# MODULE 07 Linux and Mac Forensics Report

Lara Alofi

2110886

Y

Computer Hacking Forensic Investigator (CHFI)

Lab Session Identifiers

1. <https://labclient.labondemand.com/LabClient/13784160-86e6-48b1-9d8b-39c5a2fd0a8f>

Username on EC-Council System

1. 2110886@uj.edu.sa

A screenshot of a computer

Description automatically generated

**Lab 01:**

This lab guides how to collecting and analyzing volatile data from a live Linux machine to support forensic investigations. Tasks include checking system uptime, login sessions, network connections, running processes, and auditing logs using tools like netstat, lsof, ps, and nmap. Command history analysis is performed with a Python script, aiding in identifying evidence and tracing attacks.

**Lab 02:**

This lab focuses on collecting and analyzing non-volatile data from a live Linux system for forensic investigations. Students learn to gather system logs, user information, login history, and metadata using commands and Python scripts. Tools such as rkhunter are used to detect rootkits, while metadata extraction and log analysis help build a timeline of events. This process is essential for understanding system states and user activities.

**Lab 03:**   
This lab covers analyzing forensic image files from Linux and Mac systems using Autopsy and other tools. Students learn to extract potential artifacts, including deleted files, system logs, and metadata, to understand past events. Tasks include examining system directories, recovering deleted data, and parsing metadata with spotlight\_parser for detailed insights into file usage and system activities.

**Lab 04:**

This lab teaches how to conduct a forensic investigation on a Linux memory dump using the Volatility Framework. Key tasks include creating Linux kernel profiles, listing processes, detecting injected code, analyzing command history, identifying loaded kernel modules, and examining file systems. The lab aims to equip students with the skills to gather critical evidence from memory dumps to support investigations of data breaches and cyber-attacks.

**Lab 05:**

This lab demonstrates how to recover data from a Linux memory dump using the PhotoRec tool. Students learn to install and run PhotoRec, navigate through recovery options, and extract data to a designated folder. The lab focuses on retrieving critical artifacts like web pages and communication logs for forensic investigations, emphasizing practical skills in memory dump analysis to support cybercrime cases.