**Theory part:-**

**Practical 1: Creating a Forensic Image using FTK Imager**

Forensic imaging is the process of making an exact bit-by-bit copy of a storage device, ensuring all data, including deleted files and system artifacts, are preserved for investigation.

**Step-by-Step Explanation**

**Step 1: Launch the FTK Imager Software**

* Open **FTK Imager** on your computer.
* Click on **File** > **Create Disk Image**.
* This step initiates the forensic imaging process.

**Step 2: Choose Physical Drive**

* Select the **Physical Drive** option and click **Next**.
* This ensures the entire physical drive (HDD, SSD, USB) is imaged, not just a partition.

**Step 3: Select the Drive**

* A list of detected drives appears.
* Select the target drive that needs to be imaged.
* Click **Finish** to proceed.

**Step 4: Add Image Type**

* Click on the **Add** button to define the image format.

**Step 5: Select Raw (dd) Format**

* Choose the **Raw (dd)** format.
* Raw format is an uncompressed forensic image format that preserves every bit of data.
* Click **Next** to continue.

**Step 6: Input Case Information**

* Enter relevant case details such as:
  + **Case Number** (Unique ID for case identification)
  + **Examiner Name** (Investigator’s name)
  + **Evidence Number** (Reference number for evidence tracking)
  + **Description** (Any additional details about the case)
* Click **Next**.

**Step 7: Specify Destination**

* Select a **destination folder** where the forensic image will be saved.
* It is recommended to save the image on an external drive to prevent overwriting.

**Step 8: Start Imaging Process**

* Click **Start** to begin the imaging process.
* The progress bar will show the status of the imaging.

**Step 9: Verify Data Integrity**

* Once imaging is complete, FTK Imager will generate a **hash value (MD5/SHA-1)**.
* This hash ensures the forensic image is identical to the original drive.
* If the hash values match, data integrity is verified.

**Step 10: Locate the Image File**

* Go to the destination folder specified in Step 7.
* Confirm the forensic image file is created.

**Step 11: View Image Summary**

* Click the **Summary** button to review details such as:
  + Source drive information
  + Image format
  + Hash values
  + Imaging duration
* This summary is useful for documentation and verification.

**Viva Questions & Answers**

Here are some possible viva questions along with their answers:

**1. What is forensic imaging?**

**Answer:** Forensic imaging is the process of creating an exact bit-by-bit copy of a storage device to preserve digital evidence for investigation without altering the original data.

**2. Why do we create a forensic image instead of working directly on the original disk?**

**Answer:** Working on the original disk can modify or corrupt evidence. A forensic image allows investigators to analyze data while preserving the integrity of the original evidence.

**3. What are the different formats of forensic images?**

**Answer:** Common forensic image formats include:

* **Raw (.dd, .img)** – Uncompressed bit-by-bit copy.
* **E01 (EnCase Evidence File)** – Compressed format with metadata.
* **AFF (Advanced Forensic Format)** – Open-source, compressed format.

**4. What is the importance of hashing in forensic imaging?**

**Answer:** Hashing generates a unique digital fingerprint (MD5/SHA-1) of the data before and after imaging. If the hash values match, it confirms the forensic image is identical to the original drive.

**5. What hashing algorithms are commonly used in digital forensics?**

**Answer:** The commonly used hashing algorithms are:

* **MD5 (Message Digest Algorithm 5)**
* **SHA-1 (Secure Hash Algorithm 1)**
* **SHA-256 (Secure Hash Algorithm 256-bit)**

**6. What is the difference between Logical and Physical Imaging?**

**Answer:**

* **Logical Imaging** captures only active files and folders.
* **Physical Imaging** captures the entire disk, including deleted files and unallocated space.

**7. What is the difference between FTK Imager and EnCase Imager?**

**Answer:**

* **FTK Imager** is lightweight and allows quick previewing of data before imaging.
* **EnCase Imager** supports advanced forensic analysis and the EnCase proprietary format.

**8. What precautions should be taken before forensic imaging?**

**Answer:**

* Use **write blockers** to prevent modification of evidence.
* Verify **storage space** before creating an image.
* Ensure the **source disk is intact and undamaged**.

**9. What is a Write Blocker, and why is it used?**

**Answer:** A write blocker is a device that prevents any modifications to the original evidence while allowing read access.

**10. What happens if the hash values don’t match after imaging?**

**Answer:** If the hash values do not match, it indicates that the forensic image is different from the original, meaning data might have been altered or corrupted.

**Conclusion**

This practical ensures that forensic investigators can create a **forensic image** while maintaining **data integrity**

👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌

**Practical 2: Perform Data Acquisition using USB Write Blocker + FTK Imager**

**✅ Aim:**

To perform data acquisition from a USB device using **software-based write protection** via **Registry Editor** and then image the USB using **FTK Imager**.

**⚙️ Step-by-Step Explanation**

**🔹 Step 1: Open Registry Editor**

* Press **Win + R**, type regedit, and hit **Enter**.
* This opens the **Registry Editor**, where Windows settings are stored in a hierarchical database.

**🔹 Step 2: Locate HKEY\_LOCAL\_MACHINE**

* This registry hive contains system-wide settings that apply to all users.

**🔹 Step 3: Navigate to Control Path**

* Expand:

sql

CopyEdit

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control

* Right-click on **Control** → Click **New → Key**.

**🔹 Step 4: Name the Key StorageDevicePolicies**

* This is a special key used to control storage device behavior like **write protection**.

**🔹 Step 5: Create a New DWORD Value**

* Right-click on StorageDevicePolicies → **New → DWORD (32-bit) Value**

**🔹 Step 6: Name the DWORD → WriteProtect**

**🔹 Step 7: Set Value Data to 1**

* Double-click WriteProtect, and set **Value Data = 1**
* This **enables write protection** for all USB devices.

**🔹 Step 8: Test Write Protection**

* Try to **copy, cut, or delete** a file on the USB drive.
* You will receive a **"disk is write-protected" warning**.
* This confirms that the USB device is now in **read-only mode**, just like a **hardware write blocker**.

**🔹 Step 9: Disable Write Protection**

* Go back to the WriteProtect DWORD.
* Set **Value Data = 0** to **disable write protection**.

**🔹 Step 10: Confirm Access Restored**

* You can now **add, delete, or modify** files on the USB.

**🧠 Understanding the Practical**

* **Why do we do this?**
  + In digital forensics, we **never modify the original evidence**.
  + Write blockers (hardware or software) protect data from being altered during analysis.
  + This method uses the **Windows registry** as a **software-based write blocker**.
* **What is next after write-blocking?**
  + Use **FTK Imager** to **create a forensic image** of the USB.
  + This image can then be analyzed without altering the original evidence.

**🎤 Viva Questions and Answers**

**1. What is a Write Blocker? Why is it important?**

**Answer:**  
A write blocker is a device or software that **prevents any modifications** to storage media while allowing read access. It ensures the integrity of digital evidence during forensic acquisition.

**2. What is the difference between hardware and software write blockers?**

**Answer:**

* **Hardware write blocker** is a physical device placed between the computer and the drive.
* **Software write blocker** uses system-level settings (like registry) to prevent writing to the drive.

**3. Why did we create the StorageDevicePolicies key?**

**Answer:**  
This key is required for setting **write protection policies** for storage devices in Windows. It doesn’t exist by default, so we manually create it.

**4. What does setting the WriteProtect value to 1 do?**

**Answer:**  
It **enables write protection** for all USB storage devices connected to the system.

**5. What tool do we use to image the write-protected USB?**

**Answer:**  
We use **FTK Imager** to create a **forensic image** of the USB device after enabling write protection.

**6. Why do we verify write protection before imaging?**

**Answer:**  
To ensure that **no data on the USB is altered** during the acquisition process, maintaining **evidence authenticity**.

**7. How do you confirm that the USB is write protected?**

**Answer:**  
By attempting to **copy, delete, or modify** a file on the USB. If it gives a **"write-protected" warning**, the protection is active.

**8. Why do we use FTK Imager in this process?**

**Answer:**  
FTK Imager allows us to **preview, acquire, and verify** forensic images in a legally acceptable format like .dd or .E01.

**9. Is software write protection as reliable as hardware?**

**Answer:**  
No. Software write protection can be **bypassed** or **disabled** by a knowledgeable user, while **hardware write blockers** are more secure and tamper-proof.

**10. Can you use this method in a real forensic investigation?**

**Answer:**  
It’s more of a **lab or educational setup**. In real investigations, hardware write blockers are preferred due to **higher reliability** and **legal acceptance**.

**✅ Conclusion**

In this practical, you learned to:

* Use **Windows registry** to enable **USB write protection**.
* Simulate the behavior of a **write blocker**.
* Protect evidence before creating a **forensic image using FTK Imager**.

👌👌👌👌👌👌👌 👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌

**Practical 4: Capturing and analysing network packets using Wireshark (Fundamentals)**

**Aim:**

The purpose of this practical is to capture and analyze network packets using **Wireshark**, a popular packet-sniffing tool. This will help us understand how data is transmitted over a network, identify network activities, and troubleshoot network issues.

**Steps in Detail:**

**Step 1: Start Packet Capturing in Wireshark**

* **Wireshark captures all network traffic** (data packets) that enter or leave your computer.
* Open **Wireshark** and identify the network interface you want to capture packets from.
* If you are connected via **Wi-Fi**, right-click on the "Wi-Fi" interface and click **"Start Capture"**.
* If using a wired connection, select **"Ethernet"** instead.

**Step 2: Generate Network Traffic**

* Open a **web browser** (Chrome, Firefox, etc.).
* Visit any **website** (e.g., www.google.com) and perform some actions like searching for something or clicking on a link.
* These actions generate network traffic, which is captured by Wireshark in real time.

**Step 3: Stop Capturing and Analyze the Packets**

* Go back to **Wireshark** and **stop the capture** by clicking the red stop button.
* Now, we can **filter** packets using various **display filters**.

**Filtering and Analyzing Packets**

Once we have captured the packets, we can apply **filters** in Wireshark to analyze specific network activities.

**1. Display packets with a specific IP address**

ini

CopyEdit

ip.addr == 192.168.0.101

* This filter shows **all packets** (incoming and outgoing) involving the IP **192.168.0.101**.
* Useful for tracking traffic from/to a particular device.

**2. Display packets where a specific IP is the source**

ini

CopyEdit

ip.src == 192.168.211.1

* This filter shows **only outgoing packets** from the IP **192.168.211.1**.
* Useful to analyze what data is being sent from a specific device.

**3. Display packets where a specific IP is the destination**

ini

CopyEdit

ip.dst == 192.168.211.134

* This filter shows **only incoming packets** to the IP **192.168.211.134**.
* Useful for monitoring what data is being received by a device.

**4. Display packets using HTTP protocol**

nginx

CopyEdit

http

* Shows all packets using **HTTP (HyperText Transfer Protocol)**.
* Useful to track **web browsing activities** (unencrypted).

**5. Display only HTTP requests**

CopyEdit

http.request

* Shows packets where the client **requests** a webpage from the server.
* Helps track what websites a user is trying to access.

**6. Display packets with successful HTTP responses**

ini

CopyEdit

http.response.code == 200

* Filters out **only successful responses** (where the web page was successfully loaded).
* Useful for checking which requests were successfully completed.

**7. Display packets using port 80 (HTTP) or port 443 (HTTPS)**

ini

CopyEdit

tcp.port == 80 || udp.port == 443

* **Port 80** is used for **unencrypted** web browsing (HTTP).
* **Port 443** is used for **secure** web browsing (HTTPS).
* Useful to filter web traffic based on security.

**8. Display packets that contain the keyword "Google"**

sql

CopyEdit

tcp contains google

* Shows packets that contain the word **"Google"** in their data.
* Useful for tracking searches or requests related to Google.

**Viva Questions and Answers**

Here are some possible viva questions and how to answer them:

**Basic Questions:**

1. **What is Wireshark?**
   * Wireshark is a **network packet analyzer** used to capture and analyze network traffic.
2. **Why do we use Wireshark?**
   * To monitor network traffic, troubleshoot network issues, and analyze security threats.
3. **What are packets?**
   * Packets are **small units of data** transmitted over a network.
4. **What is an IP address?**
   * An IP address is a unique identifier assigned to a device on a network.
5. **What is a port?**
   * A port is a **communication endpoint** used to distinguish different types of network services (e.g., HTTP on port 80, HTTPS on port 443).

**Technical Questions:**

1. **What is the difference between ip.src and ip.dst?**
   * ip.src filters **outgoing packets** (sent by a device).
   * ip.dst filters **incoming packets** (received by a device).
2. **What is the difference between TCP and UDP?**
   * **TCP (Transmission Control Protocol)** is connection-oriented and reliable.
   * **UDP (User Datagram Protocol)** is connectionless and faster but less reliable.
3. **What does the HTTP response code 200 mean?**
   * It means the request was **successful**, and the server returned the requested content.
4. **Why do we filter packets using port numbers?**
   * Different services use different ports. Filtering by port helps analyze specific types of traffic (e.g., web traffic, email, gaming).
5. **How can Wireshark help in cybersecurity?**
   * It helps detect **suspicious activity, unauthorized access, and network attacks**.

**Conclusion**

* This practical helps in understanding how network traffic flows and how to capture packets using **Wireshark**.
* By using filters, we can extract useful data for troubleshooting, monitoring, and cybersecurity analysis.

👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌

**Practical 5: Analyzing Packets Using Wireshark**

**Aim**

The objective of this practical is to analyze pre-captured network packets in Wireshark and extract specific information using filters and tools.

**Steps in Detail**

**1. Identifying the Web Server Software Used by www.snopes.com**

* The Host header in HTTP requests contains the domain name.
* To display all domain names in Wireshark:
  + Select any HTTP request packet.
  + Expand the HyperText Transfer Protocol section.
  + Right-click on the Host header and choose Apply as Column to make it visible in the packet list.
* Locate a request with www.snopes.com.
* Right-click the packet and select Follow → TCP Stream.
* The Server header in the response reveals the web server software used.
* In this case, it shows Microsoft IIS 5.0.

**2. Finding the Cell Phone Problem the Client is Concerned About**

* To identify the issue, filter packets containing the word "cell" using:

ruby

CopyEdit

frame matches “(?)cell”

* Check HTTP request packets that include "cell" in their URLs or payloads.
* Upon inspection, the issue is related to a cell phone charging problem.

**3. Finding What Instrument Ryan Will Learn to Play According to Zillow**

* Use the filter:

ruby

CopyEdit

frame matches “(?)zillow”

* Only one packet contains the word Zillow.
* Select this packet and expand the Transmission Control Protocol section.
* Enable TCP stream reassembly:
  + Right-click on Transmission Control Protocol → Protocol Preferences → Enable Allow subdissector to reassemble TCP stream.
* Extract HTTP objects:
  + File → Export Objects → HTTP.
  + Save all objects from the packet.
* Upon extracting files, an SWF (Flash) file related to Zillow is found.
* Opening the SWF file reveals that Ryan is learning to play the saxophone.

**4. Counting the Number of Web Servers Running Apache**

* Use the filter:

CopyEdit

http.response

* This displays all HTTP response packets.
* Add the Server header as a column:
  + Select any HTTP response packet.
  + Expand the HyperText Transfer Protocol section.
  + Right-click on the Server header → Apply as Column.
* Filter only packets from Apache servers:

sql

CopyEdit

http.server contains "Apache"

* To count the number of Apache web servers:
  + Go to Statistics → Endpoints.
  + Check Limit to display filter to apply the Apache filter.
  + The result shows 21 connections, meaning there are 21 Apache servers.

**5. Identifying Hosts That Think Jokes Are More Entertaining When Explained**

* Apply the filter:

ruby

CopyEdit

frame matches “(?)jokes”

* Find the HTTP packet where the server response includes the phrase "jokes are better explained."
* Expand the HyperText Transfer Protocol section and locate the same text.
* The corresponding IP addresses of the hosts that share this belief are:
  + 173.241.244.153
  + 173.241.244.99
  + 173.241.244.7

**Viva Questions and Answers**

**Basic Questions**

1. What is Wireshark?
   * Wireshark is a network packet analyzer used for capturing and analyzing network traffic.
2. What is a packet?
   * A packet is a small unit of data sent across a network.
3. What is the HTTP protocol used for?
   * HTTP is used for transferring webpages, images, and other data between a web browser and a server.
4. What is the difference between a request and a response in HTTP?
   * A request is sent by the client (browser), while a response is sent by the web server.

**Technical Questions**

1. How can we find out which web server software a site is using?
   * By looking at the Server header in the HTTP response.
2. Why do we need to enable ‘Allow subdissector to reassemble TCP stream’?
   * It helps reconstruct fragmented network data to view complete information.
3. What is Apache, and why is it important?
   * Apache is an open-source web server used to host websites.
4. How do we extract objects from HTTP packets?
   * By going to File → Export Objects → HTTP in Wireshark.
5. How can we filter packets that contain specific words?
   * Using the frame matches "(?)word" filter.

**Conclusion**

This practical helps in deep packet inspection and teaches how to extract useful information from captured network traffic. Using filters and statistical tools in Wireshark, we can analyze web servers, track client concerns, and gather insights from communication data.

👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌

**Practical 6: Using Sysinternals Tools for Network Tracking and Process Monitoring**

**🎯 Aim:**

To use **Sysinternals Suite** tools for:

* Live process monitoring
* Capturing network traffic (TCP/UDP)
* Tracking memory (RAM, virtual memory, cache)
* Monitoring hard disk usage

**⚙️ Tool-Wise Detailed Practical Explanation**

**🔹 1. Monitor Live Processes (Tool: ProcMon)**

**✔️ Steps:**

* Open **ProcMon (Process Monitor)**.
* Click **Filter → Filter...** to set custom filters (e.g., by Process Name, PID, Result, etc.)
* Click on **Tools → Process Tree** to see the **parent-child relationship** of processes.

**🧠 What’s happening?**

ProcMon captures **real-time activity** of all processes, file systems, registry access, and threads. It helps spot:

* Suspicious processes
* Unauthorized access
* Malware activity

**📌 Example Use in Forensics:**

Used to track if any **malware is modifying registry entries**, or accessing unauthorized files.

**🔹 2. Capture TCP/UDP Packets (Tool: TcpView)**

**✔️ Steps:**

* Open **TcpView**.
* It lists all **active TCP and UDP connections** with their local/remote IPs and ports.
* Right-click on a process and choose **“Whois”** to check info about the remote IP.

**🧠 What’s happening?**

TcpView shows **network communication** of each process — IPs, ports, connection state.

**📌 Example Use:**

Used to detect if a **suspicious process is communicating with an external server**, possibly for data exfiltration.

**🔹 3. Monitor Hard Disk (Tool: RAMMap)**

**✔️ Steps:**

* Open **RAMMap**.
* It displays usage of **physical memory** by file system, processes, drivers, etc.

**🧠 What’s happening?**

RAMMap breaks down how your **RAM is being utilized** — useful to identify memory leaks, abnormal usage.

**📌 Forensic Use:**

Investigators use it to identify **which files or drivers are consuming memory**, and if unauthorized software is loaded.

**🔹 4. Monitor Virtual Memory (Tool: VMMap)**

**✔️ Steps:**

* Open **VMMap**.
* Choose a running process — it visualizes its **virtual memory allocation** (stack, heap, DLLs, reserved blocks).

**🧠 What’s happening?**

VMMap helps visualize how **memory is segmented and allocated** in a process.

**📌 Use Case:**

Used in malware analysis to track **how a process is injecting or reserving memory** for malicious code.

**🔹 5. Monitor Cache Memory (Tool: CacheSet)**

**✔️ Steps:**

* Open **CacheSet**.
* It allows you to **view and modify the system file cache size**.

**🧠 What’s happening?**

CacheSet manages how much memory Windows uses to **cache recently accessed files**.

**📌 Use in Forensics:**

Analysts can monitor or adjust cache to prevent **data tampering or overwriting**, especially during memory acquisition.

**🎤 Viva Questions and Answers**

**1. What is the Sysinternals Suite?**

**Answer:**  
It is a collection of advanced system utilities developed by Microsoft for **system monitoring, troubleshooting, and digital forensics**.

**2. What is the use of Process Monitor (ProcMon)?**

**Answer:**  
ProcMon captures **real-time file system, registry, and process/thread activity**. It's used to detect **unauthorized or suspicious activities** in a system.

**3. What is TCPView used for?**

**Answer:**  
TcpView displays **real-time TCP and UDP connections** made by running processes. It helps identify **malicious or suspicious network communication**.

**4. What is the difference between TCP and UDP?**

**Answer:**

* **TCP** is **connection-oriented**, reliable, and used for web traffic (HTTP/HTTPS).
* **UDP** is **connectionless**, faster but less reliable, used in games, video calls, DNS.

**5. What is RAMMap used for?**

**Answer:**  
RAMMap gives a **detailed breakdown of physical memory usage**, showing how memory is allocated by files, drivers, processes, etc.

**6. What is the role of VMMap?**

**Answer:**  
VMMap shows how a process is using its **virtual memory**, including stack, heap, DLLs, and reserved memory — useful in detecting memory manipulation.

**7. What does CacheSet do?**

**Answer:**  
CacheSet is used to **view and adjust** the Windows system file cache, which affects how files are stored in RAM for quick access.

**8. Why are these tools important in forensics?**

**Answer:**  
They help investigators:

* Monitor live system behavior
* Capture evidence of malicious activity
* Analyze memory and network behavior
* Prevent data tampering

**9. What is the difference between physical and virtual memory?**

**Answer:**

* **Physical Memory** is the actual **RAM** installed.
* **Virtual Memory** is simulated memory on the **hard disk** used when RAM is full.

**10. Can Sysinternals tools modify system settings?**

**Answer:**  
Some tools (like CacheSet) can change memory parameters, but most are used for **monitoring and analysis** without making changes.

**✅ Conclusion**

This practical shows how Sysinternals tools help in:

* Real-time monitoring of **processes**
* Analyzing **network connections**
* Inspecting **memory and storage usage**

👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌

**Practical 7: Recovering and Inspecting Deleted Files Using FTK Imager**

**🎯 Aim:**

To recover and analyze deleted files using **FTK Imager**, a forensic tool used to create **disk images** and extract lost data.

**⚙️ Step-by-Step Practical Explanation**

**🔹 Part 1: Creating a Disk Image**

A **disk image** is a bit-by-bit copy of a storage device (HDD, SSD, USB). Forensic investigators use it to ensure the **original data remains unaltered**.

**✔️ Steps to Create a Disk Image:**

1. **Open FTK Imager**.
2. Click **File → Create Disk Image**.
3. **Select Source Evidence Type** (Physical Drive, Logical Drive, Image File).
4. Select the **source drive/path** (the one you want to create an image of).
5. Choose the **destination folder** to store the disk image.
6. Click **Finish** to begin the imaging process.

**🧠 What’s happening here?**

* FTK Imager captures a **forensic copy** of the storage device without modifying the original data.
* The image contains **all files, including deleted and hidden ones**.
* This is a crucial step to maintain **data integrity in forensic investigations**.

**🔹 Part 2: Recovering Deleted Files from Disk Image**

Once we have the disk image, we can analyze it and recover **deleted files**.

**✔️ Steps to Recover Deleted Files:**

1. Open **Forensic Toolkit (FTK Imager)**.
2. Click **"Start a New Case"**, fill in case details, and click **Next**.
3. Enter **Forensic Examiner Information** (name, case ID, etc.).
4. Keep clicking **Next** until you reach the **Add Evidence** section.
5. Click **Add Evidence → Acquired Image of Drive**.
6. Select the disk image you created earlier and **click OK**.
7. Click **Finish** to load the image.
8. **Browse the file system**, locate **deleted files**, and **export them** for analysis.

**🧠 What’s happening here?**

* FTK Imager **mounts the disk image** in a read-only mode.
* It retrieves **deleted files** by scanning **file system metadata**.
* Even if a file is deleted, **traces of it remain on the disk** until overwritten.

**🔥 Why is This Important in Forensics?**

* Helps recover **crucial evidence** in cybercrime investigations.
* Prevents **tampering with the original disk**.
* Can retrieve **accidentally deleted files** or data wiped by criminals.

**🎤 Viva Questions and Answers**

**1. What is FTK Imager?**

**Answer:**  
FTK Imager is a **forensic imaging tool** used to create disk images and analyze deleted files.

**2. What is a disk image?**

**Answer:**  
A disk image is a **bit-by-bit copy** of a storage device, preserving all data, including deleted and hidden files.

**3. What is the difference between a logical and a physical image?**

**Answer:**

* **Logical Image**: Copies only active files & folders.
* **Physical Image**: Copies **entire disk**, including **deleted and hidden data**.

**4. Why do we create a forensic image instead of working on the original disk?**

**Answer:**  
To maintain **data integrity** and prevent **accidental modification or corruption** of original evidence.

**5. How can FTK Imager recover deleted files?**

**Answer:**  
Even after deletion, file traces remain in the **file system metadata** until overwritten. FTK Imager scans these **unallocated spaces** to recover files.

**6. What is the importance of metadata in file recovery?**

**Answer:**  
Metadata stores **file creation, modification, and deletion timestamps**, helping investigators track digital evidence.

**7. What is the role of the Master File Table (MFT) in recovery?**

**Answer:**  
In **NTFS file systems**, the **MFT keeps records** of all files. Even if a file is deleted, **MFT entries** can help restore it.

**8. Can permanently deleted files be recovered?**

**Answer:**  
Yes, unless they have been **overwritten** by new data. **Forensic tools** like FTK Imager and Autopsy can recover **traces of deleted files**.

**9. What file systems does FTK Imager support?**

**Answer:**

* NTFS
* FAT32
* exFAT
* HFS+ (Mac)
* EXT3/EXT4 (Linux)

**10. How can you ensure the recovered files are authentic?**

**Answer:**  
By calculating a **hash value (MD5/SHA256)** before and after recovery to verify data integrity.

**✅ Conclusion**

This practical demonstrates:

* How to **capture a forensic disk image**.
* How to **recover and analyze deleted files**.
* The **importance of digital forensics** in cybercrime investigations.

👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌

**Practical No. 08: Acquisition of Cell Phones and Mobile Devices**

**🎯 AIM:**

To perform forensic acquisition of mobile devices using **MOBILedit! Forensic Software** and an Android **Forensic Tool APK**, capturing essential data such as messages, contacts, emails, and call logs.

**⚙️ Step-by-Step Practical Explanation**

**🔹 Step 1: Download Required Tools**

Before starting the forensic acquisition, ensure you have the following tools:

1. **MOBILedit! Forensic** (Installed on PC/Laptop)
   * This tool allows forensic data extraction from mobile devices.
2. **Forensic Tool APK** (Installed on the target Android device)
   * This application helps in acquiring deeper data access for forensic analysis.

**🔹 Step 2: Connect Your Device**

1. Open **MOBILedit! Forensic** on your PC/Laptop.
2. Click on **“Connection Wizard”** to detect and connect the mobile device.

**🔹 Step 3: Enable Developer Mode on Phone**

To allow data extraction, follow these steps:

1. **Go to Phone Settings → About Phone → Tap "Build Number" 7 times.**
   * This enables **Developer Mode**.
2. Open **Developer Options** and **Enable USB Debugging**.
   * This allows the PC to communicate with the mobile device over USB.

**🔹 Step 4: Ensure Proper USB Connection**

1. **When prompted on your phone**, select **“Allow USB Debugging”** and **tick “Always Allow”** if required.
2. Enable **USB Tethering** to establish a stable connection.

**🔹 Step 5: Select Data to Extract**

1. After successful connection, MOBILedit! will show **extraction options**.
2. Select **“Specific Selection”** to choose the type of data to retrieve:
   * **Messages (SMS, MMS, WhatsApp, etc.)**
   * **Call logs**
   * **Contacts**
   * **Emails**
   * **Installed applications**
   * **Screenshots & multimedia**

**🔹 Step 6: Configure Report Options**

1. Select **report details** to include in the forensic analysis.
2. Choose output format:
   * **HTML Report** (for easy viewing)
   * **PDF Report** (for legal documentation)

**🔹 Step 7: Export Data and Generate Report**

1. Set **report destination path** where extracted data will be saved.
2. Click **“Export”** and confirm the backup process.
3. Allow permissions on the Android device for **backup extraction**.

**🔹 Step 8: Completion of Data Extraction**

1. The **forensic extraction process** will now begin.
2. Once completed, the **forensic report will be available** at the specified path.
3. You can now **review extracted data** for analysis.

**🔥 What’s Happening in This Process?**

* **MOBILedit! Forensic** interacts with the mobile device using **ADB (Android Debug Bridge)** to extract data.
* USB Debugging allows **full access** to the phone's file system.
* The forensic tool **retrieves and organizes** messages, contacts, and app data.
* A **structured report** is generated for legal or investigative use.

**🎤 Viva Questions and Answers**

**1. What is MOBILedit! Forensic?**

**Answer:**  
MOBILedit! Forensic is a forensic tool used for **extracting and analyzing mobile device data**, including messages, call logs, and contacts.

**2. Why do we enable Developer Mode and USB Debugging?**

**Answer:**

* **Developer Mode** unlocks advanced features for debugging.
* **USB Debugging** allows the PC to **interact with the phone’s system** and extract data.

**3. Why is forensic mobile acquisition important?**

**Answer:**

* Helps in **cybercrime investigations**.
* Recovers **deleted messages and call logs**.
* Preserves digital evidence **without altering original data**.

**4. What are the different types of mobile forensic acquisition?**

**Answer:**

1. **Logical Acquisition** – Extracts **only active files** (messages, call logs).
2. **Physical Acquisition** – Extracts **entire device storage** (including deleted files).

**5. What file systems are used in mobile devices?**

**Answer:**

* **Android:** ext3, ext4
* **iOS:** APFS, HFS+

**6. What kind of data can be extracted in a forensic investigation?**

**Answer:**

* Contacts
* Call logs
* SMS/MMS/WhatsApp messages
* Emails
* Installed apps
* Browser history

**7. What formats can forensic reports be exported in?**

**Answer:**  
Reports can be saved in **HTML, PDF, XML, CSV** formats.

**8. How can you verify the integrity of extracted data?**

**Answer:**  
By using **hashing algorithms (MD5, SHA256)** to ensure **data has not been altered**.

**✅ Conclusion**

This practical demonstrates how to:  
✔ Connect a mobile device and extract forensic data.  
✔ Enable **Developer Mode & USB Debugging**.  
✔ Extract **messages, contacts, call logs, emails**.  
✔ Generate **forensic reports in PDF/HTML format**.

This process is **widely used in cyber forensics and law enforcement investigations**.

👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌

**Practical No. 9: Email Forensics**

**🎯 AIM:**

To perform **email forensic investigation** using the **Forensic Toolkit (FTK)** by analyzing **email headers, attachments, and recovering deleted emails** from **.PST (Personal Storage Table) files**.

**⚙️ Step-by-Step Practical Explanation**

**🔹 Step 1: Create a New Case in FTK**

1. Open **Forensic Toolkit (FTK)**.
2. Click on **File → New Case** to start a new forensic investigation.

**🔹 Step 2: Enter Case Details**

1. Fill in details such as **Case Name, Case Number, and Examiner’s Name**.
2. Click **Next** to proceed.

**🔹 Step 3: Configure Case Settings**

1. Ensure that all **checkboxes are checked** to include metadata, attachments, and email content.
2. Click **Next** to continue.

**🔹 Step 4: Select Email Analysis Emphasis**

1. Choose **“Email Emphasis”** to focus on email forensics.
2. Click **Next** to move forward.

**🔹 Step 5: Add Evidence (PST File)**

1. Click on **“Add Evidence”**.
2. Select **“Individual File”** option.
3. Browse and **select the .PST file** (Outlook email archive).
4. Click **OK**.

💡 **Why PST?**

* A **PST file** stores **email messages, contacts, calendar events, and attachments** in Microsoft Outlook.
* Digital forensics tools analyze these files to extract **hidden, deleted, or altered** messages.

**🔹 Step 6: Process and Analyze the Email Data**

1. Click **Next** and then **Finish**.
2. The **PST file will be processed**, and its contents will be displayed in FTK.
3. Now, emails can be filtered and analyzed.

**🔹 Step 7: Recover Deleted Emails**

1. Navigate to the **email section** in FTK.
2. Click on **“From Email”** to view emails.
3. Select an email that appears deleted or suspicious.
4. Click on **“Export”** to recover the email.

**🔹 Step 8: Export and View the Email**

1. **Export the email in .HTML format** for better readability.
2. Ensure the **“Export HTML view if available”** option is **checked**.
3. Click **OK** to save the email at the specified location.
4. Open the exported **.HTML file in a browser** to view the recovered email.

**🔥 What’s Happening in This Process?**

* FTK **extracts** and **processes** email messages from **PST files**.
* It identifies **deleted** or **altered** emails and **recovers them**.
* The recovered emails are **exported in HTML format** for easy viewing.

**🎤 Viva Questions and Answers**

**1. What is Email Forensics?**

**Answer:**  
Email forensics is the **investigation and analysis** of email communication to detect **fraud, phishing, data breaches, or cybercrimes**.

**2. What is a PST file?**

**Answer:**  
A **PST (Personal Storage Table) file** is a **Microsoft Outlook data file** that contains **emails, contacts, calendar events, and attachments**.

**3. How can we recover deleted emails?**

**Answer:**  
Using **FTK or other forensic tools**, we analyze PST files, retrieve deleted emails, and **export them in readable formats** like HTML or EML.

**4. What information can we extract from an email header?**

**Answer:**

* **Sender & Receiver email addresses**
* **IP address of sender**
* **Time & Date of sending**
* **Email routing path (SMTP servers used)**

**5. What are some common email fraud techniques?**

**Answer:**

1. **Phishing** – Fake emails pretending to be legitimate.
2. **Spoofing** – Faking email sender details.
3. **Malware Attachments** – Spreading viruses via email.

**6. Why do we export emails in HTML format?**

**Answer:**  
**HTML format retains the email structure, embedded images, and hyperlinks**, making it easier to view and analyze.

**7. What are the challenges in email forensics?**

**Answer:**

* **Encryption** – Some emails are encrypted.
* **Anonymization** – Attackers hide their identity.
* **Metadata manipulation** – Hackers alter timestamps.

**8. What hashing algorithms are used in forensic investigations?**

**Answer:**

* **MD5 (Message Digest Algorithm 5)**
* **SHA-256 (Secure Hash Algorithm 256-bit)**

These are used to **ensure data integrity** in forensic investigations.

**✅ Conclusion**

This practical covers:  
✔ Extracting emails from **PST files**.  
✔ Recovering **deleted emails**.  
✔ **Exporting email evidence** for legal or forensic use.  
✔ **Understanding email headers and forensic analysis**.

This process is **crucial for investigating email fraud, phishing, and cybercrimes**

**👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌👌**

**No. 10: Web Browser Forensics**

**🎯 AIM:**

To perform **web browser forensics** by analyzing:  
✅ **Browsing history**  
✅ **Cache & cookies**  
✅ **Last internet activity**  
✅ **Stored login credentials and search history**

This practical helps in **cybercrime investigations**, where digital footprints from web browsers are analyzed to uncover **evidence of malicious activities, hacking attempts, or illegal browsing behavior**.

**⚙️ Step-by-Step Practical Explanation**

**🔹 Step 1: Capture Web Browser History**

1. Open **Web Browser History Examiner** (a forensic tool).
2. Go to **File → Capture History**.

📌 **What is Happening?**  
The tool **extracts** browsing history, cookies, cache, and other stored data from the web browser for forensic analysis.

**🔹 Step 2: Select Data Source**

1. Choose **“Capture History from this computer”** and click **Next**.

📌 **Why?**  
This step **collects** all browsing-related data stored on the computer.

**🔹 Step 3: Select User Profile & Data**

1. Select **user profile** (e.g., "Admin").
2. Check the **boxes** for the data you want to extract:  
   ✅ **Bookmarks**  
   ✅ **Cached Files, Images, and Web Pages**  
   ✅ **Cookies**  
   ✅ **Downloads**  
   ✅ **Email Addresses**  
   ✅ **Favicons** (Icons of visited websites)  
   ✅ **Form History (Auto-fill data)**  
   ✅ **Logins (Saved usernames & passwords)**  
   ✅ **Search History**  
   ✅ **Session Tabs** (Recently closed tabs)  
   ✅ **Thumbnails** (Small previews of websites)  
   ✅ **Website Visits** (History of visited sites)
3. Select a **destination folder** to save the extracted data and click **Next**.

📌 **Why?**  
This step allows us to **filter specific browser data** for forensic analysis.

**🔹 Step 4: Process & Load Captured Data**

1. Once processing is completed, click **Yes** to load the extracted data.
2. The extracted **browsing data** is displayed in separate categories.

📌 **Why?**  
This allows forensic experts to **categorize and analyze** browsing behavior easily.

**🔹 Step 5: Analyze Captured Data**

The loaded data is organized into **different tabs** in the forensic tool:

| **Category** | **What It Stores** |
| --- | --- |
| **Bookmarks** | List of saved websites |
| **Cached Files** | Locally stored web data for faster loading |
| **Cached Images** | Images from visited websites |
| **Cached Web Pages** | Copies of entire websites saved for quick access |
| **Cookies** | Small data files storing login status, tracking info |
| **Downloads** | List of downloaded files |
| **Email Addresses** | Stored email IDs used on websites |
| **Favicons** | Small icons of visited websites |
| **Form History** | Auto-filled text from forms |
| **Logins** | Saved usernames & passwords |
| **Searches** | List of searches made on search engines |
| **Session Tabs** | Previously opened tabs before closing browser |
| **Thumbnails** | Small previews of visited web pages |
| **Website Visits** | Full browsing history |

📌 **Why?**  
This allows investigators to track a user's online behavior, including **visited websites, search queries, login credentials, and downloads**.

**🔹 Step 6: Export Data for Forensic Analysis**

1. Click on **File → Export → Export to HTML**.
2. Select the **data to export** and click **Export**.

📌 **Why?**  
The extracted data is **saved in an HTML format**, making it easy to view in any web browser.

**🔹 Step 7: Open Extracted Data**

1. Navigate to the **destination folder** where the exported file is saved.
2. Open the **.HTML file** in a web browser.
3. The complete forensic report of browsing activity is displayed.

📌 **What’s Happening?**  
This allows **investigators to review and present digital evidence** in a structured format.

**🔥 What’s Happening in This Process?**

✅ Capturing **browsing history, cache, cookies, logins, downloads**.  
✅ Recovering **deleted internet activity**.  
✅ Identifying **potential security threats** or **evidence of illegal activity**.  
✅ Exporting browser data for **forensic reporting and legal use**.

**🎤 Viva Questions and Answers**

**1. What is Web Browser Forensics?**

**Answer:**  
Web Browser Forensics is the **investigation of internet activities** by analyzing a user’s browsing history, cache, cookies, and other stored data.

**2. What types of browser data can be recovered?**

**Answer:**

* **Browsing history** (List of visited websites)
* **Cookies** (Tracking & login info)
* **Cache files** (Stored web content)
* **Search history** (Google, Bing searches)
* **Form history** (Auto-fill text)
* **Downloaded files**

**3. What is the importance of cookies in forensic analysis?**

**Answer:**  
Cookies store:

* **Login session data**
* **Tracking information** (advertisements, analytics)
* **Authentication tokens**  
  These help in **tracking user behavior** and **recovering deleted login sessions**.

**4. How can browser forensics help in cybercrime investigations?**

**Answer:**

1. Identifies **visited illegal websites**.
2. Tracks **phishing attempts and data leaks**.
3. Recovers **deleted browsing history**.
4. Identifies **compromised accounts** (stolen credentials).

**5. What are Cached Files and why are they important?**

**Answer:**

* **Cached files** are stored **copies of visited web pages and images**.
* These allow forensic experts to **reconstruct past internet activity** even if browsing history is deleted.

**6. How can an attacker erase browsing history? Can it be recovered?**

**Answer:**

* Attackers use **"Incognito Mode"**, delete history, or use **privacy tools**.
* Forensic tools like **FTK, Web Browser History Examiner, and Autopsy** can still **recover deleted data** from disk storage.

**7. What are the challenges in web browser forensics?**

**Answer:**

* **Encrypted browsing data** (e.g., in Brave browser, Tor)
* **Incognito/Private Mode** (Limits tracking)
* **Anti-forensic tools** (VPNs, secure browsers)

**8. Which hashing algorithms are used to verify forensic data integrity?**

**Answer:**

* **MD5 (Message Digest 5)**
* **SHA-256 (Secure Hash Algorithm 256-bit)**  
  These ensure the extracted evidence is **unaltered and legally valid**.

**✅ Conclusion**

This practical covers:  
✔ Extracting **browser history, cookies, cache, logins, and searches**.  
✔ **Recovering deleted browsing activity**.  
✔ **Identifying potential cyber threats or criminal activities**.  
✔ **Exporting and analyzing forensic reports**.