# MODULE 02 Computer Forensics Investigation Process LAB REPORT

Lara Alofi

2110886

Y

Computer Hacking Forensic Investigator (CHFI)

Lab Session Identifiers

1. <https://labclient.labondemand.com/LabClient/c398319e-2459-4f70-abd8-ac577bbf7ee5>
2. <https://labclient.labondemand.com/LabClient/b2a7f009-5808-49ee-ad90-41f5b349e0af>

Username on EC-Council System

1. 2110886@uj.edu.sa

A screenshot of a computer

Description automatically generated

**Lab 01: Analyze File System of a Linux Image**  
In this lab, I utilized Autopsy, a comprehensive digital forensics tool, to analyze the file system of a Linux image within the context of a murder investigation. The scenario presented involved examining the disk image of a deceased individual’s machine, which contained crucial digital evidence potentially linked to the crime.

I began by installing Autopsy on my forensic workstation, following the installation guidelines to ensure all necessary components were properly configured. After setting up the software, I created a new case file to document my analysis and incorporated the disk image as a source for examination.

The initial steps involved navigating through the Linux file system, focusing particularly on critical directories such as /etc and /var. One of my key tasks was to investigate the crontab files, which are essential for scheduling tasks in Linux. Analyzing the crontab provided insights into any automated processes that may have been set up by the user. Additionally, I computed the MD5 hash of a particular document, which allowed me to verify the file's integrity and potentially match it against known evidence.

Throughout this analysis, I learned how to effectively utilize Autopsy’s various features, including keyword searching, file filtering, and timeline analysis, which are invaluable in uncovering hidden data and reconstructing user activities.

**Lab 02: Analyze File System of Windows Images**  
In this lab, I employed The Sleuth Kit (TSK), a collection of command-line tools, to conduct a thorough file system analysis of Windows images related to a cyberattack incident. The forensic investigation aimed to uncover the methods employed by attackers to compromise the organization’s systems.

To initiate my analysis, I first examined the partition tables of the forensic images to understand their structure. I then focused on analyzing the Master File Table (MFT), which provides metadata about files on NTFS file systems. This step was critical in identifying recently created, modified, or accessed files that could be indicative of malicious activity.

As part of my analysis, I recovered various files from the two evidence images, focusing on suspicious files and documents that might contain indicators of compromise. I used TSK commands to navigate the file system effectively, employing tools like fls to list files and icat to extract specific files of interest. My exploration revealed significant metadata structures, including timestamps and user access patterns, which helped in building a comprehensive picture of the incident and identifying the actions taken by the attackers.

**Lab 03: Recover Deleted Files from Hard Disks**  
In this lab, I utilized WinHex, a powerful hex editor and forensic analysis tool, to recover files that had been entirely deleted from a forensic image as part of an investigation into a data breach. The investigation aimed to identify the individual responsible for accessing and erasing sensitive company information.

To begin the recovery process, I imported a Linux image file into WinHex. I used the software's search capabilities to identify specific file types, such as Word documents and spreadsheets, that were likely to contain critical information. The user-friendly interface allowed me to navigate through the hex values effectively, and I could visualize both the raw data and the file structures.

Once I located the deleted files, I utilized WinHex’s recovery features to restore them. This involved selecting the identified file entries and saving them to a designated location on my workstation. The experience of using WinHex for data recovery enriched my practical skills in forensic investigations, highlighting the importance of thorough examination and the potential to recover valuable evidence even after files have been deleted.

**Lab 04: File System Timeline Creation and Analysis Using The Sleuth Kit (TSK)**  
In this lab, I focused on utilizing The Sleuth Kit (TSK) to create detailed timelines that outline user activities on a suspicious computer. The context for this investigation stemmed from a cyberattack, where it was essential to track the suspect's actions leading up to and during the incident.

I started by employing various TSK commands to extract temporal data from the forensic image. This data included timestamps for file creation, modification, and access, which were critical in understanding the timeline of events. After gathering this information, I compiled it into a structured format for analysis.

To generate a comprehensive timeline, I installed Perl to execute the mactime.pl script. This script took the extracted data and transformed it into a readable timeline that included essential details such as date, time, file size, activity type, and user privileges. The resulting timeline was instrumental in reconstructing the sequence of events and provided valuable insights into the suspect’s activities on the computer.

Overall, this lab enhanced my skills in timeline analysis, a crucial aspect of digital forensics that aids investigators in visualizing and interpreting events surrounding an incident.

**Lab 05: Analyze Popular File Formats Using Hex Editor**  
In this lab, I explored different file types using Hex Editor Neo, a powerful hex editor that allows detailed examination of file structures. The primary focus was on analyzing various file formats, including Word documents, JPEG images, PNG files, and RAR archives, to gain a deeper understanding of their internal representations.

Upon opening these files in Hex Editor Neo, I examined the hexadecimal values that compose each file format. This analysis involved identifying specific signatures associated with each file type, which are critical for file identification and forensic investigations. For instance, JPEG files begin with a specific byte sequence that distinguishes them from other formats.

I also explored the metadata contained within these files, including creation dates, last modified timestamps, and author information. This lab provided practical insights into how data is structured within different file formats, reinforcing the importance of understanding file signatures and metadata in digital forensics.