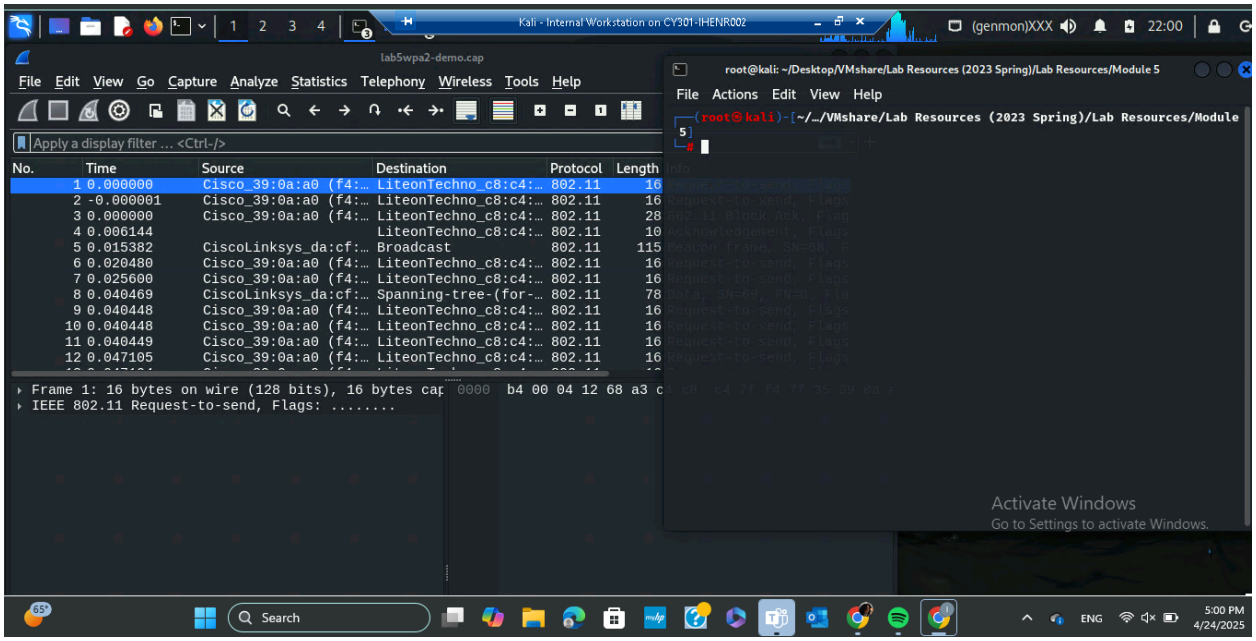
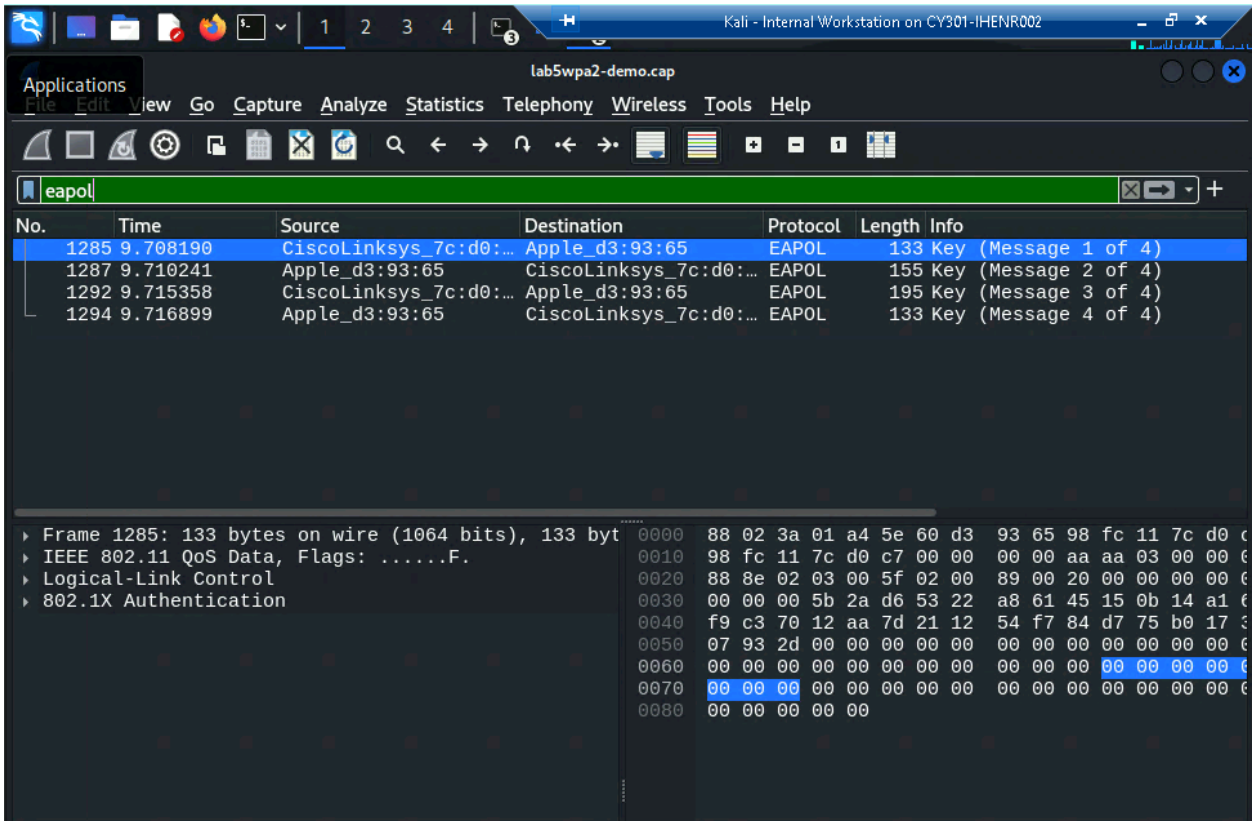
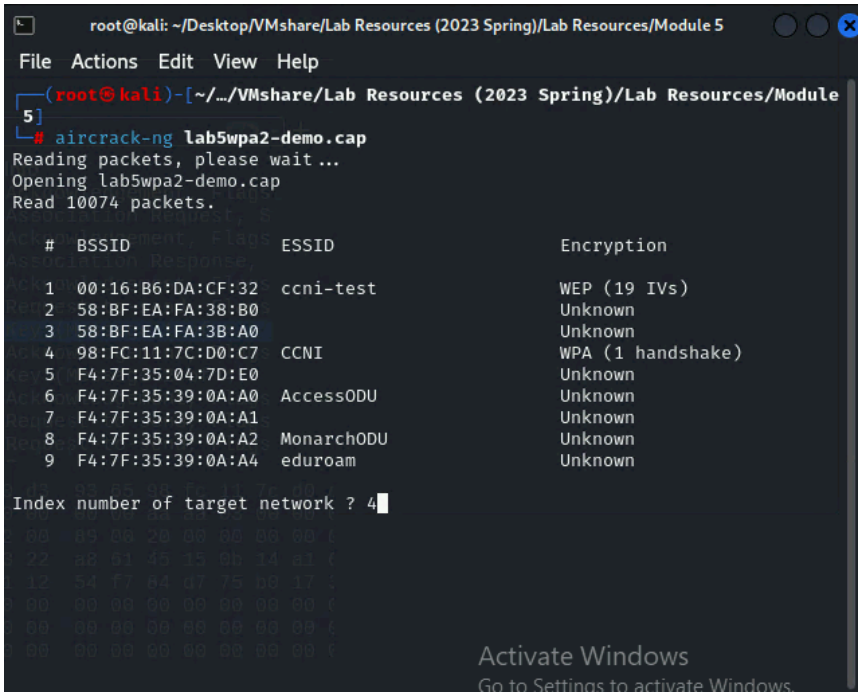
1. **Decrypt the lab4wpa2.cap file and perform a detailed traffic analysis**



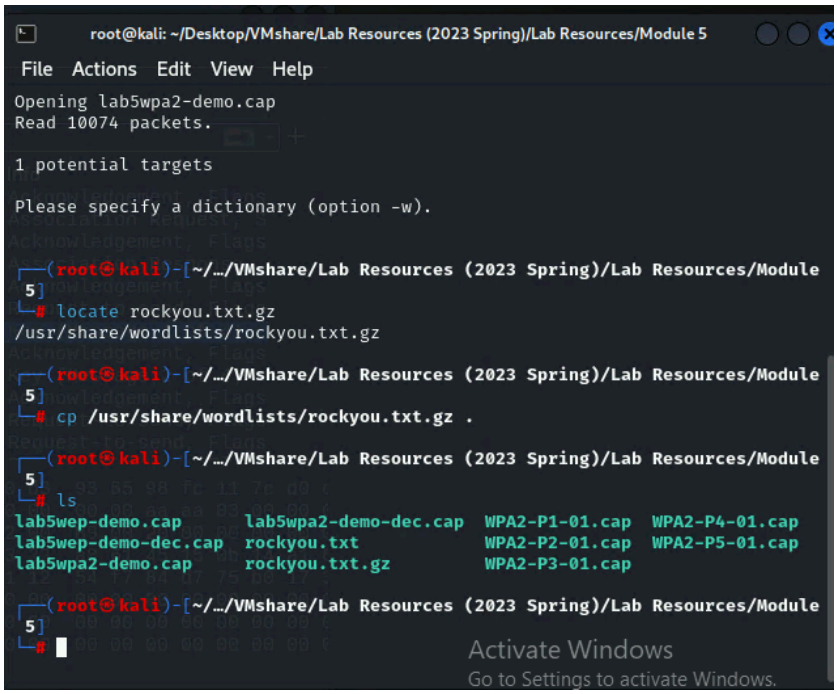
Opening the lab 5 WPA file for encrypted wireshark and terminal



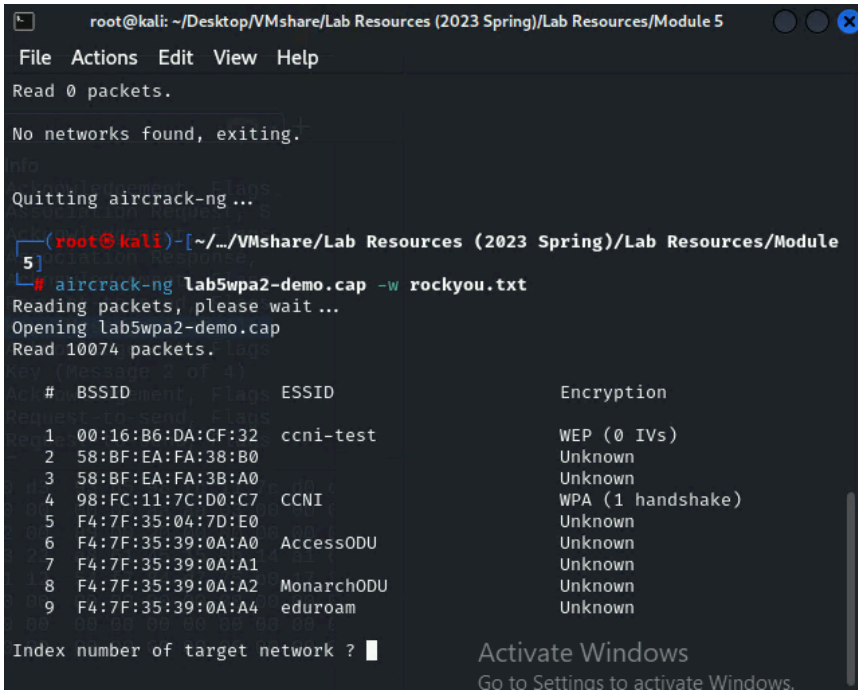
Filtering eapol to see the four-way handshake, which is the weakest point of the wifi connection

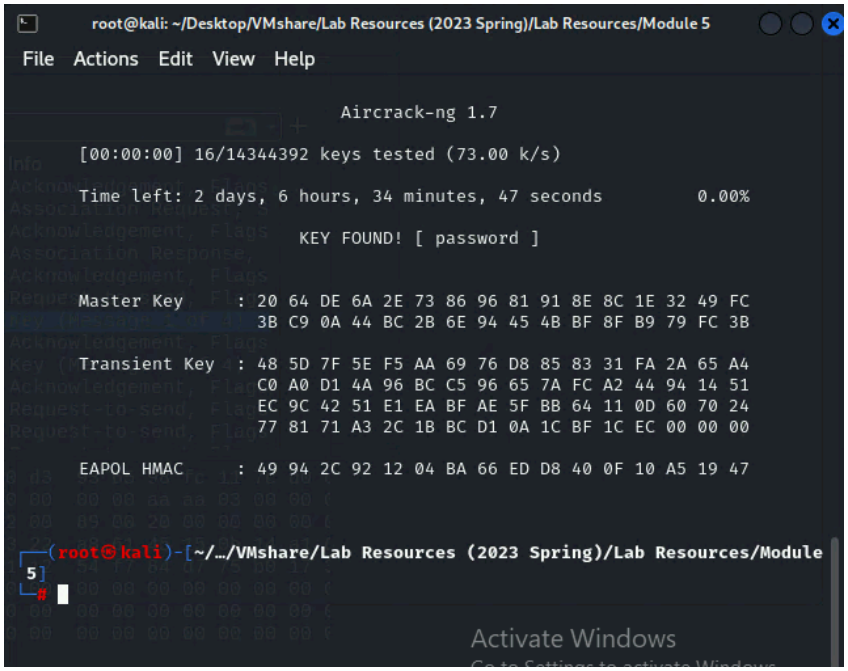


Using aircrack common and choosing the WPA target

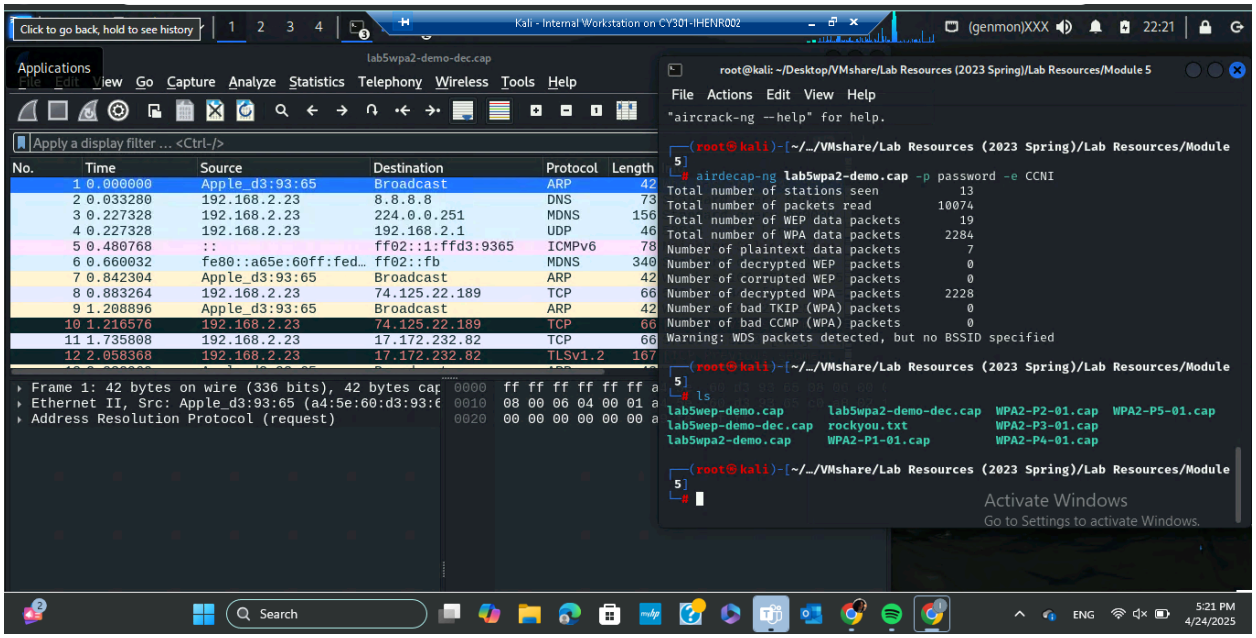


Locating the zipped rockyou file and copying it to the current directory



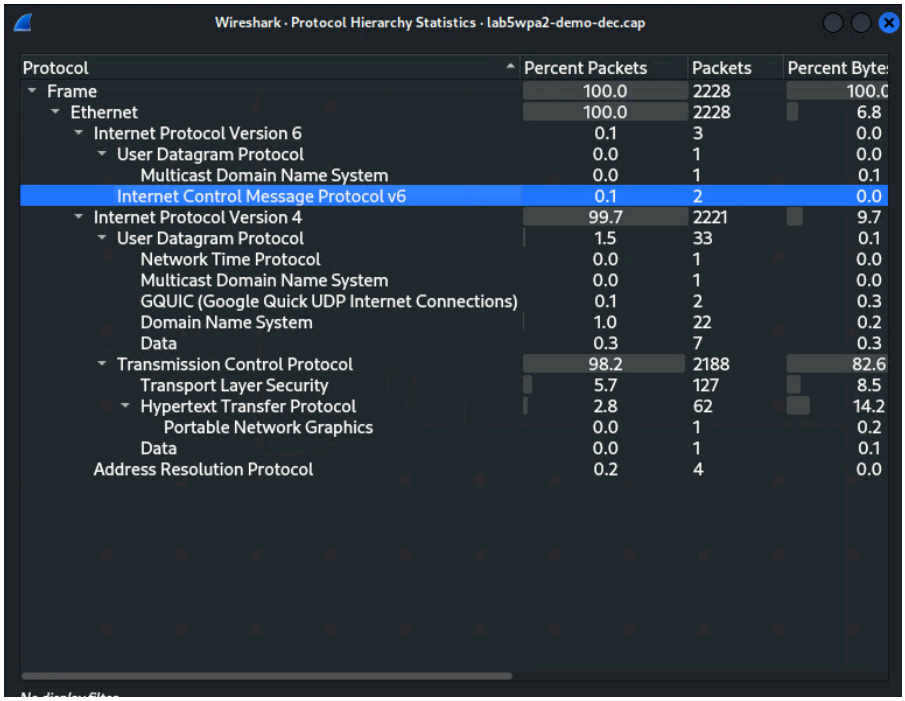


Unzipping the rockyou file, using aircrack command and choosing WPA; find the key: password



Using the airdecap command with the passcode to decrypt packets; using ls command to ensure the file is in the current directory; opening the decrypted wpa file.

With the traffic decrypted, we can see the communication between the packets



Most of the packets are ipv4 and tcp, which means most of the packets that are communicating are using ipv4 ip addresses and ensuring the reliable transmission of packets using tcp.