Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-27

ANÁLISIS DE HERRAMIENTAS OPENSOURCE PARA LA INFORÁTICA FORENSE CON ÉNFASIS EN LA RECOLECCIÓN DE EVIDENCIA DIGITAL.

Emerson Yamit Atehortúa Meneses

Edison Fabián Jaramillo

Programa Académico

Ingeniería de Sistemas

Director(es) del trabajo de grado

Gabriel Taborda

INSTITUTO TECNOLÓGICO METROPOLITANO

2018

RESUMEN

La información es actualmente el bien más valioso para todo tipo de organizaciones, al ser almacenada en medios informáticos se hace vulnerable a daños, perdidas y/o modificaciones no autorizadas. La seguridad informática juega un importante papel en el intento de mantener a salvo dicha información. A pesar de los indiscutibles avances para detectar y prevenir amenazas, aún sigue habiendo fisuras en continuo aumento. La realidad es que hay muchas facetas para asegurar la infraestructura o información de una organización o persona, sin embargo, los criminales cibernéticos están modificando constantemente su estrategia de ataque para sacarle el máximo provecho a los espacios vulnerables de la seguridad y las personas.

Los ciberdelincuentes manejan técnicas avanzadas para realizar ataques informáticos, casi sin dejar rastros. En el presente trabajo se da a conocer gran cantidad de herramientas de informática forense, herramientas útiles en el proceso de recuperación de información y de recolección de evidencias digitales frente a un acontecimiento imprevisto, que facilitan a los investigadores en la exploración e investigación de un ordenador u otro medio en el cuál se tenga almacenada información, se muestran cuáles son las herramientas de software libre más utilizadas y se realizan pruebas con algunas de ellas mostrando su funcionalidad y resultados .

***Palabras clave*:** *Informática forense, herramientas de informática forense, evidencia digital, cadena de custodia, forensics tools, Tools for computer forensics, Open source digital evidence collection tools.*

RECONOCIMIENTOS

Agradecemos primero a Dios por darnos salud y vida, por ser nuestro guía y darnos la oportunidad de culminar nuestros estudios, a la institución ITM, a nuestro asesor Gabriel Taborda por su "tiempo y conocimientos" brindados y a los demás docentes que hicieron parte en nuestro proceso de formación, a Carolina Muñoz por estar apoyándonos en el desarrollo de este trabajo, a nuestros familiares por su apoyo, comprensión y paciencia, a todos los que contribuyeron de una u otra forma en la elaboración de esta tesis.

ACRÓNIMOS

AFF: Advanced Forensics Format

AND: Ácido desoxirribonucleico

AOL: America Online

ARJ: Archived by Robert Jung

AVI: Audio Video Interleave

BMP: Bitmap image file

CART: Computer analysis and response team

CD: Compact Disc

CDR: Vector image file format

CMD: Command Prompt

DBF: Database system

DIBS: Portable Evidence Recovery Unit

DOC: Microsoft word file format

DXF: Drawing Exchange Format

EWF: Enhanced Write Filter

EXE: Executable

EXIF: Exchangeable image file format

FAT: File Allocation Table

GIF: Graphics Interchange Format

GNU: Free Software Foundation

GPS: Global Positioning System

HTML: HyperText Markup Language

ICC: International Color Consortium

IMAP: Internet Message Access Protocol

IOCE: International Organization on Computer Evidence

IP: Number that identifies each device within a network

IPTC: International Press Telecommunications Council

IRS: Internal Revenue Service

JFIF: File Interchange Format

JPG: Joint Photographic Group

KEY: Clave

LZH: Data compression format

MAC: Address MAC

MBR: Master boot record

MD5: Abreviatura de Message-Digest Algorithm 5

MFT: Managed file transfer

MID: Mobile Internet Device

MOV: Filename extension for the QuickTime multimedia file format

MP3: Audio file format

NTFS: New Technology File System

PCAP: Interface of a programming application for packet capture

PDA: Personal digital assistant

PDF: Portable Document Format

PNG: Portable Network Graphics

POP3: Post Office Protocol

RAID: Redundant array of independent disks

RAM: Random Access Memory

RAW: Digital File Format of Images

RCFL: Regional Computer Forensic Laboratory

RFC: Request for Comments

RTF: Rich Text Format

SCSI: Small Computer System Interface

SD: Secure Digital

SDHC: Secure Digital High Capacity

SMTP: Simple Mail Transfer Protocol

TAR: Compression file environment Unix

TCP: Transmission Control Protocol

TIF: Tagged Image File Format

UDP: User Datagram Protocol

URL: Uniform Resource Locator

USB: Universal Serial Bus

USM: Simplified Security Intelligence

WAV: Audio File Format

XLS: Microsoft Excel file format

XMP: Extensible Metadata Platform

ZIP: Lossless Compression Format

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE IMÁGENES

1. INTRODUCCIÓN

En la informática forense la investigación de los medios digitales está creciendo cada día mucho más, ya que la tecnología está avanzando con dispositivos capaces de transportar información de un lugar a otro, en medios como celulares, dispositivos pendrive, equipos o cámaras que pueden almacenar datos muy importantes.

La delincuencia informática evoluciona constantemente, muchas personas y organizaciones han sido víctimas de delitos informáticos y necesitan saber qué fue lo que sucedió y como sucedió el incidente, en estos casos la evidencia digital cobra vital importancia.

(Almedia, 2015) Afirma que, así como un crimen físico deja evidencias, un crimen informático también las deja, pero dichas evidencias quedan almacenadas de forma digital y en la mayoría de los casos dicha información no se puede leer o recolectar por medios comunes o mecanismos tradicionales. Esto abre paso a un nuevo campo de investigación criminal que permite recolectar evidencia de una manera confiable y segura.
Por esta razón se realiza un estudio de la informática forense y de algunas herramientas para la recolección de evidencia digital, enfatizando en las herramientas de software libre, básicamente para la recolección de evidencia en memoria y disco, haciendo un comparativo entre las más importantes.

1.1 OBJETIVO GENERAL

Realizar un estudio comparativo de herramientas opensource de informática forense para la recolección de evidencia digital.

1.2 OBJETIVOS ESPECÍFICOS

- Realizar una revisión bibliográfica a cerca de la informática forense y sus herramientas, con énfasis en los aplicativos para la recolección de información.
- Seleccionar las herramientas de software libre más empleadas, según la revisión bibliográfica, para la recolección de evidencia digital.
- Definir los criterios para la construcción de un cuadro comparativo para las herramientas de análisis forense de recolección de evidencia digital.
- Realizar la valoración de las herramientas más empleadas para la recolección de evidencia digital, teniendo en cuenta los criterios definidos en el cuadro comparativo.
- Seleccionar del cuadro comparativo dos herramientas que reporten mejor valoración para la recolección de evidencia digital.
- Realizar una prueba de funcionalidad con las dos herramientas seleccionadas para hacer un análisis comparativo entre ellas.

1.3 ORGANIZACIÓN DEL TRABAJO

El presente trabajo se organizó en cinco unidades de la siguiente manera:

En la Unidad 1 se presenta una breve introducción sobre la problemática en cuanto al crecimiento acelerado de la tecnología, la delincuencia informática y la informática forense como herramienta para mitigar esta problemática. También se incluyen los objetivos que se pretenden alcanzar en la realización de este proyecto.

En la Unidad 2 se presenta el marco teórico, en el cual se pueden apreciar conceptos como Seguridad informática, Informática forense, Evidencia digital, Cadena de Custodia, también se puede observar acerca de la Historia de la Informática Forense y algunas de las herramientas más utilizadas en este campo.

La Unidad 3 contiene la Metodología utilizada en la realización de este trabajo, esta fue

desarrollada por medio de fases así: La primera fase se refiere a la revisión de la literatura, en la segunda fase se seleccionan las herramientas más empleadas, para la fase 3 se realiza un cuadro comparativo y en la cuarta fase se seleccionan las herramientas a las que se le realizan las pruebas.

En la Unidad 4 se presentan los resultados obtenidos en la realización del proyecto.

En la Unidad 5 se puede observar las conclusiones que se obtuvieron a partir de esta investigación, las recomendaciones y posibles trabajos futuros

2. MARCO TEÓRICO

El estudio de la informática forense es cada día más necesario, es un campo muy extenso por lo cual, para su estudio se necesita bastante tiempo y dedicación, para obtener todos los conocimientos y herramientas necesarias. En la realización de este proyecto se estudiarán conceptos y técnicas que nos ayudarán a entender mejor su aplicación.

2.1 SEGURIDAD INFORMÁTICA

Llamada también seguridad de tecnologías de la información, es el área de la informática cuyo principal objetivo es la protección de la infraestructura computacional y todo lo que con esta se relaciona y, especialmente, la información que contiene. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, hardware y todo lo que la organización valore y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada (Ideas integrales, 2016).
(Mendosa, 2014) Afirma que para que un sistema informático sea seguro, se deben garantizar tres medidas fundamentales: Confidencialidad, integridad y disponibilidad.

- **Confidencialidad:** Es una propiedad que garantiza que el acceso a la información sea permitido únicamente a entes autorizados.

La confidencialidad se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático, basándose en este principio, las herramientas de seguridad informática deben proteger el sistema de invasores y accesos por parte de personas o programas no autorizados. Este principio es particularmente importante en sistemas distribuidos, es decir, aquellos en los que los usuarios, computadores y datos residen en localidades diferentes, pero están físicamente y lógicamente interconectados.

(Gonzalez, 2014).

- **Integridad:** Es una propiedad que permite verificar que los datos no han sido modificados sin autorización.

Es necesario asegurar que los datos no sufran cambios no autorizados, la pérdida de integridad puede acabar en fraudes, decisiones erróneas o como paso a otros ataques. El sistema contiene información que debe ser protegida de modificaciones imprevistas, no autorizadas o accidentales. (Jerez, 2004).

- **Disponibilidad**: Es una característica de la información que garantiza el acceso a los recursos o a un servicio, ya sea a personas, procesos o aplicaciones.

La disponibilidad se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deben reforzar la permanencia del sistema, en condiciones de actividad adecuadas para que los usuarios accedan a los datos con la frecuencia y dedicación que requieran, este principio es importante en sistemas informáticos cuyos compromisos con el usuario, son prestar servicio permanente.
(Gonzalez, 2014).

Además de estas medidas, la seguridad informática también debe garantizar:

- **Autenticidad:** Es el proceso por el que se garantiza la correcta identificación de personas, equipos, interfaces, datos y procesos.

El método más usado para proporcionar autenticidad es la firma digital, basada en la criptografía, empleando llaves o claves. Las llaves son una secuencia bastante larga de caracteres y números, generadas por un procedimiento matemático. Su utilización es un proceso por el cual los comunicantes poseen cada uno dos llaves: Una llave privada, que mantienen en su poder, y una llave pública, que está a disposición de los posibles intercomunicadores. La criptografía permite autenticar la persona con quien se está

realizando la comunicación. (Castañeda & Morales, 2004).

- **No Repudio:** Es un servicio de seguridad que permite probar la ejecución de un proceso (transacción, comunicaciones, etc.).

Una vez enviado un documento, su emisor no puede negar haber sido el autor de dicho envío. El no repudio es la condición de imposibilidad de negación del envío de un mensaje. Para ello se utiliza la posibilidad de firmar virtualmente los mensajes. El destinatario aplicará entonces la llave pública del remitente, única manera de desencriptar el mensaje y por tanto, garantía de que este está expedido por él. El No repudio es condición suficiente para la Autenticidad, por lo que si un documento es no repudiable es auténtico, pero no al revés. (Castañeda & Morales, 2004).

Imagen 1: Medidas básicas de un sistema seguro. (Tomado de *(Sánchez, 2015)***)**

2.1.1 Amenazas

Los recursos que forman parte de un sistema informático facilitan su funcionamiento y son los principales activos que se deben proteger, estos se pueden clasificar según (Aguilar, 2010) de la siguiente manera:

- Hardware
- Software
- Datos
- Redes
- Soportes
- Instalaciones

- Personal
- Servicios

De estos activos los más expuestos a amenazas son datos, hardware y software, en especial los datos.

El diccionario de la lengua de la lengua española define amenaza como el "anuncio de un mal o peligro", por su parte (Reyes, 2012) afirma: "*una amenaza representa la acción que tiende a causar un daño a los dispositivos o sistemas en donde se encuentra almacenada la información, atentando contra su confidencialidad, integridad y disponibilidad.*"

Teniendo en cuenta el factor de seguridad que comprometen, las amenazas se pueden clasificar en cuatro grupos: (Mifsud, 2012).

- **Interceptación:** Cuando un elemento no autorizado consigue acceso al sistema.

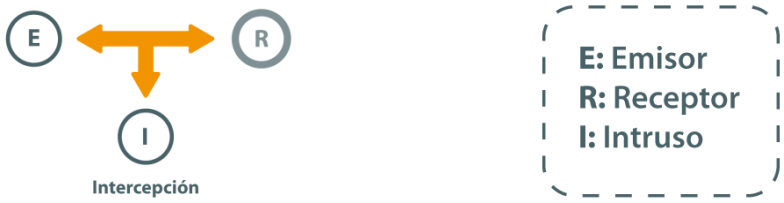


Imagen 2: Interceptación.

- **Modificación:** Un elemento no autorizado, además de acceder a la información, la modifica.

Imagen 3: Modificación

- **Interrupción:** Tiene como objetivo deshabilitar el acceso a la información.

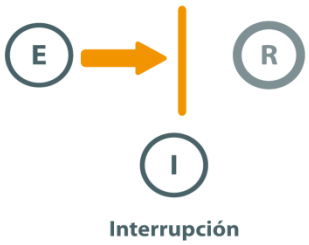


Imagen 4: Interrupción

- **Fabricación:** Se agrega información falsa consiguiendo un objeto similar al atacado.

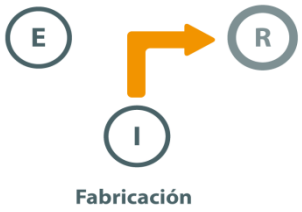


Imagen 5: Fabricación

Las amenazas pueden ser de tipo Humanas, físicas y lógicas y se describen a continuación según (Reyes, 2012).

Humanas

Las personas son el factor que representan el mayor número de amenazas o ataques, ya sea con intención o sin ella, en ocasiones un individuo realiza acciones indebidas por falta de conocimiento, por simple diversión o con la intención de causar algún daño. A continuación, se listan algunos casos que corresponden a este tipo de amenazas:

- Ingeniería social
- Trashing (cartoneo)
- Terroristas
- Robo
- Intrusos remunerados
- Personal interno
- Exempleados

- Curiosos
- Crackers

Físicas

Este tipo de ataque comprende las amenazas ocasionadas tanto por el hombre como por la naturaleza. Según las principales amenazas de este tipo son:

- Incendios
- Inundaciones
- Terremotos
- Señales de radar
- Instalaciones eléctricas

Lógicas

En este tipo de amenazas se encuentran una gran variedad de programas que, de una u otra forma, dañan los sistemas creados de manera intencionada (software malicioso conocido como malware) o simplemente por error (bugs o agujeros). Las amenazas más comunes son:

- Adware
- Backdoors
- Cabayos de troya
- Bómbas lógicas
- Exploits
- Gusanos (worms)
- Malware
- Pharming
- Phishing
- Spam
- Spyware

- Virus

2.1.2 Vulnerabilidades

Son debilidades o fallos en un sistema de información que ponen en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, las vulnerabilidades son condiciones y características propias de los sistemas de una organización que la hacen susceptible a las amenazas. Estos "agujeros" pueden tener distintos orígenes, por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos. (Incibe, 2017).

Las organizaciones están expuestas a diversos tipos de vulnerabilidades, a continuación, se describen las principales: (Cols, 2011).

- **Vulnerabilidades físicas:** Están presentes en los ambientes en los cuales se almacena la información como instalaciones de trabajo o centros de cómputo. Este tipo de vulnerabilidades afecta los principios básicos de la información, en especial la disponibilidad.
- **Vulnerabilidades naturales:** Son aquellas relacionadas con las condiciones de la naturaleza que pueden poner en riesgo la información, como incendios, inundaciones, terremotos, huracanes, entre otros.
- **Vulnerabilidades de hardware:** Se refiere a los posibles defectos de fábrica o a la mala configuración de los equipos de cómputo de la empresa que puedan permitir un ataque o alteración de éstos.
- **Vulnerabilidades de software:** Se relaciona con la mala programación, diseño, instalación y configuración de los programas de computadora, y el acceso indebido a los sistemas informáticos.
- **Vulnerabilidades de medios de almacenaje:** Comprende los soportes físicos o magnéticos que se utilizan para almacenar la información como los disquetes, cd, cintas magnéticas, discos duros, entre otros, que si se usan de manera inadecuada

podrían ser vulnerables a diversos factores que afecten la integridad, confidencialidad y disponibilidad de la información.

- **Vulnerabilidades de comunicación:** Se refiere al tránsito de la información, ya sea vía cable, satélite, fibra óptica u ondas de radio, cualquier vulnerabilidad a estos medios de comunicación afectarían los principios básicos de la seguridad informática.
- **Vulnerabilidades humanas:** Se refiere a los daños que las personas puedan causar a la información y al ambiente tecnológico que la soporta sea de manera intencional o no. La principal vulnerabilidad es la falta de capacitación y la falta de conciencia de seguridad para las actividades de rutina, los errores, omisiones, etc. También existen las vulnerabilidades humanas de origen externo, como son; el vandalismo, estafas, invasiones, etc.

2.2 INFORMÁTICA FORENSE

Los criminales informáticos se han vuelto cada vez más expertos a medida que la tecnología avanza, debido a esto los investigadores han visto la necesidad de crear técnicas que permitan recuperar, preservar, analizar datos o recolectar evidencia de un crimen informático.

Según (Acurio, 2009) las Ciencias Forenses son procedimientos y conocimientos científicos utilizados para encontrar, adquirir, preservar y analizar la evidencia de un crimen para ser presentados ante un Tribunal. El objetivo principal de las ciencias forenses es la recuperación y el análisis de la evidencia latente, como huellas dactilares, comparación de muestras de ADN, etc.

(Pagés, 2013) Define la Informática Forense como "una disciplina criminalística que tiene como objeto la investigación en sistemas informáticos de hechos con relevancia jurídica o para la simple investigación privada".

Por su parte (Sandoval & Vaca, 2013) la definen como el proceso de investigar dispositivos no solo informáticos, por medio de técnicas y métodos con el fin de descubrir y analizar información disponible, suprimida u oculta que pueda servir como evidencia en un asunto

legal.

(Zuccardi & Gutiérrez, 2006) Mencionan tres objetivos importantes de la informática forense:

1. La compensación de los daños causados por los criminales o intrusos.
2. La persecución y procesamiento judicial de los criminales.
3. La creación y aplicación de medidas para prevenir casos similares.

2.3 TIPOS DE ANÁLISIS FORENSE

"Tenemos que tener en cuenta que las memorias RAM en la actualidad son capaces de gestionar gigabytes de datos, y esto, es una gran cantidad de datos e información a estudiar." (Gomez, 2016).

Para realizar un adecuado análisis forense, se requieren herramientas y conocimientos específicos. Hay dos modos de realizar análisis forense:

Análisis en caliente: También llamado análisis On Line, se realiza cuando el equipo está todavía encendido y/o el ataque está siendo ejecutado. Este tipo de análisis es de vital importancia, ya que permite recolectar mayor cantidad de información como los datos volátiles. (López M. , 2007) Menciona un orden de volatilidad descrito en el RFC 3227 muy útil en el momento de recolectar evidencias:

- Registros y contenidos de la caché.
- Contenidos de la memoria.
- Estado de las conexiones de red, tablas de rutas.
- Estado de los procesos en ejecución.
- Contenido del sistema de archivos y de los discos duros.
- Contenido de otros dispositivos de almacenamiento.

Y añade que será muy importante también recuperar datos del sistema en tiempo real como: Fecha y hora, procesos activos, conexiones de red, puertos TCP/UDP abiertos y aplicaciones asociadas "a la escucha", usuarios conectados remota y localmente.

Análisis en frio o post-mortem: Se realiza sobre una copia de la evidencia original, que se ha extraído del sistema cuando este se ha parado o se ha encontrado en ese estado. Permite realizar un análisis más exhaustivo y menos intrusivo con la evidencia original (al trabajar sobre una copia idéntica no se alteran las pruebas originales), pero perdiendo la información volátil si esta no se ha podido extraer antes del sistema a analizar. En ciertos ataques puede ser que no obtengamos toda la información posible debido a la volatilidad de ciertas pruebas, que desaparecen al parar el sistema, pero se puede trabajar más a fondo que en los análisis en caliente, realizando algunas operaciones que no serían posibles de otra forma. (La huella oculta, 2014).

Dependiendo del punto de vista nos vamos a encontrar diferentes tipos de análisis forense. Si lo vemos desde el punto de vista de lo que se va a analizar, nos encontraremos los siguientes tipos: (Rifà, Serra, & Rivas, 2009).

• **Análisis forense de sistemas:** en este análisis se tratarán los incidentes de seguridad acaecidos en servidores y estaciones de trabajo con los sistemas operativos: Mac OS, sistemas operativos de Microsoft (Windows 9X/Me, Windows 2000 server/workstation, Windows 2003 Server, Windows XP, Windows Vista, Windows 2008 Server, etc.), sistemas Unix (Sun OS, SCO Unix, etc.) y sistemas GNU/Linux (Debian, RedHat,Suse, etc.).

• **Análisis forense de redes**: en este tipo se engloba el análisis de diferentes redes (cableadas, wireless, bluetooth, etc.).

• **Análisis forense de sistemas embebidos:** en dicho tipo se analizarán incidentes acaecidos en móviles, PDA, etc. Un sistema embebido posee una arquitectura semejante a la de un ordenador personal.

2.4 FASES DE ANÁLISIS FORENSE

Según (Piedrahita, 2014) Las fases del análisis forense son los procedimientos que siguen los investigadores profesionales para un correcto procedimiento forense.

Basado en las definiciones de (Chala, 2015), la siguiente figura muestra los pasos que se deben seguir para un adecuado análisis forense.

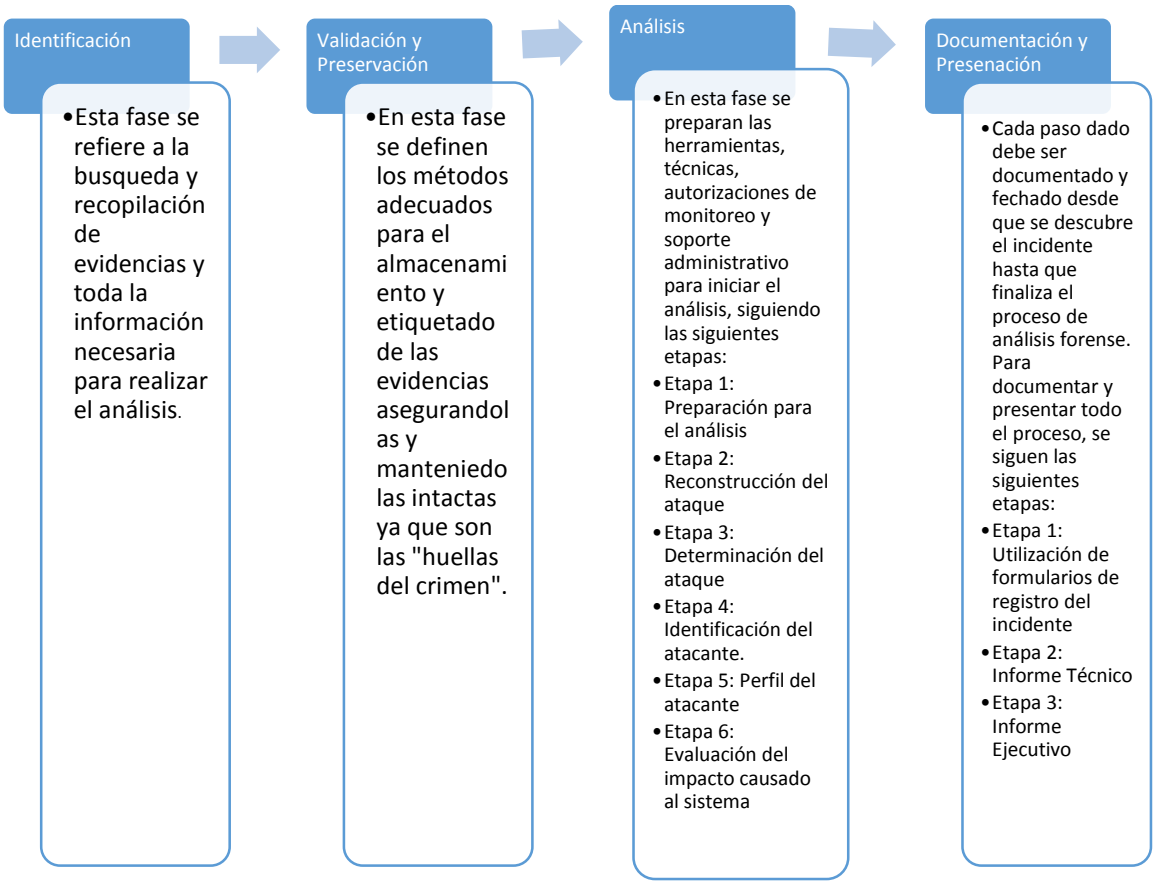


Imagen 6: Pasos para un análisis forense

2.5 LA EVIDENCIA DIGITAL

(Cano J. , 2003) La define como "tipo de evidencia física construida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales".

En su definición, (Beltrán, s,f) sostiene que la evidencia digital es un tipo de evidencia menos tangible que las demás, la cual puede ser duplicada de tal manera que sea idéntica a la original y aun cuando es alterada o eliminada se puede recuperar con las herramientas adecuadas.

Se puede decir entonces que la evidencia digital está conformada por datos, documentos y/o cualquier tipo de información almacenada en medios digitales y que puede ser utilizada

como valor probatorio para la solución de un delito.

Es importante recordar, como lo mencionan (López, Amaya, & León, 2013) que los datos digitales que se obtienen de copias, no deben ser alterados de los originales del disco, porque la evidencia perdería su validez; por esto los investigadores deben revisar con frecuencia que sus copias sean exactas a las del disco del sospechoso por medio de técnicas especiales como las Técnicas de Hashing como checksums o hash MD5.

La IOCE (International Organization On Computer Evidence) define los siguientes cinco puntos como los principios para el manejo y recolección de evidencia computacional: (López, Amaya, & León, 2013).

1. Sobre recolectar evidencia digital, las acciones tomadas no deben cambiar por ningún motivo esta evidencia.
2. Cuando es necesario que una persona tenga acceso a evidencia digital original, esa persona debe ser un profesional forense.
3. Toda la actividad referente a la recolección, el acceso, almacenamiento o a la transferencia de la evidencia digital, debe ser documentada completamente, preservada y disponible para la revisión.
4. Un individuo es responsable de todas las acciones tomadas con respecto a la evidencia digital mientras que ésta esté en su posesión.
5. Cualquier agencia que sea responsable de recolectar, tener acceso, almacenar o transferir evidencia digital es responsable de cumplir con estos principios.

Este manejo de evidencia digital se realiza mediante un conjunto de pasos o procedimientos seguidos conocido como “Cadena de Custodia”, de modo que permita convertirla y usarla como prueba en un proceso judicial.

2.5.1 Fuentes de la evidencia digital

(Acurio, 2009) Sostiene que para que los investigadores forenses sepan dónde buscar evidencia digital, deben identificar las fuentes más comunes, además afirma que dichas fuentes se clasifican en tres grandes grupos:

- **Sistemas de computación abiertos:** son aquellos que están compuestos de los llamados computadores personales y todos sus periféricos como teclados, ratones y monitores, las computadoras portátiles, y los servidores.
- **Sistemas de comunicación:** Estos están compuestos por las redes de telecomunicaciones, la comunicación inalámbrica y el Internet.
- **Sistemas convergentes de computación** Son los que están formados por los teléfonos celulares llamados inteligentes o SMARTPHONES, los asistentes personales digitales PDAs, las tarjetas inteligentes y cualquier otro aparato electrónico que posea convergencia digital y que puede contener evidencia digital.

2.5.2 Clasificación de la evidencia digital

(Mosquera, Certain, & Cano, 2005) Basado en el estándar norteamericano de "searching and seizing computers and obtaining electronic evidence in criminal investigations", afirma que la evidencia digital se clasifica en tres categorías:

- **Registros generados por computador:** Son los registros que se generan por la programación de un computador y los cuales no pueden ser alterados por el hombre. Estos archivos son: archivos de registro (log files), registros telefónicos, registros de transacciones bancarias, informes de datos de SWIFT, donde no hay afirmaciones generados por humanos sino por sistemas o computadores.
- **Registros no generados sino simplemente almacenados por o en computadores: S**on los registros creados por una persona y almacenados en un formato electrónico, como correos electrónicos, escritos o información generados por procesadores de palabras, etc. Es muy importante demostrar la identidad de quién genera este tipo de registros, vinculándolo directamente a la creación de los datos.
- **Registros híbridos que incluyen tanto registros generados por computador como almacenados en los mismos:** Es una combinación de registros que incluyen tanto los generados por computador como los generados por el hombre, para hacer valer estos registros como prueba se debe cumplir con los dos requisitos anteriormente mencionados.

2.5.3 Características de la evidencia digital

(Santos, 2013) Menciona los siguientes elementos de la evidencia digital que hacen un desafío para los investigadores forenses:

- volátil
- anónima
- duplicable
- alterable y modificable
- eliminable

Además de esto indica las características que mitigan el problema generado por las personas involucradas en un crimen cuando éstas intentan manipular y alterar la evidencia digital:

- La evidencia digital puede ser duplicada de forma exacta y se puede sacar una copia para ser examinada como si fuera la original. Esto se hace comúnmente para no manejar los originales y evitar el riesgo de dañarlos.
- Actualmente con los instrumentos existentes, es muy fácil comparar la evidencia digital con su original, y determinar si la evidencia digital ha sido alterada.
- La evidencia digital es muy difícil de eliminar. Aun cuando un registro es borrado del disco duro del computador, y éste ha sido formateado, es posible recuperarlo.
- Cuando los individuos involucrados en un crimen tratan de destruir la evidencia, existen copias que permanecen en otros sitios.

2.5.4 Criterios de admisibilidad

(Cano J. J., 2003) Afirma que las legislaciones y las instituciones de justicia han fundado sus reflexiones sobre la admisibilidad de la evidencia en cuatro conceptos, que a continuación se detallan:

a. **Autenticidad:** La autenticidad es entendida como aquella característica que muestra la no alterabilidad de los medios originales y busca confirmar que los

registros aportados correspondan a la realidad evidenciada en la fase de identificación y recolección.

b. Confiabilidad: Es otro factor relevante para asegurar la admisibilidad de la misma. La confiabilidad nos dice si, efectivamente, los elementos probatorios aportados vienen de fuentes que son creíbles y verificables y que sustentan elementos de la defensa o del fiscal en el proceso que se sigue.

c. Suficiencia: Es la presencia de toda la evidencia necesaria para adelantar el caso; esta característica, al igual que las anteriores, es factor crítico de éxito en las investigaciones adelantadas en procesos judiciales. Con frecuencia, la falta de pruebas o insuficiencia de elementos probatorios ocasiona la dilación o terminación de procesos que podrían haberse resuelto.

d. Conformidad con las leyes y reglas de la administración de justicia: Hace referencia a los procedimientos internacionalmente aceptados para recolección, aseguramiento, análisis y reporte de la evidencia digital.

2.5.5 Manipulación de la evidencia digital

Es importante tener presente los siguientes requisitos que se deben cumplir en cuanto a la manipulación de la evidencia digital. Informática Forense. (Zuccardi & Gutiérrez, 2006)

- Hacer uso de medios forenses estériles (para copias de información).
- Mantener y controlar la integridad del medio original. Esto significa, que a la hora de recolectar la evidencia digital, las acciones realizadas no deben cambiar nunca esta evidencia.
- Cuando sea necesario que una persona tenga acceso a evidencia digital forense, esa persona debe ser un profesional forense.

- Las copias de los datos obtenidas deben estar correctamente marcadas, controladas y preservadas. Y al igual que los resultados de la investigación, deben estar disponibles para su revisión.
- Siempre que la evidencia digital este en poder de algún individuo, éste será responsable de todas las acciones tomadas con respecto a ella, mientras esté en su poder.
- Las agencias responsables de llevar el proceso de recolección y análisis de la evidencia digital serán quienes deben garantizar el cumplimiento de los principios anteriores.

2.6 LA CADENA DE CUSTODIA

La cadena de custodia es el conjunto de pasos o procedimientos de control que debe seguirse para preservar la prueba digital de manera que pueda usarse como evidencia en un juicio.

Consideramos la cadena de custodia como un procedimiento controlado que se aplica a los indicios materiales (prueba indiciaria) relacionados con un hecho delictivo o no, desde su localización hasta su valoración, por parte de los encargados de administrar justicia y que busca asegurar la inocuidad y la esterilidad técnica en el manejo de los mismos, evitando alteraciones, sustituciones, contaminaciones o destrucciones, hasta su disposición definitiva por orden judicial. (Arellano & Castañeda, 2012).

La cadena de custodia debe: (Fernández, 2004).

- Reducir al máximo la cantidad de agentes implicados en el manejo o tratamiento de evidencias.
- Mantener la identidad de las personas implicadas desde la obtención hasta la presentación de las evidencias.
- Asegurar la inmutabilidad de las evidencias en los traspasos de estas entre agentes.
- Registros de tiempos, firmados por los agentes, en los intercambios entre estos de las evidencias. Cada uno de ellos se hará responsable de las evidencias en cada momento.

- Asegurar la inmutabilidad de las evidencias cuando las evidencias están almacenadas asegurando su protección.

(Fernández, 2004), indica que la cadena de custodia tiene la siguiente secuencia:

- Recolección e identificación.
- Análisis.
- Almacenamiento.
- Preservación.
- Transporte.
- Presentación en el juzgado.
- Retorno a su dueño.

La cadena de custodia de la evidencia muestra quién la obtuvo, dónde y cuándo fue obtenida, quien la protegió y quien ha tenido acceso a esa evidencia.

2.7 HISTORIA DE LA INFORMÁTICA FORENSE

El campo de la informática forense se inició en la década de 1980, poco después de que las computadoras personales se convirtieran en una opción viable para los consumidores. En 1984, fue creado un programa del FBI. Conocido por un tiempo como el Programa de Medios Magnéticos, que ahora se conoce como CART (CART, del inglés computer analysis and response team), o análisis de informática y equipo de respuesta. Poco después, el hombre al que se le atribuye ser el "padre de la informática forense", comenzó a trabajar en este campo. Su nombre era Michael Anderson, y era un agente especial de la División de Investigación Criminal del IRS (Internal Revenue Service). Anderson trabajó para el gobierno en esta capacidad hasta mediados de 1990, tras lo cual fundó New Technologies, Inc., un equipo que lleva la firma forense (Guerra, 2014).

2.7.1 Plan cronológico de la informática forense

A continuación se presentan los acontecimientos más importantes en la evolución de la informática forense a través de los años, según (Villamil, 2014), (TimeToast, 2017) y (El

Pais, 2017).

Tabla 1: Historia de la informática forense

Año	Acontecimiento
1984	Se creó el Programa de Medios Magnéticos del FBI, que ahora se conoce como CART (computer analysis and response team).
1993	Se celebra la primera Conferencia Internacional sobre la Evidencia Digital.
1995	Se formó la Organización Internacional de Evidencia Digital (IOCE).
1997	En diciembre, los países del G8 en Moscú declararon que "los funcionarios encargados de hacer cumplir la ley deben estar capacitados y equipados para hacer frente a los delitos de alta tecnología.".
1998	Desde marzo de este año, la función principal de la IOCE fue realizar una lista de principios internacionales de los procedimientos relacionados con la evidencia digital. Se realizó el lanzamiento del libro Proceedings of the 12th Interpol Forensic Science Symposium.
1999	El programa CART del FBI abordó 2000 casos individuales a través del análisis de 17 terabytes de datos.
2000	El FBI estableció el primer laboratorio de Informática Forense, el RCFL por primera vez en San Diego, y hoy hay 16 laboratorios patrocinados por la oficina ubicada en todo el país, integrada por agentes y otras autoridades federales, estatales y agencias locales de aplicación de la ley.
2003	El trabajo total del FBI en casos forenses informáticos excede 6500, a través del análisis de 782 terabytes de datos.
2004	Un ingeniero de la compañía que había sido despedido utilizó sus conocimientos de la empresa para infiltrarse en la red interna de AOL, y robar la lista con los correos de sus 92 millones de usuarios. Después

	vendió la lista online a un grupo de spammers.
2005	El gran hack de EE.UU no afectó a una sola compañía, sino a una larga lista de ellas que incluía el índice bursátil NASDAQ, 7-Eleven, JC. Penney, JetBlue, Dow Jones o Global Payment entre otras. El ataque se prolongó durante siete años, y robo los datos de tarjetas bancarias de 160 millones de clientes.
2007	En enero de 2007, responsables del grupo TJX hicieron público un ataque informático que puso en peligro los datos bancarios de 94 millones de clientes entre sus cadenas de tiendas Marshals, Maxx y T.J.
2008	El hacker Albert González fue acusado de coordinar el ataque que se llevó datos de 130 millones de tarjetas de débito y crédito de la multinacional de pagos Heartland Payment Systems. Sucedió en 2008, pero no se hizo público hasta mayo de 2009.
2009	Un disco duro que se envió a un servicio técnico en 2009 fue el punto por el que se robaron 76 millones de fichas personales de veteranos de guerra estadounidenses, incluyendo sus números de la seguridad social.
2013	En marzo de 2013, Evernote envió una notificación a sus usuarios para que cambiaran sus contraseñas ante indicios de que su red había sido hackeada. No se reportó robó de información personal. La medida fue cautelar. Este es de los pocos casos en los que la compañía reaccionó tan rápido que no hubo que lamentar daños. En noviembre el 2013 el ataque a la cadena de tiendas estadounidense Target fue especialmente peligroso porque que los hackers se llevaron números de tarjeta bancaria y claves de 40 millones de personas que utilizaron sus tarjetas en alguna tienda Target a finales de 2013. Otros 30 millones de usuarios vieron vulnerados datos personales como el teléfono o la dirección de email.
2014	El asalto a la base de datos de usuarios de la página de comercio online

	eBay ha obligado a cambiar sus contraseñas a 145 millones de personas. Aún no se ha podido calcular el volumen de la información filtrada. En diciembre de 2014 un ataque robó información de las cuentas de 77 millones de usuarios de los servicios PlayStation en todo el mundo, Sony tuvo que compensar a los usuarios y recibió varias sanciones en países como Reino Unido.
2017	El virus, conocido como ransomware, afectó, entre otros, a los equipos de la sede de Telefónica en Madrid, al sistema de salud británico o el ministerio del Interior ruso. En un tuit, Costin Raiu, el director global del equipo de investigación y análisis de Kaspersky Lab, empresa de seguridad informática, estimó que ayer se habían registrado más de 45.000 ataques en 74 países

2.8 HERRAMIENTAS DE INFORMÁTICA FORENSE

Las herramientas forenses son programas, aplicaciones o hardware con los que un investigador forense puede explorar un ordenador de forma completa. Cada herramienta es creada y diseñada para una o varias funciones determinadas, y por tanto podemos hablar de muchos tipos de herramientas forenses según la función que realicen.

El uso de herramientas sofisticadas se hace necesario debido a: (López, Amaya, & León, 2013).

- La gran cantidad de datos que pueden estar almacenados en un computador.
- La variedad de formatos de archivos, los cuales pueden variar enormemente, aún dentro del contexto de un mismo sistema operativo.
- La necesidad de recopilar la información de una manera exacta, y que permita verificar que la copia es exacta.
- Limitaciones de tiempo para analizar toda la información.
- Facilidad para borrar archivos de computadores.
- Mecanismos de inscripción, o de contraseñas.

Las herramientas informáticas forenses se pueden clasificar en varias categorías: (Ghirardi, 2017).

- Herramientas de captura de datos y discos
- Visualizadores de archivos
- Herramientas de análisis de archivos
- Herramientas de análisis de registro
- Herramientas de análisis de Internet
- Herramientas de análisis de correo electrónico
- Herramientas de análisis de dispositivos móviles
- Herramientas de análisis de Memoria
- Herramientas forenses de la red
- Herramientas forenses de base de datos

A continuación, se realizará una descripción de los diferentes tipos de herramientas empleadas en el análisis forense para la recolección de información tanto de software propietario, como de software libre, enfatizando en estas últimas dado que es el objetivo central de la investigación.

Las siguientes son algunas de las herramientas utilizadas en el análisis forense:

EnCase

EnCase Forensic le permite buscar, identificar y priorizar rápidamente la evidencia potencial para determinar si se justifica una investigación más profunda, puede recopilar de una amplia variedad de sistemas operativos y de archivos, incluidos dispositivos móviles. EnCase Forensic está diseñado pensando en el investigador, ofreciendo una amplia gama de capacidades que le permiten realizar análisis forenses profundos, así como análisis de triaje rápido desde la misma solución. EnCase Forensic proporciona un marco de informes flexible que le da la oportunidad de adaptar informes de casos para satisfacer sus necesidades específicas. (Guidance Software, 2017).

Dd (Duplicate DisK)

Herramienta incluida en distribuciones Unix/Linux, que se ejecuta mediante la terminal de comandos y se utiliza para clonar o copiar información bit a bit del disco duro, o también para copiar particiones o discos completos unos sobre otros.

Esta sencilla pero poderosa herramienta, también tiene la capacidad de crear imágenes completas de disco, para que luego puedan ser analizadas como evidencia (Diaz & Usme, 2011).

Los sistemas de Unix tratan a todos los dispositivos como archivos y estos archivos de dispositivos se encuentran en el directorio / dev de su sistema. Por lo tanto, típicamente su unidad de disco duro es un archivo en el directorio / dev con el prefijo hd o sd (dependiendo del controlador IDE o SCSI). Este concepto de dispositivo como archivos hace que dd sea un candidato perfecto para realizar copias de seguridad y restaurar imágenes de discos o clonar algunas particiones o todo el disco. (Tech Guides, 2018).

Air (Imagen y Restauración Automática)

AIR (Automated Image & Restore) es una aplicación de código abierto que proporciona una interfaz gráfica de usuario al comando dd/dcfldd (Dataset Definition (dd)). AIR está diseñado para crear fácilmente imágenes forenses de disco/partición. Es compatible con hashes MD5/SHAx, unidades de cinta SCSI, imágenes a través de una red TCP/IP, división de imágenes y registro de sesión detallado. En su forma más simple, AIR proporciona una interfaz conveniente para ejecutar el conjunto dd de comandos. Elimina el riesgo de "digitación de grasa" un error en el terminal de shell y, en última instancia hace que el uso del comando dd sea más fácil de usar para aquellos que no tienen tanta experiencia. Tenga en cuenta que el uso de la interfaz AIR todavía requiere algunos conocimientos básicos sobre cómo funcionan los comandos dd (o dcfldd). (HowtoForge, 2017).

AIR tiene las siguientes características:

- Autodetección de discos IDE y SCSI, CD-ROMs, y unidades de cinta
- Opción de elegir entre dd o dc3dd

- Verificación de imágenes entre fuente y copia vía MD5 o SHA1/256/384/512
- Compresión/descompresión de imagen vía gzip/bzip2
- Soporte a unidades de cinta SCSI
- División de imágenes en múltiples segmentos

(Mesa, 2015).

The Forensic ToolKit (FTK)

Es una plataforma de investigaciones digitales citada por la corte construida para velocidad, estabilidad y facilidad de uso. Le ayuda a encontrar evidencias relevantes más rápidamente, aumenta drásticamente la velocidad de análisis y reduce los atrasos. Además, debido a su arquitectura, FTK puede ser configurado para procesamiento distribuido e incorporar la gestión de casos basada en la web y el análisis colaborativo. (AccessData, 2017).

Este ToolKit (conjunto de herramientas) le permitirá recopilar información sobre el ataque, se compone de una serie aplicaciones en línea de comandos que permiten generar diversos informes y estadísticas del sistema de archivos a estudiar (López M. , 2007).

Sirve para procesar datos de archivos de correo electrónico, analizar el registro. Llevar a cabo una investigación, descifrar archivos, descifrar contraseñas y elaborar un informe de todos con una sola solución (TechnologyINT, 2014).

FTK Imager

FTK Imager es una herramienta de previsualización e imagen de datos que le permite evaluar rápidamente la evidencia electrónica para determinar si se justifica el análisis posterior con una herramienta forense como AccessData Forensic Toolkit (FTK). FTK Imager también puede crear copias perfectas (imágenes forenses) de datos de computadora sin hacer cambios a la evidencia original. (AccessData, 2017).

Es importante mencionar el uso de un bloqueador de escritura al utilizar FTK Imager para crear la imagen forense desde un disco duro u otro dispositivo electrónico. Esto asegura que el sistema operativo no alterará la unidad fuente original cuando se le adjunte a la computadora.

Para prevenir la manipulación accidental o intencional de la evidencia original, FTK Imager realizar una imagen duplicado bit a bit del medio. La imagen forense es idéntica en cualquier forma al original, incluyendo espacio de holgura o residual y espacio sin asignar o espacio libre de la unidad. Esto permite almacenar el medio original en un lugar seguro de daño mientras se procede con la investigación utilizando la imagen forense. (Caballero, 2014).

Coroner's Toolkit, TCT

TCT es un conjunto de herramientas forenses de código abierto para realizar análisis post-mortem en sistemas Unix. Este producto está destinado a usuarios experimentados de Unix, existe una comprensión implícita de las funciones y convenciones comunes de Unix, creación de archivos, páginas man, utilidades, etc.

El uso de un programa forense de línea de comando puede ser difícil, aunque los analistas forenses que han usado las Herramientas NTI anteriores se sentirán como en casa. (SC Media, 2018).

TCT es una colección de herramientas principalmente utilizada en la recolección de grandes cantidades de datos para proceder a su análisis posterior. Algunos de sus componentes son las herramientas que restaura y recupera archivos borrados, también la restauración de claves criptográficas desde un proceso activo o desde algún archivo. Este kit de herramientas ha sido diseñado principalmente en ambientes Unix, Solarix, Linux, (Arismendi, 2015).

Las aplicaciones más importantes de la suite son:

- **grave-robber:** Una utilidad para capturar información sobre i-nodes, para luego pueda ser procesada por el programa mactime del mismo toolkit.
- **unrm y Lazarus:** Herramientas para la recuperación de archivos borrados (logs, RAM, swap, etc.). Estas aplicaciones identifican y recuperan la información oculta en los sectores del disco duro.
- **Mactime:** El programa para visualizar los ficheros/directorios su timestamp MAC (Modification, Access, y Change). (Dittrich, David, 2018).

Foremost

Foremost es un programa de consola para recuperar archivos basados en sus encabezados, pies de página y estructuras de datos internas. Este proceso se conoce comúnmente como tallado de datos. Foremost puede trabajar en archivos de imagen, como los generados por dd, Safeback, Encase, etc, o directamente en una unidad. Los encabezados y pies de página se pueden especificar mediante un archivo de configuración o puede utilizar parámetros de línea de comandos para especificar tipos de archivo incorporados. Estos tipos integrados miran las estructuras de datos de un formato de archivo dado permitiendo una recuperación más fiable y más rápida. (Foremost SourceForge, 2017).

Foremost permite recuperar una gran variedad de formatos: avi, bmp, dll, doc, docx, exe, gif, htm, jar, jpg, mbd, mov, mp4, mpg, ole, pdf, png, ppt, pptx, rar, rif, sdw, sx, sxc, sxi, sxw, vis, wav, wmv, xls, xlsx, zip. (Cultura Geek, 2014).

Hachoir-Metadata

Es un marco genérico para la manipulación de archivos binarios. Escrito en Python, es independiente del sistema operativo y tiene muchas interfaces de usuario de texto / gráfico. Aunque contiene algunas funciones para modificar archivos, por lo general está destinado a examinar archivos existentes. Hachoir actualmente admite más de sesenta formatos de archivo. El reconocimiento de formato de archivo se basa en los encabezados y pies de página en una imagen de archivo de disco. Tiene un analizador tolerante a errores diseñado para manejar archivos truncados o con errores. El marco también se ajusta automáticamente para problemas de endian o juego de caracteres. El marco puede ser escrito y extendido.

El paquete incluye varios programas de muestra basados en el marco central y el analizador:

hachoir-metadata: extraer metadatos

hachoir-strip: eliminar metadatos y otras informaciones "inútiles"

hachoir-grep: encuentre la subcadena en un archivo binario (usando los analizadores de hachoir: para que la búsqueda tenga conocimiento de Unicode)

hachoir-subfile: encuentra todos los subarchivos en un archivo. (Forensicswiki, 2012).

Al extraer la información de un metadato de un archivo se puede adquirir evidencia como nombre, tamaño, tipo de dato, estructura, ubicación etc. Su principal característica es la propiedad de dividir los archivos binarios en campos con una cantidad más pequeña de bit, lo que permite recabar aún más profundamente en la evidencia encontrada (Diaz & Usme, 2011).

Ddrescue

Es una herramienta de recuperación de datos. Copia datos de un archivo o dispositivo de bloque (disco duro, cdrom, etc.) a otro, tratando de rescatar primero las partes buenas en caso de errores de lectura.

La operación básica de ddrescue es completamente automática. Es decir, no tiene que esperar un error, detener el programa, reiniciarlo desde una nueva posición, etc.

Si utiliza la función mapfile de ddrescue, los datos se rescatan de manera muy eficiente (solo se leen los bloques necesarios). También puede interrumpir el rescate en cualquier momento y reanudarlo más tarde en el mismo punto. El archivo de mapa es una parte esencial de la efectividad de ddrescue. Úselo a menos que sepa lo que está haciendo.

El archivo de mapa se guarda periódicamente en el disco. Entonces, en caso de un accidente, puede reanudar el rescate con poca copia.

Además, el mismo archivo de mapa se puede usar para múltiples comandos que copian diferentes áreas del archivo y para múltiples intentos de recuperación en diferentes subconjuntos.

Una de las mayores fortalezas de ddrescue es que es independiente de la interfaz y, por lo tanto, puede utilizarse para cualquier tipo de dispositivo compatible con su núcleo (ATA, SATA, SCSI, unidades MFM antiguas, disquetes o incluso tarjetas multimedia flash como SD). (Gnu, 2018).

OSForensic

Es una aplicación que incluye un conjunto de utilidades para hacer análisis forenses, tales como búsqueda de avanzada de ficheros, creación y búsqueda en un índice, ficheros eliminados, obtención de contraseñas, creación de imagen forense, entre otras. (Escolar, 2014).

R-Studio

R-STUDIO es la solución más completa de recuperación de datos para los archivos de recuperación de particiones. También utiliza la recuperación de archivos en bruto (exploración para detectar tipos de archivo conocidos) para sistemas de archivos muy dañados o desconocidos. Funciona en discos locales y de red, incluso si dichas particiones están formateadas, dañadas o borradas (R-Tools Technology Inc, 2017).

R-Studio Agent

Es una herramienta potente y práctica que trabaja en conjunto con el programa R-Studio y es capaz de crear conexiones remotas a través de la red con el propósito poder recuperar los archivos (R-Tools Technology Inc, 2017).

E-Detective.

E-detective es un sistema de interceptación de Internet en tiempo real, el seguimiento y análisis forense que captura, decodifica y reconstruye diversos tipos de tráfico de Internet. Se utiliza comúnmente para Internet organización y seguimiento del comportamiento, auditoría, registro, análisis forense y de investigación, así como la interceptación legal y lícito a los organismos de aplicación legales, tales como información de la policía, de Inteligencia Militar, Departamento de Seguridad Cibernética, agencias de seguridad nacional, penales organismos de investigación , Contra Terrorismo Agencias etc. (Dicision Group, 2011).

Paraben

Es una de las herramientas de examen de correo electrónico válida a efectos legales más completos disponibles. Es un examinador de correo electrónico que permite analizar encabezados de los mensajes, los cuerpos y archivos adjuntos, recupera correo electrónico borrado de elementos eliminados (Paraben Corporation, 2017).

The Sleuth Kit y Autopsy

The Sleuth Kit es una colección de herramientas de línea de comandos y una biblioteca C que le permite analizar imágenes de disco y recuperar archivos de ellas. Autopsy es una plataforma forense digital e interfaz gráfica para The Sleuth Kit y otras herramientas forenses digitales. Es utilizado por los encargados de hacer cumplir la ley, militares, y examinadores corporativos para investigar qué sucedió en una computadora. Incluso puede utilizarlo para recuperar fotos de la tarjeta de memoria de su cámara.

Autopsy es un programa fácil de usar, basado en GUI que le permite analizar de manera eficiente discos duros y teléfonos inteligentes. Tiene una arquitectura de plug-in que le permite encontrar módulos complementarios o desarrollar módulos personalizados en Java o Python.

Algunas de las características de Autopsy

- **Casos multiusuario:** colabore con otros examinadores en casos grandes.
- **Análisis de línea de tiempo:** muestra los eventos del sistema en una interfaz gráfica para ayudar a identificar la actividad.
- **Búsqueda de palabras clave:** la extracción de texto y los módulos de búsqueda de índice le permiten buscar archivos que mencionan términos específicos y encontrar patrones de expresiones regulares.
- **Artefactos web:** extrae la actividad web de los navegadores comunes para ayudar a identificar la actividad del usuario.
- **Análisis del registro:** utiliza RegRipper para identificar los documentos y dispositivos USB a los que se accedió recientemente.
- **Análisis de archivos LNK:** identifica accesos directos y documentos accedidos

- **Análisis de correo electrónico**: analiza mensajes en formato MBOX, como Thunderbird.
- **EXIF:** extrae la ubicación geográfica y la información de la cámara de archivos JPEG.
- **Clasificación de tipo de archivo**: agrupe los archivos por su tipo para encontrar todas las imágenes o documentos.
- **Análisis robusto del sistema de archivos:** Admite sistemas de archivos comunes, incluidos NTFS, FAT12 / FAT16 / FAT32 / ExFAT, HFS +, ISO9660 (CD-ROM), Ext2 / Ext3 / Ext4, Yaffs2 y UFS de The Sleuth Kit.

Entre otras. (Sleuthkit, 2017).

ExifTool

Es una herramienta de línea de comandos capaz de leer y editar los metadatos de una amplia variedad de formatos de imágenes, así como archivos de música, videos o texto. ExifTool dispone de una gran cantidad de funciones para la lectura y escritura de metadatos. Se destaca su capacidad para editar completamente la información EXIF (Exchangeable image file format) de una foto obtenida con una cámara digital, permitiendo cambiar las fechas de modificación o los datos de geoposición muy fácilmente. (ExifTool, 2017).

Algunas de sus características según (Harvey, 2018).

- Potente, rápido, flexible y personalizable
- Admite una gran cantidad de formatos de archivos diferentes
- Lee EXIF, GPS, IPTC, XMP, JFIF, MakerNotes, GeoTIFF, perfil ICC, Photoshop IRB, FlashPix, AFCP, ID3 y más.
- Escribe EXIF, GPS, IPTC, XMP, JFIF, MakerNotes, GeoTIFF, perfil ICC, Photoshop IRB, AFCP y más.
- Lee y escribe notas del fabricante de muchas cámaras digitales
- Lee los metadatos cronometrados (por ejemplo, la pista GPS) de los videos MOV / MP4 / M2TS / AVI

- Procesa árboles de directorios completos
- Crea archivo de salida de texto para cada archivo de imagen
- Realiza una copia de seguridad automática de la imagen original al escribir
- Organiza la salida en grupos.

Helix CD

Se trata de un Live CD de respuesta ante incidentes, basado en una distribución Linux denominada *Knoppix* (que a su vez está basada en Debian). Posee la mayoría de las herramientas necesarias para realizar un análisis forense tanto de equipos como de imágenes (López M. , 2007).

Algunas herramientas que contiene son: wireshark, varios antivirus, recuperadores de contraseña, copias de seguridad y restauración de particiones, navegador de particiones MAC, examinador de archivos binarios, entre otros. (Mesa, 2015).

F.I.R.E. Linux

Es una distribución basada en cdrom portátil, con el objetivo de proporcionar un entorno inmediato para realizar análisis forenses, respuesta a incidentes, recuperación de datos, análisis de virus y evaluación de vulnerabilidades. También proporciona las herramientas necesarias para el análisis forense en caliente en hosts win32, sparc solaris y x86 linux simplemente montando el cdrom. (Biatchux Dmzs, 2017).

Hetman software

Es un software que recupera Ficheros eliminados accidentalmente, Papelera de reciclaje vaciada, discos duros formateados y reparticionados, ataques de virus y sistemas de ficheros dañados. herramientas están diseñadas específicamente para realizar el proceso de recuperación de datos de forma completamente segura. soportando la creación de imágenes de unidad virtual y permitiendo guardar su información en cualquier medio de almacenamiento local o remoto. Es muy fácil de usar ya que contiene un asistente interactivo le guiará paso a paso, en el completo proceso de recuperación.

(Hetman Software, 2016).

WinHex

Software para informática forense y recuperación de archivos, Editor hexadecimal de Archivos. Apropiado también para peritaje informático, procesamiento de datos de bajo nivel y seguridad informática. Inspecciona archivos binarios, recupera datos borrados o perdidos en unidades dañadas. Un editor hexadecimal es capaz de mostrar completamente el contenido de cada tipo de archivo. A diferencia de un editor de texto, uno hexadecimal incluso muestra los códigos de control y el código ejecutable, usando un número de dos dígitos basado en el sistema de numeración hexadecimal (Espinoza, 2009).

TestDisk

Es una herramienta gratuita para la recuperación de datos, esta fue diseñada principalmente para ayudar a recuperar particiones perdidas o dañadas, o volver discos no booteables a booteables cuando estos síntomas son causados por fallas de software, por virus o algún error humano (que por equivocación borra la tabla de particiones)

TestDisk tiene características para expertos y principiantes. Para aquellos que saben poco o nada sobre técnicas de recuperación de datos, TestDisk puede ser usado para recolectar información detallada sobre un disco que no bootea, la cual después puede ser enviada a un técnico para mayor análisis. Aquellos más familiarizados con dichos procedimientos pueden encontrar en TestDisk una herramienta útil para realizar recuperación de datos on-site.

TestDisk puede ahcer los siguiente

- Arreglar la Tabla de Particiones, recuperar particiones eliminadas
- Recuperar sectores de booteo FAT32 de su copia de respaldo
- Reconstruir sectores de booteo FAT12/FAT16/FAT32
- Arreglar tablas de booteo de tipo FAT
- Reconstruir sectores de booteo NTFS
- Recuperar sectores de booteo NTFS de su copia de respaldo

- Arreglas la MFT usando la MFT mirror
- Localizar el Superblock de copia de respaldo de ext2/ext3
- Recuperar archivos de sistemas de archivos FAT, NTFS y ext2
- Copiar archivos de particiones FAT, NTFS y ext2/ext3 eliminadas (Dragonjar, 2018).

Digital Forensics Framework

Es una herramienta de investigación forense digital y una plataforma de desarrollo que le permite recoger, preservar y revelar la evidencia digital. Entre otras, las funciones del DFF incluyen la capacidad de leer RAW, EWF y AFF formatos de archivos forenses, acceder a los dispositivos locales y remotos, analizar los datos del registro, buzón y del sistema de archivos y recuperar archivos ocultos y eliminados (Toolwar, 2013).

Las carcteristicas de DFF según (Github, 2018).

- Monta particiones, sistemas de archivos y extrae metadatos de archivos y otra información útil de forma automática.
- Genera un informe HTML con actividad de sistema y usuario
- Dispositivos directos que leen soporte
- Formatos de archivo de imagen forense admitidos: AFF, E01, Ex01, L01, Lx01, dd, sin procesar, bin, img
- Volúmenes admitidos y sistemas de archivos con espacio no asignado, elementos eliminados, espacio libre: DOS, GPT, VMDK, Volume Shadow Copy, NTFS, HFS, HFSX, EXT2, EXT3, EXT4, FAT12, FAT16, FAT32
- Buzones de correo de Outlook y Echange (PAB, PST, OST)
- Historial del navegador: Firefox, Chrome, Opera
- Análisis de memoria volátil con interfaz gráfica para Volatility
- Generación de videos en miniatura
- Soporte para Sqlite, Registro de Windows, Evt y Evtx
- Análisis completo de Skype (Sqlite y antiguo formato DDB)
- Hashset admite etiquetado automático "conocido malo", "conocido bueno"

PC Inspector file recovery

Es una herramienta para recuperar archivos y rescatar datos eliminados, datos perdidos e incluso unidades perdidas. Posee además la función especial de recuperación, que salva los archivos que no tienen ninguna indicación de directorio. También ofrece una guía de ayuda y la posibilidad de cambiar el idioma. Reconstruye también los datos en los que no exista posible indicación del directorio al que pertenecen.

Estas son algunas de las características de la herramienta:

- Encuentra particiones automáticamente, incluso si el sector de arranque o FAT se ha borrado o dañado
- Recupera archivos con la marca de fecha y hora original
- Admite el almacenamiento de archivos recuperados en unidades de red
- Recupera archivos, incluso cuando una entrada de encabezado ya no está disponible. La "Función de recuperación especial" admite los siguientes formatos de disco: ARJ, AVI, BMP, CDR, DOC, DXF, DBF, XLS, EXE, GIF, HLP, HTML, HTM, JPG, LZH, MID, MOV, MP3, PDF, PNG, RTF, TAR, TIF, WAV y ZIP.

Está disponible de manera gratuita. (Pc Inspector, 2017)

Disk Recovery

DiskRecovery busca archivos que se borraron accidentalmente o se perdieron a causa de una falla o un error del software. A continuación, reconstruye y recupera los archivos de forma rápida y sencilla. Escanea todo el disco duro, la partición o el dispositivo USB para detectar archivos perdidos, fotos, videos, archivos de música y muchos otros tipos de datos antes de reconstruirlos y recuperarlos. También puede llevar a cabo la recuperación de la tarjeta SD. Es eminentemente fácil de usar con un asistente paso a paso que le dice cómo recuperar los archivos eliminados, haciendo que la recuperación de datos sea simple incluso para usuarios con poca o ninguna experiencia. (O&O Software, 2018).

GetDataBack

Herramienta para la recuperación de archivos en dispositivos extraíbles, aunque Windows no lo reconozca como unidad, o se haya perdido toda la información de estructura de directorios. Recupera información de memorias sin formato, todo tipo de datos, aunque el borrado se haya realizado hace tiempo. No sin antes saber qué sistema de archivos es, NTFS o FAT (Quituisaca, 2010).

Remo Recuperar

Es una herramienta considerada de las mejores aplicaciones para rescatar información, recuperación de archivos perdidos/borrados. Se desarrolla con gran variedad de opciones de recuperación para que no sólo rescate los datos del disco duro del ordenador, sino también restaura archivos desde unidades de almacenamiento como tarjetas de memoria flash, unidades USB. Remo Recover es una herramienta ideal para recuperar datos perdidos o eliminados del pendrive, independientemente de la situación de pérdida de datos. Es segura y confiable para recuperar datos. Este software funciona con éxito en todo el sistema operativo Windows (Remo Software, 2017).

Wondershare Data Recovery

Es un software efectivo para recuperación de datos en ordenadores y dispositivos de almacenamiento, recupera vídeos, fotos, emails, música y documentos perdidos en el disco duro, así como en memorias USB y otros dispositivos de almacenamiento, recupera archivos en más de 550 formatos de forma rápida, segura y completa (WonderShare, 2017).

Undelete 360

Undelete 360 es un software de recuperación de datos que puede recuperar efectivamente archivos borrados debido a muchas razones como errores humanos, infección de troyanos, fallas de software o hardware, cierre inesperado del sistema. El programa funciona directamente con medios de almacenamiento como disco duro, unidad flash, unidad externa USB, ZIP, unidades Firewire, tarjeta de cámara digital y más.

Los resultados del escaneo se muestran tanto en un tipo de archivo como en una vista de carpeta. Puede obtener una vista previa de los archivos antes de la recuperación y eso le ayuda a encontrar los archivos de destino en poco tiempo. La función de filtro permite a los usuarios realizar una búsqueda de ciertos archivos en lugar de escanear todo el volumen. También puede recuperar archivos comprimidos y cifrados eliminados en unidades NTFS.
Undelete 360 recupera archivos de todo tipo, incluidos: DOC, XLS, RTF, PDF, PPT, MDB, HTML, CSV, TXT, PAS, CPP, EML, archivos de audio y video: AVI, MP3, WAV, WMA, MPG, MOV, ASF, archivos de imagen: JPEG, JPG, PNG, BMP, GIF, TIF, TGA, EML, RAW, y así sucesivamente. (Undelete360, 2017).

2.8.1 Herramientas para el Monitoreo y/o Control de Computadores

Algunas veces se necesita información sobre el uso de los computadores, por lo tanto, existen herramientas que monitorean el uso de los computadores para poder recolectar información. Existen algunos programas simples como *key loggers* o recolectores de pulsaciones del teclado, que guardan información sobre las teclas que son presionadas, hasta otros que guardan imágenes de la pantalla que ve el usuario del computador, o hasta casos donde la máquina es controlada remotamente.
Existe gran cantidad de keyloggers, a continuación, se presentan algunos de los más destacados:

Spytech SpyAgent:

Es un poderoso software de espionaje de computadoras que le permite monitorear TODOS los usuarios en su computadora en total sigilo. SpyAgent proporciona una gran variedad de funciones esenciales de monitoreo de computadoras, así como bloqueo de sitios web, aplicaciones y chat, registro de logs y entrega remota de registros por correo electrónico o FTP. (Spytech-Web, 2017).

Elite Keylogger:

Este programa supervisa y captura todas las pulsaciones de teclado. Además de eso, es

capaz de tomar imágenes, registra la actividad de Internet (sitios web visitados) y la memoria del portapapeles. (TOPAttack, 2017).

Refog Personal Monitor:

Funciona de modo silencioso y desapercibido en su PC a la hora de hacer capturas de pantalla, registrar cada tecla presionada, guardar la información sobre las aplicaciones usadas y sitios web visitados. Usted puede acceder a estos registros localmente o remotamente en cualquier momento aun cuando no está en casa. (Refog, 2017).

Revealer Keylogger:

Permite grabar todas las pulsaciones en un equipo determinado. Cuenta con una interfaz muy limpia, donde se puede ver todos los datos grabados: palabras clave introducidas y los títulos de las ventanas (TOPAttack, 2017).

2.8.2 Herramientas de Marcado de documentos

Un aspecto interesante es el de marcado de documentos; en los casos de robo de información, es posible, mediante el uso de herramientas, marcar software para poder detectarlo fácilmente. Básicamente el objetivo de este tipo de herramientas es el de insertar una marca a la información sensible para poder detectar el robo o tráfico con la misma, si bien no equivale al sistema LoJack de rastreo y localización de vehículos hurtados, si podría compararse con las marcas que se hace a los vehículos. (Romo & Ramiro, 2011).

Existe una gran variedad de herramientas para realizar este proceso de inserción de marcas de agua digitales, entre ellas:

Adobe Photoshop:

Es un software de tratamiento de imágenes el cual utiliza la tecnología Digimarc para la inserción de marcas de agua digitales. Además de esto, Digimarc también realiza el proceso en archivos de audio, video y en documentos digitales. (Adobe, 2017).

WatermarkIt:

Solo permite las marcas de agua digitales en imágenes y fotos. Esta herramienta inserta una marca de agua en las fotos, es decir, un texto que identifica la imagen en cuestión como propia, poniéndole un texto personal o un mensaje de copyright. WatermarkIt cuenta con varias opciones a la hora de "marcar" las fotos: personalizar el texto, seleccionar tipo de letra y color, elegir su ubicación en la imagen, añadir efectos como sombra o transparencia, etc. (Watermarkit, 2017).

Sandmark:

Esta herramienta protege al software de la piratería, la manipulación y la ingeniería inversa. La meta del software es la de desarrollar técnicas que les permitan a los usuarios determinar empíricamente cuales algoritmos para la inserción de marcas de agua digitales tienen el mejor rendimiento y la mayor resistencia a ataques. Sandmark en realidad es un framework que está diseñado para la implementación y evaluación de técnicas como las marcas de agua digitales. (Sandmark, 2017).

2.8.3 Herramientas de Hardware

Debido a que el proceso de recolección de evidencia debe ser preciso y no debe modificar la información, se han diseñado varias herramientas de hardware como:

- DIBS "Portable Evidence Recovery Unit".
- Un equipo portable "F.R.E.D.D.I.E", (Forensic Recovery of Evidence Device Diminutive Interrogation Equipment)
- Conjunto portable de duplicación de discos.
- Impresora portable, inalámbrica.
- Soporte inalámbrico para todos los dispositivos del kit
- Dispositivos varios.
- USBDeview (Para análisis de USB). Permite saber que dispositivos USB perconectan con una PC, estén conectados o no. Da tipo de dispositivo, número de serie y fecha. (Martinez Rivera, 2013).

Nota: Estas herramientas no se describen en el presente trabajo ya que no hacen parte fundamental de la tesis.

2.8.4 Herramientas para recuperar contraseñas

Las contraseñas son un sistema de protección usado por muchos sitios web, programas de mensajería y herramientas ofimáticas. Recolectar las claves existentes permite rescatar mucha información valiosa (GITSinformatica, 2003).

A continuación, se describen algunas herramientas utilizadas para la recuperación de contraseñas.

Fuerza Bruta

Un ataque de fuerza bruta es un método de ensayo y error usado para obtener información, tal como una clave de acceso o el PIN (Número de Identificación Personal). En un ataque de fuerza bruta, se emplea software automatizado para generar una lista larga de posibles contraseñas de acceso, para ingresarlas en la cuenta de un usuario objetivo. Los ataques de fuerza bruta pueden ser usados por los criminales para "crackear" o descubrir datos encriptados, o por analistas de seguridad para probar la seguridad de la red de una organización. (Dtyoc, 2015).

Browser Password Decryptor.

Es un software gratuito para recuperar instantáneamente las contraseñas de inicio de sesión de sitios web. Actualmente puede recuperar las contraseñas de acceso guardadas en los siguientes navegadores:

Firefox, Google Chrome, Microsoft Edge, Internet Explorer, UC Browser, Torch Browser, Google Chrome Canary/SXS, CoolNovo Browser, Opera Browser, Apple Safari, Comodo Dragon Browser, SeaMonkey Browser, SRWare Iron Browser, Flock Browser. (Security X Ploded, 2017).

Mail PassView

Es una pequeña herramienta de recuperación de contraseñas que revela las contraseñas y

otros detalles de la cuenta para los siguientes clientes de correo electrónico: Outlook Express Microsoft Outlook 2000 (POP3 and SMTP Accounts only), Microsoft Outlook 2002/2003/2007/2010/2013/2016 (POP3, IMAP, HTTP and SMTP Accounts), Windows Mail, Windows Live Mail, IncrediMail y Eudora. (Nirsoft, 2016).

AsteriskKey

Es un software gratuito que revela contraseñas ocultas bajo asteriscos. Revela las contraseñas ocultas en los cuadros de diálogo y las páginas web. Recuperación de la contraseña de inicio. Soporte completo para contraseñas multilingües Fácil de usar Fácil de configurar. (Passware, 2017).

WirelessKeyDump.

Es una aplicación de consola (Command Prompt) que descarga la lista de todas las claves inalámbricas almacenadas por el módulo de redes inalámbricas del sistema operativo Windows. (Nirsoft, 2011).

Ntpwedit

Es un editor de contraseña para los sistemas basados en Windows NT (como Windows 2000, XP, Vista, 7 y 8), se puede cambiar o eliminar las contraseñas de cuentas de sistema local. No valido para Active Directory. (Theoven, 2017).

SecurityXploded

Tienen muchas herramientas dedicadas exclusivamente a la recuperación de contraseñas, casi todas ejecutables desde memorias USB. Conviene recordar que solo obtienen contraseñas almacenadas sin protección y que para romper el cifrado es necesario recurrir a ataques criptográficos. (Security X Ploded, 2017).

2.8.5 Herramientas de Adquisición y análisis de la memoria

Set de utilidades que permite la adquisición de los datos presentes en la memoria RAM

para posteriormente hacer un análisis con ella. (Conexioninversa, 2011).

A continuación, se describirán algunas herramientas utilizadas para la adquisición y análisis de la memoria RAM.

Process Dump

Process Dump es una herramienta de línea de comandos de ingeniería inversa de Windows para volcar los componentes de memoria maliciosa en el disco para su análisis. Process Dump funciona para sistemas operativos Windows de 32 y 64 bits y puede volcar componentes de memoria de procesos específicos o de todos los procesos que se estén ejecutando actualmente. Process Dump admite la creación y el uso de una base de datos limpia-hash, por lo que se puede omitir el volcado de todos los archivos limpios como kernel32.dll.

Sus características principales incluyen:

- Volcado código de un proceso específico o todos los procesos.
- Encuentra y descarga módulos ocultos que no están cargados correctamente en los procesos.
- Encuentra y descarga fragmentos de código sueltos, incluso si no están asociados con un archivo PE. Construye un encabezado PE e importa la tabla para los fragmentos.
- Reconstruye las importaciones usando un enfoque agresivo.
- Puede ejecutarse en el modo de monitor de vuelco cerrado ('-closemon'), donde los procesos se pausarán y se descartarán justo antes de que finalicen.
- Multi-threaded, por lo que cuando está descargando todos los procesos en ejecución, irá bastante rápido.
- Puede generar una base de datos limpia de hash. Genere esto antes de que una máquina se infecte con malware, por lo que Process Dump solo volcará los nuevos componentes maliciosos maliciosos. (Github, 2017).

DumpIt

Esta utilidad se usa para generar un volcado de memoria física de máquinas con Windows. Funciona con máquinas x86 (32 bits) y x64 (64 bits). El volcado de memoria sin procesar se genera en el directorio actual, solo se solicita una pregunta de confirmación antes de comenzar. Perfecto para desplegar el ejecutable en llaves USB, para necesidades de respuestas rápidas a incidentes. (Hacking Articles, 2014).

Volatility

El Volatility Framework es una colección completamente abierta de herramientas, Implementado en Python bajo la Licencia Pública General GNU, para la Extracción de artefactos digitales de muestras de memoria volátil (RAM). Las técnicas de extracción se realizan completamente independientemente a la del sistema que se está investigando, pero ofrecen visibilidad en el estado de ejecución.

Características de Volatility

- Analiza los volcados de RAM de Windows 32 y 64 bits, sistemas Linux, Mac y Android. El diseño modular de Volatility le permite soportar fácilmente nuevos sistemas operativos y arquitecturas a medida que se lanzan.
- Es Open Source GPLv2, lo que significa que puedes leerlo, aprender de él y ampliarlo.
- Está escrito en Python, un lenguaje forense y de ingeniería inversa establecido con muchas bibliotecas que pueden integrarse fácilmente en Volatility.
- La API extensible y programable le da el poder de ir más allá y continuar innovando. Por ejemplo, puede usar la volatilidad para crear una interfaz web o GUI personalizada, manejar su entorno de prueba de malware, realizar una introspección de la máquina virtual o simplemente explorar la memoria del núcleo de manera automatizada.
- Volatility proporciona capacidades que el propio depurador de kernel de Microsoft no permite, como historiales de comandos de talla, búferes de entrada / salida de

consola, objetos USER (memoria GUI) y estructuras de datos relacionadas con la red. El hecho de que no esté documentado no significa que no puedas analizarlo.

- Volatility puede analizar volcados sin procesar, volcados de emergencia, archivos de hibernación, VMware. vmem, archivos de estado y suspendidos de VMware (.vmss / .vmsn), volcados de núcleo de VirtualBox, LiME (Extractor de memoria de Linux), testigo experto (EWF) y memoria física directa a través de Firewire.
- Los algoritmos rápidos y eficientes le permiten analizar los volcados de memoria RAM de los sistemas de gran tamaño sin gastos generales innecesarios ni consumo de memoria. Por ejemplo, volatility puede enumerar los módulos del núcleo de un sistema de 80 GB en solo unos segundos. Siempre hay margen de mejora, y el tiempo varía según el comando, sin embargo, otros marcos de análisis de memoria pueden tardar varias horas en hacer lo mismo en volcados de memoria mucho más pequeños.
- Volatility fue diseñado por expertos forenses, de respuesta a incidentes y de malware para centrarse en los tipos de tareas que suelen formar estos analistas.
- Volatility también está siendo desarrollada por una serie de grandes organizaciones como Google, National DoD Laboratories, DC3 y muchas tiendas de antivirus y seguridad.

(Github, 2017).

RedLine

Esta Herramienta proporciona capacidades de investigación a los usuarios para detectar signos de actividad maliciosa mediante el análisis de memoria y archivos y el desarrollo de un perfil de evaluación de amenazas. Con redline se puede auditar y recopilar exhaustivamente todos los procesos y controladores en ejecución de la memoria, los metadatos del sistema de archivos, los datos de registro, los registros de eventos, la información de red, los servicios, las tareas y el historial web.

Redline, permite:

- Realizar una auditoría exhaustiva y recopilar todos los procesos y controladores en ejecución desde la memoria, los metadatos del sistema de archivos, los datos del registro, los registros de eventos, la información de red, los servicios, las tareas y el historial web.
- Analizar y ver los datos de auditoría importados, incluida la capacidad de filtrar los resultados en un plazo determinado utilizando la funcionalidad Línea de tiempo de Redline con las funciones TimeWrinkle y TimeCrunch.
- Agilizar el análisis de memoria con un flujo de trabajo comprobado para analizar malware basado en prioridad relativa.
- Realizar análisis de Indicadores de Compromiso (IOC). Suministrado con un conjunto de IOC, el Agente portátil de Redline se configura automáticamente para reunir los datos necesarios para realizar el análisis de IOC y una revisión de IOC.

(Fireeye, 2017).

Responder pro

Responder PRO permite a los profesionales de respuesta a incidentes recolectar y analizar residuos de ataque y artefactos de la memoria. Los usuarios pueden aprovechar la información que se encuentra en la memoria física para validar incidentes de seguridad y profundizar para determinar la causa raíz y el impacto potencial. Los forenses y los ingenieros inversos pueden escanear fragmentos de documentos, historial de Internet, y las claves y contraseñas se extraen automáticamente de la memoria y se ponen a disposición. (Countertack, 2017).

Memoryze

Es un software forense libre para la memoria RAM que ayuda a los que responden a los incidentes a encontrar el mal en la memoria en caliente. Memoryze puede adquirir y/o analizar imágenes de memoria y en sistemas en caliente puede incluir el archivo de paginación en su análisis.

Características de Memoryze:

- Imagine el rango completo de la memoria del sistema (sin dependencia de las llamadas API).
- Imagen de un espacio de direcciones completo del proceso en el disco, que incluye un proceso de archivos DLL, EXEs, montones y pilas cargados.
- Imagen de un controlador especificado o todos los controladores cargados en la memoria en el disco.
- Enumera todos los procesos en ejecución (incluidos los ocultos por los rootkits).
- Identifica todos los controladores cargados en la memoria, incluidos los ocultos por los rootkits.
- Informe el dispositivo y las capas del controlador, que se pueden usar para interceptar paquetes de red, pulsaciones de teclas y actividad de archivos.
- Identifica todos los módulos kernel cargados al recorrer una lista vinculada. Identifica los enlaces (a menudo utilizados por los rootkits) en la tabla de llamadas del sistema, las tablas de descriptores de interrupción (IDT) y las tablas de funciones del controlador.

(Fireeye, 2017).

WinPmem

Es una herramienta de adquisición de memoria forense de código abierto, desarrollada activamente, para Windows. Si no se especifica ninguna otra operación, WinPmem imitará inmediatamente la memoria y también adquirirá ciertos archivos, como los controladores y la imagen del kernel. Es útil para conservar las versiones exactas de los binarios que se ejecutan en el sistema en el momento de la adquisición. Por defecto WinPmem utiliza una técnica llamada PTA Remapping para adquirir memoria. Esta técnica fue desarrollada originalmente para evitar el malware potencial que engancha las APIs usadas normalmente para la adquisición. (Cohen, 2013).

Winpmem es una fantástica herramienta que surge del proyecto Rekall para analizar la memoria RAM. Winpmem permite obtener la memoria RAM principalmente con el

formato AFF4, un formato que realmente es un contenedor zip, donde se puede almacenar más información a parte del volcado de la memoria RAM.

Además de poder usar el formato AAF4 y poder llevarse en un único fichero varias evidencias, también permite usar el formato RAW como con DumpIt u otras herramientas. (Jaume, 2018).

LiME (Linux Memory Extractor)

Permite la adquisición de memoria volátil de dispositivos basados en Linux. Esto hace que LiME sea único, ya que es la primera herramienta que permite realizar capturas de memoria completas en dispositivos Android. También minimiza su interacción entre los procesos del usuario y del espacio del kernel durante la adquisición, lo que le permite producir capturas de memoria que son más forenses que las de otras herramientas diseñadas para la adquisición de la memoria de Linux.

Son caracteristicas de LiME:

- Adquisición total de memoria Android
- Adquisición sobre la interfaz de red
- Huella mínima del proceso
- Hash de memoria objeto de dumping.

(Github, 2017).

Volatilitux

Volatilitux es un framework Python que ayuda a extraer artefactos digitales de volcados de memoria física (RAM) de sistemas Linux. El objetivo de esta herramienta es ofrecer una herramienta en un campo que carece cruelmente de herramientas.

Estas son las principales características de la herramienta:

- Detección automática de compensaciones de estructura de kernel
- Detección manual de esas compensaciones utilizando un Módulo de kernel cargable
- Admite varias arquitecturas: ARM, x86, x86 con PAE habilitado

- Se puede usar como un módulo de Python para automatizar tareas y ser integrado con otros proyectos

A diferencia de Volatility, solo es compatible con un conjunto restringido de comandos:

- pslist: imprime la lista de todos los procesos
- memmap: imprime el mapa de memoria de un proceso
- memdmp: volcar la memoria direccionable de un proceso
- filedmp: volcar un archivo abierto
- filelist: imprime la lista de todos los archivos abiertos para un proceso determinado

Ha sido probado en volcados de memoria física de las siguientes distribuciones de Linux: Android 2.1, Fedora 5 y 8, Debian 5, CentOS 5, Ubuntu con y sin PAE. (Segmentation fault, 2017).

Crash de Red Hat

La utilidad de análisis de fallos de Red Hat se basa libremente en el comando de bloqueo SVR4 UNIX, pero se ha mejorado significativamente al fusionarla por completo con el depurador GNU gdb. El matrimonio de los dos combina eficazmente la naturaleza específica del kernel de la utilidad de bloqueo de UNIX tradicional con las capacidades de depuración del nivel de código fuente de gdb. La utilidad se puede usar para investigar:

- Sistemas Live Linux
- Vaciados de núcleo del kernel de Linux creados por la instalación de Kdump
- Volcados del núcleo kernel comprimidos de Linux creados por el comando makedumpfile (desde kdump dumpfiles)
- Volcados del núcleo del kernel de Linux creados por las instalaciones de Red Hat Netdump
- Vaciados de núcleos de kernel de Linux creados por la instalación de Red Hat Diskdump
- Volcados del núcleo del kernel de Linux comprimido creados por la instalación de Red Hat Diskdump

- Volcados del núcleo del kernel de Linux invitados Xen creados por la instalación xendump original
- Volcados del kernel Linux kernel invitado Xen creados por la instalación xendump formato ELF
- Volcados del núcleo del hipervisor Xen creados por las instalaciones de Kdump
- Volcados de núcleos de kernel de Linux invitados de KVM creados por la instalación de volcado de virsh
- volcados del núcleo del kernel de Linux s390x creados por el recurso de volcado de núcleo independiente de IBM.
- Volcados del núcleo del kernel de Linux creados por el proyecto Sourceforge de LKCD (Linux Kernel Crash Dumps)
- Volcados del kernel Linux kernel creados por el parche Mcore ofrecido por Mission Critical Linux

La utilidad de bloqueo está diseñada para ser independiente de las dependencias de la versión de Linux. Cuando el nuevo código fuente del kernel impacta en la funcionalidad correcta de crash y su conjunto de comandos, la utilidad se actualizará para reconocer nuevos cambios en el código del kernel y mantener la compatibilidad con versiones anteriores. (PeopleRedhat, 2015)

Foriana

Esta herramienta es útil para la extracción de información de procesos y listas de módulos desde una imagen de la RAM con la ayuda de las relaciones lógicas entre las estructuras del sistema operativo (HackPlayers, 2017).

Desarrollada por Ivor Kollár como parte de su tesis de maestria. Básicamente se trata de una herramienta para el análisis de volcados de memoria de sistemas linux que no se basa en patrones, por lo que supuestamente funcionaría con cualquier tipo de sistema/kernel linux origen. Integrado en dicha herramienta se incluye un lkm (o Loadable Kernel Module) que crea un nuevo dispositivo (/dev/fmem) el cual permite acceder directamente a la memoria y, por lo tanto, obtener un volcado de la misma utilizando dd, tal como antes de

la rama 2.6 del kernel era posible hacer utilizando el dispositivo virtual /dev/mem. (Neo System Forensics, 2012).

Forensic Analysis Toolkit (FATKit)

FATKit es un marco modular que permite a los que responden a incidentes extraer, analizar, agregar y visualizar datos forenses en los diversos niveles de complejidad de datos inherentes a la memoria del sistema. El diseño de FATKit se centra en el concepto de definir abstracciones del sistema y crear módulos para implementar la funcionalidad necesaria en cada nivel de abstracción, como la memoria física, la memoria virtual, las estructuras de datos del programa y la interpretación de datos específicos de la aplicación. Este enfoque estratificado permite a los expertos razonar desde el punto de vista de una abstracción particular (por ejemplo, el espacio de direcciones virtuales de un proceso particular) y hacer que esos datos estén disponibles para análisis de mayor nivel.

FATKit permite a los analistas centrarse en tareas de mayor nivel al proporcionar métodos novedosos para derivar automáticamente definiciones de objetos digitales del código fuente C, extraer esos objetos de imágenes de memoria y visualizar los datos subyacentes de varias maneras. FATKit actualmente incluye módulos para la reconstrucción y visualización general del espacio de direcciones virtuales, así como para el análisis del kernel específico de Linux y Windows. (PetroniJr, Walters, Fraser, & Arbaugh, 2006).

FATKit incluye las siguientes características:

- Soporte para espacios de direcciones virtuales basados en x86 y tipos de datos nativos.
- Análisis kernel específicos de Linux y Windows que incluyen enumeración de procesos / tareas, enumeración de módulos y detección de códigos maliciosos residentes en la memoria.
- El sistema de tipo basado en perfiles permite asignar tipos de bajo nivel a construcciones de mayor nivel y distribuirlos para diversas compilaciones de software.

- Las herramientas automatizadas de generación de perfiles permiten la extracción de formatos de objetos de bajo nivel cuando el código fuente está disponible.
- Los módulos de análisis por script permiten a los analistas implementar fácilmente técnicas de extracción especializadas o patentadas utilizando un lenguaje de alto nivel, en lugar de rutinas codificadas a mano.
- El diseño modular permite la fácil extensión a nuevas arquitecturas y sistemas operativos.
- El buscador de objetos FATKit permite a los analistas interpretar objetos de memoria binaria en el nivel de abstracción del lenguaje de alto nivel del código fuente. Con el soporte actual para aplicaciones escritas en el lenguaje de programación C, el navegador permite a los analistas expandir y colapsar objetos en memoria y sus campos anidados, seguir punteros y lanzar objetos a otros formatos de datos.
- El Visor de espacios de direcciones FATKit permite a los analistas visualizar los datos tal como aparecen en un espacio de direcciones virtuales o físicas en particular. El Address Space Viewer también se integra con el Object Browser para permitir vistas múltiples y consistentes de los mismos datos de bajo nivel.

(DarkNessgate, 2016).

Puran File Recovery

Herramienta para recuperar archivos / particiones eliminados / perdidos. Los archivos también se pueden recuperar desde discos formateados. Casi todo lo que Windows detecta como unidad de disco puede analizarse independientemente de su sistema de archivos. Ya sean discos duros, pen drive, tarjetas de memoria, teléfonos móviles, CD, DVD, básicamente cualquier medio de almacenamiento.

Características principales:

- Una interfaz muy simple con un motor de recuperación extremadamente potente. Una perfecta combinación de velocidad, precisión y simplicidad.
- Una exploración rápida que enumera los archivos eliminados en un clic y unos segundos. Es compatible con FAT12 / 16/32 y NTFS.
- Una exploración profunda que puede escanear de forma inteligente un byte a byte de la unidad, lo que da como resultado un listado de alta velocidad de muchos más archivos eliminados y perdidos.
- Una exploración completa que puede detectar particiones eliminadas / eliminadas e incluso recuperar archivos de unidades formateadas. Las unidades RAW y físicas también se pueden escanear.
- Deep / Full Scan no solo busca registros de archivos perdidos, sino que también detecta archivos de diferentes formatos basados en patrones de datos.
- Se incluyen más de 50 formatos / listas de patrones de datos ampliables a cientos de formatos. De ahí que casi todo se pueda recuperar.
- En muchos casos, se mostrarán las rutas completas de los archivos eliminados. Este es el caso de las unidades formateadas también.
- Los archivos recuperados se pueden guardar con su estructura de ruta intacta.
- Los archivos se enumeran en árbol y vistas de lista. Todos los archivos se pueden previsualizar antes de la recuperación.
- Un cuadro de búsqueda que admite comodines le permite localizar rápidamente sus archivos eliminados.
- También está disponible una versión portátil oficial que incluso puede ejecutarse en el entorno BartPE.
- Puran File Recovery es compatible con Windows XP / 2003 / Vista / 2008/7/8/10, incluidas las versiones de 64 bits.

Gratuita solo para uso privado y no comercial. (Puran Software, 2013).

2.8.6 Herramientas de Montaje de Discos

Utilidades para montar imágenes de disco o virtualizar unidades de forma que se tenga acceso al sistema de ficheros para posteriormente analizarla.

Algunas herramientas utilizadas para el montaje de discos son:

ImDisk

ImDisk es un controlador de disco virtual para Windows NT / 2000 / XP / Vista / 7/8 / 8.1 / 10 y Windows Server 2003/2003 R2 / 2008/2008 R2 / 2012/2012 R2, ediciones de 32 y 64 bits. Puede crear discos duros virtuales, disquetes o unidades de CD / DVD usando archivos de imagen o memoria del sistema. El paquete de instalación instala un programa de control en modo consola llamado imdisk.exe y un applet del Panel de control. El controlador ImDisk admite el reenvío de solicitudes de E / S a manejadores de formato de archivo de imagen de terceros o a servicios en otras computadoras en la red. Esto permite iniciar una máquina con particiones NTFS con un Live-CD y usar la herramienta devio incluida para permitir que ImDisk en otra computadora con Windows en la red monte la partición NTFS en la máquina con una partición NTFS defectuosa. De esta manera puede recuperar información e incluso ejecutar chkdsk en unidades en máquinas donde Windows no arranca.

ImDisk Toolkit ofrece funciones como la creación automática de discos de memoria al inicio del sistema y el montaje de muchos formatos de archivos de imágenes diferentes. (LTR Data logo, 2018) (LTR Data logo, 2018).

OSFMount

Es una herramienta que permite montar archivos de imagen de disco local (copias bit a bit de una partición de disco) en Windows con una letra de unidad. Los archivos de imagen se montan como de sólo lectura para que no se alteren los archivos originales. (Osforensics, 2017).

Raw2vmdk

Es una utilidad de Java independiente del sistema operativo que le permite montar imágenes de disco sin formato, como imágenes creadas por "dd", utilizando VMware, VirtualBox o cualquier otra plataforma de virtualización que admita el formato de disco VMDK.

Es una herramienta interesante para hacer exámenes forenses en cajas comprometidas cuando todo lo que tienes es un volcado de la unidad para trabajar, te permite montar fácilmente el disco en tu plataforma de virtualización favorita y ponerte a trabajar haciendo un análisis forense.

Analiza la imagen sin procesar y crea un archivo ".vmdk" formateado apropiadamente que se puede usar para montar la imagen de inmediato.

Raw2vmdk está escrito en Java y está diseñado para ser independiente del sistema operativo, simple y flexible. Crea un archivo VMDK adecuadamente estructurado que hace referencia a la imagen sin procesar, que luego puede ser montada por VMware, VirtualBox o cualquier otra plataforma de virtualización que admita el formato de disco VMDK, como si fuera una unidad virtual real. De esta forma, se preserva el espacio y se permite un despliegue muy rápido. Es extremadamente simple de usar y proporciona los resultados requeridos en segundos. (Darknet, 2017).

LiveView

Live View es una herramienta gráfica forense basada en Java que crea una máquina virtual VMware a partir de una imagen de disco sin procesar (estilo dd) o un disco físico. Esto permite que el examinador forense "arranque" la imagen o el disco y obtenga una perspectiva interactiva del entorno a nivel de usuario, todo ello sin modificar la imagen o el disco subyacente. Debido a que todos los cambios realizados en el disco se escriben en un archivo separado, el examinador puede revertir instantáneamente todos sus cambios al estado prístino original del disco. El resultado final es que no es necesario crear copias adicionales "desechables" del disco o la imagen para crear la máquina virtual.

Live View es capaz de arrancar

- Imágenes en bruto de disco completo
- Imágenes sin formato de partición de arranque
- Discos físicos (conectados a través de un puente USB o Firewire)
- Formatos de imagen especializados y cerrados (con software de montaje de imágenes de terceros)

Soporta los sistemas operativos: Windows 2008, Vista, 2003, XP, 2000, NT, Me, 98, Linux (soporte limitado). (Sourceforge, 2013).

MountImagePro

Es una herramienta de informática forense que Permite el montaje de imágenes forenses incluyendo: Encase, Imágenes de Unix/Linux, Archivos Iso, etc.

Mantiene por completo la integridad MD5 HASH, que se puede probar mediante una readquisición del disco montado y una comparación de sumas de verificación MD5.

Características principales:

- Asigna imágenes como una sola letra de unidad para explorar el espacio en disco "Sin usar / No particionado" o asigna letras de unidad específicas a cualquiera o todas las particiones dentro de los archivos de imagen.
- Usa herramientas de terceros sin la necesidad de restaurar imágenes a otra PC. Ahora puede desarrollar o usar sus propias herramientas sin las limitaciones de un lenguaje de scripting.
- No necesita tener EnCase instalado ni necesita un dongle EnCase para usar Mount Image Pro. Esto le brinda a usted y a sus clientes una flexibilidad total cuando manejan los archivos de evidencia de EnCase.

(MountImage, 2017).

2.8.7 Herramientas de Carving y Herramientas de Disco.

El Carving permite la recuperación de datos perdidos, borrados, búsqueda de patrones y ficheros con contenido determinado como por ejemplo imágenes, vídeos. Recuperación de

particiones y tratamiento de estructuras de discos.

Entre estas herramientas para la recuperación de información encontramos las siguientes:

PhotoRec

- Se puede ejecutar en los sistemas operativos: DOS/Win9x, Windows NT 4/2000/XP/2003, Linux, FreeBSD, NetBSD, OpenBSD, Sun Solaris, Mac OS X.
- Recupera archivos perdidos incluyendo videos, documentos y archivos de los discos duros y CDRoms
- Recupera imágenes perdidas de las memorias de las cámaras fotográficas, MP3 players, PenDrives, etc.
- Ignora el sistema de archivos y hace una búsqueda profunda de los datos, funcionando incluso si su sistema de archivos está muy dañado o ha sido reformateado.
- Usa acceso de solo lectura para manejar la unidad o la tarjeta de memoria de la que está a punto de recuperar los datos perdidos.
- Funciona con discos duros, CD-ROM, tarjetas de memoria (CompactFlash, Memory Stick, Secure Digital / SD, SmartMedia, Microdrive, MMC, etc.), unidades de memoria USB, imagen sin formato DD, imagen EnCase E01, etc.
- Busca encabezados de archivos conocidos, puede recuperar todo el archivo.
- Reconoce y recupera numerosos formatos de archivo, incluyendo ZIP, Office, PDF, HTML, JPEG y varios formatos de archivos gráficos.

(Cgsecurity, 2012).

Scalpel

Esta herramienta se utiliza para recuperar archivos del sistema, es una herramienta de código abierto para sistemas operativos Linux. Para la recuperación de datos borrados es un fork actualizado de foremost, aunque más rápida y más eficiente en el rastreo y búsqueda de patrones de archivos. Es una herramienta que permite restaurar información que ha sido eliminada.

Scalpel analiza un disco o un dispositivo de almacenamiento buscando patrones de bytes que responden a los encabezados y pies de página, de esta manera intentará recuperar los

datos pertenecientes al archivo. Scalpel puede detectar diversos tipos de archivos. Soporta distintas estructuras de disco y formatos de archivos para ello utiliza una base de datos con encabezados y pies de archivos con reglas de expresión para detectar que formatos puede recuperar.
Scalpel brinda un rendimiento de escaneo a gran velocidad, soporta formatos de disco desde FAT, NTFS, ext2 o particiones sin formato. Es útil tanto para la investigación forense digital, como para recuperación de archivos. (Culoccioni, 2016).

NTFS Recovery

Es un conjunto de herramientas para analizar problemas con particiones y archivos NTFS y recuperación de datos en modos manual y automatizado.

El modo manual le permite analizar las estructuras del disco y definir el problema utilizando el editor de discos freeware incluido. Puede solucionar el problema con Disk Editor o con Freeware Partition Manager o utilidades de sistema de Microsoft Windows. El modo automatizado simplifica su trabajo evitando el análisis de superficies de disco de bajo nivel y le permite concentrarse en la recuperación de datos específicos utilizando las herramientas de software de recuperación de archivos y recuperación de particiones incluidas. Tiene versión libre y versión de pago (Ntfs, 2016).

Recuva

Es un programa que puedes usar para recuperar imágenes, música, documentos, videos o cualquier otro tipo de archivos en tu disco duro, tarjetas de memoria, disquetes, iPod o reproductor de MP3 o USB. Normalmente, cuando usted o Windows eliminan un archivo, una gran parte del archivo se deja atrás, incluso si no puede verlo en el Explorador de Windows. Recuva recorre sus medios de comunicación (excepto CDs, DVDs y otros medios ópticos) y reúne las piezas para que pueda recuperar los archivos que necesita. Recuva también tiene la capacidad especial de borrar de forma segura los archivos recuperados. Por ejemplo, puede haber borrado un documento sensible de la forma habitual (vaciar la papelera de reciclaje o resaltar el archivo y presionar la tecla Suprimir). Este tipo de eliminación podría permitir que otros recuperaran el archivo. Al utilizar la función de restauración y eliminación segura de Recuva, puede asegurarse de que se borra de una vez

por todas. Tiene una versión gratuita y versión de pago. (Piriform, 2017).

Las características de Recuva son:

- Recupera todos los archivos que han sido borrados en el ordenador.
- Recupera los datos que se han perdido en un disco duro dañado o que se ha formateado.
- Recupera los correos electrónicos que se han eliminado.
- Recupera la música perdida en dispositivos iPod.
- Restaura documentos de Word que no se han guardado.
- Incluye un sencillo y a la vez intuitivo asistente.
- Hace un análisis en profundidad de la unidad en la que tenemos que efectuar la recuperación.
- Elimina de forma segura todos los archivos que no deseamos, de los que no queremos que queden rastros.
- Existe una versión portátil o portable del programa.
- Soporta todas las versiones de Windows en una gran cantidad de idiomas. (Fabriciano, 2016).

Raid Reconstructor

Herramienta para recuperar datos de un arreglo RAID de nivel 5 o RAID 0. Incluso si no conoce los parámetros RAID, como el orden de las unidades y el tamaño del bloque, Raid Reconstructor analiza las unidades y determina los valores correctos. (Runtime, 2017).

CNWrecovery.

Herramienta para la recuperación de datos, fotos y videos que se han perdido o eliminado desde el Disco duro, NTFS, FAT, MAC, CD, DVD, vídeo, GoPro, cámaras, RAID y más. (Cnwrecovery, 2017).

Restoration

Es un programa pequeño y gratuito de recuperación de archivos. Su principal característica es la simplicidad, ya que no requiere una instalación compleja, sino solo un clic en el archivo .exe. Además, una vez abierto, funciona desde una ventana única, que contiene todo lo necesario para la recuperación, y es muy fácil de entender.

Es uno de los mejores programas de recuperación de datos que rescata archivos de discos duros internos y externos, tarjetas de memoria y otros dispositivos de almacenamiento comunes. Da buenos resultados de escaneo, con una velocidad de recuperación eficiente. (CleverFiles, 2018).

Es una herramienta fácil de usar y directa para recuperar archivos que se eliminaron de la papelera de reciclaje o se eliminaron directamente desde Windows.
Algunas de sus características:

- Al comenzar, puede buscar todos los archivos que se pueden recuperar y también limitar los resultados ingresando un término o extensión de búsqueda.
- Ofrece la opción de borrar los archivos encontrados más allá de la recuperación simple.
- Es pequeño e independiente, no requiere instalación.
- Funciona con FAT y NTFS, así como con tarjetas de cámaras digitales.
- Es muy rápida, práctica, sencilla de usar y efectiva.
- A la inversa, este programa también permite volver irrecuperables los datos que se quieren eliminar a fin de proteger datos confidenciales.
  (Kato, 2018).

Freerecover.

Es un programa gratuito de recuperación de archivos para las unidades NTFS. Le permite buscar y previsualizar archivos borrados para encontrar datos perdidos. También estima la integridad de los archivos eliminados, así como recupera sus rutas de archivo originales.
Tiene las siguientes características

- Recupera archivos eliminados de unidades NTFS
- Genera previsualizaciones de archivos eliminados
- Proporciona estimaciones de la integridad de los archivos encontrados
- Búsqueda instantánea de archivos eliminados

(SourceForge, 2017).

DMDE

Es un potente software para la búsqueda, edición y recuperación de datos en discos. Puede recuperar la estructura de directorios y archivos en algunos casos complicados mediante el uso de algoritmos especiales cuando otro software no puede ayudar. (Dmde, 2016).

IEF (Internet Evidence Finder)

Es una herramienta para recuperar evidencia de una variedad de fuentes de datos, e integrarlas en un solo caso Magnet IEF. Construye una vista integrada e integral de las actividades digitales de una persona independiente del tipo de dispositivo o del sistema operativo. (Magnet Forensics, 2017).

Bulk_extractor

Es una útil herramienta de investigación forense para muchas tareas tales como el malware y las investigaciones de intrusión, investigaciones de identidad e investigaciones cibernéticas, así como el análisis de imágenes y el descifrado de palabras clave.

Las características de Bulk extractor:

- Encuentra direcciones de correo electrónico, URL y números de tarjetas de crédito. Puede procesar datos comprimidos (como archivos ZIP, PDF y GZIP) y datos incompletos o parcialmente corruptos. Puede grabar archivos JPEG, documentos de oficina y otros tipos de archivos a partir de fragmentos de datos comprimidos. Detectará y tallará archivos RAR encriptados.
- Construye listas de palabras basadas en todas las palabras encontradas en los datos, incluso aquellas en archivos comprimidos que están en espacio no asignado. Esas listas de palabras pueden ser útiles para descifrar contraseñas.
- Es multi-hilo; ejecutar bulk_extractor en una computadora con el doble de núcleos generalmente lo hace completar una carrera en la mitad del tiempo.
- Crea histogramas que muestran las direcciones de correo electrónico, las URL, los dominios, los términos de búsqueda y otros tipos de información más comunes en el disco.

- Incluye una interfaz gráfica de usuario, Bulk Extractor Viewer, para examinar las funciones almacenadas en los archivos de características y para iniciar escaneos bulk_extractor

(Tools Kali, 2014).

2.8.8 Herramientas para el sistema de ficheros

Conjunto de herramientas para el análisis de datos y ficheros esenciales en la búsqueda de un incidente. A continuación, alguna de estas herramientas:

AnalyzeMFT

Es una herramienta de Python diseñada para analizar completamente el MFT y presentar los resultados en un formato que permite un análisis posterior con otras herramientas. Extraer el MFT de un sistema de archivos NTFS y analizarlo con analyzeMFT le proporcionará una gran cantidad de información contenida en estas entradas. AnalyzeMFT., analiza los atributos de un archivo MFT produciendo resultados como:

- Número de registro
- Tipo de registro
- Fecha de creación, fecha de modificación, fecha de acceso, fecha de entrada.

Para cada entrada en el MFT un registro se escribe en un archivo de salida en formato CSV. AnalyzeMFT se ejecutará en cualquier sistema con Python instalado. (Forensic Focus, 2018).

Prefetch

PrefetchForensics es una aplicación para extraer información de los archivos Prefetch de Windows. Los archivos Prefetch pueden proporcionar información útil en una investigación forense como la fecha en que se ejecutó por última vez la aplicación y la cantidad de veces que se ejecutó la aplicación. El formato de archivo es relativamente directo, aunque existen diferentes formatos binarios entre XP y Vista.

PrefetchForensics analizará todos los archivos de búsqueda previa en un directorio determinado, calcula el valor de hash utilizando el algoritmo de determinación, que debe ser el mismo valor que se agrega al nombre de archivo. PrefetchForensics debe ejecutarse como un usuario de nivel de administrador debido a las operaciones de bajo nivel realizadas por la aplicación. Si no se ejecuta la aplicación como usuario de nivel de administrador, la aplicación puede fallar.

Tiene las siguientes Caracteristicas:

- Exportación de CSV
- Exportación de HTML
- Soporte de compensación de zona horaria
- Analizado la fecha de la última ejecución, número de veces ejecutado, hash de ruta, calcula el hash de ruta como verificación secundaria, extrae la ruta original y los archivos a los que se accedió.
  (Woanware, 2018).

Winprefectchview

Es una utilidad que lee los archivos Prefetch almacenados en su sistema y muestra la información almacenada en ellos. Al examinar estos archivos, puede saber qué archivos utiliza cada aplicación y qué archivos se cargan en el inicio de Windows. (Nirsoft, 2016).

Fileassassin

Es una herramienta gratuita diseñada con el objetivo de eliminar ficheros malignos rebeldes a métodos comunes de eliminación. Esos archivos son difíciles de eliminar y están bloqueados porque están en uso, generalmente por malwares. Esta herramienta utiliza avanzadas técnicas de descarga de módulos y finalización de procesos, liberando el archivo sospechoso de su bloqueo y así dejarlo libre para su eliminación. (Infospyware, 2017).

2.8.9 Herramientas para el Análisis del Registro de Windows

Permite obtener datos del registro como usuarios, permisos, ficheros ejecutados,

información del sistema, direcciones IP, información de aplicaciones. Las siguientes son herramientas para el registro de Windows.

RegRipper

RegRipper es una herramienta de código abierto, escrita en Perl, para extraer / analizar información (claves, valores, datos) del Registro y presentarla para su análisis.

RegRipper consta de dos herramientas básicas, ambas proporcionan una capacidad similar. La GUI de RegRipper le permite al analista seleccionar una colmena para analizar, un archivo de salida para los resultados y un perfil (lista de complementos) para ejecutar contra la colmena. Cuando el analista lanza la herramienta contra la colmena, los resultados van al archivo que el analista designó. Si el analista elige analizar la sección Sistema, también pueden elegir enviar los resultados a system.txt. La herramienta GUI también creará un registro de su actividad en el mismo directorio que el archivo de salida, utilizando el mismo nombre de archivo, pero utilizando la extensión .log (es decir, si el resultado se escribe en system.txt, el registro se escribirá en registro del sistema).

RegRipper también incluye una herramienta de línea de comandos (CLI) llamada Rip. que se puede apuntar contra una colmena y puede ejecutar un perfil (una lista de complementos) o un plugin individual contra esa colmena, y los resultados se envían a STDOUT. Rip se puede incluir en archivos por lotes, utilizando los operadores de redirección para enviar la salida a un archivo. Rip no escribe un registro de su actividad. (Kali Tools, 2014).

WRR (Windows Registry Recovery)

Esta aplicación permite leer archivos que contengan Windows XP, 7,8 y 10. Extrae mucha información útil sobre la configuración de Windows en la máquina como: cuentas de usuarios y grupos locales, el nombre, la ID y la clave de Windows, la fecha de instalación y la información de registro del usuario, muestra el nombre de usuario y de la máquina. Contiene un potente buscador e intérprete de datos. La sección de registro se puede exportar al formato REGEDIT4. Toda la información encontrada se puede guardar en CSV. Está diseñado en la interfaz de múltiples documentos.

Contiene los siguientes exploradores individuales:

- Información de archivo
- Explorador de registros de seguridad
- SAM
- Instalación de Windows
- Hardware
- Datos de usuario
- Aplicaciones de inicio
- Servicios y controladores
- Configuración de red
- Configuración del Firewall de Windows
- Entorno
- Carpetas de Shell
- Outlook Express
- Datos sin procesar

(Mitec, 2017).

Registry Decoder

Es una aplicación de software cuya finalidad es ayudarlo a analizar, buscar, explorar e informar los contenidos de la sección del registro. La herramienta es adecuada para los investigadores encargados de hacer cumplir la ley que necesitan extraer datos rápidamente y enviarlos a un informe.

Registry Decoder le ofrece la posibilidad de iniciar un nuevo caso o cargar uno existente especificando la carpeta de destino. La aplicación le da la libertad de agregar o eliminar evidencia y escanear el registro actual; incluidas las copias de seguridad creadas a través de puntos de restauración del sistema. Permite hacer una copia de seguridad de la carcasa y exportar complementos, búsquedas y rutas.

Puede obtener una vista previa de un resumen de caso que revela información sobre el nombre y el número del caso, el investigador, los comentarios, el directorio de guardado, así como la lista de pruebas. (Softpedia, 2015).

Registry Decoder es un proyecto de código abierto Python. Su objetivo es ayudar a automatizar la adquisición, el análisis y reporte de contenido del registro, contiene dos componentes:

Una herramienta de adquisición en vivo (Registry Decoder Live): Realiza la adquisición en vivo de los archivos de la colmena, admite XP, Vista y 7, 32/64 bit. Puede adquirir archivos históricos de la Restauración del sistema y Volume Shadow Service.

Una herramienta de análisis fuera de línea (Registry Decoder): Realiza análisis fuera de línea de archivos de registro, facilita el análisis de registro integral de cualquier cantidad de archivos dentro de una interfaz gráfica, la interfaz genera una nueva pestaña o pestañas para los resultados de cada acción tomada por el usuario. (Marziale, 2012).

2.8.10 Herramientas para el Análisis de la Red

Todo lo relacionado con el tráfico de red, en busca de patrones anómalos, malware, conexiones sospechosas, identificación de ataques, etc.

Entre las herramientas más destacadas para el análisis en la red tenemos las siguientes:

WireShark

Es la herramienta de análisis de protocolos de red más utilizado y ampliamente utilizado en el mundo. Le permite ver lo que está sucediendo en su red a nivel microscópico y es el estándar de factor en muchas empresas comerciales y sin fines de lucro, agencias gubernamentales e instituciones educativas. El desarrollo de Wireshark prospera gracias a las contribuciones voluntarias de expertos en redes de todo el mundo y es la continuación de un proyecto iniciado por Gerald Combs en 1998.

Wireshark tiene un completo conjunto de características que incluye lo siguiente:

- Inspección profunda de cientos de protocolos.
- Captura en vivo y análisis fuera de línea
- Navegador de paquetes estándar de tres paneles
- Multiplataforma: se ejecuta en Windows, Linux, OS X, Solaris, FreeBSD, NetBSD y muchos otros
- Los datos de red capturados se pueden navegar a través de una GUI, o mediante la utilidad TShark TTY-mode
- Los filtros de visualización más potentes de la industria.
- Rich análisis de VoIP
- Lee / escribe muchos formatos de archivos de captura diferentes: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor,

Network General Sniffer (comprimido y sin comprimir), Sniffer Pro y NetXray, Network Instruments Observer , NetScreen snoop, Novell LANalyzer, RADCOM WAN / LAN Analyzer, Shomiti / Finisar Surveyor, Tektronix K12xx, Visual Networks Visual UpTime, WildPackets EtherPeek / TokenPeek / AiroPeek y muchos otros

- Los archivos de captura comprimidos con gzip se pueden descomprimir sobre la marcha
- Los datos en vivo se pueden leer desde Ethernet, IEEE 802.11, PPP / HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI y otros (según su plataforma)
- Soporte de descifrado para muchos protocolos, incluidos IPsec, ISAKMP, Kerberos, SNMPv3, SSL / TLS, WEP y WPA / WPA2
- Las reglas de coloreado se pueden aplicar a la lista de paquetes para un análisis rápido e intuitivo
- La salida se puede exportar a XML, PostScript, CSV o texto sin formato

(Wireshark, 2017).

NetworkMiner

Es una Herramienta de análisis forense de redes para Windows (pero también funciona en Linux/Mac OS X/FreeBSD). NetworkMiner puede utilizarse como una herramienta de captura de paquetes/sniffer de red pasiva para detectar sistemas operativos, sesiones, nombres de host, puertos abiertos, etc. sin poner ningún tráfico en la red. NetworkMiner también puede analizar archivos PCAP para análisis fuera de línea y para regenerar/reensamblar archivos transmitidos y certificados de archivos PCAP.

NetworkMiner facilita la realización de Análisis de tráfico de red (NTA) avanzado proporcionando artefactos extraídos en una interfaz de usuario intuitiva. La forma en que se presentan los datos no sólo hace que el análisis sea más sencillo, sino que también ahorra un tiempo valioso para el analista o el investigador forense. Tiene versión gratuita y versión de pago.

La versión gratuita de NetworkMiner tiene las siguientes características

- Live sniffing
- Analizar archivos PCAP
- Soporte de IPv6
- Extraiga archivos de FTP, TFTP, HTTP, SMB, SMB2, SMTP, POP3 y tráfico

IMAP

- Extraiga los certificados X.509 del tráfico cifrado SSL como HTTPS, SMTPS, IMAPS, POP3S, FTPS, etc.
- Desencapsulación de GRE, 802.1Q, PPPoE, VXLAN, OpenFlow, SOCKS, MPLS y EoMPLS
- Recibir Pcap-over-IP
- Toma de huellas dactilares del SO

(Netresec, 2017).

Xplico

El objetivo de esta herramienta es extraer de una captura de tráfico de Internet las aplicaciones contenidas. Por ejemplo, a partir de un archivo pcap, Xplico extrae cada correo electrónico (protocolos POP, IMAP y SMTP), todo el contenido HTTP, cada llamada VoIP (SIP), FTP, TFTP, etc. Xplico no es un analizador de protocolo de red. Xplico es una herramienta de análisis forense de red de código abierto (NFAT).

Caracteristicas de Xplico:

- Protocolos compatibles: HTTP, SIP, IMAP, POP, SMTP, TCP, UDP, IPv6
- Identificación de protocolo independiente de puerto (PIPI) para cada protocolo de aplicación.
- Multihilo.
- Datos de salida e información en la base de datos SQLite o en la base de datos y/o archivos Mysql
- En cada información reensamblada por Xplico se asocia un archivo XML que identifica de forma única los flujos y el pcap que contiene los datos reensamblados
- Elaboración en tiempo real (depende de la cantidad de flujos, los tipos de protocolos y el rendimiento de la computadora -RAM, CPU, tiempo de acceso a HD)
- Reensamblado de TCP con verificación de ACK para cualquier paquete o verificación de ACK suave

- Búsqueda inversa de DNS desde paquetes DNS contenidos en los archivos de entrada (pcap), no desde un servidor DNS externo
- No hay límite de tamaño en la entrada de datos o el número de archivos ingresados (el único límite es el tamaño HD)
- Compatibilidad con IPv4 e IPv6
- Cada componente de Xplico es modular. La interfaz de entrada, el decodificador de protocolo (Disector) y la interfaz de salida (despachador) son todos módulos
- La capacidad de crear fácilmente cualquier tipo de despachador con el que organizar los datos extraídos de la manera más adecuada y útil para usted.

(Xplico, 2016).

Snort

Es un sniffer de paquetes y un detector de intrusos basado en red (se monitoriza todo un dominio de colisión). Es un software muy flexible que ofrece capacidades de almacenamiento de sus bitácoras tanto en archivos de texto como en bases de datos abiertas como lo es MySQL. Implementa un motor de detección de ataques y escaneo de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida. Así mismo existen herramientas de terceros para mostrar informes en tiempo real (ACID) o para convertirlo en un Sistema Detector de Intrusos.

Snort se puede configurar para ejecutarse en tres modos:

• **Modo Sniffer**: en el que se motoriza por pantalla en tiempo real toda la actividad en la red en que Snort es configurado.

• **Modo de registro de paquetes**: en el que se almacena en un sistema de log toda la actividad de la red en que se ha configurado Snort para un posterior análisis.

• **Modo de sistema de detección de intrusión de red (NIDS**): en el que se motoriza por pantalla o en un sistema basado en log, toda la actividad de la red a través de un fichero de configuración en el que se especifican las reglas y patrones a filtrar para estudiar los posibles ataques. (Snort, 2017).

Splunk

Es una Herramienta para buscar, monitorizar y analizar datos generados por máquinas (Big Data) de aplicaciones, sistemas e infraestructura IT a través de una interfaz web. Splunk captura, indexa y corre en tiempo real, almacenándolo todo en un repositorio donde busca para generar gráficos, alertas y paneles fácilmente definibles por el usuario. (Splunk, 2017).

AlientVault

Herramienta de gestión de seguridad digital integrada (USM, por sus siglas en inglés), es una plataforma unificada diseñada para proporcionar y garantizar una defensa completa contra las amenazas de seguridad más recientes a un precio razonable, y enfocada especialmente a Pequeñas y Medianas Empresas (PYME). (Alienvault, 2017).

2.8.11 Herramientas para Dispositivos Móviles

Las siguientes son herramientas muy importantes utilizadas en dispositivos móviles, disponer de estas herramientas es una maravilla y un lujo el poder utilizarlas. Rápidas y concisas. Lo peor en alguna de ellas es el precio. (Conexioninversa, 2011).

UFED Standard

La innovadora UFED está diseñada para los examinadores forenses e investigadores que requieren herramientas completas de extracción y decodificación de datos móviles, ayuda a los examinadores forenses a recopilar, proteger y actuar con decisión sobre los datos móviles con rapidez y precisión. (Cellebrite, 2016).

XRY

Es una aplicación de software diseñada para ejecutarse en el sistema operativo Windows que le permite realizar una extracción forense seguro de datos desde una amplia variedad de dispositivos móviles, como teléfonos inteligentes, tablets, módems, reproductores de música y unidades de navegación por satélite. (Msab, 2017).

Mobilyze

Es una herramienta que permite a los investigadores averiguar rápidamente si un dispositivo contiene evidencia forense relevante que justifique una acción adicional. Los casos de Mobilyze se pueden importar sin problemas en BlackLight para un análisis más exhaustivo si es necesario, sin tener que realizar otra colección. (Blackbagtech, 2017).

SecureView2

Secure View se convirtió en el primer software forense móvil en el mercado. Es la solución definitiva de software y hardware, permite la extracción de datos de contenido almacenado en teléfonos móviles. Facilita el acceso a información vital en cuestión de segundos sin necesidad de esperar los resultados de un laboratorio forense. También contiene un conjunto completo de herramientas; Análisis, marcadores y reportes. (Mobileforensics, 2017).

MobilEdit

Permite la extracción completa de datos desde teléfonos y SIM. Con MOBILedit Forensic puede ver, buscar o recuperar todos los datos de un teléfono con sólo unos pocos clics, Estos datos incluyen historial de llamadas, agenda telefónica, mensajes de texto, mensajes multimedia, archivos, calendarios, notas, recordatorios y datos de aplicaciones en bruto. También recuperará toda la información del teléfono, como IMEI, sistemas operativos, firmware incluyendo detalles de SIM (IMSI), ICCID e información de área de ubicación. MOBILedit Forensic también puede recuperar bypass la contraseña, el PIN y el cifrado de respaldo del teléfono. (Mobiledit, 2017).

Oxygen Forensic

Es un software forense para la extracción y análisis de datos de teléfonos celulares, teléfonos inteligentes y tabletas, extrae muchos más datos sin dejar rastros y sin hacer modificaciones en el contenido del dispositivo. El software se distribuye a la policía, los organismos gubernamentales, militares, investigadores privados y otros especialistas

forenses. (Oxygen Forensic, 2017).

Mobile Phone Examiner

Es una solución autónoma de investigación de dispositivos móviles que incluye capacidades avanzadas de adquisición y análisis de dispositivos inteligentes. Con un enfoque diferente a la forense digital móvil, permite a los examinadores forenses móviles tomar el control de la investigación, proporcionándoles herramientas únicas necesarias para recopilar rápidamente, identificar fácilmente y obtener de manera efectiva los datos clave. (AccessData, 2017).

Device Seizure

Es una herramienta de análisis forense para el examen de los teléfonos móviles, PDAs y dispositivos GPS. Device Seizure incluye software y hardware. Fue diseñado desde el principio como una herramienta de análisis forense de modo que ha sido confirmada en un sinnúmero de casos judiciales. (Paraben Corporation, 2017).

3. METODOLOGÍA

La información está expuesta a diferentes tipos de incidentes y siendo el bien más valioso para todo tipo de organización, justifica cada esfuerzo posible para su recuperación. En el presente trabajo se exploran diversas herramientas de informática forense que permiten la recuperación de información y evidencias digitales.

La metodología utilizada en este proyecto consta de las siguientes fases:

3.1 REVISIÓN DE LA LITERATURA

En esta fase se seguirán los pasos propuestos por (Serna & Serna, 2013) de la siguiente manera:

3.1.1 Definir el área temática.

Análisis forense, herramientas de software libre para la recolección de evidencia digital.

3.1.2 Preguntas de investigación.

Para la realización de la revisión de la literatura se plantearon las siguientes preguntas:

P1. ¿Qué se entiende por el término "Recolección de evidencia digital"?

P2. ¿Cuál es el panorama de la recolección de evidencia digital?

P3. ¿Qué herramientas existen para el proceso de recolección de evidencia digital?

P4. ¿Cuáles son los tops de herramientas privativas y libres más usadas para la recolección de evidencia digital?

P5. ¿Cuáles son los controles preventivos más usados para evitar la pérdida de información en el contexto digital?

P6. ¿Cuáles son los riesgos más comunes que se podrían presentar durante el proceso de recolección de evidencia digital?

3.1.3 Proceso de búsqueda.

En el proceso de búsqueda de la presente investigación se utilizaron palabras claves como: *informática forens*e, *forensics*, *herramientas de análisis forense informático, forensics tools, tools for collecting digital evidence, Digital forensic evidence tools, Tools for computer forensics, Digital evidence and tools, Open source digital evidence collection tools.*

Se consultaron buscadores como google y google académico y las bases de datos IEEE, Scielo, Scopus, ScienceDirect, Dialnet.

3.1.4 Criterios de inclusión y exclusión.

Para la inclusión y exclusión de documentos se aplicaron 4 pasos propuestos por (Dyba & Dingsoyr, 2008).

- Identificar los estudios relevantes.
- Excluir estudios con base en el título.
- Excluir estudios con base en los resúmenes.
- Analizar los estudios y seleccionar los más relevantes para la temática en cuestión con base en el texto completo.

Basados en (Serna & Serna, 2013), se tuvo en cuenta como criterios: Formalidad y pertinencia del sitio donde se aloja, calidad y aporte del contenido, la fuente de los datos y la coherencia de los resultados, y fecha con rango desde 2004 hasta la fecha.

En este paso se encontraron 395 documentos.

3.1.5 Valoración de la calidad.

Se validó que los estudios tuvieran credibilidad, que fueran de fuentes confiables y/o recomendados por expertos y que hayan hecho un aporte relevante a la informática forense.

Luego de aplicar la valoración de la calidad, los 395 documentos encontrados en el punto anterior se redujeron a 172.

3.2 SELECCIONAR LAS HERRAMIENTAS MÁS EMPLEADAS.

Con la información obtenida en la fase anterior podemos determinar que son muchas herramientas útiles para realizar análisis forense, basados en la información encontrada en el estado del arte, se diseña la siguiente tabla con las herramientas que facilitan la recolección de evidencia digital en disco y memoria.

Tabla 2: Herramientas para la recolección de evidencia digital en disco y en memoria.

HERRAMIENTA	LICENCIA PAGA/OPEN SOURCE	SISTEMA OPERATIVO	FUNCIÓN	CASA FABRICANTE	SITIO WEB
EnCase Forensics	Paga	Windows, Linux	Recolecta datos digitales, realiza análisis, produce una duplicación binaria exacta del dispositivo usando un estándar sin pérdida	Guidance Software	https://www.guidancesoftware.com/encase-forensic?cmpid=nav_r
DD (duplicate disk)	OpenSource	Unix/Linux	Se utiliza para clonar o copiar información bit a bit del disco duro, o también para copiar particiones o discos completos unos sobre otros.	Proyecto GNU	https://github.com/coreutils/coreutils
Air (Imagen y Restauración Automática)	OpenSource	Linux	AIR está diseñado para crear fácilmente imágenes forenses de disco/partición. Es compatible con hashes MD5/SHAx, unidades de cinta SCSI, imágenes a través de una red TCP/IP, división de imágenes y registro de sesión detallado.	Desconocido	https://sourceforge.net/projects/air-imager/
FTK Imager	OpenSource	Windows	Es una herramienta de previsualización e imagen de datos que le permite	AccessData	http://www.accessdata.com/downloads.html

			evaluar rápidamente la evidencia electrónica para determinar si se justifica el análisis posterior con una herramienta forense como AccessData Forensic Toolkit		
HERRAMIENTA	**LICENCIA PAGA/OPEN SOURCE**	SISTEMA OPERATIVO	**FUNCIÓN**	**CASA FABRICANTE**	**SITIO WEB**
Ddrescue	OpenSource	Linux	Herramientas de mayor alcance en el proceso de recuperación de datos dañados, Tiene la característica de copiar datos con errores de lectura de un archivo o dispositivo de bloques (disco duro, cdrom, etc) a otro, tratando de rescatar y recuperar la mayor cantidad de información posible, para su posterior análisis.	Proyecto GNU	https://www.gnu.org/software/software.html
Digital Forensics Framework	software libre	Mac, Windows y Linux	Permite recoger, preservar y revelar la evidencia digital, accediendo a los dispositivos locales y remotos, analizando los datos del registro, buzón y del sistema	Frédéric Baguelin, Solal Jacob, Jérémy Mounier	www.digital-forensic.org

			de archivos para recuperar archivos ocultos y eliminados		
OSForensic	Paga	Windows	Permite extraer pruebas forenses de computadoras rápidamente con la búsqueda avanzada de archivos y la indexación y permite que estos datos sean administrados de manera eficaz.	PassMark Software	https://www.osforensics.com/
HERRAMIENTA	**LICENCIA PAGA/OPEN SOURCE**	SISTEMA OPERATIVO	**FUNCIÓN**	**CASA FABRICANTE**	**SITIO WEB**
WinHex	Paga	Windows	Analiza el espacio libre en disco, creando así una descripción detallada de las unidades, inspecciona archivos binarios, recupera datos borrados o perdidos en unidades dañadas. Es un editor hexadecimal capaz de mostrar completamente el contenido de cada tipo de archivo, incluso los códigos de control y el código ejecutable, usando un número de dos dígitos basado en el sistema de numeración hexadecimal	X-Ways	http://www.winhex.com/winhex/index-e.html

R-Studio	Paga	Windows/Linux	Es la solución más completa de recuperación de datos para los archivos de recuperación de particiones.	RStudio, Inc	www.rstudio.com
The Sleuth Kit y Autopsy	OpenSource	Windows/Linux	Permite analizar imágenes de disco y recuperar archivos de ellas. Autopsy es una plataforma forense digital e interfaz gráfica para The Sleuth Kit y otras herramientas forenses digitales.	Brian Carrier	www.sleuthkit.org
HELIX CD	OpenSource	Linux	Posee la mayoría de las herramientas necesarias para realizar un análisis forense tanto de equipos como de imágenes.	Desconocido	e-fense.com
HERRAMIENTA	**LICENCIA PAGA/OPEN SOURCE**	SISTEMA OPERATIVO	**FUNCIÓN**	**CASA FABRICANTE**	**SITIO WEB**
F.I.R.E. Linux	OpenSource	Linux	Herramienta para la recuperación de datos, análisis de virus y evaluación de vulnerabilidades.	Desconocido	http://biatchux.dmzs.com/
Hetman software	Paga	Windows	Su función es recupera datos de discos duros, externos y USB, todo tipo de tarjetas de memoria como SD, SDHC, Usb	Hetman Software	hetmanrecovery.com

Pd ProccessDumper	OpenSource	Windows /Linux	Esta herramienta puede utilizarse para tomar una instantánea de la memoria de un proceso en ejecución.	Desconocido	https://github.com/glmcdona/Process-Dump
DumpIt	Paga	Windows	Herramienta para tomar muestras de la memoria RAM en Ambientes Windows,	MoonSols Ltd	http://hotfixed.net/adquisicion-de-memoria-en-windows-con-dumpit/
TestDisk	software libre	Windows/ Linux/Mac	Recupera archivos eliminados, tablas de particiones cuando están dañadas o han sido borradas por error, ayuda a reconstruir sectores de arranque. Usada especialmente para resolver problemas causados por software defectuoso, algunos tipos de virus o errores provocados.	Christophe Grenier	http://www.cgsecurity.org/wiki/testDisk_
Volatility	OpenSource	Windows/Linux	Su función es la Extracción de artefactos digitales de muestras de memoria volátil	The Volatility Foundation	https://github.com/volatilityfoundation/volatility
HERRAMIENTA	**LICENCIA PAGA/OPEN SOURCE**	SISTEMA OPERATIVO	**FUNCIÓN**	**CASA FABRICANTE**	**SITIO WEB**
RedLine	OpenSource	Windows	Con readline se puede auditar y recopilar exhaustivamente todos los procesos y	endpoint	https://www.fireeye.com/services/freeware/redline.

			controladores en ejecución de la memoria.		html
Memorize	OpenSource	Windows/ Mac OS X	Memoryze puede adquirir y/o analizar imágenes de memoria y en sistemas en caliente puede incluir el archivo de paginación en su análisis.	Desconocido	https://www.fireeye.com/services/freeware/memoryze.html
PhotoRec	OpenSource	Windows/ Linux/ Mac OS X	Software diseñado para recuperar archivos perdidos incluyendo videos, documentos y archivos de los discos duros y CDRoms así como imágenes perdidas.	Christophe Grenier	www.cgsecurity.org/wiki/PhotoRec
Scalpel	OpenSource	Linux	Permite recuperar los archivos que hemos borrado accidentalmente en nuestro equipo.	Golden G. Richard III and Lodovico Marziale	https://github.com/sleuthkit/scalpel
NTFS Recovery	Paga	Windows	Esta herramienta sirve para analizar problemas con particiones y archivos NTFS y recuperación de datos en modos manual y automatizado.	NTFS.com	http://www.ntfs.com/recovery-toolkit.htm
HERRAMIENTA	**LICENCIA PAGA/OPEN SOURCE**	SISTEMA OPERATIVO	**FUNCIÓN**	**CASA FABRICANTE**	**SITIO WEB**
Recuva	Paga	Windows/	Herramienta que puedes usar para	Piriform	www.piriform.com/recuv

		Mac OS X	Recuperar imágenes, música, documentos, videos o cualquier otro tipo de archivos en tu disco duro, tarjetas de memoria, disquetes y USB.		a
Raid Reconstructor	Paga	Windows	Herramienta para recuperar datos de un arreglo RAID de nivel 5 o RAID 0. Incluso si no conoce los parámetros RAID.	Runtime Software	https://www.runtime.org/raid.htm
CNWrecovery	Paga	Windows	Herramienta para la recuperación de datos, fotos y videos que se han perdido o eliminado desde el Disco duro.	CnW Recovery	https://www.cnwrecovery.com/
Freerecover	OpenSource	Windows	Recuperación de archivos para las unidades NTFS. Le permite buscar y previsualizar archivos borrados para encontrar datos perdidos.	Dcorphan	https://sourceforge.net/projects/freerecover/
DMDE	Paga	Windows/Linux	Software para la búsqueda, edición y recuperación de datos en discos.	DMDE	https://dmde.com/download.html
Remo Recuperar	Paga	Windows, Mac, Android	Rescata información, recupera archivos perdidos debido a errores en el sistema de archivos. Tiene una función integrada “encontrar”, lo que ayuda a encontrar y	Remosoftware	http://www.remorecover.com/es/windows/recupere-archivos.html

			localizar cualquier archivo en particular sobre la base de diferentes atributos de archivo.		
HERRAMIENTA	**LICENCIA PAGA/OPEN SOURCE**	SISTEMA OPERATIVO	**FUNCIÓN**	**CASA FABRICANTE**	**SITIO WEB**
GetDataBack	Paga	Windows	Recupera todo tipo de datos, aunque no sea reconocido el dispositivo o se haya perdido toda la información de estructura de directorios. Aun si se ha realizado un borrado tiempo atrás, no sin antes saber qué sistema de archivos es NTFS o FAT.	Runtime Software	https://www.runtime.org/data-recovery-software.htm
Responder pro	Paga	Windows	Responder PRO permite a los profesionales de respuesta a incidentes recolectar y analizar residuos de ataque y artefactos de la memoria. Los forenses y los ingenieros inversos pueden escanear fragmentos de documentos, historial de Internet, y las claves y contraseñas se extraen automáticamente de la memoria y se ponen a disposición.	Countertack	http://www.countertack.com/responder-pro

Winpmem	Opensource	Windows	Es una herramienta de adquisición de memoria forense de código abierto, desarrollada activamente, para Windows Por defecto WinPmem utiliza una técnica llamada PTA Remapping para adquirir memoria.	Rekall Forensics	http://www.rekall-forensic.com
LiME (Linux Memory Extractor)	Opensource	Linux	Permite la adquisición de memoria volátil de dispositivos basados en Linux. Esto hace que LiME sea único, ya que es la primera herramienta que permite realizar capturas de memoria completa.	Proyecto GNU	https://github.com/halpomeranz/lmg/
HERRAMIENTA	**LICENCIA PAGA/OPEN SOURCE**	SISTEMA OPERATIVO	**FUNCIÓN**	**CASA FABRICANTE**	**SITIO WEB**
Wondershare Data Recovery	Paga	Windows, Mac	Recupera archivos perdidos en más de 550 formatos de forma rápida, segura y completa: vídeos, fotos, emails, música, etc.	Wondershare Recovery	http://www.wondershare.es/disk-utility/usb-flash-drive-recovery.html
Undelete 360	OpenSource	Windows	Permite restaurar archivos borrados de su computadora, Construido sobre un algoritmo muy rápido y eficiente, el	File Recovery Ltd.	http://www.undelete360.com/

			programa explorará, buscará y recuperará archivos que han sido eliminados		
Volatilitux	openSource	Linux	Permite extraer artefactos digitales de volcados de memoria física (RAM) de sistemas Linux.	segmentationfault	http://www.segmentationfault.fr/projets/volatilitux-physical-memory-analysis-linux-systems/
Crash de Red Hat	Open source	Linux	Es una herramienta independiente para investigar tanto los sistemas en funcionamiento como los volcados de memoria del kernel hechos con los paquetes de Red Hat netdump, diskdump o kdump. También se puede utilizar para el análisis forense de memoria.	Proyecto GNU	http://people.redhat.com/anderson/crash_whitepaper/
HERRAMIENTA	**LICENCIA PAGA/OPEN SOURCE**	SISTEMA OPERATIVO	**FUNCIÓN**	**CASA FABRICANTE**	**SITIO WEB**
Wise data recovery	OpenSource	Windows	Permite la recuperación de los datos para solucionar sus problemas de pérdida de datos Si usted suprimió algunos archivos por accidente, formateó una impulsión o encontró un desplome del sistema y	WiseCleaner	http://www.wisecleaner.com/wise-data-recovery.html

			perdió algunos archivos, puede conseguir detrás archivos perdidos del disco duro.		
Disk Recovery	OpenSource	Windows	Recupera la información perdida, reconstruye sistemas de archivos dañados o formateados. Escanea todos los sectores.	O&O Software	http://o-o-diskrecovery.softonic.com/descargar
Restoration	OpenSource	Windows	Restoration es una aplicación que destaca por su poco peso y su facilidad de uso. Simplemente seleccionas la unidad en la que quieres recuperar archivos y te muestra la lista de los archivos que puedes recuperar.	Desconocido	http://www3.telus.net/mikebike/RESTORATION.html
Cd recovery Toolbox	OpenSource	Windows	Tiene la opción de la recuperación de archivos en disco duro, pero su principal función es la de recuperar archivos en discos ópticos	Recovery Toolbox	https://www.oemailrecovery.com/cd_recovery.html
Scrounge-Ntfs	OpenSource	Windows/Linux	Permite la recuperación de datos para sistemas de archivos NTFS. Lee cada bloque del disco duro y recupera el árbol del sistema de archivos de reconstrucción en otra partición.	Recovery tools	http://thewalter.net/stef/software/scrounge/
Zeitline	Open	Winows/Linux	Proporciona una ayuda a la hora de	CERIAS,	https://sourceforge.net/pr

	Source		procesar grandes cantidades de datos, con una interfaz gráfica cuyo elemento principal es el "evento". Un evento consiste en un intervalo de tiempo en el que tuvo lugar, una fuente que denote el origen del evento, y una descripción del evento.	Purdue University	ojects/zeitline/
Redo Backup and Recovery	OpenSource	Windows/Linux	Esta herramienta fue diseñada para recuperar nuestros datos en caso de problemas. Una de sus mayores virtudes es lo rápido que carga, lo que facilita mucho su uso en equipos con menos recursos.	Redobackup	http://redobackup.org/download.php
SystemRescueCd	OpenSource	Linux	Herramienta para administrar o reparar el sistema y los datos después de un accidente. Su objetivo es proporcionar una forma sencilla de llevar a cabo tareas de administración en su computadora, como crear y editar las particiones del disco duro.	GPL-2	http://www.system-rescue-cd.org/
PC Inspector file	software libre	Windows,	Recupera archivos y rescata datos	Convar	http://pc-inspector-file-

recovery		Linux	eliminados, perdidos e incluso unidades perdidas. Posee además la función especial de recuperación, que salva los archivos que no tienen ninguna indicación de directorio. En su listado de formatos. También ofrece una guía de ayuda.		recovery.softonic.com/
Ubuntu Rescue Remix	OpenSource	Linux	Esta herramienta está centrada en este caso en facilitar las herramientas adecuadas para poder recuperar nuestros datos en caso de fallo del sistema operativo o de una partición.	Desconocido	http://iso.linuxquestions.org/ubuntu-rescue-remix/
Foriana	OpenSource	Winows	Permite la extracción de información de procesos y listas de módulos desde una imagen de la RAM con la ayuda de las relaciones lógicas entre las estructuras del sistema operativo.	Desconocido	http://www.hackplayers.com/2013/10/herramientas-analisis-forense-memoria-linux.html
Forensic Analysis Toolkit	OpenSource	Windows/Linux	Herramienta multiplataforma, modular y extensible para analizar la memoria del sistema volátil. Esta herramienta esa dirigida a investigadores, profesionales de la aplicación de la ley y analistas forense	FATKit	http://www.darknessgate.com/2016/09/15/the-forensic-analysis-toolkit-fatkit/

			que están interesados en extraer e interpretar información relevante a raíz de un crimen o incidente.		
Puran file recovery	OpenSource	Windows	Es una Herramienta que se utiliza para recuperar archivos eliminados/perdidos/ particiones. Los archivos se pueden recuperar de los discos formateados también. Casi todo lo que se detecta como una unidad de Windows.	PuranSoftware	http://www.puransoftware.com/File-Recovery.html
Glary undelete	OpenSource	Windows	Herramienta libre para la recuperación de archivos eliminados. De este programa se destaca que tiene una interfaz muy limpia y sencilla, lo cual la hace una herramienta ideal para personas que buscan algo que funcione sin demasiadas opciones.	GlarySoft	http://www.glarysoft.com/glary-undelete/download/
Softperfect file recovery	OpenSource		Es una herramienta gratuita y útil para restaurar archivos y rescatar datos que se eliminaron accidentalmente de discos duros	SoftPerfect	https://www.softperfect.com/products/filerecovery/

Con base en el cuadro anterior, se seleccionan las herramientas opensource de recolección de evidencia digital en disco y memoria, que según los estudios realizados anteriormente y basados en tops representativos consultados y además teniendo en cuenta las opiniones de: (Techsupportall, 2017), (Fossbytes, 2017), (TechTalk, 2017), (InfosecInstitute, 2017), (GeekFlare, 2016), (ForensicControl, 2017), (Wondershare, 2017), (CursoHacker, 2014), serían las más empleadas. De acuerdo con el número de herramientas encontradas se realiza un top 10 para las herramientas de recolección de evidencia en disco y un top 5 para las herramientas útiles en memoria.

Tabla 3 : Top 10 de las Herramientas opensource de recolección de evidencia digital en disco

HERRAMIENTA	SISTEMA OPERATIVO	CASA FABRICANTE	SITIO WEB
Air (Imagen y Restauración Automática)	Linux	Desconocido	https://sourceforge.net/projects/air-imager/
Ddrescue	Linux	Proyecto GNU	https://www.gnu.org/software/software.html
Digital Forensics Framework	Mac, Windows y Linux	Frédéric Baguelin, Solal Jacob, Jérémy Mounier	www.digital-forensic.org
The Sleuth Kit y Autopsy	Windows/Linux	Brian Carrier	www.sleuthkit.org
TestDisk	Windows/Linux/ Mac	Christophe Grenier	http://www.cgsecurity.org/wiki/TestDisk_
PhotoRec	Windows/Linux/ Mac OS X	Christophe Grenier	www.cgsecurity.org/wiki/PhotoRec
Recuva	Windows/Mac OS X	Piriform	www.piriform.com/recuva

Undelete 360	Windows	File Recovery Ltd.	http://www.undelete360.com/
Restoration	Windows	Desconocido	http://www3.telus.net/mikebike/RESTORATION.html
Puran file recovery	Windows	PuranSoftware	http://www.puransoftware.com/File-Recovery.html

Tabla 4 : Top 5 de las Herramientas opensource de recolección de evidencia digital en memoria

HERRAMIENTA	SISTEMA OPERATIVO	CASA FABRICANTE	SITIO WEB
FTK Imager	Windows	AccessData	http://www.accessdata.com/downloads.html
Volatility	Windows/Linux	The Volatility Foundation	https://github.com/volatilityfoundation/volatility
RedLine	Windows	Endpoint	https://www.fireeye.com/services/freeware/redline.html
Memorize	Windows/Mac OS X	Desconocido	https://www.fireeye.com/services/freeware/memoryze.html
LiME (Linux Memory Extractor)	Linux	Proyecto GNU	https://github.com/halpomeranz/lmg/

3.3 CUADRO COMPARATIVO.

A continuación, se presenta el cuadro comparativo de las herramientas de recolección de información, seleccionadas en el top ten y top five de la fase anterior, en el cual se organizan en orden según su relevancia de acuerdo con la información encontrada en la revisión bibliográfica, en dicha tabla se resaltan las características más importantes, el enlace de descarga y el sistema operativo para el cual están diseñadas

Tabla 5 : Cuadro comparativo herramientas de recolección de información en disco

RELEVANCIA	HERRAMIENTA/ SITIO DE DESCARGA	SISTEMA OPERATIVO	CARACTERISTICAS PRINCIPALES	TIPO
1	Autopsy y the Sleuth Kit https://www.sleuthkit.org/autopsy/download.php	Windows/Linux	• La instalación es fácil y los asistentes le guían a través de cada paso. • Análisis de la línea de tiempo • Marcar archivos mal conocidos e ignorar los buenos conocidos. • Búsqueda por palabra clave • Recuperar archivos borrados de espacio no asignado usando PhotoRec • Ejecuta las tareas de fondo en paralelo utilizando múltiples núcleos • Muestra los eventos del sistema en una interfaz gráfica para ayudar a identificar la actividad. • Extrae la actividad web de los navegadores comunes para ayudar a identificar la actividad del usuario. • Utiliza RegRipper para identificar los documentos y dispositivos USB a los que se accedió recientemente. • Identifica accesos directos y documentos accedidos • Extrae la ubicación geográfica y la información de la cámara de	Análisis y recuperación

			archivos JPEG. • Agrupa los archivos por su tipo para encontrar todas las imágenes o documentos. • Admite sistemas de archivos comunes, incluidos NTFS, FAT12 / FAT16 / FAT32 / ExFAT, HFS +, ISO9660 (CD-ROM), Ext2 / Ext3 / Ext4, Yaffs2 y UFS de The Sleuth Kit. Fabricada por SleuthKit, la última versión es 4.4.1 del 28/01/2017.	
2	Recuva http://www.piriform.com/recuva/download	Windows/Mac OS X	• Recupera todos los archivos que han sido borrados en el ordenador. • Recupera los datos que se han perdido en un disco duro dañado o que se ha formateado. • Recupera los correos electrónicos que se han eliminado. • Recupera la música perdida en dispositivos iPod. • Restaura documentos de Word que no se han guardado. • Incluye un sencillo y a la vez intuitivo asistente. • Hace un análisis en profundidad de la unidad en la que tenemos que efectuar la recuperación. • Elimina de forma segura todos los archivos de los que no queremos que queden rastros. • Existe una versión portátil o portable del programa. • Soporta todas las versiones de Windows en una gran cantidad de idiomas. Fabricada por Piriform, la última versión es 1.53.1087 del 08/06/2016	Recuperación

3	Undelete 360 http://www.undelete360.com/download.html	Windows	• Recupera archivos borrados de discos duros de computadora, unidades USB / thumb y tarjetas de memoria, camaras digitales, unidades de disquete • El programa es compatible con la recuperación de archivos y la recuperación de carpetas. Usando Undelete 360, puedes restaurar archivos: • Eliminado accidentalmente de su PC u otro medio • eliminado por virus • demasiado grande para caber en la papelera de reciclaje • eliminado en los recursos compartidos de red de Windows • eliminado de una memoria USB • Se elimina al presionar las teclas "Shift + Delete" • borrado cuando se ha usado el comando Mover o Cortar • creado y eliminado por ciertas aplicaciones • eliminado de la línea de comando. Fabricada por Undelete360, la última versión es 2.16 del 28/02/2016	Recuperación
	Restoration https://restoration.softonic.com/	Windows	• Recupera archivos que se eliminaron de la papelera de reciclaje o se eliminaron directamente desde	Recuperación

4			Windows. • Al comenzar, puede buscar todos los archivos que se pueden recuperar y también limitar los resultados ingresando un término o extensión de búsqueda. • Ofrece la opción de borrar los archivos encontrados más allá de la recuperación simple. • Es pequeño e independiente, no requiere instalación. • Funciona con FAT y NTFS, así como con tarjetas de cámaras digitales. • Es muy rápida, práctica, sencilla de usar y efectiva. • A la inversa, este programa también permite volver irrecuperables los datos que se quieren eliminar a fin de proteger datos confidenciales. Autor: Brian Kato, la última versión es 3.2.13 del 31/03/2010	
5	TestDisk http://www.cgsecurity.org/wiki/TestDisk_Descargar	Windows/Linux/Mac	TestDisk se utiliza para recopilar información detallada acerca de una unidad que no arranca que luego se puede enviar a un técnico para su posterior análisis. TestDisk puede: • Arregla la Tabla de Particiones, recupera particiones eliminadas • Recupera sectores de booteo	Análisis y recuperación

			FAT32 de su copia de respaldo • Reconstruye sectores de booteo FAT12/FAT16/FAT32 • Arregla tablas de booteo de tipo FAT • Reconstruye sectores de booteo NTFS • Recupera sectores de booteo NTFS de su copia de respaldo • Arregla la MFT usando la MFT mirror • Localiza el Superblock de copia de respaldo de ext2/ext3 • Recupera archivos de sistemas de archivos FAT, NTFS y ext2 • Copia archivos de particiones FAT, NTFS y ext2/ext3 eliminadas. Fabricada por DataRecovery, la última versión es 7.0 del 18/04/2015	
6	Digital Forensics Framework http://linux.softpedia.com/get/Security/Digital-Forensics-Framework-102398.shtml	Mac, Windows y Linux	• Monta particiones, sistemas de archivos y extrae metadatos de archivos y otra información útil de forma automática. • Genera un informe HTML con actividad de sistema y usuario • Formatos de archivo de imagen forense admitidos: AFF, E01, Ex01, L01, Lx01, dd, • Buzones de correo de Outlook y Echange (PAB, PST, OST) • Historial del navegador:	Análisis y recuperación

			Firefox, Chrome, Opera • Generación de videos en miniatura • Análisis completo de Skype (Sqlite y antiguo formato DDB) • Preservar cadena digital de custodia • Software bloqueador de escritura, el cálculo de hash criptográfica • El acceso a los dispositivos locales y remotos • Lee formatos de archivo estándares de forense digital • Reconstrucción de discos de máquina virtual • Búsqueda rápida de metadatos • Recuperación de objetos ocultos y eliminados • Archivos eliminados/carpetas,espacios no asignados/carving Fabricada por Digital-Forensic, la última versión es 1.3.0 del 28/02/2016.	
	PhotoRec http://www.cgsecurity.org/wiki/TestDisk_Download	Windows/Linux/Mac OS X	• Se puede ejecutar en los sistemas operativos: DOS/Win9x, Windows NT 4/2000/XP/2003, Linux, FreeBSD, NetBSD, OpenBSD, Sun Solaris, Mac OS X. • Recupera archivos perdidos	Recuperación

7			incluyendo videos, documentos y archivos de los discos duros y CDRoms • Recupera imágenes perdidas de las memorias de las cámaras fotográficas, MP3 players, PenDrives, etc. • Ignora el sistema de archivos y hace una búsqueda profunda de los datos, funcionando incluso si su sistema de archivos está muy dañado o ha sido reformateado. • Usa acceso de solo lectura para manejar la unidad o la tarjeta de memoria de la que está a punto de recuperar los datos perdidos. • Funciona con discos duros, CD-ROM, tarjetas de memoria (CompactFlash, Memory Stick, Secure Digital / SD, SmartMedia, Microdrive, MMC, etc.), unidades de memoria USB, imagen sin formato DD, imagen EnCase E01, etc. • Busca encabezados de archivos conocidos, puede recuperar todo el archivo. • Reconoce y recupera numerosos formatos de archivo, incluyendo ZIP, Office, PDF, HTML, JPEG y varios formatos de archivos gráficos.	

			Fabricada por el proyecto GNU, la última versión es 7.0 del 18/04/2015	
8	Puran file recovery http://www.puransoftware.com/File-Recovery-Download.html	Windows	• Exploración rápida que enumera los archivos eliminados en un clic y unos segundos. Es compatible con FAT12 / 16/32 y NTFS. • Exploración profunda que puede escanear de forma inteligente un byte a byte de la unidad. • Exploración completa que puede detectar particiones eliminadas / eliminadas e incluso recuperar archivos de unidades formateadas. • Deep / Full Scan no solo busca registros de archivos perdidos, sino que también detecta archivos de diferentes formatos basados en patrones de datos. • Se incluyen más de 50 formatos / listas de patrones de datos ampliables a cientos de formatos. • Los archivos recuperados se pueden guardar con su estructura de ruta intacta. • Los archivos se enumeran en árbol y vistas de lista. Todos los archivos se pueden previsualizar antes de la recuperación. • También está disponible una versión portátil oficial que incluso puede ejecutarse en el entorno BartPE.	Recuperación

			• Es compatible con Windows XP / 2003 / Vista / 2008/7/8/10, incluidas las versiones de 64 bits. Fabricada por Puransoftware, la última versión es 1.2.1 del 15/06/2016	
9	Ddrescue https://www.gnu.org/software/software.html	Linux	• Copia datos de un archivo o dispositivo de bloque (disco duro, cdrom, etc.) a otro, tratando de rescatar primero las partes buenas en caso de errores de lectura. • La operación básica de ddrescue es completamente automática. Es decir, no tiene que esperar un error, detener el programa, reiniciarlo desde una nueva posición, etc. • Si utiliza la función mapfile de ddrescue, los datos se rescatan de manera muy eficiente (solo se leen los bloques necesarios). • Puede interrumpir el rescate en cualquier momento y reanudarlo más tarde en el mismo punto. • El archivo de mapa se guarda periódicamente en el disco. Entonces, en caso de un accidente, puede reanudar el rescate con poca copia. • El archivo de mapa se puede usar para múltiples comandos que copian diferentes áreas del archivo y para múltiples intentos de recuperación	Recuperación

			en diferentes subconjuntos. • Es independiente de la interfaz y, por lo tanto, puede utilizarse para cualquier tipo de dispositivo compatible con su núcleo (ATA, SATA, SCSI, unidades MFM antiguas, disquetes o incluso tarjetas multimedia flash como SD) Fabricada por el proyecto GNU, la última versión es 2.0 del 21/02/2017.	
10	Air (Imagen y Restauración Automática) https://sourceforge.net/projects/air-imager/	Linux	• Autodetección de discos IDE y SCSI, CD-ROMs, y unidades de cinta • Opción de elegir entre dd o dc3dd • Verificación de imágenes entre fuente y copia vía MD5 o SHA1/256/384/512 • Compresión/descompresión de imagen vía gzip/bzip2 • Soporte a unidades de cinta SCSI • División de imágenes en múltiples segmentos Fabricada por el proyecto GNU, la última versión es 6.12.3 del 26/04/2013.	Analisis y recuperación

Tabla 6 : Cuadro comparativo herramientas de recolección de información Memoria

RELEVANCIA	HERRAMIENTA/ SITIO DE DESCARGA	SISTEMA OPERATIVO	DESCRIPCIÓN	TIPO
1	FTK Imager http://www.accessdata.com/downloads.html	Windows	Esta herramienta tiene una gran ventaja para los que no se llevan bien con la línea de comandos: su interfaz gráfica, que permite crear imágenes de todo tipo con cómodos asistentes y funciones agrupadas en menús. Además, al tratarse de una herramienta Windows, FTK Imager es fácil de instalar y permite operar con dispositivos sujetos a controladores no universales, que muchas veces dificultan su montaje otros sistemas y que dotan al análisis en este tipo de plataformas de una laboriosidad adicional que no todo el mundo puede afrontar. Fabricada por AccesData, su última versión es la 3.4.3 del 2016/11/07z	Recuperación y análisis
	Volatility http://www.volatilityfoundation.org/releases	Windows/Linux	Volatility admite volcados de memoria de las principales versiones y paquetes de servicios de 32 y 64 bits de Windows, incluidos XP, 2003 Server, Vista, Server 2008, Server 2008 R2 y Seven. Ya sea que el volcado de memoria esté en formato sin formato, un volcado de fallas de Microsoft, un archivo de hibernación o una instantánea de máquina virtual, Volatility puede trabajar con él. También ahora admite volcados de memoria de	Análisis

2			Linux en formato raw o LiME e incluyen más de 35 complementos para analizar núcleos de Linux de 32 y 64 bits de 2.6.11 - 3.5.x y distribuciones como Debian, Ubuntu, OpenSuSE, Fedora, CentOS y Mandrágora. Admite 38 versiones de volcados de memoria Mac OSX de 10.5 a 10.8.3 Mountain Lion, tanto de 32 como de 64 bits. Los teléfonos Android con procesadores ARM también son compatibles. El soporte para Windows 8, 8.1, Server 2012, 2012 R2 y OSX 10.9 (Mavericks). Fabricada por Volatility Foundation, su última versión es la 2.6 del 2016/12/12.	
3	Memorize https://www.fireeye.fr/content/dam/fireeye-www/services/freeware/ug-memoryze.pdf	Windows/ Mac OS X	Memoryze puede adquirir y/o analizar imágenes de memoria, puede incluir el archivo de paginación en su análisis. Puede realizar lo siguiente: • Enumerar todos los procesos en ejecución (incluidos los ocultos por rootkits), incluyendo: • Informa todos los identificadores abiertos en un proceso (incluidos todos los archivos, claves del registro, etc.) • Enumere el espacio de direcciones virtuales de un proceso dado incluyendo todas las DLL cargadas y todas las partes asignadas del montón y la pila	Recolección y análisis

			• Enumera todos los sockets de red que el proceso ha abierto, incluidos los ocultos por los rootkits. • Especifique las funciones importadas y exportadas por el EXE y las DLL. • Hachea el EXE y los DLL en el espacio de direcciones del proceso (MD5, SHA1, SHA256. Está basado en disco). • Comprueba las firmas digitales de los EXE y DLL (basado en disco). • Produce todas las cadenas en memoria por proceso. Puede ser utilizada en los sistemas operativos de Windows y Mac. Fabricada por Mandian, su última versión es la 3.0 del 2013/06/23.	
4	RedLine https://www.fireeye.com/services/freeware/redline.html	Windows	Esta herramienta le permite analizar una memoria potencialmente comprometida del sistema operativo (OS) de Windows y estructura de archivos para encontrar signos de actividad maliciosa. Con Redline, puede: - Recopilar procesos de ejecución, archivos, datos de registro e imágenes de memoria. - Ver los datos importados, incluyendo el estrechamiento y el	Análisis

			filtrado de los resultados alrededor de un plazo determinado - Realizar el análisis de Indicadores de Compromiso (IOC). Fabricada por Endpoint, su última versión es la 1.20 del 2017/05/03	
5	LiME (Linux Memory Extractor) https://github.com/halpomeranz/lmg/	Linux	Permite la adquisición de memoria volátil de dispositivos basados en Linux como Android. Esto hace que LiME sea única ya que es la primera herramienta que permite obtener capturas de memoria completas en dispositivos Android. También minimiza su interacción entre los procesos del usuario y del espacio del kernel durante la adquisición, lo que le permite producir capturas de memoria que son más forenses que las de otras herramientas diseñadas para la adquisición de la memoria de Linux. LiME está destinado a capturar evidencia que puede ser relevante en investigaciones criminales y civiles. Características: • Completa adquisición de memoria Android • Adquisición sobre la interfaz de red • Mínima huella de proceso Fabricada por Proyecto GNU, su última versión es la 1.7.2.	Recuperación

3.4 SELECCIÓN Y PRUEBA DE HERRAMIENTAS.

Basados en la fase anterior se decide tomar las herramientas Autopsy y Recuva de las herramientas de recolección de información en disco y, FTKimager y Volatility de las herramientas de recolección de información en memoria para la realización de las pruebas, ya que cuentan con mejor calificación dentro del cuadro comparativo registrado en las tablas 5 y 6 respectivamente, su manejo es más sencillo, cuentan con mejores características y técnicas de recolección de información más apropiadas.

3.4.1 Descarga, instalación y prueba con Autopsy

1. Descarga.

Nos dirigimos al enlace de descarga https://www.sleuthkit.org/autopsy/download.php

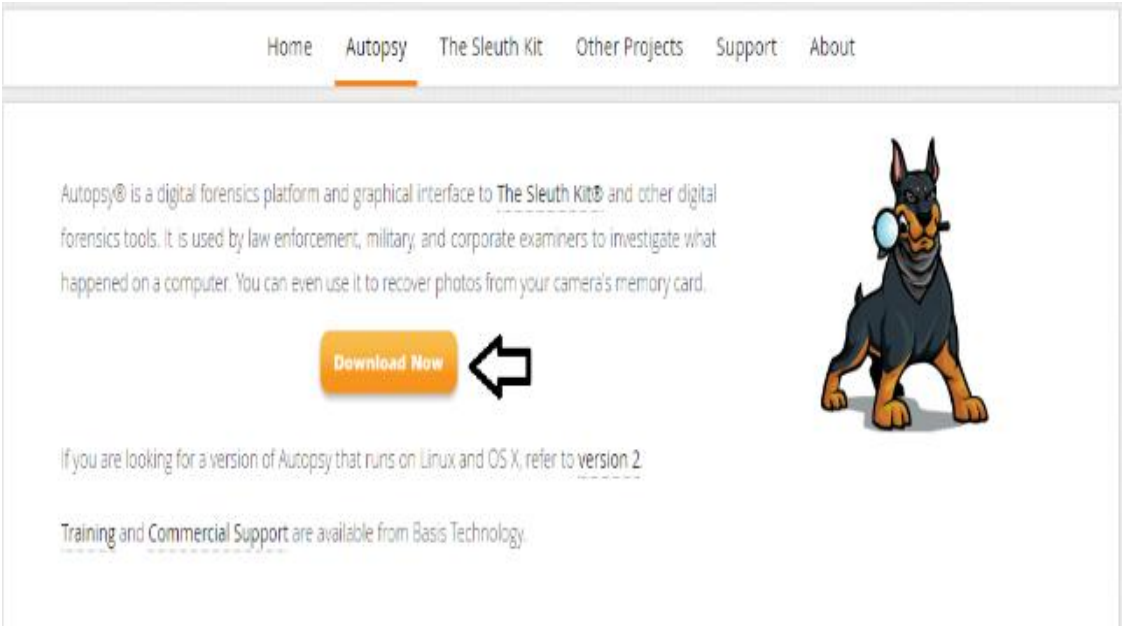


Imagen 7 : Captura descarga de autopsy

Se elige 32 -bit o 64-bit, dependiendo del sistema operativo que se tenga.

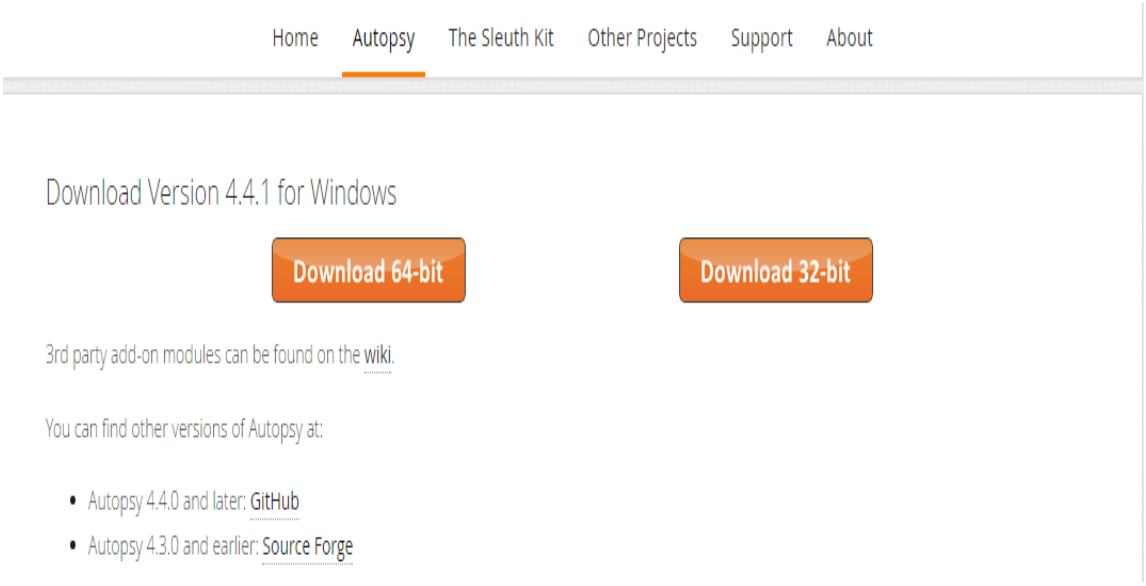


Imagen 8: Captura opción de descarga de autopsy

2. Instalación de Autopsy

Buscar el archivo que se descargó y dar click para abrir el asistente de instalación.

Click en Next.

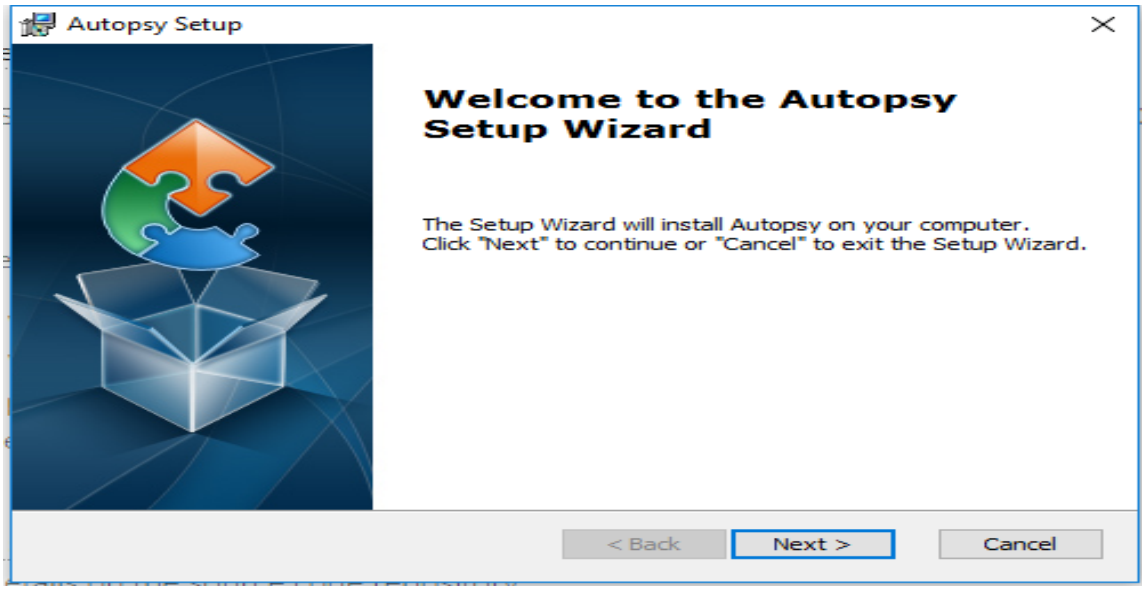


Imagen 9: Captura instalación autopsy

Se elige la ruta donde quedará instalado, click en next.

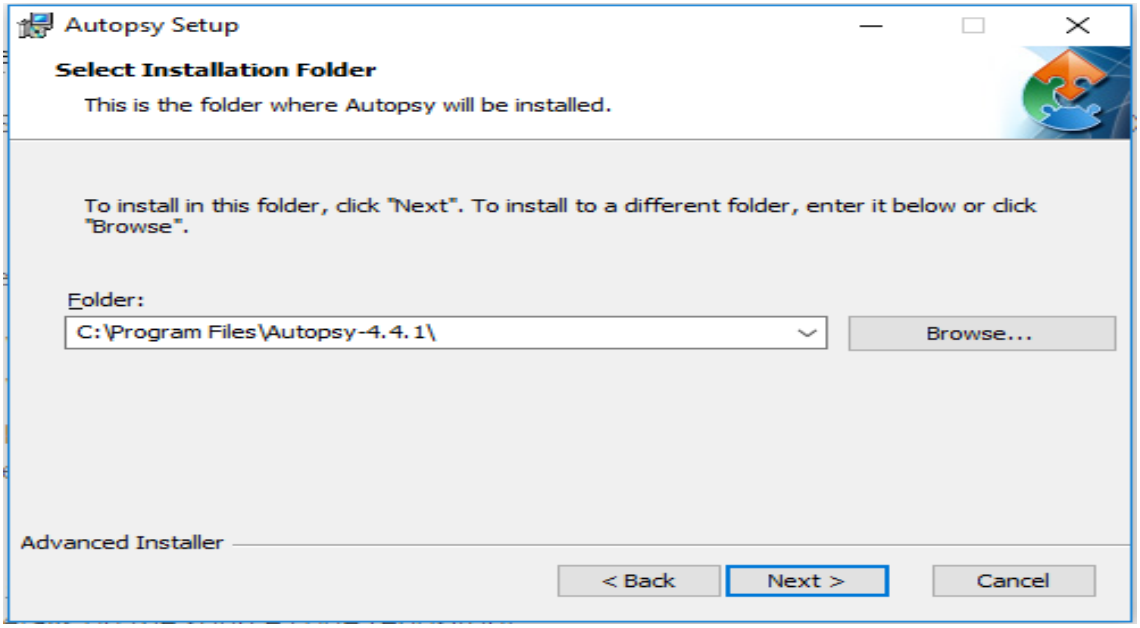


Imagen 10: Captura ruta instalación

Click en Install, para iniciar la instalación.

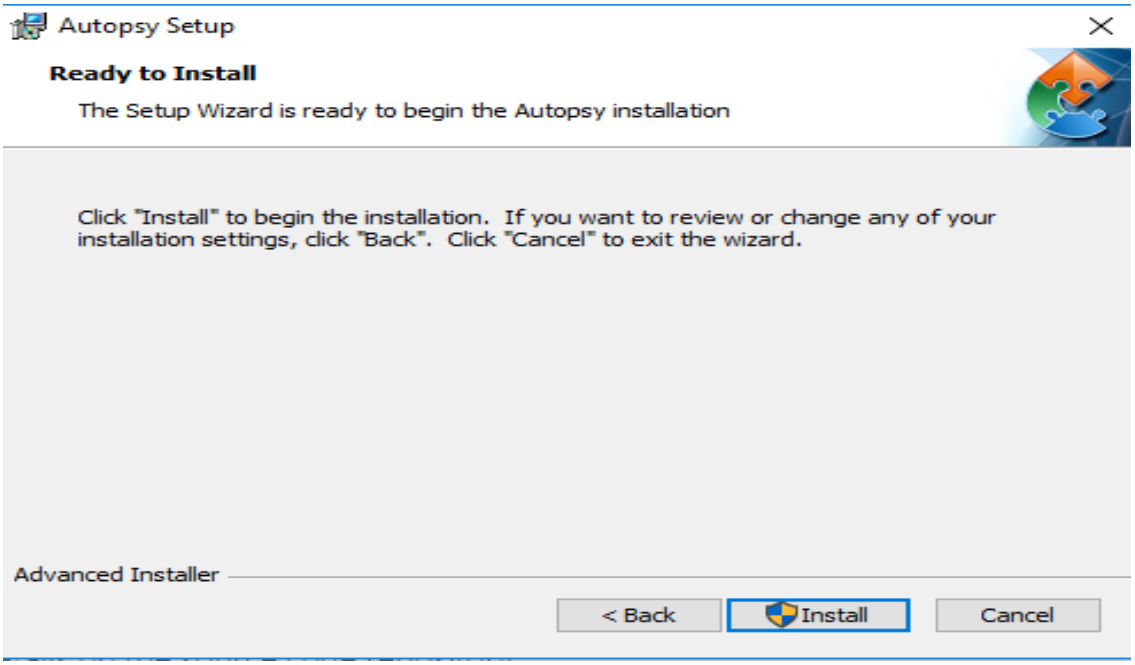


Imagen 11: Instalación

Se espera que termine el proceso de instalación.

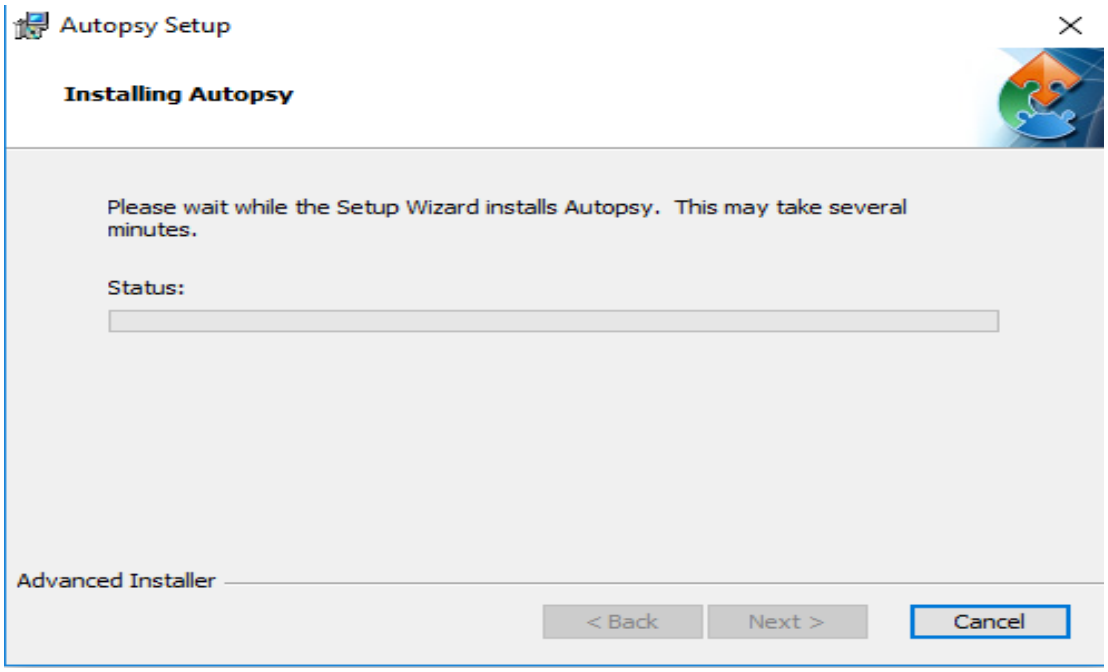


Imagen 12: Proceso de instalación

Click en finalizar

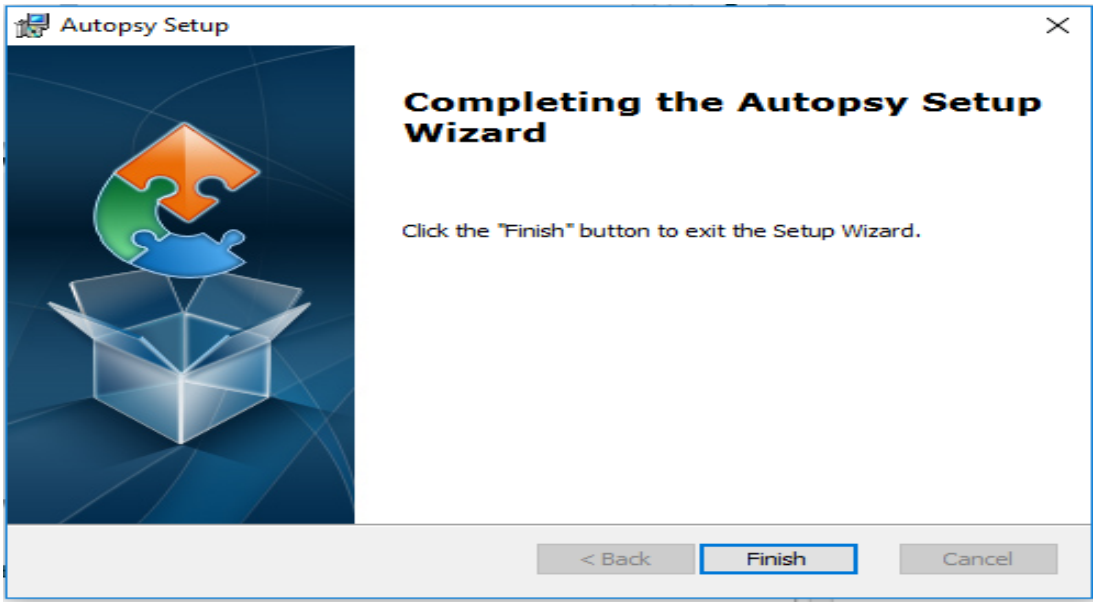


Imagen 13: Finalización de la instalación.

3.4.1.1 Prueba de Autopsy

Autopsy crea una imagen del disco que se va a analizar con toda la información que este contiene, con el fin de analizarla y así no alterar la información que se encuentra en el disco original, esta herramienta es muy útil para realizar análisis forense en casos judiciales o a empleados que estén afectando una empresa ya que con esta se puede realizar el análisis sin alterar la evidencia original

Para la prueba se va a utilizar un disco duro con sistema operativo Windows 7, extraído de un computador portátil HP.

Disco Duro

Imagen 14: Disco Duro para pruebas

La prueba se realizará con el programa Autopsy de la siguiente manera:

1. Se abre el programa y se le da la opción “Create New Case” (Crear un caso nuevo) o si ya tiene un caso abierto se le da en “Open existing Case” (caso existente).

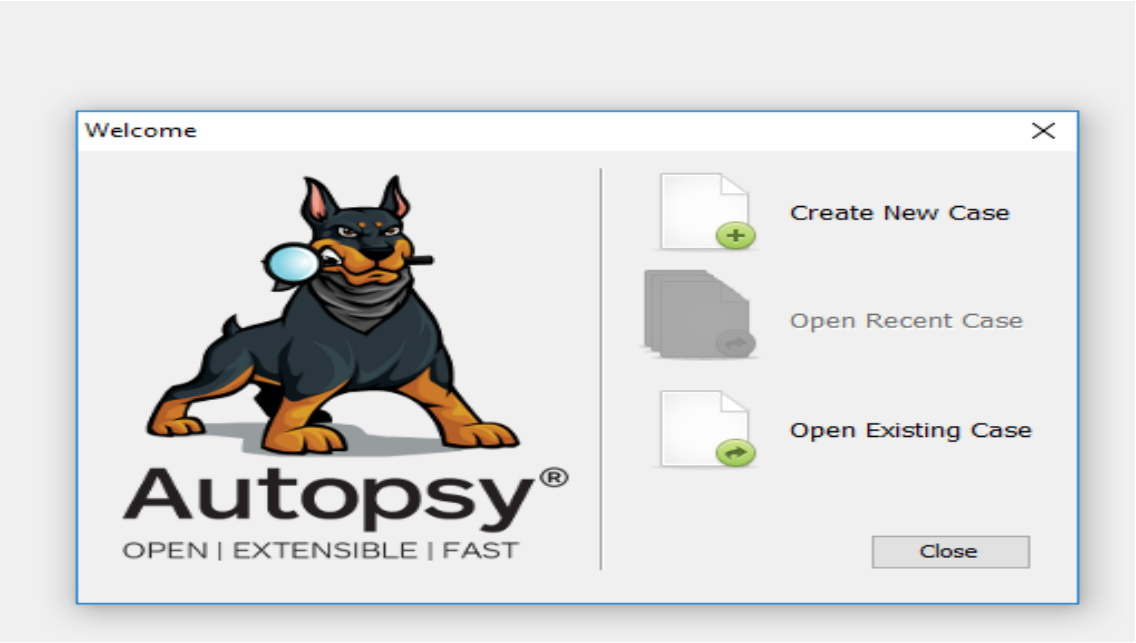


Imagen 15: Captura creación caso autopsy

2. Se coloca el nombre del caso o procedimiento que se va a realizar, la ruta donde se va a guardar la imagen y click en “Next”.

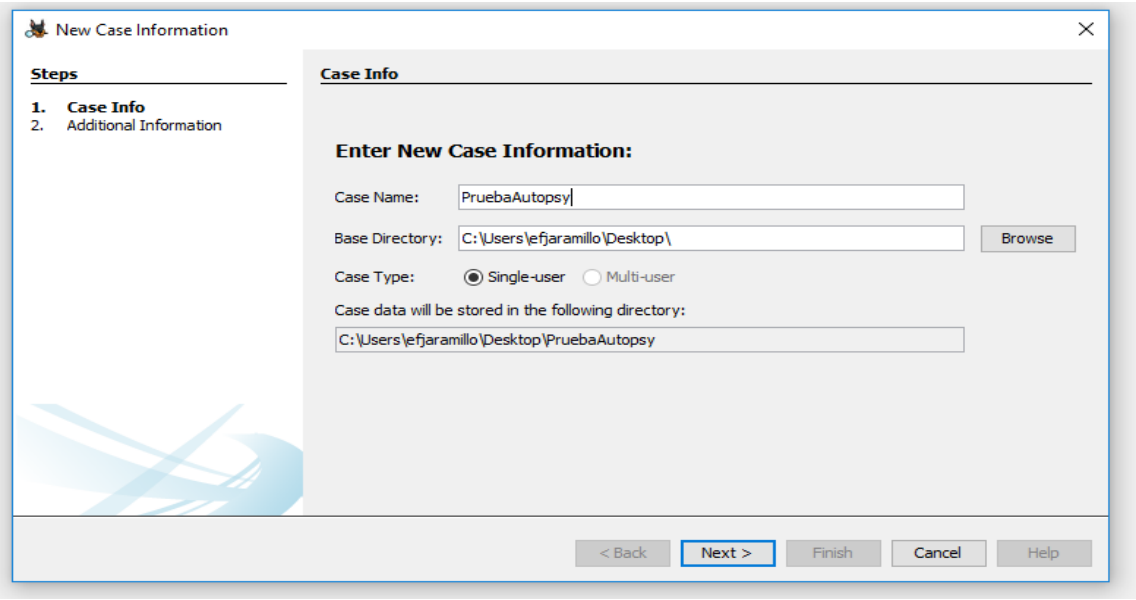


Imagen 16: Captura Ruta del caso autopsy

3. Se coloca el número del caso y quien lo está realizando y click en “finish”.

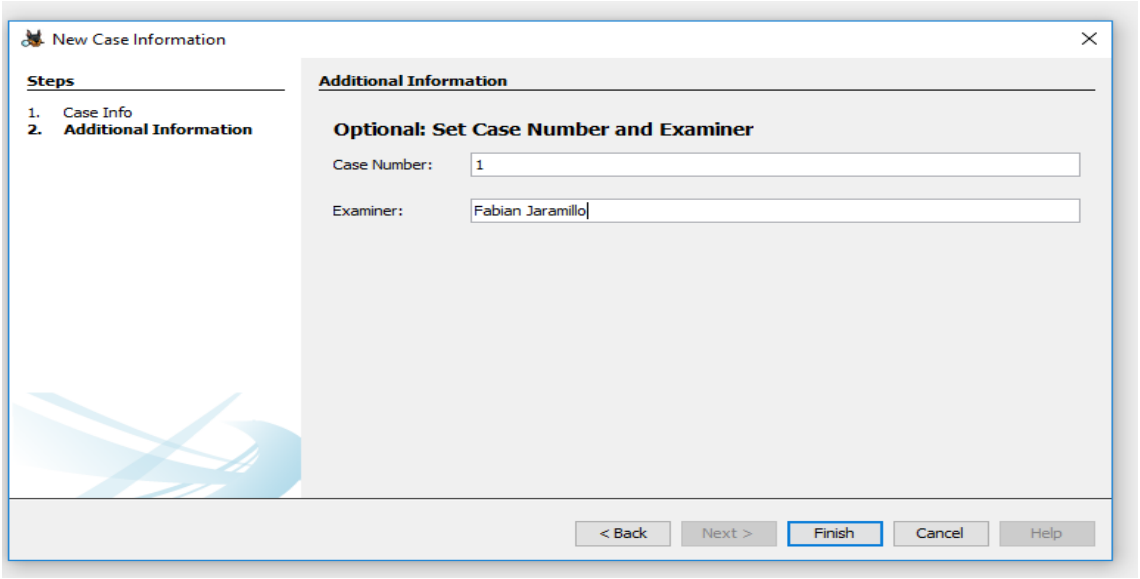


Imagen 17: Captura número de caso autopsy.

4. Comienza la creación del caso.

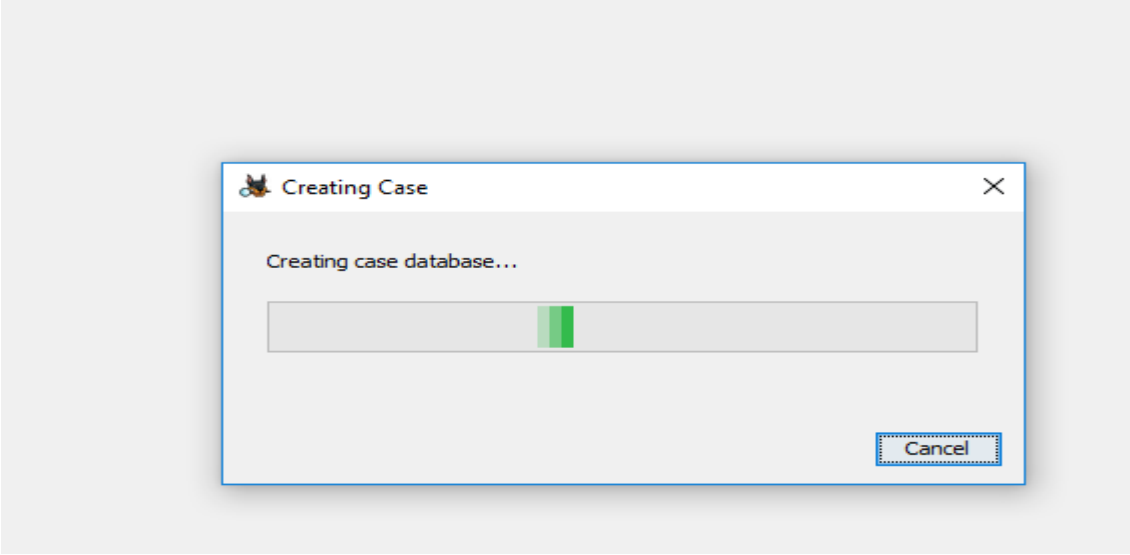


Imagen 18: Captura creación base datos del caso

5. En esta parte se va a elegir la fuente de donde se va a sacar la imagen la cual va a ser analizada, tiene 4 opciones.

- Disco de máquinas virtuales

- Disco Local
- Archivos Lógicos
- Archivo de imagen de espacio sin asignar.

En este caso se va a utilizar un disco físico, por tanto, seleccionamos la segunda opción "Local Disk" y click en "Next".

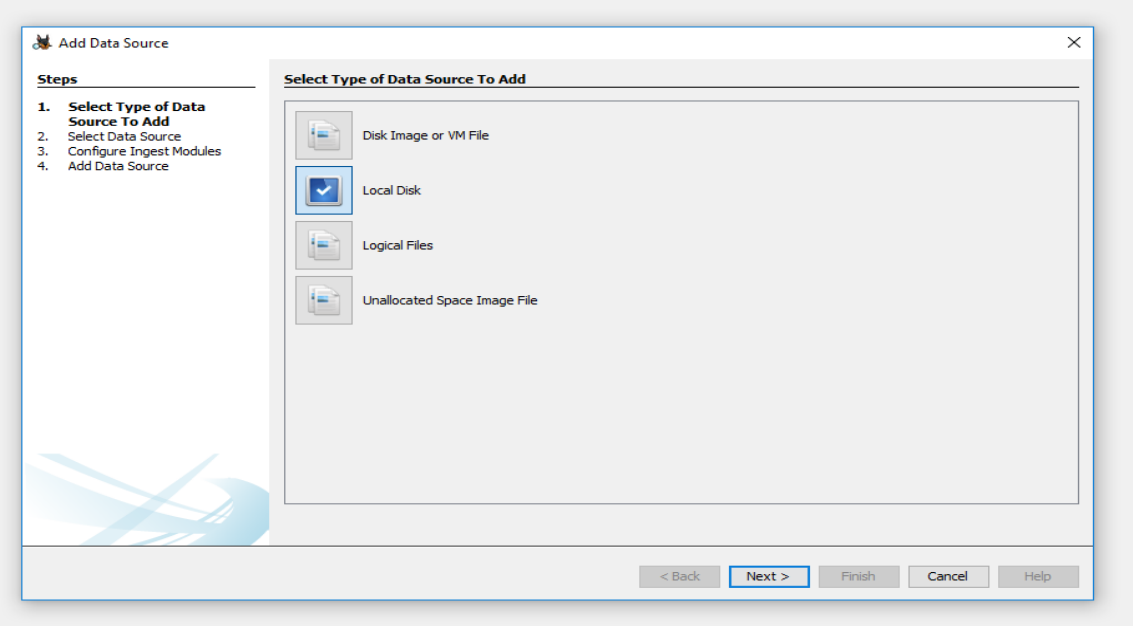


Imagen 19: Captura opciones del caso

6. Seleccionamos la unidad a la cual se le va a sacar la imagen, en este caso es la unidad Disco Local (I:), y click en "Next".

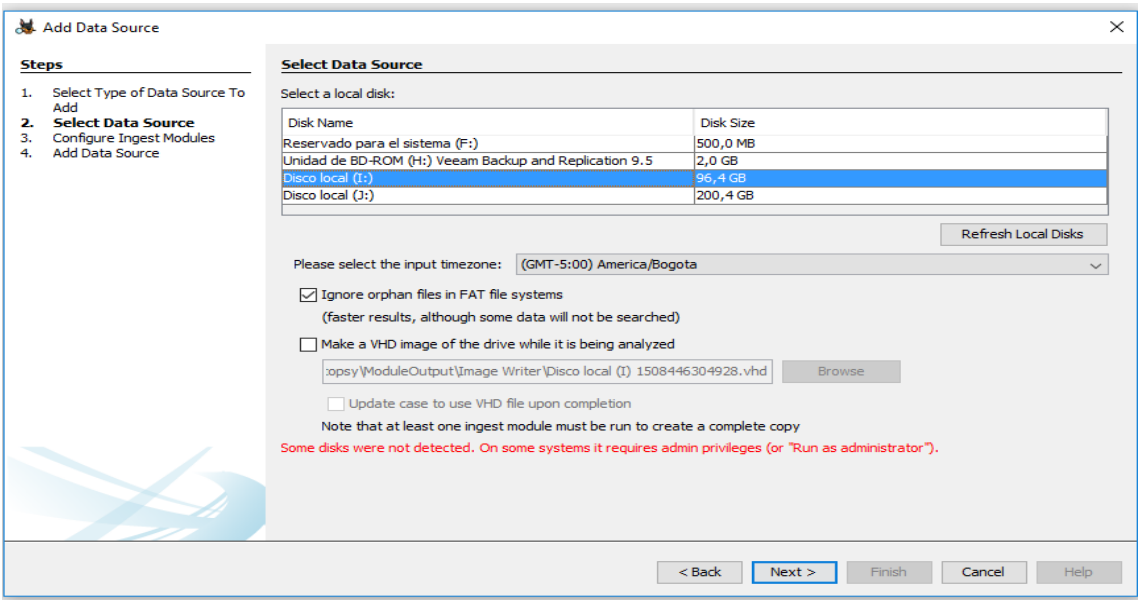


Imagen 20: Captura selección del disco a analizar.

7. La siguiente ventana muestra la configuración de los módulos que van a ser analizados en la imagen, se seleccionan los necesarios y click en “Next”.

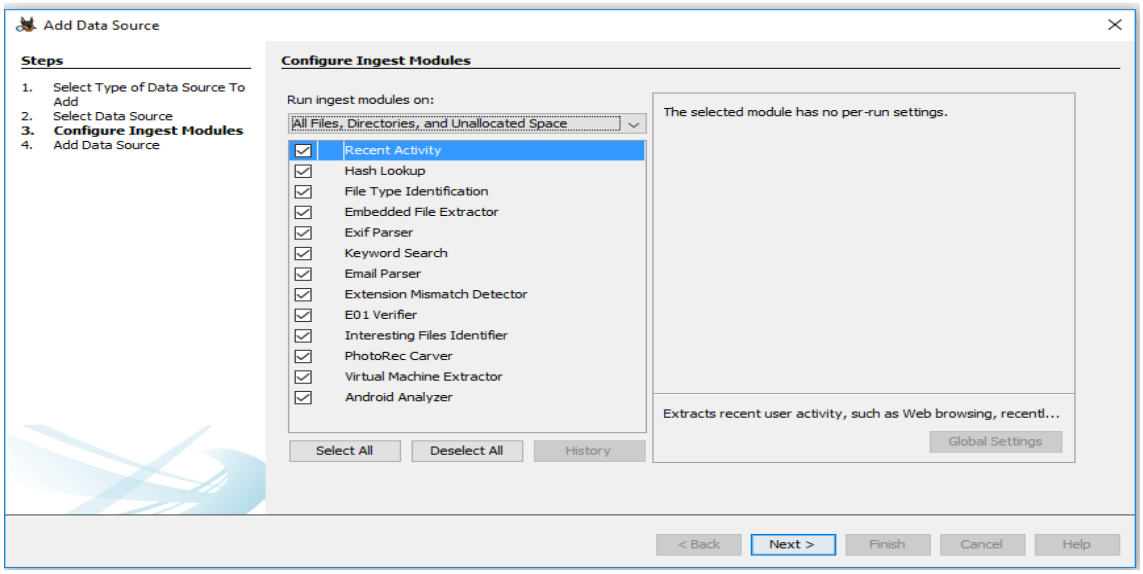


Imagen 21: Captura de lo que va a escanear el programa

8. Comienza el proceso de creación de la imagen a analizar, el disco original se entrega para su custodia, así no sufrirá ninguna alteración.

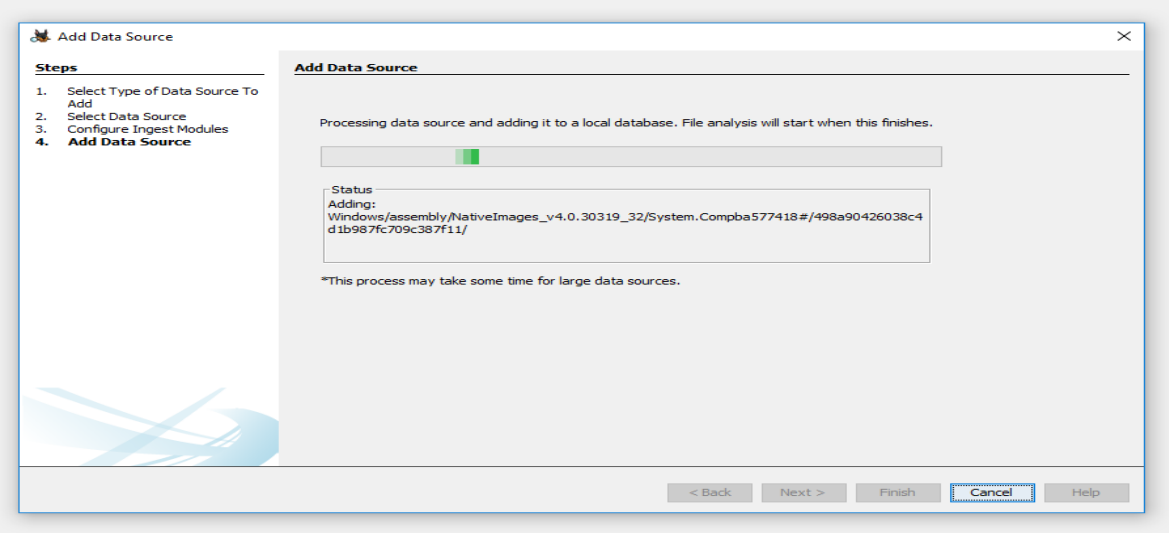


Imagen 22: Captura del proceso de creación de disco virtual

9. Termina la creación del disco, clic en "Finish".

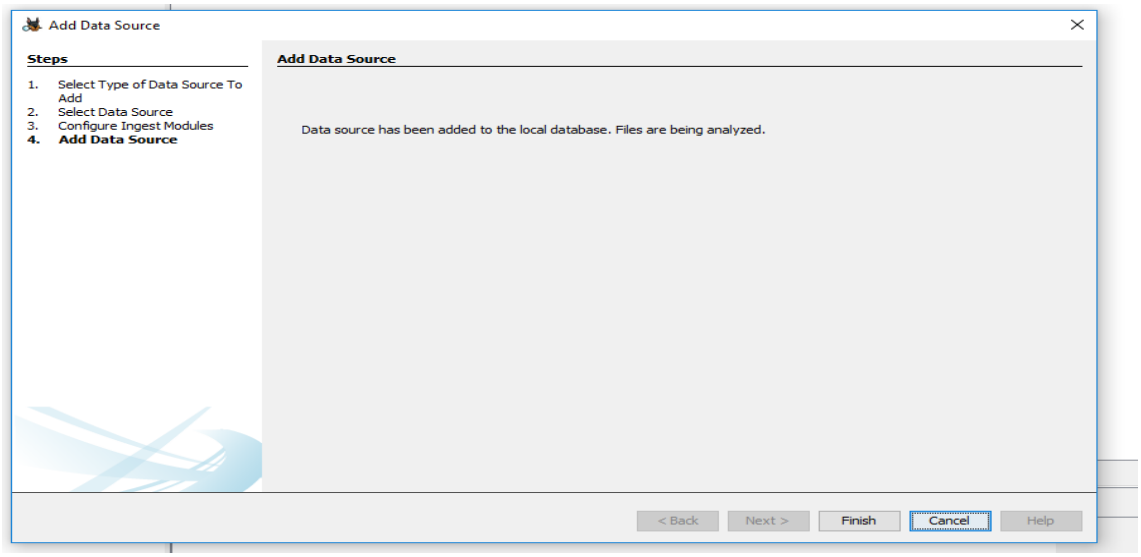


Imagen 23: Captura finalización de la creación del disco virtual

10. En la siguiente imagen se observa que Autopsy realiza la extracción de contenido muy valioso para una investigación, como búsquedas web realizadas y documentos recientemente abiertos, también muestra la cantidad de archivos encontrados de cada tipo. Esto tomaría mucho tiempo y sería tedioso de realizar para un investigador en forma

manual.

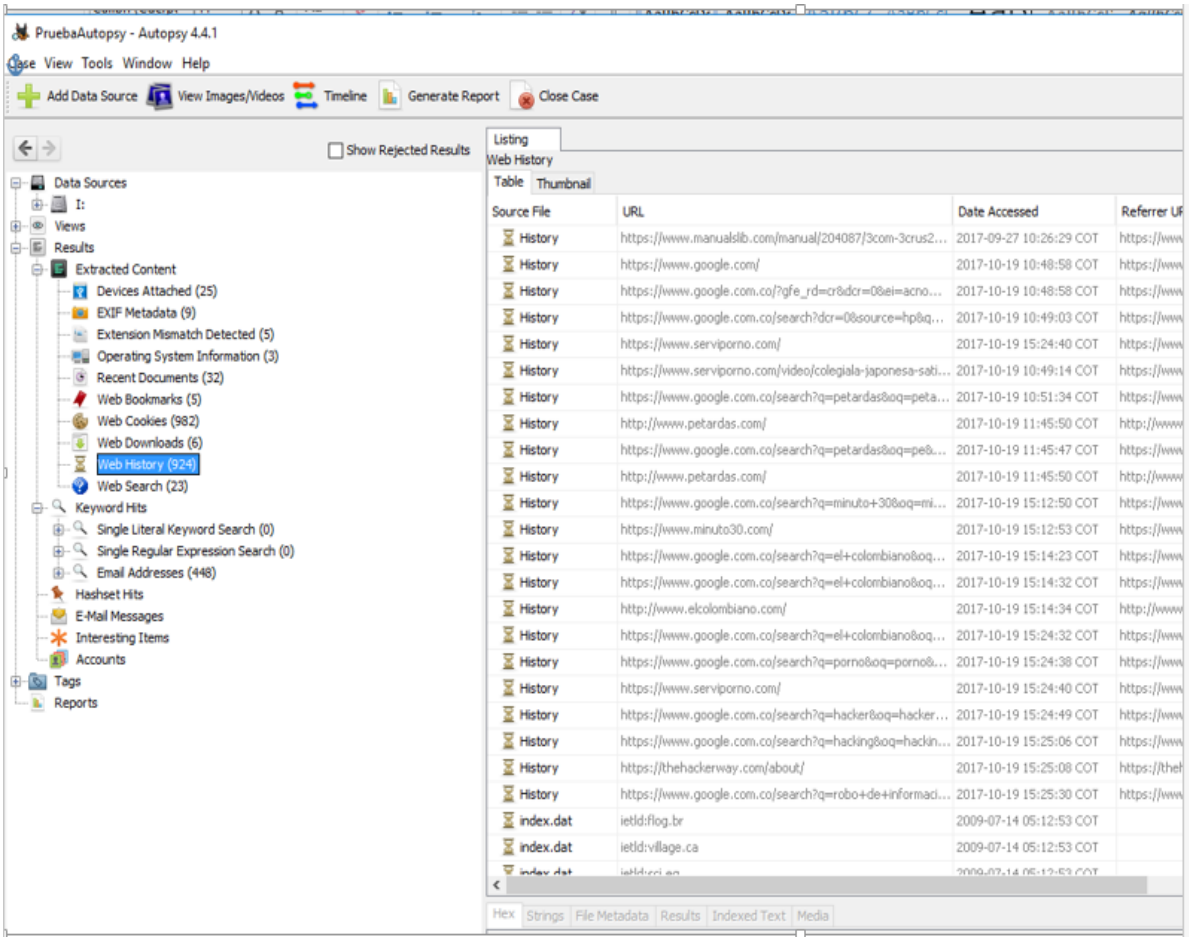


Imagen 24: Captura historial web

En la imagen a continuación se observa que el sistema de archivos es de tipo NTF y que existen varios usuarios en el sistema. Luego, a partir de simple inspección y del análisis del registro de Windows, puede obtenerse información como la zona horaria utilizada, el nombre bajo el cual fue registrado el sistema operativo.

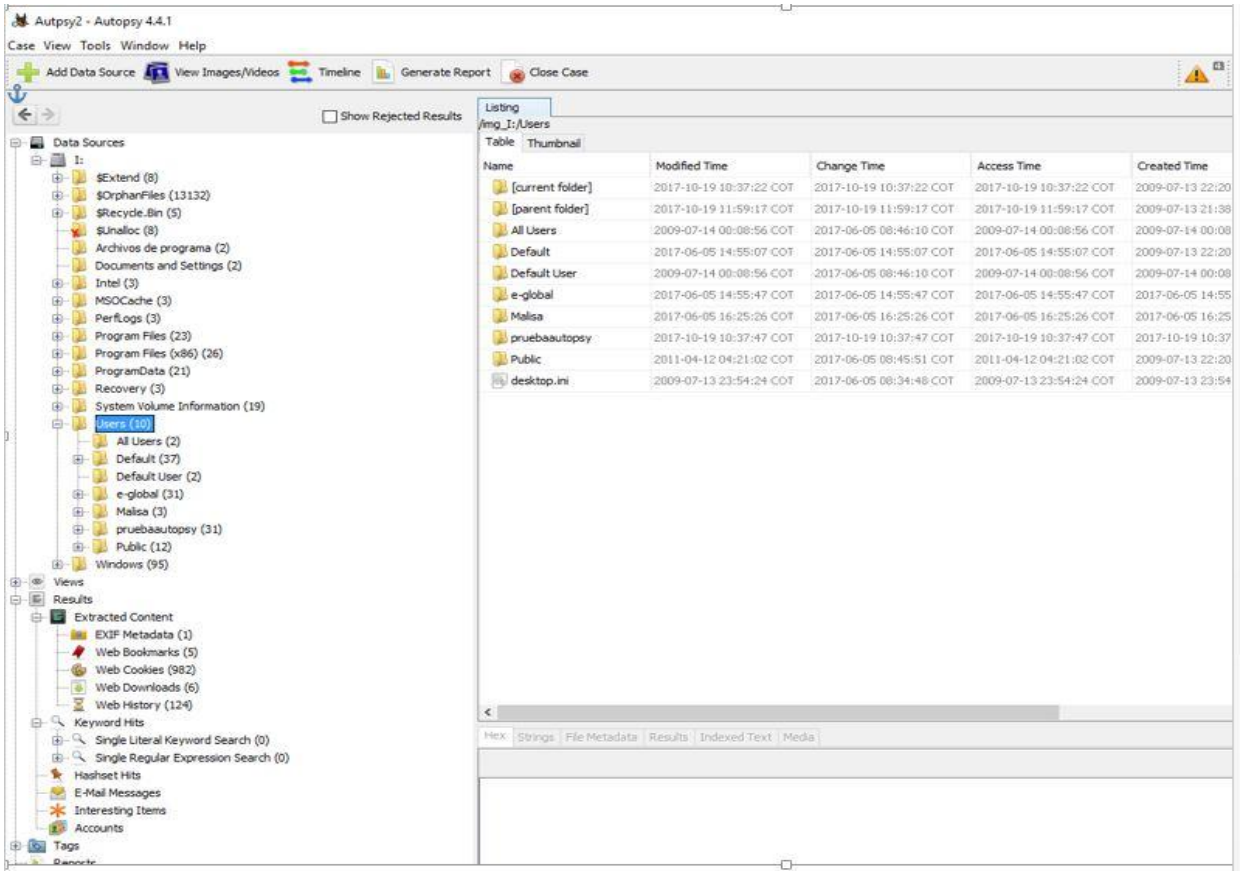


Imagen 25: Captura usuarios en el disco

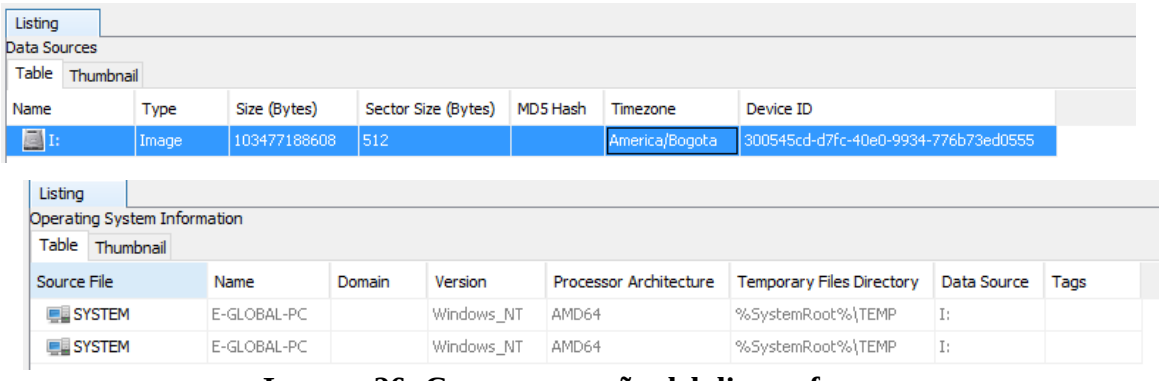


Imagen 26: Captura tamaño del disco y formato

Autopsy agrupa los archivos en categorías, de tal manera que puedan verse rápidamente la cantidad de imágenes, audio o documentos presentes en el sistema de archivos, clasificados por extensión.

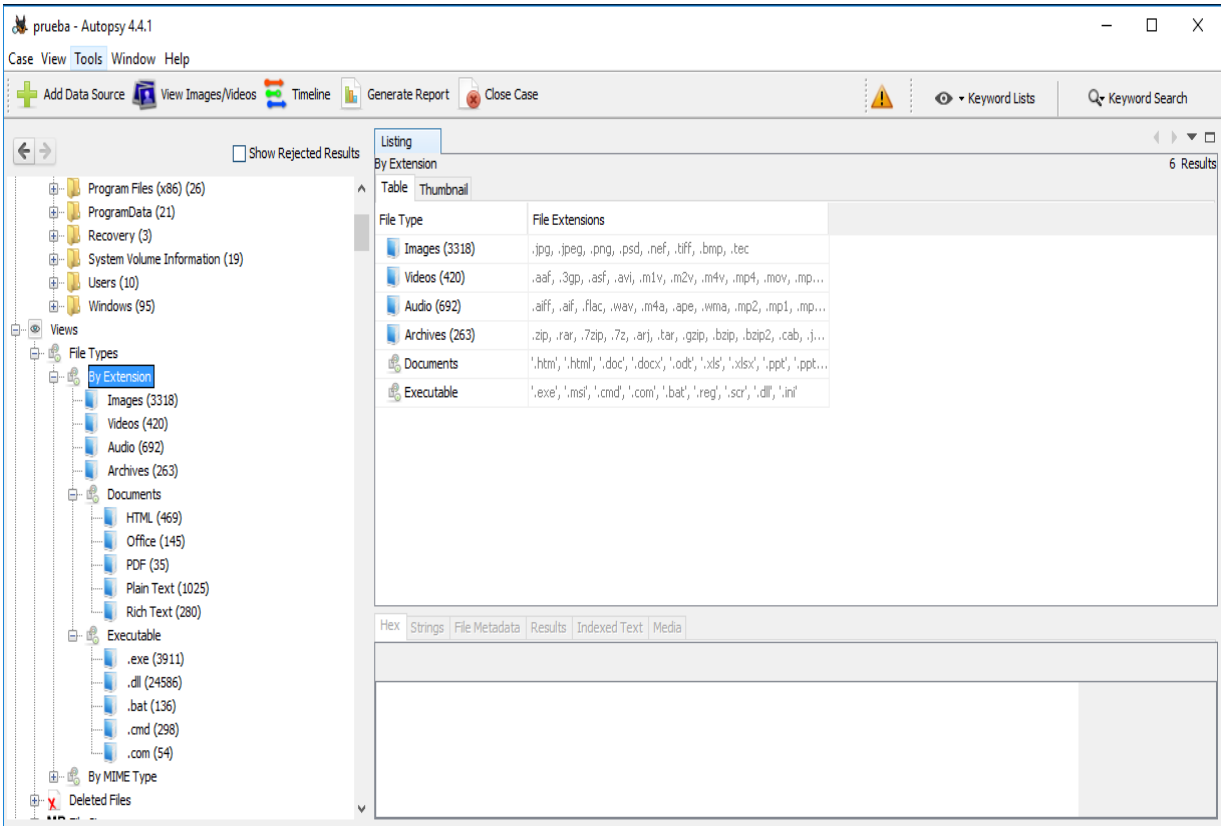


Imagen 27: Captura total de archivos en el disco

Autopsy indica los documentos más recientes que fueron abiertos, la fecha y el usuario que los abrió.

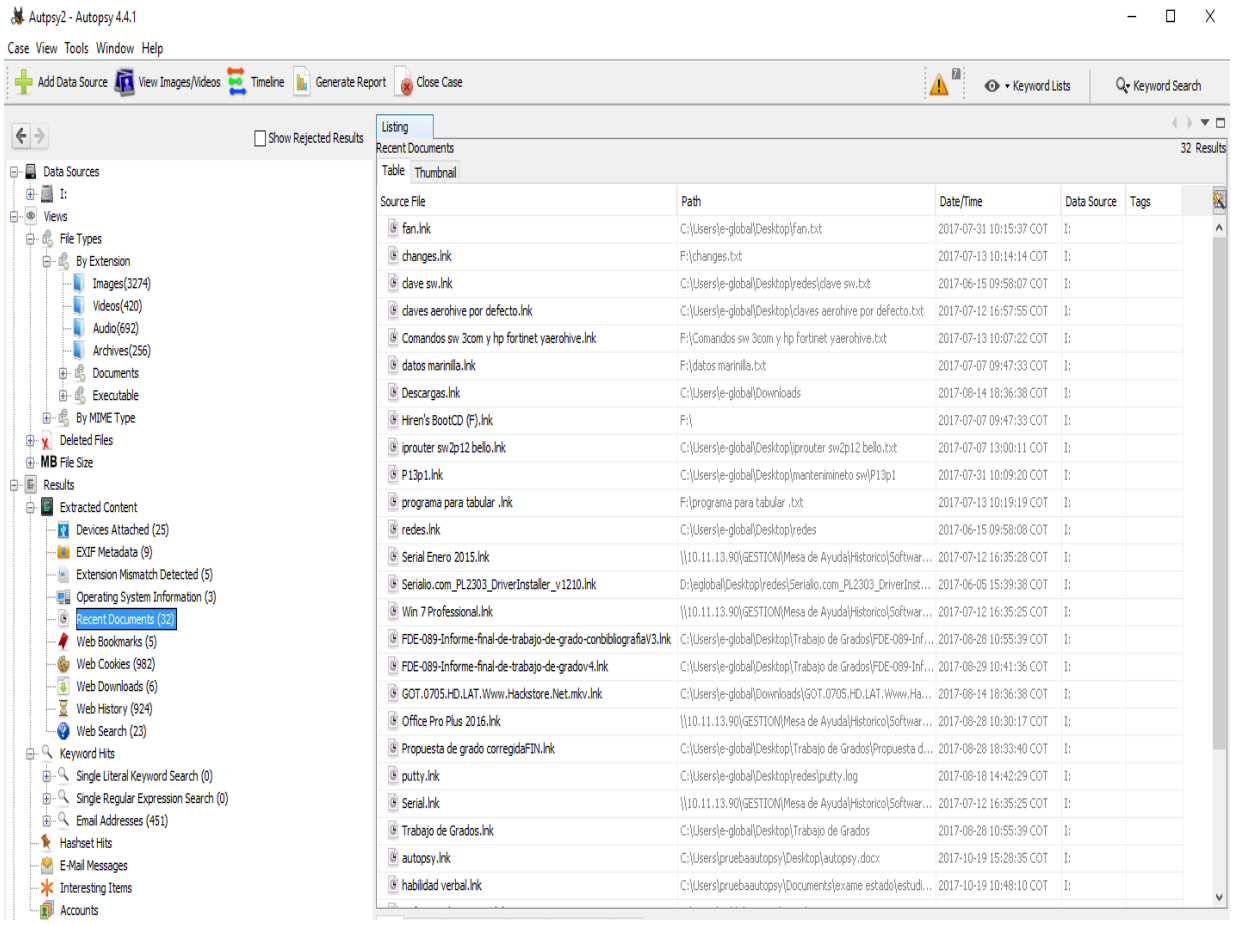


Imagen 28: Captura archivos abiertos recientes

También es posible conocer las direcciones de correo que el usuario ha utilizado para el envío de mensajes.

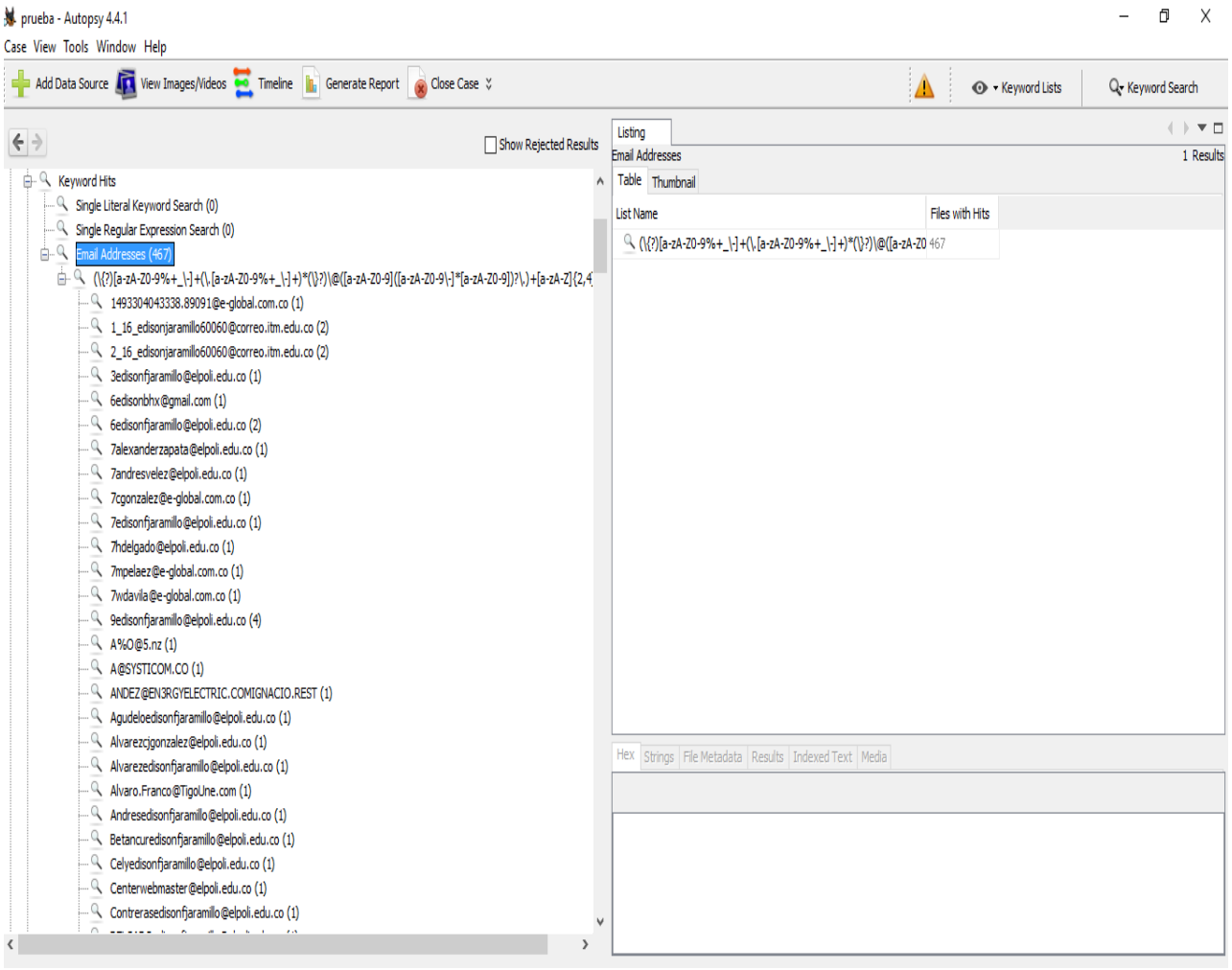


Imagen 29: Captura Direcciones de correo usadas

Los resultados obtenidos pueden ser exportados a documentos HTML, entre otros formatos ofrecidos, para la presentación de lo encontrado en cualquier otro equipo que no cuente con Autopsy.

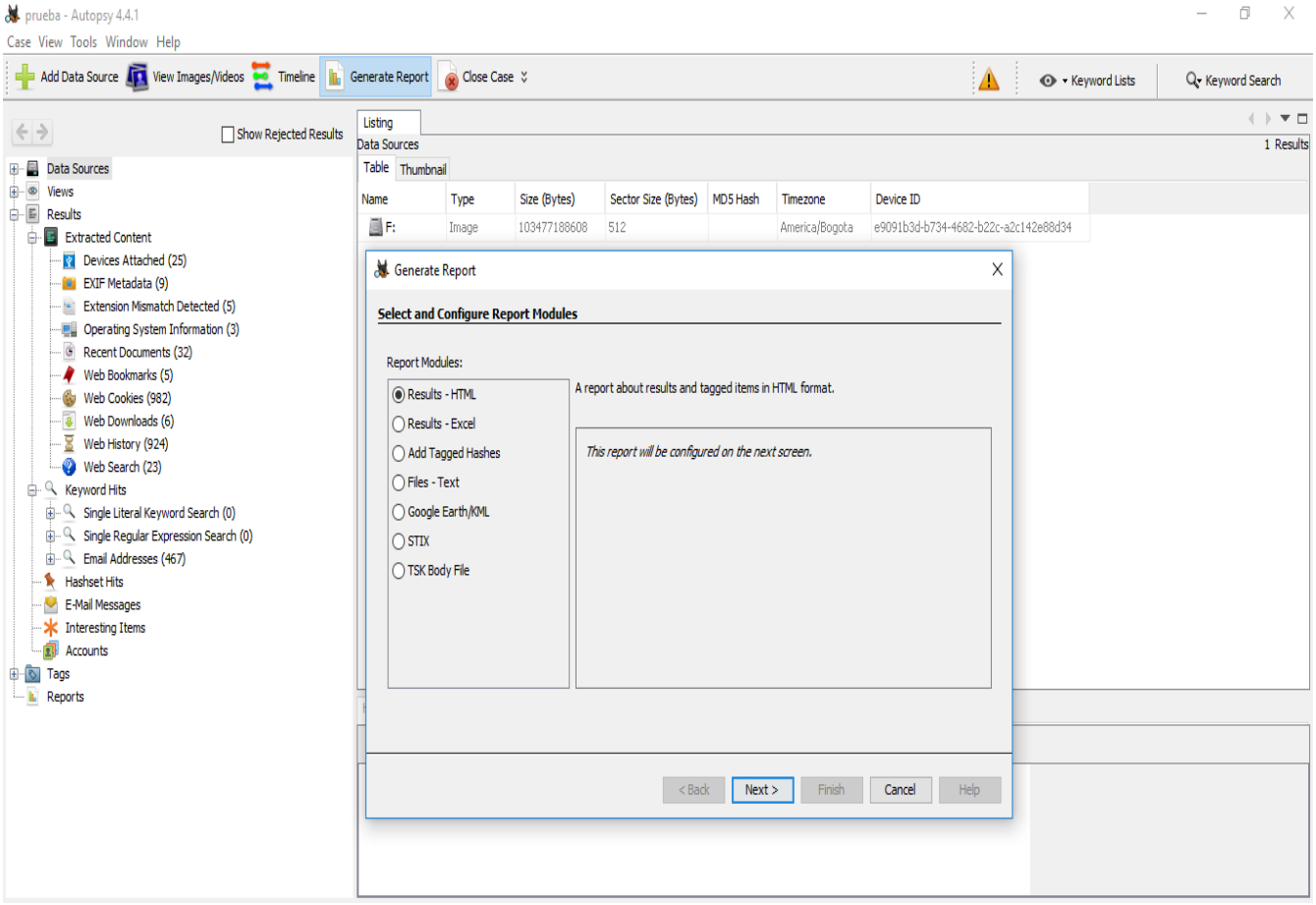


Imagen 30: Captura formatos de exportar los resultados

Conclusión de la herramienta Autopsy

De acuerdo con los resultados de la prueba con Autopsy, se puede decir que es una herramienta muy completa para un análisis forense, ya que recopila mucha información importante para la investigación y que pueden ser evidencias. Una de sus ventajas es que no se altera la información en el disco original, ya que crea una imagen, el origen queda intacto, respetando la cadena de custodia.

3.4.2 Descarga, instalación y prueba con Recuva.

1. El programa se puede descargar de la página https://www.piriform.com/recuva.

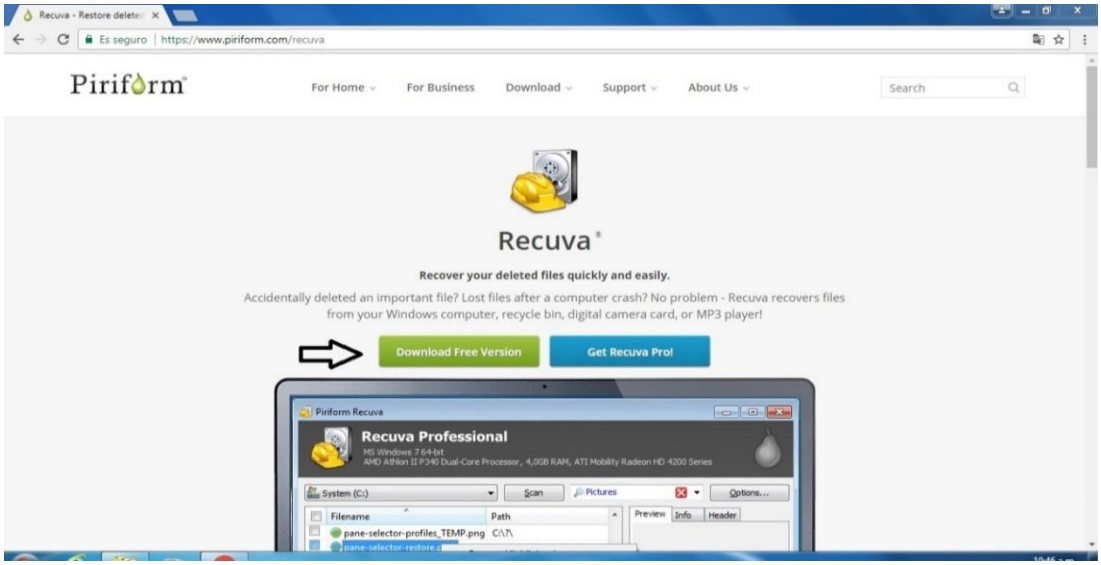


Imagen 31: Captura de descarga Recuva

2. Dar clic donde indica la flecha para descargar la versión libre.

Imagen 32 :Captura de versión Recuva

3. Se descarga del servidor de Piriform como lo muestra la imagen.

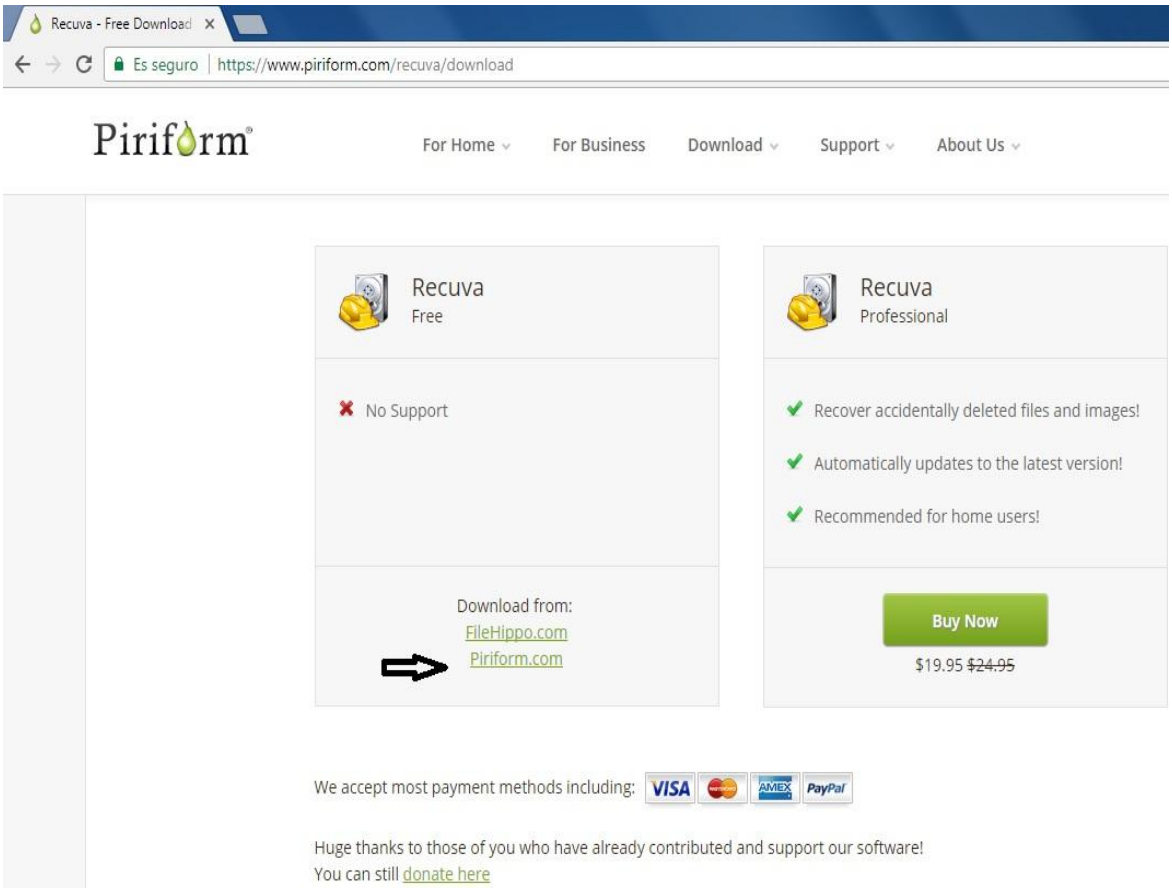


Imagen 33: Captura descarga versión free

4. Después de descargar el programa, lo ejecutamos y le damos en la opción “install” como muestra la imagen siguiente.

Imagen 34: Captura instalación Recuva

5. Cuando haya terminado la instalación, se da clic en la opción "Run Recuva".

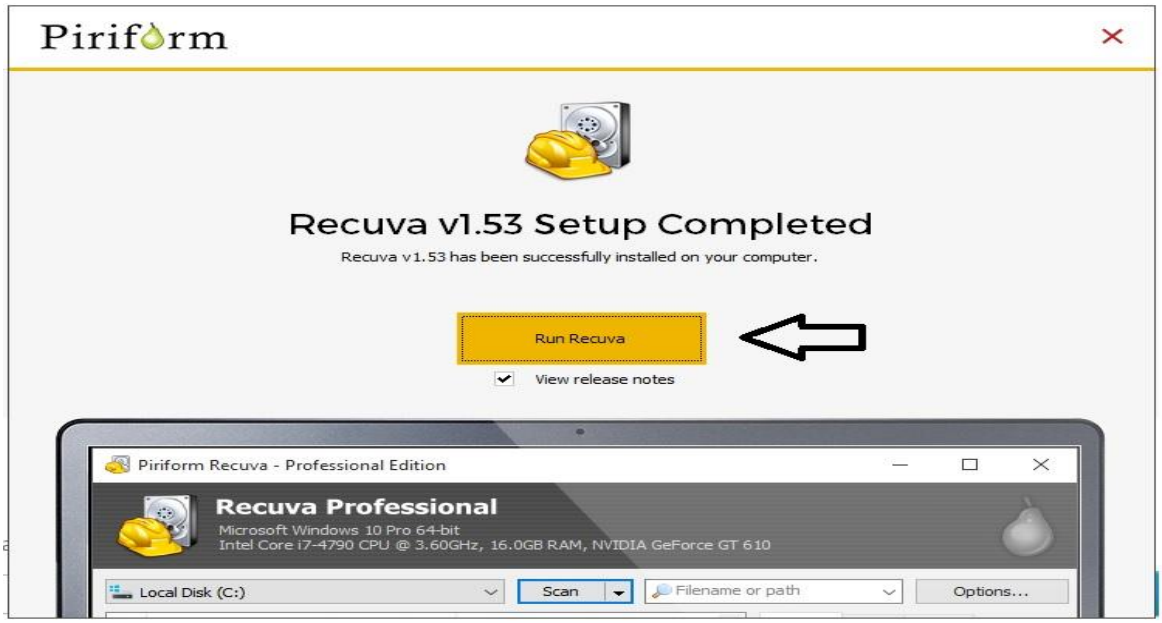


Imagen 35: Captura abrir recuva

3.4.2.1 Prueba de Recuva

Para la prueba se va a utilizar un computador portátil HP, el cual tiene un sistema operativo Windows 7 con particiones C y D, se realizará un borrado de información contenida en una carpeta en la unidad D y se eliminará también de la papelera de reciclaje y se procederá a reiniciar el equipo. La carpeta que se va a borrar tiene un total de 37 elementos entre archivos e imágenes.

La siguiente imagen muestra la información que se borrará.

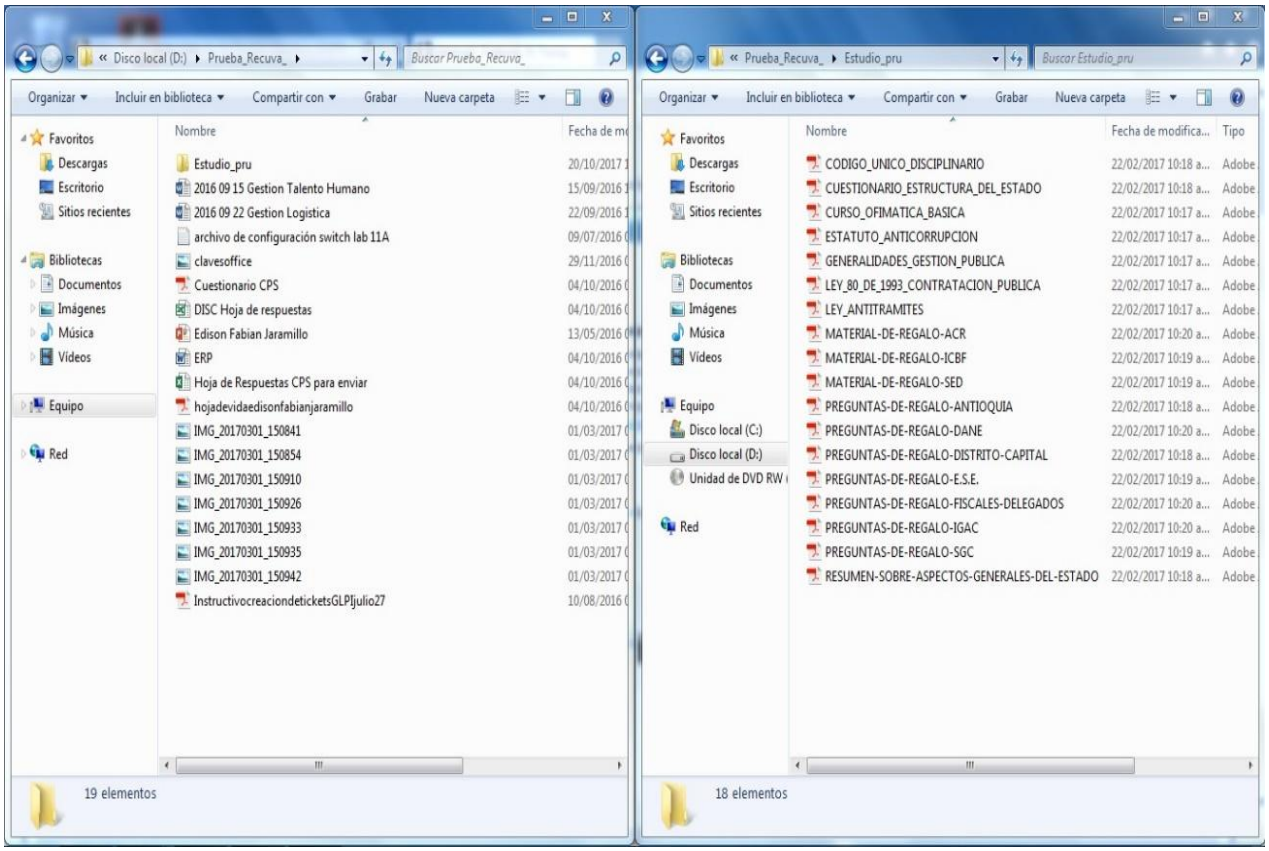


Imagen 36: Captura archivos a borrar

A continuación, la imagen muestra que la carpeta ya no está presente en la unidad D ni en la papelera

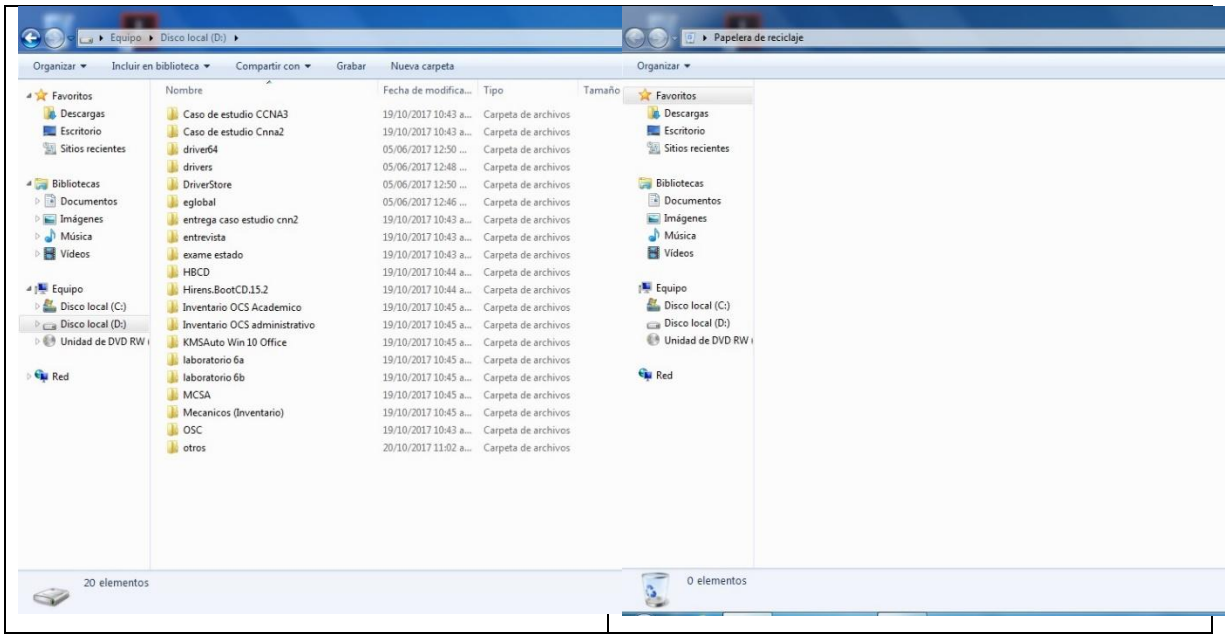


Imagen 37: Captura archivos borrados

1. Se procede abrir el programa Recuva y se le da en la opción siguiente.

Imagen 38: Captura asistente Recuva

2. En esta ventana se muestran varias opciones que se pueden elegir de acuerdo con las necesidades que se tengan, para la presente prueba se selecciona “Todos los archivos”, ya que la carpeta que se eliminó anteriormente contenía elementos de diferente tipo. Clic en

"Siguiente".

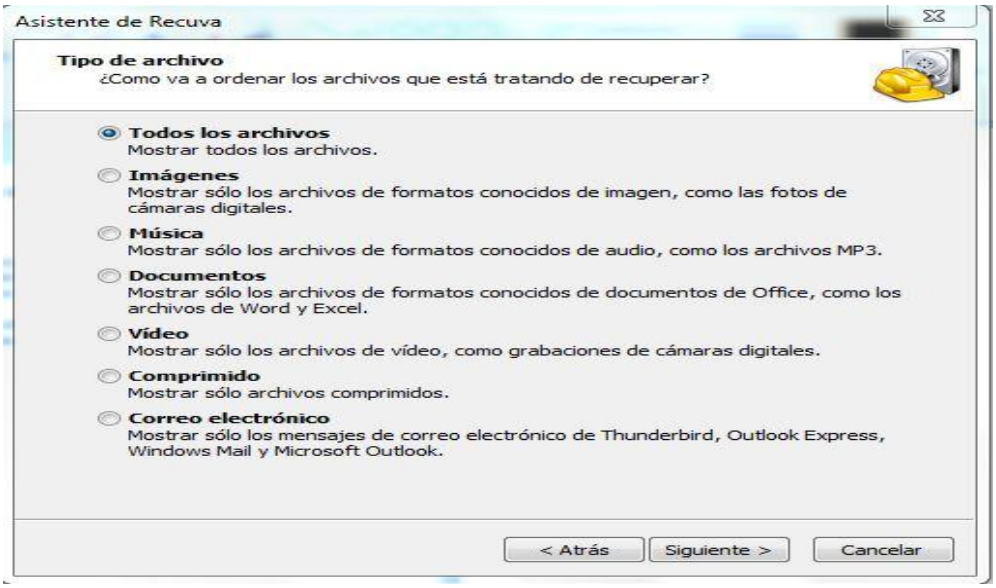


Imagen 39: Captura tipos de archivos a recuperar

3. Seleccionamos la ubicación o la unidad donde se encontraban los archivos borrados, Clic en "Siguiente".

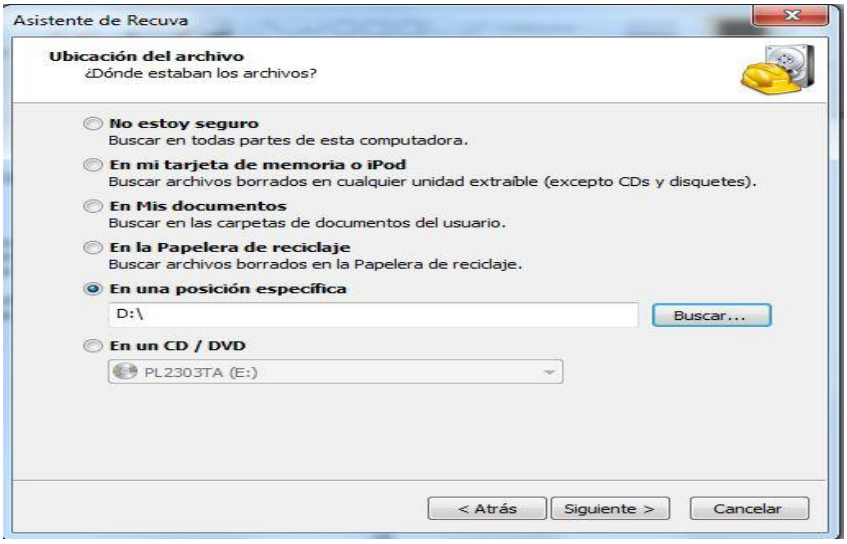


Imagen 40: Captura unidad que se escaneara

4. Se selecciona la opción "Activar escaneo profundo" para que el programa realice un escaneo más detallado y se le da clic "iniciar".

Imagen 41: Captura Inicio proceso de recuperación

5. La siguiente imagen nos muestra los archivos eliminados y su posible recuperación, los archivos marcados con verde son los que recuperara totalmente, los marcados con naranja serán parcialmente recuperados y los rojos no se podrán recuperar.

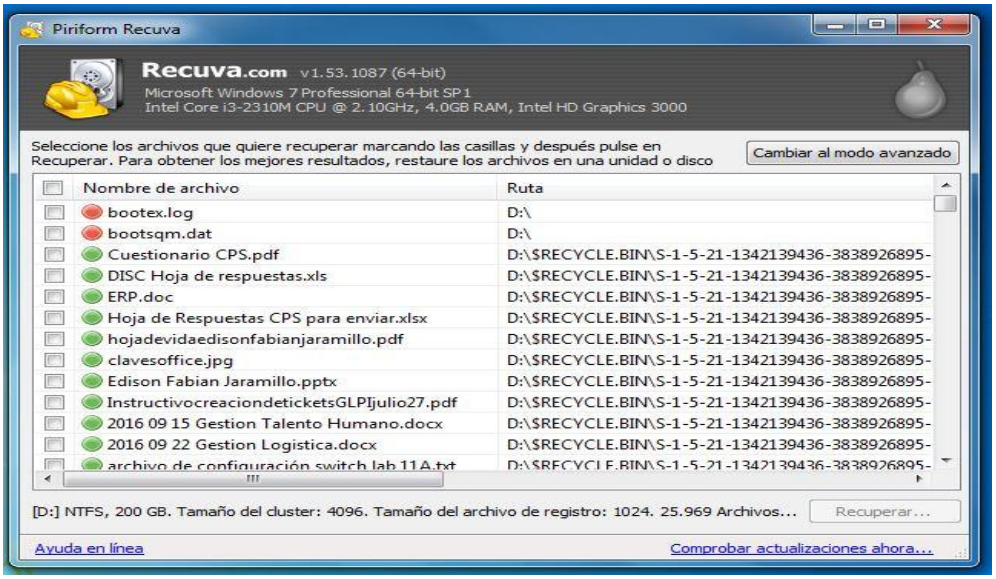


Imagen 42: Captura archivos a recuperar

6. Se seleccionan los archivos en verde los cuales vamos a proceder a recuperar y también la ruta donde se van a recuperar, se recomienda que no sea la misma de donde se realizó el escaneo.

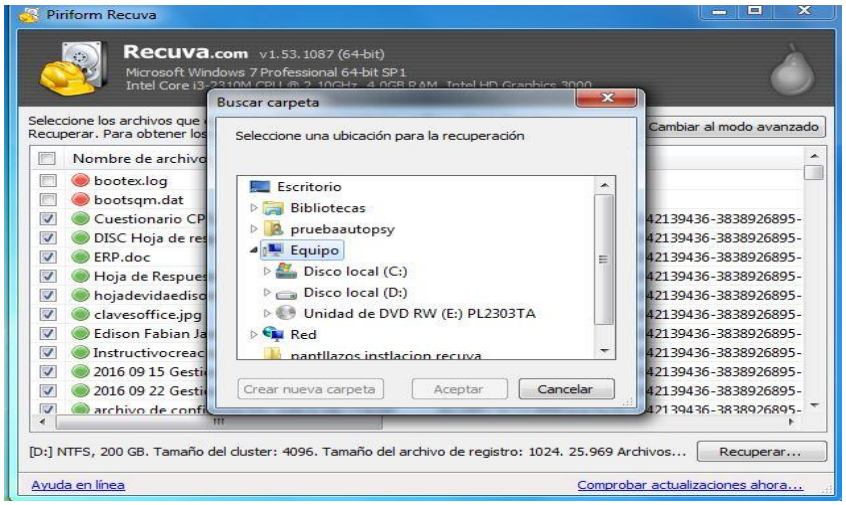


Imagen 43: Captura de selección de destino para los archivos recuperados

7. Se comienza el proceso de recuperación a la nueva ruta, en esta prueba se recuperaron un total de 36 archivos, lo que quiere decir que la herramienta recuperó aproximadamente un 97.3% ya que el total de archivos eliminados fueron 37.

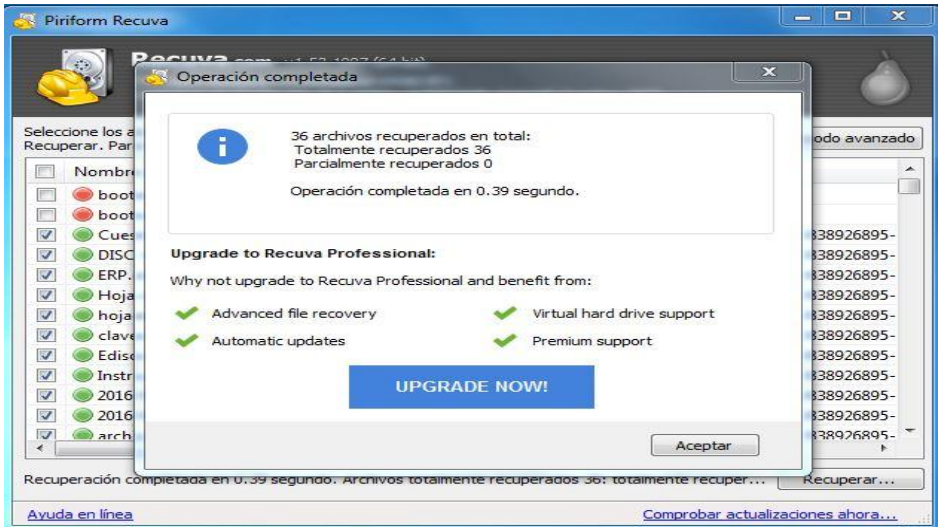


Imagen 44: Captura total archivos recuperados

8. La imagen siguiente muestra los archivos recuperados.

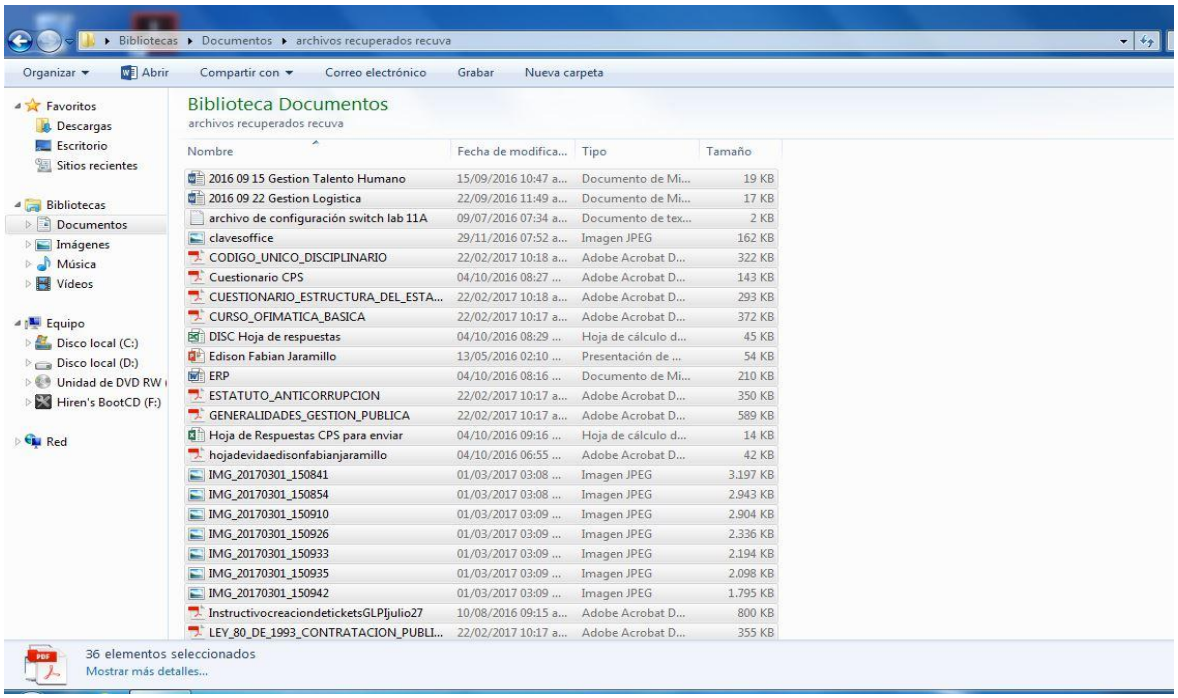


Imagen 45: Captura archivos recuperados

Conclusión de la herramienta Recuva

Los resultados en eficacia y en tiempo de recuperación para esta prueba son muy buenos, recuperó 36 de 37 archivos borrados. Es importante resaltar que los resultados pueden variar de acuerdo con diversos factores como: la cantidad de archivos que se quieren recuperar, si los archivos han sido sobrescritos, el tiempo que estuvieron eliminados dichos archivos y que tipo de versión de la herramienta se utilice para la recuperación (libre o comercial), entre otros.

3.4.3 Pruebas de herramientas de adquisición de información en memoria.

Las dos herramientas para probar son FTKimager y Volatility.

3.4.3.1 Descarga, instalación y prueba con FTKimager

1. Descargar el aplicativo de la siguiente página http://accessdata.com/product-download/ftk-imager-version-4.1.1 dando clic en "DOWNLOAD NOW".

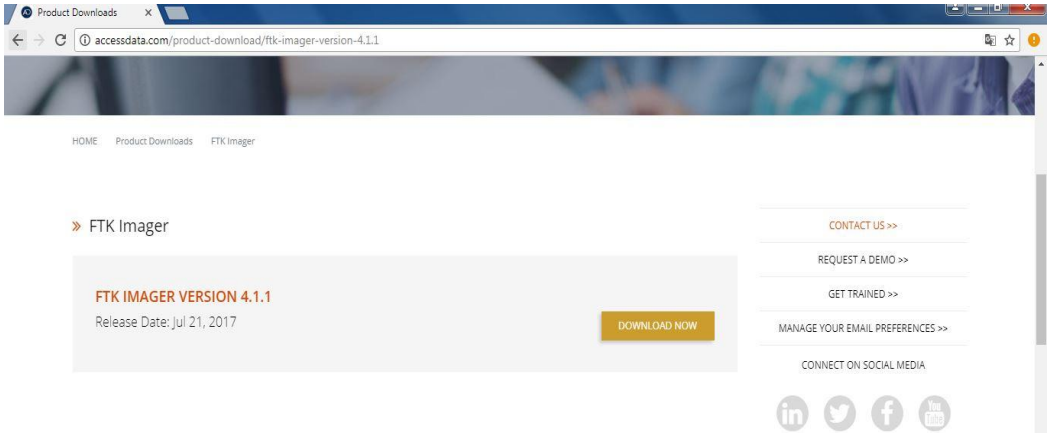


Imagen 46: Captura descarga FTKimager

2. Se debe diligenciar los datos solicitados para proceder con la descarga.

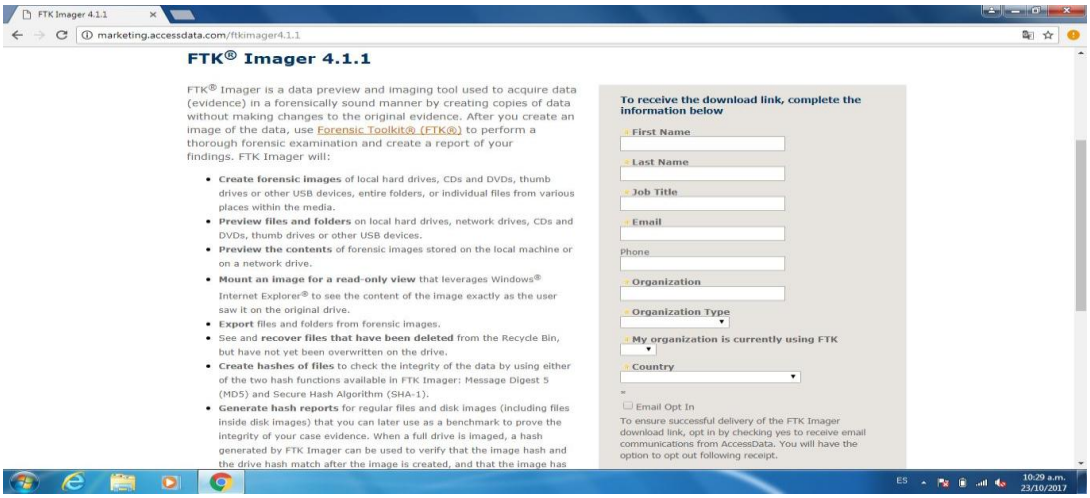


Imagen 47: Captura registro para descargar

3. Al correo que se registró en el paso anterior, llegará un mensaje que contiene el link de descarga, abrir y dar clic en "Download FTK Imager 4.1.1".

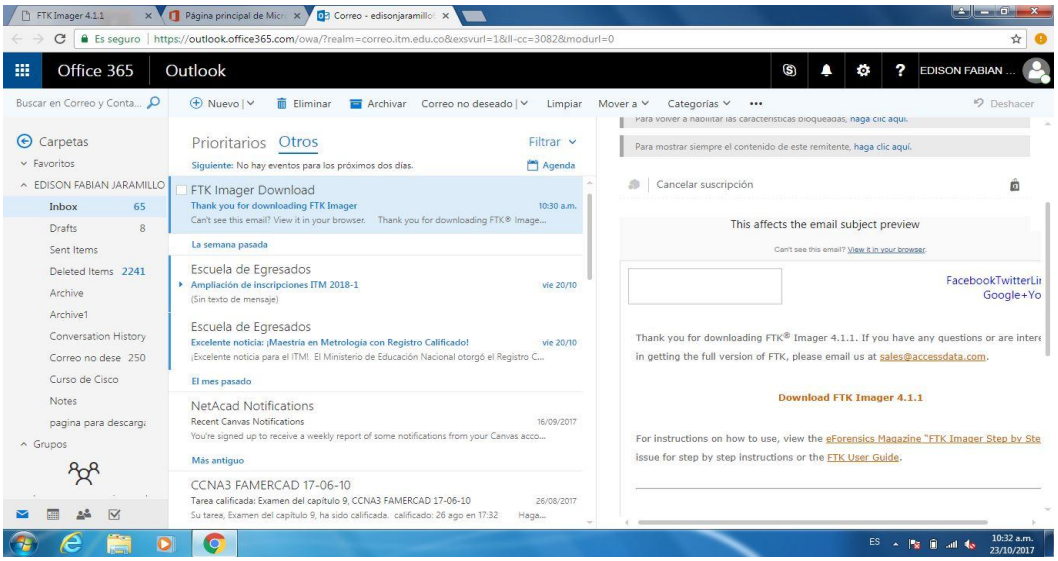


Imagen 48: Captura correo con link de descarga

4. Ejecutar el programa descargado.

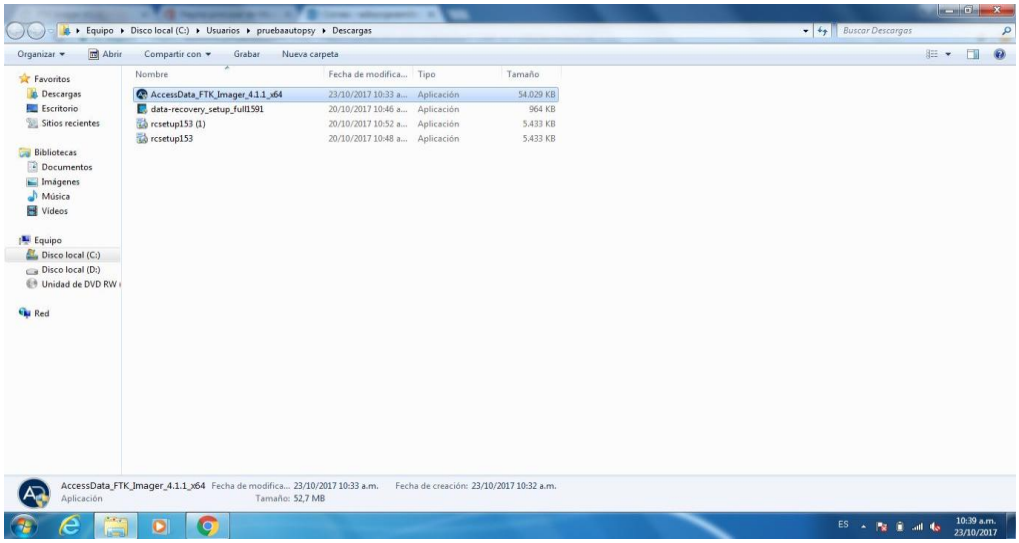


Imagen 49: Captura archivo de instalación

5. Comienza el proceso de instalación, se le da clic en la opción “Next”.

Imagen 50: Captura proceso de instalación

6. Se aceptan los términos y condiciones y siguiente.

Imagen 51: Captura aceptación de términos

7. Aparece la ruta donde quedará instalado el programa con opción de cambiarla, clic en "Next".

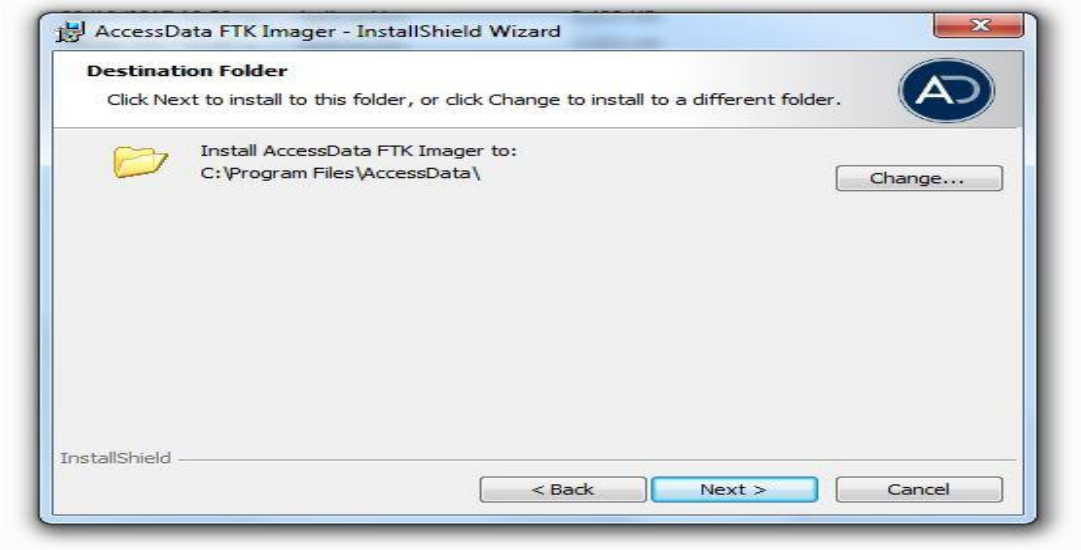


Imagen 52: Captura ruta de instalación

8. Clic en “Install”.

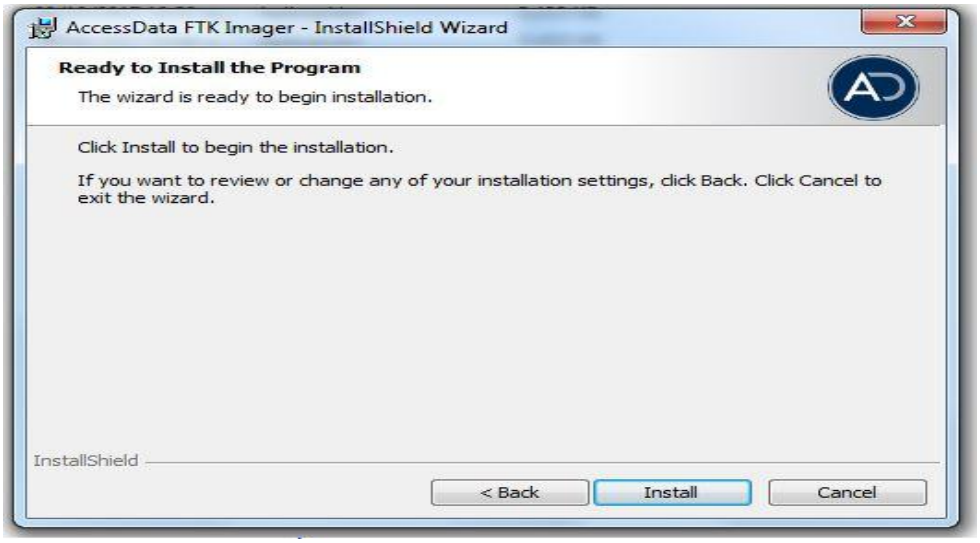


Imagen 53: Captura de instalar

9. La instalación se ha completado, clic en “Finish”.

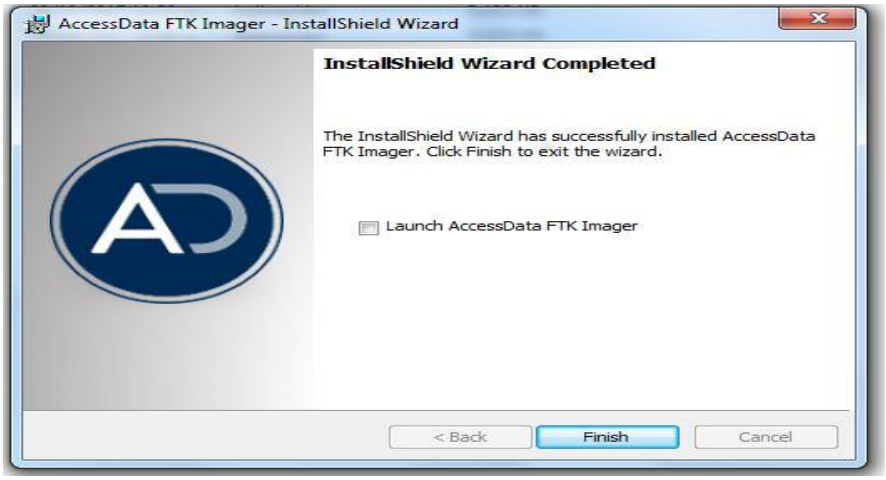


Imagen 54: Captura de finalización de la instalación

3.4.3.2 Prueba de FTKimager

FTKimager crea una imagen de la memoria del equipo, la cual se puede analizar con ella misma o con otras herramientas que soporten el formato con el cual se crea.

1. Abrir el programa y en la pestaña “File”, seleccionar “Capture Memory”.

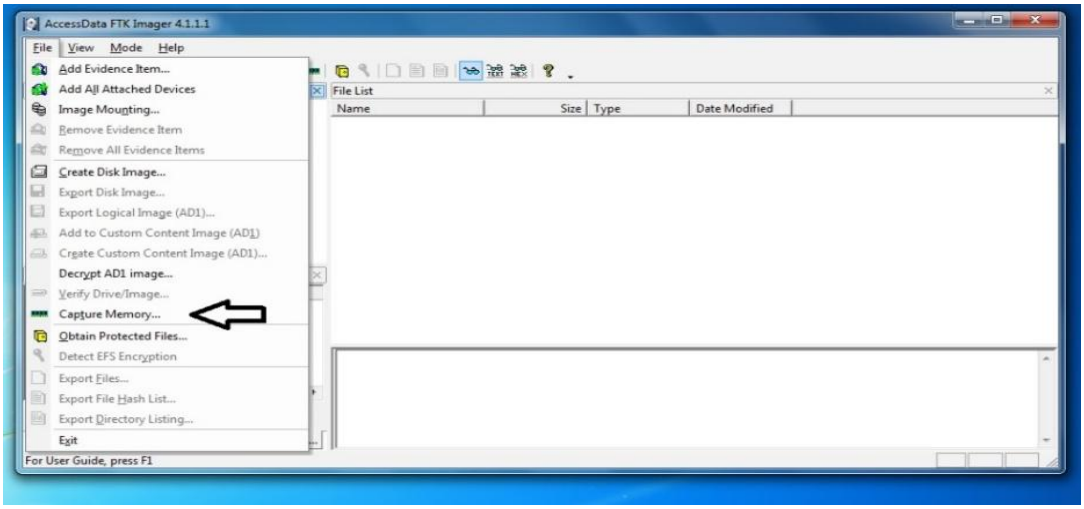


Imagen 55: Captura proceso de captura de memoria

2. Se selecciona la ruta dónde se va a guardar la imagen, además de la memoria el programa puede extraer la configuración del archivo de paginación.

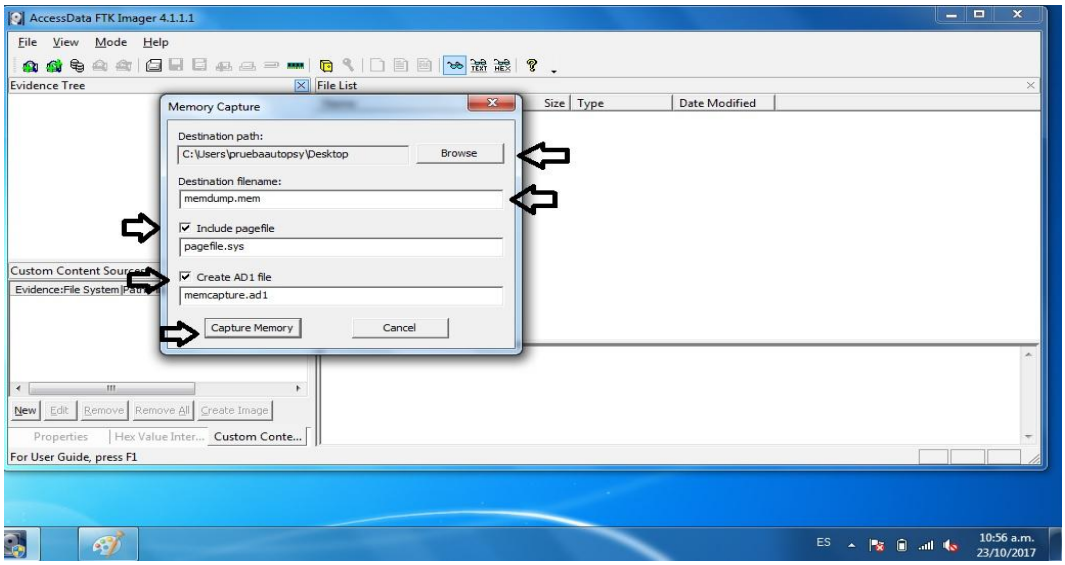


Imagen 56: Captura registro de datos

3. Comienza el proceso de extracción de la memoria, al finalizar, dar clic en “Close”.

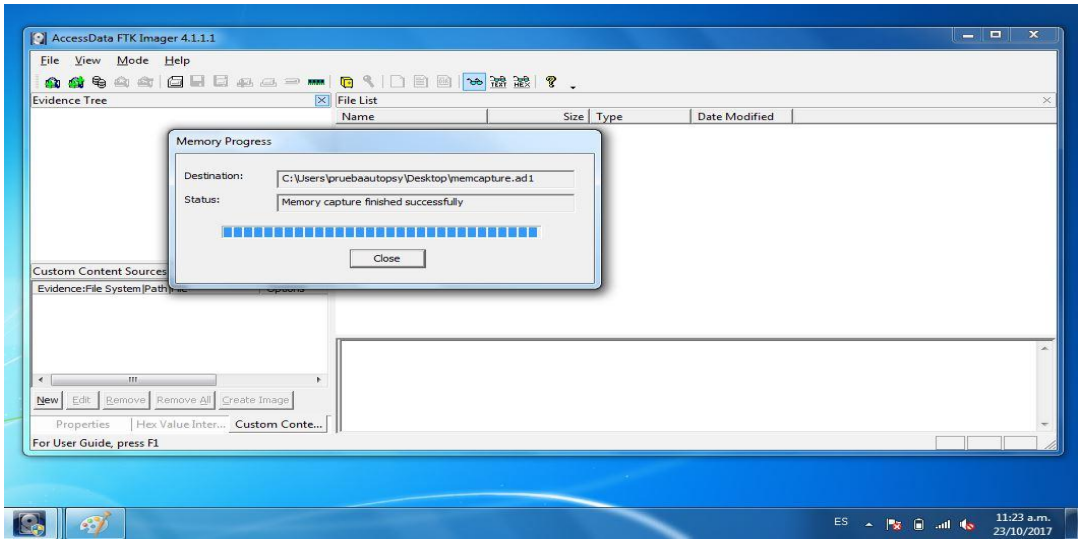


Imagen 57: Captura Proceso de adquisición de la memoria

4. Dar clic en la opción “Add Evidence Item”.

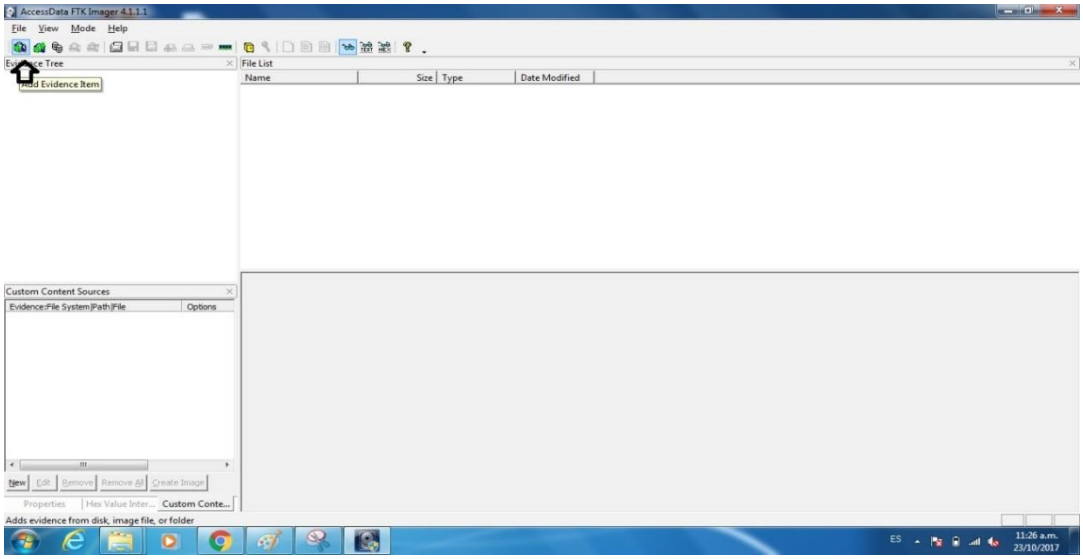


Imagen 58: Captura validación del archivo de la memoria

5. Se selecciona la opción "Image file", ya que vamos a tomar la imagen que creamos en los pasos anteriores. Clic en "Siguiente".

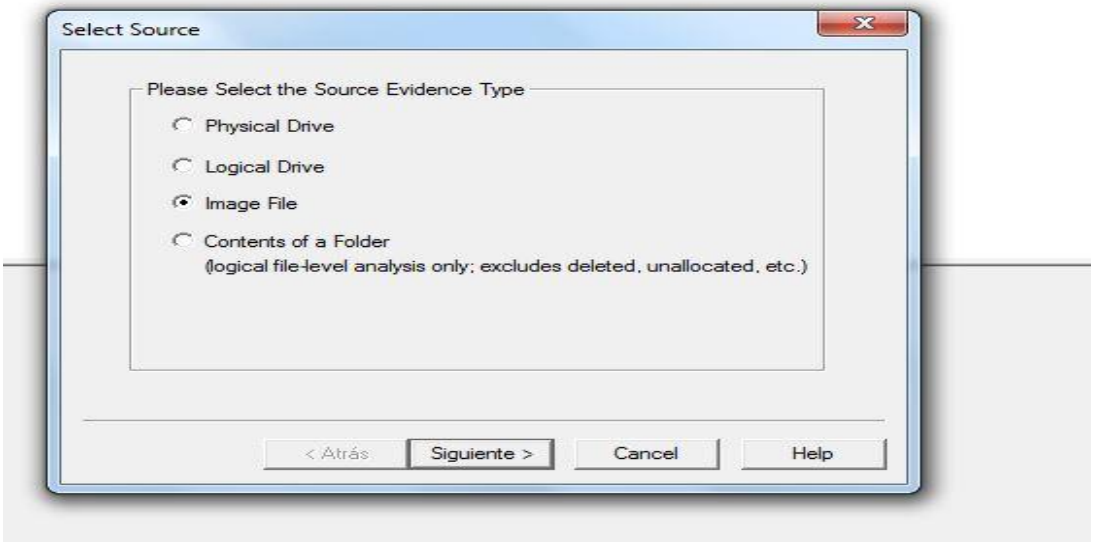


Imagen 59: Captura selección de la imagen adquirida

6. Se busca la ruta donde se tiene la imagen almacenada y abrir.

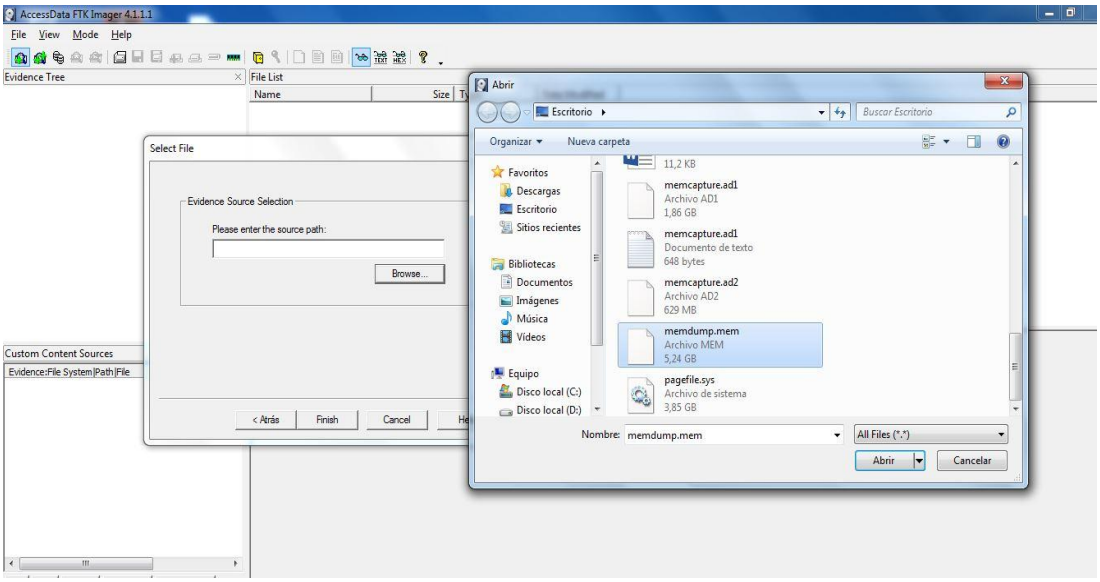


Imagen 60: Captura selección del archivo

7. Clic en “Finish”.

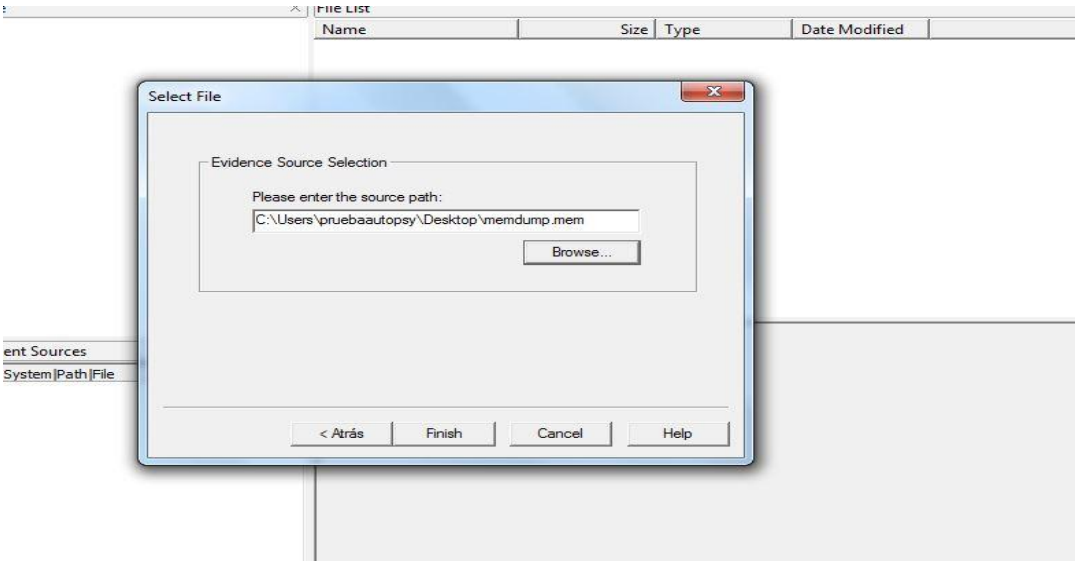


Imagen 61: Captura Finalizar para abrir

8. La imagen es cargada correctamente para su análisis.

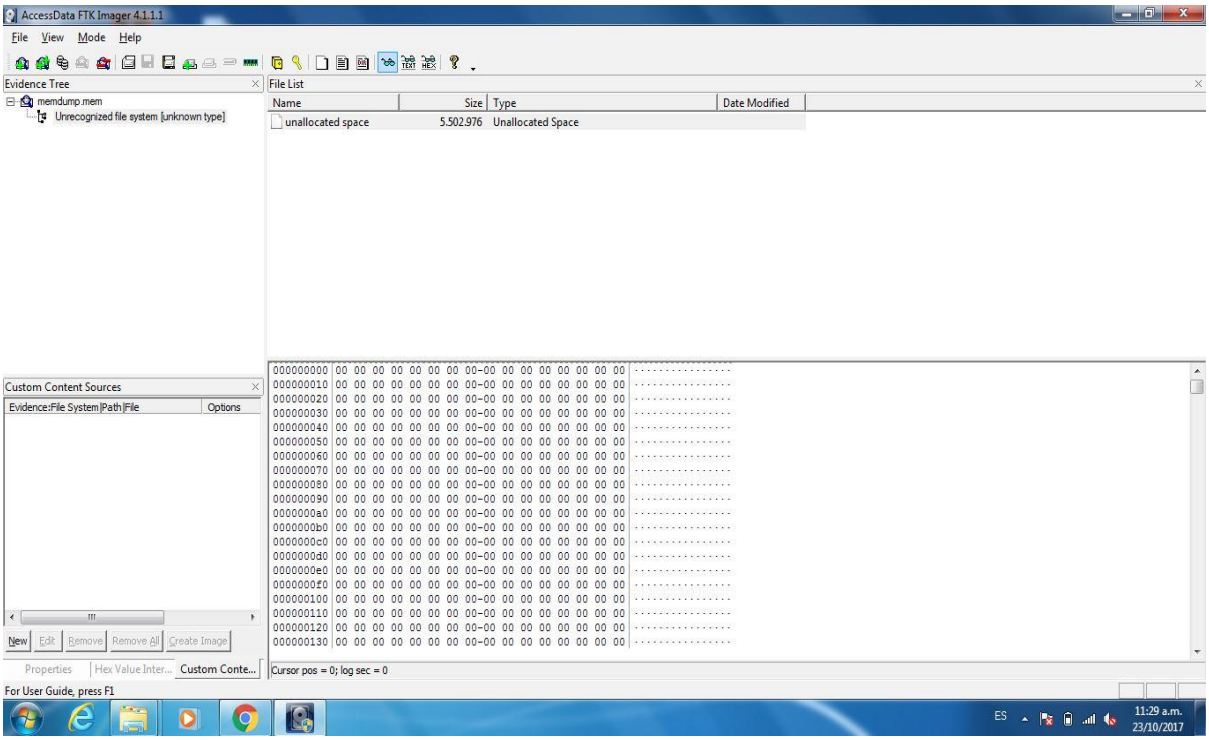


Imagen 62: Captura archivo abierto para análisis

9. Para realizar la prueba de la herramienta FTK Imager se envió un correo electrónico al profesor y asesor de este trabajo y, se verifica que la herramienta haya recuperado la información contenida en dicho correo. Los resultados se evidencian en la siguiente imagen.

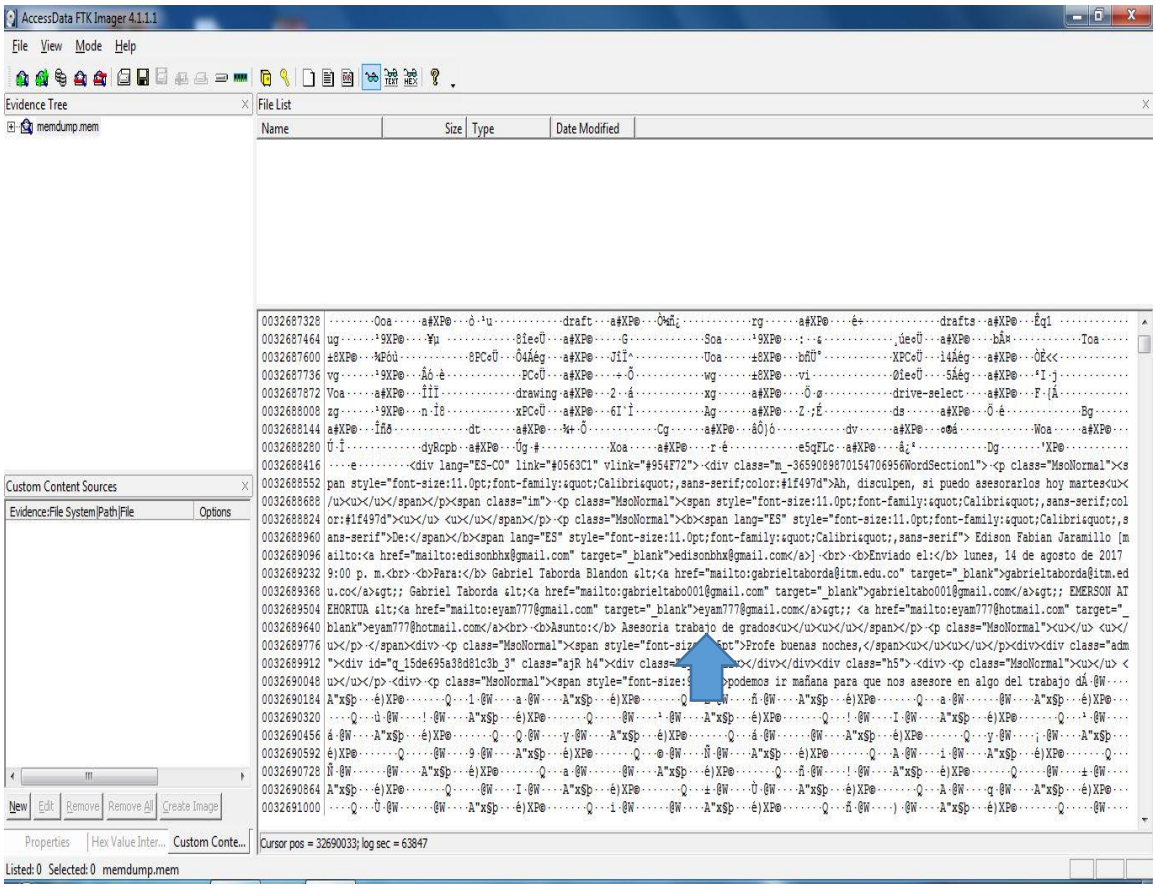


Imagen 63: Captura página historial correo

9.1 En esta imagen podemos observar cómo se logra la captura del correo y la clave de Hotmail del usuario el cual se había logueado antes de la captura de la memoria, esta información queda almacenada en la memoria.

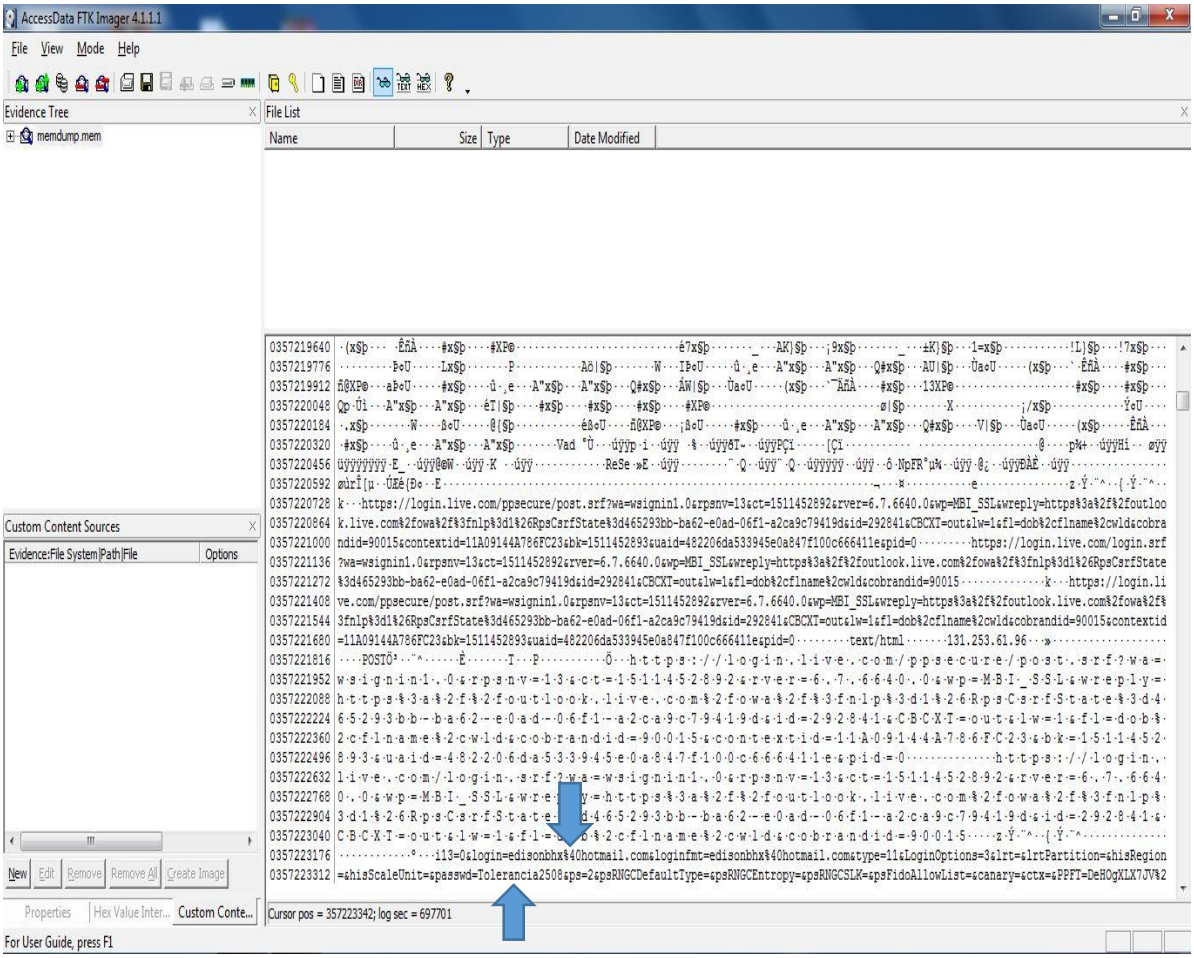


Imagen 64: Captura clave de correo Hotmail

Conclusión de la herramienta FTK Imager

En conclusión, se puede decir que la herramienta cumple con los requisitos para la adquisición de memoria, es muy fácil de usar y la imagen también pude ser transportada en cualquier medio de almacenamiento para que después pueda ser analizada.

3.4.4 Descarga, instalación y prueba con Volatility

Para realizar el análisis de la memoria obtenida, se instaló una distribución de Linux llamada Kali Linux en la cual ya está instalada la herramienta volatility, dicha distribución fue instalada en una máquina virtual utilizando la herramienta virtualbox

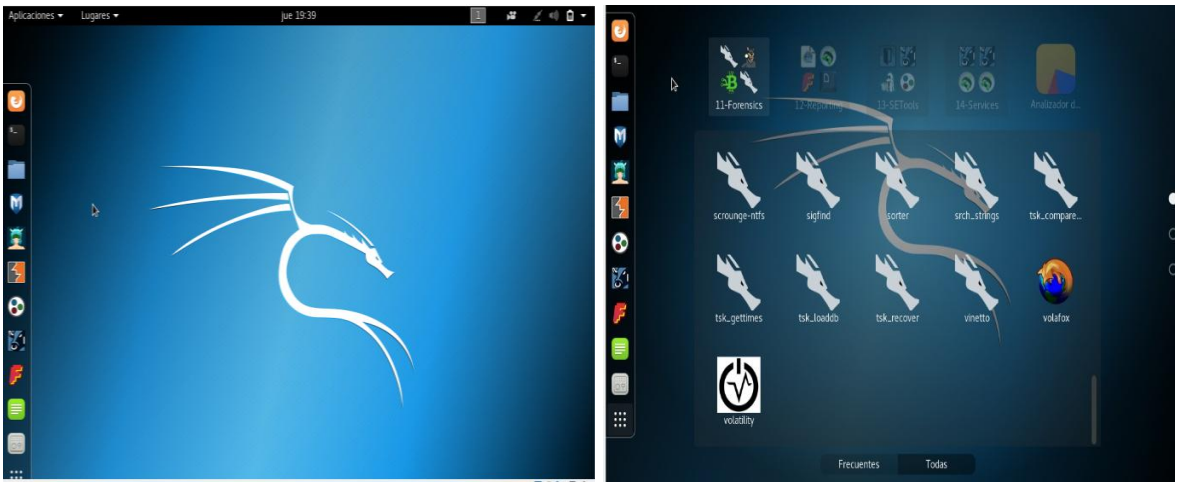


Imagen 65: Captura Kalilinux

3.4.4.1 Prueba con Volatility.

1. Para la realización de la prueba con la herramienta Volatility, se utilizó un equipo con sistema operativo Windows 10 de 64 bits y 8Gb de memoria Ram como muestra la imagen siguiente.

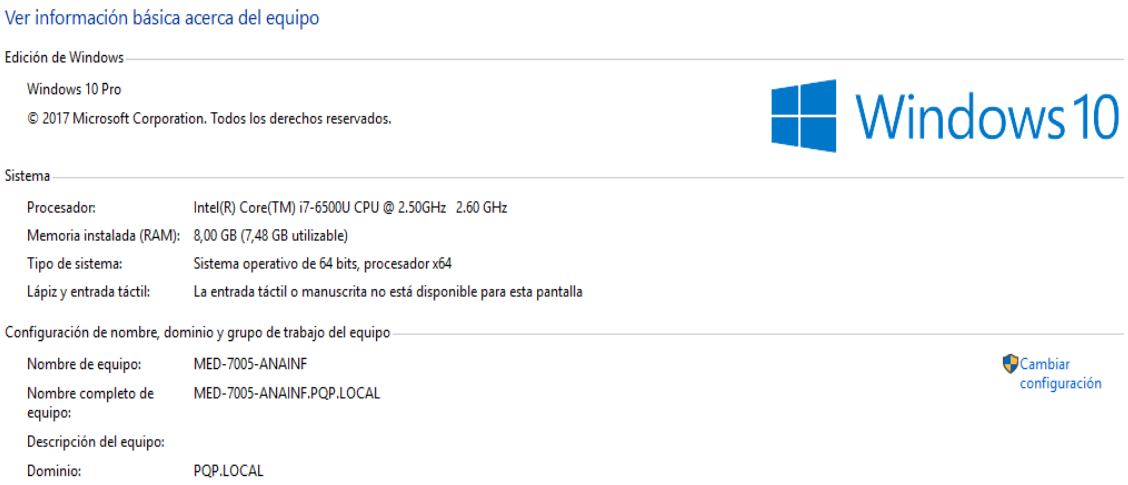


Imagen 66: Captura equipo de pruebas

Para la adquisición de la memoria se utilizó la herramienta FTK Imager, ésta genera un archivo .mem. el cuál es la imagen de la memoria a analizar.

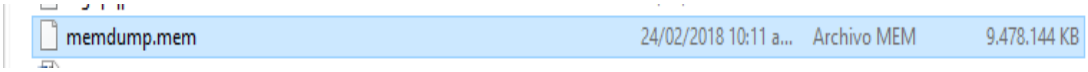


Imagen 67: Captura archivo generado

El tamaño de la imagen varía de acuerdo con la memoria que tenga instalada el equipo, para esta prueba la memoria del equipo de donde se obtuvo la imagen es de 8GB.

Se procede a pasar el archivo. mem a la máquina virtual para poder realizar el análisis respectivo. El archivo. mem es transferido a la máquina virtual mediante una aplicación llamada WinSCP.

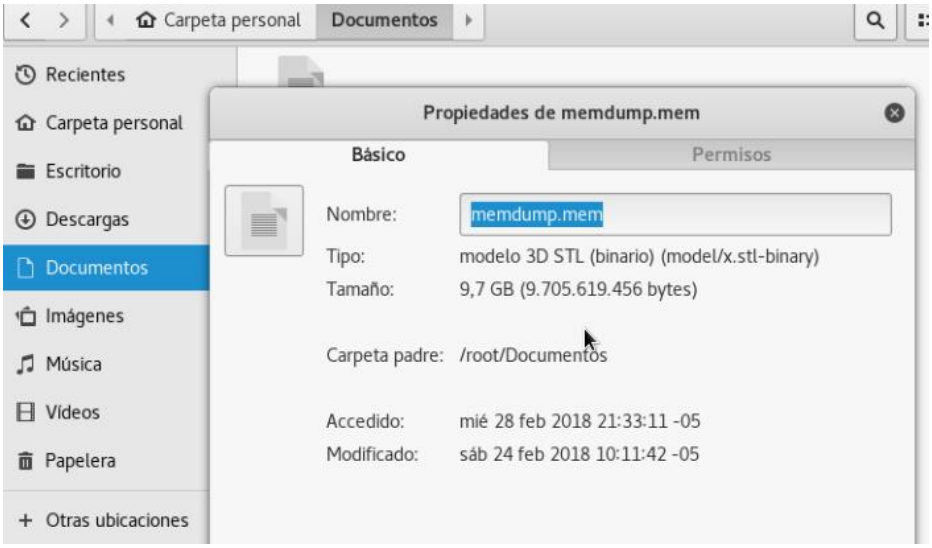


Imagen 68: Captura ubicación archivo. mem

El primer comando que vamos a utilizar con la herramienta volatility es "imageinfo -f" y la ruta donde está alojado el archivo.

root@kalivolatil: ~# voalatility imageinfo -f /root/Documentos/memdump.mem

Este comando nos arroja la información del sistema operativo del equipo de donde se sacó la imagen de la memoria, también el servicie pack que tiene instalado el equipo, el número

de procesadores y la fecha en la cual se creó la imagen.

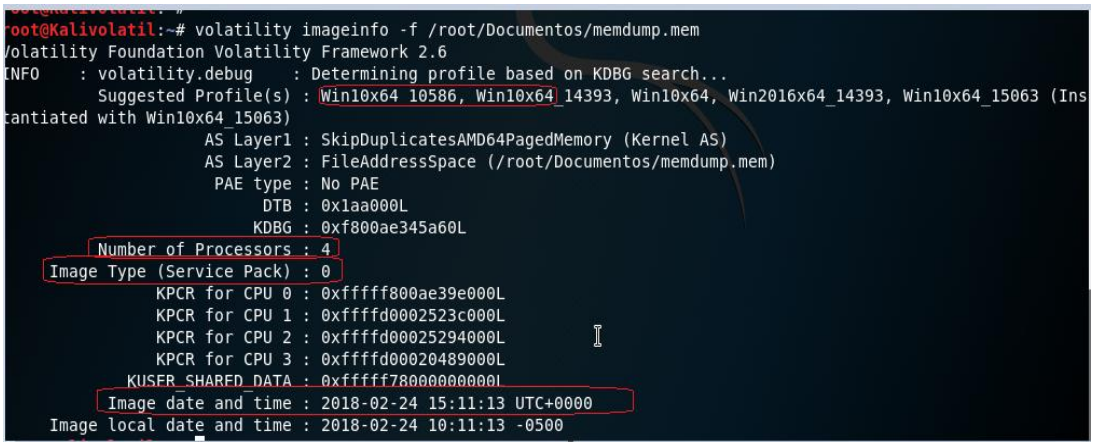
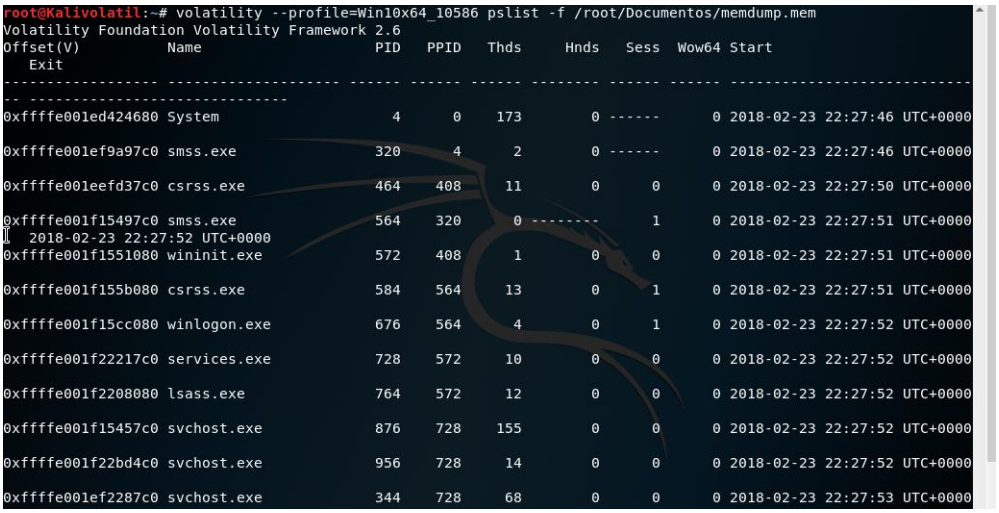


Imagen 69: Captura de comando imageinfo

El siguiente comando lista los procesos que había activos en el momento.

root@kalivolatil: ~# voalatility - -profile=win10x64_10586 pslist -f /root/Documentos/memdump.mem



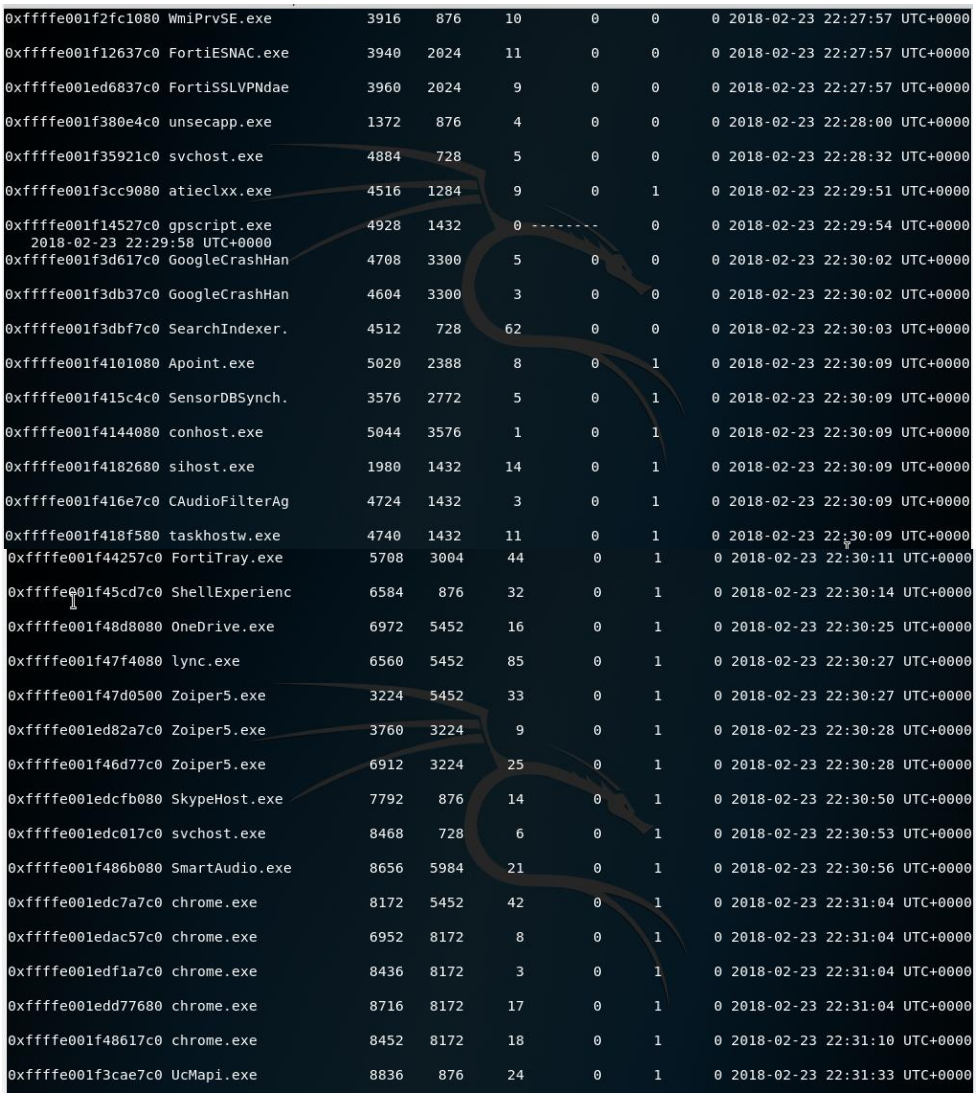


Imagen 70: Captura procesos abiertos

El siguiente comando muestra los procesos ejecutados en la última sesión **root@kalivolatil:** ~# voalatility - -profile=win10x64_10586 sessions -f /root/Documentos/memdump.mem

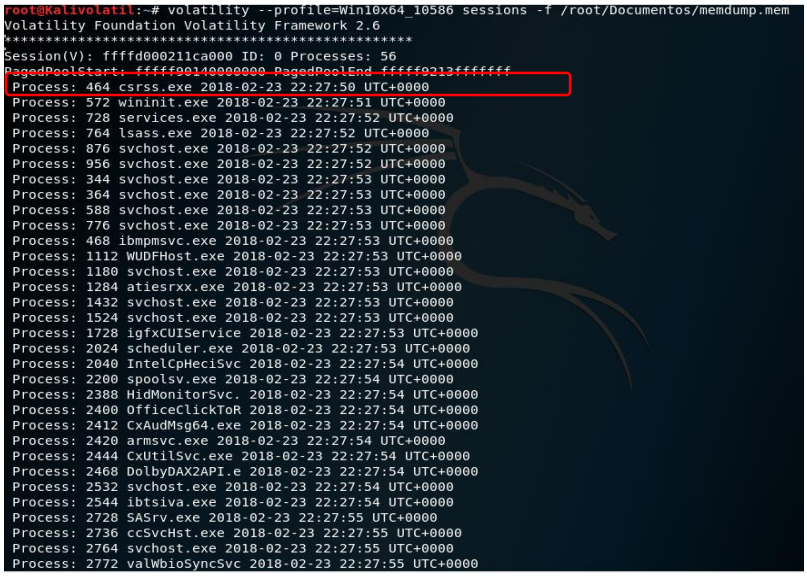


Imagen 71: Captura de proceso

Se puede observar el proceso csrss.exe, en cual puede camuflarse uno o varios troyanos.

Con el siguiente comando podemos observar el historial de los comandos utilizados en la consola.

root@kalivolatil: ~# voalatility - -profile=win10x64_10586 consoles -f /root/Documentos/memdump.mem

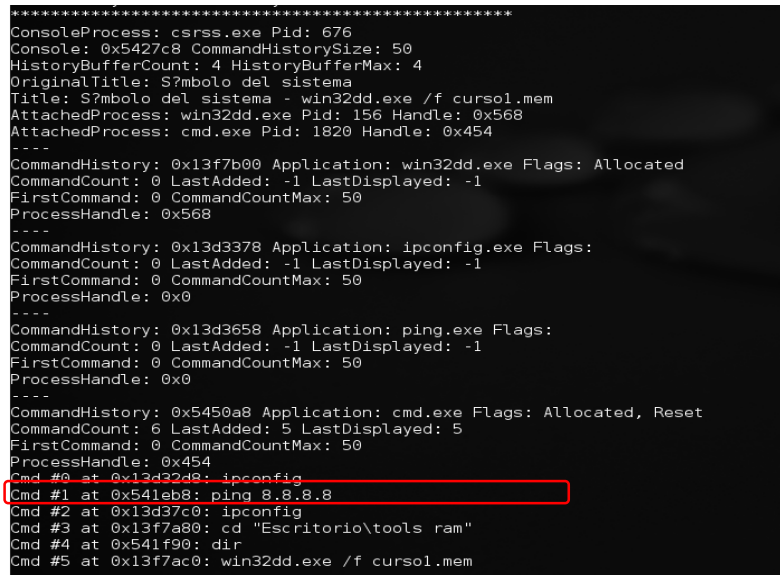
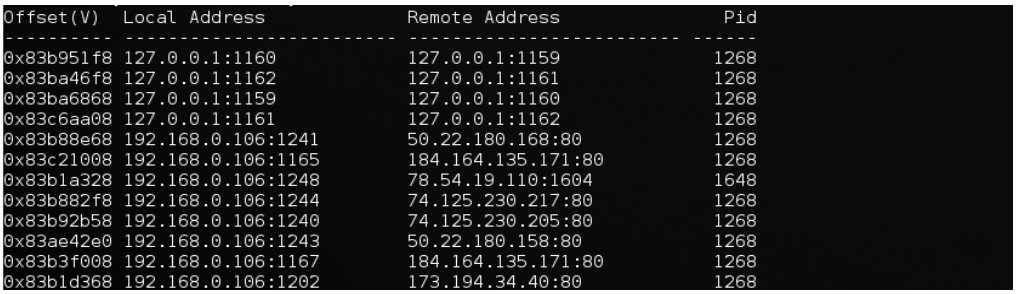


Imagen 72: Captura historial de comandos

Se puede observar que realizaron un ping al 8.8.8.8 y un ipconfig.

Con el siguiente comando podemos observar las conexiones que estaban abiertas en el momento que se realizó la adquisición de la memoria.

root@kalivolatil: ~# voalatility - -profile=win10x64_10586 connections -f /root/Documentos/memdump.mem

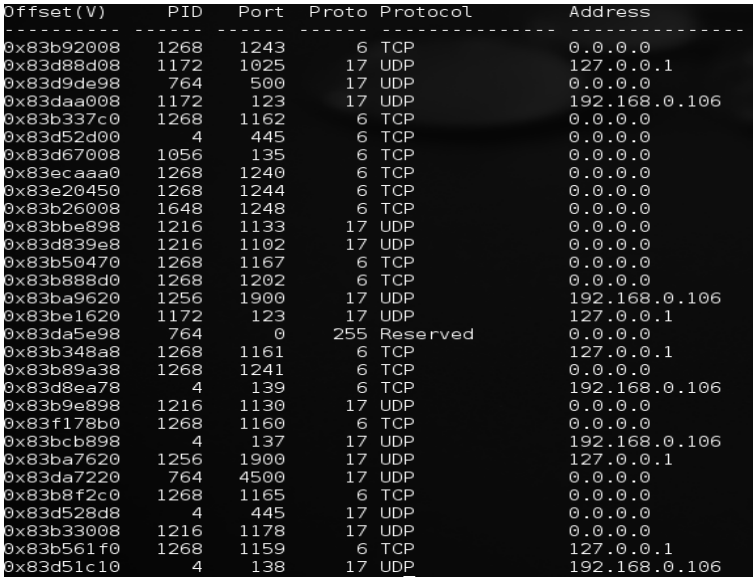


Offset(V)	Local Address	Remote Address	Pid
0x83b951f8	127.0.0.1:1160	127.0.0.1:1159	1268
0x83ba46f8	127.0.0.1:1162	127.0.0.1:1161	1268
0x83ba6868	127.0.0.1:1159	127.0.0.1:1160	1268
0x83c6aa08	127.0.0.1:1161	127.0.0.1:1162	1268
0x83b88e68	192.168.0.106:1241	50.22.180.168:80	1268
0x83c21008	192.168.0.106:1165	184.164.135.171:80	1268
0x83b1a328	192.168.0.106:1248	78.54.19.110:1604	1648
0x83b882f8	192.168.0.106:1244	74.125.230.217:80	1268
0x83b92b58	192.168.0.106:1240	74.125.230.205:80	1268
0x83ae42e0	192.168.0.106:1243	50.22.180.158:80	1268
0x83b3f008	192.168.0.106:1167	184.164.135.171:80	1268
0x83b1d368	192.168.0.106:1202	173.194.34.40:80	1268

Imagen 73: Captura conexiones abiertas

Con el siguiente comando podemos observar los puertos que estaban abiertos y en escucha en el momento de la captura

root@kalivolatil: ~# voalatility - -profile=win10x64_10586 -f /root/Documentos/memdump.mem sockets



Offset(V)	PID	Port	Proto	Protocol	Address
0x83b92008	1268	1243	6	TCP	0.0.0.0
0x83d88d08	1172	1025	17	UDP	127.0.0.1
0x83d9de98	764	500	17	UDP	0.0.0.0
0x83daa008	1172	123	17	UDP	192.168.0.106
0x83b337c0	1268	1162	6	TCP	0.0.0.0
0x83d52d00	4	445	6	TCP	0.0.0.0
0x83d67008	1056	135	6	TCP	0.0.0.0
0x83ecaaa0	1268	1240	6	TCP	0.0.0.0
0x83e20450	1268	1244	6	TCP	0.0.0.0
0x83b26008	1648	1248	6	TCP	0.0.0.0
0x83bbe898	1216	1133	17	UDP	0.0.0.0
0x83d839e8	1216	1102	17	UDP	0.0.0.0
0x83b50470	1268	1167	6	TCP	0.0.0.0
0x83b888d0	1268	1202	6	TCP	0.0.0.0
0x83ba9620	1256	1900	17	UDP	192.168.0.106
0x83be1620	1172	123	17	UDP	127.0.0.1
0x83da5e98	764	0	255	Reserved	0.0.0.0
0x83b348a8	1268	1161	6	TCP	127.0.0.1
0x83b89a38	1268	1241	6	TCP	0.0.0.0
0x83d8ea78	4	139	6	TCP	192.168.0.106
0x83b9e898	1216	1130	17	UDP	0.0.0.0
0x83f178b0	1268	1160	6	TCP	0.0.0.0
0x83bcb898	4	137	17	UDP	192.168.0.106
0x83ba7620	1256	1900	17	UDP	127.0.0.1
0x83da7220	764	4500	17	UDP	0.0.0.0
0x83b8f2c0	1268	1165	6	TCP	0.0.0.0
0x83d528d8	4	445	17	UDP	0.0.0.0
0x83b33008	1216	1178	17	UDP	0.0.0.0
0x83b561f0	1268	1159	6	TCP	127.0.0.1
0x83d51c10	4	138	17	UDP	192.168.0.106

Imagen 74: Captura puertos abiertos

Con el siguiente comando se puede observar los servicios que estaban corriendo y parados cuando se realizó la captura de la memoria

root@kalivolatil: ~# voalatility - -profile=win10x64_10586 -f /root/Documentos/memdump.mem svcscan

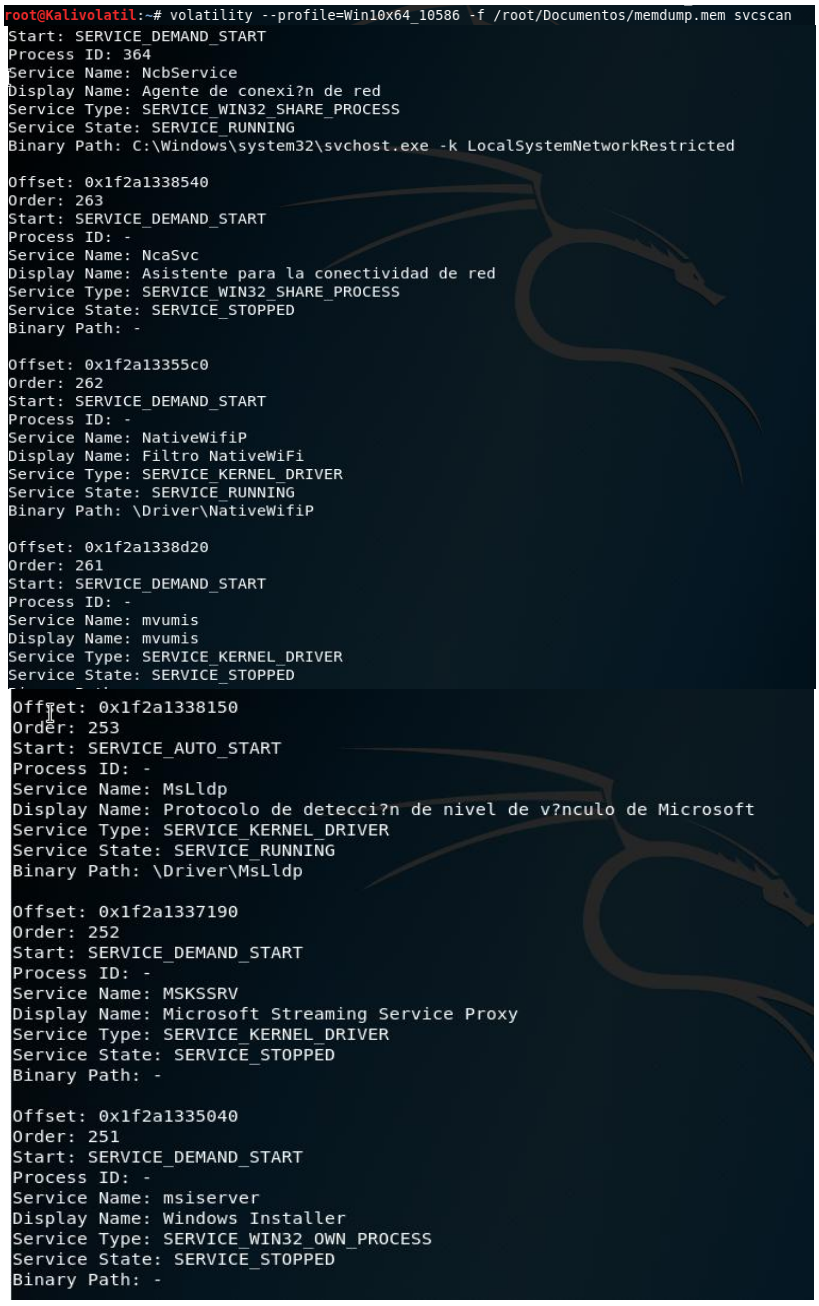


Imagen 75: Captura servicios

El siguiente comando muestra la ayuda de la herramienta y la definición de cada comando

root@kalivolatil: ~# voalatility - -help

Imagen 76: Captura opciones de ayuda

Conclusión de la herramienta Volatility

Se puede concluir que la herramienta cumple el objetivo de analizar la memoria, sin embargo, una de sus desventajas es que necesita otra herramienta para el proceso de adquisición de la misma.

4. RESULTADOS Y DISCUSIÓN

Los resultados obtenidos con base en el estudio del estado del arte y las pruebas realizadas se encuentran presentes en todo el trabajo de la siguiente manera:

En la realización de la búsqueda bibliográfica se encontraron 395 documentos relacionados con el tema de investigación propuesto en la presente tesis, los cuales se redujeron a 172 teniendo en cuenta los criterios de inclusión y exclusión descritos en la página 86.

Los resultados de búsqueda de importantes términos como "Seguridad Informática", que se encarga de proteger toda la infraestructura computacional, especialmente la información contenida en ésta; se encuentra en la página 15 de este trabajo, "La Informática forense" cuyo objetivo es la investigación de medios informáticos con el fin de recuperar y analizar información que pueda servir como evidencia en un proceso, se encuentra en la página 22, "La Evidencia Digital", la cual está constituida por datos, documentos y/o cualquier tipo de información almacenada en medios digitales que puede ser utilizada como valor probatorio para la solución de un delito, éste último término es de suma importancia en el desarrollo del trabajo y se encuentra a partir de la página 25.

Es importante conocer la historia de la informática forense y algunos de los acontecimientos más importantes a través de ésta, los resultados de esta búsqueda se encuentran a partir de la página 32 de esta tesis.

Existe gran cantidad de herramientas para realizar análisis forense, diseñadas para cumplir funciones determinadas. En el marco teórico, en las páginas 35 a 84 se presentan cerca de 90 herramientas que cumplen diferentes funciones en cuanto a análisis forense se refiere.

Para la realización de este trabajo se utilizó una metodología por fases (ver página 85). La primera fase corresponde a la revisión de la literatura, en la cual se utilizó la metodología propuesta por (Serna & Serna, 2013) que consiste en los siguientes pasos:

Definir el área temática, definir las preguntas de investigación, definir el proceso de búsqueda, definir los criterios de inclusión y exclusión, definir la valoración de la calidad, definir la recopilación de datos. El resultado de dicha revisión de la literatura se ve

reflejado entre las páginas 85 y 86.

La segunda fase corresponde a los resultados de la búsqueda de herramientas para informática forense, en esta fase se seleccionan las herramientas para recolección de evidencia digital en disco y en memoria, en total se encontraron 51 herramientas de este tipo y se muestran en la **Tabla 2**, entre las páginas 88 y 101. Con base en dicha tabla, se seleccionan las herramientas más destacadas: en un top 10 (**Tabla 3**) las herramientas de recolección de evidencia en disco y en un top 5 (**Tabla 4**) las herramientas de recolección en memoria, resultados que se muestran en las páginas 102 y 103 respectivamente. Es importante resaltar que la información acerca de estas herramientas es escasa y a pesar de que se encontraron diversos listados con las herramientas más representativas, pocas de ellas presentaban buenos argumentos para tomarlas como las mejores; otro de los factores, fue la delimitación que se les hizo al buscar las que fueran de software libre.

Para el desarrollo de la fase 3 se toman las herramientas elegidas en el top 10 y top 5 de la fase anterior y, se realizan dos cuadros comparativos (**Tabla 5 y Tabla 6 respectivamente**) con sus características más relevantes, estos cuadros se evidencian entre las páginas 104 y 117.

Basados en el cuadro comparativo de la fase 3, se procede al desarrollo de la cuarta fase que consiste en seleccionar dos herramientas de cada tipo (disco y memoria) y realizar pruebas con cada una de ellas. Las herramientas seleccionadas teniendo en cuenta su funcionalidad y usabilidad fueron: **Autopsy** y **Recuva** de las herramientas de recolección de información en disco y, **FTKimager** y **Volatility** de las herramientas de recolección de información en memoria. Los procesos realizados con las herramientas fueron descarga, instalación y prueba.

En la página 118 se inicia el proceso con la herramienta Autopsy, el link de descarga y el proceso de instalación hasta la página 121, en la página 122 se inicia la prueba de la herramienta, los elementos a utilizar y los pasos a seguir para la recolección de información hasta la página 127. Los resultados muestran el historial web (**Imagen 24**, página 128), los usuarios que ingresaron al sistema (**Imagen 25**, página 129), total de archivos encontrados (**Imagen 27**, página 130), los archivos abiertos recientemente (**Imagen 28**, página 131) y

las direcciones de correo que el usuario ha utilizado para el envío de mensajes (**Imagen 29**, página 132). Los resultados obtenidos pueden ser exportados a documentos HTML, Excel, .Text, entre otros, para el reporte y documentación de lo encontrado (**Imagen 30**, página 133).

En la página 134 se inicia el proceso con la herramienta Recuva, las imágenes 31, 32, 33, y 34, muestran el proceso de descarga e instalación hasta la página 136 y en la página 137 se inicia la prueba de la herramienta. Para la prueba utilizó un computador portátil HP, con sistema operativo Windows 7 y con particiones C y D, la prueba consistió en borrar información del equipo e intentar recuperarla con la herramienta Recuva. La **Imagen 36** (página 137) muestra la información que se borró del equipo y la **Imagen 37** (página 138) confirma que la información ha sido eliminada completamente. Recuva cuenta con un asistente que facilitará al usuario en el proceso de recolección (**Imagen 38**, página 138), la **Imagen 39** en la página 139 muestra el tipo de archivo que se quiere recuperar, teniendo en cuenta que la carpeta que se eliminó anteriormente contenía elementos de diferente tipo, se selecciona "Todos los archivos", posteriormente se selecciona la unidad donde se encontraban los archivos borrados (**Imagen 40**, página 139). Se da clic en iniciar para que Recuva recupere los archivos (**Imagen 41**, página 140), la **Imagen 42** en la página 140 muestra los archivos y su posible recuperación, marcados en verde los que se pueden recuperar sin problema, estos se seleccionan y se da clic en recuperar y se le da la ruta donde quedarán los archivos recuperados (**Imagen 43**, página 141), la **Imagen 44** (Página 141) muestra la notificación de los archivos que se recuperaron y en la **Imagen 45** (Página 142) se puede observar la carpeta con los archivos recuperados. Los resultados con la herramienta Recuva fueron muy buenos en esta prueba, sin embargo, es posible que varíen teniendo en cuenta factores como la cantidad de archivos a recuperar o el tiempo que hayan estado eliminados, entre otros.

Las pruebas de las herramientas de recolección de información en memoria comienzan con FTKimager en la página 143, donde se muestra el link de la página de donde se puede descargar (**Imagen 46**), luego de dar click en "Download Now", se muestra un formulario que se debe llenar para continuar con la descarga (**Imagen47**). Al correo que se registró en

el formulario anterior, llegará en un mensaje la herramienta para poder descargarla (**Imagen 48 y 49**, página 144), posteriormente se inicia el asistente de instalación que se muestra en imágenes (**Imágenes 50, 51, 52, 53 y 54**) hasta que finaliza desde la página 145 a 147. Después de realizar la descarga e instalación, se procede a hacer la prueba, a partir de la página 147 se siguen los pasos para el proceso de recolección de información. La **Imagen 55** muestra la elección que se debe tomar para realizar la imagen de la memoria que se quiere analizar, luego se selecciona la ruta dónde se va a guardar la imagen y comienza el proceso de extracción de la memoria (**Imagen 56 y 57**, página 148). Cuando la imagen ha sido creada, se procede a abrirla como muestran las **Imágenes 58, 59, 60, 61** en las páginas 149 y 150. **La Imagen 62** en la página 151 muestra la imagen cargada y lista para ser analizada, podemos ver algunos resultados de la búsqueda en las **Imágenes 63, 64** así:

La **Imagen 63** (página 152), muestra la información de un correo electrónico, quién lo envía, a quién va dirigido y el contenido del correo. Se puede observar mucha información que puede ser muy importante en un proceso investigativo, incluso la **Imagen 64** (página 153), muestra que es posible obtener el usuario y clave de un correo electrónico.

El proceso con la herramienta Volatility se inicia en la página 154, inicialmente se instala en una máquina virtual la distribución Kali de Linux, en la cual viene instalada la herramienta Volatilty (**Imagen 65**), para la prueba, se adquiere una imagen de memoria de un sistema operativo Windows 10 (**Imagen 66**, página 154) utilizando la herramienta FTK Imager y se transfiere a la máquina virtual mediante la aplicación WinSCP (**Imagen 68**, página 155). Al abrir la herramienta Volatility y tomando la imagen de memoria adquirida, podemos recopilar información importante para analizar por medio de comandos como se explica a continuación:

Con el comando *"~# voalatility imageinfo -f /root/Documentos/memdump.mem"*, en la **Imagen 69**, en la página 156, se muestra la información del sistema operativo del equipo de donde se sacó la imagen de la memoria, también el servicie pack que tiene instalado el equipo, el número de procesadores y la fecha en la cual se creó la imagen. Con el comando *"~# voalatility - -profile=win10x64_10586 pslist -f /root/Documentos/memdump.mem"* se

puede observar los procesos que había activos en el momento de la captura de la imagen de memoria, (**Imagen 70**, página 156 y 157). También se puede ver los procesos ejecutados en la última sesión con el comando *"~# voalatility - -profile=win10x64_10586 sessions -f /root/Documentos/memdump.mem"* (**Imagen 71**, página 158). El comando *"~# voalatility - -profile=win10x64_10586 consoles -f /root/Documentos/memdump.mem"*, muestra el historial de los comandos utilizados en la consola. (**Imagen 72**, página 158). Con el comando *"~# voalatility - -profile=win10x64_10586 connections -f /root/Documentos/memdump.mem"*, se observan las conexiones que estaban abiertas (**Imagen 73**, página159), también se observan los puertos que estaban abiertos y en escucha en el momento de la captura con el comando *"~# voalatility - -profile=win10x64_10586 -f /root/Documentos/memdump.mem sockets"* (**Imagen 74**, página159). Con el comando *"~# voalatility - -profile=win10x64_10586 -f /root/Documentos/memdump.mem svcscan"*, se puede observar los servicios que estaban corriendo y parados cuando se realizó la captura de la memoria (**Imagen 75**, página 160).

5. CONCLUSIONES, RECOMENDACIONES Y TRABAJO FUTURO

El propósito de esta investigación fue dar a conocer las herramientas de recolección de evidencia digital, enfocándose en las de software libre, adicionalmente se muestra como instalarlas y probarlas. A continuación, se presentan las conclusiones, las recomendaciones relacionadas y los trabajos futuros.

- Al analizar los resultados de las pruebas realizadas con las herramientas de recolección de evidencia digital seleccionadas, se observa que el proceso de descarga e instalación de la herramientas es muy sencillo, que estas cumplieron con el proceso de recuperación de información digital, no obstante, en algunos casos los resultados de éxito no son garantizados en un 100%, la información se recupera totalmente en la mayoría de ellos pero en ocasiones solo se hace de manera parcial, en forma de ficheros dañados.

    - Luego de realizar la revisión bibliográfica sobre las herramientas de recolección de evidencia digital, se observó que hay muy pocas investigaciones en las revistas científicas sobre este tema, pero en el internet se encontró información muy valiosa sobre ellas lo cual fue muy útil para la realización de esta investigación.
    - Se encontraron muchas herramientas para la recuperación de información digital, las cuales se clasificaron en la **Tabla 2** que son las de software libre, se puede concluir que cada herramienta tiene funciones y requerimientos específicos.

- Para obtener las tablas del top ten y top five de las herramientas más usadas en la recolección de evidencia digital en disco y en memoria, se tuvo en cuenta los tops de las más nombradas en el internet.
- Finalmente se realiza el cuadro comparativo de las herramientas de recolección de evidencia de disco y memoria, las cuales se les aplicó los criterios de sistemas operativos, usabilidad, última versión y funcionalidad.
- Las herramientas gratuitas son muy útiles y en muchos casos cumplen con el objetivo de la recuperación de la información sustituyendo el uso de software costoso.
- Con la ayuda del cuadro comparativo y los tops ten encontrados en el internet se logró seleccionar las dos herramientas de recolección de evidencia digital de disco y memoria con las cuales se realizaron las pruebas de funcionalidad.
- El método para recuperar información es un paso a paso de la utilización de las técnicas de software elegidas para cada caso en particular.

5.1 RECOMENDACIONES

- Es recomendable retirar el dispositivo a intervenir con el fin de garantizar la autenticidad de la información recuperada para el análisis.
- Iniciar el proceso con la herramienta indicada inmediatamente se descubra el incidente o el usuario a investigar.
- Mantener los dispositivos protegidos, con el fin de evitar ataques que pueda afectar o dañar la información de una persona o empresa
- No darse por vencido; si un programa no da resultado, se debe probar con cada herramienta disponible con el fin de tener un resultado positivo.

5.2 TRABAJO FUTURO

- Desarrollar una investigación sobre las herramientas de software propietario para la recuperación de evidencia digital y realizar un comparativo frente al desarrollado en esta investigación.
- Actualizar el análisis de herramientas con nuevas técnicas de software que den solución a la mayoría de los casos de daño o robo de información, que podrán ir incluyendo a medida que vayan apareciendo durante los avances de la tecnología.

REFERENCIAS

AccessData. (2017). *Digital Forensics*. Obtenido de http://accessdata.com/product-download

Acurio, D. P. (2009). *Informatica forense en el ecuador: Una mirada introductoria.* Recuperado el 2016, de http://goo.gl/DclJLZ

Adobe. (2017). *Adobe Photoshop*. Recuperado el 2017, de https://www.adobe.com

Aguilar, P. (2010). *Seguridad Informatica.* Madrid: Editex. Obtenido de https://goo.gl/6qWsgV

Alienvault. (2017). *Welcome to AlienVault Open Threat Exchange*. Recuperado el 2017, de https://www.alienvault.com/open-threat-exchange

Almedia, O. (2015). *Metodología de Análisis Forense.* Obtenido de http://goo.gl/8JiOxH

Antioquia, Tecnologico de. (2013). Evaluación y comparación de herramientas para el análisis forense en redes. *Revista cientifica de la facultad de Ingeniería*(5), 31-37.

Antonio. (18 de 03 de 2016). *Ddrescue - Herramienta de recuperación de datos*. Obtenido de https://goo.gl/E3lxh9

Arellano, L., & Castañeda, C. (2012). La cadena de custodia informático-forense. *Revista ACTIVA*, 67-81.

Arismendi, J. (2015). *Herramientas de Software Utilizadas en la Informática Forense*. Recuperado el 2016, de http://goo.gl/oH6EED

Beltrán, S. (s,f). *EVIDENCIA DIGITAL E INFORMÁTICA FORENSE.* Obtenido de https://goo.gl/sN5ogQ

Biatchux Dmzs. (2017). *Fire*. Obtenido de http://biatchux.dmzs.com/

Blackbagtech. (2017). *MOBILYZE*. Recuperado el 2017, de https://goo.gl/5Nh66q

Caballero, A. (05 de 02 de 2014). *Crear La Imagen Forense Desde Una Unidad Utilizando FTK Imager.* Obtenido de https://goo.gl/TMvtJu

Cano, J. (2003). *Evidencia Digital Reflexiones Tecnicas Administrativas y Legales.* Obtenido de https://goo.gl/gjcYqC

Cano, J. J. (2003). *Admisibilidad de la evidencia digital: de los conceptos legales a las características técnicas.*

Castañeda, M., & Morales, M. (2004). *Seguridad en las transacciones electronicas.* Obtenido de https://goo.gl/rDrr3F

Cellebrite. (2016). *Simplifying the Complexity of Mobile Data Forensics*. Recuperado el 2017, de https://goo.gl/rqWnaw

Cert. (2017). *Digital Intelligence and Investigation*. Recuperado el 2017, de http://www.cert.org/digital-intelligence/tools/liveview.cfm

Cgsecurity. (2012). *PhotoRec, Digital Picture and File Recovery*. Recuperado el 2017, de http://www.cgsecurity.org/wiki/PhotoRec_ES

CgSecurity. (2015). *TestDisk*. Obtenido de https://goo.gl/17Vnqx

Chala, Y. (2015). *FASES DE LA INFORMÁTICA FORENSE.* Obtenido de https://goo.gl/guj0ny

CleverFiles. (10 de 01 de 2018). *Herramientas de Recuperación de Datos: Ventajas y Funcionalidad*. Obtenido de https://goo.gl/w1BQQx

Cnwrecovery. (2017). *Data recovery software*. Recuperado el 2017, de https://www.cnwrecovery.com/

Cohen, M. (2013). Recuperado el 2017, de https://rekall.readthedocs.io/en/gh-pages/Tools/pmem.html

Cohen, M. (2013). *Anti-forensic resilient memory acquisition.* Recuperado el 2017, de http://www.rekall-forensic.com

Cols, C. (2011). *Amenazas y Vulnerabilidades en la Informatica*. Obtenido de https://goo.gl/8PzPmv

Conexioninversa. (2011). *Forensics PowerTools (Listado de herramientas forenses)*. Recuperado el 2016, de http://goo.gl/jNOOAp

Countertack. (2017). *Memory Forensics for Deep Endpoint Investigation.* Obtenido de http://www.countertack.com/responder-pro

Culoccioni, S. (21 de 05 de 2016). *Herramienta para recuperar archivos borrados Linux*. Obtenido de https://goo.gl/YWDnbg

Cultura Geek. (27 de 03 de 2014). *Recuperar datos del disco duro y memorias externas con Foremost.* Obtenido de https://goo.gl/2ddD7A

CursoHacker. (2014). *Recuperar archivos borrados, PROGRAMAS*. Obtenido de

https://goo.gl/xJdoUf

DarkNessgate. (2016). *The Forensic Analysis Toolkit*. Obtenido de https://goo.gl/M3CVoy

Darknet. (2017). *Raw2vmdk – Mount Raw Hard Disk (dd) Images As VMDK Virtual Disks*. Recuperado el 2017, de https://goo.gl/LbY11f

Diaz, G., & Usme, J. (2011). *El software libre y la informatica forense*. Recuperado el 2016, de http://goo.gl/ziAfuI

Dicision Group. (2011). *E-Detective - análisis forense de red en tiempo real y sistema de interceptación legal*. Recuperado el 2016, de http://www.edecision4u.es/E-DETECTIVE.html

Dittrich, David. (Septiembre de 2018). *Investigación Forense de Sistemas GNU/Linux.* Obtenido de https://goo.gl/yu6UEZ

Dmde. (2016). *DM Disk Editor and Data Recovery Software*. Recuperado el 2017, de https://dmde.com/

Dragonjar. (08 de 2018). *Testdisk recupera tus particiones y archivos.* Obtenido de https://goo.gl/M1xupk

Dtyoc. (18 de 10 de 2015). *Seguridad Informática: Ataque de Fuerza Bruta*. Obtenido de https://goo.gl/HTfE4a

Dyba, T., & Dingsoyr, T. (2008). Information and Software Technology. *ScienceDirect*, 833-859. Obtenido de https://goo.gl/7VD8AP

El Pais. (2017). *El ataque de 'ransomware' se extiende a escala global*. Obtenido de https://goo.gl/psNp3L

Eltein Lab. (2009). *Foremost*. Recuperado el 2016, de https://goo.gl/RUwwv7

Escolar, S. (09 de 06 de 2014). *Informatica Forense UNAD*. Recuperado el 2016, de http://inforforenseunad.blogspot.com.co/

Espinoza, C. I. (2009). Software para informatica forense y recuperacion de archivos " WinHex". *Revista de Información, Tecnología y Sociedad*, http://www.revistasbolivianas.org.bo/scielo.php?pid=S1997-40442009000200016&script=sci_arttext.

ExifTool. (2017). Obtenido de http://es.ccm.net/download/descargar-32898-exiftool

Fabriciano. (22 de 10 de 2016). *Recuva, para recuperar archivos borrados*. Obtenido de https://goo.gl/wbeCp3

Fernández, D. (2004). *Informatica forense: Teoria y Práctica.* Recuperado el 2016, de http://goo.gl/oY1ujk

Fireeye. (2017). *Memoryze*. Recuperado el 2017, de https://www.fireeye.com/services/freeware/memoryze.html

Fireeye. (2017). *Redline*. Recuperado el 2017, de https://www.fireeye.com/services/freeware/redline.html

Foremost SourceForge. (2017). *Foremost*. Obtenido de http://foremost.sourceforge.net/

Forensic Focus. (08 de 2018). *analyzeMFT - a Python tool to deconstruct the Windows NTFS*. Obtenido de https://goo.gl/jiCAQ1

ForensicControl. (2017). *forensiccontrol*. Obtenido de https://goo.gl/ywGGsd

Forensicswiki. (05 de 04 de 2012). *Hachoir.* Obtenido de https://goo.gl/8ti4VK

Forensicswiki. (2017). *Regripper*. Recuperado el 2017, de http://www.forensicswiki.org/wiki/Regripper

Fossbytes. (2017). *Top 15 Best Free Data Recovery Software Of 2017*. Obtenido de https://goo.gl/7fsXxb

Garcia, E. (2013). *Antecedentes y terminología del cómputo forense (CF) o informática forense (IF).* Recuperado el 2016

geek, G. y. (27 de 03 de 2014). *Recuperar datos del disco duro y memorias externas con Foremost.* Obtenido de https://goo.gl/v8Nazv

GeekFlare. (2016). *23 FREE Forensic Investigation Tools for IT Security Expert*. Obtenido de https://goo.gl/EHRrxU

Ghirardi, H. A. (2017). *Peritaje Informático*. Obtenido de https://goo.gl/xn9Qyr

Github. (2017). *LiME (formerly DMD)*. Obtenido de https://github.com/504ensicslabs/lime

Github. (12 de 02 de 2017). *Process Dump.* Obtenido de https://goo.gl/rRPDW6

Github. (2017). *Volatilityfoundation Volatility*. Recuperado el 2017, de https://github.com/volatilityfoundation/volatility

Github. (08 de 2018). *Digital Forensics Framework.* Obtenido de https://github.com/arxsys/dff

GITSinformatica. (2003). *Análisis Forense y Peritaje Informático*. Recuperado el 2016, de http://goo.gl/xlsyxJ

Gnu. (12 de 07 de 2018). *Ddrescue - Data recovery tool.* Obtenido de https://goo.gl/8Pt4mD

Gomez, L. M. (2016). *PROTOCOLO DE ACTUACIÓN EN PERITACIONES INFORMATICAS.* Obtenido de https://goo.gl/HgiJpo

Gonzalez, D. (2014). *EL RIESGO Y LA FALTA DE POLITICAS DE SEGURIDAD INFORMÁTICA UNA.* Obtenido de https://goo.gl/B7zttb

Guerra, C. C. (2014). *Análisis y aplicación de software para la recuperación forense de evidencia digital en dispositivos moviles andriod.* Quito.

Guerrero, A. (2009). Informática forense y sus beneficios. *Revista de información tecnologica y sociedad*, 105-107.

Guidance Software. (2017). *EnCase Forensic*. Obtenido de https://www.guidancesoftware.com/encase-forensic

Hacking Articles. (14 de 01 de 2014). *DumpIt – RAM Capture Tool.* Obtenido de https://goo.gl/UFtQ9U

HackPlayers. (2017). *Recopilación de herramientas para la extracción y el análisis de memoria en Linux*. Obtenido de https://goo.gl/gGbexc

Harvey, P. (08 de 2018). *ExifTool by Phil Harvey.* Obtenido de https://goo.gl/qdNxZT

Hetman Software. (2016). *Herramientas de recuperación*. Obtenido de https://hetmanrecovery.com/es/

HowtoForge. (2017). *Creating a dd/dcfldd Image Using Automated Image & Restore (AIR)*. Obtenido de https://www.howtoforge.com/creating_dd_images_with_air

Ideas integrales. (2016). *Seguridad Informatica*. Obtenido de http://goo.gl/Spi2qu

Incibe. (2017). *Amenaza vs Vulnerabilidad, ¿sabes en que se diferencias?* Obtenido de https://goo.gl/SAsvT4

InfosecInstitute. (2017). *7 Best Computer Forensics Tools*. Obtenido de https://goo.gl/f87Nfj

Infospyware. (2017). *FILEASSASSIN*. Recuperado el 2017, de

https://www.infospyware.com/herramientas/fileassassin/

Jaume, M. (17 de 05 de 2018). *Adquisición de memoria RAM.* Obtenido de https://goo.gl/3NokT2

Jerez, C. (2004). *Seguridad para lograr Confiabilidad y Calidad de los Servicios Digitales en Internet.* Obtenido de https://goo.gl/TgkvDZ

Kali Tools. (18 de 02 de 2014). *RegRipper*. Obtenido de https://goo.gl/xGeHYU

Kato, B. (08 de 2018). *Restoration*. Obtenido de https://goo.gl/w8qQD8

Klein, T. (22 de 7 de 2006). *Forensical acquisition and analyses of volatile data.* Recuperado el 2017, de https://goo.gl/lexj5W

La huella oculta. (2014). *Seguridad y Análisis Forense Informáticos*. Obtenido de https://lahuellaoculta.wordpress.com/

Lamirada del replicante. (9 de 12 de 2013). *Recuperar archivos borrados con Scalpel*. Recuperado el 2017, de https://goo.gl/kkCDYF

López, M. (2007). *Análisis Forense Digital.* Recuperado el 2016, de http://goo.gl/yC928h

López, O., Amaya, H., & León, R. (2013). *Informática forense : generalidades, aspectos técnicos y herramientas* . Recuperado el 2016, de http://goo.gl/UPnnhB

LTR Data logo. (08 de 2018). *Tools and utilities for Windows*. Obtenido de https://goo.gl/yFjkEt

Luzuriaga, H. A. (2011). *Herramietas de analisis forense y la recuperacion en los dispositivos de almacenamiento.* Obtenido de https://goo.gl/hDQYe4

Magnet Forensics. (2017). *MAGNET IEF*. Recuperado el 2017, de https://www.magnetforensics.com/magnet-ief/

Martinez Rivera, M. A. (2013). *La informatica forense, su aplicacion legal y su relacion con la criminalistica.* Obtenido de https://goo.gl/PyyP1l

Martinez, M. A. (2103). *La informática forense, su aplicación legal y su relación con la criminalística.* Recuperado el 2016, de http://goo.gl/RyvsPL

Marziale, V. (03 de 10 de 2012). *Advanced Registry Forensics with*. Obtenido de https://goo.gl/xunU2w

Mendosa, A. (2014). Introducción a la informatica y su seguridad. En U. d. Guatemala, *Seguridad de la información* (págs. 7 - 18). Carolina Villatoro. Recuperado el 2016

Mesa, J. (10 de 05 de 2015). *HERRAMIENTAS PARA EL ANÁLISIS FORENSE.* Obtenido de HERRAMIENTAS PARA EL ANÁLISIS FORENSE: https://goo.gl/WKcu3e

Mifsud, E. (2012). *MONOGRÁFICO: Introducción a la seguridad informática*. Obtenido de https://goo.gl/MgFHuF

Mitec. (2017). *Windows Registry Recovery*. Recuperado el 2017, de http://www.mitec.cz/wrr.html

Mobiledit. (2017). *Software used by millions of users*. Recuperado el 2017, de http://www.mobiledit.com/

Mobileforensics. (2017). *Secure View*. Recuperado el 2017, de http://mobileforensics.susteen.com/

Mosquera, J., Certain, A., & Cano, J. J. (2005). *Evidencia Digital: contexto, situación e implicaciones nacionales.* Obtenido de https://goo.gl/RGPqWh

MountImage. (2017). *Mount Forensic Images*. Recuperado el 2017, de http://www.mountimage.com/

Msab. (2017). *XRY Products*. Recuperado el 2017, de https://www.msab.com/products/xry/

Neo System Forensics. (31 de 08 de 2012). *Linux, volatility y sus perfiles.* Obtenido de https://goo.gl/6rv7nb

Netresec. (2017). *NetworkMiner*. Recuperado el 2017, de http://www.netresec.com/?page=NetworkMiner

Nirsoft. (2011). *WirelessKeyDump*. Recuperado el 2017, de http://www.nirsoft.net/utils/wireless_key_dump.html

Nirsoft. (2016). *Mail PassView*. Recuperado el 2017, de http://www.nirsoft.net/utils/mailpv.html

Nirsoft. (2016). *WinPrefetchView*. Recuperado el 2017, de http://www.nirsoft.net/utils/win_prefetch_view.html

Ntfs. (2016). *NTFS Data Recovery Toolkit*. Recuperado el 2017, de http://www.ntfs.com/recovery-toolkit.htm

O&O Software. (08 de 2018). *O&O DiskRecovery.* Obtenido de https://goo.gl/etc5Tz

Osforensics. (2017). *OsfMount*. Recuperado el 2017, de http://www.osforensics.com/tools/mount-disk-images.html

Oxygen Forensic. (2017). *Oxygen Forensic*. Recuperado el 2017, de https://www.oxygen-forensic.com/es/

Pagés, L. J. (2013). *Temas avanzados en seguridad y sociedad de la infomacion.* Recuperado el 2016, de http://goo.gl/Ue8U7A

Paraben Corporation. (2016). *E-mail Forensics*. Recuperado el 2016, de https://goo.gl/xb6XGo

Paraben Corporation. (2017). *UNIVERSAL PLATFORM FOR DIGITAL EVIDENCE*. Recuperado el 2017, de https://goo.gl/xb6XGo

Passware. (2017). *Asterisk Key*. Obtenido de https://www.passware.com/asterisk/

Pc Inspector. (2017). *PC INSPECTOR*. Obtenido de http://www.pcinspector.de/?language=1

PeopleRedhat. (2015). *Crash RedHat*. Obtenido de https://goo.gl/sR5ECQ

PetroniJr, N. L., Walters, A., Fraser, T., & Arbaugh, W. A. (2006). FATKit: A framework for the extraction and analysis of digital forensic data from volatile system memory. *Science Direct*, 197-210. Obtenido de https://goo.gl/vNT416

Piedrahita, E. (2014). *FASES DE LA INFORMATICA FORENSE.* Obtenido de FASES DE LA INFORMATICA FORENSE: https://goo.gl/VnRbrF

Piriform. (2017). *Recuva Documentation*. Recuperado el 2017, de http://www.piriform.com/docs/recuva

Puran Software. (2013). *Puran File Recovery Description*. Obtenido de https://goo.gl/Xbhmur

Pypi Python. (2017). *AnalyzeMFT*. Recuperado el 2017, de https://pypi.python.org/pypi/analyzeMFT/2.0.19

Quituisaca, L. (2010). *Informática Forense.* Obtenido de https://goo.gl/7yXfEj

Refog. (2017). *Registrador de teclado exclusivo para controlar*. Recuperado el 2017, de https://es.refog.com/personal-monitor/

Remo Software. (2017). Obtenido de Remo Recuperar : https://www.remorecover.com/es/

Reyes, M. (2012). *Propuestas para impulsar la seguridad informática en materia de educación.* Obtenido de http://www.ptolomeo.unam.mx:8080/xmlui/handle/132.248.52.100/217

Rifà, H., Serra, S., & Rivas, J. L. (2009). *Análisis forense de sistemas informàticos.* Obtenido de https://goo.gl/ukQKQJ

Rodriguez, D. (23 de 9 de 2014). *Adquisición de Memoria en Windows con DumpIt*. Obtenido de http://hotfixed.net/adquisicion-de-memoria-en-windows-con-dumpit/

Romo, A., & Ramiro, O. (25 de 5 de 2011). *Metodología para la implementación de informática forense en sistemas operativos Windows y Linux Capitulo III.* Obtenido de http://repositorio.utn.edu.ec/handle/123456789/539

R-Tools Technology Inc. (2016). *Software de recuperación de discos y herramienta de recuperación de discos duros*. Recuperado el 2016, de http://www.r-studio.com/es/

R-Tools Technology Inc. (2017). *Software de recuperación de discos y herramienta de recuperación de discos duros*. Recuperado el 2017, de http://www.r-studio.com/es/

Runtime. (2017). *RAID Reconstructor*. Recuperado el 2017, de https://www.runtime.org/raid.htm

Sánchez, K. (Noviembre de 2015). *Seguridad en Cómputo.* Obtenido de http://blogs.acatlan.unam.mx/lasc/2015/11

Sandmark. (2017). *Tool for the Study of Software Protection Algorithms*. Recuperado el 2017, de http://sandmark.cs.arizona.edu/downloads.html

Sandoval, C., & Vaca, E. (5 de 2013). *Implanatcion de Tecnicas y Administracion de Laboratorio para Investigacin de EthicalHhacking.* Obtenido de https://repositorio.espe.edu.ec/bitstream/21000/6483/1/T-ESPE-047094.pdf

Santos, J. (2013). *PROCEDIMIENTOS EN LA INVESTIGACIÓN, RECOLECCIÓN Y MANEJO DE LA EVIDENCIA DIGITAL EN LA ESCENA DEL CRIMEN.* Obtenido de https://goo.gl/fDGzMn

SC Media. (2018). *Coroner's Toolkit.* Obtenido de https://goo.gl/UYW3Bq

Security X Ploded. (2017). *Browser Password Decryptor*. Recuperado el 2017, de http://securityxploded.com/browser-password-decryptor.php

Segmentation fault. (2017). *Physical memory analysis of Linux systems*. Obtenido de https://goo.gl/aKshLs

Serna, E., & Serna, A. (2013). *Está en crisis la ingeniería en el mundo? Una revisión a la literatura.* Obtenido de https://goo.gl/mKumJC

Sleuthkit. (2017). *Open Source Digital Forensics*. Recuperado el 2017, de https://www.sleuthkit.org/

Snort. (2017). *Snort*. Recuperado el 2017, de https://www.snort.org/

Softpedia. (7 de 5 de 2015). *Registry Decoder*. Obtenido de https://goo.gl/cAKPXM

Softpedia. (7 de 05 de 2015). *Registry Decoder*. Obtenido de https://goo.gl/vv88vG

Sourceforge. (2013). *Live View*. Obtenido de https://goo.gl/DnD9LS

SourceForge. (2017). *ImDisk Toolkit*. Recuperado el 2017, de https://sourceforge.net/projects/imdisk-toolkit/

Splunk. (2017). *Que es Splunk*. Recuperado el 2017, de https://www.splunk.com/es_es

Spytech-Web. (2017). *Spytech*. Obtenido de https://www.spytech-web.com/index.shtml

Tech Guides. (27 de 02 de 2018). *Disk cloning in Linux using dd command.* Obtenido de https://goo.gl/5jUea9

TechnologyINT. (2014). *Forensic Toolkit® (FTK®): Reconocido alrededor del Mundo como el Estandar en Software de Informática Forense.* Recuperado el 2016, de http://goo.gl/RHsbP1

Techsupportall. (2017). Obtenido de https://goo.gl/mAQHpa

TechTalk. (2017). *Top 20 Free Digital Forensic Investigation Tools for SysAdmins*. Obtenido de https://goo.gl/3BTu9D

Theoven. (2017). *NTPWEdit version 0.6 GPL*. Recuperado el 2017, de http://theoven.org/index.php?topic=1103.0

TimeToast. (2017). *Los ciberataques más importantes de la historia*. Obtenido de https://goo.gl/u83Wym

Tools Kali. (2014). *Bulk-Extractor*. Recuperado el 2017, de http://tools.kali.org/forensics/bulk-extractor

Toolwar. (2013). *Infosec Tools*. Obtenido de http://www.toolwar.com

TOPAttack. (2016). *Best Keyloggers & Monitoring Software Review*. Recuperado el 2016, de http://goo.gl/gJUuxq

TOPAttack. (2017). *Best Keyloggers & Monitoring Software Review*. Recuperado el 2017, de http://goo.gl/gJUuxq

Tzworks. (2017). *Windows Prefetch Parser*. Recuperado el 2017, de https://goo.gl/DwTBrh

Umaña, G., & Mosquera, I. (2014). *Diseño e implementación de un centro de informática forense*

en la universidad autónoma de occidente. Obtenido de http://red.uao.edu.co/bitstream/10614/6473/1/T04529.pdf

Undelete360. (2017). *undelete360*. Obtenido de http://www.undelete360.com/info.html

Villamil, C. (2014). *Seguridad Informatica*. Recuperado el 2016, de http://goo.gl/tPxsLF

Watermarkit. (2017). *WatermarkIt*. Obtenido de https://watermarkit.uptodown.com/windows

Welivesecurity. (23 de 09 de 2013). *Análisis forense con Autopsy*. Recuperado el 2016, de http://goo.gl/3DKPzU

Wireshark. (2017). *Wireshark*. Recuperado el 2017, de https://www.wireshark.org

Woanware. (08 de 2018). *PrefetchForensics*. Obtenido de https://goo.gl/p2ZPLJ

Wondershare. (2017). *Top 5 Software de Data Recovery de disco duro*. Obtenido de https://goo.gl/tY6h48

WonderShare. (2017). *wondershare Data Recovey*. Obtenido de https://goo.gl/A78sRy

Xplico. (2016). *Xplico*. Recuperado el 2017, de http://www.xplico.org/about

Zuccardi, G., & Gutiérrez, J. D. (11 de 2006). *Informática Forense.* Obtenido de https://goo.gl/sJMJyT

Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

FIRMA ESTUDIANTES Emerson Yamit Gtelortuga Meneses.
Edison Fabian Jaramillo

FIRMA ASESOR Rcdo 03/11/2018 informe final, correcciones

FECHA ENTREGA: _____

FIRMA COMITÉ TRABAJO DE GRADO DE LA FACULTAD _____

RECHAZADO__ ACEPTADO____ ACEPTADO CON MODIFICACIONES_____

ACTA NO._____

FECHA ENTREGA: _____

FIRMA CONSEJO DE FACULTAD_____

ACTA NO._____

FECHA ENTREGA: _____

64