INFORMÁTICA FORENSE : GENERALIDADES, ASPECTOS TÉCNICOS Y HERRAMIENTAS

Autores : Óscar López, Haver Amaya, Ricardo León

Coautora : Beatriz Acosta

Universidad de Los Andes
Bogotá, Colombia
{os-lopez, h-amaya, ri-leon, bacosta}@uniandes.edu.co

Abstracto. El presente documento de investigación pretende mostrar una panorámica general de la informática forense, resaltando en primer lugar su importancia, sus objetivos y usos. Acto seguido, se explica brevemente el concepto de evidencia informática, seguida de los detalles técnicos del almacenamiento de ésta en medios magnéticos y las técnicas para eliminarla de manera segura. A continuación se muestran algunos de los tipos de programas y herramientas usadas por los investigadores forenses, haciendo especial énfasis en EnCase, una de tales herramientas. Para finalizar, se presentan algunas de las dificultades encontradas por los investigadores forenses en la actualidad, y se muestran algunas referencias a casos de investigación de la vida real.

1 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/o al uso que se le da a ésta, al desarrollo de nuevos espacios donde es usada (por Ej. el Internet), y al extenso uso de computadores por parte de las compañías de negocios tradicionales (por Ej. bancos). 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 información forma tal que no puede ser recolectada o usada como prueba utilizando medios comunes, se deben utilizar mecanismos diferentes a los tradicionales. Es de aquí que surge el estudio de la computación forense como una ciencia relativamente nueva.

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. 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.

En este escrito se pretende mostrar una panorámica muy general de la Informática Forense, explicando en detalle algunos aspectos técnicos muchas veces olvidados en el estudio de esta ciencia.

2 Informática Forense

2.1 ¿Qué es la Informática Forense?

Según el FBI, la informática (o computación) forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional. [10]

Desde 1984, el Laboratorio del FBI y otras agencias que persiguen el cumplimiento de la ley empezaron a desarrollar programas para examinar evidencia computacional.

2.2 Importancia de la Informática Forense

"High-tech crime is one of the most important priorities of the Department of Justice" [11]. Con esta frase podemos ver cómo poco a poco los crímenes informáticos, su prevención, y procesamiento se vuelven cada vez más importantes. Esto es respaldado por estudios sobre el número de incidentes reportados por las empresas debido a crímenes relacionados con la informática (ver [12]).

Sin embargo, la importancia real de la informática forense proviene de sus objetivos.

2.2.1 Objetivos de la Informática Forense

La informática forense tiene 3 objetivos, a saber:

1. La compensación de los daños causados por los criminales o intrusos.
2. La persecución y procesamiento judicial de los criminales.
3. 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.

2.2.2 Usos de la Informática Forense [16]

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:

1. 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.
2. Litigación Civil: Casos que tratan con fraude, discriminación, acoso, divorcio, pueden ser ayudados por la informática forense.
3. Investigación de Seguros: La evidencia encontrada en computadores, puede ayudar a las compañías de seguros a disminuir los costos de los reclamos por accidentes y compensaciones.
4. 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.
5. Mantenimiento de la ley: La informática forense puede ser usada en la búsqueda inicial de órdenes judiciales, así como en la búsqueda de información una vez se tiene la orden judicial para hacer la búsqueda exhaustiva.

2.3 La Investigación Tecnológica

Los investigadores de la computación forense usan gran cantidad de técnicas para descubrir evidencia, incluyendo herramientas de software que automatizan y aceleran el análisis computacional.

2.3.1 Evidencia Digital [7]

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 *checksums* o *hash* MD5. [1]

La IOCE (International Organization On Computer Evidence)[3] define los siguientes cinco puntos como los principios para el manejo y recolección de evidencia computacional:

1. Sobre recolectar evidencia digital, las acciones tomadas no deben cambiar por ningún motivo esta evidencia.
2. Cuando es necesario que una persona tenga acceso a evidencia digital original, esa persona debe ser un profesional forense.
3. Toda la actividad referente a la recolección, el acceso, almacenamiento o a la transferencia de la evidencia digital, debe ser documentada completamente, preservada y disponible para la revisión.
4. Un individuo es responsable de todas las acciones tomadas con respecto a la evidencia digital mientras que ésta esté en su posesión.
5. Cualquier agencia que sea responsable de recolectar, tener acceso, almacenar o transferir evidencia digital es responsable de cumplir con estos principios.

Además definen que los principios desarrollados para la recuperación estandarizada de evidencia computarizada se deben gobernar por los siguientes atributos: [2]

1. Consistencia con todos los sistemas legales.
2. Permitir el uso de un leguaje común.
3. Durabilidad.
4. Capacidad de cruzar límites internacionales.
5. Capacidad de ofrecer confianza en la integridad de la evidencia.
6. Aplicabilidad a toda la evidencia forense.

2.3.2 Grabación en Medios Magnéticos : Principios Físicos [26]

En general, los medios de almacenamiento magnético se basan directamente en cuatro fenómenos físicos:

A. Una corriente eléctrica produce un campo magnético
B. Algunos materiales se magnetizan con facilidad cuando son expuestos a un campo magnético débil. Cuando el campo se apaga, el material de desmagnetiza rápidamente. Se conocen como *Materiales Magnéticos Suaves*.
C. En algunos materiales magnéticos suaves, la resistencia eléctrica cambia cuando el material es magnetizado. La resistencia regresa a su valor original cuando el campo magnetizante es apagado. Esto se llama *Magneto-Resistencia*, o efecto MR. La Magneto-Resistencia Gigante, o efecto GMR, es mucho mayor que el efecto MR y se encuentra en sistemas específicos de materiales de películas delgadas.
D. Otros materiales se magnetizan con dificultad (es decir, requieren de un campo magnético fuerte), pero una vez se magnetizan, mantienen su magnetización cuando el campo se apaga. Se llaman *Materiales Magnéticos Duros*, o *Magnetos Permanentes*.

Estos cuatro fenómenos son explotados por los fabricantes de cabezas grabadoras magnéticas, que leen y escriben datos, para almacenar y recuperar datos en unidades de disco, de cinta y otros dispositivos de almacenamiento magnético.

Aplicaciones en almacenamiento de datos:

- Cabezas de Escritura : Cabezas usadas para escribir bits de información en un disco magnético giratorio, dependen de los fenómenos A y B para producir y controlar campos magnéticos fuertes.

- Cabezas de lectura : Éstas dependen de los fenómenos A, B y C y son sensibles a los campos magnéticos residuales de los medios de almacenamiento magnetizados (D).

- Medios de Almacenamiento : (Como discos de computador) Los medios de almacenamiento magnético son magnetizados de manera permanente en una dirección (Norte o Sur) determinada por el campo de escritura. Estos medios explotan el fenómeno D.

2.3.2.1 Escribiendo Datos Magnéticos

En la figura 1 se muestra un esquema simplificado de una cabeza de escritura. La vista superior de una cabeza de escritura (izquierda) muestra un rollo espiral, envuelto entre dos capas de material magnético suave; a la derecha está un corte transversal de esta cabeza, vista de lado. Nótense dos detalles sobre esta figura: En el extremo inferior, hay un espacio entre las capas, y en el extremo superior, las capas están unidas. Las capas superior e inferior de material magnético se magnetizan con facilidad cuando fluye una corriente eléctrica en el rollo espiral, de tal forma que estas capas se vuelven los polos Norte y Sur magnéticos de un pequeño electro-magneto. (En una cabeza real, la distancia desde el espacio hasta la parte superior del rollo es de aproximadamente 30 mm).

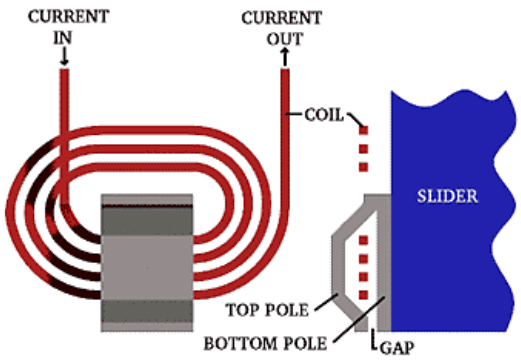

Fig. 1. Una cabeza de escritura [26]

Los polos N-S en el extremo de la separación de la cabeza de escritura concentran el campo para hacer de esta región el “extremo de negociación”, que es el área en donde el campo de escritura sale al espacio por fuera de la cabeza. Cuando un medio

de almacenamiento magnético (por ejemplo, un disco giratorio en un computador) es ubicado muy cerca de la cabeza de escritura, el material magnético duro en la superficie del disco queda magnetizado de manera permanente (escrito) con una polaridad que corresponde a la del campo de escritura. Si la polaridad de la corriente eléctrica se invierte, la polaridad magnética en la separación también se invierte.

Los computadores almacenan datos en un disco giratorio en la forma de dígitos binarios, o bits transmitidos a la unidad de disco en una secuencia de tiempo correspondiente a los dígitos binarios (*bits*) uno y cero. Estos bits son convertidos en una onda de corriente eléctrica que es transmitida por medio de cables al rollo de la cabeza de escritura. Este proceso se esquematiza en la figura 2. En su forma más simple, un *bit* uno corresponde a un cambio en la polaridad de la corriente, mientras que un *bit* cero corresponde a una ausencia de cambio en la polaridad de la corriente de escritura. Entonces, un disco en movimiento es magnetizado en la dirección positiva (Norte) para una corriente positiva y es magnetizado en la dirección negativa (Sur) para un flujo de corriente negativo. En otras palabras, los unos almacenados aparecen en donde ocurre una inversión en la dirección magnética en el disco, y los ceros residen entre los unos.

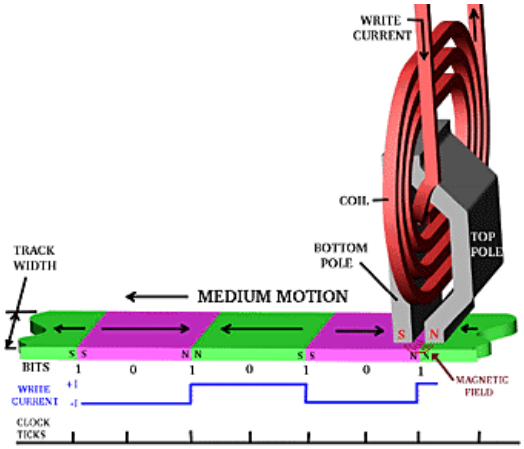

Fig. 2. Escribiendo datos en un medio de almacenamiento [26]

Un reloj de regulación está sincronizado con la rotación del disco y existen *celdas de bit* para cada *tick* del reloj; algunas de estas celdas de bits representarán un *uno* (una inversión en la dirección magnética, tal como N cambiando a S o S cambiando a N) y otras representarán *ceros* (polaridad N constante o S constante). Una vez escritos, los bits en la superficie del disco quedan magnetizados permanentemente en una dirección o la otra, hasta que nuevos patrones sean escritos sobre los viejos. Existe un campo magnético relativamente fuerte directamente sobre la localización de los *unos* y su fuerza se desvanece rápidamente a medida que la cabeza de grabación se aleja. Un movimiento significativo en cualquier dirección que se aleje de un *uno* causa una dramática pérdida en la fuerza del campo magnético, lo que implica que

para detectar bits de datos de manera confiable, es extremadamente importante que las cabezas de lectura vuelen muy cerca de la superficie del disco magnetizado.

2.3.2.2 Leyendo Datos Magnéticos

En la actualidad, las cabezas de lectura leen datos magnéticos mediante resistores magnéticamente sensitivos llamados *Válvulas Spin* que explotan el efecto GMR. Estas cabezas *GMR/Válvula Spin* son situadas muy cerca del disco de almacenamiento magnético rotatorio, exponiendo el elemento GMR a los campos magnéticos de *bit* previamente escritos en la superficie del disco. Si la cabeza GMR se aleja ligeramente del disco (2 o 3 millonésimas de pulgada) la intensidad del campo cae por fuera de un nivel útil, y los datos magnéticos no pueden ser recuperados fielmente.

Cuando una corriente atraviesa el elemento GMR, los cambios en la resistencia (correspondientes a los cambios en los estados magnéticos que surgen de los bits escritos N y S) son detectados como cambios en el voltaje. Estas fluctuaciones de voltaje –es decir, la señal- son conducidas a las terminales sensoras del GMR. Sin embargo, el ruido eléctrico está presente en todos los circuitos eléctricos (las cabezas GMR no son la excepción), por lo que la señal combinada con el ruido de un lector GMR son enviados por medio de cables los circuitos electrónicos de la unidad de disco, para decodificar la secuencia de tiempo de los impulsos (y los espacios entre los impulsos) en unos y ceros binarios. El proceso de lectura, incluyendo el indeseable pero siempre presente ruido, se esquematiza en la figura 3.

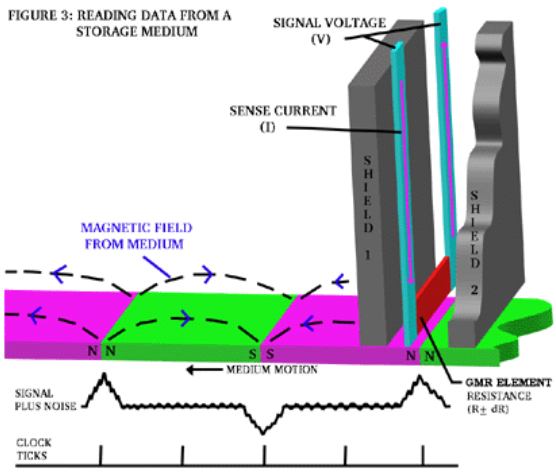

Fig. 3. Leyendo datos desde un medio de almacenamiento [26]

2.3.3 Análisis de Discos

La clave de la computación forense es el análisis de discos duros, disco extraíbles,

CDs, 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.

2.3.3.1 *File Slack* [4]

Los archivos son creados en varios tamaños dependiendo de lo que contengan. Los sistemas basados en DOS, Windows 95/98/ME/XP y Windows NT/2000 almacenan los archivos en bloques de tamaño fijo llamados *clusters*, en los cuales raramente el tamaño de los archivos coinciden perfectamente con el tamaño de uno o muchos *clusters*.

El espacio de almacenamiento de datos que existe desde el final del archivo hasta el final del *cluster* se llama "file slack". Los tamaños de los *clusters* varían en longitud dependiendo del sistema operativo involucrado y, en el caso de Windows 95/98/ME/XP, del tamaño de la partición lógica implicada.

Un tamaño más grande en los *clusters* significan más *file slack* y también mayor pérdida de espacio de almacenamiento. Sin embargo, esta debilidad de la seguridad del computador crea ventajas para el investigador forense, porque el *file slack* es una fuente significativa de evidencia y pistas.

El *file slack*, potencialmente contiene octetos de datos aleatoriamente seleccionados de la memoria del computador. Esto sucede porque DOS/Windows escribe normalmente en bloques de 512 bytes llamados sectores. Los *clusters* están compuestos por bloques de sectores, si no hay suficientes datos en el archivo para llenar el ultimo sector del archivo, DOS/Windows diferencia hacia arriba(los datos) completando el espacio restante con datos que se encuentran en ese momento en la memoria del sistema.

2.3.3.2 Archivo *Swap* de Windows [4]

Los sistemas operativos Microsoft Windows utilizan un archivo especial como un "cuaderno de apuntes" para escribir datos cuando se necesita memoria de acceso aleatorio adicional. En Windows 95/98/ME/XP, a estos archivos se les conoce como Archivos *Swap* de Windows. En Windows NT/2000 se conocen como directorios de página de Windows pero tiene esencialmente las mismas características que los de Win9x.

Los archivos de intercambio son potencialmente enormes y la mayoría de los usuarios de PC son inconscientes de su existencia. El tamaño de estos archivos puede extenderse desde 20MB a 200MB, el potencial de estos es contener archivos sobrantes del tratamiento de los procesadores de texto, los mensajes electrónicos, la actividad en Internet (*cookies*, etc), *logs* de entradas a bases de datos y de casi cualquier otro trabajo que haya ocurrido durante las últimas sesiones. Todo esto genera un problema de seguridad, porque el usuario del computador nunca es informado de este almacenamiento transparente.

Los Archivos *Swap* de Windows actualmente proporcionan a los especialistas en computación forense pistas con las cuales investigar, y que no se podrían conseguir de otra manera.

2.3.3.3 *Unallocated File Space* [6]

Cuando los archivos son borrados o suprimidos en DOS, Win9x, WinNT/2000, el contenido de los archivos no es verdaderamente borrado. A menos que se utilice algún software especial que ofrezca un alto grado de seguridad en el proceso de eliminación, los datos "borrados", permanecen en un área llamada espacio de almacenamiento no-asignado (*Unallocated File Space*). Igual sucede con el *file slack* asociado al archivo antes de que éste fuera borrado. Consecuentemente, siguen existiendo los datos, escondidos pero presentes, y pueden ser detectados mediante herramientas de software para el análisis de la computación forense.

2.4 Eliminación de datos

Hasta el momento, se ha hablado de la forma de almacenar y leer los datos en un disco de computador, sin embargo pueden darse casos legítimos en donde sea necesario *destruir* información sin dejar rastro alguno. En este numeral, se describen las prácticas adecuadas para la eliminación de información.

2.4.1 Eliminación de Datos en un Medio Magnético

Borrar de manera definitiva los datos en un medio magnético tiene toda una problemática asociada. Como se vio en una sección anterior, la información es escrita y leída aprovechando las características de magnetización de un material determinado.

Sin embargo, y dependiendo del medio usado (unidades de disco, cintas, diskettes, etc.) , el proceso de eliminación total de los datos se ve afectado por diversos factores. El Departamento de Defensa de los Estados Unidos (DoD) cuenta con toda una serie de recomendaciones sobre cómo "sanitizar" un medio magnético, esto es, el proceso por el cual la información clasificada es removida por completo, en donde ni siquiera un procedimiento de laboratorio con las técnicas conocidas a la fecha o un análisis pueda recuperar la información que antes estaba grabada.[28] Aunque en un comienzo los procedimientos a seguir pueden parecer algo paranoicos, la (relativa) facilidad con la que se puede recuperar información que se creía borrada hace necesario tomar medidas extremas a la hora de eliminar datos confidenciales o comprometedores. En enero de 1995, el DoD publicó un documento, el "National Industrial Security Program Operating Manual" (NISPOM), más comúnmente referenciado como "DoD 5220.22-M" [27], que detalla toda una serie de procedimientos de seguridad industrial, entre ellos, cómo eliminar datos contenidos en diferentes medios.

A partir de los lineamientos presentes en 5220.22-M , otro organismo estadounidense, el Defense Scurity Service, publicó una "Matriz de Sanitización y Borrado" que explica de manera práctica los pasos a seguir para remover por completo información sensitiva. En las siguientes secciones se hacen algunas precisiones técnicas, y en el apéndice A se muestra y se explica la Matriz.

2.4.1.1 *Degaussing* de Medios Magnéticos [28]

La Matriz de Limpieza y Sanitización es una acumulación de métodos conocidos y aprobados para limpiar y/o sanitizar diversos medios y equipo. Cuando NISPOM fue publicado, el Rango Extendido Tipo II, Tipo III y los *degaussers* de Propósito Especial no existían. Esto resultaba en la necesidad de destruir todos los medios con un factor de coercividad (cantidad de fuerza eléctrica requerida para reducir la fuerza magnética grabada a cero) mayor que 750 oersteds (unidad que mide la fuerza magnetizante necesaria para producir una fuerza magnética deseada a lo largo de una superficie) y la mayoría de discos magnéticos cuando ya no fueran necesarios como soporte para una misión clasificada. Ahora, la "National Security Agency norteamericana" (NSA) ha evaluado *degaussers* de cinta magnética que satisfacen los requerimientos del gobierno para sanitizar cintas magnéticas de hasta 1700 oersteds.

Las cintas magnéticas se encuentran divididas en Tipos. La cinta magnética de Tipo I tiene un factor de coercividad que no excede los 350 oersteds y puede ser usada para sanitizar (*degauss*) todos los medios de Tipo I .La cinta magnética de Tipo II tiene un factor de coercividad entre 350 y 750 oersteds y puede ser usada para sanitizar todos los medios Tipo I y II. La cinta magnética Tipo II de Rango Extendido tiene un factor de coercividad entre 750 y 900 oersteds y puede ser usada para sanitizar todos los medios Tipo I, Tipo II y Rango Extendido. Finalmente, las cintas magnéticas Tipo III, comúnmente conocidas como cintas de alta energía (por ejemplo, cintas de 4 ó 8mm), tiene un factor de coercividad actualmente identificado como entre 750 y 1700 oersteds y puede ser usada para sanitizar todos los tipos de cintas magnéticas.

Para sanitizar (*degauss*) todos los medios de disco, rígidos o flexibles (por ej., *diskettes*, Bernoulli, Syquest y unidades de Disco Duro) se deben usar *degaussers* de Unidad de Disco. Para este tipo de dispositivos la NSA tiene una nueva categoría de *degaussers*, conocida como *Degaussers* de Propósito Especial.

DSS, como todas las agencias del DoD, referencia el "Information Systems Security Products and Services Catalog" como guía de sanitización de memoria y medios. NSA publica el "Information Systems Security Products and Services Catalog" entre sus productos y servicios de seguridad para sistemas de información. La lista de productos *degausser* (DPL) está dedica a los *degaussers* de discos y cintas magnéticas. La DPL hace un excelente trabajo identificando los fabricantes de *degaussers* y los diferentes tipos de éstos.

2.4.2 Eliminación de Datos en CDs [20]

Los datos de un CD están almacenados en la parte superior del CD por medio de una capa reflectiva que es leída por un láser. Los CDs ofrecen buenas alternativas para almacenar información por largos periodos de tiempo, pero puede ser necesario destruirlos. Se mencionan algunos medios para hacer esto:

1. Retiro de la lámina reflectiva : Se puede retirar la lámina con algún elemento cortante, sin embargo se debe destruir la lámina reflectiva, y aún así pueden quedar algunos rastros de datos en el policarbonato.
2. Cortar en pedazos : Con una cortadora industrial de papel, el CD podría ser destruido, sin embargo, la lámina reflectiva podría separarse del CD y no ser cortada correctamente.
3. Destruir el CD por medios químicos : Una posible alternativa es introducir el CD en Acetona, lo cual dejaría la lámina superior inservible, sin embargo es posible que la lámina de policarbonato aún contenga algunos rastros de información.
4. Destrucción por Incineración : Probablemente es el método más rápido y eficiente, pero es realmente nocivo para el medio ambiente. El humo del policarbonato puede ser perjudicial para la salud de las personas.
5. Destrucción por medio de un horno microondas : Introduciendo el CD en un microondas por unos 3 segundos puede destruir gran parte del CD, sin embargo no todas las partes serán destruidas. Este método no se recomienda, especialmente porque puede dañar el horno debido a los campos magnéticos que usa el horno y que pueden causar un cortocircuito debido a que el CD contiene metales.
6. Reescritura : Para los CDs re-escribibles, es posible volverlos a escribir de tal forma que el proceso dañe los datos. Sin embargo, no se sabe si por mecanismos especiales sea posible recuperar la información.
7. Rayado Simple : A menos que uno quiera ser realmente precavido, la forma mas fácil de destruir un CD es rayando la parte superior. La razón por la que se debe rayar la parte superior es porque es esta la que mantiene los datos. Si es rayada la parte inferior es fácil recuperar la capa y corregir el problema, utilizando productos comerciales para recuperar CDs.

2.5 Pasos para la Recolección de Evidencia [22], [23]

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:

2.5.1 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. Lo primero que se debe preguntar el investigador es qué partes se deben buscar o investigar.

2.5.2 Cuidados en la Recolección de Evidencia [19]

La recolección de evidencia informática es un aspecto frágil del 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.

2.6 Herramientas de Investigación Forense

En la actualidad existen cientos de herramientas [14], las cuales se pueden clasificar en cuatro grupos principales.

2.6.1 Herramientas para la Recolección de Evidencia

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

1. La gran cantidad de datos que pueden estar almacenados en un computador.
2. La variedad de formatos de archivos, los cuales pueden variar enormemente, aún dentro del contexto de un mismo sistema operativo.

3. La necesidad de recopilar la información de una manera exacta, y que permita verificar que la copia es exacta.
4. Limitaciones de tiempo para analizar toda la información.
5. Facilidad para borrar archivos de computadores.
6. Mecanismos de encripción, o de contraseñas.

2.6.1.1 EnCase [8]

EnCase es un ejemplo de herramientas de este tipo. Desarrollada por Guidance Software Inc. (http://www.guidancesoftware.com), 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 mismos tiempo, examinando la 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 graficas 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 sospechosos 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 y 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 (Sun, Open BSD), CD-ROM, y los sistemas de archivos DVD-R. 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 *cluster*, permitiendo al investigador examinar inmediatamente y determinar cuándo el archivo reescrito fue creado. Los archivos *Swap* y *Print Spooler* son 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 y 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 *.gif* y *.jpg* 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 sea soportado por EnCase.

EnCase es un software costoso, y en Estados Unidos los costos se dividen así:

- Gobierno y Educación US$1,995
- Sector Privado US$2,495

Actualmente EnCase se encuentra en su versión 3.0.

2.6.2 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 *key loggers* o 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 [15].

2.6.2.1 KeyLogger [9]

"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.

2.6.3 Herramientas de Marcado de documentos

Un aspecto interesante es el de marcado de documentos; en los casos de robo de información, es posible, mediante el uso de herramientas, marcar software para poder detectarlo fácilmente.

El foco de la seguridad está centrado en la prevención de ataques [13]. Algunos sitios que manejan información confidencial o sensitiva, tienen mecanismos para validar el ingreso, pero, debido a que no existe nada como un sitio 100% seguro, se debe estar preparado para incidentes.

2.6.4 Herramientas de Hardware

Debido a que el proceso de recolección de evidencia debe ser preciso y no debe modificar la información se han diseñado varias herramientas como DIBS "Portable Evidence Recovery Unit" (Ver [17]).

2.7 Dificultades del Investigador Forense [18]

El investigador forense requiere de varias habilidades que no son fáciles de adquirir, es por esto que el usuario normal se encontrará con dificultades como las siguientes:

1. Carencia de software especializado para buscar la información en varios computadores.
2. Posible daño de los datos visibles o escondidos, aún sin darse cuenta.
3. Será difícil encontrar toda la información valiosa.
4. Es difícil adquirir la categoría de 'experto' para que el testimonio personal sea válido ante una corte.
5. Los errores cometidos pueden costar caro para la persona o la organización que representa.
6. Dificultad al conseguir el software y hardware para guardar, preservar y presentar los datos como evidencia.
7. Falta de experiencia para mostrar, reportar y documentar un incidente computacional.
8. Dificultad para conducir la investigación de manera objetiva.
9. Dificultad para hacer correctamente una entrevista con las personas involucradas.
10. Reglamentación que puede causar problemas legales a la persona.

Es por esto que, antes de lanzarse a ser un investigador forense, se necesita bastante estudio y experiencia, entre otras cosas, y si no se cumple con los requisitos, en caso de un accidente es aconsejable llamar a uno o varios expertos.

3 Resultados

En este artículo se logró mostrar una panorámica muy general de lo que es la computación forense, discutiendo algunos temas muchas veces ignorados pero de gran interés en el área, tales como los principios físicos de la grabación en medios magnéticos, las técnicas apropiadas de borrado permanente de datos y una clasificación general de las herramientas a disposición del investigador forense, en particular del famoso EnCase.

4 Conclusiones

En últimas se logró dar una mirada al amplio e interesante tema de la informática forense, útil para quien desee encontrar en un solo texto las generalidades de esta ciencia, con énfasis en detalles técnicos que rara vez son mencionados en escritos similares.

Las limitaciones naturales de un trabajo de este tipo consisten en la imposibilidad de profundizar demasiado en un tema en particular, puesto que lo que se pretendía era dar una visión amplia de la naciente ciencia de la computación forense. En trabajos posteriores se podría mirar con mayor detenimiento alguno de los temas tocados, pero por el momento invitamos al lector que desee profundizar más sobre el tema a que consulte nuestra bibliografía.

Referencias

Las siguientes direcciones electrónicas fueron consultadas entre el 2 y el 5 de julio de 2001.

1. http://www.forensics-intl.com/art12.html
2. http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm
3. http://www.ioce.org/ioceprinc.shtml
4. http://www.forensics-intl.com/def6.html
5. http://www.forensics-intl.com/def7.html
6. http://www.forensics-intl.com/def8.html
7. http://www.forensics-intl.com/def3.html
8. http://www.encase.com/html/how_encase_works.html
9. http://www.keylogger.com/
10. http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm
11. Janet Reno, U.S. Attorney General, Oct 28, 1996
12. http://www.cert.org/stats/cert_stats.html
13. http://www.softmart.com/connected/Spring2001/forensics.htm
14. http://www.itl.nist.gov/div897/docs/computer_forensics_tools_verification.html
15. http://www.softmart.com/connected/Spring2001/forensics2.htm
16. http://www.softmart.com/connected/Spring2001/forensics.htm
17. http://www.computer-forensics.com/products/welcome.html?peru.html

18. http://www.compukirk.com/kk00010.html
19. http://www.usdoj.gov/criminal/cybercrime/search_docs/sect3.htm
20. http://www.cdrfaq.org/faq07.html#S7-8
21. http://www.itworld.com/Career/1969/ITW0302weinstein/
22. http://www.usdoj.gov/criminal/cybercrime/search_docs/toc.htm
23. http://www.auscert.org.au/Information/Auscert_info/Papers/win-UNIX-system_compromise.html
24. http://www.terra.com.co/
25. http://www.khaleejtimes.com/uae.htm#story1
26. http://www.readrite.com/html/magbasic.html
27. http://www.dss.mil/isec/nispom.htm
28. http://www.dss.mil/infoas/magnetic_tape_degaussing.doc
29. http://www.dss.mil/infoas/clearing_and_sanitization_matrix.doc

Apéndice A : Matriz de Limpieza y Sanitización

Tabla 1 : Matriz de Limpieza y Sanitización **[29]**

Medio	Limpieza					Sanitización															
Cinta Magnética																					
Tipo I	a						b									m					
Tipo II	a						b									m					
Tipo III	a						b									m					
Disco Magnético																					
Bernoullis	a	c					b									m					
Disco Flexible	a	c					b									m					
Disco Rígido no-removible		c				a			d							m					
Disco Rígido removible	a	c				a			d							m					
Disco Óptico																					
Read Many, Write Many		c														m					
Read Only																m	n				
Write Once, Read Many (Worm)																m	n				
Memoria																					
Dynamic Random Access Memory (DRAM)		c	h					c				h				m					
Electronically Alterable PROM (EAPROM)				i										j		m					
Electronically Erasable PROM (EEPROM)				i							g					m					
Erasable Programmable ROM (EPROM)					k			c							l	m					l luego c
Flash EPROM (FEPROM)				i				c					i			m					c luego i
Programmable ROM (PROM)		c														m					
Magnetic Bubble Memory		c				a		c								m					
Magnetic Core Memory		c				a				e						m					
Magnetic Plated Wire		c						c			f					m					c y f
Magnetic Resistive Memory		c														m					
NonVolatile RAM (NOVRAM)		c	h					c				h				m					
Read Only Memory (ROM)																m					
Synchronous DRAM (SDRAM)		c	h					c				h				m					
Static Ryom Access Memory (SRAM)		c	h					c			f	h				m					c y f
Equipos																					
Monitor			h																	q	
Impresora de Impacto			h									h							p		p luego h
Impresora Láser			h									h						o			o luego h

a. Degauss con un degausser Tipo I, II o III.
b. Degauss con el mismo Tipo (I, II o III) de degausser.
c. Sobreescriba todos los lugares direccionables con un sólo caracter.
d. ESTE MÉTODO NO ES APROBADO PARA SANITIZAR MEDIOS QUE CONTENGAN INFORMACIÓN *TOP SECRET*.
    1. Antes de adquirir un producto de sanitización, se deben analizar cuidadosamente los costos totales asociados con la sobreescritura/sanitización. Dependiendo del ambiente del contratador, el tamaño del drive y las diferencias en los

tiempos individuales de los productos sobre los que se va a efectuar la sanitización, podría ser que la destrucción de los medios fuera la elección más económica como método de sanitización.

2. Sobreescribir todas las locaciones direccionables con un carácter, luego con su complemento. Verificar que el carácter "complemento" fue escrito exitosamente en todas las locaciones direccionables, después sobreescribir todas las locaciones direccionables con caracteres aleatorios; verificar la tercera sobreescritura. La utilidad de sobreescritura debe escribir/leer para "crecer" las listas/sectores defectuosos o el disco debe estar mapeado antes del uso clasificado inicial y re-mapeado antes de la sanitización. La diferencia en la comparación de listas debe ser discutida con el Representante de Seguridad Industrial de DSS (IS Rep) y/o Information System Security Professional (ISSP) antes de la desclasificación. *Nota: Las utilidades de sobreescritura deben estar autorizadas por DSS antes de ser usadas.*

e. Sobrescriba todas las locaciones direccionables con un carácter, su complemento y luego un carácter aleatorio.
f. Cada sobreescritura debe residir en memoria por un periodo mayor al que residieron los datos clasificados.
g. Sobreescriba todas las locaciones con un patrón aleatorio, después con ceros binarios y finalmente con unos binarios.
h. Remueva todas las fuentes de poder, incluyendo el poder de la batería.
i. Realice un borrado de chip completo de acuerdo a las especificaciones del fabricante.
j. Efectúe i, luego c un total de tres veces.
k. Efectúe un borrado ultravioleta de acuerdo con las recomendaciones del fabricante.
l. Haga k, pero incremente el tiempo por un factor de tres.
m. Destrucción. Ver 1) y 2) más abajo.
n. Destrucción requerida sólo si se contiene información clasificada.
o. Correr una página (podría ser la prueba de tipos de letra) cuando el ciclo de impresión no fue completado (por Ej., si el papel se atoró o hubo una falla eléctrica). Eliminar la salida como no-clasificada si un examen visual no revela ninguna información clasificada.
p. Las cintas deben ser destruidas y los rodillos deben ser limpiados.
q. Inspeccione y/o pruebe la superficie de la pantalla buscando evidencia de información "quemada" (burn-in). Si se encuentra, la pantalla debe ser destruida.

1) Todos los métodos de destrucción deben ser autorizados por el DSS antes de ser usados. Los posibles tipos de destrucción son: Desintegrar, Incinerar, Pulverizar, Picar o Fundir.
2) NSA ofrece destruir medios AIS (Automated Information Systems) clasificados no relacionados con COMSEC (Communications Security), del gobierno o de contratantes. Contratantes que no sean del DoD deben obtener una carta de su cliente autorizando a NSA para destruir su información clasificada o haber revisado los contratos de especificación de clasificación de seguridad (DD254).

Apéndice B : *Log* de KeyLogger

```
Wed Jul 04 17:49:59 2001 - The Keylogger is
initiated.

DEMO VERSION! Can't be made invisible!

[ ** USER Administrador on COMPUTER DELL-
KXRKAP201R ** ]



[ Ghost Keylogger Demo V2.0, Wed Jul 04
17:49:59 2001 ]


[ Ghost Keylogger Configuration               ,
Wed Jul 04 17:50:01 2001 ]
  Edit {Default Mail 1}


[ Exit, Wed Jul 04 17:50:01 2001 ]
  Static {Do you want to save before you
exit ?}


[ Ghost Keylogger Configuration               ,
Wed Jul 04 17:50:04 2001 ]
  Edit {Default Mail 1}


[ Config, Wed Jul 04 17:50:04 2001 ]
  Static {The configuration data was
successfully saved to the file gklconfig.cfg}


[ Ghost Keylogger Demo V2.0, Wed Jul 04
17:50:05 2001 ]


[ Netscape Messenger Express 3.5.2 Login -
Microsoft Internet Explorer, Wed Jul 04
17:50:11 2001 ]
  Edit
{http://correo.uniandes.edu.co/login.pl}
  Keys
  {

RI'<RETROCESO><RETROCESO><RETROCES
O><RETROCESO><BLOQ
MAYUS>ri.leo<RETROCESO><RETROCESO><R
ETROCESO><RETROCESO>.<RETROCESO> }

[ Autocompletar, Wed Jul 04 17:50:25 2001 ]
  Static {¿Desea que Windows recuerde esta
contraseña para no tener que volver a
escribirla la próxima vez que visite esta
página?}


[ Netscape Messenger Express 3.5.2 Login -
Microsoft Internet Explorer, Wed Jul 04
17:50:29 2001 ]
  Edit
{http://correo.uniandes.edu.co/login.pl}
  Keys
  {
    <RETROCESO><RETROCESO> dsfdsas

  }

[ Ghost Keylogger Demo V2.0, Wed Jul 04
17:50:47 2001 ]
```

[http://correo.uniandes.edu.co/login.pl - Microsoft Internet Explorer, Wed Jul 04 17:50:51 2001]
  Edit {http://correo.uniandes.edu.co/login.pl}

[Ghost Keylogger Demo V2.0, Wed Jul 04 17:50:54 2001]

[Netscape Messenger Express - Microsoft Internet Explorer, Wed Jul 04 17:50:55 2001]
  Edit {http://correo.uniandes.edu.co/mainindex.ht ml}

[Microsoft Internet Explorer, Wed Jul 04 17:51:10 2001]
  Static {Esta seguro que desea salir?}

[Netscape Messenger Express - Microsoft Internet Explorer, Wed Jul 04 17:51:11 2001]
  Edit {http://correo.uniandes.edu.co/mainindex.ht ml}

[Ghost Keylogger Demo V2.0, Wed Jul 04 17:51:14 2001]

[Connections Tray, Wed Jul 04 17:51:17 2001]

[Ghost Keylogger Demo V2.0, Wed Jul 04 17:51:21 2001]

[Program Manager, Wed Jul 04 17:51:23 2001]

Wed Jul 04 17:51:23 2001 - The Keylogger closed.

Wed Jul 04 17:51:49 2001 - The Keylogger is initiated.

DEMO VERSION! Can't be made invisible!

[** USER Administrador on COMPUTER DELL-KXRKAP201R **]

[Ghost Keylogger Demo V2.0, Wed Jul 04 17:51:49 2001]

[Program Manager, Wed Jul 04 17:51:51 2001]

Wed Jul 04 17:51:51 2001 - The Keylogger closed.