

Aim:

To use Wireshark to capture, save, and analyze network traffic over multiple protocols (TCP, UDP, IP, HTTP, ARP, DHCP, ICMP, DNS).

Introduction:

Wireshark is a packet analyzer used for network troubleshooting and protocol analysis.

Algorithm (Procedure):

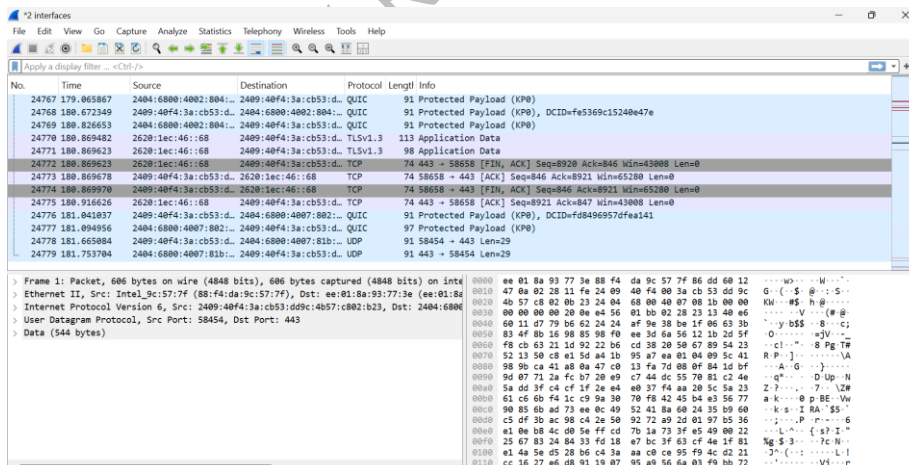
- Launch Wireshark and select the active network interface.
- Start capturing packets.
- Perform network activities (e.g., browsing, ping, DHCP request).
- Stop the capture and save the file.
- Use filters to isolate TCP, UDP, HTTP, ARP, DHCP, ICMP, and DNS traffic.
- Analyze details and packet contents.

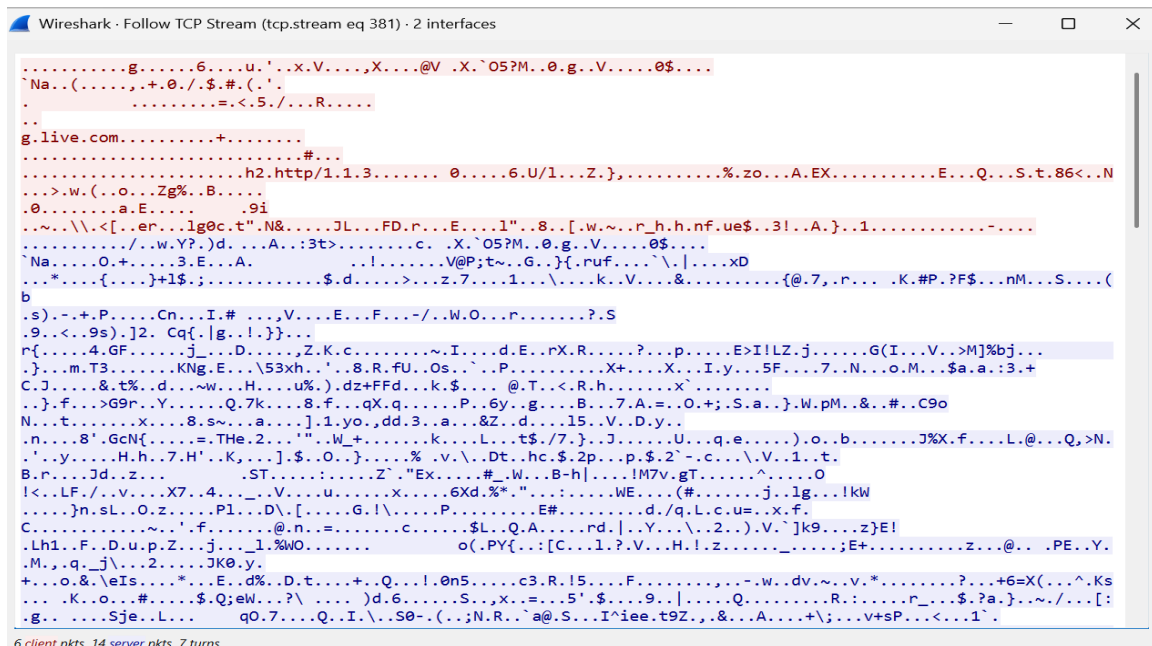
Result:

Traffic captured and analyzed; protocol communications are observed for learning or troubleshooting.

Output:**1. Capture or Open a Packet Capture File**

- Start by capturing live traffic via your network interface or open an existing .pcap file.
- Click **File > Open** to load a saved capture file.

**Follow TCP streams**



Protocol Hierarchy:

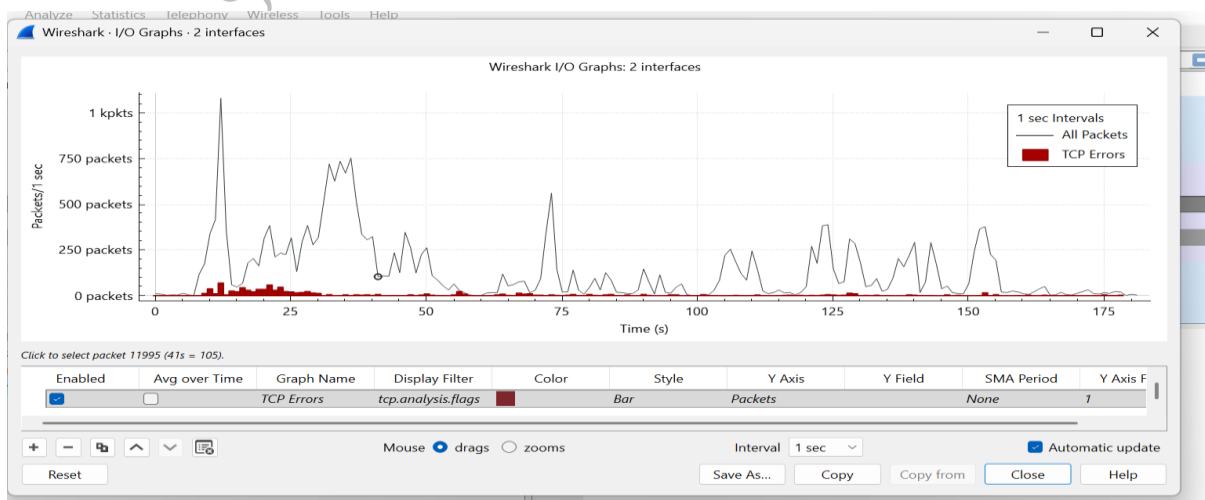
Shows a breakdown of protocols seen in the capture with counts and percentages.

Go to Statistics > Protocol Hierarchy.

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	41	100.0	13365	1174	0	0	0	41
Ethernet	100.0	41	4.3	574	50	0	0	0	41
Internet Protocol Version 6	100.0	41	12.3	1640	144	0	0	0	41
Transmission Control Protocol	100.0	41	6.6	880	77	25	560	49	41
Transport Layer Security	39.0	16	81.2	10857	954	16	4052	356	17

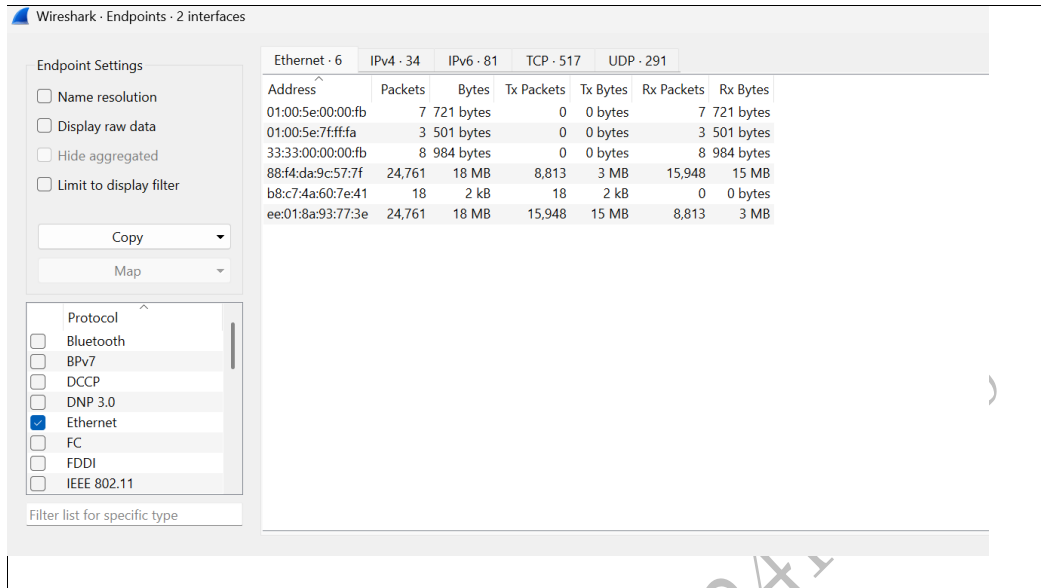
I/O GRAPHS;

Use statistics > I/O graphs to visualize traffic rate and identify spikes or drops over time



Endpoints:

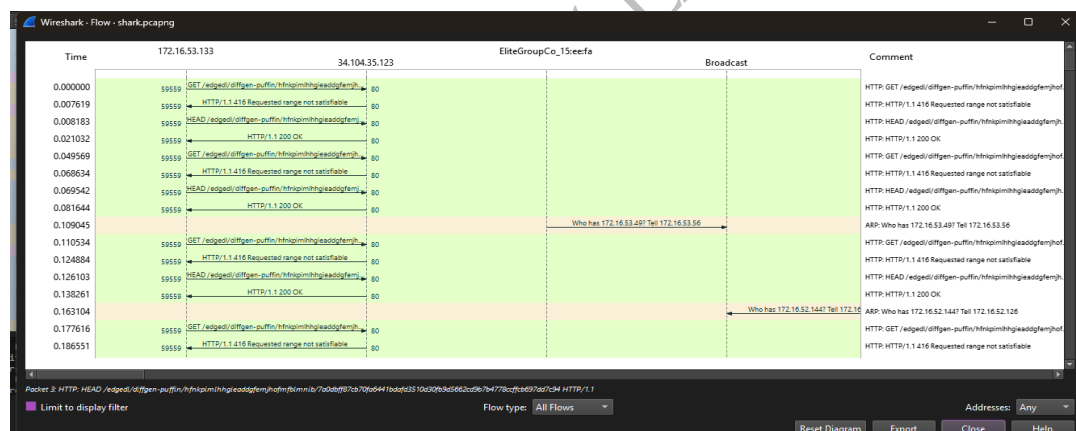
Lists all endpoints (IPs, MACs) involved in the capture and summarizes traffic per endpoint.
Go to Statistics > Endpoints.



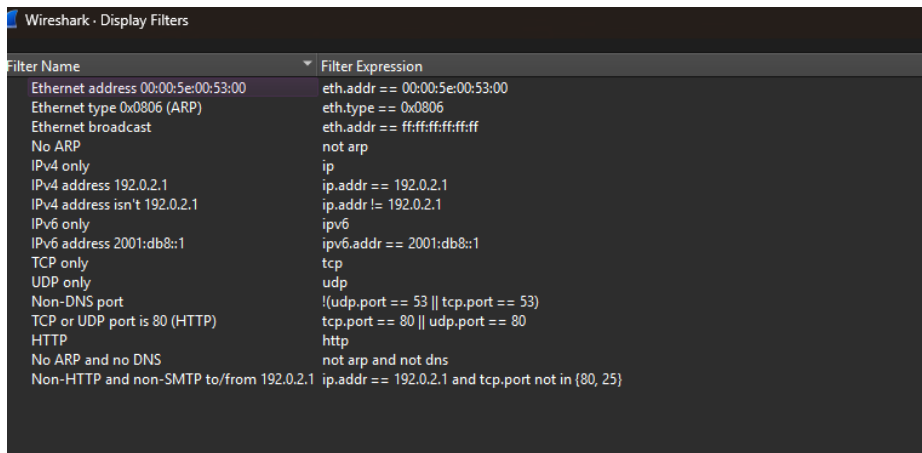
The screenshot shows the 'Endpoints' window in Wireshark. On the left, the 'Endpoint Settings' panel is visible with options for Name resolution, Display raw data, Hide aggregated, and Limit to display filter. Below these are 'Copy' and 'Map' buttons, and a 'Protocol' list with 'Ethernet' selected. The main table displays statistics for various protocols: Ethernet (6), IPv4 (34), IPv6 (81), TCP (517), and UDP (291). The table has columns for Address, Packets, Bytes, Tx Packets, Tx Bytes, Rx Packets, and Rx Bytes. The data is summarized for the following addresses: 01:00:5e:00:00:fb, 01:00:5e:7f:ff:fa, 33:33:00:00:00:fb, 88:f4:da:9c:57:7f, b8:c7:4a:60:7e:41, and ee:01:8a:93:77:3e.

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
01:00:5e:00:00:fb	7	721 bytes	0	0 bytes	7	721 bytes
01:00:5e:7f:ff:fa	3	501 bytes	0	0 bytes	3	501 bytes
33:33:00:00:00:fb	8	984 bytes	0	0 bytes	8	984 bytes
88:f4:da:9c:57:7f	24,761	18 MB	8,813	3 MB	15,948	15 MB
b8:c7:4a:60:7e:41	18	2 kB	18	2 kB	0	0 bytes
ee:01:8a:93:77:3e	24,761	18 MB	15,948	15 MB	8,813	3 MB

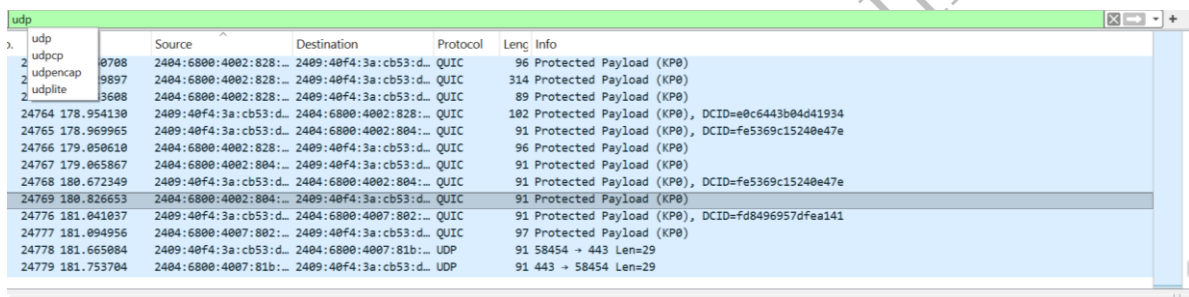
Flow: Depicts directional communication between network hosts, showing data exchanges in sequential context for analysis



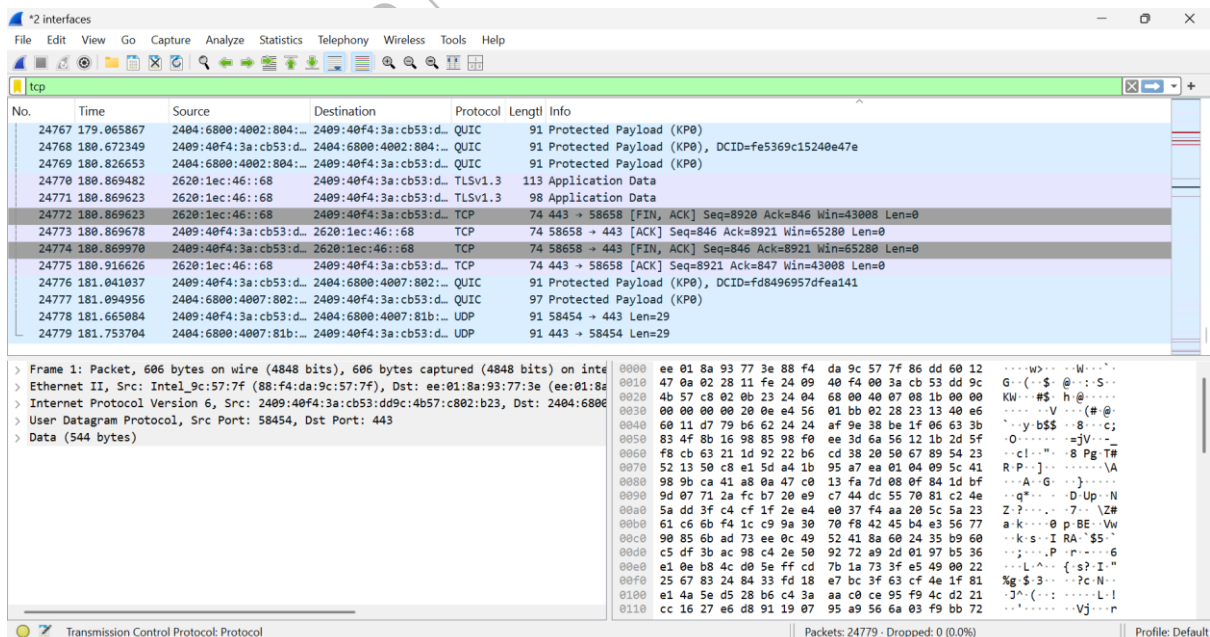
Display Filters: Enable precise viewing of packets by protocol fields, source/destination, or conditions (e.g., tcp.port == 80 or frame.len > 500).



UDP: A connectionless transport protocol providing fast but unreliable message delivery, ideal for real-time or broadcast communications.



TCP: A connection-oriented transport protocol that ensures reliable data delivery through mechanisms like acknowledgments and retransmissions.



Conversations:

Displays all conversations between IP addresses or MAC addresses. Useful for identifying

communication pairs.
Go to Statistics > Conversations.

Wireshark - Conversations - 2 interfaces

Conversation Settings

☐ Name resolution

☐ Absolute start time

☐ Display raw data

☐ Limit to display filter

Conv

Ethernet - 4

IPv4 - 32

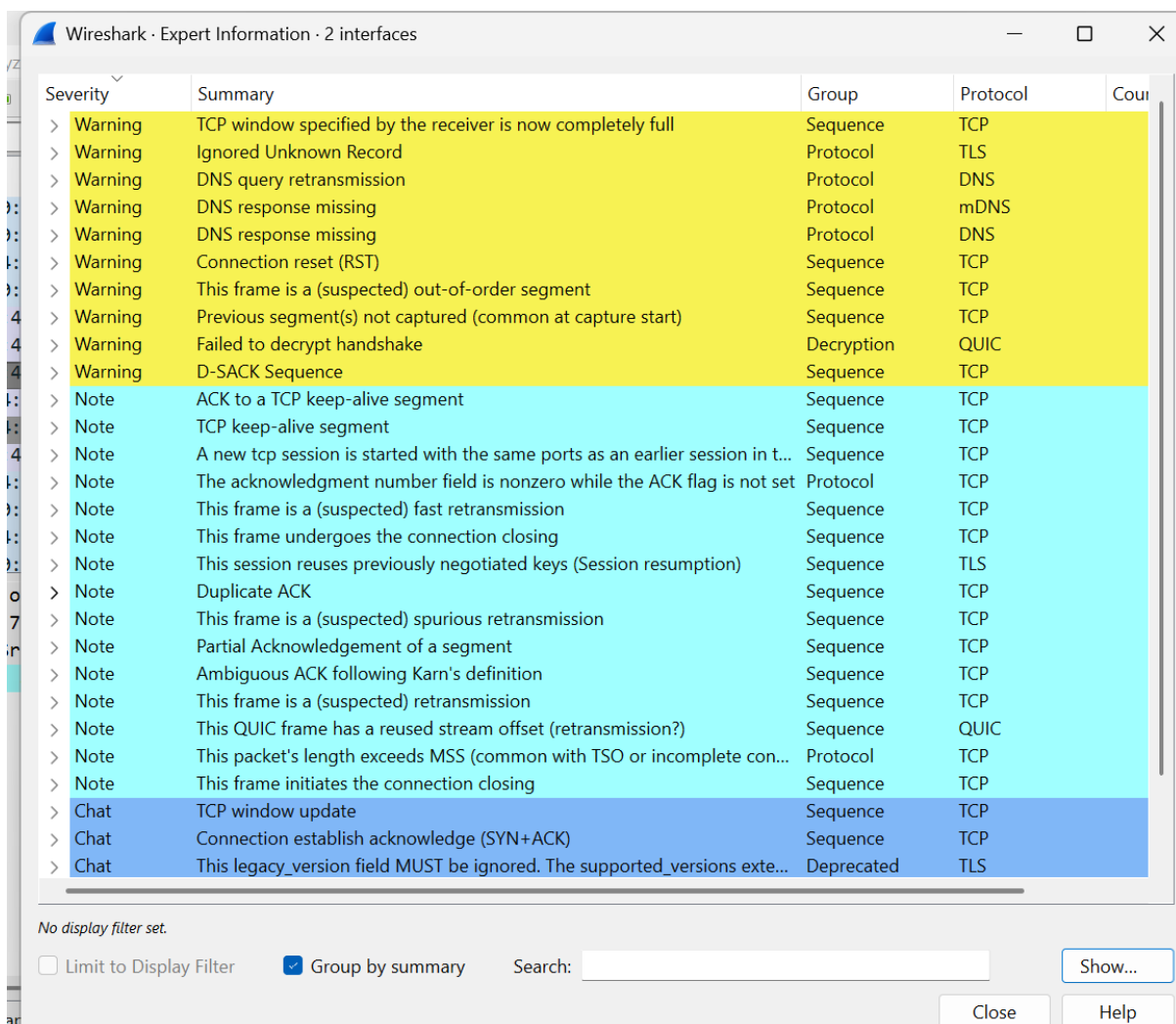
IPv6 - 79

TCP - 426

UDP - 241

Address A	Address B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
88:f4:da:9c:57:7f	ee:01:8a:93:77:3e	24,761	18 MB	0	8,813	3 MB	15,948	15 MB	0.000000	181.7537	131 kbps	676 kbps
b8:c7:4a:60:7e:41	01:00:5e:00:00:fb	7	721 bytes	1	7	721 bytes	0	0 bytes	17.070934	140.2051	41 bits/s	0 bits/s
b8:c7:4a:60:7e:41	01:00:5e:7f:ff:fa	3	501 bytes	3	3	501 bytes	0	0 bytes	43.680103	119.9296	33 bits/s	0 bits/s
b8:c7:4a:60:7e:41	33:33:00:00:00:fb	8	984 bytes	2	8	984 bytes	0	0 bytes	17.070934	140.2051	56 bits/s	0 bits/s

Expert Information: Displays protocol anomalies, warnings, and potential issues detected during packet capture for network troubleshooting.



Wireshark - Expert Information - 2 interfaces

Severity	Summary	Group	Protocol	Count
> Warning	TCP window specified by the receiver is now completely full	Sequence	TCP	
> Warning	Ignored Unknown Record	Protocol	TLS	
> Warning	DNS query retransmission	Protocol	DNS	
> Warning	DNS response missing	Protocol	mDNS	
> Warning	DNS response missing	Protocol	DNS	
> Warning	Connection reset (RST)	Sequence	TCP	
> Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	
> Warning	Previous segment(s) not captured (common at capture start)	Sequence	TCP	
> Warning	Failed to decrypt handshake	Decryption	QUIC	
> Warning	D-SACK Sequence	Sequence	TCP	
> Note	ACK to a TCP keep-alive segment	Sequence	TCP	
> Note	TCP keep-alive segment	Sequence	TCP	
> Note	A new tcp session is started with the same ports as an earlier session in t...	Sequence	TCP	
> Note	The acknowledgment number field is nonzero while the ACK flag is not set	Protocol	TCP	
> Note	This frame is a (suspected) fast retransmission	Sequence	TCP	
> Note	This frame undergoes the connection closing	Sequence	TCP	
> Note	This session reuses previously negotiated keys (Session resumption)	Sequence	TLS	
> Note	Duplicate ACK	Sequence	TCP	
> Note	This frame is a (suspected) spurious retransmission	Sequence	TCP	
> Note	Partial Acknowledgement of a segment	Sequence	TCP	
> Note	Ambiguous ACK following Karn's definition	Sequence	TCP	
> Note	This frame is a (suspected) retransmission	Sequence	TCP	
> Note	This QUIC frame has a reused stream offset (retransmission?)	Sequence	QUIC	
> Note	This packet's length exceeds MSS (common with TSO or incomplete con...	Protocol	TCP	
> Note	This frame initiates the connection closing	Sequence	TCP	
> Chat	TCP window update	Sequence	TCP	
> Chat	Connection establish acknowledge (SYN+ACK)	Sequence	TCP	
> Chat	This legacy_version field MUST be ignored. The supported_versions exte...	Deprecated	TLS	

No display filter set.

☐ Limit to Display Filter ☒ Group by summary Search: Show...

Close Help

Result

Hence using windows Wireshark, we captured the packets and executed the functions.