un archivo en un clúster, aunque sobren sectores libres en el mismo.

6.5.1. Carving en NTFS

Las versiones más modernas de Windows usan el sistema de archivos NTFS o New Technology File System, los archivos almacenados en NTFS tienen un "**Flag**" en el MFT o tabla maestra de ficheros que indica si están activos o inactivos. Al borrar un fichero se marca como inactivo, pero los clústeres que ocupa no se borran y, de hecho, siguen indexados en la MFT.

En Windows 10 y se puede utilizar una herramienta comercial para hacer Carving, en este caso, se utilizará WinUndelete, cuya dirección de descarga se encuentra en https://www.winundelete.com/ y se puede descargar una versión de prueba, la página principal de esta herramienta se muestra en la Figura 72.

Figura 72. Herramienta de recuperación de archivos WinUndelete.
Fuente: recuperado de https://www.winundelete.com/.

En la figura anterior, se puede utilizar la versión de prueba y se descarga la versión ejecutable como muestra la Figura 73.

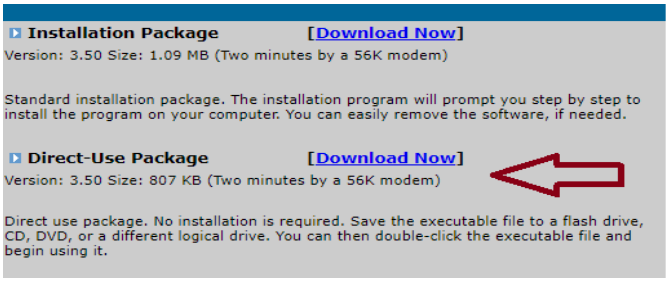


Figura 73. Descarga de la versión ejecutable de la herramienta WinUndelete.
Fuente: recuperado de https://www.winundelete.com/.

Se puede mover el archivo descargado al escritorio, para la recuperación se tiene que crear una carpeta qué será llamada "**Destino**", al utilizar la versión de prueba no va a recargar los archivos completos, pero se necesita, aun así, la carpeta.

Se puede conectar una unidad USB al equipo, y lo primero que se quiere comprobar es verificar si hay otros ficheros que se han borrado con anterioridad, se ejecuta la aplicación, la cual solicitará permiso de administración y automáticamente inicia el proceso de configuración, como se muestra en la Figura 74.

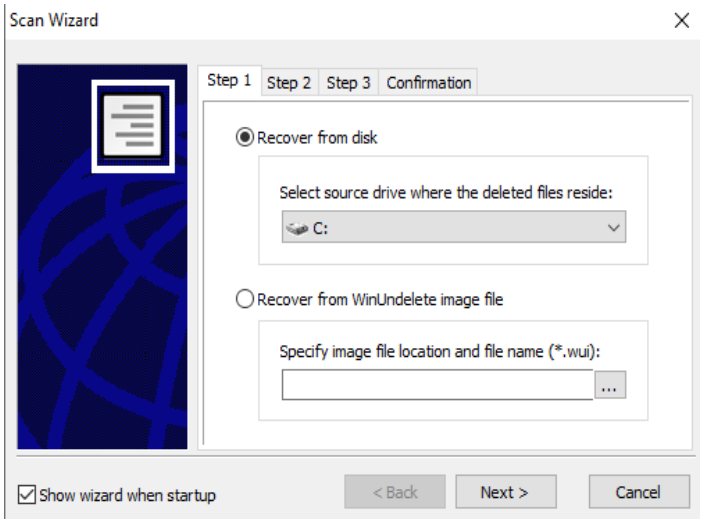


Figura 74. Configuración de la herramienta WinUndelete.
Fuente: elaboración propia.

En la figura anterior, se tiene que seleccionar la unidad sobre la que se va a realizar el Carving, se pulsa siguiente y se le indica que busque todo tipo de ficheros o también, se puede especificar si se busca algún tipo concreto, en un caso de forense no se debe permitir ignorar ningún tipo de información, ni por tamaño, ni porque fuesen archivos temporales o de internet, como se muestra en la Figura 75.

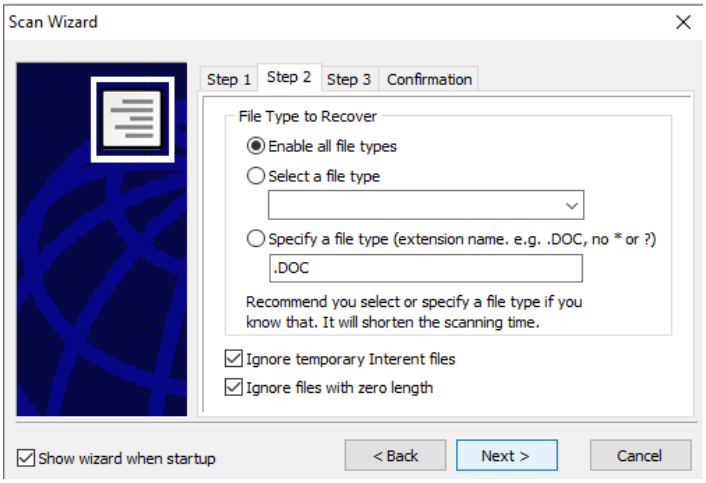


Figura 75. Búsqueda de todo tipo de archivos en WinUndelete.
Fuente: elaboración propia.

En el siguiente paso, se debe indicar la carpeta de destino, donde se guardaría los archivos que se recuperen, se ejecuta el proceso y se finaliza la configuración, se muestra una lista de archivos que han sido borrados como se muestra en la Figura 76.

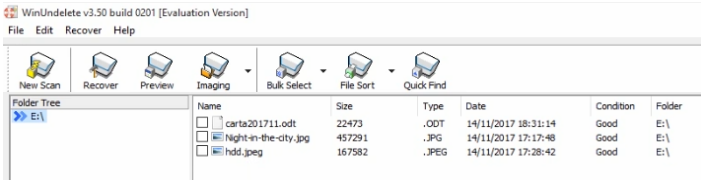


Figura 76. Resultado de la búsqueda de archivos en WinUndelete.
Fuente: elaboración propia.

En la figura anterior, se recuperó tres archivos que estaban marcados como borrados, sin embargo, continuaban en la tabla, en la versión de prueba no se puede recuperar el archivo, pero si se puede visualizarlo.

6.6. Trabajar con soportes dañados

En ocasiones es posible encontrarse con soportes que han sufrido daños y que se tenga que recuperar lo que sea posible, a grandes rasgos se puede encontrar con daños en el soporte físico o la información almacenada.

Con los daños físicos se tiene que asumir que siempre van a suponer pérdida de información, puede llegar a corromper la estructura de ficheros, así que, si se puede hacer una lectura de la información, la primera tarea a realizar es reconstruir todo lo que sea posible.

Lo que no se debe hacer nunca es reparar daños de la electrónica o mecánica del dispositivo si no se tiene experiencia, herramientas adecuadas y un laboratorio preparado, si no es así, mejor recurrir a empresas de recuperación de discos, que las hay buenas y profesionales, aunque no sea un servicio barato.

Se puede empezar por comprobar el estado de un disco dañado, para eso se empieza por desconectar el disco del pc original y conectarlo a un equipo de pruebas, se enciende el equipo y se comprueba si mecánicamente el disco funciona, es decir si gira y suena, lo ideal es no dejar que arranque el sistema operativo que pueda alojar el disco, para ello, al encender la computadora se debe forzar el acceso a la BIOS o UEFI del PC del equipo de pruebas y comprobar si el sistema reconoce la unidad de disco, si no funciona, o la BIOS no lo reconoce, se debe derivar el disco a un especialista, hay que recordar que se tiene que mantener la cadena de custodia.

6.7. Daños lógicos

Los daños en la información o daños lógicos pueden deberse a múltiples causas, como, por ejemplo, un apagado forzoso, una extracción inadecuada, etc., aunque algunos sistemas de ficheros como NTFS proporcionan cierta capacidad de recuperación en estos casos.

Los dos métodos principales para recuperar información dañada son:

- Zero – knowledge protocol.
- Consistency checking.

6.7.1. Zero – Knowledge protocol

El Zero – Knowledge protocol o protocolo de conocimiento nulo, es un método muy complejo, pero poderoso, desarrollado por criptoanalistas. A nivel teórico la premisa es que un usuario denominado probador, puede probar a otro usuario el verificador, que una afirmación, generalmente de tipo matemático es verdadera, sin para ello, compartir dicha afirmación, ni nada que no sea la prueba de veracidad.

La idea es ser capaz de reconstruir la información sin disponer de información previa, es decir, no se sabe si hay o no información, ni de qué tipo y se tiene que establecer una serie de pruebas que den esa respuesta.

6.7.2. Consistency checking

El otro método se denomina, Consistency Checking o comprobación de consistencia, es un método para armonizar los datos localizados en una computadora, el objetivo es asegurar que todos los datos están sincronizados entre grupos de protección y réplicas, lo que se busca, es localizar patrones conocidos, por ejemplo, en casi todo sistema de ficheros un directorio contiene dos punteros muy específicos, un punto que es el propio directorio y los dos puntos que hacen referencia al directorio de nivel superior, esto permite reconstruir un sistema de archivos a partir de las cosas conocidas que se van detectando.

6.8. Recuperar datos de navegadores web

Gran cantidad de actividades de los usuarios se realizan en servicios web desde el navegador y estas acciones dejan pistas. A nivel básico y fácilmente accesibles se tienen los historiales de navegación, la lista de páginas de favoritos o la lista de lecturas de leer más tarde.

Desde un punto de vista más técnico y en algunos casos más complejos, se tienen las cachés, las bases de datos de los distintos navegadores, las cookies que descargan los servidores a los que se conectan los usuarios, datos de sesiones guardados, el almacén de contraseñas guardadas o las herramientas de rellenado automático de formulario, cada navegador guarda estas informaciones de forma distinta y hay que saber analizarlas.

En Windows 10, concretamente con el navegador Chrome, si se quiere ver dónde se encuentra la información del usuario registrado, se puede ir a la siguiente dirección chrome://version/ y se encontrara una pantalla con la ruta del perfil como se muestra en la Figura 77.

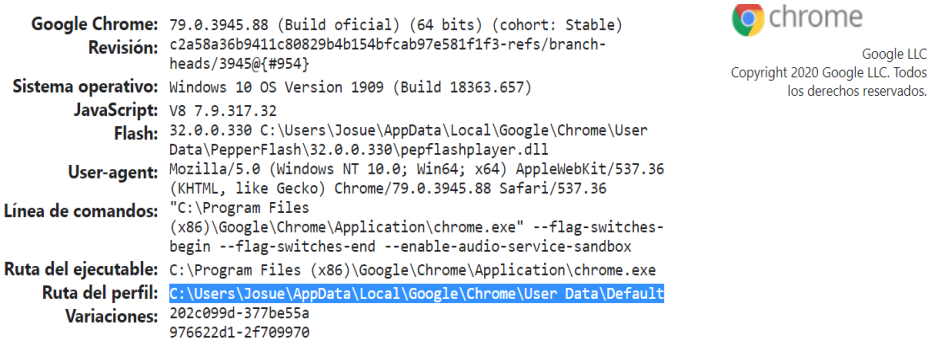


Figura 77. Ruta del perfil del usuario del navegador Chrome.
Fuente: elaboración propia.

En la figura anterior, si se copia esta dirección se puede ir a un explorador de archivos, se pega la dirección y se encontrará toda la información relativa al usuario registrado en Chrome como se muestra en la Figura 78.

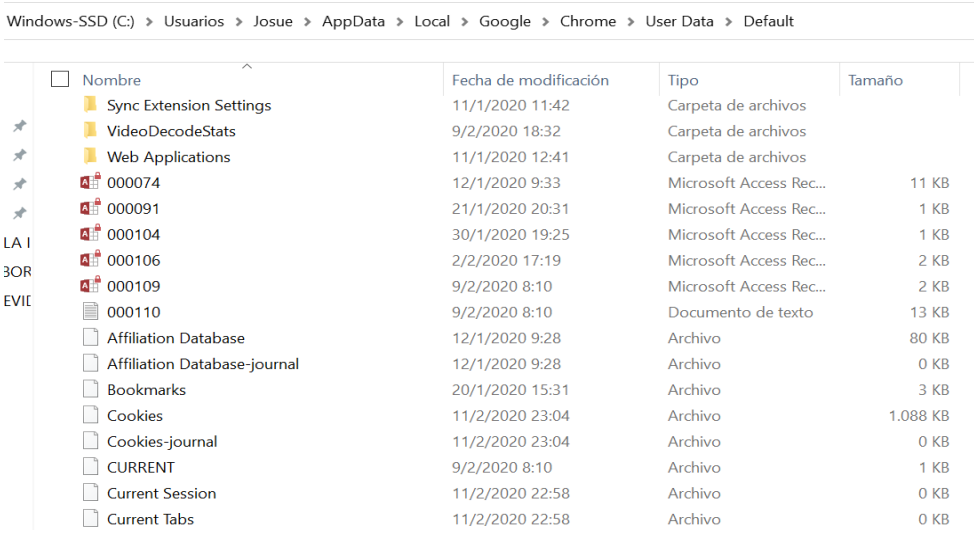


Figura 78. Revisión de los archivos de navegación del usuario extraídos de Chrome.
Fuente: elaboración propia.

Por ejemplo, se puede abrir la aplicación de visualización de bases de datos en SQL Lite y se puede a abrir las cookies, como se muestra en la Figura 79.

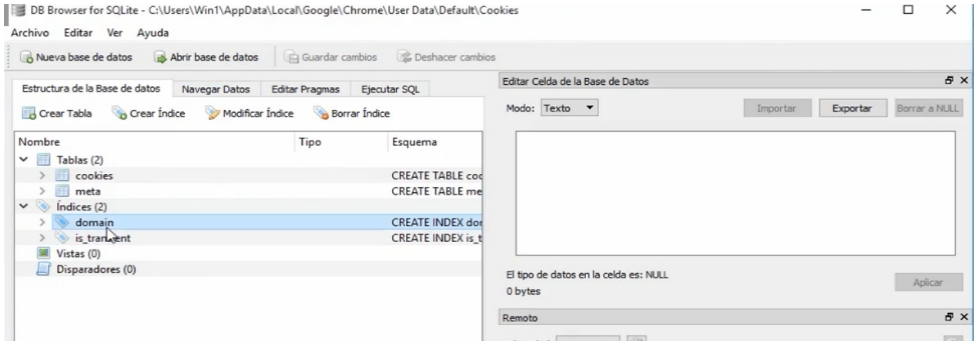
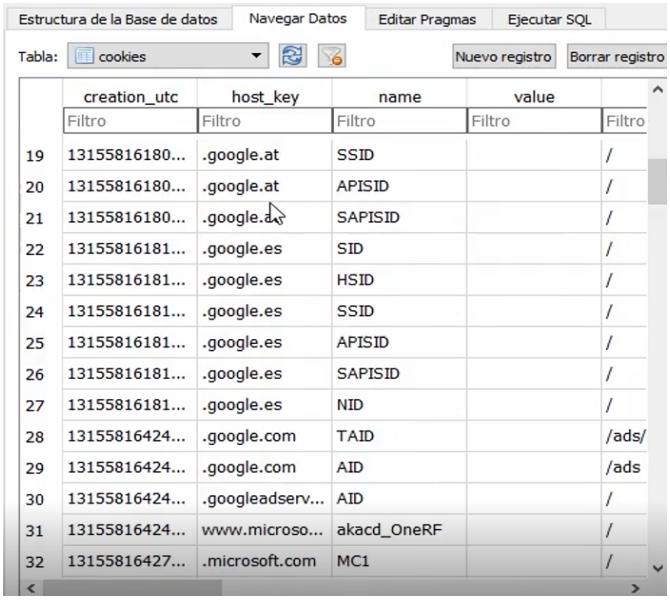


Figura 79. Visualización de la información de las cookies con SQL Lite.
Fuente: elaboración propia.

En la figura anterior, se puede navegar por la información, por ejemplo, por dominios y también se puede obtener información de las cookies que han ido instalando en el navegador los distintos servidores a las que se puede haber conectado el usuario como se muestra en la Figura 80.



	creation_utc	host_key	name	value	
	Filtro	Filtro	Filtro	Filtro	Filtro
19	13155816180...	.google.at	SSID		/
20	13155816180...	.google.at	APISID		/
21	13155816180...	.google.at	SAPISID		/
22	13155816181...	.google.es	SID		/
23	13155816181...	.google.es	HSID		/
24	13155816181...	.google.es	SSID		/
25	13155816181...	.google.es	APISID		/
26	13155816181...	.google.es	SAPISID		/
27	13155816181...	.google.es	NID		/
28	13155816424...	.google.com	TAID		/ads/
29	13155816424...	.google.com	AID		/ads
30	13155816424...	.googleadserv...	AID		/
31	13155816424...	www.microso...	akacd_OneRF		/
32	13155816427...	.microsoft.com	MC1		/

Figura 80. Listado de cookies instaladas por diferentes servidores de navegación.
Fuente: elaboración propia.

En la figura anterior, se puede ver un ejemplo del tipo de información que se puede obtener explorando el directorio asociado al perfil del usuario de Chrome.

Otro ejemplo un poco distinto de recuperación de información, se lo tiene en "**What every Browser Knows about you**", una aplicación web que muestra lo que el servidor es capaz de obtener de un navegador cuando éste se conecta, por ejemplo, información sobre el software, como se muestra en la Figura 81.

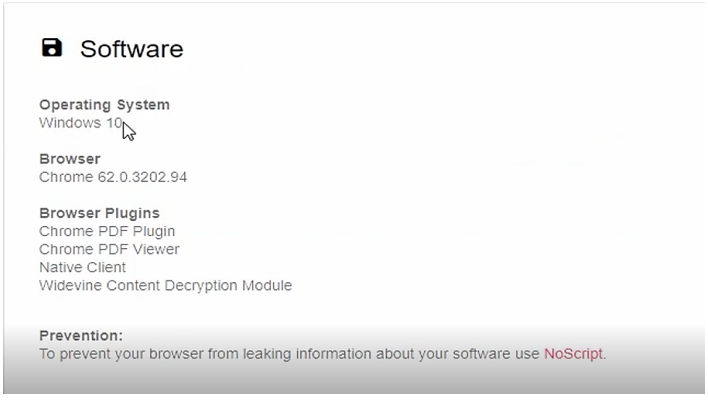


Figura 81. Obtención de los datos de navegación a través de aplicaciones externas.
Fuente: elaboración propia.

Otro tipo de información que muestra es la del hardware de la computadora desde la que se conecta llegando a saber incluso, los núcleos de servidor, el tipo de interfaz gráfica, si es una computadora portátil, información sobre la batería, también, informa si se está conectado a distintos servicios como redes sociales, en este caso, una cuenta de Google, puede incluso mostrar información del giroscopio o hacer un análisis de red para detectar otros equipos dentro de la red y esto es sólo un ejemplo de lo que desde el lado del servidor se puede obtener.

Otro ejemplo, es el navegador EDGE de Microsoft, en este caso, si se quiere acceder a la información se debe ir a la ruta que se muestra en la Figura 82.

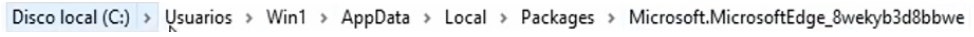


Figura 82. Acceso a la información del usuario a través del navegador EDGE.
Fuente: elaboración propia.

En la figura anterior, se puede encontrar la información relativa al historial la caché, las páginas visitadas, etc.

6.9. Recuperar evidencias de Smartphones

La telefonía móvil está totalmente instalada en las vidas de las personas, tanto es así, que mientras la tendencia del mercado de venta de computadoras desciende, la de smartphone no deja de crecer, ni se espera que deje de hacerlo, así que, es cada vez más común tener que hacer trabajos de investigación forense sobre teléfonos móviles, por lo que es necesario comprender el funcionamiento de las redes de telefonía móvil.

6.9.1. Redes telefónicas

Hay que saber los tipos de tecnología de red que existen y qué implicaciones tienen con respecto al uso de los dispositivos, por ejemplo, el HLR y VLR son las bases de datos de una red GSM que registran el estado de los clientes, indicando su localización en la red, si están o no activos, cada número de teléfono está registrado en la HLR con sus datos permanentes y los datos de carácter temporal como la localización o el número IMEI del terminal se registran en el VLR, esto es sólo un ejemplo, pero es necesario saber cómo interpretar la información de las últimas células a las que se ha conectado un celular, porque la información de localización es muy relevante cuando se habla de telefonía móvil.

6.9.2. Almacenamiento

Otra cosa que se debe tener clara es el almacenamiento de datos en los smartphones, este es independiente de la tarjeta SIM, en las tarjetas de memoria del propio teléfono o tarjetas de expansión, generalmente Micro SD, se almacenan datos del sistema operativo, de las aplicaciones y del usuario, como si fuesen discos duros de una computadora, la Figura 83 muestra en ejemplo de una tarjeta Micro SD.

Figura 83. Ejemplo de una memoria Micro SD.
Fuente: recuperado de https://www.kubii.es/.

6.9.3. SIM y el teléfono

La SIM es un chip de identificación que contiene la información que requiere el proveedor de servicio para identificar una línea, también, puede almacenar datos, pero muy pocos. La SIM está protegida por un código PIN que permite desbloquearla para que el operador pueda registrar el teléfono en el VLR. El código PUK se emplea para recuperar el código PIN de una tarjeta SIM y suele entregarse impreso en la tarjeta en la que se entrega la SIM, por lo que, si se recupera esa información se puede aplicar un nuevo PIN a una SIM para acceder a la información, además, la mayor parte de los teléfonos están bloqueados por un código de usuario que puede ser una contraseña, un patrón gráfico o mediante un sistema biométrico, aunque éstos suelen estar asociados a una contraseña por si no se puede operar con el acceso biométrico, la Figura 84 muestra un ejemplo de una tarjeta SIM.

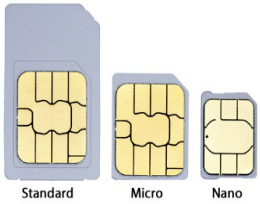


Figura 84. Ejemplo de tarjeta SIM.
Fuente: recuperado de https://www.internautas.org/.

Al trabajar con smartphone y con Tables, se encuentra con una mayor granularidad de sistemas operativos, entre todos ellos, los dominantes en el mercado son Android, desarrollado por Google o iOS de la compañía Apple.

También, se puede encontrar terminales más antiguos o incluso descontinuados con sistemas operativos BlackBerry, Windows Phone, Symbian, etc., sin olvidar que también, existen los teléfonos sencillos, los que no son smartphone. Según Gómez Ocampo (2009) existen muchas herramientas forenses para extraer información de la SIM entre la que se puede mencionar a Forensic Card Reader que muestra los datos en formato XML.

6.9.4. Información en smartphone

La información más básica a la que se debe aspirar al enfrentarse a un smartphone es la que componen la agenda de contactos, el historial de llamadas, los SMS, el correo electrónico, la mensajería de aplicaciones de chat, información de geolocalización y de conexiones de red, tanto GSM como a redes inalámbricas, e incluso de dispositivos Bluetooth.

El protocolo de adquisición cuando de teléfono se trata, empieza por conservarlo en el estado en el que se lo encuentre, preferiblemente encendido y desbloqueado, si hay riesgo de pérdida de datos, acceso remoto o similares, conviene aislarlo de cualquier conexión de red, sea telefónica o inalámbrica, para ello, se puede recurrir a bolsas que actúan como jaula de Faraday y cuando por fin se pasa a conectar el teléfono a la computadora del laboratorio, se debe asegurarse de impedir la sincronización automática entre ambos equipos, para evitar modificaciones de la evidencia, al menos hasta que sea seguro e imprescindible.

6.9.5. Software forense para smartphones

Cuando todo esté dispuesto, lo que corresponde es emplear una suite de análisis forense para telefonía móvil, que permita generar una imagen del teléfono sobre la que poder desarrollar la investigación, sin necesidad de manipular mucho más el terminal original, incluso, permitiendo en algunas circunstancias que su propietario pueda recuperarlo.

Para ello, se puede emplear aplicaciones genéricas con sus complementos para telefonía móvil como:

- EnCase.
- Cellebrite.
- Oxygen Forensics.
- Mobile Phone Examiner.
- XRY.

CAPÍTULO VII: EVIDENCIAS BASADAS EN RED

Este capítulo tiene como objetivo analizar la forma de recuperar las evidencias basadas en red para una investigación forense, desde el análisis del registro del firewall, la detección de las diferentes intrusiones en la red hasta el análisis de los datos que tienen los routers.

7.1. Registros de firewalls

Según Aguilera (2011) un firewall es un dispositivo de seguridad de red, que se utiliza para conectar dos o más redes entre sí y así facilitar yo registrar las comunicaciones que se establecen entre ellas. Los firewalls permiten controlar, registrando y autorizando o bloqueando qué tipo de tráfico o información permite pasar de una red a otra y los destinos y orígenes del tráfico que se autoriza, es decir, se crea reglas para decidir qué conexiones se pueden establecer con la red desde el exterior y a qué servicios externos se permite que se conecten los equipos de la organización.

7.2. Categorías de firewall

Existen distintas categorías de firewall, pero se puede centrar en la clasificación que se hace a partir del tratamiento de los paquetes de datos.

En primer lugar, se tiene os los de filtro de paquetes, que permiten o bloquean el flujo de paquetes en base a reglas como direcciones IP y puertos de origen o destino, protocolos de comunicación, es decir, se centran en el continente del paquete, no en el contenido.

En segundo lugar, se tiene los inspectores de paquetes o SPI, siglas de Stateful Packet Inspection, que inspecciona cada paquete y toma decisiones tanto para los paquetes inspeccionados, como para sus asociados, el decir, que aplica reglas de filtrado, no sólo en base a los datos del paquete en sí, también en base al contenido del mismo, y además los pone en un contexto con el flujo de datos al que pertenece.

La inspección de registros de firewall requiere de práctica, constancia y repetición para poder detectar anomalías, lo primero que hace falta es reconocer como es el tráfico normal de la red en la que se trabaja, ya que, si no se sabe que es normal, difícilmente se podrá discriminar lo anómalo, por ejemplo, un escaneo de puertos sirve para comprobar qué puertos están abiertos en un equipo específico al que se tiene acceso por red.

7.2.1. Escaneo de puertos

Según Pacheco y Jara (2010) el escaneo de puertos es una técnica que utilizan los atacantes para identificar qué servicios tiene activos el equipo que están escaneando, por ejemplo, si el puerto 21 está abierto, posiblemente tenga un servidor FTP, si el puerto 22 está abierto, un servidor SSH, el puerto 80 para servicios web y así muchos otros, por tanto, la inspección de puertos implica cierta comunicación e intentos de conexión que deben ser registrados por el firewall y que sirven de alerta, ya que un escaneo suele ser una fase previa a un ataque.

7.2.2. Conexiones de malware

Otro tipo de incidente que se puede detectar revisando los registros de un firewall, son conexiones salientes sospechosas, que pueden indicar que un malware, este filtrando información o conectándose a su centro de mando y control. Según Rascagneres (2016) un malware se lo puede definir como un programa malicioso, creado para comprometer un sistema sin el consentimiento del usuario. La identificación de ese tráfico saliente anómalo ayuda a identificar qué equipo de la red lo está generando y así, se puede pasar a analizarlo o supervisarlo con más detalle sí que hubiese algún incidente en curso.

7.2.3. Denegación de conexión

Un ejemplo genérico de una entrada de un registro de un log, es la denegación de una conexión, esto es una única entrada de registro mostrada en varias líneas como se muestra en la Figura 85.

```
20171016 11:55:34 fw00 fw00: NetScreen device_id=fw00  [Root]system-
notification-00257(traffic): start_time="2017-10-16 11:55:34" duration=0
policy_id=193 service=udp/port:7001 proto=17 src zone=Trust dst
zone=Untrust action=Deny sent=0 rcvd=0 src=172.16.12.1 dst=11.22.33.44
src_port=3036 dst_port=7001
```

Figura 85. Entrada de registro de conexión.
Fuente: elaboración propia.

En primer lugar, se debe tener la fecha y hora del registro, esto es así para cualquier sistema, después se indica qué dispositivo hace el registro, en este caso, el firewall identificado, el siguiente dato importante es cuando sucedió el evento y cuánto duró, a continuación, el identificador de la política que se ha violado y por lo que el tráfico ha sido bloqueado y en el resto de información, se muestra la red IP del puerto de origen, y la red IP del puerto de destino de la conexión, que en efecto ha sido

denegada, este ejemplo, es una única línea así que no se debe olvidar que una red con decenas o cientos de computadoras, puede estar generando registros enormes en más de un firewall, así que conviene practicar la interpretación de estos registros.

7.3. Detectar intrusiones en la red

Revisando registros de red y con las herramientas al alcance, habrá ocasiones en las que se tenga que ser capaces de detectar si se está sufriendo ataques a través de la red, para ello, lo más importante es saber cómo funciona.

Se puede analizar algunos ejemplos de varios ataques conocidos que se detallan a continuación:

Teardrop: se trata de un ataque basado en el envío masivo de información, cuya fragmentación en paquetes TCP ha sido deliberadamente corrompida por el atacante, el equipo que recibe dicha conexión acumula los paquetes mientras intenta reconstruir la información original, pero no puede, porque no llega completa, la técnica es tan simple como efectiva, se trata de que el servidor que recibe la información intenta reconstruir los datos, pero se satura causando la caída del sistema, aunque para eso, hoy día hace falta una cantidad realmente grande de datos.

Ataques LAND: este tipo de ataques se dan dentro de la red de área local y LAND no es el vocablo inglés para tierra, sino, Local Area Network Denial, consiste en enviar paquetes TCP de inicio de conexión, o sin al objetivo haciéndole creer que es el mismo el que está conectando consigo mismo, es una estratagema sencilla, pero si se ejecuta con suficiente intensidad, puede dejar sin servicio de red al equipo atacado, ya que tiene que gestionar los falsos paquetes TCP-SYM entrantes, el envío de respuestas a sí mismo y la recepción de esas mismas respuestas.

Ataques Smurg y Fraggle: el ataque Smart es la técnica más clásica empleada en ataques distribuidor de denegación de servicio, el objetivo es sobrecargar el tráfico de red de la víctima mediante el envío masivo de paquetes ICMP con una gran carga, una variación del Smurg es el ataque Fraggle, que consiste en hacer lo mismo, pero con paquetes UDP, que, dado que no están estableciendo sesión, sino, se pueden enviar tantos como se desee saturando al objetivo.

En Windows 10 se va a instalar un analizador de tráfico de red, en concreto, Wireshark que se lo descarga de la siguiente dirección web https://www.wireshark.org/ y se lo ejecuta para la instalación como se muestra en la Figura 86.

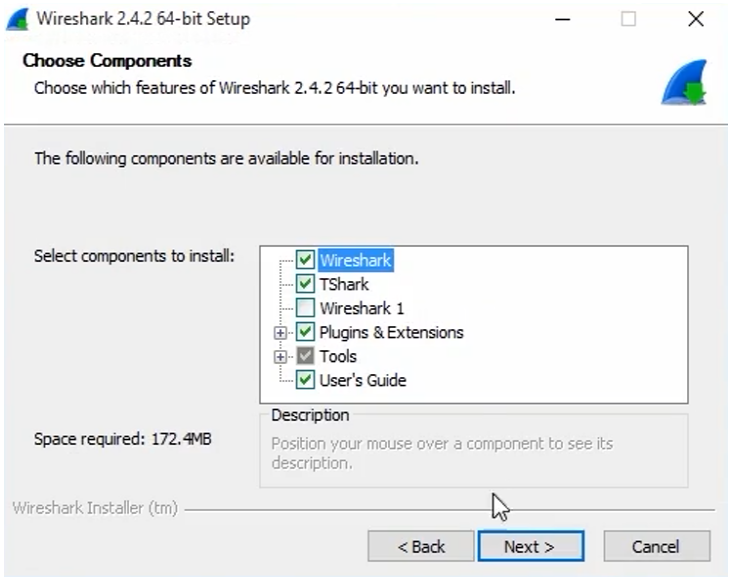


Figura 86. Instalación de Wireshark.
Fuente: elaboración propia.

En el proceso de instalación también, pide instalar el WinpCap que es la librería que se ocupa de gestionar los paquetes de información como se muestra en la Figura 87.

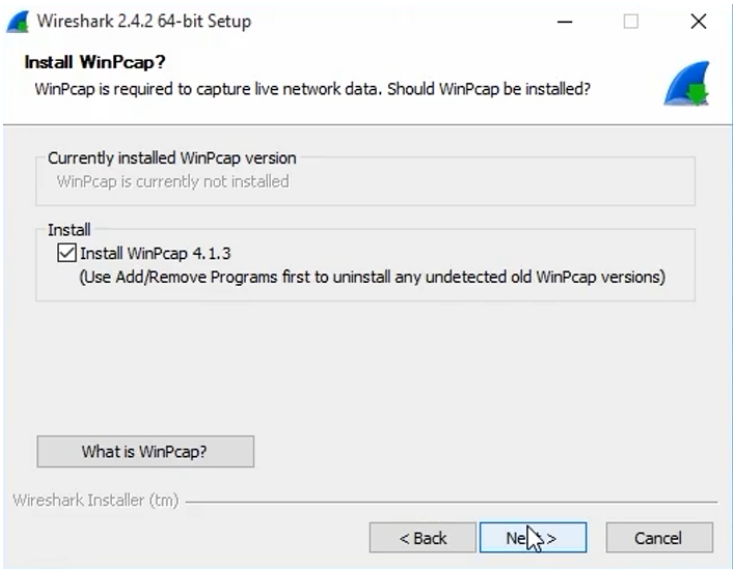


Figura 87. Instalación de librería para gestionar paquetes de información.
Fuente: elaboración propia.

También, la instalación permite seleccionar si se desea analizar tráfico de USB, como se muestra en la Figura 88.

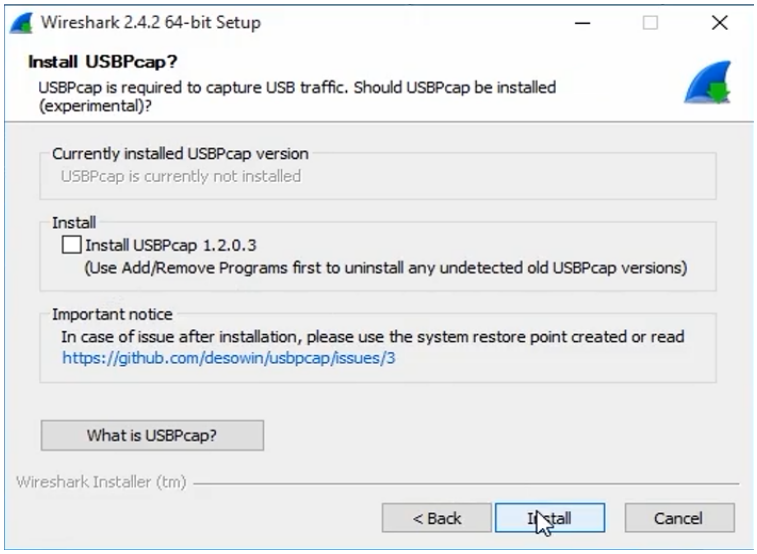


Figura 88. Instalación de aplicación para capturar tráfico USB.
Fuente: elaboración propia.

Una vez instalada la herramienta, se ejecuta y se muestra la pantalla principal de la herramienta como se muestra en la Figura 89.

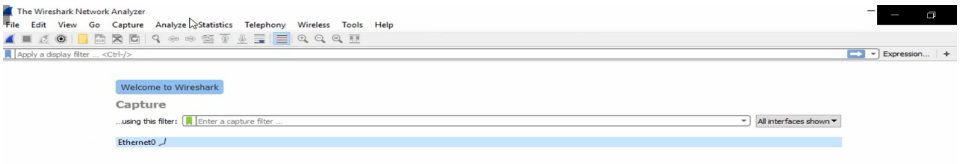


Figura 89. Interfaz principal de Wireshark.
Fuente: elaboración propia.

En las opciones del menú principal Capture ⟶ Option ⟶ se puede elegir la interfaz de red que se quiere capturar como se muestra en la Figura 90.

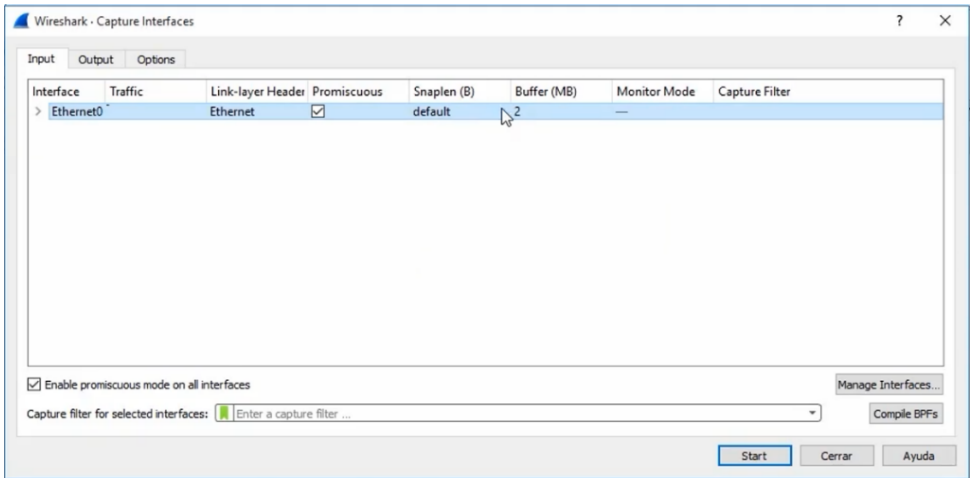


Figura 90. Selección de la interfaz de red para capturar tráfico en Wireshark.
Fuente: elaboración propia.

En un entorno de infraestructura bien desarrollado, esta interfaz sería una secundaria ya que se tendría una propia para navegar, conectarse a las redes etc., y se tendría una interfaz independiente conectada a un puerto mirror o espejo del switch de la red que se está gestionando, ese puerto mirror lo que hace reflejar todo el tráfico de la red en ese puerto, de forma que se pueda capturarlo con la aplicación de Wireshark.

Esta aplicación también permite mostrar archivos guardados de capturas anteriores y se muestra la información de la captura como se muestra en la Figura 91.

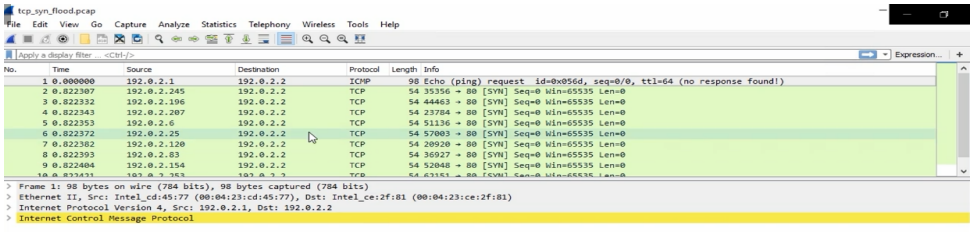


Figura 91. Análisis de tráfico de datos guardado en archivo en Wireshark.
Fuente: elaboración propia.

En la figura anterior, se puede observar que todas Las capturas son de protocolo TCP y de tipo SYM, si se despliega más lo conexión se puede obtener detalles de la captura como se muestra en la Figura 92.

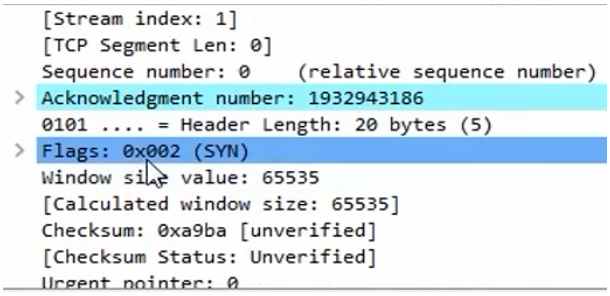


Figura 92. Detalle de la conexión de captura del tráfico en Wireshark.
Fuente: elaboración propia.

La figura anterior, indica que el **Flags** es de tipo **SYN**, entonces se está viendo que se tiene una captura de una conexión en la que todos los paquetes tienen distinto origen y mismo destino, en protocolo TCP y de tipo SYN, está claro que el objetivo es atacar al sistema alojado en esta dirección IP. Al tratarse de distintas direcciones de IP de origen, se trata de un ataque de denegación de servicio distribuido, así que, hay que aprender a monitorizar el tráfico.

7.4. Evidencias en los routers

Otro elemento fundamental de las redes, son los routers, de hecho, en gran cantidad de pequeñas empresas ni siquiera el firewall de red, más allá de los firewalls propios que puedan incluir los sistemas operativos de las computadoras, la Figura 93 muestra un ejemplo de un router.

Figura 93. Router para la conexión inalámbrica.
Fuente: recuperado de https://www.aboutespanol.com/.

7.4.1. Ataques de routers

Los routers también pueden ser víctimas de ataques, entre los cuales algunos de los más comunes que se puede encontrar, son la modificación del firmware o el sistema operativo del equipo para hacer que pase a formar parte de una botnet, una red equipos controlados sin saberlo sus propietarios, por una tercera persona cuya intención es utilizarlos para atacar a otros objetivos o para camuflar sus ataques.

Otro ataque común y sencillo es el de denegación de servicio, ya que puede verse saturado por cantidades ingentes de paquetes entrantes, que al intentar enrutarlos acabe saturando al equipo, propiciando su fallo o forzando a descartar solicitudes de conexión legítimas, que dejan sin servicio dichas conexiones.

Como se ha indicado las rutas forman parte intrínseca de la red, de hecho, son dispositivos diseñados para interconectar redes y direccionar el tráfico entre ellas, así que, en investigación forense, pueden contener información interesante como sus contraseñas, las tablas de enrutamiento, información de estructuras de red y por supuesto los registros de conexiones y actividades de gestión.

7.4.2. Registro de los routers

Casi toda la información que se pueda obtener de un router a nivel de sucesos, proviene del log del propio equipo, de su registro, sin embargo, la mayor parte de las rutas desplegados en domicilios, pequeñas empresas y algunas de tamaño considerable, trabajan con routers que les proporciona el proveedor de servicio de acceso a internet, que suelen ser bastante económicos y por tanto, su capacidad de almacenamiento escasa, por lo que los log abarcan un periodo de tiempo relativamente corto.

Son más cortos cuanto más tráfico gestione ese router, si los registros son la información más volátil, la configuración del mismo es la más estable.

7.4.3. Problemas en los routers

Los problemas a los que se pueden enfrentarse los peritos cuando un router está comprometido, son bastante variados.

Puede anular o modificar el tráfico de red, puede comprometer otros dispositivos de red, puede ayudar al atacante a evadir sistemas de protección de red, como firewalls IDS o IPS, puede facilitar la monitorización no autorizada del tráfico legítimo y puede redirigir el tráfico legítimo a través de proxys controlados por el atacante o derivarlo a destinos no deseados.

7.3.4. Los routers en la investigación forense

Lo que se debe y se puede hacer al llevar a cabo investigaciones forenses, pues lo primero es no reiniciar o apagar los routers, hay que recordar que se debe conservar el estado de los equipos tal y como se encuentran, lo siguiente sería localizar información o manuales del modelo de router para poder operar con seguridad, y además, hay que conseguir la contraseña por defecto o la que aplicó el responsable para poder acceder a su configuración y registros, a partir de ahí analizando configuración registros e incluso el firmware del propio router, se debe discriminar si el problema que se está investigando es un accidente, incidente fortuito o un ataque.

CAPÍTULO VIII: INVESTIGACIÓN FORENSE EN WINDOWS

Este capítulo tiene como objetivo determinar la forma de cómo realizar una investigación forense en el sistema operativo Windows, ya que, la mayor parte del equipo tecnológico está basado en este sistema operativo, se verificará el registro de eventos de Windows, los directorios especiales a los que tiene que recurrir un perito informático, hasta verificar las huellas que dejan los usuarios en el registro de Windows.

8.1. Windows y el análisis forense

En la actualidad y durante décadas el sistema operativo de escritorio más extendido ha sido Microsoft Windows, y por eso, se va a estudiar algunos fundamentos básicos de su funcionamiento para conocerlo mejor.

En primer lugar, un investigador forense debe familiarizarse con el funcionamiento del sistema operativo y una de las partes esenciales es el arranque, es conveniente estudiar instalaciones limpias y analizar procesos y archivos para conocer el funcionamiento normal del sistema, de esta forma, se será capaz de detectar procesos anómalos como, por ejemplo, los que puedan derivar de infecciones por malware que alteran el comportamiento del sistema, sea durante el arranque o durante la utilización por parte del usuario.

8.1.1. Archivos clave del sistema

Para empezar, se va a listar algunos ficheros importantes del sistema que se detallan a continuación:

- ntdetect.com, es un programa de Windows NT, que se ejecuta durante el proceso de arranque del sistema para identificar el hardware disponible en la computadora.
- ntbootdd.sys, es el controlador de dispositivos SCSI para comunicar con dispositivos de almacenamiento.
- hal.dll, es controlador que ejerce como capa de abstracción del hardware del equipo, respecto al sistema, se ejecuta en el kernel del sistema por lo que su integridad es crítica.
- winlogon.exe, es el programa encargado de identificar a los usuarios del sistema y cargar sus perfiles.
- explorer.exe, el proceso que administra la interfaz de usuario el escritorio, las ventanas, la barra de inicio, etc.

En el entorno de Windows 10 para ver algunos de los ejemplos de los que ficheros que se detallaron en el apartado anterior, se puede abrir el administrador de tareas o Task Manager como se muestra en la Figura 94.

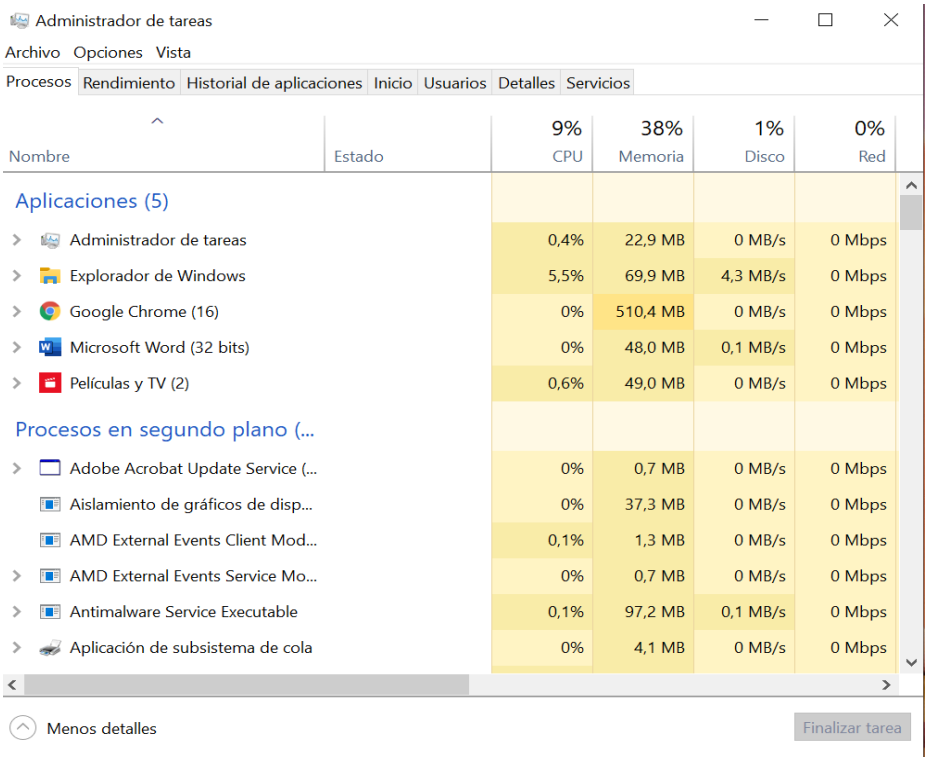


Figura 94. Administrador de tareas de Microsoft Windows.
Fuente: elaboración propia.

En la figura anterior, se aprecia la imagen nueva que se ha implementado en el sistema del administrador de tareas y si se va a detalles se visualiza los perfiles detallados de cada proceso como se muestra en la Figura 95.

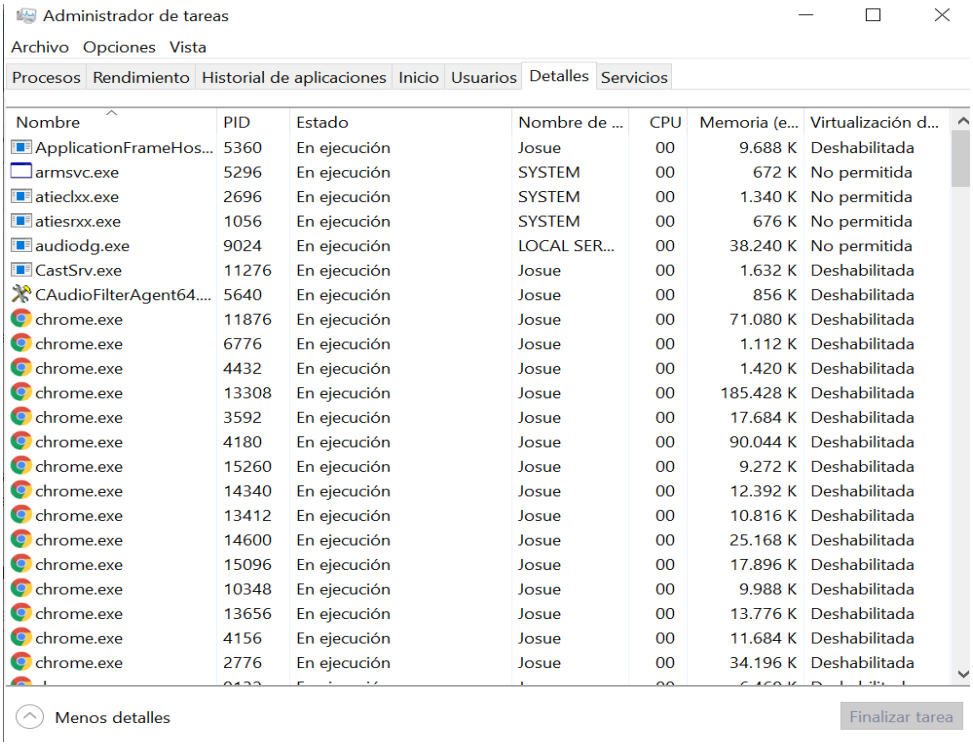


Figura 95. El administrador de tareas de Microsoft Windows.
Fuente: elaboración propia.

La figura anterior, se visualiza el indicador de proceso, el estado, el nombre de usuario que ejecuta este proceso, el uso de la CPU, de la memoria y una descripción, se puede buscar, por ejemplo, explorer.exe como se muestra en la Figura 96.

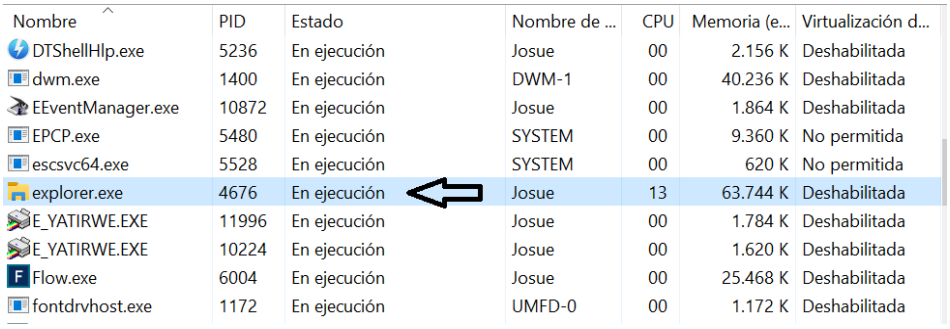


Figura 96. Ubicación del fichero explorer.exe en el administrador de tareas.
Fuente: elaboración propia.

En la figura anterior, se puede intentar detener este proceso, pero se advierte de que puede haber procesos dependientes ya que es un programa crítico del sistema como se muestra en la Figura 97.

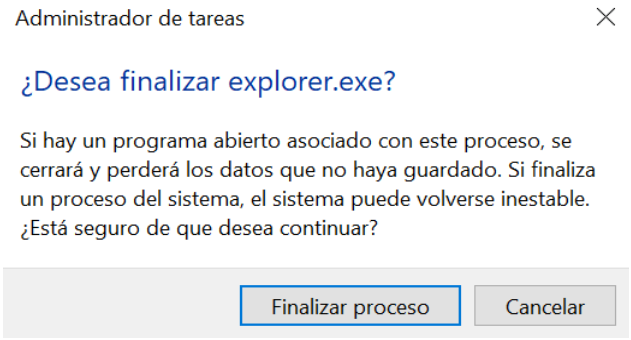


Figura 97. Finalización de un proceso crítico en el administrador de tareas.
Fuente: elaboración propia.

Otro proceso importante en Windows, en este caso, es el de winlogon.exe, es importante conocer los procesos fundamentales de Windows no sólo los que se ha detallado, porque el malware puede usar nombres similares a los procesos nativos del sistema operativo o puede incluso suplantarlo, por eso, es importante conocerlo.

8.1.2. Herramientas básicas.

Algunas herramientas básicas del sistema que se deben conocer son:

- IPconfig, para consultar y modificar la configuración de red.
- Netstat, que muestra las conexiones entrantes y salientes.
- Ping, para ver si se puede alcanzar una máquina via red.
- Traceroute, muestra la ruta que sigue una conexión entre el equipo en el que se lo ejecuta y el equipo de destino.
- Assoc, permite ver la asociación de los tipos de fichero con los programas que los abren.
- Driverquery, sirve para ver los controladores de un equipo las dll, básicamente.
- Powercfg, se puede ver cómo se gestiona la energía en el equipo.
- SFC, es un comprobador del sistema de archivos que, si se lo ejecuta con el verbo “scan now”, por ejemplo, comprueba la integridad de los archivos protegidos del sistema, y si detecta problemas intenta repararlo.
- Por último, se mencionará a tasklist, que es el equivalente al administrador de tareas, pero en línea de comandos.

8.2. Registro de eventos de Windows

Es una herramienta de soporte informático, para ver los errores y sucesos que está teniendo el sistema operativo, por detrás de forma transparente, sin que se sepa que está fallando, que se registra de forma automática como copia de seguridad, por lo tanto, si se encuentra algún error en el sistema operativo, se debemos acudir al visor de eventos. Entre los diferentes tipos de registros que puede incluir e puede mencionar a:

- Los de seguridad, relacionados con los accesos de los usuarios.
- Los de aplicaciones, relacionados con los programas que se ejecutan en el computador.
- Los del sistema, propios del mismo sistema operativo.

En Windows se puede acceder a través del menú o se puede buscar en la barra de búsqueda con el nombre de "visor de eventos" y ejecutado aparece la pantalla principal, como se muestra en la Figura 98.

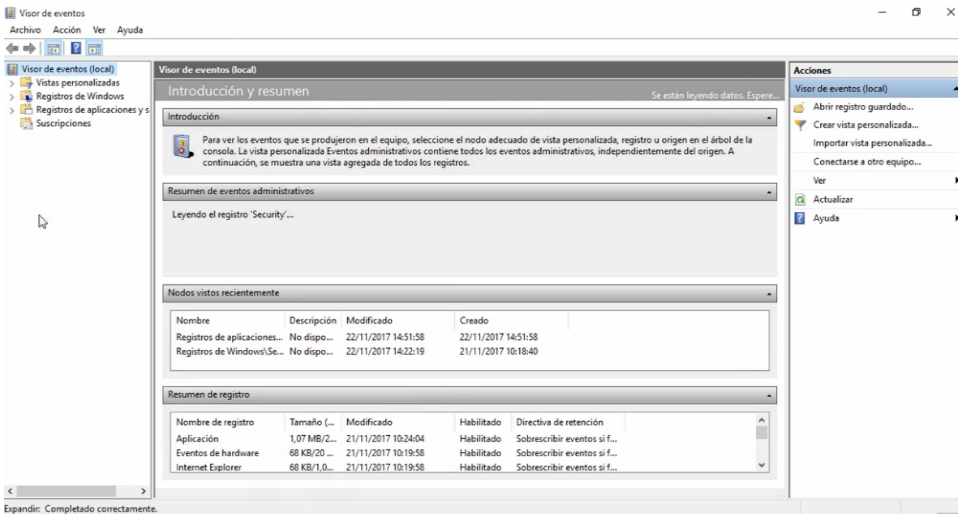


Figura 98. Registro de eventos en Windows.
Fuente: elaboración propia.

En los eventos de la máquina local, por ejemplo, se puede ir al registro de Windows, a la sección de seguridad y mostrar, por ejemplo, el primer evento se lo selecciona y aquí indica se ha realizado un intento de consultar la existencia de una contraseña en blanco para una cuenta, como se muestra en la Figura 99.

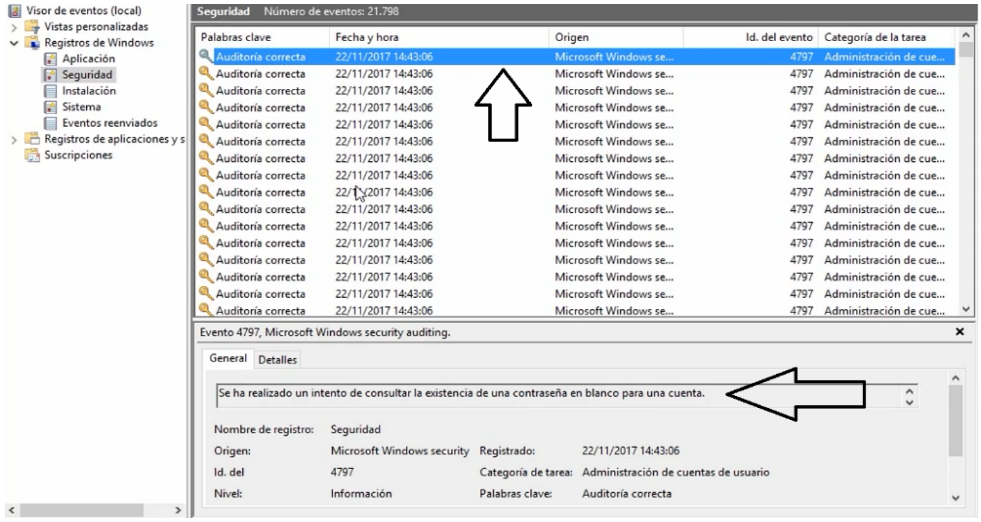


Figura 99. Selección y visualización de eventos en Windows.
Fuente: elaboración propia.

Cualquier evento que se encuentre, tiene su correspondiente ID y su descripción, otro ejemplo podría ser algo relacionado con la conexión de memorias USB, para esto se puede ir al registro de aplicaciones y servicios, se despliega, se selecciona la pestaña Microsoft, Windows y se busca la carpeta driver framework y aparece operativo como se muestra en la Figura 100.

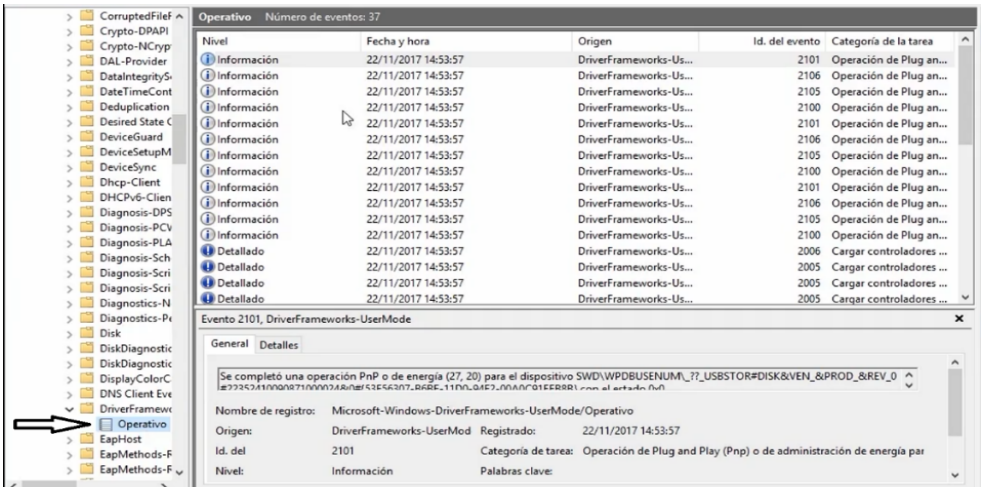


Figura 100. Visualización del registro de aplicaciones en el visor de eventos.
Fuente: elaboración propia.

En la figura anterior, se tiene una serie de eventos, pero por defecto es un registro de Windows que no está habilitado, para habilitarlo se tiene que hacer clic derecho, propiedades y habilitar registro como se muestra en la Figura 101.

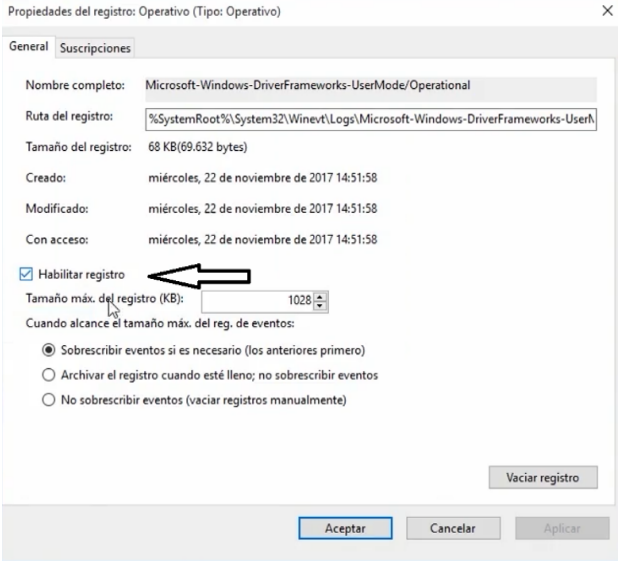


Figura 101. Habilitación de un registro de Windows en el visor de eventos.
Fuente: elaboración propia.

Hay que tener en cuenta que los registros ocupan espacio, así que, se tiene que decidir el tamaño máximo que se le va a permitir utilizar, se acepta y se va a visualizar algunos de estos eventos, por ejemplo, se puede buscar uno y con doble clic se puede ver los detalles más grandes, como se muestra en la Figura 102.

Figura 102. Detalles de un registro en el visor de eventos en Windows.
Fuente: elaboración propia.

En la figura anterior, se ha pedido al proceso host que cargue los controladores del dispositivo y toda esta información, el host es el sistema y este dispositivo es la memoria USB que se ha conectado, así que, de esta forma se tiene un registro en Windows de que se ha conectado una memoria USB.

El siguiente registro el siguiente evento, es el proceso host que cargó correctamente los controladores del dispositivo y así sucesivamente, se puede navegar arriba y abajo en orden cronológico por los eventos, por eso, esta herramienta de visor de eventos de Windows es tan importante a la hora de reconstruir hechos pasados, puede ayudar con el ejemplo que se ha visto, incluso a identificar una memoria USB concreta, saber si estuvo o no conectada en alguna computadora.

Es importante aclarar que los números de ID de evento varían en función de la versión del sistema operativo, así que, ante la duda siempre leer la descripción general, tomar nota de los números que interesen para poderlo consultarlos y, si no, hacer búsquedas online.

De esta, manera siempre se puede hacer las consultas que sean necesarias de ese tipo de búsquedas que sean frecuentes para el trabajo del forense.

8.3. Directorios especiales de Windows

Igual que se ha visto archivos, herramientas y procesos interesantes de Windows, se debe tener claro cómo está organizado y estructurado la información de las carpetas del sistema operativo para luego saber encontrar la información. Por lo general uno de los directorios más importantes es el relacionado con el usuario que usa el equipo, encontrado generalmente en "**C:\Users\NomUsu**", aquí se puede encontrar una serie de carpetas de documentos, descargas, el escritorio y una carpeta especial denominada "**AppData"** en donde se almacenan configuraciones personalizadas. También, se puede encontrar un directorio especial donde se instalan los programas denominado "**Program Files**" o archivos de programas, en la cual se crean dos carpetas, una para aplicaciones de 32 bits y otra para 64 bits, también se puede encontrar carpeta que almacena drivers o controladores del hardware, el cual es el directorio "**C:\Windows\System32**\", de hecho, uno de sus directorios es drivers, además, en este directorio se puede encontrar muchas de las herramientas del sistema que se ejecutan por línea de comandos, conocer la estructura de archivos del sistema operativo, es útil tanto para investigar incidentes, como para saber dónde buscar información oculta.

En Windows 10 y si se abre el explorador de archivos, se puede ir al disco "**C**:" y localizar la carpeta usuarios que se detalló anteriormente, dentro de la carpeta se tiene los directorios por defecto, búsqueda, contactos, la carpeta de descargas, de documentos, el escritorio y como carpeta oculta esta "**AppData**", como se muestra en la Figura 103.

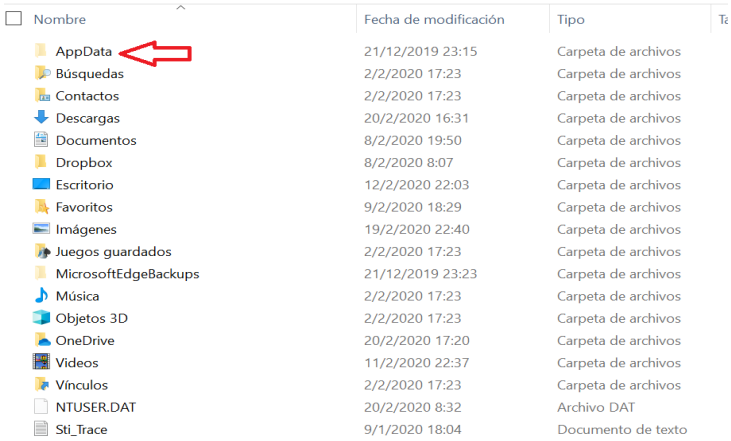


Figura 103. Carpeta de archivos de los Usuarios en Windows 10.
Fuente: elaboración propia.

En la carpeta "**AppData**" se tiene información de distintas aplicaciones pertenecientes a Google, Microsoft, el navegador Microsoft Edge, dado que Windows 10 ya tiene arquitectura de 64 bits se tienen dos carpetas separadas una para los programas con esa arquitectura y otra para los de 32 bits, la carpeta donde se encuentra la mayor parte de los drivers es en Windows y system32, de hecho, aquí se tiene la carpeta drivers con.

Algo interesante en este directorio es la carpeta "etc", donde se encuentra "**host**", que es un archivo que se puede editar, donde se indican rutas similares al servicio del DNS, es decir, una dirección que se ubica aquí, asociada a su dirección IP y nombre de dominio, como se muestra en la Figura 104.

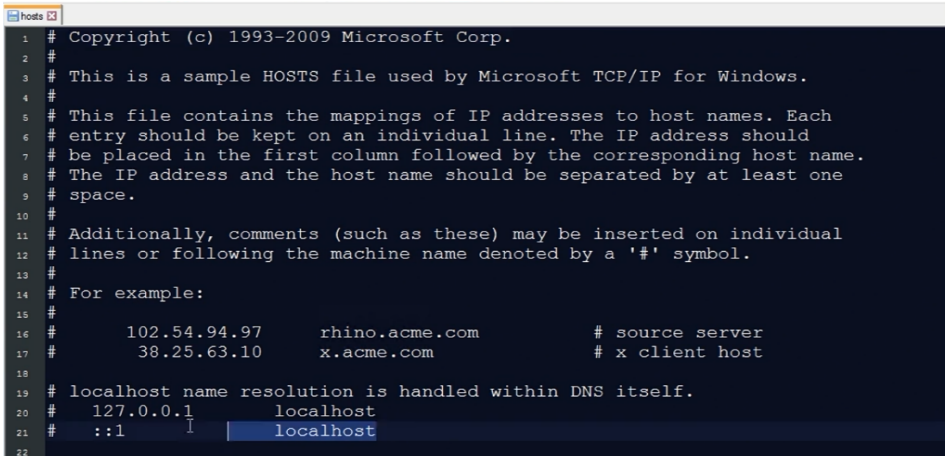


Figura 104. Detalles del archivo host en la carpeta ETC de Windows.
Fuente: elaboración propia.

Este archivo sólo se puede editar si se abre con permisos de administrador, en ocasiones algunos malware que alcanzan privilegios de administrador, pueden modificar este archivo para que cuando al visitar una página web, halla una conexión a una URL normal de un servicio, aunque sea de publicidad, por ejemplo, al estar registrado ese dominio en este archivo de host, en vez de ir a la IP legítima correspondiente, irá a la que se indica en este archivo de host, por eso, hay que tener precaución con lo que se escribe aquí.

En la carpeta "**System32**", se pueden encontrar muchos programas, uno de ellos es el comando Ping.exe, Netstat, etc., la mayor parte de los comandos pueden ser encontrados en este directorio, de esta manera, se conocen los directorios principales de Windows, se sabe para qué sirve cada uno de ellos y se sabe que debería poder encontrar en ellos y que no, por si se oculta información o por si algún actor malicioso sea una persona o un malware oculta información.

8.4. El registro de Windows

El registro de Windows es el repositorio de valores empleados por aplicaciones y por el propio sistema para almacenar parámetros, valores, Flags de estado, etc., es esencialmente un lugar donde almacenar parámetros de configuración.

Las secciones en las que se clasifican las claves del registro son:

- HKEY_CLASSES_ROOT: o Clase raíz donde se encuentran atajos de teclado, reglas para arrastrar y soltar elementos, información de la interfaz de usuario, etc.

- HKEY_CURRENT_USER: o usuario actual que almacena información del usuario registrado y puede contener mucha información interesante de cara a investigaciones forenses.
- HKEY_LOCAL_MACHINE: máquina local, es el lugar donde se registran las configuraciones que afectan a todo el equipo, no sólo, a usuarios específicos.
- HKEY_USERS: o usuarios, contiene los perfiles y las preferencias de cada cuenta de ellos, aquí también, se puede encontrar detalles importantes para investigaciones vinculadas a los usuarios.
- HKEY_CURRENT_CONFIG: por último, el de configuración actual, qué es el conjunto de parámetros de configuración que se están aplicando al equipo en cada momento, así que, HKEY_CURRENT_USER y HKEY_CURRENT_CONFIG serían información volátil correspondiente a lo que está sucediendo en el ordenador con el usuario que está actualmente registrado.

En Windows 10 para acceder al registro se busca "**REGEDIT**", se solicita permiso de administrador y se ejecuta el registro de Windows como se muestra en la Figura 105.

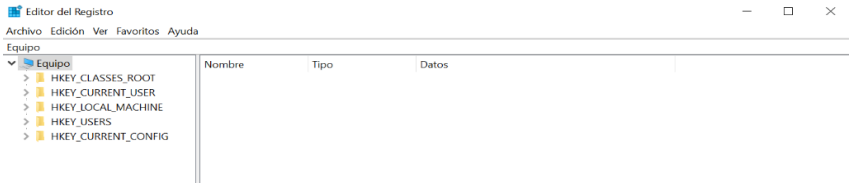


Figura 105. Editor de registro de Windows.
Fuente: elaboración propia.

En REGEDIT, se puede verificar la configuración de la máquina local, se ingresa en "**HKEY_LOCAL_MACHINE**", la opción de "Software", después "**Microsoft**", luego "**Windows**" y dentro de Windows se encuentra "**CurrentVersion**" o versión actual, aquí se encuentran unas variables qué es "**ProgramFileDirectory**", que indica que el directorio de archivos de programas "Programa Files" y el de 32 bits, es el programa files y entre paréntesis x86, como se muestra en la Figura 106.

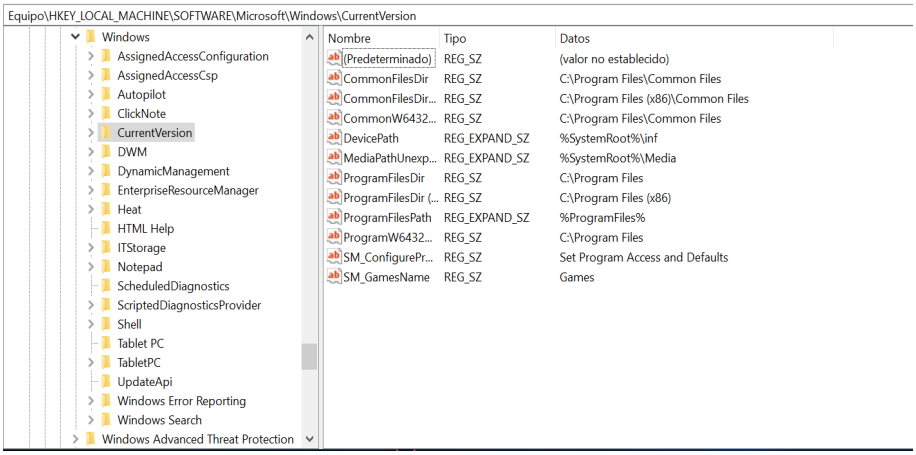


Figura 106. Visualización del registro de Windows para HKEY_LOCAL_MACHINE.
Fuente: elaboración propia.

Dentro de este mismo directorio de la clave de Local Machine, si se despliega se puede encontrar otro directorio que se llama “RUN”, aquí se encuentran aplicaciones que se ejecutan al inicio del sistema, este directorio es muy habitual que sea utilizado por malware para que cuando se reinicie la máquina, el malware inicia también su ejecución, así que, se debe siempre tenerlo en cuenta, analizando el resto de lugares del registro de Windows, se puede descubrir valores interesantes del sistema, e incluso investigar a un usuario activo u obtener información de la configuración de otros usuarios del sistema.

REFERENCIAS BIBLIOGRÁFICAS

Aguilera, P. (2011). *Redes seguras (Seguridad informática).* Editex.

Astudillo, S., y Morales, G. (2018). *Software y dispositivos utilizados en la computación forense.*

Course Hero. (s.f.). https://www.coursehero.com/

Domínguez, F. L. (2013). *Introducción a la informática forense.* Grupo Editorial RA-MA.

Estrada, A. C. (2010). La informática forense y los delitos informáticos. *Revista Pensamiento Americano,* (4), 81-88. https://www.academia.edu/27115286/La_inform%C3%A1tica_forense_y_los_delitos_inform%C3%A1ticos

Gallego, J. C., y Folgado, L. (2011). *Gestión de discos (Montaje y mantenimiento de equipos).* Editex.

Gómez Ocampo, L. M. (2009). Informática Forense Para Móviles. *Revista de Información, Tecnología y Sociedad, 32*. http://www.revistasbolivianas.org.bo/scielo.php?script=sci_arttext&pid=S1997-40442009000200007&lng=en&nrm=iso3

Gómez, H. H. S. (2009). *Informática Forense.* https://docplayer.es/4758786-Informatica-forense-hernan-herrera-sebastian-gomez.html

Mena, Y. (2009). Algoritmos HASH y vulnerabilidad a ataques. *Revista de Información, Tecnología y Sociedad, 108.* http://www.revistasbolivianas.org.bo/scielo.php?script=sci_arttext&pid=S1997-40442009000200026&lng=es&nrm=iso

Pacheco, F. G., y Jara, H. (2010). *Hackers al descubierto.* USERSHOP.

Rascagneres, P. (2016). *Seguridad informática y malwares: análisis de amenazas e implementación de contramedidas*. Ediciones ENI.

Ingeniería y Tecnología

3ciencias