Title: Network Traffic Analysis Using Wireshark

Objective

To capture live network packets and identify basic network protocols.

Tool Used

Wireshark

Procedure

(Briefly summarize the steps you followed.)

Protocols Identified

1. DNS

- Used for domain name resolution.
- Observed query to google.com.
- Uses UDP port 53.

2. TCP

- Transport layer protocol.
- Provides reliable communication.
- Observed TCP handshake (SYN, SYN-ACK, ACK).

3. TLS

- Used for secure communication (HTTPS).
- Encrypts website traffic.

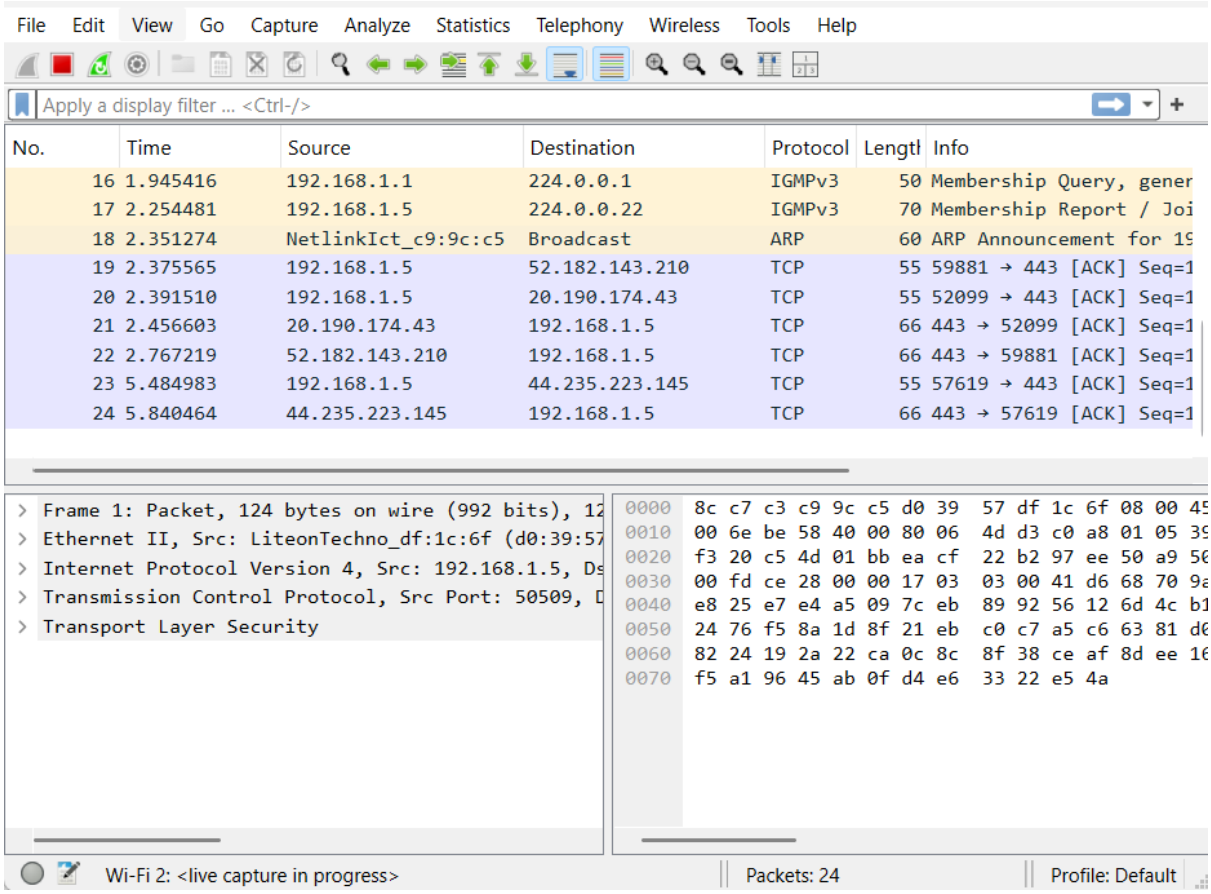
4. ICMP

- Used for ping.
- Observed echo request and reply.

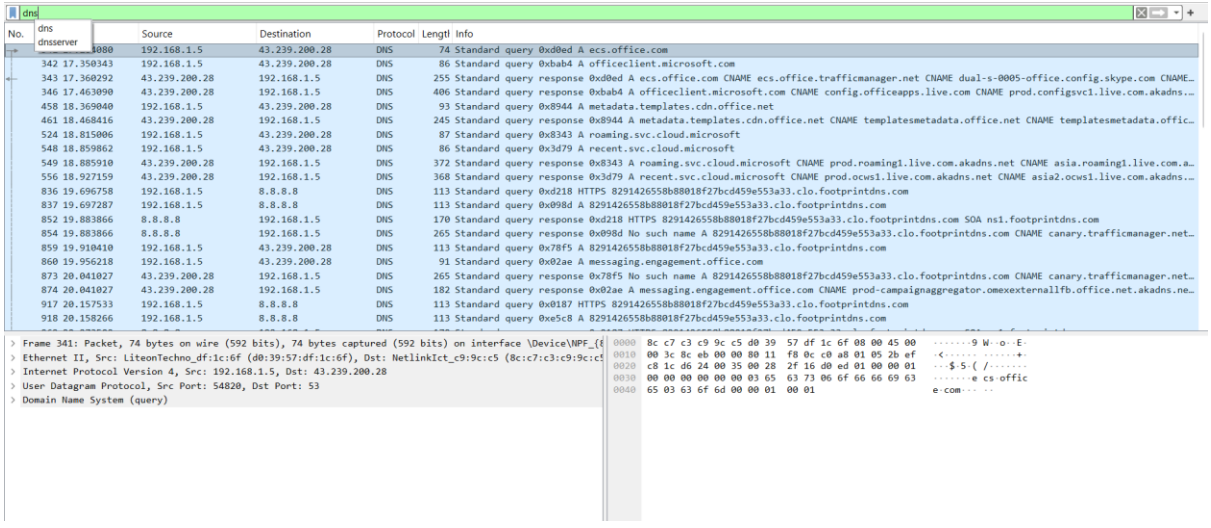
5. Observations

- Large number of TCP packets observed.
- DNS queries precede website loading.
- HTTPS traffic encrypted using TLS.

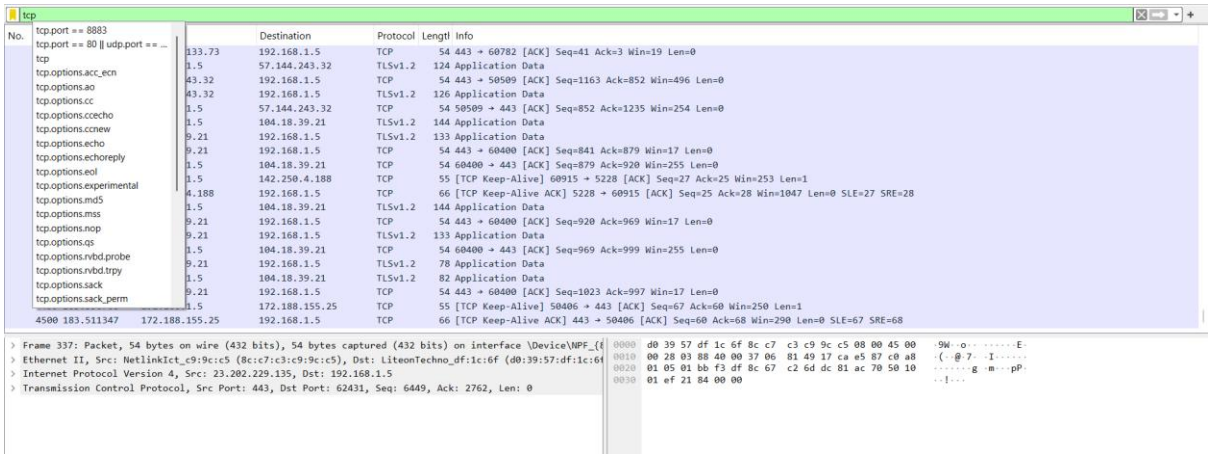
We get into the wireshark tools and use the wifi port



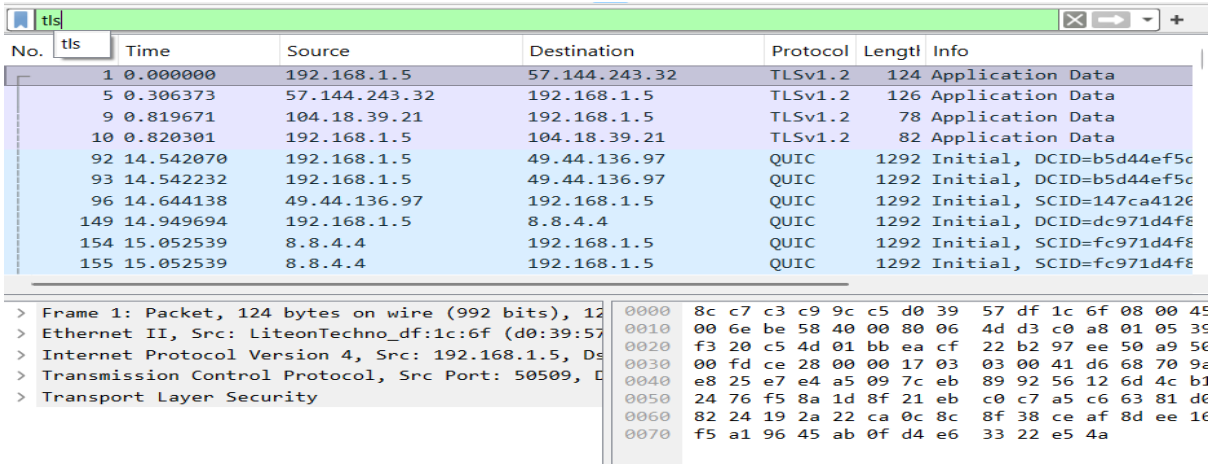
DNS Packet Captured :



TCP Packet Captured :



TLS Packet Captured :



ICMP Packet Captured :