# Experiment No .4

**4.1 Aim:** Storage Media and Hardware Devices: Detecting Flash Drive Usage, Removing the Suspect's HDD, Retrieving Data from HDD Labels

**Example Scenario**: A government office suspects that an employee named **Rahul Khanna** secretly copied confidential files using a USB pen drive. After copying, he deleted the files and removed the pen drive, thinking no one would notice.

You are part of the digital forensics team asked to **check the computer**, **see if any USB drives were used**, **remove the hard disk safely**, and **note important information from it**.

## 4.2 Lab Outcome :

- Demonstrate how to detect flash drive usage, remove and handle a suspect's hard drive properly, and document useful information from hardware labels for forensic purposes.

## 4.3Learning Objectives:

- Check if a USB device was connected to a computer in the past.
- Safely remove a hard disk from a desktop or laptop.
- Read and record important details from the hard disk label.
- Understand how these steps help in real-world cybercrime investigations.

## 4.4 Requirement:

**Hardware:**

- Desktop or laptop system (for investigation)
- USB flash drive (for testing)

- Screwdriver kit (for opening the system)
- Anti-static bag or protective box (for storing HDD)

**Software Tools:**

- **USBDeview** (to check USB history)
- **Event Viewer** (optional, for log checking)
- **Notepad or printed log sheet** (to record details)

**Documents/Forms:**

- Chain of Custody Form (optional)
- Evidence Label Sheet (to tag HDD after removal)

## 4.5 Related Theory :

### Magic Numbers:

- The unique hexadecimal pattern at the beginning of a file (e.g., JPEG starts with FF D8 FF, PDF starts with %PDF).
- Used by forensic tools to identify file types, even if extensions are missing or altered.

### Extension Obfuscation:

- Renaming files to hide their actual type (e.g., report.docx renamed as report.txt).
- Attackers use this to trick systems or users.
- File signature analysis can detect this obfuscation.

**Bit and Block Shifting:**

- A data hiding or encryption method that shifts bits or blocks of data.
- Bit-shifting example: Right-shifting every byte by 1 changes the content’s meaning.
- Forensics experts reverse engineer such manipulations to access original content.

**Recovering Deleted Files:**

- When a file is deleted, only the file system’s pointer is removed; data remains until overwritten.
- Tools scan for recoverable clusters.

**File Carving:**

- A **signature-based recovery** method that scans raw disk data for known file headers/footers.
- Useful when file system metadata is missing or corrupted.
- Example: Scalpel or PhotoRec identifies and extracts files using predefined header/footer rules.

## 4.6 Output:

## 4.7 Conclusion: