UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN

EL FUNCIONAMIENTO DE LOS DISCOS DUROS, MEMORIAS USB Y CÓMO TRABAJAN LAS HERRAMIENTAS DE INFORMÁTICA FORENSE EN LA RECUPERACIÓN DE DATOS EN ESTOS DISPOSITIVOS

TESIS PROFESIONAL
QUE PARA OBTENER EL TÍTULO DE:
LICENCIADO EN INFORMÁTICA
PRESENTA:

ALEJANDRO HAMUD FUENTES

ASESOR:
L. A. E. Y M. A. JESUS ROMERO ESTRADA

AGOSTO 2010

Agradecimientos

Quiero dedicar esta tesis a mis padres y hermana a quienes no tengo manera de agradecer todo lo que han hecho por mí, los llevo conmigo siempre.

Agradezco a mis familiares que también han sido parte de mi vida abuelos, tíos, primos y sobrinos.

Agradezco a mis amigos por su apoyo y lealtad a mi persona.

Agradezco a los profesores que encaminaron mi desarrollo a lo largo de mi trayectoria escolar.

Agradezco a la UNAM por haberme dado la oportunidad de desarrollarme y crecer profesionalmente dentro de sus aulas.

Considero que no debo dar gracias a quienes han sido parte de mi vida, he aprendido que dar gracias solo debe de hacerse cuando hay un favor de por medio y todos los que han sido parte de mi vida no lo han hecho por hacerme un favor. Las personas que realmente me han apoyado lo hacen sin pedir nada a cambio.

Titulo

El funcionamiento de los discos duros, memorias USB y cómo trabajan las herramientas de informática forense en la recuperación de datos en éstos dispositivos.

Índice.

Introducción

La velocidad con que la Informática avanza en nuestros días ha provocado que surjan distintos medios de almacenamiento, no es ahora concebible trabajar con tarjetas perforadas, cintas de papel perforado, cintas magnéticas o disquetes cuando se dispone de otros medios magnéticos para estos fines.

Es común ahora disponer de herramientas para el almacenamiento externo denominas “Memorias Flash” o más comúnmente conocidas como USB (Universal Serial Bus) por sus siglas en Inglés, cuyas capacidades varían acordes a las necesidades de los usuarios.

Sin embargo, tal facilidad para almacenar, llevar y traer información nos ha puesto en gran riesgo, primeramente de que la información pueda ser sustraída sin ninguna dificultad; segundo punto: tal y como se dice en el argot informático “Las memorias auxiliares no tienen palabra de honor”, esto es, que en cualquier momento se puede limitar o perder el acceso a los datos que en ellas se hayan almacenado y como tercer observación, existe el riesgo de contaminación por tal diversidad de usuarios que accedan nuestros sistemas electrónicos.

Está situación nos pone en gran riesgo, obligando a establecer mayores controles respecto al uso de los “USB’S” y el trato que se deberá dar a los HDD (Hard Disk Drive) discos duros o a las memorias auxiliares referidas para recuperar los datos, y evitar infecciones por virus informáticos.

El presente trabajo, tiene como finalidad anticipar estos problemas, pero a su vez ayudar al usuario a recuperar los datos que en ocasiones se piensan “perdidos” al momento de dañarse o contaminarse involuntariamente. Para tal efecto se están proponiendo las hipótesis siguientes:

Hipótesis

Hipótesis nula:

Es importante e indispensable para el usuario informático y aun el profano conocer los componentes que integran los HDD, las memorias USB y la manera en que trabajan.

El personal relacionado con Informática deberá conocer y dominar algunas técnicas desde el enfoque del Hardware y del Software que se utilizan para rescatar archivos que fueron borrados por error, por formateo del dispositivo o por falla física del mismo.

Hipótesis alternativa:

No se tiene consecuencia alguna el desconocimiento de cómo funcionan las memorias ya sean HDD o USB en el proceso electrónico de datos y control de los mismos.

Contenido

- *Dispositivos*

Los discos duros, sus componentes, características y funcionamiento.

- El HDD.
- Los componentes lo integran.
- La interacción de los componentes para lograr su función.

Las memorias USB, sus componentes, características y funcionamiento.

- Memorias USB.
- Los componentes las integran.
- Funcionamiento.

- *Técnicas de recuperación de información*

Recuperación de información con Software.

Recuperación de información a nivel Hardware.

Análisis de fundamentos

Hoy en día el uso de dispositivos de almacenamiento masivo se ha vuelto literalmente parte de nuestra vida diaria y generalmente no lo notamos. El problema surge cuando los dispositivos fallan de manera lógica o física y dichos errores pueden ser generados por el usuario o por algún mal funcionamiento de los componentes internos del dispositivo.

Es desagradable saber que la información que se tiene alojada en alguna memoria USB o en el HDD, por algún error; sea de sistema operativo, error físico o falla generada por el usuario, provoque la perdida de información. Es en este momento donde se deben aplicar ciertos métodos para la recuperación de información.

Explicar el funcionamiento de los dispositivos de almacenamiento tanto internos como externos; en este caso HDD y USB facilitará el entendimiento de las herramientas a utilizar para la recuperación de datos contenidos en discos duros formateados por error, discos que generalmente se catalogan como “descompuestos” debido a que no funcionan como debieran y datos de memorias flash que se creen perdidos.

Capítulo I – Dispositivos

Los dispositivos son herramientas que nos han ayudado a simplificar la vida humana, es por ello que se han convertido en parte de la vida cotidiana de muchas personas sin importar el nivel social. Los dispositivos no son perfectos y por lo mismo presentan fallas o errores, nunca debemos confiar 100% de un dispositivo al almacenar información porque es vulnerable es por ello que hago recomendación de tener duplicados de información en diferentes dispositivos cuando se maneja información de alta importancia.

Esto se debe a que en momento de fallo de alguno de los dispositivos ya sea mecánico o a nivel software que pueda dañar la información que contiene, se cuente con más respaldos que faciliten el acceso a la misma.

En caso de no tener dichos respaldos se procede a intentar recuperar la información utilizando técnicas especializadas en la materia.

Discos duros

Los discos duros son dispositivos que nos permiten almacenar y recuperar grandes cantidades de información. Son partes esenciales de una computadora, y están catalogados dentro de la memoria secundaria de la computadora. Trabajan en conjunto con la memoria RAM siendo estas las 2 principales memorias en un sistema de cómputo.

Al momento de operar, la memoria RAM contiene los datos utilizados al instante por la computadora, pero se apoya del HDD para poder recuperar datos que pueda requerir posteriormente o que necesiten ser almacenados permanentemente, esta es la forma en la que trabajan.

Sin embargo tienen importantes diferencias: la memoria RAM es volátil, por lo que su contenido al apagar la computadora se pierde, pero son muy eficaces y eficientes por estar conformadas por componentes electrónicos. En cambio los HDD no son volátiles, son menos eficientes debido a trabajar mecánicamente pero su capacidad de almacenamiento es mucho mayor.

Características.

Al momento de analizar un disco físicamente se deben tener presentes ciertos aspectos que describen las capacidades de almacenamiento y funcionalidad del mismo, éstos son:

- Capacidad – Cantidad de Megabytes que puede almacenar, actualmente se manejan unidades de Gb (Gigabytes) y Tb (Terabytes).

- Tiempo de acceso – El tiempo de acceso es la latencia que tiene la aguja del disco duro para leer un sector del mismo.

- Velocidad de transferencia – Se refiere a la velocidad con la que se escriben, leen y borran datos del HDD, pero ésta depende también del SO (Sistema Operativo).

- Velocidad de rotación – Es la rapidez con la que gira el plato o disco dentro del disco, se mide en RPM (Revoluciones Por Minuto), las más utilizadas son 4’500, 5’400, 7’200, y 10’000 RPM.

- Caché de disco – Es un área reservada en el disco la cual almacena información. La forma en la que trabaja es almacenar una copia del documento original, también alojado en el disco duro, pero al ser grabado en la memoria caché el tiempo de acceso es más corto por lo tanto hace mucho más eficiente el funcionamiento del sistema operativo y físico.

Tipos de HDD

Existen actualmente 4 estándares principales, de discos duros IDE, SCSI, SAS y SATA.

- ***IDE (PATA)***

Integrated Device Electronics (Dispositivo con electrónica integrada), Parallel Advanced Technology Attachment (Tecnología Paralela Avanzada de Escritura), Es un conector estándar utilizado para discos duros y unidades ópticas comúnmente. Se caracteriza por tener 40 pines por los cuales viajan datos. Lo cual hace que la transferencia sea efectiva. Éste estándar se utilizaba en computadoras de escritorio, y se comenzó a utilizar en las primeras laptops.

- ***SCSI***

Small Computer System Interface (Sistema de Interfaz para Pequeñas Computadoras) es un conector estándar que normalmente se utiliza para servidores. Este conector tiene la peculiaridad de ser muy rápido debido a que utiliza 50 pines, pero para su configuración es necesario un drive externo para hacer uso del Software. No se puede utilizar si se conecta directamente. Éste tipo de conectores se emplea generalmente en servidores y algunas estaciones de trabajo.

- ***SAS***

Serial Attached SCSI (Sistema de Escritura Serial para Interfaz de Pequeñas Computadoras) es un estándar que se crea a partir del SCSI. Debido a esto incluye todas las ventajas que posee el SCSI.

- ***SATA***

Serial Advanced Technology Attachment (Tecnología Serial Avanzada de Escritura) actualmente la interfaz más utilizada en equipos de computación. Proporciona la opción de conectarse mediante un cable más largo que todos los tipos de disco y puede ser conectado o desconectado estando el equipo encendido sin problema alguno. La taza de transferencia es mucho más eficiente que el IDE (PATA) utilizando solo 7 pines. Éste tipo de conector es el que se utiliza actualmente tanto para computadoras de escritorio, laptops y servidores.

Estructura del HDD

Los HDD están conformados por una caja de aluminio, cerrada herméticamente, la que contiene partes que no pueden ser alteradas o intercambiadas por un usuario común. Estas piezas son los discos, las “agujas” o cabezales de lectura y escritura.

Los discos son también conocidos como platos y están fabricados de un material conformado por una gran cantidad de elementos que tienen la característica de ser cargados positiva o negativamente y tiene la capacidad de almacenar información por ambas caras. La forma en la que escribe o se magnetiza la superficie de estos discos es mediante las agujas que interpretan los valores binarios que caracterizan un BIT, siendo uno la carga positiva, y el cero la carga negativa.

Para que el HDD pueda trabajar es necesario que los platos giren, es por esto que se necesita de un motor que los haga girar y mantenga una velocidad constante.

Las “agujas” viajan sobre la superficie del disco, tienen un brazo mecánico que trabaja por magnetismo el cual hace que el cabezal se traslade a la posición que sea necesaria para interpretar o grabar datos. (Ver fig. 1).

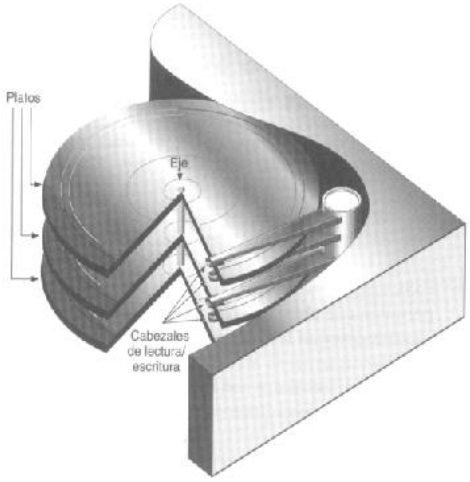


Fig. 1

Partes del HDD

- Discos

Los discos que integran el HDD están hechos con aluminio pulido y cubiertos por una capa de aleación metálica que tiene la cualidad de ser magnetizada. Estos discos se encuentran anclados en un eje que gira con la ayuda de un motor y por consecuencia mantiene a los discos girando a una velocidad constante. Los discos utilizan ambas caras generalmente para almacenar datos. (Ver fig. 2).

- Los cabezales

Se encuentran apilados y se encargan de la lectura y escritura de la información que contengan los discos. Algunos discos poseen dos cabezales de lectura en la misma cara del disco para agilizar la lectura y la escritura de datos. Se encuentran flotando en la superficie del disco para no rayarla, es por eso que los discos trabajan herméticamente cerrados, cualquier suciedad o impureza puede causar que la cabeza toque la superficie del disco y lo marque, dañando esa sección del disco. Las agujas trabajan gracias a una bobina de cobre que es movida por el campo magnético que genere por la corriente emitida por la circuitería del disco duro. (Ver fig. 2).

- El eje

Es el lugar en donde están anclados los platos y tiene la funcionalidad de girar para que las agujas puedan interpretar los datos almacenados magnéticamente en la superficie de cada cara de los platos. (Ver fig. 2).

- El actuador.

Es el encargado de dar impulso a la bobina de las agujas que transportan los cabezales en la superficie de los discos. Actúa por magnetismo y cuando se pierde este magnetismo por falta de energía eléctrica, las agujas son desplazadas al centro del plato para que no se corra el riesgo de rayar la superficie del disco, esto gracias a un resorte que las retrae. (Ver fig. 2).

- El circuito impreso.

Se encarga de llevar a cabo varias funciones para que se logre el funcionamiento del HDD. Tales funciones son:

  - Establece un control del flujo de información entre el procesador y el HDD.
  - Funge como codificador y decodificador de la información que va a ser almacenada en los platos del HDD
  - Se encarga del control de las revoluciones que debe mantener el motor que hace girar los platos.
  - Controla la cantidad de energía que se envía a la bobina que controla la posición de las agujas sobre la superficie de los platos para que éstas estén en la posición precisa para leer o escribir datos.
  - Efectúa una revisión de todos los elementos que integran al HDD y si alguna de ellas falla manda un informe.
  - Tiene un chip que funge como memoria caché, dependiendo del tamaño total del disco será la memoria, esto para agilizar la lectura y escritura de datos en el HDD.

Es por ello que la circuitería impresa que está presente con los HDD es tan importante, porque se encarga de administrar las funciones internas del mismo y la comunicación que existe entre el HDD y la tarjeta madre de la computadora.

Existen casos que ya no son necesarias debido a que están integradas en la tarjeta madre, pero existen todavía discos que requieren este tipo de tarjetas para poder funcionar, un ejemplo de esto son los discos que utilizan interfaz SCSI. (Ver fig. 2).

- Conexión del disco duro.

La conexión del disco duro se hace por medio de estándares, puede ser IDE o ATA, SCSI, SATA y SAS. Es la clavija que se encarga de transmitir los datos al HDD. (Ver fig. 2).

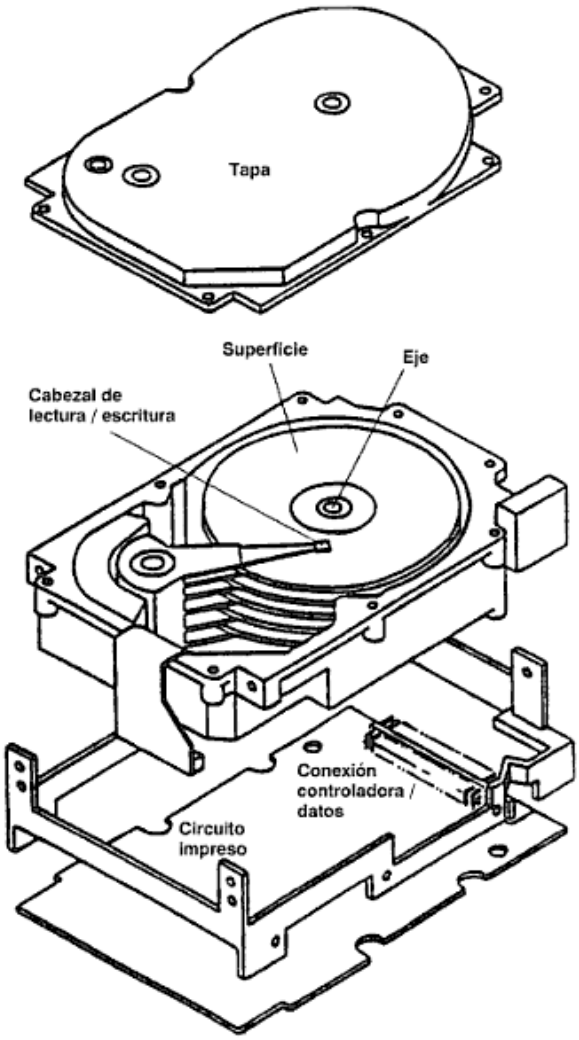


Fig. 2

Funcionamiento del HDD

El funcionamiento del HDD utiliza el principio de los discos de tornamesa; un disco, una aguja, un brazo que transporte esa aguja, y un medio por donde transmita la información, de dicha manera, el HDD compuesto por los platos magnéticos en donde se almacena la información, los cabezales para cada plato y el brazo mecánico que transporta esos cabezales por la superficie de todo el plato.

Para que los cabezales puedan tener acceso a todo el plato es necesario que éste gire de manera constante para esto, los HDD, utilizan un motor que mantiene ésta velocidad la cual se mide en RPM (Revoluciones por minuto).

Las funciones que se realizan al leer escribir o borrar datos, básicamente son: desplazar los cabezales de las “agujas”, hasta el lugar en donde se tenga que realizar cualquier operación.

Una vez que se encuentre el primer dato, o el indicador en donde se localice en el plato, realizará la lectura o escritura, dependiendo del cabezal.

Cada disco, como se ha visto se compone por 2 superficies, también conocidas como caras. Existen discos que solo utilizan un cabezal, pero generalmente se utilizan 2, uno para cada cara del disco. Cada cara de plato se divide en anillos concéntricos llamados pistas. En los discos duros se le conoce como cilindros, y estos cilindros se dividen a su vez en sectores de escritura. (Ver fig. 3).

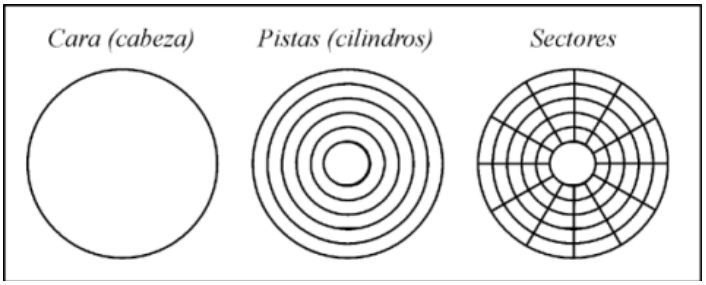


Fig. 3

Los sectores son las unidades mínimas de información que puede leer o escribir un disco duro y normalmente son 512 bytes los que pueden almacenar.

Las cabezas y cilindros comienzan a numerarse desde el cero y los sectores desde el uno. Es decir el primer sector del disco corresponde a la cabeza cero, cilindro cero y sector uno.

La manera en la que se graban los documentos en un sistema FAT (File Allocation Table), Tabla de Asignación de Archivos es la siguiente:

Cuando se hace una petición al SO ya sea de escritura, lectura o borrado de datos, manda una señal al disco duro para que lea la tabla de asignación de archivos y sepa en donde realizar la operación. Una vez que recibe la señal de lo que tiene que hacer, las agujas se transportan por la superficie del disco para saber en qué pista del disco se puede realizar la operación.

En el momento que las agujas o cabezales se encuentran en la pista que va a ser la elegida para realizar la operación, las agujas interpretan los sectores y verifican la información que se encuentra en ellos. Ya identificado el sector y la pista adecuada para la operación, se mandan pulsos eléctricos para que se pueda imantar la superficie del disco.

Cabe mencionar que un archivo completo es fragmentado en diferentes secciones del o de los platos que contenga el HD. Luego de hacer esta grabación se escribe en la tabla FAT la ruta o dirección de donde están almacenadas estas partes del archivo para que posteriormente se pueda tener acceso a ellas.

Sistemas de archivos comunes

Los sistemas de archivos son las estructuras que se encargan de la organización de datos que se graba en la unidad de almacenamiento para ser interpretada de manera textual o gráfica dependiendo el sistema operativo el cual utiliza un gestor de archivos para dicha tarea. Los sistemas de archivos más conocidos son:

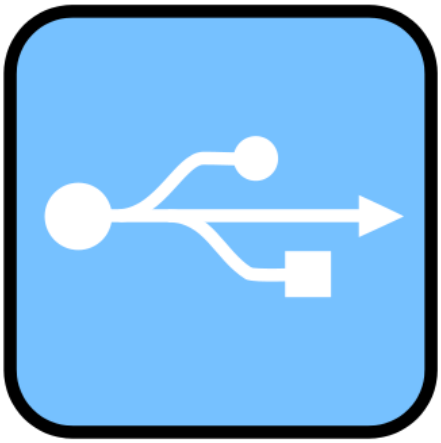
Características Particiones	**FAT 32**	**NTFS**	**EXT4**	**HFS**
Limitantes				
Tamaño máximo	2 TB	2 TB	2 TB	2 TB
Total de archivos	ilimitado	ilimitado	ilimitado	ilimitado
Tamaño máximo de archivos	4 Gb	Dependiendo el tamaño del disco	1 EiB	8 EiB
Número máximo de clústeres	268435456	ilimitado	ilimitado	ilimitado
Longitud máxima de nombre de un archivo	Arriba de 255 bytes	Arriba de 255 bytes	Arriba de 255 bytes	Arriba de 255 bytes
Características				
Codigos en nombres de archivos	Solo Sistema	Sistema y Unicode	Sistema y Unicode	Sistema y Unicode
Sector de boot	Primer sector	Primer y último sector	Primer y último sector	Primer y último sector
Compresión	NO	SI	SI	SI
Encriptación	NO	SI	SI	SI
Recuperación	NO	SI	SI	SI
Rendimiento	Alto en pequeños volúmenes. Alto en bajos volúmenes	Bajo en pequeños volúmenes. Alto en altos volúmenes.	Bajo en pequeños volúmenes. Alto en altos volúmenes.	ALTO EN AMBAS

USB

Las memorias que conocemos como USB, debido al conector o interfaz que utilizan para establecer comunicación con la computadora, emplean un chip capaz de almacenar datos a través de pulsos eléctricos. Dicho chip utiliza tecnología de las memorias flash la cual se basa en la estructura de la memoria EEPROM la que permite que varios sectores de la memoria sean escritos o borrados al mismo tiempo al permitir trabajar a velocidades rápidas para agilizar la manipulación de archivos. Las memorias se han convertido en la manera más práctica de almacenar y transportar datos.

Las memorias USB trabajan con 5 volts y 2.5 watts como máximo de energía haciendo que éstas sean vulnerables a cambios de energía.

Las memorias USB fueron desarrolladas por IBM en 1998 como un remplazo de disquetes en su línea de productos ThinkPad. Y aun siendo invento de IBM la patente fue adquirida por M-Systems quien fue la empresa que ayudó a IBM en el desarrollo de las USB y finalmente se apropió de ésta.



EEPROM

Se define como una memoria ROM la cual tiene la peculiaridad de poder ser programada para ser borrada y reutilizar su capacidad de manera eléctrica.

Esta memoria es un chip regrabable que almacena la información sin necesidad de tener una fuente de energía trabajando a la par. La manera en la que actúa es direccionando bits a una dirección registrada en la memoria. Esto es debido a que la memoria está integrada por bloques los cuales son almacenan la información y trabajan en una constante grabación y borrado de datos.

Los chips EEPROM se utilizan en circuitos con la finalidad de almacenar instrucciones y datos. Estos chips tienen una vida útil de 10 a 100 ciclos de escritura. Después de éste numero de ciclos la memoria deja de funcionar.

MEMORIA FLASH

La memoria flash es un tipo de memoria no volátil, se compone por un chip regrabable, basándose en la arquitectura de las memorias EEPROM, fue desarrollada por Toshiba y el nombre fue adoptado por la velocidad con la que se borraban y guardaban datos. Son utilizadas para guardar información, implementadas en las que generalmente se conocen como memoria USB, tarjetas de cámaras digitales.

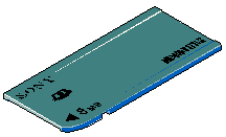
Algunas memorias conocidas que utilizan dicho tipo de chip son:

- Type II PC Card

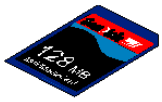
- Compact Flash

- SmartMedia

- Memory Stick



- MultiMediaCard



- RS-MMC

- SD Memory Card

- xD Picture Card

- MiniSD Card

SSD

Los SSD (Solid State Drive) o Dispositivos de estado sólido, son unidades físicas de almacenamiento que combinan la tecnología de las memorias flash para ser utilizadas como un dispositivo HHD. De esta manera los datos son almacenados en chips en lugar de los platos de un HHD. (Ver Fig. 4)

Fig 4.

Las ventajas conocidas de los SSD son:

- El sistema carga más rápido
- La velocidad de escritura, lectura y eliminado de datos es más rápida debido a los arreglos (RAIDS) contenidos.
- Baja latencia de lectura y escritura, cientos de veces más rápido que los discos mecánicos.
- Menor consumo de energía y producción de calor - Resultado de no tener elementos mecánicos.
- No emite ruido - La misma carencia de partes mecánicas los hace completamente inaudibles.
- Mejorado el tiempo medio entre fallos, superando 2 millones de horas, muy superior al de los discos duros.
- Implementa una mejor seguridad - permitiendo una muy rápida "limpieza" de los datos almacenados.
- El Rendimiento no se deteriora mientras el medio se llena.
- Menor peso y tamaño a mismas dimensiones.
- Resistente - Soporta caídas, golpes y vibraciones sin estropearse y sin descalibrarse
- Borrado más seguro e irrecuperable de Datos

Las desventajas conocidas son:

- Precios elevados.
- Menor recuperación - Después de un fallo mecánico los datos son completamente perdidos pues la celda es destruida, mientras que en un disco duro normal que sufre daño mecánico los datos son frecuentemente recuperables usando ayuda de expertos.
- Vulnerabilidad contra ciertos tipo de efectos - Incluyendo pérdida de energía abrupta (especialmente en los SSD basado en DRAM), campos magnéticos y cargas estáticas comparados con los discos duros normales (que almacenan los datos dentro de una Jaula de Faraday
- Capacidad - A día de hoy, tienen menor capacidad que la de un disco duro convencional el cual llega a superar los 2 Terabytes.

Capítulo II – Informática Forense.

Día con día se incrementan los ilícitos generados a partir del uso de tecnologías de información, éstos evolucionan a grado de ser más sofisticados e imperceptibles al momento de realizar un ataque, lo que conlleva a fraudes económicos mucho más grandes que los realizados comúnmente a mano armada.

Dicho de otra manera, los delincuentes encuentran y generan estrategias que les permitan proyectar sus acciones evitando procesos de investigación que logre asociarlos con hechos que los inculpen. Estas personas poseen perfiles de alguien que gusta de la tecnología, logrando con ello explotar sus habilidades provocando fraude, vulnerando derechos, garantías y aprovechándose del desconocimiento de éstas técnicas por parte de los ciudadanos en general.

Estudios realizados en Latinoamérica relacionados con el tema especifican:

-No existe una definición clara y concisa de perito informático.
-La formación que tienen estas personas no es especializada.
-No existe una ley que aplique específicamente en casos de ilícitos informáticos.
-La persona que se considera perito informático debe, aparte de tener conocimiento en el área de tecnologías de información, tener conocimiento de disciplinas jurídicas, criminalísticas y forenses.

Es por ello que resulta complejo dar seguimiento a un caso en el cual se haya cometido un fraude electrónico por llamarlo de cierta manera.

La Informática Forense.

La informática forense se encarga de dar seguimiento y solución a problemas tecnológicos relacionados con la seguridad informática y la protección de datos. Trabaja directamente con problemas de privacidad, fraude, hurto de información y espionaje industrial obtenidos con el uso indebido de las tecnologías de información que existen actualmente. La función que tiene es recopilar evidencias, analizarlas y presentar pruebas electrónicas que posteriormente se utilizarán en un proceso legal. De esta manera se garantizan las políticas de seguridad y la protección de información.

Una empresa al contratar los servicios que ofrece la informática forense no necesariamente tiene que ser para resolver algún ilícito, puede ser de manera preventiva para evitar vulnerabilidades anticipándose a ellas con pruebas que muestren dicha vulnerabilidad.

Las metodologías que utiliza son:

-Obtener los datos y evidencias desde distintos medios digitales.

-Los datos obtenidos no deben ser alterados al momento de recuperarlos.

-Se catalogan las fuentes de información para su análisis posterior y se documenta cada prueba aportada.

-Una vez obtenidas las evidencias, se debe elaborar un dictamen, claro, conciso, fundamentado y justificado.

El proceso debe efectuarse con la conciencia de los requerimientos legales vigentes, esto para no vulnerar ningún momento los derechos de terceros que puedan verse involucrados.

Actualmente la informática Forense se clasifica como una especialidad técnica el cual es un recurso importante que apoya las ciencias modernas de Forense, que es el conjunto de varias tareas. Entre ellas se encuentra la computación forense, forense de redes y forense digital.

- **La computación forense:**

Es una disciplina asociada con la evidencia la cual trata de descubrir e interpretar la información en los medios informáticos para establecer hechos y formular hipótesis relacionadas con el caso en cuestión haciendo un análisis de información en los equipos que se están analizando.

- **Forense en redes:**

En la rama de redes, es un poco más difícil debido a que se debe tener conocimiento de protocolos, configuraciones e infraestructuras de comunicación. Cómo es que éstas interactúan y de esta manera establecer rastros movimientos y acciones mal intencionadas generadas por intrusos con fines mal intencionados.

- **Forense digital:**

Es una manera de aplicación de conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, esto con el fin de ayudar en la aplicación de leyes a los delincuentes que las infringen con fraudes haciendo uso indebido de la Informática. Dichos fraudes son hechos por profesionales con bajos niveles de ética debido a que ejecutan una amplia gama de situaciones que una persona sin conocimiento pudiera realizar. Es por ello que las personas que realizan la informática forense deben ser profesionales y al contrario deben tener altos niveles de ética pues son ellos quienes respalden la información y la toma de decisiones que deban tomarse ante los hechos analizados.

Objetivos de la Informática forense

La informática forense utilizada de manera preventiva sirve para realizar auditorías de los mecanismos de protección utilizados en los sistemas detectando las vulnerabilidades que existen en los mismos con el fin de corregirlas.

Por otra parte, cuando ya ha sido vulnerada la seguridad, la informática forense permite analizar los rastros que quedan latentes y así averiguar lo que sucedió siguiendo las evidencias electrónicas de donde se originó el ataque. O las posibles alteraciones, manipulaciones, fugas o destrucciones de datos dentro de la empresa.

Para realizar un análisis de Informática forense se requiere un equipo de profesionales expertos en derecho de las Tecnologías de Información y expertos técnicos en metodología forense con el fin de garantizar el cumplimiento tanto de los requerimientos jurídicos como los técnicos derivados de la metodología.

La evidencia digital

Se define como cualquier tipo de información obtenida o escrita en algún medio informático. De esta manera la evidencia digital es un término que describe cualquier registro generado o almacenado en cualquier sistema de computación y así, ser utilizado como evidencia en un proceso que puede llegar a ser legal.
De esta manera la evidencia digital puede ser divida en tres categorías:

- Registros almacenados (correos, archivos de ofimática, imágenes).
- Registros generados por equipos de tecnología informática (registros de auditoría, registro de transacciones).
- Registros parcialmente generados y almacenados en los equipos (hojas de cálculo, bases de datos)

La evidencia digital como tal tiene ciertas características que se pueden interpretar como pros y contras dependiendo el punto de vista; estas características son:

- Es volátil.
- Es anónima.
- Es duplicable.
- Es alterable y modificable.
- Es eliminable.

Dichas características denotan la importancia y el seguimiento que se le debe dar en procedimientos, técnicas y herramientas que se utilizan para obtener, revisar, resguardar, analizar y presentar la evidencia presente en una escena del delito.
Por lo mismo se debe tener un conocimiento de las leyes aplicables a las pruebas así como las técnicas y los procesos que ayudan a mantener la confiabilidad de los datos recuperados.

Procedimientos

Teniendo en cuenta la vulnerabilidad del manejo de información en medios digitales se deben tener medidas de seguridad y control para tratar de adelantarse a los hechos y tener una prevención de cualquier falla que pueda existir, se describirán algunos de los procedimientos que deben ser considerados al momento de tratar con información digital:

1. Esterilidad en los medios de trabajo: Los medios de trabajo deben estar certificados, esto se refiere a que no hayan sido alterados magnética u ópticamente porque pueden contaminarse. Esto por ser de manera similar a la medicina forense, pues al estar contaminado puede provocar una mala interpretación o un análisis erróneo.

2. Verificación de las copias: Las copias de los medios esterilizados antes mencionados deben ser una copia fiel sin alteraciones. Esto se logra a partir de procedimientos matemáticos y algoritmos que comprueban la información. Dichos procedimientos se basan en las firmas digitales que comprueban la información del medio del que originalmente se extrae y al medio al que se destina.

3. Documentación de los procedimientos, herramientas y resultados: Al momento de aplicar las técnicas de recuperación, todas las herramientas utilizadas en el proceso. Es decir las versiones del Software utilizado, los medios y sus capacidades, las limitaciones que se tienen, etc. Para que cualquier persona externa tenga la documentación del proceso y aparte porque un tercero podría reproducir con esto los resultados.

4. Mantenimiento de la cadena de custodia: Siguiendo el punto 3 se debe registrar quien hace entrega de la evidencia, cuándo, el estado de la misma, la forma en que se transporta, quien ha tenido acceso a ella entre otras situaciones que sirven para tener una correcta administración de las pruebas.

5. Informe y presentación de resultados: Es importante debido a que la mala presentación de los resultados puede generar falsas expectativas o interpretación de los hechos. Se debe utilizar un lenguaje sin tecnicismos, la redacción no debe tener juicios de valor.

6. Administración del caso: En algún momento del juicio de la información los investigadores forenses pueden ser requeridos para dar un veredicto ante un juzgado, por ello se debe mantener un sistema automatizado de documentación de expedientes de los casos, con una adecuada cuota de seguridad y control con el fin de resguardar la información.

7. Auditoría de los procedimientos: Se debe realizar una auto evaluación de los procedimientos realizados con el objetivo de tener la evidencia de la práctica de investigación forense cumpliendo el ciclo PHVA (planear, hacer, verificar y actuar) para incrementar la confiabilidad de sus procedimientos y poder cuestionar las prácticas y técnicas utilizadas para mejorar el ejercicio profesional.

Hacking

Nace a partir de las vulnerabilidades que presentan los sistemas de información. Los hackers como tal son personas inconformes con lo establecido que buscan el talón de Aquiles de los sistemas de información y de esta manera saber las debilidades de los sistemas que los propios desarrolladores no conocen.

Si nos propusiéramos saber el porqué de los hackers debemos hacer referencia a las motivaciones de hacer cosas que otros no hacen. Podemos encontrar los términos cyberterrorista, phreaker, script kiddies, crackers, desarrollador de virus; los cuales tienen una motivación distinta.

- Cyberterrorista: es el calificativo más reciente y actual que se utiliza para categorizar a un atacante que crea un plan estratégico para recabar información de las redes de información las cuales le brindan la posibilidad de estar en todas partes y en ninguna a la vez ofreciéndole un anonimato y total imperceptibilidad ante los usuarios comunes. De esta manera genera inestabilidades en los sistemas, incertidumbre en las operaciones y fallas de comunicación lo que conlleva a la pérdida de control por parte del usuario en cuestión. Tienen actualmente una difusión en las organizaciones delincuenciales.

- Los phreakers: también conocidos como amantes del teléfono, son las personas que con base en los tonos telefónicos, las ondas hertzianas y los espacios electromagnéticos tienen la capacidad para distinguir los códigos que dichas señales llevan, traduciéndolos en números, indicaciones o llamadas. Tratan de lograr un mundo propio en donde las comunicaciones telefónicas no tengan costo alguno utilizando técnicas de sincronización y transmisión de información evadiendo dispositivos que rarifican y controlan el uso del canal de transmisión.

La idea de ellos es mostrarles a las compañías que los servicios que ofrecen no son competentes de acuerdo a las tarifas que cobran[1].

- Script Kiddies: son las personas que utilizan técnicas y herramientas que ya han sido creadas por hackers y/o phreakers con la finalidad de penetrar o vulnerar sistemas de comunicaciones o de tecnologías de información. El problema de ellos surge que por cuestiones de presunción pueden llegar a un punto en donde pierden el control de sus actos siendo éstos una amenaza latente.

- Crackers: hace referencia a las personas que se encargan de destruir, desestabilizar sistemas de información y comunicación. Tiene como objetivo vulnerar sistemas por venganza o por cuestiones económicas lo cual lo hace traspasar la línea de lo permitido y legal. Busca, estudia y analiza las debilidades de los sistemas para crear nuevas formas de vender sus servicios.

- Desarrolladores de virus: son personas que actúan por ego, retos, revanchas, dinero, frustraciones etcétera. Viviendo en un mundo de inconformidad, con el talento que poseen desean demostrar que existen nuevas y diferentes formas de pensar lo cual se ve traducido en los códigos maliciosos que generan los cuales han perjudicado a gran parte de los usuarios computacionales.

Generan estrategias de espionaje silencioso que les permite coleccionar información que les permite mantener una posición de ventaja ante cualquier persona u organización. No es inspirado por la tecnología y los desafíos que esta presenta, sino es controlado por ella y por sus posibilidades, es la diferencia que presenta con el hacker.

[1] El iPhone que se presumía de estar bloqueado para ser utilizado con AT&T fue liberado con apenas 2 días de su salida al mercado.

- Atacantes internos: son personas que laboran dentro de las empresas que tienen acceso a información confidencial y por su insatisfacción perjudican a la empresa dando mal uso a la información. Estas personas generalmente están limitados por sus conocimientos quebrantando su profesionalismo.

Rastros de ataques.

Para llevar a cabo el rastreo de objetos, lograr reconstrucciones de hechos es necesario generar un registro de eventos sucedidos por lo que se debe tener sincronización, control e integridad de los archivos. A esto se le conoce como “trazabilidad” que hace referencia a un concepto sistemático que establece relaciones y observaciones del sistema atacado utilizando los índices que deja el intruso en su ataque.

Para comenzar se debe tener previo conocimiento del sistema operativo con el que cuenta el afectado, sus políticas de seguridad, el sistema de archivos, los servicios que brinda, aplicaciones, trafico de la red y memoria RAM que se tenga. Todo esto debido a que en cada uno de ellos puede existir el rastro que permita identificar el origen del ataque.

Ataque a nivel S.O.

Los ataques que se hacen al sistema operativo y a sus estructuras lógicas son imperceptibles debido a que se alojan en la memoria o archivos temporales que se clasifican como volátiles. Por tanto entre más se tenga el riesgo de que el atacante se enfoque en el sistema operativo mayores serán los problemas que se presenta al momento de hacer el rastreo del intruso.

Ataque a nivel BD.

Cuando se tiene un ataque a nivel de base de datos los rastros se asocian con los diseños creados en el DBM; es decir que se debe configurar previamente un sistema de alertas sobre objetos que puedan afectar el funcionamiento de la BD. Esto mediante disparadores o *triggers* los cuales se ejecutan al momento de identificar alguna alteración de datos u objetos sensibles a la aplicación.

Ataque a nivel Redes.

Cuando se hace un ataque a nivel redes se utilizan sesiones TCP la cual tiene la función de coordinar múltiples conexiones concurrentes entre un par de hosts. La acción del TCP es identificar en una tabla los datos importantes del cliente (hablando de la maquina que hace la petición de conexión) y el servidor analizando el paquete TCP que contiene registrado:

- El puerto de origen y el puerto destino
- Un identificador de 32 bits que sirve para validar el flujo de datos de acuerdo a una serie de números que van del 0 al 232.
- Los datos que están siendo enviados.

Al realizar una sesión TCP se hace una sincronización entre cliente y el servidor conocida como “Three Way Handshake” en donde ambas máquinas hacen reconocimiento mutuo de la configuración para manejar sesiones de cada una.

- IP Spoofing.

  Hace referencia a la suplantación de dirección IP esto con el fin de generar un ataque al servidor haciendo una modificación al paquete TCP para que el servidor al momento de pedir acceso dé permiso debido a que se utilizará una dirección “segura” de acuerdo con las tablas de IP que guarda y a las que les permite tener acceso a él. Existen dos tipos de Spoofing:

  - Non-Blind – En donde el atacante se encuentra dentro de la subred del atacado lo cual permite visualizar al atacante el tráfico de información en la red.

  - Blind Spoofing – Es un ataque externo en donde los números de secuencia y confirmación no están al alcance del atacante.

El uso de esta técnica es seguro que los paquetes enviados por el atacante no son rechazados por el servidor debido a que se interpreta que la información proviene de una dirección segura.

- SYN Flood.

El TCP al establecer una conexión existe posibilidad de que quede el servidor en espera de respuesta del cliente pueda ser atacado. Al estar éste en escucha. Es ahí en donde se aprovecha para lograr una interrupción de conexión inundándolo de paquetes los cuales logran reducir la capacidad de respuesta haciendo lenta la conexión hasta suspender el servicio de una maquina. Trabaja en conjunto con el IP Spoofing de la maquina del atacante para evitar rastreos posteriores.

- Escaneo de puertos.

El escaneo de puertos es una técnica de reconocimiento para localizar servicios activados que se conocen como huecos de vulnerabilidad. Esto se logra enviando paquetes a cada puerto de la maquina, y si la respuesta es un SYN/ACK significa que hay disponibilidad, de lo contrario si devuelve un RST/ACK, no hay disponibilidad. Si la respuesta es ICMP significa que la maquina no está conectada a la red, y si devuelve un ICMP admin se refiere a que la máquina está detrás de un firewall con lista de accesos.

- Envenenamiento de ARP

El protocolo ARP (Address Resolution Protocol, *Protocolo de resolución de direcciones*) asocia las direcciones IP con las direcciones físicas MAC en una tabla dinámica. El proceso es sencillo, al enviar datos de una máquina que maneje ARP se hace una consulta a las tablas dinámicas para comparar las IP

que deben coincidir con la MAC. Para lograr un registro en la tabla se debe mandar un paquete en el cual se hace la petición del registro y al enviar la respuesta aceptando el registro se almacena automáticamente en la tabla la dirección IP y la MAC donde proviene el archivo de confirmación.

El ataque de envenenamiento de ARP se basa en la vulnerabilidad que presenta tanto Windows como Linux ya que no manejan estados de protocolo ARP, por lo cual aceptan mensajes ARP Reply, sin importar si se ha enviado un ARP Request aprovechando esa vulnerabilidad se modifica la tabla ARP de la victima dando acceso a la máquina que se quiera tener acceso.

- Sniffer

El Sniffer es un programa que se utiliza para monitorear el tráfico de datos dentro de una red, dando la posibilidad de observar los paquetes que viajan a través de ella. En una red sin switch o router todas las maquinas interconectadas reciben la información que está siendo enviada, pero no es mostrada hasta que dicha información encuentra la IP a la que va dirigida. Es así como el Sniffer establece la tarjeta de red de la maquina como receptor de todas la información que llegue a captar. De esta manera el atacante usa sniffers para observar el tráfico en la red que desea atacar, haciendo una recopilación de la información que requiera para obtener el beneficio que desee.

Existen diversas herramientas para lograr ataques por TCP, la mayoría son gratuitas, la gran mayoría solo funcionan en S.O. Linux, Algunas de ellas son:

- Juggernaut que sirve para rastrear secciones TCP utilizando un criterio de búsqueda actuando como sniffer, y armando paquetes desde cero siendo capaz de hacerlos con los encabezados que se deseen para pasar inadvertido en un ataque.

- TTY-Watcher que a diferencia del Juggernaut solamente puede utilizarse en maquinas que utilicen S.O. Solaris, esto porque en dicho sistema, todo lo que se teclea en la maquina es registrado en la terminal TTY del atacante permitiendo saber todos los comandos tecleados por la victima. También permite enviar mensajes a la terminal que está utilizando la víctima.

- DsSniff que son un conjunto de herramientas para la auditoría de redes y pruebas de penetración, sus funciones principales son monitorear las redes, interceptar paquetes que normalmente no están disponibles para sistemas sin sniffers.

- T-Sight es una herramienta comercial producida por y se utiliza para el S.O. Windows específicamente. Se creó originalmente para el monitoreo de tráfico sospechoso pero actualmente se utiliza para captar comunicaciones de un segmento de red en tiempo real y para realizar asaltos de sesión.

Recuperando Información: FAT y NTFS.

La información que cada usuario posee en su computadora personal es invaluable, es por ello que debe ser protegida, más cuando se trata de asuntos confidenciales. Debido a las posibilidades actuales, el borrar un archivo confidencial puede ser no seguro debido a que los archivos que creemos eliminados pueden ser recuperados. Existen métodos de borrados seguros pero aún no son procedimientos implementados; los archivos que son borrados que no pasan por este proceso pueden ser recuperados por Software dedicado a ésta tarea.

Los usuarios promedio tienen la idea de que una vez eliminados los datos de la papelera de reciclaje estos son irrecuperables, situación que no es verdad. Si se tiene un conocimiento suficiente del almacenamiento de la información puede ser recuperada con facilidad.

La información como tal se almacena en medios magnéticos, los cuales se clasifica en duros y blandos. Los medios duros requieren de campos magnéticos grandes para lograr un magnetismo permanente y de magnetismos intensos para revertir dicha magnetización y borrar los datos. A diferencia de los medios duros, los blandos requieren campos bajos para lograr la magnetización. Un ejemplo de medios blandos son los disquetes, conformados por un plástico delgado maleable recubierto con una capa de óxido.

En los medios magnéticos existe el deterioro, el cual se da de diferentes maneras, la manera más común es que las partículas que se encuentran en la capa magnética llegan a ser inestables perdiendo esa fidelidad por lo que se llegan a perder los datos.

Almacenamiento de la información:

La información que se almacena en los discos duros tiene que ser controlada por un sistema operativo que a su vez se basa en un sistema de archivos y éste tiene su propia forma de almacenamiento, lectura y borrado de datos.

Los sistemas de archivos contienen un índice, conocido como “tabla de archivos” que es la sección en donde se almacena la información que apunta a nuestro archivo, esto se refiere a que no se encuentra nuestro archivo almacenado, y si este es muy grande puede estar almacenado en varias partes del disco. Se hace de esta manera para que cada vez que se haga la petición del documento no se tenga que recorrer la superficie completa del disco y ahorrar tiempo leyendo la tabla que indica en que sector del disco se encuentra el documento.

Estructura FAT

El sistema FAT divide al disco en estructuras que cumplen distintas funciones, típicamente esta estructura tiene las siguientes partes:

Sector de inicio	Sector reservado (opcional)	Tabla 1 de localizacion de archivos	Tabla 2 de localizacion de archivos	Directorio raiz (unicamente FAT 12 y16)	Region de datos (para archivos y directorios)...(Hasta el fin de la particion o disco)

El sistema de archivos FAT se compone de 4 secciones diferentes:

1. Los sectores reservados del principio del disco denominado sector de booteo. En éste sector se aloja un conjunto de instrucciones pertenecientes al BIOS.

2. La sección FAT contiene dos tablas idénticas de la tabla de localización de archivos, esto para brindar una mayor confiabilidad, aunque la segunda es rara vez utilizada. Dichas secciones contienen un índice de los clústeres que utilizan los archivos y directorios alojados en él HDD.

3. La región del directorio raíz. Es una tabla de directorio que almacena información acerca de los archivos y directorios localizados en el directorio raíz. Esta región es utilizada solamente en FAT12 y FAT16 y significa que el directorio raíz tiene un tamaño máximo predeterminado en el momento de la creación de la partición. En cambio FAT 32 almacena el directorio raíz a lo largo de la región de datos con otros archivos y directorios, permitiendo a este directorio crecer sin ninguna restricción.

4. La región de datos es la sección en donde se almacenan los archivos y directorios los cuales tienen la posibilidad de ocupar el mayor espacio de la partición y pueden crecer mientras existan clústeres libres.

Estructura NTFS

Proporcionando desempeño, seguridad y confiabilidad la cual no existe en FAT. Posee una arquitectura especial la que utiliza un esquema que facilita la introducción de nuevas características, realizando un mínimo de cambios. El total de las estructuras que se utilizan para manejar la partición. En general todas las secciones en NTFS se consideran archivos, a excepción del sector de booteo que es responsable de cargar el sistema operativo como lo muestra a continuación:

Sector de arranque	Tabla maestra de archivos	Archivos del sistema	Area de archivos

1. El sector de arranque es fundamental y se encarga de manejar la información de arranque. Se conforma internamente por dos estructuras, el bloque de parámetros del BIOS y el código de arranque o bootstrap. El bloque de parámetros del BIOS contiene la información para identificar la partición como NTFS, saber el tamaño total del disco y de la partición y la información de donde se encuentran los archivos de meta data.

2. La MFT (Master File Table) es una tabla de base de dato relacional que contiene atributos para cada uno de los archivos que existen dentro de la partición.

3. Los archivos del sistema son todos los datos que integran al sistema operativo que se instale en esta partición.

4. El área de archivos es el área en donde se almacenarán los archivos que genere el usuario

Borrado y eliminado de datos

En FAT los registros almacenados en clústeres, ya sean archivos o archivos eliminados implican tres formas para poder borrar un archivo o un directorio completo.

La primera opción que tenemos es dejar los clústeres como libres, lo cual hace que el archivo se quede en disco pero no se pueda encontrar.

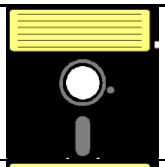
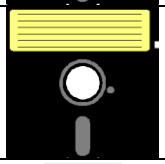
La segunda es borrarlo mandando el archivo o el directorio a la papelera de reciclaje, lo que está haciendo es enviar el archivo a una carpeta reservada por el sistema operativo.

La tercera es el borrado seguro que es eliminar un archivo totalmente, esto es sobrescribiendo el lugar físico en donde se encontraba el archivo.

Se debe recalcar que los sistemas de archivos son estructuras que manejan apuntadores para localizar archivos.

Al momento de eliminar los datos de un medio magnético se requiere una fuerza magnética alrededor de 5 veces la coercitividad del medio.

Medios Magnéticos.

Imágenes	Medio	Coercitividad
	Floppy 5 1/4 360K	300 Oe
	Floppy 5 1/4 1.2M	675 Oe
	Floppy 3 1/2 720K	300 Oe
	Floppy 3 1/2 1.44M	700 Oe
	Floppy 3 1/2 2.88M	750 Oe
	Floptical 3 1/2 21M	750 Oe
	HDD (1980's)	900-1.400 Oe
	HDD (1990's)	1.400-2.200 Oe
	Cinta magnética 1/2"	300 Oe
	QIC metálica 1/4"	550 Oe
	Cinta metálica 8mm	1.500 Oe
	Cinta metálica DAT	1.500 Oe

Metodologías para eliminar.

Las metodologías más utilizadas para eliminar datos fueron definidas por el Departamento de Defensa de Estados Unidos de América, cada método es aplicado dependiendo el tipo de disco. Los métodos son:

- Degaussing: Este proceso hace que el medio (el HDD) vuelva a tener su estado inicial de fabricación.

- Sobre escritura múltiple: Se ejecutan en el medio (el HDD) como sobre escribir los campos magnéticos de manera alternada, sobre escribir el medio con documentos basura, entre otras.

- Técnica de sobre escritura de Guttman: esta técnica especifica 35 diferentes métodos de sobre escritura y tiene como propósito evitar la recuperación de datos lo cual logra con éxito.

- Destrucción física: Se utilizan distintas herramientas para dañar los medios pero éstos presentan una sorprendente resistencia.

Borrado en FAT

Las tablas FAT se encuentran almacenadas como arreglos lineales de entradas, es decir, todos los datos que se almacenan van seguidos uno de otro. Cuando un archivo es borrado lo que se está haciendo es desvincular la tabla que direcciona al archivo con el mismo y se le agrega un carácter para identificar el espacio libre en el cual se puede almacenar posterior mente algo.

La acción de desvincular una tabla es interpretado por el sistema operativo como notificarle que el espacio que está libre puede ser escrito aunque el archivo esté presente físicamente, será reemplazado posteriormente por un nuevo archivo que se sobre escriba.

De modo que puede ser recuperado posteriormente con Software que esté diseñado para dicha tarea. Con esto se aclara que al momento de 'eliminar' algo de la papelera, la acción que se está haciendo realizando es solo borrar el apuntador que dirige al archivo por lo que el archivo sigue almacenado.

Esto deja en claro que para eliminar un archivo del FAT se requiere borrarlo y escribir sobre el área en donde dicho documento se encuentra alojado. Dicho proceso puede darse por voluntad de una persona o como consecuencia del borrado del mismo y posterior mente trabajar sobre el HDD, esto debido a que al momento de borrar el archivo el sistema operativo interpreta que ese espacio está libre y cualquier archivo generado posteriormente ocupará ese lugar físicamente.

Existe Software dedicado a la eliminación de archivos trabajando sobre direcciones de memoria o áreas en donde se encuentra alojado el archivo. Estos métodos son totalmente ajenos al sistema operativo y pueden llegar a eliminar archivos corruptos o dañados sin dejar rastro de ellos.

Para asegurar el eliminado correcto de los datos, los métodos de borrado de datos sugieren mínimo 27 escrituras sobre el área (Guttman).

Si llegan a aplicarse métodos más rápidos no se asegura la eliminación correcta de los datos. La Informática Forense sugiere que para un eliminado correcto de datos se debe hacer una escritura sobre esa área mínimo 35 veces.

Recuperación de información en FAT

En las primeras versiones de Windows se incluía en DOS Software para recuperación, después de Windows 95 en la que apareció la papelera de reciclaje, se creía que un archivo después de eliminado de ésta era irrecuperable.

Actualmente se cuenta con Software que permite recuperar dichos archivos el cual actúa analizando el HHD para encontrar los valores que indican que son archivos borrados, de esta manera se encuentran las áreas que han sido borradas. De esta misma forma se pueden encontrar inconsistencias sobre el tamaño o dirección del clúster de los archivos, lo cual demuestra que un archivo pudo ser eliminado para ocultar un posible rastro de alguna transacción que pudo ser ilícita.

Al recuperar la información se puede complicar un poco dependiendo del estado del sistema de archivos, esto está en función de la fragmentación en la que se encuentre el HDD y la utilización que tenga. Si se encuentra muy fragmentado y es muy utilizado, existe la posibilidad de que un nuevo archivo ocupe uno de los clústeres que pertenece al archivo que se quiere rescatar y por lo mismo se complica la tarea de recuperación.

El procedimiento que se sigue para recuperar los datos es: Primero buscar en el Root Directory el registro de datos que se tenga para encontrar el archivo eliminado. Estos archivos se pueden localizar rápidamente debido a que el primer carácter del nombre del archivo ha sido remplazado por E5h. Luego hay que cambiar este carácter por el original. Posteriormente hay que buscar el clúster lógico, en la partición FAT, que se refiere al valor que se encuentra en el campo Clúster Number, del registro y cambiarlo con uno de los siguientes criterios:

- Si el tamaño del archivo es menor al tamaño del clúster se coloca un clúster lógico que puede ser FF7-FFF ó FFF7-FFFF.

- Si el tamaño del archivo es mayor que el del clúster, se tiene que calcular el número de clúster que ocupa. En teoría el siguiente clúster lógico debe ser parte del archivo. Al clúster lógico se le coloca el valor del siguiente clúster disponible y así hasta completar el número de clúster requerido. Esto es válido cuando el disco no esté muy fragmentado, porque si lo está es posible que se encadene mal el archivo y se corrompa el mismo.

Recuperación de información en NTFS

NTFS trabaja bajo un sistema de archivos basado en transacciones por lo cual ciertas acciones se pueden recuperar utilizando las funciones del sistema de archivos. Por otra parte, tiene la capacidad de recuperar información posterior a un error crítico en el sistema de archivos; no permite operaciones a medio terminar, pero una vez terminadas las operaciones esta puede deshacerse.

En NTFS existe la manera de recuperar datos automáticamente, lo cual es conocido como recuperación de 3 pasadas la que tiene aplicación cuando el log de persistencia se queda una transacción inconclusa con lo que se pueden generar errores de coherencia en el sistema de archivos.

Las acciones que se realizan en el proceso de 3 pasadas son:

- Analizar el log de persistencia para identificar los sectores que necesitan corrección.

- Rehacer todas las transacciones desde el último punto de control conocido que haya estado funcionando correctamente.

- Deshacer las transacciones generadas posteriores al último punto.

Cabe mencionar que los puntos de control se realizan cada 8 segundos y se registran en un log de persistencia.

Nada garantiza que la información no se pierda. Esto es, si una transacción no se completa y el sistema tiene un fallo, la transacción será pérdida y por causa de la naturaleza del sistema de archivos, el usuario no notará cambios debido a que no se efectuará la modificación por haber quedado inconclusa.

Similar a FAT, el archivo enviado a la papelera o eliminado directamente, dependiendo de la configuración del sistema, este es enviado a una carpeta especial (en el caso de la papelera) y si es eliminado ya sea de la papelera o directamente lo que está sucediendo es que el sistema de archivos va al a MTF y localiza el registro del archivo para eliminar el apuntador a éste. Quedando de esta manera disponible el espacio que ocupa el archivo además de dejar un registro en el log de persistencia.

En NTFS es más complicado aplicar el proceso de eliminar datos, esto debido a su estructura superior que FAT por lo cual se recomienda que al borrar un documento la manera de recuperarlo es escribir nuevamente sobre el área que ocupaba dicho documento para reemplazar la información.

Como método de seguridad NTFS provee sistemas de auditoría y detección de intrusos en donde se almacena un registro de sucesos como el borrado de archivos.

Después de un tiempo el diario de operaciones o log de persistencia de las transacciones desaparece y es cuando se requiere de Software dedicado a la recuperación de datos, el cual busca primero en la MTF los registros de borrado, luego busca el bloque de datos en donde se encuentre el archivo, pudiendo encontrarlo debido a que se localiza entre los clústeres que se encuentran disponibles, recuperando el archivo en cuestión.

Estos clústeres disponibles se van agrupando a medida que se vayan liberando y se van utilizando conforme aumente la cantidad de información almacenada. La búsqueda de archivos eliminados en NTFS es posible al buscarse atributos que se tengan en común y a diferencia de FAT en NTFS los archivos eliminados poseen un campo de encabezado conformado por 2 bytes los cuales definen el estado del archivo importándonos en este caso el primer byte que se encarga de definir si el archivo se encuentra en uso o ha sido eliminado.

Al haberse encontrado el registro del documento eliminado, se debe hacer un encadenamiento de clústeres hasta recuperar el archivo. Esto se logra haciendo una búsqueda clúster por clúster para alcanzar el tamaño del archivo que es indicado por el mismo atributo.

Al encadenar los clústeres se recurre a un archivo llamado DATA que se encuentra encriptado el cual posee la información de los clústeres en donde se deben buscar los datos del archivo, posteriormente se encadenan los datos para reconstruir el archivo.

Capítulo III – Caso práctico.

Para detallar esta sección se utiliza el programa Ontrack EasyRecovery. Con el se muestra la manera en la que se pueden rescatar datos de una memoria flash.

Teniendo una memoria a la cual le hemos borrado los datos y suponiendo que fue por error se pondrá a prueba el software utilizado. Se elige la memoria por ser un dispositivo de más rápido acceso que un HD, en el caso de utilizar uno de estos se requiere más tiempo para permitir que sea analizada la superficie o superficies de los platos que contenga el HD.

Ontrack Easy Recovery Professional V6.1

Es un software de recuperación de datos que brinda soluciones a usuarios comunes con el fin de que puedan recuperar información que eliminaron por error o por algún tercero.

Existen un gran número de casos en los que se pierde información (fotos, documentos familiares, documentos del trabajo, información privada y muchas cosas más. Por ello la tecnología con la que cuenta el software provee al usuario la capacidad de recuperar información que se cree perdida y puede ser recuperada en la mayoría de los casos.

Al momento de recuperar la información se debe tener en cuenta algunos factores como, que es lo que se quiere recuperar, que valor tienen esos archivos y el tiempo que se requiere para dedicarse a la recuperación de datos.

El programa

Muestra una interfaz bastante amigable y fácil de utilizar, en la cual con tan solo unos clics y un poco de paciencia será fácil lograr el cometido. En el caso de recuperar los datos que hemos perdido se debe seleccionar la opción recuperación de datos. (Ver fig. 5)

Fig. 5.

Es un software bastante poderoso y robusto, el cual cuenta con varias operaciones que pueden ser útiles al momento de analizar discos, memorias flash o cualquier dispositivo de almacenamiento que esté en comunicación con el S.O.

Diagnostico de disco.

Fig. 6.

Esta herramienta permite hacer un análisis del funcionamiento del HD. Esto para conocer si existen errores de coherencia, errores físicos, la capacidad del disco, conocer los sistemas de archivos que se encuentran en él, crear un disquete de booteo con opciones de análisis de la unidad y un acceso a un software para tener un monitoreo del funcionamiento del disco. (Ver fig.6)

Recuperación de datos.

En este apartado tenemos las opciones de recuperación avanzada, recuperar posterior al formateo, retomar la recuperación, recuperar archivos eliminados, recuperación en bruto y un acceso para crear un disquete o un CD de arranque para recuperar datos. (Ver fig.7)

Fig. 7.

La recuperación avanzada nos muestra el nombre de las unidades que tenemos conectadas, el tamaño de dicha unidad, cuanto espacio tiene ocupado, el sector inicial y final de escritura, el sistema de archivos que utiliza y opciones avanzadas de búsqueda en donde podremos elegir desde que sector deseamos comenzar el análisis. (Ver. Fig. 8)

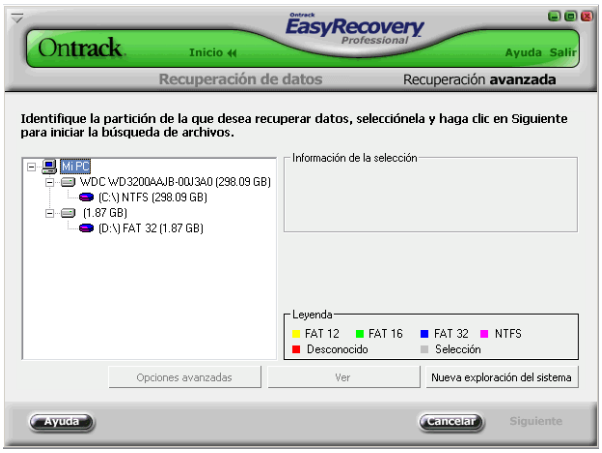


Fig. 8.

La recuperación posterior al formateo hace un análisis (Ver fig.10) de toda la unidad y muestra una lista (Ver fig. 11) de los documentos que lee y los organiza por el tipo de archivo que logra recuperar.(Ver fig. 9)

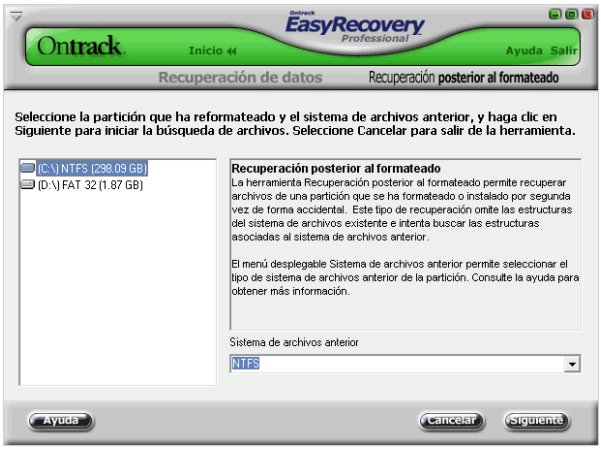


Fig. 9.

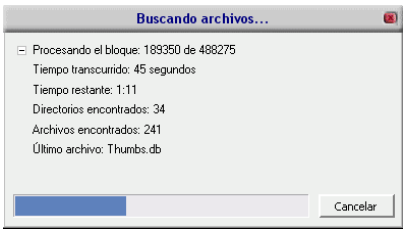


Fig.10.

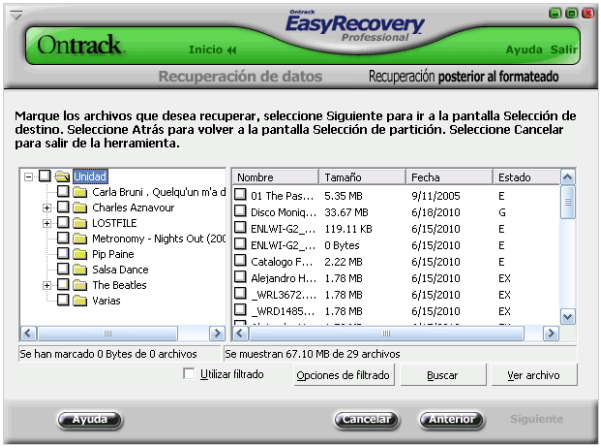


Fig.11.

Retomar la recuperación es una opción que da el programa para continuar recuperando archivos, esto sucede cuando se está haciendo una recuperación y se decide pausarla, automáticamente el programa sugiere generar un archivo que guarda el registro del último clúster que revisó para posteriormente continuar con la recuperación, esto es útil cuando son dispositivos con gran tamaño debido a que entre más capacidad tenga es más tardado el proceso, por esto se tiene la opción de continuar más tarde generando un archivo.

Recuperar archivos eliminados sirve para hacer una búsqueda de archivos más específicos, ayuda cuando conocemos el nombre del archivo o el tipo de archivo que se desea buscar seleccionando el dispositivo en el que se desea realizar la búsqueda. (Ver. Fig.12)

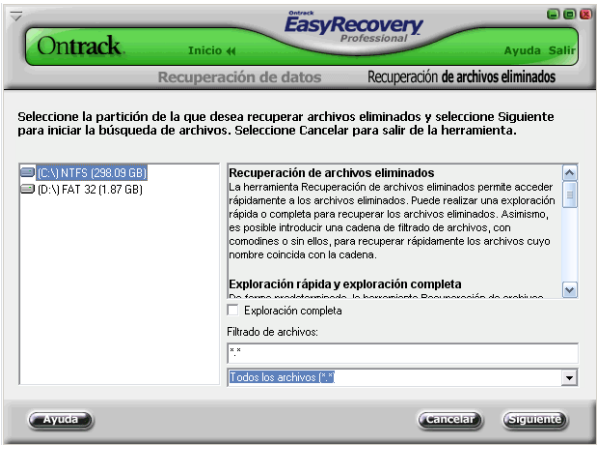


Fig. 12.

La recuperación en bruto hace una recuperación de todos los archivos que encuentre en el HD, para esto necesita tener otro HD del mismo tamaño o uno más grande que esté vacío para poder escribir tal cual la información que reconozca del HD por recuperar. (Ver fig.13)

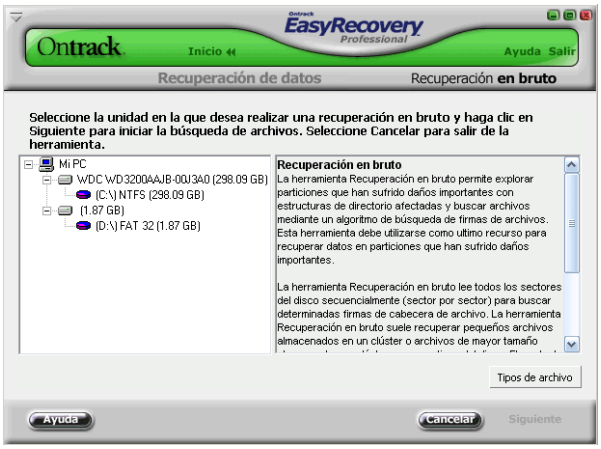


Fig. 13.

Emergency Media da la opción de crear un CD o un disquete booteable para arrancar una máquina y poder recuperar los datos sin necesidad de entrar al sistema operativo. (Ver. Fig.14)

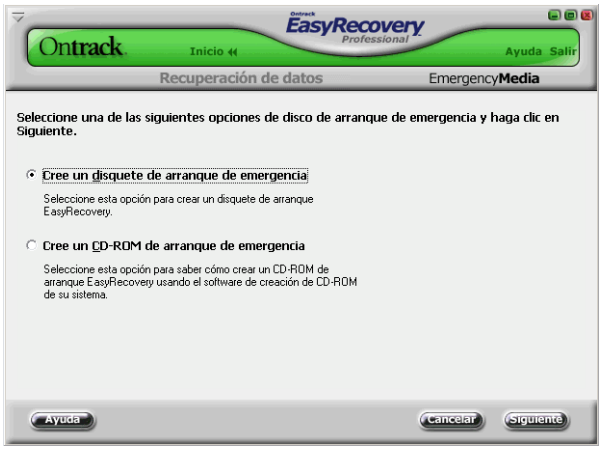


Fig. 14.

Recuperación de archivos y correo electrónico.

Esta sección es útil para reparar incoherencias en los archivos que se hayan recuperado, Access, Excel, Word, Power Point y Zip. (Ver Fig. 15) En la sección de correo electrónico se pueden reparar incoherencias de archivos

Fig. 15

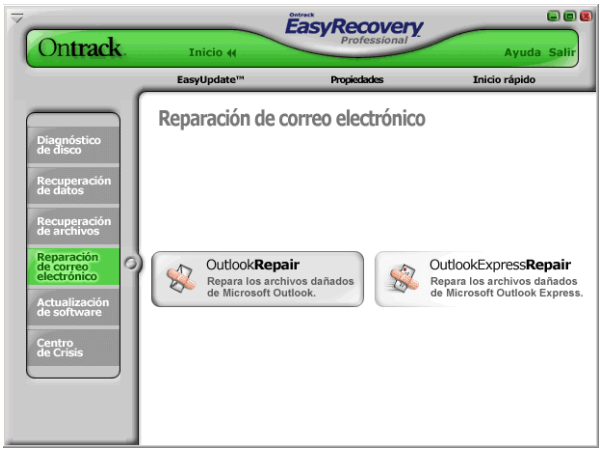


Fig. 16

Actualización de software y centro de crisis

La actualización de software permite actualizar la versión del software a la más reciente y ver los nuevos productos que ofrece Ontrack, y el centro de crisis brinda información de los sitios web y los teléfonos a donde llamar para poder recibir soporte técnico sobre el programa.

Fig. 17

Fig. 18

Conclusiones

Al dar a conocer el mecanismo y funcionamiento de las partes que integran los dispositivos de almacenamiento se comprende más sencillamente el porqué se puede recuperar información después de creerse eliminada.

En Informática Forense se conoce la manera en la que los ataques por medio de la Internet logran efectuarse; las agresiones que consiguen lograrse por vulnerabilidades que los usuarios desconocen al ser estas muy comunes y realizadas por varias técnicas logradas por personas que buscan vulnerabilidad en los sistemas operativos (Hackers).

Al explicar la manera en la que trabajan los dos sistemas de archivos más utilizados por sistemas operativos Windows (FAT y NTFS) se comprende su funcionamiento y como trabajan así como la manera en la que almacenan la información, por lo que se advierte cómo se desempeña el software dedicado a la recuperación de información.

Por último se mencionan las características que presenta un software dedicado a la restauración de información que resulta útil para los usuarios comunes dado que hay veces que se requiere recuperar información eliminada por error o por algún ataque externo, o involuntariamente.

Bibliografía y consultas electrónicas

Biblioteca de Ingeniería Eléctrica y Electrónica – Ecuador. http://bieec.epn.edu.ec [Consulta: 04 de mayo del 2010]

DURAN RODRIGUEZ, Luis. El gran libro del PC Interno. México D.F.: Alfaomega Grupo Editor, S.A. 2007. ISBN 978-970-15-1247-0

CANO MARTINEZ, Jeimi J. Computación forense. Descubriendo los rastros informáticos, Primera Edición. México, Alfaomega Grupo Editor, S.A. de C.V. 2009

CANO, J. (2005), Estado del arte del peritaje informático en Latinoamérica. Comunidad Alfa-Redi.- http://www.alfa-redi.com/ar-dnt-documento.shtml?x=728. [Consulta:14 junio- 2010]

FURNELL, S. (2002) Cybercrime. Vandalizing the information society. Adison Wesley

La excepción de la red – Argentina. http://www.alegsa.com.ar [Consulta:23 enero-2010]

Microsoft – España http://www.microsoft.com/business/smb/es-es/legal/forensic.mspx [Consulta 26 Abril-2010]

Ontrack – Estados Unidos de América http://www.ontrackdatarecovery.com/index.aspx [Consulta 26 Abril-2010]

Glosario

BIT – (Binary Digit) Unidad mínima de almacenamiento en una computadora.

BIOS – (Basic Input Output System) Sistema básico de entrada y salida.

BOOT – Se refiere al arranque de la computadora.

DBM – (Data Base Manager) Manejador de base de datos.

EEPROM – (Electrically-Erasable Programmable Read-Only Memory) Memoria de lectura y escritura programable para ser borrada electrónicamente.

FAT – (File Allocation Table) Tabla de asignación de archivos.

Formateo – Se refiere a la acción de eliminar del dispositivo de almacenamiento la información que este contenga, al permitir disponer de la capacidad total del mismo.

HDD – (Hard Disk) Disco duro.

Host – También conocido como servidor, es la computadora que está permanentemente conectada a Internet el cual brinda alojamiento de datos.

IDE – (Integrated Device Electronics) “Dispositivo integrado de componentes electrónicos”

MAC – (Media Access Control) Control de acceso de datos, se refiere a la dirección física de un dispositivo que establezca la comunicación en la red.

MTF – (Master File Table) Tabla maestra de archivos.

NTFS – (New Technology File System) Nueva tecnología de sistemas de archivos.

Oe – (Oesterd) Unidad con la que se cuantifica la intensidad de un campo magnético.

Periférico – Dispositivo, ya sea de entrada o salida, que se conecta a la computadora para cumplir con una tarea específica para la cual haya sido diseñado.

Pin – (Palabra inglesa que significa “Clavija”) Terminal metálica conductora que sirve como contacto entre componentes.

RAID – (Redundant Array of Independent Disks) *Arreglo de redundancia de datos en discos independientes.* Hace referencia a un arreglo de discos conectados a la máquina que trabajan simultáneamente dependiendo el nivel de RAID que se utilice.

RAM– (Random Access Memory) o Memoria de Acceso Aleatorio, es un dispositivo indispensable de una computadora el cual tiene como función alojar operaciones de manera volátil, refiriéndose a que en cuanto la máquina se apaga o se ejecuta una nueva operación en la máquina se pierde la información que contienen y se utiliza para una nueva información.

ROM – (Read Only Memory) Memoria de solo lectura.

Root Directory – Directorio raíz de datos.

SATA – (Serial Advanced Technology Attachment) “Tecnología Serial Avanzada de Escritura”

SO - Sistema Operativo.

SSD - (Solid State Drive) Dispositivo en estado sólido.

TCP – (Transmission Control Protocol) Protocolo de control de transmisión.

USB- (Universal Serial Bus) Bus Universal en Serie, es un puerto que tiene como propósito estandarizar la manera de conectar equipos periféricos a la computadora.