1. Introduction

This project simulates how forensic investigators collect and analyze digital evidence from a suspect's system.

2. What is Digital Forensics?

Digital forensics is the process of identifying, preserving, analyzing, and presenting electronic evidence in a legal and systematic way. It is commonly used in cybercrime cases like hacking, data theft, or fraud.

3. About Project

In our project, we've created a realistic investigation environment using a VMware virtual machine. Inside the VM, we've used tools like FTK Imager and Autopsy to simulate the investigation. We've also included sample scripts, logs, screenshots, and an actual email file in .eml format.

4. Tools Demonstration
   Tools inside the virtual machine. - FTK Imager: FTK Imager is used to acquire a forensic image of the suspect's disk or file without changing the original data. - Autopsy: Autopsy is a GUI-based forensic tool used to analyze disk images, extract files, browser history, emails, and more.
5. Showing the Evidence File
   We've saved a sample email file with the .eml extension. This type of file is commonly used in email forensics. Here we can see details like sender, receiver, subject, date, and email content - this helps investigators identify phishing or other malicious activity
6. Running PowerShell & Batch Scripts
   We've created basic PowerShell and batch scripts for live evidence acquisition. - hash_file.ps1: This calculates the SHA256 hash of a file - important to prove integrity. - copy_usb.bat: This simulates copying data from a suspect's USB drive. - extract_logs.bat: This extracts system logs that show login attempts or device history.
7. Chain of Custody
   We've also included a chain of custody form. This document tracks who accessed the evidence, when, and why - which is necessary for legal procedures.
8. Conclusion
   In conclusion, our project demonstrates a simplified yet practical approach to digital forensics. We've included data acquisition scripts, email analysis, and forensic tools to cover each phase of the investigation.