Curso de Recuperación de Datos

Profesor: Federico Sebastián Alcoba

Duración del curso: 3 meses.

Objetivos:

Al terminar el curso los alumnos/as estarán en condiciones de:

-Conocer y aplicar los conceptos, de las técnicas de Identificación y recuperación de datos.
-Desarrollar prácticas de recolección de datos conociendo una amplia gama de herramientas.
-Analizar y reparar discos duros dañados, memorias usb y micro sd.
-arreglar sistemas operativos dañados.

Introducción:

La recuperación de datos es una práctica que se encuentra en relación con múltiples disciplinas, y conocimientos, como ser:

La programación, La ingeniería informática, La seguridad informática , Ingeniería de Sistemas de Telecomunicaciones, El análisis de redes , La electrónica, Reparación de computadoras y periféricos externos, el manejo de hardware y software especializado, conocimientos de software libre etc.

La recuperación de datos posee un importante protagonismo en la resolución de situaciones de la vida cotidiana, como ser la perdida accidental de datos personales, debido a fallas de hardware o software, al igual que es de gran importancia en la resolución de crímenes o situaciones más complejas.

Por ejemplo:

Ciberdelitos contra el Estado
Litigios civiles en los casos de divorcio y acoso.
Evidencia de malversación de fondos.
Fraude o robo de propiedad intelectual.
Evidencias de discriminación por edad, sexo, raza o por despidos injustificados.
Investigaciones de compañías de seguros
Homicidios culposos
Casos relacionados con seguros y reclamaciones.
Invasiones a sistemas informáticos empresariales.
Ciberdelitos contra las personas
Ciberterrorismo
Fraudes de contabilidad.
Robos de identidad etc.

Como ya dijimos, los datos obtenidos a partir de un examen digital pueden ser útiles en una amplia gama de situaciones.

"La recuperación de datos basa sus fundamentos operacionales en las leyes de la física, de la electricidad y el electromagnetismo.
Gracias a los cuales la información se puede producir, transmitir, almacenar, leer e incluso recuperar cuando se creía eliminada, o completamente destruida."

En este curso se utilizará una forma de Aprendizaje con una doble vertiente, la descriptiva en el sentido informático al hablar de software y hardware, utilizando conceptos típicamente usados en otras aéreas que están en profundo contacto con la recuperación de datos, como ser la seguridad informática y la informática forense.

El otro aspecto es el práctico, que nos pondrá en contacto con los materiales de trabajo, aprenderemos aquellos detalles del oficio que no están escritos en ningún manual, los cuales solo se aprenden haciendo.

La examinacion digital se perfila como una de las profesiones más solicitadas tanto en el ámbito empresarial y privado así como judicial.
Todo medio tecnológico que haya sido utilizado para transmitir recibir o almacenar información de cualquier clase, puede ser examinada a nivel digital, por lo que se incluyen en tal estudio, los siguientes dispositivos:

Disco duro de una Computadora o Servidor
Teléfonos celulares.
Memorias micro sd.
Sistema de Telecomunicaciones
MAC address
Logs de seguridad.
Información de Firewalls
IP, redes Proxy. lmhost, host, Crossover,
Credenciales de autentificación
Trazo de paquetes de red.
Teléfono Móvil o Celular, parte de la telefonía celular,
Agendas Electrónicas (PDA)
Dispositivos de GPS.
Impresora
Memoria USB
Bios

El desarrollo de algunas de estas herramientas gratuitas de recuperación, surgió gracias al gran número de usuarios de computadoras personales que con frecuencia pierden sus datos debido a accidentes o errores en su manejo.
La creación de algunos programas de recuperación de datos emergieron en el contexto de un área muy especializada, "La informática forense".

La cual tiene diferentes nombres según el país al que pertenezca, se le llama, **computación forense, cómputo forense**, **informática forense**, **exanimación forense digital o análisis forense digital** etc.

Software de Recuperación:

Los inicios de la recuperación de datos:
Sus orígenes se remontan a los Estados unidos a mediados de 1980. Respondiendo al crecimiento de crímenes relacionados con las computadoras, los Estados Unidos comenzaron a desarrollar programas de adiestramiento y a construir su propia infraestructura para ocuparse del problema.

Estas iniciativas derivaron en la creación de centros capacitados como SEARCH, Federal Law Enforcement Center (FLETC), y el National White Collar Crime Center (NW3C).

En 1985 se crea el FBI Magnetic Media Program, que más tarde pasará a ser el Computer Analysis and Response Team (CART).

En 1990, el Laboratorio de Inspección Postal de los Estados Unidos se traslada a una nueva instalación en Dulles, Virginia, y entre 1996 y 1997 establece una unidad de
Informática Forense. Trabajan junto con el FBI durante muchos años, en el desarrollo de sus habilidades en informática forense.

En 1993 se celebra la primera conferencia anual sobre evidencias de computadoras

En 1994, el juicio de O.J. Simpson expuso muchas de las debilidades de la Investigación criminal y la ciencia forense. La investigación fue entorpecida desde el
inicio con colecciones de evidencias, documentación y preservación de la escena del
crimen incompletas.
Esta crisis motivó a muchos laboratorios y agencias de investigación a revisar sus procedimientos, mejorar su entrenamiento y hacer otros cambios para evitar situaciones similares en el futuro.
Por esa época hubo muchos desarrollos notables hacia la estandarización en este campo. Se fundó la Organización Internacional de Evidencias de Computadoras a mediados de los años 90, que anunció :

“asegurar la armonización de métodos y prácticas entre naciones y garantizar el uso de evidencias digitales de un estado en las cortes de otro estado”.

En España se crea en 1995 la Brigada de Investigación Tecnológica, perteneciente al Cuerpo Nacional de Policía.
En 1997, los países del G8 declararon que “la policía debe estar adiestrada para hacer frente a delitos de alta tecnología” en el Comunicado de Moscú de diciembre.

En Marzo del año siguiente, el G8 designa al IOCE para crear principios internacionales para los procedimientos relacionados con la evidencia digital.
Ese mismo año se crea el Grupo de Delincuencia Informática de la Guardia Civil, que pasó a llamarse Grupo de Investigación de Delitos de Alta Tecnología antes de tomar su nombre actual de Grupo de Delitos Telemáticos.

Los directores del Laboratorio Federal de Crímen en Washington, DC, se reunieron dos veces en 1998 para discutir asuntos de interés mutuo. Se formó lo que es ahora conocido como el Scientific Working Group Digital Evidence (SWGDE). El concepto de encontrar "evidencias latentes en una computadora" se pasó a llamar informática forense.
El concepto de evidencia digital, que incluye audio y video digital se llevó ante los directores del laboratorio federal el 2 de Marzo de 1998, en un encuentro albergado por el Servicio de Inspección Postal de los Estados Unidos y la División de Servicios Técnicos. La primera discusión se centraba principalmente en la fotografía digital.
El resultado de esa reunión fue que se necesitaba personal experto para abordar el tema, por lo que e1 2 de Mayo de ese año se reunieron de nuevo con expertos del FBI y de otros grupos especializados en el tema.
De ese encuentro surgió la formación de otro Grupo de trabajo técnico para tratar los asuntos relacionados con la evidencia digital.

El 17 de Junio de 1998, el SWGDE celebra su primer encuentro, dirigido por Mark Pollitt, agente especial del FBI y Carrie Morgan Whitcomb, del departamento forense del Servicio de Inspección Postal de los Estados Unidos. Como laboratorios forenses invitados estuvieron los del Departamento de Alcohol, Tabaco y Armas de Fuego(ATF), el Departamento de Control de Drogas(DEA), Inmigración(INS), Hacienda(IRS), la NASA, los Servicios Secretos(USSS) y el servicio de Inspección Postal. Decidieron algunos procedimientos administrativos y desarrollaron documentos relevantes.
Se establece que "La evidencia digital es cualquier información de valor probatorio que es almacenada o transmitida en formato binario". Más tarde "binario" cambió a "digital".
La evidencia digital incluye hardware, audio, video, teléfonos móviles, impresoras, etc. Ese mismo año se celebra el primer Simpósium de ciencia forense de la INTERPOL.

En 1999, la carga de casos del FBI CART excede los 2000 casos, habiendo examinado 17 terabytes de datos. El IOCE presenta un borrador con estándares sobre
informática forense al G8.

En el año 2000 se establece el primer laboratorio de informática forense regional del FBI.The FBI Laboratory Seal

En 2001, se realizó el primer taller de investigación forense digital -Digital Forensics Research Work Shop (www.dfrws.org)-, reuniendo a los expertos de

universidades, militares y el sector privado para discutir los retos principales y buscar las necesidades de este campo.
Este taller también impulsó una idea propuesta muchos años atrás, provocando la creación de la revista Publicación Internacional de Evidencias Digitales - International Journal of Digital Evidence (www.ijde.org)-.

El rápido desarrollo de la tecnología y los crímenes relacionados con computadoras crean la necesidad de especialización:
- "First Responders" (Técnicos de escena de crimen digital): expertos en recogida de datos de una escena del crimen. Deberían tener entrenamiento básico en manejo de evidencias y documentación, así como en reconstrucción básica del crimen para ayudarles a ubicar todas las fuentes posibles de evidencias.

- Analistas de Evidencias Digitales: procesan la evidencia adquirida por los anteriores para extraer todos los datos posibles sobre la investigación.
- Investigadores digitales: analizan todas las evidencias presentadas por los dos anteriores para construir un caso y presentarlo ante los encargados de tomar las decisiones.

Estas especializaciones no están limitadas solamente a los agentes de la ley y se han desarrollado también en el mundo empresarial. Aún cuando una sola persona sea responsable de recopilar, procesar y analizar las evidencias digitales, es útil considerar estas tareas por separado.
Cada área de especialización requiere diferentes habilidades y procedimientos; tratándolos por separado hace más fácil definir el adiestramiento y los estándares en cada área.
Entendiendo la necesidad de estandarización, en 2002, el Scientific Working Group for Digital Evidence (SWGDE) publicó unas líneas generales para el adiestramiento y buenas prácticas. Como resultado de estos esfuerzos, la American Society of Crime Laboratory Directors (ASCLD) propuso requerimientos para los analistas forenses de evidencias digitales en los laboratorios.

Hay además algunos intentos de establecer estándares internacionales (ISO 17025; ENFSI 2003).
En 2004 los Servicios de Ciencias Forenses del Reino Unido planearon desarrollar un registro de expertos calificados, incluyendo la Red Europea de Institutos de Ciencias Forenses, donde se publicaron líneas básicas para investigadores digitales.
Además, Elsevier comenzó la publicación de una nueva revista llamada "Digital Investigation: The International Journal of Digital Forensics and Incident Response" . Investigación Forense: el diario internacional de forenses digitales y de respuesta a incidentes. (http://www.compseconline.com/digitalinvestigation/).

A comienzos del 2005 se celebra el Reto Rediris v2.0, junto con la Universidad Autónoma de México. Se presentaron casi 1000 participantes y los premios fueron cursos de análisis forense y licencias de software.
A mediados del 2006 se celebra el III Reto Rediris, en el cual había 3 premios para los mejores de España y 3 para los mejores de Iberoamérica.

El análisis forense de computadoras es una ciencia relativamente nueva, por lo que aún no hay estándares aceptados.
No hay una única herramienta que lo haga todo, de modo que cumplir con los objetivos específicos de cada recuperación, va a necesitar la utilización de diferentes herramientas de software. tanto de pago como gratuitas, y de acuerdo al nivel de minuciosidad tomará mas o menos tiempo.
Así también la cantidad de datos a procesar ser algo a tener en cuenta en el examen digital, junto con la capacidad de la computadora que se utiliza para tal fin.
como se puede apreciar en cada caso habrá muchas variables a tener en cuenta, y numerosos detalles a ser considerados.

Breve historia de la Evolución del disco duro.

El disco duro es el dispositivo principal de almacenamiento de cualquier PC. Su característica principal es que es una memoria no volátil, es decir, no pierde datos aunque no esté alimentada por corriente eléctrica. En este artículo vamos a dar un repaso por los hechos principales que le han ocurrido a lo largo de la historia.

1956. Aparece la computadora IBM 350 junto a ella, el disco duro RAMAC I, que era capaz de almacenar cinco millones de palabras de seis bits, es decir 3.75 megabytes.

Pesaba una tonelada y era tan grande como un armario de dos puertas. Su precio rondaba los $10.000 el megabyte.

1961. IBM crea el primer disco que utiliza cabezas lectoras sin rozamiento. Hasta esta fecha las cabezas tocaban los platos con el peligro que esto conllevaba en caso de que hubiera algún tipo de movimiento.

1963. Primer disco extraíble, era tan grande como una lavadora y podía almacenar dos megabytes.

1973. Aparece el disco IBM Winchester que es el gran precursor de los discos duros modernos. Entre otras características que ofrece es que esta sellado, y sus cabezas lectoras son muy pequeñas.

1976. Dataram comercializa el primer disco SSD.

1978. Se patenta la tecnología RAID muy usada en la actualidad sobre todo en entornos servidores.

1979. Seagate, lanza el ST506, que puede almacenar hasta 5 MB se incluye en los primeros microcomputadores precursores de lo que hoy conocemos por PCs.

1980. IBM crea el primer disco duro de 1 GB es tan grande como una nevera y cuesta $40.000.

1980. Seagate crea el primer disco duro de 5 y 1/4.

1984. Western digital crea el primer disco duro para el IMB PC/AT.

1985. Aparece el estándar IDE creado por Control Data, Compaq Computer y Western Digital.

1985. Imprimis crea el primer disco duro con la placa integrada ya no es necesario tener una placa adicional sobre la placa base.

1986. Aparece el SCSI.

1988. Prairie Tek lanza el 220, el primer disco de 2.5 pulgadas que será usado en los portátiles.

1988. Connor introduce el disco de una pulgada de alto y 3.5 de ancho que es el más usado hasta la fecha.

1992. Seagate introduce el primer disco duro con protección para golpes. Durante años los discos duros habían tenido muchos problemas con las cabezas.

1992. Seagate lanza el primer disco de 7200 rpm un barracuda de 2.1 GB.

1994. Se crea el estándar EIDE que consigue romper la barrera de los 528 MB y puede ser usado para unidades ópticas o de cinta.

1996. Seagate introduce los primeros discos que funcionan a 10.000 rpm, con la familia Cheetah

2000. Seagate introduce los primeros discos que funcionan a 15.000 rpm, con el Cheetah X15.

2002. Otro primer puesto para Seagate, la aparición del primer disco duro SATA.

2005. Toshiba introduce el primer disco duro usando grabación magnética perpendicular que le permite tener 40GB en un solo plato.

2006. Seagate crea el primer disco de grabación magnética perpendicular para portátiles llegando a 160GB.

2007. Aparece el primer disco duro de un terabyte lo crea Hitachi.

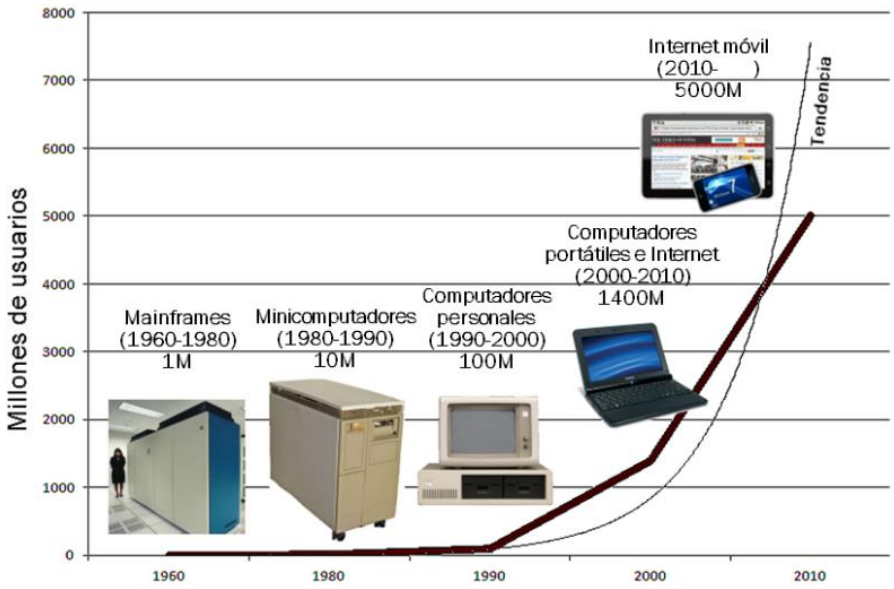
2009. Primer disco duro de dos terabyte lo crea Western Digital.

2010. Aparece el primer disco de tres terabyte, lo crean Seagate y Western Digital.

2011. Aparece el primer disco de cuatro terabyte, lo crea Seagate.

En la actualidad existen incluso modelos de hasta 10 terabyte y aumentando.

En la siguiente Imagen se puede percibir la reducción en el tamaño y el aumento de cantidad de información que es posible de ser almacenada, la Ley de Moore se mantuvo constante en el desarrollo de esta tecnología de almacenamiento junto con el desarrollo gradual de las computadoras modernas.



EVOLUCIÓN DE LA TECNOLOGIA

Antes de la década de los 60 sólo organismos gubernamentales y de investigación y grandes multinacionales podían contar con sistemas informáticos.

- En la década de los 60 y de los 70, los mainframes ya eran comunes en las grandes empresas y se estima que había 1 millón de usuarios en todo el mundo, en su mayoría técnicos.

- Los minicomputadores aparecieron en la década de los 80, estaban al alcance de muchas más empresas y centros universitarios, dando paso a muchos nuevos usuarios que alcanzábamos los 10 millones.
- En la década de los 90, los computadores personales, de la década anterior, llegaron masivamente a las pequeñas empresas y a los hogares, alcanzándose los 100 millones de usuarios.
- En la 1ª década del tercer milenio, los computadores portátiles e internet permitieron alcanzar una cifra estimada de 1.400 millones de usuarios, una cifra que representa del orden de un 20% de la población mundial.
- Durante esta 2ª década, gracias a los dispositivos móviles con acceso a internet, lo que se está denominando internet móvil las previsiones de [Morgan Stanley; 2009] son alcanzar los 5.000 millones de usuarios.

Combinando la evolución tecnológica con el crecimiento del volumen de usuarios, incluso en los escenarios de previsión más conservadores, el análisis digital será cada vez más habitual.

Dispositivos de memoria:

El Disco duro es un dispositivo no volátil, que conserva la información aun con la perdida de energía, que emplea un sistema de grabación magnética digital, en el interior existen una serie de discos con una capa de material magnetizable que giran a gran velocidad.

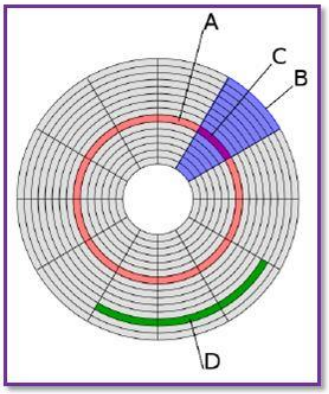
Sobre los discos se sitúan los cabezales encargados de leer o escribir los impulsos magnéticos.

Existen diferentes estándares para comunicar un disco duro con la computadora, las interfaces más usadas son integrados electrónicos (IDE también llamado ata) ,

SCSI generalmente usado en servidores, sata, este ultimo estandarizado en el año 2004 y FC usado exclusivamente en servidores.

Un disco duro al ser fabricado no se puede utilizar para ser leído y escrito por un sistema operativo, primero debe ser aplicado un formato de bajo nivel y aplicarle una o más particiones según la preferencia de cada uno.

Y luego se le debe dar un formato que pueda ser interpretado por el sistema operativo

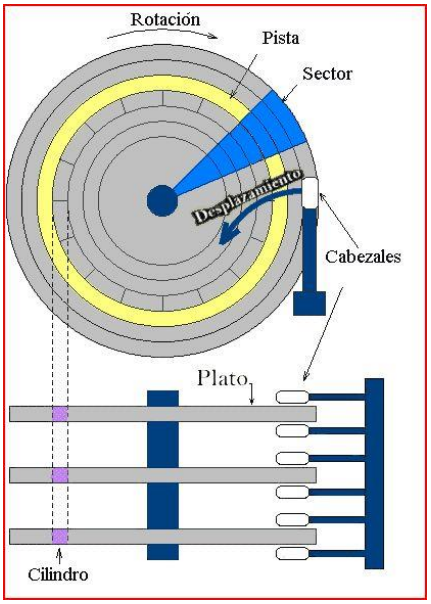


A: PISTA

B: SECTOR

C: SECTOR DE UNA PISTA

D: CLUSTERS



Estructura: dentro de un disco duro hay uno o varios platos (2 o 4) incluso pueden haber hasta 6 o 7 fabricados de aluminio o cristal los cuales giran a gran velocidad.

El cabezal (dispositivo de lectura y escritura) es un conjunto de brazos alineados verticalmente que se mueven hacia dentro o fuera según convenga, todos a la vez.

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.

Estructura lógica;

Dentro del disco se encuentran: el máster–boot record (en el sector de arranque) que contiene la tabla de particiones.

Las particiones necesarias para poder colocar los sistemas de archivos.

Direccionamiento: Hay varios conceptos para referirse a zonas del disco

Plato: cada uno de los discos que hay dentro del disco duro

Cara: cada uno de los lados de un plato.

Cabeza: contiene el número de cabezales.

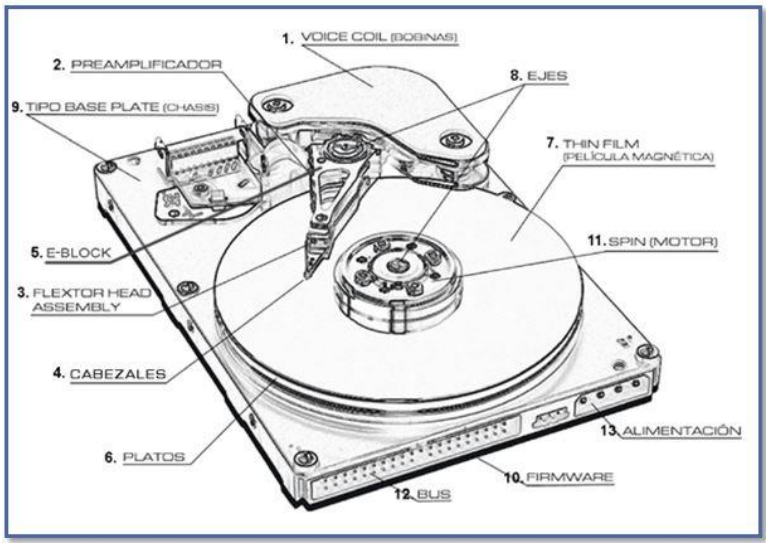
Pista: una circunferencia dentro de una cara, la pista esta en el borde exterior.

Cilindro: conjunto de varias pistas, son todas las circunferencias que están alineadas, verticalmente, una de cada cara.

Sector: cada una de las divisiones de una pista, el tamaño del sector no es fijo, siendo el estándar actual 512 bytes.

Antes el número de sectores por pista era fijo, lo que desaprovechaba el espacio, ya que en las pistas exteriores pueden almacenarse más sectores que en las interiores.

Así apareció la tecnología ZBR, grabación por bits por zonas, que aumenta el número de sectores en las pistas exteriores, y usa más eficazmente el disco duro.



Funcionamiento mecánico:

Un disco duro suele tener:

.Platos en donde se graban los datos

.Cabezal de lectura y escritura.

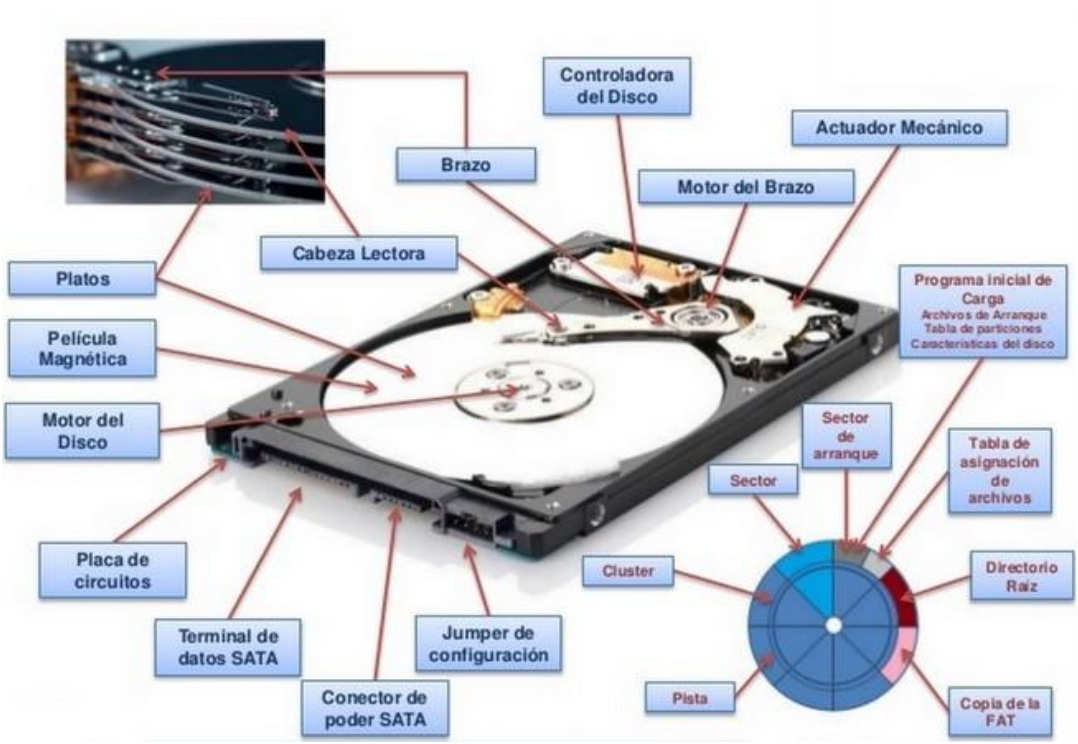
.Motor que hace girar los platos.

.Electroimán que mueve el cabezal como parte del actuador Mecánico.

.Circuito electrónico de control, que incluye una interfaz con la computadora y memoria caché.

.Bolsita desecante (gel de sílice) para evitar la humedad.

.Armazón de aluminio con tapa de acero ajustada con tornillos Allen para proteger los discos y también incluye un pequeño filtro de aire integrado en el armazón.



Características del disco duro:

Las características que se deben tener en cuenta en un disco duro son:

a) Tiempo medio de acceso: tiempo que tarda la aguja en posicionarse en la pista y el sector deseado, es la suma del tiempo medio de búsqueda (situarse en la pista).

b) Tiempo de lectura/escritura: tiempo medio que tarda el disco en leer y escribir nueva información. Depende de la cantidad de información que se quiere leer y escribir, el tamaño de bloque, el número de cabezales, el tiempo por vuelta y la cantidad de sectores por pista.

c) Latencia media: tiempo que tarda la aguja en situarse en el sector deseado, es la mitad del tiempo empleado en una rotación, completa del disco.

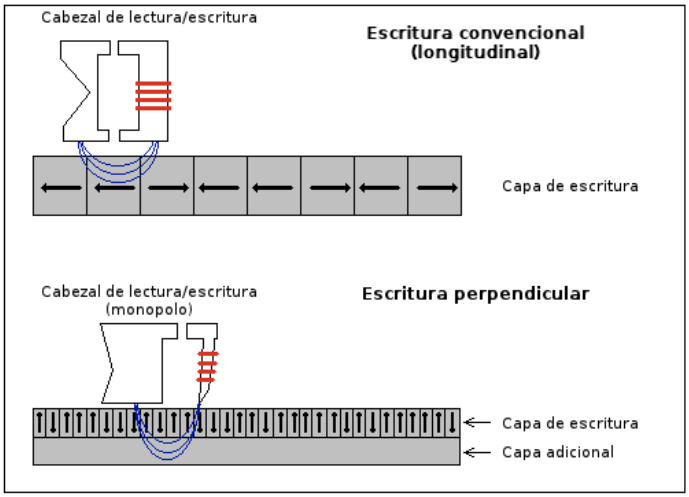
d) Velocidad de rotación: Revoluciones por minuto de los platos, a mayor velocidad de rotación menor latencia media.

e) Tasa de transferencia: velocidad a la que puede transferir la información, a la computadora una vez que la aguja está situada en la pista y sector correctos, puede ser velocidad sostenida o de pico.

De la arquitectura longitudinal a la perpendicular

En la constante carrera por hacer cada vez discos duros con más capacidad se supo que la tecnología de grabación longitudinal tenía un límite físico debido al llamado

"efecto superparamagnético" y que éste era de 100 a 200GB por pulgada cuadrada. Es por eso que ya se está utilizando en algunos modelos la tecnología PMR (Grabación Magnética Perpendicular), la cual tiene en teoría diez veces la densidad de almacenamiento que la longitudinal (hasta 1TB por pulgada cuadrada), lo que a la postre alargará en varios años más la vida del disco magnético.



Del PATA al SATA

El caso de las interfaces que se utilizan en un PC común y corriente hoy en día en bien particular, si bien una es muy superior a la otra, aún conviven sanamente en la mayoría de los computadores de escritorio actuales y algunos laptops también, ya sea por un disco duro antiguo o debido a algún dispositivo de lectura/escritura óptico como un grabador de DVDs. Así es, estamos hablando de la tecnología PATA (Parallel Advanced Technology Attachment) y la tecnología SATA (Serial ATA).

La tecnología PATA y sus dispositivos, también conocidos como dispositivos IDE, ha ido evolucionando junto con el disco duro. El ATA original de los '80 soportaba una transferencia total de 8,3MB/s, lo que era bastante para la época. ATA-2 increíblemente dobló esa cifra a un máximo de 16.6MB/s. Posteriormente llegó Ultra ATA y Ultra DMA-33 (Direct Memory Access) con 33MB/s, hasta el Ultra DMA-133 con 133MB/s, también conocidos simplemente como Ultra ATA-33 y Ultra ATA-133, pasando por Ultra ATA-66 y Ultra ATA-100.

Cuando el Ultra ATA-133 quedó obsoleto por el cuello de botella que significaba, se diseñó SATA. Actualmente SATA existe en tres sabores, SATAI, SATAII y SATAIII: 150MB/s, 300MB/s y 600MB/s respectivamente.

Tipo de conexión:

Si hablamos de discos duros podemos citar los distintos tipos de conexión que poseen los mismos con la placa madre, es decir pueden ser SAT,IDE,SCSI O SAS.

IDE: Integrated Device Electronics o ATA (Advanced Technology Attachment Packet Interface).

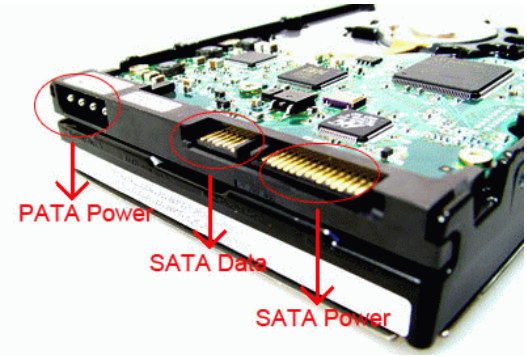
SCSI. Son discos duros de gran capacidad de almacenamiento, Se presentan bajo 3 especificaciones: SCSI Estandard, SCSI rápido y SCSI ancho-rápido.

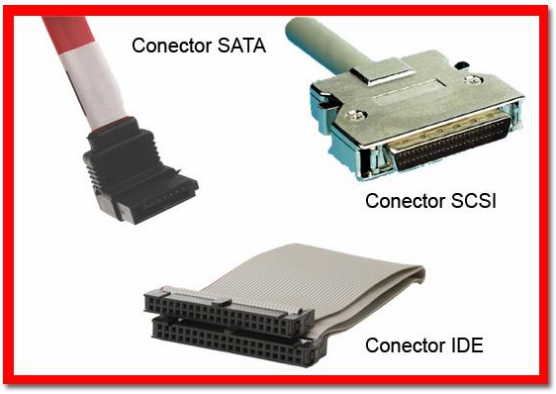
El tiempo medio de acceso puede llegar a 7 mseg y su velocidad de transmisión secuencial de información puede alcanzar teóricamente a los 5 Mbytes por segundo en los discos Estándar, los 10 Mbytes por segundo en los discos SCSI rapidos y los 20 Mbytes por segundo en los discos SCSI anchos-rapidos.(SCSI 2)

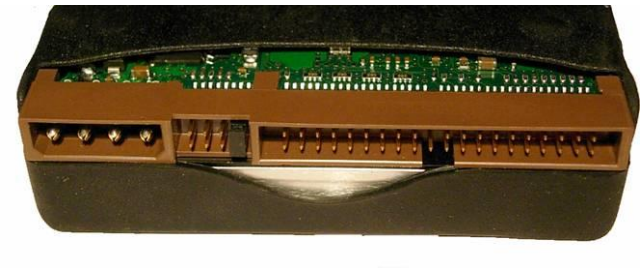
SATA: (serial ATA), nuevo estándar de conexión que utiliza un bus serie para la transmisión de datos.

Notablemente más rápido y eficaz que el disco IDE, en la actualidad hay 2 versiones SATA 1 con una velocidad de 1,5 GB por segundo, y SATA 2 de hasta 3 GB por segundo de velocidad de transferencia.

SAS: (Serial Attached SCSI): interfaz de transferencia de datos en serie, sucesor del SCSI paralelo, Aumenta la velocidad, y permite la conexión y desconexión de forma rápida.







Calidad de discos duros:

#1 HITACHI – Los discos duros Hitachi son la marca más confiable, Hitachi fue la primera marca en introducir helio dentro de los discos duros, y la confiabilidad es parte de la tradición de esta empresa al hacer dispositivos de almacenamiento de alta duración.

#2 WESTERN DIGITAL – La marca Western Digital consigue el Segundo puesto de confiabilidad en discos duros, sin embargo cuando se trata de la facilidad para recuperar datos borrados la marca Western Digital hace los datos más "recuperables" debido a la buena calidad de grabación magnética y la facilidad para conseguir repuestos.

TOSHIBA – El tercer lugar lo ocupa la marca Toshiba, produciendo discos duros de buen rendimiento para computadoras portátiles.

#4 SEAGATE – El cuarto lugar es para la marca Seagate, esta marca hizo numerosos discos duros de 1.5 TB que poseen una gran posibilidad de fallar.

Así también hubieron reportes de discos duros de 3 TB Seagate ST3000M001 y el de 4TB Seagate ST4000DX000 que no poseían un buen desempeño.

Sin embargo los últimos discos Seagate de 6 TB tienen indicadores de ser muy confiables.

Es necesario estar familiarizado con las diferentes marcas de fabricantes y todo disco existente en el mercado, existen casos en los cuales la clase de disco lo hace mas o menos dificil de leer y recuperar datos por medio de ciertos programas.

Tipos de Discos duros:

IDE, E-IDE, ATA, S-ATA (Serial Ata), SCSI, discos de portatil 2,5"(laptop y notebook), Ultra-SCSI, wide scsi, SCA80, Cintas y cartuchos de cinta (tape cartridges):DLT, SDLT, DLTIII, DLTIV, DLT2000, DLT4000, DLT7000, DLT8000, 4 mm: DAT, DDS, DDS2, DDS3, DDS4, DDS5 (DAT72 / DDS 72), 8mm: AIT, Exabyte, 8900, QIC, Mammoth, HP JetStore, Surestore..., Streamers TRAVAN: TR, TR1, TR2,

TR3, TR5, TR7...Tandberg SLR, VXA, MO, CDROM, DVD, DVD-R, DVD+R, DVD-RW, DVD+RW, tarjetas de memoria Flash y fotografía digital: Smart Card, Memory Card, Smart Media, Memory Stick, Compact Flash, Syquest, Jaz, Zip, Floppy (diskettes, Disquete LS 120).

Fabricantes y marcas:

WD Western Digital, ST Seagate, Maxtor, Toshiba, Samsung, Hitachi, IBM, Quantum, Fujitsu, NEC, Iomega, Micropolis, Sony, Conner, Creative, JVC, Panasonic, Conceptronic, Lacie, Matshusita, Emtec, Basf, Digital, Compaq, Goldstar, HP Hewlett-Packard, JTS, LG, ExcelStore, Storagetek, Qualstar, Adic, SanDisk, Cannon, MDT Magnetic Data Technologies .

La gran mayoría de los problemas con las pérdidas de datos ocurren debido al hardware del disco duro. Según la Empresa Kroll Ontrack, el 44% de los problemas de pérdida de datos están ocasionados por fallos en el hardware del disco, ya sea HDD o SSD.

El error humano también está presente en el 32% de los casos de pérdida de datos, ya sea por manipulación o mal uso del dispositivo.

Causas de la pérdida de datos:

Corrupción del sistema de archivos. Archivos desaparecidos, ficheros corrompidos, pérdida de directorios, archivos corruptos, bases de datos dañadas.etc

Golpes, caídas, roturas: Los cuales producen fallos generalizados. Es posible salvar los datos incluso en estos casos de daños físicos al reemplazar sus componentes mecánicos y/o electrónicos.

Recuperación en extremo difícil o imposible.

- Discos expuestos a altas temperaturas
- Discos muy dañados físicamente
- Datos sobrescritos con método guttmann
- Expuesto a campos magnéticos muy fuertes.
- Doblamiento de la superficie o grietas.
- Platos de discos duros rotos

Metodología de recuperación básica:

Usualmente hay 4 Etapas cuando se trata de una recuperación exitosa de datos, sin embargo esto puede variar dependiendo de la clase de corrupción de datos y la clase de reparación que es necesaria de hacer.

Reparar el disco duro:

Si el motor no alcanza la velocidad necesaria, los platos internos deben ser movidos a un nuevo disco duro, junto con los brazos y el cabezal lector
Alguno de los componentes del motor puede presentar fallos que provoquen la pérdida de datos o su inaccesibilidad, como problemas que afectan al correcto giro de los platos o a la simetría del disco duro.
Los problemas más comunes que presentan son:
Bobinas del motor comunicadas.
Rodamientos dañados.

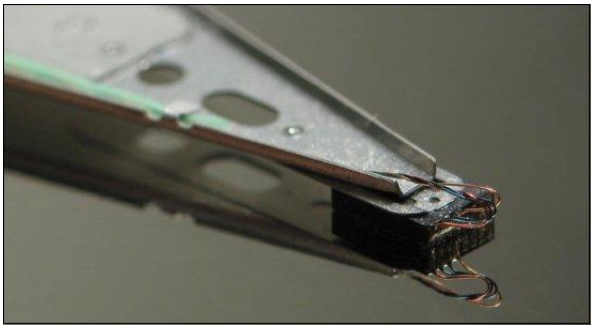
Cabeza lectora:

Los datos deben ser leídos en forma estable para poder aplicar procedimientos de software en la recuperación.

Por ejemplo si el brazo lector y la cabeza lectora están en mal estado deben ser reemplazadas.

Si la placa lógica no funciona adecuadamente, o se percibe un sobrecalentamiento en algún componente, se debe reemplazar.

El cabezal lector pierde calibración con el paso de los años y muchas veces se desprende, haciendo contacto con la superficie del disco rayándola y ocasionando la perdida de datos.

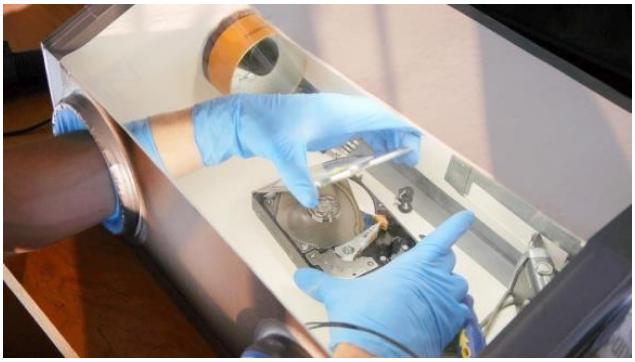


El disco duro debido a sus componentes mecánicos son los que mas fallan, se detectan al percibir ruidos extraños y repetitivos provenientes del disco.

El cabezal lector es una pieza móvil encargada de leer, escribir y borrar datos. Cualquier fallo en alguno de sus componentes imposibilita el acceso a la información.

Las averías que presentan son de varios tipos en función de su ubicación:

Bobinas.
Problemas en el amplificador del cabezal.
Cabezales.
Descompensación térmica (este tipo de avería puede incluirse en otros apartados dependiendo dónde ha afectado la descompensación térmica).
Las averías de discos duros correspondientes a este apartado son las más comunes, debido al gran número de componentes que lo integran.
Si existe un fallo físico, lo siguiente es pasar a la cámara limpia para hacer un análisis más exhaustivo, detectar las piezas dañadas y reemplazarlas.

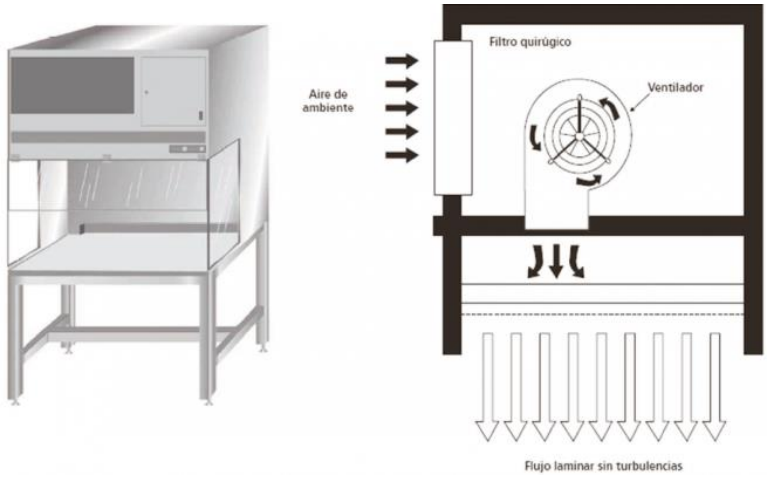


Para esto, debemos contar con repuestos originales, incluso de discos duros que hace tiempo no se comercializan. La forma de conseguirlos es tan sencilla como comprar varias unidades usadas o que no funcionen y extraerles la placa lógica y otras partes en caso de que se encuentren en buen estado.

La cámara limpia

Todos hemos oído muchas veces que si abrimos un disco duro en nuestra casa o trabajo, podríamos dañarlo para siempre y no poder recuperar los datos. Esto es debido a que las partículas de polvo podrían meterse entre el disco y el brazo del disco duro, dichas partículas hacen “saltar” al brazo del disco y terminará rayando su superficie.

La distancia entre el brazo y el propio disco magnético es de 0,012 **micrómetros**. Aquí es donde entra en acción la cámara limpia, a continuación se muestra un esquema de cómo funciona:



Hay varios tipos de cámaras limpias según las partículas que son capaces de eliminar. Cuanto mejor es la cámara limpia, menos partículas deja entrar en su interior. A continuación se muestra un gráfico con las certificaciones de las

Certificaciones de Cámara Limpia

Class	Partículas/m³ (máximo)						FED STD 209 E
	≥0.1 µm	≥0.2 µm	≥0.3 µm	≥0.5 µm	≥1 µm	≥5 µm	equivalente
ISO 1	10	2					
ISO 2	100	24	10	4			
ISO 3	1,000	237	102	35	8		Class 1
ISO 4	10,000	2,370	1,020	352	83		Class 10
ISO 5	100,000	23,700	10,200	3,520	832	29	Class 100
ISO 6	1,000,000	237,000	102,000	35,200	8,320	293	Class 1000
ISO 7				352,000	83,200	2,930	Class 10,000
ISO 8				3,520,000	832,000	29,300	Class 100,000
ISO 9				35,200,000	8,320,000	293,000	Aire de ambiente

Electrónica:
El problema más habitual:
Las averías de tipo electrónico suelen producirse por un suministro incorrecto de energía, causando un cortocircuito en la placa controladora que imposibilita el acceso a la información.

Firmware:
Durante la fase de arranque los discos duros necesitan cargar una serie de parámetros que se encuentran almacenados en los platos. La avería de firmware se produce cuando dichos parámetros, imprescindibles para el funcionamiento de los discos, sufren una corrupción que impide proceder a su lectura.

Etapa 2: hacer una imagen del disco, la importancia de sacar la información fuera del disco tiene que ser la prioridad número uno.

Mientras mayor sea el tiempo que un disco duro continúa funcionando con una falla interna grave, es más posible que ocasione la destrucción irrecuperable de los datos.

Crear una imagen del disco usando el espejeo o la técnica llamada mirroring, nos permite hacer una copia secundaria en otro dispositivo, en el cual es más seguro utilizar las técnicas de recuperación usando diferentes programas sin dañar la fuente original de los datos.

Etapa 3: recuperación lógica de archivos, particiones, MBR y estructuras del sistema de archivos.

Después de que el disco a sido clonado, es mas cómodo intentar la recuperación de datos, si el disco duro a fallado a un nivel lógico, hay un numero de razones para eso.

Usando el clon (mirroring) es más posible reparar la tabla de particiones o el máster boot record (MBR) para poder leer la estructura de datos del sistema de archivos y recuperar la información almacenada.

Etapa 4: Reparar archivos dañados.

El daño a la información puede ser causada cuando por ejemplo un archivo es escrito en un sector dañado, esta es la causa más común en un disco duro que está fallando, lo que significa que la información debe ser reconstruida para poder ser leída.

Documentos corruptos pueden ser recuperados por numerosos métodos de software o incluso hacerse manualmente reconstruyendo el archivo usando un Hex editor.

Clases de mal funcionamiento: A nivel mecánico, A nivel electrónico, A nivel de firmware.

No hay dos situaciones de recuperación de datos iguales. Muchas veces, es posible recuperar completamente los archivos perdidos de un disco, incluyendo los nombres de archivo originales y estructura de carpetas. Otras veces, los archivos y los datos pueden ser recuperados, pero los nombres de archivo, fecha / marcas de tiempo y rutas de las carpetas no. En los peores casos, no hay archivos recuperables en el dispositivo.

La recuperación de datos profesional normalmente requiere años de experiencia y un profundo conocimiento de los matices técnicos de los sistemas de archivos y la física de los discos duros, los cuales además, difieren dependiendo de la tecnología

utilizada (IDE, SATA, SAS, SSD,…). En este artículo, vamos a echar un vistazo muy por encima sobre cómo funciona la recuperación de archivos.

¿Cómo se almacenan los archivos en el disco?

Para entender cómo los archivos se pueden recuperar después de un borrado accidental, hay que conocer cómo se almacenan los ficheros en los discos duros u otros dispositivos de bloque. En la familia de entornos Microsoft, las particiones son denominadas “discos lógicos”, a los cuales se les asigna letras de unidad y etiquetas descriptivas opcionales. Por ejemplo, C: (sistema) o D: (Datos).

Cada partición tiene su propio tipo de sistema de archivos, que es algo 100% independiente entre las diferentes particiones que puede albergar un disco físico. Por ejemplo, un disco duro físico para un sistema de Windows puede contener dos discos lógicos con diferentes sistemas de ficheros, por ejemplo uno con sistema de ficheros NTFS y otro FAT32. Si se tiene también sistemas UNIX, la variedad de sistemas de archivos que se puede utilizar es muy numerosa.

La información sobre las particiones en el disco se almacena normalmente en el comienzo de la unidad de disco duro. Esto se conoce generalmente como una “tabla de particiones” o “mapa de particiones.”

Cada partición se se divide en dos partes: Una guarda información sobre el disco (estructura de carpetas, sistema de archivos, etc.) y la otra contiene los datos en si. Esto es así ya que ofrece ventajas de rendimiento, mejoras en la gestión del espacio en disco y fiabilidad.

Los sistemas de ficheros contienen la información sobre los archivos y carpetas mediante registros de ficheros que almacenan los nombres, tamaño, fecha y otra información técnica, son los denominados metadatos. Esta información también incluye las ubicaciones físicas exactas (direcciones) de los datos del archivo en el disco. Esta información, la cual suele estar en forma de tablas / base de datos, suele tener copias de seguridad dentro del mismo disco por si una de ellas se corrompiera. La manera en la que se almacena esa información depende mucho del sistema de ficheros utilizado, no es lo mismo NTFS que ZFS o EXT4 por nombrar alguno.

Por ejemplo, en sistemas de ficheros FAT, esta información se guarda en lo que se denomina una tabla de asignación de archivos (FAT) y en sistemas NTFS se almacena en la tabla maestra de archivos (MFT). Cuando un equipo tiene que leer un archivo, primero busca la información sobre dicho fichero / carpeta archivos (Tipo de archivo, tamaño, permisos, etc). A continuación, se busca la dirección que tiene, donde está físicamente. Una vez obtenida la información, el programa / sistema va al lugar especificado en el disco y lee los datos.

La agrupación de los datos que conforma un fichero juega un papel fundamental a la hora de poder recuperar información. Esta puede ser contigua o fragmentada (no adyacente), siendo el primer caso el más optimo a la hora de recuperar

información. Cuando los ficheros se encuentran fragmentados, la información sobre las distintas ubicaciones de las partes que lo componen es contenida en esas tablas mencionadas anteriormente como es de suponer.

En los volúmenes NTFS, la MFT no se encuentra en un sector predefinido y además, este puede variar en el tiempo si hay sectores defectuosos en la ubicación actual de la MFT. Al arrancar, Windows consulta otro tipo de información en su sector de arranque para poder localizar la actual tabla MFT en uso, si esos datos están dañados, la MFT no puede ser localizada y Windows invitará al usuario a formatear la partición.

Borrado de ficheros

Al borrar un archivo, en la inmensa mayoría de casos, realmente no se destruyen los datos del fichero inmediatamente. En lugar de ello, el sistema de archivos hace algunos cambios en la información de las tablas para informar que el archivo se ha eliminado y el espacio físico donde estaba ubicado queda disponible para ser usado. En algunos casos se conservan también todos los metadatos sobre el archivo hasta que se sobrescriban con otros metadatos de un nuevo fichero (Windows). Por el contrario, otros sistemas como Mac OS X destruyen por completo el registro de archivo del fichero eliminado.

Si bien los sistemas operativos y sus sistemas de ficheros varían en el número de metadatos guardados y su trato al eliminar archivos y carpetas, todos los sistemas dejan los datos de archivo reales sin tocar hasta que sea necesario asignar ese espacio a otro nuevo archivo. Esto hace que en algunos casos, ficheros borrados hace mucho tiempo puedan ser recuperados si no se generaron muchos ficheros nuevos en el sistema posteriormente. Hay aplicaciones de borrado seguro como “srm” en sistemas GNU/Linux que permiten borrar de forma 100% segura archivos.

Recuperación de archivos

Se debe tener claro que si los datos del disco se sobrescriben, los datos antiguos desaparecen y ningún programa / método de recuperación de datos podrá recuperarlos. Por eso siempre se recomienda no utilizar un disco del cual se quiera rescatar información eliminada.

Para los archivos que no han sido sobrescritos, hay dos métodos básicos de recuperación de archivos que la gran mayoría de software de recuperación de datos implementa. Uno es usando los metadatos y/o haciendo lo que denominan File carving (Recuperación de archivos en bruto).

A) Recuperación de archivos a través de análisis de la información sobre los archivos y carpetas.

Este es el primer método que un programa de recuperación de archivos intenta realizar. Si la zona de metadatos está accesible se podrán recuperar los archivos

junto con su nombre, fecha de creación, etc. El software empieza por tratar de leer y procesar la primera copia de la información sobre los archivos y carpetas (metadatos). En algunos casos (como el borrado accidental de archivos), este es el único método que el software debe realizar con el fin de recuperar los archivos en su totalidad. Si la primera copia de la información sobre los archivos y carpetas está muy dañado, el software escanea el disco para la segunda copia de la información sobre los archivos y carpetas.

Dependiendo del estado de dichas tablas de información, el programa de recuperación podrá regenerar todo el árbol de directorios, parte o en el peor de los casos nada. Por eso muchas veces, a la hora de recuperar archivos con este método se pueden ver ciertos ficheros y carpetas huérfanas.

B) Recuperación de archivos mediante la búsqueda de los tipos de archivos conocidos (Recuperación de archivos en bruto).

Si el primer método no produce resultados satisfactorios, una búsqueda de archivos en bruto se suele llevar a cabo. Este segundo método de recuperación de datos puede recuperar datos de archivos con mayor éxito que el primer, pero no puede reconstruir los nombres de archivo originales, fechas y demás.

Una búsqueda de los tipos de archivos conocidos, o la recuperación de archivos en bruto, funciona analizando el contenido del disco mediante “firmas de archivo”. Patrones comunes que identifican el principio y/o final de un archivo.

Por ejemplo, todos los archivos de imagen png (Portable Network Graphics) comienzan con la cabecera (cadena de texto) “‰ PNG”. Estas firmas se utilizan para reconocer que una porción de datos en el disco pertenece a un determinado tipo de archivo y por lo tanto se puede recuperar. Aunque sin conocer su nombre, fecha de creación, permisos, etc.

Pero no todo es de color de rosas, se da el caso de que algunos tipos de archivos tienen una “cabecera” que les puede identificar, pero no tienen un “final” definido. Tampoco todas las cabeceras son reconocidas por todos las herramientas de recuperación de discos. En casos de software no muy extendido, los peritos forenses deben manualmente identificar dichos patrones manualmente para poder extraer determinados ficheros del sistema.

Resumiendo, si el software de recuperación de datos puede identificar el “principio” y “final” (firma) del archivo, este puede ser fácilmente identificado y recuperado. Para los archivos que no tienen un “fin” de firma de archivo, se presupone que los datos de un archivo terminan al comienzo del siguiente. Para los archivos sin firma, como contenedores de discos cifrados, una búsqueda en bruto no será capaz de verlos, dejando solo la opción de intentarlo manualmente con un editor hexadecimal.

Lógicamente si a esto se le suma que los ficheros pueden estar fragmentados en el disco,.. la dificultad de recuperarlo crece exponencialmente. Además, los archivos

sin firmas de archivo reconocibles pueden tener largas áreas de “basura” después de una recuperación. Eso explica por qué algunas veces se recuperan ficheros pero estos aparentan estar corruptos.

Además de las complicaciones de archivos fragmentados, una búsqueda de archivos en bruto también puede ofrecer “falsos positivos”. Por ejemplo, la cadena “ID3” (cabecera de ficheros .mp3) puede estar también dentro de un archivo de texto, identificando incorrectamente una parte de texto como el comienzo de un archivo MP3. La calidad del software de recuperación juega también un papel fundamental.

Algunos programas permiten al usuario especificar manualmente conjuntos complejos y avanzados de firmas de archivos de manera personalizada.

Detalles a tener en cuenta

El daño causado a un sistema de archivos puede ser impredecible. El estado de los archivos dependerá de la causa que hizo perder los archivos, la salud del disco antes de la falla o pérdida de datos y cualquier acción realizada antes de los intentos de recuperación de datos.

La recuperación de datos no se debe intentar en discos con fallos de hardware. Cualquier intento de manipulación con un disco dañado físicamente pueden causar más pérdida de datos, lo que hace posteriores intentos de recuperación de datos inútiles.

Recomendamos realizar todas las tareas de recuperación de datos de imágenes de los discos reales con el fin de preservar los datos originales en el disco. Esto permite ejecutar múltiples intentos de recuperación de datos sin causar cambios en el disco o correr el riesgo de una mayor pérdida de datos.

La recuperación de ficheros eliminados de un disco duro depende de todos estos factores.

Si el fallo es mecánico dependerá de la tecnología utilizada y la avería.
Sistema de ficheros utilizado.
Tipo de borrado (Problema con la tabla de particiones, formateo, avería mecánica, simple borrado, etc)
Programa de recuperación: Normalmente en relación con el sistema de ficheros en uso. Puede haber programas muy buenos a la hora de recuperar datos en determinados tipos de borrado o con determinados sistemas de ficheros. La recomendación es siempre trabajar con copias (imágenes) de discos a recuperar y si se echan en falta determinados ficheros, probar con otras herramientas.

Tipo de problemas en discos duros y su solución

Recuperación de archivos desde un disco duro con metadatos dañados

Si un disco se desmonta de manera inadecuada (debido a un corte de energía o un error del usuario), puede causar daños a parte o la totalidad de los tablas de información. Como se dijo anteriormente, aunque se pierda esa información sobre ubicación, nombre, etc de los datos, estos pueden ser recuperados en la gran mayoría de casos (en bruto).

Recuperación de archivos desde un disco duro reparticionado

Si un disco se reparticiona accidentalmente, el panorama es similar al caso anterior, con una excepción. Cuando se crea una nueva estructura de partición, algunos datos nuevos se escriben en el disco, pero no suelen afectar a los metadatos. Por lo que el sistema de ficheros suele permanecer intacto, incluyendo la información sobre los archivos y carpetas.

Por lo tanto, los programas de recuperación de archivos pueden escanear el disco, encontrar esta información, y recuperar esos archivos y carpetas que no han sido afectados por los nuevos datos de la partición. Una búsqueda adicional para tipos de recuperaciones rara vez es necesaria.

La recuperación de archivos a partir de una partición formateada

El cambio de formato es típicamente más perjudicial que la nueva partición y depende en gran parte del tipo de operación de formateo de disco realizada. Si el formateo fue completo y todos los datos de la partición fueron sobrescritos (generalmente con valor 00 o FF) es imposible recuperar los archivos de la partición. Por suerte lo habitual es realizar un formateo rápido (Por motivos de tiempo).

Un formato rápido hace que algunos o todos de la información sobre los archivos y carpetas sean sobrescritos (metadatos), pero deja los datos de archivos sin tocar. Los programas de recuperación de archivos pueden escanear el disco, encontrar lo que queda del sistema de archivo anterior, y recuperar archivos y carpetas en consecuencia.

Recuperación de archivos desde un disco con un sistema de archivos dañado

Este caso depende en gran medida del daño que tenga el sistema de ficheros. Se seguirá el orden normal, primero búsqueda de metadatos y después recorrer todo el disco en busca de firmas para extraer todo lo que se si es necesario.

Recuperación de archivos cuando los archivos se han movido a través del disco

Si se bloquea el ordenador durante una operación de desfragmentación de disco o al sobrescribir particiones, los resultados pueden ser desastrosos. Este suele ser el peor de los casos para la recuperación de archivos. Aunque la información sobre los archivos y carpetas puede parecer saludable, los metadatos puede señalar direcciones físicas equivocadas para los archivos que estaban en proceso de ser movido.

Por ejemplo, los datos pueden haber sido escritos a una nueva ubicación, pero la información sobre los archivos y carpetas no se hayan actualizado todavía (o al contrario). En estos casos, incluso una búsqueda adicional en bruto puede ser poco efectiva dependiendo de la fragmentación de los ficheros.

Discos SSDs

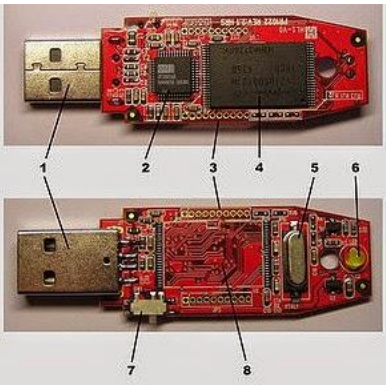
Una unidad SSD, siglas del inglés 'Solid State Drive' o 'Unidad de estado sólido' es un medio de almacenamiento que no depende de piezas mecánicas para su funcionamiento.
En cambio un SSD posee almacenamiento de datos gracias a memoria no volátil o del tipo *flash*, lo que lo hace menos susceptible a los golpes, prácticamente no hacen ruido y tienen un menor tiempo de acceso y de latencia. Por otro lado los SSDs utilizan la misma interfaz que los discos actuales, SATA, por lo tanto son completamente compatibles con un sistema actual.
La lenta adopción de esta tecnología se debe básicamente al alto costo de estas unidades, esto a su vez porque las memorias flash son considerablemente más caras de fabricar. Sin embargo esta no es una desventaja técnica, con el correr de los años el mercado madurará y se equiparará, tarde o temprano, con uno disco duro mecánico. Por otro lado está la baja capacidad actual si los comparamos con su par magnético que ya supera los 2TB (como el Seagate GoFlex externo de 3TB).
Una desventaja técnica de los SSDs es su baja o nula recuperación luego de un fallo de alguna de las celdas que lo componen, al fallar la celda queda completamente destruida, inutilizable y por ende imposible de recuperar, a diferencia de uno mecánico que bajo supervisión experta es posible lograr alguna recuperación.

Tipos de Memorias:

- USB
- Pendrives USB
- Discos Jaz
- Discos Zip
- Cartuchos SyQuest
- Medios de Cámaras Digitales – tarjetas SD, microSD, Flash
- SyQuest
- Discos flexibles (disquetes)
- Optical Disks
- DVD, CD-ROM

Memorias USB:

Memoria usb: Estructura y Funcionamiento



Componentes internos de una memoria USB típica

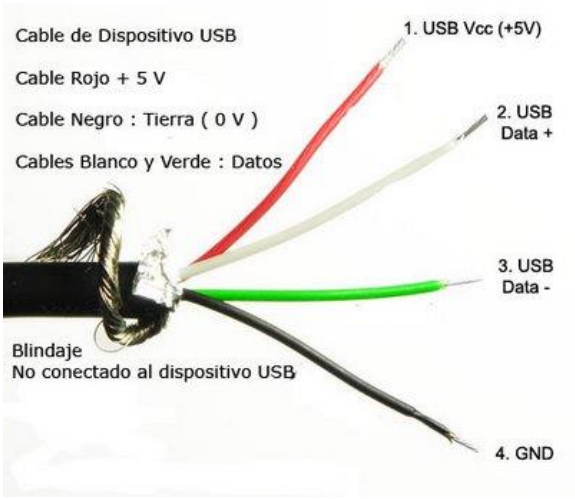
1	Conector USB
2	Dispositivo de control de almacenamiento masivo USB
3	Puntos de Prueba
4	Circuito de Memoria flash
5	Oscilador de cristal
6	Led
7	Interruptor de seguridad contra escrituras
8	Espacio disponible para un segundo circuito de memoria flash

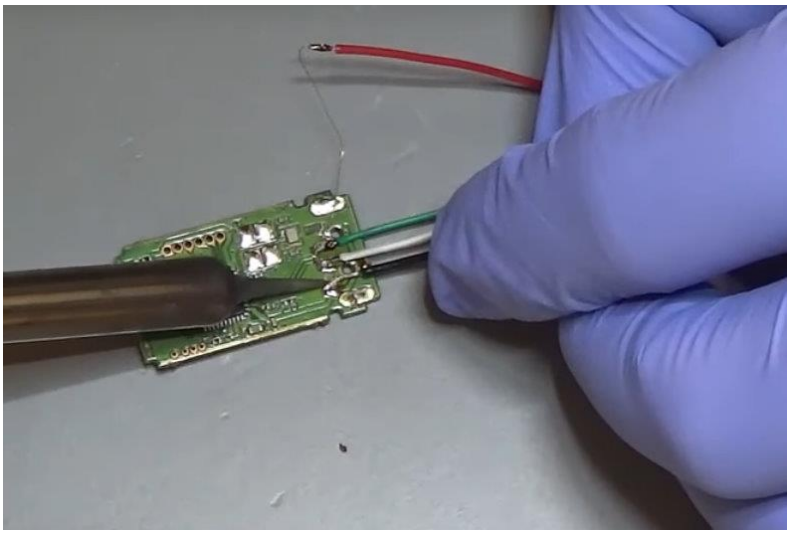
La forma en que está compuesta una memoria USB es la siguiente:

La parte más importante es el chip de memoria donde se almacenan los datos. El pendrive se compone principalmente de dos transistores que tienen como nombres "compuerta flotante" y "compuerta de control", dentro de ellos hay millones de celdas que se conectan entre ellas gracias a un elaborado circuito. Luego encontramos el dispositivo de control, el cual cuenta con un microprocesador muy pequeño y cantidades mínimas de memoria RAM y ROM.
El conector USB es la puerta de enlace hacia el ordenador. Cuando se conecte se activará el oscilador que es lo que controla el acceso de datos. Partes de carácter secundario que pueden o no estar dentro del pendrive son el LED o luz que indica que indica la conexión o trasferencia de datos y el dispositivo de seguridad que sirve para proteger los datos contra escritura o borrado de información de manera accidental.
En cuanto a su uso solo se tiene que conectar al puerto USB y esperar a que sea reconocido para poder trabajar con los datos o programas de nuestra memoria usb.

Para ser capaz de reparar los daños a nivel de hardware es necesario entender las conexiones y las casos más comunes como ser una usb quebrada, con algo de paciencia podemos soldar filamentos para reconstruir las pistas electrónicas originales y con mucho cuidado conectarla a la computadora para poder recuperar los datos.

En caso que sea muy difícil conectar la pieza original el circuito con algo de soldadura y conociendo los códigos de colores de alimentación y cables de datos seremos capaces de hacer diferentes puentes hacia el circuito del usb.

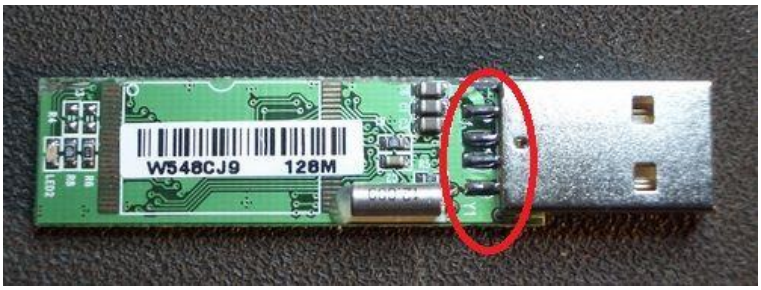




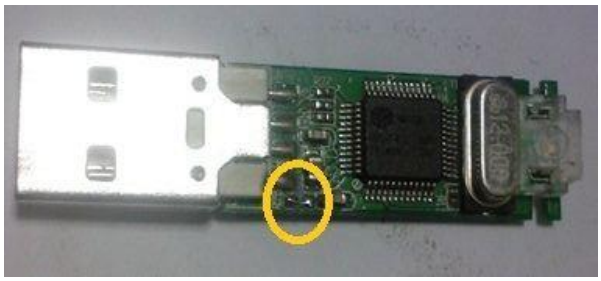
Si el USB recibió un golpe muy fuerte, entonces lo más probable, es que el cristal de cuarzo se haya quebrado.

En este caso hay que buscar dicho componente en otro USB o alguna tarjeta electrónica que lleve dicho componente es importante ver el valor de su frecuencia de oscilación generalmente es de 12 o 24 Mhz obtenido dicho componente lo reemplazaremos para ello usaremos un cautín, cuidando de no juntar sus pines.

Cuando al estar moviendo el USB estando conectada a la pc y este lo reconoce solo por momentos entonces hay una mala soldadura en los pines del conector usb.
Debemos destapar con cuidado el USB y resoldar con cuidado los terminales de conexión, teniendo en cuenta que los pines no entren en contacto o no se sobrecaliente la zona. Destruyendo el circuito.

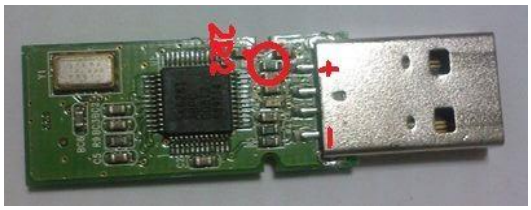


Los dispositivos USB cuentan con una protección en caso de polarización inversa es típico que uno conecte su USB en una computadora y este quede estropeado por la mala polarización de los puertos USB ; en este caso no siempre lograremos rescatar al USB.
La protección de los dispositivos consiste en una simple resistencia fusible este componente posee una baja resistencia generalmente en el orden de 1 a 5 ohm
Lo ideal es reemplazarlo con otro de su misma resistencia,
Pero si queremos darle una solución rápida se puede soldar un trozo de alambre fino y procedemos a hacerle un puente tal como se muestra en la imagen.
Cabe recalcar que esta no es la solución adecuada, pero si nos permitiría usar el usb lo suficiente para recuperar los datos.
Nota:



Para dete rminar cuál es la resistencia a cambiar o puentear seguimos el rastro con un milímetro desde el terminal positivo, hasta encontrar la primera resistencia, si no tenemos un multimetro agarramos una lupa y nos fijamos el valor, en el circuito indica

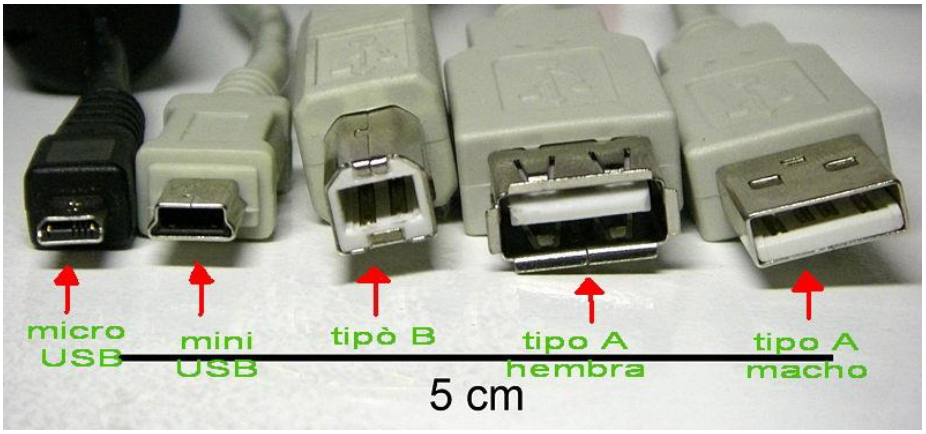
2R2 generalmente esta cerca del puerto usb.



A veces nos encontramos con memorias USB, que se encuentran quebradas de modo que tenemos que soldar filamentos para poder extraer la información, recordando la disposición de los terminales positivo negativo, datos (+) y datos (-).

Diferentes clases de conectores:

Es necesario conocer los diferentes conectores que existen en el mercado, así como tener práctica en el uso del cautín o soldador.



Cuando de trata de recuperar datos de celulares, necesario tener diferentes conectores para que nos sea mucho más fácil y practico poder iniciar la etapa de recuperación con el software necesario.

Un caso muy común son los dispositivos de almacenamiento genérico conectados por el puerto USB de la máquina, que sí son retirados sin emplear el diálogo que ofrece el sistema (“Retirar de forma segura”) pueden dañarse y perder su formato, apareciendo vacío de contenido para el explorador de archivos.

En estos casos, aunque el formato se haya perdido, los archivos siguen existiendo, por lo cual, con la aplicación adecuada, será posible recuperar una gran parte de ellos. Si el usuario inexperto cae en el “error” de dar formato disco, con la ilusión de poder recuperar los archivos borrados, solamente estaría haciendo aún más inaccesibles los archivos borrados.

Otro problema que afecta a la memoria el estado sólido, y en rigor de verdad a cualquier otro tipo de soporte de información, son las infecciones por virus. En estos casos, la recuperación de datos será bastante más complicada, siendo necesario eliminar el script nocivo antes de proceder a recuperar los datos borrados.

Como recuperar archivos almacenados en una memoria USB dañada o no reconocida

Lo primero que tendremos que hacer será descargar el programa de terceros Wondershare Data Recovery.

Una vez descargado e instalado en nuestro ordenador, deberemos insertar la memoria USB a nuestro ordenador, para renglón seguido ejecutar el programa. Una vez dentro de la interfaz, deberemos hace clic en la opción Siguiente (Next) para que de manera automática nos lleve a una ventana en la que tendremos que seleccionar el tipo de archivos que deseamos recuperar.

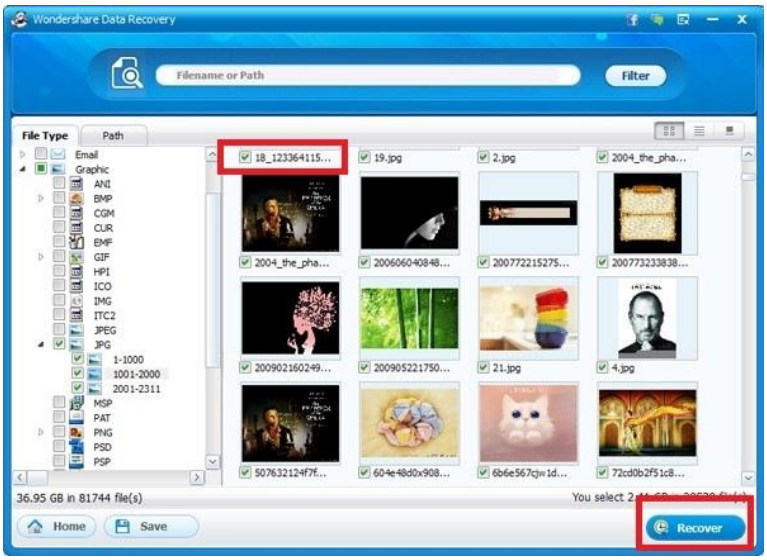
En este caso se recomienda marcar la opción:

Todo tipo de Archivos.

Una vez marcada vuelve a pulsar sobre la opción **Siguiente**. Esto nos llevará a una nueva ventana en la que tendremos que seleccionar el lugar desde donde deseas recuperar los archivos. En nuestro caso deberás seleccionar la opción **Recuperar datos desde un dispositivo Externo**. Tras marcar esta opción vuelve hacer clic en Siguiente.

En la nueva ventana tendremos que seleccionar la opción En la que te recomendamos que marques la opción "**Escaneo profundo**". Luego vuelve a pulsar siguiente y el proceso de recuperación comenzará automáticamente. Una vez terminado dicho proceso se mostrará un resumen con todos los archivos recuperados junto con la posibilidad de previsualizarlos. Por último podremos

seleccionar los archivos a recuperar e indicar en que carpeta de nuestro disco duro queremos almacenarlos.



Cómo reparar memoria USB/Pendrive dañada o no reconocida.

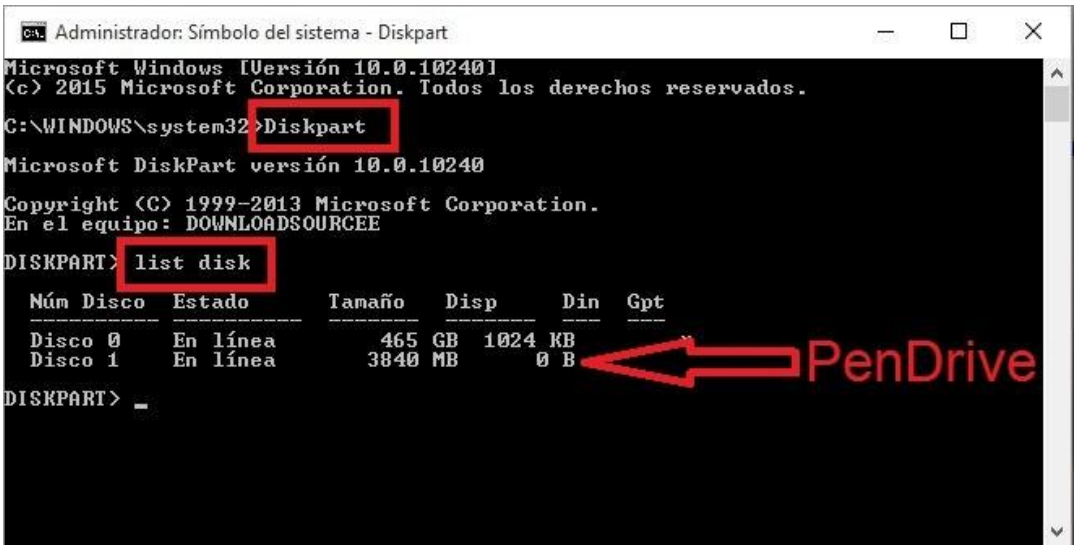
En el caso de que conectemos nuestra memoria USB a nuestra computadora y no podamos hacer uso de ella, bien por algún mensaje de error, por no tener formato o cualquier otro motivo .

Lo primero que tendremos que hacer, es conectar nuestra memoria USB a nuestro ordenador mediante el puerto USB, para renglón seguido abrir la herramienta **Símbolos del Sistema como Administrador (CMD)**. Una vez dentro de símbolo del sistema, debemos escribir el siguiente comando y luego pulsar la tecla Enter para ejecutarlo: **DiskPart**

DiskPart

A continuación tendremos que introducir el comando: **list disk**

list disk



Tras pulsar sobre la tecla Enter para ejecutar el comando anterior, veréis como se muestra una lista con los discos actualmente conectados en tu ordenador. Como es normal se mostrará el disco duro así como la memoria USB externa que tenemos conectada. Para diferenciarlos podremos fijarnos en el tamaño del disco, ya que por lo general el disco duro interno de nuestro ordenador será de mayor tamaño. Además el Disco nº 0 será el que se corresponda al disco duro y el Disco nº 1 a la memoria USB conectada.

Por lo tanto el siguiente comando que deberemos utilizar será: **select disk 1**

select disk 1

Donde el nº representa la memoria USB que vamos a reparar. Tras pulsar la tecla Enter, ya habremos seleccionado el Pendrive que nos interesa y por lo tanto deberemos escribir y ejecutar el comando: **clean**

clean

Tras pulsar la tecla Enter verás como tu memoria USB a sido formateada por completo. A continuación deberemos crear una partición primaria en dicha

memoria USB para lo cual debermos introducir el comando: **create partition primary**

create partition primary

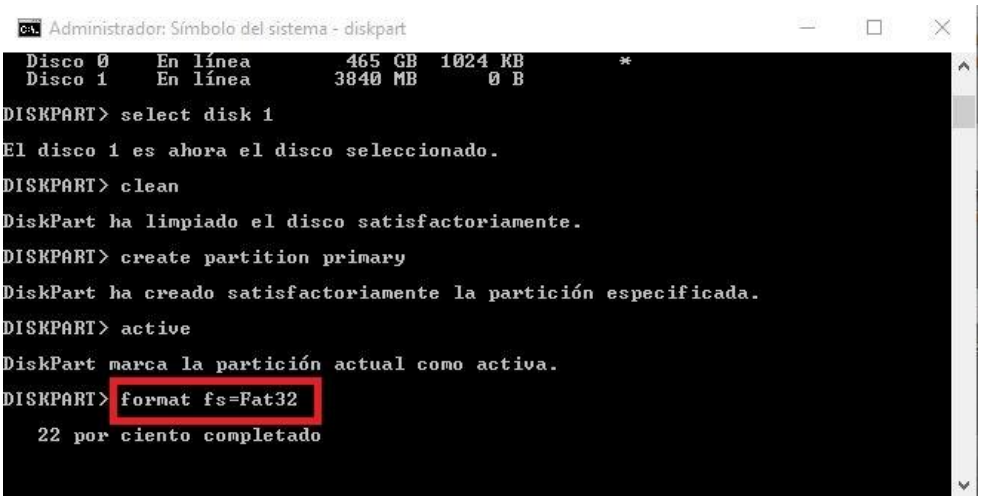
Tras pulsar la tecla Enter la partición habrá sido creada pero aun tendremos que activarla, para lo cual tendremos que introducir el comando y ejecutar el comando: active

Una vez activado, deberemos formatear la partición creada, para ello tendremos que introducir el comando: **format fs=Fat32** o **Format fs=NTFS** esto dependerá del tipo de formato que queramos dar a nuestro PenDrive.

format fs=Fat32

o

Format fs=NTFS



Una vez que el proceso de formateado halla terminado, ya podremos utilizar nuestra memoria USB de nuevo en cualquier ordenador o dispositivo con puerto USB.

Una vez terminado este proceso, podremos utilizar un software de recuperación para intentar recuperar la posible información que aun pueda almacenar nuestro dispositivo tras haber sido formateado.

Memorias Micro SD:

Cuando la memoria micro sd se encuentra quebrada es imposible repararla.

Software de recuperación:

Las herramientas utilizadas para la recuperación de datos pueden ser divididas en 2.
Tenemos herramientas de pago y herramientas Open source, cuya distribución es gratuita y para uso personal.

A continuación nombraré y daré detalles de diferentes programas de distribución gratuita (open source) y sus principales características:

Software Libre - Herramientas para Linux y Windows

Open Source Forensics: http://www.opensourceforensics.org

CromWell Intl: http://www.cromwell-intl.com/security/security-forensics.html

Computer Forensic Resources:
http://www.evestigate.com/computer%20forensic%20resources.htm

Centrux (ex Condor Linux), basado en Debian, herramientas para Informática Forense y Respuesta a Incidentes, desarrollado por Marcos Pablo Russo (egresado del curso de Informática Forense 2004).

AU, George M. Garner Jr. conjunto de herramientas y librerías para Microsoft Windows http://www.gmgsystemsinc.com/fau/

Smart Linux, basado en Slackware de Linux, diseñado para análisis informático forense, http://www.asrdata2.com

Snarl, basado en Unix FreeBSD, http://www.securitydistro.com/security-distros/SNARL

The Coroner´s Toolkit (TCT), de Dan Farmer y Wietse Venema, http://www.opensourceforensics.org

The Penguin Sleuth Kit, http://www.linux-forensics.com, (sleuth: detective), de Ernest Baca, http://www.knopper.net/knoppix/

The Sleuth Kit, herramientas de línea de comandos de Unix para el análisis forense, http://www.sleuthkit.org

The Autopsy Forensic Browser, para analizar discos y sistemas de archivos de Windows y UNIX, Linux, de Brian Carrier.http://www.sleuthkit.org/autopsy/index.php

The Open Computer Forensics Architecture (OCFA) de la Agencia Nacional Policial Alemana. http://ocfa.sourceforge.net/

Sysinternals Suite, de Mark Russinovich. http://technet.microsoft.com/en-us/sysinternals/bb842062.aspx

Telefonía, Celulares, PDA, GPS

E-evidence Info, http://www.e-evidence.info/cellular.html, listado de herramientas comerciales y libres

Bitpin, visualiza y administra información de teléfonos LG, Samsung, etc (Licencia GPL) http://www.bitpim.org

Chip IT, http://home.scarlet.be/chipit/Chipit.html

SIMfill, Subscriber Identity Modules (SIMs), NIST National Insitute of Standards and Technology http://nist.com

Oxygen Forensic Suite 2010, (comercial) http://www.oxygen-forensic.com/en/

Mobiledit, (comercial) http://www.mobiledit.com/forensic/

UFED Cellebrite, (comercial) extracción de datos, análisis físico y lógico, http://www.cellebrite.com

XRY-Lógico, Físico, (comercial) http://www.msab.com/

Device Seizure 4.0, celulares, PDA , GPS, (comercial) http://www.paraben.com/

Neutrino, (comercial) de Guidance Software. http://www.guidancesoftware.com

Recuperación de ficheros

CDRoller
Data Recovery Wizard
Data Rescue PC3
Disk Drill Basic
dvdisaster.
FileSalvage.
GetDataBack.
IsoBuster.
Mac Data Recovery Guru.
Norton Utilities.
PhotoRec.
Recover My Files.

Recuva.
TestDisk.
TotalRecovery.
TuneUp Utilities.

Ontrack EasyRecovery: por Kroll Inc, NTFS, HFS, FAT, proprietario.

Herramientas de Cómputo Forense

Sleuth Kit (Forensics Kit. Command Line)
Autopsy (Forensics Browser for Sleuth Kit)
Volatility (Reconstrucción y análisis de memoria RAM)
Py-Flag (Forensics Browser)
Dumpzilla (Forensics Browser: Firefox, Iceweasel and Seamonkey)
dcfldd (DD Imaging Tool command line tool and also works with AIR)
foremost (Data Carver command line tool)
Air (Forensics Imaging GUI)
md5deep (MD5 Hashing Program)
netcat (Command Line)
cryptcat (Command Line)
NTFS-Tools
Hetman software (Recuperador de datos)
qtparted (GUI Partitioning Tool)
regviewer (Windows Registry)
Viewer
X-Ways WinTrace
X-Ways WinHex
X-Ways Forensics
R-Studio Emergency (Bootable Recovery media Maker)
R-Studio Network Edtion
R-Studio RS Agent
Net resident
Faces
Encase
Snort
Helix
NetFlow
Deep Freeze
hiren´s boot
Canaima 3.1
Mini XP

Herramientas para el análisis de discos duros

AccessData Forensic ToolKit (FTK)
Guidance Software EnCase
Kit Electrónico de Transferencia de datos

Herramientas para el análisis de dispositivos móviles

AccessData Mobile Phone Examiner Plus (MPE+)

PlainSlight: es un programa informático forense, y sin dudas su mejor característica es la facilidad de uso, Mediante PlainSlight podemos ver:

- Información del disco duro y sus particiones
- Extraer usuario e información de grupo
- Ver historial de internet
- Examinar la configuración de firewall de Windows
- revisar documentos recientes
- Recuperar más de 15 diferentes formatos diferentes
- Revisar información de almacenamiento de USB.
- Examinar los dumps de las memorias físicas.
- Examinar información del usuario etc

Bulk Extractor

Bulk Extractor es una herramienta informática forense que es capaz de analizar una imagen de disco, un archivo o un directorio de archivos y extraer la información útil **sin necesidad de analizar las estructuras del sistema de archivos.**

Otra de las grandes ventajas de ignorar para el análisis los sistemas de archivos es que este software se puede utilizar para procesar cualquier medio digital**, incluyendo discos duros, medios de almacenamiento SSD, medios ópticos, tarjetas de memoria como las utilizadas en cámaras y smartphones, registros de paquetes de red** y muchos otros tipos de información digital.

Si bien no es una herramienta que se destaca por su facilidad de uso, **lo cierto es que la minuciosidad y velocidad con que se hacen los análisis de los medios de almacenamiento** es más que suficiente para convertirla en una de nuestras herramientas principales.

P2 eXplorer

Básicamente, **P2 Explorer es un programa que nos permite montar imágenes de discos Encase (E01), Forensic Replicator (PFR), SafeBack 1, 2, & 3, SMART, FTK DD & E01, Raw DD, WinImage, Paraben's Forensic Containers (P2S), vmWare, VirtualPC, y VirtualBox (VDI).**

Para utilizar estas herramienta, lo único que tenemos que hacer **es montar la imagen de disco que queremos analizar** en cualquiera de las letras de unidad disponibles en nuestra computadora y luego abrir el explorador de archivos.

Debido a que se trata de una imagen de disco, la misma se montará con atributos de **"Sólo lectura",** que en pocas palabras significa que podremos ver el contenido del disco, pero no modificarlo en modo alguno, **lo que en cierto modo nos garantiza que todo seguirá estando almacenado como en el primer momento.**

Cabe destacar que **P2 eXplorer se encuentra disponible en dos versiones: una gratuita y la otra de pago.** La versión gratuita de la misma tiene como limitación que **sólo se puede ejecutar en equipos de 32 bits** y la imposibilidad de montar imágenes de máquina virtual.

Aun así, P2 eXplorer es una de las mejores herramientas disponibles para cuando **tenemos que analizar con minuciosidad gran cantidad de discos,** ya que gracias a que todas las funciones y características para estudiar los mismos se encuentran a la mano en la interfaz del programa, que por otra parte es muy fácil de aprender y entender.

HxD

Sin duda alguna, **una de las mejores herramientas para la recuperación de archivos que podemos encontrar en el mercado,** y además es completamente gratuita. **Mediante HxD estaremos en posición de analizar el sistema de archivos completo para poder encontrar aquellos archivos que han sido borrados,** tanto en forma intencional como accidental.Una de sus mejores características se centra en la facilidad de uso, y en ello tiene mucho que ver la interfaz, muy sencilla de entender y con todas sus funciones cómodamente dispuestas.

Sin embargo, sus diseñadores no han dejado de lado la capacidad de análisis y comprobación, y **para ello ofrece herramientas muy versátiles como la posibilidad de buscar y reemplazar, exportar sumas de comprobación, inserción de patrones de bytes y destructor de archivos,** además de opciones para la concatenación o división de archivos, registro de estadísticas y mucho más.

Con respecto a lo que podemos lograr con HxD, es realmente mucho, ya que como mencionamos es una herramienta muy flexible, **pero que sin embargo ha sido simplificada de tal modo para que lo demasiado técnico o lo que no nos serviría a un nivel básico de conocimientos no nos confunda,** un interesante punto de vista como para que cualquier tipo de usuario pudiera usar sus funciones **sin complicarse ni tener que saber mucho de informática.**

Esto es fácilmente comprobable cuando inspeccionamos las unidades y la memoria RAM, que se muestran de forma similar a un archivo, de forma contraria a como lo hacen otras aplicaciones, **en donde estos elementos se observan como regiones que recortan los datos que deberían estar juntos.**

Digital Forensics Framework

Digital Forensics Framework, también conocida como DFF, **es un suite de análisis forense digital de software libre,** o mejor dicho es una API construida arriba de una serie de

herramientas específicas, **y que por su complejidad puede ser utilizada tanto por profesionales como por usuarios con pocos conocimientos,** y que nos permitirá analizar, extraer y almacenar muchos datos que nos pueden servir para evaluar el estado de una computadora.

Entre estas herramientas se encuentra la posibilidad de acceder a dispositivos locales y remotos, análisis de discos y unidades extraíbles y remotos, leer diferentes formatos de datos forenses, **reconstrucción de discos de máquinas virtuales,** búsqueda de metadatos, recuperación de datos y archivos ocultos y eliminados, **análisis forense de memoria volátil** y muchísimas otras tareas más.

Autopsy: Es una interfaz gráfica para el análisis forense informático, mediante herramientas de líneas de comandos. El cual permite a los investigadores lanzar auditorías forenses no intrusivas en los sistemas a investigar. Estos análisis se centran en análisis genérico de sistemas de archivos y líneas temporales de ficheros. Se puede analizar los discos de Windows y UNIX y sistemas de archivos (NTFS, FAT, UFS1 / 2, Ext2 / 3). Debido a que este software se basa en HTML, se puede conectar con el servidor de Autopsy de cualquier plataforma con un navegador HTML. Autopsy proporciona un "Administrador de archivos"-como el interfaz y muestra detalles acerca de los datos eliminados y estructuras del sistema de archivos.

OSforensic: Es una herramienta de investigación digital que le permite extraer datos forenses o descubrir información oculta de una computadora. Ofrece una variedad de características de búsquedas avanzadas que le permiten descubrir las actividades realizadas en el equipo o en Internet, archivos borrados, contraseñas almacenadas y otras informaciones forenses.

Kali Linux: Es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general. Es una distribución de Linux avanzada para pruebas de penetración y auditorías de seguridad.

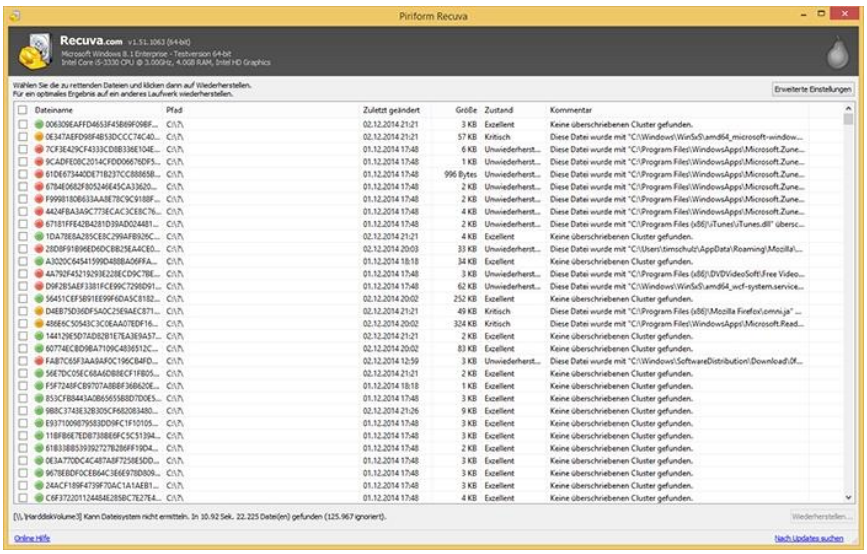
CAINE: Uno de las mejores distribuciones Linux forenses es Caine 2.0(Computer Aided Investigative Environment). Esta distribución cuenta con una serie de utilidades y herramientas especializadas en dar soporte a cada una de las cuatro fases de la Informática Forense: Estudio preliminar, recolección de la evidencia, análisis de la evidencia y la elaboración del informe final.

AL ser una herramienta gratuita, deberán buscar en internet los link de descarga, luego de bajar la imagen .iso tendrán que grabarla en un dvd y luego ingresar al bios de la computadora, booteando desde el dvd para poder ingresar al entorno del programa.

En la actualidad el desarrollo de software destinado a reconstruir informacion, sigue en crecimiento, las empresas privadas, programadores e ingenieros, poseen

una fuerte presencia en el desarrollo de estas herramientas de recuperación de datos y análisis digital, con cada año se hace más presente la necesidad de personal capacitado en esta área relativamente nueva de las ciencias informáticas.

Recuperar datos en Windows con Recuva



Para recuperar datos en Windows **usaremos un programa llamado Recuva**, creado por los mismos desarrolladores que otras herramientas útiles que CCleaner o Defraggler, Piriform.

Para poder hacerlo en primer lugar tenemos que descargar Recuva de su página web oficial e instalarlo. Cuando lo hayamos hecho, abrimos el programa y nos encontraremos con un asistente.

Si pulsamos *Siguiente* en la pantalla de bienvenida, accederemos a otra ventana en la que veremos **qué tipos de archivo queremos recuperar**. Esto nos permitirá filtrar si queremos recuperar cualquier tipo de archivo, archivos de música, imágenes o vídeo. Pulsamos en siguiente y se nos pedirá que elijamos dónde tenemos que buscar esos archivos borrados. Después de esto, el programa ya estará listo para empezar.

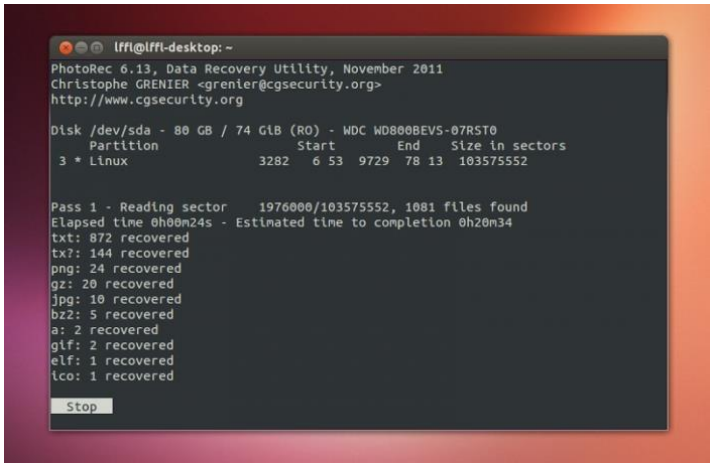
El proceso tardará un rato, pero cuando termine debería **mostrarnos una lista de archivos** con un código de colores al lado de cada uno: verde para archivos fáciles de recuperar, amarillo para recuperaciones intermedias y rojo para archivos díficiles de recuperar. Elegimos los archivos que queremos recuperar, elegimos la ubicación donde los guardaremos y aceptamos. Con esto ya sería suficiente.

Disk Drill, la solución para OS X

Si tienes un Mac y necesitas recuperar datos borrados, entonces **lo que necesitas es Disk Drill**. Funciona de forma muy similar a Recuva, sólo que en lugar de mostrar el estado de recuperación de los datos borrados mediante un código de colores, lo hará mediante una columna con texto situada a la derecha.

El programa cuenta con **una versión gratuita y una de pago**, así que si quieres probarla no dudes en descargar Disk Drill y darle una oportunidad.

Photorec te ayuda a recuperar datos en Ubuntu



Photorec es un programa gratuito que se puede descargar desde los repositorios de Ubuntu y que funciona desde la terminal. Para poder conseguirlo abre una terminal e introduce este comando:

```
sudo apt-get install testdisk
```

Con este paquete instalaremos también Photorec. Este programa **funciona desde la terminal**, y para ejecutarlo tendremos que usar este comando:

```
sudo photorec
```

Cuando lo hagamos nos mostrará una pantalla donde tendremos que **elegir en qué disco duro vamos a recuperar los datos**. Lo seleccionamos presionando ENTER, y después tendremos que elegir la partición en la que se encuentran esos datos. A continuación nos preguntará en qué tipo de partición se va a realizar la

búsqueda, y por último tendremos que elegir si vamos a realizar la búsqueda sólo en el espacio en blanco o en todo el disco duro.

Por último elegimos **en qué carpeta se recuperarán los archivos borrados** –por defecto es /home–. A partir de aquí empezará el proceso de recuperación propiamente dicho.

La recuperación consumirá más o menos tiempo dependiendo del tamaño del disco, y cuando termine **habrá recuperado todos los archivos borrados**, no tendremos posibilidad de elegir.

Recuperación de datos de forma física

Todo lo anterior nos sirve perfectamente si hemos borrado los datos por accidente, pero *¿qué pasa si el disco ha sufrido un accidente?* Supongamos que la unidad se nos cae mientras la instalamos en un *slot* nuevo, que sufre un cortocircuito durante una tormenta o que hace los famosos "clics de la muerte". Lo único que podemos hacer es **acudir a una empresa especializada en recuperar datos de discos duros**.

Un ejemplo de este tipo de empresas es Kroll Ontrack, que dispone de **servicios para empresas y para ámbitos domésticos**. En estos lugares existen talleres especializados con salas limpias que garantizan que los discos se pueden abrir sin peligro, ya que con que caiga una simple mota de polvo en la superficie los daños serían catastróficos.

El proceso normal que se sigue en estas empresas pasa por **evaluar las causas de la avería, evaluar el tipo de reparación y recuperar los datos**, y sin duda se trata de la mejor opción si el disco sufre algún tipo de avería física.

El futuro del disco duro:

Actualmente la nueva generación de discos duros utiliza la tecnología de grabación perpendicular (PMR), la cual permite mayor densidad de almacenamiento.
También existen discos llamados "Ecológicos" los cuales hacen un uso más eficaz de la energía.

Se está empezando a observar que la unidades de estado sólido posiblemente terminen sustituyendo al disco duro a largo plazo.

También hay que añadir los nuevos discos duros basados en el tipo de memorias flash, que algunas empresas, como ASUS, incorporó en sus modelos, de 4 GB a 512 GB.

Son muy rápidos ya que no tienen partes móviles y consumen menos energía, todo esto los hace muy fiables y casi indestructibles. Un nuevo formato de discos duros basados en memorias, sin embargo el costo por GB es muy elevado ya que el costo de un disco duro común de500 GB es equivalente a un SSD de 8 a 16 GB.

Conceptos básicos.

Metadatos o metadata:

técnica del espejado o espejeo: También se le conoce con otros nombres como ser "mirroring", esta técnica consiste en hacer una copia bit a bit del disco original, el cual permitirá recuperar en el siguiente paso, toda la información contenida y borrada del disco duro.
Para evitar la contaminación del disco duro, normalmente se ocupan bloqueadores de escritura de hardware para no arriesgar la copia original.
Un ejemplo de una buena práctica forense es hacer 2 copias, en caso de algún accidente o imprevisto no se pierda información vital.
la preservación es fundamental en una buena examinacion digital.

Partición: Una **partición** podríamos decir que es un espacio de uso que asignamos en un disco duro. En cada disco duro podremos hacer varias particiones, de tal modo que todas ellas son en cierto modo **independientes entre sí** y podemos trabajar de manera individual sobre cada una, es decir, los datos que introduzcamos en una de ellas no afectan al espacio de las otras, si borramos los datos de una las demás no sufren variaciones, etc.
A efectos de empleo en una computadora con un solo disco duro, si desde windows abrimos Mi PC y solo vemos una letra de disco (generalmente **C**), podemos entender que "para nuestro uso", ese disco solo cuenta con una partición, si contásemos por ejemplo con dos letras (**C** y **D**) tendríamos dos particiones en ese disco.
Las particiones son un detalle importante a tener en cuenta en nuestros ordenadores, pues nos van a permitir por ejemplo:

Tener instalado el sistema operativo, drivers, programas, etc., en la primera partición.
Guardar archivos personales, música, películas, fotografías, etc., en la segunda partición.
Además de permitirnos tener **organizada nuestra información**, si llegado el caso tenemos que formatear el equipo (borrar y volver a instalar todo), solo borraríamos **C** y **No perderíamos** lo que se encuentre en **D**, que en este caso sería la segunda partición.

Sistema de ficheros: (File System). En computación, un sistema de archivos es un método para el almacenamiento y organización de archivos de computadora y los datos que estos contienen, para hacer más fácil la tarea encontrarlos y accederlos. Los sistemas de archivos son usados en dispositivos de almacenamiento como discos duros y CD-ROM e involucran el mantenimiento de la localización física de los archivos.

Más formalmente, un sistema de archivos es un conjunto de tipo de datos abstractos que son implementados para el almacenamiento, la organización jerárquica, la manipulación, el acceso, el direccionamiento y la recuperación de datos. Los sistemas de archivos comparten mucho en común con la tecnología de las bases de datos.

En general, los sistemas operativos tienen su propio sistema de archivos. En ellos, los sistemas de archivos pueden ser representados de forma textual (ej.: el shell de DOS) o gráficamente (ej.: Explorador de archivos en Windows) utilizando un gestor de archivos.

El software del sistema de archivos se encarga de organizar los archivos (que suelen estar segmentados físicamente en pequeños bloques de pocos bytes) y directorios, manteniendo un registro de qué bloques pertenecen a qué archivos, qué bloques no se han utilizado y las direcciones físicas de cada bloque.

Los sistemas de archivos pueden ser clasificados en tres categorías: sistemas de archivo de disco, sistemas de archivos de red y sistemas de archivos de propósito especial.

Ejemplos de sistemas de archivos
son: FAT, UMSDOS, NTFS, UDF, ext2, ext3, ext4, ReiserFS, XFS, etc.

Unidad Central de Procesamiento(UCP o CPU):

Descripción: El microprocesador o "micro" se encuentra alojado en la placa madre o motherboard , es un circuito electrónico que puede o no ser extraíble.

Función : Realiza todas las funciones aritméticas y lógicas en la computadora. Controla el funcionamiento de la computadora.

Información útil : El dispositivo en sí mismo puede darnos el número de serie utilizando un programa de extracción.

Modelo publicado (2001)

Este modelo de trabajo se publicó en el año 2001 por el U.S. Dep. of Justice (Departamento de justicia de Estados Unidos) y quizás sea el más sencillo. Básicamente existen cuatro elementos clave en un análisis de computadoras. que son:

1. Identificación
2. Conservación
3. Análisis
4. Presentación

Este modelo supuso una de las grandes bases en este campo ya que a partir de estos conceptos clave, varios autores han desarrollado sus modelos para englobar todos los pasos de una investigación forense de computadoras.

Sistemas operativos:

Windows 7, Windows Vista, Windows XP Professional, Windows XP Home, Windows Server 2003, Windows 2000 Professional, Windows 2000 server, Windows NT 4, Windows 98, Windows 95, Windows NT 3.5, Windows ME, Linux, DOS, Solaris on Sparc, Solaris on Intel, Sun OS, Novell Netware, MAC OS, MAC OSX, Cámaras Digitales.

Recuperación de datos a nivel de averías mecánicas: producidas por el desgaste de los componentes micro-mecánicos por golpes, (discos duros que no encienden, fallas en la placa lógica, errores de lectura, discos duros que hacen ruido y no les queda mucho tiempo de vida útil.

daños electrónicos, discos duros dañados debido a subidas de tensión en la red eléctrica, envejecimiento de los componentes electrónicos, descargas eléctricas debido a tormentas, discos irreconocibles en el sistema operativo los cuales no son detectados en el BIOS.

Tipos de información

Datos almacenados: Archivos ofimáticos, archivos de música, videos, fotos.

Datos generados: cookie, historial, cache, log de sistema, chats de redes sociales, envío de correo electrónico.

Formatos de Archivos:

Formatos de datos de entrada soportados

Formatos de almacenamiento de emails:

- EDB,STM (Microsoft Exchange)
- PST,OST (Microsoft Outlook)
- MSG (Microsoft Outlook – ficheros con un solo correo)
- NSF (Lotus Notes / Domino)
- DBX,MBX (Microsoft Outlook Express)
- MBOX (Estándar)
- EML (Estándar, un email por archivo)
- EMLX (Apple Mac OS X Mail.app)

- BOX (Foxmail)
- Hotmail y Yahoo! Mail HTML (extraídos de la caché del explorador)

Protocolos de servidores de email:

- IMAP
- POP
- Novell GroupWise (vía IMAP como una "aplicación de confianza")

Formatos de imagen de disco:

- E01 (EnCase)
- Imágenes en bruto “dd” en un fichero individual

Tipos de sistemas de ficheros:

- NTFS (Microsoft Windows NT)
- FAT32 (MS-DOS, Microsoft Windows)
- Ext2 (Linux)

Formatos de documentos:

- HTML
- Texto plano
- PDF
- DOC,DOT (Microsoft Word)
- XLS,XLT (Microsoft Excel)
- PPT,POT,PPS (Microsoft PowerPoint)
- RTF
- WPS,WKS,XLR (Microsoft Works)
- WPD (Corel WordPerfect)
- CPR,SHW (Presentaciones Corel, Corel SlideShow)
- WK4 (Lotus 1-2-3) *

Formatos de imágenes:

- PNG (Portable Network Graphics)

- JPEG (Joint Photographic Experts Group)
- TIFF (Tagged Image File Format)
- GIF (Graphics Interchange Format)
- BMP (Windows bitmap)
- PBM,PPM,PGM (Portable bitmaps, pixelmaps, greymaps)
- RAW (Imágenes en bruto de cámaras digitales)
- WBMP (Wireless bitmaps)

Formatos de archivos comprimidos:

- ZIP
- GZIP

Otros formatos a comentar:

- Caché del explorador Internet Explorer
- Caché del explorador Mozilla

Las imagénes digitales se pueden guardar en distintos formatos. Cada uno se corresponde con una extensión específica del archivo que lo contiene. Los más utilizados en la actualidad son: BMP, GIF, JPG, TIF y PNG.

BMP (Bitmap = Mapa de bits)

- Ha sido muy utilizado porque fue desarrollado para aplicaciones Windows.
- La imagen se forma mediante una parrilla de píxeles.
- El formato BMP no sufre pérdidas de calidad y por tanto resulta adecuado para guardar imágenes que se desean manipular posteriormente.
- Ventaja: Guarda gran cantidad de información de la imagen.
- Inconveniente: El archivo tiene un tamaño muy grande.

GIF (Graphics Interchange Format = Formato de Intercambio Gráfico)

- Ha sido diseñado específicamente para comprimir imágenes digitales.
- Reduce la paleta de colores a 256 colores como máximo (profundidad de color de 8 bits).
- Admite gamas de menor número de colores y esto permite optimizar el tamaño del archivo que contiene la imagen.
- Ventaja: Es un formato idóneo para publicar dibujos en la web.

- Inconveniente: No es recomendable para fotografías de cierta calidad ni originales ya que el color real o verdadero utiliza una paleta de más de 256 colores.

JPG-JPEG (Joint Photographic Experts Group = Grupo de Expertos Fotográficos Unidos)

- A diferencia del formato GIF, admite una paleta de hasta 16 millones de colores.
- Es el formato más común junto con el GIF para publicar imágenes en la web.
- La compresión JPEG puede suponer cierta pérdida de calidad en la imagen. En la mayoría de los casos esta pérdida se puede asumir porque permite reducir el tamaño del archivo y su visualización es aceptable. Es recomendable utilizar una calidad del 60-90 % del original.
- Cada vez que se modifica y guarda un archivo JPEG, se puede perder algo de su calidad si se define cierto factor de compresión.
- Las cámaras digitales suelen almacenar directamente las imágenes en formato JPEG con máxima calidad y sin compresión.
- Ventaja: Es ideal para publicar fotografías en la web siempre y cuando se configuren adecuadamente dimensiones y compresión.
- Inconveniente: Si se define un factor de compresión se pierde calidad. Por este motivo no es recomendable para archivar originales.

TIF-TIFF (Tagged Image File Format = Formato de Archivo de Imagen Etiquetada)

- Almacena imágenes de una calidad excelente.
- Utiliza cualquier profundidad de color de 1 a 32 bits.
- Es el formato ideal para editar o imprimir una imagen.
- Ventaja: Es ideal para archivar archivos originales.
- Inconveniente: Produce archivos muy grandes.

PNG (Portable Network Graphic = Gráfico portable para la red)

- Es un formato de reciente difusión alternativo al GIF.
- Tiene una tasa de compresión superior al formato GIF (+10%)
- Admite la posibilidad de emplear un número de colores superior a los 256 que impone el GIF.
- Debido a su reciente aparición sólo es soportado en navegadores modernos como IE 4 o superior.

Existen multitud de formatos para comprimir las imágenes digitales, aunque son tres los más utilizados: JPG (ó JPEG), GIF y PNG. Normalmente, las cámaras digitales guardan las imágenes en JPG, el más empleado para las fotografías. Para

cambiar su tamaño, resolución o formato hay que emplear un editor de imágenes, como Photoshop o Paint Shop Pro. Para elegir el formato adecuado para una imagen hay que valorar su contenido (fotografía, gráfico, etc.), la calidad (dependiendo de su destino: impresión en papel, publicación en web...) y el tamaño del archivo.

Formatos para la Web

- **GIF**
  El Graphic Interchange Format o GIF fue creado por Compuserve. GIF emplea el algoritmo de compresión LZW (Lempel Ziv Welch) para reducir el peso de la imagen sin pérdida de datos. La forma más sencilla de reducir el tamaño de un archivo GIF es disminuir el número de colores.

Es un formato masivamente empleado en Internet, pues es ideal para gráficos, dibujos, iconos o imágenes de muy pocos colores (soporta sólo hasta 256 colores) o con grandes áreas del mismo color. Es decir, es bueno para todo excepto para las fotografías. Además es el único formato que permite realizar animaciones (sin entrar en técnicas más complejas como el *flash*) y, en su versión GIF89a, soporta transparencias -la parte transparente de la imagen adoptará el color del fondo de la página donde se coloca- e interlineado, que hace que la imagen se vea rápidamente en el navegador a baja resolución, hasta que se descarga por completo.

- **JPG**
  JPEG (siglas de Joint Photographic Experts Group) ó JPG soporta 16,7 millones de colores (24 bits) y es el más empleado (y adecuado) para las fotografías. Al contrario que GIF, su algoritmo de compresión elimina información de la imagen, por lo que cuanto más se comprime más se aprecia la pérdida de calidad (es posible ajustar el grado de compresión).

El algoritmo de comprensión con pérdida utilizado por JPG hace que al descomprimir una imagen no se obtenga exactamente lo mismo que teníamos antes de la compresión. Y esa pérdida se acumula: cada vez que se abre y se vuelve a guardar la imagen se comprime y va perdiendo calidad (los datos perdidos son irrecuperables). Por eso, a la hora de almacenar una fotografía que se tiene pensado editar, es preferible hacerlo en un formato sin pérdidas (BMP o TIFF). Después se puede guardar la versión final en JPG para que ocupe menos espacio.

- **PNG**
  Este formato fue desarrollado para superar las limitaciones del GIF. Utiliza también un algoritmo de compresión sin pérdidas y no está sujeto a las patentes que pesan sobre el empleo del GIF. El formato permite imágenes con color verdadero, escala de grises y paleta de 8 bits. Al igual que el GIF es adecuado para imágenes con pocas variaciones de colores.

Otros formatos

- **BMP.** El BitMaP es el formato nativo del sistema operativo Windows deMicrosoft y el más simple de todos: define los valores de cada pixel, uno a uno, de abajo a arriba y barriendo las líneas de izquierda a derecha. Los datos se pueden comprimir, pero esta opción casi nunca se emplea. Su gran problema es que genera archivos enormes.

  TIFF (Tagged-Image File Format) o TIF. Formato propiedad de Adobe Systems empleado para intercambiar archivos (fotografías, fundamentalmente) entre distintas aplicaciones y plataformas (sirve tanto para PC como para Macintosh). Comprime las imágenes sin pérdida de calidad pero el peso de los archivos no lo convierte en un formato óptimo para almacenar gran cantidad de fotos o enviarlas por correo electrónico.

- **PSD**. Formato utilizado por el popular editor de imágenes Photoshop. No utiliza compresión y se emplea para guardar la imagen durante el proceso de edición, pues mantiene toda la información sobre capas sin acoplar.
- **PCX.** Formato creado por ZSoft para los programas de dibujo Paintbrush. Los datos están comprimidos con un algoritmo llamado RLE.

¿Cuál elegir?La regla general dice que JPG es el mejor formato para las fotografías o cualquier imagen que pierda calidad con menos de 256 colores. Para el resto, gráficos, textos o combinaciones de ambos, GIF o PNG ofrecen la mejor relación calidad - peso del archivo. Cualquiera de estos tres formatos son indicados para publicar imágenes en páginas web o enviarlas por correo electrónico.Para fotografía de alta calidad se puede emplear la compresión sin pérdida del TIFF. De hecho, hay cámaras digitales de gama alta en las que se pueden grabar las fotos en este formato, aunque ocupan un 80% más que si se guardan en JPG.
Colores: En función del número de colores de la imagen, para pintarla serán necesarios más o menos bits por píxel (puntos o elementos de la imagen). Normalmente el número de colores es de 16, 256 -aunque con el formato GIF se ponen los que se quieran entre 2 y 256-, 65.536 (alta densidad) y 16,7 millones (color verdadero).El número de colores aumentará el peso de la imagen: hacen falta 4 bits por píxel para 16 colores, 8 bits para 256 y 16 bits por píxel para el color verdadero (*True Color*). Una imagen en modo CMYK (Cian, Magenta, Amarillo y Negro), utilizada para la impresión en cuatricomía, alcanza los 68,7 millones, 32 bits por píxel.

Usos principales: Captura imágenes y/o video en un formato digital que es

Fácilmente transferible a una computadoras para visualizar o editar.

Información Potencial

- - Imágenes.

- - Sellos de fecha y hora.

- - Carretes/Tarjetas de memoria.

- - Video.

- - Sonido.

Dispositivos Portátiles (Asistentes Digitales Personales) [PDAs],

Agendas Electrónicas

Descripción: Un asistente digital personal (PDA) es un computador de mano

Originalmente diseñado como agenda electrónica. Hoy en día se puede usar como una

Computadora doméstica (ver películas, crear documentos, navegar por Internet...).

Usos Primarios: Computación de mano, almacenamiento y comunicación.

Información almacenada:

- - Libreta de direcciones.

- - agenda personal

- - Documentos.

- - E-mails.

- - Passwords.

- - Libreta de teléfonos .

- - Mensajes de texto.

- - Mensajes de voz.

Tarjetas de Memoria

Descripción: Dispositivos electrónicos de almacenamiento extraíbles, que no

Pierden la información cuando no se suministra con corriente de la tarjeta. Estas tarjetas

Suelen tener una memoria de tipo flash, aunque en algunos casos, como en las

compactFlash, se le puede incluir un minidisco duro, que aunque almacena más

Información, es más sensible a los golpes y consume más energía. Se usan en una

Variedad de dispositivos como cámaras digitales, MP3s, PDAs, ordenadores, etc.

Algunos ejemplos son:

- CompactFlash (CF) I y II
- Memory Stick (MS)
- MicroSD
- MiniSD
- Multi Media Card (MMC)
- Secure Digital (SD)
- SmartMedia Card (SM/SMC)
- xD-Picture Card

Usos principales: Proporciona métodos adicionales extraíbles para el

almacenamiento y transporte de información.

Conclusión Final:

La realizacion de este curso, señala la falta de unicidad de criterios y procedimientos, que puedan ser implementados en la practica de recuperacion de datos.

La informacion disponible al respecto de esta area es numerosa, y las problematicas son variadas, tanto a nivel mecanico-electronico como a nivel de software, sin mencionar la diversidad de formatos que puede adoptar la informacion buscada.

En el presente trabajo se reunen conocimientos variados provenientes de diferentes fuentes e idiomas, la integracion de estos datos nos provee flexibilidad a la hora de enfrentar y brindar soluciones a multiples clases de fallas en dispositivos de almacenamiento.

Con el empleo de la metodologia propuesta se cuenta con una herramienta sistematica, que permite realizar un analisis y estudio minucioso de los archivos de manera eficaz y confiable.

En el presente trabajo en vez de utilizar la exclusion del software libre optè por la complementacion, debido a que en mi experiencia ninguna herramienta es mejor que todas las demàs, utilizar las mejores caracteristicas de diferentes herramientas existentes asegura la confiabilidad del procedimiento.

A la vez que el proceso a nivel individual se encuentra en constante refinamiento, comparando metodos vs resultados, seleccionando las herramientas adecuadas de acuerdo al caso en particular.

Lo cual requiere flexibilidad en el manejo de conceptos y experiencia practica, asi como un profundo entendimiento de los multiples factores involucrados en la naturaleza del problema.

La experiencia que adquirì con el paso de los años en la reparacion y mantenimiento de computadoras, me permitio estar mas conciente de la necesidad del presente trabajo.

La creacion de este curso a sido pensado en el contexto de generar nueva informacion y presentar una metodologia mucho mas practica asì como multidisciplinaria, en un contexto de una Sociedad digital y de la Informaciòn.

Profesor: Federico Sebastián Alcoba

Mes de Septiembre del año 2017

Bibliografía:

*Casey, E. (2000). Digital Evidence and Computer Crime: Forensic Science, Computers and the

Internet. San Diego, CA: Academic Press.

*Icove, D., Seger, K., & VonStorch, W. (1995). Computer Crime. O'Reilly & Associates.

*Kruse, W. G., & Heiser, J. G. (2001). Computer Forensics: Incident Response Essentials .

Addison Wesley.

*Masters, G., & Turner, P. (2007). Forensic Data Recovery aand Examination of Magnetic

Swipe Cloning Devices. Digital Investigation , 4 (1), 16-22.

Robbins, J. (2008). An Explanation of Computer Forensics. Retrieved April 9, 2008, from

http://computerforensics.net/forensics.htm

*Stallings, W. (2003). Cryptography and Network Security 3/e. Prentice Hall.

*Turner, P. (2007). Applying a Forensic Approach to Incident Response, Network Investigation

and System Administration using Digital Evidence Bags. Digital Investigation , 4 (1), 30-35.

*Turner, P. (2006). Selective and Intelligent Imaging Using Digital Evidence Bags. Digital

Investigation , 3 (1), 59-64.

US-CERT. (2005). Computer Forensics. US-CERT , 1 (2).

*Wang, S.-J. (2007). Measures of Retaining Digital Evidence to Prosecute Computer-Based

Cyber-Crimes. Computer Standards & Interfaces , 29 (2), 8.

[1] Computer Forensics: Computer Crime Scene Investigation, John R. Vacca,

Charles River Media © 2002 (731 paginas) ISBN:1584500182

[2] An Extended Model of Cybercrime Investigations, de Séamus Ó Ciardhuáin,

International Journal of Digital Evidence Summer 2004, Volume 3, Issue 1

[3] Electronic Crime Scene Investigation: A guide for first responders, U.S.

Department of Justice

[4] Report From the First Digital Forensic Research Workshop (DFRWS),

Agosto de 2001, Utica, New Cork

[5] An Examination of Digital Forensic Models, de Mark Reith, Clint Carr, Gregg

Gunsch, International Journal of Digital Evidence Fall 2002, Volume 1, Issue 3

[6] Getting Physical with the Digital Investigation Process, de Brian Carrier y Eugene

H. Spafford, International Journal of Digital Evidence Fall 2003, Volume 2, Issue 2

[7] Digital Evidence and Computer Crime: Forensic Science, Computers, and

the Internet, Segunda edición, por Eoghan Casey, Academic Press 2004,

http://www.datarecovercenter.co/Servicios/Informatica-Forense/Auditoria-e-Investigacion-Forense/Historia-de-la-Informatica-Forense

"Seguridad en las Comunicaciones y en la Información", G. Díaz Orueta y otros. Ed. UNED

"Hackers 2". J. Scambray, S. McClure y G. Kurtz. ED. Osborne-McGraw-Hill.