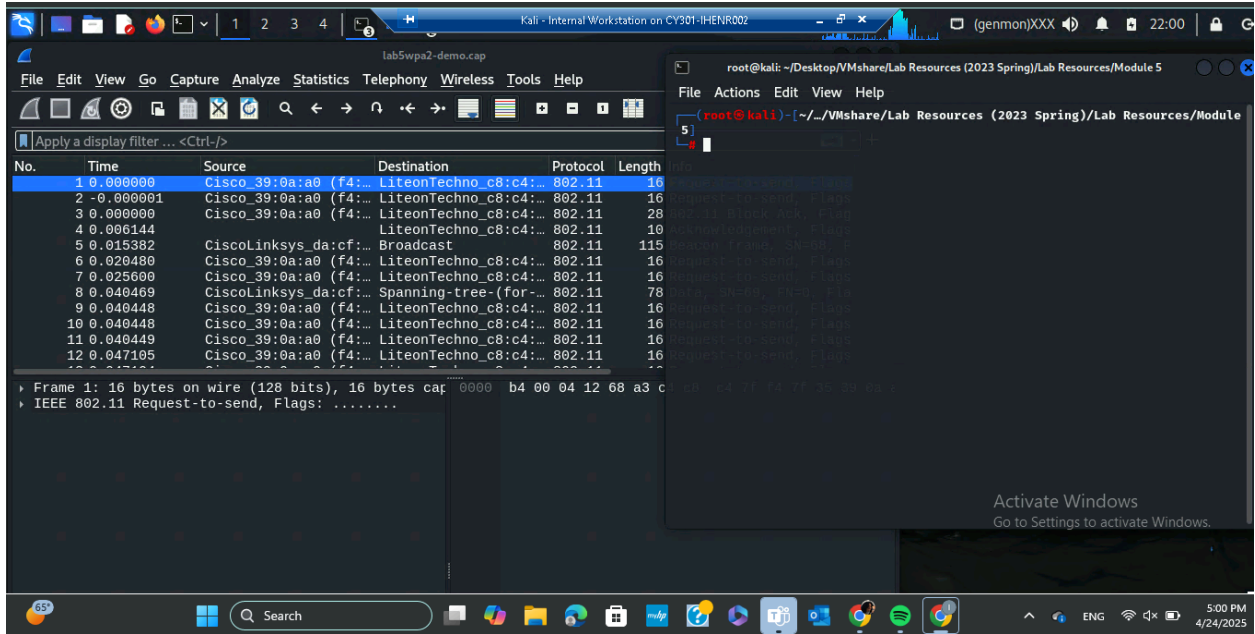
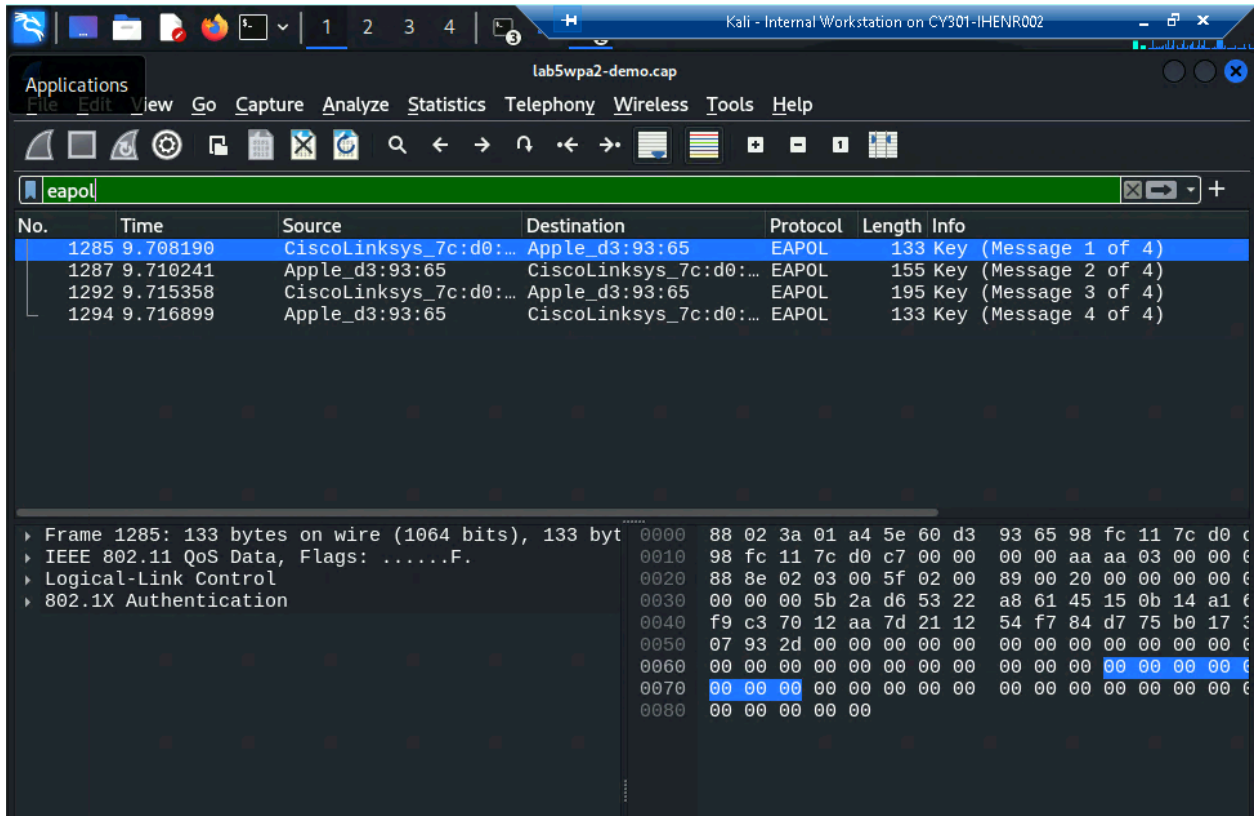


1. Decrypt the lab4wpa2.cap file and perform a detailed traffic analysis



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


```

root@kali: ~/Desktop/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5
File Actions Edit View Help
Read 0 packets.
No networks found, exiting.
Quit
Quitting aircrack-ng...

(root@kali)-[~/Desktop/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# aircrack-ng lab5wpa2-demo.cap -w rockyou.txt
Reading packets, please wait...
Opening lab5wpa2-demo.cap
Read 10074 packets.

# BSSID      Flag      ESSID      Encryption
1 00:16:B6:DA:CF:32  ccni-test  WEP (0 IVs)
2 58:BF:EA:FA:38:B0  Unknown
3 58:BF:EA:FA:3B:A0  Unknown
4 98:FC:11:7C:D0:C7  CCNI      WPA (1 handshake)
5 F4:7F:35:04:7D:E0  Unknown
6 F4:7F:35:39:0A:A0  AccessODU Unknown
7 F4:7F:35:39:0A:A1  Unknown
8 F4:7F:35:39:0A:A2  MonarchODU Unknown
9 F4:7F:35:39:0A:A4  eduroam   Unknown

Index number of target network ? █

```

```

root@kali: ~/Desktop/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5
File Actions Edit View Help

Aircrack-ng 1.7

[00:00:00] 16/14344392 keys tested (73.00 k/s)
Time left: 2 days, 6 hours, 34 minutes, 47 seconds 0.00%
KEY FOUND! [ password ]

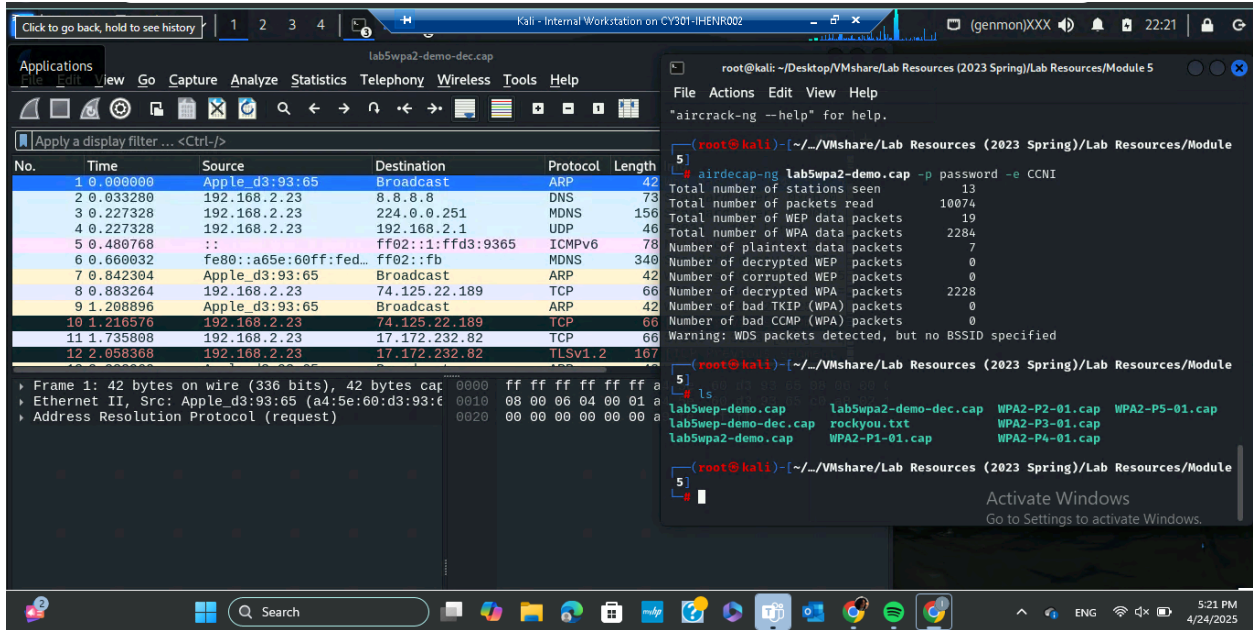
Master Key      : 20 64 DE 6A 2E 73 86 96 81 91 8E 8C 1E 32 49 FC
                  3B C9 0A 44 BC 2B 6E 94 45 4B BF 8F B9 79 FC 3B

Transient Key   : 48 5D 7F 5E F5 AA 69 76 D8 85 83 31 FA 2A 65 A4
                  C0 A0 D1 4A 96 BC C5 96 65 7A FC A2 44 94 14 51
                  EC 9C 42 51 E1 EA BF AE 5F BB 64 11 0D 60 70 24
                  77 81 71 A3 2C 1B BC D1 0A 1C BF 1C EC 00 00 00

EAPOL HMAC     : 49 94 2C 92 12 04 BA 66 ED D8 40 0F 10 A5 19 47

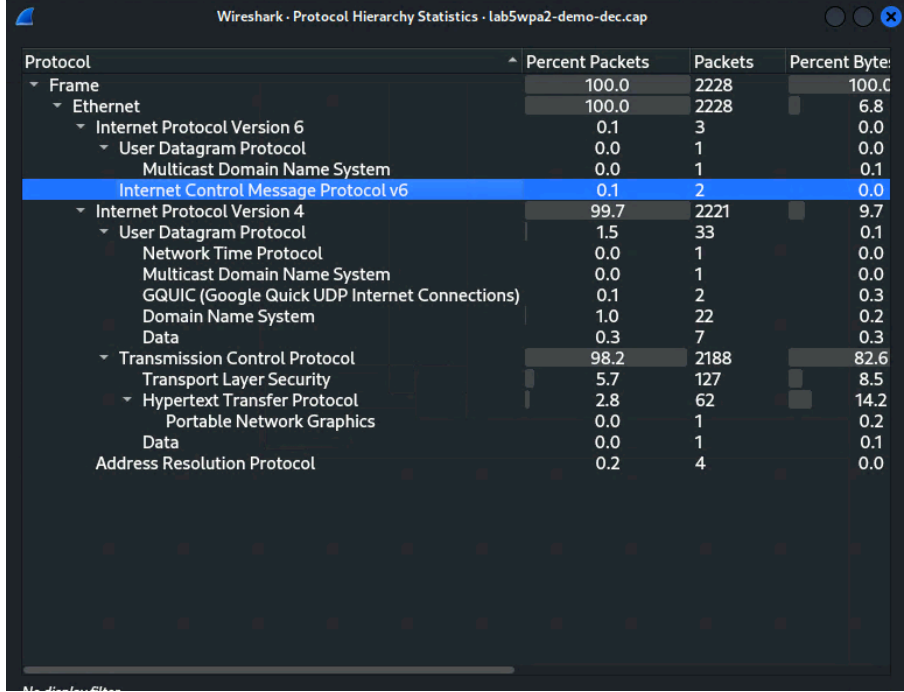
```

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.