Task-5: Packet Capture and Analysis using Wireshark

Tools Used

- **Operating System**: Kali Linux
- **Network Analyzer**: Wireshark

Steps Performed

1. Installed Wireshark

sudo apt update

sudo apt install wireshark -y

Launched Wireshark using:

sudo wireshark

2. Started Capture on Active Interface

- Opened Wireshark GUI.
- Selected active interface (eth0/wlan0).
- Clicked the **Start Capture** (shark fin icon).

3. Generated Network Traffic

- Opened a web browser and visited https://example.com.
- Ran ping google.com in terminal to generate ICMP and DNS traffic.

4. Stopped Capture

- Stopped capture after one minute using the red square **Stop button**.

5. Filtered Captured Packets

Applied filters in the top filter bar:

- dns → Showed DNS packets
- http → Showed HTTP requests
- tcp → Showed all TCP traffic

6. Identified 3 Protocols

Observed at least three different protocols:

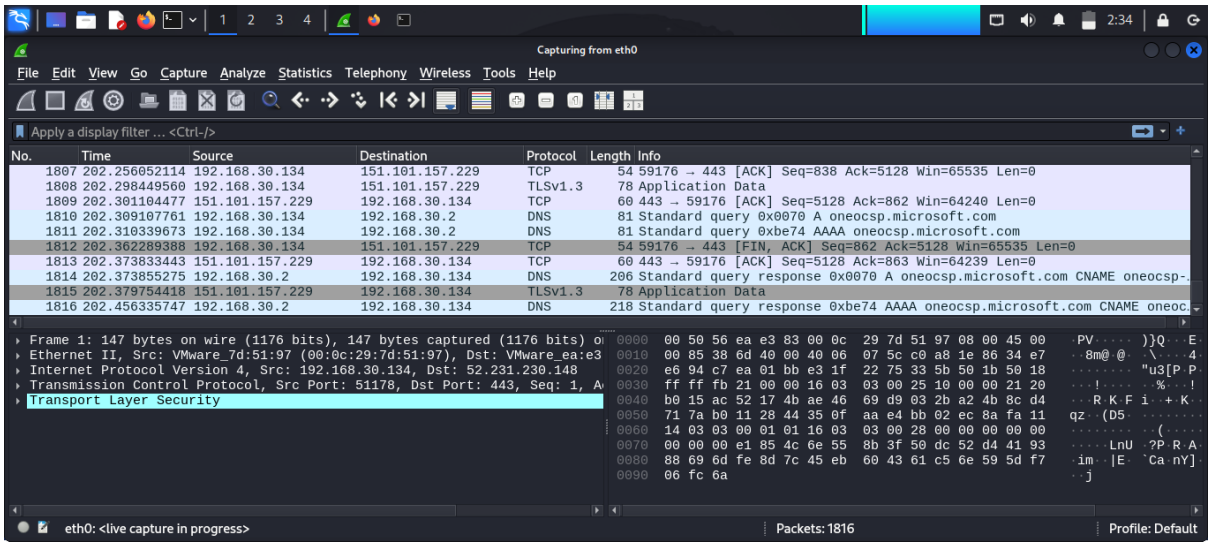
- **DNS** – Domain resolution traffic
- **TCP** – Transport layer communication
- **HTTP** – Website request and response

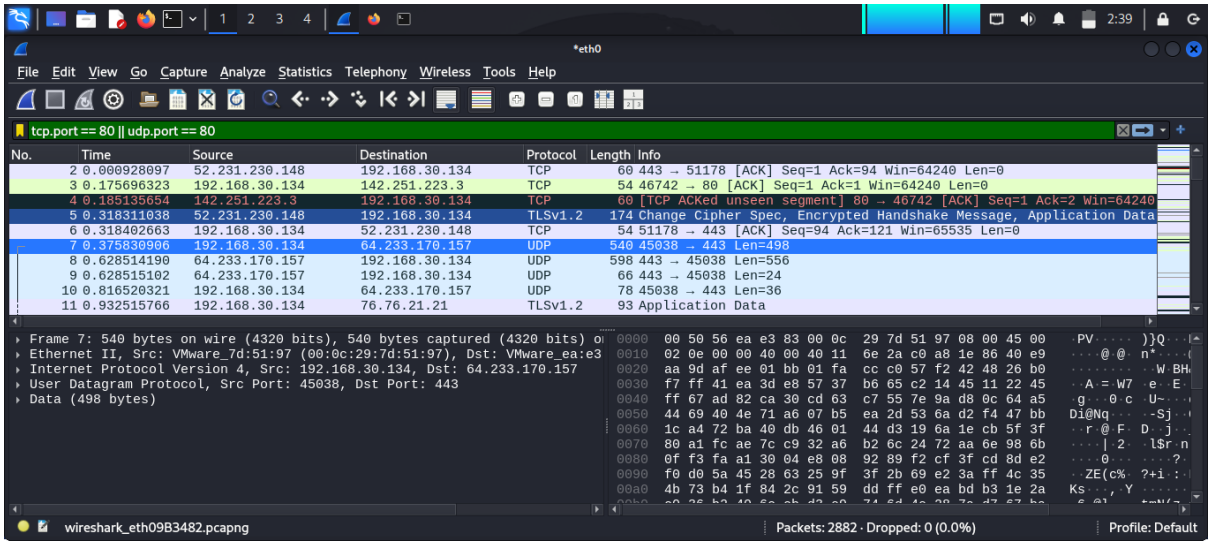
Screenshot taken showing protocol column with all three.

7. Exported Capture as .pcap File

- File → Export Specified Packets...
- Saved as my_capture.pcap in default location

Output:




*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 80 || udp.port == 80
No. Time Source Destination Protocol Length Info
2 0.000928097 52.231.230.148 192.168.30.134 TCP 60 443 → 51178 [ACK] Seq=1 Ack=94 Win=64240 Len=0
3 0.175696323 192.168.30.134 142.251.223.3 TCP 54 46742 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4 0.185135654 142.251.223.3 192.168.30.134 TCP 60 [TCP ACKed unseen segment] 80 → 46742 [ACK] Seq=1 Ack=2 Win=64240
5 0.318311038 52.231.230.148 192.168.30.134 TLSv1.2 174 Change Cipher Spec, Encrypted Handshake Message, Application Data
6 0.318402663 192.168.30.134 52.231.230.148 TCP 54 51178 → 443 [ACK] Seq=94 Ack=121 Win=65535 Len=0
7 0.375830906 192.168.30.134 64.233.170.157 UDP 540 45038 → 443 Len=498
8 0.628514190 64.233.170.157 192.168.30.134 UDP 598 443 → 45038 Len=556
9 0.628515102 64.233.170.157 192.168.30.134 UDP 66 443 → 45038 Len=24
10 0.816520321 192.168.30.134 64.233.170.157 UDP 78 45038 → 443 Len=36
11 0.932515766 192.168.30.134 76.76.21.21 TLSv1.2 93 Application Data
Frame 7: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) o
Ethernet II, Src: VMware_7d:51:97 (00:0c:29:7d:51:97), Dst: VMware_ea:e3
Internet Protocol Version 4, Src: 192.168.30.134, Dst: 64.233.170.157
User Datagram Protocol, Src Port: 45038, Dst Port: 443
Data (498 bytes)
0000 00 50 56 ea e3 83 00 0c 29 7d 51 97 08 00 45 00
0010 02 0e 00 00 40 00 40 11 6e 2a c0 a8 1e 86 40 e9
0020 aa 9d af ee 01 bb 01 fa cc c0 57 f2 42 48 26 b0
0030 f7 ff 41 ea 3d e8 57 37 b6 65 c2 14 45 11 22 45
0040 ff 67 ad 82 ca 30 cd 63 c7 55 7e 9a d8 0c 64 a5
0050 44 69 40 4e 71 a6 07 b5 ea 2d 53 6a d2 f4 47 bb
0060 1c a4 72 ba 40 db 46 01 44 d3 19 6a 1e cb 5f 3f
0070 80 a1 fc ae 7c c9 32 a6 b2 6c 24 72 aa 6e 98 6b
0080 0f f3 fa a1 30 04 e8 08 92 89 f2 cf 3f cd 8d e2
0090 f0 d0 5a 45 28 63 25 9f 3f 2b 69 e2 3a ff 4c 35
00a0 4b 73 b4 1f 84 2c 91 59 dd ff e0 ea bd b3 1e 2a
wireshark_eth09B3482.pcapng
Packets: 2882 · Dropped: 0 (0.0%)
Profile: Default