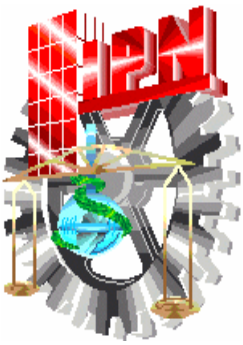


INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA

MECÁNICA Y ELÉCTRICA

UNIDAD CULHUACAN

RECUPERACIÓN DE INFORMACIÓN EN D I S C O S D U R O S

T E S I S

QUE PARA OBTENER EL TÍTULO DE:
INGENIERO EN COMUNICACIONES Y E L E C T R Ó N I C A

P R E S E N T A:
MARIO RODRÍGUEZ ARGUETA

ASESORES:

M. en C. RUBÉN VAZQUEZ MEDINA

M. en C. ROMÁN ARTURO VALVERDE DOMÍNGUEZ

MÉXICO, D.F. 2007

INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE INGENIERIA MECANICA Y ELECTRICA
UNIDAD CULHUACAN

TESIS INDIVIDUAL

Que como prueba escrita de sus Exámenes Profesionales para obtener el Título de Ingeniero en Comunicaciones y Electrónica que deberá desarrollar el C.:

MARIO RODRIGUEZ ARGUETA

"RECUPERACION DE INFORMACION EN DISCOS DUROS"

Con base en la documentación nacional e internacional vigente en esta materia, proporcionar una metodología que sirva de guía y referencia para peritos y especialistas en seguridad informática, para obtener o recuperar la información de un dispositivo de almacenamiento masivo, como un disco duro, a través de herramientas forenses en software libre.

CAPITULADO

I- UNIDADES DE ALMACENAMIENTO DE INFORMACION
II- SISTEMAS DE ARCHIVO
III- METODOLOGIA PROPUESTA
IV- EVALUACION DE LA METODOLOGIA

México D. F., a 12 de Febrero del 2007.

PRIMER ASESOR:

M. en C. RUBEN VAZQUEZ MEDINA

SEGUNDO ASESOR:

M. en C. ROMAN A. VALVERDE DOMINGUEZ

Vo. Bo.

M. en C. HECTOR BECERRIL MENDOZA
JEFE DE LA CARRERA DE I.C.E.

APROBADO

ING. RUBEN JUAREZ BARRIENTOS
SUBDIRECTOR ACADÉMICO

AGRADECIMIENTOS

A tí, principalmente a tí, que me has mirado con ojos misericordiosos y trataré de hacer siempre lo que es justo y correcto para honrarte, mi Padre Celestial.

A mi madre, por haberme apoyado en una forma incondicional, sincera y desinteresada, gracias por ayudarme a ser quien soy.

A mi amigo Jesús Flores Silva, te agradezco en el alma por los consejos maravillosos que trato de seguir en mi vida; siempre recordaré que debo ser discreto, fino y sencillo.

A Ernesto M. Moratilla a quien admiro, respeto y aprecio. Gracias por enseñarme a ver las cosas que están más allá de la vista, gracias por creer en mí.

A mis amigos Julio Servín Paredes, Miguel Ortiz de la Peña, Edelia Beltrán Arreola, Miguel Ángel Acosta, Alejandro Morales Rodríguez, Adrián López Aguado y en general a todos los compañeros del 9C1M, a mis amigos del alemán Felipe Gómez Noguez, Beatriz Ribero Lara y Alejandro García Villar, la maestra Ada Garcés Botello, gracias por darme su amistad, los quiero.

Al profesor Rubén Vázquez Medina, por haber confiado en mí sin conocerme y por ayudarme a realizar este sueño. Mil gracias.

Zu meiner Freundin Elisa Perez Blanco, bleib mit mir für immer, irgendwo, irgendwann, denn du weisst, dass ich dich liebe und du mein anderes Teil bist.

R E C U P E R A C I Ó N D E I N F O R M A C I Ó N E N D I S C O S D U R O S

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

La naturaleza técnica de los crímenes cibernéticos hizo posible una gran rama de la ciencia forense llamada informática forense. En lugar de cadáveres, los científicos forenses digitales recolectan y analizan la información producida, transmitida y almacenada por los elementos digitales. La ayuda del análisis digital permanece igual para aclarar los eventos del incidente, hasta llegar al extremo de identificar a los perpetradores.

En esta tesis se propone una metodología para la identificación, preservación y análisis de la evidencia digital contenida en el dispositivo de almacenamiento por excelencia: el disco duro.

La integridad de la evidencia es lo más importante; las herramientas y metodologías utilizadas tienen sólo una dirección posible, es decir, mejorar con el paso del tiempo.

Antes de llevar a cabo cualquier acción en un sistema comprometido, es necesario elaborar un reporte preliminar, en el cual se detalle el procedimiento a seguir para la recolección de evidencia, donde también se deben hacer anotaciones después de terminar cada paso del proceso, como recordatorios, en caso de que algo anormal ocurra en la extracción de información. Esto es importante, ya que reducirá el riesgo de cometer algún error al recuperar la información perdida del disco comprometido que pueda repercutir, en caso de llevar esta evidencia a un juicio legal.

En el último capítulo se muestra un ejemplo de aplicación de esta metodología en un caso particular para la recuperación de información en un disco duro, que ha sido comprometido debido a una falta de precaución y seguridad por parte del usuario propietario, aplicando la metodología propuesta basada en las cuatro fases del proceso forense y haciendo uso de los conocimientos expuestos en los primeros tres capítulos.

En materia legal, las leyes nacionales tipifican los delitos informáticos en el Código Penal Federal para el Distrito Federal en Materia de Fuero Común y para toda la República Mexicana en Materia de Fuero Federal, en los artículos 211 bis 1 a bis 7, los cuales se exponen en el Apéndice B.

ORGANIZACIÓN DE LA TESIS

Esta tesis fue realizada como producto de una inquietud. Actualmente, personas que comenten fraudes, extorsionan o lucran con la explotación sexual de niños, ya sea por medio de la pornografía infantil o prostituyéndolos, utilizan los medios digitales como una forma de distribución de esta información. Dado que la mayoría de esta información tal como videos, fotografías, enlaces, etc. se guarda en dispositivos de almacenamiento masivo, este tipo de personas tratan de eliminarla para evadir a la justicia. Debido a lo anterior, considere necesario proponer una metodología que sirva como guía a peritos y especialistas en seguridad informática para recuperar la información de estos dispositivos, con el fin de poner tras las rejas a estos individuos. Dicha metodología se basa en las recomendaciones de organismos internacionales como el IOCE, el NIST, entre otros.

Este trabajo está organizado en cuatro capítulos, el último de los cuales ofrece la mayor aportación de este trabajo. A continuación se presenta una breve introducción a cada uno de ellos.

El *primer capítulo* aborda lo relacionado a dispositivos de almacenamiento. Se inicia con sus aspectos mecánicos, eléctricos, magnéticos y funcionales, hasta la explicación del software asociado, el cual ayuda a almacenar adecuadamente un archivo. Se explican, además, las diferentes interfaces, marcas y modelos de las unidades de almacenamiento.

En el *segundo capítulo* se mencionan los sistemas de archivos más utilizados, según el sistema operativo que se maneje, como los de Windows o los basados en UNIX. Además, se hace una clasificación de los diferentes tipos de archivos, la forma en como se presentan al usuario y la forma en como se administran.

En el *tercer capítulo* se describen los modelos existentes de la informática forense para el manejo de la evidencia, de acuerdo con las recomendaciones establecidas por los organismos nacionales e internacionales como el IOCE, el NIST, entre otros; aunque cabe

destacar, que en México no se tiene un organismo como tal, ni mucho menos procedimientos para el tratamiento de la evidencia forense digital. Además, se mencionan algunas de las herramientas que intervienen en el proceso forense, se hace una comparación de las diferentes propuestas del manejo de la evidencia de estos organismos y finalmente, con base en estas recomendaciones, propongo una metodología para el manejo de la evidencia forense en México.

En el *cuarto capítulo* se lleva a cabo la evaluación de la metodología propuesta, la cual es el producto final del desarrollo de esta tesis. Se presentan y explican las cuatro fases principales de la informática forense dentro de la metodología propuesta, aplicadas en un escenario específico, partiendo de la idea de que el disco ha sido comprometido, debido a un mal manejo de la seguridad en un equipo de cómputo que lo tenía.

R E S U M E N

R E C U P E R A C I Ó N D E
I N F O R M A C I Ó N E N D I S C O S D U R O S

Con base en las recomendaciones de organismos internacionales como el IOCE (International Organization on Computer Evidence), NIST (National Institute of Standards and Technology), entre otros, propongo una metodología que sirva como referencia a peritos y especialistas en seguridad informática.

En esta tesis se describen y analizan principalmente los conceptos de disco duro y sistema de archivos, los cuales ayudarán a un investigador a entender como puede preservar la evidencia digital de una manera integra y completa utilizando la metodología propuesta en este trabajo. El objetivo de esta metodología es brindar a los especialistas en seguridad informática una referencia para la recuperación de la información de un dispositivo de almacenamiento masivo, como un disco duro a través de herramientas forenses utilizando software libre.

Esta metodología consta de diez pasos, que bien aplicados, permiten recuperar la información que ha sido “eliminada”. De una manera muy general, el primer paso consiste en determinar el tipo de incidente, después preparar las herramientas de trabajo necesarias, crear la cadena de custodia, crear la imagen del disco comprometido, aplicar la herramienta forense, recuperar la información perdida y finalmente, sugerir medidas de seguridad a los usuarios de los equipos de cómputo.

Además, se explica como la información de un determinado archivo perdura, aún después de haber sido borrado. Por otra parte, se describe la utilización de las herramientas forenses para recuperar información eliminada de un dispositivo de almacenamiento y como un proceso forense exitoso de recuperación de la información depende de la habilidad de recolectar, examinar y analizar los archivos que residen en un medio de almacenamiento, como un disco duro.

A B S T R A C T

D A T A R E C O V E R Y O N H A R D D I S K S D R I V E S

Based on the recomendations of international organizations like IOCE (International Organization on Computer Evidence), NIST (National Institute of Standards and Technology), among others, I propose a methodology to work as a reference for computer security specialists.

In this thesis, *Hard Disk Drive* and *Filesystem* concepts are principally described and analyzed, which will help to an investigator to understand how he can preserve the digital evidence in an upright-whole way using the proposed methodology in this work. The methodology that is proposed has the goal to give to the computer security specialists a reference for the data recovery from a storage -massive device like a hard disk drive through the forensics tools using freeware.

This methodology consists of ten steps that correctly applied, let to recover the data that has been “erased”. In a very general way, the first step consists of determine the kind of incident, after that, to prepare the needed – work tools, create the chain of custody, create the compromised disk image, apply the forensic tool, recover the lost data and finally, suggest security policies to the computer users.

Besides that, it is discussed how data from a certain file lasts, even after it has been erased. In the other hand, the use of the forensics tools from a storage device is described here and how a successful forensic processing of computer media depends on the ability to collect, examine and analyze the files that reside on a media like a hard disk drive.

D E F I N I C I Ó N D E L P R O B L E M A

La informática forense es una disciplina relativamente nueva y poco aplicada en México. Por ello, creemos que no existe en México una metodología que sea referencia nacional, la cual permita garantizar que el proceso forense cumpla con su cometido de aplicar técnicas científicas y analíticas e infraestructura tecnológica para identificar, preservar, analizar y presentar evidencia, de manera que sea admisible en un proceso legal. Consideramos que en muchos casos, se manipula la evidencia de una forma equivocada, si no se respetan los protocolos internacionales del manejo de evidencia digital, y por ello, se estaría cometiendo un delito a los sistemas de información, penado por ley en el Código Penal Federal para el Distrito Federal en Materia de Fuero Común y para toda la República Mexicana en Materia de Fuero Federal (artículo 211 bis 1 a bis 7). Sin embargo, lo que se toma como mundialmente válido son las mejores prácticas, como las del Servicio Secreto de EUA y recomendaciones de organismos especializados como el NIST; por lo que es necesario sentar las bases de un procedimiento que permita recuperar y preservar la información de un dispositivo de almacenamiento, como un disco duro.

O B J E T I V O

Con base en la documentación nacional e internacional vigente en esta materia, proporcionar una metodología que sirva de guía y referencia para peritos y especialistas en seguridad informática, para obtener o recuperar la información de un dispositivo de almacenamiento masivo, como un disco duro, a través de herramientas forenses en software libre.

J U S T I F I C A C I Ó N

La informática forense es una ciencia muy poco difundida en nuestro país, a comparación de otros países como Argentina, Estados Unidos, Canadá, Australia, España, Reino Unido y China, quienes cuentan con instituciones certificadas y mundialmente conocidas, que crean recomendaciones para el manejo de la evidencia forense. Asimismo, dichas recomendaciones, señalan los roles de cada una de las personas encargadas de manejar la evidencia, desde el personal responsable de recolectarla y crear la cadena de custodia, hasta el personal que analiza y reporta sus hallazgos. Por lo tanto, en México es necesaria una referencia nacional para que las personas que hagan la labor del manejo de evidencia, como ingenieros, administradores de sistemas, u organizaciones públicas y privadas eviten problemas de origen legal, como demandas por negligencia en su labor forense.

CAPÍTULO I

UNIDADES DE ALMACENAMIENTO DE INFORMACIÓN

RESUMEN. En este capítulo se explica que un dispositivo de almacenamiento como el disco duro es uno de los elementos más importantes de las computadoras actuales, ya que guarda la mayoría de la información almacenada en el equipo. Es la unidad sellada que la PC utiliza para almacenar datos en forma no volátil o permanente, lo cual significa que el dispositivo conserva los datos aún cuando la computadora se encuentre sin corriente eléctrica. Además, se explica el funcionamiento de los discos duros, las partes que lo conforman, de cómo logran almacenar los datos y finalmente cuales son las interfaces existentes en el mercado, las cuales se utilizan para conectar una unidad de disco duro a una PC moderna.

1.1 ALMACENAMIENTO DE LA INFORMACIÓN

El almacenamiento permanente de datos en una computadora opera de acuerdo con principios ópticos, magnéticos o una combinación de ambos. En el caso del almacenamiento magnético, se almacena un flujo de bits de datos binarios (unos y ceros) magnetizando diminutas partículas de metal incrustadas en la superficie de un disco o cinta, en un patrón que representa los datos. Posteriormente, ese patrón magnético puede ser leído y convertido nuevamente en un flujo de bits exactamente igual al original.

Como se usan los campos magnéticos para almacenar datos

Todos los dispositivos de almacenamiento magnético, como las unidades de disco flexible y disco duro, escriben y leen datos por medio del electromagnetismo. Este principio básico de la física establece que, cuando fluye una corriente eléctrica a través de un conductor (alambre), se genera un campo magnético alrededor del mismo (vea figura 1.1).

Otro efecto del electromagnetismo es que si se pasa un conductor a través de un campo magnético en movimiento, se genera una corriente eléctrica. Al cambiar la polaridad del campo magnético, cambia la dirección del flujo de la corriente eléctrica.

Como el electromagnetismo trabaja de dos maneras, cuando se aplica esta característica a los dispositivos de almacenamiento magnético, es posible grabar datos en un disco y leerlos posteriormente. Al grabar, la cabeza convierte los impulsos eléctricos en campos magnéticos; al leer, convierte los campos magnéticos en impulsos eléctricos.

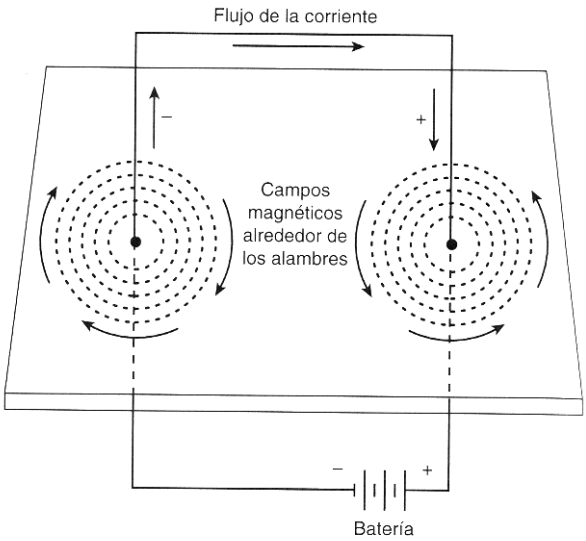


Figura 1.1. Generación de un campo magnético alrededor de un alambre [1]

Las cabezas de lectura / escritura de un dispositivo de almacenamiento magnético son piezas de material conductor en forma de U, con los extremos de la U situados directamente encima de la superficie del medio de almacenamiento de datos (con una distancia relativamente pequeña de manera que las cabezas nunca tocan la superficie del disco). La cabeza en forma de U está envuelta en bobinas, es decir, alambre enrollado, a través de las cuales puede fluir la corriente eléctrica (vea figura 1.2). Cuando los circuitos lógicos de la unidad magnética hacen pasar una corriente eléctrica a través de estas bobinas, se genera un campo magnético en la cabeza de la unidad; al invertir la polaridad de la corriente eléctrica, también se invierte la polaridad del campo magnético. En esencia, las cabezas son electroimanes cuyo voltaje puede cambiar de polaridad muy rápidamente.

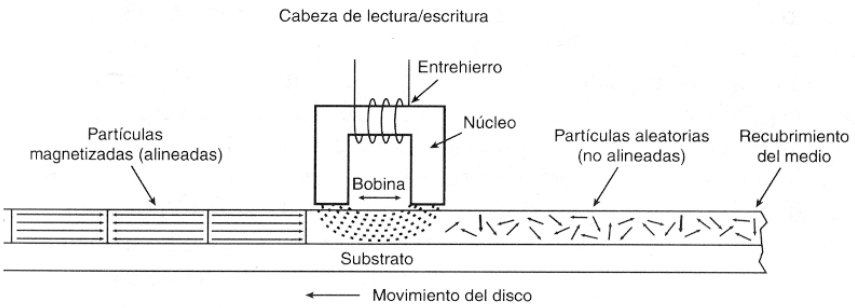


Figura 1.2. Cabeza magnética de lectura / escritura[2]

El disco o la cinta que constituyen el medio de almacenamiento está formado por algún material (como aluminio o cristal en los discos duros) en el cual se ha depositado una capa de material magnetizable. Generalmente este material es aleación de óxido de hierro con algunos otros elementos. Cada una de las partículas magnéticas en el medio de almacenamiento tiene su propio campo magnético. Cuando el medio está en blanco

[1] Scout Mueller. Manual de Actualización y Reparación de PC´s. 12ª edición. Edit. Pearson Educación. Pág. 590. México 2001.
[2] Scout Mueller. Manual de Actualización y Reparación de PC´s. 12ª edición. Edit. Pearson Educación. Pág. 591. México 2001.

(no contiene información), las polaridades de esos campos normalmente se encuentran en desorden debido a que los campos de las partículas apuntan en direcciones aleatorias, cada campo magnético es cancelado por algún otro que apunte en la dirección opuesta; por lo que cuando se tienen muchos campos orientados aleatoriamente, el efecto neto resultante es que no se observa un campo unificado o polaridad.

Para grabar datos, la cabeza de la unidad magnética crea inversiones de flujo en el medio. Por cada fragmento de dato (bit) que escribe la unidad, se crea un patrón de inversiones de positivo a negativo y de negativo a positivo en áreas específicas del medio, conocidas como bits o celdas de transición. Una *celda bit* o *celda de transición* es un área específica del medio, controlada por el tiempo y la velocidad a la cual viaja el medio, en el cual la cabeza de la unidad magnética crea inversiones de flujo. El patrón particular de las inversiones de flujo dentro de las celdas de transición usadas para almacenar fragmentos de datos (bits) es conocido como *método de codificación*. La lógica de la unidad magnética o controlador toma los datos que van a ser almacenados y los codifica como una serie de inversiones de flujo en un periodo dado, de acuerdo con el patrón específico del método de codificación que se utilice. Los dos métodos más empleados de codificación en medios magnéticos sobre la Modulación de Frecuencia Modificada (MFM) y Longitud de Recorrido Limitado (RLL). Actualmente las unidades de disco duro utilizan alguna de las variantes del método de codificación RLL, [1].

Como puede verse, las unidades de disco duro y otros dispositivos de almacenamiento magnético leen y escriben datos basándose en los principios electromagnéticos. A continuación se detallan los tipos de cabezas magnéticas que hacen posible la lectura / escritura en el disco magnético y sus formas de codificación.

Tipos de cabezas de lectura / escritura

Conforme ha ido evolucionando la tecnología de unidades de disco, también lo han hecho las cabezas de lectura / escritura. Con el paso de los años, el diseño de las cabezas ha evolucionado de los primeros núcleos de ferrita a los diversos tipos y tecnologías disponibles hoy en día. A lo largo de los años se han utilizado cuatro tipos diferentes de cabezas:

a) Ferrita
b) Película delgada (TF)
c) Metal en el entrehierro(MIG)
d) Magneto – resistiva (MR)

a) *Ferrita*

Estas cabezas tienen un núcleo de óxido de hierro recubierto con bobinas, las cuales son más grandes y pesadas que las de película delgada y, por lo tanto, requieren mayor altura de flotación para evitar contacto con el disco mientras está girando. Estas cabezas son, hoy en día, prácticamente obsoletas, ya que no pueden escribir en el medio de alta coercitividad requerido para los discos de alta densidad y tienen una respuesta en frecuencia muy baja con altos niveles de ruido.

b) *Metal en el entrehierro*

En las cabezas MIG, se aplica una sustancia metálica (aleación) al entrehierro de la cabeza de grabación. Esta aleación magnética tiene el doble de la capacidad de magnetización de la ferrita y permite a la cabeza de grabación escribir en los medios de película delgada de alta coercitividad requerida para densidades mayores. Las cabezas MIG producen también un gradiente más definido en el campo magnético, lo que permite un pulso magnético de mayor definición.

c) *Película delgada*

Las cabezas de película delgada (TF) son fabricadas por medio de un proceso fotolitográfico. Estas tienen un entrehierro extremadamente angosto y controlado, el cual es creado por medio de la deposición electrónica de aluminio duro. Debido a que este material encierra completamente al entrehierro, el área queda muy bien protegida, lo que reduce al mínimo las posibilidades de daño por contacto en el disco. El núcleo es una combinación de hierro con una aleación de níquel, la cual tiene de dos a cuatro veces mas potencia magnética que el núcleo de ferrita. Las cabezas TF pueden escribir a densidades extremadamente altas y pueden flotar a mucha menor altura que las de ferrita y las MIG lo cual permite a las cabezas captar y transmitir una señal mucho más fuerte de los discos, aumenta la proporción de señal a ruido, mejorando la precisión. Otra de las ventajas de las cabezas TF es que su reducido tamaño permite que los discos sean apilados más juntos, permitiendo así acomodar más discos dentro del mismo espacio.

d) *Cabezas magneto – resistivas*

Un avance más reciente en grabación magnética, o más específicamente, en la fase de lectura de la grabación magnética, es la cabeza magneto – resistiva (MR). Todas las cabezas son detectoras, esto es, están diseñadas para detectar la transición de flujo en el medio y reconvertirlo en una señal eléctrica que podría ser interpretada como datos. Un problema con la grabación magnética es el siempre creciente deseo de mayor densidad, lo cual significa poner más información (transiciones de flujo) en un espacio más pequeño.

Hace mucho tiempo se descubrió otro efecto del magnetismo en un alambre. Cuando se pasa un alambre a través de un campo magnético, no solo se genera un pequeña corriente, sino que además cambia la resistencia del alambre.

Un circuito hace pasar un voltaje por la cabeza magneto – resistiva (MR) y espera a que se produzca un cambio en el voltaje, lo cual ocurre cuando cambia la resistencia de la cabeza conforme pasa a través de las inversiones de flujo en el medio. Este mecanismo de la cabeza tiene como resultado una señal mucho más clara y limpia del medio, y hace posible incrementar la densidad.

Las cabezas MR son más costosas y complejas de fabricar, ya que requieren de más pasos de enmascaramiento, deben de aislarse debido a que son muy susceptibles a campos magnéticos desviados y deben contar con alambres adicionales de la cabeza y hacia ésta, para conducir la corriente detectada.

Debido que las cabezas MR solo pueden leer datos y no escribirlos, requieren de otro recurso para escribir. El conjunto consta de una cabeza TF estándar para escribir datos y una MR para leerlos. Como las dos cabezas están montadas juntas, cada cabeza está optimizada para su tarea específica [2].

Guía deslizable de la cabeza

El término *guía deslizable* se usa para referirse al cuerpo del material que soporta la cabeza del disco duro. La guía deslizable es la que en realidad flota o se desliza sobre la superficie del disco, llevando la cabeza a la distancia correcta del medio, para la lectura / escritura. La mayoría de las guías deslizables se parecen a un trimarán con dos capsulas externas que flotan a lo largo de la superficie del medio del disco y la porción de un casco central, la cual de hecho soporta la cabeza y el entrehierro.

La figura 1.3 muestra una guía deslizable típica. Observe que la cabeza con el entrehierro de lectura / escritura está situada donde termina el eje de la guía deslizable.

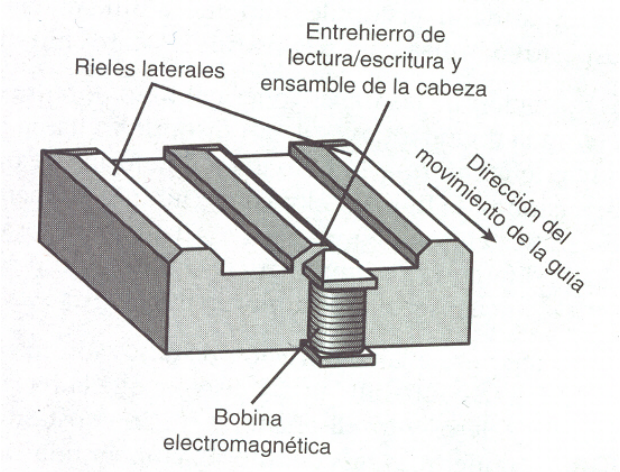


Figura 1.3. Parte inferior de una guía deslizable típica[3]

Las guías deslizables más pequeñas reducen la masa soportada en el extremo del brazo actuador de las cabezas proveyendo una mayor aceleración y desaceleración, lo que conduce a tiempos de acceso más rápidos. Los nuevos diseños de nanoguías y picoguías deslizables tienen, además, patrones de superficie especialmente modificados para mantener la misma altura de flotación sobre la superficie del disco, ya sea que la guía deslizable esté colocada arriba de los cilindros internos o de los externos.

Las guías deslizables convencionales reducen o incrementan su altura de flotación de acuerdo a la velocidad a la que viaja la superficie del disco debajo de éstas.

Arriba de los cilindros externos, la velocidad y la altura de flotación son mayores. Este arreglo no es deseable en los nuevos discos que usan grabación por zonas de bits, en la cual la densidad de bits es la misma en todos los cilindros.

Cuando la densidad de bits es uniforme en todo el disco, la altura de flotación de las cabezas debería ser relativamente constante para obtener el máximo desempeño. Los

[3] Scout Mueller. Manual de Actualización y Reparación de PC´s. 12ª edición. Edit. Pearson Educación. Pág. 591. México 2001.

patrones de superficie de textura especial, así como las técnicas de fabricación permiten a las guías deslizables flotar a una altura mucho más uniforme, haciéndolas ideales para discos que utilicen grabación por zonas de bits.

Sistemas de codificación de datos

El almacenamiento magnético se lleva a cabo en un medio analógico; sin embargo, los datos almacenados en una PC son información digital, esto es, unos y ceros.

Cuando la unidad magnética manda información digital a la cabeza magnética de grabación, la cabeza crea dominios magnéticos en el medio de almacenamiento con polaridades específicas, las cuales forman las fronteras entre las áreas de polaridad positiva y negativa que el controlador de la unidad usa para codificar los datos digitales en el medio analógico.

Para optimizar la posición de las transiciones de flujo durante el almacenamiento magnético, se utiliza un dispositivo llamado *codificador / decodificador* (endec), el cual convierte la información binaria a una forma de onda diseñada para poner de manera óptima las inversiones de flujo en el medio.

Con el paso de los años, se han desarrollado diferentes sistemas para la codificación de datos. La codificación de señales permite al sistema utilizar al máximo la tecnología de hardware de la unidad. Aunque se han desarrollado varios sistemas de codificación, los siguientes tipos han llegado a ser los más populares:

- Modulación de Frecuencia Modificada (MFM)

- Longitud de Recorrido Limitado (RLL)

Codificación MFM

La codificación MFM fue diseñada para reducir el número de inversiones de flujo y para poner más datos en el disco. La codificación MFM graba los datos de transición solo cuando un bit cero es precedido por otro; en cualquier otro caso la transición del reloj no es requerida, permitiéndole a la codificación MFM almacenar el doble de bits de datos en el mismo número de transiciones de flujo. Este tipo de codificación es utilizada en discos flexibles.

Codificación RLL

Actualmente el sistema de codificación más empleado en los discos duros es el llamado RLL (Longitud de Recorrido Limitado), el cuál puede poner más del doble de información en un disco que MFM. En lugar de codificar un solo bit, RLL normalmente codifica un grupo de bits de datos a la vez.

El término *Longitud de Recorrido Limitado* se deriva de las dos especificaciones de este código, las cuales son el número mínimo (longitud de recorrido) y el número máximo (recorrido limitado) de celdas de transición permitido entre dos inversiones de flujo. Se han logrado algunas variaciones de este sistema cambiando los parámetros de longitud y límite, pero solo dos se han difundido realmente: RLL 2.7 y RLL 1.7.

La mayoría de los discos duros de alta calidad en la actualidad utilizan codificación RLL 1.7, la cual ofrece una relación de densidad de 1.27 veces la de una MFM y ofrece mayor margen de error y un código más confiable, lo cual es importante cuando las tecnologías de medio y de cabeza son llevadas a sus límites.

Los materiales de fabricación, así como los métodos de codificación, ayudan a optimizar el desempeño de los discos duros. Sin embargo, existe un tercer aspecto, el cual es y será un punto clave para la evolución de la capacidad de almacenamiento de un disco duro.

Densidad de área

En ocasiones, se utiliza la densidad de área como indicador de la tasa de crecimiento de la tecnología para la industria de los discos duros.

La *densidad de área* se puede definir como el producto de bits lineales por pulgada (bpi) medidos a lo largo de la longitud de las pistas del disco y multiplicados por el número de pistas por pulgada (tpi), las cuales se miden radialmente en el disco (vea figura 1.4).

Actualmente existen discos duros muy eficientes que tienen una gran cantidad de almacenamiento en un espacio más pequeño. Por ejemplo, en diciembre del 2006, Toshiba presentó el primer disco duro de 1.8 pulgadas, llamado MK1011GAH con una capacidad de almacenamiento de 100 GB.

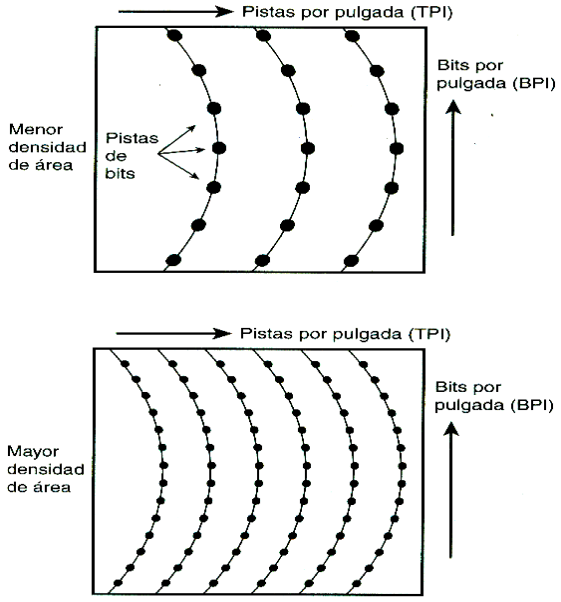


Figura 1.4. Densidad de área[4]

Según Susan Nowack, Directora de Marketing de Toshiba Storage Device Division, dice: “nuestro disco duro de 100 GB marca un hito en la capacidad de almacenamiento de los dispositivos de pequeño formato.” “…hubo un tiempo en que solo los ordenadores de sobremesa ofrecían 100 GB. Pero ahora se pueden desarrollar terminales móviles con la mima capacidad de almacenamiento” [3].

[4] Scout Mueller. Manual de Actualización y Reparación de PC´s. 12ª edición. Edit. Pearson Educación. Pág. 607. México 2001.

1.2 DISCOS DUROS Y UNIDADES DE ALMACENAMIENTO

Un disco duro es un elemento de almacenamiento de información no volátil, es decir, que guarda largo tiempo los bits almacenados, aunque se retire el suministro de energía eléctrica.

Se le denomina unidad, al conjunto de componentes electrónicos y mecánicos que hacen posible el almacenamiento y recuperación de los datos en el disco, mientras que el disco es una pila de discos, llamados platos, quienes almacenan información magnéticamente.

Cada uno de los platos tiene dos superficies magnéticas: la superior y la inferior. Estas superficies magnéticas están formadas por millones de pequeños elementos capaces de ser magnetizados positiva o negativamente, como se explicó en la sección anterior.

De esta manera, se representan los dos posibles valores que forman un bit de información (un cero o un uno). Ocho bits contiguos constituyen un byte (un carácter).

La mejor manera de entender como trabaja un disco duro es dar un vistazo al interior. Cabe mencionar, que para ilustrar el interior y exterior de un disco duro, se dispuso de una unidad descompuesta, de la marca *Seagate*. Es importante señalar, que si se abre un disco podría dañarse, por lo que se recomienda no hacerlo a no ser que dicho dispositivo ya no funcione. La figura 1.5 muestra el aspecto de un disco duro típico.

Figura 1.5. Fotografía de un disco duro [5]

Es una caja de aluminio sellado con controladores electrónicos unidos en la base de dicha caja. La electrónica controla el mecanismo de lectura / escritura y el motor que hace girar los platos. Al remover la cubierta del disco duro se expone un simple pero preciso interior como se observa en la figura 1.6. En esta figura se pueden observar los platos y el cabezal.

[5]Fuente. Elaboración propia.

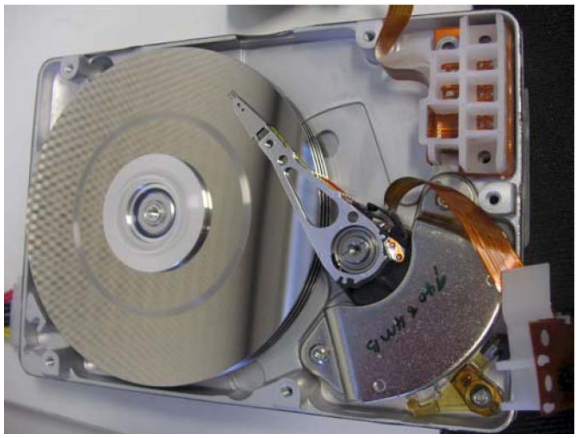


Figura 1.6. Fotografía del interior de un disco duro [6]

Los platos están hechos de aluminio o de vidrio con implante cerámico actualmente. Existen discos rígidos fijos, como los que están en una caja hermética en el interior del gabinete de una PC, y también los hay removibles, los cuales son transportables. Las unidades de disco están compuestas por varios platos, de 2 a 4, y algunas otras llegan a tener 11 o más.

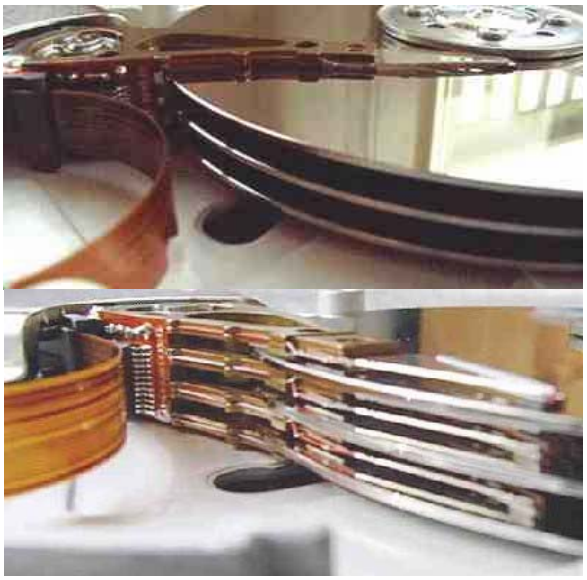
Por fabricarse los platos bajo normas estrictas, y variar muy poco de tamaño con la temperatura, el material magnético que los recubre permite 3000 tpi o más, a la par que 50.000 o más bytes por pista (o sea 100 ó más sectores por pista).

También ha influido en esto la aplicación de magnetización perpendicular a la superficie de la capa magnetizable, en lugar de la polarización de superficie. Resulta así una elevada capacidad de almacenaje en uno o dos platos pequeños, y unidades compactas. Además, debido a la gran velocidad de giro, y por tener el cabezal movimiento rápido en discos de pequeño radio, se tiene comparativamente tiempos cortos de acceso.

Más sectores por cilindro posibilitan que un archivo entre en un solo cilindro, para que el cabezal, en lo posible, no deba cambiar a otro cilindro, resultando más rápida la escritura y posteriores lecturas; a la par que reduce la fragmentación de archivos en varios cilindros, con la pérdida de tiempo que ello ocasiona, [4].

Los platos son discos concéntricos que giran todos a la vez. El cabezal o brazo de lectura y escritura es un conjunto de brazos alineados verticalmente, que se mueven hacia dentro o hacia fuera, según convenga, todos a la vez. El mecanismo que mueve los brazos tiene que ser increíblemente rápido y preciso. El cabezal en un disco duro típico puede moverse del centro a la orilla y de regreso hasta 50 veces por segundo. En la punta de dichos brazos están las cabezas de lectura/escritura, que gracias al movimiento del cabezal pueden leer tanto zonas interiores como exteriores del disco. Es decir los platos son leídos en ambas caras. La figura 1.7 (a) y (b) muestra un ejemplo de cómo lucen los platos y el brazo.

[6] Fuente. Elaboración propia.



(a) (b)

Figura 1.7. Fotografía del interior de un disco duro. (a) Platos. (b) Brazo. [7]

Cada plato tiene dos *caras*, y es necesaria una cabeza de lectura/escritura *para cada cara*. En realidad, cada uno de los brazos es doble y contiene 2 cabezas: una para leer la cara superior del plato, y otra para leer la cara inferior. Las cabezas de lectura/escritura nunca tocan el disco, sino que pasan muy cerca (hasta a 3 nanómetros).Si alguna llega a tocarlo, causaría muchos daños en el disco, debido a lo rápido que giran los platos (uno de 7.200 revoluciones por minuto se mueve a 120 Km/h en el borde), [5].

La información es almacenada en la superficie del plato en sectores y pistas. Por definición, un plato es cada uno de los discos que integran al disco duro. Las cabezas leen y escriben datos en anillos concéntricos llamados pistas, las cuales están divididas en segmentos llamados sectores cada uno de los cuales almacena 512 bytes.

Un *clúster* es un conjunto contiguo de sectores que componen la unidad más pequeña de almacenamiento de un disco. Los archivos se almacenan en uno o varios clústeres, dependiendo de su tamaño. Sin embargo, si el archivo es más pequeño que un clúster, éste lo ocupa completo, [6].

El tamaño de los clústeres depende del sistema de archivos empleado, por lo que el espacio de almacenamiento perdido, debido a los archivos que ocupan menos que el tamaño del clúster, depende del sistema de archivos que emplee el disco. Por otro lado, el conjunto de posiciones idénticas en cada lado o cara de cada plato constituye un cilindro. Lo anteriormente dicho se muestra en la figura 1.8 (a) y (b).

El número total de sectores de un disco duro se puede calcular mediante la siguiente formula:

$$N_S=N_C N_{PC} N_{SP}$$

En donde:

N_S= Número de sectores
N_C= Número de caras

[7] Fuente. Elaboración propia.

N_{PC}=Número de pistas por cara
N_{SC}= Número de sectores por pista

Por tanto, cada sector queda unívocamente determinado si conocemos los siguientes valores: cabeza, cilindro y sector. Por ejemplo, el disco duro *ST32122A de Seagate,* utilizado como disco de pruebas, tiene las siguientes especificaciones: cilindros = 4092, cabezas = 16 y sectores = 63. susttuyendo estos datos enla formula anterior se tiene que:

$$N_S=4092*16*63$$

$$N_S= 4124736\text{sectores}$$

Para calcular la capacidad máxima de un disco duro se utiliza la siguiente formula:

$$C_M=512*N_S$$

En donde:

C_M= Capacidad máxima del disco duro

Si cada sector almacena 512 bytes de información, la capacidad máxima de este disco duro será de:

512 bytes/sector*4124736sectores = 2111864832bytes ~ 2 GB.

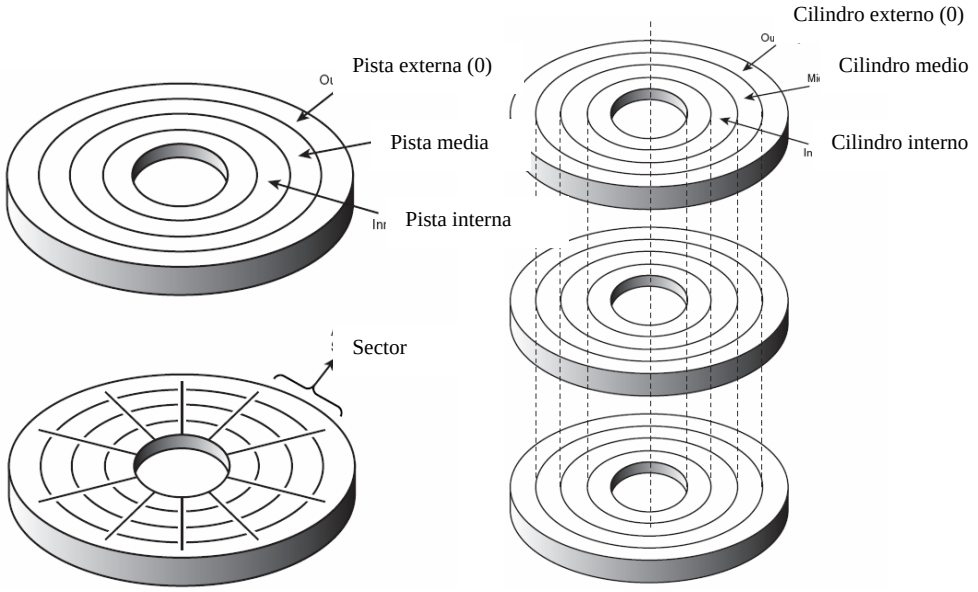


Figura 1.8. Organización del disco duro. (a) Pistas y sectores. (b) Cilindros[8]

Aunque esta fórmula, sin embargo, no es valida en los discos modernos, debido a que el número de sectores por pista no es constante si se utiliza el método de grabación de bits por zonas, el cual es utilizado por los fabricantes de discos para asegurar que todas las pistas sean del mismo tamaño, de otro modo las pistas interiores guardarían menos información que las exteriores, [7].

[8] Scout Mueller. Manual de Actualización y Reparación de PC´s. 12ª edición. Edit. Pearson Educación. Pág. 614- 615. México 2001.

Los sectores de las pistas se numeran comenzando por el 1, aunque las cabezas o cilindros están numerados a partir del 0. Cuando se formatea un disco, el programa para formatear crea identificadores (ID) de áreas antes y después de los datos del sector que el controlador del disco usa para numerar los sectores y para identificar el inicio y el fin de cada sector. Cada sector del disco tiene u prefijo o encabezado, que identifica el inicio del sector y contiene su número correspondiente, así como un sufijo que contiene una suma de control que ayuda a asegurar la integridad de los datos contenidos.

Este proceso de formateo de bajo nivel llena normalmente los bytes de datos con algún valor específico como F6h (hexadecimal) o algún otro patrón de prueba utilizado por el fabricante de la unidad. Los encabezados de los sectores son independientes del sistema operativo, de los sistemas de archivos y de los archivos almacenados en la unidad. Además de los encabezados hay espacios dentro de los sectores, entre los sectores en cada pista y también entre las pistas, pero en ninguna de estas separaciones se puede guardar datos.

Para el 2007, cerca del 98% de los discos duros mundiales son fabricados por un conjunto de compañías mundialmente reconocidas, las cuales son, [8]:

- Seagate
- Western Digital
- Samsung
- Hitachi

Filtros de aire

Casi todas las unidades de disco duro tienen dos filtros de aire. Uno se llama filtro de recirculación y el otro barométrico o de respiración. Estos filtros se encuentran permanentemente sellados dentro de la unidad y están diseñados para no ser cambiados nunca durante la duración de la unidad. El filtro de recirculación esta diseñado para filtrar solamente aquellas pequeñas partículas desprendidas de los platos durante el arranque y el estacionamiento de las cabezas. Debido a que los discos duros están sellados permanentemente y no puede circular aire desde afuera, pueden funcionar en ambientes extremadamente sucios. La figura 1.9 representa la forma en como circula el aire en el interior de una unidad de almacenamiento.

El disco duro esta sellado pero no es hermético. Este se ventila a través de un filtro barométrico o de respiración que permite la igualación de la presión (respiración) entre el interior y el exterior de la unidad. Por esta razón la mayoría de las unidades están diseñadas para operar en rangos específicos de altitud, usualmente entre 305 metros bajo el nivel del mar y 3050 metros sobre el nivel del mar.

Filtro de recirculación Bobina de voz rotatoria

Movimiento del fluio de aire

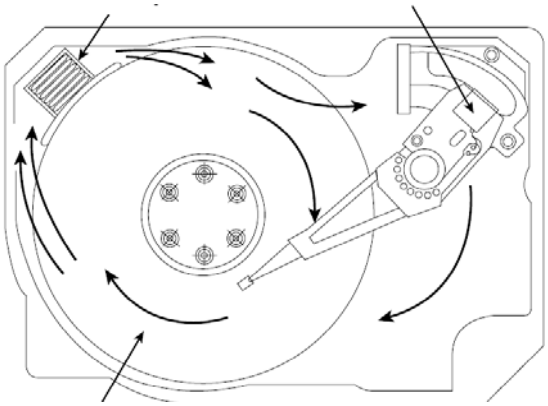


Figura 1.9. Circulación de aire en un disco duro[9]

De hecho hay algunas unidades no soportan altitudes mayores de 3215 metros sobre el nivel del mar, cuando están en operación, debido a que la presión del aire llega a ser demasiado baja dentro de la unidad para que puedan flotar adecuadamente las cabezas.

Aunque el aire fluye a través de un respiradero, la contaminación no es de preocupar, porque el filtro barométrico del respiradero esta diseñado para filtrar partículas mayores de 0.3 micras para cumplir con las especificaciones de pureza dentro de la unidad.

En la mayoría de las unidades se pueden observar los agujeros de ventilación, los que generalmente están cubiertos internamente por este filtro de respiración. Algunas unidades tienen filtros más finos para filtrar partículas aún más pequeñas.

Formateo de discos

Se requieren dos procedimientos de formateo para que puedan escribirse datos en el disco:

- Formateo físico o de bajo nivel
- Formateo lógico o de alto nivel

Un disco duro requiere dos operaciones separadas de formateo. Las particiones del disco son necesarias porque un disco duro esta diseñado para aceptar más de un sistema operativo.

Es posible usar múltiples sistemas operativos en un disco, separando el formateo físico, que es un procedimiento independiente del sistema operativo que se vaya a utilizar, y el formateo de alto nivel (que es diferente para cada sistema operativo).

La partición permite que un disco pueda ejecutar más de un sistema operativo o posibilita a un sistema operativo utilizar el disco como varios volúmenes o unidades lógicas. Un volumen o unidad lógica es cualquier sección del disco, a la cual el sistema operativo asigna una letra o nombre de unidad, [9].

[9] Scout Mueller. Manual de Actualización y Reparación de PC´s. 12ª edición. Edit. Pearson Educación. Pág. 642. México 2001.

En el capítulo II se tratará mas a detalle la forma en como un sistema operativo se encarga de organizar los diferentes archivos y carpetas, esto es, a través de un sistema de archivos. A continuación se explicarán los dos tipos de formateo que tiene un disco duro.

Básicamente, el proceso de formateo de bajo nivel en un disco duro establece a las pistas y a los sectores en los platos. Así los puertos de inicio y término de cada sector son escritos en el plato. Este procedimiento prepara al dispositivo para almacenar los bloques de bytes.

El formateo de alto nivel escribe pues las estructuras de almacenaje de archivos, como por ejemplo, una tabla de asignación de archivos (FAT) en los sectores. Este proceso prepara al disco para alojar los archivos.

En consecuencia, preparar un disco duro para el almacenamiento de datos, comprende tres pasos:

a) Formateo de bajo nivel (LLF)
b) Partición
c) Formateo de alto nivel (HLF)

a) *Formateo de bajo nivel*

Durante un formateo de bajo nivel, el programa de formato divide las pistas del disco en un número específico de sectores, creando separaciones entre sectores y entre pistas y grabando la información de los encabezados.

El programa llena también el área de datos del sector con bytes ficticios o un patrón de valores de prueba. En los discos duros, el número de sectores por pista depende del disco y de la interfaz del controlador.

Las unidades IDE y SCSI utilizadas actualmente en las PC´s pueden tener de 17 a 700 o más sectores por pista. Prácticamente todas las unidades IDE y SCSI usan una técnica de grabación llamada grabación de bits por zonas, la cual escribe un número variable de sectores por pista.

Cuando no se usa dicho método de grabación, el número de sectores y, por lo tanto, el número de bits en cada pista es constante. Eso significa que el número de bits por pulgada será variable. Habrá más bits por pulgada en las pistas internas que en las externas. La figura 1.10 muestra una unidad grabada con el mismo número de sectores por pista.

Una grabación estándar desperdicia capacidad de almacenamiento en las pistas externas debido a que dicha capacidad es mayor aunque almacena la misma cantidad de datos (más separados) que las pistas internas.

Una forma de incrementar la capacidad del disco durante el proceso de formateo de bajo nivel, es creando más sectores en los cilindros externos que en los internos, debido a que tienen una mayor circunferencia, los cilindros externos pueden acomodar más datos.

Las unidades que utilizan grabación de bits por zonas, dividen los cilindros en grupos llamados zonas. El número de zonas varía según la unidad, aunque la mayoría de las unidades tienen 10 o más zonas. La figura 1.11 muestra una unidad con grabado de bits por zonas.

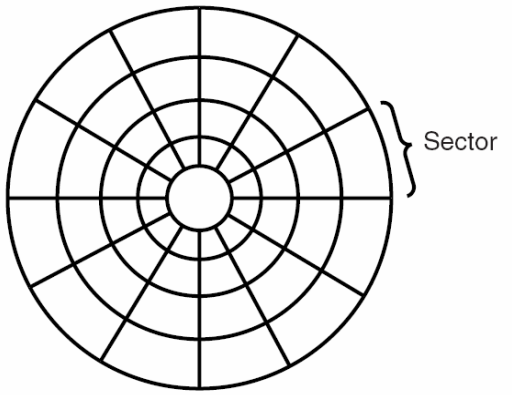


Figura 1.10. Grabación estándar con el mismo número de sectores por pista[10]

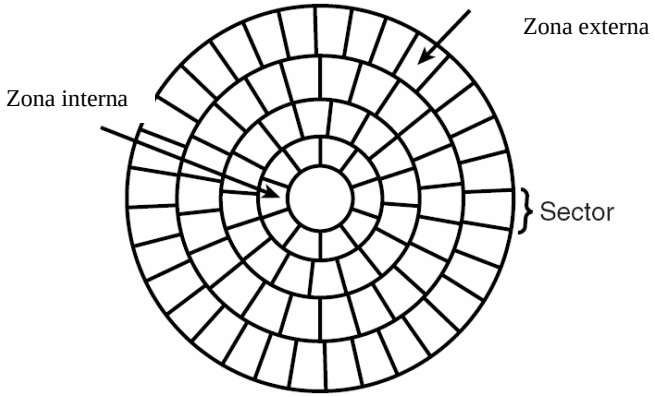


Figura 1.11. Grabación estándar con el mismo número de sectores por pista[11]

Otro efecto de la grabación de bits por zonas, es que la velocidad de transferencia varía de acuerdo con la zona en la que se encuentren las cabezas. Una unidad con grabación por zonas de todos modos gira a velocidad constante; debido a que hay más sectores por pista en las pistas externas, sin embargo, la transferencia de datos será mayor ahí y por consecuencia la transferencia de datos será menor en la lectura y escritura de las zonas internas.

El uso de la grabación de bits por zonas permite a los fabricantes de unidades incrementar la capacidad de sus unidades de 20 a 50 por ciento en relación con el sistema de número fijo de sectores por pista.

Todas las unidades modernas ATA (IDE y SCSI) aplican la grabación de bits por zonas. El formateo de bajo nivel en discos IDE y SCSI lo lleva a cabo el fabricante y nunca el usuario final.

[10] Scout Mueller. Manual de Actualización y Reparación de PC´s. 12ª edición. Edit. Pearson Educación. Pág. 622. México 2001.
[11] Scout Mueller. Manual de Actualización y Reparación de PC´s. 12ª edición. Edit. Pearson Educación. Pág. 623. México 2001.

b) *Particionado*

Crear una partición en el disco duro permite el manejo de sistemas de archivos separados, cada uno en su propia partición. Cada sistema de archivos puede tener su propio método de asignación de espacio en unidades lógicas llamadas unidades de asignación o clusters.

Cada disco duro debe tener al menos una partición y puede tener hasta cuatro, cada una de las cuales admite el mismo o diferentes tipos de sistemas de archivos.

c) *Formateo de alto nivel*

Durante el formateo de alto nivel, el sistema operativo escribe estructuras necesarias para administrar los archivos y los datos en el disco.

Estas estructuras de datos le permiten al sistema operativo administrar el espacio en disco, darle seguimiento a los archivos e incluso manipular las áreas defectuosas para evitar problemas.

El formateo de alto nivel no es en realidad un formateo físico de la unidad, sino la creación de una tabla de contenido para el disco.

Partiendo de la suposición que un disco duro tiene cargado un sistema operativo con sistemas de archivo NTFS o ext3, (los cuales se tratarán más a detalle en el capítulo II), es necesario mencionar los tipos de archivos producidos en forma general como particular como los del sistema (una vez instalado el sistema operativo), así también como los que son creados por el usuario cuando realiza ciertas actividades como, escribir una carta, un correo electrónico, etc.

Clasificación de archivos

Un archivo es una entidad que permite al usuario almacenar información, activar dispositivos o permitir procesos de comunicación. Existen dos formas de clasificar a los archivos, de una manera general y una manera particular, desde el punto de vista de una distribución de Linux.

Tipos de archivos generales

- **Archivos ordinarios**

Son los más comunes, son los que almacenan datos, es decir, puede ser un programa, un archivo de texto, código fuente o cualquier cosa que pueda guardarse en cualquier lugar. El kernel soporta acceso secuencial y aleatorio en todos estos archivos.

- **Directorios**

Tienen en común con los archivos ordinarios en que también contienen datos, sólo que en este caso el dato es una lista de otros archivos.

- **Archivos especiales**

Se identifican porque cada uno tiene un número de dispositivo mayor y uno menor (*major and minor device number*). El número mayor identifica al manejador del dispositivo, quien necesita el kernel para acceder al dispositivo.

El número menor significa un parámetro dependiente del manejador del dispositivo usado típicamente para diferenciar entre diversos tipos de dispositivos soportados por el manejador, o distintos modos de operación.

Utilizan un inodo[12] pero no bloques de datos. Representan dispositivos en los que se pueden leer o escribir cantidades arbitrarias de datos. Incluyen sistemas de archivos[13], puertos seriales, puertos paralelos, terminales y cintas.

También se les conoce como "*raw devices*" debido a que no manipulan la I/O. Los discos duros y flexibles pueden ser accedidos de esta manera.
Podemos ver archivos de este tipo en el directorio */dev*.

- **Entubamientos (FIFO [*First In First Out*])**

Son aquellos que permiten la comunicación entre dos procesos ejecutándose en el mismo nodo. Los entubamientos pueden ser creados con el comando *mknod* y eliminados con el comando *rm*.

- **Ligas Duras**

En realidad una liga no es un archivo, es un nombre adicional para otro archivo. Cada archivo tiene al menos una liga, usualmente el nombre bajo el cual fue originalmente creado. Cuando se hace una nueva liga hacia un archivo, un alias para este archivo es creado.

Una liga es indistinguible del archivo al cual está ligado; LINUX mantiene el conteo de la cantidad de ligas que apuntan hacia un archivo en particular y no libera el espacio que ocupa el archivo hasta que la última liga es eliminada.

La liga dura es una conexión directa entre archivos, por lo que ésta no puede existir a través de distintos sistemas de archivos.

- **Ligas Simbólicas**

Son archivos que simplemente contienen el nombre de otro archivo. Cuando el kernel trata de abrir o pasar a través de la liga, su atención es directamente hacia el archivo.

Tipos de archivos particulares

- **Archivos creados por el usuario**

[12] El concepto de inodo se describirá en el capítulo II
[13] El concepto de sistemas de archivos de tratará a profundidad en el capítulo II

Los archivos creados por el usuario pueden contener evidencia importante de actividad criminal, tales como libretas de direcciones y bases de datos que pueden probar asociación criminal, imágenes o videos digitales, los cuales pueden evidenciar actividad pedofílica y comunicaciones entre criminales, tales como mensajes vía e-mail o de voz. Puede ser también que inventarios de narcotráfico estén contenidos en una hoja de cálculo.

- Libreta de direcciones
- Archivos de audio o video
- Agendas y calendarios
- Documentos o archivos de texto
- Bases de datos
- Archivos de e-mails
- Archivos gráficos
- Lista de páginas Web favoritas
- Archivos de hojas de cálculo

- **Archivos protegidos por el usuario**

Los usuarios tienen la oportunidad de esconder evidencia en una gran variedad de formas. Por ejemplo, pueden encriptar o proteger con contraseña los datos que son importantes para ellos.

Pueden también esconder archivos en el disco duro o dentro de otros archivos u ocultar evidénciales bajo un nombre inofensivo.

- Archivos comprimidos
- Archivos encriptados
- Archivos ocultos
- Archivos sin nombres
- Archivos protegidos con contraseña
- Archivos esteganografiados

- **Archivos creados por la computadora**

La evidencia puede ser también encontrada en archivos y otras áreas de datos creadas, como una función de rutina del sistema operativo de la computadora. En muchos casos, el usuario no está conciente de que datos están siendo creados.

Algunos ejemplos de esta actividad interna del sistema son los archivos de contraseñas, actividad en Internet y archivos de respaldo temporales. Estos son los tipos de archivos que pueden ser recuperados y examinados.

- Archivos de respaldo
- Archivos de configuración
- Archivos “cookies”
- Archivos ocultos
- Archivos de historial
- Archivos de registro (logs)
- Archivos de impresión
- Archivos de intercambio (swap)
- Archivos de hojas de cálculo
- Archivos temporales

Todos los archivos tienen como común denominador guardar información de cualquier clase. Sin embargo, los sistemas operativos actuales, tanto libres como comerciales, tienen una forma propia de organización de archivos, conocida como sistemas de archivos, los que se estudiarán en el capítulo II. A continuación se describirán los tipos de archivos más importantes de un sistema operativo, los cuales ayudan a mejorar el rendimiento del disco duro.

- **Otras áreas de datos**

Existen algunos componentes dentro de los archivos que pueden tener algún valor como evidencia. Estos componentes pueden ser la fecha y hora de creación, modificación, borrado, acceso; nombre de usuario o identificación. Estos componentes son muy frágiles y aún en el encendido del equipo puede modificar algo de esta información.

- Clusters dañados
- Fecha, hora y contraseña de la PC
- Archivos borrados
- Espacio libre
- Particiones ocultas
- Clusters perdidos
- Metadatos
- Otras particiones
- Áreas reservadas y de sistema
- Espacio inactivo (*slack*)
- Información de registro de software
- Espacio sin asigna**r**

Dentro de la clasificación de estos tipos de datos, los metadatos y la zona de *slack*, son muy importantes, debido a que en una examinación forense, estos datos permiten conocer más a detalle la información relacionada con un archivo y su ubicación.

Metadatos para la Accesibilidad

Los metadatos son una excelente vía para comunicar información, sobre un documento, o sobre los recursos que directamente se relacionan con la accesibilidad.

Los metadatos son información sobre un documento. La información que se use para describir un documento, puede ayudar a los usuarios a identificar si el documento es útil para ellos y a localizarlo rápidamente. El precursor de los metadatos es el catálogo con tarjetas. Para cada elemento en una biblioteca, hay tres entradas en la tarjeta del catálogo: título, autor, y tema. Una tarjeta, indica la localización de un elemento en la biblioteca, y proporciona información adicional sobre él, tal como el editor, formato, género, fecha de publicación, y número de volúmenes. Mientras que la tarjeta sirve como base de datos para la biblioteca, los metadatos van un paso más allá, los metadatos son la estructura interna de un sistema de archivos que asegura que todos los datos están adecuadamente organizados y accesibles en el disco, [10].

Esencialmente, se trata de “datos acerca de los datos.” Como se explicará en el capítulo II, la mayoría de los sistemas de archivos disponen de su propia estructura de metadatos, que es la causa, en parte, de que los sistemas de archivos exhiban diferentes niveles de prestaciones.

Mantener los metadatos intactos es de la mayor importancia, ya que de otro modo podría llegar a corromperse la totalidad del sistema de archivos.

Además, un metadato al ser un conjunto de bloques de información del contenido de un archivo, tiene un número identificador llamado inodo, el cual se explicará a detalle en el capítulo II.

Espacio inactivo (slack space)

Básicamente se considera como espacio de bloques o clusters que no es utilizado, [11]. Según Henry B. Wolf [12], la definición del *espacio inactivo* es “el espacio entre el fin lógico y el fin físico de un archivo y se llama archivo inactivo. El fin lógico de un archivo se presenta antes del fin físico de un cluster en el cual se almacena. Los bytes remanentes en el cluster son remanentes de archivos o directorios previos almacenados en ese cluster”.

Hasta el momento, se ha explicado la forma en como los discos duros almacenan la información, el tipo de materiales de que están elaborados, y como los métodos de codificación permiten que los discos tengan una mayor densidad para almacenar los datos. A continuación se estudiarán las dos interfaces más utilizadas en los discos duros para comunicar datos con el sistema.

1.3 INTERFAZ DE COMUNICACIÓN IDE Y SCSI

Los discos duros son el medio de almacenamiento masivo y permanente por excelencia en los equipos de cómputo. Existen dos grandes grupos de discos en función de su interfaz con la PC, IDE y SCSI. En esencia, ambos grupos son equivalentes, salvo en aspectos de rendimiento, fiabilidad y precio.

Difieren, eso sí, en las limitaciones que el software de sistemas ha impuesto de forma artificial a los discos IDE en el mundo de los PCs. La interfaz básica para conectar una unidad de disco duro a una PC es la llamada IDE (Integrated Drive Electronics). Este nombre deriva de que la interfaz o controlador está incorporado en la misma unidad a diferencia de una unidad SCSI , la cual es básicamente igual a una IDE, excepto por que cuenta adicionalmente con un circuito adaptador de bus SCSI. IDE es también conocida como ATA (Conexión AT) y aunque IDE se usa de manera más coloquial y quizá sea un término más reconocido, desde el punto de vista técnico, ATA es su verdadero nombre.

Interfaz IDE

Actualmente se usa la IDE no sólo para conectar discos duros, sino también unidades de CD-ROM, de DVD, etc. La tarea principal del controlador de disco duro o interfaz es transmitir y recibir datos de la unidad.

Los diferentes tipos de interfaz limitan la velocidad a la que los datos pueden transferirse de la unidad al sistema y otros índices de rendimiento. El termino IDE es un termino genérico aplicado a cualquier unidad con un controlador de disco integrado.

Combinar la unidad y el controlador simplifica en gran medida la instalación, ya que no hay cables separados de suministro eléctrico y datos que vayan del controlador a la unidad. Además se reduce el número total de componentes, la trayectoria de las señales es más corta y las conexiones eléctricas son menos vulnerables al ruido.

Esto produce un diseño más confiable de lo que es posible, cuando se emplea un controlador separado, conectado por cables a la unidad.

La ventaja básica de las unidades IDE sobre las interfaces separadas en el controlador como SCSI o IEEE 1394 es el costo, ya que se elimina el controlador y se simplifican las conexiones.

Señales ATA

Con el fin de trasportar las señales entre los circuitos del adaptador de bus y la unidad, se ha especificado un cable plano de 40 conductores.

Para mejorar la integridad de la señal y eliminar posibles problemas de temporización y ruido, el cable no debe exceder en longitud a los 46 centímetros ni medir menos de 25 centímetros.

El pin 20 se usa como identificador de la orientación del cable y no está conectado en la interfaz. El pin debe de estar ausente en cualquier conector ATA, el cable debe tener inhabilitado el agujero del pin 20 y además debe tener una marca o protuberancia, diseñada para impedir que sea conectado al revés.

La regla general básica es que el pin 1 debe estar orientado hacia el conector de corriente del dispositivo. El pin 39 lleva la señal DSAP (Unidad Activa/Unidad Esclava Presente), la cual es una señal multiplexada de propósito dual.

La figura 1.12 muestra la disposición de los pines mencionados en el conector de la interfaz ATA-IDE.

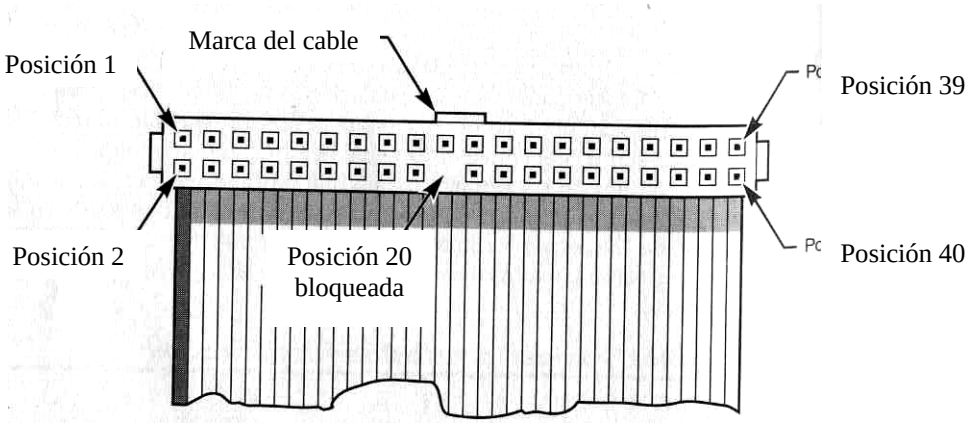


Figura 1.12. Detalle del conector de 40 pines de la interfaz ATA-IDE[14]

Durante la inicialización de energía esta señal indica si en la interfaz está presente una unidad esclava. Después de eso, cada unidad confirma la señal para indicar que está activa. El pin 28 lleva la señal Selección de cable (CSEL) o señales de sincronización del eje (SPSYNC), que es un conductor de doble propósito. La función CSEL es la más utilizada y esta diseñada para controlar la designación de una unidad como maestra (unidad 0) o como esclava (unidad 1).

Las controladoras IDE casi siempre están incluidas en la placa base, normalmente dos conectores para dos dispositivos cada uno. De los dos discos duros, uno tiene que

[14] Scout Mueller. Manual de Actualización y Reparación de PC´s. 12ª edición. Edit. Pearson Educación. Pág. 524. México 2001.

estar como esclavo y el otro como maestro para que el controlador sepa de qué dispositivo manda o recibe los datos.

La configuración se realiza mediante *jumpers*. Habitualmente, un disco duro puede estar configurado de una de estas tres formas:

Como maestro (*master*). Si es el único dispositivo en el cable debe tener esta configuración, aunque a veces, también funciona si está como esclavo. Si hay otro dispositivo, el otro debe estar como esclavo.

Como esclavo (*slave*). Debe haber otro dispositivo que sea maestro.

Selección por cable (*cable select*). El dispositivo será maestro o esclavo en función de su posición en el cable. Si hay otro dispositivo, también debe estar configurado como *cable select*. Si el dispositivo es el único en el cable, debe estar situado en la posición de maestro. Para distinguir el conector en el que se conectará el primer bus Ide (Ide 1) se utilizan colores distintos.

Este diseño (dos dispositivos a un bus) tiene el inconveniente de que mientras se accede a un dispositivo, el otro dispositivo del mismo conector IDE no se puede usar.

Comandos ATA

Una de las mejores características de la interfaz ATA-IDE es su conjunto mejorado de comandos. La interfaz ATA-IDE esta basada en el controlador WD1003 y todas las unidades de este tipo deben aceptar el conjunto original de comandos WD (ocho comandos) sin excepciones, razón por la cual es tan fácil instalar estas unidades en los sistemas actuales.

Además de admitir todos los comandos WD1003, la especificación ATA agrega numerosos comandos para mejorar el rendimiento y las capacidades. Estos comandos son parte opcional de la interfaz ATA, pero muchos de ellos se usan en las unidades actuales.

Quizás el comando más importante es el de *Identificar Unidad*, el cual hace que la unidad transmita un bloque de datos de 512 bytes, que proporciona todos los detalles acerca de la unidad, mediante la ejecución de subrutinas del BIOS donde puede averiguar exactamente que tipo de unidad esta conectada, el fabricante, su número de modelo, los parámetros operativos e incluso el número de serie.

Otros dos comandos muy importantes son los de lectura múltiple y escritura múltiple. Estos comandos permiten transferencias de datos de secotes múltiples y, si se combinan con la capacidad de Entrada/Salida Programada (PIO) en modo de bloque en el sistema, permiten una increíble velocidad de transferencia de datos. Para tal fin, se deben ejecutar instrucciones de subrutinas del BIOS.

Cuando se debe de leer o escribir, el controlador de la electrónica IDE realiza los siguientes pasos:

- Traduce dichos comandos en señales para que el cabezal se posicione en el cilindro elegido; y que luego la pista correspondiente a la cabeza seleccionada sea leída por ésta hasta encontrar el sector buscado.

- La cabeza lee el número de identificación de cada sector que encuentra en la pista que va leyendo, el cual es transmitido a la electrónica IDE, para determinar si es o no el comienzo del sector buscado, a fin de escribir o leer (según sea la orden) los datos en la zona correspondiente del sector buscado.

- Si es una orden de lectura, todos los bits del sector son leídos en serie por la cabeza. A medida que son leídos se realiza la verificación ECC (semejante a la CRC).

En el sistema IDE el controlador del dispositivo se encuentra integrado en la electrónica del dispositivo. Las diversas versiones de sistemas ATA son:

ATA-1
ATA-2, soporta transferencias rápidas en bloque y multiword DMA.
ATA-3, es el ATA2 revisado.
ATA-4, conocido como Ultra-DMA o ATA-33 que soporta transferencias en 33 Mbps.
ATA-5 o Ultra ATA/66, originalmente propuesta por Quantum para transferencias en 66 Mbps.
ATA-6 o Ultra ATA/100, soporte para velocidades de 100Mbps.
ATA-7 o Ultra ATA/133, soporte para velocidades de 133Mbps.

Serial ATA, remodelación de ATA con nuevos conectores (alimentación y datos), cables y tensión de alimentación. El SATA proporcionará mayores velocidades, mejor aprovechamiento cuando hay varios discos, mayor longitud del cable de transmisión de datos y capacidad para conectar discos en caliente (con la computadora encendida).

Fue estandarizado a mediados de 2004, con definiciones específicas de cables y conectores; la longitud de cable se restringe a 2 metros; USB y Firewire permiten mayores distancias.

Actualmente, la mayoría de las placas bases no tienen un conector para SATA, pero es posible usar adaptadores de bus o tarjetas *PC-Card y CardBus*. La interfaz SATA ofrece velocidades de transferencia superiores a 3.0Gb/s.

En definitiva, subrutinas del BIOS al enviar comandos a los puertos de la interfaz (IDE, SCSI u otra) dan origen a lecturas y escrituras en el disco, siendo que los tiempos de las señales involucradas están determinados por los circuitos de la interfaz , donde los tiempos son más cortos en los últimos modelos, [14].

Interfaz SCSI

SCSI (Small Computer System Interface) se refiere a una interfaz de propósito general empleada para conectar a una PC dispositivos de varios tipos. SCSI es un bus que acepta hasta 7 o 15 dispositivos por canal.

El controlador SCSI, conocido como adaptador host, funciona como gateway entre el bus SCSI y el bus del sistema de la PC. Cada dispositivo del bus tiene un controlador incorporado; el bus SCSI no se comunica directamente con los discos duros u otros dispositivos, sino con el controlador incorporado integrado en la unidad. La figura 1.13 nuestra la forma de interconexión de elementos SCSI.

Un solo bus SCSI acepta hasta 8 o 16 unidades físicas, cada una identificada por el sistema. Una de estas unidades es la tarjeta del adaptador host SCSI de la PC; las otras 7 o 15 pueden ser otros periféricos.

La mayoría de los sistemas admiten hasta cuatro adaptadores host, cada uno de hasta 15 dispositivos, lo cual hace un total de 60 dispositivos. De hecho, ya que las PC modernas aceptan los baratos puertos USB integrados para la expansión externa, en la mayoría de los casos, los dispositivos SCSI son necesarios, sólo cuando el alto rendimiento es una cuestión crítica.

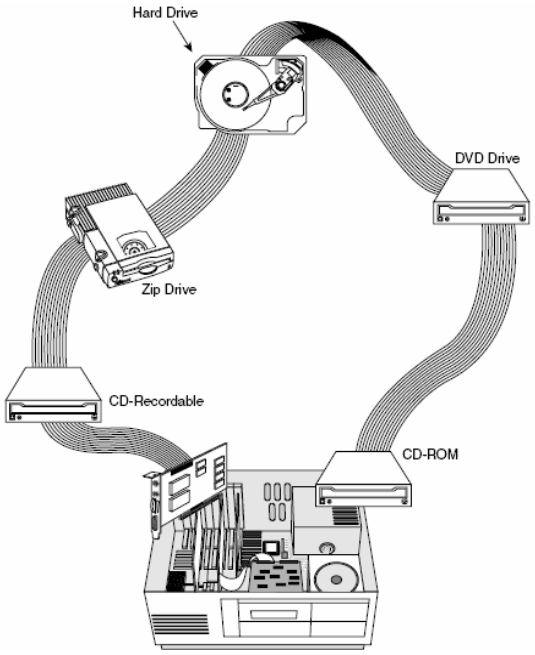


Figura 1.13. Conexiones en cadena del bus SCSI[15]

Ahora SCSI es un estándar, en cierta medida como lo es USB ya que solo define las conexiones de hardware, no las especificaciones de los controladores requeridos para comunicarse con los dispositivos.

Tipos de SCSI

- SCSI 1 Bus de 8 bits. Velocidad de transmisión de datos a 5 Mbps. Su conector genérico es de 50 pines (ver figura 1.14) y baja densidad. La longitud máxima del cable es de seis metros. Soporta hasta 8 dispositivos (incluida la controladora), identificados por las direcciones 0 a 7.

[15] Scout Mueller. Manual de Actualización y Reparación de PC´s. 12ª edición. Edit. Pearson Educación. Pág. 571. México 2001.

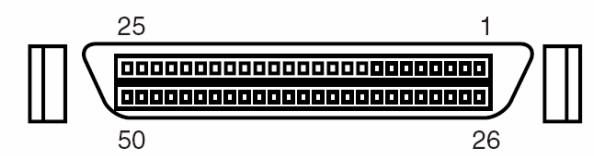


Figura 1.14. Conector SCSI de 50 pines y alta densidad[16]

- SCSI 2 Fast: Con un bus de 8, dobla la velocidad de transmisión (de 5 Mbps a 10 Mbps). Su conector genérico es de 50 pines y alta densidad. La longitud máxima del cable es de tres metros. Soporta hasta 8 dispositivos (incluida la controladora), identificados por las direcciones 0 a 7.

- Wide: Dobla el bus (pasa de 8 a 16 bits). Su conector genérico es de 68 pines (ver figura 1.15) y alta densidad. La longitud máxima del cable es de tres metros. Soporta hasta 16 dispositivos (incluida la controladora), identificados por las direcciones 0 a 15.

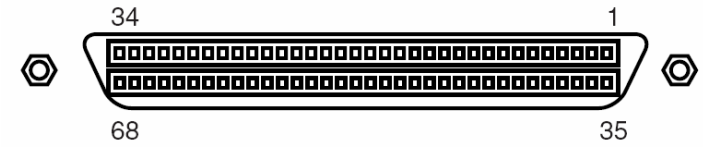


Figura 1.15. Conector SCSI de 68 pines y alta densidad[17]

- SCSI Ultra Wide: Dispositivos de 16 bits con velocidad de ejecución de 40 Mbps. Su conector genérico es de 68 pines y alta densidad. La longitud máxima del cable es de 1,5 metros. Admite un máximo de 15 dispositivos. También se conoce como Fast SCSI-3.

- SCSI Ultra 3 Dispositivos de 16 bits con velocidad de ejecución de 80 Mbps. Su conector genérico es de 68 pines y alta densidad. La longitud máxima del cable es de doce metros. Admite un máximo de 15 dispositivos.

Direccionamientos CHS / LBA

Traducción CHS extendida

En realidad el direccionamiento CHS (Cylinder-Head-Sector) extendido es un truco aritmético por el que se informa a la BIOS que el disco instalado (suponemos que es una unidad IDE) tiene un número de cilindros, cabezas y sectores distintos de los reales, pero adaptado a lo que puede manejar la BIOS (lo que se denomina geometría trasladada).

Para ello, si el número de cilindros del dispositivo IDE es superior a los 1024 soportados por la BIOS, se divide este número por 2, 4, 8 o 16, hasta que el valor resultante sea igual o menor que los mentados 1024.

[16] Scout Mueller. Manual de Actualización y Reparación de PC´s. 12ª edición. Edit. Pearson Educación. Pág. 560. México 2001.
[17] Scout Mueller. Manual de Actualización y Reparación de PC´s. 12ª edición. Edit. Pearson Educación. Pág. 561. México 2001.

El valor resultante es el que se pasa a la BIOS como número de cilindros. Por su parte, el número de cabezas se multiplica por el factor 2, 4, 8 o 16 utilizado, y éste es el que se suministra a la BIOS (podríamos decir que se cambian cilindros por cabezas).

Por ejemplo, las características de un disco IDE indican que tiene 12000 cilindros, 16 cabezas y 63 sectores por pista (un total de 12096000 clusters). Su número CHS real sería 12000-16-63, pero como 12000 es superior al número de cabezas que soporta la BIOS, se divide este número por 16, para que el resultado sea igual o menor que 1024.

En este caso el resultado es 12000/16 = 750, con lo que en el *setup* se informa a la BIOS que el disco instalado tiene 750 cilindros.

A cambio, el número real de cabezas (16) se multiplica por 16; el resultado 256 es el que se pasa como número de cabezas, así que la BIOS cree que el disco instalado es de 750 cilindros, 256 cabezas y 63 sectores por pista.

Las BIOS que soportan direccionamiento ECHS realizan automáticamente las conversiones adecuadas. En realidad esta "traducción" funciona entre el disco IDE/ATA y la interrupción 13h de la BIOS.

La BIOS toma la geometría lógica del disco (según el estándar ATA) y la traduce a una geometría equivalente, pero que ajuste dentro de los límites aceptables por la interrupción 13h estándar. El sistema permitió sobrepasar la barrera de 528 MB del conjunto BIOS estándar/dispositivo IDE, aunque es evidente que aún se encontraba limitado por el tope de 8.455 GB de la propia BIOS.

Direccionamiento LBA

Como la capacidad de los discos crecía de forma imparable, pronto se hizo necesario sobrepasar también el límite de los 8,455 GB de la interrupción 13h de la BIOS. Para esto se ideó un sistema denominado LBA (Logical Block Addressing), que implica un sistema radicalmente distinto de direccionar los clusters.

En lugar de referirse a ellos en términos geométricos (Cilindro, Cabeza y Sector), a cada cluster se le asigna un número único, Número de Sector. Para ello se numeran 0, 1, 2, ..., N-1, donde N es el número total de sectores del disco.

Actualmente LBA es el sistema dominante para direccionamiento de discos grandes, puesto que desde que alcanzaron el límite de 8.455 GB, se hizo imposible expresar su geometría en términos de Cilindro, Cabeza y Sector.

En realidad LBA es un sistema radicalmente nuevo de direccionamiento que, en principio, no implica por sí mismo ampliar ningún límite. Aunque desde luego, las BIOS que detectan sistemas LBA también disponen de la traducción adecuada para solventar las limitaciones de la combinación BIOS/ATA (saltar la limitación de 528 MB o incluso la de 8.455 GB).

Esta traducción es la que resuelve el paso de la barrera, ya que la interrupción 13h no sabe nada sobre direccionamientos LBA. Por supuesto todas las nuevas unidades de

disco soportan LBA, y cuando esta circunstancia es auto-detectada por la BIOS, se establece automáticamente este modo de direccionamiento y se habilita la traducción correspondiente.

Esta traducción es parecida a la ECHS, aunque el algoritmo es diferente; se denomina traducción auxiliar LBA. La diferencia substancial es que en ECHS, la BIOS traslada los parámetros utilizados por la interrupción 13h desde la geometría trasladada a la geometría local del disco. En la traducción LBA, la BIOS traslada la geometría trasladada directamente en un número de sector.

Con posterioridad al establecimiento del sistema, se empezó a utilizar una extensión conocida como LBA48, que aumentaba de 24 a 48 los bits reservados para representar los números de sector. Asumiendo que el formateo se realiza en sectores de 512 Bytes, el método permite unidades con un máximo teórico de 512 x 248 = 144.11 Petabytes, [15].

1.4 ESTRUCTURA LÓGICA DEL DISCO DURO

Esta formada por tres partes principales:

- El sector de arranque (Master Boot Record)
- Espacio particionado
- Espacio sin particionar

El sector de arranque

Es el primer sector de cada disco duro y en el se almacena la tabla de particiones, además de un pequeño programa de iniciación. Este programa lee la tabla de particiones y cede el control a la partición principal. En caso de no haber partición activa, se desplegara un mensaje de error. La figura 1.16 muestra la representación de la estructura lógica del disco duro.

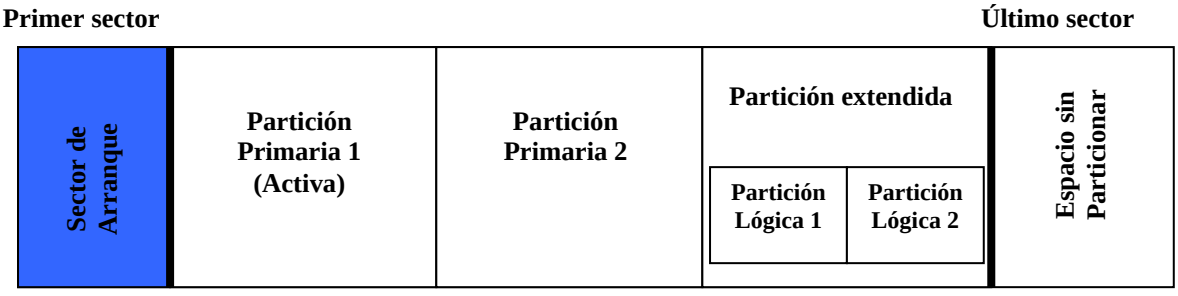


Figura 1.16. Posición del sector de arranque[18]

Espacio particionado

Espacio del disco duro que ha sido asignado a alguna partición (vea figura 1.17).

[18] Angelina E. Trujillo. Alternate Data Stream. Pág. 7. México 2006.

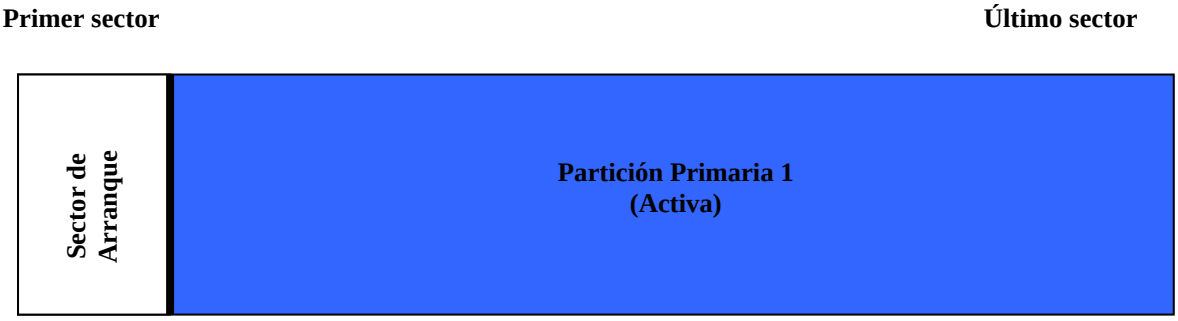


Figura 1.17. Posición de la partición activa[19]

Espacio sin particionar

El espacio no particionado, es espacio no accesible del disco ya que todavía no ha sido asignado a ninguna partición, (vea figura 1.18) [14].

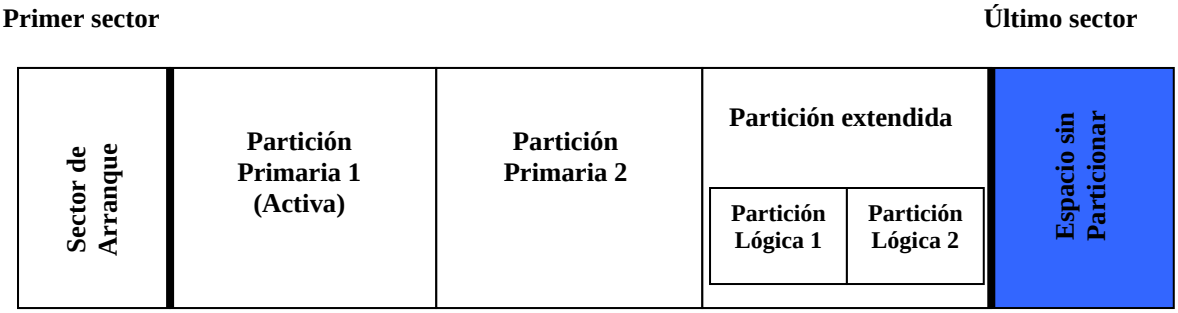


Figura 1.18. Posición de la partición activa[20]

Particiones de disco

En el primer sector de un disco duro reside el denominado MBR (o Master Boot Record). En estos 512 bytes residen el código inicial de carga del sistema operativo, la tabla de particiones primarias y la firma del disco. El código de carga más frecuente es el que define el sistema operativo DOS, el cual se encarga de buscar la partición de arranque, cargar en memoria el primer sector de dicha partición y cederle el control. Éste es el método utilizado por todos los sistemas operativos de Microsoft. Este código de carga puede recuperarse (reinstalarse) con el mandato DOS FDISK /MBR, el cual deja intacta la tabla de particiones.

Otros códigos de carga bastante utilizados son los cargadores que vienen con el sistema operativo Linux: LILO y GRUB. En realidad, el código que se ubica en el MBR es el correspondiente a la primera fase del proceso de arranque. Estos cargadores son más complejos y flexibles que el código de carga de DOS, y utilizan la información que reside en el directorio */boot* de Linux para determinar qué sistema operativo debe cargarse.

El código de carga se utiliza tan sólo en el disco principal del sistema (es decir, el disco maestro del interfaz IDE primario). Hay BIOS que permiten arrancar de otros discos duros, pero generalmente aparecen numerosos problemas al utilizar esta opción.

[19] Angelina E. Trujillo. Alternate Data Stream. Pág. 7. México 2006.
[20] Angelina E. Trujillo. Alternate Data Stream. Pág. 7. México 2006.

La tabla de particiones está formada por cuatro entradas, donde cada una de ellas describe una potencial partición primaria. Los detalles de cada entrada son algo oscuros, y su utilización varía sensiblemente de un sistema operativo a otro. No obstante, simplificando un poco, cada entrada indica, para la partición que describe, la siguiente información:

- El sector del disco donde comienza
- Su tamaño
- Si es una partición de arranque (activa)
- Su tipo

El indicador de partición de arranque es utilizado tan sólo por el código de carga de DOS. Linux ignora por completo esta información. Existen numerosos tipos de particiones, en función de su utilización o de su organización interna (establecida por el sistema operativo que la defina). Existe una convención que establece el identificador de cada tipo de partición como un número concreto en hexadecimal. La tabla 1.1 expone los tipos de particiones más habituales.

Una partición extendida es un contenedor para otras particiones, a las cuales se les denomina particiones lógicas. Sólo una de las particiones primarias puede declararse como extendida. La representación de las unidades lógicas se realiza utilizando una lista enlazada que reside dentro de la partición extendida, por lo que no hay límite en cuanto al número de particiones lógicas que se pueden crear.

Tipo	Uso	Limitación
0	Partición vacía	
5	Partición extendida	1024 cilindros
6	DOS FAT 16	2 GB
7	NTFS	2TB
B	Win 95 FAT 32	2TB
F	Extendida Win 95	2TB
80	Old Minix	-
82	Linux swap	-
83	Linux native	2TB

Tabla 1.1 Tipos de particiones más habituales[21]

Asignación de letras de unidad

La letra de unidad es una forma lógica de denominar y reconocer las unidades de disco o particiones en los sistemas operativos MS-DOS y Microsoft Windows. Otros sistemas como Unix consiguen que los discos se vean en un directorio que se puede elegir. Normalmente, tanto MS-DOS como Windows denominan a sus discos o particiones como sigue:

A:\ - Unidad de disquete (3.5 pulgadas es el estándar actual).
B:\ - Reservada tradicionalmente para la segunda unidad de disquete.
C:\ - Partición o disco duro principal. Suele ser en el que se instala el sistema operativo.
D:\ hasta Z:\ - Otros discos duros o particiones.

[21] Fuente. Elaboración propia.

D:\ hasta Z:\ - Después de los discos duros, van las unidades de CD y DVD, tarjetas de memoria flash, cámaras digitales y demás dispositivos con capacidad de almacenamiento, sobre todo extraíbles.

El orden en que se asigna las unidades a partir de *C* son:

- Primero todas las particiones primarias. MSDOS supone que cada disco solo tiene una primaria.
- Primero la primaria del primero, luego la primaria del segundo
- Después haber asignado todas las primarias se asigna las lógicas.
- Primero todas las lógicas del primero en orden, luego todas las del segundo, hasta acabar.
- Luego las unidades extraíbles (CD-ROM y otros). Si son dispositivos hot plug como las memorias USB, son asignadas por orden de aparición. Con lo que una unidad que ahora es *F:* \ luego puede ser otra letra.

Se pueden usar hasta 24 letras de unidad, desde C hasta Z. Se reservan las letras de unidad A y B para unidades de disco. Sin embargo, si no tiene una unidad de disco B, podrá utilizar la letra B para una unidad de red.

1.5 COMENTARIOS

Una definición propia de disco duro es “aquel elemento físico que puede almacenar información de una manera electrónica, en el cual la información persiste, aún si por alguna razón se le deja de proporcionar energía eléctrica”.

La tecnología evoluciona y cambia constantemente, por ejemplo, en la década de los 70’s el tamaño de los discos duros ocupaba un espacio semejante al que ocupa una lavadora actualmente, en los 80’s aparecieron los discos de 5.25 pulgadas con obvias mejoras como tamaño y velocidades de transmisión. En los 90´s con el uso de interfaces como la USB fue posible hacer que los discos duros pudieran ser portátiles e intercambiables. Actualmente hay discos duros tan pequeños, como del tamaño de una identificación o de una tarjeta de crédito además de una gran capacidad de almacenamiento y portabilidad. Seguramente en el futuro, se verán discos tan pequeños como del tamaño de una uña, capaces de almacenar mucha más información de la que se almacena hoy en día.

Es importante saber el principio básico de funcionamiento de estos dispositivos de almacenamiento, a fin de comprender y apreciar mejor los beneficios que proporcionan; no obstante, también se requiere de personas que sepan recuperar la información de estos dispositivos, ya que esta información en ocasiones es más valiosa que el mismo disco. Si se sabe como operan estas unidades, es más probable evitar cometer errores en el momento de la recolección de la evidencia forense, de la cual se hablará a detalle en los capítulos III y IV.

Referencias

[1] Scout Mueller. Manual de Actualización y Reparación de PC´s. 12ª edición. Edit. Pearson Educación México 2001
[2]M.C. Ginzburg, “Introducción General a la Informática“, 1999, consulta Enero 2007, Disponible en: http://www.monografias.com/trabajos14/discosduros/discosduros.shtml
[3] Manuela Hernandez, “Toshiba presenta el primer disco duro de 1.8 pulgadas con 100GB de Almacenamiento”, Toshiba Storage Device Division, dic. 2006, consulta: Feb 2007. Disponible en: http://www.toshiba-europe.com/storage/products/documents/pressrelease/PR_MK1011GAH_Esp.pdf
[4] M.C. Ginzburg, “Funcionamiento de los Discos Magnéticos y Ópticos”, 1999, consulta Feb 2007. Disponible en: http://www.monografias.com/trabajos14/discosfuncionam/discosfuncionam.shtml
[5] Eduardo Tapia "Los Discos Duros", Mayo 2005, consulta: Dic. 2006. Disponible en: http://computer.howstuffworks.com
[6] Revista.consumer.es "PC´s silenciosos", jun 2006, consulta: Enero 2007. Disponible en: http://www.cienciaviva.net/noticias/grabmagnetica.pdf
[7] Alberto Cobo, Hector Gonzalez, "Discos", 1999, consulta: Enero 2007. Disponible en: http://media.wiley.com/product_data/excerpt/57/07821443/0782144357.pdf
[8] Recovery Labs, "Consejos sobre Discos Duros", 2007, consulta: Enero 2007. Disponible en: http://www.seagate.com/content/pdf/datasheet/disc/ds_barracuda_7200_10.pdf
[9] Alfonso Jimenez,"Forzando Discos Duros", 2007, consulta: Enero 2007. Disponible en: http://www.pcguide.com/ref/hdd/file/part-i.htm
[10] Camilo Sperberg "Discos duros: Conceptos, Configuraciones e Historia", Feb 2006, consulta: Dic. 2006. Disponible en: http://www.novell.com/es-es/documentation/suse8enterprise/pdfdoc/sles-inst-ipseries.pdf
[11] Darío Pescador Albiach, "El Disco Duro en Internet", Ene 2007, consulta: Ene 2007. Disponible en: http://www.cs.albany.edu/~berg/incident_handling/Lectures/IncidentHandlingWeek2.pdf
[12] Wolf B. Henry. *An Introduction to Computer Forensics. Gathering Evidence in a Computing Environment.* Disponible en: http://inform.nu/Articles/Vol4/v4n2p047-052.pdf
[13] Alberto Ballestin, "Unidad de Estado Solido de 32 GB", Scandisk, Enero 2007, consulta: Enero 2007. Disponible en: http://www.seagate.com/support/disc/manuals/ata/d1153r17.pdf
[14] Jeff Wilson,“Computer Hardware”, Dic. 2005, consulta: Enero 2007. Disponible en: http://www.hardwarezone.com/articles/view.php?cid=1&id=1805&pg=2
[15] Angelina E. Trujillo, “Alternate Data Stream” México 2006, consulta Enero 2007.

CAPÍTULO II

SISTEMAS DE ARCHIVOS

RESUMEN. En este capítulo se explica lo que es un sistema de archivos (*file system*), el cual contiene directorios que asocian nombres de archivos con archivos, usualmente conectando el nombre de archivo a un índice en una tabla de asignación de archivos de algún tipo, como FAT en sistemas de archivos MS-DOS o los inodos de los sistemas Unix. Además se describen los sistemas de archivos más importantes, tanto de software propietario como de software libre, se explica, con que elemento se lleva a cabo la manipulación de archivos, es decir, como el usuario interactúa con el sistema y finalmente se explica como se almacenan los archivos en los sectores del disco, desde el punto de vista del sistema de archivos.

2.1 SISTEMAS OPERATIVOS

Según la definición de W. Stallings [1]:

Un sistema operativo es un programa que controla la ejecución de los programas de aplicación y que actúa como interfaz entre el usuario de un computador y el hardware de la misma. Puede considerarse que un sistema operativo tiene tres objetivos o lleva a cabo tres funciones:

- **Comodidad**: Un sistema operativo hace que un computador sea más cómodo de utilizar.

- **Eficiencia**: Un sistema operativo permite que los recursos de un sistema informático se aprovechen de una manera más eficiente.

- **Capacidad de evolución**: Un sistema operativo debe construirse de modo que permita el desarrollo efectivo, la verificación y la introducción de nuevas funciones en el sistema y, a la vez, no interferir en los servicios que brinda.

Además una de las funciones más importantes del sistema operativo es aumentar la productividad del usuario permitiéndole ejecutar varios programas de forma simultanea (si la máquina dispone de varios procesadores), o pseudo-simultánea (si sólo dispone de uno, alternando rápidamente la ejecución de varios programas para dar la sensación de ejecución en paralelo), y evitar que los programas puedan interferirse entre si.

Esto es un sistema operativo visto desde un punto de vista muy interno. Desde una perspectiva más amplia, se puede considerar al sistema operativo como la suma de varios componentes:

- **Kernel ó Núcleo**: se puede definir como el corazón de un sistema operativo. Es el encargado de que el software y el hardware de una computadora puedan trabajar

juntos. Es el software responsable de facilitar a los distintos programas acceso seguro al hardware de la computadora o en forma más básica, es el encargado de gestionar recursos, a través de servicios de llamada al sistema. Como hay muchos programas y el acceso al hardware es limitado, el núcleo también se encarga de decidir qué programa podrá hacer uso de un dispositivo de hardware y durante cuánto tiempo, lo que se conoce como multiplexado.

- **Shell**: es la parte del sistema operativo que interactúa realmente con el usuario, utilizando las llamadas al sistema proporcionadas por el núcleo, para permitir al usuario ejecutar programas y algunas otras funciones de apoyo (como cambiar un directorio). Si bien suele considerarse al shell como la interfaz de línea de comandos (por ejemplo en Windows, "la ventana de ms-dos"), no hay ningún problema en considerar a la interfaz gráfica de ventanas también como shell, aunque en Unix (al contrario que en los sistemas operativos Windows o MacOS), se da la característica de que el usuario puede elegir entre varias shell, tanto de línea de comandos como gráficas, para elegir y personalizar aquella con la que más a gusto se sienta.

Los sistemas operativos existen en estados volátiles y no volátiles. Los *datos no volátiles* son aquellos que permanecen, incluso después de que se apaga una computadora. Tal como un sistema de archivos en un disco duro. Los *datos volátiles* son aquellos, que cuando un sistema está en operación y se apaga la estación de trabajo, dichos datos se pierden, tal como ocurre en las conexiones de red.

En el capítulo anterior se explicó que las unidades de disco duro solamente se encargan de leer y escribir datos basándose en los principios electromagnéticos.

No entienden que es un archivo o directorio, por lo que el sistema operativo se encarga crear estas entidades para administrar la información a través de un sistema de archivos. En este capítulo se explicará como los sistemas de archivos son capaces de organizar toda esa información.

Cabe mencionar que la fuente principal de datos *no volátiles* en un sistema operativo es el sistema de archivos. El sistema de archivos es generalmente la fuente de información más rica y grande en el sistema operativo, llegando a contener la mayoría de la información recuperada durante un típico evento forense.

El sistema de archivos almacena al sistema operativo en uno o más medios. Un sistema de archivos generalmente contiene muchos tipos de archivos, cada uno de los cuales adquiere cierto valor para los analistas en diferentes situaciones.

Así mismo, se puede recuperar información importante residual ubicada en el espacio libre de un sistema de archivos.

2.2 SISTEMAS DE ARCHIVOS

Un sistema de archivo es una colección de archivos y directorios que realizan un conjunto estructurado de información, [2].

Los sistemas de archivos deben ser consistentes entre los sistemas que usan el mismo sistema de archivo. Por ejemplo, un sistema de archivos necesita su propia estructura de organización de archivos de información y, el otro componente es la información proporcionada por el usuario. Debido a que un sistema de archivos esta contenido en una partición, debe haber datos o archivos que describan su distribución y tamaño, así como también un cálculo aproximado acerca de que tan grandes serán las unidades de almacenaje de datos (clusters, bloques, etc.).

Las unidades de almacenaje de información, los cuales son grupos de sectores que mantienen la información, se les denomina unidades de asignación, clusters, bloques y nombres similares dependiendo del tipo de sistema de archivo que se esté usando. Un sistema de archivo necesita tener un método para nombrar a la información y por lo tanto un sistema de nombres de archivos. Los nombres de archivos están usualmente contenidos en directorios como un atributo o campo, en una base de datos de archivos y directorios, [3].

La naturaleza de las estructuras lógicas en un disco duro tiene una importante influencia en el rendimiento, confiabilidad y capacidad de expansión en el medio, [4].

Los nombres de archivo tienen que enlazarse a la información actual que incluye ese nombre de archivo, para que el sistema operativo pueda localizar la información, esto lo hace por medio de tablas, como lo hace el sistema de archivo FAT (File Allocation Table) o como la tabla maestra de archivo MFT (Master File Table) en NTFS (New Technology File System).

Estas tablas son utilizadas por los sistemas de archivos de Windows FAT y NTFS para saber el tamaño de la información que se va a almacenar, así como el uso y la disponibilidad de la unidad de asignación, ya que sin esta función la información se podría sobrescribir. Cabe señalar que en NTFS y otros sistemas, la descripción de la información de las unidades de asignación se lleva a cabo con el mapa de bits de volumen VBM (Volume Bit Map), el cual es un arreglo de bits, en donde cada bit representa una unidad de asignación. Un 0 significa que está disponible y un 1 significa que está ocupado.

La mayoría de los sistemas de archivos contienen mucha más información acerca de los archivos que almacena, esto es, que la información toma la forma de fechas y horas del último acceso de la creación del archivo y la última fecha de modificación, así como también toma la forma de permisos de archivo y listas de control ACL´s (Access Control Lists).

NTFS almacena una lista de control de acceso con cada archivo o carpeta contenidos en un volumen NTFS. Esta lista contiene todas las cuentas de usuario y grupos que tienen garantizado el acceso a dicho archivo o carpeta, así como los permisos que tienen concedidos. Cuando un usuario intenta acceder a un recurso, la ACL debe contener una entrada denominada entrada de control de acceso ACE (Access Control Entrance). Si no existe una ACE en la ACL, el usuario no podrá acceder a dicho recurso.

En resumen, cuando se crea una partición, sus límites y tipo se describen en una tabla de partición, es decir, en esta tabla se señala el punto de inicio y término de la partición, así como su tamaño entre otras cosas.

Como se explicó, un sistema de archivos permite mantener a los archivos organizados. Por otro lado, el medio que utiliza el usuario para manipular los archivos y directorios es un gestor, selector o administrador de archivos, el cual, se estudiará a continuación.

Administrador de archivos

El administrador de archivos es la parte del sistema operativo que maneja la organización, lectura y escritura de los datos localizados en los dispositivos físicos de almacenamiento de información, como un disco duro. Esta información incluye la información de documentos, así como otras colecciones de información utilizada para mantener la jerarquía en un sistema de archivos y otros servicios de sistema.

Para realizar estas tareas, el administrador de archivos interactúa con muchos otros componentes lógicos del sistema. Por ejemplo, el administrador de recursos utiliza las rutinas del administrador de archivos, cuando necesita leer o escribir información en el disco duro. Algo similar ocurre cuando el administrador de archivos llama al administrador de elementos para leer o escribir información acerca de las dependencias de un archivo o para leer o escribir información acerca de la información de un archivo. También se utiliza el administrador de archivos para ejecutar operaciones en directorios y volúmenes [5].

El administrador de archivos provee un gran número de rutinas para ejecutar varias operaciones en los archivos, directorios y volúmenes. Los requerimientos de la aplicación a realizar determinarán cual de estas rutinas se va a utilizar. Muchas aplicaciones simplemente necesitan abrir archivos, leer o escribir información en esos archivos y finalmente cerrarlos. Otras aplicaciones quizás proporcionen más capacidades, tal como las de copiar o mover un archivo a otro directorio. Algunas pocas utilidades del sistema de archivos llevan a cabo más operaciones de archivos y de ahí, que se necesite el uso de rutinas avanzadas proporcionadas por el administrador de archivos.

Hasta ahora se ha explicado la definición de un sistema de archivos en general, asimismo la definición del administrador de archivos. A continuación se explicará la forma en como se clasifican los sistemas de archivos. En el capítulo IV se utilizará lo aprendido en este capítulo, para poder identificar el tipo de sistema de archivos de un disco duro comprometido y para recuperar su información.

Inodos

Cuando se maneja Linux, al revisar el sistema de archivo aparece una serie de números conocidos como inodos. Un *inodo* es el objeto usado para grabar información acerca de un archivo.

En general los inodos contienen dos partes. La primera parte contiene las características (permisos, fechas, ubicación, pero NO el nombre) de un archivo regular, directorio, o cualquier otro objeto que pueda contener el sistema de archivos.

La segunda parte contiene punteros hacia los bloques de información, asociados con el contenido del archivo. Los inodos están numerados y cada sistema de archivos contiene su propia lista de inodos. Cuando se crea un nuevo sistema de archivos, una lista completa de inodos se crea en ese sistema de archivos.

En la figura 2.1 se observa la forma en como se estructura el contenido de un archivo.

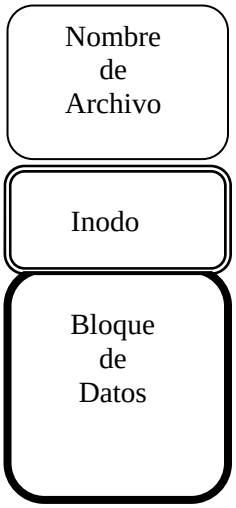


Figura 2.1. Relación entre los componentes de un archivo*

El concepto es particularmente importante para la recuperación de los sistemas de archivos dañados.

Cada inodo queda identificado por un número entero, único dentro del sistema de archivos, y los directorios recogen una lista de parejas formadas por un número de inodo y nombre que permite acceder al archivo en cuestión, cada archivo tiene un único inodo, pero puede tener más de un nombre en distintos o incluso en el mismo directorio para facilitar su localización.

* Fuente. Elaboración propia

Dentro de cada inodo existe la siguiente información:

- El identificador del dispositivo que alberga al sistema de archivos.
- El número de inodo que identifica al archivo dentro del sistema de archivos.
- La longitud del archivo en bytes.
- El identificador de usuario del creador o un propietario del archivo con derechos diferenciados.
- El identificador de grupo de un grupo de usuarios con derechos diferenciados.
- El modo de acceso: capacidad de leer, escribir, y ejecutar el archivo por parte del propietario, del grupo y de otros usuarios.
- Las marcas de tiempo con las fechas de última modificación (*mtime*), acceso (*atime*) y de alteración del propio inodo (*ctime*).
- El número de enlaces, esto es, el número de nombres (entradas de directorio) asociados con este inodo.

En la figura 2.2 se muestra la estructura de un inodo

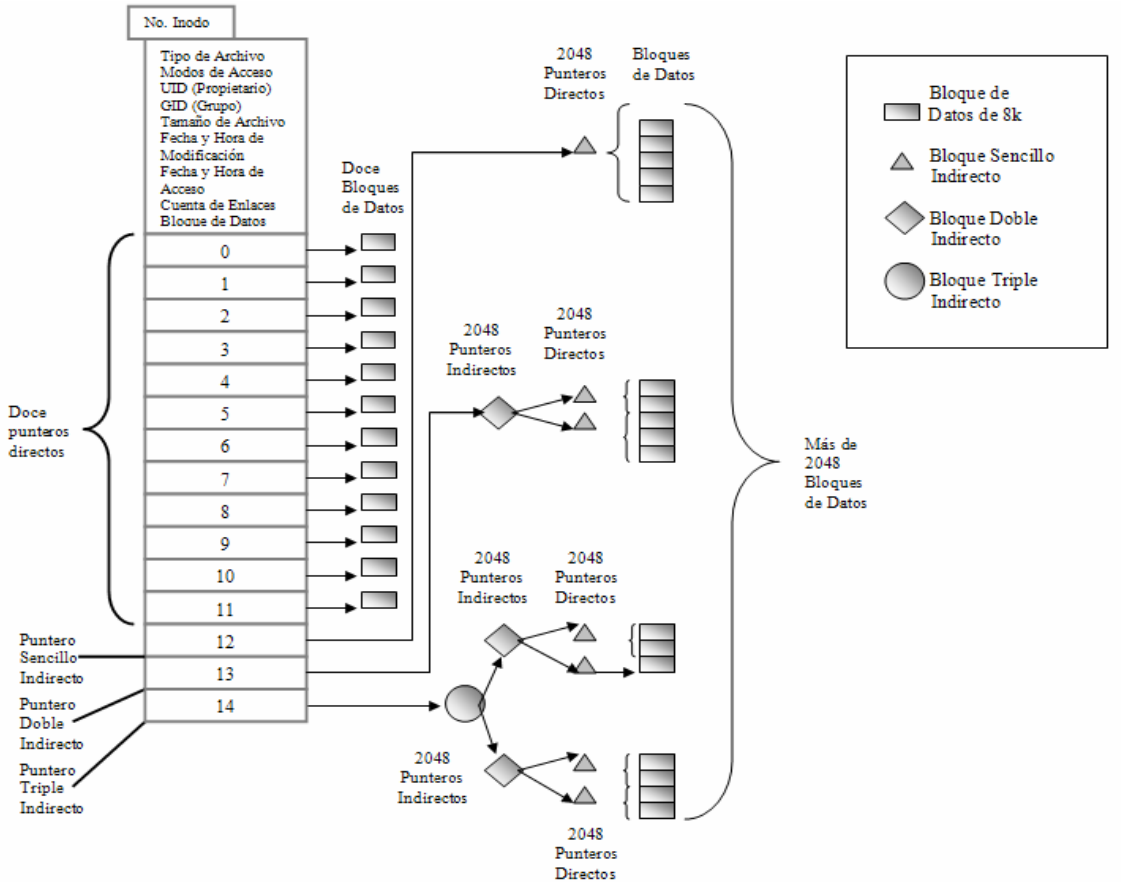


Figura 2.2. Estructura de un inodo[*]

[*] *Fast Track Solaris 10, Modulo I, Student Guide.* Pág. 4-10

Como se observa en la figura 2.2, un inodo contiene quince punteros a bloques de información. Los primeros doce punteros, son punteros directos a doce bloques de información. Cada uno de estos punteros señala hacia un bloque de información de 8 KB hasta completar un archivo mayor de 96 KB.

Los tres tipos de punteros indirectos en un inodo son:

- *Apuntador sencillo indirecto*. Señala hacia un bloque de sistema de archivos que contiene punteros hacia bloques de información. Este bloque contiene 2048 direcciones adicionales, donde cada bloque de información es de 8KB, obteniendo un bloque de información de 16 MB.

- *Apuntador doble indirecto*. Señala hacia un bloque de sistema de archivos que contiene apuntadores sencillos indirectos, en total 2048. cada puntero señala hacia un bloque los punteros de bloque de información. Los punteros dobles indirectos apuntan a un bloque de información de 32 GB.

- *Apuntador triple indirecto.* Pueden señalar a 64 TB de información.

Se puede ver toda esta información contenida en una archivo o directorio si se ejecuta el comando *ls -li* en cualquier directorio del sistema, como se observa en la figura 2.3.

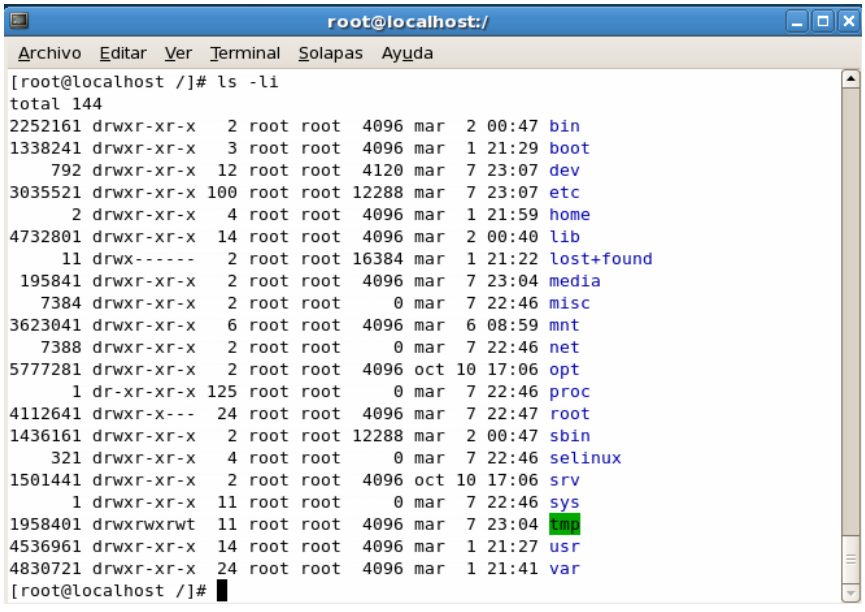


Figura 2.3. Descripción de la información en Linux Fedora 6*

* Fuente. Elaboración propia

El campo de contador de vínculos especifica el número de nombres distintos que tiene el archivo dentro del sistema. En el campo modo de archivo, se especifica para qué se ha abierto el archivo (lectura, escritura, etc.).

La Id del usuario, conocida también como UID es la ID del propietario del archivo. El campo *permisos de acceso* especifica quién puede acceder al archivo y para qué tipo de operación.

La ubicación del archivo en el disco queda especificada, mediante un cierto número de punteros directos e indirectos de bloques de disco que contienen datos del archivo.

El trabajar sobre un sistema de archivos basado en inodos resulta al principio confuso para usuarios que no están habituados a él.

Si múltiples nombres están enlazados, o sea, asociados a un mismo inodo (lo que se denomina enlaces duros o simplemente enlaces), entonces todos los nombres son equivalentes entre sí.

El que fue creado en primer lugar, no tiene ningún estatus especial, contrario a lo que ocurre con los enlaces simbólicos o con los denominados accesos directos, en donde todos dependen del nombre original.

Un inodo puede incluso no tener ningún enlace. Tal archivo sería eliminado del disco, y sus recursos serían liberados para ser reasignados (el proceso normal de suprimir un archivo); pero, si algún proceso estuviera accediendo al archivo, puede seguir haciéndolo, y finalmente el archivo sería sólo suprimido, cuando la última referencia a él quede completamente cerrada.

Esto afecta también los archivos ejecutables, que de forma implícita permanecen abiertos por los procesos que los ejecutan.

Por esta razón, cuando se actualiza un programa, se recomienda suprimir primero el viejo ejecutable y crear a continuación un nuevo archivo y un nuevo inodo para la versión actualizada, de modo que si la versión anterior estaba en ejecución, en ese instante pueda mantenerse temporalmente el archivo y continuar funcionando sin problemas.

Tradicionalmente no era posible identificar un archivo abierto con el nombre del archivo que fue utilizado para abrirlo. El sistema operativo convertiría inmediatamente el nombre a un número de inodo y prescindiría de éste.

Anteriormente era posible hacer enlaces (enlaces duros) a directorios. Esto hacía que la estructura de directorios fuera un grafo dirigido en vez de un árbol.

Se podía dar la paradoja de que un directorio fuera su propio padre. Los sistemas modernos prohíben generalmente este estado confuso.

2.3 CLASIFICACIÓN DE SISTEMAS DE ARCHIVOS

Los sistemas de archivos pueden ser clasificados en tres ramas:

- Sistemas de archivos de disco
- Sistemas de archivos de red
- Sistemas de archivos de propósito especial

Ejemplos de los sistemas de archivos más utilizados son: FAT, NTFS, ext2, ext3, reiserFS.

Sistemas de archivos de disco

Este tipo especial de sistema de archivos está diseñado para el almacenamiento, acceso y manipulación de archivos en un dispositivo de almacenamiento.

Son sistemas de archivos de disco: EFSa, EXT2, EXT3, FAT (sistema de archivos de DOS y algunas versiones de Windows), UMSDOS, FFS, Fossil ,HFS (para Mac OS), HPFS, ISO 9660 (sistema de archivos de solo lectura para CD-ROM), JFS, kfs, MFS (para Mac OS), Minix, NTFS (sistema de archivos de Windows NT, XP y Vista), OFS, ReiserFS, Reiser4, UDF (usado en DVD y en algunos CD-ROM), UFS, XFS, etc, [6].

Sistemas de archivos de red

Es un tipo especial de sistema de archivos diseñado para acceder a sus archivos a través de una red. Este sistema se puede clasificar en dos: los sistemas de ficheros distribuidos (no proporcionan E/S en paralelo) y los sistemas de ficheros paralelos (proporcionan una E/S de datos en paralelo).

Son ejemplos de sistema de archivos distribuidos: AFS, AppleShare, CIFS (también conocido como SMB o Samba), Coda, InterMezzo, NSS (para sistemas Novell Netware 5), NFS. Son ejemplos de sistema de archivos paralelos: PVFS, PAFS.

Sistemas de archivos de propósito especial

Son aquellos tipos de sistemas de archivos que no son ni sistemas de archivos de disco, ni sistemas de archivos de red, [7].

Ejemplos: acme (Plan 9), archfs, cdfs, cfs, devfs, udev, ftpfs, lnfs, nntpfs, plumber (Plan 9), procfs, ROMFS, swap, sysfs, TMPFS, wikifs, LUFS, etc.

Ahora que se ha mencionado la clasificación de los sistemas de archivos podrán ser explicados más detalladamente. Asimismo, siendo Linux el sistema operativo que se maneja en esta tesis, se menciona una breve reseña histórica de su evolución; con el

propósito de dar a conocer que, con esta plataforma, además de contar con herramientas forenses especializadas de código libre como Sleuthkit, es posible analizar los sistemas de archivos de cualquier sistema operativo.

Tipos de sistemas de archivos

Anteriormente se explicó la clasificación de los sistemas de archivos, mencionándose algunos ejemplos de forma general. A continuación, se detallan dichos ejemplos utilizando la misma clasificación anterior.

Para los *sistemas de archivos de discos* se tiene:

FAT (File Allocation Table)

Se conoce como el sistema de archivos más sencillo, compatible con Windows NT. Es un sistema de archivos desarrollado para MS-DOS, así como el sistema de archivos principal de las ediciones no empresariales de Microsoft Windows hasta Windows Me. Es sencillo y por ello, es popular para disquetes, admitido por todos los sistemas operativos existentes para computadora personal.

Contiene una tabla de asignación, la cual se ubica en la parte superior del volumen. Para proteger dicho volumen se conservan dos copias de la FAT, esto previniendo algún daño en alguna de ellas. El disco que esta asignado bajo partición FAT, se asigna en clústeres, cuyo tamaño es determinado por el tamaño del volumen.

Cuando un archivo es creado, se crea a su vez una entrada en el directorio y se establece el primer número de cluster que contiene datos. Funcionando como eslabón de lista indica que éste es el último cluster y señala al siguiente cluster que será utilizado. Dicha tabla debe actualizarse, ya que de lo contrario se pierden datos, sin embargo, esto ocasiona consumo de tiempo, ya que las cabezas lectoras deben cambiar de posición y ponerse a cero en la pista lógica de la unidad cada vez que dicha tabla se actualiza.

El sistema de archivos FAT se compone de cuatro secciones:

- *El sector de arranque*. Siempre es el primer sector de la partición (volumen) e incluye información básica, punteros a las demás secciones, y la dirección de la rutina de arranque del sistema operativo.

- *La región FAT*. Contiene dos copias de la tabla de asignación de archivos (por motivos de seguridad). Estos son mapas de la partición, e indican qué clusters están ocupados por los archivos.

- *La región del directorio raíz*. Es el índice principal de carpetas y archivos.

- *La región de datos.* Es el lugar donde se almacena el contenido de archivos y carpetas. Por tanto, ocupa casi toda la partición. El tamaño de cualquier archivo o carpeta puede ser ampliado, siempre que queden suficientes clusters libres. Cada cluster está enlazado con el siguiente mediante un puntero. Si un determinado cluster no se ocupa por completo, su espacio remanente se desperdicia.

NTFS (New Technology File System)

Sistema de archivos diseñado específicamente para Windows NT, con el objetivo de crear un sistema de archivos eficiente, robusto y con seguridad incorporada desde su base. No hay ninguna dependencia del hardware subyacente, como sectores de 512 bytes, además no hay ninguna ubicación especial en el disco, como las tablas de FAT.

NTFS es un sistema de archivos recuperable, porque hace un seguimiento de las transacciones con el sistema de archivos.

Los nombres de archivo y de directorio pueden tener hasta 255 caracteres de longitud, incluyendo cualquier extensión. Los nombres conservan el modelo de mayúsculas y minúsculas, pero no distinguen mayúsculas de minúsculas. NTFS no realiza ninguna distinción de los nombres de archivo basándose en el modelo de mayúsculas y minúsculas.

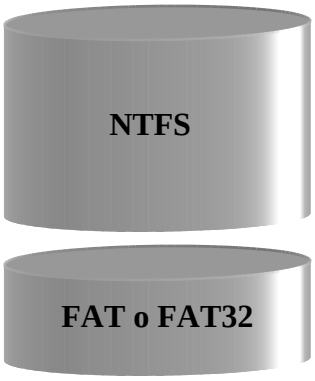
NTFS es un sistema adecuado para las particiones de gran tamaño requeridas en estaciones de trabajo de alto rendimiento y servidores. Puede manejar discos de hasta 2 Terabytes.

Los inconvenientes que plantea son:

- Necesita para sí mismo una buena cantidad de espacio en disco duro, por lo que no es recomendable su uso en discos con menos de 400 MB libres.
- No es compatible con MS-DOS, Windows 95, Windows 98 ni Windows ME.
- No puede ser utilizado en disquetes.

En la figura 2.4 se hace una breve comparación entre los sistemas de archivos de Windows más utilizados.Cabe mencionar que GNU/Linux tiene soporte parcial de escritura y total de lectura en NTFS. Para Enero del 2007 los controladores para Linux en beta están muy avanzados, y han sido incorporados por múltiples distribuciones como Ubuntu, Gentoo, Debian, openSUSE, Mandriva, Fedora, sólo por mencionar algunas.

En NTFS se almacena en forma de *metadatos*, todo lo que tiene que ver con los archivos: nombre, fecha de creación, permisos de acceso, e incluso contenidos, se almacena en forma, los cuales se explicaron en el capítulo I.



- Seguridad a nivel archivo y carpeta
- Compresión de disco.
- Cuotas de cifrado
- Cifrado de archivos.

- Permite un inicio dual.
- Carece de seguridad a nivel de archivo

Figura 2.4. Diferencias entre Sistemas de Archivos de Windows [*]

ext2 (second extended filesystem)

Ext2, se convirtió en el sistema de archivos más popular para Linux durante muchos años. Posee solidez debido a que tras producirse, por ejemplo, un fallo en el suministro de energía, no pudiéndose desmontar el sistema de archivos correctamente, *e2fsck* comienza a analizar los datos del sistema de archivos. Los metadatos son llevados a un estado consistente y los archivos o bloques de datos que estaban pendientes son escritos en un directorio designado para este fin (llamado *lost+found*).

De forma contraria a la mayoría de los sistemas de archivos con bitácora, e2fsck analiza la totalidad del sistema de ficheros y no sólo las pequeñas partes de metadatos modificados recientemente. Este proceso se dilata mucho más que el originado por la comprobación del registro de los datos de un sistema de archivos con bitácora. Dependiendo del tamaño del sistema de ficheros, esta tarea puede llegar a tardar media hora o más. Por tanto, no sería recomendable elegir Ext2 para un servidor que necesite disponer de una alta disponibilidad.

Por otro lado, como Ext2 no necesita mantener un registro y utiliza menos memoria, algunas veces es más rápido que otros sistemas de archivos. El código de Ext2 es el culpable de los sólidos cimientos por los que Ext3 podría convertirse en un sistema de archivos de gran éxito. Su fiabilidad y solidez han sido combinadas elegantemente con las ventajas de un sistema de archivos con bitácora tipo Journaling, [11].

ext3 (third extended filesystem)

Ext3 no sigue la filosofía de utilizar un diseño completamente nuevo. Se basa en Ext2. Estos dos sistemas de archivos están muy estrechamente relacionados.

La diferencia más importante entre Ext2 y Ext3 es que Ext3 soporta la bitácora o Journaling.

[*] Fuente. Elaboración propia

En resumen, Ext3 ofrece tres ventajas principales:

- *Actualizaciones sencillas y muy fiables desde Ext2*. Como Ext3 está basado en el código de Ext2 y comparte su esquema de estructura de disco así como el formato de metadatos, las actualizaciones de Ext2 a Ext3 son increíblemente sencillas. Pueden incluso ser transformadas aunque los sistemas de archivos Ext2 se encuentren montados.

A diferencia de las transiciones a otros sistemas de archivos Journaling, el paso a Ext3 es una cuestión de minutos. Se trata asimismo de un proceso muy seguro, en contraposición a la necesidad de recrear completamente el sistema de archivos, acción que no siempre se produce exenta de errores.

Considerando el número de sistemas Ext2 existentes que esperan una actualización a un sistema de archivos Journaling, es fácil deducir por qué Ext3 puede llegar a tener una gran importancia para muchos administradores de sistemas. Asimismo, pasar de Ext3 a Ext2 es tan fácil como el camino inverso. Sólo es necesario desmontar normalmente el sistema de archivos Ext3 y volverlo a montar como uno Ext2.

- *Fiabilidad y prestaciones.* Otros sistemas de archivos Journaling siguen el modelo "sólo metadatos". Esto significa que los metadatos serán siempre guardados bajo un estado de consistencia pero esto mismo no puede ser garantizado de igual forma para los datos del propio sistema de archivos. Ext3 está diseñado para salvaguardar tanto los metadatos como los datos.

El grado de "seguridad" puede ser personalizado. Si se habilita Ext3 en el modo *data=journal*, se obtiene la máxima seguridad (es decir, integridad de datos) pero esto puede ralentizar el sistema ya que tanto los metadatos como los datos están en modo Journaling.

Una estrategia relativamente nueva consiste en utilizar el modo *data=ordered*, que asegura la integridad tanto de los datos como de los metadatos, pero utiliza Journaling sólo para los metadatos.

El controlador del sistema de archivos recopila todos los bloques de datos que corresponden a una actualización de los metadatos. Estos bloques se agrupan entorno a una "transacción" y son escritos a disco antes de que se actualicen los metadatos. Como resultado, se logra la consistencia de los metadatos y los datos sin necesidad de sacrificar prestaciones.

- *Utilización de data=writeback*. Permite que los datos sean escritos en el sistema de archivos principal una vez que los metadatos han sido consignados en el registro (journal). Esta alternativa se considera frecuentemente como la mejor en relación al rendimiento obtenido.

No obstante, puede hacer que reaparezcan datos antiguos en los archivos tras una situación de bloqueo y recuperación del sistema, aunque la integridad interna del sistema de archivos es mantenida. A no ser que especifique lo contrario, Ext3 se ejecuta con la opción *data=ordered* establecida por defecto.

ReiserFS

Los puntos clave de ReiserFS son las mejoras en la utilización del espacio en disco, prestaciones de acceso y recuperación de bloqueos.

Sin embargo, existe un pequeño inconveniente: ReiserFS presta mucha atención a los metadatos pero no a los datos propiamente dichos. Las futuras generaciones de ReiserFS incluirán Journaling para datos (tanto los metadatos como los datos en sí se escriben en el registro) así como el modo "*ordered*".

Las ventajas de ReiserFS son las siguientes:

- *Una mejor utilización del espacio en disco*. En ReiserFS, todos los datos se organizan en una estructura denominada B*-balanced tree. La estructura en árbol contribuye a una mejora en la utilización del espacio en disco debido a que los archivos de dimensiones reducidas pueden ser almacenados directamente en las hojas del árbol B* en lugar de ser guardados en otro lugar, manteniendo simplemente un referente a la ubicación real en el disco.

Además de esto, el almacenamiento no se distribuye en grupos de 1 o 4 KB, sino en porciones de tamaño exacto al que se necesita. Otro de los beneficios consiste en la asignación dinámica de los inodos.

Esto aumenta la flexibilidad del sistema de archivos a diferencia de las alternativas más tradicionales tales como Ext2, donde la densidad del inodo ha de ser especificada en el momento de creación del sistema de archivos.

- *Mejora en el rendimiento de acceso a disco.* Cuando se trata de archivos pequeños, con frecuencia sucede el hecho de que tanto los datos del archivo como la información del "*stat_data*" (inodo) están almacenados unos junto a otros. Pueden ser leídos mediante una sola operación de E/S en el disco, lo que significa que sólo se requiere un único acceso para recuperar toda la información necesaria.

- *Una rápida recuperación tras los bloqueos*. El hecho de utilizar un registro para monitorizar las recientes modificaciones en los metadatos hace que la comprobación del sistema de archivos pueda tener lugar en unos segundos, incluso si se trata de un sistema de gran tamaño.

XFS

Es un sistema de archivos de 64 bits con journaling de alto rendimiento.

XFS es lo suficientemente estable para incorporarlo en la rama principal de desarrollo del kernel. Los programas de instalación de las distribuciones de SuSE, Gentoo, Mandriva, Slackware, Fedora Core, Ubuntu y Debian ofrecen XFS como un sistema de archivos más. En FreeBSD se añadió el soporte para solo-lectura de XFS a partir de Diciembre de 2005 y en Junio de 2006 fue incorporado un soporte experimental de escritura a FreeBSD-7.0-CURRENT.

JFS

Debido a que se trata enteramente de un sistema de archivos de 64 bits, JFS soporta tanto archivos como particiones de gran tamaño, lo cual constituye una ventaja adicional para su utilización en entornos de servidor.

A continuación se detallan las razones de por qué JFS puede considerarse como una buena opción para un servidor Linux:

- *Journaling eficiente*. JFS sigue un modelo "sólo metadatos" de forma equivalente a ReiserFS. En lugar de realizar una comprobación exhaustiva, sólo se examinan los cambios en los metadatos generados por una actividad reciente en el sistema de archivos, hecho que ahorra una gran cantidad de tiempo en la recuperación. Por otro lado, pueden combinarse operaciones coincidentes que requieran múltiples entradas concurrentes en el registro en una única operación en grupo, lo que disminuye las pérdidas de rendimiento del sistema de archivos durante la ejecución de múltiples operaciones de escritura.

- *Una organización de directorios efectiva*. JFS utiliza diferentes organizaciones de directorio. Para directorios pequeños, permite que el contenido de éstos se almacene directamente en su inodo correspondiente. En el caso de los de mayor tamaño, utiliza los árboles B*, lo que facilita en gran medida la gestión de los directorios.

- *Un mejor uso del espacio mediante la asignación dinámica de los inodos.* En Ext2, es necesario definir la densidad del inodo con antelación (el espacio ocupado por la información de gestión), lo que restringe el máximo número de archivos o directorios en el sistema de archivos. JFS exime de estas obligaciones: es capaz de asignar dinámicamente el espacio del inodo y liberarlo cuando ya no es necesario.

ISO 9660

El estándar ISO 9660 es una norma publicada, que especifica el formato para el almacenaje de archivos en los soportes de tipo disco compacto.

El estándar ISO 9660 define un sistema de archivos para CD-ROM. Su propósito es que tales medios sean legibles por diferentes sistemas operativos, de diferentes proveedores y en diferentes plataformas, por ejemplo, MS-DOS, Microsoft Windows, Mac OS y UNIX.

La norma ISO 9660 es descendiente directa de un esfuerzo de estandarización anterior llamado 'HSG (acrónimo de High Sierra Group), el cual fue propuesto por un conjunto de actores de la industria que se reunieron en 1985 en el hotel High Sierra, de Lake Tahoe, Nevada. Aunque la ISO aceptó una gran mayoría de las propuestas del HSG, existen algunas diferencias menores. Los discos compactos por definición están divididos en sectores, y se define que hay 75 sectores por cada segundo de audio.

Dado que el formato de audio en un disco compacto se define con una codificación PCM de 16 bits, estéreo, cada segundo de audio tiene 176400 bytes. El tamaño del sector físico luego es de 2352 bytes (176400 bytes/75 sectores). Los DVDs pueden utilizar también la norma ISO 9660, pero el formato UDF es por lo general el más utilizado.

Para los *sistemas de archivos de red* se tiene:

SAMBA

Samba es un servidor SMB libre, y como casi todos los proyectos distribuidos, bajo la Licencia Publica General de GNU. Samba es capaz de ejecutarse en una gran cantidad de variantes Unix, como Linux, Solaris, SunOS, HP-UX, ULTRIX, Unix de Digital, SCO Open Server y AIX por nombrar tan sólo algunas. Con Samba se puede hacer que un sistema Linux actúe como servidor SMB dentro de una red, permitiendo a otros equipos (que por lo general serán otras máquinas Windows) acceder a recursos compartidos como directorios e impresora.

Samba es en sí un paquete muy complejo, el cual brinda a los usuarios Unix un sin fin de posibilidades a la hora de interactuar con equipos Windows y Unix, que estén coexistiendo en redes heterogéneas, lo que permite que:

- Compartir una unidad de Linux con computadoras Windows.
- Compartir una unidad de Windows con computadoras Linux.
- Compartir una impresora de Linux con computadoras Windows.
- Compartir una impresora de Windows con computadoras Linux.

Los beneficios de utilizar samba son:

- Compartir uno o más sistemas de archivos.
- Compartir impresoras, instaladas tanto en el servidor como en los clientes.
- Samba permite compartir entre máquinas Windows y Linux recursos.
- Siendo un recurso una carpeta o la impresora.

NFS (Network File System)

Permite acceder a los archivos remotos exactamente igual que si fueran locales. Esto se hace programando parte de la funcionalidad a nivel del núcleo (en el lado del cliente) y la otra parte como un demonio servidor. El acceso a los archivos es totalmente transparente al cliente, funcionando con muchas arquitecturas de servidores.

Se recomienda utilizar NFS dentro de una red local, detrás de un firewall que permita el acceso sólo a las máquinas que integren la red local, nunca para compartir sistemas de archivos a través de Internet.

Al no contar con un sistema de autenticación por contraseñas, es un servicio susceptible del ataque de algún atacante. SAMBA es un protocolo mucho mejor y más seguro para compartir sistemas de archivos.

Los beneficios de utilizar este sistema de archivo son:

- Los datos accedidos por todo tipo de usuarios pueden mantenerse en un nodo central, con clientes que montan los directorios en el momento de arrancar. Por ejemplo, puede mantener todas las cuentas de usuario en una máquina, y hacer que las demás monten dichas cuentas en su directorio /home por NFS. Además si se instala NIS, los usuarios podrían entrar y trabajar de forma transparente en cualquiera de las máquinas.
- Los datos que consumen grandes cantidades de espacio de disco pueden mantenerse en un nodo.
- Los datos de administración pueden mantenerse también en un solo nodo. Ya no será necesario usar rcp para instalar el mismo fichero en 20 máquinas distintas.

Para los *sistemas de archivos de propósito general* se tiene:

SWAP

La *swap* es el espacio de intercambio, es una zona del disco que se usa para guardar las imágenes de los procesos que no han de mantenerse en memoria física.

La mayoría de los sistemas operativos modernos poseen un mecanismo llamado memoria virtual, que permite hacer creer a los programas que tienen más memoria que la disponible realmente; por ejemplo, 4 Gigabytes en un ordenador de 32 bits. Como en realidad no se tiene físicamente toda esa memoria, algunos procesos no podrán ser ubicados en la memoria RAM.

En este caso es útil el espacio de intercambio: el sistema operativo puede buscar un proceso poco activo, y moverlo al área de intercambio (el disco duro) y de esa forma liberar la memoria principal para cargar otros procesos. Mientras no haga falta, el proceso extraído

de memoria puede quedarse en el disco, ya que ahí no gasta memoria física. Cuando sea necesario, el sistema vuelve a hacer un intercambio, pasándolo del disco a memoria RAM. Es un proceso lento comparado con usar sólo la memoria RAM, pero permite dar la impresión de que hay más memoria disponible.

- **En Windows**

Hay una opción llamada *"Memoria Virtual"*, con la cual se puede configurar el tamaño del archivo de paginación usado por Windows.

- **En Linux**

Linux se suele usar con una partición de intercambio, aunque también permite usar ficheros de intercambio. Se pueden asignar varios dispositivos de intercambio, incluso de diferentes tipos, y asignar a cada uno una prioridad.

devfs

Es un sistema de archivos virtual utilizado por el sistema operativo Unix y los sistemas operativos derivados de este, cuyo propósito es controlar los archivos de dispositivos, que se hallan almacenados en el directorio /*dev* de la estructura de archivos convencional.

Se introdujo como solución a los problemas de límite de números de dispositivos en los kernel de versiones anteriores y en la nomenclatura.

Devfs permite crear los archivos de dispositivos, cuando se carga el módulo correspondiente. Además, el autor de módulo puede controlar el nombre del archivo y los derechos de acceso a éste. Además, se puede crear los enlaces simbólicos y directorios para organizar los archivos, aunque es la tarea del devfsd; además devfs está en los núcleos 2.4.

2.4 COMENTARIOS

Se aprendió que la función que cumple un sistema de archivos es la de organizar de una manera estructurada la información en forma de archivos, en carpetas o directorios. También se aprendió que existe una gran variedad de sistemas de archivos, los cuales le dan un formato lógico a la partición donde se va a instalar un sistema operativo. Usualmente cuando se instala un sistema operativo Windows XP, el sistema de archivos que se utiliza para darle formato al disco es la de NTFS.

En el caso particular de esta tesis, se instaló un sistema operativo SUSE Linux con un sistema de archivos ext3 en un disco duro de 80 Gigabytes, con el fin de analizar un disco duro comprometido de 2 Gigabytes con un sistema de archivos del tipo NTFS.

El conocer como se organiza la información en un determinado sistema de archivo es sumamente importante, desde el punto de vista de la informática forense, ya que permite al investigador saber en que partición se puede encontrar evidencia que sea vital en un proceso legal.

En los capítulos III y IV se explicará lo que es la informática forense, así como las instituciones nacionales e internacionales que se encargan de manejar la evidencia electrónica. Asimismo, se expondrá la metodología a seguir para la recolección de evidencia del disco comprometido, haciendo uso de la herramienta *Sleuthkit*, de código abierto, que corre en sistemas operativos Linux y que permite, en la mayoría de los casos, recuperar la información perdida, manteniendo la integridad de la evidencia.

Referencias

[1] W.Stallings, “Sistemas Operativos” , 1999, consulta: Enero 2007. Disponible en : http://www.escomposlinux.org/fer_y_juanjo/index.php
[2] *Fast Track Solaris 10, Modulo I, Student Guide.*
[3] *Ismael Olea, "Sistema de Archivos", Abril 2001, consulta: Feb 2007. Disponible en:* http://media.wiley.com/product_data/excerpt/57/07821443/0782144357.pdf
[4] Microsoft, "Elija el sistema de archivos que se ajuste a sus necesidades", marzo 2002, consulta: Feb. 2007. Disponible en: https://www.microsoft.com/latam/windowsxp/pro/evaluacion/resumen/filesystem.asp
[5] Gonzalo Alvarez Marañón y Pedro Pablo Fábrega Martínez "Seguridad del Sistema de Archivos", 1999, consulta: Feb. 2007. Disponible en: http://developer.apple.com/documentation/Carbon/Reference/File_Manager/file_manager.pdf
[6] Thomas Tempelmann, Natasha Portillo "Sistema de Archivos para Mac", abril 2002, consulta: Feb 2007. Disponible en: http://www.tempel.org/joliet/es/index.html
[7] Cornella, Alfonso. Los recursos de información: ventaja competitiva de las empresas. Madrid: McGrawHill,1994
[8] Enciso Carvajal, Berta La Biblioteca: bibliosistemática e información Alicante: Biblioteca Virtual Miguel de Cervantes, 2000. Disponible en:http://www.cervantesvirtual.com
[9] M. Benoit, "Linux File System Benchmarks", 2003, consulta: Feb 2007, Disponible en: http://www.enespanol.com.ar/2006/04/23/comparacion-de-sistemas-de-archivos-en-linux/
[10] *Linux Máxima Seguridad*. *Edición especial*. Editorial Prentice Hall
[11] J. Piszcz, "Benchmarking Filesystems Part II", 2006, consulta: Feb. 2007, disponible en: http://linuxgazette.net/122/TWDT.html#piszcz

CAPÍTULO III

METODOLOGÍA PROPUESTA

RESUMEN. En este capítulo se presentan los conceptos de informática, evidencia y proceso forense, sus objetivos e importancia; así como también los roles y responsabilidades de cada una de las personas que participan directamente en el proceso forense. Además, se analizan los principios para el manejo de la evidencia digital, recomendados por organizaciones internacionales como el IOCE (International Organization on Computer Evidence), el NIST (National Institute of Standards and Technology), entre otras, para finalmente, establecer una metodología propia que servirá como una referencia a especialistas en seguridad informática para recuperar la información borrada de un disco duro, a través de una herramienta que funciona en software libre, con base a los criterios que ofrecen estos organismos tales como respetar y mantener la integridad de la evidencia digital, utilizar herramientas forenses de fácil manejo para la recuperación de información, generación de copias de trabajo de la evidencia, etc.

3.1 ANTECEDENTES

Es necesario explicar el concepto de informática forense, así como lo relacionado con esta ciencia, para entender como puede ayudar a la sociedad; para que los resultados obtenidos de la evidencia ayuden a las instituciones jurídicas correspondientes a encarcelar a personas que hacen mal uso de la tecnología, con el fin de sacar provecho de una manera deshonesta, lo cual puede afectar a terceras partes.

Definición de la informática forense

Por definición, la ciencia forense es cualquier aspecto de una ciencia relacionado con el derecho. Cualquier técnica o principio científico que pueda aplicarse a la identificación, preservación, análisis y presentación de la evidencia durante una investigación es parte de la ciencia forense. A continuación se enlistan por categoría criminal, las actividades ilícitas que podrían motivar una investigación en los sistemas informáticos [1]:

Crímenes de Fraude o Financieros

- Intrusiones por computadora
- Fraude Económico
- Extorsión
- Fraudes en subastas

Crímenes Sexuales

- Abuso o explotación de niños
- Pornografía
- Prostitución

Crímenes en contra de Personas

- Investigación de la muerte de una persona
- Violencia doméstica o social
- Amenaza por E-mail / Acoso / Acecho

Como se puede observar en esta lista, los sistemas informáticos pueden estar involucrados de manera sutil en una gran cantidad de crímenes, los cuales ya se encontraban previamente tipificados y en los que la computadora no es usada para cometer el delito. Sin embargo, contiene evidencia relativa al crimen. La informática forense persigue los siguientes tres objetivos fundamentales:

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

Evidencia digital

Una definición más precisa tomada de Casey, [2] señala que:

"La evidencia digital comprende todos los datos digitales que permitan establecer que un crimen ha sido cometido o proporcionen un vínculo entre un crimen y su víctima, o un crimen y su autor."

La evidencia digital en un ataque informático puede encontrarse en gran cantidad de fuentes. El disco duro, que es el dispositivo de almacenamiento masivo por excelencia puede almacenar gran cantidad de información relativa al comportamiento del atacante en el sistema; las cámaras digitales pueden contener fotografías que han sido sometidas a un proceso de esteganografía; los registros de un firewall pueden indicar los intentos hechos para entrar en la red privada. Es necesario que los investigadores estén bien versados en el manejo técnico y legal de la evidencia digital, ya que una recolección inadecuada conduciría a resultados incorrectos o falta de credibilidad en la autenticidad de la evidencia. Dadas las características tan particulares de la evidencia digital, su manejo y estudio supone ciertas ventajas y desventajas en el campo forense.

Ventajas

- Puede copiarse de manera exacta y manejarse tal como si fuera el original.
- Con herramientas adecuadas es relativamente fácil identificar si la evidencia ha sido alterada, comparada con la original.
- Aún si la información es borrada, es posible, en la mayoría de los casos, recuperarla.
- Cuando se trata de destruir evidencia, existen copias o información conexa que permanecen en otros sitios.

Desventajas

- Carencia de software especializado para buscar datos sin alterarlos.
- Posible daño no intencional a los datos visibles o a los escondidos.
- Si el original ha sido copiado de manera exacta es difícil distinguir la copia del original si no se han identificado adecuadamente.
- Conflicto entre las técnicas utilizadas para incautar la evidencia y los sistemas legales.
- Falta de capacitación de la persona que descubre la escena y actúa incorrectamente en detrimento de la evidencia digital.

Por naturaleza propia, la evidencia digital es frágil y efímera. Puede ser alterada, dañada o destruida con mucha facilidad debido a un manejo inadecuado o a un examen impropio. Por esta razón, se deben tomar cuidados especiales para el adecuado manejo de la evidencia digital. El proceso forense, a continuación descrito, provee las herramientas necesarias para el manejo de la evidencia digital en una investigación informática.

El proceso forense

La naturaleza de la evidencia digital es tal, que posee retos especiales para su admisibilidad en una investigación, ya sea de orden legal o corporativa. La ciencia forense provee una metodología básica que contempla el correcto manejo de la evidencia en cada una de sus etapas, según los principios formulados por la IOCE. Este procedimiento comprende, en general, cuatro fases principales, [3].

- Recolección de la evidencia sin alterarla o dañarla.
- Autenticación de la evidencia recolectada para asegurar que es idéntica a la original.
- Análisis de los datos sin modificarlos.
- Reporte final.

FASE 1: RECOLECCIÓN DE LA EVIDENCIA

Es un principio básico de la informática forense tratar de "congelar" la escena del ataque con el propósito de conservar sus características sin alteraciones posteriores. Asimismo, se debe documentar detalladamente cada una de las acciones realizadas, ya que estas notas facilitaran posteriormente la explicación del ataque ante cualquier instancia. La recolección inicial de evidencia debe hacerse de modo tal, que no afecte en lo absoluto, los datos contenidos en el dispositivo general. Existen dos alternativas que permiten recolectar la evidencia digital siguiendo este principio básico: usar un sistema dedicado para la investigación forense e instalar y examinar el dispositivo original que contiene la evidencia en modo de solo lectura; la segunda alternativa es realizar una copia idéntica del dispositivo original y realizar el estudio forense sobre esta copia "imagen" de la evidencia original. La segunda opción es la más aconsejable, ya que posee la ventaja de que se puede trabajar sobre esta copia de respaldo, tal cual fuera la evidencia original, y siendo así, a continuación se puede instalar en modo de solo lectura y comenzar el examen.

FASE 2: AUTENTICACIÓN DE LA EVIDENCIA

Es difícil demostrar que la evidencia recolectada es la misma que la dejada por el atacante. Los dispositivos de almacenamiento se deterioran muy lentamente pero los datos que contienen pueden sufrir alteraciones que cambien completamente su significado. La cadena de custodia y otros métodos a continuación expuestos aseguran que ningún cambio accidental o deliberado ha sido introducido en los datos que conforman la evidencia. Con los datos digitales se tiene la ventaja de que se puede demostrar que la evidencia no ha cambiado en lo absoluto desde el proceso de recolección. Una técnica criptográfica que se realiza en software y que permite

caracterizar numéricamente, y de manera universal, un archivo o incluso los datos de un disco duro entero son las funciones hash como MD5 o SHA-1.

En la fase de recolección de evidencia, se calcula y almacena el valor hash para cada archivo. Con este instrumento se puede comprobar que los datos, con los cuales se está trabajando son idénticos a los originales, inicialmente recolectados.

FASE 3: ANÁLISIS

El proceso de análisis tiene como objetivo revelar todos aquellos datos que tengan un valor probatorio en la investigación y que aporten información para la reconstrucción del incidente. El análisis puede realizarse en el sistema operativo que se desee, siempre y cuando se observe la regla de oro en el manejo de la evidencia: *en cualquier acción que se realice no debe dañarse la evidencia*.

Se cree que no existe una metodología precisa para reconstruir un ataque informático, en vez de ello se realiza un proceso de razonamiento en el que se estudia cada pieza de evidencia disponible (archivo, proceso, entrada en un registro, etc.). Luego se trata de encontrar los vínculos entre estas piezas, se crean hipótesis acerca de cómo se creo esa evidencia y se realizan pruebas para confirmar o contradecir esa hipótesis. Con este proceso se puede reconstruir el ataque de forma muy aproximada a lo que en realidad ocurrió en el sistema atacado. En la ciencia forense, la certeza es un concepto que se usa con mucho cuidado.

El investigador forense no puede estar completamente seguro de lo que ocurrió en la escena del ataque, ya que sólo posee una limitada cantidad de información. Por lo tanto, sólo puede presentar explicaciones posibles basadas en la limitada cantidad de información que ofrece la evidencia. Es importante mencionar que la investigación de un ataque informático consume tiempo y recursos, y que normalmente no se cuenta con demasiado tiempo para responder ante un incidente de seguridad.

FASE 4: REPORTE FINAL

Se debe mencionar cual es el software y número de versión que se usó para su análisis y cuál para la recolección. Que métodos se utilizaron para recolectar y analizar los datos del dispositivo y el por qué se prosiguió de tal o cual forma.

El proceder de las acciones del investigador durante el caso debe regirse por la toma de la mejor decisión. Esta decisión debe fundamentarse en su conocimiento, su habilidad, las circunstancias del incidente y su papel de neutralidad en la investigación. El reporte final debe estar redactado con base en las anotaciones que se hicieron a lo largo del proceso investigativo y debe ser detallado de forma extensa, pero conservando la objetividad en cuanto a lo que es relevante para la investigación.

3.2 IDENTIFICACIÓN DE UN INCIDENTE INFORMÁTICO

Definición de evento o incidente

Un evento es cualquier suceso o circunstancia que se puede observar en un sistema o equipo. Por ejemplo, un usuario accesando a un archivo, un servidor que hace una petición a una página Web, un usuario mandando un e-mail o un firewall bloqueando un intento de conexión son algunos eventos. Los eventos adversos son aquellos con consecuencias negativas, como la caída de sistemas, una negación del servicio debido a saturación de paquetes, uso no autorizado de privilegios de sistema y ejecución de código malicioso que destruye información, [4].

La definición de un incidente de seguridad informática ha cambiado. En el pasado, un incidente de seguridad informática fue idealizado como un evento adverso relacionado con la seguridad, en donde había pérdida de la información, interrupción de la información o la integridad del sistema o alguna interferencia. Nuevos tipos de incidentes han aparecido desde entonces, por lo que la definición de incidente se ha modificado. Un incidente, en estos días, se puede definir como una violación de las políticas de seguridad informática, del uso incorrecto de políticas o prácticas estándares de seguridad. Asimismo, ejemplos actuales de incidentes actuales son, [5]:

- Negación del Servicio *(Denial of Service)*
- Código malicioso
- Acceso no autorizado
- Uso inapropiado

Señales de un incidente

Para muchas organizaciones, el reto del proceso de una respuesta a incidentes es la precisión de la detección de los posibles incidentes, determinando si en efecto un incidente ocurrió, y si fue así, que de que tipo fue, cual fue la extensión que tuvo y la magnitud del problema.

Lo que convierte esto en un reto es la combinación de tres factores:

- Los incidentes se pueden detectar a través de diversos medios, con varios niveles de detalle y fidelidad. La capacidad automática de detección incluye IDS´s, antivirus y analizadores de registros. Los incidentes se pueden detectar también por medios manuales, como los reportes de los usuarios. Algunos incidentes son fáciles de identificar.

- El nivel de señales potenciales de incidentes es típicamente alto: por ejemplo, es común para una organización recibir cientos o incluso millones de alertas de detección de intrusos por día.

- Un conocimiento técnico especializado y una amplia experiencia son necesarias para un análisis eficiente de la información comprometida. En la mayoría de las organizaciones, las pocas personas con este nivel de conocimiento son probablemente asignadas a otras tareas.

Las señales de un incidente pueden caer en una de dos categorías: *Indicadores* y *precursores*.

Un *precursor* es una señal de que un incidente puede ocurrir en el futuro. Una *indicación* es una señal de que un incidente pudo haber ocurrido o que incluso se esta llevando a cabo ahora.

Existe una gran cantidad de tipos de indicadores; como para nombrar a continuación se dan algunos ejemplos:

- El sensor del IDS de red alerta cuando hay un intento de sobreflujo del buffer contra un servidor FTP.
- El antivirus alerta cuando detecta que un host esta infectado con un gusano.
- Se cae el sistema de un servidor Web.
- Los usuarios se quejan de un lento acceso a los host en Internet.
- El administrador del sistema ve un archivo con caracteres poco usuales.
- Los usuarios reportan una amenaza por medio de un e-mail.
- El host guarda un cambio en la configuración de auditoria en su registro.
- La aplicación registra múltiples intentos fallidos de conexión remota de un sistema desconocido.
- El administrador de e-mail ve un gran número de correos rebotados con un contenido sospechoso.
- El administrador de red nota un cambio poco usual en el tráfico de red.

Necesidad de una respuesta a incidentes

Ha llegado a ser sumamente necesaria una respuesta a incidentes, ya que los ataques muy a menudo comprometen tanto al personal, como a la información [6]. El código malicioso como los gusanos *SQL Slammer, Blaster* y *Love* Setter han afectado a millones de sistemas y redes alrededor del mundo.

Por lo tanto se requiere de una respuesta inmediata y efectiva, cuando las defensas de la seguridad informática han sido superadas.

El gobierno federal, el sector privado y universidades han aceptado e implementado el concepto de respuesta a incidentes en la seguridad informática, ya que esta ofrece los siguientes beneficios:

- Respuesta sistemática a incidentes para llevar a cabo los pasos apropiados.
- Ayudar al personal a recuperarse rápida y eficientemente de los incidentes de seguridad, minimizando la pérdida de información y la interrupción de servicios.
- Utilizar la información recabada durante un ataque para estar mejor preparados, la próxima vez que ocurra uno nuevo.

- Manejar apropiadamente las cuestiones legales que pueden surgir en los incidentes.

Los procedimientos deben estar basados en una política de respuesta a incidentes. Los estándares de los procesos operativos son una descripción de los procesos técnicos específicos, procedimientos, listas de verificación y formas utilizadas por el equipo de respuesta a incidentes.

Dichos procesos deben de ser probados, para validar su exactitud y utilidad, para después distribuirlo a todos los miembros del equipo.

Aspecto jurídico

Una razón, por la cual muchos incidentes relacionados con la seguridad no terminan en aprehensiones, es la falta de asesoría jurídica por parte de las organizaciones involucradas.

Varios niveles de aspecto jurídico están disponibles para investigar los incidentes. Agencias de investigación federal como el FBI, y el Servicio Secreto de los Estados Unidos, oficinas de fiscales y departamento jurídico a nivel local y estatal.

El equipo de respuesta a incidentes debe contar con sus propios representantes jurídicos, antes de que un incidente ocurra, con el propósito de discutir las condiciones bajo las cuales se les debe de reportar, como se debe llevar el reporte, que evidencia se recolecto y como fue recolectada.

Estructura del equipo de respuesta a incidentes

Un equipo de respuesta a incidentes debe estar siempre disponible por cualquiera que descubra o sospeche que un incidente involucró a la organización. Uno o más miembros del equipo lo manejarán, dependiendo de la magnitud del incidente y habilidad del personal.

Los analistas estudian la información, determinan el impacto del incidente y actúan apropiadamente para limitar el daño a la organización y reestablecer normalmente los servicios. Sin embargo, el equipo puede contar sólo con algunos miembros, por lo que el éxito del equipo depende de la participación y cooperación individuales.

Asimismo, la estructura de un equipo de respuesta a incidentes recae en una de estas tres categorías:

- Central — Un único y pequeño equipo que maneja los incidentes, efectivo para organizaciones pequeñas.
- Distribuido — Múltiples equipos responsables del manejo de los incidentes de un particular segmento de la organización, es útil para organizaciones con recursos informáticos grandes.

- Coordinado — Un equipo que provee consejos a otros equipos sin tener autoridad sobre ellos.

Personal de respuesta a incidentes

Sin importar cual sea el modelo de respuesta a incidentes que una organización escoja, un sólo empleado tiene que estar a cargo de la respuesta a incidente. En la mayoría de los modelos, la responsabilidad se alcanza generalmente al tener un equipo administrador principal y otro equipo subordinado o secundario, el cual asume la autoridad en la ausencia del principal.

Los administradores usualmente llevan a cabo una variedad de tareas, incluyendo la coordinación con otros equipos y organizaciones superiores y asegurándose de que el equipo cuenta con el personal, recursos y habilidades necesarios. Finalmente el equipo administrador debe ser capaz de mantener buenas relaciones con otros grupos, aún bajo tiempos de gran estrés.

3.3 ROLES Y RESPONSABILIDADES

Las investigaciones de los incidentes son manejados en diferentes formas dependiendo de las circunstancias del incidente y su gravedad, de la preparación y experiencia del equipo de investigación. Los investigadores digitales se comparan a las escenas del crimen, donde las técnicas de investigación son utilizadas por la ley, a fin de ser aplicadas para la creación de procedimientos del manejo de evidencia digital.

Cualquiera que sea el tipo de incidente, todos los tipos de roles son similares. El tratamiento de los incidentes permite saber como el personal existente se desempeña en estos roles, al responder y conducir una investigación. Se puede identificar un conjunto genérico de roles y responsabilidades asociadas, las cuales incluyen, [7]:

- Respuesta Inicial (First Responders)
- Investigadores
- Técnicos
- Custodios de evidencia
- Examinadores Forenses
- Analistas Forenses

Respuesta Inicial

Es el personal calificado, el cuál, es el primero en llegar a la escena del incidente, provee asesoría inicial, y comienza con los procedimientos indicados para la recolección de evidencia.

Las responsabilidades de este equipo son las de asegurar la escena del crimen, pedir apoyo y recolectar evidencias.

Investigadores

Ellos plantean y administran la adquisición, examinación, análisis y reportes de la evidencia electrónica. El líder de la investigación se asegura de que las actividades en la escena de un incidente se lleven a cabo en el orden correcto y a la hora adecuada. También es responsable de entregar la evidencia, preparar un reporte completo y comunicar de cualquier hallazgo o decisión a sus superiores.

Técnicos

Ellos actúan bajo la dirección del líder de la investigación. Son responsables de identificar y recolectar las evidencias, así como de documentar la escena del incidente. Están altamente capacitados para tomar el equipo electrónico y obtener imágenes digitales que residen en la memoria. Más de un técnico se involucra en un incidente, debido a sus diferentes habilidades y conocimiento; además de su experiencia en la escena del incidente para llevar todos los diferentes medios electrónicos involucrados en el incidente.

Guardianes de la evidencia

Ellos protegen toda la evidencia analizada, la cual es depositada en un lugar especial o central. Aceptan la evidencia recolectada por los técnicos, se aseguran de que este debidamente etiquetada, la registran y la mantienen bajo una estricta cadena de custodia, cuyo objetivo es proteger la integridad de la evidencia cuando las personas tengan acceso a ella, documentando dónde se encuentra almacenada la evidencia, que persona estuvo a cargo de la evidencia, por qué motivo tuvo acceso a ella y en qué periodo de tiempo.

Con esto se tiene un control formal sobre la integridad y acceso a la evidencia y se disminuye la posibilidad de que se argumente que, debido a la carencia o mala instrumentación de una política de acceso a la evidencia, alguien haya plantado o modificado la evidencia.

.

Examinadores forenses

Es un personal altamente calificado, el cuál reproduce las imágenes adquiridas del equipo electrónico y recuperan la información digital. Los examinadores hacen la información del elemento visible, a través de un equipo sumamente especializado, ingeniería intensiva de restitución o de otro medio apropiado, no disponible para los técnicos forenses.

Analistas forenses

Ellos evalúan el producto de los examinadores forenses por su significado y valor probativo en el caso.

3.4 DIRECTRICES Y PROCEDIMIENTOS

Los principios del manejo de la evidencia

Para realizar cualquier investigación se deben de seguir los principios básicos para el manejo de la evidencia digital, la cual maneja aspectos tanto físicos como lógicos.

El aspecto físico contempla el hardware, los periféricos y otros medios de almacenamiento, los cuales pueden contener información o los medios para acceder a ella, mientras el aspecto lógico maneja la extracción de información de una fuente de información relevante. La Guía Practica Correcta basada en la Evidencia Electrónica [8] sugiere cuatro principios para el manejo de la evidencia digital.

- Las acciones tomadas por cualquier investigador no deben cambiar la información contenida en los elementos digitales o medios de almacenamiento.
- El personal que tenga acceso a la información original deben ser sumamente competentes y tener la habilidad de explicar sus acciones.
- Se debe documentar o grabar los procesos aplicados convenientemente para una revisión posterior de una tercera parte como seria en el aspecto jurídico, otros equipos de respuesta incidentes, vendedores de software, proveedores de servicio de Internet, etc. Cada paso en la investigación se debe documentar de una manera precisa y adecuada.
- La persona a cargo de la investigación tiene toda la responsabilidad de asegurarse que los principios que han sido mencionados anteriormente se sigan y cumplan con respecto a las leyes gubernamentales.

Según la International Organization on Computer Evidence (IOCE), [9], el manejo de la evidencia digital debe regirse por los siguientes principios fundamentales:

- Cuando se trata con evidencia digital, todos los principios forenses y procedimientos generales deben ser aplicados.
- Al recolectar evidencia digital, las acciones tomadas no deben cambiar esta evidencia.
- Cuando sea necesario que una persona tenga acceso a la evidencia digital original, dicha persona debe estar entrenada para este propósito.
- Toda la actividad referente a la recolección, el acceso, almacenamiento o a la transferencia de evidencia digital, debe documentarse completamente, preservarse y estar disponible para su revisión.
- Un individuo es responsable de todas las acciones tomadas con respecto a la evidencia digital, mientras esté en su poder.
- Cualquier instancia que sea responsable de recolectar, tener acceso, almacenar o transferir evidencia digital es responsable de cumplir con estos principios.

Estos principios ayudan a mantener la integridad y confiabilidad de la evidencia digital. Un manejo adecuado de la evidencia es vital para que sea admisible en un proceso legal. Asimismo, diferentes estándares se aplican en diferentes tipos de investigaciones. El grado de entrenamiento y experiencia requeridos para llevar a cabo una tarea forense depende del nivel de la evidencia requerido en cada caso.

El método de Daubert, propuesto en 2004, en Wesleyan Collage, en EUA, es una serie de estándares que sirven como una guía para el manejo de la evidencia en una corte, propone varios factores de confiabilidad, que se deben de tomar en cuenta a la hora de aplicar y reportar sobre una técnica científica utilizada en una examinación forense. [10]

- **Aplicación.** ¿Se ha probado empíricamente la técnica o teoría científica? De acuerdo a K. Popper (1989) en el Crecimiento del Conocimiento Científico, "el criterio sobre el estatus científico de una teoría es su falsedad, refutabilidad y aplicación."
- **Aceptación.** ¿Ha sido sujeta a revisión o publicación la teoría científica o técnica? Esto asegura que las imperfecciones en la metodología serían detectadas y que la técnica encuentra su camino a través de la vía de la literatura.
- **Tasa de error.** ¿Se conoce cuál es la tasa de error? Las mediciones científicas generalmente se asocian con tazas de error, las cuales se aceptan de acuerdo al grado de precisión. Las amenazas conocidas existen en contra de la validación y confiabilidad en una prueba (experimental o semi-experimental) de una teoría.
- **Credibilidad.** ¿Cuáles son las credenciales de los expertos y su reputación en la comunidad científica? ¿La técnica recae especialmente en las habilidades y equipo de un experto o se puede reproducir por otros expertos en cualquier otro lugar?
- **Claridad.** ¿Se pueden explicar con suficiente claridad y sencillez la técnica y sus resultados para que la corte y el jurado puedan comprender su significado completamente? Se supone que este criterio está incorporado en la explicación de Daubert.

En general, la evidencia debe ser recolectada de una manera tal que sea completamente admisible en la corte y de esa manera evitar que la evidencia pueda ser ignorada, manejada inadecuadamente, o destruida accidentalmente ante la seriedad del incidente.

Modelos de procedimiento para la recolección de evidencia

La Investigación de la Escena del Crimen Electrónica, es una guía de procedimientos para el personal de Respuesta Inicial con el proceso forense, producida por el Departamento de Justicia de los Estados Unidos [11], da las siguientes sugerencias para realizar una aproximación a la escena del crimen digital.

- **Asegurar y evaluar la escena**. Se deben seguir los pasos indicados, de manera segura, para mantener la integridad de la evidencia potencial.
- **Documentación de la escena**. Crear un seguimiento permanente de la escena del crimen y de la evidencia digital de una manera exacta, hasta donde sea posible.
- **Recolección de la evidencia.** Recolectar la evidencia tradicional y digital de manera que preserve su valor probativo.
- **Empaquetado, transporte y almacenaje.** Tener la precaución adecuada cuando se empaque, transporte y almacene la evidencia. Manteniendo la cadena de custodia.

Respuesta a Incidente, [12] una "Metodología de Respuesta al Incidente", propone las siguientes fases al toparse con un incidente o realizar una investigación digital.

- **Preparación previa al incidente.** A través del entrenamiento y la educación, se obtiene un conocimiento para responder a un incidente.
- **Detección de incidentes.** Desarrollo de técnicas sobre como detectar actividades sospechosas.

- **Respuesta inicial.** Confirmar que ocurrió un incidente y obtener la evidencia volátil.
- **Formulación de una estrategia de respuesta.** Responder a un incidente basado en el conocimiento de todos los hechos conocidos desde la fase Inicial de Respuesta.
- **Duplicado.** También respaldos forenses. Basado en el escenario, tratar de recrear una imagen forense física o hacer una recuperación en vivo de la evidencia.
- **Investigación.** Determinar que pasó, quién lo hizo y prevenir que este incidente se repita en el futuro.
- **Implementación de medidas de seguridad.** Aplicar medidas de seguridad para aislar y contener los sistemas infectados.
- **Monitoreo de red.** Monitorear el tráfico de red para el seguimiento de ataques adicionales.
- **Recuperación.** Restaurar el sistema infectado para asegurar el estado operacional.
- **Reporte.** Documentar todos los detalles y los pasos de la investigación del incidente.
- **Seguimiento.** Aprender del incidente al revisar cómo y por qué pasó y hacer los ajustes necesarios.

Una investigación realizada por la Fuerza Aérea de los Estados Unidos propone los siguientes pasos al manejar una investigación forense.

- **Identificación.** Reconocer y determinar el tipo de incidente.
- **Preparación.** Preparar herramientas, técnicas, garantías de búsqueda, autorizaciones y aprobaciones administrativas.
- **Estrategia de aproximación.** Mantener la legalidad de la recolección de evidencia al minimizar el impacto sobre la víctima.
- **Preservación.** Aislar, asegurar, y preservar el estado de la evidencia física y digital.
- **Recolección.** Grabar la escena física y duplicar la evidencia digital.
- **Examinación.** Búsqueda de evidencia relacionada a la sospecha del crimen.
- **Análisis.** Determinar el significado, reconstruir los fragmentos de información y obtener conclusiones basadas en la evidencia encontrada. La fase de Análisis puede pasar por numerosas iteraciones hasta que se sostenga una teoría.
- **Presentación.** Resumir y dar una explicación de las conclusiones.
- **Regreso de evidencia.** Asegurarse de que la propiedad física y digital sea regresada al dueño original.

Cada uno de los modelos de procedimiento y los principios de evidencia contienen puntos clave que deberían considerarse al manejar la evidencia digital.

3.5 HERRAMIENTAS FORENSES

El componente especial de cualquier investigación de un crimen informático es el uso de recolección de herramientas de software especializado o conjunto de herramientas (toolkit), el cual puede extraer y prever información detallada acerca de la computadora o red que se este examinando. Los sets de herramientas vienen en dos tipos, [13]:

- Armada por uno mismo.

- Prefabricada bajada o comprada de cualquiera de los muchos proveedores de software forense.

Durante una investigación informática habrá ocasiones, en las que sea necesario monitorear el tráfico, husmear en la información, e incluso obtener contraseñas. Un conjunto de herramientas forenses para respuesta a incidentes debe contar con los programas adecuados para llevar a cabo estas tareas.

Asimismo, un conjunto de herramientas prefabricado contiene todas las herramientas necesarias para *duplicar*, *capturar* y *analizar* el sistema de archivos y la información almacenada en el disco.

Aquellos que deseen armar su propio conjunto de herramientas a mano pueden hacerlo utilizando una combinación de utilidades freeware y shareware. Los siguientes son tipos de herramientas que se pueden incluir al iniciar una examinación forense.

- Una herramienta para capturar tráfico de red para su análisis.
- Una utilidad para crear imágenes de disco o clones a nivel de bits.
- Una herramienta para obtener contraseñas.
- Una herramienta que reporte puertos TCP/IP abiertos y después los mande de regreso a su proceso original.
- Una herramienta que recupere información eliminada.
- Una utilidad que respalde y edite el registro de Windows.
- Una utilidad que muestre todas las actividades del sistema de archivos en tiempo real.
- Una herramienta que analice las propiedades de los archivos.
- Una herramienta de monitoreo que muestre toda la actividad del registro en tiempo real.
- Una utilidad que muestre cualquier red compartida, incluyendo las locales o las remotas.
- Una herramienta de monitoreo que muestre entradas, salidas y privilegios.
- Una herramienta que muestre archivos abiertos, procesos de objetos, llaves de Registro, DLLs, etc.

Asimismo, cuando se seleccionen las herramientas, hay algunas directrices que deben seguirse:

- Las herramientas de línea de comando son mejores, aquí se debe evitar utilizar herramientas que utilicen una interfaz gráfica.
- Utilizar herramientas que se sepan manejar.
- Crear un disco de respaldo o utilizar una memoria USB para contener las herramientas de recolección de información más importantes.

En el caso de esta tesis, se propone la utilización de la herramienta llamada Sleuthkit, con Autopsy, la cual permite recuperar información “borrada” de un disco duro. A continuación se explicará de manera general qué es Sleuthkit, cuales son sus funciones y

sobre que plataformas trabaja. En el capítulo IV se llevara a cabo una demostración de esta herramienta para la obtención de datos de un disco comprometido.

Sleuthkit

Sleuthkit es un conjunto de herramientas forenses de código abierto para el análisis de los sistemas de archivo de Windows y Unix; permite a los investigadores identificar y recuperar la evidencia de imágenes obtenidas durante la respuesta al incidente o de sistemas activos; es de código abierto, lo que permite a los investigadores verificar las acciones de las herramientas o adecuarlo a necesidades específicas. Además utiliza código de la herramienta de los sistemas de archivo de TCT, pero el código fue modificado para ser una plataforma independiente.

En suma se le agrego la capacidad de analizar los sistemas de archivos del tipo NTFS y FAT. Utiliza un visor forense llamado Autopsy, el cual es una interfaz gráfica de las herramientas del Sleuthkit para automatizar muchos de los procesos y proveer búsquedas de imágenes y verificación de la integridad de la imagen por medio de MD5, [14].

Permite analizar un disco o una imagen de sistema de archivo creada por dd Linux o una aplicación similar, que crea una imagen en crudo. Estas herramientas son de bajo nivel y cada una ejecuta una descripción del sistema de archivos,

Un disco puede contener una o más particiones. Cada una de estas particiones contiene un sistema de archivo. Ejemplos de sistemas de archivo, que manejan esta herramienta son: ext2, ext3, FAT, NTFS, UFS etc. La herramienta *fsstat* muestra los detalles del sistema de archivos en un formato ASCII.

Ejemplos de la información que se muestra: nombre del volumen, último montaje, hora y los detalles acerca de cada “grupo” en el sistema de archivos UNIX. El contenido de capa de un sistema de archivo contiene información de la imagen. La información se almacena en grandes cantidades con nombres como bloques, fragmentos o clusters. Todas las herramientas en esta capa empiezan con la letra “*d”*.

La herramienta *dcat* se utiliza para mostrar los contenidos de una unidad específica, unidades no asignadas de un sistema de archivo, resultando en una cadena de bytes o de contenido eliminado. Se puede buscar la salida del contenido del archivo borrado.

El programa *dcalc* permite identificar la localización de la unidad en la imagen original de una unidad en la imagen generada *dls*. Una nueva característica del Sleuthkit con respecto a TCT es que el argumento “l” en *dls* (o unrm en TCT) lista los detalles de las unidades de información y es similar al comando *ils* en TCT.

Las herramientas del sistema de volumen (dispositivo de administración) permiten examinar el contenido del disco y de otros medios. Soporta particiones DOS, BSD, Mac, Sun, etc. Con estas herramientas se puede identificar dónde se localizan las particiones y extraerlas, para que puedan ser analizadas con las herramientas de análisis de sistemas de archivos.

Sleuthkit se probó en sistemas operativos como:

- Linux
- MAC OS X
- Open Free BSD
- Solaris

Descripción de Autopsy

Es una interfaz gráfica a las herramientas de análisis de investigación digital de la línea de comandos en el Sleuthkit, el cual es de código abierto al igual que Autopsy y funcionan en plataformas UNIX. Como Autopsy está basado en HTML, se puede conectar al servidor de Autopsy desde cualquier otra plataforma. Esta herramienta provee una especie de administrador de archivos y muestra los detalles acerca de la información borrada y las estructuras

Modos de análisis

- Un análisis de *Autopsy* ocurre cuando un sistema de análisis dedicado se utiliza para examinar la información de un sistema comprometido. En este caso, Autopsy y Sleuthkit funcionan en un ambiente adecuado, usualmente un laboratorio.

- Un análisis *en vivo* ocurre cuando el sistema comprometido se analiza, mientras esta en operación. En este caso Autopsy y Sleuthkit corren desde un CD en un ambiente poco adecuado. Esto frecuentemente se utiliza durante una respuesta al incidente, mientras se confirma. Después de que se confirma, se puede obtener la información del sistema, al llevar a cabo un análisis de Autopsy.

Técnicas de búsqueda de evidencia:

- **Listado de archivos.** Se analizan los archivos y directorios incluyendo los nombres de archivos borrados y de archivos basados con nombres en Unicode.

- **Contenido de archivo.** El contenido de los archivos puede ser revisado en crudo, hexa o se puede extraer en formato ASCII. Cuando se interpreta la información, Autopsy lo protege para evitar un posible daño al sistema de análisis local.

- **Clasificación del tipo de archivo.** Las clases de archivos están basadas en sus firmas internas para identificar archivos de un tipo conocido. La extensión del archivo también será comparada con el tipo de archivo para comprobar si a éstos se les cambio su extensión, con el fin de ocultarlos.

- **Actividad del archivo.** En algunos casos tener una línea de tiempo de la actividad del archivo puede ayudar a identificar las áreas de un sistema de archivo que pudiera contener evidencia.

- **Detalles de imagen.** Los detalles de un sistema de archivos se pueden revisar, incluyendo las horas de actividad, lo cual provee información útil durante la recuperación de la información.

dd Linux

El comando dd copia un archivo (de una entrada a una salida estándar, por default) con un tamaño variable de bloque, y además, se pueden ejecutar conversiones de manera opcional en la imagen, [15].

En otras palabras, dd es un comando que convierte y da formato a una imagen de acuerdo a las siguientes opciones:

- if=”archivo” Lee desde el archivo
- of=”archivo” Escribe al archivo
- bs=”bytes” Especifica el tamaño del bloque

La *Computer Forensics Tool Testing (CFTT)*, así como el *National Institute of Standards and Technology (NIST)* tienen como objetivo proveer a los investigadores y analistas forenses herramientas, que ofrezcan resultados precisos. Es por eso que *dd* esta recomendado por estas organizaciones, ya que cumple con los siguientes requisitos:

- Mantiene la integridad del disco
- Registra errores de I/O
- Hace un duplicado o imagen de un disco o una partición por medio de *bit stream*
- Tiene una documentación de ayuda

Existen más opciones para la creación de una imagen, pero estas opciones son suficientes para realizar la imagen del disco comprometido que se estudiará en el capítulo IV.

3.6 INSTITUCIONES INTERNACIONALES

Hay países que cuentan con instituciones dedicadas al mejoramiento de la seguridad informática, a través de la creación de normas y reglas que se ponen en práctica al presentarse un incidente que compromete la seguridad de sus equipos.

En este trabajo se ha revisado el objetivo de estas instituciones internacionales desde el punto de vista de la evidencia forense, con el fin de poder ofrecer una metodología que sea de fácil entendimiento así como también que cumpla con los pasos del proceso forense para poder servir como una referencia para el manejo y recuperación de la información eliminada.

Debido a lo anterior se hace una descripción de cada una de ellas y al final del apartado se presenta una tabla resalando los aspectos más importantes que aborda cada organismo.

IICTFA (Instituto de Investigaciones Científicas y Técnicas de la Federación Argentina)

Este organismo posee un Laboratorio llamado SI6, el cual es un lugar de desarrollo en seguridad informática, [16]. El SI6 tiene como objetivo la generación de conocimiento en el área de Seguridad Informática a través de la investigación y el desarrollo.

Consideran que la suma de esfuerzos mediante la investigación aplicada de tecnologías innovadoras interactuando con la comunidad, es una de las formas más eficientes de crecer en el conocimiento. Por otra parte piensan que la educación, en especial en estas áreas tecnológicas avanzadas, es un pilar fundamental para el bienestar de la sociedad. Por este motivo, los resultados y derivados de las investigaciones de carácter público realizadas por el SI6, se publican bajo la licencia GPL.

Como parte de esta política de intercambio con otros grupos y personas, CITEFA (Ciencias y Tecnologías de la Federación Argentina) celebra convenios de colaboración Científico-Tecnológica, con el propósito de conformar una red con otras instituciones o grupos posibilitando así, la generación de conocimiento de mayor calidad. El SI6 se crea oficialmente como grupo de investigación dependiente del Departamento de Informática de CITEFA en Enero del 2004.

NIST (National Institute of Standards and Technology)

El NIST es una institución de EUA, [17]. Fue fundado en 1901, su misión consiste en elaborar y promover patrones de medición, normas y tecnología con el fin de realzar la productividad, facilitar el comercio y mejorar la calidad de vida. El NIST consta de varios laboratorios, así como también cuenta con el programa de tecnología avanzada. El laboratorio de tecnología de información o ITL (Information Technology Laboratory) tiene la misión de apoyar a los Estados Unidos.

La industria del gobierno y la academia han incrementando la innovación, así como la competitividad industrial a través del progreso de la ciencia de la tecnología de información. La tecnología de información es el motor reconocido para el crecimiento económico nacional y regional. Los investigadores de ITL han desarrollado protocolos detallados y patrones de operaciones, que mitigan las discrepancias anticipadas en su operación; y han establecido los criterios de valoración. Dentro del papel tradicional de NIST como, el superintendente del sistema de medición nacional, ITL está abordando los problemas difíciles en investigación de medición de IT.

ITL formula las métricas, las pruebas, y las herramientas, a pesar de la complejidad de información y la comprensión de software de confianza, los dispositivos de almacenamiento móvil, también los asuntos de la calidad de información, su integridad, y su utilización. Actualmente el NIST continúa desarrollando los patrones de seguridad en el Internet. Las pautas, bajo la ley de administración de seguridad de información federal, asociando los métodos y las técnicas.

Dentro de los laboratorios se concentran en el laboratorio de división de seguridad de computadora, el cual a su vez en una de las ocho divisiones dentro del laboratorio de tecnología de información del NIST.

Su misión general de esta división es aumentar el conocimiento de los riesgos de tecnologías informáticas, informar sobre las vulnerabilidades y los requisitos de protección, particular mente para tecnologías nuevas, investiga e estudia, aconseja a

organismos de la vulnerabilidades, crea técnicas de seguridad redituable, brinda privacidad de sistemas federales delicados.

POLCYB (Police Cyberspace)

La sociedad para patrullar el ciberespacio (POLCYB), [18], fue constituida como una sociedad no lucrativa, ubicada en la colonia británica en Canadá, su objetivo es aumentar patentes internacionales entre profesionales, públicos y particulares para prevenir y combatir los crímenes en el ciberespacio.

Su red internacional incluye a profesionales y público en general, en sectores privados y todos los niveles organizativos. Sus profesionales trabajan en las áreas de ejecución de justicia, en la ley tribunal de justicia, corporaciones de seguridad, e instituciones académicas.

Luchan para compartir información entre ejecutivos, administradores y profesionales de primer nivel, así como pedir un consejo a un experto en su administración global y diversa. También provee la enseñanza pública sobre la protección de información y la seguridad en Internet, conocimiento del cibercrimen, incluyendo los crímenes cometidos por niños y jóvenes. Para cumplir su objetivo ofrecen reuniones trimestrales, conferencias internacionales anuales y foros de debates en enseñanza pública.

NIFS (National Institute of Forensic Science)

Esta institución australiana (NIFS), [19] tiene la misión de ser una parte esencial, así como un soporte para la comunidad de la ciencia forense, así como trabajar con todos los elementos en la comunidad, para el avance de la ciencia forense.

El NISF ha tenido un compromiso para el establecimiento de la educación relevante y el entrenamiento, para garantizar la calidad, crear proyectos de investigación y desarrollo. Proporciona becas para el extranjero, la prevención del manejo de información en bases de datos de referencia y se ha fundado como una parte esencial de la ciencia forense.

El desarrollo de un enfoque estratégico y nacional para la investigación y el desarrollo de la ciencia forense lleva acabo un proceso capaz de aumentar el conocimiento de las actividades de NIFS entre profesionales forenses.

La prevención en educación es relevante en los programas de entrenamiento y oportunidades, por ejemplo el uso eficiente de recursos, incluyendo el financiamiento para la terminación de proyectos en el momento oportuno y programas, facilitan la prueba de competencia en el uso más eficaz de la comunicación electrónica.

Seguridad y Tecnologías de la Información

Esta institución de origen española, brinda servicios sobre seguridad informática, creada por un grupo de especialistas con el propósito de divulgar y conscientizar a los usuarios sobre la importancia de este sector en el campo de las nuevas tecnologías, [20].

En el año 2000 crean un laboratorio de seguridad informática con el propósito de mantener y aumentar los servicios públicos y gratuitos para la comunidad, así como atender la demanda creciente de profesionales y empresas.

Ofrecen servicios de consultaría, como: cristología, revisión de políticas de seguridad, consultaría de Windows y Unix en general, desarrollo de sistemas seguros, clusters, VNP (Virtual Network Private), sistemas de monitoreo y alerta. Estos son algunos de sus servicios, entre otros un antivirus público en Internet, el cual tiene el nombre de virus total y servicio de anti-phishing.

IWS (The Information Warfare Site)

Esta organización del Reino Unido es un recurso en línea que aspira a estimular el debate sobre un rango de asignaturas de seguridad de información u operaciones de información, como es el comercio electrónico. El objetivo de este sitio es desarrollar un énfasis especial sobre las operaciones de información ofensivas y defensivas. [21].

En enero del 2001 IWS lanzó su centro de amenaza de INFOCON (Information Concentrated), el cual es un proyecto de investigación muy importante, que debe crecer rápidamente durante los siguientes meses.

El objetivo es monitorear fuentes de Internet de diferentes actividades y luego analizar tendencias de seguridad. A diferencia de otras organizaciones INFOCON está libre para quien este interesado.

En general IWS es un recurso en línea que aspira a estudiar el debate sobre todo lo que involucra la seguridad informática, como son las operaciones de información, las operaciones de red de computadoras, la seguridad contra la piratería.

El objetivo de este sitio es desarrollar un énfasis especial sobre las operaciones de información ofensivas y defensivas.

ISFS (Information Security and Forensics Society)

La principal misión del ISFS, [22] es hacer cumplir con profesionalismo, la integridad y la innovación en la seguridad informática forense de las computadoras en Hong Kong y las regiones circundantes. Organiza y normaliza la práctica de seguridad informática en cuanto a los profesionales forenses, evalúa con exámenes para verificar que los profesionales en este ramo son calificados tanto en seguridad informática como en la informática forense.

Provee de cursos para apoyar el estudio de la seguridad informática y la informática forense, teniendo cursos de entrenamiento regulares y seminarios, para promover el conocimiento público de la seguridad de información e informática forense.

Sus principales objetivos son el desarrollo de la seguridad informática y técnicas de informática forense, para tener una visión más amplia de tecnologías de información, comparten conocimientos de seguridad informática e informática forense para prevenir la explotación de tecnología para propósitos ilícitos.

Ayuda a fundar disciplinas científicas de seguridad informática y pruebas digitales con profesionales locales e internacionales. A fin de desarrollar programas de entrenamiento y acreditación internacional.

Policía Cibernética de la PFP (Policía Federal Preventiva)

La Unidad de Policía Cibernética de la Policía Federal Preventiva de México [23] toma acciones preventivas en materia de delitos cometidos en Internet y usando medios informáticos, cuenta con un área específica en materia de prevención y atención de denuncias de delitos contra personas menores de edad.

Analiza cómo se comportan las grandes bandas que están en territorio mexicano y que proveen a redes de prostitución infantil, además la Policía Cibernética se encarga de atender las denuncias sobre instrucciones ilegales, rastrear las direcciones sospechosas, identificar hackers, hacer rastreo de programas malignos. Elabora una base de datos para la identificación de patrones para los casos de personas menores de edad extraviadas y analizar las redes que presentan tráfico de niños, niñas y adolescentes.

La tabla 4.1 es una recopilación de la información más importante de los organismos internacionales anteriormente explicados.

Institución	País	Funciones Principales
IICTFA (Instituto de Investigaciones Científicas y Técnicas de la Federación Argentina)	Argentina	• Generar de conocimiento en el área de Seguridad Informática a través de la investigación y el desarrollo. • Publicar los resultados y derivados de las investigaciones de carácter público bajo la licencia GPL.
NIST (National Institute of Standards and Technology)	EUA	• Elaborar y promover patrones de medición, normas y tecnología con el fin de realzar la productividad, facilitar el comercio y mejorar la calidad de vida. • Desarrollar protocolos detallados y patrones de operaciones bajo la ley de administración de seguridad de información federal. • Aumentar el conocimiento de los riesgos de tecnologías informáticas, informar sobre las vulnerabilidades y los requisitos de protección, particular mente para tecnologías nuevas.
POLCYB (Police Cyberspace)	Canada	• Aumentar patentes internacionales entre profesionales, públicos y particulares para prevenir y combatir los crímenes en el ciberespacio. • Proveer la enseñanza pública sobre la protección de información y la seguridad en Internet, conocimiento del cibercrimen, incluyendo los crímenes cometidos por niños y jóvenes.
NIFS (National Institute of Forensic Science)	Australia	• Ser un soporte para la comunidad de la ciencia forense, así como trabajar con todos los elementos en la comunidad, para el avance de la ciencia forense. • Establecer educación relevante y entrenamiento, para garantizar la calidad, crear proyectos de investigación y desarrollo como una parte esencial de la ciencia forense.
Seguridad y Tecnologías de la Información	España	• Brindar servicios sobre seguridad informática con el propósito de divulgar y conscientizar a los usuarios

		sobre la importancia de este sector en el campo de las nuevas tecnologías.
IWS (The Information Warfare Site)	Reino Unido	• Es un recurso en línea que aspira a estudiar el debate sobre todo lo que involucra la seguridad informática, como son las operaciones de información, las operaciones de red de computadoras, la seguridad contra la piratería
ISFS (Information Security and Forensics Society)	China	• Evaluar con exámenes para verificar que los profesionales en este ramo son calificados tanto en seguridad informática como en la informática forense.
Policía Cibernética de la PFP (Policía Federal Preventiva)	Mexico	• Atender delitos como la pornografía infantil, prostitución infantil en Internet, así como el turismo sexual en el que se tiene a la computadora como un medio o fin. • Brindar información sobre las acciones que pueden realizar las personas particulares cuando se encuentren con un caso de pornografía a través de la red.

Tabla 4.1 Organizaciones internacionales [1]

La institución internacional en la que más me apoyé para plantear mi metodología fue el NIST, debido a que proporciona documentos conocidos como "Special Publications 800 -XX (sp800 -XX)" relacionados con el tratamiento de la evidencia digital, así como los roles y responsabilidades de las personas que tienen contacto directo en el proceso forense, además de ser una de las instituciones internacionales más reconocidas en el campo de la ciencia forense.

3.7 METODOLOGÍA PROPUESTA

Con base en los conceptos anteriormente presentados y analizados, así como las recomendaciones de organismos internacionales como el IOCE, NIST, Fuerza Aérea de EUA, entre otros, se propone la siguiente metodología para la recuperación de información en discos duros, la cual servirá como referencia para los especialistas en seguridad informática. Cabe mencionar que no se tomo como referencia ninguna institución o documento nacional debido a que no existe un organismo en México como tal que se dedique al desarrollo de normas o técnicas que sean un soporte para la comunidad de la ciencia forense.

- **Detección del Incidente.** Desarrollo de técnicas sobre como detectar actividades sospechosas. Esto se puede realizar al utilizar herramientas de monitoreo que permitan explorar archivos de registro, archivos de historia del tipo del navegador de Internet.

- **Respuesta Inicial.** Confirmar que sucedió una violación a las políticas de seguridad. Debemos de preguntarnos como y desde donde se llevo a cabo el ataque para poder dar un seguimiento adecuado, manteniendo la integridad de la evidencia que pudiera ser encontrada por el personal de respuesta inicial.

[1] Fuente. Elaboración propia

- **Preparación al Incidente.** Preparar herramientas, técnicas, garantías de búsqueda, autorizaciones y aprobaciones administrativas. Esto quiere decir que es necesario tener una estación de trabajo capaz de manejar la evidencia forense que se recolecte y que a su vez sea manejada adecuadamente. Además, es necesario presentar ante las instancias correspondientes órdenes de trabajo y acceso a los lugares de trabajo, así como a los equipos comprometidos para evitar demandas por negligencias en la labor forense.

- **Aseguramiento de la Evidencia**. Cuidar el dispositivo de almacenamiento de información para mantener la integridad de los datos a través de bolsas antiestáticas, cajas fuertes, o cualquier otro medio de protección, así como también contar con herramientas de desensamble como desarmadores, dados, cutter, etc. Esto es sumamente importante, ya que de esto depende que los implicados en el incidente puedan ser procesados y encarcelados, al realizar un correcto trabajo en la recolección de la evidencia forense.

- **Cadena de Custodia**. Al aplicar la cadena de custodia se asegura que ningún cambio accidental o deliberado se introduzca en los datos que conforman la evidencia, por lo que también se hace uso de algoritmos de encriptación como el MD5 para aplicarlo a la imagen del disco comprometido. Se toma esta medida con el fin de que solo las personas autorizadas tengan acceso a la información y evitar que personas ajenas al área de recuperación de la información puedan borrar parcial o definitivamente las pruebas que pueden llegar a ser una evidencia confiable.

- **Aplicación de la Herramienta Forense en Software Libre.** Después de que se hizo la instalación de una distribución Linux en el laboratorio de pruebas, además de la herramienta forense Sleuthkit con la interfaz gráfica Autopsy, se agrega la imagen que se va analizar, tomando en cuenta que esta es la copia de trabajo. Es necesario saber que tipo de sistema de archivo se va a examinar para poder hacer la elección correcta de la distribución de Linux, evitando problemas innecesarios. Por ejemplo, para examinar un sistema de archivos ext3, se puede utilizar cualquier versión que soporte este sistema de archivos, pero si se desea examinar un sistema de archivos NTFS lo mejor es utilizar una distribución que cuente con librerías que permitan montar este sistema de archivos, por ejemplo, Knoppix, el cual es una versión basada en Debian. Además, la herramienta Autopsy que contiene una interfaz gráfica puede gestionar sistemas de archivos como el NTFS.

- **Búsqueda de la Información.** A través de la interfaz gráfica es más fácil realizar la búsqueda de los datos que han sido eliminados en el menor tiempo posible. Esto se realiza en la copia de trabajo que es creada con el comando dd de Linux y montándolo en forma de sólo lectura como un sistema de archivos por medio de la opción loop de manera que se pueden examinar los datos del disco comprometido.

- **Localización y Recuperación de la Información.** Después de que se ha comprobado que la información esta presente en la imagen del disco comprometido, se debe recobrar para regresarla a su dueño. La localización y recuperación de la información comprometida se debe hacer lo más rápido

posible para que en caso de ser necesario, la información recuperada pueda ser admisible como evidencia en un proceso legal.

- **Elaboración de Reporte.** Es necesario elaborar un reporte donde se explique que tipo de incidente sucedió, y que solución se le dio. En caso de no haber recuperado la información, es necesario especificar las causas.

- **Recomendaciones de Seguridad.** Finalmente se hace una sugerencia a los usuarios de los equipos de cómputo: realizar un respaldo de sus archivos importantes, así como mantener su equipo actualizado con los parches indicados para el sistema operativo que estén manejando, de igual manera una actualización diaria de las bases de antivirus.

Debido a que cada investigación es diferente, con su único conjunto de circunstancias y un particular procedimiento de solución, los resultados para la recuperación de la información eliminada pueden variar.

3.8 COMENTARIOS

La metodología expuesta en el apartado anterior se hizo pensando en las carencias que actualmente se tienen con respecto al manejo de la evidencia digital en nuestro país, ya que ni siquiera se cuenta con una institución dedicada al desarrollo de técnicas y normas relacionadas con la ciencia forense como es el caso de EUA, Canadá, Argentina, etc.

Además, esta metodología fue diseñada para ser lo suficientemente clara y entendible como para poder ser reproducida por cualquier persona o institución, que tenga un incidente donde su información sea comprometida y desee recobrarla nuevamente sin pagar licencias por el uso de software especializado.

En este trabajo como se demostrará en un ejemplo de aplicación en el capítulo IV, se toma como una ventaja la utilización de software libre para la recuperación de los datos eliminados.

Otra parte importante de esta metodología son los requerimientos físicos y lógicos que la estación de trabajo o laboratorio de pruebas debe poseer, por ejemplo, debe de tener un disco duro con gran capacidad (se recomienda un par de discos de 160 GB para los discos duros de estaciones forenses), así como también una cantidad de memoria RAM de al menos 2 GB, una unidad quemadora de CD´s, un procesador de 3.2 GHz o más y finalmente, una distribución de Linux que tenga incorporadas las librerías necesarias del sistema de archivos que se va a examinar y la herramienta para la creación de imágenes o clones para realizar la copia maestra y la copia de trabajo del disco comprometido por medio del método de copiado de archivos *bit stream*.

Estas recomendaciones están dadas por el NIST y aunque en el ejemplo de aplicación que se detallará en el capítulo siguiente no se cumple con algunos de los requerimientos como los de memoria RAM o espacio en disco duro por cuestiones económicas, el resultado que se obtiene es sumamente satisfactorio.

Lo que mundialmente se toma como válido son las recomendaciones de organizaciones cono el NIST, el IOCE y las mejores prácticas como las del servicio

secreto de los Estados Unidos. Asimismo, dentro de las metodologías que ofrecen estas organizaciones se pueden tomar como ejemplo, como un punto de partida para desarrollar una capacidad forense, realizar un modelo, de tal manera que concuerde con las leyes y regularizaciones de cada país, en especial de la República Mexicana.

Se debe recordar siempre, que el computo forense es el proceso de utilizar técnicas científicas y analíticas e infraestructura tecnológica, para realizar cuatro pasos que son: *identificar*, *preservar*, *analizar* y *preservar* la evidencia, para que pueda ser admisible en un proceso legal; y además, si se tiene la intensión de ser un experto forense, la regla de oro que jamás se debe olvidar es la siguiente: *en cualquier acción que se realice no debe dañarse la evidencia*.

Referencias

[1] *Computo forense*, disponible en: http://www.e-evidence.info/version2.html
[2] Case E. (2000) *Digital Evidence and Computer Crime*. Estados Unidos: Academic Press
[3] Kruse II G., Warren, Heiser G., Jay (2001*) Computer Forensics: Incident Response Essentials*. Estados Unidos: Addison-Wesley
[4] Carrier, Brian (2005) *File System Forensic Analysis*. Estados Unidos: Addison-Wesley
[5] NIST SP 800-61 *Computer Security Incident Handling Guide*, disponible en: http://csrc.nist.gov/publications/nistpubs/index.html
[6] CERT Coordination Center, CERT/CC Statistics 1988 - 2006. Estados Unidos. Disponible en: http://www.cert.org/stats/cert_stats.html.
[7] NIST SP 800-72 *Guidelines on PDAs Forensics*, disponible en: http://csrc.nist.gov/publications/nistpubs/index.html
[8] Brown C. (2005) *Computer Evidence: Collection & Preservation (Networking Series)*. Estados Unidos: Charles River Media
[9] International Organization on Computer Evidence, IOCE, [en línea]. Disponible en: http://ioce.org/ [2007]
[10] Recovering and Examining Computer Forensiscs Evidence Background. Disponible en: http://www.treas.gov/usss/ectf.shtml
[11] NIST SP 800-86 *Guide to Integrating Forensic Techniques into Incident Response*. Disponible en: http://csrc.nist.gov/publications/nistpubs/index.html
[12] Kevin Mandia, Chris Prosise, *Incident Response: Investigating Computer Crime*, McGrawHill Osborne Media, 2001
[13] Schweitzer, Douglas (2003) *Incident Response: Computer Forensics Toolkit.* Estados Unidos: Wiley
[14]Brian Carrier, "Sleuth Kit Informer". Documentación de software. Disponible en: http://www.sleuthkit.org/
[15] National Institute of Justice, "Test Results for Disk Imaging Tools", Estados Unidos, Ago. 2002, consulta: Feb. 2007. Disponible en: http://www.ncjrs.gov/pdffiles1/nij/196352.pdf
[16] http://www.citefa.gov.ar/soluciones_tecno/si6/SitioSI6_ES/index.htm
[17] National Institute of Standards and Technology, NIST, Disponible en: http://www.nist.gov [2007, febrero]
[18] Police Cyberspace, POLCYB. Disponible en http://www.polcyb.org/index.htm [2007,febrero]
[19] National Institute of Forensic Science, NIFS. Disponible en:http://www.nifs.com.au/home.html
[20] Seguridad y Tecnologías de la Información, Hispasec. Disponible en: http://www.hispasec.com/directorio/hispasec/origenes.html
[21] The Information Warfare Site, IWS. Disponible en: http://www.iwar.org.uk/general/statistics.htm
[22] Information Security and Forensics Society, ISFS. Disponible en :http://www.isfs.org.hk/
[23] Policía Cibernética de la PFP. Disponible en: http://www.ssp.gob.mx/

CAPÍTULO IV

EVALUACIÓN DE LA METODOLOGÍA

RESUMEN. En este capítulo se realiza la evaluación de la metodología que se propuso en el capítulo anterior. Al inicio, se presentan las técnicas de copiado de archivos para realizar las imágenes o clones del disco duro comprometido que utiliza la herramienta forense Autopsy; así como la manera en como se realiza la recolección y examinación de los archivos. Después se analizan los criterios de evaluación que se utilizarán para verificar si la metodología cumple con las recomendaciones de los organismos internacionales relacionados con el manejo de la evidencia digital como el IOCE, el NIST, entre otros. Finalmente se hacen comentarios acerca de los retos y problemas que se tuvieron en la realización de este trabajo.

4.1 MANEJO DE LOS ARCHIVOS

Recolección de los archivos

Durante la recolección de información el analista debe hacer múltiples copias de los archivos o de los sistemas de los archivos relevantes, es decir, una copia maestra y una copia de trabajo.

El propósito de la copia maestra es generar copias de trabajo adicionales, si es que la primera copia de trabajo ya no puede ser utilizada debido a una alteración u otras razones.

El analista puede entonces utilizar una copia de trabajo que no afecte los archivos originales de la copia maestra.

Copiado de archivos de un dispositivo

Los archivos pueden ser copiados de un dispositivo utilizando dos diferentes técnicas, [1]:

- RESPALDO LÓGICO. Un respaldo lógico copia los directorios de un volumen lógico. No captura ninguna otra información que pueda estar presente en el dispositivo, como archivos borrados o información residual almacenada en un espacio poco utilizado.

- CREACIÓN DE IMÁGENES POR *BIT STREAM*. Esta técnica genera bit por bit, creando así una copia del contenido del dispositivo, incluyendo el espacio libre y el espacio poco utilizado. Esta técnica requiere más espacio de almacenaje y toma más tiempo de ejecución que un respaldo lógico.

Si se necesita la evidencia para alguna acusación o acciones disciplinarias, el analista debe de crear una imagen por *bit stream* del dispositivo original, etiquetar el dispositivo original y almacenarlo en un lugar seguro como evidencia.

Todo el análisis subsecuente debe de realizarse con la copia de la información para asegurar que la información original no sea modificada, y si es necesario, se pueda crear una copia del medio original. Se debe documentar todos los pasos que fueron tomados para crear la imagen del disco; el hacerlo así, permitirá a cualquier otro analista producir un duplicado exacto del medio original, siempre y cuando lleve a cabo los mismos procedimientos. Asimismo, se puede utilizar una documentación adecuada para demostrar que la evidencia no fue mal manejada durante el proceso de recolección.

Además de los pasos que se siguieron, para tomar la imagen, el analista debe documentar adicionalmente la información concerniente al modelo de disco duro, número de serie, capacidad del almacenaje (por ejemplo el nombre, número de versión, información de la licencia). Todos estos aspectos apoyan el mantenimiento de la cadena de custodia.

Cuando se crea una imagen bit por bit *(Bit stream)* se puede hacer una copia de *disco a disco* o una copia de *disco a archivo*. Una copia de *disco a disco*, como su nombre sugiere, copia los contenidos de un dispositivo directamente a otro. Una copia de ***disco a disco*** es útil, desde el momento, en que el dispositivo copiado se puede conectar directamente a otra computadora y su contenido es revisado inmediatamente. Asimismo, una copia ***disco a disco*** requiere de un segundo medio de almacenamiento, similar al original. Este segundo dispositivo debe estar completamente limpio antes de que se cree la copia y, además, debe tener una capacidad de almacenamiento mayor a la del dispositivo que se va a copiar, generalmente es el doble.

Una copia *disco a archivo* permite al archivo de información de imagen ser transportado y respaldado fácilmente. De la misma forma para ver el contenido lógico de un archivo de imagen, el analista debe de restaurar la imagen a un medio donde pueda abrirlo y leerlo desde una aplicación que sea capaz de mostrar el contenido lógico de las imágenes de *bit stream*.

Numerosos tipos de hardware y herramientas de software pueden crear imágenes de *bit stream* y respaldos lógicos. Las herramientas de hardware son generalmente portátiles, proveen imágenes bit por bit, se conectan directamente a la interfaz del disco duro de la computadora para ser copiados y tienen incorporadas funciones hash. Las herramientas de hardware pueden obtener información de discos duros que utilizan diferentes tipos de controladores, como IDE o SCSI. Las soluciones de software generalmente constan de un disco de inicio, como un diskette, CD, o programas instalados que corran en una estación de trabajo, a la cual se conecta el dispositivo que se desee copiar. Ejemplos de las herramientas de hardware y software se mencionan en el Apéndice C**.**

Algunas soluciones de software crean copias lógicas de archivos o particiones que pueden ignorar el espacio libre o no asignado en el disco, mientras que otras, crean una copia de imagen bit por bit del dispositivo.

Adicionalmente a su función principal, algunas herramientas de creación de imágenes de disco ejecutan una documentación forense, semejantes a una auditoria automatizada y a una cadena de custodia. La utilización de dichas herramientas puede apoyar consistentemente en el proceso de examinación, exactitud y reproducción de resultados.

Un creciente número de herramientas para la creación de imágenes de disco están disponibles con mayor frecuencia. En respuesta a esta proliferación y a la falta de estándares para probarlas, el proyecto de la Prueba de Herramientas Forenses Informáticas o Computer Forensics Tool Testing (CFTT por sus siglas en inglés) del NIST, ha desarrollado rigurosos procedimientos de prueba para la validación de los resultados de las herramientas. Actualmente sólo unas pocas herramientas han llegado a ser probadas en el CFTT, [2].

Generalmente las herramientas que crean una imagen por medio de *bit stream*, no deben ser utilizadas para obtener copias bit por bit de un elemento físico de un *sistema vivo* (un sistema en uso), porque los archivos y la memoria en ese sistema están cambiando constantemente y por lo tanto, no se puede validar. Por ejemplo, los servicios o procesos que están corriendo en el sistema podrían estar escribiendo en un disco duro de sistema, incluso, si la persona no está utilizando la computadora en ese momento.

De acuerdo a esto, los analistas deben decidir si copiar los archivos de un sistema vivo es factible o no; basándose en los archivos que necesitan ser obtenidos, su precisión, la integridad necesaria que deben tener los archivos al copiarse y la importancia del sistema que está corriendo.

Por ejemplo, no es necesario derribar un servidor crítico utilizado por cientos de personas, sólo para recolectar archivos del directorio de un usuario. Para respaldos lógicos de sistemas “vivos”, o mejor dicho, sistemas en uso, los analistas pueden utilizar software estándar de respaldo de sistema. Del mismo modo la ejecución de un respaldo puede afectar el rendimiento de un sistema y consumir una cantidad significativa de ancho de banda, dependiendo si el respaldo es ejecutado local o remotamente.

Las organizaciones deben tener políticas, directrices y procedimientos que indiquen las circunstancias, bajo las cuales se pueden realizar las técnicas para el copiado de archivos (incluyendo aquellas de sistemas en uso) con propósitos forenses y el personal que puede hacerlo.

Es más efectivo para ellas establecer políticas, directrices y procedimientos basados en categorías de sistemas (niveles de impactos bajos, moderados o intermedios y altos) y la naturaleza del evento de interés; algunas organizaciones deciden además, crear separadamente establecimientos de políticas y normas, particularmente para sistemas importantes. Las directrices y procedimientos deben identificar a los individuos o grupos con autoridad para tomar decisiones, al momento de hacer el respaldo o imagen

de cada tipo de sistema. El acceso a algunos sistemas es restringido, debido a la sensibilidad de las operaciones o a la información en el sistema.

Integridad de los archivos

Durante los respaldos y la creación de imágenes la integridad del medio original se debe mantener. Para asegurar que el respaldo o el proceso de la creación de imagen no alteren la información del dispositivo original, los analistas pueden utilizar un bloqueador de escritura al respaldar la información o al crear una imagen. Un *bloqueador de escritura* es una herramienta de tipo hardware o software, la cual previene a una computadora de escribir sobre el dispositivo al que está conectado.

Los bloqueadores contra escritura en hardware están físicamente conectados a la computadora y al dispositivo de almacenaje para evitar cualquier clase de escritura sobre el dispositivo. Los bloqueadores contra escritura en software son instalados en el sistema forense del analista y actualmente están disponibles solo para MS-DOS y sistemas Windows. Algunos sistemas operativos como por ejemplo, MAC OS X, Linux no requieren de bloqueadores contra escritura en software, porque pueden ser configurados para iniciar con elementos secundarios no montados.

Por otro lado, al conectar un bloqueador de escritura en hardware asegura que se mantenga la integridad. Los bloqueadores basados en MS-DOS trabajan al atrapar la Interrupción 13 y la Interrupción 13 extendida que escribe el disco. Windows trabaja al utilizar filtros para clasificar las interrupciones mandadas a los dispositivos, a fin de prevenir que cualquier clase de escritura se almacene en el dispositivo.

En general, al utilizar un bloqueador contra escritura en hardware se debe conectar entre el dispositivo a ser leído y respaldado y la computadora que lo va a respaldar o a crear la imagen. Para un bloqueador en software, se debe instalar este programa antes de conectar el elemento a ser respaldado o al crear la imagen.

Los bloqueadores deben de ser probados frecuentemente para ver si soportan nuevos elementos dispositivos. Por ejemplo, un nuevo elemento puede hacer uso de funciones reservadas o previamente inutilizadas para implementar funciones específicas que podrían hacer que escribiera en el dispositivo comprometido y alterar su contenido.

Después de hacer un respaldo o crear una imagen, es importante verificar que la copia de la información sea un duplicado exacto de la información original. Al registrar el mensaje clasificado de la información que se copió se puede utilizar para asegurar y verificar la integridad de dicha información.

Un *mensaje clasificado* es una hash que únicamente identifica la información y tiene la propiedad de generar un mensaje codificado al cambiar un solo bit en la información. Hay muchos algoritmos para registrar el mensaje clasificado de información, pero los más utilizados son el MD5 y el SHA-1. Estos algoritmos toman como entrada información de longitud arbitraria y producen una salida de un mensaje clasificado de 128 bits.

Para ambas técnicas de copiado de archivos, los mensajes clasificados creados para asegurar la integridad de la información deben de ser almacenados en modo de *solo lectura* o imprimirlo y después colocarlo en un lugar seguro.

Modificación de los archivos, acceso y tiempos

Cuando se crea un archivo es importante saber cuándo se utilizó o manipuló; la mayoría de los sistemas operativos mantiene un registro de ciertas estampas de tiempo relacionadas con los archivos. Las estampas de tiempo más comunes son las de modificación, acceso, y creación, [3].

- **Tiempo de modificación.** Hace referencia a la última vez que un archivo cambió de alguna forma, incluyendo el momento en que se escribió en él y cuándo fue cambiado por otro programa.

- **Tiempo de acceso.** Indica la última vez que se llevó a cabo cualquier acceso en un archivo, por ejemplo, cuando se abrió, cuando se leyó o cuando se imprimió.

- **Tiempo de creación.** Esta es generalmente la hora y fecha en la que el archivo fue creado; sin embargo, cuando un archivo es copiado a un sistema la hora de creación será en la que el archivo fue copiado al nuevo sistema. La hora de modificación permanecerá intacta.

Diferentes tipos de sistema de archivos pueden almacenar distintos tipos de tiempos. Por ejemplo, los sistemas Windows retienen la última hora de modificación, la última hora de acceso y la hora de creación de los archivos.

Los sistemas Windows utilizando el sistema de archivos NTFS también guardan la entrada de la hora modificada. En los sistemas UNIX se retiene la última modificación, el último cambio de inodo (un inodo es un conjunto de información a las que le pertenecen ciertas características de un archivo como privilegios, propietario, etc.), y la última hora de acceso; asimismo, algunos sistemas UNIX (incluyendo las versiones BSD y SUN) no actualizan la última hora de acceso de los archivos ejecutables, mientras están corriendo. Algunos sistemas UNIX guardan la hora en la que recientemente se altero el *metadat*o de un archivo.

Un *metadato* es la información de la información, tal como se explicó en el capítulo I; para los sistemas de archivos, el *metadato* es la información que provee la información acerca del contenido de un archivo.

Si un analista necesita establecer una línea precisa de tiempo de los eventos, entonces los tiempos de archivo se deben preservar. De acuerdo a esto, los analistas deben estar concientes de que no todos los métodos para la recolección de archivos de información pueden preservar los archivos de tiempo.

Las imágenes creadas por *bit stream* pueden preservar los archivos de tiempo, porque se genera una copia bit por bit. Llevar a cabo un respaldo lógico utilizando algunas herramientas puede causar que se alteren los archivos de creación, mientras se copia el archivo de información. Por esta razón, cuando los archivos de tiempo son

esenciales, la técnica de la creación de imagen por *bit stream* es la adecuada para la recolección de información.

Los analistas deben también de estar conscientes de que los archivos de tiempo no siempre son precisos. Entre las razones de imprecisión se encuentran:

- El reloj de la computadora, al no tener la hora correcta. Por ejemplo, el reloj puede que no este sincronizado regularmente con una fuente de tiempo confiable.

- La hora quizá no pueda ser grabada con el nivel de detalle esperado, tal que se omitan los minutos o los segundos.

- Un atacante pudo haber alterado los archivos de tiempo grabados.

Examinación de los archivos de datos

Después de que se realizó un respaldo lógico o se creó una imagen por *bit stream*, el respaldo o la imagen quizá tenga que ser restaurado a otro dispositivo antes de que se pueda examinar la información. Esto es dependiendo de las herramientas forenses que se utilicen para llevar a cabo el análisis.

Algunas herramientas pueden analizar la información desde la imagen, sin embargo, otras requieren primero que el respaldo o la imagen sean restauradas en un medio. Alguna vez cuando las herramientas tenían capacidades mas limitadas, a menudo se recomendaba que los archivos de información se restauraran a un sistema que utilizara el mismo sistema operativo o uno similar.

Las herramientas actuales son más avanzadas y están diseñadas para trabajar con muchos tipos de archivos de infamación, sin importar el tipo de sistema operativo, así que ya no es necesario -en la mayoría de los casos- restaurar los archivos de información a un sistema operativo en particular.

Sin importar si un archivo imagen o una imagen restaurada es utilizada en la examinación, se debe acceder a la información como *solo lectura* para asegurar que la información que está siendo examinada no es modificada y que proveerá resultados consistentes en lo sucesivo.

Los bloqueadores contra escritura se pueden utilizar en este proceso para prevenir escrituras en la imagen restaurada. Después de restaurar el respaldo (si es necesario), el analista empieza a examinar la información recolectada y realiza una valoración de los archivos relevantes al localizar todos los archivos, incluyendo los archivos borrados, remanentes de archivos en el espacio libre o no asignado del disco y archivos ocultos.

A continuación, el analista necesita extraer la información de alguno o de todos los archivos, lo cual puede ser complicado debido a medidas de seguridad como la encriptación y las contraseñas.

Localización de los archivos

El primer paso en la examinación de los archivos es la localización de estos. Una imagen de disco puede capturar muchos gibabytes de espacio libre y sin utilizar, los cuales pueden contener cientos de archivos y fragmentos de archivos. La extracción manual de información de espacio estéril puede ser un proceso el cuál consume tiempo valioso, además de difícil, ya que requiere del conocimiento esencial del formato del sistema de archivos.

Afortunadamente, varias herramientas son capaces de automatizar el proceso de extracción de información del espacio estéril en el disco y salvarlo en archivos de información, así como recuperar archivos borrados y archivos en la papelería de reciclaje. Los analistas pueden también mostrar el contenido del espacio no utilizado con editores hexa o herramientas especiales de recuperación de archivos poco utilizados.

Extracción de los archivos

El resto del proceso de examinación involucra la extracción de la información de alguno o de todos los archivos. Para tomar conciencia del contenido de un archivo, el analista debe saber que tipo de información contienen los archivos; por ejemplo una extensión *jpg* indica un archivo gráfico, y una extensión *mp3* indica un archivo de música.

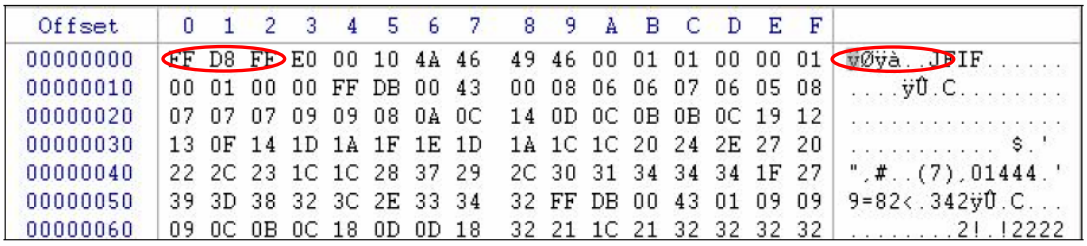
Asimismo los usuarios pueden asignar cualquier extensión de archivo a cualquier archivo, tal como nombrar un archivo de texto *micancion.mp3* u omitir una extensión. En suma algunas extensiones de archivo pueden estar escondidas o no reconocidas en otro sistema operativo. Por lo tanto, los analistas no deben asumir que las extensiones de archivo son precisas.

Los analistas pueden identificar con mayor precisión el tipo de información almacenada en muchos archivos al mirar en los archivos de cabecera. Un *archivo de cabecera* contiene información de identificación acerca de un archivo y posiblemente metadatos que proveen información acerca del contenido del archivo.

Como se muestra en la figura 4.1, el archivo de cabecera contiene una firma de archivo que identifica el tipo de información de manera particular que contiene el archivo. Los archivos de cabecera pueden también indicar si el archivo está encriptado.

Los atacantes pueden alterar las cabeceras de archivo con un editor hexa para esconder el tipo de archivo actual y después alterar de nuevo la cabecera del archivo. En algunos casos, un archivo puede utilizarse aún cuando su cabecera sea alterada. El ejemplo de la figura 4.1 tiene una cabecera de FFD8, lo que indica que es un archivo JPEG. Una cabecera de archivo podría localizarse en un archivo separado del archivo de información actual.

Otra técnica efectiva para identificar el tipo de información en un archivo es un simple histograma que muestre la distribución de los valores ASCII como un porcentaje del total de caracteres en un archivo. Por ejemplo, en la palabra “espacio”, las letras “a” y “e” generalmente indican que es un archivo de texto, mientras que en el histograma se indica un archivo comprimido. Otros patrones son indicativos de archivos que están encriptados o que fueron modificados por esteganografía.



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	00	00	01	ÿØÿà..JFIF.....
00000010	00	01	00	00	FF	DB	00	43	00	08	06	06	07	06	05	08	....ÿÛ.C.....
00000020	07	07	07	09	09	08	0A	0C	14	0D	0C	0B	0B	0C	19	12	.....
00000030	13	0F	14	1D	1A	1F	1E	1D	1A	1C	1C	20	24	2E	27	20	..... $.'
00000040	22	2C	23	1C	1C	28	37	29	2C	30	31	34	34	34	1F	27	",#..(7),01444.'
00000050	39	3D	38	32	3C	2E	33	34	32	FF	DB	00	43	01	09	09	9=82<.342ÿÛ.C...
00000060	09	0C	0B	0C	18	0D	0D	18	32	21	1C	21	32	32	32	32	........2!.!2222

Figura 4.1. Información de cabecera de archivo[1]

La encriptación representa a menudo retos para los analistas. Los usuarios pueden encriptar archivos individuales, carpetas, volúmenes o particiones para que otros no tengan acceso a sus contenidos. Sin embargo, es relativamente fácil identificar un archivo encriptado, pero no es tan fácil desencriptarlo.

El analista puede identificar el método de encriptación al analizar la cabecera del archivo, identificar los programas de encriptación instalados en el sistema o encontrar llaves de encriptación (las cuales están almacenadas en otro dispositivo). Una vez que se conoce el método de encriptación el analista puede determinar mucho mejor la factibilidad de desencriptar el archivo.

En muchos casos, no es posible desencriptar los archivos, porque el método de encriptación es fuerte y la autentificación como una contraseña utilizada para desencriptar no esta disponible.

Sin embargo, un analista puede detectar la presencia de información encriptada, pero el uso de la esteganografía es más difícil de detectar. La *esteganografía* también conocida como *steg*, es el proceso de ocultar la información de otra información. Marcas de agua digitales, el esconder las palabras e información en imágenes, son ejemplos de esteganografía.

Algunas técnicas que un analista puede usar para localizar información oculta incluyen mirar múltiples versiones de la misma imagen, identificar la presencia de imágenes a escala de grises, buscar metadatos y registros, utilizar histogramas y utilizar funciones hash para buscar software conocido de esteganografía, [4].

Una vez seguro de que la información oculta existe, los analistas pueden extraer la información escondida al determinar que tipo de software creó la información y entonces encontrar la llave *steg* o en su defecto utilizar ataques de fuerza bruta para determinar la contraseña.

4.2 CRITERIOS DE EVALUACIÓN

En el capítulo anterior se explicaron las directrices y procedimientos para el manejo de la evidencia, así como la manera de llevar a cabo el proceso forense.

En este capítulo se evalúa la metodología propuesta en el capítulo anterior, basado en las fases del proceso forense: recolección, examinación, análisis y reporte, así como

[1]NIST SP 800-86 *Guide to Integrating Forensic Techniques into Incident Response*, pág. 4-12

también en las recomendaciones proporcionadas por los organismos del manejo de la evidencia digital como la IOCE, el NIST y la Fuerza Aérea de los EUA.

Para esto es necesario fundamentar los criterios de evaluación, los cuales permitirán calificar adecuadamente dicha metodología para lo cual se debe contestar a las siguientes preguntas:

- ¿La metodología propuesta consigue recuperar la información perdida de un disco duro?
- ¿La metodología propuesta cumple con los requerimientos de las instituciones internacionales como el NIST, IOCE entre otras?
- ¿La metodología propuesta es lo suficientemente clara y entendible para cualquier usuario de cómputo?
- ¿La metodología propuesta puede ser reproducida en cualquier lugar por cualquier usuario si se siguen fielmente cada uno de los pasos que la constituyen?
- ¿Son los pasos de la metodología propuesta suficientes para la recuperación de la información perdida?

Para averiguar si la metodología propuesta contesta afirmativamente a los criterios que han sido planteados, a continuación se expone un ejemplo de aplicación que permite poner a prueba la metodología propuesta en el capítulo III.

4.3 EJEMPLO DE APLICACIÓN

Detección del incidente

A continuación se describe la situación, en la cual operaba el sistema, cuya imagen o clon se analizará por medio de la herramienta forense Autopsy-2.08.

El *Usuario A* de una pequeña empresa a notado, que un archivo con información sumamente importante para él, ha sido eliminado, por lo que sospecha de algún ingreso no autorizado. Según el *Usuario A*, estaba trabajando en su sistema, capturando algunos datos. Por alguna circunstancia dejó momentáneamente su lugar de trabajo y cuando regreso notó que el archivo que había generado estaba borrado.

Sin embargo, también mencionó que no había respaldado su información y, que al dejar su estación de trabajo no bloqueó su sistema o colocó alguna contraseña de acceso, es decir, no se preocupó por tomar alguna medida de seguridad.

Instalación del laboratorio

Para elaborar el análisis se preparó un laboratorio, mismo que a continuación se describe:

- Workstation Compaq 6130LA.
- Disco Duro Maestro de 80 GB.
- Memoria RAM de 512 MB.

- Procesador Pentium 4 de 2.0 GHz.
- Tarjeta de gráficos ATI Radeon 7000 de 64 MB.
- Sistema Operativo Fedora 6.

Las características del disco duro comprometido son:

- Disco Duro IDE *ST32122A de Seagate*.
- 4092 Cilindros.
- Cabezas.
- 63 Sectores.
- Capacidad 2 GB.

Una vez instalado el sistema operativo Fedora se instalaron:

- Sleuthkit-2.06, el cual fue descargado de la página http://www.sleuthkit.org. Este paquete contiene una serie de herramientas *open source* que permite recolectar información de imágenes o clones creados con la herramienta *dd Linux*.

- Autopsy-2.08, el cual puede ser descargado de la página http://sleuthkit.orr/autopsy. Es un paquete que contiene una interfaz gráfica para el uso de las herramientas de Sleuthkit y además permite gestionar el caso.

Respuesta Inicial, Preparación al Incidente y Aseguramiento de la Evidencia

Lo primero que se debe hacer llevar el equipo que ha sido comprometido a un laboratorio donde se removerá el disco duro, se protegerá contra cargas electrostáticas y se hará una cadena de custodia para tener un control de quienes tengan acceso a la información.

Aplicación de la Herramienta Forense en Software Libre

La estación de trabajo que servirá como laboratorio de pruebas debe estar apagada para poder colocar el disco comprometido que ha sido previamente removido. A continuación, se coloca el disco comprometido como esclavo (*slave)*, ya que el disco duro que va a analizar al disco comprometido esta configurado como maestro (*master*).

Una vez instalado, se configura el BIOS del sistema, de tal manera que, al iniciar el sistema operativo del disco maestro, sea capaz de reconocer el nuevo elemento de hardware, es decir, el disco comprometido. En el caso del BIOS de esta estación de trabajo, éste autodetectó inmediatamente el nuevo hardware tal como lo muestra la figura 4.2.

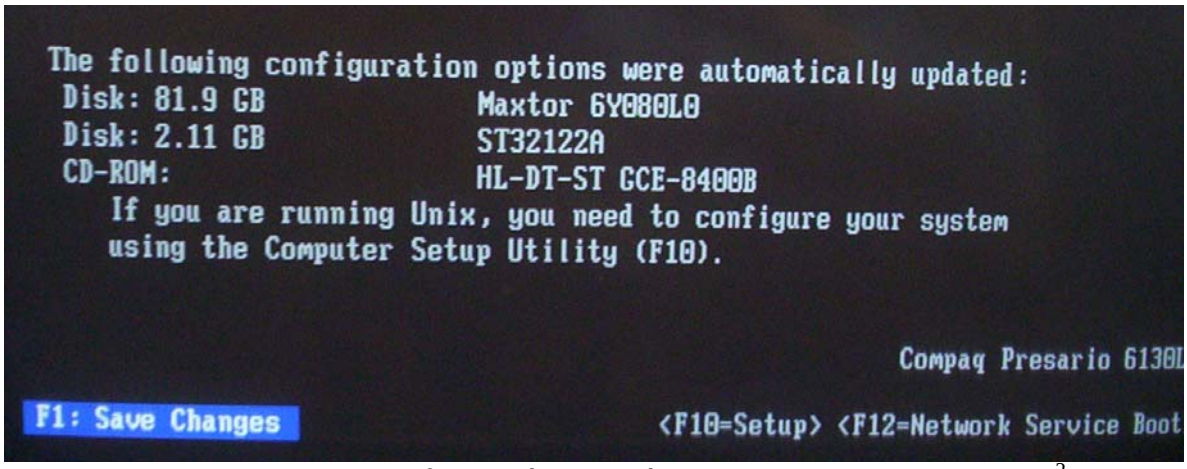


Figura 4.2. Pantalla de configuración automática del Laboratorio de Pruebas[2]

A continuación, se ingresa al sistema como *root* y se abre una terminal. Entonces se escribe el comando *fdisk –l* para observar las diferentes particiones de los discos instalados, como se observa a en la figura 4.3

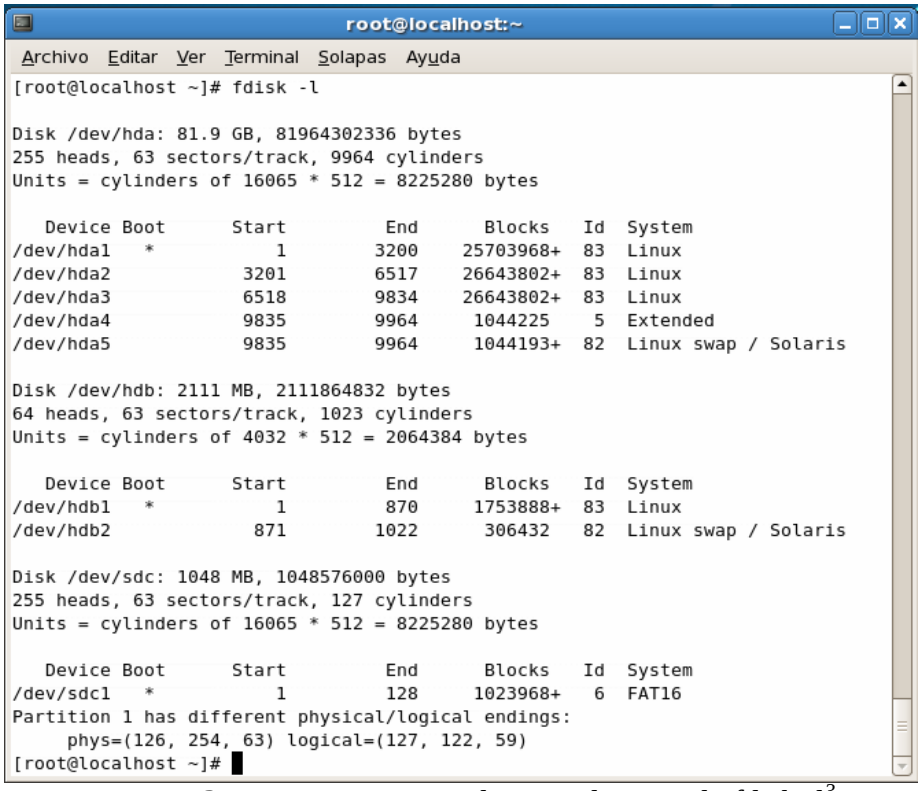


Figura 4.3. Particiones mostradas con el comando fdisk -l[3]

Ahora que se sabe que el sistema ha reconocido el disco duro comprometido, antes de montarlo en forma de solo lectura, es necesario crear un punto de montaje con el comando *mkdir* de la siguiente forma:

[root@localhost ~]# cd /mnt

[2] Fuente. Elaboración propia
[3] Fuente. Elaboración propia

[root@localhost mnt]# mkdir redhat

Ya que se tiene el punto de montaje, se procede a montar el elemento */dev/hdb1* mediante el comando *mount*.

[root@localhost mnt]# mount –t ext3 –o ro /dev/hdb1 /mnt/redhat

Cabe señalar que el comando *mount* tiene diversas opciones, pero en este caso lo único que se expreso fue el tipo de sistema de archivos con la opción *–t* y con la opción *–o ro* se especificó, que el elemento se montara como solo lectura.

Para asegurarse de que el elemento se montó correctamente, se escribe nuevamente el comando *mount* sin ninguna opción.

En este paso no ha surgido ninguna clase de contratiempos, ni sorpresas desagradables, por lo que la siguiente fase es crear un directorio, en donde se va a guardar la imagen o clon del disco comprometido.

Ahora que se tiene montado el dispositivo, se recomienda crear una carpeta, en la cual se va a colocar la imagen del disco comprometido con el comando *mkdir*.

[root@localhost mnt]# cd /usr/local

[root@localhost local]#mkdir images

[root@localhost images]#

Ya que se creo la carpeta, se debe realizar la imagen. A continuación se explicará el proceso de la realización de una imagen.

Para crear la imagen del disco comprometido se utilizara la herramienta *dd Linux*, la cual como se explicó en el capítulo III, convierte y da formato a una imagen, utilizando la técnica de copiado por *bit stream*. Esta técnica, así como la técnica de respaldo lógico son dos diferentes técnicas para el copiado de archivos de un dispositivo.

Ya que se encuentra en la carpeta recién creada la expresión para crear la imagen del disco comprometido es la siguiente:

[root@localhost images]#dd if=/dev/hdb1 of=./HDB1.dd

En donde la opción *if* indica la partición que ha de ser "clonada" y la opción *of* indica el lugar donde se debe de guardar el clon. HDB1.dd es el nombre que recibe la imagen.

El tiempo estimado para la realización del clon para un disco duro de 2 GB fue de aproximadamente cinco minutos.

Uno de las cosas más importantes del proceso de recolección es justamente la obtención de la imagen, por lo que una vez que ha sido obtenida, se opta por desmontar el elemento */dev/hdb1*, pues el objeto de estudio en cuestión es la imagen. Para desmontar el elemento se utiliza el comando *umount.*

[root@localhost images]#umount /dev/hdb1

El siguiente paso consiste en montar la imagen recién creada, protegiendo la integridad de la información por medio de las opciones *noatime, noexec* y *nodev* del comando *mount.*

Donde:

- **Noatime**. Una vez que se termina de crear la imagen, se procede a desmontar el disco comprometido.

- **Noexec.** Permite montar el sistema, sin embargo, no permite la ejecución de algún programa o binario ubicado en el sistema de archivo montado.

- **Nodev.** Si se monta una imagen de un sistema de archivos Linux, que alguna vez estuvo instalado en un disco duro, es recomendable montarlo con esta opción, ya que al no ser montado como sistema de arranque principal, no es necesario interpretar los dispositivos de bloque o carácter que estaban conectados al sistema y que de hecho, no lo estarán por ser una imagen del sistema.

[root@localhost images]#mount –t ext3 –o ro,noatime,noexec,nodev,loop /usr/local/images/HDB1.dd /mnt/redhat

Una imagen o clon, es por definición, un archivo regular que almacena el contenido exacto del disco duro a examinar.

Al realizar una imagen, se debe cumplir con el principio de no trabajar directamente con la evidencia original. Sin embargo, sería complicado revisar los archivos lógicos que se encontraban almacenados en el disco duro original con tan solo este nuevo archivo. Por lo tanto, este archivo regular debe ser transformado en un archivo de dispositivo especial para simular un disco duro.

Después, el investigador puede analizar el sistema de archivos, tal como si trabajara con el disco duro original, por lo que para trabajar con esas imágenes es necesario agregar a la instrucción *mount* la opción *loop.*

Es necesario comprobar la integridad de la imagen por medio de un mecanismo que ayude a determinar, que la evidencia no ha sido alterada o dañada. Esto se hace utilizando el comando *md5sum* de la siguiente manera:

[root@localhost images]#md5sum HDB1 >> VFC.txt

Lo que se hace es hacer un identificador hash para la imagen y al mismo tiempo el identificador se guarda en un archivo de texto llamado VFC.txt. A continuación, se debe averiguar el tipo de sistema operativo instalado en la máquina vulnerada. Aunque el *Usuario A* dijo que el sistema que estaba utilizando era RedHat, es necesario verificarlo; esto se hace por medio del comando *file*.

[root@localhost images]#file HDB1.dd

Se comprueba que el tipo de sistema de archivos que se tiene es un *ext3*, lo que asegura que se trata de un sistema operativo Linux. A continuación se verifica su versión, partiendo de la suposición, de que efectivamente se trata de un RedHat, se comprueba por medio del comando *cat.*

[root@localhost images]#cat /mnt/redhat/etc/redhat-release

Y el resultado muestra que es una versión 9. Por último, se verifica el nombre de host con el mismo comando *cat* de la siguiente forma:

[root@localhost images]# cat /mnt/redhat/etc/sysconfig/network

Y ahora se sabe que el nombre de host del equipo comprometido es *localhost.localdomain*. Estos últimos tres datos obtenidos son importantes, ya que se requieren para crear el *host* de la pantalla *ADD A NEW HOST* del Autopsy.

Búsqueda de la información

A continuación se explicará como por medio de la herramienta Autopsy de código libre, es posible recuperar información "borrada". Una vez que se tiene la herramienta Autopsy instalada y configurada, además de entrar como *root* al sistema, se abre una terminal y se escribe el nombre de la herramienta, de la siguiente manera:

[root@localhost ~]#autopsy

Como resultado el sistema arroja una pantalla como la de la figura 4.4. Y sin cerrar la terminal, se da un clic sobre el URL http://localhost:9999/autopsy para tener acceso a la interfaz gráfica por medio del navegador, como lo muestra la figura 4.5.

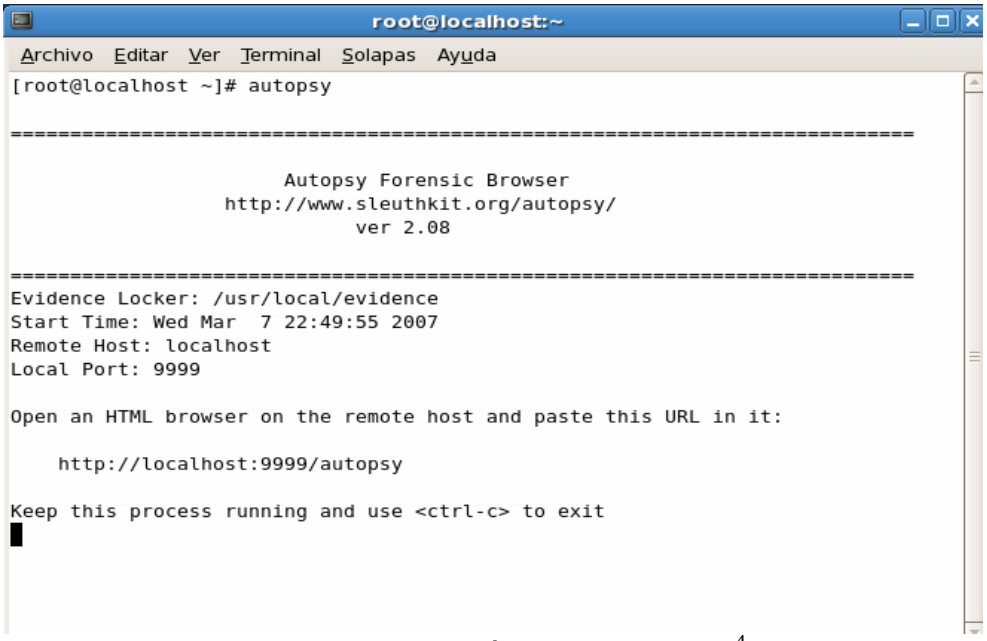


Figura 4.4. Ejecución de Autopsy 2.08[4]

[4] Fuente. Elaboración propia

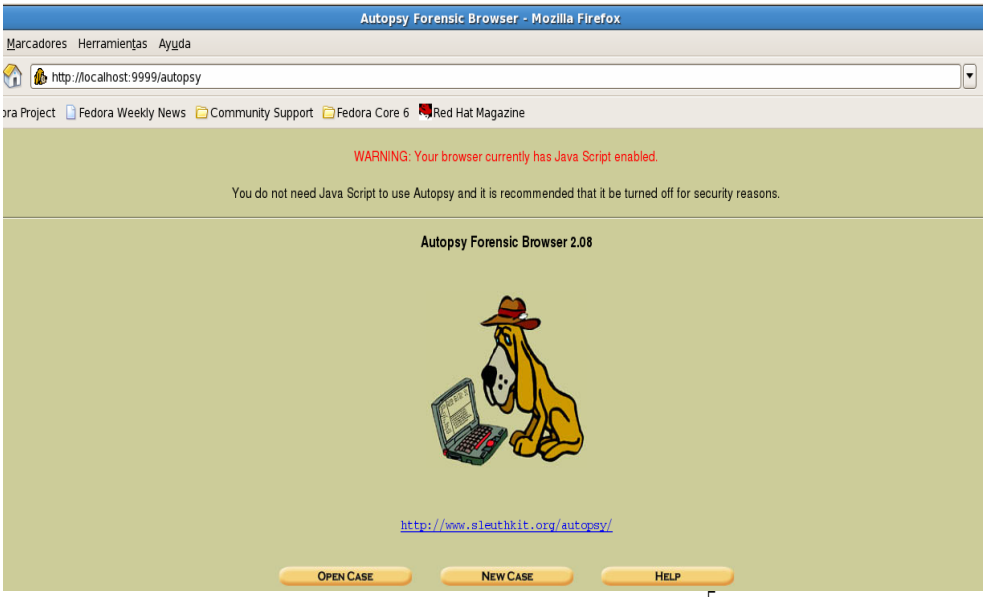


Figura 4.5. Visor de Autopsy 2.08[5]

Como se mencionó en el capítulo III, Sleuthkit y Autopsy manejan imágenes para analizarlas y posteriormente recuperar, si es posible, la información perdida. Trabajan dividiendo cada investigación en casos. Cada caso puede contener uno o más *hosts* y cada uno de ellos puede a su vez contener una o varias imágenes del sistema de archivos, y por otra parte, cada caso puede tener asignados uno o más investigadores. Como ya se posee la imagen del disco comprometido llamada *HDB1.dd*, se debe empezar el análisis creando el primer caso, pulsando sobre *New* Case y se llenan los espacios correspondientes, como se muestra en la figura 4.6.

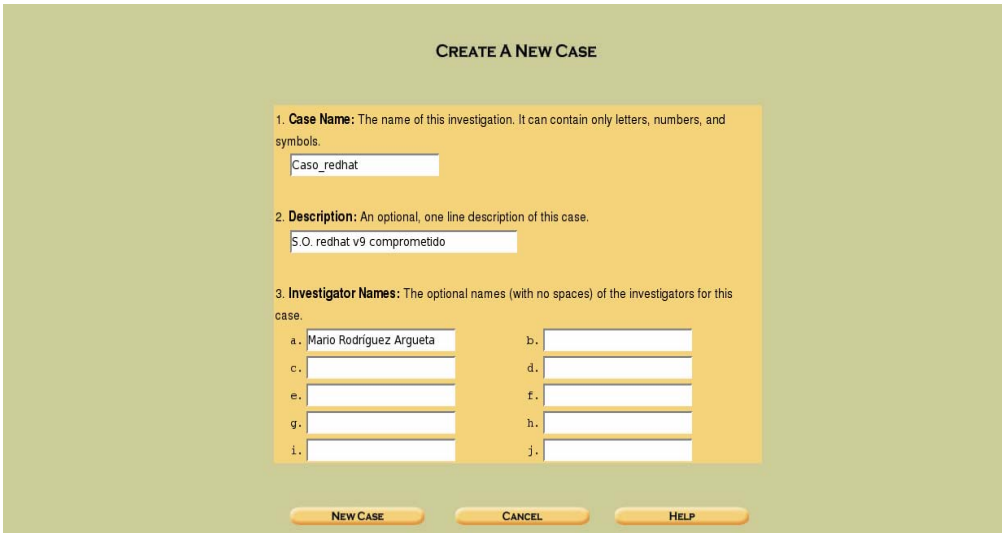


Figura 4.6. Creación de un nuevo caso[6]

Ya que se introdujo el nombre del caso y el nombre del investigador, se pulsa sobre *New Case*. En seguida se debe agregar al menos un host al caso (vea figura 4.7).

[5] Fuente. Elaboración propia
[6] Fuente. Elaboración propia

Para completar los campos requeridos se puede hacer uso de comando *file*, para averiguar el tipo de sistema de archivo que tiene la partición. Como previamente se habían obtenido estos datos, sólo se llenan los espacios.

Es importante señalar que, cuando se crea un *host*, se puede especificar la *zona horaria* o *time zone*. Si se desconoce la zona horaria, por default, se utilizará la zona horaria del sistema que analice el disco comprometido.

Si el sistema que está siendo investigado viniera de una zona horaria diferente, entonces se necesitaría saber el nombre de dicha zona. Autopsy cuenta con una lista de zonas horarias, las cuales son conocidas por la mayoría de los sistemas, [5].

Figura 4.7. Adición de un nuevo host[7]

Si se pulsa nuevamente sobre *Add Host* se agregará una entrada para la máquina en el primer caso. Entonces se incluye la imagen del sistema de archivos utilizado por el sistema comprometido. Para ello se pulsa sobre *Add Image* y en la siguiente pantalla sobre *Add Image File* (vea figura 4.8).

[7] Fuente. Elaboración propia

Figura 4.8. Localización, Selección y Copiado de la imagen[8]

En la opción *Location* se escribe la ruta completa de la imagen que se va a analizar. En el campo *Type* se selecciona la opción *Partition,* ya que se trabajará solamente con la partición root (/).

Por último, como se mencionó anteriormente, es necesario crear una copia maestra del disco comprometido y una copia de trabajo. Es por esta razón que se escoge la opción *Copy*. En seguida se pulsa sobre *Next*, donde para mantener la integridad de la imagen se puede calcular o agregar un identificador.

Previamente se obtuvo el identificador de la imagen, por lo que, se coloca en el campo *Add the following MD5 hash value for this image*, se selecciona la casilla de verificación para verificar el identificador después de que se haya importado la imagen.

Entonces se escoge el punto de montaje y el tipo de sistema de archivos y a continuación se pulsa sobre *Add* (vea figura 4.9).

[8] Fuente. Elaboración propia

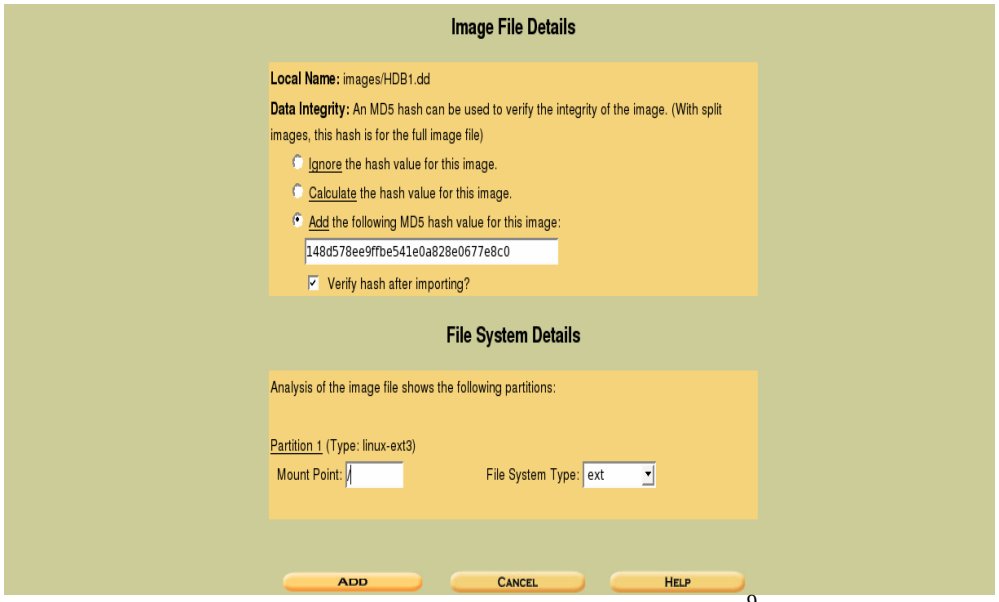


Figura 4.9. Detalles del archivo imagen[9]

A continuación, la figura 4.10 muestra una ventana de Autopsy donde se incluye la imagen del disco comprometido.

Figura 4.10. Tabla de entradas de imágenes[10]

Localización y Recuperación de la Información

Es en esta ventana donde se pulsa la opción *Analyze*, donde se abre una nueva ventana con opciones diferentes. En este caso, se busca el archivo borrado por el nombre del archivo en la opción *Keyword Search*, donde en el campo correspondiente se escribe el nombre del archivo eliminado (vea figura 4.11).

[9] Fuente. Elaboración propia.
[10] Fuente. Elaboración propia.

Figura 4.11. Opción de búsqueda Keyword Search[11]

Después de terminar la búsqueda y mostrar los resultados en pantalla, se procedió a analizar cada uno de los resultados, hasta que finalmente se encontraron cuatro archivos en la última parte de la búsqueda, donde uno de ellos era el archivo eliminado con número de inodo 546 y con su respectiva estructura de bloques, como se observa en la figura 4.12.

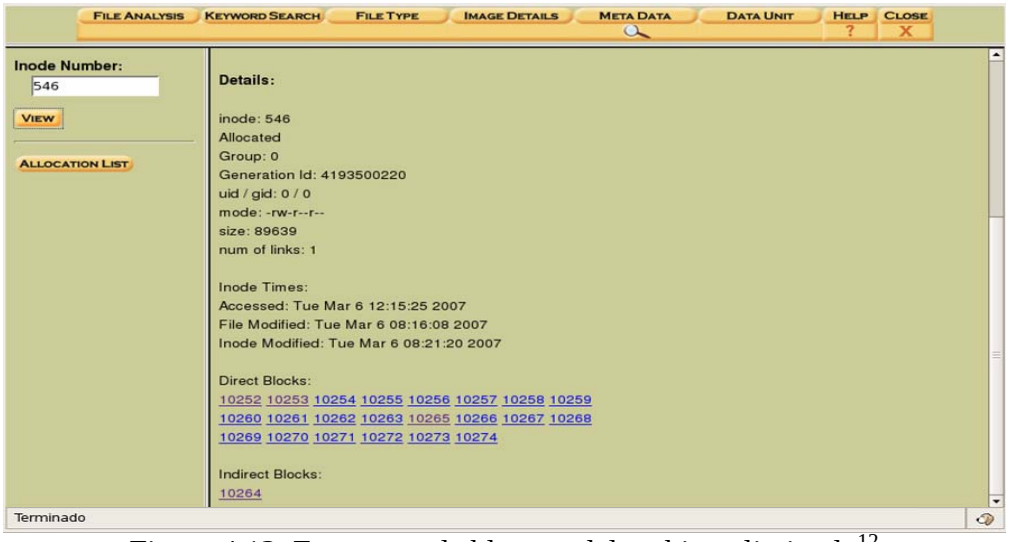


Figura 4.12. Estructura de bloques del archivo eliminado[12]

Finalmente se observa el contenido del archivo y efectivamente es el archivo eliminado.

A continuación se exporta dicho archivo y con esto se ha recuperado la información borrada (ver figura 4.13)

[11] Fuente. Elaboración propia
[12] Fuente. Elaboración propia

Figura 4.13. Vista del archivo recuperado[13]

Elaboración de Reporte

Es necesario elaborar un reporte para documentar todo lo sucedido con la recuperación de la información, y en caso de que la recuperación no haya sido exitosa, explicar las causas.

Recomendaciones de Seguridad

Finalmente es necesario establecer políticas de seguridad en los lugares de trabajo, para mantener seguros la información que caca uno de los usuarios considere importante, como por ejemplo la creación de respaldos en CD´s, colocar contraseñas a sus respectivos equipos, no compartir contraseñas, etc.

4.4 EVALUACIÓN DE LA APLICACIÓN

Se comprobó que la metodología propuesta consigue recuperar la información perdida de un disco duro. Es preciso mencionar que aunque existen otros tipos de incidentes como una negación del servicio (DOS), código malicioso, acceso no autorizado, como fue el caso del ejemplo del apartado anterior, es posible recuperar la información eliminada, si bien, no en su totalidad, si parcialmente, claro está manteniendo la integridad de la evidencia para que pueda servir como prueba en un proceso legal.

[13] Fuente. Elaboración propia

Además, también se comprobó que la metodología propuesta cumple con los requerimientos de las instituciones internacionales como el NIST, debido a que en los diez pasos de esta metodología se mantienen los pasos principales del proceso forense, lo cual es de gran importancia, ya que toda la evidencia que logra ser recolectada y ser considerada como autentica, permite identificar a delincuentes que cometen ilícitos contra personas, especialmente con menores de edad.

La metodología pretende ser clara y entendible para cualquier usuario de computo, no obstante, es necesario tener un conocimiento de los sistemas operativos opensource o de código libre para poder instalarlo, ya sea en una estación de trabajo o como una máquina virtual, por lo que sólo los usuarios que sepan instalar un sistema operativo como Linux podrán comprender con mayor facilidad esta metodología.

Otro criterio que se evalúa en esta metodología es que si se siguen fielmente cada uno de los pasos que la constituyen, puede ser reproducida en cualquier lugar, por cualquier usuario, sin embargo, como se explicó en el punto anterior, sería de más ayuda para el usuario, si éste estuviera familiarizado con los sistemas operativos y por lo tanto, con los sistemas de archivos que se pretenden analizar.

Finalmente, se considera que los pasos de la metodología propuesta son suficientes para la recuperación de la información perdida, ya que en primer lugar, cumplen con el modelo de proceso forense, en segundo lugar, cumplen con las recomendaciones de instituciones internacionales como el NIST y por último, se asegura que se cumple el objetivo para lo cual esta metodología fue diseñada, es decir, sirve como referencia para especialistas en seguridad informática para la recuperación de información en discos duros.

4.5 RECOMENDACIONES

El primer grupo de recomendaciones aplica a la capacidad forense de una organización. El resto de las recomendaciones se agrupó de acuerdo a las fases del proceso forense: recolección, examinación, análisis y reporte.

Capacidades forenses en una organización

- **Las organizaciones deben ser capaces de llevar a cabo un proceso forense.** La informática forense se necesita para varias tareas en una organización, incluyendo la investigación de crímenes y de comportamiento inapropiado, reconstrucción de incidentes de seguridad, recuperación después de un daño accidental al sistema, etc. Sin esta capacidad, una organización tendrá dificultades para determinar que eventos ocurrieron en sus sistemas y redes.

Participantes forenses

- **Las organizaciones deben de manejar las partes correspondientes a cada aspecto forense.** La mayoría de las organizaciones combinan esfuerzos tanto de

su personal como de partes externas, basándose en las habilidades y experiencia del personal.

- **Los analistas deben tener un conocimiento técnico.** Debido a que las herramientas tienen limitantes en el análisis es importante que los analistas tengan un conocimiento sobre los principios de sistemas, principios de redes, aplicación de protocolos, etc.

- **Los equipos del manejo de los incidentes deben ser eficientes en la informática forense.** Más de un miembro del equipo debe ser capaz de llevar a cabo labores forenses. Al tener cursos de capacitación y ejercicios que ayuden a aumentar las habilidades.

Directrices, políticas y procedimientos forenses

- **Se deben hacer consideraciones forenses claras en las políticas de la organización.** En un nivel mayor, las políticas permiten al personal autorizado monitorear los sistemas y redes y llevar a cabo investigaciones por razones legítimas bajo circunstancias apropiadas. Las organizaciones pueden tener una política forense separada para personal de incidentes y otros con roles forenses que proveen más reglas detalladas para un comportamiento apropiado. Cada uno de quienes sean llamados para asistir a una organización debe estar familiarizado con la política forense.

- **Las organizaciones deben mantener directrices y procedimientos para ejecutar tareas forenses.** Las directrices deben incluir metodologías generales para la investigación de un incidente utilizando técnicas forenses, procedimientos del tipo paso por paso para poder ejecutar las tareas de rutina.

Preparación técnica

- **Los analistas deben tener un set de herramientas forenses para la recolección, examinación y análisis de los datos**. Debe proveerse de herramientas para recolectar y examinar la información volátil y no volátil y ejecutar revisiones rápidas de los datos también como un análisis profundo. El set de herramientas debe ser rápido y eficiente como una estación forense.

Ejecución del proceso forense

- **Las organizaciones deben llevar a cabo un proceso forense consistente.** En la metodología propuesta se presenta un proceso forense de cuatro fases, los cuales son la recolección, examinación, análisis y reporte. Los detalles exactos de cada fase pueden variar debido a las necesidades que se tengan.

Recolección de información

- **Los analistas deben de estar consientes del rango de fuentes posibles de información**. Los analistas deben de ser capaces de inspeccionar un área física y reconocer las posibles fuentes de información.

- **Los analistas deben de ejecutar la recolección de información utilizando un proceso estándar**. Los pasos recomendados en este proceso son identificar las fuentes de información, desarrollar un plan de adquisición de información, adquirir la información y verificar su integridad.

- **Los analistas deben de utilizar un set de herramientas forense para recuperar datos volátiles del sistema operativo.** El uso de un set de herramientas forense permite la precisión de la recolección de información volátil del sistema operativo minimizando los cambios al sistema. El analista debe conocer cada herramienta de manera que sepa como afecta al proceso de recolección de información.

- **Los analistas deben preservar y verificar la integridad de los archivos.** Al utilizar un bloqueador de escritura durante los respaldos y la creación de imágenes, previene a una computadora escribir sobre el dispositivo que se está examinando. La integridad de los datos copiados se debe verificar a comparar los mensajes clasificados de los archivos. Se debe acceder a los archivos y las imágenes en modo de solo lectura.

Examinación y análisis

- **Los analistas deben utilizar una aproximación metódica para estudiar los datos.** La base de la informática forense es utilizar una aproximación metódica al analizar la información disponible para que de esta manera se puedan obtener conclusiones basadas en la disponibilidad de la evidencia.

- **Los analistas deben analizar las copias de los archivos, no los originales.** Durante la fase de recolección se deben hacer múltiples copias de los archivos o sistemas de archivos deseados, usualmente una copia maestra y una copia de trabajo. De esta manera el analista puede trabajar con la copia de trabajo sin afectar la evidencia original o la copia maestra.

- **Los analistas deben confiar en las cabeceras de archivos y no en las extensiones para identificar el contenido y tipo de los archivos.** Debido a que los usuarios pueden asignar cualquier extensión a cualquier archivo, los analistas no deben asumir que las extensiones de archivo son precisas, por lo que deben identificar el tipo de datos almacenados en muchos archivos al examinar sus cabeceras.

Reporte

- **Los analistas deben revisar sus procesos y prácticas.** Las revisiones recientes de las acciones forenses pueden ayudar a identificar errores de procedimientos y otras cuestiones que necesiten ser remediadas, al mismo tiempo se mantiene a la organización constantemente actualizada, en lo que se refiere a cambios en la tecnología y cambios en la ley.

4.6 COMENTARIOS

Uno de los principales retos para llevar a cabo este trabajo fue el de encontrar información que especificara cual era la distribución de Linux más recomendable para analizar un sistema de archivos del tipo NTFS, por lo que después de un extenso periodo de búsqueda, opté por simular un ataque a un sistema, que tuviera un sistema de archivos del tipo ext3 en un sistema operativo Red Hat versión 9, debido a que no sabía como manipular en Linux un sistema de archivos de Windows. Durante el desarrollo de este trabajo, encontré nueva información sobre una convocatoria lanzada por el equipo de respuesta a incidentes de la UNAM (UNAM - CERT), la cual invitaba a los especialistas en seguridad informática a resolver y deducir como se había llevado a cabo un ataque a un servidor Windows 2003. Esto me proporcionó nuevos conocimientos acerca de herramientas, tipos de ataque, escaneos de vulnerabilidades y conceptos como "ingeniería social", el cual establece que personas, cuyo fin es obtener información personal de otras, usurpan personalidades, y aprovechándose de la buena voluntad y confianza de otras personas, realizan fraudes u otros delitos.

Todo esto me ayudo para proponer el escenario anteriormente explicado en el apartado 4.3. Escogí el sistema operativo Fedora 6 por ser un sistema operativo con una interfaz gráfica de fácil y rápido entendimiento y porque la herramienta de análisis Autopsy, la instalé sin problema alguno. Había utilizado una versión llamada SUSE 10.0, pero esta versión no venia con las dependencias necesarias para que la herramienta funcionara como debía de hacerlo. Además tomé en cuenta que el sistema de archivos del disco comprometido fuera ext3, para que el escenario estuviera homogeneizado y para aprender a instalar un sistema operativo como Red Hat. El conocimiento que adquirí en el capítulo I y II fue de gran ayuda, ya que SUSE, Fedora y Red Hat requieren que se les asigne una partición, donde el tamaño depende del número de cilindros que uno quiera que la partición tenga y por supuesto, dependiendo del tamaño del disco.

Finalmente, después eliminé un archivo y posteriormente lo recuperé utilizando la metodología propuesta, puedo decir que el objetivo de la tesis se cumplió, debido a que esta metodología funciona para recuperar los datos borrados y cumple con las recomendaciones de organismos internacionales como el IOCE, el NIST, entre otros.

Referencias

[1] NIST SP 800-86 *Guide to Integrating Forensic Techniques into Incident Response*, disponible en: http://csrc.nist.gov/publications/nistpubs/index.html
[2] CCFT Computer Forensics Tool Testing http://www.cftt.nist.gov/disk_imaging.htm.
[3] Schweitzer, Douglas (2003) *Incident Response: Computer Forensics Toolkit.* Estados Unidos: Wiley
[4] Carrier, Brian (2005) *File System Forensic Analysis*. Estados Unidos: Addison-Wesley
[5] Brian Carrier, "Sleuth Kit Informer". Documentación de software. Disponible en: http://www.sleuthkit.org/

CONCLUSIONES

Las computadoras son en la actualidad un reflejo de la vida de una persona. Pueden contener cartas para personas especiales, estados de cuenta, canciones, que permiten recordar momentos importantes o fotografías con un gran valor sentimental.

¿Qué pasa entonces, cuando por alguna circunstancia se pierden estos datos? Tal vez las preguntas que formularía cualquier persona serian las siguientes:

- ¿Puedo recuperar mi información?
- ¿Cómo puedo recuperar mi información?
- ¿Se eliminó definitivamente?
- ¿Puedo recuperarla en su totalidad?
- ¿Quién la borró?

Para contestar estas preguntas es necesario saber cómo funcionan los dispositivos que guardan nuestra información, conocer como la organizan y cómo se muestra ante el usuario.

Además, se sabe que existen varias clases de ataques informáticos que pueden ocurrir tanto dentro, como fuera de los hogares, instituciones de educación, organizaciones privadas, etc., en donde dichos ataques se pueden tipificar según las leyes, como abuso de confianza, espionaje industrial, venganza de usuarios que hayan sido despedidos, etc.

Es por eso, que la intención de esta investigación es ofrecer una metodología dirigida principalmente a los ingenieros en comunicaciones y electrónica, para que sean capaces de rescatar la información de un dispositivo de almacenamiento, y en caso de que no sea posible rescatarla, explicar con bases sólidas, el porqué no se logró el objetivo; cumpliendo con las recomendaciones de los organismos internacionales relacionados con el tratamiento de evidencia digital.

Cabe destacar que el objetivo planteado se cumplió de acuerdo con los criterios de evaluación establecidos basados en las recomendaciones de los organismos internacionales relacionados con el manejo de la evidencia digital como el IOCE, el NIST entre otros; dichos criterios se utilizaron para verificar la efectividad de dicha metodología y se demostró que es posible recuperar la información que ha sido eliminada de un dispositivo de almacenamiento masivo a través de herramientas que funcionan en software libre como Linux.

Además, es importante que los ingenieros en comunicaciones y electrónica entiendan, que utilizar un sistema como Linux ofrece muchas ventajas, por ejemplo, en el aspecto económico, Linux se puede instalar en un gran número de equipos sin tener que pagar un solo peso por la licencia, hace los equipos más seguros al utilizar más de un tipo de

partición para almacenar los archivos y finalmente, desde el punto de vista de la examinación forense, Linux permite al investigador crear una imagen idéntica del sistema de archivos para poder analizarla como si se tratara del dispositivo original; de esta manera, se cumple con una de las recomendaciones de un organismo internacional dedicado al manejo de la evidencia forense digital, es decir el NIST.

Traté de que mi metodología tuviera diez puntos, considerando que cada uno de los conceptos que la constituyen, explicaran claramente su objetivo y que estuvieran acorde con el proceso forense.

La instalación de la herramienta Autopsy 2.08 no debe de causar problemas al momento de ser instalada en una distribución de Linux como Fedora 6; si los hubiera, hay que poner atención a los errores de salida que muestra la herramienta después de la compilación que hace, ya que por ejemplo, si se utiliza una distribución de Linux que viene incluida en una revista de computación, esta versión no viene completa, por lo que se tiene que instalar adicionalmente las dependencias faltantes.

Inicialmente se utilizó SUSE 10, pero esta versión de revista no incluía *perl y openssl*, además de verificar que estuviera presente el compilador *gcc*. Por lo que después de varios intentos para hacer instalar y correr la herramienta forense en SUSE, se decidió cambiar a la distribución de Fedora 6. Con esta versión no se tuvo ningún problema; una vez que la herramienta se instala y se empieza a adjuntar la imagen del disco comprometido para su análisis, lo demás es más sencillo, pues sólo se completan los campos con la información necesaria.

Es importante saber cómo se guarda la información, es decir, entender lo que es un nombre de archivo y cómo se relacionan los inodos y los metadatos. Al crearse un archivo, se crea también un número o identificador llamado inodo. También se crea una estructura de información por bloques llamada metadatos. Al “borrarse” un archivo, realmente sólo se borra el enlace que hay entre el nombre del archivo y el contenido del mismo, pero la información perdura. Lo que se hace realmente es cambiar un carácter y esto lo interpreta la computadora como que en este lugar se puede sobrescribir.

El tiempo, tanto para la creación de la imagen, como para la búsqueda de un archivo en particular, es muy variable. Por ejemplo, para la creación de la imagen de este disco duro de 2 GB se necesitaron entre 5 a 6 minutos. No se decir con certeza, cuanto tiempo se necesita para hacer la copia de un archivo, por ejemplo, de uno de 40 GB; ya que no se tuvo la oportunidad de contar con un elemento así. Lo que si puedo decir es que entre más grande sea la capacidad de almacenamiento de un disco duro, más tiempo se necesita para crear su imagen.

Durante el desarrollo aprendí mucho acerca de los discos duros, por ejemplo, que son elementos que guardan grandes volúmenes de información, a través de las leyes del electromagnetismo, y que este es el principio de su funcionamiento. También aprendí que, con el paso del tiempo, estos dispositivos tienden a hacerse más pequeños, lo que permite crear equipos móviles más compactos y con más capacidad de almacenamiento.

La herramienta Autopsy puede hacer el análisis de discos con interfaz IDE o SCSI, solamente hay que especificárselo al momento de crear la imagen de disco.

Autopsy puede recuperar, en la mayoría de los casos, la totalidad de la información borrada. La razón de existir de las herramientas de recuperación de información es que, si el comando o la aplicación encargada de eliminar los archivos o información no deseada, funcionara, no se tendría la necesidad de recuperar la información, ya que se daría por perdida.

Se puede recuperar toda clase de información, como el tipo de datos que comúnmente utiliza o elabora cualquier persona, por ejemplo, cartas, control de gastos, diarios, fotografías digitales, canciones, etc., en otras palabras, toda información perdida es recuperable, siempre y cuando no se cree un archivo nuevo o se corra alguna otra aplicación que modifique la estructura de bloques de la información eliminada, ya que en ese momento se puede sobrescribir, lo que podría hacer, que la información pudiese cambiar y deformarse, haciendo más difícil su completa o integra recuperación.

Por lo que se recomienda antes que nada, crear un respaldo de toda la información que el usuario considere importante, a fin de evitar pasar por una situación semejante; pero, si el problema existe, lo que se sugiere es crear inmediatamente la copia o imagen maestra del disco duro comprometido, ya que de esta manera se aseguran más probabilidades de la recuperación total de la información.

Este proyecto me dio la oportunidad de ver un panorama que jamás me había imaginado. Anteriormente, creía que si se formateaba un disco se eliminaba toda la información que poseía, pero la realidad es completamente diferente, es decir, la información perdura. La única forma de asegurarse que la información de un disco duro sea eliminada en un 100%, es destruyendo completamente el disco en cuestión.

Hay personas quienes realmente se preocupan por el contenido de sus equipos, ya que pueden contener información que los podría comprometer y ocasionarles problemas con la justicia.

Dicha información puede ser de contenido pornográfico, también puede contener información de entrega de mercancía de drogas o contactos con narcotraficantes, etc., en fin el abanico de escenarios es gigantesco, pero lo que si es un hecho es que la recuperación de este tipo de información es muy importante, ya que de eso depende poner tras las rejas a personas que atentan contra la integridad física, moral y espiritual de las personas. Este es el campo de la informática forense, la cual a través de las técnicas analíticas permite recuperar evidencia incriminatoria que, bien manejada, puede ser admitida en un procedimiento legal.

APÉNDICE A

GLOSARIO

Análisis: La tercera fase del proceso forense, la cuál involucra el uso de métodos y técnicas legalmente justificables para proporcionar información útil para elaborar las preguntas necesarias que justifican las acciones de la recolección y la examinación.

Anti-forense: Una técnica para esconder o destruir datos para que otros no puedan accesarlos.

Archivo: Una colección de información lógicamente agrupada como una sencilla entidad identificada con un nombre único, conocido como nombre de archivo.

Archivo borrado: Un archivo que ha sido lógicamente, pero no necesariamente físicamente borrado del sistema operativo, quizás para eliminar evidencia potencial. El borrar los archivos no necesariamente elimina la posibilidad de recuperarlos todos o parte de a evidencia original.

Archivo inactivo: Espacio entre el fin lógico el archivo y el fin de la última unidad de asignación para ese archivo.

BIOS: Basic Input Output System. Es una colección de rutinas almacenadas en la memoria de solo lectura que habilitan a la computadora para arrancar el sistema operativo y permitir la comunicación con los varios dispositivos en el sistema tales como discos duros, teclado, monitor, impresora y puertos de comunicaciones.

Bit Stream: Una técnica de copiado de datos bit por bit del dispositivo original, que incluye el espacio libre y el espacio inactivo. Esta técnica se conoce también como “clonado”.

Bloqueador contra escritura: Una herramienta que previene modificar la información de un disco duro comprometido una vez que esta conectado a una estación de análisis.

Buffer: Un área de la memoria, comúnmente conocida como "cache", usada para acelerar el acceso a dispositivos. Es usada para el almacenamiento temporal de datos que son leídos de o serán enviados a un dispositivo, el disco duro por ejemplo.

Cadena de custodia: Un proceso de seguimiento de la evidencia desde su recolección, su protección, así como su análisis al documentar a cada persona que ha tenido contrato con la evidencia, la fecha y hora que fue recolectada o transferida.

Ciencia forense: La aplicación de la ciencia a la ley.

Cluster: Un grupo de sectores contiguos.

Código Malicioso: Un virus, gusano, troyano u otro código que infecta un sistema.

Compilación: Proceso por el cual se 'traduce' un programa escrito en un lenguaje de programación a un lenguaje que entienda la computadora.

Computadora "stand alone": Es una computadora que no está conectada a la red o a otras computadoras.

Copia forense: Una reproducción exacta, bit por bit, de la información contenida en un elemento electrónico o medio asociado cuya validez e integridad se verifican utilizando un algoritmo.

Datos: Diferentes fragmentos de información digital, los cuales poseen un formato determinado.

Directorio: Una estructura que agrupa y mantiene a los archivos organizados.

Encabezado de archivo: La información en un archivo que contiene información de identificación y posiblemente metadatos con información acerca del contenido del archivo.

Espacio libre: Un área en el medio o en la memoria que no esta asignada.

Espacio inactivo: El espacio que no es utilizado en un bloque de asignación de archivo que puede contener información residual.

Especialista forense: Localiza, identifica, recolecta, analiza y examina los datos mientras preserva la integridad y mantiene una estricta cadena de custodia de la información descubierta.

Esteganografía: El arte y la ciencia de la comunicación de una manera que esconde la existencia de la comunicación. Por ejemplo una imagen pornográfica de un niño se puede esconder dentro de otro archivo de imagen, un archivo de audio u otro formato de archivo.

Examinación: La segunda fase del proceso forense. La cual involucra el procesamiento de grandes cantidades de datos recolectados utilizando una combinación de métodos automáticos y manuales para valorar y extraer la información de interés particular, mientras se preserva la integridad de la información.

Evidencia Digital: Información electrónica almacenada o transmitida de forma binaria.

Forensia Digital: La aplicación de la ciencia a la identificación, recolección, examinación y análisis de los datos mientras se preserva la integridad de la información y se mantiene una estricta cadena de custodia.

Hashing: El proceso de utilizar un algoritmo matemático en los datos para producir un valor numérico el cual representa a la información.

Host: Suele utilizarse en el contexto de las redes de computadoras para referirse a cualquier computadora conectada a la red.

Imagen: Una copia exacta por la técnica de bit stream, de todos los datos electrónicos en un elemento, llevada a cabo en una forma que la información no sea alterada.

Incidente: Una violación o amenaza inminente de violación de las políticas de seguridad informáticas o de prácticas estándares de seguridad informática.

Información no volátil: Información que persiste incluso después de que se apaga la computadora.

Información volátil: La información en un sistema activo que se pierde después de que la computadora se apaga.

Inodo (nodo-i o i-nodo): Es un área de almacenamiento de 64 bytes. El modo de un archivo normal o de un directorio contiene la localización de su(s) bloque(s) de disco. El modo de un archivo especial contiene la información que identifica al dispositivo periférico. Un modo puede contener otra información que incluye: permiso de acceso del archivo, identificación de propietario y de grupo, número de enlaces del archivo, hora de la última modificación del archivo, hora del último acceso, localización de bloques para cada archivo, y número de identificación del dispositivo para archivos especiales. Los modos se enumeran secuencialmente.

Kernel: También conocido como núcleo. Es el nivel más interno del software del sistema operativo. Es el único nivel que interacciona directamente con el hardware.

Linux: Sistema operativo de licencia pública para computadoras personales, derivado de Unix.

Medios removibles: Objetos (disquetes, CD’s, DVD’s, cartuchos, cintas, etc.) que almacenan datos y que pueden ser fácilmente removidos.

Medios magnéticos: Pueden ser discos, cintas, cartuchos, disquetes o casetes que son usados para almacenar datos magnéticamente.

Metadato: Información acerca de la información. Para los sistemas de archivos, los metadatos son la información que provee información acerca del contenido de un archivo.

Montaje: Proceso por el cual se permite hacer presente un sistema de archivos hasta que sea desmontado.

Negación del servicio (DOS): Un ataque que impide el uso autorizado de redes, sistemas o aplicaciones al agotar los recursos.

Nombre de archivo: Un nombre único utilizado para identificar a un archivo.

Partición: Una porción lógica de un medio que funciona como si estuviera físicamente separada de otras porciones lógicas.

Proceso: Un programa en ejecución.

Recolección: La primera fase del proceso forense, la cual involucra el identificar, etiquetar, grabar y adquirir información de fuentes posibles y relevantes, mientras se siguen las directrices y procedimientos que preservan la integridad e la evidencia.

Reporte: La fase final del proceso forense. Involucra el reporte de los resultados del análisis; esto incluye la descripción de las acciones que se levaron a cabo, la explicación de como fue que se selecciono las herramientas y técnicas, así como otras acciones y proveer recomendaciones el mejoramiento de políticas, directrices, procedimientos, herramientas y otros aspectos del proceso forense.

Respaldo lógico: Una copia de los directorios y archivos de un volumen lógico.

Sector: La unidad más pequeña a la que se puede accesar en el medio.

Sistema de archivo: Un método para nombrar, almacenar, organizar y accesar a los archivos en volúmenes lógicos.

Sistema operativo: Un programa que se ejecuta en una computadora y que provee una plataforma sobre la cual se pueden ejecutar otros programas.

Subdirectorio: Un directorio al cual lo almacena otro directorio.

Swap: Área que comprende una o más particiones de disco para guardar páginas de memoria temporales.

UID: User Identifier. Número único que identifica a cada usuario en el sistema.

USB: Universal Serial Bus: Interfaz de hardware para periféricos de baja velocidad tales como el teclado, ratón, joystick, escáner, impresora, etc.

APÉNDICE B

LEYES QUE CONTEMPLAN LOS ASPECTOS INFORMÁTICOS EN MÉXICO

Esta investigación toma como referencia las respectivas leyes federales actualizadas hasta el 12 de junio de 2003[*].

Dada la extensión de cada una de estas leyes y sus artículos, solo se presenta la parte o fracción que hace referencia explícita al aspecto informático. Se presentan según lo que cada ley pretende legislar.

B.1 DE LOS DELITOS INFORMÁTICOS

Código Penal Federal

Artículo 167.- Se impondrán de uno a cinco años de prisión y de cien a diez mil días multa:

VI.- Al que dolosamente o con fines de lucro, interrumpa o interfiera las comunicaciones, alámbricas, inalámbricas.

CAPITULO II Corrupción de menores e incapaces. Pornografía infantil y prostitución sexual de menores

Artículo 201 bis.- Al que procure o facilite por cualquier medio el que uno o más menores de dieciocho años, con o sin su consentimiento, lo o los obligue o induzca a realizar actos de exhibicionismo corporal, lascivos o sexuales, con el objeto y fin de videograbarlos, fotografiarlos o exhibirlos mediante anuncios impresos o electrónicos, con o sin el fin de obtener un lucro, se le impondrán de cinco a diez años de prisión y de mil a dos mil días multa.
…

TITULO NOVENO Revelación de secretos y acceso ilícito a sistemas y equipos de informática

[*] Poder Legislativo Federal (12 junio 2003). Legislación Federal de México, [en línea]. México: Cámara de Diputados del H. Congreso de la Unión. Disponible en: http://www.diputados.gob.mxlleyinfo/ [2003, junio].

CAPITULO I Revelación de secretos

Artículo 210.- Se impondrán de treinta a doscientas jornadas de trabajo en favor de la comunidad, al que sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto.

Artículo 211.- La sanción será de uno a cinco años, multa de cincuenta a quinientos pesos y suspensión de profesión en su caso, de dos meses a un año, cuando la revelación punible sea hecha por persona que presta servicios profesionales o técnicos o por funcionario o empleado público o cuando el secreto revelado o publicado sea de carácter industrial.

Artículo 211 Bis.- A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.

Capítulo II Acceso ilícito a sistemas y equipos de informática

Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Artículo 211 bis 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

Artículo 211 bis 4.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las

instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.
Artículo 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Artículo 211 bis 6.- Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.

Artículo 211 bis 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

TITULO VIGESIMO SEXTO De los Delitos en Materia de Derechos de Autor

Artículo 424 bis.- Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa:

II. A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación.

Código Penal para el Distrito Federal

TITULO DÉCIMO QUINTO Delitos contra el patrimonio
Capítulo III Fraude

Artículo 230.- Al que por medio del engaño o aprovechando el error en que otro se halle, se haga ilícitamente de alguna cosa u obtenga un lucro indebido en beneficio propio o de un tercero, se le impondrán:

XIV.- Para obtener algún beneficio para sí o para un tercero, por cualquier medio accese, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la Institución;

Ley Federal de Telecomunicaciones

Artículo 3.- Para los efectos de esta Ley se entenderá por:

VIII. Red de telecomunicaciones: sistema integrado por medios de transmisión, tales como canales o circuitos que utilicen bandas de frecuencias del espectro radioeléctrico, enlaces satelitales, cableados, redes de transmisión eléctrica o cualquier otro medio de transmisión, así como, en su caso, centrales, dispositivos de conmutación o cualquier equipo necesario;
IX. Red privada de telecomunicaciones: la red de telecomunicaciones destinada a satisfacer necesidades específicas de servicios de telecomunicaciones de determinadas personas que no impliquen explotación comercial de servicios o capacidad de dicha red;

X. Red pública de telecomunicaciones: la red de telecomunicaciones a través de la cual se explotan comercialmente servicios de telecomunicaciones. La red no comprende los equipos terminales de telecomunicaciones de los usuarios ni las redes de telecomunicaciones que se encuentren más allá del punto de conexión terminal;

Artículo 28.- Las redes privadas de telecomunicaciones no requerirán de concesión, permiso o registro para operar, salvo que utilicen bandas de frecuencias del espectro, en cuyo caso se estará alo dispuesto en el artículo 14.

Para que los operadores de redes privadas puedan explotar comercialmente servicios, deberán obtener concesión en los términos de esta Ley, en cuyo caso adoptarán el carácter de red pública de telecomunicaciones.

Artículo 44.- Los concesionarios de redes públicas de telecomunicaciones deberán:

VIII. Permitir la conexión de equipos terminales, cableados internos y redes privadas de los usuarios, que cumplan con las normas establecidas;

CAPITULO IX Infracciones y sanciones

Artículo 71.- Las infracciones a lo dispuesto en esta Ley, se sancionarán por la Secretaría de conformidad con lo siguiente:

A. Con multa de 10,000 a 100,000 salarios mínimos por:

V Interceptar información que se transmita por las redes públicas de telecomunicaciones.

B. Con multa de 4,000 a 40,000 salarios mínimos por:

III. Cometer errores en la información de base de datos de usuarios, de directorios, y en el cobro de los servicios de concesionarios de redes públicas, no obstante el apercibimiento de la Secretaría,

B.2 DEL COMERCIO ELECTRÓNICO

Código de Comercio

Artículo 48.- Tratándose de las copias de las cartas, telegramas y otros documentos que los comerciantes expidan, así como de los que reciban que no estén incluidos en el artículo siguiente, el archivo podrá integrarse con copias obtenidas por cualquier medio: mecánico, fotográfico o electrónico, que permita su reproducción posterior íntegra y su consulta o compulsa en caso necesario

Artículo 49.- Los comerciantes están obligados a conservar por un plazo mínimo de diez años los originales de aquellas cartas, telegramas, mensajes de datos o cualesquiera otros documentos en que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones.

Para efectos de la conservación o presentación de originales, en el caso de mensajes de datos, se requerirá que la información se haya mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y sea accesible para su ulterior consulta. La Secretaría de Comercio y Fomento Industrial emitirá la Norma Oficial Mexicana que establezca los requisitos que deberán observarse para la conservación de mensajes de datos.

Artículo 80.- Los convenios y contratos mercantiles que se celebren por correspondencia, telégrafo, o mediante el uso de medios electrónicos, ópticos o de cualquier otra tecnología, quedarán perfeccionados desde que se reciba la aceptación de la propuesta o las condiciones con que ésta fuere modificada.

Artículo 89.- En los actos de comercio podrán emplearse los medios electrónicos, ópticos o cualquier otra tecnología. Para efecto del presente Código, a la información generada, enviada, recibida, archivada o comunicada a través de dichos medios se le denominará mensaje de datos.

Artículo 90.- Salvo pacto en contrario, se presumirá que el mensaje de datos proviene del emisor si ha sido enviado:

I.- Usando medios de identificación, tales como claves o contraseñas de él, o

II.- Por un sistema de información programado por el emisor o en su nombre para que opere automáticamente.

Artículo 92.- Tratándose de la comunicación de mensajes de datos que requieran de un acuse de recibo para surtir efectos, bien sea por disposición legal o por así requerirlo el emisor, se considerará que el mensaje de datos ha sido enviado, cuando se haya recibido el acuse respectivo.

Salvo prueba en contrario, se presumirá que se ha recibido el mensaje de datos cuando el emisor reciba el acuse correspondiente.

Artículo 93.- Cuando la ley exija la forma escrita para los contratos y la firma de los documentos relativos, esos supuestos se tendrán por cumplidos tratándose de mensaje de datos siempre que éste sea atribuible a las personas obligadas y accesibles para su ulterior consulta.

En los casos en que la ley establezca como requisito que un acto jurídico deba otorgarse en instrumento ante fedatario público, éste y las partes obligadas podrán, a través de mensajes de datos, expresar los términos exactos en que las partes han decidido obligarse, en cuyo caso el fedatario público, deberá hacer constar en el propio instrumento los elementos a través de los cuales se atribuyen dichos mensajes a las partes y conservar bajo su resguardo una versión íntegra de los mismos para su posterior consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige.

Artículo 94.- Salvo pacto en contrario, el mensaje de datos se tendrá por expedido en el lugar donde el emisor tenga su domicilio y por recibido en el lugar donde el destinatario tenga el suyo.

Artículo 1205.- Son admisibles como medios de prueba todos aquellos elementos que puedan producir convicción en el ánimo del juzgador acerca de los hechos controvertidos o dudosos y en consecuencia serán tomadas como pruebas las declaraciones de las partes, terceros, peritos, documentos públicos o privados, inspección judicial, fotografías, facsímiles, cintas cinematográficas, de videos, de sonido, mensajes de datos, reconstrucciones de hechos y en general cualquier otra similar u objeto que sirva para averiguar la verdad.

Artículo 1298-A.- Se reconoce como prueba los mensajes de datos. Para valorar la fuerza probatoria de dichos mensajes, se estimará primordialmente la fiabilidad del método en que haya sido generada, archivada, comunicada o conservada.

Ley Federal de Protección al Consumidor

Artículo 1.- La presente ley es de orden público e interés social y de observancia en toda la República. Sus disposiciones son irrenunciables y contra su observancia no podrán alegarse costumbres, usos, prácticas o estipulaciones en contrario.

VIII.- La efectiva protección al consumidor en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología y la adecuada utilización de los datos aportados.

Los derechos previstos en esta ley no excluyen otros derivados de tratados o convenido internacionales de los que México sea signatario; de la legislación interna ordinaria; de reglamentos expedidos por las autoridades administrativas competentes; así como de los que deriven de los principios generales de derecho, la analogía, las costumbres y la equidad.

Artículo 24.- La Procuraduría tiene las siguientes atribuciones:

IX bis.- Promover en coordinación con la Secretaría la formulación, difusión y uso de códigos de ética, por parte de proveedores, que incorporen los principios previstos por esta Ley respecto de las transacciones que celebren con consumidores a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología;

CAPITULO VIII BIS De los derechos de los consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología

Artículo 76 bis.- Las disposiciones del presente Capítulo aplican a las relaciones entre proveedores y consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología. En la celebración de dichas transacciones se cumplirá con lo siguiente:

I. El proveedor utilizará la información proporcionada por el consumidor en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente;

II. El proveedor utilizará alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el consumidor e informará a éste, previamente a la celebración de la transacción, de las características generales de dichos elementos;

III. El proveedor deberá proporcionar al consumidor, antes de celebrar la transacción, su domicilio físico, números telefónicos y demás medios a los que pueda acudir el propio consumidor para presentarle sus reclamaciones o solicitarle aclaraciones;

IV. El proveedor evitará las prácticas comerciales engañosas respecto de las características de los productos, por lo que deberá cumplir con las disposiciones relativas a la información y publicidad de los bienes y servicios que ofrezca, señaladas en esta Ley y demás disposiciones que se deriven de ella;

V. El consumidor tendrá derecho a conocer toda la información sobre los términos, condiciones, costos, cargos adicionales, en su caso, formas de pago de los bienes y servicios ofrecidos por el proveedor;

VI. El proveedor respetará la decisión del consumidor en cuanto a la cantidad y calidad de los productos que desea recibir, así como la de no recibir avisos comerciales, y

VII. El proveedor deberá abstenerse de utilizar estrategias de venta o publicitarias que no proporcionen al consumidor información clara y suficiente sobre los servicios ofrecidos, y cuidará las prácticas de mercadotecnia dirigidas a población vulnerable, como niños, ancianos y enfermos, incorporando mecanismos que adviertan cuando la información no sea apta para esa población.

Artículo 128.- Las infracciones a lo dispuesto por los artículos 8, 10, 12, 60, 63, 65, 74, 76 bis, 80 y 121 serán sancionadas con multa por el equivalente de una y hasta dos mil quinientas veces el salario mínimo general vigente para el Distrito Federal.

Ley de Instituciones de Crédito

Artículo 52.- Las instituciones de crédito podrán pactar la celebración de sus operaciones y la prestación de servicios con el público, mediante el uso de equipos, medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean privados o públicos, estableciendo en los contratos respectivos las bases para determinar lo siguiente:

I. Las operaciones y servicios cuya prestación se pacte;

II. Los medios de identificación del usuario y las responsabilidades correspondientes a su uso, y

III. Los medios por los que se hagan constar la creación, transmisión, modificación o extinción de derechos y obligaciones inherentes a las operaciones y servicios de que se trate.

El uso de los medios de identificación que se establezcan conforme a lo previsto por este artículo, en sustitución de la firma autógrafa, producirá los mismos efectos que las leyes otorgan a los documentos correspondientes y, en consecuencia, tendrán el mismo valor probatorio.

La instalación y el uso de los equipos y medios señalados en el primer párrafo de este artículo, se sujetarán a las Reglas de carácter general que en su caso, emita la Comisión Nacional Bancaria y de Valores.

Lo anterior, sin perjuicio de las facultades con que cuenta el Banco de México para regular las operaciones que efectúen las instituciones de crédito relacionadas con los sistemas de pagos y las de transferencias de fondos en términos de su ley.

Artículo 57.- En las operaciones a que se refieren las fracciones I y 11 del artículo 46 de esta Ley, los depositantes o inversionistas podrán autorizar a terceros para hacer disposiciones de dinero, bastando para ello la autorización firmada en los registros especiales que lleve la institución de crédito.

Las autorizaciones, instrucciones y comunicaciones a que se refiere este artículo podrán llevarse a cabo por escrito con firma autógrafa o a través de los medios electrónicos, ópticos o de cualquier otra tecnología que previamente convengan las partes, debiendo contar las instituciones de crédito con los registros, archivos u otros medios que les permitan presentar ante la autoridad competente, la fecha y demás características principales de las reclamaciones que, en su caso, presenten los usuarios.

Artículo 112 Bis.- Se sancionará con prisión de tres a nueve años y de treinta mil a trescientos mil días multa, al que:

I. Produzca, reproduzca, introduzca al país, imprima o comercie tarjetas de crédito, de débito, formatos o esqueletos de cheques, o en general instrumentos de pago utilizados por el sistema bancario, sin consentimiento de quien esté facultado para ello;

II. Posea, utilice o distribuya tarjetas de crédito, de débito, formatos o esqueletos de cheques, o en general instrumentos de pago utilizados por el sistema bancario, a sabiendas de que son falsos;

III. Altere el medio de identificación electrónica y acceda a los equipos electromagnéticos del sistema bancario, con el propósito de disponer indebidamente de recursos económicos, u

IV. Obtenga o use indebidamente la información sobre clientes u operaciones del sistema bancario, y sin contar con la autorización correspondiente.

La pena que corresponda podrá aumentarse hasta en una mitad más, si quien realice cualquiera de las conductas señaladas en las fracciones anteriores tiene el carácter de consejero, funcionario o empleado de cualquier institución de crédito.

Ley de Sociedades de Inversión

Artículo 45.- Los precios actualizados de valuación de las acciones de las sociedades de inversión, se darán a conocer al público a través de medios impresos o electrónicos de amplia circulación o divulgación,...

Artículo 79.- Las sociedades de inversión, sociedades operadoras de sociedades de inversión y sociedades distribuidoras de acciones de sociedades de inversión, deberán publicar en medios impresos o electrónicos de amplia circulación o divulgación, los estados financieros trimestrales y anuales,...

B.3 DE LA PROTECCIÓN JURÍDICA DE LA INFORMACIÓN ELECTRÓNICA

Ley Federal del Derecho de Autor

Artículo 16.- La obra podrá hacerse del conocimiento público mediante los actos que se describen a continuación:

II. Publicación: La reproducción de la obra en forma tangible y su puesta a disposición del público mediante ejemplares, o su almacenamiento permanente o provisional por medios electrónicos, que permitan al público leerla o conocerla visual, táctil o auditivamente;

VI.- Reproducción: La realización de uno o varios ejemplares de una obra, de un fonograma o de un videograma, en cualquier forma tangible, incluyendo cualquier almacenamiento permanente o temporal por medios electrónicos, aunque se trate de la realización bidimensional de una obra tridimensional o viceversa.

Artículo 27.- Los titulares de los derechos patrimoniales podrán autorizar o prohibir:

I. La reproducción, publicación, edición o fijación material de una obra en copias o ejemplares, efectuada por cualquier medio ya sea impreso, fonográfico, gráfico, plástico, audiovisual, electrónico u otro similar;

CAPITULO IV De los Programas de Computación y las Bases de Datos

Artículo 101.- Se entiende por programa de computación la expresión original en cualquier forma, lenguaje o código, de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica.

Artículo 102.- Los programas de computación se protegen en los mismos términos que las obras literarias. Dicha protección se extiende tanto a los programas operativos como a los programas aplicativos, ya sea en forma de código fuente o de código objeto. Se exceptúan aquellos programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos.

Artículo 103.- Salvo pacto en contrario, los derechos patrimoniales sobre un programa de computación y su documentación, cuando hayan sido creados por uno o varios empleados en el ejercicio de sus funciones o siguiendo las instrucciones del empleador, corresponden a éste.

Como excepción a lo previsto por el artículo 33 de la presente Ley, el plazo de la cesión de derechos en materia de programas de computación no está sujeto a limitación alguna.

Artículo 104.- Como excepción a lo previsto en el artículo 27 fracción IV, el titular de los derechos de autor sobre un programa de computación o sobre una base de datos conservará, aún después de la venta de ejemplares de los mismos, el derecho de autorizar o prohibir el arrendamiento de dichos ejemplares. Este precepto no se aplicará cuando el ejemplar del programa de computación no constituya en sí mismo un objeto esencial de la licencia de uso.

Artículo 105.- El usuario legítimo de un programa de computación podrá realizar el número de copias que le autorice la licencia concedida por el titular de los derechos de autor, o una sola copia de dicho programa siempre y cuando:

I. Sea indispensable para la utilización del programa, o

II. Sea destinada exclusivamente como resguardo para sustituir la copia legítimamente adquirida, cuando ésta no pueda utilizarse por daño o pérdida. La copia de respaldo deberá ser destruida cuando cese el derecho del usuario para utilizar el programa de computación.

Artículo 106.- El derecho patrimonial sobre un programa de computación comprende la facultad de autorizar o prohibir:

I. La reproducción permanente o provisional del programa en todo o en parte, por cualquier medio y forma;

II. La traducción, la adaptación, el arreglo o cualquier otra modificación de un programa y la reproducción del programa resultante;

III. Cualquier forma de distribución del programa o de una copia del mismo, incluido el alquiler, y

IV. La decompilación, los procesos para revertir la ingeniería de un programa de computación y el desensamblaje.

Artículo 107.- Las bases de datos o de otros materiales legibles por medio de máquinas o en otra forma, que por razones de selección y disposición de su contenido constituyan creaciones intelectuales, quedarán protegidas como compilaciones. Dicha protección no se extenderá a los datos y materiales en sí mismos.

Artículo 108.- Las bases de datos que no sean originales quedan, sin embargo, protegidas en su uso exclusivo por quien las haya elaborado, durante un lapso de 5 años.

Artículo 109.- El acceso a información de carácter privado relativa a las personas contenida en las bases de datos a que se refiere el artículo anterior, así como la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, requerirá la autorización previa de las personas de que se trate.

Quedan exceptuados de lo anterior, las investigaciones de las autoridades encargadas de la procuración e impartición de justicia, de acuerdo con la legislación respectiva, así como el acceso a archivos públicos por las personas autorizadas por la ley, siempre que la consulta sea realizada conforme a los procedimientos respectivos.

Artículo 110.- El titular del derecho patrimonial sobre una base de datos tendrá el derecho exclusivo, respecto de la forma de expresión de la estructura de dicha base, de autorizar o prohibir:

I. Su reproducción permanente o temporal, total o parcial, por cualquier medio y de cualquier forma;

II. Su traducción, adaptación, reordenación y cualquier otra modificación;

III. La distribución del original o copias de la base de datos;

IV. La comunicación al público, y

V. La reproducción, distribución o comunicación pública de los resultados de las operaciones mencionadas en la fracción II del presente artículo.

Artículo 111.- Los programas efectuados electrónicamente que contengan elementos visuales, sonoros, tridimensionales o animados quedan protegidos por esta Ley en los elementos primigenios que contengan.

Artículo 112.- Queda prohibida la importación, fabricación, distribución y utilización de aparatos o la prestación de servicios destinados a eliminar la protección técnica de los programas de cómputo, de las transmisiones a través del espectro electromagnético y de redes de telecomunicaciones y de los programas de elementos electrónicos señalados en el artículo anterior.

Artículo 113.- Las obras e interpretaciones o ejecuciones transmitidas por medios electrónicos a través del espectro electromagnético y de redes de telecomunicaciones y el resultado que se obtenga de esta transmisión estarán protegidas por esta Ley.

Artículo 114.- La transmisión de obras protegidas por esta Ley mediante cable, ondas radioeléctricas, satélite u otras similares, deberán adecuarse, en lo conducente, a la legislación mexicana y respetar en todo caso y en todo tiempo las disposiciones sobre la materia.

Artículo 123.- El libro es toda publicación unitaria, no periódica, de carácter literario, artístico, científico, técnico, educativo, informativo o recreativo, impresa en cualquier soporte, cuya edición se haga en su totalidad de una sola vez en un volumen o a intervalos en varios volúmenes o fascículos.

Comprenderá también los materiales complementarios en cualquier tipo de soporte, incluido el electrónico, que conformen, conjuntamente con el libro, un todo unitario que no pueda comercializarse separadamente.
Artículo 231.- Constituyen infracciones en materia de comercio las siguientes conductas cuando sean realizadas con fines de lucro directo o indirecto:

V. Importar, vender, arrendar o realizar cualquier acto que permita tener un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación;

VII. Usar, reproducir o explotar una reserva de derechos protegida o un programa de cómputo sin el consentimiento del titular;

Ley de la Propiedad Industrial

Artículo 19.- No se considerarán invenciones para los efectos de esta Ley:

I.- Los principios teóricos o científicos;

II.- Los descubrimientos que consistan en dar a conocer o revelar algo que ya existía en la naturaleza, aún cuando anteriormente fuese desconocido para el hombre;

III.- Los esquemas, planes, reglas y métodos para realizar actos mentales, juegos o negocios y métodos matemáticos;

IV.- Los programas de computación;

TITULO TERCERO De los Secretos Industriales

Artículo 82.- Se considera secreto industrial a toda información de aplicación industrial o comercial que guarde una persona física o moral con carácter confidencial, que le signifique obtener mantener una ventaja competitiva o económica frente a terceros en la realización de actividades económicas y respecto de la cual haya adoptado los medios o sistemas suficientes para preservar confidencialidad y el acceso restringido a la misma.

La información de un secreto industrial necesariamente deberá estar referida a la naturaleza, características o finalidades de los productos; a los métodos o procesos de producción; o a medios o formas de distribución o comercialización de productos o prestación de servicios.

No se considerará secreto industrial aquella información que sea del dominio público, la que resulte evidente para un técnico en la materia, con base en información previamente disponible o la deba ser divulgada por disposición legal o por orden judicial. No se considerará que entra dominio público o que es divulgada por disposición legal aquella información que proporcionada a cualquier autoridad por una persona que la posea como secreto industrial, cuando la proporcione para el efecto de obtener licencias, permisos, autorizaciones, registros, cualesquiera otros actos de autoridad.

Artículo 83.- La información a que se refiere el artículo anterior, deberá constar en documentos, medios electrónicos o magnéticos, discos ópticos, microfilmes, películas u otros instrumentos similares.

CAPITULO III De los delitos

Artículo 223.- Son delitos:

I.- Falsificar marcas en forma dolosa y escala comercial;

II. Falsificar, en forma dolosa y con fin de especulación comercial, marcas protegidas por esta Ley;

III. Producir, almacenar, transportar, introducir al país, distribuir o vender, en forma dolosa y fin de especulación comercial, objetos que ostenten falsificaciones de marcas protegidas por Ley, así como aportar o proveer de cualquier forma, a sabiendas, materias primas o insumos destinados a la producción de objetos que ostenten falsificaciones de marcas protegidas por
Ley;

IV. Revelar a un tercero un secreto industrial, que se conozca con motivo de su trabajo, puesto, cargo, desempeño de su profesión, relación de negocios o en virtud del otorgamiento de licencia para su uso, sin consentimiento de la persona que guarde el secreto industrial, habiendo sido prevenido de su confidencialidad, con el propósito de obtener un beneficio económico para sí o para el tercero o con el fin de causar un perjuicio a la persona que guarde el secreto;

V. Apoderarse de un secreto industrial sin derecho y sin consentimiento de la persona que lo guarde o de su usuario autorizado, para usarlo o revelarlo a un tercero, con el propósito de obtener un beneficio económico para sí o para el tercero o con el fin de causar un perjuicio a la persona que guarde el secreto industrial o a su usuario autorizado, y

VI. Usar la información contenida en un secreto industrial, que conozca por virtud de su trabajo, cargo o puesto, ejercicio de su profesión o relación de negocios, sin consentimiento de quien lo
guarde o de su usuario autorizado, o que le haya sido revelado por un tercero, a sabiendas que éste no contaba para ello con el consentimiento de la persona que guarde el secreto industrial o su usuario autorizado, con el propósito de obtener un beneficio económico o con el fin de causar un perjuicio a la persona que guarde el secreto industrial o su usuario autorizado.

Los delitos previstos en este artículo se perseguirán por querella de parte ofendida.

Artículo 223 bis.- Se impondrá de dos a seis años de prisión y multa de cien a diez mil días de salario mínimo general vigente en el Distrito Federal, al que venda a cualquier

consumidor final en vías o en lugares públicos, en forma dolosa y con fin de especulación comercial, objetos que ostenten falsificaciones de marcas protegidas por esta Ley. Si la venta se realiza en establecimientos comerciales, o de manera organizada o permanente, se estará a lo dispuesto en los artículos 223 y 224 de esta Ley.

B.4 DE LA VALIDEZ JURÍDICA DE LA INFORMACIÓN ELECTRÓNICA EN LOS PROCEDIMIENTOS CIVILES

Código Federal de Procedimientos Civiles

Artículo 210-A.- Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología.
Para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimará primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta.

Cuando la ley requiera que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta.

Código Civil Federal

Artículo 1803.- El consentimiento puede ser expreso o tácito, para ello se estará a lo siguiente:

I.- Será expreso cuando la voluntad se manifiesta verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos, y

Artículo 1805.- Cuando la oferta se haga a una persona presente, sin fijación de plazo aceptarla, el autor de la oferta queda desligado si la aceptación no se hace inmediatamente. La misma regla se aplicará a la oferta hecha por teléfono o a través de cualquier otro medio electrónico, óptico o de cualquier otra tecnología que permita la expresión de la oferta y la aceptación de ésta forma inmediata.

Artículo 1811.- La propuesta y aceptación hechas por telégrafo producen efectos si los contratantes con anterioridad habían estipulado por escrito esta manera de contratar, y si los originales de respectivos telegramas contienen las firmas de los contratantes y los signos convencionales establecidos entre ellos.

Tratándose de la propuesta y aceptación hechas a través de medios electrónicos, ópticos cualquier otra tecnología no se requerirá de estipulación previa entre los contratantes para produzca efectos.

Artículo 1834 bis.- Los supuestos previstos por el artículo anterior se tendrán por cumplidos mediante la utilización de medios electrónicos, ópticos o de cualquier otra tecnología, siempre la información generada o comunicada en forma íntegra, a través de dichos medios sea atribuible las personas obligadas y accesibles para su ulterior consulta.

En los casos en que la ley establezca como requisito que un acto jurídico deba otorgarse instrumento ante fedatario público, éste y las partes obligadas podrán generar, enviar, recibir, archivar o comunicar la información que contenga los términos exactos en que las partes decidido obligarse, mediante la utilización de medios electrónicos, ópticos o de cualquier tecnología, en cuyo caso el fedatario público, deberá hacer constar en el propio instrumento elementos a través de los cuales se atribuye dicha información a las partes y conservar bajo resguardo una versión íntegra de la misma para su ulterior consulta, otorgando dicho instrumento conformidad con la legislación aplicable que lo rige.

B.5 DE LA VALIDEZ JURÍDICA DE LA INFORMACIÓN ELECTRÓNICA EN LA ADMINISTRACIÓN PÚBLICA

Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público

TITULO TERCERO De los Procedimientos de Contratación

Artículo 26.- Las dependencias y entidades, bajo su responsabilidad, podrán contratar adquisiciones, arrendamientos y servicios, mediante los procedimientos de contratación que continuación se señalan:

I. Licitación pública;

II. Invitación a cuando menos tres personas, o

III. Adjudicación directa.

…

La Contraloría pondrá a disposición pública, a través de los medios de difusión electrónica que establezca, la información que obre en su base de datos correspondiente a las convocatorias y bases de las licitaciones y, en su caso, sus modificaciones; las actas de las juntas de aclaraciones y de visita a instalaciones, los fallos de dichas licitaciones o las cancelaciones de éstas, y los datos relevantes de los contratos adjudicados; ya sea por licitación, invitación a cuando menos tres personas o adjudicación directa.

Artículo 27.- Las adquisiciones, arrendamientos y servicios se adjudicarán, por regla general, a través de licitaciones públicas, mediante convocatoria pública, para que

libremente se presenten proposiciones solventes en sobre cerrado, que será abierto públicamente, a fin de asegurar al Estado las mejores condiciones disponibles en cuanto a precio, calidad, financiamiento, oportunidad y demás circunstancias pertinentes, de acuerdo con lo que establece la presente Ley.

En el caso de las proposiciones presentadas por medios remotos de comunicación electrónica el sobre será generado mediante el uso de tecnologías que resguarden la confidencialidad de la información de tal forma que sea inviolable, conforme a las disposiciones técnicas que al efecto establezca la Contraloría.

Las proposiciones presentadas deberán ser firmadas autógrafamente por los licitantes o sus apoderados; en el caso de que éstas sean enviadas a través de medios remotos de comunicación electrónica, se emplearán medios de identificación electrónica, los cuales producirán los mismos efectos que las leyes otorgan a los documentos correspondientes y, en consecuencia, tendrán el mismo valor probatorio.

La Contraloría operará y se encargará del sistema de certificación de los medios de identificación electrónica que utilicen los licitantes y será responsable de ejercer el control de estos medio, salvaguardando la confidencialidad de la información que se remita por esta vía.

Artículo 67.- En las inconformidades que se presenten a través de medios remotos de comunicación electrónica deberán utilizarse medios de identificación electrónica en sustitución de la firma
autógrafa.

Dichas inconformidades, la documentación que las acompañe y la manera de acreditar la personalidad del promovente, se sujetarán a las disposiciones técnicas que para efectos de la transmisión expida la Contraloría, en cuyo caso producirán los mismos efectos que las leyes otorgan a los medios de identificación y documentos correspondientes.

Ley de Obras Públicas y Servicios Relacionados con las Mismas

TITULO TERCERO De los Procedimientos de Contratación

Artículo 27.- Las dependencias y entidades, bajo su responsabilidad, podrán contratar obras públicas y servicios relacionados con las mismas, mediante los procedimientos de contratación que a continuación se señalan:

I. Licitación pública;

II. Invitación a cuando menos tres personas, o

III. Adjudicación directa.

…

La Contraloría pondrá a disposición pública, a través de los medios de difusión electrónica que establezca, la información que obre en su base de datos correspondiente a las convocatorias y bases de las licitaciones y, en su caso, sus modificaciones; las actas de las juntas de aclaraciones y de visita a instalaciones, los fallos de dichas licitaciones o las cancelaciones de éstas, y los datos relevantes de los contratos adjudicados, sean por licitación, invitación o adjudicación directa.

Artículo 28.- Los contratos de obras públicas y los de servicios relacionados con las mismas se adjudicarán, por regla general, a través de licitaciones públicas, mediante convocatoria pública, para que libremente se presenten proposiciones solventes en sobre cerrado, que será abierto públicamente, a fin de asegurar al Estado las mejores condiciones disponibles en cuanto a precio, calidad, financiamiento, oportunidad y demás circunstancias pertinentes, de acuerdo con lo que establece la presente Ley.

En el caso de las proposiciones presentadas por medios remotos de comunicación electrónica el sobre será generado mediante el uso de tecnologías que resguarden la confidencialidad de la información de tal forma que sea inviolable, conforme a las disposiciones técnicas que al efecto establezca la Contraloría.

Las proposiciones presentadas deberán ser firmadas autógrafamente por los licitantes o sus apoderados; en el caso de que éstas sean enviadas a través de medios remotos de comunicación electrónica, en sustitución de la firma autógrafa, se emplearán medios de identificación electrónica, los cuales producirán los mismos efectos que las leyes otorgan a los documentos correspondientes y, en consecuencia, tendrán el mismo valor probatorio.

La Contraloría operará y se encargará del sistema de certificación de los medios de identificación electrónica que utilicen los licitantes y será responsable de ejercer el control de estos medios, salvaguardando la confidencialidad de la información que se remita por esta vía.

Artículo 85.- En las inconformidades que se presenten a través de medios remotos de comunicación electrónica, deberán utilizarse medios de identificación electrónica en sustitución de la firma autógrafa.

Dichas inconformidades, la documentación que las acompañe y la manera de acreditar la personalidad del promovente, se sujetarán a las disposiciones técnicas que para efectos de la transmisión expida la Contraloría, en cuyo caso producirán los mismos efectos que las leyes otorgan a los medios de identificación y documentos correspondientes.

Ley Federal de Procedimiento Administrativo

Artículo 69-C.- Los titulares de las dependencias u órganos administrativos desconcentrados y directores generales de los organismos descentralizados de la

administración pública federal
podrán, mediante acuerdos generales publicados en el Diario Oficial de la Federación, establecer plazos de respuesta menores dentro de los máximos previstos en leyes o reglamentos y no exigir la presentación de datos y documentos previstos en las disposiciones mencionadas, cuando puedan obtener por otra vía la información correspondiente.

En los procedimientos administrativos, las dependencias y los organismos descentralizados de la Administración Pública Federal recibirán las promociones o solicitudes que, en términos de esta Ley, los particulares presenten por escrito, sin perjuicio de que dichos documentos puedan presentarse a través de medios de comunicación electrónica en las etapas que las propias dependencias y organismos así lo determinen mediante reglas de carácter general publicadas en el Diario Oficial de la Federación. En estos últimos casos se emplearán, en sustitución de la firma autógrafa, medios de identificación electrónica.

El uso de dichos medios de comunicación electrónica será optativo para cualquier interesado, incluidos los particulares que se encuentren inscritos en el Registro de Personas Acreditadas a que alude el artículo 69-B de esta Ley.

Los documentos presentados por medios de comunicación electrónica producirán los mismos efectos que las leyes otorgan a los documentos firmados autógrafamente y, en consecuencia, tendrán el mismo valor probatorio que las disposiciones aplicables les otorgan a éstos.
La certificación de los medios de identificación electrónica del promovente, así como la verificación de la fecha y hora de recepción de las promociones o solicitudes y de la autenticidad de las manifestaciones vertidas en las mismas, deberán hacerse por las dependencias u organismos descentralizados, bajo su responsabilidad, y de conformidad con las disposiciones generales que al efecto emita la Secretaría de Contraloría y Desarrollo Administrativo.

Las dependencias y organismos descentralizados podrán hacer uso de los medios de comunicación electrónica para realizar notificaciones, citatorios o requerimientos de documentación e información a los particulares, en términos de lo dispuesto en el artículo 35 de esta Ley.

Ley de Servicio de la Tesorería de la Federación

Artículo 14-Bis.- La Tesorería estará facultada para celebrar las operaciones y prestar los servicios a que se refiere la presente Ley, mediante la utilización de documentos escritos con la correspondiente firma autógrafa del servidor público competente, o bien, a través de equipos o sistemas automatizados, para lo cual, en sustitución de la firma autógrafa, se emplearán medios de identificación electrónica.

Para la utilización de los equipos o sistemas automatizados a los que alude el párrafo anterior, la Tesorería dará a conocer a las dependencias y entidades de la administración pública federal como mínimo lo siguiente:

I. Las operaciones y servicios cuya prestación se establezca;

II. Los medios de identificación del usuario y las responsabilidades correspondientes a su uso, y

III. Los medios por los que se haga constar la creación, establecimiento, transmisión, modificación o extinción de derechos y obligaciones inherentes a las operaciones y servicios de que se trate.
El uso de los medios de identificación que se establezca conforme a lo previsto en esta Ley, en sustitución de la firma autógrafa, producirá los mismos efectos que las leyes otorgan a los documentos correspondientes y, en consecuencia, tendrán el mismo valor probatorio.

La Tesorería será responsable de llevar un estricto control de los medios de identificación electrónica que autorice, así como de cuidar la seguridad y protección de los equipos o sistemas automatizados y, en su caso, de la confidencialidad de la información en ellos contenida.

APÉNDICE C

Herramientas y Recursos en Línea

Las siguientes listas proveen ejemplos de herramientas y recursos en línea (especialmente de código abierto) que pueden ser de gran ayuda al establecimiento de una capacidad forense o de llevar a cabo un análisis forense de sistema o de red.

Organizaciones que Apoyan la Ciencia Forense

Organización	URL
Crimen Informático y Sección de Propiedad Intelectual (CCIPS), Departamento de Justicia de Estados Unidos	http://www.cybercrime.gov/
Federal Bureau of Investigation (FBI)	http://www.fbi.gov/
Asociación de Florida de Investigadores del Crimen Informático (FACCI)	http://www.facci.org/
Asociación de la Investigación del Crimen de Alta Tecnología (HTCIA)	http://www.htcia.org/
Asociación Internacional de Especialistas e Investigadores de la Informática (IACIS)	http://www.cops.org/
Procuración de Justicia Nacional y Centro Noreste de Correciones Tecnológicas (NLECTC-NE)	http://www.nlectc.org/nlectcne/
Centro Nacional de Crimenes de Cuello Blanco(NW3C)	http://www.nw3c.org/
Laboratorio Regional Forense de Informática (RCFL)	http://www.rcfl.gov/
SEARCH: Consorcio Nacional para la Justicia, Información y Estadísticas	http://www.search.org/

Sitios para recursos técnicos

Nombre del recurso	URL
Centro de Investigación para el Crimen Informático	http://www.crime-research.org/
Enlaces para el Cómputo Forense (compilado por David Dittrich)	http://staff.washington.edu/dittrich/
Enlaces y Apuntes para el Cómputo Forense	http://www.forensics.nl/links
Proyecto de Prueba de Herramientas Forenses Informáticas (FCTT)	http://www.cftt.nist.gov/
Recursos Legales y Técnicas Digitales	http://www.digitalmountain.com/technical_resources
Centro de Información de Electrónica Digital	http://www.e-evidence.info/
Enlaces Forenses	http://www.forensicfocus.com/
Instituto Nacional de Justicia (NIJ) y Programa del Crimen Electrónico	http://www.ojp.usdoj.gov/nij/topics/ecrime/welcome.html
Biblioteca Nacional de referencia de Software (NSRL)	http://www.nsrl.nist.gov/
Centro de tecnología e Investigación Pathways	http://www.techpathways.com/DesktopDefault.aspx?tabindex=8&tabid=14
Wotsit´ Format	http://www.wotsit.org/

Recursos de entrenamiento

Nombre del recurso de entrenamiento	URL
CompuForensics	http://www.compuforensics.com/training.htm
Computer Forensic Services	http://www.computerforensic.com/training.html
Computer Forensics Training Center Online	http://www.cftco.com/
Federal Law Enforcement Training Center (FLETC), Computer & Financial Investigations (CFI) Division	http://www.fletc.gov/cfi/index.htm
Foundstone	http://www.foundstone.com/
IACIS	http://www.iacis.info/iacisv2/pages/training.php
InfoSec Institute	http://www.infosecinstitute.com/courses/computer_forensics_training.html
MIS Training Institute (MISTI)	http://www.misti.com/
New Technologies Inc. (NTI)	http://www.forensics-intl.com/training.html
NW3C	http://www.nw3c.org/ocr/courses_desc.cfm
SANS Institute	http://www.sans.org/

Otros Documentos y Recursos Técnicos

Nombre del Recurso	URL
Basic Steps in Forensic Analysis of Unix Systems, por Dave Dittrich	http://staff.washington.edu/dittrich/misc/forensics/
Computer Forensics: Introduction to Incident Response and Investigation of Windows NT/2000, por Norman Haase	http://www.sans.org/rr/whitepapers/incident/647.php
Digital Investigation: The International Journal of Digital Forensics & Incident Response	http://www.compseconline.com/digitalinvestigation/
Electronic Crime Scene Investigation: A Guide for First Responders	http://www.ncjrs.gov/
Evidence Seizure Methodology for Computer Forensics, por Thomas Rude	http://www.crazytrain.com/seizure.html
Forensic Analysis of a Live Linux System, por Mariusz Burdach	http://www.securityfocus.com/infocus/1769 (part one), http://www.securityfocus.com/infocus/1773 (part two)
How to Bypass BIOS Passwords	http://labmice.techtarget.com/articles/BIOS_hack.htm
International Journal of Digital Evidence	http://www.utica.edu/academic/institutes/ecii/ijde/
NIST Interagency Report (IR) 7100, PDA Forensic Tools: An Overview and Analysis	http://csrc.nist.gov/publications/nistir/index.html
NIST IR 7250, Cell Phone Forensic Tools: An Overview and Analysis	http://csrc.nist.gov/publications/nistir/index.html
NIST SP 800-31, Intrusion Detection Systems	http://csrc.nist.gov/publications/nistpubs/index.html
NIST SP 800-44, Guidelines on Securing Public Web Servers	http://csrc.nist.gov/publications/nistpubs/index.html
NIST SP 800-45, Guidelines on Electronic Mail Security	http://csrc.nist.gov/publications/nistpubs/index.html
NIST SP 800-61, Computer Security Incident Handling Guide	http://csrc.nist.gov/publications/nistpubs/index.html
NIST SP 800-72, Guidelines on PDA Forensics	http://csrc.nist.gov/publications/nistpubs/index.html
NIST SP 800-83, Guide to Malware Incident Prevention and Handling	http://csrc.nist.gov/publications/nistpubs/index.html
An Overview of Steganography for the Computer Forensic Examiner, por Gary Kessler	http://www.fbi.gov/hq/lab/fsc/backissu/july2004/research/2004_03_research01.htm
RFC 3164: The BSD Syslog Protocol	http://www.ietf.org/rfc/rfc3164.txt
RFC 3227: Guidelines for Evidence Collection and Archiving	http://www.ietf.org/rfc/rfc3227.txt

Sitios Web con Listas de Software Forense*

Tipo de software	Sitio Web	URL
Detección de Intrusos y Sistemas de Prevención	Honeypots.net	http://www.honeypots.net/ids/products/
Sniffers y Analizadores de Protocolos	Packet Storm	http://packetstormsecurity.org/defense/sniff/
Analizadores de Protocolos	Softpedia	http://www.softpedia.com/get/Network-Tools/Protocol-Analyzers-Sniffers/
Varias Herramientas para Análisis de Estaciones de Trabajo y de Redes	Forensic and Incident Response Environment (F.I.R.E.)	http://fire.dmzs.com/?section=tools
	Foundstone	http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/freetools.htm
	Freshmeat	http://freshmeat.net/search/?q=forensic&section=projects
	Helix	http://www.e-fense.com/helix/
	Open Source Digital Forensics Analysis Tool Categories	http://www.opensourceforensics.org/tools/categories.html
	Penguin Sleuth Kit	http://www.linux-forensics.com/forensics/pensleuth.html
	Talisker Security Wizardry Portal	http://www.networkintrusion.co.uk/
	The Sleuth Kit	http://www.sleuthkit.org/sleuthkit/tools.php
	The Ultimate Collection of Forensic Software (TUCOFS)	http://www.tucofs.com/tucofs.htm
	Top 75 Security Tools	http://www.insecure.org/tools.html
	Trinux	http://trinux.sourceforge.net/
Varias Herramientas para Análisis de Estaciones de Trabajo	Checksum Tools	http://lists.thedatalist.com/pages/Checksum_Tools.htm
	Computer Forensics Tools, Software, Utilities	http://www.forensix.org/tools/
	Funduc Software	http://www.funduc.com/
Varias Herramientas para Análisis de Redes	Common Vulnerabilities and Exposures (CVE)	http://www.cve.mitre.org/compatible/product.html

* Las aplicaciones que se muestran en esta tabla no es de ningún modo una lista completa de aplicaciones para el uso de propósitos forenses, ni se asegura ninguna confirmación de ciertos productos