Elevate Labs- Cyber security - Task 3

Network Traffic Analysis Using Wireshark

Objective:
To capture and analyze live network traffic to understand protocols and security aspects.

Basics of Computer networks learnt:

- **IP Address** → Identifies a device (like home address)
- **MAC Address** → Hardware identity of network card
- **DNS** → Converts website name → IP address
- **TCP** → Reliable connection (websites, login)
- **UDP** → Fast but no guarantee (DNS, video)

Downloaded Wireshark from internet and learned about its uses and key notes:

Observations:

- **Captured live network traffic using Wireshark**
- **Packet Capture Process**

Wireshark was installed and launched on the system. The Wi-Fi network interface was selected, and live packet capture was started. During the capture, websites were accessed to generate

- **Protocol Filtering**

The following filters were used in Wireshark:

- **TCP:** `tcp`
- **UDP:** `udp`
- **DNS:** `dns`
- **HTTP:** `http`
- **TLS (HTTPS):** `tls`

- Observed TCP three-way handshake (SYN, SYN-ACK, ACK)
- DNS queries resolved domain names to IP addresses

- **DNS Traffic Analysis**

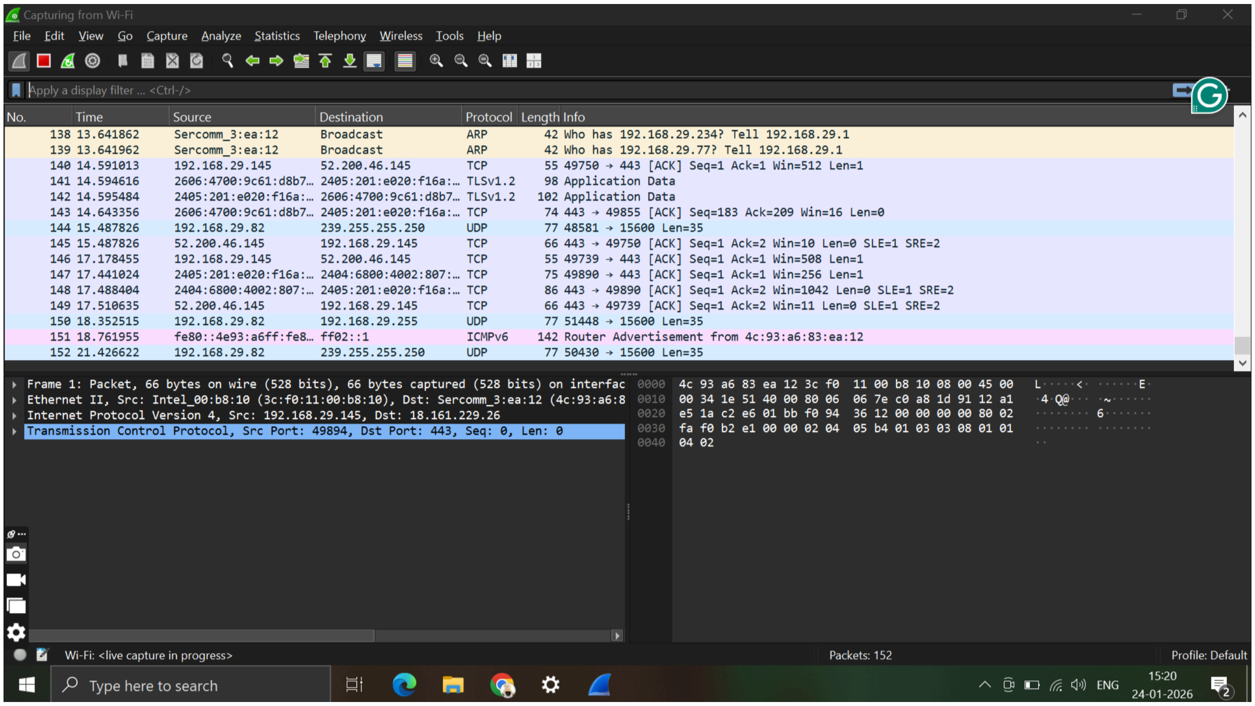
DNS packets were captured while accessing websites.
The following observations were made:

- DNS queries request the IP address of a domain name
- DNS responses contain the resolved IP address
- DNS traffic mainly uses the UDP protocol

- **Packet Capture File**

The captured network traffic was saved using Wireshark in the `.pcapng` format for further analysis.

File Name:analysis.pcapng



```
No.   Time        Source                 Destination            Protocol Length Info
  138 13.641862   Sercomm_3:ea:12        Broadcast              ARP       42 Who has 192.168.29.234? Tell 192.168.29.1
  139 13.641962   Sercomm_3:ea:12        Broadcast              ARP       42 Who has 192.168.29.77? Tell 192.168.29.1
  140 14.591013   192.168.29.145         52.200.46.145          TCP       55 49750 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1
  141 14.594616   2606:4700:9c61:d8b7…   2405:201:e020:f16a:…   TLSv1.2   98 Application Data
  142 14.595484   2405:201:e020:f16a:…   2606:4700:9c61:d8b7…   TLSv1.2  102 Application Data
  143 14.643356   2606:4700:9c61:d8b7…   2405:201:e020:f16a:…   TCP       74 443 → 49855 [ACK] Seq=183 Ack=209 Win=16 Len=0
  144 15.487826   192.168.29.82          239.255.255.250        UDP       77 48581 → 15600 Len=35
  145 15.487826   52.200.46.145          192.168.29.145         TCP       66 443 → 49750 [ACK] Seq=1 Ack=2 Win=10 Len=0 SLE=1 SRE=2
  146 17.178455   192.168.29.145         52.200.46.145          TCP       55 49739 → 443 [ACK] Seq=1 Ack=1 Win=508 Len=1
  147 17.441024   2405:201:e020:f16a:…   2404:6800:4002:807:…   TCP       75 49890 → 443 [ACK] Seq=1 Ack=1 Win=256 Len=1
  148 17.488404   2404:6800:4002:807:…   2405:201:e020:f16a:…   TCP       86 443 → 49890 [ACK] Seq=1 Ack=2 Win=1042 Len=0 SLE=1 SRE=2
  149 17.510635   52.200.46.145          192.168.29.145         TCP       66 443 → 49739 [ACK] Seq=1 Ack=2 Win=11 Len=0 SLE=1 SRE=2
  150 18.352515   192.168.29.82          192.168.29.255         UDP       77 51448 → 15600 Len=35
  151 18.761955   fe80::4e93:a6ff:fe8…   ff02::1                ICMPv6   142 Router Advertisement from 4c:93:a6:83:ea:12
  152 21.426622   192.168.29.82          239.255.255.250        UDP       77 50430 → 15600 Len=35
```

```
> Frame 1: Packet, 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interfac
> Ethernet II, Src: Intel_00:b8:10 (3c:f0:11:00:b8:10), Dst: Sercomm_3:ea:12 (4c:93:a6:8
> Internet Protocol Version 4, Src: 192.168.29.145, Dst: 18.161.229.26
> Transmission Control Protocol, Src Port: 49894, Dst Port: 443, Seq: 0, Len: 0
```

```
0000  4c 93 a6 83 ea 12 3c f0  11 00 b8 10 08 00 45 00   L·····<· ······E·
0010  00 34 1e 51 40 00 80 06  06 7e c0 a8 1d 91 12 a1   ·4·Q@··· ·~······
0020  e5 1a c2 e6 01 bb f0 94  36 12 00 00 00 00 80 02   ········ 6·······
0030  fa f0 b2 e1 00 00 02 04  05 b4 01 03 03 08 01 01   ········ ········
0040  04 02                                              ··
```

Wi-Fi: <live capture in progress>   Packets: 152   Profile: Default