dmf LAB

🧪 Experiment 1: Installation of Sleuth Kit on Linux

Aim:

To install Sleuth Kit on Linux and list all data blocks, analyze allocated and unallocated blocks of a disk image.

Viva Questions & Answers

1. **Q:** What is Sleuth Kit?

   A: Sleuth Kit is an open-source forensic toolkit used for analyzing disk images and recovering digital evidence.

2. **Q:** What command is used to install Sleuth Kit on Linux?

   A: `sudo apt install sleuthkit`

3. **Q:** Which command lists all partitions in a disk image?

   A: `mmls diskimage.dd`

4. **Q:** What is the purpose of `fsstat` command?

   A: It displays file system statistics and metadata information.

5. **Q:** What is the difference between allocated and unallocated blocks?

   A: Allocated blocks store active data, while unallocated blocks contain deleted or unused space.

🧪 Experiment 2: Installation of Sleuth Kit and List All Data Blocks

Aim:

To install Sleuth Kit on Linux and list all data blocks from a disk image.

Viva Questions & Answers

1. **Q:** What is the use of `img_stat` command?

   A: It displays metadata and structure information of the disk image.

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

   A: A disk image is an exact copy of a physical storage device saved in a single file.

3. **Q:** Which command is used to create a disk image?

   A: `dd if=/dev/sdb of=disk.dd bs=4M`

4. **Q:** What information does `mmls` provide?

   A: It shows partition layout and data block structure of a disk image.

5. **Q:** Why is listing data blocks important in forensics?

   A: It helps in identifying used, unused, and deleted areas for evidence recovery.

🧪 Experiment 3: Analyze Allocated and Unallocated Blocks

Aim:

To analyze allocated and unallocated blocks of a disk image using Sleuth Kit.

Viva Questions & Answers

1. **Q:** What is the function of the `fls` command?

   A: It lists files and directories in a file system, including deleted entries.

2. **Q:** What command helps recover deleted files?

   A: `icat` or `tsk_recover` commands are used for file recovery.

3. **Q:** Why are unallocated blocks analyzed in forensics?

   A: Because they may contain deleted or hidden data relevant to an investigation.

4. **Q:** How can you differentiate between allocated and unallocated data?

   A: Allocated data has valid file entries; unallocated space shows no file references.

5. **Q:** What type of evidence can be found in unallocated space?

   A: Deleted files, fragments of documents, and hidden artifacts.

🧪 Experiment 4: Allocate a Disk Image Using Sleuth Kit

Aim:

To allocate and mount a disk image for forensic analysis using Sleuth Kit.

Viva Questions & Answers

1. **Q:** What is disk image allocation?

   A: It is the process of mapping and mounting partitions for forensic analysis.

2. **Q:** How do you mount a partition from a disk image?

   A: By using the offset value and `mount` command with loop device.

3. **Q:** What is an offset in digital forensics?

   A: It's the starting byte or sector of a partition used to access file system data.

4. **Q:** Which command lists partition offsets?

   A: `mmls` lists partition start and end sectors (offsets).

5. **Q:** Why mount a disk image as read-only?

   A: To ensure original evidence is not modified during analysis.

🧪 Experiment 5: Data Extraction from Call Logs Using Sleuth Kit

Aim:

To extract and analyze call logs from a disk image using Sleuth Kit (Autopsy).

Viva Questions & Answers

1. **Q:** What is Autopsy?

   A: Autopsy is a GUI-based digital forensics platform built on Sleuth Kit.

2. **Q:** What kind of data can be extracted using Autopsy?

   A: Files, call logs, contacts, SMS, browser history, and more.

3. **Q:** Which module in Autopsy is used for call log extraction?

   A: The "Call Logs" or "Communications" analysis module.

4. **Q:** What format is used to export extracted data?

   A: Usually `.CSV` or `.XLS` formats for reports.

5. **Q:** Why are call logs important in mobile forensics?

   A: They provide communication patterns, timestamps, and contact links useful for investigations.

🧪 Experiment 6: Allocate a Disk Image and Extract Call Logs Using Sleuth Kit

Aim:

To allocate a disk image and extract call log data using Sleuth Kit and Autopsy.

Viva Questions & Answers

1. **Q:** Why do we allocate a disk image before analysis?

   A: To map partition boundaries and prepare data for forensic extraction.

2. **Q:** Which command is used to list partitions in an image file?

   A: `mmls diskimage.dd`

3. **Q:** What is the role of Autopsy in call log extraction?

   A: It automatically detects and extracts communication artifacts such as call logs.

4. **Q:** What file type usually stores call log data?

   A: SQLite databases (e.g., `calllog.db`).

5. **Q:** What is the output format of extracted call data?

   A: Usually exported as a `.csv` file for easy viewing and reporting.

🧪 Experiment 7: Data Extraction from SMS and Contacts Using Sleuth Kit

Aim:

To extract SMS and contact information from a disk image using Sleuth Kit and Autopsy.

Viva Questions & Answers

1. **Q:** Where are SMS and contacts usually stored on Android devices?

   A: In SQLite databases (`mmssms.db` and `contacts.db`).

2. **Q:** Which tool is used to open `.db` files?

   A: SQLite Browser or DB Browser for SQLite.

3. **Q:** What is the use of the `fls` command in Sleuth Kit?

   A: It lists directory and file entries from a disk image.

4. **Q:** How can extracted data be exported for analysis?

   A: Using "Export to CSV" or by querying the SQLite database.

5. **Q:** Why are SMS and contacts critical in forensic investigations?

   A: They provide evidence of communication between suspects or devices.

🧪 Experiment 8: Install Sleuth Kit and Create SMS and Contacts

Aim:

To install Sleuth Kit and create sample SMS and contact databases for analysis.

Viva Questions & Answers

1. **Q:** What is the purpose of creating sample databases?

A: To simulate forensic analysis on known data.

2. **Q:** Which type of file format is used for storing SMS and contacts?

   A: `.db` files in SQLite format.

3. **Q:** Can Sleuth Kit directly open `.db` files?

   A: No, it extracts them for use with database viewers like SQLite Browser.

4. **Q:** What is the difference between extraction and creation in this experiment?

   A: Extraction retrieves existing data; creation generates test data for analysis.

5. **Q:** Which Autopsy module is used to analyze communication data?

   A: The “Communications” or “Message” module.

🧪 Experiment 9: Create Data and Allocate a Disk Image on Sleuth Kit

Aim:

To create test data and allocate it within a disk image for forensic examination.

Viva Questions & Answers

1. **Q:** What command is used to create a disk image?

   A: `dd if=/dev/sdb of=diskimage.dd bs=4M`

2. **Q:** Why is `mmls` important in Sleuth Kit?

   A: It helps identify partitions and allocate data areas.

3. **Q:** What is the purpose of creating artificial data?

   A: To practice and verify forensic extraction techniques.

4. **Q:** What is the typical file extension of a disk image?

   A: `.dd` or `.img`

5. **Q:** How can you check image integrity?

   A: Using hash verification (MD5/SHA1).

🧪 Experiment 10: Install Autopsy Tool and Create Dataset

Aim:

To install Autopsy forensic tool and create a dataset for investigation.

Viva Questions & Answers

1. **Q:** What is Autopsy primarily used for?

   A: Analyzing digital evidence through a graphical interface.

2. **Q:** How do you install Autopsy on Linux?

   A: Using `sudo apt install autopsy`.

3. **Q:** What is a dataset in Autopsy?

   A: It refers to a case or collection of digital evidence sources.

4. **Q:** What are the default modules in Autopsy?

   A: File analysis, keyword search, hash lookup, and timeline analysis.

5. **Q:** Can Autopsy analyze both mobile and computer images?

   A: Yes, it supports multiple data types.

🧪 Experiment 11: How to Extract Data in Autopsy Tool

Aim:

To extract data artifacts using Autopsy forensic tool.

Viva Questions & Answers

1. **Q:** What types of data can Autopsy extract?

   A: Files, messages, logs, contacts, browser history, and more.

2. **Q:** Which option allows adding a data source?

   A: "Add Data Source" in the case creation wizard.

3. **Q:** What is the purpose of the “Keyword Search” module?

   A: To find specific words or file types in evidence.

4. **Q:** What does the “File Analysis” module show?

   A: Detailed metadata and content of files.

5. **Q:** Why is Autopsy used instead of manual Sleuth Kit commands?

   A: It provides an easy GUI for quicker analysis.

🧪 Experiment 12: How to Install Mobile Verification Toolkit (MVT)

Aim:

To install MVT (Mobile Verification Toolkit) for analyzing mobile backups.

Viva Questions & Answers

1. **Q:** What is MVT?

   A: A tool used for analyzing iOS and Android device data for forensic purposes.

2. **Q:** How do you install MVT?

   A: Using the Python command `pip install mvt`.

3. **Q:** What does MVT help detect?

   A: Malware, spyware traces, and suspicious activity on mobile backups.

4. **Q:** Which platforms does MVT support?

   A: iOS and Android.

5. **Q:** Why do we need dependencies before installing MVT?

   A: They provide necessary Python libraries for the toolkit to run properly.

🧪 Experiment 13: Install or Reinstall Mobile Verification Toolkit

Aim:

To install or reinstall the latest version of MVT for forensic analysis.

Viva Questions & Answers

1. **Q:** What command is used to reinstall MVT?

   A: `pip install --upgrade mvt`

2. **Q:** How to check the installed version of MVT?

   A: By running `mvt --version`.

3. **Q:** Why is updating MVT important?

   A: It ensures compatibility with newer device versions.

4. **Q:** Can MVT decrypt iOS backups?

   A: Yes, using built-in iOS decryption modules.

5. **Q:** What is the difference between MVT-iOS and MVT-Android?

   A: They analyze different operating systems and data structures.

🧪 Experiment 14: Process and Parse Records from the iOS System

Aim:

To process and parse records from iOS system backups for forensic analysis.

Viva Questions & Answers

1. **Q:** What file formats are commonly found in iOS backups?

   A: SQLite and plist (property list) files.

2. **Q:** Which tool is used to view plist files?

   A: Xcode or any plist editor.

3. **Q:** What command is used to decrypt iOS backups in MVT?

   A: `mvt-ios decrypt-backup`

4. **Q:** What does parsing data mean?

   A: Extracting and structuring raw data into readable form.

5. **Q:** Why is iOS parsing important in forensics?

   A: It reveals user activities like messages, contacts, and logs.

🧪 Experiment 15: Extract Installed Applications from Android Devices

Aim:

To extract installed application packages (APKs) from an Android device using ADB.

Viva Questions & Answers

1. **Q:** What is ADB?

   A: Android Debug Bridge — a tool for communicating with Android devices.

2. **Q:** Which command lists installed packages?

   A: `adb shell pm list packages -f`

3. **Q:** How do you extract an APK file?

   A: Using `adb pull` command.

4. **Q:** What must be enabled on the phone for ADB to work?

   A: USB Debugging in Developer Options.

5. **Q:** What is the purpose of extracting APKs?

   A: To analyze installed applications for evidence or malware.

🧪 Experiment 16: Extract Diagnostic Information via ADB Protocol

Aim:

To extract diagnostic information from Android devices using ADB protocol.

Viva Questions & Answers

1. **Q:** What is the purpose of `adb bugreport`?

   A: It generates a complete system report with logs and errors.

2. **Q:** Which command saves logcat output to a file?

   A: `adb logcat > log.txt`

3. **Q:** What does the `dumpsys` command do?

   A: It provides detailed system service information (battery, memory, etc.).

4. **Q:** Why collect diagnostic info in forensics?

   A: To trace device behavior, crashes, or data leaks.

5. **Q:** What file format is used for saving bug reports?

   A: Plain text (`.txt`) format.

🧪 Experiment 17: Generate Unified Chronological Timeline of Extracted Records

Aim:

To generate a single timeline combining all extracted forensic records.

Viva Questions & Answers

1. **Q:** What is a forensic timeline?

   A: A chronological sequence of digital events and activities.

2. **Q:** Which tool in Sleuth Kit helps in timeline creation?

   A: `mactime` command.

3. **Q:** What data types are included in a timeline?

   A: File modifications, calls, messages, and app activities.

4. **Q:** Why is a timeline important?

   A: It helps reconstruct events during an investigation.

5. **Q:** Which file formats are used to export timelines?

A: CSV or HTML.

🧪 Experiment 18: Extract Installed Applications (Repeat)

Aim:

To verify and extract all installed applications from Android devices.

Viva Questions & Answers

1. **Q:** Which ADB command checks if a device is connected?

   A: `adb devices`

2. **Q:** What is the default directory of installed APKs?

   A: `/data/app/`

3. **Q:** What is the difference between system and user apps?

   A: System apps come pre-installed; user apps are downloaded.

4. **Q:** Why are extracted apps analyzed in forensics?

   A: To detect unauthorized or malicious software.

5. **Q:** What tool can inspect APK contents?

   A: APKTool or JADX.

🧪 Experiment 19: Extract Diagnostic Information (Repeat)

Aim:

To extract and store Android system diagnostic data using ADB commands.

Viva Questions & Answers

1. **Q:** How do you check if ADB is installed?

   A: Run `adb version` command.

2. **Q:** What does the command `adb shell dumpsys battery` do?

   A: Displays battery status and health information.

3. **Q:** How can you store ADB output in a file?

   A: Using redirection operator (`>`).

4. **Q:** What is the purpose of `adb bugreport` ?

   A: To capture complete system diagnostics and logs.

5. **Q:** What is the importance of diagnostic reports?

   A: They help understand device behavior and possible tampering.

🧪 Experiment 20: Generate Unified Chronological Timeline of Extracted Records

Aim:

To generate a unified timeline of extracted data from Android or iOS devices.

Viva Questions & Answers

1. **Q:** What is the main goal of timeline analysis?

   A: To correlate events and identify sequence of user actions.

2. **Q:** What types of events are plotted in a timeline?

   A: Calls, messages, app activities, file changes.

3. **Q:** Which Sleuth Kit command is used for generating timelines?

   A: `mactime -b bodyfile.txt > timeline.csv`

4. **Q:** What does MAC in timeline refer to?

   A: Modified, Accessed, Changed timestamps.

5. **Q:** Why is the timeline important for investigators?

   A: It provides a visual sequence of evidence events for easy analysis.
