INSTITUTO NACIONAL DE CIBERSEGURIDAD

ANÁLISIS FORENSE DIGITAL

Unidad 3 – Medios de Almacenamiento

universidad de león

MINISTERIO DE DEFENSA

SAPROMIL

MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

INDICE

incibe_

INSTITUTO NACIONAL DE CIBERSEGURIDAD

universidad de león

MINISTERIO DE DEFENSA

SAPROMIL

MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

1. Medios físicos y sus particularidades: Discos duros, HDD y SSD

❑Medios físicos de almacenamiento

Hacemos referencia a físico para distinguir la técnica de memorización de la información de la abstracción lógica, que venimos llamando sistema de ficheros.

Los medios físicos son los dispositivos, que bien mediante tecnología electrónica, memorias flash y discos SSD, magnética, discos duros HDD tradicionales u óptica, CD's y DVD's, son capaces de almacenar y recuperar información digital.

A efectos de la forensia digital conviene conocer ciertos aspectos de cada una de las tecnologías, que pueden tener impacto en el la recuperación de datos, la ocultación de estos así como en el cálculo de integridad.

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

1. Medios físicos y sus particularidades: Discos duros, HDD y SSD

❑Discos duros HDD

Hacemos referencia a físico para distinguir la técnica de memorización de la información de la abstracción lógica, que venimos llamando sistema de ficheros.

Los medios físicos son los dispositivos, que bien mediante tecnología electrónica, memorias flash y discos SSD, magnética, discos duros HDD tradicionales u óptica, CD's y DVD's, son capaces de almacenar y recuperar información digital.

A efectos de la forensia digital conviene conocer ciertos aspectos de cada una de las tecnologías, que pueden tener impacto en el la recuperación de datos, la ocultación de estos así como en el cálculo de integridad.

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

1. Medios físicos y sus particularidades: Discos duros, HDD y SSD

❑Discos duros HDD

Aunque es la tecnología “saliente”, muchos términos y conceptos están asociados a esta.

La información se guarda orientando partículas magnéticas que se distribuyen en pistas concéntricas a lo largo de la superficie de cada cara de cada disco.

La pista mas externa es la denominada pista 0 y tiene especial relevancia por ubicar información relevante para el funcionamiento del sistema.

En cada operación de lectura/escritura, el dispositivo puede leer o escribir un mínimo de información. Ese mínimo es lo que denominamos tamaño de bloque o sector. Es un valor físico determinado por la construcción del disco. Habitualmente toma el valor de 512 bytes.

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

1. Medios físicos y sus particularidades: Discos duros, HDD y SSD

❑Discos duros HDD

- ✓ Pistas, divididas en sectores o bloques (físicos)
- ✓ Bloque o sector (físico)
- ✓ Clúster o bloque lógico. Agrupación de bloques o sectores.
- ✓ Primer bloque o sector de la pista 0, de especial relevancia por almacenar configuración de la configuración del disco. Primeros 512 bytes.

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

1. Medios físicos y sus particularidades: Discos duros, HDD y SSD

❑Discos SSD

- ✓ Utilizan puertas lógicas, es decir, electrónicas, para almacenar datos digitales.
- ✓ La tecnología flash permite dar persistencia a los datos memorizados en las celdas NAND.
- ✓ Emula en todo lo posible a los discos magnéticos, por lo que los conceptos de bloques y clusters son vigentes, así como el primer bloque de 512 bytes.
- ✓ Realiza procesos de mantenimiento, debido a la vida limitada de las celdas flash, intenta repartir las operaciones de escritura de una forma homogénea. Para ello, realiza un proceso denominado “Trim”, que consiste en el borrado de la información almacenada en celdas no usadas, para disponer de ellas en caso de necesitar reubicar información.
- ✓ Esto es de vital importancia en las técnicas forenses, porque:
  - ✓ Elimina datos de forma definitiva e irrecuperable, con el simple hecho de suministrar corriente eléctrica, independientemente de bloqueadores hw o sw.
  - ✓ Modifica el contenido de una imagen bit a bit del disco, y por lo tanto una comprobación básica de integridad como un hash, nos daría indicios de haber modificado el contenido copiado.

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

1. Medios físicos y sus particularidades: Discos duros, HDD y SSD

❑Discos Ópticos

- ✓ Utilizan una superficie que de forma permanente es modificada para reflejar o no la luz de un emisor laser y memorizar de este modo datos binarios.
- ✓ Algunas de estas tecnologías permiten la reescritura de información, pero en ningún caso de forma tan ágil como los discos SSD o HDD, por lo que los dispositivos ópticos son prácticamente de sólo lectura, y están en otro orden en relación a los discos antes mencionados.
- ✓ A efectos forenses, carecen de la relevancia de los anteriores discos, por no ser habitual encontrar trazas de un sistema operativo o de la actividad de un usuario.

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

1. Medios físicos y sus particularidades: Discos duros, HDD y SSD

❑Cintas magnéticas

- ✓ Utilizan la célula magnética como principio para el almacenaje de información.
- ✓ Ofrecen buena capacidad y precio, pero no pueden competir con los discos en velocidad de acceso, ya que son de acceso secuencial, al contrario de los discos que son de acceso aleatorio.
- ✓ Por el motivo anterior, tampoco encontraremos información de interés para el análisis forense, más allá de los propios ficheros almacenados, copias de seguridad, etc...

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

1. Medios físicos y sus particularidades: Discos duros, HDD y SSD

❑Interfaces físicos de los discos HDD y SSD

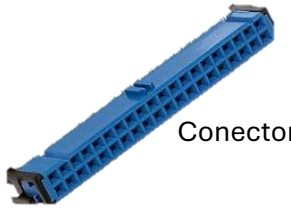
La importancia de conocer los interfaces radica en la necesidad de acceder a estos dispositivos para clonarlos. Parte del kit de clonado siempre es el set de cables para el acceso a estos diversos interfaces, que deberemos mantener actualizados ante modificaciones o incorporaciones.

Es importante mencionar que el trabajo de un analista forense se parece al del personal de emergencias, cuando no está interviniendo en una, debe de estar preparándose para la siguiente.

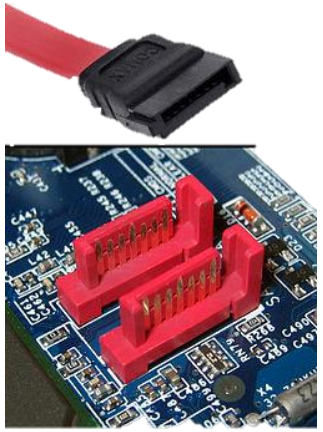
UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

1. Medios físicos y sus particularidades: Discos duros, HDD y SSD

❑Interfaces físicos de los discos HDD y SSD



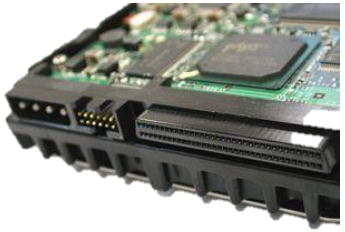
Conector IDE



Conector SATA

- ✓ ATA o IDE: Interface obsoleto, paralelo, de 40 pin.
- ✓ SATA o serial ATA: El más habitual en entorno PC.
- ✓ SCSI: Interface de bus para entorno de servidores, empresarial. Paralelo.
- ✓ SAS o Serial SCSI: La evolución de SCSI en puerto serie, de entorno empresarial.

Conector SAS



Conector SCSI

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

1. Medios físicos y sus particularidades: Discos duros, HDD y SSD

Unidad SSD M.2

❑Interfaces físicos de los discos HDD y SSD

- ✓M.2: Interface SSD sustituto de SATA y que encontraremos en portátiles y dispositivos móviles y tablets.
- ✓PCIe (NVMe): Interface de expansión que ahora se usa para la conexión de almacenamiento SSD, de modo que debemos ser conectar estos dispositivos para su clonado.
- ✓USB 3.0: Interface serie multiusos, al que podemos adaptar otros para conectarnos a nuestra estación de clonado.

Unidad SSD PCIe

Conector USB 3.0

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

2. Organización lógica del almacenamiento: Sistemas de ficheros. EXT y NTFS.

❑Master Boot Record, MBR (I)

- ✓ El espacio de los discos lo podemos usar de forma única o realizar “particiones”, que son divisiones lógicas de la capacidad física.
- ✓ La función de las particiones puede ser muy variada:
  - Disponer de distintos sistemas de ficheros.
  - Separar datos de usuario de binarios
  - Limitar el uso de almacenamiento por un determinado programa/usuario
  - Flexibilizar el reparto de espacio.
  - Administrar seguridad, aplicando cifrado a nivel de sistema de ficheros.
  - Etc…
- ✓ Para establecer las particiones con la que configuramos los discos, existen dos opciones: MBR y GPT.

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

2. Organización lógica del almacenamiento: Sistemas de ficheros. EXT y NTFS.

❑Master Boot Record, MBR (II)

- ✓ Es el sistema tradicional y que aún se encuentra muy extendido.
- ✓ Reserva los primeros 512 Bytes del disco, Pista 0, sector 1, para guardar información sobre la configuración de particiones en la denominada tabla de particiones. Esta área del disco no pertenece a ninguna partición.
- ✓ Debido a esos escasos 512 bytes, tiene limitaciones en cuanto al número de particiones que admite, en concreto cuatro particiones primarias.
- ✓ Admite una firma de 32 bits, que usa el SO para identificar el dispositivo HW.
- ✓ También contiene el Master Boot Code, cuya funcionalidad es identificar el primer clúster de la partición activa y cargar el boot loader del SO si existe.

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

2. Organización lógica del almacenamiento: Sistemas de ficheros. EXT y NTFS.

❑Master Boot Record, MBR (III)

✓ Podemos hacer una copia de la MBR en Linux, con el comando:

```
dd if=dev/xxx of=mbr.bak bs=512 count=1
```

✓ De cada partición primaria, se dispone de la siguiente información:

Layout of 16-byte Partition Record

Offset	Description
0x00	Status (0x80 = bootable, 0x00 = non-bootable, other = malformed)
0x01	**Cylinder-head-sector** address of the first sector in the partition
0x04	**Partition type**
0x05	Cylinder-head-sector address of the last sector in the partition
0x08	(4 bytes) **Logical block address** of the first sector in the partition
0x0C	(4 bytes) Length of the partition, in sectors

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

2. Organización lógica del almacenamiento: Sistemas de ficheros. EXT y NTFS.

❑Master Boot Record, MBR (IV)

- ✓ El interés forense de la MBR viene por recuperar datos borrados, en caso de haberse borrado la tabla de particiones como mecanismo antiforense, así como entender y poder ofrecer evidencias de la configuración del disco y particiones booteables.
- ✓ No hay datos de la actividad de usuario en la MBR, más allá de su borrado o manipulación.

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

2. Organización lógica del almacenamiento: Sistemas de ficheros. EXT y NTFS.

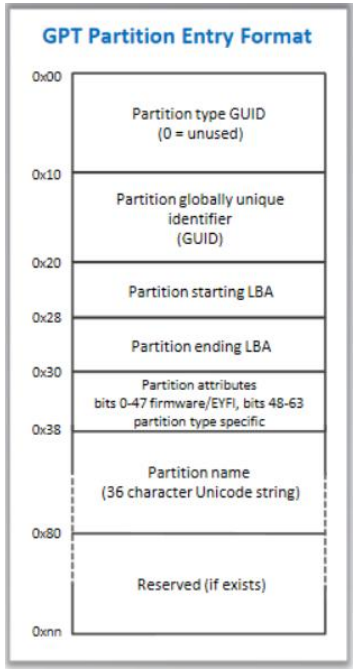
❑Global Unique Identifier o GUID

- ✓ De forma genérica, se denomina así a un identificador único de objeto, pudiendo ser este un usuario, una librería, una sesión o un dispositivo, entre otros.
- ✓ De forma específica, el estándar EFI, Extensible Firmware Interface, define el sistema de particionado GPT y como clave en este, los identificadores de cada partición, que son cadenas de 128 bit de longitud. Este sistema de nombrado está definido por Microsoft.
- ✓ Se escriben en formato hexadecimal, entre llaves, divididos en cinco conjuntos, el primero representa 4 bytes, los tres siguientes 2 cada uno, y 6 bytes la secuencia restante:

```
{936DA01F-9ABD-4d9d-80C7-02AF85C822A8}
```

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

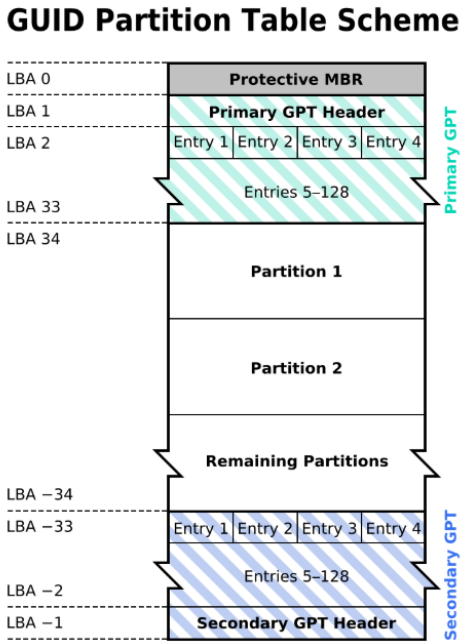
2. Organización lógica del almacenamiento: Sistemas de ficheros. EXT y NTFS.



Estructura de cada entrada de partición GPT

❑Global Unique Identifier Partition Table o GPT (I)

- ✓ Es el sistema actual de establecer las particiones en una unidad de almacenamiento.
- ✓ Elimina las limitaciones de número de particiones, hasta 128, y tamaño máximo de estas, hasta 18 exabytes.
- ✓ Ocupa los primeros 32 bloques de 512 bytes, 16 KB, y los 32 últimos como redundancia, guardando en el primero un "Protective MBR" para que el disco pueda ser accedido aún si el sistema no soporta GPT.
- ✓ Asigna un GUID tanto al disco como a cada una de las particiones.
- ✓ La entrada por cada partición ocupa 128 bytes.



UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

2. Organización lógica del almacenamiento: Sistemas de ficheros. EXT y NTFS.

❑ BIOS y UEFI

Es importante comprender el proceso de arranque de un sistema operativo, para poder confirmar y evidenciar desde qué sistema de ficheros ha arrancado un dispositivo o qué alteraciones se han podido realizar como medidas antiforense.

Asimismo nos será útil al analizar un dispositivo dañado que no sea arrancable.

Disponemos de dos sistemas, el tradicional BIOS: Basic Input Output System, asociado con MBR, por el que básicamente mediante el firmware del dispositivo se busca en la mbr de los discos disponibles particiones arrancables, y en el caso de encontrarlas, se provee de un mecanismo para cargar el “Partition boot code” a la memoria y cederle el control. Este será el responsable de cargar el “loader” del sistema operativo. No es capaz de acceder a sistemas de ficheros como tal, sólo a ciertas ubicaciones predeterminadas del disco.

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

2. Organización lógica del almacenamiento: Sistemas de ficheros. EXT y NTFS.

❑ BIOS y UEFI (ii)

Y por otro lado, disponemos del UEFI, Unified Extensible Firmware Interface, un moderno sistema cuyo fin es dejar atrás el obsoleto e inseguro arranque por BIOS y MBR.

Básicamente, UEFI es capaz de cargar aplicaciones UEFI ubicadas en los sistemas de ficheros de las particiones, teniendo que ser del tipo FAT (12, 16 o 32). Estas aplicaciones pueden ser drivers, utilidades o cargadores del SO.

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

2. Organización lógica del almacenamiento: Sistemas de ficheros. EXT y NTFS.

❑Organización lógica de información

Sobre el soporte físico, se estable una organización lógica, que permite:

- ✓ Asignar bloques o sectores a agrupaciones lógicas, clúster o bloques lógicos.
- ✓ Asignar estos clústeres a ficheros, de manera que se pueda guardar la información que lo representa en esos clústeres.
- ✓ Saber qué clústeres están en uso o están disponibles para guardar información.
- ✓ Conocer en todo momento el contenido del sistema de ficheros, con sus nombres, fechas de creación, modificación y acceso (Fechas MAC).

Adicionalmente, a un sistema de ficheros se le pueden pedir prestaciones extra, como:

- ✓ Journaling o bitácora de operaciones, que permite cierta tolerancia a fallos, al registrar las operaciones realizadas antes de que se lleven a acabo.
- ✓ ACL's sobre ficheros, para controlar las operaciones que sobre él puede hacer un determinado usuario.
- ✓ Cuotas, que permiten controlar la cantidad de información que guarda un determinado usuario en el sistema de ficheros.

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

2. Organización lógica del almacenamiento: Sistemas de ficheros. EXT y NTFS.

❑Distintos sistemas de ficheros

Existen distintos sistemas para dotar de las funcionalidades mencionadas, algunos vinculados a la naturaleza del dispositivo y otros dependientes de los SSOO que los utilizan.

- ✓ Para dispositivos ópticos: ISO 9660 y UDF entre otros.
- ✓ Para discos HDD y SSD en SSOO Windows: FAT, NTFS.
- ✓ Para discos HDD y SSD en SSOO Linux: EXT, BTRFS, entre otros muchos.
- ✓ Para discos HDD y SSD en SSOO Apple: HFS+, APFS.

Con la finalidad del análisis forense, nos interesa en primer lugar, NTFS, por tratarse de un sistema que ofrece muchas prestaciones y por lo tanto aporta mucha información, además de estar muy implantado por ser el estándar utilizado en Windows, y en segundo lugar EXT y HFS+ por ser los segundos más implantados.

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

2. Organización lógica del almacenamiento: Sistemas de ficheros. EXT y NTFS.

❑File Allocation Table – FAT (I)

- ✓ Es un sistema muy utilizado, incorporado por MS-DOS, sencillo y de prestaciones limitadas en comparación con sistemas más modernos.
- ✓ Aún así, es utilizado actualmente para el arranque UEFI así como en dispositivos extraíbles.
- ✓ Está soportado por prácticamente la totalidad de SSOO.
- ✓ Existen distintas versiones, FAT12, 16 y 32 bits, que indican la capacidad de almacenar direcciones de clusters, bloques lógicos, y por lo tanto, de la capacidad máxima del volumen.
- ✓ Se basa en la llamada tabla FAT, que se almacena al principio del volumen, y que almacena los datos relativos a los clúster y su contenido.

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

2. Organización lógica del almacenamiento: Sistemas de ficheros. EXT y NTFS.

❑File Allocation Table – FAT (III)

✓ Un volumen o sistema de ficheros FAT consta de tres áreas:

- RESERVED AREA: El primer sector, 512 bytes, llamado Volume Boot Record, VBR, dónde se guarda información sobre el tipo de volumen y en su caso, parte del código de arranque del SSOO.
- FAT AREA: Almacena la tabla FAT, por duplicado.
- DATA AREA: Los clúster con el contenido de datos.

✓FAT ofrece como metadatos, nombre, tipo, MAC, y atributos de sólo lectura, oculto, sistema y archivo.

Detalle del contenido de VBR FAT

Byte Offset (in Hex)	Field Length	Sample Value	Meaning
00	3 bytes	EB 3C 90	Jump instruction
03	8 bytes	MSDOS5.0	OEM name in text
0B	25 bytes		BIOS Parameter Block (BPB)
24	26 bytes		Extended BIOS parameter block
3E	448 bytes		Bootstrap code
1FE	2 bytes	0x55AA	End of the sector marker

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

2. Organización lógica del almacenamiento: Sistemas de ficheros. EXT y NTFS.

❑File Allocation Table – FAT (IV)

- ✓ Para cada fichero o directorio, la FAT almacena una entrada de 32 bits.
- ✓ Además almacena para cada cluster, el valor “next”, que indica el siguiente clúster, EOF o clúster erróneo.
- ✓ El borrado de un fichero en FAT consiste en la sustitución por un guión bajo del primer byte, es decir el primer carácter del nombre del fichero. Esto es relevante de cara a la recuperación de ficheros borrados.

Entrada de fichero/directorio fat

Byte Range	Description
0 – 0	First character of file name in ASCII and allocation status (0xe5 or 0x00 if unallocated)
1 – 10	Characters 2 to 11 of file name in ASCII
11 – 11	File Attributes
12 – 12	Reserved
13 – 13	Created time (tenths of second)
14 – 15	Created time (hours, minutes, seconds)
16 – 17	Created day
18 – 19	Accessed day
20 – 21	High 2 bytes of first cluster address (0 for FAT12 and FAT16)
22 – 23	Written time (hours, minutes, seconds)
24 – 25	Written day
26 – 27	Low 2 bytes of first cluster address
28 – 31	Size of file (0 for directories)

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

2. Organización lógica del almacenamiento: Sistemas de ficheros. EXT y NTFS.

❑New Technology File System– NTFS (I)

- ✓ Es un sistema introducido con Windows NT y el adoptado cómo estándar por los SSOO Windows.
- ✓ Actualmente está en su versión 5.1
- ✓ Ofrece prestaciones adicionales a FAT, como journaling, compresión, cuotas, permisos de usuario, auditoría, alternate data stream (ADS) y cifrado.
- ✓ Al igual que en FAT, el primer sector del volumen incluye la información sobre el tipo de partición.
- ✓ Adicionalmente reserve hasta 16 sectores para metadatos del arranque.
- ✓ NTFS se soporta en una serie de ficheros a modo de base de datos, para almacenar los datos necesarios para las prestaciones indicadas. Algunos de ellos se consideran Artifacts vitales en el análisis forense.

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

2. Organización lógica del almacenamiento: Sistemas de ficheros. EXT y NTFS.

❑New Technology File System– NTFS (II)

Ficheros de metadatos de un volumen NTFS

File Name	Description
$attrdef	Contains definitions of all system-and user-defined attributes of the volume
$badclus	Contains all the bad clusters
$bitmap	Contains bitmap for the entire volume
$boot	Contains the volume's bootstrap
$logfile	Used for recovery purposes
$mft	Contains a record for every file
$mftmirr	Mirror of the MFT used for recovering files
$quota	Indicates disk quota for each user
$upcase	Converts characters into uppercase Unicode
$volume	Contains volume name and version number

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

2. Organización lógica del almacenamiento: Sistemas de ficheros. EXT y NTFS.

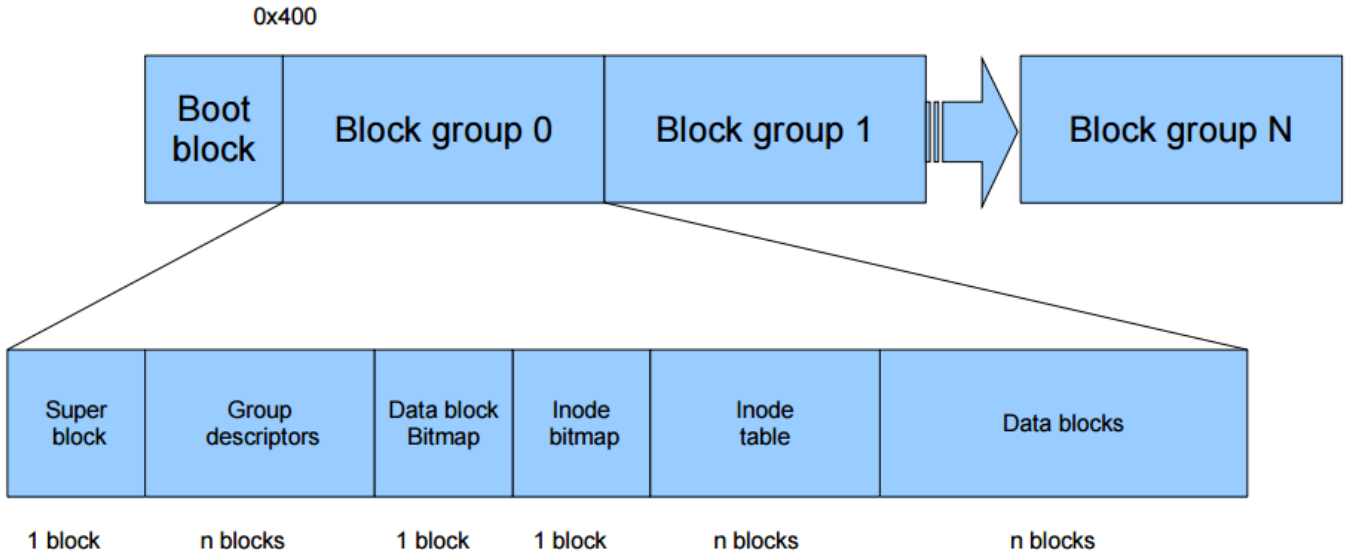
❑Estructura del file system EXT

- ✓ La estructura es muy distinta a FAT o NTFS, tratándose de una estructura distribuida, en vez de una única tabla o BBDD maestra.
- ✓ Los sectores se organizan en bloques lógicos y a su vez en grupos. Cada grupo de bloques tiene sus propios metadatos, funcionando como un sistema de ficheros independiente.
- ✓ Cada fichero es representado por un “inodo”, que almacena todos los metadatos y la relación de bloques que lo conforman.
- ✓ Por cada grupo se almacena bitmap con los bloques disponibles, un bitmap con el conjunto de inodos y una tabla de estos inodos..
- ✓ El “Superbloque”, de 1024 bytes, que dispone de información sobre la partición, tamaño de bloque, número de grupos y ubicación, etc… De este superbloque se guarda una copia en varios grupos de bloques, como redundancia.

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

2. Organización lógica del almacenamiento: Sistemas de ficheros. EXT y NTFS.

- Estructura del file system EXT2

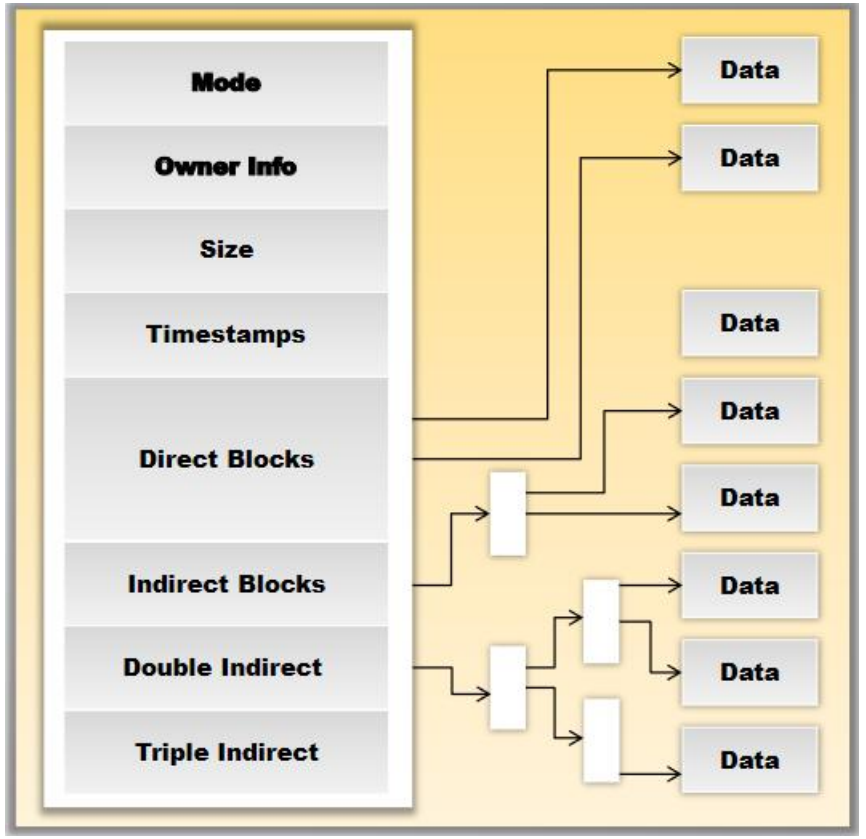


UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

2. Organización lógica del almacenamiento: Sistemas de ficheros. EXT y NTFS.

❑Estructura de un inodo Ext2

- ✓ Cada inodo representa a un directorio o fichero, con los metadatos de este, fechas MAC, permisos, tamaño, nombre, links, y los bloques de datos que lo contienen.
- ✓ Como particularidad en forense, el borrado de un fichero implica su puesta a cero en tamaño y en la dirección de bloques en su inodo, por lo que la recuperación "rápida" no existe en sistemas Ext, siendo sólo posible el carving.

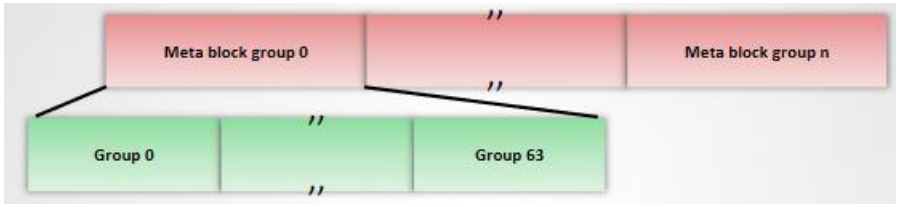


UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

2. Organización lógica del almacenamiento: Sistemas de ficheros. EXT y NTFS.

❑Ext3, Ext4

- ✓ La filosofía del resto de sistemas Ext es similar, aunque se van añadiendo funcionalidades:
- ✓ Ext3 incluye journaling, mayores tamaños de file system, mayor integridad y velocidad.
- ✓ Ext4 soporta aún mayores tamaños de files system y de fichero, hasta 1 EiB y 16 TiB respectivamente.
- ✓ Ext4 introduce un sistema de extensión del tamaño de ficheros que reduce la fragmentación.
- ✓ Ext4 introduce el concepto de Metablock group, un nivel más de agregación:4



UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

2. Organización lógica del almacenamiento: Sistemas de ficheros. EXT y NTFS.

❑Otros sistemas de ficheros

- ✓ Nos hemos ocupado de los sistemas más habituales. Una vez conocidas las particularidades de estos, veremos que podemos investigar nuevos sistemas buscando los mismos artifact que nos pueden proporcionar información sobre la actividad.
- ✓ En ciertos casos, grandes almacenamientos en RAID, o bien buscamos herramientas específicas o podemos justificar la adquisición a nivel de fichero.

El conocimiento de los sistemas de ficheros es fundamental para hacer recuperación manual y también para entender los resultados de herramientas automáticas, así como abordar el análisis de otros sistemas menos conocidos.

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

3. Particularidades del NTFS. $MFT y $LOG. Extracción de estos ficheros.

❑Particularidades NTFS

- ✓ NTFS ofrece mucha funcionalidad y por lo tanto muchos artefactos.
- ✓ El artefacto mas relevante es el fichero $MFT, del que podremos obtener información de archivos presentes en el sistema de ficheros, fechas MAC, fechas de modificación de metadatos, existencia de “Alternate Datastream” (ADS), si se trata de un fichero eliminado, etc… en un instante de tiempo.
- ✓ Adicionalmente podremos analizar los cambios en el sistema de ficheros mediante los metadatos de journaling, $UsnJrnl y $LogFile.
- ✓ El ADS nos permite identificar información interesante cómo origen de descarga en los ficheros descargados, versiones anteriores o buscar información estenografiada con este método.

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

3. Particularidades del NTFS. $MFT y $LOG. Extracción de estos ficheros.

❑Master File Table – MFT (I)

- ✓ Es el archivo clave dentro del sistema NTFS.
- ✓ Contiene una entrada por cada fichero, incluidos los propios ficheros de metadatos del sistema.
- ✓ Las primeras 16 entradas de la MFT corresponden con los 16 ficheros “especiales” del volumen NTFS.
- ✓ Cada entrada de fichero dispone de una serie de atributos, que pueden estar guardados en la propia entrada, para ficheros pequeños, en cuyo caso se denominan “residentes” o pueden estar almacenados fuera de la MFT, en cuyo caso se denominan, no residentes.
- ✓ En el borrado de ficheros, se marca en la MFT la entrada como “borrado” y se identifican los clúster como disponibles, por lo que podremos encontrar en la MFT la referencia a los ficheros borrados con su “timestamp”, lo que tiene relevancia en el entorno forense.

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

3. Particularidades del NTFS. $MFT y $LOG. Extracción de estos ficheros.

❑Master File Table – MFT (II)

- ✓ Por defecto, se reserva un 12,5% del espacio del volumen para la MFT, que ocupara un mínimo de 1KB por fichero o directorio que contenga..
- ✓ La MFT se almacena en un fichero binario, siendo necesario un “parser” para extraer los datos.
- ✓ MFTeCMD es un analizador gratuito muy utilizado para esta labor, permitiendo extraer la salida en formato csv.
- ✓ Se puede descargar de https://github.com/EricZimmerman/MFTECmd

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

3. Particularidades del NTFS. $MFT y $LOG. Extracción de estos ficheros.

❑Alternate Data Stream - ADS

- ✓ Esta característica de NTFS permite asociar a un fichero, es decir, a una entrada de la MFT, distintos orígenes de datos, es decir, distintos clúster. ¿Un mismo nombre de fichero para contenidos distintos?¿para qué?.
- ✓ Windows lo usa en los ficheros descargados de Internet, y nos dá información sobre el origen y detalles de la descarga.
- ✓ Hay usos adicionales legítimos, pero es una prestación que también puede ser usada de forma maliciosa, para ocultar información.
- ✓ Podemos acceder al ADS identificando primero el nombre de dicho ADS, mediante el comando `dir /r` e invocándolo con el comando `more`.

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

3. Particularidades del NTFS. $MFT y $LOG. Extracción de estos ficheros.

❑Registros de cambios (Journaling) – Ficheros $UsnJrnl y $LogFile

- ✓ El journaling es el registro de la actividad del sistema de ficheros, con la finalidad de reconstrucción en caso de no finalizar las operaciones correctamente.
- ✓ USN es el acrónimo de Update Sequence Number.
- ✓ El $Usnjrnl se encuentra en \$Extend y dispone de dos ADS. El $J es en el que tenemos los registros de la actividad. Dispone de información adicional sobre el motivo del cambio en el sistema de ficheros.
- ✓ El $LogFile se encuentra en el directorio raíz.
- ✓ Una herramienta gratuita para parsear el fichero y encontrar las operaciones sobre una determinada entrada de la MFT es NTFS Log Tracker v1.4, que permite parsear ambos ficheros.

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

3. Particularidades del NTFS. $MFT y $LOG. Extracción de estos ficheros.

❑Adquisición de artefactos de NTFS

- ✓ Todos los artefactos son ficheros del mismo sistema de ficheros.
- ✓ Podremos adquirirlos tanto de la máquina víctima en una adquisición en caliente, mediante FTK Imager.
- ✓ Asimismo, podremos obtenerlos de una imagen forense, accediendo a ella mediante el mismo FTK Imager.
- ✓ En caso de sólo disponer de un volcado de RAM, algunos artefactos de NTFS se pueden obtener de la memoria, como la propia $MFT, mediante la herramienta volatility.

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

4. Concepto de “Artifact”

En Digital Forensic hablamos de “artifacts” para distinguir los datos, el contenido como tal de un dispositivo, documentos, correos, bases de datos, etc… de las evidencias de la actividad del usuario, lo que en el forense tradicional serían “las huellas”.

https://www.vestigeltd.com/thought-leadership/digital-forensics-content-vs-artifacts-whats-difference/

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

5. Las instantáneas de volumen en Windows

❑Concepto de “instantánea”

- ✓ Es una tecnología de almacenamiento que permite crear copias de seguridad consistentes del estado de un volumen.
- ✓ Consisten en marcar en un instante dado un volumen consistente como sólo lectura, guardando a partir de ahí los cambios aparte. De este modo tendremos distintas versiones del volumen completo:
  - La correspondiente a la instantánea.
  - La versión “actual” del volumen, que es la instantánea aplicando los cambios almacenados.
- ✓ Se realizan a nivel de bloque, no a nivel de fichero, y se hacen de un volumen completo.
- ✓ Se pueden realizar de forma automática o manual.

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

5. Las instantáneas de volumen en Windows

❑Windows Volume Shadow Copy Service (VSS)

- ✓ Windows proporciona el servicio de creación de instantánea mediante el servicio VSS.
- ✓ Se generan, en los clientes, de forma automática en forma de puntos de restauración.
- ✓ En los Servidores, se pueden programar como parte del plan de copia de seguridad.
- ✓ En Windows podemos administrar las shadow copies mediante la cli vssadmin.
- ✓ En concreto, con el comando `vssadmin list shadows`, podemos listar las instantáneas disponibles.
- ✓ Las instantáneas están accesibles como dispositivo a través de la ruta `\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopyX`
- ✓ Con el comando `mklink /d` podemos hacerlas accesibles para su análisis, además de con herramientas específicas forenses, como OSForensic, o X-Way Forensics.

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

6. Las instantáneas de volumen en Linux

❑LVM, Logical Volume Manager

- ✓ Linux soporta distintos sistemas de ficheros, y algunos de ellos ofrecen el servicio de instantánea de forma nativa, como BTRFS.
- ✓ En el caso de sistemas EXT se usa un servicio adicional por debajo, el LVM.
- ✓ El funcionamiento es el explicado anteriormente, y una vez habilitado el servicio, podemos crear y acceder a las instantáneas:

```
lvcreate --size 1G --snapshot --name snap_home /dev/vg0/home
mount /dev/vg0/snap_home /mnt/snapshot
```

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

7. Recuperación de información de medios físicos. Carving. Herramientas

❑El editor hexadecimal

- ✓ Es importante la distinción de un fichero de texto a uno binario.
- ✓ Los primeros, los representamos con los caracteres que corresponden al contenido binario, usando para ello una tabla de correspondecia nº->carácter.
- ✓ Existen múltiples tablas y por lo tanto codificaciones, siendo ASCII las más básica y primitiva, y que es la base para las codificaciones actuales.
- ✓ Los segundos, dado que no tienen representación en caracteres, los analizamos en su representación hexadecimal, por lo conveniente de este sistema de numeración para expresar números binarios.
- ✓ Entender un editor hexadecimal es importante para visualizar ficheros binarios, volcados de memoria, capturas de red, etc...

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

7. Recuperación de información de medios físicos. Carving. Herramientas

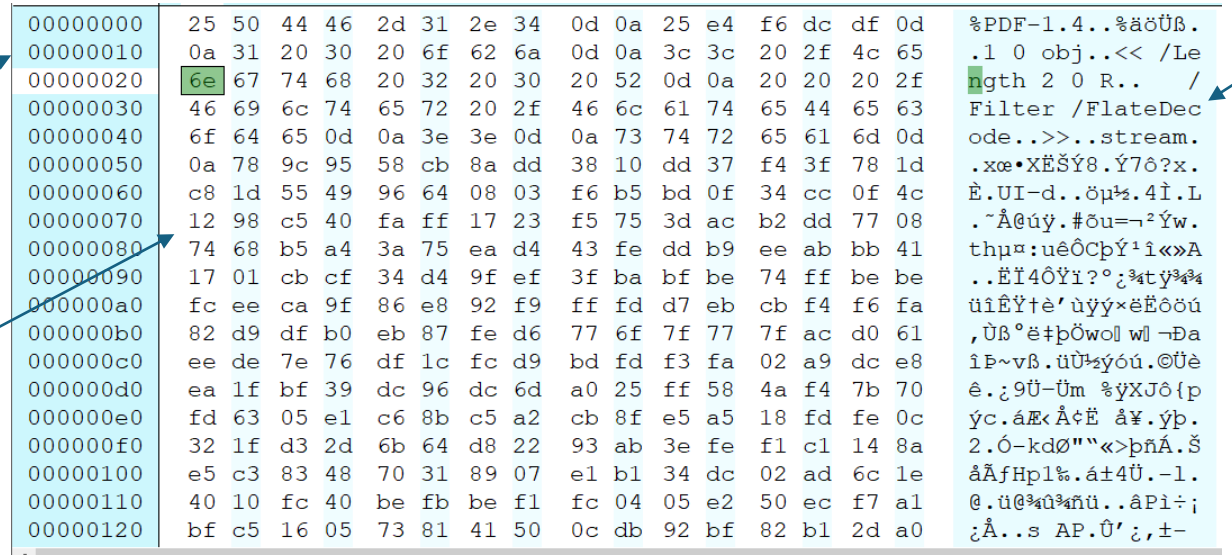
❑El editor hexadecimal (ii)

Área de datos del editor hexadecimal NEO

Columna de dirección u offset.

Columna de datos en representación Hex

Columna de interpretación como texto ASCII



00000000	25	50	44	46	2d	31	2e	34	0d	0a	25	e4	f6	dc	df	0d	%PDF-1.4..%äöÜß.
00000010	0a	31	20	30	20	6f	62	6a	0d	0a	3c	3c	20	2f	4c	65	.1 0 obj..<< /Le
00000020	6e	67	74	68	20	32	20	30	20	52	0d	0a	20	20	20	2f	ngth 2 0 R.. /
00000030	46	69	6c	74	65	72	20	2f	46	6c	61	74	65	44	65	63	Filter /FlateDec
00000040	6f	64	65	0d	0a	3e	3e	0d	0a	73	74	72	65	61	6d	0d	ode..>>..stream.
00000050	0a	78	9c	95	58	cb	8a	dd	38	10	dd	37	f4	3f	78	1d	.xœ•XËŠÝ8.Ý7ô?x.
00000060	c8	1d	55	49	96	64	08	03	f6	b5	bd	0f	34	cc	0f	4c	È.UI–d..öµ½.4Ì.L
00000070	12	98	c5	40	fa	ff	17	23	f5	75	3d	ac	b2	dd	77	08	.˜Å@úÿ.#õu=¬²Ýw.
00000080	74	68	b5	a4	3a	75	ea	d4	43	fe	dd	b9	ee	ab	bb	41	thµ¤:uêÔCþÝ¹î«»A
00000090	17	01	cb	cf	34	d4	9f	ef	3f	ba	bf	be	74	ff	be	be	..ËÏ4ÔŸï?°¿¾tÿ¾¾
000000a0	fc	ee	ca	9f	86	e8	92	f9	ff	fd	d7	eb	cb	f4	f6	fa	üîÊŸ†è'ùÿý×ëËôöú
000000b0	82	d9	df	b0	eb	87	fe	d6	77	6f	7f	77	7f	ac	d0	61	‚Ùß°ë‡þÖwo wa ¬Ða
000000c0	ee	de	7e	76	df	1c	fc	d9	bd	fd	f3	fa	02	a9	dc	e8	îÞ~vß.üÙ½ýóú.©Üè
000000d0	ea	1f	bf	39	dc	96	dc	6d	a0	25	ff	58	4a	f4	7b	70	ê.¿9Ü–Üm %ÿXJô{p
000000e0	fd	63	05	e1	c6	8b	c5	a2	cb	8f	e5	a5	18	fd	fe	0c	ýc.áÆ‹Å¢Ë å¥.ýþ.
000000f0	32	1f	d3	2d	6b	64	d8	22	93	ab	3e	fe	f1	c1	14	8a	2.Ó-kdØ"“«>þñÁ.Š
00000100	e5	c3	83	48	70	31	89	07	e1	b1	34	dc	02	ad	6c	1e	åÃƒHp1‰.á±4Ü.-l.
00000110	40	10	fc	40	be	fb	be	f1	fc	04	05	e2	50	ec	f7	a1	@.ü@¾û¾ñü..âPì÷¡
00000120	bf	c5	16	05	73	81	41	50	0c	db	92	bf	82	b1	2d	a0	¿Å..s AP.Û'¿‚±-

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

7. Recuperación de información de medios físicos. Carving. Herramientas

❑El editor hexadecimal (iii)

La columna de dirección u offset nos indica el byte de comienzo de la línea en relación al total del fichero. En el caso del ejemplo, la primera línea empieza en 0 y la segunda en $(10)_{16}$,es decir, en el byte 16.

Cada carácter hexadecimal representa 4 bits. En la primera línea tenemos 32 caracteres hex, o lo que es lo mismo, 128 bits, o 16 bytes, del 0 al 15.

En la columna de datos, tenemos la secuencia de ceros y unos convertida a hexadecimal, 128 bits, o 32 hexadecimales.

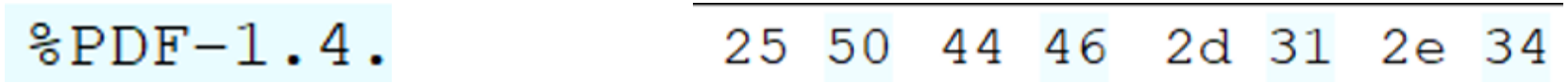
Por último, en la columna de interpretación como texto, el editor busca la correspondencia de cada 8 bits con su carácter de la tabla ASCII, por lo que nos presentará 16 caracteres. Si la información origen es texto, total o parcialmente, aparecerán cadenas legibles.

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

7. Recuperación de información de medios físicos. Carving. Herramientas

❑Tipos de ficheros

- ✓ Acostumbramos a distinguir el tipo de fichero por la extensión, que se corresponde con la cadena de texto que aparece a la derecha del punto en el nombre del fichero.
- ✓ Este tipo de identificación es precaria, ya que es fácilmente modificable.
- ✓ Sin embargo, todos los ficheros contienen un campo de firma o de cabecera (o ambos), que nos permiten identificar de qué tipo de fichero se trata. Este valor se conoce como "**Magic number**" y no sigue un estándar para todos los ficheros.
- ✓ En el caso del ejemplo, en la columna de texto, vemos que la primera línea comienza por unos caracteres, %PDF-1.4, o en hexadecimal, 25 50 44 46 2d 31 2e 34. Los primeros 8 bytes son la cabecera, en la que se indica que es un fichero pdf en formato 1.4



UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

7. Recuperación de información de medios físicos. Carving. Herramientas

❑Ficheros de imagen

✓JPEG – Comienza con los caracteres `0xffd8ff` (el 0x indica notación hexadecimal) y a continuación es habitual encontrar la cadena de texto JFIF.

✓BMP – Comienza con los caracteres `0x42 4d` (BM)

✓GIF – Comienza con los caracteres `0x47 49 46` (GIF)

✓PNG – Comienza con los caracteres `0x89 50 4e 47` (%PNG)

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

7. Recuperación de información de medios físicos. Carving. Herramientas

❑Microsoft Office

Utilizan como firma los primeros 8 bytes:

✓DOCX, PPTX, XLSX – Comienzan con los caracteres `0x50 4b 03 04 14 00 06 00`

Puedes consultar la firma para otros ficheros en
https://en.wikipedia.org/wiki/List_of_file_signatures

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

7. Recuperación de información de medios físicos. Carving. Herramientas

❑Recuperación de ficheros

- ✓ Dependiendo de la casuística se usarán una u otra técnica.
- ✓ En el caso de FAT y NTFS, con herramientas sencillas se pueden obtener buenos resultados, siempre que se encuentre intacto el sistema de ficheros.
- ✓ En caso de que el sistema de ficheros esté corrupto, sólo nos queda usar la técnica de “carving”, consistente en la búsqueda de fragmentos de ficheros, recorriendo toda la superficie del disco. Se basa en la búsqueda de patrones como firmas, y reconstrucción de ficheros a partir de estos.
- ✓ En el caso de EXT es prácticamente la única técnica disponible, por los motivos comentados anteriormente.

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

7. Recuperación de información de medios físicos. Carving. Herramientas

❑Herramientas Carving

Las herramientas de carving son independientes del sistema de ficheros, ya que buscan por un tipo de fichero en concreto, con las cabeceras y los pies conocidos de dicho fichero, y los entregan como salida. Además algunas tratan de obtener información del sistema de ficheros que facilite la recuperación (Photorec)

- ✓ Scalpel. Pertenece a la herramienta TSK. Es un fork de Foremost. Muy rápido, pero no el que obtiene el mejor resultado. Lo hay para Windows y para Linux
- ✓ Foremost. Herramienta desarrollada por el ejercito de EEUU, es, junto con Photorec, la que mejores resultados obtiene.
- ✓ Photorec: es la que mejores resultados ofrece, porque no procesa únicamente las cabeceras o pies de los ficheros, sino que procesa todos los bloques. Realiza múltiples comprobaciones basadas en el tamaño del fichero. Es multiplataforma y dispone de un asistente en modo texto. Eso si, es con diferencia la que más tiempo toma en el proceso.

UNIDAD 3 – MEDIOS DE ALMACENAMIENTO

7. Recuperación de información de medios físicos. Carving. Herramientas

❑Otras herramientas

- ✓ Siempre que el sistema de ficheros esté intacto, hay múltiples herramientas que nos ayudan a recuperar ficheros borrados de forma sencilla y eficiente:
- ✓ Recuva, Recover my files, Data Rescue Pc, R-Studio, Disk Digger, etc…

****IMPORTANTE****

En general en análisis forense y en particular en recuperación de datos, es vital tener el sistema de ficheros de origen bloqueado para escritura. Cualquier operación de escritura, por pequeña que sea, puede llevarse por delante justo la información que necesitamos. Por supuesto, la información recuperada ha de ir a otro sistema de ficheros diferente del original .

FIN UNIDAD

Unidad 3
MEDIOS DE ALMACENAMIENTO

INSTITUTO NACIONAL DE CIBERSEGURIDAD

universidad de león

MINISTERIO DE DEFENSA

SAPROMIL

MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES