Practical 1 – Creating a Forensic Image using FTK Imager/Encase Imager

Aim: To create a forensic image of a storage device using FTK Imager/Encase Imager and check the integrity of data for analysis.

Tools Used: - FTK Imager / Encase Imager - Windows computer

Procedure: 1. Launch FTK Imager → File → Create Disk Image. 2. Select evidence type (physical drive, logical drive, or image file). 3. Choose the source drive/file path. 4. Specify the destination folder and filename for the image. 5. If space is insufficient, FTK asks for a new destination. 6. Start imaging → the tool copies data sector by sector. 7. Generate Image Summary Report with MD5/SHA1 hash values. 8. Add the created image as evidence → analyze it using the Evidence Tree.

Observation: A complete forensic image was created. Hash verification confirmed no data tampering.

Conclusion: Creating a forensic image ensures original data remains intact. Investigators work only on the verified copy of evidence.

Practical 2 – Data Acquisition using USB Write Blocker and FTK Imager

Aim: To perform safe data acquisition from a suspect device using a USB Write Blocker and FTK Imager/ProDiscover.

Tools Used: - USB Write Blocker - ProDiscover Basic / FTK Imager

Procedure: 1. Start ProDiscover and create a new case. 2. In the left pane, select Add → Capture & Add Image. 3. Enter case details and start acquisition. 4. The tool captures a forensic image of the device connected through a Write Blocker. 5. Open the image → explore cluster view and gallery view. 6. Perform keyword search in the acquired image. 7. Generate a final report of findings.

Observation: The data was safely acquired without altering the original device, and evidence could be searched and analyzed.

Conclusion: Using a Write Blocker ensures integrity of evidence during acquisition, making the process reliable and legally acceptable.

Practical 3 – Forensics Case Study using Autopsy/EnCase Investigator

Aim: To analyze a forensic case study by examining a given disk image file using Autopsy.

Tools Used: - Autopsy Forensic Tool / EnCase Investigator

Procedure: 1. Open Autopsy → create a new case → enter details. 2. Select evidence type (disk image/VM file) and add the file. 3. Enable ingest modules for analysis and click Finish. 4. Autopsy processes the disk and displays files in the Table tab. 5. Expand Evidence Tree → view files, documents, and metadata. 6. Recover deleted files by right-click → Extract Files. 7. Save extracted files in the export folder. 8. Generate a case report in Excel/PDF format.

Observation: Autopsy displayed the entire disk contents, including hidden and deleted files. Reports documented the findings.

Conclusion: Autopsy is a powerful tool for analyzing disk images, recovering data, and generating forensic reports.

Practical 4 – Capturing and Analyzing Network Packets using Wireshark

Aim: To capture and analyze live network traffic using Wireshark.

Tools Used: - Wireshark Network Analyzer

Procedure: 1. Open Wireshark and select network interface. 2. Enable promiscuous mode to capture all packets. 3. Start capture → packets appear in real time. 4. Stop capture with red button. 5. Observe color codes: TCP (light purple), UDP (light blue), Errors (black). 6. Analyze packet details by selecting a frame. 7. Apply filters like: - ip.addr == 192.168.1.1 - http - tcp.port == 80 8. Note protocol usage, source/destination, and errors.

Observation: Packets of TCP, UDP, and HTTP traffic were captured and analyzed. Filters helped isolate useful evidence.

Conclusion: Wireshark is effective for monitoring and investigating network activity, essential in cybercrime investigations.

Practical 5 – Packet Analysis using Wireshark (Case-based)

Aim: To analyze captured packets and solve forensic questions using Wireshark.

Tools Used: - Wireshark

Procedure: 1. Open given packet capture file (.pcap). 2. Use host header column to identify domains. 3. Follow TCP stream → check server software. 4. Search keywords to find client concerns. 5. Export objects (HTTP objects) to find files like Zillow.swf. 6. Apply filter http.server contains "Apache" to count Apache servers. 7. Generate statistics → endpoints → verify active servers.

Observation: Identified web server software, client issue, instrument (saxophone), and number of Apache servers (21).

Conclusion: Wireshark allows deep inspection of network captures, useful for solving forensic cases.

Practical 6 – Using Sysinternals Tools for Network & Process Monitoring

Aim: To explore Sysinternals tools for monitoring processes, RAM, network packets, hard disk, and memory.

Tools Used: - Sysinternals Suite (ProcMon, RAMCapture, TcpView, DiskMon, VMMap, RAMMap)

Procedure: 1. ProcMon → filter processes, view tree, count occurrences. 2. RAMCapture → dump system memory into .mem file. 3. TcpView → capture live TCP/UDP packets, save logs. 4. DiskMon → monitor disk read/write operations. 5. VMMap → analyze virtual memory usage. 6. RAMMap → view and save cache memory usage.

Observation: System activities were monitored in real time. Memory dumps and logs were generated successfully.

Conclusion: Sysinternals tools are essential for low-level monitoring of Windows systems, useful in forensic and incident response.

Practical 7 – Recovering and Inspecting Deleted Files using Autopsy

Aim: To recover and analyze deleted files from a local disk using Autopsy.

Tools Used: - Autopsy

Procedure: 1. Start Autopsy → create new case. 2. Add source type as local disk. 3. Autopsy analyzes and lists all files. 4. Expand Deleted Files node → right click → Extract. 5. Files saved in Export folder. 6. Generate report (Excel) of recovered files.

Observation: Deleted files were successfully located and recovered. Reports documented the recovery.

Conclusion: Autopsy makes file recovery easy and reliable, which is crucial in investigations.

Practical 8 – Acquisition of Mobile Devices

Aim: To study methods of acquiring forensic data from cell phones and mobile devices.

Tools Used: - Mobile forensic tools (UFED, Oxygen Forensics, etc.)

Procedure: 1. Connect mobile device using data cable. 2. Use mobile acquisition tool to detect device. 3. Select logical or physical acquisition method. 4. Extract SMS, call logs, contacts, app data, and media. 5. Save acquired data in standard format for analysis.

Observation: Important data such as messages, images, and logs can be retrieved from mobile devices.

Conclusion: Mobile acquisition is vital as phones store personal and criminal evidence. Specialized tools are required for reliable extraction.

Practical 9 – Email Forensics

Aim: To recover and analyze emails and their headers using FTK.

Tools Used: - FTK (Forensic Toolkit)

Procedure: 1. Start FTK → create new case. 2. Add Outlook .pst file as evidence. 3. View recovered emails in E-mail Messages section. 4. Expand Deleted Items → open deleted emails. 5. Export email as .html file and open in browser. 6. Analyze headers for sender, recipient, IP, and route.

Observation: Deleted emails were recovered and headers provided metadata about sender and routing.

Conclusion: Email forensics helps trace communication, recover evidence, and track suspicious activities.

Practical 10 – Web Browser Forensics

Aim: To analyze web browser activity including cache, cookies, and history.

Tools Used: - BrowserHistoryExaminer

Procedure: 1. Open BrowserHistoryExaminer → File → Capture History. 2. Select capture folder → extract browser data. 3. Browse results: Bookmarks, Cached files, Images, Cookies. 4. Export report in PDF/HTML format.

Observation: The browsing history, cookies, and cache revealed user internet activities.

Conclusion: Browser forensics provides crucial information about user behavior and visited websites.