UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL
CENTRO DE ESTUDIOS DE POSGRADO
MAESTRÍA EN REDES Y TELECOMUNICACIONES

TEMA:

"HERRAMIENTAS DE ANÁLISIS FORENSE Y LA RECUPERACIÓN DE INFORMACIÓN EN LOS DISPOSITIVOS DE ALMACENAMIENTO EN LOS LABORATORIOS DE LA FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL DE LA UNIVERSIDAD TÉCNICA DE AMBATO DURANTE EL PRIMER TRIMESTRE DEL 2010"

TESIS DE GRADO

Previa a la obtención del Título de Magister en Redes y Telecomunicaciones

Autor:

Ing. Luzuriaga Jaramillo Héctor Alberto

Director:

M.Sc. Diego Ávila

Ambato - Ecuador

2011

AL CONSEJO DE POSGRADO DE LA UTA

El comité de defensa de la Tesis de Grado **"HERRAMIENTAS DE ANÁLISIS FORENSE Y LA RECUPERACIÓN DE INFORMACIÓN EN LOS DISPOSITIVOS DE ALMACENAMIENTO EN LOS LABORATORIOS DE LA FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL DE LA UNIVERSIDAD TÉCNICA DE AMBATO DURANTE EL PRIMER TRIMESTRE DEL 2010"** presentada por el Ing. Héctor Alberto Luzuriaga Jaramillo y conformada por: los Señores Miembros del Tribunal de Defensa Ing. M.Sc. Julio Cuji, Ing. M.Sc. Franklin López, Ing. M.Sc. Jaime Ruiz, Ing. M.Sc. Diego Ávila, Director de Tesis y precedido por Ing. M.Sc. Oswaldo Paredes, Presidente del Tribunal de Defensa, Ing. M.Sc. Luis Anda Torres, Director (e) del CEPOS-UTA, una vez escuchada la defensa oral y revisada la Tesis de Grado escrita en la cual han constatado el cumplimiento de las observaciones realizadas por el tribunal de Defensa de la Tesis, remite la presente tesis pata uso y custodia en las bibliotecas de la UTA.

_____ _____

Ing. M.Sc. Oswaldo Paredes O. Ing. M.Sc. Luis Anda Torres
PRESIDENTE DEL TRIBUNAL DE DEFENSA Director (e) del CEPOS-UTA

_____
Ing. M.Sc. Diego Ávila
DIRECTOR DE TESIS

_____
Ing. M.Sc. Julio Cuji
MIEMBRO DEL TRIBUNAL

_____
Ing. M.Sc. Franklin Mayorga
MIEMBRO DEL TRIBUNAL

_____
Ing. M.Sc. Jaime Ruiz
MIEMBRO DEL TRIBUNAL

AUTORÍA DE LA INVESTIGACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el trabajo de investigación con el tema **"HERRAMIENTAS DE ANÁLISIS FORENSE Y LA RECUPERACIÓN DE INFORMACIÓN EN LOS DISPOSITIVOS DE ALMACENAMIENTO EN LOS LABORATORIOS DE LA FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL DE LA UNIVERSIDAD TÉCNICA DE AMBATO DURANTE EL PRIMER TRIMESTRE DEL 2010"**, nos corresponde exclusivamente a Ing. Héctor Alberto Luzuriaga Jaramillo, Autor y del Ing. M.Sc. Diego Ávila, Director de la tesis de grado; y el patrimonio intelectual de la misma a la Universidad Técnica de Ambato.

Ing. Luzuriaga Jaramillo Héctor Alberto	Ing. M.Sc. Diego Ávila
AUTOR	**DIRECTOR DE TESIS**

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga de esta tesis o parte de ella un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los Derechos en línea patrimoniales de mi tesis, con fines de difusión pública, además apruebo la reproducción de esta tesis, dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor.

_____

Ing. Luzuriaga Jaramillo Héctor Alberto

DEDICATORIA

Este proyecto está dedicado directamente aquellas personas que nos han guiado por el camino del saber y la tolerancia durante nuestra vida estudiantil y profesional, llenándonos de sabiduría, convirtiendo en realidad nuestros objetivos y de esta manera fortalecernos siendo mejores.

Alberto L.

AGRADECIMIENTO

Agradezco primeramente a Dios, por haberme dado la oportunidad de vivir este sueño, de luchar cada día esforzándome, dando guerra a todas las adversidades de la vida, ayudándome a trazar metas y alcanzarlas; a mis padres, por el gran apoyo incondicional; a las personas que de una u otra manera estuvieron apoyándome moralmente y llenándome de valor para conseguir lo anhelado.

Alberto L.

ÍNDICE GENERAL

ÍNDICE DE IMAGENES

ÍNDICE DE TABLAS

UNIVERSIDAD TÉCNICA DE AMBATO
CENTRO DE ESTUDIOS DE POSGRADO
MAESTRÍA EN REDES Y TELECOMUNICACIONES

"HERRAMIENTAS DE ANALISIS FORENSE Y RECUPERACIÓN DE INFORMACION EN LOS DISPOSITIVOS DE ALMACENAMIENTO, EN LOS LABORATORIOS DE LA FISEI-UTA, DURANTE EL PRIMER TRIMESTRE DEL 2010"

Autor: Luzuriaga Jaramillo Héctor Alberto
Tutor: Ing. Ávila Diego, M. Sc.

RESUMEN

La investigación sobre "HERRAMIENTAS DE ANALISIS FORENSE Y RECUPERACIÓN DE INFORMACION EN LOS DISPOSITIVOS DE ALMACENAMIENTO, EN LOS LABORATORIOS DE LA FISEI-UTA, DURANTE EL PRIMER TRIMESTRE DEL 2010", tiene como objetivo general reflexionar sobre la pérdida de información que actualmente existe de manera intencionada, por diferentes fallos físicos en los dispositivos de almacenamiento, virus o por falta de conocimiento, entre otros. Para esto se tratará de analizar diversas herramientas de computación forense las cuales nos brindarán a través de un estudio la posibilidad de obtener evidencias de cuáles son las principales causas de la pérdida de datos, la posibilidad de su recuperación mediante distintos escenarios realizados ya que cada caso es único, de darse la posibilidad de un ataque mediante un informe este punto se tratará judicialmente de acuerdo a las normas establecidas en el Ecuador. Además se intentará brindar un completo estudio de tareas de análisis forense, que nos brinden la solución casi en su totalidad, permitiéndonos saber cuál es la herramienta más adecuada de acuerdo a sus características según el caso.

DESCRIPTORES: El presente proyecto trata sobre Las Herramientas de Análisis forense que permitirá la Recuperación de Información en dispositivos de Almacenamiento.

INTRODUCCIÓN

Actualmente se han visto de muchas maneras que las empresas o instituciones a nivel mundial han sido víctimas de varios delitos informáticos en el que se demuestra que en realidad se debería realizar estudios que garanticen seguridad y confiabilidad de la información que se encuentran almacenado en dispositivos de almacenamiento como son disco duros, CD, pendrives, memorias extraíbles entre otros. Ecuador no está exento de este problema ya que de la misma manera han existido varios casos de fraudes informáticos y en la misma Institución como es la FISEI - UTA que por investigación o prácticas tratan de buena o mala manera jugar con la información.

Este proyecto está realizado en base a datos reales de la Institución es por esto que el tema consiste en un estudio de herramientas de análisis forense y recuperación de información en los dispositivos de almacenamiento, en los laboratorios de la FISEI-UTA, durante el primer trimestre del 2010, tomando en cuenta que la investigación es de mucha importancia porque se analizará y demostrará que diferentes herramientas de análisis forense ayudará a reparar daños causados por intrusos informáticos, sean cual fueren sus intensiones como robo, alteración o borrado de información que se encuentran almacenados en diferentes dispositivos de almacenamiento.

El trabajo investigativo realizado tendrá impacto en el desarrollo tanto de laboratoristas, estudiantes, docentes ya que servirá de soporte científico y sobre todo que sirva para solucionar el problema de falta de herramientas estudiadas de manera minuciosa bajo distintas plataformas.

El estudio está realizado en la ciudad de Ambato en los laboratorios de la Facultad de Ingeniería en Sistemas Electrónicos Industriales de la Universidad Técnica de Ambato y sus capítulos están distribuidos de la siguiente manera:

Primer capítulo hacemos referencia al PROBLEMA en sí, en el que se encuentra el planteamiento del mismo su contextualización, su problematización a nivel

global, particular y local, Análisis crítico, delimitación, justificación que tiene como particular su originalidad, importancia, factibilidad su misión y visión así como también los beneficiarios e interés del estudio. A esto agregamos los objetivos tanto generales como específicos que se deberá tomar en cuenta ya que son objetivos primordiales solo del problema.

Segundo capítulo el MARCO TEÓRICO se realiza una revisión bibliográfica de trabajos de investigación relacionados con las variables de la investigación, bibliografía actualizada y especializada respecto a la temática estudiada, en la misma se citan categorías tales como: fundamentaciones, conceptualizaciones, así como también señalamiento de variables.

Tercer capítulo la METODOLOGIA se hace notar la modalidad de la investigación, el trabajo de campo realizado, la población con la que se realizaron las encuestas, o en su defecto si el investigador realiza un muestreo no probabilístico Casual o Incidental en el que selecciona directa e intencionadamente los individuos de la población, operacionalización de variables además del contexto exploratorio y descriptivo que orienta el trabajo en general.

Cuarto capítulo ANALISIS E INTERPRETACION DE RESULTADOS se recalcan las observaciones más significativas del trabajo como que para el administrador de red, laboratoristas y docentes varían sus resultados en conocimiento a cerca de los procedimientos que se llevaran a cabo durante el estudio.

Quinto capítulo CONCLUSIONES Y RECOMENDACIONES se cita las conclusiones y recomendaciones más importantes del problema ya que la metodología inicia en el problema y culmina con la propuesta. Prácticamente son respuestas a los Objetivos general, específicos e hipótesis, además las que creyeren conveniente los investigadores.

Sexto Capítulo LA PROPUESTA se realiza estrategias de solución al problema planteado, además antecedentes, objetivos generales y específicos de acuerdo a la solución, análisis si es factible hacerlo, modelo operativo, plan de acción en este

punto se tomará en cuenta la metodología que consiste en un estudio más no realizar la implementación de acuerdo al caso. Conclusiones y recomendaciones
Se concluye con Bibliografía y Anexos

CAPÍTULO I

EL PROBLEMA

Planteamiento del Problema

Contextualización

Macro

En la dirección electrónica http://informaniaticos.blogspot.com/2010/01/china-lanzo-varios-ataques-hacker.html, hace relucir un ataque a Petroleras importantes de Estados Unidos en donde su información sobre fondos petroleros mundiales, así como sobre cantidades y valores del crudo fue la víctima de piratas informáticos. Entre los datos robados están claves para correos electrónicos y otras informaciones. Internacionalmente al menos 6% de todas las computadoras sufren pérdida de información todos los años. Tomando en cuenta el número de computadoras que se utilizaron en las empresas de Estados Unidos en un año y que les costó a las empresas estadounidenses 11.8 mil millones de dólares estas estadísticas se encuentran en el siguiente enlace:
http://www.nerdsbackup.com/estadisticas_perdida_informacion.asp. Siempre que una empresa o Institución fue motivo de un ataque informático su principal objetivo es la destrucción copia o alteración de sus datos que se encuentran en algún dispositivo de almacenamiento.

Meso

En Nuestro País se dio un fraude informático en el Seguro Social en el cual no existía un buen control en todo el sistema al momento de entregar préstamos

quirografarios a los afiliados al Seguro Social. Este problema se generó debido a robo de información de claves a través del internet, esto ya constituye un delito informático que es sancionado penalmente. Esta información está detallada en la dirección electrónica.
"http://www.ecuadorinmediato.com/Noticias/news_user_view/ecuadorinmediato_noticias--13563". Entonces es de mucha importancia saber el problema que afecta de igual manera a nuestro país con la alteración y en otros casos la pérdida de información provocadas por personas que la mayoría de mala manera tratan de ingresar a su sistema y alteran o borran su información ocasionando muchos daños para cualquier Institución.
Este punto es muy importante de tener en cuenta ya que en diferentes empresas existe la posibilidad de que no posean un respaldo y prácticamente se perdería toda su información teniendo que recurrir a tratar de recuperar de manera inadecuada por la desesperación de rescatar sus datos.

Micro

En Nuestra ciudad y como punto principal en la UTA-FISEI ponemos como antecedente un ataque a un Swicth Capa 3 CISCO que rompiendo la seguridad desconfiguraron dejando al punto 0 sin dejar rastro hace unos 4 meses aproximadamente, además no se dispone de suficientes herramientas de Análisis Forense en caso de darse un delito informático teniendo en cuenta que existen alumnos que tienen conocimiento tecnológico sobre el área de sistemas en el que tratan por motivos de pruebas o investigación llegar al punto máximo como adquirir más ancho de banda u otros. La Recuperación de información está dado por programas básicos como Easy Recovery, lo cual no garantiza su recuperación al momento de rescatar datos sumamente más importantes. Información es tomada de la parte de Administración de Sistemas de la UTA-FISEI.

Análisis Crítico

Los factores causales en la que puede ocurrir la pérdida de datos en dispositivos de almacenamiento son: Ataques informáticos, que por falta de seguridad tanto interna como externa y la mala administración de sus servidores ocasionan la pérdida, robo y alteración de información, además existen sistemas wireless en las que estudiantes pueden ingresar con un poco de conocimiento tecnológico y de buena o mala manera borrar información o modificarla.

La Mala utilización de Herramientas de Análisis Forense que conlleva a la recuperación errónea en un porcentaje mínimo y sin control.

La Falta de evidencias provocaría que no se pudiera prevenir y mejorar la preparación en incidentes futuros, riesgo de responsabilidades y por último si se da el caso de denunciar, es decir no tendríamos un informe garantizado.

La carencia de respaldos de discos duros, memorias u otro dispositivo de almacenamiento no nos garantizaría su información.

Por otro lado también existe el caso de sectores defectuosos, pistas dañadas en los discos duros, memorias ya sea por diferentes motivos como el rápido crecimiento de virus informáticos que producen la pérdida y alteración de datos sumamente importantes.

Los efectos derivados de la problemática son el reducido interés para utilizar herramientas sofisticadas bajo Windows y Linux que no se han puesto en práctica en el caso de darse este problema, así como también la mala recuperación, información no garantizada y por ende la pérdida de datos.

Prognosis

Se estima como una proyección de no solucionarse la problemática ya sea por diferentes motivos como ataques informáticos, mala recuperación, dispositivos de almacenamiento dañados, carencia de respaldos u otros, la información no estaría garantizada y segura, además se estaría negando la posibilidad de contribuir a la Institución, en especial a sus laboratorios informáticos de una adecuada utilización de herramientas de análisis forense y recuperación de información bajo diferentes plataformas estudiadas, además de una buena obtención de evidencias que de darse el caso que la parte afectada desee demandar judicialmente.

Formulación del Problema

¿Las Herramientas de Análisis Forense influyen en la Recuperación de información en los dispositivos de almacenamiento?

Interrogantes de la Investigación

- ¿Con qué Herramientas de Análisis Forense cuenta la FISEI de la UTA?
- ¿Cuáles son los principales problemas en la Recuperación de la Información en la FISEI de la UTA?
- ¿Existen Alternativas para minimizar el problema de la perdida de información en los dispositivos de almacenamiento?

Delimitación de la Investigación

Delimitación de Contenido:

El proyecto de investigación planteado se basa en la utilización de conocimientos en el área de Herramientas de Análisis Forense y Recuperación de Información que ha sido investigado, además de discernimientos adquiridos durante la Maestría de Redes y Telecomunicaciones.

El investigador desarrollará mediante una investigación bibliográfica de diferentes heramientas de Análisis forense bajo las plataformas Linux Windows de manera que permita obtener resultados a un porcentaje máximo de recuperación.

Delimitación Espacial:

El estudio estará dado de acuerdo a distintos escenarios que se realizarán en los laboratorios de la FISEI de la UTA en particular en la facultad de sistemas.

El objeto de estudio y la parte bibliográfica comprende la recolección de información de papers, direcciones electrónicas, sitios web seguros sirviendo esto de aporte científico tecnológico para fundamentar la utilización de herramientas adecuadas de análisis forense.

Delimitación Temporal:

La investigación se llevara a cabo durante el primer trimestre del año 2010. El progreso del proyecto de investigación que se basa en la utilización de herramientas de análisis forense esta dado con la culminación en distintos escenarios a realizarse en los laboratorios de la FISEI de la UTA y comprende una planificación de tres meses.

Justificación

La presente investigación es de mucha importancia porque se analizará y demostrará que diferentes herramientas de análisis forense ayudará a compensar los daños causados por los criminales o intrusos informáticos, ya sea por motivos de robo, alteración o borrado de información que se encuentran almacenados en diferentes dispositivos de almacenamiento.

El Investigador dispondrá de Recursos tecnológicos como software actualizado bajo sistemas operativos estudiados que garanticen su estudio. En la parte de

hardware contaremos con Dispositivos de Almacenamiento en los cuales a través de escenarios realizados en los laboratorios de la FISEI-UTA nos servirá para obtener un cuadro comparativo de mayor eficacia, además de la información obtenida del departamento de Administración de Sistemas ya que cada caso es único determinando así evidencias claras Qué, Cómo Dónde fue ocasionado y qué herramienta es la más adecuada.

El interés por parte del Investigador nace porque es un tema nuevo dentro de la UTA-FISEI teniendo en cuenta que se ocupa mundialmente en casos de diversos delitos informáticos, la mala utilización de herramientas, el no tener un respaldo adecuado, la pérdida de información en diferentes dispositivos de almacenamiento e incluso de darse una demanda judicial.

La FISEI de la UTA será beneficiada porque contaría de un aporte científico y tecnológico tanto para estudiantes y profesores los mismos que dispondrán de información más detallada sobre herramientas de Análisis forense y Recuperación de información en dispositivos de almacenamiento.

La Utilidad teórica y práctica justifica en base a lo investigado antes, durante y después del desarrollo del proyecto.

Objetivos

Objetivo General

- Determinar las herramientas de Análisis Forense que se utilizan para la recuperación de información en los dispositivos de almacenamiento en la FISEI - UTA.

Objetivos Específicos

- Determinar las Herramientas de Análisis Forense con que cuenta la FISEI de la UTA

- Cuantificar los problemas en la Recuperación de la Información en la FISEI de la UTA
- Proponer Alternativas para minimizar el problema de la pérdida de información en los dispositivos de almacenamiento

CAPITULO II

MARCO TEÓRICO

Antecedentes de Investigación

"Auditoria Forense: Metodología, Herramientas y Técnicas Aplicadas en un siniestro informático de una empresa del sector comercial".
Viviana Marcela Villacís Ruiz, Bertha Alice Naranjo Sánchez

La clave del éxito en el uso de software forense es, donde sea posible, identificar cuáles son las herramientas más apropiadas para cada caso y ganar familiaridad con las mismas antes que la investigación lo requiera.

"Análisis inicial de la anatomía de un Ataque a un sistema informático".
Daniel Monroy López
De manera final se recomienda emplear unas buenas políticas de seguridad para proteger nuestra información, mantener nuestros sistemas actualizados, ejecutar sólo los servicios que sean necesarios y lo más importante, aplicar las técnicas presentadas aquí para probar y mejorar la seguridad en nuestros sistemas.

"Estudio y aplicación de procedimientos de análisis forense para recuperar datos de medios de almacenamiento" caso practico: cisco-espoch.
Nadia Cecilia Gutiérrez Paredes, Paúl Hernán Machado Herrera.

Las actividades realizadas, la destrucción de datos y la manipulación de los mismos pueden rastrearse y recuperarse con la aplicación adecuada de la guía de procedimientos propuesta.

Fundamentaciones

Fundamentación Legal

La información hoy en día es uno de los más importantes activos para las empresas y organizaciones, por este motivo requiere ser asegurada y protegida en forma apropiada.

La norma ISO 27002, **Según (http://www.cavaju.com, 2009)**

Es un estándar internacional de buenas prácticas sobre la gestión de la seguridad de la información, cuyo objetivo es crear una cultura organizacional sobre el manejo e implementación de la seguridad a través de políticas, procesos, procedimientos y controles para minimizar el impacto de las diferentes amenazas a las que está expuesta la información.

ISO/IEC 17799, Según (wikipedia.org/wiki)

(Denominada también como ISO 27002) es un estándar para la seguridad de la información publicado por primera vez como ISO/IEC 17799:2000 por la International Organization for Standardization y por la Comisión Electrotécnica Internacional en el año 2000, con el título de Information technology - Security techniques - Code of practice for information security management. Tras un periodo de revisión y actualización de los contenidos del estándar, se publicó en el año 2005 el documento actualizado denominado ISO/IEC 17799:2005. El estándar ISO/IEC 17799 tiene su origen en el British Standard BS 7799-1 que fue publicado por primera vez en 1995.

Directrices del estándar

ISO/IEC 17799 proporciona recomendaciones de las mejores prácticas en la gestión de la **seguridad de la información** a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)".

Certificación

La norma ISO/IEC 27001 (Information technology - Security techniques - Information security management systems - Requirements) sí es certificable y especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información según el famoso "Círculo de Deming": PDCA - acrónimo de **P**lan, **D**o, **C**heck, **A**ct (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 17799 y tiene su origen en la norma británica British Standard BS 7799-2 publicada por primera vez en 1998 y elaborada con el propósito de poder certificar los Sistemas de Gestión de la Seguridad de la Información implantados en las organizaciones y por medio de un proceso formal de auditoría realizado por un tercero.

El software libre

Según (http://www.monografias.com):

Trae consigo numerosas ventajas y pocas desventajas, por ejemplo:

Ventajas

- Libertad de uso y redistribución.
- Económico.
- Fomento de la libre competencia al basarse en servicios y no licencias.
- Sistemas sin puertas traseras y más seguros.
- Sistema de expansión.
- Entre otras ventajas.

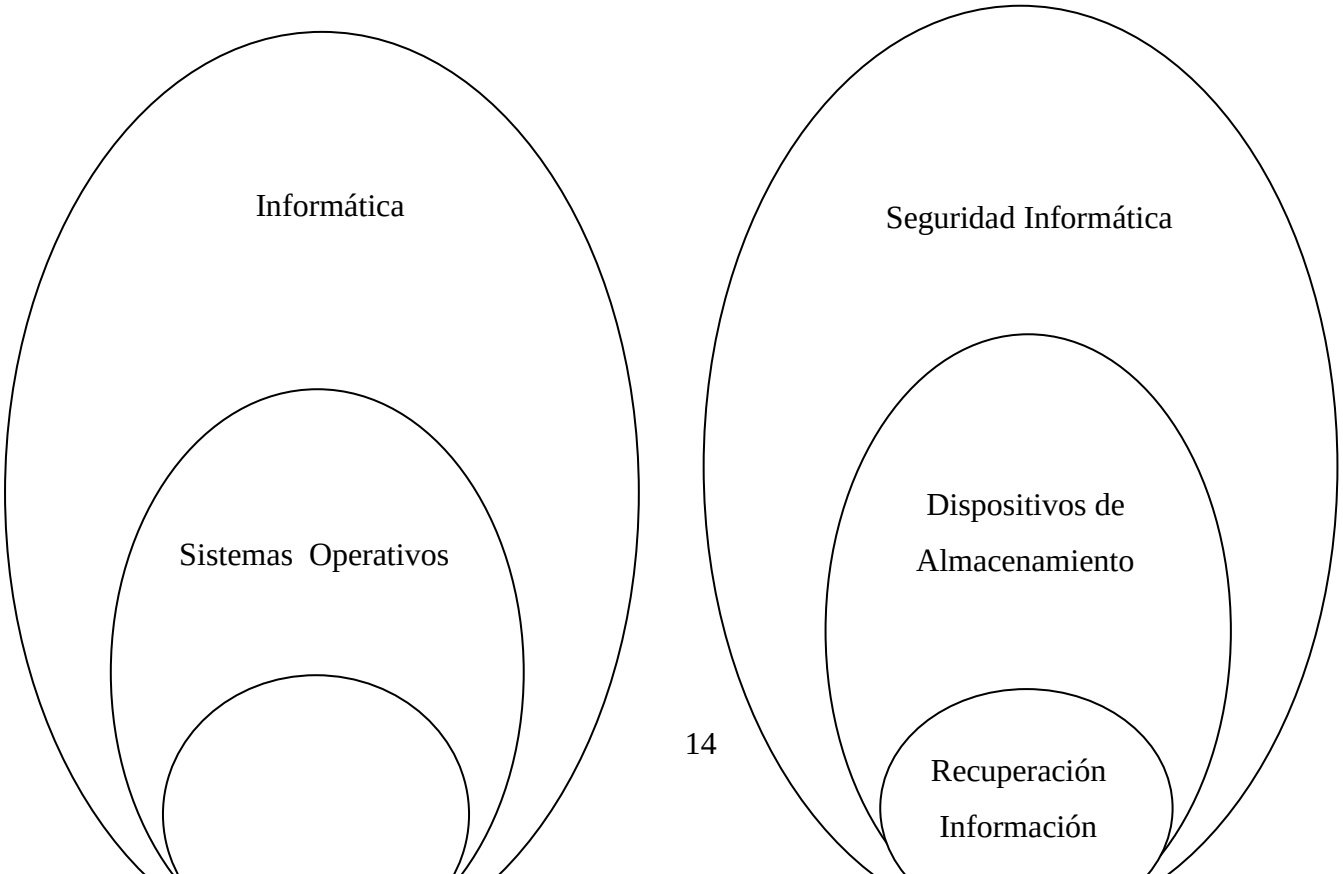
Desventajas

- No existen compañías únicas que respalden toda la tecnología.
- Se adquiere sin garantías el software.
- La mayoría de la configuración de hardware no es intuitiva.

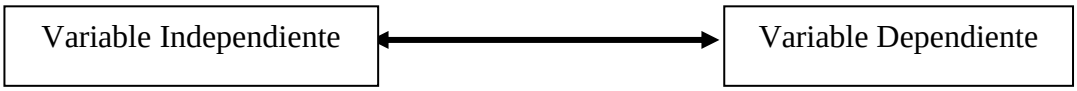
Tipos de licencias Según (http://es.wikipedia.org): Una licencia es aquella autorización formal con carácter contractual que un autor de un software da a un interesado para ejercer "actos de explotación legales".

Categorías Fundamentales

Imagen No. 1: Categorías Fundamentales



Herramientas
de Análisis
Forense



Elaborado por Investigador

Para Recuperar

ANÁLISIS FORENSE

Según (Delgado, 2007): Conjunto de principios y técnicas que comprende el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias digitales y que llegado el caso puedan ser aceptadas legalmente en un proceso judicial.

Por **evidencia digital** se entiende al conjunto de datos en formato binario, esto es, comprende los ficheros, su contenido o referencias a éstos (meta-datos) que se encuentren en los soportes físicos o lógicos del sistema atacado.

Dentro del Análisis Forense Digital podemos destacar las siguientes fases:

1ª. Identificación del incidente.
2ª. Recopilación de evidencias.
3ª. Preservación de la evidencia.
4ª. Análisis de la evidencia.
5ª. Documentación y presentación de los resultados.

Por otro lado, hay que definir otro concepto importante, el de Incidente de Seguridad Informática, pues éste ha evolucionado en los últimos tiempos. En principio un incidente de este tipo se entendía como cualquier evento anómalo que pudiese afectar a la seguridad de la información, como podría ser una pérdida de disponibilidad, su integridad o confidencialidad, etc. Pero la aparición de nuevos tipos de incidentes ha hecho que este concepto haya ampliado su definición.

Actualmente un **Incidente de Seguridad Informática** puede considerarse como una violación o intento de violación de la política de seguridad, de la política de Uso adecuado o de las buenas prácticas de utilización de los sistemas informáticos.

Incidentes de Denegación de Servicios (DoS): Son un tipo de incidentes cuya finalidad es obstaculizar, dañar o impedir el acceso a redes, sistemas o aplicaciones mediante el agota-miento de sus recursos.

Incidentes de código malicioso: Cualquier tipo de código ya sea, virus, gusano, "caballo de Troya", que pueda ejecutarse en un sistema e infectarlo.

Incidentes de acceso no autorizado: Se produce cuando un usuario o aplicación accede, por medio de hardware o software, sin los permisos adecuados a un sistema, a una red, a una aplicación o los datos.

Incidentes por uso inapropiado: Se dan cuando los usuarios se "saltan" la política de uso apropiado de los sistemas (por ejemplo ejecutando aplicaciones P2P en la red interna de la organización para la descarga de música).

Incidente múltiple: Se produce cuando el incidente implica varios de los tipos anteriores.

La mayoría de los incidentes que se dan en la realidad, pueden enmarcarse en varias de las categorías expuestas, por lo que una buena forma de identificarlos es por el mecanismo de transmisión empleado. Por ejemplo un virus que crea en el sistema atacado una puerta tras-era debe ser manejado como un incidente de código malicioso y no como un acceso no autorizado, ya que el virus es el mecanismo de transmisión.

AUTENTICAR

Según (Oset, 2004): Comprobar que las evidencias recogidas y que van a ser la base de la investigación son idénticas a las abandonadas por el delincuente en la escena del crimen. Las técnicas y herramientas de control de integridad que mediante la utilización de una función *hash* generan una huella electrónica digital de un fichero o un disco completo constituyen una ayuda básica

ADQUIRIR EVIDENCIAS

Consiste en adquirir evidencias sin alterar ni dañar el original. La forma ideal de examinar un sistema consiste en detenerlo y examinar una copia de los datos originales, es importante tener en cuenta que no se puede examinar un sistema presuntamente comprometido utilizando las herramientas que se encuentran en dicho sistema pues estas pueden estar afectadas. La Cadena de Custodia documenta el proceso completo de las evidencias durante la vida del caso, quién la recogió y donde, quien y como la almacenó, quién la procesó… etc. Cada evidencia deberá ser identificada y etiquetada a ser posible en presencia de testigos, con el número del caso, una breve descripción, la firma y la fecha en que fue recogida.

HERRAMIENTAS DE ANÁLISIS FORENSE

Según (Investigador, 2010): Son diferentes procedimientos, que permiten realizar un Análisis forense con el objetivo de garantizar la conservación de la información bajo distintos Sistemas Operativos estudiados y que llegado al caso puedan ser aceptadas legalmente en un Proceso Judicial.

Existe diversidad de herramientas utilizadas para análisis forense pero no estudiadas minuciosamente para saber cuáles son las más recomendadas. El investigador deberá analizarlas muy bien debido a que los atacantes emplean cada vez herramientas más silenciosas y perfeccionadas para realizar sus delitos.

Dejando aparte el software comercial, en el que podrá encontrar herramientas específicas como EnCase de la empresa Guidance Software, considerado un

estándar en el análisis forense de sistemas, nos centraremos en herramientas de código abierto (Open Source) que podrá descargar libremente

Software de Libre Distribución y Open Source

Se va a comenzar con una recopilación de herramientas que necesitan ser ejecutadas bajo un sistema operativo anfitrión, bien sea MS Windows o UNIX/Linux.

The forensic toolkit

Según (Anaya): Se trata de una colección de herramientas forenses para plataformas Windows, creadas por el equipo de Foundstone. Puede descargarlo desde www.foundstone.com, donde además encontrará gran cantidad de herramientas de seguridad. Este ToolKit le permitirá recopilar información sobre el ataque, y se compone de una serie aplicaciones en línea de comandos que permiten generar diversos informes y estadísticas del sistema de archivos a estudiar. Para poder utilizarlos deberá disponer de un intérprete de comandos como cmd.exe.

Distribuciones 'livecd'

Según (Martinez, 1998-2010): Para los que quieren probar como funciona y se utiliza un sistema Linux, sin necesidad de instalaciones y espacio libre en el disco duro, existe lo que llamamos distribuciones "LiveCD".

Un "LiveCD" no es otra cosa que una distribución de Linux que funciona al 100%, sin necesidad de instalarla en el ordenador donde la probamos. Utiliza la memoria RAM del ordenador para 'instalar' y arrancar la distribución en cuestión. En la memoria también se instala un "disco virtual" que emula al disco dure de un ordenador.

De esta forma solamente hace falta introducir el CD o DVD en el ordenador en cuestión y arrancarlo, al cabo de unos minutos tendremos un sistema Linux funcionando en el mismo. Este tipo de distribuciones solamente sirve para demostraciones y pruebas, ya que una vez que apagamos el ordenador, todo lo que hemos hecho desaparece.

SISTEMAS OPERATIVOS

Según (O´brien, 2006): Un **Sistema Operativo** (SO) es un software que actúa de interfaz entre los dispositivos de hardware y los programas usados por el usuario para manejar un computador. Es responsable de gestionar, coordinar las actividades y llevar a cabo el intercambio de los recursos y actúa como estación para las aplicaciones que se ejecutan en la máquina.

Uno de los más prominentes ejemplos de sistema operativo, es el núcleo Linux, el cual junto a las herramientas GNU, forman las llamadas distribuciones Linux.

Nótese que es un error común muy extendido denominar al conjunto completo de herramientas sistema operativo, pues este, es sólo el núcleo y no necesita de entorno operador para estar operativo y funcional. Este error de precisión, se debe a la modernización de la informática llevada a cabo a finales de los 80, cuando la filosofía de estructura básica de funcionamiento de los grandes computadores se rediseñó a fin de llevarla a los hogares y facilitar su uso, cambiando el concepto de computador multiusuario, (muchos usuarios al mismo tiempo) por un sistema monousuario (únicamente un usuario al mismo tiempo) más sencillo de gestionar. (Véase AmigaOS, beOS o MacOS como los pioneros de dicha modernización, cuando los Amiga, fueron bautizados con el sobrenombre de Video Toaster por su capacidad para la Edición de vídeo en entorno multitarea round robin, con gestión de miles de colores e interfaces intuitivos para diseño en 3D con programas como Imagine o Scala multimedia, entre muchos otros.)

Uno de los propósitos de un sistema operativo como programa estación principal, consiste en gestionar los recursos de localización y protección de acceso del

hardware, hecho que alivia a los programadores de aplicaciones de tener que tratar con estos detalles. Se encuentran en la mayoría de los aparatos electrónicos que utilizan microprocesadores para funcionar. (Teléfonos móviles, reproductores de DVD, computadoras, radios, etc.)

Parte de la infraestructura de la World Wide Web está compuesta por el Sistema Operativo de Internet, creado por Cisco Systems para gestionar equipos de interconexión como los conmutadores y los enrutadores.
Entre algunos sistemas operativos tenemos:

WINDOWS

Según (Lanzillotta, 2005): Windows es el sistema operativo de la compañía Microsoft que fue lanzado al mercado a fines de 1985 con su versión 1.0, como una aplicación para utilizar con el sistema MS-DOS. Desde ese entonces hasta el momento, sus diversas ediciones fueron ganando popularidad hasta convertirse en lo que es hoy. Esta última salió en 1993, con su versión Windows NT, la que después sería actualizada con Windows 2000. Mientras que en la línea del hogar, a Windows 95 le siguió Windows 98 y luego la edición Millennium, hasta que finalmente con el Windows XP, de 2001, se logró fusionar ambas líneas: la profesional y la del hogar. Actualmente se encuentra en el mercado la versión Windows Vista, pero que no logra afianzarse, por lo que XP sigue siendo la número uno en todo el mundo.

UNIX

Según (System., 2002):Unix (registrado oficialmente como **UNIX**®) es un sistema operativo portable, multitarea y multiusuario; desarrollado, en principio, en 1969 por un grupo de empleados de los laboratorios Bell de AT&T, entre los que figuran Ken Thompson, Dennis Ritchie y Douglas McIlroy.

Hasta 2009, el propietario de la marca *UNIX*® fue The Open Group, un consorcio de normalización industrial. A partir de marzo de 2010 y tras una larga batalla legal, esta ha pasado nuevamente a ser propiedad de Novell, Inc. Sólo los sistemas totalmente compatibles y que se encuentran certificados por la especificación Single UNIX Specification pueden ser denominados "UNIX®" (otros reciben la denominación "similar a un sistema Unix" o "similar a Unix"). En ocasiones, suele usarse el término "Unix tradicional" para referirse a Unix o a un sistema operativo que cuenta con las características de UNIX Versión 7 o UNIX System V.

UNIX

Es una marca registrada de The Open Group en Estados Unidos y otros países. Esta marca sólo se puede aplicar a los sistemas operativos que cumplen la "Single Unix Specification" de esta organización y han pagado las regalías establecidas.
En la práctica, el término UNIX se utiliza en su acepción de familia. Se aplica también a sistemas multiusuario basados en POSIX (tales como GNU/Linux, Mac OS X [el cual, en su versión 10.5 ya ha alcanzado la certificación UNIX], FreeBSD, NetBSD, OpenBSD), los cuales no buscan la certificación UNIX por resultar cara para productos destinados al consumidor final o que se distribuyen libremente en Internet. En estos casos, el término se suele escribir como "UN*X", "*NIX", o "*N?X".

LINUX

Según (lfmontalvan, 2009): Sistema multitarea, multiusuario, multiplataforma y multiprocesador; en las plataformas Intel corre en modo protegido; protege la memoria para que un programa no pueda hacer caer al resto del sistema; carga sólo las partes de un programa que se usan; comparte la memoria entre programas aumentando la velocidad y disminuyendo el uso de memoria; usa un sistema de memoria virtual por páginas; utiliza toda la memoria libre para cache; permite usar bibliotecas enlazadas tanto estática como dinámicamente; se distribuye con código fuente; usa hasta 64 consolas virtuales; tiene un sistema de archivos

avanzado pero puede usar los de los otros sistemas; y soporta redes tanto en TCP/IP como en otros protocolos.

MAC

Según (wikipedia, 2010): Macintosh (abreviado Mac) es el nombre con el que actualmente nos referimos a cualquier computadora personal diseñada, desarrollada, construida y comercializada por Apple Inc. El Macintosh 128K fue lanzado el 24 de enero de 1984. Fue el primer ordenador personal que se comercializó exitosamente, que usaba una interfaz gráfica de usuario (GUI) y un mouse en vez del estándar de esa época: la interfaz por línea de comandos. La línea de producción de Macs en la actualidad varía desde el básico Mac mini de escritorio hasta los servidores de rango medio como Xserve.

Los sistemas Mac tienen como objetivo principal de mercado el hogar, la educación y la creatividad profesional. La producción de Mac está basada en un modelo de integración vertical en los que Apple proporciona todos los aspectos de su hardware y crea su propio sistema operativo que viene preinstalado en todas las Macs. Esto contrasta con las PC preinstalados con Microsoft Windows, donde un vendedor proporciona el sistema operativo y múltiples vendedores crean el hardware. En ambos casos, el hardware permite el funcionamiento de otros sistemas operativos: las Mac modernas, así como las PC son capaces de soportar sistemas operativos como Linux, FreeBSD y Windows, éste último gracias al software de Apple Boot Camp o a otros softwares de virtualización como por ejemplo Parallels Desktop o VMWare Fusion. En la actualidad también es posible modificar el sistema operativo de Apple para hacerlo compatible con la mayoría de hardware existente; es el llamado movimiento OSx86.

Los primeros Macintosh estaban basados en los microprocesadores de la familia Motorola MC68000, de tecnología CISC. En marzo de 1994, Apple introdujo en

la gama Macintosh los chips PowerPC del Consorcio Apple/IBM/Motorola, que suponían el cambio a la tecnología RISC. En el 2006 Apple inició la transición desde la línea de PowerPC line a los procesadores Intel con arquitectura x86. Los Macs actuales usan la serie de microprocesadores Intel Core 2 Duo, Intel Core i5, Intel Xeon e Intel Core i7. Todos los modelos de Mac actuales vienen con una versión nativa de la última versión de Mac OS X, que desde el 28 de agosto de 2009 está en su versión Mac OS X v10.6 Snow Leopard.

INFORMÁTICA

Según (DRAE): La Informática es la ciencia aplicada que abarca el estudio y aplicación del tratamiento automático de la información, utilizando dispositivos electrónicos y sistemas computacionales. También está definida como el procesamiento automático de la información.

Conforme a ello, los sistemas informáticos deben realizar las siguientes tres tareas básicas:

- Entrada: Captación de la información digital.
- Proceso: Tratamiento de la información.
- Salida: Transmisión de resultados binarios.

En los inicios del procesado de información, con la informática sólo se facilitaba los trabajos repetitivos y monótonos del área administrativa, gracias a la automatización de esos procesos, ello trajo como consecuencia directa una disminución de los costes y un incremento en la producción.

En la informática convergen los fundamentos de las ciencias de la computación, la programación y metodologías para el desarrollo de software, la arquitectura de computadores, las redes de computadores, la inteligencia artificial y ciertas cuestiones relacionadas con la electrónica. Se puede entender por informática a la unión sinérgica de todo este conjunto de disciplinas.

Esta disciplina se aplica a numerosas y variadas áreas del conocimiento o la actividad humana, como por ejemplo: gestión de negocios, almacenamiento y consulta de información, monitorización y control de procesos, industria, robótica, comunicaciones, control de transportes, investigación, desarrollo de juegos, diseño computarizado, aplicaciones/herramientas multimedia, medicina, biología, física, química, meteorología, ingeniería, arte, etc. Una de la aplicaciones más importantes de la informática es proveer información en forma oportuna y veraz, lo cual, por ejemplo, puede tanto facilitar la toma de decisiones a nivel gerencial (en una empresa) como permitir el control de procesos críticos.
Actualmente es difícil concebir un área que no use, de alguna forma, el apoyo de la informática. Ésta puede cubrir un enorme abanico de funciones, que van desde las más simples cuestiones domésticas, hasta los cálculos científicos más complejos.

Entre las funciones principales de la informática se cuentan las siguientes:

- Creación de nuevas especificaciones de trabajo.
- Desarrollo e implementación de sistemas informáticos.
- Sistematización de procesos.
- Optimización de los métodos y sistemas informáticos existentes.

RECUPERACIÓN DE INFORMACIÓN

Según (Molina, 2004): Proceso donde se accede a una información previamente almacenada, mediante herramientas informáticas que permiten establecer ecuaciones de búsqueda específicas. Dicha información ha debido de ser estructura previamente a su almacenamiento

Por otro lado también se menciona al proceso de recuperación que se lleva a cabo mediante consultas a la base de datos donde se almacena la información estructurada, mediante un lenguaje de interrogación adecuado. Es necesario tener en cuenta los elementos clave que permiten hacer la búsqueda, determinando un mayor grado de pertinencia y precisión, como son: los índices, palabras clave, tesauros y los fenómenos que se pueden dar en el proceso como son el ruido y silencio documental. Uno de los problemas que surgen en la búsqueda de información es si lo que recuperamos es "mucho o poco" es decir, dependiendo del tipo de búsqueda se pueden recuperar multitud de documentos o simplemente un número muy reducido. A este fenómeno se denomina Silencio o Ruido documental.

Silencio documental: Son aquellos documentos almacenados en la base de datos pero que no han sido recuperados, debido a que la estrategia de búsqueda ha sido demasiado específica o que las palabras clave utilizadas no son las adecuadas para definir la búsqueda.

Ruido documental: Son aquellos documentos recuperados por el sistema pero que no son relevantes. Esto suele ocurrir cuando la estrategia de búsqueda se ha definido demasiado genérica

La recuperación de información es un estudio interdisciplinario. Cubre tantas disciplinas que eso genera normalmente un conocimiento parcial desde tan solo una u otra perspectiva. Algunas de las disciplinas que se ocupan de estos estudios son la psicología cognitiva, la arquitectura de la información, diseño de la información, el comportamiento humano hacia la información, la lingüística, la semiótica, informática, biblioteconomía y documentación.

Recuperación de datos

Según (Hordeski): La Recuperación de datos de un HARD DISK servidor dañado solicitando un servicio externo. Estas compañías por lo general llevan a cabo la recuperación de datos y la reconstrucción de discos en sitios llamados cuartos limpios. Muchas de estas compañías manejan el DOS así como también NetWare y otros sistemas operativos de Red.

Los problemas típicos que se pueden presentar con los discos NetWare, incluyen una falla en la tarjeta del controlador, donde la tarjeta, debido a la característica de respaldo por duplicación del disco de SFT NetWare, escribe datos de manera inapropiada en la primera unidad y los mismos datos incorrectos se escriben a la segunda unidad. En este caso, se debe reparar o reemplazar la tarjeta del controlador pareada y reconstruir los directorios afectados. Si se destruye el registro maestro de arranque, este se debe reconstruir byte por byte.

Por otro lado en una unidad de CD-DVD-ROM, los sistemas de rastreo óptico son delicados y están alineados de fábrica para un rendimiento óptico y reemplazo. El ajuste del usuario puede afectar esta alineación y hacer inutilizable la unidad. Recuerde que está tratando con un mecanismo muy delicado. Aisle el problema y obtenga el acceso a la parte sospechosa antes de desarmar la unidad. Si usted no puede encontrar la parte, con frecuencia significa que el desensamble se debe realizar en el centro d servicio.

Recuperación De Evidencias En Discos

Según (Prieto., 2004): Estrictamente hablando, el Análisis Forense se refiere a la recopilación d evidencias bajo notario que puedan servir como prueba judicial. Es por ello que la mayor parte de las técnicas se basan en la recuperación de información de discos duros, ahora que comienza a decaer las técnicas denominadas Floppy Disk Forensics

En este sentido, el líder del mercado en entornos forenses de discos es ENCASE, que puede realizar duplicaciones exactas del contenido de un disco, incluso de forma remota. SMART es una utilidad que permite instalar en un disco las imágenes capturadas con Encase. A la sombra de esta herramienta, líder del mercado, han surgido muchas otras herramientas similares, como por ejemplo Forensic Toolkit

La empresa Checa LEC, s.r.o. dispone de dos productos de análisis forense de discos, Disk Doubler II (un duplicador hardware de discos) y DiskDoubler Plus, una aplicación de búsqueda de cadenas en los datos adquiridos. La recuperación de ficheros borrados o no accesibles entra también dentro de este campo, búsqueda de cadenas en los datos adquiridos. Lo más normal en caso de querer recuperar datos de un disco es intentar montar la partición con un arranque del sistema operativo Linux.

Por otro lado, el análisis forense también se refiere a determinar las causas del compromiso de seguridad de un sistema, es decir, la alteración de sus datos o la caída o mal funcionamiento del sistema. Tripwire y Osiris y son dos sistemas de control de integridad de ficheros.

Recuperación De Contraseñas

Según (Prieto., http://www.ausejo.net, 2004): John the Ripper es el crackeador de contraseñas fuerza bruta más famoso, probablemente por ser gratuito y uno de los primeros. El proyecto OpenWall es una recopilación de recuperadores de contraseñas, al igual que Russian Password Crackers. Ambos incluyen crackeadores para compresores, para utilidades de cifrado, BIOS, formatos de ficheros (Office, PDF, etc.), bases de datos, Sistemas Operativos, Aplicaciones, etc. se incluyen además enlaces sobre los algoritmos y sus debilidades. MDcrack es capaz de romper hashes MD4, MD5 y NTLM1. Existen varias formas de recuperar o restablecer una contraseña en Windows.

Dispositivos de Almacenamiento de un Computador

Según (ANTONIO, (2002). Aula Siglo XXI.): Los sistemas informáticos pueden almacenar los datos tanto interna (en la memoria) como externamente (en los dispositivos de almacenamiento). Internamente, las instrucciones o datos pueden almacenarse por un tiempo en los chips de silicio de la RAM (memoria de acceso

aleatorio) montados directamente en la placa de circuitos principal de la computadora, o bien en chips montados en tarjetas periféricas conectadas a la placa de circuitos principal del ordenador. Estos chips de RAM constan de conmutadores sensibles a los cambios de la corriente eléctrica, esto quiere decir que los datos son almacenados por tiempo limitado (hasta que dejamos de suministrar energía eléctrica) por esta razón aparecen los dispositivos de almacenamiento secundarios o auxiliares, los cuales son capaces de conservar la información de manera permanente, mientras su estado físico sea óptimo. Los dispositivos de almacenamiento externo pueden residir dentro del CPU y están fuera de la placa de circuito principal.

CD-R

Es un disco compacto de 650 MB de capacidad que puede ser leído cuantas veces se desee, pero cuyo contenido no puede ser modificado una vez que ya ha sido grabado. Dado que no pueden ser borrados ni regrabados, son adecuados para almacenar archivos u otros conjuntos de información invariable.

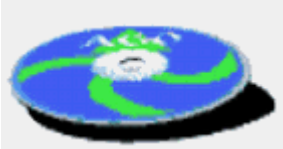


Imagen No. 2: CD-R

CD-RW

Posee la capacidad del CD-R con la diferencia que estos discos son regrabables lo que les da una gran ventaja. Las unidades CD-RW pueden grabar información sobre discos CD-R y CD-RW y además pueden leer discos CD-ROM y CDS de audio. Las interfaces soportadas son EIDE, SCSI y USB.

DVD-ROM

Es un disco compacto con capacidad de almacenar 4.7 GB de datos en una cara del disco, un aumento de más de 7 veces con respecto a los CD-R y CD-RW. Y esto es en una sola cara. Los futuros medios de DVD-ROM serán capaces de

almacenar datos en ambas caras del disco, y usar medios de doble capa para permitir a las unidades leer hasta cuatro niveles de datos almacenados en las dos caras del disco dando como resultado una capacidad de almacenamiento de 17 GB. Las unidades DVD-ROM son capaces de leer los formatos de discos CD-R y CD-RW. Entre las aplicaciones que aprovechan la gran capacidad de almacenamiento de los DVD-ROM tenemos las películas de larga duración y los juegos basados en DVD que ofrecen videos MPEG-2 de alta resolución, sonido inmersivo Dolby AC-3, y poderosas graficas 3D

Imagen No. 3: DVD - ROM

DVD-RAM

Este medio tiene una capacidad de 2.6 GB en una ca ra del disco y 5.2 GB en un disco de doble cara, Los DVD-RAM son capaces de leer cualquier disco CD-R o CD-RW pero no es capaz de escribir sobre estos. Los DVD-RAM son regrabables pero los discos no pueden ser leídos por unidades DVD-ROM.

Imagen No. 4: DVD-RAM

DISCOS DUROS

Según (http://www.monografias.com, 2010): Parte de la PC donde se guarda la información; los hay de capacidad distinta aunque en la actualidad la tendencia es una capacidad de 2.1 GB como mínimo, habiendo de varias marcas como Seagate, Quantum, etc.

Con un bajo tiempo medio de acceso (menos de 20 ms) y una velocidad de transferencia de data tan alta que deben girar a más de 5.000 rpm, convirtiéndolo en una fuente de calor dentro de la PC, debiendo instalarles un ventilador para su refrigeración.

Parte física:

Compuesto de numerosos discos de material sensible a los campos magnéticos (denominados platos), unos sobre otros (figura 1); asemejan un conjunto de discos CD con un mecanismo de giro y un brazo lector incluido.

Imagen No. 5: DVD-RAM

Parte Lógica:

Denominando así al circuito o placa que tiene cada disco duro, que será la encargada de hacer que el disco duro lea y grabe la data que deseamos almacenar en el.

Imagen No. 6: Parte lógica del Disco Duro

De presentarse un problema en esta parte del disco duro, no hay peligro de perder la data, solo tendríamos un problema de acceso a el, la solución inmediata seria la de cambiar el circuito para proceder a rescatar nuestra data.

Formato a alto nivel

Según (http://www.monografias.com): El formato a alto nivel es aquel que realiza el sistema, por ejemplo MS-DOS, cuando introducimos el comando **format c:**. Con esta orden, el sistema operativo inicializa el área del disco que comprende la partición C:, estableciendo el valor por defecto de su contenido y creando las tablas que a la postre alojarán la información de cómo y dónde, dentro de esa partición, estarán almacenados los archivos.

En un formateo a alto nivel, el sistema operativo creará todas estas estructuras de datos específicas en el área que comprenda la partición a la que dé formato.

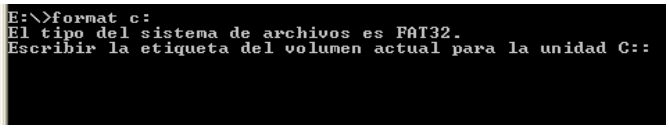


Imagen No. 7: Formato Alto nivel

Formato a bajo nivel

Es el formato físico del disco, operando a nivel de disco, y sin crear ninguna estructura de datos, simplemente establece un valor por defecto a la totalidad del disco duro, acabando con toda la información que contiene el disco, incluida la tabla de particiones y el gestor de arranque (que un formateo a alto nivel nunca toca).

Esta opción estaba presente en las BIOS de los equipos antiguos (486, primeros equipos Pentium), pero dada la mala costumbre de algunos fabricantes de discos duros de alojar cierta información necesaria en ciertos sectores, se elimino esta función en las actuales BIOS.

Este formato también elimina los virus de sector de arranque, que no podían ser eliminados con un formateo a alto nivel o de sistema, ya que este proceso no altera la información alojada en el sector de arranque (MBR).

Seagate tiene software para formatear sus productos a bajo nivel.

Pen Drive O Memoria Flash

Imagen No. 8: Pen drive o Memoria flash

Según (ANTONIO L., (2002). Aula Siglo XXI): Es un pequeño dispositivo de almacenamiento que utiliza la memoria flash para guardar la información sin necesidad de pilas. Los Pen Drive son resistentes a los rasguños y al polvo que han afectado a las formas previas de almacenamiento portable, como los CD y los disquetes. Los sistemas operativos más modernos pueden leer y escribir en ello sin necesidad de controladores especiales. En los equipos antiguos (como por ejemplo los equipados con Windows 98) se necesita instalar un controlador de dispositivo

Unidades de Zip

Según (ROMERO & TOLEDO): La unidad Iomega ZIP es una unidad de disco extraíble. Está disponible en tres versiones principales, la hay con interfaz SCSI, IDE, y otra que se conecta a un puerto paralelo. Este documento describe cómo

usar el ZIP con Linux. Se debería leer en conjunción con el HOWTO SCSI a menos que posea la versión IDE.

Imagen No. 9: Unidades de zip

TARJETAS DE MEMORIA

Según (http://es.wikipedia.org): Hoy en día, la mayoría de los nuevos PC tienen ranuras incorporadas para una gran variedad de tarjetas de memoria; Memory Stick, CompactFlash, SD, etc. Algunos dispositivos digitales soportan más de una tarjeta de memoria para asegurar compatibilidad.

Tabla No. 1: Tabla de datos de los formatos de tarjeta de memorias

Nombre	Sigla	Dimensiones	Sistema DRM
PC Card	PCMCIA	85.6 × 54 × 3.3 mm	Ninguno
CompactFlash I	CF-I	43 × 36 × 3.3 mm	Ninguno
CompactFlash II	CF-II	43 × 36 × 5.5 mm	Ninguno
SmartMedia	SM / SMC	45 × 37 × 0.76 mm	Ninguno
Memory Stick	MS	50.0 × 21.5 × 2.8 mm	MagicGate
Memory Stick Duo	MSD	31.0 × 20.0 × 1.6 mm	MagicGate
Memory Stick PRO Duo	MSPD	31.0 × 20.0 × 1.6 mm	MagicGate
Memory Stick PRO-HG Duo	MSPDX	31.0 × 20.0 ×	MagicGate

		1.6 mm	
Memory Stick Micro M2	M2	15.0 × 12.5 × 1.2 mm	MagicGate
Miniature Card		37 x 45 x 3.5 mm	Ninguno
MultiMediaCard	MMC	32 × 24 × 1.5 mm	Ninguno
Reduced Size Multimedia Card	RS-MMC	16 × 24 × 1.5 mm	Ninguno
MMCmicro Card	MMCmicro	12 × 14 × 1.1 mm	Ninguno
Secure Digital card	SD	32 × 24 × 2.1 mm	CPRM
SxS	SxS		
Universal Flash Storage	UFS		
miniSD card	miniSD	21.5 × 20 × 1.4 mm	CPRM
microSD card	microSD	15 × 11 × 0.7 mm	CPRM
xD-Picture Card	Xd	20 × 25 × 1.7 mm	Ninguno
Intelligent Stick	IStick	24 x 18 x 2.8 mm	Ninguno
Serial Flash Module	SFM	45 x 15 mm	Ninguno
µ card	µcard	32 x 24 x 1 mm	Desconocido
NT Card	NT NT+	44 x 24 x 2.5 mm	Ninguno

SEGURIDAD INFORMÁTICA

Según (http://www.scribd.com): La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la

información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Según (www.ramosoft.com): Podemos entender como seguridad un estado de cualquier tipo de información o la (informático o no) que nos indica que ese sistema está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo. Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro. Para que un sistema se pueda definir como seguro debe tener estas cuatro características:

- **Integridad**: La información sólo puede ser modificada por quien está autorizado y de manera controlada.
- **Confidencialidad**: La información sólo debe ser legible para los autorizados.
- **Disponibilidad**: Debe estar disponible cuando se necesita.
- **Irrefutabilidad** (No repudio): El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.

Según (http://www.scribd.com): Dependiendo de las fuentes de amenaza, la seguridad puede dividirse en tres partes: seguridad física, seguridad ambiental y seguridad lógica.

En estos momentos la seguridad informática es un tema de dominio obligado por cualquier usuario de Internet, para no permitir que su información sea comprometida.

Algunos términos:

- **Activo**: recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.
- **Amenaza**: es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
- **Impacto**: medir la consecuencia al materializarse una amenaza.
- **Riesgo**: Es la probabilidad de que suceda la amenaza o evento no deseado
- **Vulnerabilidad**: Son aspectos que influyen negativamente en un activo y que posibilita la materialización de una amenaza.
- **Ataque**: evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.
- **Desastre o Contingencia**: interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio.

Hipótesis

Las Herramientas de Análisis forense permitirá la Recuperación de Información en dispositivos de Almacenamiento.

Señalamiento de Variables

Variable Independiente: Herramientas de Análisis Forense

Variable Dependiente: Recuperación de Información

CAPITULO III

METODOLOGÍA

Enfoque

El presente proyecto de investigación tiene un enfoque analítico, comparativo y comprobatorio de información recuperada en dispositivos de almacenamiento de manera confiable a través de programas adecuados de análisis forense bajo la plataforma windows y linux.

Modalidad de Investigación

Es de esencial importancia que los efectos obtenidos o nuevos conocimientos a base de la tecnología tengan el máximo grado de exactitud y confiabilidad.
Durante el desarrollo del análisis trazado se emplearán dos tipos de investigación como son:

Investigación Bibliográfica
Investigación Experimental

La Investigación Bibliográfica constituye en la recolección de información técnica que sirve de fundamento teórico – científico para el desarrollo de la tesis, la misma que se realizará a través de textos referentes al Análisis forense y como punto principal la protección y recuperación de sus datos. Además de la información obtenida desde el Internet.

La Investigación Experimental depende completamente del investigador, de las decisiones que tome para manejar su comprobación, de tal manera que constituye en la realización de las pruebas necesarias con distintos escenarios en la FISEI-UTA para el análisis planteado, a través de la utilización de herramientas adecuadas de análisis forense bajo Windows y Linux.

Niveles

Descriptivo, porque el objeto de estudio fue analizado en todos sus detalles, para poder caracterizarlos con propiedad y enmarcarlo en el contexto.

Población y Muestra

El Investigador se basa en un muestreo no probabilístico Casual o Incidental ya que se trata de un proceso en el que el investigador selecciona directa e intencionadamente los individuos de la población. En este caso se utiliza como muestra los individuos a los que se tiene fácil acceso como son el Administrador de Sistemas, laboratoristas y docentes involucrados en el tema.
Es decir se trabajará directamente con la muestra.

Tabla No. 2: Muestra

Personal	Frecuencia
Administrador de Sistemas	1
Laboratoristas	4
Docentes	5
Total	**10**

Elaborado por: Investigador

Operacionalización de Variables

Variable Independiente: Herramientas de Análisis Forense

Tabla No. 3: Herramientas de Análisis Forense

Conceptualización	Dimensiones	Indicadores	Ítems Básicos	Técnicas e Instrumentos
Son diferentes procedimientos, que permiten realizar un **Análisis forense** con el objetivo de garantizar la conservación de la información bajo distintos **Sistemas Operativos** estudiados y que llegado al caso puedan ser aceptadas legalmente en un P**roceso Judicial**	Análisis Forense	Adquirir evidencias Autenticar (Comprobar) Análisis de datos sin modificar Recuperación de datos	¿Qué procedimientos de Análisis Forense utiliza la FISEI-UTA?	Entrevista / Cuestionario
	Sistemas Operativos	Unix Linux Windows MAC	¿En qué tipo de Sistema Operativo utilizan en la FISEI-UTA?	Entrevista / Cuestionario
	Proceso Judicial	Normas ISO Aspecto Legal Documentación Informe	¿Qué tipo de información se basa la FISEI-UTA en un Proceso judicial?	Entrevista / Cuestionario

Variable Dependiente: Recuperación de Información

Tabla No. 4: Recuperación de Información

Conceptualización	Dimensiones	Indicadores	Ítems Básicos	Técnicas e Instrumentos
Proceso donde se accede a una información previamente almacenada, mediante **Herramientas informáticas** que permiten establecer ecuaciones de búsqueda específicas. Dicha **información** ha debido de ser estructurada previamente a su **almacenamiento**	Herramientas Informáticas	Open Source Software Propietario Distribución Live	¿Qué herramientas informáticas dispone la FISEI-UTA?	Entrevista/Cuestionario
	Información	Bases de Datos Archivos Planos Otros	¿Qué tipo de información maneja la FISEI-UTA?	Entrevista/Cuestionario
	Almacenamiento	Disco Duro Pendrive CD/DVD Cinta Magnética Tarjetas de Memoria	¿Qué tipo de dispositivos de Almacenamiento existe en la FISEI-UTA?	Entrevista/Cuestionario

Plan para Recolección de la Información

Entrevista:

Dirigida al Administrador de sistemas, laboratoristas, docentes que tienen conocimiento en el tema y que laboran en la FISEI-UTA.

Su instrumento será un cuestionario elaborado con preguntas cerradas y objetivas

Plan para el Procesamiento de la Información

- Análisis de los resultados estadísticos, destacando tendencias o relaciones fundamentales de acuerdo con los objetivos e hipótesis.
- Interpretación de los resultados, con apoyo del marco teórico, en el aspecto pertinente.
- Comprobación de hipótesis. Para la verificación estadística conviene seguir la asesoría de un especialista.
- Establecimiento de conclusiones y recomendaciones.

CAPITULO IV
ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Entrevista dirigida a: Administradores de Sistemas, Laboratoristas y Docentes involucrados en el tema.

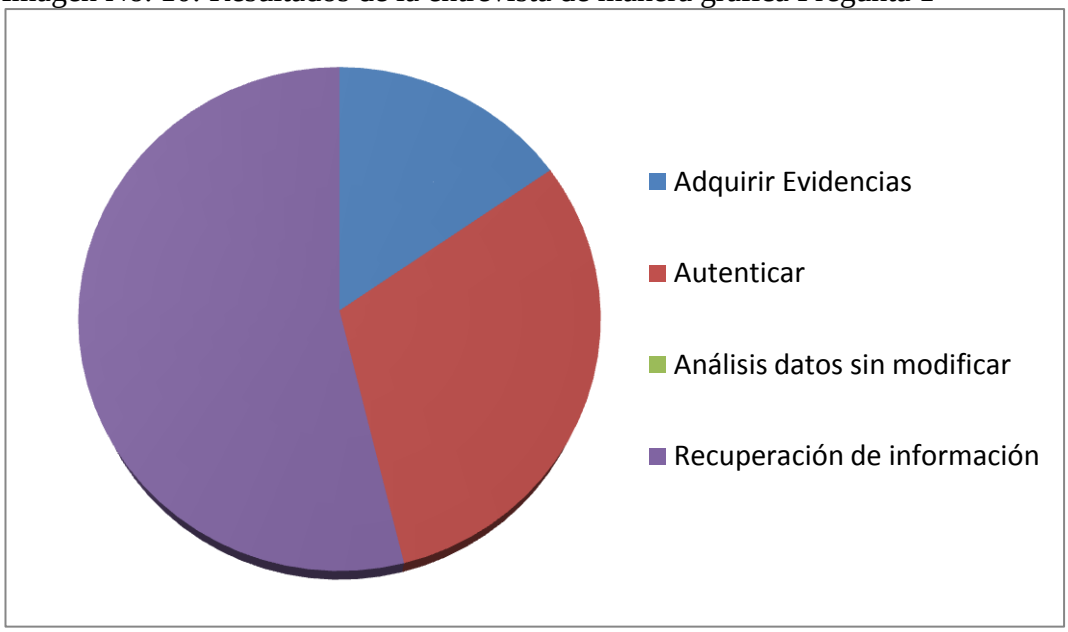
Pregunta N. 1: ¿Qué procedimientos de Análisis Forense utiliza la FISEI-UTA?

Tabla No. 5: Resultados de la entrevista Pregunta 1

	OPCIONES			
ENTREVISTADO	Adquirir Evidencias	Autenticar	Análisis datos sin modificar	Recuperación de Información
Administrad. Redes		**X**		**X**
Laboratorista 1		**X**		
Laboratorista 2				**X**
Laboratorista 3		**X**		**X**
Laboratorista 4				**X**
Docente 1				**X**
Docente 2	**X**			
Docente 3		**X**		**X**
Docente 4				**X**
Docente 5	**X**			

Elaborado por: Investigador

Imagen No. 10: Resultados de la entrevista de manera gráfica Pregunta 1



Elaborado por: Investigador

INTERPRETACIÓN

De acuerdo a los resultados obtenidos se puede apreciar que el método principalmente utilizado es el de Recuperación de información que consiste en acceder a una información previamente almacenada, mediante herramientas informáticas que permiten establecer ecuaciones de búsqueda específicas, posteriormente el procedimiento de Autenticar que determina la comprobación de evidencias recogidas en el caso de darse un delito informático en la FISEI-UTA las mismas que deberán ser idénticas a las abandonadas al instante de la escena del crimen, por último realizándose esporádicamente el proceso de adquirir evidencias que inspecciona un sistema y que se encarga de detenerlo y examinar una copia de datos originales según el caso, cabe indicar que el procedimiento de análisis de datos sin modificar no es tomado en cuenta para ninguna de las personas motivo de la entrevista.

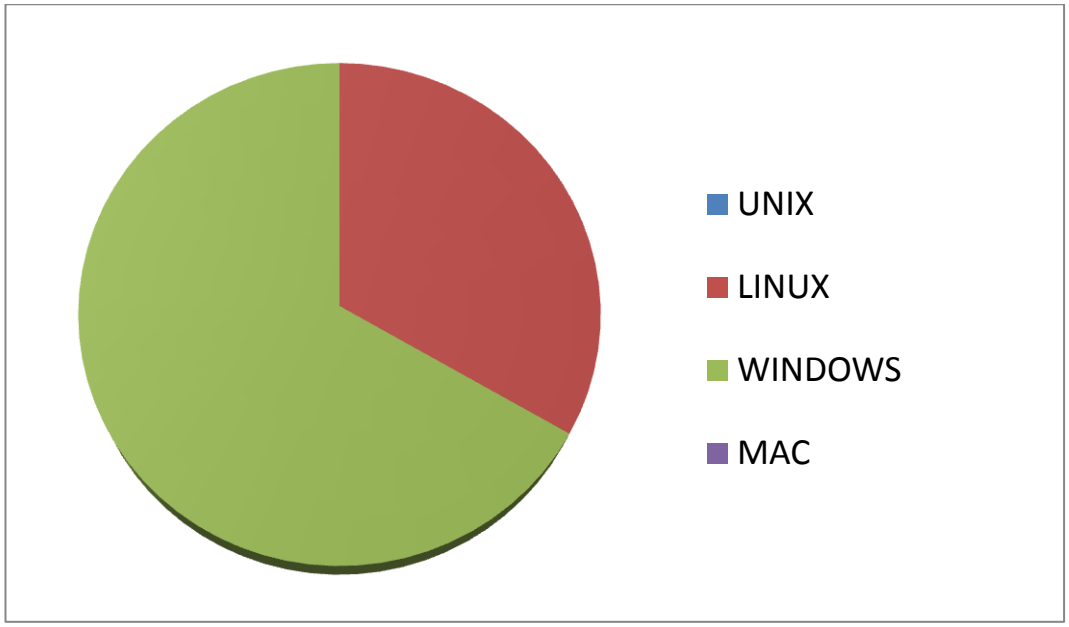
Pregunta N. 2: ¿Qué tipo de Sistema Operativo utilizan en la FISEI-UTA?

Tabla No. 6: Resultados de la entrevista Pregunta 2

	OPCIONES			
ENTREVISTADO	UNIX	LINUX	WINDOWS	MAC
Administrad. Redes		**X**	**X**	
Laboratorista 1		**X**	**X**	
Laboratorista 2		**X**	**X**	
Laboratorista 3			**X**	
Laboratorista 4			**X**	
Docente 1			**X**	
Docente 2			**X**	
Docente 3		**X**	**X**	
Docente 4		**X**	**X**	
Docente 5			**X**	

Elaborado por: Investigador

Imagen No. 11: Resultados de la entrevista de manera gráfica Pregunta 2



Elaborado por: Investigador

INTERPRETACIÓN

De acuerdo a los resultados obtenidos se puede apreciar que el sistema operativo Windows es el más utilizado en la FISEI-UTA por su interfaz y facilidad de manejo a nivel gráfico desarrollado por Microsoft el más considerado en el mercado en equipos Cliente dispone de nuevas versiones como Windows 7 y para servidores Windows 2008.

Posteriormente Linux debido a que se debe tener más conocimiento para poder manipularlo es un sistema operativo multitarea, multiusuario, multiplataforma y multiprocesador utilizado por muchos administradores para aplicaciones de configuración de servidores y proporcionar herramientas para seguridad de datos de igual manera empleado en la FISEI-UTA pero no en su mayoría.

Pregunta N. 3: ¿En qué tipo de información se basa la FISEI-UTA en un proceso judicial?

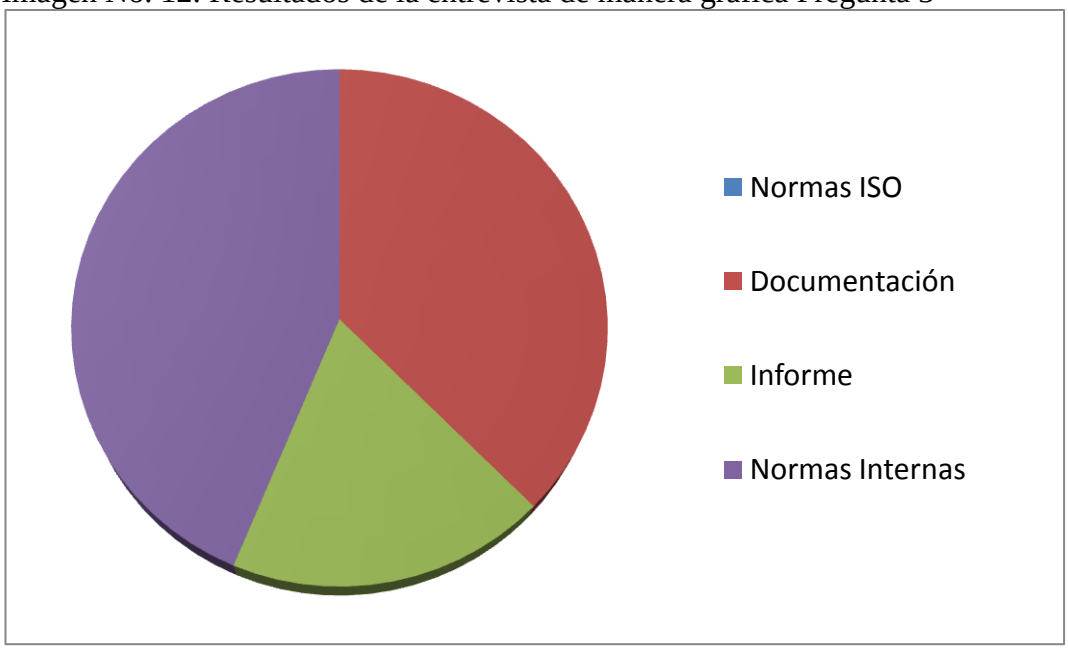
Tabla No. 7: Resultados de la entrevista Pregunta 3

	OPCIONES

ENTREVISTADO	Normas ISO	Documentación	Informe	Normas Internas
Administrad. Redes		**X**	**X**	**X**
Laboratorista 1				**X**
Laboratorista 2		**X**		**X**
Laboratorista 3		**X**	**X**	**X**
Laboratorista 4				**X**
Docente 1				**X**
Docente 2		**X**	**X**	
Docente 3		**X**		
Docente 4				**X**
Docente 5		**X**		

Elaborado por: Investigador

Imagen No. 12: Resultados de la entrevista de manera gráfica Pregunta 3



Elaborado por: Investigador

INTERPRETACIÓN

De acuerdo a los resultados obtenidos se puede apreciar que el tipo de información en la que se basa la FISEI-UTA en un proceso judicial son las Normas Internas que serán establecidas por los diferentes estatutos de la Universidad, posteriormente en la documentación y el informe el mismo que en un análisis forense los resultados deberán ser verificables independientemente del investigador de las herramientas empleadas y de su metodología que pueden llevar a un proceso judicial si se da el caso.

Pregunta N. 4: ¿Qué herramientas informáticas dispone la FISEI-UTA?

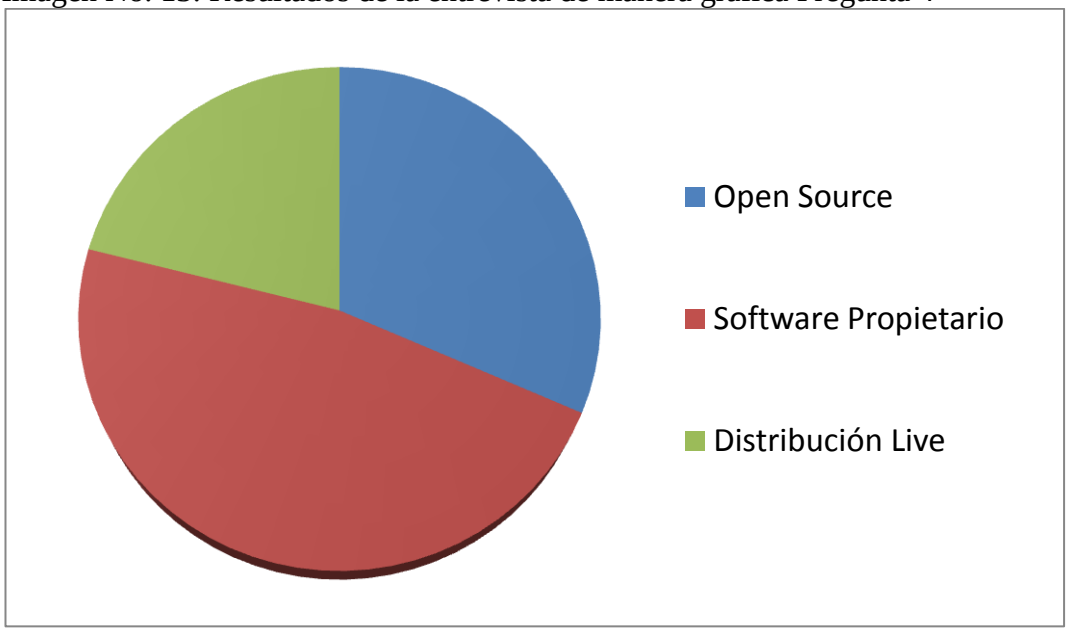
Tabla No. 8: Resultados de la entrevista Pregunta 4

	OPCIONES		
ENTREVISTADO	Open Source	Software Propietario	Distribución Live
Administrad. Redes	**X**	**X**	
Laboratorista 1	**X**	**X**	
Laboratorista 2	**X**	**X**	**X**
Laboratorista 3		**X**	
Laboratorista 4		**X**	
Docente 1		**X**	
Docente 2	**X**	**X**	**X**
Docente 3	**X**	**X**	**X**

Docente 4	**X**		**X**
Docente 5		**X**	

Elaborado por: Investigador

Imagen No. 13: Resultados de la entrevista de manera gráfica Pregunta 4



Elaborado por: Investigador

INTERPRETACIÓN

De acuerdo a los resultados obtenidos se puede apreciar que las herramientas informáticas que dispone la FISEI-UTA son principalmente Software propietario los cuales se tienen que pagar por su licencia, posteriormente bajo dependencia open source es decir de libre utilización y descarga y eventualmente distribución live que son cd's live que vienen booteables directamente sin utilizar su disco duro para instalarlo.

Pregunta N. 5: ¿Qué tipo de información maneja la FISEI-UTA?

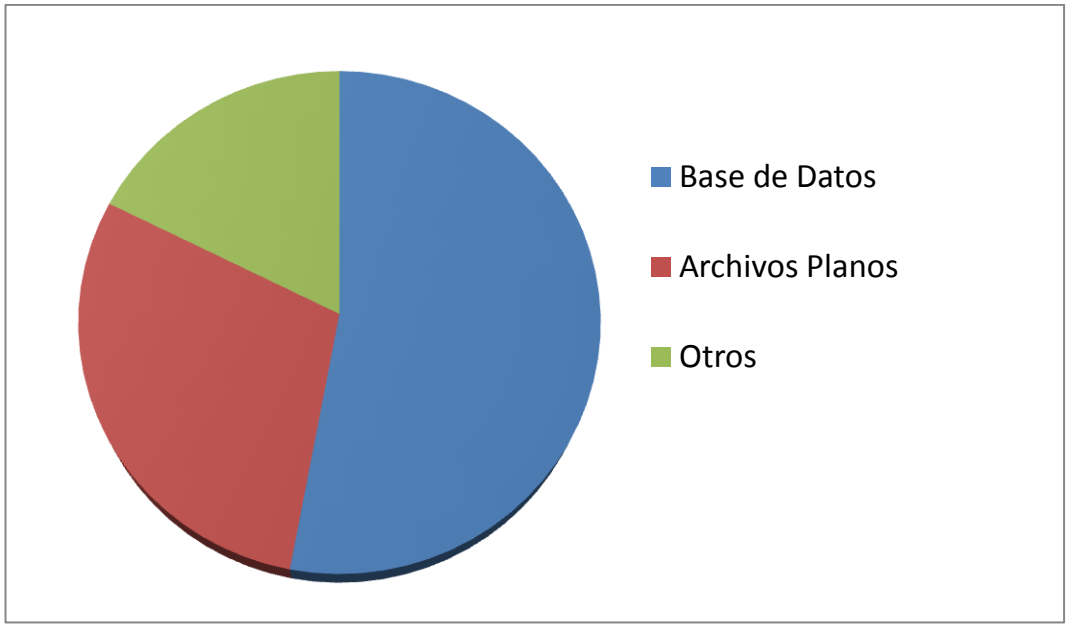
Tabla No. 9: Resultados de la entrevista Pregunta 5

OPCIONES

ENTREVISTADO	Base de Datos	Archivos Planos	Otros
Administrad. Redes	**X**	**X**	
Laboratorista 1	**X**		
Laboratorista 2	**X**	**X**	**X**
Laboratorista 3		**X**	
Laboratorista 4	**X**		
Docente 1	**X**		
Docente 2	**X**	**X**	
Docente 3	**X**	**X**	**X**
Docente 4	**X**		**X**
Docente 5	**X**		

Elaborado por: Investigador

Imagen No. 14: Resultados de la entrevista de manera gráfica Pregunta 5



Elaborado por Investigador

INTERPRETACIÓN

De acuerdo a los resultados obtenidos se determina que el tipo de información que maneja la FISEI-UTA es principalmente una Base de Datos la misma que se encuentra ordenada y clasificada en un repositorio y utilizado a través de diferentes programas que son gestores de Base de datos.
Posteriormente Archivos planos y otro tipo de información que se maneja en los diferentes departamentos de la facultad

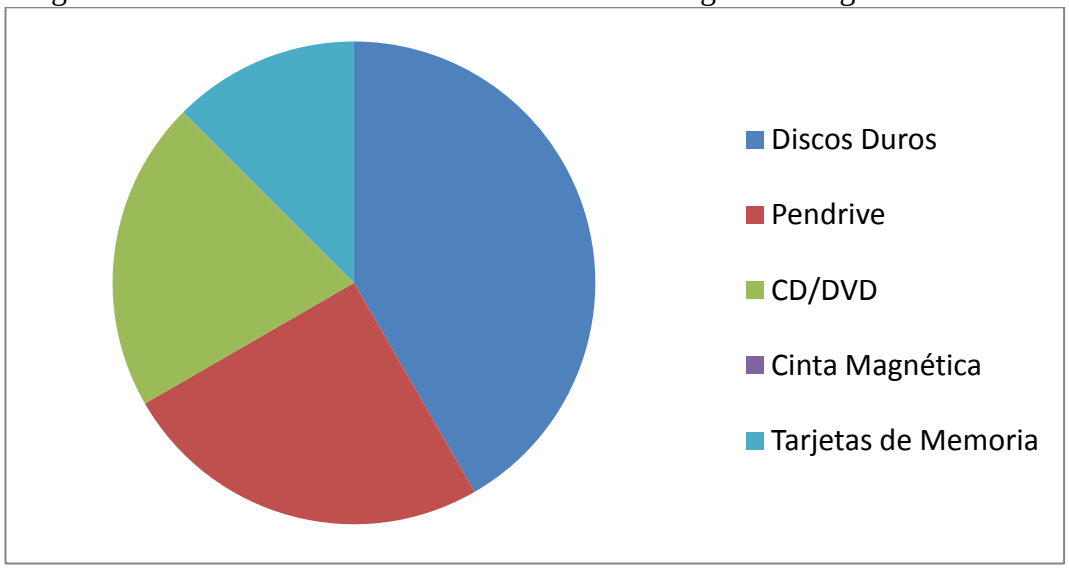
Pregunta N. 6: ¿Qué tipo de dispositivos de almacenamiento existe en la FISEI-UTA?

Tabla No. 10: Resultados de la entrevista Pregunta 6

	OPCIONES				
ENTREVISTADO	Discos Duros	Pendrive	CD/DVD	Cinta Magnética	Tarjetas de Memoria
Administrad. Redes	**X**	**X**	**X**		
Laboratorista 1	**X**				**X**
Laboratorista 2	**X**	**X**	**X**		**X**
Laboratorista 3	**X**				
Laboratorista 4	**X**				
Docente 1	**X**	**X**			**X**
Docente 2	**X**	**X**	**X**		
Docente 3	**X**	**X**	**X**		
Docente 4	**X**	**X**	**X**		
Docente 5	**X**				

Elaborado por: Investigador

Imagen No. 15: Resultados de la entrevista de manera gráfica Pregunta 6



Elaborado por: Investigador

INTERPRETACIÓN

De acuerdo a los resultados obtenidos se puede apreciar que los dispositivos de almacenamiento que se utilizan en su mayoría en la FISEI-UTA son los discos duros los hay de capacidad distinta y marca como Seagate, Quantum, Werter digital, maxtor, etc.

Posteriormente los pendrive o flash memory que se los denominan y esporádicamente diversos dispositivos de almacenamiento que actualmente están apareciendo y siendo muy utilizados como son las tarjetas de memoria, cabe indicar que las cintas magnéticas ya son obsoletas y no se las utiliza.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- Con el presente estudio realizado se ha determinado que las diferentes herramientas de análisis forense que se utiliza para la recuperación de información en la FISEI-UTA no son lo suficientemente adecuadas y requeridas.

- El estudio establece principalmente en la falta de herramientas de computación forense con las que se pueda contar en el caso de haber algún incidente informático.

- Una vez realizado el estudio es viable tener una medición casi exacta de los problemas que existen en la Recuperación de Información.

- No se cuenta con un estudio de diferentes escenarios que permita minimizar los diversos problemas de pérdida de información en dispositivos de almacenamiento.

- A través del estudio efectuado no se puede trabajar de forma directa en los dispositivos de almacenamiento ya que debido algún error en su manipulación, se podrían perder evidencias.

Recomendaciones

- Es recomendable disponer de diferentes herramientas adecuadas de análisis forense en calidad más no en cantidad para la recuperación de información.

- Es recomendable en el caso de darse un incidente informático determinar las herramientas necesarias con el objetivo de adquirir evidencias que serán base para una demanda judicial de darse el caso.

- Para minimizar los problemas de pérdida de información es recomendable determinar una política de seguridad como usos, contraseñas, permisos, perfiles, etc, y de esta manera mantener la integridad de los datos.

- Establecer escenarios que permita medir el nivel de pérdida de información a través de cuadros estadísticos etc.

- Obtener imágenes, hacer copias idénticas de disco duro u otro dispositivo de almacenamiento, para trabajar con dicha copia en el análisis forense y no comprometer el original.

CAPITULO VI

LA PROPUESTA

Datos Informativos

Título

Herramientas de Análisis Forense y Recuperación de información en los dispositivos de almacenamiento, en los laboratorios de la FISEI-UTA, durante el primer trimestre del 2010

Beneficiarios

La Institución beneficiada será FISEI de la UTA porque contaría de un aporte científico y tecnológico para estudiantes, laboratoristas y docentes, los mismos que dispondrán de información más detallada sobre herramientas de Análisis forense y Recuperación de información en dispositivos de almacenamiento.

Ubicación

La FISEI de la Universidad Técnica de Ambato se encuentra ubicada en el sector de Huachi Chico

Antecedentes de la Propuesta

A través del estudio realizado en los laboratorios de la FISEI-UTA y en base a información obtenida a través de encuestas a laboratoristas, administradores de

sistemas y personal docente se ha determinado que las herramientas utilizadas para análisis forense y recuperación de información en dispositivos de almacenamiento no son lo suficientemente adecuadas para su seguridad y confiabilidad, además de la falta de conocimiento de las mismas.

Además hay que recalcar como antecedente investigativo que por pruebas o investigación los estudiantes especialmente de sistemas pueden llegar a destruir o borrar datos, además de tratar de alcanzar el mayor ancho de banda.

Es de mucha importancia saber de la existencia de información importante que se maneja dentro de la facultad y en sus diferentes departamentos así como también responsables del manejo de servidores, swiches capa 3, etc. En el caso de los laboratorios la última opción debido a virus o archivos dañados es el formateo de sus máquinas, además del levantamiento de imágenes cada fin de mes ya su vez realizar respaldos de servidores.

Justificación

Los diversos delitos informáticos que se dan actualmente y a su vez el no tener un respaldo adecuado de su Hard Disk, la pérdida de información importante ya sea en su mismo Hard Disk, CD-DVD ,Pen drive, Memorias como SD-XD-Stick, hacen que dispositivos de almacenamiento como estos sufran daños muy fuertes.
En La FISEI-UTA actualmente no se ha realizado un estudio de análisis forense lo cual sería muy importante no solamente en la facultad sino en toda la Universidad.
La Utilización de herramientas de Computación Forense para recuperación y reparación de archivos como Rescuepro Deluxe V4.0, RecoverMyFiles, GetDataBack, Photorec, Foremost, Disk Recovery, Pc Inspector, Magic Recovery, Easy Recovery, etc y por otro lado bajo Linux software para tareas de análisis forense Autopsy con Sleuthkit, Knofix , así como también Helix LIVE Cd que nos permitirán ejecutarlos sin necesidad de instalar en el computador, programas para creación de imágenes lógicas, copias idénticas de bit a bit y otros se justifica por la necesidad de desarrollar tareas de recuperación de información

en dispositivos de almacenamiento y obtener un cuadro comparativo de mayor eficacia Windows / Linux determinando que herramienta es la más adecuada para cada tipo de formato y por otro lado algo muy importante establecer evidencias claras e incluso de darse el caso de un ataque informático Qué, Cómo Dónde fue ocasionado y qué herramienta es la más adecuada según el caso como datos, imagen, video y de esta manera resolver estos grandes inconvenientes que suceden a nivel mundial.

Objetivos

Objetivo General

- Realizar un análisis de las diferentes herramientas de computación forense para la recuperación de información en dispositivos de almacenamiento bajo las plataformas Linux y Windows.

.

Objetivos Específicos

- Determinar la lista de software open source y propietario necesario para tareas de rescate de información y captura de evidencias permitiéndonos obtener claramente qué herramienta es la más adecuada que garantice su estudio.
- Aplicar tareas de rescate utilizando herramientas de análisis forense necesarias en dispositivos de almacenamiento como Hard Disk, CD – DVD, Pen drive, Memorias como FLASH, SD- XD - STICK para este propósito en distintos escenarios en los laboratorios de la UTA.
- Estudiar características principales de cada una de las herramientas que van hacer utilizadas durante el proceso de recuperación de información teniendo en cuenta su alcance ya que cada caso es único.

- Realizar pruebas necesarias para la obtención de evidencias que nos permita tener un informe más claro y completo en el caso de darse un ataque informático.

- Elaborar cuadros comparativos de recuperación de información bajo las plataformas Windows y Linux realizado un estudio para cada caso como datos, imagen, video a través de escenarios en los laboratorios de la UTA.

ANÁLISIS DE FACTIBILIDAD

ECONÓMICO

La FISEI-UTA dispone de laboratorios en los cuales es factible realizar distintos escenarios para la elaboración de la propuesta.

En cuanto a licencias es factible ya que se dispondrá de software libre y programas propietarios que se dispone pero que no son parte de la FISEI-UTA sino del investigador.

Tabla No. 11: Factibilidad económica

Cantidad	Detalle	Costo
1	Laptop Hp dv 2000	870,00
1	Switch	35,00
1	Tarjeta de red	30,00
	Software Libre	-
1	Disco Duro SATA	70,00
2	CD	1,00
	TOTAL	1006,00

Elaborado por: Investigador

TÉCNICO

Para la ejecución de las actividades de la presente propuesta se cuenta con los laboratorios de la FISEI-UTA además del material técnico con el permiso de su administración. Por tanto es factible realizarlo.

Material Técnico

- Fundas Antiestáticas
- Guantes de látex
- Caja de destornilladores
- Cámara Fotográfica

FUNDAMENTACIÓN

TEORICA

EL MODELO EN ESPIRAL se divide en un número de actividades estructurales, también llamadas regiones de tareas. Generalmente, existen entre tres y seis regiones de tareas.

Comunicación con el cliente: las tareas requeridas para establecer comunicación para este caso el investigador y la Institución donde se lleva a cabo el estudio.

Planificación: las tareas requeridas para definir recursos, el tiempo y otras informaciones relacionadas con el estudio. Son todos los requerimientos.

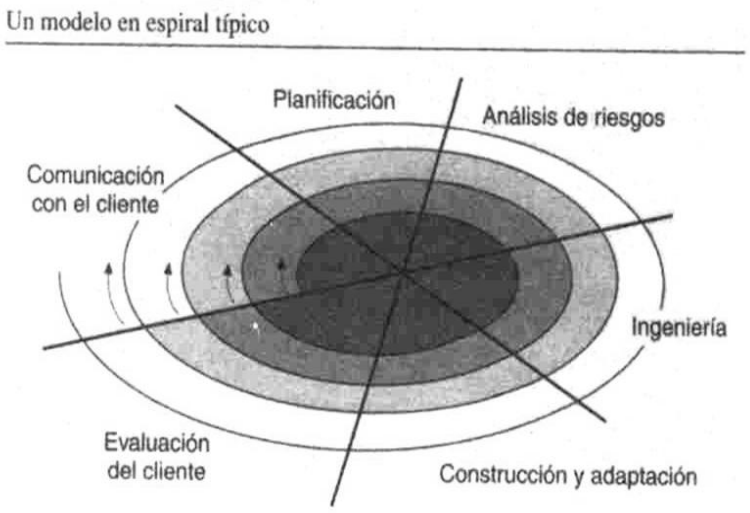
Análisis de riesgos: las tareas requeridas para evaluar riesgos técnicos y otras informaciones relacionadas con el proyecto.

Ingeniería: las tareas requeridas para construir uno o más escenarios para la correcta aplicación.

Construcción y adaptación: Pruebas, escenarios en los distintos laboratorios instalaciones soporte para laboratoristas de la FISEI-UTA.

Evaluación al cliente: Consiste en un estudio pero de darse el caso de implementación tareas requeridas que la institución lo solicite.

Imagen No. 16: Modelo en espiral



Fuente: http://148.202.148.5/cursos/cc321/fundamentos/unidad1/espiral.htm

METODOLOGÍA

Para el desarrollo de este estudio informático se decidió utilizar la metodología de prototipo, y además usar las etapas del modelo espiral, para complementar con el diseño de la metodología variante.

Para el desarrollo de la aplicación, se considera las fases del Modelo en espiral:

1°.- Planificación: Tener un cronograma de actividades, especificando las tareas a realizar.

2°. - Análisis de Riesgo: Identificar la población o datos que serán utilizados para identificar los archivos borrados como imagen, video, texto, etc, además de evaluar cada uno de los datos.

3°. - Ingeniería: Desarrollar cada uno de los procedimientos de análisis forense y recuperación de información, es decir realizar el diseño detallado de la etapa.

4°. - Evaluación: A partir del desarrollo de los procedimientos se realiza el análisis de herramientas y prueba de los datos.

5°. - Toma de Decisiones: Se evalúa el resultado, a través de cuadros estadísticos en el q nos demuestra q herramienta es la más adecuada.

6°.- Refinamiento: Generan las posibilidades de sofisticar indicadas anteriormente a fin de llegar al objetivo.

MODELO OPERATIVO

La Solución al problema está dada en base al desarrollo detallado de cada uno de los objetivos planteados en la propuesta que tiene como punto principal el análisis de las diferentes herramientas de computación forense para la recuperación de información en dispositivos de almacenamiento bajo las plataformas Linux y Windows.

ANÁLISIS DE LAS DIFERENTES HERRAMIENTAS DE COMPUTACIÓN FORENSE Y RECUPERACION DE INFORMACION EN DISPOSITIVOS DE ALMACENAMIENTO

Antes de empezar a analizar las diferentes herramientas de análisis forense y recuperación de información en los dispositivos de almacenamiento como discos duros, pendrive, tarjetas de memorias, CD-DVD, entre otros, detallaremos las herramientas que se utilizarán durante la propuesta a ejecutarse, las mismas serán explicadas con detalle más adelante:

Software para Reparación de discos duros

Tabla No. 12: Software para Recuperación de discos duros

Software	Sistema Operativo
HDD Regenerator	Windows
DiskRepair	Windows

Elaborado por: Investigador

Software para creación de imágenes lógicas

Tabla No. 13: Software para creación de imágenes lógicas.

Software	Sistema Operativo
Acronis true image	Windows
Genie Backup	Windows
Snapshot	Windows

DD	Linux

Elaborado por: Investigador

Software para Recuperación de datos – Restauración de Archivos (Pendrive, Discos Duros, Papelera de Reciclaje, Memorias SD, Stick, CD-DVD)

Tabla No. 14: Software para Recuperación de datos – Restauración de Archivos

Software	Sistema Operativo
Easy Recovery	Windows
RecoverMyFiles	Windows
GetDataBack	Windows
RescuePro Delux v4	Windows
Photorec	Linux
Pc Inspector	Windows
Disk Recovery	Windows
Foremost	Linux

Elaborado por: Investigador

Software para tareas de Análisis Forense

Tabla No. 15: Software para tareas de Análisis Forense

Software	Sistema Operativo

Autopsy con Sleuthkit	Linux
Windows Forensic Toolchest (WFT)	Windows
Helix	Linux/Windows
Incident Response Collection Report (IRCR2)	Windows
Auditoría de Registros	

Elaborado por: Investigador

INSTALACION DE HERRAMIENTAS

Para mayor detalle de la instalación de las herramientas referirse al **ANEXO A**

DISCOS DUROS CON SECTORES DEFECTUOSOS

Existen dos tipos de sectores defectuosos:

Sectores mal magnetizados

Defectos materiales del disco

Los primeros se pueden arreglar fácilmente con el software adecuado. Los segundos muy difícil de arreglarlo pero si no son demasiados podremos seguir utilizando el disco sin problemas Lo malo que tienen los defectos materiales es que, si son muchos, pueden indicar que el deterioro del disco va creciendo. Sea cual sea el caso y poniendo a parte el problema del disco duro, lo peor que nos puede pasar es que perdamos algún archivo.

Lo primero que hay que hacer cuando Windows empieza a tambalearse es ejecutar el **CHKDSK** antes se llamaba SCANDISK y si aún Windows no llega a iniciarse pues se puede optar por programas como **NTFS Dos Pro**, que lo primero que hace es ejecutar CHKDSK. Una vez confirmado ya los sectores defectuosos procedemos a utilizar herramientas sofisticadas como el caso de **HDD Regenerator** el cual repara los sectores defectuosos debidos a errores magnéticos

sin pérdida de datos**.** Solamente habría que volver a copiar los archivos del sistema de Windows si no carga porque estaban dañados y solucionado el problema. **DiskRepair** es otra opción.

Cuando los sectores están materialmente dañados existen programas como **Seagate Seatools Graphical** es capaz de encontrar los sectores defectuosos y marcarlos, haciendo una lista con ellos. Así, el sistema operativo los ignora, y es como si no existieran, como si tuviéramos un disco duro más pequeño

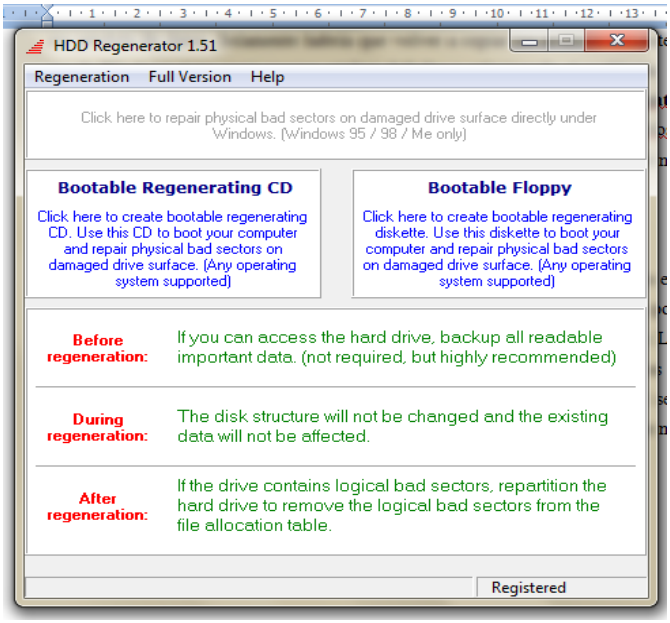
SOFTWARE PARA REPARACIÓN DE DISCOS DUROS

HDD REGENERATOR

Herramienta muy sofisticada el cual su función es que escanea el disco duro en busca de sectores defectuosos y se encarga de reparar los que fueron creados por errores magnéticos, obviamente quedan fuera los sectores dañados físicamente. Lo interesante de esta aplicación es que es independiente del sistema de archivos y del sistema operativo instalado en el disco duro, ya que el chequeo, al ser realizado a bajo nivel, ignora la información que está en el disco por lo que no será necesario formatear.

EJECUCIÓN

Imagen No. 17: Captura Opciones HDD Regenerator parte 1



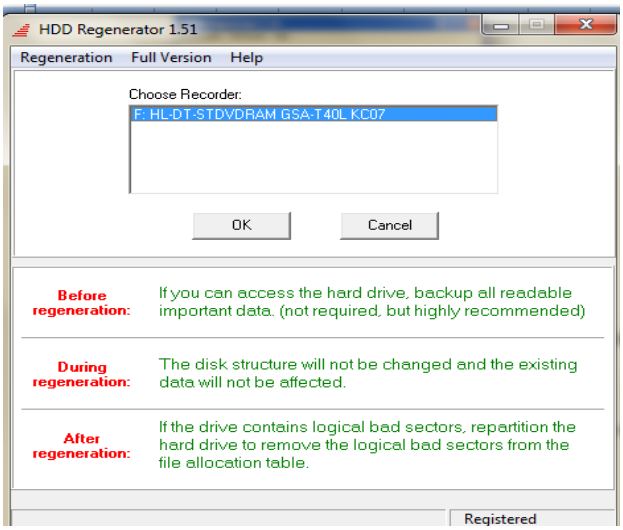
Elaborado por: Investigador

Nos aparece una pantalla en la que nos visualiza dos tipos de opciones:

1. **Bootable Regenerating CD** .- Para crear un CD bootable para boot en el computador y reparar los sectores malos, dañados en la parte física.
2. **Bootable Floopy.-** Para crear un diskette bootable para boot en el computador y reparar los sectores malos, dañados en la parte física.

Para ese caso utilizaremos la opción de CD Bootable ya que resultaría mucho más fácil debido a que la unidad de floppy ya va quedando obsoleta. Siendo de esta manera:

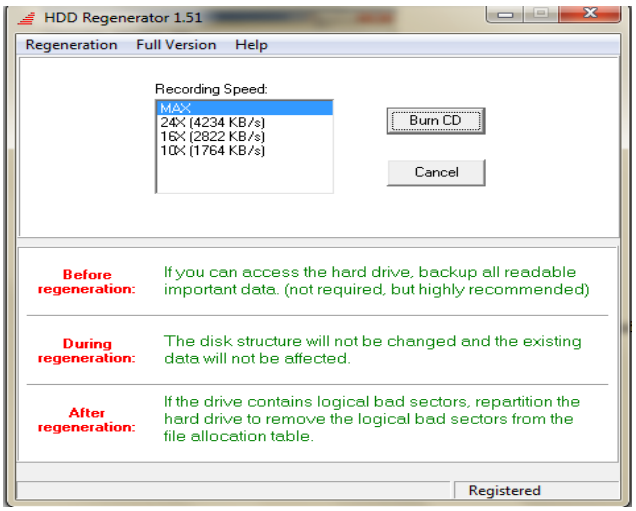
Imagen No. 18: Captura Opciones HDD Regenerator parte 2



Elaborado por: Investigador

Nos aparece la siguiente pantalla en la que escogemos la opción de la unidad a grabar y damos click en Ok

Imagen No. 19: Captura Opciones HDD Regenerator parte 3

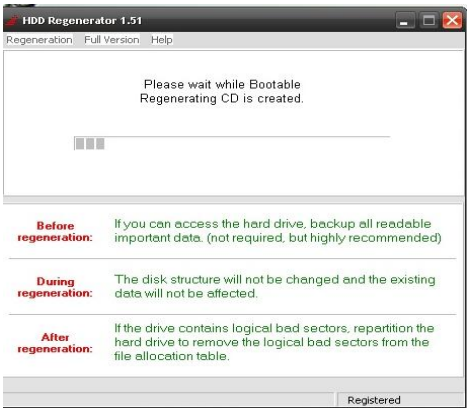


Elaborado por: Investigador

Escogemos la velocidad a grabar y hacemos click en burn CD

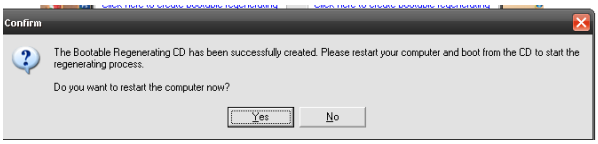
De esta manera se empezará a crear el Cd bootable

Imagen No. 20: Captura Opciones HDD Regenerator parte 4



Elaborado por: Investigador

Imagen No. 21: Captura HDD Regenerator parte 5



Elaborado por: Investigador

Luego de haber de reiniciar se ejecutará el cd bootable con el que utilizaremos para arrancar el sistema de la máquina en donde se encuentra el disco a reparar los sectores defectuosos

Verificamos el disco duro que se encuentra comprometido para este proceso necesitaremos de CD bootable HDD Regenerator

Imagen No. 22: CD booteable HDD Regenerator

Elaborado por: Investigador

Disco Duro a reparar

Maxtor 160 GB

Disco con sectores defectuosos

Contiene Windows XP

Imagen No. 23: Disco duro a reparar con HDD Regenerator

Elaborado por: Investigador

- Computador para realizar el respectivo proceso

  Intel Core 2Duo

  2GB RAM

  Disco Duro 500GB Sistema Operativo Windows 7

A continuación el disco duro será conectado al computador a utilizar

Imagen No. 24: Conexión Disco duro a reparar con HDD Regenerator parte1

Elaborado por: Investigador

Imagen No. 25: Conexión Disco duro a reparar con HDD Regenerator parte2

Elaborado por: Investigador

Conectamos el disco duro defectuoso a la máquina como esclavo y procedemos a realizar la reparación de sectores.

Debemos tomar en cuenta de configurar en la BIOS en la opción de configuración de arranque que inicialice desde el CD . Se lo puede realizar presionando F2 Arranque boot desde el CD

Al ingresar el CD bootable nos aparecerá una pantalla como la siguiente

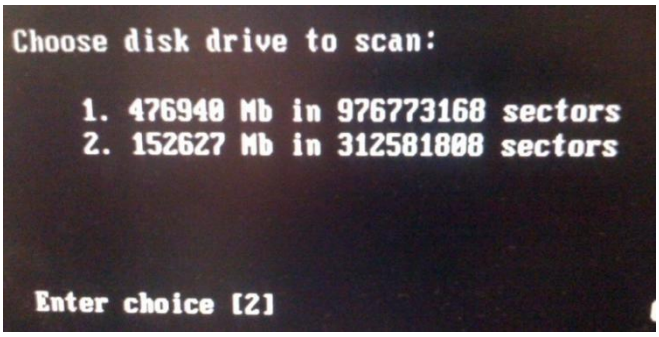
Imagen No. 26: Captura pantalla procedimiento HDD Regenerator parte1

Elaborado por: Investigador

En este caso nos presenta los 2 discos duros el (1) principal del Computador a utilizar que contiene 500GB y el disco duro (2) que sería de 160 GB a reparar.

Escogemos para esto la opción [2]

Imagen No. 27: Captura pantalla procedimiento HDD Regenerator parte2



Elaborado por: Investigador

La opción 2 nos dará el inicio de escaneo del disco duro a reparar

Imagen No. 28: Captura pantalla procedimiento HDD Regenerator parte3

Elaborado por: Investigador

Escogemos la opción 0 que se encuentra por defecto para que vaya desde el punto 0 como tal

Imagen No. 29: Captura pantalla procedimiento HDD Regenerator parte4

Elaborado por: Investigador

Luego empezará el análisis del disco, este proceso puede durar varias horas según el tamaño del disco duro.

En la parte de abajo aparecerán luego los sectores encontrados y los reparados.

FLOBO HARD DISK REPAIR

Herramienta destinada a realizar un minucioso y exhaustivo chequeo de todos los sectores de tu disco duro, detectando cualquier anomalía defectuosa. Dispone de herramientas para intentar reparar los sectores dañados y obtener la información SMART, además de utilidades para prevenir posibles fallos y errores futuros que se puedan producir en el disco.

El programa se puede instalar y ejecutarlo en ambiente Windows en una interfaz gráfica no así como el anterior el HDD Regenerator.

Imagen No. 30: Fotografía procedimiento F. H. Disk Repair parte1

Elaborado por: Investigador

Al ejecutar nos presenta una pantalla como la siguiente para lo cual debemos tener listo los dispositivos que tienen sectores defectuosos como el ejemplo anterior:

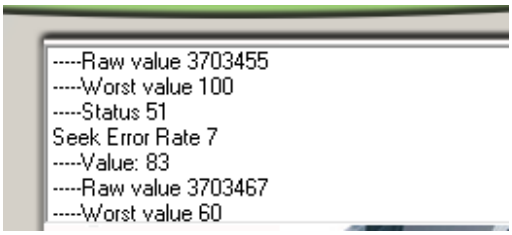
Imagen No. 31: Procedimiento F. H. Disk Repair parte2

Elaborado por: Investigador

Ubicamos el disco duro en la parte superior derecha e inicializamos desde el sector 0 para que vaya a escanear desde el inicio todos los sectores.

Este proceso puede durar varias horas e incluso todo depende del tamaño del disco duro. Una vez terminado el proceso nos da una estadística de todos los sectores que se han reparado y sus respectivos errores

Imagen No. 32: Procedimiento F. H. Disk Repair parte3



Elaborado por: Investigador

Otros tipos de errores que se dan y que se pueden solucionar a través de ciertos métodos es cuando nos da mensajes de error el computador al iniciar el sistema

justo en el mismo instante que va a ejecutarse el sistema operativo y los archivos están dañados o no existen.

Cuando el sistema ignora tu CD bootable

Si fue ignorado tu CD booteable por el sistema, será necesario cambiar la secuencia de arranque de la BIOS (pequeño programa que se encuentra en la placa madre del PC)

La secuencia de arranque es la parte de la BIOS que determina el orden de búsqueda de los dispositivos del PC para iniciar el sistema. Una vez que encuentra el dispositivo donde se encuentra el sistema, éste se inicia.

Por lo tanto, para arrancar desde el CD, es necesario que la unidad de CD esté declarada antes que el disco duro en la secuencia de búsqueda. Por lo que, si deseas reinstalar XP desde el CD y la secuencia de arranque es primero el disco duro y luego la unidad de CD, no podrás hacerlo. El disco duro tendrá prioridad. Hay que tener cuidado, la BIOS es el programa de base del PC. No modifiques nada en la BIOS si no estás seguro.

Si la BIOS no permite arrancar desde el CD

Algunos PC antiguos no permiten arrancar desde el CD, lo que puede ser un inconveniente en algunos casos LiveCD.

Sin embargo hay un método para hacerlo, que consiste en utilizar un disquete especial que cuando está insertado permite arrancar desde un CD. Arranca desde este disquete y selecciona “CD-Rom” para arrancar el mismo.

Cómo iniciar su computadora en Modo a prueba de fallos

También llamado "Modo seguro", para resolver algún problema puntual, o para ejecutar un antivirus o borrar manualmente algún virus, etc. De acuerdo a su sistema operativo, estas son las acciones a llevar a cabo:

Windows 7 y Windows Vista

1. Cierre todos los programas.
2. Desde Iniciar escriba MSCONFIG.EXE y pulse Enter. Aparecerá una ventana "Configuración del sistema".

3. Haga clic en la pestaña "Arranque".
4. En "Opciones de arranque", marque "Arranque a prueba de errores"
5. Haga clic en el botón [Aceptar], y en el mensaje siguiente confirme reiniciar su computadora.

Para volver a la normalidad el sistema, reitere los pasos 1 a 4, pero en ese punto, desmarque la casilla "Arranque a prueba de errores". Luego confirme los cambios, y reinicie su computadora.

Windows XP

1. Cierre todos los programas.
2. Desde Inicio, Ejecutar, escriba MSCONFIG.EXE y pulse Enter. Aparecerá la "Utilidad de configuración del sistema".
3. Haga clic en la pestaña "BOOT.INI".
4. En "Opciones de inicio", marque la casilla "/SAFEBOOT"
5. Haga clic en el botón [Aceptar], y en el mensaje siguiente confirme reiniciar su computadora.

Para volver a la normalidad el sistema, reitere los pasos 1 a 4, pero en ese punto, desmarque la casilla "/SAFEBOOT". Luego confirme los cambios, y reinicie su computadora.

Windows 98/Me

1. Cierre todos los programas.
2. Desde Inicio, Ejecutar, escriba MS
3. CONFIG y pulse Enter. Aparecerá el "Programa de configuración del sistema".
4. En la pestaña "General", haga clic en el botón [Avanzado].
5. En Configuración marque la casilla "Activar Menú de inicio"

6. Confirme los cambios y reinicie su computadora. Recuerde que debe apagarla físicamente, durante por lo menos 30 segundos.
7. Al aparecer el Menú de Inicio bajo MS-DOS seleccione "Modo a prueba de fallos" y pulse Enter.

Para volver a la normalidad el sistema, reitere los pasos 1 a 4, pero en ese punto, desmarque la opción "Activar Menú de inicio". Luego confirme los cambios, y reinicie su computadora.

Windows 2000

Windows 2000 no incluye por defecto la utilidad de configuración del sistema, pero en algunos casos puede haber sido instalada por el administrador. Si así fuera, siga las mismas instrucciones vistas para Windows 98/Me o Windows XP (dependerá de la versión instalada). En caso contrario, siga las instrucciones siguientes:

1. Cierre todos los programas.
2. Seleccione Inicio, Apagar el sistema.
3. Apague la computadora, y aguarde 30 segundos (no use el botón RESET, usted debe apagar su PC para borrar cualquier posible virus en memoria).
4. Encienda su PC.
5. Cuando aparezca la barra de Windows cargándose, pulse F8. Debería salir el menú de opciones avanzadas de Windows 2000.
6. Seleccione "Modo a prueba de fallas", "Modo seguro", o similar, y Windows debería arrancar en este modo.

Windows 95

1. Cierre todos los programas.
2. Seleccione Inicio, Apagar el sistema.
3. Apague la computadora, y aguarde 30 segundos (no use el botón RESET, usted debe apagar su PC para borrar cualquier posible virus en memoria).
4. Encienda su PC.

5. Cuando aparezca la leyenda "Iniciando Windows 95...", pulse F8. Debería salir el menú de inicio de Windows.
6. Seleccione "Modo a prueba de fallas" o similar, y Windows debería arrancar en este modo.

Reparara a través de la consola recuperación

Insertamos el cd de instalación del sistema operativo en este caso de XP**,** luego presionar la tecla R para iniciar la consola de recuperación.

Imagen No. 33: Captura pantalla Instalación XP

Elaborado por: Investigador

Luego nos pedirá la clave de administrador y ya podemos ingresar a los archivos de configuración si se desea reparar algún archivo tales como:

Reparar el archivo Boot.ini defectuoso

usar el comando **Bootcfg**. Estas son las opciones disponibles para Bootcfg:

· Bootcfg / add Busca en el disco duro instalaciones de Windows y permite añadirlas al archivo Boot.ini

· Bootcfg / scan Busca en el disco duro instalaciones de Windows

· Bootcfg / list Muestra cada entrada del archivo Boot.ini

· Bootcfg / Default Establece el sistema operative de arranque por defecto.

· Bootcfg / Rebuild Reconstruye el archive Boot.ini

Por ejemplo si lo que quieres es reconstruir el Boot.ino debes escribir el comando Bootcfg / Rebuild

Cuando se borra el NTDLR

1. escribimos FIXMBR y presionamos Enter luego nos pregunta si queremos continuar y escribimos S y damos Enter.
2. Ahora debemos copiar los archivos ntldr y ntdetect desde el CD de instalación de Windows hasta la unidad C:, esto lo vamos a hacer con los siguientes comandos:
3. copy **D**:\i386\ntldr C:\copy **D**:\i386\ntdetect.com C:\

Estos comandos los debemos escribir línea por línea y presionar Enter, pero es importante verificar cual es la letra que le corresponde la nuestra unidad de CD-ROM para reemplazarla por la letra D en los comandos mencionados anteriormente.

Ahora reiniciamos la PC y si se solucionó el problema se va a iniciar Windows correctamente, pero si no debemos plantearnos la opción de reinstalar Windows.

Una solución similar se aplica para cuando hay problemas de arranque con el Boot.ini y hal.dll o la reparación del MBR.

Repara un sector de arranque defectuoso

El sector de arranque es una pequeña parte del disco duro que contiene información acerca del sistema de archivos (NTFS o FAT32). Desde la consola de recuperación ejecutar el comando Fixboot C: y presiona Enter.

Donde C: se lo puede reemplazar por la letra de la unidad, que normalmente es C:

Repara el MBR defectuoso

El MBR o master boot record ocupa el primer sector del disco duro y es responsable de ceder el control a Windows para que este inicie su arranque. Para reparar el MBR lo puede hacer desde la consola de recuperación ejecutamos el comando Fixmbr DeviceHardDisk0 y presionar enter.

SOFTWARE PARA CREACIÓN DE IMÁGENES LÓGICAS

ACRONIS TRUE IMAGE HOME 2010

Paquete de Software que permite realizar copias de seguridad del sistema Operativo, aplicaciones, configuraciones y datos del computador. Se puede restaurar los datos de copia de seguridad rápida y fácilmente sean estos causados por virus o disco dañado.

Proporciona todas las herramientas esenciales que necesita para recuperar el sistema de su ordenador en caso de que suceda un desastre, como por ejemplo pérdida de datos, eliminación accidental de archivos o carpetas críticos o el fallo completo de la unidad del disco

Puede almacenar copias de seguridad en prácticamente cualquier dispositivo de almacenamiento de PC: unidades de discos duros internos o externos, unidades de red o diversos IDE, SCSI, FireWire (IEEE-1394), USB (1.0, 1.1 y 2.0) y Tarjeta PC (previamente denominada PCMCIA), unidades de medios extraíbles, así como en unidades de CD-R/RW, DVD-R/RW, DVD+R/RW, unidades magnéticas-

ópticas, Iomega Zip y Jaz. Puede crear una imagen de disco exacta, sector por sector.

Sistemas operativos compatibles

• Windows® 2000 Professional SP 4

• Windows XP SP 2

• Windows XP Professional x64 Edition

• Windows Vista (todas las ediciones)

Sistemas de archivos compatibles

• FAT16/32

• NTFS

• Ext2/Ext3

• Linux SWAP

Si un sistema de archivos no es compatible o está dañado, Acronis True Image Home puede copiar los datos utilizando un enfoque de sector por sector.

ACRONIS TRUE IMAGE HOME 2010

EJECUCION

Ejecutamos el programa

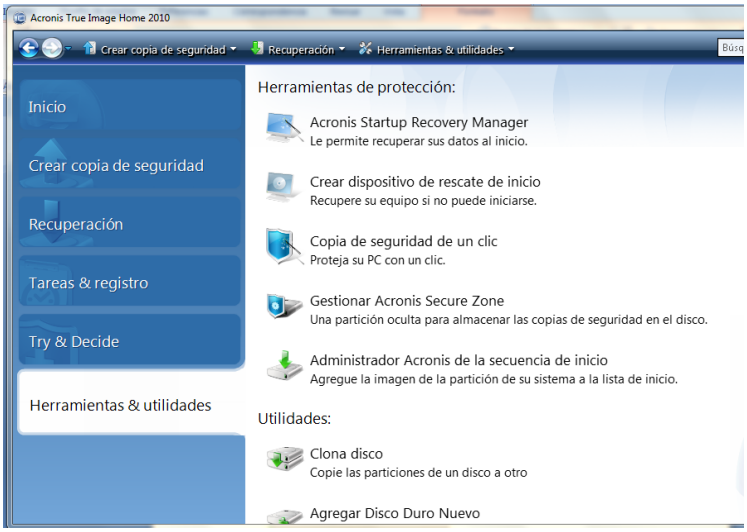
Imagen No. 34: Ejecución Acronis True Image Home 2010

Elaborado por: Investigador

En la siguiente pantalla nos muestra varias opciones

Escogemos herramienes y utilidades para clonar el disco por completo

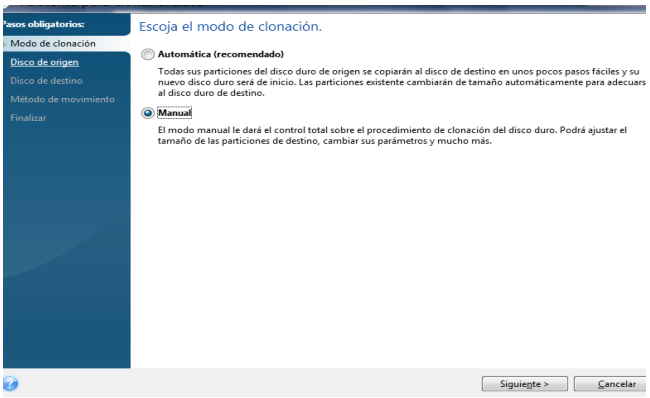
Imagen No. 35: Opciones Acronis True Image parte1



Elaborado por: Investigador

Escogemos el modo de clonación manual ya que podemos ajustar el tamaño de Las particiones como administradores ya que de darse el caso automático el software actuará las particiones por defecto

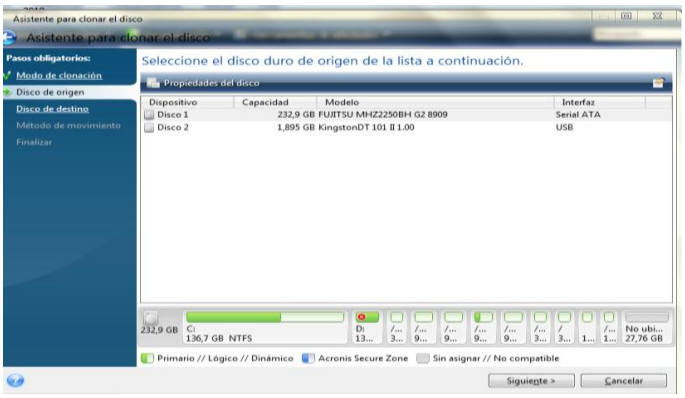
Imagen No. 36: Opciones Acronis True Image parte2



Elaborado por: Investigador

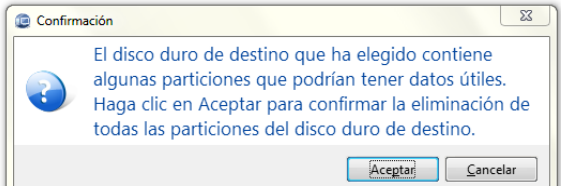
Ponemos en siguiente y escogemos el disco origen a clonar y ponemos siguiente para este caso pondremos el origen el 2

Imagen No. 37: Opciones Acronis True Image parte3



Elaborado por: Investigador

Aquí ponemos el disco destino a copiar que sería el 1



Nos despliega un mensaje en el que se van a eliminar si tiene el disco varias particiones Aceptar e inicia la clonación

GENIE_BACKUP_MANAGER_PRO_80312482

Genie Backup Manager Pro es la solución de copia de seguridad para las pequeñas y medianas empresas usuarias que fácilmente se desea realizar una copia de seguridad y recuperación todo su sistema. Nunca más tiene que sufrir de ejecución.

Características:

32-bit y 64-bit

Copia de seguridad de su PC o sólo directorio específico / archivos

Copias de seguridad remota segura

Copia de seguridad y restauración a través de cuenta en línea

Los archivos de copia de seguridad cerrado y abierto

Proteja sus activos de negocios con fuerte encriptación

Copia de seguridad en prácticamente cualquier dispositivo de almacenamiento como el famoso Iomega REV unidad

Protección Continua de Datos - Establecer la ejecución automática de copias de seguridad a intervalos de tiempo preestablecidos y rotar los distintos tipos de copia de seguridad.

Windows 2000, XP, Vista, 7

GENIE_BACKUP_MANAGER_PRO_80312482

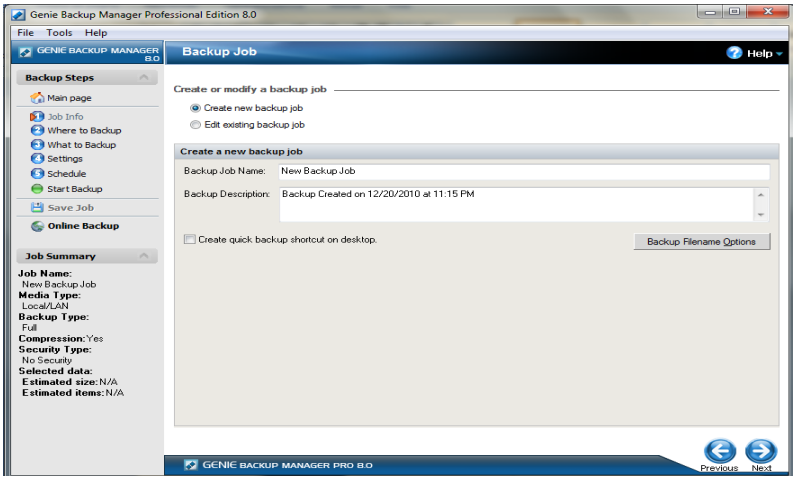
EJECUCION

Imagen No. 38: Ejecución Genie Backup Manager Pro parte1

Elaborado por: Investigador

Click en Backup

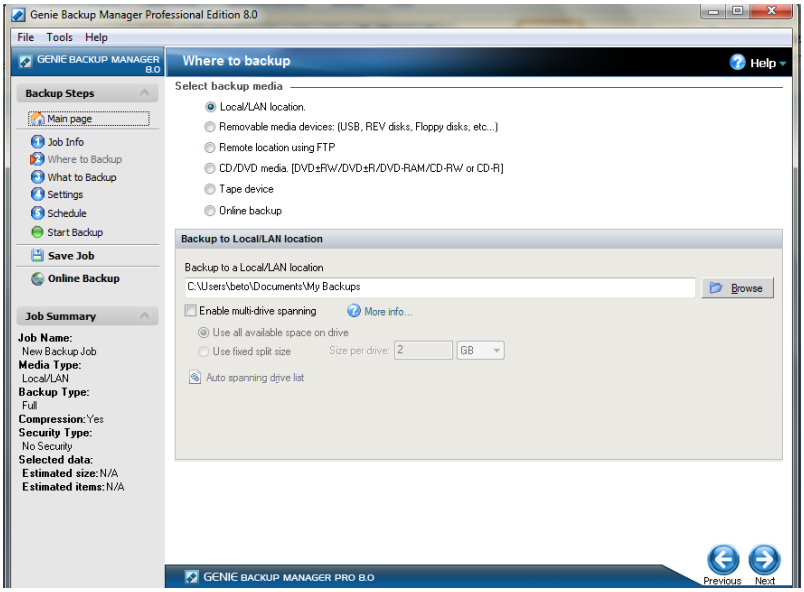
Imagen No. 39: Ejecución Genie Backup Manager Pro parte2



Elaborado por: Investigador

Creamos un nuevo respaldo de trabajo

Imagen No. 40: Ejecución Genie Backup Manager Pro parte3

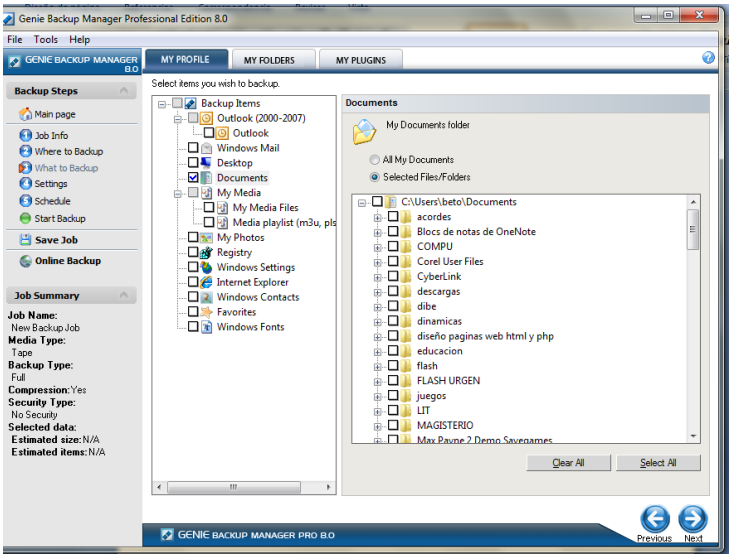


Elaborado por: Investigador

Localizamos el destino a donde vamos a guardar nuestro backup para este caso lo vamos hacer en el disco local, existe muchas opciones como en un sitio de red, un cd, dispositivo removible, localización remota, etc.

Podemos navegar por una serie de opciones en las que podemos escoger cualquier ítem, ya sea como archivos, carpetas, directorios partición, etc.

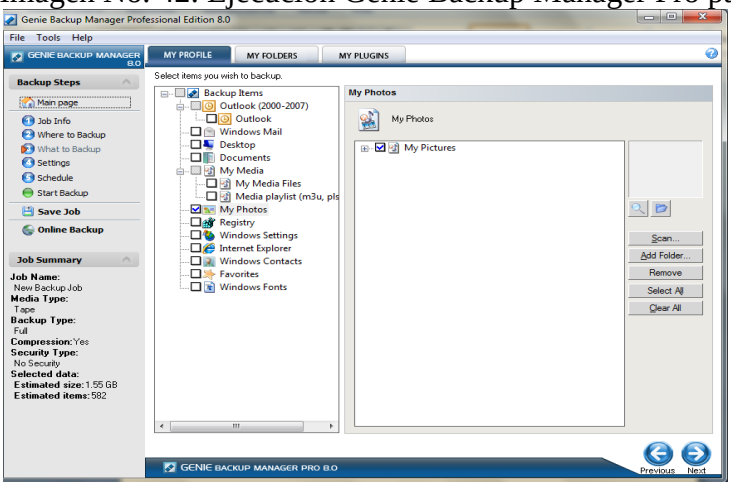
Imagen No. 41: Ejecución Genie Backup Manager Pro parte4

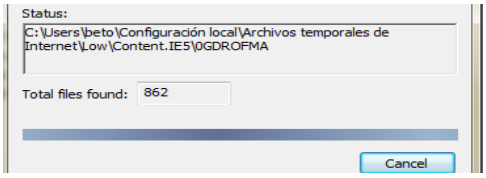


Elaborado por: Investigador

En este caso lo hemos puesto un directorio

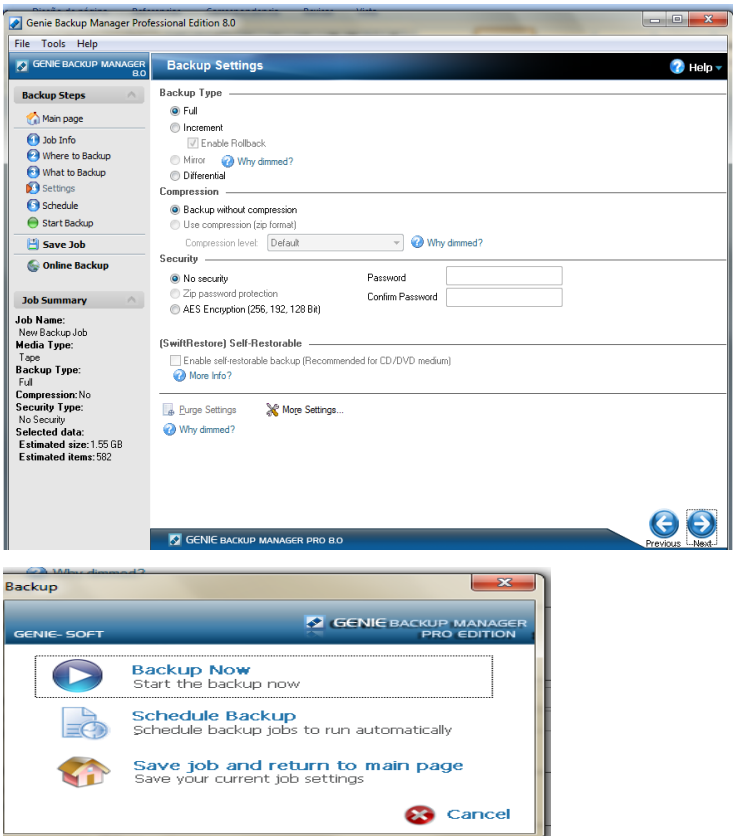
Imagen No. 42: Ejecución Genie Backup Manager Pro parte5





Elaborado por: Investigador

Imagen No. 43: Ejecución Genie Backup Manager Pro parte6



Elaborado por: Investigador

Una vez ya recolectado todo realizamos el backup definitivo

Backup Now y listo

DRIVE SNAPSHOT

Drive Snapshot crea una imagen exacta de disco de tu sistema en un archivo, incluyendo el sistema operativo, programas instalados, sus datos y todos los atributos de seguridad - mientras que las ventanas se está ejecutando y que continuará trabajando. Drive instantánea que te permite copia de seguridad de su partición o unidad de disco duro y también puede crear una imagen de disco de tu sistema.

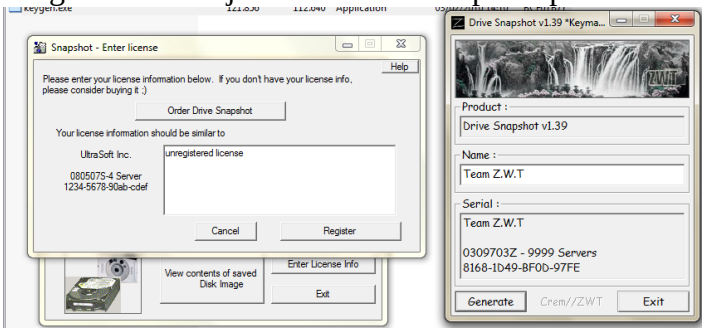
Crea Imagen de disco Copias de seguridad, al tiempo que ejecuta Windows No hay restart (para DOS). Nunca.

DRIVE SNAPSHOT

EJECUCION

Ponemos al inicio la serie del software para realizar la demostración ya que la versión Demo no garantiza su funcionamiento al 100%

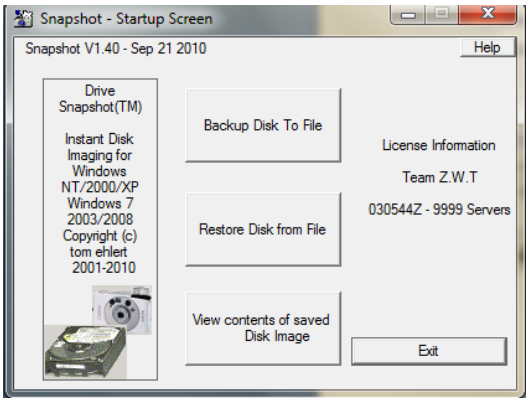
Imagen No. 44: Ejecución Drive Snapshot parte1



Elaborado por: Investigador

Imagen No. 45: Ejecución Drive Snapshot parte2

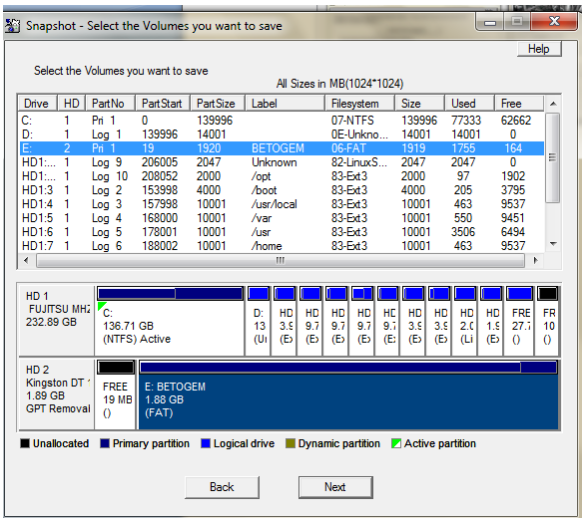
Nos aparece la siguiente pantalla



Elaborado por: Investigador

En esta pantalla nos muestra la pantalla en la que podemos escoger la partición a la imagen para este caso vamos crear para un pendrive

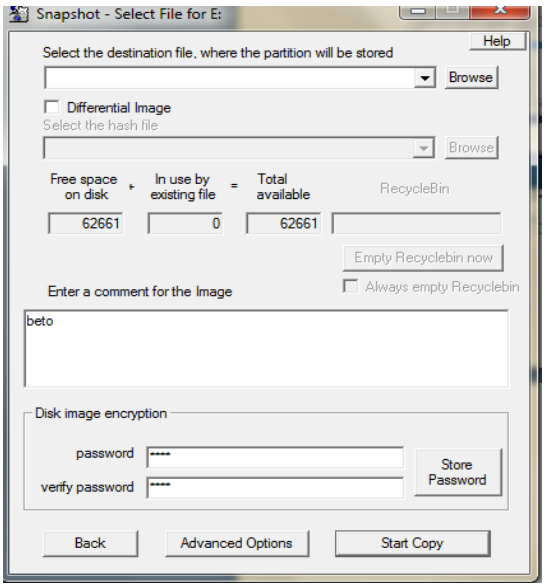
Imagen No. 46: Ejecución Drive Snapshot parte3



Elaborado por: Investigador

Selección de la ubicación donde va hacer almacenado, si desea se puede poner un password.

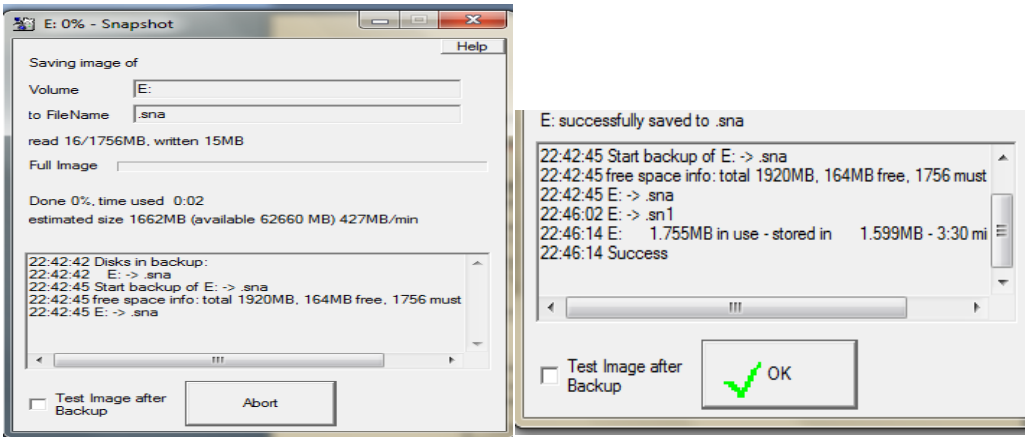
Imagen No. 47: Ejecución Drive Snapshot parte4



Elaborado por: Investigador

Inicio de la copia

Imagen No. 48: Ejecución Drive Snapshot parte5



Elaborado por: Investigador

Al finalizar la copia aparecerá todas las estadísticas como la pantalla siguiente

DD

dd - convierte y copia un fichero

con un tamaño de bloque seleccionable por el usuario, a la par que, opcionalmente, realiza sobre él ciertas conversiones.

El comando **dd** (duplicate disk) es un comando bastante útil para transferir datos desde un dispositivo/archivo hacia un dispositivo/archivo/etc.

La sintaxis básica del comando es la siguiente:

dd if=origen of=destino donde **if** significa "input file", es decir, lo que queremos copiar **of** significa "output file", o sea, el archivo destino (donde se van a copiar los datos); **origen** y **destino** pueden ser dispositivos (lectora de CD, diskettera, etc.), archivos, etc.

Haciendo imágenes ISO de un CD:

La forma mas fácil y efectiva de crear nuestras "imagenes" de CD es la siguiente:

dd if=/dev/cdrom of=micd.iso

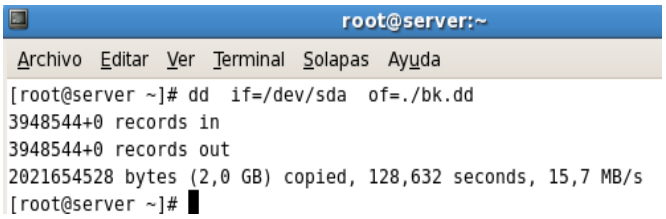
El comando **dd** también sirve para copiar particiones o discos completos unos sobre otros. Básicamente podemos decir que mediante **dd** podemos "clonar" particiones o nuestro disco rígido completo:

dd if=/hdxa of=/hdyb (copia una partición en otra)

dd if=/hdx of=/hdy (copia de un disco duro en otro) Donde: **x**: disco rígido origen, **y**: disco rígido destino, **a**: partición origen, **b**: partición destino.

EJECUCION

Imagen No. 49: Ejecución DD



Elaborado por: Investigador

SOFTWARE PARA RECUPERACIÓN DE DATOS – RESTAURACIÓN DE ARCHIVOS (PENDRIVE, DISCOS DUROS, PAPELERA DE RECICLAJE, MEMORIAS SD, STICK, CD-DVD)

EASY RECOVERY

Herramienta profesional, designada especialmente para discos duros o algún otro dispositivo de almacenamiento. Nos ayuda al análisis y chequeo exhaustivo del disco en la búsqueda de posibles errores de hardware, además de la manera como recuperar archivos perdidos o corruptos, reparación de correo electrónico, gestor de actualización de software, incluyendo los archivos de documentos, archivos de música MIDI, archivos de voz, archivos de medios digitales, y mucho más.

Tipos de medios

IDE / ATA / EIDE / SATA / SCSI duro

Jaz / Zip medios extraíbles

Disquetes

Los dispositivos de medios externos (USB / FireWire, USB portátil) Medios Digitales (CompactFlash, SmartMedia, memoria flash, memory sticks)

Sistema Operativo

Windows 98 SE y Windows Me

Windows 2000, Windows NT ® y Windows XP

Reparación de archivos capacidades para:

Microsoft Outlook 97, 2000, XP y 2003 (PST y OST)

Microsoft Outlook Express 5.0, 5.01, 5.5 y 6.0 (DBX)

Microsoft Word (DOC)

Microsoft Excel (XLS)

Base de datos Microsoft ® Access (MDB)

Microsoft PowerPoint (PPT)

Zip de archivos comprimidos (ZIP)

EJECUCION

Imagen No. 50: Ejecución Easy Recovery parte1

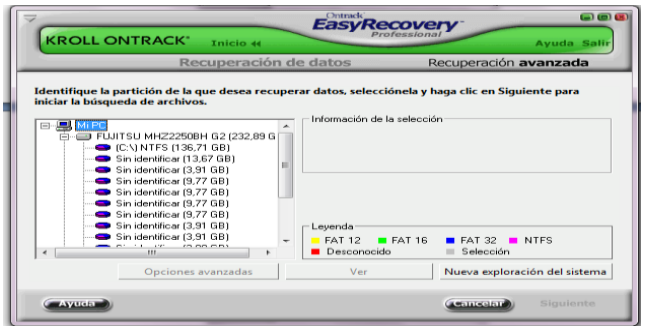
Elaborado por: Investigador

Imagen No. 51: Ejecución Easy Recovery parte2

Elaborado por: Investigador

Recuperación de datos de una flash

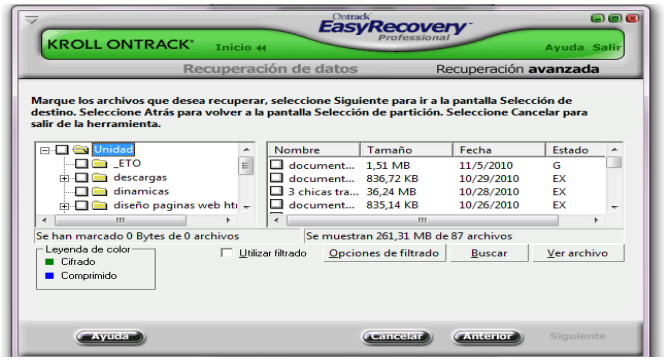
Imagen No. 52: Ejecución Easy Recovery parte3



Elaborado por: Investigador

Escogemos la partición

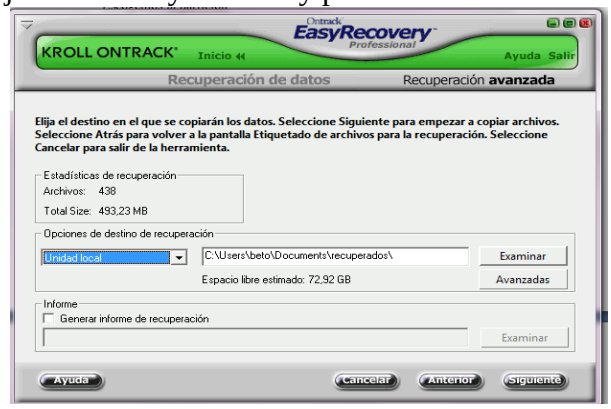
Imagen No. 53: Ejecución Easy Recovery parte4



Elaborado por: Investigador

Una vez recuperado los datos seleccionamos la carpeta que deseamos recuperar y la carpeta de destino a donde copiar lo recuperado

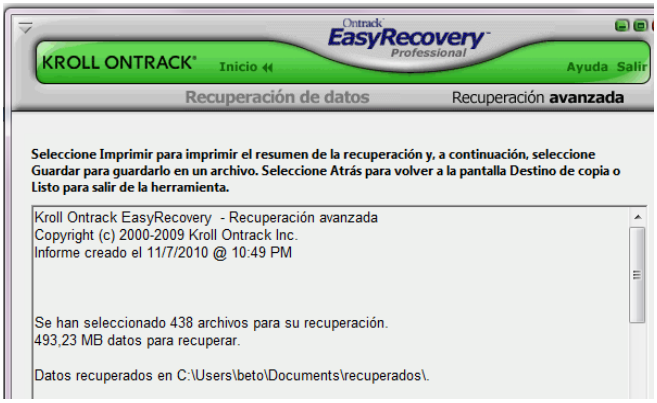
Imagen No. 54: Ejecución Easy Recovery parte5



Elaborado por: Investigador

Siguiente y nos dará la estadística recuperada

Imagen No. 55: Ejecución Easy Recovery parte6



Elaborado por: Investigador

RECOVERMYFILES

Herramienta que nos permite recuperar archivos borrados que se han eliminado de la Papelera de reciclaje o que se han perdido por dar formato al disco duro, por corrupción del mismo, por infección mediante un virus o un trojan, por un bloqueo inesperado del sistema o por un fallo de software, Además unidades de almacenamiento corrompidas que ya no son reconocidas por Windows, unidades a las que se ha dado formato.

Herramienta para la recuperación:

- Unidades de disco duro

- Las unidades USB

- Las unidades de almacenamiento externo

- Los medios de almacenamiento digital de la cámara - CDs y DVDs

Soporta ficheros:

• FAT16 – una primera versión del sistema de ficheros FAT, ahora rara vez se usa

• FAT32 – común para los medios de almacenamiento externo y equipos de cámaras digitales

exFAT – (Extended File Allocation Table), un sistema de archivos adaptadas especialmente para unidades de flash

• GPT – Tabla de partición GUID, un estándar para el diseño de la tabla de particiones en un disco duro físico

• NTFS – Standard archivos de sistema para Windows Vista, Windows 7

• CDFS – CD / DVD de los sistemas de archivos (Próximamente)

• MAC – HFS (Próximamente)

• EXT2 – Linux (Próximamente)

• RAID – RAID JBOD, 0, 1, 5, hardware y software,

EJECUCION

Nos presenta la siguiente pantalla en la tenemos 2 opciones Recuperar archivos y recuperar unidad escogemos lo que necesitamos hacer, para este caso vamos a recuperar archivos de un dispositivo de almacenamiento:

Imagen No. 56: Ejecución Recovery My Files parte1

Elaborado por: Investigador

Imagen No. 57: Ejecución Recovery My Files parte2

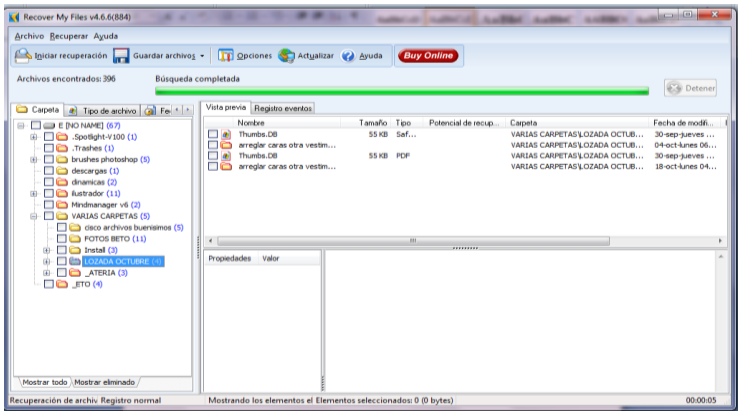
Elaborado por: Investigador

Escogemos la unidad en este caso lo haremos en una flash

Imagen No. 58: Ejecución Recovery My Files parte3

Elaborado por: Investigador

Imagen No. 59: Ejecución Recovery My Files parte4



Elaborado por: Investigador

GETDATABACK

Potente herramienta de recuperación de archivos, capaz de recuperar los datos perdidos tras una infección de virus, un fallo general del sistema, un problema grave con el disco duro o un simple borrado accidental.

Puede recuperar los archivos de un disco duro incluso aunque Windows no lo reconozca como unidad, o se haya perdido toda la información de estructura de directorios.

Es fácil de usar, gracias a su sistema de recuperación dividido en cinco pasos que te va indicando qué hacer en cada momento. GetDataBack utiliza avanzados algoritmos para garantizar la recuperación total y correcta de archivos y directorios.

El programa viene en dos versiones, una para sistemas de archivos FAT y otra para sistemas NTFS, y también permite recuperar unidades a través de red local o con un cable serie.

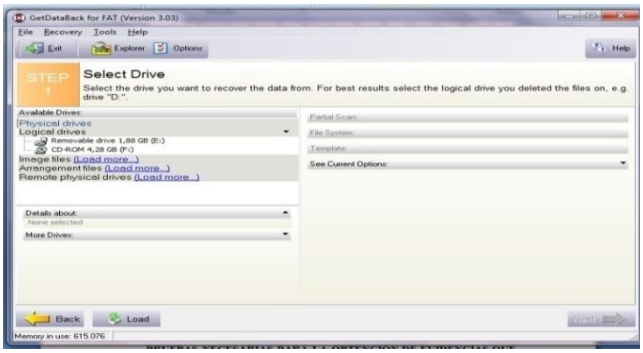
EJECUCION

Imagen No. 60: Ejecución Get Data Back parte1

Elaborado por: Investigador

Escogemos la opción a recuperar archivos borrados. Ubicamos la unidad a recuperar

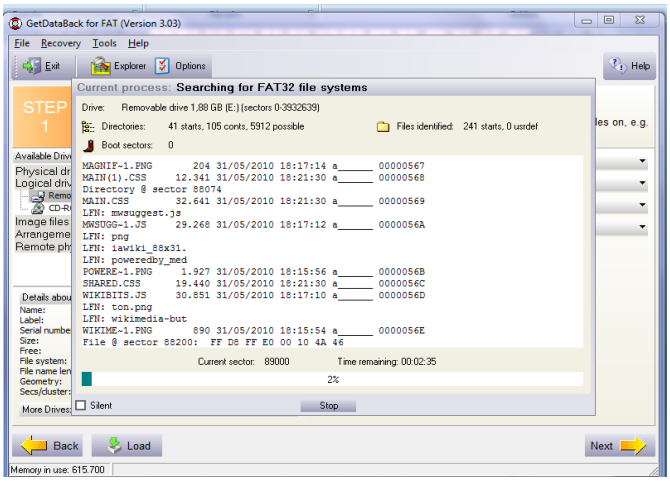
Imagen No. 61: Ejecución Get Data Back parte2



Elaborado por: Investigador

Escaneamos o inicia el proceso

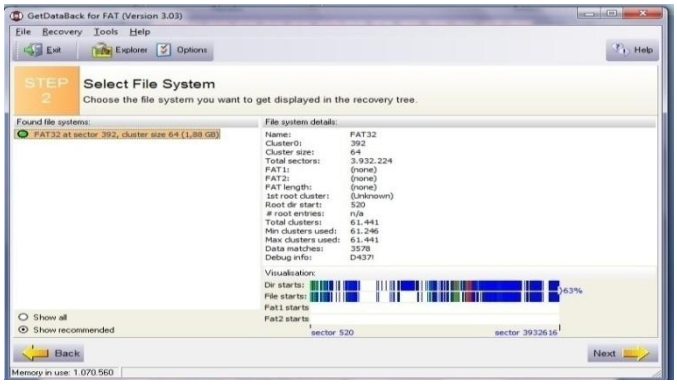
Imagen No. 62: Ejecución Get Data Back parte3



Elaborado por: Investigador

Recomendado

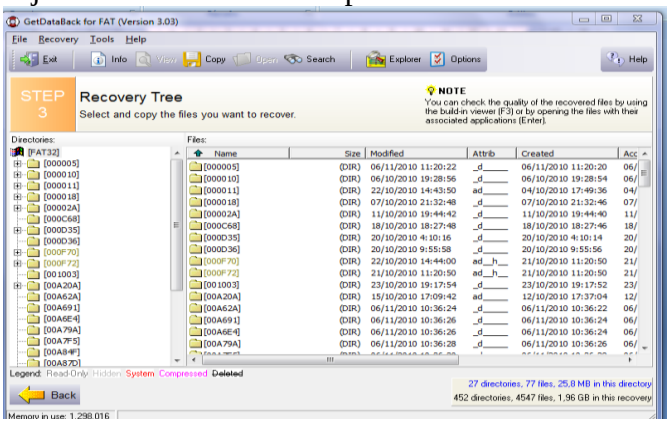
Imagen No. 63: Ejecución Get Data Back parte4



Elaborado por: Investigador

Nos despliega los archivos recuperados

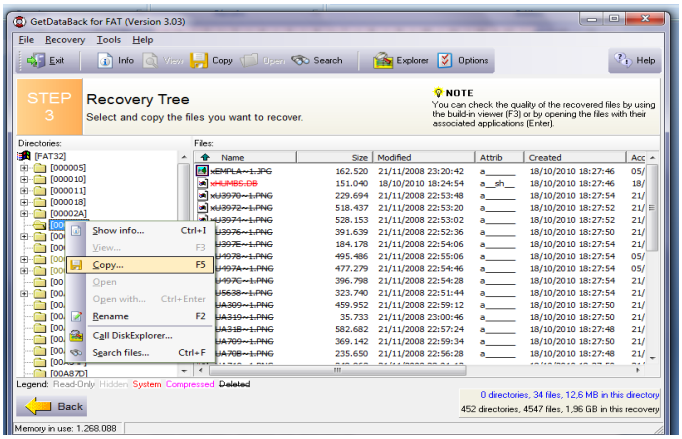
Imagen No. 64: Ejecución Get Data Back parte5



Elaborado por: Investigador

Escogemos copiar y grabamos el destino a copiar

Imagen No. 65: Ejecución Get Data Back parte6



Elaborado por: Investigador

Imágenes recuperadas al 100%

RESCUEPRO DELUX V4

Herramienta para recuperar las imágenes borradas accidentalmente, las imágenes digitales perdidas o los datos de cualquier tarjeta de memoria SanDisk; RescuePro recupera documentos de imágenes, correo, vídeos, música en su mayoría.

Con modernos algoritmos de recuperación de medios, RescuePro muestra pre visualizaciones de los datos recuperables. También presenta un algoritmo de recuperación único en el mundo para recuperación de audio MPEG y de vídeo MPEG (MPEG-1/2/3).

Todo lo que vea y escuche podrá recuperarlo.

RescuePro funciona con la mayoría de adaptadores USB, FireWire o FlashPath, y puede recuperar datos de dispositivos Palm Pilots, Windows CE, cámaras digitales, videocámaras digitales y reproductores de MP3. Es compatible con Windows y Macintosh, y no necesita descargas de controlador ni lectores de tarjeta especiales.

EJECUCION

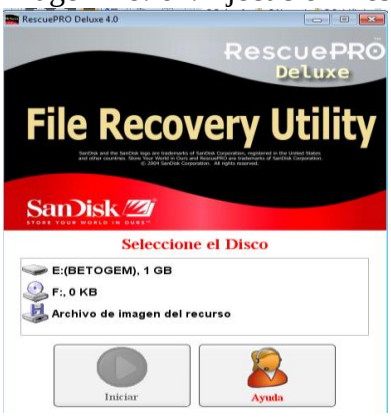
Imagen No. 66: Ejecución RescuePro parte1

Elaborado por: Investigador

Ejecutamos el programa y para este caso insertamos las memorias como compact flash, memory stick, sd , etc, en un lector de memorias conectado al computador , hoy en día los lectores de tarjeta reemplazan a la disquetera que ya está obsoleta. Podríamos hacerlo a una flash u otro dispositivo extraíble.

Escogemos la opción

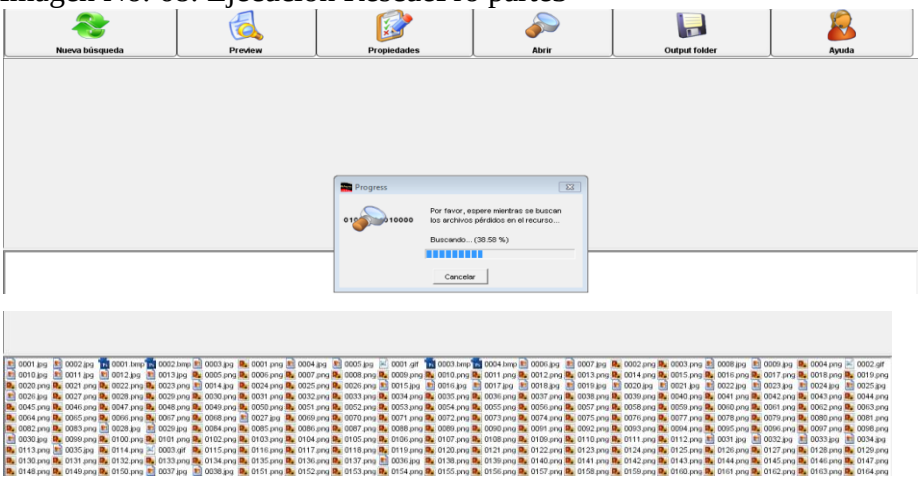
Imagen No. 67: Ejecución RescuePro parte2



Elaborado por: Investigador

Seleccionamos la unidad extraíble a recuperar

Imagen No. 68: Ejecución RescuePro parte3



Elaborado por: Investigador

Aparecen los archivos recuperados a guardar

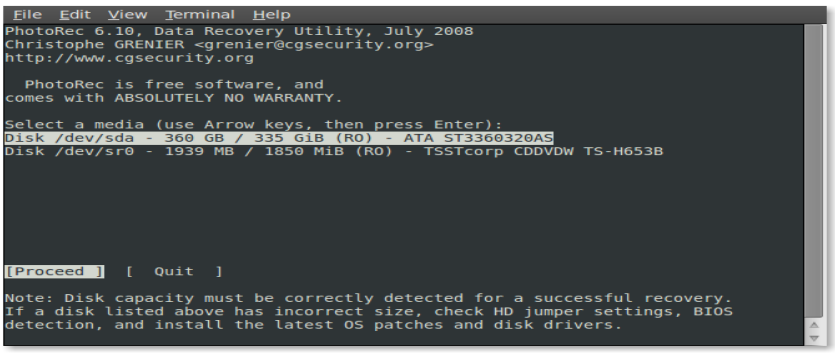
PHOTOREC

Photorec es un software creado para recuperar archivos incluyendo videos, imágenes y otro tipo de archivos que se hayan encontrado en el disco duro o en un cd/dvd.

EJECUCION

Una vez ejecutado en la terminal de Linux el programa nos presenta la siguiente pantalla para escoger el disco duro o la unidad a la que vamos a recuperarlo.

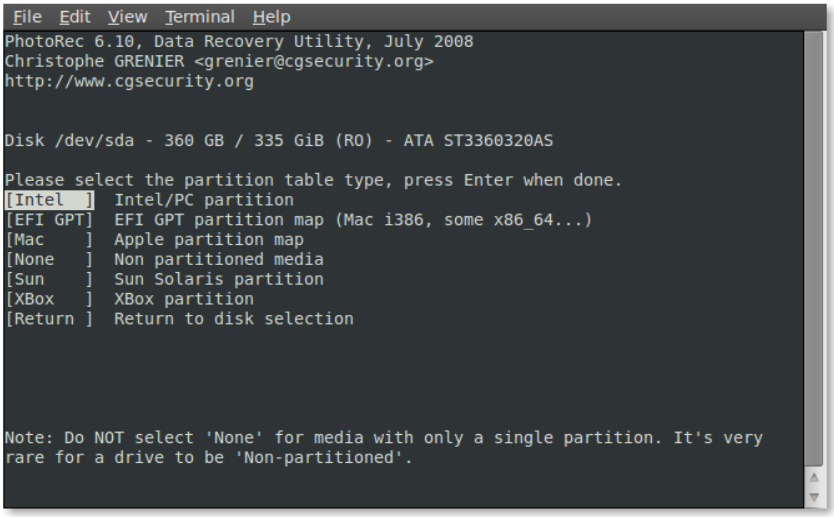
Imagen No. 69: Ejecución Photorec parte1



Elaborado por: Investigador

Escogemos el tipo de partición, en este caso de ejemplo será Intel y damos enter.

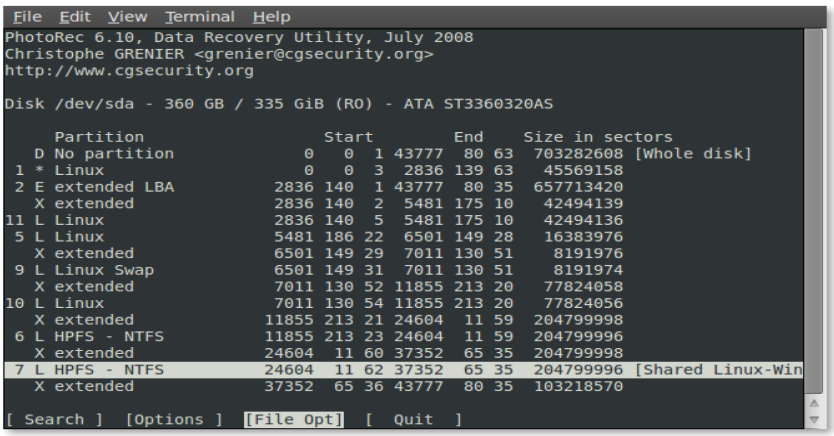
Imagen No. 70: Ejecución Photorec parte2



Elaborado por: Investigador

Escogemos la partición de donde hemos perdido el archivo, también podemos seleccionar la opción [File Opt] que sirve para seleccionar la extensión del archivo que vamos a recuperar.

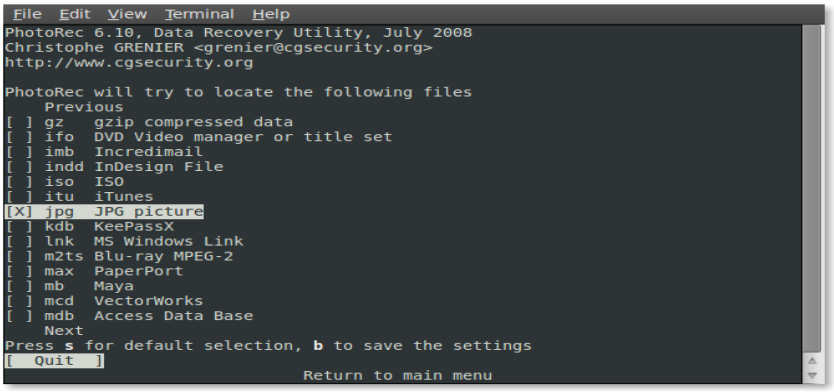
Imagen No. 71: Ejecución Photorec parte3



Elaborado por: Investigador

[File Opt] opciones.

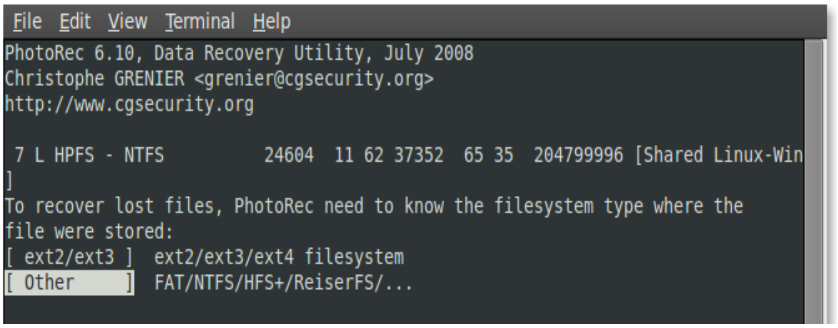
Imagen No. 72: Ejecución Photorec parte4



Elaborado por: Investigador

Ahora escogemos el tipo de archivos de sistema, en este caso será NTFS.

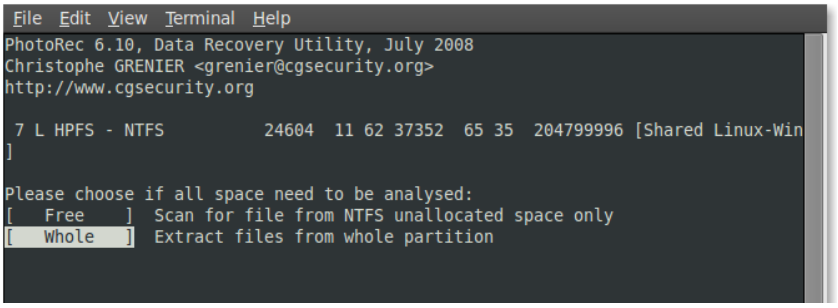
Imagen No. 73: Ejecución Photorec parte5



Elaborado por: Investigador

Grabamos en este caso será [Whole] que es en toda la partición.

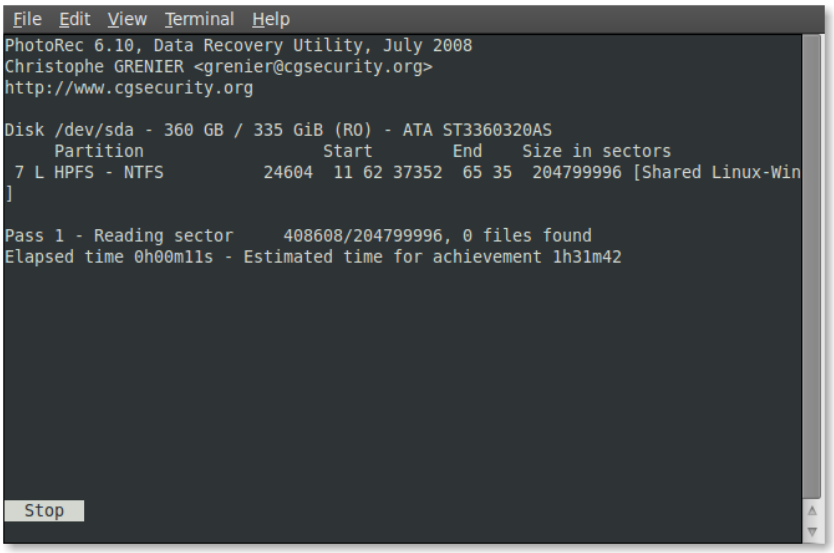
Imagen No. 74: Ejecución Photorec parte6



Elaborado por: Investigador

Este proceso demorara bastante tiempo, pero es algo muy valido cuando hemos perdido archivos importantes.

Imagen No. 75: Ejecución Photorec parte7



Elaborado por: Investigador

PC INSPECTOR`

Se trata de un programa capaz de recuperar archivos y rescatar datos perdidos en el disco duro o disquetes, de uso gratuito. Soporta los sistemas FAT 12 (disquetes), FAT 16, FAT 32 y también NTFS (NT, 2000, XP).

Reconstruye también los datos en los que no exista posible indicación del directorio a que pertenecen. Otros productos similares no son capaces de esta

reconstrucción. La "Función Especial de Recuperación" soporta los siguientes formatos de archivos:

ARJ AVI BMP CDR DOC DXF DBF XLS
EXE GIF HLP HTML HTM JPG LZH MID
MOV MP3 PDF PNG RTF TAR TIF WAV
ZIP

PC Inspector File Recovery 4.x es un producto FREEWARE, es decir este software es completamente gratuito.

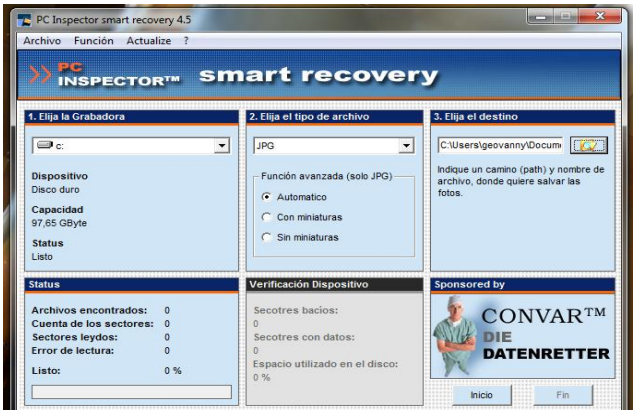
EJECUCION

Imagen No. 76: Pantalla principal PC Inspector

Elaborado por: Investigador

Nos presenta la siguiente pantalla en la que nos da una serie de opciones de:
Origen
Tipo de archivo a recuperar
Destino

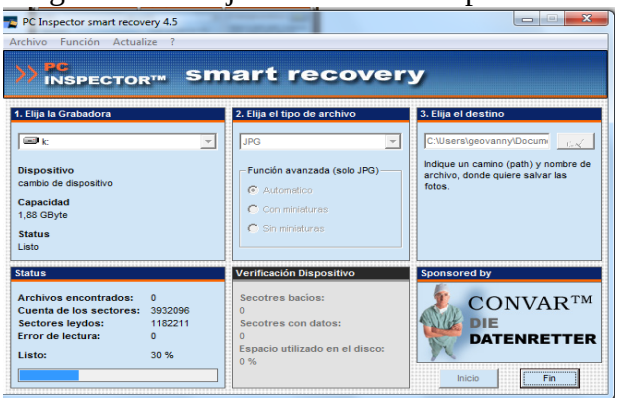
Imagen No. 77: Ejecución Photorec parte1



Elaborado por: Investigador

Ponemos Inicio este proceso durara varios minutos según el tamaño del disco

Imagen No. 78: Ejecución Photorec parte2



Elaborado por: Investigador

Luego ponemos finalizar y nos muestra las estadísticas resultantes de los sectores archivos encontrados, errores y demás.

DISK RECOVERY

O & O DiskRecovery es una herramienta de gran alcance para recuperar la información perdida. Escanea todos los sectores del disco duro, tarjeta de memoria o cámara digital para asignar la presencia de los archivos perdidos. Incluso si el sistema de archivos está dañado o formateado, se puede reconstruir los datos que se extraían.

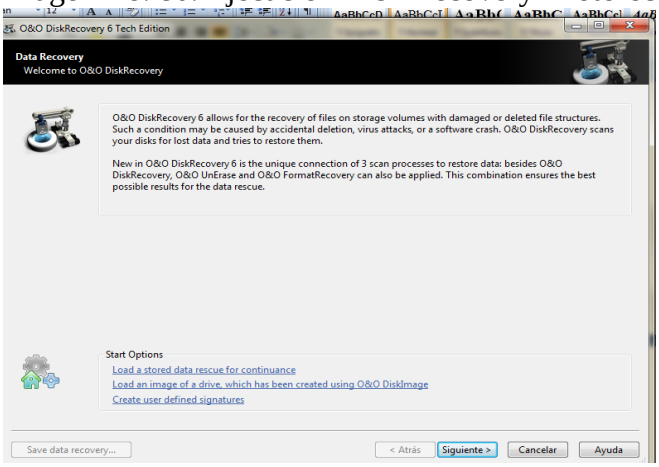
EJECUCION

Imagen No. 79: Ejecución Disk Recovery Photorec parte1

Elaborado por: Investigador

Siguiente

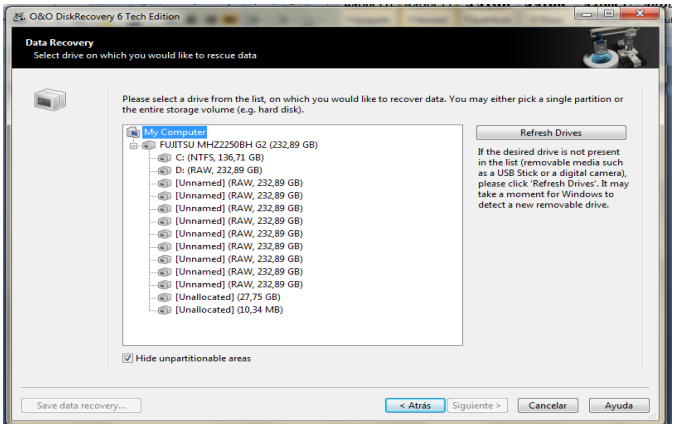
Imagen No. 80: Ejecución Disk Recovery Photorec parte2



Elaborado por: Investigador

Aquí debemos ubicar el drive a recuperar sus datos

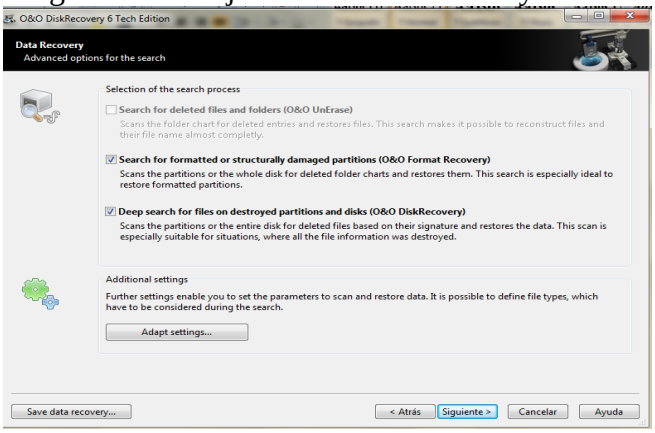
Imagen No. 81: Ejecución Disk Recovery Photorec parte3



Elaborado por: Investigador

Escanea las particiones o unidades de disco duro

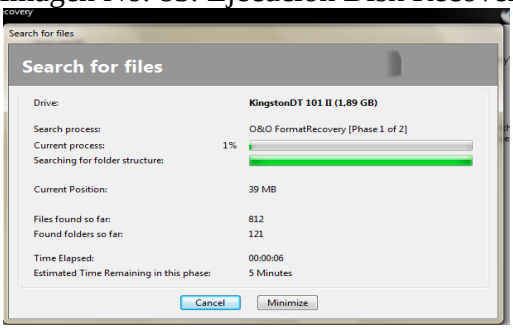
Imagen No. 82: Ejecución Disk Recovery Photorec parte4



Elaborado por: Investigador

Proceso en marcha durar algunos minutos de acuerdo al tamaño del disco

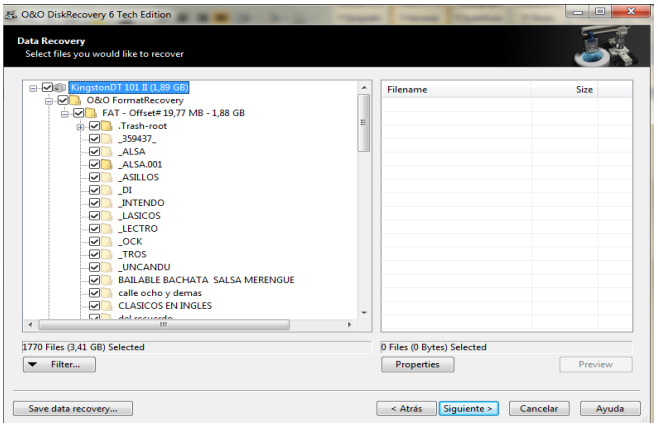
Imagen No. 83: Ejecución Disk Recovery Photorec parte5



Elaborado por: Investigador

En este paso guardamos las carpetas recuperadas

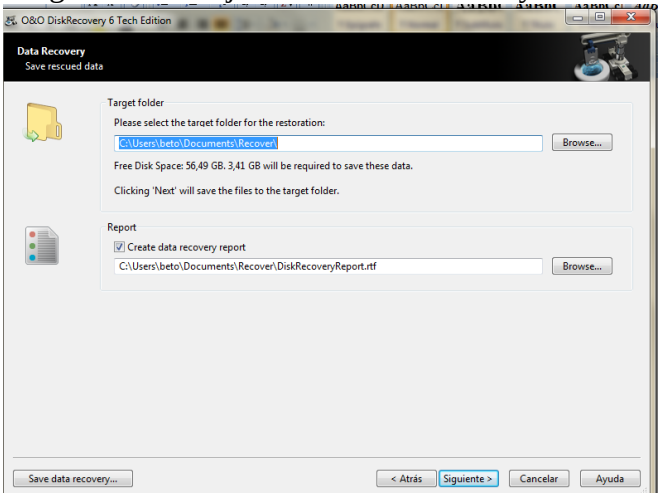
Imagen No. 84: Ejecución Disk Recovery Photorec parte6



Elaborado por: Investigador

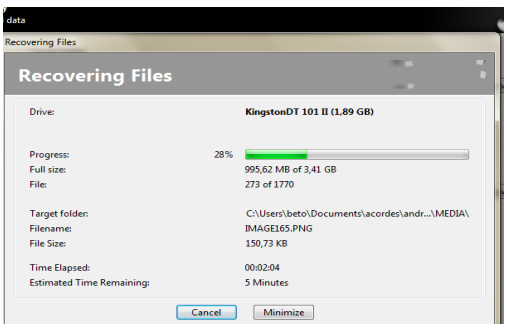
Ubicación para guardar los datos

Imagen No. 85: Ejecución Disk Recovery Photorec parte7



Elaborado por: Investigador

Imagen No. 86: Ejecución Disk Recovery Photorec parte8
Progreso



Elaborado por: Investigador

FOREMOST

Herramienta recuperadora de archivos: avi, mp3, gimp-xcf, jpg, png, doc, odt, etc, esta herramienta analiza una imagen de disco buscando todo tipo de archivo y recuperándolo.

EJECUCION

Instalamos

Descomprimir el archivo por ejemplo Foremost.tar

Posterior a esto, ubicarse dentro de la carpeta usando el comando CD.

Escribir ./configure

Make

Make install

foremost -t doc -o /tmp/recuperado -i /home/usuario/apuntes

-Con la opción -t indicamos el tipo de archivo a buscar.

-Con la opcion -o indicamos el lugar donde almacenar los archivos recuperados.

- Con la opción -i indicamos el lugar a escanear

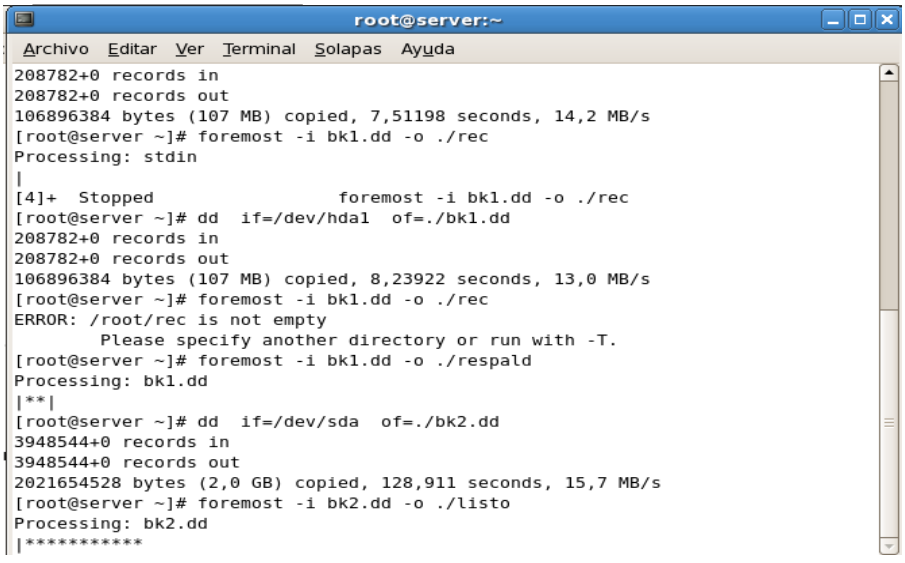
Recuperacion Desde Una Imagen

$ foremost -i bk1.dd -o ./respald

Donde -i indica el archivo de entrada y

-o el directorio donde se van a guardar los archivos recuperados y un reporte de auditoria

Imagen No. 87: Ejecución Foremost



SOFTWARE PARA TAREAS DE ANÁLISIS FORENSE

Elaborado por: Investigador

AUTOPSY CON SLEUTHKIT

Cuando se borran archivos con los métodos habituales (como el comando rm) a veces pueden recuperarse ya que lo que se borra realmente es el inodo (la tabla de asignación de archivos). El ordenador simplemente marca el espacio como sin uso, permaneciendo el contenido del archivo en el disco hasta que sea sobrescrito por otros archivos.

Veamos cómo recuperar datos 'borrados'. Lo más normal cuando un disco duro falla es que tenga sectores dañados o corruptos en los que no se puede leer ni escribir. Para recuperar los datos lo mejor es hacerlo en dos pasos:

1. primero copiamos la unidad dañada en otro disco:
2. `# dd if=/dev/old_disk of=/home/recovery.img conv=noerror`
   `# mount -t ntfs -o loop /home/recovery.img /home/recover_src`

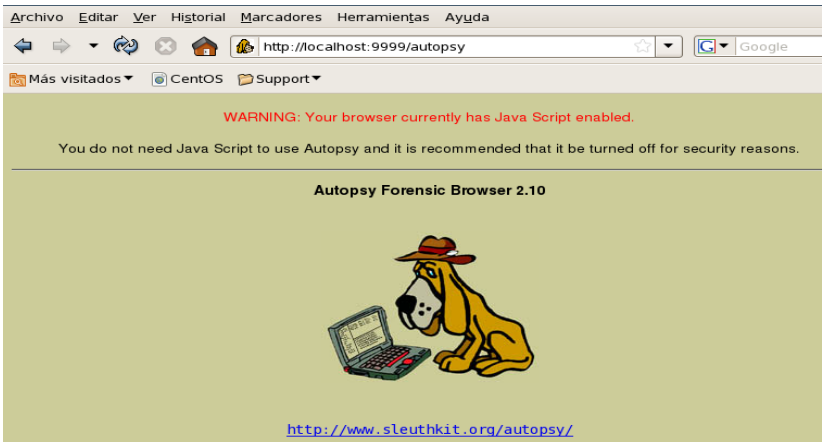
3. después intentaremos recuperar los datos con alguna herramienta de recuperación de datos.

The Sleuth Kit (sleuthkit.org, *paquete* sleuthkit*):* herramientas para la línea de comandos que permiten examinar filesystems y recuperar archivos perdidos. Se utiliza normalmente con **Autopsy** *(*paquete autopsy), un frontal con interfaz web que incorpora un servidor web al que se accede en la dirección http://localhost:9999/autopsy.

EJECUCION

Nos aparece la pantalla de ejecución del Proceso Autopsy

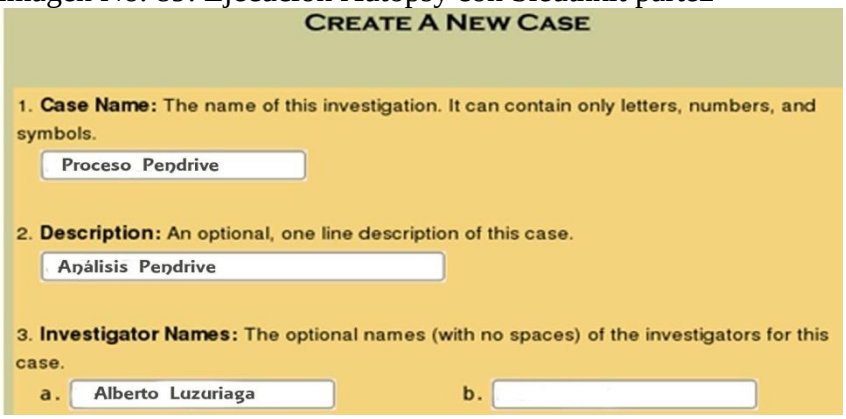
Imagen No. 88: Ejecución Autopsy con Sleuthkit parte1



Elaborado por: Investigador

A continuación creamos un nuevo caso que seria para este el de los datos perdidos de un pendrive

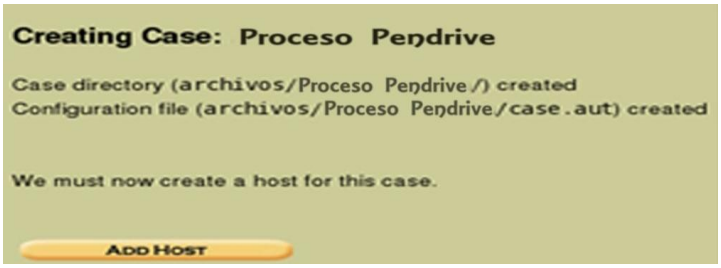
Imagen No. 89: Ejecución Autopsy con Sleuthkit parte2



Elaborado por: Investigador

Adicionamos un host, datos sobre el equipo afectado

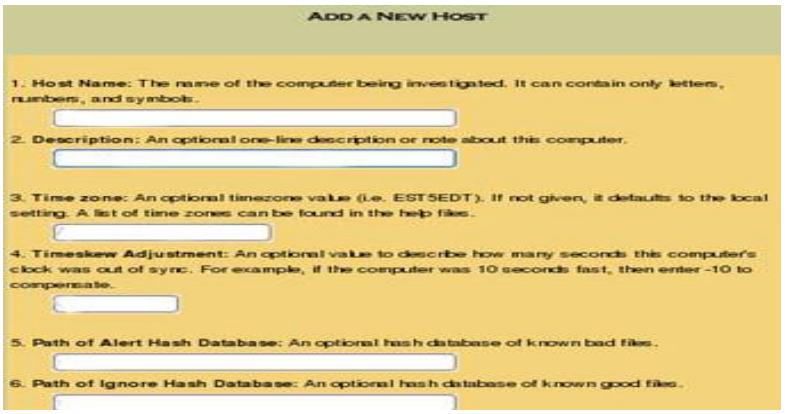
Imagen No. 90: Ejecución Autopsy con Sleuthkit parte3



Elaborado por: Investigador

Ingresamos los datos

Imagen No. 91: Ejecución Autopsy con Sleuthkit parte4



Elaborado por: Investigador

HELIX (LIVE CD HERRAMIENTAS PARA ANALISIS FORENSE)

Helix es una medicina forense y de respuesta a incidentes de CD en vivo basado en la distribución de Knoppix. Este a su vez contiene diversidad de herramientas útiles en un entorno Windows.

Los requisitos son mínimos como 128MB RAM y una arquitectura X86 Intel o AMD.

NO necesita instalarse Hélix prácticamente en un CD booteable solo se necesita lo siguiente:

- Descargar la imagen de CD desde http://www.e-fense.com/helix/downloads.php
- Grabar la imagen de CD (Helix.iso) a un CD.
- Asegúrese de que su máquina puede arrancar desde un CD. (Verificar la BIOS)

- Reinicie la máquina con el CD en la unidad de CD-ROM.

- Usar Hélix.

EJECUCION

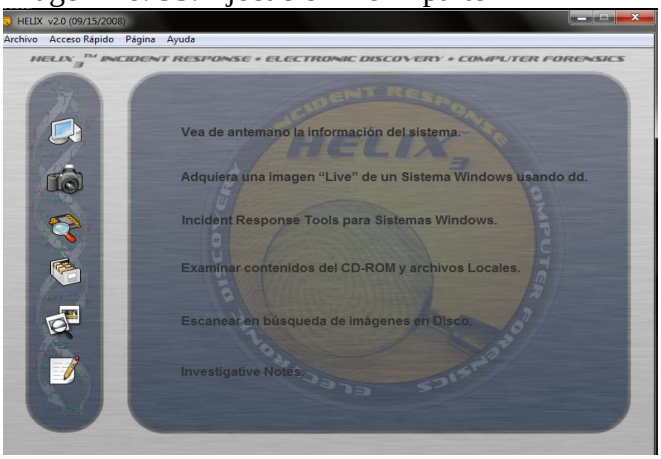
Seleccionamos el idioma

Imagen No. 92: Ejecución Helix parte1

Elaborado por: Investigador

Nos presenta una serie de opciones

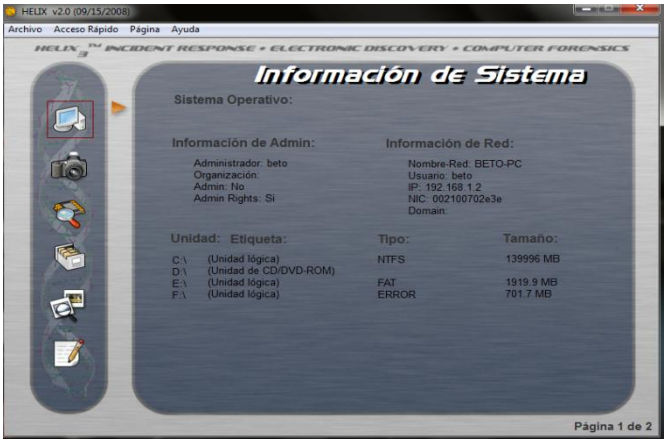
Imagen No. 93: Ejecución Helix parte2



Elaborado por: Investigador

Empezamos observando la información del sistema en la opción 1, nos despliega la información básica del equipo.

Imagen No. 94: Ejecución Helix parte3



Elaborado por: Investigador

En la siguiente opción vamos a encontrar distintas herramientas de creación de imágenes y nos despliega unidades de discos duros y extraíbles

Imagen No. 95: Ejecución Helix parte4

Elaborado por: Investigador

Ubicamos el destino de la imagen a guardar y listo

HERRAMIENTAS APLICADAS PARA ANALISIS FORENSE

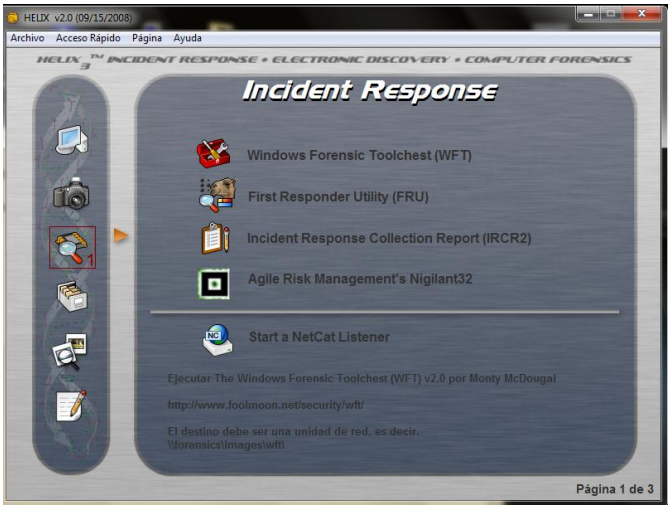
WINDOWS FORENSIC TOOLCHEST

Windows Toolchest forense (WFT) se diseña para proporcionar una respuesta forense automatizada estructurada y repetible, respuesta del incidente, o la intervención en un sistema de Windows mientras que recoge la información security-relevant del sistema. WFT es esencialmente una cápsula forense realzada del procesamiento por lotes capaz de funcionar con otras herramientas de la seguridad y de producir informes basados HTML.

Un profesional bien informado de la seguridad puede utilizar WFT para ayudar a buscar muestras de un incidente, intrusión, o a confirmar uso erróneo o la configuración de la computadora.

EJECUCION

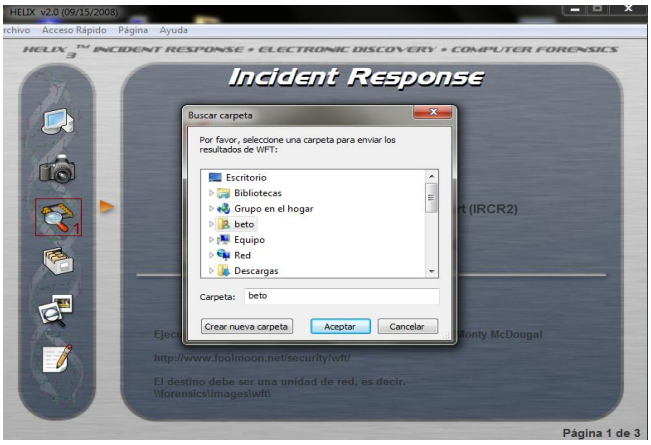
Imagen No. 96: Ejecución Windows Forensic Toolchest parte1



Elaborado por: Investigador

Seleccionamos la carpeta a donde a guardarse el WFT

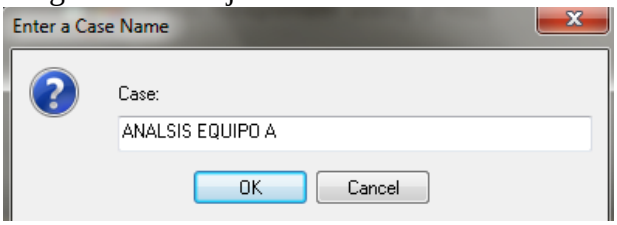
Imagen No. 97: Ejecución Windows Forensic Toolchest parte2



Elaborado por: Investigador

Luego nos pide el nombre del caso

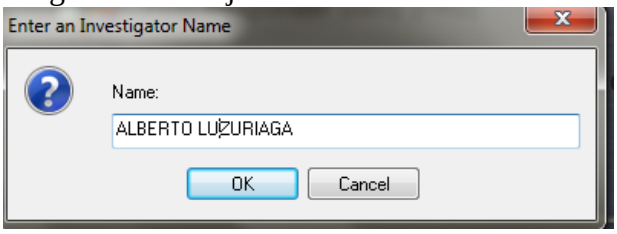
Imagen No. 98: Ejecución Windows Forensic Toolchest parte3



Elaborado por: Investigador

El nombre del Investigador

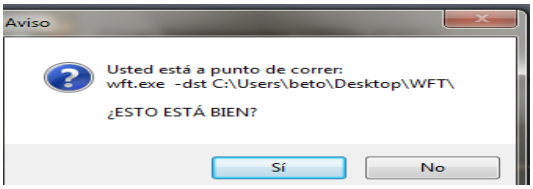
Imagen No. 99: Ejecución Windows Forensic Toolchest parte4



Elaborado por: Investigador

Pantalla de confirmación para realizar el proceso

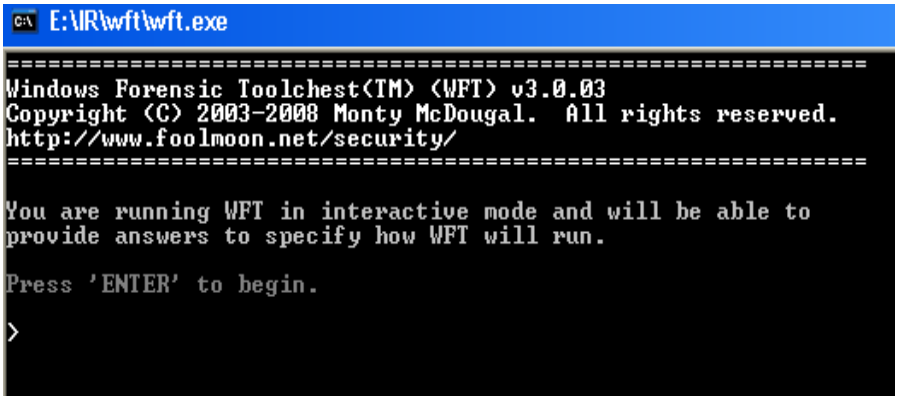
Imagen No. 100: Ejecución Windows Forensic Toolchest parte4



Elaborado por: Investigador

Ingresado los datos básicos que nos pide nos visualiza la siguiente pantalla:

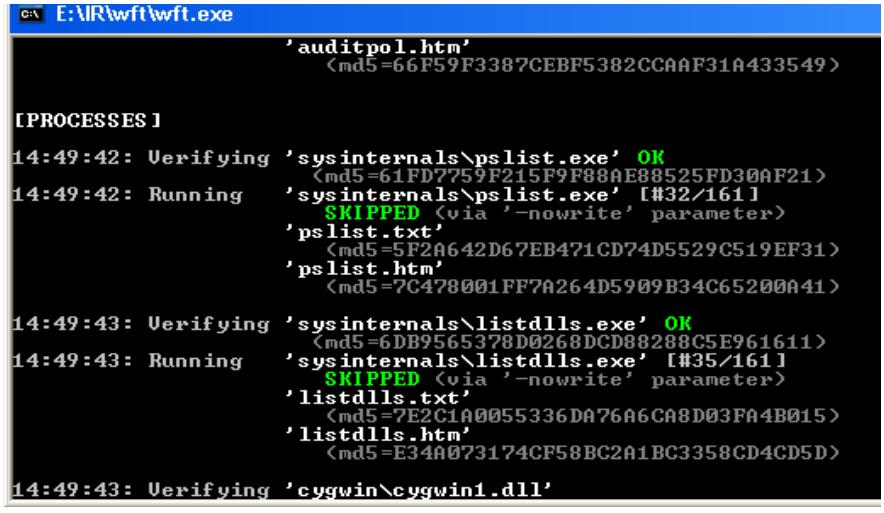
Imagen No. 101: Ejecución Windows Forensic Toolchest parte5



Elaborado por: Investigador

Proceso

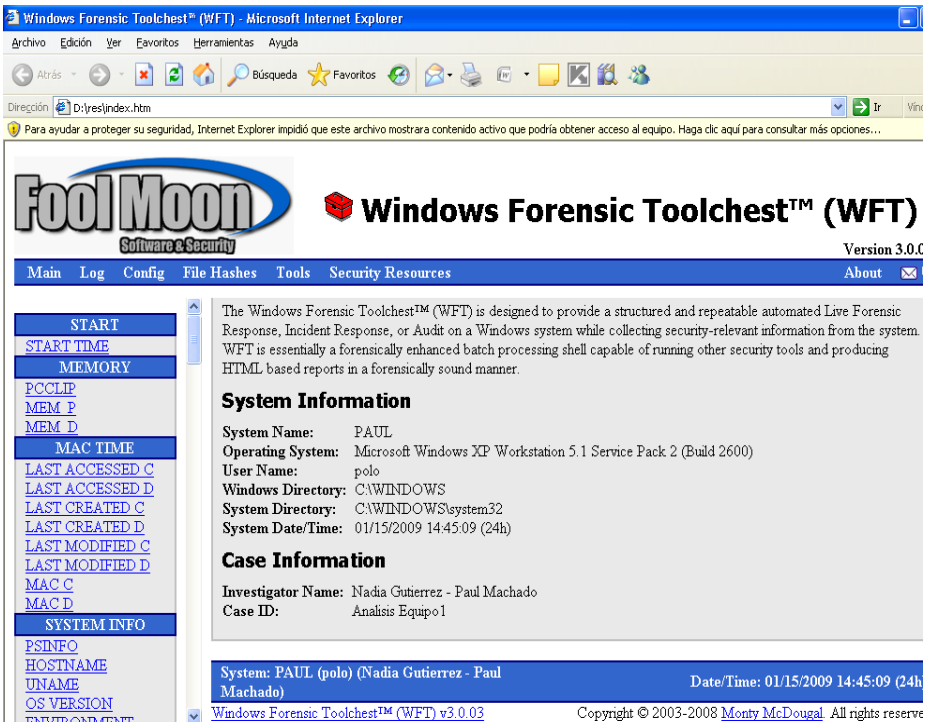
Imagen No. 102: Ejecución Windows Forensic Toolchest parte6



Elaborado por: Investigador

Herramienta se visualiza en HTML

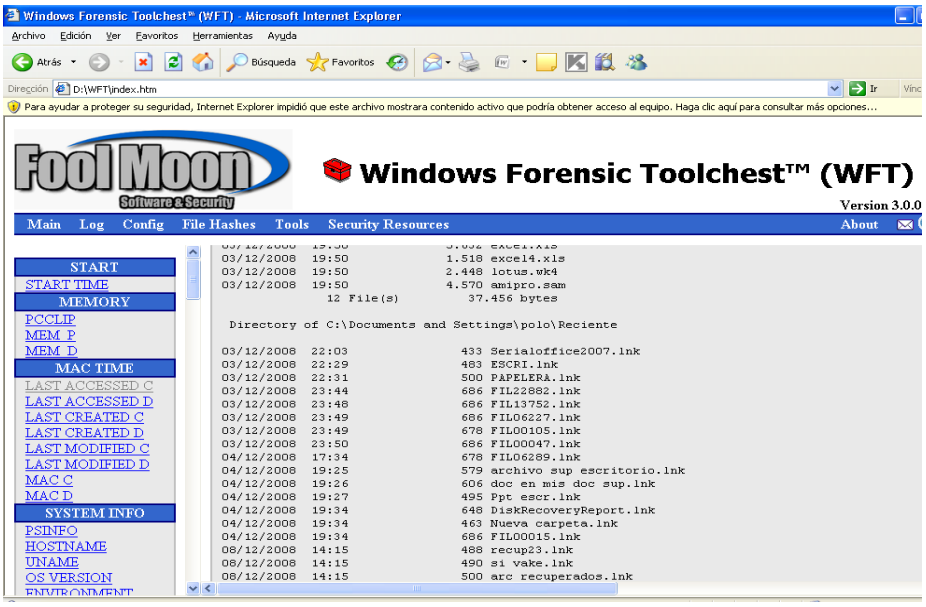
Imagen No. 103: Ejecución Windows Forensic Toolchest parte7



Elaborado por: Investigador

Archivos con último acceso al disco local C

Imagen No. 104: Ejecución Windows Forensic Toolchest parte8



Elaborado por: Investigador

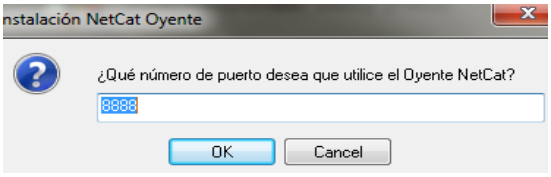
INCIDENT RESPONSE COLLECTION REPORT (IRCR2)

Servidor NetCat(oyente) ejecutamos en esta computadora y esperara información desde alguna computadora remota, se deberá escoger nuero de puerto a usar ejemplo origen - destino

EJECUCION

Puerto a utilizar

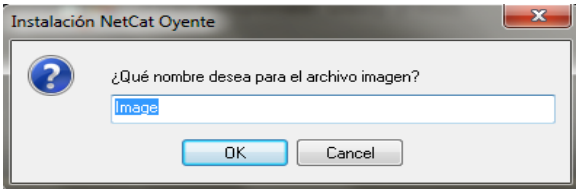
Imagen No. 105: Ejecución Incident Response Collection Report parte1



Elaborado por: Investigador

Nombre del archivo imagen

Imagen No. 106: Ejecución Incident Response Collection Report parte2



Elaborado por: Investigador

Ubicación a guardarse

Imagen No. 107: Ejecución Incident Response Collection Report parte3

Elaborado por: Investigador

Tamano en MB

Imagen No. 108: Ejecución Incident Response Collection Report parte4

Elaborado por: Investigador

Abrimos IRCR2, para que se ejecuten simultáneamente.

Luego nos presentará el reporte definitivo

AUDITORIA DE ARCHIVOS Y REGISTROS DEL SISTEMA

Dentro de lo que es la Auditoría informática debemos tener en cuenta la recopilación de varios sucesos realizados en el computador.

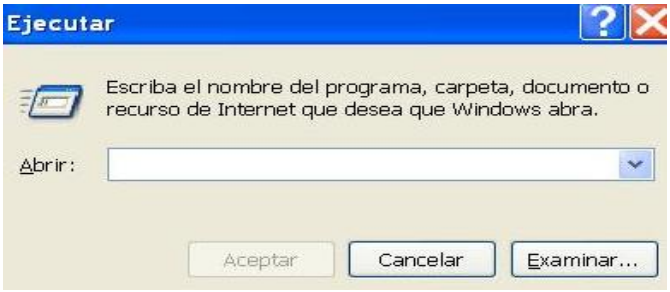
Registros y análisis de registros

Un registro es un archivo que almacena hechos en un orden cronológico, por ejemplo, el tráfico de una red. La información se almacena en el registro de forma automática. Los registros sirven, por ejemplo, para elaborar estadísticas sobre un servicio.

Para configurar las Directivas locales/Directivas de auditorías

- Vas a *Inicio / Ejecutar*, escribes el comando y haces clic en *Aceptar*

Imagen No. 109: Ejecución Auditoría de registros parte1



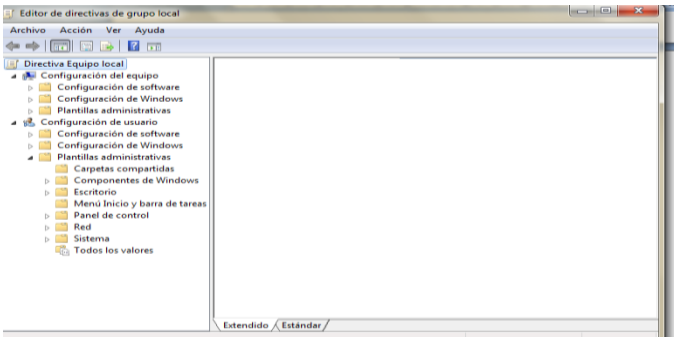
Elaborado por: Investigador

Ejecute en menú INICIO> Ejecutar: **GPEDIT.MSC**

Las directivas que se encuentren en la sección Configuración de usuario pueden encontrarse a nivel general o de equipo en la sección Configuración del equipo.

Algunas de las directivas que encontrará son:

Imagen No. 110: Ejecución Auditoría de registros parte2

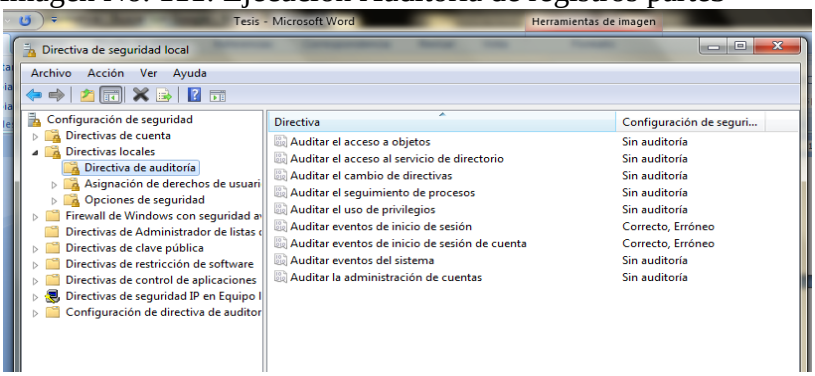


Elaborado por: Investigador

Ejecute en menú INICIO> Ejecutar: **SECPOL.MSC**

Encontraremos las directivas de auditoría en la que se encuentra la configuración por ejemplo auditoría de acceso a objetos, inicios de sesión, acceso l servicio de directorio, administración de cuentas, cambio de directivas, privilegios, entre otros.

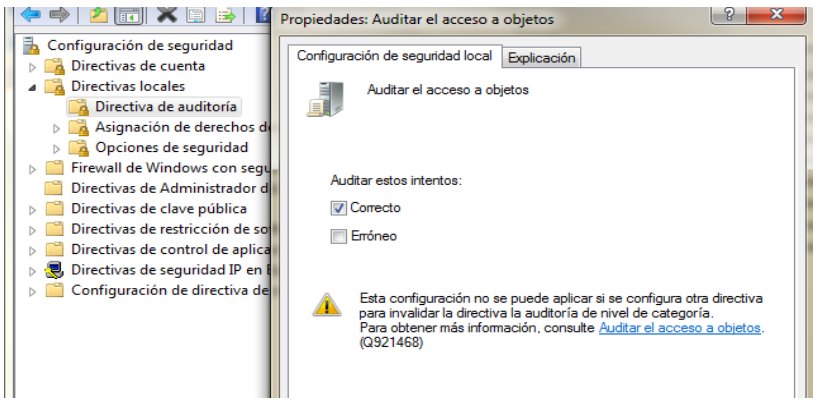
Imagen No. 111: Ejecución Auditoría de registros parte3



Elaborado por: Investigador

Para este caso vamos auditar el acceso a los objetos, damos doble click sobre auditar el acceso a los objetos y activamos correcto asi:

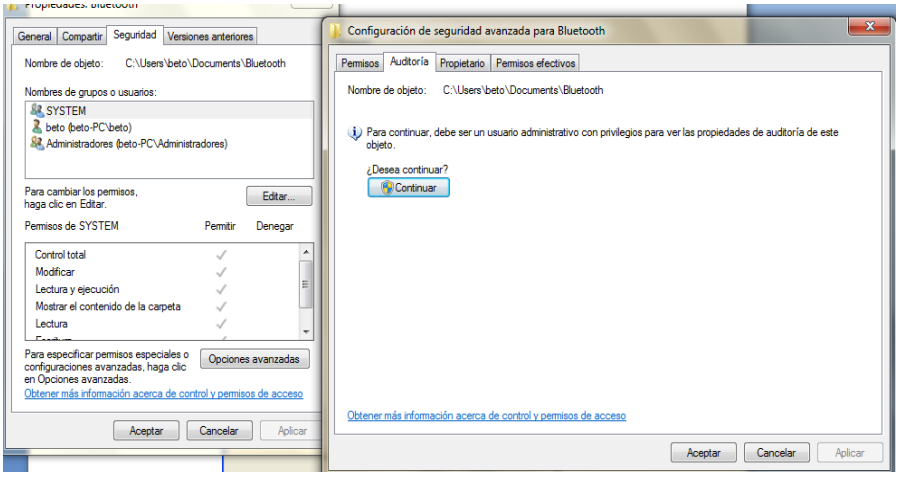
Imagen No. 112: Ejecución Auditoría de registros parte4



Elaborado por: Investigador

Para auditar una carpeta nos ubicamos en la que necesitamos, propiedades en la opción seguridad, opciones avanzadas y click en auditoría

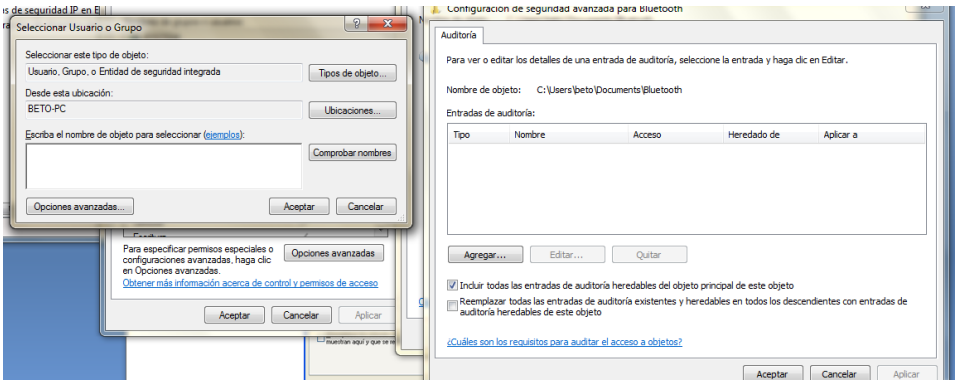
Imagen No. 113: Ejecución Auditoría de registros parte5



Elaborado por: Investigador

Configuramos la auditoría para un usuario o grupo nuevo Agregar. escriba el nombre del usuario o el grupo que desea

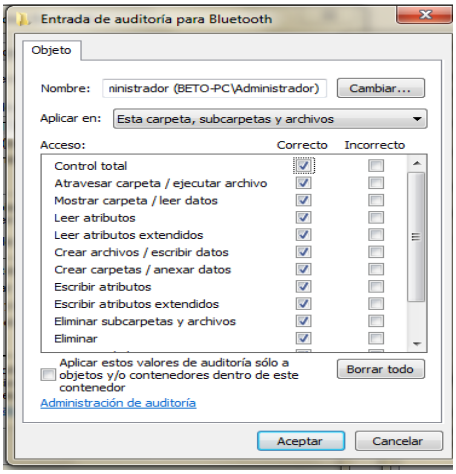
Imagen No. 114: Ejecución Auditoría de registros parte6



Elaborado por: Investigador

Entrada de auditoría para La carpeta a ser auditada si se necesita tener un control total activamos la casilla control total de no ser así marcamos la que necesitemos

Imagen No. 115: Ejecución Auditoría de registros parte7

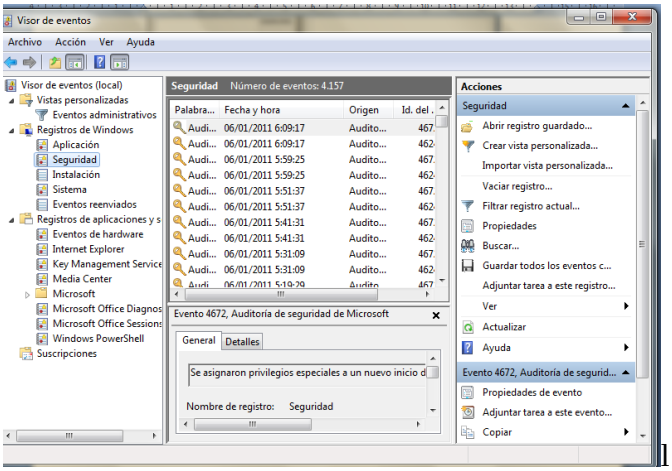


Elaborado por: Investigador

Si desea evitar que los archivos y las subcarpetas del árbol hereden estas entradas de auditoría, active la casilla de verificación derecho sobre Mi PC/Administrar/Herramientas de sistema/Visor de sucesos/Seguridad

Ejecutar Eventvwr.Msc

Imagen No. 116: Ejecución Auditoría de registros parte8



Elaborado por: Investigador

O en su defecto podemos borrar todos los sucesos

METRICAS: PRUEBAS CUADROS COMPARATIVOS DE INFORMACIÓN BAJO LAS PLATAFORMAS WINDOWS Y LINUX

SOFTWARE PARA CREACIÓN DE IMÁGENES LÓGICAS

CASO PRACTICO DE PRUEBA

La manera como preservar evidencias lo analizaremos a través de diferentes herramientas de computación forense para creación de imágenes de su sistema operativo tomando en cuenta dos puntos de vista muy importantes como son la facilidad de utilización y su Aplicación, para esto se utilizara discos duros con

características similares además de pruebas con conexiones en red para el análisis de las imágenes del sistema comprometido en otro equipo.

PARAMETROS PARA LA MATRIZ

Facilidad de utilización:

- Instalación
- Interfaz
- Facilidad de manejo de la herramienta

Aplicación:

- Permite copia de bit a bit
- Permite crear imagen rápida
- Permite trabajar en red
- Trabaja bajo plataforma Linux
- Trabaja bajo plataforma Windows

Tabla No. 16: Valores para los parámetros en la matriz (creación imágenes)

Valor	1	Difícil	Conocimientos Sólidos
Valor	2	Intermedio	Conocimientos básicos
Valor	3	Fácil	Intuición informática

Elaborado por: Investigador

Tabla No. 17: Cuadro de herramientas de análisis forense para la matriz (Creación de imágenes lógicas)

Software
Acronis true image

Genie Backup
Snapshot
DD

Elaborado por: Investigador

ANALISIS EN WINDOWS 7

Valoración

1	Difícil

2	Intermedio
3	Fácil

Tabla No. 18: Matriz 1 Facilidad de utilización (Plataforma Windows Creación de imágenes lógicas)

	PARAMETROS				
HERRAMIENTAS	INSTALACION	FAC.MANEJO	INTERFAZ	TOTAL	%
Acronis true image	3	2	3	8	88.88
Genie Backup	3	2	3	8	88.88
Snapshot	3	2	2	8	88.88

Elaborado por: Investigador

ANALISIS EN LINUX DISTRIBUCION CENTOS 5.3

Valoración

1	Difícil
2	Intermedio
3	Fácil

Tabla No. 19: Matriz 2 Facilidad de utilización (Plataforma Linux Creación de imágenes lógicas)

	PARAMETROS				
HERRAMIENTAS	INSTALACION	FAC.MANEJO	INTERFAZ	TOTAL	%
Acronis true image	3	2	3	8	88.88
Genie Backup	3	2	3	8	88.88
DD	2	1	2	5	55.55

Elaborado por: Investigador

ANALISIS EN WINDOWS 7 Y LINUX DISTRIBUCION CENTOS 5.3

Valoración

SI	✓
NO	X

Tabla No. 20: Matriz 3 Aplicación (Plataforma Windows & Linux Creación de imágenes lógicas)

	PARAMETROS					
HERRAMIENTAS	Permite copia de bit a bit	Permite crear imagen rápida	Permite trabajar en Red	Trabaja en Plataforma Windows	Trabaja en Plataforma Linux	%
Acronis true image	✓	✓	✓	✓	✓	100
Genie Backup	✓	X	✓	✓	X	60
DD	✓	✓	✓	✓	✓	100
Snapshot	✓	X	✓	✓	X	60

Elaborado por: Investigador

RESULTADOS HERRAMIENTAS SOFTWARE PARA CREACIÓN DE IMÁGENES LOGICAS Y RESTAURACION DE SISTEMA OPERATIVO

Como resultado tenemos que las herramientas más adecuadas para creación de imágenes lógicas de sistemas operativos son :

- Acronis True Image
- Herramienta DD

Se justifica por la manera de trabajar bajo las plataformas Windows y Linux, considerándolas así las más recomendadas. La aplicación que se la ha realizado nos ha dado como resultante de un 100%, además de permitirnos ejecutarlas con imágenes en las que se puede realizar copias sector por sector, es decir de bit a bit muy importante al momento de realizar tareas de análisis forense.

SOFTWARE PARA RECUPERACIÓN DE DATOS – RESTAURACIÓN DE ARCHIVOS (PENDRIVE, DISCOS DUROS, PAPELERA DE RECICLAJE, MEMORIAS)

CASO PRACTICO DE PRUEBA

En este caso se realiza puntos importantes como la recuperación de datos luego de un formateo de un dispositivo de almacenamiento, restauración de archivos borrados, para esto hemos de trabajar con un total de 10 archivos los mismos que nos presentarán un resultado de acuerdo al volumen recuperado

PARAMETROS PARA LA MATRIZ

Facilidad de utilización:

- Instalación
- Interfaz
- Facilidad de manejo de la herramienta
- Ubicación a recuperar

Tipo de Software:

- Libre distribución
- Pagado
- Trial

Aplicación y Recuperación:

- De archivos borrados de papelera de reciclaje
- Luego de Formateo de discos
- De diferentes tipos de archivos según volumen de información
- Recupera de discos con fallos físicos

Tabla No. 21: Valores para los parámetros en la matriz (Recuperación)

Valor	1	Difícil	Conocimientos Sólidos
Valor	2	Intermedio	Conocimientos básicos

Valor	3	Fácil	Intuición informática

Elaborado por: Investigador

Tabla No. 22: Cuadro de herramientas de análisis forense para la matriz (Recuperación de datos de Discos Duros, Pendrive, Memorias)

Software
Easy Recovery
Recovery My Files
GetDataBack
RescuePro Delux v4
Photorec
Pc Inspector
Disk Recovery
Foremost

Elaborado por: Investigador

ANALISIS EN WINDOWS 7

Tabla No. 23: Matriz 4. Volumen de Información (Plataforma Windows Recuperación de datos)

	PARAMETROS			
HERRAMIENTAS	UBICACIÓN	VOLUMEN ARCHIVOS A RECUPERAR	VOLUMEN ARCHIVOS RECUPERADO	TOTAL %
Easy Recovery	Otros	10	8	80 %
	Papelera Reciclaje	10	6	60%
	Pendrive	10	10	100%
Recovery My Files	Otros	10	8	80%
	Papelera Reciclaje	10	8	80%
	Pendrive	10	10	100%
GetDataBack	Otros	10	10	100%
	Papelera Reciclaje	10	10	100%
	Pendrive	10	10	100%

RescuePro Delux v4	Otros	10	4	40%
	Papelera Reciclaje	10	0	-
	Pendrive	10	6	60%
Pc Inspector	Otros	10	10	100%
	Papelera Reciclaje	10	10	100%
	Pendrive	10	10	100%
Disk Recovery	Otros	10	2	20%
	Papelera Reciclaje	10	1	10%
	Pendrive	10	5	50%

Elaborado por: Investigador

ANALISIS EN LINUX DISTRIBUCION CENTOS 5.3

Tabla No. 24: Matriz 5. Volumen de Información (Plataforma Linux Recuperación de datos)

	PARAMETROS			
HERRAMIENTAS	UBICACIÓN	VOLUMEN ARCHIVOS A RECUPERAR	VOLUMEN ARCHIVOS RECUPERADO	TOTAL %
Foremost	Otros	10	7	70%
	Papelera Reciclaje	10	8	80%
	Pendrive	10	10	100%
Photorec	Otros	10	6	60%
	Papelera Reciclaje	10	8	80%
	Pendrive	10	10	100%

Elaborado por: Investigador

ANALISIS EN WINDOWS 7

Valoración

1	Difícil
2	Intermedio
3	Fácil

Tabla No. 25: Matriz 6. Facilidad de utilización (Plataforma Windows Recuperación de datos)

	PARAMETROS				
HERRAMIENTAS	INSTALACION	FAC.MANEJO	INTERFAZ	TOTAL	%
Easy Recovery	3	2	3	8	80.88
Recovery My Files	3	2	3	8	80.88
GetDataBack	3	2	3	8	80.88
RescuePro Delux v4	3	3	3	9	90

Pc Inspector	3	2	3	8	90
Disk Recovery	3	2	3	8	90

Elaborado por: Investigador

ANALISIS EN LINUX DISTRIBUCION CENTOS 5.3

Valoración

1	Difícil
2	Intermedio
3	Fácil

Tabla No. 26: Matriz 7. Facilidad de utilización (Plataforma Linux Recuperación de datos)

	PARAMETROS				
HERRAMIENTAS	INSTALACION	FAC.MANEJO	INTERFAZ	TOTAL	%
Foremost	1	1	2	4	44.44

Photorec	1	1	2	4	44.44

Elaborado por: Investigador

ANALISIS EN WINDOWS 7

Valoración

SI	✓
NO	X

Tabla No. 27: Matriz 8 Aplicación (Plataforma Windows Recuper de datos)

	PARAMETROS						
HERRA MIENTAS	Recuperación de Archivos borrados	Recuperación discos formateados	Recupera de discos con fallos físicos	Recupera archivos de la papelera	Muestra características físicas del disco duro	Recupera diferentes tipos de archivos según vol.de información	%

Easy Recovery	✓	✓	✓	✓	X	X	66.7%
Recovery My Files	✓	✓	✓	✓	X	X	66.7%
GetData Back	✓	✓	✓	✓	X	X	66.7%
RescuePro Delux v4	✓	X	X	X	X	X	16.7%
Pc Inspector	✓	✓	✓	✓	X	X	66.7%
Disk Recovery	✓	✓	X	X	✓	X	50%

Elaborado por: Investigador

ANALISIS EN LINUX DISTRIBUCION CENTOS 5.3

Valoración

SI	✓
NO	X

Tabla No. 28: Matriz 9 Aplicación (Plataforma LINUX Recuperación de datos)

	PARAMETROS							
HERRAMIENTAS	Recuperación de Archivos borrados	Recuperación discos formateados	Recupera de discos con fallos físicos	Recupera archivos de la papelera	Muestra características físicas del disco duro	Recupera diferentes tipos de archivos según vol.de información	Informe de tareas ejecutadas	%

Foremost	✓	✓	✓	✓	X	X	✓	71
Photorec	✓	✓	✓	✓	✓	X	✓	85

Elaborado por: Investigador

RESULTADOS HERRAMIENTAS SOFTWARE PARA RECUPERACIÓN DE DATOS – RESTAURACIÓN DE ARCHIVOS (PENDRIVE, DISCOS DUROS, PAPELERA DE RECICLAJE, MEMORIAS)

Como resultado tenemos que las herramientas más adecuadas para recuperación de información son :

- Get Data Back
- Recovery My Files

Easy recovery tiene de la misma manera una utilidad parecida a la de Recovery My Files

RescuePro nos ayudará a recuperar en un buen porcentaje archivos de imagen ya que trabaja específicamente para tarjetas de memoria como XD, SD, Memory Stick, entre otras.

Foremost.- Se justifica por la manera de trabajar bajo las plataforma Linux considerándolas así las más recomendadas ya que mantiene un buen nivel de volumen de recuperación

Nota.- Cabe indicar que existen herramientas que al momento de recuperar la información perdida mantienen un límite de volumen de información.

SOFTWARE PARA TAREAS DE ANALSIS FORENSE

CASO PRÁCTICO DE PRUEBA

En este caso se analizó un sistema utilizando herramientas necesarias como un CD Live Helix , además de imágenes de un disco duro, pendrive, para el mismo.

PARAMETROS PARA LA MATRIZ

Facilidad de utilización:

- Instalación
- Interfaz
- Facilidad de manejo de la herramienta

Aplicación:

- Permite recuperación de archivos eliminados intencionadamente o casual
- Permite crear informe de tareas realizadas

- Especifica 4W Que?, Cómo?, Quién?
- Trabaja bajo plataforma Linux
- Trabaja bajo plataforma Windows

Tabla No. 29: Valores para los parámetros en la matriz (Tareas de análisis forense)

Valor	1	Difícil	Conocimientos Sólidos
Valor	2	Intermedio	Conocimientos básicos
Valor	3	Fácil	Intuición informática

Elaborado por: Investigador

Tabla No. 30: Herramientas Tareas de análisis forense

Software
Autopsy con Sleuthkit
Windows Forensic Toolchest (WFT)
Helix
Incident Response Collection Report (IRCR2)

Auditoría de Registros

Elaborado por: Investigador

ANALISIS EN WINDOWS 7 Y LINUX DISTRIBUCION CENTOS 5.3

Valoración

1	Difícil
2	Intermedio
3	Fácil

Tabla No. 31: Matriz 10. Facilidad de utilización (Plataforma Windows y Linux - Tareas de Análisis Forense)

PARAMETROS

HERRAMIENTAS	TIPO INSTALACION	INSTALACION	FAC.MANEJO	INTERFAZ	TOTAL	%
Autopsy con Sleuthkit	Instalación Manual	2	1	2	5	55.55
	Helix Live Cd	2	2	3	7	77.77
Incident Response Collection Report (IRCR2)	Helix Live Cd	2	2	2	6	66.66
Windows Forensic Toolchest (WFT)	Helix Live Cd	2	2	3	7	77.77

Elaborado por: Investigador

ANALISIS EN WINDOWS 7 Y LINUX DISTRIBUCION CENTOS 5.3

Valoración

SI	✓
NO	X

Tabla No. 32: Matriz 11. Aplicación (Plataforma Windows & Linux Tareas de Análisis forense)

	PARAMETROS					
HERRAMIENTAS	Permite recuperación de archivos eliminados intencionadamente o casual	Permite crear informe de tareas realizadas	Permite 4W	Permite trabajar con Windows	Permite trabajar con Linux	Total %
Autopsy con Sleuthkit	✓	✓	✓	✓	✓	100%
Incident Response Collection Report (IRCR2)	X	✓	X	✓	X	40%
Windows Forensic Toolchest (WFT)	X	✓	X	✓	X	40%

Elaborado por: Investigador

RESULTADOS HERRAMIENTAS DE ANÁLISIS FORENSE

Como resultado tenemos que las herramientas más adecuadas para tareas de análisis forense son :

- Autopsy
- CD Live Helix

Se justifica por la manera de que la Herramienta Autopsy trabaja bajo las plataformas de Windows y Linux, además de su aplicación para informática forense

El conjunto de herramientas que posee un cd live como Helix para este caso estudiado nos da varias ventajas debido a que el cd es booteable y trabaja como un sistema muy independiente en el que se puede trabajar de manera segura en sistema sospechoso.

PROCEDIMIENTOS Y METODOLOGIAS PARA REALIZAR UN ANALISIS FORENSE

ANÁLISIS PRELIMINAR

Principios Considerados en la ley Ecuatoriana

A continuación se describen brevemente algunos de los artículos de la Ley Ecuatoriana sobre Infracciones Informáticas. Para más detalle referirse al **ANEXO B** LEY DE COMERCIO ELECTRÓNICO

Según : (http://www.icm.espol.edu.ec/materias/icm01438/archivos.htm)

Artículo 57.- Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente Ley.

Reformas al Código Penal Artículo 58.- A continuación del Art. 202, inclúyanse los siguientes artículos enumerados: El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Sobre la Falsificación electrónica.- Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio, alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático

FASES DEL ANÁLISIS FORENSE

1. ADQUISICION DE LA EVIDENCIA
2. IDENTIFICACIÓN DE LA EVIDENCIA
3. PRESERVACIÓN DE LA EVIDENCIA

4. RECOLECCION
4. ANÁLISIS
5. INFORME

DESARROLLO:

1. ADQUISICION DE LA EVIDENCIA

Autorización Legal
Autoridad e Investigador responsable
Normas Legales a seguir
Preparación y Aseguramiento de la escena
Herramientas básicas a utilizar

2. IDENTIFICACIÓN DE LA EVIDENCIA

Describe el método por el cual el investigador es notificado sobre un posible incidente. Además en este punto se identifican los equipos afectados, información que ha sido alterada, etc.

3. PRESERVACIÓN DE LA EVIDENCIA

Mecanismos utilizados para el correcto mantenimiento de la evidencia. Importante para acciones legales según el caso. En la preservación lo que más nos interesa es saber con la mayor exactitud qué fue lo que ocurrió para luego entender toda la información que podamos procesar en un análisis. Hay diferentes maneras de preservar la evidencia

Debemos tener en cuenta que la prioridad es preservar lo más íntegramente posible las evidencias del crimen en un estado íntegro. Eso significa colocar el sistema fuera de servicio (offline) cuando todos los usuarios del sistema están presionando para volver a ponerlo on-line.

Sí el sistema, por parte del administrador, fue forzado a seguir funcionando, eliminando las posibles vulnerabilidades o cualquier otra supuesta vía de acceso al servidor, la investigación forense no podrá seguir el rumbo correcto ya que:

1. Se eliminaría cualquier posibilidad de persecución del intruso en un futuro ya que se modifica la "escena del crimen" y no se podría calcular los daños estimados con un grado elevado de certeza.

2. Hay muchas posibilidades de que se le pasó algo importante por alto al administrador y el intruso (o intrusos) siguen teniendo acceso al sistema. Por lo tanto es mejor sufrir un "downtime" de red, mientras que se realiza el análisis forense del sistema.

Se tiene que establecer una prioridad entre:

(a) Funcionamiento inmediato, teniendo presente que las huellas dejadas por el/los intruso(s) pueden haberse eliminado por descuido del administrador y su equipo, y que el servidor puede seguir teniendo puertas traseras bien ocultas. Esta opción permite estar operativo en poco tiempo.

(b) Investigación forense detallada. Esta opción supone un mayor tiempo de permanencia offline sí no existen planes de contingencia y procedimientos para el backup del servicio.

Lugar seguro - Retención de tiempos – Identificación – Empaquetamiento - Transporte

4. RECOLECCION

Técnicas y métodos específicos utilizados en la recolección de evidencias, no alterar el sistema en riesgo ni ejecutar ningún software en el mismo.
Evidencias volátiles Como aquellas que se perderán al apagar el equipo
Hora del sistema y desfase horario, Contenido de la memoria
Procesos en ejecución:

Módulos/Controladores del Sistema Operativo

Programas en ejecución

Usuarios conectados

Configuración de red

Direcciones IP, tabla de rutas, cache arp, etc

Conexiones activas, puertos abiertos

Evidencias no volátiles

Aquellas que permanecerán tras apagar el equipo

Copiarlas al equipo de análisis

De forma local o a través de la red

Hacer checksum

Nunca utilizar programas del sistema para hacer la copia, No montar los sistemas de ficheros en modo escritura tampoco logs de IDS/Cortafuegos externos

4. ANÁLISIS

Dentro del análisis hay que basarse en las evidencias de datos ya que se va a tratar ficheros tipo de datos, metadatos, Analizar adecuadamente los programas en entornos seguros, Archivos normales, Archivos temporales, Archivos ocultos, Archivos borrados.

¿Quién?

Individuo (s) involucrados en la escena.

¿Qué?

Eventos ocurridos.

¿Cuándo?

Reconstruir la secuencia de los hechos.

¿Cómo?

Analizar qué tipo de herramientas fue utilizada para dicho delito.

5. INFORME

Características del análisis forense

Documentado

Reproducible

Resultados verificables

Independientemente del investigador, de las herramientas empleadas, de la metodología.

Aspectos Legales

Minimizar el tratamiento de los datos originales

Anotar cualquier cambio

Cumplir las reglas de gestión de las evidencias

No sobrepasar nuestros propios conocimientos

Admisibilidad de Evidencias Digitales

Principios generales

Las evidencias tienen que ser recogidas de la forma y por el personal autorizados

Las evidencias deben ser recogidas de acuerdo a los requerimientos formales, para establecer su fiabilidad

Debe respetarse el derecho a la intimidad

La integridad y autenticidad de las evidencias debe establecerse en el tribunal.

Utilizar técnicas y métodos estandarizados para recoger, almacenar y presentarlas

Las evidencias digitales no son autoexplicativas

Es probable que sea necesario un experto para explicarlas

Legislación Aplicable

Esto ira de acuerdo a los artículos definidos en la Asamblea Nacional según la Ley de Seguridad de la Información y delitos informáticos.

Preparación para el Análisis Forense

Recursos Hardware

Capacidad de proceso:

– Procesador de última generación

– 512MB o 1GB RAM

Almacenamiento:

– Sistema (>10GB)

– Trabajo (>60GB)

– Grabadora CD/DVD

Conexiones:

– IDE

– SCSI

– USB

– FireWire

– Lectores de Tarjetas de Memoria

– FastEthernet

Portátil

– Disco USB/FireWire

- Laptop

Hardware Software preinstalado

Imagen No. 117: Hardware preinstalado

Fuente: www.monografias.com

Recursos Software

En la estación de análisis:

– Linux / Windows según el caso

En equipo móvil

– Linux /Windows según el caso

Herramientas para creación de imágenes lógicas

Herramientas para recuperación de información
Herramientas para tareas de análisis forense

PLAN DE ACCIÓN

TAREAS DE ANALISIS FORENSE Y RECUPERACION DE INFORMACION EN DISPSITIVOS EN LOS LABORATORIOS DE LA FISEI-UTA

Es muy importante tener en cuenta cada una de las fases anteriormente expuestas para conservar de manera correcta la metodología a seguir para la respectiva tarea en el siguiente escenario.

ESCENARIO LABORATORIO FISEI-UTA

Se seguirá en primer orden con la petición formal del permiso correspondiente para poder realizar la presente práctica en los laboratorios al Sr. Administrador de Sistemas obteniendo anticipadamente la autorización del Ing. Oswaldo Paredes Decano de la Facultad que fue concedida al inicio de la presentación del tema.
Hay que tener en cuenta que este es un caso práctico de demostración ya que la investigación no requiere de su aplicación en la Universidad pero deja constancia de que es necesario un estudio profundo de herramientas de análisis forense y recuperación de información en los equipos y dispositivos de almacenamiento que mantengan riesgo de alteración o sean víctimas de un delito informático.
El estudio se centra en analizar uno de los equipos del laboratorio de la FISEI-UTA utilizando diversas herramientas con el fin de no comprometer el equipo o sistema sospechoso y de la misma manera preservar y recolectar evidencias.

La Investigación está a cargo del Ing. Héctor Alberto Luzuriaga Jaramillo con cédula No. 1803253150
Habiendo un acuerdo entre las partes se inicia el caso práctico entre el Investigador y la persona responsable de la Institución el mismo que consiste en conocer la información sobre la carpeta **RESPALDOS.**

EJECUCION DEL CASO DE TAREAS DE ANALISIS FORENSE EN BASE A LA METODOLOGIA ESTUDIADA CON EL RESPALDO DE HERRAMIENTAS ADECUADAS.

INFORME PERICIAL

ANALISIS PRELIMINAR

El respectivo proceso de análisis forense se realiza con la autorización por parte del Sr. Decano como del Administrador de sistemas, el cual es como sigue:
Análisis de uno de los equipos que se encuentra en el laboratorio de la FISEI-UTA y la intensión es la de recuperar una carpeta con archivos significativos para la institución que de de buena o mala manera ha sido eliminada y que tiene como nombre RESPALDOS, se trata de conocer registros, tiempos de acción como: hora, fecha, cuenta de usuario, hay que tener en cuenta que los laboratorios son utilizados por personas que tienen conocimiento informático, facilitadores y otros. La investigación hace uso de distintas herramientas, con el fin de no comprometer el equipo o sistema sospechoso y de la misma manera preservar y recolectar evidencias.

Caso realizado con la autorización de*:*

Administrador de sistemas

Ing. Decano de la Facultad

Caso realizado:

En los Laboratorios de la FISEI-UTA

Fecha del informe:

Lunes, 09 de noviembre del 2010.

Información del investigador.

NOMBRE: HECTOR ALBERTO LUZURIAGA JARAMILLO

C.I.: 1803253150

LICENCIA: xxxx123

Antecedentes

Descripción los equipos intervenidos

Nombre Del Equipo: EQUIPO1

Sistema Operativo: Windows 7

Características de los equipos

Memoria RAM: 512 Mb

Capacidad de Disco Duro: 150 Gb.

Herramientas utilizadas y su función.

Creación de Imágenes Lógicas

Acronis True Image, DD.

Recuperación de información

GetDataback, Foremost, Recovery My Files.

Análisis forense

Autopsy ¨+ Sleuthkit, Windows Forensic Toolchest (W.F.T)

Utilerías del S.O.

CRONOGRAMA DE ACTIVIDADES DEL ESTUDIO

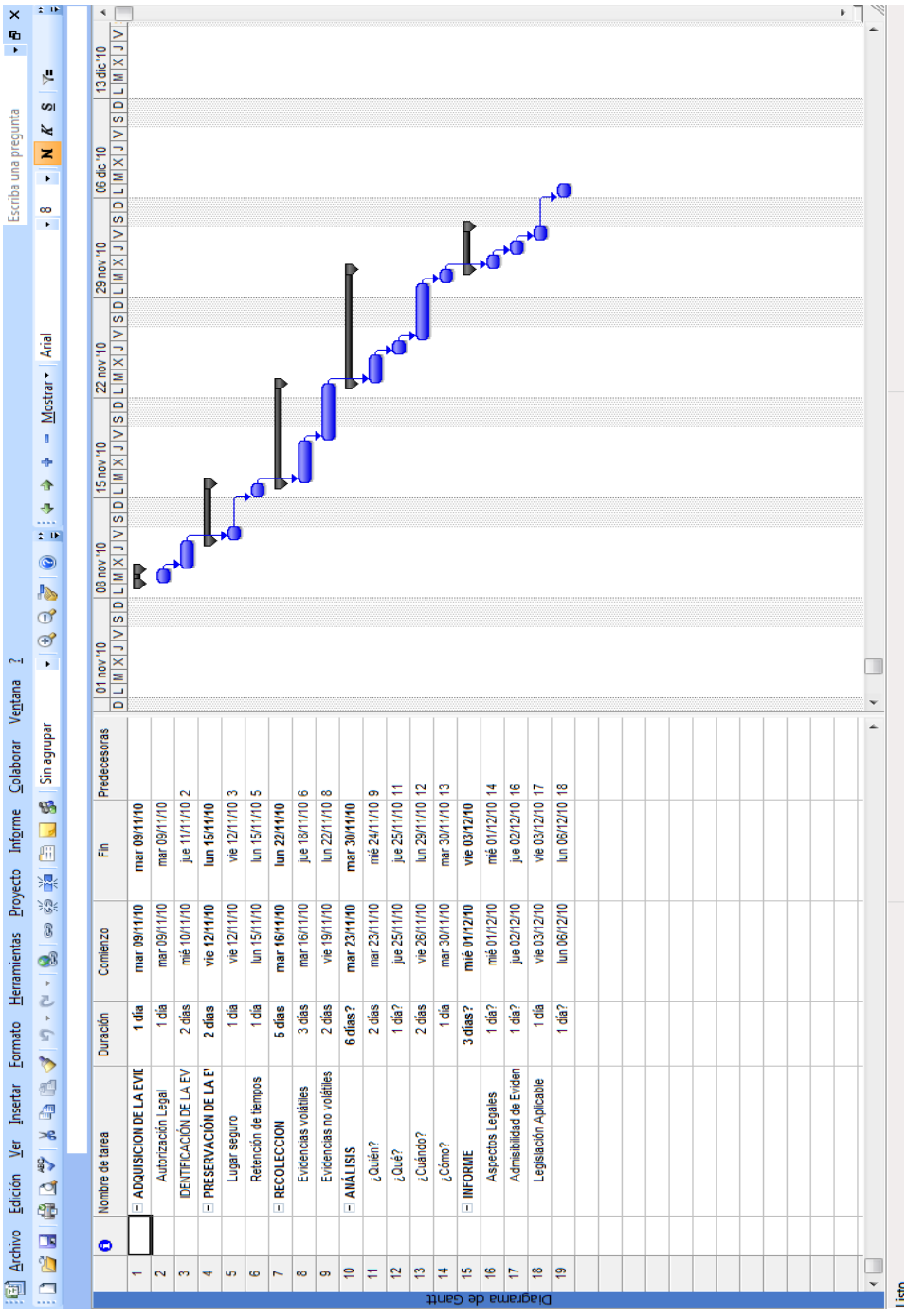


Imagen No. 117: Cronograma Análisis Forense

1. ADQUISICIÓN DE EVIDENCIA

Autorización Legal.- autorización por parte del Ing. Decano de la Facultad y del Administrador de sistemas

Autoridad e Investigador responsable.- A cargo del Investigador Héctor Alberto Luzuriaga Jaramillo

Normas Legales a seguir.- según metodologías estudiadas y regidas a los reglamentos de la UTA.

Preparación y Aseguramiento de la escena

Herramientas básicas a utilizar:

Imagen No. 118: Fotografía herramientas básicas para el proceso

Elaborado por: Investigador

Destornilladores

Cámara digital

Bolsa aislante

Guantes de látex

Cinta aislante

Bolsa antiestática

CDs

Disco Duro

Identificación de la escena del crimen.

Imagen 119: Perímetro Campus Universitario

Fuente: www.uta.com

Imagen 120: FISEI-UTA

Fuente: www.uta.com

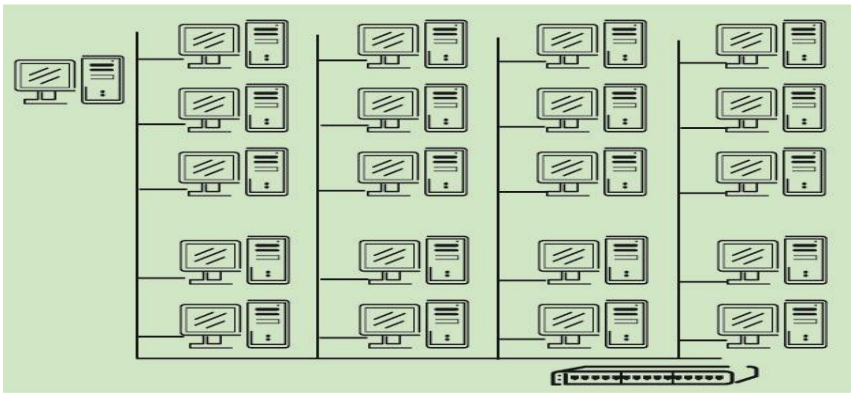


Imagen 121: Distribución equipos Laboratorio 1 FISEI-UTA

Elaborado por: Investigador

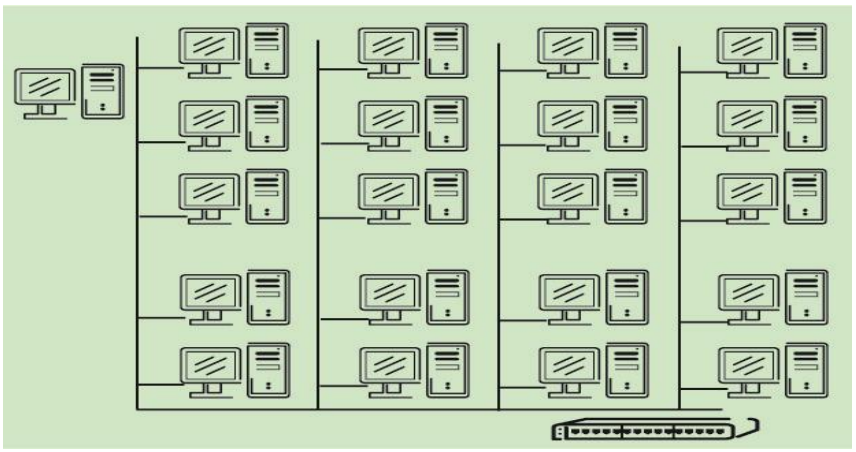


Imagen 122: Distribución equipos Laboratorio 2 FISEI-UTA

Elaborado por: Investigador

Sistemas involucrados.

Windows 7, Linux Distribución Centos 5.3.

Acceso hacia el perímetro de análisis autorizado, es decir al laboratorio.

Preservación toda huellas digitales, con el uso de guantes de látex.

Estado de los dispositivos

Se verifico que la máquina está en acción:

1 = Activado

0 = Desactivado

Apagado	1
Sleep	0
Encendido	0

Conexión en red

Existe conexión a red y se procede a desconectar

No existen impresoras conectadas

2. IDENTIFICACIÓN DE LA EVIDENCIA

Identificación de los equipos afectados

Imagen 123: Equipo Laboratorio FISEI-UTA

Elaborado por: Investigador

Para este caso se trata de la pérdida de la carpeta denominada RESPALDOS

3. PRESERVACIÓN DE LA EVIDENCIA

Las primeras evidencias que se deberán preservar son las volátiles las mismas que al momento de almacenarlas o guardarlas directamente se convertirán en evidencias no volátiles. Estas a su vez se deberá documentarlo.

Pasos a seguir:

El equipo para el caso deberá estar en un lugar seguro para realizar la adquisición de datos.

Retención de tiempos.

HORA SISTEMA: 15:00 PM

FECHA SISTEMA: 9 de Noviembre del 2010

HORA ACTUAL: 15:10 PM

FECHA ACTUAL: 9 de Noviembre del 2010

Preservación a cargo del Investigador

Ing. Alberto Luzuriaga

Empaquetamiento de los dispositivos

Se deberán guardar dentro de bolsas antiestáticas y sellarlas para no exponer la evidencia.

Imagen 124: Disco duro empaquetado y etiquetado

Elaborado por: Investigador

Transporte

Luego de haber preservado las evidencias estos deberán ser transportados a un lugar cerrado y seguro en el que podamos realizar el análisis, para esto no se deberá trabajar en el mismo sistema comprometido.

Se realizará el proceso realizando copias de la imagen de bit a bit.

Procedemos a extraer el dispositivo comprometido para esto utilizamos guantes de látex como se muestra en la figura siguiente:

Imagen 125: Guantes de látex para extraer el dispositivo comprometido

Elaborado por: Investigador

Imagen 126: Extracción del disco comprometido

Elaborado por: Investigador

4. ANÁLISIS

Se analizan las diferentes herramientas adecuadas para el caso

Datos Base

EQUIPO A

Equipo comprometido con pérdida de información

EQUIPO B

Equipo en el que se deberá realizar el análisis forense

ANALISIS EQUIPO A UTILIZANDO WINDOWS 7

Obtención de la imagen

Contamos con la herramienta DD

Recuperación de Información

Recovery My Files, GetDataBack, Foremost.

Tareas de Análisis Forense

Live CD (HELIX) sobre una imagen obtenida del sistema del equipo comprometido.

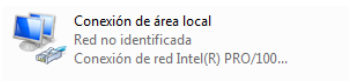
Análisis de la imagen del sistema operativo Windows 7 desde un equipo en Linux distribución Centos 5.3, herramientas necesarias para su investigación como Autopsy.

Conexión en Red

Copia de bit a bit de la imagen Herramienta a utilizar DD

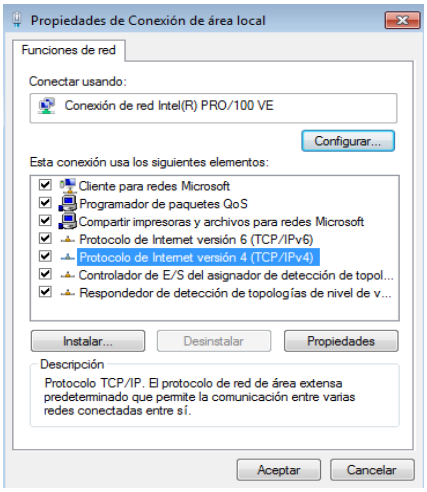
CONFIGURACION EQUIPO B

Mis conexiones de red



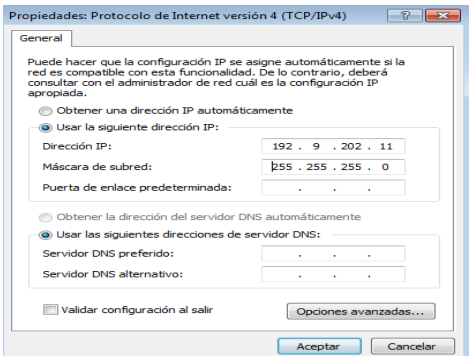
Asignamos una IP

Imagen 127: Asignación de IP parte1



Elaborado por: Investigador

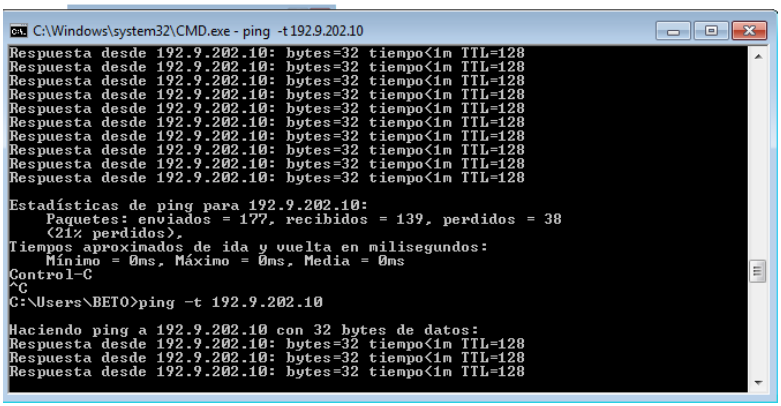
Imagen 128: Asignación de IP parte2



Elaborado por: Investigador

Realizamos un ping para establecer si la conexión está correcta

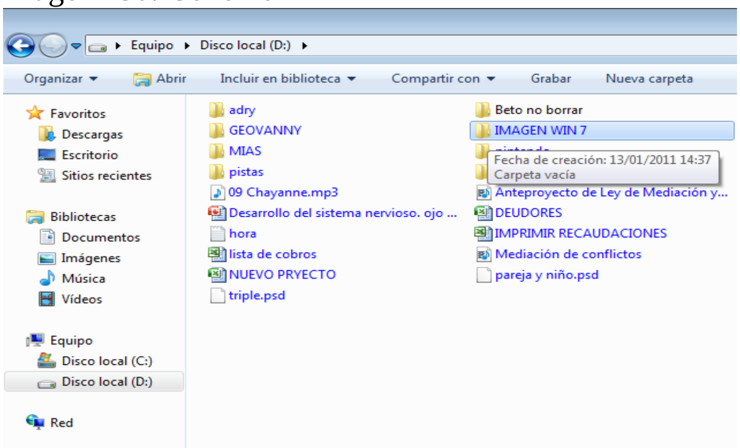
Imagen 129: ping de conexión



Elaborado por: Investigador

Ya tenemos una conexión en red y vamos a compartir una carpeta para la imagen que vendrá del EQUIPO A

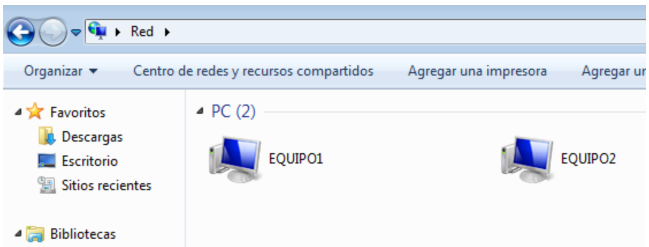
Imagen 130: Conexión



Elaborado por: Investigador

Tenemos la conexión lista

Imagen 131: Conexión parte2



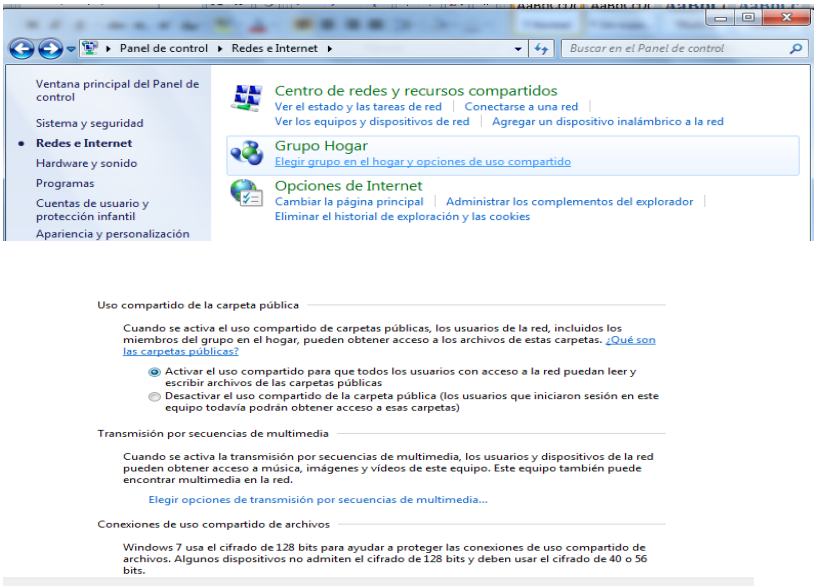
Elaborado por: Investigador

CREACION DE LA IMAGEN

Para esto necesitamos acceder al EQUIPO 2 (B) desde conexiones de red del EQUIPO 1 (A) y nos localizamos en la carpeta compartida IMAGEWIN7.

Hay que tener en cuenta que en Windows 7 se debe configurar la manera de compartir archivos en el Grupo Hogar para no tener dificultad y manjar los permisos.

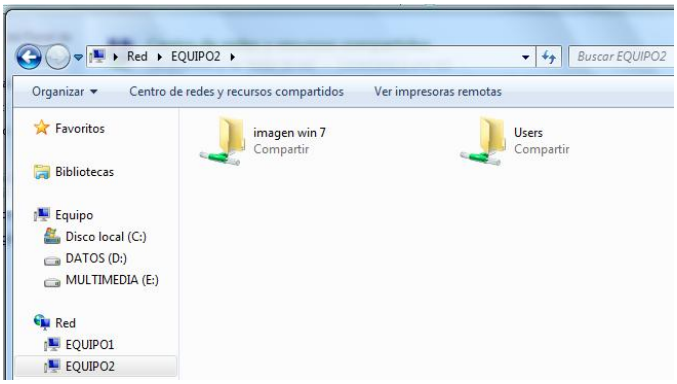
Imagen 132: Creación de la imagen parte1



Elaborado por: Investigador

Accedemos a la carpeta compartida en este caso se denomina IMAGENWIN 7

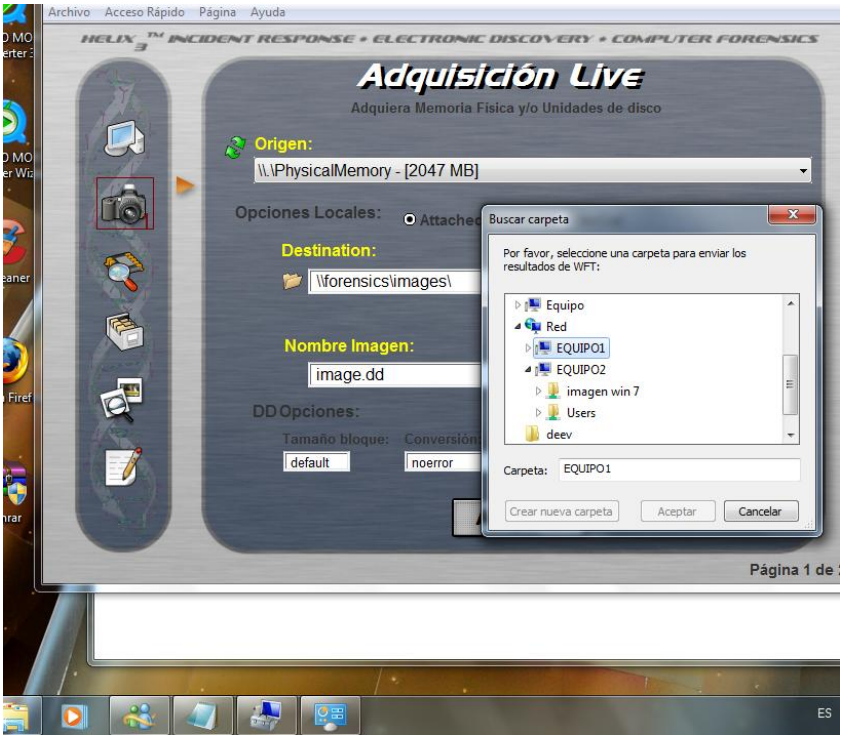
Imagen 133: Creación de la imagen parte2



Elaborado por: Investigador

Ejecutamos Cd Live hélix para este caso

Imagen 134: Creación de la imagen parte3



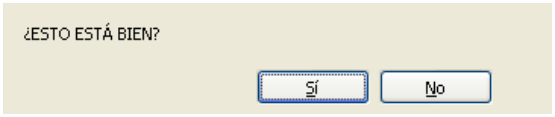
Elaborado por: Investigador

Enviamos la imagen a la red hacia el otro equipo en el va hacer analizada

Imagen 135: Creación de la imagen parte4

Elaborado por: Investigador

Nos presenta un cuadro de diálogo en el que nos pide aue verifiquemos si todo está correcto



Ponemos si

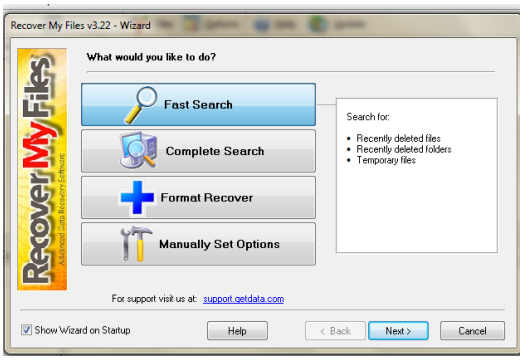
Hora de ejecución: 17:05

Hora de finalización: 19:33

RECUPERACION DE LA INFORMACION PLATAFORMA WINDOWS 7

Herramienta Recovery My Files

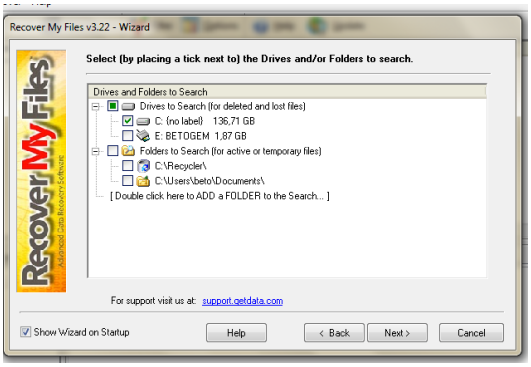
Imagen 136: Recuperación de la información Recovery My Files parte1



Elaborado por: Investigador

Nos pedirá la unidad a recuperar

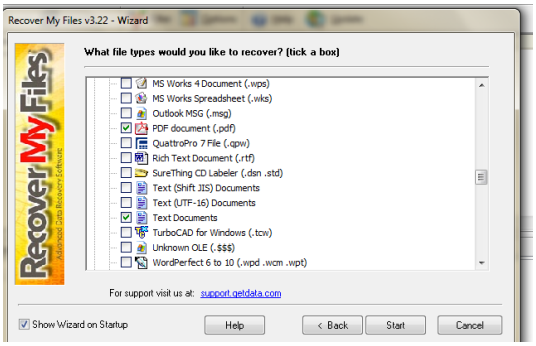
Imagen 137: Recuperación de la información Recovery My Files parte2



Elaborado por: Investigador

Tipo de archivo a recuperar para este fin tenemos perdidos archivos pdf, doc, ppt, mp3.JPEG y aplicación DOS debido a unos instaladores que se encontraban en la carpeta eliminada.

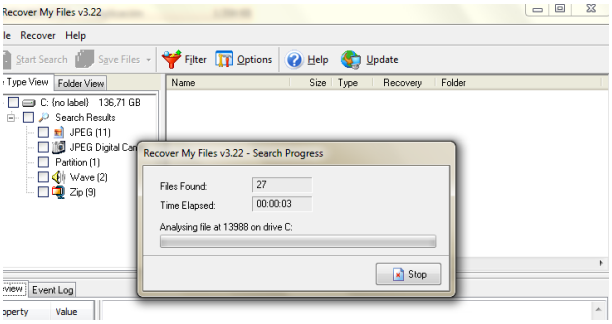
Imagen 138: Recuperación de la información Recovery My Files parte3



Elaborado por: Investigador

Ejecutamos click en start

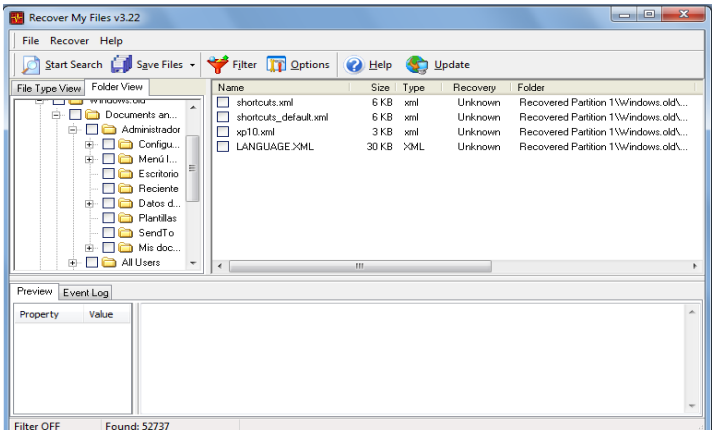
Imagen 139: Recuperación de la información Recovery My Files parte4



Elaborado por: Investigador

Una vez terminado el proceso de recuperación procedemos a copiar

Imagen 140: Recuperación de la información Recovery My Files parte5



Elaborado por: Investigador

Hora ejecución: 17:56

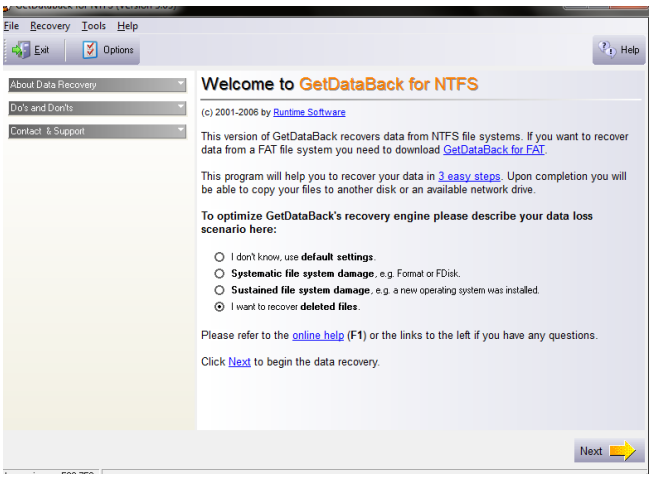
Hora Finalización: 21:33

RECUPERACION DE LA INFORMACION

GetDataBack

Nos presenta las opciones a recuperar no sin antes saber que sistema de archivos es NTFS o FAT para este caso NTFS

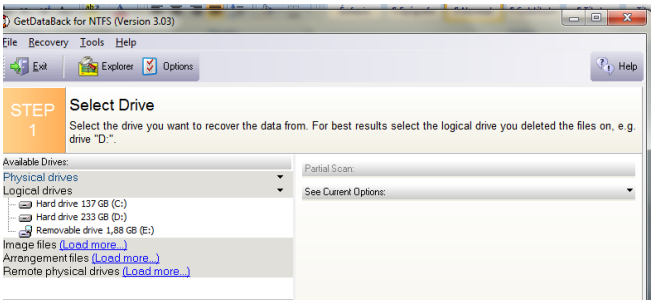
Imagen 141: Recuperación de la información GetDataBack parte1



Elaborado por: Investigador

Escogemos el volumen lógico

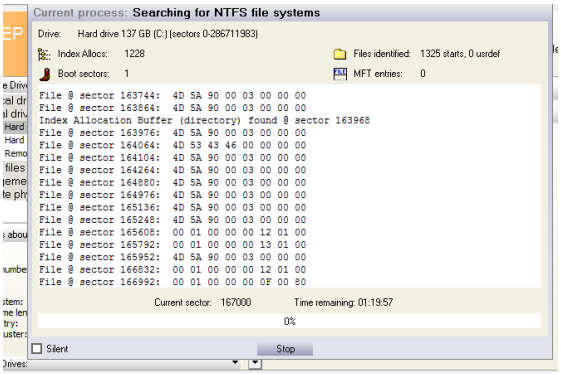
Imagen 142: Recuperación de la información GetDataBack parte2



Elaborado por: Investigador

Buscando sistema de archivos para NTFS

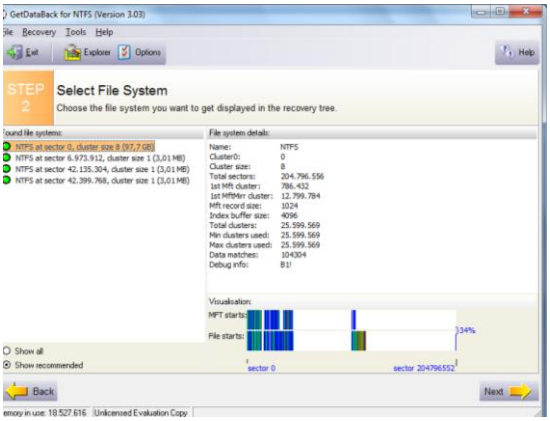
Imagen 143: Recuperación de la información GetDataBack parte3



Elaborado por: Investigador

Terminado el proceso de recuperación next

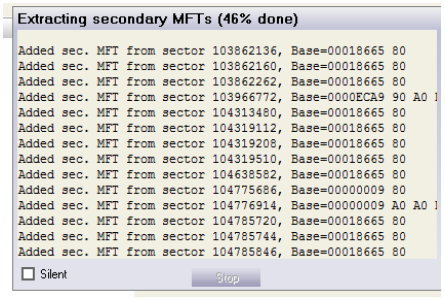
Imagen 144: Recuperación de la información GetDataBack parte4



Elaborado por: Investigador

Se cargan los archivos recuperados

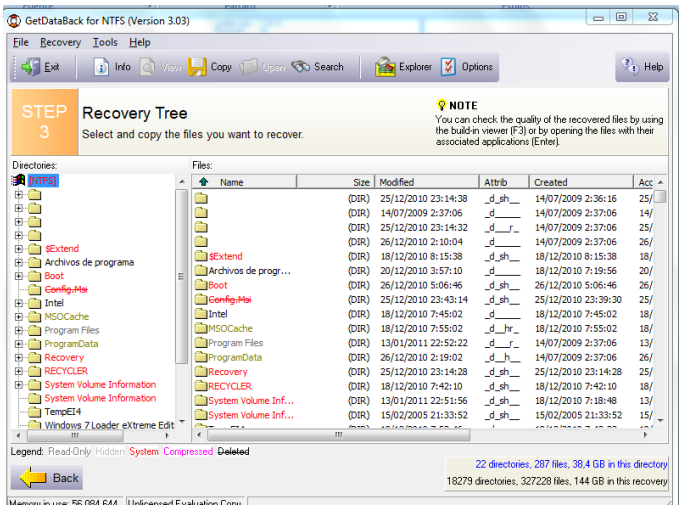
Imagen 145: Recuperación de la información GetDataBack parte5



Elaborado por: Investigador

Copiamos la carpeta o los archivos recuperados

Imagen 146: Recuperación de la información GetDataBack parte6



Elaborado por: Investigador

Hora ejecución: 17:55

Hora Finalización: 18:40

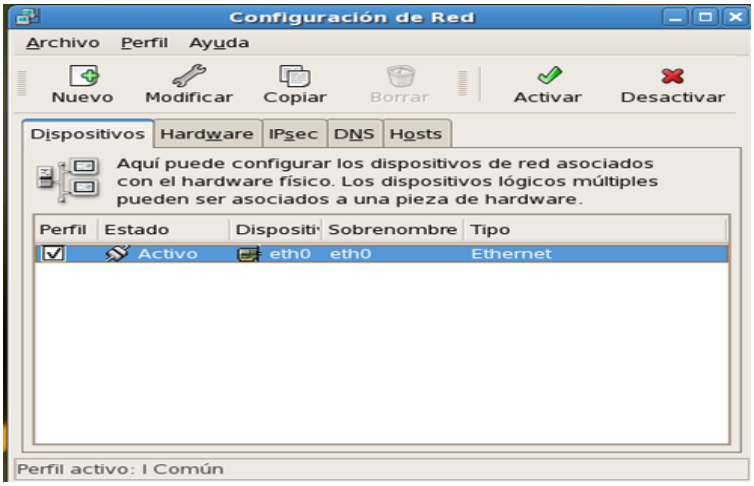
RECUPERACION DE INFORMACION PLATAFORMA LINUX DISTRIBUCION CENTOS 5.3

Primeramente procedemos a configurar el equipo de Linux Distribución Centos 5.3 hacia Windows 7

Configuramos la IP

Configuración de red para esto lo tenemos como eth0

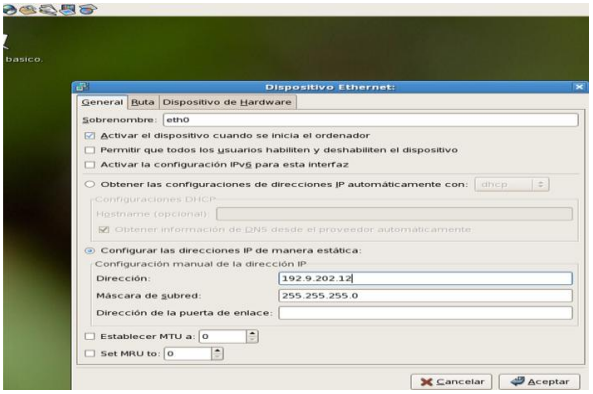
Imagen 147: Configuración en Linux parte1



Elaborado por: Investigador

Modificamos ponemos la IP

Imagen 148: Configuración en Linux parte2



Elaborado por: Investigador

Abrimos la terminal

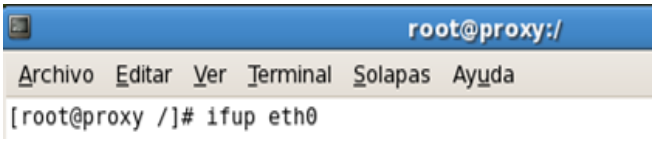
Imagen 149: Configuración en Linux parte3

Elaborado por: Investigador

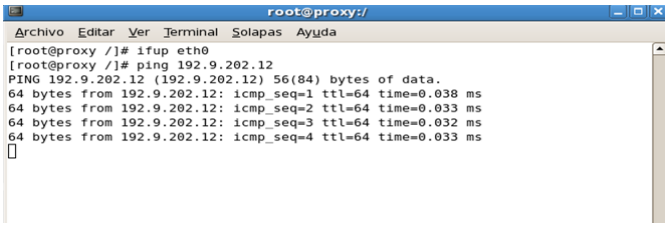
En donde vamos a levantar primeramente la interfaz de la red para esto utilizamos

If up eth0

Imagen 150: Configuración en Linux parte4

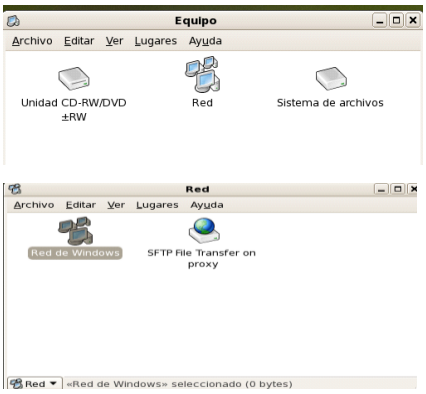


Verificamos haciendo ping



Elaborado por: Investigador

Imagen 151: Configuración en Linux parte5



Elaborado por: Investigador

Tenemos la red de Windows tenemos nuestro WORKGROUP

Imagen 152: Configuración en Linux parte6

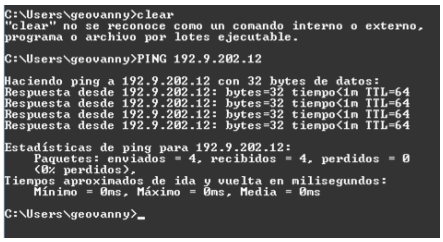
Elaborado por: Investigador

Equipo1 de Windows dentro de Linux

VERIFICACION DESDE WINDOWS

Hacemos ping a la máquina de Linux desde el prompt de Windows

Imagen 153: verificación en windows



Elaborado por: Investigador

Con esto está establecida la conexión Linux /Windows para el siguiente proceso

CONFIGURAMOS SAMBA

La manera por la que queremos configurar Samba es porque este servicio nos permite crear usuarios y compartir archivos con permisos lo que nos vá a dar mayor seguridad a los datos.

Lo único que tenemos que hacer es dentro de Samba crear los usuarios s{olo para samba

Para esto tenemos dos ambientes el Global

Manipulamos el archivo smb.conf

WORKGROUP = WORKGROUP para nuestro caso

Server string = samba versión %v esto para la versión

Netbios = LINUX SERVER

Interfaces = eth0 192.9.202.12/24

Host allow = 127.192.168.0

127 significa que va a aceptar todas las conexiones del 127

[datos]

192.9.202.x

X puede ser 13,14,15

useradd –s/sbin/nologin BETO

#smbpasswd –a BETO

Reiniciamos el servicio

Service smb status

Service smb start

Ejecutamos en windows 192.9.202.12 esto para comprobar

RECUPERACION DE INFORMACION LINUX

Herramienta Foremost

$ foremost -i image.dd -o ./respald

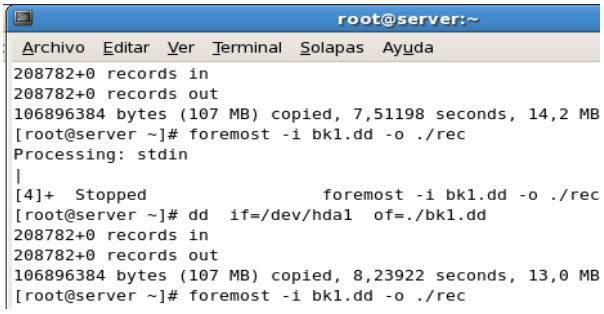
i = entrada

o = salida

esto como archivos donde se va almacenar lo recuperado

Nos presenta un reporte de auditoria

Imagen 154: Recuperación de información Linux



Elaborado por: Investigador

ANALISIS FORENSE.

ANALISIS DE LA IMAGEN CON AUTOPSY

Ingresamos el cd live hélix para esto para prender arrancar el computador con el disco

Imagen 155: Captura Análisis forense parte1

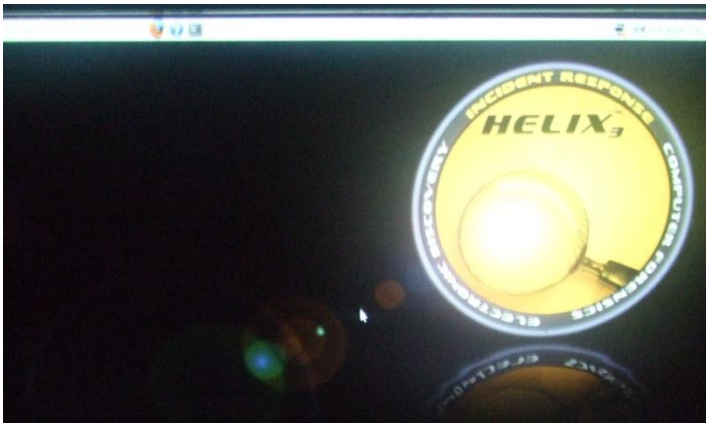
Escogemos la primera opción

Imagen 155: Captura Análisis forense parte2

Elaborado por: Investigador

Pantalla del hélix con algunas herramientas ya instaladas

Imagen 156: Captura Análisis forense parte3



Elaborado por: Investigador

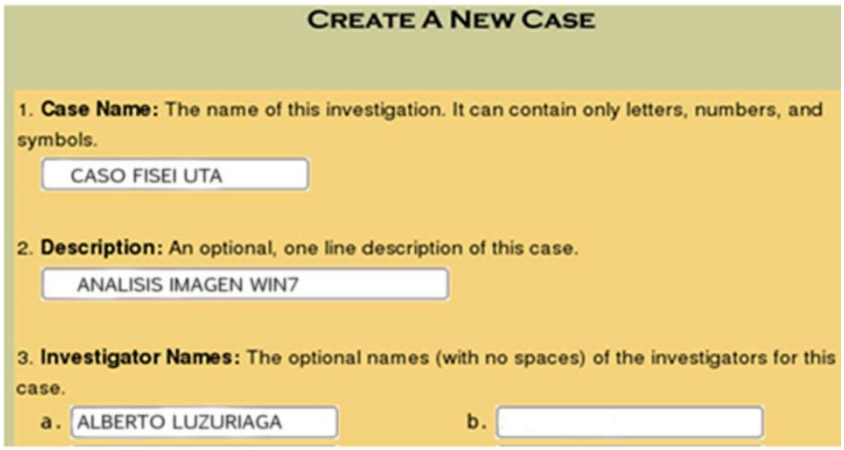
ANALISIS CON AUTOPSY

Imagen 157: Análisis forense parte1

Elaborado por: Investigador

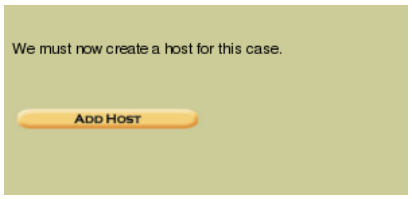
Creación del caso datos generales

Imagen 158: Análisis forense parte2



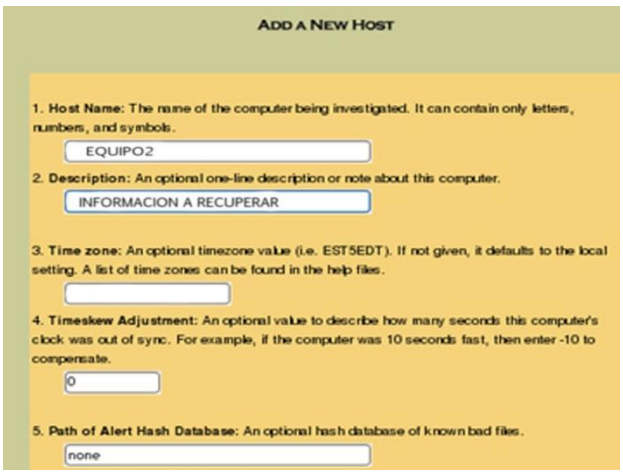
Elaborado por: Investigador

Adicionar un nuevo host



Datos al host

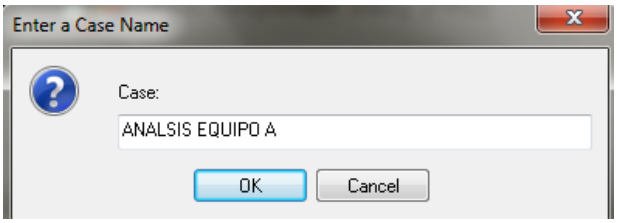
Imagen 159: Análisis forense parte3



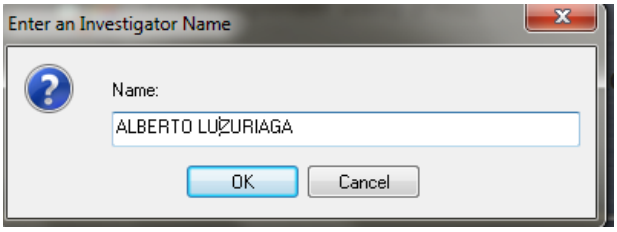
Elaborado por: Investigador

WINDOWS FORENSIC REPORTE

Imagen 160: Análisis forense parte4



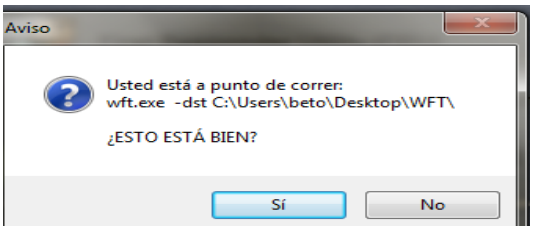
Investigador



Elaborado por: Investigador

Pantalla de confirmación para realizar el proceso

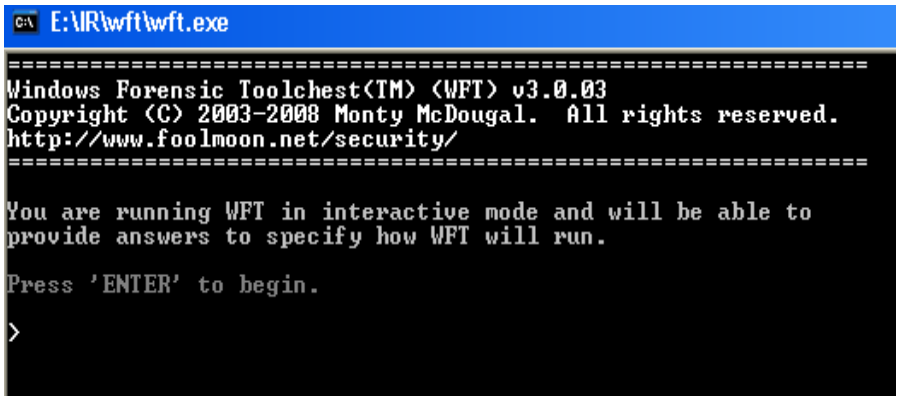
Imagen 161: Análisis forense parte5



Elaborado por: Investigador

Ingresado los datos básicos que nos pide nos visualiza la siguiente pantalla:

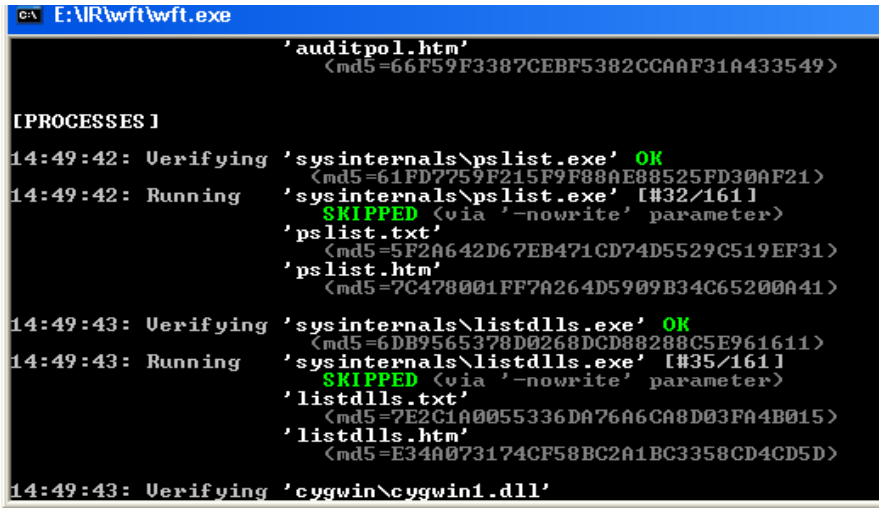
Imagen 162: Análisis forense parte6



Elaborado por: Investigador

Proceso

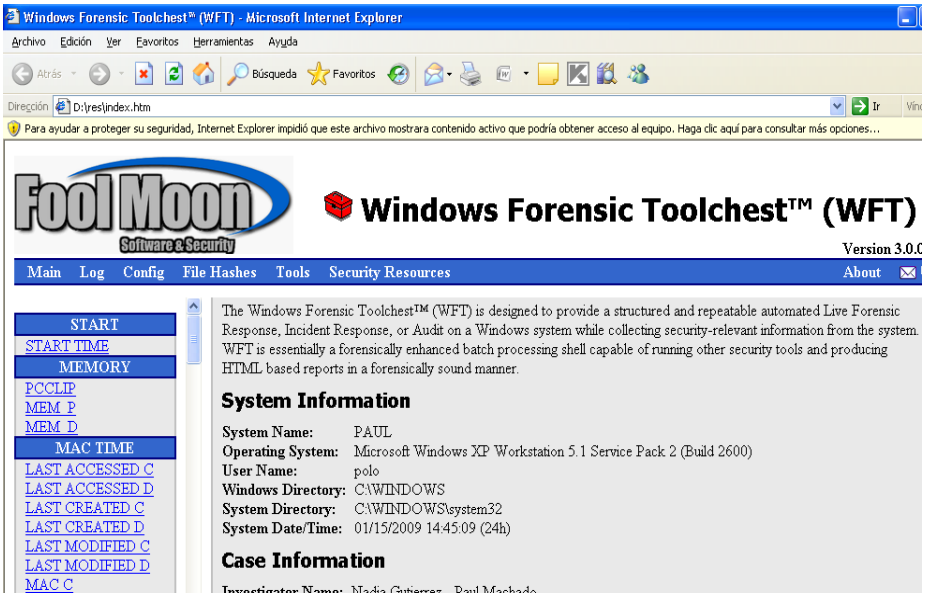
Imagen 163: Análisis forense parte7



Elaborado por: Investigador

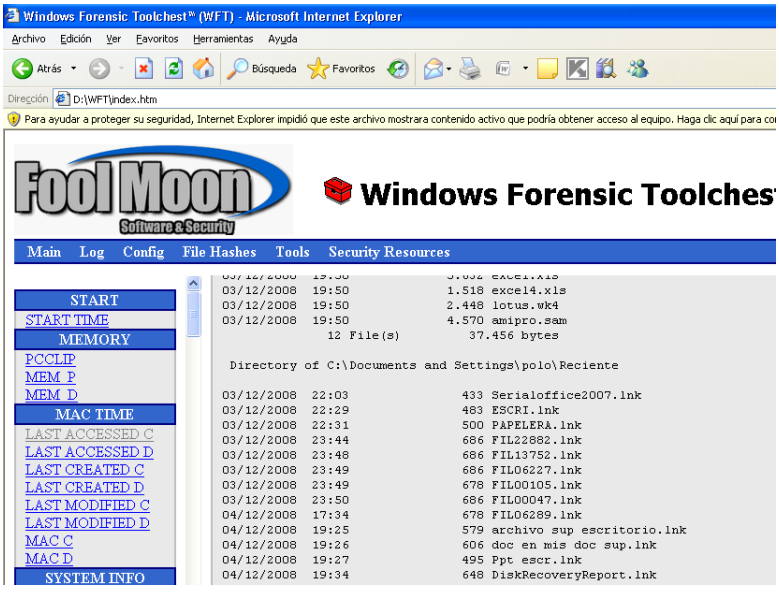
Herramienta se visualiza en HTML

Imagen 164: Análisis forense parte8



Archivos con último acceso al disco local C

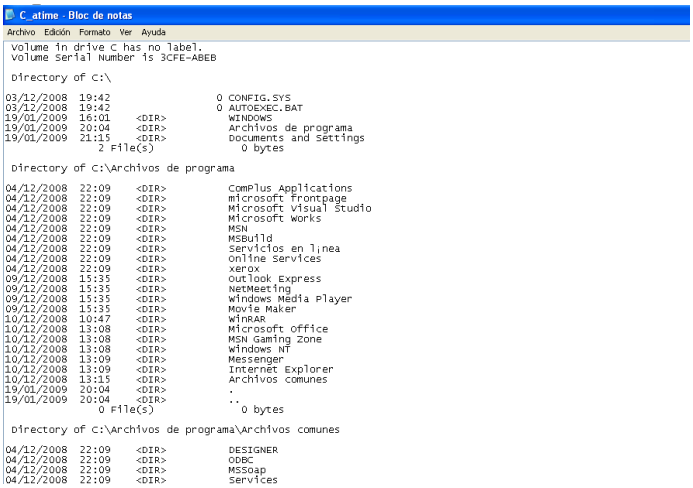
Imagen 165: Análisis forense parte9



Elaborado por: Investigador

Resultado en archivo de texto

Imagen 166: Análisis forense reportes



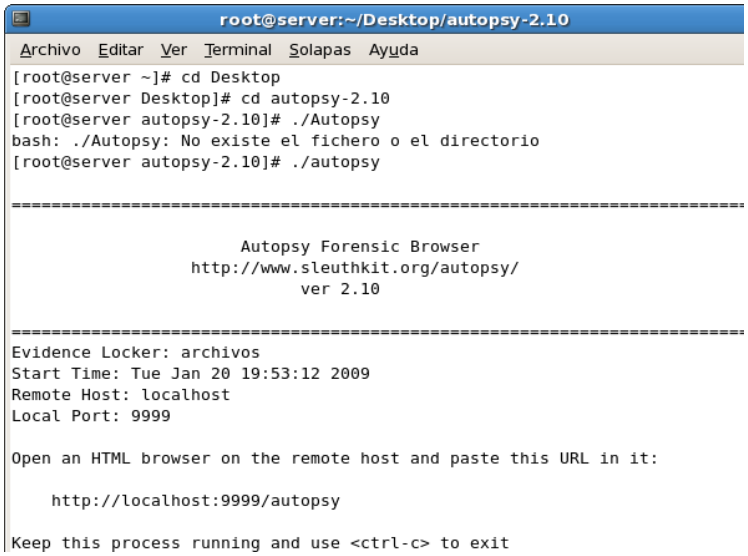
Elaborado por: Investigador

ANALISIS FORENSE.

ANALISIS DE LA IMAGEN CON AUTOPSY INSTALADO DESDE LA DISTRIBUCION CENTOS 5.3

Se procede a ejecutar el autopsy abriendo un terminal el procedimiento a seguir es parecido al de la distribución live con el hélix

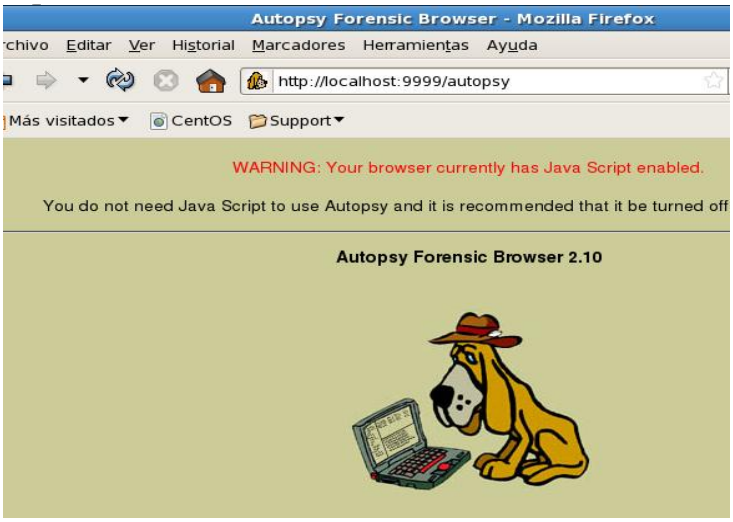
Imagen 167: Análisis de la imágen



Elaborado por: Investigador

Abrimos en el navegador http://localhost:9999/autopsy

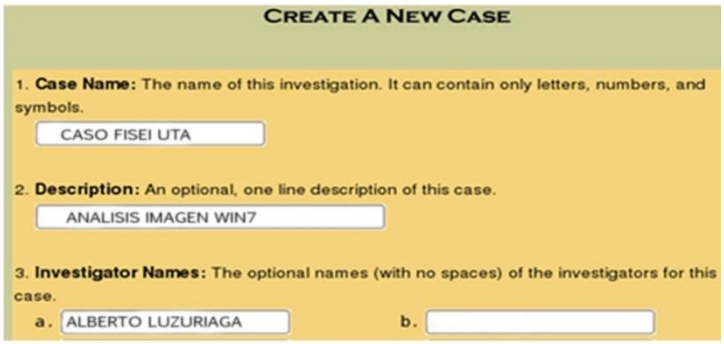
Imagen 168: Análisis de la imagen procedimiento2



Elaborado por: Investigador

Creamos un nuevo caso y seguimos el procedimiento anterior

Imagen 169: Análisis de la imagen nuevo caso



Elaborado por: Investigador

INFORME

Se ha preservado la evidencia digital sin alterar

Se ha recuperado información que ha sido eliminada intencionada o no

Se registran hora , fecha en la que el intruso ingreso al equipo

El informe de las herramientas como Autopsy y Windows Forensic Tolls muestran ingreso de dispositivos al equipo

VERIFICACIÓN DE LAS HIPOTESIS

CASO DE PRUEBA

Se toma en cuenta los dispositivos de almacenamiento siguientes:

Disco duro, Pendrive,

Se procedió a:

Eliminación de archivos en distintos escenarios

Procedimiento a recuperar

Determinar tiempos de acción como registros de fecha, hora, y usuario logueado.

FICHAS TECNICAS FORMATO

Variable Independiente: Herramientas de Análisis Forense

Variable Dependiente: Recuperación de Información

Basado en las variables

Tabla No. 33: Formato Ficha Técnica

OBJETIVO:

ESCENARIO		Análisis de Indicadores		
		Cantidad de Información	**Tiempo**	**Resultado**
Las Herramientas de Análisis Forense	Disco Duro			
	Pendrive			
Sin herramientas de Análisis forense	Disco Duro			
	Pendrive			

Elaborado por: Investigador

RESULTADOS CASO PRUEBA

Siguiendo las tareas de herramientas de análisis forense se ha determinado que en la plataforma Windows en discos duros nos ha dado como reultado un 100% con un tiempo de 30 minutos de éxito en recuperación y un 70% bajo Linux en 180 minutos siendo el resultado confiable.

Siguiendo las tareas de herramientas de análisis forense se ha determinado que en la plataforma Windows en los dispositivos como Pendrive nos ha dado como resultado un 100% de éxito en recuperación y un 100% bajo Linux en 10 minutos siendo el resultado confiable.

Siguiendo las tareas de herramientas de análisis forense se ha determinado evidencias recolectar registros de fecha, usuario logueado, y dispositivos en un 100%.

Variable Independiente: Herramientas de Análisis Forense

Variable Dependiente: Recuperación de Información

Tabla No. 34: Ficha técnica para probar la hipótesis

Basado en las variables

OBJETIVO: Recuperación de información de los dispositivos de almacenamiento determinados para el caso, se basa en indicadores como volumen de información, tiempos, y resultado legible o no.					
ESCENARIO		**Análisis de Indicadores**			
		Cantidad de Información	**Tiempo**	**Resultado**	**Registros**
Las Herramientas de Análisis	Disco Duro	Windows (100 %) Linux	30 min 180 min	Confiable	100%

Forense		(70%)			
	Pendrive	Windows (100 %) Linux (100%)	10 min 10 min	Confiable	100%
Sin herramientas de Análisis forense	Disco Duro	0%	0 min	-	
	Pendrive	0%	0 min	-	

Elaborado por: Investigador

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- Las tareas de análisis forense es una solución al problema de diferentes delitos informáticos ya que nos proporcionan de manera detallada cualquier intento

de intrusiones dándonos un respaldo si se desea demandar judicialmente según el caso.

- Queda demostrado que herramientas que son de libre distribución nos ayuda a crear imágenes de bit a bit exactas sin tener que pagar licencias y de una manera mucho más eficaz como son Acronis True Image y DD .

- Existen diferentes herramientas para recuperación de información que nos ha dado como resultado un porcentaje del 98% de éxito como Recovery My Files, Getdataback, Photorec, Foremost.

- Se determino que para realizar tareas de análisis forense bajo la plataforma de Linux se necesita de más conocimientos que de Windows siendo las más significativas Autopsy y Windows Forensic tolls

- Distribuciones Live Cd que contienen diferentes herramientas han contribuido en gran parte ya que es un cd booteable con el que no necesita de instalación y trabaja en un 100%

Recomendaciones

- Se deberá tener en cuenta que las tareas de análisis forense a través de un estudio determinado que nos ayudará a recolectar evidencias en el caso de que exista un delito informático.

- Es recomendable estudiar características de cada una de las herramientas para determinar cuál es la más adecuada ya que cada caso es único.

- Es aconsejable realizar un estudio de las herramientas que nos permiten recuperar información para saber a qué volumen de información trabajan, si es el caso de un flash, disco duro, memorias, u otros.

- Revisar manuales de Linux y Windows , para de esta manera no tener problemas al momento de proceder a utilizar herramientas de análisis y recuperación de información

- Se recomienda realizar procesos de prueba de análisis forense informático en la FISEI-UTA ya que se trata de estudiantes con conocimientos informáticos y exponer sus pro y contra de las actividades que se realizan en un equipo y lo más importante poder recuperar datos de distintos dispositivos de almacenamiento.

- Se deberá regirse a las leyes existentes dentro de laLa Constitución de la República del Ecuador.

BIBLIOGRAFÍA

www.ramosoft.com. (n.d.). Retrieved from http://www.slideshare.net/contiforense/seguridad-informtica-y-policia-informtica-4667479

Anaya, T. H. (n.d.). *http://www.oas.org.* Retrieved from http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

ANTONIO L. ((2002). Aula Siglo XXI). *Computación y Tecnología.* Madrid, España.

ANTONIO, L. ((2002). Aula Siglo XXI.). *Computación y Tecnología.* España.

Delgado, M. L. (2007). *"Análisis Forense Digital".*

DRAE. (n.d.). *http://es.wikipedia.org.* Retrieved from http://es.wikipedia.org/wiki/Inform%C3%A1tica

Hordeski, M. F. *Localización y Reparación de fallas de computadoras personales* .

http://es.wikipedia.org. (n.d.). Retrieved from http://es.wikipedia.org/wiki/Software_libre

http://es.wikipedia.org. (n.d.). Retrieved from http://es.wikipedia.org/wiki/Tarjeta_de_memoria

http://www.cavaju.com. (2009, septiembre 3). Retrieved from http://www.cavaju.com/2009/09/03/curso-sistema-gestion-seguridad-informacion-iso-27002-27001/

http://www.icm.espol.edu.ec/materias/icm01438/archivos.htm. (n.d.).

http://www.monografias.com. (n.d.). Retrieved from http://www.monografias.com/trabajos12/elsoflib/elsoflib.shtml#VENTAJ

http://www.monografias.com. (n.d.). Retrieved from http://www.monografias.com/trabajos37/disco-duro/disco-duro2.shtml

http://www.monografias.com. (2010). *http://www.tutorialesenlared.com/manual3620.html*. Retrieved from Url: http://www.monografias.com

http://www.scribd.com. (n.d.). Retrieved from http://www.scribd.com/doc/30020382/La-seguridad-informatica

Investigador. (2010). Ecuador.

Lanzillotta, A. (2005, febrero 2005). *http://www.mastermagazine.info*. Retrieved 2010, from http://www.mastermagazine.info: http://www.mastermagazine.info/termino/7238.php

lfmontalvan. (2009, abril 17). *www.utpl.edu.ec.* Retrieved from http://blogs.utpl.edu.ec/sistemasoperativos/2009/04/17/linux-red-hat-linux/

Martinez, R. (1998-2010). *El rincon de linux.*

Molina, M. P. (2004, 0ctubre 15). *http://www.mariapinto.com.* Retrieved from http://www.mariapinto.es/e-coms/recu_infor.htm

O´brien, J. A. (2006). *Sistemas de Información Gerencial.* Mexico.

Oset, J. M. (2004). *ANÁLISIS FORENSE DE SISTEMAS LINUX.* Madrid.

Prieto., R. A. (2004, julio). *http://www.ausejo.net.* Retrieved from http://www.ausejo.net/seguridad/forense.htm

Prieto., R. A. (2004). *http://www.ausejo.net*. Retrieved noviembre lunes, 2010, from http://www.ausejo.net/seguridad/forense.htm

ROMERO, R., & TOLEDO, M. *Unidades de Zip.*

System., T. C. (2002). *http://es.wikipedia.org.* Retrieved from http://es.wikipedia.org: http://es.wikipedia.org/wiki/Unix

wikipedia. (2010). *http://es.wikipedia.com.* Retrieved from http://es.wikipedia.org/wiki/Macintosh

wikipedia.org/wiki. (n.d.). *http://es.wikipedia.org/wiki/ISO/IEC_17799*. Retrieved noviembre lunes, 2010, from http://es.wikipedia.org/wiki/ISO/IEC_17799: http://www.google.com.ec

Sabotaje informático ecuador

http://www.proasetel.com/paginas/articulos/sabotaje_informatico.htm

http://www.ecuadorinmediato.com/Noticias/news_user_view/ecuadorinmediato_noticias--13563

Recuperación de datos

Localización y Reparación de fallas de computadoras personales Michael F. Hordeski

http://eprints.ucm.es/5979/1/Modelos_RI_preprint.pdf
http://descargas.cervantesvirtual.com/servlet/SirveObras/02472741989036164198835/010010_3.pdf
http://alarcos.inf-cr.uclm.es/doc/ari/trans/Tema2.pdf
ojo http://bvs.sld.cu/revistas/aci/vol13_6_05/aci100605.htm
http://www.tdr.cesca.es/TESIS_UJI/AVAILABLE/TDX-1205107-095639//sanz2.pdf

Herramientas De Análisis Forense
http://www.ausejo.net/seguridad/forense.htm
Análisis Forense Digital
http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

Curso Análisis Forense
http://www.ati.es/IMG/pdf/CursoAnalisisForensejunio2007.pdf

Hardware parte física y recuperación de datos
Hardware - Anaya Multimedia editores - 2006
Pc World 2006
Tutorial Multimedia de Hardware - Macro editorial 2005
Enciclopedia Multimedia de Electrónica Básica – Editorial F&G S.A.

Herramientas para análisis forense
http://www.porcupine.org/forensics/tct.html • The Sleuth Kit (TSK)
http://www.sleuthkit.org/sleuthkit/index.php • Autopsy:
http://www.sleuthkit.org/autopsy/index.php • mac-robber:
http://www.sleuthkit.org/mac-robber/index.php • Foundstone Forensic Utilities:
http://www.foundstone.com/resources/forensics.htm
http://odessa.sourceforge.net/

Páginas web de proyectos

Honeynet Project: http://www.honeynet.org

- SANS Institute (SANS InfoSec Reading Room): http://www.sans.org/rr/
- Página web de Wietse Venema http://www.porcupine.org/
- Forensics-es: http://www.forensics-es.org
- Codes of Practices for Digital Forensics: http://cp4df.sourceforge.net
- Phrack: http://www.phrack.org

Códigos éticos en I.F. y seguridad en general:

http://www.isc2.org/
http://www.osstmm.org/
http://www.thesedonaconference.org/

Paginas de ataques a nivel internacional

http://informaniaticos.blogspot.com/2010/01/china-lanzo-varios-ataques-hacker.html
http://www.elmundo.es/elmundo/2010/01/26/navegante/1264493080.html
http://www.nerdsbackup.com/estadisticas_perdida_informacion.asp
http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

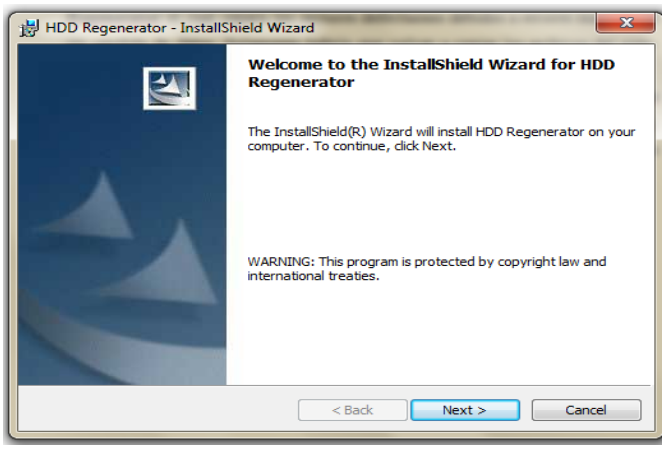
ANEXOS

ANEXO A

HERRAMIENTAS PARA RECUPERACION DE DISCOS DUROS

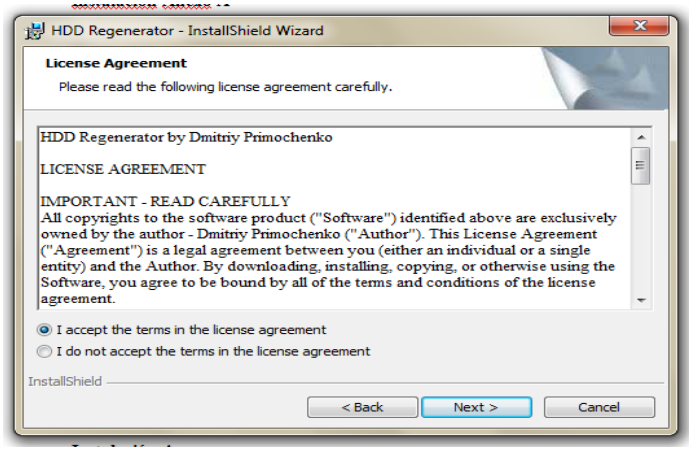
INSTALACIÓN HDD REGENERATOR

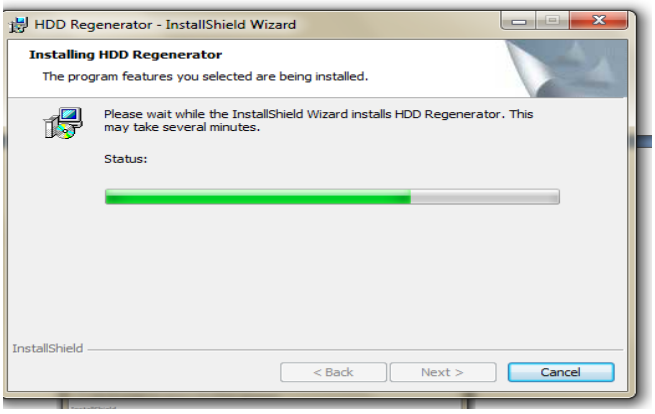
Doble click sobre el ícono setup del HDD Regenerator



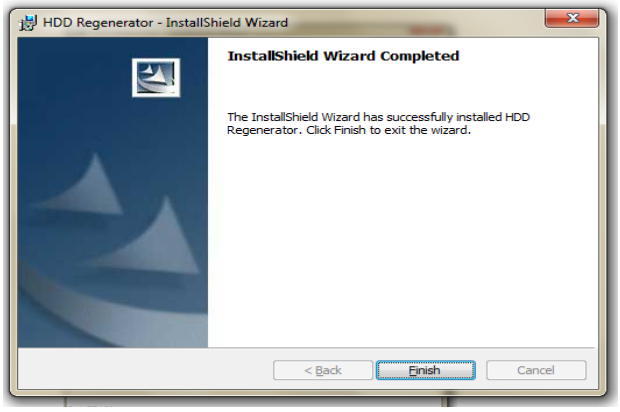
Click en Next

Aceptamos acuerdo de licencia





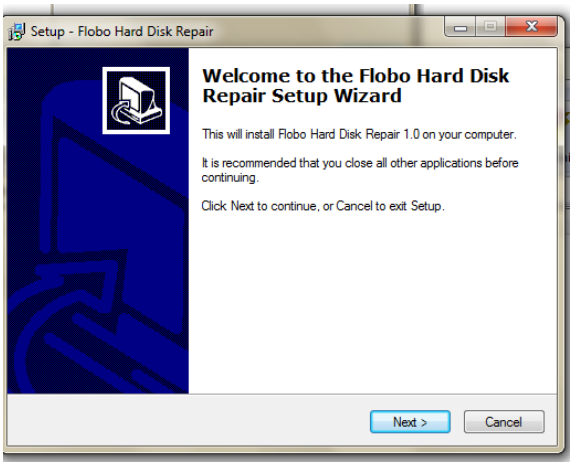
Copiando archives

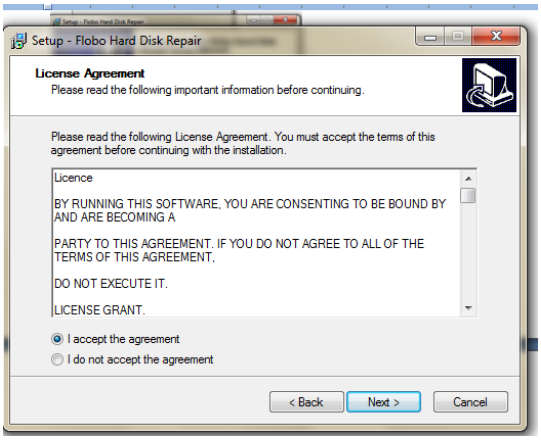


Finalizar

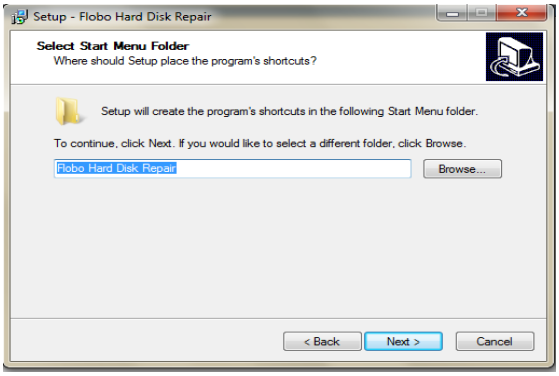
INSTALACIÓN DISK REPAIR

Doble click sobre el ícono setup del Disk Repair





Acuerdo de licencia cick en Next



Next y Finalizar

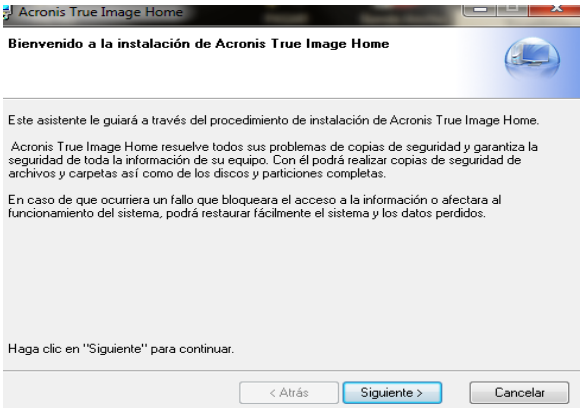
HERRAMIENTAS PARA CREACION DE IMÁGENES LOGICAS

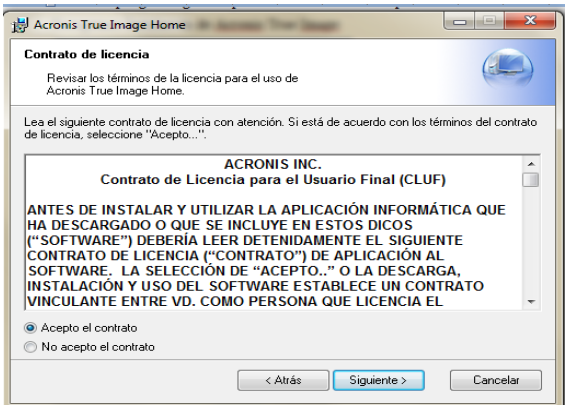
INSTALACIÓN ACRONIS TRUE IMAGE

Doble click sobre el ícono setup del Acronis True Image

Se nos despliega la siguiente pantalla con 4 diferentes opciones

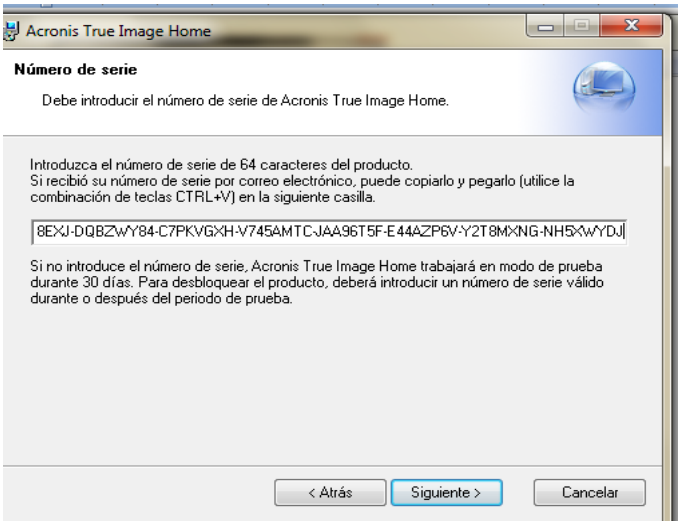
Escogemos Instalación de Acronis True Image



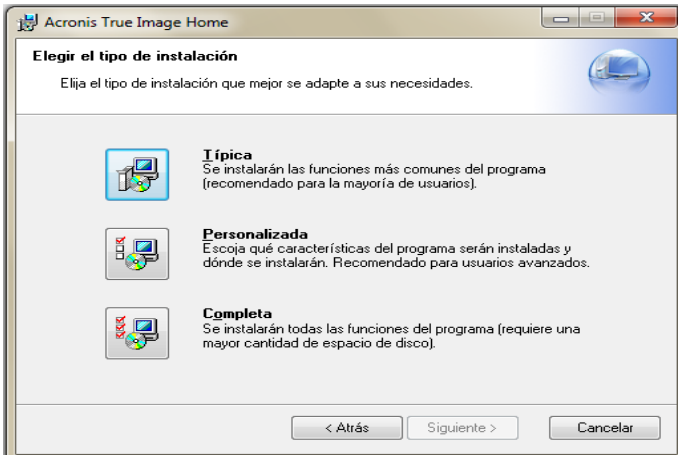


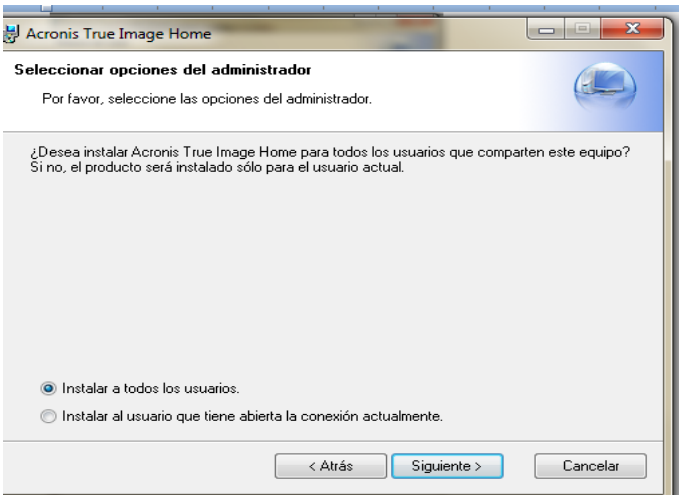
Acuerdo de licencia siguiente

A continuación nos pide la serie del programa pegamos la clave y ponemos siguiente



Escogemos el tipo de instalación Típica en este caso

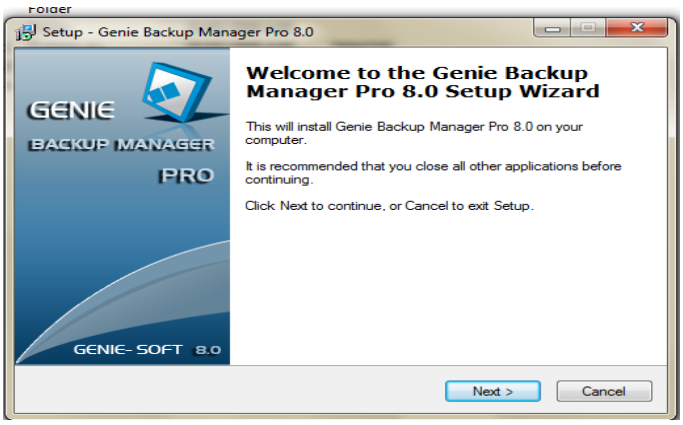




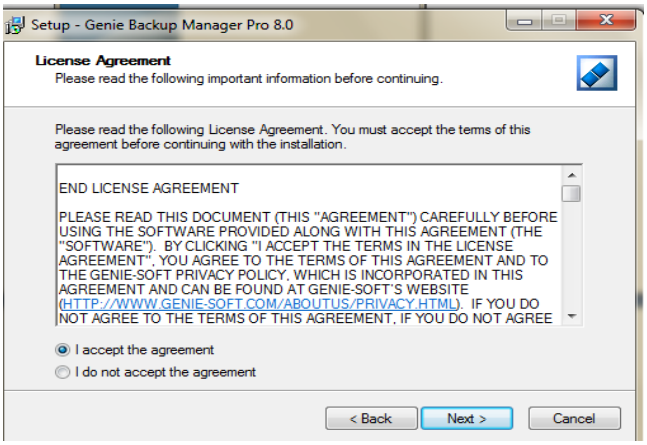
Nos pide reiniciar la computadora para que surjan los cambios efecto

INSTALACIÓN GENIE_BACKUP_MANAGER_PRO_80312482

Doble click sobre el ícono setup **Genie_Backup_Manager_Pro_80312482**

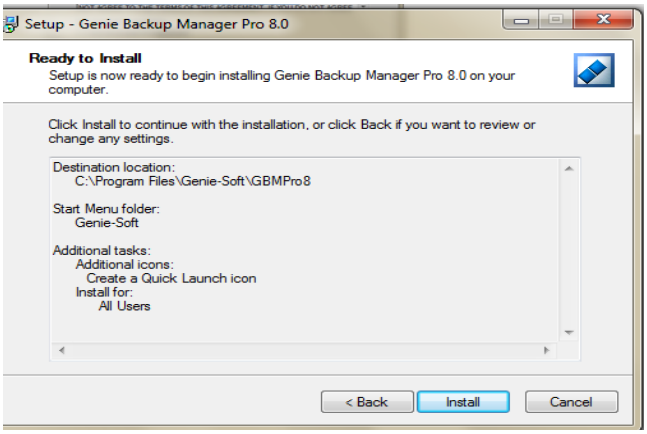


Click en Next

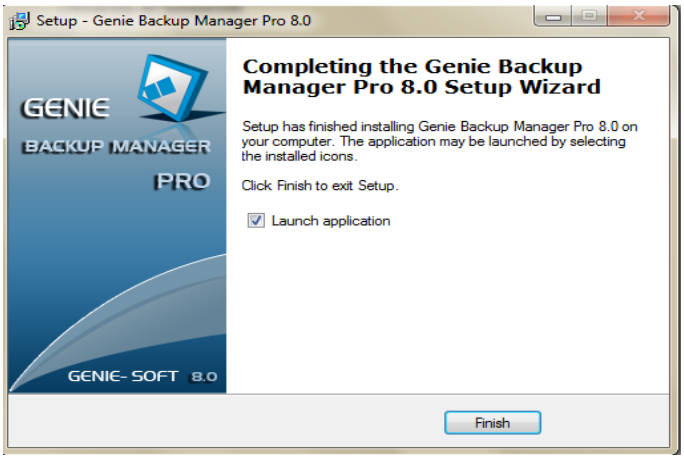


Pantalla Acuerdo de licencia aceptamos Next

Ubicación de instalación



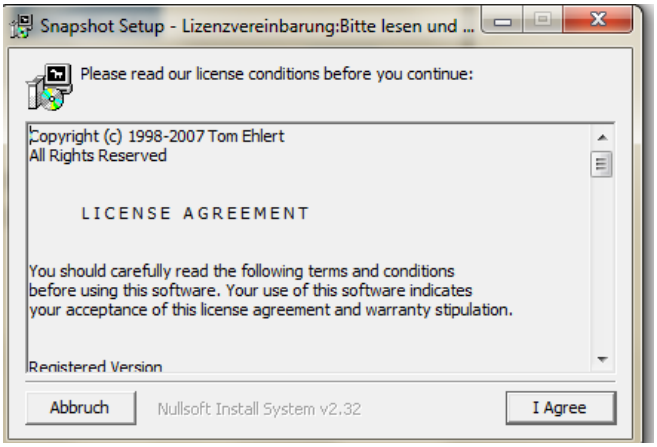
Click en Install



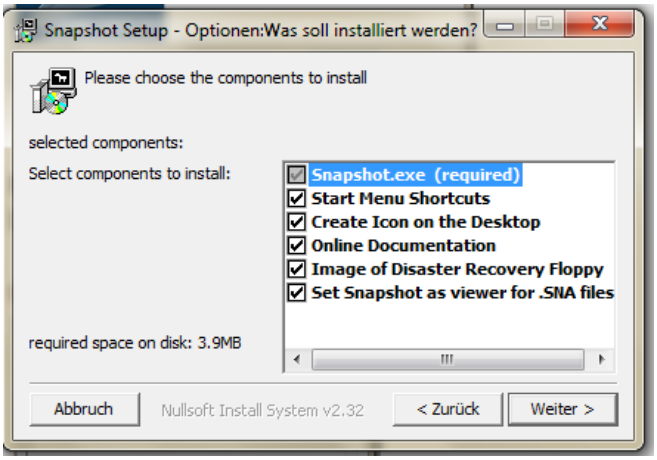
INSTALACIÓN DRIVE SNAPSHOT

Doble click sobre el ícono setup **Drive Snapshot**

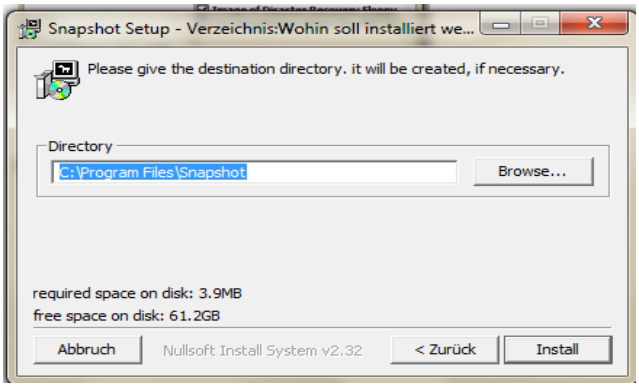
Click in I Agree



Instalación de componentes



Click en Install



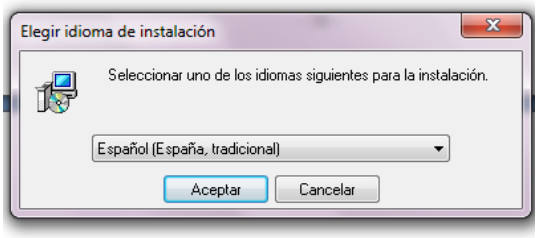
INSTALACIÓN COMANDO DD DE LINUX

Este comando viene instalado con el sistema operativo

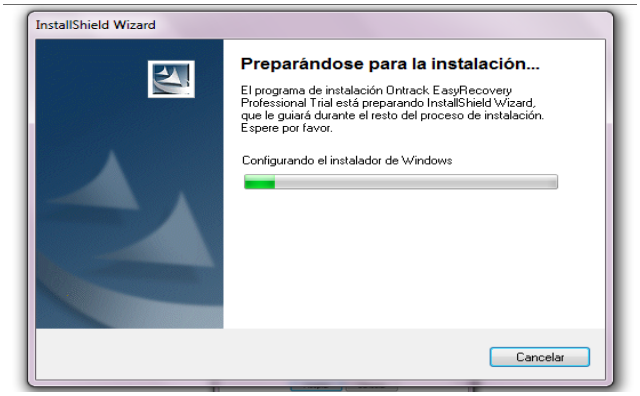
INSTALACIÓN EASY RECOVERY

Doble click sobre el ícono setup del Easy recovery

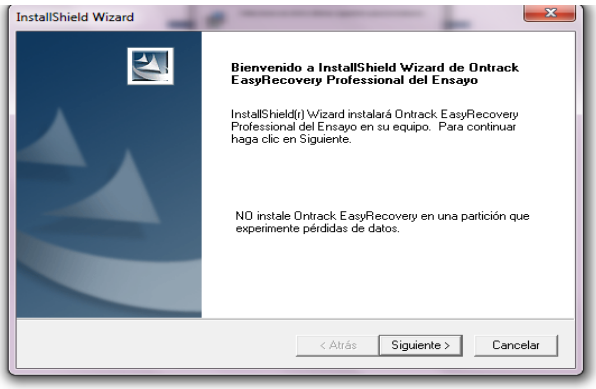
Se despliega una pantalla como la siguiente



Seleccionamos el idioma a continuación click en Aceptar

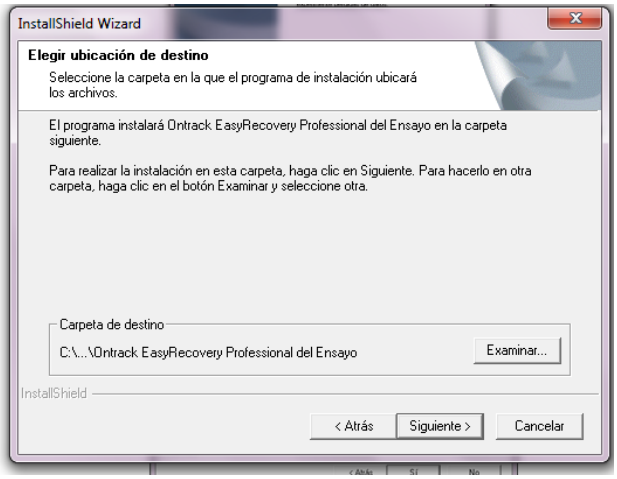


Nos aparece la pantalla en la que se prepara la instalación

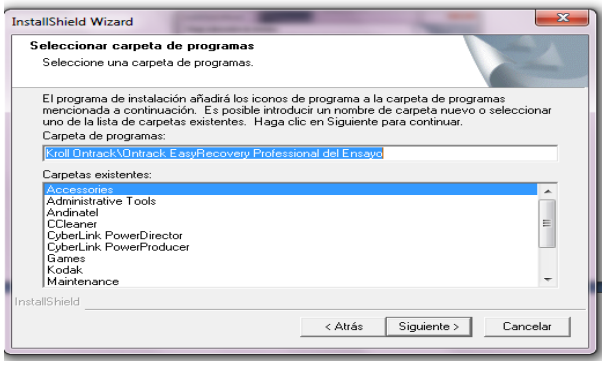


Esta es la pantalla de bienvenido del instalador del EasyReovery a continuación click en siguiente

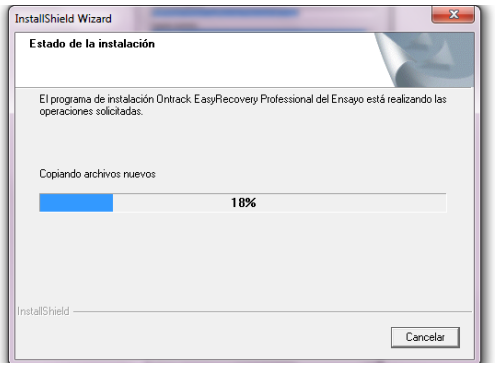
Pantalla del contrato de licencia si está de acuerdo dar click en si



Seleccionamos la ubicación en la que queremos instalar click en siguiente



Pantalla de inicio de copia de archivos click en siguiente



Estado de la instalación

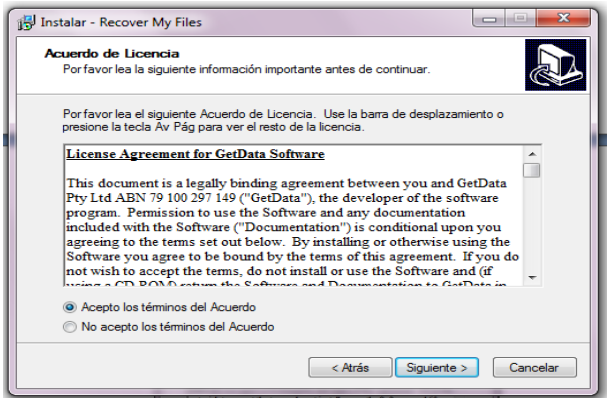
Click en finalizar

INSTALACIÓN RECOVERMYFILES-SETUP

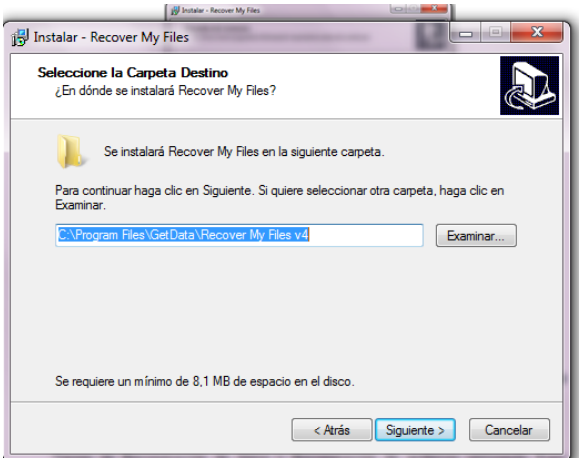
Doble click sobre el ícono setup de RecoverMyFiles-Setup

Se despliega una pantalla como la siguiente

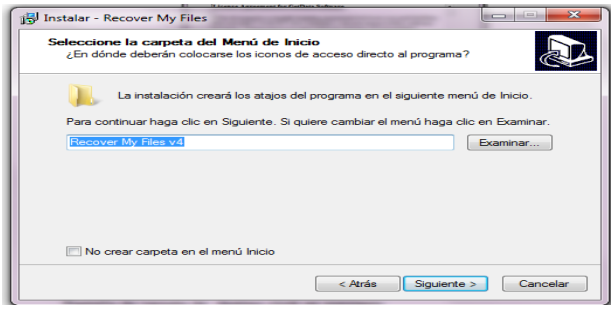
Pantalla de bienvenida a la Instalación click en siguiente



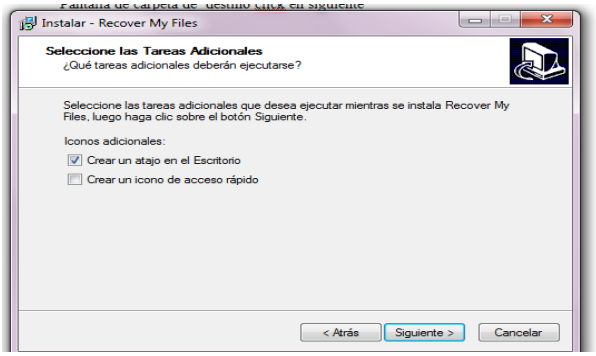
Contrato de licencia Acepto y click en siguiente



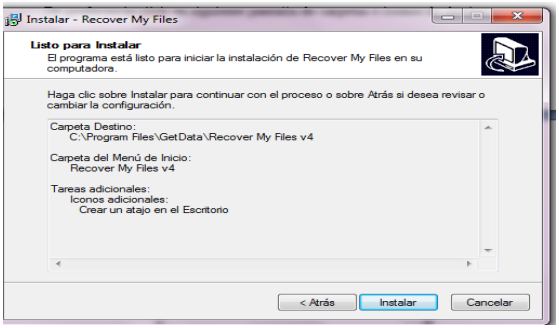
Pantalla de carpeta de destino click en siguiente



De preferencia click en siguiente pantalla de carpetas e iconos de destino



Click en siguiente para creau un acceso directo al escritorio



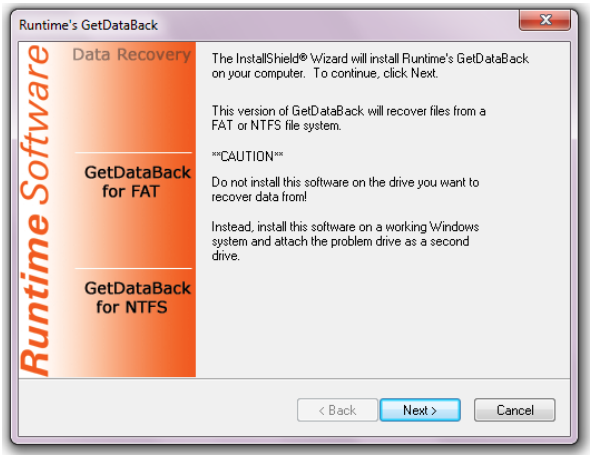
Instalar luego nos aparece la pantalla de culminación

Click en terminar

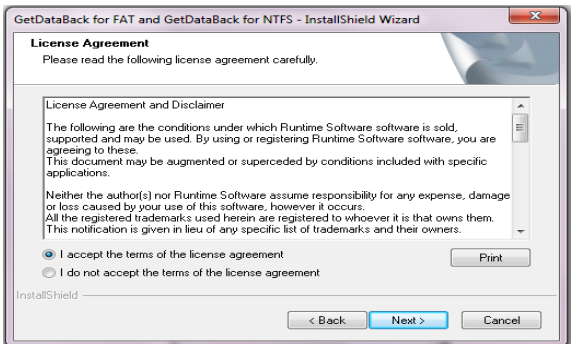
INSTALACIÓN GETDATABACK

Doble click sobre el ícono setup de GetDataBack

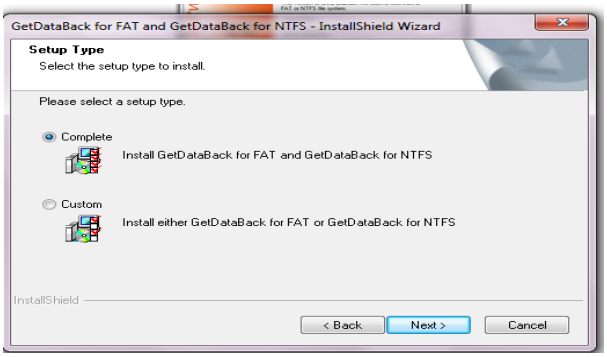
Se despliega una pantalla como la siguiente



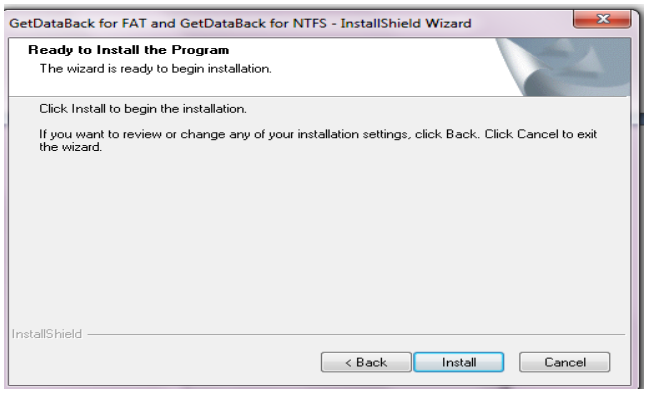
Pantalla en la que nos muestra opciones para FAT y NTFS click en next



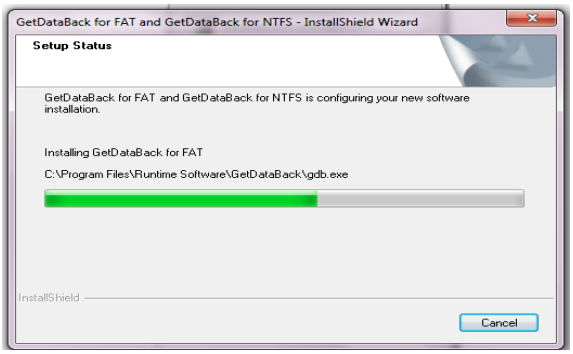
click en next

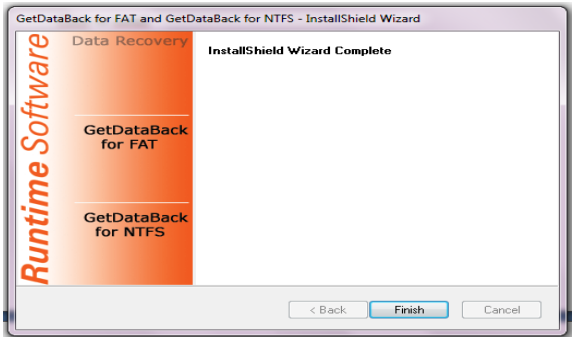


Instalación completa click en next



Click en install



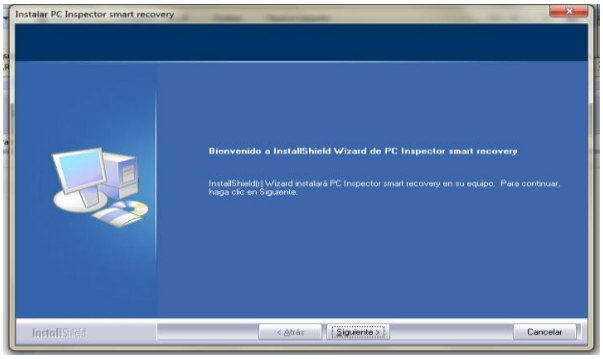


Click en Finish

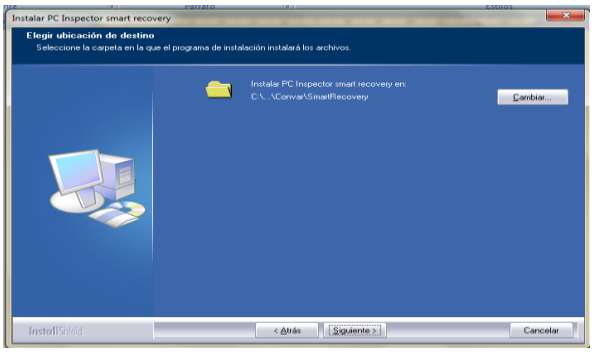
INSTALACION PC INSPECTOR

Doble click sobre el ícono setup de pc Inspector

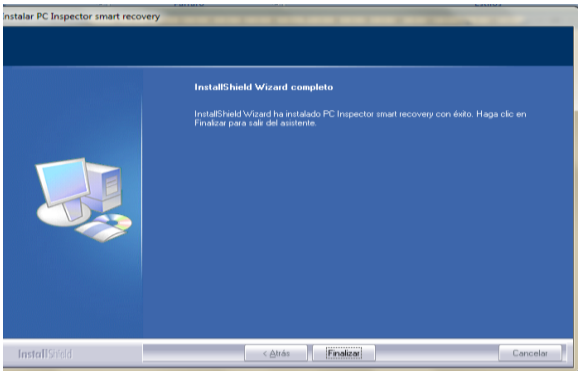
Se despliega una pantalla como la siguiente



Siguiente



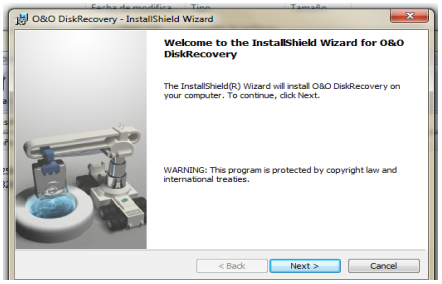
Ubicación de instalación Proceso de grabación y Finalizar



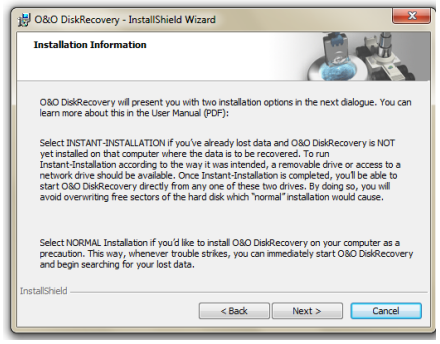
INSTALACION PC O&O DISKRECOVERY

Doble click sobre el ícono setup O&O Diskrecovery

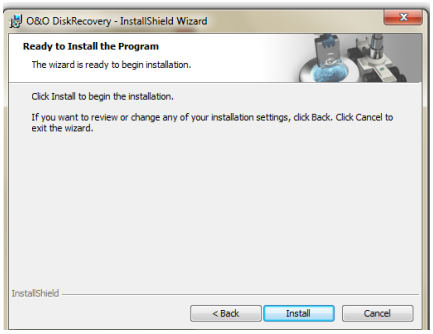
Se despliega una pantalla como la siguiente



Next



Install



Finish

ANEXO B

LEY DE COMERCIO ELECTRONICO LEY ECUATORIANA

EL H. CONGRESO NACIONAL

Considerando:

Que, el uso de sistemas de información y de redes electrónicas, incluida la Internet ha adquirido importancia para el desarrollo del comercio y la producción, permitiendo la realización y concreción de múltiples negocios de trascendental importancia, tanto para el sector público como para el sector privado.

Que, es necesario impulsar el acceso de la población a los servicios electrónicos que se generan por y a través de diferentes medios electrónicos.

Que, se debe generalizar la utilización de servicios de redes de información e Internet, de modo que éstos se conviertan en un medio para el desarrollo del comercio, la educación y la cultura.

Que, a través del servicio de redes electrónicas, incluida la Internet se establecen relaciones económicas y de comercio, y se realizan actos y contratos de carácter civil y mercantil que es necesario normarlos, regularlos y controlarlos, mediante la expedición de una Ley especializada sobre la materia.

Que, es indispensable que el Estado Ecuatoriano cuente con herramientas jurídicas que le permitan el uso de los servicios electrónicos, incluido el comercio electrónico y acceder con mayor facilidad a la cada vez más compleja red de los negocios internacionales.

En uso de sus atribuciones, expide la siguiente:

“LEY DE COMERCIO ELECTRONICO, FIRMAS ELECTRONICAS Y MENSAJES DE DATOS”

TÍTULO PRELIMINAR

Artículo 1.- Objeto de la Ley .- Esta Ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.

TITULO V

DE LAS INFRACCIONES INFORMÁTICAS

CAPÍTULO I

DE LAS INFRACCIONES INFORMATICAS

Artículo 57.- Infracciones Informáticas.- Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente Ley.

Reformas al Código Penal

Artículo 58.- A continuación del Art. 202, inclúyanse los siguientes artículos innumerados:

"Artículo ....- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.

La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, será sancionada con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Artículo ...- Obtención y utilización no autorizada de Información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica.".

Artículo 59.- Sustitúyase el Art. 262 por el siguiente:

"Art. 262.- Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados en razón de su cargo".

Artículo 60.- A continuación del Art. 353, agréguese el siguiente artículo innumerado:

"Art….- Falsificación electrónica.- Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio, alteren o modifiquen mensajes de datos, o la información incluída en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:

1.- Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;
2.- Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;
3.- Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.

El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este Capítulo."

Artículo 61.- A continuación del Art. 415 del Código Penal, inclúyanse los siguientes artículos innumerados:

"Art.....- Daños informáticos.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.

La pena de prisión será de tres a cinco años y multa de doscientos a seis cientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculada con la defensa nacional.

Art. .....- Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seis cientos dólares de los Estados Unidos de Norteamérica.".

Artículo 62.- A continuación del Art. 549, introdúzcase el siguiente artículo innumerado:

"Art.... Apropiación ilícita.- Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

"Art. ….- La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios:

1. Inutilización de sistemas de alarma o guarda;

2. Descubrimiento o descifrado de claves secretas o encriptadas;
3. Utilización de tarjetas magnéticas o perforadas;
4. Utilización de controles o instrumentos de apertura a distancia; y,
5. Violación de seguridades electrónicas, informáticas u otras semejantes.".

Artículo 63.- Añádase como segundo inciso del artículo 563 del Código Penal el siguiente:

"Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando los medios electrónicos o telemáticos".

Artículo 64.- A continuación del numeral 19 del Art. 606 añádase el siguiente:

"..... Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.".

DISPOSICIONES GENERALES

Primera.- Los certificados de firmas electrónicas, emitidos por entidades de certificación extranjeras y acreditados en el exterior, podrán ser revalidados en el Ecuador siempre que cumplan con los términos y condiciones exigidos por la Ley. La revalidación se realizará a través de una entidad de certificación de información acreditada que garantice en la misma forma que lo hace con sus propios certificados, dicho cumplimiento.

Segunda.- Las entidades de certificación de información acreditadas podrán prestar servicios de sellado de tiempo. Este servicio deberá ser acreditado técnicamente por el Consejo Nacional de Telecomunicaciones. El Reglamento de aplicación de la Ley recogerá los requisitos para este servicio.

Tercera.- Adhesión.- Ninguna persona está obligada a usar o aceptar mensajes de datos o firmas electrónicas, salvo que se adhiera voluntariamente en la forma prevista en esta Ley.

Cuarta.- No se admitirá ninguna exclusión restricción o limitación al uso de cualquier método para crear o tratar un mensaje de datos o firma electrónica, siempre que se cumplan los requisitos señalados en la presente Ley y su reglamento.

Quinta.- Se reconoce el derecho de las partes para optar libremente por el uso de tecnología y por el sometimiento a la jurisdicción que acuerden mediante convenio, acuerdo o contrato privado, salvo que la prestación de los servicios electrónicos o uso de estos servicios se realice de forma directa al consumidor.

Sexta.- El Consejo Nacional de Telecomunicaciones tomará las medidas necesarias, para que no se afecten los derechos del titular del certificado o de terceros, cuando se produzca la revocatoria del certificado, por causa no atribuible al titular del mismo.

Séptima.- La prestación de servicios de certificación de información por parte de entidades de certificación de información acreditadas, requerirá de autorización previa y registro.

Octava.- El ejercicio de actividades establecidas en esta ley, por parte de instituciones públicas o privadas, no requerirá de nuevos requisitos o requisitos adicionales a los ya establecidos, para garantizar la eficiencia técnica y seguridad jurídica de los procedimiento e instrumentos empleados.

Novena.- Glorario de Términos.- Para efectos de esta ley los siguientes términos serán entendidos conforme se definen en este artículo:

Mensaje de datos: Es toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que puede ser intercambiada por cualquier medio. Serán considerados como mensajes de datos, sin que esta enumeración limite su definición, los siguientes: documentos electrónicos, registros electrónicos, correo electrónico, servicios web, telegrama, télex, fax e intercambio electrónico de datos.

Red Electrónica de Información: Es un conjunto de equipos y sistemas de información interconectados electrónicamente.

Sistema de información: Es todo dispositivo físico o lógico utilizado para crear, generar, enviar, recibir, procesar, comunicar o almacenar, de cualquier forma, mensajes de datos.

Servicio Electrónico: Es toda actividad realizada a través de redes electrónicas de información.

Comercio Electrónico: Es toda transacción comercial realizada en parte o en su totalidad, a través de redes electrónicas de información.

Intimidad.- El derecho a la intimidad previsto en la Constitución Política de la República, para efectos de esta Ley, comprende también el derecho a la privacidad, a la confidencialidad, a la reserva, al secreto sobre los datos

proporcionados en cualquier relación con terceros, a la no divulgación de los datos personales y a no recibir información o mensajes no solicitados.

Datos personales: Son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta Ley.

Datos personales autorizados: Son aquellos datos personales que el titular ha accedido a entregar o proporcionar de forma voluntaria, para ser usados por la persona, organismo o entidad de registro que los solicita, solamente para el fin para el cual fueron recolectados, el mismo que debe constar expresamente señalado y ser aceptado por dicho titular.

Datos de creación: Son los elementos confidenciales básicos y necesarios para la creación de una firma electrónica.

Certificado electrónico de información: Es el mensaje de datos que contiene información de cualquier tipo.

Dispositivo electrónico: Instrumento físico o lógico utilizado independientemente para iniciar o responder mensajes de datos, sin intervención de una persona al momento de dicho inicio o respuesta.

Dispositivo de emisión.- Instrumento físico o lógico utilizado por el emisor de un documento para crear mensajes de datos o una firma electrónica.

Dispositivo de comprobación: Instrumento físico o lógico utilizado para la validación y autenticación de mensajes de datos o firma electrónica.

Emisor: Persona que origina un mensaje de datos.

Destinatario: Persona a quien va dirigido el mensaje de datos.

Signatario: Es la persona que posee los datos de creación de la firma electrónica, quién, o en cuyo nombre, y con la debida autorización se consigna una firma electrónica.

Desmaterialización electrónica de documentos: Es la transformación de la información contenida en documentos físicos a mensajes de datos.

Quiebra técnica: Es la imposibilidad temporal o permanente de la entidad de certificación de información, que impide garantizar el cumplimiento de las obligaciones establecidas en esta Ley y su reglamento.

Factura electrónica.- Conjunto de registros lógicos archivados en soportes susceptibles de ser leídos por equipos electrónicos de procesamiento de datos que documentan la transferencia de bienes y servicios, cumpliendo los requisitos exigidos por las Leyes Tributarias, Mercantiles y más normas y reglamentos vigentes.

Sellado de tiempo: Anotación electrónica firmada electrónicamente y agregada a un mensaje de datos en la que conste como mínimo la fecha, la hora y la identidad de la persona que efectúa la anotación.

Décima.- Para la fijación de la pena en los delitos tipificados mediante las presentes reformas al Código Penal, contenidas en el Título V de esta Ley. Se tomarán en cuenta los siguientes criterios: el importe de lo defraudado, el quebranto económico causado, los medios empleados y cuantas otras circunstancias existan para valorar la infracción.

DISPOSICIONES TRANSITORIAS

Primera.- Hasta que se dicte el reglamento y más instrumentos de aplicación de esta Ley, la prestación del servicio de sellado de tiempo, deberá cumplir con los requisitos de seguridad e inalterabilidad exigidos para la firma electrónica y los certificados electrónicos.

Segunda.- El cumplimiento del artículo 57 sobre las notificaciones al correo electrónico se hará cuando la infraestructura de la Función Judicial lo permita, correspondiendo al organismo competente de dicha función organizar y reglamentar los cambios que sean necesarios para la aplicación de esta Ley y sus normas conexas.

Para los casos sometidos a Mediación o Arbitraje por medios electrónicos, las notificaciones se efectuarán obligatoriamente en el domicilio judicial electrónico en un correo electrónico señalado por las partes.

DISPOSICIÓN FINAL

El Presidente de la República, en el plazo previsto en la Constitución Política de la República, dictará el reglamento a la presente Ley.

La presente Ley entrará en vigencia a partir de su publicación en el Registro Oficial.

Dado en la ciudad de San Francisco de Quito, Distrito Metropolitano, en la sala de sesiones del Pleno Nacional del Ecuador, a los diez días del mes de abril del año dos mil dos.

ANEXO C

Guía de la Entrevista dirigida a: Administradores de Sistemas, Laboratoristas, Docentes involucrados en el tema de la FISEI-UTA

Datos Generales: Fecha de la Entrevista: ……. Entrevistado: ……...		
Objetivo: Determinar las herramientas de Análisis Forense que se utilizan para la recuperación de información en los dispositivos de almacenamiento en la FISEI - UTA.		
No.	Pregunta	Respuesta
1	¿Qué procedimientos de Análisis Forense utiliza la FISEI-UTA?	- ADQUIRIR EVIDENCIAS ( ) - AUTENTICAR ( ) - ANALISIS DE DATOS SIN MODIFICAR ( ) - RECUPERACIÓN DE INFORMACIÓN ( )
2	¿Qué tipo de Sistema Operativo	- UNIX ( )

	utilizan en la FISEI-UTA?	- LINUX ( ) - WINDOWS ( ) - MAC ( )
3	¿En qué tipo de información se basa la FISEI-UTA en un Proceso judicial?	- NORMAS ISO ( ) - DOCUMENTACIÓN ( ) - INFORME ( ) - NORMAS INTERNAS( )
4	¿Qué herramientas informáticas dispone la FISEI-UTA?	- OPEN SOURCE ( ) - SOFTWARE PROPIETARIO () - DISTRIBUCION LIVE( )
5	¿Qué tipo de información maneja la FISEI-UTA?	- BASE DE DATOS ( ) - ARCHIVOS PLANOS ( ) - OTROS ( )
6	¿Qué tipo de dispositivos de Almacenamiento existe en la FISEI-UTA?	- DISCOS DUROS ( ) - PENDRIVE ( ) - CD/DVD ( ) - CINTA MAGNÉTICA ( ) - TARJETAS DE MEMORIA( )

Elaborado por: Investigador