UNIT 2

Understanding Hard Disks and File Systems

This topic focuses on the structure, functionality, and examination of hard disks and file systems. Below is a detailed explanation for each subtopic:

---

1. Types of Disk Drives

- **HDD (Hard Disk Drive):** Traditional storage with magnetic platters and mechanical arms. Slower but cheaper and with larger storage capacity.
- **SSD (Solid State Drive):** Modern storage without moving parts. Uses flash memory, offering faster performance and reliability.
- **Hybrid Drives:** Combines SSD speed with HDD capacity.
- **External Drives:** Portable devices for storage and backups, connected via USB or other interfaces.

---

2. Logical Structure of a Disk

- A disk is divided into **sectors**, **clusters**, and **partitions.**
- **Master Boot Record (MBR):** Contains partition table and boot loader for the operating system.
- **Partition Table:** Defines how the disk is segmented for different files and operating systems.
- **File Allocation Table (FAT):** Tracks which areas of the disk store files.

---

3. Booting Process of Windows and Linux

- **Windows Boot Process:**
    1. BIOS/UEFI initializes hardware and loads the bootloader from the MBR.
    2. Bootloader starts the Windows OS by loading ntoskrnl.exe.
    3. Drivers and services are initialized.
- **Linux Boot Process:**
    1. BIOS/UEFI loads the bootloader (GRUB or LILO).
    2. Kernel is loaded and initialized.
    3. init or systemd starts system services.

---

4. File Systems of Windows and Linux

- **Windows File Systems:**
  - **FAT32:** Old system, compatible with most devices, limited file size (4GB max).
  - **NTFS (New Technology File System):** Supports large files, encryption, and permissions.
  - **exFAT:** Designed for flash drives with no size limits.
- **Linux File Systems:**
  - **ext2/ext3/ext4:** Extensible file systems, commonly used in Linux.
  - **XFS and Btrfs:** High-performance systems for servers.
  - **swap:** Used for virtual memory.

---

5. File System Examination Using Autopsy

- **Autopsy:** A digital forensics tool used to analyze disks and recover data.
  - Can extract file system metadata, deleted files, and hidden data.
  - Displays timeline analysis and allows forensics investigators to identify suspicious activity.

---

6. Storage Systems

- **RAID (Redundant Array of Independent Disks):** Combines multiple disks for redundancy or performance:
  - **RAID 0:** Striped disks for performance (no redundancy).
  - **RAID 1:** Mirrored disks for redundancy.
  - **RAID 5/6:** Striped with parity for fault tolerance.
- **NAS (Network Attached Storage):** Dedicated storage accessible over a network.
- **SAN (Storage Area Network):** High-speed network that connects servers to storage devices.

---

7. Encoding Standards and Hex Editors

- **Encoding Standards:** Determines how data is represented in binary.
  - ASCII and Unicode are commonly used for text encoding.
  - UTF-8 is a widely adopted format.
- **Hex Editors:** Tools to view and edit raw binary data on a disk.
  - Useful for analyzing file headers and recovering corrupted files.
  - Shows data in hexadecimal and ASCII format for low-level investigation.

Important MCQ

1. What is the primary function of the Master Boot Record (MBR)?
a) Storing user files
b) Partitioning a disk and bootstrapping the OS
c) Encrypting the file system
d) Managing disk formatting
Answer: b) Partitioning a disk and bootstrapping the OS

2. Which file system supports file sizes larger than 4GB?
a) FAT32
b) NTFS
c) ext2
d) None of the above
Answer: b) NTFS

3. What is the default file system for most modern Linux distributions?
a) FAT32
b) ext4
c) NTFS
d) HFS+
Answer: b) ext4

4. What does RAID stand for?
a) Random Array of Independent Data
b) Redundant Array of Independent Disks
c) Reliable Array for Integrated Disks
d) None of the above
Answer: b) Redundant Array of Independent Disks

5. In RAID 1, data is stored as:
a) Striped across multiple disks
b) Mirrored across multiple disks
c) Parity information on all disks
d) Stored on a single disk only
Answer: b) Mirrored across multiple disks

6. What is the purpose of the swap file system in Linux?
a) To store user files
b) To provide virtual memory
c) To act as a backup for the kernel
d) None of the above
Answer: b) To provide virtual memory

7. Which of the following tools is used to examine file systems in forensic investigations?
a) Autopsy
b) Wireshark
c) Nmap
d) Nessus
Answer: a) Autopsy

8. Which type of disk drive uses magnetic platters for storage?
a) SSD
b) HDD
c) NAS
d) RAID
Answer: b) HDD

9. What is a Hex Editor used for?
a) Formatting a disk
b) Viewing and editing raw binary data
c) Encrypting files
d) Compressing data
Answer: b) Viewing and editing raw binary data

10. What does the GRUB bootloader primarily do in Linux systems?
a) Initialize the BIOS
b) Load the kernel into memory
c) Format the hard disk
d) Encrypt the file system
Answer: b) Load the kernel into memory

11. What is the primary purpose of the file allocation table (FAT)?
a) Managing file encryption
b) Tracking file locations on the disk
c) Monitoring network traffic
d) Organizing directory structures
Answer: b) Tracking file locations on the disk

12. Which file system is specifically optimized for flash storage?
a) NTFS
b) exFAT
c) ext3
d) XFS
Answer: b) exFAT

13. Which RAID level provides fault tolerance through parity but no mirroring?
a) RAID 0
b) RAID 1
c) RAID 5
d) RAID 10
Answer: c) RAID 5

14. What is the main disadvantage of HDD compared to SSD?
a) Higher cost
b) Slower read/write speeds
c) Larger size
d) Noisy operation
Answer: b) Slower read/write speeds

15. What does the term "boot sector" refer to?
a) A section of memory used for virtual storage
b) The portion of the disk that contains OS boot code
c) A reserved area for file metadata
d) None of the above
Answer: b) The portion of the disk that contains OS boot code

16. Which encoding standard is most widely used for text representation?
a) ASCII
b) Hexadecimal
c) Unicode
d) UTF-8
Answer: d) UTF-8

17. What is the main function of a storage area network (SAN)?
a) Store application code
b) Provide shared disk access to multiple servers
c) Back up user files
d) Encrypt all disk data
Answer: b) Provide shared disk access to multiple servers

18. Which file system is commonly used on macOS?
a) NTFS
b) HFS+
c) ext4
d) FAT32
Answer: b) HFS+

19. How does Autopsy assist in file system analysis?
a) Encrypts file systems
b) Provides an interface to recover deleted files
c) Formats drives
d) Monitors network activity
Answer: b) Provides an interface to recover deleted files

20. What does a hex editor display data in?
a) Plain text format
b) Decimal and ASCII
c) Hexadecimal and ASCII
d) Binary and hexadecimal
Answer: c) Hexadecimal and ASCII

21. Which file system does not support journaling?
a) NTFS
b) ext4
c) FAT32
d) XFS
Answer: c) FAT32

22. What happens during the Linux kernel initialization step?
a) Bootloader loads OS drivers
b) Kernel is loaded into memory and hardware is initialized
c) BIOS identifies boot devices
d) None of the above
Answer: b) Kernel is loaded into memory and hardware is initialized

23. What is the purpose of parity in RAID?
a) Increase disk speed
b) Provide fault tolerance by storing recovery data
c) Mirror data on multiple disks
d) Encrypt data stored on disks
Answer: b) Provide fault tolerance by storing recovery data

24. Which tool can examine file system metadata?
a) Autopsy
b) Nessus
c) Wireshark
d) Nmap
Answer: a) Autopsy

25. Which of the following describes RAID 10?
a) Striped and mirrored
b) Mirrored only
c) Striped only
d) Parity only
Answer: a) Striped and mirrored

26. In Windows, which file system supports encryption and large volume sizes?
a) FAT32
b) exFAT
c) NTFS
d) HFS+
Answer: c) NTFS

27. What is the main role of the partition table?
a) Track file locations
b) Define disk partitions
c) Encrypt disk data
d) Manage memory allocation
Answer: b) Define disk partitions

28. Which Linux file system feature supports snapshots?
a) ext2
b) ext4
c) Btrfs
d) FAT32
Answer: c) Btrfs

29. What is the significance of the boot loader?
a) Initializes the BIOS
b) Loads and starts the operating system
c) Organizes the directory structure
d) Manages user authentication
Answer: b) Loads and starts the operating system

30. Which encoding standard is most efficient for international text?
a) ASCII
b) Unicode
c) Hexadecimal
d) Binary
Answer: b) Unicode