Universidad de Buenos Aires
Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Título

HERRAMIENTAS OPEN SOURCE PARA INFORMÁTICA FORENSE

Subtítulo

HERRAMIENTAS FORENSES APLICADAS A WINDOWS

Autor: Ing. Leonardo Rafael Iglesias

Tutor: Lic. Julio César Ardita

2015

Declaración Jurada de Origen de los Contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

LEONARDO RAFAEL IGLESIAS
INGENIERO ELECTRÓNICO
DNI: 22.888.554

Prefacio

Dentro de la rama de la Seguridad Informática, destaca un área específica: la Informática Forense. El uso de técnicas forenses aplicadas a la informática no es antiguo, sino más bien reciente.

La informática forense no tiene más de 3 décadas de existencia y ya es una disciplina en pleno desarrollo y de vital importancia para la investigación judicial o privada, que emplea técnicas y herramientas propias para tales fines.

Como ocurre con la mayoría de las innovaciones y evoluciones en materia de tecnología, tanto en hardware como de software, esta disciplina no es ajena; debiendo constantemente refundarse y generar nuevos aplicativos o programas para estar a la altura de las exigencias actuales.

Es en éste sentido donde se observan herramientas o programas forenses, libres o comerciales, que permiten investigar y validar los resultados que se van obteniendo.

El correcto uso de dichas herramientas, sumado al de conocimientos metodológicos en materia de informática, así como la aplicación de un adecuado protocolo de trabajo conforman los elementos esenciales que caracterizan a esta rama de la informática.

Son muchos los programas que se emplean hoy en día en materia de informática forense, en particular los programas comerciales dependen en gran medida del poder adquisitivo que posea el especialista forense.

Otra alternativa radica en las herramientas "open source" o software de código abierto, que si bien no cuentan con tanto reconocimiento internacional en procesos legales como lo son las aplicaciones o herramientas licenciadas (Ej: Encase, FTK, etc), vienen haciendo un importante aporte en materia forense compitiendo mano a mano con éstas últimas.

Es en este punto donde deseo hacer hincapié, sobre las posibilidades y alcances que ofrecen dichas herramientas con respecto a las comerciales y en particular sus limitaciones y fortalezas.

Palabras clave: forense, protocolo, Encase.

Índice

Introducción

Los grandes costos y nuevas necesidades técnicas en materia de software comercial en estos últimos años, han hecho que se exploren otras herramientas no muy usadas en materia de informática forense.

Éstas herramientas la componen los programas denominados "**open source**", que brindan una alternativa gratuita a los programas comerciales como lo son ENCASE, FTK, etc.

Si bien las aplicaciones comerciales brindan un paquete de software completo y muy poderoso, éstas exigen por parte del cliente un oneroso intercambio para adquirir las permanentes actualizaciones y las licencias de los mismos.

Indagar en éstas herramientas y ver todas las posibilidades y recursos que ofrecen es de vital importancia cuando no se consiguen adquirir las mismas por problemas o inconvenientes en su adquisición.

Las Fuerzas de Seguridad en materia de informática forense han ido avanzando lentamente en la modernización de sus respectivos laboratorios informáticos, lo que hace interesante contar con diversas alternativas forenses.

Objetivos y alcance

- Conocer todas las capacidades, potencialidades y el alcance que brindan las herramientas o software de uso legal y gratuito o de código abierto; así como sus debilidades.

- Comparar fortalezas y debilidades de éstas herramientas "open source" respecto de los programas comerciales.

1. ¿Qué es la Informática Forense?

La Informática Forense, es una disciplina criminalística, que tiene por objeto, la investigación en sistemas de Tecnologías de Información de hechos con relevancia jurídica o para simple investigación privada[1].

Para conseguir sus objetivos, los expertos se basan en técnicas idóneas para ubicar, reproducir y analizar evidencia digital. La evidencia digital puede ser ubicada también en una amplia gama de equipos electrónicos como teléfonos móviles, agendas electrónicas, fax, dispositivos móviles de almacenamiento, Discos Compactos, Flash Cards y otro tipo de dispositivos de almacenamiento de información digital.

En principio, todo hecho acaecido en un sistema informático puede ser objeto de estudio y análisis y por ende puede ser utilizado en tribunales como medio probatorio.

Los peritos en la materia, utilizan entre otros el método de reconstrucción relacional, es decir, la ubicación en los ordenadores de los datos vinculados al caso tomando en consideración su secuencia de producción, teniendo como meta establecer el tiempo y concatenación de estos hechos a efectos de dar a conocer los elementos básicos de la investigación policial, como lo son: ¿Qué?, ¿Cómo?, ¿Cuándo?, ¿Dónde? y el ¿Por qué? de los hechos.

Los expertos en informática forense pueden hacer investigaciones sobre páginas Web, sus autores y servidores de todo tipo. Los análisis sobre imágenes digitales, archivos y la recuperación de datos borrados también entran dentro de la especialidad. El uso de computadores y redes puede ser reconstruido con fines de defensa y prevención de ataques o bien para establecer responsabilidades.

La informática forense tiene tres 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.

---

1 Daniel Fernández Bleda, "Informática Forense – Teoría y Práctica", Isec Auditors, 2004.

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

1.1. Evidencia Digital[2]

Un principio fundamental en la ciencia forense, empleado continuamente para relacionar un criminal con el crimen que ha cometido, es el "Principio de Intercambio o transferencia"[3], el cual manifiesta 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 lo lleva consigo), en otras palabras: "cada contacto deja un rastro".

Cada crimen tiene una "escena del crimen" que puede llegar a ser asegurada para buscar evidencia; pero algunas veces, la evidencia que se tiene que analizar no es una gota de sangre, una huella digital o la fibra de una alfombra. Son los bits y los bytes contenidos en un disco duro de una máquina. En estos casos, los investigadores necesitan tener el conocimiento necesario y la experiencia para poder obtener evidencia que puede estar dentro de la computadora, pero otras veces se encuentra escondida dentro de la misma.

En el caso que el crimen se haya cometido, es necesario hacer la investigación de lo que sucedió con esa computadora, pero si el crimen todavía no se comete; los investigadores deben de obtener evidencias y poder mantener una vigilancia para poder encontrar al sospechoso.

Pareciera cosa de un programa de investigación, de la televisión o el cine; pero esta es la realidad. Hoy en día, por medio del análisis forense, se pueden llegar a descifrar muchos delitos informáticos; delitos que son realizados usando la computadora como un medio para cometer el delito o simplemente cuando alguien ataca una computadora para poder sustraer información de ella, algo que conocemos como robo de secretos industriales o de información confidencial.

El análisis forense es una disciplina que permite identificar, analizar, preservar y presentar evidencia digital obtenida de infraestructura tecnológica de tal manera que sea válida en un proceso legal, pero muchas

---

[2] *Guía práctica operativa para procedimientos judiciales con secuestro de Tecnología Informática"*, Dirección de Policía Científica, Departamento Estudios Especiales, División Delitos Informáticos, 2008.

[3] Edmond Locard, Locard, "La Police et les Méthodes Scientifiques", Les Éditions Rieder, 1934.

de las veces el proceso se convierte únicamente en interno, ya que muchas empresas deciden el no denunciar al respecto, pero también hay muchas que sí lo hacen.

Esta infraestructura tecnológica puede ser desde un teléfono celular, una cámara digital, una computadora, una impresora, una memoria digital o hasta una agenda. Todos estos elementos hoy en día tienen memoria, dispositivos que poco a poco se convierten en computadoras, ya que por ejemplo en un celular ya podemos tomar fotografías y almacenarlas en el mismo teléfono.

Delitos como el secuestro, fraude en portales financieros, fraudes en general, pornografía infantil, narcotráfico y pornografía son hoy por hoy investigados por personas especialistas en el área en todo el mundo. Pero el análisis forense no solo se realiza de manera judicial o pericial para poder presentarlo ante la ley; sino que también puede ser utilizado como herramienta dentro de las empresas para poder determinar si alguien está realizando un fraude, ha robado información propietaria o secretos industriales. En pocas palabras, para poder determinar qué fue lo que pasó en la computadora o infraestructura de cómputo.

A diferencia con la disciplina forense tradicional, tenemos también una escena del crimen, la cual puede ser una computadora o un archivo. Una de las características principales de la investigación de infraestructura tecnológica es la fragilidad de la evidencia. Por ejemplo, al abrir un archivo de texto, con el simple hecho de darle doble clic a el archivo, se modifica la última fecha de acceso al mismo, por lo tanto, ¿cómo podemos mantener la evidencia sin ningún cambio?

Esta es una de las partes más difíciles dentro de la investigación, ya que con un simple cambio a la evidencia digital, ésta puede ser descartada por el mal manejo que haya tenido el investigador.

Si seguimos con la analogía con un caso normal, el arma dentro de una computadora puede llegar a ser una acción, o un flujo de datos que al llegar a la computadora desaparece y no es posible saber de ella. Por lo mismo, son muchos elementos los que hay que tomar en cuenta para poder hacer la investigación.

La Informática Forense puede ser usada para descubrir evidencia potencial en una variedad de casos, incluyendo:

- Delitos contra la Propiedad Intelectual, en caso de Software Pirata o documentos con el debido registro de derechos de Autor.
- Robo de Propiedad Intelectual y Espionaje industrial (que existe a gran escala en nuestro país).
- Lavado de Dinero, vía transferencia de fondos por Internet.
- Acoso Sexual (vía e-mail); Chantaje o amenazas (vía e-mail).
- Acceso no autorizado a propiedad intelectual.
- Corrupción.
- Destrucción de Información Confidencial.
- Fraude (en apuestas, compras, etc. Vía e-mail).
- Pornografía en todas sus formas, inclusive en la más devastadora: Pornografía infantil.

Del mismo modo, la evidencia digital que contiene texto en puede dividirse según sus características en tres categorías[4]:

- 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.

---

[4] *"Evidencia Digital, Reflexiones Técnicas, Administrativas y Legales"*, Jeimy. J. Cano, Universidad de los Andes, Facultad de Ingeniería, 2004.

- 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.

En resumen, la prueba digital es un tipo de evidencia física. Está constituida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales

1.2. Conceptos clave. Delitos Informáticos

En primera instancia, resulta necesario especificar que la **Evidencia Digital**, objeto del análisis informático forense abordado en el presente trabajo, se clasifica en DOS (2) tipos:

- **Evidencia Digital VOLÁTIL** (SE PIERDE si el equipo es apagado).
- **Evidencia Digital NO VOLÁTIL** (NO SE PIERDE si el equipo es apagado).

Ahora bien, es necesario señalar que los equipos de computación, en su generalidad, constan de distintos medios de almacenamiento, siendo los más comunes los siguientes:

A. **MEMORIA RAM** (RANDOM ACCESS MEMORY): Memoria de Acceso Aleatorio – Almacena información VOLÁTIL.
B. **HD** (HARD DISK): Disco Duro – Almacena información.
C. **CD** o **DVD** – Almacena información NO VOLÁTIL.
D. **PEN DRIVE (MEMORIAS EXTRAÍBLES, etc.)** – Almacena información NO VOLÁTIL.

Es dable mencionar que el empleo por defecto, de tales medios de almacenamiento depende del usuario, ya que el mismo, en todo momento, puede establecer la ubicación final (o temporal) de la información que desee almacenar. Por ejemplo, mientras que algunos usuarios guardan todos los datos críticos en una carpeta del tipo "Mis Documentos", otros guardan todo en otra carpeta, o bien en otro medio de almacenamiento.

1.3. Metodología forense de trabajo

La metodología aplicada en la Dirección de Criminalística y Estudios Forenses de Gendarmería Nacional Argentina - División Informática Forense, organización de la que dependo, consisten en técnicas y métodos empleados a nivel mundial en lo que se denominan "buenas prácticas forenses". Para desarrollar un estudio informático y dilucidar los puntos de pericia que en cualquier caso se soliciten, consta de CUATRO (4) etapas bien definidas:

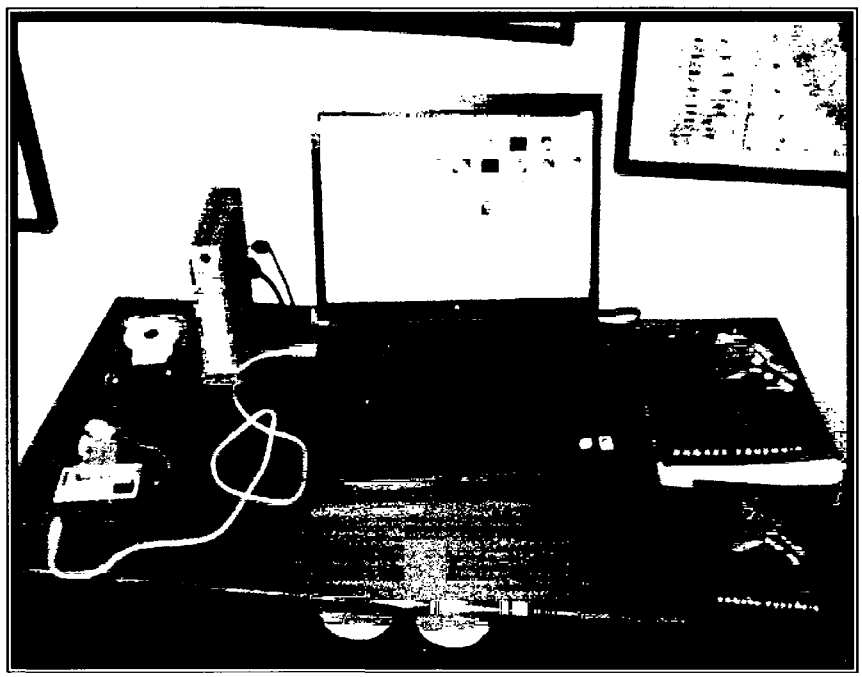
1ra. Acceso informático forense
2da. Identificación de la evidencia
3ra. Autenticación de la evidencia
4ta. Preservación de la evidencia

La 1ra etapa se concreta mediante el uso de la herramienta forense "Encase" de "Guidance Software" cuya licencia se encuentra a nombre de la Dirección anteriormente mencionada **(VER GRÁFICO INFERIOR)** y tiene por objetivo obtener la mayor cantidad de evidencia digital almacenada en los HD (Hard Disk) de las computadoras cuestionadas, sin alterar tal evidencia.

Para efectuar el acceso forense al medio de almacenamiento cuestionado, se debe emplear un dispositivo que asegure la lectura (READ)

de los datos y que impida la modificación, borrado o sobreescritura (WRITE) de los mismos. Tal dispositivo se denomina "WRITE BLOCKER" (Bloqueador de escritura) y la conexión se describe a continuación:

- El Disco Rígido (HD) examinado se conecta al dispositivo bloqueador de escritura ("WRITE BLOCKER") a través de un cable de datos IDE o SATA (dependiendo de la interfaz del HD). Luego el "WRITE BLOCKER" se conecta a la computadora del investigador, en la cual se encuentra instalado el software forense "ENCASE", empleando para ello UN (1) cable USB en la generalidad de los casos ***(VER GRÁFICO INFERIOR)***.



En la 2da etapa (IDENTIFICACIÓN DE LA EVIDENCIA), se identifican un conjunto de objeto y/o pruebas las cuáles serán las adecuadas para ser tomadas como evidencia. La recopilación de evidencia puede resultar complicada, puesto que no se debe alterar la misma; teniendo en cuenta que es susceptible a variaciones y tiende a perderse si no se tratan con software y hardware adecuados.

Es dable de mencionar que, generalmente la información más sensible se encuentra en carpetas convencionales, las cuales se identifican

de distinta manera ya que obviamente pueden existir distintos perfiles de usuarios que emplean un mismo equipo informático. El tipo de información que se obtiene, por lo general no se encuentra al alcance del usuario convencional.

Entre los atributos fecha de creación del archivo, fecha de modificación, fecha de último acceso; para el caso de los archivos borrados se puede determinar la fecha en la que fue borrado, resultando inclusive recuperar el archivo, para aquellos casos en que sea factible.

Está claro que el filtrado de la evidencia digital relevada se encontrará en función de la línea de investigación de la causa, en razón al oficio Judicial recibido y a los puntos Periciales solicitados.

En la 3ra etapa, se autentica la evidencia, lo cual implica el cálculo de firmas digitales, empleando para ello DOS (2) Algoritmos de hash distintos: MD5 y SHA1. El cálculo de tales firmas digitales garantiza, en todo momento, el origen y la integridad de las evidencias digitales recolectadas.

Es dable de mencionar, que se calculan DOS (2) algoritmos de manera simultánea, ya que de esa manera se garantiza que los mismos, de manera conjunta, resultan ser otra forma de identificar UNÍVOCAMENTE a tales archivos.

En la 4ta etapa, se preservan las evidencias recolectadas mediante una copia en formato óptico (por lo general en formato DVD). Esta copia permite disponer en todo momento, a las autoridades judiciales y al personal que trabaja en la investigación de las distintas causas, de un respaldo de los archivos que resultan de interés para la investigación.

1.4. Tipos de análisis forense

Dependiendo del punto de vista nos vamos a encontrar diferentes tipos de análisis forense. Teniendo en cuenta la perspectiva de lo que se va a analizar, nos encontraremos los siguientes tipos:

• Análisis forense de sistemas: en este tipo de estudios se analizarán los casos de seguridad acontecidos en servidores, estaciones de trabajo, pc de tipo hogareña, etc; con los diferentes sistemas operativos que nos podemos encontrar, como ser: Mac OS, todas las variantes de sistemas operativos de Microsoft (Windows 9X/Me, Windows 2000 server/workstation, Windows 2003 Server, Windows XP, Windows Vista, Windows 2008 Server, etc.), sistemas Unix (Sun OS, HP-UX, AIX, etc.) y sistemas GNU/Linux (Debian, RedHat, Suse, etc.).

• Análisis forense de redes: en este tipo se engloba el análisis de diferentes redes (cableadas, wireless, bluetooth, etc.). Este tipo de análisis es bastante complejo. Puede consistir en analizar si un archivo o registro se ha sido enviado desde determinada computadora, analizar los logs de los firewall, etc, etc.

• Análisis forense de sistemas embebidos: en dicho tipo de estudio se analizaran los diferentes incidentes ocurridos en dispositivos móviles, tablets, etc. Un sistema embebido posee una arquitectura semejante a la de un ordenador personal. Por lo general los sistemas de análisis de equipos de telefonía celular (UFED, XRY, etc), efectúan en forma automática la imagen forense de los móviles celulares para luego realizar un informe con sus correspondientes HASH, que puede ser presentado en formato html, doc, pdf, etc.

1.5. Las esperadas normas ISO

Hoy en día, el análisis forense informático se realiza sobre medios ópticos, magnéticos y de estado sólido, apoyándose los expertos forenses en lo que se denominan "las buenas prácticas internacionales". Estas prácticas se basan en una serie de pasos, que pueden ser 4 o 5, para efectuar el correcto aseguramiento de la evidencia digital.

Estas modalidades de trabajo, que se efectúan sobre componentes informáticos, no estaban unificadas en una única norma internacional. Solo existían documentos en determinados países, como la **HB171-2003** Guidelines for the Management of IT Evidence, creada en Australia por la academia, industria, administración de justicia, gobierno y entes policiales, las guías del NIST sobre esta temática, las indicaciones del Departamento de Justicia de los Estados Unidos en los documentos como Forensic Examination of Digital Evidence: A Guide for Law Enforcement, Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition, etc, etc. Dichos elementos son empleados como base referencial al momento de presentar pruebas ante los organismos que así lo requieran (juzgados, universidades, entes gubernamentales, etc).

Es en este sentido, que aparece una norma de alcance global: la norma **ISO/IEC 27037:2012** donde se instituyen las pautas para la identificación, recolección, adquisición y preservación de la evidencia digital, como un primer documento reconocido por la comunidad internacional y de alcance global. Si bien su implementación está orientado hacia las pericias de índole informático, el mismo aún está incompleto, faltando aún varios años para su completitud.

Desde ya, dicho documento será a futuro un referente mundial, un estándar en lo que se refiere a las buenas prácticas en materia forense informática

2. Herramientas de análisis

En la actualidad es posible contar con un sinfín de aplicaciones forenses para uso informático. Todo depende de qué tipo de análisis forense vamos a realizar y la plataforma a analizar. No es lo mismo un Windows xp o de otra generación a examinar una versión de Linux o una mac os.

En este sentido es conveniente contar con diversas herramientas, no todas las aplicaciones comerciales y/o de tipo "open source" cubren todas las posibilidades o casos que vayamos a encontrarnos. Es necesario contar con un abanico de elementos para hacer frente a imprevistos.

Desde ya, que contar con aplicaciones como el ENCASE o FTK comerciales agiliza mucho el trabajo, sin mencionar que a eso le agreguemos duplicadores forenses, discos externos, bloqueadores de escritura, etc.

Estas herramientas comerciales como el ENCASE, disponen de un abanico de aplicaciones internas muy potentes que las diferencian de las herramientas libres y las hacen ideales para hallar elementos que permitan probar un determinado delito informático. Estas aplicaciones van desde el crear un caso, realizar una imagen forense, visualizar el contenido de esa copia bit a bit efectuada, seleccionar archivos por fecha o extensión, asignarles a cada elemento extraído firmas digitales (SHA o MD5), reproducir o visualizar archivos, etc, etc.

A diferencia de lo anterior, las herramientas o programas gratuitos, a excepción del DEFT, constituyen aplicaciones específicas que realizan determinadas actividades forenses, como son efectuar una imagen forense, hacer cálculo de hash, realizar una búsqueda de palabras clave, etc.

2.1. Software "open source" vs. Software comercial

Desde hace años ha existido una cuestión entre el software de código abierto respecto de las herramientas de código cerrado respecta a su utilización en un medio legal.

Hallar evidencia de la comisión de un delito con determinada aplicación forense debe cumplir con ciertos requisitos legales.

En un principio el software forense empleado era de características propietario, personalizado y realizado principalmente por agencias del gobierno. A medida que pasaron los años, el análisis se hizo disponible para los sectores público y privado. Desde no hace muchos años, han aparecido versiones de tipo "open source" que proporcionan características semejantes a las de tipo comercial.

La elección de una u otra opción estará determinada por las posibilidades monetarias que posea el examinador forense, estando siempre la libertad o posibilidad de comenzar empleando las herramientas o programas libres que existen.

2.2. Ventajas y desventajas en cada caso

Software "Open Source"

El software de código abierto goza de una ventaja distintiva frente a la versión comercial, la económica, dicho de otro modo el usuario no paga por la licencia de uso del programa.

Asimismo, si el software presenta algún tipo de problema, se puede modificar para que se acomode a las necesidades de cada uno.

No todos los Juzgados aceptan de igual modo por igual estas herramientas libres, por ello es necesario que al momento de fundamentar en el informe se agreguen las correspondientes certificaciones de que gocen la misma, expedidas por organismos reconocidos a nivel mundial (Ej: NIST[5], BCR[6], etc).

Es en este sentido, que NIST en su sitio[7] web, realiza un profundo análisis de estas herramientas libres, destacando sus capacidades de trabajo, que son de suma importancia para acreditar los beneficios de las mismas.

Es por ello que es esencial que éstas herramientas sean analizadas en profundidad para determinar si las capacidades que les otorgan sus creadores son ciertas y no perjudiquen o eliminen con su accionar al valor de la prueba.

Software comercial

El software propietario, privativo o de código cerrado, en el que el usuario tiene limitaciones para usarlo, modificarlo o redistribuirlo. Su acceso se halla restringido por un acuerdo de licencia.

---

[5] National Institute of Standards and Technology: el instituto nacional de normas y tecnología es una agencia del Departamento de Comercio de los Estados Unidos, cuya misión es promover la innovación y la competencia industrial en Estados Unidos.

[6] Community Bureau of Reference: sienta las directivas y bases legales para la armonización y regulación de los estándares de la comunidad europea.

[7] http://www.cftt.nist.gov/

Dadas las características de los programas de código cerrado, un usuario cualquiera ignora el contenido del mismo y por tanto si existe algún tipo de amenaza contra su pc o información personal.

3. Bloqueadores de Escritura

Para efectuar el acceso forense a cualquier medio de almacenamiento a analizar (disco magnético, disco de estado sólido, pendrive, disco óptico, etc), se debe emplear un dispositivo que asegure la lectura (READ) de los datos y que impida la modificación, borrado o sobreescritura (WRITE) de los mismos. Tal dispositivo se denomina "WRITE BLOCKER" (Bloqueador de escritura) y cuya conexión se efectúa entre el disco a analizar y la pc que realiza la imagen forense (bloqueador por hardware).

Para el caso de bloqueadores por software, estas vienen asignadas por defecto en todas las herramientas comerciales y en las de código abierto, cuando el caso se trate de unidades USB. Para el caso de discos magnéticos o de estado sólido se puede bloquear la escritura desde el comando de Windows o con alguna aplicación específica para tal fin. En éste caso se instala el software que desea bloquear el acceso USB, permitiéndole seleccionar el tipo de bloqueo USB en los equipos informáticos.

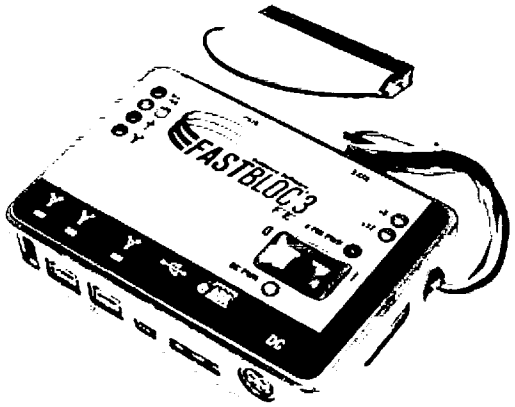
3.1. Bloqueadores por hardware

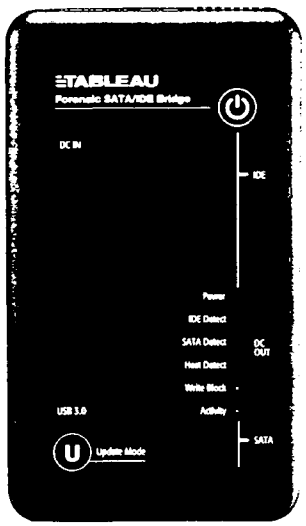
Es un dispositivo de hardware para bloqueo de escritura que permite al investigador obtener una adquisición segura de un medio de almacenamiento o ya sea para tener una vista preliminar o conectar un dispositivo.

Cuando se activa la capacidad de bloqueo contra escritura de un equipo hardware bloqueador, asegura que no se escriban ni modifiquen datos en el dispositivo bloqueado contra escritura.

La aplicación de estos productos es para los investigadores policiales y de seguridad corporativa o para examinadores forenses de computadoras.

Equipos de éstas características lo constituyen: "Fastbloc" y el equipo "tableau", tal cual se observan en la siguientes imágenes ilustrativas:





3.2. Bloqueadores por software

Existen diversas herramientas y/o aplicaciones que efectúan bloqueo por software.

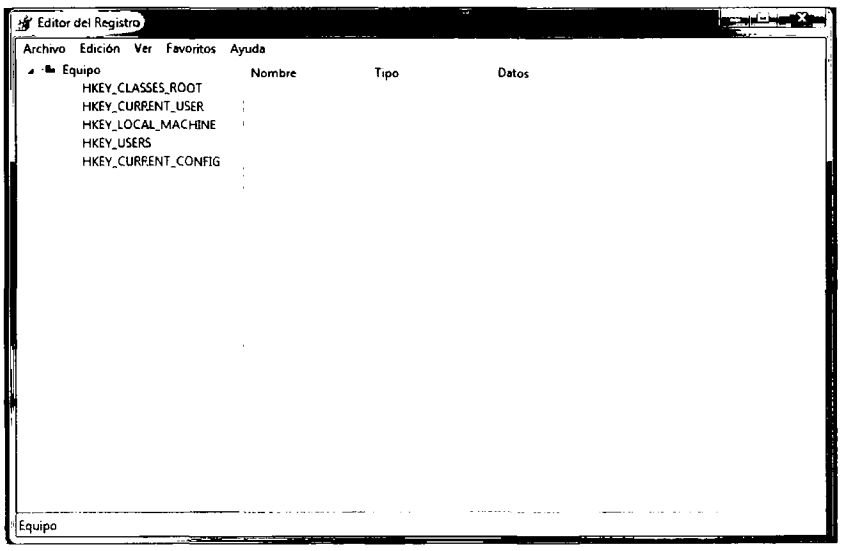
En general se prefiere este tipo de bloqueador, debido a que nos permite seleccionar el tipo de bloqueo a implementar en el equipo elegido.

Para dicha medida, se implementa un bloqueo de los puertos USB en los ordenadores empleados como equipos de laboratorio mediante la implementación de algún software forense. Este programa puede además venir integrado en la herramienta de análisis forense como un aplicativo más.

Esto último, hace en principio que no contaminemos por error el elemento de estudio que se conecta (disco externo, pendrive, etc), impidiendo que quede algún registro de acceso a la prueba, realizando lo que se denomina un acceso de "solo lectura".

Dicho bloqueo de puertos, se realiza de la siguiente manera:

1. Se coloca dichos puertos en modo "Solo Lectura", es decir, al conectar un pendrive USB, podrás acceder a los archivos de este, pero no podrás copiar nada al mismo.
2. Para realizar esto, debo entrar al regedit. Hago clic en "Inicio/Ejecutar", y escribo "regedit". Se debe abrir una ventana tal como la vez abajo.



Una vez que hayamos entrado debemos buscar la siguiente llave:

HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Control/ StorageDevicesPolicies

3. De no existir la llave "StorageDevicesPolicies", podemos crearla a mano, y luego en el lado derecho de la ventana, crear una clave "DWORD", con el nombre "WriteProtect", cuyo valor será "1". La llave WriteProtect la creo haciendo clic derecho en el panel derecho de la ventana, donde aparecerá el menú contextual "Nuevo/Valor DWORD".
4. No se necesita reiniciar. De ahora en adelante siempre que se inserte un pendrive USB, este trabajará como "Solo Lectura". Si se quiere volver al estado anterior, es decir, totalmente libre, se ingresa a la llave que se detalla arriba, "WriteProtect", y se cambia el valor de "1" a "0". Cada vez que se cambien los valores de esta clave se deberá reiniciar, sino no detectará el cambio.

4. Imagen forense y/o Copia espejo

La imagen forense y/o copia espejo, es un duplicado a nivel binario de un medio electrónico de almacenamiento.

En ésta imagen forense quedan resguardados los espacios donde se hallan alojados los archivos y las áreas borradas incluyendo particiones que se hallaren ocultas.

La copia forense guarda suma importancia cuando se desea preservar un elemento en el tiempo para su estudio posterior.

Es en este sentido que cobra interés una ciencia, la criptografía, la cual viene en auxilio de la informática, aportando un elemento fundamental, los algoritmos de hash.

Estos algoritmos de hash, constituyen ni más ni menos que firmas digitales que dan determinados atributos a la prueba: integridad, autenticación y disponibilidad del material a peritar.

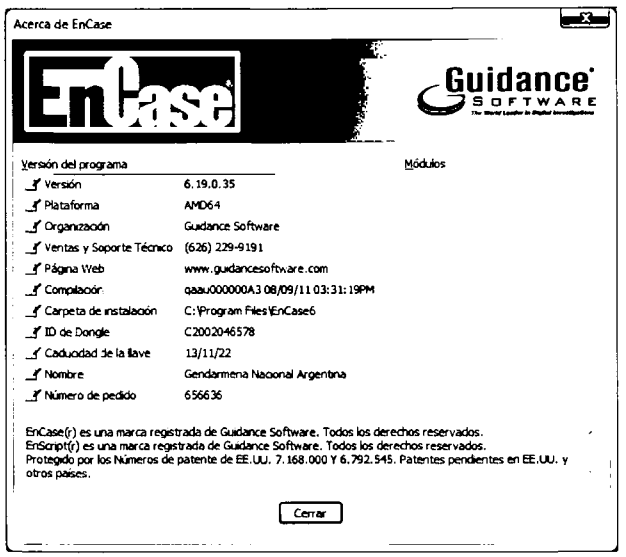
En el presente capítulo se mostrarán TRES (3) casos de adquisición de imágenes forenses, empleando herramientas forenses actuales, desde el momento que se inicia la aplicación hasta que finaliza la copia espejo con su respectivo reporte de resultados.

Los programas seleccionados para tal fin son los siguientes que se detallan a continuación:

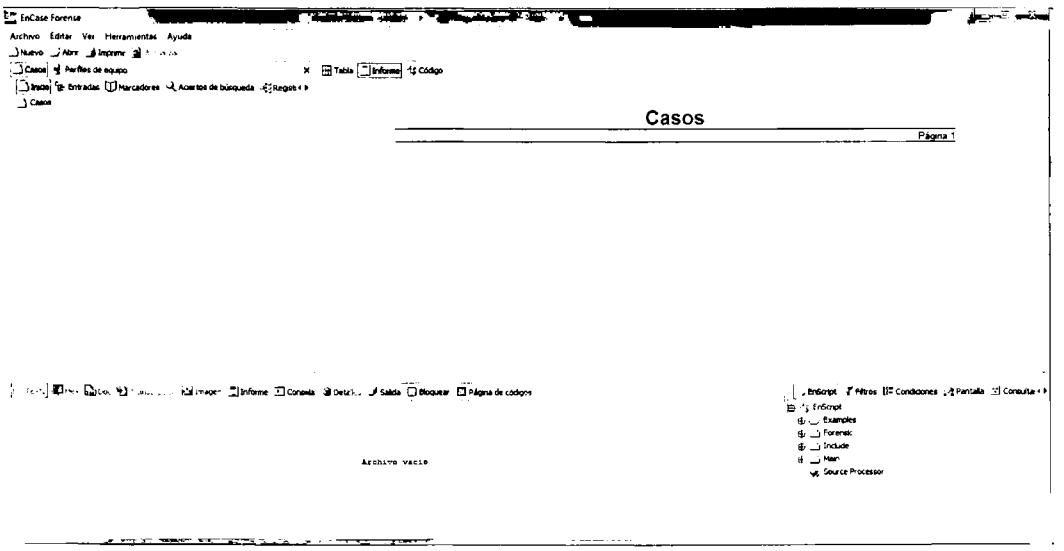
- **Encase V6.19**
- **FTK Imager V3.0.1.1467**
- **DEFT - Guymager**

4.1. Empleando Encase V6.19

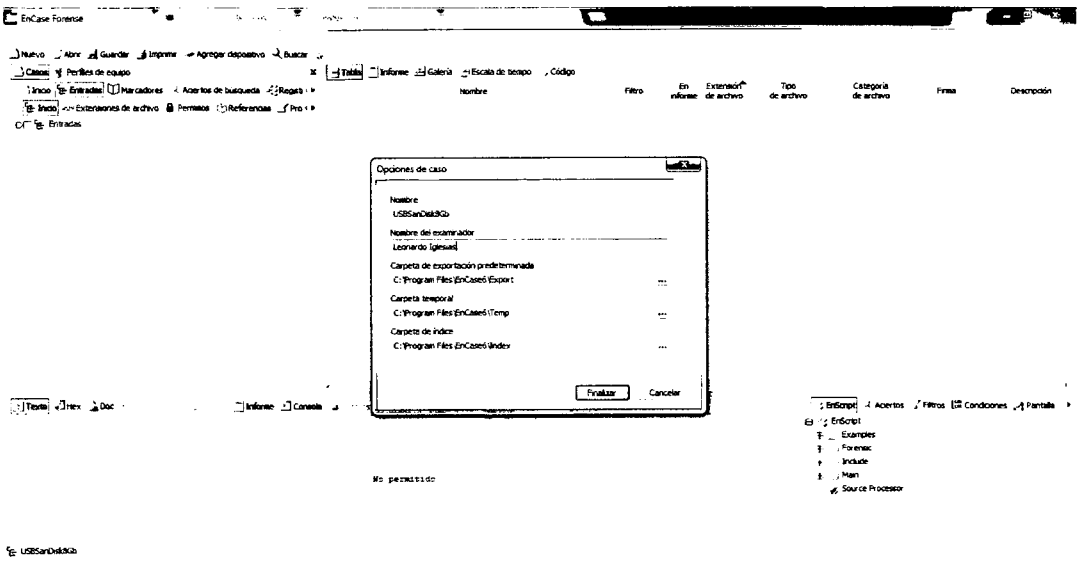
Antes de dar inicio a una investigación y adquisición de dispositivos, debemos seleccionar la herramienta con la que vamos a iniciar la imagen forense o copia espejo. En este caso emplearemos la herramienta ENCASE, cuyos detalles de versión, usuario y demás datos aparecen debajo.



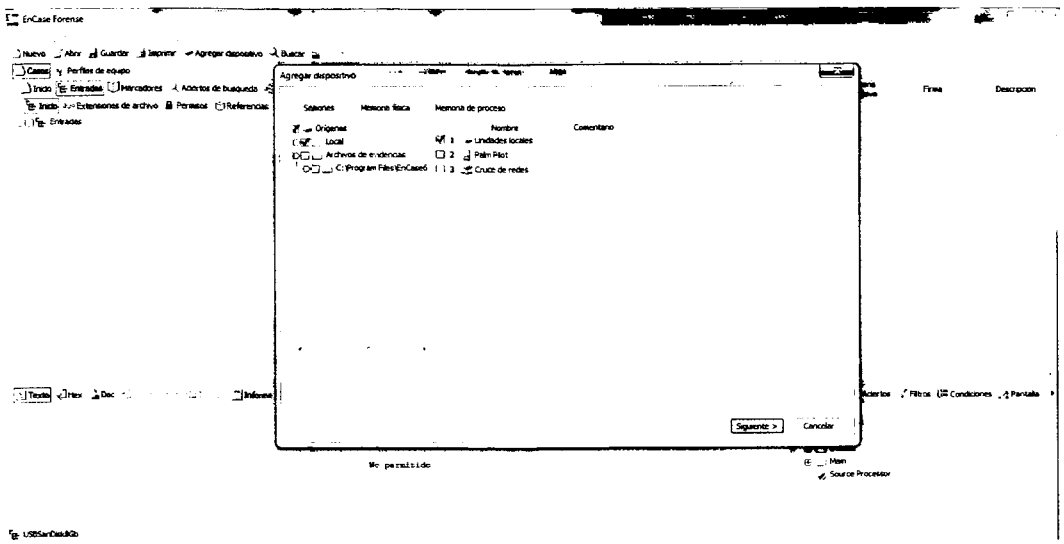
Como primera medida, una vez abierto el programa ENCASE se debe crear un Caso, donde se resguardarán a futuro los archivos de evidencia, para lo que es necesario hacer clic en el botón "Nuevo" del Menu.



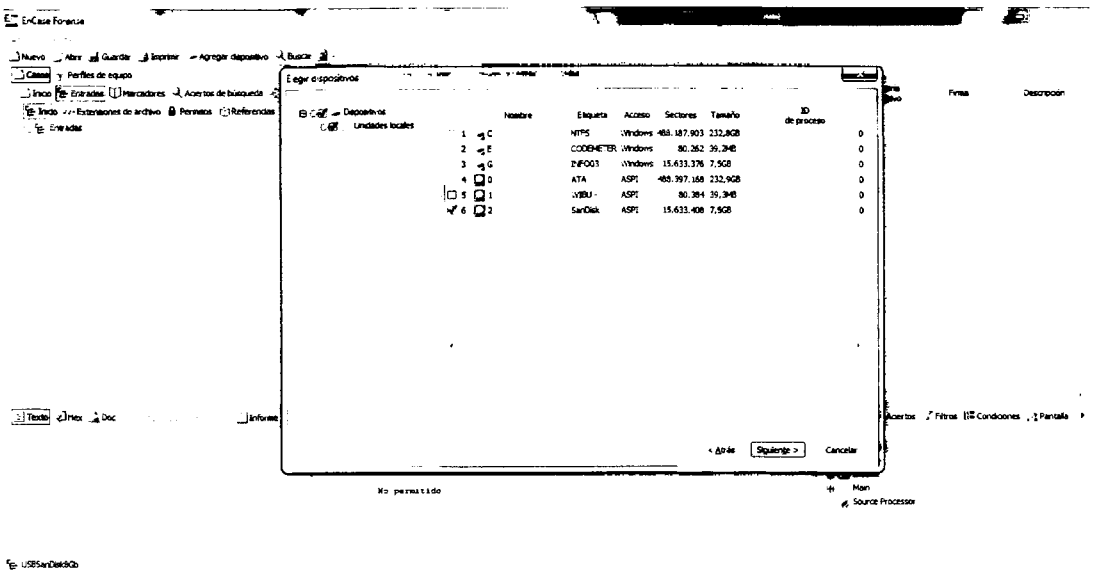
La ventana que continúa, solicita cierta información sobre el examinador y el caso en cuestión (Perito, causa, caratula, etc). Una vez completado el mismo se debe dar clic en "Finalizar".



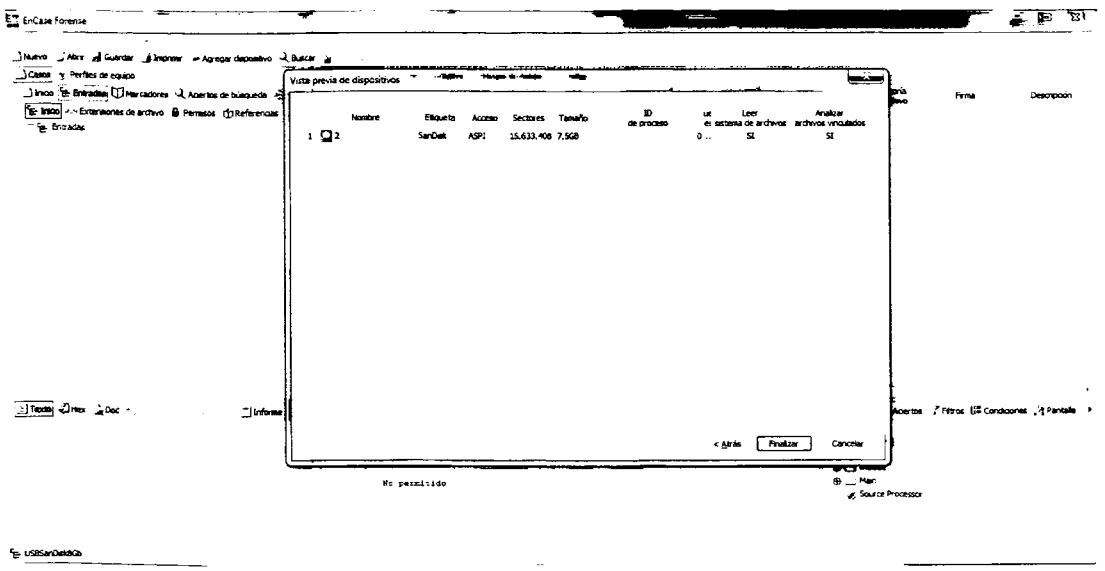
Una nueva ventana muestra un menú, en el cual se debe seleccionar el tipo de Unidad Fuente que agregaremos al caso (disco en cuestión), para luego hacer clic en el botón "Siguiente".



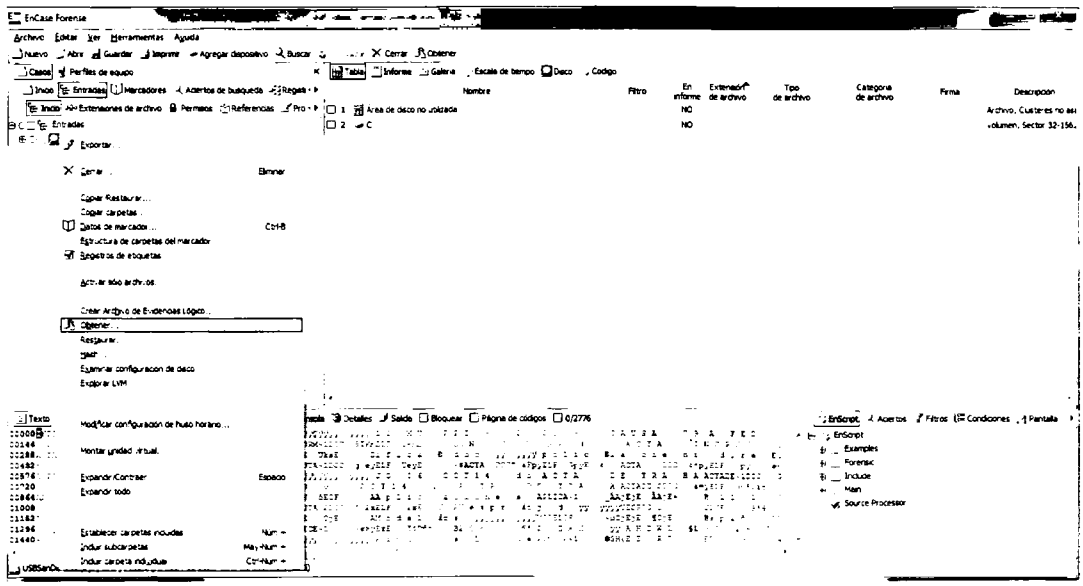
A continuación se aprecian las unidades disponibles, en el cual se agrega al Caso la Unidad Fuente propiamente dicha, para luego hacer clic en el botón "Siguiente".



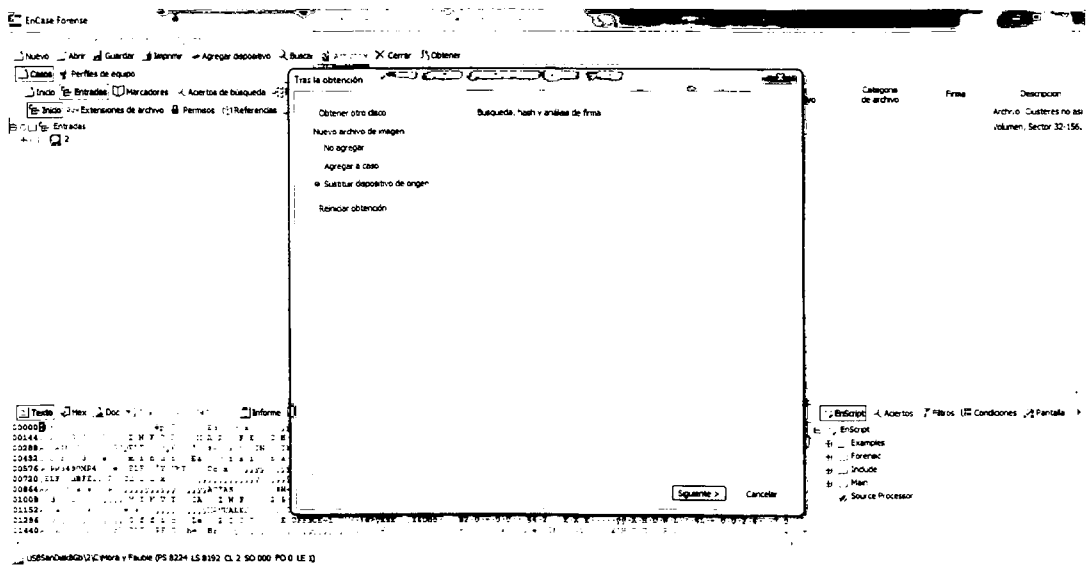
Acto seguido se muestran las propiedades de la Unidad seleccionada. Para terminar de agregar la misma al Caso, se debe hacer clic en el botón "Finalizar".



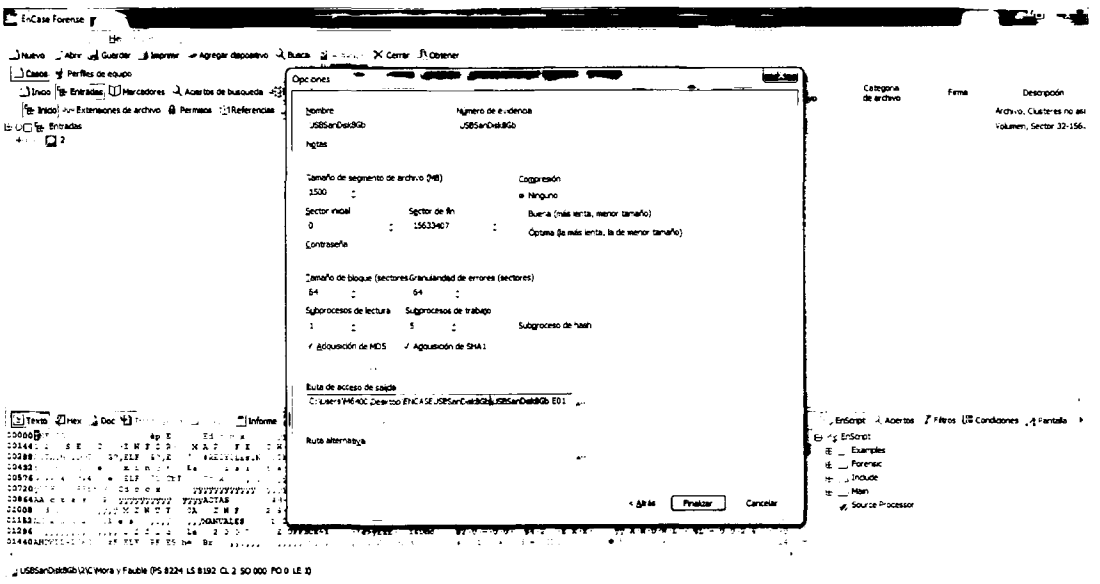
Una vez agregada la evidencia al Caso, para comenzar con el procedimiento de obtención de la Imagen Forense se debe hacer clic con el botón derecho sobre la Unidad y a partir del menú desplegable seleccionamos la opción "Obtener".



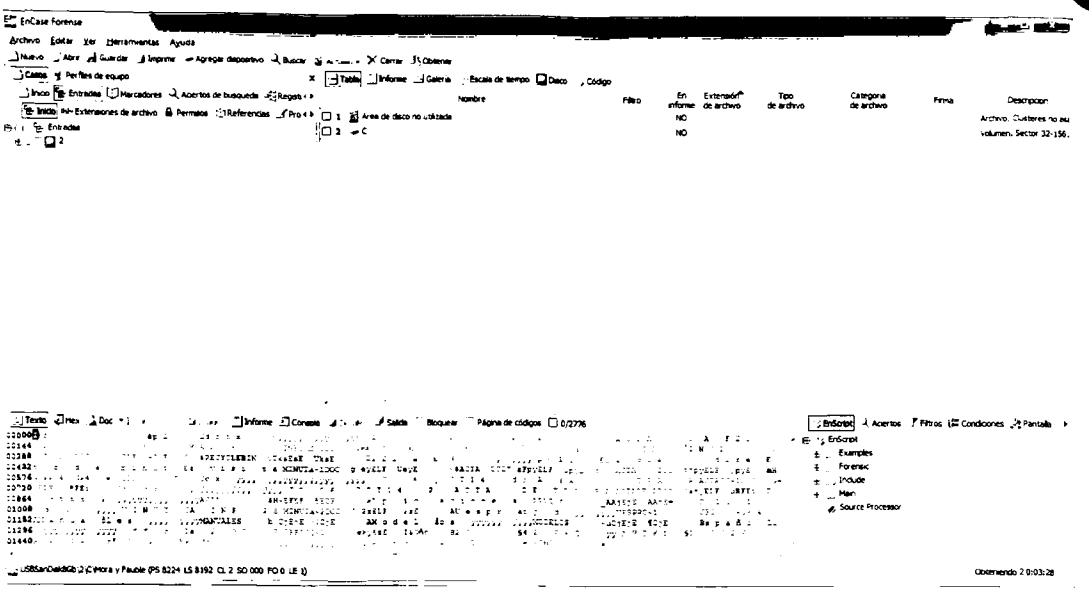
Se abre una nueva ventana donde se requiere definir si se obtendrá una nueva imagen desde otro dispositivo o si la imagen forense creada será agregada o no al caso, o sustituirá el dispositivo de origen, como lo es el caso para la presente prueba de concepto. Luego hacer clic en el botón "Siguiente".



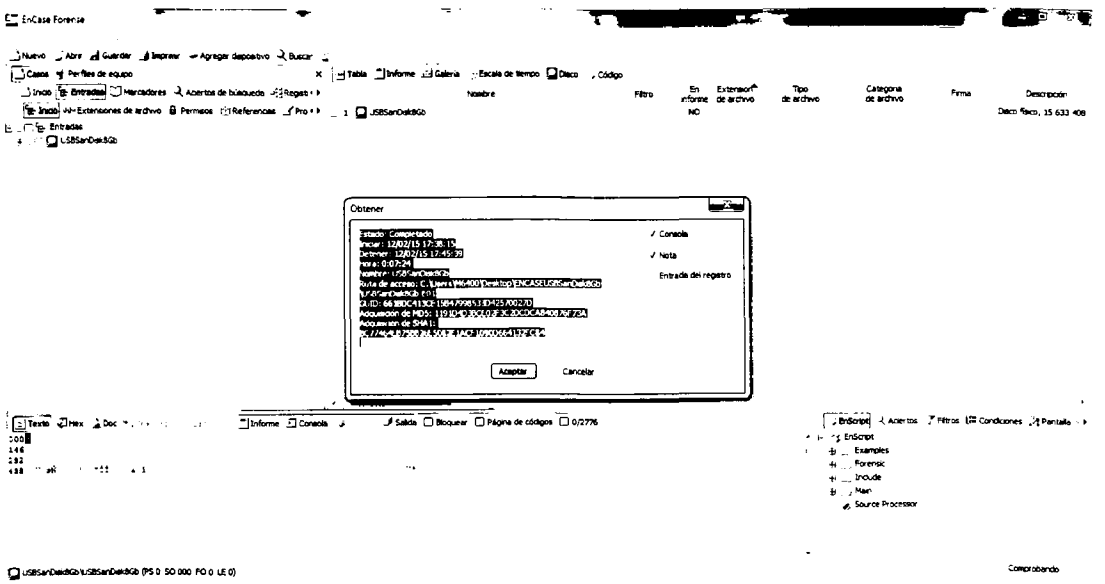
La ventana que continúa solicita cierta información sobre la evidencia, procediendo a nombrarse la misma (USBSanDisk8Gb). Además se puede definir si la imagen resultante será realizada en un archivo único o dividida en fragmentos. Para el presente caso la misma será divida, por lo tanto se define el valor "1500" en el campo "Tamaño de segmento de archivo". Por otro lado, se puede establecer el formato de "Compresión" de la imagen obtenida, para el presente caso no se escogerá por comprimir la imagen. Para finalizar se debe seleccionar el destino de la Imagen, siendo necesario seleccionar el campo "Ruta de acceso de salida" y hacer clic en el botón "...".A continuación se debe hacer clic en el botón "Finalizar".



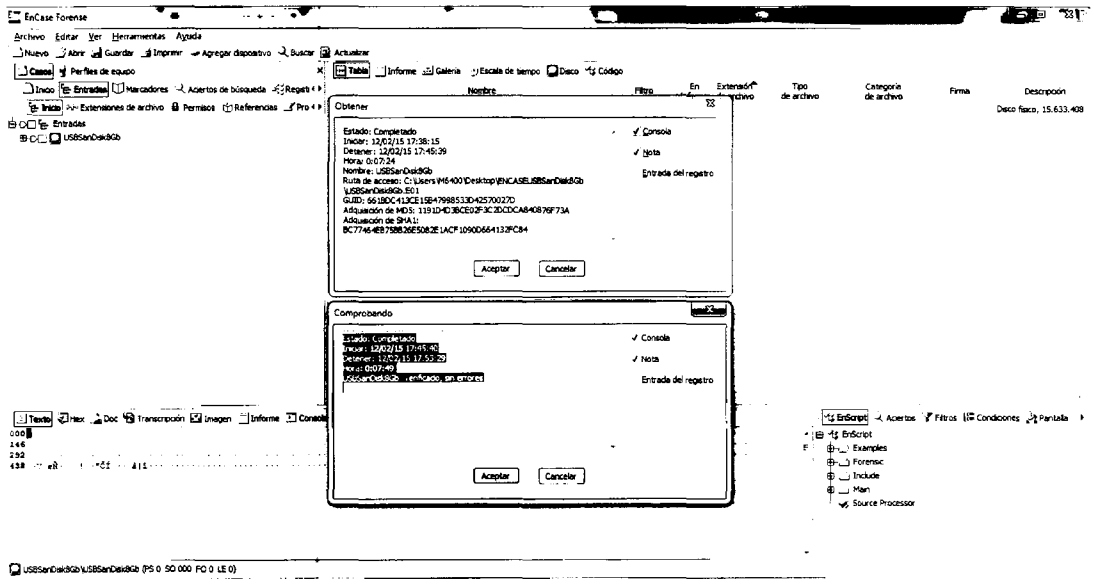
El proceso de creación de la imagen forense desde el disco rígido, unidad USB o MemoryStick iniciará al hacer clic en el botón "Finalizar", apreciándose una barra de estado en el margen inferior derecho de la pantalla.



Una vez finalizada la obtención de la imagen forense se presenta un reporte, en el mismo se aprecian el número GUID de la evidencia y los algoritmos de seguridad Hash MD5 y SHA-1. Al mismo tiempo que se inicia de forma automática la verificación correspondiente.

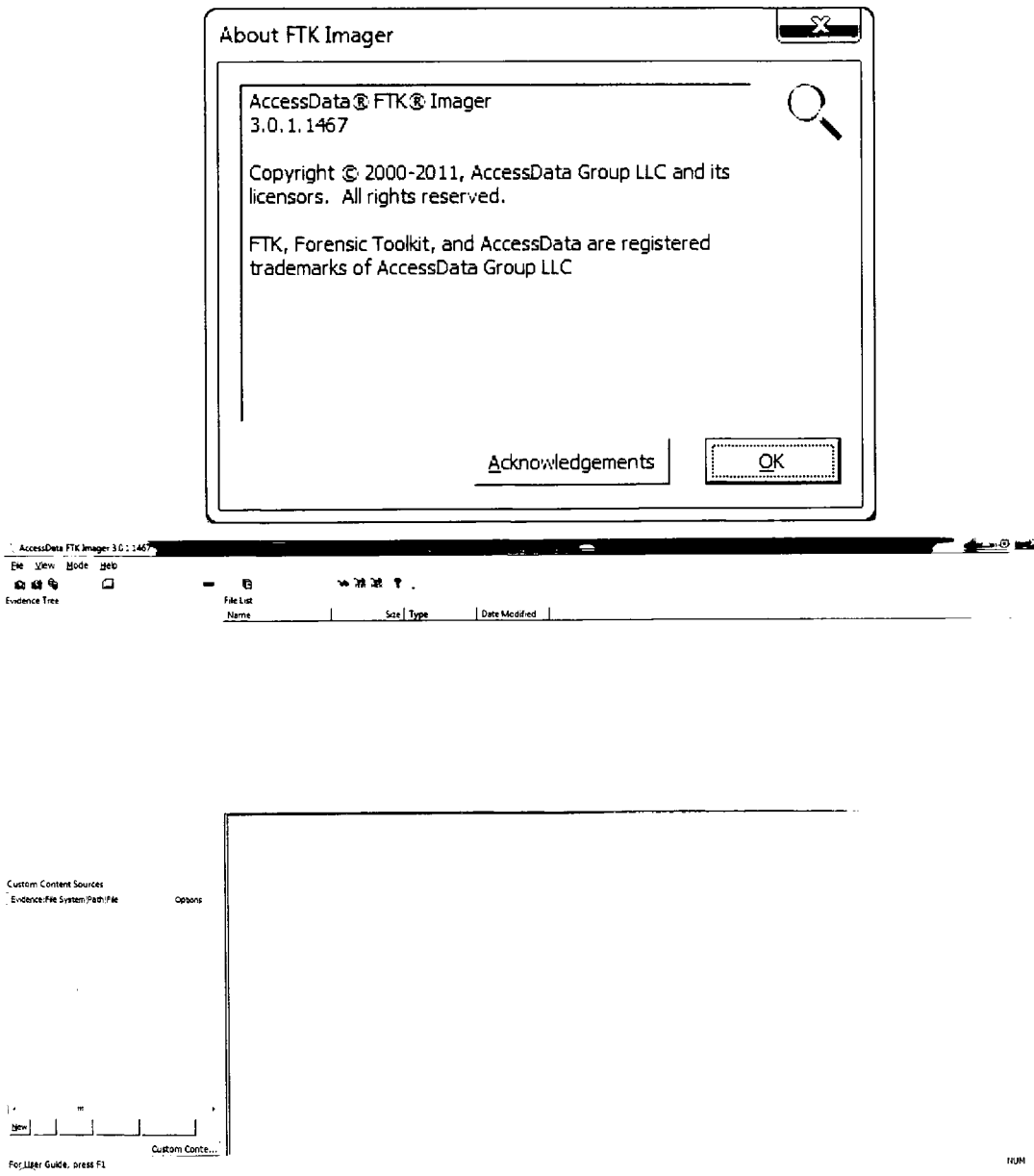


Una vez finalizada la comprobación de la imagen forense se presenta un reporte. En el mismo se aprecia el estado del proceso, la fecha y hora de inicio y finalización, el tiempo transcurrido y la verificación del disco.

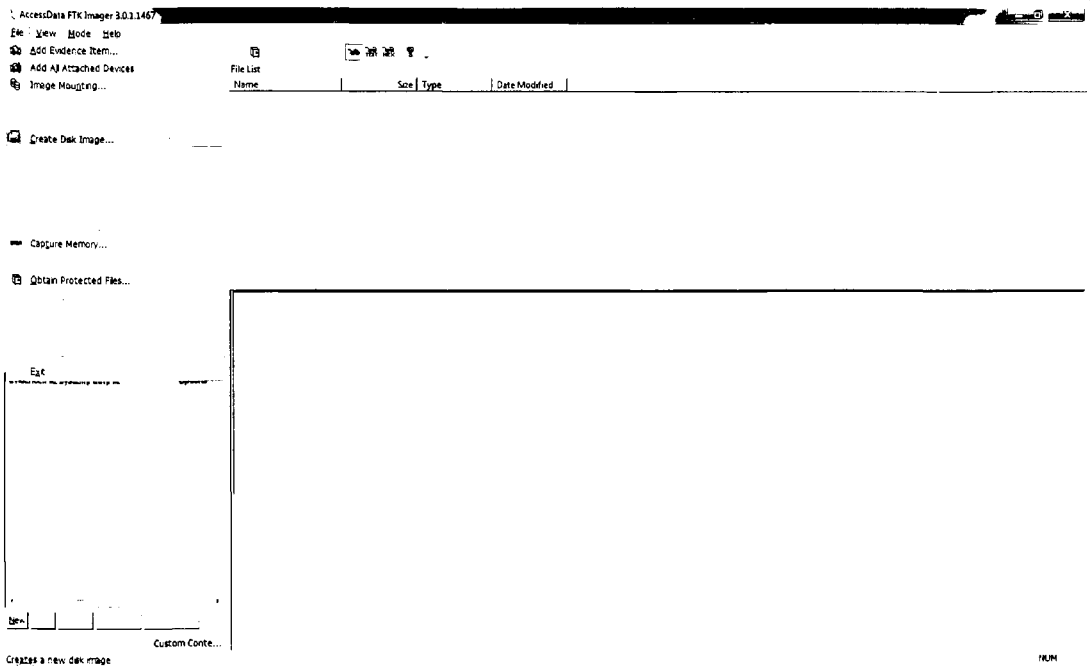

EnCase Forense
Archivo Editar Ver Herramientas Ayuda
Obtener
Estado: Completado
Iniciar: 12/02/15 17:38:15
Detener: 12/02/15 17:45:39
Hora: 0:07:24
Nombre: USBSanDisk8Gb
Ruta de acceso: C:\Users\M6400\Desktop\ENCASE\USBSanDisk8Gb\USBSanDisk8Gb.E01
GUID: 661BDC413CE15B47988533D42570027D
Adquisición de MD5: 1191D4D3BCE02F3C3DCDCA840876F73A
Adquisición de SHA1:
BC7746 4EB758B26E50B2E1ACF1090D664132FC84
Consola
Nota
Entrada del registro
Aceptar
Cancelar
Comprobando
Estado: Completado
Iniciar: 12/02/15 17:45:40
Detener: 12/02/15 17:53:29
Hora: 0:07:49
USBSanDisk8Gb: verificado sin errores
Consola
Nota
Entrada del registro
Aceptar
Cancelar
EnScript
Examples
Forensic
Include
Main
Source Processor
USBSanDisk8Gb\USBSanDisk8Gb (PS 0 SO 000 FO 0 LE 0)

4.2. Empleando FTK Imager V3.0.1.1467

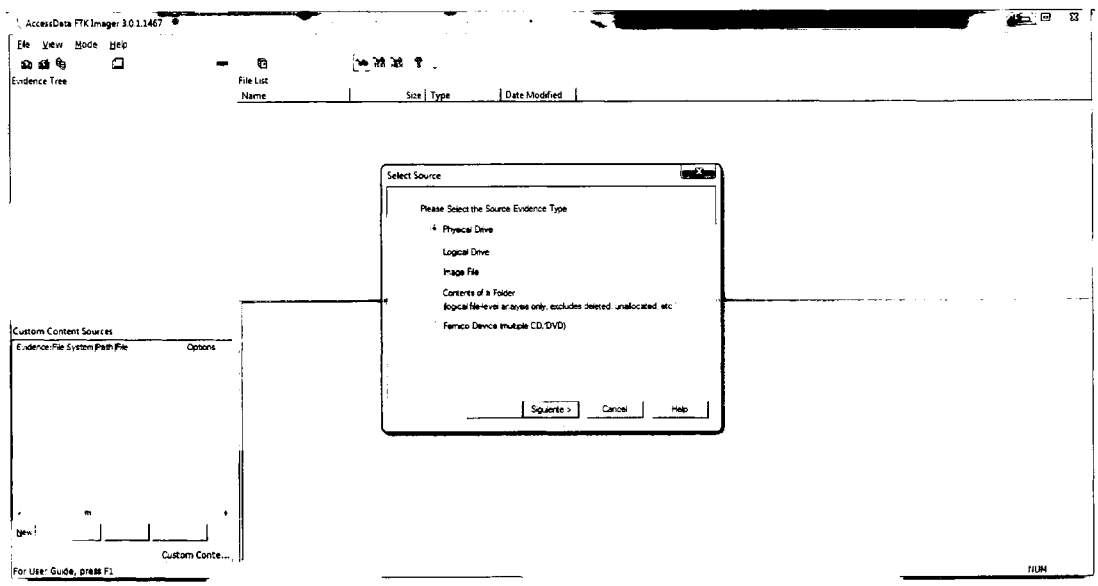
La herramienta FTK Imager, a diferencia del software Encase, presenta menos opciones de menú, siendo una opción directa de generación de una imagen forense y de posterior visualización.



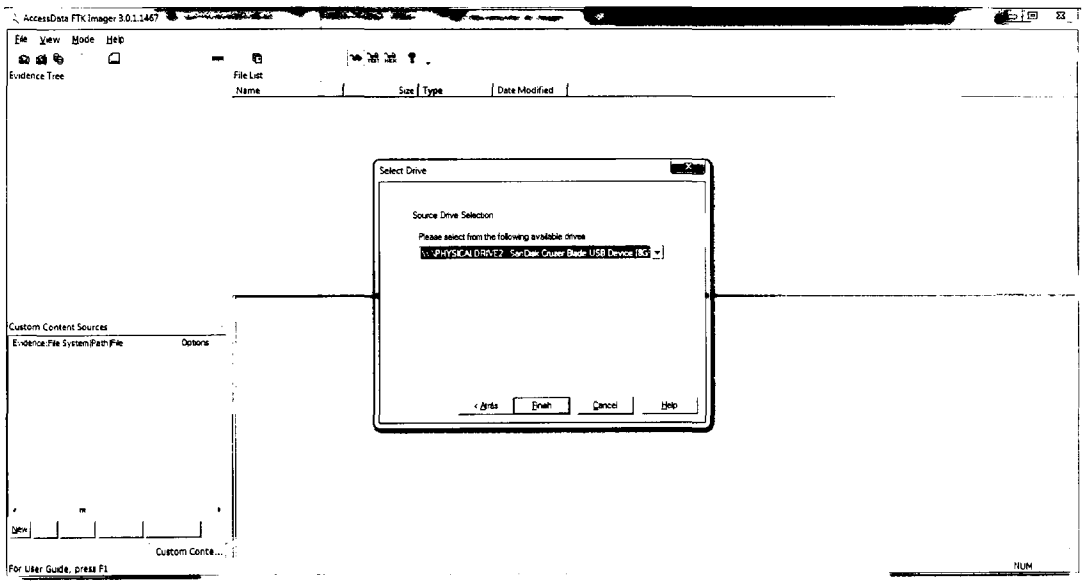
Como primera medida, una vez inicializado el programa, debemos hacer clic en la opción "File ->Create Disk Image" o Archivo -> Crear Imagen de Disco.



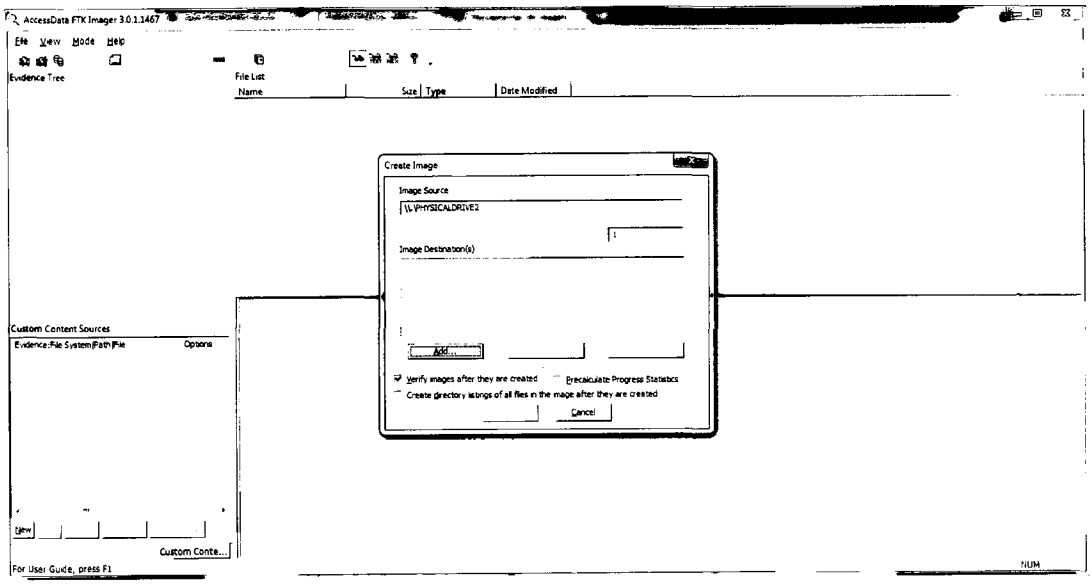
Se abre una nueva ventana donde se requiere definir la Fuente. Para el presente caso, la opción permite crear una imagen forense de un disco rígido, una unidad USB o una MemoryStick, por lo tanto se selecciona la opción "Physical Drive" o Unidad Física. Luego se debe hacer clic en el botón "Siguiente".



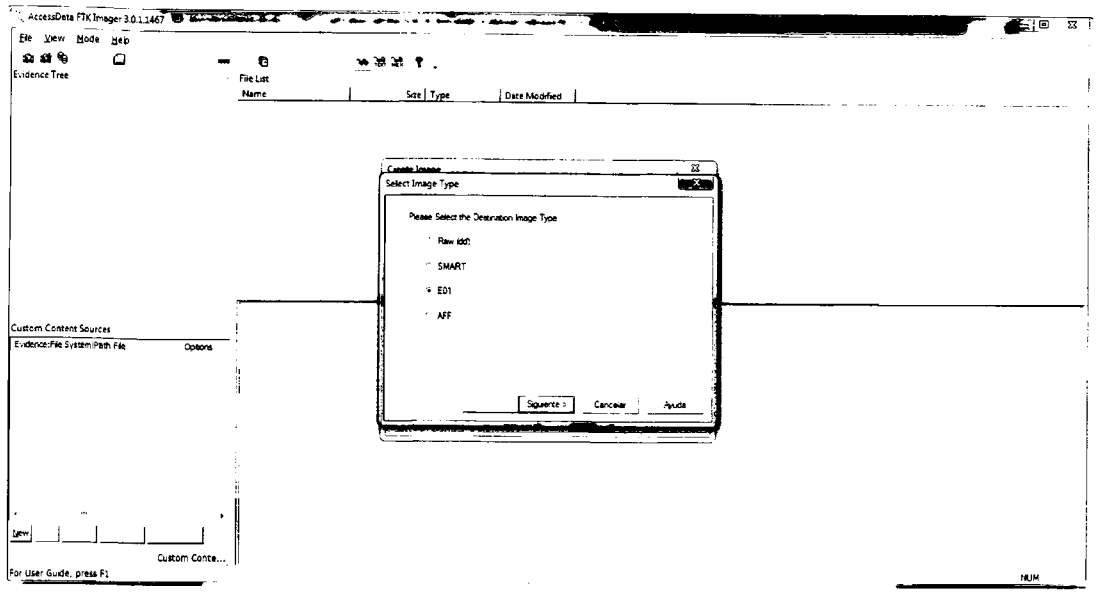
Una nueva ventana muestra un menú, en el cual se selecciona la Unidad Fuente correspondiente, para luego hacer clic en el botón "Finish" o Finalizar.



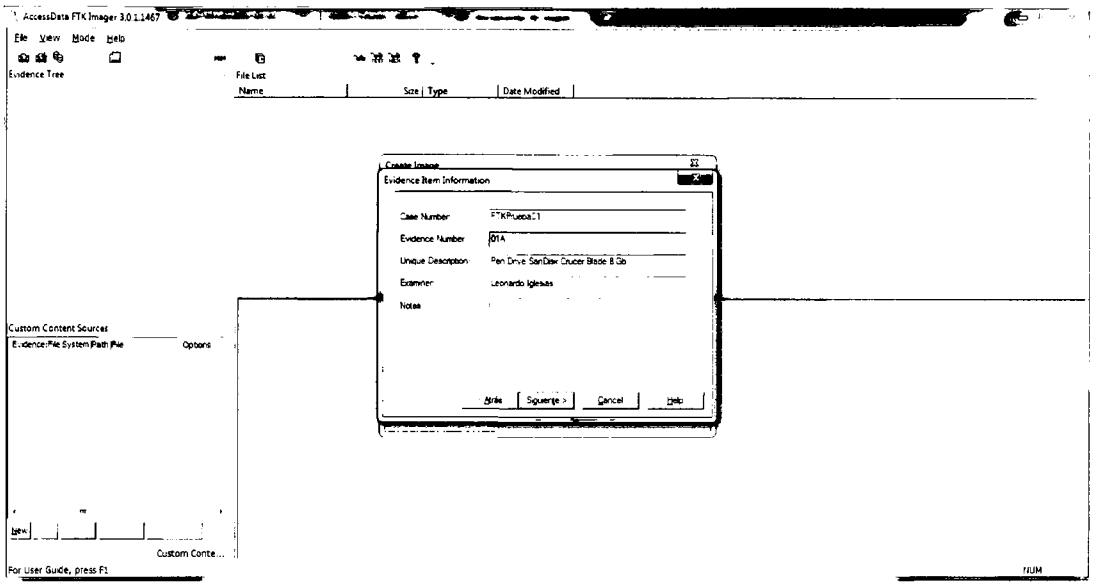
En la siguiente ventana se debe seleccionar el destino de la Imagen, siendo necesario hacer clic en el botón "Add..."



En la ventana posterior se define el "tipo" de la imagen a crear. Para el caso de la presente práctica será una imagen de extensión "E01", es decir tal y como sería creada utilizando una herramienta Encase.

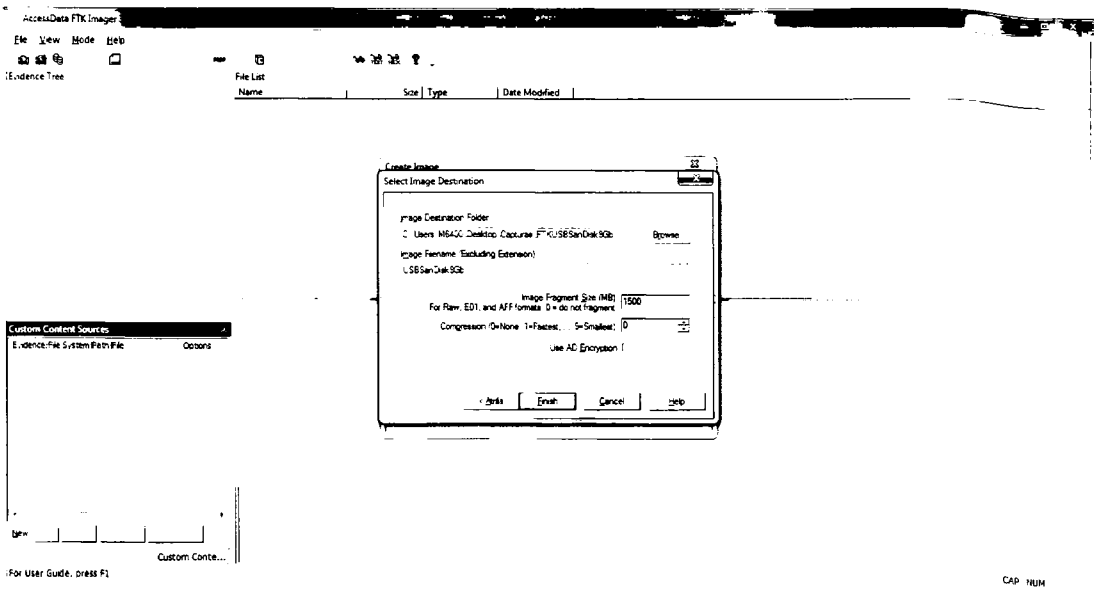


La ventana que continúa solicita información sobre la evidencia, que tras ser completada debemos hacer clic en el botón "Siguiente".

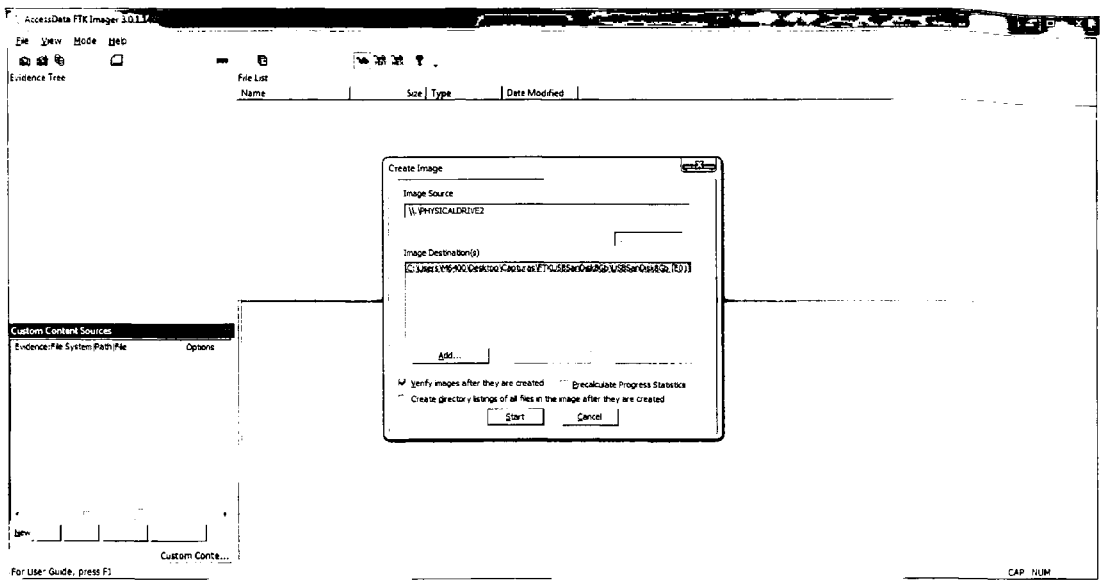


A continuación se debe definir la carpeta donde se almacenará la imagen forense, la cual es seleccionada haciendo clic en el botón "Browse" o Navegar. Seguidamente se debe nombrar la imagen forense (USBSanDisk8Gb). Y opcionalmente definir si la imagen resultante será realizada en un archivo único o dividida en fragmentos. Para el presente

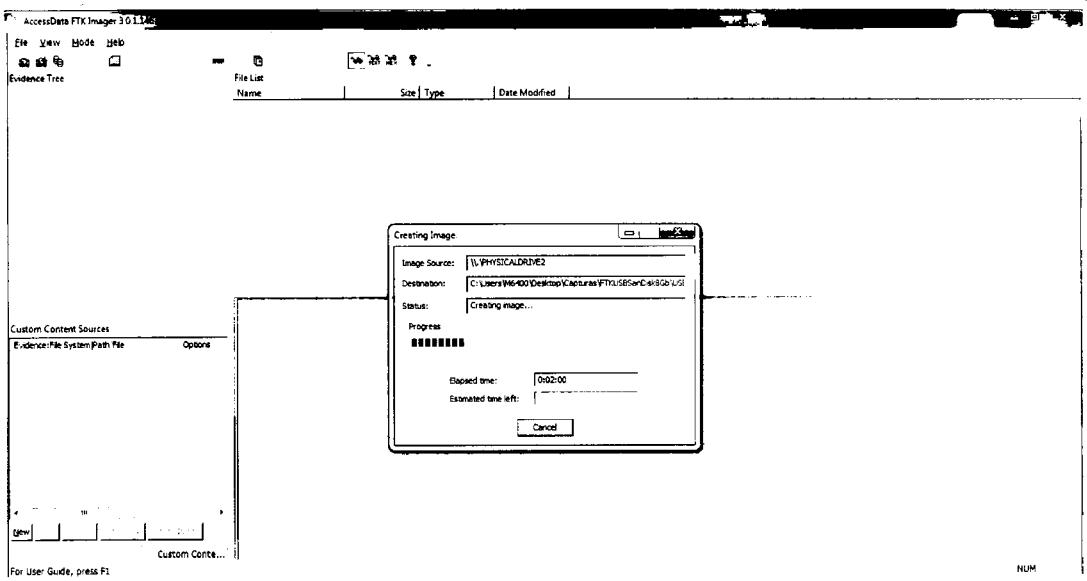
caso la misma será divida, por lo tanto se define el valor "1500" en el campo "ImageFragmentSize (MB)" o Tamaño del Fragmento de la Imagen.



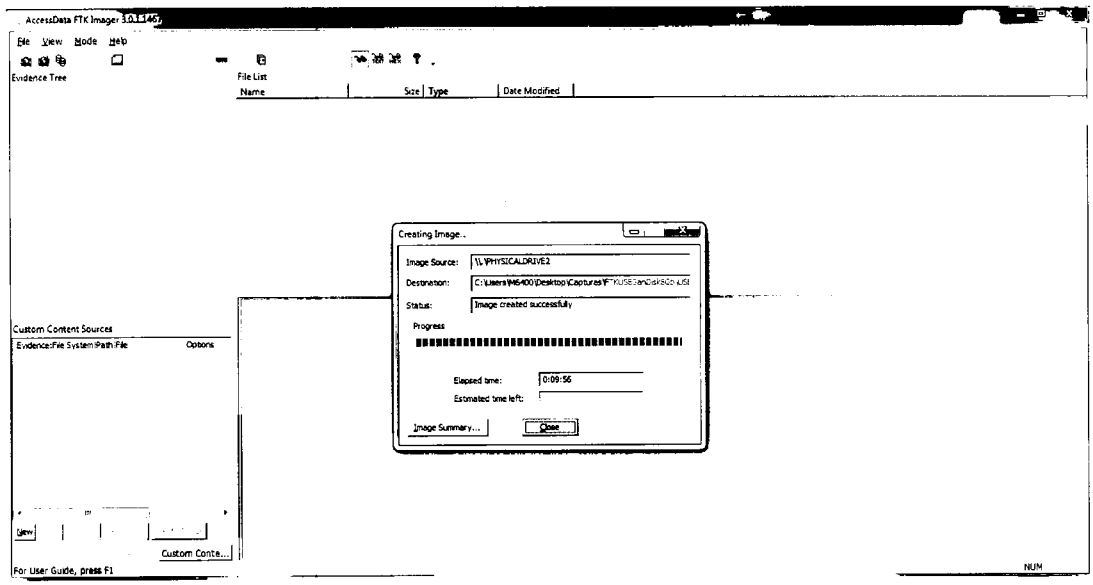
Al Hacer clic en el botón "Finish", se mostrará un resumen de las opciones seleccionadas.

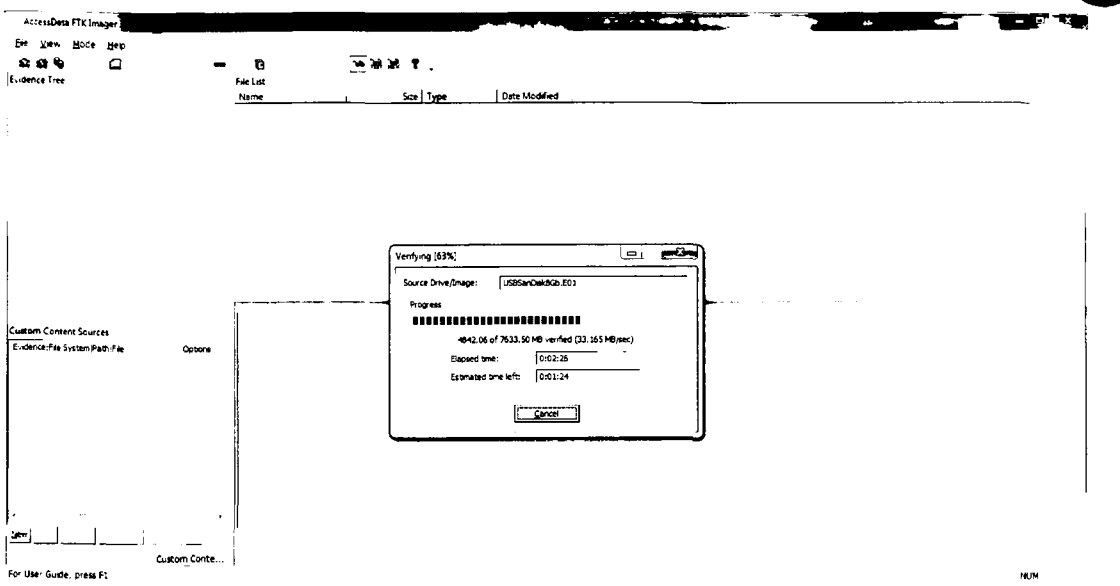


El proceso de creación de la imagen forense desde el disco rígido, unidad USB o MemoryStick iniciará al hacer clic en el botón "Start" o Iniciar.

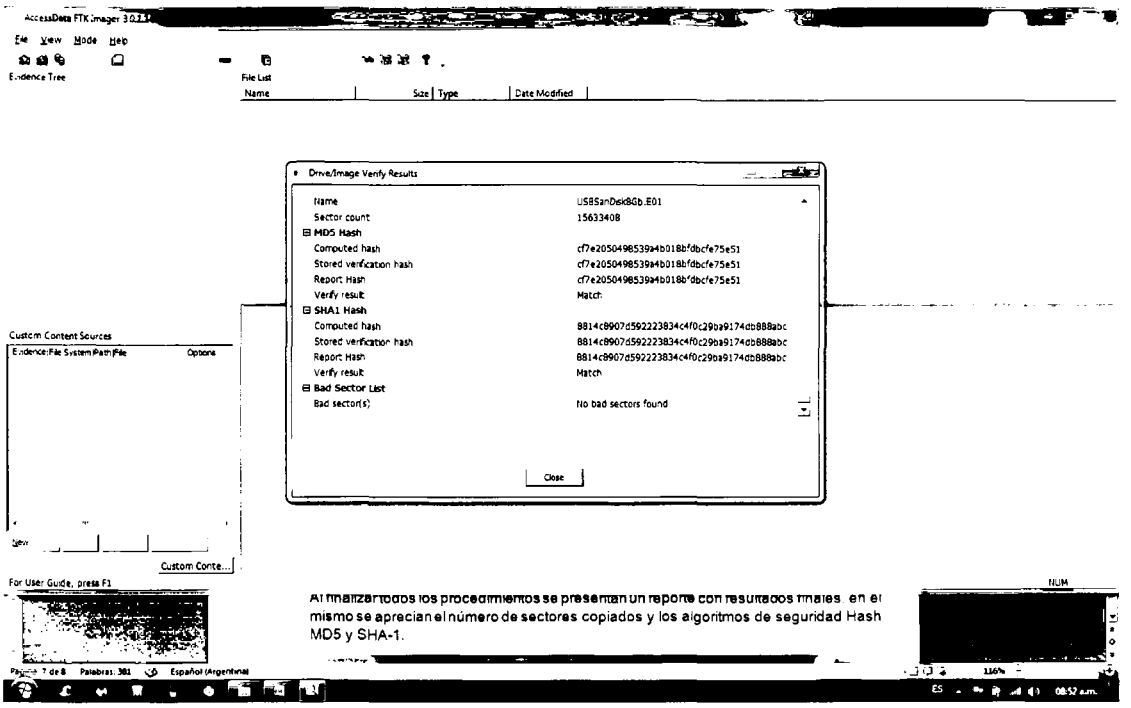


Una vez finalizada la obtención de la imagen forense, se inicia la verificación correspondiente.

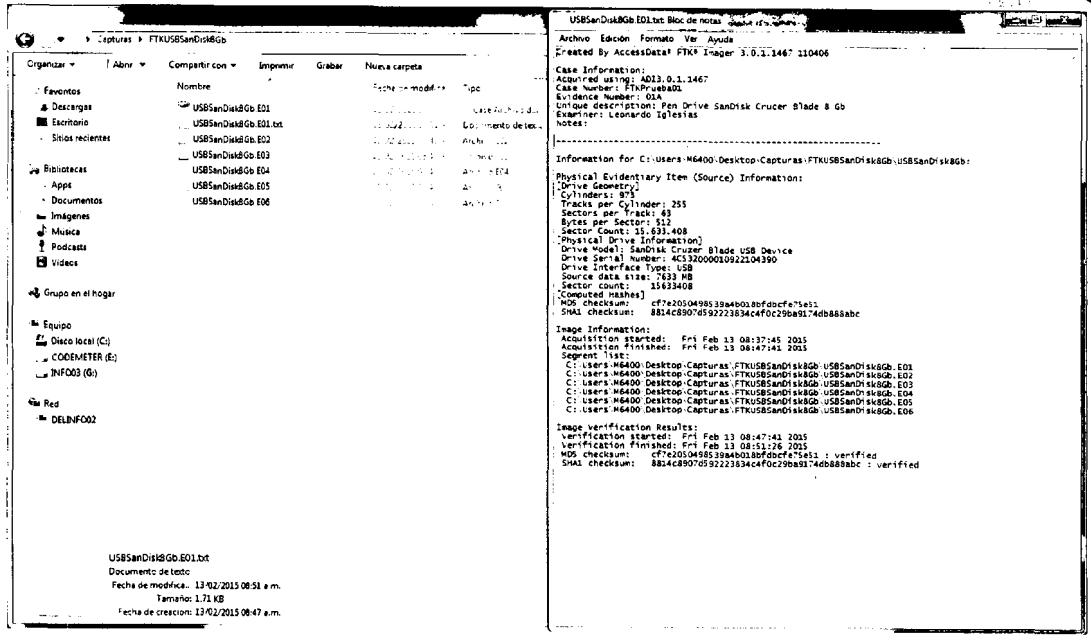




Al finalizar todos los procedimientos se presenta un reporte con resultados finales, en el mismo se aprecian el número de sectores copiados y los algoritmos de seguridad Hash MD5 y SHA-1.



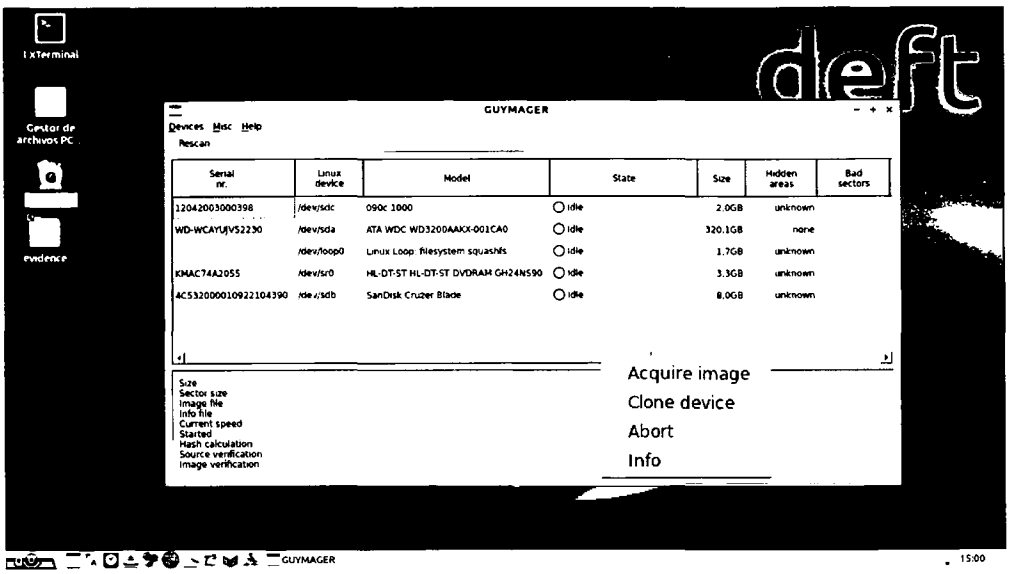
En el mismo directorio o unidad donde se creó la imagen forense, encontraremos un archivo de texto con el mismo nombre de la imagen forense obtenida (USBSanDisk8Gb.E01.txt), en el cual se encuentra disponible toda la información detallada anteriormente.


Capturas ▸ FTKUSBSanDisk8Gb
Organizar
Abrir
Compartir con
Imprimir
Grabar
Nueva carpeta
Favoritos
Descargas
Escritorio
Sitios recientes
Bibliotecas
Apps
Documentos
Imágenes
Música
Podcasts
Videos
Grupo en el hogar
Equipo
Disco local (C:)
CODEMETER (E:)
INFO03 (G:)
Red
DELINFO02
Nombre
Tipo
USBSanDisk8Gb.E01
USBSanDisk8Gb.E01.txt
Documento de tex...
USBSanDisk8Gb.E02
USBSanDisk8Gb.E03
USBSanDisk8Gb.E04
USBSanDisk8Gb.E05
USBSanDisk8Gb.E06
USBSanDisk8Gb.E01.txt
Documento de texto
Fecha de modifica... 13/02/2015 08:51 a.m.
Tamaño: 1.71 KB
Fecha de creación: 13/02/2015 08:47 a.m.
USBSanDisk8Gb.E01.txt: Bloc de notas
Archivo Edición Formato Ver Ayuda
Created By AccessData® FTK® Imager 3.0.1.1467 110406
Case Information:
Acquired using: AD13.0.1.1467
Case Number: FTKPruebaDD
Evidence Number: 01A
Unique description: Pen Drive SanDisk Crucer Blade 8 Gb
Examiner: Leonardo Iglesias
Notes:
Information for C:\Users\M6400\Desktop\Capturas\FTKUSBSanDisk8Gb\USBSanDisk8Gb:
Physical Evidentiary Item (Source) Information:
[Drive Geometry]
Cylinders: 975
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 15,631,408
[Physical Drive Information]
Drive Model: SanDisk Cruzer Blade USB Device
Drive Serial Number: 4C532000010922104390
Drive Interface Type: USB
Source data size: 7633 MB
Sector count: 15631408
[Computed Hashes]
MD5 checksum: cf7e2050498539a4b018bfdbcfe75e51
SHA1 checksum: 8814c8907d592223834c4f0c29ba9174db888abc
Image Information:
Acquisition started: Fri Feb 13 08:37:45 2015
Acquisition finished: Fri Feb 13 08:47:41 2015
Segment list:
C:\Users\M6400\Desktop\Capturas\FTKUSBSanDisk8Gb\USBSanDisk8Gb.E01
C:\Users\M6400\Desktop\Capturas\FTKUSBSanDisk8Gb\USBSanDisk8Gb.E02
C:\Users\M6400\Desktop\Capturas\FTKUSBSanDisk8Gb\USBSanDisk8Gb.E03
C:\Users\M6400\Desktop\Capturas\FTKUSBSanDisk8Gb\USBSanDisk8Gb.E04
C:\Users\M6400\Desktop\Capturas\FTKUSBSanDisk8Gb\USBSanDisk8Gb.E05
C:\Users\M6400\Desktop\Capturas\FTKUSBSanDisk8Gb\USBSanDisk8Gb.E06
Image Verification Results:
Verification started: Fri Feb 13 08:47:41 2015
Verification finished: Fri Feb 13 08:51:26 2015
MD5 checksum: cf7e2050498539a4b018bfdbcfe75e51 : verified
SHA1 checksum: 8814c8907d592223834c4f0c29ba9174db888abc : verified

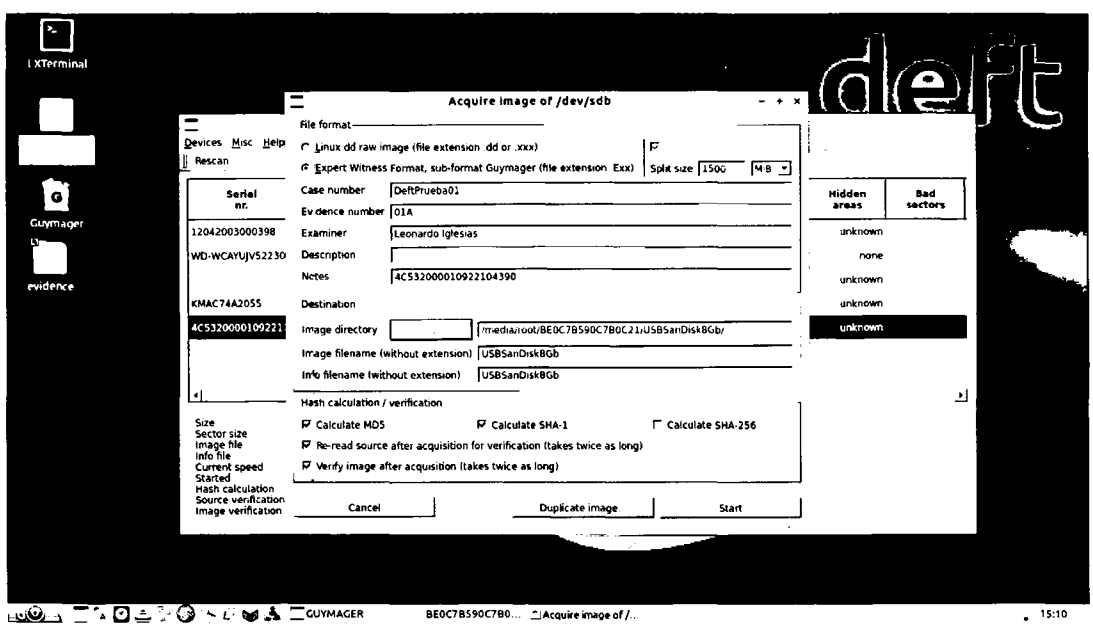
4.3. Empleando DEFT – Guymager

Antes de iniciar, es de destacar que la distribución de Linux basada en Ubuntu denominada DEFT, se haya constituida por un conjunto de herramientas forenses. Una de estas herramientas la constituye "Guymager" que se haya en el escritorio.

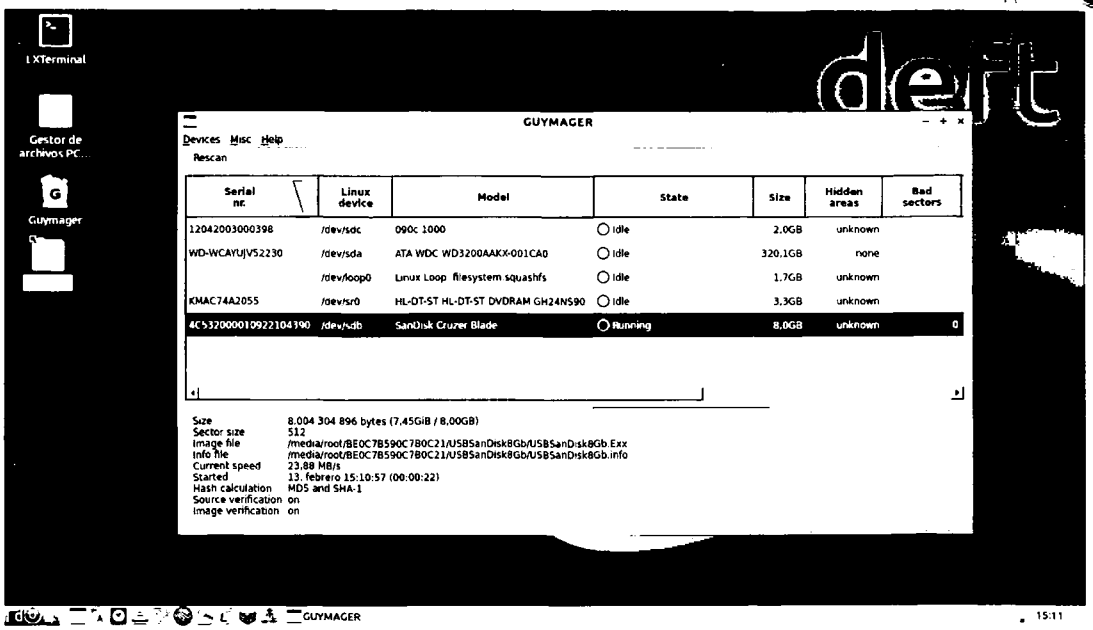
Al hacer click sobre el icono de la misma, se abre la ventana de la aplicación, a partir de la cual se debe seleccionar la Fuente desde dónde se creará la imagen forense. Posteriormente, se despliega un menú donde se debe hacer clic en "Acquire image" (Adquirir imagen).



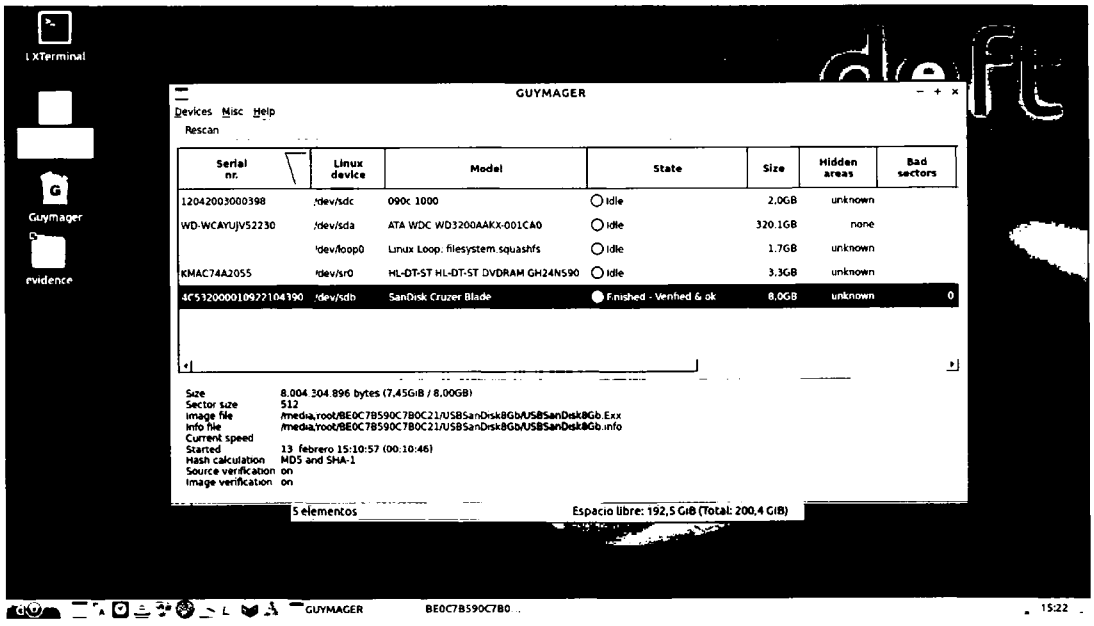
En la ventana siguiente se define el "tipo" de imagen a crear, siendo para el presente caso el formato "E01", tal como sería mediante la herramienta Encase. Asimismo se debe aportar información sobre el caso, definir la carpeta donde se almacenará la imagen, la cual es seleccionada haciendo clic en el botón "..." de la opción "Imagedirectory" (Directorio de la imagen). Se debe nombrar la imagen forense (USBSanDisk8Gb) y definir si la imagen resultante será realizada en un archivo único o dividida en fragmentos, la que para este caso será divida y se define el valor "1500" en el campo "Split size" (MB) (Tamaño de la división). Se deben seleccionar los algoritmos de seguridad Hash MD5 y SHA-1. Para iniciar la obtención de la imagen se debe hacer clic en "Start" (Iniciar).



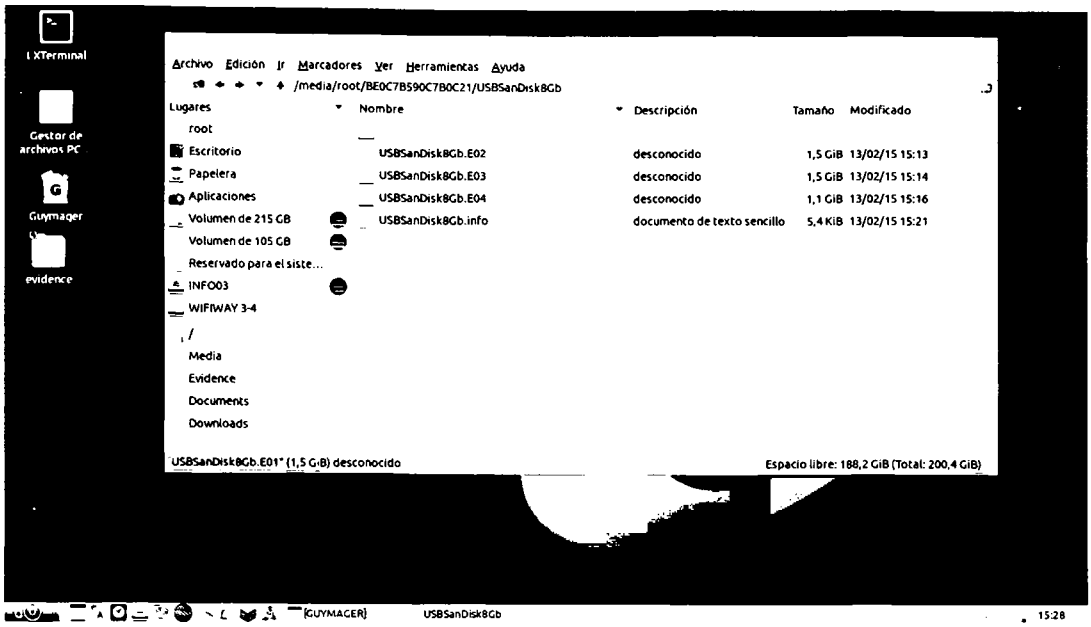
En la ventana de la aplicación se aprecia que el proceso se encuentra en ejecución.



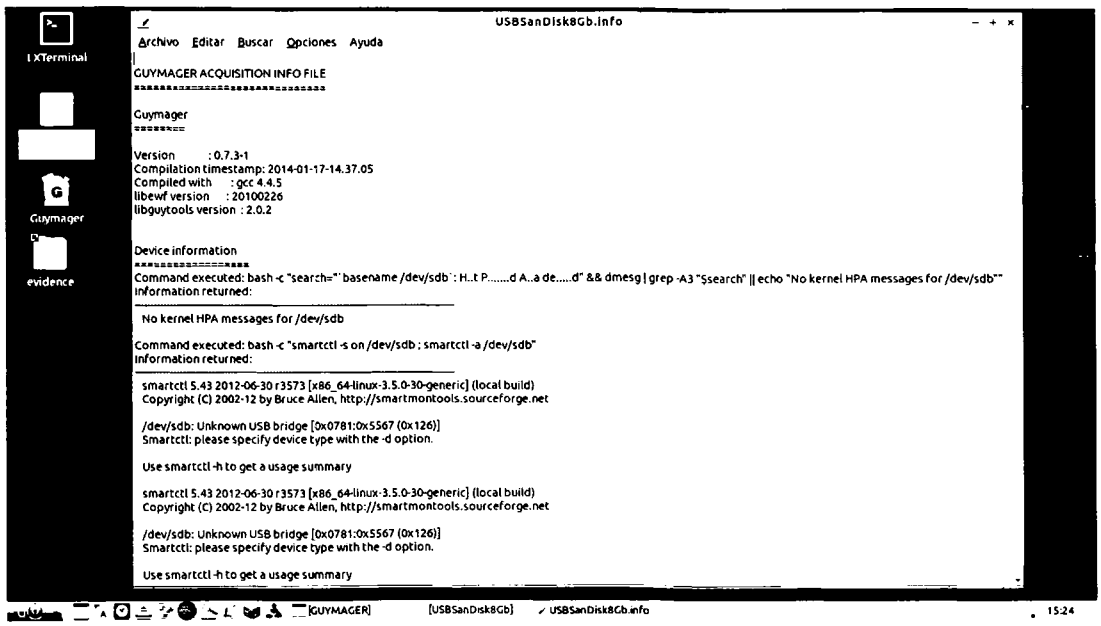
Una vez culminada la obtención de la imagen forense, en la ventana de la aplicación se aprecia que el proceso se encuentra finalizado.

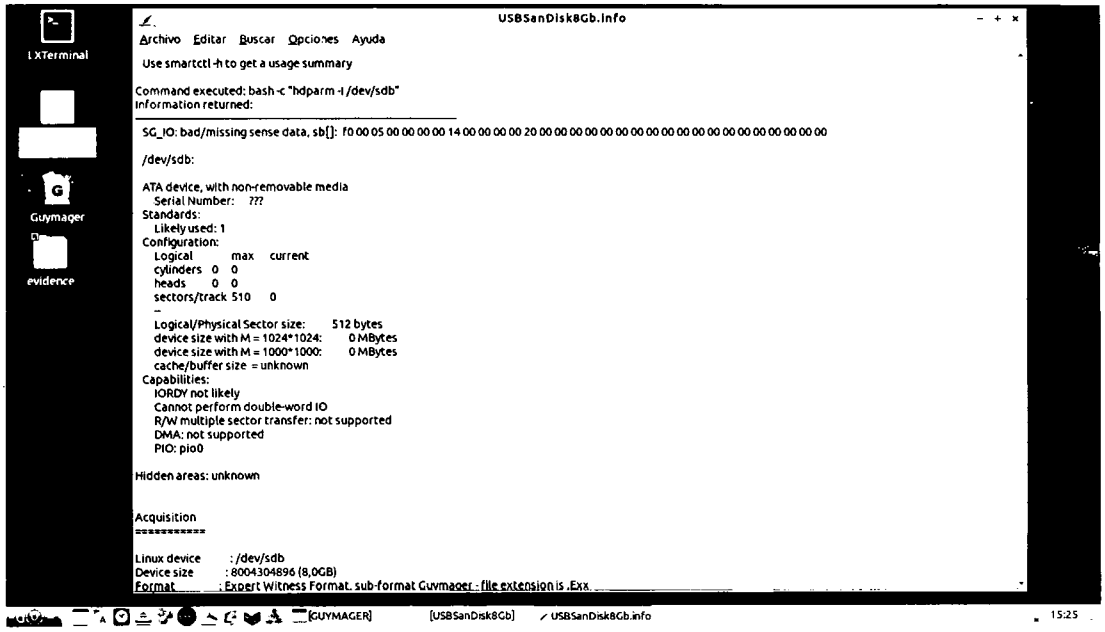


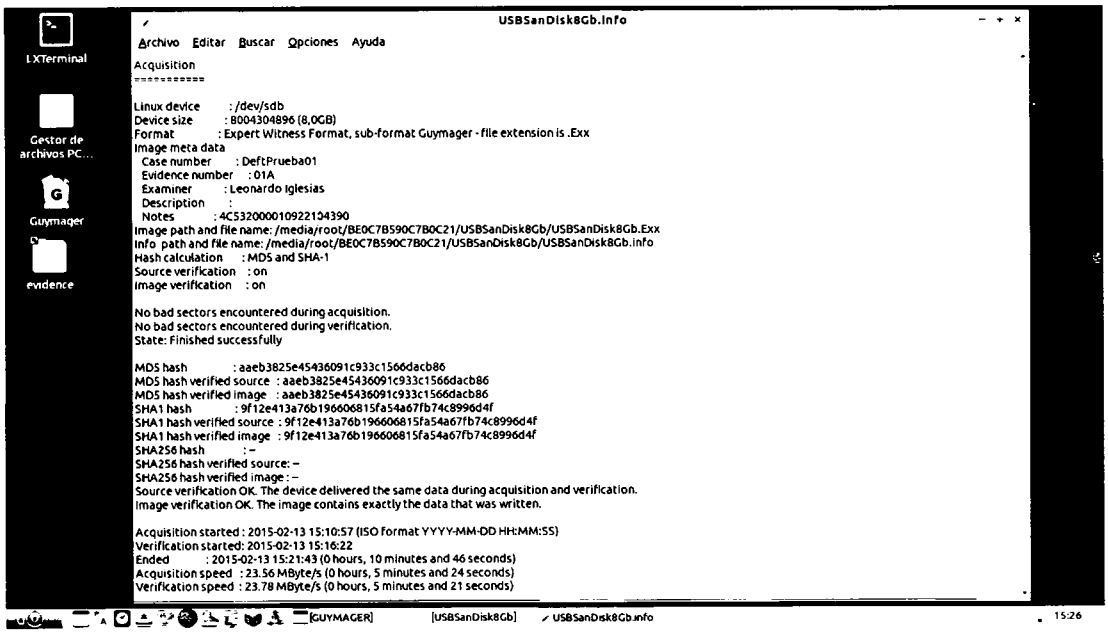
Al finalizar todos los procedimientos, el mismo directorio o unidad donde se creó la imagen forense se crea un reporte (USBSanDisk8Gb.info) con los resultados finales, en el mismo se aprecia diferente información, incluyendo los algoritmos de seguridad Hash MD5 y SHA-1.

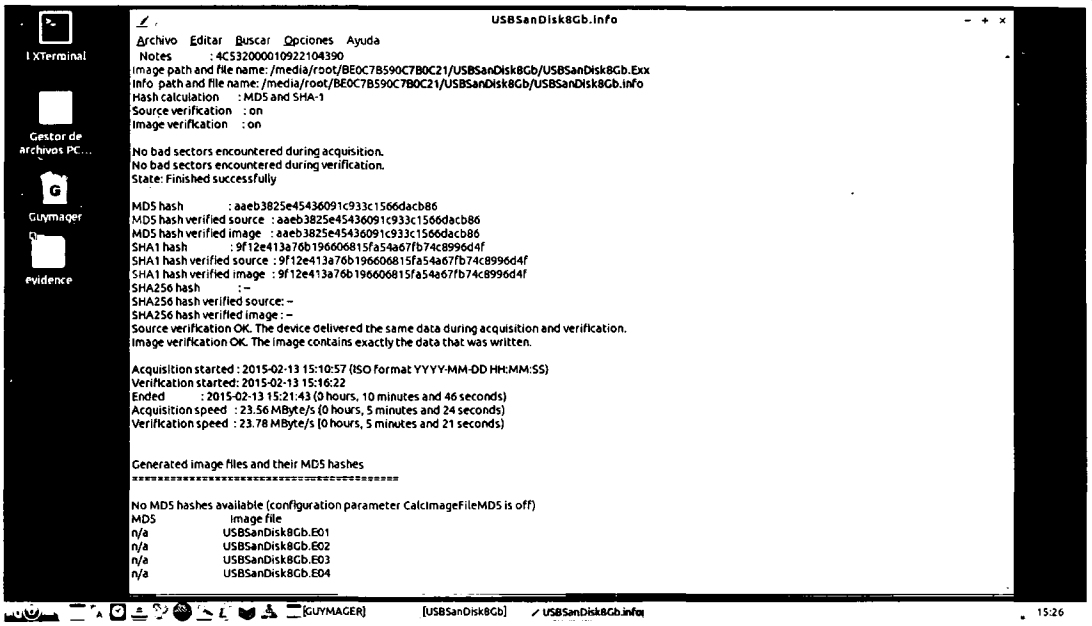


En el reporte en cuestión (USBSanDisk8Gb.info) se encuentra disponible toda la información del procedimiento llevado a cabo, según se aprecian en los gráficos inferiores.




LXTerminal
Guymager
evidence
USBSanDisk8Gb.info
Archivo Editar Buscar Opciones Ayuda
Use smartctl -h to get a usage summary
Command executed: bash -c "hdparm -I /dev/sdb"
Information returned:
SG_IO: bad/missing sense data, sb[]: f0 00 05 00 00 00 00 14 00 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
/dev/sdb:
ATA device, with non-removable media
Serial Number: ???
Standards:
Likely used: 1
Configuration:
Logical max current
cylinders 0 0
heads 0 0
sectors/track 510 0
--
Logical/Physical Sector size: 512 bytes
device size with M = 1024*1024: 0 MBytes
device size with M = 1000*1000: 0 MBytes
cache/buffer size = unknown
Capabilities:
IORDY not likely
Cannot perform double-word IO
R/W multiple sector transfer: not supported
DMA: not supported
PIO: pio0
Hidden areas: unknown
Acquisition
Linux device : /dev/sdb
Device size : 8004304896 (8,0GB)
Format : Expert Witness Format, sub-format Guymager - file extension is .Exx
[GUYMAGER]
[USBSanDisk8Gb]
USBSanDisk8Gb.info
15:25


LXTerminal
Gestor de archivos PC...
Guymager
evidence
USBSanDisk8Gb.info
Archivo Editar Buscar Opciones Ayuda
Acquisition
Linux device : /dev/sdb
Device size : 8004304896 (8,0GB)
Format : Expert Witness Format, sub-format Guymager - file extension is .Exx
Image meta data
Case number : DeftPrueba01
Evidence number : 01A
Examiner : Leonardo Iglesias
Description :
Notes : 4C532000010922104390
Image path and file name: /media/root/BE0C7B590C7B0C21/USBSanDisk8Gb/USBSanDisk8Gb.Exx
Info path and file name: /media/root/BE0C7B590C7B0C21/USBSanDisk8Gb/USBSanDisk8Gb.info
Hash calculation : MD5 and SHA-1
Source verification : on
Image verification : on
No bad sectors encountered during acquisition.
No bad sectors encountered during verification.
State: Finished successfully
MD5 hash : aaeb3825e45436091c933c1566dacb86
MD5 hash verified source : aaeb3825e45436091c933c1566dacb86
MD5 hash verified image : aaeb3825e45436091c933c1566dacb86
SHA1 hash : 9f12e413a76b196606815fa54a67fb74c8996d4f
SHA1 hash verified source : 9f12e413a76b196606815fa54a67fb74c8996d4f
SHA1 hash verified image : 9f12e413a76b196606815fa54a67fb74c8996d4f
SHA256 hash : -
SHA256 hash verified source: -
SHA256 hash verified image : -
Source verification OK. The device delivered the same data during acquisition and verification.
Image verification OK. The image contains exactly the data that was written.
Acquisition started : 2015-02-13 15:10:57 (ISO format YYYY-MM-DD HH:MM:SS)
Verification started: 2015-02-13 15:16:22
Ended : 2015-02-13 15:21:43 (0 hours, 10 minutes and 46 seconds)
Acquisition speed : 23.56 MByte/s (0 hours, 5 minutes and 24 seconds)
Verification speed : 23.78 MByte/s (0 hours, 5 minutes and 21 seconds)
[GUYMAGER]
[USBSanDisk8Gb]
USBSanDisk8Gb.info
15:26


1 XTerminal
Gestor de archivos PC...
Guymager
evidence
USBSanDisk8Gb.info
Archivo Editar Buscar Opciones Ayuda
Notes : 4C532000010922104390
Image path and file name: /media/root/BE0C7B590C7B0C21/USBSanDisk8Gb/USBSanDisk8Gb.Exx
Info path and file name: /media/root/BE0C7B590C7B0C21/USBSanDisk8Gb/USBSanDisk8Gb.info
Hash calculation : MD5 and SHA-1
Source verification : on
Image verification : on
No bad sectors encountered during acquisition.
No bad sectors encountered during verification.
State: Finished successfully
MD5 hash : aaeb3825e45436091c933c1566dacb86
MD5 hash verified source : aaeb3825e45436091c933c1566dacb86
MD5 hash verified image : aaeb3825e45436091c933c1566dacb86
SHA1 hash : 9f12e413a76b196606815fa54a67fb74c8996d4f
SHA1 hash verified source : 9f12e413a76b196606815fa54a67fb74c8996d4f
SHA1 hash verified image : 9f12e413a76b196606815fa54a67fb74c8996d4f
SHA256 hash : -
SHA256 hash verified source: -
SHA256 hash verified image : -
Source verification OK. The device delivered the same data during acquisition and verification.
Image verification OK. The image contains exactly the data that was written.
Acquisition started : 2015-02-13 15:10:57 (ISO format YYYY-MM-DD HH:MM:SS)
Verification started: 2015-02-13 15:16:22
Ended : 2015-02-13 15:21:43 (0 hours, 10 minutes and 46 seconds)
Acquisition speed : 23.56 MByte/s (0 hours, 5 minutes and 24 seconds)
Verification speed : 23.78 MByte/s (0 hours, 5 minutes and 21 seconds)
Generated image files and their MD5 hashes
No MD5 hashes available (configuration parameter CalcImageFileMD5 is off)
MD5 Image file
n/a USBSanDisk8Gb.E01
n/a USBSanDisk8Gb.E02
n/a USBSanDisk8Gb.E03
n/a USBSanDisk8Gb.E04
[GUYMAGER]
[USBSanDisk8Gb]
USBSanDisk8Gb.info
15:26

4.4. Resumen

Empleando Encase

Debido a la familiaridad en el uso de esta aplicación y además de la facilidad que le otorga su interfaz gráfica, su empleo resulta bastante sencilla.

Del resultado práctico efectuado en la obtención de imagen forense realizada sobre una memoria tipo pendrive de 8 GB de capacidad, la misma arrojó un tiempo estimado de 7 minutos con 24 segundos.

Empleando FTK Imager

Si bien no es tan familiar, su interfaz gráfica resulta amigable.

En cuanto al término de tiempo que demanda la obtención de imágenes forenses, esta aplicación fue la más lenta, arrojando para el mismo tipo de memoria enunciada anteriormente (8 GB), una cantidad de 10 minutos con 4 segundos.

Empleando DEFT - Guymager

En este caso en particular, no se trata de una aplicación a la cual los usuarios acceden como primera opción, dada la interfaz que posee la aplicación (consola).

Sin perjuicio de lo expresado con anterioridad, al emplear esta aplicación (Guymager) contenida en este pack de herramientas (DEFT) se observó que la obtención de imágenes forenses ofrece una mayor velocidad, registrándose para la misma memoria un tiempo de 5 minutos con 25 segundos.

Sin lugar a dudas el empleo para discos de más de 1 TB dicha diferencia de tiempo resultaría muy notoria y hace que sea la aplicación elegida al efectuar una copia forense.

Hay que destacar que independientemente de cualquier herramienta tipo software, un duplicador de discos forense (hardware) es lo más rápido para efectuar imágenes o copias forenses.

5. Búsqueda por palabras clave

La búsqueda por palabras claves en cualquier ubicación de un dispositivo de almacenamiento, constituye una de las actividades más importantes para la obtención de evidencias en un caso.

Es en este punto que debe existir una comunicación fluida entre los oficiales judiciales, que proporcionan la lista de palabras clave, y el examinador forense.

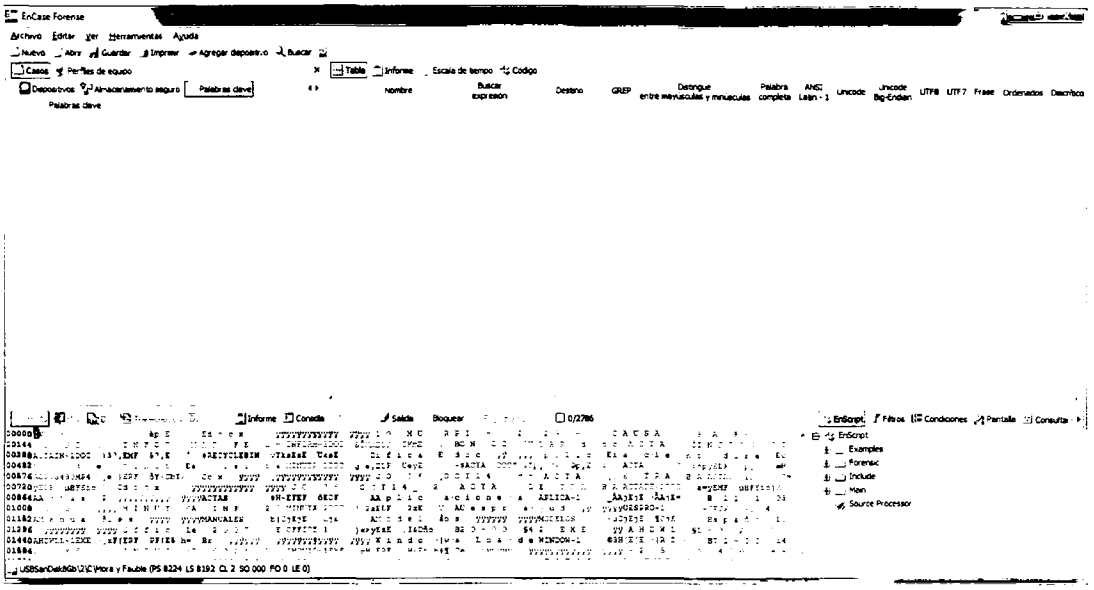
Esta lista de palabras claves puede estar constituida por una palabra clave simple, una frase o una expresión GREP. La expresión GREP es empleada para restringir más una búsqueda, limitando los resultados erróneos y en aquellos casos donde se conocen solo ciertos fragmentos de las palabras clave.

Para el presente caso se realizaron búsquedas de palabras clave empleando las siguientes herramientas:

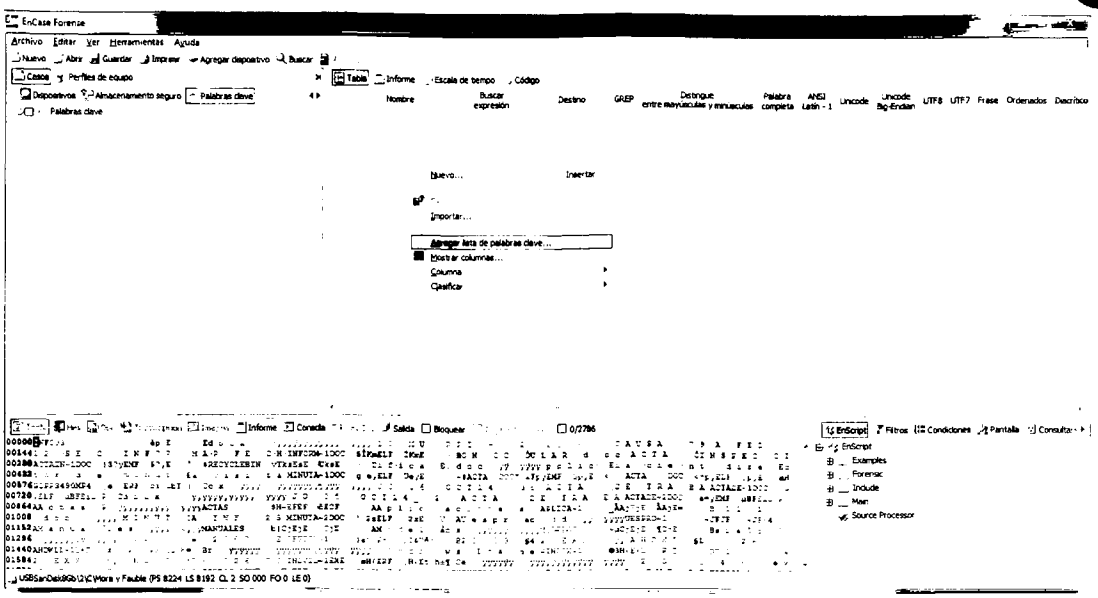
- **Encase V6.19**
- **DEFT - Autopsy**

5.1. Búsqueda por palabras clave empleando Encase

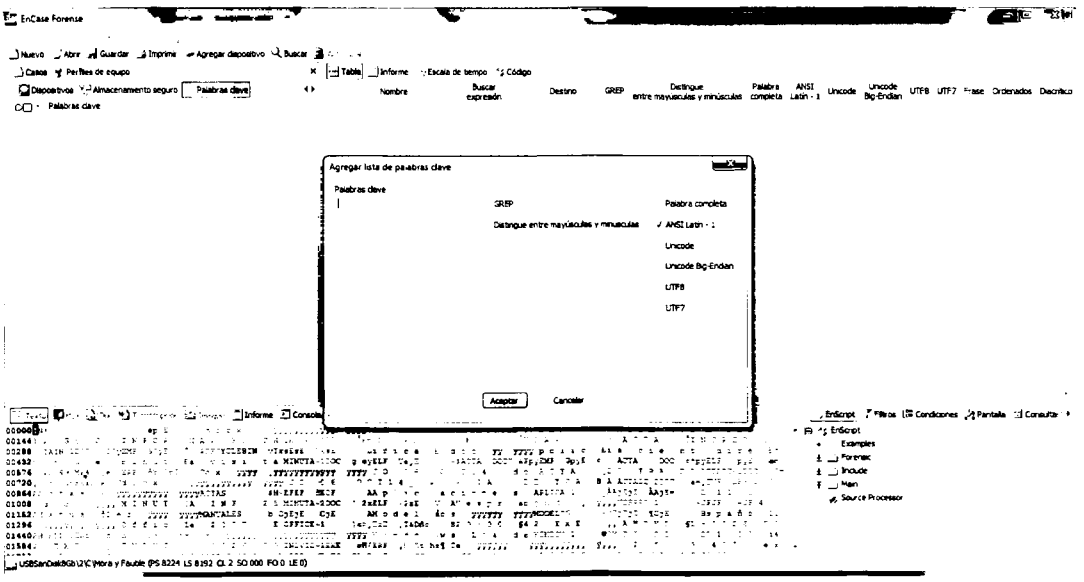
A partir de la evidencia agregada al Caso, para iniciar el procedimiento de búsqueda por palabras clave, se debe seleccionar la herramienta "Palabras Clave", el cual se haya evidenciada por un icono en forma de llave.



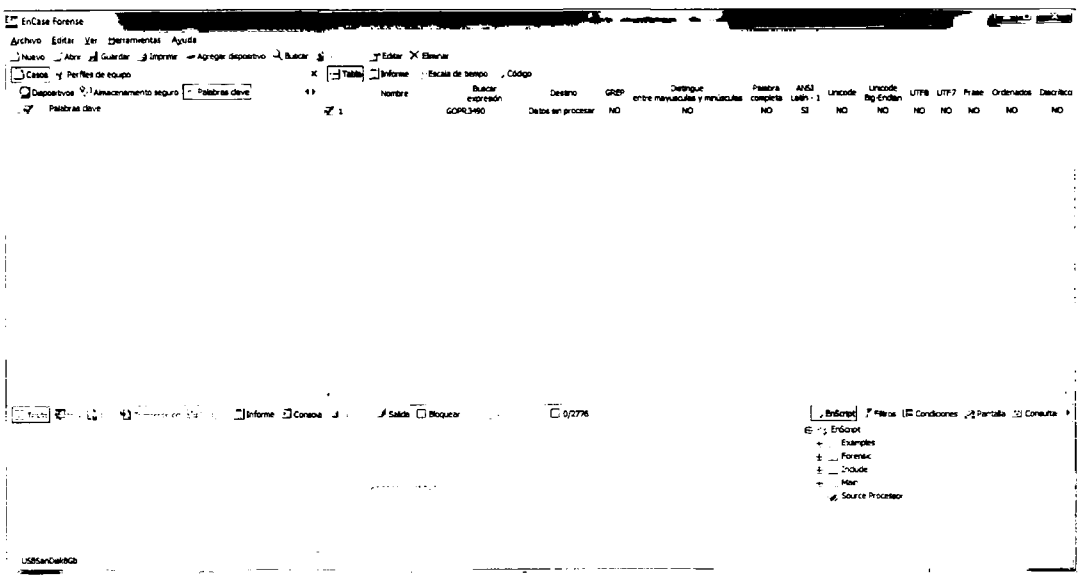
Acto seguido, se debe hacer clic con el botón derecho sobre el lado izquierdo del panel, desplegándose un menú donde se debe seleccionar "Agregar lista de palabras clave".



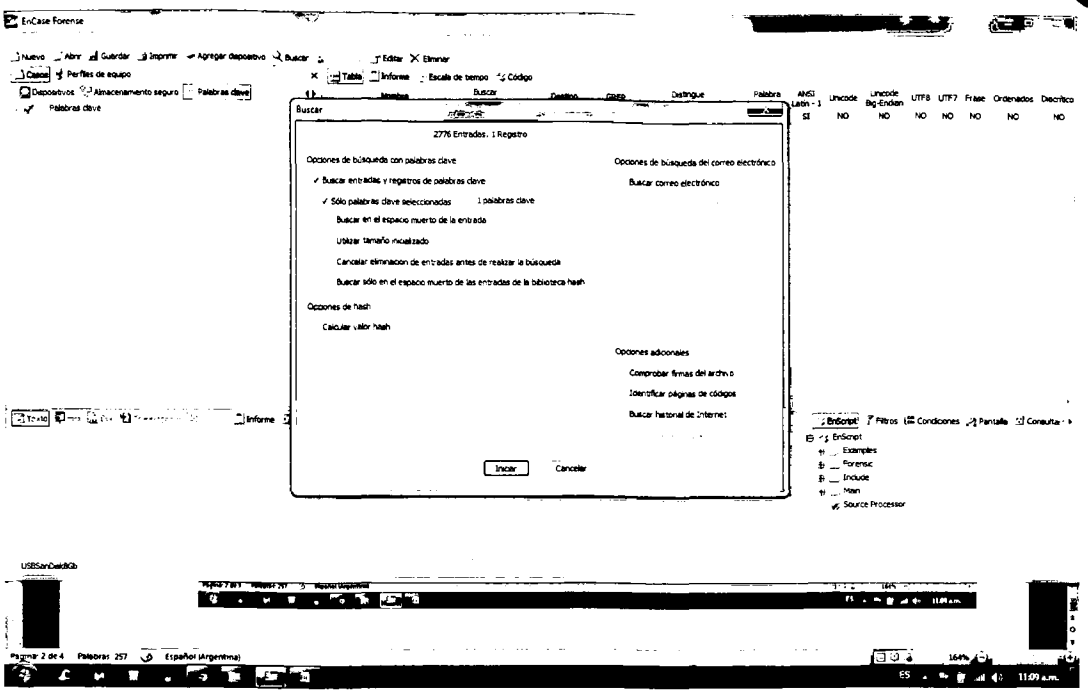
La ventana que continúa nos proporciona a la izquierda un cuadro donde se deben ingresar las palabras clave específicas para cada caso en particular. Asimismo se puede optar por realizar una búsqueda "GREP" (aplicando fórmulas especiales) o distinguiendo entre "Minúsculas y mayúsculas". Por otro lado se pueden establecer parámetros tales como la búsqueda por "Palabra completa", codificación "ANSI Latín - 1", "Unicode", etc. Para el presente caso se agregó la palabra "GOPR3490", para continuar se debe hacer clic en el botón “Aceptar”.



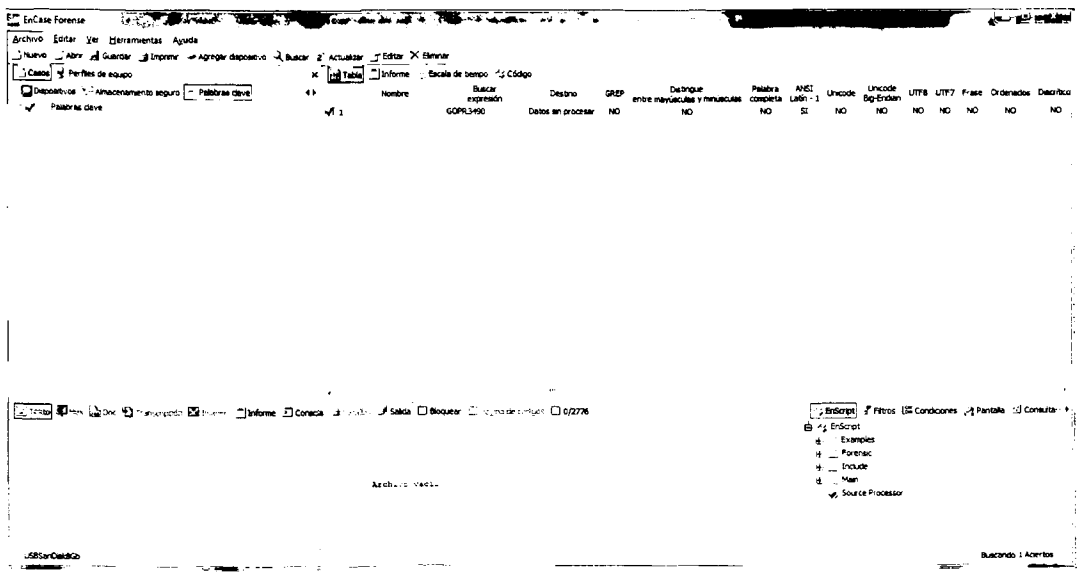
Seguidamente, se debe seleccionar la palabra clave agregada, haciendo click en un recuadro delante de la palabra clave con el puntero del mouse, lo que añade una tilde de color azul.



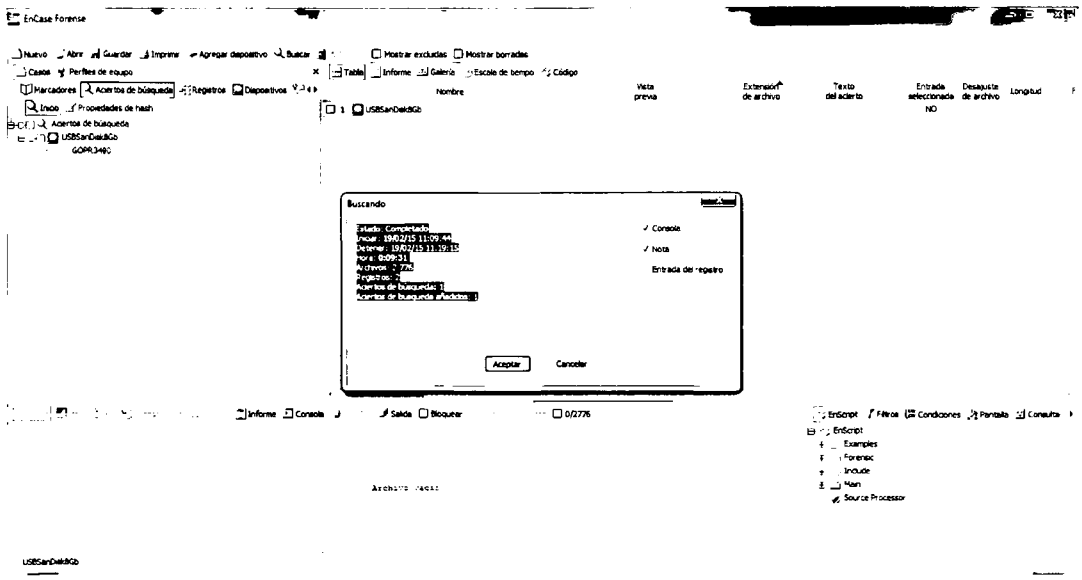
Posteriormente, se debe seleccionar la herramienta "Buscar", a partir de las opciones de búsqueda. Para el presente caso se debe seleccionar "Sólo palabras clave seleccionadas" y hacer clic en "Iniciar".



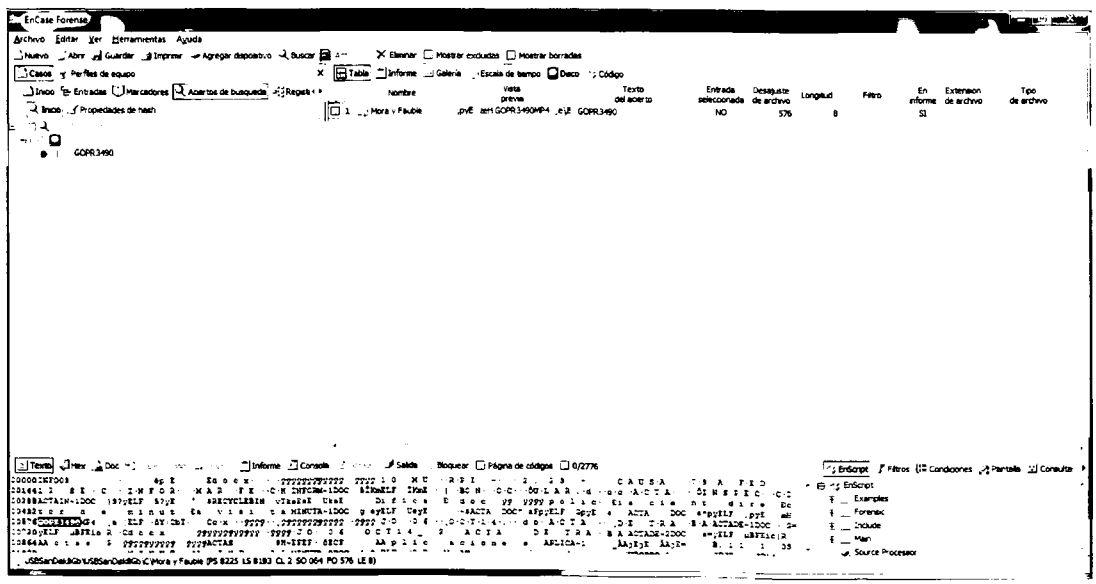
Esto da inicio en forma automática a la búsqueda en todo el dispositivo de almacenamiento cuestionado, de la palabra seleccionada, mostrando los avances obtenidos en la parte inferior derecha como aciertos de búsqueda.



Una vez concluida la búsqueda, se aprecia una ventana donde se puede visualizar un reporte con los resultados obtenidos, los aciertos y el tiempo demandado en la búsqueda.



En la siguiente pantalla se aprecia que la palabra clave "GOPR3490", impactó de forma positiva indicando que existe un archivo con dicho nombre, aunque no lo ubica específicamente a pesar de su existencia en el dispositivo analizado.



5.2. Búsqueda por palabras clave empleando Autopsy

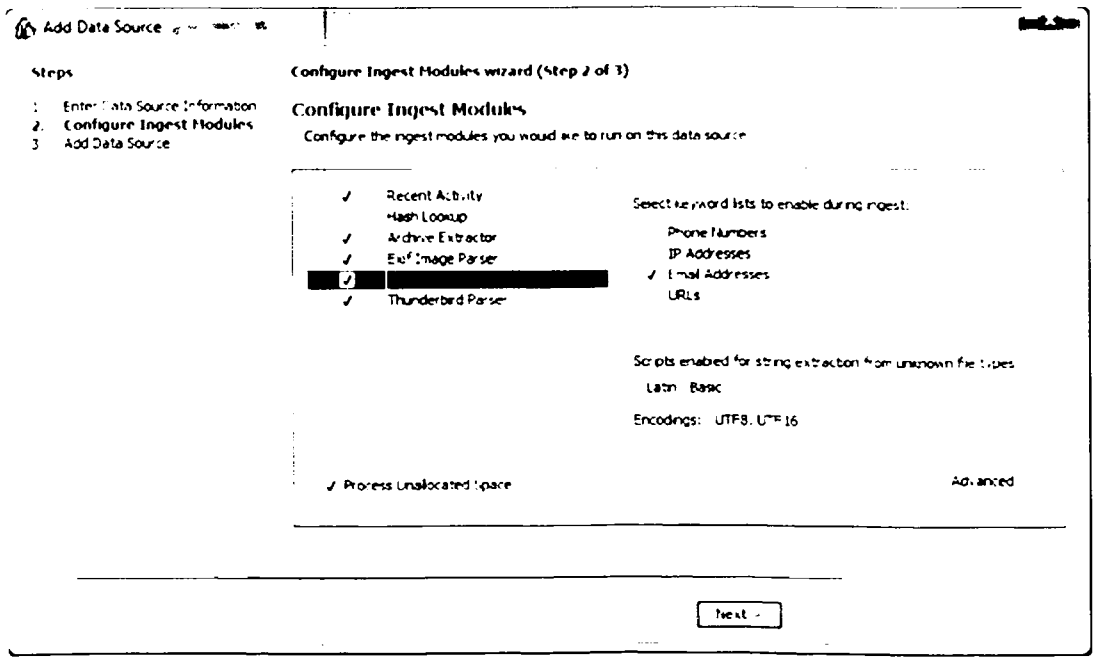
El conjunto de herramientas libres denominado DEFT, contiene una aplicación llamada "Autopsy". Este recurso, al igual que el software Encase, cuenta con algunas similitudes, las cuales detallaré más abajo.

En principio, al abrir Autopsy, lo primero que se debe realizar es crear un nuevo caso, o si ya está existente se procederá a abrirlo (se considera caso a aquella unidad lógica que posee lo investigado).

Es en este punto, donde se solicita información respecto al nombre, número de la persona que realizará el análisis forense.

El siguiente paso corresponderá a asociar los discos orígenes, sea una imagen forense o un disco rígido conectado a la computadora a ser analizada.

Como paso final, Autopsy, a diferencia de Encase, solicita la configuración de módulos para utilizar en el análisis, tal cual se observa en la imagen siguiente:



Estos módulos consisten en CINCO (5) tópicos de búsqueda, a saber:

- **Recent Activity**
- **Hash Lookup**
- **Archive Extractor**
- **Exif Image Parser**
- **Keyword Search**

Para el caso de **Recent Activity**, al efectuar el análisis, se extrae toda la actividad reciente realizada, esto es: documentos recientemente aperturados, dispositvos que se hayan conectados, historial web, etc, etc.

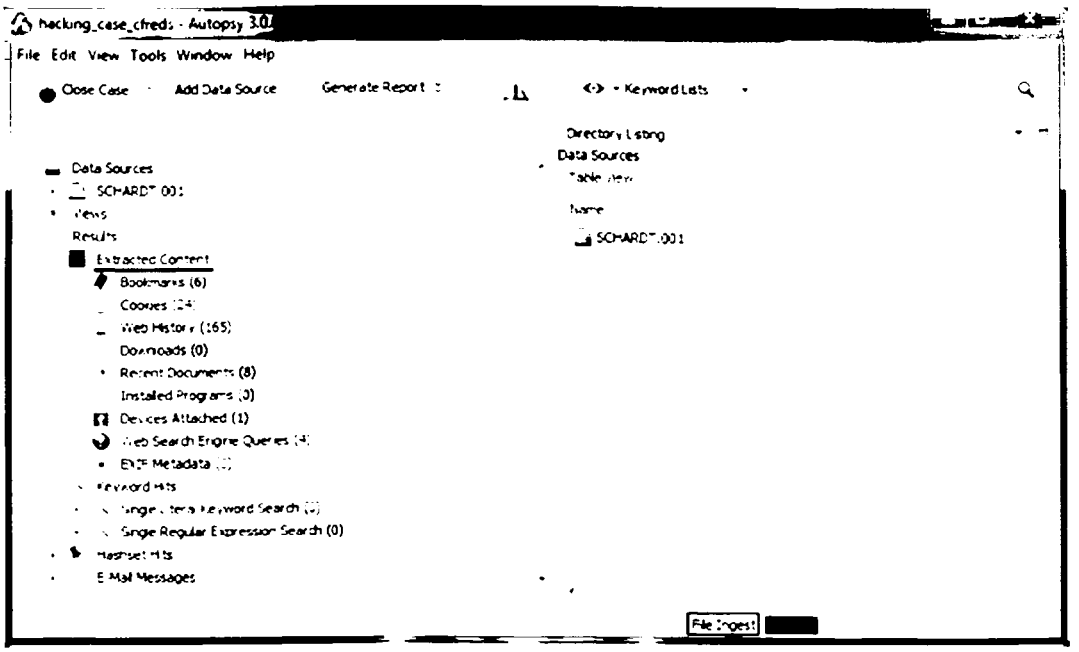
El **Hash Lookup** permite conociendo de antemano el valor hash de determinado documento, hallarlo rápidamente sin perder tiempo.

Archive Extractor, permite recuperar archivos borrados y/o eliminados empleando la detección de los encabezados, cualquiera sea su posición donde se hallen, en espacios asignados o no asignados.

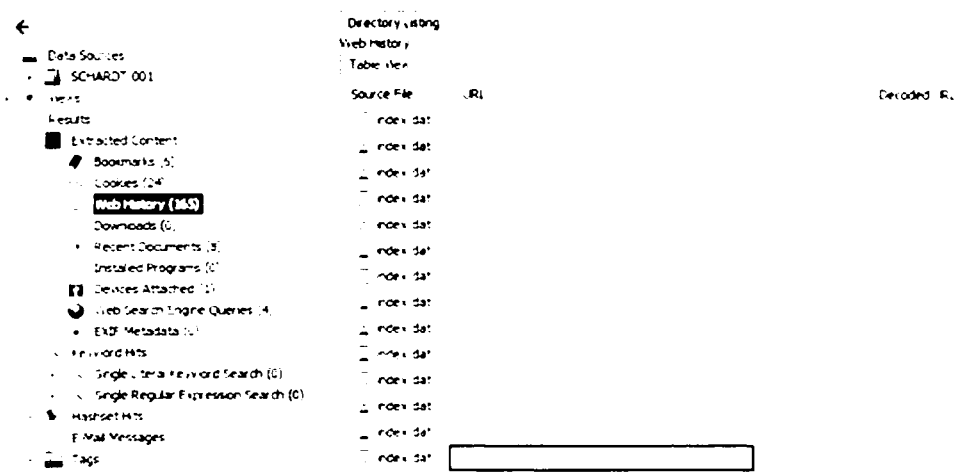
El **Exif Image Parser**, permite analizar con la información disponible en los metadatos de un archivo.

Y por último, y tal vez la más importante; **keyword Search**, permite el agregado de simples palabras clave, frases, números, etc.

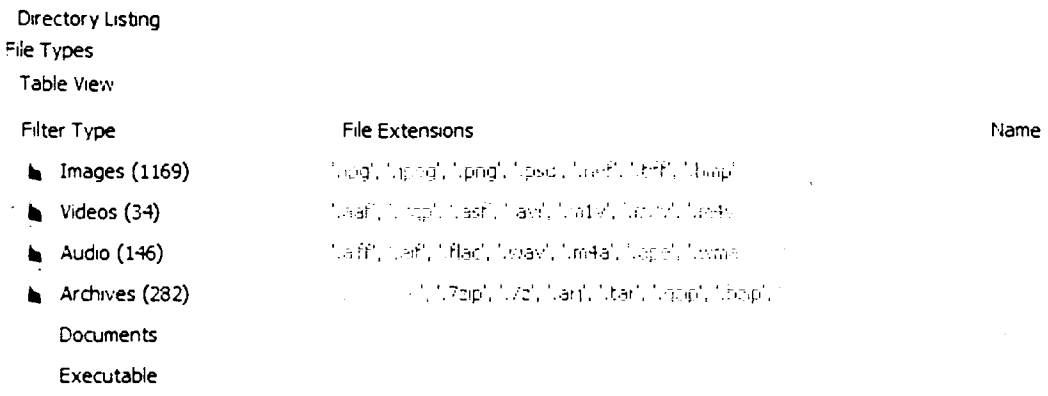
Una vez seleccionados los módulos de interés para correr en la imagen forense y/o disco rígido conectado, el programa va mostrando una línea de progreso en la parte inferior derecha, tal cual se observa en el siguiente gráfico demostrativo:



Una vez finalizada la extracción de información del disco analizado, como ser palabras clave, documentos abiertos en forma reciente, etc; lo cual conlleva un tiempo considerable, dicho proceso arroja una ventana como la siguiente:

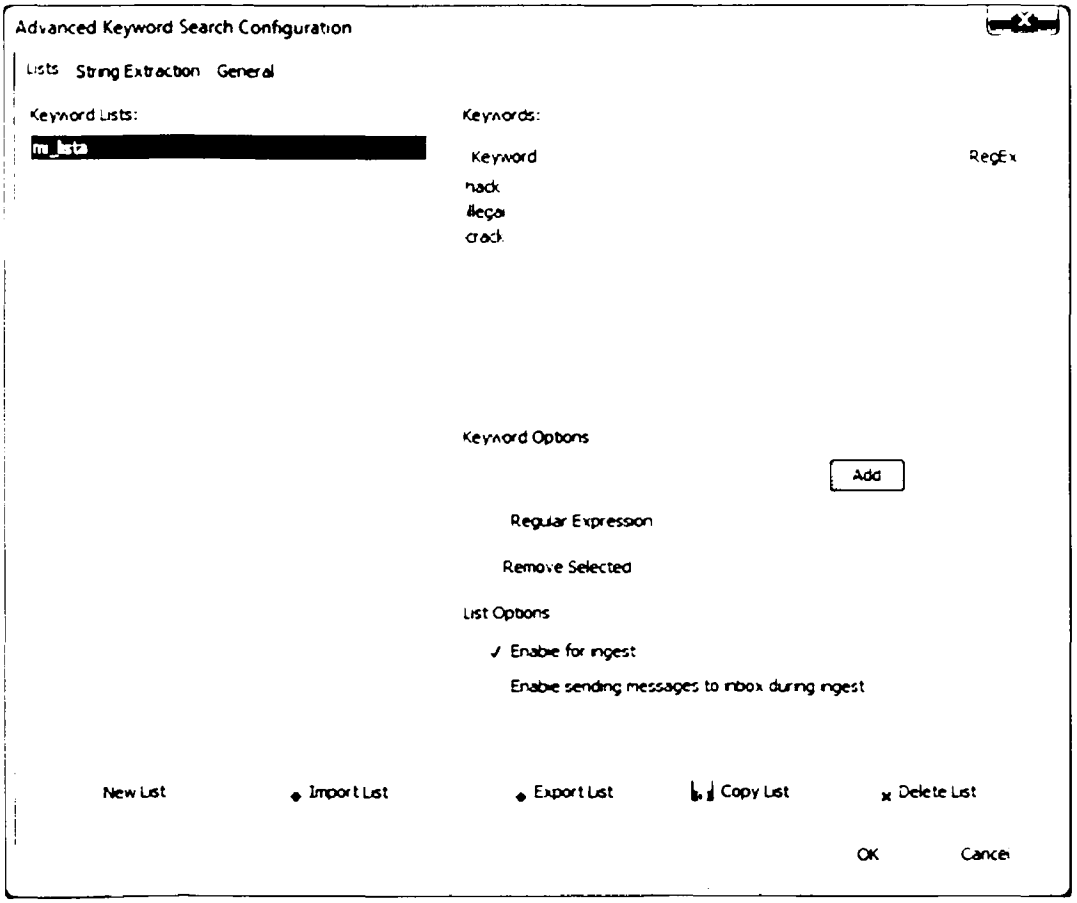


Una opción muy interesante del Autopsy es aquella que agrupa los archivos en categorías, o sea permite observar: cantidad de archivos de imágenes, cantidad de archivos de video, etc; discriminados cada uno de ellos por extensión, conforme se aprecia en la siguiente imagen:

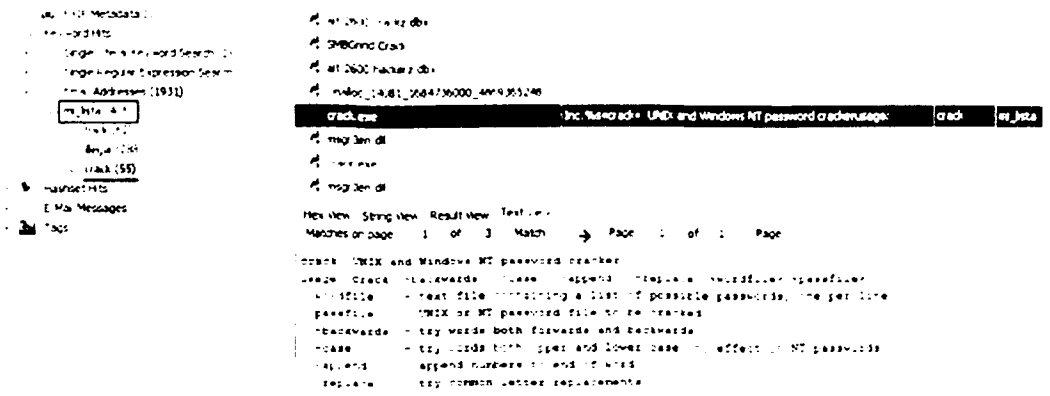


Además, a similitud de Encase, Autopsy clasifica los diferentes tipos de archivo con fecha de último acceso, tamaño, etc.

Ahora bien, para el caso de que nuestra búsqueda fuera por palabras clave, Autopsy permite al investigador definir un listado de palabras clave o expresiones para buscar en todos los sectores del disco en análisis (aún en los sectores no asignados), de la siguiente manera que se aprecia a continuación:



El resultado de lo hallado, se observa en la siguiente fotografía de pantalla, donde arroja la cantidad de resultados (hits) por palabra clave buscada.



Autopsy permite una vez culminados los resultados obtenidos, exportarlos a documentos HTML o cualquiera de los otros formatos ofrecidos para presentación.

5.3. Resumen

Empleando Encase

Encase a diferencia de cualquier herramienta libre ofrece una facilidad de trabajo que se debe en gran medida a su destacada interfaz gráfica. Es sin duda su más importante fortaleza que hace muy amena, en particular en éste caso, la actividad de búsqueda de palabras clave.

Otros elementos a destacar son sin duda los siguientes: la posibilidad de extraer la totalidad de hits o resultados y resguardarlos en una carpeta con sus correspondientes hash de seguridad, seleccionar por tipo/extensión de archivo, por tamaño, etc.

Como aspecto negativo debemos mencionar que esta herramienta comercial necesita de grandes recursos en lo que se refiere a proceso de cómputo, algo en lo que las aplicaciones libre no lo requieren.

Como similares modos de análisis, ambas herramientas presentan el análisis "en reposo" y análisis "en vivo".

Empleando DEFT - Autopsy

Esta herramienta libre presenta ciertas similitudes con respecto a la herramienta comercial "ENCASE", en lo que refiere a su empleo y a la interfaz gráfica.

Como diferencia sustancial, este programa permite no solo analizar discos con plataformas Windows, sino también discos con sistemas operativos UNIX.

Además Autopsy al basarse en código HTML, permite ser conectado desde cualquier plataforma empleando un navegador HTML, proporcionando una interfaz tipo "Manejador de archivos" donde muestra detalles diversos de los metadatos de los archivos (fechas borradas y estructura de los archivos).

Las búsquedas en autopsy pueden ser realizadas sobre la imagen completa, al igual que Encase, o solamente en los espacios sin asignar (clústeres no asignados).

Las búsquedas pueden ser configuradas dentro del autopsy en forma automatizadas, al igual que el Encase.

6. Data Carving

Este término es utilizado para describir la identificación y extracción de distintos tipos de archivos del espacio no utilizado del disco utilizando las firmas de archivo (files signature). Las firmas de archivo son constantes numéricas o valores de texto utilizados para identificar un formato de archivo específico.

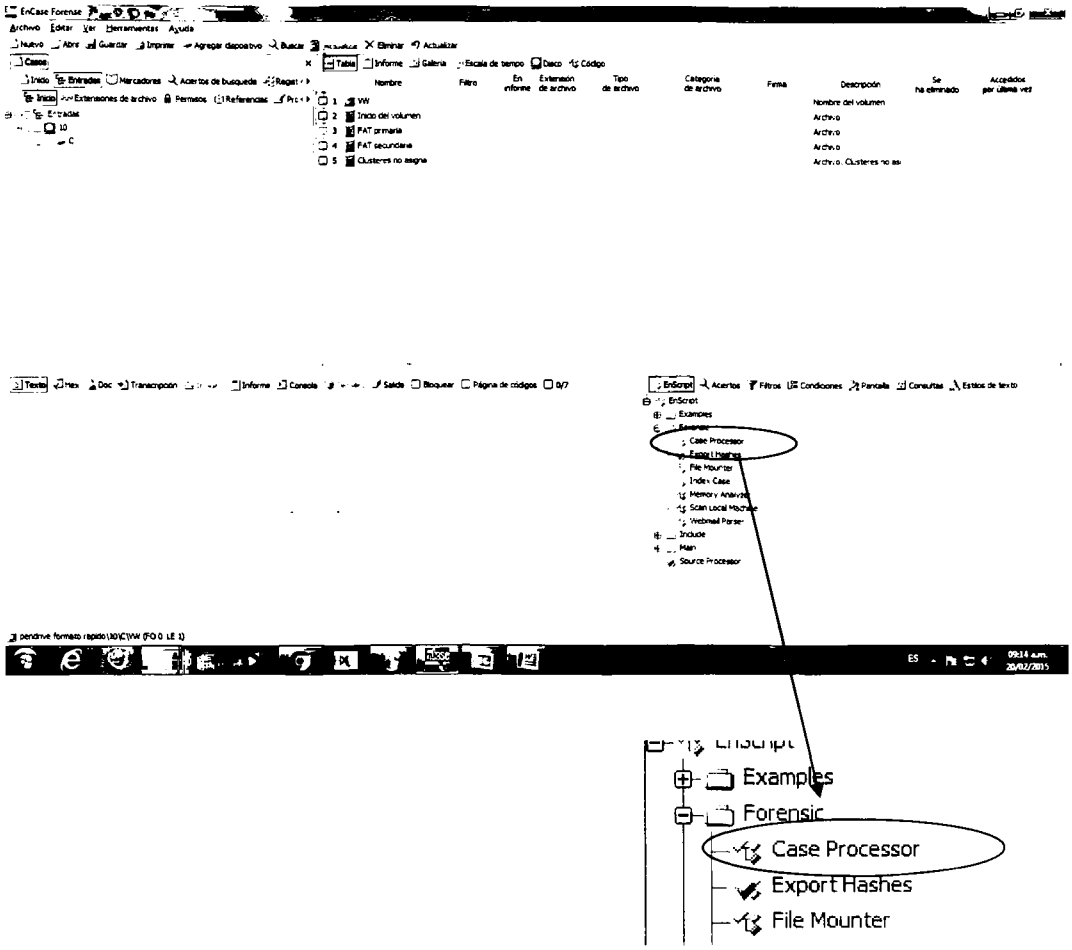
Este proceso realiza un análisis del disco duro, en búsqueda no solo de archivos ocultos sino también de aquellos que no tienen información de asignación.

Un archivo que no posee información de asignación no es posible llegar a él a través de los medios tradicionales.

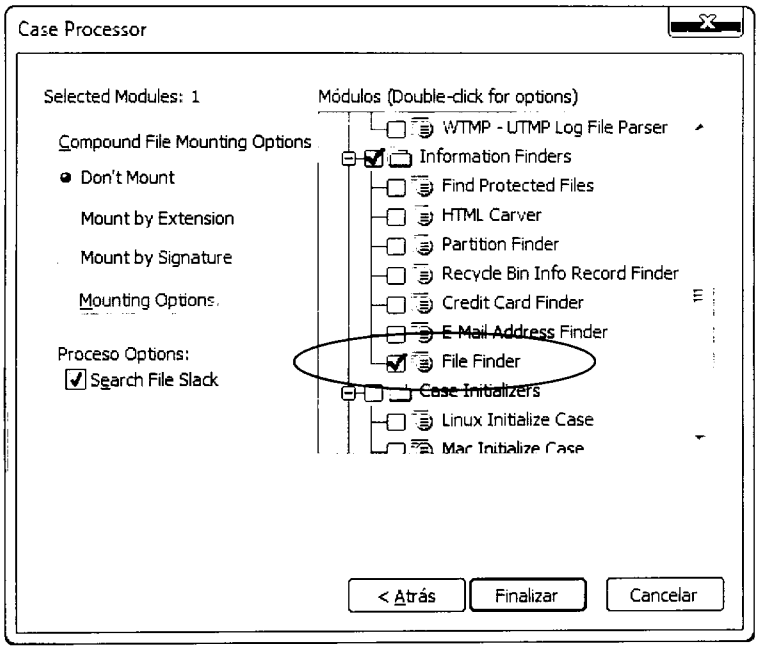
Ocurren casos en que un disco rígido falla y comienza a borrar archivos importantes de forma aleatoria, habiendo una buena probabilidad de que hayan sido escondidos. Una forma de rastrearlos es usar ésta técnica a través de las firmas de los archivos.

6.1. Data Carving empleando ENCASE

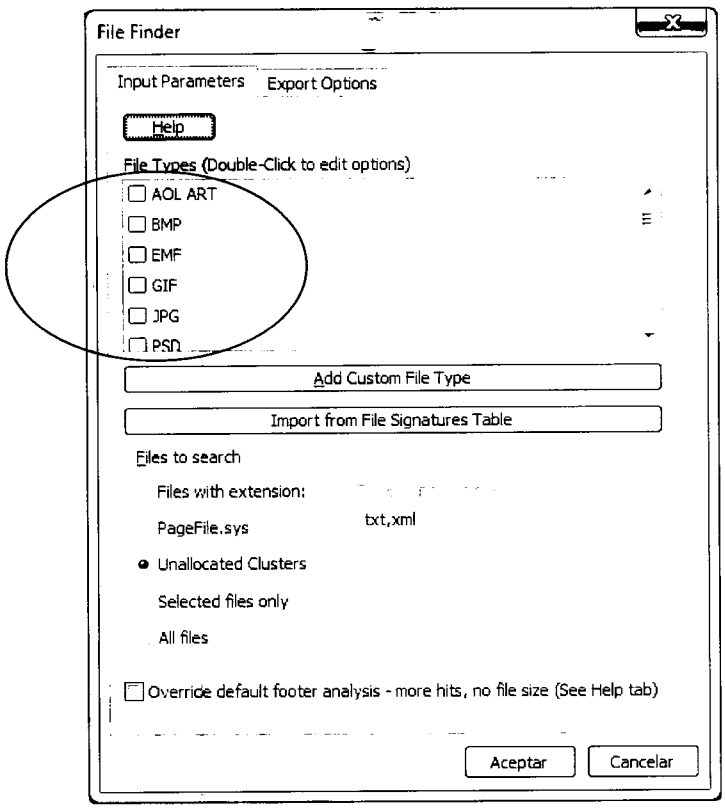
En el caso de la herramienta forense Encase 6.19.0.35, esta actividad se realiza con la opción "Case Processor".



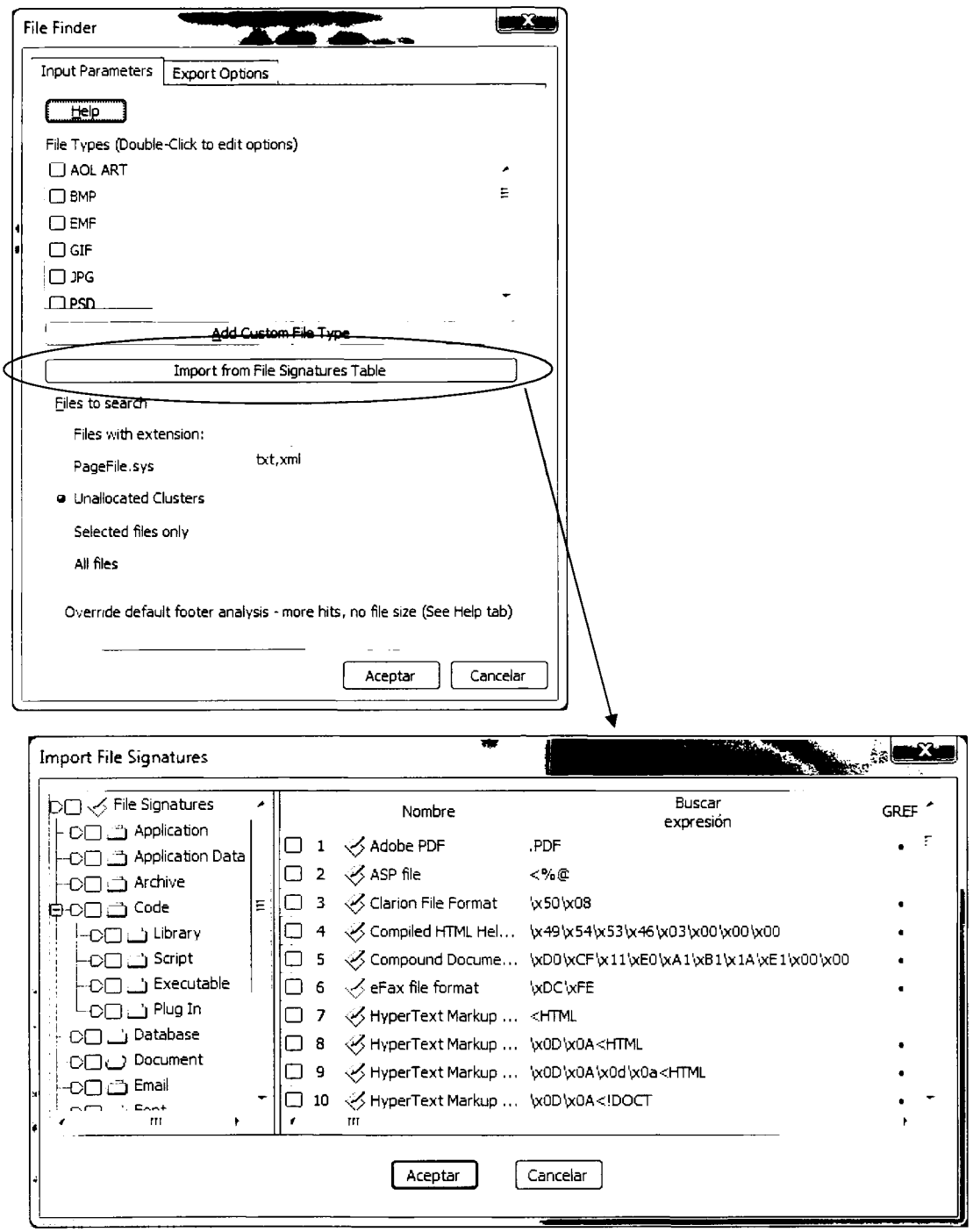
Una vez ingresado al submenu "Case Processor", se debe seleccionar una vez clickeado el mismo y a posteriori de que aparece un cuadro de diálogo, la opción "File Finder"



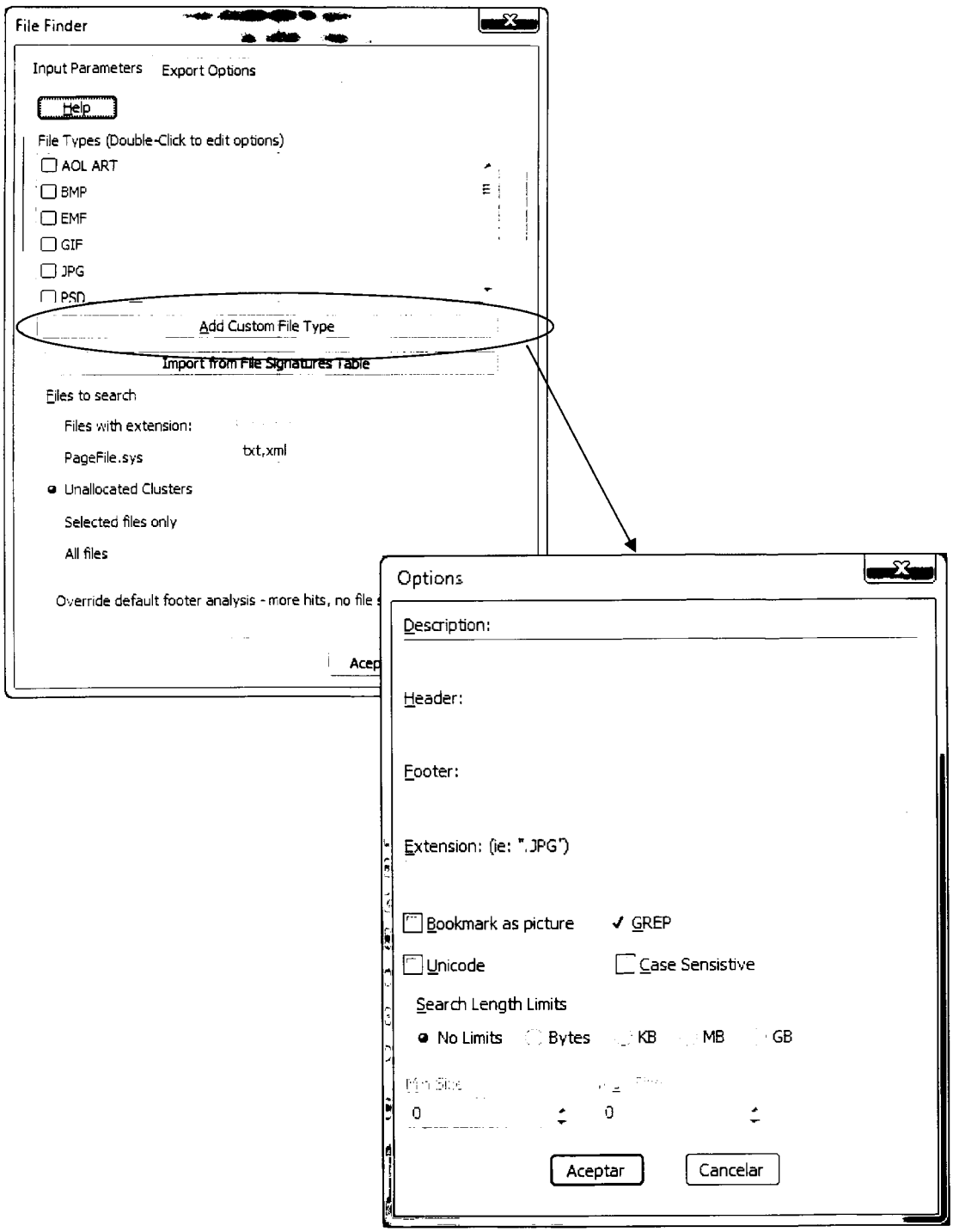
Haciendo doble clic sobre la misma se abre una ventana en la cual se cargan los tipos de archivos que serán buscados en el espacio no asignado del disco. Algunos vienen cargados en forma predeterminada, y con solo tildarlos, el proceso comenzará a buscarlos.



Trae la posibilidad, de incorporar nuevas firmas de archivos mediante una tabla de firmas de archivo.

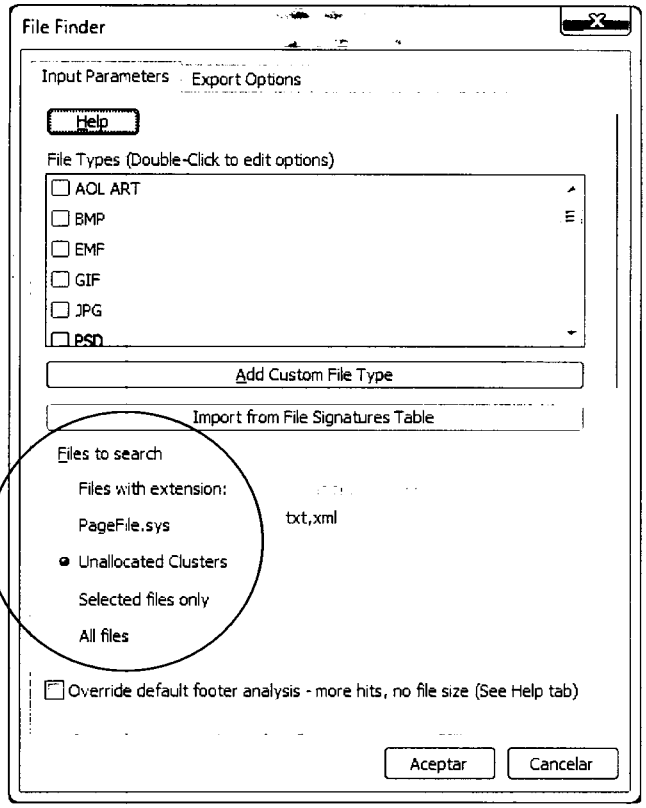


Además permite cargar una nueva firma de archivo que no figure en la tabla anterior. Se debe cargar el encabezado y pie en hexadecimal, como así también si se desea darle una longitud máxima de archivo.

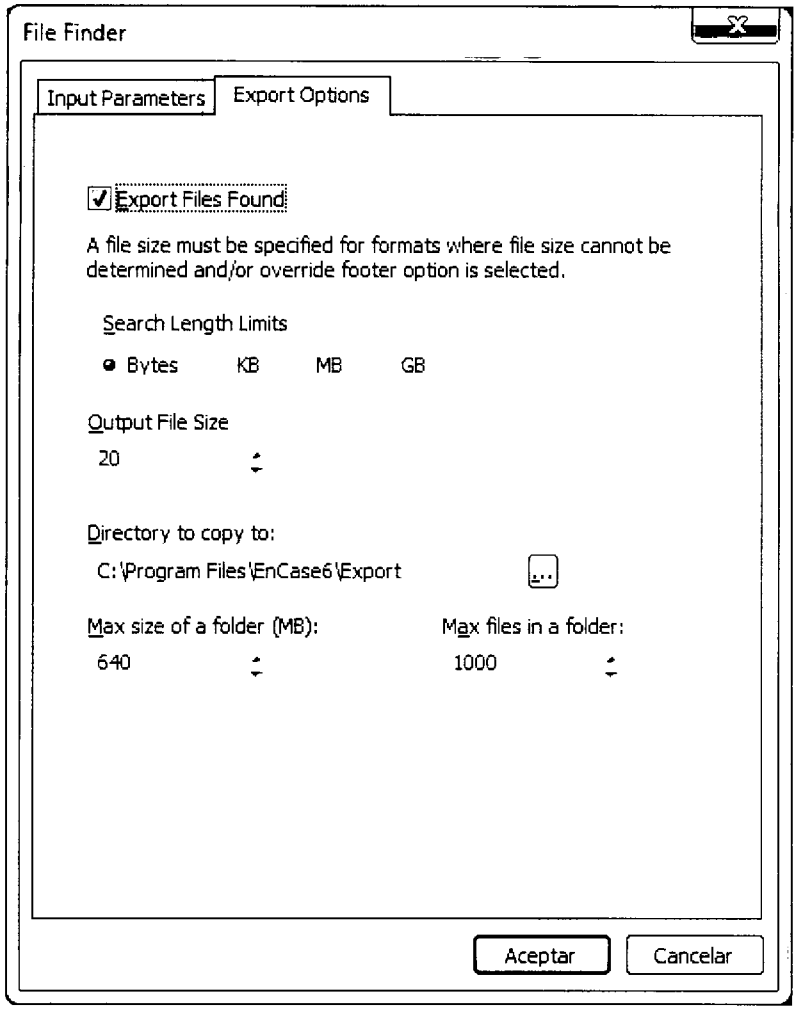


Una vez seleccionadas las firmas que desean buscarse, se debe elegir donde se quiere buscar. Encase permite buscar en archivos existentes con una extensión determinada, en el archivo "pagefile.sys", en el sector no

asignado del disco, en algunos archivos ya seleccionados o en todos los archivos.

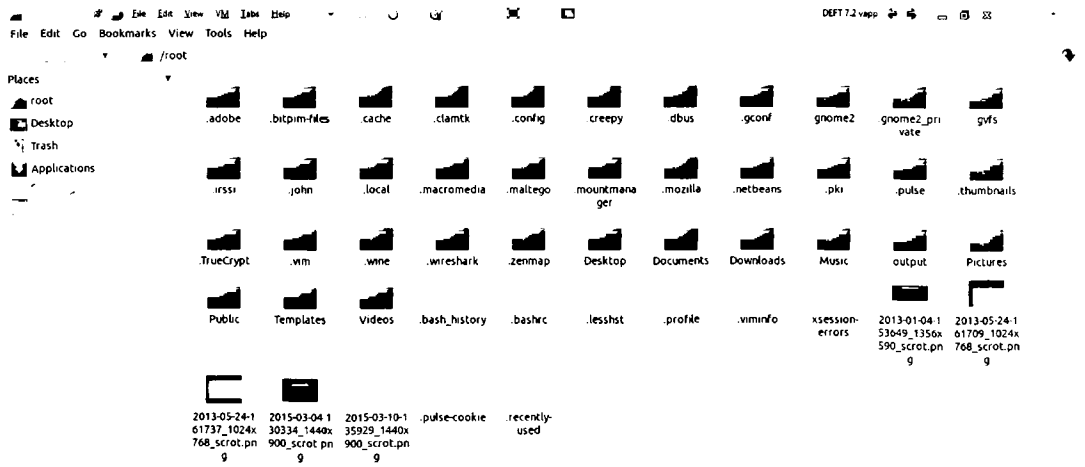


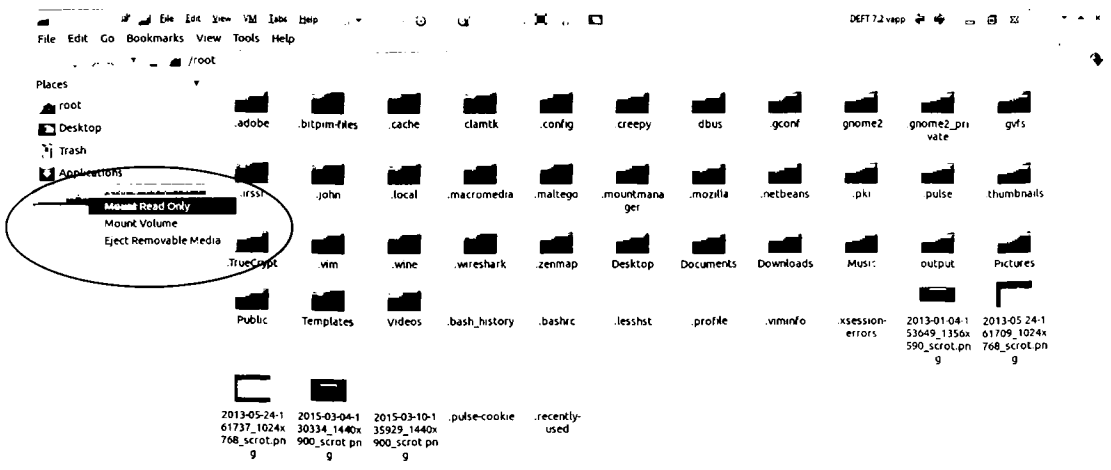
Por último se debe seleccionar si todos los archivos encontrados serán exportados y donde serán almacenados.


File Finder
Input Parameters
Export Options
Export Files Found
A file size must be specified for formats where file size cannot be determined and/or override footer option is selected.
Search Length Limits
Bytes
KB
MB
GB
Output File Size
20
Directory to copy to:
C:\Program Files\EnCase6\Export
Max size of a folder (MB):
640
Max files in a folder:
1000
Aceptar
Cancelar

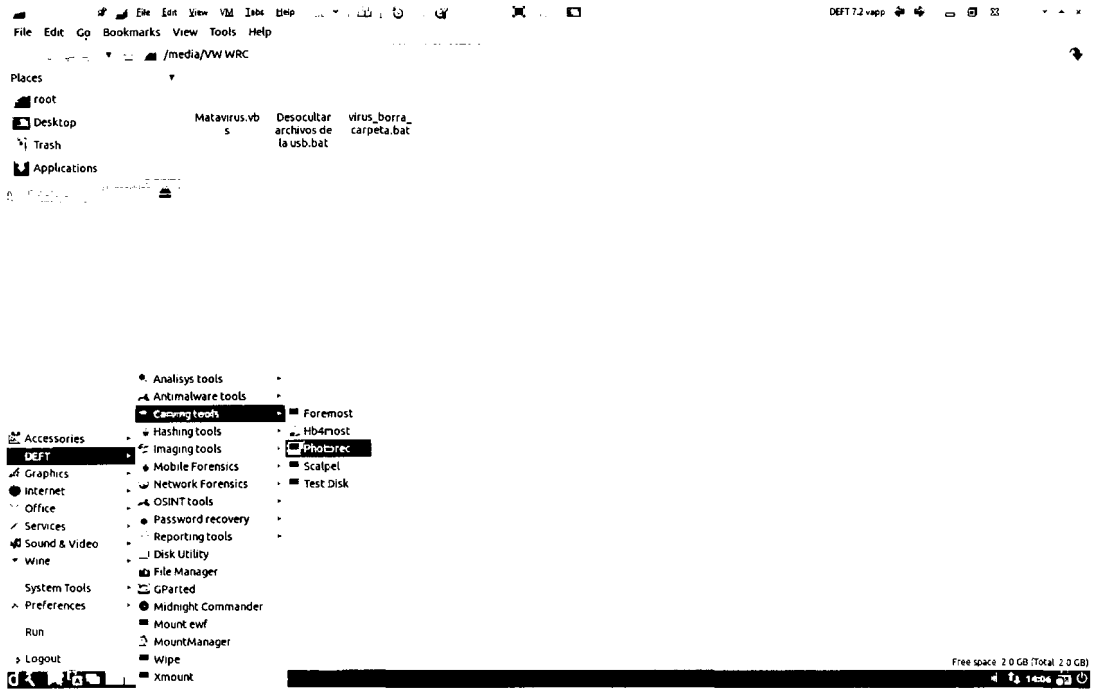
6.2. Data Carving empleando DEFT

En primer lugar hay que montar la unidad que se desea analizar en modo de solo lectura, realizando un clic derecho del mouse sobre la misma y seleccionando la opción "Mount Read Only".





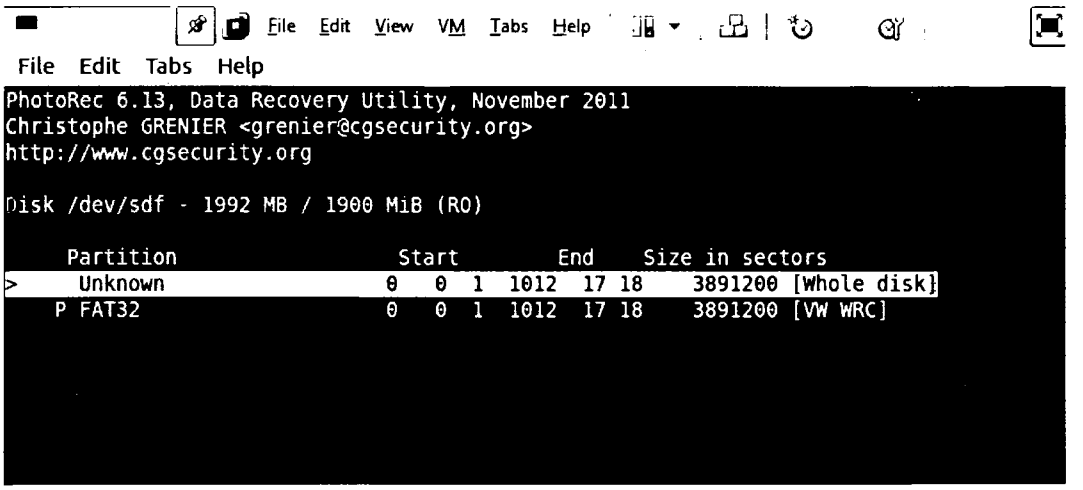
A continuación se selecciona la herramienta “Photorec”



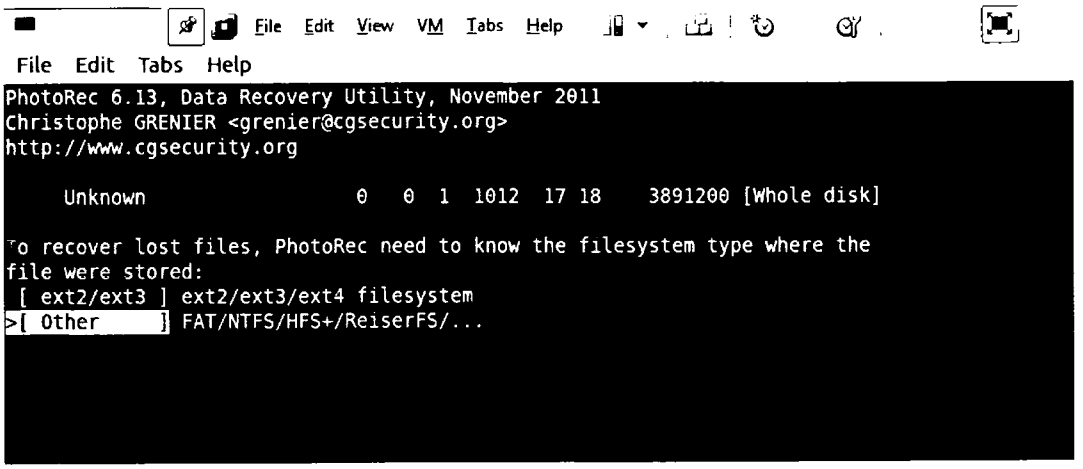
6.2.1. PHOTOREC

En la primera pantalla que muestra el software se debe seleccionar la unidad que se desea analizar, en este caso la misma se encuentra en "/dev/sdf".

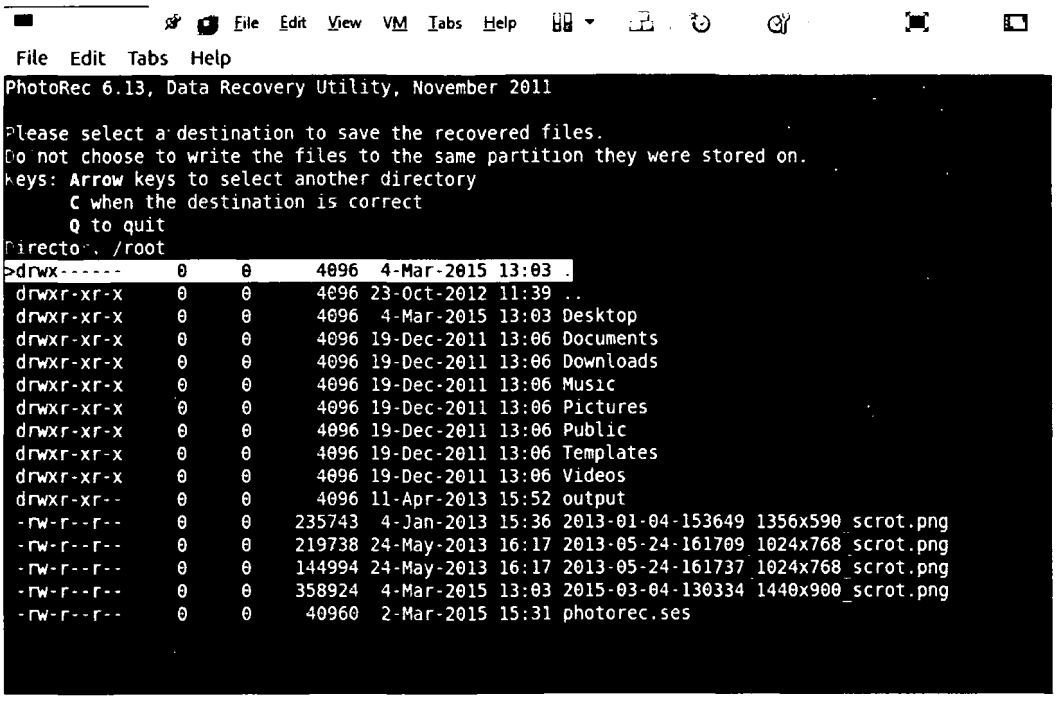
En el segundo paso, se debe elegir si se va a realizar un escaneo sobre una partición en particular o en todo el disco.

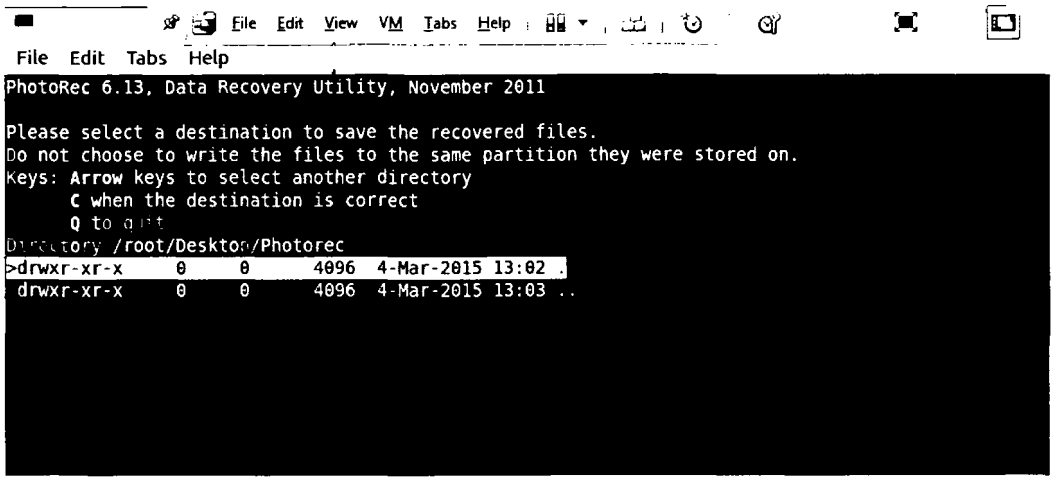


A continuación se selecciona el sistema de archivos que puede haber en la unidad.

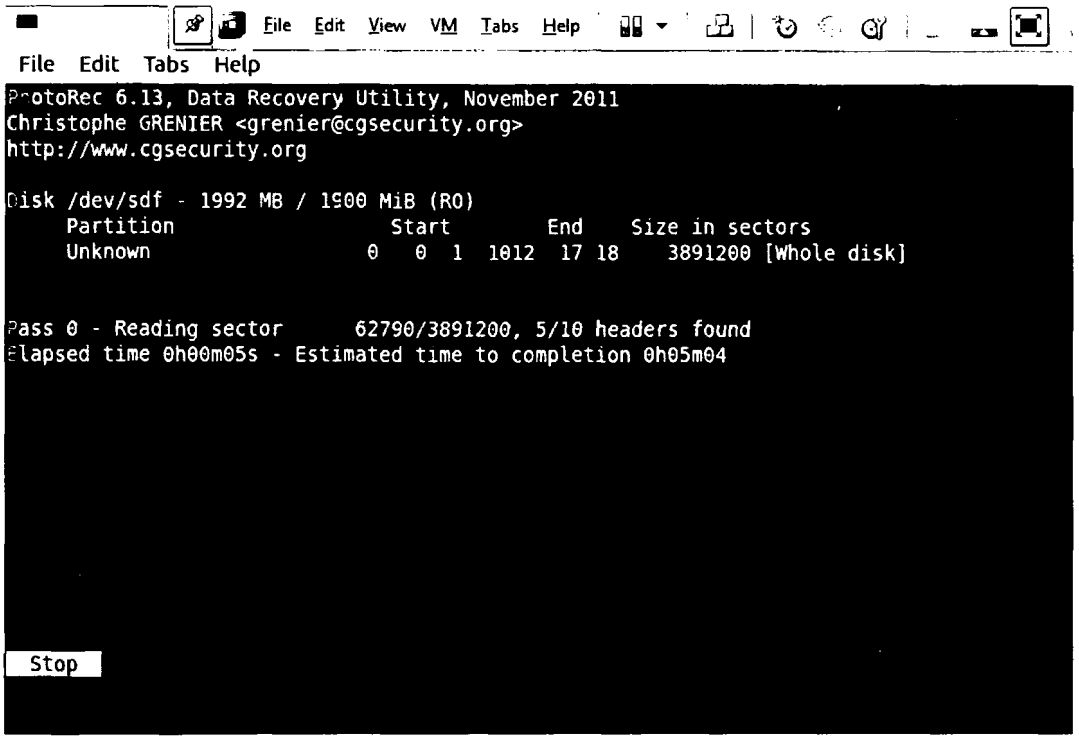


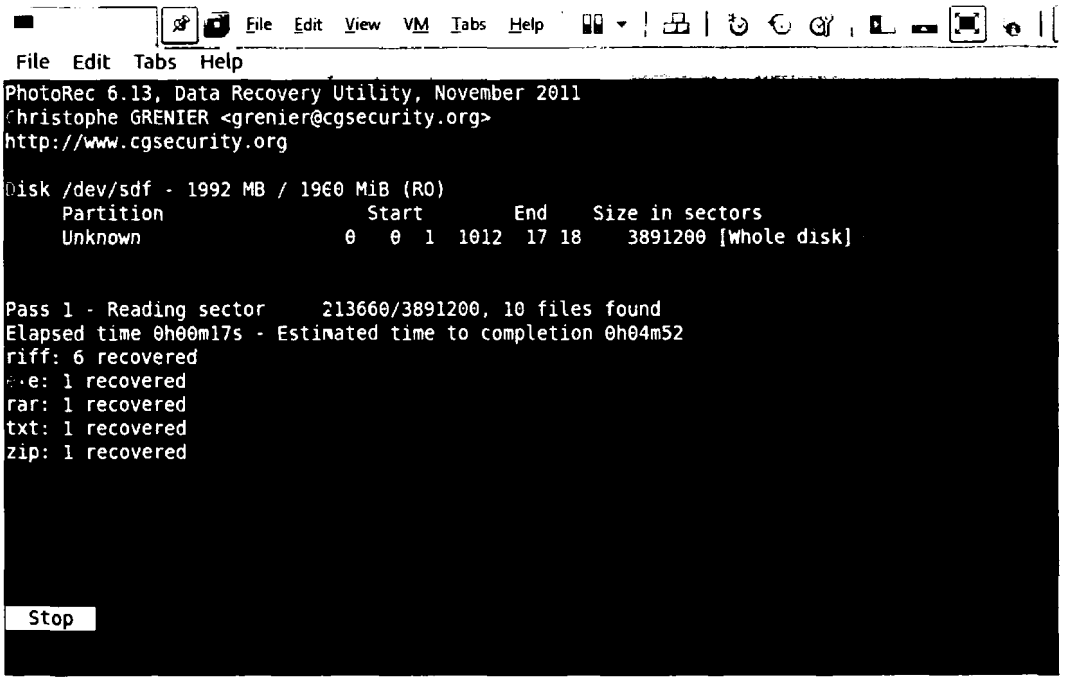
El siguiente paso es seleccionar el destino de los archivos recuperados, para el ejemplo se selecciona "/root/Desktop/Photorec".

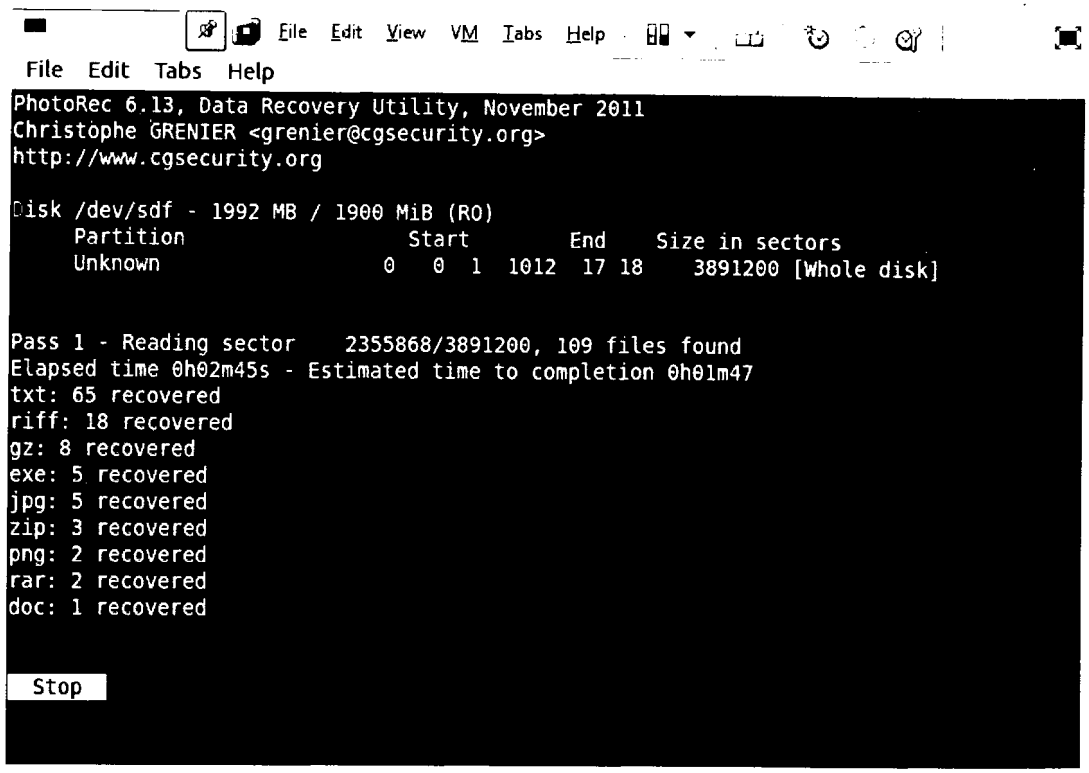




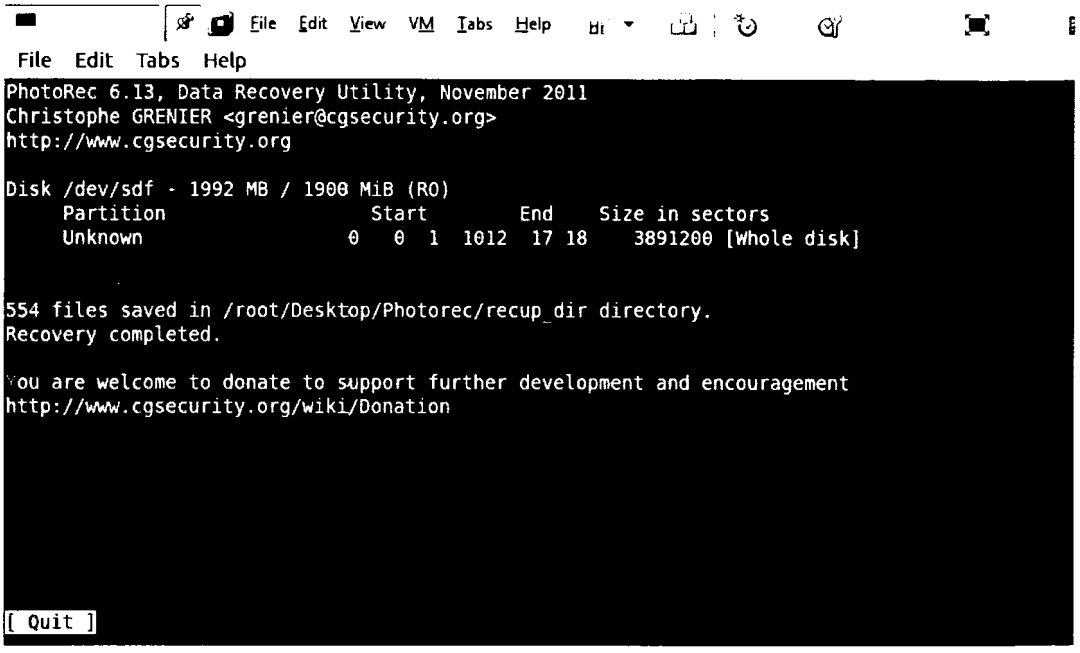
El proceso inicia mostrando un tiempo aproximado de duración. Y continua mostrando para cada extensión la cantidad de archivos que va recuperando.


File Edit View VM Tabs Help
File Edit Tabs Help
PhotoRec 6.13, Data Recovery Utility, November 2011
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
Disk /dev/sdf - 1992 MB / 1900 MiB (RO)
Partition Start End Size in sectors
Unknown 0 0 1 1012 17 18 3891200 [Whole disk]
Pass 0 - Reading sector 62790/3891200, 5/10 headers found
Elapsed time 0h00m05s - Estimated time to completion 0h05m04
Stop


File Edit View VM Tabs Help
File Edit Tabs Help
PhotoRec 6.13, Data Recovery Utility, November 2011
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
Disk /dev/sdf - 1992 MB / 1960 MiB (RO)
Partition Start End Size in sectors
Unknown 0 0 1 1012 17 18 3891200 [Whole disk]
Pass 1 - Reading sector 213660/3891200, 10 files found
Elapsed time 0h00m17s - Estimated time to completion 0h04m52
riff: 6 recovered
exe: 1 recovered
rar: 1 recovered
txt: 1 recovered
zip: 1 recovered
Stop



Una vez finalizado el proceso, muestra la cantidad total de archivos recuperados.



En este caso dentro de la carpeta "/root/Desktop/Photorec", se crearon dos carpetas "recup_dir.1" y "recup_dir.2", los cuales contienen los archivos recuperados. Los almacena todos juntos sin separarlos por extensión.

6.2.2. FOREMOST y SCALPEL

Este software de recuperación trabaja por línea de comandos, en la cual hay que determinar mínimamente, cuál es la unidad a analizar, la carpeta de destino, donde serán almacenados los archivos y el archivo de configuración que será utilizado.

El archivo de configuración es el que contiene todos los encabezados de archivos que serán buscados, y el cual puede ser editado para agregarle el encabezado hexadecimal del archivo que necesite ser recuperado.

Un ejemplo de la sintaxis sería:

foremost all –i /dev/sdf –o /root/Desktop/Foremost

"**all**": hace referencia a todas las extensiones que maneje,

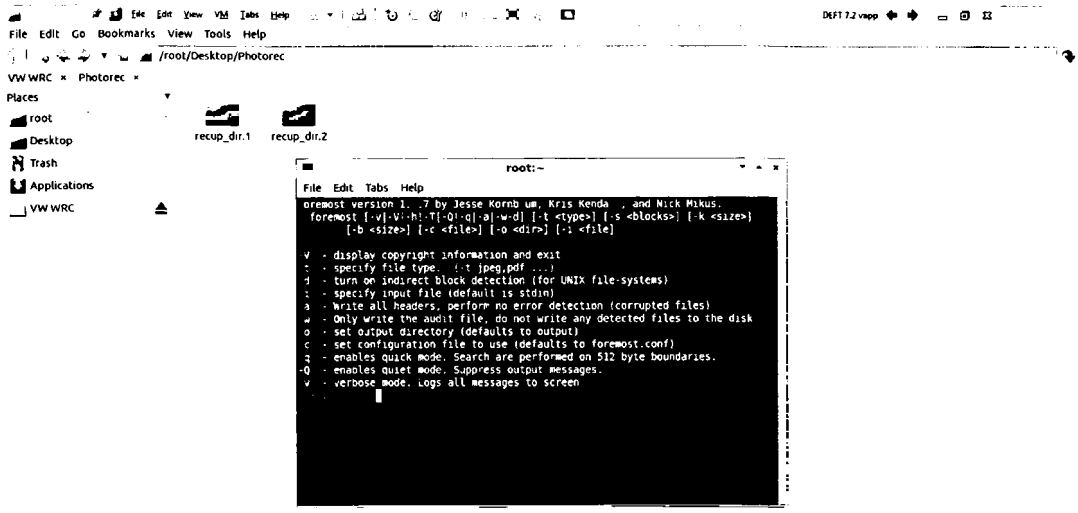
- **i**: hace referencia a la unidad a analizar,
- **o**: es el destino de los archivos recuperados.

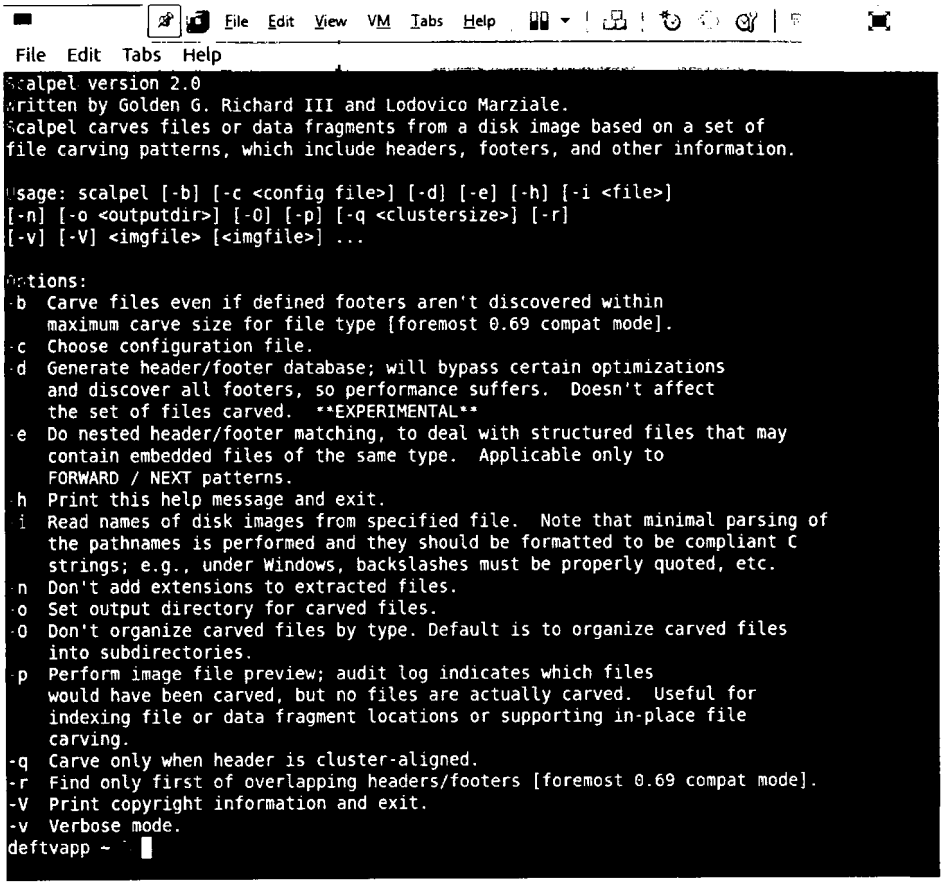
El archivo de configuración viene predeterminado, si se desea utilizar otro, debe indicarse:

scalpel -c /etc/scalpel.conf /dev/sdf -o /root/Desktop/scalpel

archivo de configuración — origen — destino de los archivos recuperados

En este caso si o si, se debe seleccionar el archivo de configuración. Los archivos de configuración son: foremost.conf y scalpel.conf y se encuentran en la carpeta "/etc"





Para el caso de archivos microsoft office docx, xlsx, etc; el programa foremost recupera mediante la elección de la extensión ZIP, debido a que este tipo de archivos poseen un método de compresión, en cambio el programa scalpel los reconoce pero con extensión zip haciendo más difícil su identificación.

6.3. Resumen

Empleando Encase

Debemos destacar como principal diferencia al momento de realizar un datacarving con la herramienta Encase, es su muy amigable entorno de trabajo, que hace sencilla dicha actividad de búsqueda.

Este entorno visual permite individualizar rápidamente las herramientas que ofrece el panel de control, ubicar botones de acceso directo, etc.

Mediante el empleo de ésta técnica de trabajo, se realizaron determinadas búsquedas de archivos por encabezado y extensión, observándose resultados distintos a los obtenidos con las aplicaciones libres.

Un ejemplo de lo anterior lo constituyó cuando se intentó buscar archivos de extensión xls y xlsx. En particular sobre la primera extensión (xls) el resultado fue más que positivo, pudiendo recuperar la totalidad de los archivos existentes. Para el caso de la extensión (xlsx), no fue posible concretar la obtención los archivos existentes en la memoria de estudio.

Empleando Software Libre

Una diferencia sustancial que existe con el software comercial es su entorno por comandos, que hace la tarea un poco aburrida y diferente a la herramienta anterior.

Una discrepancia que resultó a favor de las herramientas libres (Photorec, Foremost y Scalpel) fue la recuperación total de los archivos de extensión xls y xlsx que nos propusimos obtener.

Sin embargo ésta recuperación de archivos no se realiza en su totalidad, sino que cada elemento debe extraerse por separado, es decir hacerse archivo por archivo.

Esta última característica, hace que comparada ésta aplicación con la comercial sea mucho más lenta, en lo que respecta a extracción de archivos como evidencia.

7. CONCLUSIONES

De los diferentes análisis realizados empleando una u otra herramienta, tanto libre como comercial, se observaron características distintivas así como también semejanzas entre ambas.

El programa forense Encase ofrece un único entorno de trabajo en un mismo programa, pudiendo efectuar todos los pasos forenses en la misma aplicación, esto es: realizar la imagen forense, exportar archivos de evidencia, extraer cálculos de hash, presentación de informes de resultados, etc.

A diferencia de Encase, las herramientas libres, se hallan dispersas en un sinfín de aplicaciones, que si bien permiten obtener similares resultados al del software comercial, hace que el investigador se exija mucho más por hallarlas y en aprender el funcionamiento de cada herramienta de tipo "open source".

Encase presenta un entorno de trabajo sencillo y ameno, exigiendo a diferencia de las herramientas libres el uso de un potente ordenador para correr las aplicaciones y levantar la/las imágenes forenses como las búsquedas halladas.

Las aplicaciones de tipo libre no ofrecen un entorno de trabajo tan sencillo, requiriendo para su empleo de un ordenador no tan poderoso, al ser de base Linux, como si requiere el programa Encase.

Las normas ISO llenan un gran vacío en lo que respecta a contar con una norma internacional que regule la temática de informática forense, existiendo solamente como respaldo normas de diferentes países (NIST y otras más). A partir de la norma ISO/IEC 27037, se han unificado todas ellas en un único documento, el cual a futuro se espera brinde un abanico a toda esta disciplina.

Tanto la realización de imágenes forenses como la búsqueda de palabras clave, se observaron diferencias notorias en lo que refiere al resultado de las evidencias obtenidas como del tiempo de proceso insumido en ambos tipos de estudio, las que fueron señaladas en los

correspondientes apartados al final de los capítulos (Resumen), tanto para las herramientas comerciales como de las de tipo "open source".

Evidentemente una de las diferencias distintivas entre una y otra lo constituye el costo económico. Sin embargo poseer una herramienta comercial constituye un evidente ahorro de tiempo al poder analizar en profundidad un dispositivo de almacenamiento con una única suite de aplicaciones muy bien integradas.

Son diversas las temáticas para analizar dentro de la informática forense y que no se tocaron en este trabajo, pero que son interesantes de estudiar para futuros trabajos, como lo son: el análisis de archivos compuestos, los archivos virtuales, las técnicas avanzadas de búsquedas (grep), archivos de paginación, etc, etc.

8. GLOSARIO

Palabras	Significado
Encase	Herramienta comercial forense
Forense	todo tipo de medidas que aseguran la cadena de custodia
Hit	resultados o coincidencias obtenidos de búsquedas
Foremost	aplicación forense libre o gratuita
Hash	cálculo algorítmico
Imagen forense	copia bit a bit efectuada de un disco
Write blocker	bloqueador de escritura
FTK	Herramienta comercial forense
Protocolo	Procedimientos específicos o conjunto de acciones establecidos en un plan de trabajo.

9. ANEXOS

El sitio que ofrece el NIST es una excelente página web donde hallaremos un sinfín de recursos útiles, no sólo en lo que se refiere a publicaciones sino también a la información respecto al testeo de herramientas forenses que se realizan continuamente y se detallan en ese sitio. Ejemplos de publicaciones realizados por el NIST son los siguientes:

- **http://csrc.nist.gov/publications/nistpubs/800-72/sp800-72.pdf**

NIST
National Institute of
Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-72
Sponsored by the Department
of Homeland Security

Guidelines on PDA Forensics

Recommendations of the National Institute of Standards and Technology

Wayne Jansen
Rick Ayers

- **http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf**

NIST Special Publication 800-101
Revision 1

Guidelines on Mobile Device Forensics

Rick Ayers
Sam Brothers
Wayne Jansen

http://dx.doi.org/10.6028/NIST.SP.800-101r1

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

- http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-86

Guide to Integrating Forensic Techniques into Incident Response

Recommendations of the National Institute of Standards and Technology

Karen Kent
Suzanne Chevalier
Tim Grance
Hung Dang

10. BIBLIOGRAFÍA ESPECÍFICA

1. Computación Forense: Descubriendo los rastros Informáticos. Jeimy Cano. Editorial ALFAOMEGA.

2. ENCASE Computación Forense I. Professional Development and Training. Guidance Software, Inc. 2008.

3. ENCASE Computación Forense II. Professional Development and Training. Guidance Software, Inc. 2011.

4. http://www.gfi.com/blog/top-20-free-digital-forensic-investigation-tools-for-sysadmins/

5. http://www.cftt.nist.gov/