#### Guide to Computer Forensics and Investigations Fourth Edition

#### Chapter 6 Working with Windows and DOS Systems

#### Objectives

- Explain the purpose and structure of file systems
- Describe Microsoft file structures
- Explain the structure of New Technology File System (NTFS) disks
- List some options for decrypting drives encrypted
   with whole disk encryption

#### **Objectives** (continued)

- Explain how the Windows Registry works
- Describe Microsoft startup tasks
- Describe MS-DOS startup tasks
- Explain the purpose of a virtual machine

#### **Understanding File Systems**

#### • File system

- Gives OS a road map to data on a disk
- Type of file system an OS uses determines how data is stored on the disk
- A file system is usually directly related to an OS
- When you need to access a suspect's computer to acquire or inspect data
  - You should be familiar with the computer's platform

#### Understanding the Boot Sequence

- Complementary Metal Oxide Semiconductor (CMOS)
  - Computer stores system configuration and date and time information in the CMOS
    - When power to the system is off
- Basic Input/Output System (BIOS)
  - Contains programs that perform input and output at the hardware level

# Understanding the Boot Sequence (continued)

#### Bootstrap process

- Contained in ROM, tells the computer how to proceed
- Displays the key or keys you press to open the CMOS setup screen
- CMOS should be modified to boot from a forensic floppy disk or CD

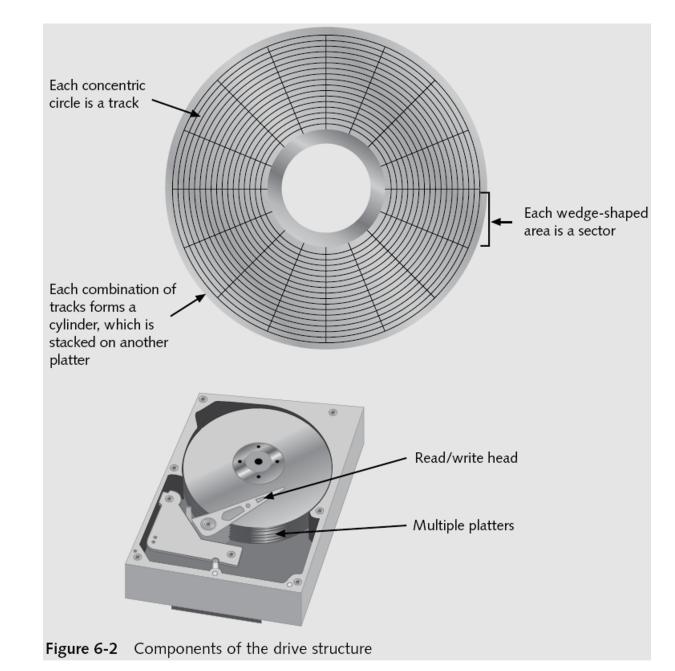
# Understanding the Boot Sequence (continued)

		Phoenix	dBIOS Setup l	Itility			
Nain	Advanced	Security	Boot	Exit			
Optical D Floppy Di					It	cem Specific Help	Boot sequence accesses the optical drive (CD or DVD)
+Hard Disk Network	Drive				collap <crtl+ <shift disabl <space< td=""><td><pre>&gt; expands or ses devices. Enter&gt; expands all +1&gt; enables or es a device. &gt; or &lt;+&gt; moves the : up, &lt;-&gt; moves it</pre></td><td>first</td></space<></shift </crtl+ 	<pre>&gt; expands or ses devices. Enter&gt; expands all +1&gt; enables or es a device. &gt; or &lt;+&gt; moves the : up, &lt;-&gt; moves it</pre>	first
F1 Help	↑↓Select 1	Item -/+,Sp	ace Chan	ge Values	F9	Setup Defaults	
ESC Exit	← Select 1	Henu Press l	Enter Sele	et > Sub-M	F10	Save and Exit	

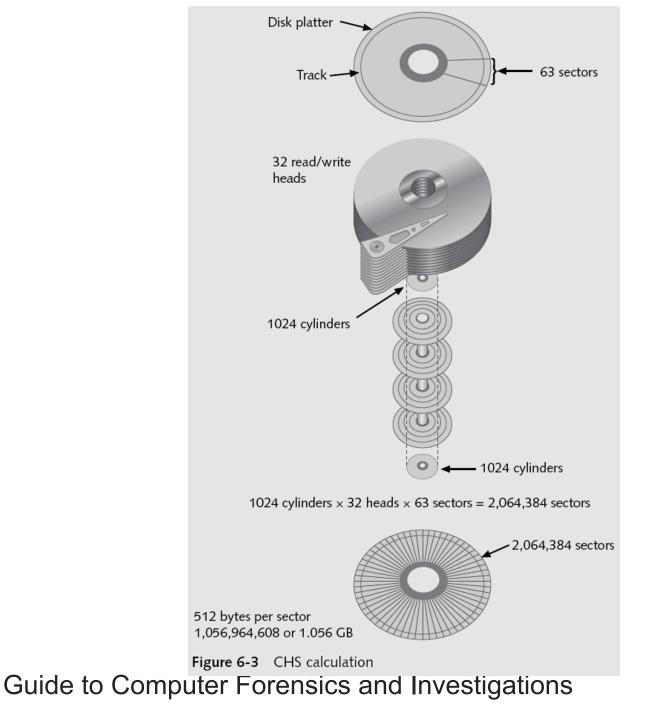
Figure 6-1 A typical CMOS setup screen

#### **Understanding Disk Drives**

- Disk drives are made up of one or more platters coated with magnetic material
- Disk drive components
  - Geometry
  - Head
  - Tracks
  - Cylinders
  - Sectors







### Understanding Disk Drives (continued)

- Properties handled at the drive's hardware or firmware level
  - Zoned bit recording (ZBR)
  - Track density
  - Areal density
  - Head and cylinder skew

#### Exploring Microsoft File Structures

- In Microsoft file structures, sectors are grouped to form clusters
  - Storage allocation units of one or more sectors
- Clusters are typically 512, 1024, 2048, 4096, or more bytes each
- Combining sectors minimizes the overhead of writing or reading files to a disk

# Exploring Microsoft File Structures (continued)

- Clusters are numbered sequentially starting at 2
  - First sector of all disks contains a system area, the boot record, and a file structure database
- OS assigns these cluster numbers, called logical addresses
- Sector numbers are called **physical addresses**
- Clusters and their addresses are specific to a logical disk drive, which is a disk partition

#### **Disk Partitions**

- A partition is a logical drive
- FAT16 does not recognize disks larger than 2 MB
   Large disks have to be partitioned
- Hidden partitions or voids
  - Large unused gaps between partitions on a disk
- Partition gap
  - Unused space between partitions

#### Disk Partitions (continued)

Disk editor utility can alter information in partition table

– To hide a partition

• Can examine a partition's physical level with a disk editor:

Norton DiskEdit, WinHex, or Hex Workshop

 Analyze the key hexadecimal codes the OS uses to identify and maintain the file system

Table 6-1 Hexade	ecimal codes in the partition table
Hexadecimal code	File system
01	DOS 12-bit FAT
04	DOS 16-bit FAT for partitions smaller than 32 MB
05	Extended partition
06	DOS 16-bit FAT for partitions larger than 32 MB
07	NTFS
08	AIX bootable partition
09	AIX data partition
OB	DOS 32-bit FAT
OC	DOS 32-bit FAT for interrupt 13 support
17	Hidden NTFS partition (XP and earlier)
1B	Hidden FAT32 partition
1E	Hidden VFAT partition
3C	Partition Magic recovery partition
66–69	Novell partitions
81	Linux
82	Linux swap partition (can also be associated with Solaris
	partitions)
83	Linux native file systems (Ext2, Ext3, Reiser, xiafs)
86	FAT16 volume/stripe set (Windows NT)
87	High Performance File System (HPFS) fault-tolerant mirrored
	partition or NTFS volume/stripe set
A5	FreeBSD and BSD/386
A6	OpenBSD
A9	NetBSD
C7	Typical of a corrupted NTFS volume/stripe set
EB	BeOS

 Table 6-1
 Hexadecimal codes in the partition table

				2 63 10 10		20	1	1. 4	1.5.	-											-	17
0000000	0	X @	8	ie m	0	-			+	8	0	<u> </u>	-	_		٠	\$2.et	- % Z •				
	0	1				8	A501					1	4 4	P	×.							
			2	3 4	4 5	ń	7	8	9	A	В	C	D	Ε	P	10	1	0123456789ABC	DEFOL	Data inspect		
0000012	KB	52	90	4E 5	4.46	53	20	20	20	20	0.0	0.2	08	0.0	DD	0.0	00	R.NTFS		Date at offs	et 0x000000000	
	00	00	00.1	0 83	0.00	38	00	E.E.	0.0	37	00	00	0.0	0.0	0.0	00	0.0		· · · · · 💷	int8	-21	
0000024	80	00	80	00 E	2 85	24	33	00	00	00	00	00	00	DC	DD	00	00	\$3		uint8	235	- [
0000036	DD	0.0	SE.	48 3	2 03	0.0	0.0	0.0	0.0	E6	0.0	0.0	0.0	D.1.	DD	0.0	0.0	^H2		int16	21227	
0000048	C4	92	74.1	88 A	5 74	88	08			DD	00	PA.	33	CI	BK	DD	BC		3	uint16	21227	
A200000	00	70	201	00 C	0 07	100	00	0.3	10	00	00	00	00	3.0	CO	- 22	DD			int32	1318081259	
000006C	CB.	U.S.	100 /	1 DU	0 20	0.5	00	68	22	0.0	0.5	0.6	02	CB DG	0.6	10	24	S.hhj		uint2	1318081259	
00000000	DP.	84	51 1	80 F	2 12	87	F 2	86	ch.	20	ET.	0.6	41	1.1	DF.	87	20		ar er	int54	2020202700080	
00000A2	5.5	F7	E1	66 Å	3 20	00	63	84	41	EB	2.2	55	BA	15	24	0.0	CD	FE	6	uint54	2329282350089	
00000B4	13	72	OF I	81 F	8 55	AA.	75	0.9	F6	C1	01	74	0.4	ĒΕ	D.6	14	οā	.rU.ut		fee	1.2106795e+009	
00000006	03	66	60	1E 0	6 66	A.1	10	0.0	66	03	0.6	10	0.0	66	3B	0.6	20	.f'ff		double.	5.7502983e-153	
8400000	0.0	07	82.3	JA D	0 - 1E	66	6A	0.0	66	50	0.5	53	5.5	5.8	10	00	01	Ej.fP.S	£h	DATE	<irvalid></irvalid>	
00000EA	DD	80	3E	14 0	0 00	0 F	85	0 C	00	ΕB	83	FF	80	ЗE	14	00	00			DOS data	7/11/2021	
ICODOCEC.	DF	84	61	00 E	4 42	8A	16	24	0.0	16	1.F	8B	F4	CD	13	6.6	58	aB\$		DOS time	10:23:22 AM	
0000105	5B	07	0.0	58 0	0 50	28	EВ	20	66	33	DZ	6.6	Пħ	37	DK	15	ЦQ	[.fXfX.,-f3.f		FILETING	< invalide	
0000120	55 86	F7 D6	E 1 1	EE C	2 8A 4 DD	CA	66	88	DO F4	6.6	C1	EA	10	17	36	13	00	fff		time t	1.40/59 PM 10/	1

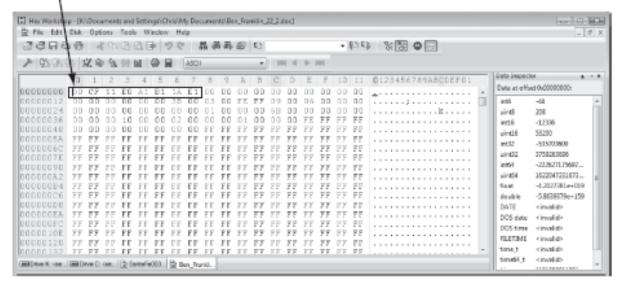
Figure 6-4 Hex Workshop identifying the file system

#### Disk Partitions (continued)

Hex Workshop allows you to identify file headers
 To identify file types with or without an extension

월 Her Worksho 월 File Edit 김 영 대 전	Disk:	Opti	083	Tech	W	inclew	He	lp .					a e de F	s007.1	lawe			pse	850 o			-	
1 05.00	11	2.9	- 94	88.1	1	0.6		ASOI				•	110	1.4		141							
	0	1	2	3	4	5.	6	7	8	ġ	A	В	C	D	E.	F		11	0123456789ABCDEF01	- 11	Data Inspects	H 0+00000000	* 3
	42	4D	46	50	DC	00	0.0	0.0	0.0	00	36	0.0	0.0	0.0	28	DD		D.D.	BMP				-
00000012	58	20	00	00	CZ.	01	0.0	00	01	00	18	00	00	00	00	DD		SC	X	-	int8	66	1
0000024	100	20	24	UE -	55	20	24	UE C T	20	50	20	12	20	00	00	00	00	50	ORPTUTEWOPRKOONUOP		uir48	66	
00000048	52	57	417	5.7	52	50	12	54	AF.	21	8.2	4.0	11	57	4.17	55	21	30	REORRERINGROUSE		erf16	19778	
AC000005A	51	53	40	52	55	40	51	52	40	53	51	4.0	57	51	4.2	58	54	50	QSMRSMQRMSQMRSNZTP		untili	19778	
0000006C	57	54	47	54	51	410	51	52	40	54	53	48	55	52	48	56	52		WTOTOMORMTSNURHVB.J		int32	1548111170	
0000007E	55	SD	4B	55	52	49	54	51	44	57	52	40	54	54	51	5A	60		UPRURITOJWRLTTOZ' >		uint/0	1548111170	
00000000	53	$5\Sigma$	54	59	55	41	57	53	40	53	54	$4\lambda$	53	55	4.4	55	36	48	V*TYURWSLSTJSLJUVN		in154	50087718722	
00000082	55	57	56	60	60	60	68	68	68	72	73	73	82	85	82	BC.	89	70	UWV jkkros		uint54	53087718722	
00000084	97	91	83	9F	9B	81	A.2	À1	95	$^{\rm A7}$	3.6	99	A5	A3	96	84	à2				fex	2.3336797e+047	
000000006	$\lambda 2$	AD	95	A2	Å1	96	98	À1	95	Å4	$\lambda 2$	95	λS	$\lambda 2$	97	A6	2.4	99			double .	2.6239858e-313	
adobadbe.	84	84	99	83	85	9A	A.3	A4	98	86	85	97	85	84	97	87	8.5				DATE	<irwalid></irwalid>	
VEDDOODO	22	λh,	9B	82	2.6	99	A5	A6	98	A5	2.6	9/1	AS	A6	9D	λħ.	99				DO5 date	30/2/2018	
DODDDDFC	AF	AC	A1	ВO	AD	A1	AD	AA.	99	83	70	79	83	89	BC	79	77	7A.	·····   y · · · y · z		DOS time	04204 AM	
0000030E	6.D	71	92	78	2.6	76	27	76	22	72	75	79	21	74	92	71	72	23	mdrzzaneneirbdrudid		FILETIME	< invalid>	
00000120		7.B	12	6E	18	6.0	12	12	39	78	24	12	11	20	18	55	60		thrownedge. (our	- 11	time t	10.5250 PM 1/-	. U
00000332	_	60				6.8	21	6F.	60.	2.0	21	60	ńP.	32	60	23	25	71	hminnienmoelnymsue		timelid_1	< invalido	
BDINN K. INC.		the C:	98	(2) Sec.	ntel-le	001														- 1	in the second	A DAMAGE I DATE MAD	1

Figure 6-5 Hex Workshop indicating a .bmp file



#### Indicates a Microsoft Office file

Figure 6-6 Hex Workshop indicating a Microsoft Office file

#### Master Boot Record

- On Windows and DOS computer systems
  - Boot disk contains a file called the Master Boot Record (MBR)
- MBR stores information about partitions on a disk and their locations, size, and other important items
- Several software products can modify the MBR, such as PartitionMagic's Boot Magic

#### Examining FAT Disks

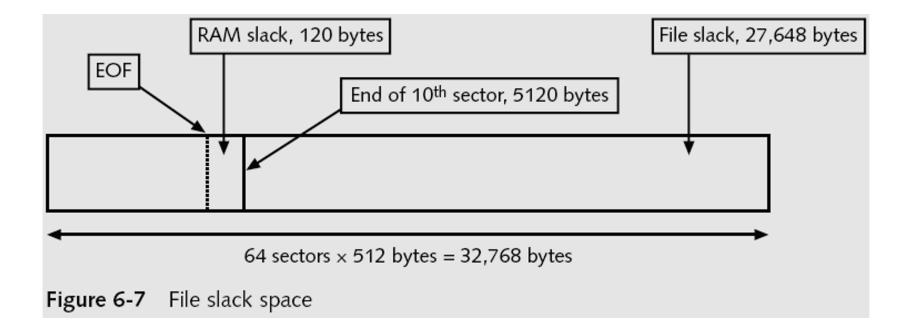
- File Allocation Table (FAT)
  - File structure database that Microsoft originally designed for floppy disks
  - Used before Windows NT and 2000
- FAT database is typically written to a disk's outermost track and contains:
  - Filenames, directory names, date and time stamps, the starting cluster number, and file attributes
- FAT versions
  - FAT12, FAT16, FAT32, and VFAT

 Cluster sizes vary according to the hard disk size and file system

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

Table 6-2 Sectors and bytes per cluster

- Microsoft OSs allocate disk space for files by clusters
  - Results in drive slack
    - Unused space in a cluster between the end of an active file and the end of the cluster
- Drive slack includes:
  - RAM slack and file slack
- An unintentional side effect of FAT16 having large clusters was that it reduced fragmentation
  - As cluster size increased



Guide to Computer Forensics and Investigations

25

- When you run out of room for an allocated cluster
  - OS allocates another cluster for your file, which creates more slack space on the disk
- As files grow and require more disk space, assigned clusters are chained together
  - The chain can be broken or fragmented

List of Clusters							
List of Sectors for the file:							
C:\Work\Chap06\InChp6-1.eve\Pictures\Friends\åIST.PDF							
82e9 (33513)							
82ea (33514)							
82ec (33516)							
82ed (33517) 82ee (33518)							
Copy to Clipboard Show File							
Close							

Figure 6-8 Chained sectors associated with clusters as a result of increasing file size

- When the OS stores data in a FAT file system, it assigns a starting cluster position to a file
  - Data for the file is written to the first sector of the first assigned cluster
- When this first assigned cluster is filled and runs out of room

- FAT assigns the next available cluster to the file

- If the next available cluster isn't contiguous to the current cluster
  - File becomes fragmented

# **Deleting FAT Files**

- In Microsoft OSs, when a file is deleted
  - Directory entry is marked as a deleted file
    - With the HEX E5 ( $\sigma$ ) character replacing the first letter of the filename
    - FAT chain for that file is set to 0
- Data in the file remains on the disk drive
- Area of the disk where the deleted file resides becomes unallocated disk space
  - Available to receive new data from newly created files or other files needing more space

#### Examining NTFS Disks

#### New Technology File System (NTFS)

- Introduced with Windows NT
- Primary file system for Windows Vista
- Improvements over FAT file systems
  - NTFS provides more information about a file
  - NTFS gives more control over files and folders
- NTFS was Microsoft's move toward a journaling file system

- In NTFS, everything written to the disk is considered a file
- On an NTFS disk
  - First data set is the Partition Boot Sector
  - Next is Master File Table (MFT)
- NTFS results in much less file slack space
- Clusters are smaller for smaller disk drives
- NTFS also uses Unicode
  - An international data format

Table 6-5 Cluster sizes III a	all MIFS USK	
Drive size	Sectors per cluster	Cluster size
0–512 MB	1	512 bytes
512 MB–1 GB	2	1024 bytes
1–2 GB	4	2048 bytes
2–4 GB	8	4096 bytes
4–8 GB	16	8192 bytes

 Table 6-3
 Cluster sizes in an NTFS disk (continued)

Table 6-3 Cluster sizes in an NTES disk

Drive size	Sectors per cluster	Cluster size
8–16 GB	32	16,384 bytes
16–32 GB	64	32,768 bytes
More than 32 GB	128	65,536 bytes

#### NTFS File System

- MFT contains information about all files on the disk
   Including the system files the OS uses
- In the MFT, the first 15 records are reserved for system files
- Records in the MFT are called **metadata**

# NTFS File System (continued)

Table 6-4	ivietadata rec	oras in the	/V\F1
Filename	System file	Record position	Description
\$Mft	MFT	0	Base file record for each folder on the NTFS volume; other record positions in the MFT are allocated if more space is needed.
\$MftMirr	MFT 2	1	The first four records of the MFT are saved in this position. If a single sector fails in the first MFT, the records can be restored, allowing recovery of the MFT.
\$LogFile	Log file	2	Previous transactions are stored here to allow recovery after a system failure in the NTFS volume.
\$Volume	Volume	3	Information specific to the volume, such as label and version, is stored here.
\$AttrDef	Attribute definitions	4	A table listing attribute names, numbers, and definitions.
\$	Root file- name index	5	This is the root folder on the NTFS volume.

Guide to Computer Forensics and Investigations

Table 6-1 Motadata records in the MET

# NTFS File System (continued)

Table 6-4	Metadata	records in	the MFT	(continued)
-----------	----------	------------	---------	-------------

Filename	System file	Record position	Description
\$Bitmap	Boot sector	6	A map of the NTFS volume showing which clus- ters are in use and which are available.
\$Boot	Boot sector	7	Used to mount the NTFS volume during the bootstrap process; additional code is listed here if it's the boot drive for the system.
\$BadClus	Bad cluster file	8	For clusters that have unrecoverable errors, an entry of the cluster location is made in this file.
\$Secure	Security file	9	Unique security descriptors for the volume are listed in this file. It's where the access control list (ACL) is maintained for all files and folders on the NTFS volume.
\$Upcase	Upcase table	10	Converts all lowercase characters to uppercase Unicode characters for the NTFS volume.
\$Extend	NTFS extension file	11	Optional extensions are listed here, such as quo- tas, object identifiers, and reparse point data.
		12–15	Reserved for future use.

#### MFT and File Attributes

- In the NTFS MFT
  - All files and folders are stored in separate records of 1024 bytes each
- Each record contains file or folder information
  - This information is divided into record fields containing metadata
- A record field is referred to as an attribute ID
- File or folder information is typically stored in one of two ways in an MFT record:
  - Resident and nonresident

### MFT and File Attributes (continued)

- Files larger than 512 bytes are stored outside the MFT
  - MFT record provides cluster addresses where the file is stored on the drive's partition
    - Referred to as **data runs**
- Each MFT record starts with a header identifying it as a resident or nonresident attribute

Table 6 5 Attributes in the MET

Table 6-5 At	ttributes in the MFT
Attribute ID	Purpose
0x10	\$Standard Information This field contains data on file creation, alterations, MFT changes, read dates and times, and DOS file permissions.
0x20	\$Attribute_List Attributes that don't fit in the MFT (nonresident attributes) are listed here along with their locations.
0x30	\$File_Name The long and short names for a file are contained here. Up to 255 Uni- code bytes are available for long filenames. For POSIX requirements, additional names or hard links can also be listed. Files with short filena- mes have only one attribute ID 0x30. Long filenames have two attribute ID 0x30s in the MFT record: one for the short name and one for the long name.
0x40	\$Object_ID (for Windows NT, it's named \$Volume_Version) Ownership and who has access rights to the file or folder are listed here. Every MFT record is assigned a unique GUID. Depending on your NTFS setup, some file records might not contain this attribute ID.
0x50	\$Security_Descriptor Contains the access control list (ACL) for the file.
0x60	\$Volume_Name The volume-unique file identifier is listed here. Not all files need this unique identifier.
0x70	\$Volume_Information This field indicates the version and state of the volume.
0x80	\$Data File data or data runs to nonresident files.
0x90	\$Index_Root Implemented for use of folders and indexes.
0xA0	\$Index_Allocation Implemented for use of folders and indexes.
OxBO	\$Bitmap Implemented for use of folders and indexes.
0xC0	\$Reparse_Point This field is used for volume mount points and Installable File System (IFS) filter drivers. For the IFS, it marks specific files used by drivers.
0xD0	\$EA_Information For use with OS2 HPFS file systems.
OxEO	\$EA For use with OS2 HPFS file systems.
0x100	\$Logged_Utility_Stream This field is used by Encrypting File System in Windows 2000 and XP.

035B3400 0 035B3410 0 035B3420 0 035B3420 0 035B3430 0 035B3440 0 035B3450 6 035B3450 6 035B3460 B 035B3460 B 035B3460 0 035B3480 0 035B3480 0 035B3490 0	2 00 0 00 3 00 0 00 2 16 0 78	01 00 3 00 00 0 00 00 0	B 4 5 6 8 00 01 8 00 01 0 00 00 0 00 00 0 00 00 0 00 00		1 00 00 00 0 00 00 A	00 00 00 04 00 00 17 00 00	✓ Q] ■ILE0
035B3400 0 035B3410 0 035B3420 0 035B3430 0 035B3440 0 035B3450 6 035B3450 6 035B3460 B 035B3470 2 035B3470 0 035B3490 0	6 49 2 00 0 00 3 00 0 00 2 16 0 78	4C 45 3 01 00 3 00 00 0 00 00 0 00 00 0	0 00 03 0 00 01 0 00 00 0 00 00	00 9B 99 80 A8 03 00 D4 00 00 10 00	9 98 00 00 1 00 00 00 2 00 00 A	00 00 00 04 00 00 17 00 00	FILE0
035B3410 0 035B3420 0 035B3430 0 035B3440 0 035B3440 0 035B3460 B 035B3470 2 035B3470 2 035B3480 0 035B3490 0	2 00 0 00 3 00 0 00 2 16 0 78	01 00 3 00 00 0 00 00 0 00 00 0		80 A8 01 00 D4 01 00 10 01	1 00 00 00 0 00 00 A	04 00 00 17 00 00	
035B3420 0 035B3430 0 035B3440 0 035B3450 6 035B3460 B 035B3460 B 035B3470 2 035B3480 0 035B3490 0	0 00 3 00 0 00 2 16 C 78	00 00 0 00 00 0 00 00 0	0 00 00		) 00 00 A	17 00 00	
035B3430 0 035B3440 0 035B3450 6 035B3460 B 035B3460 B 035B3470 2 035B3480 0 035B3490 0	3 00 0 00 2 16 10 78	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	0 00/00	00 10 0			
035B3440 0 035B3450 6 035B3460 B 035B3470 2 035B3480 0 035B3490 0	0 00 2 16 1C 78	00 00 0	· · · · · · ·			00 00 00	* *
035B3450 6 035B3460 B 035B3470 2 035B3480 0 035B3480 0	2 16 C 78			00 48 00	\[		
035B3470 20 035B3480 00 035B3490 00			A 7C C)				b.∎h.  É.¾s.h.  É.
035B3470 20 035B3480 00 035B3490 00		9D 68 0	à 7C C9	Q1 BC 70		7C C9 01	Max.h. É.Max.h. É.
035B3490 0		00 00 0		1	0 00 00 00		
	0 0 0	00 00 0	9 01 00	00 00 00	) OO OO 👌	00 00 00	
02552480 0	0 00	00 00 0	0 00 00	00 30 0	0 00 00 70	00 00 00	p
naoposten in	0 00	00 00 0	0 00 02	00 52 00	0 00 00 18	00 01 00	
035B34B0 8/	A 00	00 00 0	0 00 01	00 62 10	5 9B 68 04	7C C9 01	[b.]h. É.
035B34C0 B	C 78	9D 68 0	à 7C C9	01 BC 78	3 9D 68 02	7C C9 01	lix.h. É. lix.h. É.
035B34D0 B	IC 78	9D 68 0	à 7C C9	01 00 00	0 00 00 00	00 00 00	¥x.h. É
035B34E0 0	0 00	00 00 0	0 00 00	00 20 00	0 00 00 00	00 00 00	
035B34F0 0	8 03	42 00 6	5 00 6E	00 31 00	) 2E 00 74	00 78 00	B.e.n.1t.x.
035B3500 7	4 00	00 00 0	0 00 00	00 40 00	0 00 00 28	00 00 00	t@(
035B3510 0	0 00	00 00 0	0 00 03	00 1 0	0 00 00 1	00 00 00	
035B3520 F	4 7C	F1 27 D	F E7 DD	11 A8\3	7 00 22 19	D5 88 06	6 11'BçŸ.`?.".Õ∥.
035B3530 段	00 0	00 00 7	0 00 00	00 00 00	18 00 00	00 01 00	Ip
035B3540 🎜	4 00		🖉 00 00	00/41 2	) 63 6F 75	6E 74 72	TÅ countr
035B3550 /7	9 6D	61 6E 🗶		JA 177 6!	65 6E 20	74 77 6F	yman between two
035B3560 / 2		61 77/7		73/ 20 6	9\73 20 60		lavyers is like
035B3570/ 2		20 🌮 6 6		2/0 62 6!	5 <b>\7</b> 4 77 65	65 6E 20	a fish between
035B358 <b>/</b> 0 7		6F/20 6					tvo catsBenja
					: 69(6E 00	<b>0</b> 0 00 00	min Franklin
035B3#A0 FI	F FF	FF FF 3	Z 79 <b>/</b> 7	11 DO 00	0 00/00 00	0 00 00	<del>ÿÿÿÿ</del> ∎ÿG
1	/	1	/		\	G	
н́ ,	<u></u>	.í	ĸ		F	G	

- I: Length of attribute 0x80 (value 70)
- J: Attribute 0x80 resident flag
- K: Starting position of resident data

Figure 6-9 Resident file in an MFT record

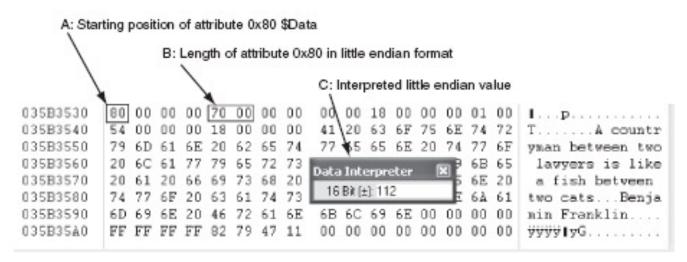
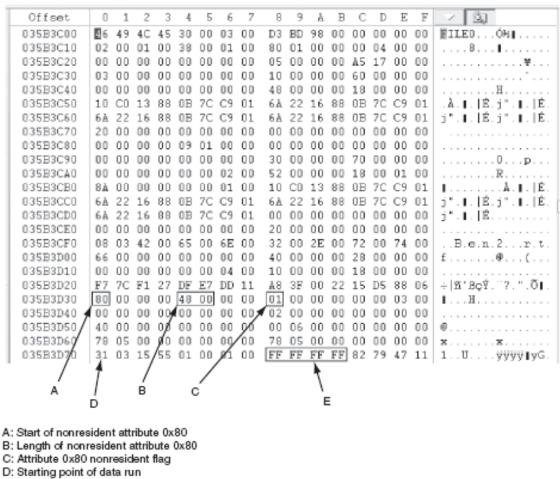


Figure 6-10 File data for a resident file



E: End-of-record marker (FF FF FF FF) for the MFT record



### MFT and File Attributes (continued)

- When a disk is created as an NTFS file structure
   OS assigns logical clusters to the entire disk partition
- These assigned clusters are called logical cluster numbers (LCNs)
  - Become the addresses that allow the MFT to link to nonresident files on the disk's partition

#### **NTFS** Data Streams

#### Data streams

- Ways data can be appended to existing files
- Can obscure valuable evidentiary data, intentionally or by coincidence
- In NTFS, a data stream becomes an additional file attribute
  - Allows the file to be associated with different applications
- You can only tell whether a file has a data stream attached by examining that file's MFT entry

### NTFS Compressed Files

- NTFS provides compression similar to FAT DriveSpace 3
- Under NTFS, files, folders, or entire volumes can be compressed
- Most computer forensics tools can uncompress and analyze compressed Windows data

### NTFS Encrypting File System (EFS)

#### • Encrypting File System (EFS)

- Introduced with Windows 2000
- Implements a public key and private key method of encrypting files, folders, or disk volumes
- When EFS is used in Windows Vista Business Edition or higher, XP Professional, or 2000,
  - A recovery certificate is generated and sent to the local Windows administrator account
- Users can apply EFS to files stored on their local workstations or a remote server

### EFS Recovery Key Agent

- Recovery Key Agent implements the recovery certificate
  - Which is in the Windows administrator account
- Windows administrators can recover a key in two ways: through Windows or from an MS-DOS command prompt
- MS-DOS commands
  - Cipher
  - Сору
  - Efsrecvr (used to decrypt EFS files)

### **Deleting NTFS Files**

- When a file is deleted in Windows XP, 2000, or NT
   The OS renames it and moves it to the Recycle Bin
- Can use the Del (delete) MS-DOS command
  - Eliminates the file from the MFT listing in the same way FAT does

### Understanding Whole Disk Encryption

- In recent years, there has been more concern about loss of
  - Personal identity information (PII) and trade secrets caused by computer theft
- Of particular concern is the theft of laptop computers and other handheld devices
- To help prevent loss of information, software vendors now provide whole disk encryption

# Understanding Whole Disk Encryption (continued)

- Current whole disk encryption tools offer the following features:
  - Preboot authentication
  - Full or partial disk encryption with secure hibernation
  - Advanced encryption algorithms
  - Key management function
  - A Trusted Platform Module (TPM) microchip to generate encryption keys and authenticate logins

# Understanding Whole Disk Encryption (continued)

- Whole disk encryption tools encrypt each sector of a drive separately
- Many of these tools encrypt the drive's boot sector
  - To prevent any efforts to bypass the secured drive's partition
- To examine an encrypted drive, decrypt it first
  - Run a vendor-specific program to decrypt the drive

### Examining Microsoft BitLocker

- Available only with Vista Enterprise and Ultimate editions
- Hardware and software requirements
  - A computer capable of running Windows Vista
  - The TPM microchip, version 1.2 or newer
  - A computer BIOS compliant with Trusted Computing Group (TCG)
  - Two NTFS partitions
  - The BIOS configured so that the hard drive boots first before checking other bootable peripherals

### Examining Third-Party Disk Encryption Tools

- Some available third-party WDE utilities:
  - PGP Whole Disk Encryption
  - Voltage SecureDisk
  - Utimaco SafeGuard Easy
  - Jetico BestCrypt Volume Encryption
  - SoftWinter Sentry 2020 for Windows XP
- Some available open-source encryption tools:
  - TrueCrypt
  - CrossCrypt
  - FreeOTFE

### Understanding the Windows Registry

#### Registry

- A database that stores hardware and software configuration information, network connections, user preferences, and setup information
- For investigative purposes, the Registry can contain valuable evidence
- To view the Registry, you can use:
  - Regedit (Registry Editor) program for Windows 9x systems
  - Regedt32 for Windows 2000 and XP

# Exploring the Organization of the Windows Registry

- Registry terminology:
  - Registry
  - Registry Editor
  - HKEY
  - Key
  - Subkey
  - Branch
  - Value
  - Default value
  - Hives

# Exploring the Organization of the Windows Registry (continued)

Table 6-6 Registry file locations and purposes				
Filename and location	Purpose of file			
Windows 9x/Me				
Windows\System.dat	User-protected storage area; contains installed pro- gram settings, usernames and passwords associ- ated with installed programs, and system settings			
Windows\User.dat Windows\profile\user-account	Contains the most recently used (MRU) files list and desktop configuration settings; every user account created on the system has its own user data file			
Windows NT, 2000, XP, and Vista				
Documents and Settings\ user-account\Ntuser.dat	User-protected storage area; contains the MRU files list and desktop configuration settings			
Winnt\system32\config\Default	Contains the computer's system settings			
Winnt\system32\config\SAM	Contains user account management and security settings			
Winnt\system32\config\Security	Contains the computer's security settings			
Winnt\system32\config\Software	Contains installed programs settings and associ- ated usernames and passwords			
Winnt\system32\config\System	Contains additional computer system settings			

#### Table 6-6 Registry file locations and purposes

## Exploring the Organization of the Windows Registry (continued)

#### 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
HKEY_DYN_DATA	Used only in Windows 9x/Me systems; stores hardware configuration settings

#### Examining the Windows Registry

Use ProDiscover Basic to extract System.dat and User.dat from an image file

Search		×
Content Search   Cluster Search		
Search in Meta Files     Select all matches	F Search in Selected Files	only
ASCI     Cost Sensitive     Match whole word	C Hex	
<ul> <li>Search for files named :</li> <li>Search for the pattern(s) :</li> </ul>		Load from file
system.dat uner.dat		<u>~</u>
Select the Disk(s) / Image(s) you D/tw/wk//Dhap06/Projects//GEP		
Filter files by Date(s)		
C Nodied betw File: C Dested C Accessed	MM - DD - YYYYY	
	OK Cancel	Apply

Figure 6-26 Searching for Registry files

Profilis over Basic - Millarph	_ 5 X
The Action trave focks rails	
fur Help, press F1	103

Figure 6-27 Selecting files in the search results

Use AccessData Registry Viewer to see what information you can find in these files

Find	×
Find what: superior	Find Next
Look at	Cancel
Keys	Heb
Values	Hep
🔽 Data	

Figure 6-28 Entering a search term in Registry Viewer

	ipkow Mi E HTML Editor O ant Windows atris atris	e Culton S ov_Chan	R65,52 R65,32 R65,32 R65,52 R65,52 R65,52 R65,52 R65,52 R65,54 R6	Deba // // // // // // // // // // // // //	Right-click the folder to copy the key name
<	Copy Non Name	arrester.	880,32	http://www.iechannelgude.com/lgude/en/en_i.M	
Key Properties		00 60 74 74 7 10 69 62 72 6	0 3a 2f 2f 73 2 69 63 79 63	-77 27 26 75 15 70 65 72 http://www -6c 65 73 2e 62 69 7e 2f isthicycle	

Figure 6-29 Copying a key name in Registry Viewer

🗈 InChap6-reg-smarch.tst - Notepad	
Min Edit Pormat View Help	
Search results for word: superior UMER.3AT\.DEFAULT\Software\Ricrosoft\Internet Explorer\Rain USER.3AT\.DEFAULT\Software\Ricrosoft\Internet Explorer\TypedURLs USER.3AT\.DEFAULT\Software\Ricrosoft\Internet Account Manager\Accounts\000000001 USER.3AT\.DEFAULT\Software\Sun Hicrosystems\setup\recycle	1
Search repulto for word: denipe USER.DAT\.DEFAULT\Software\Nicrosoft\Internet Account Manager\Accounts\00000001 USER.DAT\.DEFAULT\Software\Sun Microsystems\setup\recyule	

Figure 6-30 The search results showing paths for keys of interest

### Understanding Microsoft Startup Tasks

- Learn what files are accessed when Windows starts
- This information helps you determine when a suspect's computer was last accessed
  - Important with computers that might have been used after an incident was reported

#### Startup in Windows NT and Later

- All NTFS computers perform the following steps when the computer is turned on:
  - Power-on self test (POST)
  - Initial startup
  - Boot loader
  - Hardware detection and configuration
  - Kernel loading
  - User logon

# Startup in Windows NT and Later (continued)

- Startup Files for Windows XP:
  - NT Loader (NTLDR)
  - Boot.ini
  - BootSect.dos
  - NTDetect.com
  - NTBootdd.sys
  - Ntoskrnl.exe
  - Hal.dll
  - Pagefile.sys
  - Device drivers

# Startup in Windows NT and Later (continued)

Windows XP System Files

#### Table 6-8 Windows XP system files

Filename	Description
Ntoskrnl.exe	The XP executable and kernel
Ntkrnlpa.exe	The physical address support program for accessing more than 4 GB of physical RAM
Hal.dll	The Hardware Abstraction Layer (described earlier)
Win32k.sys	The kernel-mode portion of the Win32subsystem
Ntdll.dll	System service dispatch stubs to executable functions and internal support functions
Kernel32.dll	Core Win32 subsystem DLL file
Advapi32.dll	Core Win32 subsystem DLL file
User32.dll	Core Win32 subsystem DLL file
Gdi32.dll	Core Win32 subsystem DLL file

# Startup in Windows NT and Later (continued)

- Contamination Concerns with Windows XP
  - When you start a Windows XP NTFS workstation, several files are accessed immediately
    - The last access date and time stamp for the files change to the current date and time
  - Destroys any potential evidence
    - That shows when a Windows XP workstation was last used

#### Startup in Windows 9x/Me

- System files in Windows 9x/Me containing valuable information can be altered easily during startup
- Windows 9x and Windows Me have similar boot processes
  - With Windows Me you can't boot to a true MS-DOS mode
- Windows 9x OSs have two modes:
  - DOS protected-mode interface (DPMI)
  - Protected-mode GUI

### Startup in Windows 9x/Me (continued)

- The system files used by Windows 9x have their origin in MS-DOS 6.22
  - **Io.sys** communicates between a computer's BIOS, the hardware, and the OS kernel
    - If F8 is pressed during startup, Io.sys loads the Windows Startup menu
  - Msdos.sys is a hidden text file containing startup options for Windows 9x
  - Command.com provides a command prompt when booting to MS-DOS mode (DPMI)

### Understanding MS-DOS Startup Tasks

• Two files are used to configure MS-DOS at startup:

#### – Config.sys

 A text file containing commands that typically run only at system startup to enhance the computer's DOS configuration

#### – Autoexec.bat

- A batch file containing customized settings for MS-DOS that runs automatically
- Io.sys is the first file loaded after the ROM bootstrap loader finds the disk drive

# Understanding MS-DOS Startup Tasks (continued)

- Msdos.sys is the second program to load into RAM immediately after lo.sys
  - It looks for the Config.sys file to configure device drivers and other settings
- Msdos.sys then loads Command.com
- As the loading of Command.com nears completion, Msdos.sys looks for and loads Autoexec.bat

#### Other Disk Operating Systems

- Control Program for Microprocessors (CP/M)
  - First nonspecific microcomputer OS
  - Created by Digital Research in 1970
  - 8-inch floppy drives; no support for hard drives
- Digital Research Disk Operating System (DR-DOS)
  - Developed in 1988 to compete with MS-DOS
  - Used FAT12 and FAT16 and had a richer command environment

# Other Disk Operating Systems (continued)

- Personal Computer Disk Operating System (PC-DOS)
  - Created by Microsoft under contract for IBM
  - PC-DOS works much like MS-DOS

#### **Understanding Virtual Machines**

#### Virtual machine

- Allows you to create a representation of another computer on an existing physical computer
- A virtual machine is just a few files on your hard drive
  - Must allocate space to it
- A virtual machine recognizes components of the physical machine it's loaded on
  - Virtual OS is limited by the physical machine's OS



Figure 6-32 A virtual machine running on the host computer's desktop

# Understanding Virtual Machines (continued)

- In computer forensics
  - Virtual machines make it possible to restore a suspect drive on your virtual machine
    - And run nonstandard software the suspect might have loaded
- From a network forensics standpoint, you need to be aware of some potential issues, such as:
  - A virtual machine used to attack another system or network

#### **Creating a Virtual Machine**

- Two popular applications for creating virtual machines
  - VMware and Microsoft Virtual PC
- Using Virtual PC
  - You must download and install Virtual PC first

Op	otions You can create a new virtual machine or add an existing one to the Virtual PC Console.
	Select an option:
	Create a virtual machine
	This option guides you through the basic configurations necessary for creating a new virtual machine.
	O Use default settings to create a virtual machine
	You can automatically create a .vmc file with default settings. The resulting virtual machine will not have a virtual hard disk associated with it, so you will have to select one using the Settings dialog.
	O Add an existing virtual machine
	You can add a virtual machine to the Virtual PC Console from existing .vmc files.
	< Back Next> Cancel

Figure 6-33 Creating a new virtual machine

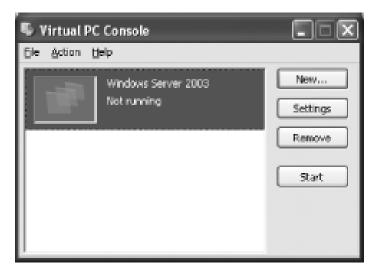


Figure 6-34 The Virtual PC Console with a virtual machine available

- You need an ISO image of an OS
  - Because no OSs are provided with Virtual PC
- Virtual PC creates two files for each virtual machine:
  - A .vhd file, which is the actual virtual hard disk
  - A .vmc file, which keeps track of configurations you make to that disk
- See what type of physical machine your virtual machine thinks it's running
  - Open the Virtual PC Console, and click Settings

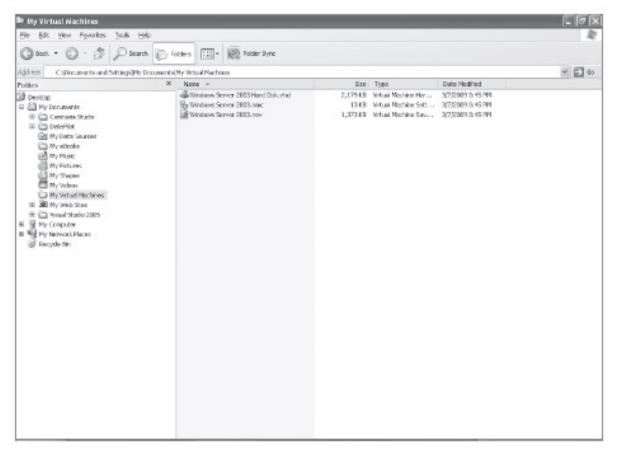


Figure 6-35 Virtual machine configuration files

Setting	Ourrent Value	1) File Nome	
Hard Name     Memory     Hard Disk 1     Hard Disk 2     Hard Disk 2     Hard Disk 3     Undo Disks     CO/DVD Drive     Floppy Disk     CON1     CON2     CON2     CON2     CON2     Sund     Mouse     Shared Folders     Display     Close	Windows 2003 Server 256 MB Windows 2003 Server None Disabled Secondary controller Auto detected None None None None None None Network adapters:1. Enabled No pointer integration Not installed Default Show message	Ele name:	me the virtual machine. Windows 2003 Server e's name typically identifies its softwar nfiguration.

Figure 6-36 Properties of a virtual machine

#### Summary

- When booting a suspect's computer, using boot media, such as forensic boot floppies or CDs, you must ensure that disk evidence isn't altered
- The Master Boot Record (MBR) stores information about partitions on a disk
- Microsoft used FAT12 and FAT16 on older operating systems
- To find a hard disk's capacity, use the cylinders, heads, and sectors (CHS) calculation

#### Summary (continued)

- When files are deleted in a FAT file system, the Greek letter sigma (0x05) is inserted in the first character of the filename in the directory
- New Technology File System (NTFS) is more versatile because it uses the Master File Table (MFT) to track file information
- In NTFS, data streams can obscure information that might have evidentiary value

#### Summary (continued)

- Maintain a library of older operating systems and applications
- NTFS can encrypt data with EFS and BitLocker
- NTFS can compress files, folders, or volumes
- Windows Registry keeps a record of attached hardware, user preferences, network connections, and installed software
- Virtual machines enable you to run other OSs from a Windows computer