CSE 4482
Computer Security Management:
Assessment and Forensics

Computer Forensics: Working with Windows and DOS Systems

Instructor: N. Vlajic, Fall 2010

Required reading:

Guide to Computer Forensics and Investigations

Chapter 6, pp. 207-219, pp. 232-240

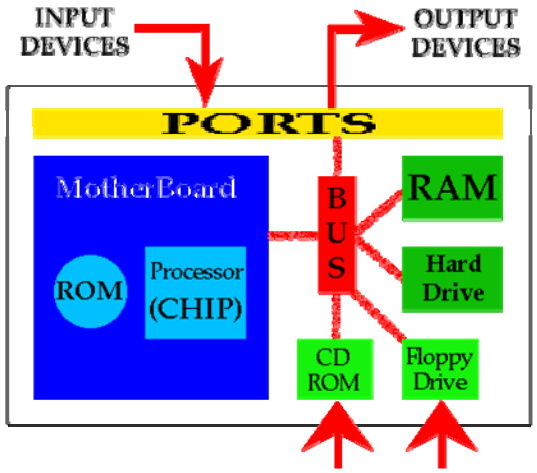
Learning Objectives

Upon completion of this material, you should be able to:

- List the key components of a disk drive.
- Explain the purpose and structure of Microsoft FAT (and NTFS) file system.
- Describe different types of file deletion, and what is required to completely remove a file from a disk.
- Explain how the Windows Registry works, and enlist different types of useful forensics information it stores.

How Computers Work

- **Main Components of a Computer**

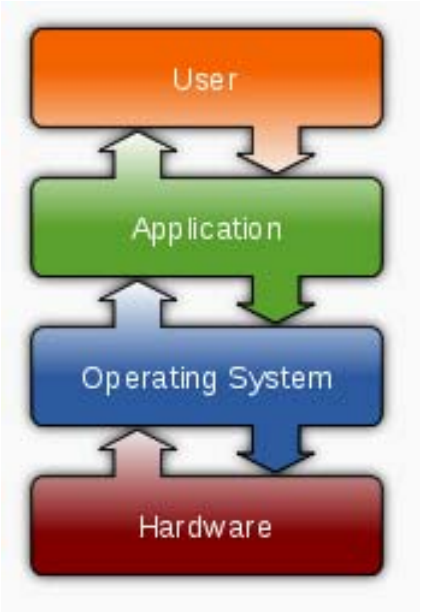


Storage	Speed	Capacity	Relative Cost ($)	Permanent?
Registers	Fastest	Lowest	Highest	No
RAM	Very Fast	Low/Moderate	High	No
Floppy Disk	Very Slow	Low	Low	Yes
Hard Disk	Moderate	Very High	Very Low	Yes

- CPU / Matherboard
  - processor
  - ROM (stores system-level programs that should be available at all times, e.g. BIOS)
  - busses / registers
- Main Memory – RAM (fast temporary memory)
- Input Devices
  - keyboard, mouse, ...
- Output Devices
  - monitor, printer, ...
- Secondary (Permanent) Storage
  - hard disks / drive, CD-ROM, USB, floppy, ...

Operating System

- **Operating System** – **software (program + data) that runs on a computer – it manages computer hardware & provides common services for efficient execution of various application software**

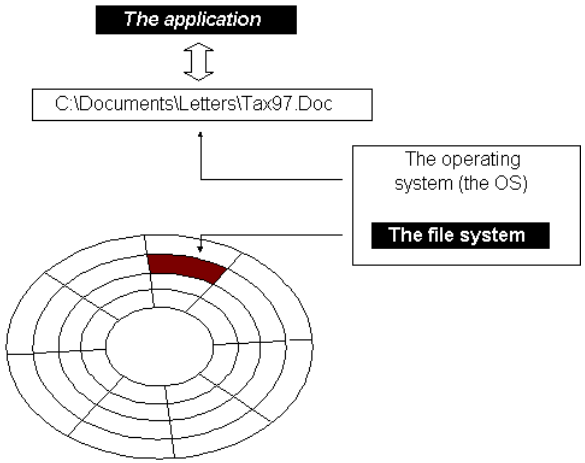


http://en.wikipedia.org/wiki/Operating_system

  - OSs are found on almost all ‘computing’ devices, e.g. cellular phones, video game consoles, web servers, routers, ...

File System

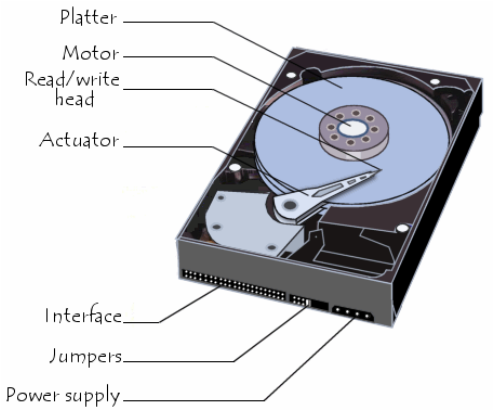
- **File System** – **method of storing and organizing computer files and their data**
  - gives an OS a road map to data on a data storage device (e.g. hard drive or CD-ROMs)
  - file system is usually directly related to an OS



http://www.karbosguide.com/images/u1901.gif

Disk Drives

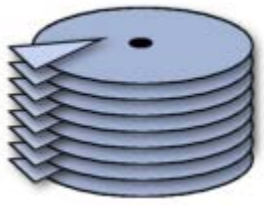
- **Disk Drive** – **consists of 1 or more platters coated with magnetic material – data is stored on platters in a particular way**



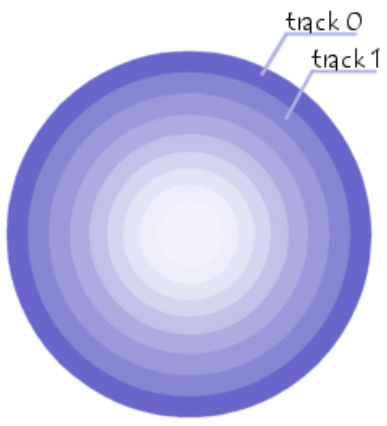
http://en.kioskea.net/contents/pc/disque.php3

  - each platters has 2 surfaces: top & bottom
  - key disk drive components/elements:
    - **geometry** – refers to a disk's structure of platters, tracks, and sectors
    - **head** – the device that reads and writes data to a drive – there is one head per platter
    - **tracks** – concentric circles on a disk platter where data is located
    - **sector** – a pie shaped section on a track, usually made up of 512 bytes (512 B)
    - **a cylinder** – consists of corresponding tracks on all platters (e.g. track 12 on all d.d. platters)

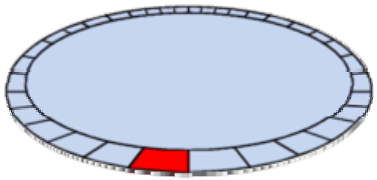
Disk Drives (cont.)



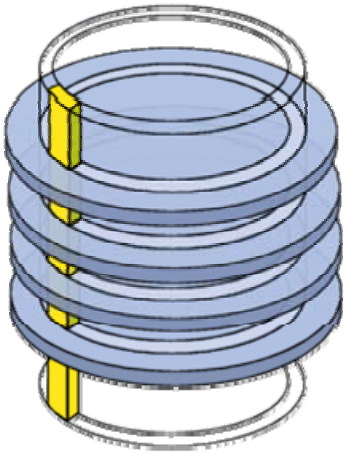
platters



tracks



sector

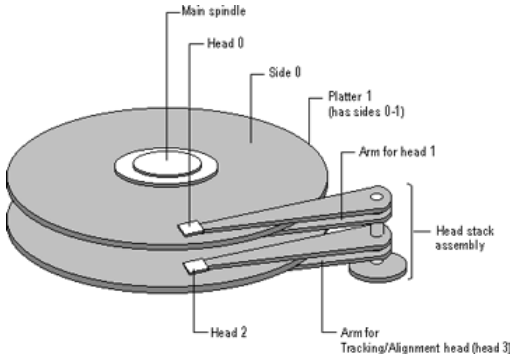


cylinder

http://en.kioskea.net/contents/pc/disque.php3

Disk Drives (cont.)

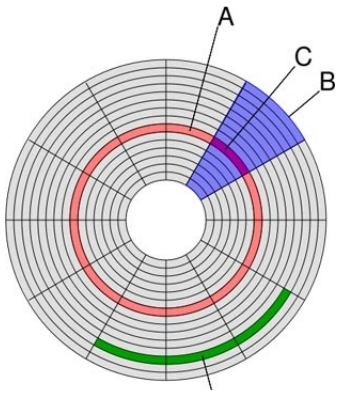
- **Heads – located on both sides of (each) platter only a few microns from the surface**
  - heads are static, disk/platters rotate at speed of n*1000 revolutions per minute! (~ 250km/h)
  - heads are 'inductive' – they can generate a magnetic field
    - by creating positive or negative fields, they polarise the disk (platter) surface in a very tiny area
    - when these areas are read afterwards, the detected polarity is transformed by a ADC into a 0 or 1



http://www.active-undelete.com/3tracks.htm

Disk Drives (cont.)

- **Cluster – a group of multiple sectors – logical unit of file storage on a hard drive**



cluster

  - number of sectors in a cluster (2^n), depends on:
    - disk size: bigger disk ⇒ bigger cluster
    - logical disk organization (FAT12 /16 /32 or NTFS)
  - whatever the logical size of a file, it is allocated disk space in multiples of clusters!
    - sectors in a cluster are physically adjacent on the disk
    - clusters in a file may NOT be adjacent
  - clusters are managed by computers OS

In FAT systems, individual sectors are NOT allocated to files, as it would take lots of overhead (time and space) to keep track of pieces of files that were 512 bytes small.
10GB disk ⇒ 20,000,000 sectors!

Disk Drives (cont.)

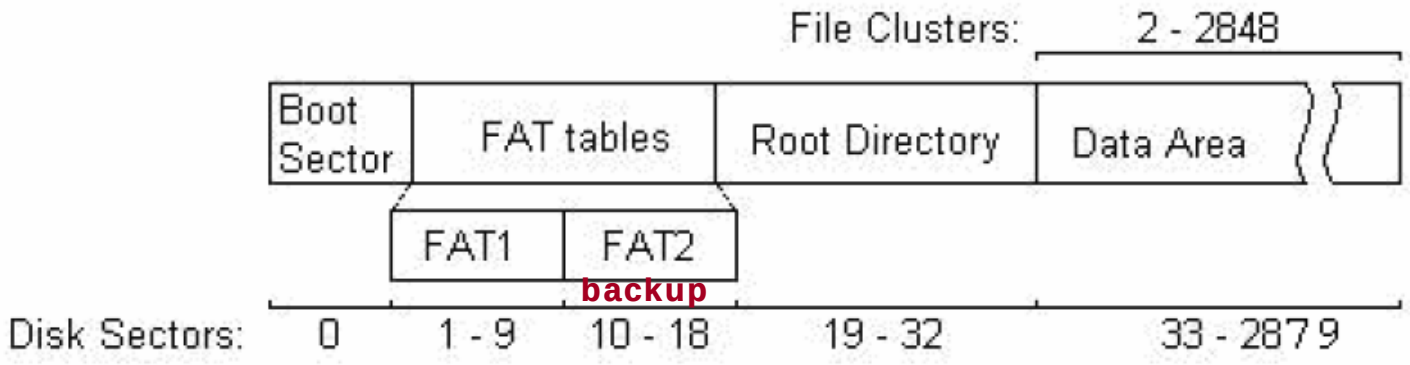
Table 6-2 Sectors and bytes per cluster

Drive size	Number of sectors per cluster	FAT16
0–32 MB	1	512 bytes
33–64 MB	2	1 KB
65–128 MB	4	2 KB
129–255 MB	8	4 KB
256–511 MB	16	8 KB
512–1023 MB	32	16 KB
1024–2047 MB	64	32 KB
2048–4095 MB	128	68 KB

FAT16 is not recommended for volumes larger than 511 MB. When relatively small files are placed on a FAT16 volume, FAT uses disk space inefficiently!

FAT File System

- **FAT x** – File Allocation Table **– family of file systems for DOS/Windows operating systems**
  - FAT (table) stores information on status of all clusters on the disk
    - equivalent to ‘table of content’
  - x = 12, 16, or 32 – number of bits used for cluster identification/numbering
    - bit-size of each FAT table entry



http://www.disc.ua.es/~gil/FAT12Description.pdf

FAT File System (cont.)

Example: FAT12, FAT16, FAT32

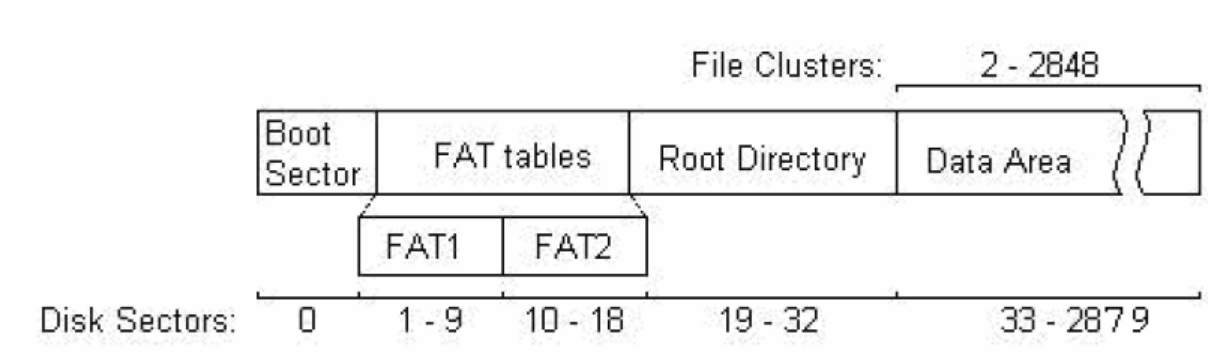
FAT			
Developer	Microsoft		
Full Name	File Allocation Table		
	(12-bit version)	(16-bit version)	(32-bit version with 28 bits used)
Introduced	August 1980 (QDOS)	November 1987, (Compaq DOS 3.31)	August 1996 (Windows 95 OSR2)

Attribute	FAT12	FAT16	FAT32
Used For	Floppies and very small hard disk volumes	Small to moderate-sized hard disk volumes	Medium-sized to very large hard disk volumes
Size of Each FAT Entry	12 bits	16 bits	28 bits
Maximum Number of Clusters	4,086	65,526	~268,435,456
Cluster Size Used	0.5 KB to 4 KB	2 KB to 32 KB	4 KB to 32 KB
Maximum Volume Size	16,736,256	2,147,123,200	about 2^41

http://www.pcguide.com/ref/hdd/file/partSizes-c.html

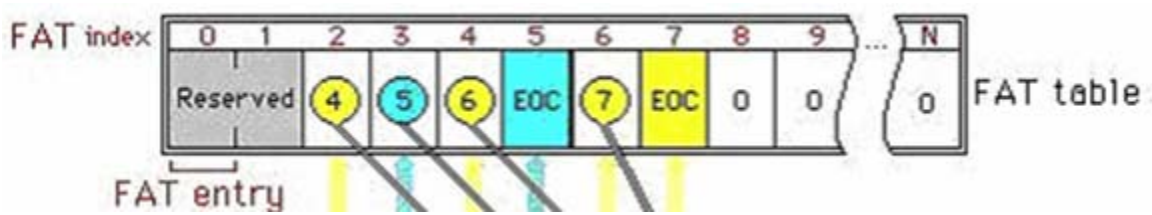
FAT File System (cont.)

- **FAT x (cont.)**
  - major sections on a FAT hard disk:
    1) **Boot Sector** – occupies the 1st cluster on the disk
       - contains specific information about organization of the file system, including: type of FAT (12/16/32) system, # of bytes per sector, # of sectors per track, # of sectors per cluster, # of read heads, # of FAT tables, # of clusters per FAT table, etc.
    2) **FAT Tables**
       - list of entries corresponding to clusters on the disk
       - each entry records current status of respective cluster



FAT File System (cont.)

Example: FAT entry values



FAT entry values:

FAT12	FAT16	FAT32	Description
0x000	0x0000	0x00000000	Free Cluster
0x001	0x0001	0x00000001	Reserved value; do not use
0x002–0xFEF	0x0002–0xFFEF	0x00000002– 0x0FFFFFEF	Used cluster; value points to next cluster
0xFF0–0xFF6	0xFFF0–0xFFF6	0x0FFFFFF0– 0x0FFFFFF6	Reserved values; do not use[30].
0xFF7	0xFFF7	0x0FFFFFF7	Bad sector in cluster or reserved cluster
0xFF8–0xFFF	0xFFF8–0xFFFF	0x0FFFFFF8– 0x0FFFFFFF	Last cluster in file (EOC)

http://en.wikipedia.org/wiki/File_Allocation_Table

FAT File System (cont.)

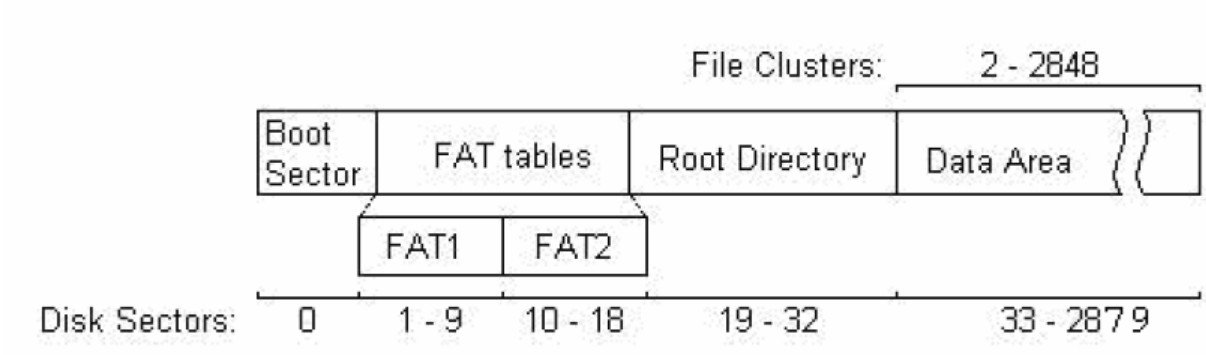
- **FAT x (cont.)**
  - major sections on hard disk (cont.):

3) **Root Directory** (FAT12/16 only)

- stores Directory Table – table of 32-bit long entries for each file & directory created on the disk

4) **Data Area**

- contains file & directory data – occupies remaining sectors (clusters) on the disk
- first cluster of Data Area is numbered 2; though, this is physical sector 33!



FAT File System (cont.)

Example: (Root) Directory Table entries

0-7	8-10	11	12-21	22-23	24-25	26-27	28-31
File name	exten	attributes	Reserved space	Time	date	Starting cluster	File size

ASCII characters padded with spaces. Possibilities:
0x00 – entry unused
0x2E – subdirectory
0xE5 – file deleted

Name extension, e.g. txt, doc, pdf, ...

Describes how the file is treated by the system:
0 – read only
1 – hidden
2 – system file, ...

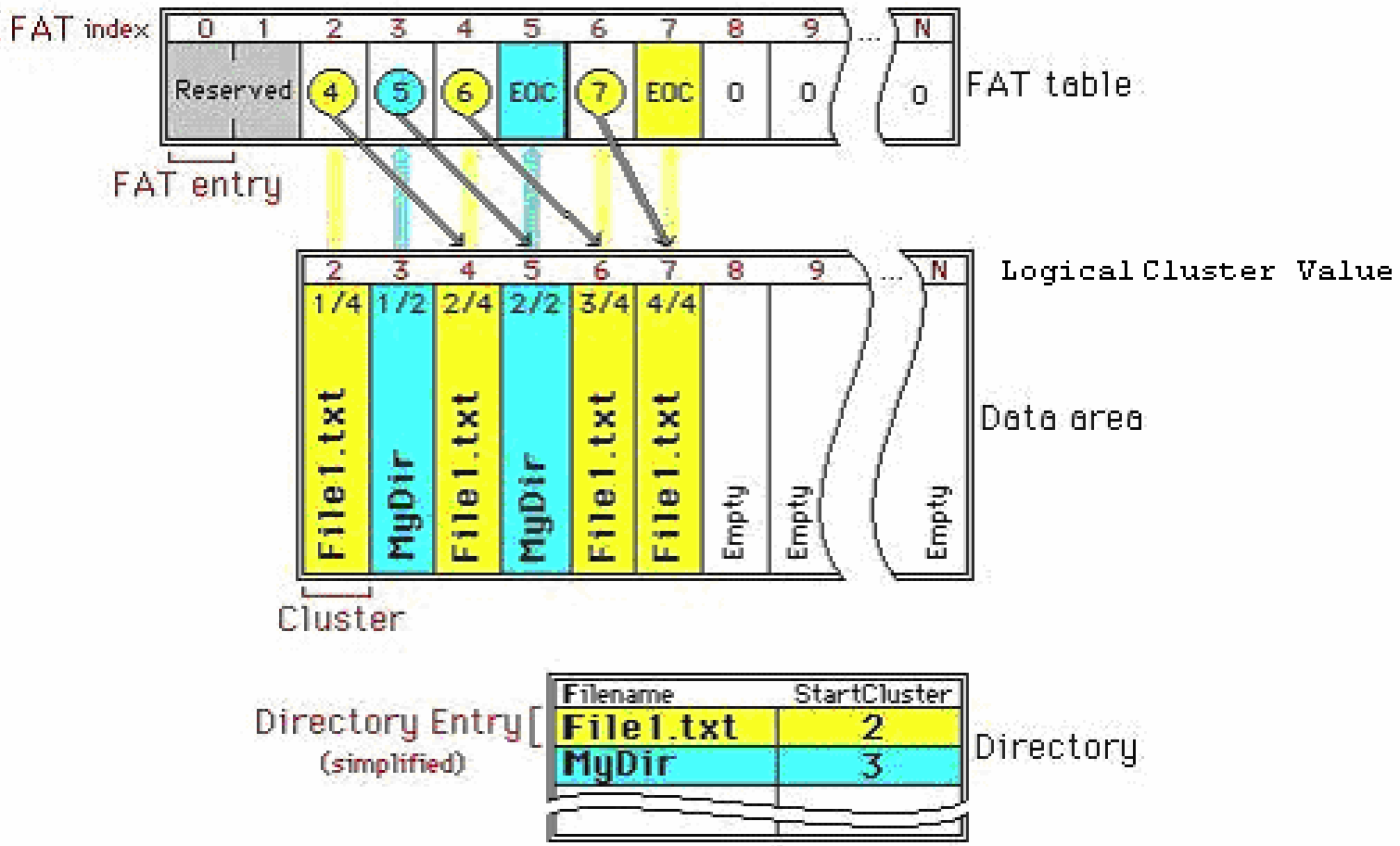
Record the last change of file:
seconds/minutes/hours
day/month/year

Cluster number where the file begins.

Number of clusters allocated to this file. (May be different from the actual amount of data in the file.)

FAT File System (cont.)

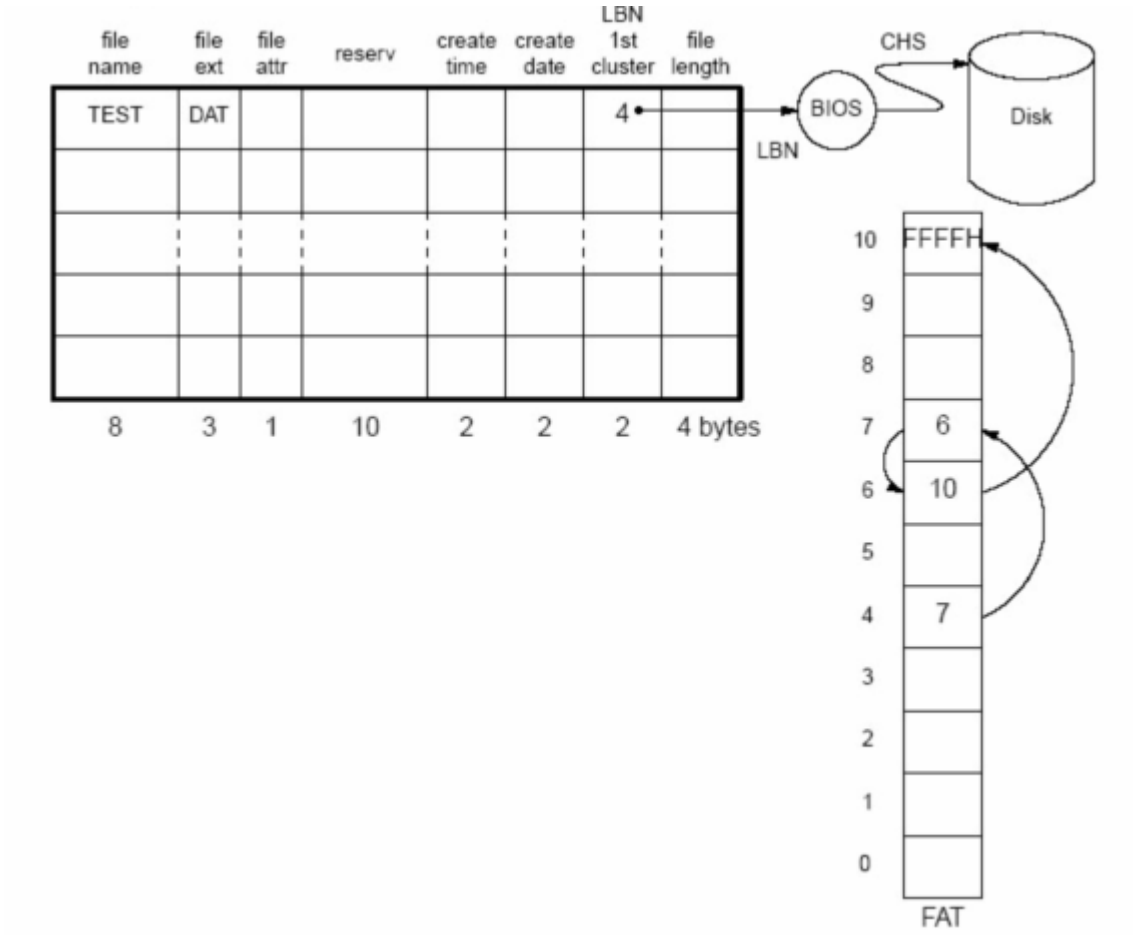
Example: Use of FAT system



http://www.disc.ua.es/~gil/FAT12Description.pdf

FAT File System (cont.)

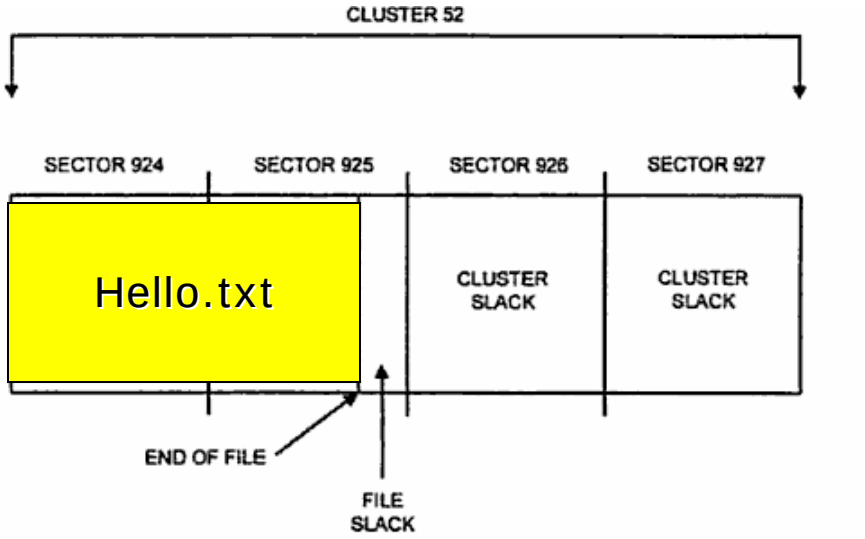
Example: File fragmentation / cluster allocation in FAT



http://homepage.cs.uri.edu/courses/fall2004/hpr108b/FAT.htm

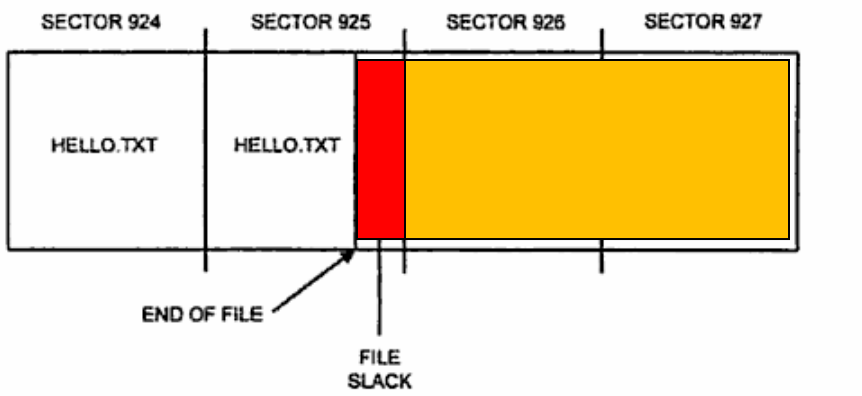
FAT File System (cont.)

- **Slack Space in FAT** – **phenomenon caused by the way how computers store data/files:**
  - files are allocated cluster-sized chunks and they are written in sector-sized chunks – regardless of the actual size of data/file
    - data may not be big enough to fill (all) segments, i.e. clusters



FAT File System (cont.)

- **Slack Space in FATs**
  - sector slack - space between EOF and end of last sector that file was written to
    - also known as RAM slack as OS pulls any info available in RAM at that point (memory dump) to fill this space – e.g. logon IDs, passwords, segments of other files
    - not an issue in post Windows 98 / NT
  - cluster slack - remaining sectors in cluster
    - also known as file slack – contains whatever was last written by disk in those sectors (e.g. parts of a deleted file)



FAT File System (cont.)

Common misconception: when we delete a file, OS writes 0-bytes over corresponding segments/clusters on the disk.

- **Deleting FAT Files** – **system places deletion mark on the file**
  - deletion mark $\Rightarrow$ first letter of the file name is replaced with E5 (lower-case Greek letter σ)
  - FAT entries of respective clusters are still unchanged!
  - in DATA AREA cluster still preserve the original data!

FAT File System (cont.)

Example: Deleting by sending to Recycle Bin

File Directory Table (FDT) before and after deletion of “test1.txt” file.

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0008233120	42	78	00	74	00	00	00	FF	FF	FF	FF	0F	00	B9	FF	FF	Bx.t...ÿÿÿÿ..¹ÿÿ
0008233136	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	00	00	FF	FF	FF	FF	ÿÿÿÿÿÿÿÿÿÿ..ÿÿÿÿ
0008233152	01	74	00	65	00	73	00	74	00	20	00	0F	00	B9	66	00	.t.e.s.t. ...¹f.
0008233168	69	00	6C	00	65	00	20	00	32	00	00	00	2E	00	74	00	i.l.e. .2.....t.
0008233184	54	45	53	54	46	49	7E	32	54	58	54	20	00	54	5C	53	TESTFI~2TXT .T\S
0008233200	B2	34	B2	34	00	00	81	53	B2	34	16	00	F0	4B	00	00	²4²4..S²4..ðK..
0008233216	54	45	53	54	31	20	20	20	54	58	54	20	18	54	5C	53	TEST1 TXT .T\S
0008233232	B2	34	B2	34	00	00	7B	53	B2	34	0C	00	E0	97	00	00	²4²4..{S²4..à..
0008233248	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0008233120	42	78	00	74	00	00	00	FF	FF	FF	FF	0F	00	B9	FF	FF	Bx.t...ÿÿÿÿ..¹ÿÿ
0008233136	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	00	00	FF	FF	FF	FF	ÿÿÿÿÿÿÿÿÿÿ..ÿÿÿÿ
0008233152	01	74	00	65	00	73	00	74	00	20	00	0F	00	B9	66	00	.t.e.s.t. ...¹f.
0008233168	69	00	6C	00	65	00	20	00	32	00	00	00	2E	00	74	00	i.l.e. .2.....t.
0008233184	54	45	53	54	46	49	7E	32	54	58	54	20	00	54	5C	53	TESTFI~2TXT .T\S
0008233200	B2	34	B2	34	00	00	81	53	B2	34	16	00	F0	4B	00	00	²4²4..S²4..ðK..
0008233216	E5	45	53	54	31	20	20	20	54	58	54	20	18	54	5C	53	åEST1 TXT .T\S
0008233232	B2	34	B2	34	00	00	7B	53	B2	34	0C	00	E0	97	00	00	²4²4..{S²4..à..

http://www.easeus.com/data-recovery-ebook/file-deletion-in-FAT32.htm

FAT File System (cont.)

Example: Deleting by sending to Recycle Bin (cont.)

File Allocation Table (FAT) before and after deletion of “test1.txt” file.

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0000018432	F8	FF	FF	0F	FF	FF	FF	FF	FF	FF	FF	0F	FF	FF	FF	0F
0000018448	FF	FF	FF	0F	FF	FF	FF	0F	FF	FF	FF	0F	FF	FF	FF	0F
0000018464	FF	FF	FF	0F	FF	FF	FF	0F	FF	FF	FF	0F	FF	FF	FF	0F
0000018480	0D	00	00	00	0E	00	00	00	0F	00	00	00	10	00	00	00
0000018496	11	00	00	00	12	00	00	00	13	00	00	00	14	00	00	00
0000018512	15	00	00	00	FF	FF	FF	0F	17	00	00	00	18	00	00	00
0000018528	19	00	00	00	1A	00	00	00	FF	FF	FF	0F	FF	FF	FF	0F
0000018544	FF	FF	FF	0F	FF	FF	FF	0F	00	00	00	00	00	00	00	00
0000018560	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0000018432	F8	FF	FF	0F	FF	FF	FF	FF	FF	FF	FF	0F	FF	FF	FF	0F
0000018448	FF	FF	FF	0F	FF	FF	FF	0F	FF	FF	FF	0F	FF	FF	FF	0F
0000018464	FF	FF	FF	0F	FF	FF	FF	0F	FF	FF	FF	0F	FF	FF	FF	0F
0000018480	0D	00	00	00	0E	00	00	00	0F	00	00	00	10	00	00	00
0000018496	11	00	00	00	12	00	00	00	13	00	00	00	14	00	00	00
0000018512	15	00	00	00	FF	FF	FF	0F	17	00	00	00	18	00	00	00
0000018528	19	00	00	00	1A	00	00	00	FF	FF	FF	0F	FF	FF	FF	0F
0000018544	FF	FF	FF	0F	FF	FF	FF	0F	00	00	00	00	00	00	00	00
0000018560	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

http://www.easeus.com/data-recovery-ebook/file-deletion-in-FAT32.htm

FAT File System (cont.)

Example: Deleting by clearing from Recycle Bin

File Allocation Table (FAT) before and after clearing Recycle Bin.

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0000018432	F8	FF	FF	0F	FF	FF	FF	FF	FF	FF	FF	0F	FF	FF	FF	0F
0000018448	FF	FF	FF	0F	FF	FF	FF	0F	FF	FF	FF	0F	FF	FF	FF	0F
0000018464	FF	FF	FF	0F	FF	FF	FF	0F	FF	FF	FF	0F	FF	FF	FF	0F
0000018480	0D	00	00	00	0E	00	00	00	0F	00	00	00	10	00	00	00
0000018496	11	00	00	00	12	00	00	00	13	00	00	00	14	00	00	00
0000018512	15	00	00	00	FF	FF	FF	0F	17	00	00	00	18	00	00	00
0000018528	19	00	00	00	1A	00	00	00	FF	FF	FF	0F	FF	FF	FF	0F
0000018544	FF	FF	FF	0F	FF	FF	FF	0F	00	00	00	00	00	00	00	00
0000018560	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0000018432	F8	FF	FF	0F	FF	FF	FF	FF	FF	FF	FF	0F	FF	FF	FF	0F
0000018448	FF	FF	FF	0F	FF	FF	FF	0F	FF	FF	FF	0F	FF	FF	FF	0F
0000018464	FF	FF	FF	0F	FF	FF	FF	0F	FF	FF	FF	0F	FF	FF	FF	0F
0000018480	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000018496	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000018512	00	00	00	00	00	00	00	00	17	00	00	00	18	00	00	00
0000018528	19	00	00	00	1A	00	00	00	FF	FF	FF	0F	FF	FF	FF	0F
0000018544	FF	FF	FF	0F	FF	FF	FF	0F	00	00	00	00	00	00	00	00
0000018560	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

Only after Recycle Bin is emptied, FAT clusters of the deleted file are set to ‘free’ (0x00).

FAT File System (cont.)

Why is it critical to stop using a computer as soon as it is learned that the computer is/was involved in an illegal case
(until a computer forensics specialist can examine it)?

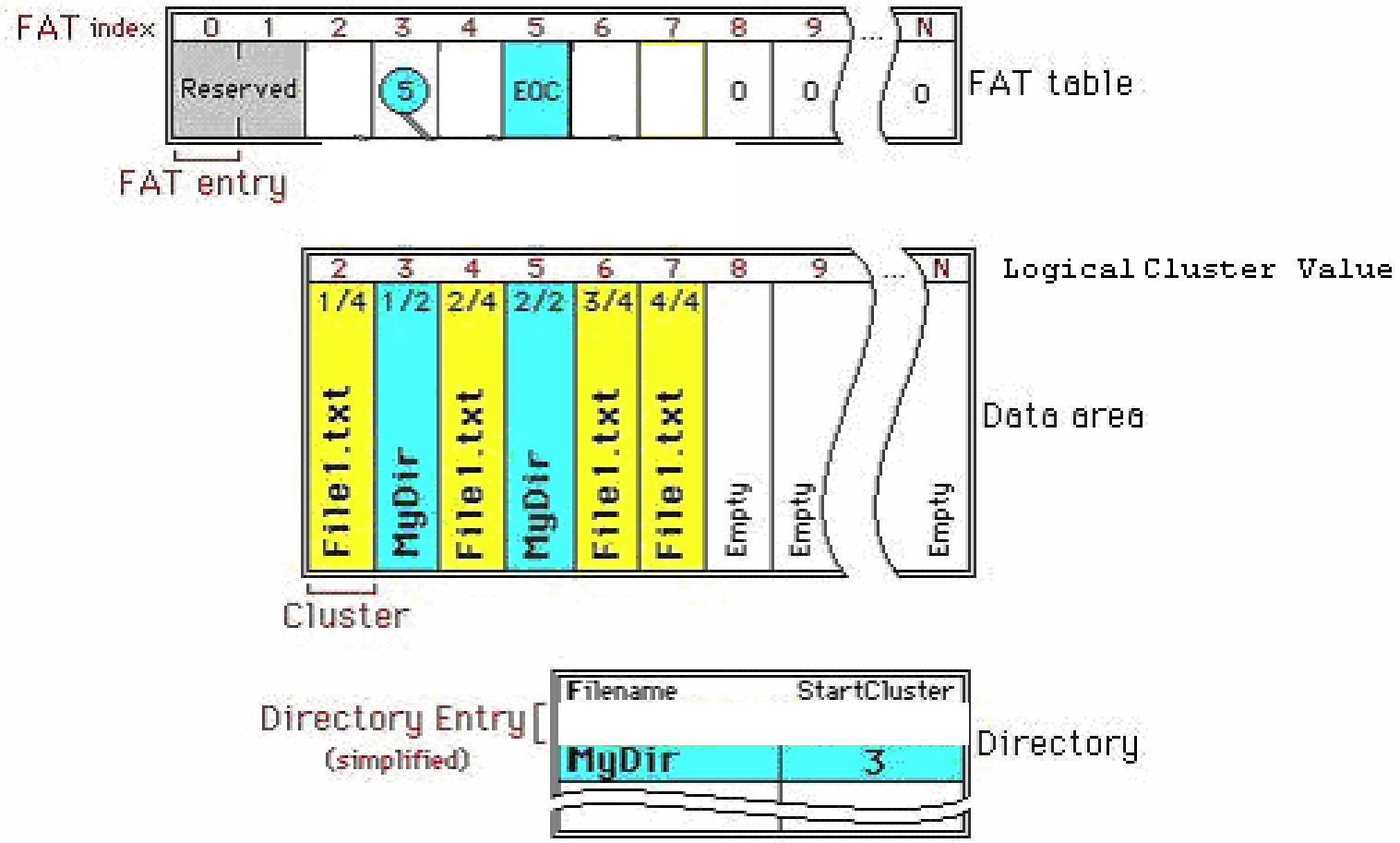
http://pctechnotes.com/wp-content/uploads/2009/05/computer-forensic.jpg

FAT File System (cont.)

- **Forensics Implications**
  - On deletion of a file, the data contained in a file is NOT ‘gone’ – it is merely ‘hidden’ from he operating system and the space it occupies is made available for reuse.
  - Deleted data still resides in the space previously allocated to it, unless overwritten.
  - It is possible to ‘undelete’ (reconstruct) a file – or some of its parts – even after Recycle bin has been emptied – the only information that cannot be recovered is the first letter of the file!
  - However, there may be evidential difficulties with files recovered from unallocated space. We cannot state the date and time attributes of even a complete file found in unallocated space, as there is no respective entry in the File Directory Table.

FAT File System (cont.)

Example: Content of a file after emptying of Recycle Bin



FAT File System (cont.)

- **Disk Formatting** – **still does not erase data!**
  - only pointers (FAT and FDT) get destroyed
  - data that formed the file remains intact in their locations

- **Disk Wiping** – **secure deletion – wiped files have their directory entries and allocated space physically overwritten by random or user-defined characters**
  - Windows wiping tools:
    - Disk Wipe: http://www.diskwipe.org/
    - Eraser: http://eraser.heidi.ie/

NTFS File System

- **NTFS** – New Technology File System **– introduced for Windows NT and Vista**
  - provides significant improvements over FAT, including:
    - **file and folder permissions** – folder and file access can be controlled individually
    - **file encryption** – NTFS enables strong encryption of files and folders extremely resistant to attacks
    - **file compression** – NTFS enables lossy compression on both files and folders
    - **disk efficiency** – NTFS supports smaller cluster size than FAT32
    - **greater reliability** – NTFS writes a log of changes being made to files and folders (NTFS journal), which helps the OS to recover from system failures ...

Windows Registry

- **Windows Registry** – **critical part of any Windows OSs - hierarchical database containing configuration information about:**
  - system hardware;
  - installed software (programs);
  - property settings;
  - profile for each user, etc.

  - OS uses instructions stored in the registry to determine how installed hardware and and software should function

  - e.g. typical software comes with a Windows installer that writes to the registry during installation

    - system must be restarted for changes to take place ...

Windows Registry (cont.)

Example: Opening Windows Registry

Type '**regedit'** in cmd window.

Registry comprises 5 to 7 hierarchical folders – **hives**.

Folders' names start with HKEY – Handle to a Key.

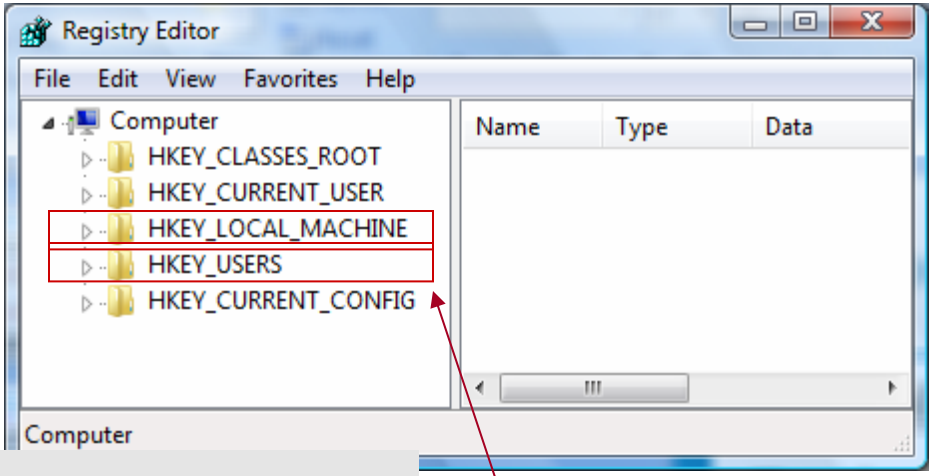


Table 6-7 Registry HKEYs and their functions

HKEY	Function
HKEY_CLASS_ROOT	A symbolic link to HKEY_LOCAL_MACHINE\SOFTWARE\Classes; provides file type and file extension information, URL protocol prefixes, and so forth
HKEY_CURRENT_USER	A symbolic link to HKEY_USERS; stores settings for the currently logged-on user
HKEY_LOCAL_MACHINE	Contains information about installed hardware and software
HKEY_USERS	Stores information for the currently logged-on user; only one key in this HKEY is linked to HKEY_CURRENT_USER
HKEY_CURRENT_CONFIG	A symbolic link to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profile*xxxx* (with *xxxx* representing the current hardware profile); contains hardware configuration settings

These 2 folders are 'real' – the other three are shortcuts (aliases) to branches within the two main hives.

Windows Registry (cont.)

- **Forensics Implications** – **information (**i.e. potential evidence**) that reside in the Registry make it a significant forensics resource**
  - information that can be found in the registry include:
    - general information about the OS
    - startup (boot-time) applications
    - logs of computers that have communicated with the host
    - logs of USBs that have been connected to the host
    - logs of Web site histories and typed URLs
    - downloaded files/programs, e.g. wiping programs to destroy evidence
    - auto complete Internet Explorer passwords

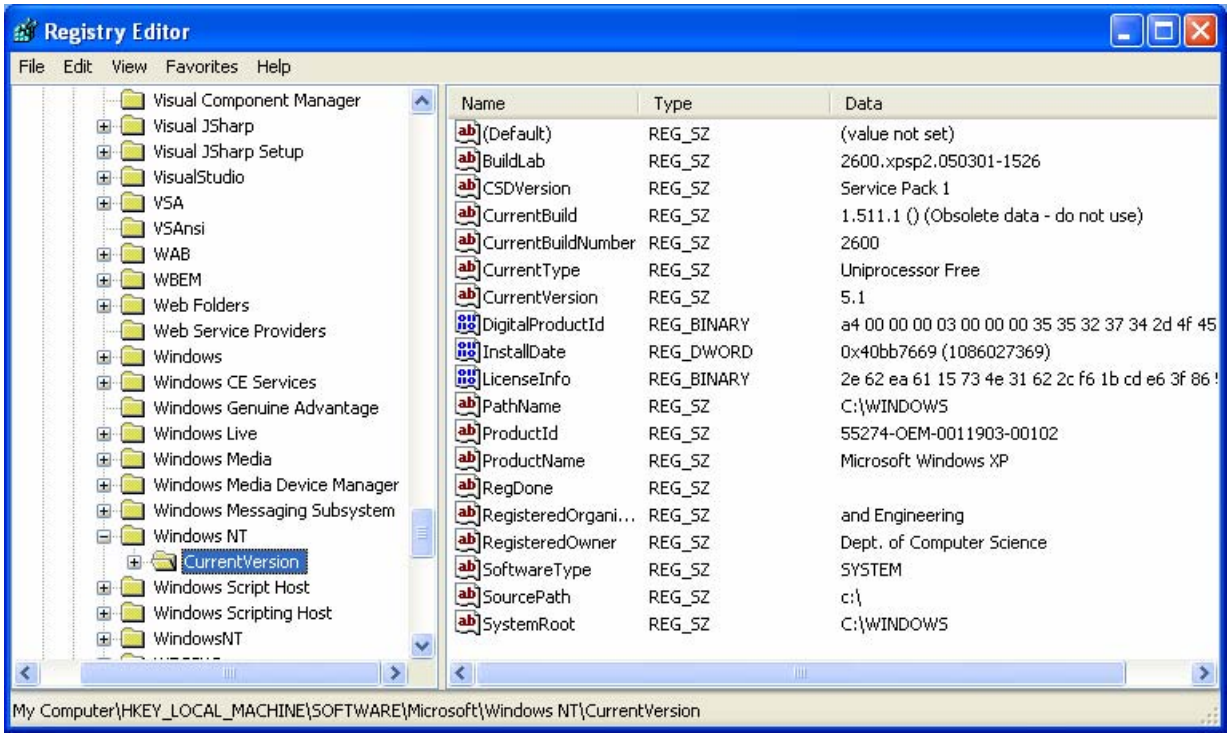
Windows Registry (cont.)

Example: Registry Information about OS

Keys to look at (investigate):

HKLM\Software\Microsoft\Windows NT\CurrentVersion

Obtained info: OS version, Installation Date, Product ID, etc.



Windows Registry (cont.)

Example: Registry Information about Startup Applications

Keys to look at (investigate):

HKLM\Software\Microsoft\Windows\CurrentVersion\Run

HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce

(Typically used to load an application for installation the next time the computer boots. After the machine reboots, the entry is removed.)

Services/programs enlisted in these 'files' run each time / when a user logs on.

Malware (spyware, trojans, worms, viruses) often attempt to embed themselves in these startup areas.

If a computer is suspected to have been involved in an intrusion case, and the user denies their involvement, it is possible that the system was compromised and used to initiate the attack

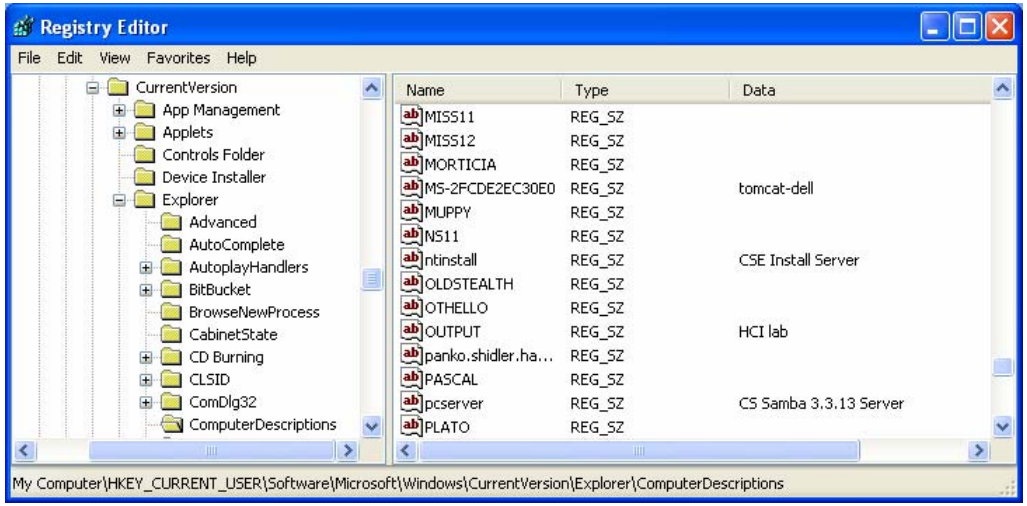
Windows Registry (cont.)

Example: Registry Information about LAN Computers

Keys to look at (investigate):

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComputerDescriptions

A computer on a properly configured LAN should be able to display all the computers on that network through MyNetworkPlace. The list of these computer – i.e. devices that the host has ever connected to – is stored in the Registry.



ComputerDescription feature is useful in determining whether the host/user was connected to certain computers or belonged to a specific LAN.

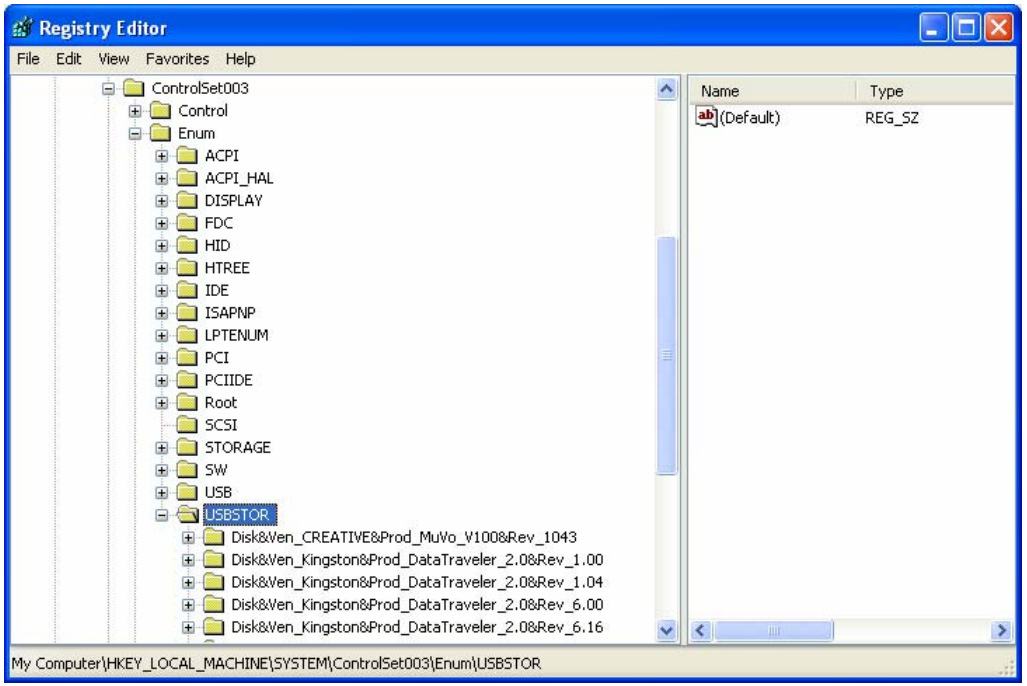
Windows Registry (cont.)

Example: Registry Information about USB Devices

Keys to look at (investigate):

HKLM\System\ControlSet00x\Enum\USBSTOR

Anytime a device is connected to a USB, driver are queried and the device's information is stored into the Registry.



Windows Registry (cont.)

Example: Registry Information about Internet Explorer

Keys to look at (investigate):

HKCU\Software\Microsoft\InternetExplorer\.....

----------\TypedURLs

Stores all URS that the user has typed into the address field of the web browser. “Clear History” deletes TypedURLs entirely ☹.

----------\Download

Reveals the last directory used to store a downloaded file from Internet explorer.

Windows Registry (cont.)

Example: Registry Information about Windows Passwords

Keys to look at (investigate):

HKCU\Software\Microsoft\InternetExplorer\Main
Key to look at: "FormSuggest PW Ask" – should be "yes" ⇒ Windows AutoComplete Password feature is enabled.

List of 'memorized' passwords can be found at:
HKCU\Software\Microsoft\InternetExplorer\IntelliForms\SPW