UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO

UNIDAD ACADÉMICA PROFESIONAL TIANGUISTENCO

“GENERACIÓN DE UN MANUAL BASADO EN CÓMPUTO FORENSE QUE SIRVA COMO SOPORTE EN EL PROCESO DE RECUPERACIÓN DE INFORMACIÓN EN DISCOS DUROS”

TESINA

PARA OBTENER EL TÍTULO DE

INGENIERO EN SOFTWARE

Q U E P R E S E N T A

CRISTIAN GIOVANNI PICHARDO SÁNCHEZ

ASESOR:

L. CID MARTIN GARCIA AVILA

TIANGUISTENCO, MÉX. OCTUBRE, 2017

Pensamiento…

La mente que se abre a una nueva idea nunca vuelve a su tamaño original.

Resumen

En el presente trabajo se detalla la generación de un manual basado en cómputo forense que sirva como soporte en el proceso de recuperación de información en discos duros, está dirigido para usuarios con conocimientos básicos de informática que en algún momento lleguen a perder información de sus discos duros y requieran recuperar dicha información o la gran mayoría de ella. En este trabajo se menciona el análisis, diseño e implementación del manual, así como los resultados obtenidos al aplicarlo; actualmente existen manuales orientados a recuperar información, sin embargo, la mayoría de estos están orientados a usuarios con amplios conocimientos en cuanto a computadoras e informática y se orientan por recuperar únicamente información eliminada, sin embargo, la perdida de información abarca más allá de la simple eliminación de información. Por otra parte, se involucra y se le saca provecho a todas las bondades que ofrece el cómputo forense siendo una ciencia con un alto potencial y efectividad en cuanto a resultados por obtener.

Contenido

Índice de Figuras

Índice de Tablas

CAPÍTULO I
INTRODUCCIÓN

A mediados del 2016 las computadoras están por todas partes, son utilizadas en hogares, escuelas y empresas.

La gente utiliza las computadoras para muchos propósitos diferentes, por ejemplo, para escribir cartas, analizar información y navegar por internet, son muy importantes y poco a poco se han convertido en una necesidad para las personas, empresas y sociedad en general. Las computadoras ofrecen maneras de organizar, investigar, procesar y almacenar información.

El disco duro es el principal dispositivo de almacenamiento de las computadoras, la bondad más grande que ofrece un disco duro es su capacidad de almacenamiento, se puede contener grandes volúmenes de información con diferente grado de importancia para cada usuario, desafortunadamente, también el disco duro es el dispositivo de almacenamiento que mayor pérdida de información tiene, originado por diversos factores. En este capítulo se explica cómo se originó el problema y como solucionarlo de una manera eficiente, con el empleo de cómputo forense.

1.1. Antecedentes

En la actualidad las computadoras son herramientas indispensables para la realización de tareas y trabajos (Santana Tiznado, 2001), Guillermo García Lambert en su investigación realizada en el año 2014 que lleva por nombre "Reglas que describen la deserción y permanencia en los estudiantes de la UAP Tianguistenco de la UAEM" recalca una regla muy importante encontrada, la cual señala que los alumnos que no tienen computadora o que se limita a una computadora en casa, tienen más riesgo de ser dados de baja debido a la gran importancia que tienen las computadoras para realizar tareas hoy en día. (García Lambert, García Hernández , & Ledeneva, 2014).

La computadora se generaliza en hardware y software, (Norton, 2006) dentro del hardware el almacenamiento es de los elementos más importantes de una computadora (Santana Tiznado, 2001). El disco duro es el principal dispositivo de almacenamiento de información, es un dispositivo magnético y mecánico, con partes móviles, siendo por tanto más delicado que otros sistemas de almacenamiento (Herrerías Rey, 2006).

La información es aquello que tiene un significado para nosotros, esta se representa en los sistemas de información utilizando el sistema de numeración binario, que está compuesto únicamente de ceros y unos. Uno de los factores clave en el mantenimiento de la seguridad de información es la selección de medidas de seguridad. Si no existen medidas de seguridad, la información es vulnerable a amenazas, la mayor de ellas es la pérdida de información (Aceituno Canal, 2007).

En la figura 1 se muestra un ejemplo de la cantidad de información y los tipos de esta que puede contener un disco duro según su capacidad, tomando en consideración que solamente es un tipo de información a la vez dentro del disco duro. Los datos fueron tomados de la página oficial SEAGATE.com

Tipos de archivos/ Capacidad	Música digital MP3	Fotografías digitales	Video digital	Películas con calidad DVD
500 GB	8.330 horas	160.000	500 horas	125
1 TB	16.660 horas	320.000	1,000 horas	250
1.5 TB	24.990 horas	480.000	1,500 horas	375
2 TB	33.320 horas	640.000	2,000 horas	500

Tabla 1. Tabla de capacidades de discos duros.

Fuente: SEAGATE.com

Se pueden contener diferentes tipos de información, existiendo siempre alguno más importante que otro. Si esta información se llega a perder por alguna razón, esta acción representa una gran amenaza en caso de no contar con respaldos ya que implica volver a recolectar o capturar la información perdida demandando recursos, tiempo y costo, por lo que lo más conveniente sería poder recuperar la información.

La recuperación de información concierne a la representación, almacenamiento, búsqueda y hallazgo de información relevante para un usuario humano (Igwersen, 1992) & (Baeza Yates & Ribeiro Neto, 1999). Ante la gran cantidad de información que se maneja actualmente por medios electrónicos, y el valor tan alto que tiene esta para las personas y organizaciones, es que el cómputo forense está siendo considerado como una herramienta muy valiosa ante la necesidad de contar con algún método que facilite la obtención de pruebas digitales en los casos donde se cometen fraudes o crímenes que atenten contra los usuarios de la información, el cómputo forense aprovecha su enfoque científico, empleando una serie de fenómenos electromagnéticos con la idea de recuperar, recolectar, analizar, verificar y validar todo tipo de información, ya sea existente, o considerada como borrada o perdida de la computadora para beneficio de quienes han sufrido ataques mal intencionados o accidentales a sus sistemas informáticos y bases de datos. Bajo ese concepto, se puede considerar al cómputo forense como una herramienta muy importante dentro de una auditoria informática, ya que sirve, como un mecanismo para obtener pruebas contundentes que pueden ser consideradas como evidencia legal en algún delito que se persiga en instancias

mayores como los juicios penales. Los datos destruidos y manipulados también pueden rastrearse y recuperarse (Arias Chavez , 2007).

En los últimos años han aparecido multitud de empresas que ofrecen herramientas comerciales de análisis forense. El auge del cómputo forense ha hecho que se incremente la cantidad de gente interesada en el tema, y muchas de ellas han creado herramientas *open source* de potencial muy elevado y que son accesibles para cualquier persona (Fernández Bleda, 2004). En las próximas décadas, e incluso hoy en día, el área del cómputo forense ha tenido una gran expansión. Las empresas privadas han seguido la estrategia de empleo directo a profesionales de seguridad informática forense o computadora, o bien recurrir a otras empresas especializadas basadas en las necesidades existentes (Salmerón, 2015).

1.2. Planteamiento del problema

Los discos duros pueden contener información, tal como: documentos escolares (tareas, investigaciones, proyectos finales, artículos, presentaciones electrónicas, tesis). En el aspecto laboral (contratos, facturas electrónicas, inventarios, formatos oficiales, constancias de trabajo, cartas de recomendación, datos de trabajadores, datos de productos, bases de datos). Además, se puede encontrar información personal como: fotos familiares, fotos personales o de viajes, videos, canciones, conversaciones, y tipos de archivos e información que posiblemente ha sido recolectada a través de varios años y que resulta muy valiosa para cada persona.

Hasta mediados de 2016 el usuario se enfrenta con una situación desagradable y común al momento de trabajar con los discos duros, es la pérdida de información, misma que puede darse por diversos factores entre los más comunes se encuentra la eliminación accidental (dentro de la eliminación accidental el borrado de carpetas que no se sabía su contenido, que la persona sea inexperta en el manejo de las computadoras), eliminación intencional (esto implica que la persona que elimina tenga el conocimiento de lo que está haciendo), daños por algún funcionamiento anormal del dispositivo (instalación de software erróneo), virus y

errores del sistema (daños a la información por infección de diferentes programas malignos, eliminación provocada por la infección, actualizaciones del sistema), daños físicos (algún golpe o caída del disco duro), situaciones climáticas(inundaciones), daños eléctricos (descarga eléctrica).

Existen técnicas y herramientas de cómputo forense que pueden ayudar en la recuperación; sin embargo, debido a la inexperiencia en el manejo de estas, el no aplicar la metodología de manera adecuada, y no seguir los pasos que implica el cómputo forense, propicia que se pueda dañar aún más la información en proceso de recuperación, teniendo una menor probabilidad de recuperación, ya que la aplicación correcta del cómputo forense hace más probable el éxito en la recuperación de información.

Hasta mediados de 2016, la poca práctica y el nulo uso del cómputo forense aplicado en la recuperación de información en discos duros propicia que:

- No existan estadísticas de comparación de herramientas de cómputo forense para la recuperación de información en discos duros.
- No haya instrumentos basados en cómputo forense para facilitar el proceso de recuperación de información con técnicas y herramientas que ya estén probadas.
- Se invierta tiempo en procedimientos poco efectivos para recuperar la información de manera efectiva.
- Se deba capturar nuevamente la información perdida, que involucra demanda de recursos, tiempo y costo.
- El intentar recuperar información de manera normal sea muy riesgoso ya que durante todo el proceso se trabaja directamente con el dispositivo que contenía la información y se puede llegar a dañar el dispositivo o la información.
- Se pierda por completo la información.
- Se pierdan clientes.
- El último recurso es mandar a un laboratorio especializado el disco duro, a un costo muy alto.

Los problemas mencionados suceden habitualmente; sin embargo, se debe tener mucho cuidado ya que el valor de la información depende de cada usuario.

Lo antes mencionado origina la necesidad de contar con un instrumento a utilizar basado en cómputo forense que acompañe al usuario no experto en informática y cómputo forense para recuperar información en discos duros.

1.3. Justificación

En el presente trabajo se emplearán los conocimientos adquiridos para solucionar problemas referentes a la pérdida de información en discos duros que hoy en día es muy común. El cómputo forense se considera muy importante en esta tarea ya que permite trabajar con el dispositivo de almacenamiento en el que se encontraba la información y analizarlo sin la necesidad de interactuar todo el tiempo con él, ya que el trabajar directamente con el dispositivo a analizar es muy riesgoso, el cómputo forense permite trabajar con imágenes forenses que son copias exactas del dispositivo a analizar, con el fin de no exponer el dispositivo a sufrir más daños. El trabajar con la metodología propuesta garantiza que se cubrirán los procesos que implica el cómputo forense, de tal manera que al cumplirse cada uno de ellos, como resultado se obtendrá una buena solución. El probar y comparar diferentes técnicas y herramientas para la recuperación de información en discos duros basadas en cómputo forense y el desarrollar un manual, ayudará, en general, a todas las personas que sufran alguna perdida de información y que sea necesario recuperar de manera eficiente y completa sin dañarla aún más, ni alterarla o modificarla, manteniendo siempre la integridad de la misma (para utilizarla si es requerida como prueba contundente ante una corte o juicio penal), además de obtener una mayor probabilidad de éxito en dicha tarea ya que se espera que al aplicar cómputo forense se puedan romper barreras de permisos especiales que con la recuperación normal no es posible. El manual está dirigido tanto a usuarios con experiencia como a los que no la tengan, el único requisito es que el usuario posea conocimientos en el manejo de la computadora.

1.4. Objetivo general

Generar un manual basado en cómputo forense que sirva como soporte en el proceso para recuperar información en discos duros.

1.5. Objetivos específicos

- Identificar los problemas relacionados con la perdida de información en discos duros.
- Comparar herramientas de cómputo forense para la recuperación de información en discos duros.
- Crear un manual basado en cómputo forense que ayude con los pasos que se deben seguir durante el proceso de recuperación de información en discos duros.
- Utilizar el manual en casos en los que se necesite recuperar información en discos duros.

1.6. Metodología

En este trabajo se utiliza la metodología en cascada que consta de cinco etapas: análisis, diseño, implementación, pruebas, mantenimiento.

Análisis: En esta etapa se comparan las herramientas de cómputo forense para seleccionar la mejor y se determinan los requerimientos para la generación del manual basado en cómputo forense para la recuperación de información en discos duros.

Diseño: Etapa en la que se realizará la descripción de las partes que contendrá el manual.

Implementación: Etapa en la que se aplicaran los pasos establecidos en el manual.

Pruebas: Etapa en la que se medirá la efectividad del manual.

Mantenimiento: etapa en la que se propondrán acciones para mejorar el contenido de los pasos del manual para incrementar la efectividad en el proceso.

CAPÍTULO II
MARCO TEÓRICO

En la presente investigación se emplearon algunos conceptos que no son de conocimiento público, algunos de ellos son: disco duro, partes físicas del disco duro, partes lógicas del disco duro, seguridad de la información, amenazas y vulnerabilidades, perdida de información, recuperación de información, cómputo forense, etcétera. En este capítulo se presentan conceptos utilizados en el presente trabajo, así mismo se explica su objetivo e importancia, ya que son fundamentales para entender el objetivo del trabajo desarrollado.

2.1. Computadora

Norton Define la computadora como un dispositivo que procesa datos y los convierte en información útil para las personas. Cualquier computadora se controla con instrucciones programadas, las cuales le dan a la maquina un propósito y le dicen lo que debe hacer, las computadoras más utilizadas son las computadoras personales (Norton, 2006). Por su parte Diego Pérez Villa menciona que las computadoras están diseñadas para ser utilizadas por una persona a la vez (Pérez Villa, 2008). Antonio Santana Tiznado menciona que las computadoras más usadas son las de escritorio y las portátiles, estas últimas pueden llevarse de un lugar a otro además de contar con las mismas características que una computadora de escritorio, pero no requieren energía de manera permanente.

En un término general las computadoras son herramientas muy importantes que ayudan a realizar tareas cotidianas de una manera rápida y eficaz, ya que procesan datos y los convierten en información útil para usar en el momento que sea requerida (Santana Tiznado, 2001).

2.1.1. Partes de un sistema de cómputo

Según Norton las computadoras son fabricadas en muchas variedades, desde las pequeñas computadoras que están integradas en los aparatos domésticos hasta las grandes súper computadoras que han ayudado a los científicos a trazar el genoma humano. Cada computadora es parte de un sistema (Norton, 2006). Un sistema de cómputo completo consiste en cuatro partes:

- Hardware.
- Software.
- Datos (información).
- Usuarios.

Según Josefina Pérez Martínez, el hardware se refiere a todos los elementos físicos de la computadora (Pérez Martínez, 2012), Norton concuerda con ello, ya que define que hardware es cualquier parte de la computadora que se puede tocar, consiste en dispositivos electrónicos interconectados que puede utilizar para

controlar la operación, además de los datos de entrada y salida de una computadora (Norton, 2006).

Josefina Pérez Martínez menciona que el software se refiere a los elementos lógicos de la computadora (Pérez Martínez, 2012), por otra parte Norton dice que el software es un conjunto de instrucciones que hace que la computadora realice tareas. En otras palabras, el software le dice a la computadora lo que debe hacer (Norton, 2006).

Según Norton los datos consisten en hechos o piezas individuales de información que por sí mismos no tienen mucho sentido para las personas. El trabajo principal de una computadora es el de procesar estas pequeñas piezas de datos de distintas maneras convirtiéndolas en información útil. Información y los conceptos referentes a información se describen de la página 32 a la 40.
Mismo autor define a los usuarios como las personas que operan a las computadoras (Norton, 2006) .

Por lo antes mencionado se puede decir que un sistema de cómputo completo es el trabajo conjunto entre hardware, software, datos y usuario, si alguno llegase a faltar no se podría trabajar, ya que todos se complementan entre sí.

2.1.2. Dispositivos de almacenamiento

Norton menciona que una computadora puede funcionar utilizando únicamente la capacidad de procesamiento, memoria, dispositivos de entrada y de salida. Sin embargo, para ser realmente útil, una computadora también requiere de un lugar en el cual pueda colocar los archivos de programa y los datos relacionados cuando estos no están en uso. De tal manera explica que el propósito del almacenamiento es guardar datos permanentemente, incluso cuando la computadora está apagada. Menciona que existen dos tipos principales de dispositivos de almacenamiento: el magnético y el óptico (Norton, 2006).

2.1.2.1. Almacenamiento magnético

Norton explica que existen muchos tipos de almacenamiento de computadoras, pero el más común es el disco magnético. Un disco es un objeto redondo y plano que gira alrededor de su centro. (Los discos magnéticos casi siempre están alojados dentro de una cubierta de algún tipo, de manera que no puede ver al disco a menos que abra la cubierta). Las cabezas de lectura escritura/escritura funcionan de forma muy parecida a las cabezas de una grabadora de cintas o videocasetera, se utilizan para leer datos desde el disco o escribir datos en él.

El dispositivo que aloja un disco se conoce como unidad de disco o drive. Algunos discos están integrados en la unidad y no pueden ser removidos; otros tipos de unidades le permiten quitar y remplazar discos. La mayoría de las computadoras personales cuentan con al menos un disco duro no removible (o disco fijo). Además, también existe una unidad de discos flexibles, la cual le permite utilizar disquetes removibles (o discos flexibles).

El disco duro funciona como el archivero principal de la computadora debido a que puede almacenar muchos más datos de los que puede contener un disquete; estos se utilizan para cargar datos en el disco duro, intercambiar datos con otros usuarios y hacer copias de respaldo de los datos que están en el disco duro (Norton, 2006).

2.1.2.2. Almacenamiento óptico

Además del almacenamiento magnético, Norton recalca que casi todas las computadoras que se venden actualmente incluyen al menos una forma de almacenamiento óptico, los cuales son dispositivos que utilizan rayos laser para leer datos desde la superficie reflectora de un disco óptico o para escribir datos sobre ella.

La unidad de CD-ROM es el tipo más común de dispositivo de almacenamiento óptico, los discos compactos (CD) son un tipo de dispositivo de almacenamiento óptico, idéntico a los CD de audio.

En términos generales se puede decir que un dispositivo de almacenamiento se refiere a una unidad que es capaz de guardar datos aun cuando no esté en uso (Norton, 2006).

2.1.2.3. Almacenamiento de estado solido

Herrerías Rey menciona que existe otro tipo de almacenamiento el cual es el almacenamiento de estado sólido que es un método de almacenamiento de datos creado mediante dispositivos de circuitos integrados para almacenar datos en lugar de utilizar soportes ópticos o magnéticos móviles. (Herrerías Rey, 2006), por su parte la empresa SEAGATE por medio de un artículo comparte que el almacenamiento de estado sólido utiliza tecnología de memoria flash no volátil, entre las ventajas destacan el rápido acceso a datos de manera aleatoria, bajo consumo de energía, pequeño tamaño y alta resistencia física, sin embargo la mayor desventaja ante otras unidades de almacenamiento es su precio, ya que son extremadamente elevados sus precios en comparación con otros tipos de almacenamiento de datos y esto se ve reflejado en sus pocas ventas y fuerza en el mercado (Seagate, 2010).

2.1.3. Diferentes tipos de dispositivos de almacenamiento y su historia

Según Norton han aparecido diferentes tipos de dispositivos de almacenamiento de información, que a través de los años han sido mejorados por el humano para darles un buen uso y explotarlos al máximo. Años atrás los dispositivos para almacenar información eran de grandes tamaños, hoy en día se busca que el dispositivo sea lo más pequeño posible y con mayor capacidad para guardar información, en otras palabras, que sea más practico su uso (Norton, 2006).

Gómez de Silva y de Jesus Briseño en su trabajo mencionan que los primeros dispositivos que se utilizaron para almacenar datos fueron las tarjetas perforadas. Estas tarjetas se colocaban en un dispositivo conectado a la computadora que podía leer su contenido. El cual dependía de las posiciones de las perforaciones que se les hubieran hecho a las tarjetas. Las tarjetas perforadas eran un tipo de memoria cuyo contenido no se podía modificar y el acceso al conjunto de tarjetas

que se alimentaban a la computadora era secuencial, pues el lector sólo podía procesar una tarjeta a la vez y lo hacía en orden.

Posteriormente, se empezaron a utilizar cintas magnéticas de dos tipos para almacenar datos. El primer tipo, que se comenzó a utilizar cuando todavía no había computadoras personales consistía de bobinas de distintos tamaños relativamente grandes (de 20-30 cm de diámetro) que contenían una cinta magnética de 1-2 cm de ancho (también había varios tamaños disponibles). El segundo tipo, que comenzó a utilizarse cuando se empezaron a usar las computadoras personales, guardaba la información en casetes idénticos a los que se usan para grabar música (que también tienen dos bobinas, pero más pequeñas y escondidas dentro de un cartucho de aproximadamente 10 cm de largo, 4 cm de alto y 0.5 de ancho). Los dos tipos de cinta magnética se han dejado de utilizar casi por completo, y eran memorias de acceso secuencial cuyo contenido se podía modificar varias veces (aunque a la larga perdían la capacidad de que su contenido cambiara completamente por la forma en que se usaban las orientaciones magnéticas del material del que están hechas para representar los 0s y 1s).

Después de las cintas magnéticas surgieron los discos magnéticos de distintos tipos, muchos de los cuales siguen utilizándose, todos los discos son de acceso directo, su contenido se puede modificar, y como las cintas magnéticas, también utilizan las orientaciones magnéticas de las partículas del material del que están hechos para representar los valores 0 y 1. Algunos discos son permanentes, en el sentido de que no se pueden desconectar de los circuitos que los rodean y que sirven para comunicarse con la computadora para leer y escribir la información en el disco, y son los que han terminado llamándose discos duros. Otros discos duros se pueden remover del dispositivo que lee y escribe su información llamado unidad de disco o drive, para almacenar en una biblioteca de discos magnéticos o transportar a otras computadoras. Estos discos son una capa delgada, flexible, circular, de plástico cubierto de un material ferromagnético, contenidos dentro de una cubierta de plástico un poco más duro, menos delgado y de forma cuadrada,

para protegerlos del polvo, las huellas digitales, los rayones y otros factores que pueden dañar la información que contienen o evitar que el drive la pueda leer y escribir correctamente. Estos discos flexibles muchas veces también se conocen como disquetes, floppy discs o simplemente floppies. Los primeros floppies tenían un diámetro de aproximadamente 25 cm, luego surgieron unos de 14 cm, y los que siguen usándose hoy en día, aunque cada vez menos, son de 8cm de diámetro, se conocían por sus diferentes formatos los cuales son 5 ¼ y 3 ½.

Después de los floppies los siguientes dispositivos que se utilizaron para almacenar información fuera de la computadora son los CD (primero los que no se podían borrar llamados CD-ROM y luego los re-escribibles, llamados CD-RW) y los DVD (también primero los que no se podían borrar, DVD-ROM y luego los modificables, DVD-RW). Estos dos dispositivos son discos de 12 cm de diámetro parecidos a los floppies (aunque no son flexibles) pero en los que la información no se almacena de forma magnética sino óptica. Los drives de CD y DVD por lo tanto contienen un láser que puede grabar y/o leer la información óptica sobre la superficie del disco correspondiente. Tanto los CD como los DVD son de acceso directo, para los dos existen variantes que permiten modificar los datos que contienen y los dos se pueden remover de sus unidades correspondientes.

Normalmente el CPU tiene también varios tipos de enchufes, también conocidos como puertos, que se pueden usar para conectarle a la computadora varios dispositivos externos. Algunos de estos dispositivos externos son dispositivos de memoria secundaria adicionales que se le conectan a una computadora generalmente a través de los puertos USB (siglas que significan en inglés Universal Serial Bus). Aparte de discos duros externos (los discos están atrapados dentro de su unidad, pero la unidad es externa al CPU y por lo tanto se puede conectar y desconectar conforme se necesite) hoy en día han proliferado, principalmente gracias a las cámaras digitales, varios tipos de memorias externas de acceso directo. Algunos de estos tipos de memoria se pueden conectar

directamente a un puerto USB (pues tienen su propio conector USB), como los memory stick.

Por otra parte, hay otros tipos de memoria externa que requieren de su propio drive (que a veces puede ser la misma cámara digital cuyas fotos pueden almacenar, aunque también se pueden usar para almacenar cualquier otro tipo de información digital), que tiene que conectarse mediante un cable a un puerto USB del CPU. Algunos ejemplos son las memorias tipo xD, sD, Compact Flash, y otros que en conjunto se les da el nombre de flash memory o memoria flash (Gómez de Silva Garza & de Jesus Briseño, 2008).

2.1.4. Disco duro

Según Pérez Villa y Santana Tiznado, el disco duro es la principal forma de almacenamiento permanente de datos, es decir, de la memoria física del ordenador. El nombre viene del inglés Hard Disc y a menudo se abrevia como HD. En el disco duro residen los datos que el ordenador necesita con más asiduidad como, por ejemplo, los programas instalados y el sistema operativo. Los discos duros permiten un acceso mucho más rápido a los datos que se encuentran grabados dentro (Pérez Villa, 2008) & (Santana Tiznado, 2001). Pérez Villa menciona que los programas y los archivos son cada vez de mayor tamaño y por eso los discos duros deben tener, cada vez más, una gran capacidad para guardar datos. Según Santana Tiznado un disco duro funciona de una manera muy similar al disco flexible: guarda información en pistas divididas en sectores. Un punto muy importante que toca es que el disco duro es la única parte mecánica de la computadora, y al ser la única parte mecánica es más susceptible de descomponerse (Santana Tiznado, 2001).

Cabe mencionar que en la actualidad existen discos de estado sólido, SSD, la empresa Seagate en un artículo publicado en su página oficial en el año 2010 menciona que los discos de estado sólido utilizan chips de memoria estáticos principalmente memoria flash NAND no volátil, sin embargo cuenta con grandes desventajas como lo son: solo poder escribir un determinado número de veces en

cada bloque, falta de estándares en cuanto al guardado de información y funcionamiento, alto coste en piezas y adquisición, preocupaciones en cuanto a la duración y la fiabilidad de los mismos (Seagate, 2010).

Por las desventajas antes mencionadas se decidió trabajar con discos duros además de que actualmente son los dispositivos de almacenamiento más utilizados por los usuarios y fabricantes de computadoras.

Por lo tanto, se puede definir al disco duro como un dispositivo de almacenamiento de información muy importante, ya que permite guardar grandes volúmenes de información sin importar que se retire o no el suministro de energía eléctrica.

Figura 1. Disco duro.

Fuente: http://www.taringa.net/comunidades/serviciotecnico/9364217/Consulta-Que-marca-de-disco-duro-me-recomiendan.html - revisado 21/10/2016 11:50 a.m.

2.1.4.1. Estructura física del disco duro

Antonio Santana Tiznado explica en su trabajo la estructura física del disco duro y dice que este dispositivo consta de discos metálicos sobre un eje que les permite girar un disco. Los platos (platters) están elaborados de compuestos de vidrio, cerámica o aluminio finamente pulidos y revestidos por ambos lados con una capa

muy delgada de una aleación metálica. Los discos están unidos a un eje y un motor que los hace girar a una velocidad constante de entre 3600 y 7200 rpm.

A diferencia del disco flexible, el cual necesita de una unidad de lectura y escritura, el disco duro está fabricado de tal forma que la unidad de lectura y escritura conforman el dispositivo.

La mayoría de las computadoras tiene un disco duro en el que se puede guardar los datos.

La comunicación entre el disco duro y el procesador se realiza a través del bus de datos, el cual se conecta desde la tarjeta principal del disco duro.

Entre las partes más importantes del disco duro se encuentran las siguientes:

- Cabezales de lectura y escritura, que son unas platinas magnetizadas que tienen como función principal escribir, leer, mover y borrar información en el disco duro.
- Eje, que se encarga de hacer girar los platos durante el proceso de lectura o escritura.
- Brazo de lectura y escritura, el cual permite que los cabezales se desplacen por toda la superficie del disco (Santana Tiznado, 2001).

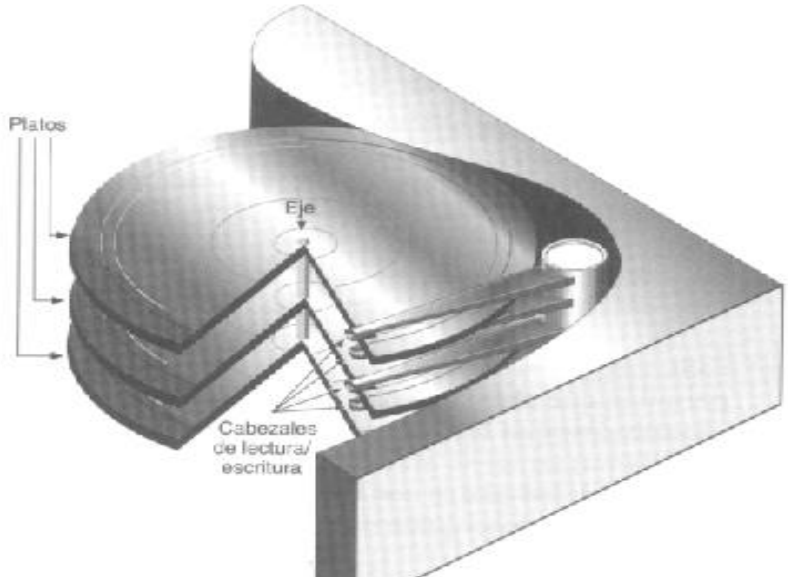

Figura 2. Partes del disco duro.

Fuente: http://jaimesegundo.edu.gva.es/web_mestre.inf/treball/si/disco_duro.htm revisado - 21/10/2016 12:15 p.m.

2.1.4.2. Estructura lógica del disco duro

La estructura lógica de un disco duro, según Jaime Segundo está formada por:

- El sector de arranque.
- Espacio particionado.
- Espacio sin particionar.

El sector de arranque es el primer sector de todo disco duro (cabeza 0, cilindro 0, sector 1). En él se almacena la tabla de particiones y un pequeño programa master de inicialización, llamado también Master Boot. Este programa es el encargado de leer la tabla de particiones y ceder el control al sector de arranque de la partición activa. Si no existiese partición activa, mostraría un mensaje de error. Si tenemos instalado el sistema operativo linux, este instala un menú de arranque en este sector para elegir con que partición arrancar.El espacio particionado es el espacio del disco que ha sido asignado a alguna partición. El espacio no particionado, es espacio no accesible del disco ya que todavía no ha sido asignado a ninguna partición. A continuación, se muestra un ejemplo de un disco duro con espacio particionado (2 particiones primarias y 2 lógicas) y espacio todavía sin particionar.

Podemos crear como máximo cuatro particiones primarias (podremos instalar hasta cuatro sistemas operativos si queremos)

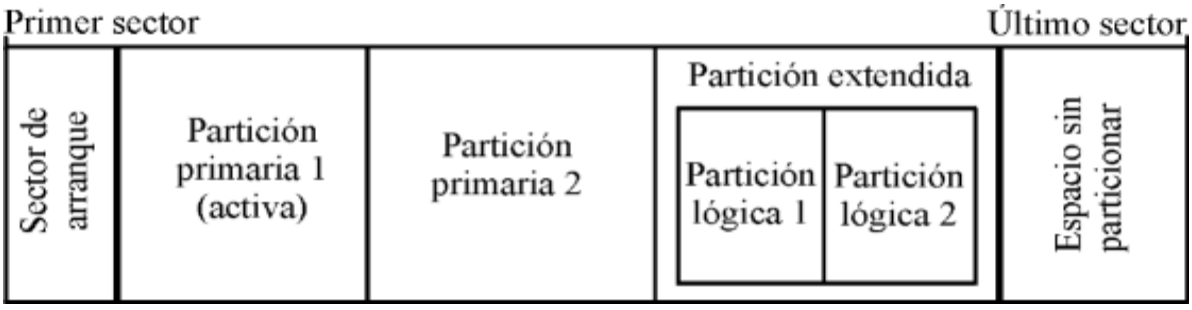

Figura 3. Ejemplo de una estructura lógica de disco duro.

Fuente: http://jaimesegundo.edu.gva.es/web_mestre.inf/treball/si/disco_duro.htm - revisado 21/10/2016 12:38 p.m.

El caso más sencillo consiste en un sector de arranque que contenga una tabla de particiones con una sola partición, y que esta partición ocupe la totalidad del

espacio restante del disco. En este caso, no existiría espacio sin particionar (Jaime Segundo, 2009).

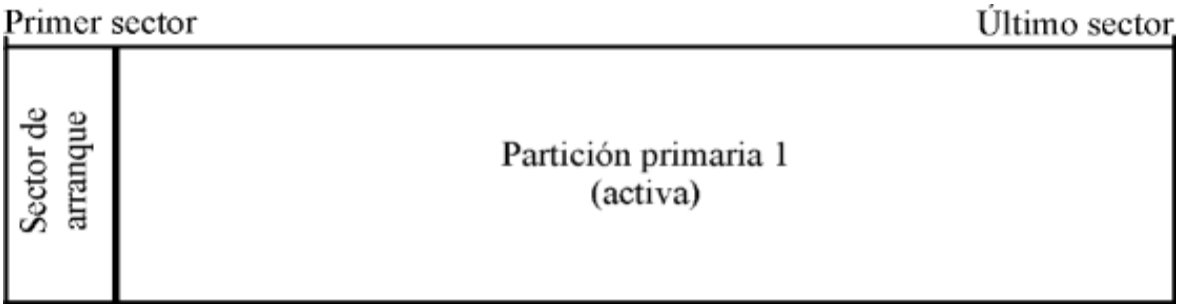

Figura 4. Ejemplo 2 de estructura lógica del disco duro.

Fuente: http://jaimesegundo.edu.gva.es/web_mestre.inf/treball/si/disco_duro.htm - revisado 21/10/2016 12.42 p.m.

2.1.4.3. Particiones de un disco duro

Jaime Segundo menciona que cada disco duro constituye una unidad física distinta. Sin embargo, los sistemas operativos no trabajan con unidades físicas directamente sino con unidades lógicas. Dentro de una misma unidad física de disco duro puede haber varias unidades lógicas. Cada una de estas unidades lógicas constituye una partición del disco duro. Esto quiere decir que podemos dividir un disco duro en, por ejemplo, dos particiones (dos unidades lógicas dentro de una misma unidad física) y trabajar de la misma manera que si tuviésemos dos discos duros (una unidad lógica para cada unidad física).

Como mínimo, es necesario crear una partición para cada disco duro. Esta partición puede contener la totalidad del espacio del disco duro o sólo una parte. Las razones que nos pueden llevar a crear más de una partición por disco se suelen reducir a dos.

Razones organizativas. Considérese el caso de un ordenador que es compartido por dos usuarios y, con objeto de lograr una mejor organización y seguridad de sus datos deciden utilizar particiones separadas.

Instalación de más de un sistema operativo. Debido a que cada sistema operativo requiere (como norma general) una partición propia para trabajar, si queremos

instalar dos sistemas operativos a la vez en el mismo disco duro (por ejemplo, Windows y Linux), será necesario particionar el disco (Jaime Segundo, 2009).

2.1.4.3.1. Particiones primarias y particiones lógicas.

Jaime Segundo menciona en su trabajo que las particiones pueden ser de dos tipos: primarias o lógicas. Las particiones lógicas se definen dentro de una partición primaria especial denominada partición extendida.

En un disco duro sólo pueden existir 4 particiones primarias (incluida la partición extendida, si existe). Las particiones existentes deben inscribirse en una tabla de particiones situada en el primer sector de todo disco duro. Es necesario que en la tabla de particiones figure una de ellas como partición activa. La partición activa es aquella a la que el programa de inicialización (Master Boot) cede el control al arrancar. El sistema operativo de la partición activa será el que se cargue al arrancar desde el disco duro (Jaime Segundo, 2009).

2.2. Información

Según Josefina Pérez Martinez la información es aquello que tiene un significado para nosotros, y aclara algo muy importante, señala que existe una distinción muy importante entre información y datos, define que los datos son valores numéricos que soportan la información (Pérez Martínez, 2012).

2.2.1. Importancia de la información

Josefina Pérez Martínez menciona que los datos son la mínima unidad de información, por si solos carecen de sentido, ya que no tienen propósito o utilidad, no sirven para orientar una acción o para apoyar en la toma de decisiones.

La información se deriva de los datos, los cuales son un conjunto organizado y procesado que tiene un significado y es de utilidad. La información se organizada para un propósito y se genera en un contexto. Es un elemento fundamental para resolver problemas o tomar decisiones.

La definición de Shannon de información indica que hay más información, dependiendo del entorno, y cuanto mayor sea (Pérez Martínez, 2012).

Vicente Aceituno Canal y Josefina Pérez Martinez concuerdan en que el hecho de que la información tenga significado para nosotros quiere decir que cumple con una sintaxis que comprendemos. La información se representa en los sistemas de información utilizando el sistema de numeración binario, que está compuesto únicamente de ceros y unos, la información es un elemento de suma importancia tanto para usuarios individuales como para las empresas, ya que es necesaria para ejecutar diferentes procesos y además es un elemento fundamental para tomar decisiones (Aceituno Canal, 2007) & (Pérez Martínez, 2012).

2.3. Seguridad de la información

Josefina Pérez Martínez menciona en su trabajo que la información es uno de los recursos más valiosos, tanto para las personas como para las organizaciones, por lo tanto, es indispensable protegerla y garantizar su seguridad (Pérez Martínez, 2012). Según Vicente Aceituno Canal, uno de los factores clave en el mantenimiento de la seguridad de información es la selección de medidas de seguridad. Si elegimos mal en el mejor de los casos la medida será poco rentable. En el peor de los casos nos dará una falsa sensación de seguridad, sin mejorarla en absoluto. La selección de medidas depende de varios factores, como el entorno, nuestras expectativas, el valor de los activos, el presupuesto, etcétera. Al decidir cuáles son las mejores medidas de seguridad para una organización, debemos tener en cuenta que:

- Existe un riesgo residual que no puede eliminarse.
- Toda medida será un compromiso entre nivel de protección, eficacia, facilidad de uso, facilidad de gestión, coste, etc. no hay medidas perfectas.
- Dado que no hay medidas perfectas, es mejor una solución buena hoy, que una “perfecta” mañana.
- Para poder confiar en una medida debemos ponerla periódicamente a prueba.
- El coste de la selección de una medida de seguridad debería ser despreciable en comparación con el coste de la medida.

Vicente Aceituno Canal explica que para decir cuánto vamos a gastar en, por ejemplo, el control de accesos, debemos decir primero cual es el nivel de acceso deseado, y comprobar si ese nivel es alcanzable con el presupuesto que tenemos. El presupuesto de seguridad determinará qué medidas podemos permitirnos. Cuando estas son insuficientes para garantizar el cumplimiento de las expectativas de la organización, es el momento de informar a la dirección para bien aumentar el presupuesto, o rebajar las expectativas. La medida de seguridad más simple es la eliminación de oportunidades. Por ejemplo, si un edificio tiene quince entradas, es más eficaz convertir las innecesarias en salidas de emergencia en lugar de poner guardia continua entre ellas. De igual modo, es más eficaz limitar a lo impredecible el número de servidores y servicios conectados directamente con internet. Es más eficaz que todas las líneas de teléfono sean digitales que establecer medidas para impedir que se introduzcan modem analógicos en el edificio.

Vicente Aceituno Canal en su trabajo menciona algunos ejemplos de medidas que previenen incidentes y por consiguiente disminuyen la vulnerabilidad a amenazas conocidas:

- Cortafuegos externos.
- Candados.
- Control de accesos.
- Limitaciones horarias.
- Reservas de suministros.
- Activación solo de los servicios necesarios.

Ejemplos de medidas que disminuyen el impacto, y por tanto protegen tanto contra amenazas previsibles como imprevisibles:

- RAID (hace referencia a un sistema de almacenamiento de datos en tiempo real que utiliza múltiples unidades de almacenamiento de datos)

- Copia de respaldo
- Centro de respaldo.
- Líneas de comunicación redundantes.
- DMZ (red perimetral)

Ejemplos de medidas que mejoran la seguridad indirectamente, al capacitar a la organización para mejorar la seguridad:

- Medidas de gestión de incidentes, incluyendo detección de intrusiones, reacción, identificación del atacante etc.
- Auditorias periódicas.
- Selección de personal de seguridad por especialistas.
- Sistemas de detección de intrusiones.
- Análisis forense de equipos.

Aun que podamos recuperarnos de un incidente gracias a las medidas de seguridad, esto puede acarrear interrupciones en la disponibilidad del activo. Si además de proteger el activo tenemos expectativas de disponibilidad elevadas, debemos evitar que el activo pueda ser afectado por un incidente aislado, adoptando medidas en capas que eliminen los puntos únicos de fallo. Tomar medidas que impidan los incidentes a pesar del fallo de una medida de seguridad individual se conoce en la literatura de seguridad como “defense in depth” (Aceituno Canal, 2007).

2.3.1. Amenazas y vulnerabilidades

Vicente Aceituno Canal menciona en su trabajo que una definición frecuente considera la vulnerabilidad como la evaluación objetiva de la probabilidad de sufrir un determinado ataque en un plazo de tiempo dado. Por otro lado, las amenazas son cualquier circunstancia potencial que pueda afectar a los procesos y expectativas de la organización. Para proteger estas expectativas debemos, evaluar y prever que amenazas pueden afectar a su cumplimiento continuado y ser capaces de medir, sea cuantitativa o cualitativamente, la posibilidad y

probabilidad de materialización de esas amenazas. Las amenazas se pueden clasificar en tres grandes grupos:

- Amenazas terciarias o directas, que son las que amenazan directamente el cumplimiento de nuestras expectativas: ejemplo inundación.
- Amenazas secundarias, que son las que disminuyen o eliminan el grado de éxito de las medidas que ponemos para mitigar las amenazas primarias. Ejemplo: Defectos de cortafuegos.
- Amenazas primarias, que son las que evitan que se mantengan o lleguen a establecerse las medidas que mitigan las amenazas terciarias o secundarias. Ejemplo: Organización de seguridad ineficaz.

En la literatura de seguridad se presta una enorme atención a las amenazas terciarias. Sin embargo, las que tienen un mayor impacto potencial, y además a largo plazo, son las amenazas primarias (Aceituno Canal, 2007).

2.3.2. Pérdida de información

Ni el hardware ni el software son perfectos. El hardware sufre fallos aleatorios fruto de fallos de fabricación, de electricidad estática, o envejecimiento del material que suele agravarse por efectos térmicos. La fabricación de software, es por su parte más un arte que una ciencia, y se encuentran continuamente fallos incluso en software de la industria espacial, como el fallo que destruyo el primer Ariane V.

Vicente Aceituno Canal explica que a pesar de todas las medidas que se pongan para prevenir la pérdida de información, siempre es posible que el error humano aparezca, por motivos como falta de diligencia o incompetencia (Aceituno Canal, 2007). Josefina Pérez Martínez menciona en su trabajo que, aunque parezca sorprendente, diariamente diversas compañías, profesionistas y estudiantes, pierden información valiosa y con ella tiempo dinero y esfuerzo, debido a virus informáticos o a fallas de los dispositivos de almacenamiento. Estos trastornos son ocasionados por el simple e irresponsable hecho de no contar con respaldos o copias de seguridad de su información, lo que ha originado buscar métodos de recuperación de información (Pérez Martínez, 2012).

2.4. Recuperación de información

Baeza Yates y Ribeiro Neto mencionan en su trabajo que el término Recuperación de información fue usado por primera vez por C. Mooers en un escrito de 1952 y luego alcanzó popularidad con un trabajo de R. Fairthorne de 1961. Se utilizó para designar un área emergente de investigación que después de la Segunda Guerra Mundial (1945) encontró dos razones suficientes para prosperar: En primer lugar, existía una necesidad creciente de resolver el problema del acceso físico e intelectual al conocimiento científico. Este conocimiento estaba registrado en una masa documental cuyo crecimiento exponencial se había dado en llamar "explosión documental". En segundo lugar, surgía la tecnología computacional, que siendo capaz de procesar tanto números como textos, brindaba nuevas posibilidades al tratamiento de la información.

Baeza Yates y Ribeiro Neto mencionan que la recuperación de información concierne a la representación, almacenamiento, organización y acceso a los items de información (Baeza Yates & Ribeiro Neto, 1999). Según Igwersen la recuperación de información tiene que ver con los procesos que involucran la representación, almacenamiento, búsqueda y hallazgo de información relevante a los requerimientos de un usuario (Igwersen, 1992). Michael Arias Chavez menciona que ante la gran cantidad de información que se maneja actualmente por medios electrónicos, y el valor tan alto que tiene esta para las personas y organizaciones, es que el cómputo forense está siendo considerado como una herramienta muy valiosa ante la necesidad de contar con algún método que facilite la obtención de pruebas digitales en los casos donde se cometen fraudes o crímenes que atenten contra los usuarios de la información, máxime en tiempos donde el uso de la internet se ha expandido por todo el mundo y donde día a día más negocios tradicionales pasan a formar parte de la gran red de redes a nivel mundial (Arias Chavez , 2007).

2.5. Cómputo forense

El FBI define al cómputo forense como la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente en un medio computacional (Noblett, 2000).

José Cano Martínez menciona que el cómputo forense es una disciplina de las ciencias forenses, que considera las tareas propias asociadas con la evidencia, procura descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso (Cano Martínez, 2006).

Michael Arias Chavez describe al cómputo forense como el conjunto de herramientas y técnicas que son necesarias para encontrar, preservar y analizar pruebas digitales, que son susceptibles de ser borradas o sufrir alteración de muchos niveles. El cómputo forense aprovecha su enfoque científico, aprovechando una serie de fenómenos electromagnéticos con la idea de recuperar, recolectar, analizar, verificar y validar todo tipo de información, para beneficio de quienes han sufrido ataques mal intencionados a sus sistemas informáticos y bases de datos (Arias Chavez , 2007).

2.5.1. Enfoque del cómputo forense

Michael Arias Chavez menciona que se puede incluir al cómputo forense como una herramienta muy importante a tomar en cuenta dentro de una auditoria informática, ya que sirve como un mecanismo para obtener pruebas contundentes que pueden ser tomadas en cuenta si comprobado algún crimen se procede a llevar a instancias mayores como los juicios penales. La destrucción de datos y manipulación de los mismos también pueden rastrearse y recuperarse. Los hábitos de los usuarios de los computadores y las actividades realizadas pueden ayudar a la reconstrucción de hechos, siendo saber de todas las actividades realizadas en un computador determinado (Arias Chavez , 2007).

Según Fernández Bleda en los últimos años han aparecido multitud de empresas que ofrecen herramientas comerciales de análisis forense. El auge de la informática forense ha hecho que se incremente la cantidad de gente interesada en el tema, y muchas de ellas han creado herramientas open source de potencial muy elevado y que son accesibles para cualquier persona (Fernández Bleda, 2004).

Según Antonio Salmerón, en las próximas décadas, e incluso hoy en día, el área de la informática forense ha tenido una gran expansión. La policía y las fuerzas militares siguen marcando una fuerte presencia en las áreas de seguridad de la información y la informática forense. Las empresas privadas han seguido la estrategia de empleo directo a profesionales de seguridad informática forense o computadora, o bien recurrir a otras empresas especializadas basadas en las necesidades existentes (Salmerón, 2015).

2.5.2. Evidencia digital

Eoghan Casey define la evidencia de digital como cualquier dato que puede establecer que un crimen se ha ejecutado o puede proporcionar un enlace entre un crimen y su víctima o un crimen y su autor (Casey, 2004).

Según Ghosh Ajoy, la evidencia digital es cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático (Ajoy, 2004).

Giovanni Zuccardi y David Gutiérrez mencionan que a diferencia de la documentación en papel, la evidencia digital es frágil y una copia de un documento almacenado en un archivo es idéntica al original (Zuccardi & Gutiérrez, 2006).

2.5.3. Hash

Según José Luis Rivas, una función de hash es una función para resumir o identificar probabilísticamente un gran conjunto de información, dando como resultado un conjunto imagen finito, generalmente menor (por ejemplo, un

subconjunto de los números naturales). Una propiedad fundamental del hashing es la que dicta que si dos resultados de una misma función son diferentes, entonces las dos entradas que generaron dichos resultados también lo son (Rivas López, 2009).

Arturo Palacios menciona que en informática hash se refiere a una función o método para generar claves o llaves que representen casi unívoca a un documento, registró archivo, refiere a resumir o identificar un dato (Palacios Ugalde, 2010).

2.5.4. Imagen Forense

Según José Rivas, adquisición de datos. Se realiza una obtención de los datos e informaciones esenciales para la investigación. Se duplican o clonan los dispositivos implicados para un posterior análisis. En esta fase habrá que tener mucho cuidado en la adquisición de los datos puesto que cabe la posibilidad de incumplir los derechos fundamentales del atacante (Rivas López, 2009).

CAPÍTULO III
ESTADO DEL ARTE

A través de los años ha ido creciendo el interés de la gente por la seguridad informática, un área que ha causado gran interés es la del cómputo forense, esta área tiene un gran campo de estudio debido a que en los últimos años han aparecido herramientas opensource que no han podido ser explotadas en su totalidad.

Se realizó una búsqueda de artículos e investigaciones relacionadas con el presente trabajo, se encontraron trabajos interesantes que sirvieron como base para el desarrollo del presente.

En este capítulo se explican algunas investigaciones relacionadas con el presente trabajo. Algunos de los parámetros que se revisaron de dichos trabajos son sobre lo que utilizaron los autores para resolver el problema que se plantearon tal como: herramientas que utilizaron, material analizado, la profundidad de cómputo forense aplicada, sistema operativo en el que fue realizado el proceso que emplearon, método utilizado, técnicas aplicadas, grado de efectividad o los resultados que obtuvieron.

3.1. Metodología basada en el cómputo forense para la investigación de delitos informáticos, 2014.

El trabajo corresponde al autor Demian Roberto García Velázquez, lo que intenta resolver es la determinación del responsable de fuga de información confidencial relacionada con los pacientes del consultorio Médico AC, el día que se reportó el incidente fue el día 7 de mayo de 2013, los datos afectados corresponden a registros de información personal y financiera de los pacientes, esta fuga de información fue reportada por el Dr. Carlos Fernández además de que fue el mismo quien solicito una investigación de cómputo forense para determinar al responsable de la filtración de datos.

El autor detalla que para esta investigación utilizo el sistema operativo Microsoft Windows 7 de 64 Bits, trabajo con la metodología del cómputo forense, esta metodología es un método secuencial que consta de 4 etapas: identificar, preservar, analizar, reportar. Durante la investigación se realizaron actividades como:

- Generación de una imagen forense del sistema afectado.
- Ubicación de los registros del correo electrónico.
- Extracción del archivo de registros del correo electrónico.
- Análisis de los registros del correo electrónico.

La investigación se centró en el análisis del contenido del disco duro de la estación de trabajo utilizada por la secretaria Erika Lucio. Para la generación de la imagen utilizo la herramienta FTK Imager, la imagen fue almacenada en un dispositivo que se analizó en un laboratorio especializado, el proceso fue controlado y documentado durante todo el proceso, y se trabajó únicamente sobre la imagen forense, a través de la herramienta FTK se extrajo un archivo de correo a analizar, en seguida se obtuvo el hash MD5, para acceder a los datos del archivo se utilizó la herramienta PSTViewer Pro 4, esta herramienta permitió recuperar el archivo enviado como adjunto y después poderlo analizar, con esto se llegó a la conclusión que la fuga de información fue por correo electrónico y la responsable de la cuenta es la secretaria del establecimiento, el resultado fue alto.

3.2. Recuperación de información en discos duros, 2007.

El trabajo corresponde al autor Mario Rodríguez Argueta, fue realizado con propósito de investigación, está centrado en la recuperación de información en discos duros a través de una propuesta metodológica de cómputo forense.

La propuesta metodológica contiene las siguientes fases: Detección del incidente, Respuesta inicial, Preparación al incidente, Aseguramiento de la evidencia, Cadena de custodia, Aplicación de la herramienta forense en software libre, Búsqueda de la información, Localización y recuperación de la información, elaboración de reporte, Recomendaciones de seguridad.

Se trabajó en el Sistema Operativo Fedora 6, en el cual se instalaron las herramientas SleuthKit-2.06 y Autopsy-2.08, se llevó el equipo comprometido a un laboratorio en donde se removió el disco duro, se hizo una cadena de custodia para tener el control de quienes tienen acceso a la información, en seguida coloco el disco duro comprometido como esclavo, se configuro la BIOS, el disco duro fue montado como solo lectura, y se creó la imagen forense con la herramienta dd Linux, ya creada la imagen se desmonto para trabajar con ella cumpliendo con el principio de no trabajar directamente con la evidencia original, se trabajó por casos con la herramienta Autopsy y posteriormente se realizó una copia maestra del disco comprometido y una copia de trabajo, previamente se obtuvo el identificador y se analizó metiendo el nombre del archivo eliminado, el grado de efectividad fue de nivel medio.

3.3. Metodología basada en el cómputo forense para la investigación de delitos informáticos, 2014.

El trabajo corresponde al autor Demian Roberto García Velázquez, fue realizado para identificar al responsable de la fuga de información confidencial relacionada a propuestas para el desarrollo de diferentes proyectos relacionados con sistemas de seguridad, en la empresa Vigilancia y Seguridad IW.

Durante la investigación se listaron los procesos a través de la herramienta Process Explorer de Sysinternals y se identificó un proceso sospechoso, se identificaron conexiones de red con un equipo remoto desconocido, de igual

manera se identificaron puertos a la escucha de nuevas conexiones, se realizó un volcado de información en memoria RAM, el autor utilizo las herramientas Dumplt y Volatility para realizar dichas tareas, para analizar mejor el caso el autor detalla que cambio su estación de trabajo a un ambiente controlado, posteriormente realizo una imagen forense del disco duro con la herramienta FTK Imager en el sistema operativo Windows XP, trabajo con la metodología del cómputo forense, que consta de 4 etapas: identificar, preservar, analizar, y reportar. La profundidad de cómputo forense aplicada fue alta, se hizo una comprobación de valores hash MD5 entre el disco duro y la imagen forense creada para saber si era una copia exacta, en seguida se analizó la imagen forense, los resultados no fueron tan buenos debido a la falta de información, el grado de efectividad fue de nivel medio.

3.4. Auditoria forense: metodología, herramientas y técnicas aplicadas en un siniestro informático de una empresa del sector comercial, 2006.

El trabajo corresponde al autor Viviana Marcela Villacís Ruiz, fue realizado para identificar los mecanismos que usaron los empleados de ETASUM para la manipulación de datos e identificar las causas del siniestro informático de la empresa.

El autor detalla que de acuerdo con la directiva de la empresa y a las debilidades encontradas en el departamento de análisis y procesamiento de datos, se aplicaron herramientas las cuales ayudan a la integridad y confidencialidad de la información, las técnicas que aplico para recopilar información son: entrevistas y fotografías, utilizo la herramientas Project para definir el problema, todo esto bajo Windows XP, una vez que se recabaron las debilidades que se encontraron en el departamento, se comenzaron a evaluar las mismas. Las cosas que se encontraron fueron: la falta de clave de acceso al personal, falta de seguridades físicas y lógicas, en seguida se comenzaron a seguir pistas con la evaluación de comando REGEDIT se encontraron: ingreso de cada encuesta, título de día ingresado, numero de la encuesta, tiempo de ingreso y los campos ingresados, en seguida se examinó la bitácora y planificación del supervisor, ya que en la bitácora se encuentra especificado el día hora y quien está utilizando el PC, los resultados

obtenidos fueron de nivel medio, la profundidad de cómputo forense aplicada fue baja.

3.5. Análisis forense de sistemas informáticos, 2009.

El trabajo corresponde al autor José Luis Rivas López, fue realizado para investigar un equipo de cómputo ya que tiene un comportamiento errático.

El sistema atacado se analizó con una combinación de las herramientas: Vmware, The Sleuth Kit, Autopsy, bajo el sistema operativo Ubuntu server, se trabajó con la metodología de cómputo forense, que consta de 4 etapas: identificar, preservar, analizar, reportar.

El autor menciona que en primer lugar creo una imagen forense del servidor atacado, en seguida creo un disco virtual y en el volcó la imagen creada para poder analizarlo en modo no persistente, sin alterar de esta manera la información de dicho disco cuando accedemos a él. En seguida clono el disco duro con el comando dd a un disco nuevo, una vez realizada la clonación hizo un checksum para certificar que son dos copias idénticas. Después montó el disco en escritura y lectura y se procedió a analizarlo. Se identificó que el sistema ha sido objeto de un ataque, logrando acceso como administrador del sistema, el resultado fue de nivel alto, de igual manera, la profundidad de cómputo forense aplicada fue alta.

3.6. Estrategia de informática forense para dispositivos móviles bajo tecnología Android en la universidad regional autónoma de los andes, 2016.

El trabajo corresponde al autor Luis Ernesto Peñaloza Reinoso, fue realizado como una investigación para mejorar las estrategias de informática forense para dispositivos móviles con tecnología Android en la Universidad Regional de los Andes, ya que existen posibles vulnerabilidades a las que se encuentran expuestos los usuarios de la tecnología Android en la UNIANDES como lo son: sustracción de claves, sustracción ilícita de información, accesos a aplicaciones sin permiso, eliminación de información, usurpación de identidad, daño de aplicaciones, daño de equipo entre otras.

El autor menciona que utilizo la metodología de informática forense para dispositivos, la cual consta de tres fases: identificación, análisis, y recuperación de información. El autor describe que probo varias herramientas, entre las que más destacaron son: Oxygen Forensic Suite 2014 y MOBILedit Forensic 2014, son herramienta de las técnicas que utilizo para recolectar información son: encuestas, entrevistas, observación científica, se trabajó directamente con el dispositivo móvil, bajo el sistema operativo Windows XP, la profundidad de cómputo forense fue media, obteniendo un resultado de nivel alto.

3.7. Metodología para un análisis forense, 2014.

El trabajo corresponde al autor Carles Gervilla Rivas fue realizado para investigar un ordenador de un ministerio que se supone está comprometido con un archivo malicioso, se trata de un portátil utilizado por un agente de seguridad infiltrado que ha sido descubierto por un delincuente implicado en la trama que se investigaba, y se sospecha que ha sido por un malware que le han instalado en el ordenador que utilizaba.

El autor menciona que le proporcionaron una imagen forense para poder analizarla, posteriormente se ejecutó una máquina virtual con el sistema operativo Windows XP Service Pack 3, la metodología que utilizo es de propuesta propia y consta de 5 fases: asegurar la escena, identificar y recolectar evidencias, preservar las evidencias, analizar las evidencias obtenidas, redactar informes.

En primera instancia realizó un volcado de memoria sin ejecutar ninguna aplicación, un volcado de memoria directamente de la imagen del sistema sin arrancar la máquina virtual, intento cargar la imagen forense con el software Autopsy, le dio un nuevo formato a la imagen forense con el software qemu pero ninguna técnica tuvo éxito ya que la imagen no se podía leer. Al no tener éxito, ejecuto el antivirus del sistema, Avast, busco archivos txt y capturas de red PCAP las cuales no aportaron ningún resultado, al reiniciar el equipo y volver a realizar los últimos procesos mencionados, el antivirus indico que había un malware, una vez detectado comenzó el análisis correspondiente con la herramientas SIPVicious y Wireshark, al finalizar el proceso de análisis se concluye que era un

virus de tipo keylogger, encontrando direcciones IP y la información que estaba siendo robada, la profundidad de cómputo forense aplicada fue alta, obteniendo un resultado de nivel alto.

3.8. Metodología para el análisis forense informático en sistemas de redes y equipos de cómputo personal, 2010.

El trabajo corresponde al autor Arturo Palacios Ugalde, el trabajo fue realizado como una propuesta de metodológica de análisis forense, la cual se aplica a un caso hipotético en el que se plantea localizar un archivo de texto con información bancaria el cual es relacionado con un fraude bancario teniendo como objetivo principal el identificar cualquier información relacionada con tarjetas bancarias. La metodología que propone consta de cinco fases: Planteamiento del problema, identificación, adquisición de la evidencia, análisis de datos y presentación de resultados obtenidos.

El autor menciona que lo primero es conocer el elementó de estudio que en este caso es una computadora personal, utilizo Windows XP en todo el proceso, al momento de analizar el disco duro de dicha computadora utilizo un bloqueador o protector contra escritura para no alterar de ninguna manera la información contenida, en seguida monto el disco duro a la herramienta FTK imager, opto por realizar la imagen forense de solo una parte del disco duro, una vez creada la imagen la monto a la herramienta y procedió a analizarla, el análisis fue profundo y exitoso a lo solicitado, la profundidad de cómputo forense fue alta, obteniendo un resultado alto.

3.9. Metodología para un análisis forense, 2014.

El trabajo corresponde al autor Carles Gervilla Rivas, realizado para investigar una maquina virtualizada sobre un servidor de un ministerio, que se presume ha sido comprometido, la metodología que utilizo es de propuesta propia y consta de 5 fases: asegurar la escena, identificar y recolectar evidencias, preservar las evidencias, analizar las evidencias obtenidas, redactar informes.

El autor menciona que lo primero que hizo fue realizar un análisis de memoria con la herramienta Volatility versión 2.3.1 después de que se le indico que el sistema operativo era Windows XP Service Pack 2, procedió a realizar el volcado de memoria de la máquina virtual y se encontró un proceso sospechoso que fue realizado con la herramienta netcat, al analizar el archivo malicioso con Volatility se obtuvo la repuesta de que el equipo está siendo atacado por alguien con amplios conocimientos por lo que se concluye y se da la recomendación de analizar la máquina de una manera más profunda y especializada ya que su uso no es seguro, la profundidad de cómputo forense fue media, obteniendo un resultado bajo.

3.10. Herramientas de análisis forense y la recuperación de información en los dispositivos de almacenamiento en los laboratorios de la facultad de ingeniería en sistemas electrónica e industrial de la universidad técnica de Ambato, 2011.

El trabajo corresponde al autor Héctor Alberto Luzuriaga Jaramillo, el trabajo fue realizado para realizar un análisis a un equipo de cómputo que se encuentra en un laboratorio de FISEI-UTA y la intención es la de recuperar una carpeta con archivos significativos para la institución que fue eliminada y que lleva por nombre RESPALDOS, se requiere conocer registros, tiempos de acción como: hora, fecha, y cuenta de usuario, teniendo en cuenta que los laboratorios son utilizados por personas que tienen conocimiento informático.

El autor utilizo como metodología fases generales de cómputo forense tal como: Adquisición de evidencia, identificación de la evidencia, preservación de la evidencia, análisis, e infirme, menciona que lo primero que hizo fue la preparación y aseguramiento de la escena, en seguida identifico la computadora y extrajo el disco duro, la computadora para realizar el análisis del disco duro comprometido tiene instalado Linux distribución Centos 5.3, Helix 3 y Windows 7. En Windows 7 realizo una imagen forense con la herramienta Acronis True Image, sobre la imagen ejecuto programas de recuperación de información los cuales son: Recovery My Files y GetDataBack obteniendo un resultado alto en el hallazgo de

la carpeta solicitada. En la distribución de Linux Helix 3, realizo la imagen forense con la herramienta DD un reporte de auditoria con la herramienta Foremost e hizo un análisis con autopsy el cual arrojo resultados medios. Desde la distribución de Linux Centos 5.3 inicio un análisis de la imagen con la herramienta autopsy la cual arrojo resultados medios. La profundidad de cómputo forense en las distribuciones de Linux fue alta, obteniendo un resultado medio. En Windows 7 la profundidad de cómputo forense fue media, obteniendo un resultado medio.

CAPÍTULO IV

MANUAL BASADO EN CÓMPUTO FORENSE PARA RECUPERAR INFORMACIÓN EN DISCOS DUROS

En este capítulo se presenta la propuesta del manual desarrollado a lo largo de la investigación. El manual contiene los pasos detallados que se deben dar seguimiento para obtener probablemente un buen resultado en la tarea solicitada, así mismo detalla el material a utilizar durante el proceso de recuperación de información. En el presente capítulo de igual manera se hace una breve explicación del por qué se escogió la herramienta sobre la cual se desarrollará el manual y los antecedentes que fueron tomados en cuenta para el desarrollo del mismo.

4.1. Manual basado en cómputo forense para la recuperación de información en discos duros.

4.1.1. Herramientas de recuperación.

La herramienta que se utilizó para la elaboración del manual basado en cómputo forense que sirva como soporte en el proceso de recuperación de información en discos duros es AccessData FTK Imager versión 3.3.0.5, se decidió realizar dicho manual sobre esta herramienta ya que anteriormente se hizo la comparación entre tres herramientas de análisis forense para recuperar información en discos duros, las cuales son Foremost, Autopsy y AccessData FTK imager, las primeras dos herramientas mencionadas se trabajaron en el sistema operativo Kali Linux 1.0 apoyadas de la herramienta DD y la última mencionada sobre el sistema operativo Windows 8.

Se realizaron pruebas de cómputo forense con discos duros que han sufrido perdida de información para tratar de recuperarla. Al finalizar los procesos con las herramientas antes mencionadas, se hizo una comparación de las mismas, tomando en cuenta aspectos tales como:

- Sistema operativo en el que trabajan.
- Fácil instalación.
- Fácil uso.
- Tiempos de ejecución y repuesta.
- Herramienta intuitiva.
- Resultados obtenidos.
- Profundidad de cómputo forense que ofrecen.
- Uso del sistema operativo en el que se alojan.

A continuación, se muestra una tabla con la información que se utilizó para realizar la comparación de las tres herramientas y así poder evaluar cuál era la más adecuada a utilizar para el presente trabajo.

Aspectos \ Herramientas	Foremost	Autopsy	FTK Imager
Sistema operativo	Kali Linux	Kali Linux	Windows 8
Uso del sistema operativo	Bajo	Bajo	Alto
Fácil instalación de herramienta	Si	Si	Si
Fácil uso	No	No	Si
Intuitiva	No	No	Si
Profundidad de cómputo forense	Alta	Alta	Alta
Nivel de resultados obtenidos	Bajo	Medio	Alto
Nivel de ejecución y respuesta, según resultados	Bajo	Medio	Alto

Tabla 2. Tabla comparativa de herramientas.

Fuente: Elaboración propia.

De las tres herramientas antes mencionadas, la que mostro mejores resultados para la tarea solicitada fue AccessData FTK Imager, cabe mencionar que las tres herramientas son gratuitas. La profundidad de cómputo forense que realiza FTK es alta ya que el escaneo es a bajo nivel, esto quiere decir que escanea completamente todos los sectores del disco duro, el nivel de ejecución y respuesta es alto ya que, a comparación con las otras herramientas, realiza la creación y montaje de la imagen forense de una manera más rápida, de igual manera los resultados obtenidos son altos ya que permite recuperar grandes volúmenes de información contenida, de una manera eficiente.

AccessData FTK Imager es una herramienta de uso libre muy completa, la licencia pertenece a la compañía AccessData, su función principal es el análisis forense de dispositivos de almacenamiento, entre las bondades más destacadas que ofrece esta herramienta es que permite: creación de imágenes forenses, volcados de memoria, análisis lógicos de los dispositivos, análisis físicos de los dispositivos, análisis de imágenes forenses en diferentes formatos entre otras cosas. La herramienta se puede descargar desde el sitio web oficial de AccessData (http://accessdata.com/product-download) para elegir la versión correcta es necesario conocer de cuantos bits es el sistema operativo de la PC en la que se instalará. Una vez que se ha descargado se procede con la instalación del programa, cabe mencionar que la instalación de la herramienta es muy sencilla, la cual se detalla más abajo.

4.1.2. Material a utilizar.

El manual está dirigido para trabajar con la recuperación de información en discos duros, de tal manera que para comenzar se necesitará evidentemente el disco duro dañado o en el que se ha producido la perdida de información, un kit usb de cables SATA/IDE, una computadora la cual contendrá la herramienta AccessData FTK Imager, y un dispositivo de almacenamiento con mayor o igual capacidad al dispositivo que se desea recuperar la información, además de contar con una distribución instalada del sistema operativo Windows.

4.1.3. Instalación de la herramienta ACCESSDATA FTK IMAGER.

Lo primero que se debe realizar es descargar la herramienta del sitio mencionado anteriormente. Una vez que se ha descargado, se buscará el instalador que se descargó, se seleccionará con un clic y en seguida se dará clic izquierdo.

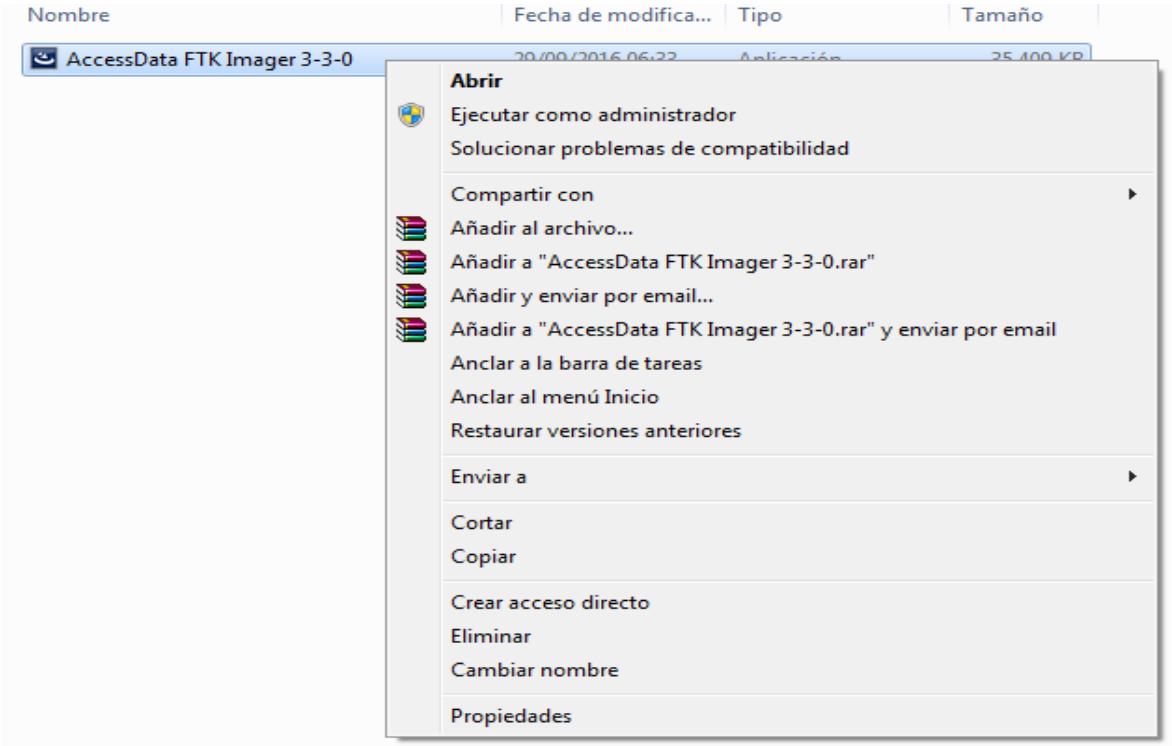

Figura 5. Ejecutable AccessData FTK Imager 3-3-0.

Fuente: Elaboración propia.

En seguida se dará clic en la opción “Ejecutar como administrador”, aparecerá una ventana y se le dará clic en el botón Next.

Figura 6. Pantalla de instalación.

Fuente: Elaboración propia.

Se abrirá una nueva venta con los términos y condiciones que implica el uso de la herramienta, una vez leídos se seleccionará la opción que se aceptan los términos establecidos y se dará clic en el botón Next.

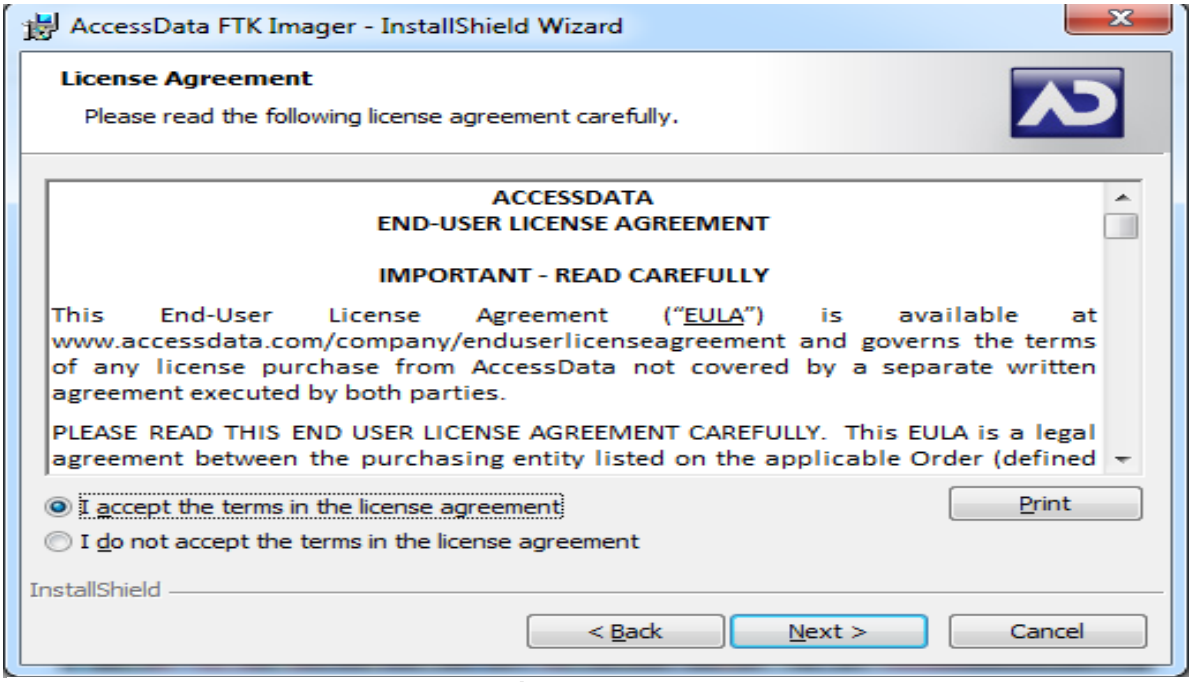

Figura 7. Términos y condiciones.

Fuente: Elaboración propia.

Se abrirá una nueva ventana en la cual aparecerá una dirección por default en donde se instalará la herramienta, si se desea cambiar la dirección se puede hacer, una vez especificado el destino se dará clic en Next.

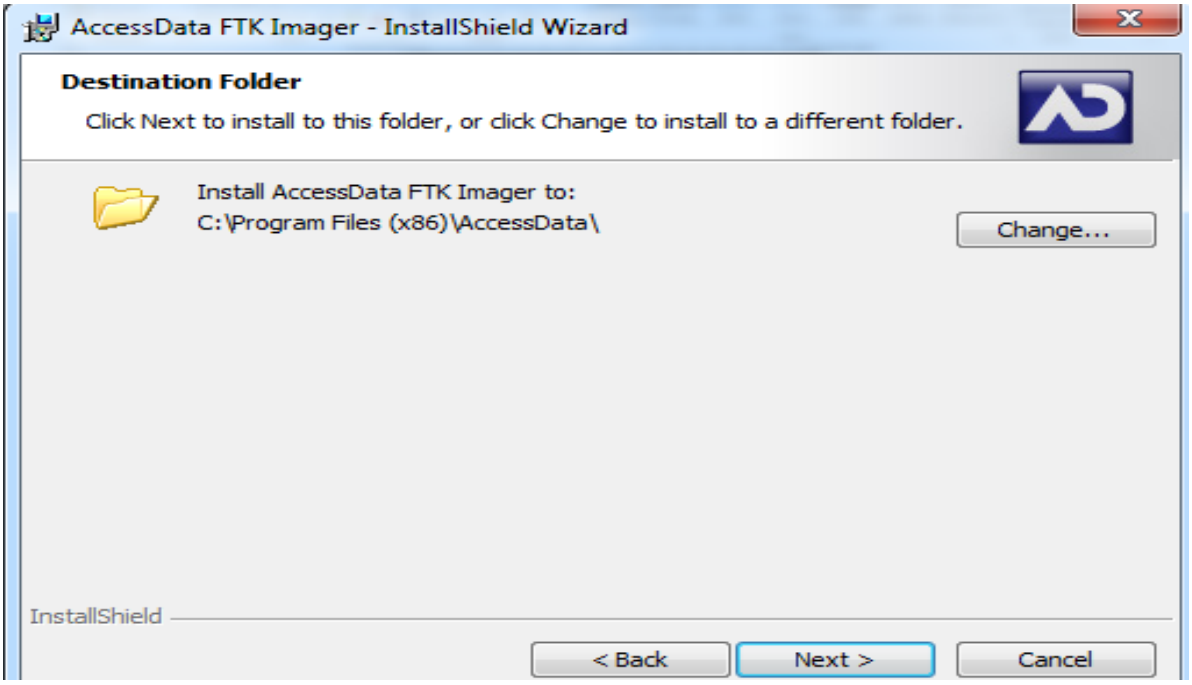

Figura 8. Folder de destino.

Fuente: Elaboración propia.

Aparecerá una nueva ventana en la cual se debe especificar con un clic en el botón Install que se desea comenzar con la instalación de la herramienta.

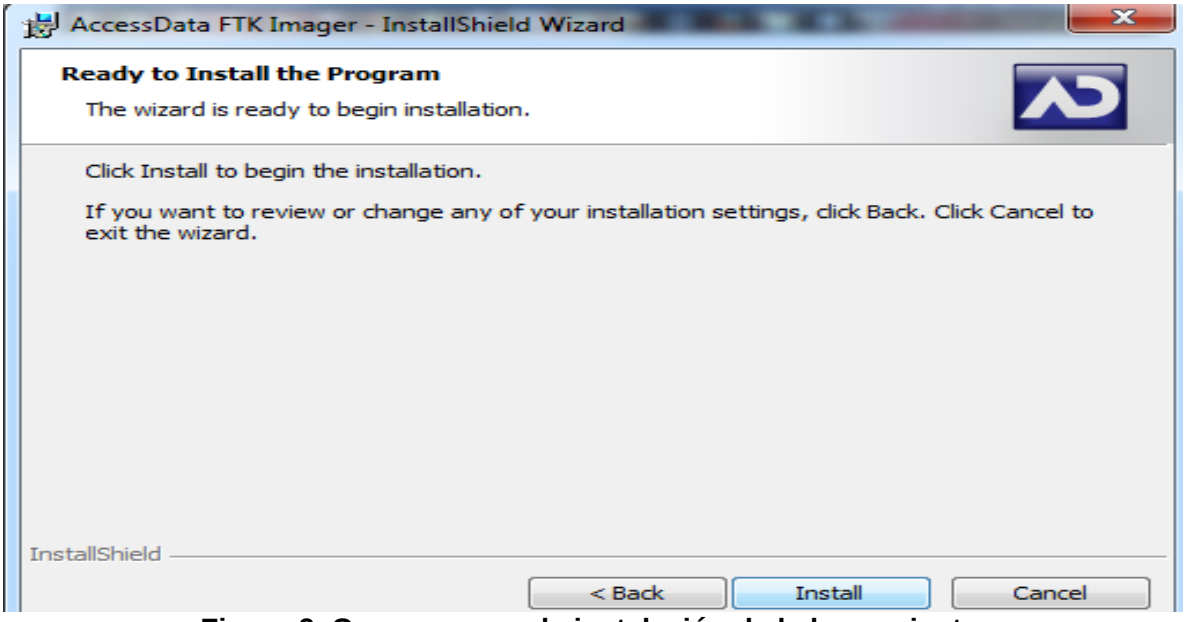

Figura 9. Comenzar con la instalación de la herramienta.

Fuente: Elaboración propia.

Al realizar lo antes mencionado, se abrirá una nueva ventana con el progreso de la instalación, se debe esperar a que el proceso termine.

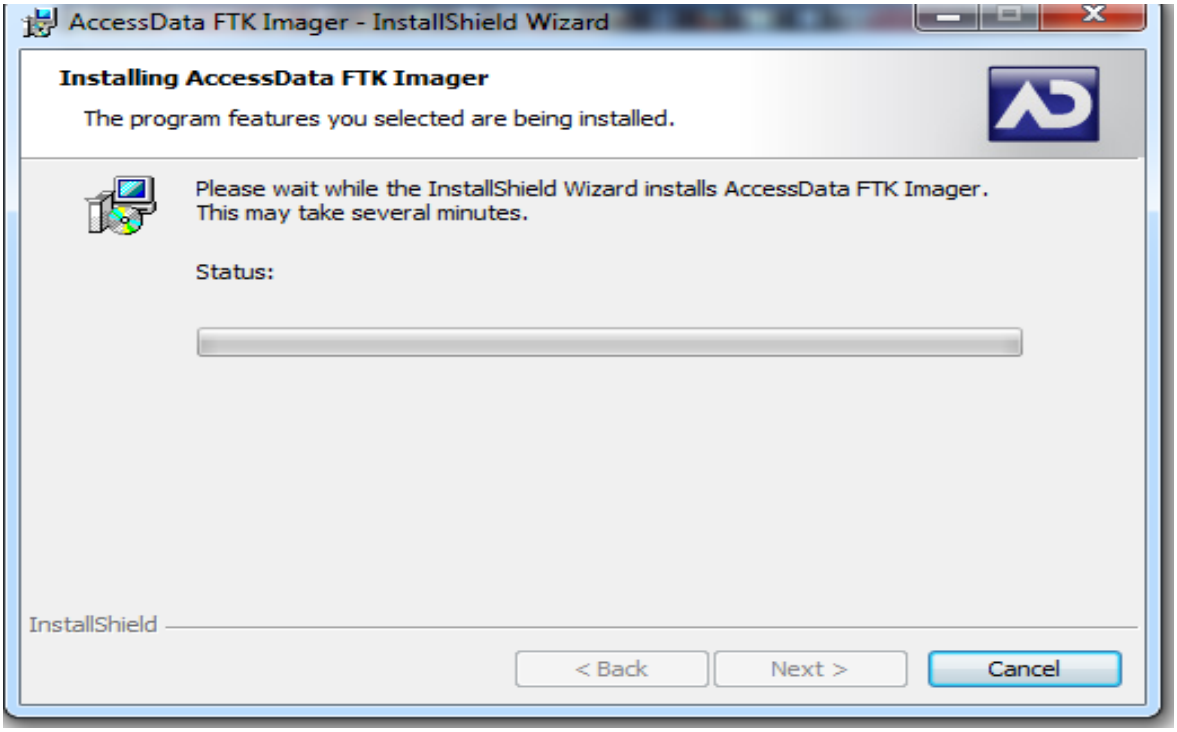

Figura 10. Estado de instalación.

Fuente: Elaboración propia.

Al finalizar el proceso aparecerá una ventana indicando que la herramienta ha sido instalada, en seguida se seleccionará la casilla Launch AccessData FTK Imager para indicar que se desea un acceso directo de la herramienta en la pantalla de inicio, para finalizar se dará clic sobre el botón Finish.

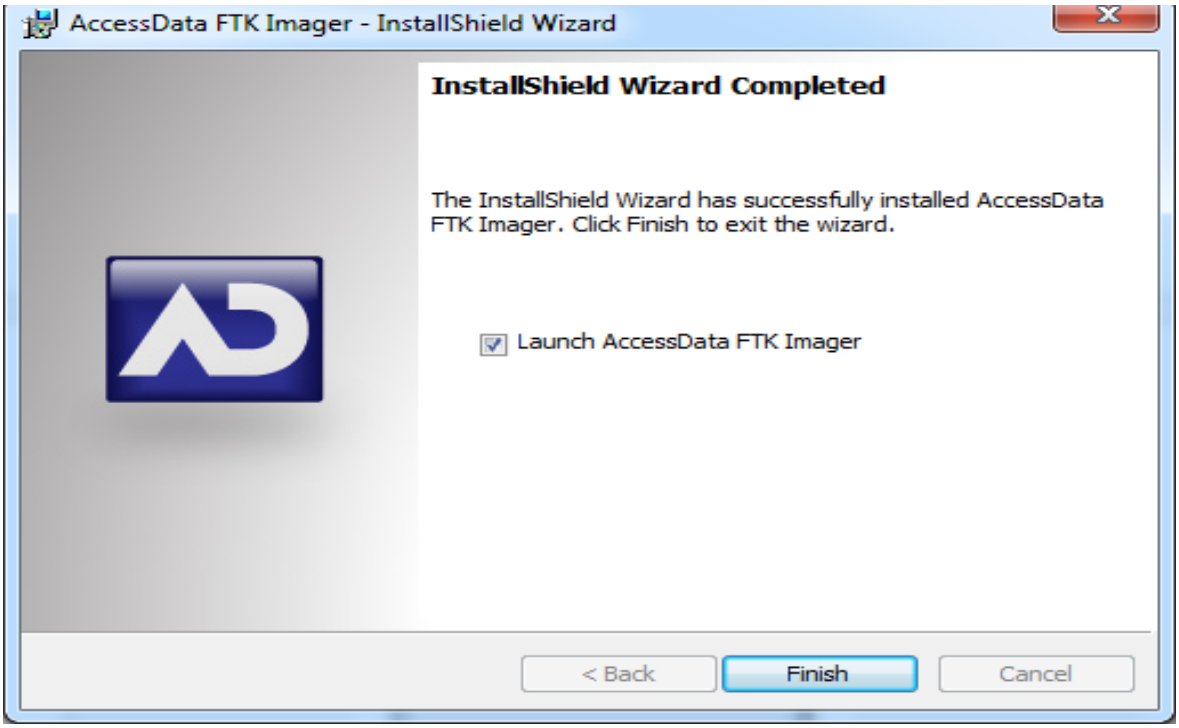

Figura 11. Instalación Completada.

Fuente: Elaboración propia.

Al dar clic en Finish se abrirá la herramienta y estará lista para utilizarse.

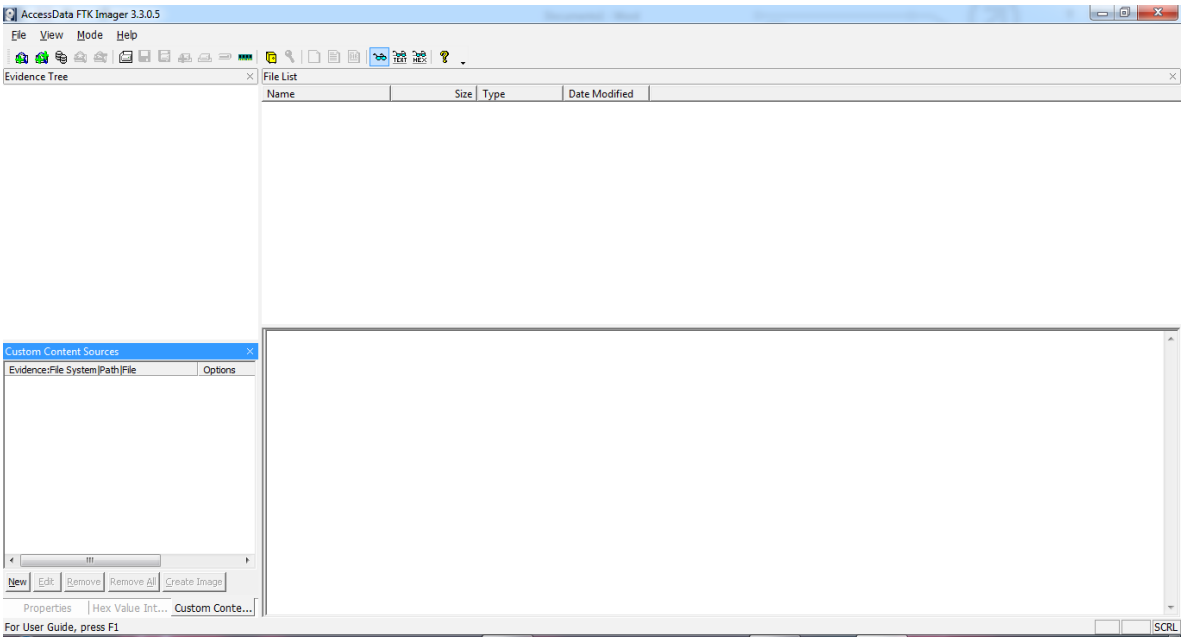

Figura 12. Pantalla principal de la herramienta.

Fuente: Elaboración propia

4.1.4. Preparación Cables SATA/IDE.

La preparación de los cables SATA/IDE se describe brevemente ya que al comprarlos la mayoría trae un pequeño manual de uso, además de ser muy intuitivos en las partes que los componen.

Contenido de la caja

- 1 Adaptador USB a SATA/IDE
- 1 Fuente de alimentación universal
- 1 Cable de alimentación
- 1 Manual

Requisitos

- Un puerto USB disponible
- Un enchufe a la red eléctrica

Instrucciones

1) Conectar uno de los extremos de un cable de datos SATA en el puerto SATA del adaptador para discos duros.
2) Insertar el extremo restante del adaptador para discos duros en el puerto SATA del disco duro a analizar.
3) Conectar la interfaz de conexión del disco duro IDE con el puerto IDE incluido en el adaptador para discos duros.
4) Insertar el conector de alimentación SATA incluida con la fuente de alimentación al puerto de alimentación SATA ubicado en el panel trasero de la unidad del disco duro a analizar.
5) Insertar el conector USB a un puerto USB del ordenador utilizado para el análisis del disco duro.

4.1.5. Proceso.

El proceso está conformado de cuatro y dos etapas según sea el caso por el cual se necesite recuperar información. Las etapas para el primer caso son: identificación, preservación, análisis y reporte, las etapas para el segundo caso son: identificación y análisis.

NOTA: Si el objetivo es recuperar información para posteriormente presentarla como evidencia legal ante una corte, diríjase al proceso 1. Si el objetivo únicamente es recuperar información por cuestiones personales, diríjase al proceso 2.

4.2. Proceso para recuperar información con validez legal (proceso 1).

Todo lo que se realice deberá ser documentado ya que se puede llegar a necesitar documentación que sirva como evidencia para ser utilizada ante un proceso legal.

4.2.1. Identificación.

Se debe conocer el disco duro a analizar, cosas tales como: capacidad del disco duro, tomar fotografía del disco duro sometido, así como información de número de serie, modelo, marca y toda la información visible que se pueda recabar, sobre qué información se desea recuperar, los daños que causaron la perdida de información, la fecha en la que se recibió el disco duro, nombre completo de la persona que solicita la recuperación de información y toda la información posible que se considere para cada caso, es muy importante recabar y documentar lo antes mencionado ya que sirve como evidencia ante un proceso legal.

4.2.2. Preservación.

Teniendo en cuenta lo antes mencionado, se conecta el disco duro del cual se desea recuperar la información a la computadora que contiene la herramienta por medio de los cables SATA/IDE, en seguida se debe abrir la herramienta AccessData FTK Imager.

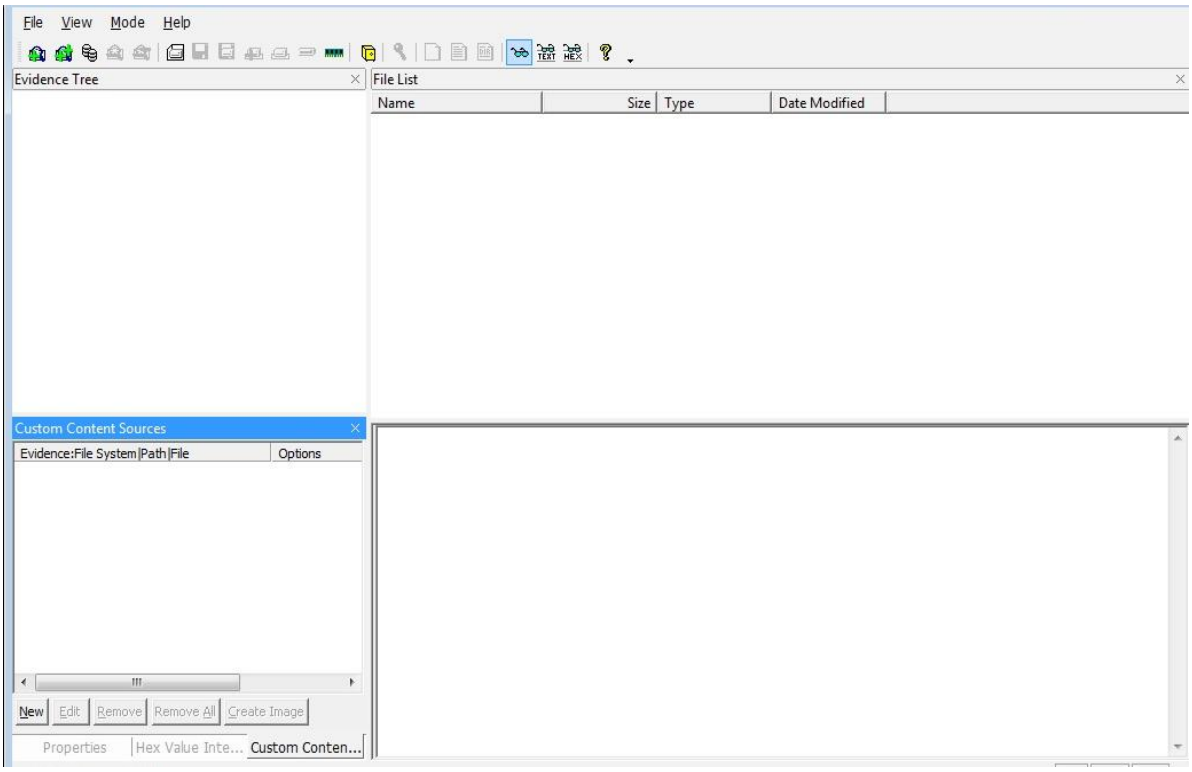

Figura 13. Pantalla principal de la herramienta FTK.

Fuente: Elaboración propia.

Una vez abierta la herramienta, se procede a realizar la imagen forense, para esto se da clic en la pestaña File,

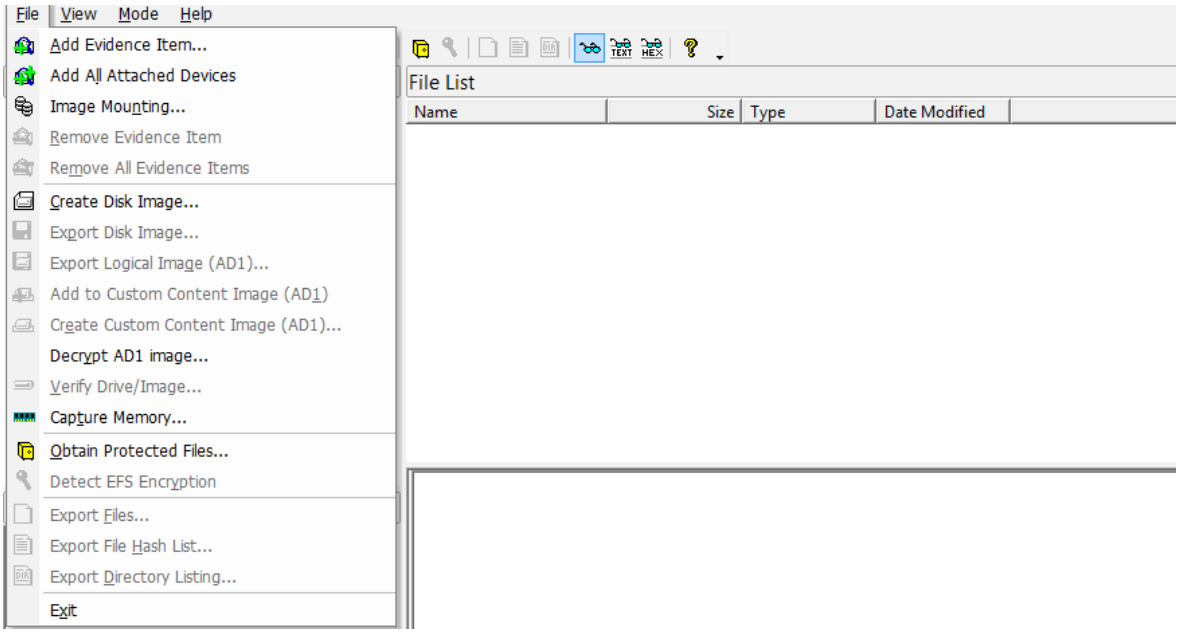

Figura 14. Pestaña File.

Fuente: Elaboración propia.

Se desplegará un menú en el cual se le dará clic en la opción Create Disk Image.

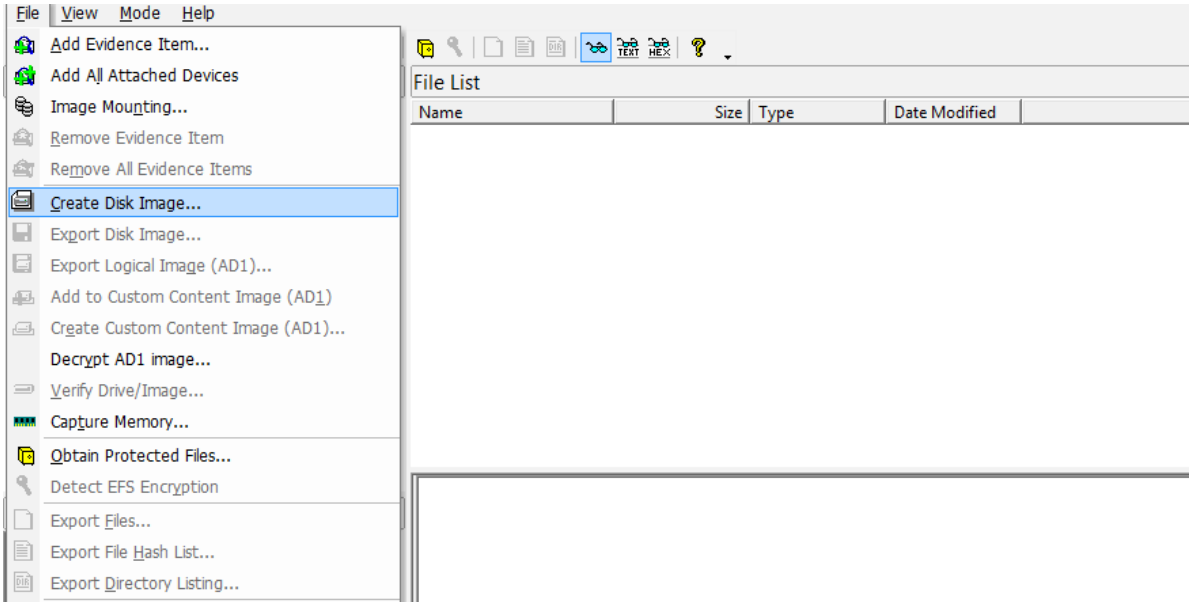

Figura 15. Opción Create Disk Image.

Fuente: Elaboración propia.

En seguida se debe seleccionar la opción desde donde se desea realizar la imagen forense, es decir de un disco físico, disco lógico (particiones), archivo de imagen, folder, entre otros. Como se está trabajando con un disco duro físico se procederá a seleccionar esa opción.

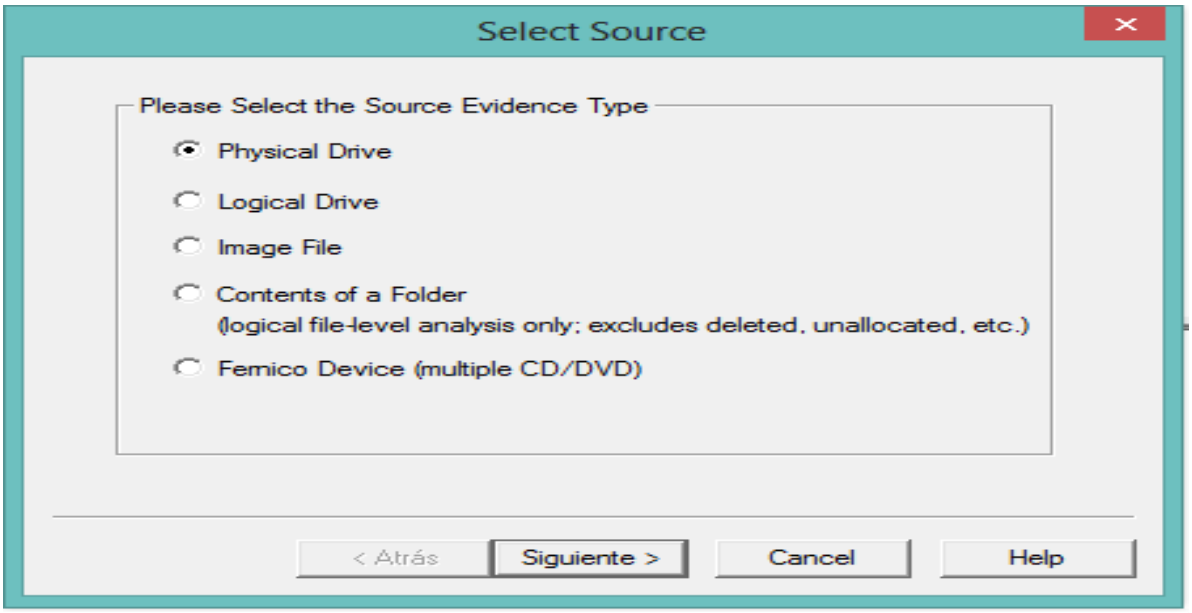

Figura 16. Selección de fuente.

Fuente: Elaboración propia.

Posteriormente se debe seleccionar la unidad en la que está montado en el equipo y dar clic en Finalizar.

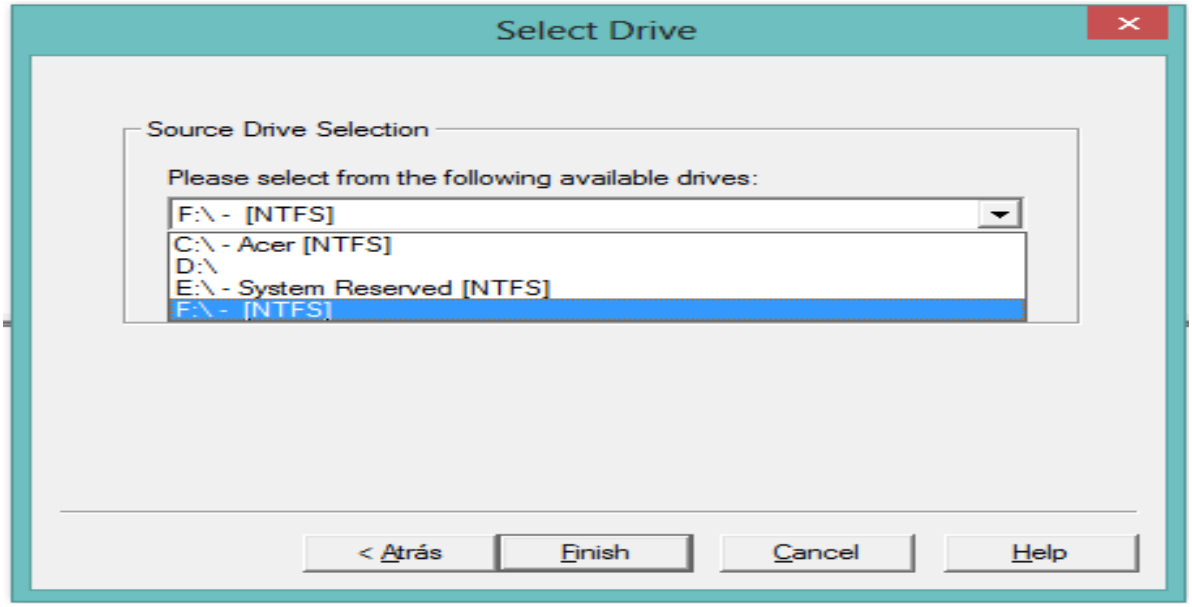

Figura 17. Selección de unidad.

Fuente: Elaboración propia.

Al dar clic en el botón finalizar se abrirá una nueva pantalla llamada creación de imagen.

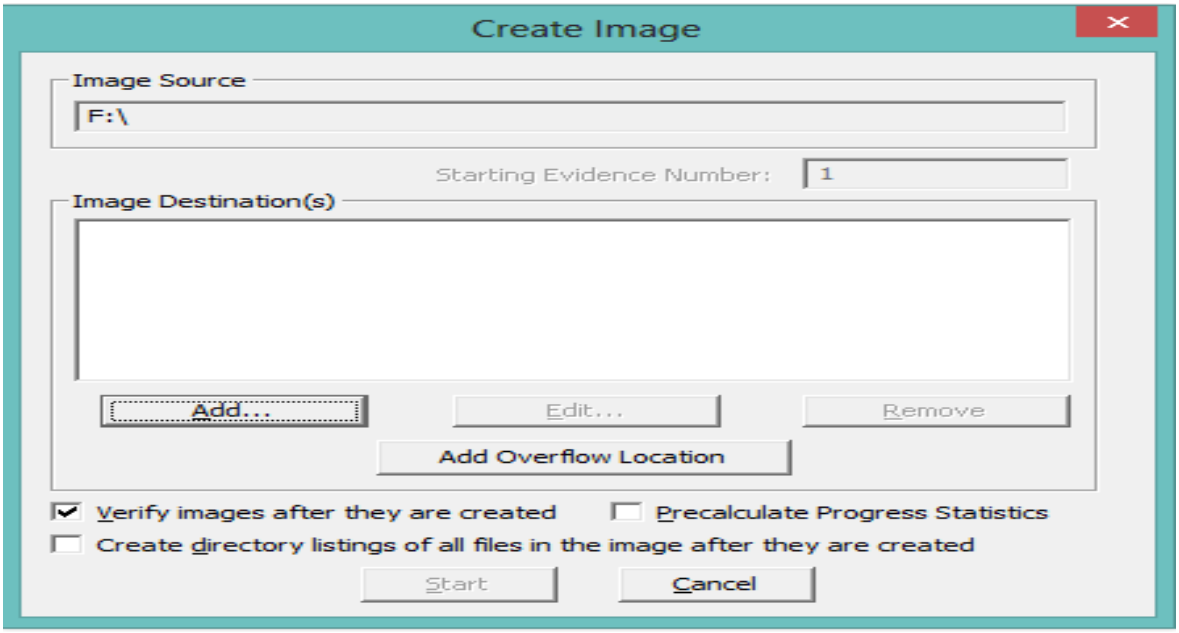

Figura 18. Creación de imagen.

Fuente: Elaboración propia.

A continuación, se deberá dar clic en el botón Add de dicha ventana y seleccionar el tipo de extensión de la imagen forense y dar clic en el botón siguiente, se recomienda seleccionar Raw (dd) ya que es la extensión más utilizada por la mayoría de herramientas de análisis forense.

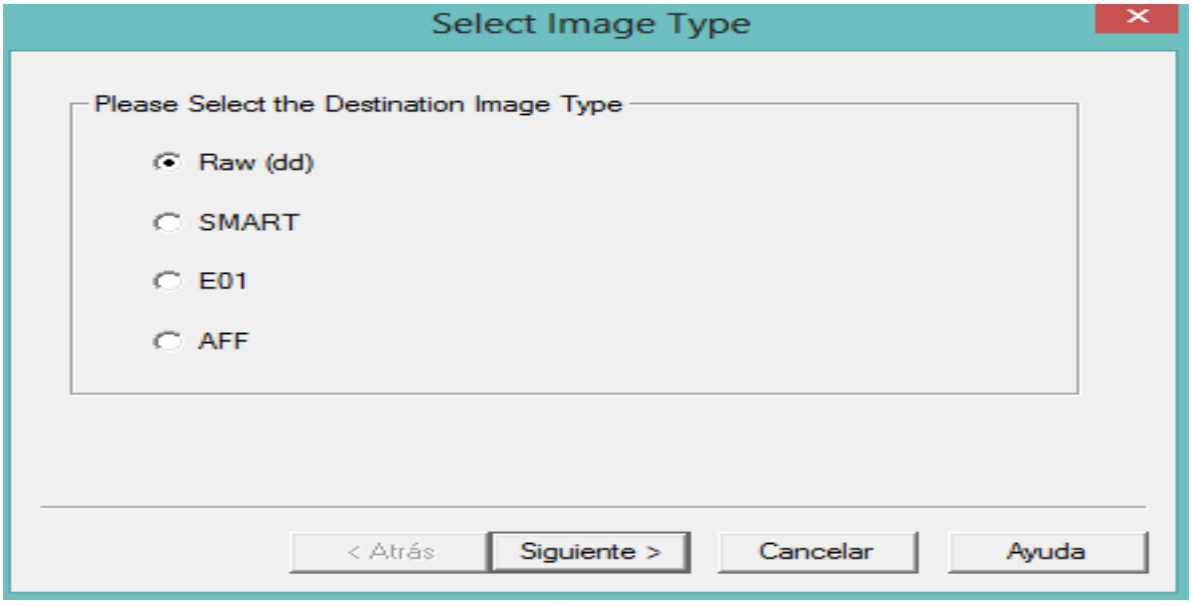

Figura 19. Selección del tipo de la imagen.

Fuente: Elaboración propia.

Se abrirá una nueva ventana llamada Evidence Item Information la cual se deberá llenar con información solicitada del caso en el cual se está trabajando y una vez llenados los campos se dará clic en el botón siguiente, es muy importante ya que aparecerá en el reporte que se creará.

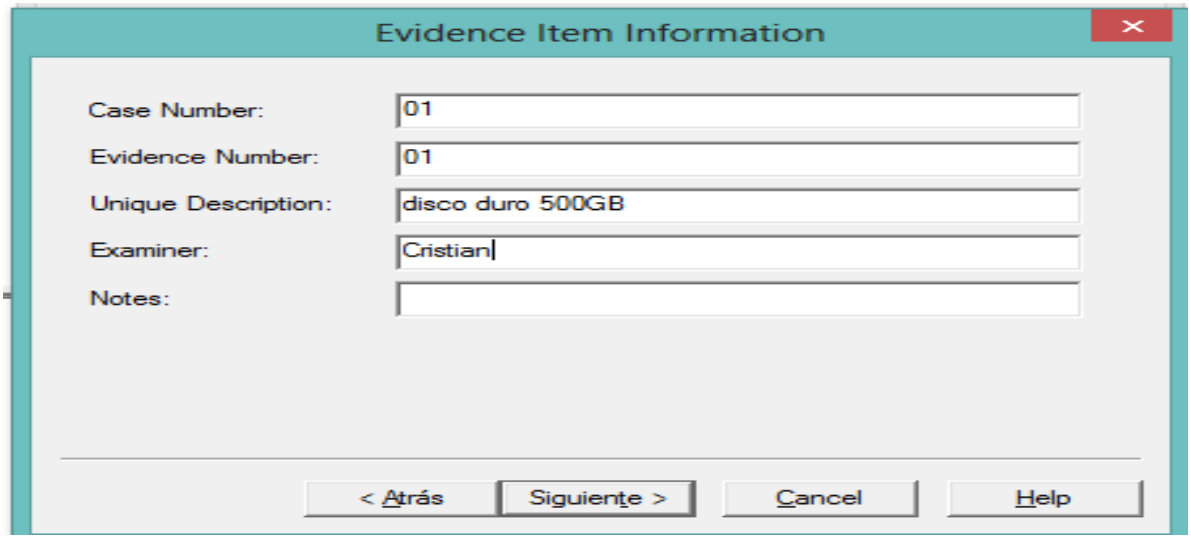

Figura 20. Información de la evidencia.

Fuente: Elaboración propia.

Al concluir el proceso anterior se abrirá una nueva ventana llamada Select Image Destination en la cual se debe escribir el destino y nombre de la imagen forense que se creará, en seguida se deberá dar clic en el botón Finish.

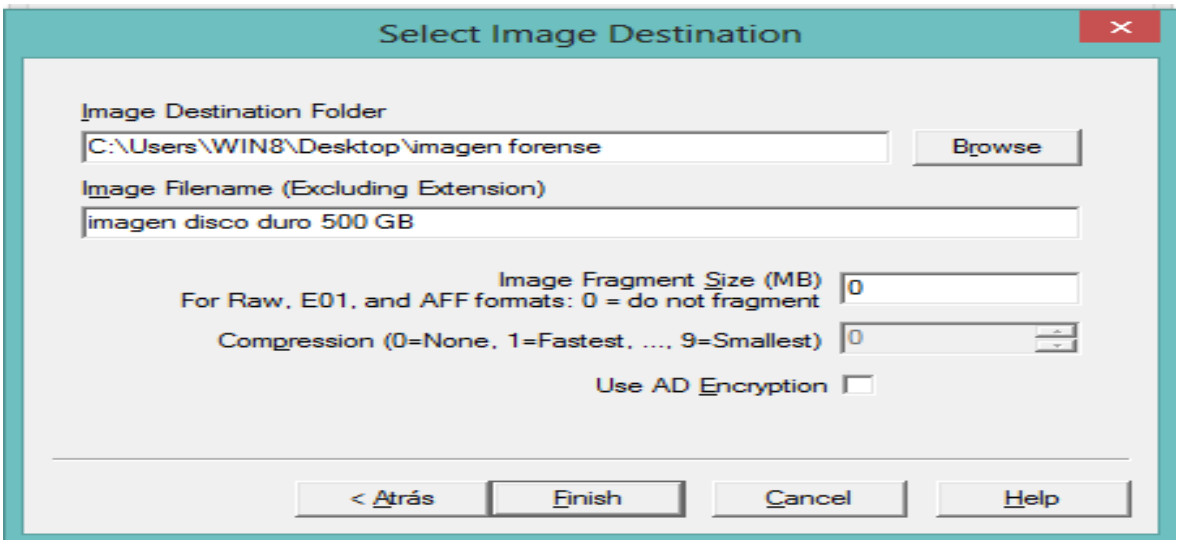

Figura 21. Campos llenados correctamente.

Fuente: Elaboración propia.

Completado lo anterior, se seleccionará la opción Verify images after they are created, esta opción es para indicar que deseamos verificar que la imagen es una copia exacta del disco sometido, dicha verificación se hará de manera automática por medio de algoritmos de autentificación llamados hash.

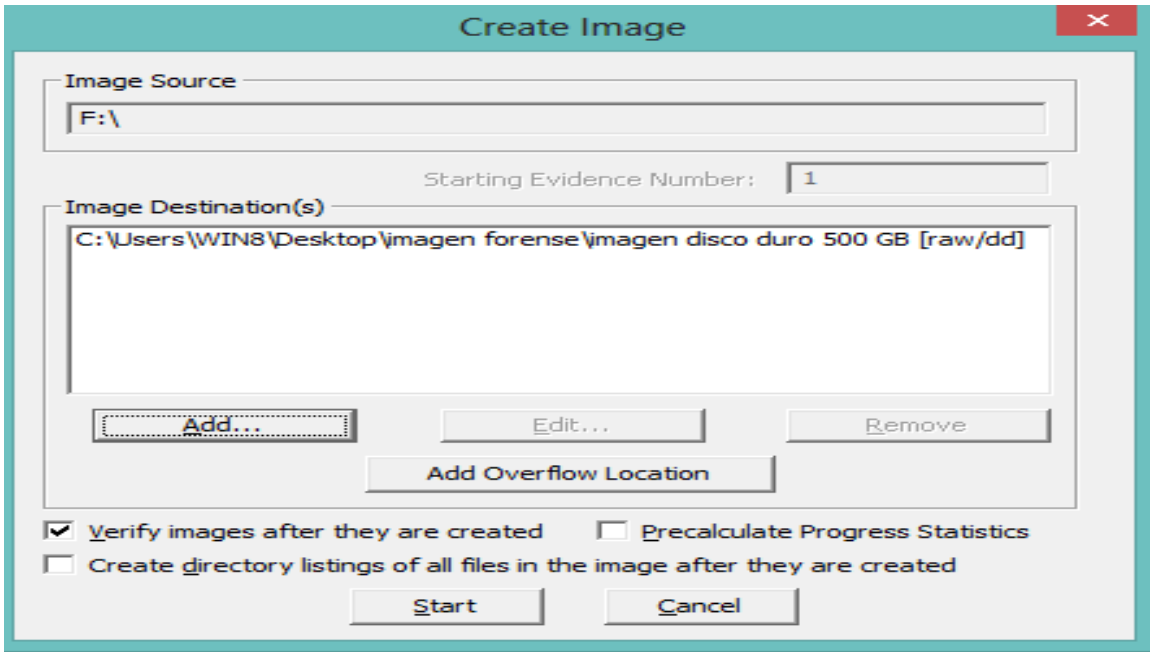

Figura 22. Pantalla lista para la creación de la imagen.

Fuente: Elaboración propia.

En seguida se procederá a dar clic en el botón start para comenzar con la creación de la imagen, de tal manera que abrirá una nueva ventana llamada Creating Image en la cual se verá reflejado el progreso de creación de la imagen forense. Hay casos en los que nos es posible la correcta creación de una imagen forense por lo tanto se puede trabajar directamente con el disco duro físico yendo directamente a la etapa 3.

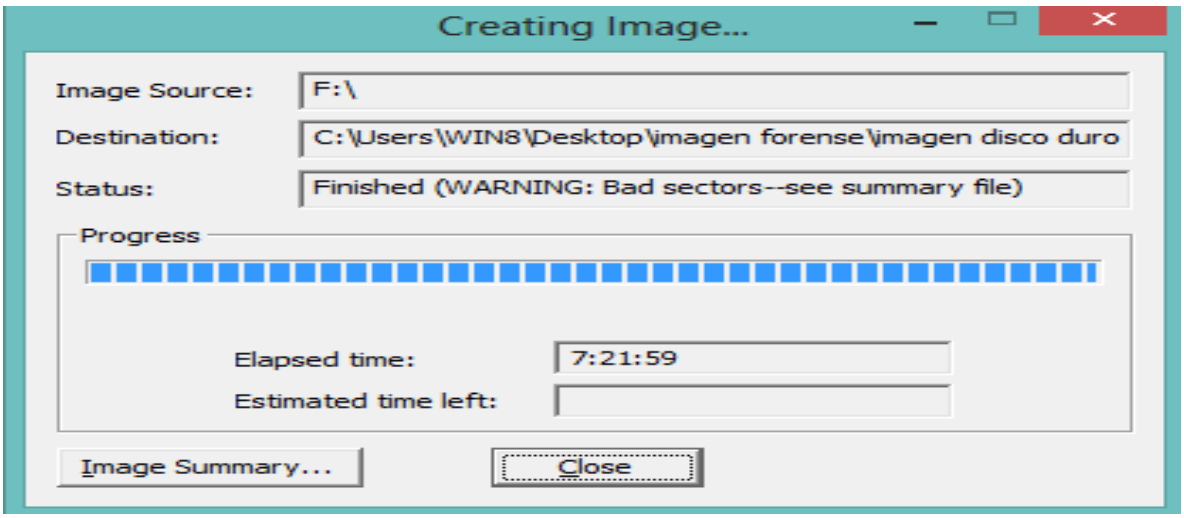

Figura 23. Estado de la creación de la imagen.

Fuente: Elaboración propia.

El tiempo de creación de la imagen forense es diferente para cada usuario según la capacidad del disco duro a analizar. Al finalizar la imagen forense y dar clic en el botón close, automáticamente se comenzará a calcular el hash.

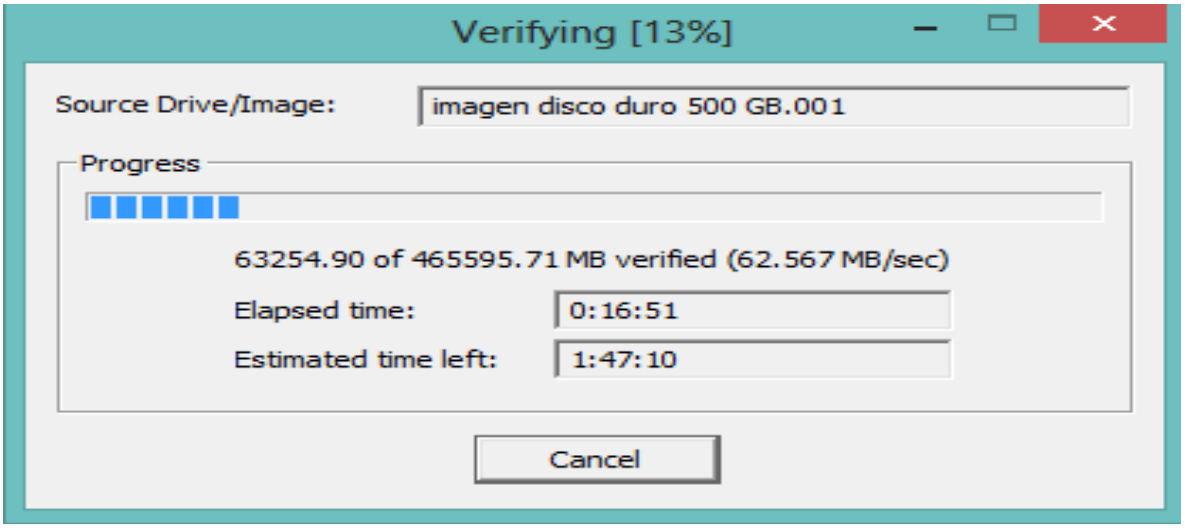

Figura 24. Verificación de la imagen creada.

Fuente: Elaboración propia.

Al finalizar el proceso aparecerá una ventana con información de los resultados obtenidos durante la verificación de la imagen. Esta parte es la más importante ya que el hash calculado deberá ser igual, al ser iguales indica que se realizó una copia exacta (imagen forense) del dispositivo que se analizará.

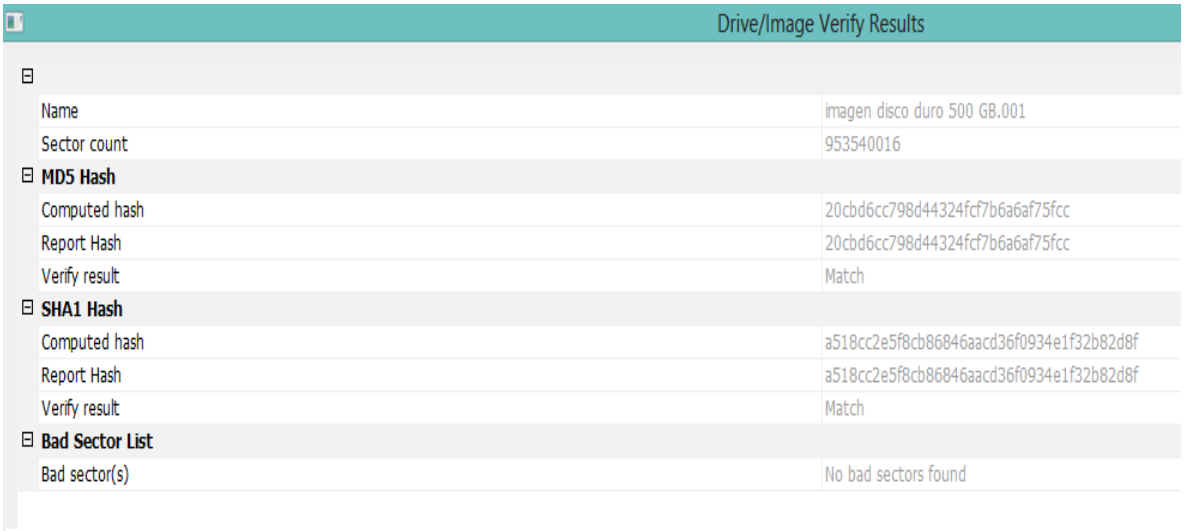

Figura 25. Resultados de la verificación.

Fuente: Elaboración propia.

En seguida se dará clic en el botón close y se verificará la creación de los archivos en la ubicación que se colocó como destino de la imagen forense. En la ubicación se encontrará la imagen forense y un reporte con formato txt que contiene los detalles del proceso de la creación de la imagen.

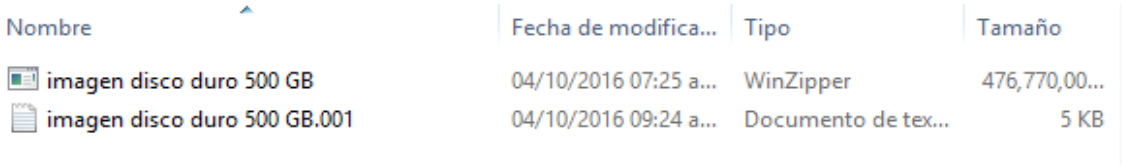

Figura 26. Archivos creados.

Fuente: Elaboración propia.

Ahora que ya se ha creado la imagen forense, el disco duro se puede desconectar y se debe colocar en un lugar seguro.

4.2.3. Análisis.

Lo que sigue es el análisis de la imagen forense creada, entonces lo que se debe hacer es montar la imagen forense a la herramienta que se está utilizando.

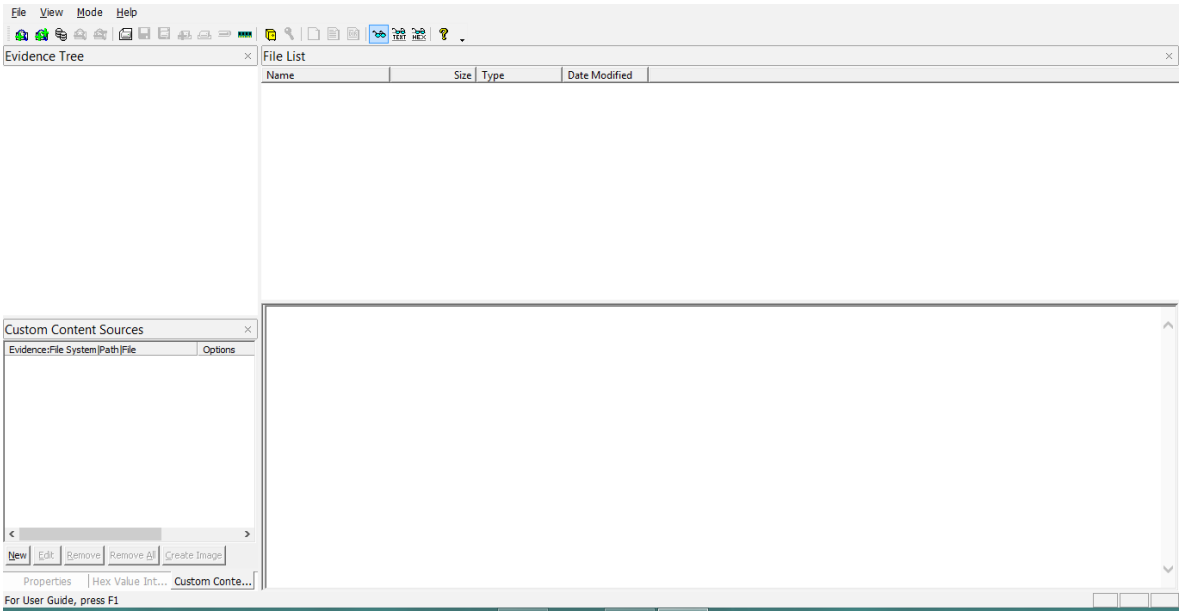

Figura 27. Pantalla principal de FTK para realizar análisis.

Fuente: Elaboración propia.

Para realizar el montaje se da clic en la pestaña File y en seguida en la opción Add Evidence Item.

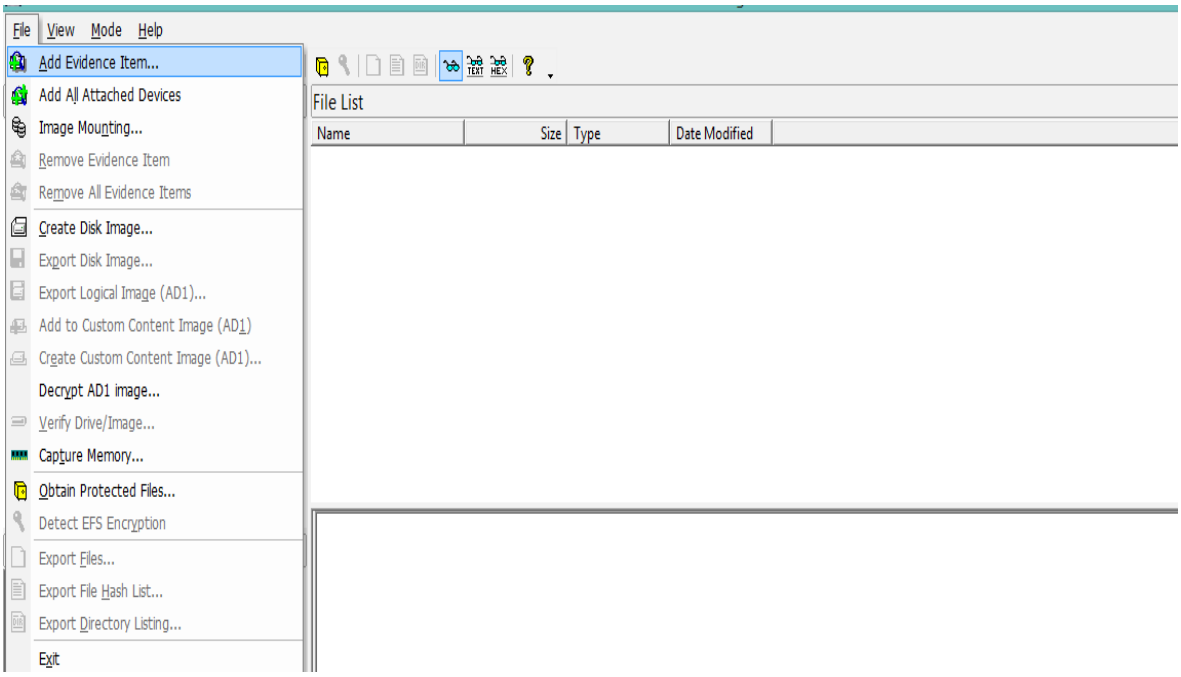

Figura 28. Montar Imagen.

Fuente: Elaboración propia.

En seguida se elige el tipo de evidencia a agregar y se da clic en el botón siguiente, así que se seleccionará la opción Image file ya que se trabajará con la imagen forense antes creada (hay casos en los que nos es posible la correcta creación de una imagen forense por lo tanto se puede trabajar directamente con el disco duro físico).

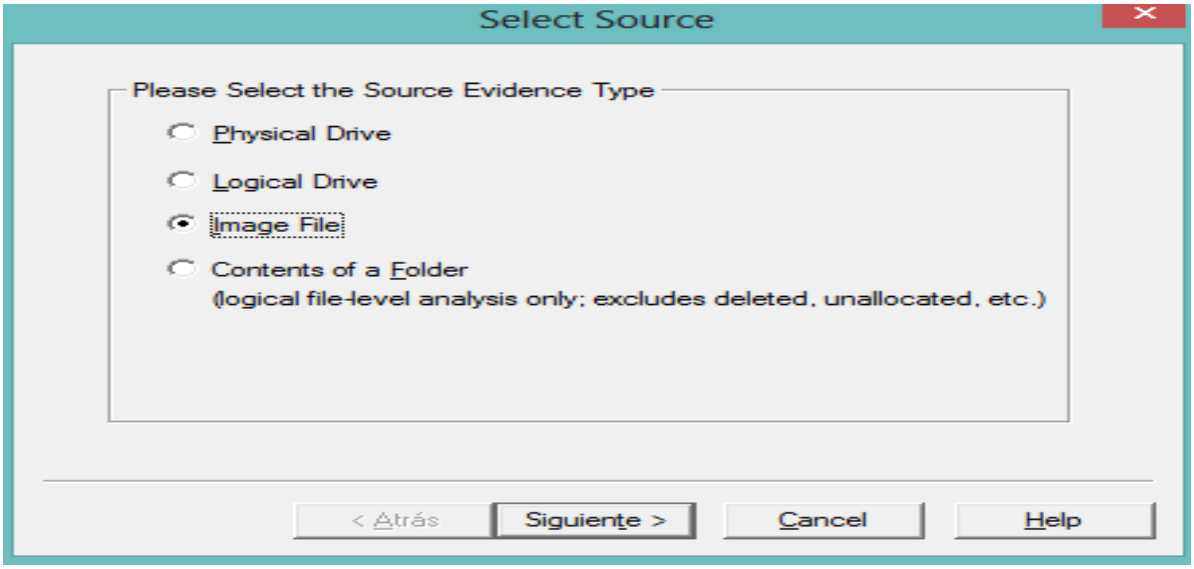

Figura 29. Selección de fuente.

Fuente: Elaboración propia.

En seguida se debe seleccionar la ubicación de donde se encuentra la imagen forense y dar clic en el botón finish.

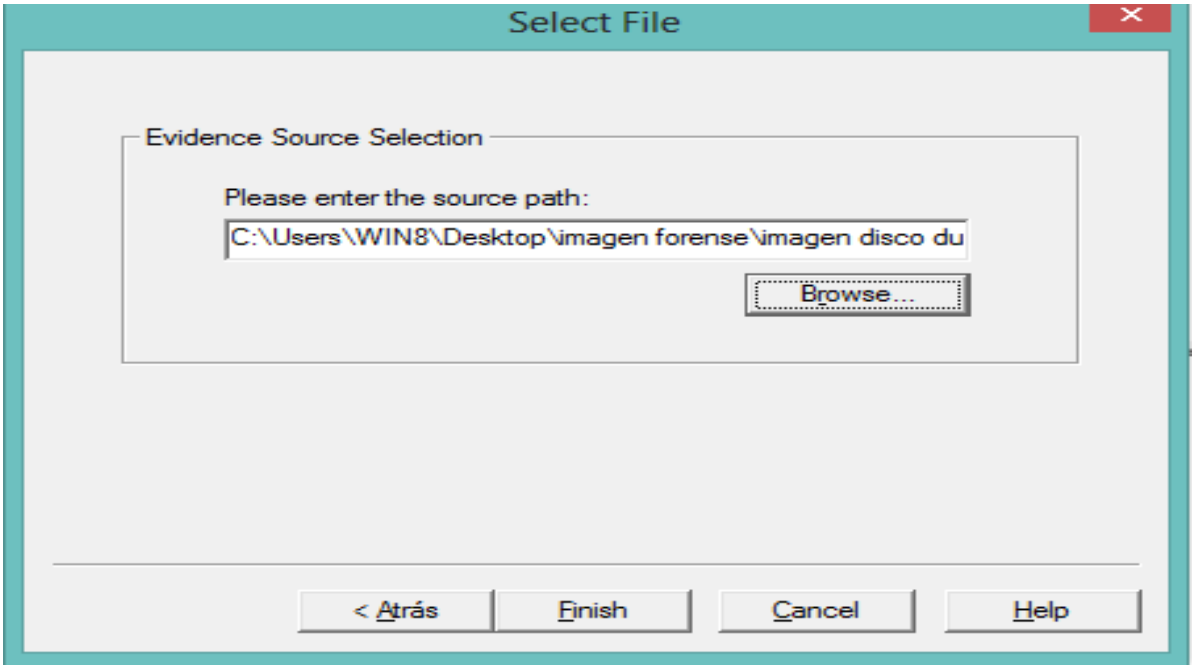

Figura 30. Selección de archivo.

Fuente: Elaboración propia.

Una vez montada correctamente la imagen forense, se procede al análisis del contenido de la misma, para comenzar a analizar basta con dar clic sobre el icono + que se encuentra a lado de la imagen forense.

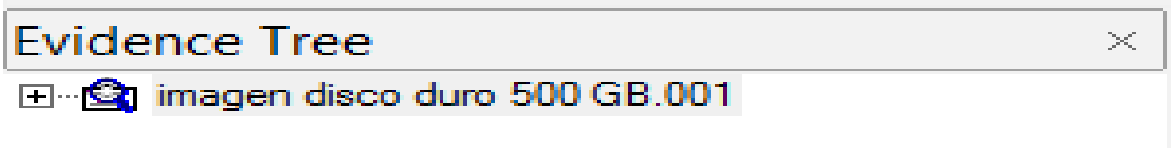

Figura 31. Imagen montada.

Fuente: Elaboración propia.

Regularmente la información de los discos duros internos se guarda dentro de la carpeta llamada root, sin embargo, no todos los discos duros tienen la misma estructura lógica, por lo que lo más recomendable es explorar en general el disco duro, esto ya dependerá de cada caso.

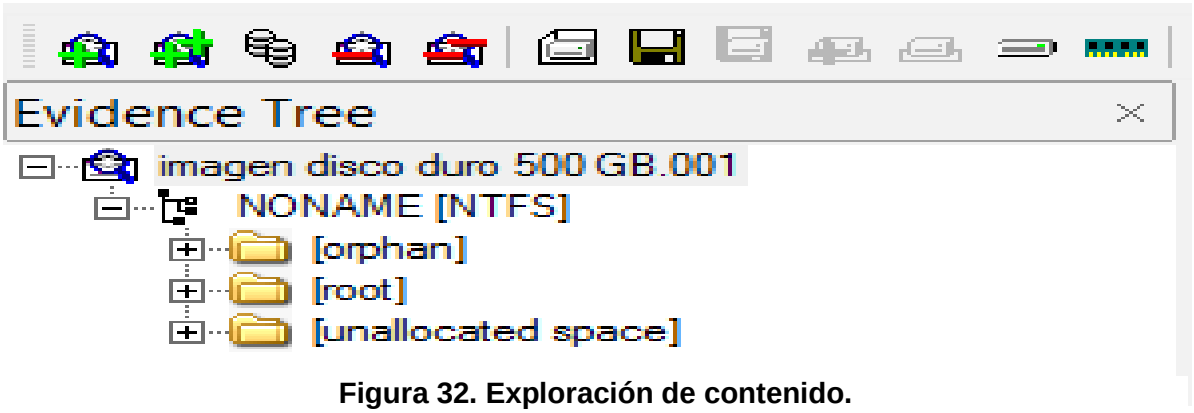

Figura 32. Exploración de contenido.

Fuente: Elaboración propia.

Al analizar el contenido y saber en dónde se encuentra la información que se necesita recuperar hay que dar un clic sobre el archivo o carpeta a recuperar.

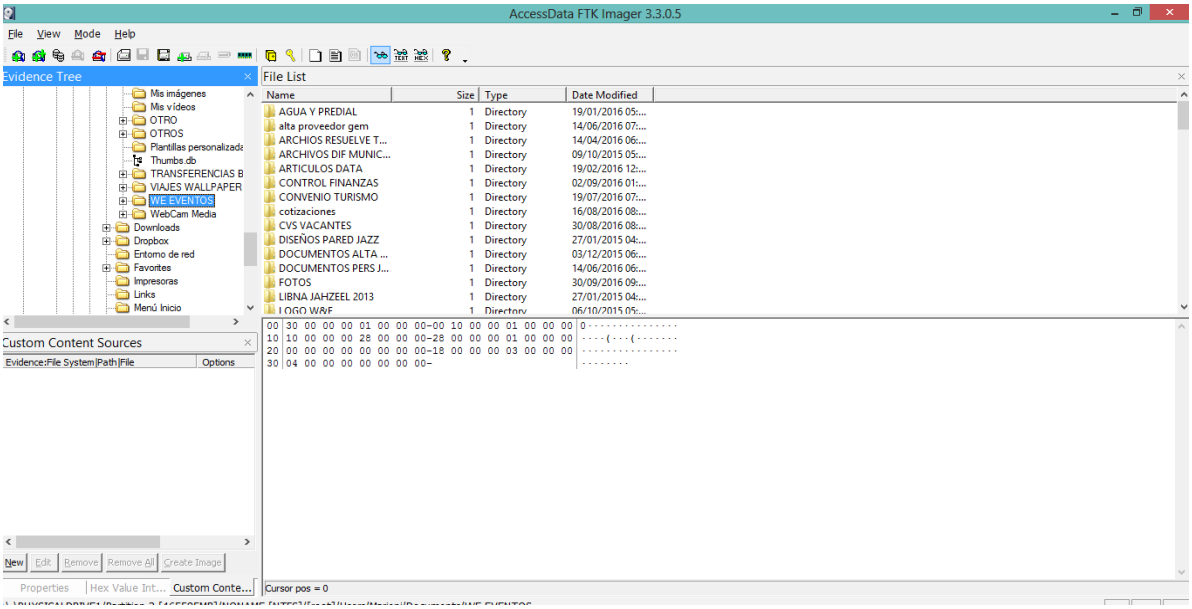

Figura 33. Exploración de carpetas.

Fuente: Elaboración propia.

Al dar clic en los archivos o carpetas se muestra la información contenida de manera codificada, así mismo los sectores y direcciones en hexadecimal.

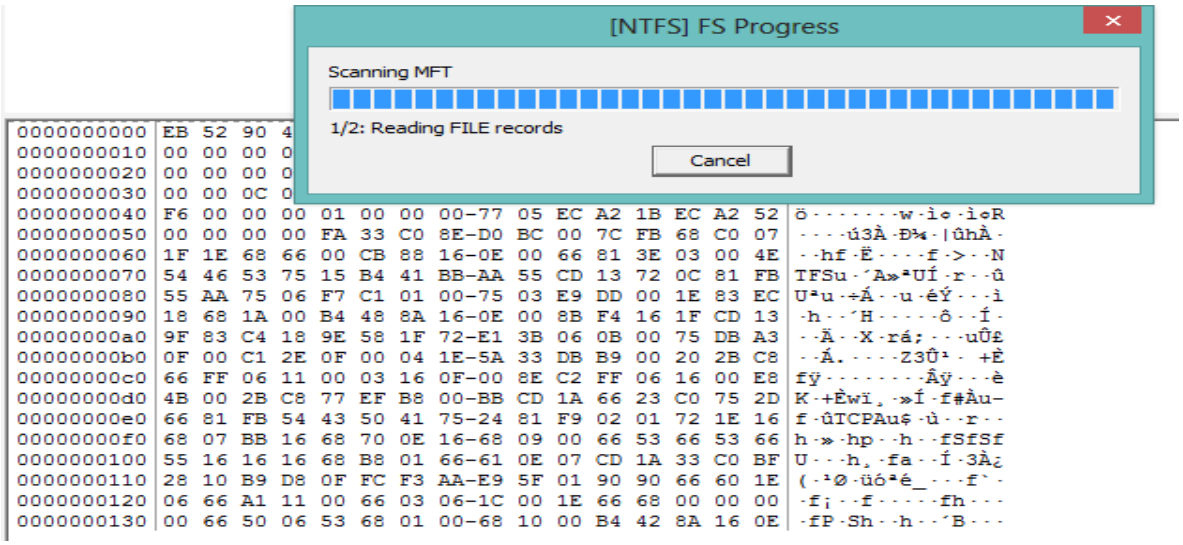

Figura 34. Información encriptada.

Fuente: Elaboración propia.

Una vez que se ha identificado la información a recuperar, basta con un clic izquierdo sobre el archivo y dar clic en la opción Export Files.

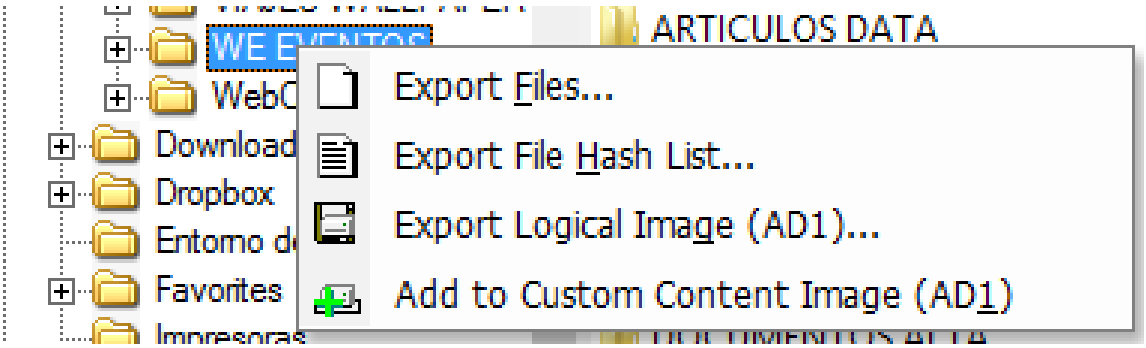

Figura 35. Exportación de archivos.

Fuente: Elaboración propia.

En seguida se debe elegir el destino en donde se exportará la información y se da clic en el botón aceptar.

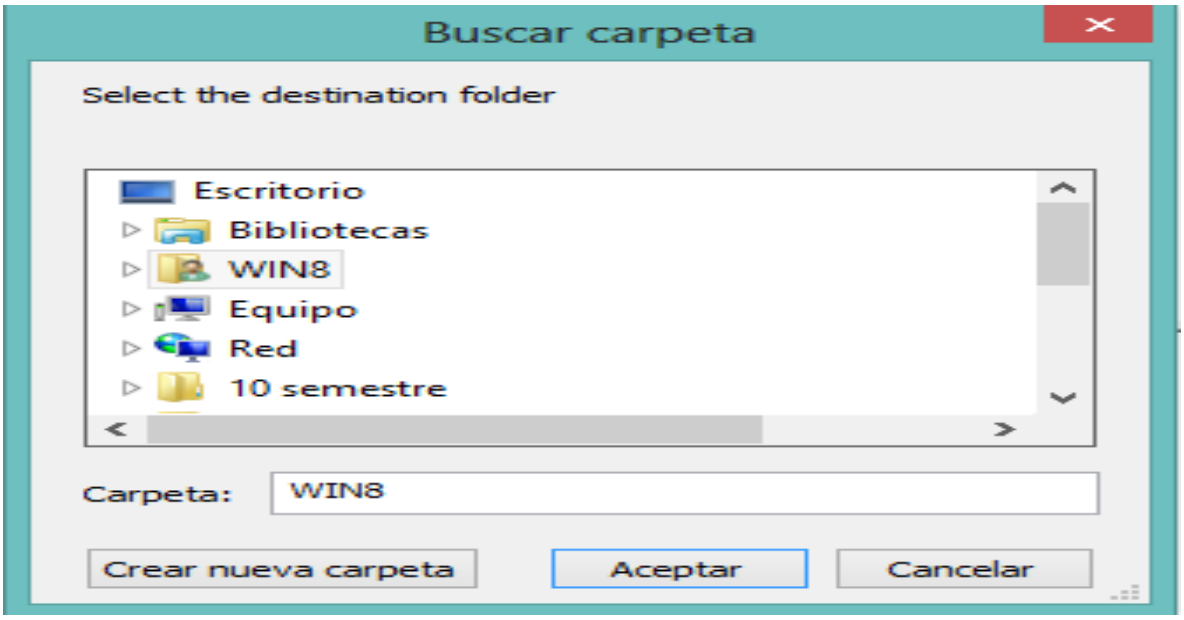

Figura 36. Folder de destino de la exportación.

Fuente: Elaboración propia.

Al dar clic en el botón aceptar se abrirá una ventana con el progreso de la exportación de la información solicitada, una vez realizado esto hay que esperar a que termine el proceso de recuperación. Al finalizar se podrá verificar la información recuperada en la ubicación en la que se exporto.

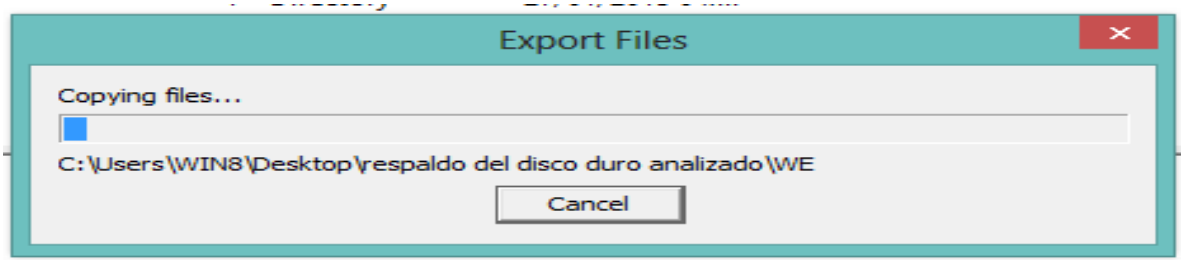

Figura 37. Estado de la exportación de archivos.

Fuente: Elaboración propia.

4.2.4. Reporte

Al finalizar se debe realizar un reporte, es muy importante realizarlo ya que contiene la descripción y conclusiones retomadas a lo largo del proceso realizado. El reporte debe ser muy detallado sobre los tiempos, si hubo problemas con algo durante el proceso, si se pudieron resolver dichos problemas, si fue exitosa la recuperación, sobre cuanta información fue recuperada, todo esto con base en lo descrito en la etapa de identificación, debe contener recomendaciones. En general debe contener una descripción sobre qué es lo que se realizó durante el proceso de principio a fin, todo debe estar en el archivo en donde se fue documentando todo lo realizado anteriormente ya que es parte de la evidencia.

4.3. Proceso para recuperar información sin validez legal (Proceso 2).

Para el caso dos el objetivo únicamente es recuperar información sin importar que el proceso no tenga efecto legal. Se utilizarán dos etapas durante el proceso las cuales son identificación y análisis.

4.3.1. Identificación.

Se debe conocer la capacidad del disco duro, y si es posible la capacidad de la información que se desea recuperar, todo esto con el fin de preparar un dispositivo de igual o mayor capacidad para almacenar la información a recuperar.

4.3.2. Análisis.

Lo siguiente es el análisis del disco duro físico, entonces lo que se debe hacer es montar el disco duro a la herramienta que se está utilizando.

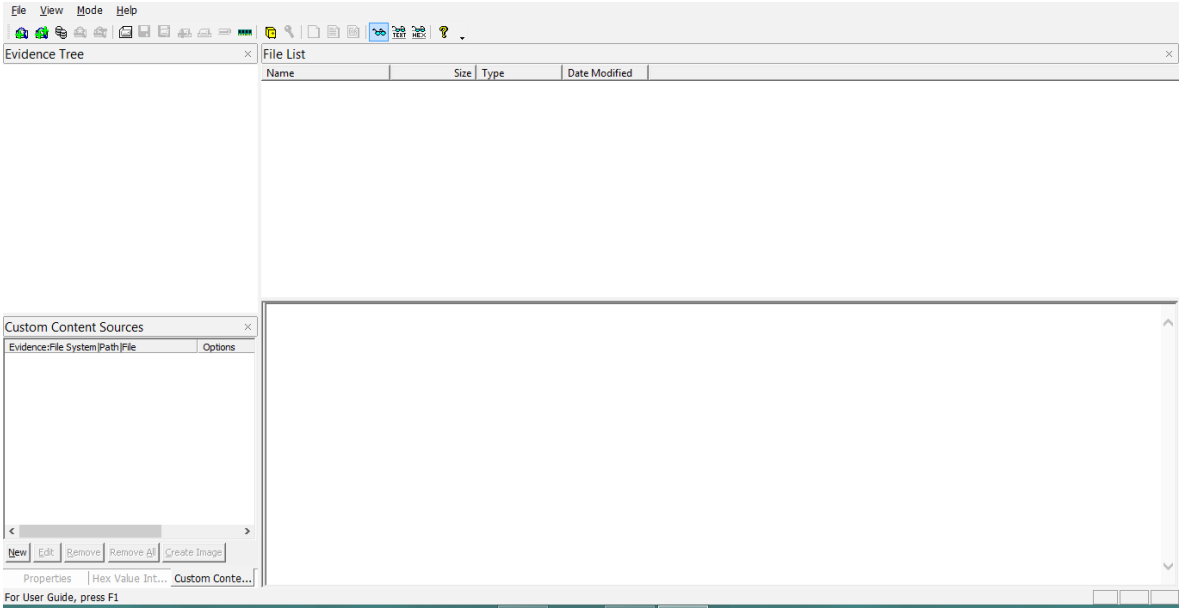

Figura 38. Pantalla principal FTK Imager.

Fuente: Elaboración propia.

Para realizar el montaje se da clic en la pestaña File y en seguida en la opción Add Evidence Item.

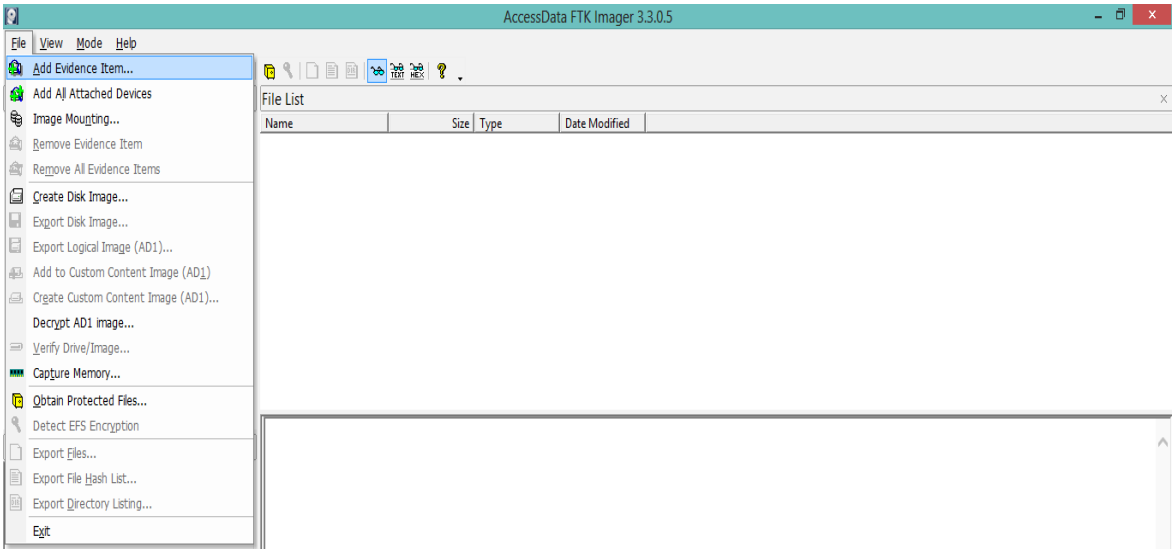

Figura 39. Selección de opción Add Evidence Item.

Fuente: Elaboración propia.

En seguida se elige el tipo de evidencia a agregar y se da clic en el botón siguiente, así que se seleccionará la opción Physical Drive ya que se trabajará con el disco duro físico.

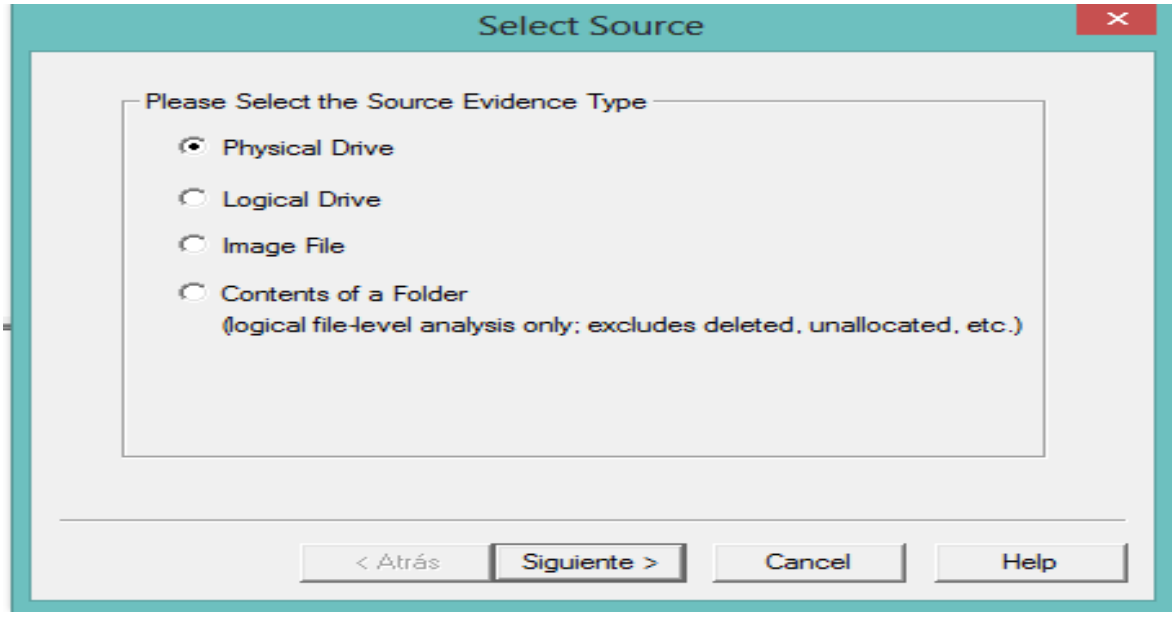

Figura 40. Pantalla para seleccionar el tipo de evidencia.

Fuente: Elaboración propia.

En seguida se debe seleccionar la ubicación de donde se encuentra el disco duro y dar clic en el botón finish.

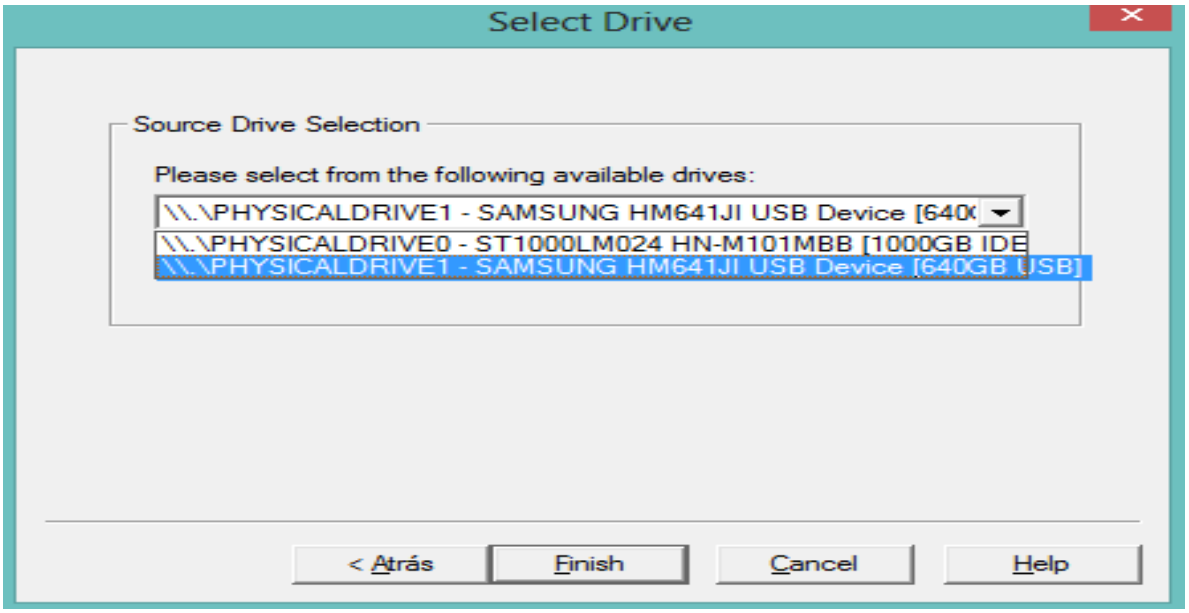

Figura 41. Pantalla de ubicación de dispositivo a analizar.

Fuente: Elaboración propia.

Una vez montado correctamente el disco duro, se procede al análisis del contenido del mismo, para comenzar a analizar basta con dar clic sobre el icono + que se encuentra a lado del disco duro montado.

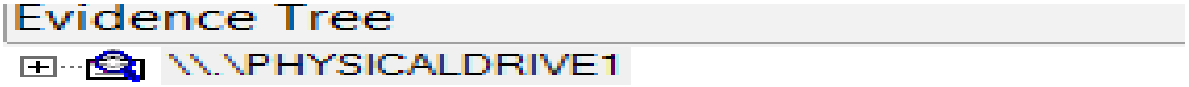

Figura 42. Montaje de disco duro.

Fuente: Elaboración propia.

Regularmente la información de los discos duros se guarda dentro de la carpeta llamada root, sin embargo, no todos los discos duros tienen la misma estructura lógica, por lo que lo más recomendable es explorar en general el disco duro, esto ya dependerá de cada caso.

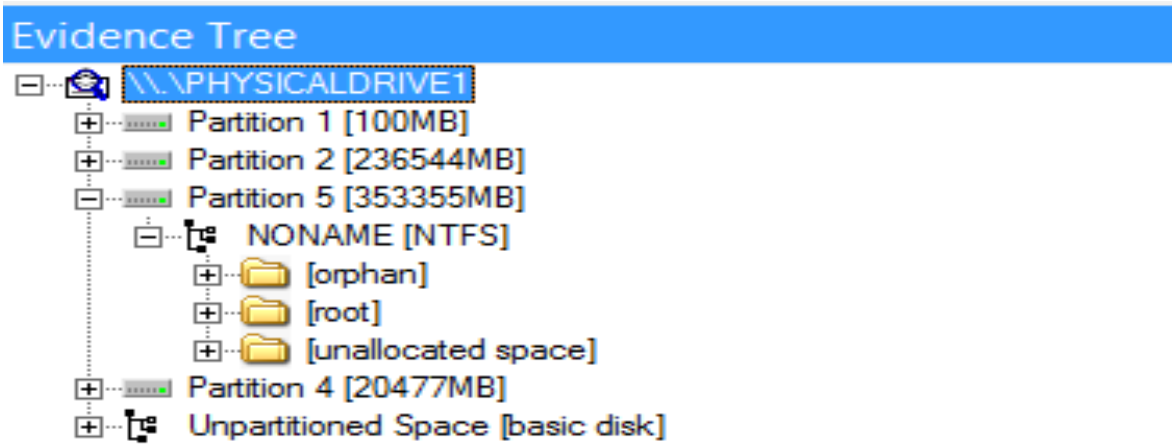

Figura 43. Árbol de evidencia.

Fuente: Elaboración propia.

Al analizar el contenido y saber en dónde se encuentra la información que se necesita recuperar hay que dar un clic sobre el archivo o carpeta a recuperar.

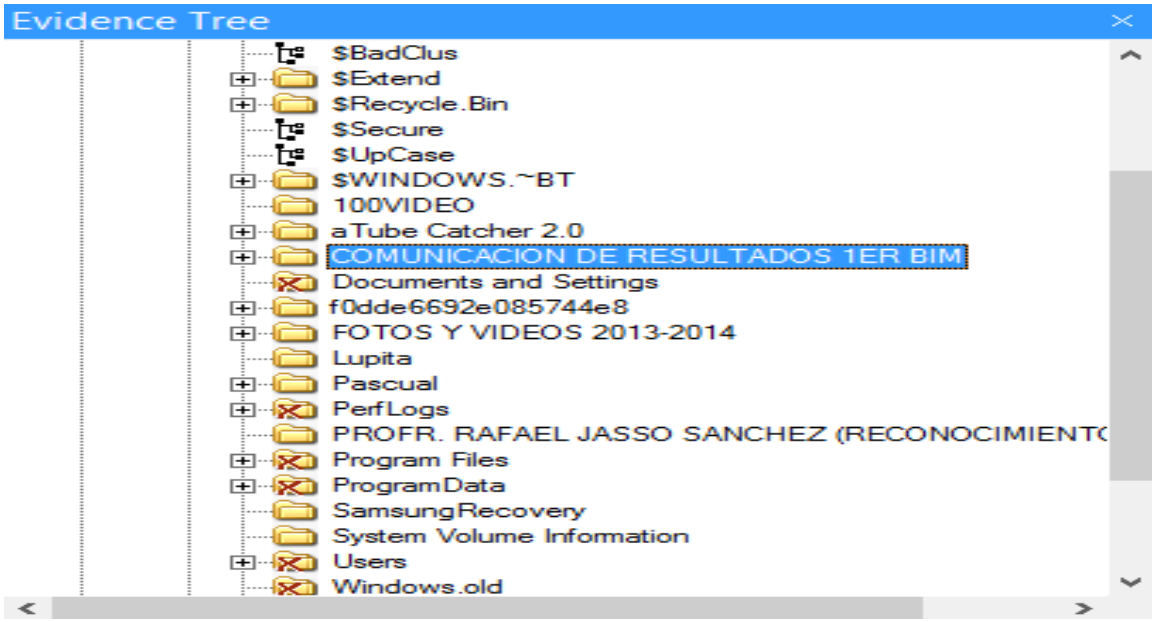

Figura 44. Información contenida.

Fuente: Elaboración propia.

Al dar clic en los archivos o carpetas se muestra la información contenida de manera codificada, así mismo los sectores y direcciones en hexadecimal.

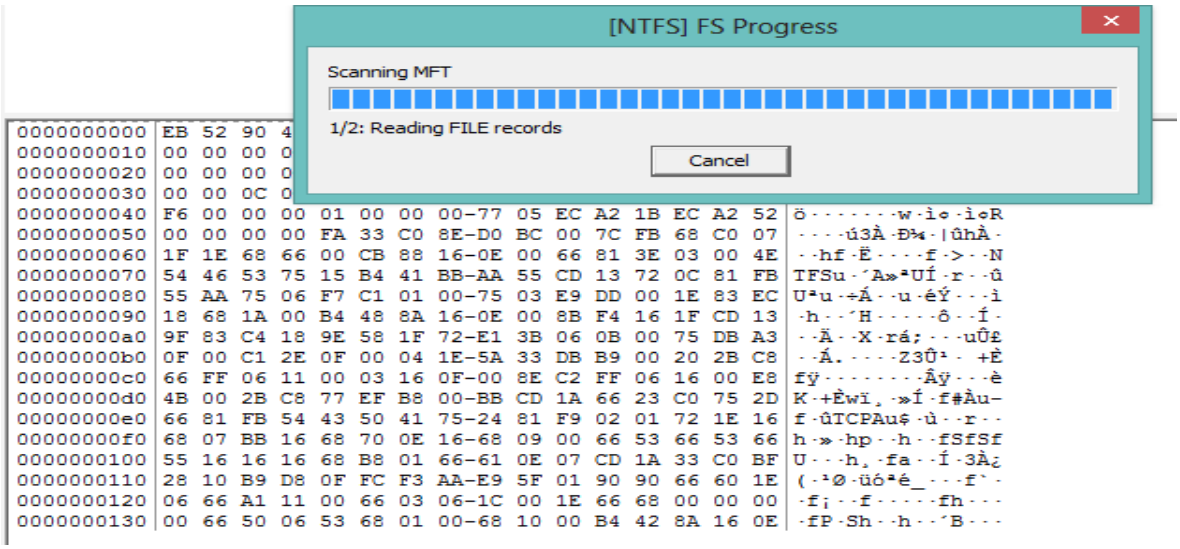

Figura 45. Información mostrada de manera codificada.

Fuente: Elaboración propia.

Una vez que se ha identificado la información a recuperar, basta con un clic izquierdo sobre el archivo y dar clic en la opción Export Files.

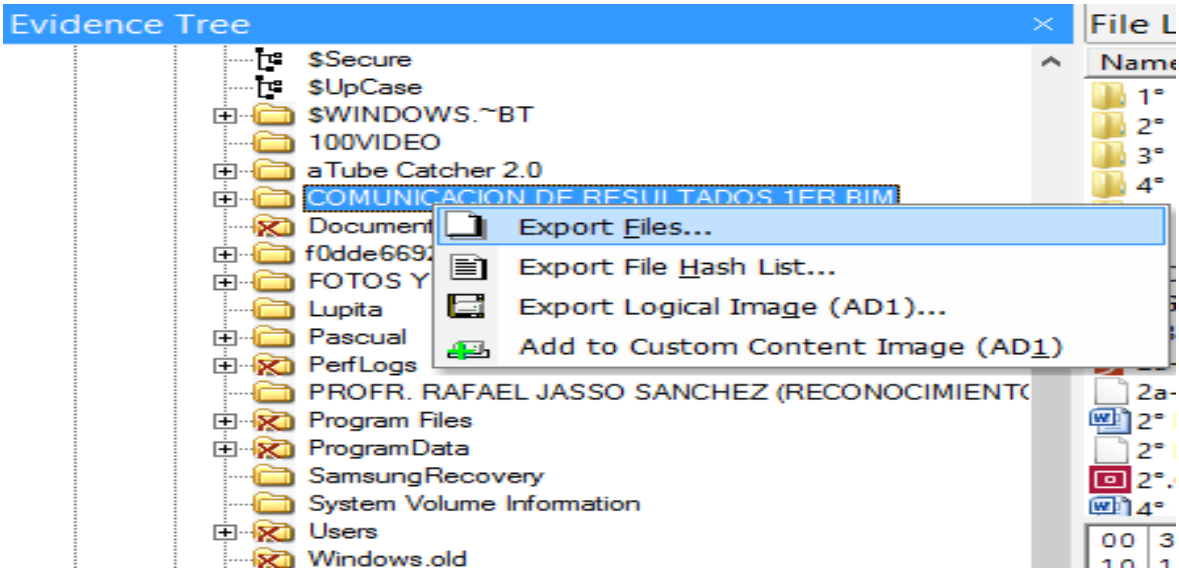

Figura 46. Opción de exportar información encontrada.

Fuente: Elaboración propia.

En seguida se debe elegir el destino en donde se exportará la información y se da clic en el botón aceptar.

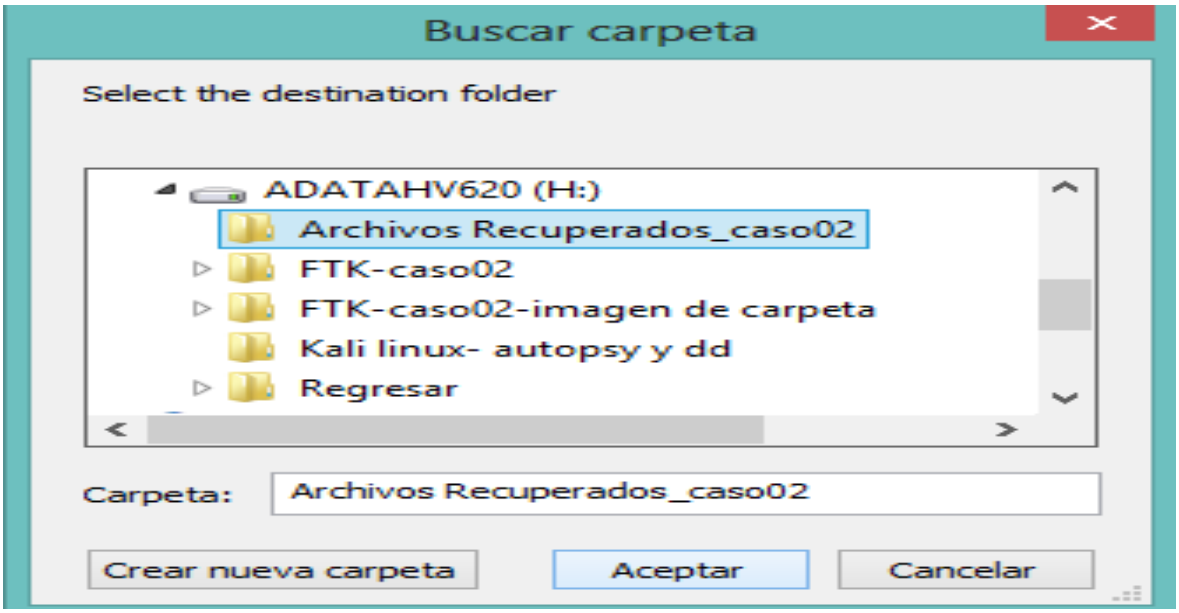

Figura 47. Destino de exportación de información.

Fuente: Elaboración propia.

Al dar clic en el botón aceptar se abrirá una ventana con el progreso de la exportación de la información solicitada.

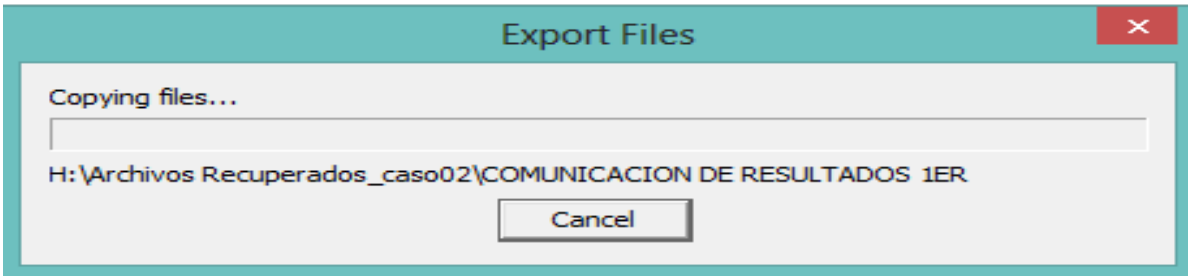

Figura 48. Barra de estado de progreso de exportación de información.

Fuente: Elaboración propia.

Al finalizar el proceso, se abrirá una nueva ventana con los resultados obtenidos de la exportación. Por último, se dará clic en el botón aceptar y se puede checar la información recuperada en la ubicación en la que se exporto. Para concluir se debe incluir dentro de esta etapa un reporte de manera general de lo obtenido durante la investigación.

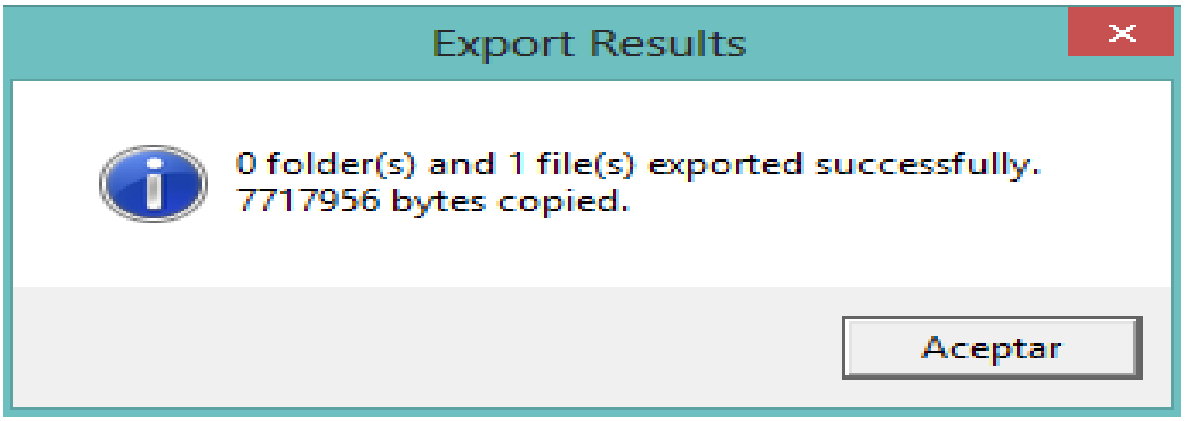

Figura 49. Resultados de exportación.

Fuente: Elaboración propia.

CAPÍTULO V

EXPERIMENTACIÓN Y CONCLUSIONES

En este capítulo se presenta la experimentación realizada con base en el proceso que se debe llevar a cabo según el manual propuesto en el capítulo anterior. La experimentación fue realizada planteando dos casos, cada caso se realizó con un disco duro diferente, en ambos casos se requiere recuperar toda la información posible almacenada dentro de los discos duros dañados, ya que es considerada información de gran valor por las personas solicitantes. El primer disco duro se analizará siguiendo el primer caso propuesto en el manual del capítulo anterior, el segundo disco duro se analizará siguiendo el segundo caso propuesto en el manual del capítulo anterior.

Los discos duros presentan daños graves, anterior a eso los solicitantes comentan que intentaron recuperar información de manera normal sin tener éxito en la tarea realizada. Por tal motivo se espera que aplicando el manual basado en cómputo forense se obtengan buenos resultados.

5.1. Experimentación 01

5.1.1. Identificación

Se recibió un disco duro el día 29 de septiembre del 2016, la problemática que presenta es que el disco duro es parte de una computadora portátil que sufrió perdida de información, al sufrir un golpe al caerse el portátil, el disco duro contiene información de gran valor para el usuario, lo principal que se necesita recuperar es una carpeta llamada "*we eventos"* con todo su contenido, en seguida todas las fotos ya que tienen un valor que va más allá de personal. La carpeta llamada *"we eventos"* se encuentra dentro del usuario *"Marieni"* en el apartado de documentos, las fotos se encuentran dentro del mismo usuario en el apartado de imágenes, de igual manera se mencionó que si era posible recuperar toda la información se hiciera de esa manera.

Características de disco duro a analizar:

El disco a analizar es un disco duro de 500 GB modelo WD5000BEVT55A0RT0
WD Scorpio Blue
El código de barras WXC1AB0Y5546
WWN: 50014EE6AB5D95B0
DATE: 30 NOV 2010
DCM: HBNTJHB
DCX: YA040B4R5
U.S. Patents 6178056, 5956196, 6289484, 6263459
Product of Malaysia
Canadá ICES-003 Class B/
NMB-003B Class B
LBA: 976773168
5VDC: 0.55A
R/N: 771672

Figura 50. Disco duro a analizar 1.

Fuente: Elaboración propia.

Se conectó el disco duro a la computadora por medio de un cable SATA/IDE-usb que contiene un cable adaptador SATA/IDE-usb 2.0 un cable sata y una fuente o regulador.

Ya conectado mostraba un mensaje de que había problema con la unidad.

Figura 51. Problema con disco duro a analizar 1.

Fuente: Elaboración propia.

Al entrar en la unidad en la carpeta users mostraba las siguientes carpetas que representan los diferentes usuarios que se contienen en el disco duro, se ubicó la carpeta que corresponde al usuario *Marieni*.

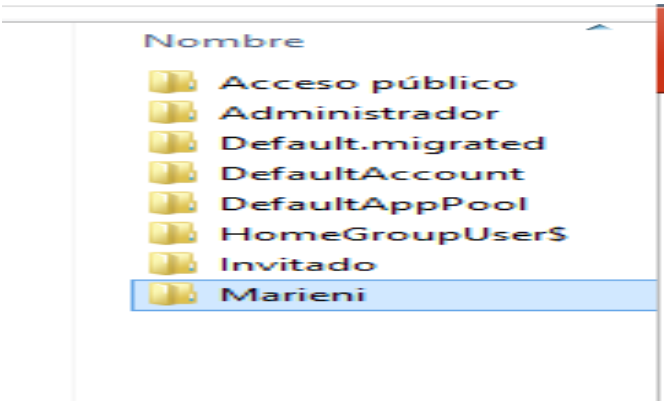

Figura 52. Carpetas contenidas de disco duro 1.

Fuente: Elaboración propia.

Al intentar accesar al contenido de la carpeta *Marieni*, se mostraba una advertencia.

Figura 53. Carpetas contenidas en disco duro 1.

Fuente: Elaboración propia.

Al cerrar la ventana de advertencia de virus se abrió la carpeta que corresponde al usuario *Marieni* no mostrando información ya que la carpeta contenía permisos especiales de usuario.

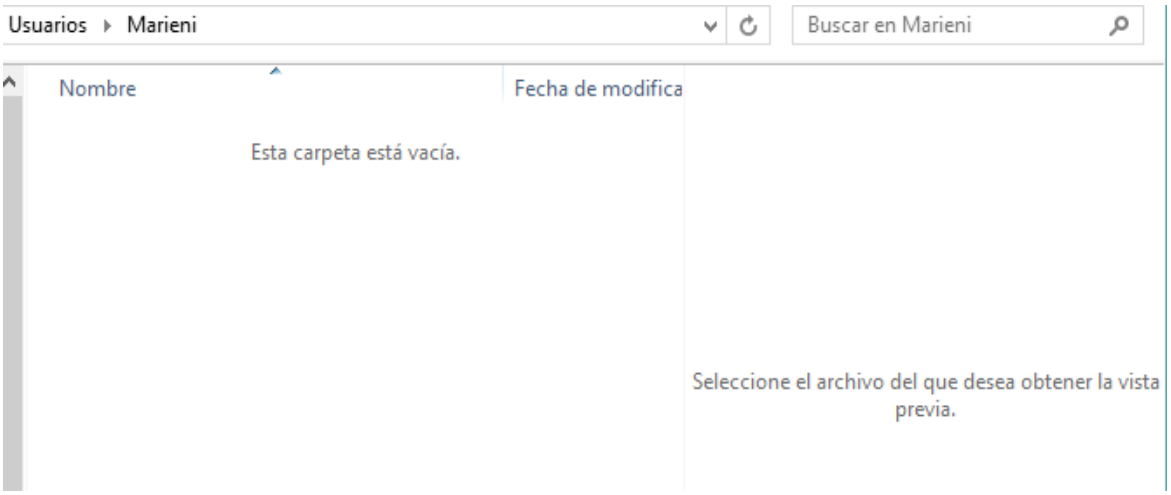

Figura 54. Contenido de carpeta Marieni.

Fuente: Elaboración propia.

5.1.2. Preservación

Para crear la imagen forense se dio clic en la pestaña File, en seguida se abrió un menú y se le dio clic en la opción Create Disk Image.

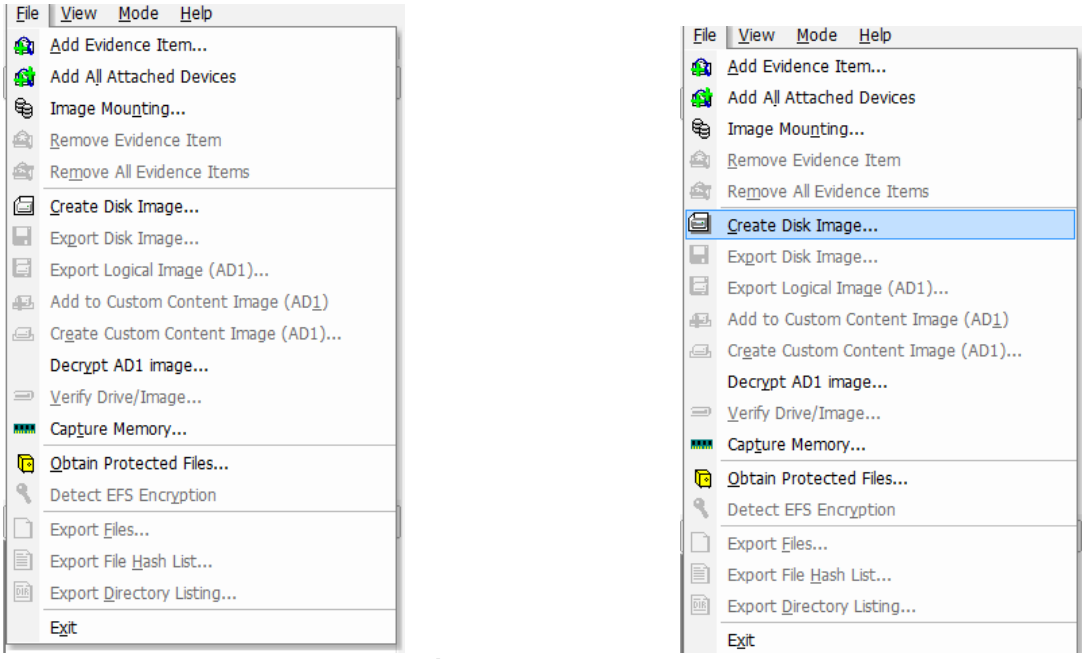

Figura 55. Creación de imagen forense de disco duro 1.

Fuente: Elaboración propia.

Apareció una venta en la cual se seleccionó la opción Logical Drive ya que se desea realizar la imagen forense a partir de una partición del disco duro que se encuentra conectado.

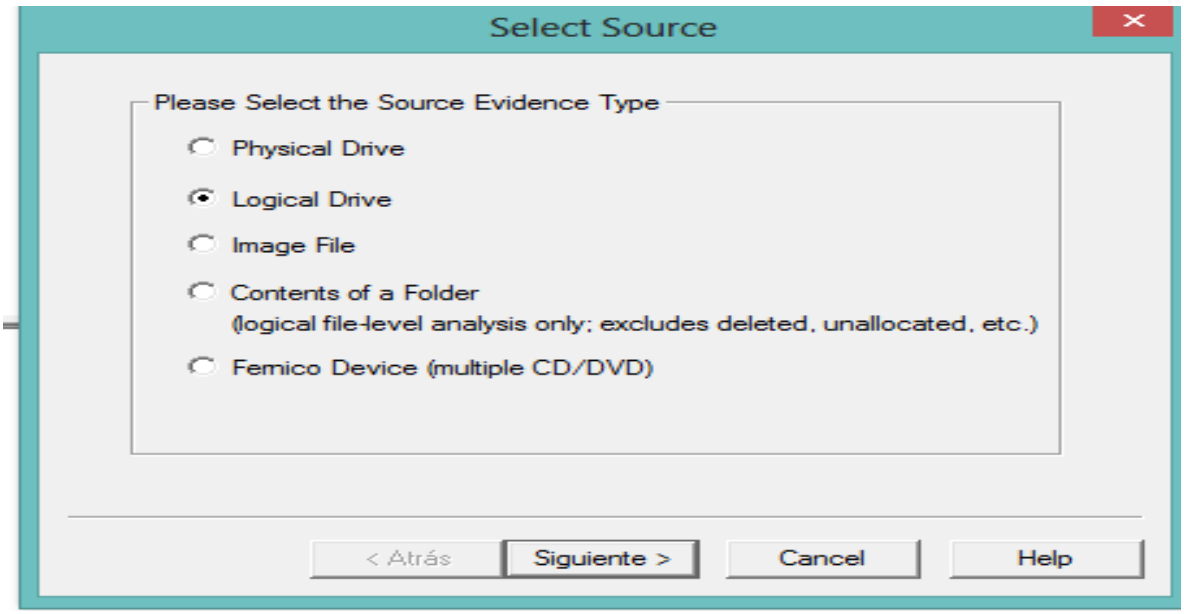

Figura 56. Selección de fuente de donde se realizará la imagen forense.

Fuente: Elaboración propia.

La unidad lógica de la cual se hará la imagen forense es de la unidad de disco local F, se especificó el disco local F ya que el disco duro contiene dos unidades lógicas una es la llamada System Reserved (E:) y la otra es el Disco local (F:) en la cual se encuentra la información que se desea recuperar.

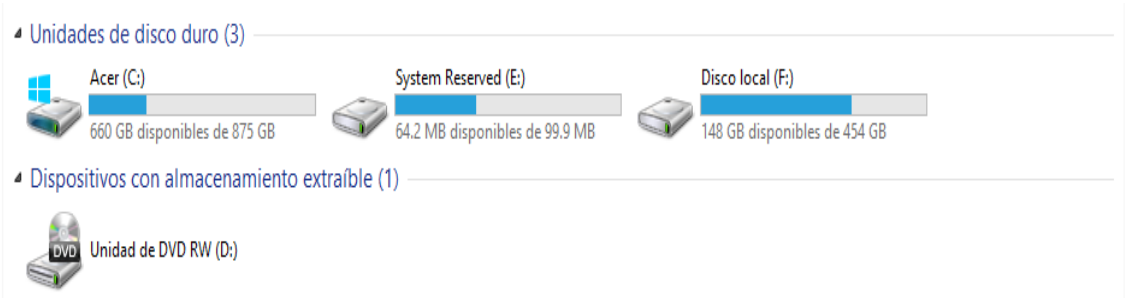

Figura 57. Unidad F, unidad en la que se sabe se encuentra la información.

Fuente: Elaboración propia.

Se seleccionó la unida F:\ que tiene un formato NTFS y se dio click en Finish.

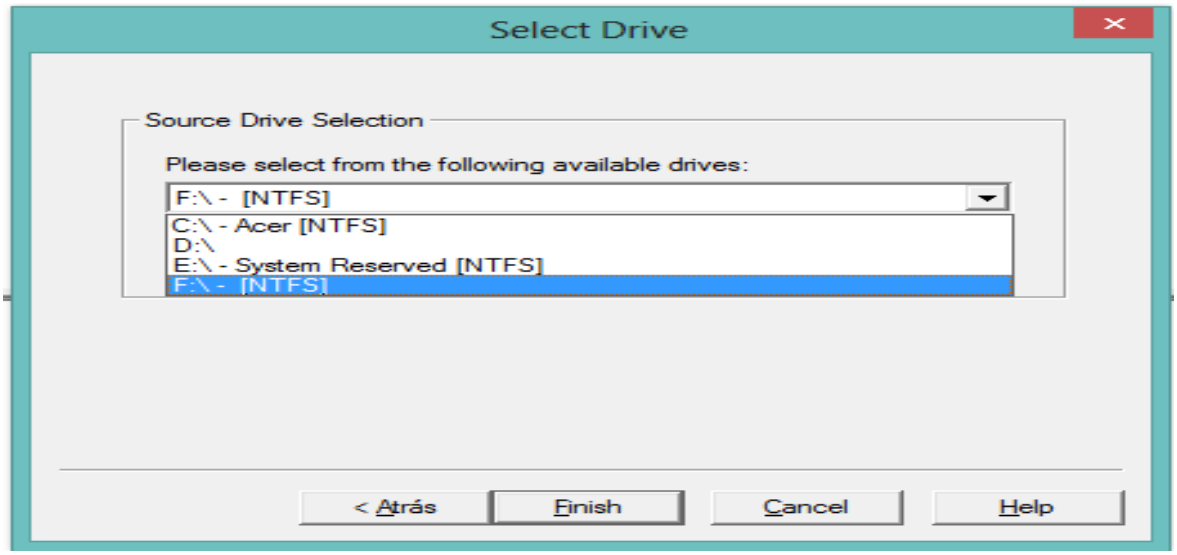

Figura 58. Selección de unidad.

Fuente: Elaboración propia.

Mostro una pantalla en la cual se seleccionó únicamente la casilla que corresponde a la opción Verify Images after they are created, para que una vez finalizado el proceso de creación de imagen inmediatamente verifique el hash de la imagen creada con el hash del disco duro, en seguida se dio clic en el botón Add.

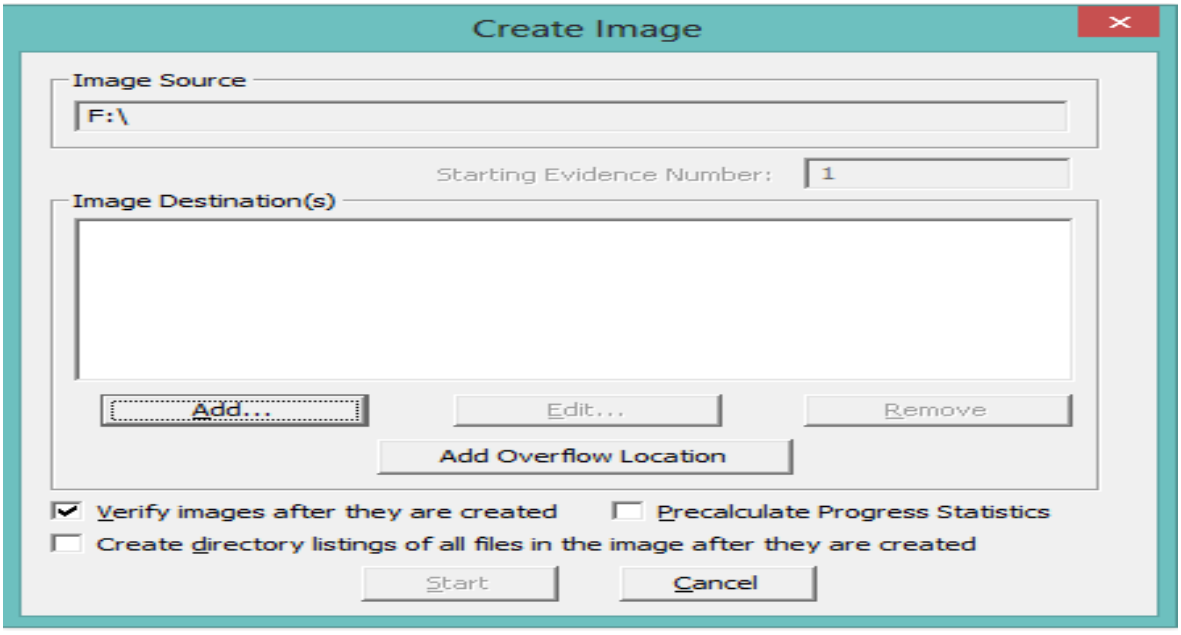

Figura 59. Pantalla a llenar para la creación de la imagen forense del disco duro 1.

Fuente: Elaboración propia.

Al dar clic en el botón Add se abrió una ventana en la cual se eligió el formato que se le dio a la imagen que se desea crear, se seleccionó la opción Raw(dd).

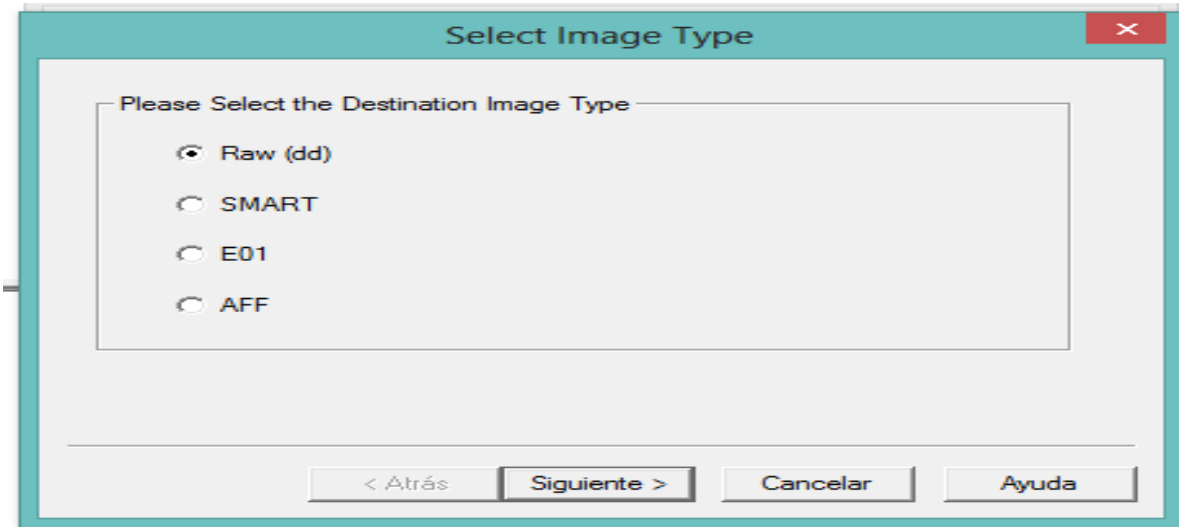

Figura 60. Selección del tipo de imagen forense.

Fuente: Elaboración propia.

Se abrió una ventana nueva en la cual se agregó la información relacionada con la imagen, tal como: número de caso, número de evidencia, descripción del caso y nombre del examinador, se llenaron los campos y se dio clic en el botón siguiente.

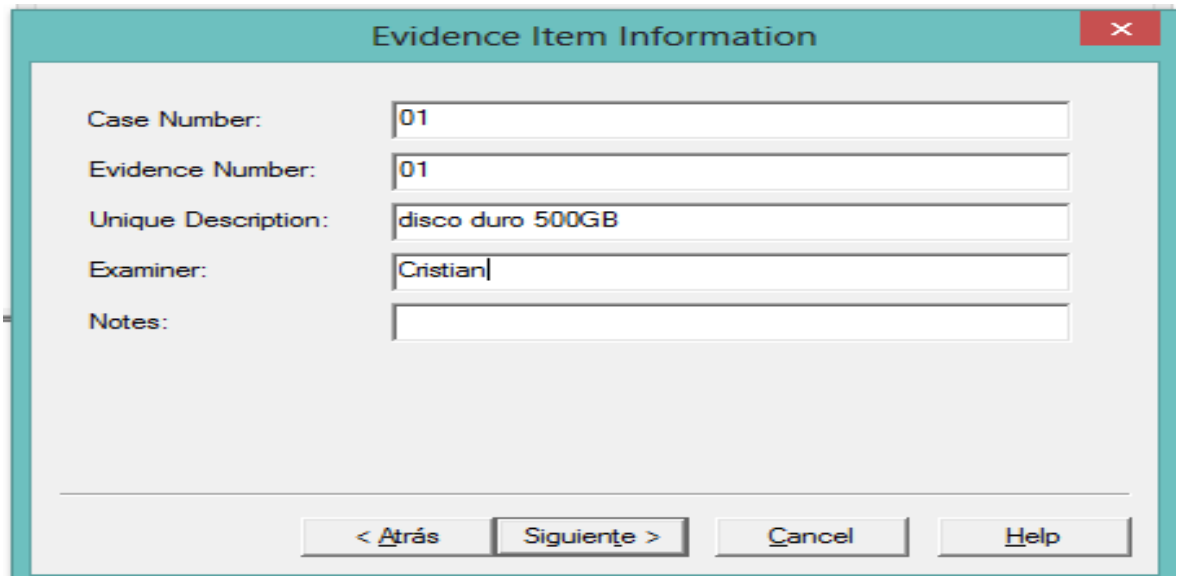

Figura 61. Información de la evidencia.

Fuente: Elaboración propia.

Se abrió una ventana en la cual se asignó la carpeta de destino de la imagen, en seguida se le asignó un nombre a la imagen próxima a crear y se dio clic en el botón finish.

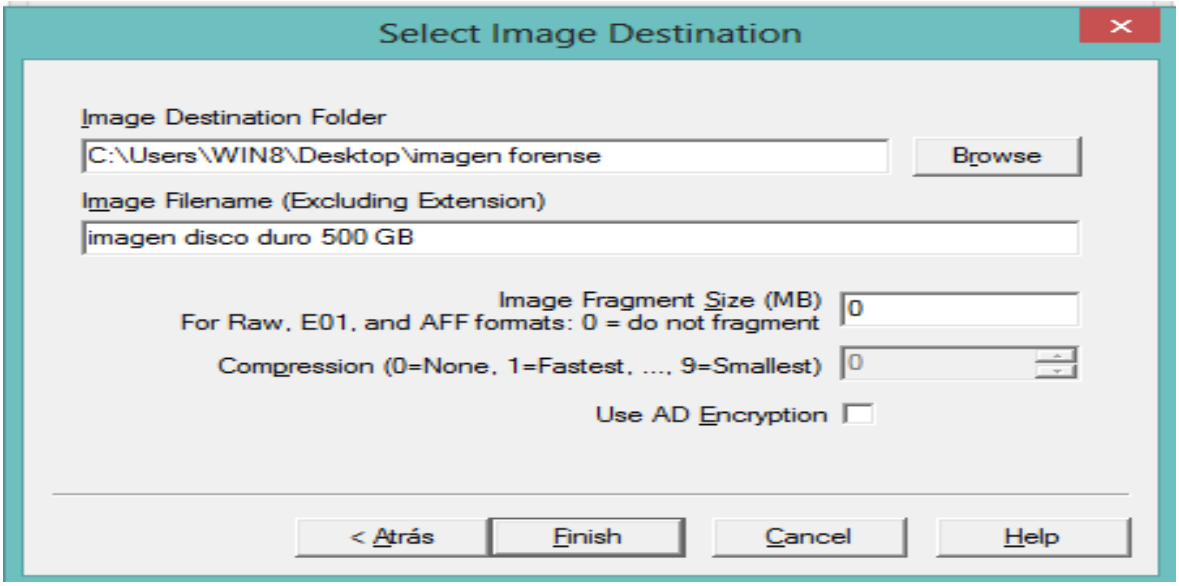

Figura 62. Destino en donde se almacenará la imagen forense a crear.

Fuente: Elaboración propia.

Al concluir lo anterior automáticamente regreso a la ventana que lleva por nombre Create Image y se dio clic en el botón Start.

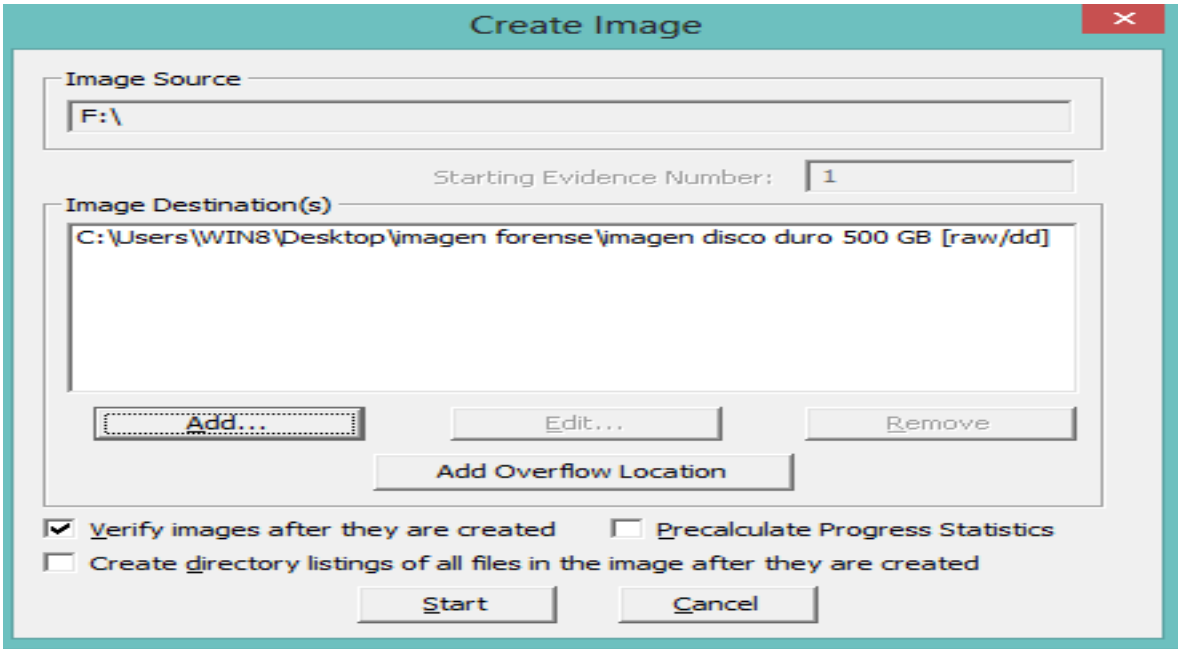

Figura 63. Pantalla lista para la creación de la imagen forense.

Fuente: Elaboración propia.

Se comenzó a crear la imagen y se esperó a que terminara el proceso, el cual tuvo una duración de 7 horas con 22 minutos y 2 segundos.

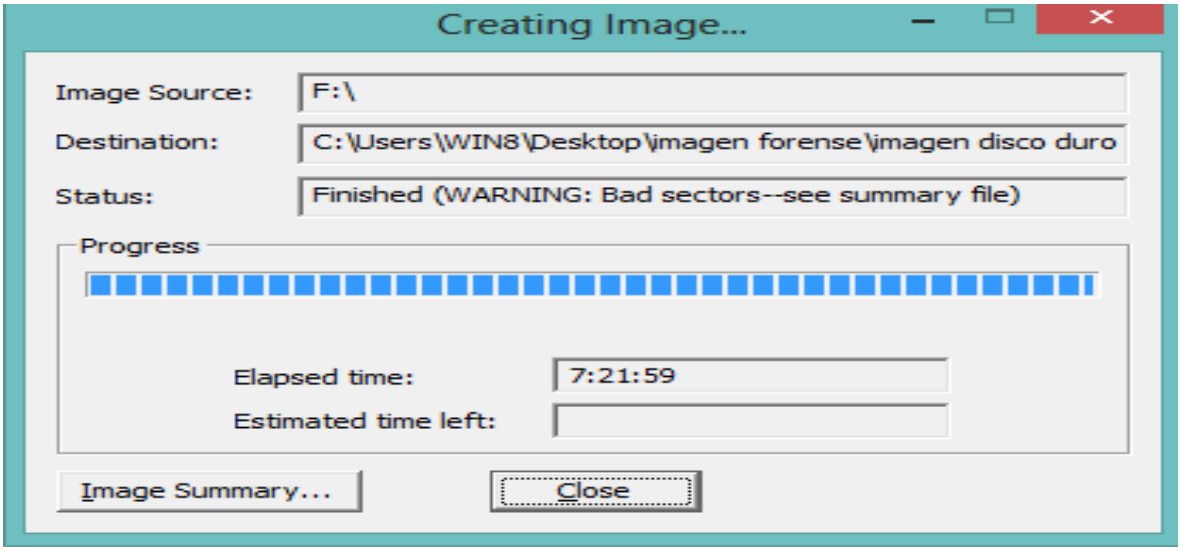

Figura 64. Status de avance de la creación de la imagen forense.

Fuente: Elaboración propia.

En cuanto termino la creación de la imagen se abrió una ventana en la cual automáticamente comenzó a realizar el proceso de verificación de la imagen creada con la unidad lógica de la cual se realizó la imagen forense, la duración del proceso de verificación fue de 1 hora con 59 minutos y 2 segundos.

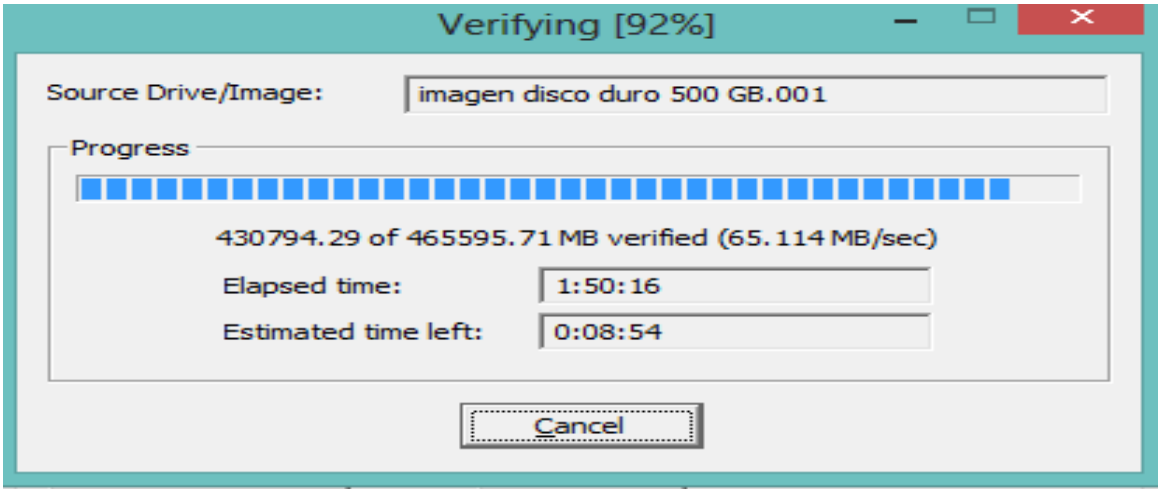

Figura 65. Verificación de la imagen forense creada.

Fuente: Elaboración propia.

Al finalizar el proceso de verificación muestro una ventana con los resultados del proceso de la creación, la cual muestra el nombre de la imagen, un conteo de los sectores copiados, reporte del algoritmo MD5 Hash el cual contiene una comparación y un resultado entre el hash calculado y el hash reportado, de igual manera la comprobación del hash calculado y el hash reportado del algoritmo SHA1 Hash, el resultado de los dos algoritmos fue bueno al realizar la verificación arrojo como iguales las cadenas concluyendo que la integridad de los datos es la adecuada, y por ultimo mostro el apartado de sectores dañados.

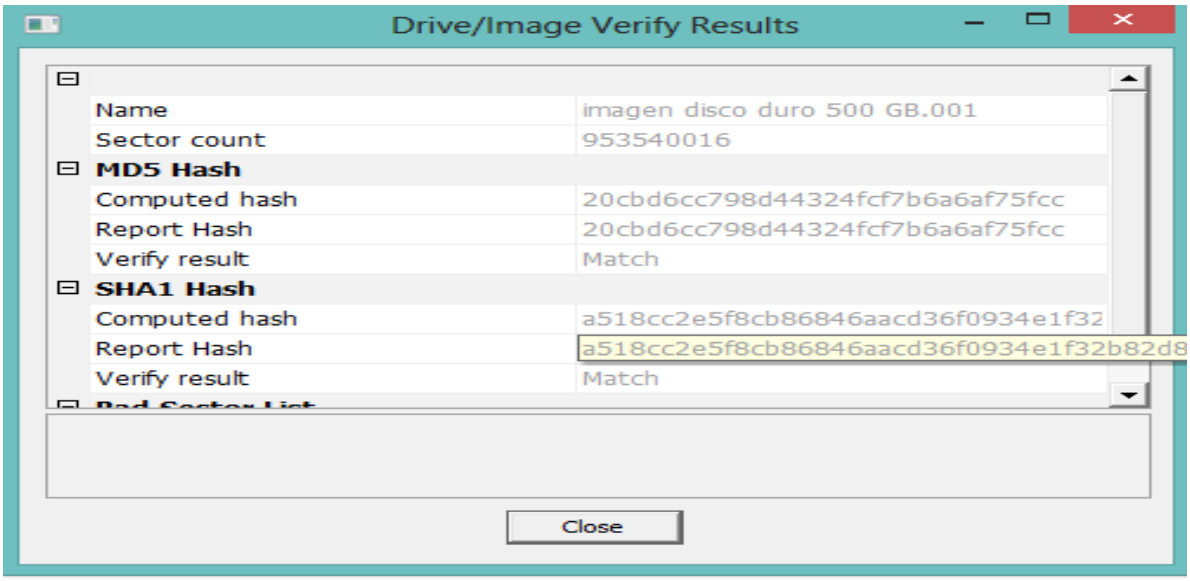

Figura 66. Resultados de la verificación de la imagen forense.

Fuente: Elaboración propia.

Al revisar la carpeta de destino se encontraron dos archivos, uno de tipo WinZipper y otro de tipo .txt, la imagen creada es la de tipo WinZipper, la de tipo txt es un reporte del proceso de la creación de la imagen y la verificación de la misma

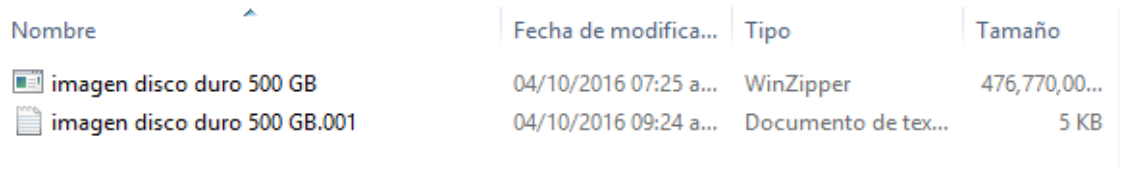

Figura 67. Archivos generados después de finalizar la creación y verificación de la imagen forense.

Fuente: Elaboración propia.

El reporte cuenta con información acerca del caso del que llevo la creación de la imagen

```
Created By AccessData® FTK® Imager 3.3.0.5

Case Information:
Acquired using: ADI3.3.0.5
Case Number: 01
Evidence Number: 01
Unique description: disco duro 500GB
Examiner: Cristian
Notes:

---------------------------------------------------------------
```

Figura 68. Reporte del proceso de creación de la imagen forense, datos del caso analizado.

Fuente: Elaboración propia.

Información relacionada con el disco duro del cual se creó la imagen forense tal como: carpeta de destino de la imagen forense, recuento de sectores, si se hizo de una unidad removible, el tipo de fuente, etc.

```
Information for C:\Users\WIN8\Desktop\imagen forense\imagen disco duro 500 GB:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Logical
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 953,540,016
[Physical Drive Information]
 Removable drive: False
 Source data size: 465595 MB
 Sector count:    953540016
```

Figura 69. Reporte del proceso de creación de la imagen forense, datos del disco duro.

Fuente: Elaboración propia.

Los sectores de la unidad lógica que no podían ser leídos

```
ATTENTION:
The following sector(s) on the source drive could not be read:
        601576396
        717013268
        796353341
        808295283
        821727424
        835702652
        838290563
        850395836
        863129198
        865023818
        865030483
        865036994
        865172627
        865690523
        866384966
        866496515
        867109207
        867791355
        868324357
        868355204
        868394886
        868451000
        868979381
        868985896
        869766575
        870278334
        871002589
        871565547
        871616793
        871617823
        871623125
        871710008
        872213604
        872993376
        872993376
        874292122
        874805608
        874872586
        874892536
        874893567
        874895629
        874898722
        874902992
        874925964
        875485542
        875502330
        875506454
        875513816
        875547245
        876053983
        876086380
        876115685
        876661151
        876665275
        876666306
        876681032
        876685155
        876691488
        876698850
        876718730
        876723885
        876762615
        876776310
        876796142
        877333068
        877335277
        877338369
        877363551
        877364581
        877421129
        877442040
        877916138
        877934987
        877975778
        877982111
        878003021
        878004052
        878010384
        878014508
        878033357
        878043812
        878529492
        878532732
        878537886
        878554729
        878593458
        878607006
        878608036
        878613337
        878617461
        878631157
        878632187
        878636310
        878638520
        878639551
        878668855
        879168083
        879201658
        879207991
        879785707
        879792040
        879809858
        879810889
        879816191
        879821345
        879835040
        879839163
        879861105
        879863314
        879875830
        879884224
        879893649
        879894680
        879915592
        879920893
        880390815
        880398179
        880429545
        880436907
        880455756
        880462089
        880467243
        880468274
        880473576
        880478729
        880486093
        880488154
        880503911
        881073382
        881079714
        881080745
        881099594
        881100625
        881105779
        881127868
        881131991
        881133022
        881166597
        881637551
        881643883
        881661702
        881673188
```

Figura 70. Sectores dañados.

Fuente: Elaboración propia.

Los valores hash calculados

```
[Computed Hashes]
MD5 checksum:    20cbd6cc798d44324fcf7b6a6af75fcc
SHA1 checksum:   a518cc2e5f8cb86846aacd36f0934e1f32b82d8f
```

Figura 71. Valores hash calculados del disco duro.

Fuente: Elaboración propia.

Información de la hora en que comenzó la creación y la hora en la que finalizo, así como la ubicación.

```
Image Information:
 Acquisition started:   Tue Oct 04 00:03:16 2016
 Acquisition finished:  Tue Oct 04 07:25:14 2016
 Segment list:
  C:\Users\WIN8\Desktop\imagen forense\imagen disco duro 500 GB.001
```

Figura 72. Información de adquisición de la imagen forense.

Fuente: Elaboración propia.

La verificación de la imagen creada con la unidad de donde se realizó, conteniendo información de hora, tanto de inicio como fin de verificación, así mismo el hash MD5 y SHA1

```
Image Verification Results:
 Verification started:  Tue Oct 04 07:25:18 2016
 Verification finished: Tue Oct 04 09:24:16 2016
 MD5 checksum:    20cbd6cc798d44324fcf7b6a6af75fcc : verified
 SHA1 checksum:   a518cc2e5f8cb86846aacd36f0934e1f32b82d8f : verified
```

Figura 73. Valores hash calculados de la imagen forense.

Fuente: Elaboración propia.

5.1.3. Análisis

Obtenida la imagen y todos los datos relacionados lo que procedió fue hacer un análisis a la imagen creada.

Para cargar la imagen se abrió la herramienta FTK.

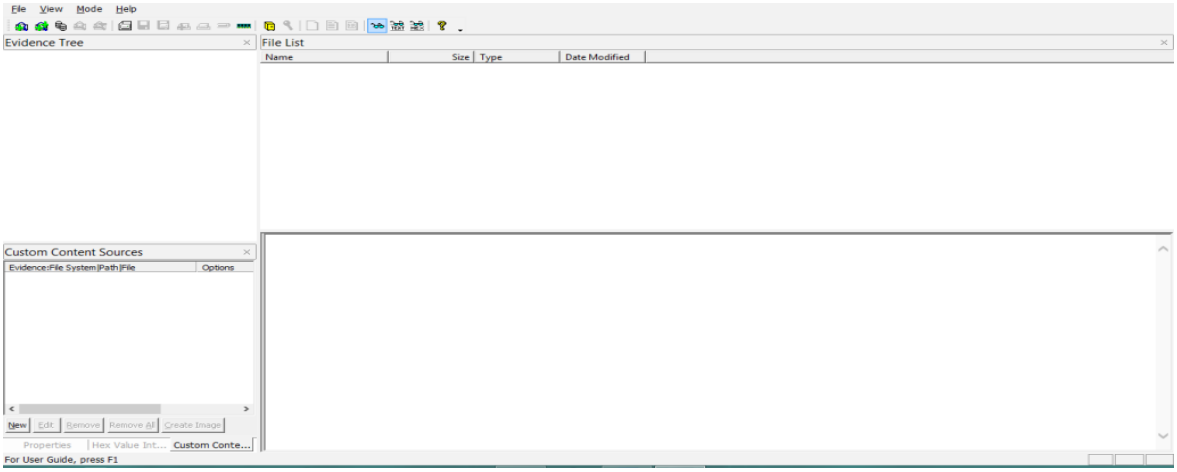

Figura 74. Pantalla principal de FTK.

Fuente: Elaboración propia.

Se dio clic en la pestaña file y en seguida en la opción Add Evidence Item…

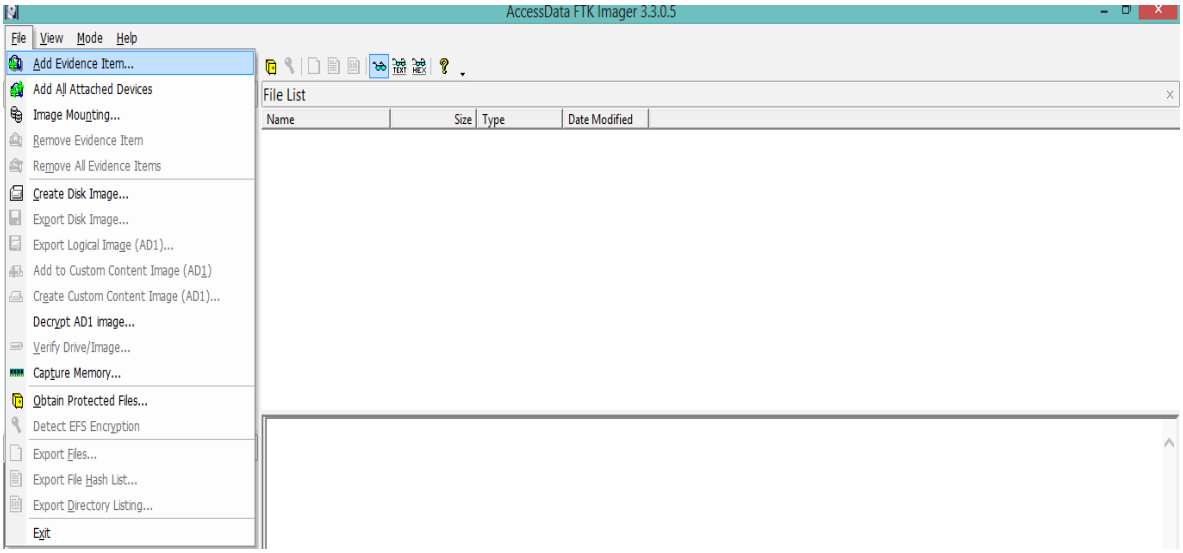

Figura 75. Selección de la opción Add Evidence Item.

Fuente: Elaboración propia.

Se eligió el tipo de evidencia que se desea agregar, se eligió la opción Image File y se le dio en siguiente.

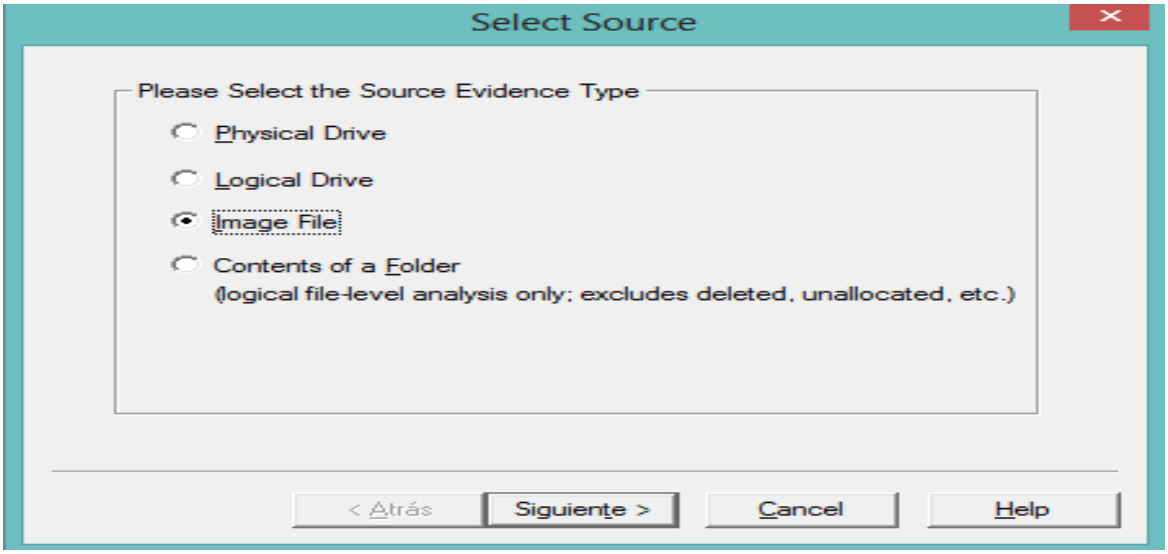

Figura 76. Selección de la opción documento de imagen para agregar.

Fuente: Elaboración propia.

Se abrió la ventana para agregar la ubicación en la que se encuentra la imagen y se le dio clic en el botón finish y se esperó a que terminara de cargar la imagen, se tardó 3 minutos con 34 segundos en cargar la imagen.

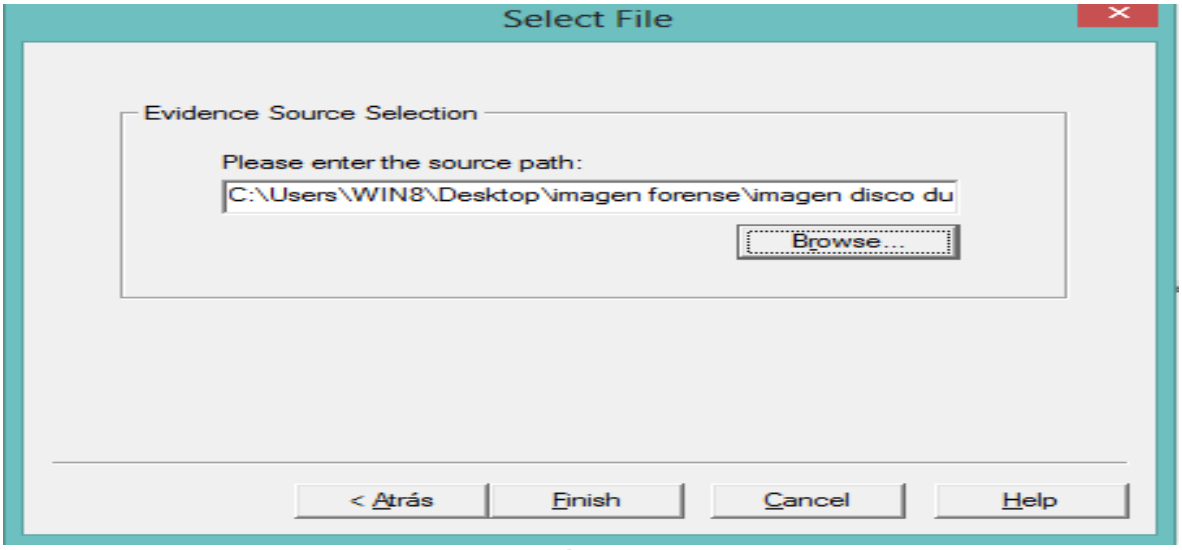

Figura 77. Ubicación de la imagen forense.

Fuente: Elaboración propia.

Una vez finalizado el proceso de cargar la imagen se mostró la imagen sometida.

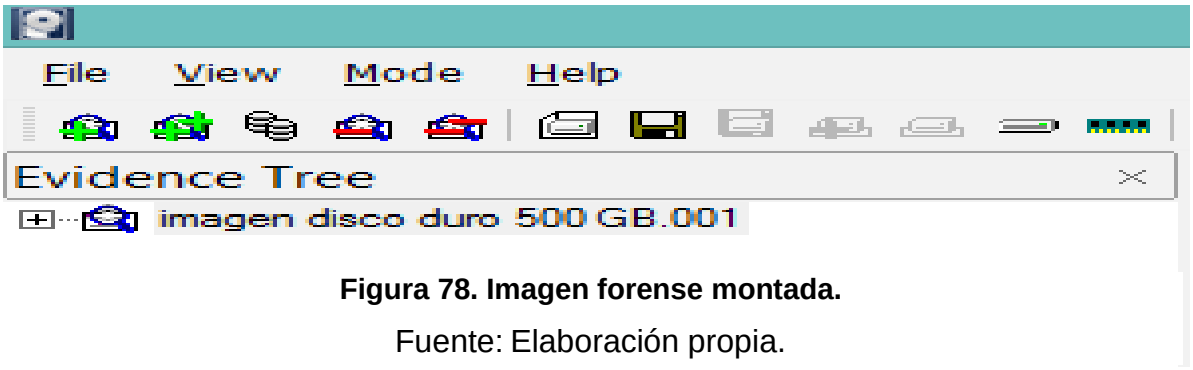

Figura 78. Imagen forense montada.

Fuente: Elaboración propia.

Al dar clic en el signo + se esperó a que terminará el proceso de escaneo el cual duro 2 minutos 33 segundos.

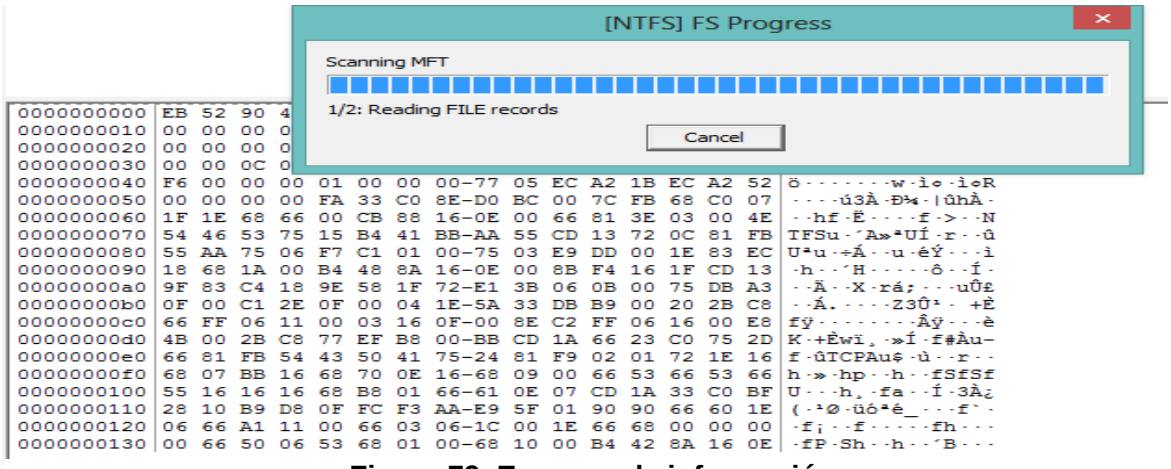

Figura 79. Escaneo de información.

Fuente: Elaboración propia.

Al desglosar el contenido de la imagen, en pantalla se mostró el contenido de la imagen sometida.

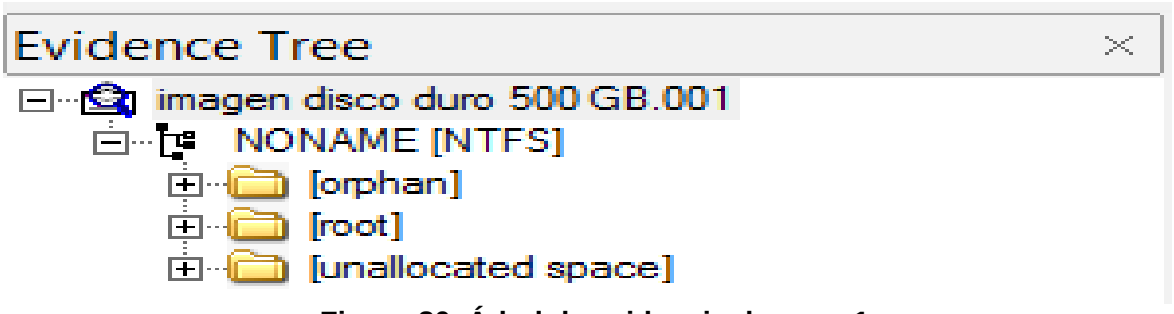

Figura 80. Árbol de evidencia de caso 1.

Fuente: Elaboración propia.

De igual manera se mostró la dirección de memoria, contenido en codificación hexadecimal y encriptación de la información.

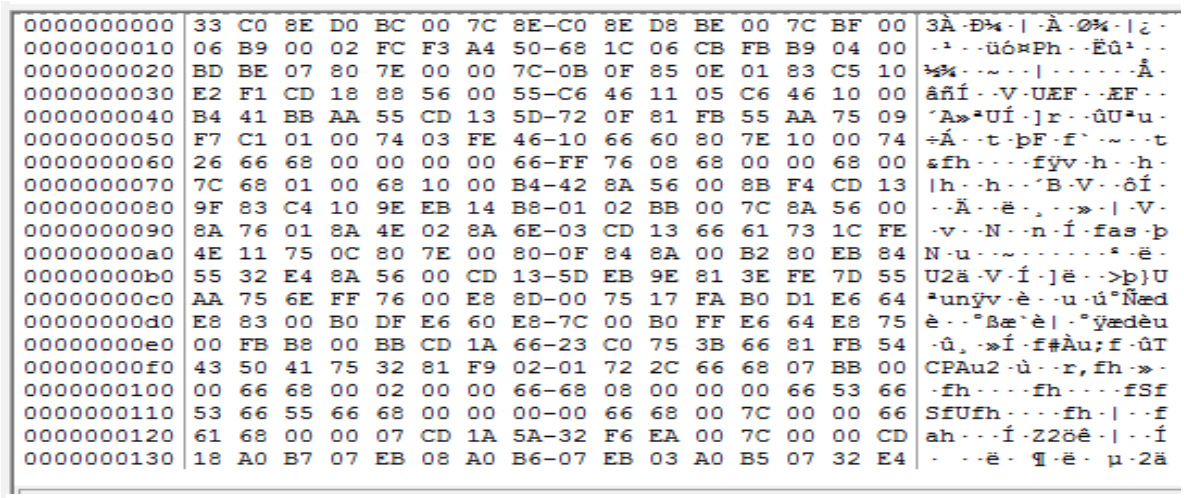

Figura 81. Información encriptada, sectores y direcciones de memoria.

Fuente: Elaboración propia.

Se examinaron las carpetas contenidas.

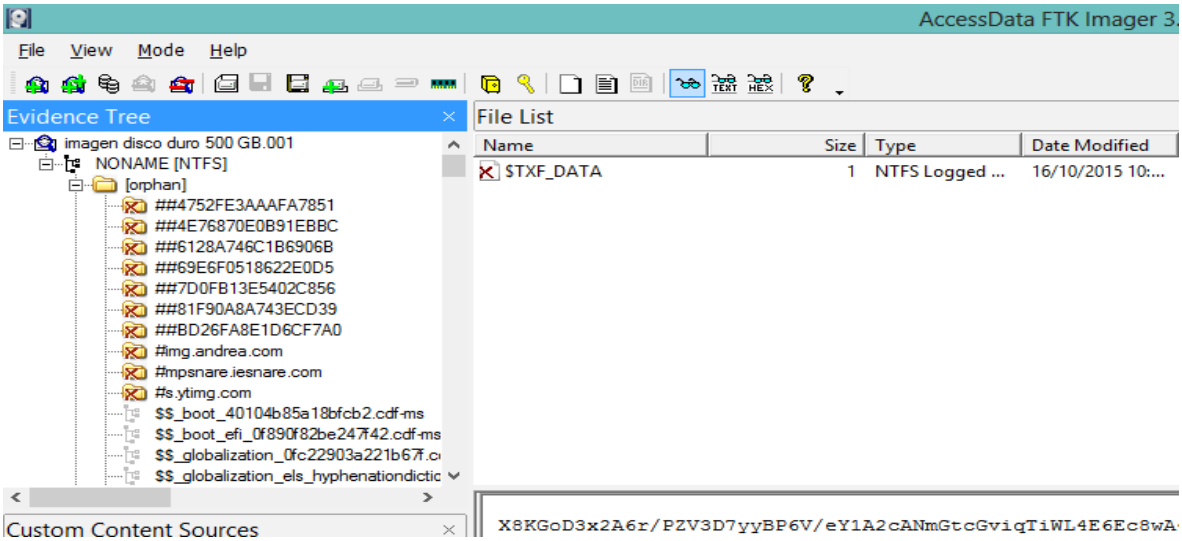

Figura 82. Examinación de la información contenida.

Fuente: Elaboración propia.

Se encontró la carpeta y el sector en la cual se encuentra la información que se deseaba recuperar.

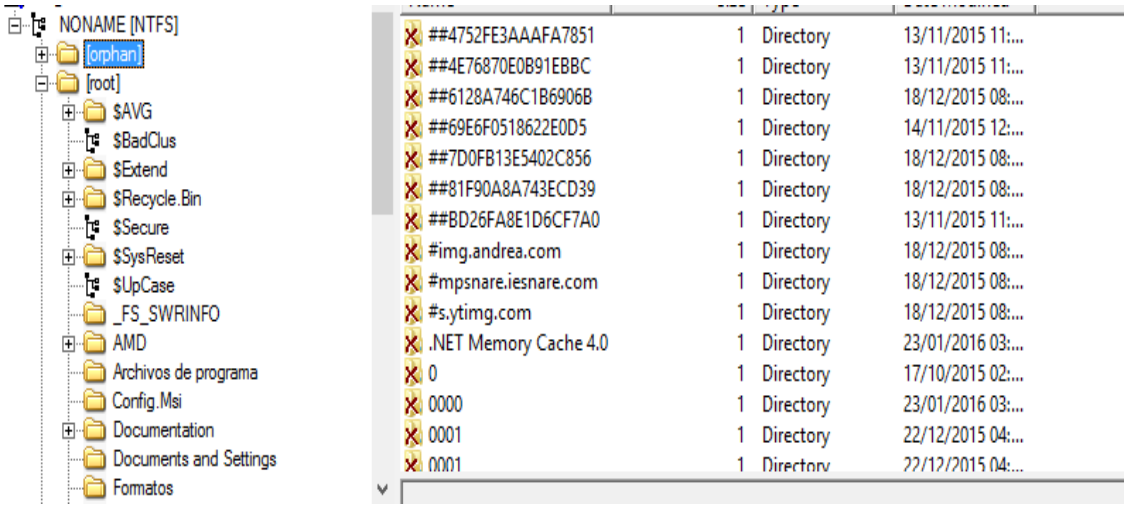

Figura 83. Información contenida.

Fuente: Elaboración propia.

El sector que se siguió analizando es el que contiene la carpeta llamada root.

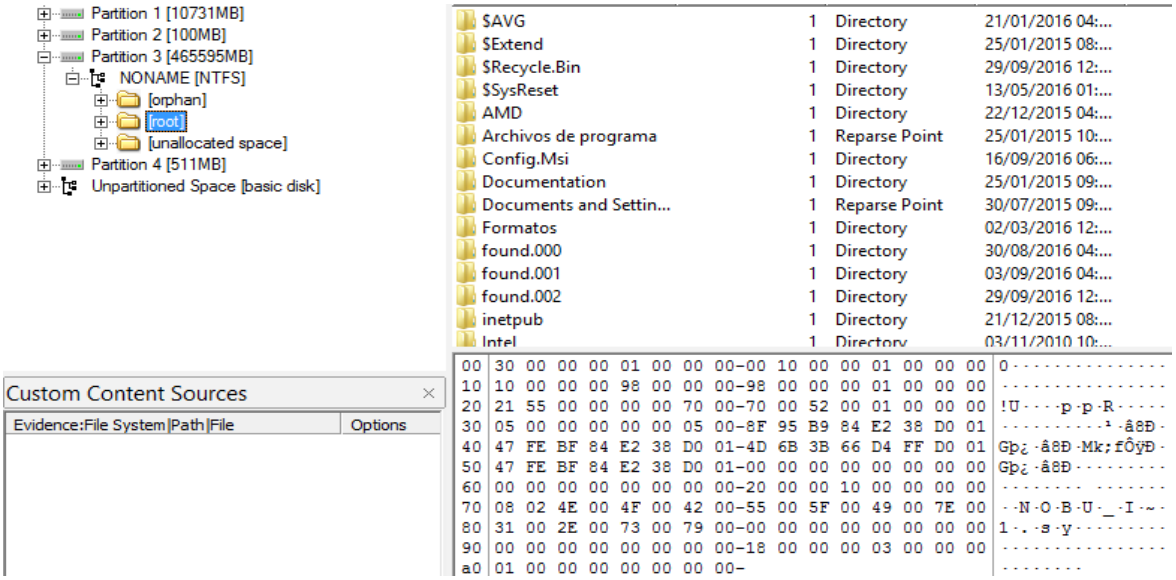

Figura 84. Análisis de la carpeta root.

Elaboración propia.

Dentro de la carpeta root se pudo visualizar lo que contenía, tal como nombre del archivo, tamaño, tipo, fecha.

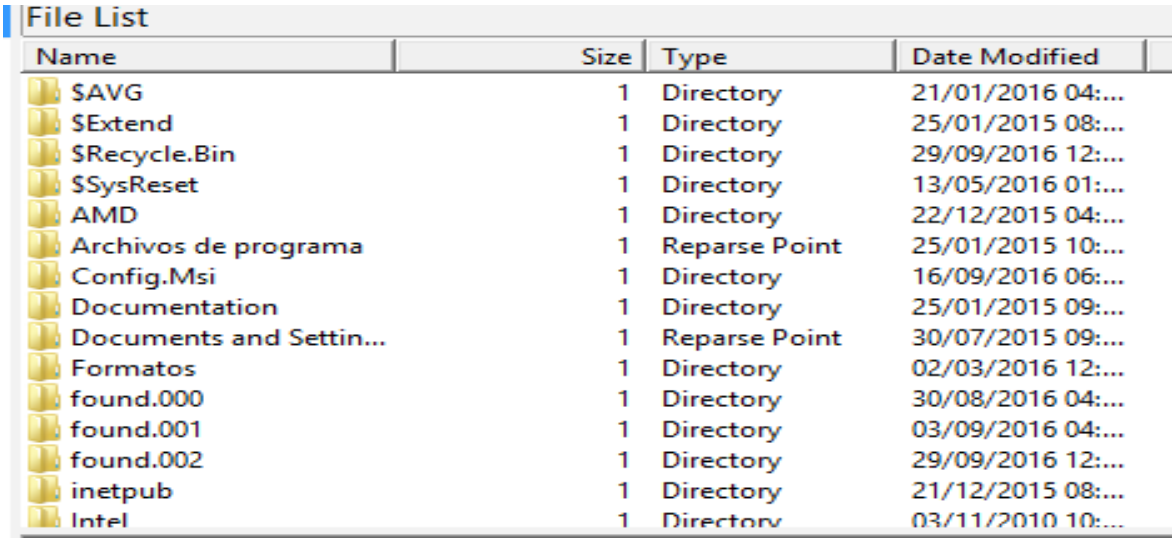

Figura 85. Información encontrada dentro de la carpeta root.

Fuente: Elaboración propia.

Se siguió desglosando el árbol de evidencia al dar clic en el signo + de la carpeta root se puedo tener acceso a su contenido que en este caso son más carpetas.

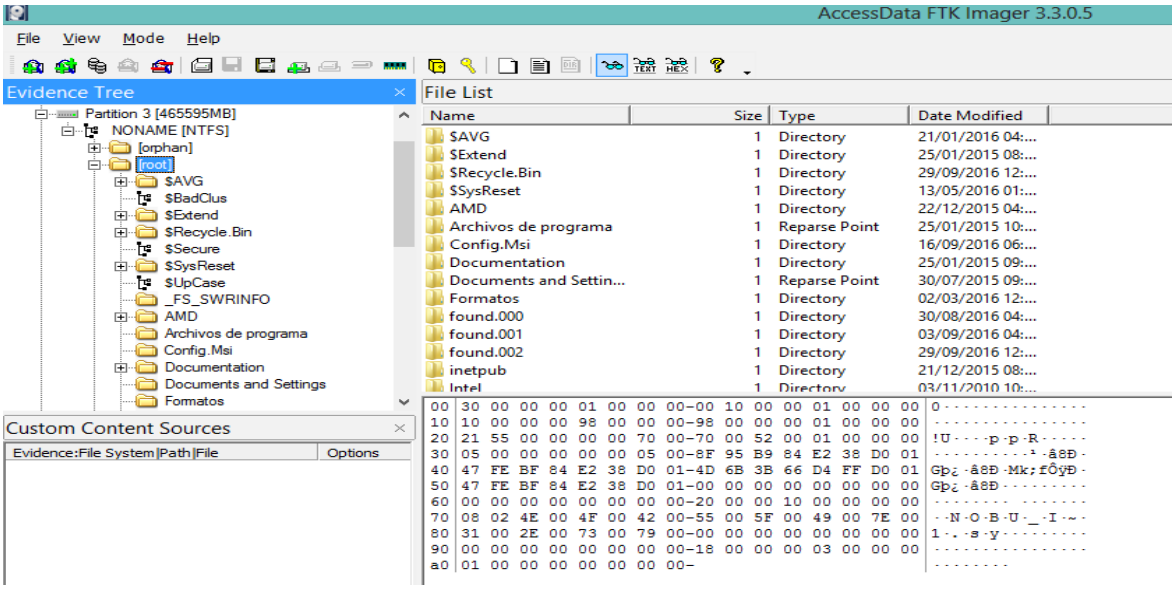

Figura 86. Análisis de información encontrada.

Fuente: Elaboración propia.

Dentro de la carpeta root se encontró una carpeta llamada Users con su respectivo sector en el que se encuentra y lo que contiene

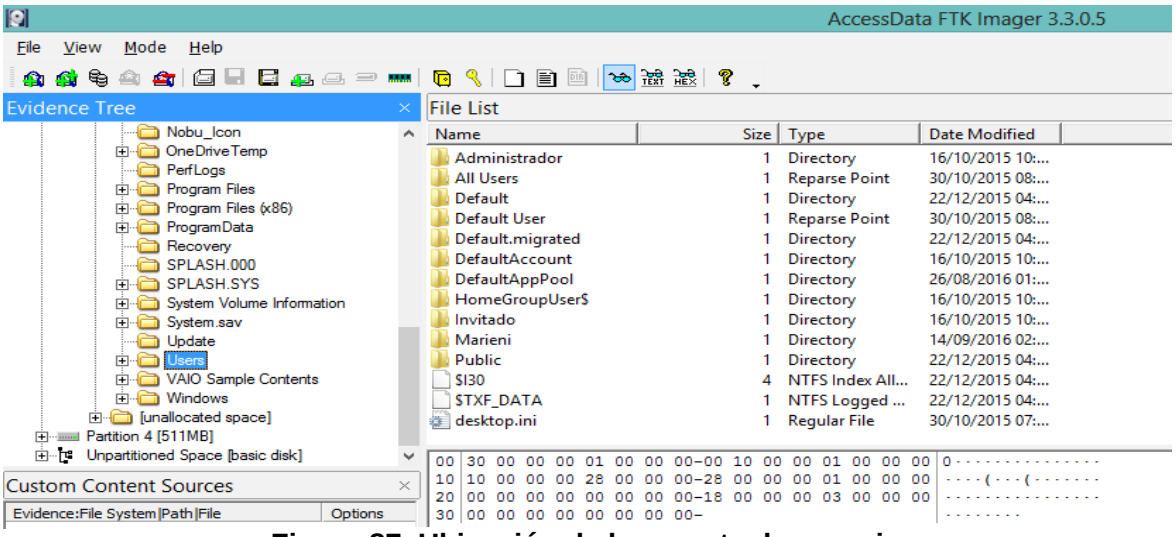

Figura 87. Ubicación de la carpeta de usuarios.

Fuente: Elaboración propia.

Al dar clic en el icono + de Users se desglosaron los usuarios que contiene el disco duro.

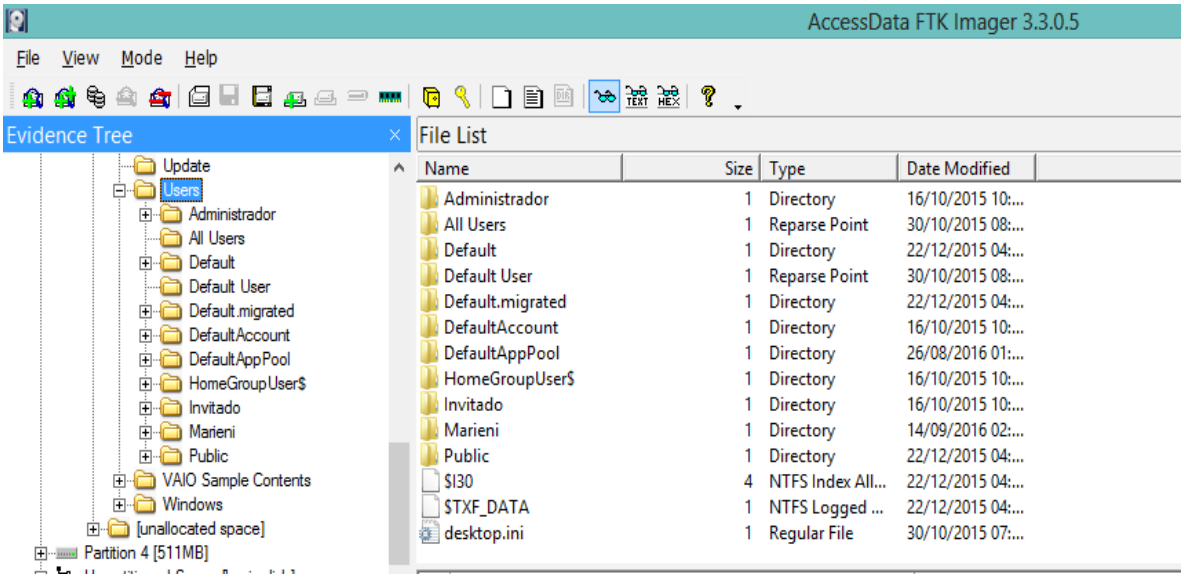

Figura 88. Contenido y análisis de la carpeta usuarios.

Fuente: Elaboración propia.

En seguida se localizó la carpeta llamada *Marieni* en la cual se encontró la información que se desea recuperar, así como su sector en disco duro en el cual se encuentra y la pre visualización de su contenido.

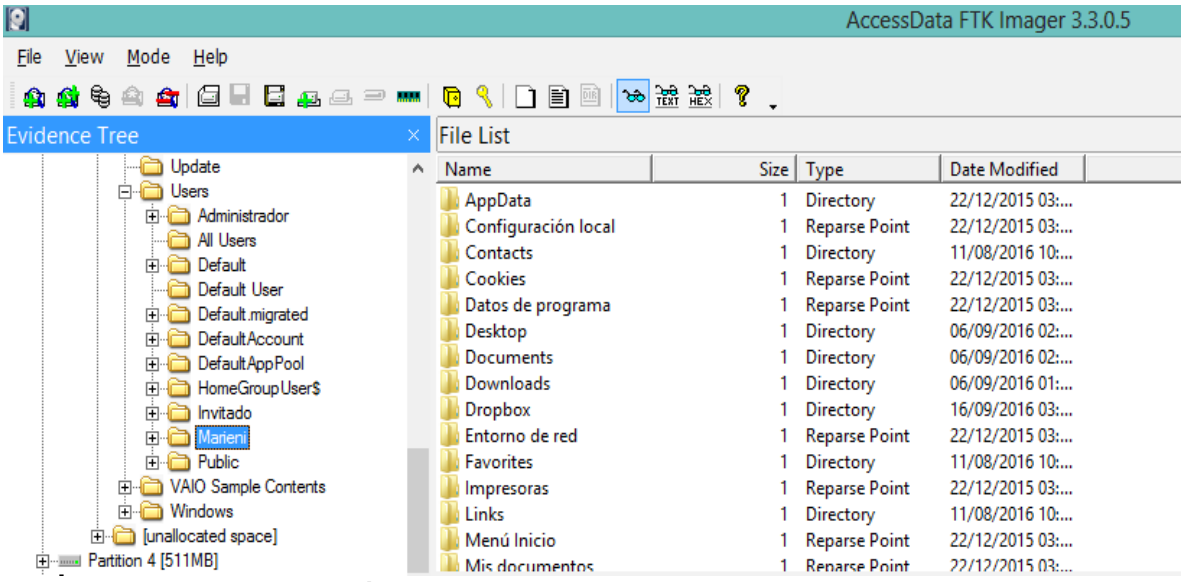

Figura 89. Ubicación de la carpeta correspondiente al usuario Marieni.

Fuente: Elaboración propia.

Se dio clic en el signo +de la carpeta con nombre *Marieni* y se desgloso lo que contiene la carpeta.

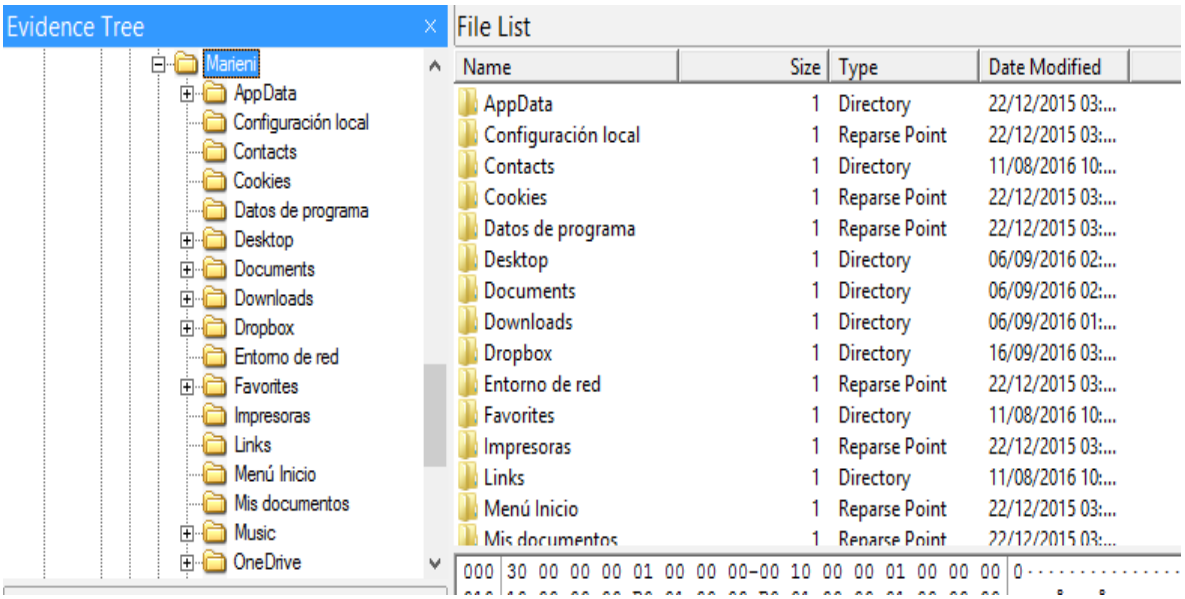

Figura 90. Análisis del contenido de la carpeta correspondiente al usuario Marieni.

Fuente: Elaboración propia.

Se localizó la carpeta llamada documentos, así como su sector en disco duro en el que se encuentra y se pre visualizó su contenido.

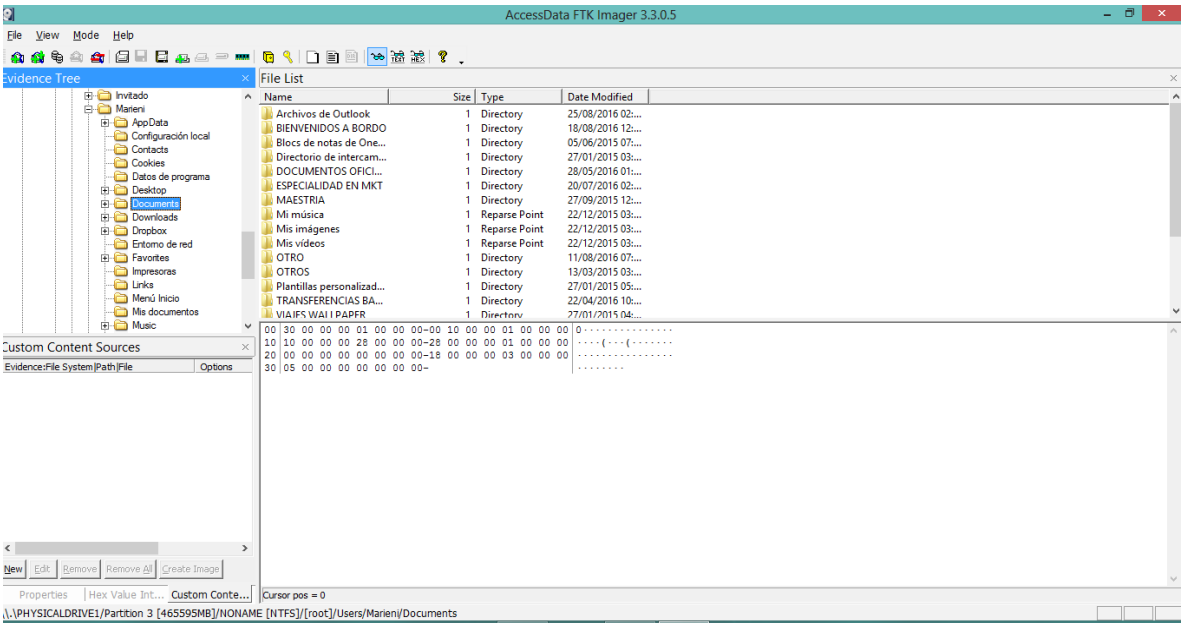

Figura 91. Ubicación y análisis de la carpeta Documentos.

Fuente: Elaboración propia.

Se localizó la carpeta llamada WE EVENTOS, su sector en el que se encuentra en el disco duro y la pre visualización de su contenido.

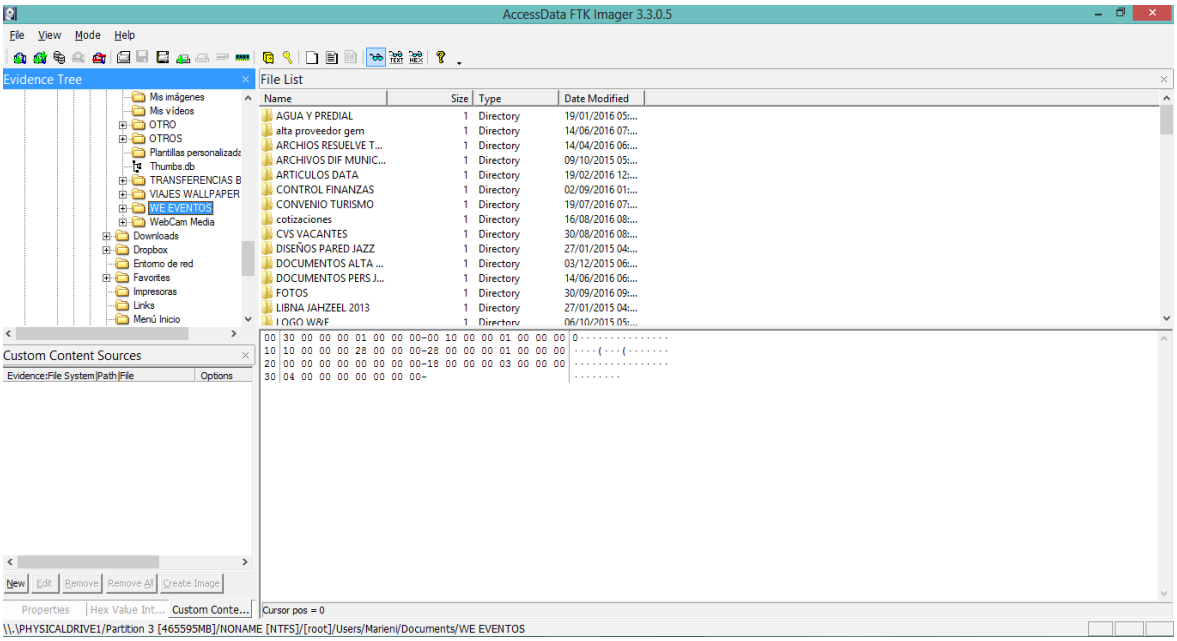

Figura 92. Análisis de la información contenida en la carpeta Documentos.

Fuente: Elaboración propia.

Ya que se encontró la carpeta que se deseaba recuperar se posiciono sobre ella, se le dio clic derecho, apareciendo las siguientes opciones.

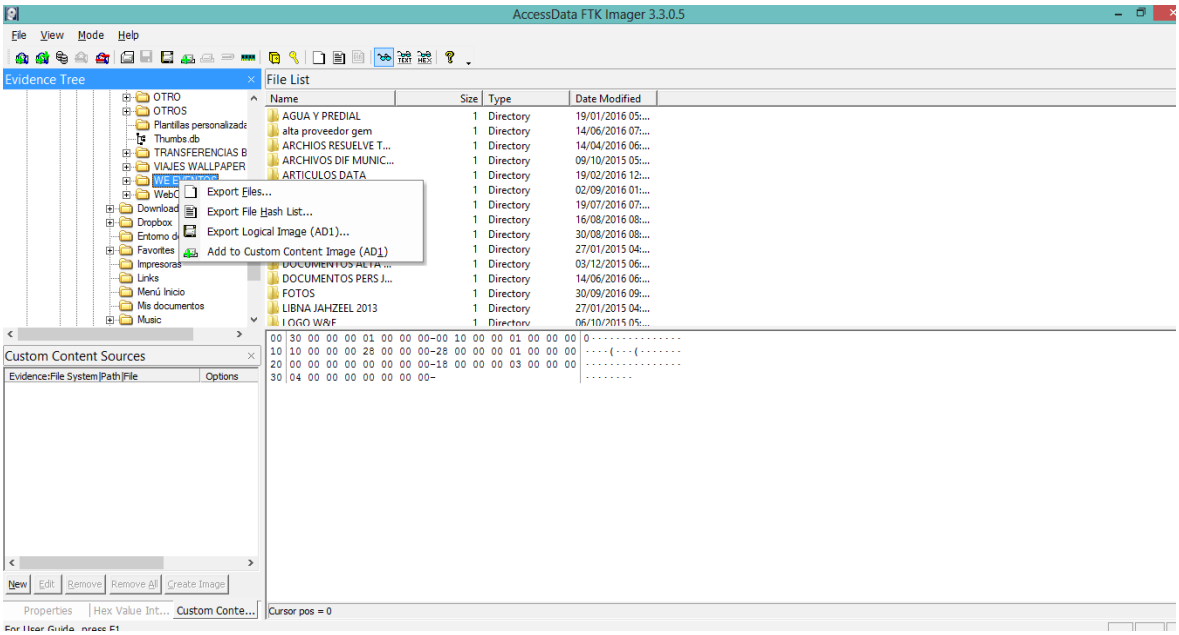

Figura 93. Menú de opciones sobre carpeta requerida.

Fuente: Elaboración propia.

Se seleccionó la opción Export Files ya que se requería recuperar todo el contenido de la carpeta.

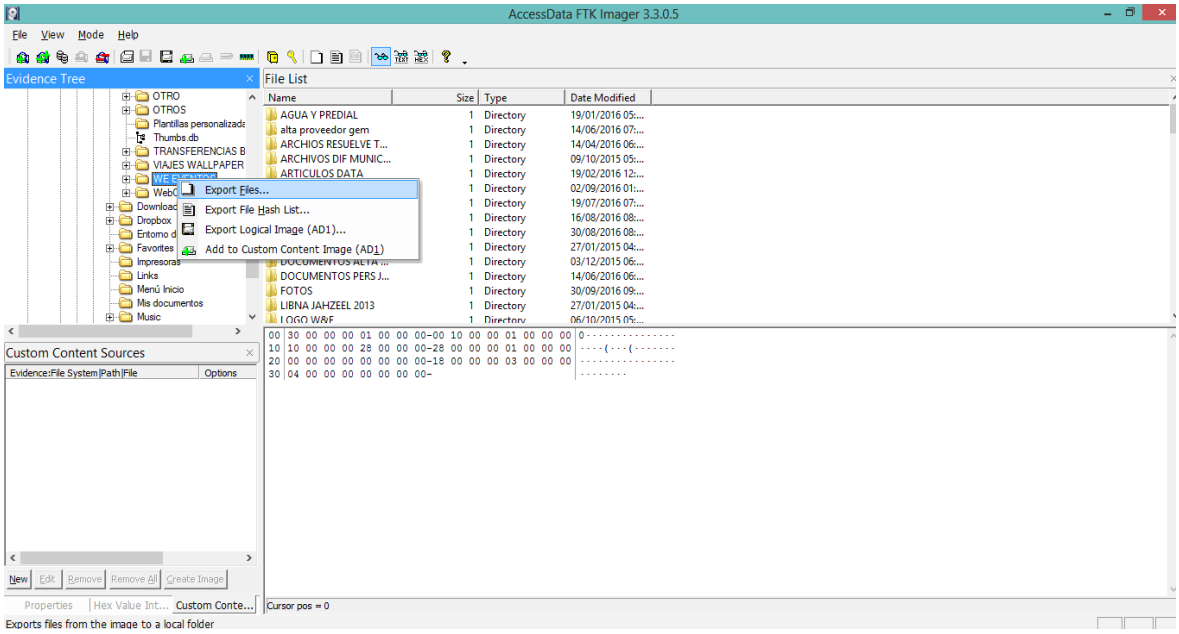

Figura 94. Selección de la opción Export Files.

Fuente: Elaboración propia.

Se abrió una ventana en la cual se especificó el destino en donde se almaceno la información que se requería recuperar.

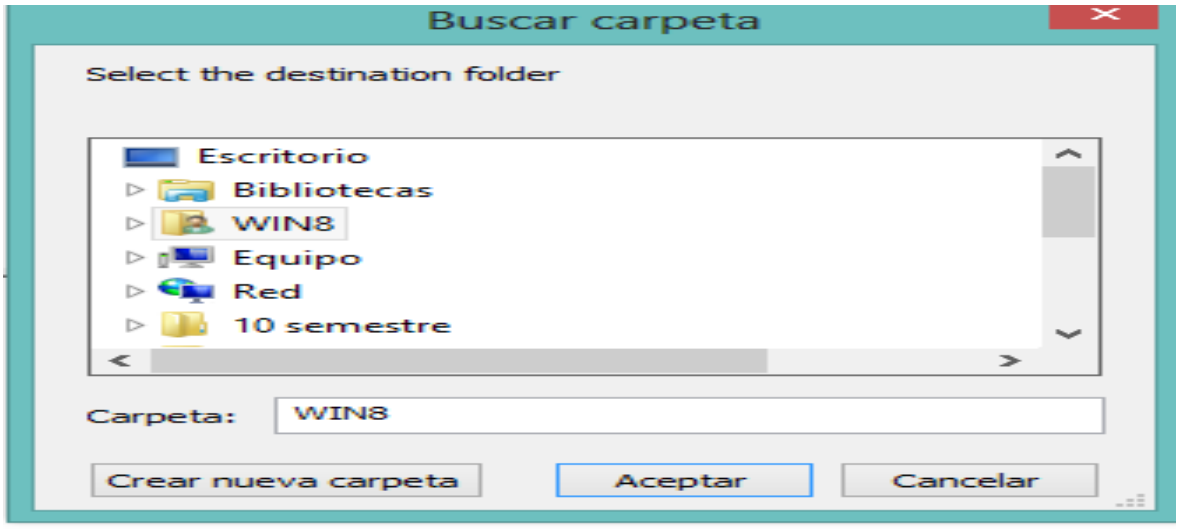

Figura 95. Ventana para seleccionar la carpeta de destino de la información que se requiere recuperar.

Fuente: Elaboración propia.

Se comenzó a recuperar la información, el proceso tardo 3 minutos con 54 segundos

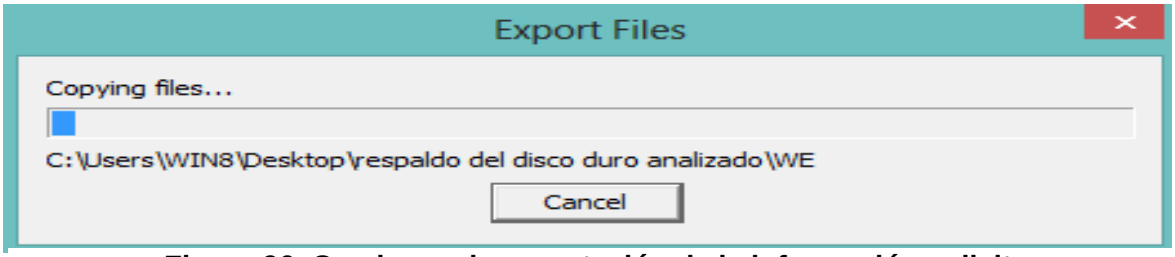

Figura 96. Comienzo de exportación de la información solicita.

Fuente: Elaboración propia.

Finalizo el proceso y se verifico la información recuperada.

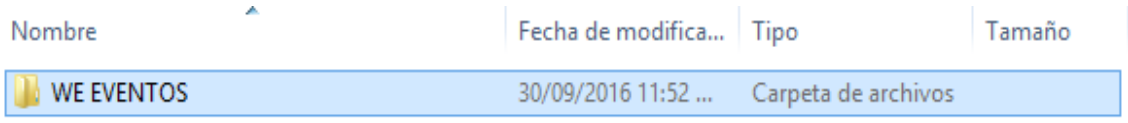

Figura 97. Información recuperada.

Fuente: Elaboración propia.

5.1.4. Reporte

Se pudo recuperar la información solicitada por el usuario, se creó la imagen forense y después se pudo analizar sin ningún problema, los sectores que se encontraban dañados para que no influyeran con la manipulación de la imagen forense se rellenaron con ceros ya que son sectores muy dañados que no permitían la lectura del disco duro y que ya no se pueden recuperar, sin embargo quedaron demasiados sectores intactos que contenían mucha información la cual se pudo recuperar mediante un análisis de la imagen forense.

Se recuperaron 11,993 archivos, y 760 carpetas, dentro de la carpeta documentos del usuario *Marieni* que corresponde a 17 GB.
Se recuperaron 172 GB que corresponden a 45,673 archivos y 5,051 carpetas dentro de la carpeta imágenes del usuario *Marieni*.
De la carpeta que se solicitó recuperar con mayor interés la información la cual es WE EVENTOS contiene 7,859 archivos y 249 carpetas que corresponde a 8 GB.

En total se recuperaron 57,666 archivos del disco duro y 5,811 carpetas que corresponden a 189 GB de información, alcanzando un porcentaje de recuperación de información de un 100% en una escala de 0 a 100, el proceso de recuperación duro 567.27 minutos.

5.2. Experimentación 02

5.2.1. Identificación

Se recibió un Disco duro el día 30 de enero del 2017, pertenece a la escuela primaria Agustín Melgar, ubicada en San Pedro de los Baños Ixtlahuaca, Estado de México. El reporte hablado fue que el disco duro de repente dejo de funcionar, este mismo contiene información de suma importancia para la escuela, como evidencia escolar y documentos importantes para la misma.

Se desea recuperar la mayor cantidad posible de información almacenada en el disco duro. La problemática que presenta es que el disco duro está dividido en tres particiones, a dos de ellas se puede tener acceso sin ningún problema, sin embargo la partición restante al intentar acceder a ella no lo permite, ya que tiene

un problema de redundancia cíclica, por tal motivo se iniciará con el proceso de recuperación de información contenida en el disco duro.

Características del disco duro a analizar:

El disco duro a analizar tiene una capacidad de 640 GB

El modelo es HM641JI

Es de la marca SAMSUMG

El código de barras S26XJDRB228775

LBA 1,250,263,728

F/W: 2AJ10002

Figura 98. Disco duro caso 2.

Fuente: Elaboración propia.

Se conectó el disco duro a la computadora por medio de un cable SATA/IDE-usb que contiene un cable adaptador SATA/IDE-usb 2.0 un cable sata y una fuente o regulador.

Ya conectado mostraba tres particiones.

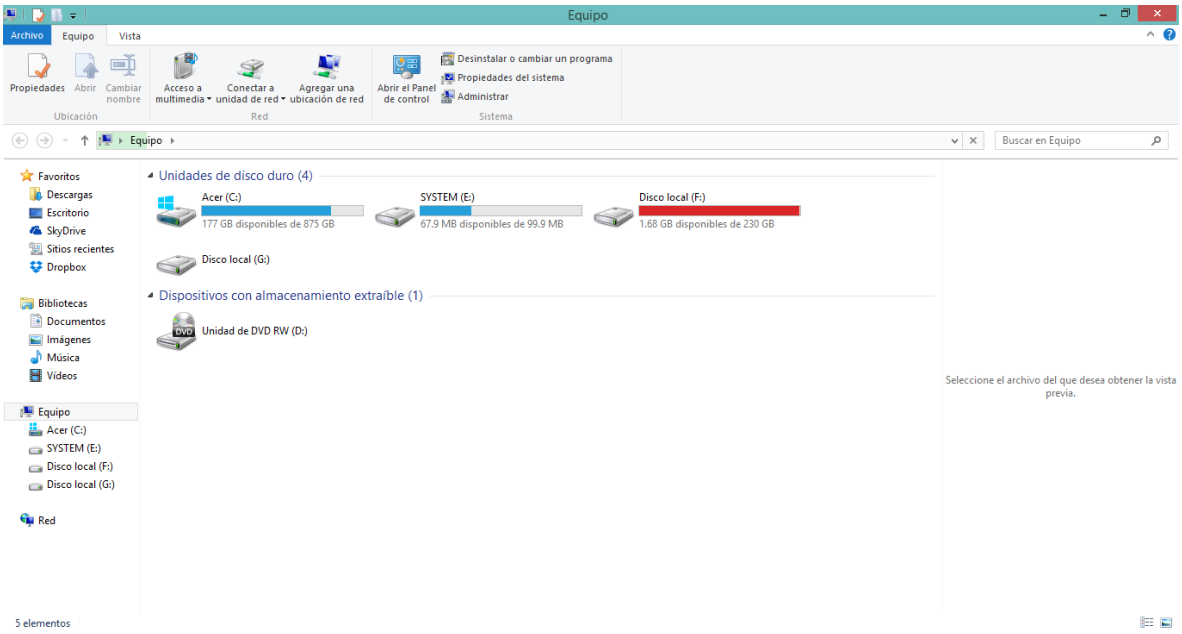

Figura 99. Particiones de disco duro caso 2.

Fuente: Elaboración propia.

Al intentar acceder a la partición requerida mostraba un mensaje de que había problema de redundancia cíclica.

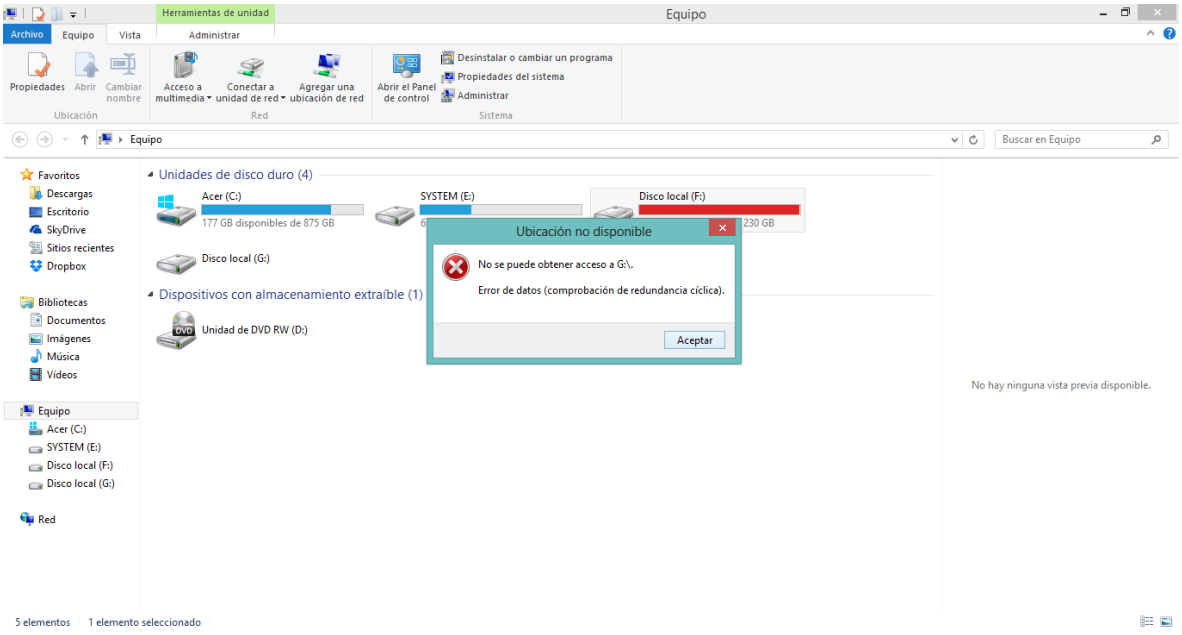

Figura 100. Problema con disco duro caso 2.

Fuente: Elaboración propia.

5.2.2. Análisis

Al dar seguimiento al manual lo que indica es que se debe montar el disco duro a la herramienta que se está utilizando.

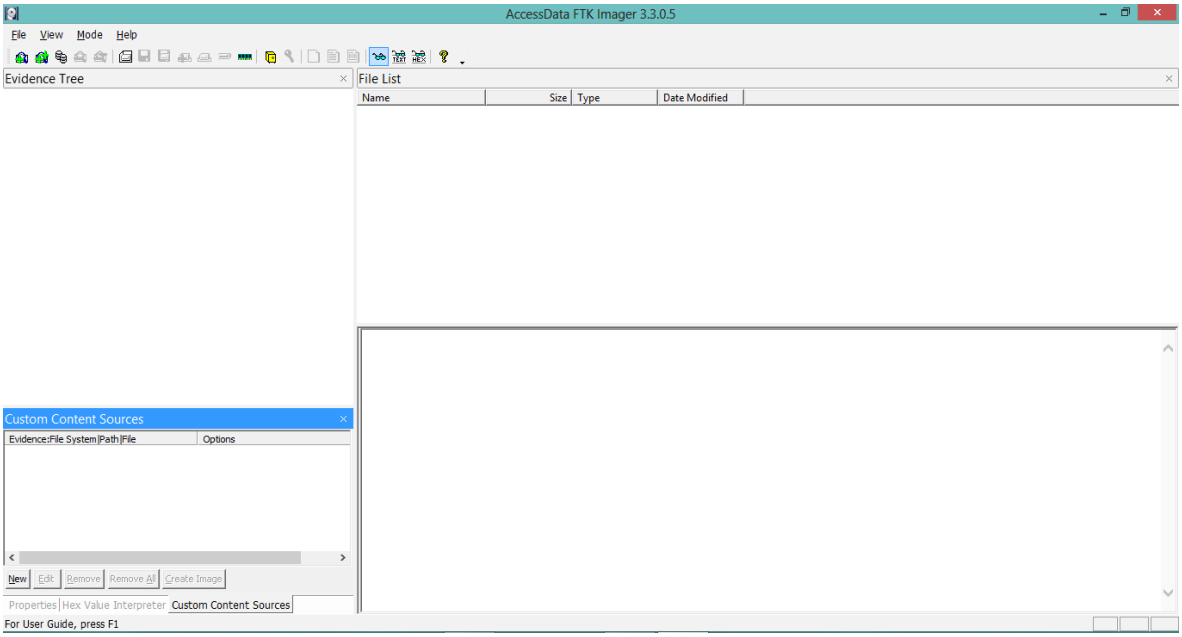

Figura 101. Pantalla principal de FTK utilizada para disco duro caso 2.

Fuente: Elaboración propia.

Se dio clic en la pestaña File y en seguida en la opción Add Evidence Item.

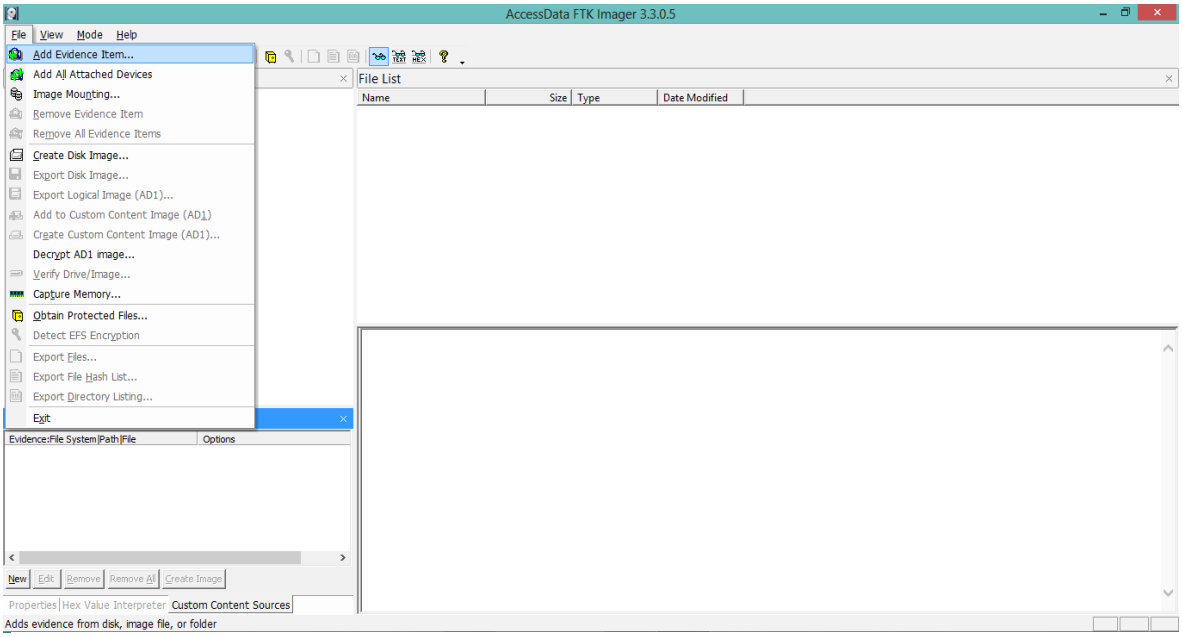

Figura 102. Agregar evidencia en caso 2.

Fuente: Elaboración propia.

En seguida se eligió el tipo de evidencia a agregar y se da clic en el botón siguiente, así que se seleccionará la opción Physical Drive ya que se trabajará con el disco duro físico.

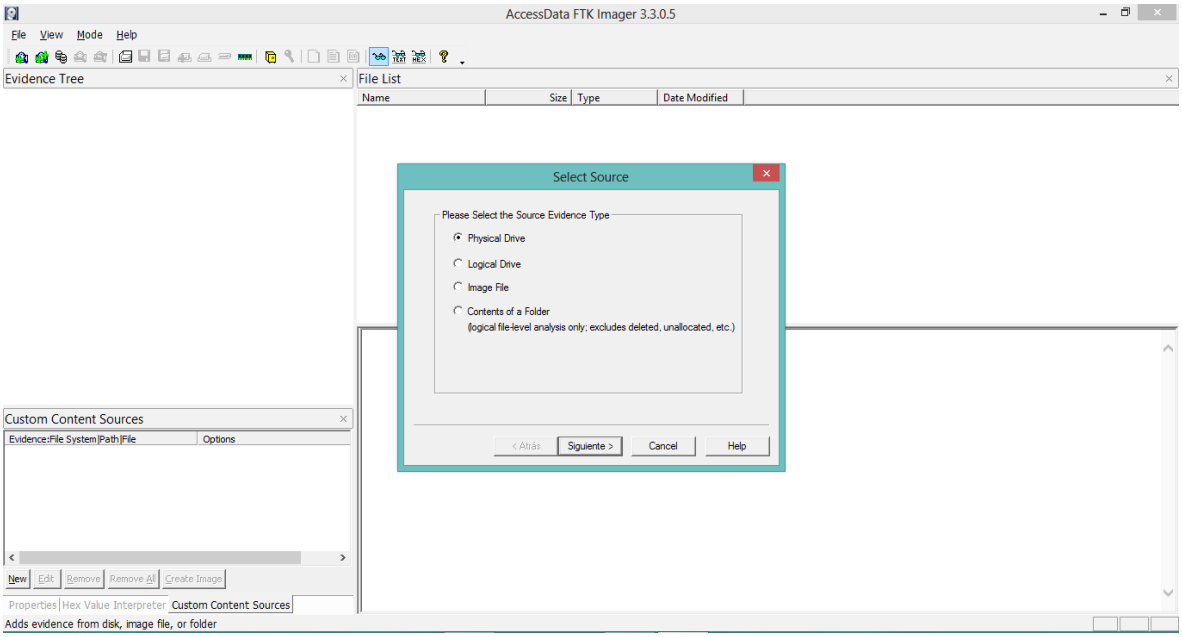

Figura 103. Tipo de evidencia a agregar.

Fuente: Elaboración propia.

En seguida se seleccionó la ubicación de donde se encuentra el disco duro y se dio clic en el botón finish.

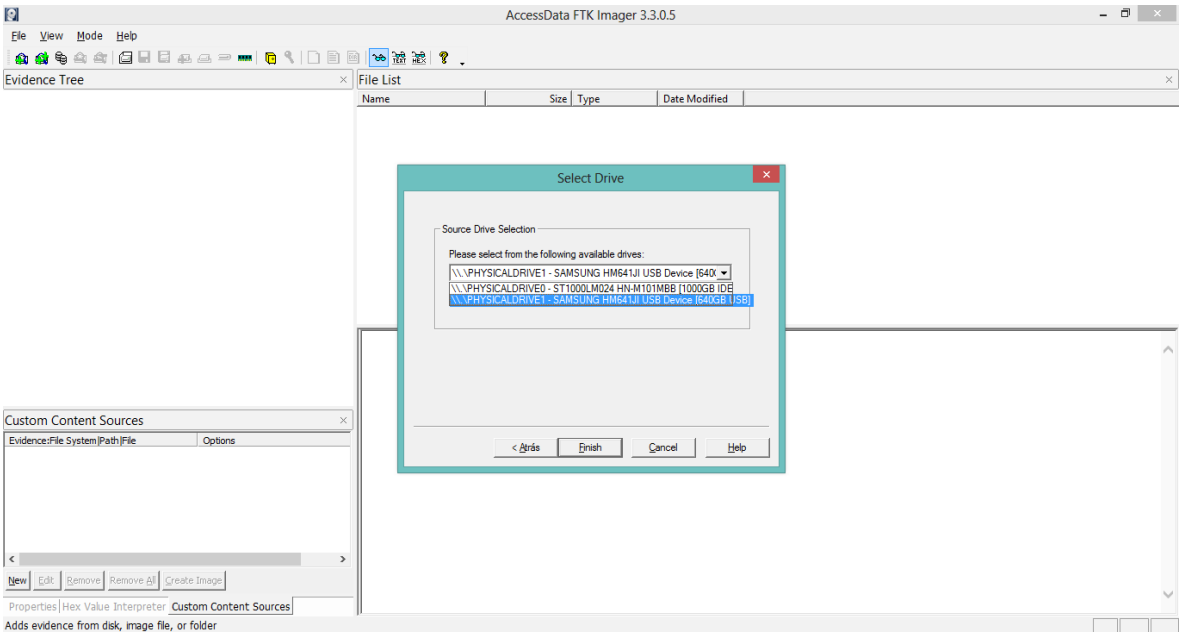

Figura 104. Ubicación de la evidencia en caso 2.

Fuente: Elaboración propia.

Una vez montado correctamente el disco duro, se procedió al análisis del contenido de mismo, para comenzar a analizarlo se dio clic sobre el icono + que se encuentra a lado del disco duro montando.

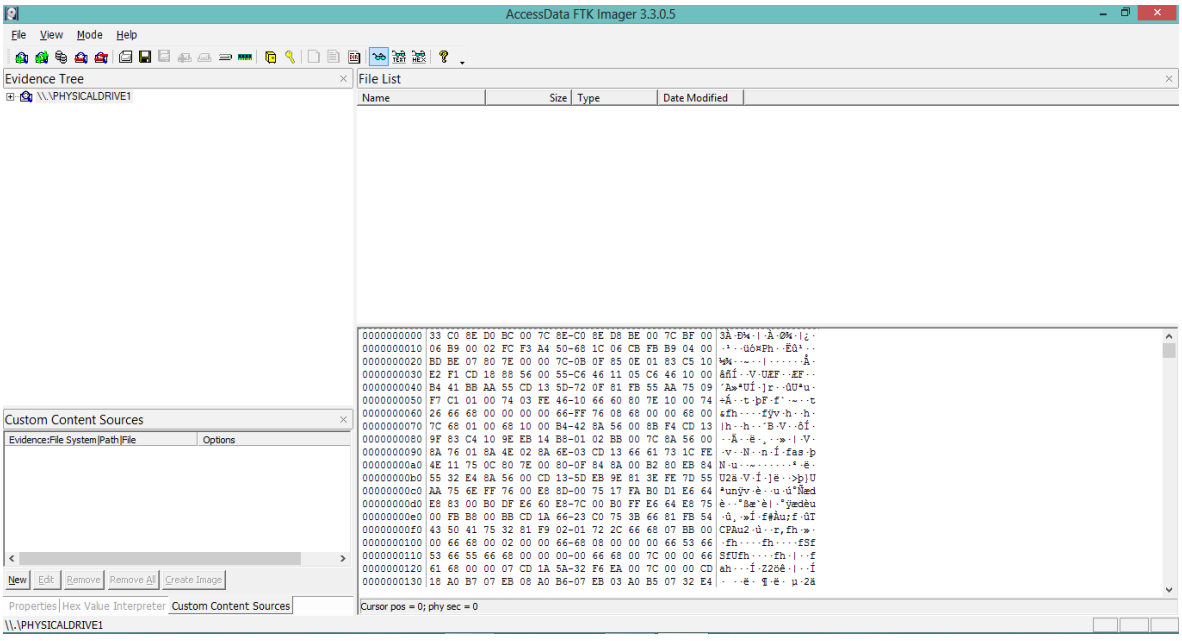

Figura 105. Disco duro de caso 2 montado.

Fuente: Elaboración propia.

Se comenzó a explorar el disco duro.

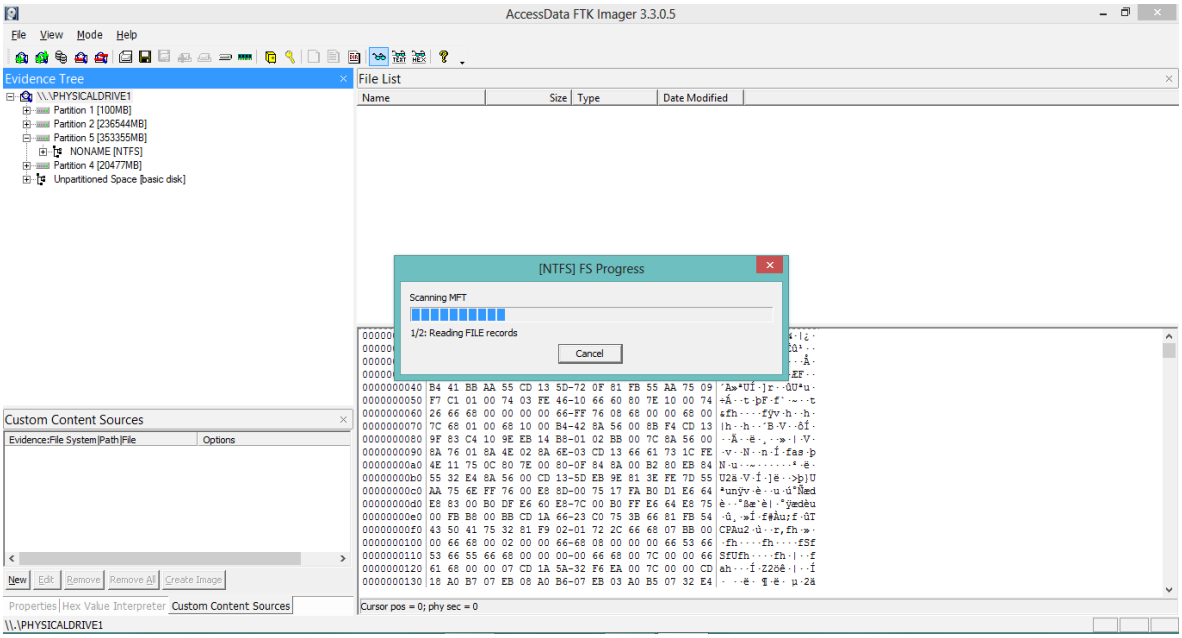

Figura 106. Exploración del disco duro del caso 2.

Fuente: Elaboración propia.

Al analizar el contenido y saber en dónde se encontraba la información que se necesita recuperar se dio un clic sobre el archivo o carpeta a recuperar.

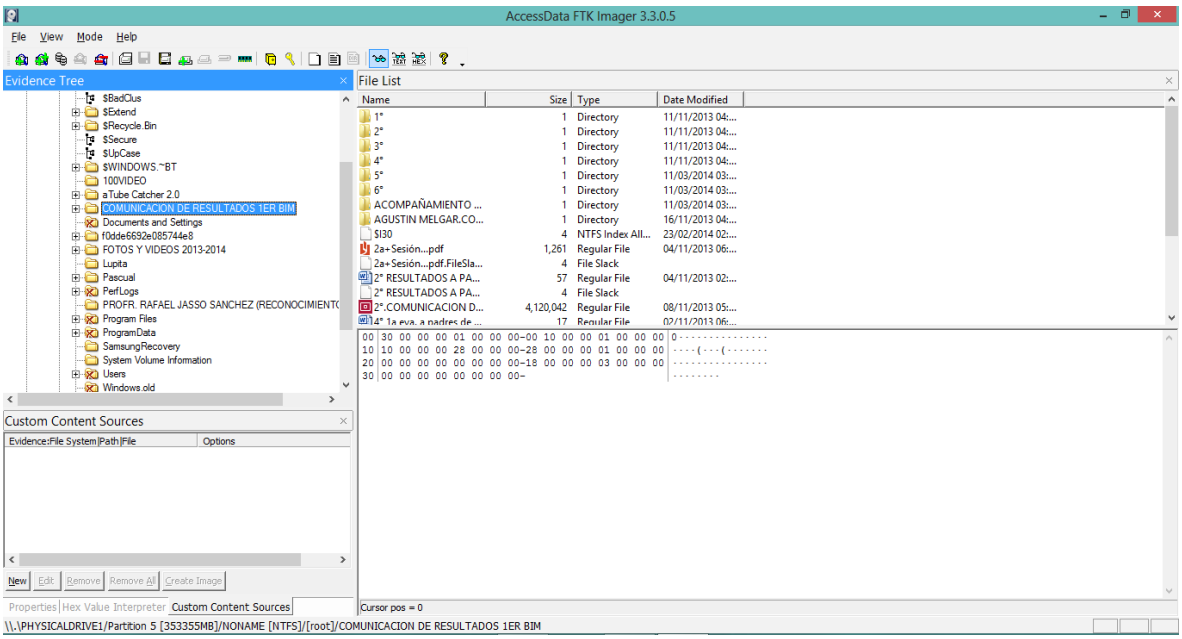

Figura 107. Ubicación de información dentro de disco duro de caso 2.

Fuente: Elaboración propia.

Una vez que se identificó la información a recuperar, se dio un clic izquierdo sobre el archivo y se dio clic en la opción Export Files.

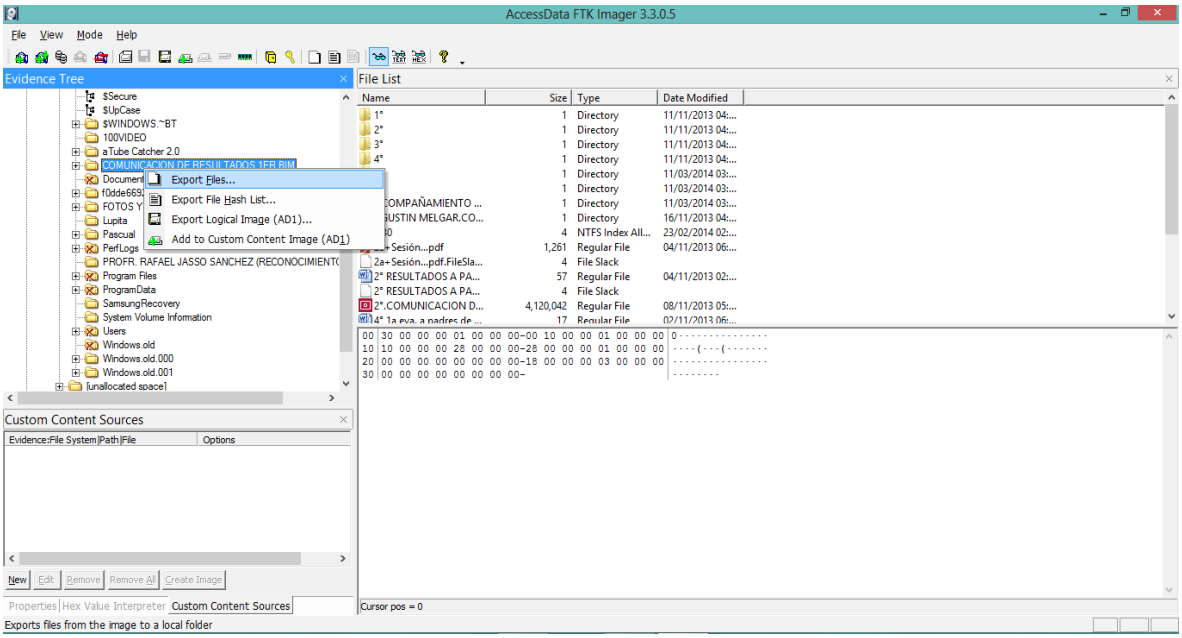

Figura 108. Elección de la opción Export Files en el caso 2.

Fuente: Elaboración propia.

En seguida se eligió el destino en donde se exporto la información y se dio clic en el botón aceptar.

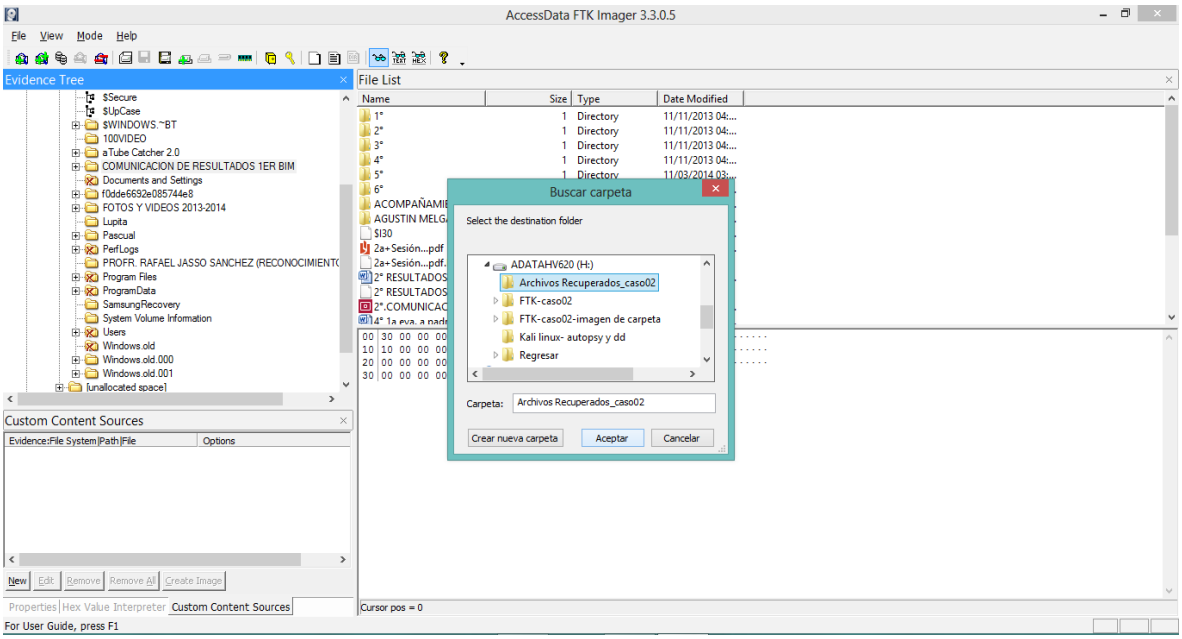

Figura 109. Elección de destino de archivos a exportar del caso 2.

Fuente: Elaboración propia.

Al dar clic en el botón aceptar se abrió una ventana con el progreso de la exportación de la información solicitada.

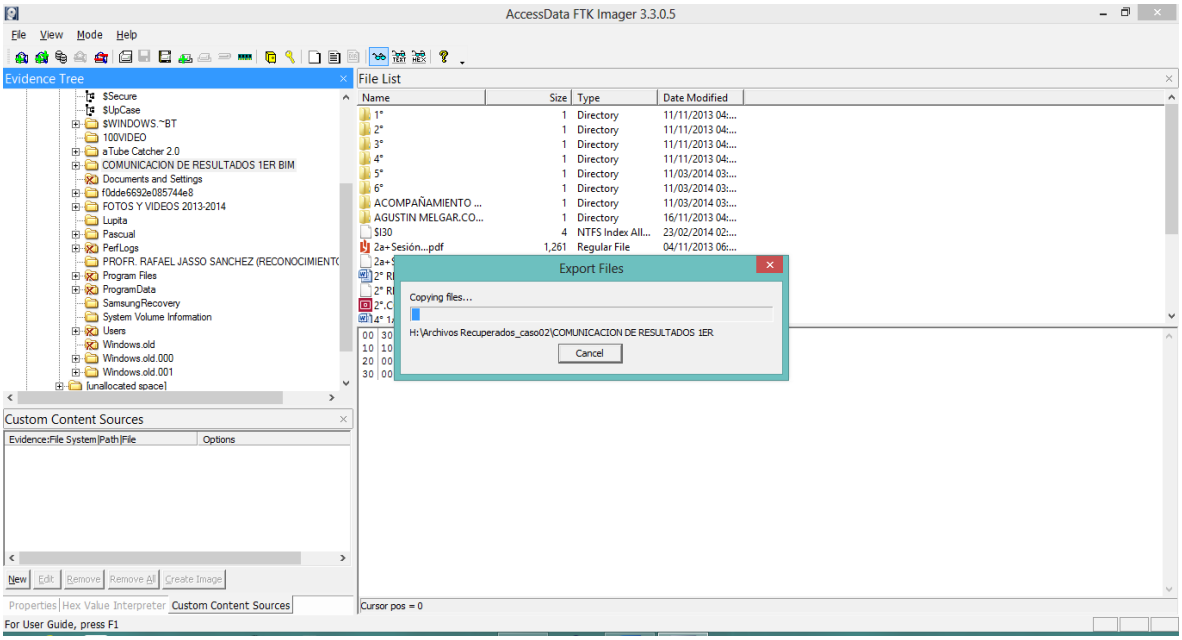

Figura 110. Progreso de la exportación de información del caso 2.

Fuente: Elaboración propia.

Se repitió el mismo proceso del paso anterior con cada una de las carpetas restantes que contienen información.

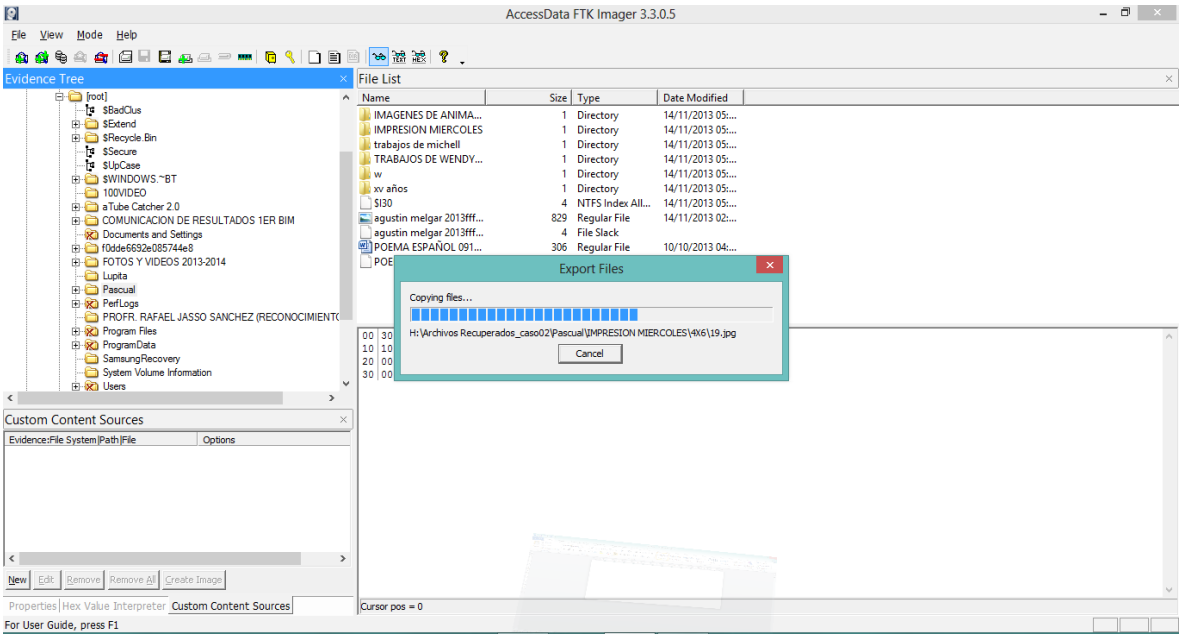

Figura 111. Exportación de la información.

Fuente: Elaboración propia.

En total tardo 538 minutos la recuperación, se pudieron recuperar 6 de 7 carpetas contenidas, una no pudo ser recuperada ya que en los sectores en los que se encuentra es en donde está el problema de redundancia cíclica que afecto al disco duro, en total se recuperaron 1963 archivos divididos en 37 carpetas con un tamaño en disco de 55.6 GB lo que corresponde a 85.71% de la información almacenada en una escala de 0 a 100.

5.3. Conclusiones

Hoy en día la información es más vulnerable a sufrir daños graves, esto mismo conlleva a que la información se pierda con mayor frecuencia sin que los usuarios puedan hacer algo para recuperarla, o al menos eso se daba frecuentemente. Actualmente el cómputo forense desempeña un papel muy importante en el ámbito de recuperación de información, ya que es un área que originalmente surgió para recuperarse o protegerse de ataques informáticos, sin embargo, hoy en día es posible emplear cómputo forense para recuperarse de diversas amenazas que atentan con nuestra información.

Este trabajo surgió después de que un familiar tuvo pérdida de información de un disco duro, dicho disco duro sufrió una caída por un descuido de la persona, el disco duro contenía almacena información muy importante para el dueño del mismo, ya que en ese tiempo era Director Escolar y manejaba diferente tipos de información de gran valor escolar como lo son: reportes escolares, archivos de calificaciones, reportes de asistencias, documentos fiscales, fotos y videos de evidencia escolar, entre otras cosas, siendo este su único dispositivo de almacenamiento y respaldo de dicha información. Dicho lo anterior, el usuario que sufrió la pérdida de información antes mencionada, intento recuperarla de distintas maneras, todas aplicadas sin tener éxito en la tarea solicitada, quedando como su única opción, la resignación a perder por completo su información.

Este tema despertó un gran interés en mi persona, de tal manera que investigué por medio de internet toda la información posible sobre el tema, navegando en internet me encontré con problemas relacionados con pérdidas de información, especialmente en discos duros, este problema es muy habitual entre los usuarios.

Platicando sobre esto con mi asesor el L.CID Martin Garcia Avila, llegamos a puntos críticos que se consideraron buenos, sobre si un gran número de personas pierde información habitualmente de sus discos duros, y si el cómputo forense es una gran alternativa para recuperar información de una manera efectiva, por qué

no hacer un manual con técnicas y herramientas ya probadas que guíen al usuario paso a paso para que dicha tarea sea exitosa, además de orientarlo a usuarios en general, no solo para usuarios con amplios conocimientos en computación, sino que pueda ser utilizado por personas que comprendan y manejen conceptos básicos de computación.

El objetivo del manual creado es dar seguimiento al proceso que se debe realizar para recuperar información en discos duros. Para determinar sobre que herramienta se trabajaría el manual, se hizo una comparación entre tres herramientas las cuales son: Foremost, Autopsy y FTK Imager, las dos primeras bajo el sistema operativo Kali Linux y la última menciona en el sistema operativo Windows 8, tal y como se mencionó anteriormente.

Para la tarea solicitada FTK Imager fue de la que se obtuvieron mejores resultados, en varios aspectos, entre los más relevantes son: FTK Imager es más intuitivo, más fácil de instalar, rápido en los procesos de respuesta, opción de recuperar información de manera masiva, entre otras cosas.

Los resultados obtenidos al dar seguimiento al manual son exitosos, alcanzando en la experimentación 01 un porcentaje de recuperación de información de un 100% en una escala de 0 a 100, mientras que en la experimentación 02 se obtuvo un porcentaje de recuperación de información de 85.7% en una escala de 0 a 100.

Algo muy importante que se debe resaltar es que los dueños de los discos duros que se sometieron a la fase de experimentación, anteriormente intentaron recuperar dicha información sin tener éxito, sin embargo, al aplicar el manual basado en cómputo forense se obtuvieron buenos resultados.

TRABAJOS FUTUROS

Como continuación de este trabajo, existen diversas líneas de investigación que quedan abiertas y en las que es posible continuar trabajando. Durante el desarrollo de este trabajo de investigación han surgido algunas líneas de investigación que han quedado abiertas y que se espera se puedan trabajar en un futuro; algunas de ellas están relacionas directamente con el presente trabajo ya que durante el desarrollo del mismo han surgido cuestiones, dichas cuestiones pueden ser tomadas en cuenta para posteriormente retomarlas como opción a trabajos futuros para otros investigadores.

A continuación, se presentan algunos trabajos futuros que pueden en un futuro desarrollarse como resultado de la presente investigación, que por cuestiones de no exceder los objetivos y el alcance del trabajo no han sido tratados con la suficiente profundidad que se requiere.

Entre los posibles trabajos futuros que destacan se encuentran los siguientes:

- Realizar un comparativo entre herramientas de cómputo forense de licencias libres y licencias de pago, con el objetivo de saber cuanto mayor es el alcance entre unas y otras.
- Probar las mismas herramientas probadas en la presente investigación en diversas plataformas, con el fin de verificar si aún pueden tener más alcance y más bondades al momento de aplicar los procesos necesarios para la recuperación de información.
- Generar Manuales técnicos y de usuario de cómo aplicar cómputo forense de manera correcta probando distintas herramientas de uso forense.
- Probar herramientas de cómputo forense que estén especializadas en disminuir el tamaño de la imagen forense sin dañar, ni alterar la información almacenada en los dispositivos de almacenamiento.
- Crear un manual de cómo realizar cómputo forense que apoye en la recuperación de información en discos duros vía remota.

- Crear un manual de cómo recuperar información desde la reconstrucción física del medio de almacenamiento, hasta el análisis forense de la parte lógica.

BIBLIOGRAFÍA

Aceituno Canal, V. (2007). *Seguridad de la información: Expectativas, riesgos y técnicas de protección.* México, D.F., México: LIMUSA, S.A. DE C.V.

Ajoy, G. (March de 2004). *Handbook Guidelines for the management of IT evidence.* Obtenido de APEC Telecommunications and Information Working Group: http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN016411.pdf

Arias Chavez , M. (2007). PANORAMA GENERAL DE LA INFORMÁTICA FORENSE Y DE LOS DELITOS INFORMÁTICOS EN COSTA RICA. *InterSedes: Revista de las sedes regionales*, 15.

Baeza Yates, R., & Ribeiro Neto, B. (1999). *Modern information retrieval.* New York: Addison Wesley.

Cano Martínez, J. J. (2006). Introducción a la informática forense. *ACIS*.

Casey, E. (2004). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the internet.* San Diego, California : Academic Press.

Choquehuanca, S. F. (Diciembre de 2006). Dispositivos de almacenamiento. *Revista de Bibliotecología y Ciencias de la Información- UMSA*, 7.

Christopher, M. D., & Prabhakar, r. (s.f.).

del Ramo Romero, J. J., Núñez de Murge, M., Núñez de Murge, J., & Pertusa Grau, J. (2010). *Introducción a la Investigación Biológica.* Valencia: OpenCourseWare.

Fernández Bleda, D. (14 de 10 de 2004). Informática forense: "Recuperación de la evidencia digital". *Ponéncies IGC/INET*, (pág. 14). Barcelona. Recuperado el 18 de Agosto de 2016, de Internet Security Auditors: www.isecauditors.com

García Lambert, G., García Hernández , R. A., & Ledeneva, Y. (Julio-Octubre de 2014). Reglas que describen la deserción y permanencia en los estudiantes de la UAP Tianguistenco de la UAEM. *Ciencia Ergo Sum, 21*(2), 121-132.

García Velázquez, D. R. (Abril de 2014). METODOLOGÍA BASADA EN CÓMPUTO FORENSE PARA LA INVESTIGACIÓN DE DELITOS INFORMÁTICOS. *TESIS*. México, México D.F., México.

Gervilla Rivas, C. (Diciembre de 2014). Tesis. *Metodología para un análisis forense*. Cataluña, España: Creative Commons.

Gómez de Silva Garza, A., & de Jesus Briseño, I. A. (2008). *Introducción a la COMPUTACIÓN* (Primera Edición ed.). (J. C. Castro, Ed.) México, D.F.: CENGAGE Learning.

Herrerías Rey, J. E. (2006). *El PC- Hardware y componentes* (Edición 2006 ed.). ANAYA.

Igwersen, P. (1992). *Information retrieval interaction.* Los Angeles: Taylor Graham.

Informática, D. d. (1999). *DICCIONARIO DE INFORMÁTICA.* Madrid,España.

J.A, S., & Avilés, A. (2005). La investigación de Información: Revisión de tendencias actuales y críticas. 17.

Jaime Segundo, I. (2009). *Red de calidad de centro docente- Dept. de informática*. Recuperado el 21 de Octubre de 2016, de Informática en el Jaime II- Dept. de informática: http://jaimesegundo.edu.gva.es/web_mestre.inf/treball/si/disco_duro.htm

Luzuriaga Jaramillo, H. A. (2011). Tesis. *Herramientas de análisis forense y la recuperación de información en los dispositivos de almacenamiento en los laboratorios de la facultad de ingeniería en sistemas electrónica e industrial de la universidad técnica de Ambato* . Ambato, Ambato, Ecuador.

MOOERS, C. N. (1952). Information retrieval viewed as temporal signalling. *En Proceedings of the International Conference of Mathematicians.* Cambridge.

Noblett, M. G. (2000). *Recovering and Examining Computer Forensic Evidence* . Obtenido de Federal Bureau of Investigation: http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm

Norton, P. (2006). *Introcucción a la computación* (sexta edición ed.). México D.F., México: McGraw-Hill Interamericana.

Palacios Ugalde, A. (Octubre de 2010). Tesis. *Metodología para el análisis forense informático en sistemas de redes y equipos de cómputo personal*. México, D.F., D.F., México.

Peñaloza Reinoso, L. E. (2016). ESTRATEGIA DE INFORMÁTICA FORENSE PARA DISPOSITIVOS MÓVILES BAJO TECNOLOGÍA ANDROID EN LA UNIVERSIDAD REGIONAL AUTÓNOMA DE LOS ANDES. *TESIS*. AMBATO, AMBATO, ECUADOR.

Pérez Martínez, M. J. (2012). *InFORMÁTICA I por competencias con los enfoques intercultural e interdisciplinar.* México: LIMUSA, S.A. de C.V.

Pérez Villa, J. D. (2008). *Introducción a la informática.* Madrid: ANAYA Multimedia.

Rivas López, J. L. (2009). *Análisis Forense de Sistemas Informáticos* (Primera Edición ed.). Barcelona, España: FUOC.

Rodríguez Argueta, M. (2007). Recuperación de información en discos duros. *Tesis*. México, México D.F., México.

Salmerón, A. (2015). *Historia informatica forense*. Recuperado el 15 de Agosto de 2016, de http://cj- worldnews.com/spain/index.php/es/criminalistica-29/item/1786-la- inform%C3%A1tica-forense-el-rastro-digital-del-crimen

Santana Tiznado, M. A. (2001). *INFORMÁTICA* (Primera edición ed.). (J. L. Campoy, Ed.) México, D.F, México: McGraw-Hill Interamericana.

Seagate. (Marzo de 2010). *www.seagate.com.* Recuperado el Agosto de 2017, de www.seagate.com: www.seagate.com

Villacís Ruiz, V. M. (2006). Auditoria Forense: Metodología, Herramientas y Técnicas Aplicadas en un siniestro informático de una empresa del sector comercial. *TESIS*. GUAYAQUIL, ECUADOR.

Zuccardi, G., & Gutiérrez, J. D. (Noviembre de 2006). Informática Forense.