EXPERIMENT 5:

Step 1: Installation Download Autopsy from the official website: https://www.sleuthkit.org/autopsy/

Step 2: Starting a New Case Launch Autopsy. Click New Case. Enter Case Name and select the location to store the case data. Fill in additional details: Case Number, Examiner’s Name, etc. → Click Next.

Step 3: Adding a Data Source Select Type of Data Source: Physical Drive, Logical Drive, Image File, or Folder. Select the specific source to analyze. Configure Ingest Modules (e.g., Keyword Search, File Type Analysis, Hash Analysis). Click Start Analysis to begin processing the data.

Step 4: Initial Analysis and Overview Monitor Ingest Progress at the lower-left corner. Use the Tree Viewer to explore resulting artifacts.

Step 5: Detailed Analysis Keyword Search: Perform searches using pre-configured or custom keywords. File Analysis: Navigate through files/folders under File Types or File System. Open, view, or export files for detailed examination. Timeline Analysis: Use the Timeline Module to visualize events by timestamp. Helps track user activity over time. Hash Analysis: Compare file hashes against known databases to identify good or bad files.

Step 6: Reporting Click Generate Report from the toolbar after completing analysis. Export reports in formats like HTML, PDF, or Excel.

Step 7: Case Closure Close the case within Autopsy once the investigation is complete. Archive all data and reports according to your organization’s policies.