Computo forense en ambientes Windows

Roberto Gómez Cárdenas
ITESM-CEM
rogomez@itesm.mx

Lámina 1 Dr. Roberto Gómez Cárdenas

Los sistemas de archivos

- Sistema archivos
  - Le indica al sistema operativo como mapear los datos en un disco.
- El tipo de sistema de archivos de un Sistema Operativo determina como se almacenan los datos en el disco.
- Un sistema de archivos esta directamente relacionado a un Sistema Operativo.
- Cuando es necesario acceder a la computadora de un sospechoso para adquirir o inspeccionar datos
  - El analizador forense debe estar familiarizado con la plataforma de la computadora.

Lámina 2 Dr. Roberto Gómez Cárdenas

La secuencia de arranque

- CMOS: Complementary Metal Oxide Semiconductor
  - Computadora almacena la configuración del sistema e información sobre fecha y hora en el CMOS.
    - Cuando la energía del sistema se apaga.
- Basic Input/Output System (BIOS)
  - Contiene programas que llevan a cabo entrada y salida a nivel hardware.

Lámina 3 Dr. Roberto Gómez Cárdenas

La secuencia de arranque

- Proceso de arranque
  - Contenido en una ROM, le indica a la computadora como proceder,
  - Despliega las teclas a presionar para que se abra la pantalla de configuración del CMOS.
- CMOS debe ser modificado para arrancar de un CD o USB con software de forensia.

Lámina 4 Dr. Roberto Gómez Cárdenas

Selección secuencia de booteo

Lámina 5 Dr. Roberto Gómez Cárdenas

Los discos

- Discos están constituidos por uno o más platos.
- Componentes del disco
  - Geometría
  - Cabeza
  - Tracks
  - Cilindros
  - Sectores

Lámina 6 Dr. Roberto Gómez Cárdenas

Componentes de un disco

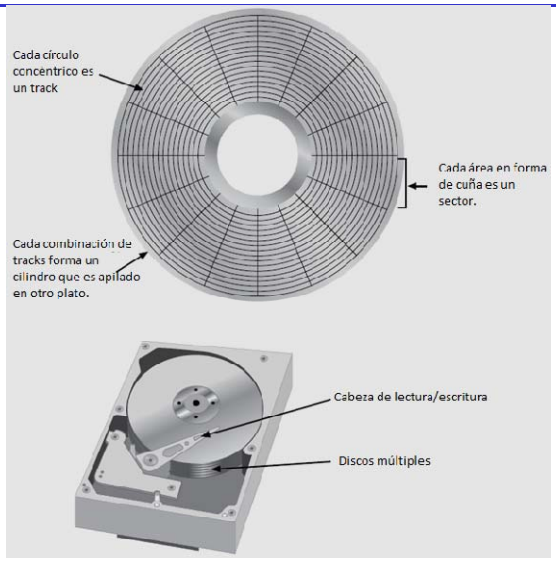


Lámina 7 Dr. Roberto Gómez Cárdenas

Cálculo CHS

CHS:
- Cilindro
- Head
- Sector

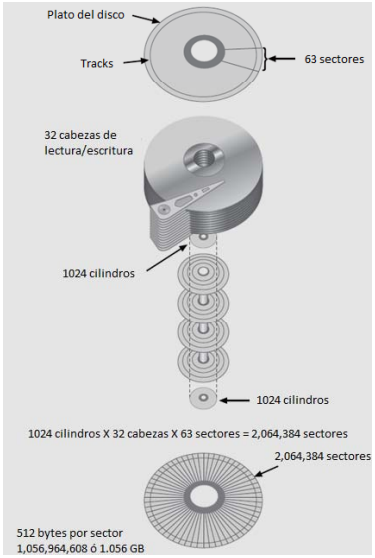


Lámina 8 Dr. Roberto Gómez Cárdenas

Discos

- Propiedades manejadas a nivel del hardware del disco o del firmware
  - ZBR: Zoned Bit Recording
    - Pistas exteriores pueden contener más sectores que las interiores.
    - Definido al formatear el disco.
  - Densidad del track
  - Densidad del área
  - Cabeza

Lámina 9 Dr. Roberto Gómez Cárdenas

Estructura archivos microsoft

- Microsoft agrupa los sectores en grupos denominados clusters.
  - Unidades de asignación de almacenamiento de uno o más sectores.
- Los clusters son típicamente de 512, 1024, 2048, 4096 o más bytes cada uno.
- Combinar sectores minimiza el overhead de la escritura o lectura de archivos en disco.

Lámina 10 Dr. Roberto Gómez Cárdenas

Clusters

- Los clusters son numerados secuencialmente empezado en 2
  - El primer sector de todos los discos contiene un área de sistema, el registro de arranque .
- Sistemas Operativos asigna los números de cluster, llamados direcciones lógicas.
- Los números de sectores son llamados direcciones físicas.
- Los clusters y sus direcciones son específicos a un drive de disco lógico, que es una partición de disco.

Lámina 11 Dr. Roberto Gómez Cárdenas

Particiones discos

- Un partición es un drive lógico.
- FAT16 no reconoce discos más grandes de 2MB
  - Discos más grandes deben ser particionados.
- Particiones escondidas o vacíos.
  - Se cuentan con espacios no utilizados entre las particiones.
- “Partition gap”
  - Espacio no usado entre particiones.

Lámina 12 Dr. Roberto Gómez Cárdenas

Editores de disco

- Utilidad de edición de discos puede alterar información en la tabla de particiones.
  - Para esconder una partición.
- Posible examinar una partición a nivel físico
- Analizar los códigos hexadecimales que el sistema operativo usa para identificar y mantener el sistema de archivos.

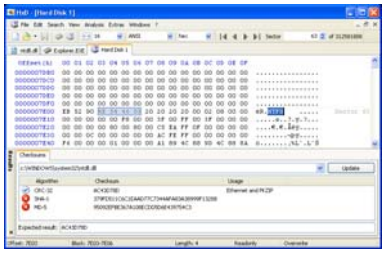


Lámina 13 Dr. Roberto Gómez Cárdenas

Ejemplos editores

Windows Freeware
- HxD
- Roadkil's Sector Editor
- ICY Hexplore
- iBored
- Hex-ed
- Hex-Editor-Neo (shareware)

Linux
- hexedit
- shed (simple hex editor)
- Linux disk editor
- debugfs
- iBored

Windows Comercial
- HHD Software Hex Editor Neo
- Hexprobe Hex Editor
- WinHex
- T-Software Technologies System Console
- Runtime Software Disk Explorer FAT/NTFS
- R-Tools R-Studio

MS-DOS
- Norton Utilities
- Wde disk editor

Mac OS X
- iBored (freeware)

Lámina 14 Dr. Roberto Gómez Cárdenas

Códigos hexadecimales en la tabla de particiones

Código Hexadecimal	Sistema de Archivos
01h	DOS FAT de 12 bits
04h	DOS FAT 16 bits para particiones menores a 32 MB
05h	Partición extendida
06h	DOS FAT 16 bits para particiones mayores a 32 MB
07h	NTFS
08h	Partición booteable de AIX
09h	Partición de datos de AIX
0Bh	DOS 32-bits FAT
0Ch	DOS FAT de 32 bits con soporte de interrupción 13
17	Partición NTFS escondida (XP y después)
1B	Partición FAT32 escondida
1E	Partición VFAT escondida

Lámina 15 Dr. Roberto Gómez Cárdenas

Códigos hexadecimales en la tabla de particiones

Código Hexadecimal	Sistema de Archivos
3C	Partición de recuperación de partition magic
66-69	Particiones Novell
81	Linux
82	Partición swap de Linux
83	Sistema archivo nativo Linux (Ext2, Ext3, Reiser, xlsfs)
86	Volumen FAT16
87	HPFS
A5	FreeBSD y BSD/386
A6	OpenBSD
A9	NetBSD
C7	Típico de un volumen coi
EB	BeOS

Lámina 16 Dr. Roberto Gómez Cárdenas

Primer Ejemplo

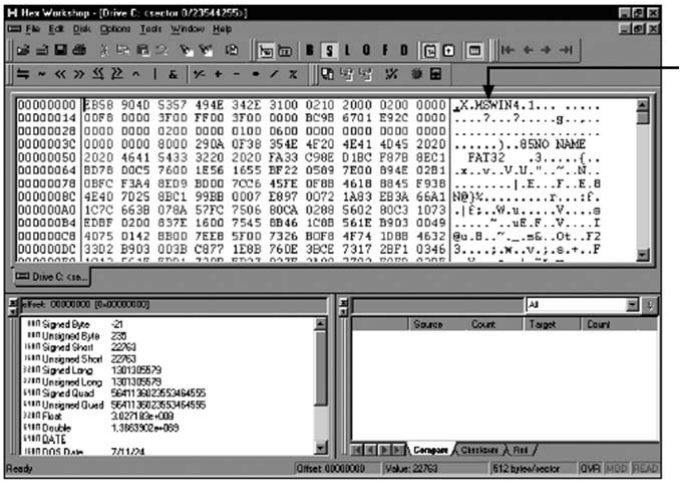


Lámina 17 Dr. Roberto Gómez Cárdenas

Segundo Ejemplo

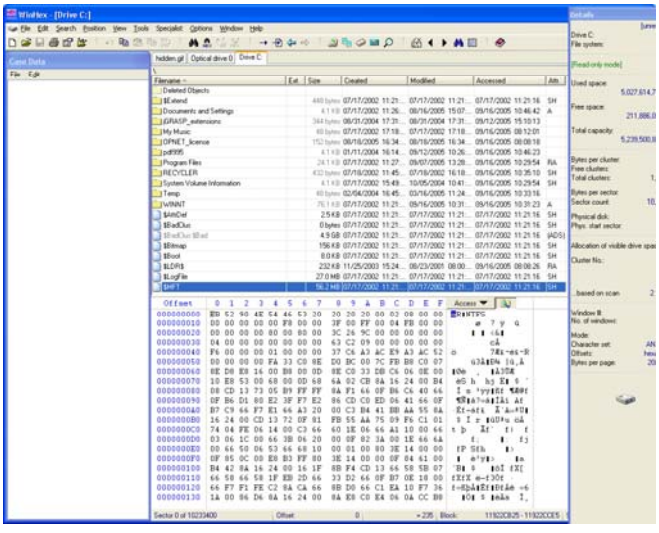


Lámina 18 Dr. Roberto Gómez Cárdenas

Identificando un archivo

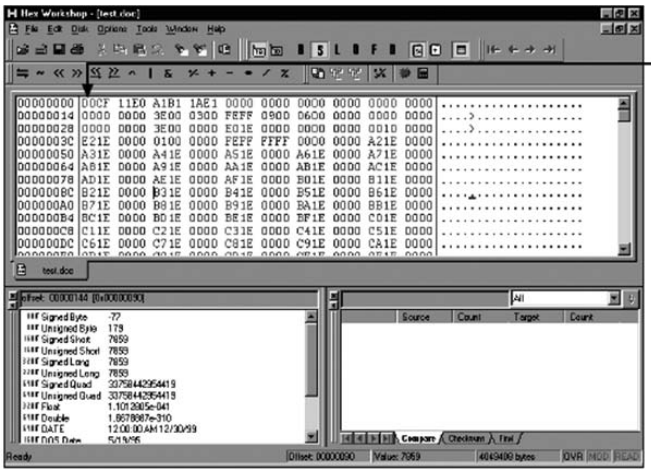


Lámina 19 Dr. Roberto Gómez Cárdenas

Master Boot Record

- Almacena información
  - Ubicación
  - Tamaño
  - Otros
- Algunas aplicaciones pueden modificar el MBR
  - Partition Magic
  - LILO
  - GRUB
  - Puede interferir con tareas de forencia
  - Utilizar más de una herramienta.

Lámina 20 Dr. Roberto Gómez Cárdenas

Discos FAT

- FAT: File Allocation Table
- Originalmente desarrollado para discos flexibles.
- Usado antes Windows NT y 2000
- Típicamente
- Evolución
  - FAT12
  - FAT16
  - FAT32

Lámina 21 Dr. Roberto Gómez Cárdenas

Sectores y bytes por cluster

Tamaño disco	Número Sectores	FAT 16	FAT 32
256-511 MB	16	8 KB	4 KB
512 MD – 1GB	32	16 KB	4 KB
1-2 GB	64	32 KB	4 KB
2-8 GB	8	N/A	4 KB
8-16 GB	16	N/A	8 KB
16-32 GB	32	N/A	16 KB
Más de dos 32GB	64	N/A	32 KB

Lámina 22 Dr. Roberto Gómez Cárdenas

Tamaño cluster en FAT16

- El tamaño de los clusters varía de acuerdo al tamaño del disco duro y el sistema de archivos.

Tamaño partición	Sectores por clusters	Tamaño estándar del cluster
0 MB–32 MB	1	512 bytes
33 MB–64 MB	2	1 KB
65 MB–128 MB	4	2 KB
129 MB–255 MB	8	4 KB
256 MB–511 MB	16	8 KB
512 MB–1023 MB	32	16 KB
1024 MB–2047 MB	64	32 KB

Lámina 23 Dr. Roberto Gómez Cárdenas

Asignación espacio en FAT

- Sistema Operativo Microsoft asigna espacio disco para archivos por clusters
  - Resulta en drive slack
    - Espacio no usado en un cluster entre el fin de archivo y el final del cluster
  - El drive slack incluye
    - RAM slack y slack de archivo
- Un efecto colateral no-intencional de FAT16 con clusters grandes era que se reducía la fragmentación.
  - Conforme el tamaño del cluster se incrementa.

Lámina 24 Dr. Roberto Gómez Cárdenas

Slack space

- Slack
  - Diferencia entre el espacio lógico y el espacio físico.
- RAM slack
  - Diferencia entre el fin de archivo y el resto del sector.
- File Slack
  - Los sectores que queddan al final del cluster.
- Resumiendo
  - RAM slack es el slack a nivel byte y sector, mienttras que File slack son los sectores a nivel cluster.

Lámina 25 Dr. Roberto Gómez Cárdenas

Ejemplo slack space

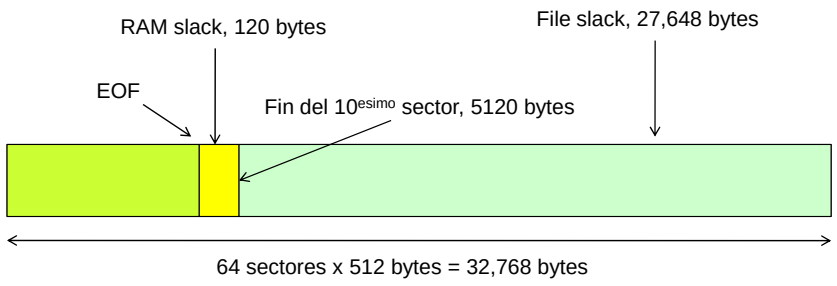


Lámina 26 Dr. Roberto Gómez Cárdenas

Cluster chaining

- Cuando se acaba el espacio para un cluster asignado.
  - Sistema operativo asigna otro cluster al archivo, el cual crea más slack space en el disco.
- Cluster chaining
  - Conforme crece el archivo y requiere más espacio en disco, los clusters son encadenados.
  - La cadena puede ser rota o fragmentada.

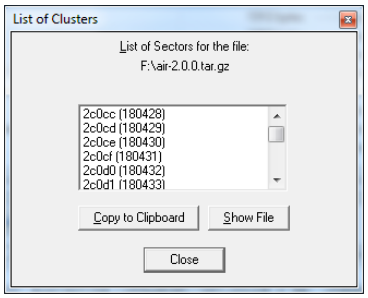


Lámina 27 Dr. Roberto Gómez Cárdenas

Borrado archivos en FAT

- Cuando un archivo se borra
  - La entrada en el directorio es marcada como un archivo borrado.
    - Con el carácter $E5_{16}$ reemplazando la primera letra del nombre del archivo.
    - La cadena FAT para dicho archivo se pone en cero.
- Los datos permanecen en el disco.
- El área del disco donde residía el archivo se convierte en espacio de disco no asignado.
  - Disponible para recibir nuevos datos de archivos creados, o de otros archivos que requieren de más espacio.

Lámina 28 Dr. Roberto Gómez Cárdenas

Ejemplo tabla asignación archivos

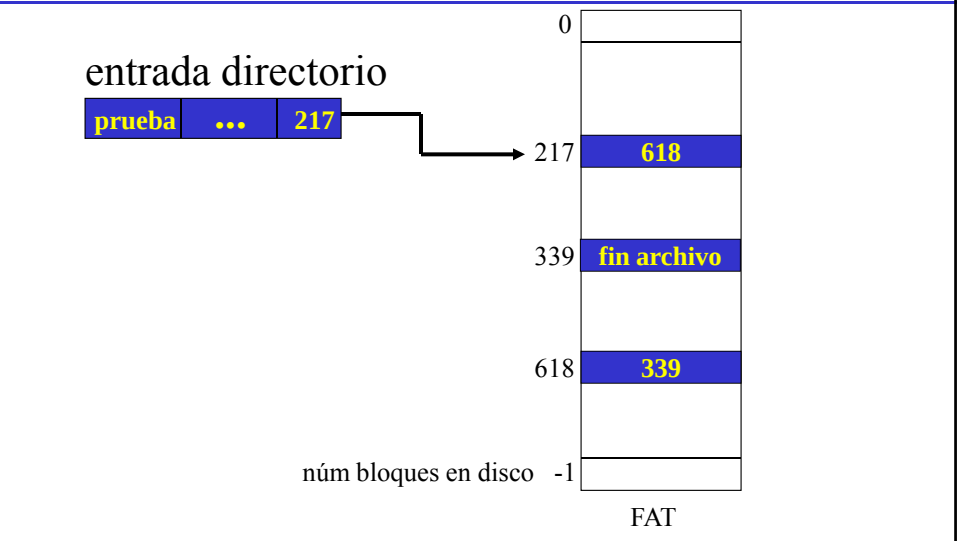


Lámina 29 Dr. Roberto Gómez Cárdenas

Asignando bloques nuevso a un archivo

- Basta con encontrar la primera entrada de la tabla que valga cero:
  - sustituir el valor de fin de archivo anterior por la dirección del nuevo bloque
  - a continuación el cero se sustituye por el valor de fin-de-archivo

Lámina 30 Dr. Roberto Gómez Cárdenas

Estructura de un volumen

- El registro de booteo (MBR), el cual siempre es el primer sector.
- Las areas donde se ubica el FAT: usualmente son dos identicas.
- El directorio raíz
- El área de datos

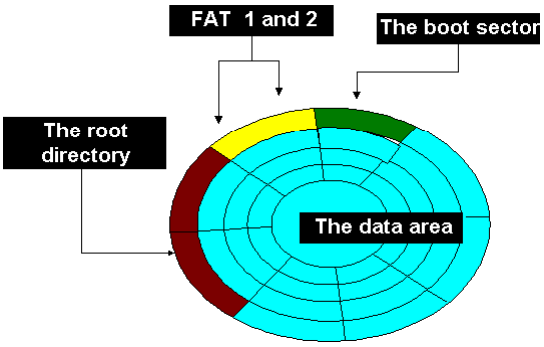


Lámina 31 Dr. Roberto Gómez Cárdenas

El MBR: Master Boot Record

- Primer sector del disco o sector de arranque principal
- Consta de tres partes:
  - El código de booteo:
    - del byte 1 al 446 (es lo que ejecuta el BIOS)
  - La tabla de particiones del disco:
    - mini lista de las particiones del disco
  - El número mágico AA55:
    - byte 511: 55
    - byte 512: AA
    - identifica a este sector como un sector de arranque

Lámina 32 Dr. Roberto Gómez Cárdenas

La Tabla de Archivos (FAT)

- Después del MBR sigue la tabla de archivos (FAT)
- Generalmente hay dos tablas, una de respaldo
- Consiste de una tabla de números
  - tiene 65,536 entradas
  - cada entrada contiene información acerca de un cluster en forma de un número.

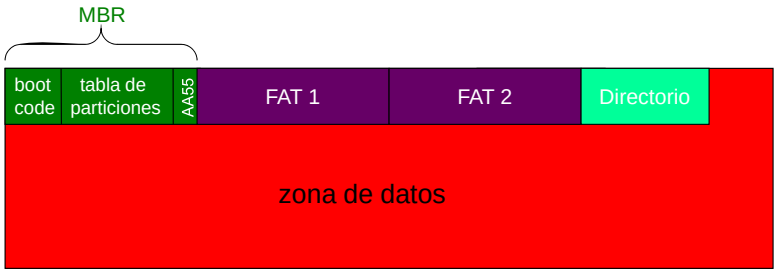


Lámina 33 Dr. Roberto Gómez Cárdenas

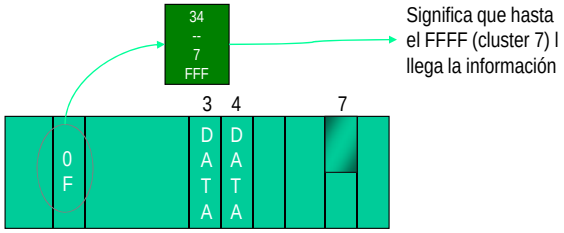
Posibles valores de los clusters en la tabla

Valor en la entrada de la Table	**Significado**
FFFF	El cluster es parte de un archivo y el último
xxxx (p.e. 18FA)	El cluster es parte de un archivo, el siguiente cluster es el xxxx (18FA)
0000	El cluster esta vacío y por lo tanto disponible.
FFF7	El cluster contiene sectores defectuosos, es marcado como malo.

Lámina 34 Dr. Roberto Gómez Cárdenas

Ejemplos

En el 1er registro de la tabla está mi primera información



Puros 111...111 significa fin de información; ya no hay información después de este sector

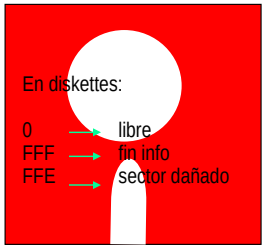


Lámina 35 Dr. Roberto Gómez Cárdenas

El tamaño de FAT

- Cada cluster tiene una entrada en la FAT, el tamaño del área de FAT depende del tamaño del disco.
  - cada entrada en el FAT ocupa 16 bits
- Considerar un disco de 160 MB
- El tamaño máximo del FAT es de 128KB,
  - 16 archivos, 2 bytes c/u: 65,536x2 = 131,072 bytes (128 KB)
  - Hay 40,400 clusters, ya que la partición es de 160 MB
- Se tienen dos FATs:
  - 40,400 x 2 bytes
  - esto nos da un total de 161,600 y eso ocupará 316 sectors

Lámina 36 Dr. Roberto Gómez Cárdenas

¿Y el directorio?

- Es la última área administrativa en el disco.
- Siempre hay 512 entradas de archivos en el directorio
  - es del mismo tamaño para todos los discos duros.
- La estructura del directorio consiste de un número de entradas de directorio.
  - cada entrada ocupa 32 bytes
  - las entradas son idénticas ya sea que estén en el directorio raíz o en algún subdirectorio
  - contienen información como:
    - el nombre del archivo (en el formato 8.3)
    - tamaño del archivo en bytes
    - fecha y hora de la última revisión

Lámina 37 Dr. Roberto Gómez Cárdenas

Estructura del directorio

File name 8 bytes
Extension 3 bytes
Attribute 1 byte
Reserved 10 bytes (FAT32 uses two of them)
TIme 2 bytes
Date 2 bytes
First cluster 2 bytes
File size 2 bytes

- Los 32 bytes están agrupados en secciones
  - válido para todas las secciones, ya sea que se trate de archivos o directorios (directorio raíz y subdirectorios)
- Se cuenta con el número del primer cluster
  - importante ya que a partir de eso empieza a buscar al archivo
  - el primer cluster es leído de la entrada del directorio, los siguientes números de clusters son leídos del FAT
- En discos duros formateados como FAT16 el directorio raíz ocupa 512 entradas, las cuales son de 32 bytes cada una.
  - entonces ocupa 16 KB

Lámina 38 Dr. Roberto Gómez Cárdenas

El área de datos

- El resto del disco alberga la parte más importante, el área de datos, donde todos los archivos y sub directorios son almacenados.
- El área de datos es la parte más grande del disco.
- Los sectores del área de datos están conjuntados en clusters.
- Como se dijo antes, el máximo número de clusters para datos es 216 =65,535
- Si el disco duro es de 160 Mb:
  - se tienen 40,400 clusters de 8 sectores cada uno

Lámina 39 Dr. Roberto Gómez Cárdenas

Un ejemplo de relación tabla particiones y FAT

0	1 - 158	159 - 316	317 - 348	349 - 323.548	Sector number
Boot record	FAT number 1	FAT number 2	Root directory with 512 entries of 32 bytes	Data area divided into 40.400 clusters, each of 8 sectors. First cluster is number 2	Containing

Sector number:	349 - 356	357 - 364	365 - 372	...	323.541 - 323.548
Contains:	Cluster 2	Cluster 3	Cluster 4	...	Cluster 40.400

Lámina 40 Dr. Roberto Gómez Cárdenas

Tipos de FAT

- VFAT
  - para versiones anteriores de Windows 95
- FAT 12
  - sectores de 512 bytes
  - sistema MS-DOS determina tamaño del FAT, basado en el número de clusters
    - si hay 4085 clustes o menos sistema usa tabla FAT-12
    - si hay 4086 o más clusters se utiliza FAT de 16 bits
- FAT 16
  - versiones Microsoft MS-DOS y posteriores permiten a FDISK particionar discos duros de hasta 4 gigabytes
    - sin embargo la tabla solo soporta 2GB por partición

Lámina 41 Dr. Roberto Gómez Cárdenas

Tipos de FAT

- FAT 32
  - Disponible en Windows 95 OSR 2 y Windows 98.
  - Aumenta el número de dígitos para direccionar clusters y también reduce el tamaño de cada cluster.
  - Se pueden usar discos más grandes (hasta dos Terabytes) y presenta una mayor eficacia de almacenaje (menos espacio desperdiciado)
  - La cuenta de clusters esta entre 65,526 y 268,435,456 inclusive
  - Archivo más grande: 4GB menos 2 bytes

Lámina 42 Dr. Roberto Gómez Cárdenas

Tabla comparativa FATs

	FAT12	FAT16	FAT32
Máximo tamaño de espacio de amacenamiento manejable	16 MB*	2 GB	255 GB*
Número teórico de clusters direccionables	2^{12}	2^{16}	2^{32}
Valor actual permitido del contador, c, de clusters	$c <= 4,085$	$4,085 < c <= 65,525$	$65,525 < c <= 2^{28}$
Año de introducción	1980	1983	1997
Sistemas operativos que lo soportan	QDOS	DOS 4.0	Windows 95, 2000, XP, Vista, 7
Ubicación y tamaño del directorio raíz.	fijo	fijo	variable
Copia del sector de arranqque	no	no	si

Lámina 43 Dr. Roberto Gómez Cárdenas

Sistema archivos NTFS

- NTFS: New Technology File System
  - Introducido con Windows NT
  - Sistema de archivos primario para Windows Vista
- Mejoras sobre sistema archivos FAT
  - NTFS proporciona más información acerca de un archivo.
  - NTFS cuenta con más control sobre archivos y carpetas.
- NTFS fue el movimiento de Microsoft hacia un sistema de archivos con seguimiento (journaling file system).

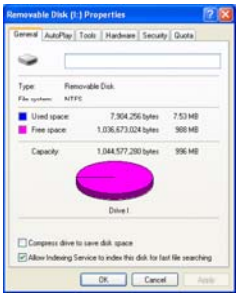


Lámina 44 Dr. Roberto Gómez Cárdenas

Sistema Archivos NTFS

- La administración se lleva a cabo a través del MFT: Master File Table.
- En NTFS, todo lo que escribe a disco es considerado un archivo.
- En un disco NTFS
  - El primer conjunto de datos es la partición del sector de arranque.
  - Después le sigue el MFT.
- NTFS provoca menos slack space.
- Los clusters son más pequeños para drives de disco más pequeños.
- NTFS usa Unicode
  - Un formato de datos internacional.

Lámina 45 Dr. Roberto Gómez Cárdenas

Tamaños clusters en disco NTFS

Tamaño disco	Sectores por cluster	Tamaño cluster
512MB o menos	1	512 bytes
512MB-1GB	2	1024 bytes
1 – 2 GB	4	2048 bytes
2 – 4 GB	8	4096 bytes
4 – 8 GB	16	81292 bytes
8 – 12 GB	32	16,384 bytes
16 – 32 GB	64	32,768 bytes
Más de 32GB	128	65,536 bytes

Lámina 46 Dr. Roberto Gómez Cárdenas

Identificando el tamaño del cluster

- En una línea de comandos con permisos de administrador teclear:

  fsutil fsinfo ntfsinfo <drive>:

- Ejemplo:

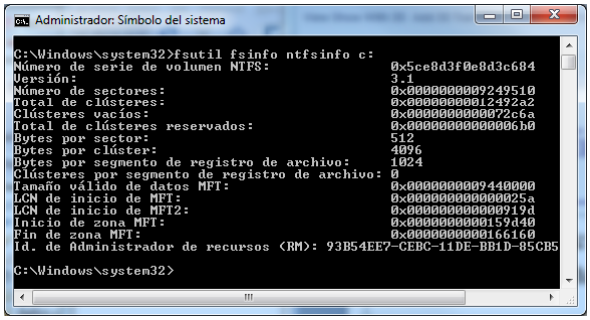


Lámina 47 Dr. Roberto Gómez Cárdenas

El MFT de NTFS

- El MFT contiene información acerca de todos los archivos en el disco.
  - Incluyendo los archivos de sistemas que el sistema operativo utiliza y del mismo MFT.
  - Esto permite que la tabla pueda crecer cuanto quiera y manejar volúmenes muy grandes (hasta 264 bytes = 16 Exabytes)
- En el MFT, los primeros 15 registros son reservados para ser usados por el mismo sistemas de archivos.
- El sector de arranque sabe donde se ubica el MFT.
- Los registros en el MFT son llamados *metadatos*.
- Nombres archivos del sistema empiezan con $
- Existe una “copia” llamada $MFTMirr,

Lámina 48 Dr. Roberto Gómez Cárdenas

Nomenclatura memorias

Gigabytes
Terabytes
Petabytes
Exabytes
Zettabytes
Yottabytes

Lámina 49 Dr. Roberto Gómez Cárdenas

Registros metadatos en NTFS

Nombre archivo	Archivo sistema	Posición registro	Descripción
$Mft	MFT	0	Archivo de base
$MftMirr	MFT 2	1	Los primeros cuatro registros del MFT son almacenados en esta posición. Es el respaldo del MFT.
$LogFile	Archivo bitácoras	2	Aquí se almacenan transacciones previas para permitir recuperación después de una falla en el volumen NTFS.
$Volume	Volumen	3	Contiene información específica al volumen, como nombre y versión.
$AttrDef	Definiciones atributos	4	Un tabla de listas de nombres de atributos, números y definiciones.
$	Archivo raíz – name index	5	Carpeta raíz del volumen NTFS

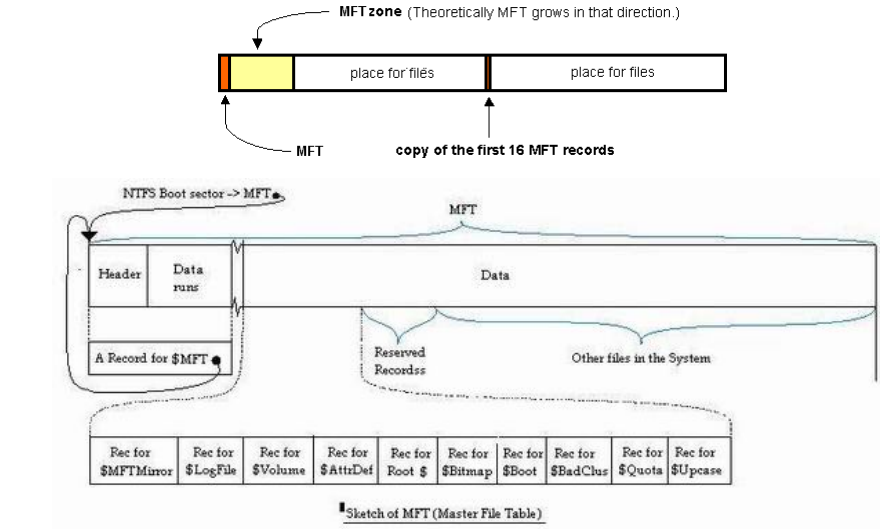
Lámina 50 Dr. Roberto Gómez Cárdenas

Registros

Nombre archivo	Archivo sistema	Posición registro	Descripción
$Bitmap	Sector arranque	6	Un mapa de volumen NTFS mostrando que clusters se encuentran ocupados y cuales libres.
$Boot	Sector arranque	7	Usado para montar el volumen NTFS durante el proceso de arranque.
$BadClus	Archivo con cluster dañado	8	Para clusters que cuentan con errores irrecuperables.
$Secure	Archivo seguridad	9	Descriptores de seguridad únicos al volumen son listados en este archivo. Es donde se mantienen las ACLs.
$Upcase	Tabla mayúsculas	10	Convierte minúsculas a mayúsculas .
$Extend	Archivo extensión NTFS	11	Extensiones opcionales son listadas aquí, tales como quotas, identificadores objetos,
		12-15	Reservado para uso futuro.

Lámina 51 Dr. Roberto Gómez Cárdenas

MFT y sus registros



Fuente figura: http://www.codeproject.com/KB/files/NTFSUndelete.aspx

Lámina 52 Dr. Roberto Gómez Cárdenas

Viendo los archivos MTFS

- Archivos metadatos empiezan con $ y son archivos ocultos.
  - No pueden ser vistos usando los medios comunes.
- Necesario utilizar software específico.
- Microsoft proporciona un conjunto de herramientas bajo el nombre de OEM TOOLS.
  - http://support.microsoft.com/kb/253066
- La herramienta nfi permite ver los archivos de metadatos del MTF.
- Usarla en combinación con comando more y con privilegios.

Lámina 53 Dr. Roberto Gómez Cárdenas

Ejemplo uso nfi

- Sintaxis:

  nfi <drive>
- Ejemplo de salida

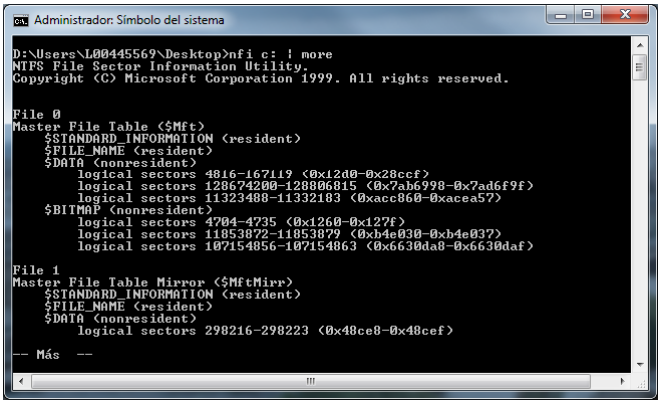


Lámina 54 Dr. Roberto Gómez Cárdenas

MFT y atributos archivos

- NTFS ve un archivo o directorio como un conjunto de atributos que describen al archivo o directorio.
  - Esto incluye a los archivos del sistema.
- En el MFT del NTFS
  - Todos los archivos y carpetas son almacenados en registros separados de 1024 bytes cada uno.
  - En algunos casos es más grande, llegando a medir un cluster.
- Cada registro contiene información del archivo o carpeta.
  - Información dividida en campos que contienen metadatos.
- Un campo del registro se conoce como un *identificador de atributo*.

Lámina 55 Dr. Roberto Gómez Cárdenas

Atributos archivos en el MFT

Id Atributo	Propósito	Descripción
0x10	$Standard_Information	Estampillas tiempo, banderas acceso.
0x20	$Attribute_list	Usado cuando el registro no cuenta con espacio suficiente para todos los atributos.
0x30	$File_Name	Nombre del archivo y el directorio al que pertenece.
0x40	$Object_ID	Identificador único para el archivo o directorio.
0x50	$Security_Descriptor	ACL (Acc. Control List) y SID (Sec. Identifier).
0x60	$Volume_Name	Nombre del volumen de disco.
0x70	$Volume_Information	Versión de NTFS y marca de apagado incorrecto del sistema
0x80	$Data	Los datos de lo archivos pequeños (menor a 660 bytes)
0x90	$Index_Root	Usado por el directorio para ser almacenado en un B-Tree
0xA0	$Index_Allocation	Usado por el directorio para ser almacenado en un B-Tree

Lámina 56 Dr. Roberto Gómez Cárdenas

Otros atributos

Atributo	Propósito
0xB0	$Bitmap
0xC0	$Reparse_Point
0xD0	$EA_Information
0xE0	$EA
0x100	$Logged_Utility_Stream

Lámina 57 Dr. Roberto Gómez Cárdenas

Procesamiento archivos

- Para procesar un archivo en NTFS
  - Los atributos dentro del archivo deben ser procesados, para obtener la información sobre el archivo.
  - Después se obtienen los datos del archivo.
  - Ahora es posible el procesamiento.

Lámina 58 Dr. Roberto Gómez Cárdenas

Información residente y no residente.

- Información del archivo se puede almacenar de forma:
  - Residente o no residente
- Residente
  - Los datos se almacenan junto con los atributos.
  - Usada cuando los archivos son muy pequeños.
  - Cuando el sistema lee este registro también lee los datos.
  - Sistema archivos no tiene que leer el disco de nuevo.
- No residente
  - Para datos más grandes que el registro MFT.
  - Datos se encuentran fuera del MFT, en alguna parte del disco.
  - Direcciones se encuentran en estructuras de nombre data runs.

Lámina 59 Dr. Roberto Gómez Cárdenas

Ejemplo información residente y no residente.

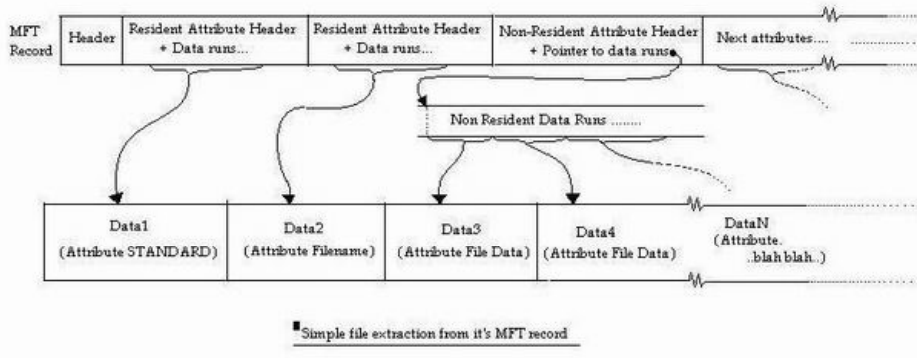


Lámina 60 Dr. Roberto Gómez Cárdenas

File Reference Number

- Cada archivo en un volumen NTFS cuenta con un identificador único de 64 bits conocido como:
  - File Quotation Number / File Reference Number
- Este número se divide en dos partes: numero de archivo y orden de archivo.
  - El número de archivo es de 48 bits y corresponde a la posición en el MFT.
  - El número de orden se incrementa conforme se usan los archivos, para consistencia interna de NTFS.

Lámina 61 Dr. Roberto Gómez Cárdenas

Logical Clusters Numbers

- LCNs son los números de todos los clusters, desde el principio del disco hasta el final de este.
- Para conocer la dirección física, NTFS multiplica el LCN por el tamaño del cluster, para obtener el offset en el volumen.
- NTFS hace referencia a un dato dentro de un archivo a través de los VCNs: Virtual Cluster Numbers.
  - Estos referencian a los clusters que pertenecen a un archivo desde 0 hasta m.
  - Los VCNs no son necesariamente contiguos.

Lámina 62 Dr. Roberto Gómez Cárdenas

Lámina 63 Dr. Roberto Gómez Cárdenas

Stream de datos alternos de NTFS

- Stream de datos
  - La forma en que los datos pueden ser añadidos a los archivos existentes.
  - Pueden ser usados para “ocultar” información, ya sea de forma intencional o por coincidencia.
- Un stream de datos se convierte en un atributo adicional.
  - Permite asociar al archivo con diferentes aplicaciones.
- Solo se puede saber cuando un archivo cuenta con un data stream, examinando la entrada de dicho archivo en el MFT.
  - No se pueden acceder con el comando TYPE ni con el explorador de Windows.

Lámina 64 Dr. Roberto Gómez Cárdenas

Carácterísticas Alternate Data Streams

- Sintaxis para referenciar los flujos

  archivo[:flujo[tipo]]
- Este tipo de archivos no deberían ser accedidos por el usuario final, sino sólo por aquellas aplicaciones que los utilicen.
- Selección del ":" puede provocar trabajo extra.
  - Necesario especificar toda la rota.
- Exclusivo de NTFS
  - No se copian a otro dispositivo con otro sistema de archivos (p.e. FAT).

Lámina 65 Dr. Roberto Gómez Cárdenas

Trabajando con ADS

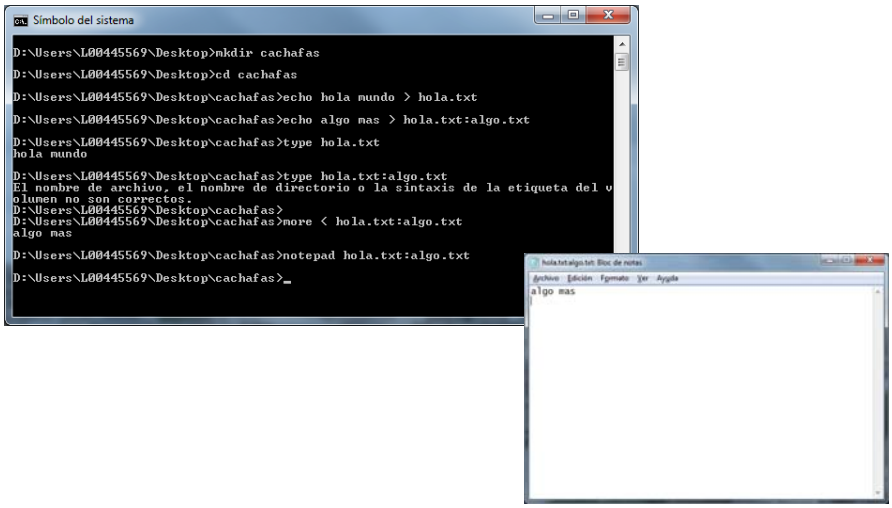


Lámina 66 Dr. Roberto Gómez Cárdenas

AdsCheck.exe

- http://www.diamondcs.com

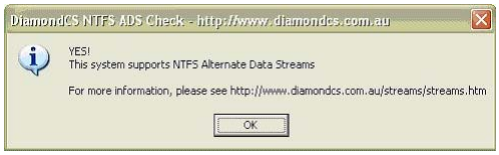


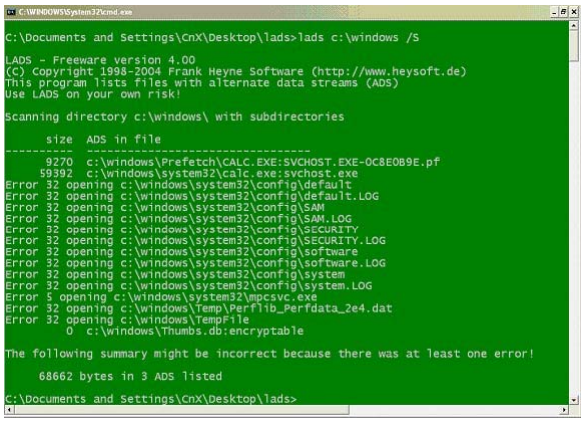
Lámina 67 Dr. Roberto Gómez Cárdenas

- Llenado del disco duro
- Ejecución en Vista y 7
- Opciones para borrar

Lámina 68 Dr. Roberto Gómez Cárdenas

Lads.exe

- www.heysoft.de



Otras

- LNS - List NTFS Streams (http://ntsecurity.nu/toolbox/lns/)
- Ads Spy (http://www.spywareinfo.com/~merijn/files/adsspy.zip)
- SFind (http://www.foundstone.com)
- Streams.exe (http://www.sysinternals.com/utilities/streams.html)

¿Solo texto?

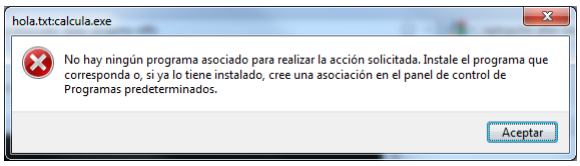


Lámina 71 Dr. Roberto Gómez Cárdenas

Ejemplo stream datos

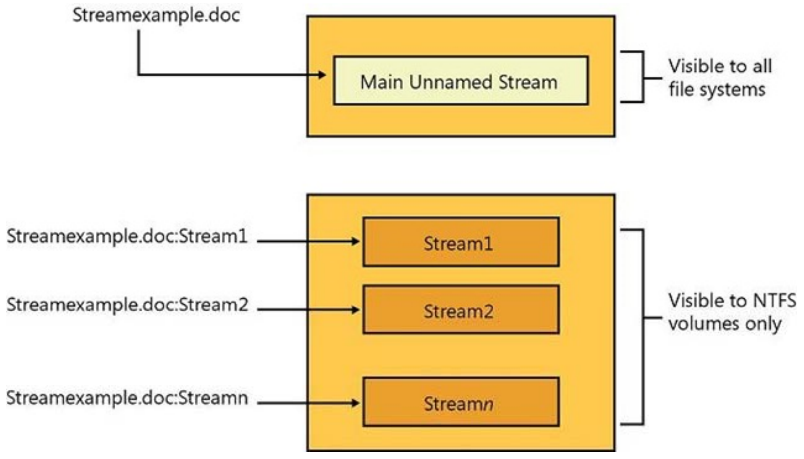


Lámina 72 Dr. Roberto Gómez Cárdenas

Archivos comprimidos en NTFS

- NTFS proporciona compresión similar a FAT DriveSpace 3
- En NTFS, archivos, folders, o volúmenes enteros pueden comprimirse.
- La mayor parte de las herramientas forenses pueden descomprimir y analizar datos comprimido por Windows.

Lámina 73 Dr. Roberto Gómez Cárdenas

NTFS Encryption File System (EFS)

- EFS: Encryption File System.
  - Introducido con Windows 2000.
  - Implementa un método de llave pública o privada para cifrar archivos, folders o volúmenes de disco.
- Cuando EFS es usado en Windows Vista Business Edition o mayor, XP Professional, o 2000:
  - Un certificado de recuperación es generado y enviado a la cuenta del administrador local de Windows.
- Usuarios pueden usar EFS sobre archivos almacenados en sus máquinas locales o en un servidor remoto.

Lámina 74 Dr. Roberto Gómez Cárdenas

¿Cómo funciona todo?

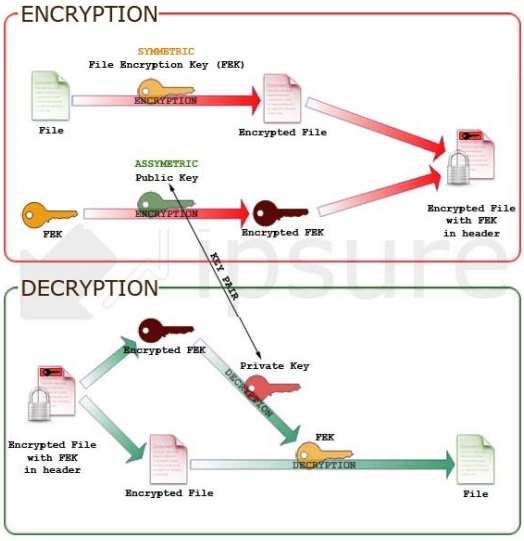
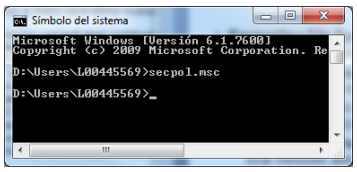


Lámina 75 Dr. Roberto Gómez Cárdenas

Propiedades EFS



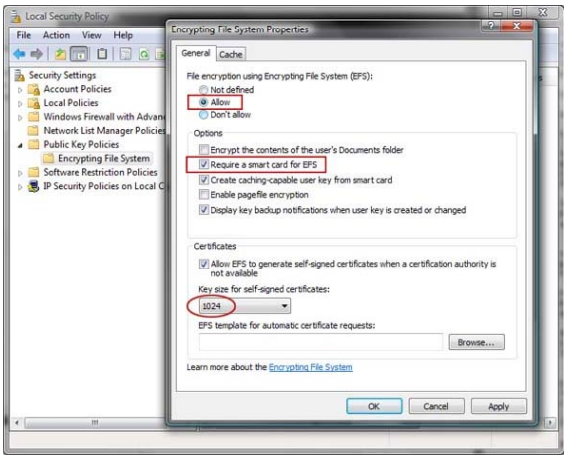


Lámina 76 Dr. Roberto Gómez Cárdenas

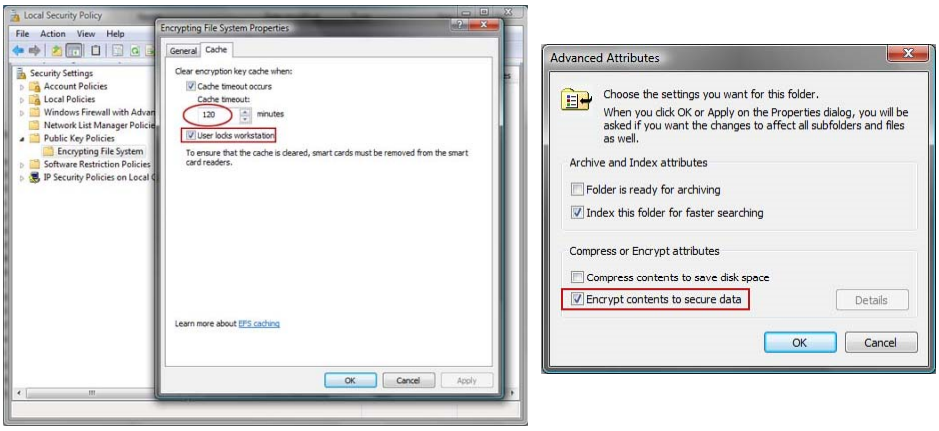


Lámina 77 Dr. Roberto Gómez Cárdenas

Agente de recuperación de llave

- El agente de recuperación de llave implementa el certificado de recuperación
  - El cual se encuentra en la cuenta del administrador.
- Administradores Windows pueden recuperar una llave de dos formas: a través de Windows o desde un prompt de MS-DOS.
- Comandos MS-DOS
  - Cipher
  - Copy
  - Efsrecvr (usado para descifrar archivos EFS)

Lámina 78 Dr. Roberto Gómez Cárdenas

Borrando archivos NTFS

- Cuando un archivo es borrado en Windows XP, 2000 o NT
  - El sistema operativo lo renombra y lo mueve a la Papelera de Reciclaje.
- Se puede usar el comando *del* de MS-DOS
  - Eliminar el archivo de la lista de MFT de la misma forma que FAT lo hace.

Lámina 79 Dr. Roberto Gómez Cárdenas

Cifrado del disco entero

- En años recientes, se ha incrementado la preocupación por la perdida de:
  - Información de Identidad Personal, y secretos corporativos debido al robo de computadoras.
- De interés particular es la perdida de laptops y otros dispositivos de mano.
- Para prevenir perdida de información, los vendedores de software proporcionan el servicio de cifrado del disco entero.

Lámina 80 Dr. Roberto Gómez Cárdenas

Características de cifrado disco entero

- Las herramientas de cifrado entero de disco ofrecen las siguientes características:
  - Autenticación de pre-arranque.
  - Cifrado de disco total o parcial con hibernación segura.
  - Algoritmos avanzados de cifrado.
  - Función de administración de llaves.
  - Un microchip TPM (Trusted Platform Module) para generación de llaves de cifrado y logins autenticados.

Lámina 81 Dr. Roberto Gómez Cárdenas

Analizando un drive cifrado

- En un cifrado de disco entero, las herramientas cifran cada sector del drive de forma separada.
- Muchas de estas herramientas cifran el sector de arranque del disco.
  - Para prevenir cualquier esfuerzo para darle la vuelta a la partición del disco asegurada.
- Para examinar un disco cifrado, es necesario descifrarlo primero.
  - Correr un programa específico del vendedor para descifrar el drive.

Lámina 82 Dr. Roberto Gómez Cárdenas

Microsoft BitLocker

- Disponible solo en ediciones Vista Enterprise y Ultimate.
- Requerimientos de hardware y software
  - Una computadora capaz de correr Windows Vista
  - El microchip TPM, versión 1.2 o superior.
  - Un BIOS compatible con el Trusted Computing Group (TCG).
  - Dos particiones NTFS.
  - El BIOS configurado de tal forma que el arranque se haga desde el disco duro,

Lámina 83 Dr. Roberto Gómez Cárdenas

Examinando herramientas de cifrado de terceros

- Algunas herramientas de terceros
  - PGP Whole Disk Encryption
  - Voltage SecureDisk
  - Utimaco SafeGuard Easy
  - Jetico BestCrypt Volume Encryption
  - SoftWinter Sentry 2020 for Windows XP
  - Pointsec Full Disk Encryption
- Algunas herramientas de cifrado open-source
  - TrueCrypt
  - CrossCrypt
  - FreeOTFE

Lámina 84 Dr. Roberto Gómez Cárdenas

Registro de Windows

- Base de datos que almacena información de configuración de hardware y software, conexiones de red, preferencias de usuario e información de setup.
- Es una base de datos jerárquica, organizada en forma de árbol.
  - cada llave contiene subllaves o un valor
- Para propósitos de investigación, el Registro puede contener evidencia valiosa.
- Para ver el registro es posible usar
  - Regedit (Registry Editor) para sistemas Windows 9x .
  - Regedt32 para Windows 2000 y XP

Lámina 85 Dr. Roberto Gómez Cárdenas

Terminología registro

- Registry
  - Colección archivos contiene información sobre sistema y usuarios.
- Registry Editor
  - Utilidad para ver y modificar datos en el Registro.
- HKEY
  - Categorías de llaves.
  - Windows 9x cuenta con seis categorías.
  - Windows 2K y posteriores cuentan con cinco llaves.

Lámina 86 Dr. Roberto Gómez Cárdenas

Terminología registro

- Key
  - Cada HKEY contiene carpetas que se conocen como llaves.
  - Llaves pueden contener otras carpetas o valores.
- Subkey
  - Llave dentro de otra llave
- Branch
  - Una llave y sus contenidos, incluyendo subllaves
- Value
  - Un nombre y un valor.
  - Similar a un archivo y su contenido.

Lámina 87 Dr. Roberto Gómez Cárdenas

Terminología registro

- Default value
  - Todas las llaves cuentan con un valor por default, que puede o no contener datos.
- Hives
  - Ramas, branches, específicas en HKEY_USER y HKEY_LOCAL_MACHINE.
  - Hives en HKEY_LOCAL_MACHINE\Software son:
    - SAM, Security, Components y System
  - Para HKEY_USER, cada cuenta de usuario cuenta con su propio hive

Lámina 88 Dr. Roberto Gómez Cárdenas

Elementos del Registro

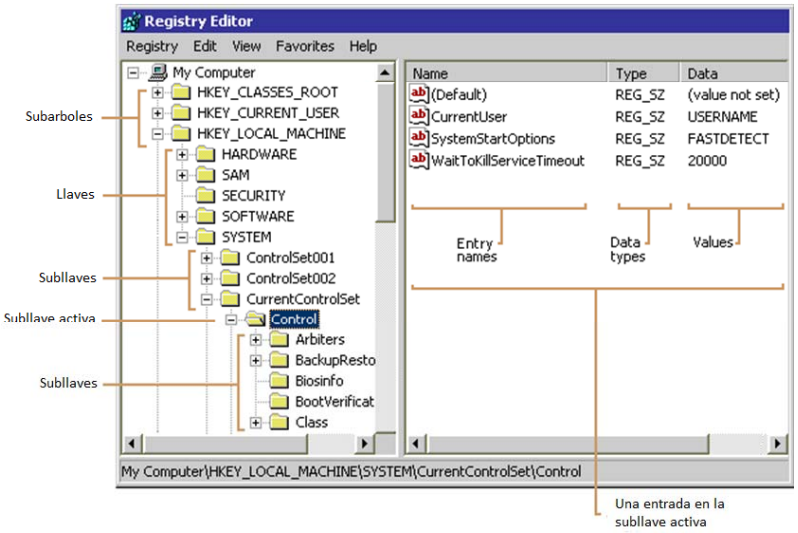


Lámina 89 Dr. Roberto Gómez Cárdenas

Ubicación de archivos registro y propósitos (Windows 9x/ME)

Nombre archivo y ubicación	Propósito del archivo
Windows\System.dat	Area de almacenamiento protegida del usuario. Contiene configuraciones de los programas instalados y passwords asociados con lo programas instalados.
Windows\User.dat Windows\profile\user-account	Contiene la lista más de los programas más recientemente usados, y las configuraciones del desktop, cada cuenta de usuario creada en el sistema.

Lámina 90 Dr. Roberto Gómez Cárdenas

Ubicación de archivos registro y propósitos (NT, 2000, XP y Vista)

Nombre archivo y ubicación	Propósito del archivo
Documents and Settings\user-account\Ntuser.dat	Area protegida contiene la lista de archivos MRU y configuraciones del desktop.
Windows\system32\config\Default	Contiene las configuraciones del sistema.
Windows\system32\config\SAM	Contiene las configuraciones
Windows\system32\config\Security	Contiene las configuraciones de manejo de cuentas y seguridad.
Windows\system32\config\Software	Contiene las configuraciones de los programas instalados así como las cuentas y contraseñas asociadas.
Windows\system32\config\System	Contiene configuraciones adicionales del sistema.

Lámina 91 Dr. Roberto Gómez Cárdenas

Las llaves del registro

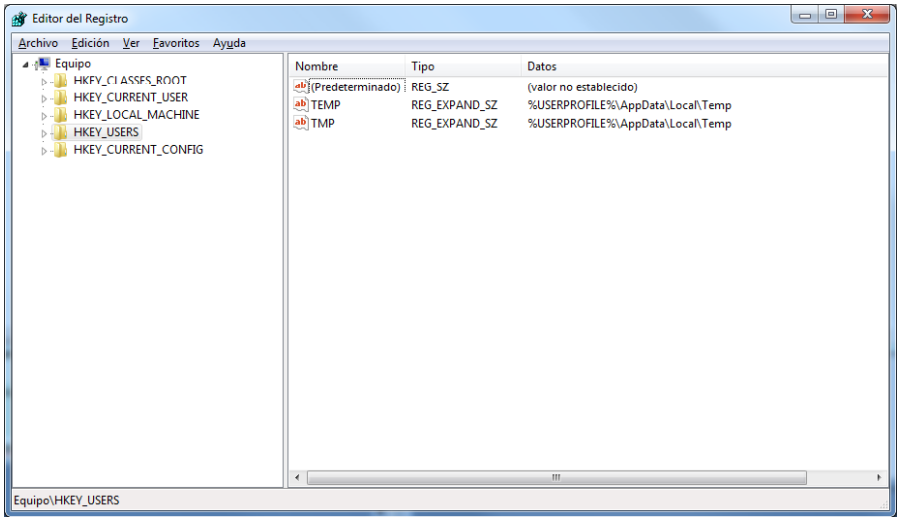


Lámina 92 Dr. Roberto Gómez Cárdenas

Descripción llaves del registro

Llave	Descripción
HKEY_CLASSES_ROOT	Liga simbólica al archivo HKEY_LOCAL_MACHINE\SOFTWARE Proporciona tipos de archivos e información sobre extensiones de archivos, prefijos de protocolos URL,etc.
HKEY_CURRENT_USER	Liga simbólica al archivo HKEY_USERS; almacena configuraciones del usuario conectado al sistema.
HKEY_LOCAL_MACHINE	Contiene información acerca de hardware y software instalado.
HKEY_USERS	Almacena información del usuario actualmente conectado, solo una llave en su HKEY esta limitada a HKEY_CURRENT_USER.

Lámina 93 Dr. Roberto Gómez Cárdenas

Descripción llaves del registro

Llave	Descripción
HKEY_CURRENT_CONFIG	Una liga simbólica del HKEY_LOCAL_MACHINE\System\CurrentControl\Set\ Hardware\Profile\xxx (donde xxx representa el profile del hardware actual); contiene las configuraciones del hardware.
HKEY_DYN_DATA	Solo usado en sistemas Windows 9x/Me; almacena configuraciones de hardware.

Lámina 94 Dr. Roberto Gómez Cárdenas

Principales tipos valores llaves

- Palabra (REG_DWORD)
  - almacena un dato numérico, con 4 bytes
- Binario (REG_BINARY).
  - almacena un grupo de datos binario.
- Cadena (REG_SZ)
  - almacena una cadena de caracteres.
- Cadena expandida (REG_EXPAND_SZ)
  - almacena una cadena de caracteres de tamaño variable.
- Cadena múltiple (REG_MULTI_SZ)
  - almacena un conjunto de cadenas de caracteres.

Lámina 95 Dr. Roberto Gómez Cárdenas

Ejemplo info registro

- Historial navegación internet explorer
  - Subarbol: HKEY_CURRENT_USER
  - Llave: Software
  - Subllave: Microsoft
  - Subllave: Internet Explorer
  - Subllave: Typed URLs
- ¿Para otro navegador?

Lámina 96 Dr. Roberto Gómez Cárdenas

Auditoria eventos Windows

- Incorporado para NT4, W2K, WXP y W2003S
  - no para W95/98/ME
- Posible auditar cualquier tipo de objeto de forma granular
  - objeto: directorios, archivos, impresora, llaves registro o estructuras internas del sistema operativo
  - posible establecer auditoria para una sola acción (lectura o escritura) de un solo archivo de un solo usurario
- SACLS controla como se audita un objeto
  - System Access Control Lists
- SRM es el responsable de generarar la información basado en las SACLs y en la política de auditoria
  - SRM: Security Reference Monitor

Lámina 97 Dr. Roberto Gómez Cárdenas

Tipos de logs

- Computadora normal
  - log aplicación
  - log seguridad
  - log sistema
- Computadora como controlador dominio
  - file replication service log
  - directory service log
- Computadora corriendo como DNS
  - DNS server log

Lámina 98 Dr. Roberto Gómez Cárdenas

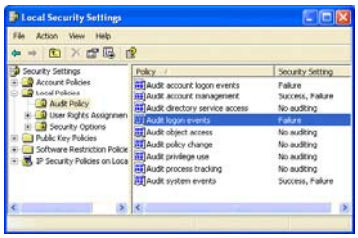
Tipos eventos

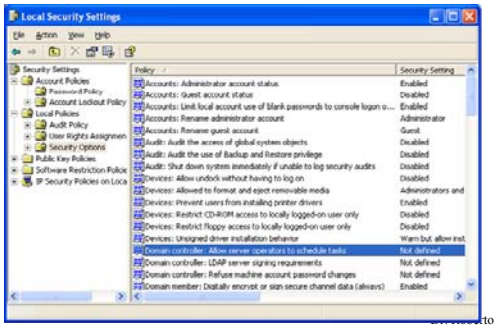
- Cinco tipos eventos
  - Information
  - Warning
  - Error
  - Audit Suceess
  - Audit Failure
- Logs de aplicación y sistema
  - information, warning y error
- Logs de seguridad
  - audit success y audit failure events

Lámina 99 Dr. Roberto Gómez Cárdenas

Definiendo politica auditoria

- Configuration Panel
- Administrative tools
- Local Security Policy





No activo para Home Edition

Lámina 100 Dr. Roberto Gómez Cárdenas

Habilitar la política auditoria para acceso de objetos

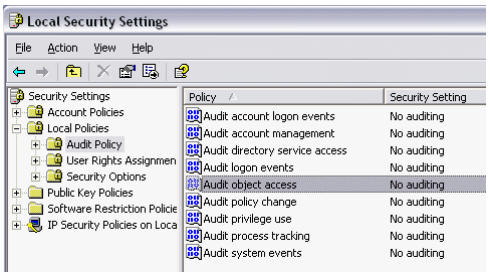
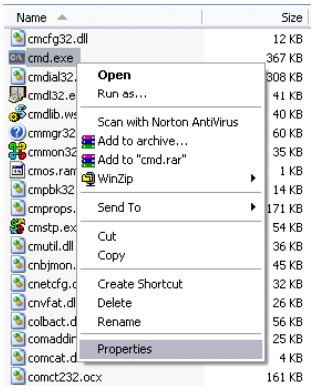
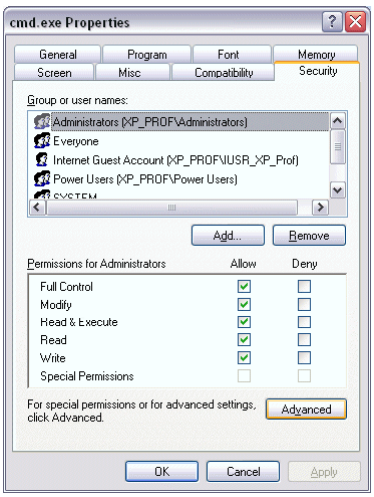


Lámina 101 Dr. Roberto Gómez Cárdenas

Habilitando auditoria para un archivo en particular





acciones a auditar

Lámina 102 Dr. Roberto Gómez Cárdenas

Habilitando auditoria para un archivo en particular

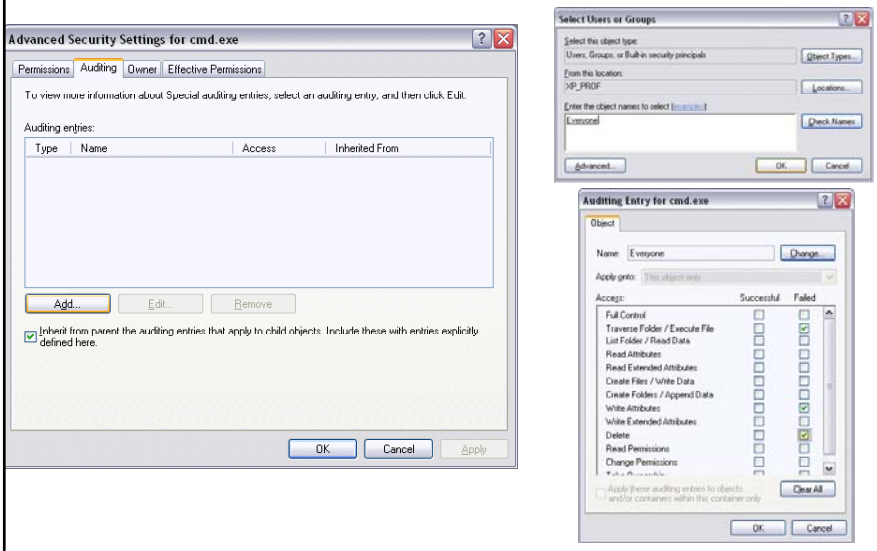


Lámina 103 Dr. Roberto Gómez Cárdenas

Verificando

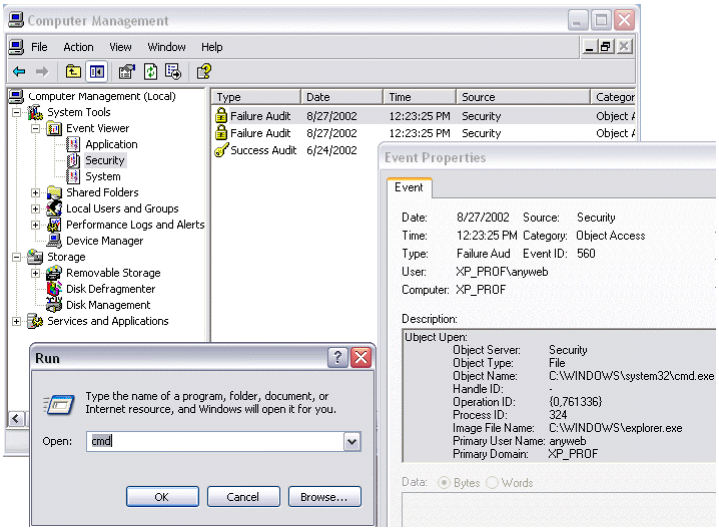
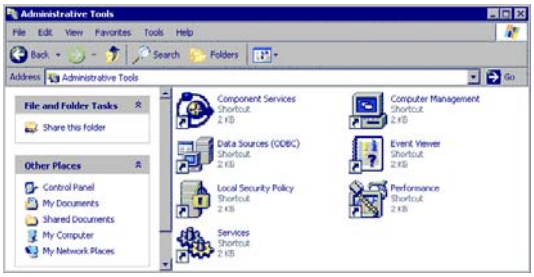


Lámina 104 Dr. Roberto Gómez Cárdenas

Event Viewer (2K, XP)



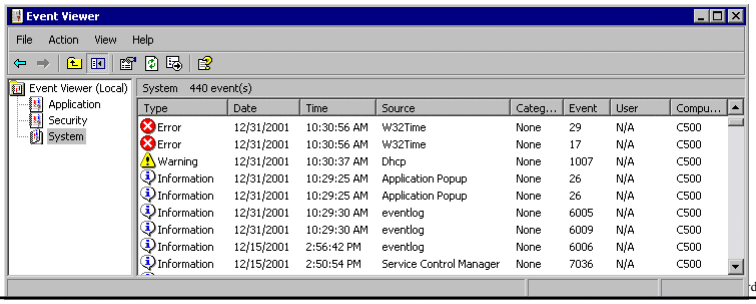
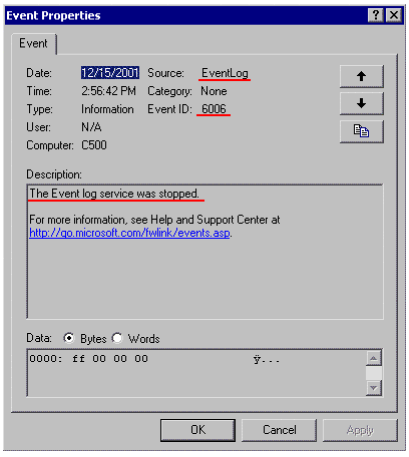


Lámina 105 denas

Ejemplo arranque y apagado



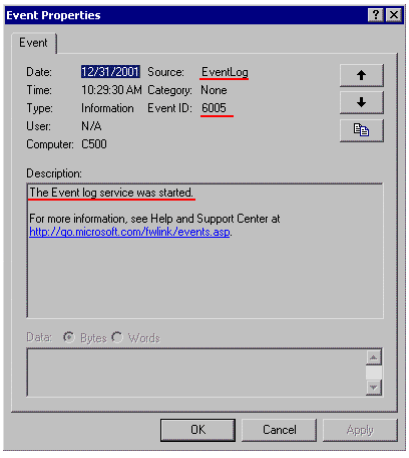


Lámina 106 Dr. Roberto Gómez Cárdenas

Ejemplo DHCP

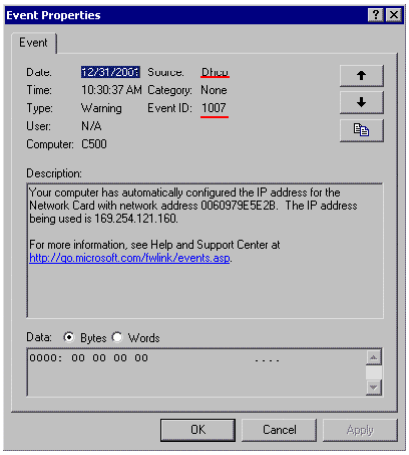
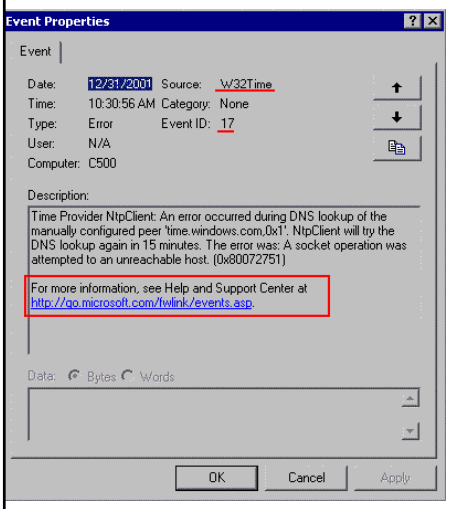


Lámina 107 Dr. Roberto Gómez Cárdenas

Ejemplo error W32Time



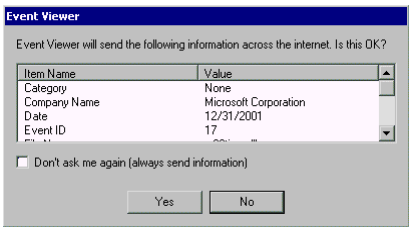
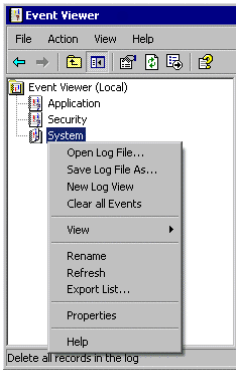


Lámina 108 Dr. Roberto Gómez Cárdenas

Almacenando eventos



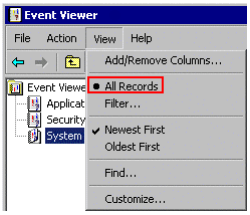
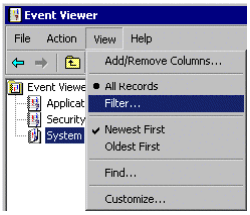
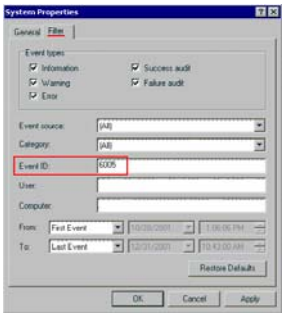


Lámina 109 Dr. Roberto Gómez Cárdenas

Búsqueda eventos





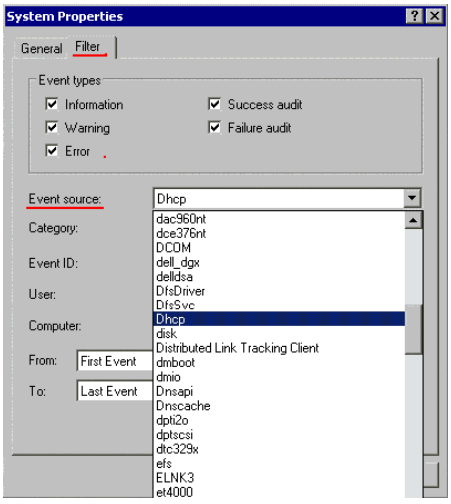


Lámina 110 Dr. Roberto Gómez Cárdenas

Definiendo políticas almacenamiento

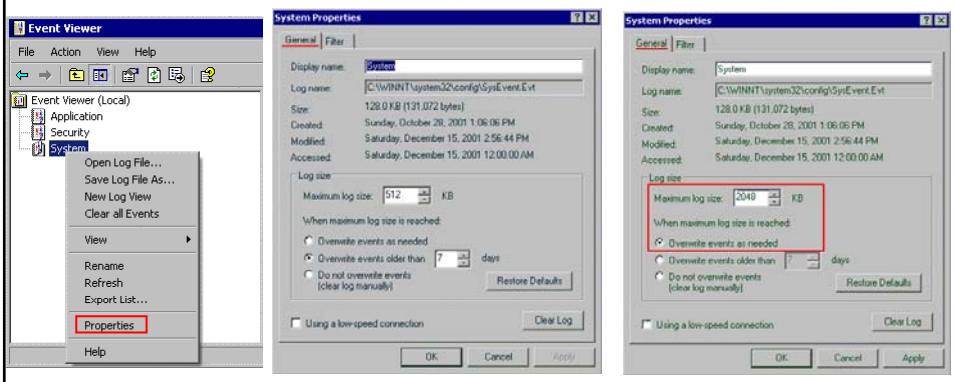


Lámina 111 Dr. Roberto Gómez Cárdenas

Event Viewer (Vista, 7)

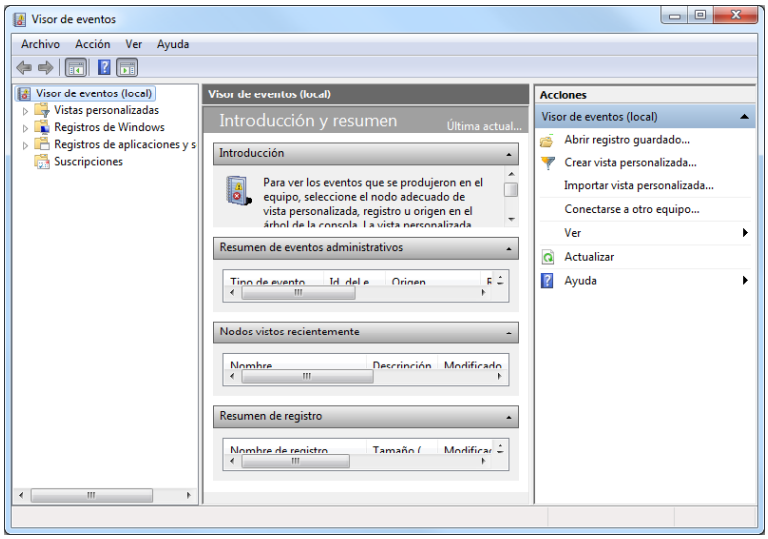


Lámina 112 Dr. Roberto Gómez Cárdenas

Las memorias USB

1. Conector USB.
2. Dispositivo de control de almacenamiento masivo USB (consta un microprocesador RISC y un pequeí número de circuitos de memoria RAM ROM).
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.

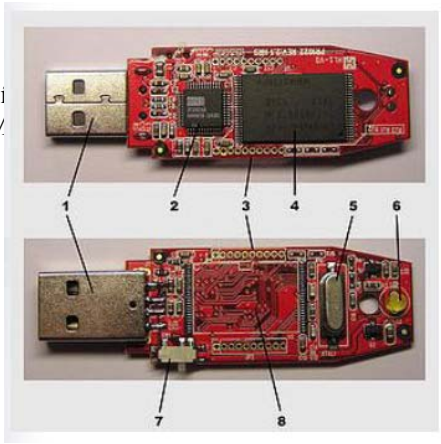


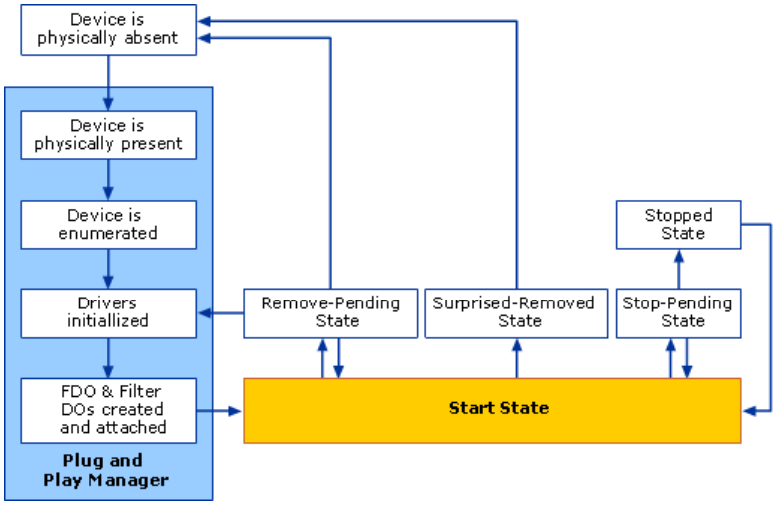
Lámina 113 Dr. Roberto Gómez Cárdenas

¿Qué ocurre cuando se inserta un USB?

- Plug and play (PnP) Manager es notificado.
- Se reconoce el dispositivo y se instala un manejador usando el driver genérico (USBTOR.SYS).
- El Windows Mount Manager (MountMgr.sys) accede al dispositivo para obtener su información única de identificación.
- El Mount Manager crea las llaves de registro apropiadas y le asigna una letra de unidad (E:, F: Z:, etc) , a través de la cual será accedido.

Lámina 114 Dr. Roberto Gómez Cárdenas

Plug and Play



Fuente: http://technet.microsoft.com/en-us/library/cc781092%28WS.10%29.aspx

Lámina 115 Dr. Roberto Gómez Cárdenas

La utilería UVCView

- La información descriptiva de los dispositivos USB no se encuentra localizada en el área de memoria.
- Una imagen forense del dispositivo USB no incluye información del descriptor del dispositivo.
- Software UVCView (USB Video Class Descriptor View) es parte del WDK (Windows Driver Kit) y permite ver los descriptores de cualquier dispostivo USB que se encuentre conectado.
  - Se puede bajar de la página de Microsoft

Lámina 116 Dr. Roberto Gómez Cárdenas

UVCView sin ningún dispositivo conectado

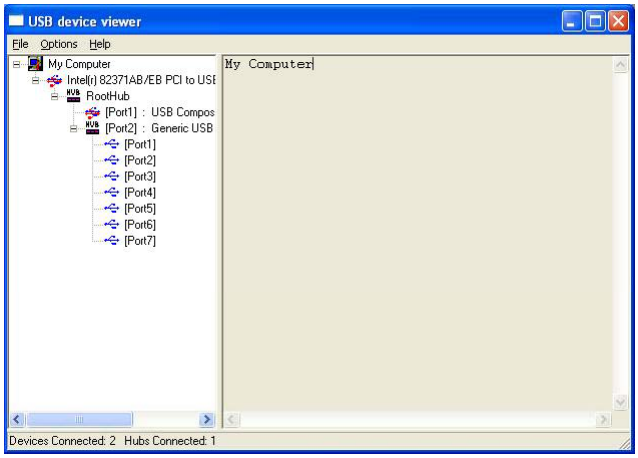


Lámina 117 Dr. Roberto Gómez Cárdenas

UVCView con dos dispositivos conectados

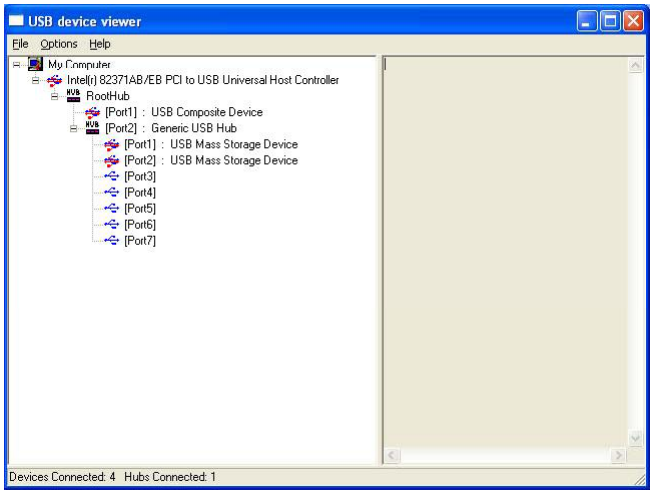
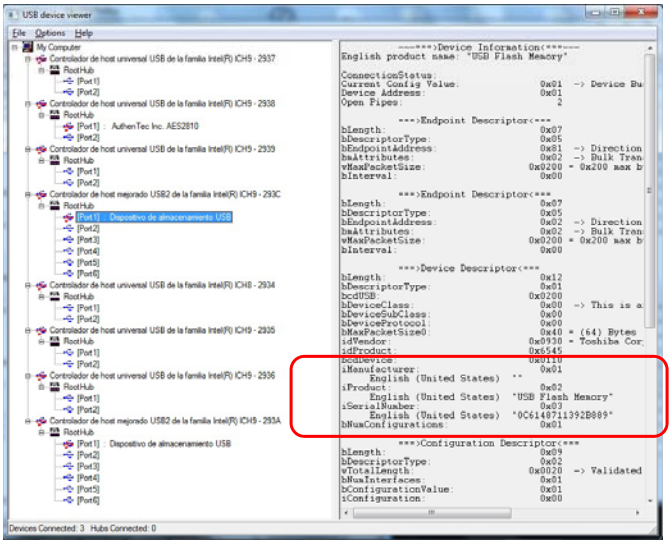


Lámina 118 Dr. Roberto Gómez Cárdenas

Información de un USB



Datos relevantes

```
bcdDevice:                          0x0110
iManufacturer:                        0x01
     English (United States)  ""
iProduct:                             0x02
     English (United States)  "USB Flash Memory"
iSerialNumber:                        0x03
     English (United States)  "0C6148711392B889"
bNumConfigurations:                   0x01

          ===>Configuration Descriptor<===
```

El archivo setupapi.log

- Es un archivo de texto plano que contiene información interesante acerca de varios dispositivos e instalación de paquetes.
- Puede contener información sobre los números de series de los dispositivos conectados a la máquina-.
- Ubicación en Windows XP
  - %windir%\setupapi.log
- Ubicación en Windows Vista y 7
  - %windir%\inf\ setupapi.app.log
  - %windir%\inf\ setupapi.dev.log

Lámina 121 Dr. Roberto Gómez Cárdenas

La herramienta SAEX

- Permite agrupar los eventos del archivo "SetuApi.log" y ordenarlos en una hoja excel.

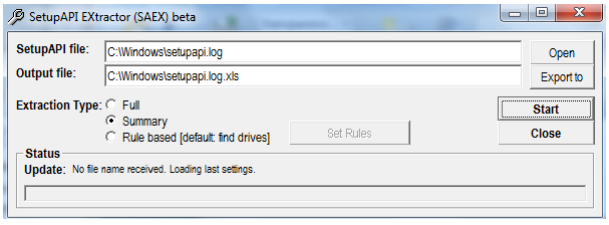
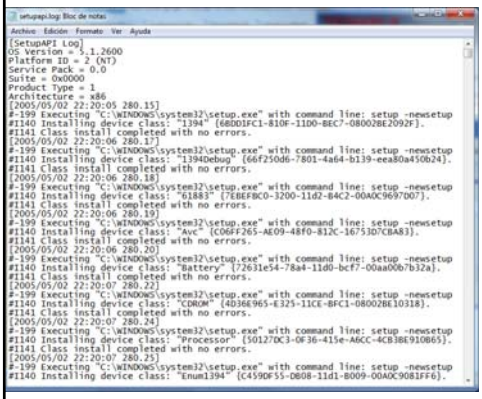


Lámina 122 Dr. Roberto Gómez Cárdenas

Ejemplo uso



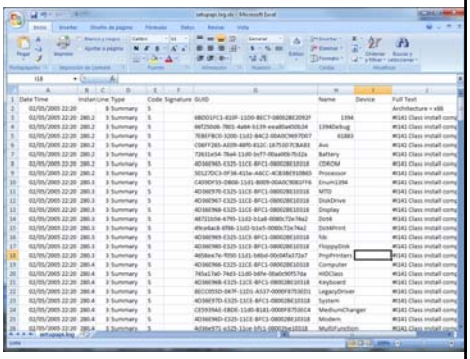


Lámina 123 Dr. Roberto Gómez Cárdenas

¿Qué nos dice setupapi.log?

- Nos indica la fecha y hora en la que el dispositivo fue conectado por PRIMERA vez al sistema.

Lámina 124 Dr. Roberto Gómez Cárdenas

Registro y USB

- La llave de registro USBSTOR contiene subllaves que son creadas cuando se conectan dispositivos USB a en una computadora.
- La ubicación de la llave en Windows XP, Vista y 7 es:
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR
  - Dentro de esta llave se genera una subllave utilizando el device ClassID del dispositivo:

    \Disk&Ven_USB_2.0&Prod_Flash_Disk&Rev_5.00
  - Dentro de esta llave se genera una instancia única que utiliza el número de serie del dispositivo:

    \0C6148711392B889&0

Lámina 125 Dr. Roberto Gómez Cárdenas

La llave USBSTOR del registro

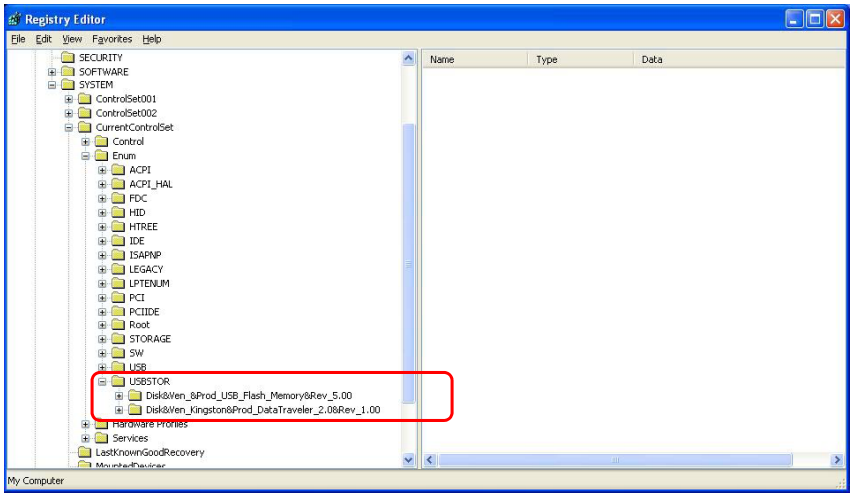
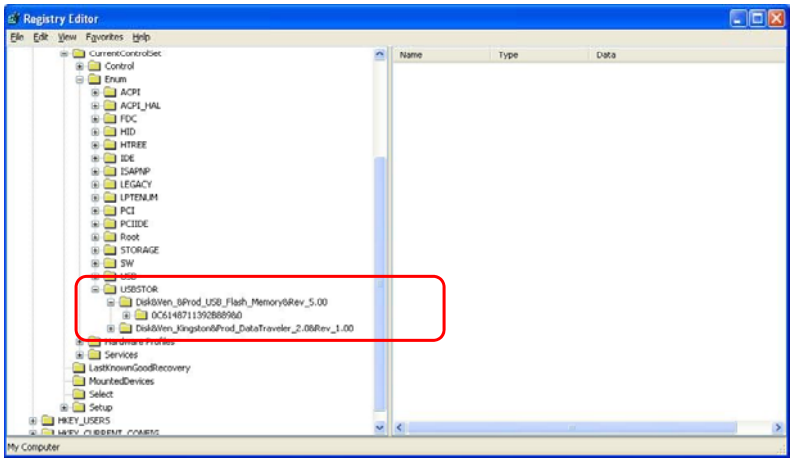


Lámina 126 Dr. Roberto Gómez Cárdenas

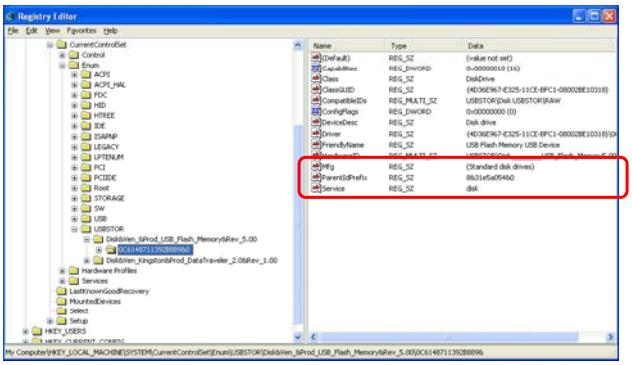
Llave USBSTOR y la instancia



ParentIdPrefix

- DWORD que permite relacionar el punto de montaje con el dispositivo USB que estuvo montado por última vez ahí.
- Cada que se asigna un punto de montaje diferente (E:, F: G:, etc) a un dispositivo USB se crea una nueva instancia que contiene un ParentIDPrefix diferente.

ParentIdPrefix y registro



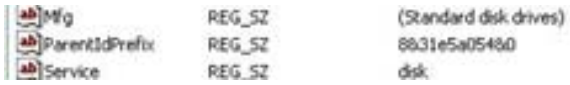


Lámina 129 Dr. Roberto Gómez Cárdenas

Los puntos de montaje

- Se encuentran en la llave
  - HKEY_LOCAL_MACHINES\System\Mounted Devices

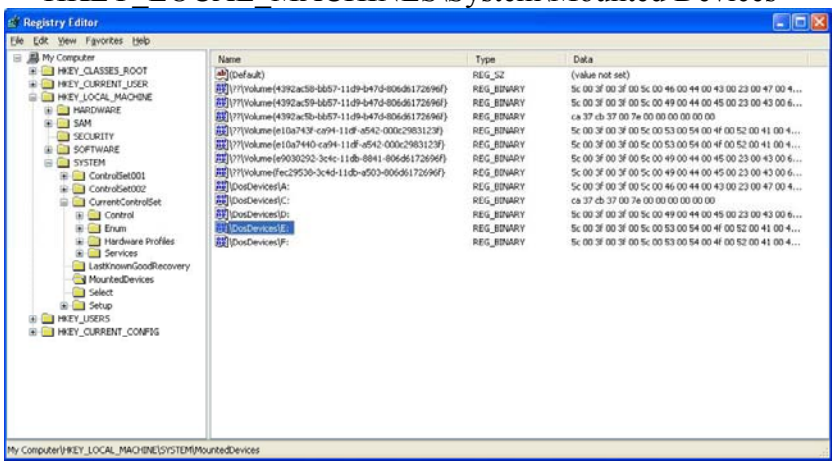


Lámina 130 Dr. Roberto Gómez Cárdenas

Información útil

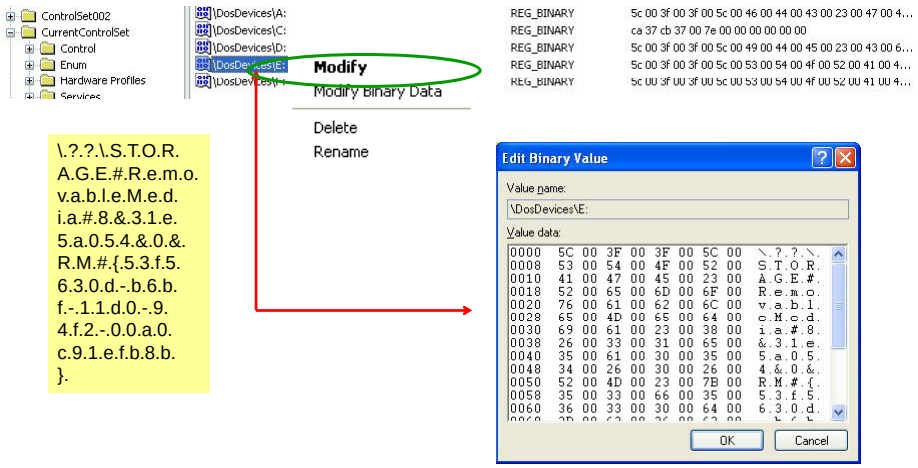
- Cada drive contiene información de tipo DWORD.
- El valor de este subllave tiene un formato similar al siguiente:

\??\STORAGE#RemovableMedia#**8&31e5a054&0**&RM#{53f5630d …..

- Este valor contiene el valor del ParentIdPrefix del último dispositivo USB que estuvo montado en dicha unidad.

Lámina 131 Dr. Roberto Gómez Cárdenas

Extrayendo la información



\??\STORAGE#RemovableMedia#8&31e5a054&0&RM#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}

Lámina 132 Dr. Roberto Gómez Cárdenas

Ultima vez que el dispositivo estuvo conectado.

- Consultar la llave en
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses
- Contiene subllaves de clase para dispositivos de discos y volúmenes
  - {53f56307-b6bf-11d0-94f2-00a0c91efb8b}
  - {53f5630a-b6bf-11d0-94f2-00a0c91efb8b}
- Las subllaves que corresponden a los discos tienen el siguiente formato.

Número de serie del dispositivo

#USBSTOR#Disk&Ven_&Prod_USB_Flash_Memory&Rev_5.00#0C6148711392B889&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

- Las subllaves que corresponden a los volúmenes tienen el siguiente formato.

\##?#STORAGE#RremovableMedia#8&31e5a054&0&RM#{53f5630a-b6bf-11d0-94f2-00a0c91efb8b}\#

ParentIdPrefix del dispositivo

Lámina 133 Dr. Roberto Gómez Cárdenas

La llave DeviceClasses y sus subllaves

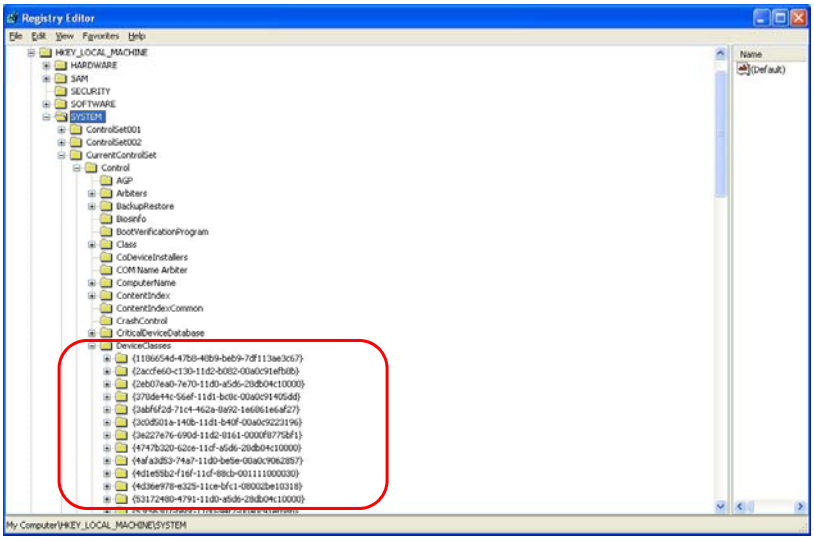


Lámina 134 Dr. Roberto Gómez Cárdenas

Disco y número de serie

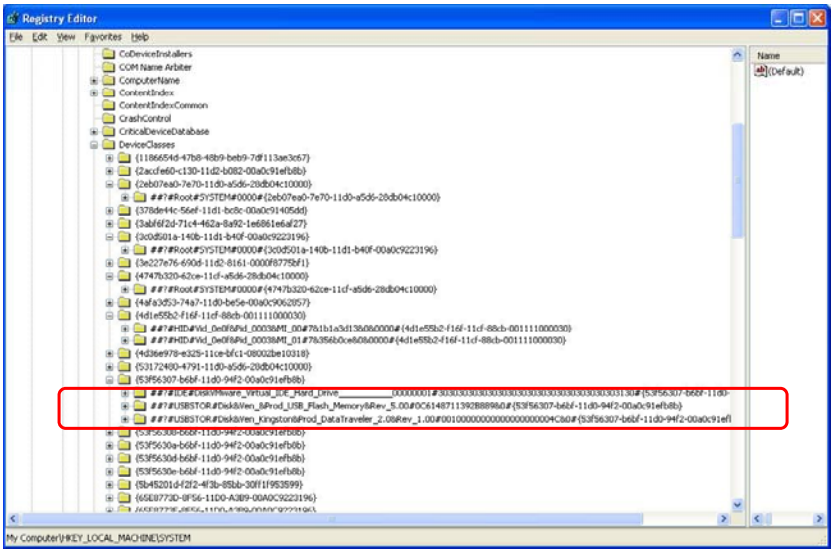


Lámina 135 Dr. Roberto Gómez Cárdenas

Volumen y ParentIdPrefix

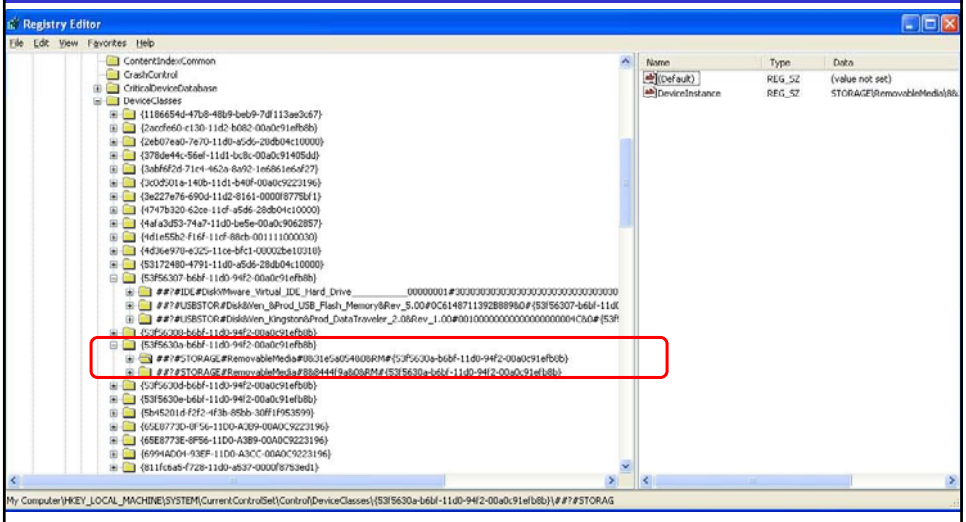


Lámina 136 Dr. Roberto Gómez Cárdenas

Obteniendo la ultima fecha y hora de escritura

- Fecha y hora almacenada en las subllave del disco.
- Necesario exportarlo a un archivo texto para analizar su contenido.

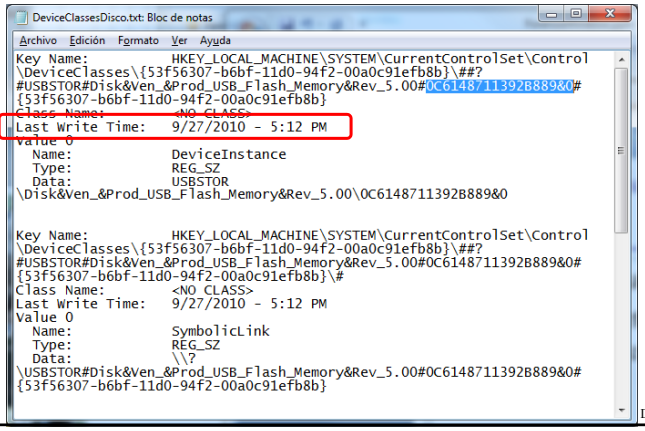


Lámina 137 Dr. Roberto Gómez Cárdenas

Otra opción

- Posible utilizar la herramienta Regscanner de Nirsoft para obtener la fecha y hora de última escritura.
  - http://www.nirsoft.net/utils/regscanner.html

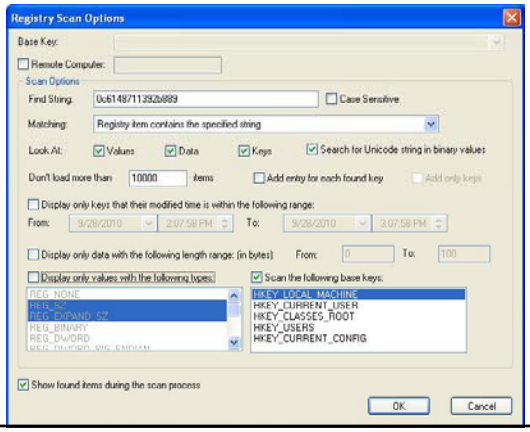


Lámina 138 Dr. Roberto Gómez Cárdenas

Salida regscanner

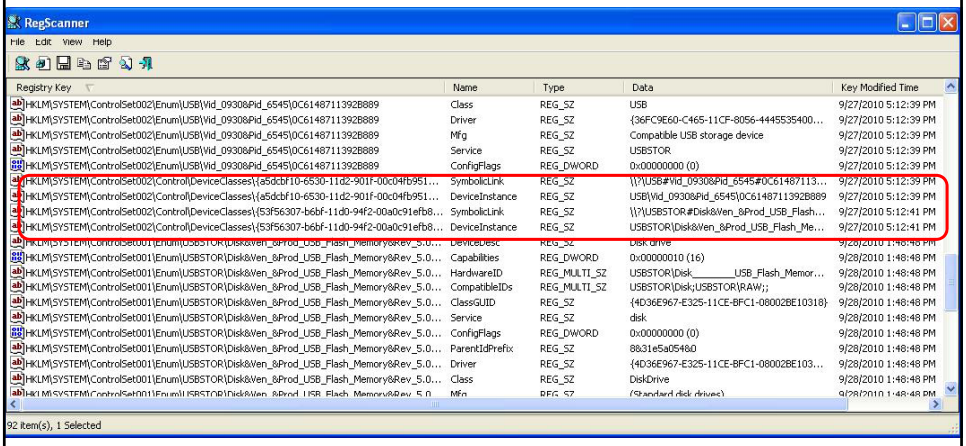


Lámina 139 Dr. Roberto Gómez Cárdenas

Herramienta automatizada

- USBDeview
  - http://www.nirsoft.net/utils/usb_devices_view.html
  - Proporciona información sobre los dispositivos USB que han estado conectados
  - Incluyendo la fecha que fue desconectado por última vez

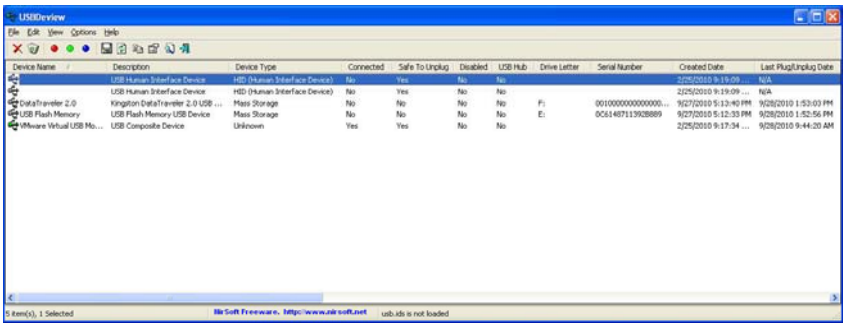
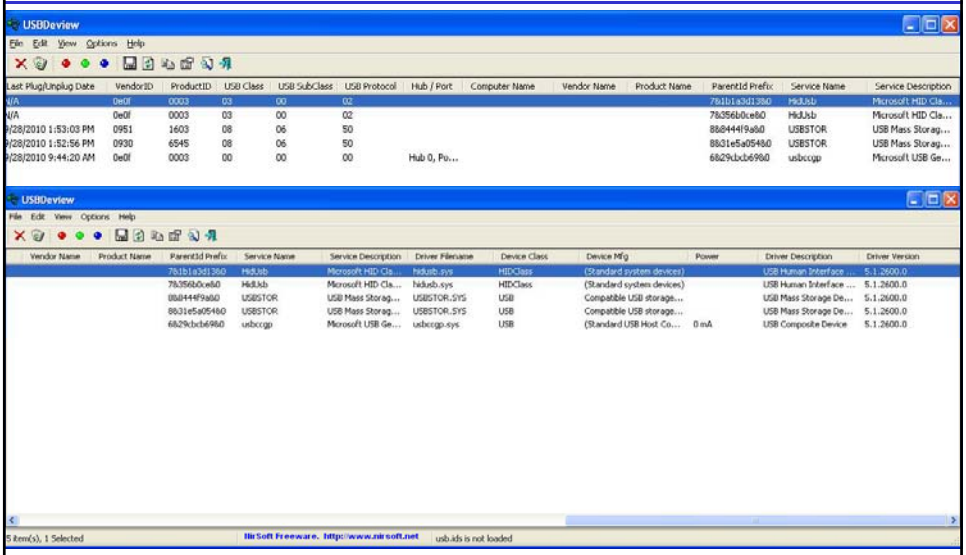


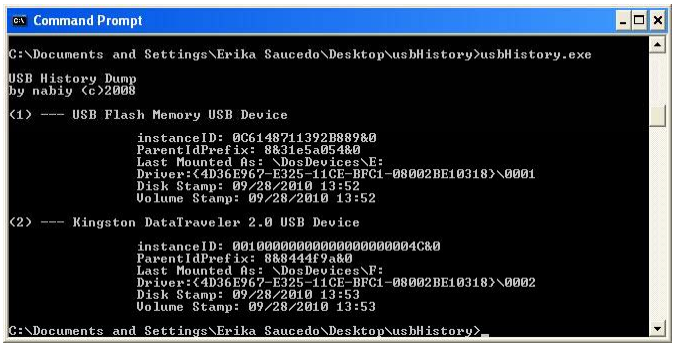
Lámina 140 Dr. Roberto Gómez Cárdenas

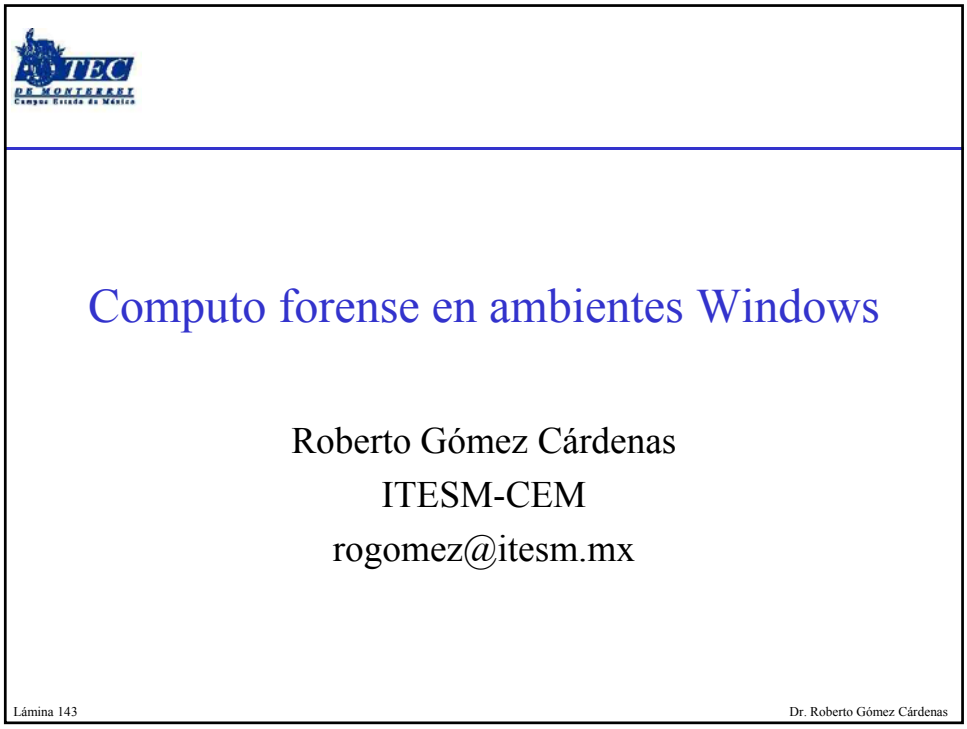
Más información proporcionada por USBDview



La herramienta UsbHistory.exe

- Liga:
  - http://nabiy.sdf1.org/index.php?work=usbHistory
- Proporciona información de la última vez que se conecto un dispositivo USB utilizando las llaves de disco y de volumen




Computo forense en ambientes Windows
Roberto Gómez Cárdenas
ITESM-CEM
rogomez@itesm.mx
Lámina 143
Dr. Roberto Gómez Cárdenas