Experiment No: AV-341-2025-Lab-3
Capture and Analysis of Network Packets

Saurabh Kumar
SC22B146
February 18, 2025

Date and Time of experiment: February 10, 2025, 14:45 IST

Objectives

- To capture packets from wireless/wired network and analyze the captured packet traffic, including parameters like average packets per second, average packet length, length distribution and inter-arrival times.

Tools Used

- PC: 12th Gen Intel(R) Core(TM) i5-1240P 1.70 GHz, Windows 11, 64-bit, (Reduced to) 4 GB RAM
- Software used: Wireshark

Procedure

1. Open Wireshark on Windows PC.

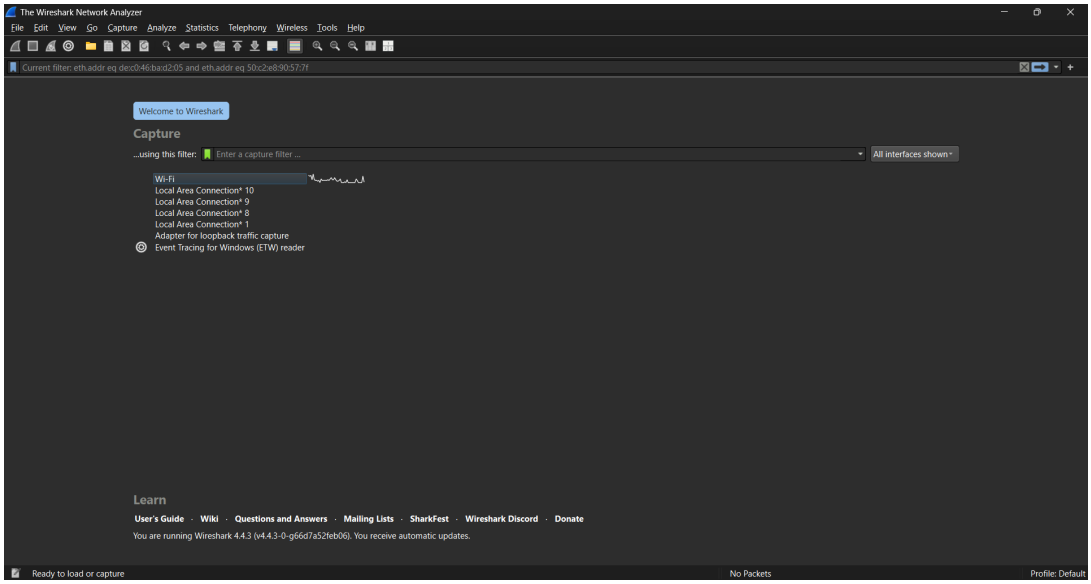


Figure 1: Wireshark welcome screen

2. Click on a connection option to start packets capturing (e.g., Wi-Fi).

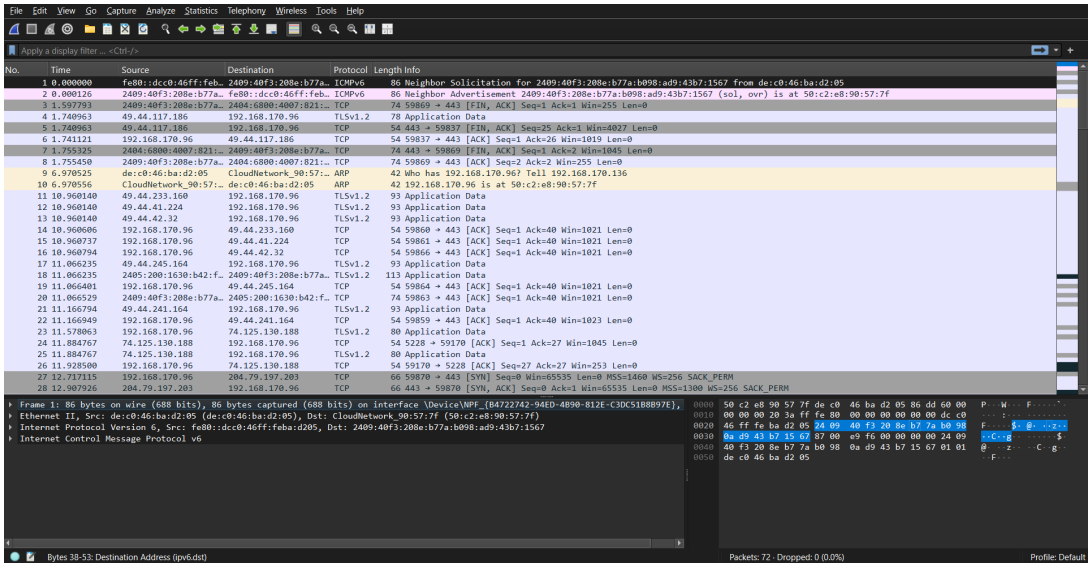


Figure 2: WiFi packet capturing

The packets search result are shown in tabular form with each packet shown in a row. The information shown are time (starting from 0) of packet receive, source and destination of the packet, protocol used, packet length (size) and other information.

3. Click on a frame to get its packet information.

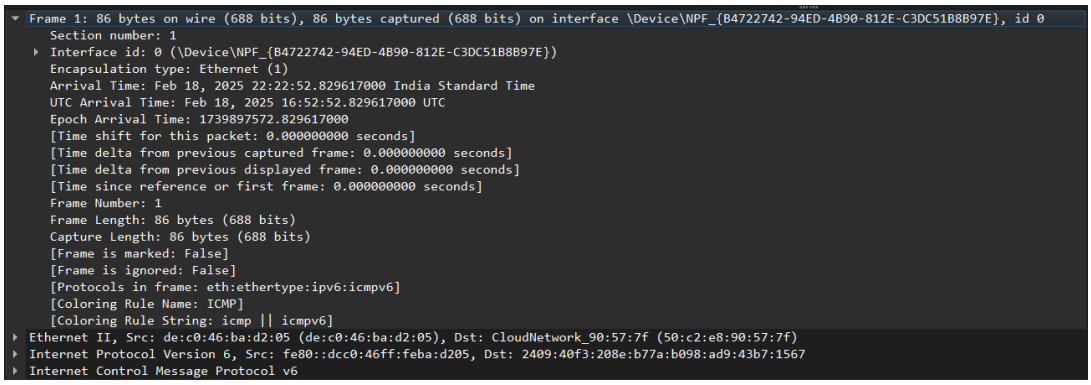
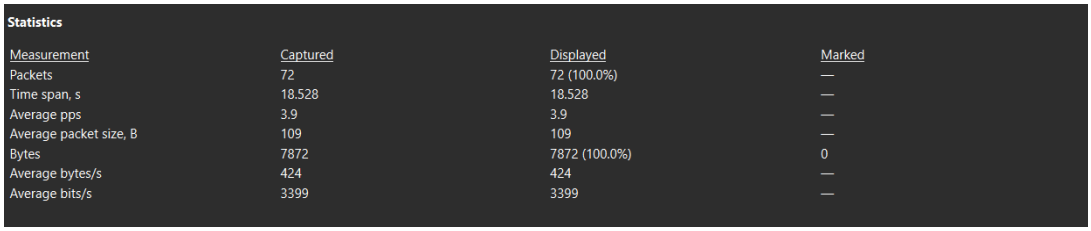


Figure 3: Frame analysis

4. *Statistics* tab contains various stats about the packets captured. Go to *Statistics* → *CaptureFileProperties* to get information about the overall capture statistics.



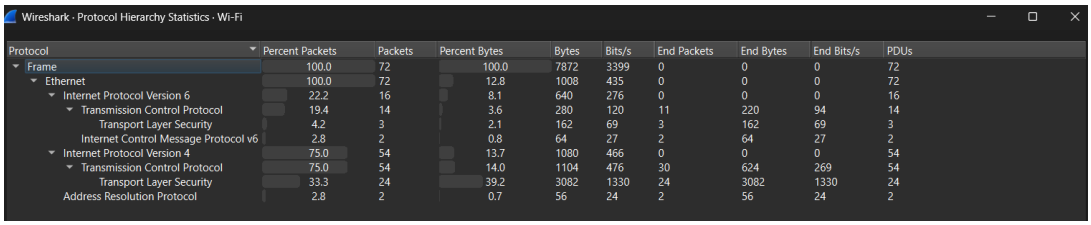
Statistics

Measurement	Captured	Displayed	Marked
Packets	72	72 (100.0%)	—
Time span, s	18.528	18.528	—
Average pps	3.9	3.9	—
Average packet size, B	109	109	—
Bytes	7872	7872 (100.0%)	0
Average bytes/s	424	424	—
Average bits/s	3399	3399	—

Figure 4: Packet File Properties

It shows information like number of packets, time span, average packets per second, average packet size, total bytes and average bytes/s.

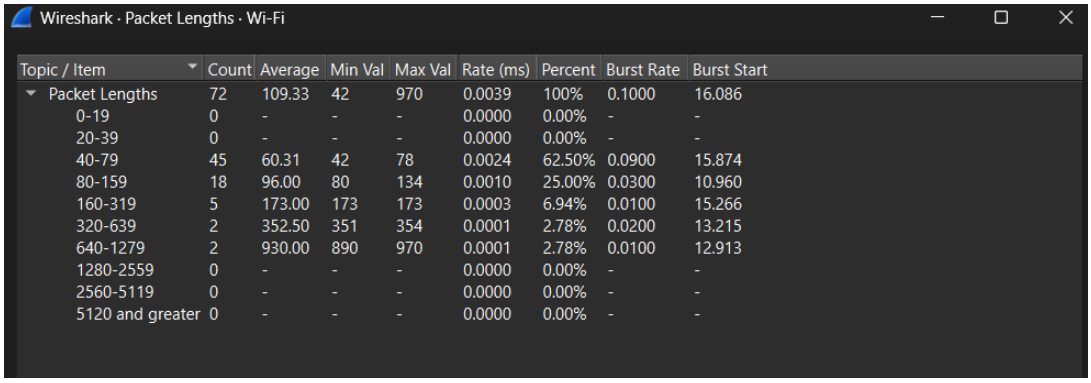
5. *Statistics* → *ProtocolHierarchy*



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	72	100.0	7872	3399	0	0	0	72
Ethernet	100.0	72	12.8	1008	435	0	0	0	72
Internet Protocol Version 6	22.2	16	8.1	640	276	0	0	0	16
Transmission Control Protocol	19.4	14	3.6	280	120	11	220	94	14
Transport Layer Security	4.2	3	2.1	162	69	3	162	69	3
Internet Control Message Protocol v6	2.8	2	0.8	64	27	2	64	27	2
Internet Protocol Version 4	75.0	54	13.7	1080	466	0	0	0	54
Transmission Control Protocol	75.0	54	14.0	1104	476	30	624	269	54
Transport Layer Security	33.3	24	39.2	3082	1330	24	3082	1330	24
Address Resolution Protocol	2.8	2	0.7	56	24	2	56	24	2

Figure 5: Protocol Hierarchy

6. *Statistics* → *PacketLengths*



Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Packet Lengths	72	109.33	42	970	0.0039	100%	0.1000	16.086
0-19	0	-	-	-	0.0000	0.00%	-	-
20-39	0	-	-	-	0.0000	0.00%	-	-
40-79	45	60.31	42	78	0.0024	62.50%	0.0900	15.874
80-159	18	96.00	80	134	0.0010	25.00%	0.0300	10.960
160-319	5	173.00	173	173	0.0003	6.94%	0.0100	15.266
320-639	2	352.50	351	354	0.0001	2.78%	0.0200	13.215
640-1279	2	930.00	890	970	0.0001	2.78%	0.0100	12.913
1280-2559	0	-	-	-	0.0000	0.00%	-	-
2560-5119	0	-	-	-	0.0000	0.00%	-	-
5120 and greater	0	-	-	-	0.0000	0.00%	-	-

Figure 6: Packet Lengths

7. *Statistics* → *I/OGraphs*

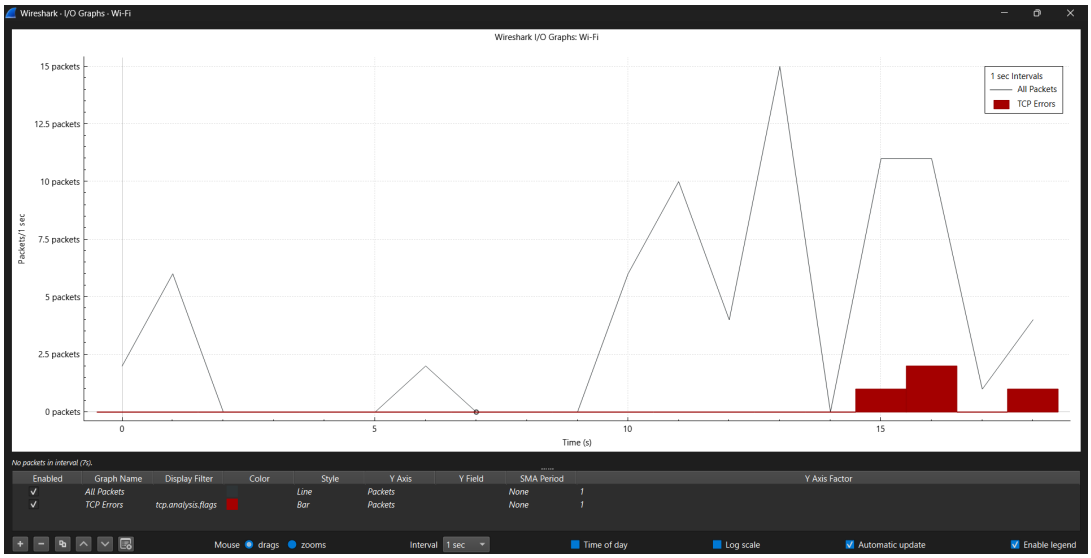


Figure 7: I/O Graphs

8. Additionally, filters can be applied to filter the packet search result.

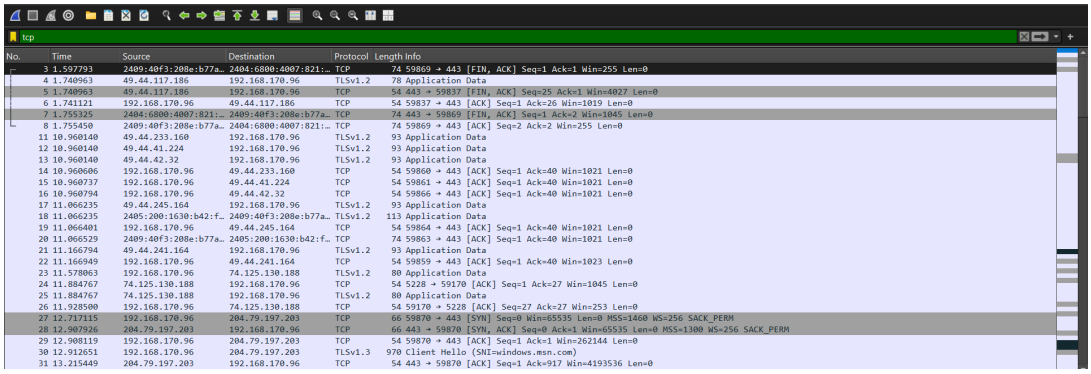


Figure 8: TCP filter applied

Observations

- Using Wireshark, network traffic through the device can be analyzed through the following parameters.
  - `Time`: Time elapsed since the packet search started.
  - `Source`: Source address of the packet.
  - `Destination`: Destination address of the packet.
  - `Protocol`: Protocol used for the communication, like TCP, UDP.
  - `Length`: Length of the packet in bytes.
  - Other stats can be viewed from the Statistics tab as shown above.
- The packet are displayed in real-time and can be started/stoped at any time.
- The packet rows are colour coded according to the protocol used, etc, as defined in the Coloring Rules.

Conclusions

- Wireshark provides a set of tools to analyize the network traffic of the device and look for packet loss or any suspicious traffic that may be passing through the device. It provides various analyzing tools to get information about the packets, packet size, timing, protocols, ip addresses of the source and the destination, etc.