# **Due Date for Assignment submission 16/7/2024**

**To be done in group of three students**

**Three practical assignment**

1. **Mobile Device Forensics Practical Assignment**

**Objective:**

To provide hands-on experience in the field of mobile device forensics by performing forensic analysis on a simulated mobile device, extracting data, and generating a comprehensive forensic report.

**Materials Required:**

1. A mobile device (preferably Android or iOS) or a mobile device emulator.
2. Forensic tools such as:
   * Cellebrite UFED
   * Magnet AXIOM
   * Autopsy
   * MOBILedit Forensic Express
   * Oxygen Forensic Detective
3. USB cables and adapters
4. Computer with forensic software installed
5. Write-blocker (if using a physical device)

**Assignment Tasks:**

**Task 1: Preparation**

1. **Setting Up the Environment:**
   * Install the necessary forensic software on your computer.
   * Connect the mobile device to the computer using a write-blocker (if applicable).
2. **Device Backup:**
   * Create a full backup of the mobile device using the forensic tool.

**Task 2: Data Acquisition**

1. **Physical Acquisition:**
   * Perform a physical acquisition of the mobile device. Document the steps taken.
2. **Logical Acquisition:**
   * Perform a logical acquisition of the mobile device. Compare the results with the physical acquisition.
3. **File System Acquisition:**
   * Acquire the file system data of the mobile device. Identify and document the file system structure.

**Task 3: Data Analysis**

1. **Extracting Data:**
   * Extract the following data from the acquired image:
     + Call logs
     + SMS/MMS messages
     + Contacts
     + Photos and videos
     + Installed applications and their data
     + Browser history
     + Location data
     + Social media and chat applications data (e.g., WhatsApp, Facebook Messenger)
2. **Keyword Search:**
   * Perform keyword searches on the acquired data. Document the findings.
3. **Analyzing Artifacts:**
   * Identify and analyze common artifacts found in mobile devices such as:
     + SQLite databases
     + PLIST files (iOS)
     + XML files (Android)
     + Log files

**Task 4: Reporting**

1. **Document Findings:**
   * Document all findings in a structured report. Include details such as:
     + Steps taken during acquisition and analysis
     + Tools and techniques used
     + Results of data extraction and analysis
     + Screenshots of important evidence
2. **Generating a Forensic Report:**
   * Generate a comprehensive forensic report that includes an executive summary, detailed findings, and conclusions.

**Submission:**

Submit the following:

1. A detailed forensic report (PDF format).
2. Screenshots of the acquisition and analysis processes.
3. Any relevant logs or evidence files.

**Evaluation Criteria:**

1. **Completeness:** All tasks are completed and all requested data is provided.
2. **Accuracy:** Correct identification and extraction of data.
3. **Documentation:** Clear and thorough documentation of steps taken and findings.
4. **Report Quality:** Professional and comprehensive forensic report.

**Tips for Success:**

* Ensure proper documentation at each step to maintain the integrity of the forensic process.
* Double-check your findings to avoid any inaccuracies.
* Keep the device and acquired data secure to prevent tampering or data loss.

**2) Network Monitoring Device Forensics Practical Assignment**

**Objective:**

To provide practical experience in network monitoring device forensics by performing forensic analysis on a network monitoring device, extracting data, and generating a comprehensive forensic report.

**Materials Required:**

1. Network monitoring device (e.g., router, firewall, IDS/IPS device, or network switch)
2. Forensic tools such as:
   * Wireshark
   * tcpdump
   * NetworkMiner
   * Xplico
   * Nmap
   * Splunk or ELK Stack
   * FTK Imager or EnCase for disk imaging (if applicable)
3. Computer with forensic software installed
4. Storage device for data extraction
5. Network cables and adapters

**Assignment Tasks:**

**Task 1: Preparation**

1. **Environment Setup:**
   * Install necessary forensic software on your computer.
   * Ensure the network monitoring device is properly connected and configured.
   * Create a secure and isolated environment for forensic analysis.
2. **Initial Assessment:**
   * Document the network monitoring device model, firmware version, and configuration settings.
   * Identify and document the interfaces and services running on the device.

**Task 2: Data Acquisition**

1. **Network Traffic Capture:**
   * Use Wireshark or tcpdump to capture network traffic from the device. Save the capture files for analysis.
   * Document the duration and scope of the traffic capture.
2. **Log File Extraction:**
   * Extract log files from the network monitoring device. These may include firewall logs, IDS/IPS alerts, and system logs.
   * Save the log files for further analysis.
3. **Configuration File Extraction:**
   * Extract configuration files from the network monitoring device. These files provide information about device settings and rules.
   * Save the configuration files securely.
4. **Disk Imaging (if applicable):**
   * If the network monitoring device has storage (e.g., hard drive, SSD), create a forensic image using FTK Imager or EnCase.
   * Verify the integrity of the forensic image using hash values.

**Task 3: Data Analysis**

1. **Traffic Analysis:**
   * Analyze the captured network traffic using Wireshark or NetworkMiner. Look for signs of suspicious activity such as unusual connections, large data transfers, or abnormal protocols.
   * Document your findings with relevant screenshots and descriptions.
2. **Log Analysis:**
   * Analyze the extracted log files for signs of security incidents, such as repeated login attempts, firewall rule violations, or IDS/IPS alerts.
   * Use Splunk or the ELK Stack for efficient log analysis and visualization.
   * Document your findings with relevant screenshots and descriptions.
3. **Configuration Analysis:**
   * Review the extracted configuration files to understand the device’s security posture. Look for misconfigurations or vulnerabilities.
   * Document any potential security issues or improvements.
4. **Disk Image Analysis (if applicable):**
   * Use forensic tools to analyze the disk image for additional artifacts, such as deleted files, hidden partitions, or malware.
   * Document your findings with relevant screenshots and descriptions.

**Task 4: Reporting**

1. **Document Findings:**
   * Compile all findings into a structured report. Include details such as:
     + Steps taken during acquisition and analysis
     + Tools and techniques used
     + Results of data extraction and analysis
     + Screenshots of important evidence
     + Any observed security incidents or vulnerabilities
2. **Generate a Forensic Report:**
   * Create a comprehensive forensic report that includes an executive summary, detailed findings, and conclusions. The report should be well-organized and professional.

**Submission:**

Submit the following:

1. A detailed forensic report (PDF format).
2. Screenshots of the acquisition and analysis processes.
3. Any relevant logs, capture files, configuration files, or forensic images.

**Evaluation Criteria:**

1. **Completeness:** All tasks are completed and all requested data is provided.
2. **Accuracy:** Correct identification and extraction of data.
3. **Documentation:** Clear and thorough documentation of steps taken and findings.
4. **Report Quality:** Professional and comprehensive forensic report.

**Tips for Success:**

* Ensure proper documentation at each step to maintain the integrity of the forensic process.
* Double-check your findings to avoid any inaccuracies.
* Keep the device and acquired data secure to prevent tampering or data loss.
* Be thorough in your analysis, considering all possible sources of evidence.

**3 Forensic Tools to Recover Deleted Files Practical Assignment**

**Objective:**

To gain hands-on experience in using forensic tools to recover deleted files from various storage media, analyze the recovered data, and document findings in a comprehensive report.

**Materials Required:**

1. Computer with forensic software installed
2. Storage media (e.g., USB flash drive, hard drive, SSD)
3. Forensic tools such as:
   * FTK Imager
   * Autopsy (Sleuth Kit)
   * EnCase
   * Recuva
   * R-Studio
   * PhotoRec
4. Write-blocker (if using a physical storage device)
5. Storage device for saving recovered data

**Assignment Tasks:**

**Task 1: Preparation**

1. **Setting Up the Environment:**
   * Install the necessary forensic software on your computer.
   * Connect the storage media to the computer using a write-blocker (if applicable).
2. **Initial Assessment:**
   * Document the storage media type, capacity, and any visible characteristics.
   * Create a hash of the storage media to ensure data integrity.

**Task 2: Data Acquisition**

1. **Creating a Forensic Image:**
   * Use FTK Imager or EnCase to create a forensic image of the storage media.
   * Verify the integrity of the forensic image using hash values.
   * Document the acquisition process with relevant screenshots and descriptions.

**Task 3: Data Recovery**

1. **Using FTK Imager:**
   * Load the forensic image into FTK Imager.
   * Navigate to the unallocated space and file slack to identify and recover deleted files.
   * Document the steps taken and any files recovered.
2. **Using Autopsy (Sleuth Kit):**
   * Load the forensic image into Autopsy.
   * Use the “File Analysis” module to search for and recover deleted files.
   * Document the steps taken and any files recovered.
3. **Using EnCase:**
   * Load the forensic image into EnCase.
   * Use the “Deleted Files” module to search for and recover deleted files.
   * Document the steps taken and any files recovered.
4. **Using Recuva:**
   * Run Recuva on the forensic image or directly on the storage media (if a write-blocker is used).
   * Follow the guided steps to search for and recover deleted files.
   * Document the steps taken and any files recovered.
5. **Using R-Studio:**
   * Load the forensic image into R-Studio.
   * Use the “Scan” feature to search for deleted files.
   * Document the steps taken and any files recovered.
6. **Using PhotoRec:**
   * Run PhotoRec on the forensic image or directly on the storage media (if a write-blocker is used).
   * Follow the guided steps to search for and recover deleted files.
   * Document the steps taken and any files recovered.

**Task 4: Data Analysis**

1. **File Analysis:**
   * Analyze the recovered files to identify their relevance and significance.
   * Categorize the files based on their type, such as documents, images, videos, and emails.
   * Document any notable findings, such as sensitive information or evidence of malicious activity.

**Task 5: Reporting**

1. **Document Findings:**
   * Compile all findings into a structured report. Include details such as:
     + Steps taken during acquisition and recovery
     + Tools and techniques used
     + Results of file recovery and analysis
     + Screenshots of important evidence
     + Any observed patterns or significant data
2. **Generate a Forensic Report:**
   * Create a comprehensive forensic report that includes an executive summary, detailed findings, and conclusions. The report should be well-organized and professional.

**Submission:**

Submit the following:

1. A detailed forensic report (PDF format).
2. Screenshots of the acquisition, recovery, and analysis processes.
3. Any relevant logs or recovered files.

**Evaluation Criteria:**

1. **Completeness:** All tasks are completed and all requested data is provided.
2. **Accuracy:** Correct identification and recovery of deleted files.
3. **Documentation:** Clear and thorough documentation of steps taken and findings.
4. **Report Quality:** Professional and comprehensive forensic report.

**Tips for Success:**

* Ensure proper documentation at each step to maintain the integrity of the forensic process.
* Double-check your findings to avoid any inaccuracies.
* Keep the storage media and recovered data secure to prevent tampering or data loss.
* Be thorough in your analysis, considering all possible sources of evidence.