UNIVERSIDAD NACIONAL AUTONOMA DE NICARAGUA

UNAN - MANAGUA

INFORMATICA FORENSE

LABORATORIO DE COMPUTACION FORENSE PARA EL DEPARTAMENTO DE CRIMINALISTICA DE LA POLICIA NACIONAL DE NICARAGUA.

Tutor

Lic. **Juan de Dios Bonilla**

Autores

Br. Keren Hapuc López Molina
Br. Juan Carlos Vindell Olivas

INDICE

DEDICATORIA Y AGRADECIMIENTOS

A Dios, por brindarnos la dicha de la salud y bienestar físico y espiritual.

A nuestros padres, como agradecimiento a su esfuerzo, amor y apoyo incondicional, durante nuestra formación tanto personal como profesional.

A nuestro docente, por brindarnos su guía y sabiduría en el desarrollo de este trabajo.

Al Personal del departamento de criminalística de la Policía Nacional de Nicaragua por darnos el voto de confianza para trabajar unidos con ellos en pro del desarrollo en nuestro país.

RESUMEN

Con este estudio se logra una primera incursión al mundo de la computación Forense, exponiendo aquellas características y particularidades propias de esta disciplina.

El tema se enfoca desde el punto de vista de las herramientas forenses, con el objetivo de realizar estudios científicos y técnicos en el departamento de criminalística. Aplicando metodologías y procedimientos específicos que permitan asegurar la calidad de las evidencias durante todo el proceso.

Los aspectos esenciales abordados en esta propuesta inician con la instalación de un servidor con soporte de tecnología de virtualización Intel (VT-Tecnología) el cual brindará un servicio de aplicaciones forenses y será utilizado para montar máquinas virtuales, tanto open source como propietario, de acuerdo a los propuestos en esta investigación, este servidor actuará funcionalmente equiparado a un NAS (Network Área Storage) para el almacenamiento de backups, evidencias digitales y reportes técnicos. Asimismo el estudio de este proyecto incluye todos los costos desde hardware, software e infraestructura del laboratorio forense.

INTRODUCCIÓN

La informática forense está adquiriendo una gran importancia dentro del área de la información electrónica, esto debido al aumento del valor de la información y al uso que se le da a ésta, al desarrollo de nuevos espacios donde es usada, y al extenso uso de computadores por parte de las compañías y negocios tradicionales. Resaltando su carácter científico, tiene sus fundamentos en las leyes de la física, de la electricidad y el magnetismo. Es gracias a fenómenos electromagnéticos que la información se puede almacenar, leer e incluso recuperar cuando se creía eliminada. Es por esto que cuando se realiza un crimen, muchas veces la información queda almacenada en forma digital. Sin embargo, existe un gran problema, debido a que los computadores guardan la información de forma tal que no puede ser recolectada o usada como prueba, utilizando medios comunes se deben utilizar mecanismos diferentes a los tradicionales. Es así que surge el estudio de la computación forense como una ciencia relativamente nueva. La informática forense, aplicando procedimientos estrictos y rigurosos puede ayudar a resolver grandes crímenes apoyándose en el método científico, aplicado a la recolección, análisis y validación de todo tipo de pruebas digitales.

Para la actual investigación el departamento de criminalística de la Policía Nacional de Nicaragua, suministró información importante sobre los diferentes delitos informáticos, también facilitaron planos y videos para el estudio de la infraestructura del laboratorio forense. Los instrumentos utilizados para la recolección de la información fueron observación, encuestas y entrevistas. Además en este estudio se logra dar un aporte al desarrollo Jurídico, tecnológico, cultural y social.

PLANTEAMIENTO DEL PROBLEMA

Formulación del Problema

El departamento de criminalística de la Policía Nacional de Nicaragua en la actualidad no posee un laboratorio de computación forense. Por lo tanto se ha considerado conveniente plantear la propuesta de un laboratorio forense, el cual reúna las condiciones ambientales, técnicas, operacionales y las herramientas adecuadas de hardware y software. Nuestro proyecto está enfocado a dar respuesta a la siguiente problemática.

¿Cómo se puede ayudar a los peritos informáticos a ampliar los estudios científicos y técnicos de una investigación?

JUSTIFICACIÓN DEL ESTUDIO

Con el presente proyecto se alcanzará una mejor visión del delito informático, Además, el desarrollo de la actual investigación permite ampliar los estudios científicos y técnicos utilizando herramientas forenses de hardware y software. Así mismo profundizar en la búsqueda de información para el esclarecimiento de los casos. Aportar estrategias de búsqueda de evidencia a través de la red, obtener evidencias claras que ayuden al cumplimiento de la ley informática.

Por lo tanto, este estudio será de gran utilidad, sobre todo hoy en día, cuando estamos comunicados mediante las redes de la Internet y la computadora se ha vuelto parte de nuestra vida social, publica, económica, cultural y política.

ANTECEDENTES

En Nicaragua, no hay antecedentes de un laboratorio de computación forense, sin embargo el departamento de criminalística de la Policía Nacional ha utilizado la informática para realizar estudios científicos y tecnológicos en delitos generales.

Algunas de las herramientas mencionada por parte del departamento fueron **Recovey manager**, **Recovery file, Toolkit, phine**, etc. Siendo estos los que abren paso para demostrar a través de nuestro estudio la utilidad de las herramientas forense.

En el contexto internacional, son pocos los países que cuentan con un laboratorio y una legislación apropiada. Entre ellos, se destacan: Estados Unidos, Alemania, Austria, Gran Bretaña, Holanda, Francia, España, Argentina y Chile.

ESTADOS UNIDOS

Este país adoptó en 1994 el Acta Federal de Abuso Computacional que modificó al Acta de Fraude y Abuso Computacional de 1986. Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y que no es un virus, un gusano, un caballo de Troya y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, a los sistemas informáticos, a las redes, información, datos o programas. La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus.

Asimismo, en materia de estafas electrónicas, defraudaciones y otros actos dolosos relacionados con los dispositivos de acceso a sistemas informáticos, la legislación estadounidense sanciona con pena de prisión y multa, a la persona que defraude a otro mediante la utilización de una computadora o red informática.

En el mes de Julio del año 2000, el Senado y la Cámara de Representantes de este país -tras un año largo de deliberaciones- establece el Acta de Firmas Electrónicas en el Comercio

Global y Nacional. La ley sobre la firma digital responde a la necesidad de dar validez a documentos informáticos -mensajes electrónicos y contratos establecidos mediante Internet- entre empresas (para el B2B) y entre empresas y consumidores (para el B2C).

Alemania

Este país sancionó en 1986 la Ley contra la Criminalidad Económica, que contempla los siguientes delitos:

- Espionaje de datos.
- Estafa informática.
- Alteración de datos.
- Sabotaje informático.

Austria

La Ley de reforma del Código Penal, sancionada el 22 de Diciembre de 1987, sanciona a aquellos que causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes comenten este hecho utilizando su profesión de especialistas en sistemas.

Gran Bretaña

Debido a un caso de hacking en 1991, comenzó a regir en este país la ComputerMisuseAct (Ley de Abusos Informáticos). Mediante esta ley el intento, exitoso o no, de alterar datos informáticos es penado con hasta cinco años de prisión o multas. Esta ley tiene un apartado que específica la modificación de datos sin autorización.

Holanda

El 1º de Marzo de 1993 entró en vigencia la Ley de Delitos Informáticos, en la cual se penaliza los siguientes delitos:

- El hacking.
- El preacking (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio).

- La ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría).
- La distribución de virus.

Francia

En enero de 1988, este país dictó la Ley relativa al fraude informático, en la que se consideran aspectos como:

- Intromisión fraudulenta que suprima o modifique datos.
- Conducta intencional en la violación de derechos a terceros que haya impedido o alterado el funcionamiento de un sistema de procesamiento automatizado de datos.
- Conducta intencional en la violación de derechos a terceros, en forma directa o indirecta, en la introducción de datos en un sistema de procesamiento automatizado o la supresión o modificación de los datos que éste contiene, o sus modos de procesamiento o de transmisión.
- Supresión o modificación de datos contenidos en el sistema, o bien en la alteración del funcionamiento del sistema (sabotaje).

España

En el Nuevo Código Penal de España, se establece que al que causare daños en propiedad ajena, se le aplicará pena de prisión o multa. En lo referente a:

- La realización por cualquier medio de destrucción, alteración, inutilización o cualquier otro daño en los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.
- El nuevo Código Penal de España sanciona en forma detallada esta categoría delictual (Violación de secretos/Espionaje/Divulgación), aplicando pena de prisión y multa.
- En materia de estafas electrónicas, el nuevo Código Penal de España, solo tipifica las estafas con ánimo de lucro valiéndose de alguna manipulación informática, sin detallar las penas a aplicar en el caso de la comisión del delito.

Chile

Chile fue el primer país latinoamericano en sancionar una Ley contra delitos informáticos, la cual entró en vigencia el 7 de junio de 1993. Esta ley se refiere a los siguientes delitos:

- La destrucción o inutilización de los de los datos contenidos dentro de una computadora es castigada con penas de prisión. Asimismo, dentro de esas consideraciones se encuentran los virus.
- Conducta maliciosa tendiente a la destrucción o inutilización de un sistema de tratamiento de información o de sus partes componentes o que dicha conducta impida, obstaculice o modifique su funcionamiento.
- Conducta maliciosa que altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.

OBJETIVO GENERAL

Elaborar propuesta de creación de un Laboratorio de Computación forense para el departamento de criminalística de la Policía Nacional de Nicaragua en el año 2011.

OBJETIVOS ESPECÍFICOS.

1. Determinar Herramientas de Hardware y software que apoyen el Análisis Forense en los delitos informáticos.
2. Determinar las condiciones ambientales, técnicas y operacionales para el laboratorio de computación forense.
3. Ampliar los estudios científicos y técnicos en apoyo a los procesos de investigación criminalística.

MARCO TEÓRICO

En el marco teórico se desarrolla un cuadro conceptual que tiene los elementos más importantes del Laboratorio Forense. Igualmente se definen los conceptos propios de dicha ciencia.

CIENCIAS FORENSES

Las ciencias forenses son la utilización de procedimientos y conocimientos científicos para encontrar, adquirir, preservar y analizar las evidencias de un delito y presentarlas apropiadamente a una corte de justicia. Tienen que ver principalmente con la recuperación y análisis de la llamada evidencia latente, ejemplo las huellas digitales, la comparación de muestras de ADN. Combinan el conocimiento científico y las diferentes técnicas que este proporciona con los presupuestos legales a fin de demostrar con la evidencia recuperada la existencia de la comisión de un acto considerado como delictivo y sus posibles responsables ante un tribunal de justicia.

Las ciencias forenses han sido desarrolladas desde hace mucho tiempo a tras uno de los primeros textos y estudios en este campo lo podemos ubicar en el año 1248 DC, cuando el médico chino, HI DUANYU, escribió el libro **"COMO CORREGIR LOS ERRORES**" en el cual se practican las diferencias entre una muerte por ahogamiento y otro por una herida de arma blanca al igual que la muerte por causa naturales.

Posteriormente con el avance de la ciencia y la tecnología las ciencias forenses han alcanzado un desarrollo inconmensurable, pero ese desarrollo a veces no ha ido de la mano del avance de la legislación penal. Esto en razón del retraso de la incorporación de nuevos elementos de prueba y medios probatorios y sobre todo en la demora de la admisibilidad de nuevas evidencias o pruebas. Esto es el caso de la prueba de ADN que fue admitida en un juicio recién en el año de 1996, pero su desarrollo y comprensión se logró desde la década de los ochentas.

1. Introducción a la informática forense. Consultada el 13 de noviembre de 2010, de http://www.alfa-redi.com/apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/Acurio.pdf

También nos proporciona los principios y técnicas que facilitan la investigación del delito criminal, en otras palabras: cualquier principio o técnica que puede ser aplicada para identificar, recuperar, reconstruir o analizar la evidencia durante una investigación criminal forma parte de la ciencia forense.

Los principios científicos que hay detrás del procesamiento de una evidencia son reconocidos y usados en procedimientos como:

- ✓ Recoger y examinar huellas dactilares y ADN.
- ✓ Recuperar documentos de un dispositivo dañado.
- ✓ Hacer una copia exacta de una evidencia digital.
- ✓ Generar una huella digital con un algoritmo hash MD5 o SHA1 de un texto para asegurar que este no se ha modificado.
- ✓ Firmar digitalmente un documento para poder afirmar que es auténtico y preservar la cadena de evidencias.

Un forense aporta su entrenamiento para ayudar a los investigadores a reconstruir el crimen y encontrar pistas. Aplicando un método científico analiza las evidencias disponibles, crea hipótesis sobre lo ocurrido para crear la evidencia y realiza pruebas, controles para confirmar o contradecir esas hipótesis. Esto puede llevar a una gran cantidad de posibilidades sobre lo que pudo ocurrir, esto es debido a que un forense no puede conocer el pasado, no puede saber qué ocurrió ya que sólo dispone de una información limitada. Por esto, sólo puede presentar posibilidades basadas en la información limitada que posee.

Un principio fundamental en la ciencia forense, que usaremos continuamente para relacionar un criminal con el crimen que ha cometido, es el Principio de Intercambio o transferencia de Locard, (EdmondLocard, francés fundador del instituto de criminalística de la universidad de Lion, podemos ver el esquema

Fig. 1 principio de Lorcard

PRINCIPIO DE TRANSFERENCIA DE LOCARD.

Este principio fundamental viene a decir que cualquiera o cualquier objeto que entra en la escena del crimen deja un rastro en la escena o en la víctima y vice-versa (se lleva consigo), en otras palabras: "cada contacto deja un rastro". En el mundo real significa que si piso la escena del crimen con toda seguridad dejaré algo mío ahí, pelo, sudor, huellas, etc. Pero también me llevaré algo conmigo cuando abandone la escena del crimen, ya sea barro, olor, una fibra, etc. Con algunas de estas evidencias, los forenses podrán demostrar que hay una posibilidad muy alta de que el criminal estuviera en la escena del crimen.

EL PRINCIPIO DE INTERCAMBIO DE LOCARD SE PUEDE RESUMIR ASÍ:

- ✓ El sospechoso se llevará lejos algún rastro de la escena y de la víctima.
- ✓ La víctima retendrá restos del sospechoso y puede dejar rastros de sí mismo en el sospechoso.
- ✓ El sospechoso dejará algún rastro en la escena.

El objetivo es establecer una relación entre los diferentes componentes:

- la escena del crimen
- la víctima
- la evidencia física
- el sospechoso

Para la correcta resolución del caso, todos estos componentes deben estar relacionados. Esto se conoce como el **concepto de relación**. Las evidencias pueden, a su vez, ser transferidas de dos formas distintas:

- Transferencia directa: cuando es transferida desde su origen a otra persona u objeto de forma directa.
- Transferencia indirecta: cuando es transferida directamente a una localización y, de nuevo, es transferida a otro lugar.

Importante resaltar que cualquier cosa y todo puede ser una evidencia. Brevemente, la ciencia forense facilita las herramientas, técnicas y métodos sistemáticos (pero científicos) que pueden ser usados para analizar una evidencia digital y usar dicha evidencia para reconstruir qué ocurrió durante la realización del crimen con el último propósito de relacionar al autor, a la víctima y la escena del crimen.

2. Informática forense. Consultada el 10 de noviembre de 2010, de http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf

¿QUÉ ES LA INFORMÁTICA FORENSE?

La Informática Forense consiguió atención durante el escándalo de Enron, por ser la investigación más grande de Informática Forense hasta la presente fecha. Hoy en día la Informática Forense y el descubrimiento electrónico se está convirtiendo en estándar de juicios y pleitos legales de todos los tipos, especialmente pleitos grandes juicios que implican materias corporativas con gran cantidad de datos.

La IF (Informática Forense) también llamado cómputo forense es el proceso de investigar dispositivos electrónicos o computadoras con el fin de descubrir y de analizar información disponible, suprimida, u ocultada que puede servir como evidencia en un asunto legal. Es Igualmente provechosa cuando se han perdido accidentalmente datos debido a fallas.

Esta ciencia se ocupa de la utilización de los métodos científicos aplicables a la investigación de los delitos informáticos.

Además recolecta y utiliza la evidencia digital para casos de delitos informáticos y para otro tipo de crímenes usando técnicas y tecnologías avanzadas. Un experto en informática forense utiliza estas técnicas para descubrir evidencia de un dispositivo de almacenaje electrónico. Los datos pueden ser de cualquier clase de dispositivo electrónico como discos duros, cintas de respaldo, computadores portátiles, memorias extraíbles, archivos y correos electrónicos.

Esta disciplina hace uso no solo de tecnología de punta para poder mantener la integridad de los datos y del procesamiento de los mismos; sino que también requiere de una especialización y conocimientos avanzados.

La importancia de éstos y el poder mantener su integridad se basa en que la evidencia digital o electrónica es sumamente frágil. El simple hecho de darle doble clic a un archivo modificaría la última fecha de acceso del mismo.

Las herramientas modernas y el software hacen la Informática Forense mucho más fácil para los expertos forenses ya que permite encontrar y restaurar evidencia más rápido y con más exactitud.

La mayoría de los usuarios pensamos que al borrar un archivo se quitará totalmente la información del disco duro. En realidad se quita solamente el archivo de localización, pero el archivo real todavía queda en su computadora.

También la informática forense es el vehículo idóneo para localizar y presentar de forma adecuada los hechos jurídicos informáticos relevantes dentro de una investigación, ya sea de carácter civil o penal.

En conclusión diremos que la informática forense es la ciencia forense que se encarga de la preservación, identificación, extracción, documentación e interpretación de la evidencia digital, para luego esta ser presentada en una corte de justicia.

3. Que es la informática forense. Consultada el 05 de noviembre de 2010, de http://www.informaticaforense.com/criminalistica/faqs/general/que-es-la-informatica-forense.html
1. Introducción a la informática forense. Consultada el 13 de noviembre de 2010, de http://www.alfa-redi.com/apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/Acurio.pdf

OBJETIVOS DE LA INFORMÁTICA FORENSE

La informática forense tiene 3 objetivos, a saber:

- ✓ La compensación de los daños causados por los criminales o intrusos.
- ✓ La persecución y procesamiento judicial de los criminales.
- ✓ La creación y aplicación de medidas para prevenir casos similares.

Estos objetivos son logrados de varias formas, entre ellas, la principal es la Recolección de evidencia.

USOS DE LA INFORMÁTICA FORENSE

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

- ✓ **Prosecución Criminal:** Evidencia incriminatoria puede ser usada para procesar una variedad de crímenes, incluyendo homicidios, fraude financiero, tráfico y venta de drogas, evasión de impuestos o pornografía infantil.
- ✓ **Litigación Civil:** Casos que tratan con fraude, discriminación, acoso, divorcio, Pueden ser ayudados por la informática forense.
- ✓ **Temas corporativos:** Puede ser recolectada información en casos que tratan sobre acoso sexual, robo, mal uso o apropiación de información confidencial o Propietaria, o aún de espionaje industrial.

TIPOS DE EVIDENCIAS

- ✓ **EVIDENCIAS FÍSICAS**

- **Evidencia transitoria**: como su nombre indica es temporal por naturaleza, por ejemplo un olor, la temperatura, o unas letras sobre la arena o nieve (un objeto blando o cambiante).
- **Evidencia curso o patrón**: producidas por contacto, por ejemplo la trayectoria de una bala, un patrón de rotura de un cristal, patrones de posicionamiento de muebles, etc.
- **Evidencia condicional**: causadas por una acción o un evento en la escena del crimen, por ejemplo la localización de una evidencia en relación con el cuerpo, una ventana abierta o cerrada, una radio encendida o apagada, dirección del humo, etc.
- **Evidencia transferida**: generalmente producidas por contacto entre personas, entre objetos o entre personas y objetos.

En la práctica las evidencias transferidas se dividen en dos tipos, conocidas como:

- Transferencia por **rastro**: aquí entra la sangre, semen, pelo, etc.
- Transferencia por **huella**: huellas de zapato, dactilares, etc.

Aunque en la realidad, estas últimas suelen mezclarse, por ejemplo una huella de zapato sobre un charco de sangre.

- ✓ **EVIDENCIA DIGITAL**

Casey define la evidencia digital como "cualquier dato que puede establecer que un crimen se ha ejecutado o puede proporcionar un enlace entre un crimen y su víctima o un crimen y su autor.

La evidencia computacional es única, cuando se la compara con otras formas de "evidencia documental". A diferencia de la documentación en papel, la evidencia computacional es frágil y una copia de un documento almacenado en un archivo es idéntica al original. Otro aspecto único de la evidencia computacional es el potencial de realizar copias no autorizadas de archivos, sin dejar rastro de que se realizó una copia. Esta situación crea problemas concernientes a la investigación del robo de secretos comerciales, como listas de clientes, material de investigación, archivos de diseño asistidos por computador, fórmulas y software propietario. Debe tenerse en cuenta que los datos digitales adquiridos de copias no se deben alterar de los originales del disco, porque esto invalidaría la evidencia; por esto los investigadores deben revisar con frecuencia que sus copias sean exactas a las del disco del sospechoso, para esto se utilizan varias tecnologías, como por ejemplo.

ChecksumsohashMD5.

CARACTERÍSTICAS QUE POSEE LA EVIDENCIA DIGITAL.

- ✓ La evidencia de Digital puede ser duplicada de forma exacta y se puede sacar una copia para ser examinada como si fuera la original. Esto se hace comúnmente para no manejar los originales y evitar el riesgo de dañarlos.
- ✓ Actualmente, con las herramientas existentes, es muy fácil comparar la evidencia digital con su original, y determinar si la evidencia digital ha sido alterada.

- ✓ La evidencia Digital es muy difícil de eliminar. Aun cuando un registro es borrado del disco duro del computador, y éste ha sido formateado, es posible recuperarlo.
- ✓ Cuando los individuos involucrados en un crimen tratan de destruir la evidencia, existen copias que permanecen en otros sitios.

CLASIFICACIÓN DE LA EVIDENCIA DIGITAL

Cano clasifica la evidencia digital que contiene texto en 3 categorías

- ✓ Registros generados por computador: Estos registros son aquellos, que como dice su nombre, son generados como efecto de la programación de un computador. Los registros generados por computador son inalterables por una persona. Estos registros son llamados registros de eventos de seguridad (logs) y sirven como prueba tras demostrar el correcto y adecuado funcionamiento del sistema o computador que generó el registro.

- ✓ Registros no generados sino simplemente almacenados por o en computadores: Estos registros son aquellos generados por una persona, y que son almacenados en el computador, por ejemplo, un documento realizado con un procesador de palabras. En estos registros es importante lograr demostrar la identidad del generador, y probar hechos o afirmaciones contenidas en la evidencia misma. Para lo anterior se debe demostrar sucesos que muestren que las afirmaciones humanas contenidas en la evidencia son reales.

- ✓ Registros híbridos que incluyen tanto registros generados por computador como almacenados en los mismos: Los registros híbridos son aquellos que combinan afirmaciones humanas y logs. Para que estos registros sirvan como prueba deben cumplir los dos requisitos anteriores.

MANIPULACIÓN DE LA EVIDENCIA DIGITAL

Es importante tener presente los siguientes requisitos que se deben cumplir en cuanto a la manipulación de la evidencia digital.

- ✓ Hacer uso de medios forenses estériles (para copias de información)
- ✓ Mantener y controlar la integridad del medio original. Esto significa, que a la hora de recolectar la evidencia digital, las acciones realizadas no deben cambiar nunca esta evidencia.
- ✓ Cuando sea necesario que una persona tenga acceso a evidencia digital forense, esa persona debe ser un profesional forense.
- ✓ Las copias de los datos obtenidas, deben estar correctamente marcadas, controladas y preservadas. Y al igual que los resultados de la investigación, deben estar disponibles para su revisión.
- ✓ Siempre que la evidencia digital este en poder de algún individuo, éste será responsable de todas la acciones tomadas con respecto a ella, mientras esté en su poder.
- ✓ Las agencias responsables de llevar el proceso de recolección y análisis de la evidencia digital, serán quienes deben garantizar el cumplimiento de los principios anteriores.

GESTIÓN DE LA EVIDENCIA DIGITAL

Existen gran cantidad de guías y buenas prácticas que nos muestran como llevar a cabo la gestión de la evidencia digital Las guías que se utilizan tienen como objetivo identificar evidencia digital con el fin de que pueda ser usada dentro de una investigación. Estas guías se basan en el método científico para concluir o deducir algo acerca de la información. Presentan una serie de etapas para recuperar la mayor cantidad de fuentes digitales con el fin de asistir en la reconstrucción posterior de eventos.

4. **Informática forense. Consultada el 10 de noviembre de 2010, de http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf**

TECNICAS EN FORENSIA DIGITAL

Las técnicas de forense son la aplicación de una técnica de investigación metódica para reconstruir una secuencia de eventos. Las técnicas de forense digital son el arte de recrear que ha pasado en un dispositivo digital. Existen dos aspectos de estas técnicas:

- ✓ que ha hecho la gente en su computador, esto incluye:
  - La recuperación de archivos eliminados es elemental
  - Búsqueda de cierto tipo de archivos
  - Búsqueda de ciertas fases
  - Observación de áreas interesantes del computador
- ✓ que ha hecho un usuario remoto en la computadora de alguien más. Esto incluye:
  - Leer archivos de registro
  - Reconstruir acciones
  - Rastrear el origen

FUENTES DE LA EVIDENCIA DIGITAL

Algunas personas tienden a confundir los términos evidencia digital y evidencia electrónica, dichos términos pueden ser usados indistintamente como sinónimos, sin embargo es necesario distinguir entre aparatos electrónicos como los celulares los PDAs. Y la información digital que estos contengan esto es indispensable ya que el foco de nuestra investigación siempre será la evidencia digital aunque en algunos casos también serán los aparatos electrónicos.

Las fuentes de evidencias digitales pueden ser clasificadas en tres grandes grupos

- ✓ **Sistema de computación abiertos,** son aquellos que están compuestos de las computadoras personales y todos sus periféricos como teclados, ratones y monitores, las computadoras portátiles y servidores. estos se convierten en una

gran fuente de evidencia digital debido a que en sus discos duros guardan grandes volúmenes de información.

- ✓ **Sistemas de comunicación,** estos están compuestos por las redes de telecomunicaciones, la comunicación inalámbrica y el Internet. Son también una gran fuente de información y de evidencia digital.

- ✓ **Sistema convergente de computación,** en un principio el tipo de evidencia digital que se buscaba en los equipos informáticos era del tipo **CONSTANTE O PERSISTENTE** es decir la que se encontraba almacenada en disco duro o en otro medio informático y que se mantenía preservada después de que la computadora era apagada. Posteriormente y gracias a las redes de interconexión el investigador forense se ve obligado a buscar también evidencias del tipo VOLATIL, es decir evidencias que se encuentran alojadas temporalmente en la memoria RAM, o en le CACHE, son evidencia que por su naturaleza inestable se pierden cuando el computador es apagado. Este tipo de evidencia deben ser recuperados casi de inmediato.

De lo planteado anteriormente se desprende que cuando se comete un delito cualquiera, muchas veces la información que directa o indirectamente se relaciona con esta conducta criminal queda almacenada en forma digital dentro de un sistema informático.

Este conjunto de datos ordenados sistemáticamente y convertidos en información se convierte en evidencia digital. He aquí que encontramos la primera dificultad en lo que se refiere la obtención de esta clase de evidencia como prueba de la infracción cometida, esto debido a que los sistemas informáticos en donde se almacena la misma.

Presentan características técnicas propias, en tal razón la información ahí almacenada no puede ser recuperada, recolectada, preservada, procesada y posteriormente presentada como indicio de convicción utilizando los medios criminalísticos comunes, se debe utilizar mecanismos diferentes a los tradicionales es entonces donde se ve la necesidad de utilizar los procedimientos técnicos legales y la rigurosidad científica que pone a disposición de

los investigadores la ciencia forense informática a fin de descubrir a los autores y cómplices del delito cometido.

La falta de información especializada en esta área de investigación científica, la existencia práctica, y entrenamiento en la obtención recolección, documentación y posterior análisis e interpretación de la evidencia digital, puede permitir que se condene a un inocente y se deje libre a un culpable.

LA DINÁMICA DE LA EVIDENCIA

La dinámica de la evidencia es la forma como se entienden y se describen los diferentes factores (humanos, de la naturaleza de los equipos) que actúan sobre las evidencias, a fin de determinar los cambios que estos producen sobre ellas.

Podemos afirmar indudablemente que existen muchos agentes que intervienen o actúan sobre la evidencia digital aquí se aplica el llamado principio de intercambio o de locard el investigador forense se ve en la necesidad de reconocer la forma como estos forenses pueden alterar la evidencia, y así tener la oportunidad de manejarla de una manera apropiada, evitando generalmente contaminarla, dañarla y hasta perderla por completo.

Los principios de criminalística, como el de locard o de intercambio y el mismísidad deben tenerse como instrumentos de la investigación de cualquier escena del crimen exclusive la informática.

Estos se pueden explicar por ejemplo en el caso de las bitácoras o LOGS del sistema operativo de un equipo informático utilizado por un Hacker o Cracker para romper las seguridades de un programa o vulnerar la integridad de un sistema informático remoto.

En dicha bitácora el investigador podría encontrar registrada dicha actividad legal. Este es un ejemplo del principio de intercambio en acción.

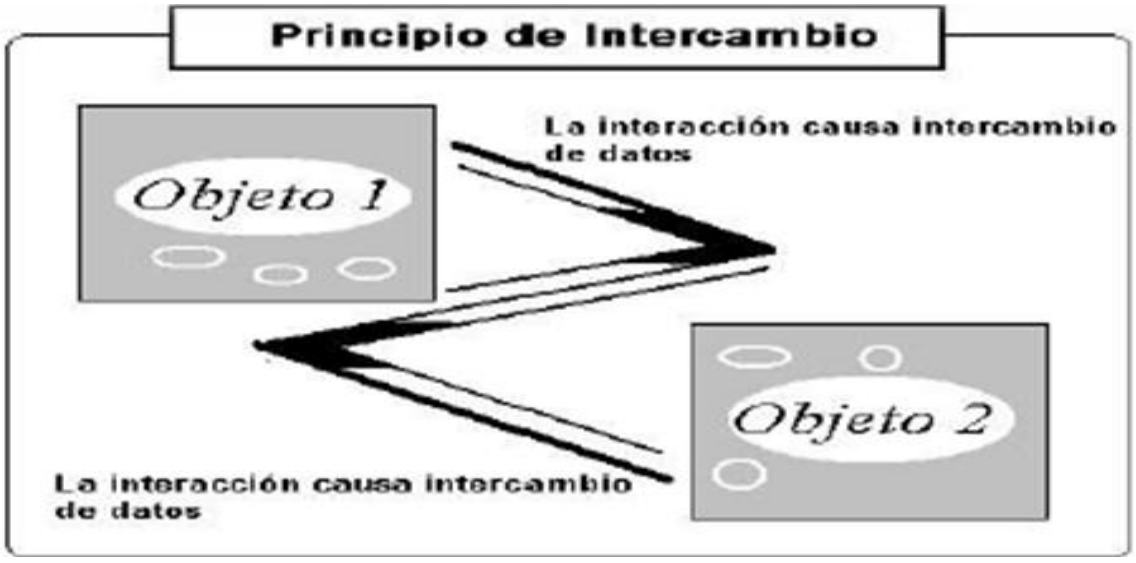


Fig.2 Principio de intercambio

Cuando en un a escena del crimen se tiene que trabajar en condiciones adversas, como en incendios, inundaciones, de gasolina o químicos peligroso, es indispensable que el investigador tome las medidas de seguridad necesarias para asegurar en primer lugar su integridad física, luego deberá implementar el procedimiento más adecuado para incrementar las posibilidades de recuperar las evidencias de la manera más completa.

De lo dicho podemos manifestar que los examinadores forenses nunca tendrán la oportunidad de revisar una escena del crimen en su estado original, siempre abra algún factor que haga que la escena del crimen presente algunas anomalías o discrepancias.

Con la finalidad de explicar cómo funciona la dinámica de las evidencias, a continuación se expondrán algunas situaciones en donde esta se ve afectada dentro de una escena del crimen.

- ✓ **Equipos de emergencias:** en el caso de un incendio los sistemas informáticos pueden ser afectados por el fuego y el humo, posteriormente sometidos a una gran presión de agua al tratar de apagar este. Esto provoca que los técnicos forenses no puedan determinar a ciencia cierta si los sistemas informáticos encontrados en la escena tuvieron comprometidos, fueron atacados o usados indebidamente. en otras ocasiones los equipos de emergencias manipulan la escena cuando es necesario para salvar la vida de una persona.

- ✓ **Personal de criminalística:**

  En algunas ocasiones el personal de criminalística por accidente cambia, reubica, o altera la evidencia. Por ejemplo en el caso de que se quisiera sacar una muestra de sangre de una gota precipitada sobre un disquete o disco compacto mediante el uso de un escarpelo, esto puede accidentalmente comprometer los datos e información almacenada en dichos soportes.

- ✓ **El sospechoso o el imputado tratando de cubrir sus rastros:** cuando el sospecho imputado deliberadamente borra o altera los datos, registros u otros mensajes de datos considerados como evidencia dentro de un disco duro.

- ✓ **Acciones de la víctima:** la víctima de un delito puede borrar correo electrónico que le causen aflicción o le provoquen una situación embarazosa.

- ✓ **Transferencia secundaria:** en algunas acciones, los sistemas informáticos usados en el acometimiento de un delito informático son usados posteriormente por alguna persona de forma inocente, causando con ello la destrucción y alteración de evidencia.

- ✓ **Testigo:** un administrador del sistema puede borrar cuentas de usuarios sospechosas, las mismas que fueron creadas por un intruso, a fin de prevenir su acceso y utilización futura.

- ✓ **El clima y la naturaleza:** los campos electromagnéticos pueden corromper la información guardada en discos magnéticos.

- ✓ **Descomposición:** en algunos casos la información almacenada en discos magnéticos, o en otros soportes pueden perderse o tornarse ilegibles para los sistemas de información a causa del tiempo y de las condiciones de almacenamiento.

En resumen el investigador forense debe entender como los factores humanos, de la naturaleza y de los propios equipos informáticos pueden alterar, borrar o destruir evidencia, debe comprender como dicha variables actúan sobre la escena misma del delito, debe por tanto encaminar la investigación desde su etapa más temprana tomando en cuenta esos cambios, a fin de adecuar el mejor método para adquirir, preservar y luego analizar las pistas obtenidas, y así reducir de manera considerable los posibles efectos de la dinámica de la evidencia.

5. Introducción a la informática forense. Consultada el 13 de noviembre de 2010, de http://www.alfa-redi.com/apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/Acurio.pdf

PASOS PARA LA RECOLECCIÓN DE EVIDENCIA

El procedimiento para la recolección de evidencia varía de país a país, y por lo tanto, un análisis exacto y completo está fuera de los límites de este documento. Sin embargo, existen unas guías básicas que pueden ayudar a cualquier investigador forense:

- ✓ **HARDWARE**

  El hardware es uno de los elementos que se deben tener en cuenta a la hora de la recolección de evidencia, debido a que puede ser usado como instrumento, como objetivo del crimen, o como producto del crimen (por Ej. contrabando o robo), es por eso que se deben tener consideraciones especiales.

CUIDADOS EN LA RECOLECCIÓN DE EVIDENCIA

La recolección de evidencia informática es un aspecto frágil de la computación Forense, especialmente porque requiere de prácticas y cuidados adicionales que no se tienen en la recolección de evidencia convencional. Es por esto que:

- ✓ Se debe proteger los equipos del daño.
- ✓ Se debe proteger la información contenida dentro de los sistemas de almacenamiento de información (muchas veces, estos pueden ser alterados fácilmente por causas ambientales, o por un simple campo magnético).
- ✓ Algunas veces, será imposible reconstruir la evidencia (o el equipo que la Contiene), si no se tiene cuidado de recolectar todas las piezas que se necesiten.

CADENA DE CUSTODIA:

Proceso ininterrumpido y documentado que permite demostrar la autenticidad de la evidencia física.

FASES DE LA INVESTIGACION FORENSE

El proceso de análisis forense a una computadora se describe a continuación:

- **Identificación**

  Es muy importante conocer los antecedentes, situación actual y el proceso que se quiere seguir para poder tomar la mejor decisión con respecto a las búsquedas y la estrategia de investigación. Incluye muchas veces la identificación del bien informático, su uso dentro de la red, el inicio de la cadena de custodia (proceso que verifica la integridad y manejo adecuado de la evidencia), la revisión del entorno legal que protege el bien y del apoyo para la toma de decisión con respecto al siguiente paso una vez revisados los resultados.

- **Preservación**

Este paso incluye la revisión y generación de las imágenes forenses de la evidencia para poder realizar el análisis. Dicha duplicación se realiza utilizando tecnología de punta para poder mantener la integridad de la evidencia y la cadena de custodia que se requiere. Al realizar una imagen forense, nos referimos al proceso que se requiere para generar una copia "bit-a-bit" de todo el disco, el cual permitirá recuperar en el siguiente paso, toda la información contenida y borrada del disco duro. Para evitar la contaminación del disco duro, normalmente se ocupan bloqueadores de escritura de hardware, los cuales evitan el contacto de lectura con el disco, lo que provocaría una alteración no deseada en los medios.

- **Análisis**

Proceso de aplicar técnicas científicas y analíticas a los medios duplicados por medio del proceso forense para poder encontrar pruebas de ciertas conductas. Se pueden realizar búsquedas de cadenas de caracteres, acciones específicas del o de los usuarios de la máquina como son el uso de dispositivos de USB (marca, modelo), búsqueda de archivos específicos, recuperación e identificación de correos electrónicos, recuperación de los últimos sitios visitados, recuperación del caché del navegador de Internet, etc.

- **Presentación**

Es el recopilar, toda la información que se obtuvo a partir del análisis para realizar el reporte y la presentación a los abogados, la generación (si es el caso) de una pericial y de su correcta interpretación sin hacer uso de tecnicismos.

6. Informática Forense, Introducción y Contenido. Consultado el 20 de octubre de 2010, de http://labs.dragonjar.org/laboratorios-informatica-forense-introduccion-y-contenido

FORENCIA EN REDES.

Es un escenario aún más complejo, pues es necesario comprender la manera como los protocolos, configuraciones e infraestructuras de comunicaciones se conjugan para dar como resultado un momento específico en el tiempo y un comportamiento particular.

Esta conjunción de palabras establece un profesional que entendiendo las operaciones de las redes de computadores, es capaz, siguiendo los protocolos y formación criminalística, de establecer los rastros, los movimientos y acciones que un intruso ha desarrollado para concluir su acción. A diferencia de la definición de computación forense, este contexto exige capacidad de correlación de evento, muchas veces disyuntos y aleatorios, que en equipos particulares, es poco frecuente.

ROLES EN LA INVESTIGACIÓN

La investigación científica de una escena del crimen es un proceso formal, donde el investigador forense, documenta y adquiere toda clase de evidencias, usa su conocimiento científico y sus técnicas para identificarla y generar indicios suficientes para resolver un caso. Es por tanto necesario dejar en claro cuáles son los roles y la participación que tiene ciertas personas dentro de una escena del crimen de carácter informático o digital, estas personas son:

- ✓ **Técnicos en escenas del crimen informáticos,** también llamados FIRST RESPONDENDERS, son los primeros en llegar a la escena del crimen, son los encargados de recolectar las evidencias que ahí se encuentran, tienen una formación básica en el manejo de evidencia y documentación, al igual que en reconstrucción del delito, y la localización de elementos de convicción dentro de la red.

- ✓ **Examinadores de evidencia digital o informática,** que son los responsables de procesar toda la evidencia digital o informática obtenida por los técnicos en escenas del crimen informáticos. Para esto dichas personas requieren tener un alto grado de especialización en el área de sistema e informática.

- ✓ **Investigadores de delitos informáticos,** que son los responsables de realizar la investigación y la reconstrucción de los hechos de los delitos informáticos de manera general, son personas que tienen un entrenamiento general en cuestiones de informática forense, son profesionales en seguridad informática, abogados, policías, y examinadores forenses.

7. Introducción a la informática forense. Consultada el 13 de noviembre de 2010, de http://www.alfa-redi.com/apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/Acurio.pdf

Adicionalmente, un examinador forense digital, dentro del proceso del cómputo forense puede llegar a recuperar información que haya sido borrada desde el sistema operativo.

DISPOSITIVOS A ANALIZAR

La infraestructura informática que puede ser analizada puede ser toda aquella que tenga una Memoria (informática), por lo que se pueden analizar los siguientes dispositivos:

- ✓ Disco duro de una Computadora o Servidor
- ✓ Teléfono Móvil o Celular, parte de la telefonía celular
- ✓ Agendas Electrónicas (PDA)
- ✓ Dispositivos de GPS
- ✓ Impresoras
- ✓ Memorias USB

ANÁLISIS DE DISCOS

La clave de la computación forense es el análisis de discos duros, disco extraíbles, CD, discos SCSI, y otros medios de almacenamiento. Este análisis no sólo busca archivos potencialmente incriminatorios, sino también otra información valiosa como ***passwords, logins*** y rastros de actividad en Internet. Existen muchas formas de buscar evidencia en un disco. Muchos criminales no Tienen la más mínima idea de cómo funcionan los computadores, y por lo tanto no hacen un mayor esfuerzo para despistar a los investigadores, excepto por borrar archivos, que pueden ser recuperados fácilmente.

Cuando los usuarios de DOS o Windows borran un archivo, los datos no son borrados en realidad, a menos que se utilice software especial para borrar. Los investigadores forenses, utilizan herramientas especiales que buscan archivos "suprimidos" que no han sido borrados en realidad, estos archivos se convierten en evidencia. En las siguientes secciones, se explican algunas de las características poco conocidas del almacenamiento de la información en un computador, que son explotadas por los expertos en informática forense para recuperar datos que se creían eliminados.[8]

8. Informática Forense, Introducción y Contenido. Consultado el 20 de octubre de 2010, dehttp://labs.dragonjar.org/laboratorios-informatica-forense-introduccion-y-contenido

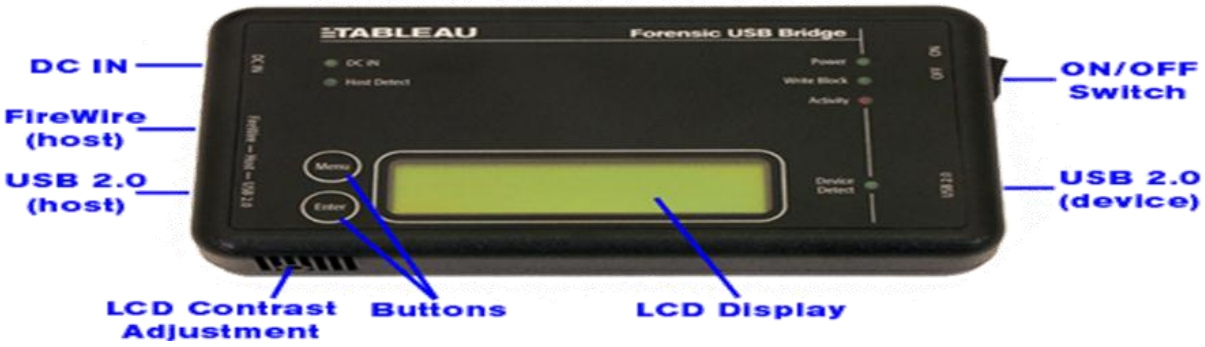
HERRAMIENTAS DE HARWARE.

El perito informático deberá portar las siguientes herramientas:

1. Lectograbadora externa de CD/DVD con conector USB
2. Switch(Networking)
3. Computadora portátil(Laptop)
4. Impresora portátil
5. Dipositivos de almacenamiento externo con conector USB
6. Pen drive
7. Disco rígido sanitizado
8. Cables UTP CAT5 para conexión Ethernet: Directo y cruzado
9. Destornilladores
10. Kit de pinzas
11. Marcadores indelebles
12. Cinta de embalaje
13. Etiquetas de seguridad
14. Guantes de latex
15. Cúter
16. Cables de datos PATA para conexión de discos rígidos
17. Cables de alimentación para PC
18. CD-R y DVD-R vírgenes

PROTECTORES CONTRA ESCRITURA Y DUPLICADORES

TABLEAU T8



El modelo T8 de Tableau se ha diseñado para permitir la extracción de imágenes válidas para el análisis forense a partir de dispositivos USB de almacenamiento masivo. Es decir, por medio del T8 es posible leer datos de dispositivos USB de almacenamiento masivo sin temor a que esos datos sean modificados accidentalmente durante el proceso de adquisición

Producto	Forense puente USB Tableau modelo T8

Conectores: lado del anfitrión

FireWire	Uno de 6 pines FireWire400 (1394A)
USB	Un puerto USB Mini-B (5 pines, USB 2.0 de alta / total / baja velocidad)
De entrada de CC	5-pin mini-DIN para el uso con fuente de alimentación Tableau TP1

Conectores: lateral del dispositivo

USB	Un USB A (de 4 pines, USB 2.0 de alta / total / baja velocidad)

Interruptores

ON / OFF	Enciende ON / OFF para T8 y dispositivo USB conectado
Interruptor DIP	interruptor DIP de 4 posiciones selecciona las opciones configurables en campo (interruptores DIP se puede acceder mediante la eliminación de un knock-out en el panel lateral de la caja T8)

Interfaz de usuario

LCD	2 filas x 16 columnas LCD monocromo carácter de la exhibición
Botones	Dos: menú e introducir los botones para la navegación

Otras características

El bloqueo de escritura	Escribe bloqueo es permanente habilitada en Tableau T8
LEDs de estado	6 LEDs: DC buena, encendido, bloqueo de escritura habilitada, la actividad, el dispositivo USB detectar, anfitrión detectar
Control de contraste LCD	LCD de ajuste de contraste a través de potenciómetro accesible externamente.

Compatibilidad

Dispositivo USB	Los dispositivos USB deben cumplir con el USB de almacenamiento masivo de especificación y en particular debe implementar la interfaz de Protocolo sólo a granel
Interfaz con el host	FireWire400 o USB 2.0
O Anfitrión / S	XP/2000/newer Windows, Macintosh OS X, la mayoría de distribuciones de Linux (nota: las distribuciones de Linux tienen diferentes niveles y la calidad de apoyo a FireWire/1394 y USB 2.0)

Físico / Ambiental

Potencia	2,5 vatios típicas de operación (sin incluir el dispositivo USB)
Tensión de alimentación (DC IN)	5 VDC @ 2A (incluye el presupuesto para el dispositivo USB)
Tensión de salida (DC OUT)	VDC@1.5A 5 (máximo)
Dimensiones	5,75 pulgadas (L) x 3.25 pulgadas (W) x 1.125 pulgadas (H)
Peso	5.9 oz (166g)
Rango de temperatura	0 a 55 grados C (sin flujo de aire)

Temperatura de almacenamiento	-40 A 70 grados C
Humedad relativa del aire	Hasta un 90% (sin condensación)

Tableau utiliza la palabra "puente" para referirse al dispositivo T8 porque puede conectarse al equipo host ya sea mediante una conexión USB 2.0 *o* una conexión FireWire 400/1394A. En el ámbito del análisis forense informático, el T8 también podría denominarse "bloqueador de escritura USB".

9. Consultado 29 mayo 2011, especificaciones tableau t8: http://www.tableau.com/index.php?pageid=specs&model=T8

Recomendaciones para el uso adecuado

Tres recomendaciones para el uso correcto "están impresos en la etiqueta colocada en la parte inferior de la T8

1. Conectar / desconectar un dispositivo USB sólo cuando T8 interruptor de encendido está apagado.
2. Nunca aplique presión en la pantalla LCD.
3. Tenga cuidado al conectar los cables FireWire/1394 y USB, Cables de conexión hacia atrás puede dañar permanentemente el T8 y anula la garantía de Tableau.
4. Cuando se utiliza el T8 con un equipo que ejecuta Microsoft Windows, utilice **siempre** el Windows "Extracción segura applet" para decirle a Windows que apague el dispositivo T8. Tableau *antes de* desconectar o apagar el T8.

DISK JOCKEY PRO FORENSIC KIT

Disk Jockey es versátil, útil, inteligente y sin igual en valor. Cuenta con siete modos de construcción en los que te permite hacer una serie de funciones diferentes.

Copias Rápidas de disco a disco copias de disco duro, sin necesidad de ordenador. Copiar discos duros sin necesidad de software adicional a grandes velocidades.

Disk Copy Verificación permite verificar que la copia que acaba de hacer es una copia exacta y que usted no tiene ninguna pérdida de datos.

Fácil de expansión Fácil de hacer un gran volumen de dos discos conectados al Disk Jockey, a continuación, conecte el Jockey disco a su USB 2.0 equipado Mac o PC con Windows.

Independiente de HD Modo Montar uno o dos discos duros en el escritorio de su ordenador Windows a través de USB 2.0 sin necesidad de instalar ningún controlador adicional.

Prueba de lectura de disco duro lleva a cabo un sector por sector del disco duro, lee la prueba en las unidades que le permite tener una idea mejor para la estabilidad general de su disco duro.

Refleja permite duplicar dos discos duros de copia de seguridad en tiempo real (RAID 1). Si falla una unidad, tiene los datos de la misma en la otra unidad.

Dos niveles de Borrar ofrece dos niveles de borrado de disco. Perfecto para aplicaciones de gobierno cuando la seguridad es imprescindible.

Disk Jockey Incluye

1. Disk Jockey PRO (of course!) Disk Jockey PRO
2. Cable USB 2.0
3. HDD de 2.5 "de cable plano x 2
4. 3.5 "HDD cable Plano x 2
5. Cable SATA x 2
6. Cable de alimentación SATA x2
7. Personalizada adaptador de CA
8. Personalizada cable de CA
9. Personalizada electrostática alfombra x2
10. Usuarios de guía o guía de inicio rápido

Sistemas operativos compatibles

- Windows 2000, Windows 7, Windows XP

10. Consultado 01 de mayo 2011, DiskJockeyUserGuide: http://www.diskology.com/DiskJockeyUserGuide.pdf

UPS: Es una fuente de suministro eléctrico que posee una batería con el fin de seguir dando energía a un dispositivo en el caso de interrupción eléctrica. Los UPS son llamados en español SAI (Sistema de alimentación ininterrumpida).
UPS significa en inglés Uninterruptible Power Supply.
Los UPS suelen conectarse a la alimentación de las
En el caso de que se produzca un corte eléctrico.
Algunos UPS también ofrecen aplicaciones que se encargan de realizar ciertos procedimientos automáticamente para los casos en que el usuario no esté y se corte el suministro eléctrico.

11. Consultado 01 de mayo del 2011, especificaciones ups.
http://www.cajasmodding.com/sai-15-kva-online-con-cpu-y-lcd-p-383.html

ROADMASSTER 3 Mobile Forensics Data Acquisition and Analysis Computer Lab

1. Posee una amplia variedad de interfaces para dispositivos (IDE, SATA, SCSI, SAS, USB, 1394A/B), permite hashing MD5, CRC32, SHA1 y SHA2, múltiples métodos de captura y copiado simultáneo. Uno de los más completos (y caros) del mercado.
2. Diseñado para aplicaciones de campo e ideal para las agencias de aplicación de la ley, así Como los organismos de seguridad corporativa para adquirir y analizar datos sobre el terreno.
3. Funciona de una forma rápida y fiable en el análisis y creación de imagen de disco duro.

Características generales:

- ✓ High Speed Forensic Tool with Drive interfaces
- ✓ Rugged Design
- ✓ Large Display 15" Color

- ✓ Modular Design
- ✓ EMI Shielding
- ✓ Shock Absorbent MD5, CRC32, SHA1 and SHA2 Hashing…etc

12. Consultado 25 de abril del 2011, http://www.lawmate.eu/itforensik/index.html

SOFTWARE BASE

Microsoft Windows Server 2008

Microsoft Windows Server 2008 **e**stá diseñado para ofrecer a las organizaciones la plataforma más productiva para virtualización de cargas de trabajo, creación de aplicaciones eficaces y protección de redes. Ofrece una plataforma segura y de fácil administración, para el desarrollo y alojamiento confiable de aplicaciones y servicios web. Del grupo de trabajo al centro de datos, Windows Server 2008 incluye nuevas funciones de gran valor, eficacia y mejoras impactantes en el sistema operativo base.

Más control

Windows Server 2008 proporciona a los profesionales de TI más control sobre sus servidores e infraestructura de red y les permite centrarse en las necesidades críticas del negocio. Capacidades mejoradas en secuencias de comandos y automatización de tareas, como las que ofrece Windows PowerShell, ayudan a los profesionales de TI a automatizar tareas comunes de TI.

La instalación y administración basadas en funciones con Administrador del Servidor facilita la tarea de administrar y proteger las múltiples funciones de servidor en una empresa. La nueva consola del administrador del servidor proporciona un único origen para administrar la configuración del servidor y la información del sistema. El personal de TI puede instalar sólo las funciones y características que sean necesarias, y hay asistentes que automatizan muchas de las tareas de implementación de sistemas que tardan más tiempo. Herramientas mejoradas de administración del sistema, como el Monitor de rendimiento y confiabilidad, ofrecen información sobre sistemas y alertan al personal de TI sobre problemas potenciales antes de que sucedan.

Mayor protección

Windows Server 2008 proporciona una serie de tecnologías de seguridad nuevas y mejoradas, que aumentan la protección del sistema operativo al ofrecer una base sólida para dirigir y construir un negocio. Incluye innovaciones de seguridad, como PatchGuard, que reducen la exposición a ataques del núcleo, lo que produce un entorno de servidor más seguro y estable.

El sistema de protección de servicios de Windows ayuda a mantener más seguros los sistemas al evitar que los servicios críticos de Servidor estén en riesgo por actividades anormales en el sistema de archivos, registro, o red. La seguridad también se mejora en el sistema operativo Windows Server 2008 por medio de protección de acceso a redes (NAP), controlador de dominio de sólo lectura (RODC), mejoras en la infraestructura de clave pública (PKI), un nuevo firewall de Windows bidireccional y compatibilidad con criptografía de última generación.

Mayor flexibilidad

Windows Server 2008 está diseñado para permitir que los administradores modifiquen su infraestructura para adaptarla a las necesidades cambiantes del negocio y continuar siendo ágiles. Se mejora la flexibilidad para trabajadores móviles mediante tecnologías que permiten que los usuarios ejecuten programas desde cualquier ubicación remota, como RemoteApp y Terminal Services Gateway. Windows Server 2008 acelera la implementación y el mantenimiento de sistemas de TI con Servicios de Implementación de Windows (WDS) y ayuda en la consolidación de servidores con Windows Server virtualization (WSv). Para organizaciones que necesitan controladores de dominio en sucursales, Windows Server 2008 ofrece una nueva opción de configuración: el Controlador de Dominio de sólo lectura (RODC), que evita exponer las cuentas si el Controlador de Dominio estuviera en riesgo.

VIRTUALIZACION

Windows Server 2008 incluirá Windows Server virtualization (WSv), una tecnología eficaz de virtualización con sólidas características de administración y seguridad. WSv permite que los negocios aprovechen su familiaridad existente con la administración de servidores Windows y la flexibilidad y beneficios de seguridad de la virtualización sin necesidad de adquirir software de terceros. Microsoft y sus asociados ofrecen el soporte técnico completo para sistemas operativos invitados Windows y Linux compatibles. WSv es una plataforma sumamente flexible, de alto rendimiento, rentable y con buen soporte.

Seguridad

La seguridad es un desafío fundamental en cada implementación de servidor. Un servidor que aloja múltiples máquinas virtuales (VM), también conocidos como servidores consolidados, está expuesto a los mismos riesgos de seguridad que los servidores no consolidados, pero agrega el desafío de separación de funciones de administrador.

WSv ayuda a aumentar la seguridad de servidores consolidados y resuelve el desafío de separación de funciones de administrador.

WSv lo lleva a cabo por medio de las siguientes características:

- ✓ Particiones fuertes: una máquina virtual (VM) funciona como un contenedor independiente de sistema operativo, completamente aislado de otras máquinas virtuales que se ejecutan en el mismo servidor físico.

- ✓ Seguridad para el hardware: características como prevención de ejecución de datos (DEP) se encuentran disponibles en el hardware más reciente para servidores y ayudan a evitar la ejecución de los virus y los gusanos más predominantes.

- ✓ Windows Server virtualization: WSv ayuda a evitar la exposición de las VM que contienen información confidencial y protege también al sistema operativo host subyacente del riesgo que comporta un sistema operativo invitado.

- ✓ Características de seguridad de red: permite la traducción de direcciones de red (NAT) automática, firewall y protección de acceso a redes (NAP).

- ✓ Base de equipos de confianza mínima: ofrece una superficie de ataque reducida y una arquitectura de virtualización simplificada y ligera. Esta característica mejora la confiabilidad de equipos virtuales basados en WSv.

La configuración de un servidor consolidado que ofrezca los mejores entornos de seguridad y sistema operativo para cada aplicación puede presentar en ciertas ocasiones un desafío difícil.

Debido a que WSv crea un entorno donde es posible configurar cada carga de trabajo con un entorno de sistema operativo y perfil de seguridad ideales, WSv resuelve el desafío de la separación de funciones en un servidor consolidado. WSv protege a las VM del sistema operativo host y viceversa, al permitir que las VM se ejecuten en una cuenta de servicio sólo con los privilegios necesarios. Con WSv, el sistema operativo host está protegido y una VM en riesgo está limitada en el daño que podría causar a otras VM.

Fuerte aislamiento

La virtualización del servidor permite que coexistan cargas de trabajo con requisitos de recursos diferentes en el mismo servidor host. WSv ofrece varias características que facilitan el uso eficaz de los recursos físicos del servidor host:

- ✓ Asignación flexible de memoria: se puede asignar una cantidad máxima y una cantidad mínima de memoria RAM garantizada a las máquinas virtuales. Esta característica permite que los administradores creen una configuración de WSv que equilibre las necesidades individuales del recurso de VM frente al rendimiento

total del servidor de WSv.

- ✓ Adición dinámica de hardware: WSv puede agregar dinámicamente procesadores lógicos, memoria, adaptadores de red y almacenamiento a sistemas operativos invitados compatibles, mientras se encuentran en ejecución. Esta característica facilita la asignación granular de capacidades de procesamiento host de WSv a los sistemas operativos invitados.

- ✓ Configuración flexible de red: WSv ofrece características avanzadas de red para las VM, que incluyen NAT, firewall y asignación de VLAN. Esta flexibilidad se puede usar para crear una configuración de WSv más compatible con los requisitos de seguridad de red.

Las características de asignación flexible de memoria, adición dinámica de hardware y configuración flexible de red de WSv facilitan una respuesta más eficaz a las cargas dinámicas de servidor. Por ejemplo, la carga de trabajo de procesamiento de fin de período es con frecuencia varias veces mayor que el promedio en algunas aplicaciones de línea de negocios (LOB). WSv se puede usar con sistemas operativos invitados compatibles, para asignar dinámicamente recursos adicionales de memoria y procesador a una VM en ejecución y administrar los requisitos ampliados de procesamiento sin reiniciar el sistema operativo invitado. Con suficientes recursos de servidor host, este cambio no disminuye el rendimiento de las demás VM que se ejecutan en el host.

Rendimiento

Los avances e integración del diseño con hardware que reconoce la virtualización permite a WSv virtualizar cargas de trabajo mucho más exigentes que en versiones anteriores y con mayor flexibilidad en la asignación de recursos.

Los avances de rendimiento incluyen:

- ✓ Arquitectura de virtualización ligera, de baja sobrecarga, basada en Hypervisorde 64 bits: hardware preparado para virtualización (Intel VT y la tecnología "Pacifica" de AMD) que permite rendimientos mayores del sistema operativo invitado.

- ✓ Compatibilidad con múltiples núcleos. A cada VM se le pueden asignar hasta ocho procesadores lógicos: esto permite la virtualización de grandes cargas de trabajo, con cálculo intensivo, que aprovechan los beneficios del procesamiento en paralelo de núcleos de VM con procesadores múltiples.

- ✓ Compatibilidad de sistemas operativos host e invitado de 64 bits: WSv se ejecuta en la versión de 64 bits de Windows Server 2008 para ofrecer acceso a grandes grupos de memoria para las VM invitadas. Cargas de trabajo intensivas en memoria que se verían muy afectadas por extensas paginaciones si se ejecutaran en sistemas operativos de 32 bits, se pueden virtualizar correctamente en WSv. WSv también es compatible con sistemas operativos invitados de 64 y 32 bits que se ejecutan en el mismo servidor consolidado.
  - ✓ Compatibilidad con Server Core. WSv puede usar una instalación Server Core de Windows Server 2008 como sistema operativo host. La superficie mínima de instalación y baja sobrecarga de Server Core dedica la mayor cantidad posible de la capacidad de procesamiento de servidor host a las VM en ejecución.

  - ✓ Acceso a disco de paso. Los sistemas operativos invitados se pueden configurar para tener acceso de forma directa a almacenamiento local o de red de área de almacenamiento (SAN) iSCSI, lo que ofrece mayores rendimientos en aplicaciones con muchas operaciones de E/S, como SQL Server o Microsoft Exchange.

Muchas cargas de trabajo de servidor demandan mucho procesamiento de servidor y subsistemas de E/S. Cargas de trabajo como SQL Server y Microsoft Exchange normalmente consumen mucha memoria y lastran el rendimiento de disco, y ha habido

resistencia a virtualizar estas cargas de trabajo. El hypervisor de 64 bits en WSv junto con características como el acceso a disco de paso hace posible y con frecuencia deseable virtualizar grandes cargas de trabajo.

Administración simplificada

En las instalaciones de centros de datos y sucursales remotas donde es posible implementar WSv, se necesitan fuertes capacidades de administración y automatización para ser totalmente consientes del potencial de reducción de costos de la virtualización. WSv satisface este desafío con las siguientes capacidades de administración y automatización:

- ✓ Administración extensible: WSv está diseñado para funcionar con Microsoft System Center Operations Manager (SCOM) y System Center Virtual Machine Manager (SCVMM). Estas herramientas de administración ofrecen informes, automatización, implementación y herramientas autoservicio de usuario para WSv.

- ✓ Interfaz MMC 3.0 para administración de VM: la familiar interfaz Microsoft Management Console (MMC) se usa para administrar la configuración de WSv y los valores de VM, reduciendo sensiblemente el proceso de aprendizaje de WSv.

    - ✓ Interfaz del instrumental de administración de Windows (WMI): WSv incorpora un proveedor WMI que ofrece acceso a información de sistema y administración mediante secuencias de comandos.

    - ✓ Secuencias de comandos de PowerShell: la configuración de host y VM de WSv se configura a través de Windows PowerShell.

Administración de objetos de directivas de grupo (GPO): WSv usa las capacidades de administración de configuración de GPO para administrar la virtualización del host WSv y la configuración del equipo virtual.

Las capacidades de administración de SCOM y SCVMM hacen posible administrar de forma eficaz tanto instalaciones de centros de datos como instalaciones sumamente distribuidas de WSv. Por ejemplo, el acceso de secuencias de comandos al

Proveedor WMI en WSv se puede usar para automatizar las ventanas de mantenimiento en varios servidores host de WSv, al apagar VM invitadas, encenderlas en un servidor en espera, realizar el mantenimiento en el servidor host y, a continuación, restaurar las VM a su host original.

Con la adición de System Center Virtual Machine Manager, esta operación se puede automatizar y realizar sin ningún tiempo de inactividad perceptible para muchas aplicaciones.

RESUMEN

La virtualización de Microsoft Windows Server combina características que resuelven muchos de los desafíos de virtualización más difíciles, ente los que se incluyen: protección de servidores consolidados, respuesta a cargas de trabajo dinámicas, obtención de alto rendimiento y escalabilidad para cargas de trabajo virtualizadas y administración simplificada. La combinación de características de seguridad y fuerte aislamiento de VM en WSv hace posible consolidar cargas de trabajo heterogéneas en servidores host WSv mientras se mantienen flexibilidad y seguridad.

La arquitectura de 64 bits de Hypervisor que forma la base para WSv ofrece alto rendimiento para cargas de trabajo exigentes. Y las fuertes características integradas de administración de Windows Server 2008, System Center Operations Manager y System Center Virtual Machine Manager permiten el control automatizado y eficaz de una gran variedad de entornos virtualizados.

13. http://www.microsoft.com/latam/technet/windowsserver/longhorn/evaluate/whitepaper.mspx

OFFICE 2007 ULTÍMATE EDITION

HERRAMIENTAS PARA LA RECOLECCIÓN DE EVIDENCIA

Hablar de informática forense sin revisar algunas ideas sobre herramientas es hablar en un contexto teórico de procedimientos y formalidades legales. Las herramientas informáticas, son la base esencial de los análisis de las evidencias digitales en los medios informáticos. Sin embargo, es preciso comentar que éstas requieren de una formalidad adicional que permita validar tanto la confiabilidad de los resultados de la aplicación de las mismas, como la formación y conocimiento del investigador que las utiliza. Estos dos elementos hacen del uso de las herramientas, una constante reflexión y cuestionamiento por parte de la comunidad científica y práctica de la informática forense en el mundo.

Existen una gran cantidad de herramientas para recuperar evidencia. El uso de herramientas sofisticadas se hace necesario debido a:

- ✓ La gran cantidad de datos que pueden estar almacenados en un computador.
- ✓ La variedad de formatos de archivos, los cuales pueden variar enormemente, aún dentro del contexto de un mismo sistema operativo.
- ✓ La necesidad de recopilar la información de una manera exacta, y que permita verificar que la copia es exacta.
- ✓ Limitaciones de tiempo para analizar toda la información.

- ✓ Facilidad para borrar archivos de computadores.
- ✓ Mecanismos de inscripción, o de contraseñas.

Por esto mismo, las herramientas de recolección de evidencia deben reunir características que permitan manejar estos aspectos, pero además incluir facilidades para el análisis.

14. Forense digital. Consultado el 15 de octubre de 2010, de http://html.rincondelvago.com/informatica-forense.html

HERRAMIENTAS DE SOFTWARE FORENSE

Dentro de las herramientas de software frecuentemente utilizadas en procedimientos forenses en informática detallamos algunas.

ENCASE

Es un ejemplo de herramientas que permite asistir al especialista forense durante el análisis de un crimen digital. Se escogió mostrar esta herramienta por tratarse del software líder en el mercado, el producto más ampliamente difundido y de mayor uso en el campo del análisis forense. Algunas de las características más importantes de EnCase se relacionan a continuación:

- ✓ **Copiado Comprimido de Discos Fuente**.

  Encase emplea un estándar sin pérdida (loss-less) para crear copias comprimidas de los discos origen. Los archivos comprimidos resultantes, pueden ser analizados, buscados y verificados, de manera semejante a los normales (originales). Esta característica ahorra cantidades importantes de espacio en el disco del computador del laboratorio forense, permitiendo trabajar en una gran diversidad de casos al mismo tiempo, examinándola evidencia y buscando en paralelo.

- ✓ **Búsqueda y Análisis de Múltiples partes de archivos adquiridos.**

  Encase permite al examinador buscar y analizar múltiples partes de la evidencia. Muchos investigadores Involucran una gran cantidad de discos duros, discos extraíbles, discos “zip” y otros tipos de dispositivos de almacenamiento de la información. Con Encase, el examinador puede buscar todos los datos involucrados en un caso en un solo paso. La evidencia se clasifica, si esta comprimida o no, y puede ser colocada en un disco duro y ser examinada en paralelo por el especialista. En varios casos la evidencia puede ser ensamblada en un disco duro grande o un servidor de red y también buscada mediante Encase en un solo paso.

- ✓ **Diferente capacidad de Almacenamiento**.

Los datos pueden ser colocados en diferentes unidades, como Discos duros IDE o SCSI, drives ZIP, y Jazz. Los archivos pertenecientes a la evidencia pueden ser comprimidos o guardados en CD-ROM manteniendo su integridad forense intacta, estos archivos pueden ser utilizados directamente desde el CD-ROM evitando costos, recursos y tiempo de los especialistas.

- ✓ **Varios Campos de Ordenamiento, Incluyendo Estampillas de tiempo**.

  Encase permite al especialista ordenar los archivos de la evidencia de acuerdo a diferentes campos, incluyendo campos como las tres estampillas de tiempo (cuando se creó, último acceso, última escritura), nombres de los archivos, firma de los archivos y extensiones.

- ✓ **Análisis Compuesto del Documento.**

  Encase permite la recuperación de archivos internos y meta-datos con la opción de montar directorios como un sistema virtual para la visualización de la estructura de estos directorios y sus archivos, incluyendo el *slack* interno y los datos del espacio unallocated. Búsqueda Automática y Análisis de archivos de tipo Zip y Attachments de E-Mail.

- ✓ **Firmas de archivos, Identificación y Análisis**.

  La mayoría de las gráficas y de los archivos de texto comunes contiene una pequeña cantidad de *bytes* en el comienzo del sector los cuales constituyen una firma del archivo. Encase verifica esta firma para cada archivo contra una lista de firmas conocida de extensiones de archivos. Si existe alguna discrepancia, como en el caso de que un sospechoso haya escondido un archivo o simplemente lo haya renombrado, Encase detecta automáticamente la identidad del archivo, e incluye en sus resultados un nuevo ítem con la bandera de firma descubierta, permitiendo al investigador darse cuenta de este detalle.

- ✓ **Análisis Electrónico Del Rastro De Intervención**.

  Sellos de fecha, sellos de hora, registro de accesos y la actividad de comportamiento reciclado son a menudo puntos críticos de una investigación por computador. Encase proporciona los únicos medios prácticos de recuperar y

de documentar esta información de una manera no invasora y eficiente. Con la característica de ordenamiento, el análisis del contenido de archivos la interfaz de Encase, virtualmente toda la información necesitada para un análisis de rastros se puede proporcionar en segundos.

- ✓ **Soporte de Múltiples Sistemas de Archivo.**

Encase reconstruye los sistemas de archivos forenses en DOS, Windows (todas las versiones), Macintosh (MFS, HFS, HFS+), Linux, UNIX (San, Open BSD), CD-ROM, y los sistemas de archivos DVDR. Con Encase un investigador va a ser capaz de ver, buscar y ordenar archivos desde estos discos concurridos con otros formatos en la misma investigación de una manera totalmente limpia y clara.

- ✓ **Vista de archivos y otros datos en el espacio Unallocated.**

Encase provee una interfaz tipo Explorador de Windows y una vista del Disco Duro de origen, también permite ver los archivos borrados y todos los datos en el espacio Unallocated. También muestra el Slack File con un color rojo después de terminar el espacio ocupado por el archivo dentro del *clúster*, permitiendo al investigador examinar inmediatamente y determinar cuándo el archivo reescrito fue creado. Los archivos Swap y PrintSpoolerson mostrados con sus estampillas de datos para ordenar y revisar.

- ✓ **Integración de Reportes.**

Encase genera el reporte del proceso de la investigación forense como un estimado. En este documento realiza un análisis y una búsqueda de resultados, en donde se muestra el caso incluido, la evidencia relevante, los comentarios del investigador, favoritos, imágenes recuperadas, criterios de búsqueda tiempo en el que se realizaron las búsquedas.

- ✓ **Visualizador Integrado de imágenes con Galería**.

Encase ofrece una vista completamente integrada que localiza automáticamente, extrae y despliega muchos archivos de imágenes como *.gay .pg*. Del disco.

Seleccionando la "Vista de Galería "se despliega muchos formatos de imágenes conocidas, incluyendo imágenes eliminadas, en el caso de una vista pequeña.

El examinador puede después escoger las imágenes relevantes al caso e inmediatamente integrar todas las imágenes en el reporte de Encase. No es necesario ver los archivos gráficos usando software de terceros, a menos que el formato de archivo no sea muy conocido y todavía no seas aportado por Encase. Actualmente Encase se encuentra en su versión 3.0.

15. ENCASE. Consultada el 05 de noviembre de 2010, de
http://www.guidancesoftware.com
http://html.rincondelvago.com/informatica-forense.html
http://www.encase.com/Products/ef_index.asp

ULTIMATE ACCESSDATA'S TOOLKIT

Integra una herramienta de recuperación capaz de descifrar casi cualquier archivo, un visor de registro mejorado, diseñado para iluminar la evidencia ocultada en el sistema, sólo las claves de registro de acceso, un limpiador de disco y un interruptor de codificación distribuida de la computación. Borde UTK es su base de datos impulsada por la plataforma. Como se importa pruebas (normalmente la unidad y las imágenes de partición), es escaneado e indexado en una base de casos. Esto permite una rápida cadena de investigaciones especiales y la organización de los archivos obtenidos y los datos sin necesidad de volver a escanear.

Característico de un instrumento comercial, FTK puede manejar un caso, desde la adquisición hasta su terminación, e incluye capacidades de reporting pulido y flexible que puede ser instalado sin esfuerzo en un auto de CD-ROM de juego para la circulación.

16. ULTIMATE ACCESSDATA'S TOOLKIT. Consultada el 05 de noviembre de 2010, de
http://kulio.crearblog.com/?p=6993
http://www.compute-rs.com/es/consejos-979135.htm
http://www.accessdata.com/products/utk/

WINHEX

Es un editor hexadecimal universal, particularmente útil en el ámbito de la informática forense, recuperación de datos, procesamiento de bajo nivel de datos y seguridad informática. Una herramienta avanzada para la utilización diaria y de emergencia: inspeccionar y editar todo tipo de archivos, recuperar archivos borrados o datos perdidos de discos duros con sistemas de archivos corruptos o desde tarjetas de cámaras digitales.

Las características incluyen:

- ✓ Editor de discos para discos duros, disquetes, CD- ROM y DVD, ZIP, Smart media, Compact Flash.
- ✓ Navegador de directorios de gran alcance para FAT, NTFS, Ext2 / 3, ReiserFS, CDFS, UDF.
- ✓ RAM editor, proporcionando acceso a la memoria virtual de otros procesos
- ✓ Analizar y comparar archivos.
- ✓ Búsqueda y reemplazo especialmente flexibles funciones.
- ✓ Clonación del disco, con una licencia de especialista también en DOS.
- ✓ Manejar las imágenes y copias de seguridad (comprimible o divisible en archivos de 650 MB).
- ✓ Cifrado de 128 bits , checksums , CRC32, hash (MD5 , SHA -1, …)
- ✓ Erase (borrar) los archivos confidenciales de forma segura, limpiar el disco duro para proteger su privacidad.
- ✓ Convertir entre binario, hexadecimal ASCII, Intel Hex y Motorola S.

17. WINHEX. Consultada el 05 de noviembre de 2010, de http://www.x-ways.net/Forensics/index-m.html
http://www.x-ways.net (shareware)

HERRAMIENTAS PARA EL MONITOREO Y/O CONTROL DE COMPUTADORES.

Algunas veces se necesita información sobre el uso de los computadores, por lo tanto existen herramientas que monitorean el uso de los computadores para poder recolectar

información. Existen algunos programas simples como keyloggers recolectores de pulsaciones del teclado, que guardan información sobre las teclas que son presionadas, hasta otros que guardan imágenes de la pantalla que ve el usuario del computador, o hasta casos donde la máquina es controlada remotamente.

KEYLOGGER

Es un ejemplo de herramientas que caen en esta categoría. Es una herramienta que puede ser útil cuando se quiere comprobar actividad sospechosa; guarda los eventos generados por el teclado, por ejemplo, cuando el usuario teclea la tecla de 'retroceder', esto es guardado en un archivo o enviado por *e-mail*. Los datos generados son complementados con información relacionada con el programa que tiene el foco de atención, con anotaciones sobre las horas, y con los mensajes que generan algunas aplicaciones.

Existen dos versiones: la registrada y la de demostración. La principal diferencia es que en la versión registrada se permite correr el programa en modo escondido. Esto significa que el usuario de la máquina no notará que sus acciones están siendo registradas. En el apéndice B se puede observar un ejemplo de un *log* generado por este programa.

18. Keylogger. Consultada el 05 de noviembre de 2010, de
http://www.keylogger.com/
http://html.rincondelvago.com/informatica-forense.html

STELLAR PHOENIX Y SUS FUNCIONES

- ✓ Software de recuperación de datos: es capaz de recuperar datos perdidos o no accesibles a causa de infecciones de virus, formateo accidental del disco duro, anulación de file, pérdida o corrupción de una repartición, file y carpeta faltantes, acciones de sabotaje por parte de dependientes, fraccionamiento o reformateo del disco. Es un programa de recuperación de datos particularmente fácil de usar que examina su disco fijo ya no accesible a causa de daños lógicos o corrupción y le permite recuperar los datos.

- ✓ Stellar Phoenix Software de Recuperación de Datos se encuentra disponible para ser utilizado en una vasta gama de sistemas operativos y archivos, incluidos los file system FAT, NTFS, HFS, HFS+, NWFS, NSS, HTFS, UFS, UFS2, VxFS, ISO 9660, EXT2, EXT3 y Reiser FS file system.
- ✓ Programa de recuperación file anulados: es capaz de recuperar del cesto de Windows datos anulados o perdidos a causa del formateo del disco duro, de una infección de virus, de una repentina caída del sistema o por un desperfecto de software.
- ✓ Software reparación files: es capaz de reparar y restablecer file Zip y file en formato Microsoft Office (file de Access, Excel, PowerPoint e Word) corrompidos o no accesibles.
- ✓ Software de recuperación mail: es capaz de reparar y recuperar mensajes de correo electrónico perdidos o dañados restableciendo file .dbx, .mbx, .pst y database de Exchange corrompidos o no accesibles.

- El programa para recuperar las password perdidas u olvidadas de documentos/archivos .zip, .doc, .xls y .pst protegidos.
- Programas para la seguridad de los datos informáticos: anulan definitivamente datos, carpetas, grupos de file, unidades lógicas completas, huellas de uso del sistema y huellas de la navegación Internet (cache del browser, cronología, cookies, completamiento automático etc.)

19. STELLAR PHOENIX. Consultada el 05 de noviembre de 2010, de http://www.stellar-info.es/software-stellar.html

OTRAS HERRAMIENTAS FORENSES

FTK IMAGER es una herramienta de software que te permite crear archivos de imagen para su uso posterior en ToolKit Forense. También puede utilizar imágenes FTK para encontrar ciertos archivos en una imagen, e incluso puede exportar archivos a través de imágenes FTK.

20. Consultada el 05 de Noviembre 2010, http://www.google.com/" \l "q=software+de+informatica+forense "http://www.ftkimager.com

HELIX

Hélix, trae herramientas para recolección de información, para copiar discos, para buscar información eliminada, etc..... la ventaja de Hélix es que tiene dos modalidades de funcionamiento, es un desde LiveCD con una gran cantidad de herramientas, y la otra estando desde sistemas Windows permite ejecutar aplicaciones para dicho sistema.

Algunas Herramientas incluidas

1. **AUTOPSY (V. 2.08)** El AutopsyForensic Browser es una interfaz gráfica para la línea de comandos del Sleuth Kit. Juntos, le permiten investigar el sistema de archivos y los volúmenes de una computadora.
2. **CHNTPW (V. 0.99.2 040105)** Es una utilidad de Linux para (re) establecer la contraseña de cualquier usuario con una cuenta valida (local) en sistemas WinNT o Win2000, modificando el password cifrado en el archivo SAM. No es necesario conocer la contraseña anterior para establecer una nueva. Trabaja ***off-line*** (es decir, se debe apagar la computadora y arrancar desde un disco de Linux). El disco de arranque incluye herramientas para acceder a las particiones NTFS. Esta utilidad trabaja con SYSKEY e incluye la opción de apagar la máquina. Se proporciona una imagen de disco de arranque
3. **CLAMAV (V. 0.88.4)** Programa Anti-Virus
4. **DCFLDD (V. 1.3.4)** Es una versión mejorada de dd con características útiles para la investigación forense y la seguridad.

21. http://www.hélix.com

CAINE 2.0 Caine es el acrónimo de Computer Aided INvestigative Environment, un entorno basado en Ubuntu cuyo objetivo es servir de herramienta para la investigación forense digital. Con Caine, una distribución Linux totalmente operativa, podrás realizar las operaciones necesarias para un completo análisis forense. Caine dispone de utilidades como AIR (Automated Image & Restore), Guymager, DC3DD, Autopsy, Foremost, Scalpel, Ophcrack y Fundl, además de un gestor para crear informes con versión para Windows.

Características importantes del software

- ✓ No requiere instalación
- ✓ Fácil de usar e intuitivo
- ✓ Buena selección de programas de análisis

CAINE (Computer Aided INvestigative Environment) es una distribución enfocada al tema de la Informática Forense. El objetivo de la distribución CAINE es ayudar a llevar el proceso de investigación de un análisis forense informático para definir el valor de la evidencia y su relación con el incidente.

Algunas herramientas incluidas son las siguientes:

1. Air 2.0.0
2. Ophcrack
3. Autopsy
4. MountManager
5. Disk Utility
6. Storage Device Manager
7. SSdeep
8. ByteInvestigator

22. **http//www.caine 2.0.com**

CAINE & ABEL Cain y Abel 4.9.30 es una herramienta que permite recuperar varios tipos de contraseñas bajo Windows. Emplea diversos métodos de recuperación, como 'escuchar' la Red, ataques mediante fuerza bruta o diccionarios. También es capaz de analizar el tipo de encriptado de las contraseñas. Cubre algunos aspectos de seguridad o debilidades presentes en los estándares de los protocolos y métodos de autentificación. Además, requiere algunos conocimientos informáticos por lo que un usuario normal puede no entender su interfaz y su funcionamiento. Trae nuevos accesorios como, ARP, que habilita el sniffing en LAN. El sniffer puede analizar protocolos encriptados como SSH y HTTPs, y contiene filtros para capturar credenciales de un amplio rango de mecanismos de autenticación. Permite recuperar varios tipos de contraseñas en programas ejecutados en Windows. Es capaz de realizar varias formas de recuperación como esnifar la red, realizar

ataques de fuerza bruta o utilizar diccionarios. También es capaz de informarte de la clase de encriptado de esas contraseñas

Este programa es capaz de realizar otras tareas como

1. Analizar contraseñas de enrutamiento.
2. Revelar el contenido oculto de las cajas de texto.
3. grabar conversaciones de VoIP.

23. http://www.emule.com/es/
http://es.software.emule.com/sc/ares/
http://es.software.emule.com/t/abel/

MOBILEDIT FORENSICS

Es una herramienta forense que permite analizar el contenido de un teléfono móvil**,** desde la versión del software, hasta las notas o mensajes SMS archivados. El programa puede conectarse a cualquier dispositivo a través de infrarrojos, Bluetooth o cable. Las características principales de este software son las siguientes. Busca, edita, añade y borra entradas de la tarjeta SIM.

- ✓ Capacidad para extraer toda la información referente a la lista de contactos, SMS, ficheros, notas del calendario o imágenes.
- ✓ Opción para generar reportes en formato RTF, XML, XLS, Word o TXT**.**
- ✓ Permite hacer copias de seguridad.
- ✓ Modo de investigación automática.
- ✓ Función para recuperar documentos borrados**.**

24. http://mobiledit-forensic.malavida.com/

SOFTWARE DE RESPALDO Y RECUPERACIÓN DE DATOS ACRONIS

Acronis True Image Home 2009 ofrece la máxima flexibilidad para asegurar que tenga la protección adecuada y pueda recuperarse de eventos imprevistos como, por ejemplo, virus, de software inestable y anomalías de disco duro. Cree una copia exacta del PC para tener una copia de seguridad completa o haga una copia de seguridad solo de los datos y ajustes de aplicaciones más importantes, como prefiera.

Ha acumulado una vida entera de recuerdos en su PC doméstico, además de documentos personales importantes, tales como notificaciones de devolución y currículos profesionales, por no hablar de todas las aplicaciones que ha instalado y los ajustes únicos de cada miembro de su familia y que tardó innumerables horas en configurar. Acronis True Image Home 2009 le ayuda a asegurarse de que tiene la protección adecuada; garantiza que podrá recuperar sus valiosos datos en caso de anomalía del PC o que un virus cause daños en el disco duro del equipo.

Copia de seguridad y recuperación fáciles de realizar

Acronis True Image Home 2009 ofrece una protección completa de su PC: realiza copias de seguridad de todo el PC, incluido el sistema operativo, además de los datos, aplicaciones, imágenes, vídeo, documentos ajustes y todo lo demás.

Acronis True Image Home 2009 es una premiada solución de copia de seguridad y recuperación por un buen motivo: protege su PC con un solo clic y le permite recuperarse de ataques de virus, descargas de productos de software inestables y anomalías en los discos duros. Cree una copia exacta de su PC y restáurela tras un error grave en cuestión de minutos, o haga una copia de seguridad de archivos importantes y recupérelos aún más rápidamente.

FACTIBILIDAD ECONÓMICA

Es donde se valora si los costos a corto plazo no son sobre pasados por las ganancias a largo plazo o no produce una disminución inmediata en los costos de operación.

LOS RECURSOS BÁSICOS A CONSIDERAR SON:

- ✓ Costo del estudio del proyecto (Construcción, electricidad, aires, otras utilidades)
- ✓ Costo estimado del hardware y software

Consideraciones tomadas para la elaboración del presupuesto del laboratorio de informática forense

1. Tomando en cuenta la magnitud del proyecto y la importancia que tiene en la sociedad nicaragüense, hemos decidido que la construcción se lleve a cabo por las normas más altas de seguridad regidas actualmente en el ramo de la construcción civil.

2. El edificio será construido a través del método de construcción conocido como mampostería reforzada: Es decir a base de bloques de concretos y refuerzo en el interior de las paredes o huecos de las piezas de mampostería que a la vez irán rellenos de concreto estructural con una resistencia a la compresión de 3000 PSI.

3. Además este diseño estará fundamentado sobre un cimiento corrido conocido como viga a sísmica la cual garantizará que toda la estructura resista un evento sísmico de las magnitudes que generalmente se conocen en nuestro país, que dicho sea de paso es altamente sísmico y aún más en el departamento de Managua.

4. Con este diseño el edificio se acopla a la realidad actual, ya que podrá resistir los movimientos telúricos que son bastante probables de ocurrir principalmente en Managua que está ubicada en la zona sísmica de las placas coco –Caribe.

5. Las paredes de mampostería reforzada están diseñadas para absorber gran parte de las vibraciones telúricas deformándose de tal manera que impida el colapso total del edificio y garantizando por ende la vida humana.

6. Toda La estructura se comportará de manera elástica ya que al estar reforzada en toda su área por el acero de refuerzo habrá una mayor capacidad de ductabilidad o capacidad de deformación de la estructura.
7. Además el diseño consta de una estructura de techo metálica a base de cerchas, lo que garantiza que todo el peso de la estructura se transmita de forma distribuida a lo largo y ancho de la estructura principal, garantizando aún más la seguridad estructural de todo el diseño.

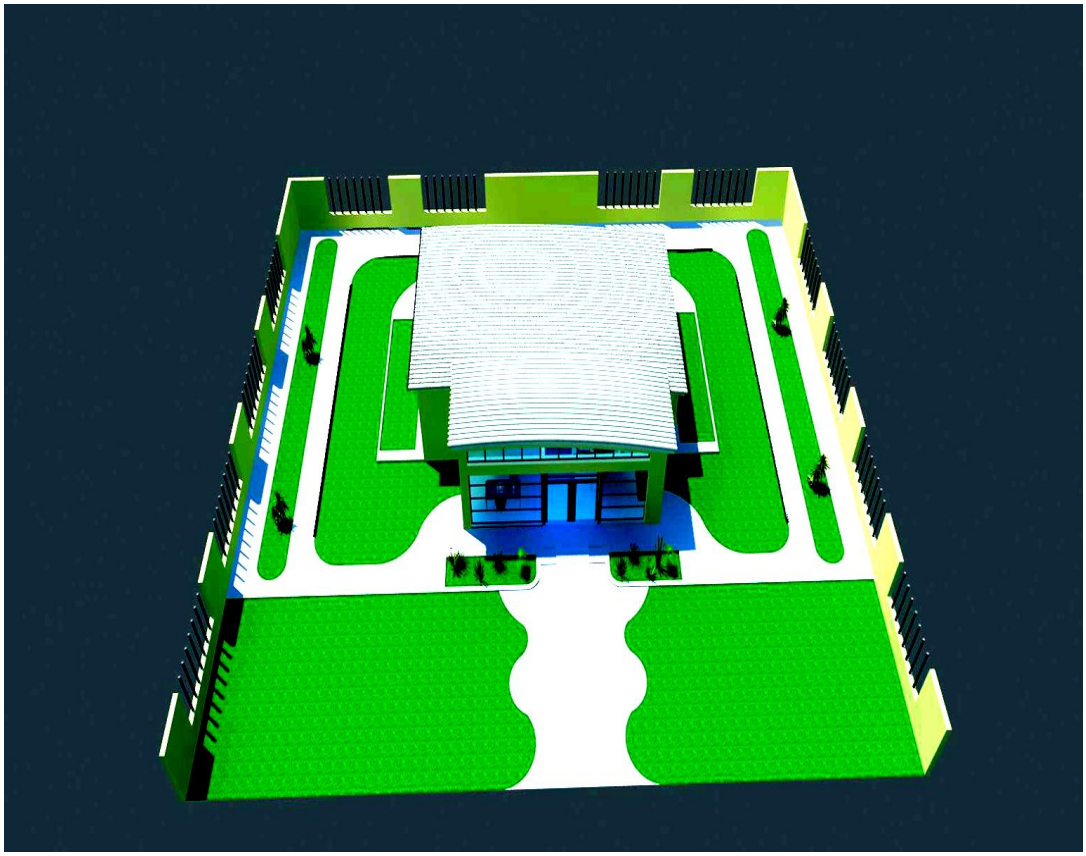
8. De esta forma dejamos bien claro el porqué del diseño escogido y la importancia y responsabilidad que esto conlleva.

9. Hemos elaborado a la par del diseño un presupuesto detallado del costo en que se incurriría si es aceptado para llevarse a cabo. En dicho presupuesto hemos tomado en cuenta el costo real de material + mano de obra el cual se refleja de manera global en cada actividad de construcción que se deba realizar, por lo que fuimos asesorados por un profesional de la construcción, que nos orientó y ayudo con la elaboración del presupuesto.

10. En el presupuesto detallado los precios unitarios están dolarizados y no se toman encuentra los costos indirectos como transporte y otros costos que se suman a la hora de realizar el proyecto. Sin embargo sabemos que si se decide realizar el costo indirecto de la obra oscila entre un 15 y 20 % de los costos directos cuyo monto lo hemos calculado ya y están reflejados en el presupuesto en cuestión.

11. Es así que concluimos esta presentación del diseño del Laboratorio de informática, y esperamos sea tomado en cuenta a la hora de llevarlo a cabo.

- ✓ **COSTO DEL ESTUDIO DEL PROYECTO**



PRESUPUESTO DE LABORATORIO DE INFORMATICA

1.COSTO DE CONSTRUCCION

No.	Nombre del Trabajo	Especificaciones	Unidad	Precio U.	Cantidad	Costo
10	Preliminares					
	limpieza	inicial	m^2	0.42	209.89	88.15
	1. Limpieza	inicial	m^2	0.42	209.89	88.15
	Trazo y nivelacion	nivelacion / valla	m^2	0.35	155.89	54.48
	1.Trazo y nivelacion	niveleta sencilla : L = 1.10 m	C/U	3.06	10	30.6
	2.Trazo y nivelacion	niveleta/doble : L = 1.50 m x 1.50 m	C/U	3.98	6	23.88
	Total (10)					142.63
30	FUNDACIONES					
	1. Excavación estructural	manual , en terreno natural	m^3	4.57	29.6	135.27
	2. Relleno y compactación	manual	m^3	1.34	18.85	25.26
	3. conformación del terreno	cortes y rellenos hasta 5 cms.	m^2	0.15	59.19	8.88
	4. Botar tierrasobrante de excavación	fuera del sitio a una dist.= 1 Km	m^3	1.99	23.075	45.92
	5. Acarreo manual de tierra suelta	Con carretilla a una dist. de 0 a 20 mts.	m^3	0.75	23.075	17.31
	6. Hierro corrugado grado 40	# 3	Kg.	1.03	25	25.75
	7. Hierro corrugado grado 40	# 4	Kg.	1.03	290	,298.70
	8. Formaleta	incluye desmoldante marca Maxikote W V 1 listo	m^2	25.92	60.14	1,558.83
	9. Concreto de 3,000 PSI	con mezcladora	m^3	134.97	11.84	1,598.04
	10. Fundir concreto		m^3	13.07	11.84	154.75
	Total (30)					3,868.71
40	Concreto Estructural					
	Acero de Refuerzo		Kg.	1.03	570.96	589.41
	1. Hierro corrugado < ó = al # 4	# 4	Kg.	1.03	439.2	452.376
	2. Hierro corrugado < ó = al # 4	# 3	Kg.	1.04	131.76	137.0304
	Concreto Estructural		M^3	148.04	12.6	1,865.30
	1. Concreto de 3,000 PSI	con mezcladora	m^3	134.97	12.6	1,700.62
	2. Fundir concreto		m^3	13.07	12.6	164.68
	Total (40)					2,454.71

PRESUPUESTO DE LABORATORIO DE INFORMATICA

1.COSTO DE CONSTRUCCION

No.	Nombre del Trabajo	Especificaciones	Unidad	Precio U.	Cantidad	Costo
50	Mamposteria					
	Paredes de division de interior	Paredes de gypsum	m^2	32.85	15	,492.75
	Pared Bloque N0 6 (manposteria reforzada)	(0.40 m x 0.20 m x 0.15 m)	m^2	29.67	135.85	4,030.67
		pared de bloque expuesto sisado				
		Area = culatas + paredes intermedias				
		Refuuerzo # 3				
	Total (50)					**4,030.67**
60	Techos y fascias					
	1. Estructura de acero(SERCHA /TUBO DE 4 PULG.)	Acero estructural A-36	Kg.	1.86	21062	39,175.32
	2. cubierta de lamina / troquelada aluminizada	Calibre 26	m^2	25	177.4	4,435.00
	3. Cumbrera de de zinc liso	Calibre 26 ;18 pulg. De desarrollo	ml	6.58	16	105.28
	4. Flashing de zinc liso	Calibre 26 ;12 pulg. De desarrollo	ml	4.69	46.6	218.55
	5. Fascia de plycem fijada a estruct.metali.	Espesor = 11 mm;acabado thinset	ml	12.23	76.5	,935.60
	Total (60)					**44,869.75**
70	Acabados					
	1. Piqueteo en concreto fresco	piqueteo en vigas y columnas	m^2	0.35	135.85	47.55
	2. Repello corriente	vigas y columnas	m^2	2.83	1.68	4.75
	3. forja de vigas y columnas hasta 0.20 m	jambas / dinteles	ml	1.04	8	8.32
	4.Fino corriente	vigas y columnas	m^2	1.99	1.68	3.34
	5. Fino en forja de vigas y columnas	jambas / dinteles	ml	0.65	1.68	1.09
	Total (70)					**65.06**

PRESUPUESTO DE LABORATORIO DE INFORMATICA

1.COSTO DE CONSTRUCCION

No.	Nombre del Trabajo	Especificaciones	Unidad	Precio U.	Cantidad	Costo
80	Cielos rasos					
	1. Lamina de plycem texturizado	2' X 4' X 8 mm, color blanco	m^2	18.11	118.72	2,150.02
		Mil suspendido en perfiles metalicos				
	Total (80)					**2,150.02**
90	Pisos					
	1.Conformacion manual del terreno	cortes y rellenos hasta 5 cms.	m^2	0.15	118.74	17.81
	2. Ladrillo ceramica de (0,30 x 0,30) m	0.30 m x 0.30 m t = 5cms.	m^2	17.2	118.74	2,042.33
	Total (90)					**2,060.14**
120	Puertas					
	1. Puertas especiales					
	Aluminio y vidrio abatibles	(0,90 x 2,30) m	c/u	340.00	6	2,040.00
	madera solida abatibles	(0,70 x 2,30) m	c/u	159	2	,318.00
	madera y plywood	(0,64 x 1,47) m	c/u	115	2	,230.00
	Total (120)					**2,588.00**
130	Ventanas					
	1. Ventanas de aluminio y vidrio t. fija / corred,	(diferentes dimensiones)	m^2	8.27	43.12	,356.60
	Total (130)					**,356.60**

PRESUPUESTO DE LABORATORIO DE INFORMATICA

1.COSTO DE CONSTRUCCION

200	Pinturas					
	1.Pintura en paredes vigas y columnas	Marca protecto	m^2	0.5	135.85	67.93
	Total (200)					**67.93**
201	Limpieza final					
	Limpieza final		m^2	0.42	209.89	88.15
	Total (201)					**88.15**

TOTAL U$ 62,742.37

✓ **COSTO ESTIMADO EN ELECTRICIDAD (Basado en la Norma ISO de la electricidad) Y OTRAS UTILIDADES (AIRE ACONDICIONADO, PLANTA ELECTRICA, EXTINTOR).**

DESCRIPCION.	CANTIDAD.	UNIDAD.	OBSERVACION.	COSTO.	
Lamparas 2x40 watts.-	7	unidades	con difusor cromado.	C$ 4,900.00	córdobas
Lamparas ahorrativas 18 watts.	2	unidades		C$ 100	córdobas
Tomas corrientes doble polarizado 120v.	10	unidades		C$ 400	córdobas
Interruptores sencillos decora blanco.	7	unidades		C$ 350.00	córdobas
tubos conduit pvc. De 1/2.	40	unidades		C$ 600.00	córdobas
socket bticino.	2	unidades		C$100.00	córdobas
Bridas EMT 1 oreja de 1/2.	50	unidades		C$ 150.00	córdobas
conectores conduit de 1/2	50	unidades		C$ 100.00	córdobas
Uniones conduit de 1/2.	50	unidades		C$ 100.00	córdobas
Curvas conduit de 1/2.	50	unidades		C$ 100.00	córdobas
Aros de repello 4x4 de 1 gang.	15	unidades		C$200.00	córdobas
Centro de carga 12 espacios CH.	1	unidades		C$ 1000.00	córdobas
Tubo EMTde 3/4.	1	unidades		C$ 60.00	córdobas
Mufa de 3/4.	1	unidades		C$ 100.00	córdobas
Breaker doble de 50 A.	4	unidades		C$ 1600.00	córdobas
Breaker sencillo de 20 A.	3	unidades		C$ 600.00	córdobas
Cajas metalicas EMT 4x4 pesada.	30	unidades		C$ 450.00	córdobas
placas para apagador.	7	unidades		C$ 350.00	córdobas
Teipe 3 m.	10	unidades		C$ 300.00	córdobas
conectores wirenut rojo.	100	unidades		C$ 100.00	córdobas
conductor electrico # 12	300	metros.		C$ 3000.00	córdobas
conductor electrico # 8	100	metros.		C$ 1500.00	córdobas
conductor electrico # 6.	20	metros.		C$ 400.00	córdobas
sockets bticino.	2	unidades.		C$ 120.00	córdobas
Unidades Aire/Acondicionado 36000 BTU	4	unidades.		C$101,700.00	córdobas
Accesorios Aire/Acondicionado., extractores. de instalacion.) tuberias,armaflex,etc.	varios.	unidades.		C$ 21,290.00	córdobas
Generador eléctrico Aw/9996	1	36 KVA		C$124200.00	córdobas
Extintor CO_2	2	20 Libras		C$3600.00	córdobas
COSTO TOTAL APROXIMADO MATERIALES:				**C$ 267,770.00**	**córdobas**
COSTO APROXIMADO MANO DE OBRA.				**C$41,991.00**	**córdobas**
COSTO TOTAL DE PROYECTO.				**C$ 309,761.00**	**córdobas**

✓ **COSTO ESTIMADO DEL HARDWARE Y SOFTWARE**

HARDWARE Y SOFTWARE		
Nº	**Listas de Nombres**	**Costo**
1	Servidor	$ 3,500.00
2	Storage	$ 2,300.00
3	Rack	$ 564.00
4	UPS de 1.5 KVA	$ 699.00
5	Fierewall/routers	$ 200.00
6	Tableau T8	$ 269.00
7	Disk jockey pro Forensic Kit	$ 657.00
8	Computadoras de escritorio	$ 600.00
9	RoadMASSter (Portable Forensic Lab)	$ 12995.00
10	Impresora láser multifuncional con conexión a red	$ 250.00
11	Caja de herramientas, pinzas, destornilladores, cables de datos, cableado de red	$ 300.00
12	Cámara digital	$ 400.00
13	Keylogger	$ 79.00
14	Stellar Phoenix	$ 100.00
15	MOBILedit	$ 599.00
16	WinHex	$ 139.00
17	Internet	$ 250.00
18	Encase	$ 3,000.00
	Costo total de hardware y software	**$ 26,901.00**

✓ **Gastos del proyecto:**

- Pago a un ingeniero por la elaboración de planos estructurales (basados en planos de diseño elaborados en nuestra propuesta) y documento de licitación que se entregaran a los oferentes (registrados en el registro de proveedores del estado autorizados por la construcción de obras verticales MTI) tienen un costo de $2500.

Es importante mencionar que aunque no se entrega planos estructurales solamente de diseño en este documento si se incluye todos los costos en el presupuesto en base a la experiencia del ingeniero civil que nos apoyo en nuestro estudio.

Además este gasto se recupera con la venta de los documentos más los planos a cada oferente. El precio puede ser de C$500 a C$1000 (dependiendo de los gastos en que se incurra y cantidad de oferentes).

- ✓ **Gastos Licitación:**

- ✓ Gasto de publicidad: Los gastos de convocatoria de licitación están sujeto a negociación entre el medio de comunicación que lo va publicar y la policía Nacional por tratarse del estado. Pero el precio por las convocatorias suelen andar en $1000, durante un mes y una vez por semana.

- ✓ **Gastos de impuesto:** El departamento de criminalística no incurrirá en gasto de impuesto porque esta exonerada.

FORMULACIÓN DE HIPÓTESIS

Hipótesis General

La implementación del laboratorio de informática forense para el departamento de criminalística permitirá un mayor control para los diferentes delitos informáticos.

Hipótesis Específicas

1. El laboratorio forense brindara más seguridad a las empresas y negocios.
2. Se obtendrá mayor control sobre los delitos informáticos
3. Ayudara a los peritos informáticos en los procesos de investigación criminalística.

DEFINICIÓN DE VARIABLES

Variable Independiente

1. Implementación del laboratorio de informática forense

Variable dependiente

2. El delito informático

DISEÑO METODOLÓGICO

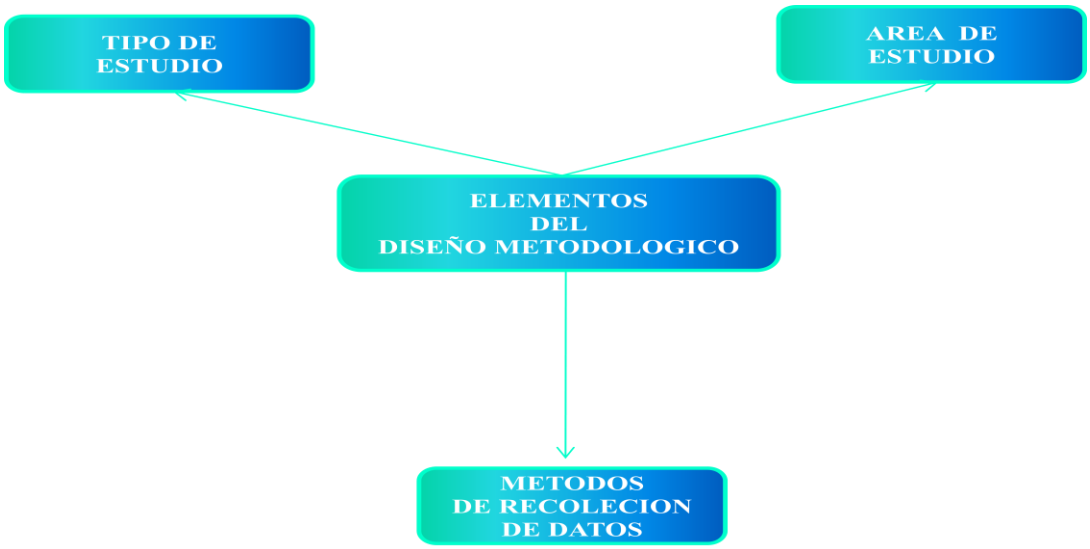


Fig. 3 Resumen contenido Elementos del diseño metodológico

TIPO DE ESTUDIO

El presente estudio es Descriptivo.

ÁREA DE ESTUDIO

- Departamento de criminalística de la Policía Nacional de Nicaragua.

UNIVERSO

La población de nuestra investigación estará constituida por

- ✓ La policía Nacional de Nicaragua.
- ✓ En este universo de estudio se tomó en cuenta a los comisionados mayores del departamento de criminalística de la policía nacional de Nicaragua, a quienes se les aplico entrevistas a fin de conocer el nivel de conocimientos, el procedimiento que darían a casos de delitos informáticos.

MÉTODOS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Las técnicas de recolección de datos utilizadas en la presente investigación serán de fuentes primarias tales como:

- ✓ **Observación**

Se realizó una observación al área de informática del departamento de criminalística de la Policía Nacional de Nicaragua en un estudio transversal en el año dos mil diez, con una frecuencia de dos observaciones en días diferentes.

- ✓ **Entrevista Semiestructurada**

Se aplicó una entrevista semiestructurada a los comisionados mayores e ingeniero informático utilizando un cuestionario con preguntas que cumplieron con determinados propósitos.

Primeramente se solicitó una entrevista con el primer comisionado y jefe del departamento de criminalística y después se hicieron otras entrevistas al segundo comisionado e ingeniero informático.

Esta fue la primera entrevista que realizaron los investigadores al primer comisionado. Necesitamos conversar con usted sobre el planteamiento de un proyecto, que consiste en una propuesta para la construcción de un laboratorio de informática forense y queremos que el departamento de criminalística sea la principal beneficiada. Le haremos algunas preguntas que tenemos escritas en nuestro cuestionario.

La entrevista al primer comisionado se realizó en una única oportunidad, con una duración de entre 30 Minutos. Todas las entrevistas y encuestas se realizaron entre los meses de agosto y septiembre del 2010. Se presentaron instancias en algunas entrevistas en

el que el ingeniero informático y segundo comisionado no contestaron a alguna de las preguntas hechas por los investigadores.

- ✓ **Encuesta** se realizo una encuesta para verificar quienes tenían conocimiento, acerca del delito informático, que métodos y procedimientos se deberían utilizar para combatir los delitos informáticos, también se incluyeron preguntas acerca de las herramientas forense. La encuesta constaba de una lista de preguntas, completes, falso o verdadero etc.

PROPUESTA DE HARDWARE, SOFTWARE E INFRAESTRUCTURA DEL LABORATORIO DE INFORMÁTICA FORENSE PARA LA POLICÍA NACIONAL DE NICARAGUA.

DIAGRAMA DEL LABORATORIO FORENSE

- ✓ **EQUIPOS FORENSE PARA EL LABORATORIO**

- ✓ **SERVIDOR**

Requerimientos

Se propone la instalación de un servidor con soporte de tecnología de virtualización Intel (VT-Tecnología) el cual será utilizado para montar máquinas virtuales, tanto open source como propietario y brindará un servicio de aplicaciones forenses, de acuerdo a lo propuesto en este documento. Este servidor actuara funcionalmente equiparado a un NAS (Network Área Storage) para el almacenamiento de backups, evidencias digitales y reportes técnicos. Tendrá un espacio de almacenamientos en discos SATA de 4Tb.

Se ha propuesto un Servidor con soporte para infraestructura virtualizada, esto con el objetivo de utilizar y optimizar al máximo los recursos. Muchos de los sistemas y/o software de análisis forense corren en distintas plataformas, desde sistemas Unix estándar hasta sistemas Microsoft.

En esencia la principal característica de la virtualización es la capacidad de correr múltiples instancias de un SO sobre un servidor físico, lo cual se traduce en un uso más eficiente de los recursos, aunque en la actualidad los sistemas requieren muchas capacidades de procesamiento, los procesadores de hoy en día son muy poderosos y en la mayoría de los casos son infrautilizados.

Entre las ventajas que nos brinda la virtualización tenemos:

- ✓ Snapshot de máquinas virtuales.
- ✓ Crecimiento sobre la marcha, es decir si los requerimientos de un sistema aumentan, basta con asignarle más recursos a la VM.
- ✓ Conversión de maquina física a virtual (P2V) y de virtual a virtual (V2V)
- ✓ Acceso iSCSI desde las máquinas virtuales (Pass Through)

- ✓ Para versiones Enterprise de Windows Server, puedo correr hasta cuatro instancias con licencia sobre una instalación física, para Datacenteredition, infinitas instancias de VMs. Se propone un servidor DELL RE710.

- ✓ **PROPUESTA DEL SISTEMA NAS**

Lo importante en el sistema de almacenamiento es la velocidad de los discos, cantidad de Storage y capacidades de administración, sistemas NAS son mucho más económicos que los sistemas SAN, esta es la razón por la que se ha decidido seleccionar los primeros.

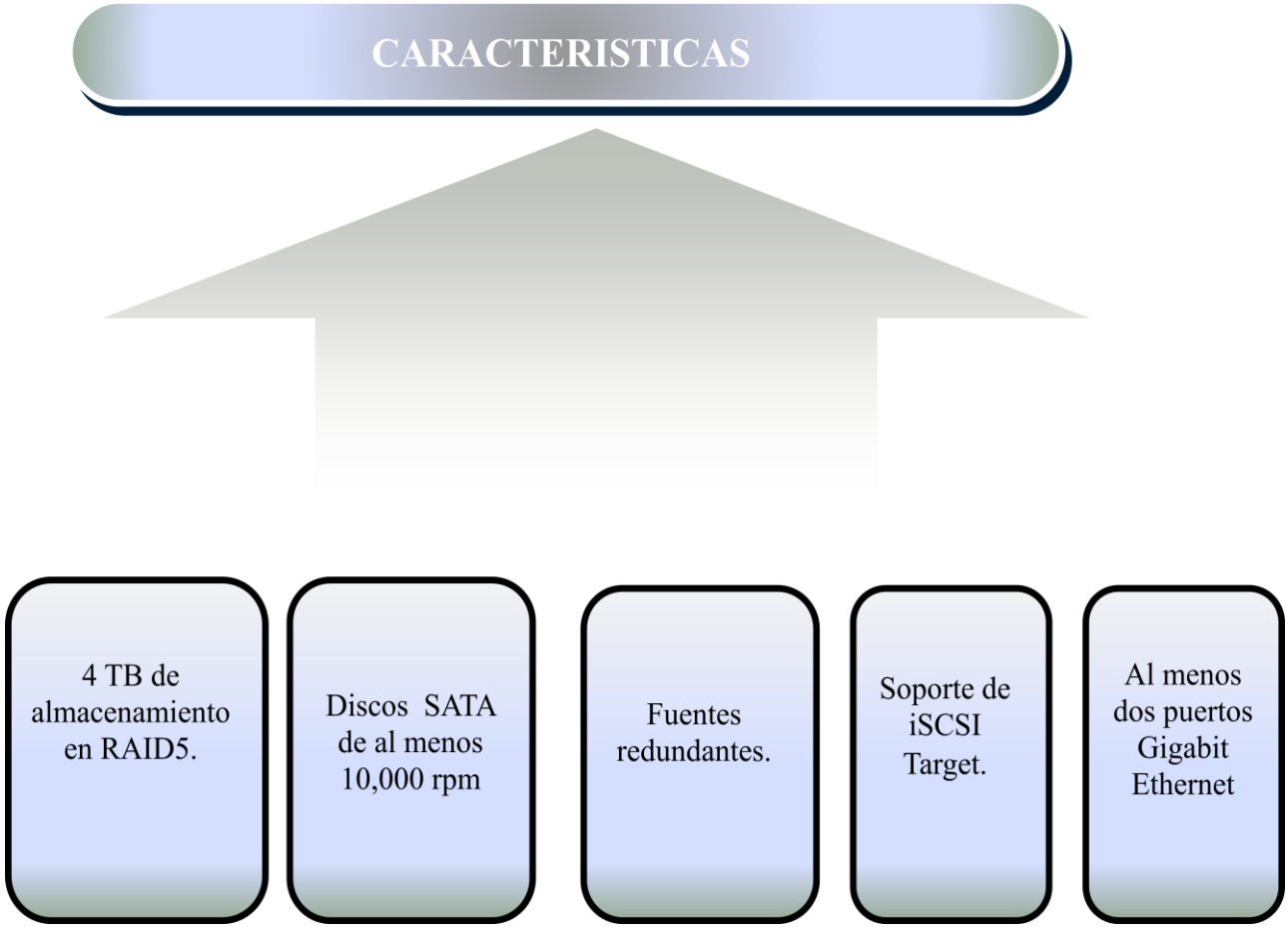
En el sistema NAS se creara un volumen RAID5, lógicamente dividido en:

- **Zona uno*:*** la primera zona se implementara como una unidad lógica de 2 Tb, este repositorio se utilizara para almacenar información de los casos trabajados (ej. Informes técnicos, dictámenes etc...) Y también se guardara de forma selectiva alguna evidencia digitales que sea conveniente resguardar, porque dicha evidencia puede ser objeto de un peritaje posterior.

- **Zona dos*:*** la segunda zona tendrá un espacio de 1.5 Tb se utilizara principalmente como repositorio de trabajo temporal para actividades forenses específicas.

  Se propone la configuración de un Raid5 para tolerancias a los fallos, y mayor capacidad de al almacenamiento. El NAS debe ser escalable al menos hasta 12 TB.

  Se propone un NAS Synology RS810.

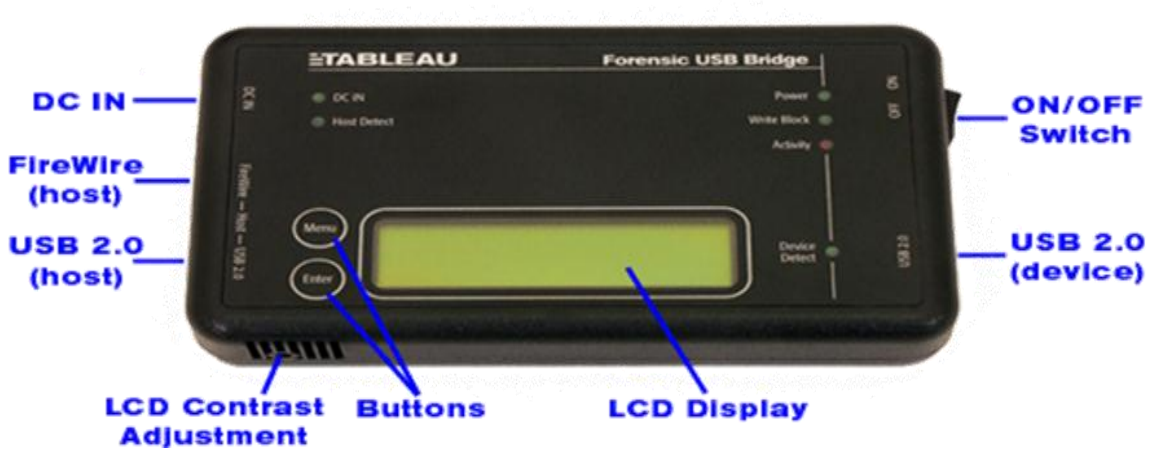


- ✓ **RACK**

- ✓ **UPS**

✓ HERRAMIENTAS DE HARDWARE FORENSE

TABLEAU T8



DISK JOCKEY

Product specifications

1. Model number, DJ-2000
2. Product Name: Disk Jockey IT
3. Interface: USB 2.0 (standard rev 2) / IEEE 1394 (S400)
4. USB Connector: Receptacle B
5. IEEE 1394 connector type: 4 pin by 2
6. Weight: Approximately 4 ounces
7. Dimensions: W 64mm D 148 mm H 42mm 8. Temperature / Humidity Specs: Temperature 5 – 35 degrees centigrade. Humidity: 20-80% (Non condensing)

MALETÍN DEL INVESTIGADOR FORENSE

Cables UTP CAT5 para conexión Ethernet: Directo y cruzado
Destornilladores
Kit de pinzas
Marcadores indelebles
Cinta de embalaje
Etiquetas de seguridad
Guantes de latex
Cúter
Cables de datos PATA para conexión de discos rígidos
Cables de alimentación para PC
CD-R y DVD-R vírgenes
Estaño
Cautil

RoadMASSter 3 Mobile Forensics Data Acquisition and Analysis Computer Lab:

Specifications

Supply Voltage: 400watt with 100 - 240V / 50 - 60 Hz

Power Consumption: 180W without drives

Operating Temperature: 5 degrees - 55 degrees C

Relative Humidity: 20% - 60% non-condensing

Net Weight: 37 lbs

Universal Auto-Switching input voltage

Processor: AMD Opteron, low power (260HE)

Memory: 4GB RAM

Hard Drive: 100GB 7200RPM internal NoteBook SATA drive

Other storage: CD-RW, DVD -/+ RW, FDD

Display: 15” TFT color LCD display, super bright with 600NIT

Sound System: Stereo speakers and line in/line out connector

Case dimension: 21.7" x 14.1" x 8.9"

Operation System: Windows XP Professional

IMPRESORA

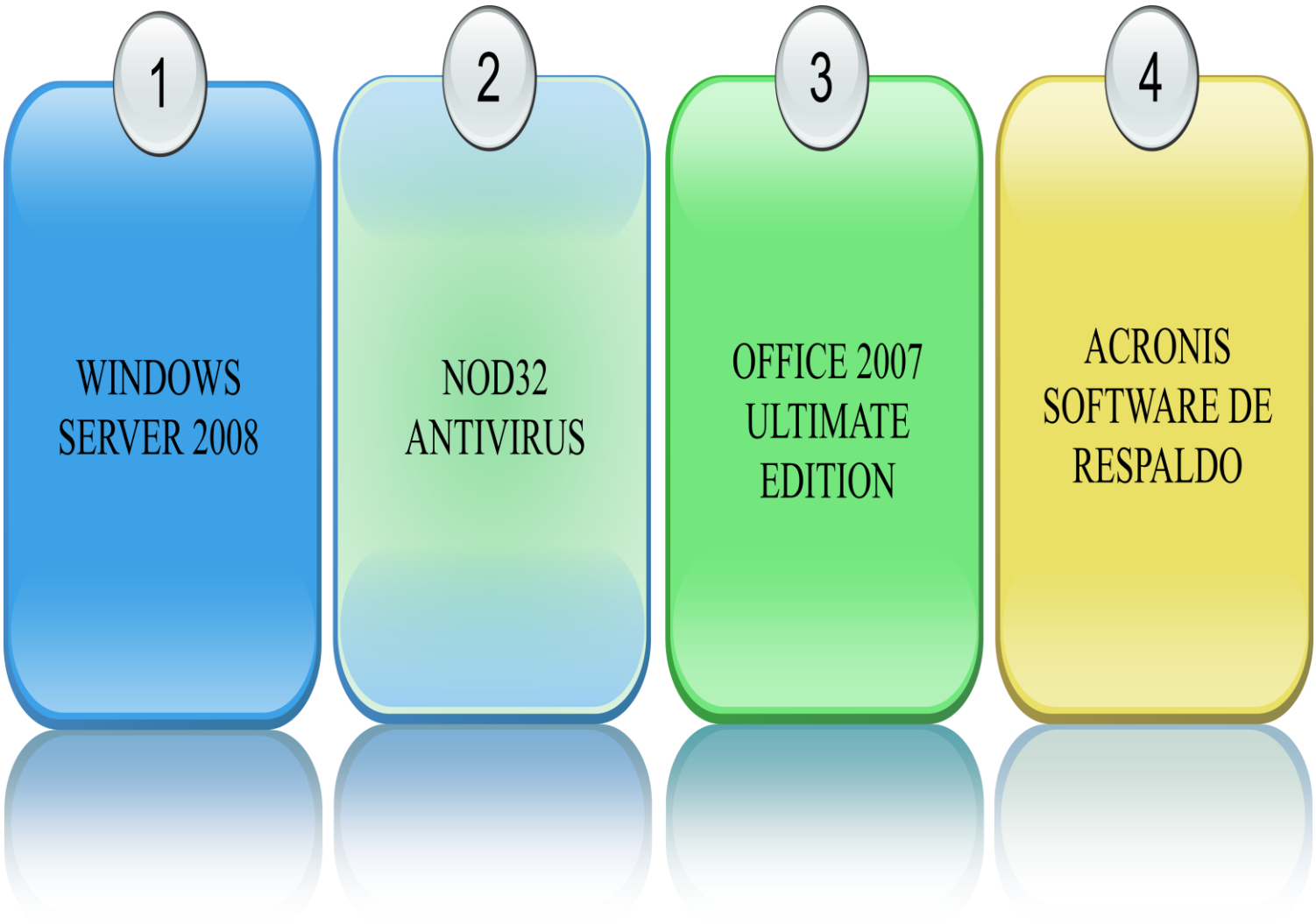
Característica
Impresora láser multifuncional con conexión a red HP OfficeJet serie H470.

Especificaciones	
Velocidad de impresión en negro (borrador, A4)	Hasta 22 ppm
Velocidad de impresión en color (borrador, A4)	Hasta 18 ppm
Calidad de impresión en negro (óptima)	**H470:** Hasta 1.200 x 1.200 ppp de reproducción cuando se imprime desde un ordenador **H470wbt / H470b:** Ofrece hasta 1.200 x 1.200 ppp (cuando imprime desde un ordenador)
Calidad de impresión en color (óptima)	Hasta 4800 ppp
Ciclo de trabajo (mensual, A4)	Hasta 500 páginas
Pantalla	Nada
Número de cartuchos de impresión	4 tintas HP Vivera, opcional de 6 tintas
Velocidad del procesador	192 MHz
Memoria de serie	32 MB
Idiomas estándar de la impresora	HP PCL 3 mejorado
Manejo de papel	
Manejo de papel estándar/entrada	Bandeja de ent. de 50 hoj.
Opciones de impresión a doble cara	Manual (soporte para controlador suministrado)
Capacidad de entrada máxima (sobres)	Hasta 5

Impresión sin bordes	Sí (100 x 150 mm, con o sin lengüeta desprendible/recortable)
Tamaños de material admitidos	A4 (210 x 297 mm), A5 (148 x 210 mm), A6 (105 x 148 mm), B5 (176 x 250 mm), C6 (114 x 162 mm), DL (110 x 220 mm), 100 x 150 mm (con o sin lengüeta desprendible/recortable)
Tamaños personalizados de soporte	de 76,2 x 210 a 215,9 x 355,6 mm
Tipos de soporte admitidos	Papel (inyección de tinta, fotográfico, normal), tarjetas (índice, felicitación), sobres, etiquetas, transparencias
Conectividad	
Conectividad estándar	**H470b / H470:** 1 USB (2.0); 1 USB (1.0); 1 PictBridge; 2 ranuras para tarjeta de memoria **H470wbt:** 1 USB (2.0); 1 USB (1.0); 1 PictBridge; 2 ranuras para tarjetas de memoria; 1 Bluetooth
Conectividad opcional	**H470wbt:** Adaptador de impresora inalámbrica HP 802.11 b/g Q6274A **H470b / H470:** Adaptador inalámbrico Q6273A HP bt500 Bluetooth USB 2.0, adaptador de impresora inalámbrico Q6274A HP 802.11 b/g
Requisitos de energía y operación	
Sistemas operativos compatibles	Preparada para Microsoft® Windows® 7. Para obtener más información, vaya a http://www.hp.com/go/windows7. Windows Vista®, Windows® XP Professional x64, Windows® 2000, Windows® Foundation Server 2008, Windows® Small Business Server 2008 Standard Edition; Mac OS X v 10.3.9, Mac OS X v 10.4 o más elevado, Palm OS, Windows Mobile® para PC de bolsillo, Linux (visite http://www.hplip.net)
Requisitos mínimos del sistema	Microsoft® Windows® 2000: Procesador Intel® Pentium® II o Celeron®, con 128 MB de RAM y 150 MB de espacio libre en el disco duro; Microsoft® Windows® XP (32 bits): Procesador Intel® Pentium® II o Celeron®, 128 MB RAM, 250 MB de espacio libre en el disco duro; Microsoft® Windows® XP Professional x64: Procesador Intel® Pentium® II o Celeron®, con 128 MB de RAM y 280 MB de espacio libre en el disco duro; Windows Vista®:

	Procesador de 800 MHz y 32 bits (x86) o 64 bits (x64), 512 MB RAM, 750 MB de espacio libre en el disco duro
Requisitos mínimos del sistema para Macintosh	Mac OS X (v10.3.9 y superior, v10.4.6 y superior): PowerPC G3 de 400 MHz (v10.3.9 y superior, v10.4.6 y superior) o Intel® Core Duo de 1.83 GHz (10.4.6 y superior), 256 MB de RAM, 200 MB de espacio libre en el disco duro, QuickTime 5.0 o superior
Gama operativa de humedad recomendada	de 15 a 90% de HR
Consumo energético	40 vatios máximo, 24 vatios máximo (activa/imprimiendo), 0,4 vatios máximo (apagada)
Emisiones de potencia acústica	5,1 B(A) (Óptima), 6,1 B(A) (Normal), 6,4 B(A) (Borrador)
Tiempo de recarga de la batería	Aprox. 1 h y 30 m.
Certificación ENERGY STAR®	Sí

- ✓ **SOFTWARE BASE**



HERRAMIENTAS SOFTWARE FORENSE

REQUISITOS PARA OPTAR A UN CARGO

Administrador de Redes

Funciones:

1) Programación de dispositivos de acceso a información basados en redes de telecomunicaciones, tanto bajo ambiente Unix como ambiente Windows.
2) Diseño, implantación y administración de redes de computadoras y sistemas para transmisión de datos.
3) Administración de sistemas operativos y servicios orientados a redes.
4) Especificación, diseño y administración de protocolos que permitan la interconexión de usuarios y aplicaciones a través de los medios de transmisión.
5) Administración de sistemas de telecomunicaciones.
6) Cooperación en la gestión de redes y servicios telemáticos

Requisitos:

a) Ing. en Telemática o Ing. en Computación
b) Experiencia Mínima 3 años
c) Idioma: Ingles
d) Software: Analista y Desarrollador de Sistemas

Analista

Funciones:

- Diseño y promoción de software.
- Revisión y evaluación de sistemas de información.
- Capacitación de personal técnico y usuarios de sistemas informáticos.
- Administración de las funciones informáticas de la empresa.
- Auditoría de sistemas.
- Manejar el software forense para la preservación, identificación, extracción, documentación e interpretación de la evidencia digital.

Requisitos:

a) Ing. En Sistemas o Lic. En Computación
b) Experiencia: 2 Años
c) Idioma: Ingles

Técnico en Reparación

Funciones:

1) Brindar Mantenimiento y Reparación de Pc
2) Soporte técnico de instalación y configuración de Programas

Requisitos:

a) Lic. En Computación o Lic. En Informática

CONCLUCIONES

En el presente estudio sobre la implementación de la informática forense para el departamento de criminalística de la Policía Nacional de Nicaragua se logra dar un aporte al desarrollo Jurídico, tecnológico, cultural y social. Siendo nuestras únicas limitaciones naturales el poder demostrar en su totalidad el funcionamiento de las herramientas comerciales de hardware y software propuestas, puesto que, es un dinero que no está al alcance de nosotros, sin embargo se pretende dar una visión amplia de las ventajas que se obtendrían al adquirirlas en unión con las herramientas libres.

RECOMENDACIONES

- ✓ Para accidentes ocurridos por fenómenos naturales como terremoto se recomienda hacer un respaldo en la nube de la información ó un segundo servidor en otra parte del país.

- ✓ Aumentar el presupuesto del laboratorio de criminalística en el área de informática forense a través de las siguientes opciones:

1. Implementar cursos de diplomado en informática forense a nivel internacional con un determinado precio.
2. Fomentar el intercambio solidario impartiendo capacitaciones gratis a nivel internacional sobre la informática en general.

BIBLIOGRAFIA

1. Introducción a la informática forense. Consultada el 13 de noviembre de 2010, de http://www.alfa-redi.com/apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/Acurio.pdf

2. Informática forense. Consultada el 10 de noviembre de 2010, de

http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf

3. Que es la informática forense. Consultada el 05 de noviembre de 2010, de http://www.informaticaforense.com/criminalistica/faqs/general/que-es-la-informatica-forense.html

4. Informática forense. Consultada el 10 de noviembre de 2010, de

http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf

5. Introducción a la informática forense. Consultada el 13 de noviembre de 2010, de http://www.alfa-redi.com/apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/Acurio.pdf

6. Informática Forense, Introducción y Contenido. Consultado el 20 de octubre de 2010, de

http://labs.dragonjar.org/laboratorios-informatica-forense-introduccion-y-contenido

7. Introducción a la informática forense. Consultada el 13 de noviembre de 2010, de http://www.alfa-redi.com/apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/Acurio.pdf

8. Informática Forense, Introducción y Contenido. Consultado el 20 de octubre de 2010, dehttp://labs.dragonjar.org/laboratorios-informatica-forense-introduccion-y-contenido

9. Consultado 29 mayo 2011, especificaciones tableau t8: http://www.tableau.com/index.php?pageid=specs&model=T8

10. Consultado 01 de mayo 2011, DiskJockeyUserGuide: http://www.diskology.com/DiskJockeyUserGuide.pdf

11. Consultado 01 de mayo del 2011, especificaciones ups. http://www.cajasmodding.com/sai-15-kva-online-con-cpu-y-lcd-p-383.html

12. Consultado 25 de abril del 2011, http://www.lawmate.eu/itforensik/index.html

13. http://www.microsoft.com/latam/technet/windowsserver/longhorn/evaluate/whitepaper.mspx

14. Forense digital. Consultado el 15 de octubre de 2010, de

http://html.rincondelvago.com/informatica-forense.html

15. ENCASE. Consultada el 05 de noviembre de 2010, de
http://www.guidancesoftware.com
http://html.rincondelvago.com/informatica-forense.html
http://www.encase.com/Products/ef_index.asp

16. ULTIMATE ACCESSDATA'S TOOLKIT. Consultada el 05 de noviembre de 2010, de
http://kulio.crearblog.com/?p=6993
http://www.compute-rs.com/es/consejos-979135.htm
http://www.accessdata.com/products/utk/

17. WINHEX. Consultada el 05 de noviembre de 2010, de
http://www.x-ways.net/Forensics/index-m.html
http://www.x-ways.net (shareware)

18. Keylogger. Consultada el 05 de noviembre de 2010, de
http://www.keylogger.com/
http://html.rincondelvago.com/informatica-forense.html

19. STELLAR PHOENIX. Consultada el 05 de noviembre de 2010, de
http://www.stellar-info.es/software-stellar.html

20. Consultada el 05 de Noviembre 2010,
http://www.google.com/" \l "q=software+de+informatica+forense
"http://www.ftkimager.com

21. http://www.hélix.com

22. http//www.caine 2.0.com

23. http://www.emule.com/es/
http://es.software.emule.com/sc/ares/
http://es.software.emule.com/t/abel/

24. http://mobiledit-forensic.malavida.com/

26.http://ads.us.eplanning.net/ei/3/805f/57caa0b06e6fa9f9?rnd=0.25981007089863717&pb=8249609d496f2efa&fi=72a3f7e5df2baf7d

ANEXOS

ENCUESTAS

1. ¿Qué entiende por informática forense?
2. Mencione 3 delitos informáticos
3. ¿Cuál es la importancia de contrarrestar los delitos informáticos para usted?
4. ¿Cuáles son los procedimientos legales que usted u otra persona relacionada con los casos de delitos informáticos realizan para no alterar las evidencias del crimen informático?
5. ¿Conoce usted cuantas denuncias por delitos informáticos aún no han sido resueltas?, ¿Cuánto tiempo aproximadamente se demora en resolver estos tipos de casos?, ¿Cuál es el motivo de la demora en la solución de los casos?
6. Marque con una x si existe un responsable que detecte, investiga y prevenga los delitos informáticos

   Detecte Sí _____ No_____
   Investigue Sí _____ No_____
   Prevenga Sí _____ No_____

7. En la escala del 1 al 10 que porcentaje de peligro tiene para usted los delitos informáticos en la ciudad contra los delitos convencionales

   1-5 Poco _____
   6-8 Bastante _____
   9-10 Mucho _____
   Si es si Justifique
   Código _____ Ley _____ Articulo _____

8. Conoce algunas herramientas (hardware o software) a utilizar para contrarrestar los delitos informáticos

   Sí _____ No _____

ENTREVISTAS Y OBSERVACIÓN

- ✓ Origen del área de informática en el laboratorio de criminalística
- ✓ ¿Se crea la unidad de informática para desarrollar software?
- ✓ ¿Qué incluye autonomía del funcionario (informática)?
- ✓ Nombre del personal, perfil y cargo en el área de informática
- ✓ Considera normal que además de realizar las funciones de dirección realice soporte técnico
- ✓ ¿Cuál es la misión y visión de la unidad de informática del laboratorio?
- ✓ Infraestructura del laboratorio de informática
- ✓ Total de computadoras existentes en todo el laboratorio
- ✓ Ejemplo de casos o actividades que han sido resuelto haciendo uso herramientas de computación
- ✓ Podría mencionar programa que les han ayudado a resolver los casos. ¿total?
- ✓ Los programas que utilizan son: software libre, comprados o por amistades que facilitan
- ✓ Evidencias sobre las que trabajan en el área de informática
- ✓ ¿Cuántos casos se han resuelto con la intervención de informática?, ¿cuántos casos no resuelto existen?
- ✓ ¿Que consideran ustedes les hace falta para mejorar en cantidad de casos resueltos?
- ✓ Existen algún manual de funciones o procedimientos en el área de informática
- ✓ Algún fiscal los ha llamado para estudiar evidencias digitales
- ✓ ¿Cuáles son los pasos a seguir cuando se presenta un caso de delitos informáticos?, ¿Cuál es la cadena de custodia?
- ✓ ¿Cuál es el motivo de la demora en la solución de los casos sobre delitos informáticos?

LISTA DE MANUALES DE LAS DIFERENTES HERRAMIENTAS PROPUESTAS PARA EL PROYECTO

MOBILEDIT FORENSICS

Manual de usuario

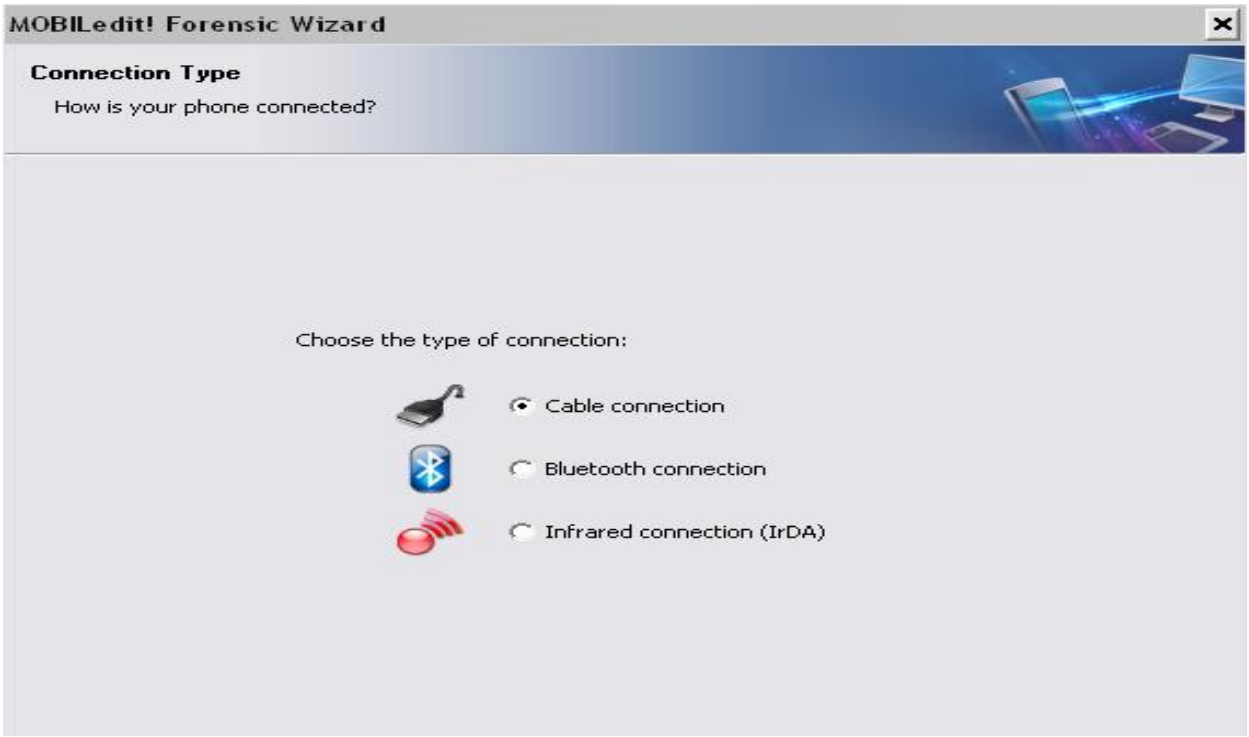
Es una herramienta forense que permite analizar teléfonos móviles, las características principales de este software son las siguientes.

- ✓ Busca, edita, añade y borra entradas de la tarjeta SIM
- ✓ Permite hacer copias de seguridad
- ✓ Exporta la libreta de direcciones a Outlook, MS Office
- ✓ Software de exploración de ficheros
- ✓ Recupera mensajes borrados del teléfono y de tarjeta SIM.
- ✓ Tiene tres tipos de conexión por cable USB, bluetooth y infrarrojo

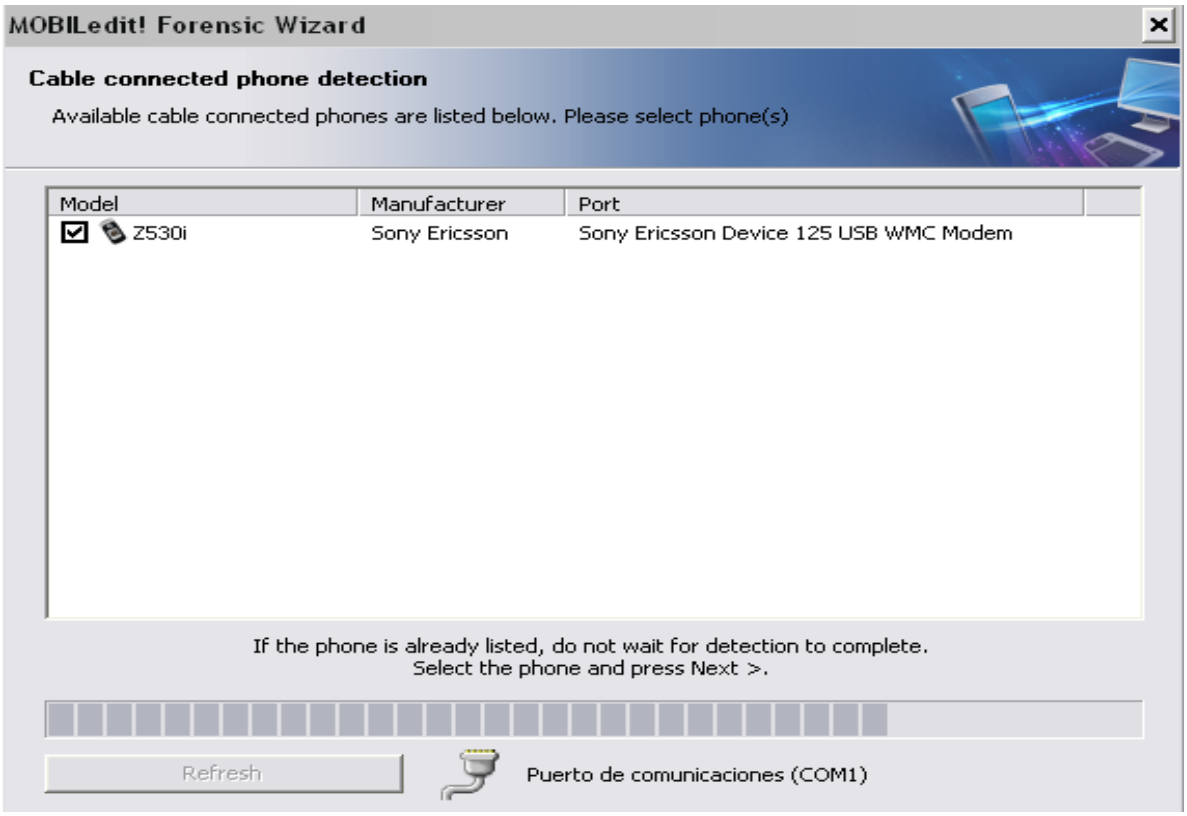
Pantalla inicial de **MOBILEDIT FORENSIC** y Seleccionamos **Connect a phone. Start**

A continuación click en **Phone**

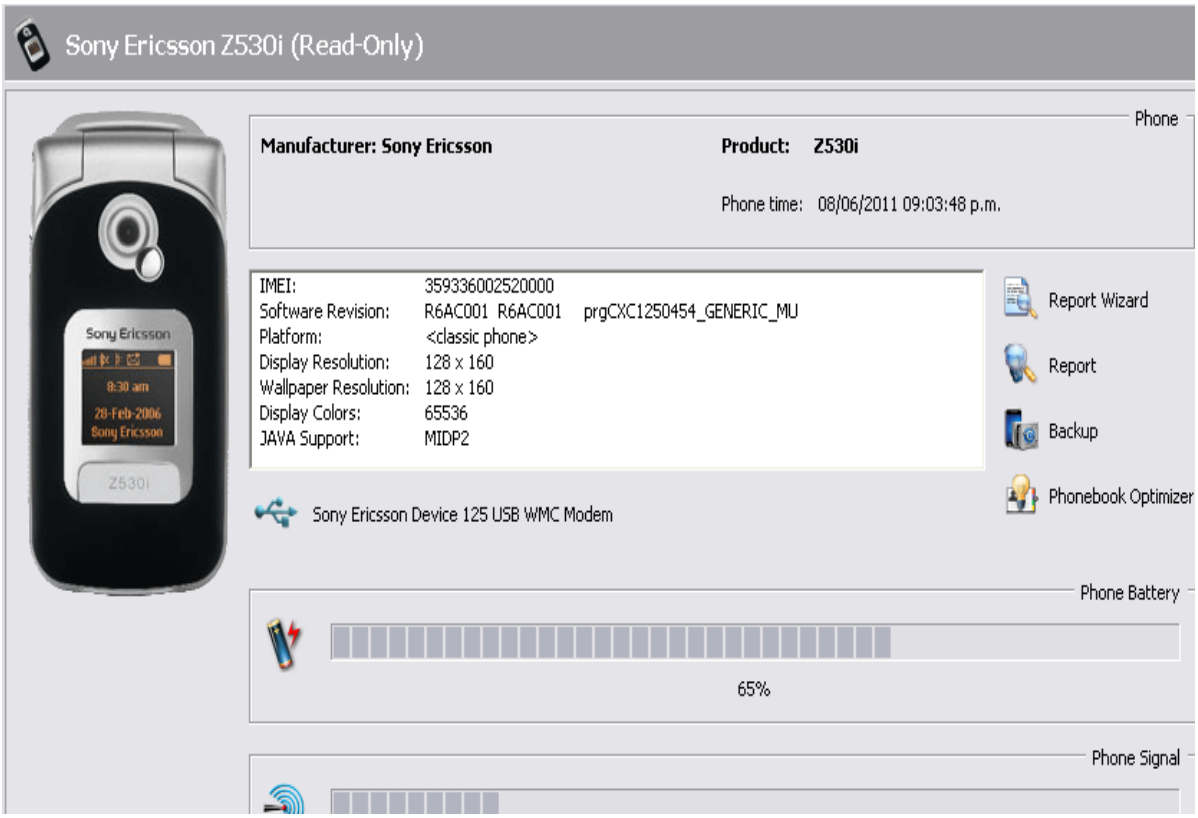
En Tipo de conexión seleccionamos **Cable connection**



Luego el móvil es detectado y posteriormente se presiona el botón S**iguiente**

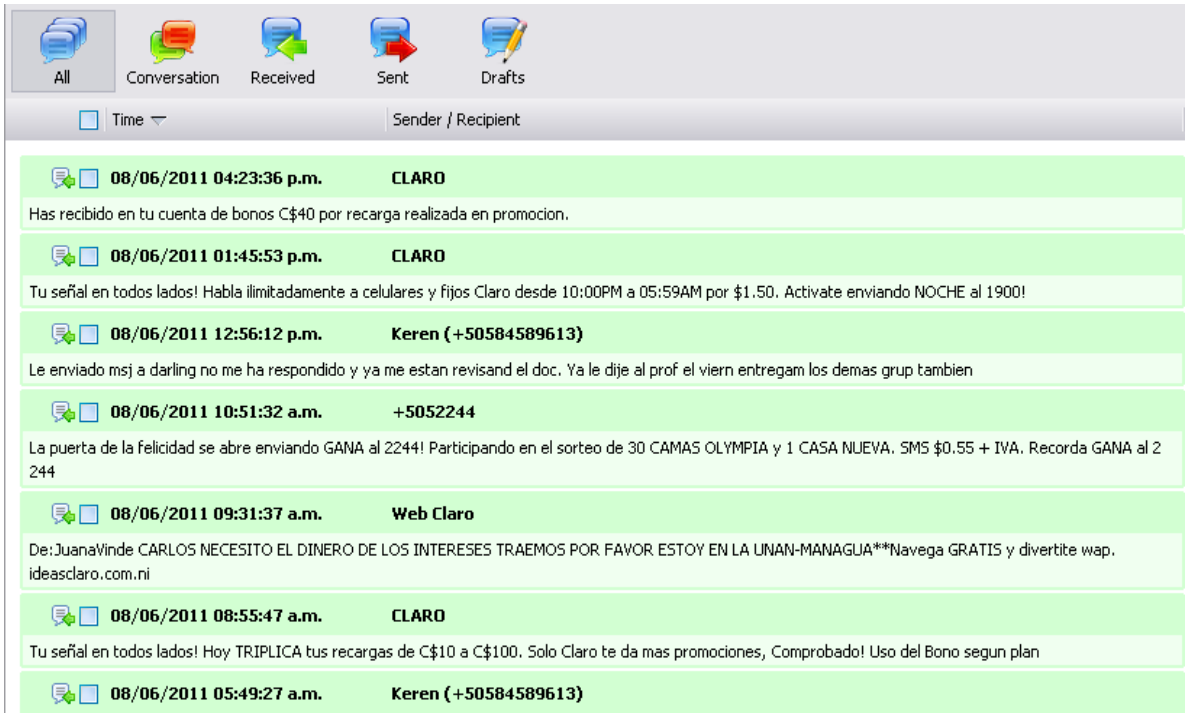


Menú principal de la herramienta, se especifica el modelo del **móvil, estado de la batería**…

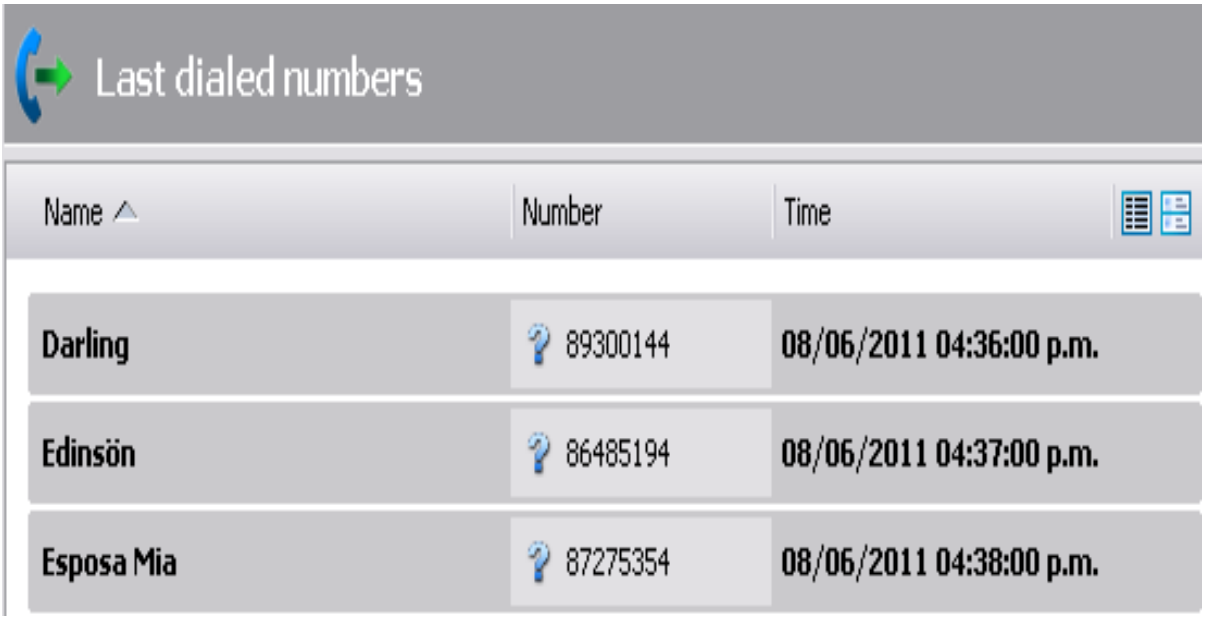


Seleccionamos **Agenda de teléfono** para visualizar todos los números contenidos en dicho móvil.

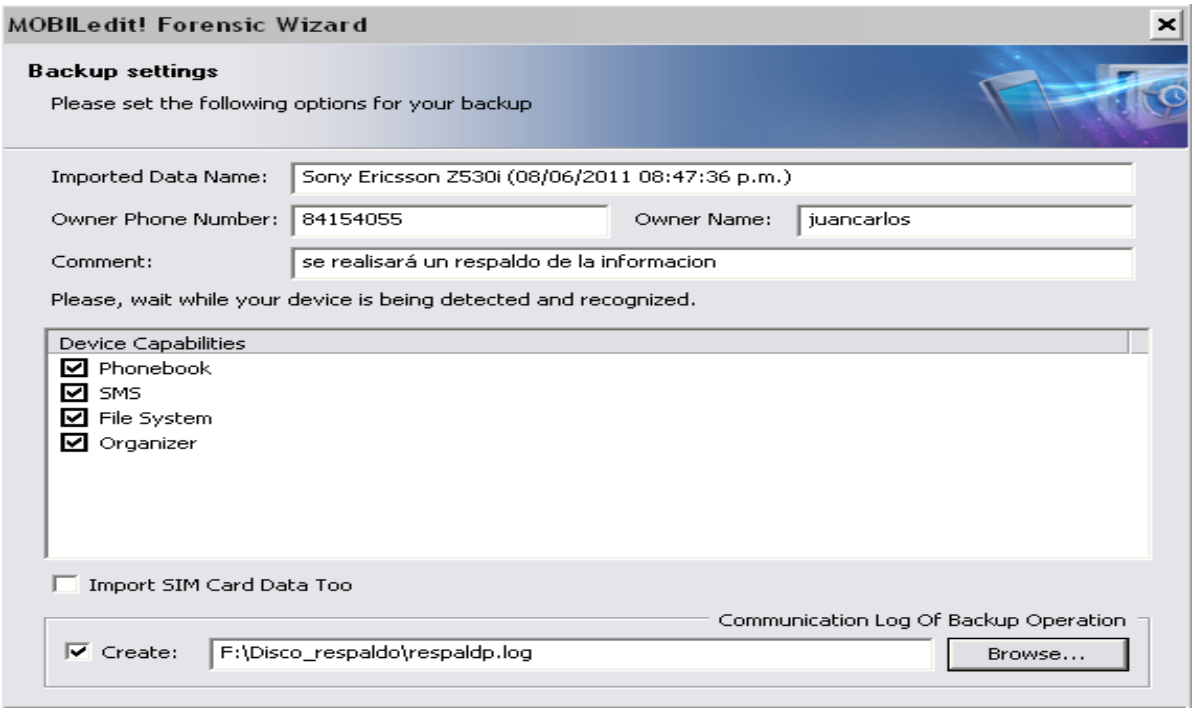
En la siguiente pantalla se visualiza los mensajes enviados, **recibidos, editados y conversaciones, también podes recuperar mensajes borrados**.



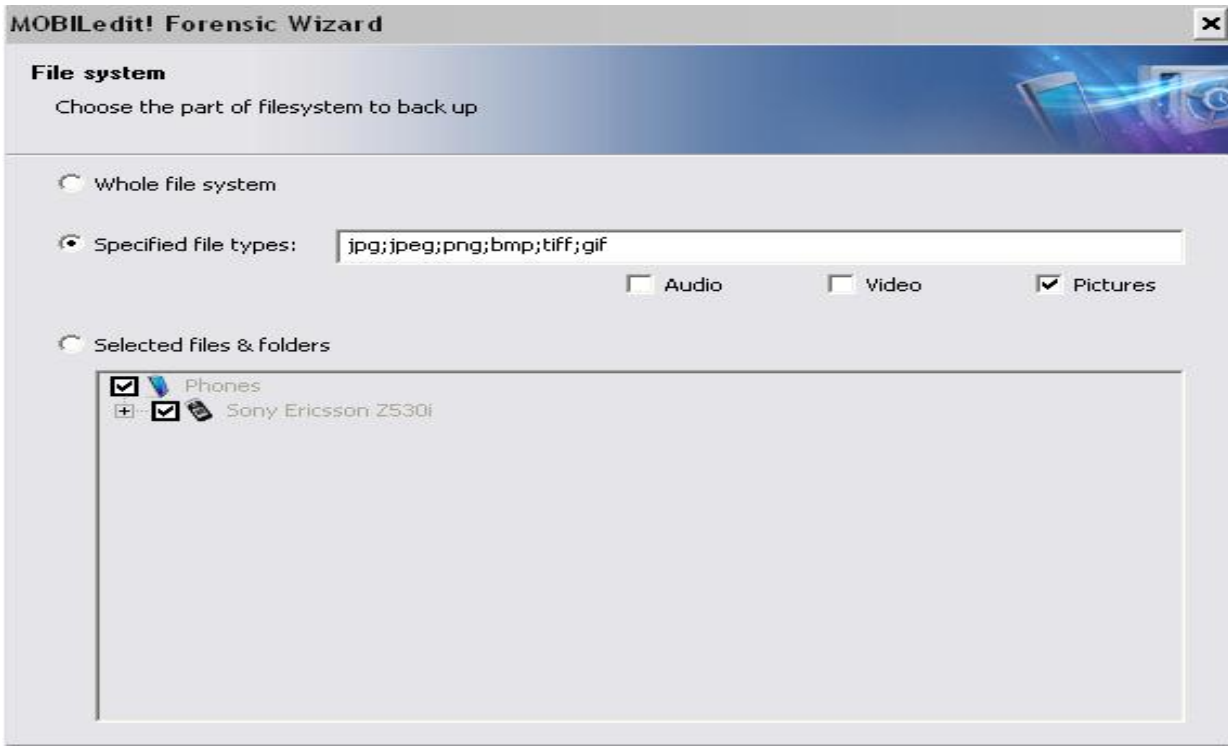
MOBILedit te permite verificas las ultimas llamadas **realizadas, recibidas, perdidas** cada llamada contiene su respectiva fecha y hora.



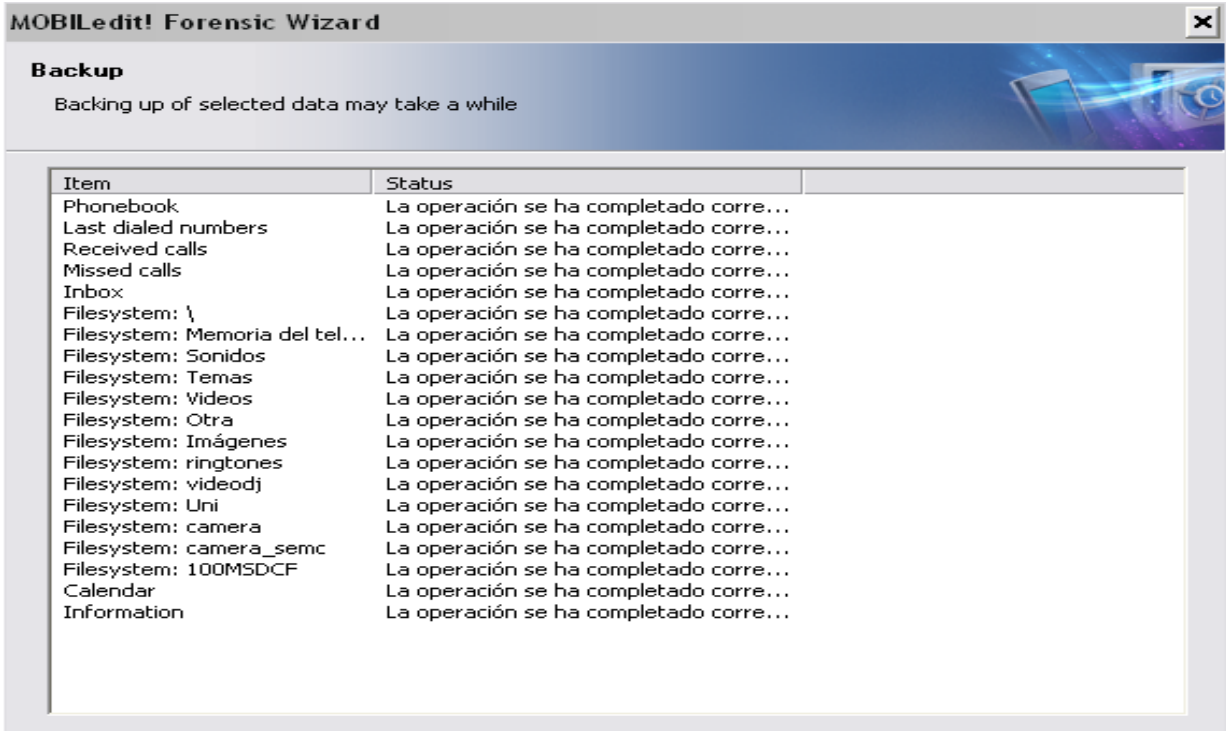
El software permite crear copias de seguridad **vea las siguientes pantallas**



9.1 Seleccionamos **Pictures** y a continuación **click Siguiente**



9.2 A continuación se muestra las operaciones terminadas, click en **Finalizar** para terminar el proceso.

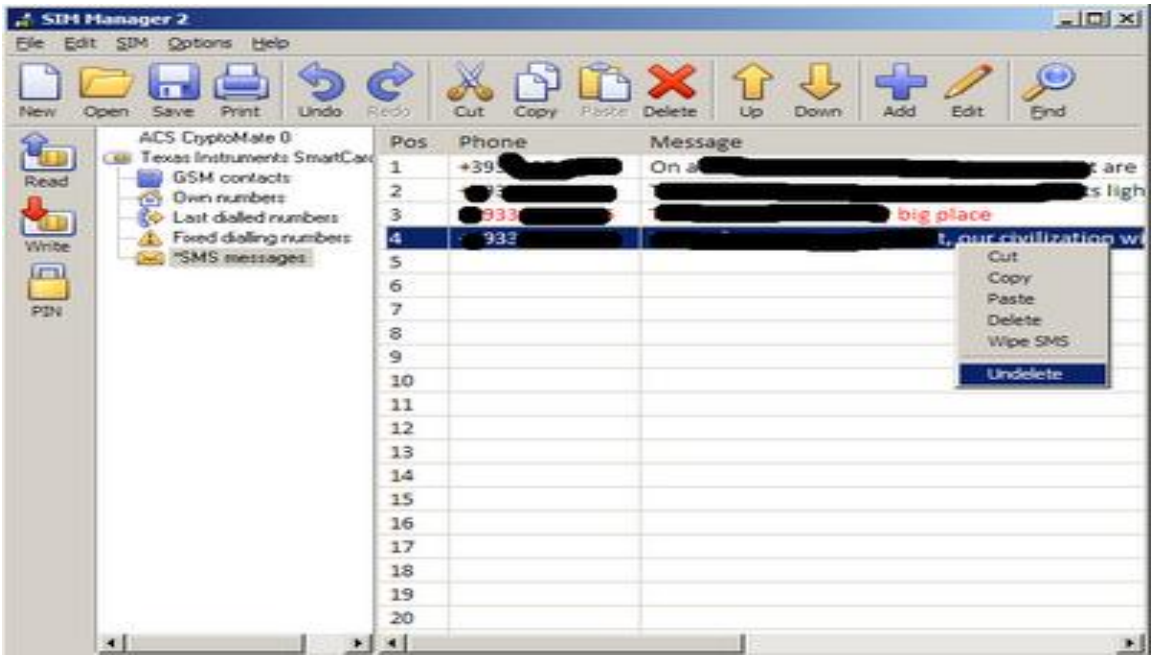


Otra herramienta para recuperar SMS'S de la SIM

Los SMS pueden ser recuperados, con la siguiente herramienta **SIM Manager.**

NOTA: ¡¡Solo funciona correctamente con la versión en Ingles!!

SIM Manager mostrará los mensajes que fueron marcados como eliminados en color rojo, pulsamos con el botón derecho del ratón y pulsamos recuperar. La siguiente captura de pantalla muestra una tarjeta SIM con 20 ranuras de SMS.

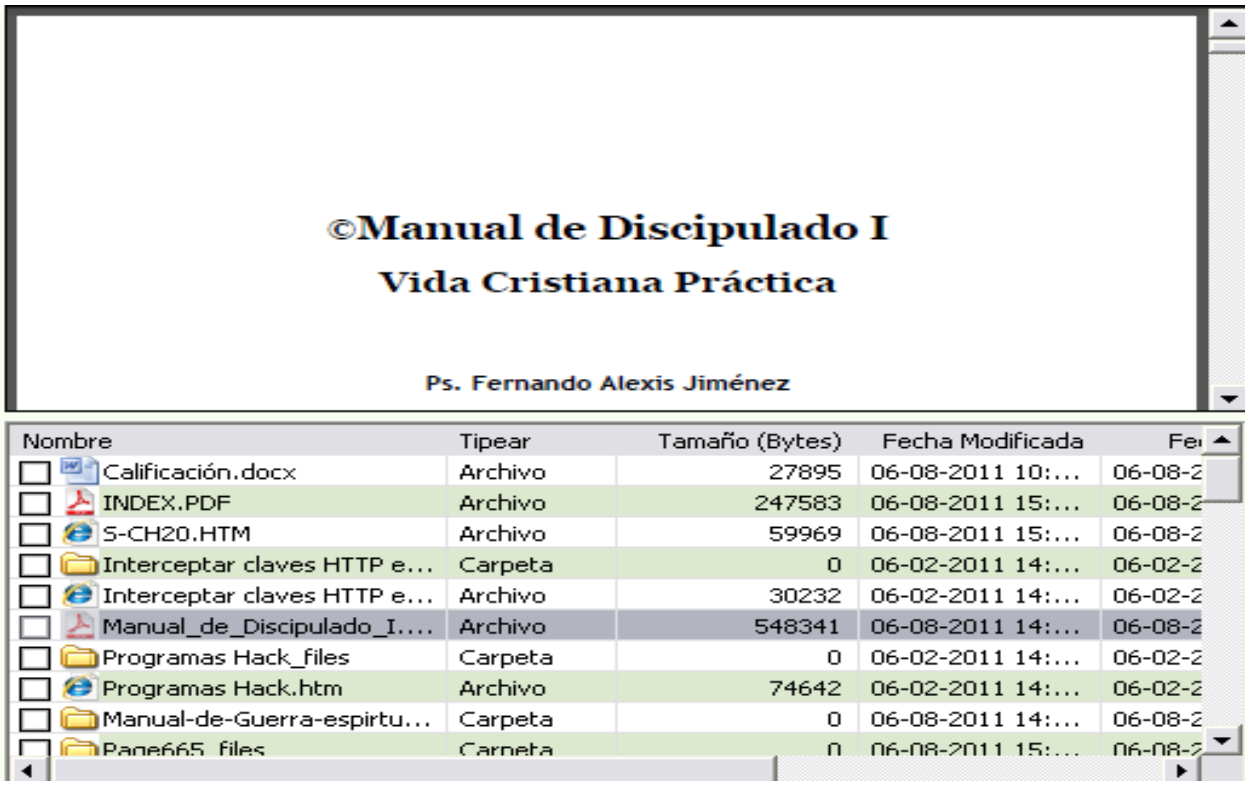


STELLAR PHOENIX WINDOWS DATA RECOVERY
Manual de usuario

1. Menú principal de la herramienta, especificamos el tipo de recuperación, en nuestro caso daremos click en **Recuperación rápida** (Solamente recupera archivos borrados.) pero también podemos seleccionar recuperación de archivos o recuperar datos después del formateo, el procedimientos es el mismo para las tres primeras opciones.

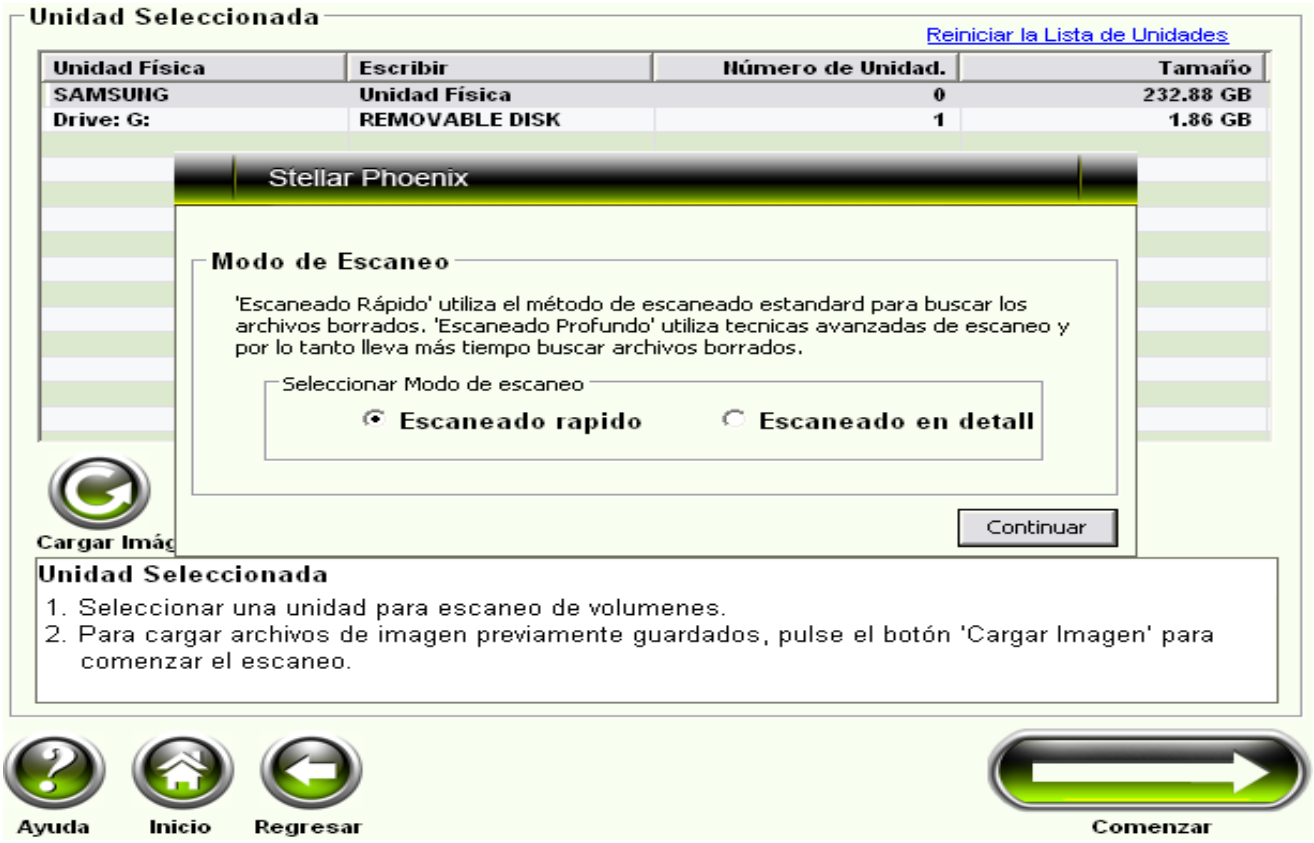
2. Click en el dispositivo que desea analizar a continuación presionamos el botón **Comenzar**
   Nota: puedes analizar todo tipo de discos duros y dispositivos USB.

3. La siguiente pantalla muestra la información recuperada, esta herramienta nos permite visualizar los datos con solo dar **doble click** en determinado documento, también se pueden ver archivos de música, video, entre otros, para guardar el archivo **click izquierdo sobre el archivo** y seleccionamos la opción **Recuperar.**



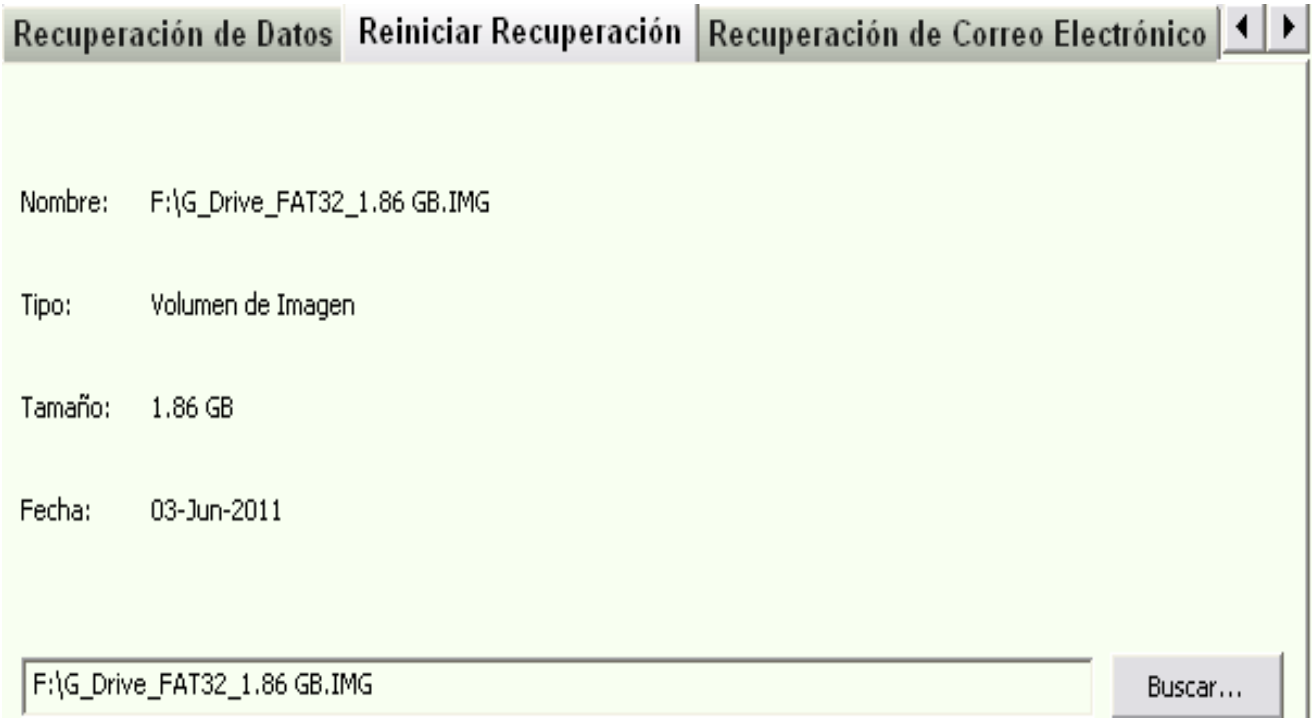
4. La opción buscar volúmenes perdidos escanea el disco duro para volúmenes borrados, cada sector de la unidad es rastreado y posteriormente recuperado.

5. Seleccionamos la unidad a la cual vamos a realizar el escaneo y damos click en **Comenzar,** se mostrara una ventana, con dos opciones de escaneo en nuestro ejemplo seleccionamos **Escaneo rápido y** damos click en **Continuar.**



6. La siguiente pantalla muestra los volúmenes que se están recuperando en el escaneo

7. Esta pantalla muestra información acerca de las diferentes operaciones realizadas con la herramienta.

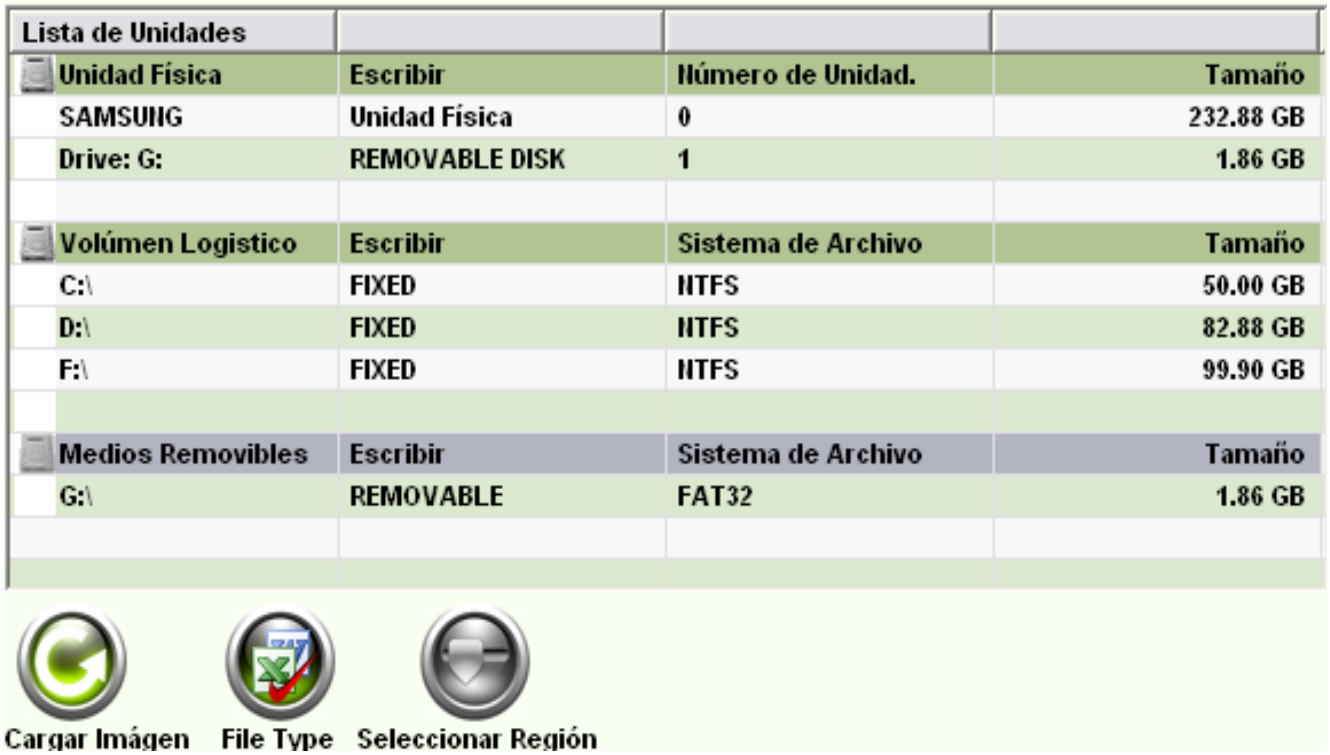


8. La pestaña recuperación de correo electrónico nos muestra dos opciones, una para escanear archivos de datos MS Outlook (PST) y la otra opción escanea archivos de datos Outlook express (DBX) para el caso de correos borrados.

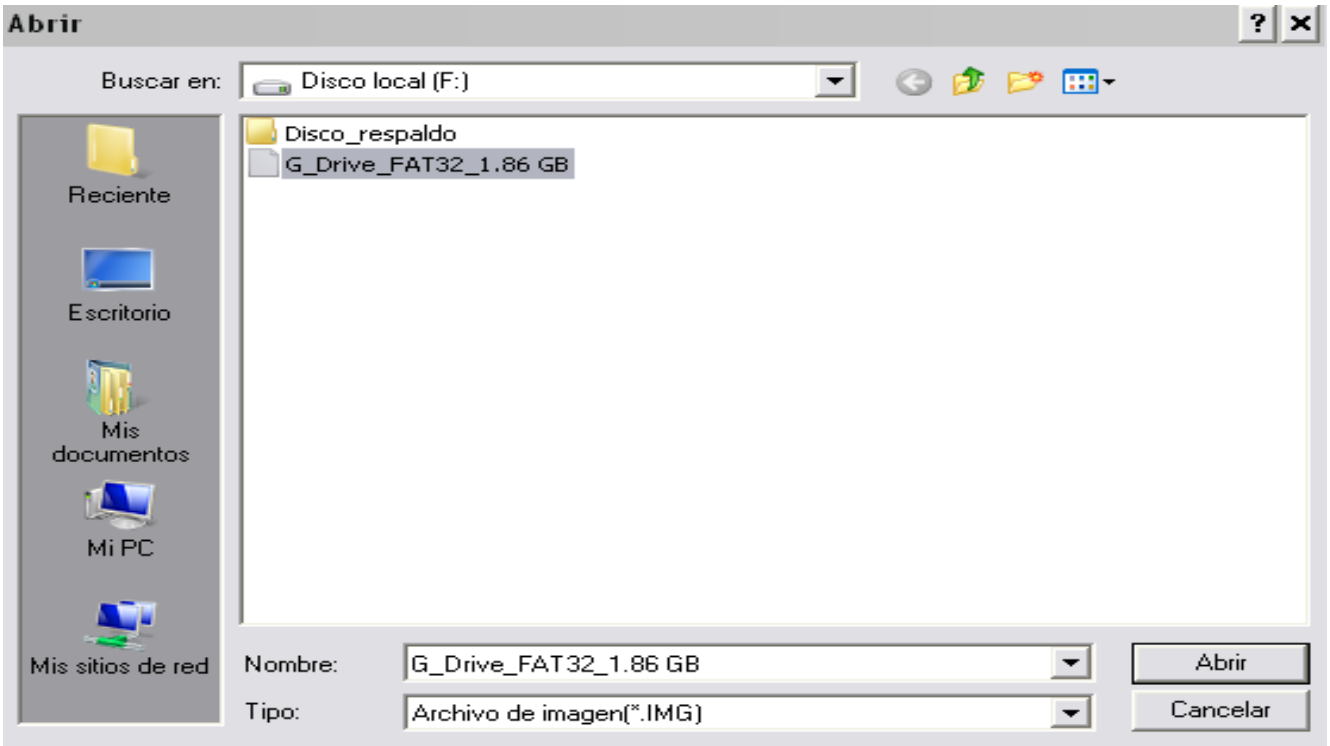
9. A continuación seleccionamos el archivo DBX desde el cual los correos borrados van hacer recuperados, click en botón **Destino** y presionamos **Iniciar el Escaneo** una vez que el archivo de escaneo está completo presionamos "**Guardar "**para guardar los correos.
   Nota el procedimiento para la siguiente opción es el mismo.

10. En la siguiente pestaña de opciones avanzadas damos click en **Recuperación de archivos Raw**
    Nota la opción **estado de la unidad** detecta fallos del disco duro.

11. Damos click en el botón **Cargar imagen**



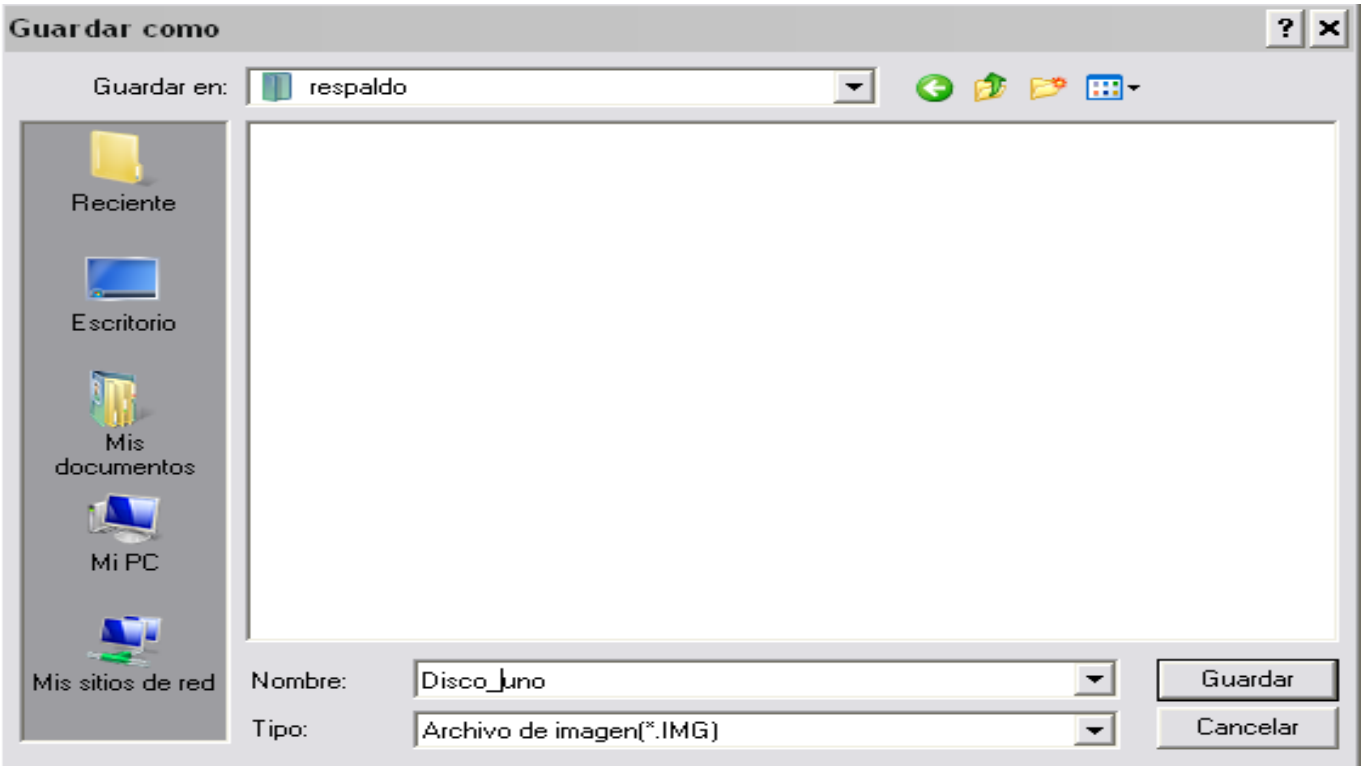
12. Seleccionamos el origen del archivo como se muestra en la siguiente pantalla, click en **Abrir** y la imagen automáticamente es cargada.

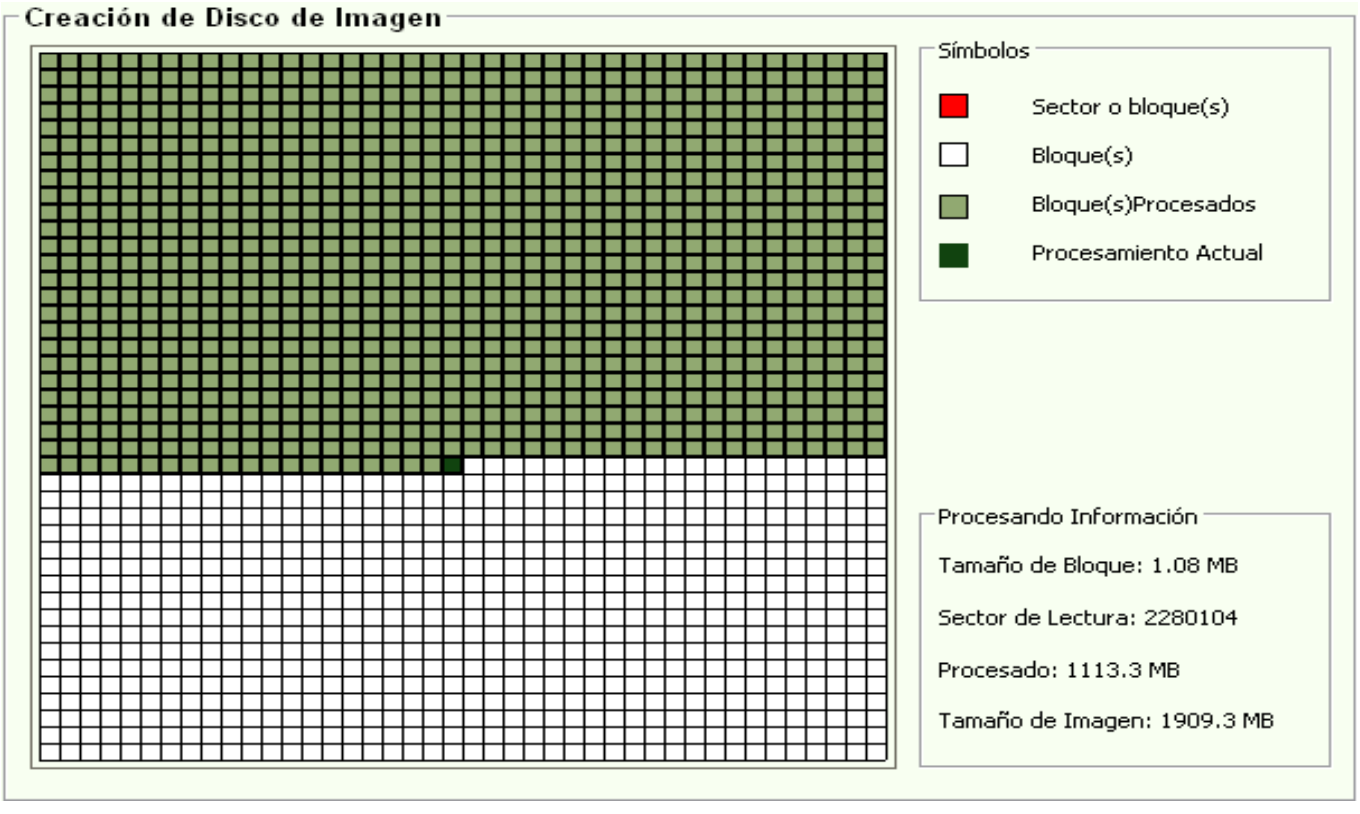


13. La opción **Crear imagen** nos permite crear imágenes de discos duros y dispositivos USB

14. Seleccionamos el dispositivo del cual queremos realizar una copia, en nuestro ejemplo seleccionamos **G:** y presionamos el botón **Continuar**

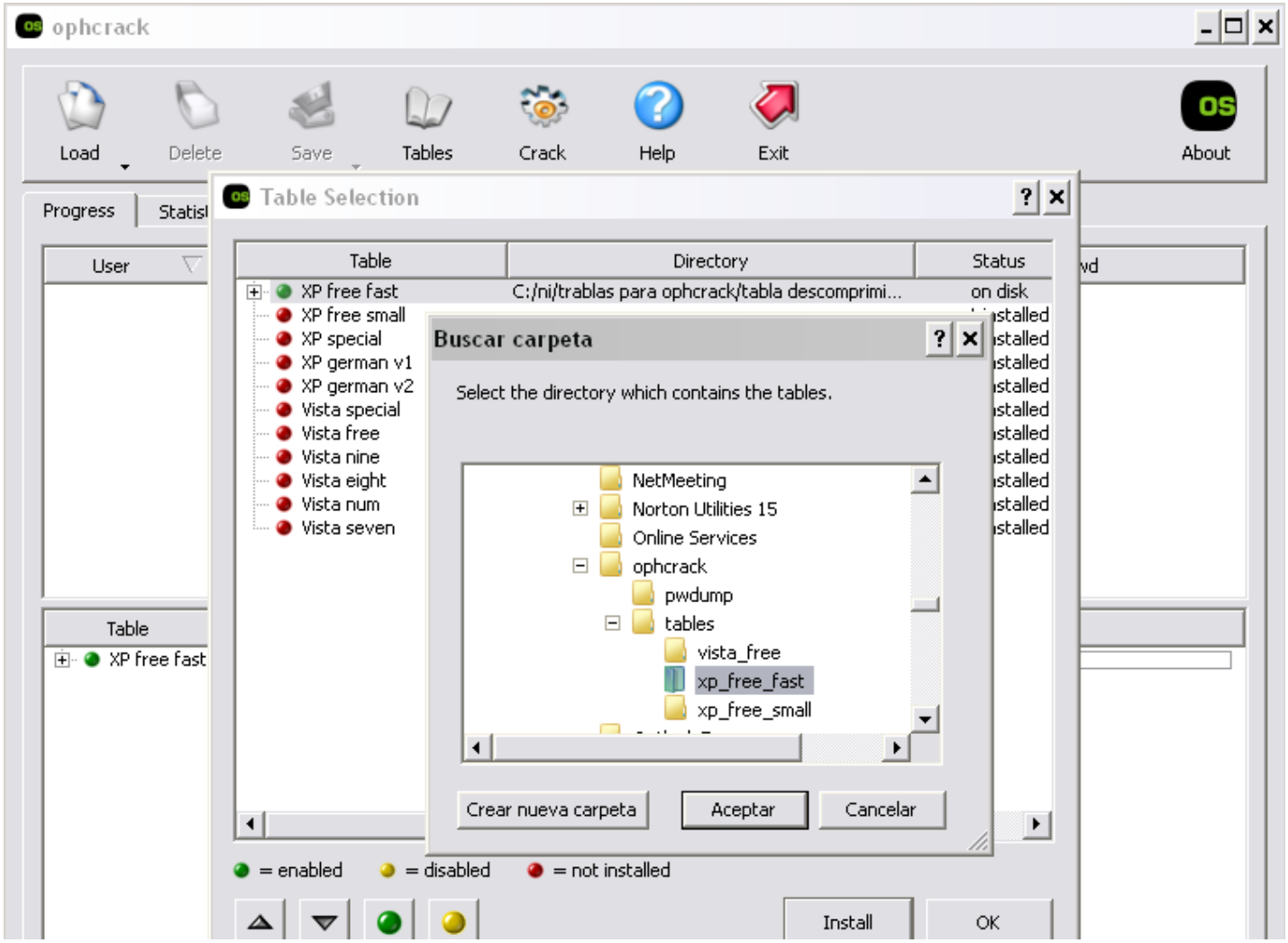
16. En las pantallas siguientes se especifica el nombre del respaldo y la ruta de destino, a continuación se muestra el proceso de creación de la imagen.



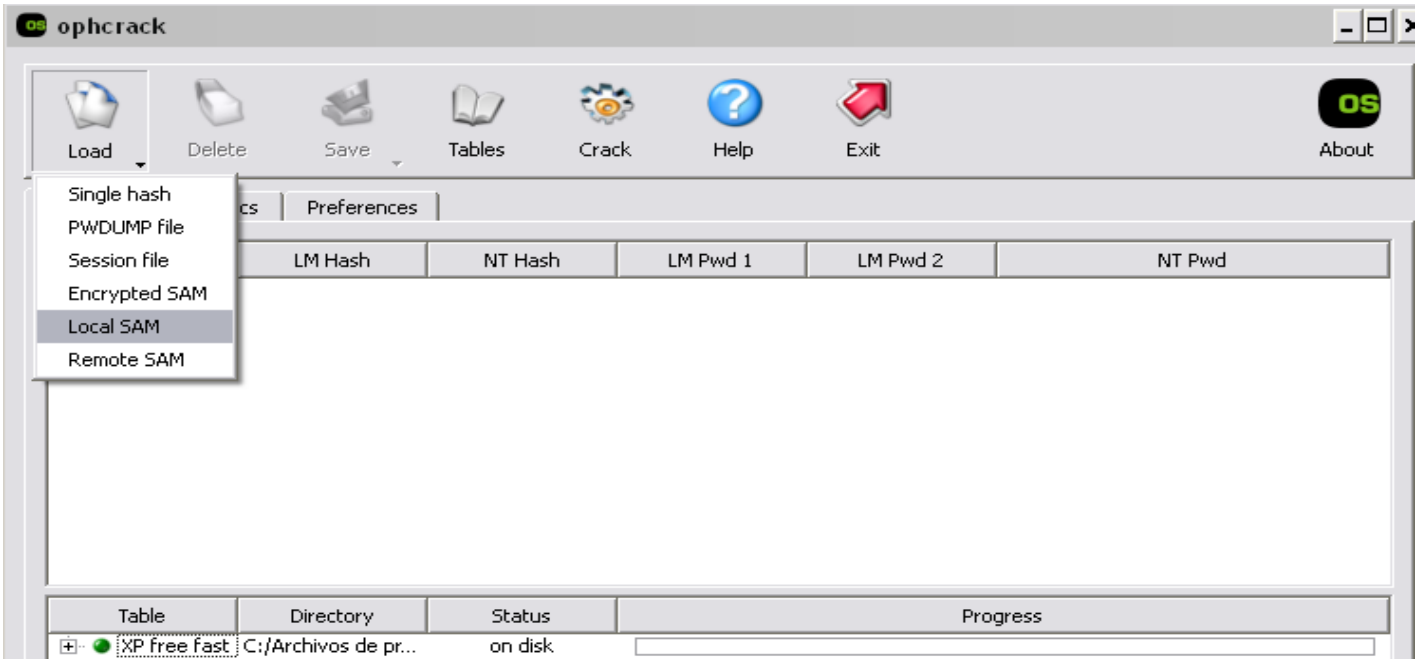


Manual de usuario de la herramienta forense OPHCRACK

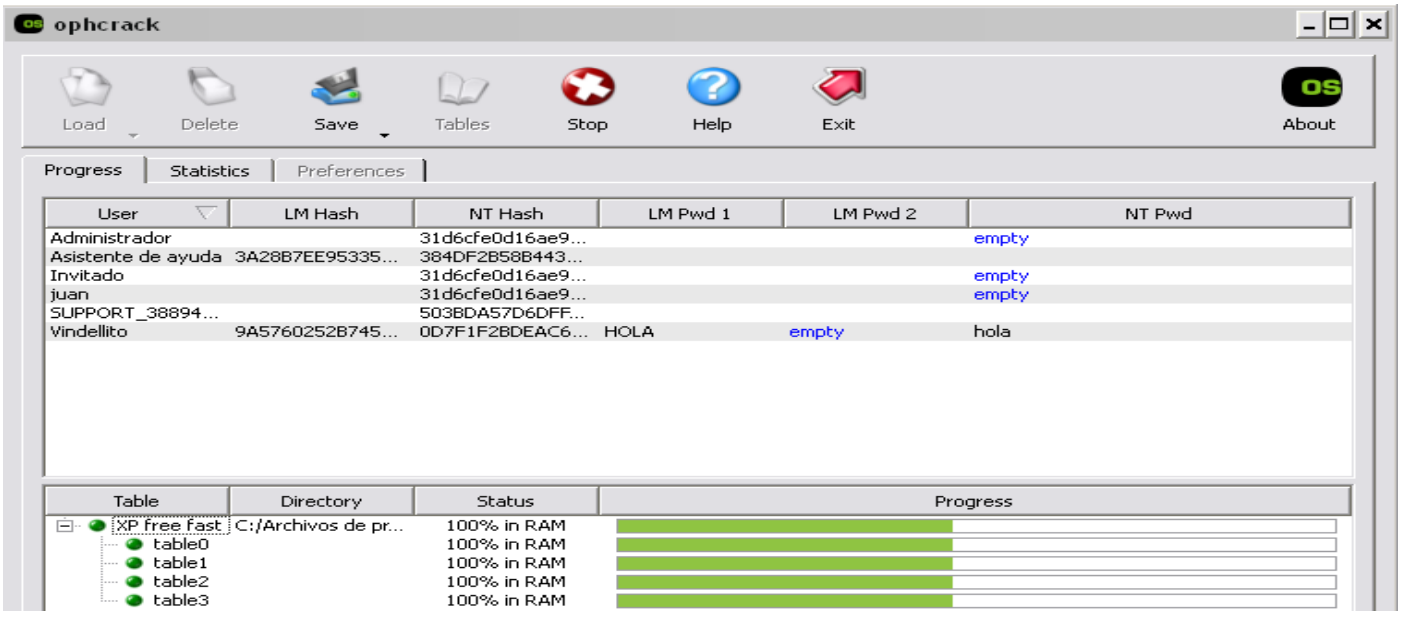
1. Pantalla principal de la herramienta OPHCRACK, hacemos click en la pestaña **Table**, en la ventana siguiente seleccionamos la tabla **XP free fast** (**NOTA** esto es para Windows xp, para vista seria **Vista free**) y presionamos el botón Install, nos aparece una pequeña ventana que nos muestra la carpeta donde se encuentran ubicadas las tablas seleccionamos **tables→xp free fast→Aceptar→Ok**



2. Seleccionamos la pestaña **Load→local Sam**

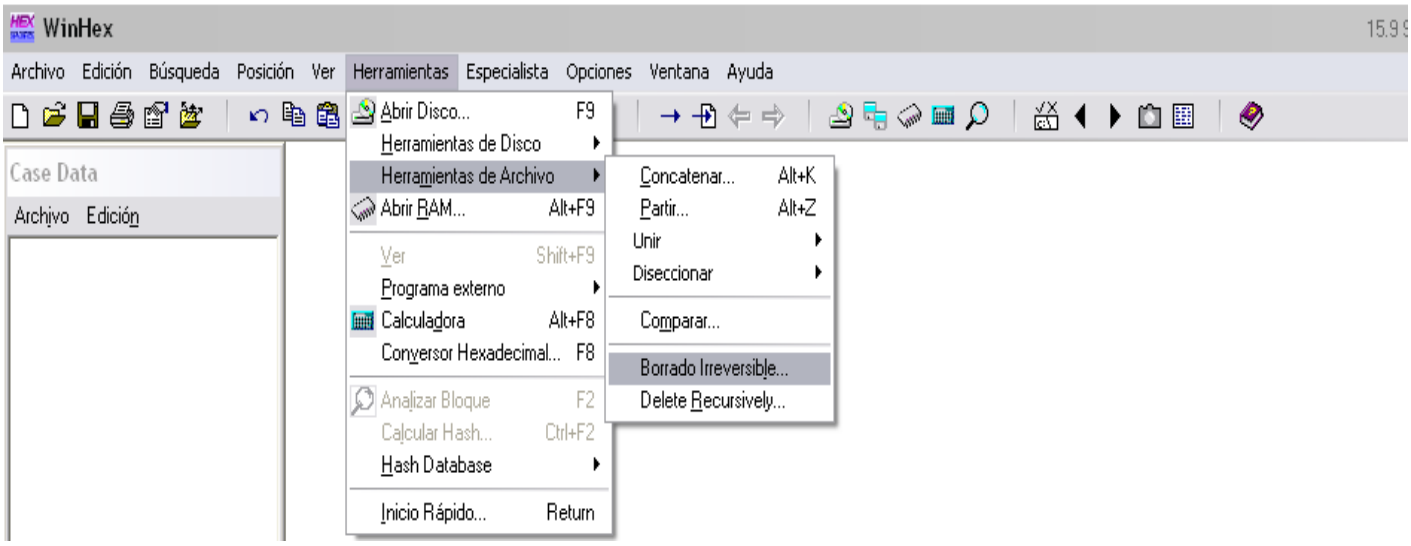


3. La siguiente pantalla muestra los usuarios pertenecientes a la PC, click en la opción **Crack**, para comenzar el análisis y presionar **Exit** para salir del programa.

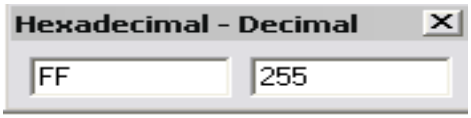


Manual de usuario de la herramienta forense WinHEX

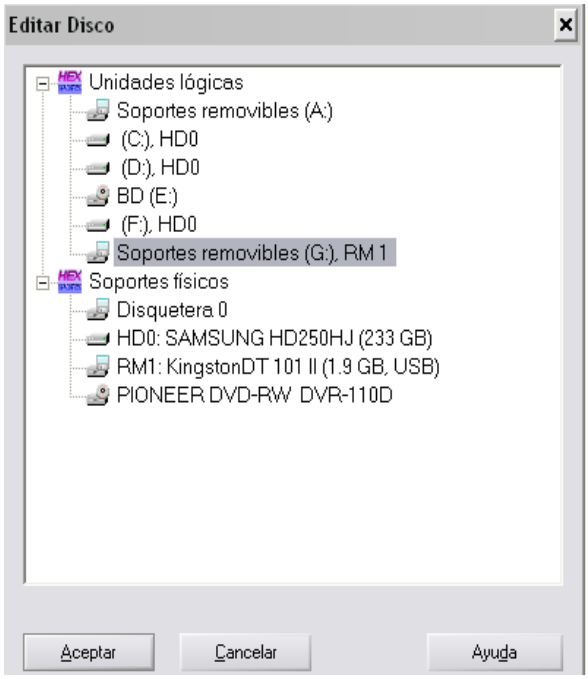
1. Pantalla inicial de WinHex, para borrar archivos seleccionamos **Herramientas→ Herramientas de archivos→Borrado irreversible→Entrar** se abrirá una ventana en la cual podes elegir el archivo que deseas borrar.

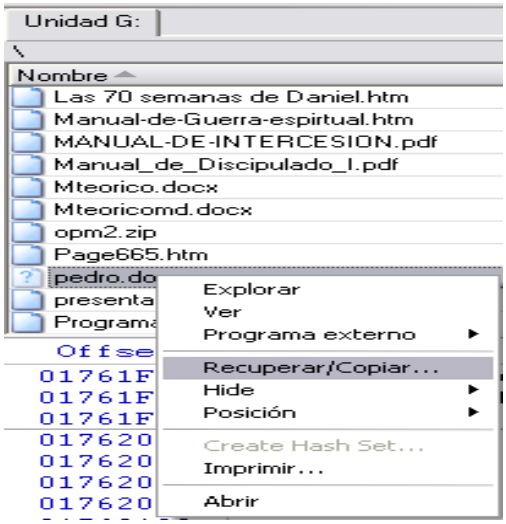


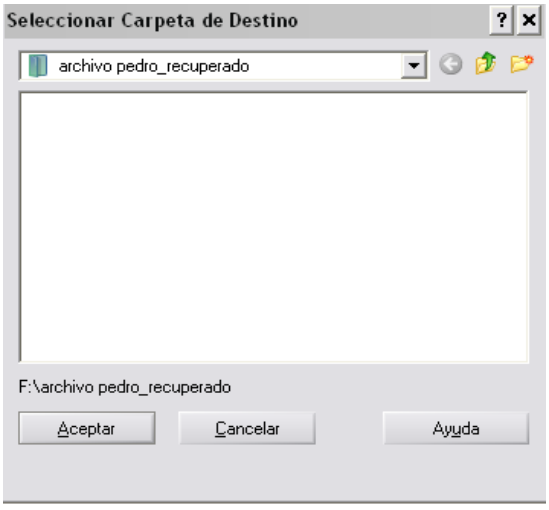
2. También podes hacer conversiones de decimal a hexadecimal y viceversa, click en la pestaña **Herramientas→Conversor Hexadecimal.**



3. Esta pantalla de WinHex muestra la recuperación de archivos borrados, **Herramientas→Abrir Disco→Seleccionar dispositivos→Aceptar** WinHEX tiene un visor que te permite visualizar los archivos borrados, les asigna un signo de interrogación esto significa que el archivo puede ser recuperado, click izquierdo sobre el archivo y seleccionas la opción **Recuperar→Aceptar**

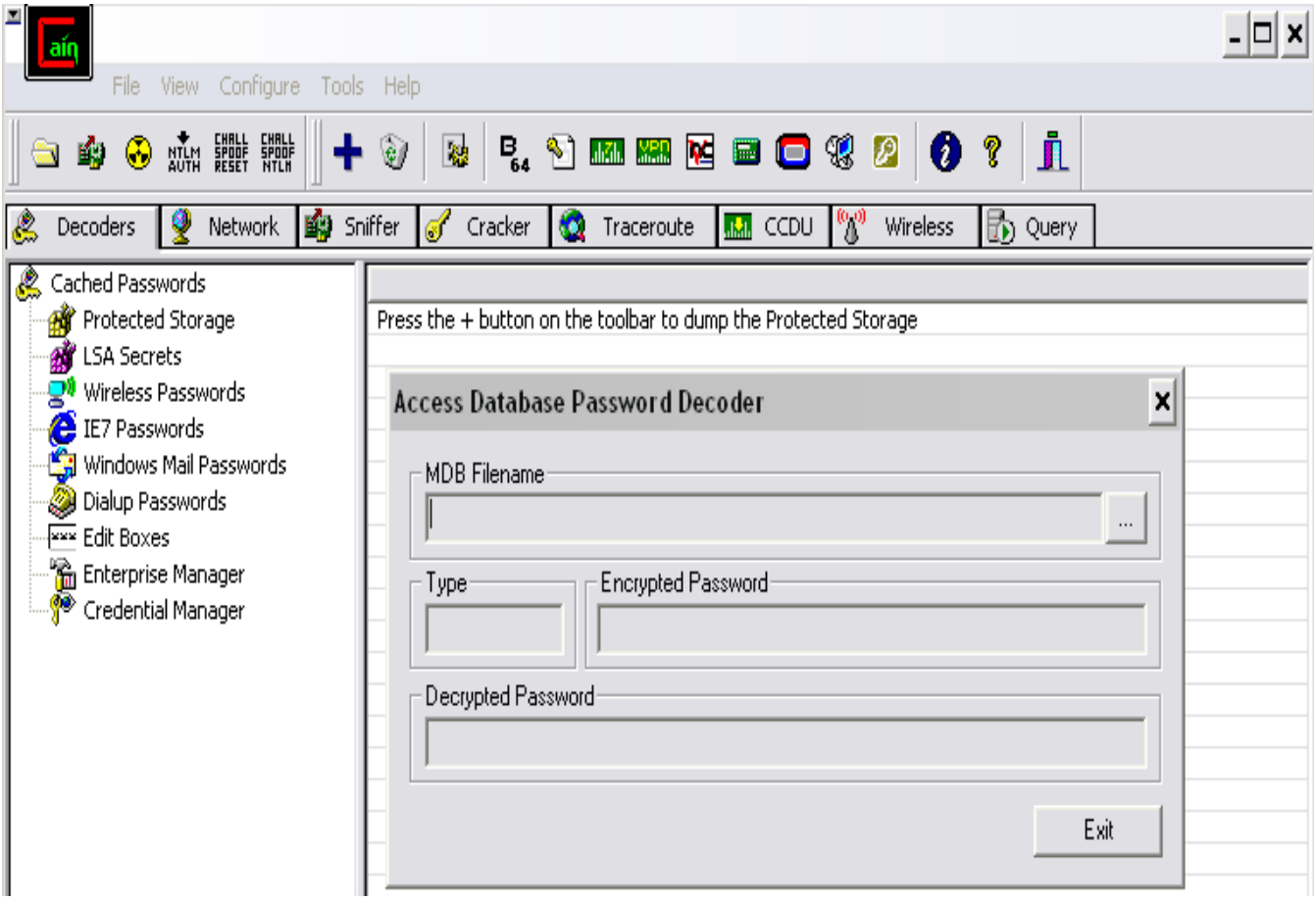




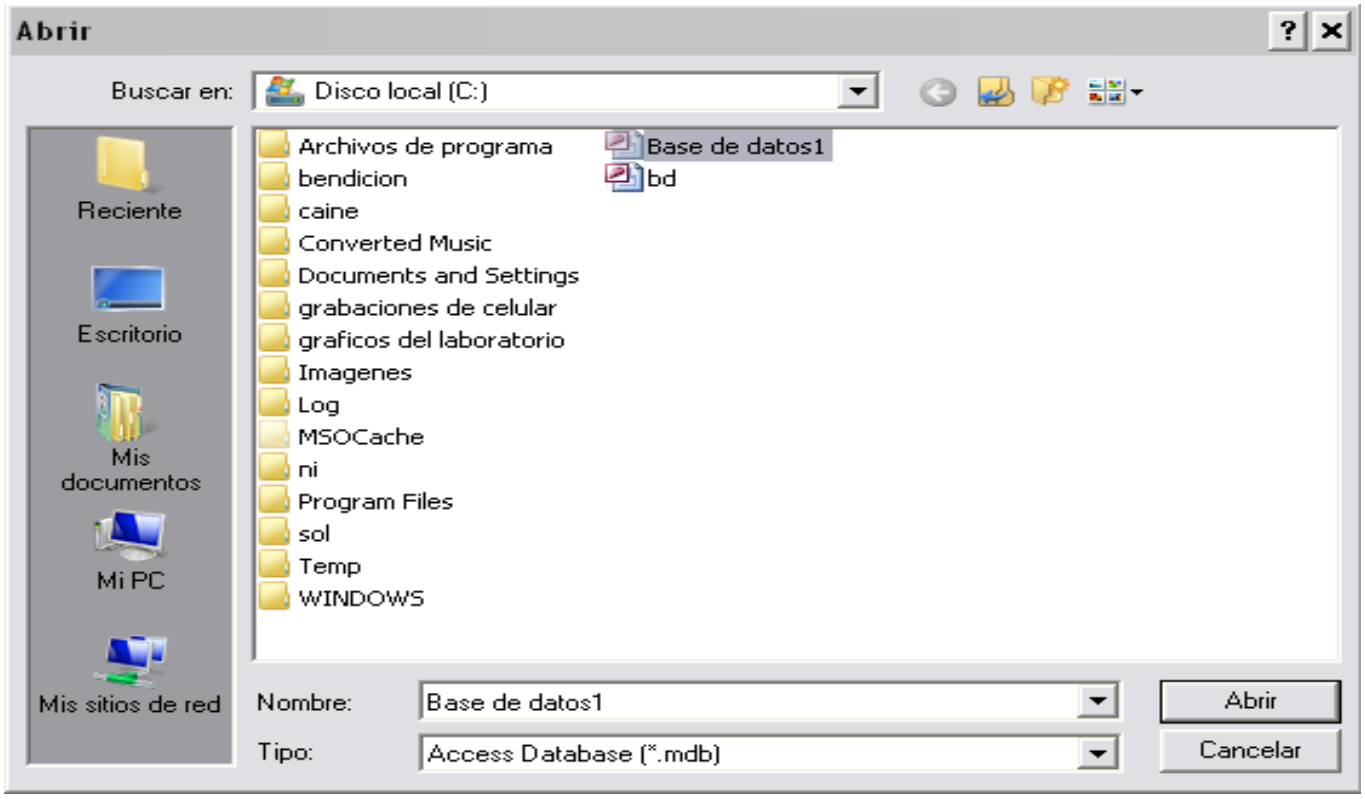


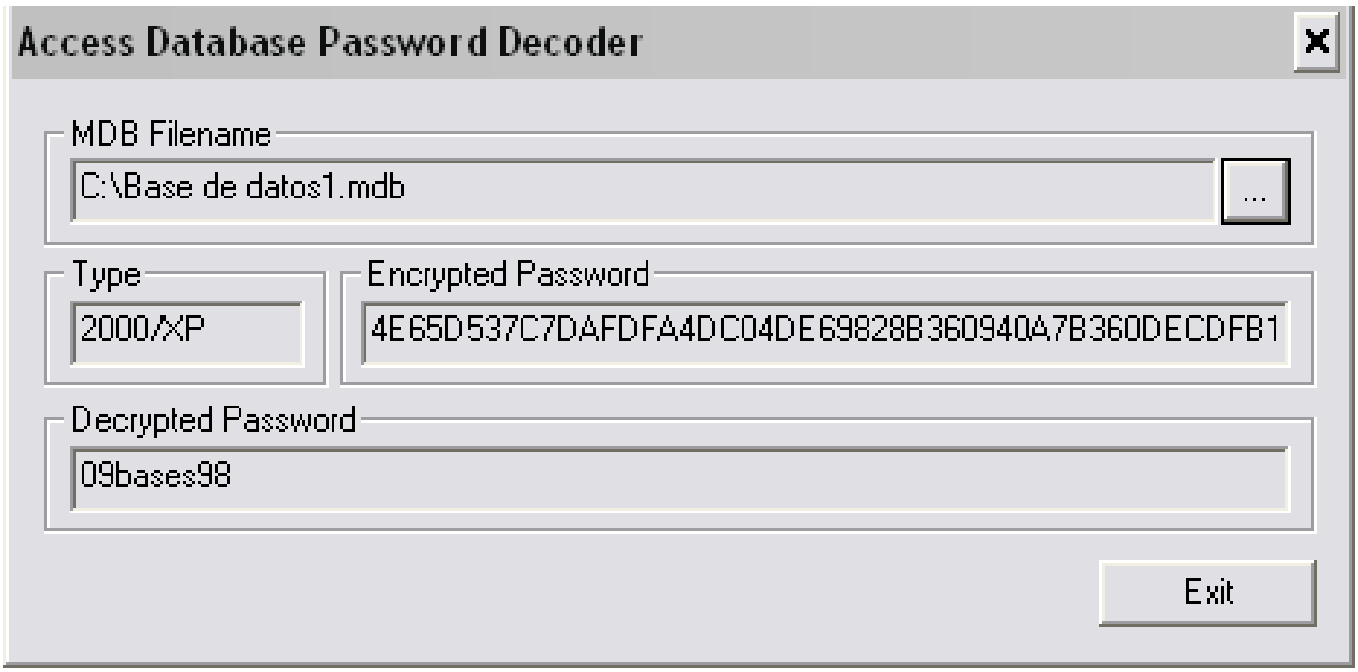
Manual de usuario de la herramienta CAIN & ABEL

1 En el menú principal de la herramienta Cain & Abel seleccionamos la pestaña **Access Database Password Decoder.**



2. A continuación Seleccionamos la **base de datos→Abrir. Nota** automáticamente la contraseña de la base de datos es descifrada.

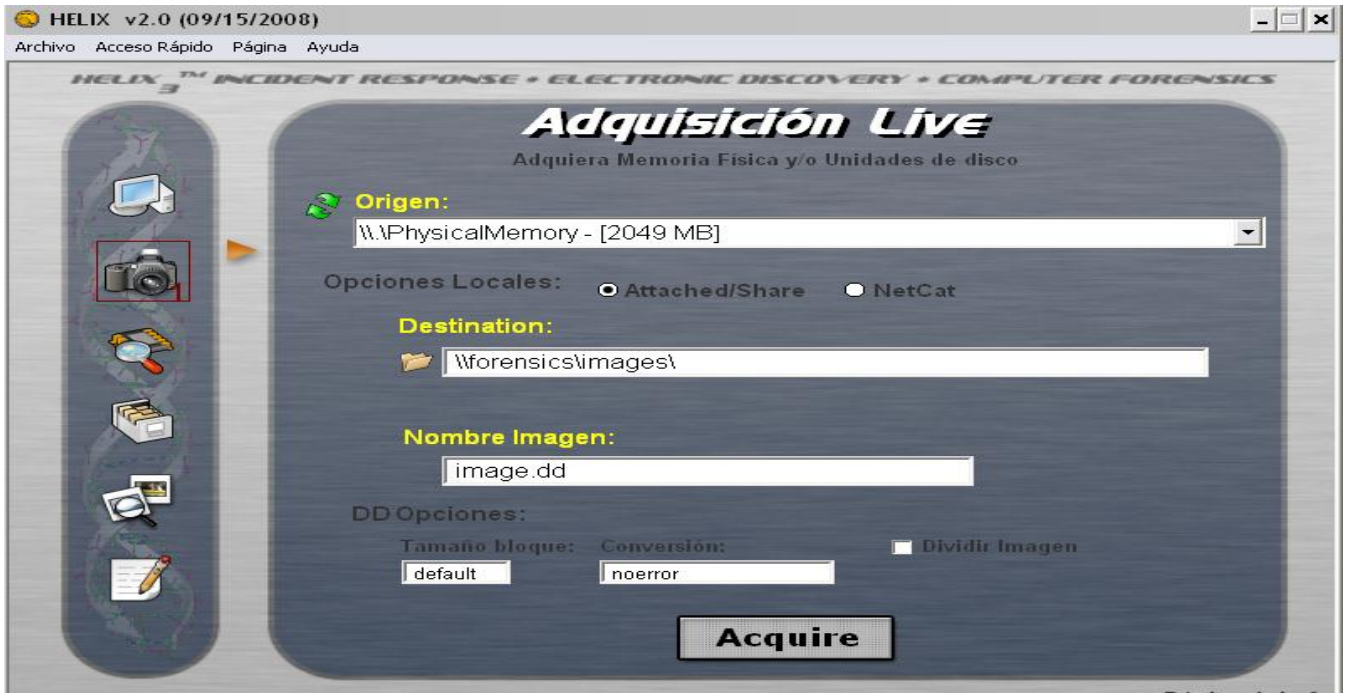


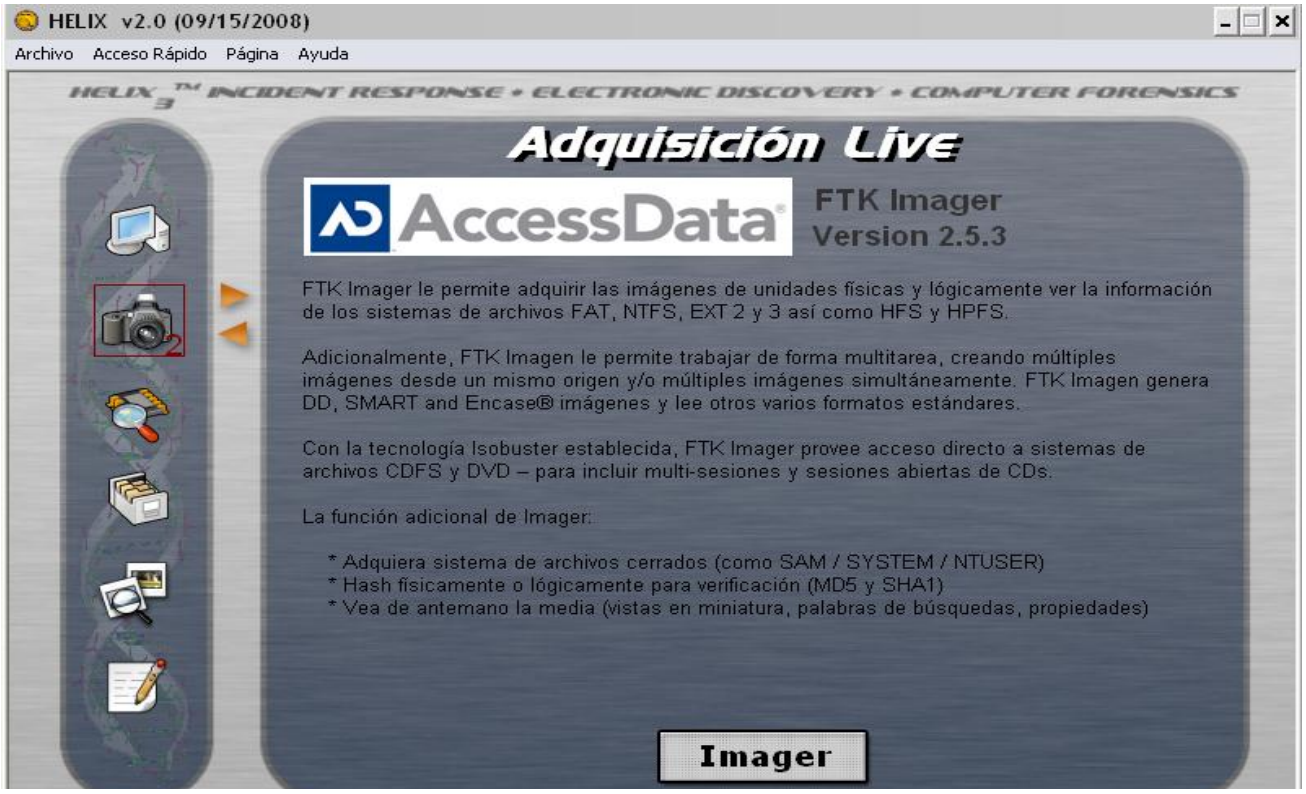


Manual de las herramienta forenses HELIX 3 Y ACCESS DATA FTK IMAGER

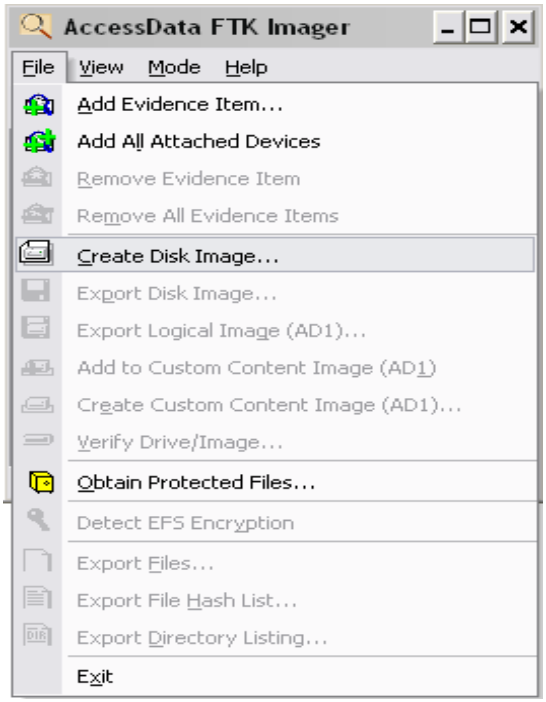
1. Pantalla inicial en la cual se puede seleccionar los diferentes idiomas en el cual desees correr la aplicación, click en la ventana **Escoja su idioma→Aceptar**

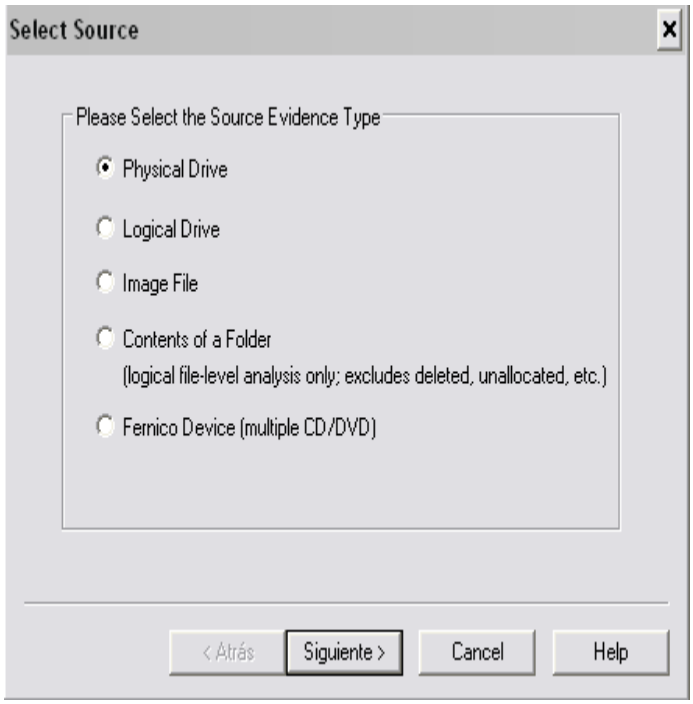
2. Estas pantallas muestran como se crea una imagen de Discos duros o USB con AccessData FTK Imager seleccionamos la opción **Acquisition→Go to FTK Imager → Imager**

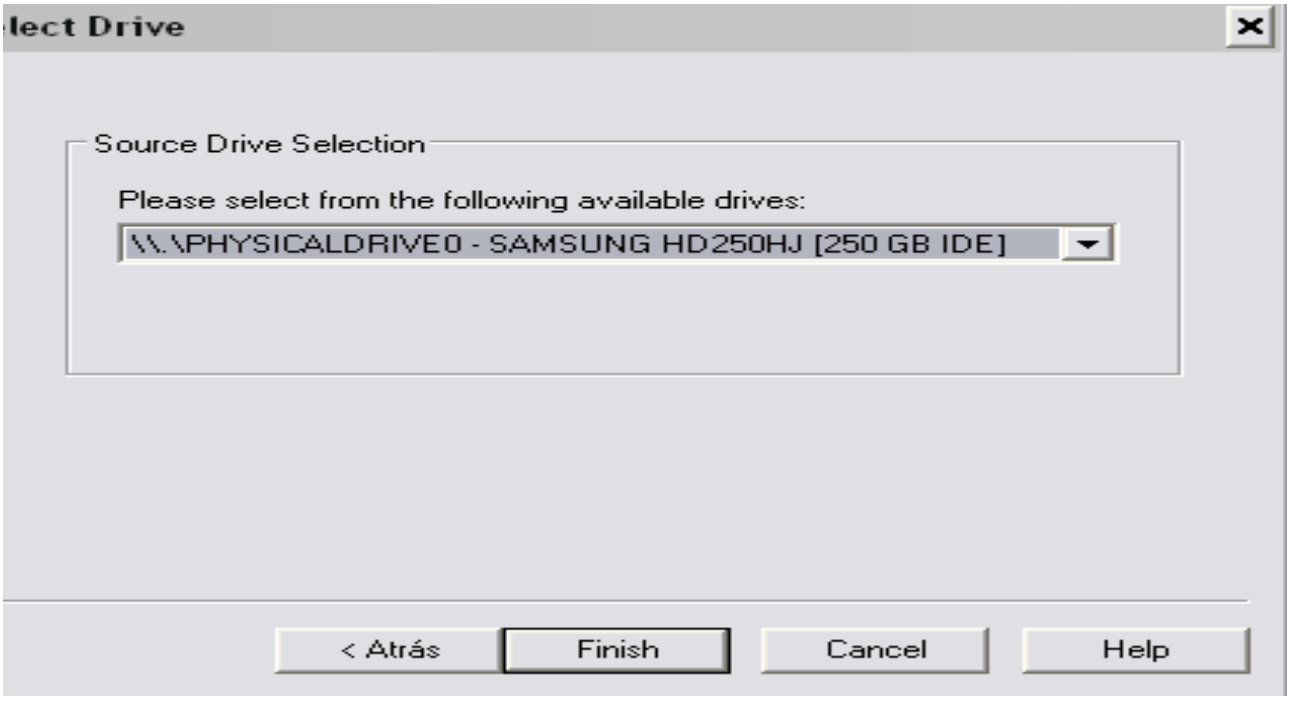

HELIX v2.0 (09/15/2008)
Archivo Acceso Rápido Página Ayuda
HELIX 3™ INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS
Adquisición Live
Adquiera Memoria Física y/o Unidades de disco
Origen:
\\.\PhysicalMemory - [2049 MB]
Opciones Locales:
Attached/Share
NetCat
Destination:
\\forensics\images\
Nombre Imagen:
image.dd
DD Opciones:
Tamaño bloque:
Conversión:
Dividir Imagen
default
noerror
Acquire

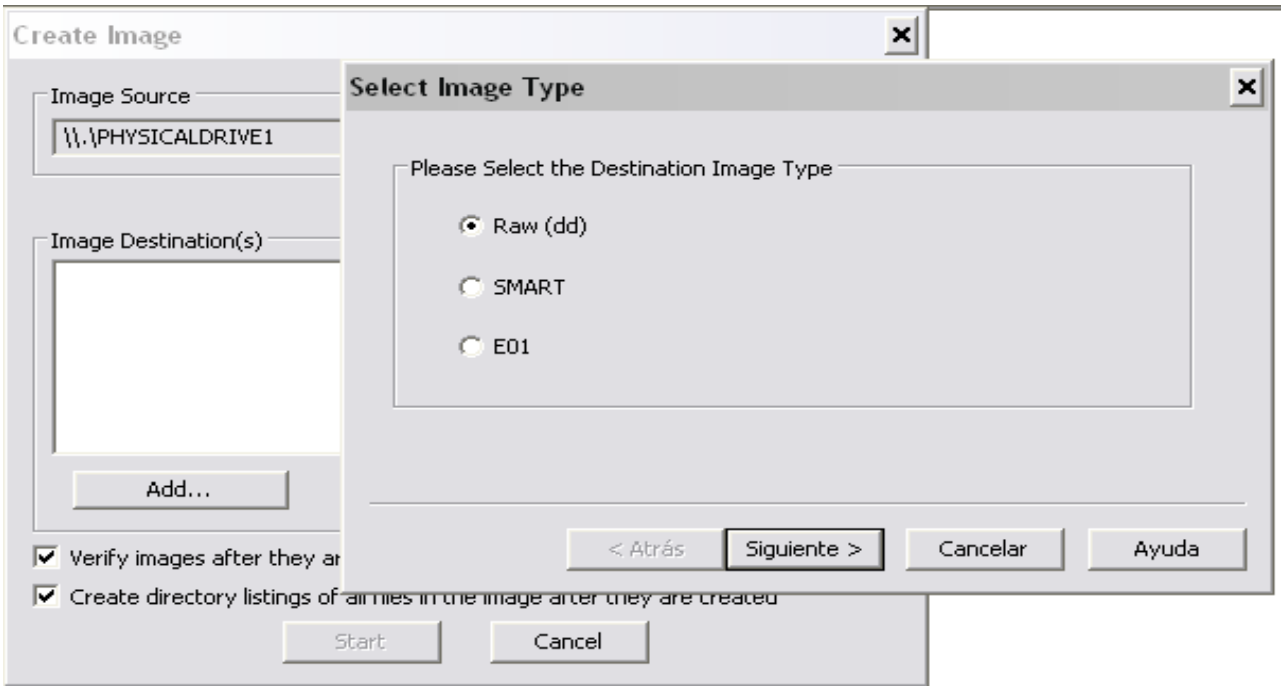

HELIX v2.0 (09/15/2008)
Archivo Acceso Rápido Página Ayuda
HELIX 3™ INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS
Adquisición Live
AccessData
FTK Imager
Version 2.5.3
FTK Imager le permite adquirir las imágenes de unidades físicas y lógicamente ver la información de los sistemas de archivos FAT, NTFS, EXT 2 y 3 así como HFS y HPFS.
Adicionalmente, FTK Imagen le permite trabajar de forma multitarea, creando múltiples imágenes desde un mismo origen y/o múltiples imágenes simultáneamente. FTK Imagen genera DD, SMART and Encase® imágenes y lee otros varios formatos estándares.
Con la tecnología Isobuster establecida, FTK Imager provee acceso directo a sistemas de archivos CDFS y DVD – para incluir multi-sesiones y sesiones abiertas de CDs.
La función adicional de Imager:
* Adquiera sistema de archivos cerrados (como SAM / SYSTEM / NTUSER)
* Hash físicamente o lógicamente para verificación (MD5 y SHA1)
* Vea de antemano la media (vistas en miniatura, palabras de búsquedas, propiedades)
Imager

3. Click **→File→Create Disk Image→Physical Drive→Siguiente** →seleccionas el dispositivo del cual vas a crear la imagen **→Finish→Add→Raw(dd)→Siguiente**

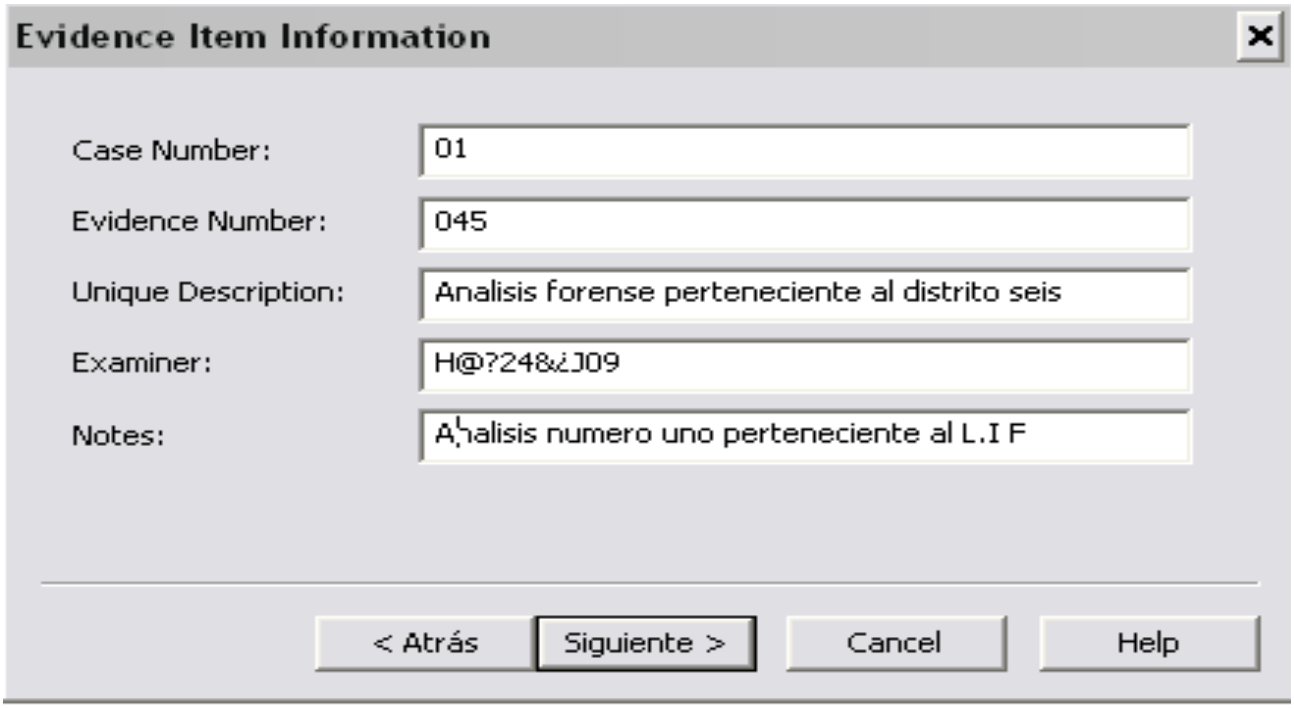




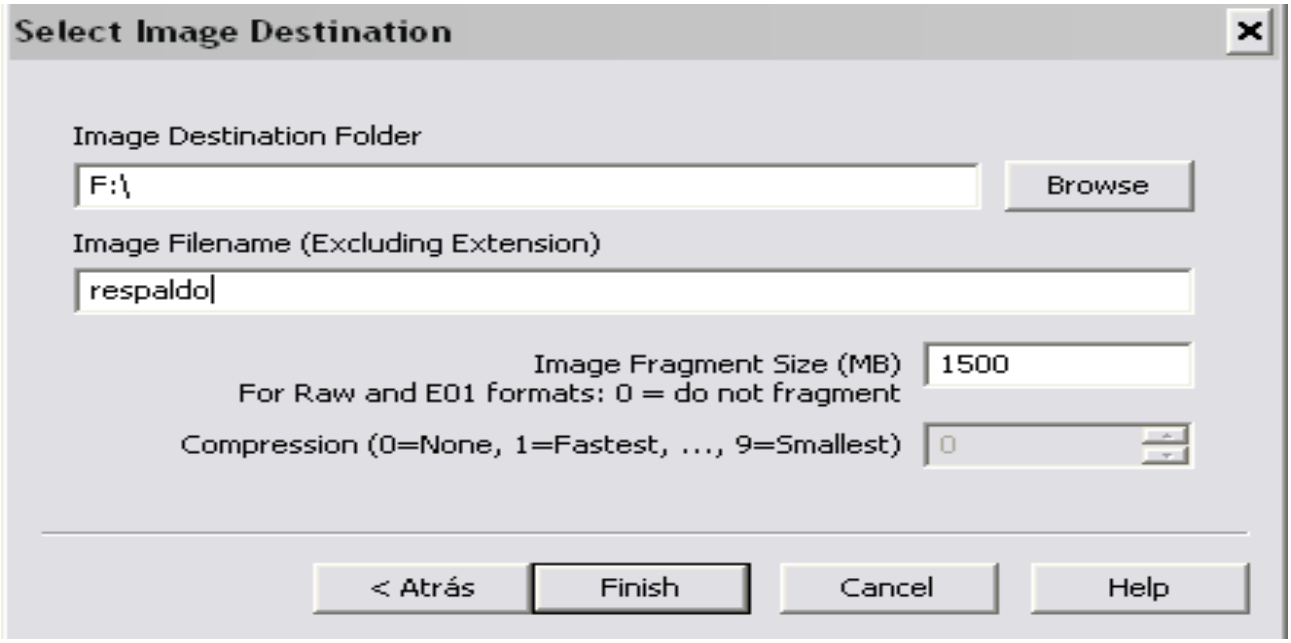


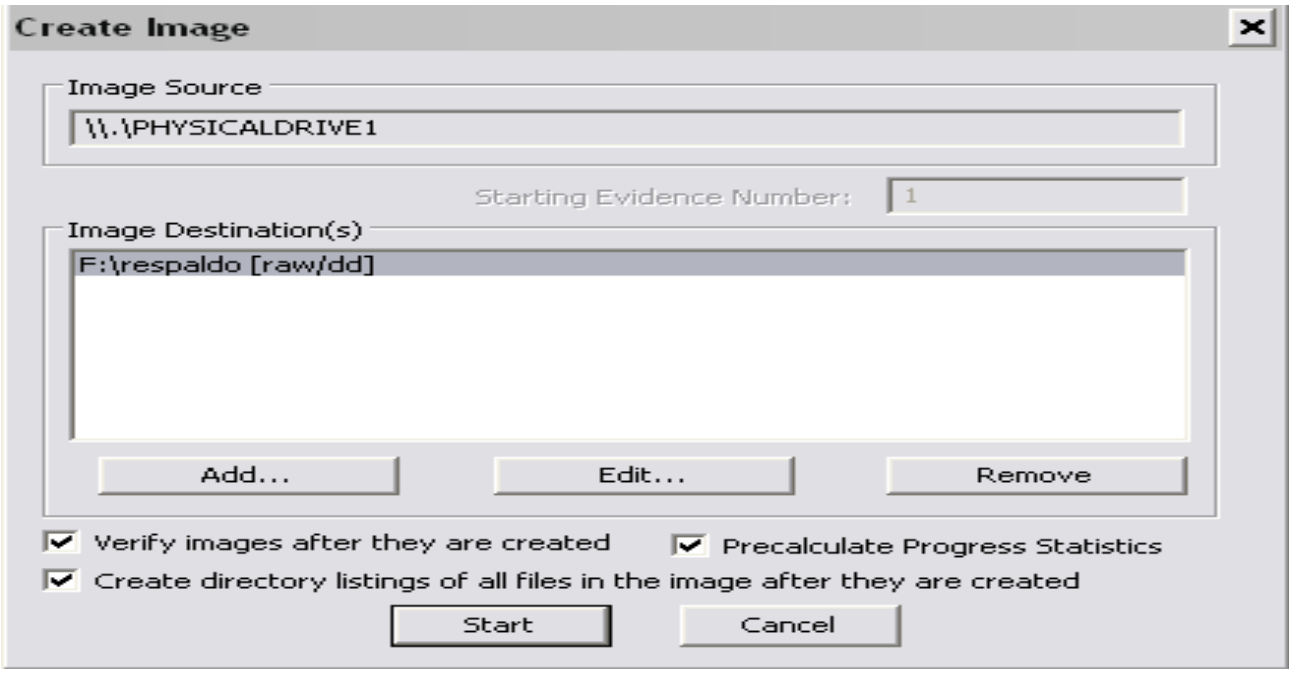


4. En la sección **Evidence Item Information** vas llenar las siguientes ventanas como se muestra en la imagen y presionas el botón→**Siguiente**→**Browse**(seleccionas destino) y escribes el nombre de la imagen→**Iniciar**

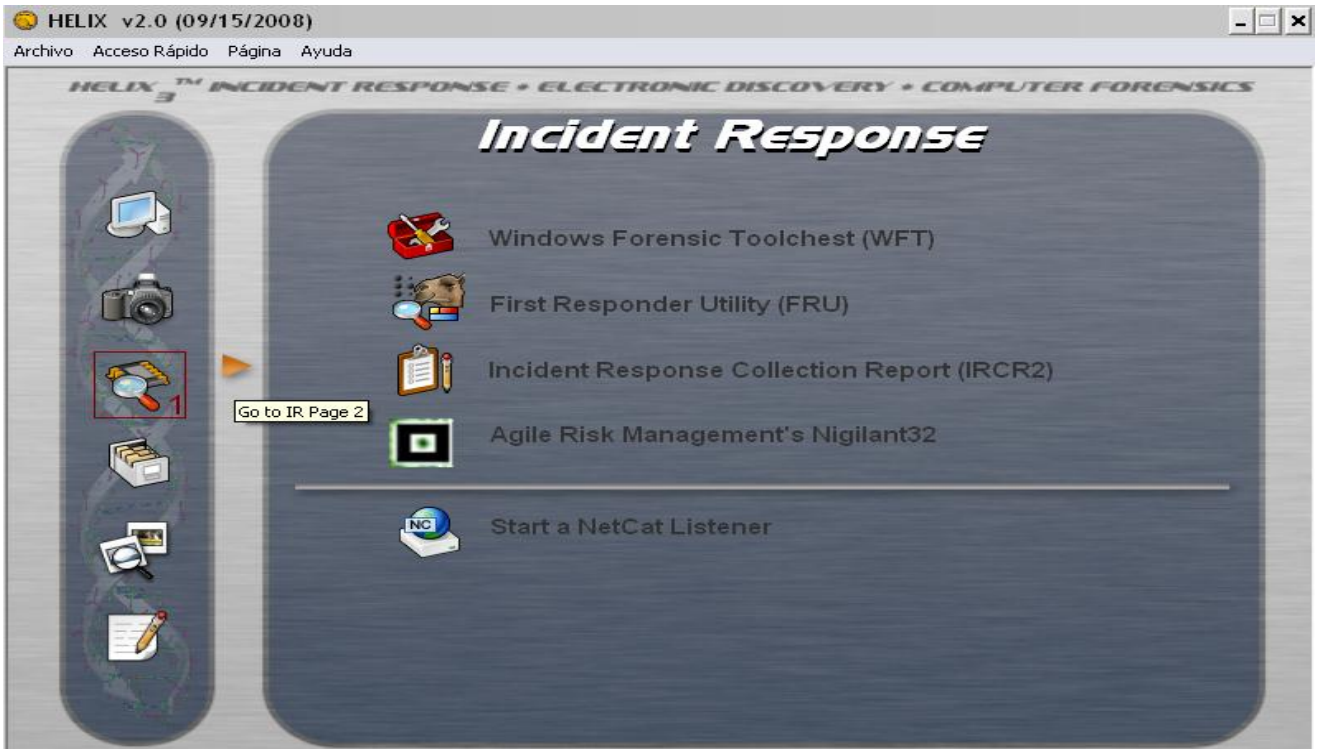


5. En la pantalla siguiente seleccionas el destino de la imagen y el nombre a continuación presionamos **Finish**→en la siguiente pantalla se presiona **Start.**

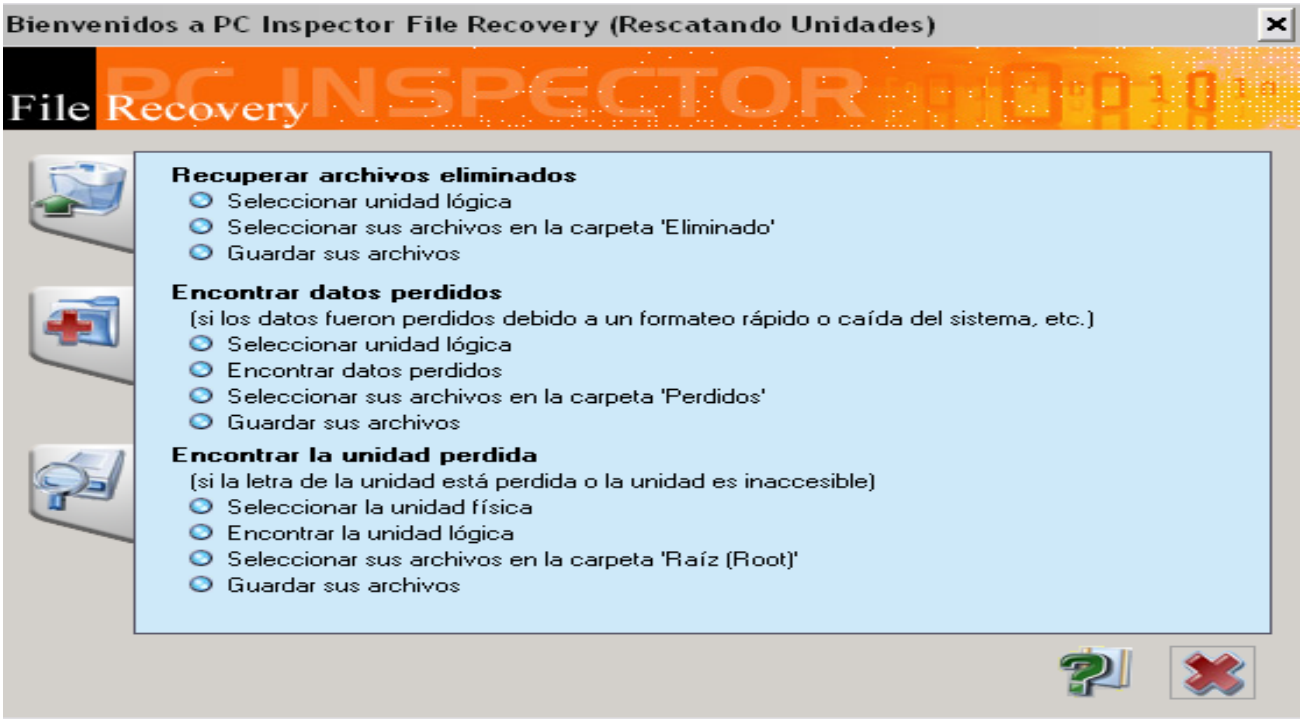


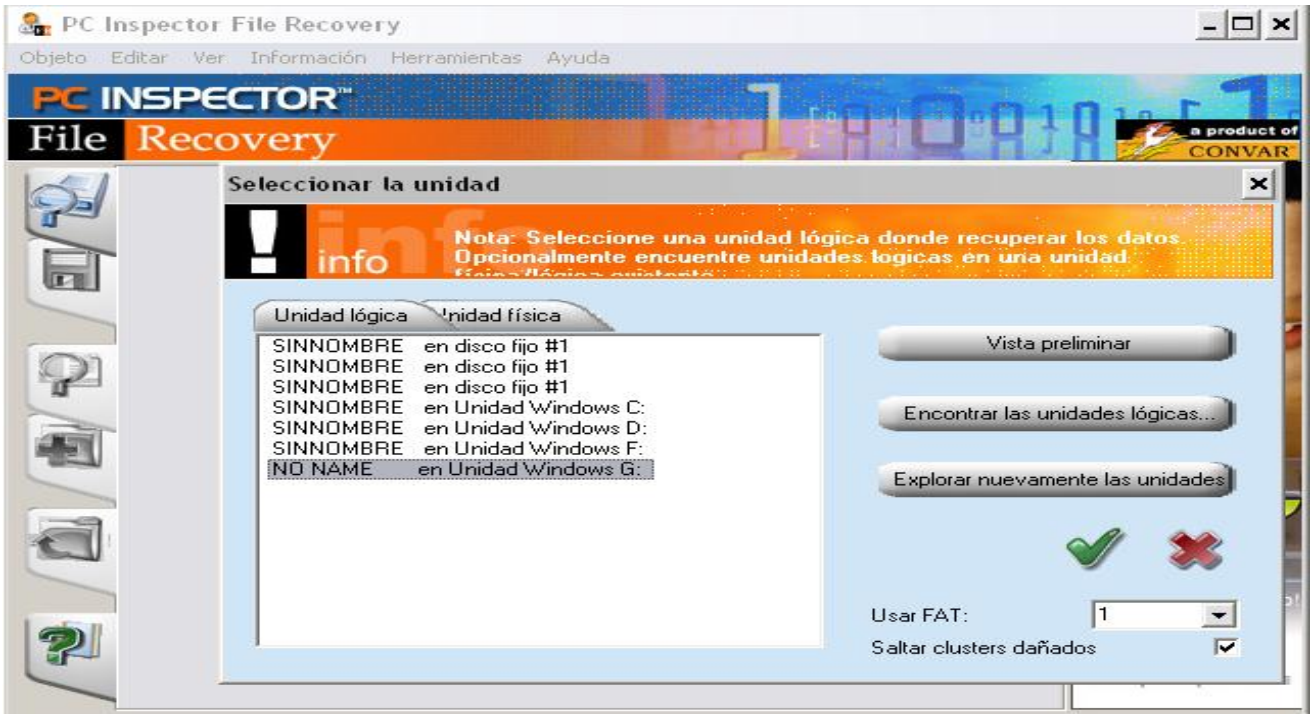


1. Nos ubicamos en la opción **Respuesta a incidentes** (Incident Response)→ **Go to IT Page 2→File Recovery→**aparece una ventana seleccionas **→Si**

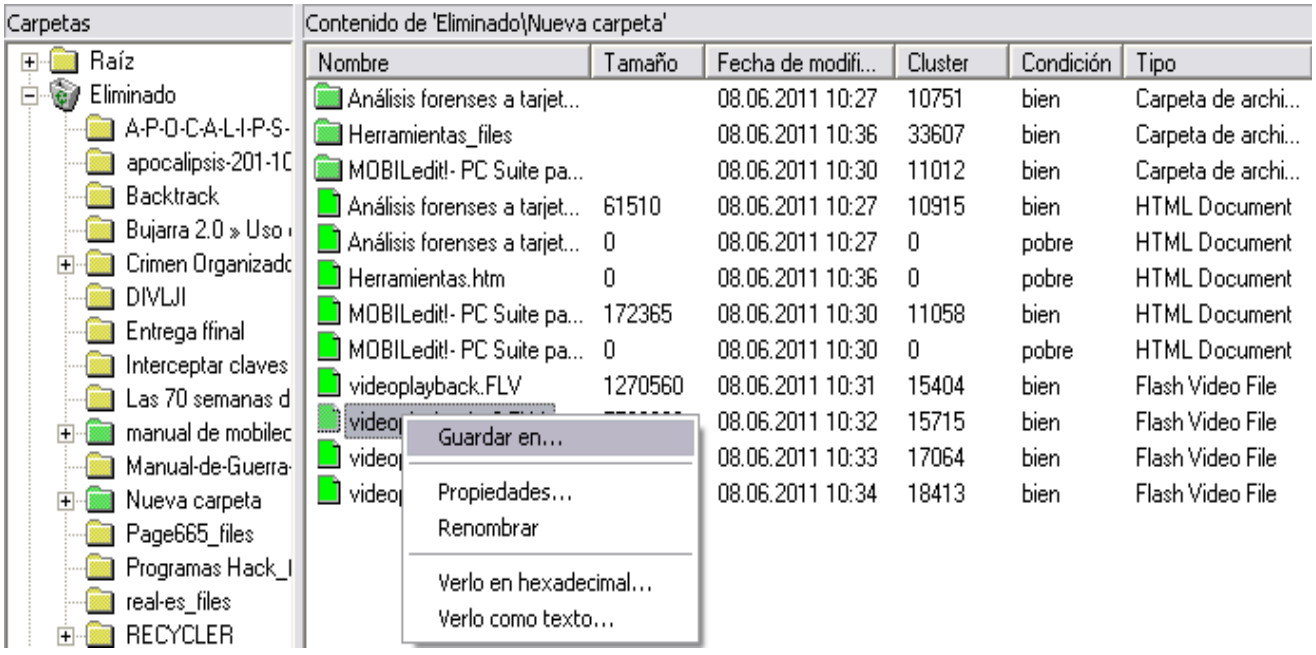


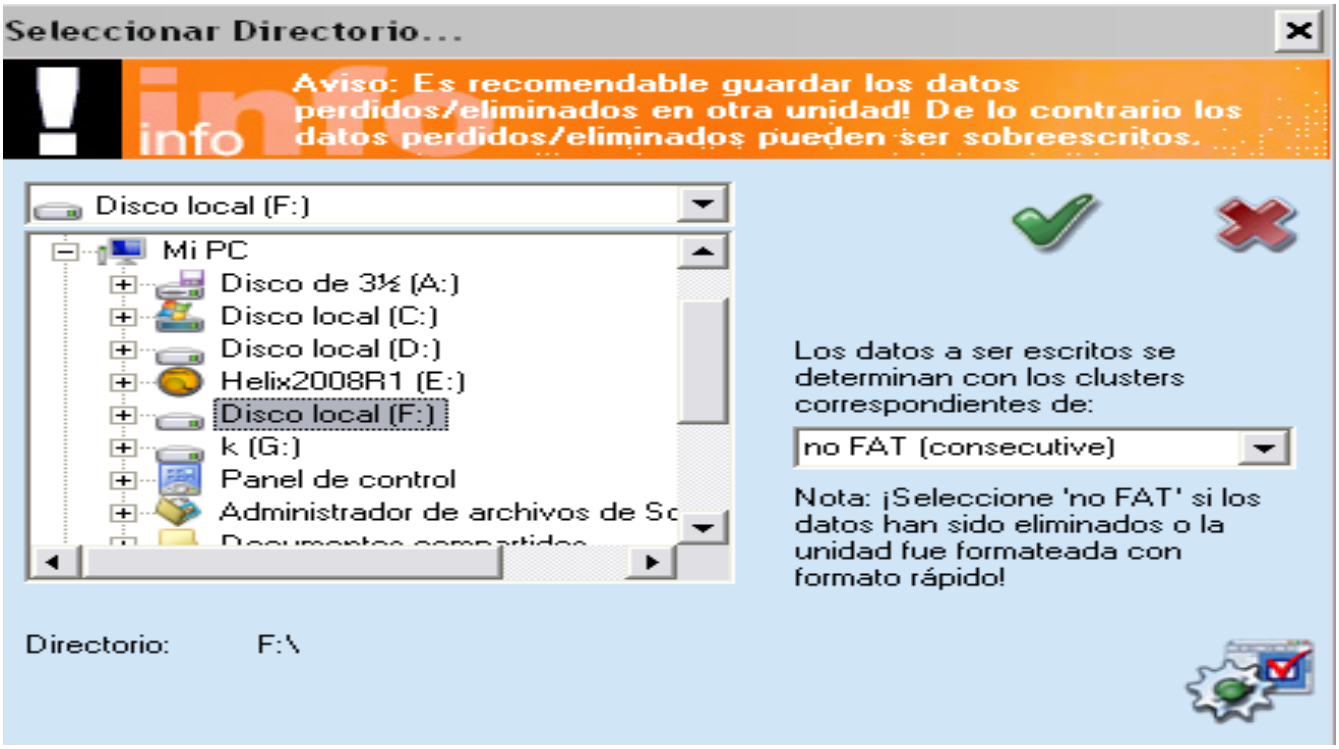
2. Menú principal de File Recovery ahora vamos a recuperar archivos perdidos, en la bandejas de idiomas seleccionamos **Español→Entrar→**aparecerá una ventana que tiene cierta información, presiona **Cerrar→** y selecciona la opción **Abrir la Unidad** en unidades lógicas seleccionamos la unidad lógica que desea analizar, **doble click sobre la unidad**.





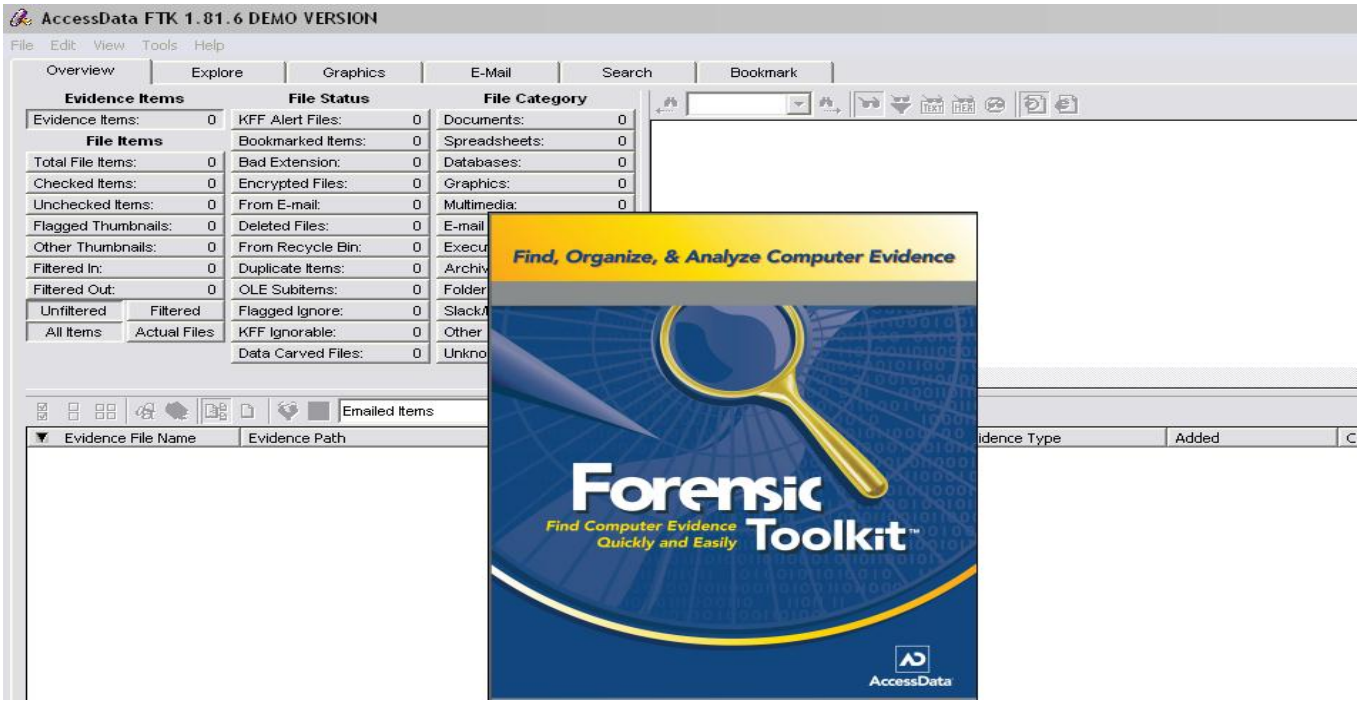
3. Esta pantalla nos presenta la lista de datos recuperados, presionas la opción eliminado y mostrara toda la información, para guardar un archivo click izquierdo sobre el archivo→**Guardar en**→seleccionas la unidad en la que vas a guardar la información→**Aceptar.**



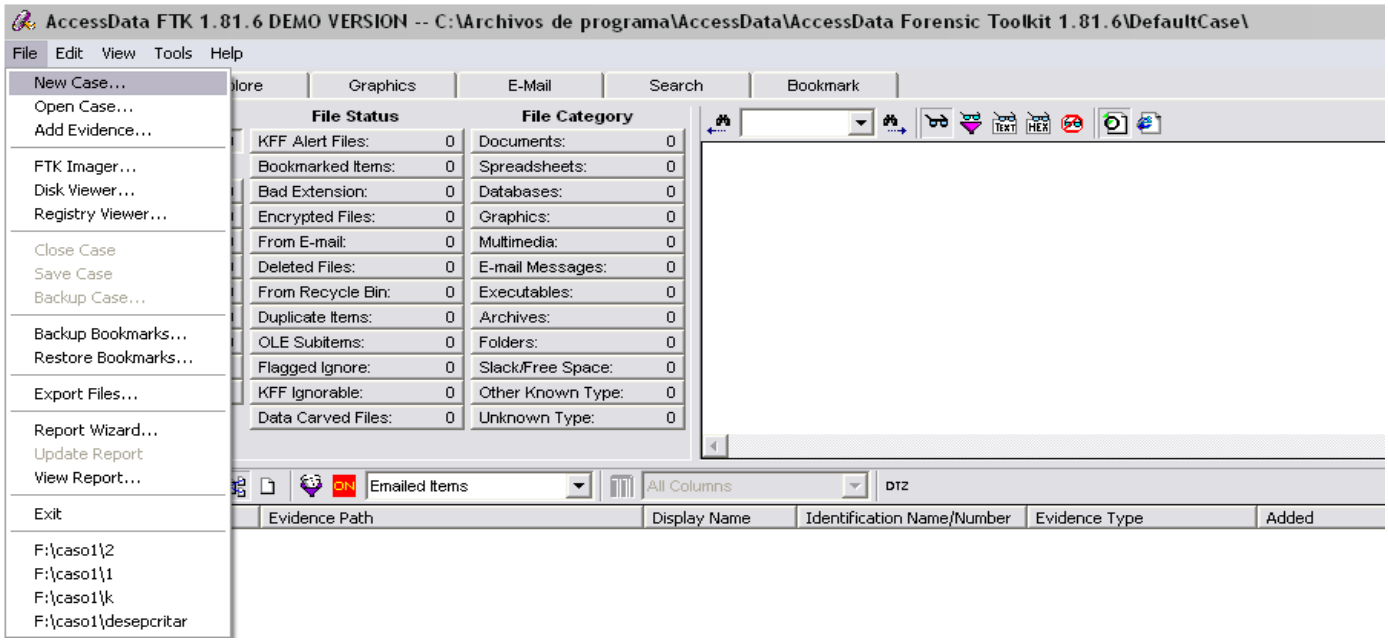


4. Si desea recuperar información que ha sido formateada nos ubicamos en la opción perdidos y presiona el botón **Encontrar datos perdidos→Entrar** el procedimiento para guardar es el mismo que el anterior.

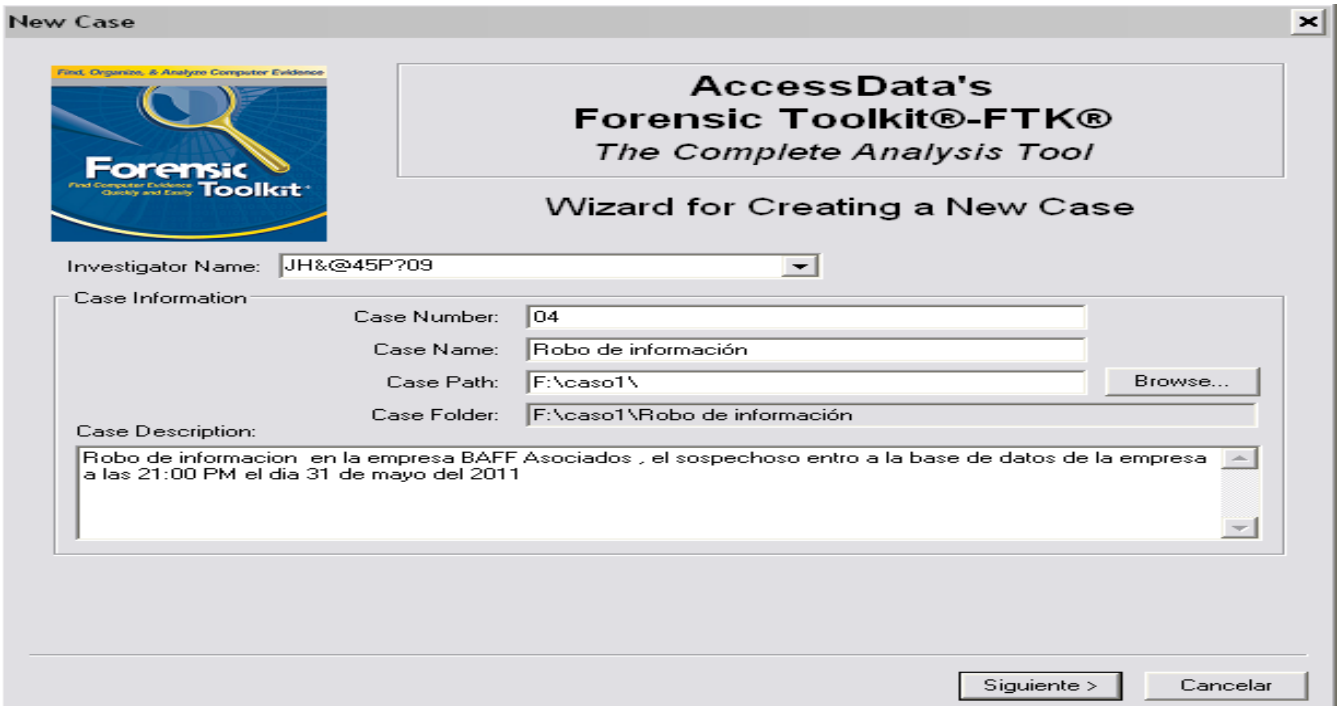
1. Pantalla inicial de ACCESDATA TOOLK´S. esta herramienta es específicamente para analizar todo tipo de discos duros, dispositivos USB y imágenes creadas con ACCESDATA FTK IMAGER Y STELLAR PHOENIX.

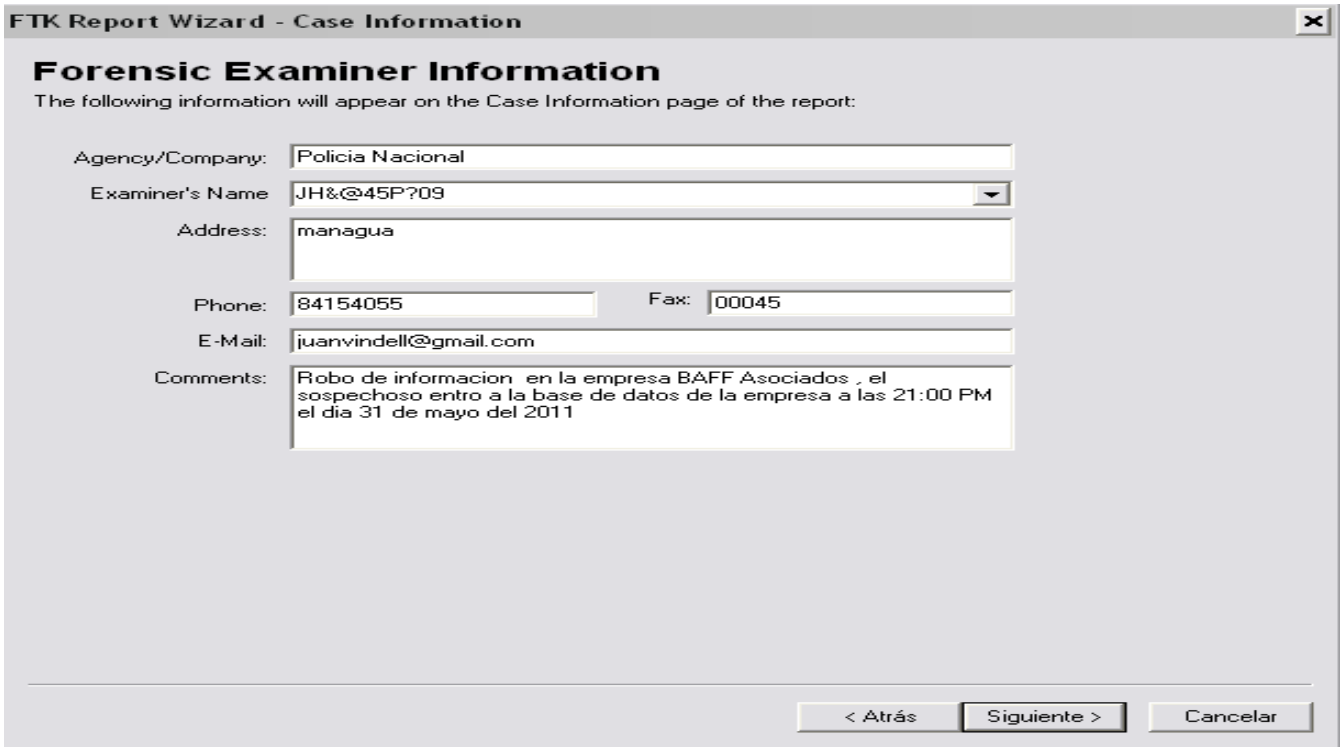


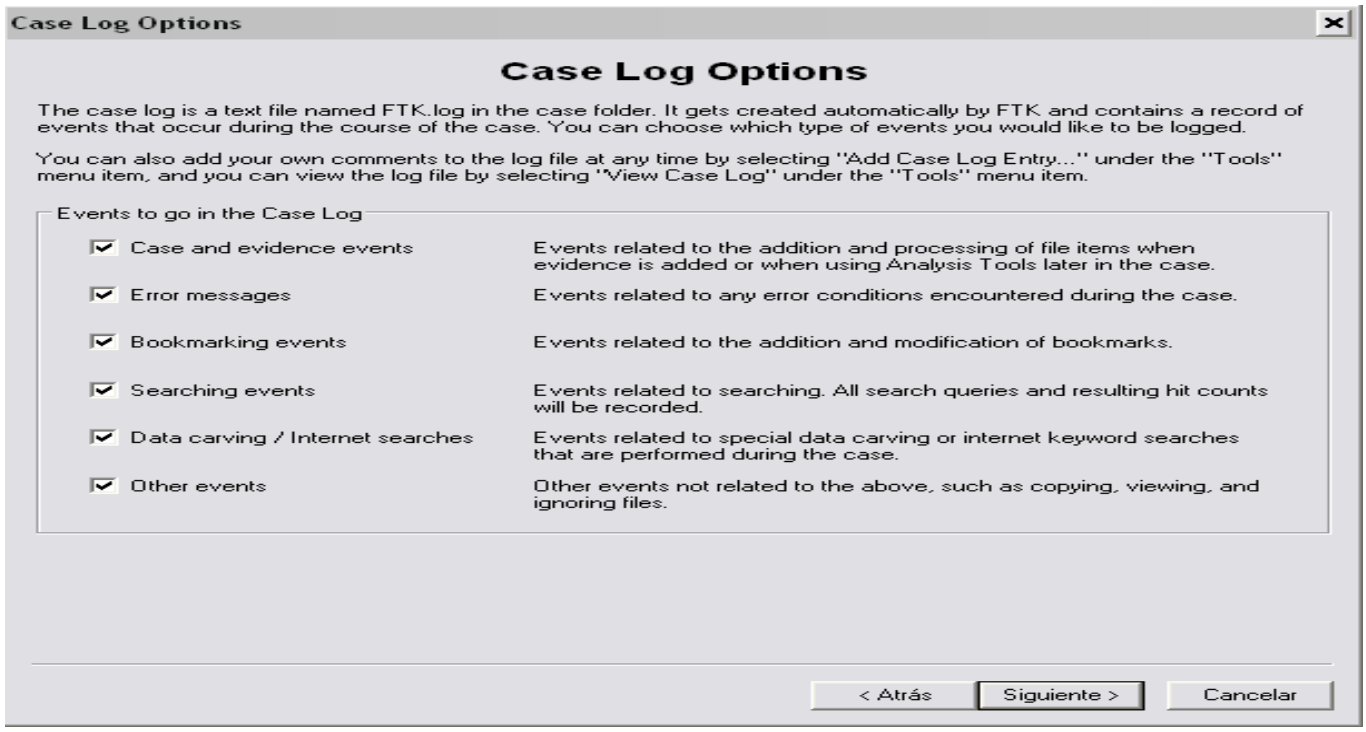
2. En la siguiente captura se muestra un análisis de la imagen de un dispositivo USB que fue creado con la herramienta **Stellar Phoenix.** Click **File→New Case**

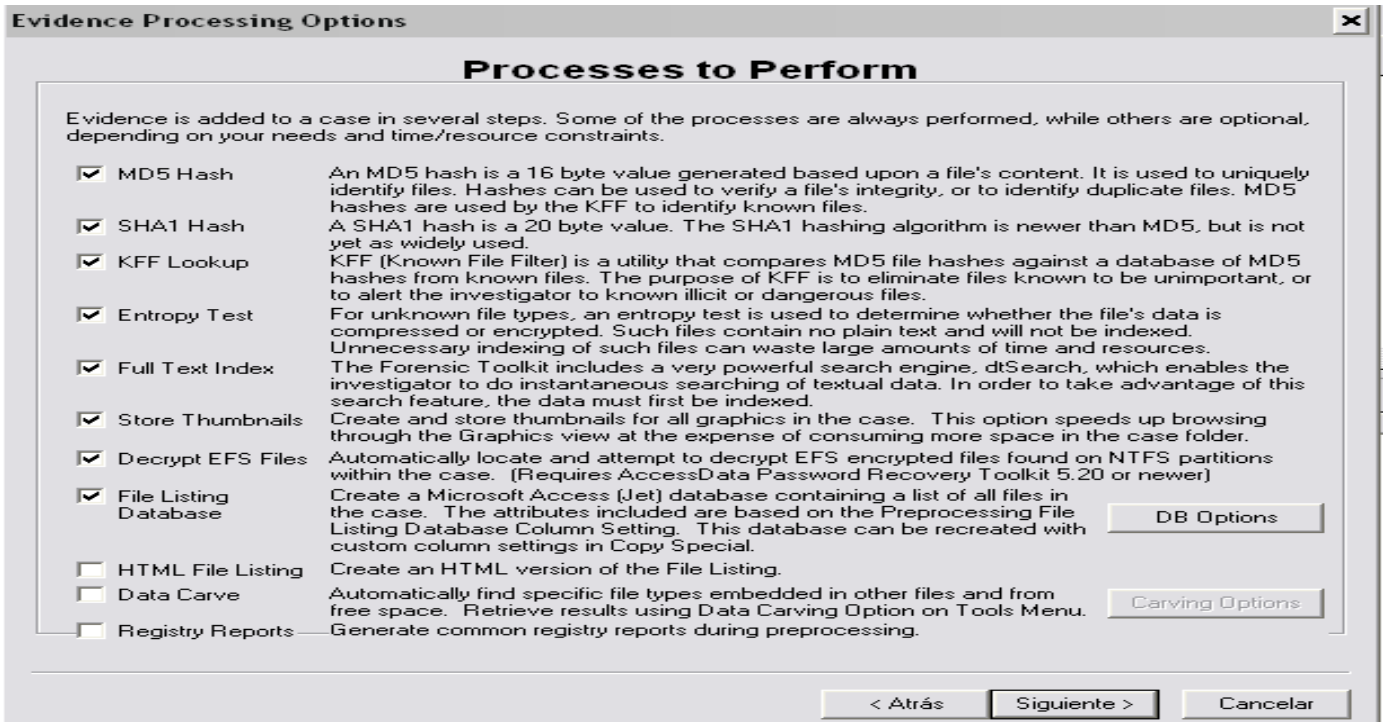


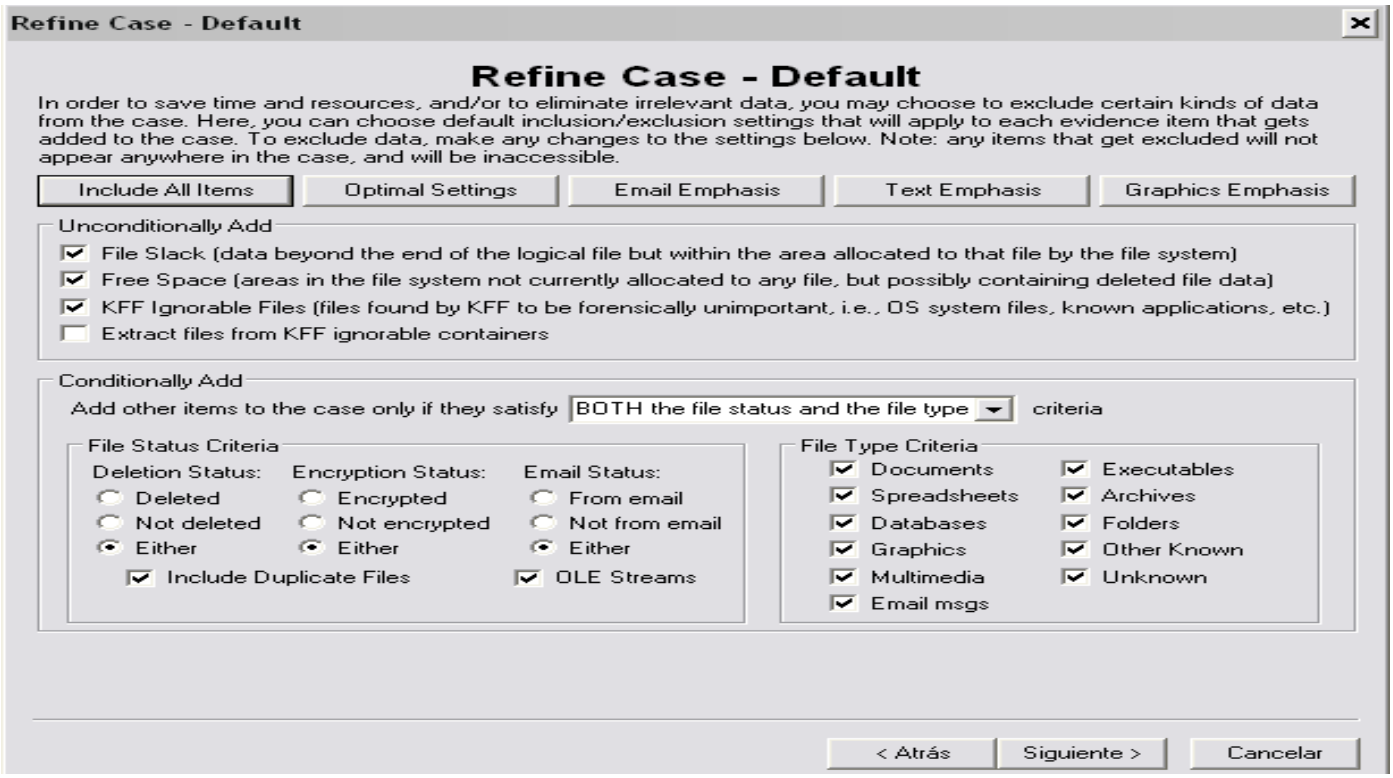
3. En la sección N**ew Case** agregamos información perteneciente al caso y presionamos **Siguiente** para llegar a la sección **Forensic Examiner Information(**verifica cierta información del examinador forense**) →Siguiente** llegas a la sección **Case log Options**(se marcan todas las opciones)**→ Siguiente** aparecerá la sección **Processes to Perform**(por defecto las tres últimas opciones no se marcan, porque esta herramienta al final del proceso genera una base de datos en Microsoft Office Access con toda la información acerca del caso analizado)**→Siguiente** accedemos a la sección **Refine Case-Default**(es recomendable dejar las opciones como aparece por defecto)**→Siguiente→Siguiente**

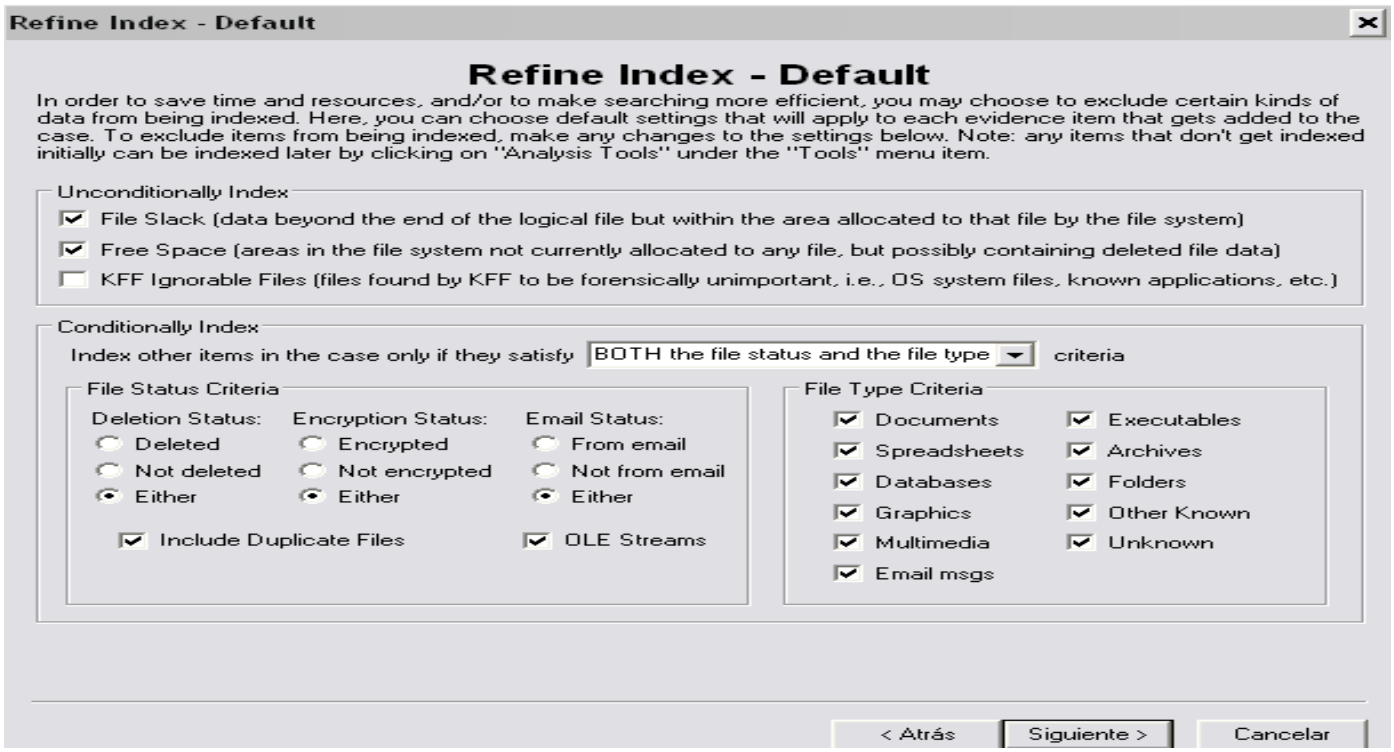




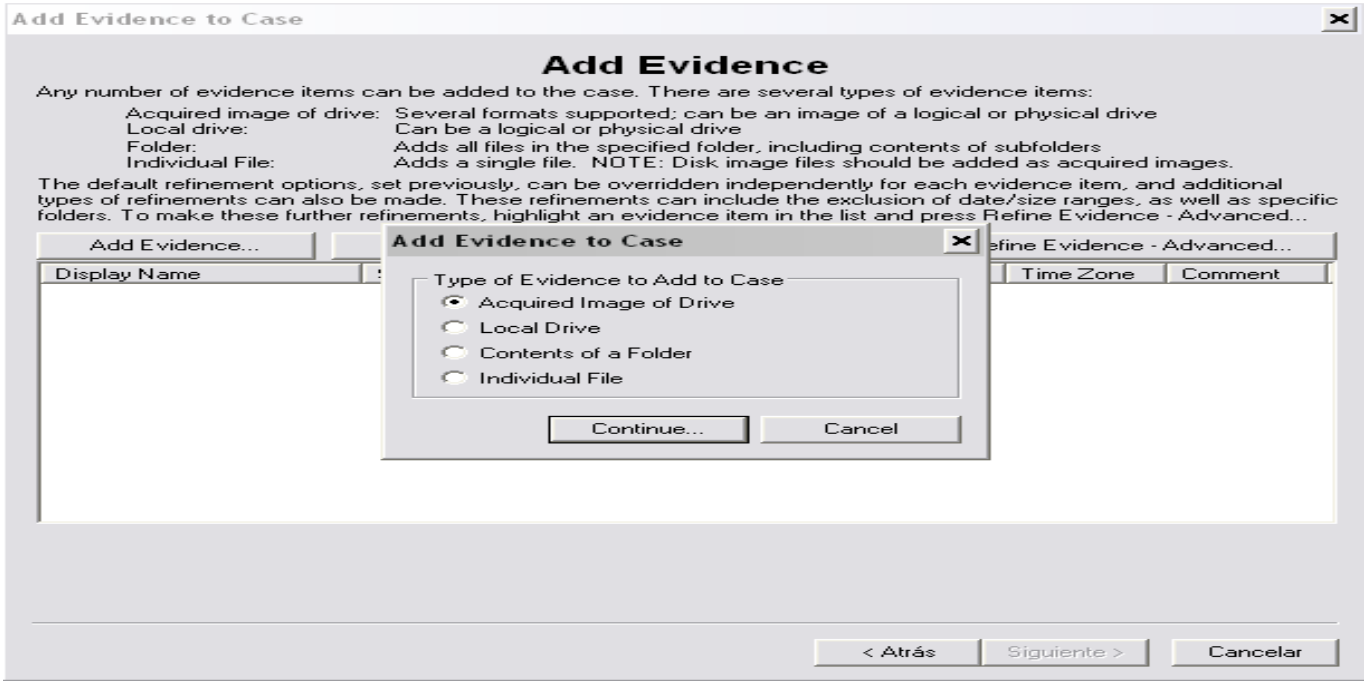

Case Log Options
Case Log Options
The case log is a text file named FTK.log in the case folder. It gets created automatically by FTK and contains a record of events that occur during the course of the case. You can choose which type of events you would like to be logged.
You can also add your own comments to the log file at any time by selecting "Add Case Log Entry..." under the "Tools" menu item, and you can view the log file by selecting "View Case Log" under the "Tools" menu item.
Events to go in the Case Log
Case and evidence events
Events related to the addition and processing of file items when evidence is added or when using Analysis Tools later in the case.
Error messages
Events related to any error conditions encountered during the case.
Bookmarking events
Events related to the addition and modification of bookmarks.
Searching events
Events related to searching. All search queries and resulting hit counts will be recorded.
Data carving / Internet searches
Events related to special data carving or internet keyword searches that are performed during the case.
Other events
Other events not related to the above, such as copying, viewing, and ignoring files.
< Atrás
Siguiente >
Cancelar

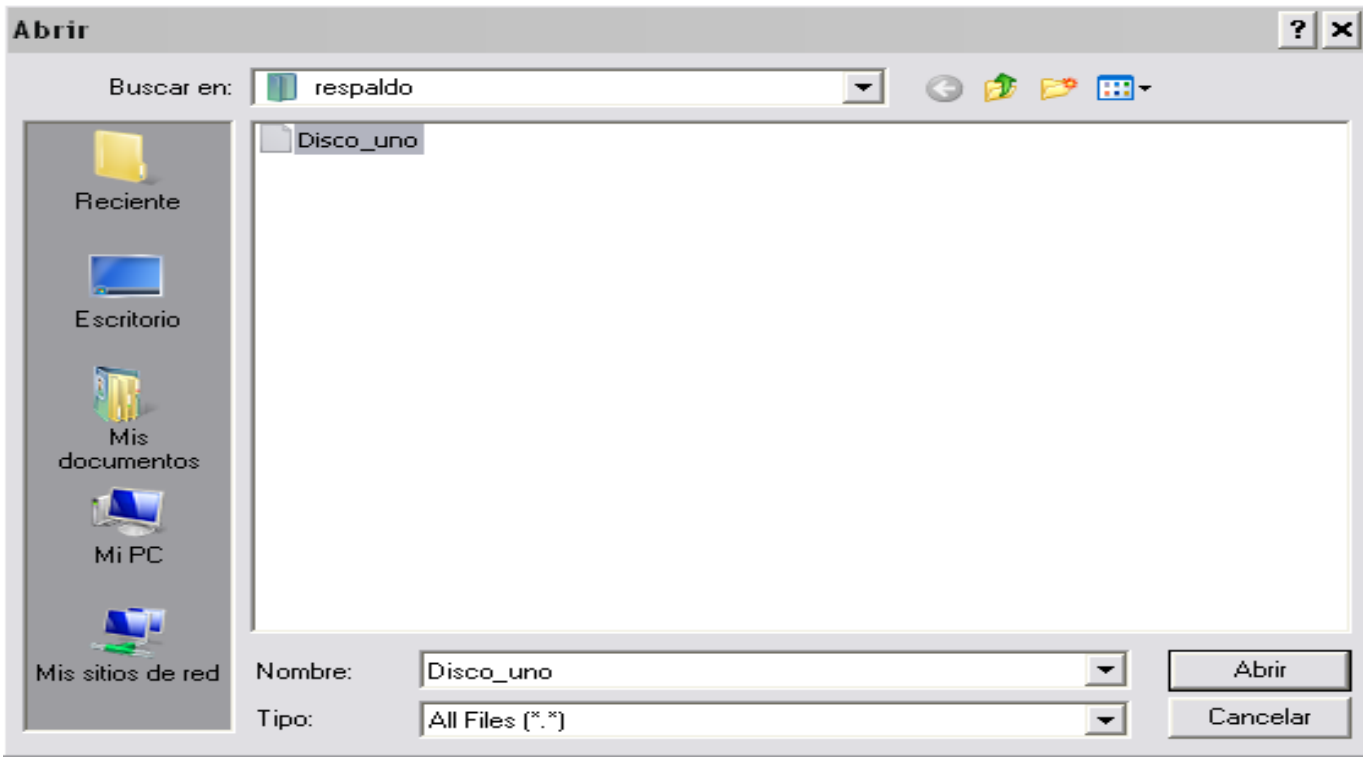

Evidence Processing Options
Processes to Perform
Evidence is added to a case in several steps. Some of the processes are always performed, while others are optional, depending on your needs and time/resource constraints.
MD5 Hash
An MD5 hash is a 16 byte value generated based upon a file's content. It is used to uniquely identify files. Hashes can be used to verify a file's integrity, or to identify duplicate files. MD5 hashes are used by the KFF to identify known files.
SHA1 Hash
A SHA1 hash is a 20 byte value. The SHA1 hashing algorithm is newer than MD5, but is not yet as widely used.
KFF Lookup
KFF (Known File Filter) is a utility that compares MD5 file hashes against a database of MD5 hashes from known files. The purpose of KFF is to eliminate files known to be unimportant, or to alert the investigator to known illicit or dangerous files.
Entropy Test
For unknown file types, an entropy test is used to determine whether the file's data is compressed or encrypted. Such files contain no plain text and will not be indexed. Unnecessary indexing of such files can waste large amounts of time and resources.
Full Text Index
The Forensic Toolkit includes a very powerful search engine, dtSearch, which enables the investigator to do instantaneous searching of textual data. In order to take advantage of this search feature, the data must first be indexed.
Store Thumbnails
Create and store thumbnails for all graphics in the case. This option speeds up browsing through the Graphics view at the expense of consuming more space in the case folder.
Decrypt EFS Files
Automatically locate and attempt to decrypt EFS encrypted files found on NTFS partitions within the case. (Requires AccessData Password Recovery Toolkit 5.20 or newer)
File Listing Database
Create a Microsoft Access (Jet) database containing a list of all files in the case. The attributes included are based on the Preprocessing File Listing Database Column Setting. This database can be recreated with custom column settings in Copy Special.
DB Options
HTML File Listing
Create an HTML version of the File Listing.
Data Carve
Automatically find specific file types embedded in other files and from free space. Retrieve results using Data Carving Option on Tools Menu.
Carving Options
Registry Reports
Generate common registry reports during preprocessing.
< Atrás
Siguiente >
Cancelar

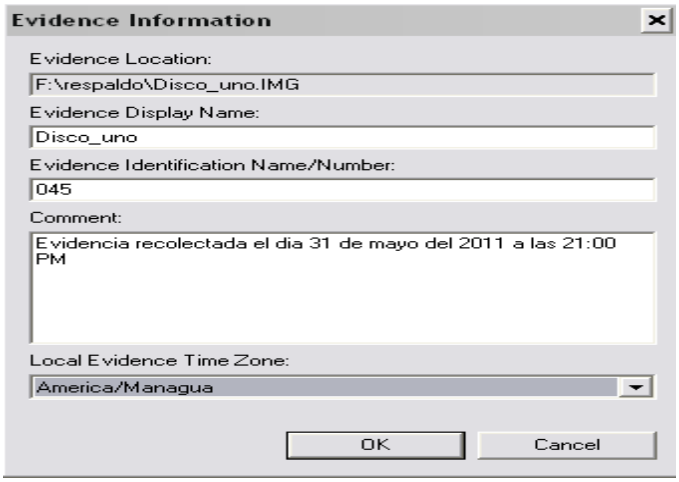

Refine Case - Default
Refine Case - Default
In order to save time and resources, and/or to eliminate irrelevant data, you may choose to exclude certain kinds of data from the case. Here, you can choose default inclusion/exclusion settings that will apply to each evidence item that gets added to the case. To exclude data, make any changes to the settings below. Note: any items that get excluded will not appear anywhere in the case, and will be inaccessible.
Include All Items
Optimal Settings
Email Emphasis
Text Emphasis
Graphics Emphasis
Unconditionally Add
File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)
Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)
KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.)
Extract files from KFF ignorable containers
Conditionally Add
Add other items to the case only if they satisfy BOTH the file status and the file type criteria
File Status Criteria
Deletion Status:
Deleted
Not deleted
Either
Encryption Status:
Encrypted
Not encrypted
Either
Email Status:
From email
Not from email
Either
Include Duplicate Files
OLE Streams
File Type Criteria
Documents
Spreadsheets
Databases
Graphics
Multimedia
Email msgs
Executables
Archives
Folders
Other Known
Unknown
< Atrás
Siguiente >
Cancelar

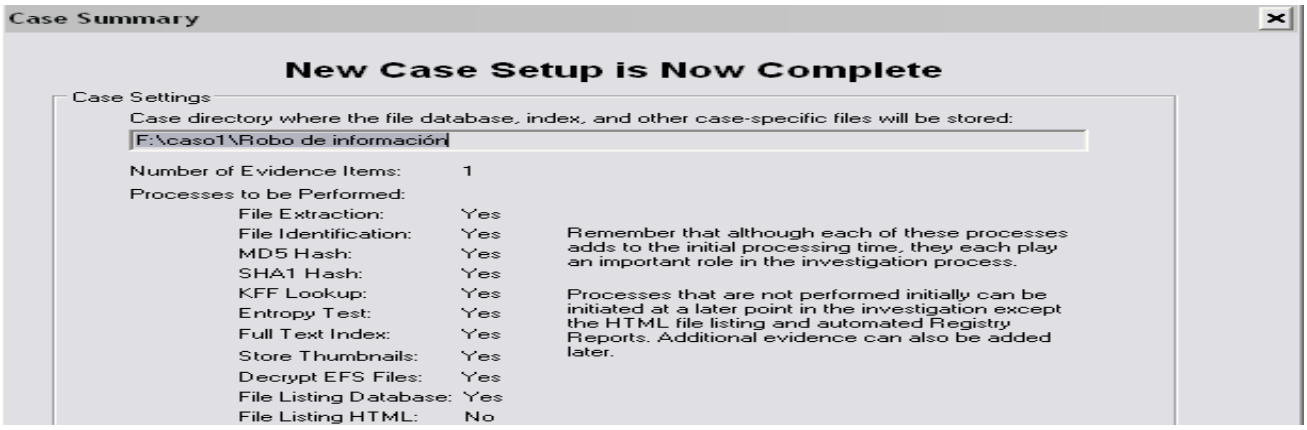

Refine Index - Default
Refine Index - Default
In order to save time and resources, and/or to make searching more efficient, you may choose to exclude certain kinds of data from being indexed. Here, you can choose default settings that will apply to each evidence item that gets added to the case. To exclude items from being indexed, make any changes to the settings below. Note: any items that don't get indexed initially can be indexed later by clicking on "Analysis Tools" under the "Tools" menu item.
Unconditionally Index
File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)
Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)
KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.)
Conditionally Index
Index other items in the case only if they satisfy BOTH the file status and the file type criteria
File Status Criteria
Deletion Status:
Deleted
Not deleted
Either
Encryption Status:
Encrypted
Not encrypted
Either
Email Status:
From email
Not from email
Either
Include Duplicate Files
OLE Streams
File Type Criteria
Documents
Spreadsheets
Databases
Graphics
Multimedia
Email msgs
Executables
Archives
Folders
Other Known
Unknown
< Atrás
Siguiente >
Cancelar

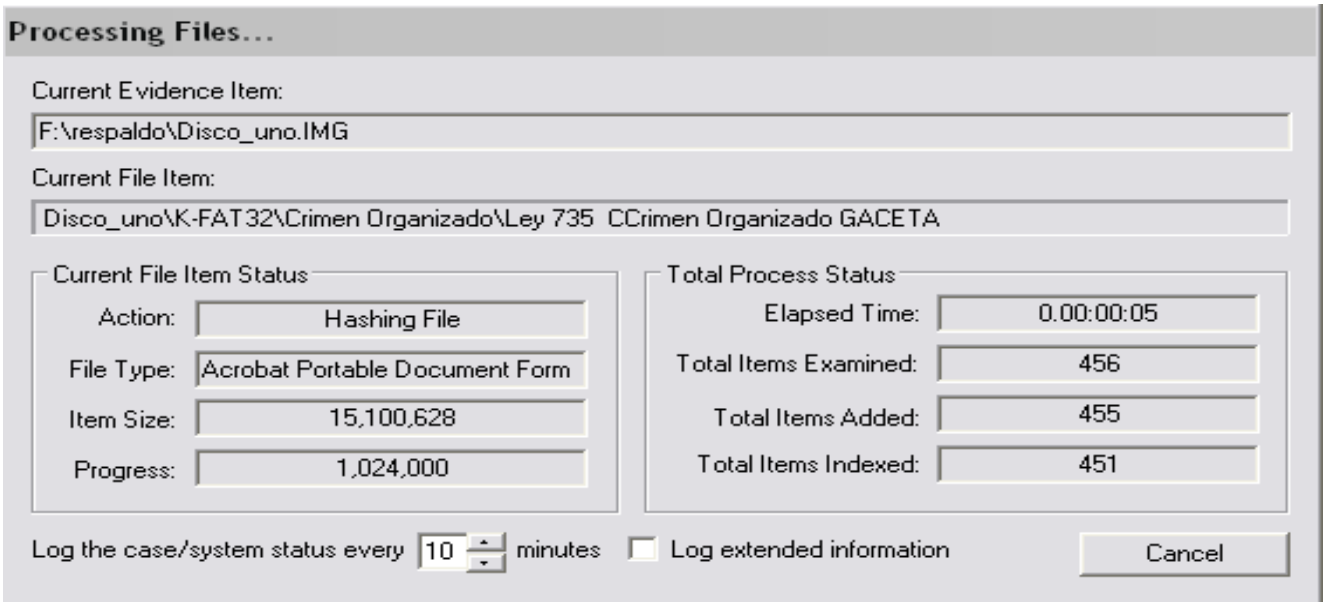
4. Aquí mostramos la sección agregar evidencia, hacemos click en la opción **Add Evidence→Acquired Image of Drive→Continue→Seleccionas la evidencia→Abrir** se muestra una ventana que contiene información de la evidencia, **agregue el numero de la evidencia**, especifique la zona **América/Managua→ Ok → Siguiente → Finalizar** (Para completar las datos del caso) continuamos con el análisis.



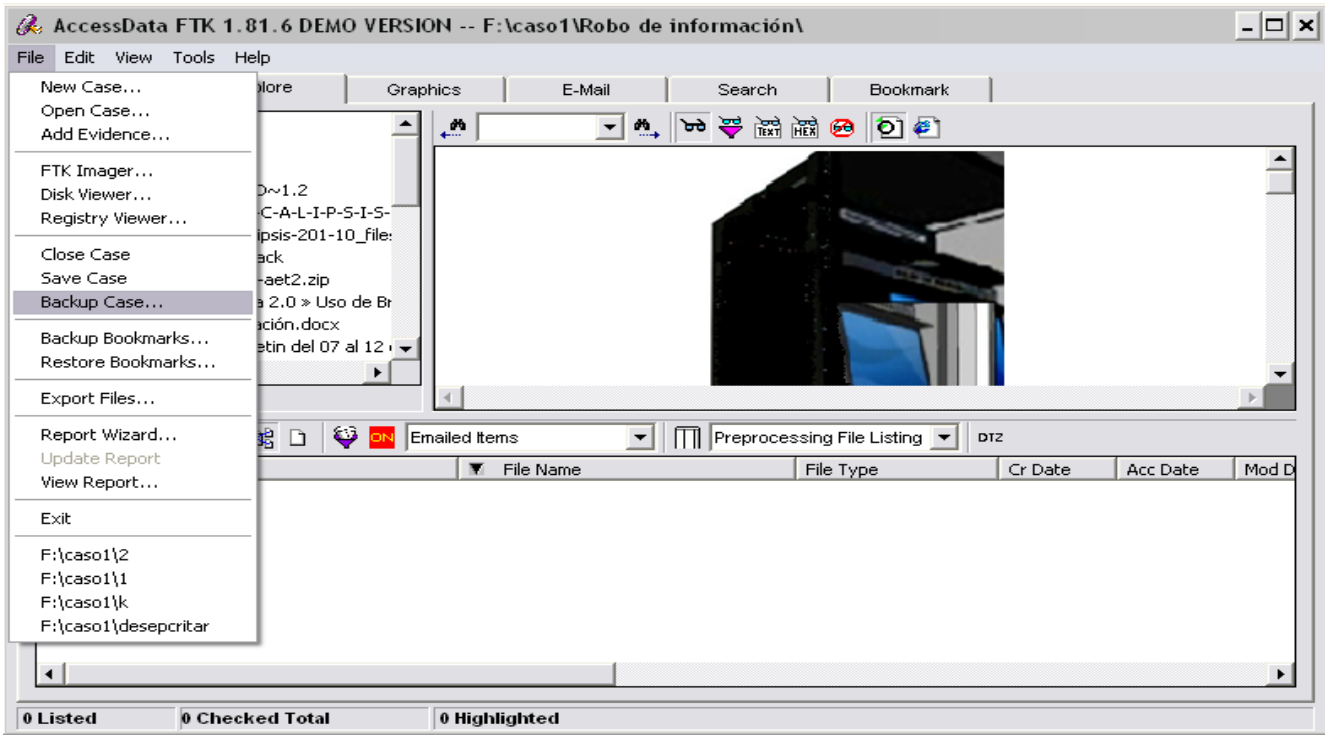


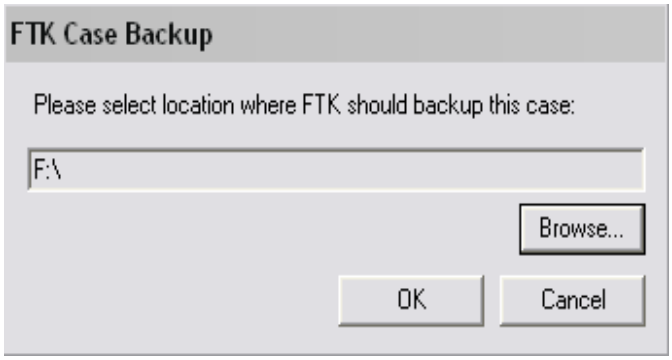

Evidence Information
Evidence Location:
F:\respaldo\Disco_uno.IMG
Evidence Display Name:
Disco_uno
Evidence Identification Name/Number:
045
Comment:
Evidencia recolectada el dia 31 de mayo del 2011 a las 21:00 PM
Local Evidence Time Zone:
America/Managua
OK
Cancel

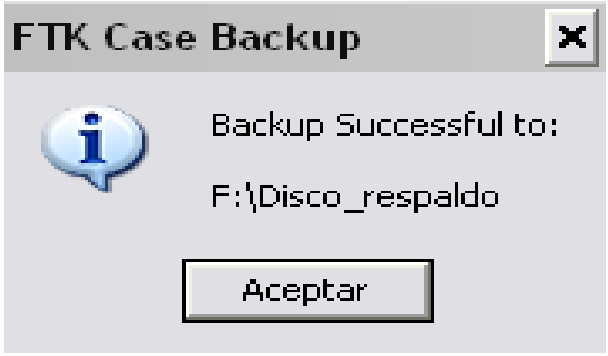

Case Summary
New Case Setup is Now Complete
Case Settings
Case directory where the file database, index, and other case-specific files will be stored:
F:\caso1\Robo de información
Number of Evidence Items: 1
Processes to be Performed:
File Extraction: Yes
File Identification: Yes
MD5 Hash: Yes
SHA1 Hash: Yes
KFF Lookup: Yes
Entropy Test: Yes
Full Text Index: Yes
Store Thumbnails: Yes
Decrypt EFS Files: Yes
File Listing Database: Yes
File Listing HTML: No
Remember that although each of these processes adds to the initial processing time, they each play an important role in the investigation process.
Processes that are not performed initially can be initiated at a later point in the investigation except the HTML file listing and automated Registry Reports. Additional evidence can also be added later.


Processing Files...
Current Evidence Item:
F:\respaldo\Disco_uno.IMG
Current File Item:
Disco_uno\K-FAT32\Crimen Organizado\Ley 735 CCrimen Organizado GACETA
Current File Item Status
Action: Hashing File
File Type: Acrobat Portable Document Form
Item Size: 15,100,628
Progress: 1,024,000
Total Process Status
Elapsed Time: 0.00:00:05
Total Items Examined: 456
Total Items Added: 455
Total Items Indexed: 451
Log the case/system status every 10 minutes
Log extended information
Cancel

5. Esta pantalla muestra la información recuperada, la herramienta permite visualizar los datos, Click en **Explorer (visualiza los datos recuperados)→K-FAT32 →** si desea crear un respaldo del caso presiona **File→Backup Case→Browse→OK**

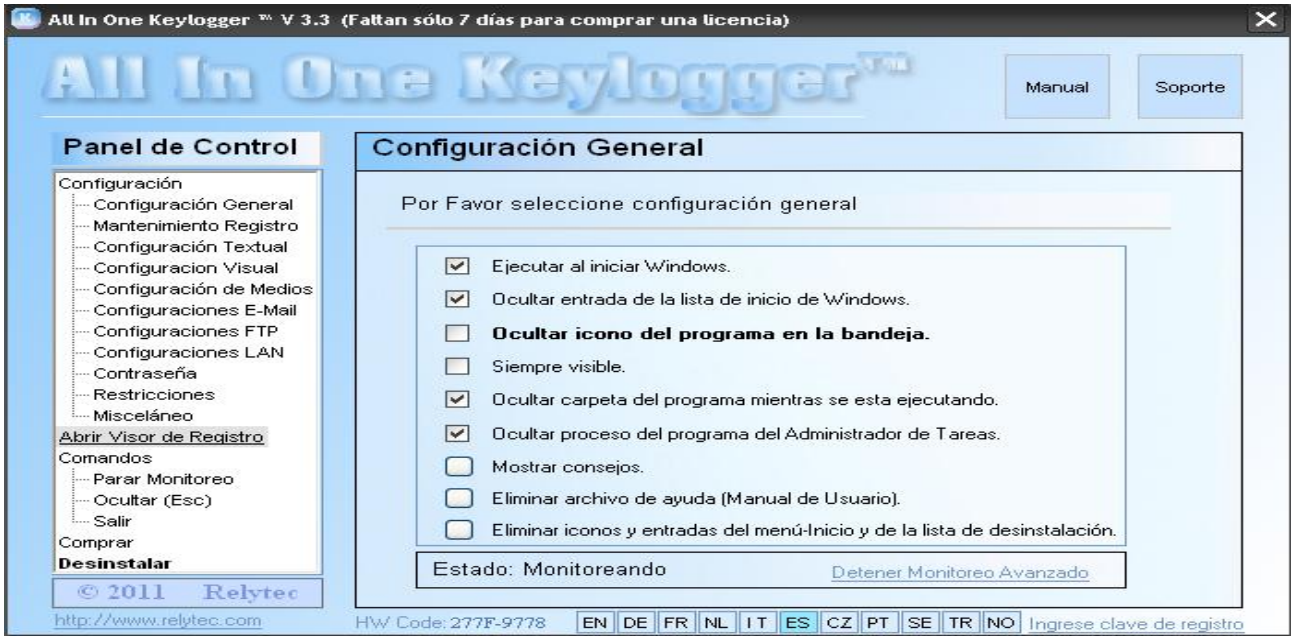






Manual de usuario de la herramienta forense KEYLOGGER

1. Menú principal de Keylogger, para revisar la información capturada por este software nos vamos a la opción **Abrir Visor de Registro→**en la sección visor de registro seleccionamos la pestaña **Ver Registro Textual→** una vez que estas dentro del registro haces click en **Ir a Registro Textual→Filtrar Registro** esta opción te permite visualizar si el sospechoso a utilizado la internet, si ha entrado a su correo, o enviado mensajes, si ha editado documento en Word, Excel etc.



2. De igual forma podes ver los registros de chat, web, audio, el procedimiento para cada registro es el mismo que se aplico en el **Visor de Registro Textual**, además podes crear reportes, doble click en **Reporte de Texto Simple**→seleccionas el dispositivo destino→**Aceptar.** Si deseas eliminar algún registro solo das doble click en el registro que deseas eliminar y presionas **Si/No**