ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad De Ingeniería En Electricidad Y Computación

INFORME DE MATERIA DE GRADUACIÓN

"DRAFT COMPLETE"

Previa a la obtención del Título de:

LICENCIADO EN REDES Y SISTEMAS OPERATIVOS

Presentada por:

ÁNGEL PATRICIO JIMÉNEZ PROCEL

JONATHAN GONZALO ZEVALLOS MEJÍA

GUAYAQUIL – ECUADOR
2013

AGRADECIMIENTO

A Dios por ser nuestra guía espiritual, por permitir culminar nuestros estudios universitarios ya que él nos da la sabiduría para mantener la fe, el esfuerzo y la perseverancia, ya que es la base fundamental y necesaria para alcanzar nuestra meta.

A nuestras familias por ser nuestra guía de formación humana por haber inculcado los buenos valores, principios, por darnos ese apoyo emocional, sentimental y económico.

A nuestros profesores por ser nuestra guía de enseñanza ya que con paciencia, y amor nos han compartido sus experiencias para ser buenos profesionales de éxito.

DEDICATORIA

A Dios porque El dirige mis pensamientos y caminos. Su fortaleza y sabiduría me dan el éxito y satisfacción en la vida, a mi familia, en especial a mis padres y hermanos por haber dado lo mejor de ellos y siempre haber mantenido la confianza en mí, a mis tíos quienes me han apoyado por mucho tiempo, a mi novia Lissette Andrade quien ha sido un gran apoyo en mi vida, a mis compañeros porque me han brindado su apoyo a lo largo de mi carrera.

Ángel Patricio Jiménez Procel.

DEDICATORIA

Primeramente a Dios porque él ha sido mi guía y me ha dado el talento para seguir adelante y cumplir con mis metas y objetivos propuestos.

A mis padres porque gracias a ellos me han enseñado los valores y responsabilidades que todo hijo quisiera aprender y sentirse orgulloso de ellos.

A esta prestigiosa Universidad, porque gracias ella hemos desarrollado nuestro aprendizaje y ha sido la guía en nuestro camino profesionalmente.

Y a todos mis compañeros, porque siempre nos apoyamos y estuvimos juntos como un buen equipo de trabajo.

Jonathan Gonzalo Zevallos Mejía.

DECLARACIÓN EXPRESA

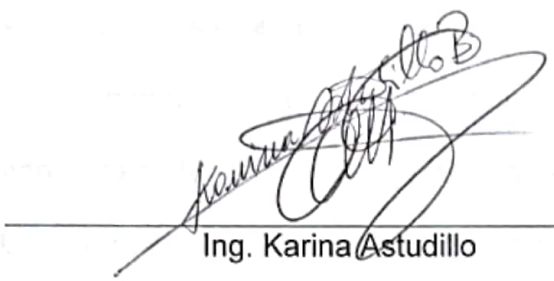
"La responsabilidad del contenido de este informe, nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral"

(Reglamento de Graduación de la ESPOL)

Ángel Patricio Jiménez Procel

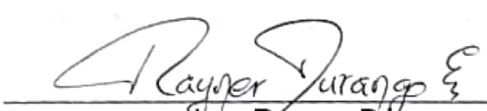
Jonathan Gonzalo Zevallos Mejía

TRIBUNAL DE SUSTENTACIÓN



Ing. Karina Astudillo

PROFESOR DE LA MATERIA DE GRADUACIÓN



Ing. Rayner Durango

PROFESOR DELEGADO POR EL DECANO

RESUMEN

El proyecto se basó en realizar un plan para el análisis forense de un dispositivo de almacenamiento, el cual nos permita utilizar las herramientas y pasos adecuados para la óptima examinación y recuperación de la información. Utilizaremos los métodos aprendidos en este curso y las herramientas las cuales nos han sido provistas.

El análisis fue realizado utilizando los siguientes métodos y herramientas que hemos creído adecuadas para este caso:

- ✓ Se utilizó un ambiente de software libre (Open Source) como es el caso de Caine 2.0, como un ambiente para realizar el análisis forense.

- ✓ Se utilizó la ayuda de la línea de comandos, para establecer la recuperación archivos borrados.

- ✓ Se utilizó la herramienta Autopsy, para la recuperación de los archivos eliminados.

- ✓ Se utilizaron herramientas para Windows, para realizar la búsqueda de más archivos ocultos una vez formateado el dispositivo.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En esta nueva era de tecnología y alta competitividad comercial, en donde las empresas buscan innovar cada vez más en sus productos, y es así que la materia prima de elaboración y seguridad de esta son cada vez más importantes y confidenciales, debido a la implementación ya sea de nuevas ideas sobre el mercado o de nuevos artículos, los cuales pueden marcar una notable diferencia entre sus competidores.

No obstante, muchas empresas realizan una gran inversión en este tipo de estrategias, además de lidiar con los problemas de amenazas externas como el hacking, robos, etc. uno de los mayores temas de seguridad en cuanto a protección de información y materiales de la empresa tiene que ver con amenazas internas de la empresa los cuales podrían facilitar información que sería de utilidad para empresas rivales o algún tipo de ataque.

En muchos de los casos estas empresas no consideran este tipo de peligros para sus estrategias. Según CNN Estados Unidos en el 2009 un 59% de de empleados despedidos se queda con información de la empresa, y un 44% de las empresas ha sido víctima de ataques por empleados y ex empleados. E indudablemente el porcentaje ascenderá en los próximos años.

CAPÍTULO 1

ANTECEDENTES Y JUSTIFICACIÓN

Nuestro informe tiene como principal rol el análisis óptimo de una imagen forense y determinar si dichos archivos mencionados en el caso fueron eliminados o alterados por la persona acusada como víctima del crimen cibernético.

1.1. ANTECEDENTES

El constante reporte de vulnerabilidades en sistemas de información, el aprovechamiento de fallas bien sea humano, procedimental o tecnológico sobre infraestructuras de computación en el mundo, ofrecen un escenario perfecto para que se cultiven tendencias relacionadas con intrusos informáticos. Estos intrusos poseen diferentes motivaciones, alcances y estrategias que desconciertan a analistas, consultores y cuerpos

especiales de investigaciones, pues sus modalidades de ataque y penetración de sistemas varían de un caso a otro.

A pesar del escenario anterior, la criminalística nos ofrece un espacio de análisis y estudio hacia una reflexión profunda sobre los hechos y las evidencias que se identifican en el lugar donde se llevaron a cabo las acciones catalogadas como criminales.

A pesar del escenario anterior, la criminalística nos ofrece un espacio de análisis y estudio hacia una reflexión profunda sobre los hechos y las evidencias que se identifican en el lugar donde se llevaron a cabo las acciones catalogadas como criminales.

En este momento, es preciso establecer un nuevo conjunto de herramientas, estrategias y acciones para descubrir en los medios informáticos, la evidencia digital que sustente y verifique las afirmaciones que sobre los hechos delictivos se han materializado en el caso bajo estudio.

La informática forense hace entonces su aparición como una disciplina auxiliar de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos, así como garante de la verdad alrededor de la evidencia digital que se pudiese aportar en un proceso.

En consecuencia, este breve documento busca ofrecer un panorama general de esta especialidad técnico legal, para ilustrar a los lectores sobre los fundamentos generales y bases de actuación de aquellos que

se han dedicado a procurar el esclarecimiento de los hechos en medios informáticos, unos nuevos científicos que a través de la formalidad de los procesos y la precisión de la técnica buscan decirle a los intrusos informáticos que están preparados para confrontarlos y procesarlos. [18]

1.2. JUSTIFICACIÒN

A medida que los casos de robo de información cada vez son más frecuentes en nuestro medio y las técnicas de las personas que realizan estos actos son cada día más complejos, nos vemos obligados a cada día instruirnos en como contrarrestar estos hechos.

Es importante y necesario planificar, analizar e implantar sistemas y políticas de seguridad, establecer medidas de control, planes de contingencia y realizar auditorías sobre los sistemas implantados y su correcto cumplimiento. Auditar las políticas de seguridad instituidas en la empresa, que tienen como objetivos analizar el nivel de cumplimiento de las políticas puestas en marcha y detectar aquellas lagunas para evolucionar en las mismas.

Es así, como un procedimiento forense digital busca, precisamente, evitar esas modificaciones de los datos contenidos en el medio magnético al analizar, que se pueden presentar en cualquier instante, desde el mismo momento en el que haya ocurrido el presunto hecho punible por razones tan diversas al simple paso del tiempo, porque

alguien haya decidido apagar la máquina, porque se haya ejecutado en ella una aplicación que sobre escribió en el almacenamiento de material informático y su correspondiente identificación para el peritaje por parte del personal policial; es así como debe ser efectuado conforme a las pautas elaboradas por los Procedimientos Informáticos.

Es de especial importancia la utilización de procedimientos rigurosos al momento del secuestro del material y de aquellos medios tendientes a garantizar la autenticidad e integridad de la evidencia digital. El requerimiento judicial deberá ser efectuado completando la información para Requerimiento de Servicios estándar; aprobados para una mayor y eficaz solución.

Es así que utilizaremos los conocimientos y recursos obtenidos en el Curso de seminario de graduación: “Computación Forense”. Por lo cual se nos ha asignado este caso de estudio.

1.3. DESCRIPCIÓN DEL PROYECTO

Draft Complete, Inc. es una microempresa especializada en el desarrollo artístico de alta joyería. Debido al alto valor del inventario en toda la sede de esta empresa, cada empleado es revisado minuciosamente al salir del edificio. Bruce Armiter es un empleado de que dejo de trabajar porque un guardia de seguridad descubrió una tarjeta de memoria entre sus

pertenencias. Específicamente, Armiter escondió la tarjeta en un dentro de sus zapatos de atletismo. El guardia de seguridad entregó la tarjeta de memoria a un oficial de policía local, por una “corazonada” que él tenía. El guardia de seguridad cree que Armiter está haciendo contrabando de información, como imágenes de nuevos productos y mapas del edificio y los está vendiendo al mejor postor. Los planos de distribución del edificio serían muy útiles para los ladrones. Un ladrón tendría tiempo para planificar mejor su ataque y extraer parte del valioso inventario en la sede.

Su trabajo consiste en probar o refutar las pretensiones del guardia de seguridad. El análisis que se realizará está orientado a alcanzar los siguientes objetivos:

1.3.1. ObjetivoGeneral

Analizar la evidencia entregada haciendo uso de técnicas de análisis de computación forense y el uso de herramientas adecuadas para poder entregar un informe claro y convincente de lo que se sospecha en torno al acusado.

1.3.2. Objetivos Específicos

- Definir la metodología adecuada para lograr nuestro objetivo.
- Entender la situación del caso que debemos analizar y dar la solución con un respectivo análisis lógico.
- Verificar el tipo de evidencia que nos han proporcionado para el posterior análisis.
- Realizar la documentación adecuada de todas las pistas encontradas en el caso.
- Preservar la integridad de la evidencia, para que no exista ninguna manipulación de la evidencia original.
- Preservar la cadena custodia.
- Realizar copias de la evidencia original, para realizar todas las tareas de análisis y recuperación de información.
- Preservar la evidencia en un lugar seguro con la temperatura y ubicación adecuada.
- Escoger la herramienta adecuada para el análisis.
- Recuperar la mayor cantidad de información.
- Realizar un estudio de toda la información encontrada a través de una evaluación realizada al investigador forense.
- Realizar un reporte del caso.
- Llegar a una conclusión en base a las evidencias.

1.4. METODOLOGÍA

Para la ejecución y el análisis de nuestro proyecto, utilizamos un entorno de trabajo con una PC, en la cual instalamos una distribución de Linux basada en Ubuntu 10.04 que es CAINE 2.0 para el análisis de nuestra imagen forense.

Entre las tareas realizas fueron:

- ✓ Determinar el incidente realizado en el caso.
- ✓ Evaluar el caso.
- ✓ Extracción de Información de la imagen Forense.
- ✓ Cálculo de las líneas de Tiempo.
- ✓ Cálculo de hashes.
- ✓ Integridad de la Imagen Forense.
- ✓ Verificación de esteganografía
- ✓ Documentación de todas las pistas encontradas.
- ✓ Realizar un reporte o documento que certifique que la solución encontrada tiene todo el análisis realizado en forma coherente.
- ✓ Conclusión y recomendaciones.

Cada una de estos pasos o tareas realizadas se explican con mayor detalle en los próximos capítulos.

CAPÍTULO 2

MARCO TEÓRICO

Se basa en parte Teórica, en donde su principal característica es el desarrollo conceptual de la Computación forense.

2.1. COMPUTACIÓN FORENSE

Informática forense, computación forense, análisis forense digital o examinación forense digital es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal. [15] [20]

"Según el FBI, la informática (o computación) forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional.

Dichas técnicas incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos". [16]

2.2. DELITOS INFORMÁTICOS

Según las Naciones Unidas tenemos los siguientes delitos informáticos más conocidos que son:

- Fraudes cometidos mediante manipulación de ordenadores.
- Manipulación de programas.
- Manipulación de datos de salida.
- Fraude efectuado por manipulación informática o por medio de dispositivos informáticos.
- Falsificaciones informáticas.
- Sabotaje informático.
- Virus, gusanos y bombas lógicas.
- Acceso no autorizado a Sistemas o Servicios de Información.

- Reproducción no autorizada de programas informáticos de protección legal.
- Producción / Distribución de pornografía infantil usando medios telemáticos.
- Amenazas mediante correo electrónico.
- Juego fraudulento on-line.

2.3. ATAQUES INFORMÁTICOS

Un ataque informático es un método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático(ordenador, red privada, etcétera). [22]

Entre los ataques más conocidos tenemos:

- **Los Insiders**: Son operadores o programadores que se aprovechan de los accesos y permisos que tienen para modificar archivos.

- **Los Outsiders:** ingresan a las redes mediante el uso de una contraseña valida, que pudo haber sido extraída por algún método o mediante intentos de "fuerza bruta".

A medida que pasan los años, las técnicas para encontrar vulnerabilidades en los sistemas y explotarlos son cada vez más sofisticadas. Podemos diferenciar distintos tipos de ataques. Como por ejemplo los ataques activos que realizan cambios en la información y sistemas afectados. y los ataques pasivos que se limitan a acceder a la información. [7]

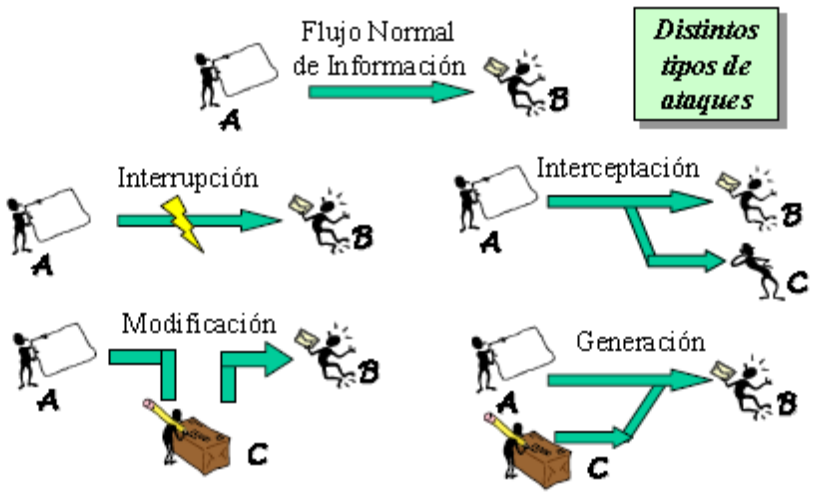


Figura 2.3-1 Diversos Ataques Informáticos

Tomado de: www.mundointernet.es/IMG/pdf/ponencia95.pdf

2.4. CLASIFICACIÓN DE LOS INTRUSOS EN LAS REDES

A continuación se describen los intrusos en las redes más conocidos en la actualidad: [21]

2.4.1. Hackers

Son intrusos que en su gran mayoría realizan actividades como ingresar a los sistemas como pasatiempo o retos, sin provocar daños en ellos.

Sin embargo, hay que tener en cuenta que pueden tener acceso a información confidencial, por lo que su actividad está siendo considerada como un delito varios países.

“El perfil típico de un hacker es el de una persona con amplios conocimientos de informática y de Internet, son auténticos expertos en varios lenguajes de programación, arquitectura de ordenadores, servicios y protocolos de comunicaciones, sistemas operativos, etcétera, que invierte un importante número de horas a la semana a su afición.**”** [21]

2.4.2. Crackers

Estas personas son intrusos que no solo tienen interés en ingresar a las redes y sistemas con el fin de beneficiarse de forma ilegal de la información sino también de hacer daños en ellos. Ya sea por motivos económicos, políticos, religiosos, etc.

2.4.3. Sniffers

Personas que se dedican a interceptar y descifrar los paquetes que son transmitidos vía internet.

2.4.4. Phreakers

Son aquellos que tratan de explotar vulnerabilidades en las redes telefónicas para obtener llamadas gratis.

2.4.5. Spammers

Son aquellos que tratan de introducir vía internet, miles de mensajes que no han sido solicitados, provocando fallos en los servidores, infección de equipos, sobrecarga de buzones de correo, correos de estafa, etc.

2.4.6. Piratas Informáticos

Son aquellos que realizan copias de programas y demás contenidos digitales, violando así las leyes de propiedad intelectual.

2.4.7. Creadores de virus y programas dañinos

“Se trata de expertos informáticos que pretenden demostrar sus conocimientos construyendo virus y otros programas dañinos, que

distribuyen hoy en día a través de Internet para conseguir una propagación exponencial y alcanzar así una mayor notoriedad.” [21]

2.4.8. Que son los Lamers

Personas llamadas “novatas” en cuanto a la utilización de herramientas informáticas que pueden ser utilizadas para realizar algún tipo de ataque a las redes o sistemas, pero que intentan realizar alguna acción con la ayuda de información obtenida en internet o libros, que en muchos casos pueden llegar a provocar daños.

2.4.9. Amenazas del personal interno

Sin duda alguna uno de los ataques más comunes son aquellos realizados desde el interior de nuestra propia empresa, ya sea por simple curiosidad sin el ánimo de causar ningún tipo de daño o con la intención de causarlo; por motivos como despidos, inconformidad, o deslealtad.

2.4.10. Ex - Empleados

Generalmente al ser despedido, el empleado trata de “vengarse” de su antigua empresa, valiéndose de la información que este aún posee, ya

sea ingresando nuevamente a los sistemas a causar daños o vendiendo la información a la competencia.

2.4.11. Intrusos Remunerados

Son personas con altos conocimientos informáticos y técnicas de intrusión en sistemas, los cuales prestan sus servicios a terceros para sustraer información de otras empresas o causar daños a los sistemas y redes.

2.5. MOTIVACIONES DE LOS ATACANTES

"El FBI ha acuñado el acrónimo MICE para resumir las distintas motivaciones de los atacantes e intrusos en las redes de ordenadores: Money, Ideology, Compromise y Ego (Dinero, Ideología, Compromiso y Autorrealización personal)". [21]

- ✓ **Consideraciones Económicas:** Realizar intrusiones a los sistemas ya sea por pedido de terceros los cuales pagan por ese servicio o realizar sobornos con la información obtenida.

- ✓ **Diversión:** Personas con alto conocimiento que realizan este tipo de actividades por pasatiempo.

- ✓ **Ideología:** Realizan ataques a ciertos portales o entidades por no compartir sus mismas ideas

- ✓ **Autorrealización:** La búsqueda de reconocimiento social y de un cierto estatus dentro de una comunidad de usuarios.

2.6. DEFINICIONES

Dentro de lo forense encontramos varias definiciones, tales como:

2.6.1. Computación Forense

"Es una serie metódica de técnicas y procedimientos de obtención de pruebas, desde los equipos de computación, diversos dispositivos de almacenamientos y medios de comunicación digitales, que se pueden presentar en un tribunal de justicia en un formato coherente y significativo". [23]

2.6.2. Forense Digital

Forma de aplicar los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, con el fin de apoyar a la administración de justicia en su lucha contra los posibles delincuentes o como una disciplina especializada que procura el

esclarecimiento de los hechos (¿quién?, ¿cómo?, ¿dónde?, ¿cuándo?, ¿por qué?) de eventos que podrían catalogarse como incidentes, fraudes o usos indebidos bien sea en el contexto de la justicia especializada o como apoyo a las acciones internas de las organizaciones en el contexto de la administración de la inseguridad informática. [17]

2.6.3. Cadena de Custodia

Es aquella documentación que se realiza en el momento de la escena del crimen, en la cual nos proporciona establecer un registro de todas las evidencias encontradas. Como resultado de esta documentación nos permitirá garantizar la integridad de todas las pruebas halladas, asegurando que la información no sea manipulada desde el momento en que se recoge la información hasta la entrega del caso a la corte.

2.6.4. Imagen Forense

Es una copia idéntica que se realiza al medio de almacenamiento o del dispositivo original. En esta copia se almacenan todos los datos exactamente iguales que el original, lo que nos permite realizar los respectivos análisis, experimentos o recuperación de la información borrada mediante el uso de técnicas forenses.

2.6.5. Análisis del Archivo

Realiza una exploración detalladamente inteligente de cada uno de los archivos hallados, esta información es de vital importancia para el investigador, porque nos proporciona toda la identificación adjunta que se encuentra registrada en los archivos que se desea conseguir todos sus antecedentes para su posterior análisis.

2.7. PASOS DE AUDITORÍA FORENSE

A continuación se describirán todo el proceso al realizar una auditoria forense:

2.7.1. Identificación

Nos permite conocer cómo se estableció el incidente ocurrido para su respectiva validación de la naturaleza de los acontecimientos reportados. Estas series de sucesos identificados llevan a la toma de decisiones y al referente levantamiento de información del caso. Realizando una determinada investigación optima que nos ayude a proporcionar las pistas efectivas, al momento de realizar todos los pasos apropiados en la búsqueda del resultado auténtico.

2.7.2. Preservación

La identificación de la evidencia debe ser preservada para mantener su integridad.

En el momento de realizar la respectiva generación de la imagen forense nuestra evidencia original deberá ser exactamente idéntica a la copia, lo que nos permitirá preservar la cadena de custodia y toda la documentación concerniente al caso.

Mediante la utilización de software o hardware inteligentes se reproducen las copias de las imágenes forenses, en las que se realiza el respectivo copiado total de los datos almacenados, con la finalidad de no manipular, ni sobrescribir la información.

2.7.3. Análisis

Este proceso se basa en la examinación de todos los elementos encontrados de la copia de la imagen forense original, en base a la realización de métodos eficientes de búsquedas e investigaciones sobre todas las pistas que se van acumulando hasta descubrir el resultado apropiado que nos lleve al objetivo propuesto.

Cada dato encontrado es minuciosamente analizado y recuperado, porque en cada uno de ellos guarda información transcendental para el investigador forense.

2.7.4. Presentación

Este proceso incluye toda la recolección de los datos encontrados y que se fueron acumulando a medida que el análisis forense avanzaba. Una gran ayuda es la bitácora, porque en ella se halla todas las respuestas encontradas para la debida solución del caso. La explicación debe ser proporcionada por diversos procesos, así como el investigador forense debe incluir en un reporte el método que utilizo, todas las pistas encontradas y que fueron analizadas por herramientas forenses, esta presentación de datos deberá ser concreta y confiable con el propósito de garantizar la cadena de custodia.

2.8. IMPORTANCIA DE LA INFORMÁTICA FORENSE

El valor de la integridad de nuestra información son de vital importancia para el desarrollo de las organizaciones, pero los fraudes informáticos son cada vez más importantes para los criminales en busca de alguna brecha de seguridad, en la cual es posible de que estas organizaciones se vean perjudicadas, estos hechos son reportados en busca de alguna solución y es donde los objetivos, técnicas y procedimientos de la informática forense se vuelve de gran eficacia e importancia en el mundo digital.

2.9. OBJETIVOS DE LA INFORMÁTICA FORENSE

- Realizar un análisis preciso y exhaustivo de la evidencia digital, recolectando todos los datos que vamos a examinar.
- Determinar y localizar mediante un procedimiento estructurado e investigativo la naturaleza del suceso ocurrido por el criminal.
- La efectiva aplicación en la búsqueda de la verdad en materia penal, civil y asuntos sociales con el fin de que la injusticia no se vuelva a repetir.

2.10. USOS DE LA INFORMÁTICA FORENSE

Existen varios usos de la informática forense, muchos de estos usos provienen de la vida diaria, y no tienen que estar directamente relacionados con la informática forense:

- ✓ **Prosecución Criminal:** Evidencia incriminatoria puede ser usada para procesar una variedad de crímenes, incluyendo homicidios, fraude financiero, tráfico y venta de drogas, evasión de impuestos o pornografía infantil.

- ✓ **Litigación Civil:** Casos que tratan con fraude, discriminación, acoso, divorcio, pueden ser ayudados por la informática forense.

- ✓ **Investigación de Seguros:** La evidencia encontrada en computadores, puede ayudar a las compañías de seguros a disminuir los costos de los reclamos por accidentes y compensaciones.

- ✓ **Temas corporativos:** Puede ser recolectada información en casos que tratan sobre acoso sexual, robo, mal uso o apropiación de información confidencial o propietaria, o aún de espionaje industrial.

- ✓ **Mantenimiento de la ley:** La informática forense puede ser usada en la búsqueda inicial de órdenes judiciales, así como en la búsqueda de información una vez se tiene la orden judicial para hacer la búsqueda exhaustiva. [17]

2.11. HISTORIA DE LA COMPUTACIÓN FORENSE

Este es el resumen a cerca de la computación forense: [17]

- Francis Galton (1822-1911)

  Hizo el primer estudio de huellas dactilares registradas.

- Leone Lattes (1887-1954)

  Descubre los grupos sanguíneos (A, B, AB y 0)

- Calvin Goddard (1891-1955)

Armas de fuego permitidas y la comparación de bala para la resolución de muchos casos judiciales pendientes

- Albert Osborn (1858-1946)

  Desarrollo de las características esenciales de examen de documentos

- Hans Gross (1847-1915)

  Utilización de un estudio científico para dirigir las investigaciones penales

- FBI (1932)

  Un laboratorio se creó para proporcionar los servicios forenses a todos los agentes sobre el terreno y otras autoridades de la ley en todo el país.

2.12. PERFIL DEL ESPECIALISTA

Figura 2.12-1 Perfil del Especialista

Tomado de: www.profesiones.com.mx/computo_forense.htm

Estas son las características que debería tener un Especialista Forense: [19]

- Debe ser un apasionado de la tecnología y respetuoso de ella.
- Ser una persona paciente.
- Gusto por la investigación.

Para poder realizar con éxito su trabajo, el investigador nunca debe olvidar:

- Ser imparcial. Solamente analizar y reportar lo encontrado.
- Realizar una investigación formal con conocimiento y experiencia.
- Mantener la cadena de custodia (proceso que verifica la integridad y manejo adecuado de la evidencia).
- Documentar toda actividad realizada

El especialista debe conocer también sobre:

- Técnicas de intrusión que utilizan los crackers y hackers para extraer información a los sistemas de cómputo.
- Desarrollo de los exploits (vulnerabilidades), esto le permite al informático forense saber qué tipo de programas se pondrán de moda, para generar una base de estudio que le permita observar patrones de comportamiento. [19]

2.13. LABOR DEL ESPECIALISTA EN CÓMPUTO FORENSE

Figura 2.13-1 Labor del Especialista en Cómputo Forense

Tomado de: www.profesiones.com.mx/computo_forense.htm

Apoyado en amplios conocimientos en informática y mediante la utilización de la tecnología más elaborada, el especialista en cómputo forense puede acceder a cualquier equipo con memoria para descubrir robos de secretos industriales, ciberfraudes financieros, pornografía infantil, secuestros o cualquier otra actividad delictiva que haya dejado huella física en el equipo.[19]

2.14. PREVENCIÓN DE PÉRDIDA DE DATOS

La mayoría de las empresas pequeñas, medianas y grandes, almacenan diferentes tipos de información, muchas de estas informaciones son de vital importancia para la empresa, pero los empleados representan ser un gran enemigo para las organizaciones que no manejan las debidas políticas de seguridad. Frecuentemente los empleados hacen un mal uso de la información confidencial y en muchas ocasiones esto tiene un impacto negativo y de mucho riesgo para las empresas.

Como resultado de la falta de seguridad, los empleados realizan actividades personales a través de la web o mediante la conexión de dispositivos de medios extraíbles, lo que puede provocar con mucha facilidad que la fuga de información sea exitosa.

Una gran solución es DLP, porque esta previene el robo de información y además permite asignarles a los empleados determinados accesos a la información, lo que nos proporciona una reducción eficaz en la fuga de información no autorizada y nos permite asegurar la integridad de la información.

2.14.1. Ventajas de DLP

- ✓ Asegurar la integridad de la información confidencial.
- ✓ Podemos identificar aquellos usuarios que están realizando un mal uso de la información o que están tratando de acceder a un archivo o directorio que es confidencial.
- ✓ La administración es totalmente centralizada, de tal manera que provee una alerta inmediata al administrador, para que el rápidamente pueda identificar y bloquear al usuario que está intentando acceder.

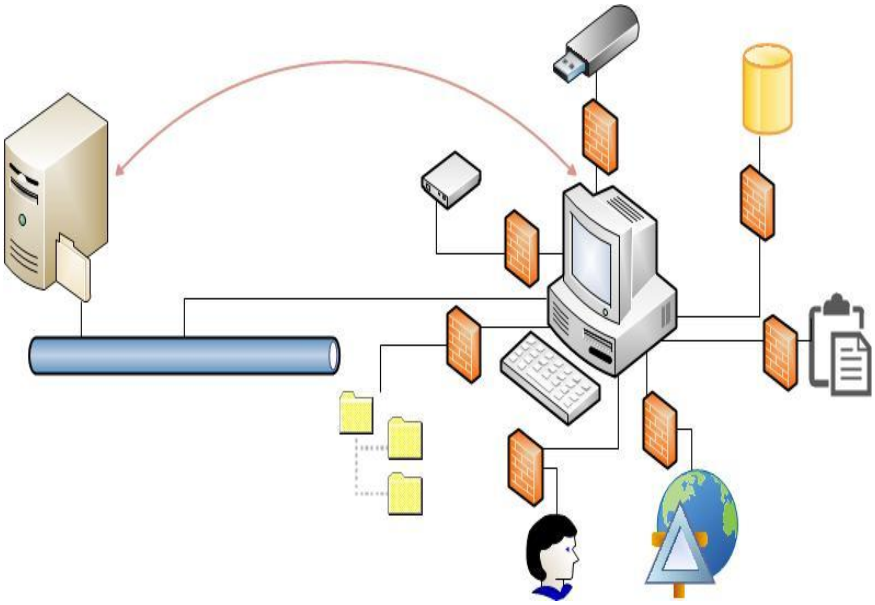


Figura 2.14.1-1 Prevención de pérdidas de datos.

2.15. CONTROL DE ADMISIÓN DE LA RED

Nos permite integrar políticas de seguridad en nuestros equipos informáticos de nuestra red, es decir que nos proporciona un control seguro para aquellos clientes que no están autorizados, denegando totalmente su acceso, si estos no cumplen las políticas implementadas en los dispositivos de comunicación.

NAC nos permite corregir aquellos errores de normas de seguridad que existen en determinados nodos de nuestra red, proporcionándonos una solución apropiada, en empresas que necesitan de una infraestructura de red segura, eficiente y de calidad. [11]

CAPÍTULO 3

HERRAMIENTAS

Este capítulo se basa en las herramientas de software utilizadas para el posterior análisis de nuestra imagen forense.

3.1. CAINE

Significa (Computer Aided Investigative Environment), es una distribución GNU/LINUX diseñado para Investigaciones Forense, en la cual le proporciona los investigadores llevar a cabo métodos óptimos en un análisis forense.

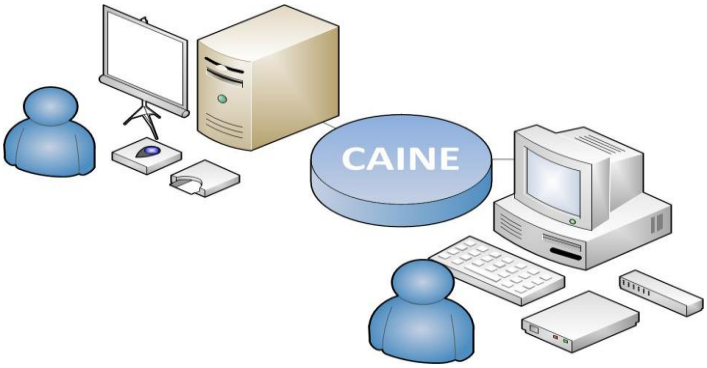


Figura 3.1-1 Investigadores Forenses unidos con Caine

3.1.1. PROPÓSITO DE CREACIÓN

El propósito de la creación de Caine se produjo como un proyecto para los investigadores que realizaban investigaciones forenses en sus diferentes casos a resolver.

Este proyecto fue creado con intensión de llegar a ser una distribución de alto rendimiento en el desarrollo forense con una alta capacidad de escalabilidad en el futuro para sus nuevas versiones. [5]

3.1.2. OBJETIVOS DE CAINE

- ✓ Ofrece un entorno amigable que le proporciona al investigador forense toda la ayuda necesaria en el momento de resolver un caso.

- ✓ Introducir herramientas forenses de alto desempeño, en donde contengan características importantes y se resalten de otras herramientas forenses en la actualidad.
- ✓ Introducir todo su código dentro de un LiveCD, en la cual pueda instalarse sin ningún tipo problemas para todos aquellos investigadores o personas que quieran hacer uso de esta importante herramienta forense.
- ✓ Prolongar su existencia para seguir siendo una herramienta de gran importancia en la investigación digital.
- ✓ Basarse en una distribución ya conocida como es el caso de LINUX, la cual funcione en óptimas condiciones.
- ✓ Comprometerse plenamente como una herramienta forense digna de ser usada como una filosofía en la investigación digital.
- ✓ Ser una herramienta organizada en su configuración, Interfaz e Instalación para realizar las tareas que conduzcan hacia el objetivo propuesto.
- ✓ Tener compatibilidad con su instalación al momento de efectuarse en arquitecturas nuevas.

3.1.3. VENTAJAS DE CAINE

- ✓ Es una distribución de código abierto que puede modificar sin ningún problema ya que no es considerado como robo de propiedad intelectual o propósitos para la piratería.
- ✓ No tiene ningún costo económico para adquirirlo.
- ✓ Está disponible en su página oficial (http://www.caine-live.net/), lo cual representa una gran ventaja al momento de conseguirlo.
- ✓ Su instalador no es pesado y lo podemos almacenar en nuestro disco duro, memoria flash o CD, debido a que está en un formato ISO.
- ✓ En su página oficial nos brinda toda la ayuda necesaria que necesitamos conocer para su uso eficiente.
- ✓ Fácil de utilizar, ya que contiene una interfaz gráfica interactiva y amigable.
- ✓ Contiene una fácil interoperabilidad en su entorno al momento de realizar una investigación forense.
- ✓ Contiene una gran variedad de herramientas útiles, de fácil uso y grandes beneficios.
- ✓ Se puede manejar en línea de comandos o haciendo uso de su interfaz gráfica.
- ✓ No afecta la parte del rendimiento en el sistema, porque está diseñado para soportar nuevas arquitecturas.

3.1.4. INTERFAZ GRÁFICA

Su diseño en su gráfica es muy amigable y de fácil uso, es como si navegáramos en cualquier interfaz gráfica de LINUX. Además contiene iconos y ventanas muy vistosas, con un diseño único para esta distribución propuesta para investigaciones forenses.

Figura 3.1.4-1 Interfaz Gráfica de Caine

3.1.5. INTERFAZ LINEA DE COMANDO

Su interfaz en línea de comando es muy simple y fácil de usar, debido a que es basada en LINUX y además proporciona manuales de ayuda acerca de la utilización de sus comandos.

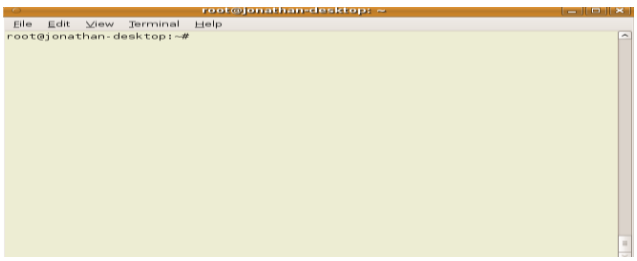


Figura 3.1.5-1 Interfaz Línea de Comando de Caine

3.2. AUTOPSY

Es una herramienta forense que nos proporciona Caine, diseñado para el análisis forense de los archivos en sistemas operativos Windows y Unix.

Es una herramienta de gran utilidad para los investigadores forenses, ya que cuenta con diferentes opciones que nos proporciona realizar un análisis óptimo en volúmenes pertenecientes a la computadora para llegar a una solución en un análisis forense.

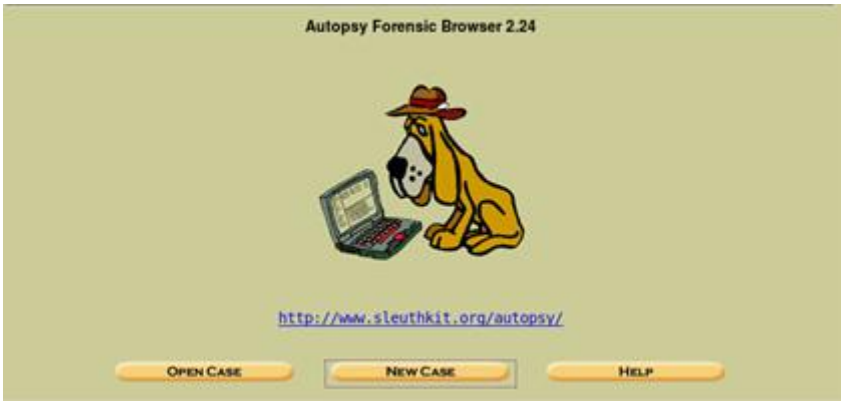


Figura 3.2-1 Interfaz Gráfica de Autopsy

3.2.1. FUNCIÓN DE AUTOPSY

- ✓ Autopsy funciona como un navegador web en donde viene instalado por defecto en Caine.
- ✓ Funciona perfectamente en sistemas operativos Linux y en sus diferentes distribuciones como es el caso de Caine.

- ✓ Con esta gran herramienta podemos analizar una imagen forense, con el propósito de encontrar alguna pista que nos sirva de utilidad en el caso a resolver.

3.2.2. MODOS DE AUTOPSY

Esta herramienta dispone de eficientes modos para realizar una investigación forense, estos son los siguientes modos:

- Files
- Meta Data
- Data Unit
- Keyword Search
- Image Details
- Image Integrity
- File Activity Timelines
- File Type Categories
- Report Generation

3.2.2.1. Files

Este modo analiza todos los directorios y archivos contenidos en una imagen forense, en la cual podemos analizar todos los archivos eliminados por equivocación o intencionalmente por el usuario.

3.2.2.2. Metadata

Este modo le permite al investigador forense realizar un análisis de metadatos sobre las estructuras del disco que contienen detalles de los diferentes archivos, como los tiempos en que se accedió al archivo y las referencias de ese metadato correspondiente al archivo que se está analizando.

Este modo es muy útil en la recuperación de los datos que han sido borrados y podemos tener una vista previa de los detalles de ese archivo.

3.2.2.3. Data Unit

Cada sistema operativo contiene su propio sistema de archivo, en la cual Autopsy llama a esta opción unidad de datos. Esta unidad de datos puede representar a un fragmento o clúster.

Este modo nos permite visualizar el contenido de una unidad de datos que están en distintas áreas del disco en donde se encuentran almacenados los datos. Este modo es muy útil cuando se está comenzando a recuperar los archivos y analizar los archivos que han sido borrados. Además se puede establecer un filtro en la visualización de los datos como por ejemplo: podemos filtrar los datos en formatos de String, Hexdump o ASCII y generar un reporte por cada uno de estos filtros establecidos.

3.2.2.4. Keyword Search

Este modo nos permite la utilización de búsquedas a través de un String establecido por el investigador.

Es muy útil en la recuperación de datos borrados, por lo que disminuye el tiempo de búsquedas y le facilita al investigador buscar una cadena con referencia a un archivo, si esta cadena hace match con el archivo almacenado, Autopsy mostrará la ubicación original del archivo.

3.2.2.5. Image Details

Este modo nos permite efectuar datos generales de la imagen forense por cada diferente sistema de archivo utilizado en la imagen.

3.2.2.6. Image Integrity

La importancia de la integridad de la imagen es de gran utilidad en un análisis forense, porque demuestra que el investigador forense no ha manipulado la evidencia. Autopsy proporciona este modo para calcular en MD5 la integridad de la imagen.

3.2.2.7. File Activity Timelines

Este modo nos facilita el análisis en una investigación forense, porque nos permite la creación de líneas de tiempo que nos van a ayudar a identificar los lugares sospechosos que debemos analizar, en la cual nos

permite observar los archivos que fueron modificados o accedidos por última vez, en donde Autopsy crea estas líneas de tiempo que le proporciona visualizar la actividad de estos archivos dependiendo del sistema de archivo que se esté utilizando.

3.2.2.8. File type Categories

Este modo es de gran ventaja en el análisis de imágenes forenses que utilizan sistemas de archivos muy extensos. Con este modo se pueden identificar los archivos analizados y establecer un orden según el tipo de archivo.

Además permite ordenar archivos que contengan sus hashes validos e inválidos, así como también aquellos archivos que contengan una extensión desconocida para el tipo de archivo.

3.2.2.9. Report Generation

Este modo le permite al investigador llevar una bitácora de todas las pistas encontradas para su posterior análisis. Este modo está presente en la navegación de los otros modos anteriores, en la cual se pueden generar reportes de acuerdo a nuestra búsqueda. Dichos reportes indican la fecha, el nombre del investigador, los cálculos en md5 y muchas otras informaciones.

3.2.3. Ventajas de Autopsy

- ✓ Contiene una interfaz web muy amigable y fácil de usar.
- ✓ Trabaja en sistemas operativos Linux, lo que significa que esta herramienta es gratuita sin ningún costo.
- ✓ Su diseño estructural es poderosamente eficiente.
- ✓ Incluye un manual de ayuda, acerca de su uso y como saber sus diferentes opciones.
- ✓ Permite recuperar archivos borrados a través de una imagen forense.
- ✓ Soporta el análisis de diferentes sistemas de archivos tales como (NTFS, FAT, UFS1/2, Ext2/3).
- ✓ Es eficiente para realizar un análisis forense porque cuenta con distintos modos en su configuración.
- ✓ Permite la validación de la integridad de la imagen, verificando los hashes en md5.
- ✓ Permite la generación de reportes que son de gran utilidad en hallar las pistas encontradas y realizar su respectivo análisis.
- ✓ Establece búsquedas de archivos profundamente en todo su sistema de archivos.
- ✓ Fácil de conseguir si no viene por defecto instalado, porque contiene una página web (http://www.sleuthkit.org/autopsy/) en donde se puede descargar el archivo o se lo puede instalar a través de línea de comando.

3.3. AIR

Viene de las siglas Automated Image and Restore, diseñada para generar imágenes forenses que se extraen de los medios de almacenamiento.

Figura 3.3-1 Interfaz Gráfica De AIR

3.3.1. Características de Air

- ✓ Compatible con dispositivos IDE, SCSI, CD-ROM y unidades de cinta SCSI.
- ✓ Se puede utilizar un formato de imagen en dd o dc3dd.
- ✓ Proporciona un Log al momento de finalizar la copia.
- ✓ Proporciona una ventana adicional para saber en qué porcentaje va la copia para su finalización. [1]

- ✓ En imagen que son extremadamente pesadas, se puede realizar una división de esa imagen en múltiples segmentos.

3.3.2. Ventajas de Air

- ✓ Es una herramienta gratuita disponible en la web sin ningún costo para descargarla.
- ✓ Su instalación es sumamente sencilla.
- ✓ Existen muchos tutoriales disponibles en la web para saber el uso esta herramienta.
- ✓ Posee toda la interpretación del comando dd, fácil para el uso de aquellas personas que se les hace complicado trabajar en línea de comandos.
- ✓ Posee un entorno grafico sencillo, con un diseño atractivo para el usuario.
- ✓ Se requieren conocimientos básicos en su uso, debido a que esta herramienta es fácil de usar.
- ✓ Se puede utilizar para realizar una imagen forense o realizar una copia de seguridad de los archivos.
- ✓ Soporta extensiones para la copia de imagen tales como: .dd, .img, .iso.
- ✓ Realiza una validación de integridad de la imagen, por que utiliza una comparación de hashes en MD5 o SHA1/256/384/512.

3.4. STEGSECRET

Desarrollada por Neils Provos, Es un proyecto (GNU/GPL) que proporciona la detección automática de diferentes herramientas estenográficas utilizadas hoy en día.

Esta herramienta permite detectar diferentes técnicas estenográficas y permite realizar un estegoanálisis de la información para poder determinar si esa información está alterada con alguna herramienta estenográfica.

Además esta importante herramienta no solo sirve para la detección que se encuentra embebida dentro una información también está orientada a la implementación de diferentes funciones que permiten poder realizar de manera automática un conjunto de procedimientos estegoanalíticos.

Tiene incorporado en algoritmos que nos permite detectar la información que esta oculta, como existen diferentes procedimientos para realizar esteganografía, y un medio general es la utilización de formato JPEG en cual podemos ocultar información dentro de este formato. Gracias a su eficiente algoritmo es capaz de realizar esta serie de procedimientos, por lo que la hace una herramienta de especial interés para los estudiantes, universidades, investigadores forenses, ya que permite realizar tareas estenográficas de diferentes medios de información. [3]

3.4.1. Objetivos de Stegsecret

Recopilación de información acerca de diferentes actos estenográficos.

Implementación de toda la información que se adquiere para proporcionar un estudio optimo que facilite la detección de una forma automática algún tipo de información oculta en diferentes medios digitales tales como: imágenes, audio y video.

Este proyecto desea convertirse en una importante herramienta de estegoanálisis, permitiendo incorporar una prevención óptima que ayude a la detección de numerosas herramientas estenográficas.

3.4.2. Herramientas Detectadas

Estas son herramientas utilizada para realizar actos estenográficos, en la cual StegSecret permite su detección:

- ✓ Camouflage V1.2.1
- ✓ inThePicture V2
- ✓ JPEGXv 2.1.1
- ✓ Pretty Good Envelope v1.0
- ✓ Appendx
- ✓ Steganography v1.6.5
- ✓ inPlainView
- ✓ DataStash v1.5 y V1.0

3.4.3. Funciones Implementadas

A continuación se mencionan las funciones implementadas que utiliza stegsecret para su correcto funcionamiento: [4]

- ✓ Función de detección de patrones fijos
- ✓ Funciones Forenses
- ✓ Funciones de Reconocimiento
- ✓ Función avanzada de imágenes digitales
- ✓ Función de clasificación

3.4.3.1. Función de detección de patrones fijos

Proporciona la detección de rastros dejados por herramientas estenográficas, en la cual estas herramientas utilizan **LSB**, que permiten la ocultación de información al final del archivo.

3.4.3.2. Funciones forenses

Proporciona un acceso a bajo nivel de diferentes sistemas de archivos tales como FAT32, NTFS, EXT 2 y EXT 3, en la cual provee la detección que se encuentra oculta en alguna fragmentación interna de un fichero, permitiendo la recuperación de archivos borrados.

3.4.3.3. Funciones de reconocimiento

Permite un reconocimiento de diferentes formatos de ficheros tales como BMP, GIF y JPEG. Dichos formatos son utilizados en la ocultación de información al final de un archivo (EOF).

3.4.3.4. Función avanzada de imágenes digitales

Sus eficientes algoritmos estegoanáliticos proporcionan una identificación de información oculta en imágenes digitales, como por ejemplo:

- ✓ Identifica la ocultación basada en LSB de una imagen BMP.
- ✓ En los índices y pixeles de los archivos GIF.
- ✓ **DCTs** de una imagen JPEG.

3.4.3.5. Función de clasificación

Proporciona un análisis de directorios cache de un servidor Proxy-Web e identifica algún tipo de información oculta en dominios Web.

3.4.4. Ventajas de Stegsecret

- ✓ Su implementación fue diseñada en java en un entorno de GNU/Linux, es decir es una herramienta de software libre.
- ✓ Proporciona su propio sitio web, en la cual podemos adquirirla.Posee una interfaz gráfica amigable y fácil de usar.

- ✓ Permite la asegurar la integridad de sistemas y la información que se utiliza.
- ✓ Cada día se sigue perfeccionando su estructura, como en la implementación de detección de otras técnicas estenográficas, para mejorar todos sus procedimientos y realizar tareas eficientes.

3.5. XSTEG

Esta es una herramienta estenográfica, utilizada para realizar un estegoanálisis de forma automática solo en imágenes JPEG. Esta herramienta viene incorporada en caine en la cual ejecuta a:

- Stegdect
- Stegbreak

Figura 3.5-1 Interfaz Gráfica De XTEG

3.5.1. Stegdect

Esta es una herramienta óptima en la detección de imágenes que contengan algún contenido estenográfico. Al seleccionar esta opción rápidamente realizará una detección eficiente de imágenes que contengan algún texto oculto. Actualmente Stegdetect puede detectar diversos métodos estenográficos tales como:

- ✓ Jsteg
- ✓ Jphide (Unix and Windows)
- ✓ Invisible Secrets,
- ✓ Outguess 01.3b
- ✓ F5 (header analysis)
- ✓ AppendX and Camouflage

3.5.2. Stegbreak

Si Stegdetect logra detectar alguna imagen estenográfica este rápidamente ejecuta a Stegbreak en donde su función es lanzar ataques de diccionario contra al archivo y conocer la clave con que está protegida ese archivo.

Puede realizar ataques a diccionario contra:

- ✓ JStegShell
- ✓ JPhide
- ✓ Outguess 0.13.b

3.5.3. Ventajas de XSTEG

- ✓ Es una herramienta de código libre, sin ningún costo.
- ✓ Posee su propio sitio web, en la cual se puede descargar sin ningún costo y posee información de ayuda sobre el uso de esta herramienta.
- ✓ No es una herramienta pesada, su peso es muy liviano.
- ✓ Contiene una interfaz gráfica aceptable y fácil de usar.
- ✓ Esta herramienta siempre ha estado escalando en perfeccionar su arquitectura.
- ✓ Contiene dos herramientas eficientes en su ejecución tales como Stegdetect y Stegbreak, estas dos herramientas se entienden perfectamente en el momento de realizar sus tareas.
- ✓ La herramienta Stegdetect y Stegbreak se la puede utilizar tanto en línea de comando o a través de interfaz gráfica mediante el uso de Xsteg.
- ✓ Mediante su interfaz gráfica realiza una detección automática de las imágenes que uno desea analizar.
- ✓ Es muy útil hoy en día debido a que la esteganografía es un método que cada día escala y cada vez salen muchas herramientas para realizar tareas estenográficas y muchas veces no existen herramientas que realicen un análisis de la información.

3.6. OSFORENSICS

Figura 3.6-1 Imagen de OSForensics

Tomado de: http://www.osforensics.com/

Es un software diseñado para la informática forense que se encarga del análisis de una evidencia original para la respectiva localización de información en los sistemas informáticos y dispositivos de almacenamiento digital.

3.6.1. Estructura de Osforensics

Esta herramienta esta compuesta por un conjunto de modulos programados con total eficiencia que proporcionan una reducción efectiva de resursos del hardware en realizar tareas de análisis de grandes cantidades de datos que contienen los medios de almacenamiento, a través de una búsqueda simple

de todos los archivos que estan alojados en dicha unidad, en cual su estructura la hace una eficaz y potente herramienta.

3.6.2. Características de Osforensics

- Creación de nuevos casos.
- Búsqueda del nombre del archivo.
- Búsqueda avanzada dentro de archivos como word, pdf, etc.
- Permiter notificar una actividad reciente.
- Búsqueda de archivos eliminados.
- Búsqueda de un archivo con extensión desconocida.
- Contiene un Visor de memoria para ver los detalles de los procesos.
- Permite una inspeción profunda de la unidad atraves de un visor.
- Contiene un explorador del Sistema de Archivos.
- Permite la Recuperación de contraseña.
- Permite conocer la información del sistema.
- Verificación o creación de hash.
- Conjuntos de hash para una identificación de archivos sospechosos.
- Preparación de unidad extraible.
- Creación de imagen de disco.
- Permiter realizar una copia forense idéntica a la evidencia original.
- Contiene un Visorde Registro para la exploración de archivos de texto
- Contiene un visor interno que permite ver el contenido de los archivos.

3.6.3. Herramientas de Osforensics

Este software contiene una serie de herramientas gratuitas de gran ayuda que permiten realizar tareas fuera del ambito de la aplicación principal. Estas son las mas importantes herramientas:

- OSFClone
- OSFMount
- ImageUSB

3.6.3.1. OSFclone

Esta herramienta permite crear o clonar imágenes de discos exactas que a la del original de una forma rapida y es idenpendiente del sistema operativo instalado.

Además permite crear imagenes en el formato dc3dd, este formato es ideal para la computación forense debido a que incrementa el nivel de presentación del progreso y errores. Mediante la comparación de hash MD5 o SHA1, permite la verificación de la integridad de la imagen que vamos a clonar. [8]

3.6.3.2. OSFmount

Esta herramienta nos permite montar imágenes de disco de acuerdo a la unidad que le asignemos. De forma predeterminada la imagen de disco se monta en modo lectura para que los archivos de la imagen original no se alteren, además esta herramienta también nos permite la creación de una imagen forense de la RAM. La siguiente tabla muestra los diferentes tipos de imágenes que pueden montar, seguido de todos sus modos compatibles que puede realizar. [12]

Formato	Lectura	Escritura	Montar como dispositivo RAM	Convertir a un archivo de imagen	Extendida	Formato
IMG,DD	✓	✓	✓	✓	✓	✓
ISO,BIN	✓	✗	✓	✓	✗	✗
00n	✓	✓	✓	✗	✗	✓
NRG	✓	✓	✓	✗	✓	✓
SDI	✓	✓	✓	✗	✓	✓
AFF	✓	✓	✓	✓	✗	✓
AFM	✓	✓	✓	✓	✗	✓
AFD	✓	✓	✓	✓	✗	✓
VMDK	✓	✗	✓	✗	✗	✗
E01	✓	✓	✓	✓	✗	✓
S01	✓	✓	✓	✓	✗	✓

Tabla 1 Funciones de OSFMount

Tomado de: http://www.osforensics.com/tools/mount-disk-images.html

3.6.3.3. Image USB

Esta es una excelente utilidad que nos permite grabar una imagen simultáneamente a múltiples unidades de memoria flash. Es capaz de crear imágenes exactas bits por bits en una copia forense.

3.6.4. Ventajas de Osforensics

- ✓ Es un software extramente eficaz para la creación de imágenes forenses.
- ✓ A través de la herramienta OSFMount podemos montar imágenes de disco sin alterar su contenido.
- ✓ Nos permite funcionar como una versión gratuita.
- ✓ Permite una verificación de hashes para la comprobación de la integridad.
- ✓ Fácil de usar y contiene una interfaz gráfica de maravilla.
- ✓ Fácil de conseguir porque posee su propio sitio web.

3.6.5. Desventajas de Osforensics

- ✓ Su versión profesional es de uso exclusivamente comercial y tiene un costo de $ 499

- ✓ Su versión gratuita posee limitaciones.

3.7. ACTIVE@UNERASER – DATA RECOVERY

Figura 3.7-1 Active@Uneraser Imagen Principal

Tomado de: http://www.uneraser.com/

Es una herramienta que trabaja en sistemas operativos Windows a través de DOS y consola.

Permite realizar una búsqueda avanzada de todos archivos alojados en una unidad determinada. Es capaz de recuperar archivos y carpetas de los siguientes sistemas de archivos:

- ✓ FAT12
- ✓ FAT16

- ✓ FAT32
- ✓ NTFS

Además es una herramienta eficaz en la recuperación de información producto de una formateada, ya que realiza un análisis profundo de toda la unidad en busca de toda la información oculta en diferentes cluster del disco.

Esta herramienta permite trabajar con nombre de ficheros muy largos, sobrescribir directamente con los datos restaurados, filtrar la información a buscar y recuperar solo los archivos que cumplan determinados requisitos. Además proporciona un ISO Bootable, en la que se puede ejecutar en el arranque de un CD. [13]

3.7.1. Características importantes de Active@Uneraser

- ✓ Permite reconocer unidades y particiones enteras.
- ✓ Muestra la información completa sobre unidades físicas y lógicas.
- ✓ Admite unidades IDE, ATA, SCSI, SSD, USB, ZIP.
- ✓ Es compatible con particiones de MS-DOS, Windows 95, 98, ME, NT, 2000, XP, Vista, 2008 y 7.
- ✓ Permite trabajar con imágenes de tipo Raw.
- ✓ Permite visualizar archivos en modo hexadecimal de archivos fragmentados, comprimidos, dispersos y cifrados.
- ✓ Muestra el contenido de cualquier sector en la unidad con un visor de disco.

3.7.2. Ventajas De Active@Uneraser

- ✓ Es gratuita, de modo que la podemos utilizar sin necesidad de adquirir una licencia.
- ✓ Fácil de conseguir, ya que posee su propio sitio web en la cual podemos descargarla para hacer uso de ella.
- ✓ Aunque su interfaz es en modo DOS, esta herramienta es muy fácil de usar, porque todas sus opciones son muy legible y posee manuales o información para aprender de su uso.
- ✓ Es una herramienta que contiene dos modos de análisis hacia la unidad uno que es básico (rápido) y uno exhaustivo (lento), este exhaustivo es el más eficaz.
- ✓ Es una herramienta que no consume recursos del sistema y su peso es muy liviano.
- ✓ Permite la detección de unidades que contengan particiones primarias y extendidas eliminadas.
- ✓ Se la puede almacenar en un dispositivo de memoria flash Cd para el arranque en modo DOS.
- ✓ Permite escanear particiones que han sido dañadas producto de un virus o por el MBR.
- ✓ Es compatible con todos los sistemas operativos Windows
- ✓ Es una herramienta que siempre sigue creciendo en sus versiones para tratar de mejorarla y optimizarla.

3.8. PC INSPECTOR FILE RECOVERY

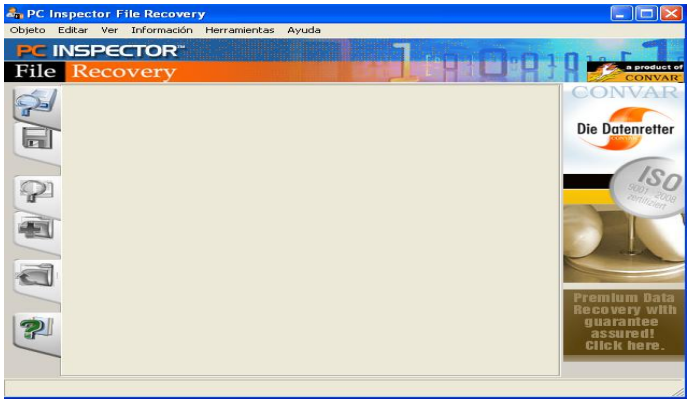


Figura 3.8-1 PC Inspector Imagen Principal

Tomado de: http://www.pcinspector.de/

Es una herramienta que permite establecer la recuperación de información borrada de archivos contenidos en alguna partición de una unidad de almacenamiento. Tiene un Soporte para soporte de sistemas de archivos tales como:

- ✓ FAT 12 /16/32
- ✓ NTFS

Esta fue una de las primeras herramientas gratuitas en la recuperación de información borrada. La información borrada ya sea eliminada por accidente o producto de un formato rápido para esta importante herramienta es muy simple, ya que cuenta con una estructura que es eficaz y veloz al realizar tareas de recuperación y reconocimiento de

información, porque analiza todos los lugares en donde la información está alojada con todas sus referencias. [14]

3.8.1. Caracteristicas de PC Inspector File Recovery

- ✓ Encuentra información automáticamente de particiones que se desea analizar.

- ✓ Si el sector de arranque o FAT ha sido borrado o dañado este permite seguir encontrando información.

- ✓ Recupera los archivos con su respectivo nombre y también con la hora y fecha en que se los creó o modificó.

- ✓ Recupera archivos incluso cuando una entrada de la cabecera no es disponible o cuando una partición ha sido eliminada, este es capaz de recuperar esa información de dicha partición.

- ✓ Posee un escaneo de bajo nivel en cual permite realizar un análisis mas exhaustivo de la información, como así tambien un análisis rápido en búsqueda de información.

- ✓ Permite la observación de todos archivos en sus localizaciones correspondientes a traves de distribuciones de carpetas parecidas al explorador de windows.

3.8.2. Ventajas de Pc Inspector File Recovery

- ✓ Contiene una interfaz gráfica atractiva para el usuario, fácil de usar y de conseguir porque es gratuito y esta disponible en su proprio sitio Web.

- ✓ Consume pocos recursos de hardware en el sistema operativo.

- ✓ Sigue escalando en su arquitectura en cada version que esta disponible.

- ✓ Posee un manual de ayuda para aquellos usuarios que no sepan utilizarla.

- ✓ Nos permite seleccionar una variedad de idiomas que deamos trabajar.

- ✓ Soporta la recuperación de los siguientes formatos: ARJ, AVI, BMP, CDR, DOC, DXF, DBF, XLS, EXE, GIF, HLP, HTML, HTM, JPG, LZH, MID, MOV, MP3, PDF, PNG, RTF, TAR, TIF, WAV

3.8.3. Desventajas de PC Inspector File Recovery

- ✓ No es compatible con Windows vista y 7.

CAPÍTULO 4

DESARROLLO DEL PROYECTO

Este Capítulo se basa en el desarrollo analítico forense, en la cual se refiere a la parte de auditoría forense y utilización de herramientas óptimas que nos permitan realizar tareas apropiadas en busca de la autenticidad de los datos encontrados.

4.1. PROCESO DE ADQUISICIÓN

El proceso de adquisición de la imagen forense ya fue establecido por el profesor, dicha imagen forense fue entregado en un CD como evidencia al grupo respectivo, para su posterior análisis.

La imagen forense adquirida del dispositivo de la memoria flash tiene un formato **.DD**, en la cual procedimos a realizar una serie de pasos para llegar a nuestro objetivo propuesto.

4.2. PRESERVANDO EVIDENCIA

Este es un punto muy importante al momento de realizar una auditoría forense debido a que debemos de mantener la integridad de nuestra evidencia.

Por esta razón en una auditoría forense siempre el análisis y los experimentos realizados para encontrar la solución al caso se trabajan en copias de la evidencia original.

En dichas copias tomadas de la evidencia, nosotros como investigadores forenses podremos realizar sin problemas todas las tareas que creamos convenientes para el análisis forense y así mantendremos integra nuestra cadena de custodia. [16]

Ahora vamos a proceder a realizar una copia de nuestra evidencia original, en la cual vamos a realizar los siguientes pasos:

- Iniciando PC.
- Creación de directorios.
- Montar Evidencia Original.
- Copiar de Evidencia Original.
- Hashes del Respaldo de la Evidencia.
- Moviendo copia a otro directorio.
- Explorar copia de Imagen.
- Hashes de la imagen cf.dd
- Duplicación de la imagen forense.
- Hashes de la copia de la imagen cf.dd

4.2.1. Iniciando PC

- ✓ Como primer paso procedemos a iniciar nuestra PC, en la cual ya tenemos instalado CAINE 2.0 y a continuación se mostrará la siguiente ventana en donde se desplegara una serie de opciones propuestas por Caine en la cual simplemente escogemos la primera opción por defecto.

Figura 4.2.1-1 Iniciando PC

- ✓ Luego solamente esperamos que carguen todos archivos de configuración de Caine.

Figura 4.2.1-2 Cargando Archivos de Configuración

- ✓ Una vez cargado todos los archivos de configuración se mostrara la interfaz grafica de inicio de Caine.

Figura 4.2.1-3 Interfaz de Inicio de CAINE

- ✓ Ahora procedemos a colocar nuestro CD en la cual contiene la evidencia del caso.

Figura 4.2.1-4 Montaje de disco en CAINE

Como podemos ver en la imagen CAINE no monta el CD que hemos colado, por eso esta es una de las ventajas que contiene esta distribución.

4.2.2. Creación de directorios

Ahora procedemos a crear los directorios en donde vamos a guardar nuestra copia de la evidencia original.

1. Primero abriremos una interfaz en línea de comando.
2. Luego accederemos como rooty nos solicitara una contraseña en la cual vamos a digitar **caine**. Para acceder como root digitaremos el comando **sudo su.**
3. Luego simplemente nos cambiamos de directorio del root con el comando **cd /** .

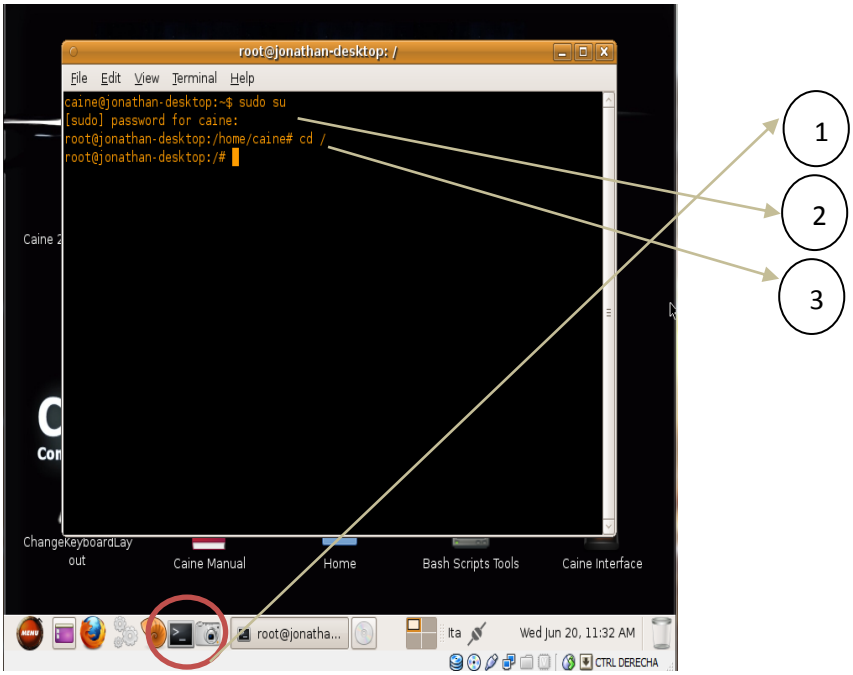


Figura 4.2.2-1 Primeros Pasos en Terminal

4. Ahora procedemos a crear los directorios con el comando **mkdir,** en la siguiente ruta **/home/caine:**

Primero crearemos el directorio **Tesis** haciendo uso de este comando:

✓ mkdir /home/caine/Tesis

Luego crearemos dentro de **Tesis** otro directorio llamado **CopiaImagenForence** con el siguiente comando:

✓ mkdir /home/caine/Tesis/CopiaImagenForence

Podemos ver en la siguiente imagen como se crearon con exito los directorios.

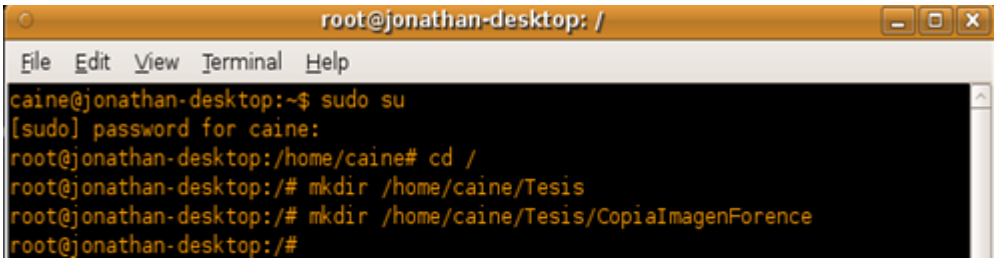


Figura 4.2.2-2 Creación de Directorios

4.2.3. Montar evidencia original

Recordemos que para montar una evidencia, nunca debemos de alterar o manipular nuestra evidencia, ya si lo hacemos nosotros nos veremos perjudicados, porque no hemos conservado la integridad de la evidencia y en el momento de exponer o dar la solución del caso, el otro investigador forense que defiende a la víctima probara que la evidencia no esté manipulada.

Para realizar esta tarea debemos de seguir los siguientes pasos:

- ✓ En la línea de comandos digitaremos en comando **df –h**, que nos ayudará a verificar las unidades montadas.
- ✓ Antes de montar el CD verificaremos que dispositivo para CD-ROM estamos utilizando.
- ✓ Nos cambiamos al directorio en donde están nuestros dispositivos y listamos el contenido de la carpeta con los siguientes comandos:

COMANDOS	TAREA
cd /dev	Se cambia al directorio de los dispositivos
Ls	Lista todos los archivos

Tabla 2 Comandos para el directorio de dispositivos

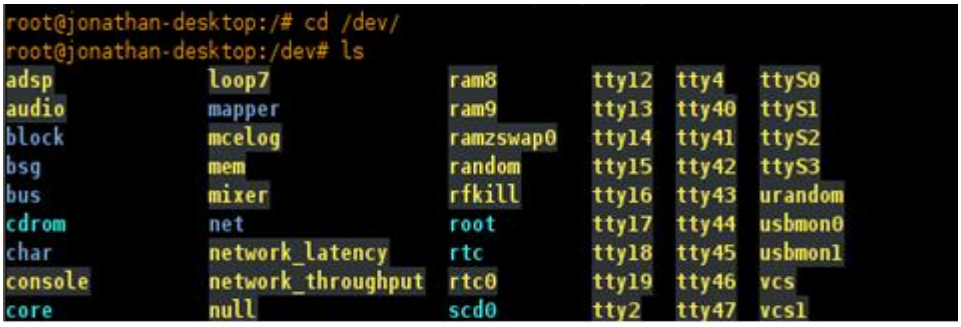


Figura 4.2.3-1 Directorio de los Dispositivos

Como podemos observar en la imagen el dispositivo utilizado en nuestra máquina es el sr0, esto nos quiere decir que es un CD-ROM de tipo IDE.

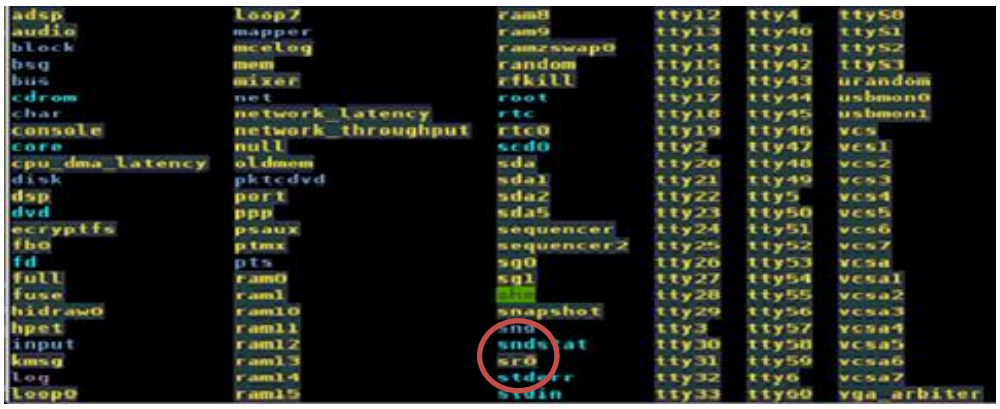


Figura 4.2.3-2 Dispositivo Sro Utilizado

- ✓ Ahora procedemos a montar nuestro CD que contiene la evidencia original pero solo en modo lectura y luego verificamos si esta montado.

COMANDO
✓ **mount –o ro /dev/sr0 /media/cdrom/** ✓ **df –h**
FUNCIÓN
✓ Monta el dispositivo /dev/sr0 que en este caso es el cd-rom en modo solo lectura , por esta razon se digitan los parametros – o y el ro (Read Only) , todo esto lo monta al directorio /media/cdrom. ✓ Con el comando df –h, vemos que el dispostivo este montado, al directorio asignado.

Tabla 3 Comandos montar cd modo lectura

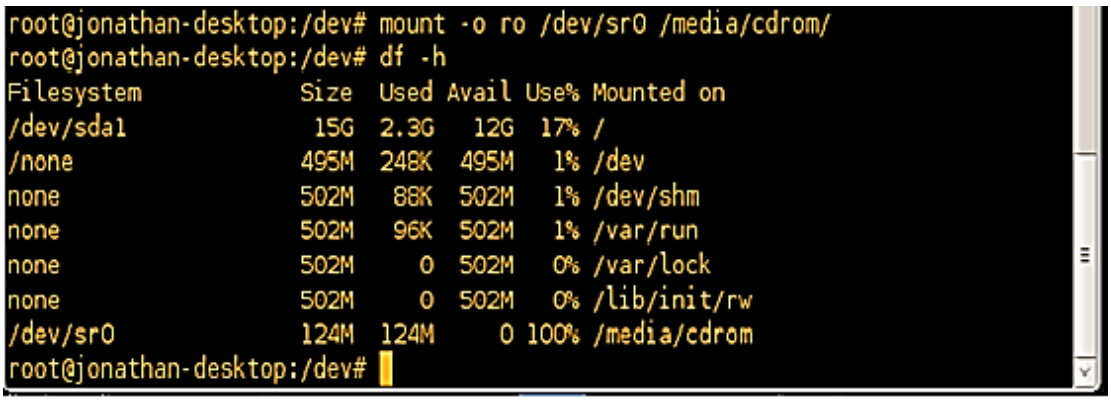


Figura 4.2.3-3 Montando en Modo Lectura Disco de la Evidencia

4.2.4. Copiar evidencia original

Para realizar una copia bloque a bloque, es decir realizar un copiado de una imagen igual que el de la evidencia original, en donde no se manipule absolutamente en nada la evidencia lo podemos realizar con la herramienta **air 2.0.0** que se encuentra en Caine. Para realizar este punto seguiremos los siguientes pasos:

- ✓ Como primer paso utilizaremos la línea de comandos, para montar una unidad del Disco Duro, en la cual esta va hacer el origen en donde guardaremos nuestra copia sacada de la evidencia original.

Comandos
✓ fdisk -l ✓ mount –o rw /dev/sda1 /mnt
Función
✓ Este comando nos ayuda a ver la estructura del disco de la máquina. ✓ Montamos la unidad /dev/sda1 en modo escritura, por eso digitamos los parámetros –o y rw (Read Wrtite), lo montamos al directorio /mnt.

Tabla 4 Comandos para montar unidad

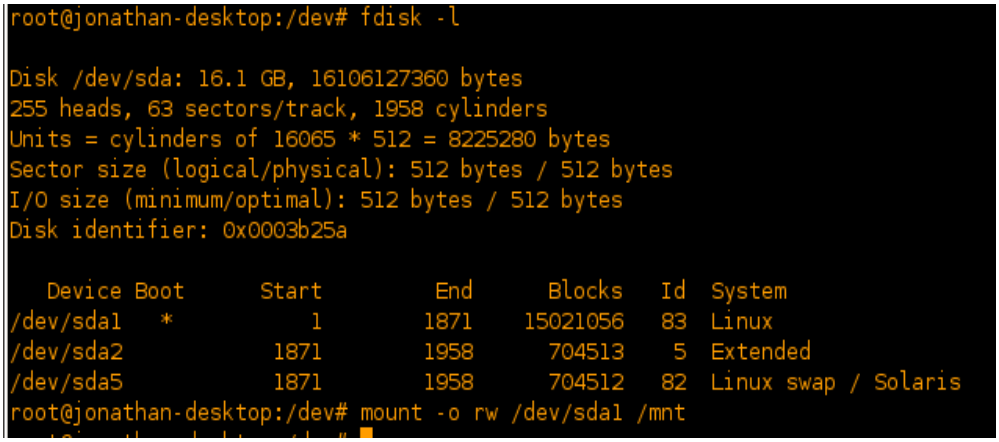


Figura 4.2.4-1 Montar en Modo de Escritura

✓ Ahora en la línea de comandos abrimos nuestra herramienta digitando **air&,** esperamos que cargue.

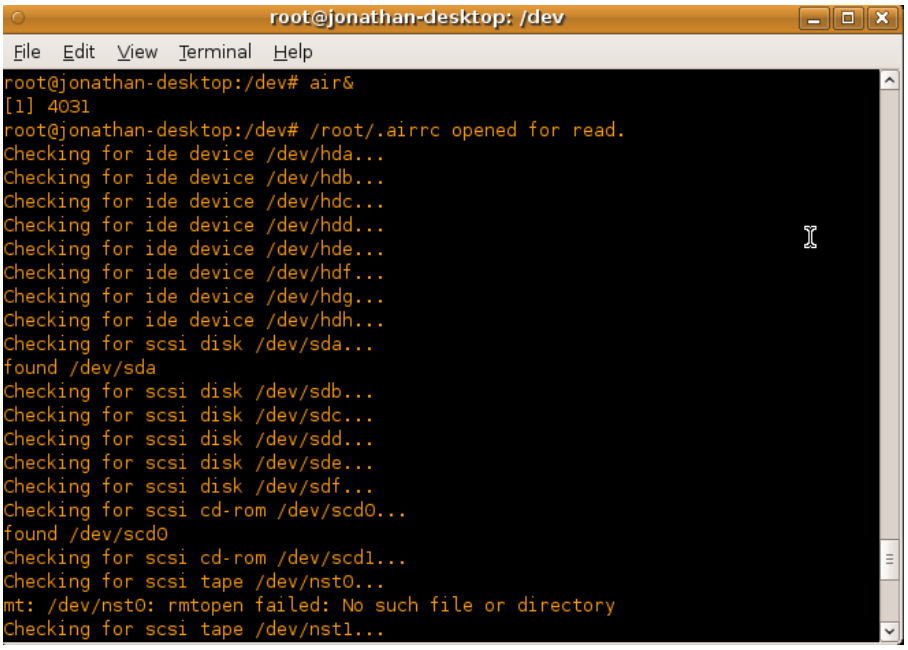


Figura 4.2.4-2 Ejecutar AIR mediante Línea de Comando

- ✓ Una vez cargada nuestra herramienta se abrirá y en el mensaje que aparece simplemente damos clic en cancelar.

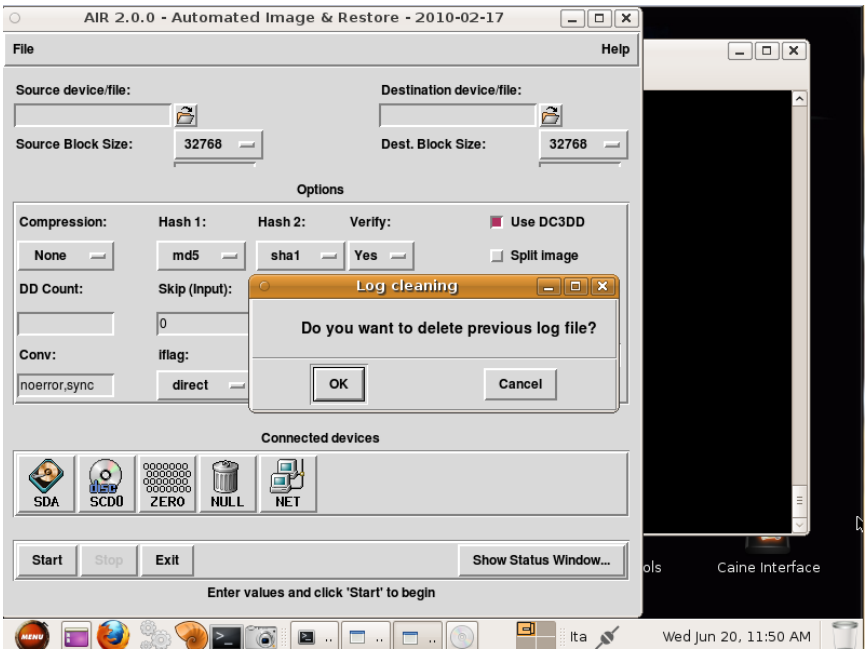


Figura 4.2.4-3 Inicio de AIR

- ✓ A continuación comenzaremos a llenar los parámetros de la herramienta, en la cual primeramente vamos a decirle en la opción **Source device/file:** nuestro origen. En este caso va hacer el **/dev/sr0** que contiene la evidencia original.

- ✓ En la siguiente opción que dice **Destination device/file:** va hacer nuestro destino en donde vamos a guardar nuestra imagen forense. La cual la guardaremos en el directorio **/mnt/** con el nombre **Respaldo.img.**

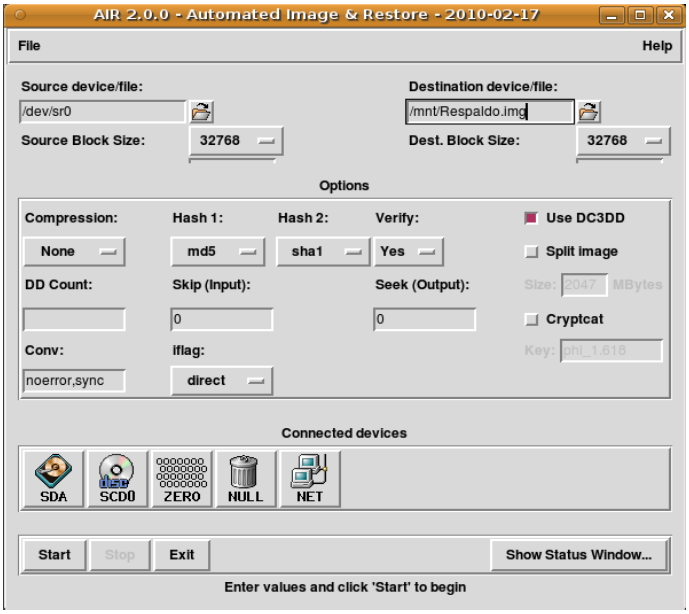


Figura 4.2.4-4 Parámetros de AIR

- ✓ El resto de las opciones las dejaremos por defecto y a continuación daremos clic en **Start** para empezar el copiado y luego en **Show Status Windows** para ver las estadísticas del copiado. [2]

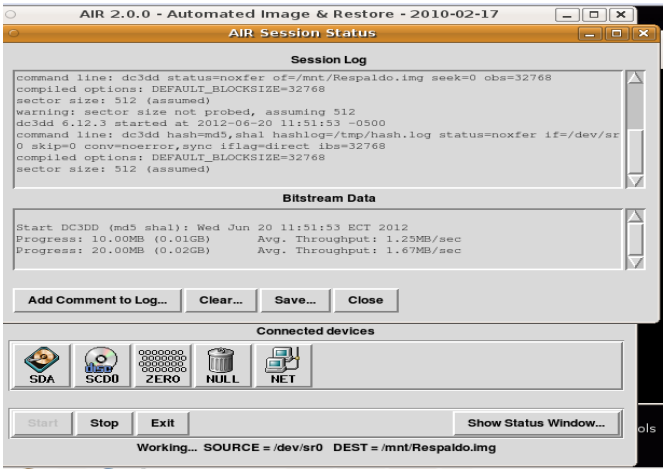


Figura 4.2.4-5 Empezando Respaldo de Imagen

- ✓ Una vez finalizada la copia nos daremos cuenta si nos dio algún tipo de error o si la copia fue exitosa, en este caso la copia tuvo éxito.

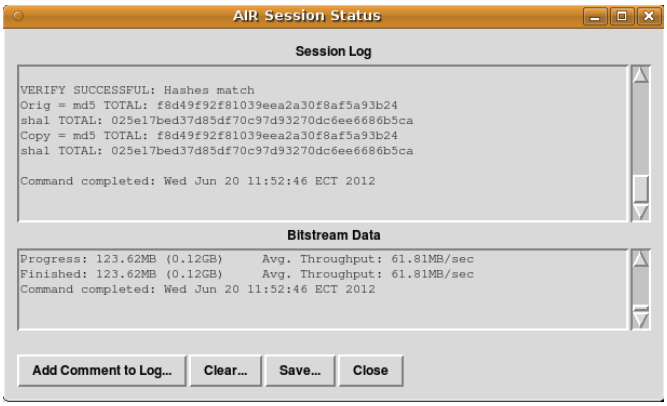


Figura 4.2.4-6 Finalización de Respaldo

4.2.5. Hashes del respaldo de la evidencia

Para realizar esta comparación de nuestros hashes daremos clic en **Add Comment to Log,** en la cual vamos a guardar nuestro log en la siguiente ruta **/home/caine/Tesis/** con el nombre**HashesResplado.log** y luego podremos verificar si nuestro hashes son idénticos y asegurarnos que no hemos manipulado la evidencia original.

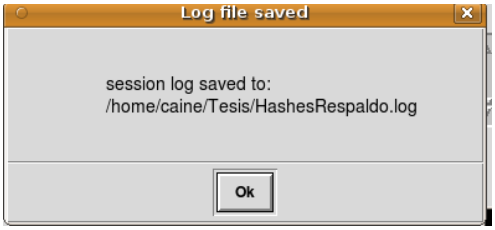


Figura 4.2.5-1 Guardar Log en un Directorio

Para ver el contenido del log realizaremos los siguientes pasos:

- ✓ Primeramente utilizaremos la linea de comando y nos cambiaremos al directorio en donde tenemos almacenado nuestro log.

- ✓ Escribiremos en la linea de comando : **cd /home/caine/Tesis/**y **l**istaremos los archivos contenidos en este directorio con el comando **ls** y cómo podemos observar en la imagen veremos que si está el archivo **HashesRespaldo.log.**

- ✓ Para ver su contenido utilizaremos el comando **cat + el nombre del archivo**, es decir **cat HashesRespaldo.log.**

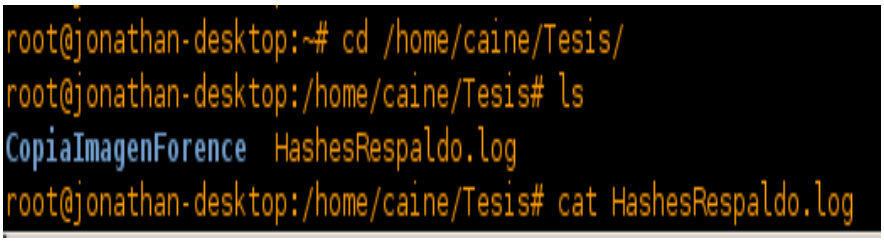


Figura 4.2.5-2 Ir al Directorio en donde se encuentra el Log

- ✓ Por último veremos que nuestros hashes son idénticos y que no hemos alterado la evidencia.

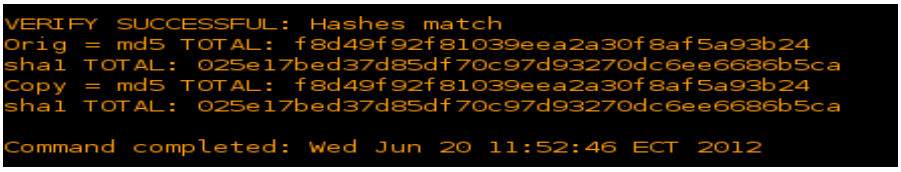


Figura 4.2.5-3 Comparación de Hashes de la Imagen Original y la Copia

4.2.6. Moviendo copia a otro directorio

Para mover la copia utilizamos el comando **df –h** , para ver en que directorio está montado la unidad de disco,en este caso es el directorio **/mnt** y procedemos a cambiarnos a ese directorio con el siguiente comando:**cd /mnt**.

En este directorio se encontrara nuestra imagen forense y procedemos a moverla hacia el directorio creado.

COMANDO
✓ mv Respaldo.img /home/caine/Tesis/CopiaImagenForence/
FUNCIÓN
✓ Movemos la imagen llamada Respaldo.img hacia el directorio CopiaImagenForence.

Tabla 5 Comandos para mover copia

```
root@jonathan-desktop:/# df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/sda1              15G  2.6G   11G  20% /
/none                 495M  248K  495M   1% /dev
none                  502M   88K  502M   1% /dev/shm
none                  502M   96K  502M   1% /var/run
none                  502M     0  502M   0% /var/lock
none                  502M     0  502M   0% /lib/init/rw
/dev/sr0              124M  124M     0 100% /media/cdrom
/dev/sda1              15G  2.6G   11G  20% /mnt
root@jonathan-desktop:/# cd /mnt
root@jonathan-desktop:/mnt# mv Respaldo.img /home/caine/Tesis/CopiaImagenForence
/
root@jonathan-desktop:/mnt#
```

Figura 4.2.6-1 Moviendo Copia de Imagen a Otro Directorio

4.2.7. Explorar copia de imagen

Para la explorarción de nuestra copia guardada, tenemos los siguientes pasos:

- ✓ Digitamos el comando para ver los directorios montados y a continuación desmontamos el directorio **/mnt** con el comando **umount /mnt.**
- ✓ Luego nos cambiaremos hacia el directorio en donde tenemos almacenda nuestra copia forense en este caso seria: **cd /home/caine/Tesis/CopiaImagenForense.**
- ✓ Luego la listamos el directorio para verificar los archivos almacenados en el con el comando **ls** y nos mostrara el archivo de la copia de la imagen llamdado **Resplado.img.**
- ✓ Luego procedemos a montar nuestra copia forense con el siguiente comando**:**

Comando
✓ mount –o ro,noexec,loop Respaldo.img /mnt
Función
✓ Monta imagen en modo lectura llamada Respaldo.img sin alterar la evidencia.

Tabla 6 Comandos para explorar información

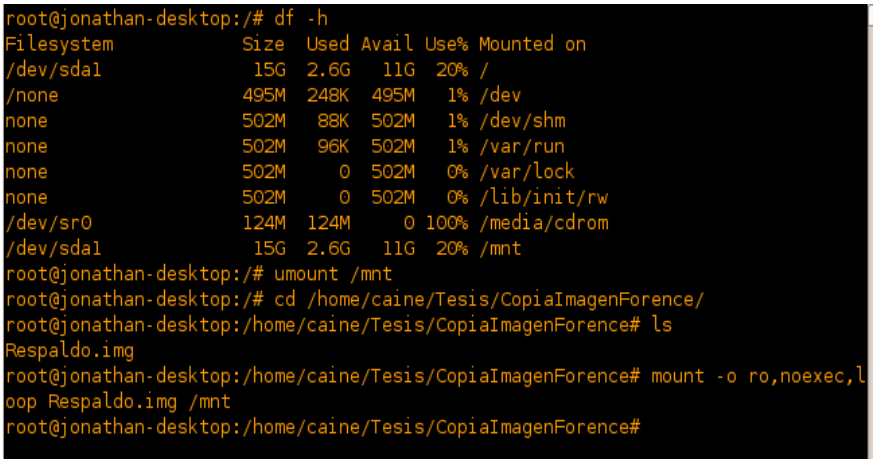


Figura 4.2.7-1 Explorando la Copia de Imagen Forense

- ✓ Una vez montado como **loop** lo verificaremos haciendo un **df –h** y si nos damos cuenta en la **Fig. 4.2.7-1** nuestra copia forense esta montado como **loop.**
- ✓ A continuación nos cambiamos al directorio **/mnt** para explorar la copia forense y listamos el directorio para ver los arhivos o directorios que estan almacendados. Como vemos habra un directorio llamado **CASO 4 – DRAFT COMPLETE.**
- ✓ Procedemos a cambiarnos al directorio **CASO 4 – DRAFT COMPLETE** y dentro de ese directorio habra otro directorio llamado **forensic_duplication**, en la cual también procedemos a cambiarnos y listamos los archivos que esten ahi.
- ✓ El arhivo **cf.dd** es la imagen obtenida de la Flash Memory, esta es la imagen la cual tendremos que analisar para llegar a nuestro objetivo propuesto.

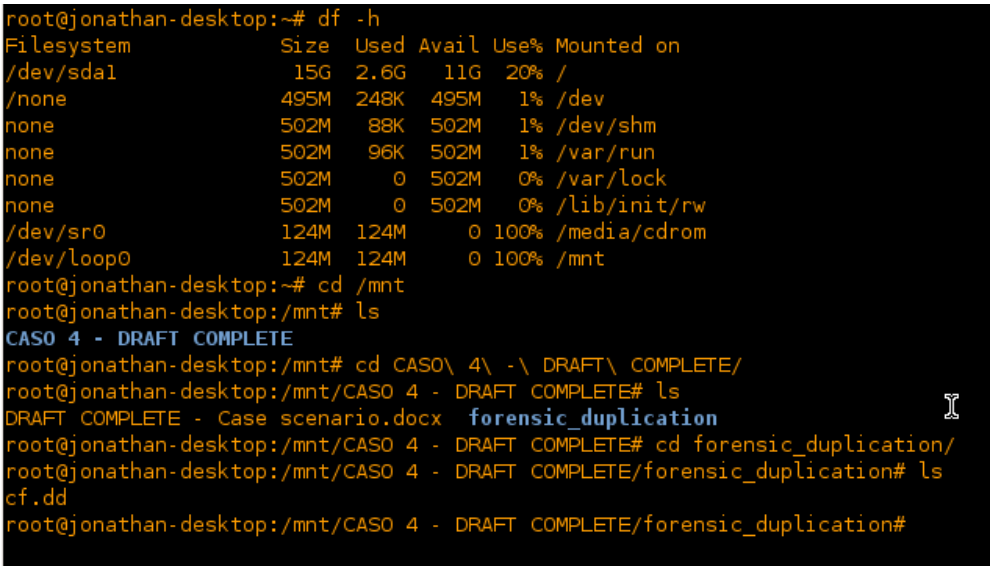


Figura 4.2.7-2 Archivo CF.DD

4.2.8. Hashes de la imagen cf.dd

Mediante el comando **md5sum** y su argumento **–b**, nos permitirá leer el md5 de la imagen forense en modo binario.

El contenido del md5 de la imagen **cf.dd** lo redireccionaremos hacia el directorio**/home/caine/Tesis** con el nombre **Hashesmd5Duplicacion.txt** para luego realizar la respectiva comparación imagen original y la duplicación.

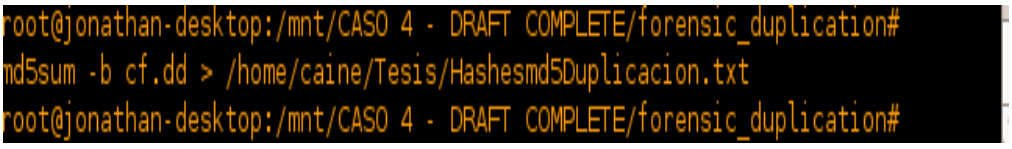


Figura 4.2.8-1 Hashes de la imagen Original

4.2.9. Duplicación de la imagen forense.

Para realizar el respectivo duplicado de la imagen forense haremos uso de línea de comando siguiendo estos pasos:

- ✓ Utilizaremos el comando **dd_rescue** para el respectivo duplicado de la imagen forense.
- ✓ Para esto crearemos un directorio en Tesis con el nombre **ImagenForence** con el siguiente comando:

  mkdir /home/caine/Tesis/ImagenForense

- ✓ Dentro de este directorio almacenaremos nuestra duplicado de la imagen forense.
- ✓ Luego de esto procedemos a realizar el duplicado con el siguiente comando:

  dd_rescue cf.dd /home/caine/Tesis/ImagenForense/cfcopia.dd

- ✓ Por último solo esperamos unos segundos hasta que se duplique la imagen forense.

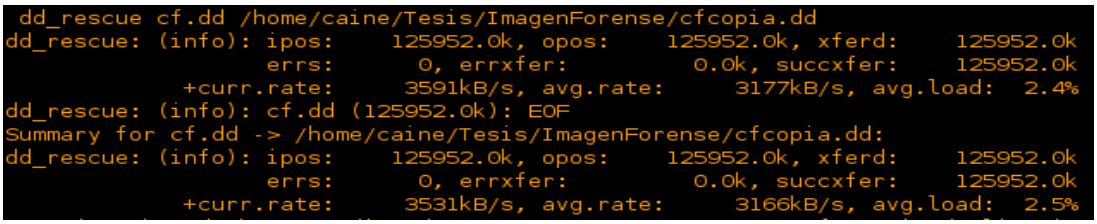


Figura 4.2.9-1 Realizando Duplicación

Como podemos en la imagen nuestra duplicacion se almaceno con éxito en el directorio asignado.

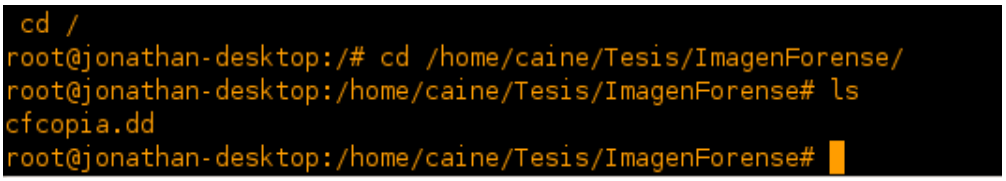


Figura 4.2.9-2 Duplicación Realizada Exitosamente

4.2.10. Hashes de la copia de la imagen cfcopia.dd

Ahora vamos a proceder a extraer el md5 en modo binario de nuestra duplicación utilizando el mismo comando mensionado anteriormente en este caso seria: **md5sum –b cfcopia.dd** El contenido lo redireccionaremos hacia el directorio **/home/caine/Tesis/** con el nombre **Hashesmd5DuplicacionCopia.txt**

Luego retrocederemos un directorio con el comando **cd ..** y listaremos los archivos que tiene almacenado el directorio Tesis. Como observamos en la **Fig. 4.2.10-1** estan los dos archivos **.txt** que redireccionamos anteriormente. Ahora con el comando cat veremos su contenido de los los 2 archivos redirecionados en este caso seria:

Cat Hashesmd5Duplicacion.txt

Cat Hashesmd5DuplicacionCopia.txt

Como observamos nuestra **Fig. 4.2.10-1** los dos archivos tienen el mismo contenido, esto significa que no hemos alterado nuestra imagen forense en el momento de la duplicación, por lo que ahora podremos trabajar en nuestra copia como si estuvieramos analizando nuestra imagen forense original.

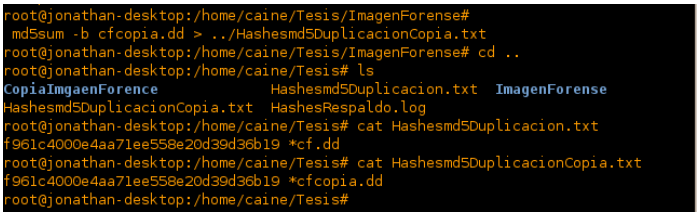


Figura 4.2.10-1 Hashes de la copia de la Imagen

4.3. EXTRACCIÓN DE LA INFORMACIÓN

Una vez realizada el respectivo duplicado, podremos realizar la extracción de la información contenida en esta imagen forense.

Para llevar a cabo este punto vamos hacer uso de la herramienta Autopsy, en la cual realizamos los siguientes pasos:

- ✓ **Iniciando Autopsy**
- ✓ **Montar Imagen Forense con Autopsy**
- ✓ **Calculo de Hashes**
- ✓ **Explorar Archivos**
- ✓ **Recuperación de Archivos Borrados**

4.3.1. Iniciando Autopsy

- ✓ Primeramente vamos a ejecutar Autopsy, ingresando en la línea de comando y digitando la palabra **autopsy&**. En donde el **&** nos ayuda a ejecutar una instrucción en segundo.

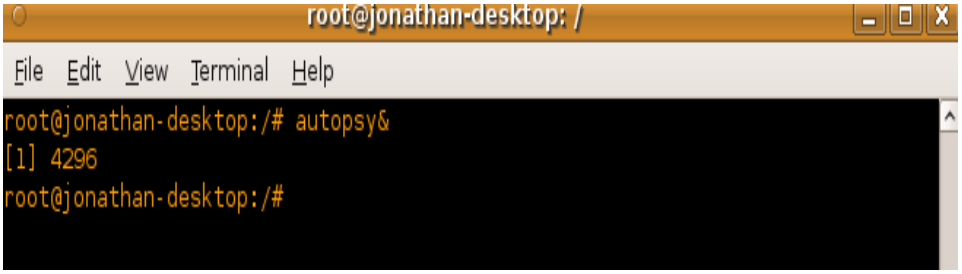


Figura 4.3.1-1 Iniciado Autopsy mediante Línea de Comando

- ✓ Una vez que termine de cargar la instrucción aparecerá la pantalla de inicial de Autopsy y a continuación daremos clic en **New Case** para crear un nuevo caso**.**

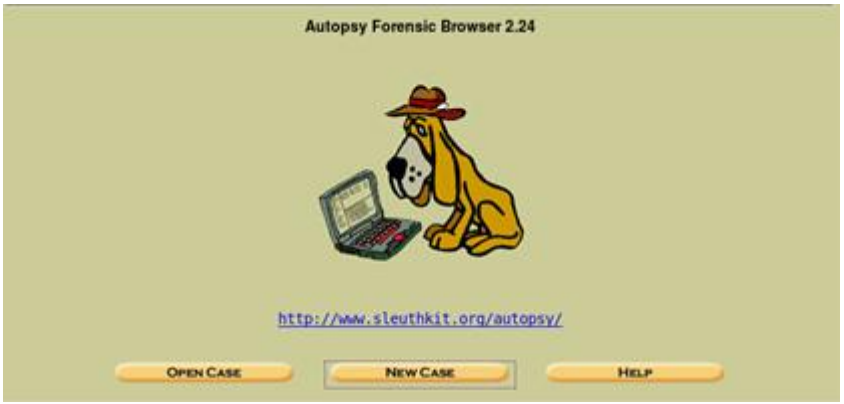


Figura 4.3.1-2 Ventana de Inicio de Autopsy

- ✓ Luego procedemos a llenar los respectivos datos, y a continuación daremos clic en **New case** para crear el caso.

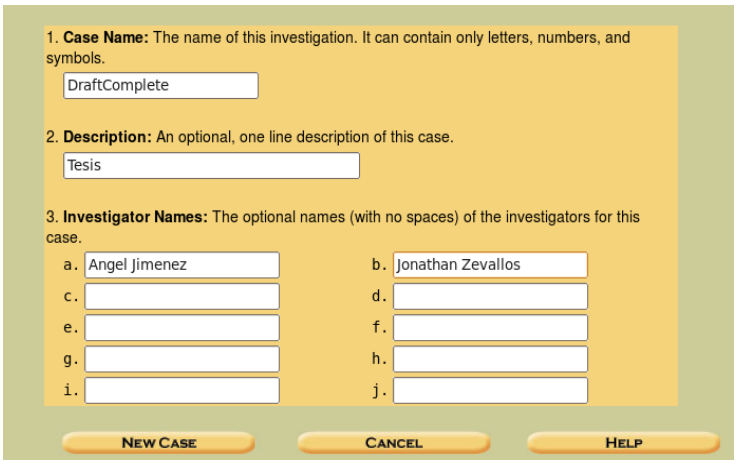


Figura 4.3.1-3 Creando un Nuevo Caso en Autopsy

- ✓ En el siguiente mensaje daremos clic en Add Host

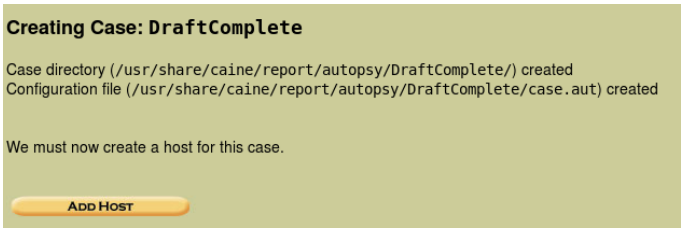


Figura 4.3.1-4 Comenzando a Añadir Host en Autopsy

- ✓ Luego en la siguiente ventana , nos diregimos al punto 3 que es **Time Zone** en la cual vamos a digitar la zona horaria en la que estamos en este caso escribiremos **/America/Guayaquil**, el resto de la opciones las dejaremos por defecto y daremos clic en **Add Host**.

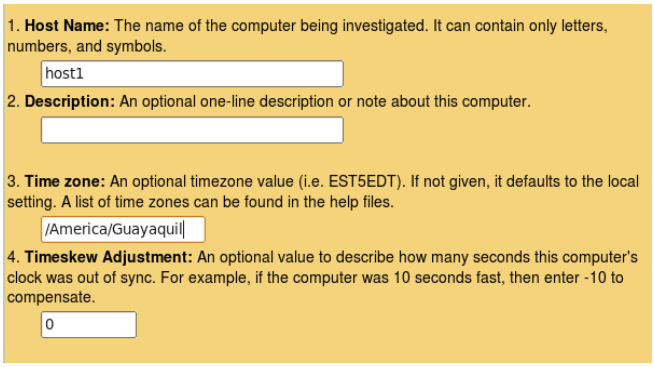


Figura 4.3.1-5 Añadir zona en Autopsy

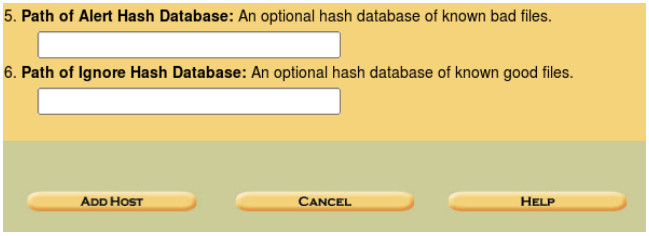


Figura 4.3.1-6 Añadir Host en Autopsy

4.3.2. Montar imagen forense con Autopsy

- ✓ Luego de añadir el host en la siguiente ventana Autopsy nos pedirá que agreguemos una Imagen, así que procedemos a Añadir nuestra imagen forense, haciendo clic en **Add Image.**

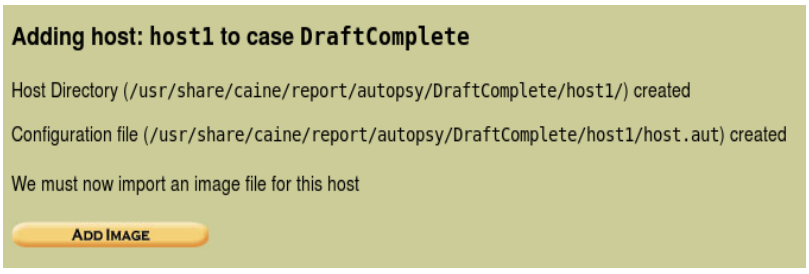


Figura 4.3.2-1 Comenzando a Añadir Imagen en Autopsy

- ✓ Como no hemos agregado ninguna imagen forense, autopsy nos dira en la parte superior que no hemos agregado ninguna imagen forense, entonces a continuación añadiremos nuestra imagen forense haciendo clic en **Add Image File.**

Figura 4.3.2-2 Agregar Imagen Forense en Autopsy

- ✓ Luego en la opción de **Location** vamos a digitar en que ruta se encuentra nuestra imagen forense que vamos a realizar el análisis. Entonces escribimos nuestra ruta que en este caso seria: **/home/caine/Tesis/ImagenForense/cfcopia.dd**y a continuación daremos clic en **Next**, recordemos que esta es la ruta en donde tenemos almacenda nuestra duplicado de la Imagen Forense.

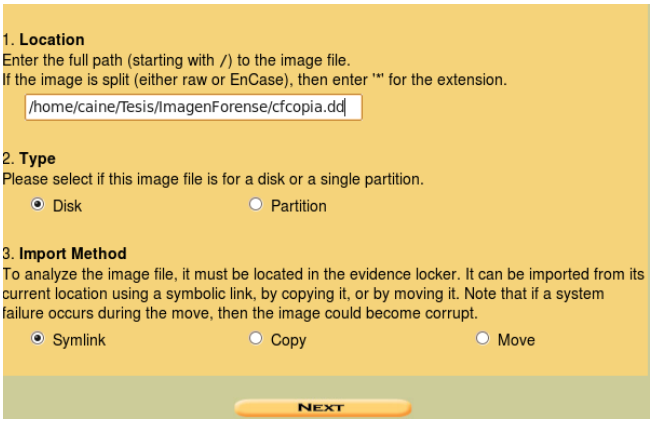


Figura 4.3.2-3 Dirección de la Imagen Forense

4.3.3. Cálculo de Hashes

Para el cálculo de los hashes tendremos que realizar los siguientes pasos:

- ✓ En la siguiente ventana tendremos tres opciones, en la cual vamos a escoger la segunda que es **Calculate** y daremos clic en **ADD,** Aquí se demorará unos segundos mientras calcula los hashes.

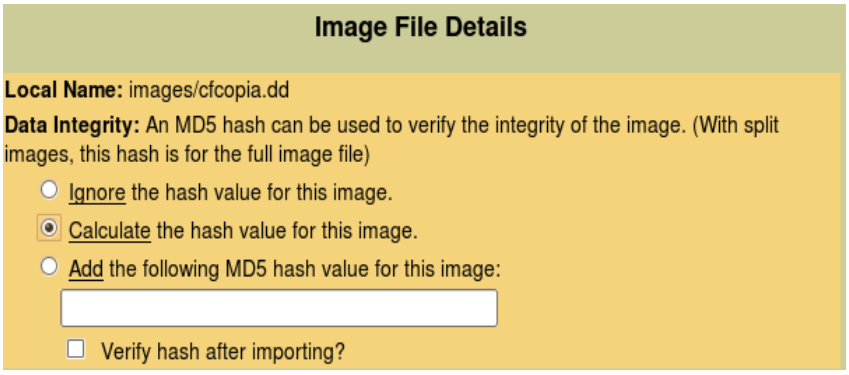


Figura 4.3.3-1 Eligiendo Opción para Calcular Hashes

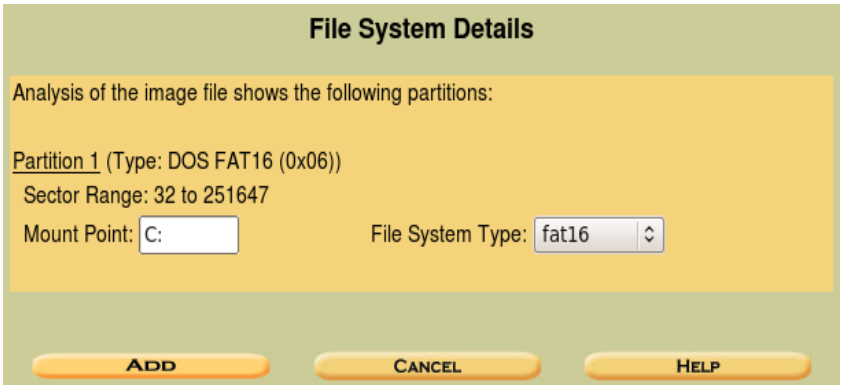


Figura 4.3.3-2 Agregar Punto de Montaje

Figura 4.3.3-3 Esperando el Cálculo de Hashes

✓ Una vez finalizado el calculo de los hashes, nos daremos cuenta cual es nuestro hash obtenido, así como podemos ver en nuestra imagen, y luego daremos clic en **OK** para continuar.

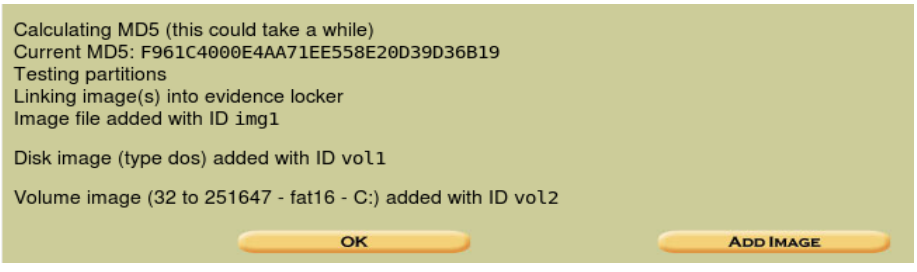


Figura 4.3.3-4 Cálculode Hashes Terminado

- ✓ Esta es la ventana vamos a realizar diferentes tareas, pero antes de comenzar a explorar las diferentes opciones, daremos clic en **Image Integrity** para ver si nuestros hashes son identicos y asegurarnos que no hemos manipulado la información.

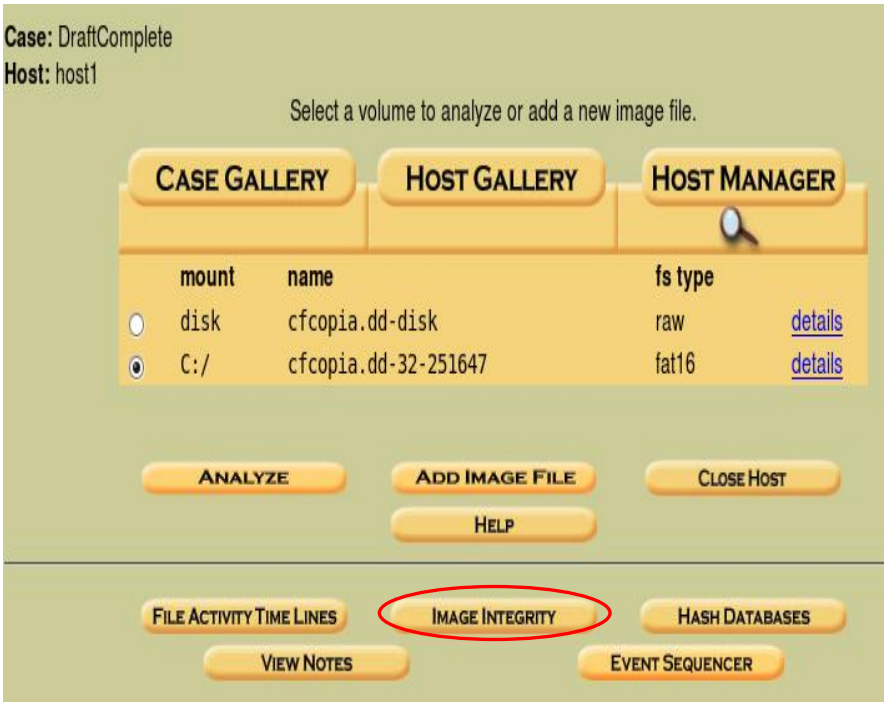


Figura 4.3.3-5 Ventana Inicial de tareas

- ✓ En la siguiente ventna daremos clic en **Validate** y si nos damos cuenta en la parte inferior nos mostrara el calculo de nuestros hashes del original y la copia.

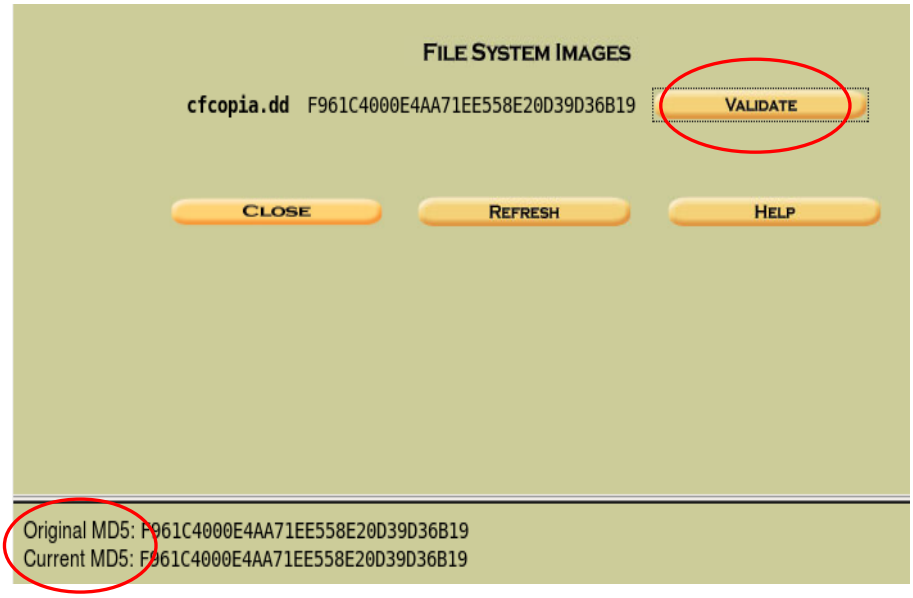


Figura 4.3.3-6 Hashes Idénticos como Resultado en Autopsy

- ✓ Como podemos observar en la imagen los hashes si son idénticos, esto significa que no hemos manipulado la información, daremos clic en **Close** y regresamos a la ventana incial **(Fig. 4.3.3-5)**, para realizar otras tareas.

4.3.4. Explorar archivos

En la **Fig. 4.3.4-1** nos mostraba diferentes opciones que podemos realizar, a continuación daremos clic en **ANALYZE** y luego se desplegara otra ventana y en la parte superior daremos clic en **FILE ANALYSIS.**

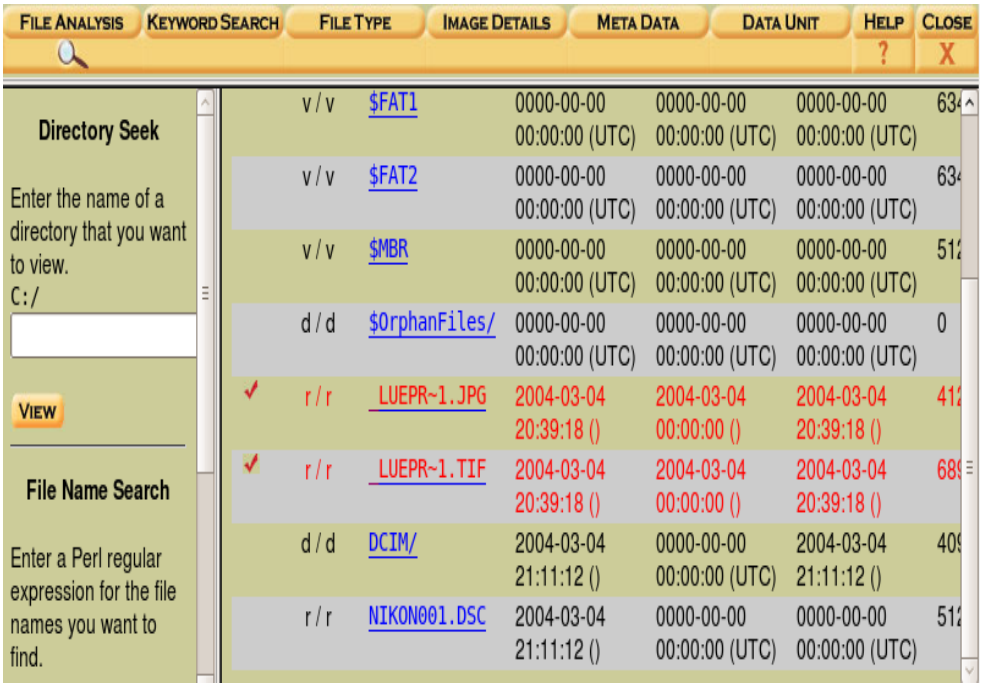


Figura 4.3.4-2 Explorando Archivos en Autopsy

Como podemos observar en la imagen **(Fig. 4.3.4-1)** Autopsy muestra todos los archivos que están almacenados en la imagen forense.

Los archivos que están de color Azul son los archivos no que están borrados y los archivos que están de color Rojo son los archivos que fueron accidentalmente o intencionalmente borrados.

4.3.5. Recuperación de archivos borrados

En esta sección vamos a verificar todos los archivos que están borrados y posteriormente a recuperarlos, realizando los siguientes pasos:

- ✓ Daremos clic en **ALL DELETED FILES** para mostrar todos los archivos eliminados.
- ✓ Ahora Daremos clic derecho sobre cada uno de estos archivos y escogeremos la opción de **Open Link in New Windows,** para que se habrá en otra ventana del explorador la información contenida del archivo**.**

Figura 4.3.5-1 Recuperando Información

- ✓ En la siguiente ventana nos mostrará toda la información de ese archivo y para recuperar ese archivo daremos clic en la parte superior donde dice **Export** y guardaremos este archivo para luego realizar el análisis respectivo**.**

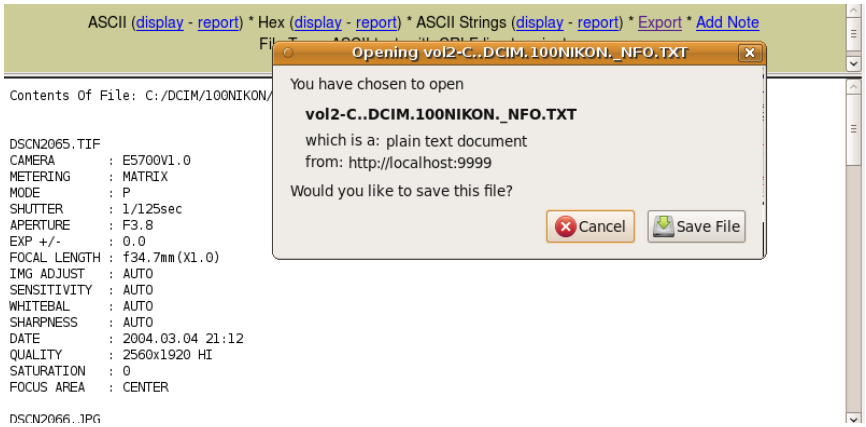


Figura 4.3.5-2 Recuperando Archivo NFO.TXT

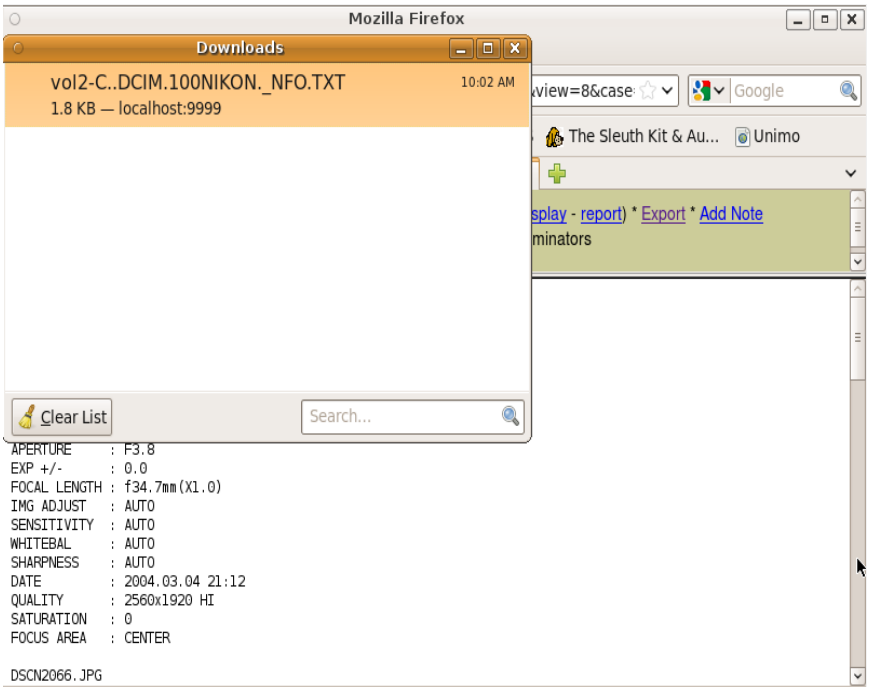


Figura 4.3.5-3 Archivo NFO.TXT Guardado Correctamente

Ahora procederemos a la recuperación de todos los demás archivos borrados realizando los pasos anteriores para la recuperación de los archivos borrados, a contracción mostraremos los demás archivos que fueron borrados:

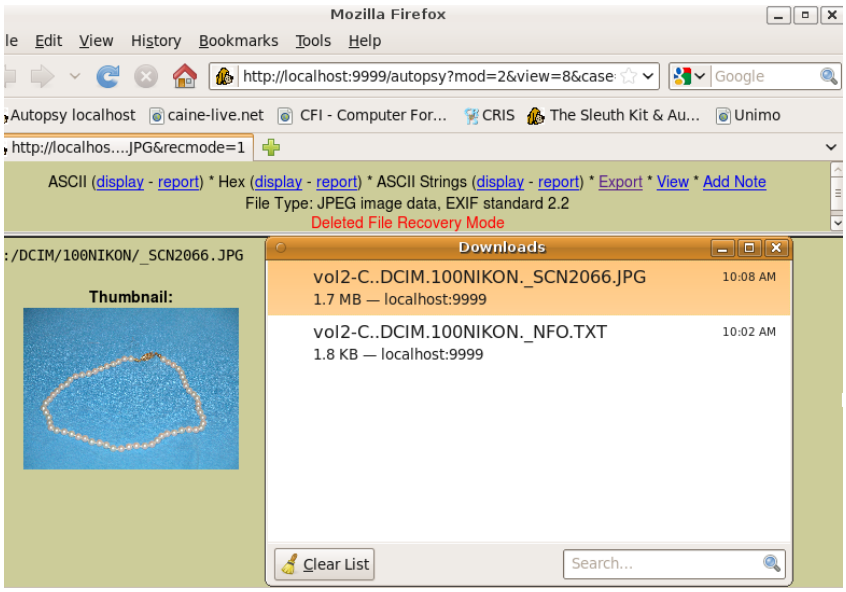


Figura 4.3.5-4 Recuperando y Guardando Archivo_SCN2066

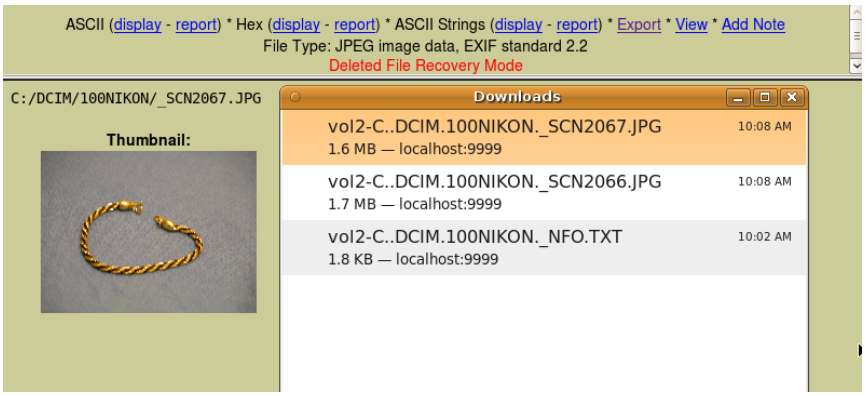


Figura 4.3.5-5 Recuperando y GuardandoArchivo_SCN2067

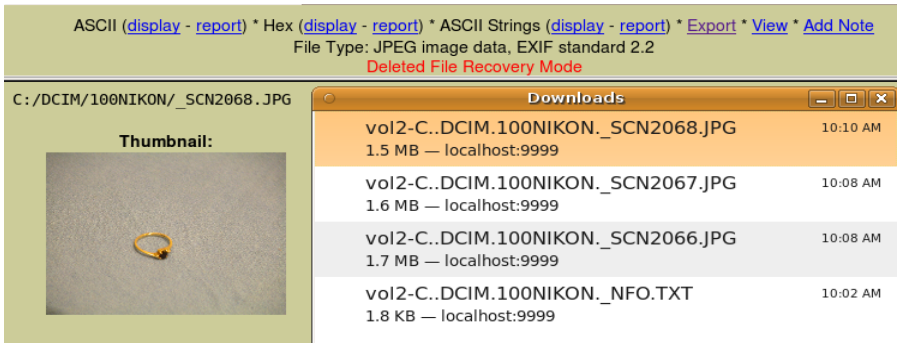


Figura 4.3.5-6 Recuperando y Guardando Archivo_SCN2068

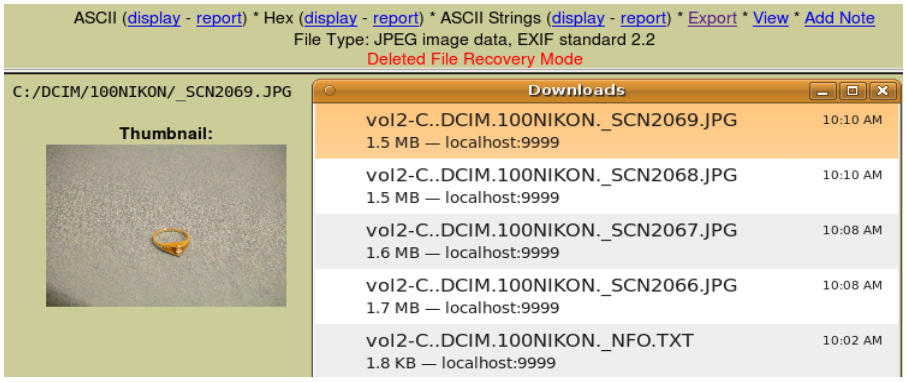


Figura 4.3.5-7 Recuperando y Guardando Archivo _SCN2069

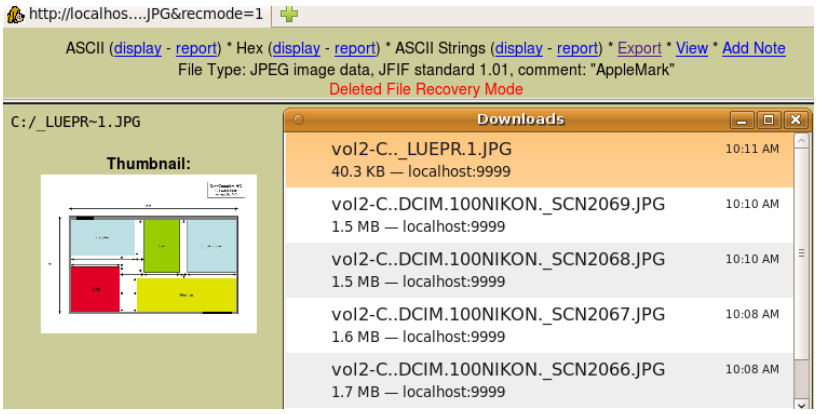


Figura 4.3.5-8 Recuperando y Guardando Archivo_LUEPR-1.JPG

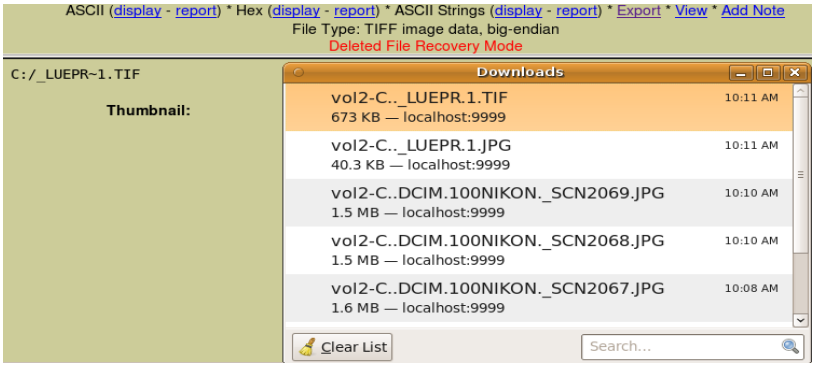


Figura 4.3.5-9 Recuperando Archivo_LUEPR-1.TIF

4.3.6. Moviendo información borrada

Toda aquella información que recuperamos la almacenaremos en un nuevo directorio para tenerla respaldada.

A continuación crearemos un directorio llamado **ImágenesRecuperadas** en el directorio **/home/caine/Tesis/RespaldoInformacion**.

Cuando anteriormente nosotros estabamos recuperando la información borrada, Autopsy va guardando estos archivos en el directorio **Desktop** por defecto, así que por lo tanto accederemos a este directorio y la listaremos con el comando **ls** , como podremos observar aquí se encuentra toda la infomación que recuperamos, luego de eso procederemos primeramente a mover todas las imágenes .JPG con el siguiente comando:

- ✓ **mv *.JPG /home/caine/Tesis/RespaldoInformacion/ImagenesRecuperadas**

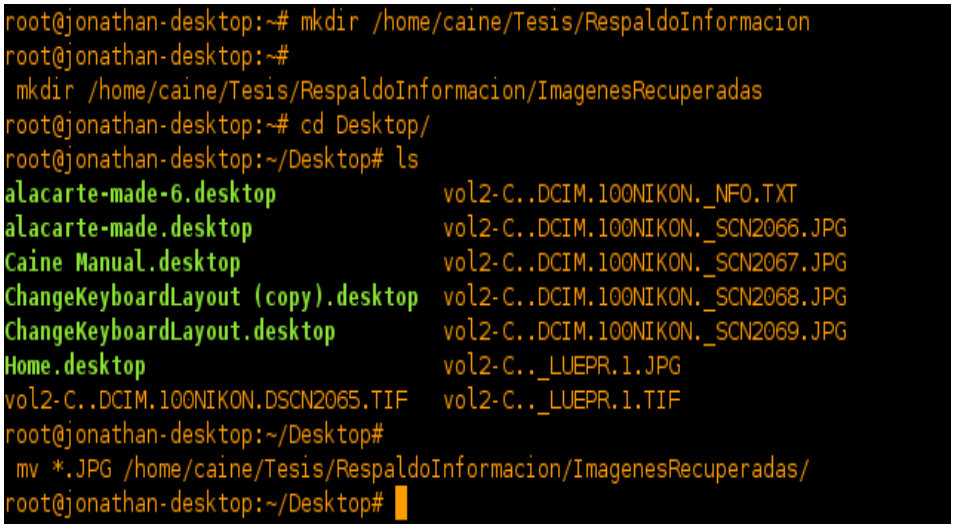


Figura 4.3.6-1 Moviendo Imágenes JPG a Otro Directorio

Por último moveremos los dos últimos archivos que nos faltan en este caso es un .TIF y .TXT, haciendo uso también del siguiente comando:

- ✓ mv *.TIF /home/caine/Tesis/RespaldoInformacion/ImagenesRecuperadas
- ✓ mv vol2-c..DCIM.100NIKON_NFO.TXT /home/caine/Tesis/RespaldoInformacion

Figura 4.3.6-2 Moviendo Información faltante a otro Directorio

4.3.7. Recuperando de información legible

Bruce Amiter no había eliminado un archivo de una imagen correspondiente a una cadena o joya, esta imagen estaba legible en su memoria Flash, entonces se procedio primero a acceder a este direcorio en donde se encontraba esta imagen.En la parte inicial del **File Analysis**, Autopsy nos permitia ver los archivos eliminados que eran los rojos y los legibles que eran los azules . Ahora como nos podemos dar cuenta **DCIM/** es un directorio que aun esta legible.

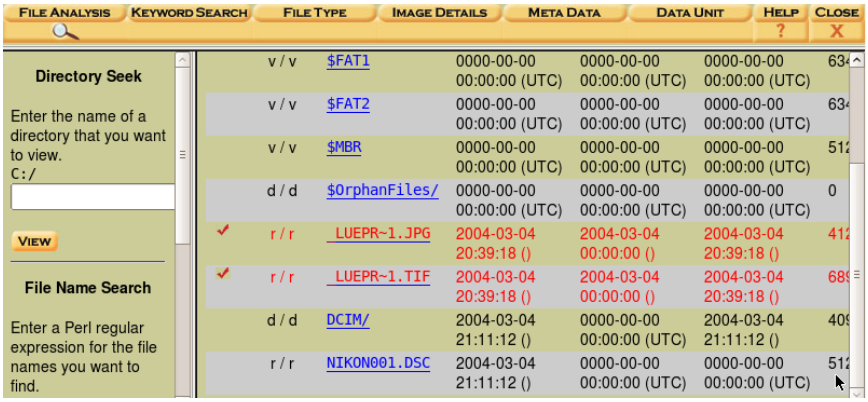


Figura 4.3.7-1 DCIM Directorio Legible

Dentro del directorio **DCIM/** se encontraba otradirectoio llamado **100NIKON/**, en la cual este tambien estaba legible.

Figura 4.3.7-2 100NIKON Directorio Legible

Como podemos observar en este directorio se encontraban las imágenes que fueron borradas por el ya sea accidentalmente o intensionalmente. Pero tambien podemos ver que habia una imagen llamada **DSCN2065.TIF** que no estaba eliminada, entonces comenzamos con su respectiva recuperación.

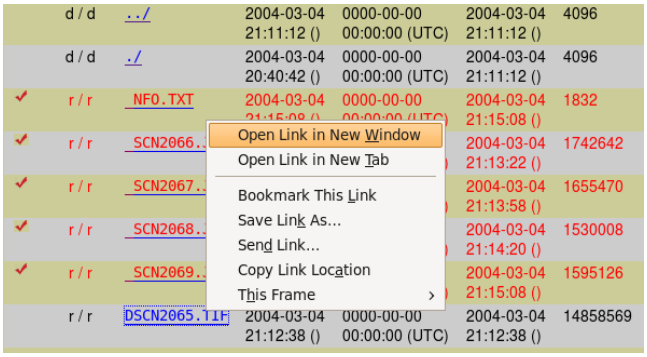


Figura 4.3.7-3 Procediendo a Recuperar Imagen DSCN2065.TIF

Como podemos darnos cuenta en la imagen, esta se pudo recuperar con éxito.

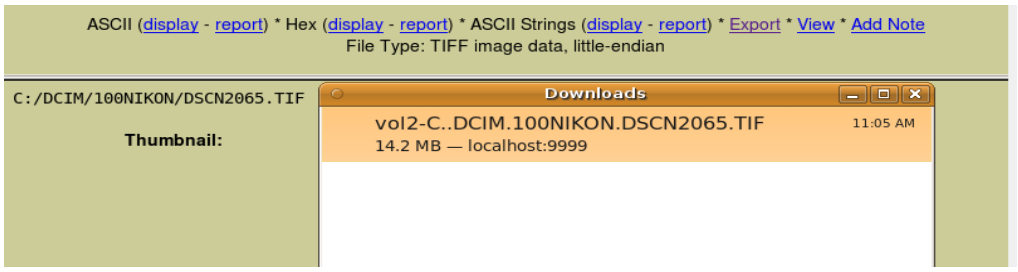


Figura 4.3.7-4 Recuperación Exitosa de la Imagen DSCN2065.TIF

Dicha imagen recuperada se guardará de nuevo por defecto en el directorio **/Desktop**, así que procederemos como en los pasos anteriores a moverla a nuestro directorio que creamos para el respaldo de información.

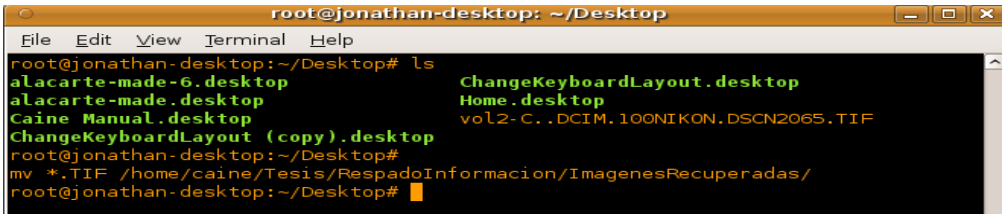


Figura 4.3.7-5 Moviendo ImagenTIF a otro Directorio

Mediante la interfaz gráfica podemos ver todas las imágenes que recuperamos, en nuestro directorio creado.

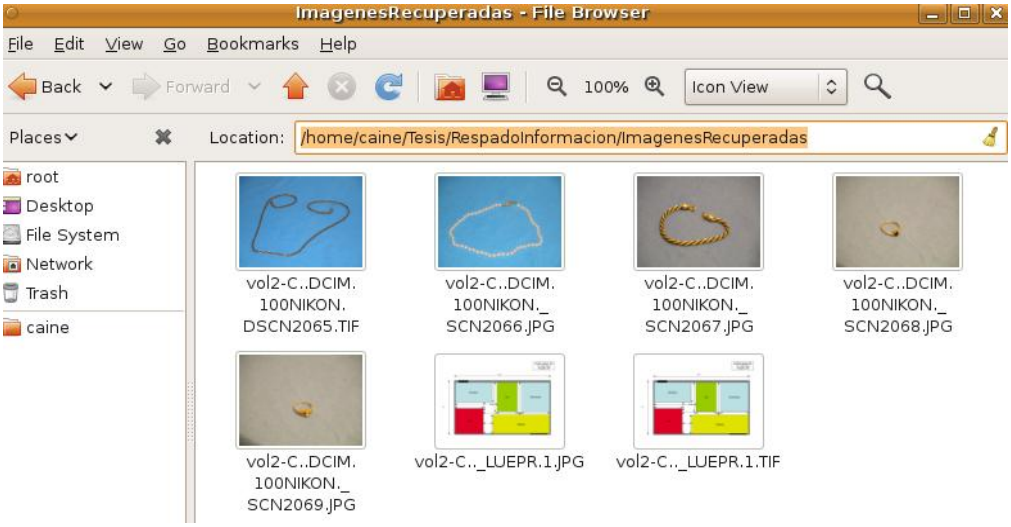


Figura 4.3.7-6 Vista Preliminar de las Imágenes

4.3.8. Recuperar información borrada mediante linea de comando

Para poder realizar la recuperación de la información borrada mediante línea de comando, nosotros deberiamos realizar las siguientes tareas:

- Montar .dd mediante linea de comando
- Utilización del comando FLS
- Recuperación de archivos mediante ICAT
- Recuperación de archivos mediante FATBACK

4.3.8.1. Montar .dd mediante linea de comando

Primeramente nosotros deberíamos montar nuestra imagen forense llamada **cfcopia.dd** y para poder realizar ese proceso primeramente digitaremos el comando **fdisk –lu** . Este comando se encarga de listar todas las particones (**- l**) y ademas nos permite visualizar el tamaño de los sectores de nuestra imagen forense (**- u**).

```
root@jonathan-desktop:~#
/sbin/fdisk -lu /home/caine/Tesis/ImagenForense/cfcopia.dd
You must set cylinders.
You can do this from the extra functions menu.

Disk /home/caine/Tesis/ImagenForense/cfcopia.dd: 0 MB, 0 bytes
8 heads, 32 sectors/track, 0 cylinders, total 0 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000

                                   Device Boot      Start         End      Blo
cks   Id  System
/home/caine/Tesis/ImagenForense/cfcopia.dd1   *          32      251647      125
808    6  FAT16
root@jonathan-desktop:~#
```

Figura 4.3.8.1-1 Utilizando el Comando FDISK –LU

Hay una diferencia entre un dispositivo USB y un disco duro y la respuesta es la tabla de partición. Nosotros podemos crear múltiples particiones en el disco duro, pero en los dispositivos USB solo existe una larga partición FAT.

Como nos podemos dar cuenta en la imagen anterior, nuestra imagen forense sacada de la memora flash empieza desde los 32 bytes, esta información es importante para poder realizar el respectivo montando.

Cada bytes por sector esta valorado en 512 bytes es decir como vamos a tomar la única partición que contiene esta imagen forense el resultado seria:

32 * 512 = 16384

Ahora procedemos a añadir esta imagen forense en un dispositivo loop, la cual nos ayudará a no manipular nuestra información de nuestra imagen forense y luego haremos un df –h que nos permitirá observar si algun dispositivo esta montado en ese momento.

- ✓ losetup /dev/loop0 /home/caine/Tesis/ImagenForense/cfcopia.dd -o $((32 * 512))

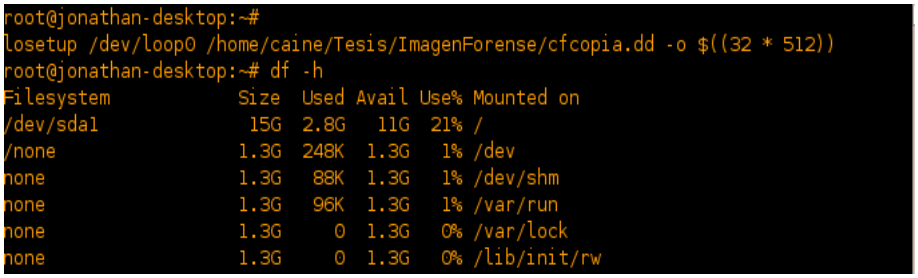


Figura 4.3.8.1-2 Añadiendo Imagen Forense a un LOOP

Ahora si podemos montar nuestro dispositivo loop que contiene la imagen forense a un directorio temporal. Pero lo montaremos en modo solo lectura, por esta razon utilizamos el **mount –r** y comprobaremos si nuestro dispositivo esta montado con el comando **df –h**. Como podemos ver en la siguiente imagen el disposivo loop esta montado correctamente, con el comando **ls –al** listaremos todos los archivos (opción **–l)** y ademas no ignoraremos todas las entradas que cominezen con punto (opción **–a**). [10]

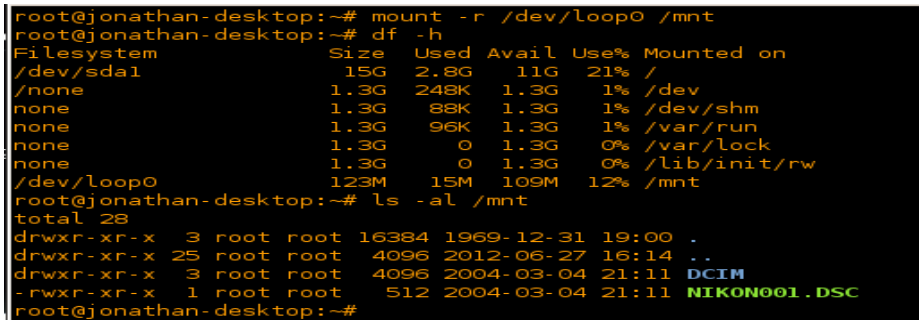


Figura 4.3.8.1-3 Montando LOOP a Directorio Temporal

4.3.8.2. Utilización del comando FLS

Este comando nos va a permitir listar todos los archivos y directorios contenidos en un dispositivo. Ademas nos permite listar todos los archivos que han sido borrados recientemente.

Este comando dispone de diferentes opciones en la cual vamos a utilizar 4 de ellas que son:

- ✓ **-r:** Mostrará todos los directorios de forma recursiva.
- ✓ **-l:** Desplegará los detalles en un formato largo.
- ✓ **-p:** Mostrará la ruta completa para cada entrada.
- ✓ **-f:** Permite especificar el tipo de sistema de archivo.

Entonces nuestro comando quedaria de la siguiente manera:

- ✓ **fls –r –l –p –f fat /dev/loop0**

Como podemos ver en la siguiente imagen, se listan todos los archivos y directorios contenidos en la imagen forense. Aquellos archivos que están con el signo *, son los archivos que han sido eliminados y en esta imagen podemos observar que existen 7 archivos eliminados.

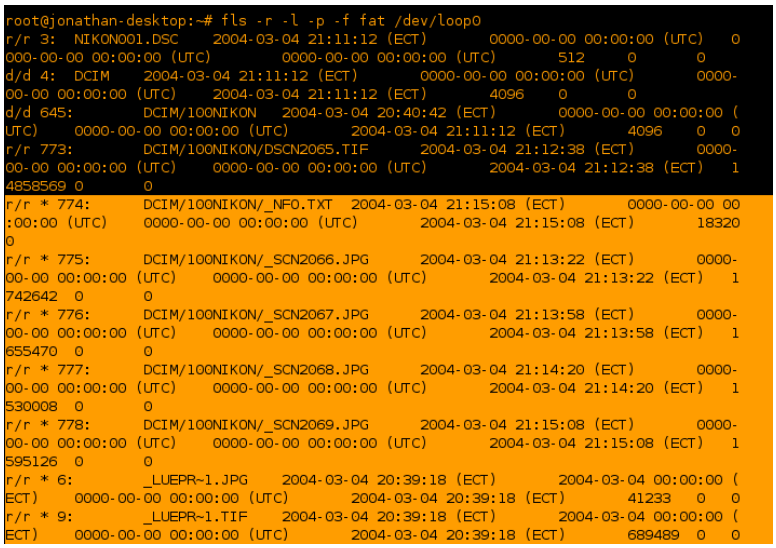


Figura 4.3.8.2-1 Comando FLS Mostrando Archivos Eliminados

4.3.8.3. Recuperación de archivos mediante ICAT

El comando **icat** nos permite realizar la recuperación de archivos que han sido borrado de un dispositivo. Para la utilización de este comando crearemos un directorio llamado **icatRespaldo**. Este directorio se encargará de almacenar todos los archivos que recuperemos de forma manual.

Los argumentos que utilizaremos es la opción **–f** que significa que vamos a especificar nuestro sistema de archivo, luego el dispositivo en el que esta montado, luego el inodo al cual esta asociado los archivos, así como anteriormente los observamos listados con la ayuda del comando **fls** y por último estableceremos el nombre del archivo, pero de acuerdo al inodo al que esta apuntando ese archivo.

Como podemos ver en la imagen digitando el comando **ls –al**, nos mostrará los archivos que hemos recuperado.

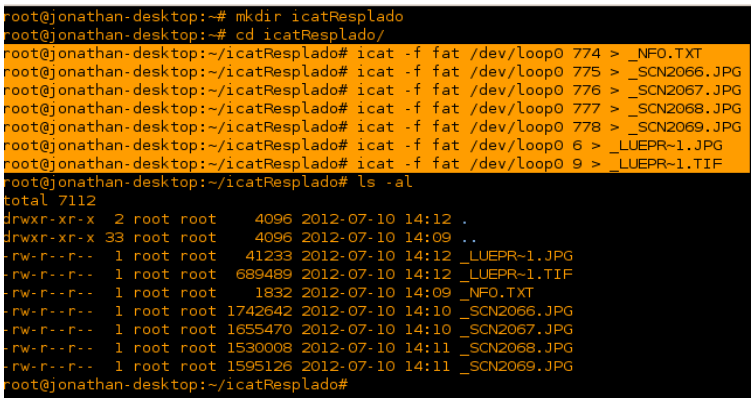


Figura 4.3.8.3-1 Comando ICAT Recuperando Archivos

4.3.8.4. Recuperación de archivos mediante FATBACK

Otro comando de gran utilidad al momento de hacer una recuperación ficheros en sistemas de archivos FAT. Tiene una similar función al comando icat. Para poder realizar una recuperación de archivos con este comando, primeramente crearemos otro directorio llamado **fatbackRespaldo**, en donde guardaremos los ficheros a recuperar.

Luego nos cambiaremos al directorio creado recientemente y digitaremos el comando **fatback /dev/loop0,** este apunta al dispositvo loop en donde se encuentra nuestra imagen forense montada. Luego con el comando **ls** listaremos su contenido y como podemos observar existen archivos que contiene el signo **?,** Este nos indica que son archivos que han sido eliminados.

Entonces comenzamos copiando nuestros 2 primeros ficheros, utilizando el comando **cp.**

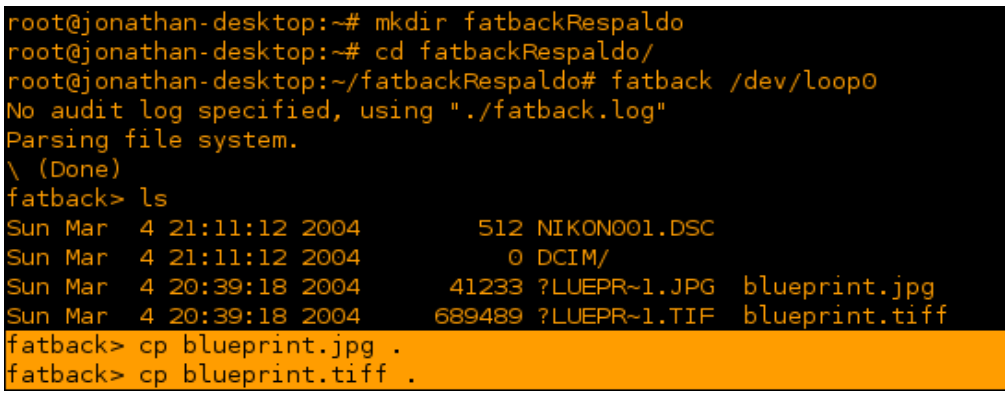


Figura 4.3.8.4-1 FACTBACK Recuperando los 2 Primeros Ficheros

Luego de recuperar nuestros 2 primeros ficheros, accederemos a el directorio **DCIM** y luego al directorio **100NIKON** mediante el comando **cd** y posteriormente listamos nuestros archivos**.** Como nos podemos dar cuenta en la imagen existen 5 archivos que han sido eliminados y un archivo llamado **DSCN2065.TIF** que no esta eliminado. Haciendo uso del comando **cp** procedemos a recuperar nuestros 5 ficheros y al finalizar la toda la copia de cada fichero digitaremos el comando **quit**, que nos permitirá salir de fatback .

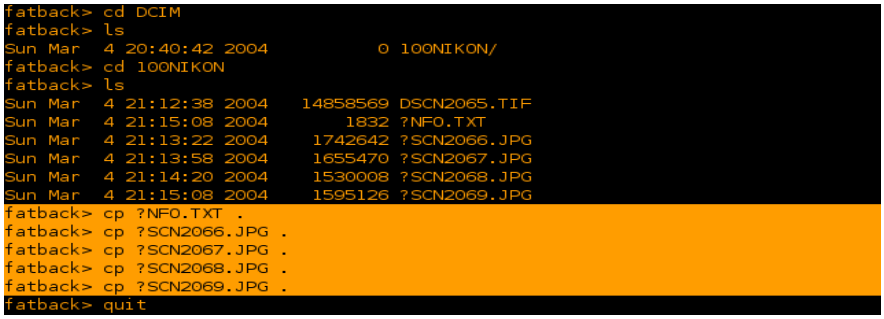


Figura 4.3.8.4-2 FATBACK Recuperando los 5 Ficheros

El uso de estos comando son esenciales en la recuperación de ficheros que habian sido borrados anteriormente en nuestra imagen forense.

A traves de linea de comandos se puede lograr este objetivo, ya sea utilizando ICAT o FATBACK ,en la cual nos permiten realizar tareas muy eficientes, al momento de un análisis forense o talvez siendo de gran ayuda para nosotros, si accidentalmente hemos borrado algun archivo importante que quisieramos recuperarlo inmeditamente.

Esta es una vista preliminar de las imágenes que recuperamos, en los directorios creados respectivamente, mediante el uso de los dos comandos utilizados anteriormente.

Figura 4.3.8.4-3 Vista Preliminar del DirectorioicatRespaldo

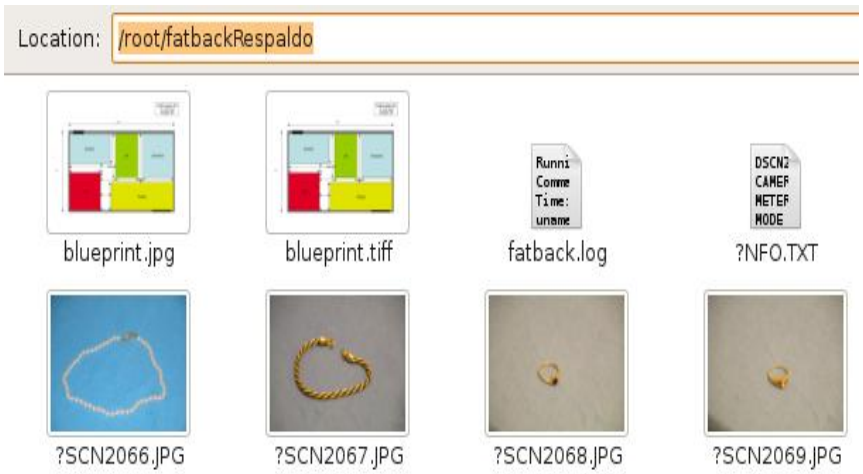


Figura 4.3.8.4-4 vista Preliminar del Directorio fatbackRespaldo

4.3.9. Recuperación de información mediante herramientas forenses para WINDOWS

Hoy en dia existen una gran variedad de herramientas forenses que trabajan con los Sistemas Operativos Windows. Estas herramientas forenses cumplen diferentes funciones en sus tareas y otras tienen muchas similitudes.

Existen herramientas gratuitas y comerciales para este Sistema Operativo, pero nosotros haremos uso de 2 herramientas forenses gratuitas, en la cual, estas herramientas nos va a permitir explorar toda la información que hubiera sido borrada o que el dispositivo hubiera sido formateado y 1 herramienta que es comercial, pero la utilizaremos en sus versión de prueba nos permitira montar nuestra imagen .dd en Windows.

Así como en caine, la utilización de sus comandos y la gran ayuda de herramienta forense Autopsy, hicieron un reconocimiento de información óptima, esta vez utilizaremos la platamaforma de windows, para analizar nuestra imagen forense y determinar si Bruce Amiter habria formateado su dispositivo con anterioridad, en donde hubiera mas información oculta.

Las herrramientas que utilizaremosson las siguientes :

- OSForensics
- Active@Uneraser – Data Recovery
- PC Inspector File Recovery

4.3.9.1. OSForensics

Primeramente alojaremos nuestra imagen forense llamada **cf.dd** en una carpeta creada en el Sistema Operativo Windows XP.

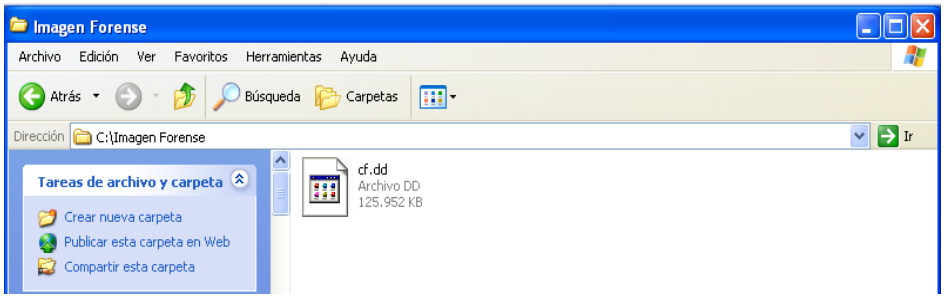


Figura 4.3.9.1-1 Carpeta Creada para la Imagen Forense en Windows

Luego ejecutaremos nuestra herramienta que nos permitirá montar nuestra imagen forense, esta herramienta nos da la opción de continuar utilizándola en su versión gratuita, así que daremos clic en **Continue Using Free Versión.**

Figura 4.3.9.1-2 OSForensics Escoger Opción Free Versión

Luego nos desplazaremos hacia las últimas opciones y en la parte de **Housekeeping** daremos clic en una opción llamada **Mount Drive Image**.

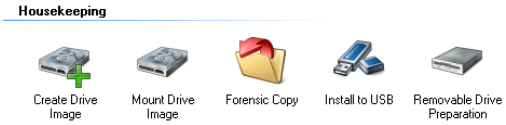


Figura 4.3.9.1-3 OSForensicsOpción Mount Drive Image

Luego se nos desplegará una ventana en donde, nos dará la opción de montar la imagen forense haciendo clic en la opción **Mount new**.

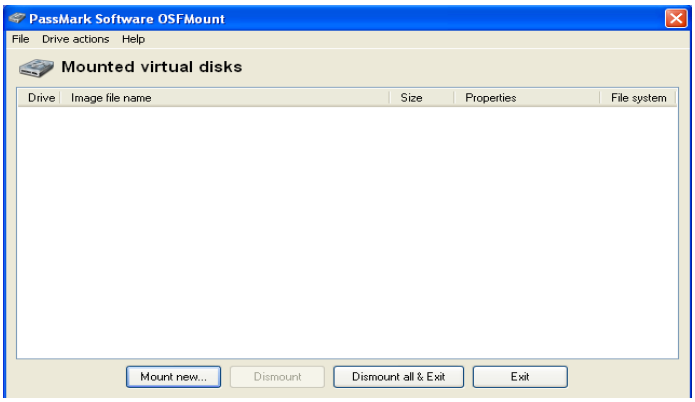


Figura 4.3.9.1-4 OSForensics Opción Mount New

Lo siguiente que haremos es buscar la ubicación de nuestra imagen forense, haciendo clic en boton de examinar en la parte de Image File. Una de las ventajas de esta herramienta es que nos va a permitir montar nuestra imagen forense en modo solo de lectura, así no manipularemos nuestra evidencia, esta opción se encuentra en la parte inferior llamada **Read Only Drive.**

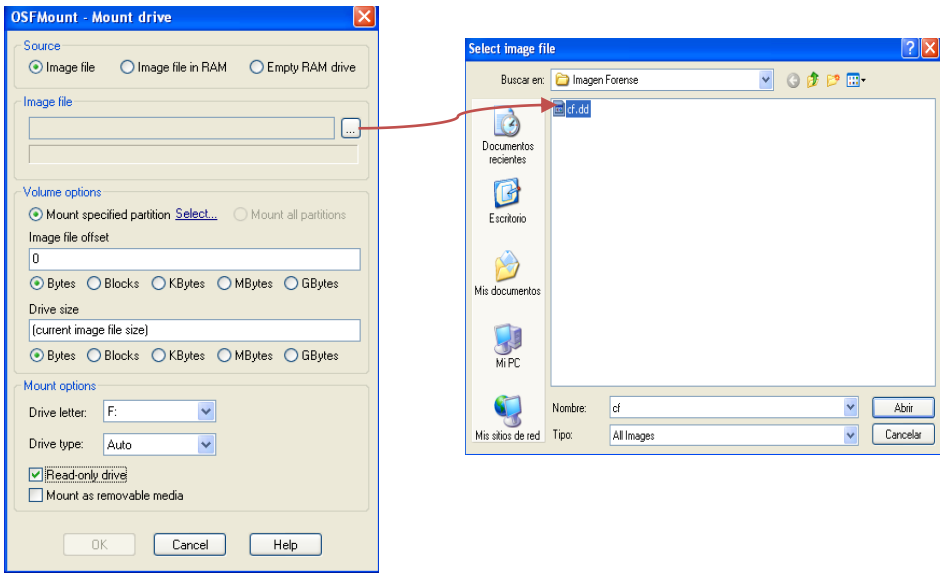


Figura 4.3.9.1-5 Buscando la Ubicación de la Imagen Forense

Como nuestra imagen forense se la adquirio de una memoria flash , en la siguiente ventana escojeremos la opción de montarla en una partición FAT 16 y luego aceptaremos para proceder con el montado de imagen.

Figura 4.3.9.1-6 OSForensics Montar en una Partición FAT 16

Como podemos observar en la Fig 87, nuestra imagen forense se tenia que montar en la unidad F y si exploramos nuestra unidades en **Mi PC** nos daremos cuenta que se monto con éxito.

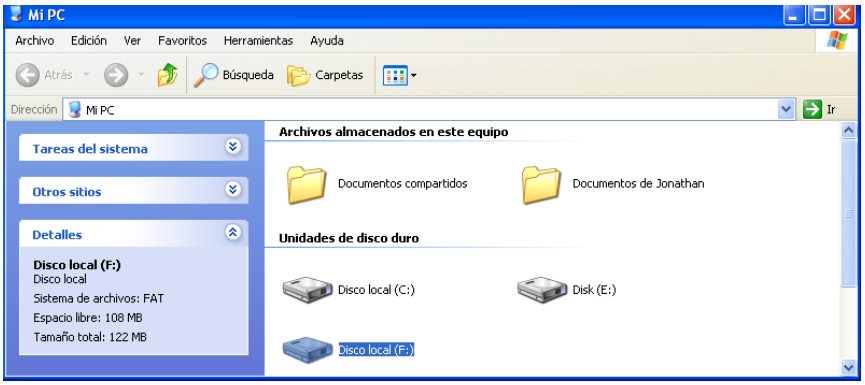


Figura 4.3.9.1-7 OSForensics Unidad F Montada con Éxito

4.3.9.2. Active@Uneraser – Data Recovery

Esta es la primera herramienta que utilizaremos para realizar las siguientes tareas:

- Escaneo de unidades mediante Uneraser
- Analizando archivos mediante Uneraser
- Recuperación de Información Mediante Uneraser

4.3.9.2.1. ESCANEO DE UNIDADES MEDIANTE UNERASER

Primeramente ejecutaremos nuestra herramienta desde la opción que dice: **Uneraser for windows(console)**.

El análisis en consola es mucho mas eficiente en la búsqueda de información perdida, por esta razón la utilizaremos.

Figura 4.3.9.2.1-1 Ejecutando UNERASER en Modo Consola

Una vez que se ejecuta esta herramienta nos mostrará todas las unidades que están montadas en ese momento, nosotros seleccionaremos nuestra unidad F.

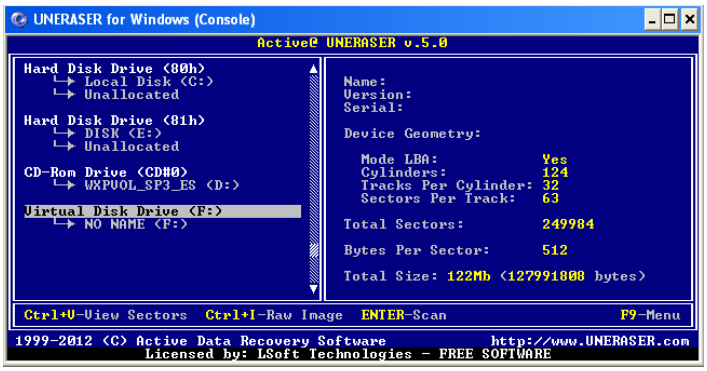


Figura 4.3.9.2.1-2 UNERASER Seleccionado Unidad F

Ahora procederemos a realizar una escaneada avanzada de la unidad, esta escaneada establecerá la búsqueda de información perdida y de datos borrados . Daremos clic en el menú **Scan** y luego en **Advanced Drive Scan**, para comenzar con el proceso**.**

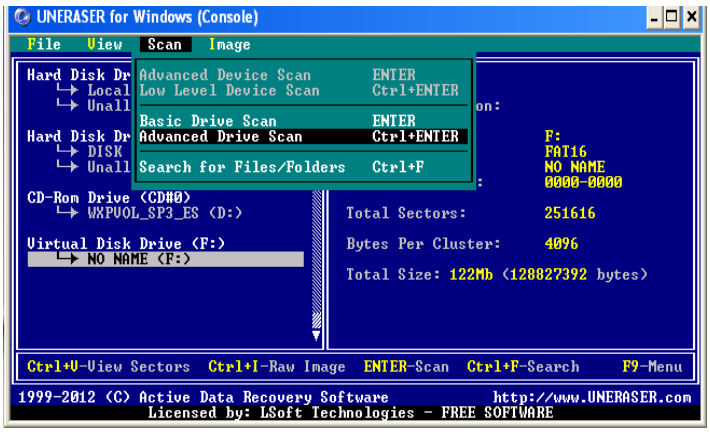


Figura 4.3.9.2.1-3 UNERASER Comenzando a Escanear Unidad F

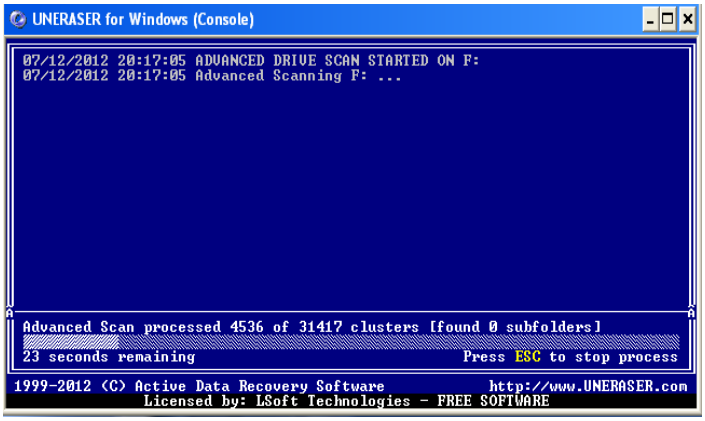


Figura 4.3.9.2.1-4 UNERASER Proceso de Escaneo

4.3.9.2.2. Analizando archivos mediante Uneraser

Una vez finalizado el proceso de escaneo, nos daremos cuenta que lista toda la información encontrada. Autopsy no mostro los archivos _b,_b,_f , al momento de realizar el análisis. Así que procedimos primeramente a realizar el análisis de estos archivos presionando enter.

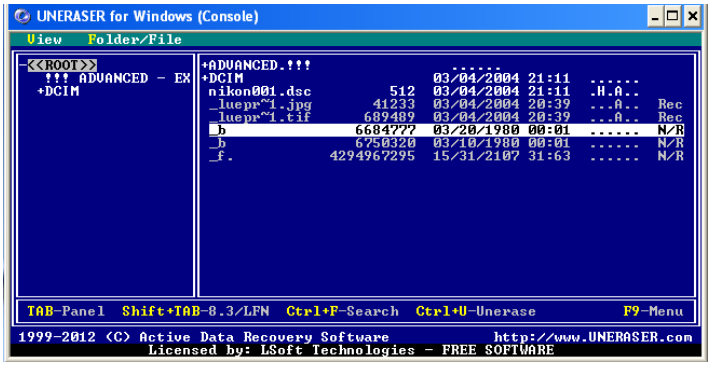


Figura 4.3.9.2.2-1 UNERASER Analizando Archivos Desconocidos _b

Figura 4.3.9.2.2-2 Proceso de Análisis de Archivos Desconocidos _b

Como vemos en la siguiente imagen, se mostrará el contenido del archivo en modo hexadecimal, si queremos ver el contenido en modo texto le podemos dar clic en la partte inferior que dice **TAB**.

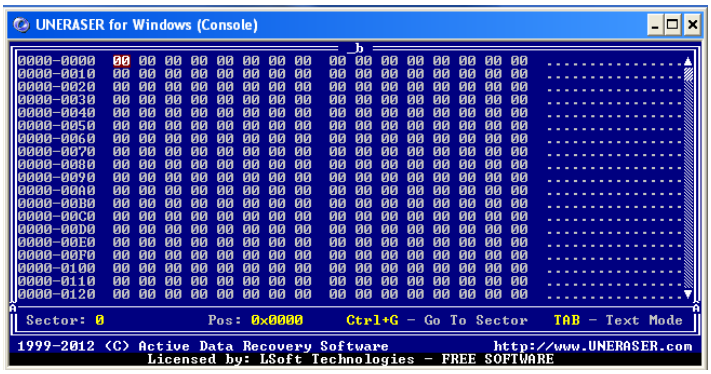


Figura 4.3.9.2.2-3 Archivo Desconocido _b Hexadecimal

Como podemos darnos cuenta, este archivo simplemente hacia referencia al archivo _**NFO.TXT** recuperado anteriormente, lo que significa que cuando se procedio a eliminar este archivo, su referencia aun estaba legible en los cluster y por lo tanto esta referencia seguia apuntando al archivo _**NFO.TXT**

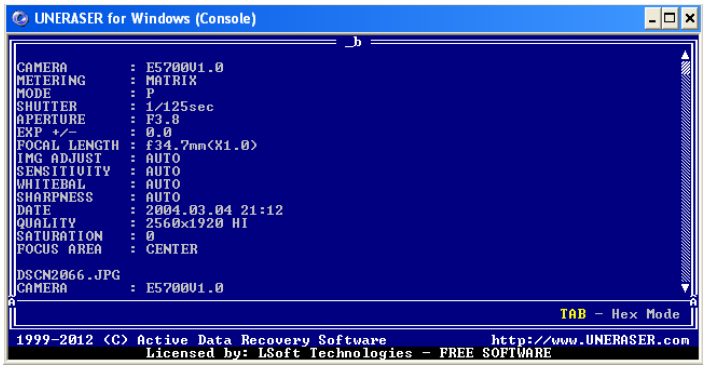


Figura 4.3.9.2.2-4 Archivo Desconocido _b Modo Texto

Tambien procedimos a realizar el análisis del otro archivo llamado _**b**, encontrado por Uneraser y simplemente este también hacia referencia al archivo _**NFO.TXT**, estas son las imágenes de su respectivo análisis mostrado en modo texto.

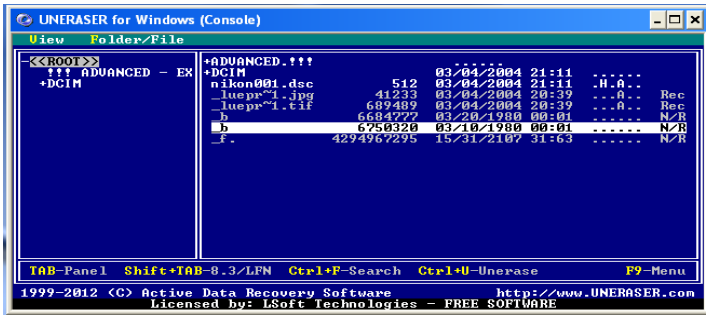


Figura 4.3.9.2.2-5 Analizando segundo Archivo Desconocido _b

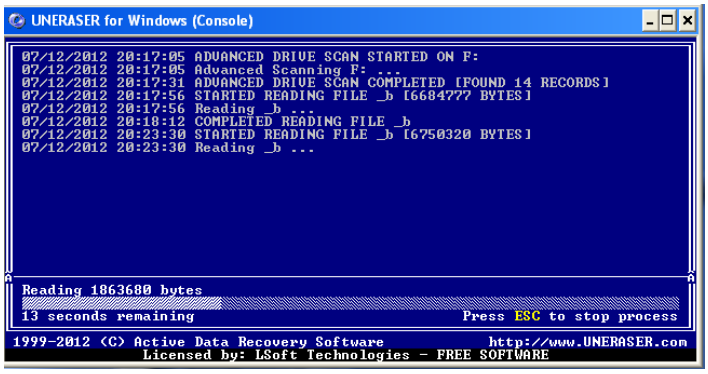


Figura 4.3.9.2.2-6 Análisis del Segundo Archivo Desconocido _b

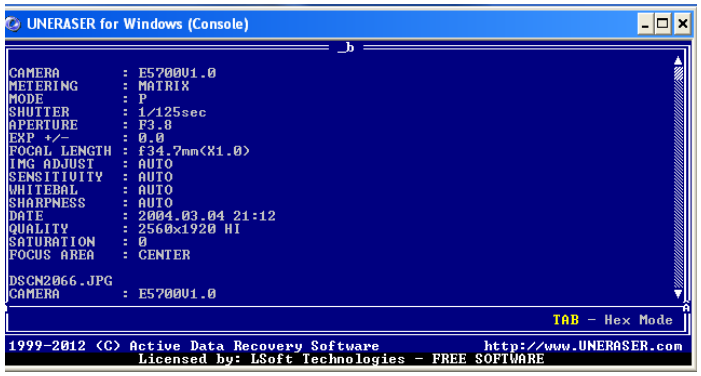


Figura 4.3.9.2.2-7 Segundo Archivo Desconocido _b Modo Texto

El siguiente archivo que nos queda por analizar es el archivo llamado _**f**, pero lastimosamente este archivo contenía errores y no se lo pudo analizar.

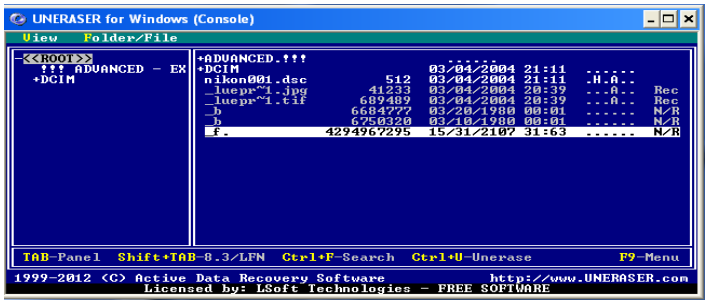


Figura 4.3.9.2.2-8 Archivo Desconocido _f

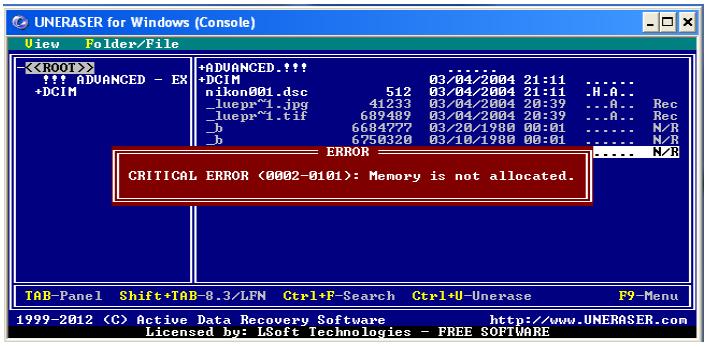


Figura 4.3.9.2.2-9 Error al Analizar el Archivo Desconocido _f

Además esta herramienta nos proporciona información tales como: si el archivo fue eliminado, su identidad, su tamaño, sus fechas de creación, modificación, acceso y mucha mas información. Haciendo clic sobre el archivo que deseamos ver la información daremos clic en el menú **Folder/File** y luego en la opción **View Info**.

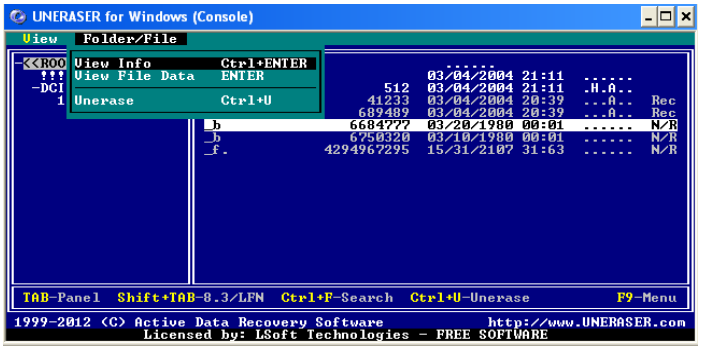


Figura 4.3.9.2.2-10 UNERASER Información del Archivo

Como nos damos cuenta en la siguiente imagen, se despliega toda la información necesaria del archivo y vemos que es un archivo que se eliminó, pero que además contiene algunos errores.

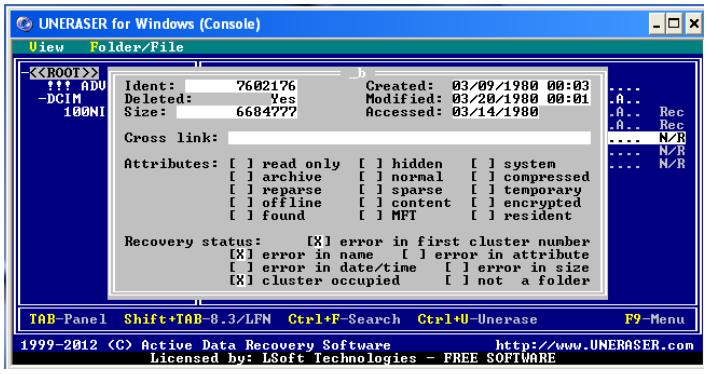


Figura 4.3.9.2.2-11 UNERASER Mostrar Información del Archivo _b

Ahora también veamos la información de los otros dos archivos desconocidos _**b** y _**f**. Como nos damos cuenta en la imagen el segundo archivo _**b** tiene una gran similitud con el anterior, pero de igual contiene errores.

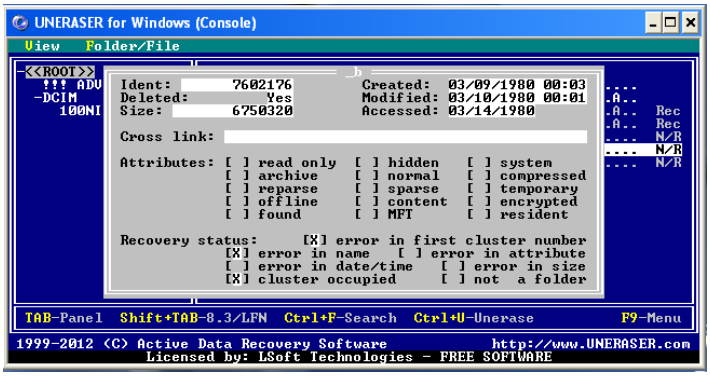


Figura 4.3.9.2.2-12 UNSERASER mostrar Información del Archivo _b

Como podemos observar en la imagen el archivo _**f** contiene más errores que los demás, como error en su tamaño y el tiempo de creación. Por lo tanto este archivo no se podra recuperar, porque esta dañado.

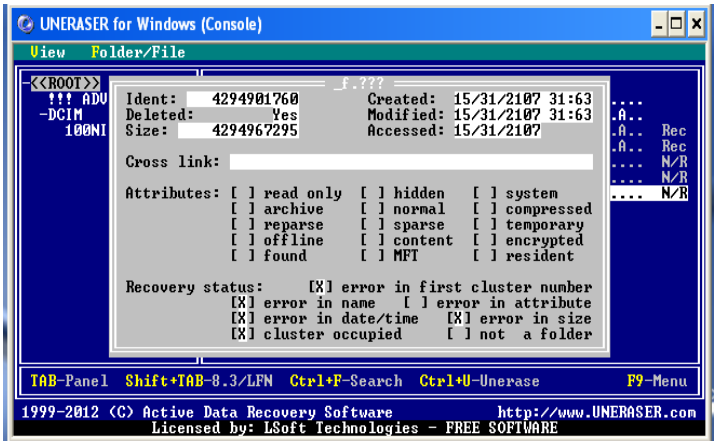


Figura 4.3.9.2.2-13 UNSERASER Mostrar Información del Archivo _F

Tambien podemos mostrar la información de un archivo que no han sido eliminado, en este caso selecionaremos la carpeta llamada **DCIM**.La información de los demás archivos como imágenes borradas , imágenes legibles y carpetas, seran iguales como las que nos mostró Autopsy o la linea de comando.

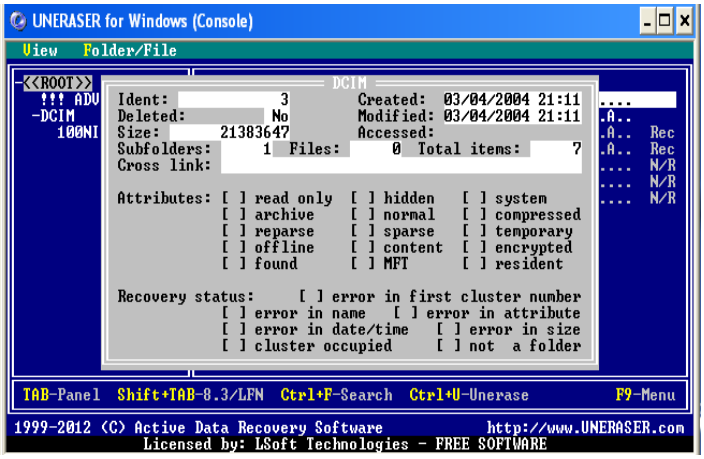


Figura 4.3.9.2.2-14 UNERASER Muestra Carpeta DCIM no Eliminada

Exploramos tambien la carpeta 100NIKON, para ver si existen más archivos desconocidos y como nos podemos dar cuenta, solo existen los archivos que se eliminaron, como anteriormente Auptopsy o mediante la linea de comando nos mostró.

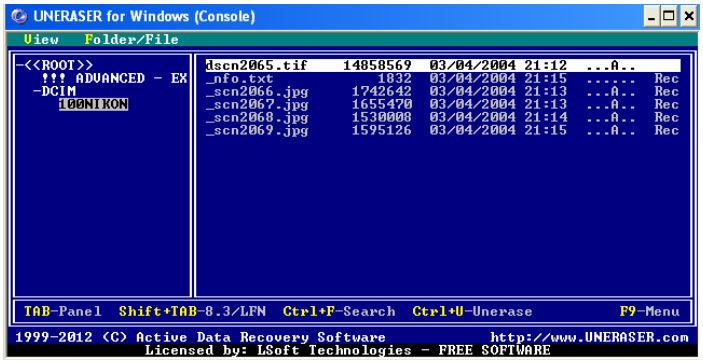


Figura 4.3.9.2.2-15 UNERASER examina carpeta 100NIKON

4.3.9.2.3. Recuperación de información mediante Uneraser

Esta herramienta también nos proporciona la recuperación de archivos que esten en buen estado, así como lo hizo Autopsy esta herramienta también lo puede hacer. Primeramente recuperaremos todos los archivos que estan en la raiz, como por ejemplo **_LUEPR.JPG,** presionando Ctrl +u sobre el archivo se mostrar una ventana en donde le asignaremos la ruta en donde lo vamos a guardar. En este caso lo almacenaremos en una carpeta llamada **RecuperacionUneraser,** creada en el una unidad C.

Figura 4.3.9.2.3-1 UNERASER Guardando Archivo _LUEPR.JPG

Luego nosotros realizamos los mismos pasos para los demás archivos que nos faltan de recuperar , aquí se muestra unas imágenes del proceso.

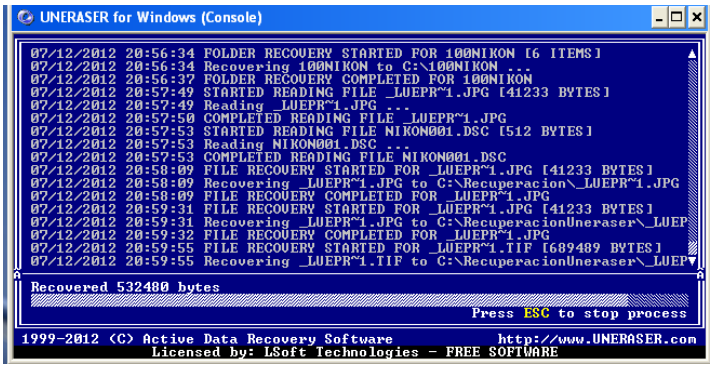


Figura 4.3.9.2.3-2 UNERASER Guardando Archivos Faltantes

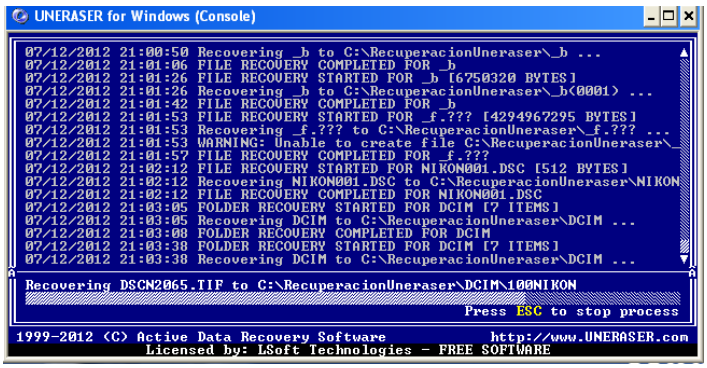


Figura 4.3.9.2.3-3 UNERASER Guardando Archivos de la Carpeta DCIM

Aquí podemos observar una vista preliminar los archivos que se recuperaron.

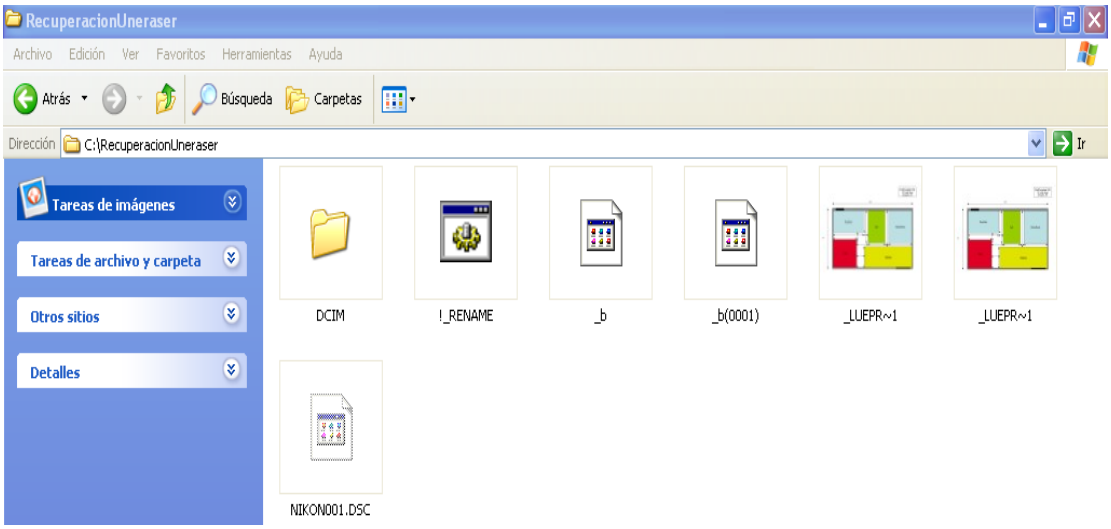


Figura 4.3.9.2.3-4 Vista Preliminar de los Archivos de la Raíz

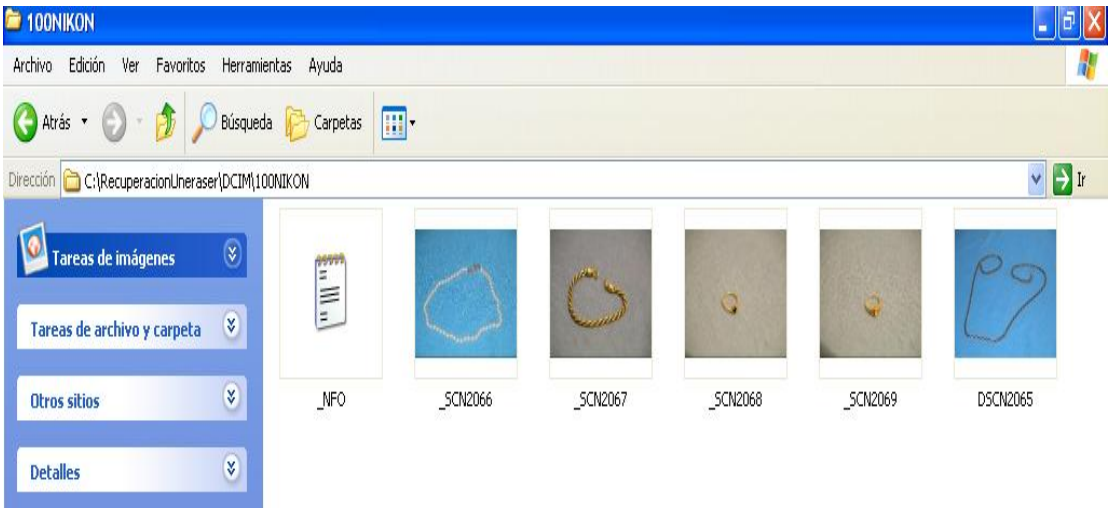


Figura 4.3.9.2.3-5 Vista Preliminar de los Archivos de la Carpeta DCIM

4.3.9.3. PC Inspector File Recovery

Esta es otra herramienta que nos permitirá recuperar la información borrada producto de una formateada, ya que nosotros tenemos que demostrar si hay mas información oculta que podria estar escondida y que seria de gran utilidad para sumar mas evidencias de las que ya contamos. Con esta herramienta vamos a determinar los siguientes puntos:

- Explorando Pc Inspector.
- Recuperación de archivos mediante Pc Inspector.

4.3.9.3.1. Explorando PC Inspector

Una vez instalada esta importante herramienta, la podremos ejecutar desde su acceso directo en el escritorio o buscandola atraves del menú inicio. Cuando se ejecuta de desplegara su interfaz grafica, en la cual nos va pedir que seleccionemos el idioma y nosotros simplemente escogemos **Spanish** y damos clic en el icono verde para aceptar.

Figura 4.3.9.3.1-1 PC Inspector Escogiendo Idioma

Luego se presentará otra ventana con varias opciones a escoger, nosotros escogeremos la segunda que dice **Encontrar datos perdidos**, porque esta permitirá encontrar datos razón de una formateada hacia el dispositivo.

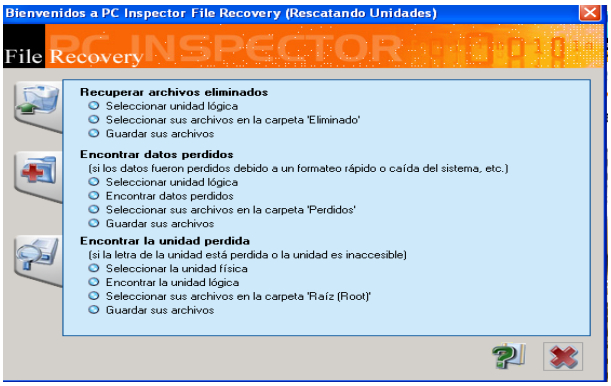


Figura 4.3.9.3.1-2 PC Inspector Escoger la Opción Datos Perdidos

Ahora PC Inspector comenzara a explorar todas las unidades montadas, nosotros escogemos la unidad F y damos clic en el icono verde para continuar.

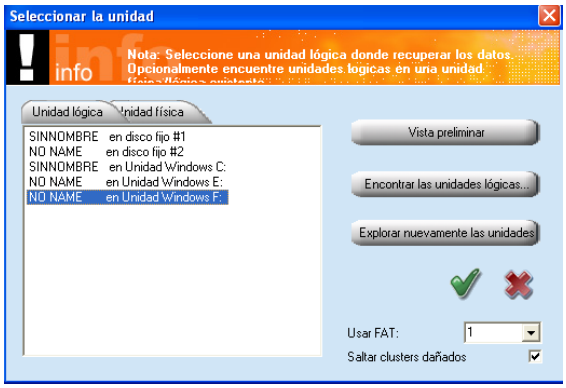


Figura 4.3.9.3.1-3 PC INSPECTOR Explorar Unidades

Luego nos pedirá que asignemos el número del cluster que vamos a empezar a buscar, nosotros digitaremos el número 0 para que empieze desde el comienzo, aceptamos y veremos el proceso de búsqueda.

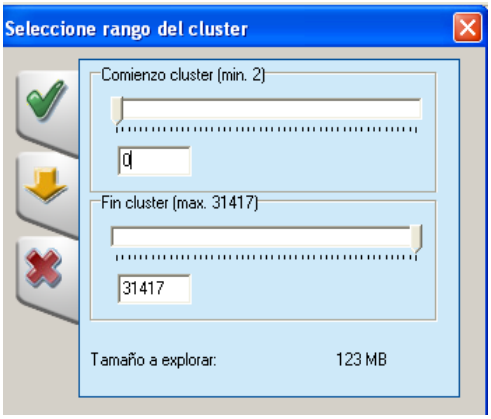


Figura 4.3.9.3.1-4 PC Inspector Asignar la Búsqueda en el Clúster

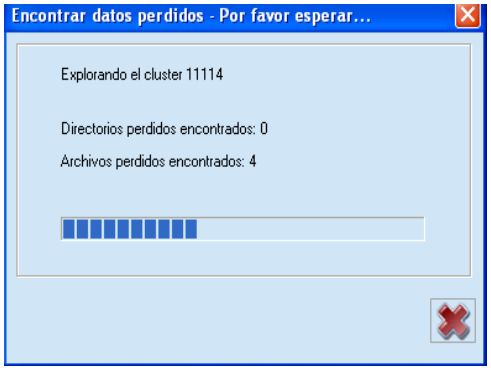


Figura 4.3.9.3.1-5 PC Inspector Proceso de Búsqueda

4.3.9.3.2. Recuperación de archivos mediante PC Inspector

Cuando termina la respectiva busqueda, nos daremos cuenta que encuentra archivos que estan como perdidos, entonces procedemos a recuperarlos en una carpeta creada en el **C:** llamada **RecuperacionPCInspector/Perdidos.**

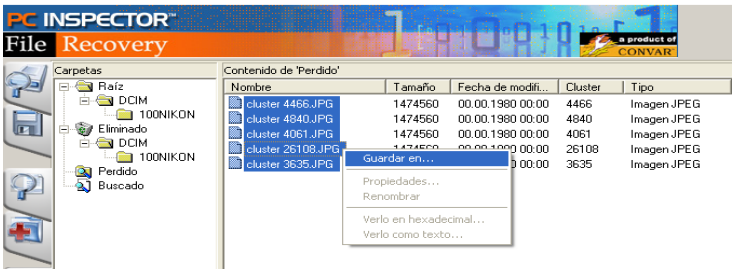


Figura 4.3.9.3.2-1 PC Inspector Recuperar Archivos Perdidos

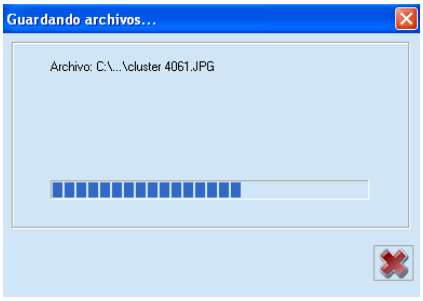


Figura 4.3.9.3.2-2 Proceso de Recuperación de Archivos Perdidos

Al finalizar este proceso de recuperación nos dirigimos hacia la carpeta creada y nos daremos cuenta que son las mismas imágenes mostradas aneriormente.

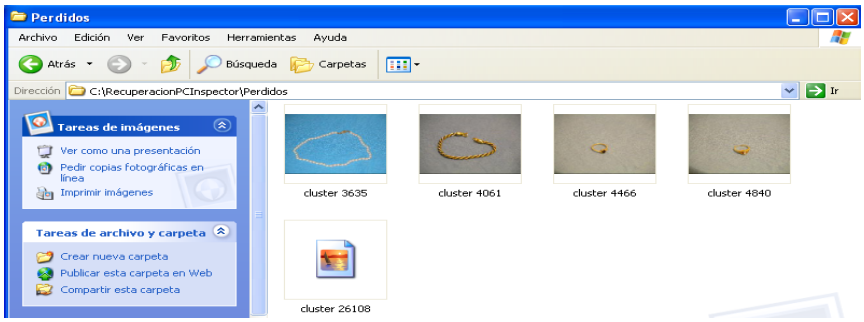


Figura 4.3.9.3.2-3 Carpeta de Recuperación de Archivos Perdidos

Luego exploraremos las demás carpetas en busca de otras nuevas pistas, pero encontramos la misma información que encontraron las demás herramientas forenses. Aquí les mostramos la exploración de todas las carpetas.

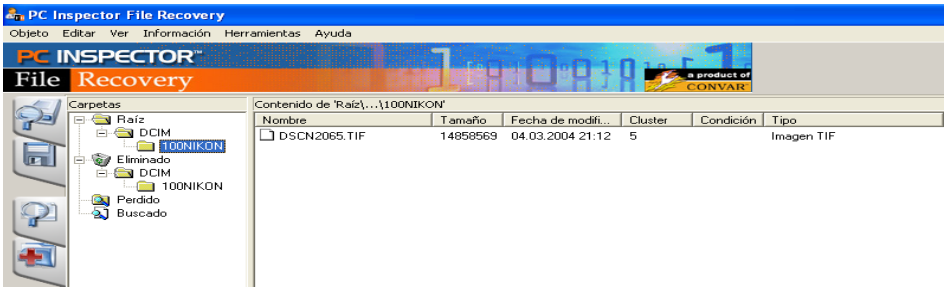


Figura 4.3.9.3.2-4 PC Inspector Explorando Raíz

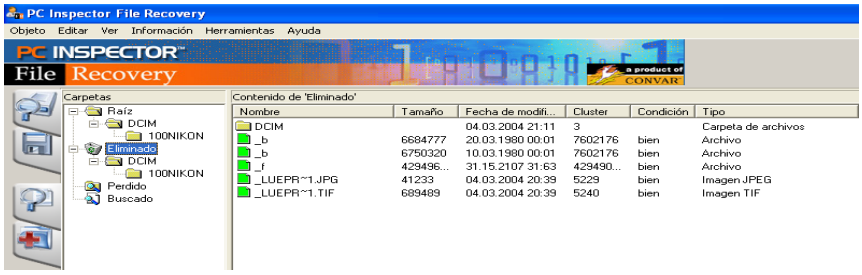


Figura 4.3.9.3.2-5 PC Inspector Explorando Eliminados

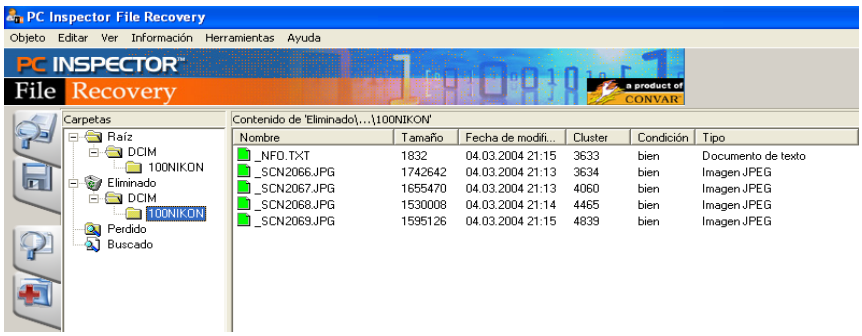


Figura 4.3.9.3.2-6 PC Inspector Explorando Carpeta 100NIKON

4.4. Análisis Mediante Autopsy

Una vez recuperada toda la información borrada procedemos a realizar un respectivo análisis de la información que estaba almacenada en la imagen forense.

4.4.1. Análisis mediante la línea de tiempo en Autopsy

Para un análisis mas influyente, en la cual investigaremos toda la serie de pasos que el sospechoso realizó para conseguir su objetivo. Por esta razon Autopsy nos provee esta opción, que nos permitirá saber todos los sucesos ocurridos ordenadamente.

Primeramente en la ventana principal seleccionaremos la raiz en donde esta montada nuestra imagen forense y luego nos dirigimos a la opción de **File Activity Time Lines.**

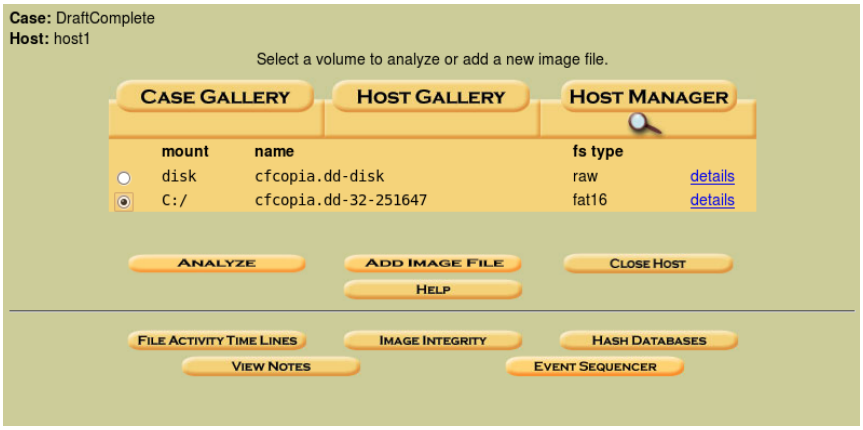


Figura 4.4.1-1 Accediendo a la Ventana de Tareas de Autopsy

Luego de esto crearemos un nuevo archivo, el cual estos archivo son meta-datos que se extraen del sistema de arhivo de la imagen forense y se la almacena en un archivo de cuerpo. Dicha opción se encuentra en la parte superior de la ventana.

Figura 4.4.1-2 Escogiendo Opciones para la Línea de Tiempo

Luego procedemos a seleccionar todas las opciones, en la cual estas opciones nos idican la siguiente información:

La primera opción : Nos permitirá a seleccionar la raíz en donde se encuentra montada nuestra imagen.

La segunda opción: Aquí tendremos dos opciones que son **Allocated Files** y **Unallocated Files**.

- ✓ **Allocated Files:** Esta opción nos va a permitir observar todos los archivos que conienen una estructura de nombre de arhivo asignado.

- ✓ **Unallocated Files:** Esta opción nos va permitir observar todos los arhivos que han sido eliminados o los archivos huerfanos que son archivos que no tienen un nombre valido pero cuyos metadatos todavia existen.

La tercera opción : Esta es aquella que crea el nombre del archivo del cuerpo. Este archivo se creará en el directorio de salida y por último establecerá un cálculo de valores de MD5.

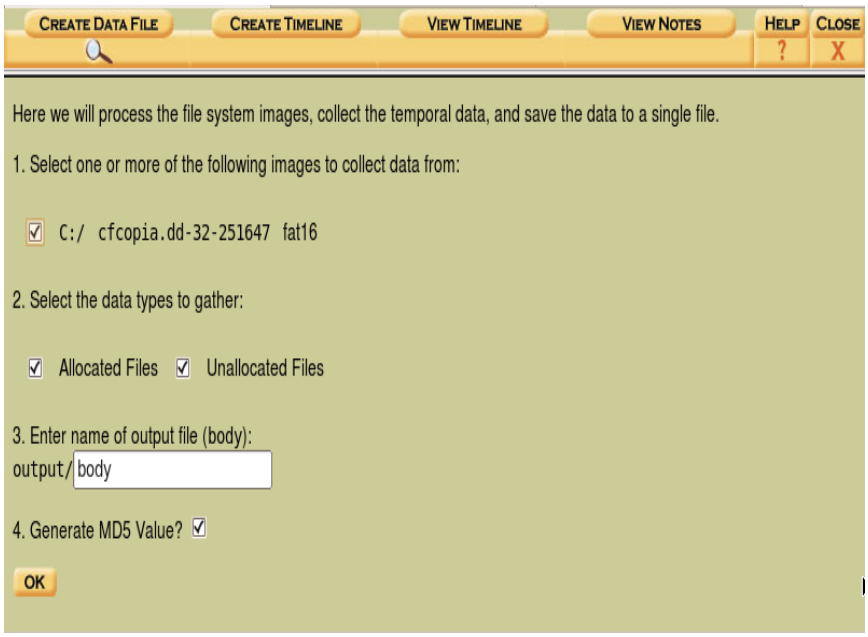


Figura 4.4.1-3 Configurando Parámetros de la línea de Tiempo

A continuación se presenta un resumen en donde indica la dirección del archivo guardado y el cálculo de los valores de md5, entonces daremos clic en Ok para continuar.

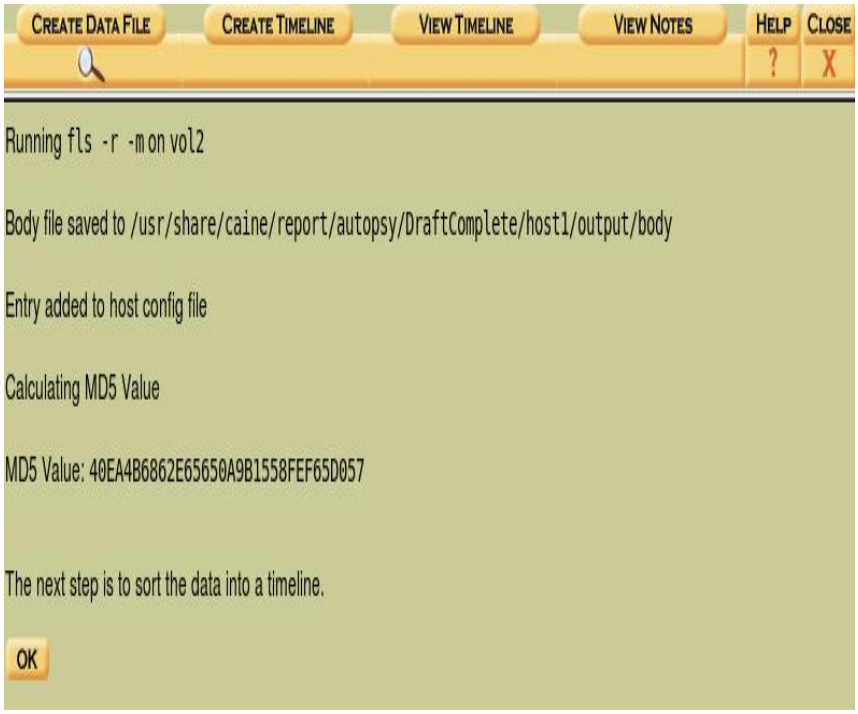


Figura 4.4.1-4 Resumen de la Configuración del Cuerpo

En esta ventana nos permitirá seleccionar una serie de opciones, en la cual solo utilizaremos la opción 2 y 3, que nos permiten buscar todos los datos desde una fecha de inicio y una fecha de finalización.

Si nos damos cuenta, al momento que recuperamos nuestros archivos eliminados todas las estas tareas realizadas por el sospecho fueron en el 2004, por esta razon vamos hacer una busqueda desde Enero del 2004 hasta diciembre del 2004 y en la siguiente ventana se presentará un resumen, solo daremos clic en ok para poder continuar.

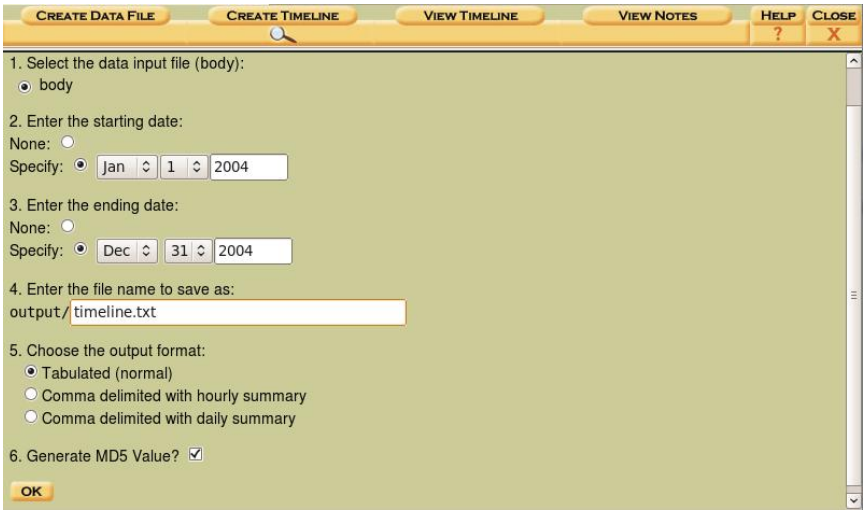


Figura 4.4.1-5 Búsqueda de Datos Mediante Fechas

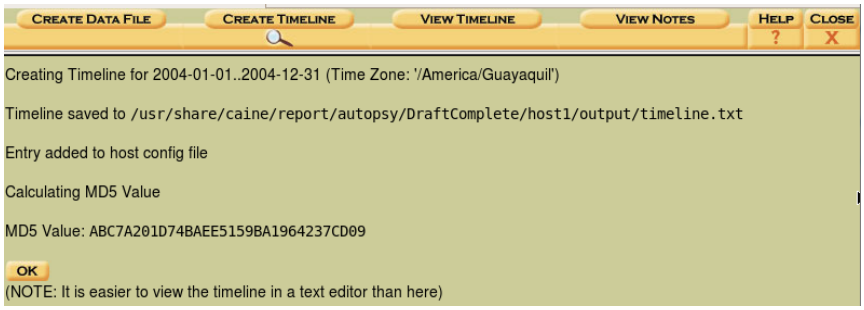


Figura 4.4.1-6 Resumen de la configuración de la Línea de Tiempo

Como nos podemos dar cuenta estas son todas las tareas que realizó el sospechoso. Esta ventana nos proporciona un análisis óptimo de la actividad que realizan los archivos. Además nos podemos dar cuenta que solo en Marzo del 2004 realizó tareas de eliminación de archivos. Esta ventana nos permite ordenar de forma automatica la actividad de los archivos según la hora y minutos que vaya relizando.

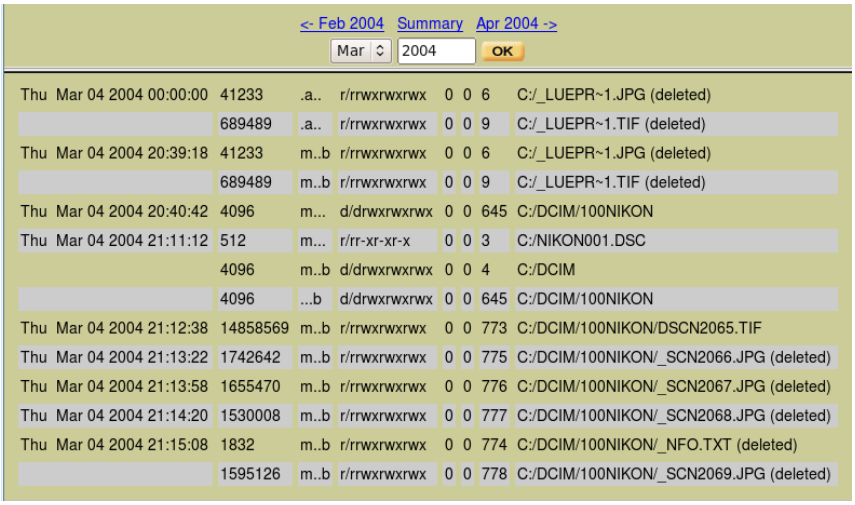


Figura 4.4.1-7 Archivos Ordenados mediante la Línea de Tiempo

Si queremos también podemos observar este archivo en un **.txt**, desde la linea de comandos accederemos al directorio en donde se encuentra almacenado nuestro archivo. El nombre de este archivo es **timeline.txt**.

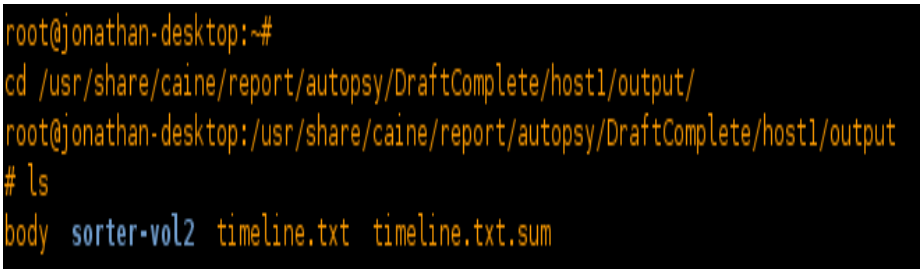


Figura 4.4.1-8 Accediendo al archivo timeline.txt

Luego con el comando cat accedemos a ver el contenido del archivo **timeline.txt**

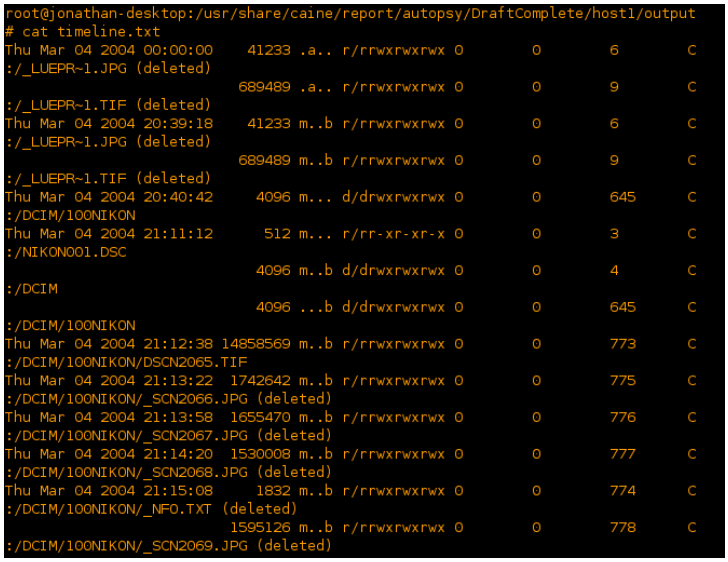


Figura 4.4.1-9 Contenido del Archivo timelines.txt

Bruce tenía 7 imágenes en su Memoria Flash 5 pertenecian a joyas y dos pertenecian a los planos del edificio. Entonces como nos podemos darnos cuenta a las 00:00:00 Bruce comenzó eliminando 1 archivo , este arhivo hace referencia hacia los planos del edificio.

Figura 4.4.1-10 Imagen Borrada a las 00:00:00

Luego en la noche se dedico a exclusivamente a eliminar archivos. Comenzando por la otra imagen del plano del edificio.

Ahora, Bruce ya había eliminado las dos imágenes con respecto a los planos, es decir ahora solo contenía 5 imágenes que pertenecian a Joyas.

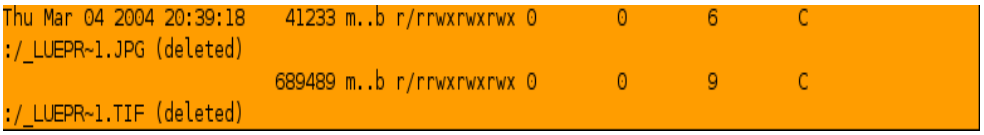


Figura 4.4.1-11 Dos Imágenes eliminadas a las 20:39:18

Luego accedió dos veces a la carpeta 100NIKON a las 20:40:42 y luego a las 21:11:12, para comenzar a borrar mas archivos almacendados en dicha carpeta, en este caso las otras imágenes que restan.

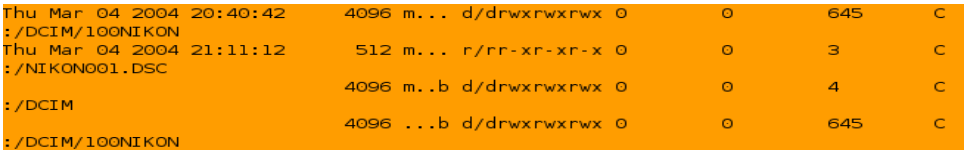


Figura 4.4.1-12 Accediendo a Diferentes directorios

Aquí podemos observar que Bruce comienza hacera realizar un borrado de todas las imágenes que estan contenidas en esa carpeta inculyendo a un archivo de texto llamado _**NFO.txt**.

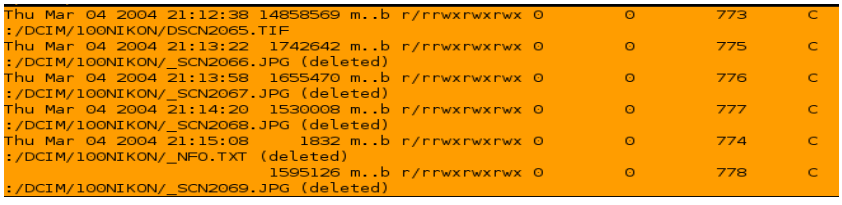


Figura 4.4.1-13 Archivos Borrados de la carpeta 100NIKON

El archivo _**NFO.txt** nos da información de la configuración de la cámara, así como también información de aquellas imágenes contenidas en la ruta de esta carpeta, por esta razón Bruce también tuvo que eliminar este archivo.

A continuación veremos toda la información que contenía este archivo, haciendo uso del comando cat observaremos la información de las imágenes almacenadas, como este archivo posteriormente tambien se recuperó, en la linea de comando digitaremos:

cat /home/caine/Tesis/ RespaldoInformacion/vol2C..DCIM.100NIKON._NFO.TXT

Como podemos observar en las siguientes imagenes, cada una de las imagenes almacenadas contiene su propia información.

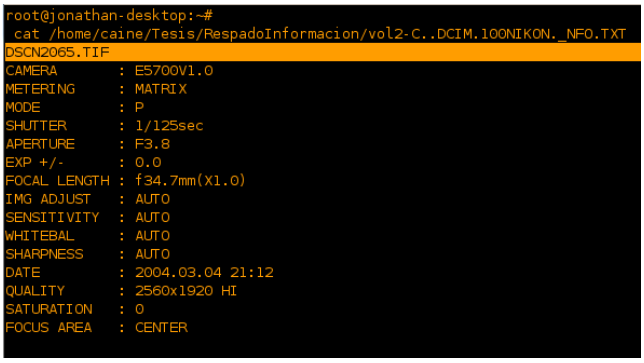


Figura 4.4.1-14 Información de la imagen DSCN2065.TIF

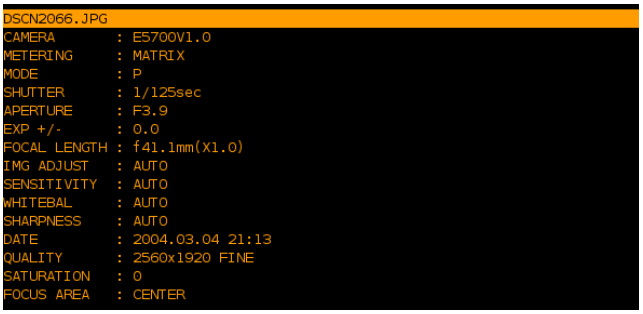


Figura 4.4.1-15 Información de la imagen DSCN2066.JPG

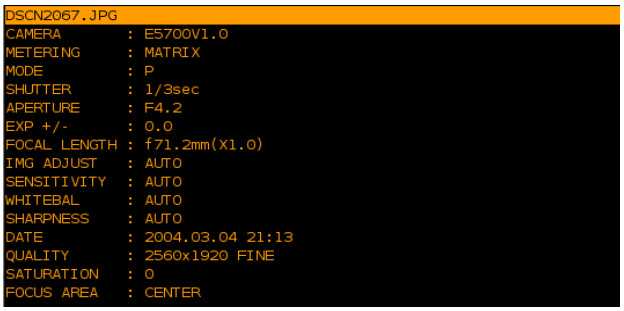


Figura 4.4.1-16 Información de la imagen DSCN2067.JPG

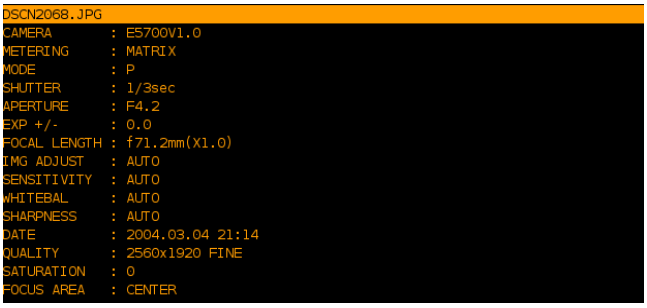


Figura 4.4.1-17 Información de la imagen DSCN2068.JPG

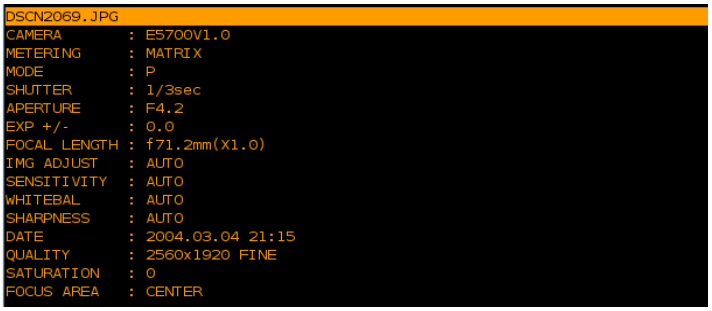


Figura 4.4.1-18 Información de la imagen DSCN2069.JPG

4.4.2. Análisis de Metadatos en Autopsy

Los metadatos son aquella información que se inserta en los archivos una vez que son creados. Estos contienen información acerca de la creación de la creación del archivo, nombre del autor, autores anteriores, así como la fecha de creación y modificación.

Esta información es de gran importancia, debido a que podemos demostrar en que tipo de cámara fueron tomadas las fotos del caso que estamos analizando.

Para acceder a esta opción nos dirigimos a la parte inicial de la pestaña **FILE ANALYSIS** de Autopsy y una vez listado todos los archivos, se desplegaran diferentes tipos de columnas, nosotros utilizaremos la columna llamada **Meta** y haremos clic sobre el número en la cual esta alojado nuestro metadato, del correspondiente archivo a analizar.

El primer archivo que analizaremos va hacer LUEPR~1.JPG que contiene el metadato número 6.

Type dir / in	Name	Written	Accessed	Created	Size	UID	GID	Meta
r / r	_LUEPR~1.JPG	2004-03-04 20:39:18 ()	2004-03-04 00:00:00 ()	2004-03-04 20:39:18 ()	41233	0	0	6
r / r	_LUEPR~1.TIF	2004-03-04 20:39:18 ()	2004-03-04 00:00:00 ()	2004-03-04 20:39:18 ()	689489	0	0	9

Figura 4.4.2-1 Empezando con el Análisis de Metadatos

Una vez dado clic sobre el número del metadato, se abrirá otra ventana indicándonos un resumen de información del archivo, tales como de que tipo es, su tamaño, su hash, ect. Si lo queremos ver de una manera mas detallada haremos clic en la parte superior que dice **Report**.

Figura 4.4.2-2 Información del Archivo LUEPR~1.JPG

Al acceder a esta opción nos dará toda información correspondiente al archivo, tales como:

- ✓ Su fecha de creación
- ✓ En que lugar reside
- ✓ Cual es el formato del archivo

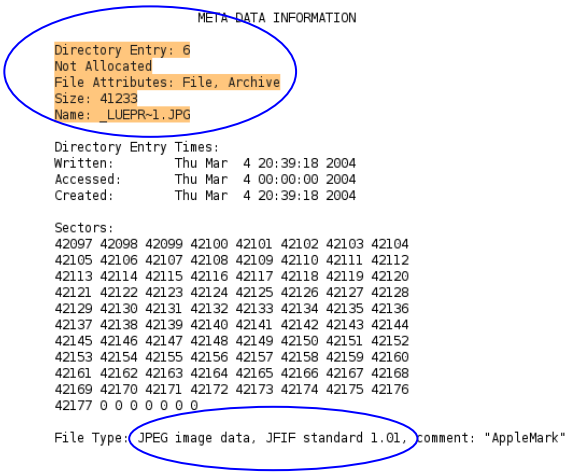


Figura 4.4.2-3 Información Meta Data del Archivo LUEPR~1.JPG

Como podemos ver, este archivo en realidad se trata de imagen JPEG de tipo JFIF. El estandar JPEG tiene diferentes variaciones en la cual los dos tipos mas comunes son EXIF y JFIF. Ambos archivos se clasifican como archivos JPEG, la diferencia es debida a los datos suplementarios que se agregan a la imagen original durante el proceso de la cámara. La mayoría de cámaras digitales solo puede mostrar imágenes con formato EXIF.

El valor en hexadecimal de una imagen JPEG es cuando su cabecera comienza con FFD8 FFE0 o 1 y como podemos observar en nuestra imagen este valor es el correcto.

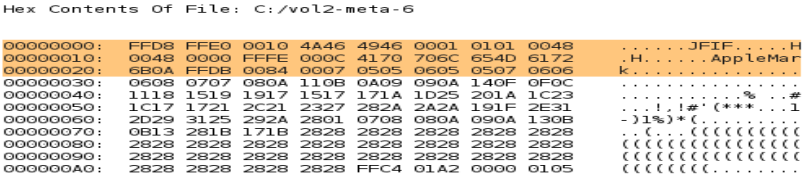


Figura 4.4.2-4 Vista Previa en Hexadecimal del Archivo LUEPR~1.JPG

Esta es la información de la segunda imagen llamada LUEPR~1.TIF, como podemos observar en la imagen, aquí se muestra la información metada del archivo y realizando un análisis de string podemos observar que esta imagen se creó con un software llamado CoreGraphics que pertenece al sistema operativo Mac.[9]

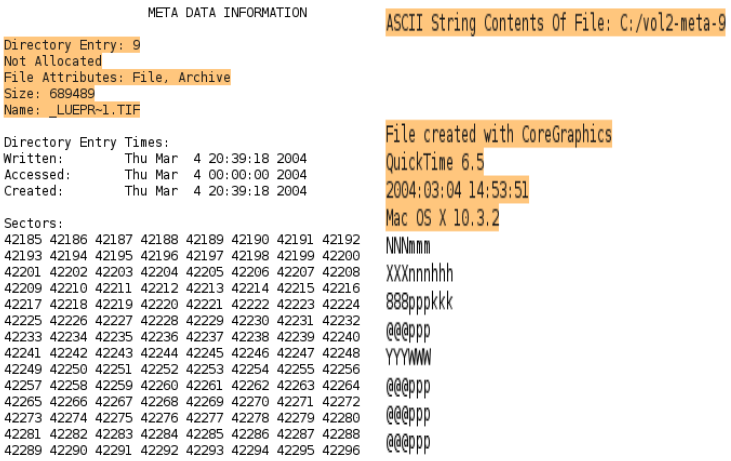


Figura 4.4.2-5 Análisis de Meta Dato del Archivo LUEPR~1.TIF

Esta es la información metada del archivo llamado NIKON001.DSC

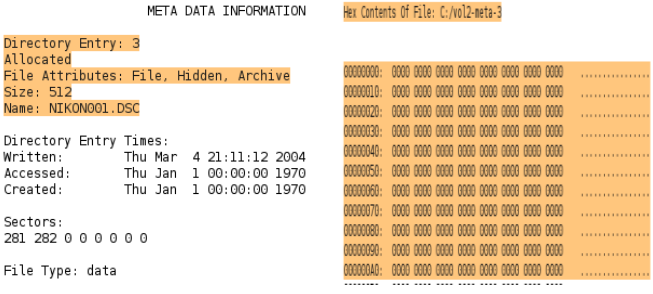


Figura 4.4.2-6 Análisis de Meta Dato del Archivo NIKON001.DSC

También procedimos a analisar el archivo _NFO.TXT, como podemos darnos cuenta este es solo un archivo de texto.

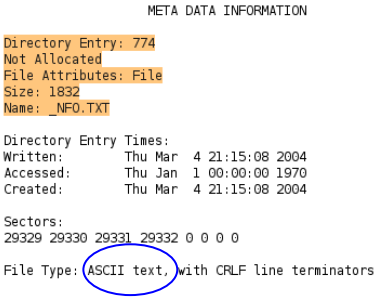


Figura 4.4.2-7 Análisis de Meta Dato del Archivo _NFO.TXT

Por último analizamos las demás imágenes que faltan, en la cual todas estas estaban configuradas en la mostración visual para la cámara digital, es decir estaban enlazadas mediante el archivo _NFO.TXT, para almacenar su información. Además nos podemos dar cuenta que las imágenes DSCN2066.JPG, DSCN2067.JPG, DSCN2068.JPG y DSCN2069.JPG utilizan el formato EXIF.

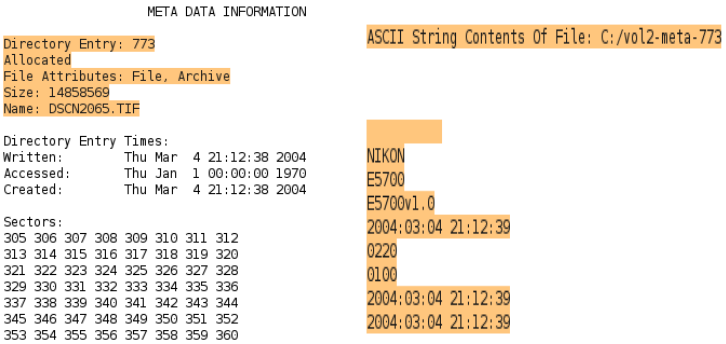


Figura 4.4.2-8 Análisis de Meta Dato del Archivo DSCN2065.TIF

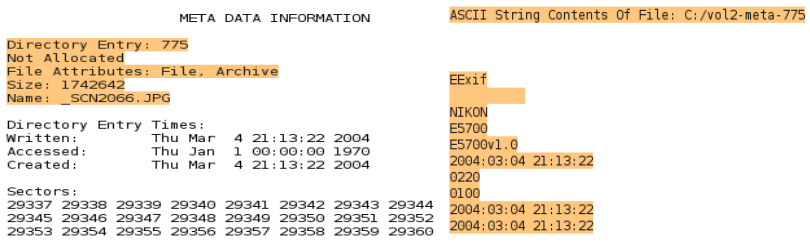


Figura 4.4.2-9 Análisis de Meta Dato del Archivo _SCN2066.JPG

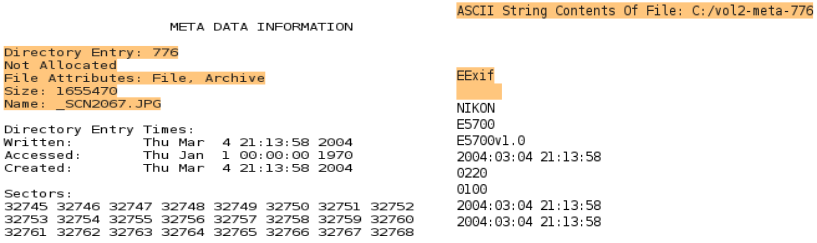


Figura 4.4.2-10 Análisis de Meta Dato del Archivo _SCN2067. JPG

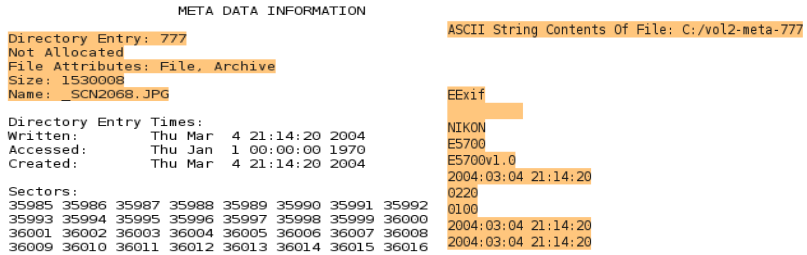


Figura 4.4.2-11 Análisis de Meta Dato del Archivo _SCN2068. JPG

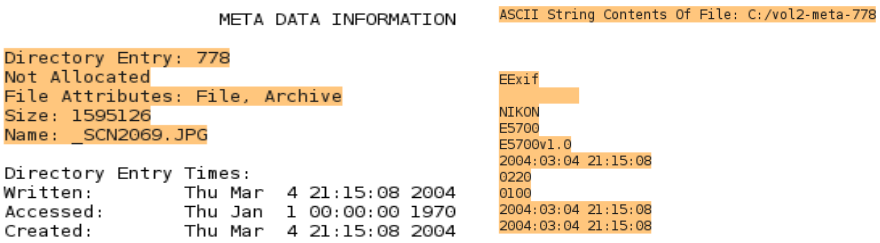


Figura 4.4.2-12 Análisis de Meta Dato del Archivo _SCN2069.JP

4.5. Estegoanálisis

Toda la información respaldada en su mayoria, eran imágenes, por esta razón tuvimos la necesidad de realizar un análisis de todas estas images, para ver si encontrábamos algun texto oculto, en donde Bruce Amiter se pudiera estar comunicando de esa manera con otras personas.

Caine nos proporciona una herramienta de estegoanálisis llamada **Stegdetect**, esta herramienta nos ayudará a determinar si existe alguna tarea estenográfica en estas imágenes. Esta herramienta se puede ejecutar de dos maneras:

- ✓ Linea de comando
- ✓ Interfaz Gráfica

4.5.1. Stegdect mediante linea de comando

Para la ejecución de esta herramienta tendremos que acceder primeramente a la ruta del directorio que contiene las imágenes y luego dijitamos el comando **stegdetect *.JPG**, en la cual le estamos diciendo que haga un análisis estenografico de todas las imágenes JPG.

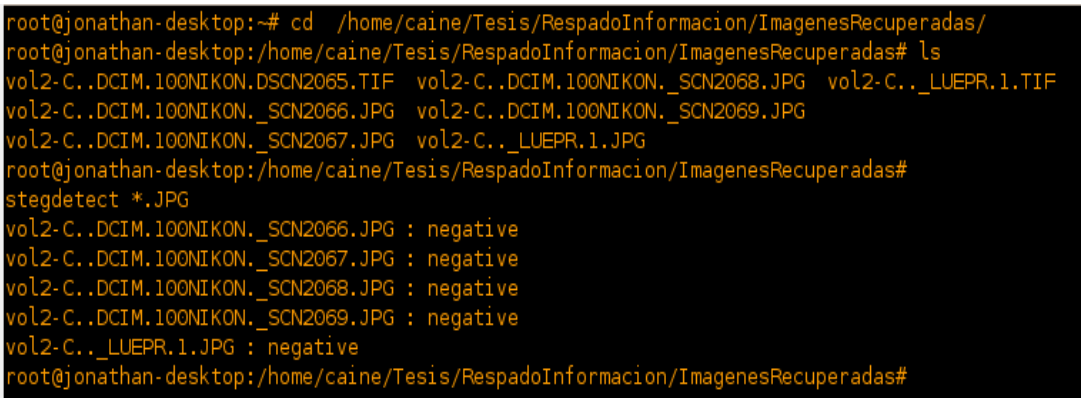


Figura 4.5.1-1 Stegdect Análisis mediante línea de Comando

Como resultado observaremos que no existe esteganografía en dichas imágenes analizadas por la herramienta, esta herramienta solo puede hacer un estegoanálisis de imágenes JPG.

4.5.2. Stegdect mediante interfaz grafica

Para la ejecución gráfica de esta herramienta, en la linea de comando la podemos ejecutar digitando **xsteg&.**

Figura 4.5.2-1 Ejecutando Xsteg mediante Línea de Comando

Esta es la interfaz gráfica para stegdetect, en donde cumple las mismas funciones que en linea de comandos, pero esta es mas amigable de usar.

Activaremos todas las opciones para su respectivo análisis y luego iremos a el menu **File** y seleccionaremos **Open**.

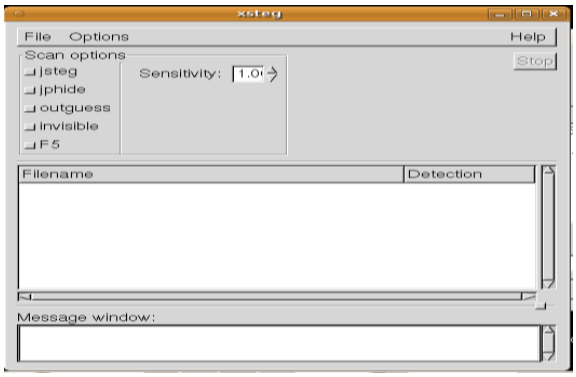


Figura 4.5.2-2 Xsteg Interfaz Grafica

En la siguiente tendremos que buscar nuestra directorio que contiene nuestras imágenes JPG y luego iremos seleccionando cada imagen para realizar el estegoanálisis.

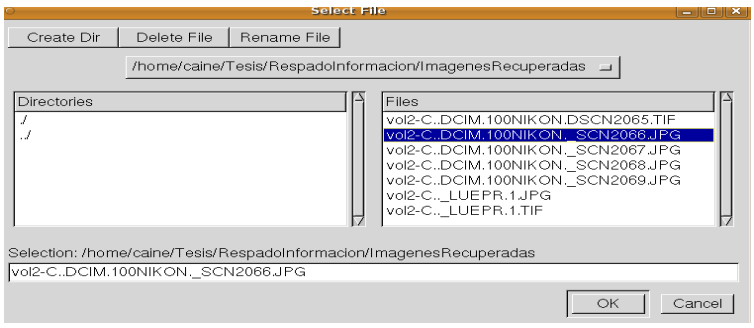


Figura 4.5.2-3 Xsteg Buscando Directorio de las Imágenes

Como nos podemos dar cuenta en la siguiente imagen ya hemos abierto todas nuestras imágenes JPG y el resultado de nuestro estegoanálisis dio

negativo, es decir que esta herramienta no detecto algun tipo de esteganografía en la imágenes. [6]

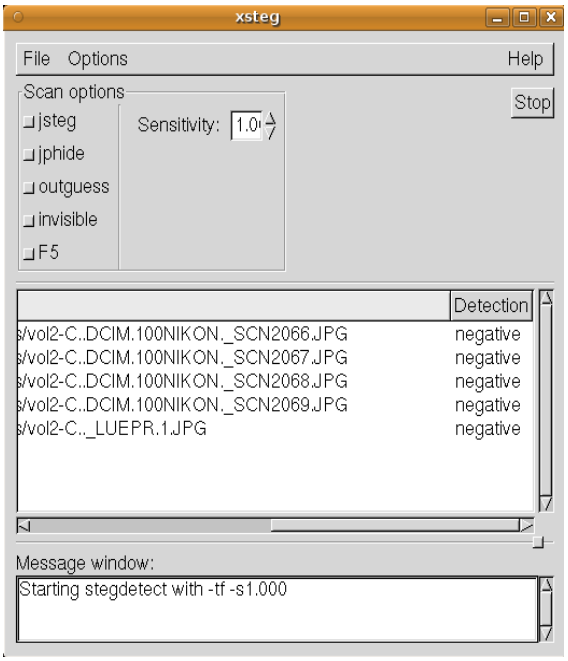


Figura 4.5.2-4 Xsteg Realizando Análisis

4.5.3. Análisis mediante Stegsecret

Esta es otra herramienta diseñada para realizar un estegoanálisis de imágenes JPG. Dicha herramienta la ejecutaremos bajo Windows en la cual esta herramienta trabaja exclusivamente con plataforma JAVA, así que para poderla ejecutar deberiamos tener Java instalado.

Debido a que esta herramienta solo deteccta las imágenes JPG, almacenaremos todas nuestras imagenes JPG en una carpeta especial.

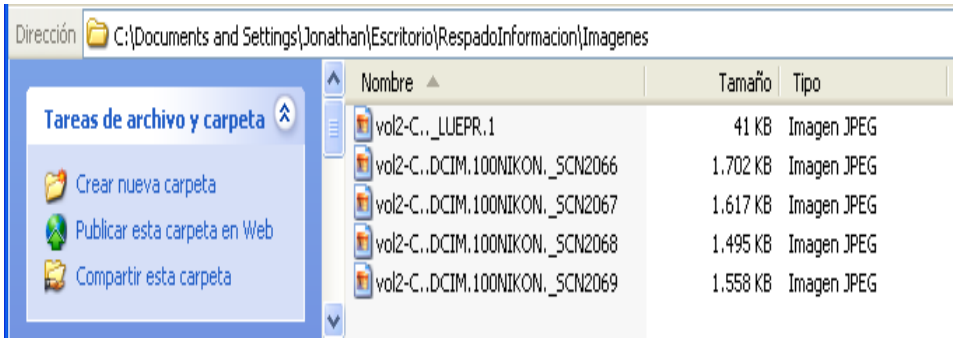


Figura 4.5.3-1 Imágenes Listas para Estegoanálisis – Stegsecret

Luego procedremos a ejecutar nuestra herramienta, si no tenemos java instalado deberiamos primero instalarlo y luego ejecutar el archivo **xstegsecret.**

Figura 4.5.3-2 Comenzando a Ejecutar Stegsecret

Una vez ejecutada la herramienta se abrira su amigable interfaz grafica que posee esta maravillosa herramienta, en la cual nuestro principal objetivo es la detección de esteganografía en las imágenes que vamos a realizar el análisis. Así que seleccionaremos la opción de **Herramienta de Detección.**

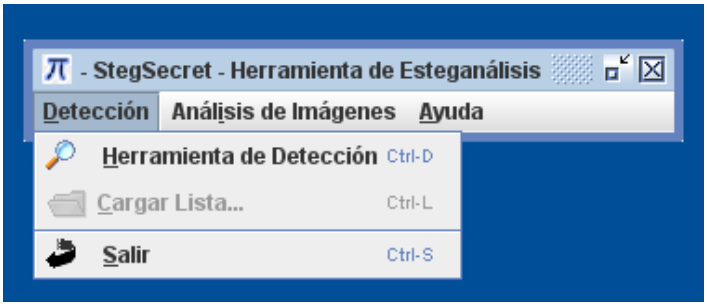


Figura 4.5.3-3 Seleccionar Herramienta de Detección Stegsecret

Ahora en la parte del árbol de directorios buscaremos nuestro directorio que contiene las imágenes y una vez encontrado dicho directorio daremos clic en el icono donde esta la lupa para que realice el estegoanálisis. Como resultado de la herramienta observaremos que tampoco existe esteganografía en las imágenes.

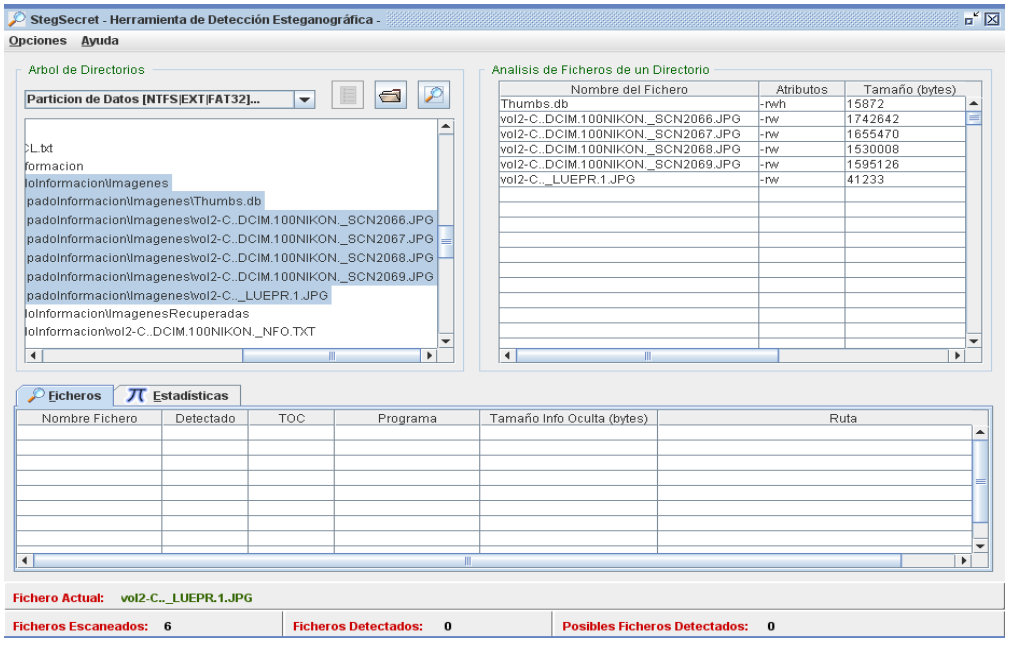


Figura 4.5.3-4 Stegsecret Análisis Finalizado de IMÁGENES

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. Con la comparación de los hashes extraídos de la imagen original y la copia se logró determinar que no se manipulo la evidencia.

2. A través de nuestro análisis forense se logró determinar que existía información que había sido eliminada.

3. Toda la información eliminada dentro de la imagen forense se logró recuperar con éxito.

4. Se logró determinar que no existía más información eliminada después de un formateo hacia la unidad.

5. A través de la línea de tiempo se logró efectuar cual fue el orden en que se eliminó la información.

6. A través de un análisis de metadatos se logró comprobar la información contenida en cada una de los archivos que fueron eliminados.

7. Se logró comprobar que no existía esteganografía en la información que se recuperó.

8. Con respecto a todas las evidencias encontradas se concluye que Bruce Armitter es culpable de la acusación del robo de información.

RECOMENDACIONES

1. Elaborar una Política de Seguridad Informática basada en el estándar ISO 27001 e implementar un Sistema de Gestión de Seguridad Informática (SGSI) que permita gestionar indicadores de cumplimiento de la política.

2. Establecer controles de seguridad física apropiados en la empresa, instalando cámaras de seguridad en todos los departamentos y realizando una revisión a todo el personal para determinar los dispositivos que salen de la empresa.

3. Rediseñar la arquitectura de red para incluir controles de seguridad informática que garanticen la confidencialidad, disponibilidad e integridad de la información.

4. Incluir dentro de la Política de Seguridad Informática procedimientos para el buen uso del internet y del correo electrónico, con el fin de prevenir que se filtre información confidencial o que se pierdan datos importantes para la organización.

5. Implementación de contrafuegos internos y sistemas de prevención de intrusos en el diseño de red, para prevenir los intentos no autorizados de accesos por posibles atacantes.

6. Asignar una contraseña al BIOS de todas las máquinas, para poder bloquear dispositivos que no deberian utilizar en los departamentos, así como puertos USB o CD / DVD e implementar un sistema de prevención de pérdida de datos (DLP).

7. Se recomienda implementar dispositivos de comunicación que utilicen mecanismos de control de admisión a la red (NAC).

8. Establecer una limitación a los permisos de las cuentas de usuarios, determinando el nivel de acceso que deberían tener los usuarios a los recursos de la red.

9. Capacitar periódicamente al personal de la empresa sobre medidas preventivas para asegurar su información.

ANEXOS A

ESET ENDPOINT SECURITY

Esta nueva tecnología presente en la nueva generación de soluciones de ESET permite comparar la reputación de archivos con una base de archivos seguros que se encuentra en Internet, la cual va creciendo gracias a la utilización de los usuarios, si un archivo fue previamente analizado por un usuario este quedara guardado en la base, lo que reducirá los tiempos de espera de futuros análisis del mismo archivo, ya que comparara los resultados obtenidos por el resto de los usuarios.

Características

Detección Inteligente:

ESET Endpoint Security se enfoca en la detección proactiva de malware utilizando Heurística Avanzada para protegerlo de las amenazas desconocidas y utiliza bases de firmas genéricas para detectar familias de malware ya conocido. Las computadoras son más vulnerables a las amenazas de internet durante el proceso en que son liberadas hasta que se genera la base de firmas correspondiente. La poderosa tecnología de ESET detrás del motor ThreatSense minimiza los riesgos de infección durante esta brecha de tiempo.

Correo electrónico limpio y seguro:

Más allá de que su empresa use Microsoft Outlook, Outlook Express, Mozilla Thunderbird, Windows Live Mail, Windows Mail, u otro cliente de correo electrónico POP3/IMAP, ESET Endpoint Security mantendrá su correo electrónico libre de cualquier tipo de malware. Además podrá evitar el molesto correo basura creando listas negras o listas blancas para categorizar el correo basura.

Control de acceso web:

Asigne permisos a usuarios o grupos de ellos dentro de su empresa para definir qué sitios web pueden ser accedidos o no. El control de acceso web cuenta con más de 140 categorías como por ejemplo: redes sociales, contenido para adultos, buscadores, mensajería instantánea, entre otras. Además podrá crear exclusiones para permitir o denegar el acceso a sitios web específicos dentro de las categorías asignadas.

Firewall personal:

Controle el tráfico de red de sus estaciones de trabajo definiendo protocolos, puertos o aplicaciones que pueden hacer uso de la red. El firewall personal de ESET Endpoint Security puede trabajar de varios modos, entre ellos el interactivo consultando que acción realizar ante cada conexión detectada en el equipo, el modo aprendizaje detecta los protocolos, puertos y aplicación más utilizados, generando reglas que permiten dichas conexiones. Además

posee un modo de configuración avanzado para los usuarios con mayor conocimiento técnico.

Autenticación de zonas de confianza:

Esta función permite identificar las zonas de red confiables por medio de las configuraciones de red (una combinación configurable de la dirección IP del servidor principal / DNS/ DHCP, red inalámbrica SSID, el perfil de conexión, etc.) y realizar la autenticación segura para el acceso a una red usando el Servidor de Autenticación de ESET.

Control de dispositivos:

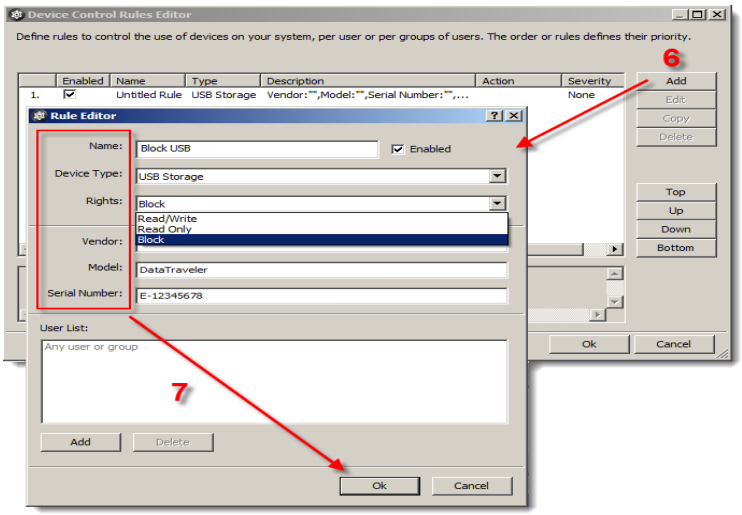


Figura 4.5.3-1 Control de dispositivos ESET

Tomado de: www.eset-la.com

ESET Endpoint Security podrá crear reglas para un usuario específico o un grupo de usuarios para permitir qué tipos de dispositivos pueden ser utilizados o no dentro de su empresa a partir de la definición de políticas por familia de dispositivos, marca o modelo. También podrá establecer los permisos de lectura y/o escritura de acuerdo a sus necesidades, y bloquear unidades de CD /DVD, dispositivos de almacenamiento masivo, impresoras USB, dispositivos Bluetooth, lectores de memorias, entre otros. Además, al momento de conectar el dispositivo en el equipo, ESET Endpoint Security le preguntara si desea analizar el mismo, o si desea crear una regla para realizar determinadas acciones sobre ese dispositivo.

ESET Remote Administrator:

Realice la instalación remota y la administración de todos los clientes de la red desde una única consola central, además puede aplicar políticas de seguridad para mantener la máxima protección activa en sus clientes. Configure distintos tipo de alertas para que se envíen a sus administradores por correo electrónico. Además podrá centralizar las actualizaciones de base de firmas para que los equipos se actualicen de manera interna sin consumir ancho de banda de manera innecesaria.

ANEXOS B

CRYPTZONE

Ayuda a las organizaciones a proteger su activo más valioso: la información. Sus soluciones ayudan a evitar fugas de datos y aseguran que los datos estarán protegidos en todo momento, vayan dónde vayan.

Beneficios de la tecnología de cifrado USB

Cuidar de la seguridad de los medios de almacenamiento extraíbles del tipo USB, es uno de los retos más importantes que en términos de seguridad informática enfrentan la mayoría de empresas en la actualidad. En vista de que el uso de este tipo de dispositivos se ha vuelto tan común, las organizaciones enfrentan la amenaza de tener su propiedad intelectual, información confidencial y otros datos importantes perdidos, dañados o robados.

Es por ello que el uso de encriptación o cifrado de medios USB es muy importante para garantizar que las empresas se ajusten a las leyes de protección de datos. Cualquier información personal que se almacene en el sistema, ya sea de los empleados o clientes, debe mantenerse segura, por lo que contar con un sistema de encriptación fiable y eficaz en medios USB, facilitará este propósito.

Cryptzone, es una compañía líder mundial en proveer tecnología para la prevención de fuga de datos, ofrece una solución completa de cifrado USB, llamada Secured eUSB, una solución de nivel empresarial para la seguridad de medios USB que ofrece control centralizado de las políticas de seguridad

y presentación completa de informes sobre el contenido de los datos almacenados. Secured eUSB es la solución perfecta para organizaciones que requieran un sistema de encriptación fiable para este tipo de unidades de almacenamiento extraíbles.

La tecnología de cifrado USB de Cryptzone asegurará sus datos para que no caigan en manos equivocadas y así evitar la pérdida de datos que se pueda dar de manera accidental o como resultado de un ataque de malware.

Sea cual sea su estrategia de negocio, la tecnología de cifrado USB de Cryptzone es la elección perfecta para resguardar su información confidencial y propietaria. Esta solución de seguridad USB, funciona de manera rápida y automática, sin importar el número de medios extraíbles que esté usando su empresa.

Entre sus características clave se destacan:

- ✓ Sistema Anti-theft, para prevenir el uso indebido de datos en caso de pérdida o robo del dispositivo.
- ✓ Administración centralizada que permite controlar, monitorear y aplicar el cifrado de unidades USB por medio de políticas.
- ✓ Generación automática de reportes que facilita las labores de auditoria para garantizar el cumplimento de normativas asociadas a las leyes de protección de datos.

- ✓ Los procesos de encriptación USB se desarrollan de manera rápida y sencilla sin que se requieran infraestructuras complejas para su adecuada gestión.

GLOSARIO

DOS: Disk Operating System, es una familia de sistemas operativos para PC, contaba con una interfaz de línea de comando mediante el uso de intérpretes de órdenes.

FAT: File Allocation Table, es un sistema de archivos desarrollado para el uso de sistemas Operativos DOS.

FAT12: Esta fue la primera versión de FAT, fue muy útil para los discos duros de poca capacidad de Computadoras IBM y también usado para el formato de diskettes.

FAT16: Fue desarrollado para discos que contaban con más capacidad de 16 Mb.

FAT32: Mucho más eficiente en el uso de espacio con discos duros de mayor capacidad mediante el uso más pequeño de tamaño de Clúster.

NTFS: New Technology File System, este es el más seguro sistema de archivos para computadoras que utilizan el Sistema Operativo Microsoft Windows.

UFS: Unix File System, usado en antiguos sistemas BSD.

UFS2: Unix File System, usado en nuevos sistemas BSD.

BSD: Distribución de Software Berkeley, es un sistema operativo derivado del sistema Unix.

RAW: Formato de imagen digital de algún dispositivo con la ventaja de copiar absolutamente todo sin la perdida de datos.

MBR: Master Boot Record, es el primer sector del disco y que contiene información de la partición.

Hashes: Usan algoritmos criptográficos para crear un mensaje resumido de los datos y representarlos como una pieza relativamente pequeña de datos.

MD5: Message-Digest Algorithm5, es un algoritmo matemático, que nos permitirá asegurar que no existan cambios en la imagen.

SHA: Secure Hash Algorithm, es un sistema de funciones de hash criptográficos.

ATA: Advanced Technology Attachment, es originalmente conocido como IDE.

IDE: Integrated Device Electronics, es un estándar de interfaz para la conexión de los dispositivos de almacenamiento masivo de datos y unidades ópticas.

SSD: Solid-state drive, es un dispositivo de almacenamiento que usa memoria no volátil, como la memoria flash.

Discos ZIP: Es un disco de almacenamiento para almacenar datos de mediana capacidad.

SCSI: Small Computers System Interface, es una interfaz estándar para la transferencia de datos entre distintos dispositivos del bus de la computadora.

DC3DD: Está basada en el GNU DD, pero con utilidades específicas para análisis forense.

BIN: Es un formato de imágenes ISO que contiene una imagen de disco.

00N: Split Raw Image

NRG: Nero Burning ROM image

SDI: System Deployment Image

AFF: Advanced Forensics Format Images

ADM: Advanced Forensics Format Images w / metadata

AFD: Advanced Forensics Format Directories

VMDK: VMWare Image

E01: Encase EWF

S01: Smart EWF

GNU/GPL: GNUGeneral Public License, está orientada principalmente a proteger la libre distribución, modificación y uso de software.

LSB: Bit menos significativo, es muy utilizado en la esteganografía, en el momento de codificar un mensaje secreto.

EOF: End Of File es un indicador que proporciona de que ya no hay más información de una fuente de datos.

Proxy-Web: es utilizado para interceptar la navegación de páginas web por motivos de seguridad, anonimato, rendimiento, etc.

ARJ: Archived by Robert Jung, es una aplicación para crear archivos comprimidos.

CDR: Dibujo oVector de imagen creado con CorelDraw, formato propietario utilizado por software de Corel.

DXF: Drawing Exchange Format, es un formato de archivo informático para dibujos de diseño, estos son usados por el programa AutoCad.

DBF: Data Base File, es un antiguo formato de base de datos, propio de clíper u dbase. Luego fue utilizado el FoxPro de Microsoft.

HLP: Help, son los archivos de ayuda de Windows

LZH: Formato para la comprensión de archivos.

MID: Formato para archivos de audio.

RTF: Rich Text Format, es un formato de archivo informático desarrollado por Microsoft para el intercambio de documentos multiplataforma.

DLP: Prevención de perdida de datos.

NAC: Control de admisión de la red.

BIBLIOGRAFÍA

[1] Steve Gibson y Nanni Bassetti, AIR, http://sourceforge.net/apps/mediawiki/air-imager/index.php?title=Main_Page, fecha de consulta enero 2011.

[2] Dream 1600, ¿Creando una imagen dd/dcfldd usando AIR?, http://www.howtoforge.com/creating_dd_images_with_air, fecha de consulta marzo 2007.

[3] Alfonso Muñoz, StegSecret. Una simple herramienta estegoanálisis, http://stegsecret.sourceforge.net/indexS.html, fecha de consulta diciembre 2007.

[4] Alfonso Muñoz y Justo Carracedo, StegSecret: Una herramienta pública de Estegoanálisis, http://vototelematico.diatel.upm.es/articulos/StegSecret_CIBSI2007.pdf, fecha de consulta noviembre 2007.

[5] Miriam Untiveros, CAINE, http://www.slideshare.net/miriam1785/caine-8768505#btnPrevious, fecha de consulta agosto 2011.

[6] Niels Provos, Detección de Esteganografia con Stegdetect http://www.outguess.org/detection.php/, fecha de consulta septiembre 2004.

[7] Alejandro Sánchez, Ataques desde el interior de la red corporativa http://www.robota.net/index.rsws?seccion=6&submenu=1&articulo=112, fecha de consulta marzo 2002.

[8] PassMark Software, OFSClone, http://www.osforensics.com/tools/create-disk-images.html, Mayo 2011.

[9] Developer.apple.com, Descripción de la tecnología MAC, http://developer.apple.com/library/mac/#documentation/MacOSX/Conceptual/OSX_Technology_Overview/MediaLayer/MediaLayer.html, fecha de consulta julio 2012.

[10] Martin F. Krafft, LOOP – Montando Particiones desde una imagen de disco, http://madduck.net/blog/2006.10.20:loop-mounting-partitions-from-a-disk-image/, fecha de consulta abril 2012.

[11] Cisco.com, Cisco mejora su Control de Admisión en Red (NAC) con nuevas funcionalidades para reforzar la seguridad, http://www.cisco.com/web/ES/about/press/press_home_s303.html, fecha de consulta diciembre 2005.

[12] PassMark Software, OFSMount, http://www.osforensics.com/tools/mount-disk-images.html, fecha de consulta mayo 2012.

[13] Uneraser.com, Recuperando archivos gratis con Uneraser, http://www.uneraser.com/, fecha de consulta agosto 2012.

[14] CONVAR, PC INSPECTOR FILE RECOVERY 4.X http://www.pcinspector.de/, fecha de modificación septiembre 2012.

[15] Wikipedia.org, Cómputo forense, http://es.wikipedia.org/wiki/C%C3%B3mputo_forense, fecha de consulta julio 2012.

[16] Franklin Contreras, Herramientas para Computación Forense control y adquisición de evidencia digital, http://www.monografias.com/trabajos74/herramientas-computacion-forense-control-digital/herramientas-computacion-forense-control-digital.shtml, fecha de consulta septiembre 2009.

[17] Giovanni Zuccardi y Juan Gutiérrez, Informática Forense, http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf, fecha de consulta noviembre 2006.

[18] Jeimy J. Cano, Introducción a la informática forense, http://www.acis.org.co/fileadmin/Revista_96/dos.pdf, fecha de consulta julio 2006.

[19] Profesionales.com.mx, Cómputo Forense, http://www.profesiones.com.mx/computo_forense.htm, fecha de consulta agosto 2012.

[20] Daniel Fernández, Informática Forense, http://www.isecauditors.com/downloads/present/hm2k4.pdf, fecha de consulta noviembre 2004.

[21] Álvaro Gómez, Tipos de Ataques e Intrusos en las Redes Informáticas, http://www.mundointernet.es/IMG/pdf/ponencia95.pdf, fecha de consulta octubre 2009.

[22] Wikipedia.org, Ataque Informático, http://es.wikipedia.org/wiki/Ataque_inform%C3%A1tico, fecha de consulta marzo 2012.

[23] Dr. H.B.Wolfe, Definición de la Computación Forense, http://www.slideshare.net/gueste0d962/chfi-v3-module-01-computer-forensics-in-todays-world, fecha de consulta julio 2009.