

UNIT –V

WORKING WITH WINDOWS and DOS SYSTEMS

Understanding file systems

To investigate computer evidence effectively, you must understand how the most commonly used OSs work and how they store files. In addition to this section on file systems, you should review books on Computer Technology Industry Association. A file system gives an OS a road map to data on a disk. The 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, although some vendors grandfather in previous OSs so that newer ones can read them. For example, most current Linux releases can access disks configured in the older Linux Ext2fs and Ext3fs file systems.

No matter which platform you use, you need to know how to access and modify system settings when necessary. When you need to access a suspect's computer to acquire or inspect data related to your investigation, you should be familiar with the computer's platform.

Understanding the Boot Sequence:

To ensure that you don't contaminate or alter data on a suspect's Windows or DOS PC, you must know how to access and modify a PC's Complementary Metal Oxide Semiconductor (CMOS) and Basic Input/ Output System (BIOS) settings. A computer stores system configuration and date and time information in the CMOS when power to the system is off. The system BIOS contains programs that perform input and output at the hardware level.

When a subject's computer starts, you must make sure it boots to a forensic floppy disk or CD, because booting to the hard disk overwrites and changes evidentiary data. To do this, you access the CMOS setup by monitoring the subject's computer during the initial bootstrap process to identify the correct key or keys to use. The bootstrap process is contained in ROM and tells the computer how to proceed. As the computer starts, the screen usually displays the key or keys, such as the Delete key; you press to open the CMOS setup screen. You can also try unhooking the keyboard to force the system to tell you what keys to use. The key you press to access.

but you can refer to the vendor's documentation or Web site for instructions on changing the boot sequence.

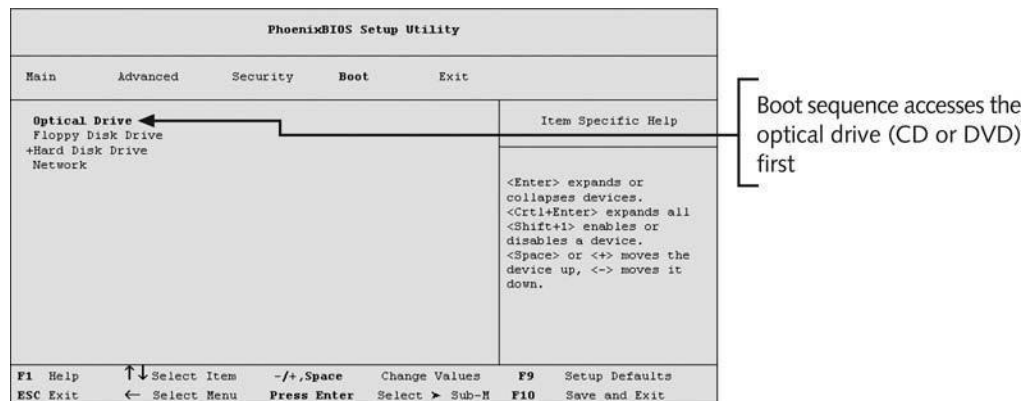


Fig: A typical CMOS setup screen

Understanding Disk Drives:

You should be familiar with disk drives and how data is organized on a disk so that you can find data effectively. Disk drives are made up of one or more platters coated with magnetic material, and data is stored on platters in a particular way. For additional information on disk drive configurations, see www.storagereview.com/guide2000/ref/hdd/index.html. Following is a list of disk drive components:

- *Geometry*—Geometry refers to a disk's structure of platters, tracks, and sectors.
- *Head*—the head is the device that reads and writes data to a drive. There's one head per platter.
- *Tracks*—Tracks are concentric circles on a disk platter where data is located.
- *Cylinders*—a cylinder is a column of tracks on two or more disk platters. Typically, each platter has two surfaces: top and bottom.
- *Sectors*—a sector is a section on a track, usually made up of 512 bytes.

The manufacturer engineers a disk to have a certain number of sectors per track, and a typical disk drive stores 512 bytes per sector. To determine the total number of addressable bytes on a disk, multiply the number of cylinders by the number of heads (actually tracks) and by the number of sectors (groups of 512 or more bytes).

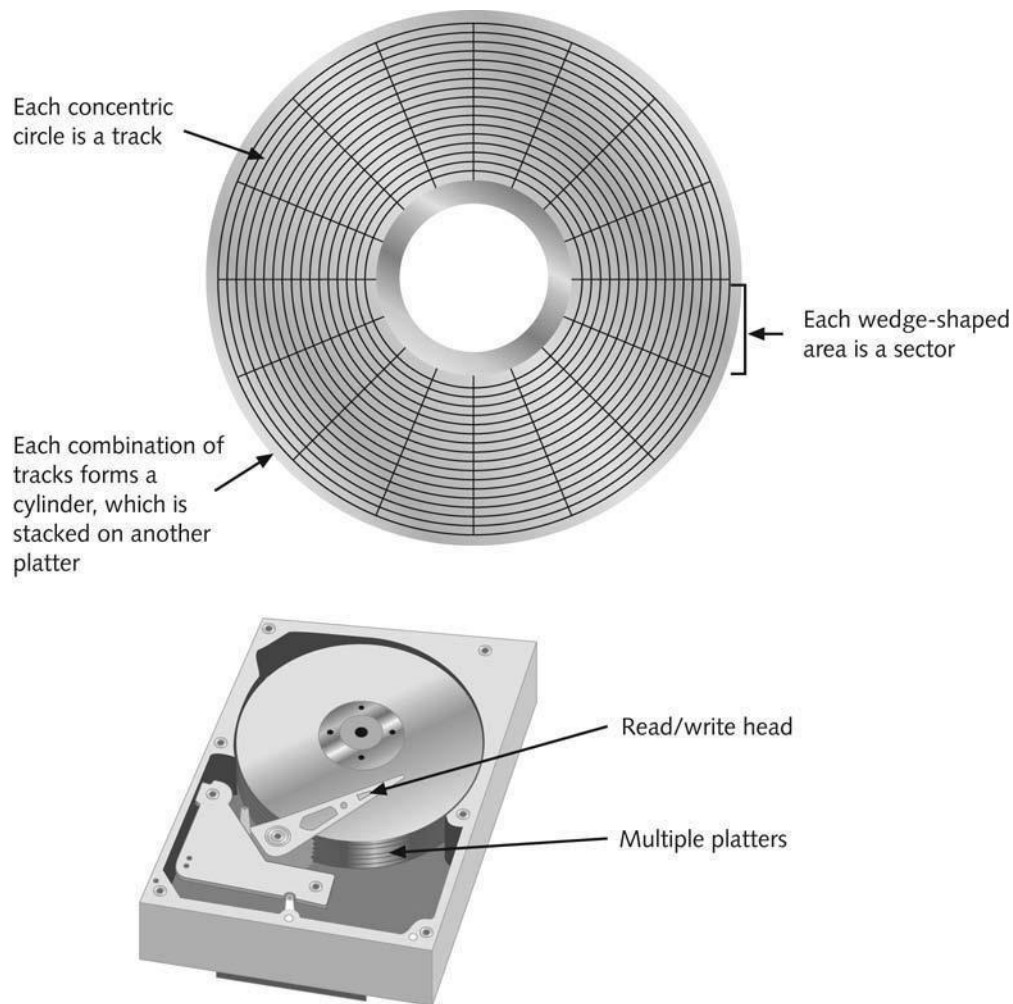


Fig : disk drives

Exploring Microsoft File Structures

Because most PCs use Microsoft software products, you should understand Microsoft file systems so that you know how Windows and DOS computers store files. In particular, you need to understand clusters, File Allocation Table (FAT), and New Technology File System (NTFS). The method an OS uses to store files determines where data can be hidden. When you examine a computer for forensic evidence, you need to explore these hiding places to determine whether they contain files or parts of files that might be evidence of a crime or policy violation.

In Microsoft file structures, sectors are grouped to form clusters, which are 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. The OS groups one or more sectors into a cluster. The number of sectors in a cluster varies according to the disk

size. For example, a double-sided floppy disk has one sector per cluster; a hard disk has four or more sectors per cluster.

Clusters are numbered sequentially starting at 2 because the first sector of all disks contains a system area, the boot record, and a file structure database. The OS assigns these cluster numbers, which are referred to as logical addresses. These addresses point to relative cluster positions; for example, cluster address 100 is 98 clusters from cluster address

Sector numbers, however, are referred to as physical addresses because they reside at the hardware or firmware level and go from address 0 (the first sector on the disk) to the last sector on the disk. Clusters and their addresses are specific to a logical disk drive, which is a disk partition.

Disk Partitions

Many hard disks are partitioned, or divided, into two or more sections. A partition is a logical drive. For example, an 8 GB hard disk might contain four partitions or logical drives. FAT16 does not recognize disks larger than 2 MB, so these disks have to be partitioned into smaller sections for FAT to recognize the additional space. Someone who wants to hide data on a hard disk can create hidden partitions or voids—large unused gaps between partitions on a disk drive. For example, partitions containing unused space (voids) can be created between the primary partition and the first logical partition. This unused space between partitions is called the partition gap. If data is hidden in a partition gap, a disk editor utility could also be used to alter information in the disk's partition table. Doing so removes all references to the hidden partition, concealing it from the computer's OS. Another technique is to hide incriminating digital evidence at the end of a disk by declaring a smaller number of bytes than the actual drive size. With disk-editing tools, however, you can access these hidden or empty areas of the disk.

One way to examine a partition's physical level is to use a disk editor, such as Norton Disk-Edit, WinHex, or Hex Workshop. These tools enable you to view file headers and other critical parts of a file. Both tasks involve analyzing the key hexadecimal codes the OS uses to identify and maintain the file system. Table 5-1 lists the hexadecimal codes in a partition table and identifies some common file system structures.

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
0B	DOS 32-bit FAT
0C	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 5-1 Hexadecimal codes in the partition table

1. If necessary, download Hex Workshop from BreakPoint Software and install it. Check with your instructor about where you should install it on your computer.

2. Insert a USB drive into a USB port.
3. Start Hex Workshop by right-clicking the Hex Workshop desktop icon and clicking Run as administrator, and then clicking the Continue button in the UAC message box.
4. In Hex Workshop, click Disk, Open Drive from the menu to see a list of your logical drives. Click the C: drive (or your working drive), and click OK.
5. Click Disk, Open Drive again, but this time, in the Open Drive drop-down list, click your USB drive, and then click OK. Compare the file system label for this drive to the one you saw in Step 4. Leave Hex Workshop open for the next activity.

With tools such as Hex Workshop, you can also identify file headers to identify file types with or without an extension. Before performing the following steps in Hex Workshop, use Windows Explorer or My Computer to find a folder on your system containing a bitmap (.bmp) file and a folder containing a Word document (.doc). Then follow these steps:

1. To open a bitmap file on your computer, click File, Open from the Hex Workshop menu. Navigate to a folder containing a bitmap (.bmp) file, and then double-click the .bmp file. (If you're prompted to select any bookmarks, click Cancel and continue with this activity.)
2. Hex Workshop window identifies the file type for the graphic. For .bmp files, it shows -BM6,| -BM,| or -BMF,| As shown in the figure, -42 4D| is also displayed to indicate a .bmp file.
3. To open a Word document, click File, Open from the menu. Navigate to a folder containing a Word document (.doc) file, and then double-click the .doc file. As shown in Figure 6-6, the first line contains a row of 0s followed by -D0 CF 11 E0 A1 B1 1A E1,| which identifies the file as a Microsoft Office document. The same file header is displayed for an Excel or a PowerPoint file but doesn't apply to Access databases.
4. Exit Hex Workshop.

Examining NTFS Disks

New Technology File System (NTFS) was introduced when Microsoft created Windows NT and is the primary file system for Windows Vista. Each generation of Windows since NT has included minor changes in NTFS configuration and features. The NTFS design was partially based on, and incorporated many features from, Microsoft's project for IBM with the OS/2 operating system; in this OS, the file system was High Performance File System (HPFS). When Microsoft created Windows NT, it provided backward compatibility so that NT could read OS/2 HPFS disk drives. Since the release of Windows 2000, this backward compatibility is no longer available.

NTFS offers significant improvements over FAT file systems. It provides more information about a file, including security features, file ownership, and other file attributes. With NTFS, you also have more control over files and folders (directories) than with FAT file systems.

In NTFS, everything written to the disk is considered a file. On an NTFS disk, the first data set is the Partition Boot Sector, which starts at sector [0] of the disk and can expand to 16 sectors. Immediately after the Partition Boot Sector is the Master File Table (MFT). The MFT, similar to FAT in earlier Microsoft OSs, is the first file on the disk. An MFT file is created at the same time a disk partition is formatted as an NTFS volume and usually consumes about 12.5% of the disk when it's created. As data is added, the MFT can expand to take up 50 % of the disk. An important advantage of NTFS over FAT is that it results in much less file slack space. Compare the cluster sizes in Table 5-3 to Table 5-2, which showed FAT cluster sizes. Clusters are smaller for smaller disk drives. This feature saves more space on all disks using NTFS.

Drive size	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 5-2 Sectors and bytes per cluster

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
8–16 GB	32	16,384 bytes
16–32 GB	64	32,768 bytes
More than 32 GB	128	65,536 bytes

Table 5-3 Cluster sizes in an NTFS disk

NTFS System Files

Because everything on an NTFS disk is a file, the first file, the 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 referred to as metadata. Table 6-4 lists the first 16 metadata records you find in the MFT.

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 filename index	5	This is the root folder on the NTFS volume.
\$Bitmap	Boot sector	6	A map of the NTFS volume showing which

			clusters 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 quotas, object identifiers, and reparse point data.
		12–15	Reserved for future use.

Table 5-2 Metadata records in the MFT

MFT and File Attributes

When Microsoft introduced NTFS, the way the OS stores data on disks changed significantly. 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 about the file or folder and the file's data or links to the file's data. 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. For very small files, about 512 bytes or less, all file metadata and data are stored in the MFT record. These types of records are called resident files because all their information is stored in the MFT record.

Files larger than 512 bytes are stored outside the MFT. The file or folder's MFT record provides cluster addresses where the file is stored on the drive's partition. These cluster addresses are referred to as data runs. This type of MFT record is called nonresident because the file's data is stored in its own separate file outside the MFT.

MFT Structures for File Data

When viewing an MFT record with a hexadecimal editor, such as WinHex, the data is displayed in little endian format, meaning it's read from right to left. For example, the hexadecimal value 400 is displayed as 00 04 00 00, and the number 0x40000 is displayed as 00 00 04 00.

The first section of an MFT record is the header that defines the size and starting position of the first attribute. Following the header are the attributes that are specific for the file type, such as an application file or a data file. MFT records for directories and system files have additional attributes that don't appear in a file MFT record. The following sections explain how data files are configured in the MFT.

MFT Header Fields

For the header of all MFT records, the record fields of interest are as follows:

- *At offset 0x00*—The MFT record identifier FILE; the letter F is at offset 0.
- *At offset 0x1C to 0x1F*—Size of the MFT record; the default is 0x400 (1024) bytes, or two sectors.
- *At offset 0x14*—Length of the header, which indicates where the next attribute starts; it's typically 0x38 bytes.
- *At offset 0x32 and 0x33*—The update sequence array, which stores the 2 two bytes of the first sector of the MFT record. It's used only when MFT data exceeds 512 bytes. The update sequence array is used as a checksum for record integrity validation.

NTFS Compressed Files

To improve data storage on disk drives, NTFS provides compression similar to FAT Drive-Space 3, a Windows 98 compression utility. Under NTFS, files, folders, or entire volumes can be compressed. With FAT16, you can compress only a volume. On a Windows Vista, XP, 2000, or NT system, compressed data is displayed normally when you view it in Windows Explorer or applications such as Microsoft Word.

During an investigation, typically you work from an image of a compressed disk, folder, or file. Most computer forensics tools can uncompress and analyze compressed Windows data, including data compressed with the Lempel-Ziv-Huffman (LZH) algorithm and in formats such as PKZip, WinZip, and GNU gzip. Forensics tools might have difficulty with third-party compression utilities, such as the RAR format. If you identify third-party compressed data, you need to uncompress it with the utility that created it.

NTFS Encrypting File System (EFS)

When Microsoft introduced Windows 2000, it added built-in encryption to NTFS called Encrypting File System (EFS). EFS implements a public key and private key method of encrypting files, folders, or disk volumes (partitions). Only the owner or user who encrypted the data can access encrypted files. The owner holds the private key, and the public key is held by a certificate authority, such as a global registry, network server, or company such as VeriSign.

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. The purpose of the recovery certificate is to provide a mechanism for recovering encrypted files under EFS if there's a problem with the user's original private key. The recovery key is stored in one of two places. When the user of a network workstation initiates EFS, the recovery key is sent to the local domain server's administrator account. If the workstation is standalone, the recovery key is sent to the workstation's administrator account.

EFS Recovery Key Agent

The 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. These three commands are available from the MS-DOS command prompt:

- Cipher
- Copy
- Efsrecvr (used to decrypt EFS files)

Deleting NTFS Files

Typically, you use Windows Explorer to delete files from a disk. When a file is deleted in Windows NT and later, the OS renames it and moves it to the Recycle Bin. Another method is using the Del (delete) MS-DOS command. This method doesn't rename and move the file to the Recycle Bin, but it eliminates the file from the MFT listing in the same way FAT does.

When you delete a file in Windows Explorer, you can restore it from the Recycle Bin. The OS takes the following steps when you delete a file or a folder in Windows Explorer:

1. Windows changes the filename and moves the file to a subfolder with unique identity in the Recycle Bin.
2. Windows stores information about the original path and filename in the Info2 file, which is the control file for the Recycle Bin. It contains ASCII data, Unicode data, and the date and time of deletion for each file or folder.

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. Company PII might consist of employees' full names, home addresses, and Social Security numbers. With this information, criminals could easily apply for credit card accounts in these employees' names. Trade secrets are any information a business keeps confidential because it provides a competitive edge over other companies. The inadvertent public release of this information could devastate a business's competitive edge.

Of particular concern is the theft of laptop computers and other handheld devices, such as PDAs. If data on these devices isn't secured properly, the owners could be liable for any damages incurred, such as stolen identities, credit card fraud, or loss of business caused by the release of trade secrets to the competition. Because of the PII problem, many states have enacted laws requiring any person or business to notify potential victims of the loss as soon as possible. To help prevent loss of information, software vendors, including Microsoft, now provide whole disk encryption this feature creates new challenges in examining and recovering data from drives.

Current whole disk encryption tools offer the following features that computer forensics examiners should be aware of:

- Preboot authentication, such as a single sign-on password, fingerprint scan, or token (USB device)
- Full or partial disk encryption with secure hibernation, such as activating a password-protected screen saver
- Advanced encryption algorithms, such as AES and IDEA
- Key management function that uses a challenge-and-response method to reset passwords or passphrases
- A Trusted Platform Module (TPM) microchip to generate encryption keys and authenticate logins

Examining Microsoft BitLocker

Microsoft's utility for protecting drive data is called BitLocker, available only with Vista Enterprise and Ultimate editions. BitLocker's current hardware and software requirements are as follows:

- 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 for the OS and an active system volume with 1.5 GB available space
- The BIOS configured so that the hard drive boots first before checking the CD/DVD drive or other bootable peripherals

Windows Registry

When Microsoft created Windows 95, it consolidated initialization (.ini) files into the Registry, a database that stores hardware and software configuration information, network connections, user preferences (including usernames and passwords), and setup information. The Registry has been updated and is still used in Windows Vista.

For investigative purposes, the Registry can contain valuable evidence. To view the Registry, you can use the Regedit (Registry Editor) program for Windows 9x and Regedt32 for Windows 2000, XP, and Vista. For more information on how to use Regedit and Regedt32, see the Microsoft Windows Resource Kit documentation for the OS.

Exploring the Organization of the Windows Registry

The Windows Registry is organized in a specific way that has changed slightly with each new version of Windows. However, the major Registry sections have been consistent, with some minor changes, since Windows 2000; they're slightly different in Windows 9x/Me. Before proceeding, review the following list of Registry terminology:

- *Registry*—A collection of files containing system and user information.
- *Registry Editor*—A Windows utility for viewing and modifying data in the Registry. There are two Registry Editors: Regedit and Regedt32.
- *HKEY*—Windows splits the Registry into categories with the prefix HKEY_. Windows 9x systems have six HKEY categories and Windows 2000 and later have five. Windows programmers refer to the —Hll as the handle for the key.
- *Key*—Each HKEY contains folders referred to as keys. Keys can contain other key folders or values.
- *Sub key*—A key displayed under another key is a subkey, similar to a subfolder in Windows Explorer.
- *Branch*—A key and its contents, including sub keys, make up a branch in the Registry.
- *Value*—A name and value in a key; it's similar to a file and its data content.

- *Default value*—All keys have a default value that may or may not contain data.
- *Hives*—Hives are specific branches in HKEY_USER and HKEY_LOCAL_MACHINE. Hive branches in HKEY_LOCAL_MACHINE\Software are SAM, Security, Components, and System. For HKEY_USER, each user account has its own hive link to Ntuser.dat.

Examining the Windows Registry

Some forensics tools, such as ProDiscover and FTK, have built-in Registry viewers. For this next activity, your company's Legal Department has asked you to search for any references to the Superior Bicycles company and e-mail addresses containing the name Denise. A paralegal tells you the home page for Superior Bicycles (www.superiorbicycles.biz) and gives you a ProDiscover .eve file containing the image of a Windows 98 computer belonging to a Superior Bicycle employee named Denise Robinson.

For this activity, you use ProDiscover Basic to extract System.dat and User.dat from the image file, and then use Access Data Registry Viewer to see what information you can find in these files. If you find any items of interest, you copy the Registry path and name to a text file that you can give to the paralegal. Although the file is an image of a Windows 98 computer, you can use Windows XP or Vista to run ProDiscover Basic and Access Data Registry Viewer in the following activities. Registry Viewer can run in Windows 9x and later and analyze all Windows Registry versions.

To extract Registry files with ProDiscover Basic, follow these steps:

1. Start ProDiscover Basic with the Run as administrator option. If the Launch Dialog box opens, click Cancel.
2. Click File, New Project from the menu.
3. In the New Project dialog box, type InChap06 in the Project Number text box and the Project File Name text box, and then click OK.
4. In the tree view of the main window, click to expand Add and then click Image File.
5. In the Open dialog box, navigate to your work folder, click the GCFI-Win98.eve image file, and click Open. Click Yes in the Auto Image Checksum message box, if necessary.
6. Click the Search toolbar button. In the Search dialog box, click the Content Search tab. Click the Search for files named option button, and in the Search text box, type system.dat and user.dat. Under Select the Disk(s)/Image(s) you want to search in, click the image file (see Figure 6-26), and then click OK.

7. In the search results, click the check box next to the SYSTEM.DAT file. When the Add Comment dialog box opens, type Registry files to extract, click the Apply to all items check box, and then click OK (see Figure 6-27).
8. Click the check box next to the USER.DAT file, and then click Tools, Copy Selected Files from the menu. In the Choose Destination dialog box, click Browse. In the Browse for Folder dialog box, navigate to and click your work folder, and then click OK. Click OK again in the Choose Destination dialog box.
9. Exit ProDiscover Basic, saving the project if prompted.

Microsoft Startup Tasks

You should have a good understanding of what happens to disk data at startup. In some investigations, you must preserve data on the disk exactly as the suspect last used it. Any access to a computer system after it was used for illicit purposes alters your disk evidence. As you learned in Chapter 4, altering disk data lessens its evidentiary quality considerably. In some instances, accessing a suspect computer incorrectly could make the digital evidence corrupt and less credible for any litigation.

In the following sections, you learn what files are accessed when Windows starts. This information helps you determine when a suspect's computer was last accessed, which is particularly important with computers that might have been used after an incident was reported.

Startup in Windows NT and Later

Although Windows NT is much different from Windows 95 and 98, the startup method for the NT OSs—NT, 2000, XP, and Vista—is about the same. There are some minor differences in how certain system start files function, but basically, they accomplish the same orderly startup.

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

Windows OSs use the files discussed in the following sections to start. These files can be located on the system partition or boot partition.

Startup Files for Windows Vista When Microsoft developed Vista, it updated the boot process to use the new Extensible Firmware Interface (EFI) as well as the older BIOS system. The EFI boot firmware is designed to provide better protection against malware than BIOS does. EFI Vista's boot processes have also changed since Windows XP. The Ntldr program in Windows XP used to load the OS has been replaced with these three boot utilities:

- *Bootmgr.exe*—The Windows Boot Manager program controls boot flow and allows booting multiple OSs, such as booting Vista along with XP.
- *Winload.exe*—The Windows Vista OS loader installs the kernel and the Hardware Abstraction Layer (HAL) and loads memory with the necessary boot drivers.
- *Winresume.exe*—This tool restarts Vista after the OS goes into hibernation mode.

Startup Files for Windows XP unless otherwise specified, most startup files for Windows XP are located in the root folder of the system partition. The NT Loader (Ntldr) file loads the OS. When the system is powered on, Ntldr reads the Boot.ini file, which displays a boot menu. After you select the mode to boot to, Boot.ini runs Ntldr.exe and reads Bootvid.dll, Hal.dll, and startup device drivers. Boot.ini specifies the Windows XP path installation and contains options for selecting the Windows version.

If a system has multiple boot OSs, including older ones such as Windows 9x or DOS, Ntldr reads BootSect.dos (a hidden file), which contains the address (boot sector location) of each OS.

When the boot selection is made, Ntldr runs NTDetect.com, a 16-bit real-mode program that queries the system for device and configuration data, and then passes its findings to Ntldr. This program identifies components and values on the computer system, such as the following:

- CMOS time and date value
- Buses attached to the motherboard, such as Industry Standard Architecture (ISA) or Peripheral Component Interconnect (PCI)
- Disk drives connected to the system
- Mouse input devices connected to the system

Contamination Concerns with Windows XP When you start a Windows XP NTFS workstation, several files are accessed immediately. When any of these or other related OS files are accessed at startup, the last access date and time stamp for the files change to the current date and time. This change destroys any potential evidence that shows when a Windows XP workstation was last used. For this reason, you should have a strong working knowledge of the startup process.

Startup in Windows 9x/Me

Like Windows XP, system files in Windows 9x/Me containing valuable information can be altered easily during startup, which affects their evidentiary value and integrity. Windows 9x OSs have similar boot processes. Windows Me is similar, too, with one important exception: You can't boot to a true MS-DOS mode. When you're conducting a computing investigation, being able to boot to MS-DOS is preferred, especially if you're running a later version of Windows 95 OEM SR2 (version 4.00.1111) or a newer one in which the MS-DOS boot mode can read and write to a FAT32 disk.

Windows 9x OSs has two modes: DOS protected-mode interface (DPMI) and protected-mode GUI (serves the same purpose as Config.sys in MS-DOS). Many older computer forensics tools use DPMI mode and can't be run from a Windows command prompt window because they use certain disk accesses that conflict with the GUI.

The system files Windows 9x uses have their origin in MS-DOS. The Io.sys file communicates between a computer's BIOS, the hardware, and the OS kernel. During the boot phase of a Windows 9x system, Io.sys monitors the keyboard for an F8 keystroke. If F8 is pressed during startup, Io.sys loads the Windows Startup menu, which has options such as booting to Windows normally and running in Safe mode to perform maintenance.

Microsoft Windows 98 Startup Menu

1. Normal
2. Logged (\BOOTLOG.TXT)
3. Safe mode
4. Step-by-step confirmation
5. Command prompt only
6. Save mode command prompt only

Enter a choice: 1

MS-DOS Startup Tasks

MS-DOS uses three files when starting, with the same names as in Windows 9x/Me: Io.sys, Msdos.sys, and Command.com. Two other files are then used to configure MS-DOS at startup: Config.sys and Autoexec.bat. Although MS-DOS and Windows 9x use some of the same startup filenames, there are some important differences between the files in these OSs.

Io.sys is the first file loaded after the ROM bootstrap loader finds the disk drive. Io.sys then resides in RAM and provides the basic input and output service for all MS-DOS functions.

Msdos.sys is the second program to load into RAM immediately after Io.sys. As mentioned, this file is the actual OS kernel, not a text file as in Windows 9x and Me. After Msdos.sys finishes setting up DOS services, it looks for the Config.sys file to configure device drivers and other

settings. Config.sys is a text file containing commands that typically run only at system startup to enhance the computer's DOS configuration.

Msdos.sys then loads Command.com, which contains the same internal DOS commands in Windows 9x. As the loading of Command.com nears completion, Msdos.sys looks for and loads Autoexec.bat, a batch file containing customized settings for MS-DOS that runs automatically. In this batch file, you can define the default path and set environmental variables, such as temporary directories. MS-DOS then accesses and resets the last access dates and times on files when powered up.

Other Disk Operating Systems

Years ago, other microcomputer OSs, such as Control Program for Microprocessors (CP/M), Digital Research Disk Operating System (DR-DOS), and Personal Computer Disk Operating System (PC-DOS) were used. Of these OSs, only DR-DOS is still available. As mentioned in Chapter 1, if you encounter an old computer running one of these OSs, you might need to call on your network of experts to research, explore, and test the OS. This section summarizes some features of these OSs.

In the 1970s, Digital Research created the first nonspecific microcomputer OS, CP/M, which had a unique file system. Computers using CP/M had 8-inch floppy drives and didn't support hard drives. The CPU was the Zilog Z-80, which could access up to 64 KB RAM. In the early 1980s, IBM supplied an expansion card with a built-in Z-80 CPU that allowed users to process applications available for CP/M.

After Microsoft developed MS-DOS, Digital Research created DR-DOS in 1988 to compete with that OS; it used FAT12 and FAT16 and had a richer command environment than MS-DOS. DR-DOS is now sold primarily as an embedded OS for out-of-the-box ROM or Flash ROM systems.

When IBM created the first PC using the Intel 8088 processor, it contracted with Microsoft, then a startup company, to create an OS. In 1981, Microsoft purchased 86-DOS from Seattle Computing; it could run on the Intel 8088 16-bit processor and was a modification of CP/M. Microsoft supplied 86-DOS to IBM for use on its PCs, and IBM called it PC-DOS. IBM maintained upgrades to PC-DOS until Microsoft released Windows 95.

PC-DOS works much like MS-DOS, although its OS files are slightly different. For example, Io.sys is called Ibmio.sys, and Msdos.sys is called Ibmdos.sys. However, PC-DOS uses FAT12 and FAT16, so accessing data is no different from working with MS-DOS.

Virtual Machines

New versions of OSs and applications are released frequently, but older versions are still widely used. As an investigator, you'll be faced with the challenge of having enough resources to support the variety of software you're likely to encounter. More companies are turning to virtualization to reduce the cost of hardware purchases, so the number of investigations involving virtual machines will increase as this practice continues.

As an investigator, you might need a virtual server to view legacy systems, and you might need to forensically examine suspects' virtual machines. Virtual machines enable you run another OS on an existing physical computer (known as the host computer) by emulating a computer's hardware environment VMware Server virtual machine running Windows XP Professional on the desktop of a host computer. Typically, a virtual machine consists of several files. The two main files are the configuration file containing hardware settings, such as RAM, network configurations, port settings, and so on, and the virtual hard disk file, which contains the boot loader program, OS files, and users' data files.

A virtual machine acts like any other file but with a twist: It performs all the tasks the OS running on the physical computer can, up to a certain point. The virtual machine recognizes hardware components of the host computer it's loaded on, such as the mouse, keyboard, and CD/DVD drive. However, the guest OS (the one running on a virtual machine) is limited by the host computer's OS, which might block certain operations. For example, most virtual machines recognize a CD/DVD drive because the host computer defaults to auto-detect. Some virtual machines don't recognize a USB drive; this capability varies with the virtualization software. Although networking capabilities are beyond the scope of this book, be aware that virtual machines can use bridged, Network Address Translation (NAT), or other network configurations to determine how they access the Internet and communicate with systems on the local network.

Creating a Virtual Machine

Some common applications for creating virtual machines are VMware Server and VMware Workstation, Sun Microsystems Virtual Box, and Microsoft Virtual PC, although others are available. Virtual Box is an open-source program that can be downloaded at www.virtualbox.org.

Consult with your instructor before doing the following activity. You must download and install Virtual PC first, and you need an ISO image of an OS because no OSs are provided with Virtual PC. Follow these steps to create a virtual machine:

1. If you haven't already done so, install Microsoft Virtual PC.
2. Start Virtual PC. In Virtual PC 2007, the New Virtual Machine Wizard starts automatically. (If it doesn't, click File, New Virtual Machine Wizard from the menu.)

3. In the welcome window of the New Virtual Machine Wizard, click Next.
4. In the Options window, click the Create a virtual machine option button, and click Next.

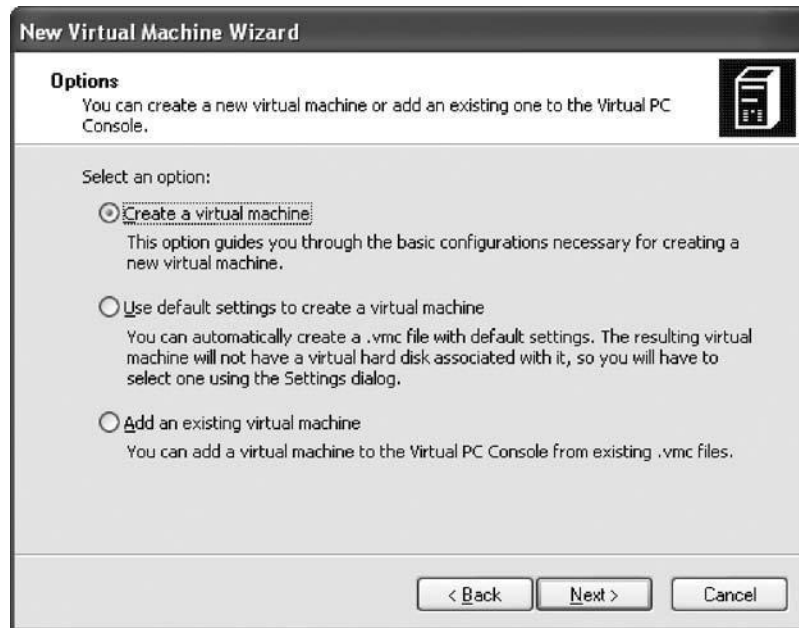


Fig: creating a new virtual machine

5. In the Virtual Machine Name and Location window, type Windows Server 2003 for the virtual machine name. Note that the default location for Vista is Documents\ Virtual Machines. Your instructor might tell you to use a different location. Click Next.
6. In the Operating System window, click Windows Server 2003 in the Operating system list box, and then click Next.
7. In the Memory window, you allocate the amount of RAM. You can increase the amount of RAM if needed, but for now, leave it at the recommended level, and then click Next.
8. In the Virtual Hard Disk Options window, click the A new virtual hard disk option button, and then click Next.
9. In the Virtual Hard Disk Location window, accept the default location and then click Next.
10. Click Finish.

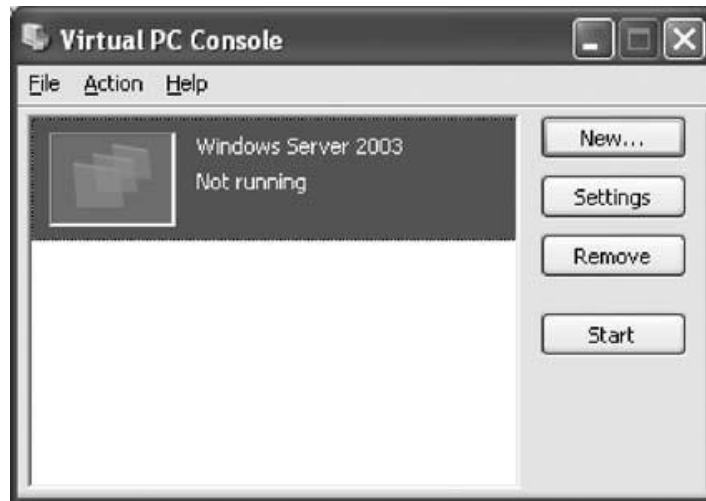


Fig: The Virtual PC Console with a virtual machine available

In the following activity, you use an ISO image that your instructor will provide on the network or a CD for installing a guest OS. For any guest OS, you must have a valid product key to install it. You can get the product key from your instructor.

1. In the Virtual PC Console, make sure the Windows Server 2003 virtual machine is selected, and then click the Start button.
2. The Virtual PC user console opens, similar to the window you see when a physical computer starts, and Virtual PC examines the host computer's hardware.
3. This book assumes you know how to install an OS, so detailed steps aren't given. Virtual PC treats an ISO image the same as an installation CD, so when you're prompted for the source disk, enter the location of the ISO image. For the name of the owner, type Sally Freidman, and for the company name, type ABC Corporation.
4. Create a domain name of Main Host.
5. Create an administrator password and make a note of it.
6. After the OS is installed, log on. Note that pressing Ctrl+Alt+Delete activates the host computer. To log on to the virtual machine, press right Alt+Delete. (You can also use Alt+Enter for full screen.)
7. You should be able to navigate through the contents of the Windows Server 2003 virtual server as though it were a real computer. To switch between the virtual machine window and the desktop, press right Alt and move the cursor.
8. To exit Virtual PC, click File, Close from the menu, and then click Turn off in the drop-down list.