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)

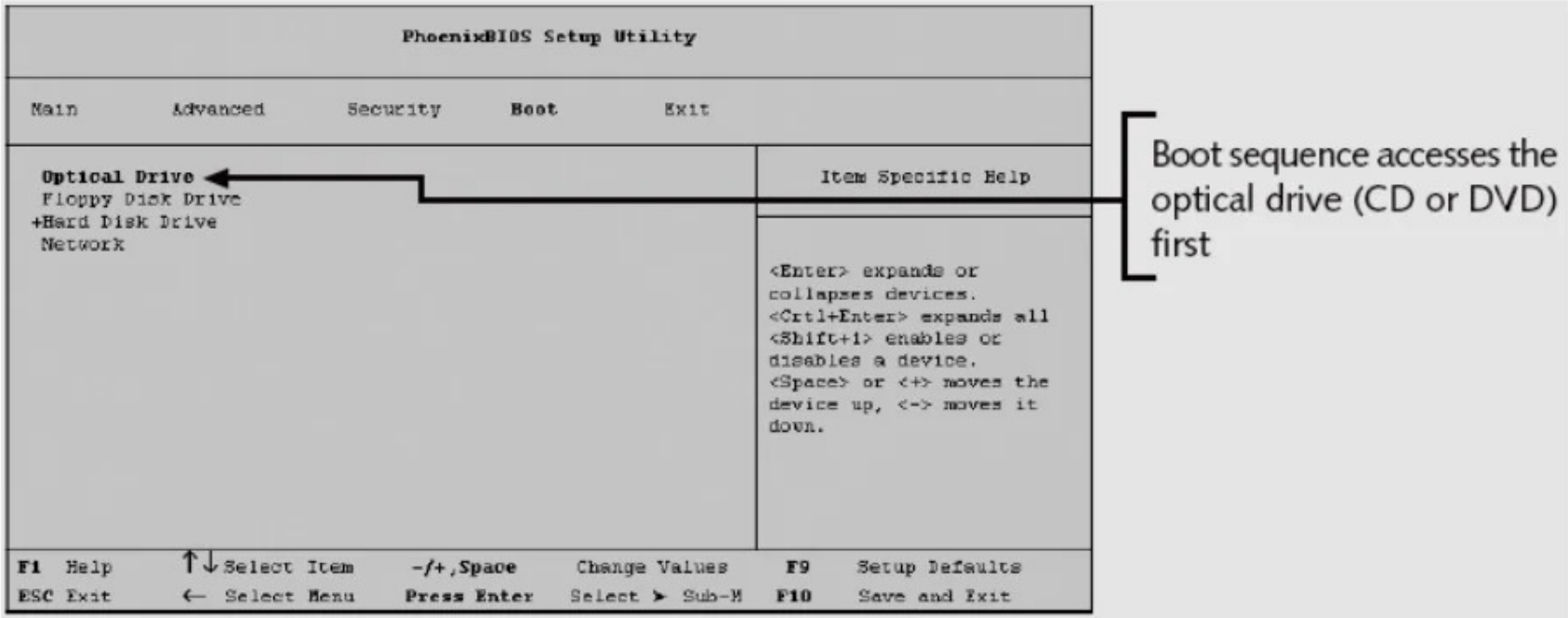

Figure 6-1 A typical CMOS setup screen

Understanding the Boot Sequence (continued)

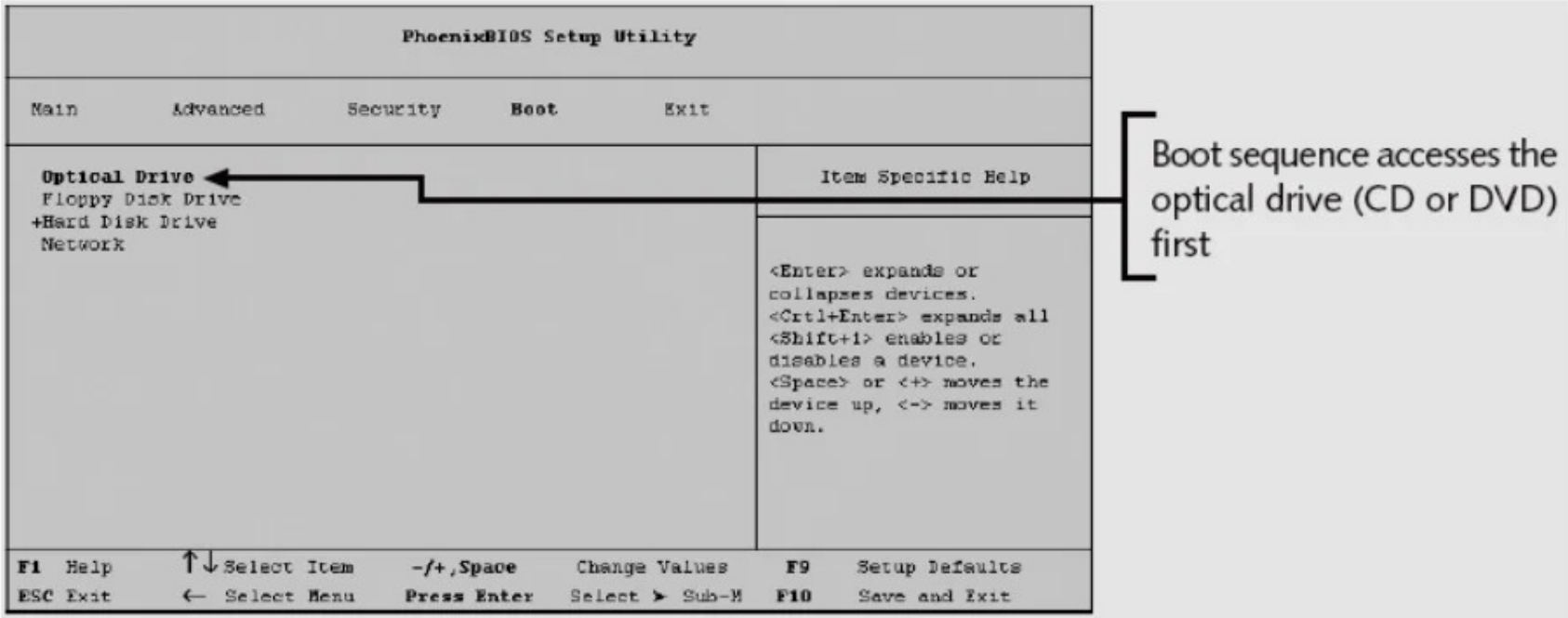

Figure 6-1 A typical CMOS setup screen

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

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

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

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)

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

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

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

Disk Partitions (continued)

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

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

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

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

Examining FAT Disks (continued)

- 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

Examining FAT Disks (continued)

- 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

Examining FAT Disks (continued)

- 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

Examining FAT Disks (continued)

- 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

Examining FAT Disks (continued)

- 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

Examining FAT Disks (continued)

- 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 (σ) 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

Examining NTFS Disks (continued)

Table 6-3 Cluster sizes in an NTFS disk

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)

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

Examining NTFS Disks (continued)

Table 6-3 Cluster sizes in an NTFS disk

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)

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 Metadata records in the MFT (continued)

Filename	System file	Record position	Description
$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.

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 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.

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)

- 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

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

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

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

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

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
  - Copy
  - 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)

- 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

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 6-7 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

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

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

Examining the Windows Registry (continued)

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

Examining the Windows Registry (continued)

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

Examining the Windows Registry (continued)

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

Examining the Windows Registry (continued)

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

Examining the Windows Registry (continued)

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)

- 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 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 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 Io.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

Creating a Virtual Machine (continued)

Figure 6-36 Properties of a virtual machine

Creating a Virtual Machine (continued)

Figure 6-36 Properties of a virtual machine

Creating a Virtual Machine (continued)

Figure 6-36 Properties of a virtual machine

Creating a Virtual Machine (continued)

Figure 6-36 Properties of a virtual machine

Creating a Virtual Machine (continued)

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)

- 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

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