

|  |
| --- |
| PROJECT 01 REPORT |
|  |
| March 10  20I-1855  Authored by: Muhammad Ahmed |

# MAC Spoofer Tool Documentation

## **Overview**

The MAC Spoofer tool is a Python script designed to display network information, spoof MAC addresses, and reset MAC addresses on a system. Developed by Muhammad Ahmed for the course "Ethical Hacking Concepts and Practices," this tool provides a user-friendly interface for managing MAC addresses.

## **Developer Information**

* **Developer Name:** Muhammad Ahmed
* **Roll Number:** 20I-1855
* **Section:** CY-T
* **Degree:** Bachelors in Software Engineering
* **Campus:** Islamabad
* **Course Subject:** Ethical Hacking Concepts and Practices

## **Purpose**

The MAC Spoofer tool serves the following purposes:

1. Shows the original and current MAC addresses of the system.
2. Allows users to choose from a variety of MAC addresses for spoofing.
3. Restores the original MAC address of the system.

## **Tool Description**

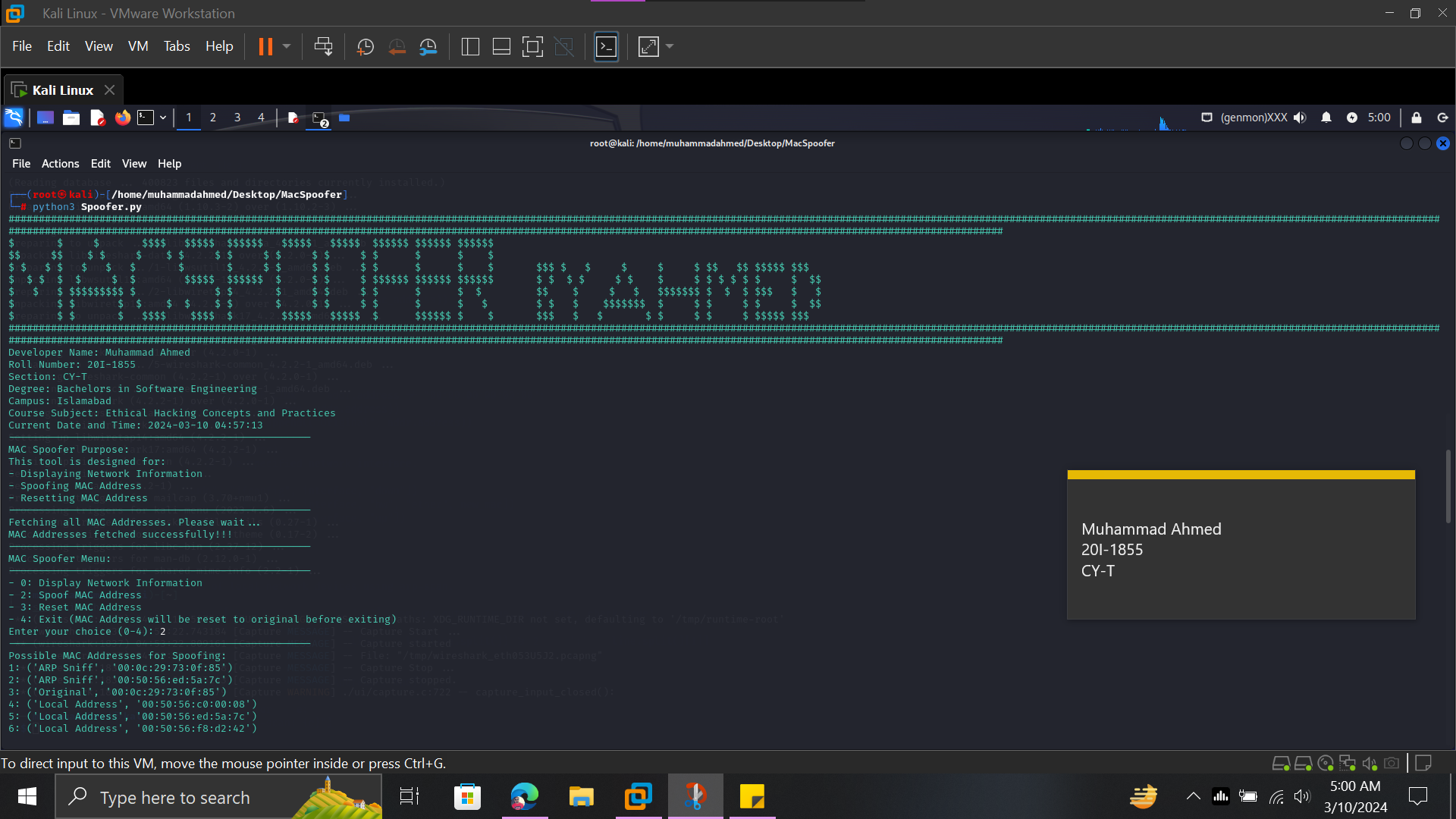
* Includes ASCII art drawings of the letters "MAC Spoofer" at the beginning of the interface.
* Interacts with the user through a menu-driven terminal interface.
* Generates a random MAC address with a locally administered bit set and ensures that the first octet is even.
* Gather MAC addresses using following methods:
  + ARP packet sniffing.
  + Reading original MAC addresses from the system.
  + Retrieving local MAC addresses using arp-scan.
  + Reading MAC addresses from a CSV file (from public sources).
* Spoofs the MAC address of the specified network interface by:
  + Disabling the interface.
  + Changing the MAC address.
  + Enabling the interface again.

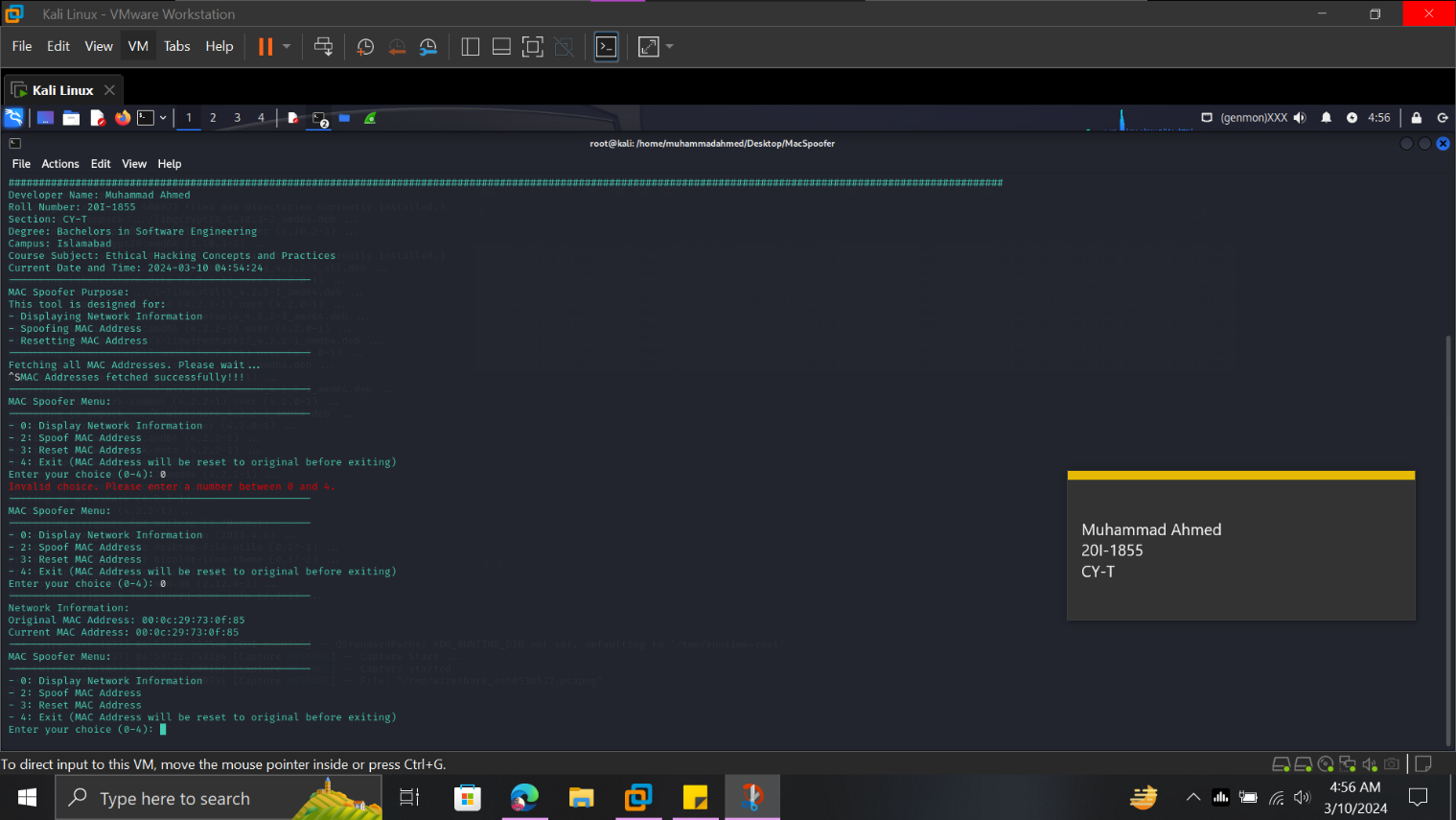
## **Dependencies**

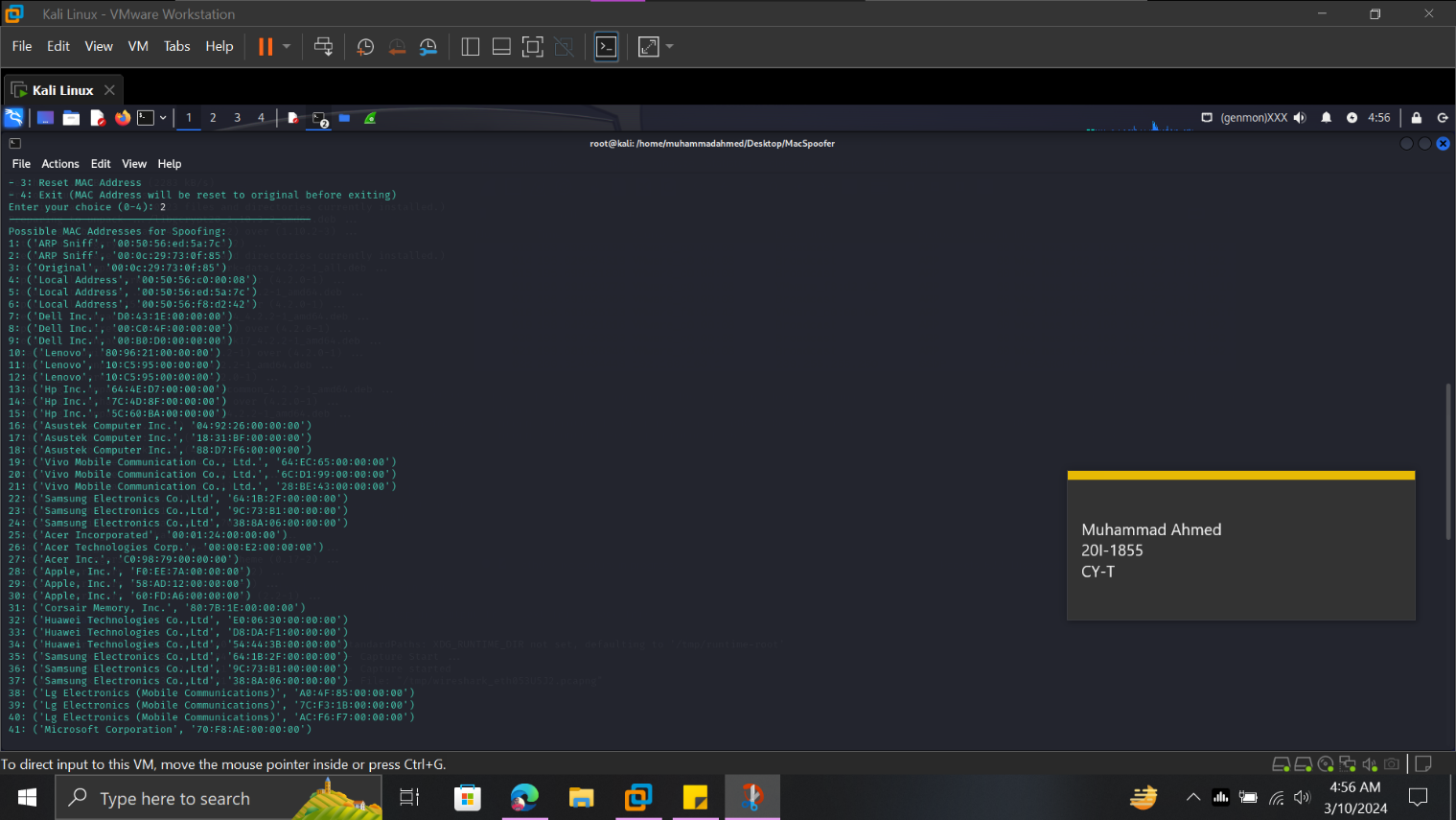
The tool relies on external libraries and commands, including:

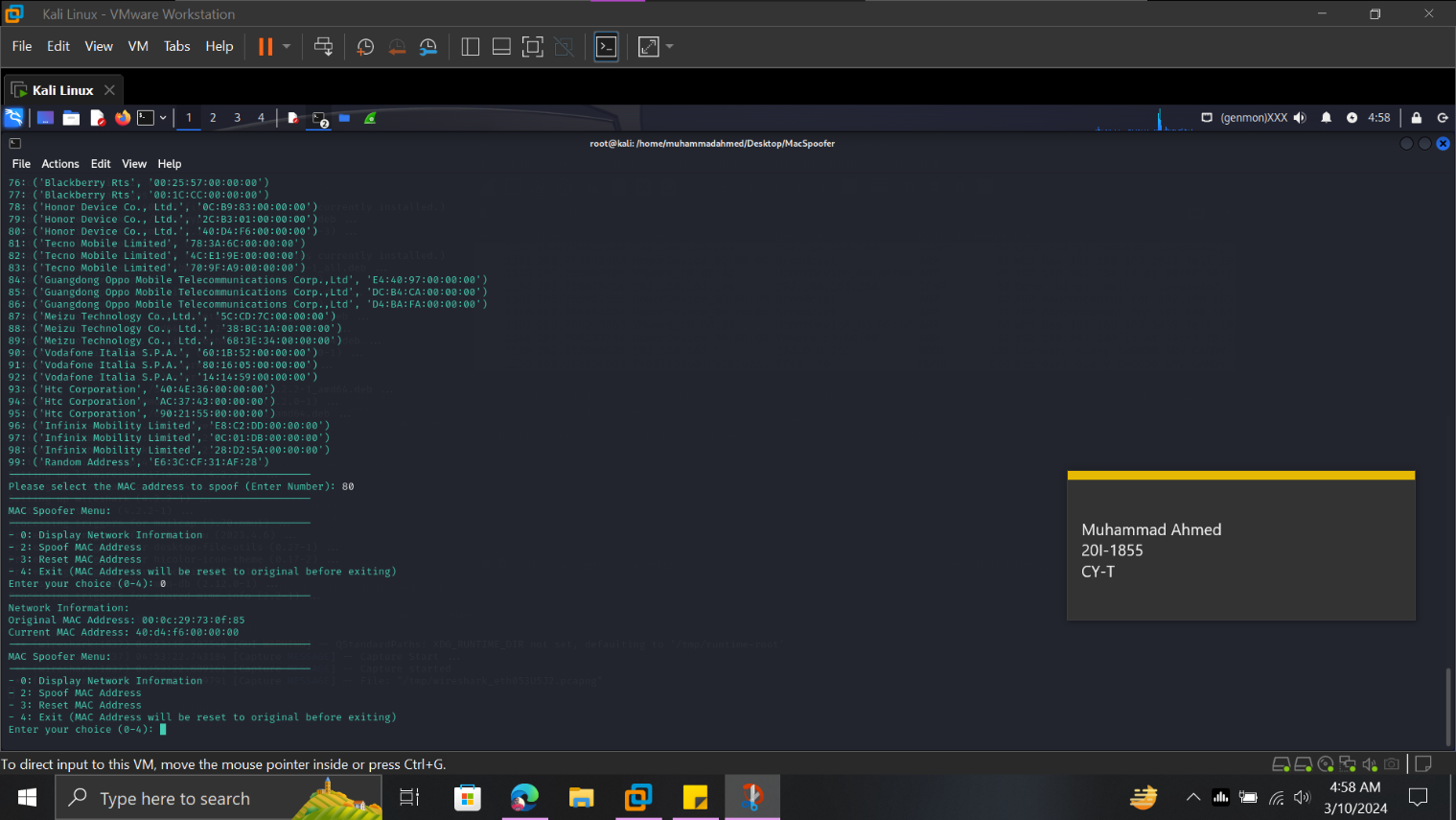
* “scapy” - packet manipulation
* “psutil” - system information retrieval
* “subprocess” - executing system commands
* “csv” - reading MAC addresses from a file

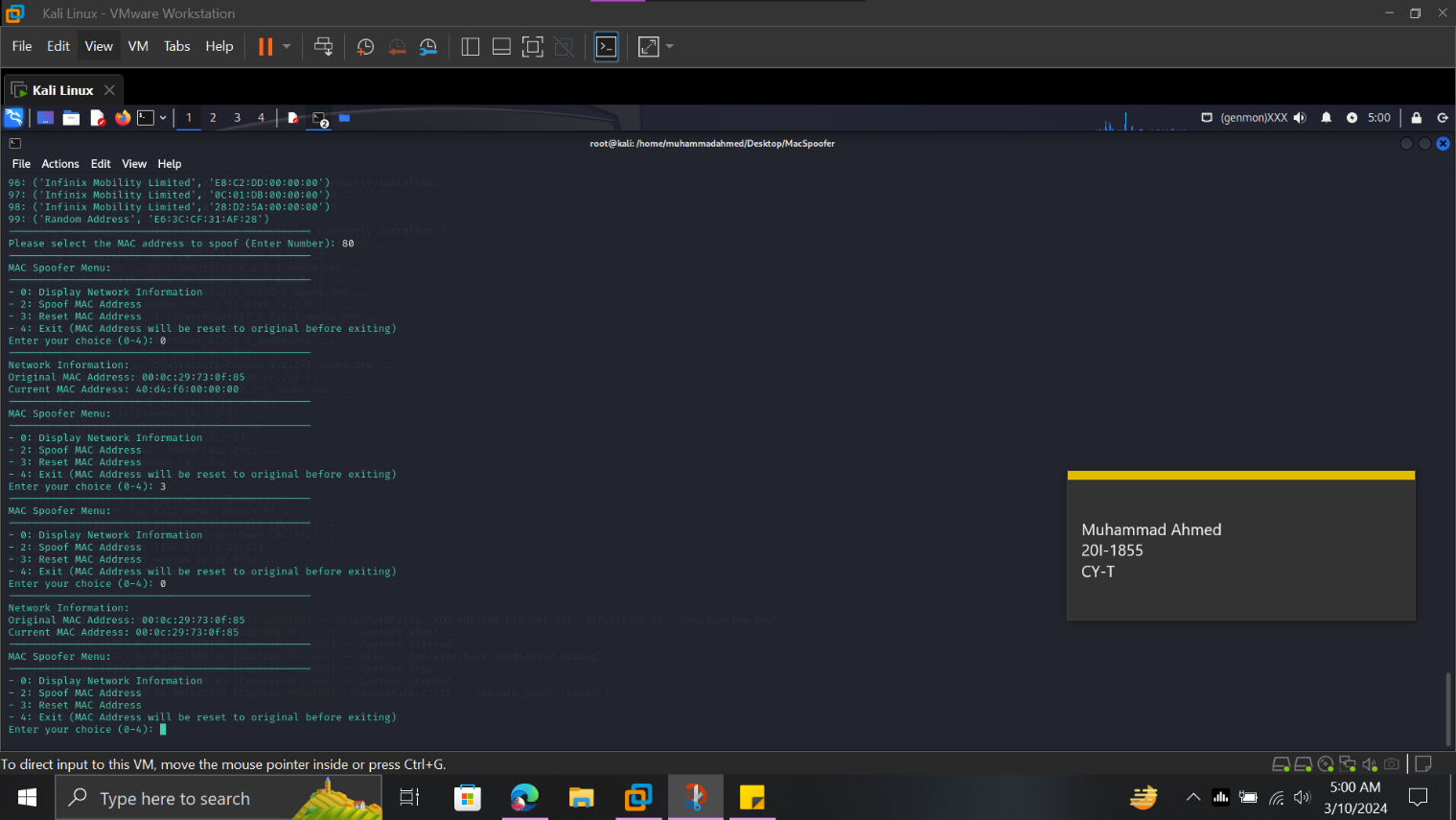
## **Code Terminal Screenshots**





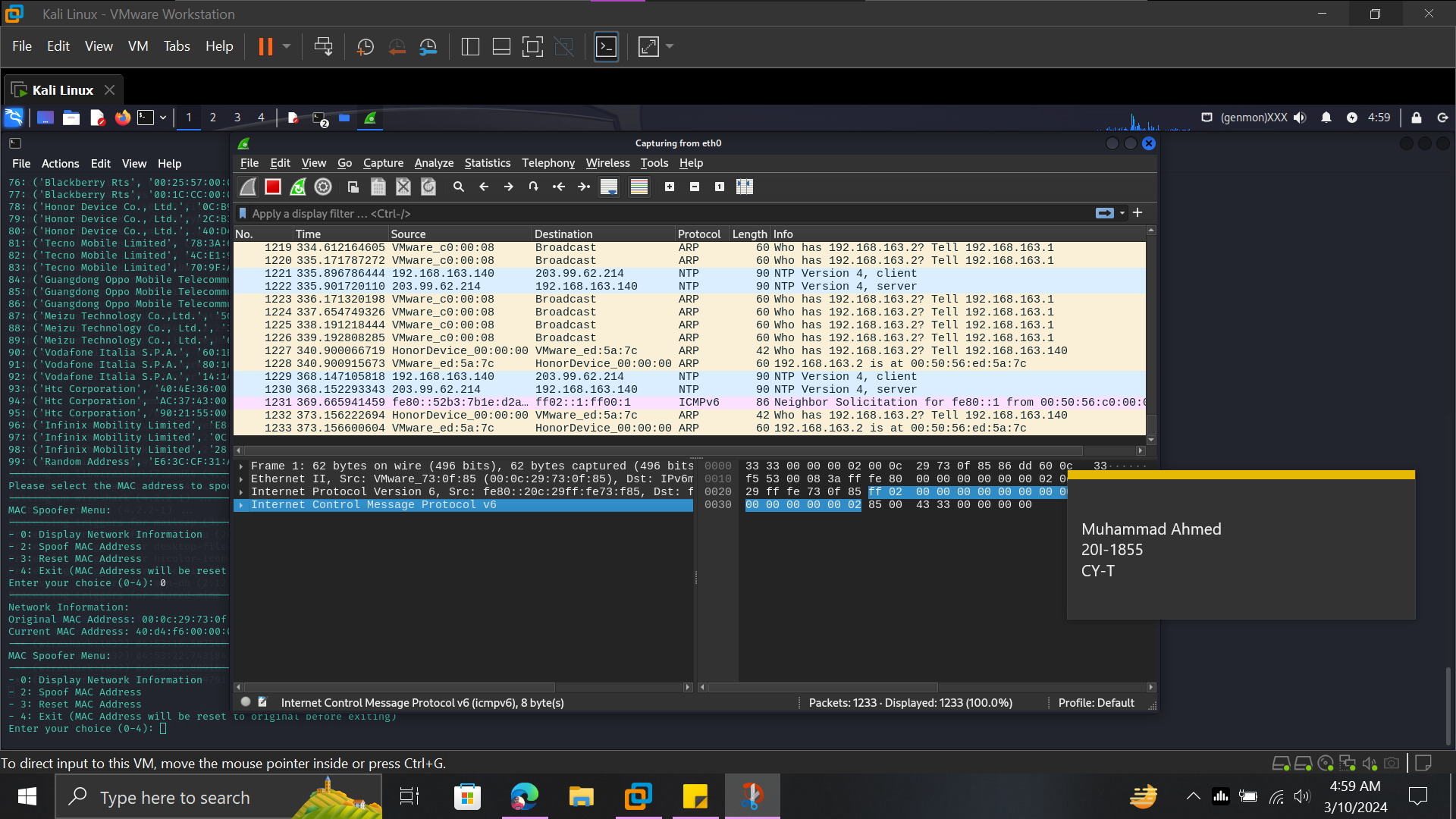






## **Wireshark Screenshots**

* Wireshark is running in the background.
* Python file is executed.
* MAC Address is spoofed.
  + MAC Address 80 is selected. (HONOR DEVICE MAC ADDRESS)
* This can be seen in this Wireshark screenshot.



## **Conclusion**

The MAC Spoofer tool provides a comprehensive and user-friendly interface for managing MAC addresses on a system. Developed as part of the Ethical Hacking Concepts and Practices course, the tool demonstrates key concepts related to network security and MAC address manipulation.