Lab Assignment: Exploring Digital Forensics Tools

The objective of this assignment is to familiarize students with various digital forensics tools, understand their functionalities, and apply them to a simulated investigation scenario. Students are expected to document their findings in a detailed report, accompanied by relevant screenshots.

Instructions:

1. Select tools from the list below:

    1. Cuckoo Sandbox (Automated malware analysis)
    2. Kali Linux (Comprehensive forensic toolkit)

- Download and install any necessary software. For web-based labs, create an account and set up your lab environment.

2. Scenario-Based Investigation
  - Imagine that you are a digital forensic investigator tasked with analyzing a suspicious computer system. Your job is to:
    - Recover deleted files.
    - Analyze potential malware.
    - Examine network traffic.
    - Investigate user activities.
  - Use the selected tools to conduct your investigation. Each tool should be used to perform a specific aspect of the forensic analysis.

3. Documentation and Reporting
 - For each tool, create a section in your report that includes the following:
 - Tool Overview: Briefly describe the tool, its purpose, and its relevance in digital forensics.
- Setup Process: Document the steps you took to install or access the tool. Include any challenges faced during setup.
 - Investigation Process: Explain how you used the tool to analyze the evidence. Be specific about the steps you took, the features you used, and any configurations made.
    - Results: Present the findings obtained from using the tool. Include data recovered, anomalies detected, or any other relevant information.

- Screenshots/Images: Provide screenshots or images of the tool in use, highlighting key findings or steps in the process.
- Analysis: Discuss the significance of the findings and how they contribute to solving the investigation scenario.
- Challenges and Reflections: Reflect on any challenges you encountered while using the tool and how you overcame them. Discuss what you learned about the tool and its effectiveness in a forensic investigation.

4. Comparison and Conclusion
- Compare the tools based on their ease of use, effectiveness, and the quality of the results obtained. Which tool did you find most valuable? Why?
- Conclude with a summary of your findings, the overall experience of using these tools, and how they can be applied in real-world digital forensic investigations.

Deliverables:
- A comprehensive report (10-15 pages) that includes all sections mentioned above.
- Reports should be professionally formatted and submitted as a PDF.
- Ensure that all images are clear and annotated where necessary to explain the findings.

Grading Criteria:
- Tool Usage (30%): Effective and appropriate use of the selected tools.
- Documentation (30%): Clarity, detail, and accuracy of the report, including setup and investigation processes.
- Analysis (20%): Depth of analysis and understanding of the forensic process.
- Images and Screenshots (10%): Quality and relevance of the images provided.
- Conclusion and Reflection (10%): Insightfulness of the comparison and overall reflections.