Computer Forensics Investigating File and Operating Systems Wireless Networks and Storage CHFI 2nd edition EC-Council Solutions Manual

SKU: 9781305883482-SOLUTIONS

Computer Forensics Investigating File and Operating Systems Wireless Networks and Storage CHFI 2nd edition EC-Council S

CHFI-Bk2_Ch01-Review Question Answers

1. **Explain the difference between fixed and removable disk drives, and give at least one example of each.**
   Fixed drives are drives like hard disks, which use media that are not removable.
   Example: Computer internal hard drive
   Removable drives are drives that use media that are removable.
   Example: USB Flash Drive

2. **Explain zoned bit recording.**
   Zoned bit recording is a technique where tracks are combined together into zones depending on their distance from the center of the disk. Each zone is assigned a number of sectors per track.

3. **Explain types of hard disk interfaces.**
   - *Small computer system interface (SCSI):* Allows a user to connect 15 peripheral devices to one PCI board known as a SCSI host adapter, which is plugged into the motherboard.
   - *Integrated drive electronics/enhanced IDE (IDE/EIDE):* Connects hard disk drives, optical disc drives, and tape drives to personal computers. With this type of interface, the drive controller is built into the drive itself.
   - *Universal Serial Bus (USB):* Connects peripheral devices such as hard disks, modems, printers, digitizers, and data gloves to a computer.
   - *Advanced technology attachment (ATA):* This type of interface comes in two forms:
     - *Serial ATA:* This provides a point-to-point channel between the motherboard and the drive.
     - *Parallel ATA:* This provides a communications channel between the drive and the computer on which data can travel only one way at a time.
   - *Fiber Channel:* A point-to-point bidirectional serial interface that supports up to 1.0625 Gbps transfer rates. This interface comes in two forms:
     - *Fiber Channel electrical interface:* This uses ECL (emitter-coupled logic) signaling levels over an unbalanced 75 W or balanced 150 W line.
     - *Fiber Channel optical interface:* This uses a long-wave laser light source that can carry data at 1 Gbps over a distance of up to 10 km. It uses a long-wave laser (LL), a short-wave laser (SL), and a light-emitting diode (LED).
       - LL: long-wave laser (1300 nm)
       - SL: short-wave laser (780 nm)
       - LED: light-emitting diode (1300 nm)

4. **Explain the difference between serial ATA and parallel ATA.**
   Serial ATA (SATA) offers a point-to-point channel between the motherboard and the drive.

Computer Forensics Investigating File and Operating Systems Wireless Networks and Storage CHFI 2nd edition EC-Council S

Parallel ATA (PATA) provides a controller on the disk drive itself and thereby eliminates the need for a separate adapter card.

5. **Describe the composition of a hard disk platter.**
   Disk platters are the round, flat, magnetic metal or ceramic disks in a hard disk that hold the actual data. They are made of two components: a substrate material and a magnetic media coating.

6. **List and describe the file systems most commonly used on Linux.**
   The ext2 file system is the standard file system that is used on the Linux operating system. The major disadvantage of using this file system is that it is not a journaling file system. This file system was introduced to solve problems like separate access, inode modification, and modification time stamps.

7. **Explain the Master File Table (MFT) and its contents.**
   The MFT is the first file on an NTFS volume and contains information about all the files and folders on the volume. The first information is about the partition boot sector, which starts at sector zero and can be up to 16 sectors long. NTFS has several versions:

8. **Describe the function of the EFS recovery key agent.**
   If there is a need to perform a recovery operation, the recovery certificate is first restored and associated with the private key in the agent's personal store by using the **Import** command in the Certificates snap-in.

9. **Explain what a partition is, including the different types of partitions.**
   Partitioning is the creation of logical drives on a disk. A partition is a logical drive that holds data.
   A partition can be one of two types:
   - *Primary partition:* This type of partition holds information regarding the operating system and system area, as well as other information required for booting.
   - *Extended partition:* This partition holds the data and files that are stored on the disk.

10. **List and describe the different tools used to examine the registry.**
    A user can examine the registry manually using the Registry Editor. There are two versions for Windows: REGEDIT (16-bit) and REGEDIT32 (32-bit). REGEDIT32 and REGEDIT are installed by default on a Windows computer.
    - Registry Monitor is a program that can be used to monitor changes to the registry as they occur.
    - Registry Checker is a part of the Windows 98 operating system. This program can be used to:
      - Backup and restore the registry.
      - Scan and fix various errors in the registry.
      - Optimize the space that is unused in the registry.

Computer Forensics Investigating File and Operating Systems Wireless Networks and Storage CHFI 2nd edition EC-Council S

Chapter 1

Understanding File Systems and Hard Disks

At a Glance

Instructor's Manual Table of Contents

- Overview
- Objectives
- Teaching Tips
- Additional Resources
- Key Terms

© Cengage Learning 2017

Computer Forensics Investigating File and Operating Systems Wireless Networks and Storage CHFI 2nd edition EC-Council S

Lecture Notes

Overview

Chapter 1 provides an introduction to storage media and file systems. An extensive presentation examines disk drives, hard disks, and the many possible attributes. The chapter moves into file systems for various types of media and various operating systems.

Chapter 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
- Understand the Sun Solaris 10 file system ZFS
- Understand the Mac OS X file system
- Understand the UFS (Unix File System)
- Understand the various Windows file systems, including FAT and NTFS
- Understand the EFS recovery key agent
- Understand CD-ROM and DVD file systems
- Examine registry data
- Enumerate Windows XP system files

Teaching Tips

Introduction to File Systems and Hard Disks

1. Note that the chapter will cover file systems and disc drives, particularly hard disks.

Disk Drive Overview

1. Give a brief description of a disk drive and point out that different types of disk drives use different types of disks.

Types of Disk Drives

1. Describe the different types of disk drives:
    a. Fixed: drives like hard disks with media that are not removable.

© Cengage Learning 2017

Computer Forensics Investigating File and Operating Systems Wireless Networks and Storage CHFI 2nd edition EC-Council S

b. Removable: use media that are removable. Examples:
    i. Floppy disk: the drive uses portable magnetic disks on which data and programs can be stored. Floppy disks are disks that are made of either flexible or rigid plastic material.
    ii. CD-ROM: uses optical discs that are sturdier than floppy disks, and can hold more data. Lasers are used to write data to the disc and read data from it.
    iii. DVD: an optical disc that holds far more information than a CD-ROM.
    iv. Zip disk: used to back up disks and larger documents.

Hard Disks

1. Highlight elements of hard disk operation.
    a. Data is organized on a hard disk similar to that of a filing cabinet.
    b. A user can easily access the data and programs.
    c. When a computer uses a program or data, the program or data is copied from its location to a temporary location.
    d. When a user makes changes to a file, the computer saves the file by replacing the older file with the new file.
    e. Data is recorded magnetically onto a hard disk.
    f. A rapidly spinning platter is used as the recording medium.
    g. Heads just above the surface of the platter are used to read data from and write data to the platter.
    h. A standard interface connects a hard disk to a computer.

Characteristics

1. Some characteristics used to differentiate kinds of hard disks:
    a. Capacity of the hard disk.
    b. Interface used.
    c. Speed in rotations per minute.
    d. Seek time.
    e. Access time.
    f. Transfer time.

Physical Makeup

1. Explain the physical aspects of a hard disk.
    a. It is a sealed unit containing platters in a stack.
    b. It can be mounted in a horizontal or vertical position.
    c. Electromagnetic read/write heads are positioned above and below each platter.
    d. As the platters spin, the drive heads move in toward the center surface and out toward the edge. In this way, the drive heads reach the entire surface of every platter.

© Cengage Learning 2017

Computer Forensics Investigating File and Operating Systems Wireless Networks and Storage CHFI 2nd edition EC-Council S

e. Data is stored in thin, concentric bands, called tracks. On a 3.5-inch hard disk, there could be a thousand tracks.
f. Tracks consist of sectors, the smallest physical storage units on a hard disk. A sector is almost always 512 bytes (0.5 kilobyte) in size.

Zoned Bit Recording

1. Explain zoned bit recording. Tracks are combined together into zones depending on their distance from the center of the disk. Each zone is assigned a number of sectors per track.
2. Note the three types of data densities on a hard disk:
    a. Track density: Space between tracks on a disk.
    b. Area density: Number of bits per square inch on a platter.
    c. Bit density: The bits per unit length of track.

Hard Disk Interfaces

1. Discuss types of hard disk interfaces:
    a. SCSI: Allows a user to connect 15 peripheral devices to one PCI board known as a SCSI host adapter, which is plugged into the motherboard.
    b. IDE/EIDE: Connects hard disk drives, optical disc drives, and tape drives to personal computers. The drive controller is built into the drive itself.
    c. USB: Connects peripheral devices such as hard disks, modems, printers, digitizers, and data gloves.
    d. ATA: comes in two forms:
        i. Serial: point-to-point channel between the motherboard and the drive.
        ii. Parallel: a communications channel between the drive and the computer on which data can travel only one way at a time.
    e. Fiber Channel: A point-to-point bidirectional serial interface that supports up to 1.0625 Gbps transfer rates. This interface comes in two forms:
        i. Fiber Channel electrical interface: uses ECL signaling levels over an unbalanced 75 W or balanced 150 W line.
        ii. Fiber Channel optical interface: uses a long-wave laser light source that can carry data at 1 Gbps over a distance of up to 10 km. It uses a long-wave laser (LL), a short-wave laser (SL), and a light-emitting diode (LED).
    f. LL: long-wave laser (1300 nm)
    g. SL: short-wave laser (780 nm)
    h. LED: light-emitting diode (1300 nm)
2. Note that most contemporary personal systems use SATA. IDE is expensive and has been completely superseded by SATA. SCSI is almost obsolete, but an understanding of each system is necessary for the forensic investigator.
3. SCSI is a set of ANSI standard electronic interfaces used for communication between computers and peripheral devices such as hard drives, CD-ROM drives, and scanners. The SCSIs currently in use are parallel interfaces. SCSI devices are supported by all

© Cengage Learning 2017

Computer Forensics Investigating File and Operating Systems Wireless Networks and Storage CHFI 2nd edition EC-Council S

major operating systems, including Linux, Mac OS, and Windows. SCSI is also very versatile; a user can attach up to 7 or 15 devices to a single SCSI port in a chain.

4. IDE is a standard electronic interface used between a computer motherboard's data paths or bus and the computer's disk storage devices. Most computers sold today use either an enhanced version of IDE, EIDE, or SATA. In today's computers, the IDE and SATA controllers are often built into the motherboard. The DupliDisk PCI card provides fault tolerance for IDE drives.
5. USB, developed by Intel, was first released in 1995 with a maximum speed of 12 Mbps. Currently available USB supports data transfer speeds up to 480 Mbps. USB allows external peripheral devices like disks, modems, printers, digitizers, and data gloves to connect to a computer. Some features of USB are:
    a. Ease of use.
    b. Expandability.
    c. Speed for the end user.
    d. High performance and ubiquity.
    e. Easy connection of peripherals outside the PC.
    f. Automatic configuration of devices by most operating systems.
    g. Usefulness in PC telephony and videoconferencing.
6. There are two different types of ATA interfaces: SATA and PATA:
    a. SATA offers a point-to-point channel between the motherboard and the drive. SATA cables are shorter than PATA cables with a maximum length of one meter. The cables consist of four wires and are shielded. SATA connectors are smaller in size when compared to PATA connectors. Features of SATA:
        i. Fast operating speed.
        ii. Upgradeable storage devices.
        iii. Ease of configuration.
        iv. Original transfer speeds of 1.5Gbits/second, with newer systems supporting 3 Gbits/second and 6 Gbits/second of transfer speed.
        v. Low cost when compared to other systems.
    b. PATA provides a controller on the disk drive itself and thereby eliminates the need for a separate adapter card. Features of PATA:
        i. Low relative cost.
        ii. Ease of configuration.
        iii. Look-ahead caching.
7. Fiber Channel is a point-to-point bidirectional serial interface that supports up to 1.0625 Gbps transfer rates. ANSI developed this interface. Features of Fiber Channel:
    a. Low costs.
    b. Support of higher data transfer rates between workstations, mainframes, supercomputers, desktop computers, storage devices, displays, and other peripherals.
    c. Multiple protocols supported:
        i. SCSI
        ii. IP
        iii. ATM
        iv. HIPPI
        v. IEEE 802.2

© Cengage Learning 2017

Computer Forensics Investigating File and Operating Systems Wireless Networks and Storage CHFI 2nd edition EC-Council S

Disk Platters

1. Describe the physical characteristics and operations of disk platters, the round, flat, magnetic metal or ceramic disks in a hard disk that hold the actual data. They are made of a substrate material and a magnetic media coating.
    a. The substrate material gives the platter structure and rigidity. To lower the chance of an uneven surface, manufacturers now use glass, glass composites, and magnesium alloys.
    b. Platters are coated with magnetic media that holds the magnetic impulses that represent the data. Usually the coating is iron oxide or a cobalt alloy. Techniques used to deposit the media material on the platters are electroplating, in which the material is deposited on the platters using electrolysis, or vapor deposition, in which a very thin magnetic layer is deposited on the surface using sputtering. Vapor deposition provides a more uniform coating and thus results in a flatter surface than electroplating does.
2. The amount of data that can be stored on a given amount of a hard disk platter is called area density, also known as bit density.
3. Platter Organization: Each platter has two read/write heads, one on the top of the platter and one on the bottom, so a hard disk with five platters has ten surfaces and ten total heads. Platters are further divided into tracks. Tracks are concentric circles that logically partition platters. Tracks are divided into smaller pieces called sectors. Each sector holds 512 bytes of information.
4. Platter Size, also known as a drive's form factor, closely approximates the hard disk size.
5. Number of Platters: may vary from one to dozens. As the number of platters increases, storage capacity rises, but the space between each platter becomes smaller. This makes hard disks with a large number of platters more sensitive to vibrations, flaws in the surface of a platter, and head misalignment. Therefore, the trend is to increase the area density of a hard drive and thus require a smaller number of platters.
6. Tracks are the concentric circles on platters where all the information is stored. A modern hard disk contains tens of thousands of tracks on each platter. Every platter in a hard disk has the same track density. The track density refers to the compactness of the track circles. Manufacturers try to increase track density so that the maximum number of bits can be placed within each unit area on the surface of a platter.
7. Tracks Numbering: typically tracks are numbered from 0 at the outer edge to 1023 at the center. The read/write heads on both surfaces of a platter are tightly packed and locked together on an assembly of head arms. The arms move in and out together so that all heads remain physically located at the same track number. Therefore, a track location is often referred to by a cylinder number rather than a track number. A cylinder is the set of tracks that can be accessed by all the heads when the heads are in a particular position. One cylinder represents a set of tracks on all the platters in a hard disk.
8. Sectors: a subsection of a track. A sector is the basic physical unit of hard drive data storage. Each sector holds 512 bytes of data and some additional bytes used for internal drive control, drive management, error detection and correction, and sector identification. The contents of a sector are:

© Cengage Learning 2017

Computer Forensics Investigating File and Operating Systems Wireless Networks and Storage CHFI 2nd edition EC-Council S

a. ID information: the sector number and location. It also contains status information about the sector.
b. Synchronization fields: helps the drive controller guide the read process.
c. Data: the actual data in the sector.
d. ECC: an error-correcting code that ensures data integrity.
e. Gaps: spaces are provided to give the drive controller time to continue the read process.

9. Sector Organization and Overhead: the contents of a sector that do not contain user data. This overhead must be minimized for greater efficiency. Data is stored on a disk in a contiguous series of sectors. For example, a 900-byte file is stored in two 512-byte sectors. The track number and the sector number can be used to refer to the address of any data on a hard disk.
10. Bad sectors: areas of a disk that have become unusable. Bad sectors can be caused by configuration problems or physical disturbances. Some common causes are excessive read/write operations, sudden voltage surges, certain viruses, and corrupted boot records.
    a. Defect mapping: once a bad sector is identified, it is marked as bad and cannot be used again.
    b. Spare sectoring: Modern hard disks contain reserved sectors that are used in place of bad sectors. When the drive controller receives a read or write command for a bad sector, it substitutes one of the sectors from the pool of reserves.
11. Clusters: the smallest logical storage units on a hard disk. A file is allocated a certain number of clusters.
    a. Cluster Organization: cluster entries are maintained by the file system running on the computer. Clusters are chained to each other and are ordered on a disk using continuous numbers, so an entire file does not have to be stored in one continuous block on the disk. Cluster chaining is invisible to the operating system.
    b. Cluster Size: determined when the disk volume is partitioned. Larger volumes use larger cluster sizes. For hard disk volumes, each cluster ranges in size from 4 sectors (2,048 bytes) to 64 sectors (32,768 bytes). In some situations, 128-sector clusters may be used (65,536 bytes per cluster).
    c. Slack Space: the area of a disk cluster between the end of the file and the end of the cluster.
    d. Lost Clusters: mainly the result of a logical structure error and not a physical disk error. They usually occur because of interrupted file activities; thus, the clusters involved never get correctly linked to a file. Operating systems mark these clusters as being used in the FAT, even though they are not assigned to any file.
    e. Disk-checking programs, such as ScanDisk, can find lost clusters using the following procedure:
        i. Create a memory copy of the FAT, noting all of the clusters marked as being in use.
        ii. Trace the clusters starting from the root directory, and mark each cluster used by a file as being accounted for. Continue through all of the directories on the disk.

© Cengage Learning 2017

Computer Forensics Investigating File and Operating Systems Wireless Networks and Storage CHFI 2nd edition EC-Council S

iii. When the scanning process is finished, any clusters that are in use but not accounted for are orphans, or lost clusters.

Disk Partition

1. Define partitioning and partitions.
2. Note that a partition can be one of two types:
    a. Primary partition: holds information regarding the operating system and system area, as well as other information required for booting.
    b. Extended partition: holds data and files stored on the disk.
3. Hidden partitions: created from the unused space between the primary partition and the first logical partition in the space known as the interpartition gap.
4. Partition tools:
    a. Data hidden in the interpartition gap can be located using disk editor utilities like Norton Disk Edit.
    b. Tools used to examine disk partitions include Disk Edit, WinHex, and Hex Workshop.

Teaching Tip	Recommended reasons to create partitions: 1. In case of system, data is less like to be affected. 2. Multiple operating systems can be installed on a single PC. 3. Improved performance. 4. Organizing data is easier.

Master Boot Record

1. Remind students that the MBR is the first sector of a data storage device such as a hard disk. It also is known as the partition sector or the master partition table.
2. The MBR contains a table about each partition that the hard disk has been formatted into. It also holds the program that reads the boot sector record containing the operating system into RAM.
    a. Boot sector: the sector of a storage device that contains the code for bootstrapping a system.
    b. Bootstrapping: the process by which a small program actually initializes the operating system installed on a computer.
    c. Information about the files present on the disk, their location, and their size is contained in the master boot record file.

Hard Disk Tools

© Cengage Learning 2017

Computer Forensics Investigating File and Operating Systems Wireless Networks and Storage CHFI 2nd edition EC-Council S

1. Emphasize that there are many tools available for analyzing and recovering data on hard disks. These tools allow investigators to:
    a. Search the text on hard disks in file space, slack space, and unallocated space.
    b. Find and recover data from files that have been deleted.
    c. Find data in encrypted files.
    d. Repair FATs, partition tables, and boot records.
    e. Concatenate and split files.
    f. Analyze and compare files.
    g. Clone hard disks.
    h. Make drive images and backups.
    i. Erase confidential files securely.
    j. Edit files using a hex editor.

Understanding File Systems

1. Introduce file systems: a type of system that is used to most effectively store, organize, and access data on a computer. Data storage devices like hard disks, CD-ROMs, flash memory devices, and floppy disks use file systems to store data.
2. A file system provides the following:
    a. Storage
    b. Hierarchical categorization
    c. Management
    d. Navigation
    e. Access
    f. Data recovery features
3. File systems are organized in the form of tree-structured directories. Directories generally require access authorization.

Types of File Systems

1. Discuss the four categories of file systems:
    a. Disk file system: used for storing and recovering the files on a storage device that is directly or indirectly connected to a computer. Examples: FAT16, FAT32, NTFS, ext2, ISO 9660, ODS-5, and UDF.
    b. Network file system: a file system that provides access to files on other computers on a network. The file system is transparent to the user. Examples: NFS, CIFS, and GFS.
    c. Database file system: files are identified by their characteristics, such as name, type, topic, and author of the file, or similar metadata. Therefore, a file can be easily searched using SQL queries or text searches.
    d. Special purpose file system: a system where the files are organized by software during runtime. This type of file system is used for various purposes, such as communication between computer processes or temporary file space.

© Cengage Learning 2017

Computer Forensics Investigating File and Operating Systems Wireless Networks and Storage CHFI 2nd edition EC-Council S

2. The student text lists 31 different file systems and their characteristics (Table 1-2), nine network file systems (Table 1-3), and nine special purpose systems are presented (Table 1-4).

Popular Linux File Systems

1. Note that the Linux operating system is a single hierarchical tree structure that represents the file system as one single entity. Some of the Linux file system types are Minix, ISO 9660, UMSDOS, NFS, SMB, HPFS. Minix was Linux's first file system. Details of some of the more popular file systems used with Linux:
    a. Ext: released in April 1992, as an elaborate extension of Minix. It has a maximum partition size of 2 GB and a maximum file name size of 255 characters. The ext file system removes the two major Minix limitations of a 64 MB partition size and short file names. The major limitation of this file system is that it doesn't support separate access, inode modification, and data modification time stamps. It keeps an unsorted list of free blocks and inodes, and the file system is also fragmented.
    b. ext2: introduced in January 1993 and extends the features of ext. It uses improved algorithms, which greatly enhances its speed, and it maintains additional time stamps. It maintains a special field in the superblock that keeps track of the status of the file system and identifies it as either clean or dirty. A dirty file system will automatically scan itself for errors. The maximum file size in the ext2 file system is 4 TB (1 terabyte is 1,024 gigabytes).
    c. ext3: a journaling version of the ext2 file system and is greatly used with the Linux operating system. It adds a journal, without which the file system is a valid ext2 file system. It can be mounted and used as an ext2 file system, and all the utilities of ext2 can be used on it.

Sun Solaris 10 File System: ZFS

1. ZFS is a dynamic file system in Solaris OS. It is supported by both x86 and SPARC platforms. ZFS fulfills all the needs of a file system for everything from desktops to data centers. It is a self-managing, general-purpose file system.
2. ZFS supports almost unlimited scalability. It supports more storage, more file systems, more snapshots, more directory entries, and more files than can possibly be created in the foreseeable future. Without interrupting any services, it can dynamically grow and shrink the storage pool. Administrators can set quotas for users to limit space consumption and also to reserve space to guarantee future space availability.
3. Features of ZFS:
    a. Copy on write: Files are backed up immediately.
    b. LVM: ZFS integrates logical volume management features into the file system and manages expansion and shrinkage as needed.
    c. Endianness: the way bytes are ordered in a system. This file system is portable between little-endian and big-endian systems.
    d. Checksums: ZFS provides data integrity features to detect and correct data corruption.

© Cengage Learning 2017

Computer Forensics Investigating File and Operating Systems Wireless Networks and Storage CHFI 2nd edition EC-Council S

e. HA Storage1: This supports cluster failover capabilities. If any server in a cluster fails to perform a task due to an interruption, then only one server can write to a shared physical disk.
f. Clones: At low cost, many copies of similar file systems can be made based on a single snapshot.
g. Compression: This removes the small, unused memory chunks and space used by small files so that the space used by files is less than in other file systems.
h. ACLs: The goal of ZFS's ACL implementation is to implement NFSv4 ACLs in a way that is compatible with Solaris.

Mac OS X File Systems

1. HFS is a file system developed by Apple Computer for Mac OS. It was originally designed for use on floppy and hard disks, but it now also works on read-only media, such as CD-ROMs.
2. Five structures make up an HFS volume:
    a. Logical blocks 0 and 1: the boot blocks, which include system startup information.
    b. Logical block 2: contains the MDB. The MDB defines a wide variety of data about the volume itself—for instance, date and time stamps for when the volume was created; the location of other volume structures, such as the volume bitmap; and the size of logical structures, such as allocation blocks.
    c. Logical block 3: the starting block of the volume bitmap, which keeps track of which allocation blocks are in use and which are free..
    d. The extent overflow file: a B*-tree including extra extents that record which allocation blocks are allocated to which files, once the initial three extents in the catalog file are used up.
    e. The catalog file: a B*-tree that holds records for all the files and directories stored in the volume.
3. Unix File System: file system utilized by many UNIX and UNIX-like operating systems. It is derived from the Berkeley Fast File System, which is an abstract of FS, the file system used in the first version of UNIX developed at Bell Labs. UFS is composed of the following:
    a. A few blocks at the beginning of the partition reserved for boot blocks.
    b. A superblock, including a magic number identifying this as a UFS file system, and some other vital numbers describing this file system's geometry, statistics, and behavioral tuning parameters
    c. A collection of cylinder groups, of which each cylinder group has the following components:
        i. Backup copy of the superblock.
        ii. Cylinder group header, with statistics, free lists, and other data about this cylinder group, similar to those in the superblock.
        iii. Number of inodes, each containing file attributes.
        iv. Number of data blocks.

© Cengage Learning 2017

Computer Forensics Investigating File and Operating Systems Wireless Networks and Storage CHFI 2nd edition EC-Council S

Windows and DOS File Systems

Teaching Tip	An important warning about NTFS and FAT: A partition can be reformatted as either FAT or NTFS; however, reformatting a partition erases all files on that partition. Back up all files on the partition before the reformatting.

1. Review the main Windows and DOS file systems:
    a. FAT16: a 16-bit file system developed for DOS and further supported by other operating systems. File names are limited to 8 characters for the name and 3 characters for the extension. Its main shortcomings are that it supports a maximum of 64 KB allocation units and that it becomes less efficient on partitions larger than 32 MB. Due to its limitations, it is not suitable for file servers.
    b. FAT12: a version of FAT specifically designed for floppy disks.
    c. FAT32: a 32-bit version of the FAT file system using smaller clusters, which results in a more efficient storage capacity. It supports drive sizes up to 2 TB. It can relocate the root directory and use the backup copy instead of the default copy. It can dynamically resize a partition.
    d. NTFS: an entirely different file system that provides enhanced security, file-by-file compression, quotas, and encryption. It is designed to quickly perform standard file operations such as read, write, search, and even advanced operations such as file-system recovery on very large hard disks.
2. FAT File Systems: the file system used with DOS, and it was the first file system used with the Windows operating system. Even the most recent versions of Windows still use the 32-bit version of FAT.
    a. Boot Sector: the first sector of a FAT file system. In UNIX, this would be called the superblock.
    b. Display Table 1-5 from the student text and discuss the contents of the boot sector.
    c. File Recovery: When a file is deleted from a FAT volume, the operating system replaces the first letter of the file name with a lowercase Greek letter. The space is then made available for new files. The deleted files can be recovered using forensic tools.
    d. A few tools that can be used for forensics are:
        i. WinHex: Forensic investigators can use the hex editor, disk editor, and RAM editor, along with many other features like concatenating, separating, combining, and evaluating files; agile searching and substitution functions; data interpretation; template editing; encryption; file editing; a highly developed backup mechanism; drive imaging; drive cloning; and printing.

© Cengage Learning 2017

Computer Forensics Investigating File and Operating Systems Wireless Networks and Storage CHFI 2nd edition EC-Council S

ii. Undelete: restores files that cannot be restored using the Recycle Bin. The following are the types of files that can be restored using Undelete:
    1. Shared files on the network.
    2. Previous versions of Office files.
    3. Large files that do not fit in the Recycle Bin.
    4. Certain files that are created and deleted by applications.
    5. Files deleted from the command line.

iii. File Scavenger: retrieves digital photos from most media. Also retrieves files ruined by viruses and files deleted by mistake from Windows Explorer, the Recycle Bin, the DOS command line, or a network share. It can also recover formatted volumes, broken spanned volumes, broken RAID volumes, and disks with bad media areas.

3. NTFS: one of the latest file systems supported by Windows. It is a high--performance file system that repairs itself. It supports several advanced features such as file-level security, compression, and auditing. It also supports large and powerful volume storage solutions such as self-recovering disks. Features of NTFS:
    a. NTFS provides data security, as it has the capability to encrypt or decrypt data, files, or folders.
    b. NTFS uses a 16-bit Unicode character set to name files and folders, which lets users around the world manage files in their native languages.
    c. It is a fault-tolerant file system. NTFS makes a note of modifications in a special log file. If a system crashes, NTFS can examine the log file and use it to restore the disk to a consistent state with minimal data loss.
    d. NTFS volumes contain a Master File Table. This table contains a record for every file and folder on the volume. The first 16 bytes of the table are reserved for metadata used to implement and maintain the file system structure. This metadata is stored in a set of system files.
    e. NTFS Partition Boot Sector: the NTFS format program allocates of each volume the first 16 sectors for the boot sector and the bootstrap code.
    f. NTFS volumes have at least one entry stored in the MFT. Information regarding file attributes like size, time and date stamps, and permissions is saved either with the MFT entries or in memory allocated outside the MFT that is described by MFT entries.
    g. NTFS Attributes: The attributes stored within an MFT record are called resident attributes, and those that lie outside the MFT are nonresident attributes. If the data attributes are small in size, then they can be stored within the MFT without the need for additional storage space on the NTFS volume. But if the attributes do not fit in the MFT, they are moved out of the MFT record as nonresident attributes.
    h. NTFS Data Streams: a data stream is a unique set of file attributes. NTFS supports multiple data streams per file. A data stream does not appear when a file is opened in a text editor; the only way to see if a data stream is attached to a file is by examining the MFT entry for the file.
    i. NTFS Compressed Files: NTFS is capable of compressing individual files, all the files within a folder, and all the files within an NTFS volume. Compression is executed within NTFS, so any Windows-based program can read and write

© Cengage Learning 2017

Computer Forensics Investigating File and Operating Systems Wireless Networks and Storage CHFI 2nd edition EC-Council S

compressed files without considering the extent of compression of the file. NTFS compression algorithms support cluster sizes of up to 4 KB.

j. NTFS EFS: To protect files from mishandling and to ensure their security, the files are encrypted. EFS uses symmetric key encryption technology with public key technology for encryption. The user is supplied with a digital certificate with a public key pair. An EFS key is used for users who are logged in to the local system.

k. EFS Recovery Key Agent: If there is a need to perform a recovery operation, the recovery certificate is first restored and associated with the private key in the agent's personal store by using 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. The recovery agent's certificate is then deleted from the computer.
    i. A Windows administrator can recover a lost key or encrypted data from the command prompt using the following tools, each of which has function-specific syntax:
        1. *CIPHER:* used to make changes to the encryption of directories or files on an NTFS partition.
        2. *COPY:* used to copy one or more files to other locations.
        3. *EFSRECVR:* helps the recovery agent recover encrypted files from the specified location.

l. Deleting NTFS Files: when a file is deleted in Windows Explorer, the file is moved into the Recycle Bin. This allows the user to restore the deleted file at a later time. The operating system takes the following steps when a file is deleted:
    i. Windows changes the name of the file and moves the file to the Recycle Bin with a unique identity.
    ii. Windows stores the information about the original path and file name in an INFO2 file, which controls the Recycle Bin. This file contains ASCII data, Unicode data, and attributes like the date and time of deletion for each and every file or folder.

m. A file deleted from the command prompt does not go into the Recycle Bin, but a part of the file or the complete file can be recovered using forensic tools. When a file is deleted at the command prompt or when a file is deleted from the Recycle Bin, then the following tasks are performed by the operating system:
    i. The clusters are made available for new data.
    ii. The MFT attribute $BITMAP is updated.
    iii. File attributes of the MFT are marked as available.
    iv. Any connections to the inodes and VFN/LCN cluster locations are removed.
    v. The list of links to the cluster locations is deleted.

CD-ROM/DVD File Systems

1. Begin discussion of data storage on CD-ROM/DVDs. Stored data is divided into sectors. These sectors contain both user data and error correction codes.

© Cengage Learning 2017

Computer Forensics Investigating File and Operating Systems Wireless Networks and Storage CHFI 2nd edition EC-Council S

2. ISO 9660 (a standard defined by the International Organization for Standardization) defines a file system for CD-ROM/DVD media. Its aim is to support different computer operating systems, such as Microsoft Windows, Mac OS, and UNIX, to allow for the exchange of data between different operating systems.
    a. ISO 9660 Specifications: There is a reserved area of 32,768 bytes at the beginning of the disk. This area's use is not specified in the ISO 9660 standard, but it is often used for boot information.
    b. Volume Descriptors: Immediately afterward, a series of volume descriptors details the contents and the kind of information contained on the disk. A volume descriptor describes the characteristics of the file system information present. It is divided into two parts: the type of volume descriptor and the characteristics of the descriptor.
    c. File attributes are very simple in ISO 9660. The most important file attribute determines whether the file is a directory or an ordinary file. File attributes for the file described by the directory entry are stored in the directory entry and, optionally, in the extended attribute record.
    d. There are two ways to locate a file on an ISO 9660 file system:
        i. One way is to successively interpret the directory names and look through each directory's file structure to find the file (much the way MS-DOS and UNIX work to find a file).
        ii. The other way is through the use of a precompiled table of paths, where all the entries are enumerated in the successive contents of a file with the corresponding entries.
3. ISO 9660 Extensions: There are common extensions to ISO 9660 to deal with its limitations. The Rock Ridge Interchange Protocol allows for longer file names (up to 255 characters) in which any ASCII character can be used. It also supports deeper directory hierarchies and symbolic links. El Torito is an extension that allows machines to boot from a CD-ROM.
4. ISO/IEC 13490 is the next version of ISO 9660 (level 3), intended to describe the file system of a CD-ROM. ISO 13490 has several improvements over its predecessor:
    a. It fully addresses the file name, POSIX attribute, and multibyte character issues that are not handled by ISO 9660.
    b. It is a more efficient format, and it permits incremental recording and both the ISO 9660 format and ISO/IEC 13490 format to coexist on the same media.
    c. It also specifies how to do multisession recording properly.

Comparison of File Systems

1. Discuss comparisons between file systems, using Table 1-9 in the student text as reference.

Registry Data

1. Review the predefined keys in the window registry:
    a. *HKEY_CURRENT_USER:* abbreviated HKCU. Can be scanned for information about the- configuration of the user currently logged in.

© Cengage Learning 2017

Computer Forensics Investigating File and Operating Systems Wireless Networks and Storage CHFI 2nd edition EC-Council S

b. *HKEY_USERS:* HKEY_CURRENT_USER is a subkey of HKEY_USERS. Can be checked for all the user profiles loaded on the computer.
c. *HKEY_LOCAL_MACHINE:* abbreviated HKLM. Can be searched for the configuration information of a particular computer.
d. *HKEY_CLASSES_ROOT:* a subkey of HKEY_LOCAL_MACHINE\Software. The information stored in this key ensures that the correct program opens when a file is opened in Windows Explorer.
e. *HKEY_CURRENT_CONFIG:* contains data about the hardware profile used by the local computer at start-up.

Examining Registry Data

1. Define registry hive: a set of keys, subkeys, and values in the Windows registry. The registry has a group of supporting files that contain backups of its data.
2. Present the various registry hives and their supporting files in Windows.
3. A user can examine the registry manually using the Registry Editor. There are two versions for Windows: REGEDIT (16-bit) and REGEDIT32 (32-bit). REGEDIT32 and REGEDIT are installed by default on a Windows computer.
4. Note other tools that a user can use to examine or monitor the registry:
    a. Registry Monitor: a program that can be used to monitor changes to the registry as they occur.
    b. Registry Checker: a part of the Windows 98 operating system that can be used to:
        i. Backup and restore the registry.
        ii. Scan and fix various errors in the registry.
        iii. Optimize the space that is unused in the registry.

Bootdisk.com

1. Recommend the Web site www.bootdisk.com, which provides boot disks for DOS, Linux, and Windows operating systems. It also offers drivers and utilities. The site also features tips and guides for maintaining hard disks and file systems.

Additional Resources

1. An extensive discussion of hard disk performance and factors related to input/output per second was published by Symantec:
http://www.symantec.com/connect/articles/getting-hang-iops

2. In the following Technet article, the MBR is called “the most important data structure on the disk.” See more at:
https://technet.microsoft.com/en-us/library/cc976786.aspx

3. Learn more about ZFS in the Oracle Solaris ZFS Administration Guide:
http://docs.oracle.com/cd/E23823_01/html/819-5461/zfsover-2.html#gayou

© Cengage Learning 2017

Computer Forensics Investigating File and Operating Systems Wireless Networks and Storage CHFI 2nd edition EC-Council S

Key Terms

- **Bad sector** an area of a disk that has become unusable
- **Boot sector** the first sector of a data storage device that contains the code for bootstrapping a system
- **Bootstrapping** the process by which a small program actually initializes the operating system installed on a computer
- **Cluster** the smallest logical storage unit on a hard disk
- **Disk drive** a mechanism that reads data from a disk and writes data onto a disk
- **Disk file system** a type of file system used for storing and recovering the files on a storage device, such as a hard disk, that is directly or indirectly connected to a computer
- **Disk platter** a round, flat, magnetic metal or ceramic disk in a hard disk that holds the actual data
- **Endianness** the way bytes are ordered in a system
- **FAT32** a 32-bit version of the FAT file system using smaller clusters, which results in a more efficient storage capacity
- **Floppy disk** a portable magnetic disk with a shell made of either flexible or rigid plastic material
- **IDE (integrated drive electronics)** a type of interface used to connect a disk drive to a computer, in which the controller is built into the drive itself
- **Internal Solid State Drives (SSD)** A newer type of internal drive that stores the data on interconnected flash memory chips that retain the data even when there's no power present, as opposed to the traditional HDD that stores data on magnetic coated metal disks. SSDs have no moving pieces, and use NAND-based flash memory, a non-volatile type of memory.
- **Lost cluster** a FAT file system error that results from how the FAT file system allocates space and chains files together
- **Master boot record (MBR)** the first sector of a data storage device such as a hard disk
- **Network file system** a type of file system that provides access to files on other computers on a network
- **NTFS (New Technology File System)** a type of file system used on Windows operating systems that provides features, such as security and file compression, that FAT does not provide
- **Parallel ATA** a type of interface that offers a connection between a hard drive and a computer, in which communication can only flow in one direction at a time
- **Partitioning** the creation of logical drives on a disk
- **Registry Checker** a part of the Windows 98 operating system that is used to backup and restore the registry and fix errors in the registry
- **Registry Monitor** a program that can be used to monitor changes to the registry as they occur
- **Sector** the basic physical unit of hard drive data storage; a series of predefined sectors form a circle on the hard drive platter called a track
- **Serial ATA** a type of interface that offers a point-to-point connection between a hard drive and a computer, in which communication can flow both ways at the same time
- **Special purpose file system** a file system where the files are organized by software

© Cengage Learning 2017

Computer Forensics Investigating File and Operating Systems Wireless Networks and Storage CHFI 2nd edition EC-Council S

during runtime

- **USB (Universal Serial Bus)** a type of interface used to connect peripherals such as hard drives, modems, printers, scanners, and digitizers to a computer
- **ZFS (Zettabyte File System)** a self-managing, general-purpose file system used in Sun's Solaris 10 operating system

© Cengage Learning 2017

Computer Forensics Investigating File and Operating Systems Wireless Networks and Storage CHFI 2nd edition EC-Council S