ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

PROYECTO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS

TEMA: "ANÁLISIS FORENSE PARA DISPOSITIVO DE ALMACENAMIENTO ÓPTICO CDS, DVDS Y BLU-RAY"

ÁREA DE CONOCIMIENTO: GERENCIA ADMINISTRATIVA
LÍNEA DE INVESTIGACIÓN: SEGURIDAD INFORMÁTICA

AUTORES: PEÑAHERRERA GUAMBA GABRIELA ALEJANDRA
ORELLANA VITERI DANIEL PATRICIO

DIRECTOR: ING. ÑACATO GERMÁN

SANGOLQUÍ
NOVIEMBRE, 2015

UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE
CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

CERTIFICADO

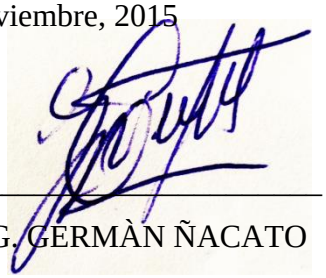
Ing. Germán Ñacato (DIRECTOR DE TESIS)

CERTIFICA

Que el presente trabajo titulado "ANÁLISIS FORENSE PARA DISPOSITIVO DE ALMACENAMIENTO ÓPTICO CDS, DVDS Y BLU-RAY" fue realizado en su totalidad por la Sra. Gabriela Alejandra Peñaherrera Guamba y el Sr. Daniel Patricio Orellana Viteri como requerimiento parcial a la obtención del título de INGENIERO EN SISTEMAS E INFORMÁTICA

_____

Noviembre, 2015



_____

ING. GERMÀN ÑACATO
DIRECTOR

UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE
CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

DECLARACIÓN DE RESPONSABILIDAD

Nosotros, Gabriela Alejandra Peñaherrera Guamba y Daniel Patricio Orellana Viteri.

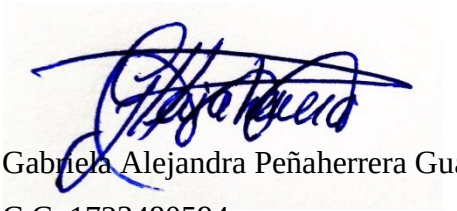
DECLARAMOS QUE:

El proyecto de grado denominado "ANÁLISIS FORENSE PARA DISPOSITIVO DE ALMACENAMIENTO ÓPTICO CDS, DVDS Y BLU-RAY", ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de nuestra autoría.

En virtud de esta declaración, nos responsabilizamos del contenido veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, Noviembre de 2015



Gabriela Alejandra Peñaherrera Guamba
C.C. 1723480594

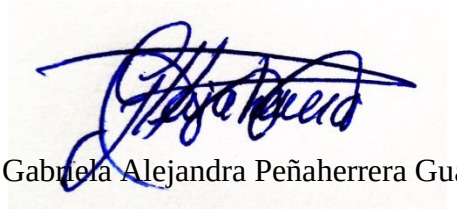
Daniel Patricio Orellana Viteri
C.C. 1720996717

UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE
CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

AUTORIZACIÓN DE PUBLICACIÓN

Nosotros, Gabriela Alejandra Peñaherrera Guamba y Daniel Patricio Orellana Viteri, autorizamos a la UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE, la publicación, en la biblioteca virtual de la Institución del proyecto de tesis "ANÁLISIS FORENSE PARA DISPOSITIVO DE ALMACENAMIENTO ÓPTICO CDS, DVDS Y BLU-RAY", cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y autoría.

Sangolquí, Noviembre de 2015



Gabriela Alejandra Peñaherrera Guamba
C.C. 1723480594

Daniel Patricio Orellana Viteri
C.C. 1720996717

DEDICATORIA

El presente proyecto va dedicado a toda mi familia que es lo mejor y más valioso que Dios me ha dado, mis padres Eduardo y Carmen, mis hermanas Margorie y Verónica, por su dedicación y amor, por ser buenos consejeros e incondicionales en los momentos difíciles de mi vida profesional y emocional, a mi amado esposo Diego y a mi adorada hija Camilita por ser la razón de mi vida, por la paciencia, por la motivación y amor incondicional, los cuales fueron la razón más importante para culminar esta etapa.

Gabriela Peñaherrera Guamba

Este proyecto va dedicado de manera muy especial a mis padres María Elena Viteri, Patricio Orellana y mi hermana Cristina Orellana por apoyarme en los momentos más complicados, por el sacrificio y confianza que tuvieron hacia mí para ayudarme a seguir adelante y no desmayar en este difícil camino, a mis abuelitos que donde estén espero se sientan orgullosos de mí.

Daniel Orellana Viteri

AGRADECIMIENTO

Agradezco a mis padres y hermanas, quienes con su ejemplo de superación y perseverancia me han permitido culminar esta etapa de mi camino, a mi esposo por su amor y su aliento diario, quien ha sido un apoyo incondicional en cada momento de mi carrera, y a mi pedacito de cielo mi hija por ser mi mayor razón de motivación y de grandes esfuerzos.

A la Universidad de las Fuerzas Armadas, Carrera de Ingeniería en Sistemas, a cada uno de los profesionales que la conforman por todos los conocimientos impartidos, de manera muy especial al Ing. Germán Ñacato, ser humano impecable y buen amigo, por su esfuerzo, dedicación, colaboración, paciencia y al Ing. Campaña por su colaboración su sabiduría impartida, que permitieron lograr cumplir mi objetivo planteado.

Gabriela Peñaherrera Guamba

Agradezco a Dios por darme las fuerzas para no desmayar en los momentos más difíciles, a mis padres y mi hermana que son el pilar fundamental en mi vida.

A mi querida Universidad De las Fuerzas Armadas ESPE por haberse convertido en mi segunda casa, a mi Director de Tesis Ing. Germán Ñacato por su ayuda, consejos, su apoyo, a mi Director de Carrera Ing. Mauricio Campaña por su apoyo, sus enseñanzas y sobre todo su amistad.

Daniel Orellana Viteri

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El análisis Forense es un área de la seguridad informática que surge a raíz de problemas de incidentes de seguridad. La tecnología avanzado aceleradamente así como también la forma en que se operan y se almacenan los medios informáticos. La idea principal de este proyecto es desarrollar una guía metodológica, que en base a la utilización de herramientas se obtiene la réplica o imagen del disco óptico donde reside la evidencia para una recolección, análisis digital y el análisis forense. La guía metodológica utilizada es: Preparar, identificar, recolectar, preservar, analizar e informar, proporcionando un marco teórico que sustente la investigación y análisis forense. Se utiliza la herramienta de distribución de Linux forense llamado Caine (Computer Aided Investigative Environment), el mismo que cuenta con una serie de utilidades y herramientas para: el estudio preliminar, recolección de la evidencia, análisis de la evidencia.

Palabras Claves

CAINE
FORENSE
AUTOPSY
EVIDENCIA

ABSTRACT

Forensic analysis is an area of computer security that arises as a result of problems of security incidents. Technology advanced rapidly as well as also the form in which they operate, and the resources are stored. The main idea of this project is to develop a methodological guide, which gets the replica or image of the optic disc resides for a collection, digital analysis and forensic evidence based on the use of tools. The methodological guide used is: prepare, identify, collect, preserve, analyze, and report, providing a framework that supports the research and forensic analysis. Using the Linux distribution forensic named Caine (Computer Aided Investigative Environment), which features a series of utilities and tools for: the preliminary study, evidence collection and analysis of evidence.

KeyWords

CAINE
FORENSE
AUTOPSY
EVIDENCE

CAPÍTULO 1

1.1 Antecedentes

El análisis forense surge a partir del incremento de diferentes incidentes de seguridad en la información, implementando y actualizando varias técnicas que permiten reconstruir un bien informático y evaluar su vulnerabilidad con el fin de mantener la integridad de los datos.

Estos incidentes de seguridad son aquellos que están fuera de la ley como ataques cibernéticos, pornografía infantil, extorsión, fuga de información confidencial, entre otros, en el cual están sometidos algunos sistemas telemáticos, por lo cual el análisis forense trata de disminuir estas amenazas, vulnerabilidades e incidentes de manera eficaz. (Sullivan, 2014)

El principal elemento que se debe proteger en una investigación de cualquier tipo es el dispositivo mismo que contiene la información útil para la investigación, por lo cual la informática forense puede detectar los ataques informáticos dentro de estos dispositivos electrónicos sean estos desde el punto de vista de software y de hardware (equipo y programa de cómputo, dispositivos digitales de almacenamiento de datos, equipo electrónico y, equipo o dispositivos de telecomunicaciones), para mantener la integridad de la información se genera una evidencia digital o electrónica que en muchos casos son frágiles y mediante un proceso forense se pueda llegar a recuperar aunque haya sido alterada anteriormente. (León, Echeverría, & Santander, 2010)

Dentro del procedimiento para realizar un análisis forense, se debe contar con una infraestructura informática apta para tal análisis, es decir, el estudio de cualquier componente que tenga una memoria informática, de aquí se realiza un estudio preliminar del caso que va a ser evaluado, se obtiene la información y los datos más

relevantes para realizar el análisis del mismo, culminando con la elaboración del informe que será transmitido.

En base a lo mencionado hay que considerar que leyes existen en el entorno legal al momento de realizar cualquier análisis forense de un sistema informático dentro del país.

En este caso se realizará el análisis forense de dispositivos de almacenamiento óptico, estos dispositivos son los más antiguos y a la vez más susceptibles de cambios en la actualidad ya que permiten administrar grandes cantidades de información dependiendo de las características del dispositivo. Para el análisis se requiere una comprensión completa tanto de la estructura física y del funcionamiento de estos medios de almacenamiento, como son la forma, el tipo (sea regrabable o normal), la estructura lógica (cómo se van almacenar los datos) y que tan frecuente son los plagios o delitos informáticos en estos sistemas específicamente en CDs, DVDs y BLU-RAY.

1.2 Planteamiento del Problema

Tomando en cuenta que en la sociedad actual existen miles de delitos informáticos que algunas veces pasan desapercibidos, un mecanismo muy común es por medio de los dispositivos de almacenamientos óptico como: CDs o DVDs y actualmente el blu-ray, estos dispositivos son frágiles al manejo de información debido a que guardan datos que poseen valor como evidencia y que es muy común que se pueda regrabar o sobrescribir la información.

Varias empresas realizan grandes inversiones en este tipo de estrategias, además de combatir con las amenazas externas como el hacking, desfalcos, etc. Una de las mayores preocupaciones con temas de seguridad es en cuanto al manejo y a la protección de información y materiales de la empresa ya que la mayoría de veces son amenazas internas de la organización las cuales podrían facilitar información que sería de gran utilidad para empresas opositoras u otro tipo de ataque.

Cada vez más estos delincuentes informáticos actúan de forma desmedida sin que los operadores de justicia puedan hacer algo, ya que han quedado aislados por la falta de

recursos tecnológicos y capacitación a fin de manejar la evidencia digital presente en toda clase de infracciones y especialmente en los llamados Delitos Informáticos.

Es importante entender el funcionamiento y la estructura de estos dispositivos como el mecanismo que usa un cd grabable a comparación de un normal, como se realiza la transferencia de datos, características físicas, estos aspectos son cruciales para evaluar si los datos aún son accesible al paso del tiempo, con el objetivo de encontrar técnicas para un mejor y óptimo análisis en caso de actos delictuosos como fraudes, espionajes, robo de identidad, etc. , con el fin de facilitar la restauración de hechos dentro de un proceso legal y que leyes permiten ser usadas durante las evidencias encontradas en estos dispositivos junto a los procedimientos que se debe aplicar para salvaguardar la evidencia, tener la información oportuna en menor tiempo.

1.3 Justificación e Importancia

Es importante entender el funcionamiento y la estructura que tienen los discos ópticos, identificar el mecanismo que usa un cd grabable a comparación de un normal, cómo se realiza la transferencia de datos, características físicas, que aspectos son cruciales para evaluar si los datos aún son accesible con el paso del tiempo y su uso, y muchos aspectos más, de esta manera identificar técnicas para un mejor y óptimo análisis en caso de actos delictuosos como fraudes, espionajes, robo de identidad, etc. , con el fin de facilitar la restauración de hechos dentro de un proceso legal y que leyes permiten ser usadas durante las evidencias encontradas en estos dispositivos junto a los procedimientos que se debe aplicar para salvaguardar la evidencia, tener la información oportuna en menor tiempo.

Se realizará una guía metodológica utilizando herramientas que permitan facilitar la toma de evidencias de forma rápida y eficaz.

Es de vital importancia e indispensable que toda empresa se enfoque en la utilización de una guía que contemple un análisis forense dentro de su política de seguridad , cumpliendo las necesidades de la organización y que este enmarcada dentro

del proceso de respuesta a incidentes en los sistemas informáticos con mayor susceptibilidad como son los discos de almacenamientos ópticos, mediante pasos adecuados para la óptima examinación de CDs, DVDs, BLU-RAY y recuperación de la información si fuese el caso.

A continuación se detallan los motivos que justifican la elaboración de este análisis:

- Deterioro de la integridad de la información ya sea por el paso del tiempo y su uso que en muchos casos es necesario recuperar información valiosa.
- Técnicas utilizadas en la actualidad para el robo de información cada día más complejas.
- Controlar el cambio de hash del disco cd/dvd/blu-ray cada vez que se realiza una lectura del dispositivo.
- Sistemas y políticas de seguridad inadecuadas, para estos dispositivos.
- Personas acusadas de delitos informáticos sin pruebas que demuestren su culpabilidad o inocencia y falta de procedimientos legales.
- Organizaciones que no cuentan con herramientas adecuadas para el análisis forense.
- Falta de conocimiento de la estructura de estos dispositivos y entender su funcionamiento.

1.4 Objetivos

1.4.1 Objetivo General

Realizar una guía metodológica que permita analizar y reconstruir la evidencia adquirida de los dispositivos ópticos, haciendo uso de técnicas y herramientas de análisis forense con el fin de entregar un informe claro de lo que se requiere en un proceso legal.

1.4.2 Objetivos Específicos

- Definir una guía metodológica adecuada que facilite la reconstrucción de los eventos dentro del proceso forense.
- Utilizar adecuadamente las herramientas con la finalidad de prevenir cualquier tipo de delito informático.
- Verificar el tipo de evidencia y sus características referentes al dispositivo que se ha proporcionado para el posterior análisis.
- Preservar la integridad de la evidencia digital, para que no exista ninguna manipulación accidental o intencional de la evidencia original.
- Conocer las leyes y estatutos vigentes que permitan corroborar las evidencias descubiertas en dispositivos de almacenamiento óptico para ser utilizados como prueba judicial.

1.5 Alcance

El alcance de la tesis es realizar una guía metodológica de un análisis forense de los procesos que hacen referencia al análisis de la información y delitos de dispositivos de almacenamientos ópticos como CDs , DVDs Y BLU-RAY, esta guía metodológica abarcara un estudio práctico, con el fin de evaluar y revelar resultados que genere cada proceso informático con la ayuda de la utilización de la respectiva herramienta.

El presente proyecto realizará el análisis forense en dispositivo de almacenamiento óptico utilizando las siguientes fases:

- Identificación: Reconocimiento de la evidencia digital.
- Recolección: Recolectar la evidencia en función del tiempo y los recursos informáticos disponibles, sustentado por el mandato judicial
- Adquisición: Es el proceso de copia forense obteniendo una copia binaria exacta del contenido lógico o físico de los objetos involucrados en la investigación.
- Preservación: la evidencia digital deberá ser preservada para asegurar su integridad durante todo el proceso. Esto incluye la manipulación del dispositivo.
- Informe técnico: Resultados del análisis forense, documentación.

CAPÍTULO 2

MARCO LEGAL, TEÓRICO Y CONCEPTUAL

3.1 Introducción

A lo largo del tiempo han surgido nuevas tecnologías, por lo tanto crecen las personas mal intencionadas, que aprovechando las vulnerabilidades que presentan los dispositivos para este caso en particular los ópticos, son capaces de acciones no autorizadas, generalmente con fines ilegales, facilitando el cometimiento de infracciones. A partir de esto se ha creado la necesidad de especializarse y capacitarse frecuentemente en el ámbito de análisis forense ya que tanto los hábitos de personas y actuación de delincuentes cada vez cambian, por lo cual se desarrolla esta guía de análisis forense para dispositivos ópticos.

La función de los medios ópticos en los archivos cambió hace mucho tiempo, que paso de ser un medio para preservar información a convertirse en un formato en riesgo, dado que es imposible contar todos los problemas de migración y conservación de la información que se almacena digitalmente, surgiendo la necesidad de un panorama más extenso sobre los medios ópticos, el cual pretende proporcionar esta guía.

Las herramientas de análisis forense permiten establecer un conjunto de evidencia para la contraparte y el juzgador, con el fin de probar la veracidad de las afirmaciones o declaraciones del proceso ejecutado y la confiabilidad de resultados.

Generalmente los analistas forenses acuden a prácticas internacionales con el fin de asegurar la evidencia digital identificada en las diferentes herramientas informáticas y tecnológicas presentes en la escena del crimen durante el desarrollo de un análisis forense digital tradicional con medios magnéticos y ópticos.

Las guías del NIST (Instituto Nacional de Estándares y Tecnología) son parte de estas prácticas en temas de dispositivos móviles, web services, entre otros, así como los documentos del Departamento de Justicia de los Estados Unidos como Forensic Examination of Digital Evidence: A Guide for Law Enforcement, Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition, son instrumentos utilizados por los analistas forenses digitales con el fin de establecer un marco formal y demostrable que permita a terceras personas validar las acciones que aumenten la evidencia digital disponible en los medios informáticos, y con apego a la ley.

3.2 Marco legal de informática forense en el Ecuador

La Informática Forense en Ecuador nace con la finalidad de implementar un marco legal como medio de prueba eficaz, el cual interrelacione la Informática y el Derecho, a partir de esto nace la Informática Jurídica y el Derecho Informático, que permiten tratar evidencia digital y electrónica de manera adecuada.

A partir de esto se tiene las siguientes ciencias forenses:

- LA INFORMÁTICA JURÍDICA: Estudia la utilización de aparatos electrónicos como la computadora en el derecho; es decir, la ayuda que estos artefactos informáticos prestan al desarrollo y aplicación del derecho. Ejm. Oficina de Sorteos de la Corte Provincial.

- EL DERECHO INFORMÁTICO: Constituye el conjunto de normas, procesos, relaciones jurídicas que nacen como consecuencia de la aplicación y desarrollo de la informática. Ejm. Ley de Firmas Electrónicas.

- COMERCIO ELECTRÓNICO: Hoy por hoy es muy fácil comprar y vender bienes, brindar servicios desde un escritorio en la oficina o desde el hogar, ésta actividad se encuentra regulada en nuestro país por le "E Commerce" (Comercio Electrónico).

El código penal Ecuatoriano es aplicable solamente cuando la infracción sea cual sea esta haya sido cometida dentro del territorio, por esta razón las leyes son netamente territoriales lo cual no está bien ya que los delitos son de carácter transnacional, es decir que se cometen en diferentes lugares, ciudades o países. (Icaza, 2010)

3.2.1 Hardware en Informática Forense

En la tabla 1 se muestran los diferentes criterios sobre el hardware en informática forense.

Tabla 1

Hardware en Informática Forense

SISTEMA INFORMATICO	
HARDWARE (Elementos Físicos)	Evidencia
• **Es Mercancía ilegal o fruto del delito**	• El hardware es una mercancía ilegal cuando su posesión no está autorizada por la ley. Ejemplo: en el caso de los decodificadores de la señal de televisión por cable, su posesión es una violación a los derechos de propiedad intelectual y también un delito. • El hardware es fruto del delito cuando este es obtenido mediante robo, hurto, fraude u otra clase de infracción.
• **Es un Instrumento**	• El hardware es un instrumento cuando cumple un papel importante en el cometimiento del delito, se puede decir que es usada como un arma o herramienta, tal como una pistola o un cuchillo. Un ejemplo serían los snifers (programa informático que registra la información que envían los diferentes periféricos de una red para poder monitorear la actividad en un determinado ordenador) y otros aparatos especialmente diseñados para capturar el tráfico en la red o interceptar comunicaciones.
• **Es evidencia**	• En este caso el hardware no puede ser fruto del delito o un instrumento para el delito, ya que es un elemento físico que se constituye como prueba de la comisión de un delito. Por ejemplo el scanner que se usó para digitalizar una imagen de pornografía infantil, cuyas características únicas son usadas como elementos de convicción.

FUENTE:(Pino, 2009)

3.2.2 Información en Informática Forense

En la tabla 2 se muestran los diferentes criterios sobre la información en informática forense.

Tabla 2

Información en Informática Forense

SISTEMA INFORMÁTICO	
INFORMACIÓN	Evidencia
• **Es mercancía ilegal o el fruto del delito.**	• La información se considera como mercancía ilegal cuando su posesión no está permitida por la ley, por ejemplo en el caso de la pornografía infantil. Es fruto del delito cuando sea el resultado del cometimiento de una infracción, como por ejemplo las copias pirateadas de programas de ordenador, secretos industriales robados.
• **Es un Instrumento**	• La información es un instrumento o herramienta cuando se usa como medio para cometer un ilícito. Como por ejemplo los programas de ordenador que se utilizan para quebrar las seguridades de un sistema informático, romper contraseñas o brindar acceso no autorizado. En conclusión cuando juegan un importante papel en el cometimiento del delito.
• **Es evidencia**	• Se puede conseguir mucha información como evidencia, debido a que muchas o varias de las acciones informáticas diarias que cometen los delincuentes dejan un rastro digital, por ejemplo la información de los ISP's, de los bancos, y de las proveedoras de servicios las cuales pueden revelar actividades particulares de los sospechosos

FUENTE:(Pino, 2009)

En resumen el propósito fundamental de las categorías antes mencionadas es el de enfatizar el rol que tienen los sistemas informáticos en el cometimiento de delitos, con el fin de que el investigador criminal tenga una visión clara y precisa al buscar y analizar las diferentes evidencias que encuentre. Por esto el hardware, software y la información

contenida en estos son objeto de estudio, para lo cual es necesario contar con las herramientas necesarias y el conocimiento que nos brinda la ciencia informática, y en particular de la Ciencia Forense Informática. (Pino, 2009)

3.3 Informática forense

Una de las causas que generan preocupación de seguridad son las conspiraciones informáticas las mismas que han causado grandes pérdidas económicas especialmente en el sector productivo y financiero donde se generan magnas manipulaciones de la información , se estima que la pérdida supera los 200 millones de dólares, sumada a la disminución de credibilidad de empresas que son afectadas.

Por tal motivo grandes países como Estados Unidos y Alemania han desarrollado varias metodologías y herramientas informáticas a fin de encontrar a los infractores acompañados de pruebas. Una de estas herramientas es la informática Forense, ciencia de criminalística que analiza sistemas informáticos, trabaja conjuntamente con las Tecnologías de la Información, contiene principios y técnicas que comprende el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias digitales. (Acurio, 2009)

3.3.1 Concepto

"La Informática forense es una disciplina dedicada a la recolección de pruebas digitales desde una maquina computacional para fines judiciales mediante la aplicación de técnicas de análisis y de investigación". (Cabrera, 2013)

La informática forense se aplica tanto para la indagación de delitos frecuentes como (homicidios, fraude, narcotráfico, terrorismo, entre otros), así como para los que se encuentran relacionados con las tecnologías de la información y las comunicaciones, entre los que recalcan la piratería de software, distribución de pornografía infantil y hacking .

Sin embargo no se ha establecido un método normalizado, por lo cual dentro de un proceso judicial es muy cuestionado, sin embargo no deja de ser una herramienta importante más aún si se maneja en base a rígidos principios científicos, normas legales y de procedimiento. (Peñaherrera & Duque, 2011)

3.3.2 Objetivos de la informática forense

Los principales objetivos de la informática forense son:

- Recolectar evidencia digital de toda clase de infracción.
- Compensación de los daños causados por los criminales o intrusos.
- Seguimiento y procesamiento judicial de los criminales.
- Creación y aplicación de medidas para prevenir casos similares.

Todo esto se logra con recolección de evidencia. (Garcia, 2013)

3.3.3 Principios forenses

Los principios forenses que se debe tener en cuenta son:

- Conocimiento de técnicas de informática forense.
- Basarse en estándares legales.
- Evitar contaminación
- Actuar sistemáticamente
- Controlar la evidencia, indagar quien, cuando y donde hubo manipulación de la evidencia.
- Documentar los cambios que han surgido en la evidencia. (Mujica, 2011)

3.4 Discos Ópticos

Los Discos ópticos nacen a finales de los 80’, debido a las exigencias del mercado las cuales implicaban que los dispositivos de almacenamiento tengan mayor velocidad de lectura y escritura, livianos y pequeños, resistentes a daños y sobre todo mayor

capacidad de almacenamiento, y como consecuencia de que su predecesor el disquete contaba con una capacidad de almacenamiento muy reducida y eran muy propensos a dañarse.

Los Discos Ópticos son un medio de almacenamiento digital, consisten en un disco circular en el cual mediante un haz de luz (laser), se codifica y guarda información de cualquier tipo, haciendo microscópicos agujeros o surcos en la superficie del disco. (Saal, 2010)

3.4.1 Ventajas y Desventajas

Tabla 3

Ventajas y Desventajas Discos Ópticos

VENTAJAS Y DESVENTAJAS DISCOS OPTICOS	
Ventajas	**Desventajas**
• Son más resistentes a los diferentes daños (polvo, agua, caídas, difícil de romperlos, fundirlos o doblarlos). • Pueden ser limpiados fácilmente. • No son propensos a daños debido a campos magnéticos. • Variedad en capacidad de almacenamiento.	• Pueden fallar o deformarse al momento de exponerlos a temperaturas elevadas. • Son propensos a rayones. • Se necesita del Hardware adecuado para su utilización. • Corrosión en el lado de la etiqueta, lo cual puede causar daños en el dispositivo.

FUENTE:(Smith, 2010)

3.4.2 Compact Disc o CD

- El disco compacto es un dispositivo óptico que nos permite almacenar cualquier tipo de información (datos, documentos, audio, video, imágenes, etc).
- Hoy en día es el medio físico más utilizado dentro de la industria musical. (Téllez, 2010)

3.4.2.1 Formatos

Tabla 4

Formatos CD

FORMATOS CD	
VIDEO-CD	• Para películas de dicho formato.
PHOTO-CD multisesión	• Cuando se lleva a revelar un carrete se puede pedir que se grabe en este formato.
CD-XA y CD-XA Entrelazado	• CD's con mezcla de música y datos.
CD-ROM	• Estos CD's pueden ser grabados y leídos, pero no puede cambiarse la información que contienen una vez grabados en ellos. En estos CD's los datos se graban sobre una aleación especial de materiales plásticos. La información que se graba en ellos se codifica en forma de espiral de pequeñas memorias anexas registradas en la superficie del disco al ser grabado, por lo que no pueden ser alteradas posteriormente.
CD-RW	• Son CD's regrabables o re escribibles. Estos contienen cambio de fase, que es una tecnología para grabadoras de CD que permite la escritura múltiple. El cambio de fase consiste en alterar las propiedades del disco compacto, cambiando su estructura de amorfa a cristalina y viceversa. Cuando está el CD en fase cristal lo puede borrar y reescribir durante la fase amorfa en él.
CD-I	• El disco compacto interactivo almacena audio, video en movimiento, gráficos y texto. Lo interesante es que puede viajarse por esa información de modo interactivo. Los discos son iguales que los CD-ROM y los componentes del sistema son: lector de CD-I, controlador multimedia, mando a distancia y tarjeta de memoria.
DVI	• El Vídeo digital interactivo es una tecnología más que un sistema integrado en un solo equipo.
WORM	• Permite al usuario grabar por una vez con el mismo aparato que emplea para la lectura. Tras ello, la información no puede cambiarse. Se emplea para registrar información permanente: los bancos para sus transacciones diarias, archivos de prensa y fotografía. Tampoco está normalizado.
DISCOS MAGNÉTICO ÓPTICOS WMRA	• Pueden leerse y modificarse a voluntad, pues bajo su superficie plástica existen cristales metálicos sensibles magnéticamente.

FUENTE:(González, 2006)

3.4.2.2 Funcionamiento

Tabla 5

Funcionamiento CD

FUNCIONAMIENTO CD	
Lectura	• El rayo láser (infrarrojo) de la unidad lectora por medio de difracción (desviación de los rayos luminosos cuando éstos pasan por un cuerpo opaco o por una abertura de diámetro menor o igual que la longitud de onda.) con la superficie reflejante del disco, determina la profundidad de la ranura, tal como se muestra en la Figura 1.
Escritura	• El rayo láser (infrarrojo), se aplica a la superficie del disco, se marcará o escribirá de diferente manera la ranura y determinará al bit (un cero ó un uno); este proceso de escritura comúnmente se le llama "quemar".

FUENTE:(Téllez, 2010)

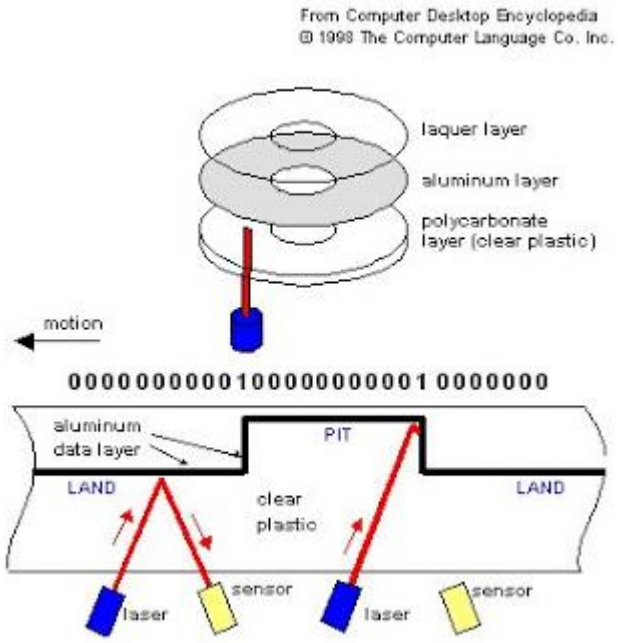


Figura 1 Funcionamiento CD

Fuente: (García I. , 2009)

3.4.3 DVD

El Disco de Video Digital es un dispositivo óptico de almacenamiento que fue creado principalmente para grabar películas de alta calidad en audio y video, pero con el paso de tiempo y de las necesidades de los usuarios se lo empezó a utilizar para guardar todo tipo de datos.

Su forma y aspecto son semejantes a las del CD pero con la gran diferencia de que están codificados en un formato distinto. (Téllez, 2010)

3.4.3.1 Formatos DVD

Tabla 6

Formatos

FORMATOS DVD	
DVD-ROM	• Las unidades DVD-ROM inicialmente tuvieron ciertos problemas de compatibilidad con los discos CD-R y CD-RW, porque la reflectividad de la superficie de estos discos los hacía imposibles de leer para la mayoría de las unidades DVD. Para los CD-RW, esto se resolvió con un láser de longitud de onda dual, y desde finales de 1998, se dispone de unidades DVD capaces de leer cualquier tipo de discos grabables o regrabables, tanto por CD como por DVD.
DVD-Vídeo	• Los discos DVD-Vídeo utilizan la compresión MPEG-2 para almacenar vídeo, y en países como Estados Unidos, almacenan también sonido digital envolvente AC-3.
DVD-Audio	• La ventaja más importante del DVD-Audio es la posibilidad de incorporar vídeo con la música y su capacidad de 2horas de sonido envolvente o 4 horas de sonido estéreo con el estándar DVD5.
DVD-R	• El DVD-R o DVD grabable apareció poco después del DVD-ROM e inicialmente alcanzó una capacidad de 3'95Gb por cada cara. Actualmente su capacidad supera los 4GB.
DVD-RAM	• Los discos DVD-RAM vienen dentro de cartuchos, imprescindibles para realizar la grabación. Su principal característica es la de ser un medio regrabable más de 100.000 veces con una capacidad de 2.6 Gb por cara, así existen discos "Type I" con 5.2 Gb y dos caras y "Type II" con 2.6 Gb y una cara.
+RW	• Es un formato competidor del DVD-RAM basado en la tecnología DVD y CD-RW, pero incompatible con el estándar DVD-RAM.

FUENTE:(González, 2006)

3.4.3.2 Funcionamiento

Tabla 7

Funcionamiento DVD

FUNCIONAMIENTO DVD	
Lectura	• El rayo láser azul de la unidad lectora por medio de difracción (desviación de los rayos luminosos cuando éstos pasan por un cuerpo opaco o por una abertura de diámetro menor o igual que la longitud de onda.) con la superficie reflejante del disco y determina la profundidad de la ranura.
Escritura	• El rayo láser rojo se aplica a la superficie del disco tal como está en la Figura 2, se marcará o escribirá de diferente manera la ranura y determinará al bit (un cero o un uno); éste proceso de escritura comúnmente se le llama "quemar".

FUENTE:(Téllez, 2010)

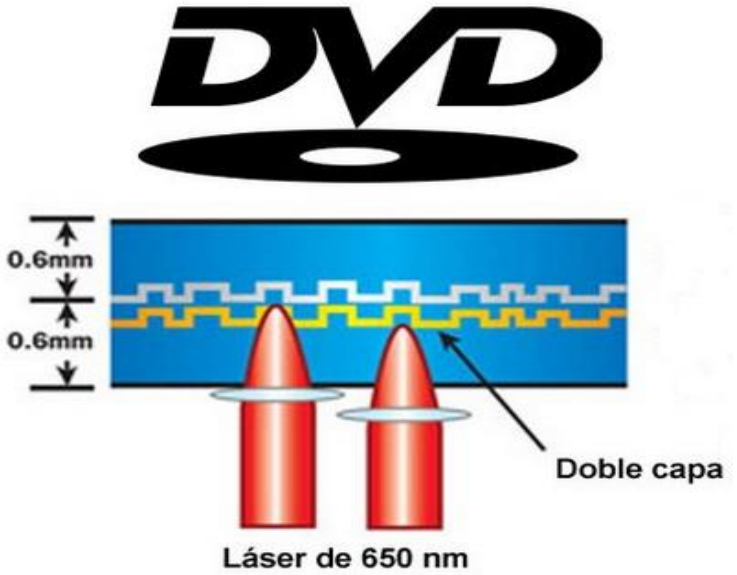


Figura 2 Funcionamiento DVD

Fuente: (Hoffmeister, 2012)

3.4.4 BD

El Blu Ray es un dispositivo óptico de nueva generación de almacenamiento que fue creado principalmente para grabar películas de alta definición en audio y video, así como datos de alta densidad.

Su forma y aspecto son semejantes a las del CD y DVD pero con la gran diferencia de que el Blu Ray cuenta con una protección física que evita ralladuras y de esta manera asegura la información contenida en él. (Ttito, 2010)

3.4.4.1 Formatos

Tabla 8

Formatos BD

FORMATOS BD	
BD-R	• Pueden ser grabados y leídos, pero no se puede cambiar la información que contienen una vez grabados en ellos.
BD-RE	• Son BD que permiten múltiples escrituras y borrados.
BD-ROM	• Son BD que vienen ya grabados con información y solo permiten la lectura de datos.

FUENTE:(Ttito, 2010)

3.4.4.2 Funcionamiento

Tabla 9

Funcionamiento BD

FUNCIONAMIENTO BD	
Lectura	• El rayo láser azul de la unidad lectora por medio de difracción (desviación de los rayos luminosos cuando éstos pasan por un cuerpo opaco o por una abertura de diámetro menor o igual que la longitud de onda.) tal como la Figura 3.
Escritura	• El rayo láser azul se aplica a la superficie del disco, se marcará o escribirá de diferente manera la ranura y determinará al bit (un cero o un uno), con la diferencia que el BD posee un rayo o laser que es hasta 5 veces más delgado que el de los CD`s o DVD`s, que proporciona mayor cantidad de ranuras en un mismo espacio para así almacenar mayor información;

FUENTE:(Ttito, 2010)

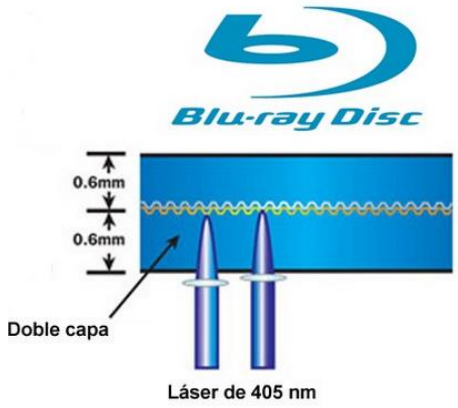


Figura 3 Funcionamiento BD

Fuente: (Gutiérrez, 2014)

El funcionamiento de los discos ópticos se resume en la Figura 4.

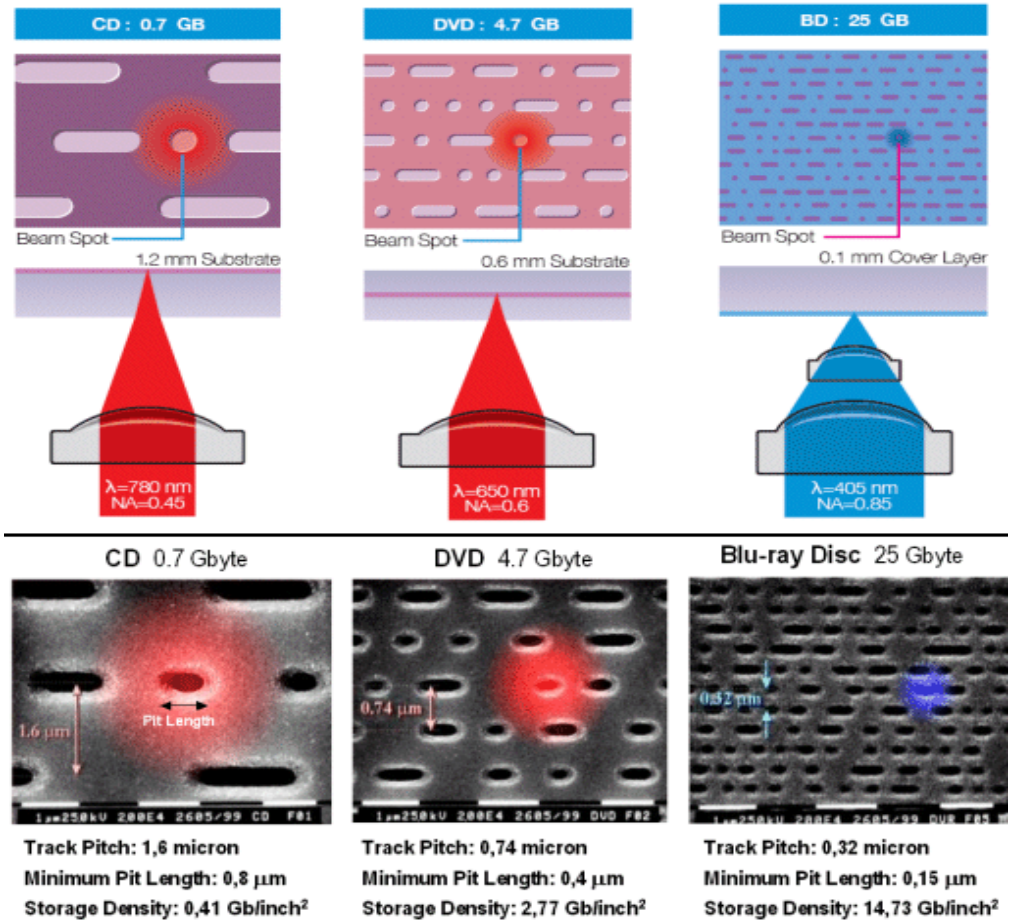


Figura 4 Funcionamiento, CD, DVD y BLU RAY

Fuente: (Hoffmeister, 2012)

3.4.5 Características y Diferencias CD, DVD y BD

Tabla 10

Características CD, DVD y BD

CARACTERISTICAS			
	CD	**DVD**	**BLU RAY**
Tamaño	12 cm de diámetro	12 cm de diámetro	12 cm de diámetro
Grosor	1.2 mm	1.2 mm	1.2 mm
Capas	1	1-2 (admite doble cara, hasta 4 capas)	Multicapa
Capacidad por capas	700 MB	4.7 GB	25 GB
Material reflectante	Aluminio (CD-ROM), aleaciones de oro o plata (regrabables)	Aluminio (DVD-ROM), aleaciones de oro y plata (regrabables)	Aluminio (BD-ROM), aleaciones de oro o plata (regrabables)
Material protector/substrato	Policarbonato	Policarbonato	Polímero durabis (patente TDK) de alta resistencia (no se raya)
Grosor protector	1.2 mm	0.6 mm	0.1 mm
Laser	Infrarrojo	Rojo	Azul-violeta
Longitud de onda	780 nm	650 nm	405 nm
Apertura numérica	0.45	0.60	0.85
Tamaño mínimo de bits	0.83 um	0.44 um	0.32 um
Separación entre pistas	1.6 um	0.74 um	0.32 um
Tasa de Transferencia	153.6 kbp	11.08 Mbps	53.94 Mbps
Velocidad de Transferencia	Hasta 48x (lectura) y 48x (escritura)	Hasta 16x (lectura) y 22x (escritura)	Hasta 8x (lectura) y 8x (escritura)

FUENTE:(Hernández, 2013)

3.5 Herramientas

3.5.1 Tipos y descripción

A continuación se describe algunas herramientas que se podrán utilizar para el desarrollo de la investigación.

- CAINE.- es una interfaz gráfica amigable que integra herramientas forenses convertidas en módulos de software, gracias a un proceso semiautomático puede generar informes, documentación y resultados de una manera eficaz. (Untiveros, 2011)

- CD and DVD Inspector.- es un software que los examinadores forenses profesionales de todo el mundo confían para adquirir la evidencia de CD y DVD, recuperación de datos, análisis forense y fuerzas del orden, esta herramienta sirve para el análisis intenso y la extracción de datos de CD-R, CD-RW así como para todos los tipos de medios DVD, incluyendo HD DVD y Blu-Ray. (Crowley, 2010).

- VSO Inspector.- Herramienta que genera un completo informe sobre la configuración de los dispositivos. Dispone de un práctico escáner de discos y un cómodo visor de sectores. (Martín, 2012)

- CDRoller.- Herramienta completa para la lectura, copia, análisis y administración de discos compactos CDs, DVDs y discos Blu-Ray (BD y HD-DVD), simple, estable, rápido y muy útil. (CDRoller, 2015)

- CD/DVD Diagnostic.- Herramienta de software avanzado que ayuda a recuperar datos de discos rayados o dañados, realiza la examinación de sectores para asegurar la información de datos y la legibilidad de la calidad del disco. (SOFTPEDIA, 2015)

3.5.2 Pesos ponderados

Existen varias herramientas para analizar los dispositivos de almacenamiento óptico, que se listan en la tabla 1 los cuales fueron definidos anteriormente, existen muchos factores y parámetros para seleccionar el tipo de herramienta a utilizar, tal como se indica en a Tabla11.

Tabla 11

Alternativas de Analizadores

Alternativas	
A	Caine
B	CD and DVD Inspector
C	VSO Inspector
D	CDRoller
E	CD/DVD Diagnostic

En la tabla 12 se enumeran los criterios y sus respectivas ponderaciones para la seleccionar la herramienta más adecuada.

Tabla 12

Criterios de Selección

Criterios de Selección		
I	Multiplataforma	10 %
II	Interfaz Amigable	30 %
III	Emisión de Reportes	40 %
IV	Open Source	10 %
V	Soporte	10 %
Total	100%	

Para elegir la mejor herramienta, cada opción ha sido calificada con un valor de 1 a 5 siendo, 1 Muy Deficiente, 2 Deficiente, 3 Regular, 4 Buena y 5 Excelente, construyendo así la matriz de selección Tabla 13.

Tabla 13

Matriz de Selección de la Herramienta

	Criterios de selección				
Alternativas	**I**	**II**	**III**	**IV**	**V**
Caine	1	5	5	5	2
CD and DVD Inspector	5	2	5	1	2
VSO Inspector	3	2	2	4	1
CDRoller	4	4	3	4	1
CD/DVD Diagnostic	4	3	1	3	1
Total	17	16	16	17	7

Una vez ponderada la matriz, se normaliza la matriz dividiendo para el total cada uno de los criterios de selección. Como se observa en la Tabla 14

Tabla 14

Matriz de selección del tipo de herramienta

	Criterios de selección				
Alternativas	**I**	**II**	**III**	**IV**	**V**
Caine	0,059	0,313	0,313	0,294	0,286
CD and DVD Inspector	0,294	0,125	0,313	0,059	0,286
VSO Inspector	0,176	0,125	0,125	0,235	0,143
CDRoller	0,235	0,250	0,188	0,235	0,143
CD/DVD Diagnostic	0,235	0,188	0,063	0,176	0,143
Total	1	1	1	1	1

Al contar con la matriz normalizada se multiplica cado uno de los criterios por la ponderación, y se suma por cada alternativa de diseño obteniendo como resultado la tabla 15.

Tabla 15

Resultado de selección de tipo de herramienta

	Criterios de selección						
Alternativas	I	II	III	IV	V	∑	%
Caine	0,006	0,094	0,125	0,029	0,029	0,283	28,3
CD and DVD Inspector	0,029	0,038	0,125	0,006	0,029	0,226	22,6
VSO Inspector	0,018	0,038	0,050	0,024	0,014	0,143	14,3
CDRoller	0,024	0,075	0,075	0,024	0,014	0,211	21,1
CD/DVD Diagnostic	0,024	0,056	0,025	0,018	0,014	0,137	13,7

Por lo tanto la herramienta más adecuada para realizar el análisis forense de dispositivo de almacenamiento óptico, es la opción de Caine ya que sus características son acorde a los requerimientos de la investigación. (Tufiño, 2012)

3.5.3 Entorno de Investigación Asistido Por Computadora (CAINE)

Caine (Entorno de Investigación Asistido Por Computadora) es una interfaz gráfica homogénea, ofrece un entorno Linux completo que guía a los investigadores digitales en el proceso de adquisición y análisis de las pruebas, lleva cientos de aplicaciones instaladas con el objetivo de facilitar la tarea del analista forense.

Esta herramienta permite hacer peritaje a cualquier dispositivo de almacenamiento siguiendo un protocolo y no contaminando la información.

Los desarrolladores Nanni Basseti y su equipo liberan nuevas versiones de CAINE (Computer Aided INvestigative Environment) basada en Ubuntu, las cuales son especializadas en el análisis forense y la recuperación de datos, llegando hasta hoy a su sexta edición.

CAINE permite determinar información clave de los archivos que están en los dispositivos (fecha de borrado, cuando fue creado, como y cuando fue guardado, etc.), pudiendo conseguir información que de ninguna otra manera se lo podría hacer.

Características

- Entorno de trabajo orientado a completar las fases de la metodología forense (Preservación, Recolección, Análisis, Reportes).
- Entorno gráfico amigable.
- Es Open Source, la herramienta está completamente abierta.
- Disponible para Linux, Ubuntu como sistema base, esto involucra un factible uso y fácil instalación o adaptación sobre nuestro entorno de trabajo.
- Generación semiautomática de reportes
- Contiene muchas herramientas usadas en el ámbito de la seguridad informática, como qPhotorec sirve para recuperar datos, Guy Manager permite generar imágenes de un disco duro, Autopsy o el programa ip Backup Analizer, con el que analiza el contenido de la copia de seguridad de los iPhone (historial de llamadas, navegación y favoritos de Safari, mensajes, etc.). (Untiveros, 2011)

3.6 Normas y estándares

3.6.1 ISO/IEC 27037

3.6.1.1 Introducción

El análisis forense tiene un modelo de actuación frente a delitos informáticos dependiendo de las leyes de cada país.

En el desarrollo de un análisis forense, los investigadores acuden a buenas prácticas internacionales con el fin de identificar, preservar, analizar y presentar evidencia que sea realmente válida.

Esta evidencia es un elemento que pretende obtener calidad probatoria, precisión en el análisis, restauración del servicio y costo de la recolección de la evidencia la cual es condesciende para la valoración y análisis que motive y concrete juicios bien fundados.

Las normas y estándares nacen a partir de experiencias sobre las necesidades, limitaciones y dificultades que han surgido consecuentemente a la hora de validar los resultados periciales de un sistema electrónico, con el objetivo de formar parte en un proceso legal. (Roatta, Casco, & Fogliato, 2015)

Intrínsecamente en la seguridad informática se destaca la normativa de la familia ISO 27000. La cual posee una serie de normas que son estándares de seguridad generalizados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

Existe una norma dedicada exclusivamente al análisis forense, se trata de la ISO 27037 la cual da directrices para identificar, recolectar, adquirir y preservar la prueba digital, esta norma nos ayudara durante todo el proceso de nuestra investigación.

(Gervilla, 2014)

- **Objetivos de la norma ISO/IEC27037**

Aplicar la norma ISO/IEC27037 en el manejo de evidencia digital contenida en dispositivos de almacenamiento óptico.

Identificar normativa del Ecuador para el manejo de la evidencia digital presente en dispositivos de almacenamiento óptico, aplicable a la Norma ISO/IEC 27037

3.6.1.2 Marco referencial

Tronco normativo de Seguridad Informática ISO 27000

- ISO/IEC 27037:2012 Guía para la Identificación, recolección, adquisición y preservación de evidencia digital.

- Diseño de un plan de gestión de seguridades de la información para instituciones públicas ecuatorianas. Tesis presentada por: Paola Chicaiza y Alex Diaz, República del Ecuador, Universidad Politécnica Nacional, Abril 2014. La tesis citada aporta a la presente investigación con información muy interesante sobre la problemática de la seguridad de la información en las instituciones púbicas, y analiza las leyes y normativas vigentes en el Ecuador basado en la familia de las normas NTE INEN-ISO/IEC 27000.

- Manejo de evidencia digital en dispositivos de almacenamiento pendrive USB aplicando la norma ISO/IEC 27037:2012. Monografía presentada por: Ing. José Bernardo Cortés De La Rosa, República de Colombia, Universidad Nacional abierta y a distancia Escuela de ciencias básicas, tecnología e ingeniería especialización en seguridad informática, Pasto 2014. La monografía señalada aporta a la presente investigación con conocimiento sobre la norma ISO/IEC 27037:2012, los procedimientos y lineamientos que se debe tener en cuenta durante la identificación, recolección y preservación de la evidencia, y aplicándolos al análisis de los diferentes tipos de dispositivos que puedan contener evidencia de naturaleza digital.

- Informática Forense en el Ecuador Una mirada Introductoria, Investigación presentada por: Dr. Santiago Acurio Del Pino, Republica del Ecuador, Fiscalía General del Estado Ecuador, Diciembre 2009. La investigación mencionada aporta al presente trabajo con conocimiento e información sobre los problemas surgidos por la mala utilización de las TIC (Tecnologías de la Comunicación e Información), como delitos y fraudes relacionados con las tecnologías en el Ecuador y un análisis exhaustivo sobre la evidencia digital.

- Inserción Jurídica de la Informática Forense, tesis presentada por: Almeida Romo, Omar Ramiro, Republica del Ecuador, Universidad Técnica del Norte, Facultad de Ingeniería en Ciencias Aplicadas, Mayo 2011. Aporta al presente trabajo con

información de la realidad procesal en el Ecuador en relación a la informática forense.

3.6.1.3 Marco Conceptual

- Cadena de Custodia. “Es el conjunto de procedimientos tendientes a garantizar la correcta preservación de los indicios encontrados en el lugar de los hechos; durante todo el proceso investigativo, desde que se produce la colección hasta su valoración por parte de la autoridad competente” (Guerra, 2014)
- Delito Informático. Acto ilícito sancionado penalmente, utiliza medios computacionales, telemáticos o electrónicos para el cometimiento del hecho delictivo. (Cuenca, 2013)
- Evidencia Digital. Información que se encuentra en formato digital estableciendo una amplia relación entre el delito y el autor, se lo utiliza como prueba legal. (Cortés, 2014)
- Función Hash. Operación que se realiza sobre un conjunto de datos obteniendo otro conjunto de datos denominado “resumen”, con un tamaño independiente del tamaño original, con la propiedad de estar asociado a los datos iniciales. (Cortés, 2014)
- Norma ISO/IEC 27037. Esta directriz proporciona lineamientos para el manejo de Evidencia Digital, proporciona pautas en actividades específicas como identificación, recolección y preservación de evidencia digital y puede intervenir como valor probatorio. (Presman, 2014)

3.6.1.4 Marco Legal

El delito informático empezó en el Ecuador desde 1999, este se puso en auge con la iniciativa del proyecto de la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, para la discusión de la Ley intervinieron organizaciones que se encontraban interesados como CONATEL, la Superintendencia de Bancos, las Cámaras de Comercio y otros, entidades.

La ley se presentó en un inicio con una serie de falencias, que hasta hoy se siguen puliendo, sobre todo basada en la realidad del Ecuador, se ha realizado cambios de manera más frecuente en la parte penal. (Almeida, 2011)

El Gobierno de Ecuador en los últimos años ha realizado un enorme esfuerzo en el perfeccionamiento normativo sobre el manejo de evidencia digital para evitar cualquier delito, promoviendo una reglamentación que da cumplimiento a los derechos de los ciudadanos u organizaciones empezando con una estructura de la unidad de delitos informáticos la cual se muestra en la Figura5, permitiendo que estas cuenten con herramientas necesarias para investigar, procesar, judicializar y penalizar gestiones criminales en las cuales se dé la intervención de medios informáticos.

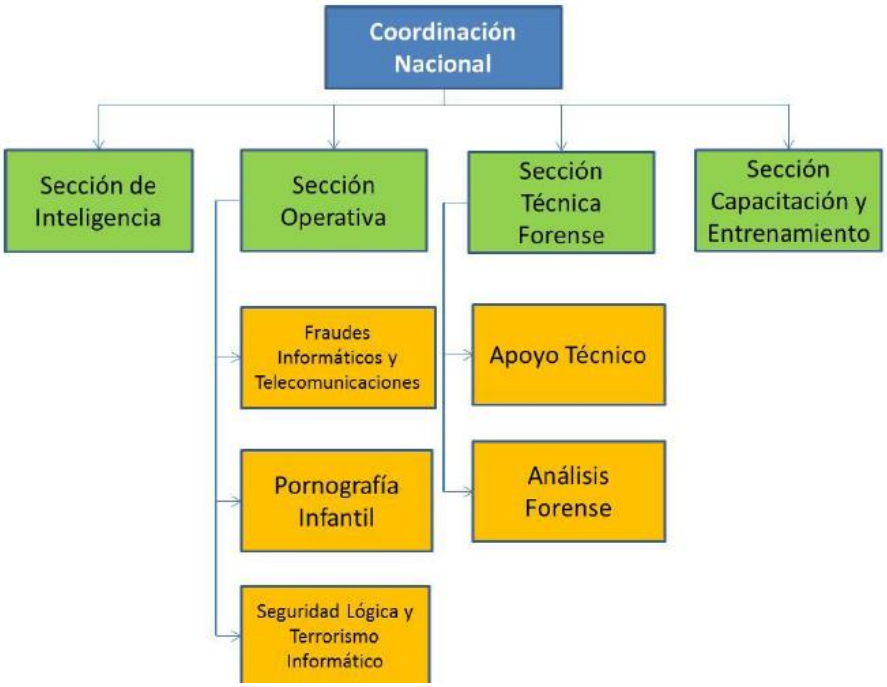


Figura 5 Estructura de la Unidad Delitos Informáticos Ministerio Público

Fuente: (Almeida, 2011)

Entre la normatividad existente se destaca:

- **Constitución Política del Ecuador**

Los artículos que se manifiestan no hacen referencia explícitamente al tema, pero es importante para esta temática tener en cuenta al manejar la información en casos específicos.

Art. 18 No existirá reserva de información generada por entidades públicas para las personas que deseen acceder a la misma excepto casos establecidos en la ley. Para este artículo se requiere contar con procedimientos de seguridad para el manejo de información.

Art. 389 El Estado garantiza el derecho a las personas a la protección frente a los desastres antrópicos mediante la prevención, mitigación, recuperación y mejoramiento de las condiciones minimizando la vulnerabilidad. En este artículo mencionan los desastres antrópicos que son incidentes de seguridad ocasionados por personas, se basa básicamente en el tratamiento del riesgo, siendo parte de la norma ISO/IEC 27037. (Asamblea Constituyente de Ecuador, 2008).

- **Código Orgánico Integral Penal**

Los artículos del código orgánico integral penal con respecto a la temática son acerca de delitos contra la seguridad de activos de los sistemas de información y comunicación, los cuales son:

Art. 229: Personas que infringen la ley de la privacidad revelando información contenida en archivos, base de datos o medios semejantes a través de un sistema electrónico o informático , las cuales se sancionaran con pena privativa de libertad de uno a tres años.

Art. 230: Interceptación ilegal de datos, personas que de alguna forma graven o alteren datos informáticos, las cuales se sancionaran con pena privativa de libertad.

Art. 231: Transferencia electrónica de activo patrimonial, donde la persona altere, manipule o modifique el funcionamiento de algún sistema informático para gestionar la

apropiación no consentida de algún activo patrimonial de otra persona en perjuicio de esta, las cuales se sancionaran con pena privativa de libertad de tres a cinco años.

Art. 232: Ataque a la integridad de sistemas informáticos, sanciona a las personas que atenten contra la integridad física y lógica de sistemas informáticos.

Al referirse a daño lógico trata sobre borrar, alterar, causar mal funcionamiento, suspenda , etc., con el fin de comprobar la validez de los mismo para ser manipulados como evidencia dentro de un delito

Art. 234: Acceso no consentido a un sistema informático, telemático o de telecomunicaciones, ayuda al análisis forense para evitar que datos e imágenes guardados en el dispositivo pueda generar un acceso no permitido. (Asamblea Nacional del Ecuador, 2014)

Algunos artículos están relacionados con las ciencias forenses en un entorno legal y procesos de tratamiento de evidencias, los cuales se mencionan a continuación:

Art. 449: Atribuciones que deben llevar el personal del sistema especializado integral de investigación como comunicar cualquier delito al fiscal, realizar las diligencias investigativas como entrevistas, tomar medidas adecuadas y oportunas, y lo más importante resguardar, vigilar, proteger y preservar la evidencia.

Art. 456: Aplicar cadena de custodia a los elementos físicos o contenido digital como materia de prueba con el fin de garantizar la autenticidad, integridad y conservación de estado original de la evidencia, llevando documentación de los hechos de cada custodio.

Art. 457: Criterios de valoración, se realiza la valoración de las pruebas en base a su autenticidad, sometimiento a cadena de custodia y en base a informes periciales fundamentados científicamente.

Art. 500: Contenido digital, hechos y representación informática que contiene conceptos de la realidad, almacenados o transmitidos por cualquier medio tecnológico.

Se menciona algunas reglas en la investigación las cuales son:

- Se realizara el análisis, recuperación y presentación del contenido digital a través de técnicas digitales forenses.
- Cuando el contenido digital se encuentre en equipos informáticos no volátiles se realizará su recolección, en lugar y tiempo real, con técnicas digitales forenses para preservar la integridad, se aplicará cadena de custodia, se realizará valoración y análisis de contenido. (Asamblea Nacional del Ecuador, 2014)

- **Ley de Comercio Electrónico, firmas electrónicas y mensaje de datos**

Esta ley regula la utilización de sistemas de la información y es importante para el análisis ya que es reconocida como evidencia digital dentro de un proceso penal, en la actualidad la utilización de estos servicios es casi un hábito para la humanidad por lo cual es necesario regularlos y controlarlos mediante esta Ley, puesto que es indispensable que los ecuatorianos cuenten con herramientas jurídicas que permitan el buen uso de las mismas.

Se dará un breve detalle de algunos de los artículos de esta ley:

Art. 4: Los mensajes de datos se someterán a la ley de propiedad intelectual, reglamentos y acuerdos internacionales.

Art. 5: Principios de confidencialidad y reserva de mensajes de datos.

Art. 7: Originalidad de datos, conservando integridad y veracidad, logrado por procedimientos para verificar si ha sido modificado.

Art. 8: Conservación de información de mensaje de datos mediante las siguientes condiciones:

- Accesibilidad de consulta
- Conservación del formato
- Conservación de información
- Garantiza integridad según la ley.

Art. 9: Se mantendrá la protección de datos, la recopilación y los usos de datos personales estarán basados en los derechos de privacidad.

Art. 12: Duplicación de mensaje de datos, cada mensaje se estudiara de manera diferente ya que se tendrá que verificar técnicamente la autenticidad

Art. 14: La firma electrónica tendrá la misma validez y pasara por los mismos procedimientos jurídicos que una firma manuscrita y será admitido como prueba.

Art. 15: Requisitos para la validez de una firma electrónica:

- Ser individual
- Posible de verificarla autoría mediante dispositivos técnicos
- Método de creación y verificación sea confiable.

Art. 17: Obligaciones del titular de la firma electrónica:

- Tomar medidas de seguridad para mantener su firma bajo su estricto control y evitar la utilización no autorizada,
- Notificar si existe cualquier manejo de personas no autorizadas.

Art. 20: Certificado de firma electrónica para certificar la identidad del titular y su uso con apego a la ley.

Art. 25: Suspensión de certificado de firma electrónica si se comprueba la falsedad de datos.

Art. 28: Reconocimiento internacional de certificados de firma electrónica, tendrá el mismo valor legal que los certificados acreditados, expedidos en el Ecuador. (Pleno del Congreso Nacional del Ecuado, 2002)

3.6.2 Evidencia digital

La evidencia digital es cualquier tipo de información (datos almacenados en formato binario) construida por campos magnéticos y pulsos electrónicos, extraída de un

medio informático físico o lógico que están involucrados en el cometimiento de algún acto ilícito, por medio de herramientas de técnicas especiales se puede recolectar, almacenar y analizar datos con el fin de guiar a los investigadores al descubrimiento de posibles infractores.

Entre algunas características se puede mencionar:

- Volátil
- Duplicable
- Alterable y modificable
- Eliminable
- Frágil

Con su equivocada manipulación la evidencia digital puede producir contaminación, y alterar su contenido. (Cortés, 2014)

3.6.2.1 Principios de la evidencia digital

La norma establece los principios de:

- Relevancia.- La evidencia digital debe relacionarse con los hechos investigados.
- Confiabilidad.- la evidencia que se extrae u obtiene debe ser fiable, repetible y auditable, si un tercero sigue el mismo proceso, deberá obtener resultados similares que se verifique y se comprueben.
- Suficiencia.- con las evidencias recolectadas se tiene elementos suficientes para sustentar los descubrimientos y confirmar aseveraciones efectuadas sobre la situación investigada. Este elemento está sujeto a la experiencia y formalidad del perito informático.

Estos tres elementos definen la formalidad de cualquier investigación basada en evidencia digital, y para que sea admisible en corte o no.

Al documentar todas las acciones, se deben regir a los siguientes principios:

- Disminuir la manipulación de la evidencia digital
- Documentar cualquier gestión que involucre un cambio irreversible
- Sujetarse a las leyes

- No excederse del límite en sus funciones. (ISSA Argentina, 2014)

3.6.2.2 Procesos para la evidencia digital

La norma está estructurada en tres procesos diferentes que se aplican a cada tipología de dispositivo:

- **Identificación** Localización y reconocimiento de las potenciales evidencias digitales.

- **Recolección y/o Adquisición** Se incautara la evidencia, copia forense y documentación, esta se verificara por medio de un método de verificación probado y se traslada al laboratorio para su adquisición, en función del tiempo y recursos disponibles en el hecho.

- **Preservación** La evidencia se debe preservar para asegurar en todo el proceso la integridad de la información y los requerimientos especiales dependiendo de cada dispositivo, para que sean admitidas como pruebas. (Whos, 2014)

3.7 Cadena de custodia

La cadena de custodia es un procedimiento controlado de seguridad que requiere cuidado y resguardo, es aplicable a las evidencias relacionadas con el suceso, desde el momento en que se encuentran en la escena hasta su análisis en el laboratorio, con el fin de que no existan dudas sobre los elementos de prueba. (Peñaherrera & Duque, 2011)

2.7.1 Principios de cadena de custodia

- Aseguramiento de la prueba: protección de medios probatorios.
- Licitud de la prueba: medios de obtención de pruebas legales.

- Veracidad de la prueba: obtención y preservación de la autenticidad de las pruebas.
- Necesidad de la prueba: prueba útil a la investigación y que puede probar un hecho. (García C. , 2014).

La Cadena de Custodia, según el Código Orgánico Integral Penal, es garantizar la autenticidad e integridad de los elementos físicos o digitales que podrían transformarse en prueba.

3.7.1 Características de cadena de custodia

La caracterización de la cadena de custodia se da por una serie de rasgos distintivos que proveen una certificación del uso adecuado del proceso, entre las características más importantes se encuentran:

- Inicia desde la recolección y conocimiento de las pruebas, finaliza con el juez y los funcionarios.
- La cadena de custodia es un proceso manual en toda su vida útil.
- La custodia se aplica a todo elemento probatorio físico. Extendiendo la misma a la documentación que acompañe al material.
- La cadena de custodia están formados por personas que tienen la responsabilidad de proteger a los elementos de prueba
- La cadena de custodia tendrá el registro de: fecha, hora, nombre y firma de quien recibe y de quien entrega. (García C. , 2014)

3.8 Guía metodológica para el análisis forense de discos ópticos

3.8.1 Introducción

Con la investigación realizada sobre las normas y estándares que existen tanto a nivel nacional como internacional se ha constatado la necesidad de realizar un análisis forense sobre discos óptico por lo cual se utiliza una metodología práctica sistemática

que contenga pasos a seguir para realizar un análisis forense con garantías de éxito, buenas conclusiones a las que ayude a mejorar la calidad de peritaje.

Desde el punto de vista jurídico en relación al análisis forense como muestra la Figura 6, el hecho de que una investigación haya seguido pautas aceptadas y ordenadas en su proceso, facilitarían la tarea de jueces y magistrados para dictaminar la sentencia. (Miguez, 2015)

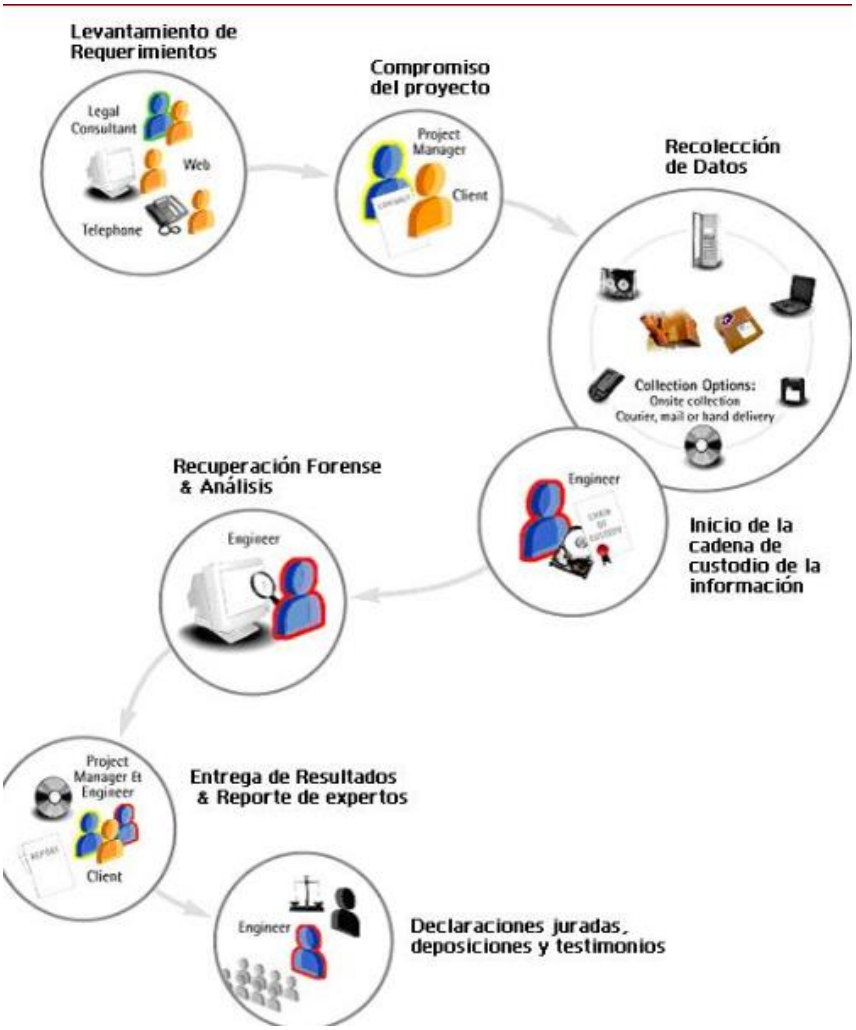


Figura 6 Parte del Proceso judicial en relación al análisis forense informático.

Fuente: (Ardita, 2007)

Por lo cual es pertinente dividir en distintas fases la metodología para obtener un análisis forense exitoso, se analizara en particular las fases descritas en la Figura 7.

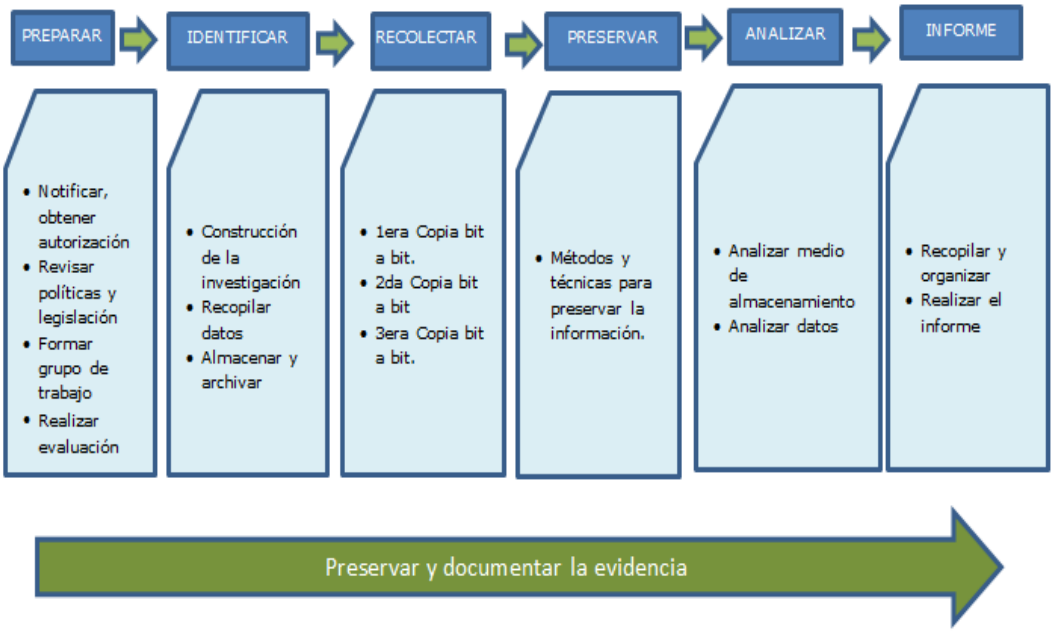


Figura 7 Metodología de análisis forense.

Fuente: (Gervilla, 2014) (DragonJAR, 2011)

3.8.2 Fases

Tomar conocimiento del hecho que ha ocurrido, es responsabilidad del investigador así como, realizar la observación de la escena, decidir acerca de la presencia de los peritos y planificar el procedimiento a seguir.

3.8.2.1 Preparación del escenario

En esta fase se realiza la recolección de evidencia se procede principalmente con:

- La escena del crimen.
- Recepción de solicitudes de análisis forense.
- Revisión de políticas y legislación en el Ecuador y a nivel internacional.
- Formación del equipo para el análisis forense.

- Reconocimiento de la organización.
- Reconocimiento del personal.
- Identificar y asegurar el escenario
- Identificar el incidente.
- Identificar cadena de custodia.
- Aseguramiento de la preservación de la evidencia.
- Establecer plan de acción. (Pinto, 2014)

Se debe asegurar y proteger el área donde se ha producido el incidente para verificar que no se haya alterado la escena esto se lo realiza desde el descubrimiento del delito hasta su posterior análisis, sin olvidar la documentación de todo lo realizado en el proceso.

Se recomienda realizar las fotografías del entorno del dispositivo con hora y fecha para que revele la evidencia del estado original del dispositivo y preferentemente el uso de guantes de látex para evitar contaminar las huellas dactilares. (POLICIA NACIONAL DE NICARAGUA, 2012)

3.8.2.2 Identificación y recolección de evidencias

Comprende dos tareas:

Identificación de evidencias y recolección de evidencias

a. Identificación de evidencias

Para el análisis de esta fase, se tomará en cuenta estas interrogantes:

- Qué evidencia hay?
- Dónde está?
- Cómo esta almacenada?

Comprende las siguientes actividades:

- Registro y contenidos del disco óptico
- Estructura física del disco óptico
- Datos contenidos en el disco óptico
- Documentos existentes

b. Recolección de evidencias

En esta fase se identifican, etiquetan, graban y recolectan los datos o información, preservando su integridad para su posterior estudio y análisis.

La recolección se lo realiza con los siguientes pasos:

- Para garantizar la aceptabilidad en el análisis forense es necesario realizar una copia exacta bit a bit del contenido de los discos incautados es decir todos los archivos ya sean temporales, ocultos, eliminados, sobrescritos, utilizando la herramienta necesaria.
- Verificación de la integridad de la copia, con el hash del disco original y el de la copia se puede certificar que ambos son idénticos, sirve para asegurarnos que no se han producido errores en el proceso de copia.
- Se realiza la segunda copia sobre la primera, esta será el respaldo en todo momento de igual manera se comprueba si son idénticos, sin embargo no se trabajara sobre esta.
- Se realiza la tercera copia la cual es la única con la que se va a trabajar, en caso de que se llegue alterar, se utiliza la segunda copia para crear otra y poder analizarla. (Gervilla, 2014)

Hasta esta fase se ha tomado la evidencia física, ha sido fotografiada previamente, y ahora se procederá a asegurar la evidencia, y para culminar se realizara el análisis electrónico de la misma. (Dueñas, 2014)

3.8.2.3 Preservación de las evidencias

En esta fase se toman todas las medidas técnicas para conservar la evidencia, como ya se dijo anteriormente debe tener la capacidad de reproducir la información contenida en el futuro.

Con una mala manipulación entorpecería el proceso de investigación, este factor estará presente en todas las fases del análisis forense al igual que las anotaciones descritas en la primera fase. (Derecho Venezolano, 2012)

Aparece la cadena de custodia que permite llevar de manera óptima este proceso, se aplica desde el inicio del perito, para ser manejado con los más estrictos estándares de preservación, con el fin de que conserve todas las características con que fue encontrado, para que al momento de ser analizado no pueda ser refutado y por ende alterado, el objetivo de esta es determinar quién accedió al dispositivo de evidencia, cuándo y para qué. (Académica México, 2014)

Con referencia al lugar de almacenamiento se debe tener cuidado con los discos ópticos, protegerlos contra electricidad o estática, con la utilización bolsas antiestáticas evitando manipulación descuidada, de igual manera el lugar donde se almacenara evadiendo sitios húmedos, cambios bruscos de temperaturas y cantidad de polvo.

3.8.2.4 Análisis de las evidencias

Se debe recolectar la máxima información y descartar datos que no tienen ninguna relevancia a la investigación.

El análisis de la evidencia digital es útil al reconstruir un delito porque puede proveer de detalles adicionales, los cuales pueden guiar al investigador hacia evidencia adicional, e inclusive hacia el mismo sospechoso del delito.

No existe un proceso estándar al cual regirse por lo cual se analizará cada caso por separado. (DocSlide, 2015)

Se destacan algunas técnicas o métodos de los cuales se podrán adaptar al proceso:

a. Preparar un entorno de trabajo

Lograr un entorno de trabajo adecuado para el análisis y la investigación. Se debe definir los equipos y la herramienta para llevar a cabo la investigación trabajar con la última copia de la evidencia.

Se tiene dos tipos de análisis:

- Análisis caliente, es realizar la investigación sobre los dispositivos originales, en modo de solo lectura, sin embargo tienen mayor riesgo.
- Análisis frio, admite realizar un análisis más exhaustivo y menos intrusivo con la evidencia original ya que permite montar imagen de disco en máquina virtual para su respectivo análisis, disminuyendo el riesgo. (La huella oculta Seguridad y Análisis Forense Informáticos, 2014)

b. Creación de la línea temporal

Su objetivo es el de intentar establecer el orden en el que se han ido ejecutando los distintos sucesos en los sistemas afectados, normalmente, por una intromisión maliciosa.

En esta línea temporal se registran los acontecimientos más relevantes del análisis del dispositivo como:

- Etiqueta de disco óptico.
- Nombre de archivos.
- Fecha, hora de creación o modificación.
- Tipo de archivo
- Tamaño del o los archivos. (Flu-Project, 2015)

Mediante una herramienta que se utilice se podrá encontrar información, ya sea archivos normales, temporales, ocultos, y eliminados sin descartar ninguna posibilidad de análisis.

Con respecto a los dispositivos ópticos se utilizan programas especiales para la recuperación de información, por ejemplo cuando un atacante elimine archivos o registros varios en afán de esconder lo que ha ocurrido, si esta información es recuperable se podrán situar en la línea temporal relacionándolos con el conjunto de sucesos. (Gervilla, 2014)

c. Determinar el origen del ataque

Determinar la utilización de documentos recientes accedidos a través de la unidad de CD.

Determinar cómo se realizó el ataque, manipulación del disco óptico, y vulnerabilidades de seguridad que se presentó. (Prezi, 2013)

Para esto se lleva a cabo una investigación sobre el disco óptico, con el fin de encontrar procesos que se han ejecutado y aquellos que han sido ocultos.

d. Identificación de autores

Para la identificación de autores se debe trabajar con prudencia, obtener y contrastar la información adquirida correctamente, es difícil averiguar el origen de un incidente por lo cual se debe evaluar los distintos perfiles de atacante para entender quién fue el infractor y llevar a cabo acciones legales.

Por una parte se tiene organizaciones dedicadas a este ámbito, en la cual su actuación va por el sentido económico, roban información muy reservada y las vende, y por otras personas naturales que buscan su beneficio personal.

Para un caso judicial se deberá encontrar un autor o al menos pistas fiables para los peritos.

e. Impacto causado

Dentro de un proceso de investigación el mayor impacto será cuantificadas sumas de dinero por la afectación del delito en comparación con otros impactos que pueden aparecer.

Se podrá utilizar el método BIA (Business Impact Analysis), que determina el impacto de daño económico con relación a ciertos eventos, que se considerara en función de los ítems afectados tras el delito, esta guía determina que necesita ser recuperado y el tiempo que tarde dicha recuperación. (Seguridad de la Información en Colombia, 2010)

Se puede evaluar como coste económico, a los daños que puede generar el robo de información secreta de alguna entidad, en cuanto se verá afectada su imagen siendo un daño incalculable, y cuanto retrasara la producción si es el caso, también el reemplazo de una maquina o de dispositivo que ha quedado inservible tras un ataque o mal uso.

3.8.2.5 Informe

Se basa en la buena redacción de informes en donde se registren cada antecedente o acontecimiento del evento, todo el trabajo realizado, conclusiones e impactos del delito.

Se puede realizar dos tipos de informe según sea el requerimiento, ambos contienen la misma información pero varía el enfoque y el grado de detalle.

a. **INFORME EJECUTIVO**. Se utiliza un lenguaje claro evitando expresiones confusas ya que va dirigido al gerente y juez los cuales no estarán muy involucrados con el tema técnicamente. Por lo cual se deberá facilitar este tipo de información.

Este deberá contener:

- Motivos del delito:

Razón del incidente

Finalidad del intruso

- Acción del delito:

¿Cómo lo hizo?

¿Qué hizo?

- Resultado del análisis:

Explorar causas.

Daños provocados y su proyección al el futuro.

Información del autor

Tipo de sanción.

- Recomendaciones:

Pasos posteriores a seguir.

Establecer técnicas de protección para no caer en el mismo delito.

Acción legal a tomar.

b. INFORME TÉCNICO. Se utilizará un lenguaje técnico, se detallarán procesos y herramientas software y técnicas utilizadas ya que las personas a las cuales se destinará están involucradas directamente en el conocimiento de los hechos.

- Referencias del incidente:

Situación actual y anterior al incidente.

- Recolección de datos:

Procedimiento del análisis de datos.

Información recolectada.

- Descripción de la evidencia:

Detalles técnicos de las evidencias recolectadas, estado, contenido, proceso.

- Análisis de la evidencia en la herramienta:

Información del uso de la herramienta.

Registrar información de las características del dispositivo, vulnerabilidades detectadas y metodología utilizada

- Resultados:

Obtener información de los archivos manipulados por el atacante.

Alcance del incidente.

Determinar el origen del incidente y como se ha encontrado.

Registrar la línea temporal de los hechos sucedidos con todo detalle posible.

Redactar conclusiones junto a valoraciones que se crean pertinentes a la vista de todo el análisis elaborado.

Establecer técnicas de protección para no repetir el incidente. (Gervilla, 2014)

CAPÍTULO 3

DESARROLLO DEL ANÁLISIS EN DISCOS ÓPTICOS

En este capítulo se procede a realizar el análisis forense, tomando como referencia los Discos Ópticos, utilizando la guía metodológica descrita en el capítulo 2

5.1 HERRAMIENTA

La herramienta a utilizar es Caine (COMPUTER AIDED FOR INVESTIGATIVE ENVIRONMENT) versión 4 instalado bajo Ubuntu

5.2 FASES

5.2.1 Preparación del escenario

Recolección de evidencia:

- Escenario: Laboratorio de Multimedia, bloque ¨H¨, cuarto piso de la Universidad de las Fuerzas Armadas.
- Recepción de solicitudes de análisis forense: Caso de estudio de tesis
- Revisión de políticas y legislación en el Ecuador y a nivel internacional: Descrito en el capítulo 2, Marco legal de informática Forense en el Ecuador.
- Formación del equipo para el análisis forense.

Tabla 16

Equipo de análisis forense

Nombres	Tipo
Gabriela Peñaherrera	Egresado de Sistemas e Informática
Daniel Orellana	Egresado de Sistemas e Informática
Germán Ñacato	Director de Tesis

- Reconocimiento de la organización: ESPE, Departamento de Ciencias de la Computación.
- Reconocimiento del personal: Personal del Departamento perteneciente al Laboratorio de Multimedia.
- Identificar y asegurar el escenario: Laboratorio de Multimedia
- Identificar el incidente: Análisis de información almacenada en discos Ópticos, ejemplo: DVD ¨Información Multimedia, 11/09/2015¨
- Identificar cadena de custodia: Garantizar el DVD bajo la custodia física de los tesistas antes mencionados, en la respectiva caja y hoja de entrega-recepción del disco óptico.
- Las fotografías del DVD para el respectivo análisis:

Tabla 17

Características de DVD

Disco Óptico	Datos
DVD	
Etiqueta	Con marcador verde: Información Laboratorio Multimedia, 11/09/2015
Hora y fecha	17:29 11/09/2015

5.2.1.1 Identificación y recolección de evidencias

Comprende dos tareas:

Identificación de evidencias y recolección de evidencias

a. Identificación de evidencias

Para el análisis se tomó en consideración los siguientes datos

Tabla 18

Identificación de evidencia

Datos	Evidencia
Evidencias: **Información Almacenada:**	- DVD: DVD-R / 16X, 4,7 GB, 2HR - Etiqueta: Con marcador verde: Información Laboratorio Multimedia, 11/09/2015 - Directorio: Plano - Archivos: • cumpleaños, 26/01/2015, Tipo: Adobe Illustrator, Tamaño: 4.489KB • la mejor música electrónica 2014-2015, 21/02/2015, Tipo: MP4 File, Tamaño: 278.980 KB
Lugar donde se encuentra:	Escritorio del Docente en el Laboratorio de Multimedia
Como está almacenado el DVD:	El DVD está en una caja plástica pequeña transparente.

b. Recolección de evidencias

Para realizar el análisis se utilizó una unidad de DVD externa con conector USB.

Pasos:

- Montar la unidad de DVD externa. Desde la opción Dispositivos/USB/unidad DVD, tal como se indica en la figura 8.

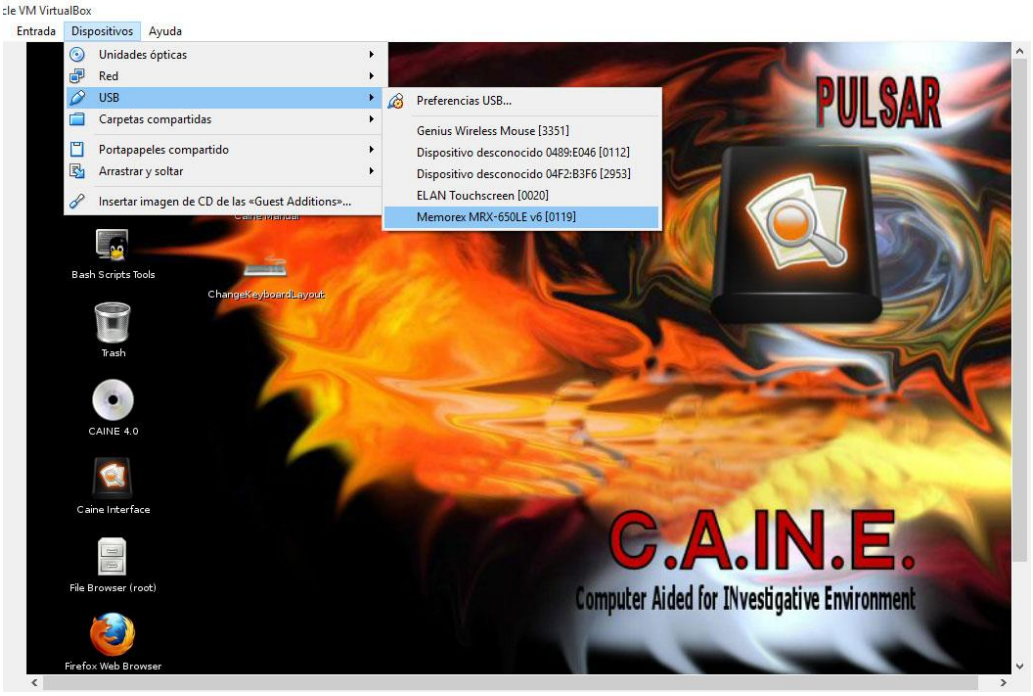


Figura 8 Montar unidad de DVD

- Desde la barra de tareas de Ubuntu hacer clic en SAFE, tal como se indica en la figura 9.

Figura 9 Opción SAFE

- Se desplegará la opción Mounter, hacer clic en el dispositivo el cual se desea montar para empezar a realizar la copia de bit a bit, tal como se indica en la figura 10.

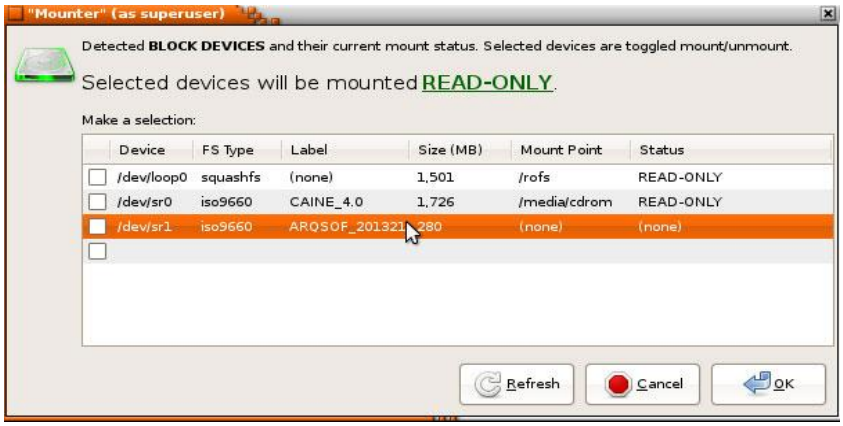


Figura 10 Opción Mounter

En esta fase se identifican, etiquetan, graban y recolectan los datos o información, preservando su integridad para su posterior estudio y análisis.

Recolección de datos: Para la recolección se utilizó el software de CAINE por cuanto permite realizar las imágenes de bit a bit. Se realiza los siguientes pasos:

Hacer clic en la opción Menú (ubuntu)/Forensic Tools/ AIR, como se muestra en la Figura 11:

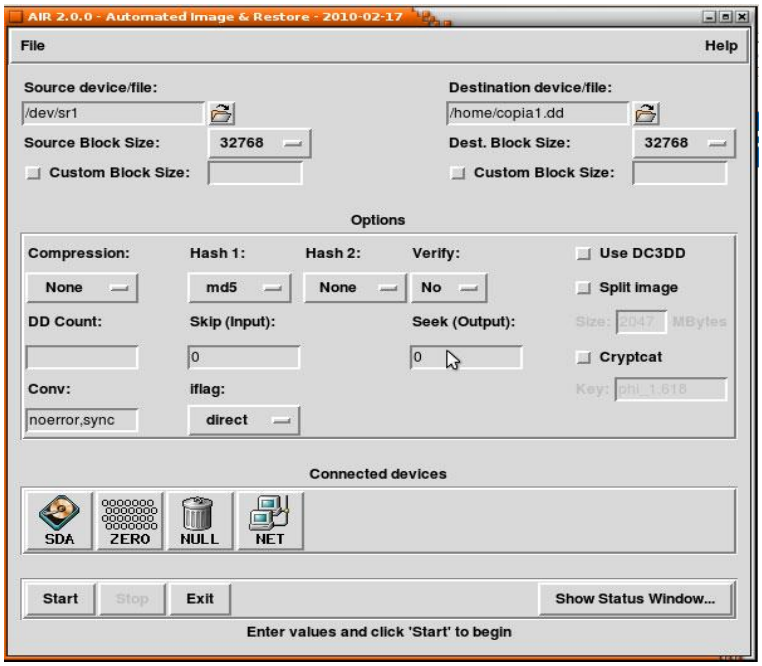


Figura 11 AIR Configuración para hacer copia bit a bit

Con la siguiente información:

Source device file: /dev/sr1 el cual se va a peritar.

Destination device/file: /home/copia1.dd representa la primera copia que se va a realizar.

Verify: No.

Desclickie en la opción Use DC3DD

- Se verifica la integridad de la imagen comparando el tamaño de la información del disco óptico del cual se va a realizar el análisis con el tamaño de la imagen creada en el AIR, como se muestra en la Figura 12:

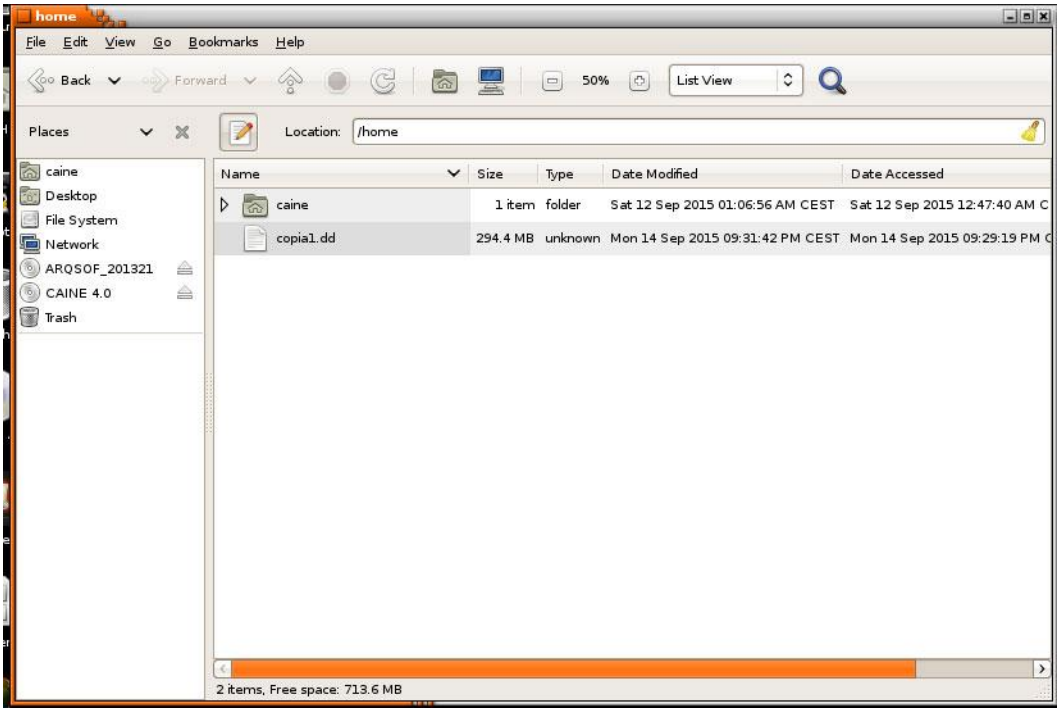


Figura 12 Creación de la imagen copia1.dd

- Se realiza la segunda y tercera copia, siguiendo el mismo proceso realizado en la primera copia.

5.2.1.2 Preservación de las evidencias

Se toman las medidas técnicas para conservar la evidencia de las copias generadas en el punto anterior, para su adecuada manipulación en el análisis forense.

Cadena de custodia

La cadena de custodia permite llevar de manera óptima el proceso de investigación, manipulando de acuerdo a la guía metodológica que se está describiendo en esta documentación, con el fin de conservar todas las características que fue encontrado el disco óptico de análisis para que al momento de ser analizado no pueda ser refutado y por ende alterado.

Se debe tomar en consideración quién accedió al disco óptico de evidencia, cuándo y para qué. (Académica México, 2014)

El dispositivo óptico debe almacenarse en un lugar protegido contra la electricidad o estática utilizando bolsas antiestáticas para evitar la incorrecta manipulación, el lugar donde se almacena no debe ser en sitios húmedos, cambios bruscos de temperaturas y cantidad de polvo.

5.2.1.3 Análisis de las evidencias

El análisis de la evidencia digital es útil al reconstruir un delito porque puede proveer de detalles adicionales, los cuales pueden guiar al investigador hacia evidencia adicional, e inclusive hacia el mismo sospechoso del delito, para lo cual se utilizó los siguientes pasos:

a. Preparar un entorno de trabajo

Para el respectivo análisis se trabajó en el Laboratorio de Multimedia con los siguientes recursos de hardware y software, para lo cual se detalla en el Anexo A (Descripción de Hardware y Software).

Se utilizó la siguiente técnica:

- Análisis frio, por cuanto se realiza un análisis exhaustivo y menos intrusivo con la evidencia original, montando la imagen de disco en máquina virtual para su respectivo análisis.

b. Creación de la línea temporal

Se crea la línea temporal, como se muestra la Tabla 19.

Tabla 19

Descripción de la información de la evidencia

Datos		**Evidencia**
Evidencias:	**Información Almacenada:**	DVD: DVD-R / 16X, 4,7 GB, 2HR -Etiqueta: Con marcador verde: Información Laboratorio Multimedia, 11/09/2015 Directorio: plano Archivos: • cumpleaños, 26/01/2015, Tipo: Adobe Illustrator, Tamaño: 4.489KB • la mejor música electrónica 2014-2015, 21/02/2015,tipo: MP4 File, tamaño: 278.980 KB

5.2.2 Procedimiento de análisis forense de discos ópticos

Para iniciar por primera vez una recolección y análisis de evidencia digital, es importante previamente haber obtenido la réplica o imagen del disco donde reside la evidencia.

Una vez generada la imagen se empleó para el análisis forense los siguientes pasos:

- Desde Menú (Ubuntu) seleccionar Forensic Tools / Autopsy, como muestra la Figura 13.

Figura 13 Menú Autopsy

- Se abre automáticamente en Firefox (u otro browser que esté instalado) la aplicación Autopsy, como muestra la Figura 14.

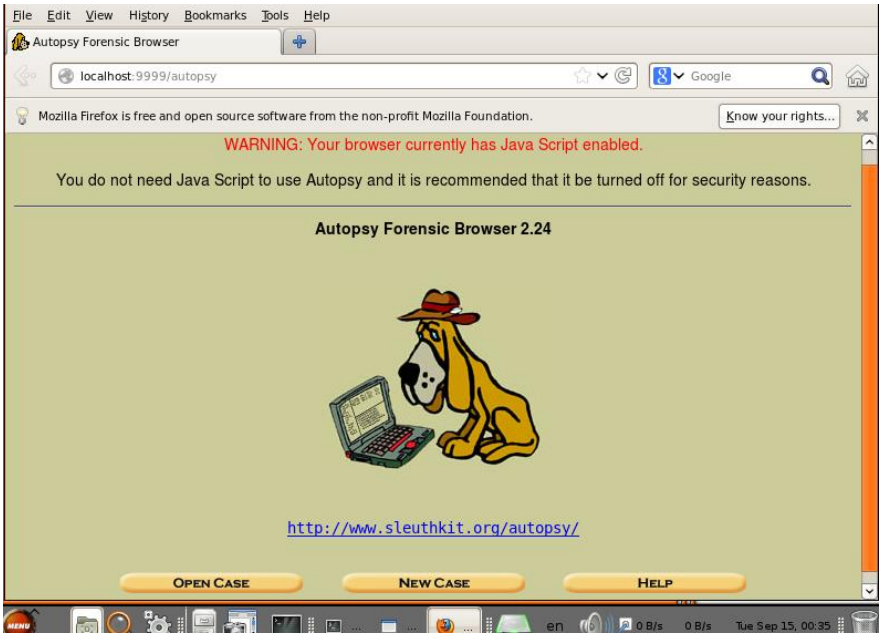


Figura 14 AUTOPSY

- Al dar click en el botón de New Case, se despliega un formulario para ingresar los datos básicos del nuevo caso (Nombre del caso, descripción, investigador), como se observa en la siguiente Figura 15.

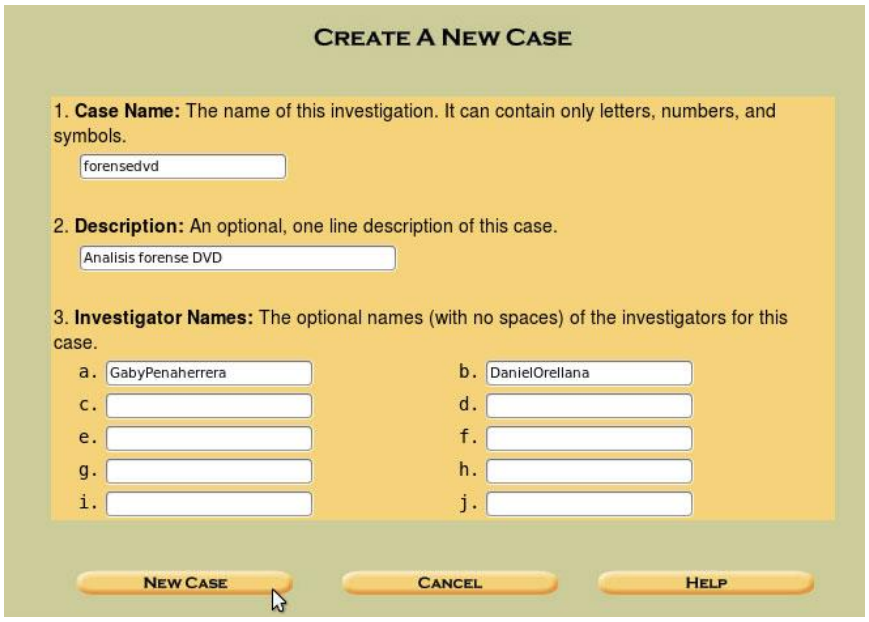


Figura 15 Creación de nuevo caso

- Luego se despliega una ventana sobre la descripción de la creación del caso forense, como se indica en la Figura 16.

Figura 16 Descripción caso creado

- Al hacer clic en Add Host de la Figura 16, se visualiza el resumen de las configuraciones anteriores, como se indica en la Figura 17.

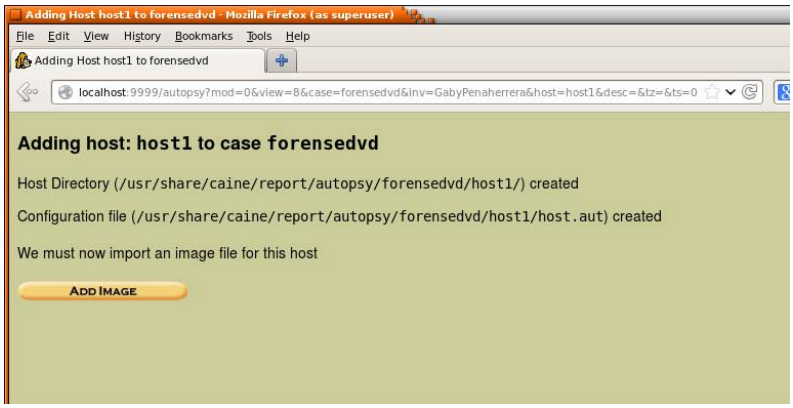


Figura 17 Creación del host

- Al hacer clic en el botón Add Image de la Figura 17, se activa la siguiente ventana como se indica en la Figura 18. Y se da clic en la opción Add Image File.

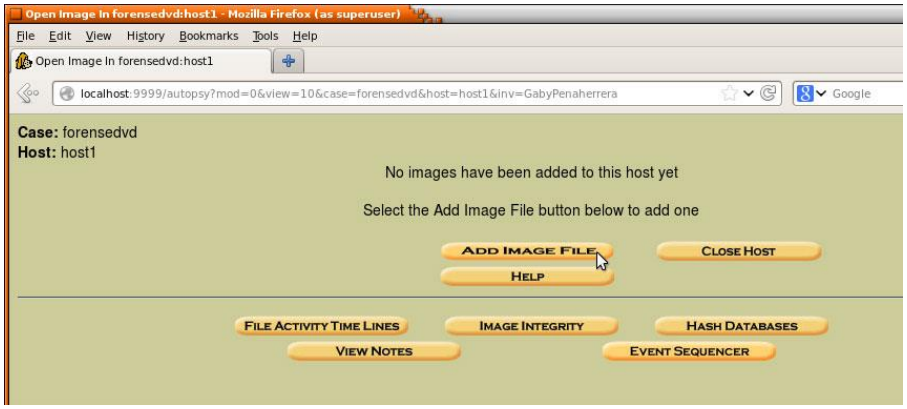


Figura 18 Opción agregar imagen

- A continuación se visualiza la siguiente ventana para llenar datos en donde está ubicado la copia del archivo imagen, tal como se muestra en la Figura 19, y hacer clic en Next.

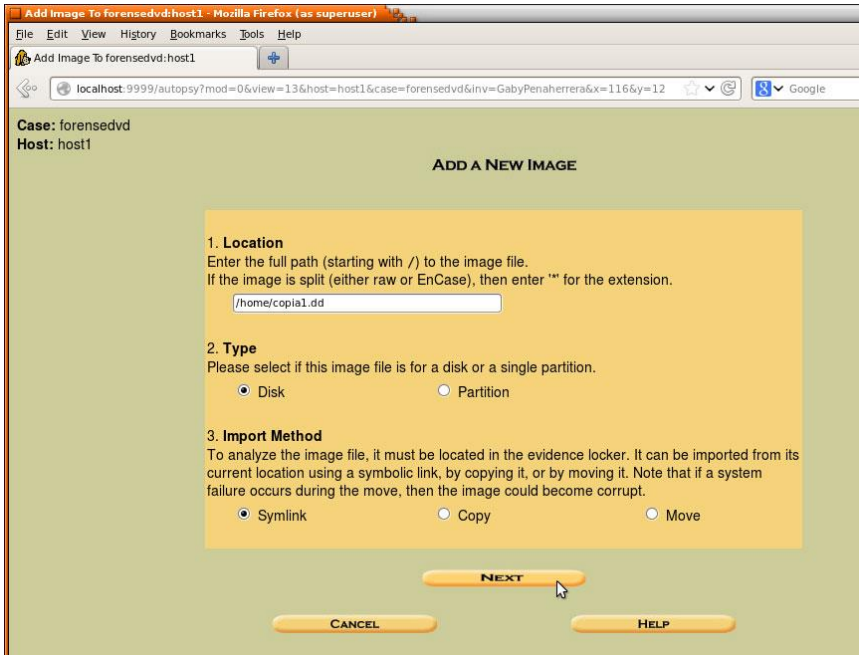


Figura 19 Agregar Imagen

- En la siguiente ventana se activa la opción de volumen imagen y hacer clic en Ok tal como se indica en la Figura 20.

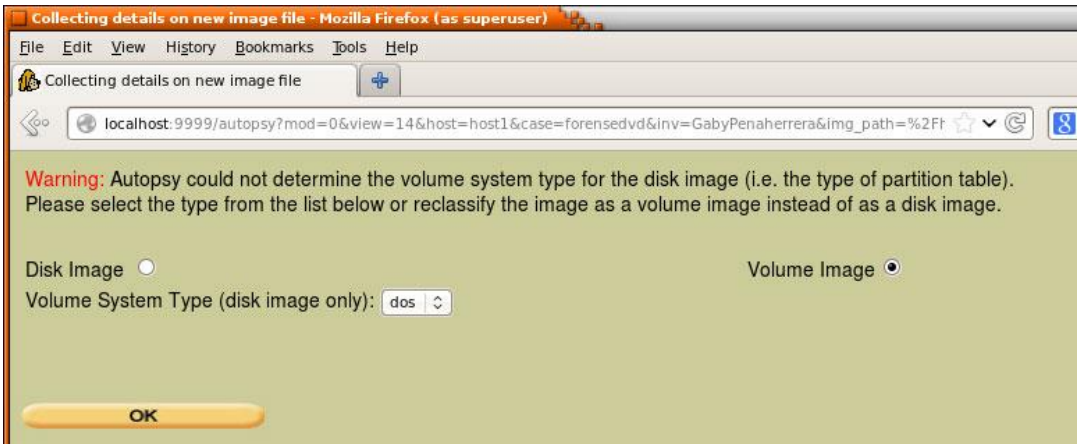


Figura 20 Determinación del volumen de la imagen

- A continuación se visualiza los detalles del archivo imagen y el detalle de los sistemas de archivos, como se indica en la Figura 21, luego hacer clic en Add.

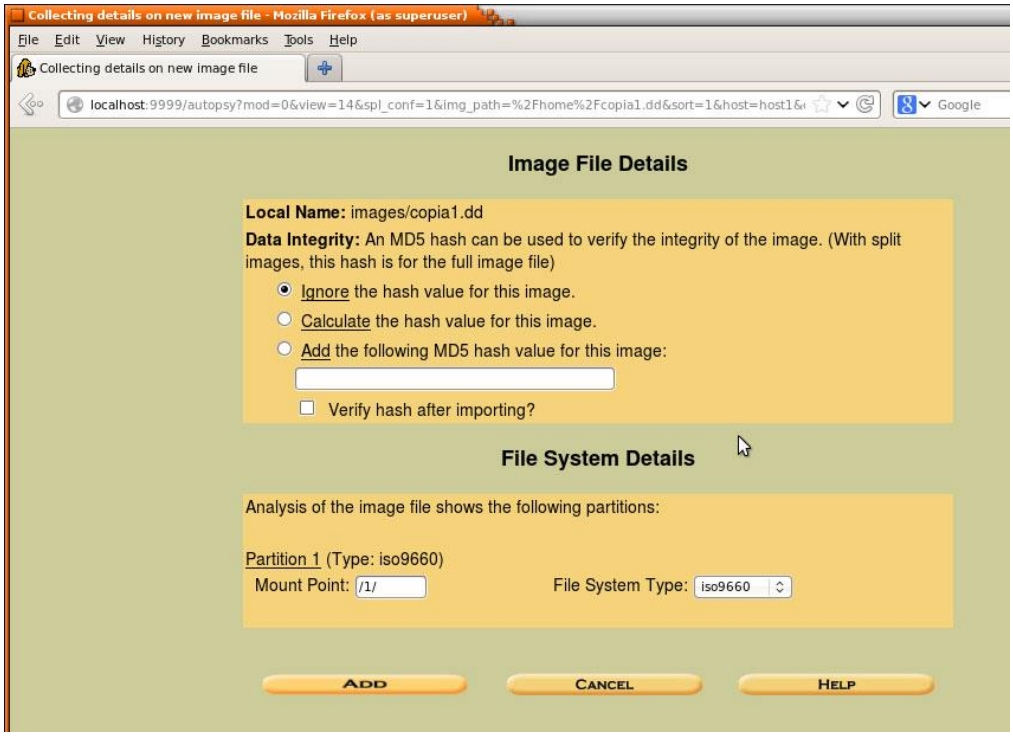


Figura 21 Detalles de la imagen

Una vez efectuado paso a paso los procesos anteriormente descritos, se obtienen los volúmenes que fueron encontrados en la imagen, para su respectiva exploración.

- Hacer clic en el botón Analize de la Figura 22, para que se proceda al análisis forense.

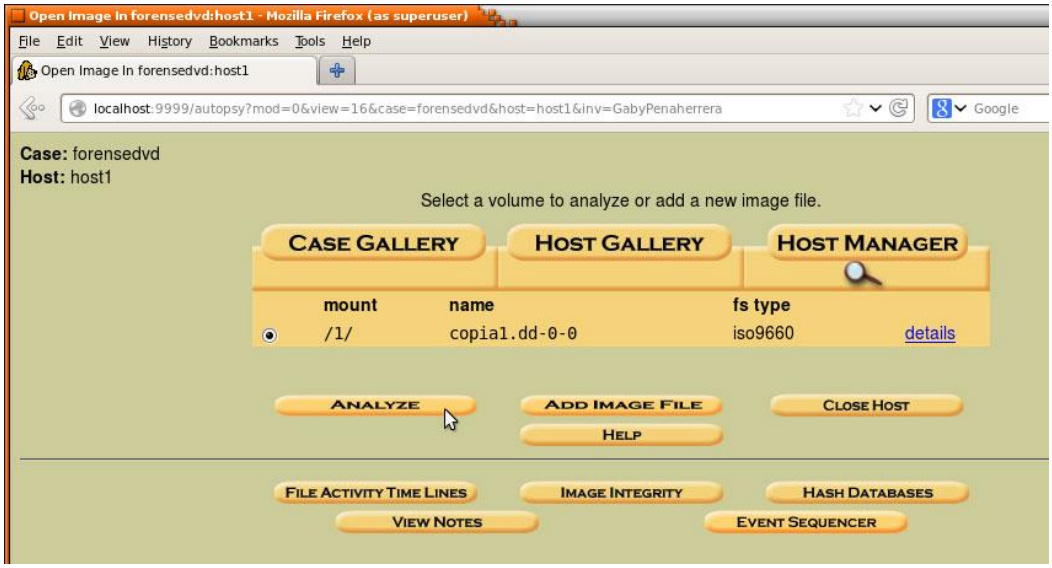


Figura 22 Opción Analize

- Hacer clic en la pestaña FileType de la Figura 23.

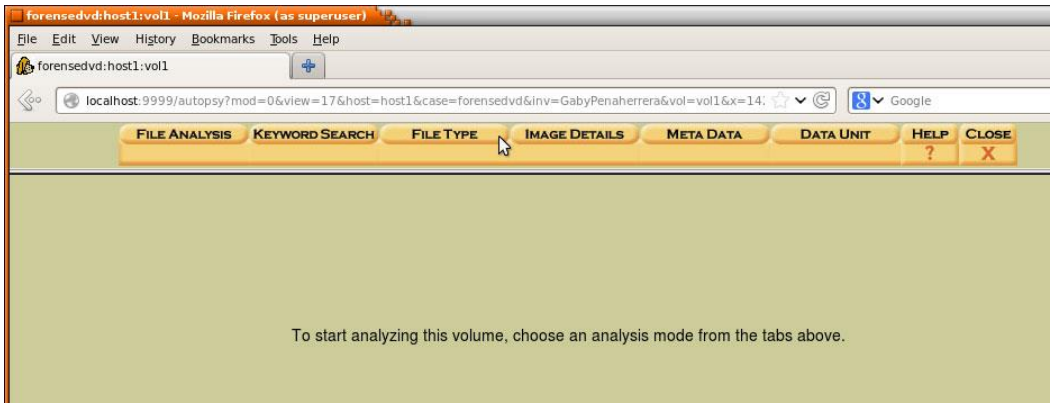


Figura 23 Opción File Type

- A continuación se visualiza la ventana de los resultados obtenidos del análisis forense. Se muestra las opciones Sort Files By Type y View Sorted Files para los reportes requeridos como se indica en la Figura 24.

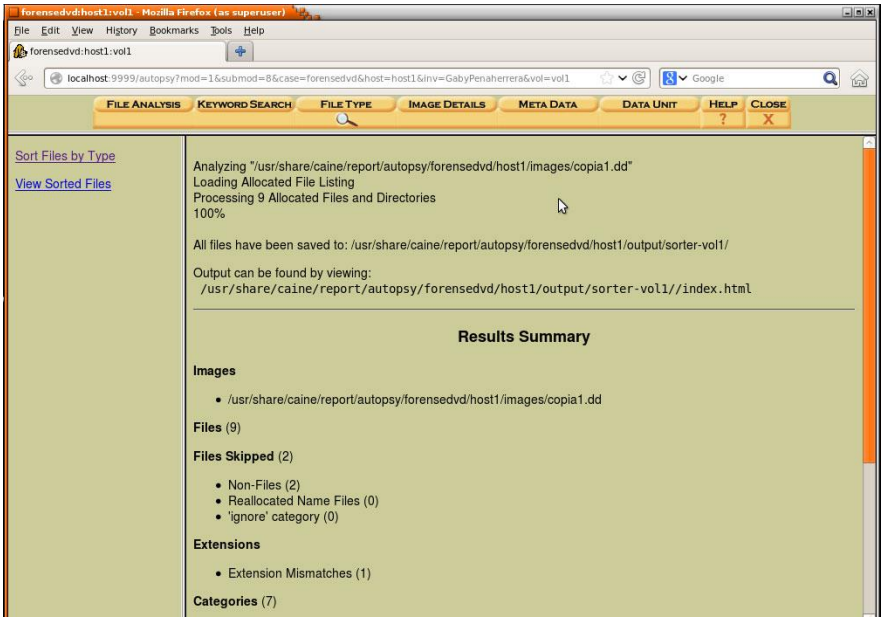


Figura 24 Resultado del análisis forense

- Seguidamente se selecciona el path:

usr/share/caine/report/autopsy/forensedvd/host1/output/sorter-vol1/, que se muestra en la Figura 25 y copiar en una nueva ventana del navegador, como se puede ver en la Figura 26 donde se visualizan los archivos que contienen información del análisis forense.

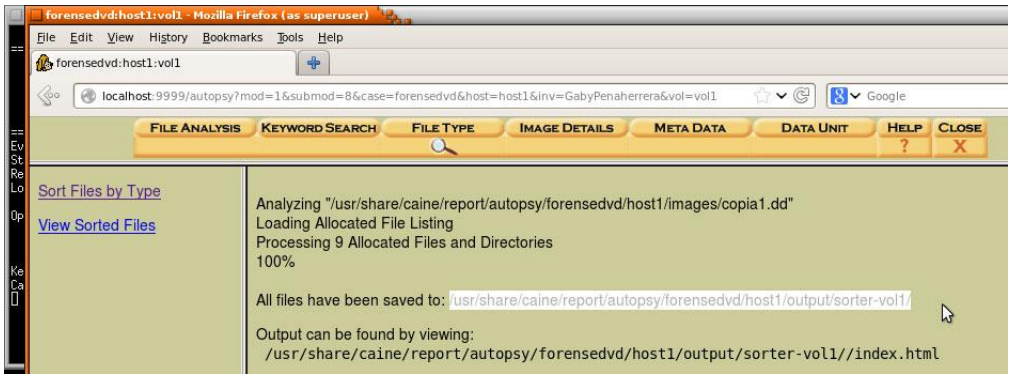


Figura 25 Path de información del análisis forense

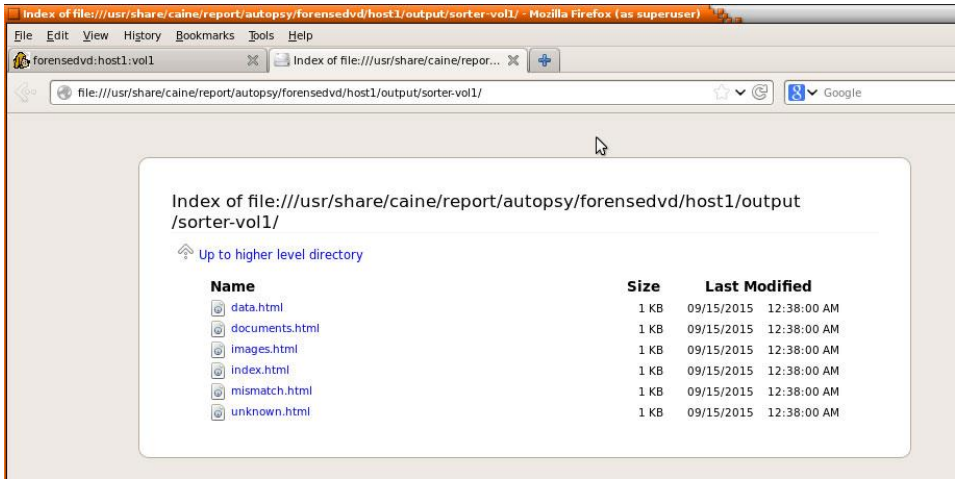


Figura 26 Archivos obtenidos del disco óptico

- Al dar un clic en el archivo data.html, se visualiza la siguiente información que corresponde al archivo PLANO.dwg que se encuentra en el directorio plano para su respectiva interpretación y estudio de dicho reporte, como se muestra en la Figura 27.

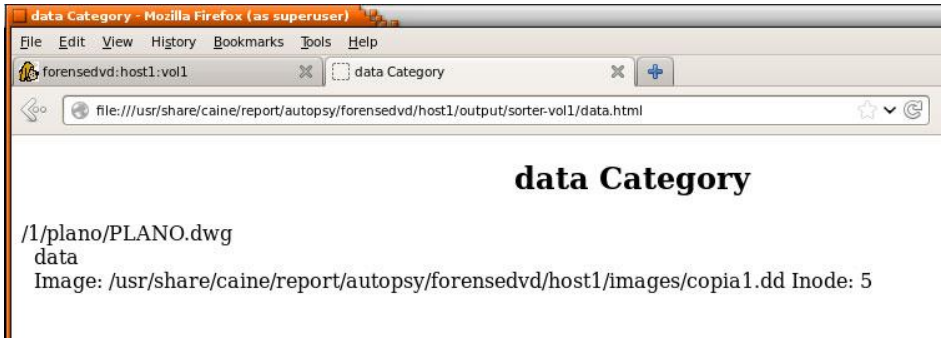


Figura 27 Información contenida en el archivo data.html

- De igual manera al dar clic documents.html de la Figura 26, se muestra la información referente en este caso a un archivo de nombre cumpleaños.ai, respaldo.vsd que está dentro de un directorio plano como se indica en la Figura 28.

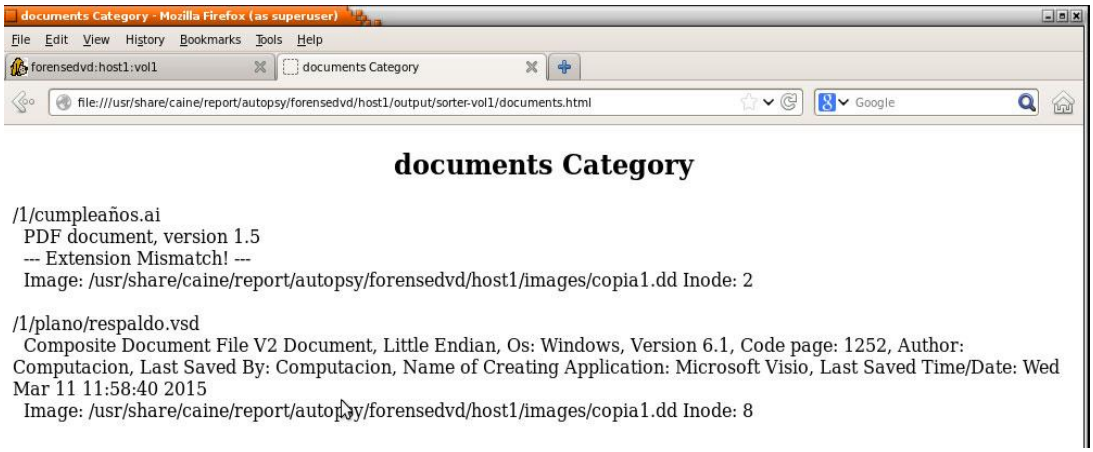


Figura 28 Información contenida en el archivo documents.html

- En la Figura 29, se indica otro archivo de nombre plano.jpg que está dentro del directorio plano y un archivo Sin-título-1.jpg.

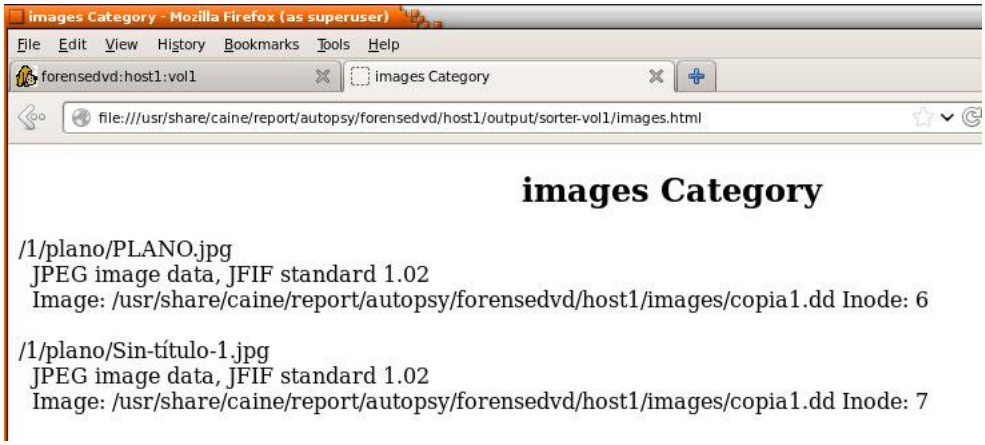


Figura 29 Información contenida en el archivo images.html

- Se describe la información de un directorio, La Mejor Música Electronica 2014-2015(REMIX) el mismo que contiene un video mp4, Figura 30.

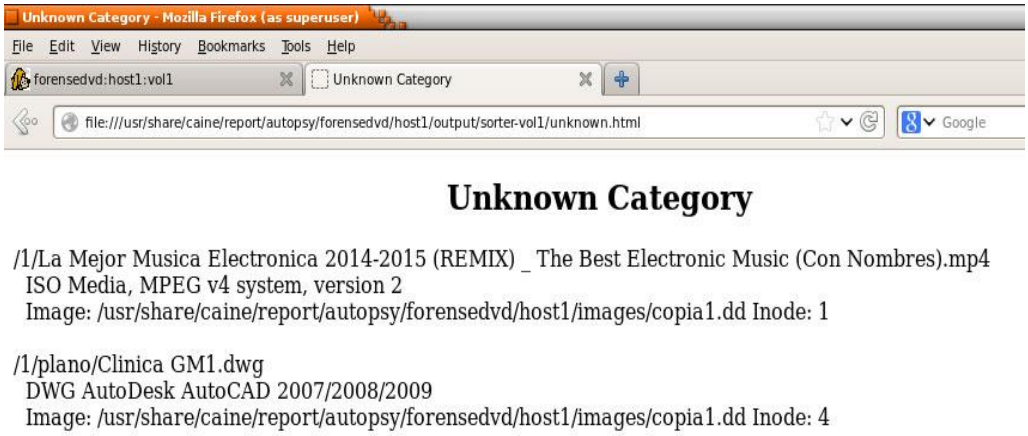


Figura 30 Información contenida en el archivo unknown.html

- **FILE ANALYSIS**

Al ingresar a la opción de análisis, se puede evidenciar cada uno de los archivos tanto temporales, permanentes, eliminados o averiados, que residen en la imagen o replica extraída del medio de almacenamiento original.

- Al hacer clic en la pestaña File Analysis que muestra en la figura 31, se genera un listado de los archivos para realizar el análisis de cada uno de ellos**.**

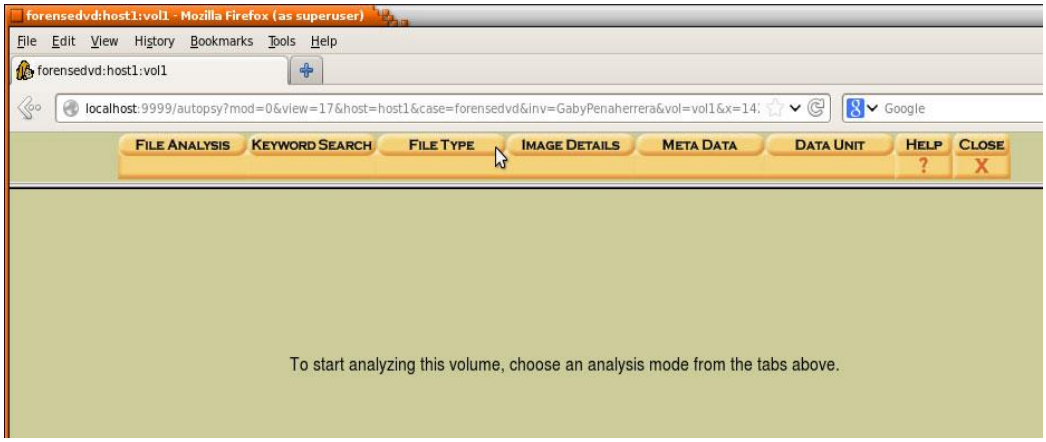


Figura 31 Opción File Analysis

- Al hacer un clic por ejemplo en el archivo cumpleaños.ai en la parte inferior de la ventana se visualiza la información del archivo correspondiente, como se visualiza en la Figura 32.

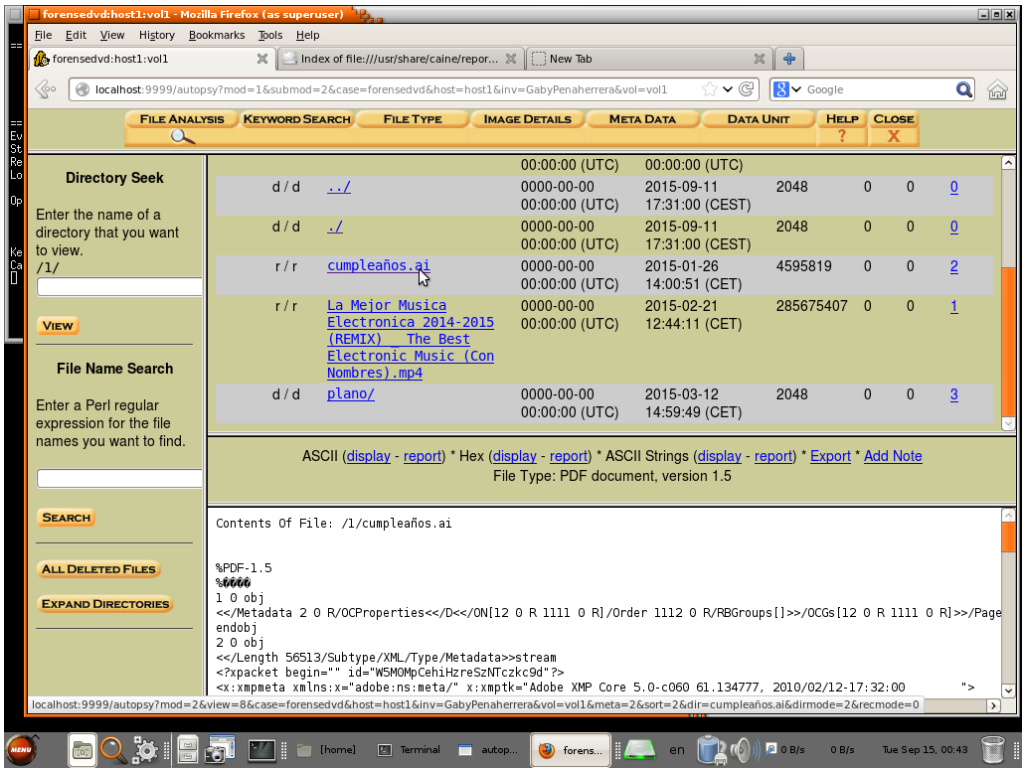


Figura 32 Detalle de archivos contenidos en el disco óptico

- La ventana anterior Figura 32, puede mostrar los archivos: que no son permanentes o que han sido borrados, se encuentra en color rojo, los demás archivo de color azul son permanentes. Teniendo en cuenta que la cantidad de archivos encontrados en la imagen puede ser demasiadamente extensa, Autopsy cuenta con una barra de menús, que tienen la opción de buscar archivos o evidencias, por palabras claves, iniciales, tipo de archivos, metadatos, sectores específicos del disco y otras series de opciones, que permiten optimizar al máximo la búsqueda de evidencia.
- Para sacar el reporte dar clic en la opción ASCCI String Report, se genera un archivo con la información del archivo digital y la estructura física del disco óptico. Ver Anexo B(Reporte de análisis forense de disco óptico DVD)

5.2.3 Informe

Se registran cada antecedente o acontecimiento del evento, todo el trabajo realizado, conclusiones e impactos del análisis.

Para el caso de estudio se realizó un informe técnico el cual está estructurado de la siguiente manera:

a. INFORME TÉCNICO. Se detallan los procesos, herramientas software y técnicas utilizadas. Ver Anexo C (INFORME TÉCNICO)

Resultados:

En la tabla 20, tabla 21, tabla 22, tabla 23, tabla 24 se visualizan los resultados luego de los análisis.

Tabla 20

Características físicas

Sistema de archivo	Nombre de Volumen	Aplicación donde se grabó el DVD	Tabla de localización	Bloque del Directorio Raíz	Nombre de Codificación
ISO 9660	ARQQSET_201321	NERO BURNING ROM	22-22	111669149719	UCS-2 LEVEL 3

Tabla 21

Características internas

Tamaño del Sector	Tamaño de Bloque	Rango Total de sectores	Rango Total de bloques	Archivos
2048 Bytes	2048 Bytes	0 -143743	0 -143743	Archivos borrados: color rojo Archivos permanentes: color azul

Tabla 22

Reporte Final CD

Disco óptico	Estado	Velocidad de transferencia	Tamaño del archivo	Tiempo, análisis forense	Error	Observación
CD	Muy bueno	48x lectura	280Mb	00:2:10	Visualiza los archivos modificados	Análisis con CD en muy buen estado, sin ningún contratiempo
CD	Bueno	48x lectura	280Mb	00:5:15	Visualiza los archivos modificados	El tiempo aumenta porque el CD está en un estado bueno, algo deteriorado la capa de protección inferior
CD	Deteriorado	48x lectura	280Mb	∞	Visualiza los archivos modificados	No culmina realizar la copia de bit a bit del CD, por cuanto está deteriorado la capa inferior y la capa de datos. El láser infrarrojo no logra interpretar la información del CD en una cadena de ceros y unos.

Tabla 23

Reporte final DVD

Disco óptico	Estado	Velocidad de transferencia	Tamaño del archivo	Tiempo, análisis forense	Error	Observación
DVD	Muy bueno	16x lectura	280Mb	00:6:20	Da el reporte de los archivos modificados	Análisis con DVD en muy buen estado, sin ningún contratiempo
DVD	Bueno	16x lectura	280Mb	00:8:39:00	NO da el reporte de los archivos modificados	El tiempo aumenta porque el DVD está en un estado bueno, algo deteriorado la capa de protección inferior. Se debe verificar la copia de bita bit activando la técnica MD5
DVD	Deteriorado	16x lectura	280Mb	∞		No culmina realizar la copia de bit a bit , por cuanto está deteriorado la capa inferior y la capa de datos. El láser infrarrojo no logra interpretar la información del DVD en una cadena de ceros y unos.

Tabla 24

Reporte final Blu Ray

Disco óptico	Estado	Velocidad de transferencia	Tamaño del archivo	Tiempo, análisis forense	error	Observación
BLU RAY	Muy bueno	8x lectura	280Mb	00:12:48	Visualiza los archivos modificados	Análisis sin ningún contratiempo
BLU RAY	Bueno	8x lectura	280Mb	00:16:17	Visualiza los archivos modificados	El tiempo aumenta porque el BLU RAY está en un estado bueno, algo deteriorado la capa de protección inferior
BLU RAY	Deteriorado	8x lectura	280Mb	00:19:21	Visualiza los archivos modificados	Realiza la copia de bit a bit para el respectivo análisis forense, ralladuras

CAPÍTULO 4

CONCLUSIONES Y RECOMENDACIONES

7.1 CONCLUSIONES

Según los diferentes criterios de selección de las herramientas descritos en la tabla No. 12 , se concluye que la herramienta CAINE cumple con los requerimientos necesarios para realizar un estudio forense para discos ópticos, facilitando el peritaje de manera completa del dispositivo óptico, cumpliendo las leyes y procedimiento para un óptimo proceso forense, con el objetivo de encontrar información y/o archivos nuevos, borrados, y modificados con especificaciones como fecha y hora, minimizando el tiempo de búsqueda y evitando contaminar la información.

La utilización de una buena guía metodológica incluye las siguientes fases: Preparación de escenario, identificación, recolección y preservación de evidencia e informe final

Una buena preservación de las evidencias permite mantener la información, con el fin de evitar la manipulación accidental e intencional de la misma, aplicando la norma ISO/IEC 27037 (Guía para la identificación, recolección, adquisición y preservación de evidencia digital), que permite construir buenas prácticas forenses.

El tiempo de análisis forense para discos ópticos depende de varios factores: el formato del disco óptico (NORMA ISO 9660), el estado físico, el tamaño de la información contenida y la velocidad de trasferencia de la lectura. El tamaño de la información analizada fue de 280Mb en el cual se demoró 6 m con 20s en ser visualizados los archivos luego del análisis.

A los investigadores forenses les permite detectar, analizar o solucionar anomalías encontradas en los dispositivos ópticos mediante la generación de reportes bien documentados.

De los tres discos ópticos (CD, DVD, BLU RAY) para el respectivo análisis forense sin ningún tipo de contratiempos fue con BLU RAY, debido a que éste disco óptico tiene resistencia a las ralladuras.

7.2 RECOMENDACIONES

Es necesario que los investigadores utilicen óptimos procedimientos para proteger la integridad de datos que se encuentran en los dispositivos ópticos para poder disminuir posibles vulnerabilidades o ataques que puedan ocurrir, con lo que permitirá salvaguardar la información.

La aplicación Caine hace un análisis estricto de las zonas de código de los discos ópticos (formatos), razón por la cual se recomienda adquirir una licencia que permita leer discos ópticos independientemente de la zona.

Llenar los datos en los formularios secuenciales que despliega Caine de acuerdo a lo descrito en capítulo 3, para obtener la imagen digital y la autopsia para obtener el reporte y análisis de la información óptima.

Trabajos citados

Académica México. (30 de Oct de 2014). *La importancia de la cadena de custodia.* Recuperado el 20 de Agos de 2015, de http://www.academica.mx/blogs/la-importancia-la-cadena-custodia

Acurio, S. (8 de Dic de 2009). *Informática Forense en el Ecuador Una mirada introductoria.* Recuperado el 25 de 07 de 2015, de https://docs.google.com/document/d/16Ap5QqNhxe5UxEWZ2wiDRt2qxeGucvmczscGLDNRs6o/edit?hl=es&pli=1

Almeida, O. (25 de May de 2011). *Inserción Jurídica de la Informática Forense.* Recuperado el 04 de Agos de 2015, de http://repositorio.utn.edu.ec/handle/123456789/539

Ardita, J. (11 de Jul de 2007). *Metodología de Análisis Forense Informático.* Recuperado el 13 de Agos de 2015, de http://www.cybsec.com/upload/ADACSI_Ardita_Analisis_Forense_Informatico v2.pdf

Asamblea Constituyente de Ecuador. (20 de Oct de 2008). *Constitución de la República del Ecuador*. Recuperado el 04 de Agos de 2015, de http://www.asambleanacional.gov.ec/documentos/constitucion_de_bolsillo.pdf

Asamblea Nacional del Ecuador. (3 de Feb de 2014). *CÓDIGO ORGÁNICO INTEGRAL PENAL*. Recuperado el 4 de Agos de 2015, de http://www.desarrolloamazonico.gob.ec/wp-content/uploads/downloads/2014/05/CODIGO-ORGANICO-INTEGRAL-PENAL-act.pdf

Cabrera, E. (2013). *Fundamentos de la Informática Forense.* Recuperado el 25 de 07 de 2015, de http://datateca.unad.edu.co/contenidos/233012/unidad_1/u1_introduccion%20a%20la%20informatica%20forense.pdf

CDRoller. (12 de May de 2015). *CDRoller 10.2* . Recuperado el 28 de Jul de 2015, de http://www.cdroller.com/

Cortés, J. (27 de Oct de 2014). *MANEJO DE EVIDENCIA DIGITAL EN DISPOSITIVOS DE ALMACENAMIENTO PENDRIVE USB APLICANDO LA NORMA ISO/IEC 27037:2012.* Recuperado el 6 de Agos de 2015, de http://repository.unad.edu.co/browse?type=author&value=Cort%C3%A9s+De+la+Rosa%2C+Jos%C3%A9+Bernardo

Crowley, P. (12 de Marz de 2010). *CD AND DVD FORENSIC.* Recuperado el 28 de Jul de 2015, de http://www.amazon.com/CD-DVD-Forensics-Paul-Crowley/dp/1597491284

Cuenca, A. (1 de Ene de 2013). *El delito informático en el Ecuador. Una nueva tendencia criminal del siglo XXI. Su evolución, punibilidad y proceso penal* . Recuperado el 12 de Agos de 2015, de http://www.criptored.upm.es/guiateoria/gt_m924a.htm

Derecho Venezolano. (1 de Oct de 2012). *EVIDENCIA FÍSICA*. Recuperado el 20 de Agos de 2015, de http://derechovenezolano.com/2012/10/01/evidencia-fisica/

DocSlide. (3 de Jul de 2015). *Evidencia Digital*. Recuperado el 21 de Agos de 2015, de http://myslide.es/documents/evidencia-digital-5597965f14647.html

DragonJAR. (15 de Sep de 2011). *Análisis Forense de Dispositivos iOS – Fase de Informes*. Recuperado el 27 de Agos de 2015, de http://www.dragonjar.org/analisis-forense-de-dispositivos-ios-fase-de-informes.xhtml

Dueñas, R. (27 de Jul de 2014). *Recolección de evidencia fisica.* Recuperado el 20 de Ago de 2015, de http://es.slideshare.net/rozitaduenasduenas/recoleccion-de-evidencias-fisica

Flu-Project. (29 de Abr de 2015). *Herramientas forense para ser un buen CSI. Parte LV: Línea temporal de PDF*. Recuperado el 21 de Agos de 2015, de http://www.flu-project.com/2015/04/herramientas-forense-para-ser-un-buen.html

García, C. (1 de Feb de 2014). *CADENA DE CUSTODIA DIGITAL DE LAS EVIDENCIAS.* Recuperado el 13 de Agos de 2015, de http://biblioteca.usac.edu.gt/tesis/08/08_0755_CS.pdf

García, I. (01 de 12 de 2009). *Cómo funciona un CD*. Recuperado el 17 de 08 de 2015, de http://museodelaciencia.blogspot.com/2009/12/como-funciona-un-cd.html

Garcia, L. (22 de Mar de 2013). *INFORMÁTICA FORENSE*. Recuperado el 25 de Jul de 2015, de http://es.slideshare.net/leidyjohanagarciaortiz/informatica-forense-17491793

Gervilla, C. (1 de Dic de 2014). *METODOLOGÍA PARA UN ANALISIS FORENSE*. Recuperado el 30 de Jul de 2015, de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/39681/6/cgervillarTFM1214memoria.pdf

González, I. Y. (01 de 03 de 2006). *Las nuevas tecnologías de almacenamiento: CD y DVD*. Recuperado el 31 de 07 de 2015, de http://www.monografias.com/trabajos25/tecnologias-almacenamiento/tecnologias-almacenamiento.shtml#anexos

Guerra, D. (26 de Agos de 2014). *CADENA DE CUSTODIA*. Recuperado el 12 de Agos de 2015, de http://es.slideshare.net/diegoguerra963/cadena-de-custodia-ecuador-38387170

Gutiérrez, F. (22 de 12 de 2014). *Características Blu-Ray*. Recuperado el 17 de 08 de 2015, de http://fernandogi.blogspot.com/

Hernández, R. (01 de 01 de 2013). *Diferencias entre CD,DVD y Blu-RAY*. Recuperado el 28 de 08 de 2015, de http://rodhzuniga.blogspot.com/2013/01/diferencias-entre-cddvd-y-blu-ray.html#

Hoffmeister, G. (21 de 11 de 2012). *Blu Ray- Mecanismos de protección*. Recuperado el 17 de 08 de 2015, de http://omarper.blogspot.com/2014/12/blu-ray-mecanismos-de-proteccion.html

Icaza, E. (01 de Sep de 2010). *Informática Forense como medio de prueba en el Ecuador*. Recuperado el 28 de 07 de 2015, de http://www.monografias.com/trabajos88/informatica-forense-como-medio-prueba/informatica-forense-como-medio-prueba.shtml

ISSA Argentina. (3 de Jul de 2014). *ISO/IEC 27037: ¿Plantea una nueva forma de hacer Análisis Forense?* . Recuperado el 12 de Agos de 2015, de http://www.issaarba.org/node/70

La huella oculta Seguridad y Análisis Forense Informáticos. (24 de Sep de 2014). *Pequeña introducción al análisis forense*. Recuperado el 21 de Agos de 2015, de

https://lahuellaoculta.wordpress.com/2014/09/24/pequena-introduccion-al-analisis-forense/

León, A., Echeverría, T., & Santander, M. (1 de Oct de 2010). *Guía metodológica para la investigación forense en el navegador web Google Chrome.* Recuperado el 25 de Jul de 2015, de http://kosmos.upb.edu.co/web/uploads/articulos/%28A%29_GUIA_METODOLOGICA_PARA_LA_INVESTIGACION_FORENSE_EN_EL_NAVEGADOR_WEB_GOOGLE_CHROME_gm810g.pdf

Martín, V. (4 de Ene de 2012). *Detecta cualquier problema en la unidad grabadora de CDs/DVDs.* Recuperado el 28 de Jul de 2015, de http://vso-inspector.malavida.com/

Miguez, G. (2015). SCOPOMETRÍA PARA LA AUTENTICIDAD DE SOPORTES OPTICOS DE INFORMACION. *Revista Digital de Criminología y Seguridad* , 11-12.

Mujica, M. (7 de Oct de 2011). *Informatica forense.* Recuperado el 25 de Jul de 2015, de http://es.slideshare.net/mmujica/informatica-forense-9598622

Peñaherrera, J., & Duque, K. (1 de Nov de 2011). *Estudio y análisis deevidencia digital en telefonos celulares con tecnología GSM para procesos judiciales.* Recuperado el 25 de Jul de 2015, de bibdigital.epn.edu.ec/bitstream/15000/4401/1/CD-3997.pdf

Pino, S. (08 de 12 de 2009). *Informática Forense en el Ecuador Una mirada introductoria.* Recuperado el 13 de 08 de 2015, de http://www.egov.ufsc.br/portal/sites/default/files/informatica_forense_en_el_ecuador.pdf

Pinto, D. (21 de Sep de 2014). *Metodología de análisis forense orientada a incidentes en dispositivos móviles*. Recuperado el 27 de Agos de 2015, de http://dspace.ucuenca.edu.ec/bitstream/123456789/21381/1/TIC.EC_04_Pinto.pdf

Pleno del Congreso Nacional del Ecuado. (2002). *LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRONICAS Y MENSAJES DE DATOS*.

Recuperado el 5 de Agos de 2015, de http://www.oas.org/juridico/spanish/cyb_ecu_ley_comelectronico.pdf

POLICIA NACIONAL DE NICARAGUA. (1 de Dic de 2012). *Manual de tratamiento de la evidencia y cadena de custodia.* Recuperado el 20 de Agos de 2015, de http://www.poderjudicial.gob.ni/comipe2013/pdf/MANUAL_EVIDENCIA_final.pdf

Presman, G. (1 de Junio de 2014). *ISO/IEC 27037 NORMALIZANDO LA PRACTICAFORENSE INFORMATICA* . Recuperado el 12 de Agos de 2015, de http://www.copitec.org.ar/comunicados/CAIF2014/CAIF-Presman.pdf

Prezi. (14 de Agos de 2013). *Análisis Forense.* Recuperado el 21 de Agos de 2015, de https://prezi.com/igyy62rfe-9s/analisis-forense/#

Roatta, S., Casco, M., & Fogliato, G. (17 de Jun de 2015). *El tratamiento de la evidencia digital y las normas ISO/IEC 27037:2012.* Recuperado el Jul de 2015, de http://sedici.unlp.edu.ar/bitstream/handle/10915/46243/Documento_completo.pdf?sequence=1

Saal, A. (01 de 01 de 2010). *Discos ópticos y sus unidades*. Recuperado el 01 de 08 de 2015, de http://www.monografias.com/trabajos7/diop/diop.shtml

Seguridad de la Información en Colombia. (30 de May de 2010). *Análisis de Impacto de Negocios / Business Impact Analysis (BIA)* . Recuperado el 27 de Agos de 2015, de http://seguridadinformacioncolombia.blogspot.com/2010/05/analisis-de-impacto-de-negocios.html

Smith, J. (01 de 01 de 2010). *Almacenamiento: Discos Ópticos*. Recuperado el 13 de 08 de 2015, de http://www.jegsworks.com/Lessons-sp/lesson6/lesson6-9.htm

SOFTPEDIA. (21 de Abr de 2015). *CD / DVD Diagnostic*. Recuperado el 28 de Jul de 2015, de http://www.softpedia.com/get/CD-DVD-Tools/CD-DVD-Rip-Other-Tools/CD-DVD-Diagnostic.shtml&prev=search

Sullivan, B. (1 de Jun de 2014). *Tendencias de Seguridad Cibernética en América Latina y el Caribe.* Recuperado el 25 de Jul de 2015, de http://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

Téllez, Y. (03 de 06 de 2010). *Las nuevas tecnologías de almacenamiento: CD y DVD*. Recuperado el 14 de 08 de 2015, de http://www.monografias.com/trabajos25/tecnologias-almacenamiento/tecnologias-almacenamiento.shtml#Comentarios

Ttito, P. (03 de 06 de 2010). *Disco Blu-ray*. Recuperado el 13 de 08 de 2015, de http://www.monografias.com/trabajos74/disco-blu-ray/disco-blu-ray2.shtml

Tufiño, O. (2012). *DIEÑO Y CONSTRUCCIÓN DE UN SISTEMA DE AUTOMATIZACIÓN HIDRAÚLICA PARA LA MAQUINA DE ENSAYOS DESTRUCTIVOS EN EL LABORATORIO DE SOLDADURA DE LA ESCUELA POLITECNICA NACIONAL*. Quito: ESCUELA POLITECNICA NACIONAL.

Untiveros, M. (4 de Ago de 2011). *Instalacion de CAINE Live CD.* Recuperado el 28 de 07 de 2015, de http://es.slideshare.net/miriam1785/caine-8768460

Whos. (21 de Jun de 2014). *Estándares de manipulación de pruebas digitales: ISO/IEC 27037:2012*. Recuperado el 12 de Agos de 2015, de http://wh0s.org/2014/06/21/estandares-de-manipulacion-de-pruebas-digitales-isoiec-270372012/

ANEXOS

ANEXO A: Descripción de Hardware y Software

HARDWARE				
Subtipo Activo	**Descripción**	**Marca**	**MODELO**	**COLOR**
CPU	Estación trabajo Intel Core 2 Quad 2,83 GHz 4GB RAM 330 GB HDD DVD-RW	FUJITSU SIEMENS	YK7T034123	Plomo
MONITOR	LCD TFT 19 Pulgadas	FUJITSU SIEMENS		Blanco

Disco óptico	**Tipo**	**Velocidad de Transferencia**	**Capacidad**	**Etiqueta**	**Archivos**
DVD	DVD-R	16 X	4,7 GB	2HR	• Cumpleaños Fecha: 26/01/2015, Tipo: Adobe Illustrator, Tamaño: 4.489KB • La mejor música electrónica 2014-2015 Fecha: 21/02/2015, Tipo: MP4 File, Tamaño: 278.980 KB

SOFTWARE					
NOMBRE	**SISTEMA OPERATIVO**	**VERSIÓN**	**INTERFAZ**	**FUNCIÓN**	**NOMBRE**
DVD	DVD-R	16 X	4,7 GB	2HR	• Cumpleaños Fecha: 26/01/2015, Tipo: Adobe Illustrator, Tamaño: 4.489KB • La mejor música electrónica 2014-2015 Fecha: 21/02/2015, Tipo: MP4 File, Tamaño: 278.980 KB

ANEXO B: Reporte de análisis forense de disco óptico DVD

```
                    Autopsy string Report

------------------------------------------------------------------
                     GENERAL INFORMATION

File: /1/cumpleaños.ai
MD5 of file: 460e57b89d505122a41df3117577a9f4  -
SHA-1 of file: 1aed58c635044a6bd0e920bd40964d7d336a5185  -
MD5 of ASCII strings: 71bbead026268aa62682d87e1e593639  -
SHA-1 of ASCII strings: 35a0254765c07bf3dacb5653b4bfda85c3c32991  -

Image:
'/usr/share/caine/report/autopsy/forensedvd/host1/images/copia1.dd'
Offset: Full image
File System Type: iso9660

Date Generated: Tue Sep 15 00:43:37 2015
Investigator: GabyPenaherrera

------------------------------------------------------------------
                     META DATA INFORMATION

Entry: 2
Type: File
Links: 1
Flags:
Name: cumpleaños.ai
Size: 4595819
Owner-ID: 0
Group-ID: 0
Mode: -r-xr-xr-x

File Times:
Created:   2015-01-26 14:00:51 (CET)
File Modified:   0000-00-00 00:00:00 (UTC)
Accessed:  0000-00-00 00:00:00 (UTC)

Sectors:
29 30 31 32 33 34 35 36
37 38 39 40 41 42 43 44
45 46 47 48 49 50 51 52
53 54 55 56 57 58 59 60
61 62 63 64 65 66 67 68
69 70 71 72 73 74 75 76
77 78 79 80 81 82 83 84
85 86 87 88 89 90 91 92
93 94 95 96 97 98 99 100
101 102 103 104 105 106 107 108
109 110 111 112 113 114 115 116
117 118 119 120 121 122 123 124
125 126 127 128 129 130 131 132
```

133 134 135 136 137 138 139 140
141 142 143 144 145 146 147 148
149 150 151 152 153 154 155 156
157 158 159 160 161 162 163 164
165 166 167 168 169 170 171 172
173 174 175 176 177 178 179 180
181 182 183 184 185 186 187 188
189 190 191 192 193 194 195 196
197 198 199 200 201 202 203 204
205 206 207 208 209 210 211 212
213 214 215 216 217 218 219 220
221 222 223 224 225 226 227 228
229 230 231 232 233 234 235 236
237 238 239 240 241 242 243 244
245 246 247 248 249 250 251 252
253 254 255 256 257 258 259 260
261 262 263 264 265 266 267 268
269 270 271 272 273 274 275 276
277 278 279 280 281 282 283 284
285 286 287 288 289 290 291 292
293 294 295 296 297 298 299 300
301 302 303 304 305 306 307 308
309 310 311 312 313 314 315 316
317 318 319 320 321 322 323 324
325 326 327 328 329 330 331 332
333 334 335 336 337 338 339 340

```
               </rdf:li>
            </rdf:Alt>
         </xmp:Thumbnails>
      </rdf:Description>
      <rdf:Description rdf:about=""
            xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/"

xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#"

xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#">
         <xmpMM:InstanceID>uuid:fb04fd7c-fbc6-4010-94c1-
da52364d7972</xmpMM:InstanceID>

<xmpMM:DocumentID>xmp.did:EEAB2C7180A5E4119895EB84CAD1D206</xmpMM:D
ocumentID>

<xmpMM:OriginalDocumentID>uuid:5D20892493BFDB11914A8590D31508C8</xm
pMM:OriginalDocumentID>
         <xmpMM:RenditionClass>proof:pdf</xmpMM:RenditionClass>
         <xmpMM:DerivedFrom rdf:parseType="Resource">
            <stRef:instanceID>uuid:ce3fe817-8f0b-4f32-888f-
b52d8be79251</stRef:instanceID>

<stRef:documentID>xmp.did:B72F3FEA81A2E411A187A88EB423DBE3</stRef:d
ocumentID>
```

```
<stRef:originalDocumentID>uuid:5D20892493BFDB11914A8590D31508C8</st
Ref:originalDocumentID>
            <stRef:renditionClass>proof:pdf</stRef:renditionClass>
         </xmpMM:DerivedFrom>
         <xmpMM:History>
            <rdf:Seq>
               <rdf:li rdf:parseType="Resource">
                  <stEvt:action>saved</stEvt:action>

<stEvt:instanceID>xmp.iid:5F83A7EF5EA2E4119A75D90FB2464FFD</stEvt:i
nstanceID>
                  <stEvt:when>2015-01-22T12:48:55-
05:00</stEvt:when>
                  <stEvt:softwareAgent>Adobe Illustrator CS6
(Windows)</stEvt:softwareAgent>
                  <stEvt:changed>/</stEvt:changed>
               </rdf:li>
               <rdf:li rdf:parseType="Resource">
                  <stEvt:action>saved</stEvt:action>

<stEvt:instanceID>xmp.iid:B72F3FEA81A2E411A187A88EB423DBE3</stEvt:i
nstanceID>
                  <stEvt:when>2015-01-22T16:59:19-
05:00</stEvt:when>
                  <stEvt:softwareAgent>Adobe Illustrator
CS5</stEvt:softwareAgent>
                  <stEvt:changed>/</stEvt:changed>
               </rdf:li>
               <rdf:li rdf:parseType="Resource">
                  <stEvt:action>saved</stEvt:action>

<stEvt:instanceID>xmp.iid:EEAB2C7180A5E4119895EB84CAD1D206</stEvt:i
nstanceID>
                  <stEvt:when>2015-01-26T12:26:20-
05:00</stEvt:when>
                  <stEvt:softwareAgent>Adobe Illustrator
CS5</stEvt:softwareAgent>
                  <stEvt:changed>/</stEvt:changed>
               </rdf:li>
            </rdf:Seq>
         </xmpMM:History>
      </rdf:Description>
      <rdf:Description rdf:about=""

xmlns:illustrator="http://ns.adobe.com/illustrator/1.0/">
         <illustrator:Type>Document</illustrator:Type>

<illustrator:StartupProfile>Print</illustrator:StartupProfile>
      </rdf:Description>
      <rdf:Description rdf:about=""
            xmlns:xmpTPg="http://ns.adobe.com/xap/1.0/t/pg/"
```

```
xmlns:stDim="http://ns.adobe.com/xap/1.0/sType/Dimensions#"
            xmlns:stFnt="http://ns.adobe.com/xap/1.0/sType/Font#"
            xmlns:xmpG="http://ns.adobe.com/xap/1.0/g/">

<xmpTPg:HasVisibleOverprint>False</xmpTPg:HasVisibleOverprint>

<xmpTPg:HasVisibleTransparency>True</xmpTPg:HasVisibleTransparency>
         <xmpTPg:NPages>1</xmpTPg:NPages>
         <xmpTPg:MaxPageSize rdf:parseType="Resource">
            <stDim:w>18.000142</stDim:w>
            <stDim:h>15.000118</stDim:h>
            <stDim:unit>Centimeters</stDim:unit>
         </xmpTPg:MaxPageSize>
         <xmpTPg:Fonts>
            <rdf:Bag>
               <rdf:li rdf:parseType="Resource">
                  <stFnt:fontName>CenturyGothic-
Bold</stFnt:fontName>
                  <stFnt:fontFamily>Century
Gothic</stFnt:fontFamily>
                  <stFnt:fontFace>Bold</stFnt:fontFace>
                  <stFnt:fontType>Open Type</stFnt:fontType>
                  <stFnt:versionString>Version
2.35</stFnt:versionString>
                  <stFnt:composite>False</stFnt:composite>

<stFnt:fontFileName>GOTHICB.TTF</stFnt:fontFileName>
               </rdf:li>
               <rdf:li rdf:parseType="Resource">
                  <stFnt:fontName>MyriadPro-Bold</stFnt:fontName>
                  <stFnt:fontFamily>Myriad Pro</stFnt:fontFamily>
                  <stFnt:fontFace>Bold</stFnt:fontFace>
                  <stFnt:fontType>Open Type</stFnt:fontType>
                  <stFnt:versionString>Version 2.062;PS
2.000;hotconv 1.0.57;makeotf.lib2.0.21895</stFnt:versionString>
0002682764 00000 n
0002682908 00000 n
0002682987 00000 n
0002683572 00000 n
0002683729 00000 n
0002683753 00000 n
0002684056 00000 n
0002684200 00000 n
0002684279 00000 n
0002684862 00000 n
0002685019 00000 n
0002685043 00000 n
0002685344 00000 n
0002685488 00000 n
0002685567 00000 n
0002686146 00000 n
0002686303 00000 n
```

0002686327 00000 n
0002686630 00000 n
0002686774 00000 n
0002686853 00000 n
0002687433 00000 n
0002687590 00000 n
0002687614 00000 n
0002687917 00000 n
0002688061 00000 n
0002688140 00000 n
0002688725 00000 n
0002688882 00000 n
0002688906 00000 n
0002689209 00000 n
0002689353 00000 n
0002689432 00000 n
0002690010 00000 n
0002690167 00000 n
0002690191 00000 n
0002690493 00000 n
0002690637 00000 n
0002690716 00000 n
0002691298 00000 n
0002691455 00000 n
0002691479 00000 n
0002691781 00000 n
0002691925 00000 n
0002692004 00000 n
0002692590 00000 n
0002692747 00000 n
0002692771 00000 n
0002693074 00000 n
0002693218 00000 n
0002693297 00000 n
0002693878 00000 n
0002694035 00000 n
0002694059 00000 n
0002694362 00000 n
0002694506 00000 n
0002694585 00000 n
0002695166 00000 n
0002695323 00000 n
0002695347 00000 n
0002695650 00000 n
0002695794 00000 n
0002695873 00000 n
0002696456 00000 n
0002696613 00000 n
0002696637 00000 n
0002696940 00000 n
0002697084 00000 n
0002697163 00000 n
0002697743 00000 n

0002697900 00000 n
0002697924 00000 n
0002698227 00000 n
0002698371 00000 n
0002698450 00000 n
0002699033 00000 n
0002699190 00000 n
0002699214 00000 n
0002699517 00000 n
0002699661 00000 n
0002699740 00000 n
0002700325 00000 n
0002700470 00000 n
0002700494 00000 n
0002700838 00000 n
0002700917 00000 n
0002703553 00000 n
0002703698 00000 n
0002703722 00000 n
0002704065 00000 n
0002704144 00000 n
0002705929 00000 n
0002706074 00000 n
0002706098 00000 n
0002706441 00000 n
0002706520 00000 n
0002708693 00000 n
0002708838 00000 n
0002708862 00000 n
0002709203 00000 n
0002709282 00000 n
0002711365 00000 n
0002711510 00000 n
0002711534 00000 n
0002711876 00000 n
0002711955 00000 n
0002712908 00000 n
0002713062 00000 n
0002713913 00000 n
0002714973 00000 n
0002723145 00000 n
0002788736 00000 n
0002854327 00000 n
0002919918 00000 n
0002985509 00000 n
0003051100 00000 n
0003116691 00000 n
0003182282 00000 n
0003247873 00000 n
0003313464 00000 n
0003379055 00000 n
0003444646 00000 n
0003510237 00000 n

```
0003575828 00000 n
0003641419 00000 n
0003707010 00000 n
0003772601 00000 n
0003838192 00000 n
0003903783 00000 n
0003969374 00000 n
0004034965 00000 n
0004092043 00000 n
0004157634 00000 n
0004223225 00000 n
0004288816 00000 n
0004354407 00000 n
0004419998 00000 n
0004485589 00000 n
0004551438 00000 n
trailer
<</Size 2202/Root 1 0 R/Info 2201 0
R/ID[<88B99EB2289B8E4E8F1B9E691F5DE352><77C6A445CA92B24AB320AE8E652
4A750>]>>
startxref
4551615
%%EOF

-------------------------------------------------------------------
---
                  VERSION INFORMATION

Autopsy Version: 2.24
The Sleuth Kit Version: 4.0.2
```