COLEGIO DE CIENCIA Y TECNOLOGÍA

LICENCIATURA EN INGENIERÍA EN SISTEMAS ELECTRÓNICOS
Y DE TELECOMUNICACIONES

Evaluación de herramientas para análisis forense de medios de almacenamiento

TRABAJO RECEPCIONAL
PARA OBTENER EL TÍTULO DE LICENCIADA EN
INGENIERÍA EN SISTEMAS ELECTRÓNICOS
Y DE TELECOMUNICACIONES

PRESENTA
ARELI FABIOLA NÁJERA OLVERA

Director del trabajo recepcional

Dr. Daniel Tapia Sánchez

Ciudad de México, agosto 2017.

UACM
Universidad Autónoma de la Ciudad de México
Nada humano me es ajeno

CA Coordinación Académica

SISTEMA BIBLIOTECARIO DE INFORMACIÓN Y DOCUMENTACIÓN

UNIVERSIDAD AUTÓNOMA DE LA CIUDAD DE MÉXICO
COORDINACIÓN ACADÉMICA

RESTRICCIONES DE USO PARA LAS TESIS DIGITALES

DERECHOS RESERVADOS©

RESUMEN del trabajo recepcional de **Areli Fabiola Nájera Olvera**, presentado como requisito parcial para la obtención del grado de **LICENCIADA EN INGENIERÍA EN SISTEMAS ELECTRÓNICOS Y DE TELECOMUNICACIONES**. Ciudad de México, agosto 2017.

EVALUACIÓN DE HERRAMIENTAS PARA ANÁLISIS FORENSE DE MEDIOS DE ALMACENAMIENTO

En este documento se describe el desarrollo del proceso de clonación y dos etapas del proceso de análisis forense realizado para recuperar archivos de un medio de almacenamiento que fueron eliminados intencionalmente. Lo primero a realizar es el proceso de sanitización a un medio de almacenamiento que será usado en el proceso de clonación, por ello dicho dispositivo de almacenamiento no debe contener información. El siguiente proceso es el análisis forense, el cual consta de seis etapas: preparación, identificación, recolección, adquisición, análisis y presentación de la evidencia.

Las dos etapas que se consideran en este documento son la adquisición y el análisis, dado que las otras etapas no requieren de herramientas informáticas.

Existen diversas herramientas para el análisis forense enfocadas a estas dos etapas, tales como Caine, Helix 3, DEFT, por mencionar algunas. Cada una de ellas contiene herramientas que realizan la adquisición y/o clonación de evidencia, incluyendo herramientas para la recuperación de archivos. En este trabajo se analizó el desempeño de las herramientas mencionadas.

Los resultados obtenidos de las pruebas realizadas a cada una de las herramientas de análisis forense, muestran que es posible recuperar todos los archivos eliminados de formato Word, Pdf y Jpeg a través de la herramienta Photorec contenida en Caine, en comparación con las otras herramientas analizadas.

Palabras clave: sanitización, clonación, imagen forense, recuperación.

Agradecimientos

A la Universidad Autónoma de la Ciudad de México por abrir sus puertas, por permitirme formar parte de ella y darme la oportunidad de prepararme profesionalmente. Así mismo, agradezco el apoyo en la impresión y el empastado del trabajo recepcional.

A mi director Daniel Tapia Sánchez, por la confianza y el apoyo brindado para la realización de este trabajo. Gracias por los conocimientos compartidos en cada una de las clases y por haber formado parte de mi formación académica.

A la profesora Magali Cortez Vázquez, por las enseñanzas y paciencia brindadas durante mi formación académica, incluyendo el apoyo en la lectura y corrección del trabajo. Gracias por su amistad y por motivarme a terminar esta etapa de mi vida.

Al Dr. Eduardo Ramos por los conocimientos compartidos en cada una de las asignaturas, por el apoyo y corrección del trabajo.

Al Dr. José Joaquín Lizardi por el apoyo y corrección del trabajo.

Al profesor Juan Gilberto Salas Márquez por el apoyo y corrección del trabajo.

Finalmente a cada uno de los profesores que formaron parte de mi preparación profesional, por su dedicación y paciencia.

Dedicatoria

A ustedes que me cuidan desde el cielo Luquitas, Clemente, Chano, Antonio y Juanita siempre los llevaré en mi corazón.

Agradezco a Dios y a la Virgen de Guadalupe por la vida y por estar siempre a mi lado. Gracias por la familia que me dieron, por guiarme en cada uno de mis pasos y decisiones que he tomado a lo largo de mi vida, y por darme las fuerzas para continuar en este largo camino.

A mis padres Eladio y Ernestina por el amor que día a día me brindan, por el apoyo durante todo este tiempo pero sobretodo por la confianza depositada en mí, a pesar de que no ha sido fácil llegar hasta aquí lo he logrado, consideren este triunfo como suyo. Recuerden que los amo y son mi mayor motivación para salir adelante, siempre los llevare en mi corazón.

A mis hermanas Ayde, Nubia y Yesica, por el cariño, el apoyo y la comprensión, sin olvidar los regaños por no dormir a mis horas, ahora sabemos que valió la pena todo el esfuerzo. A mis sobrinos Kevin y Aarón, por el cariño y los momentos de risas compartidos.

A mis tía(o)s, prima(o)s y sobrina(o)s por el cariño, el apoyo y la confianza depositada en mí.

A mis amigas Gabriela y Yanely que son mis mejores amigas de la infancia, por el cariño brindado y por los consejos, pero sobretodo por estar siempre al pendiente de mí.

A mis amigas que se convirtieron en otras hermanas Miriam y Paz, le agradezco a Dios por ponerlas en mi camino, por el tiempo compartido en cada una de las asignaturas. Muchas gracias por estar conmigo en los momentos buenos y malos, por los consejos y por todo el cariño que me han brindado, espero que esta gran amistad perdure por siempre.

A Annel por compartir sus conocimientos, más que una profesora es una gran amiga, gracias por tu cariño y tus consejos, siempre impulsándonos a cumplir nuestras metas.

A mis amigos que formaron parte de este largo camino Belen, Nohemi, Mijangos, Ariadna, Liliana, Eder, Roberto, Alonso, Jonathan, Aldo, Miguel, Abigail y Elvia, gracias por su amistad y cariño.

A mis compañeros de trabajo Marisol, Edgar, Rey, Janys, Ivette, Guillermo, Víctor, Carmen, Laura, Bere, René, Gaby, Esther, Paola, Alan y Adrián gracias por su amistad la cual espero que perdure por mucho tiempo.

A mis compadres Alejandra, Roberto, Norma, Joaquín, Julia, Mónica, Gerardo y Faustino, por el apoyo y cariño brindado.

A Angeles por esas largas platicas que me han ayudado a salir adelante, por hacerme entender que cada quien toma sus propias decisiones en la vida.

A Diego, por llegar a mi vida en el momento menos esperado. Gracias por tu amistad, cariño y confianza, por esas pláticas en las que he aprendido que en la vida nada es para siempre.

Finalmente agradezco a cada una de las personas que se quedaron y que llegaron a mi vida, por el cariño brindado y el apoyo incondicional, y también a aquellas que se marcharon para siempre, simplemente no formaban parte de ella.

Todo tiene su tiempo, y todo lo que se quiere debajo del cielo tiene su hora:
tiempo de nacer y tiempo de morir;
tiempo de plantar y tiempo de arrancar lo plantado;
tiempo de matar y tiempo de curar;
tiempo de destruir y tiempo de edificar;
tiempo de llorar y tiempo de reír;
tiempo de lamentar y tiempo de bailar;
tiempo de esparcir piedras y tiempo de juntarlas;
tiempo de abrazar y tiempo de abstenerse de abrazar;
tiempo de buscar y tiempo de perder;
tiempo de guardar y tiempo de desechar;
tiempo de rasgar y tiempo de coser;
tiempo de callar y tiempo de hablar;
tiempo de amar y tiempo de aborrecer;
tiempo de guerra y tiempo de paz.

Eclesiastés, 3

Índice General

Índice de figuras

Índice de tablas

Introducción

El desarrollo de las tecnologías de información y comunicaciones ha abierto nuevas posibilidades para cometer delitos y realizar una serie de actividades ilegales a través de los diversos dispositivos, sistemas e infraestructuras de comunicación. En la última década se ha incrementado de manera importante el número de delitos relacionados con fraudes en el sector bancario o comercial, pornografía infantil, usurpación de identidades y secuestros. Los daños ocasionados por estos delitos son a menudo superiores a los ocasionados en la delincuencia tradicional y también existe una mayor posibilidad de que no lleguen a descubrirse o castigarse tales hechos. La dificultad para demostrar la comisión de delitos informáticos radica principalmente en la naturaleza de las evidencias digitales, las cuales muchas veces son por completo intangibles y difíciles de presentar dentro de un proceso judicial. Es por eso que ante el suceso de un delito informático u otro delito en el que se considere que equipos de cómputo o de comunicaciones pueden presentar evidencia, es necesaria la intervención de un perito en informática forense.

La informática forense es el campo que se encarga de analizar sistemas informáticos para obtener evidencias digitales de algún delito o actividad ilegal, y que pueden ser presentadas en un juicio. Una de las labores más importantes en el proceso de recolección de evidencias es la recuperación y análisis de datos a partir de medios de almacenamiento utilizados para cometer algún ilícito. Los medios de almacenamiento donde se encuentran las evidencias deben ser tratados como una escena de crimen y se deben tomar todas las medidas necesarias para garantizar el manejo adecuado de evidencias en la escena.

En este documento se aborda precisamente el proceso de recuperación y análisis de datos en medios de almacenamiento cuyo contenido ha sido eliminado de manera intencional. El trabajo describe los procedimientos para recuperar archivos y datos eliminados del medio y al mismo tiempo evalúa diferentes herramientas automáticas diseñadas para asistir en la recuperación de evidencias en el proceso de análisis forense. La evaluación de las herramientas es muy importante desde el punto de vista jurídico,

pues la validez de las evidencias recolectadas está determinada por la capacidad de las herramientas para preservar su integridad.

Específicamente se abordan cuatro diferentes herramientas, de las cuales una de ellas es utilizada para el proceso de sanitización y tres de ellas para el análisis forense. Es importante mencionar que todas las herramientas utilizadas en este trabajo son de uso libre y su utilización, desde el punto de vista jurídico, aún presenta huecos importantes, por lo que la evaluación de estas herramientas en casos prácticos contribuirá a demostrar su validez en el análisis forense.

Planteamiento del problema

Dadas las diversas herramientas de uso libre para la recuperación y análisis automático de datos en medios de almacenamiento, se requiere determinar cuál ofrece el mejor desempeño para ser utilizada en procesos de análisis forense para la obtención de evidencias digitales.

Solución propuesta

Para responder a la problemática planteada, se propone evaluar el desempeño de algunas de las herramientas de uso libre para la recuperación y análisis automático de datos en medios de almacenamiento y su capacidad para recuperar archivos y datos eliminados como fuentes de evidencia digital. Se propone considerar las tres herramientas de uso libre más reconocidas en el campo de la informática forense y reemplazar el uso de dispositivos de respaldo de alto costo por procedimientos estandarizados implementados sobre discos convencionales como dispositivos USB y discos duros externos.

Objetivo

Evaluar el desempeño de tres herramientas para análisis forense aplicando procedimientos y prácticas estándar de forensia digital para la obtención de evidencias en medios de almacenamiento.

Con el fin de lograr el objetivo planteado se definen los siguientes objetivos particulares:

1) Aplicar el procedimiento de sanitización a un medio de almacenamiento, de acuerdo con el software Darink´s Boot and Nuke (DBAN).

2) Realizar la clonación y/o adquisición de un medio de almacenamiento con diferente software de análisis forense.

3) Comprobar que la clonación y/o adquisición del medio no ha sido alterada a través de herramientas como Dhash.

4) Evaluar el desempeño de las herramientas de análisis forense con respecto a la recuperación de archivos.

Alcances y limitaciones

En este proyecto se aplica el procedimiento de sanitización, clonación y se consideran únicamente las etapas de adquisición y analisis del proceso de análisis forense, siendo la principal aportación de este trabajo.

Materiales y herramientas

Para hacer uso de cada una de las herramientas mencionadas se requiere de un CD y de una USB de autoarranque, con el propósito de no instalar ninguna de éstas en la computadora que será utilizada. En el caso del software de análisis forense, éste cuenta con una interfaz gráfica de fácil manejo y es de acceso libre.

Considerando el tiempo que tarda el proceso de sanitización de un disco duro de 1 TB que es de aproximadamente 12 días, se ajustó un medio de almacenamiento de 1 GB para considerarlo como dispositivo de evidencia.

Organización del trabajo recepcional

En términos generales, el capítulo uno describe la metodología del análisis forense, que consta de seis etapas las cuales son descritas a detalle.

El capítulo dos explica el proceso de sanitización de un medio de almacenamiento, describiendo los pasos necesarios.

El capítulo tres se refiere al uso de cada una de las herramientas para la recuperación de archivos. Finalmente se presentan las conclusiones.

Capítulo 1

Marco Teórico

En este capítulo se introducen los conceptos que sirven de marco teórico para el trabajo de tesis, los cuales se relacionan esencialmente con la informática forense y el análisis forense en medios informáticos. El capítulo brinda un panorama general del análisis forense: imagen forense y metodología del análisis forense. En este último, se mencionan algunos aspectos importantes en el proceso de adquisición de imagen.

1.1 Análisis Forense

El FBI define a la informática forense como la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional [1]. La mayoría de las actividades ilícitas tales como homicidios, fraudes financieros, pornografía infantil, evasión de impuestos, discriminación, acoso, robo o pérdida de información por mencionar algunos, están relacionados con el incremento de los delitos a través de las redes de telecomunicaciones. Esta es la razón por la que se han desarrollado herramientas que permiten realizar una investigación y responder a las cuestiones: ¿qué paso?, ¿cuándo paso?, ¿cómo paso?, ¿quién es el responsable o sospechoso?, entre otras, obteniendo así las evidencias digitales necesarias para que puedan ser presentadas ante un juicio.

En México, la Secretaría de Seguridad Pública del Distrito Federal (SSP-DF) estableció el agrupamiento de la Policía Cibernética para detener delitos cibernéticos como la pornografía infantil, fraudes y trata de personas. Además, los delitos informáticos se normalizan en el Código Penal Federal, libro segundo, título noveno referido a la "Revelación de secretos y acceso ilícito a sistemas y equipos de informática".

1.2 Evidencia Digital

La evidencia digital es el elemento principal del análisis forense, la cual se define como "cualquier información de valor probatorio que se almacena o transmite de forma digital" [2]. Existen dos tipos de evidencia digital, y se relacionan exactamente cuando la computadora se apaga [3]:

- **Evidencia constante:** se denomina también evidencia no volátil y se refiere a evidencias relacionadas con datos almacenados en un medio informático que se conservan aún después de apagar el dispositivo. Se clasifica en evidencia física y evidencia lógica, según el lugar en donde se almacenen los datos.

La evidencia física se refiere a los datos localizados en medios de almacenamiento óptico (CD, CD-ROM, DVD, Blue Ray), agendas o tabletas electrónicas, así como en dispositivos de red tales como switches, routers, firewalls, módems, entre otros.

Por otra parte, la evidencia lógica se relaciona con los datos almacenados en medios magnéticos o eléctricos tales como discos, cintas magnéticas o memorias extraíbles. El tipo de información que representa la evidencia está relacionada generalmente con registros de actividad (LOGS) generados por el sistema, registros híbridos, registros de servidores, registros de tráfico de red y los registros de aplicación.

- **Evidencia volátil:** los datos que componen la evidencia se encuentran almacenados en la memoria principal RAM o caché de los equipos, por lo que en el momento en que se suspende la alimentación eléctrica se pierden.

Se debe considerar que un sistema de archivos es un sistema o método de almacenamiento y recuperación de información en un sistema informático que permite una jerarquía de directorios, subdirectorios y archivos. Algunos sistemas de archivos son: File Assignation Table (FAT12, FAT16, FAT32), NTFS (New Technology File System), HFS, HFS+, ext2, ext3, ISO 9660, UDF y UFS. El sistema de archivos determina cómo se organizan los datos en el disco y controla dónde se escriben [4].

Además, en la tabla 1.1 se mencionan algunas características de los medios de almacenamiento que se consideran en el proceso de recuperación de archivos, tales como la capacidad de almacenamiento y velocidad de transferencia.

Medio de almacenamiento	CD-RW	DVD-RW	Unidad USB	Unidad de disco duro externo HDD
Capacidad de almacenamiento	640 MB – 700 MB	4.7 GB – 17 GB	128 MB – 512 GB	60 GB – 2 TB
Velocidad de transferencia	1x = 150 Kb/s 4x = 600 Kb/s	1x = 1350 Kb/s 4x = 5400 Kb/s = 5.4 Mb/s	USB 1.1: 1.5 Mb/s USB 2.0: 60 Mb/s USB 3.0: 600 Mb/s	USB 2.0: 480 Mb/s USB 3.0: 5 Gb/s

Tabla 1. 1 Características de medios de almacenamiento

En la tabla 1.2 se realiza una breve descripción sobre los diferentes medios de almacenamiento con respecto a las partes físicas, el almacenamiento y la interfaz correspondiente.

	HDD (Hard Disk Drive: Disco Duro)	SSD (Solid State Drive: Unidad de Estado Sólido)	USB (Universal Serial Bus: Bus en Serie Universal)
Partes a nivel físico	Formado por discos, cabezas, eje, impulsor de cabeza (de manera lógica formado por pistas, sectores, cilindros y clúster)	Formado por un conjunto de chips de memoria flash NAND, caché RAM, controlador de memoria, controlador de interfaz y conector de interfaz (SATA, ATA, SAS, entre otros)	Formado por chips de memoria flash NAND Y NOR (dependiendo de la capacidad), una ranura para esta y un conector de entrada/salida para la interfaz USB
Almacenamiento	Formado por uno o varios discos apilados que giran a gran velocidad, sobre los que se mueve una pequeña cabeza magnética que graba y lee la información. Además este medio proporciona el acceso secuencial a datos	NAND (tecnología no volátil de almacenamiento) se diseña basándose en el uso de tecnología de celda. SLC (Single-Level Cell) es un elemento de memoria capaz de almacenar datos en celdas de memoria individuales. La SLC accede a alta velocidad a la SSD y escribe en ella mediante una lógica de control "más simple" de 1 bit, MLC (Multi-Level Cell) almacena 2 bits de información por celda y TLC (Triple-Level Cell) almacena tres bits por celda	NOR es una tecnología de memoria Flash de alta velocidad. Esta proporciona capacidades de acceso aleatorio de alta velocidad, pudiendo leer y escribir datos en lugares específicos de la memoria sin tener que acceder a la memoria en modo secuencial. Además permite la recuperación de datos desde un solo byte La tecnología NAND lee y escribe a alta velocidad, en modo secuencial, manejando datos en bloques de tamaño pequeño ("páginas"). La memoria Flash NAND puede recuperar o escribir datos como páginas únicas, pero no puede recuperar bytes individuales Los chips de memoria Flash NAND y NOR almacenan el valor de un bit (un “0” o un “1”) en cada celda (SLC), en el caso de nivel múltiple se almacenan dos bits (MLC) o tres bits (TLC) en cada celda
Interfaz del medio	**SAS (Serial Attached SCSI)**: interfaz que permite a los ordenadores comunicarse con los dispositivos mediante una controladora	**IDE (Integrated Drive Electronics) / ATA (Advanced Technology Attachment)**: puerto paralelo al que se conecta un cable plano que se distribuye en canales, con un máximo de dos dispositivos por canal. Además utiliza 16 bits de ancho	**USB**: interfaz que se diseñó para estandarizar la conexión de periféricos en las computadoras tales como teclados, impresoras, entre otros. Esta interfaz realiza la transmisión de datos y provee voltaje de alimentación. Se transporta la información en formato serie
		SCSI (Small Computer System Interface): puerto paralelo de alta velocidad que se utiliza en servidores. Utiliza la topología de bus en la cual ocho líneas en el bus se utilizan para la transferencia de datos. Los primeros dispositivos SCSI solo transferían un byte a la vez. Lee y escribe datos simultáneamente	
	SATA (Serial ATA): los datos se transfieren simultáneamente en paralelo por vías del cable, con mayor velocidad de transmisión	**SAS (Serial Attached SCSI)**	
		SATA (Serial ATA)	

Tabla 1. 2 Características de medios de almacenamiento con respecto a la estructura de datos

En el procedimiento del análisis forense, una evidencia digital presenta las siguientes características:

- Es confidencial
- Es alterable y/o destruible
- Es duplicable

Debido a sus características, la manipulación de evidencias digitales debe obedecer a un proceso formal, reconocido y avalado por las diferentes instancias técnico-legales reconocidas oficialmente.

1.3 Metodología del Análisis Forense

En la actualidad existen diferentes métodos para llevar a cabo un análisis forense, tales como el Modelo del Instituto Nacional de Justicia (NIJ) de los Estados Unidos, el Modelo propuesto por Brian Carrier y el Modelo de los investigadores forenses de la Academia de Policía de Noruega; y todos ellos comparten muchas similitudes. Todos estos métodos pretenden preservar la validez de la evidencia digital con el fin de presentarla en un juicio. En la figura 1.1 se muestra la metodología estándar de un análisis forense.

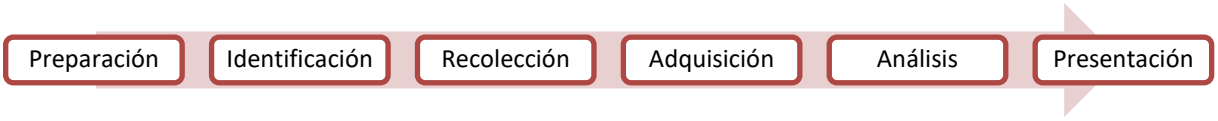


Figura 1. 1 Metodología de un análisis forense

1.3.1 Preparación de la evidencia

La principal prioridad es la protección de la escena, tratando de evitar que la evidencia sea alterada y pueda ser válida ante un juicio. Después de que el área ha sido asegurada, los investigadores forenses están listos para entrar al área y comenzar a registrar la escena a través de notas, dibujos, videos o fotografías sin que se haya tocado ni movido

algún elemento. Lo siguiente es tratar de reducir las interrogantes de la escena tal como: ¿qué paso?, ¿cómo paso?, entre otras.

Las herramientas indispensables con las que debe contar un investigador son: juegos de herramientas (kit de servicio técnico, cables, etc.); guantes de látex; manuales de referencia de computadoras; cámara digital para la captura de datos de las pantallas y la escena; cables de extensión, protectores contra sobrecargas, fuentes de alimentación ininterrumpida (SAI); cables de red cruzados y tarjetas de interfaz de red de repuesto (NICs); disquete o CD vírgenes; discos duros de almacenamiento (en el cual se colocan las imágenes), una USB y los adaptadores IDE/SATA; bolsas Faraday para protección de dispositivos móviles de la red; etiquetas, bolsas antiestáticas, cinta de pruebas, marcadores; cuaderno de registro, bolígrafos, lápices, entre otras [6].

1.3.2 Identificación

Se refiere a identificar los posibles tipos de evidencias que se encuentran en la escena: información del sistema (incluyendo el fabricante), número de serie, modelo, componentes; inclusive examinar si existe una red inalámbrica y/o cableada. Todo lo anterior debe ser registrado y fotografiado antes de ser decomisado.

1.3.3 Recolección

Lo primero a realizar en el procedimiento de recolección de evidencia digital volátil, es fotografiar la pantalla para capturar el estado del sistema dado que los datos contenidos en la memoria RAM, los procesos de ejecución, las conexiones de red y otros datos se pierden cuando la computadora se apaga. Otra opción es usar algún software que obtenga la imagen del sistema activo por medio de una conexión de red.

Para recolectar una evidencia digital constante (disco duro, CD, USB) es obligatorio el uso de guantes de látex para su manejo, para evitar la mezcla de huellas dactilares de los investigadores con las que ya se encontraban en ellos, sobre todo en caso de que se realice algún análisis de huellas dactilares.

Es muy importante conocer el procedimiento de apagado de una computadora para obtener la evidencia digital, y evitar alterar su contenido. Lo principal es determinar el tipo de sistema operativo que se está ejecutando para saber de qué manera se apagará. Por ejemplo, la mayoría de los modelos de Windows pueden apagarse desconectando el cable de alimentación o la conexión de red [7].

En la tabla 1.3 se describen algunos procedimientos de apagado de computadoras, dependiendo de su sistema operativo [8].

Sistema operativo	Procedimiento de apagado
DOS **Windows 3.1** **Windows 95** **Windows NT Workstation** **Windows 98/Me** **Windows 2000** **Windows XP** **Windows Vista** **Windows 7** **Windows 7 Enterprise**	Extraer el enchufe/cable de la parte trasera de la computadora
Windows NT Server **Windows 2000 Server** **Windows 2003 Server** **Windows 2008 Server**	Usar el procedimiento de apagado normal
Linux/Unix	Usar el procedimiento de apagado normal. En ocasiones el usuario tendrá que entrar como “root” en la terminal para apagar el sistema (con el comando shutdown –h now)
Macintosh	Extraer el enchufe/cable de la parte trasera de la computadora. Mac puede ejecutar servidores web, servidores de base de datos, email, entre otros. Para OS X, se da clic en el icono Apple y seleccionar la opción apagar, por último se confirma esta acción

Tabla 1. 3 Procedimientos de apagado de sistemas operativos

En caso de no identificar el tipo de sistema operativo de la computadora a simple vista, se sugiere realizar el apagado normal; además de registrar todo el procedimiento usado en cada caso.

Durante la protección de la evidencia se procede al etiquetado y empaquetado. El objetivo del etiquetado es proporcionar información acerca del lugar, la fecha, la hora, etc.; mientras que el empaquetado se encarga de proteger la evidencia de la contaminación y el deterioro, por lo que es recomendable hacer uso de materiales de embolsado con propiedades antiestáticas (evitando que se generen daños por descargas eléctricas).

1.3.4 Adquisición de la evidencia

El procedimiento para adquirir una evidencia digital, se realiza a través de hardware y/o software para análisis forense. La adquisición de datos implica crear una imagen forense de la evidencia digital original. La imagen o copia forense se define como un duplicado o copia exacta de un medio de almacenamiento, que puede ser protegida usando el bloqueo de escritura en el dispositivo.

Antes de realizar la imagen forense en un medio de almacenamiento, se debe verificar que el medio esté completamente limpio, es decir, todas las áreas del disco son reemplazadas por los caracteres 0 y 1 (se sobrescribe en cada archivo que haya sido almacenado). A este proceso se le llama "sanitización", y en caso de no efectuarlo, el medio podría contener datos residuales creando una imagen forense contaminada.

Para verificar que la imagen forense es exactamente igual a la evidencia original, se recurre al método llamado “hashing”, que asegura la integridad de la imagen forense adquirida ya que cualquier alteración de los datos puede ser detectada.

En la tabla 1.4 se describen algunas herramientas de software libre y en la tabla 1.5 las herramientas de hardware para desarrollar un análisis forense.

Herramienta	Descripción
EnCase Forensics Imager	Realiza adquisición de volúmenes completos, carpetas y archivos; además permite la navegación y visualización de archivos
DEFT (Digital Evidence & Forensic Toolkit)	Contiene herramientas para análisis de ficheros, cálculo de hash, creación de imagen y clonación, recuperación de contraseñas, entre otros
CAINE (Computer Aided INvestigative Enviroment)	Cuenta con herramientas para la creación de imágenes, cálculo de hash, recuperación de archivos y datos, análisis de redes forenses, entre otros
Helix 3	Incluye herramientas para realizar la adquisición de imágenes, recuperación de datos y contraseñas, cálculo de hash, análisis de red forense, por mencionar algunos
OSFClone	Procede a la adquisición de imágenes y clonación de medios de almacenamiento

Tabla 1. 4 Herramientas de software libre para realizar análisis forense

Herramienta	Descripción
Guidance Software	Empresa productora de herramientas de hardware y software para análisis forense digital, como: EnCase Enterprise v7, EnCase Forensics v7 y EnCase Portable
Tableau	Incluye hardware para la elaboración de pruebas informáticas: bloqueadores de escritura para todas las tecnologías de medios magnéticos, duplicadores forenses y aceleradores de hardware para recuperación de contraseñas
Decision Computer Group inc	Proporciona el análisis forense de paquetes de datos de una red a través de: E-Detective System, Wireless Detective, E-Detective Decoding Centre y VOIP Detective
Paraben Forensic	Provee las herramientas para análisis informático forense, correo electrónico y dispositivos móviles: Device Seizure, Email Examiner/Network Email Examiner y P2 commander

Tabla 1. 5 Herramientas de hardware para realizar análisis forense

1.3.5 Análisis de la imagen forense

En el momento de proceder al análisis de la imagen forense, lo más importante es que no se permite analizar la evidencia digital original. Cabe mencionar que tampoco se puede modificar la información contenida en la imagen y se recomienda usar cualquier software, que ejecute el bloqueo de escritura en la evidencia digital. El análisis incluye la recuperación de archivos y datos, recuperación y desbloqueo de contraseñas, análisis de red, búsqueda de antimalware, por mencionar algunos.

En el presente trabajo solo se realiza la recuperación de archivos borrados y ocultos de un dispositivo USB.

1.3.6 Presentación de resultados del análisis forense

Este es el último proceso del análisis forense, y se encarga de la elaboración y la presentación de los resultados obtenidos en el proceso anterior. Además se anexa de manera explícita cada uno de los procesos desarrollados.

Capítulo 2

Proceso de Sanitización

Para iniciar el análisis forense de un medio de almacenamiento, es necesario realizar previamente el proceso de sanitización con el objetivo de que el dispositivo no contenga ningún dato. Es necesario conseguir el software en imagen ISO para obtener un CD de autoarranque, además de un software que realice la grabación de imagen ISO en el disco, para conseguir que la computadora inicie desde este medio. En este capítulo se describen brevemente las herramientas para el proceso de sanitización, y el procedimiento estándar de la herramienta de software libre DBAN (Darink´s Boot and Nuke).

2.1 Proceso de sanitización

Cuando se realiza un análisis forense, se da por hecho de que la escena del crimen está relacionada con componentes de hardware y software, los cuales pueden ser alterados de manera intencional o accidentalmente durante la recolección de la evidencia. Para demostrar en todo momento que la escena del crimen no ha sido alterada, no se trabaja directamente con la escena, sino con una copia de la misma. El único requisito es que la copia de la escena del crimen sea una copia fiel y que contenga exactamente las mismas evidencias que la escena real. Cuando se realiza la reproducción de la escena del crimen, se utilizan medios de almacenamiento preparados especialmente mediante un proceso denominado sanitización, a través del cual se garantiza que los discos contenedores estén completamente libres de datos que pudieran alterar la escena del crimen.

2.2 Herramientas de software para el proceso de sanitización

Existen diferentes herramientas de software que ejecutan el proceso de sanitización, entre las que se encuentran Active@KillDisk, Wipe Drive Demo, Darink´s Boot and Nuke (DBAN), Eraser, entre otros. A continuación se describen estas herramientas, y el proceso de DBAN en la sanitización de un dispositivo de almacenamiento USB de 8 GB.

2.2.1 La herramienta Darink´s Boot and Nuke (DBAN)

Darink´s Boot and Nuke es un software que borra los datos contenidos en un medio de almacenamiento. Los métodos con los que cuenta para realizar tal procedimiento se describen en la tabla 2.1.

Método	Características
Quick Erase	Sobrescribe 1 vez con ceros
Royal Canadian mounted Police Technical Security Standard for Information Technology, Appendix OPS II (RCMP TSSIT OPS II)	Sobrescribe 8 veces con ceros, unos y caracteres aleatorios

DoD Short (American Department of Defense 5220.22-M short wipe)	Sobrescribe 3 veces con ceros, unos y caracteres aleatorios
DoD 5220.22-M (American Department of Defense 5220.22-M standard wipe)	Sobrescribe 7 veces con ceros, unos y caracteres aleatorios
Gutmann Wipe	Sobrescribe 35 veces con ceros, unos y caracteres aleatorios
PRNG Stream	Sobrescribe por defecto 1 vez, se puede modificar este número por el que desee él usuario

Tabla 2. 1 Métodos de borrado de DBAN

2.2.2 Wipe Drive Demo

El objetivo de Wipe Drive Demo es borrar toda la información almacenada en un medio de almacenamiento, incluyendo el sistema operativo, tablas de particiones, programas de software, entre otros.

Algunos de los métodos incluidos en Wipe Drive Demo se describen en la tabla 2.2.

Método	Características
Standard overwrite	Sobrescribe 1 vez con ceros
Department of Defense 5220.22-M	Sobrescribe 3 veces con ceros, unos y caracteres aleatorios, y una verificación
HMG Infosec Standard #5 Enhanced	
Navy Staff Office Publication (NAVSO P-5239-26)	
The National Computer Security Center (NCSC-TG-025)	
HMG Infosec Standard #5 Baseline	Sobrescribe 1 vez con ceros y una verificación

Canadian RCMP TSSIT OPS II Standard Wipe	Sobrescribe 7 veces con ceros, unos y caracteres aleatorios, y una verificación
U.S. Army AR380-19	Sobrescribe 3 veces (1° patrón de ceros, 2° patrón de unos y 3° patrón de caracteres especificados por el usuario)
U.S. Air Force System Security Instructions 5020	Sobrescribe 3 veces (1° patrón de unos, 2° patrón de ceros y 3° patrón de caracteres especificados por el usuario)
German VSITR Standard	Sobrescribe 7 veces con ceros, unos y con el carácter A
Russian Standard, GOST P50739-95 version 2	Sobrescribe 1 vez con caracteres aleatorios
Department of Defense 5220.22-M	Sobrescribe 3 veces con ceros, unos y con el carácter 97, con su respectiva verificación
Australian DSD (X0-PD)	Sobrescribe 3 veces con dos verificaciones
Australian DSD (X1-P-PD)	Sobrescribe 5 veces con dos verificaciones
Custom	Sobrescribe "n" veces. El número de patrones de sobrescritura se especifican en usrclean.txt y los caracteres son especificados por el usuario

Tabla 2. 2 Métodos de sobrescritura de Wipe Drive Demo

2.2.3 Active@KillDisk

La finalidad de Active@KillDisk es borrar los datos en el medio de almacenamiento completo y de sus particiones, incluso borra los datos localizados en un espacio no usado. Este software sobrescribe 1 vez en el medio con ceros.

2.3 Procedimiento de sanitización usando DBAN

A continuación se describe el procedimiento de sanitización usando DBAN, en un medio de almacenamiento de 8 GB.

1) Se accede a la BIOS, encendiendo la computadora y pulsando repetidamente la tecla **F12**. En este caso, se seleccionó **CD/DVD Rom** para que la computadora inicie desde este dispositivo, ver figura 2.1.

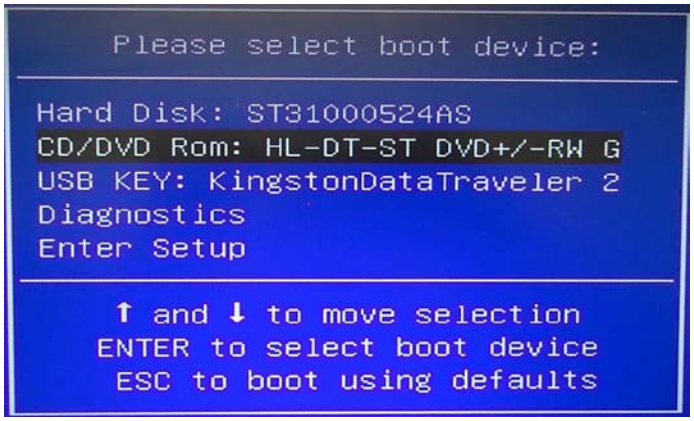


Figura 2. 1 Selección de dispositivo de arranque

2) A continuación se mostró la ventana principal (figura 2.2), en la cual se observaron las opciones que ofrece DBAN (**learn about DBAN, list of quick commands, DBAN in interactive mode** y **DBAN in automatic mode**).

Figura 2. 2 Ventana principal DBAN

Se eligió la opción **DBAN in interactive mode** por lo que se presionó la tecla **ENTER**, ya que la opción **automatic mode** realiza el borrado automático del disco que se encuentra conectado a la computadora. Después comenzó a cargarse DBAN como se muestra en la figura 2.3.

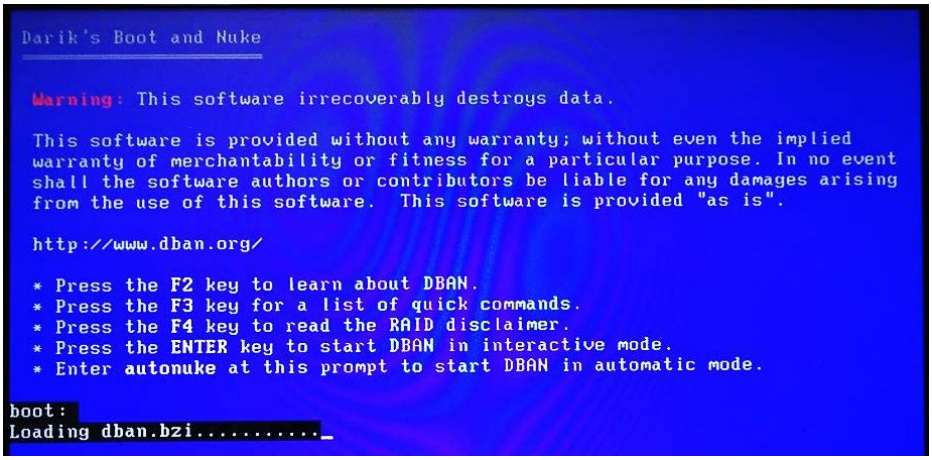


Figura 2. 3 Inicio de DBAN

3) La siguiente ventana (figura 2.4) mostró información acerca de los discos y particiones disponibles a los que se les puede aplicar el borrado, además el método seleccionado.

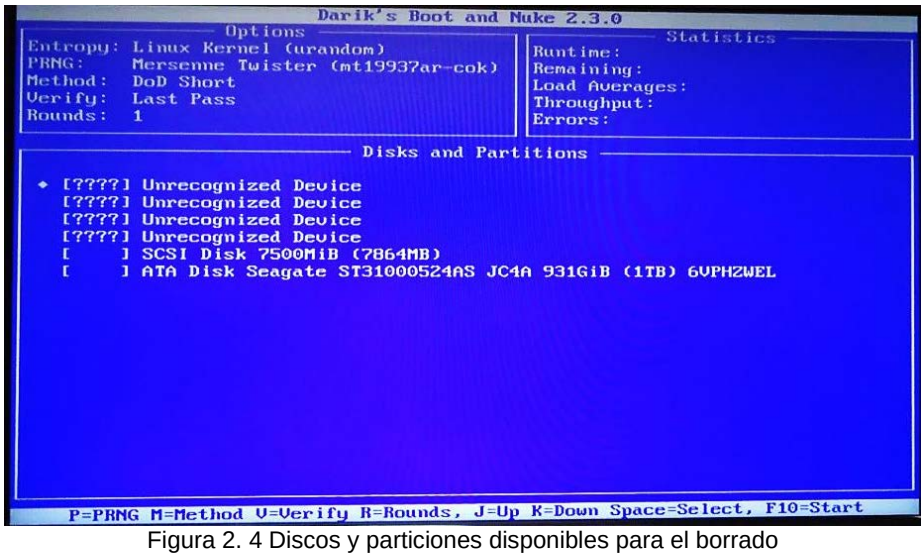


Figura 2. 4 Discos y particiones disponibles para el borrado

4) Primero se seleccionó el método presionando la tecla M, en este caso se eligió la opción **Gutmann Wipe**, que es el más fiable por el número de pasadas de sobrescritura que realiza en el disco, ver figura 2.5.

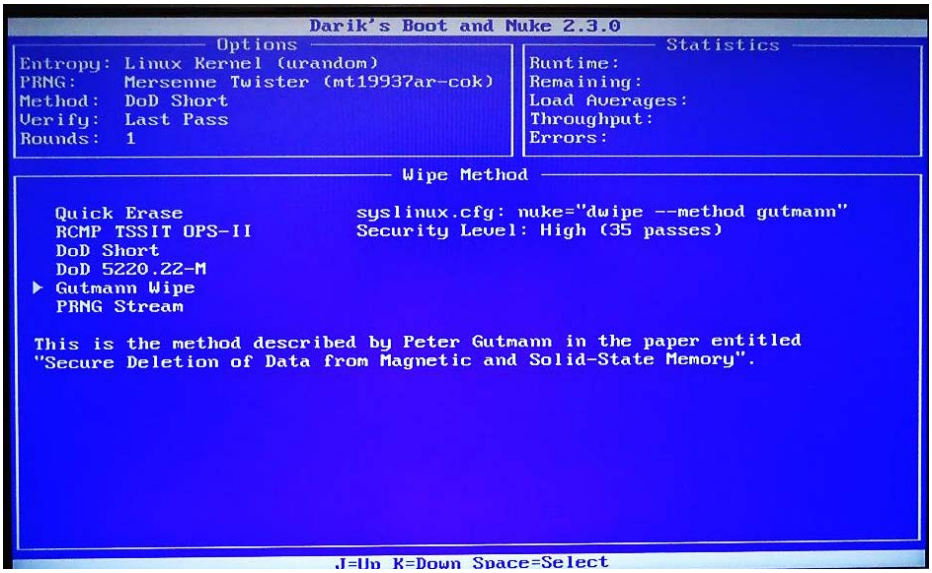


Figura 2. 5 Selección del método Gutmann Wipe

5) Después de haber elegido el método, se regresa a la ventana para seleccionar el dispositivo con la tecla de barra espaciadora; en este caso se seleccionó **SCSI Disk 7500 MiB (7864MB)** como se muestra en la figura 2.6.

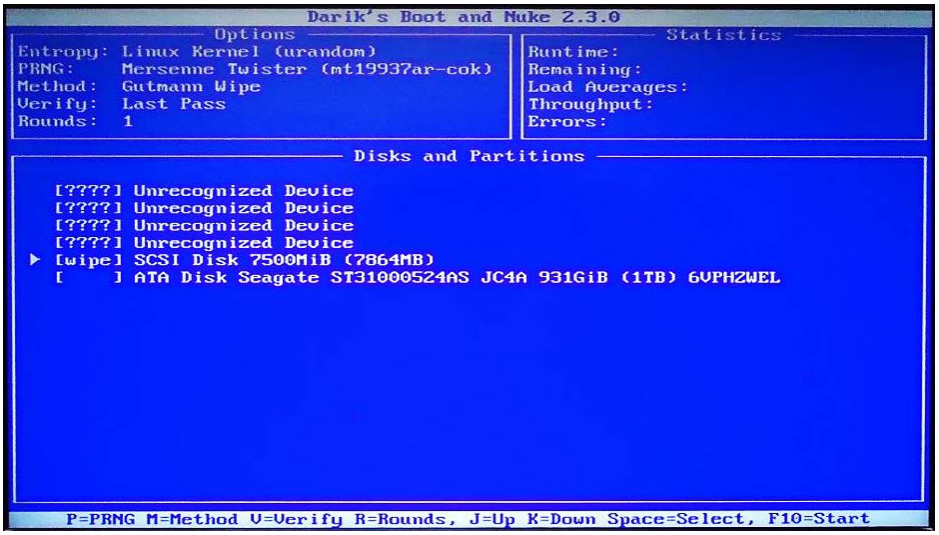


Figura 2. 6 Selección de disco

6) Para iniciar el proceso de sanitización se presionó la tecla **F12**, en la figura 2.7 se observan algunas estadísticas del proceso tal como el tiempo de ejecución, el tiempo restante, errores, entre otros.

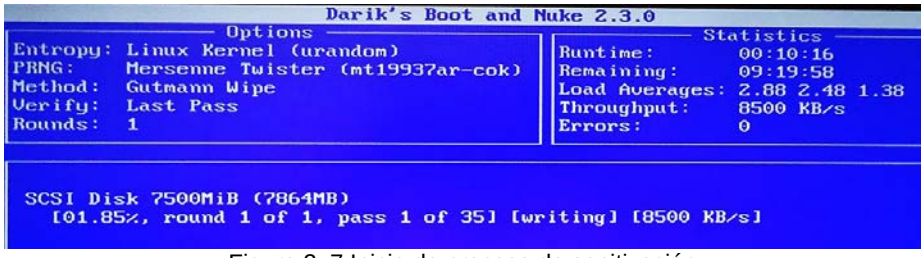


Figura 2. 7 Inicio de proceso de sanitización

7) Por último, el mensaje de la figura 2.8 indica que se ha completado el proceso de sanitización, incluyendo el **tiempo de inicio** y **fin**. Debe considerarse que por el método seleccionado tardó más de 10 horas dicho proceso. Por otro lado, se brinda la opción de guardar los registros si se desea.

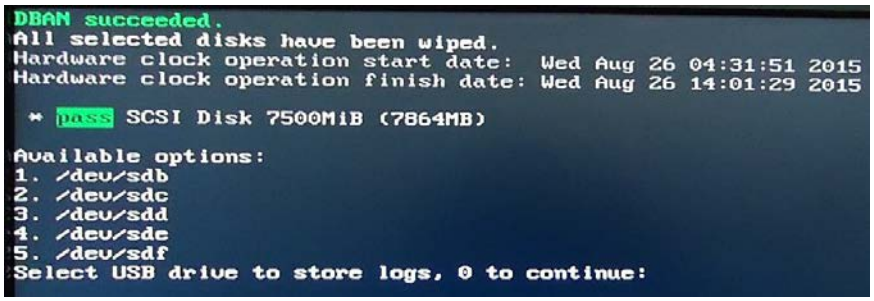


Figura 2. 8 Proceso completado

8) Para retirar el CD y el dispositivo sanitizado, se tecleó la opción "0" e inmediatamente se presentó la pantalla de la figura 2.9.

Figura 2. 9 Fin de proceso

9) Para verificar que el proceso funcionó correctamente, se conectó el dispositivo USB a una computadora y automáticamente detectó que el dispositivo **no tiene ningún formato**, ver figuras 2.10, 2.11 y 2.12.

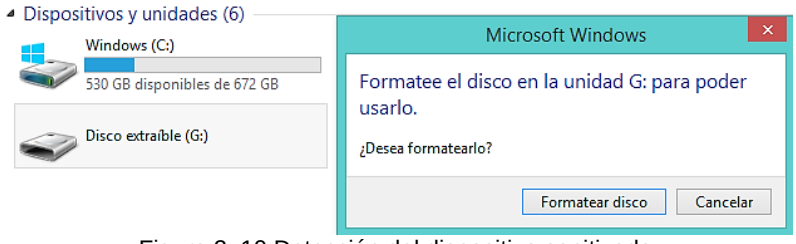


Figura 2. 10 Detección del dispositivo sanitizado

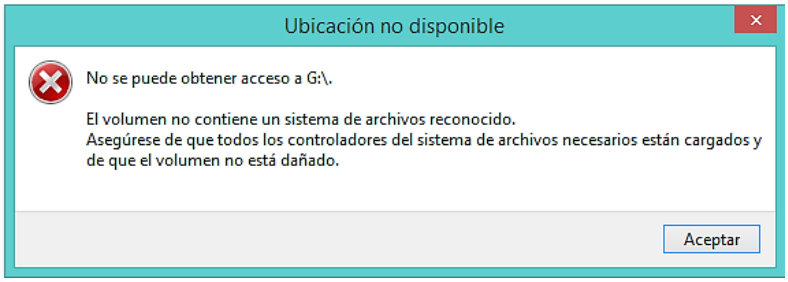


Figura 2. 11 Acceso denegado del dispositivo sanitizado

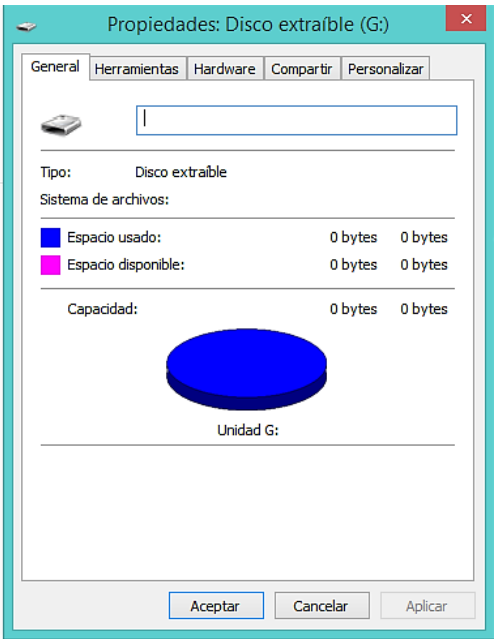


Figura 2. 12 Propiedades del dispositivo sanitizado

Capítulo 3

Análisis forense de medios de almacenamiento

En este capítulo se evalúan distintas herramientas para el análisis forense de medios de almacenamiento, con el objetivo de comparar su desempeño al realizar la recuperación de archivos de un medio de almacenamiento. Se consideran las herramientas CAINE, HELIX3 y DEFT8, las cuales permiten: establecer el dispositivo como solo lectura, la adquisición y/o clonación y el cálculo de hash del dispositivo.

3.1 Computer Aided Investigative Environment (CAINE)

El primer software usado fue Computer Aided Investigative Environment (CAINE), un software de la distribución de Linux y cuenta con herramientas que realizan la recolección y el análisis de evidencia, elaboración de informe, reporte de resultados, entre otros. En total, CAINE cuenta con 29 herramientas diferentes para el análisis forense, algunas de las cuales se describen en la tabla 3.1.

Herramienta	Descripción
Autopsy	Realiza el análisis de la evidencia digital
Gtkhash	Realiza el cálculo del valor hash de un archivo (MD5, SHA1, SHA256, SHA512, entre otros)
Guymager	Realiza la adquisición y clonación de un disco (la copia se crea bit a bit). En el caso de adquisición se consideran dos tipos de formatos: .dd y e01
iPhone Backup Analyzer (iPBA2)	Accede al sistema de archivos del iphone
Log2Timeline	Crea una línea de tiempo para analizar archivos de registro (logs)
Photorec	Recupera datos, archivos, documentos y videos perdidos de discos duros
Testdisk	Recupera particiones de almacenamiento de datos perdidos
Volatility	Analiza procesos y extrae información (para análisis forense en memoria)
Wireshark	Captura y analiza los paquetes de red

Tabla 3. 1 Herramientas de CAINE

3.1.1 Dispositivo evidencia

El dispositivo usado como evidencia contiene las siguientes características:

- Tipo: Data Traveler 1 GB
- Nombre: DATOS
- Sistema de archivos: FAT32
- Espacio usado: 407, 171, 072 bytes (388 MB)
- Espacio disponible: 620, 417, 024 bytes (591 MB)
- Capacidad: 1, 027, 588, 096 bytes (979 MB)

El dispositivo cuenta con 9 carpetas de archivos, 2 documentos de Microsoft Office Word y 6 archivos de Adobe Acrobat Document, ver figura 3.1.

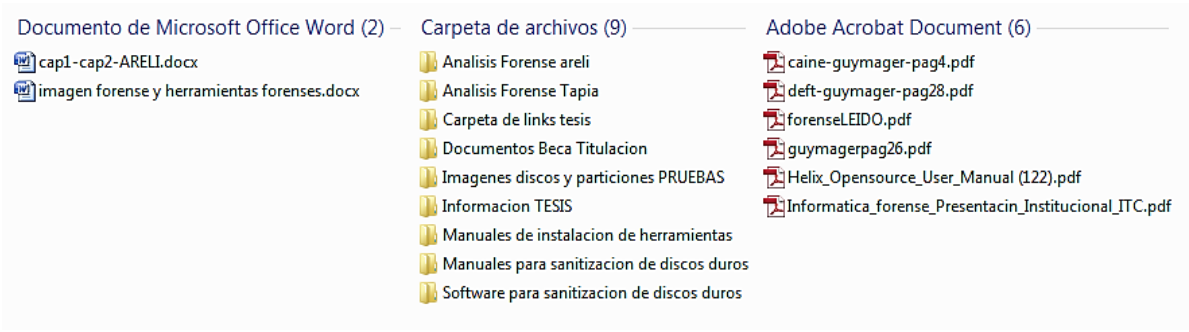


Figura 3. 1 Información del dispositivo evidencia

De manera intencional, fueron eliminados los siguientes tipos de archivos con el fin de recuperarlos más tarde con las herramientas mencionadas anteriormente:

- Docx (1 archivo)
- Epub (1 archivo)
- Jpeg (26 archivos)
- Pdf (3 archivos)
- Winrar (1 archivo)

3.1.2 Guymager y Photorec

Guymager realiza la adquisición de imagen y clonación de un dispositivo a través de una interfaz gráfica sencilla, mientras que Photorec recupera archivos y datos por medio de una interfaz de línea de comandos. **A continuación se describe el proceso completo para llevar a cabo la clonación del dispositivo evidencia y su correspondiente recuperación.**

1) Se accedió a la BIOS, encendiendo la computadora y pulsando repetidamente la tecla "F12". Se seleccionó la opción **USB KEY: KingstonDataTraveler 2** para que la computadora inicie desde este dispositivo, ver figura 3.2.

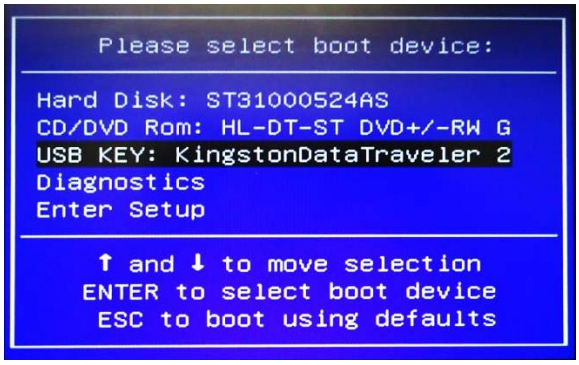


Figura 3. 2 Selección de dispositivo de arranque

2) La computadora inició desde el dispositivo de arranque, se eligió la opción **Boot Live System** para que se cargue CAINE, ver figura 3.3.

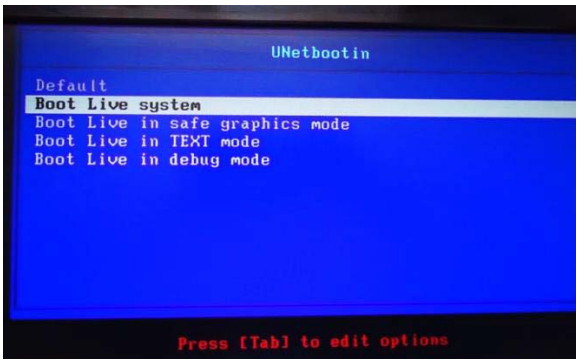
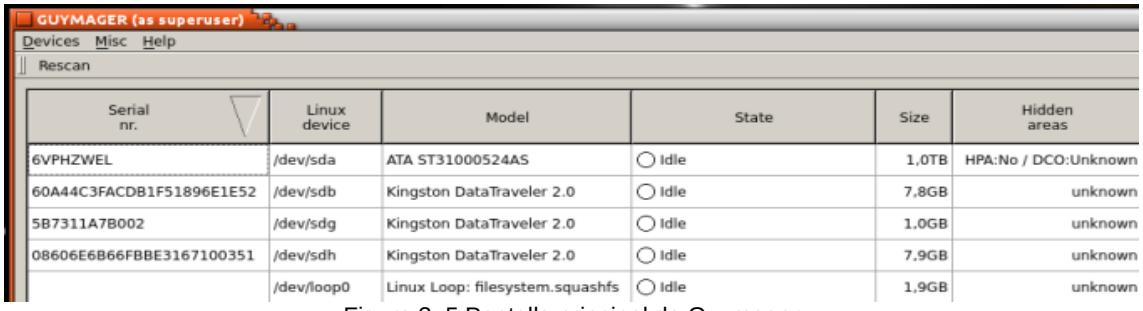


Figura 3. 3 Selección de Boot Live System

La pantalla principal de CAINE se muestra en la figura 3.4.

Figura 3. 4 Pantalla principal de CAINE

3) Para iniciar la clonación se abrió Guymager, se identificó cada uno de los dispositivos conectados como se observa en la figura 3.5:
   - ❖ Dispositivo de autoarranque CAINE: 60A44C3FACDB1F51896E1E52 → /dev/sdb
   - ❖ **Dispositivo evidencia: 5B7311A7B002 → /dev/sdg**
   - ❖ **Dispositivo para clonación: 08606E6B66FBBE3167100351 → /dev/sdh**



Serial nr.	Linux device	Model	State	Size	Hidden areas
6VPHZWEL	/dev/sda	ATA ST31000524AS	Idle	1,0TB	HPA:No / DCO:Unknown
60A44C3FACDB1F51896E1E52	/dev/sdb	Kingston DataTraveler 2.0	Idle	7,8GB	unknown
5B7311A7B002	/dev/sdg	Kingston DataTraveler 2.0	Idle	1,0GB	unknown
08606E6B66FBBE3167100351	/dev/sdh	Kingston DataTraveler 2.0	Idle	7,9GB	unknown
	/dev/loop0	Linux Loop: filesystem.squashfs	Idle	1,9GB	unknown

Figura 3. 5 Pantalla principal de Guymager

4) Se realizó el cálculo de hash del dispositivo evidencia a través de una interfaz de línea de comandos, con los comandos que se muestran en la tabla 3.2.

Cálculo de hash	
Comando	Objetivo
sudo md5sum /dev/sdg	Genera un número de 32 dígitos hexadecimal único del dispositivo

sudo sha1sum /dev/sdg	Genera un número de 40 dígitos hexadecimal único del dispositivo
sudo sha256sum /dev/sdg	Genera un número de 64 dígitos hexadecimal único del dispositivo

Tabla 3. 2 Comandos para el cálculo de hash

5) Un punto importante es que el dispositivo evidencia **/dev/sdg1** se asignó como sólo de lectura **(READ-ONLY)**, con el objetivo de que no se realice ninguna modificación en el dispositivo, ver figura 3.6.

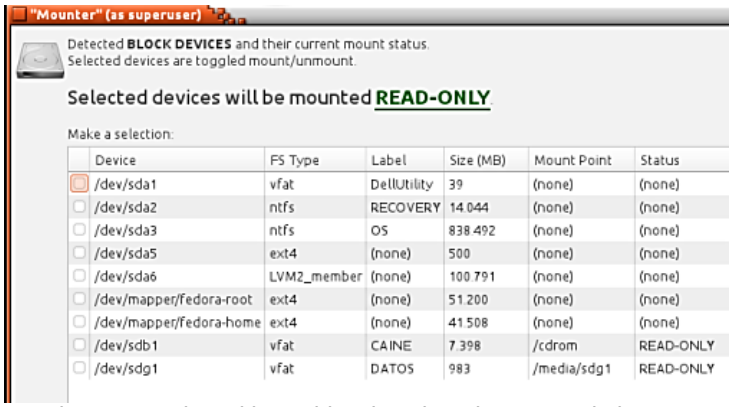


Figura 3. 6 Dispositivo evidencia asignado como solo lectura

6) Por otro lado, el dispositivo para clonación **/dev/sdh** se intentó asignar con permiso de escritura **(WRITEABLE)**, en este caso **no se logró porque no se reconoce como dispositivo ya que no contiene ningún formato**, como se observa en la figura 3.7.

Figura 3. 7 Dispositivo para clonación

7) Se regresó a la interfaz de Guymager, se seleccionó el dispositivo evidencia y en el menú secundario mostró las opciones **Acquire image** y **Clone device**, en este caso se eligió la segunda opción ver figura 3.8.

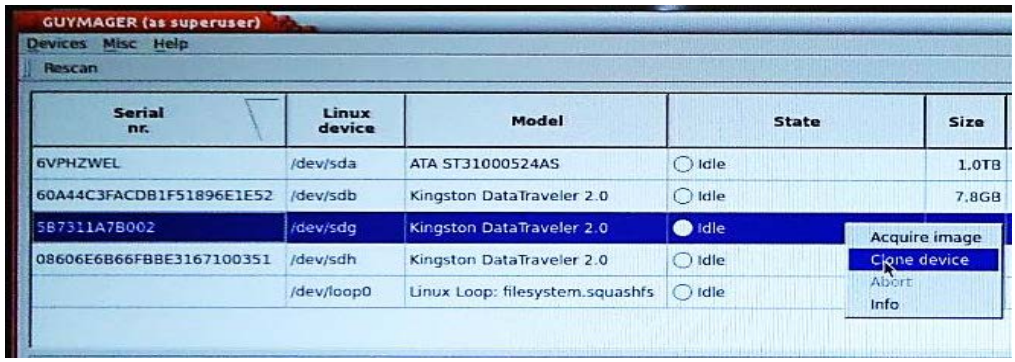


Figura 3. 8 Identificar dispositivo y seleccionar clonación de dispositivo

8) Se abrió una nueva ventana en la cual se especificaron los siguientes campos: dispositivo destino **(Destination)**, directorio de información **(Info directory)**, nombre del archivo de información **(Info filename),** por último el cálculo y verificación de hash **(Hash calculation/verification)** ver figura 3.9.

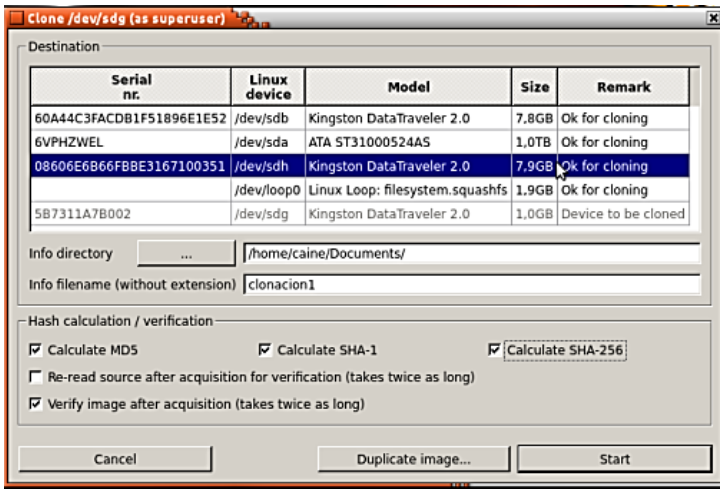


Figura 3. 9 Datos ingresados para el proceso de clonación

9) Se eligió la opción **Start** (figura 3.10) y comenzó el proceso. Por otro lado, al finalizar el proceso se mostró información sobre el tiempo de duración del proceso, incluyendo los datos que fueron asignados anteriormente, ver figura 3.11.

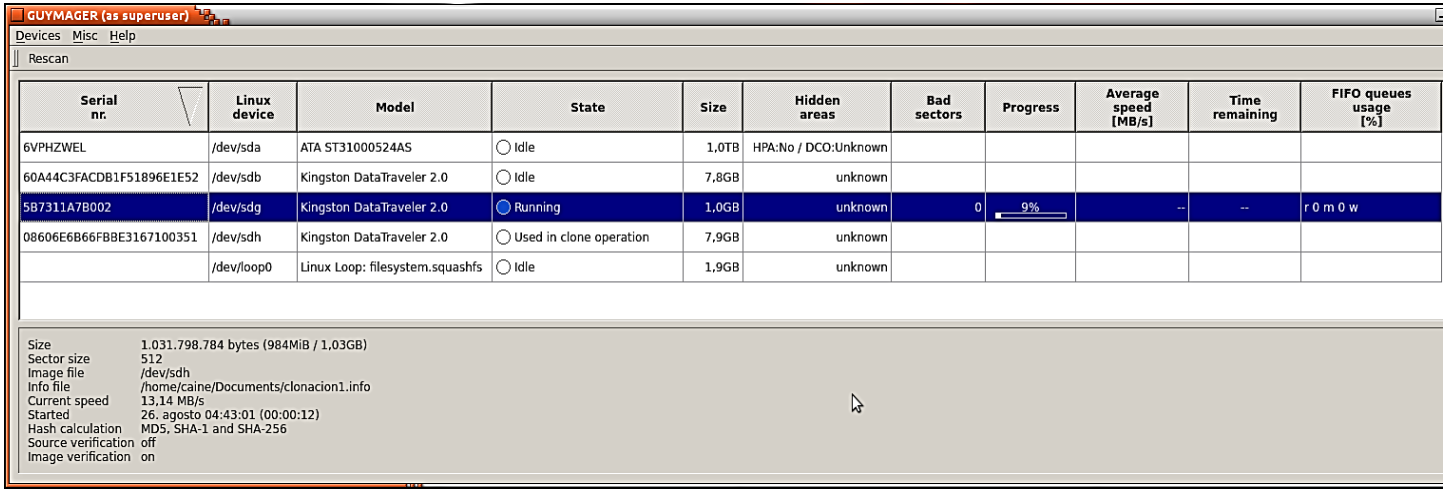


Figura 3. 10 Inicio del proceso de clonación del dispositivo evidencia

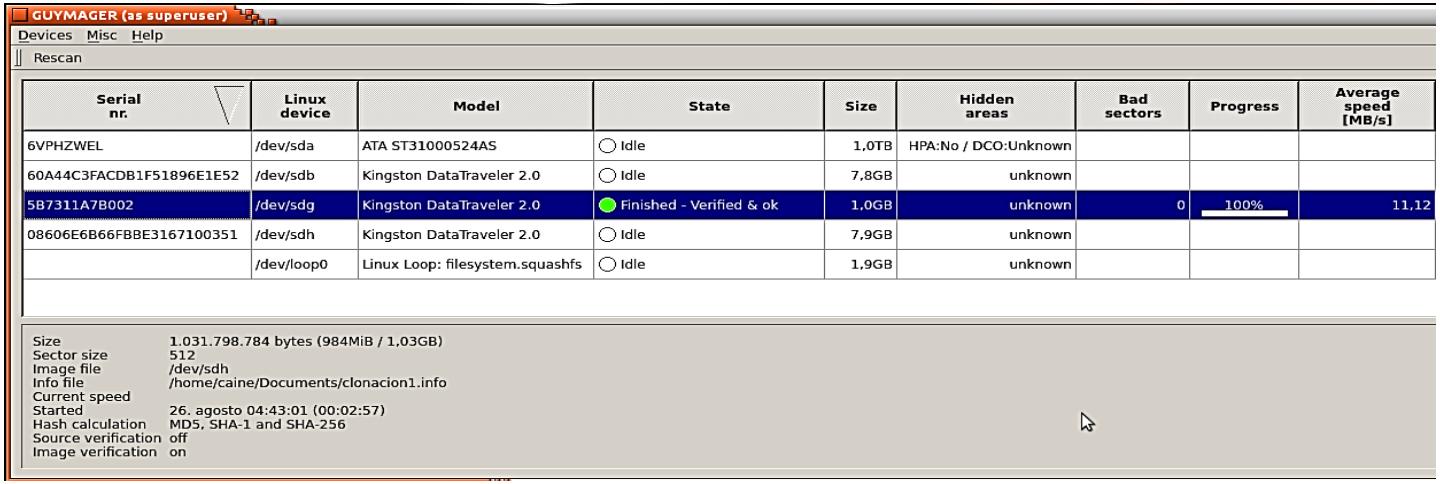
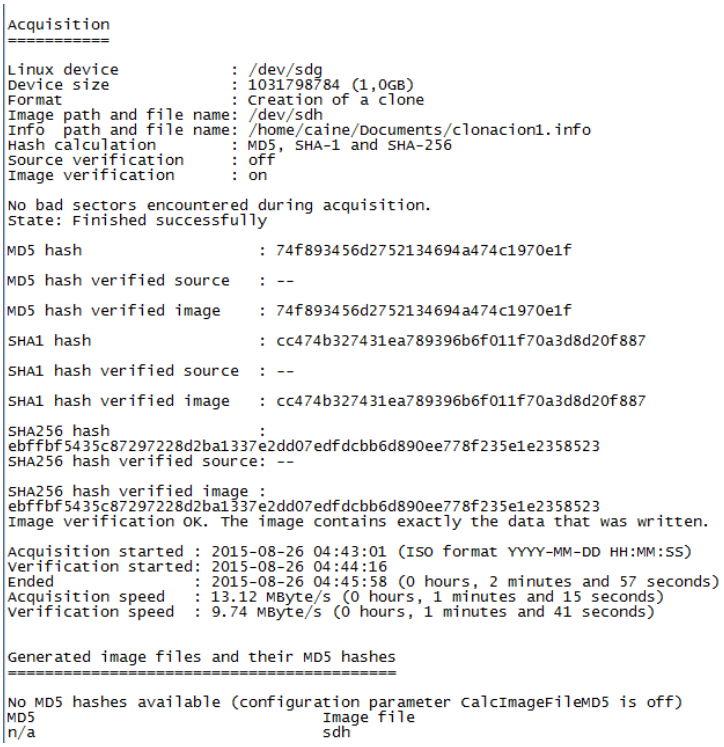


Figura 3. 11 Finalización del proceso de clonación del dispositivo evidencia

10) Justo cuando se generó la clonación también se creó un archivo llamado clonacion.info que contiene información acerca del proceso de clonación, tal como el dispositivo evidencia (/dev/sdg) y dispositivo de clonación en Linux (/dev/sdh), el hash del dispositivo de clonación, por mencionar algunos, ver figura 3.12.

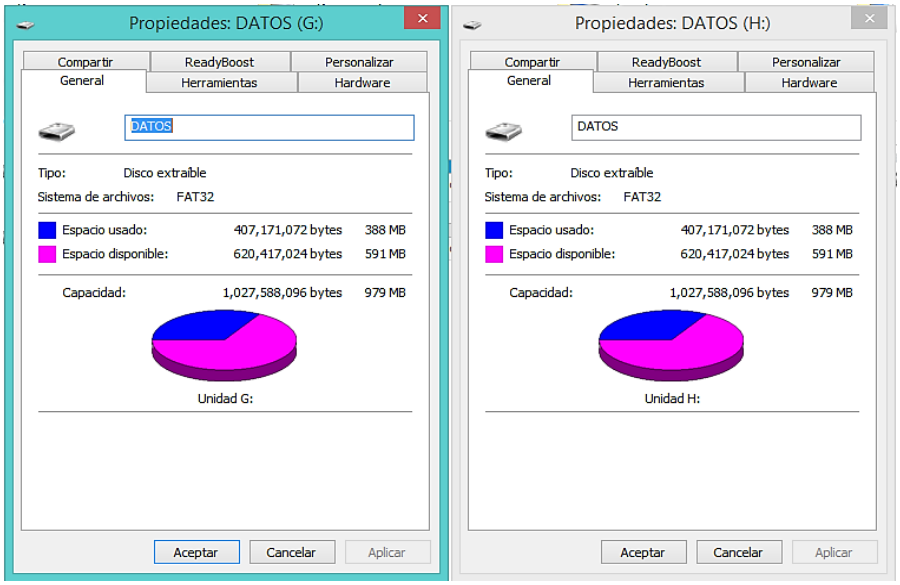


```
Acquisition
===========

Linux device            : /dev/sdg
Device size             : 1031798784 (1,0GB)
Format                  : Creation of a clone
Image path and file name: /dev/sdh
Info  path and file name: /home/caine/Documents/clonacion1.info
Hash calculation        : MD5, SHA-1 and SHA-256
Source verification     : off
Image verification      : on

No bad sectors encountered during acquisition.
State: Finished successfully

MD5 hash                    : 74f893456d2752134694a474c1970e1f

MD5 hash verified source    : --

MD5 hash verified image     : 74f893456d2752134694a474c1970e1f

SHA1 hash                   : cc474b327431ea789396b6f011f70a3d8d20f887

SHA1 hash verified source   : --

SHA1 hash verified image    : cc474b327431ea789396b6f011f70a3d8d20f887

SHA256 hash                 :
ebffbf5435c87297228d2ba1337e2dd07edfdcbb6d890ee778f235e1e2358523
SHA256 hash verified source: --

SHA256 hash verified image :
ebffbf5435c87297228d2ba1337e2dd07edfdcbb6d890ee778f235e1e2358523
Image verification OK. The image contains exactly the data that was written.

Acquisition started : 2015-08-26 04:43:01 (ISO format YYYY-MM-DD HH:MM:SS)
Verification started: 2015-08-26 04:44:16
Ended               : 2015-08-26 04:45:58 (0 hours, 2 minutes and 57 seconds)
Acquisition speed   : 13.12 MByte/s (0 hours, 1 minutes and 15 seconds)
Verification speed  : 9.74 MByte/s (0 hours, 1 minutes and 41 seconds)


Generated image files and their MD5 hashes
==========================================

No MD5 hashes available (configuration parameter CalcImageFileMD5 is off)
MD5                                 Image file
n/a                                 sdh
```

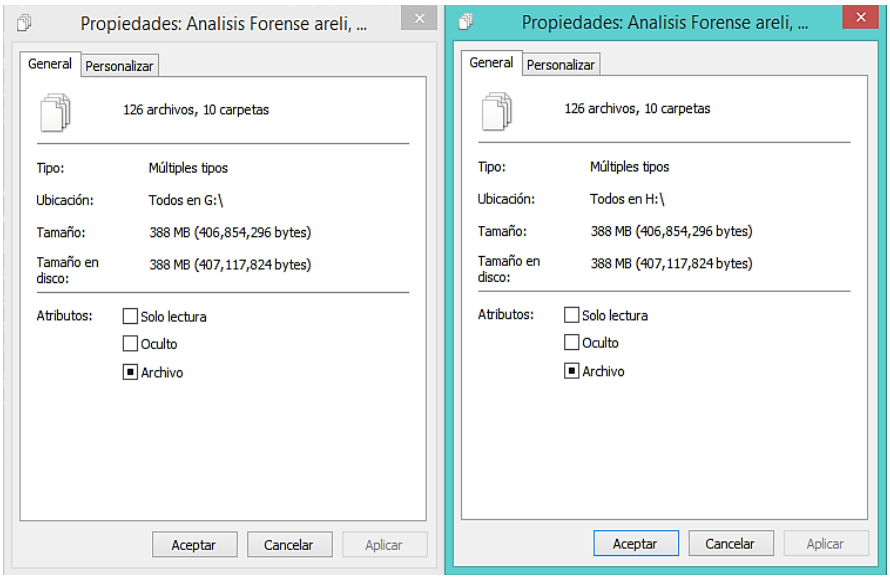
Figura 3. 12 Hash de la clonación

Se comprobó que el dispositivo evidencia y el dispositivo de clonación son iguales, al revisar la cantidad de almacenamiento usado de ambos dispositivos, ver figuras 3.13 y 3.14.

Figura 3. 13 DATOS (G:) es el dispositivo clonado y DATOS (H:) es el dispositivo evidencia



(a) Cantidad de almacenamiento



(b) Número de archivos

Figura 3. 14 Dispositivo clonado (G:) y dispositivo evidencia (H:)

11) Para la recuperación de archivos se abrió Photorec. En la primera ventana se mostró una lista con todos los dispositivos conectados a la computadora, ver figura 3.15.

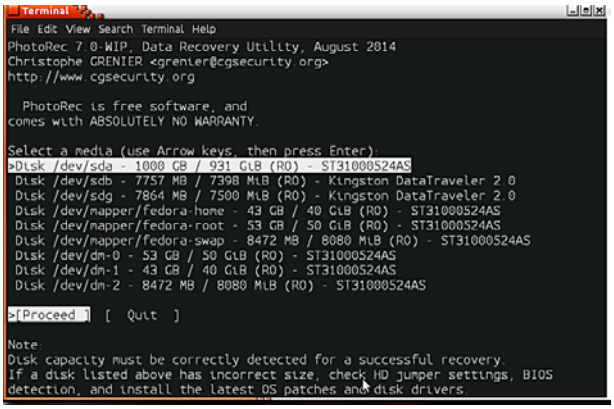


Figura 3. 15 Photorec

12) Se eligió el dispositivo clonado: **Disk /dev/sdg – 7864 MB/7500 MiB (RO) – Kingston Data Traveler 2.0** y se presionó **enter** (considerar que estaba seleccionada la opción [Proceed]), como se muestra en la figura 3.16.

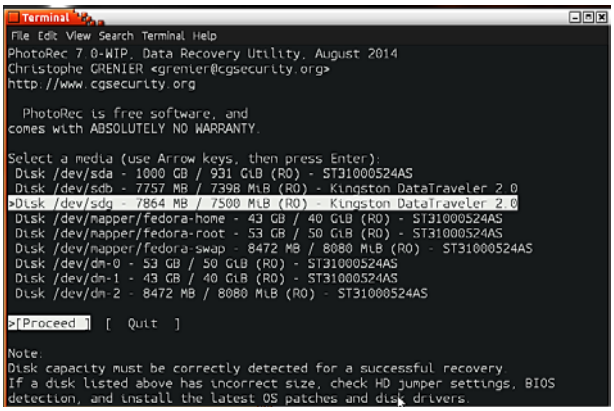


Figura 3. 16 Selección de dispositivo clonado

13) En el siguiente paso se seleccionó el tipo de partición del dispositivo clonado: **FAT32**, se considera que es la partición del dispositivo evidencia ver figura 3.17.

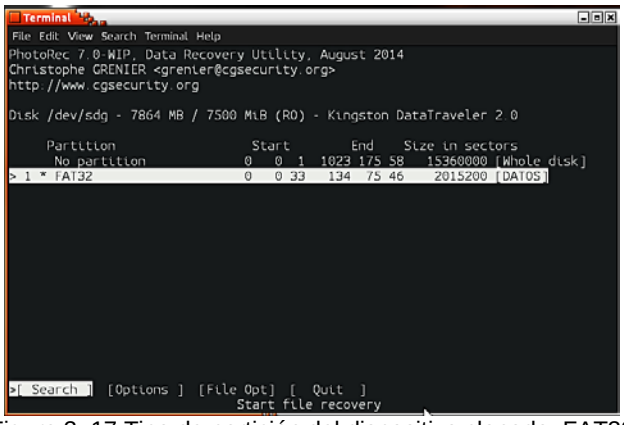


Figura 3. 17 Tipo de partición del dispositivo clonado: FAT32

14) Para que Photorec recupere los archivos perdidos se indicó el tipo de sistema de archivos del dispositivo clonado: **Other (FAT)**, ver figura 3.18.

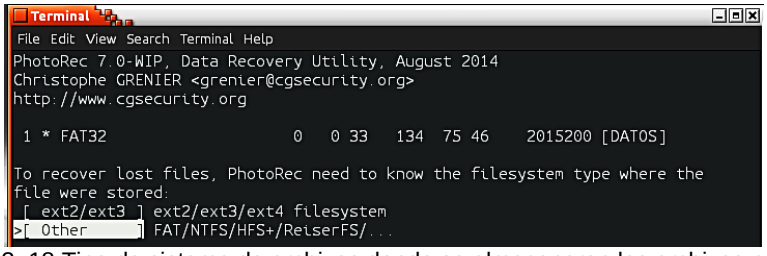


Figura 3. 18 Tipo de sistema de archivos donde se almacenaron los archivos perdidos

15) A continuación se eligió el espacio de almacenamiento que sería analizado, en este caso se seleccionó **Whole** (completo) como se observa en la figura 3.19.

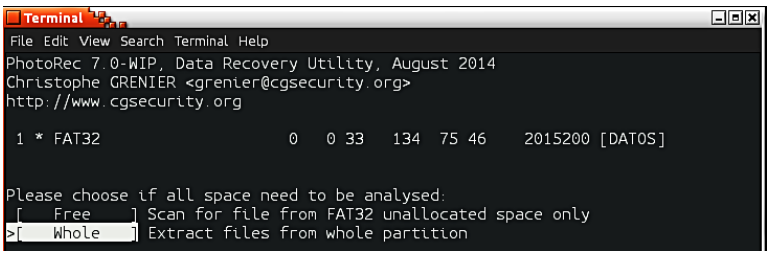


Figura 3. 19 Espacio que será analizado

16) En el último paso se seleccionó el destino donde se guardarían los archivos recuperados, se eligió la carpeta **Downloads** y se presionó la **tecla C**, ver figura 3.20.

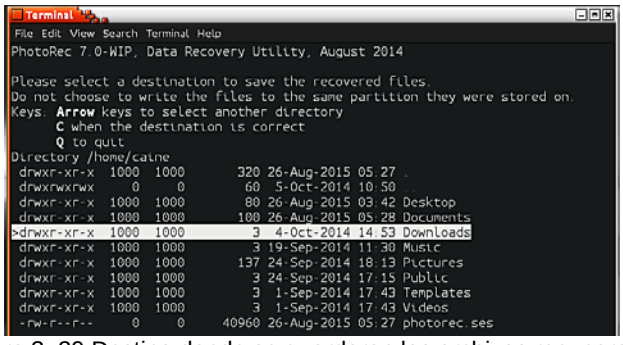
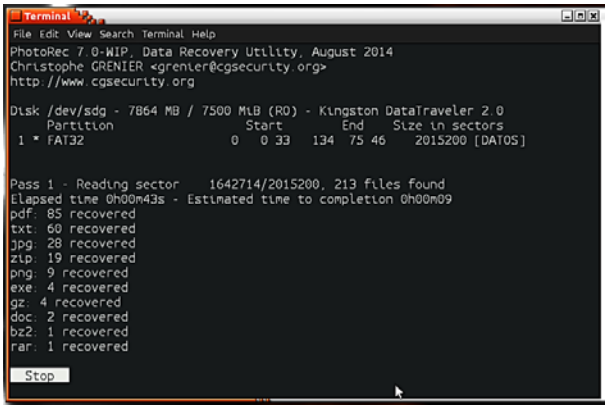
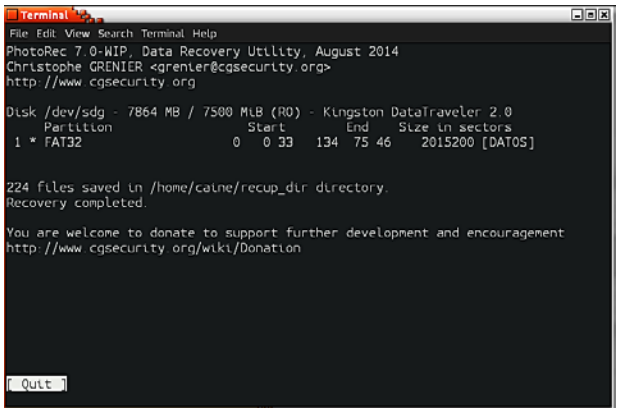


Figura 3. 20 Destino donde se guardaran los archivos recuperados

Inició el proceso y tardó unos minutos, para salir de Photorec se presionó la opción **enter**, ver figura 3.21.



(a)



(b)

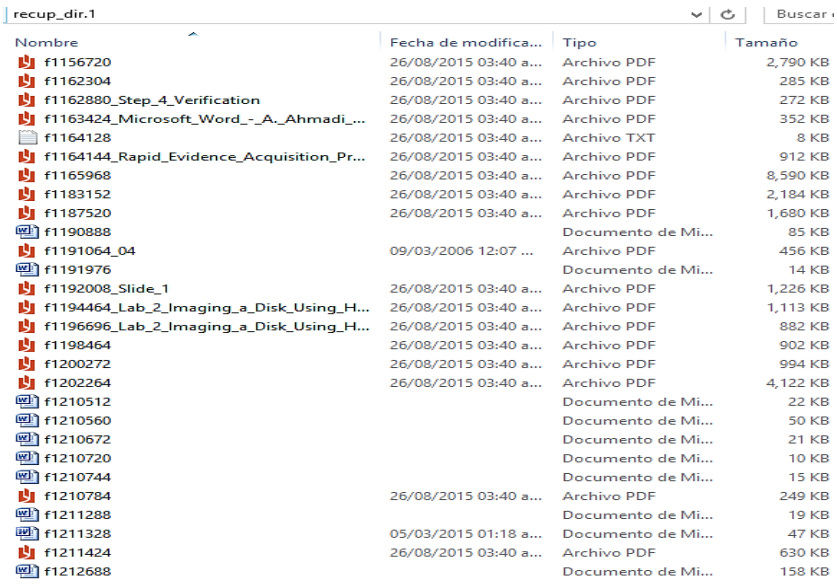
Figura 3. 21 Proceso de recuperación

17) Al término del proceso se creó una carpeta llamada **recup_dir.1**, en la cual se localizan todos los archivos recuperados. En la tabla 3.3 se indica el número de archivos recuperados.

Tipo de archivo	Número de archivos borrados	Número de archivos recuperados	Archivos recuperados legibles
Archivo por lotes de Windows (.bat)	0	1	0
Archivo	0	1	0
Docx	1	32	31
Jpeg	26	56	56
Exe	0	3	2
Pdf	3	85	85
Txt	0	59	3
Winrar	1	6	1
XML	0	1	0
Png	0	9	9
Total	31	253	187

Tabla 3. 3 Lista de archivos recuperados por Photorec

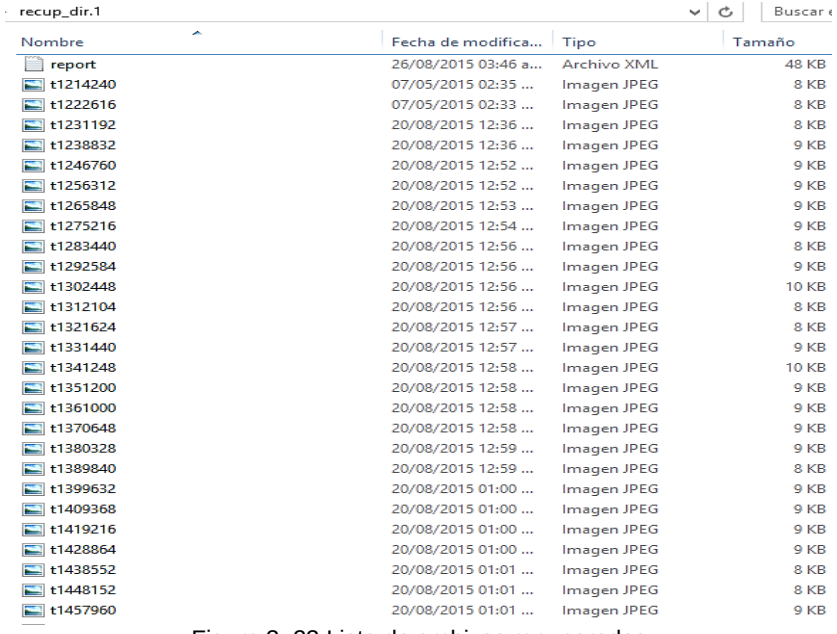
La figura 3.22 y figura 3.23 muestran algunos de los archivos recuperados.



recup_dir.1

Nombre	Fecha de modifica...	Tipo	Tamaño
f1156720	26/08/2015 03:40 a...	Archivo PDF	2,790 KB
f1162304	26/08/2015 03:40 a...	Archivo PDF	285 KB
f1162880_Step_4_Verification	26/08/2015 03:40 a...	Archivo PDF	272 KB
f1163424_Microsoft_Word_-_A._Ahmadi_...	26/08/2015 03:40 a...	Archivo PDF	352 KB
f1164128	26/08/2015 03:40 a...	Archivo TXT	8 KB
f1164144_Rapid_Evidence_Acquisition_Pr...	26/08/2015 03:40 a...	Archivo PDF	912 KB
f1165968	26/08/2015 03:40 a...	Archivo PDF	8,590 KB
f1183152	26/08/2015 03:40 a...	Archivo PDF	2,184 KB
f1187520	26/08/2015 03:40 a...	Archivo PDF	1,680 KB
f1190888		Documento de Mi...	85 KB
f1191064_04	09/03/2006 12:07 ...	Archivo PDF	456 KB
f1191976		Documento de Mi...	14 KB
f1192008_Slide_1	26/08/2015 03:40 a...	Archivo PDF	1,226 KB
f1194464_Lab_2_Imaging_a_Disk_Using_H...	26/08/2015 03:40 a...	Archivo PDF	1,113 KB
f1196696_Lab_2_Imaging_a_Disk_Using_H...	26/08/2015 03:40 a...	Archivo PDF	882 KB
f1198464	26/08/2015 03:40 a...	Archivo PDF	902 KB
f1200272	26/08/2015 03:40 a...	Archivo PDF	994 KB
f1202264	26/08/2015 03:40 a...	Archivo PDF	4,122 KB
f1210512		Documento de Mi...	22 KB
f1210560		Documento de Mi...	50 KB
f1210672		Documento de Mi...	21 KB
f1210720		Documento de Mi...	10 KB
f1210744		Documento de Mi...	15 KB
f1210784	26/08/2015 03:40 a...	Archivo PDF	249 KB
f1211288		Documento de Mi...	19 KB
f1211328	05/03/2015 01:18 a...	Documento de Mi...	47 KB
f1211424	26/08/2015 03:40 a...	Archivo PDF	630 KB
f1212688		Documento de Mi...	158 KB

Figura 3. 22 Lista de archivos recuperados



recup_dir.1

Nombre	Fecha de modifica...	Tipo	Tamaño
report	26/08/2015 03:46 a...	Archivo XML	48 KB
t1214240	07/05/2015 02:35 ...	Imagen JPEG	8 KB
t1222616	07/05/2015 02:33 ...	Imagen JPEG	8 KB
t1231192	20/08/2015 12:36 ...	Imagen JPEG	8 KB
t1238832	20/08/2015 12:36 ...	Imagen JPEG	9 KB
t1246760	20/08/2015 12:52 ...	Imagen JPEG	9 KB
t1256312	20/08/2015 12:52 ...	Imagen JPEG	9 KB
t1265848	20/08/2015 12:53 ...	Imagen JPEG	9 KB
t1275216	20/08/2015 12:54 ...	Imagen JPEG	9 KB
t1283440	20/08/2015 12:56 ...	Imagen JPEG	8 KB
t1292584	20/08/2015 12:56 ...	Imagen JPEG	9 KB
t1302448	20/08/2015 12:56 ...	Imagen JPEG	10 KB
t1312104	20/08/2015 12:56 ...	Imagen JPEG	8 KB
t1321624	20/08/2015 12:57 ...	Imagen JPEG	8 KB
t1331440	20/08/2015 12:57 ...	Imagen JPEG	9 KB
t1341248	20/08/2015 12:58 ...	Imagen JPEG	10 KB
t1351200	20/08/2015 12:58 ...	Imagen JPEG	9 KB
t1361000	20/08/2015 12:58 ...	Imagen JPEG	9 KB
t1370648	20/08/2015 12:58 ...	Imagen JPEG	9 KB
t1380328	20/08/2015 12:59 ...	Imagen JPEG	9 KB
t1389840	20/08/2015 12:59 ...	Imagen JPEG	8 KB
t1399632	20/08/2015 01:00 ...	Imagen JPEG	9 KB
t1409368	20/08/2015 01:00 ...	Imagen JPEG	9 KB
t1419216	20/08/2015 01:00 ...	Imagen JPEG	9 KB
t1428864	20/08/2015 01:00 ...	Imagen JPEG	9 KB
t1438552	20/08/2015 01:01 ...	Imagen JPEG	8 KB
t1448152	20/08/2015 01:01 ...	Imagen JPEG	8 KB
t1457960	20/08/2015 01:01 ...	Imagen JPEG	9 KB

Figura 3. 23 Lista de archivos recuperados

3.1.3 Guymager y Autopsy

Anteriormente se mencionó que Guymager ofrece la opción de adquirir una imagen en dos formatos diferentes: **DD** y **E01**, mientras que Autopsy es una interfaz gráfica que admite la recuperación de archivos, busca metadatos, crea líneas de tiempo, búsqueda de palabra clave, cálculo de hash, entre otros. Se debe considerar que el dispositivo evidencia es el mismo descrito anteriormente (Capítulo 3.1.1).

A continuación se describe el proceso completo para llevar a cabo la adquisición de imagen del dispositivo evidencia con formato **dd** y su correspondiente recuperación de archivos. Otro punto importante es que se omite el proceso de arranque de Caine, y los pasos del 1 al 6 del apartado anterior debido a que son los mismos, por lo que se describen a partir del proceso de adquisición.

1) Se regresó a la interfaz de Guymager, en el menú secundario del dispositivo evidencia seleccionado se eligió la opción **Acquire image**, ver figura 3.24.

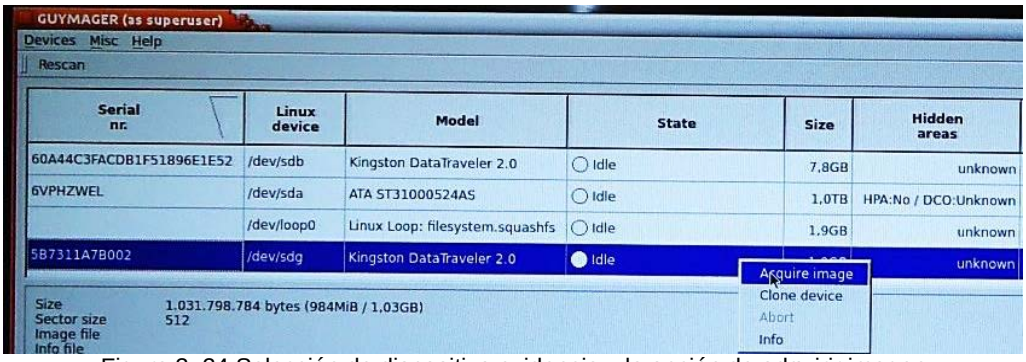


Figura 3. 24 Selección de dispositivo evidencia y la opción de adquirir imagen

2) Se mostró una nueva ventana como la figura 3.25, en la cual se especificaron los siguientes campos: **File type (dd)**, I**mage directory**, **Image filename**, **Hash calculation/verification (MD5, SHA-1 y SHA-256)** y **Verify image after adquisition** (esta opción se refiere a que verifica el hash de la imagen después del proceso de adquisición).

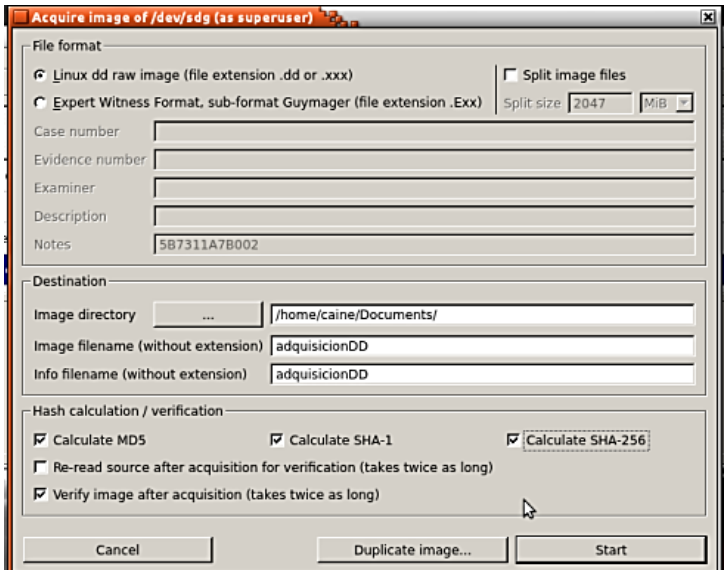


Figura 3. 25 Datos ingresados para el proceso

3) Se seleccionó la opción **Start** y comenzó el proceso de adquisición de imagen (figura 3.26). Por otro lado, al terminar el proceso se mostró información sobre el tiempo de duración de dicho proceso, conservando los datos que fueron asignados previamente, ver figura 3.27.

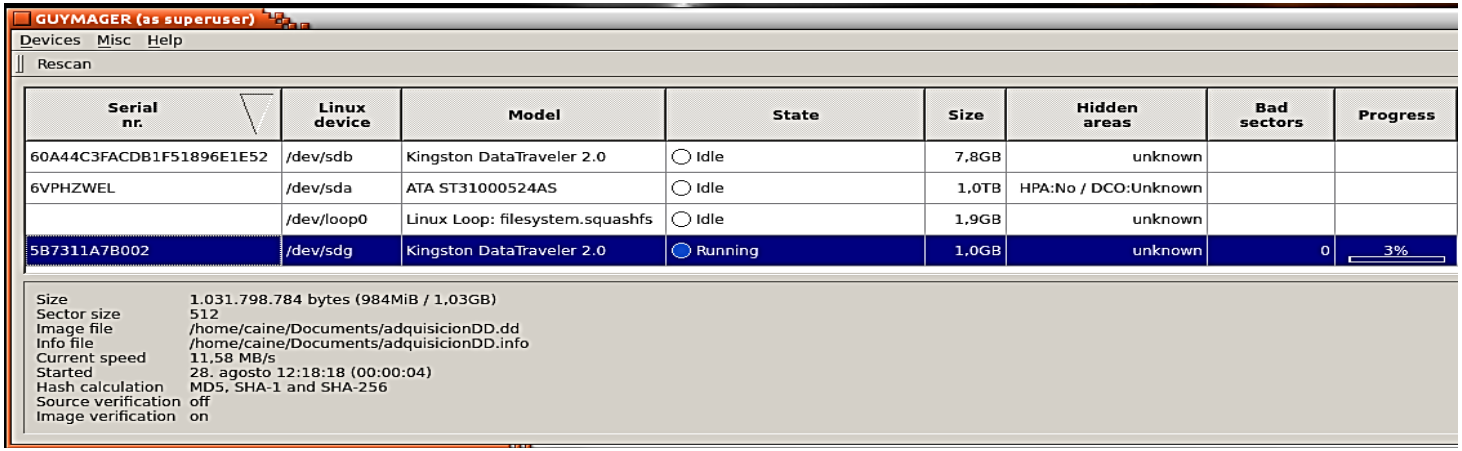


Figura 3. 26 Inicio del proceso de adquisición de imagen del dispositivo evidencia

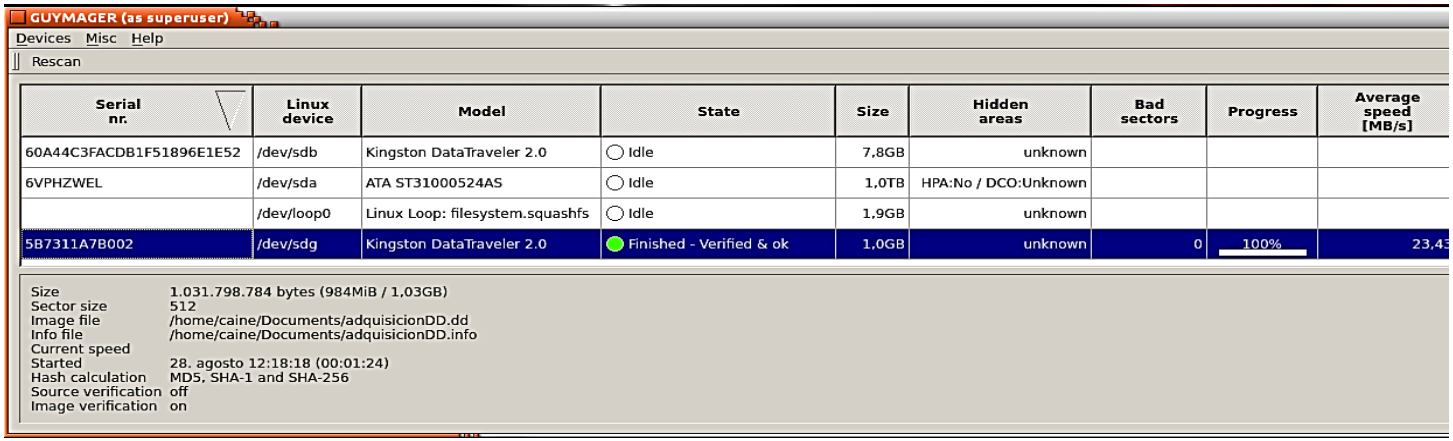


Figura 3. 27 Final del proceso de adquisición de imagen del dispositivo evidencia

4) Durante el proceso de adquisición se creó la imagen llamada **adquisicionDD.dd** y un archivo llamado **adquisicionDD.info** (figura 3.28), este último incluye la identificación (sdg) y tamaño del dispositivo evidencia, el formato de la imagen, nombre del archivo y ruta de la imagen, el hash de la adquisición, por mencionar algunos, ver figura 3.29. Se comprobó que el hash de la terminal calculado anteriormente y el hash obtenido en el proceso de adquisición son iguales, lo que significa que la adquisición no ha sido alterada.

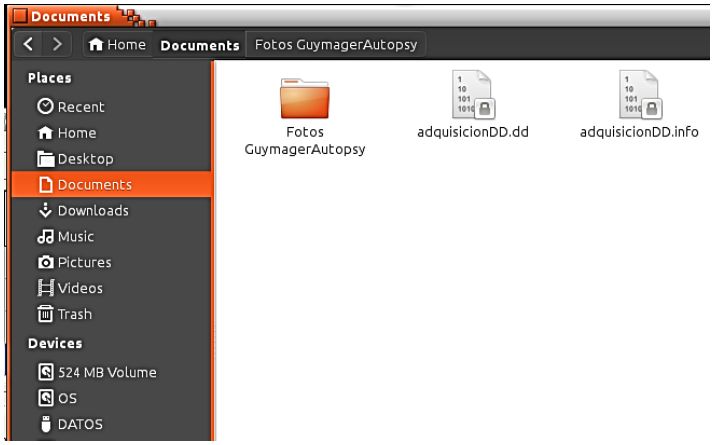


Figura 3. 28 Archivos adquisicionDD.dd y adquisicionDD.info

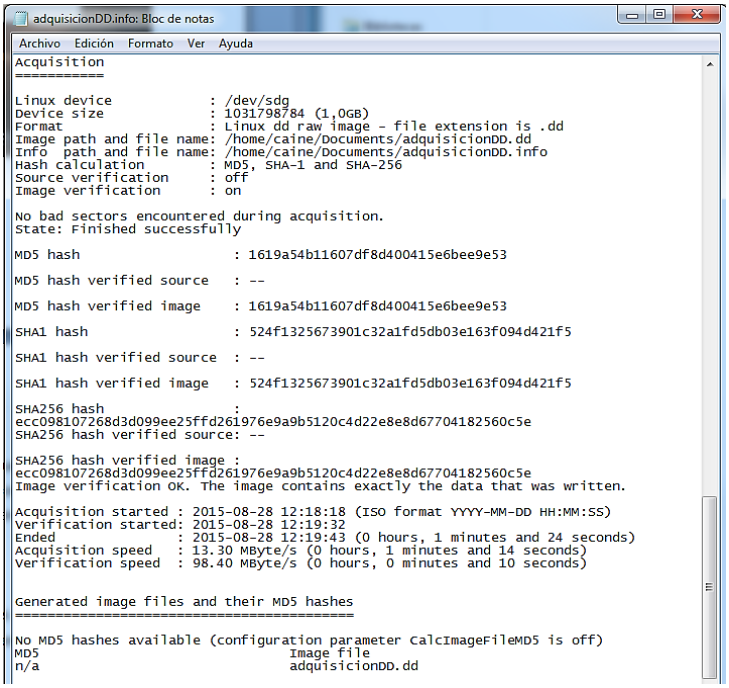


Figura 3. 29 Valor hash de la adquisición de imagen

5) Para proceder a la recuperación de archivos se inició Autopsy. En la primera ventana, se mostró una interfaz gráfica de la cual se eligió la opción **New Case** (figura 3.30).

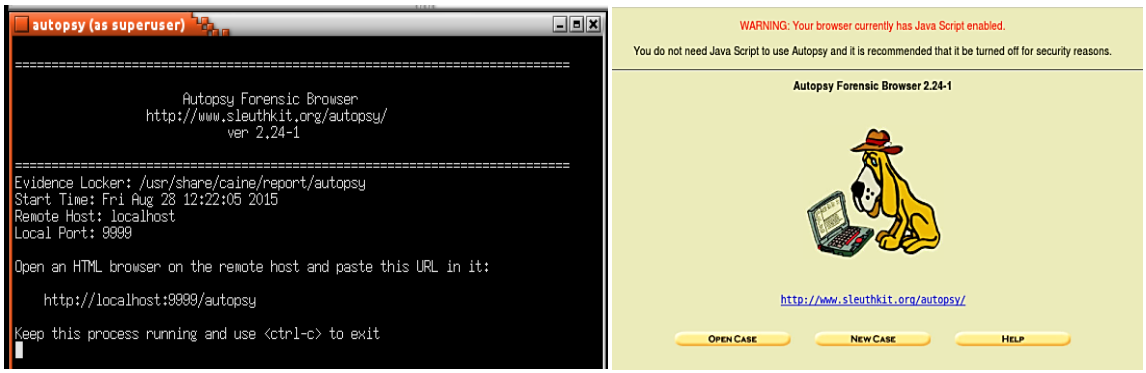


Figura 3. 30 Autopsy

6) Lo siguiente fue el ingreso de información para el nuevo caso, tal como el nombre del caso (**Case name**), su descripción (**Description**) y el nombre del investigador (**Investigator Names**), este último es opcional, ver figura 3.31. A continuación se eligió la opción **New Case**.

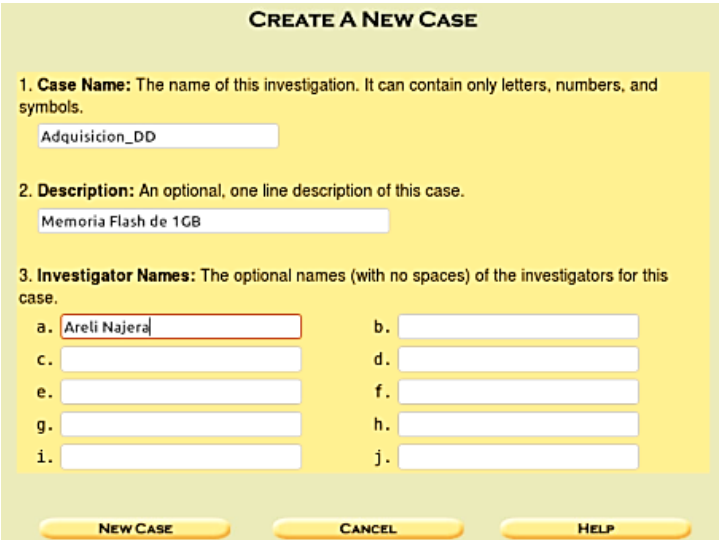


Figura 3. 31 Datos ingresados para un nuevo caso

7) En la siguiente ventana se seleccionó la opción **Add Host** (figura 3.32). Se mostró otra ventana donde se ingresaron datos de la computadora a usar como son: **Host**

Name, **Description** y **Time zone**, nuevamente se seleccionó la opción **Add host**, como se muestra en la figura 3.33.

Figura 3. 32 Agregar host

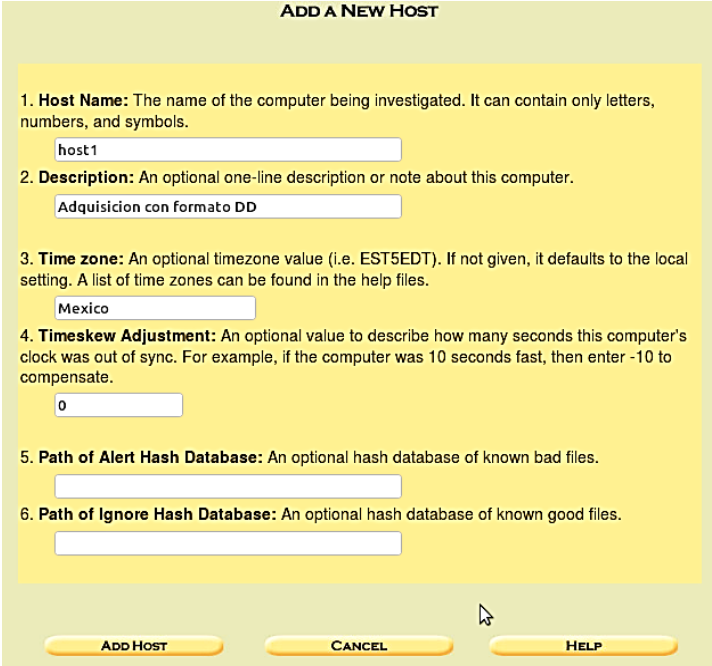


Figura 3. 33 Datos ingresados para agregar un nuevo host

8) Se eligió la opción **Add Image** ver figura 3.34. Se presentó una ventana con varias opciones como **Image Integrity**, **View Notes**, entre otras, y se seleccionó la opción para agregar un archivo de imagen (**Add Image File**), figura 3.35.

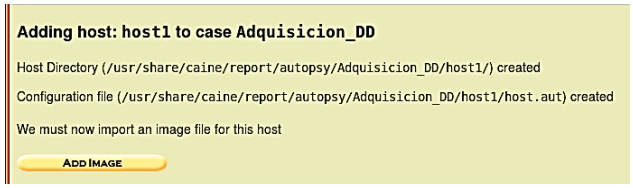


Figura 3. 34 Host agregado y agregar imagen

Figura 3. 35 Selección de agregar archivo de imagen

9) Se ingresó información de la ubicación del archivo imagen en la opción **Location**, en el tipo de archivo de imagen se seleccionó la opción **Disk** ya que en él se encuentra contenida la imagen, en la opción **Import Method** se eligió la opción **Symlink** aunque también se puede elegir la opción **Copy** y la última opción **Move** podría dañar la imagen, por último se presionó la opción **Next**, ver figura 3.36. En la siguiente ventana se omitió el valor hash de la imagen ya que posteriormente se hará el cálculo; con respecto a los detalles del sistema de archivos en **Mount Point** se eligió la unidad **C:** y el sistema de archivo **FAT32** que es el que contiene la imagen, al final se eligió la opción **Add** (figura 3.37). En la última ventana se mostró la información previamente agregada por lo que se seleccionó la opción **ok**, ver figura 3.38.

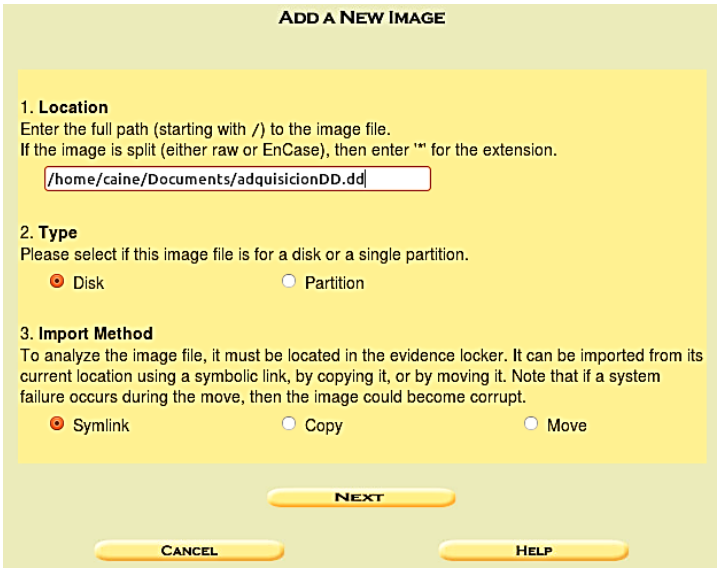


Figura 3. 36 Ingresar ubicación de la imagen

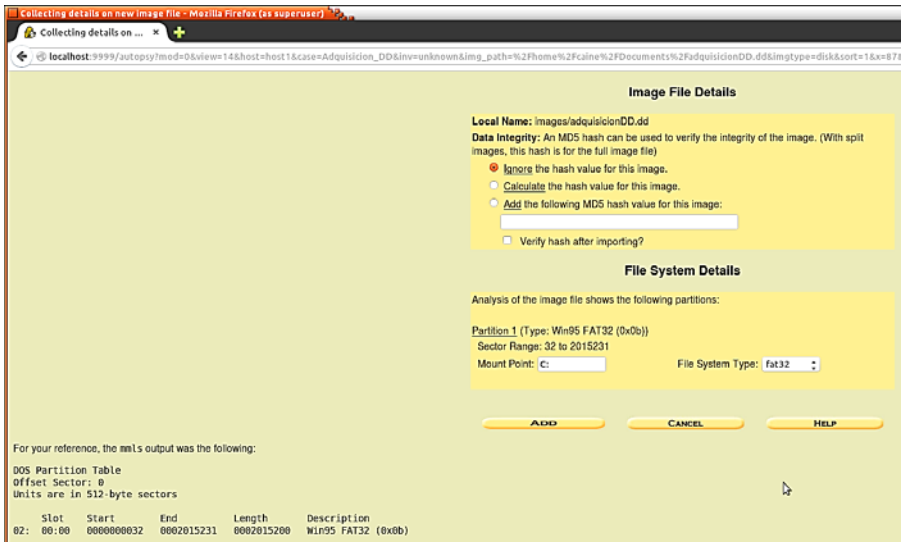


Figura 3. 37 Seleccionar Agregar

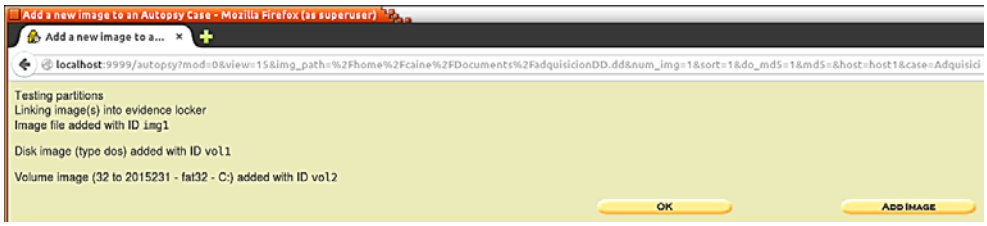


Figura 3. 38 Archivo de imagen agregado

10) Dado que anteriormente se agregó el archivo de imagen, se eligió el volumen para analizar **C: /**, en este caso se consideró el tipo de sistema de archivo que contenía el dispositivo evidencia (fat32), ver figura 3.39. Se calculó el hash de la imagen con la opción **Image Integrity**, con lo que se comprobó que la imagen agregada no fue modificada, haciendo la comparación con el hash calculado anteriormente (figura 3.40). Por último se presionó la opción **Close** (figura 3.41).

Figura 3. 39 Seleccionar volumen para analizar

Figura 3. 40 Cálculo del hash de la imagen

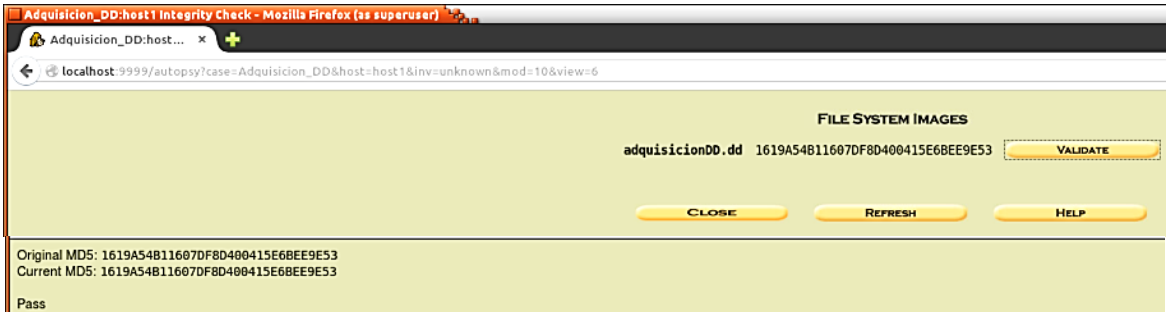


Figura 3. 41 Verificación de hash

11) La siguiente ventana mostró un menú con varias opciones para realizar el análisis, ver figura 3.42. Para este caso en particular se seleccionó la opción **File Analysis**, ver figura 3.43, en la que se observa una lista del contenido de la imagen.

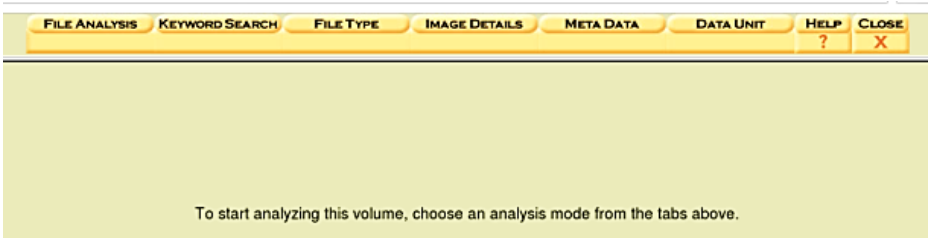


Figura 3. 42 Menú de análisis

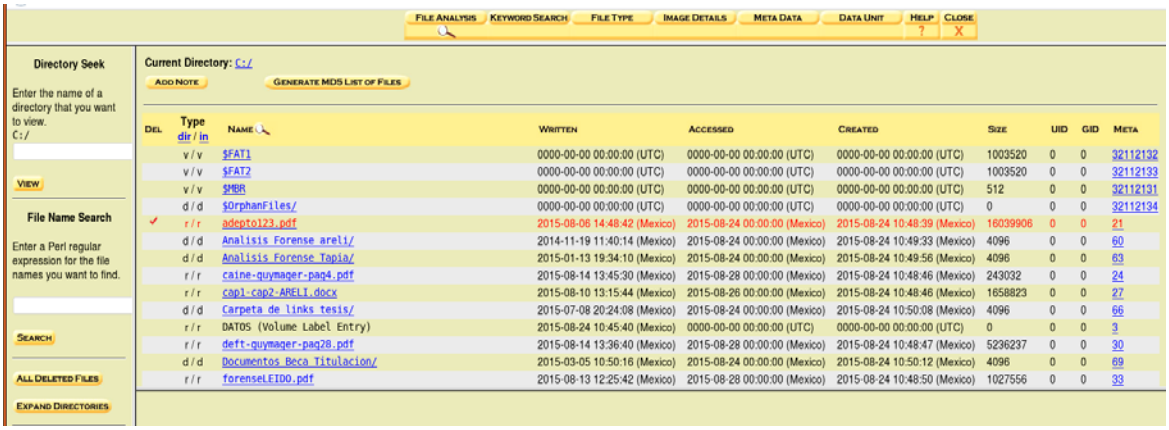


Figura 3. 43 Selección de análisis de archivo

12) En la misma ventana se seleccionó la opción **All Deleted Files**, por lo que mostró la lista de los archivos que fueron borrados intencionalmente, ver figura 3.44.

Figura 3. 44 Selección de todos los archivos eliminados

13) Para recuperar los archivos se realizó lo siguiente: se seleccionó el archivo y se buscó la opción **Export**. En la nueva ventana se eligió **Save File** y se eligió la opción **ok**. Todos los archivos borrados que se recuperaron se almacenaron en la carpeta **Downloads** por defecto, ver figura 3.45.

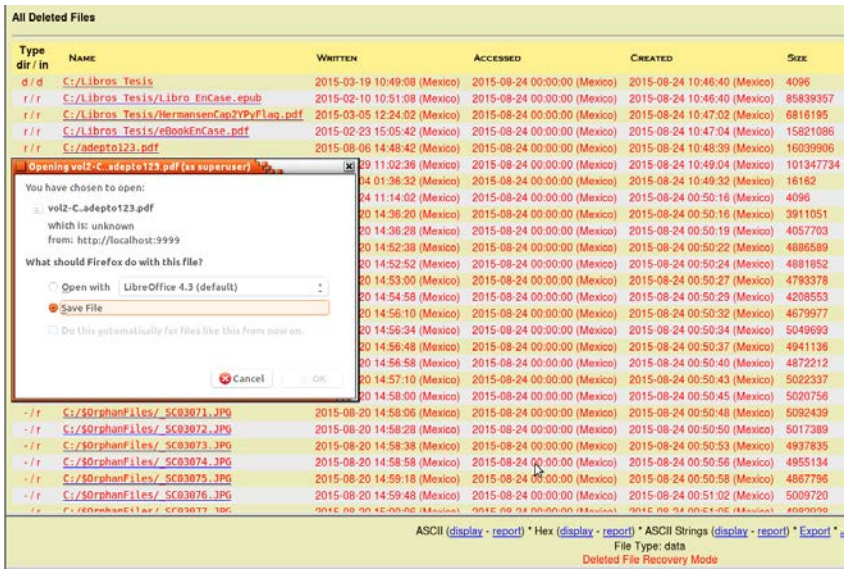


Figura 3. 45 Descarga de archivo pdf

14) Autopsy incluye la opción **File Activity Timelines** (figura 3.46) esta opción permite visualizar la lista de archivos borrados y archivos guardados en la imagen. Se eligió la opción **Create Timeline** para crear la línea de tiempo y en la siguiente ventana se presionó la opción **ok** (figura 3.47), después se seleccionó la imagen a la cual se le recopilarán los datos. Por último se eligió la opción **ok**, ver figura 3.48.

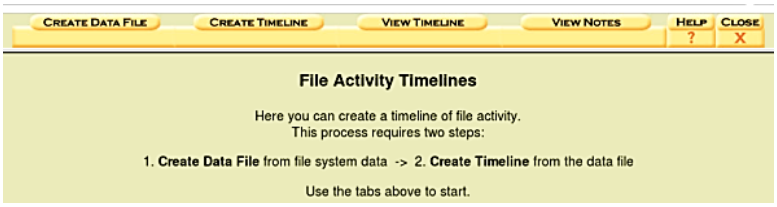


Figura 3. 46 Menú de línea de tiempo

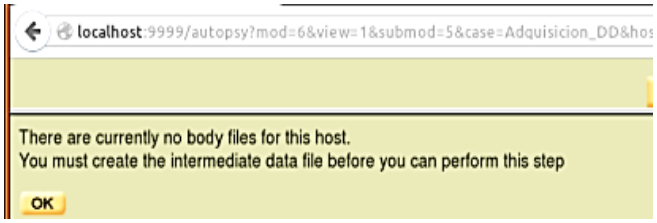


Figura 3. 47 Selección para crear línea de tiempo

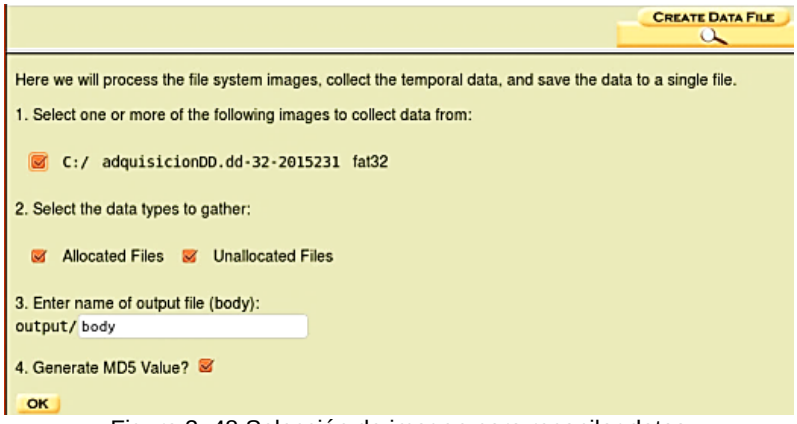


Figura 3. 48 Selección de imagen para recopilar datos

15) Después de que se agregó la imagen, el siguiente paso fue ordenar los datos en la línea de tiempo y se presionó la opción **ok**, ver figura 3.49. Por otro lado, se especificaron los siguientes campos: fecha de inicio **(starting date)**, fecha de finalización **(ending date)**, nombre del archivo y extensión que en este caso se dejó el que se mostró por defecto **(file name y output format)** y generar el valor

hash MD5 **(MD5 value)**, es importante mencionar que la extensión de la línea de tiempo está por defecto. Por último se seleccionó la opción **ok** como se muestra en la figura 3.50.

Figura 3. 49 Imagen agregada

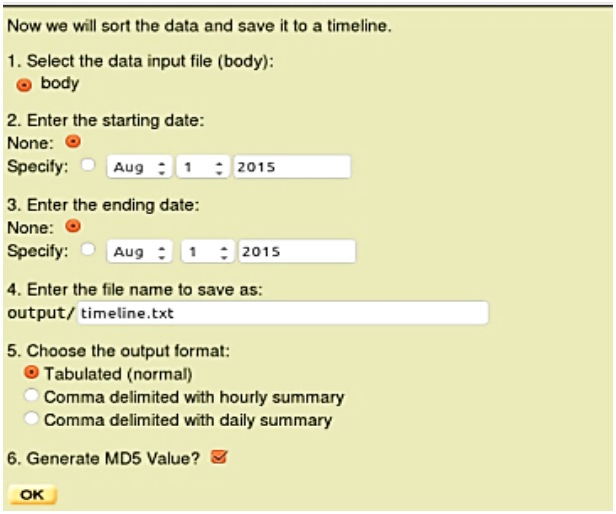


Figura 3. 50 Fecha de inicio y final de la línea de tiempo

16) A la línea de tiempo se le asignó la zona horaria que se definió anteriormente, por lo que se presionó la opción **ok**, ver figura 3.51.

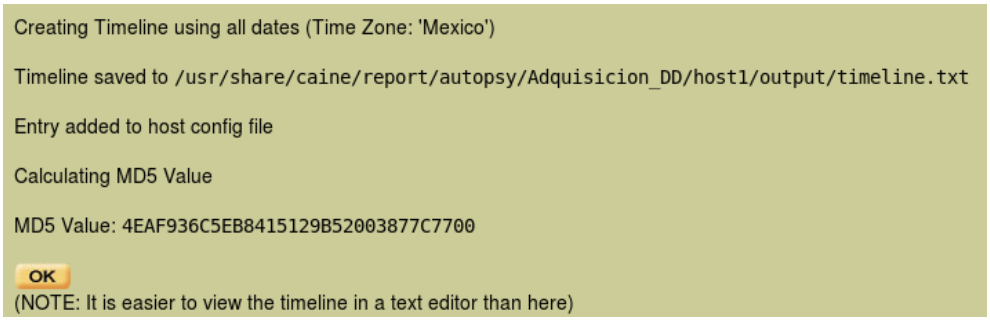
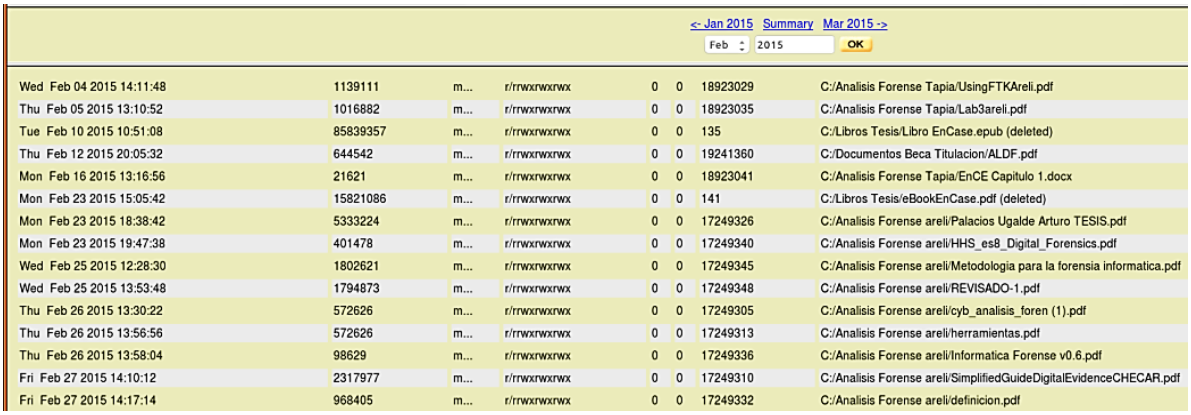


Figura 3. 51 Línea de tiempo con la zona horaria de México

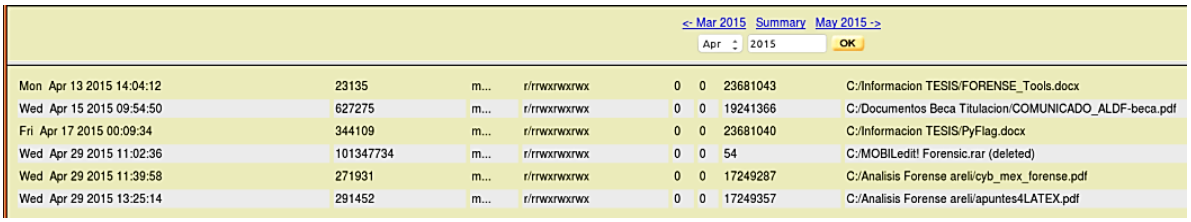
17) Otra alternativa que brinda esta herramienta es ir especificando el mes y el año que se desea visualizar, mostrando todos los archivos contenidos en la imagen tanto los que se crearon como los que fueron borrados. Aunque se visualizaron todos los meses, para fines demostrativos se muestran los meses de febrero y abril de 2015, figura 3.52 y 3.53.



<- Jan 2015 Summary Mar 2015 ->
Feb 2015 OK

Wed Feb 04 2015 14:11:48	1139111	m...	r/rrwxrwxrwx	0	0	18923029	C:/Analisis Forense Tapia/UsingFTKAreli.pdf
Thu Feb 05 2015 13:10:52	1016882	m...	r/rrwxrwxrwx	0	0	18923035	C:/Analisis Forense Tapia/Lab3areli.pdf
Tue Feb 10 2015 10:51:08	85839357	m...	r/rrwxrwxrwx	0	0	135	C:/Libros Tesis/Libro EnCase.epub (deleted)
Thu Feb 12 2015 20:05:32	644542	m...	r/rrwxrwxrwx	0	0	19241360	C:/Documentos Beca Titulacion/ALDF.pdf
Mon Feb 16 2015 13:16:56	21621	m...	r/rrwxrwxrwx	0	0	18923041	C:/Analisis Forense Tapia/EnCE Capitulo 1.docx
Mon Feb 23 2015 15:05:42	15821086	m...	r/rrwxrwxrwx	0	0	141	C:/Libros Tesis/eBookEnCase.pdf (deleted)
Mon Feb 23 2015 18:38:42	5333224	m...	r/rrwxrwxrwx	0	0	17249326	C:/Analisis Forense areli/Palacios Ugalde Arturo TESIS.pdf
Mon Feb 23 2015 19:47:38	401478	m...	r/rrwxrwxrwx	0	0	17249340	C:/Analisis Forense areli/HHS_es8_Digital_Forensics.pdf
Wed Feb 25 2015 12:28:30	1802621	m...	r/rrwxrwxrwx	0	0	17249345	C:/Analisis Forense areli/Metodologia para la forensia informatica.pdf
Wed Feb 25 2015 13:53:48	1794873	m...	r/rrwxrwxrwx	0	0	17249348	C:/Analisis Forense areli/REVISADO-1.pdf
Thu Feb 26 2015 13:30:22	572626	m...	r/rrwxrwxrwx	0	0	17249305	C:/Analisis Forense areli/cyb_analisis_foren (1).pdf
Thu Feb 26 2015 13:56:56	572626	m...	r/rrwxrwxrwx	0	0	17249313	C:/Analisis Forense areli/herramientas.pdf
Thu Feb 26 2015 13:58:04	98629	m...	r/rrwxrwxrwx	0	0	17249336	C:/Analisis Forense areli/Informatica Forense v0.6.pdf
Fri Feb 27 2015 14:10:12	2317977	m...	r/rrwxrwxrwx	0	0	17249310	C:/Analisis Forense areli/SimplifiedGuideDigitalEvidenceCHECAR.pdf
Fri Feb 27 2015 14:17:14	968405	m...	r/rrwxrwxrwx	0	0	17249332	C:/Analisis Forense areli/definicion.pdf

Figura 3. 52 Febrero 2015



<- Mar 2015 Summary May 2015 ->
Apr 2015 OK

Mon Apr 13 2015 14:04:12	23135	m...	r/rrwxrwxrwx	0	0	23681043	C:/Informacion TESIS/FORENSE_Tools.docx
Wed Apr 15 2015 09:54:50	627275	m...	r/rrwxrwxrwx	0	0	19241366	C:/Documentos Beca Titulacion/COMUNICADO_ALDF-beca.pdf
Fri Apr 17 2015 00:09:34	344109	m...	r/rrwxrwxrwx	0	0	23681040	C:/Informacion TESIS/PyFlag.docx
Wed Apr 29 2015 11:02:36	101347734	m...	r/rrwxrwxrwx	0	0	54	C:/MOBILedit! Forensic.rar (deleted)
Wed Apr 29 2015 11:39:58	271931	m...	r/rrwxrwxrwx	0	0	17249287	C:/Analisis Forense areli/cyb_mex_forense.pdf
Wed Apr 29 2015 13:25:14	291452	m...	r/rrwxrwxrwx	0	0	17249357	C:/Analisis Forense areli/apuntes4LATEX.pdf

Figura 3. 53 Abril 2015

Autopsy recuperó solo los archivos que fueron borrados intencionalmente, como se describe en la tabla 3.4. En la figura 3.54 y 3.55 se muestran los tres únicos archivos que se recuperaron y que son legibles.

Tipo de archivo	Número de archivos borrados	Número de archivos recuperados	Archivos recuperados legibles
Data Base File (.DB)	0	1	0
Epub	1	1	1

Jpeg	26	26	0
Pdf	3	3	2
Winrar	1	1	0
Word	1	1	0
Total	32	33	3

Tabla 3. 4 Lista de archivos recuperados por Autopsy

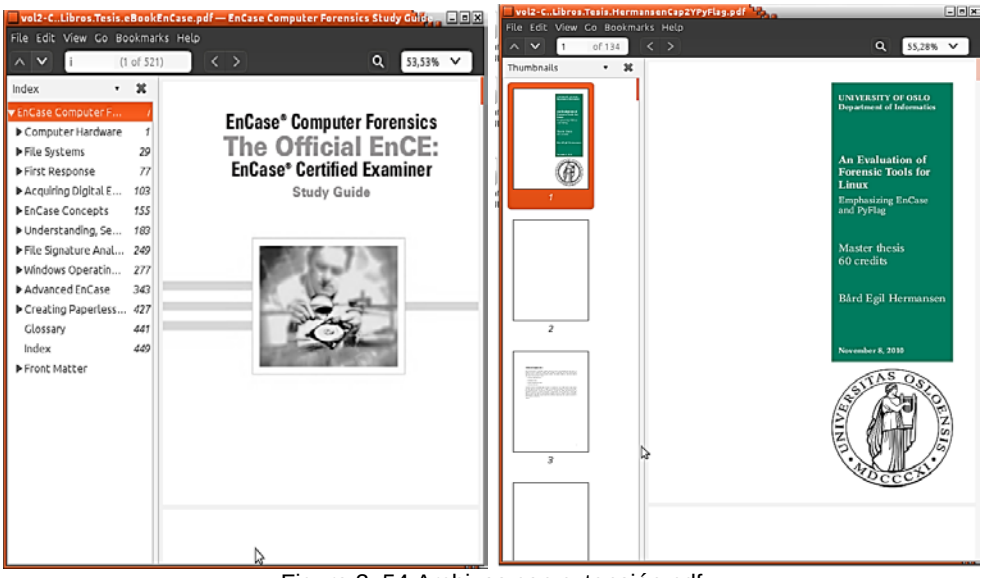


Figura 3. 54 Archivos con extensión pdf

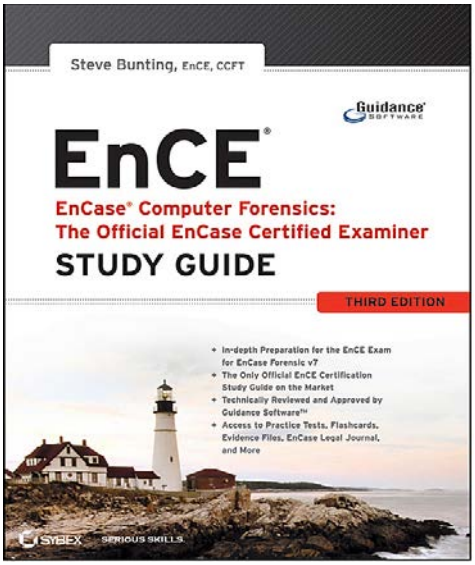


Figura 3. 55 Archivo con extensión epub

3.2 HELIX 3

El software Helix 3, es una herramienta de la distribución de Ubuntu para adquirir imágenes forenses de distintos tipos de discos duros y de particiones.

Helix 3 cuenta con distintas herramientas y en la tabla 3.5 se mencionan algunas de ellas.

Herramienta	Descripción
Adepto	Crea una imagen bit a bit (adquisición y clonación de imagen) y genera la cadena de custodia (archivo que contiene información acerca del proceso de la imagen)
Autopsy	Es la interfaz gráfica para la línea de comandos de The Sleuth Kit, que analiza los sistemas Windows y Linux
Bless Hex Editor	Edita archivos como secuencias de bytes (editor binario hexadecimal)
Foremost	Recupera archivos por el tipo de cabecera como doc, exe, gif, jpeg, ole, pdf, png, rar, zip, entre otros
GtkHash:	Programa gráfico de cálculo de hash (md5, sha1, sha256, sha512)
Linen	Crea imágenes y las procesa con las herramientas de Encase forense (herramienta de adquisición de imagen de Guidance Software)
Meld Diff Viewer	Visualiza las diferencias entre archivos y carpetas
Ophcrack	Desbloquea la contraseña de usuario en el sistema operativo Windows
Registry Viewer	Navegador de archivo de registro de Windows
Root Terminal	Línea de comandos de Linux con privilegios de administrador
Virus Scanner	Analiza el correo electrónico en gateways de correo (conjunto de herramientas GPL Clam Antivirus para Unix)
Wireshark (root)	Captura y analiza los paquetes de red

Tabla 3. 5 Herramientas de Helix 3

3.2.1 Adepto y Foremost

Adepto es una herramienta que realiza la adquisición de imagen y la clonación de dispositivos por medio de una interfaz gráfica; mientras que Foremost recupera distintos tipos de archivos a través de una interfaz de línea de comandos.

Para este caso, el dispositivo evidencia es el mismo que se utilizó anteriormente. En caso de ser necesario algún dispositivo USB para realizar la clonación, éste debió haber pasado por el proceso de sanitización descrito anteriormente (Capítulo 2.2). A continuación se describe el proceso completo para llevar a cabo la clonación de dispositivo evidencia y su respectiva recuperación.

1) Se accedió a la BIOS, encendiendo la computadora y presionando repetidamente la tecla **F12**. Se eligió la opción **USB KEY: KingstonDataTraveler 2** para que la computadora inicie desde el dispositivo, ver figura 3.56.

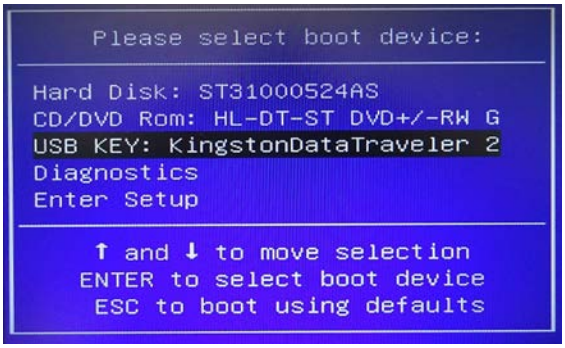


Figura 3. 56 Selección de dispositivo de arranque

2) La computadora inició desde el dispositivo de arranque Helix, se seleccionó la opción **Boot into the Helix Live CD** para que se cargue Helix, ver figura 3.57. La pantalla principal de Helix se muestra en la figura 3.58.

Figura 3. 57 Selección "Boot into the Helix Live CD"

Figura 3. 58 Pantalla principal de Helix

3) Lo siguiente fue elegir el dispositivo evidencia para poder realizar cualquier proceso en él, y se presentó en el escritorio como se muestra en la figura 3.59 y figura 3.60 (se seleccionó el dispositivo y se eligió la opción **Mount Kingston DataTraveler 2.0 (2)**).

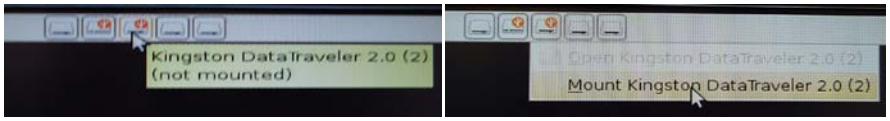


Figura 3. 59 Montar el dispositivo evidencia

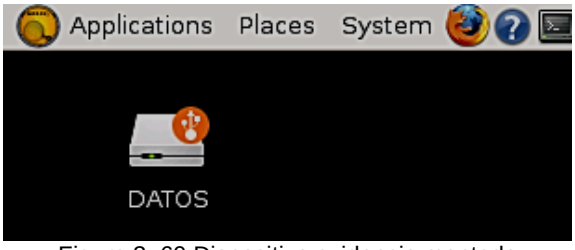


Figura 3. 60 Dispositivo evidencia montado

4) En el siguiente paso se abrió una interfaz de línea de comandos, con el objetivo de identificar el dispositivo evidencia de los demás dispositivos conectados a la computadora (figura 3.61), por lo cual se ejecutó el comando: **sudo fdisk –l**.

   A continuación se menciona cada uno de los dispositivos:

   - Dispositivo de autoarranque Helix: /dev/sdb
   - **Dispositivo evidencia: /dev/sdh**
   - **Dispositivo para clonación: /dev/sdg**

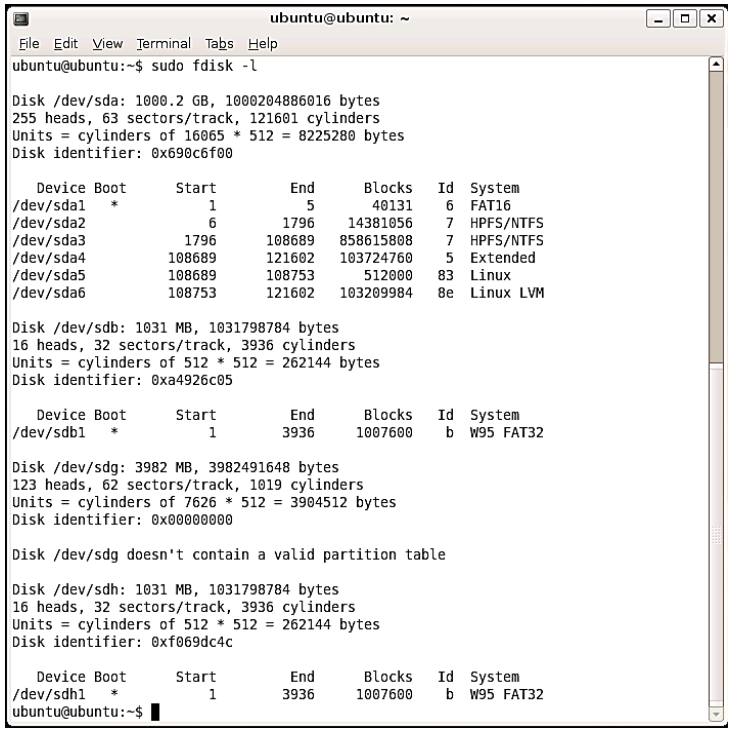


Figura 3. 61 Identificación de dispositivos

5) Se abrió otra interfaz de línea de comandos en la que se realizó el **cálculo de hash** del dispositivo evidencia, como se muestra en la figura 3.62. Para ello se usó el comando **sudo sha256sum /dev/sdh** (descrito en la tabla 3.2).

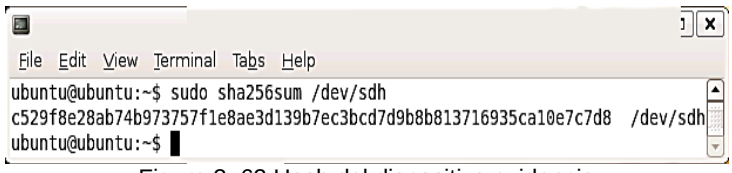


Figura 3. 62 Hash del dispositivo evidencia

6) En el caso de adquisición se inició Adepto y se esperó a que se cargara, como se observa en la figura 3.63.

Figura 3. 63 Inicialización de Adepto

7) En la primera ventana se ingresó el nombre de usuario para el procedimiento: **TesisUACM,** y se eligió la opción ir (**Go**) ver figura 3.64.

Figura 3. 64 Ingreso de nombre de usuario

8) Posteriormente se muestra la pestaña de **Device Info**, se seleccionó el dispositivo evidencia **sdh** y se indicaron ciertas características, tales como **fabricante, modelo, capacidad de almacenamiento, sectores**, por mencionar algunos (figura 3.65).

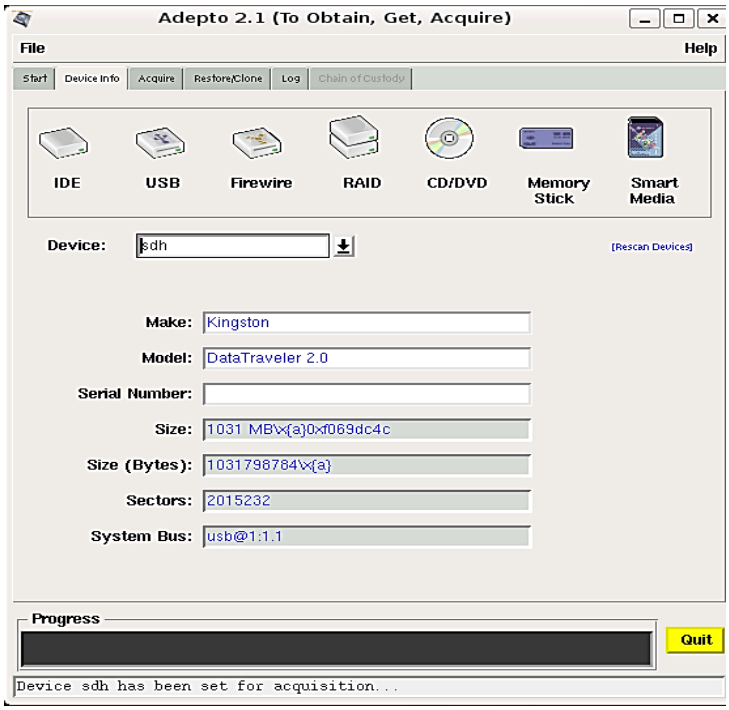


Figura 3. 65 Selección de dispositivo evidencia

9) La siguiente ventana que se abrió fue la de **Acquire** y contiene tres secciones; la primera **Source information** contiene información del dispositivo evidencia y de la imagen (se agregó una nota acerca del tamaño del dispositivo evidencia y dispositivo para la clonación), en la segunda **Destination information** se eligió el dispositivo para la clonación y en la tercera **Options** se seleccionó el hash **SHA256** y en la opción **Segment** se optó por 0 Mb (para evitar que la imagen se divida en segmentos, este caso se usa cuando el dispositivo de clonación es de menor tamaño comparado con el dispositivo evidencia), ver figura 3.66.

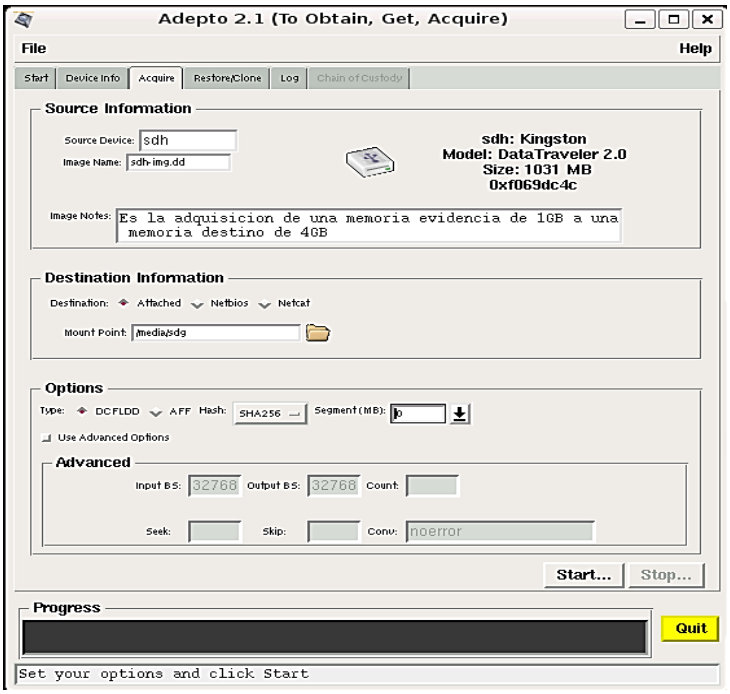


Figura 3. 66 Datos ingresados

10) Por último se seleccionó la opción **Start** y tardó unos minutos el proceso de adquisición, indicando su término como se observa en la figura 3.67. Además se efectuó automáticamente la verificación de hash, ver figura 3.68.

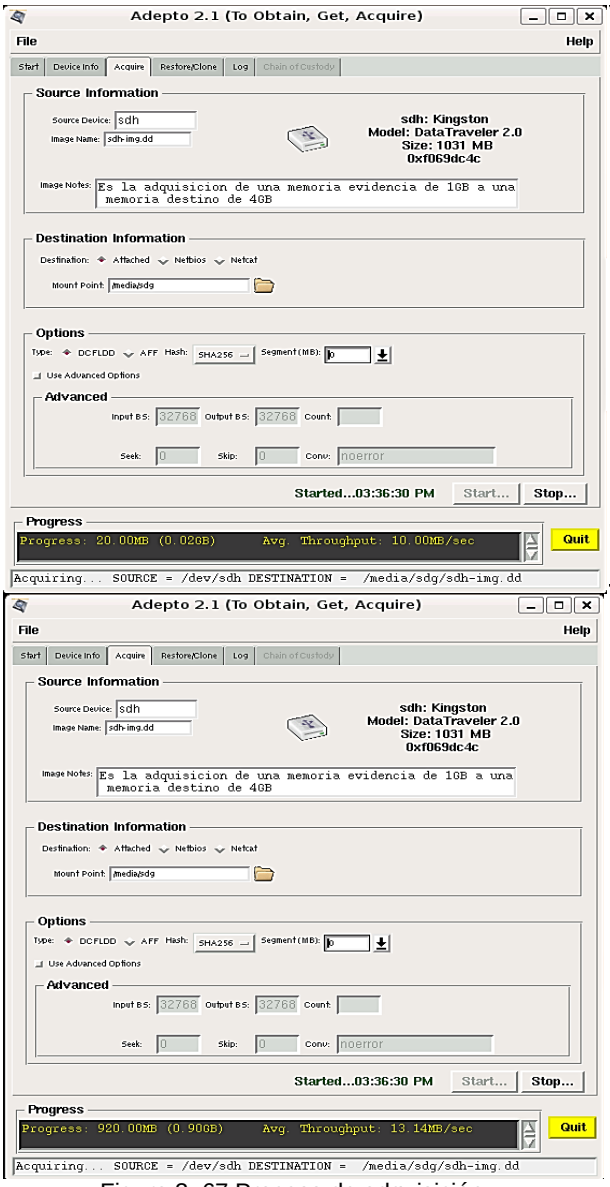


Figura 3. 67 Proceso de adquisición

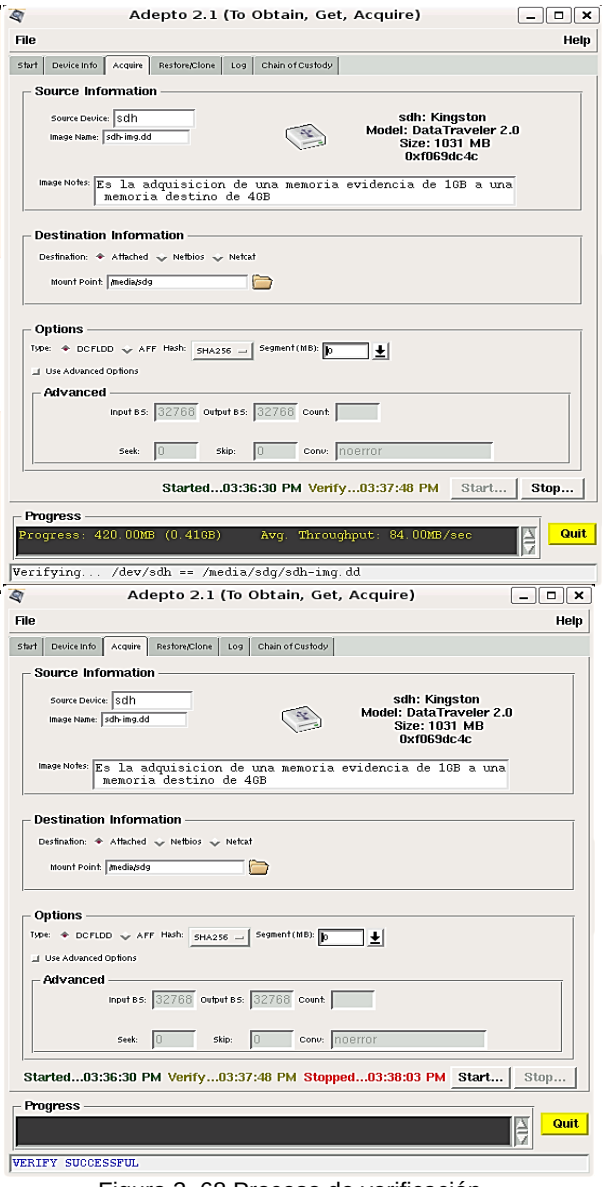


Figura 3. 68 Proceso de verificación

11) El paso siguiente fue ingresar a la pestaña **Log**, la cual presenta información acerca del proceso incluyendo el hash de la imagen, como se muestra en la figura 3.69. Este hash fue comparado con el hash del dispositivo evidencia, y se comprobó que la imagen no fue alterada.

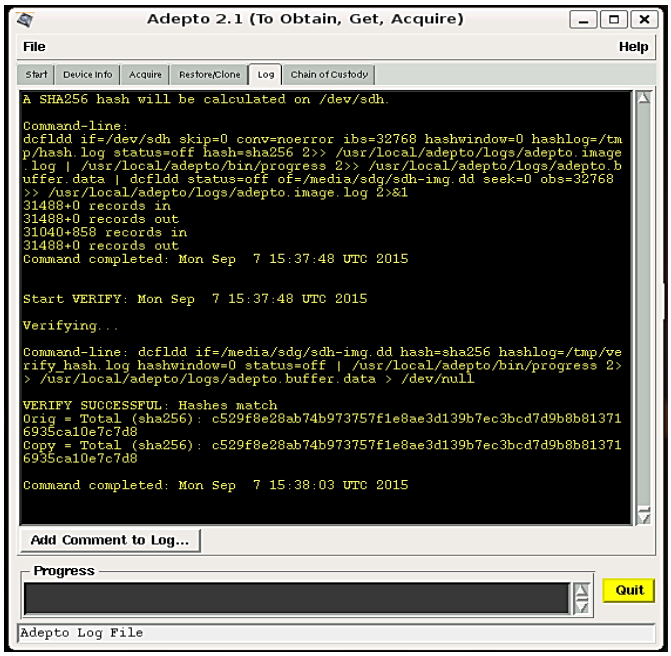


Figura 3. 69 Pestaña de registro con información de proceso de adquisición

12) Lo siguiente fue volver a la pestaña **Restore/Clone**, en este caso solo se consideró la segunda sección **Clone a device** en la que se eligió el dispositivo **sdg** (dispositivo listo para el proceso de clonación, es decir, se le realizó el proceso de sanitización descrito previamente) y se eligió la opción **Clone**. El término del proceso de clonación se muestra en la figura 3.70.

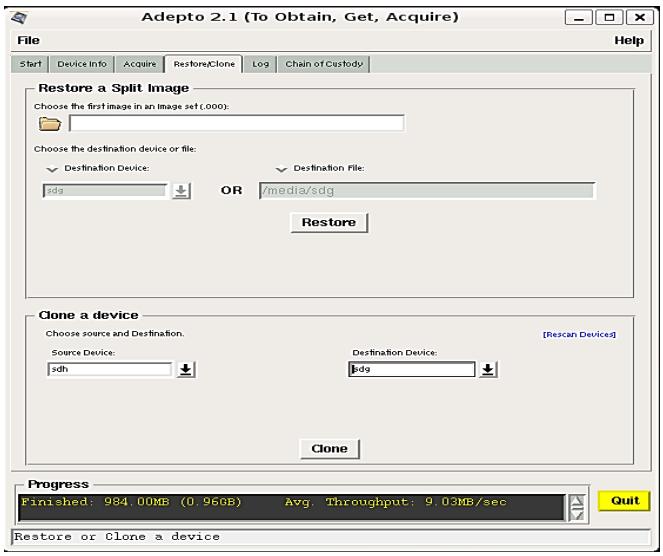


Figura 3. 70 Proceso de clonación

Automáticamente se procedió a realizar la verificación de la clonación y en la figura 3.71, se muestra que la verificación fue completa.

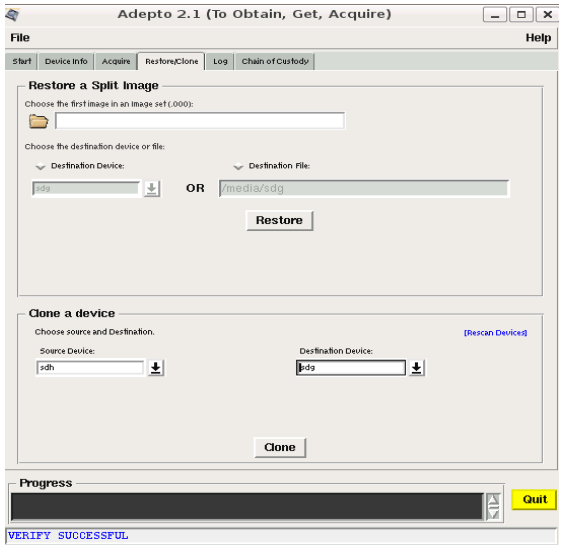


Figura 3. 71 Verificación del proceso de clonación

13) Se regresó a la pestaña **Log** y se mostró información sobre el proceso de clonación tal como los dispositivos usados, el tiempo del proceso y la verificación de hash de ambos dispositivos, ver figura 3.72.

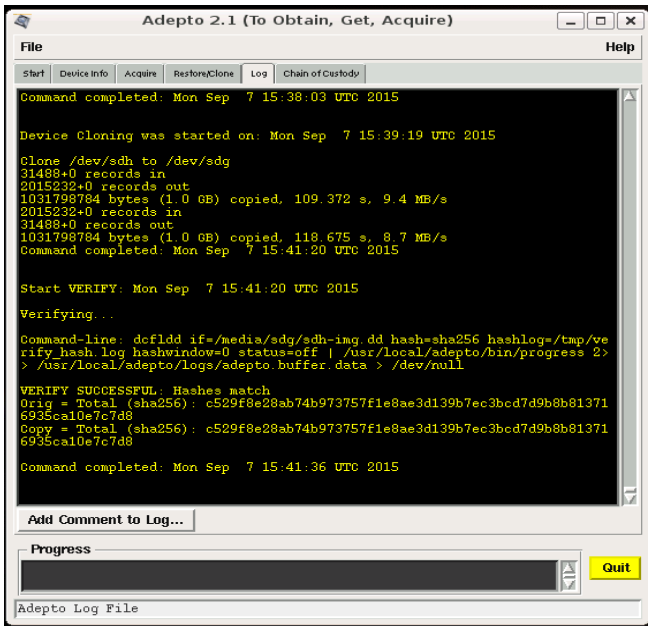


Figura 3. 72 Pestaña de registro con información de proceso de clonación

14) Por último la pestaña **Chain of Custody** presentó información sobre los procesos ejecutados, además se generó un archivo PDF con tal información, ver figura 3.73.

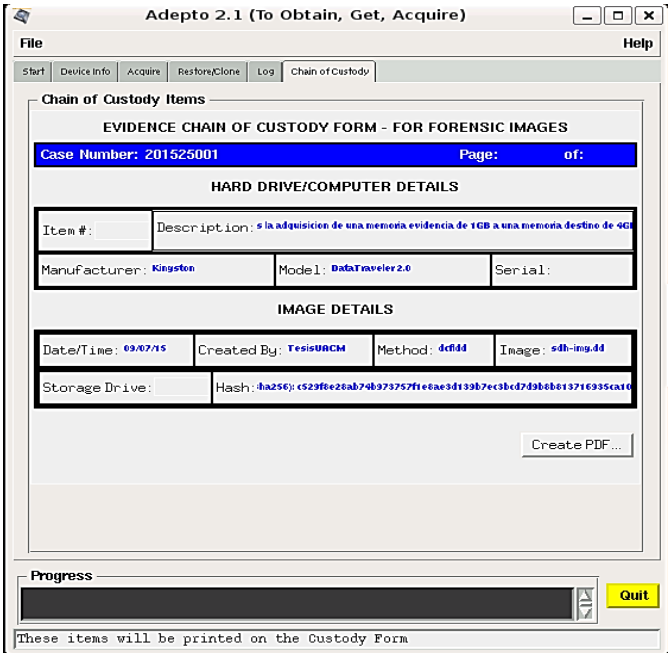
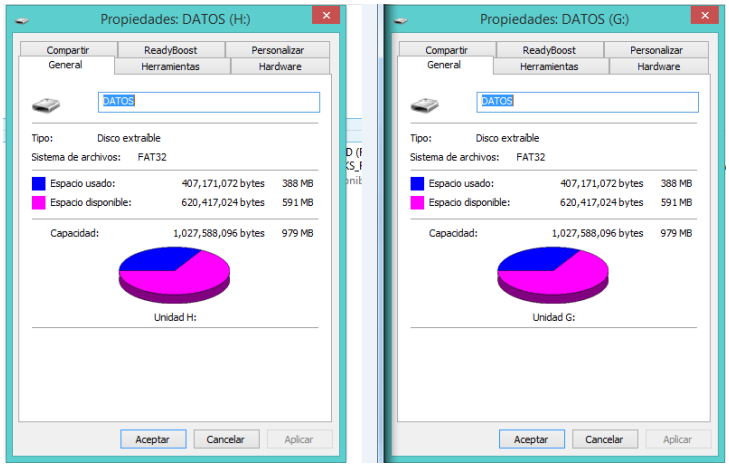


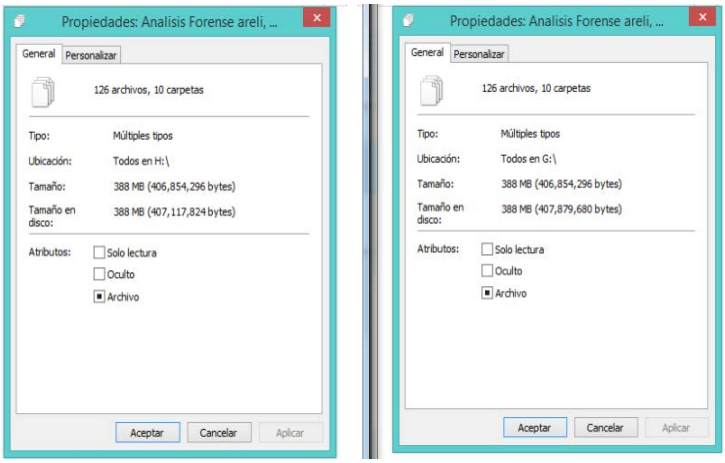
Figura 3. 73 Pestaña de cadena de custodia

15) Se verificó que el dispositivo evidencia y el dispositivo clonado tuvieran la misma cantidad de almacenamiento usado, como se muestra en las figuras 3.74 y 3.75.

Figura 3. 74 Dispositivo clonado y dispositivo evidencia



(a) Capacidad de almacenamiento



(b) Numero de archivos

Figura 3. 75 Propiedades del dispositivo evidencia y del dispositivo clonado

16) Para el proceso de recuperación de archivos fue necesario instalar Foremost a través de una interfaz de línea de comandos (figura 3.76). Por lo anterior se volvió a conectar el dispositivo clonado a la computadora; además, se creó una carpeta en el escritorio con la finalidad de que en ésta se almacenen los archivos recuperados, ver figura 3.77.

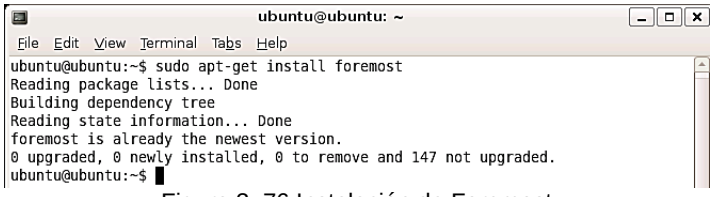


Figura 3. 76 Instalación de Foremost

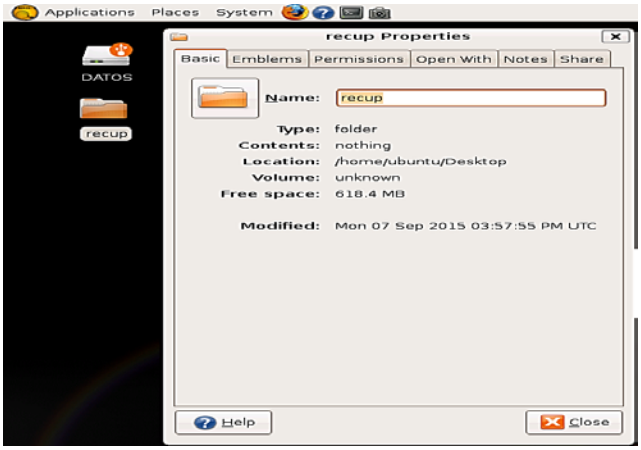


Figura 3. 77 Carpeta para almacenar los archivos recuperados

17) El comando ejecutado para la recuperación de archivos en la interfaz de línea de comandos fue: sudo foremost –t all –i /dev/sdg1 –o /home/ubuntu/Desktop/recup (ver figura 3.78).

Donde: -t all, indica el tipo de archivos a recuperar

-i /dev/sdg1, indica el dispositivo de búsqueda

-o /home/ubuntu/Desktop/recup, indica la carpeta donde guardará los archivos

```
ubuntu@ubuntu:~$ sudo foremost -t all -i /dev/sdg1 -o /home/ubuntu/Desktop/recup
Processing: /dev/sdg1
|**********|
ubuntu@ubuntu:~$
```

Figura 3. 78 Proceso para recuperar archivos

18) Se abrió la carpeta **recup** que mostró a su vez varias carpetas junto con un archivo con extensión txt (figura 3.79), que contiene información acerca del número de archivos recuperados, ver figura 3.80.

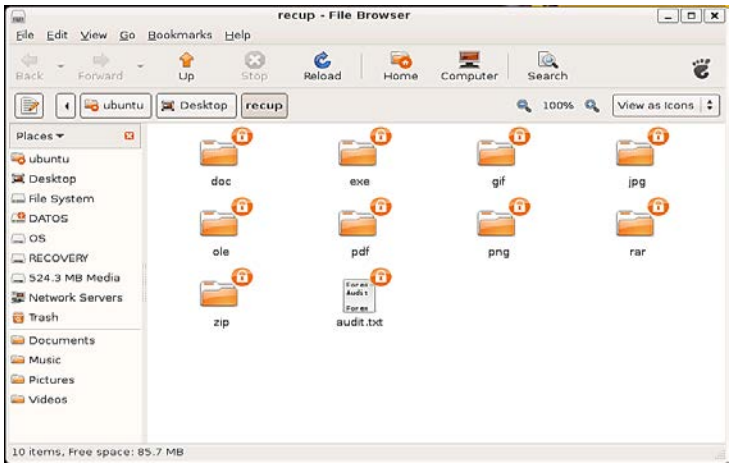


Figura 3. 79 Carpetas con archivos recuperados

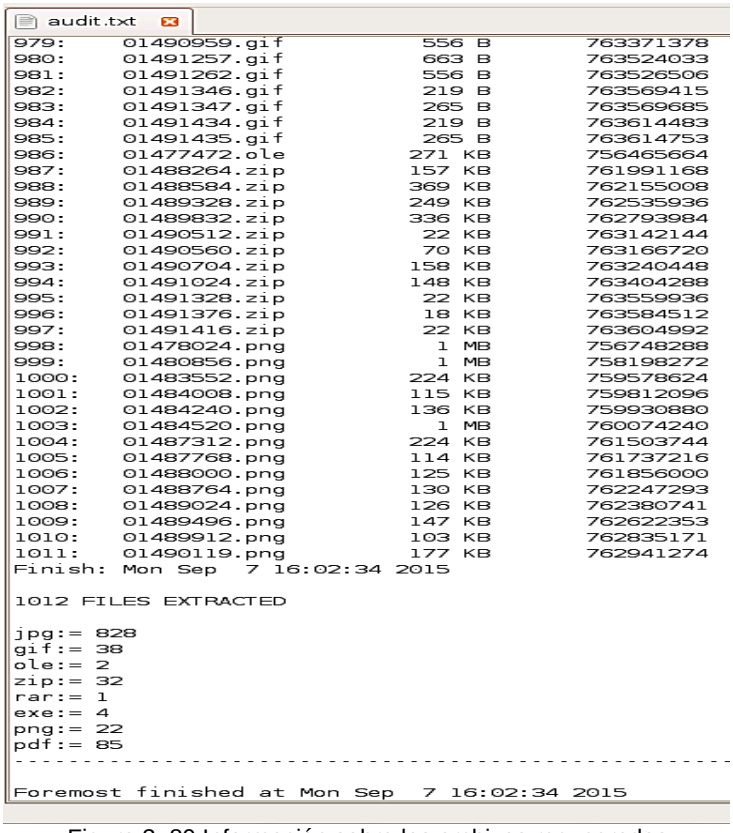


Figura 3. 80 Información sobre los archivos recuperados

19) Como las carpetas no tenían permiso de lectura y escritura, fue necesario dar los permisos a través de la interfaz de línea de comandos con el comando: sudo chmod –R 777 recup (ver figuras 3.81 y 3.82).

Donde: chmod: cambia los permisos de acceso de un fichero o directorio

-R: aplica el comando chmod a todos los ficheros y subdirectorios

777: permite la lectura, escritura y ejecución

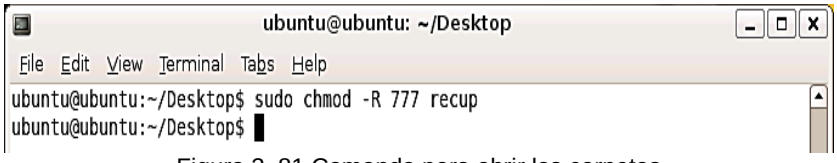


Figura 3. 81 Comando para abrir las carpetas

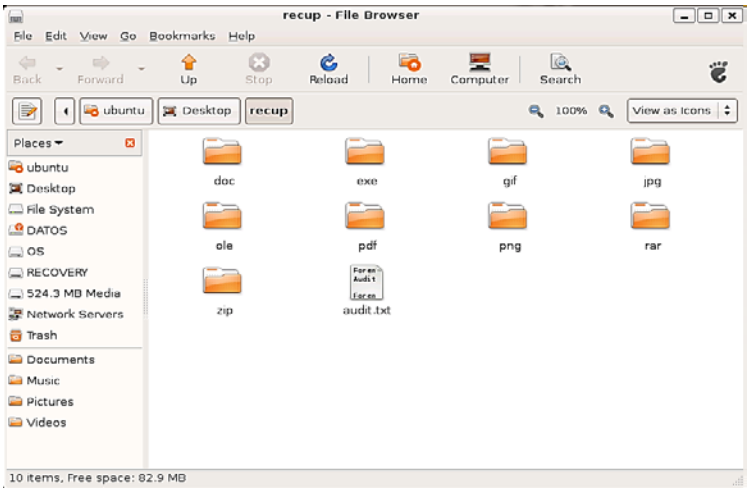


Figura 3. 82 Carpetas con permisos de lectura

La tabla 3.6 muestra la lista de los archivos recuperados por la herramienta Foremost, además se muestran algunos archivos recuperados en las figura 3.83 a 3.85.

Tipo de archivo	Número de archivos borrados	Número de archivos recuperados	Archivos recuperados legibles
Exe	0	4	3
Gif	0	38	28
Jpeg	26	828	828
Ole	0	1	0
Pdf	3	85	85
Png	0	22	22
Winrar	1	1	0
Word	1	1	1
Zip	0	32	1
Total	31	1012	968

Tabla 3. 6 Lista de archivos recuperados por Foremost

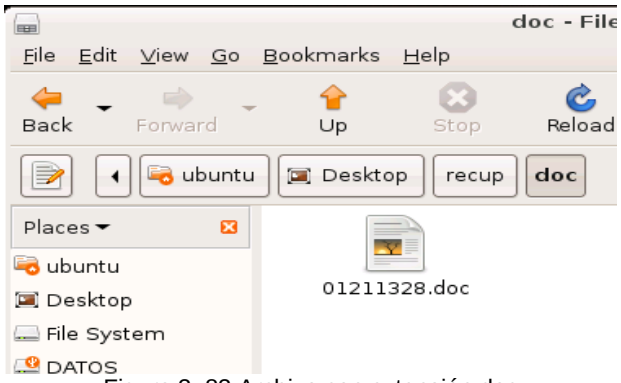


Figura 3. 83 Archivo con extensión doc

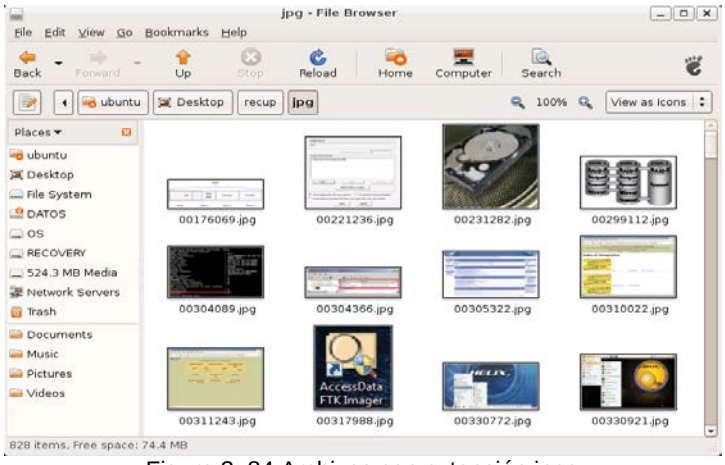


Figura 3. 84 Archivos con extensión jpeg

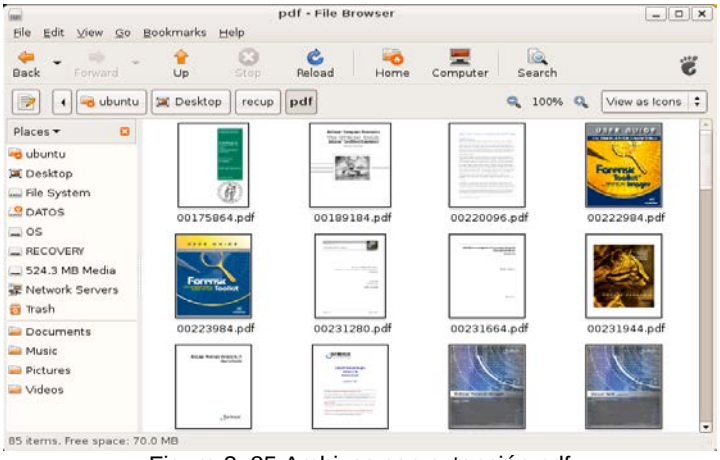


Figura 3. 85 Archivos con extensión pdf

3.3 DIGITAL EVIDENCE & FORENSIC TOOLKIT (DEFT)

Digital Evidence & Forensic Toolkit (DEFT), es un software de la distribución de GNU/Linux cuenta con herramientas que realizan el análisis forense en la red y dispositivos móviles, recuperación de contraseñas y datos, análisis de evidencia, adquisición y clonación de medios de almacenamiento, cálculo de hash, por mencionar algunas. DEFT cuenta con una amplia diversidad de herramientas para un análisis, algunas de las cuales se describen en la tabla 3.7. En las siguientes secciones se describen algunas herramientas que forman parte de DEFT.

Herramienta	Descripción
Android Debug Bridge (adb)	Herramienta de línea de comandos que comunica a un ordenador y un dispositivo Android
Autopsy	Realiza la recuperación de archivos
Cmospwd	Descifra la contraseña guardada en CMOS para entrar a la configuración del BIOS
Dhash2	Ejecuta la clonación y calcula el valor hash (MD5 y SHA1) simultáneamente
Digital Forensics Framework (DFF)	Realiza análisis de la evidencia digital (reúne, preserva e informa)
Foremost	Recupera archivos por medio de sus encabezados, pies de página y la estructura de datos interna, proceso conocido como data carving
Guymager	Realiza la adquisición y/o clonación de un disco (la copia se crea bit a bit)
Log2Timeline	Crea una línea de tiempo para analizar archivos de registro (logs)
Netmork Mapper (Nmap)	Realiza la exploración de red, análisis seguro y auditorías
Photorec	Recupera datos, archivos, documentos y videos perdidos de discos duros
Testdisk	Recupera particiones de almacenamiento de datos perdidos

Tabla 3. 7 Herramientas de DEFT

3.3.1 Dhash2 y DFF

Dhash2 es una herramienta que realiza el cálculo de hash y la adquisición de imagen, y en el caso de DFF analiza y recupera archivos, ambos a través de una interfaz gráfica. Considere que el dispositivo evidencia es el mismo utilizado en las herramientas usadas anteriormente. A continuación se describe el proceso completo para llevar a cabo la adquisición del dispositivo evidencia y la recuperación.

1) Se accedió a la BIOS, encendiendo la computadora y pulsando repetidamente la tecla **F12**. En este caso, se seleccionó **USB KEY: KingstonDT 101 G2 PMAP** para que la computadora inicie desde este dispositivo, ver figura 3.86.

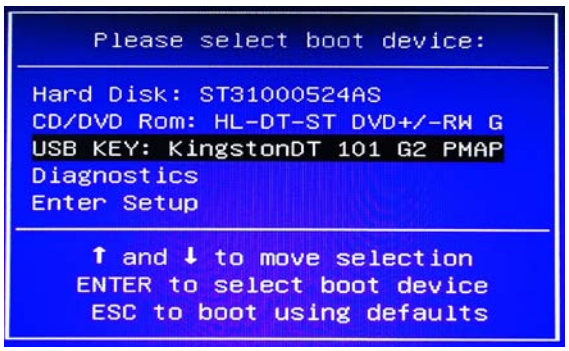


Figura 3. 86 Selección de dispositivo de arranque

2) La computadora inició desde el dispositivo de autoarranque, se seleccionó la opción **DEFT Linux 8 Live** para que se cargue DEFT, ver figura 3.87. La pantalla principal de DEFT se muestra en la figura 3.88.

Figura 3. 87 Seleccionar DEFT Linux 8 Live

Figura 3. 88 Pantalla principal de DEFT

3) En el siguiente paso se identificó y asignó el dispositivo evidencia (DATOS) en modo protegido, es decir, con la opción **Mount in protected mode (Read Only)** con el objetivo de que no pueda ser modificado, ver figuras 3.89 y 3.90.

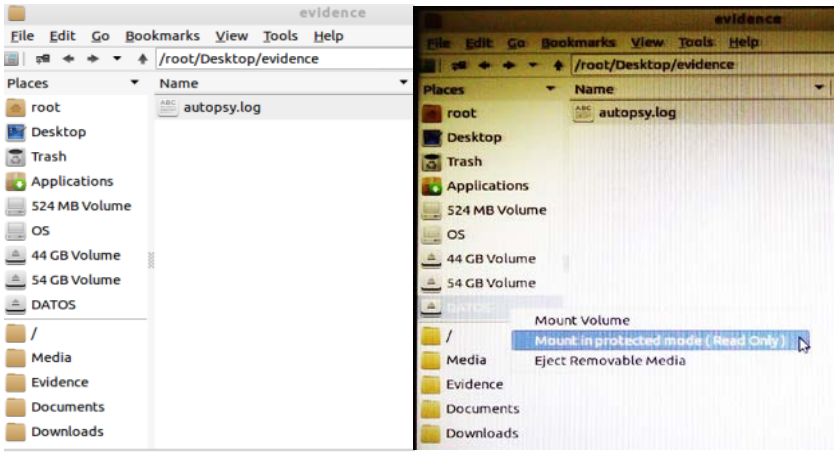


Figura 3. 89 Asignación del dispositivo evidencia en modo protegido

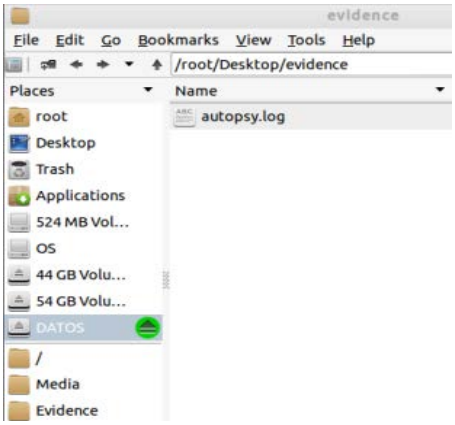


Figura 3. 90 Dispositivo evidencia asignado como solo lectura

4) Para realizar el **cálculo de hash del dispositivo evidencia** se abrió Dhash2, esto se realiza antes de la adquisición. Se eligió el cálculo hash **MD5**, **SHA1** y **Open device (/dev/sdg)** esta última para seleccionar el dispositivo, como se muestra en la figura 3.91.

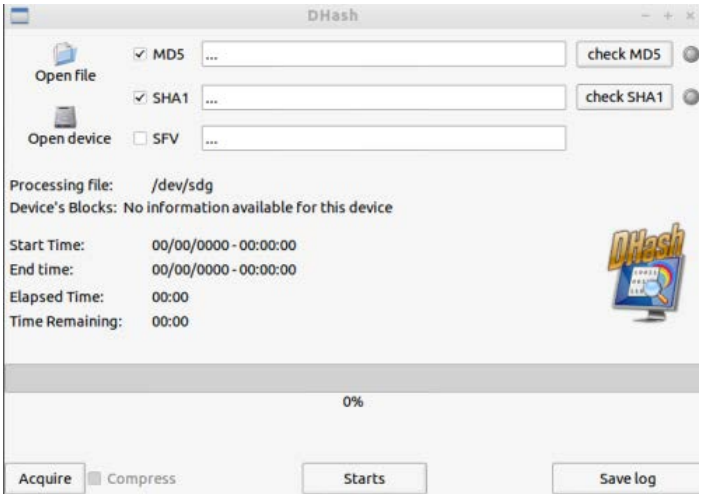


Figura 3. 91 Selección del dispositivo evidencia y hash

Se seleccionó la opción **Starts** y se mostró una barra de progreso del cálculo de hash, ver figura 3.92; además se generó un registro del hash calculado que puede ser guardado.

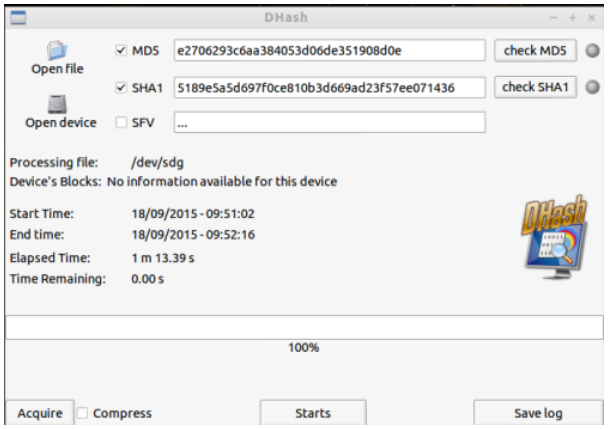


Figura 3. 92 Proceso del cálculo de hash del dispositivo evidencia

5) En la misma ventana se procedió a la adquisición de imagen con la opción **Acquire**, además se eligieron las opciones de nombre de archivo y de folder para la adquisición (figura 3.93 y figura 3.94).

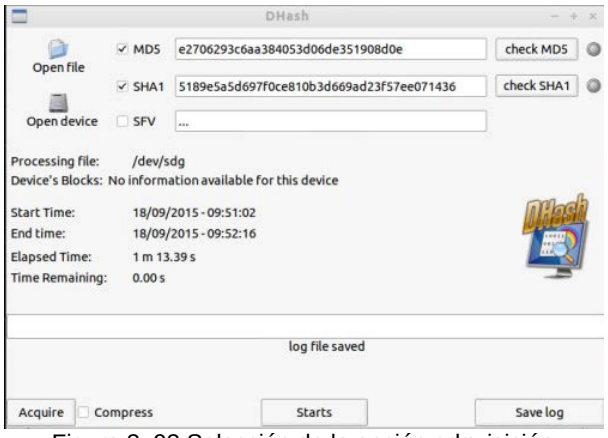


Figura 3. 93 Selección de la opción adquisición

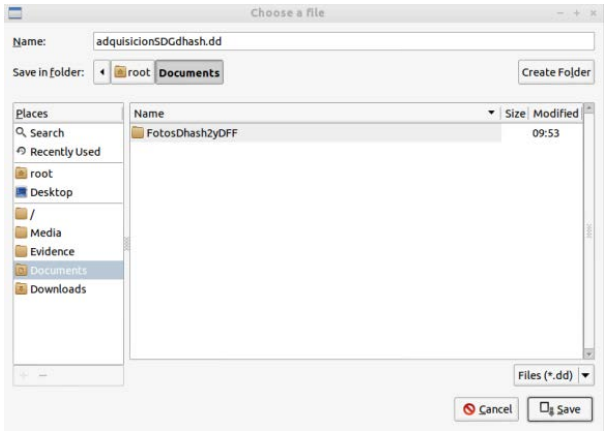


Figura 3. 94 Nombre y ruta de la imagen

6) Se inició el proceso de adquisición con una barra de progreso como se observa en la figura 3.95, en la figura 3.96 se muestra la imagen creada.

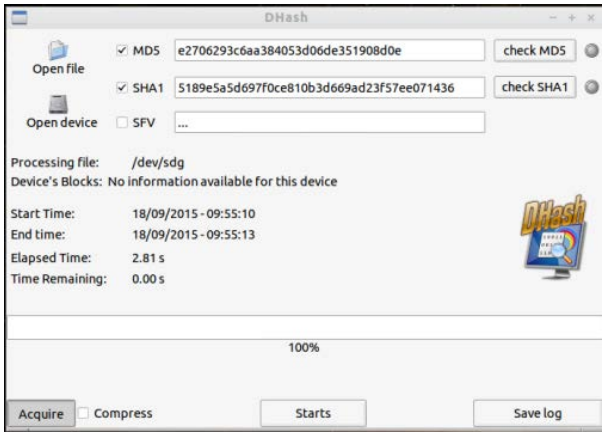


Figura 3. 95 Adquisición de imagen

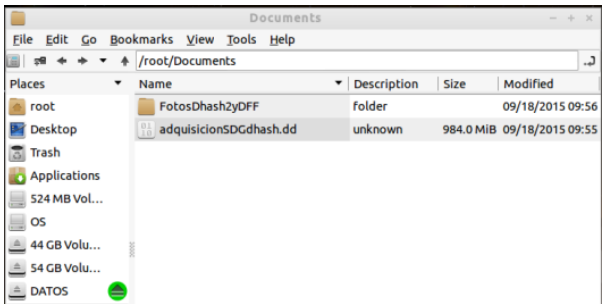


Figura 3. 96 Imagen creada

7) Se calculó el hash de la imagen creada anteriormente, ver figura 3.97. Además se verificó que el valor hash MD5 y SHA1 de la imagen (adquisicionSDGdhash.dd) y el dispositivo evidencia (sdg) son iguales, por lo tanto la imagen no fue alterada, ver figura 3.98.

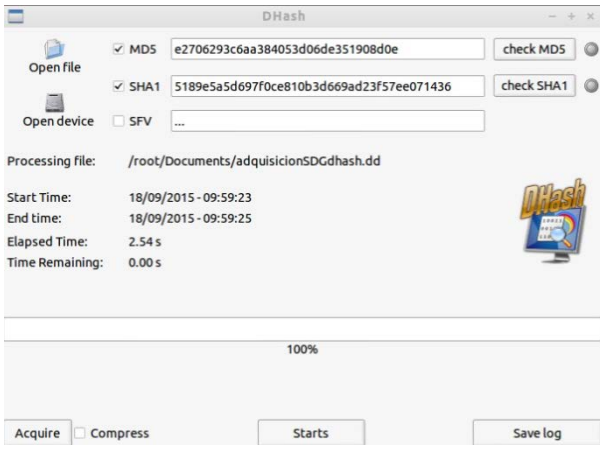


Figura 3. 97 Cálculo de hash de la imagen

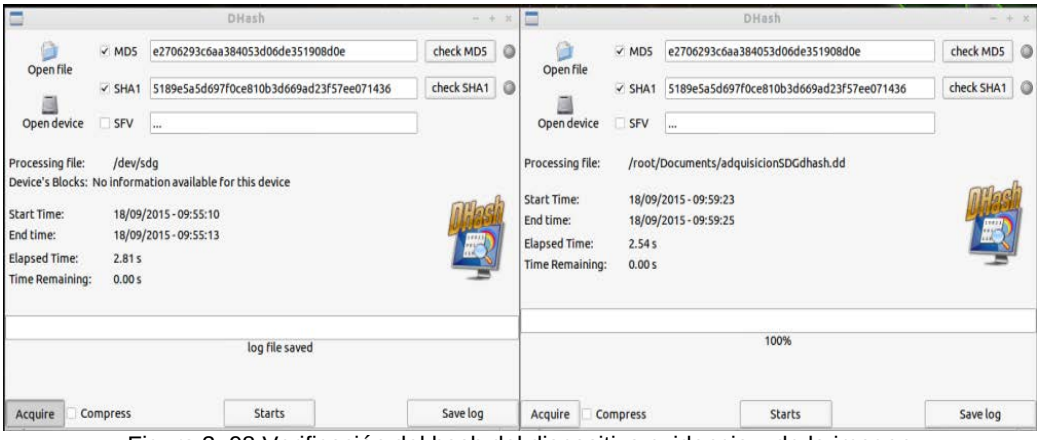


Figura 3. 98 Verificación del hash del dispositivo evidencia y de la imagen

8) Para el proceso de recuperación se inició DFF como se muestra en la figura 3.99.; la pantalla principal de DFF se observa en la figura 3.100.

Figura 3. 99 Cargar DFF

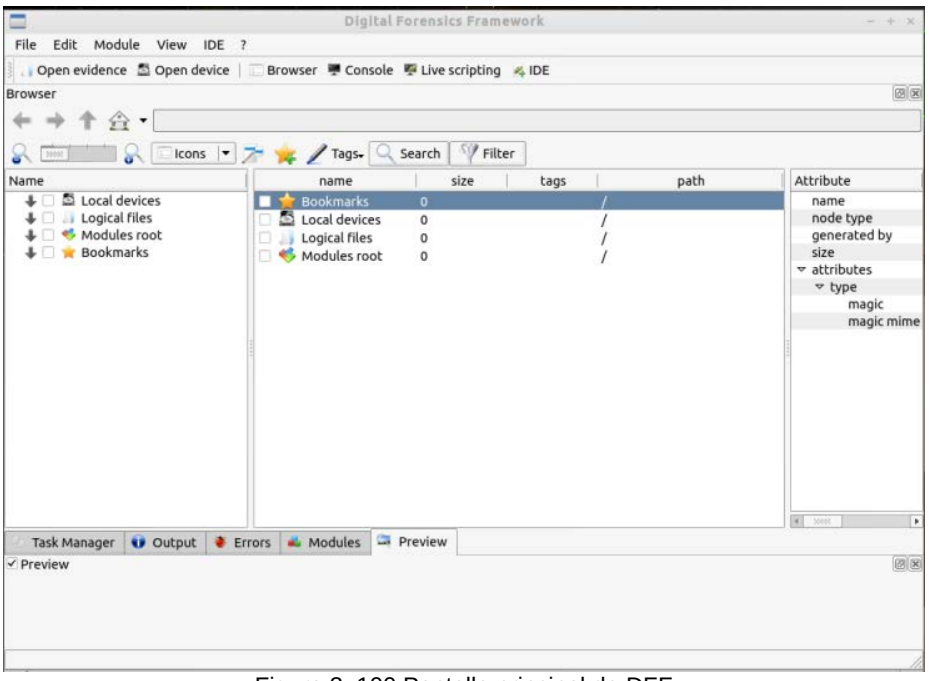


Figura 3. 100 Pantalla principal de DFF

9) En el primer paso se seleccionó **Open device**, en la siguiente ventana se eligió la opción **Select evidence type** para seleccionar el tipo de evidencia, se agregó el archivo de la imagen creada anteriormente con la opción **File**, y por último la opción **ok**, ver figura 3.101.

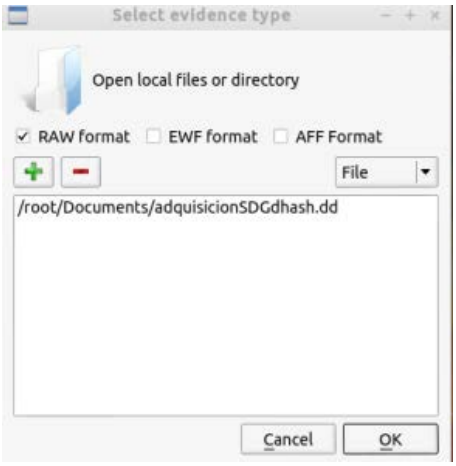


Figura 3. 101 Seleccionar formato de imagen y agregar imagen

10) Se seleccionó la opción **Local devices** (figura 3.102) y se presentó la imagen agregada anteriormente, ver figura 3.103.

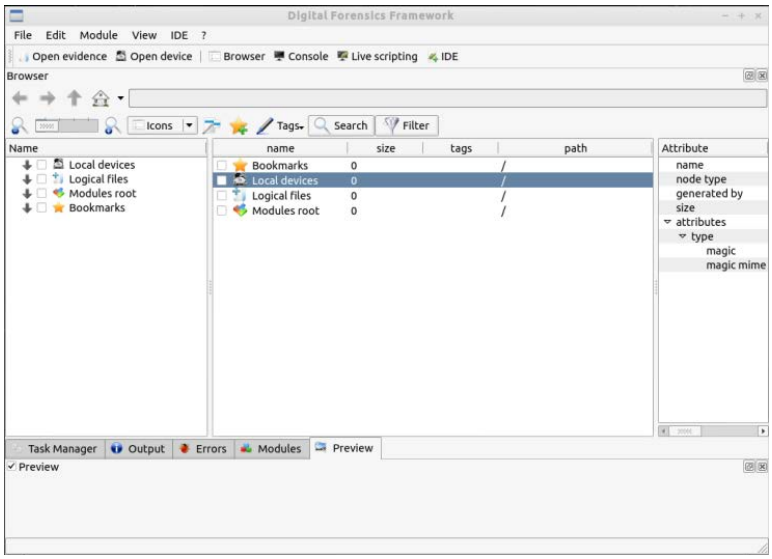


Figura 3. 102 Selección de dispositivos locales

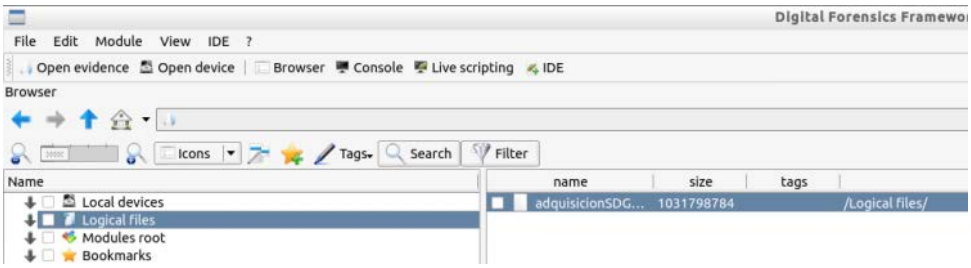


Figura 3. 103 Visualización de imagen agregada

11) Se mostró un mensaje para indicar la opción de particionar la imagen. Se seleccionó la opción **Always** para que siempre realice la partición la imagen (también la opción **Yes** permite continuar con el procedimiento, en caso de cancelar se elige la opción **No**) (figura 3.104). Se eligió la imagen anterior (**adquisicionSDGdhash.dd**) y con la opción Partitions se mostraron las particiones de la imagen seleccionada (figura 3.105).

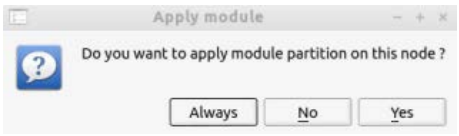


Figura 3. 104 Mensaje sobre la partición de modulo en el nodo

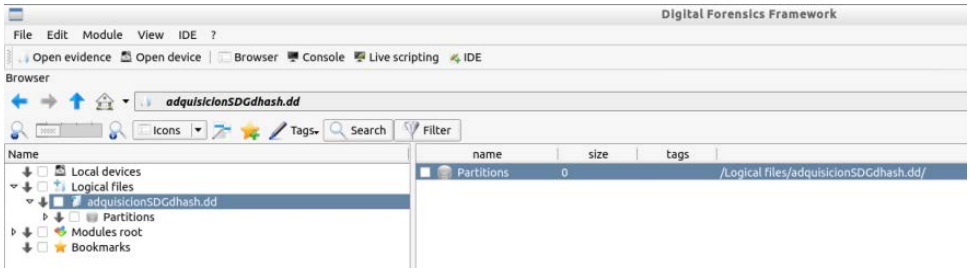


Figura 3. 105 Particiones de la imagen

12) Se seleccionó la opción **Partitions** que ofrece dos alternativas: **Partition 1** y **Unallocated** (figura 3.106), se eligió la primera opción ya que la segunda no contiene información, después envió un mensaje para indicar la opción de módulo fatfs, se seleccionó la opción **Yes** aunque también se puede elegir la opción **Always** (en caso de no continuar con el proceso elegir la opción **No**), ver figura 3.107. Se seleccionó la opción **Partition 1** y mostró información acerca de la imagen (DATOS), ver figura 3.108.

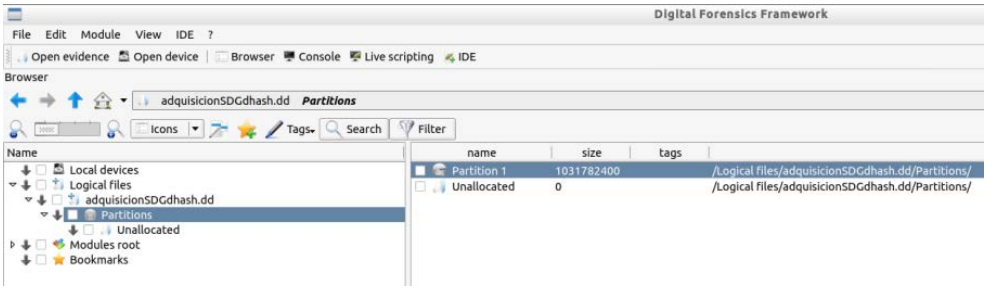


Figura 3. 106 Partición 1 y espacio no asignado de la imagen

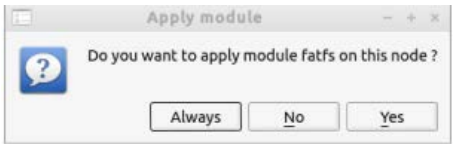


Figura 3. 107 Mensaje sobre aplicar módulo fatfs en el nodo

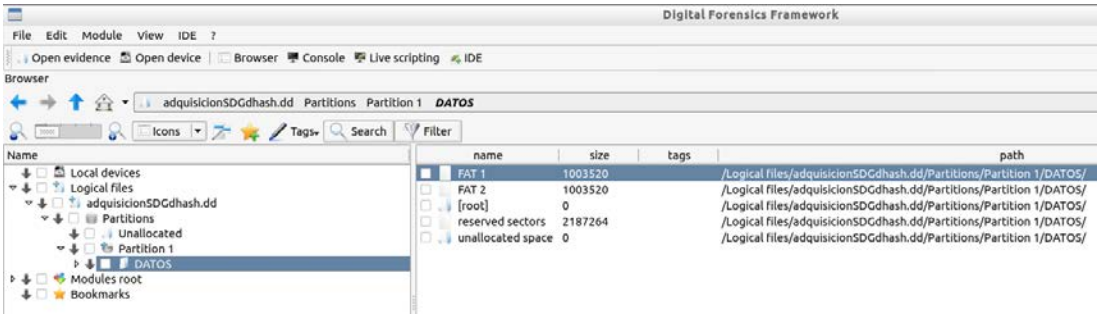


Figura 3. 108 Información de la imagen

13) Se eligió la imagen adquirida anteriormente con la opción DATOS y se desplegó una lista de archivos contenidos en la imagen, los archivos borrados aparecen en color rojo, como se observa en las figuras 3.109 y 3.110.

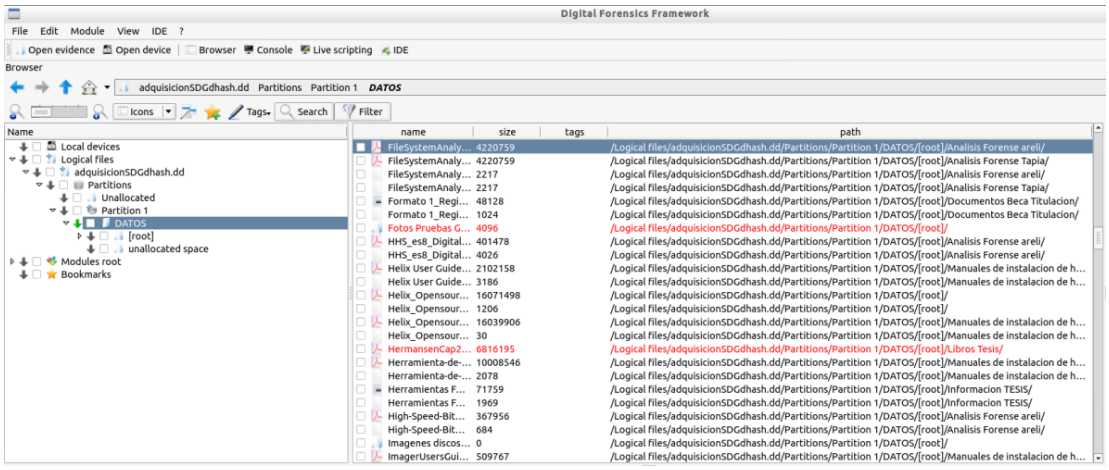


Figura 3. 109 Lista de archivos contenidos en la imagen

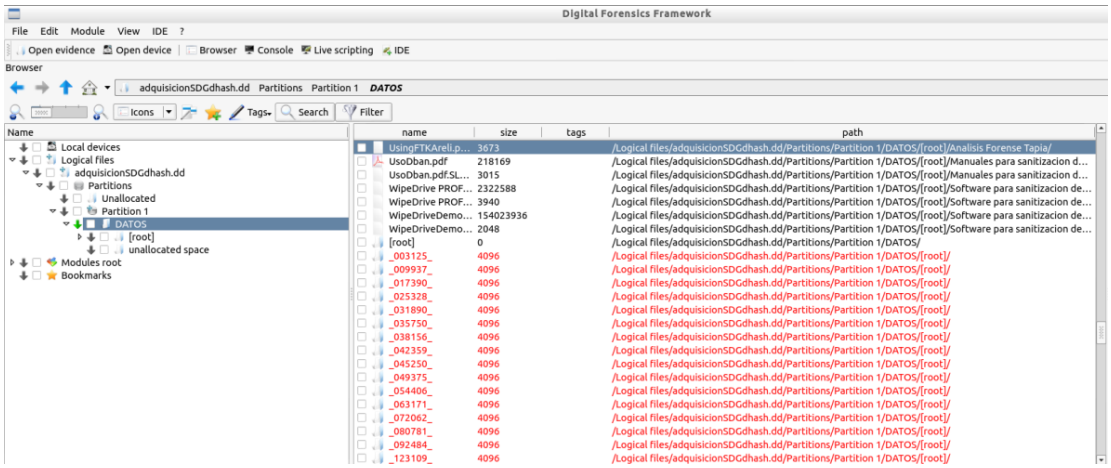


Figura 3. 110 Lista de archivos contenidos en la imagen

14) Para recuperar los archivos borrados, se seleccionó el archivo y en el menú secundario se eligió la opción **Extract**, a continuación se seleccionó la opción **Destination folder** para indicar donde se guardaran los archivos recuperados, en este caso recuperacionDFF y se seleccionó la opción **ok**, ver figura 3.111.

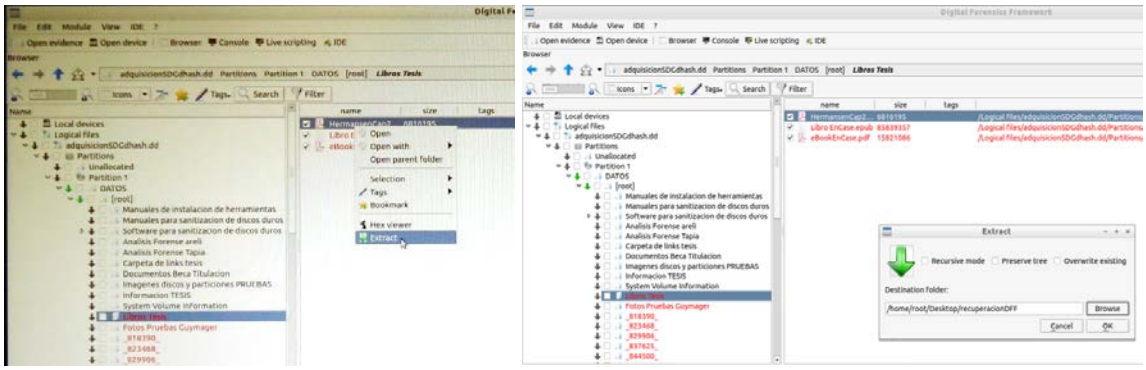


Figura 3. 111 Selección y recuperación de un archivo

La tabla 3.8 muestra la lista de los archivos recuperados de la herramienta DFF, en la figura 3.112 se observan algunos de los archivos recuperados.

Tipo de archivo	Número de archivos borrados	Número de archivos recuperados	Archivos recuperados legibles
Carpetas	0	33	0
Docx	1	1	0
Epub	1	1	1
Pdf	3	3	2
Winrar	1	1	0
Total	6	39	3

Tabla 3. 8 Lista de archivos recuperados por DFF

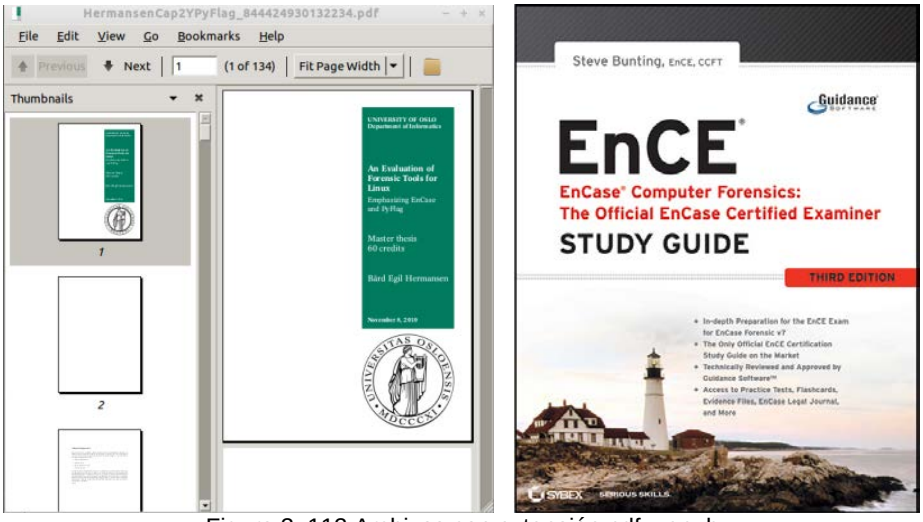


Figura 3. 112 Archivos con extensión pdf y epub

3.3.2 Dhash2 y Foremost

En el apartado anterior se describió el proceso de arranque de DEFT, la asignación de dispositivo en modo de solo lectura (para que no pueda ser modificado), el cálculo de hash y la adquisición de imagen con Dhash2 así como la comprobación de que la imagen no ha sido alterada por lo que se omitirá esta parte. A continuación se describe la recuperación de archivos con Foremost.

1) Para el proceso de recuperación se inició Foremost como se muestra en la figura 3.113.

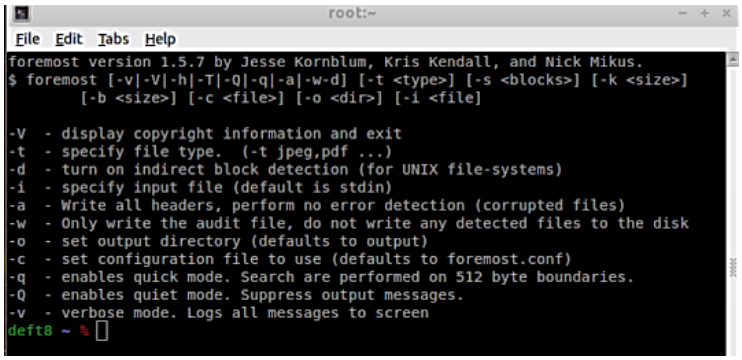


Figura 3. 113 Abrir Foremost

2) En el primer paso se cambió de directorio donde se localizaba la imagen creada anteriormente, esto fue a través del comando **cd**, ver figura 3.114. También se creó una carpeta que contendrá los archivos recuperados, en este caso llamada **recupSDG.**

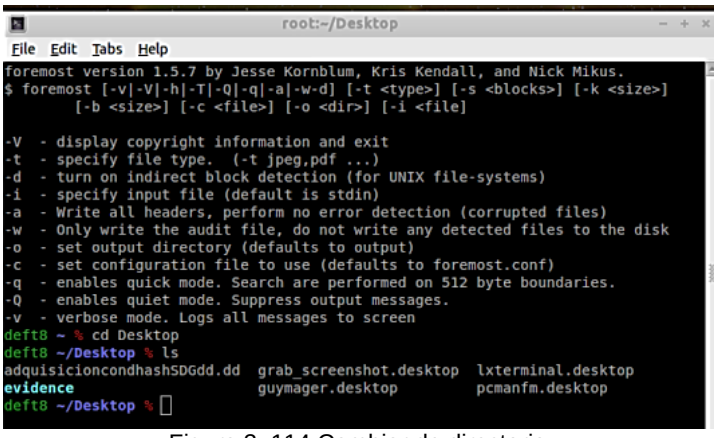


Figura 3. 114 Cambiar de directorio

3) En el siguiente paso se escribió el comando para proceder a la recuperación: foremost -t all -i adquisicioncondhashSDGdd.dd -o /root/Desktop/recupSDG, ver figura 3.115.

Donde -t all, indica el tipo de archivos a recuperar

-i adquisicioncondhashSDGdd.dd, indica la imagen de búsqueda

-o /root/Desktop/recupSDG, indica la carpeta donde guardará los archivos recuperados

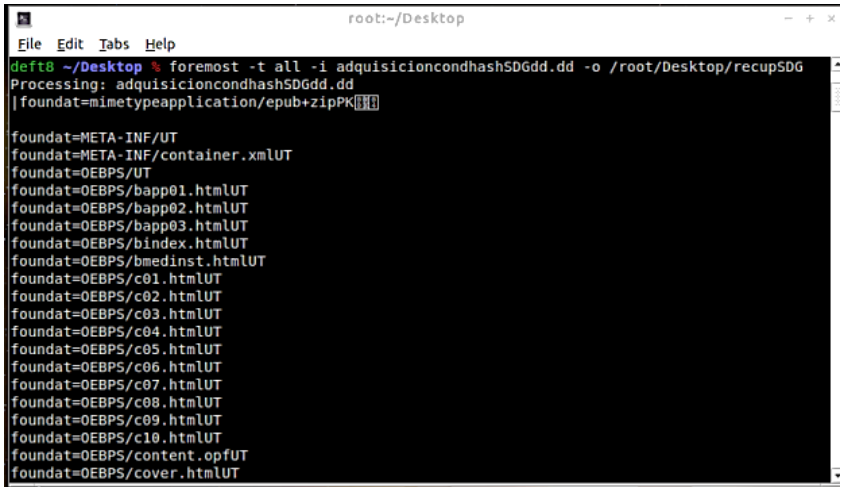


Figura 3. 115 Ejecutar comando para recuperar archivos

4) Se abrió la carpeta **recupSDG** para verificar que se guardaron los archivos recuperados, ver figura 3.116. Se observó que se recuperaron carpetas con diferente extensión y un archivo con extensión txt, este último contiene información acerca de los archivos recuperados, ver figura 3.117.

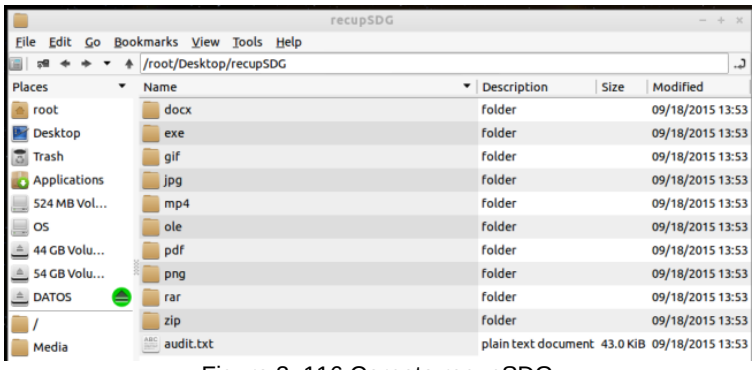


Figura 3. 116 Carpeta recupSDG

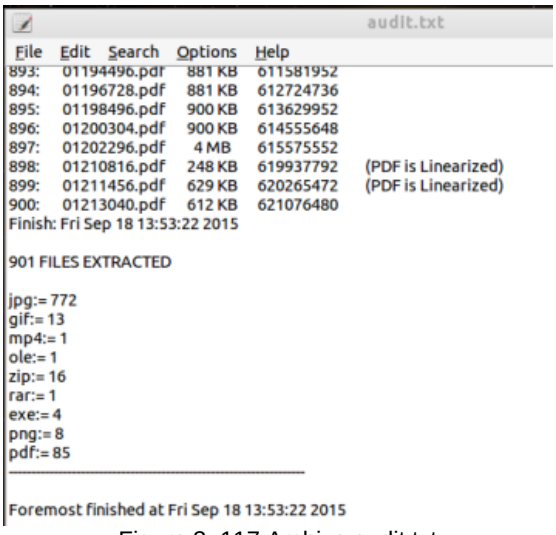


Figura 3. 117 Archivo audit.txt

Es necesario comprobar la recuperación total o parcial de los archivos, en este caso fue de 901 archivos como se muestra en la tabla 3.9. En las figuras 3.118 a 3.120 se muestran algunos fragmentos de las listas de archivos recuperados.

Tipo de archivo	Número de archivos borrados	Número de archivos recuperados	Archivos recuperados legibles
Docx	1	14	14
Exe	0	4	3
Gif	0	13	9
Jpeg	26	772	772
Mp4	0	1	0
Ole	0	1	1
Pdf	3	85	85
Png	0	8	8
Winrar	1	1	0
Zip	0	2	1
Total	31	901	893

Tabla 3. 9 Lista de archivos recuperados por Foremost

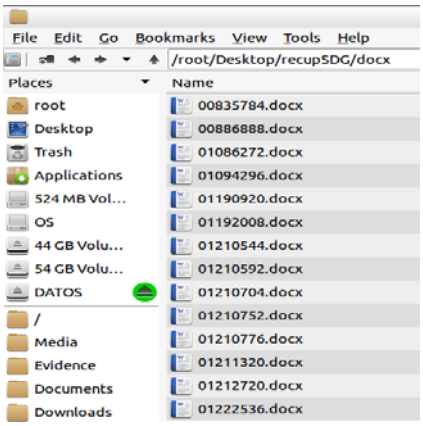


Figura 3. 118 Archivos con extensión docx

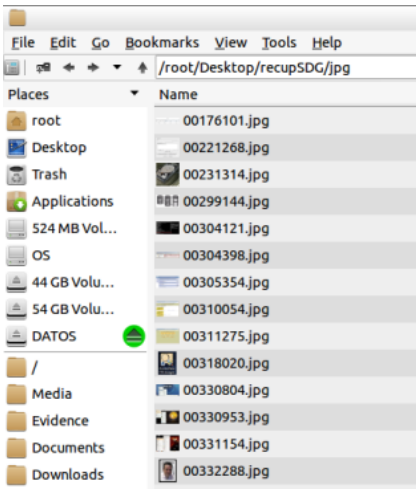


Figura 3. 119 Archivos con extensión jpeg

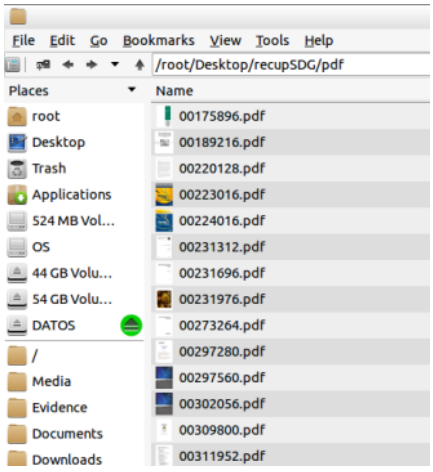


Figura 3. 120 Archivos con extensión pdf

3.3.3 Dhash2 y Autopsy

Los pasos seguidos para la adquisición de imagen y cálculo de hash (Dhash), son los mismos que en el apartado 3.3.1 donde se explica detalladamente cada uno de ellos, por lo que serán omitidos y solo se describirán los pasos más importantes del proceso de recuperación (Autopsy), considerando que esta herramienta ya fue utilizada en el apartado 3.1.3, en el cual solo sé recuperan los archivos fueron borrados.

Para comenzar con la recuperación de archivos se inició Autopsy. Tal como en la sección 3.1.3, se siguen los pasos del 5 a 13. En este caso en particular lo único diferente fue el nombre de la imagen como se muestra en la figura 3.121.

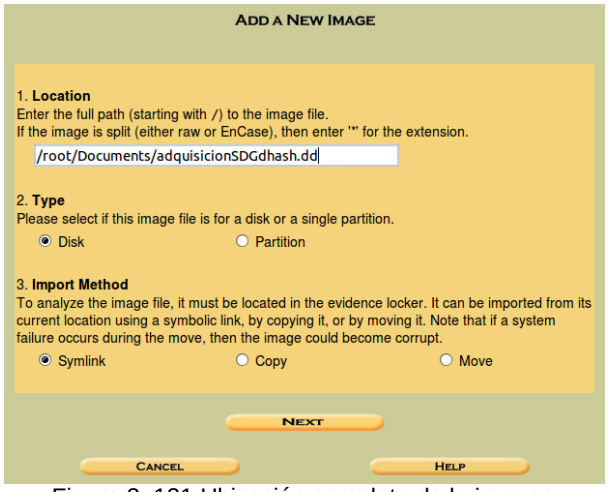


Figura 3. 121 Ubicación completa de la imagen

Es importante mencionar que Autopsy admite la creación de una línea de tiempo, esto es con la finalidad de visualizar todos los archivos localizados en la imagen (incluso los borrados), pero al pretender crearla en este caso se manda un mensaje indicando que la línea de tiempo es inválida. Debido a lo anterior no se logró crear la línea de tiempo como en el capítulo 3.1.3.

La tabla 3.10 muestra la lista de archivos que fueron recuperados por la herramienta Autopsy.

Tipo de archivo	Número de archivos borrados	Número de archivos recuperados	Archivos recuperados legibles
Docx	1	1	0
Epub	1	1	1
Jpeg	26	26	0
Pdf	3	3	2
Winrar	1	1	0
Total	32	32	3

Tabla 3. 10 Lista de archivos recuperados por Autopsy

3.3.4 Guymager y Foremost

Anteriormente se mencionó que Guymager realiza la adquisición de imagen con una interfaz gráfica, mientras que Foremost recupera archivos a través de una interfaz de línea de comandos. Los pasos seguidos para la adquisición de imagen son los mismos que en el apartado 3.1.3, considerando que el valor de hash se calculó con la herramienta Dhash2 y el formato de archivo seleccionado fue Exx. El proceso de recuperación con Foremost se realizó en el apartado 3.2.1, por lo que se omitirán algunos pasos del proceso y se mostraran los resultados obtenidos.

1) Después de abrir Guymager, se seleccionó el dispositivo evidencia y en el menú secundario, se eligió la opción adquisición de imagen como se muestra en la figura 3.122.

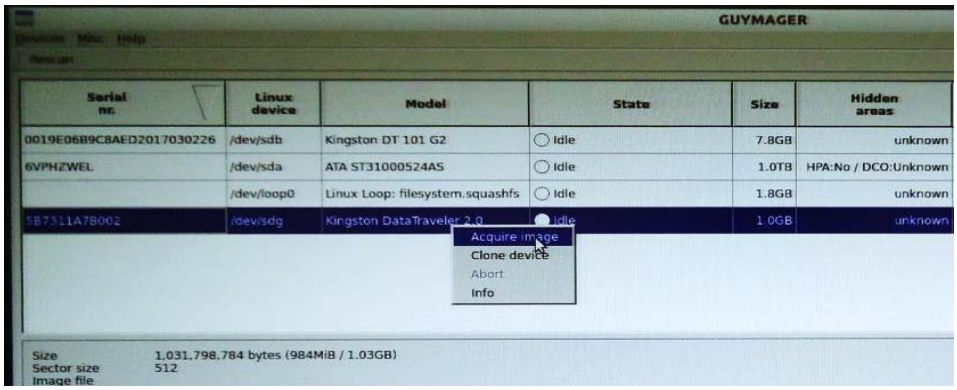


Figura 3. 122 Selección y elección de la opción de adquisición de imagen

2) Se mostró una ventana en la que se ingresaron datos como el formato del archivo (Exx), número de caso, nombre del examinador, una descripción y notas, directorio de imagen, nombre de archivo de imagen, cálculo/verificación de hash y verificar la imagen después de la adquisición para su verificación, ver figura 3.123.

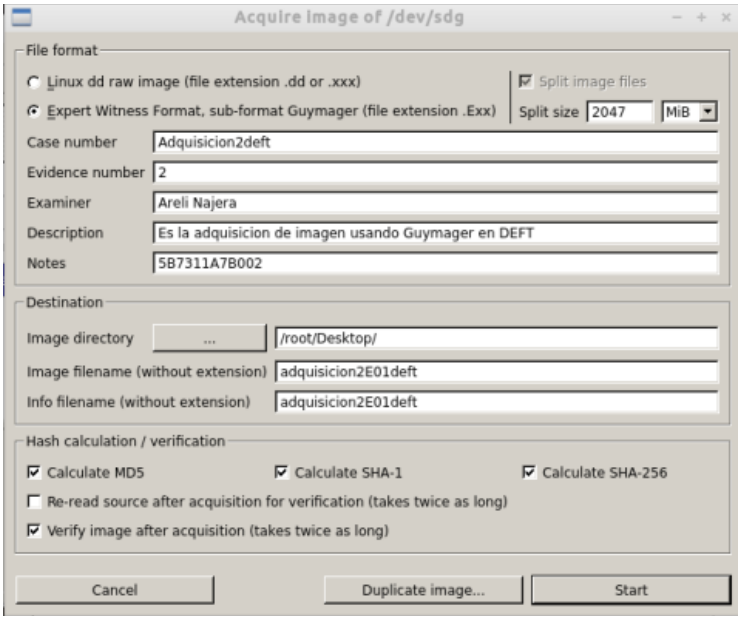


Figura 3. 123 Datos ingresados para el proceso de adquisición

3) Cuando se creó la imagen también se generó un archivo con extensión info, el cual contiene información acerca del proceso. Con el archivo de información se verificó que el hash de la imagen y el hash del dispositivo evidencia son iguales, es decir, se comprobó que la imagen no fue alterada, ver figura 3.124.

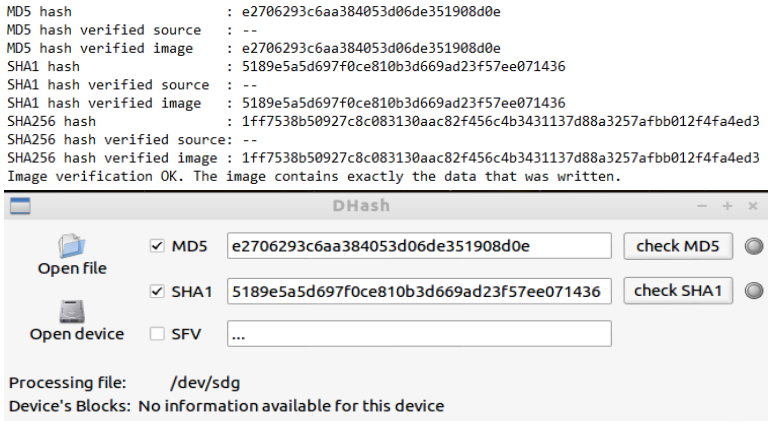


Figura 3. 124 Comparación del hash de la imagen y del dispositivo evidencia

4) Para el proceso de recuperación se abrió Foremost, primero se cambió de directorio a donde se localiza la imagen creada anteriormente, esto fue a través del comando: cd. También se creó una carpeta que contendrá a los archivos recuperados, en este caso llamada **recupE01foremost** (no es necesario crear la carpeta ya que Foremost le asigna una automáticamente). Por último se escribió el comando en la interfaz de línea de comandos para la recuperación: foremost -t all -i adquisicioncondhashSDGdd.dd -o /root/Desktop/recupE01foremost, ver figura 3.125.

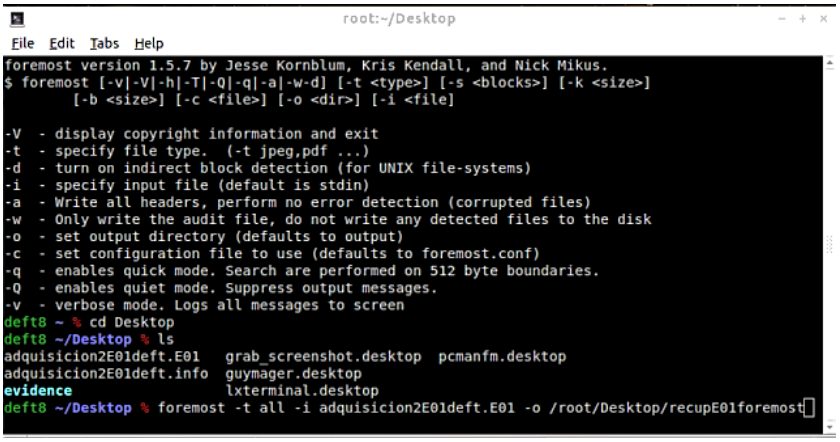


Figura 3. 125 Proceso de recuperación con Foremost

5) Se abrió la carpeta de recuperación para verificar los archivos recuperados. Por otro lado, se observó que se generó un archivo con extensión de texto txt, este último contiene información acerca de los archivos recuperados, ver figura 3.126.

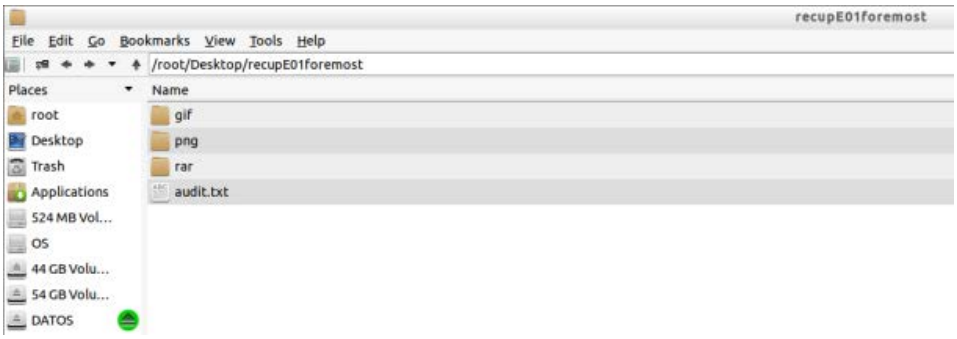


Figura 3. 126 Carpeta que contiene los archivos recuperados con la herramienta Foremost

Es necesario comprobar la recuperación total o parcial de los archivos, por lo que en la tabla 3.11 se enlista cada uno de los archivos. La figura 3.127 muestra el único archivo recuperado legible es de extensión png.

Tipo de archivo	Número de archivos borrados	Número de archivos recuperados	Archivos recuperados legibles
Gif	0	1	0
Png	0	1	1
Winrar	1	1	0
Total	1	3	1

Tabla 3. 11 Lista de archivos recuperados por Foremost

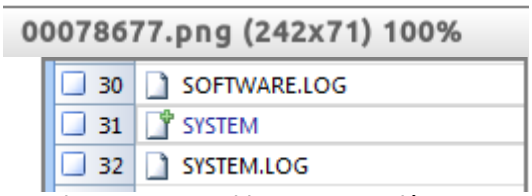


Figura 3. 127 Archivo con extensión png

3.3.5 Guymager y DFF

En el apartado anterior se describió el proceso para realizar la adquisición de imagen con formato Exx; por otro lado, la herramienta que se usó para la recuperación de archivos es

DFF la cual se describió en el apartado 3.3.1 por lo cual se omitirán los pasos para hacer la recuperación y solo se mostraran los resultados obtenidos.

En la tabla 3.12 se muestra la lista de los archivos recuperados por la herramienta DFF.

Tipo de archivos	Número de archivos borrados	Número de archivos recuperados	Archivos recuperados legibles
Carpetas	0	33	0
Docx	1	1	0
Epub	1	1	1
Pdf	3	3	2
Winrar	1	1	0
Total	6	39	3

Tabla 3. 12 Lista de archivos recuperados por DFF

3.3.6 Guymager y Autopsy

En este apartado los pasos seguidos en el proceso de adquisición de imagen, son los mismos que en el apartado 3.3.4; en el caso de la recuperación de archivos se utilizó Autopsy, herramienta que se describió en el apartado 3.1.3, por lo que se omitirán la mayoría de los pasos.

1) En el momento en que se creó la imagen también se generó un archivo con extensión info, el cual contiene información acerca del proceso. Se realizó la comparación del hash de la imagen con el hash del dispositivo evidencia y se determinó que ambos son iguales, por lo tanto la imagen no ha sido alterada, ver figura 3.128.

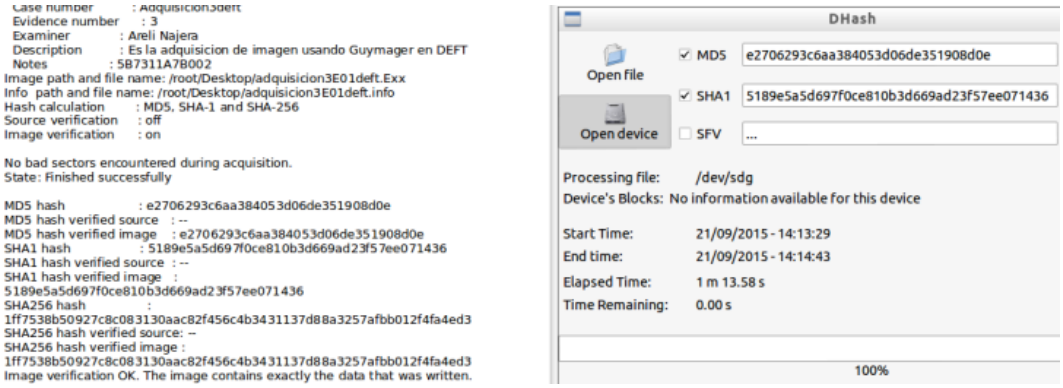


Figura 3. 128 Comparación del hash de la imagen y del dispositivo evidencia

2) En el caso del proceso de recuperación se inició Autopsy. Tal como en la sección 3.1.3 se siguieron los pasos del 5 al 8.

   En la siguiente ventana se ingresaron los datos de ruta de la imagen con la opción **Location**, se indicó que la imagen está contenida en todo el disco y no en una partición con la opción **Disk**, en el caso de método de importación se selecciona la opción **Symlink** (ya que la opción **Move** podría ocasionar alteraciones en la imagen) y por último se presionó la opción **Next**, ver figura 3.129.

   Después se mostró una ventana en la que confirma que la imagen ha sido dividida y la ruta completa de la imagen, ver figura 3.130.

Figura 3. 129 Ubicación completa de la imagen

Figura 3. 130 Confirmar imagen dividida

3) Dado que anteriormente se agregó el archivo imagen se seleccionó el volumen para analizar **C: /**, en este caso se consideró el tipo de sistema de archivo que contenía el dispositivo evidencia (fat32), ver figura 3.131. En el siguiente paso se eligió la opción **Image Integrity** para verificar que la imagen no fue modificada, pero no fue posible debido al tipo de formato de la imagen E01 (figura 3.132), por lo que se seleccionó la opción **Close**.

Figura 3. 131 Selección de volumen C: /

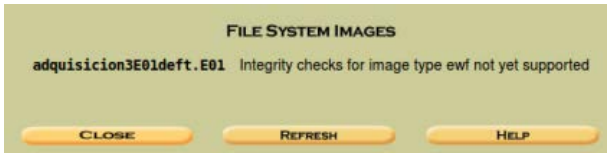


Figura 3. 132 No se realiza el cálculo de hash por el tipo de formato de la imagen

Los pasos del 11 al 13 son los mismos que en el apartado 3.1.3. Es importante mencionar que Autopsy puede generar la línea de tiempo, esto con la finalidad de visualizar todos los archivos localizados en la imagen (incluyendo los archivos borrados), pero al pretender visualizarla se envía un mensaje que indica que la línea de tiempo es inválida.

La lista de archivos recuperados con la herramienta Autopsy se muestra en la tabla 3.13.

Tipo de archivo	Número de archivos borrados	Número de archivos recuperados	Archivos recuperados legibles
Docx	1	1	0
Epub	1	1	1
Jpeg	26	26	0
Pdf	3	3	2
Winrar	1	1	0
Total	32	32	3

Tabla 3. 13 Lista de archivos recuperados por Autopsy

3.4 Recuperación de archivos con la herramienta CAINE a diferentes medios de almacenamiento

En este apartado se realiza la recuperación de archivos con CAINE ya que realiza la recuperación de mayor número de archivos legibles con las herramientas Guymager y Photorec, esto con la finalidad de comparar diferentes medios de almacenamiento (CD-RW, DVD-RW, USB y disco duro externo). Para realizar una comparación equitativa entre los diferentes medios se usaron los mismos archivos.

El CD-RW se consideró como evidencia por lo que se realizó la clonación hacia un dispositivo USB de 1 GB, y de éste la recuperación de archivos. La tabla 3.14 muestra la lista de archivos que fueron borrados y recuperados legibles en el caso del CD-RW.

CD-RW			
Tipo de archivo	Número de archivos borrados	Número de archivos recuperados	Numero de archivos legibles
Avi	1	1	1
Docx	1	1	1
Epub	1	0	0

Exe	1	1	0
Info	1	1	1 (incompleto)
Iso	1	0	0
Jpeg	3	3 (duplicadas)	3 (duplicadas)
Mp3	1	1	1
Pdf	3	3	3
Png	1	0	0
Winrar (Docx)	1	1	1
Winrar (Exe)	1	1	1
Winrar (Jpeg)	1	1	1
Winrar (Pdf)	1	1	1
Winzip (Docx)	1	0	0
Winzip (Exe)	1	1	1
Winzip (Jpeg)	1	1	1
Winzip (Pdf)	1	1	1
Wmv	1	1	1
Xlsx	1	1	1
Total	24	20	19

Tabla 3. 14 Lista de archivos recuperados por Photorec de un CD-RW

En el siguiente caso se consideró el DVD-RW como evidencia y la clonación se realizó en un dispositivo USB de 8 GB, la tabla 3.15 muestra la lista de archivos recuperados de éste caso.

DVD-RW			
Tipo de archivo	Número de archivos borrados	Número de archivos recuperados	Numero de archivos legibles
Avi	1	1	1
Docx	1	1	1
Epub	1	0	0

Exe	1	1	0
Info	1	1	1 (incompleto)
Iso	1	0	0
Jpeg	3	3 (duplicadas)	3 (duplicadas)
Mp3	1	1	1
Pdf	3	3	3
Png	1	1	1
Winrar (Docx)	1	1	1
Winrar (Exe)	1	1	1
Winrar (Jpeg)	1	1	1
Winrar (Pdf)	1	1	1
Winzip (Docx)	1	1	1
Winzip (Exe)	1	1	1
Winzip (Jpeg)	1	1	1
Winzip (Pdf)	1	1	1
Wmv	1	1	1
Xlsx	1	1	1
Total	24	22	21

Tabla 3. 15 Lista de archivos recuperados por Photorec de un DVD-RW

El siguiente medio fue el disco duro externo que se utilizó como evidencia y se realizó la clonación en un disco duro externo de 1 TB. La tabla 3.16 muestra la lista de archivos recuperados del disco duro externo.

Disco duro externo			
Tipo de archivo	Número de archivos borrados	Número de archivos recuperados	Numero de archivos legibles
Avi	1	1	1
Docx	1	1	1
Epub	1	0	0

Exe	1	1	0
Info	1	1	1 (incompleto)
Iso	1	0	0
Jpeg	3	3 (duplicadas)	3 (duplicadas)
Mp3	1	1	1
Pdf	3	3	3
Png	1	1	1
Winrar (Docx)	1	1	1
Winrar (Exe)	1	1	1
Winrar (Jpeg)	1	1	1
Winrar (Pdf)	1	1	1
Winzip (Docx)	1	1	1
Winzip (Exe)	1	1	1
Winzip (Jpeg)	1	1	1
Winzip (Pdf)	1	1	1
Wmv	1	1	1
Xlsx	1	1	1
Total	24	22	21

Tabla 3. 16 Lista de archivos recuperados por Photorec de un disco duro externo

Finalmente, se usó un dispositivo USB como evidencia por lo que se realizó la clonación en un dispositivo USB de 1 GB. La tabla 3.17 muestra la lista de archivos recuperados de este dispositivo. A diferencia de la tabla 3.3 se observa que en este caso, la recuperación de archivo de formato EXE no se obtuvo; mientras que para los formatos Docx, Jpeg, Pdf y Winrar se realizó la recuperación de archivos legibles en ambos procesos.

USB			
Tipo de archivo	Número de archivos borrados	Número de archivos recuperados	Numero de archivos legibles
Avi	1	1	1
Docx	1	1	1
Epub	1	0	0
Exe	1	1	0
Info	1	1	1 (incompleto)
Iso	1	0	0
Jpeg	3	3 (duplicadas)	3 (duplicadas)
Mp3	1	1	1
Pdf	3	3	3
Png	1	1	1
Winrar (Docx)	1	1	1
Winrar (Exe)	1	1	1
Winrar (Jpeg)	1	1	1
Winrar (Pdf)	1	1	1
Winzip (Docx)	1	1	1
Winzip (Exe)	1	1	1
Winzip (Jpeg)	1	1	1
Winzip (Pdf)	1	1	1
Wmv	1	1	1
Xlsx	1	1	1
Total	24	22	21

Tabla 3. 17 Lista de archivos recuperados por Photorec de un USB

Capítulo 4

Evaluación de herramientas para análisis forense de medios de almacenamiento

En este capítulo se presentan los resultados obtenidos de la aplicación de las herramientas CAINE, HELIX 3 y DEFT para el análisis forense de medios de almacenamiento. Estos resultados sirven para evaluar estas herramientas tomando como parámetro de desempeño su capacidad para recuperar archivos y datos como fuente de evidencia digital.

En el capítulo anterior se describió en forma detallada el análisis forense de medios de almacenamiento utilizando tres diferentes herramientas de uso libre. Los procedimientos realizados estuvieron orientados a recuperar archivos y datos de prueba intencionalmente eliminados previamente. Al utilizar cada una de las herramientas se pudo observar que la capacidad para recuperar las evidencias eliminadas varía de una herramienta a otra.

4.1 Resultados obtenidos

Como puede observarse en la tabla 4.1, la herramienta CAINE es la que demostró una mejor capacidad para recuperar la información usando de manera combinada sus componentes Guymager y Photorec. En el caso de las herramientas HELIX 3 y DEFT, aún utilizando todos sus componentes de manera conjunta, no permiten recuperar la información eliminada, y en algunos casos, permiten recuperar el archivo, pero con daño total o parcial en su formato de tal manera que no es posible leer su contenido.

Software	Herramientas		Archivos borrados						
	Proceso de adquisición /clonación	Proceso de recuperación	Archivo de texto Docx	Archivo de lectura Epub	Archivo ejecutable comprimido (Winrar)	Archivo multimedia de imagen (Jpeg)	Archivo de lectura Pdf 1	Archivo de lectura Pdf 2	Archivo de lectura Pdf 3
CAINE	Guymager	Photorec	R	NR	NR	R	R	R	R
		Autopsy	NR	R	NR	NR	R	NR	R
HELIX	Adepto	Foremost	NR	NR	NR	R	R	R	R
DEFT	Dhash2	DFF	NR	R	NR	NR	R	NR	R
		Foremost	R	R	NR	NR	R	R	R
		Autopsy	NR	R	NR	NR	R	NR	R
		Foremost	NR	NR	NR	NR	NR	NR	NR

	Guymager								
		DFF	NR	R	NR	NR	R	NR	R
		Autopsy	NR	R	NR	NR	R	NR	R

Tabla 4. 1 Evaluación de herramientas para análisis forense de medios de almacenamiento. Considérese R: Recuperado, NR: No Recuperado, incluye archivos recuperados pero no legibles

Por otro lado, la tabla 4.2 muestra los tiempos requeridos por cada herramienta para realizar la recuperación de archivos. Como puede observarse, la herramienta con el menor tiempo de análisis fue DEFT, misma que también presenta un buen desempeño en relación a la cantidad de archivos recuperados. En el caso de la herramienta HELIX, presenta el mayor tiempo de análisis y, aparentemente recupera una mayor cantidad de archivos que las otras dos herramientas. Sin embargo, los resultados obtenidos muestran que la mayor parte de archivos recuperados contienen información no legible que no coincide con las evidencias esperadas. Debido a esto, la herramienta CAINE, a pesar de no ser la más veloz, es la herramienta con el mejor desempeño, tomando en cuenta la cantidad de evidencias recuperadas que pueden mostrar su contenido.

Software	Herramienta para el proceso de clonación y/o adquisición	Duración del proceso (h:m:s)	Herramienta para el proceso de recuperación	Duración del proceso (h:m:s)	Número de archivos recuperados
CAINE	Guymager (clonación de dispositivo)	00:02:57	Photorec	00:00:50	224
	Guymager (adquisición de imagen con formato dd)	00:01:24	Autopsy	00:05:55	33
HELIX	Adepto (adquisición de imagen con formato .dd y clonación de dispositivo)	00:06:09	Foremost	00:01:10	1012
DEFT	Dhash2 (adquisición de imagen con formato dd)	00:00:03	DFF	00:06:11	10
			Foremost	00:00:07	901
			Autopsy	00:06:23	35

	Guymager (adquisición de imagen con formato E01)	00:00:24	Foremost	00:01:24	3
			DFF	00:03:00	10
			Autopsy	00:04:25	34

Tabla 4. 2 Tiempo de análisis para cada herramienta

Para tener un panorama general sobre la capacidad de recuperación de los archivos que fueron borrados, se calculó el total en MB de los archivos borrados, después se calculó el porcentaje que representa cada tipo de archivo de ese total, ver tabla 4.3 y figura 4.1.

Archivo	Extensión del archivo	Tamaño en Megabytes	Porcentaje del total (%)
Archivo de lectura 1	Pdf	36.8	4.49
Archivo de lectura 2			4.51 10.93
Archivo de lectura 3			1.93
Archivo de lectura	Epub	81.8	24.29
Archivo multimedia de imagen (26 archivos)	Jpeg	120	35.63
Archivo ejecutable comprimido	Winrar (exe)	96.6	28.68
Archivo de texto	Docx	1.6	0.47
Total	32	336.8	100

Tabla 4. 3 Porcentaje de megabytes usados en el proceso de recuperación por tipo de archivo

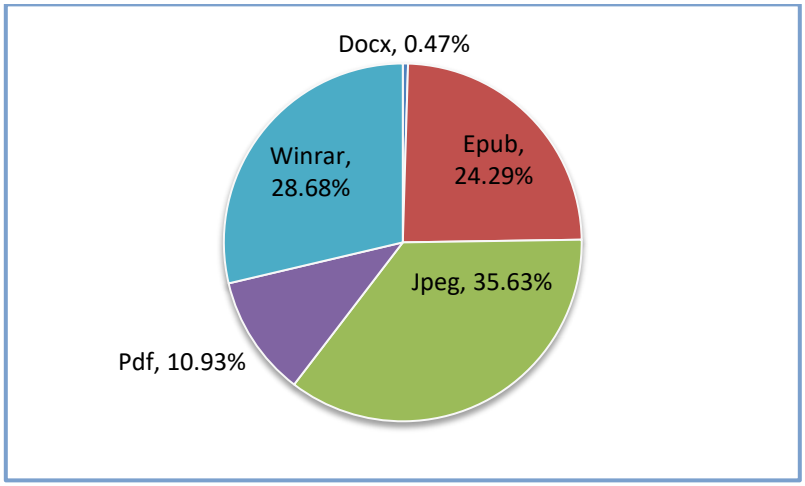


Figura 4. 1 Gráfica del porcentaje de megabytes usados en el proceso de recuperación por tipo de archivo

De la tabla 4.4 a la tabla 4.13, se indican los porcentajes de los archivos recuperados con cada una de las herramientas, junto con su respectiva gráfica. La tabla presenta el número de archivos borrados, el número de archivos recuperados, el porcentaje del número de archivos recuperados con respecto al número de archivos así como el porcentaje total de megabytes recuperados por tipo de archivo. En la tabla 4.4 se observa que la herramienta Guymager-Photorec recupera todos los archivos multimedia con extensión jpeg, sin embargo no es capaz de recuperar archivos con formato comprimido como Winrar.

En las figuras 4.3, 4.5, 4.7, 4.9 y 4.10 se observa que las herramientas DFF y Autopsy recuperan el mismo número de archivos, con extensión epub y pdf. La tabla 4.6 muestra que la herramienta Adepto-Foremost solo recupera los archivos de lectura con extensión pdf y los archivos multimedia de imagen con extensión jpeg.

La figura 4.6 indica que la herramienta Dhash2-Foremost recupera todos los archivos de lectura con extensión epub y pdf, aunque no recupera archivos multimedia de imagen con extensión jpeg. En la tabla 4.10 se observa que la herramienta Guymager-Foremost no es capaz de recuperar ningún archivo de los que fueron borrados para tal propósito (archivos con extensión epub, pdf, docx, jpeg, winrar).

Guymager – Photorec				
Extensión del archivo	Archivos borrados	Archivos recuperados legibles	% de archivos recuperados	% de megabytes recuperados con respecto al total
Docx	1	1	100	0.47
Epub	1	0	0	0
Jpeg	26	26	100	35.63
Pdf	3	3	100	10.93
Winrar	1	0	0	0
Total	32	30	-	47.03

Tabla 4. 4 Porcentaje de Guymager-Photorec

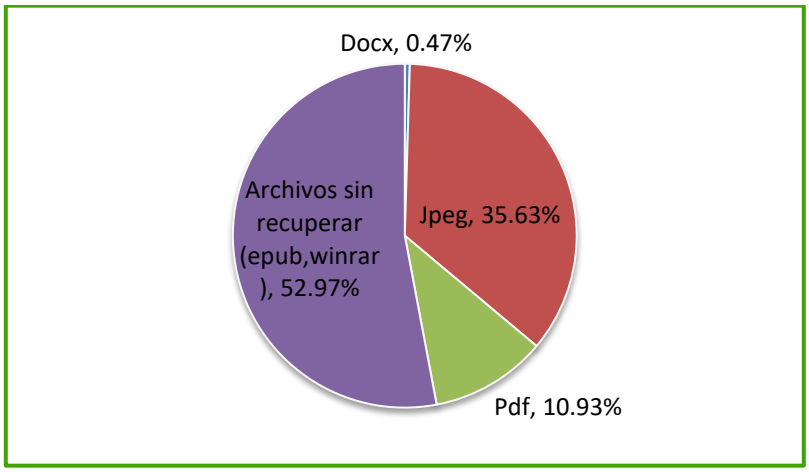


Figura 4. 2 Gráfica de porcentaje de Guymager-Photorec

Guymager – Autopsy				
Extensión del archivo	Archivos borrados	Archivos recuperados legibles	% de archivos recuperados	% de megabytes recuperados con respecto al total
Docx	1	0	0	0
Epub	1	1	100	24.29
Jpeg	26	0	0	0
Pdf	3	2	66.66	6.42
Winrar	1	0	0	0
Total	32	3	-	30.71

Tabla 4. 5 Porcentaje de Guymager-Autopsy

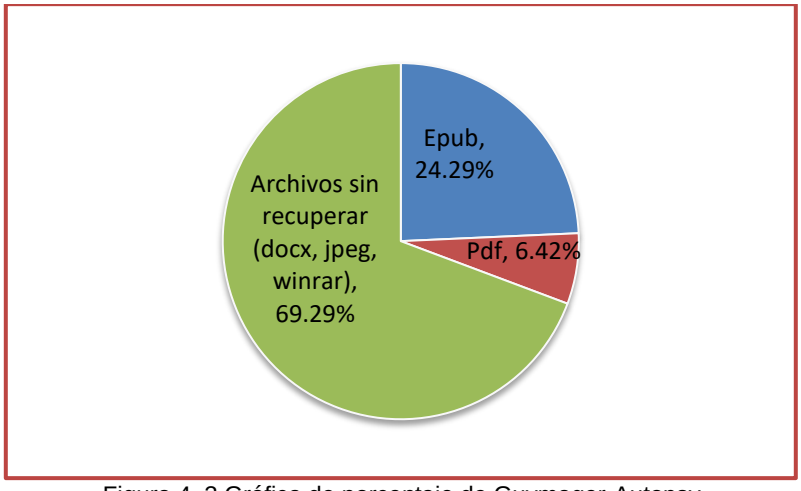


Figura 4. 3 Gráfica de porcentaje de Guymager-Autopsy

Adepto – Foremost				
Extensión del archivo	Archivos borrados	Archivos recuperados legibles	% de archivos recuperados	% de megabytes recuperados con respecto al total
Docx	1	0	0	0
Epub	1	0	0	0
Jpeg	26	26	100	35.63
Pdf	3	3	100	10.93
Winrar	1	0	0	0
Total	32	29	-	46.56

Tabla 4. 6 Porcentaje de Adepto–Foremost

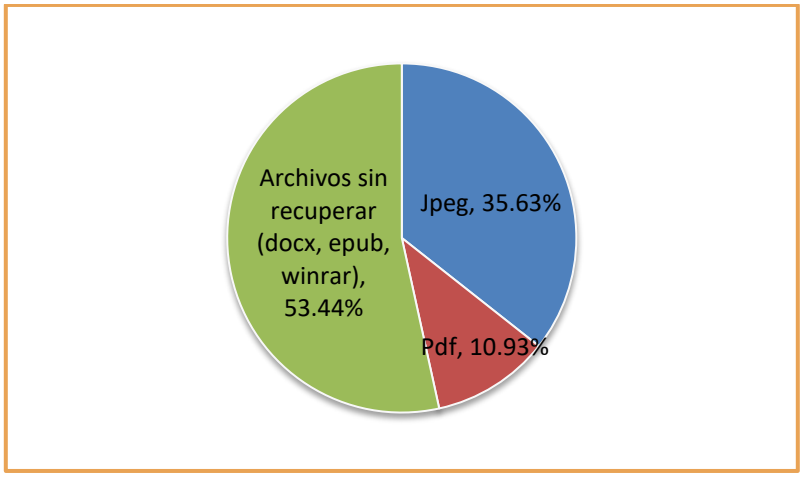


Figura 4. 4 Gráfica de porcentaje de Adepto-Foremost

Dhash2 – DFF				
Extensión del archivo	Archivos borrados	Archivos recuperados legibles	% de archivos recuperados	% de megabytes recuperados con respecto al total
Docx	1	0	0	0
Epub	1	1	100	24.29
Jpeg	26	0	0	0
Pdf	3	2	66.66	6.42
Winrar	1	0	0	0
Total	32	3	-	30.71

Tabla 4. 7 Porcentaje de Dhash2-DFF

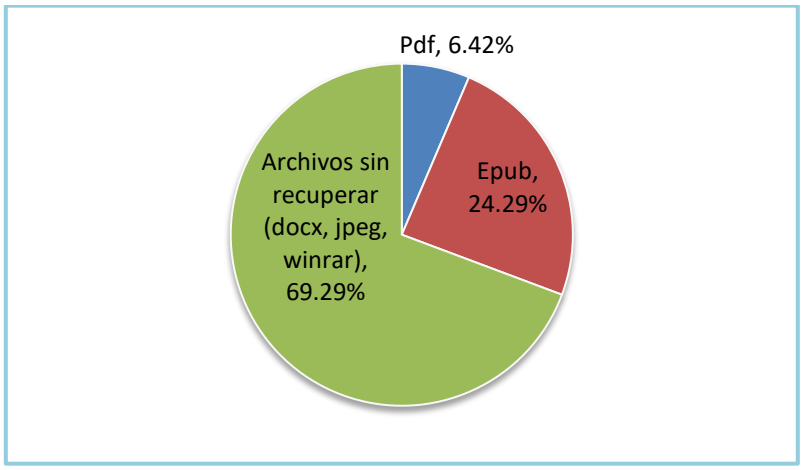


Figura 4. 5 Gráfica de porcentaje de Dhash2-DFF

Dhash2 – Foremost				
Extensión del archivo	Archivos borrados	Archivos recuperados legibles	% de archivos recuperados	% de megabytes recuperados con respecto al total
Docx	1	1	100	0.47
Epub	1	1	100	24.29
Jpeg	26	0	0	0
Pdf	3	3	100	10.93
Winrar	1	0	0	0
Total	32	5	-	35.69

Tabla 4. 8 Porcentaje de Dhash2-Foremost

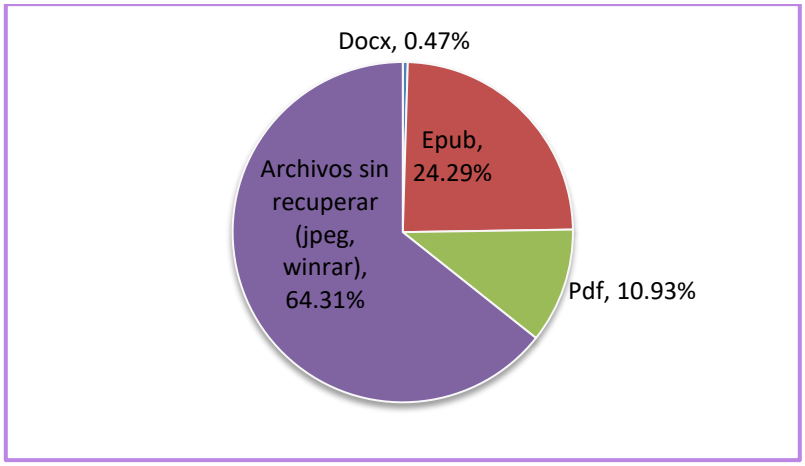


Figura 4. 6 Gráfica de porcentaje de Dhash2-Foremost

Dhash2 – Autopsy				
Extensión del archivo	Archivos borrados	Archivos recuperados legibles	% de archivos recuperados	% de megabytes recuperados con respecto al total
Docx	1	0	0	0
Epub	1	1	100	24.29
Jpeg	26	0	0	0
Pdf	3	2	66.66	6.42
Winrar	1	0	0	0
Total	32	3	-	30.71

Tabla 4. 9 Porcentaje de Dhahs2-Autopsy

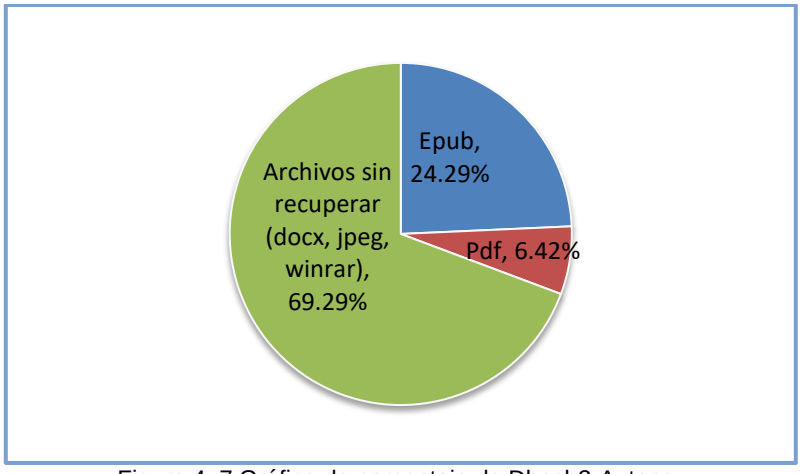


Figura 4. 7 Gráfica de porcentaje de Dhash2-Autopsy

Guymager – Foremost				
Extensión del archivo	Archivos borrados	Archivos recuperados legibles	% de archivos recuperados	% de megabytes recuperados con respecto al total
Docx	1	0	0	0
Epub	1	0	0	0
Jpeg	26	0	0	0
Pdf	3	0	0	0
Winrar	1	0	0	0
Total	32	0	-	0

Tabla 4. 10 Porcentaje de Guymager-Foremost

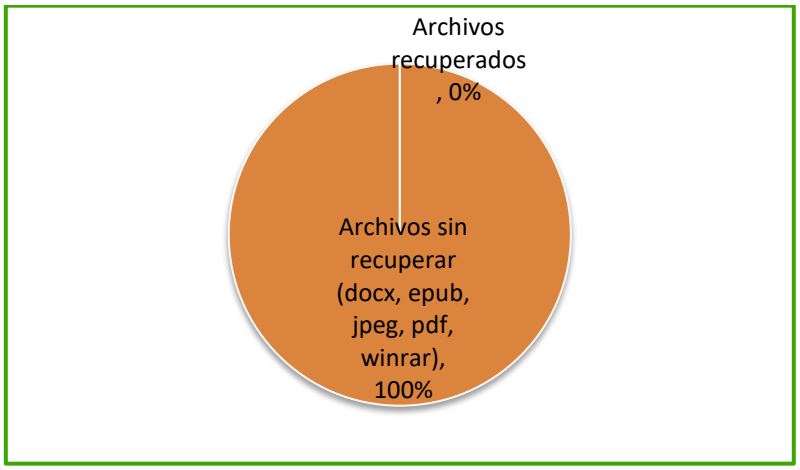


Figura 4. 8 Gráfica de porcentaje de Guymager-Foremost

Guymager – DFF				
Extensión del archivo	Archivos borrados	Archivos recuperados legibles	% de archivos recuperados	% de megabytes recuperados con respecto al total
Docx	1	0	0	0
Epub	1	1	100	24.29
Jpeg	26	0	0	0
Pdf	3	2	66.66	6.42
Winrar	1	0	0	0
Total	32	3	-	30.71

Tabla 4. 11 Porcentaje de Guymager-DFF

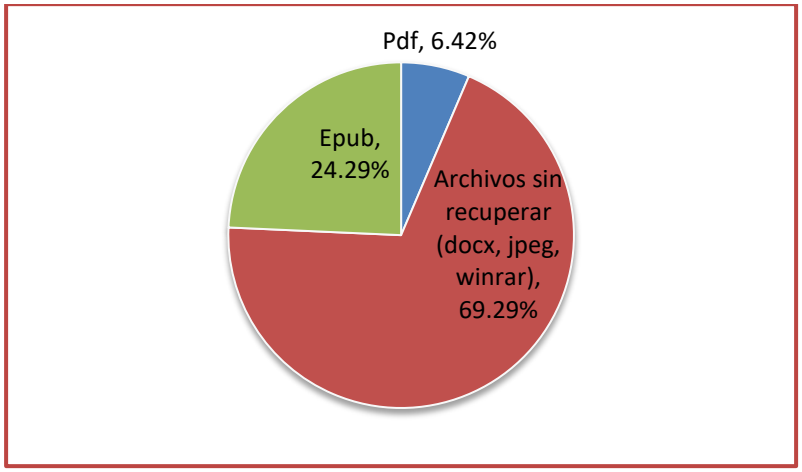


Figura 4. 9 Gráfica de porcentaje de Guymager-DFF

Guymager – Autopsy				
Extensión del archivo	Archivos borrados	Archivos recuperados legibles	% de archivos recuperados	% de megabytes recuperados con respecto al total
Docx	1	0	0	0
Epub	1	1	100	24.29
Jpeg	26	0	0	0
Pdf	3	2	66.66	6.42
Winrar	1	0	0	0
Total	32	3	-	30.71

Tabla 4. 12 Porcentaje de Guymager-Autopsy

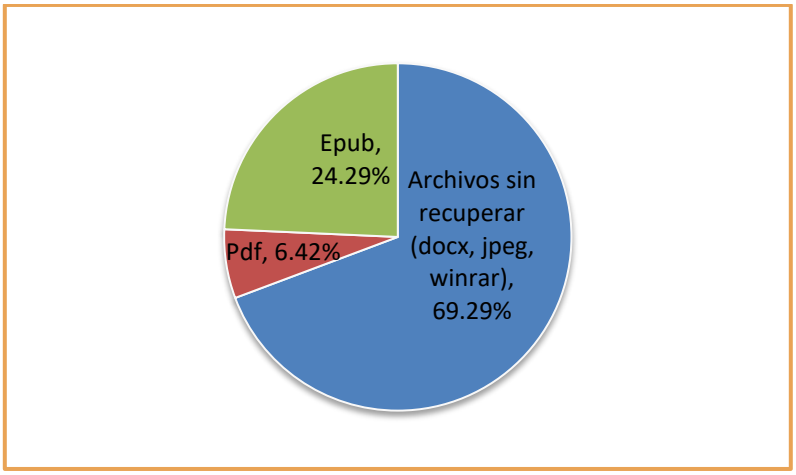


Figura 4. 10 Gráfica de porcentaje de Guymager-Autopsy

La tabla 4.13 muestra el **porcentaje de megabytes total** recuperado de las herramientas (se incluyen todos los archivos recuperados, independientemente de su tipo), se puede observar que **Guymager-Photorec recupero más archivos legibles**, en caso contrario de **Guymager-Foremost que no recupero ningún archivo de los que fueron borrados**. Además, la herramienta DFF y Autopsy recuperaron los mismos archivos (usando Caine y DEFT).

Herramientas	% de megabytes total recuperado
Guymager - Photorec	47.03
CAINE	

	Guymager - Autopsy	30.71
HELIX	Adepto - Foremost	46.56
DEFT	Dhash2 - DFF	30.71
	Dhash2 - Foremost	35.69
	Dhash2 - Autopsy	30.71
	Guymager - Foremost	0
	Guymager - DFF	30.71
	Guymager - Autopsy	30.71

Tabla 4. 13 Porcentaje de recuperación total por herramienta

Con respecto a la recuperación de archivos de diferentes medios de almacenamiento usando las herramientas de Caine (Guymager y Photorec), la tabla 4.14 muestra el número de archivos legibles recuperados. Se puede observar que el DVD-RW, USB y disco duro externo recuperaron el mismo número de archivos.

Medio de almacenamiento	Número de archivos borrados	Número de archivos recuperados legibles
CD-RW	24	19
DVD-RW	24	21
USB	24	21
Disco duro externo	24	21

Tabla 4. 14 Lista de archivos recuperados de los diferentes medios de almacenamiento

Por último, la tabla 4.15 muestra una comparación de duración de los procesos realizados en los diferentes medios de almacenamiento. Como se puede observar, debido a la gran cantidad de almacenamiento de disco duro externo, ambos procesos fueron los que tardaron horas en finalizar; mientras que para el DVD-RW y USB solo tardaron algunos minutos en los dos procesos.

Medio de almacenamiento		Duración del proceso de clonación (Guymager) **(h:m:s)**	Duración del proceso de recuperación (Photorec) **(h:m:s)**
Evidencia	Dispositivo de clonación		
CD-RW	USB (1 GB)	03: 47: 40	00: 01: 30
DVD-RW	USB (8 GB)	00: 04: 58	00: 07: 54
USB	USB (1 GB)	00: 09: 12	00: 01: 46
Disco duro externo	Disco duro externo (1 TB)	20: 40: 43	09: 00: 26

Tabla 4. 15 Duración del proceso de clonación y recuperación

4.2 Análisis de resultados

La herramienta que realizó la adquisición de imagen (.dd) en menor tiempo es **Dhash2** (contenida en el entorno DEFT), además de que calcula el hash del dispositivo y de la imagen, mientras que la herramienta que tardó menos tiempo en recuperar los archivos fue **Foremost** (incluida en el ambiente DEFT) y la herramienta que recuperó más archivos fue **Foremost** (contenida en el entorno Helix). Cabe mencionar que en los casos en que el número de archivos es muy grande alrededor de mil archivos, la mayoría de los archivos se recuperan al menos dos veces. Por otro lado, ninguna de las herramientas usadas fue capaz de recuperar un archivo ejecutable comprimido como Winrar.

Es importante considerar que Guymager y Photorec (ambos de Caine) recuperaron la mayoría de los archivos que fueron borrados en un 47.03%, en el caso de Guymager-Foremost (DEFT) no se recuperó ningún archivo borrado.

Con respecto a los diferentes medios de almacenamiento se comprobó que el DVD-RW, USB y el disco duro externo recuperaron los mismos archivos legibles (winrar, winzip, pdf, docx, jpeg, png, avi, mp3, wmv, xlxs), mientras que los tipos de formato sin recuperar en los tres casos son exe, iso y epub.

CONCLUSIONES

El análisis forense tiene la finalidad de esclarecer delitos informáticos, en particular solo se consideró la información que puede ser recuperada de los diferentes medios de almacenamiento que actualmente se utilizan.

Las tres herramientas usadas recuperaron archivos borrados, pero aproximadamente el 50% de los archivos tienen el formato dañado o corrupto por lo que no es posible visualizarlos. Por ello, de acuerdo a los resultados obtenidos se recomienda realizar la clonación de dispositivo con Guymager y su respectiva recuperación de archivos con Photorec, ambas contenidas en Caine.

Las herramientas Adepto y Dhash tienen un desempeño eficaz para una clonación de dispositivo, ambas contienen la opción de bloqueo contra escritura con lo que se comprueba que la copia del medio de almacenamiento no ha sido alterada. En el caso del proceso de recuperación las herramientas Foremost, DFF y Autopsy no ofrecen un adecuado desempeño ya que la mayoría de los archivos recuperados no son legibles ya que están dañados.

Con los resultados obtenidos al realizar la evaluación de herramientas para análisis forense de medios de almacenamiento, se concluye que la herramienta que cumple con el mejor desempeño tanto en la clonación como en la recuperación de archivos es Caine.

REFERENCIAS

[1] FBI. Forensic Science Communications [en línea]; USA, Octubre de 2000 [Consulta: Septiembre 2015] Disponible en: <https://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/oct2000/index.htm/computer.htm>

[2] FBI. Forensic Science Communications [en línea]; USA, Abril de 2000 [Consulta: Marzo 2015] Disponible en: <https://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm/>

[3] Álvarez G., María D. Capítulo 3. Fases de la Informática Forense [en línea]; 2010. [Consulta: Marzo 2015] Disponible: <http://documents.mx/documents/capitulo3pdf-5618160413f5d.html>

[4] Bunting, S. Anson, S. Mastering. Windows Network Forensics and Investigation [en línea]; 2007 [Consulta: Mayo 2016] Disponible en: <https://books.google.com.mx/books?id=BhdP2PZy6SoC&pg=PA178&dq=fat+y+ntfs&hl=es&sa=X&redir_esc=y#v=onepage&q=fat%20y%20ntfs&f=false>

[5] Rebollo Pedreulo, Miguel. Dispositivos de almacenamiento [en línea]; [Consulta: 23 de Mayo 2016] Disponible en: <https://riunet.upv.es/bitstream/handle/10251/13706/Dispositivos_de_almacenamiento.pdf?s>

[6] Bunting, Steve y Wei, William. EnCase® Computer Forensics: The Official EnCE: EnCase® Certified Examiner. Study Guide [PDF]; USA, 2006 [Consulta: Marzo 2015] Disponible en: <http://www.bk.psu.edu/faculty/bowers/ist454/eBook.pdf> pp.84

[7] Ibídem. pp. 89

[8] Ibídem. pp. 90

[9] Forensic Control [en línea]; [Consulta: 5 Mayo 2015] Disponible en: <https://forensiccontrol.com/resources/free-software/>

[10] Guidance Software [en línea]; [Consulta: 26 Febrero 2015] Disponible en: <https://www.guidancesoftware.com/products-services?cmpid=nav_r#software>

[11] Guidance Software. Tableau [en línea]; [Consulta: 4 Marzo 2015] Disponible en: <https://www2.guidancesoftware.com/products/Pages/tableau/overview.aspx>

[12] Decision Group Inc. Network Forensics and Lawful Interception Total Solutions Provider [en línea]; [Consulta: 27 Febrero 2015] Disponible en: <http://www.edecision4u.com/PRODUCTS.html>

[13] Paraben Corporation [en línea]; [Consulta: 4 Marzo 2015] Disponible en: <https://www.paraben.com/computer-forensics.html>

[14] Procedimiento para borrado seguro de un disco duro con DBAN [PDF]; [Consulta: 4 Agosto 2015] Disponible en: < http://moncayo.unizar.es/sicuz/docutec.nsf/2e52318decb4e752c1256fda004289a3/ba863e484e8d5776c12573c60033ea55/$FILE/dt0113.pdf>

[15] WipeDrive™ & WipeDrive PRO™ Quick Start Guide [Pdf]; 2006 [Consulta: 10 Julio 2015] Disponible en: <http://docs.whitecanyon.com/WipeDrive/Consumer/UserManual.pdf>

[16] Active@ KillDisk for Windows. User Guide [PDF]; [Consulta: 10 Julio 2015] Disponible en: <http://www.killdisk.com/downloads/killdisk.pdf>

[17] Caine. Computer Forensics Linux Live Distro [en línea]; [Consulta: 13 Julio 2015] Disponible en: <http://www.caine-live.net/page11/page11.html>

[18] El software libre y la informática forense. Tutorial de de Linux Caine [en línea]; [Consulta: 23 Julio 2015] Disponible en: <http://software-libre-if.blogspot.mx/p/tutorial-de-linux-caine.html>

[19] Incident Response- Data Adquisition Guidelines for Investigation Purposes. CERT-EU Security White Paper 2012-04 [Pdf]; [Consulta: 14 Agosto 2015] Disponible en: <http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_12_04_Guideline_DataAcquisition_v1_4_4.pdf>

[20] Caballero Q., Alonso. ReYDes [en línea]; [Consulta: 21 de Agosto 2015] Disponible en: <http://www.reydes.com/d/?q=Capturar_una_Imagen_Forense_utilizando_Guymager>

[21] Aliens. Clonado de disco [en línea]; [Consulta: 21 Agosto 2015] Disponible en: <http://alinez-hacker.mwik.com/t67-Clonado-de-disco.htm>

[22] García M., Vte. Javier. Análisis Forense de Sistemas [Pdf]; [Consulta: 24 Agosto 2015] Disponible en: <http://www.wadalbertia.org/docs/forensics.pdf>

[23] Caballero Q., Alonso E. Autopsy en español [Pdf]; Septiembre 2007. [Consulta: 24 Agosto 2015] Disponible en: <http://www.reydes.com/archivos/autopsy_reydes.pdf>

[24] Goga, Arturo. Recuperar archivos de memorias, discos duros, y más, con Photorec (Windows, Mac, Linux) [en línea]; [Consulta: 26 Agosto 2015] Disponible en: <https://www.arturogoga.com/recuperar-archivos-de-memorias-discos-duros-y-mas-con-photorec-windows-mac-linux-tutorial/>

[25] E-fense. Carpe Datum. Helix3 [Pdf]; 2009. [Consulta: 8 Septiembre 2015] Disponible en: <http://www.sdp-tech.com/sdp-tech/pub/helix/Helix_Opensource_User_Manual.pdf>

[26] Arquillo, José. Herramienta de apoyo para el análisis forense de computadoras [Pdf]; Universidad de Jaén, Jaé, España. Septiembre de 2007. [Consulta: 1 Julio 2015] Disponible en: <http://collection.openlibra.com.s3.amazonaws.com/pdf/Herramienta-de-Apoyo-para-el-analisis-forense-de-computadoras.pdf?AWSAccessKeyId=AKIAIGY5Y2YOT7GYM5UQ&Signature=1TG7mClDQSecnNyoQ1370vAiDuI%3D&Expires=1449268999>

[27] Fratepietro, Stefano; Rossetti, Alessandro; Dal Checco, Paolo. DEFT 7 Manual. Digital Evidence & Forensic Toolkit [Pdf]; 2012. [Consulta: 25 Agosto 2015] Disponible en: <http://www.deftlinux.net/doc/EN-deft7.pdf>

[28] Fratepietro, Stefano; Rossetti, Sandro. Deft. User Guide. R.0,6 [Pdf]; [Consulta: 27 Agosto 2015] Disponible en: <https://cs.gmu.edu/~astavrou/courses/ISA_785_F11/[en]deft_manual.pdf>

[29] Forensics with Digital Forensic Framework (DFF) [en línea]; 2013. [Consulta: 8 Septiembre 2015] Disponible en: <https://www.youtube.com/watch?v=02uZv72KS88 >

[30] Código Penal Federal [en línea]; 2015. [Consulta: 2015] Disponible en: <http://www.diputados.gob.mx/LeyesBiblio/pdf/9_120315.pdf>

[31] Documento de tecnología. Almacenamiento de estado sólido [en línea]; [Consulta: Julio 2017] Disponible en: <http://www.seagate.com/files/www-content/product-content/pulsar-fam/_cross-product/es-es/docs/ssd-faq-tp612-1-1003es.pdf>

[32] Toshiba. Semiconductores y productos de almacenamiento Europa EMEA [en línea]; [Consulta: Julio 2017] Disponible en: < https://toshiba.semicon-storage.com/es/product/storage-products/trends-technology/ssd-0.html>

[33] Rodil, Irene; Pardo, Camino. Operaciones auxiliares con tecnologías de la información y la comunicación [en línea]; Madrid, España, 2010 [Consulta: Julio 2017] Disponible en: <https://books.google.com.mx/books?id=2FtawJc7Tj0C&pg=PA22&dq=disco+duro+HDD&hl=es&sa=X&redir_esc=y#v=onepage&q=disco%20duro%20HDD&f=false>

[34] Huidobro, José; Blanco, Antonio; Jordán, J. Informática. Administración de sistemas informáticos. Redes de área local [en línea]; España, 2006 [Consulta: Julio 2017] Disponible en: <https://books.google.com.mx/books?id=V2xogIe99B8C&pg=PA59&dq=interfaz+de+entrada+y+salida+de+datos+de+una+usb&hl=es&sa=X&redir_esc=y#v=onepage&q=interfaz%20de%20entrada%20y%20salida%20de%20datos%20de%20una%20usb&f=false>