Forensics
Book 2: Investigating Hard Disk and File and Operating Systems

Chapter 1: Understanding File Systems and Hard Disks

Objectives

- Understand disk drives, hard disks, and hard disk interfaces
- Understand disk partitions
- Understand the master boot record
- Understand different types of file systems
- Enumerate and explain popular Linux file systems

Objectives (continued)

- Understand Sun Solaris 10 file system ZFS
- Understand the Mac OS X file system
- Understand the various Windows file systems, including FAT and NTFS
- Understand CD-ROM and DVD file systems
- Understand the EFS recovery key agent

Objectives (continued)

- Examine registry data
- Enumerate Windows XP system files
- Understand the Windows boot process

Introduction to File Systems and Hard Disks

- This chapter describes:
  - Disk drives
  - Hard disks
  - Physical data storage
  - File systems

Disk Drive Overview

- **Disk drive**
  - Mechanism that reads data from a disk and writes data onto a disk
- The disk in the disk drive rotates at very high speeds
- Heads in the disk drive are used to read and write data
- Different types of disk drives use different types of disks
  - HDD, FDD, ODD

Types of Disk Drives

- Disk drives are categorized into the following types:
  - Fixed
  - Removable
    - Floppy disk
    - CD-ROM
    - DVD
    - Zip disk

Hard Disks

- Data is organized on a hard disk in a method similar to that of a file cabinet
- When a computer uses a program or data, the program or data is copied from its location to a temporary location
- Data is recorded magnetically onto a hard disk
  - Rapidly spinning platter used as the recording medium
  - Heads just above the surface of the platter are used to read data from and write data to the platter
  - Two common interfaces: IDE and SCSI

Characteristics

- Characteristics include:
  - Capacity of the hard disk
  - Interface used
  - Speed in rotations per minute
  - Seek time
  - Access time
  - Transfer time
- Once damaged, a hard disk usually cannot be repaired

Physical Makeup

- Hard disk
  - Sealed unit containing a number of platters in a stack
  - Can be mounted in a horizontal or vertical position
  - Electromagnetic read/write heads are positioned above and below each platter
- Data is stored in thin, concentric bands, called tracks
- Tracks consist of sectors
- Sectors:
  - Smallest physical storage units on a hard disk
  - Sector is almost always 512 bytes (0.5 kilobyte) in size

Physical Makeup (continued)

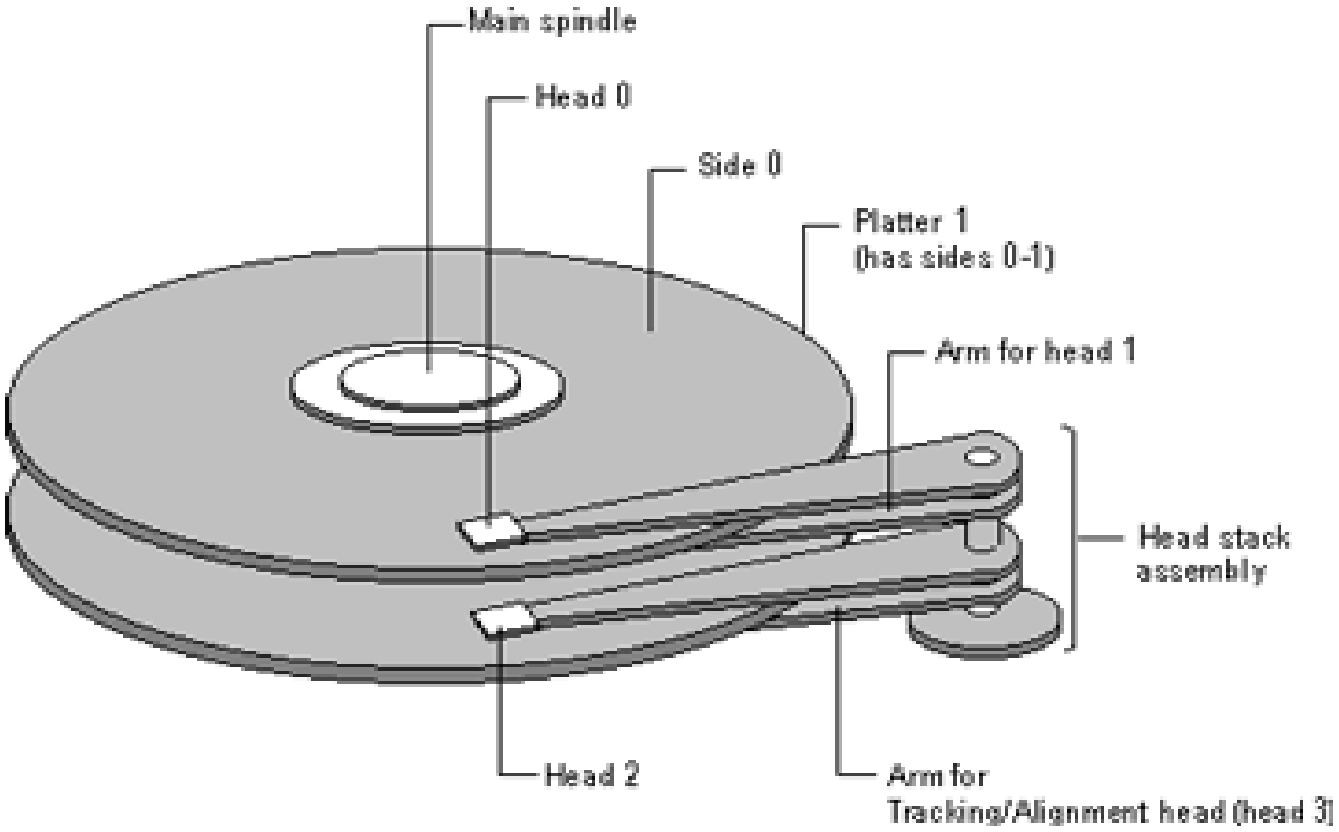


Figure 1-1 A hard disk platter has two sides, and there is a read/write head for each side.

Zoned Bit Recording

- Zoned bit recording
  - Also known as multiple zone recording
  - Combines tracks together into zones depending on their distance from the center of the disk
  - Each zone is assigned a number of sectors per track
- Three types of data densities on a hard disk:
  - Track density
  - Area density
  - Bit density

Hard Disk Interfaces

- Types of hard disk interfaces:
  - Small computer system interface (SCSI)
  - Integrated drive electronics/enhanced IDE (IDE/EIDE)
  - Universal Serial Bus (USB)
  - Advanced technology attachment (ATA)
    - Serial ATA
    - Parallel ATA
  - Fiber Channel
    - Fiber Channel electrical interface
    - Fiber Channel optical interface

Hard Disk Interfaces (continued)

- SCSI (small computer system interface)
  - Set of ANSI standard electronic interfaces that allow personal computers to communicate with peripheral hardware faster and more flexibly than previous interfaces
  - Developed by Apple Computer
  - Allows up to 7 or 15 devices to be connected to a single SCSI port in daisy-chain fashion
- Ultra-2 SCSI for a 16-bit bus can transfer data at a rate of up to 80 Mbps

Hard Disk Interfaces (continued)

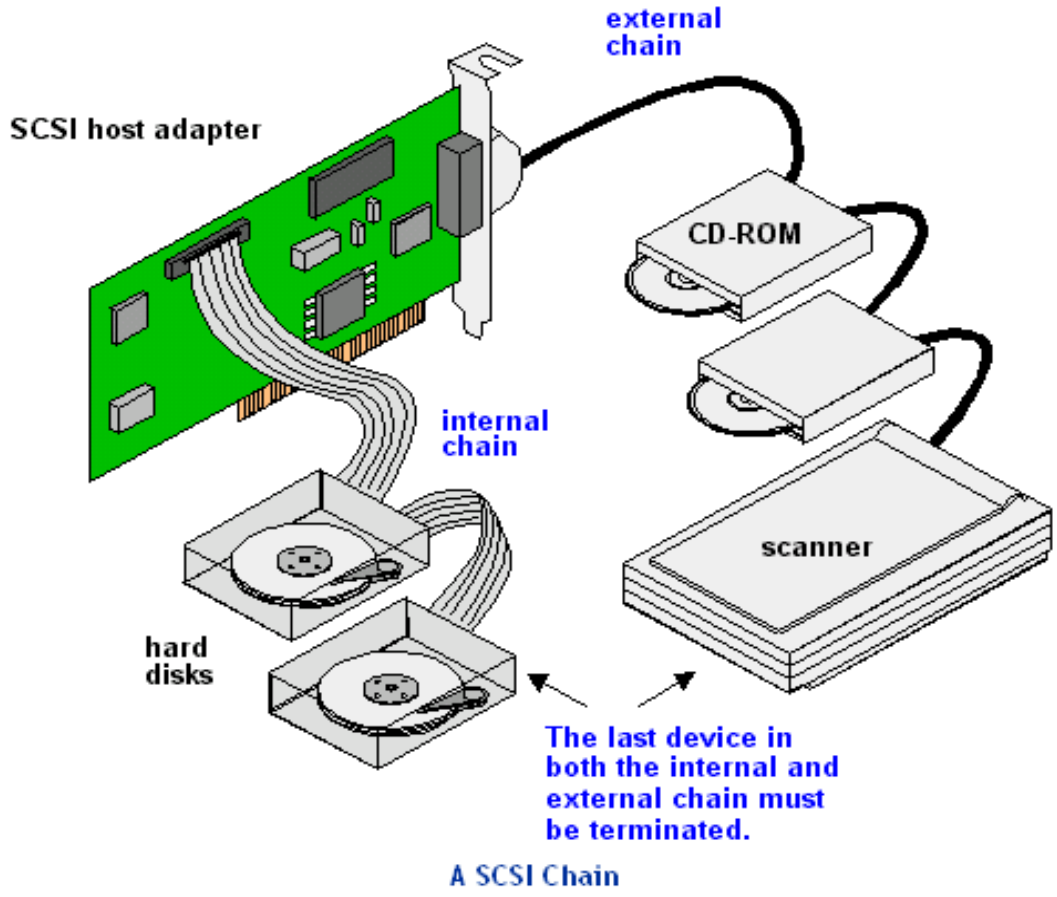


Figure 1-2 A typical SCSI chain.

Hard Disk Interfaces (continued)

Technology Name	Maximum Cable Length (meters)	Maximum Speed (Mbps)	Maximum Number of Devices
SCSI-1	6	5	8
SCSI-2	6	5–10	8 or 16
Fast SCSI-2	3	10-20	8
Wide SCSI-2	3	20	16
Fast Wide SCSI-2	3	20	16
Ultra SCSI-3, 8-bit	1.5	20	8
Ultra SCSI-3, 16-bit	1.5	40	16
Ultra-2 SCSI	12	40	8
Wide Ultra-2 SCSI	12	80	16
Ultra-3 (Ultra160/m) SCSI	12	160	16

Table 1-1 Current SCSI standards.

Hard Disk Interfaces (continued)

- IDE/EIDE
  - Standard electronic interface used between a computer motherboard's data paths or bus and the computer's disk storage devices
  - Based on IBM PC ISA 16-bit bus standard
  - Two types of enhanced IDE sockets are built into motherboards
  - IDE drives are configured as master and slave
- Most computers sold today use either:
  - An enhanced version of IDE called enhanced integrated drive electronics (EIDE)
  - Serial ATA (SATA)

Hard Disk Interfaces (continued)

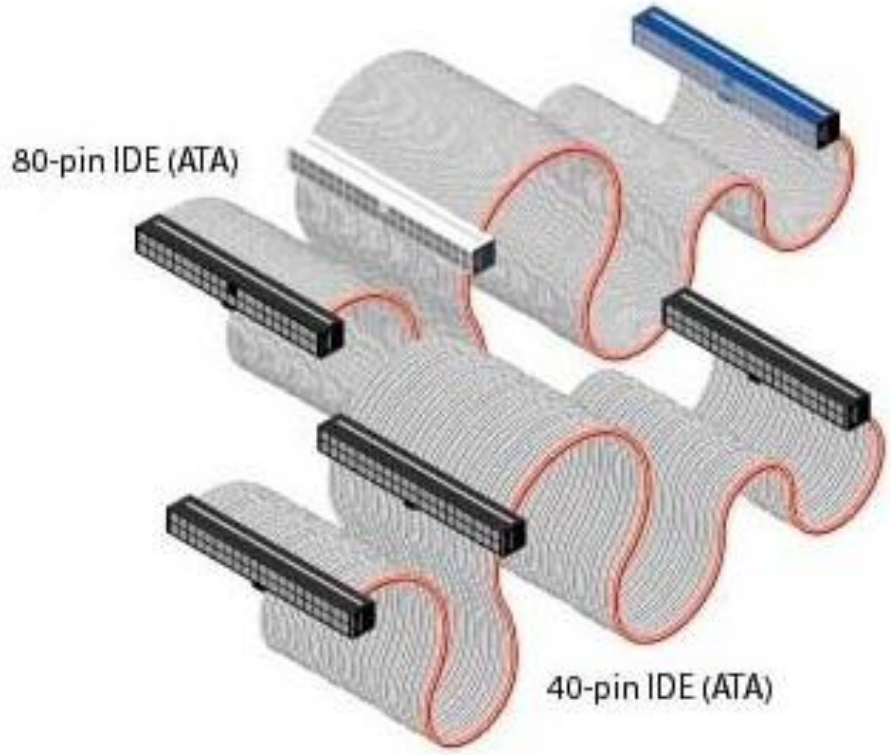


Figure 1-3 IDE cables come in both 40-pin and 80-pin versions.

Hard Disk Interfaces (continued)

- Fault tolerance for IDE drives
  - The DupliDisk PCI card provides fault tolerance for IDE drives

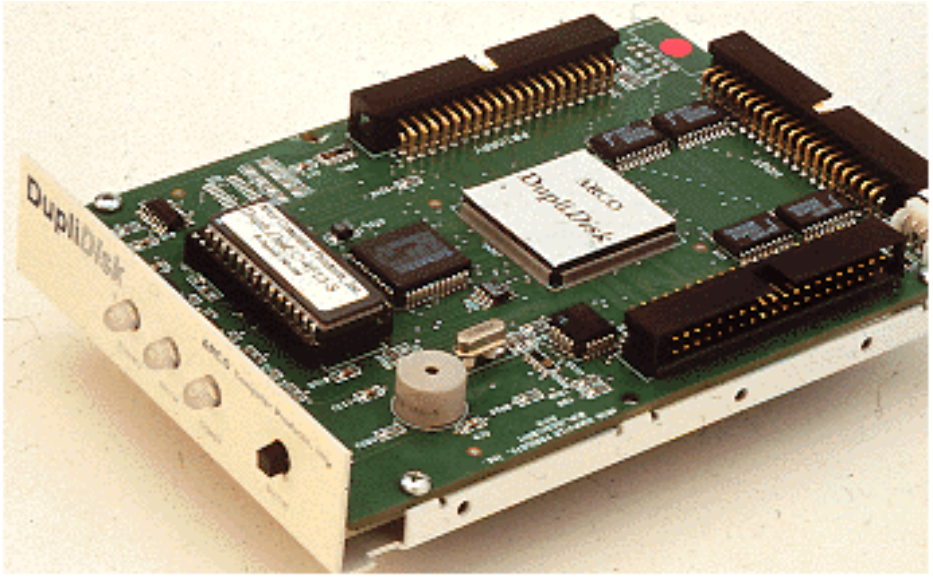


Figure 1-4 The DupliDisk PCI card provides fault tolerance.

Hard Disk Interfaces (continued)

- Universal Serial Bus (USB)
  - Developed by Intel, was first released in 1995
  - Current data transfer speed: up to 480 Mbps
  - Some features of USB:
    - Ease of use
    - Expandability
    - Speed for the end user
    - High performance and ubiquity
    - Easy connection of peripherals outside the PC
    - Automatic configuration of devices by most operating systems
    - Usefulness in PC telephony and videoconferencing

Hard Disk Interfaces (continued)

- Serial ATA (SATA)
  - Offers a point-to-point channel between the motherboard and the drive
  - Some features of SATA:
    - Fast operating speed
    - Upgradeable storage devices
    - Ease of configuration
    - Transfer speed of 1.5 Gbps

Hard Disk Interfaces (continued)

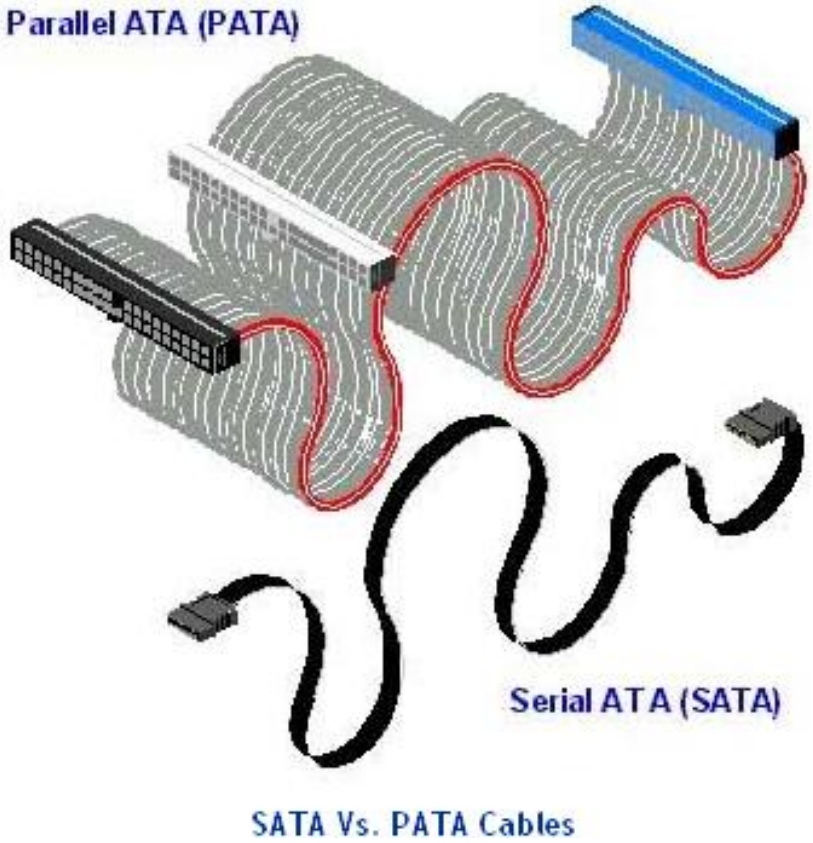


Figure 1-5 A SATA cable is thinner than a PATA cable.

Hard Disk Interfaces (continued)

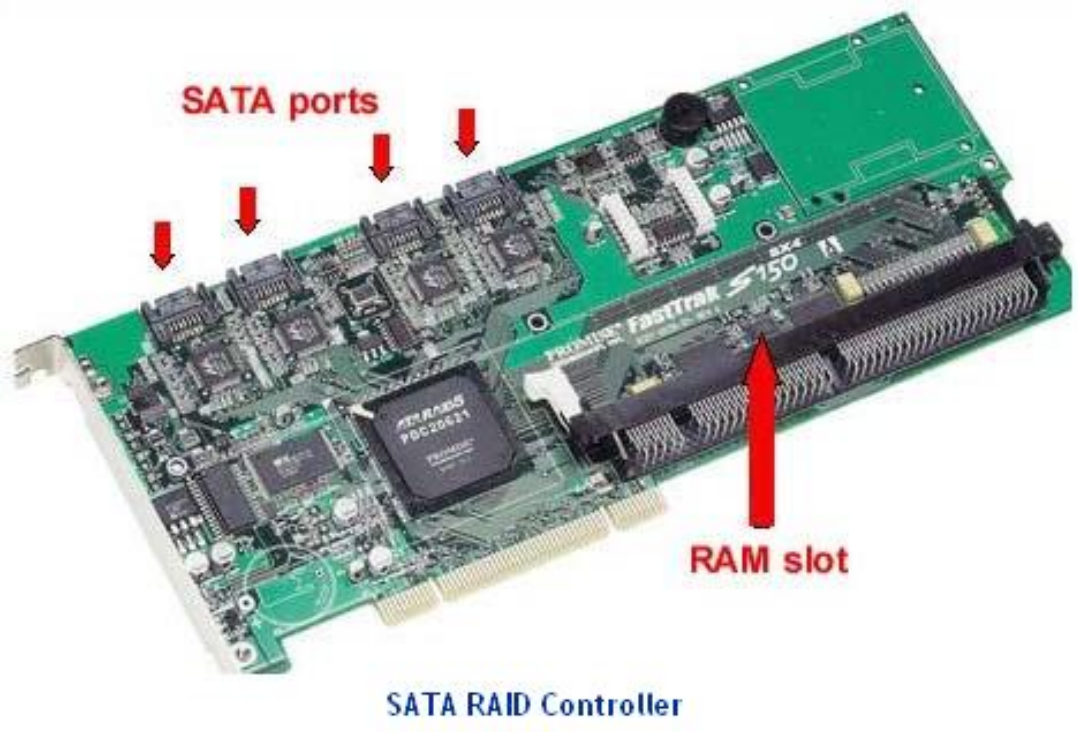


Figure 1-7 A SATA RAID controller.

Hard Disk Interfaces (continued)

- Parallel ATA (PATA)
  - Provides a controller on the disk drive itself
    - Thereby eliminating the need for a separate adapter card
  - Some features of PATA:
    - Low relative cost
    - Ease of configuration
    - Look-ahead caching
- Fiber Channel
  - Point-to-point bidirectional serial interface
  - Supports up to 1.0625 Gbps transfer rates

Hard Disk Interfaces (continued)

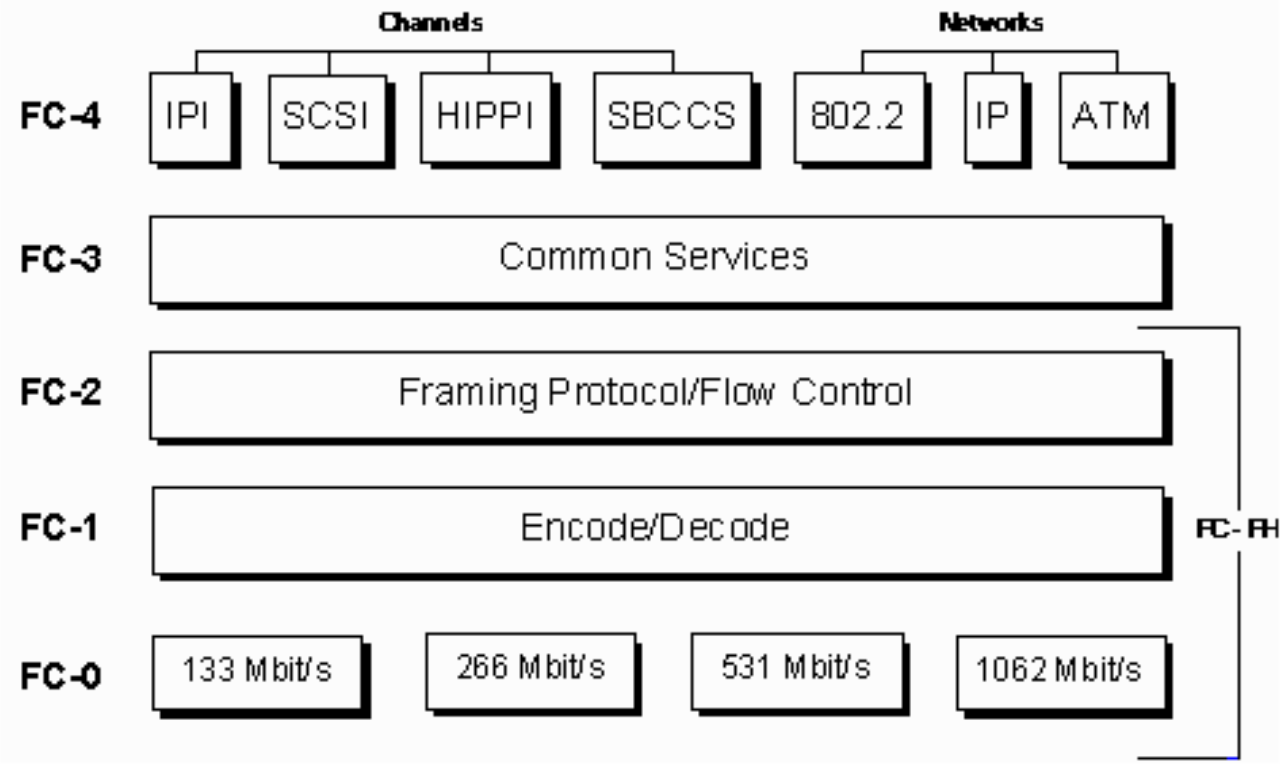


Figure 1-8 A typical Fiber Channel interface.

Hard Disk Interfaces (continued)

- Some features of Fiber Channel:
  - Low costs
  - Support of higher data transfer rates
- Types of Fiber Channels:
  - Fiber Channel electrical interface
  - Fiber Channel optical interface

Disk Platters

- **Disk platters**
  - Round, flat, magnetic metal or ceramic disks in a hard disk that hold the actual data
- Made of two components:
  - Substrate material
    - Gives the platter structure and rigidity
  - Magnetic media coating
    - Platters are coated with magnetic media: holds the magnetic impulses that represent the data
- Area density, also known as bit density
  - Amount of data that can be stored on a given amount of a hard disk platter

Disk Platters (continued)

- Platter organization
  - Each platter has two read/write heads
    - One on the top of the platter and one on the bottom
  - Platters are divided into tracks
    - Tracks are concentric circles that logically partition platters
  - Tracks are divided into sectors
    - Each sector holds 512 bytes of information
- Platter size
  - For a 5.25-inch: disk is usually 5.12 inches
  - For a 3.5-inch: disk is usually 3.74 inches

Disk Platters (continued)

- Number of Platters
  - As the number of platters increases, storage capacity rises
    - But the space between each platter becomes smaller
  - Hard disks with a large number of platters: more sensitive to vibrations, flaws in the surface of a platter, and head misalignment
- Tracks
  - Concentric circles on platters where all the information is stored
  - Every platter in a hard disk has the same track density

Disk Platters (continued)

- Track numbering
  - Typically numbered from 0 at the outer edge to 1023 at the center
  - Track location: often referred to by a cylinder number rather than a track number
- Cylinder
  - Set of tracks that can be accessed by all the heads when the heads are in a particular position
  - Represents a set of tracks on all the platters in a hard disk

Disk Platters (continued)

- Sectors contain the following information:
  - ID information
  - Synchronization fields
  - Data
  - ECC
  - Gaps
- Sector organization and overhead
  - The contents of a sector that are not user data constitute sector overhead
  - Overhead must be minimized for greater efficiency

Disk Platters (continued)

- **Bad sectors**
  - Areas of a disk that have become unusable
  - Can be caused by configuration problems or physical disturbances
  - Common causes include:
    - Excessive read/write operations
    - Sudden voltage surges
    - Certain viruses
    - Corrupted boot records
  - If data is in a sector that becomes bad, then it might not be recoverable

Disk Platters (continued)

- Bad sectors (continued)
  - Once a bad sector is identified, it is marked as bad and cannot be used again
    - Called defect mapping
  - Modern hard disks contain reserved sectors that are used in place of bad sectors
    - Called spare sectoring
  - Bad sectors are cleverly hidden and are never seen by the operating system
- **Clusters**
  - Smallest logical storage units on a hard disk

Disk Platters (continued)

- Cluster organization
  - Cluster entries are maintained by computer's file system
  - Clusters are:
    - Chained to each other
    - Ordered on a disk using continuous numbers
    - Entire file does not have to be in one continuous block
- Cluster size
  - Determined when disk volume is partitioned
  - Larger volumes use larger cluster sizes
  - Ranges from 4 sectors (2,048 bytes) to 64 sectors (32,768 bytes)

Disk Platters (continued)

- Slack space
  - Area of disk cluster between end of the file and end of the cluster
  - When a greater number of files are stored on a disk with a large cluster size
    - Much disk space is wasted as slack space
- **Lost cluster**
  - FAT file system error: results from how the FAT file system allocates space and chains files together
  - Mainly the result of a logical structure error, not a physical disk error
  - Usually occurs because of interrupted file activities

Disk Platters (continued)

- Disk-checking programs, such as ScanDisk, can find lost clusters using the following procedure:
  - Create a memory copy of the FAT, noting all of the clusters marked as being in use
  - Trace the clusters starting from the root directory, and mark each cluster used by a file as being accounted for
    - Continue through all directories on disk
  - When the scanning process is finished, any clusters that are in use but not accounted for are orphans, or lost clusters

Disk Partition

- **Partitioning**
  - Creation of logical drives on a disk
  - Partition: logical drive that holds data
- Types of partitions:
  - Primary partition
  - Extended partition
- Data can be hidden on a hard disk by creating hidden partitions on the disk drive
  - Investigators can find the data using disk editor utilities like Norton Disk Edit

Master Boot Record

- **Master boot record (MBR)**
  - First sector of a data storage device
  - Also called partition sector, master partition table
  - Includes table that contains information about each partition that the hard disk has been formatted into
- **Boot sector**
  - Sector of a storage device that contains the code for bootstrapping a system
  - Contains a program that loads the rest of the operating system into RAM

Master Boot Record (continued)

- In DOS and Windows systems, a user can create the MBR with the **fdisk /mbr** command
- Backing up the MBR
  - In UNIX and Linux, **dd** can be used to backup and restore the MBR

Disk Capacity Calculation

- Consider a hard disk drive with the following attributes:
  - 16,384 cylinders
  - 80 heads
  - 63 sectors per track
  - 512 bytes per sector
- Total capacity for this disk = 1 disk * (16,384 cylinders/disk) * (80 heads/cylinder) * (1 track/head) * (63 sectors/track) * (512 bytes/sector) = 42,278,584,320 bytes

Hard Disk Tools

- Allow investigators to perform the following tasks:
  - Search the text on hard disks in file space, slack space, and unallocated space
  - Find and recover data from files that have been deleted
  - Find data in encrypted files
  - Repair file allocation tables, partition tables, and boot records
  - Concatenate and split files
  - Analyze and compare files
  - Clone hard disks
  - Make drive images and backups

Understanding File Systems

- File system
  - Type of system to effectively store, organize and access data on a computer
- File system provides the following:
  - Storage
  - Hierarchical categorization
  - Management
  - Navigation
  - Access
  - Data recovery features

Types of File Systems

- Categories:
  - Disk file system
  - Network file system
  - Database file system
  - Special purpose file system

Types of File Systems (continued)

- Disk file systems include:
  - Advanced Disc Filing System (ADFS)
  - Be File System (BFS)
  - Encrypting File System (EFS)
  - Extent File System (EFS)
  - Extended File System (ext)
  - Second Extended File System (ext2)
  - Third Extended File System (ext3)
  - File Allocation Table (FAT)
  - Amiga Fast File System (FFS (Amiga))
  - Files-11

Types of File Systems (continued)

- Disk file systems include: (continued)
  - Hierarchical File System (HFS)
  - Hierarchical File System Plus (HFS Plus)
  - Hierarchical File System (HFSX)
  - High Performance File System (HPFS)
  - ISO 9660
  - Journaled File System (JFS)
  - Log-structured File System (LFS)
  - Macintosh File System (MFS)
  - Minix
  - New Technology File System (NTFS)

Types of File Systems (continued)

- Disk file systems include: (continued)
  - Novell Storage Services (NSS)
  - Old File System (OFS)
  - Professional File System (PFS)
  - Reiser File System (ReiserFS)
  - Reiser4 File System (Reiser4)
  - Smart File System (SFS)
  - Sprite operating system (Sprite)
  - Universal Disk Format (UDF)
  - UNIX File System (UFS)
  - UMSDOS

Types of File Systems (continued)

- Disk file systems include: (continued)
  - Veritas File System (VxFS)
  - Virtual Storage Access Method (VSAM)
  - XFS
  - Zetabyte File System (ZFS)

Types of File Systems (continued)

- Network file systems include:
  - Andrew file system (AFS)
  - AppleShare
  - Coda
  - Global File System (GFS)
  - InterMezzo File System (InterMezzo)
  - Lustre File System (Lustre)
  - Network File System (NFS)
  - OpenAFS
  - Server Message Block (SMB)

Types of File Systems (continued)

- Special purpose file systems include:
  - Acme File System (acme)
  - Compact Disc File System (cdfs)
  - WEB-DAV Linux File System (Davfs2)
  - Device File System (devfs)
  - Fuse File System (fuse)
  - Long file System (lnfs)
  - Plumber (Plan 9)
  - Process File System (procfs)
  - Wiki File System (wikifs)
  - Parallel File System (ParFiSys)

Popular Linux File Systems

- Linux operating system
  - Single hierarchical tree structure that represents the file system as one single entity
- Some popular file systems used with Linux:
  - ext (Extended File System)
  - ext2 (Second Extended File System)
  - ext3 (Third Extended File System)

Sun Solaris 10 File System: ZFS

- **ZFS (Zettabyte File System)**
  - Dynamic file system in Sun's Solaris 10 operating system (Solaris OS)
  - Supported by both x86 and SPARC platforms
  - Endian-neutral
  - Supports almost unlimited scalability by refining the file system
  - Can dynamically grow and shrink the storage pool without interrupting any services

Sun Solaris 10 File System: ZFS (continued)

- Features:
  - Copy on write
  - LVM
  - Endianness
  - Checksums
  - HA Storage+
  - Clones
  - Compression
  - ACLs (access control lists)

Mac OS X File Systems

- Hierarchical File System (HFS)
  - File system developed by Apple Computer for Mac OS
  - Divides a volume into logical blocks of 512 bytes
  - Logical blocks are then grouped together into allocation blocks
- Five structures that make up an HFS volume:
  - Logical blocks 0 and 1
  - Logical block 2
  - Logical block 3
  - The extent overflow file
  - The catalog file

UFS (Unix File System)

- UFS is a file system utilized by many UNIX and UNIX-like operating systems
  - Derived from the Berkeley Fast File System
- UFS is composed of the following parts:
  - A few blocks at the beginning of the partition reserved for boot blocks
  - A superblock, including a magic number identifying this as a UFS file system
  - A collection of cylinder groups

Windows and DOS File Systems

- Main Windows and DOS file systems:
  - FAT16 (File Allocation Table)
  - FAT12
  - FAT32
  - NTFS (New Technology File System)
- FAT file system
  - File system used with DOS
  - First file system used with the Windows operating system

Windows and DOS File Systems (continued)

- Boot sector
  - First sector (512 bytes) of a FAT file system
  - In UNIX, called the superblock
- File recovery
  - When a file is deleted from a FAT volume
    - Operating system replaces the first letter of the file name with a lowercase Greek letter
  - Space is then made available for new files
  - Files can be recovered using forensic tools, such as: WinHex, Undelete, and File Scavenger

Windows and DOS File Systems (continued)

Bytes	Content
0–2	Jump to bootstrap
3–10	OEM name/version
11–12	Number of bytes per sector
14–15	Number of reserved sectors
17–18	Number of root directory entries
19–20	Total number of sectors in the file system
21	Media descriptor type
22–23	Number of sectors per FAT
24–25	Number of sectors per track
26–27	Number of heads
28–29	Number of hidden sectors
30–509	Bootstrap
510–511	Signature

Table 1-2 The boot sector contains information about a disk.

NTFS

- New Technology File System (NTFS)
  - One of the latest file systems supported by Windows
  - High-performance file system that repairs itself
  - Supports several advanced features such as file-level security, compression, and auditing
  - Supports large and powerful volume storage solutions such as self-recovering disks
- Features
  - NTFS provides data security
  - NTFS uses a 16-bit Unicode character set to name files and folders
  - Fault-tolerant file system

NTFS (continued)

File Name	System File	Record Position	Description
$MFT	MFT 1	0	This is the base file record for an NTFS volume.
$MftMirr	MFT 2	1	The first four records of MFT are stored here for restoration purposes.
$LogFile	Log File	2	Previous transactions are listed and stored, for restoration purposes.
$Volume	Volume	3	Information regarding the volume is stored in this table.
$AttrDef	Attribute definitions	4	This list contains attributes of files.
$	Root file name index	5	This is the root folder.
$Bitmap	Boot sector	6	This is a list that shows the availability and usage of the clusters.
$Boot	Boot sector	7	This is used to mount the NTFS volume during the bootstrap process.
$BadClus	Bad cluster file	8	This contains a list of the clusters that have unrecoverable errors.
$Secure	Security file	9	This access control list has the unique security descriptors for the files on the volume.
$Upcase	Upcase table	10	This is used to convert all uppercase characters to lowercase Unicode characters.
$Extend	NTFS extension file	11	Optional extensions like quotes and object identifiers are listed here.

Table 1-3 The NTFS system files.

NTFS (continued)

Byte Offset	Field Length	Field Name
0x00	3 bytes	Jump instruction
0x03	LONGLONG	OEM ID
0x0B	25 bytes	BPB
0x24	48 bytes	Extended BPB
0x54	426 bytes	Bootstrap Code
0x01FE	WORD	End of Sector Marker

Table 1-4 Example of a boot sector on a Windows 2000 NTFS volume.

NTFS (continued)

- NTFS Master File Table (MFT)
  - Stores information regarding file attributes
- When the number of files on an NTFS volume increases, the size of the MFT increases
- Utilities that defragment NTFS volumes on Windows systems cannot move MFT entries
  - NTFS reserves space for the MFT to maintain it as it expands

NTFS (continued)

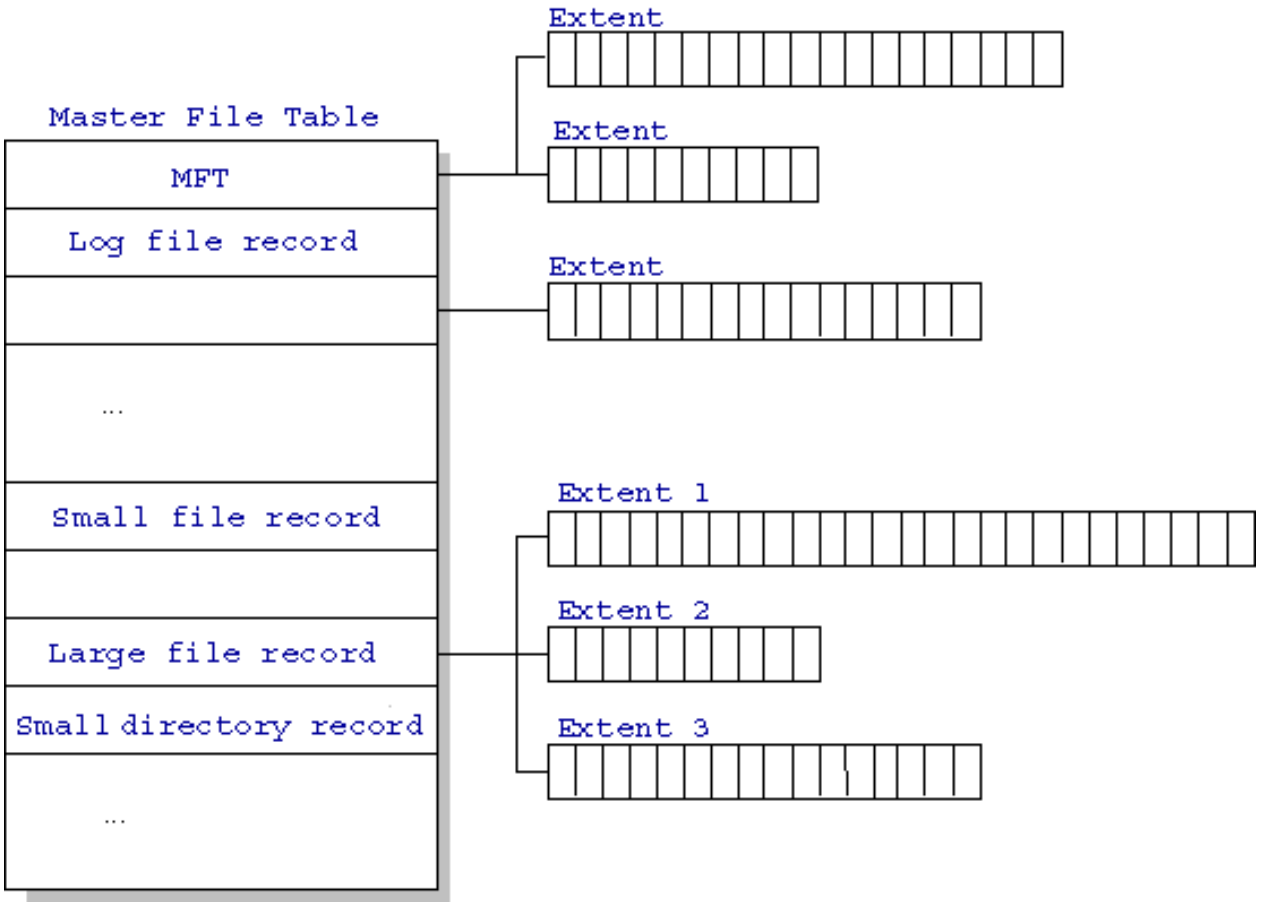


Figure 1-9 Structure of a master file table on an NTFS volume.

NTFS (continued)

- NTFS Metadata File Table (MFT)
  - Relational database that consists of information regarding the files and file attributes on an NTFS volume
  - Defines volume and retrieves information about every file and directory present on it
  - Maintains a record if a new file or a directory is created on an NTFS volume
- MFT stores information regarding files in the form of attributes
  - Rows consist of file records, and columns consist of file attributes

NTFS (continued)

Attribute Type	Purpose of the Attribute
Standard information	This lists the information regarding the time stamp data and link count information.
Attribute list	This is the list of attributes that are in the MFT. It also has a list of non-resident attributes.
File name	The file name is stored here and can be a long or short name. It stores up to 255 bytes.
Security descriptor	Ownership and access rights to the file are listed here.
Data	File data is stored here, and multiple data attributes are allowed for each file.
Object ID	The unique identifier that identifies the volume is listed here.
Logged tool stream	This attribute is used by the encrypted file system service that is used in Windows 2000 and Windows XP.
Reparse point	This lists volume mount points for installable file system filter drivers.
Index root	This is for the use of folders and files.
Index allocation	This is for the use of folders and files.
Bitmap	This is for the use of folders and files.
Volume information	This is where the version number of the volume is listed.
Volume name	The volume label is listed here.

Table 1-5 The different types of file attributes.

NTFS (continued)

- NTFS data streams
  - Data stream: unique set of file attributes
  - Can be created in an existing file on an NTFS volume
  - Only way to see if a data stream is attached to a file is by examining the MFT entry for the file
- NTFS compressed files
  - Capable of compressing individual files, all the files within a folder, and all the files within an NTFS volume
  - Compression is executed within NTFS
  - When a compressed file is opened, only a part of the file is decompressed when being read

NTFS (continued)

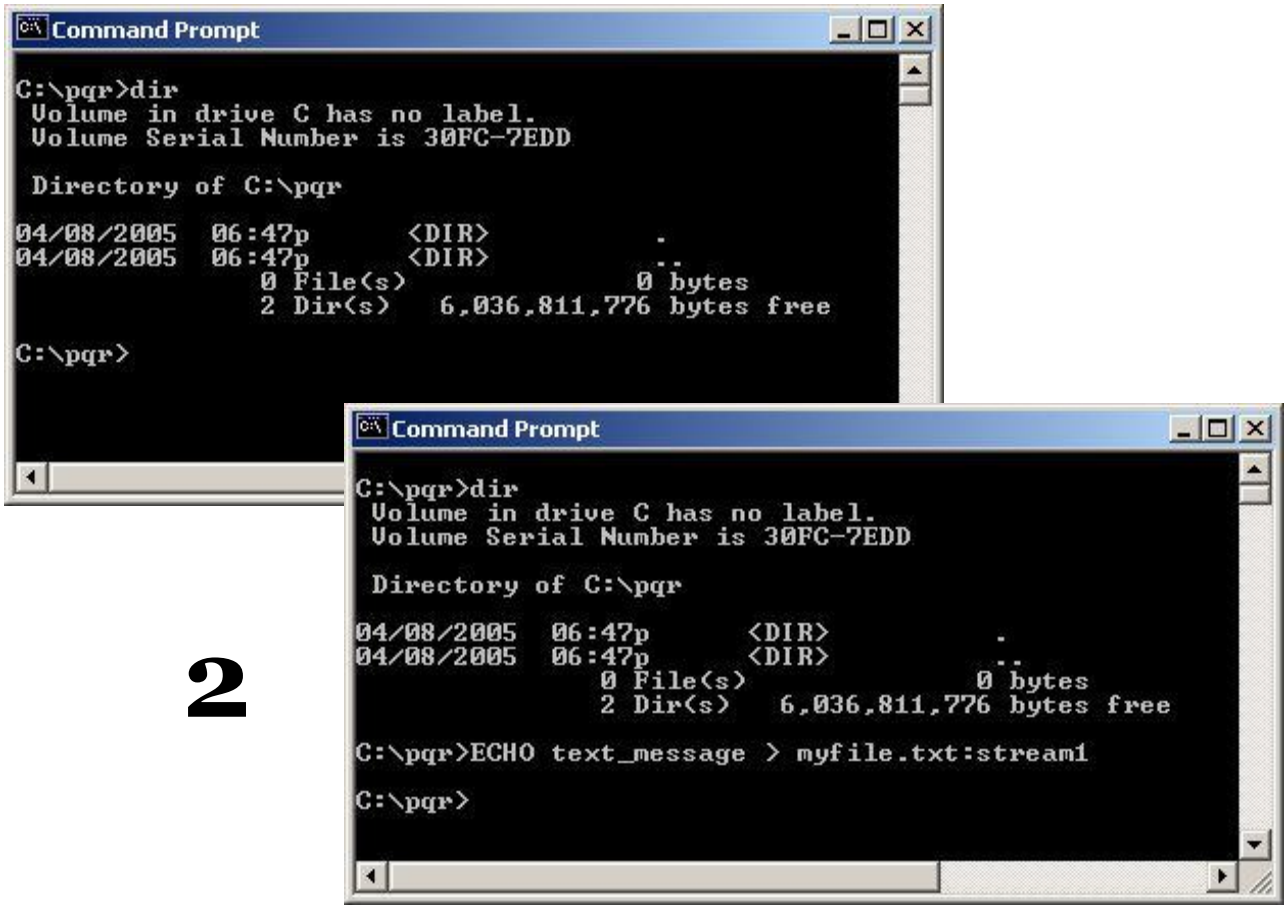
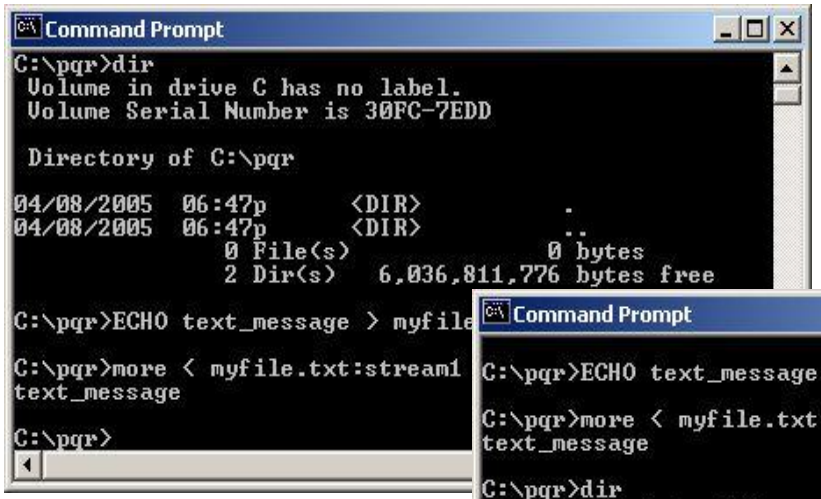


Figure 1-10 A user can create and examine data streams using the command line.

NTFS (continued)

3



4

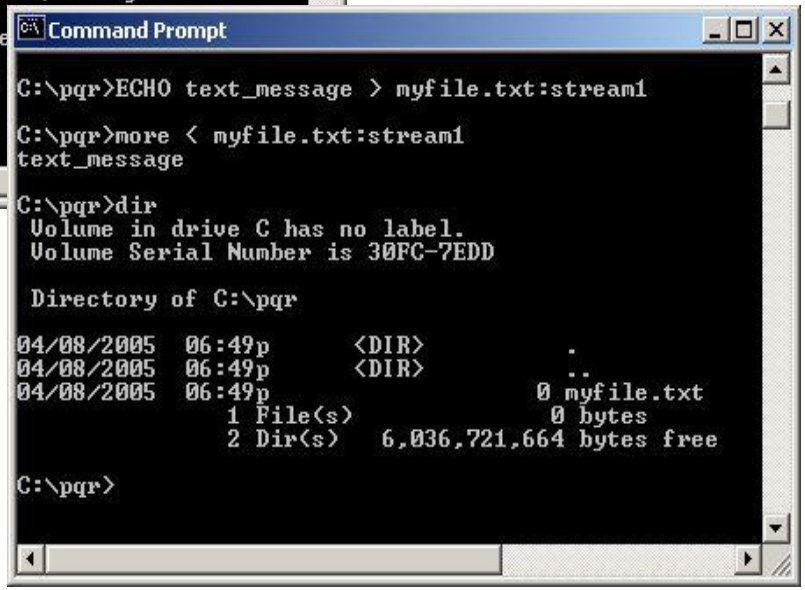


Figure 1-10 A user can create and examine data streams using the command line. (continued)

NTFS (continued)

- NTFS Encrypting File System (EFS)
  - Uses symmetric key encryption technology with public key technology for encryption
  - User is supplied with a digital certificate with a public key pair
  - Encryption technology maintains a level of transparency to the user who encrypted the file
  - User has to set the encryption attributes of the files and folders to encrypt or decrypt
  - All the files and subfolders in a folder are automatically encrypted

NTFS (continued)

- Encryption is done using the graphical user interface (GUI) in Windows
  - But a file or a folder can also be encrypted using a command line tool like Cipher
- A file encryption certificate is issued whenever a file is encrypted
  - Data recovery is performed through the recovery key agent
  - In a Windows 2000 server-based network using Active Directory, the recovery agent is assigned by default to the domain administrator

NTFS (continued)

- EFS Recovery Key Agent
  - To perform a recovery operation
    - Recovery certificate is restored and associated with the private key in the agent's personal store: uses the Import command in the Certificates snap-in
    - After the data is recovered, it is deleted from the recovery certificate in the agent's personal store
- Tools for recovering a lost key or encrypted data include:
  - CIPHER
  - COPY
  - *EFSRECVR*

NTFS (continued)

- Deleting NTFS Files (steps)
  - Windows changes the name of the file and moves the file to the Recycle Bin with a unique identity
  - Windows stores the information about the original path and file name in an INFO2 file
    - Controls the Recycle Bin
- If a file is deleted from the command prompt, the file does not go into the Recycle Bin
  - But a part of the file or the complete file can be recovered using forensic tools

NTFS (continued)

- Steps for deleting a file at the command prompt or from the Recycle Bin:
  - Clusters are made available for new data
  - MFT attribute $BITMAP is updated
  - File attributes of MFT are marked as available
  - Any connections to the inodes and VFN/LCN cluster locations are removed
  - List of links to the cluster locations is deleted

CD-ROM/DVD File Systems

- ISO 9660
  - Defines a file system for CD-ROM/DVD media
  - Supports different computer operating systems
- ISO 9660 Specifications
  - Reserved area of 32,768 bytes at the beginning of the disk
    - Often used for boot information on bootable CD-ROMs
  - Volume Descriptors
    - Details contents and kind of information contained on the disk
    - Primary volume descriptor acts much like the superblock of the UNIX file system

CD-ROM/DVD File Systems (continued)

- ISO 9660 Specifications (continued)
  - Volume Descriptors (continued)
    - First field in a volume descriptor: volume descriptor type (type)
    - Second field: called the standard identifier
    - Another interesting field: volume space size
    - File attributes are very simple in ISO 9660 (see Figure 1-11)
    - Two ways to locate a file on an ISO 9660 file system:
      - Interpret the directory names; look through each directory's file structure to find the file
      - Use a precompiled table of paths

CD-ROM/DVD File Systems (continued)

- ISO 9660 Specifications (continued)
  - ISO 9660 Extensions
    - Rock Ridge Interchange Protocol allows for longer file names (up to 255 characters) in which any ASCII character can be used
    - El Torito is an extension that allows machines to boot from a CD-ROM
- ISO/IEC 13490
  - Next version of ISO 9660 (level 3)
  - Intended to describe file system of a CD-ROM

Comparison of File Systems

File system:	NTFS	FAT32	Mac OS X UFS	HFS+	ext2	ext3	ReiserFS	XFS	JFS	FFS	Be File System
Creator	Microsoft, Gary Kimura, Tom Miller	Microsoft	Apple	Apple	R Card	Stephen Tweedie	Namesys	SGI	IBM	Marshall McKusick	Be Inc., D. Giampaolo, C. Meurillon
Original operating system	Windows NT	Windows 95[10]	Mac OS X	Mac OS	Linux	Linux	Linux	IRIX	AIX[11]	BSD	BeOS
Limits											
Maximum filename length	255 bytes	255 bytes	?	255 characters[1]	255 bytes	255 bytes	4032 bytes/255 characters	255 bytes	?	?	?
Allowable filename characters	Space plus any printable except \ / : ? * " > < |	Space plus any printable except \ / : ? * " > < |	Any Non-null except /	Any Unicode[2] except :	Any Non-null except /	Any Non-null except /	Any Non-null except /	Any Non-null except /	?	Any Non-null except /	?
Maximum pathname length	32767 bytes	at least 260 bytes	?	?	No limit defined[3]	No limit defined[3]	?	?	?	?	?
Maximum file size	16EB	4GB	?	8EB	16GB to 2TB[4]	16GB to 2TB[4]	8TB[8]	9EB[9]	8EB	8TB	?
Maximum volume size	16EB	2-8TB[4,7]	?	?	2TB to 32TB[4]	2TB to 32TB[4]	16TB	9EB[9]	512TB to 4PB[4]	?	?
Features											
File type metadata	None (file extensions)	None (file extensions)	rich (type and creator)	rich (type and creator)	None (file extensions or magic numbers)	None (file extensions or magic numbers)	?	rich (extended attributes)	?	None (file extensions)	rich
Stores file owner	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
POSIX file permissions	No[5]	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Access control lists	Yes	No	No	No	No[6]	No[6]	No[6]	No[6]	No[6]	No	No
Hard links	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Soft links	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Alternate data stream / resource fork	Yes	No	No	Yes	No	No	No	No	No	No	No
Journaling	Yes	No	No	Yes	No	Yes	Yes	Yes	Yes	No	Yes
File system:	NTFS	FAT32	Mac OS X UFS	HFS+	ext2	ext3	ReiserFS	XFS	JFS	FFS	Be File System

Registry Data

- Registry contains a set of predefined keys:
  - *HKEY_CURRENT_USER*
  - *HKEY_USERS*
  - *HKEY_LOCAL_MACHINE*
  - *HKEY_CLASSES_ROOT*
  - *HKEY_CURRENT_CONFIG*

Examining Registry Data

- Registry hive
  - Set of keys, subkeys, and values in the Windows registry
- Registry: group of supporting files that contain backups of its data
- User can examine the registry manually using the Registry Editor
  - Two versions for Windows: REGEDIT (16-bit) and REGEDIT32 (32-bit)

Examining Registry Data (continued)

- Other Registry tools
  - Registry Monitor
  - Registry Checker

Summary

- A hard disk is a sealed unit containing a number of platters in a stack
- A file system is a set of data types that is employed for storage, hierarchical categorization, management, navigation, access, and recovery of data
- A registry is a hierarchical database
- Every disk has master boot record that contains information about partitions on the disk
- EFS is the main file encryption technology used to store encrypted files in NTFS

Summary (continued)

- MFT is a relational database that consists of information regarding files and file attributes
- Windows continuously refers to the registry for information during the execution of applications