

Ex.No:12

M.Dhivya

Date:13/10/25

241901027

TO CAPTURE, SAVE, AND ANALYZE NETWORK TRAFFIC USING WIRESHARK TOOL

Aim:

To capture, save, and analyze network traffic on
TCP/UDP/IP/HTTP/ARP/DHCP/ICMP /DNS using Wireshark Tool.

Procedure:

1. Install Wireshark

Download and install Wireshark from <https://www.wireshark.org/>

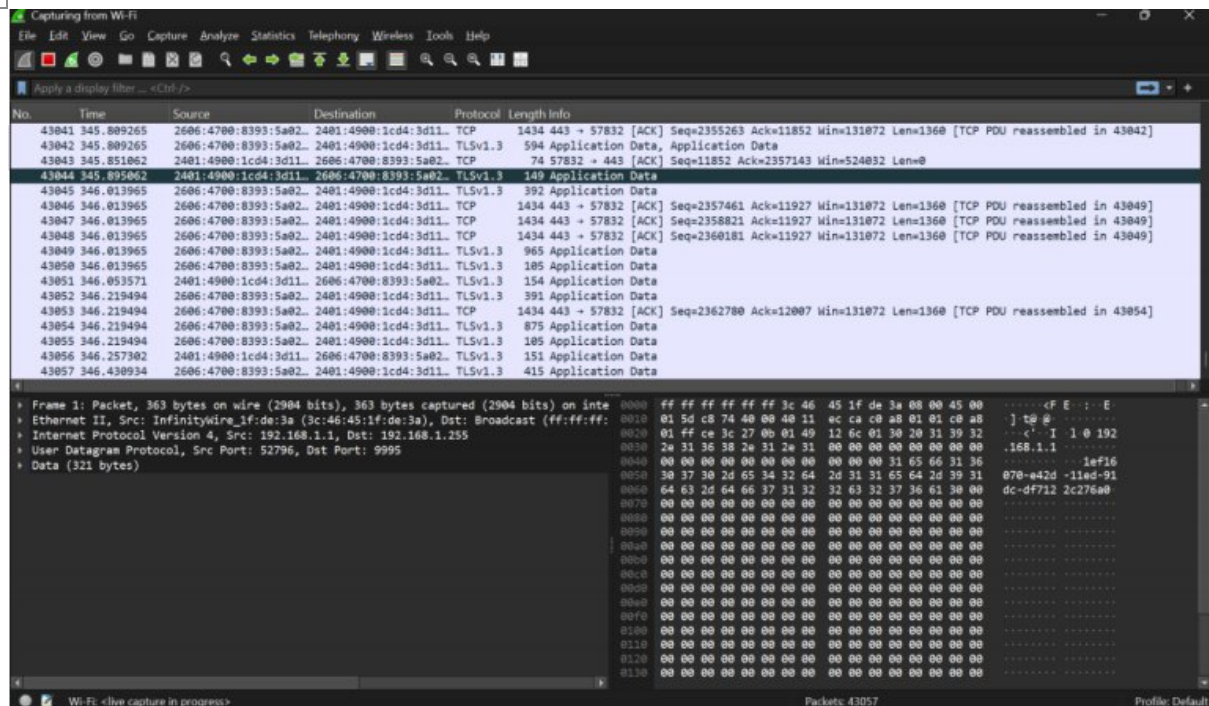
Make sure to install the required packet capture drivers (e.g.,
WinPcap or Npcap on Windows).

2. Start Capturing Traffic

Open Wireshark.

Select the correct network interface for capturing (Wi-Fi, Ethernet,
etc.).

Click on the interface to start live capture.



3. Apply Capture Filters

To reduce the amount of data captured, you can apply capture filters.

Example filters for protocols:

TCP only: tcp

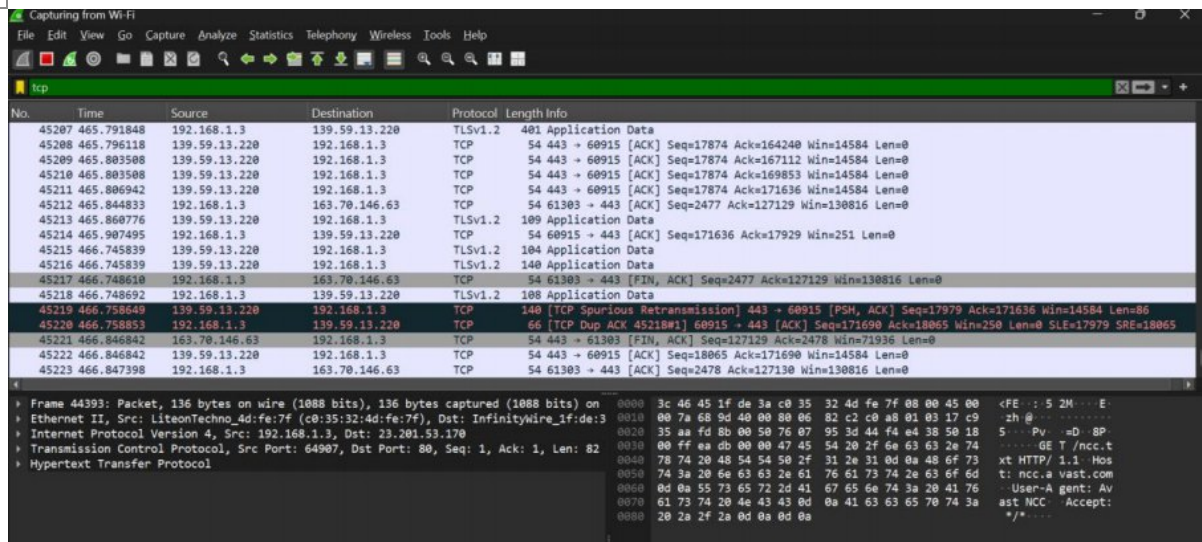
UDP only: udp

ARP only: arp

ICMP only: icmp

DHCP (uses UDP ports 67 and 68): udp port 67 or udp port 68

DNS (uses UDP or TCP port 53): port 53



4. Save Captured Traffic

When done capturing, go to File > Save As.

Save the capture file in .pcapng or .pcap format for later analysis

5. Analyze Captured Traffic

Wireshark provides powerful tools to filter and analyze packets:

Display Filters:

You can filter displayed packets without limiting the saved capture.

Examples:

TCP: tcp

UDP: udp

IP: ip

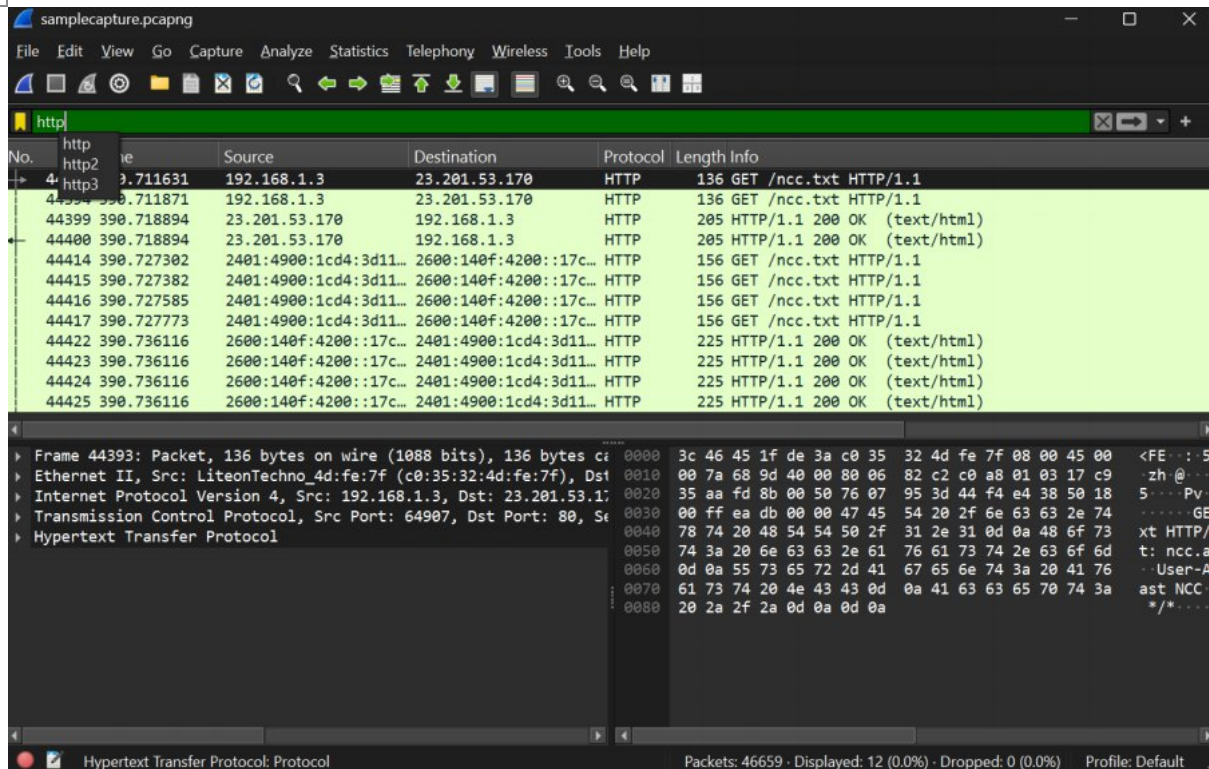
HTTP: http

ARP: arp

DHCP: bootp (DHCP is part of the BOOTP protocol)

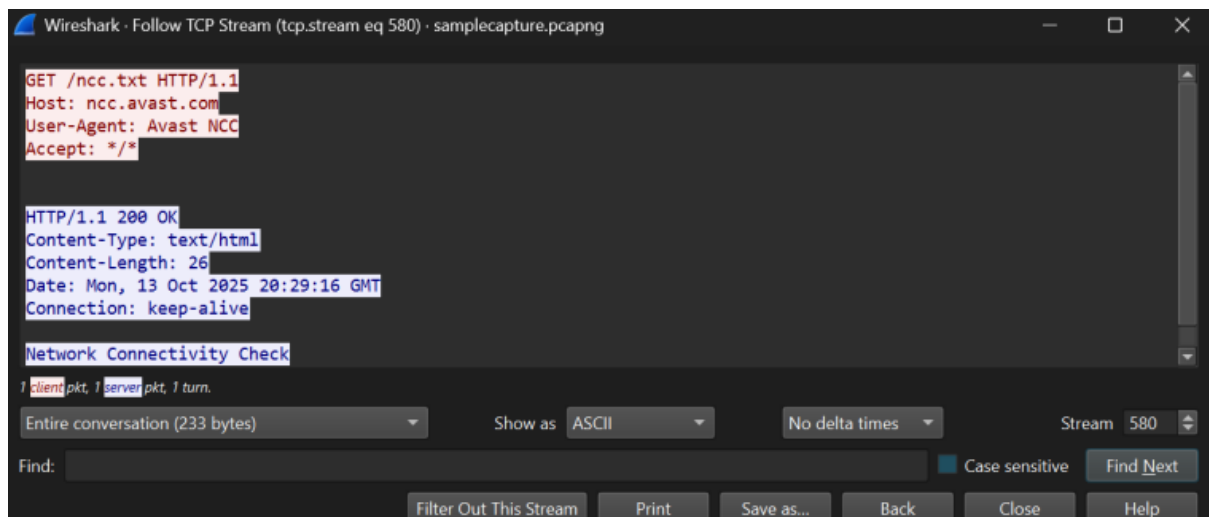
ICMP: icmp

DNS: dns



Follow Streams:

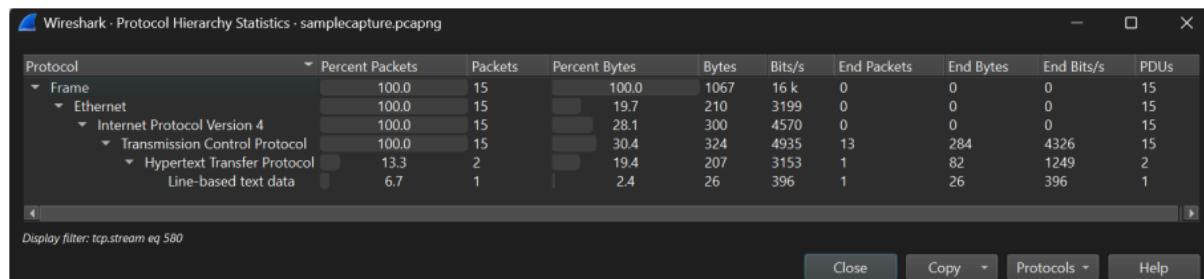
For TCP or UDP conversations, right-click a packet and select Follow > TCP Stream or Follow > UDP Stream to see the conversation in readable form.



Protocol Hierarchy:

Use Statistics > Protocol Hierarchy to get an overview of protocols

present.



Wireshark - Protocol Hierarchy Statistics - samplecapture.pcapng

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	15	100.0	1067	16 k	0	0	0	15
Ethernet	100.0	15	19.7	210	3199	0	0	0	15
Internet Protocol Version 4	100.0	15	28.1	300	4570	0	0	0	15
Transmission Control Protocol	100.0	15	30.4	324	4935	13	284	4326	15
Hypertext Transfer Protocol	13.3	2	19.4	207	3153	1	82	1249	2
Line-based text data	6.7	1	2.4	26	396	1	26	396	1

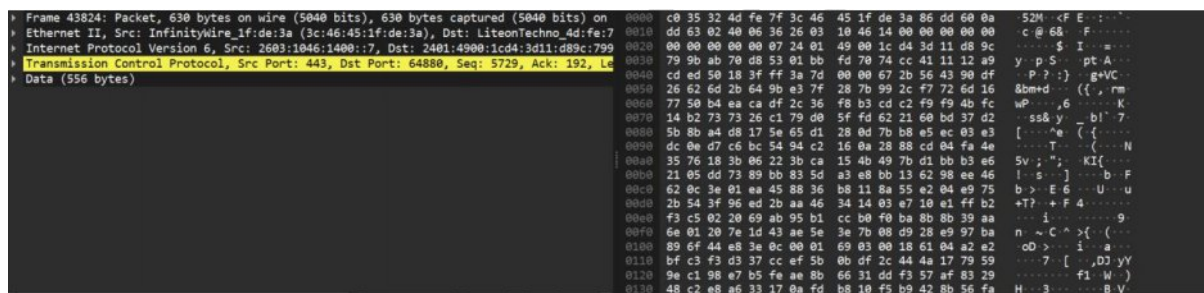
Display filter: tcp.stream eq 580

Buttons: Close, Copy, Protocols, Help

Packet Details:

Select any packet and expand protocol layers in the middle pane to analyze

headers and payload details



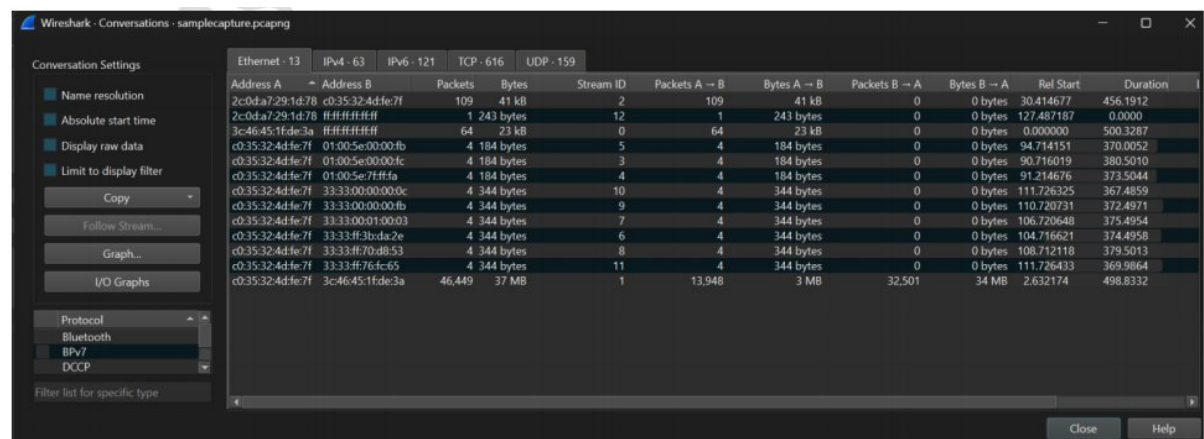
Frame 43824: Packet, 630 bytes on wire (5040 bits), 630 bytes captured (5040 bits) on Ethernet II, Src: InfinityWire_1f:de:3a (3c:46:45:1f:de:3a), Dst: LiteonTechno_4d:fe:7 Internet Protocol Version 6, Src: 2603:1046:1400::7, Dst: 2401:4900:1cd4:3d11:d89c:799 Transmission Control Protocol, Src Port: 443, Dst Port: 64880, Seq: 5729, Ack: 192, Length: 556 bytes

Protocol layers expanded: Ethernet II, Internet Protocol Version 6, Transmission Control Protocol, Hypertext Transfer Protocol.

Conversations:

Use Statistics > Conversations to analyze communication between source

and destination hosts.



Wireshark - Conversations - samplecapture.pcapng

Conversation Settings: Name resolution, Absolute start time, Display raw data, Limit to display filter, Copy, Follow Stream..., Graph..., I/O Graphs, Protocol (Bluetooth, IPv6, DCCP), Filter list for specific type

Address A	Address B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
2c0da729:1d:78	c035:32:4d:fe:7f	109	41 kB	2	109	41 kB	0	0 bytes	30.414677	456.1912
2c0da729:1d:78	ff:ff:ff:ff:ff:ff	1	243 bytes	12	1	243 bytes	0	0 bytes	127.487187	0.0000
3c46:45:1f:de:3a	ff:ff:ff:ff:ff:ff	64	23 kB	0	64	23 kB	0	0 bytes	0.000000	500.3287
c035:32:4d:fe:7f	01:00:5e:00:00:fb	4	184 bytes	5	4	184 bytes	0	0 bytes	94.714151	370.0052
c035:32:4d:fe:7f	01:00:5e:00:00:fc	4	184 bytes	3	4	184 bytes	0	0 bytes	90.716019	380.5010
c035:32:4d:fe:7f	01:00:5e:7f:ff:fa	4	184 bytes	4	4	184 bytes	0	0 bytes	91.214676	373.5044
c035:32:4d:fe:7f	33:33:00:00:00:0c	4	344 bytes	10	4	344 bytes	0	0 bytes	111.726325	367.4859
c035:32:4d:fe:7f	33:33:00:00:00:fb	4	344 bytes	9	4	344 bytes	0	0 bytes	110.720731	372.4971
c035:32:4d:fe:7f	33:33:00:01:00:03	4	344 bytes	7	4	344 bytes	0	0 bytes	106.720648	375.4954
c035:32:4d:fe:7f	33:33:4f:7b:da:2e	4	344 bytes	6	4	344 bytes	0	0 bytes	104.716621	374.4858
c035:32:4d:fe:7f	33:33:4f:7b:da:53	4	344 bytes	8	4	344 bytes	0	0 bytes	108.712118	379.5013
c035:32:4d:fe:7f	33:33:4f:7b:da:65	4	344 bytes	11	4	344 bytes	0	0 bytes	111.726433	369.9864
c035:32:4d:fe:7f	3c46:45:1f:de:3a	46,449	37 MB	1	13,948	3 MB	32,501	34 MB	2.632174	498.8332

Buttons: Close, Help

Endpoints:

Go to Statistics > Endpoints to list all active IP/MAC addresses involved

in the capture.

Wireshark · Endpoints · samplecapture.pcapng

Endpoint Settings

☒ Name resolution

☒ Display raw data

☐ Hide aggregated

☒ Limit to display filter

Copy

Map

Protocol

Bluetooth

BPv7

DCCP

Filter list for specific type

Ethernet · 13

IPv4 · 62

IPv6 · 121

TCP · 725

UDP · 228

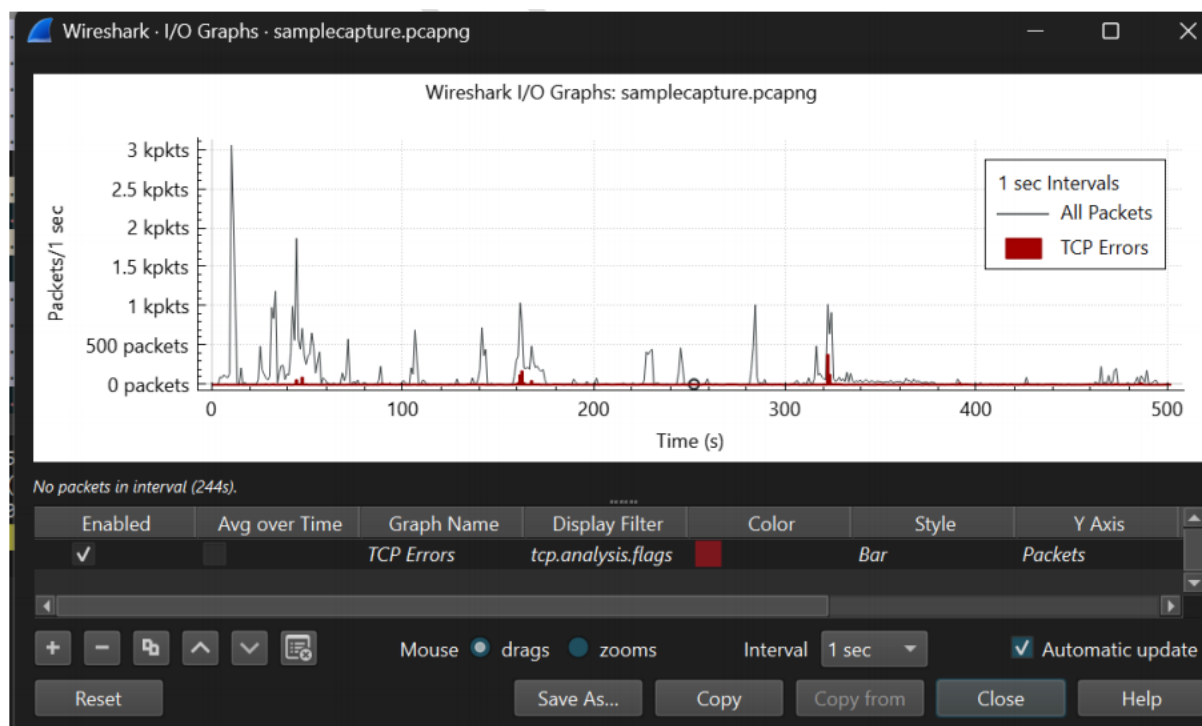
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
01:00:5e:00:00:fb	4	184 bytes	0	0 bytes	4	184 bytes
01:00:5e:00:00:fc	4	184 bytes	0	0 bytes	4	184 bytes
01:00:5e:7f:ff:fa	4	184 bytes	0	0 bytes	4	184 bytes
2c:0d:a7:29:1d:78	110	41 kB	110	41 kB	0	0 bytes
33:33:00:00:00:0c	4	344 bytes	0	0 bytes	4	344 bytes
33:33:00:00:00:fb	4	344 bytes	0	0 bytes	4	344 bytes
33:33:00:01:00:03	4	344 bytes	0	0 bytes	4	344 bytes
33:33:ff:3b:da:2e	4	344 bytes	0	0 bytes	4	344 bytes
33:33:ff:70:d8:53	4	344 bytes	0	0 bytes	4	344 bytes
33:33:ff:76:fc:65	4	344 bytes	0	0 bytes	4	344 bytes
3c:46:45:1f:de:3a	46,513	37 MB	32,565	34 MB	13,948	3 MB
c0:35:32:4d:fe:7f	46,594	37 MB	13,984	3 MB	32,610	34 MB
ff:ff:ff:ff:ff:ff	65	23 kB	0	0 bytes	65	23 kB

Close

Help

I/O Graphs:

Use Statistics > I/O Graphs to visualize traffic rate and identify spikes or drops over time.



Expert Information:

Open Analyze > Expert Information to detect errors, warnings, and

retransmissions.



Severity	Summary	Group	Protocol	Count
Warning	DNS query retransmission	Protocol	mDNS	
Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	
Warning	Ignored Unknown Record	Protocol	TLS	
Warning	Unrecognized text	Protocol	XML	
Warning	Previous segment(s) not captured (common at capture start)	Sequence	TCP	
Warning	ACKed segment that wasn't captured (common at capture start)	Sequence	TCP	
Warning	D-SACK Sequence	Sequence	TCP	
Warning	Connection reset (RST)	Sequence	TCP	
Warning	DNS response missing	Protocol	DNS	
Warning	Failed to decrypt handshake	Decryption	QUIC	
Note	Ciphersuite not implemented, contact Wireshark developers if you want ...	Undecoded	TLS	
Note	The SYN packet does not contain a SACK PERM option	Protocol	TCP	
Note	A new tcp session is started with the same ports as an earlier session in t...	Sequence	TCP	
Note	This QUIC frame overlaps a previous frame in the stream	Sequence	QUIC	
Note	Time To Live	Sequence	IPv4	
Note	ACK to a TCP keep-alive segment	Sequence	TCP	
Note	TCP keep-alive segment	Sequence	TCP	
Note	This frame is a (suspected) fast retransmission	Sequence	TCP	
Note	Coalesced Padding Data	Protocol	QUIC	
Note	This packet's length exceeds MSS (common with TSO or incomplete con...	Protocol	TCP	
Note	This session reuses previously negotiated keys (Session resumption)	Sequence	TLS	
Note	Type indicates an error	Response	ICMP	
Note	Unknown packet	Undecoded	XMPP	
Note	The acknowledgment number field is nonzero while the ACK flag is not set	Protocol	TCP	
Note	Partial Acknowledgement of a segment	Sequence	TCP	
Note	Type indicates an error	Response	ICMPv6	
Note	Ambiguous ACK following Karn's definition	Sequence	TCP	
Note	Duplicate ACK	Sequence	TCP	
Note	This frame is a (suspected) spurious retransmission	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 frame undergoes the connection closing	Sequence	TCP	
Note	This frame initiates the connection closing	Sequence	TCP	
Chat	TCP window update	Sequence	TCP	
Chat	Connection finish (FIN)	Sequence	TCP	
Chat	Connection establish acknowledge (SYN+ACK)	Sequence	TCP	
Chat	Connection establish request (SYN)	Sequence	TCP	

Result:

Thus network traffic on TCP/UDP/IP/HTTP/ARP/DHCP/ICMP /DNS were analyzed using Wireshark Tool.