

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.

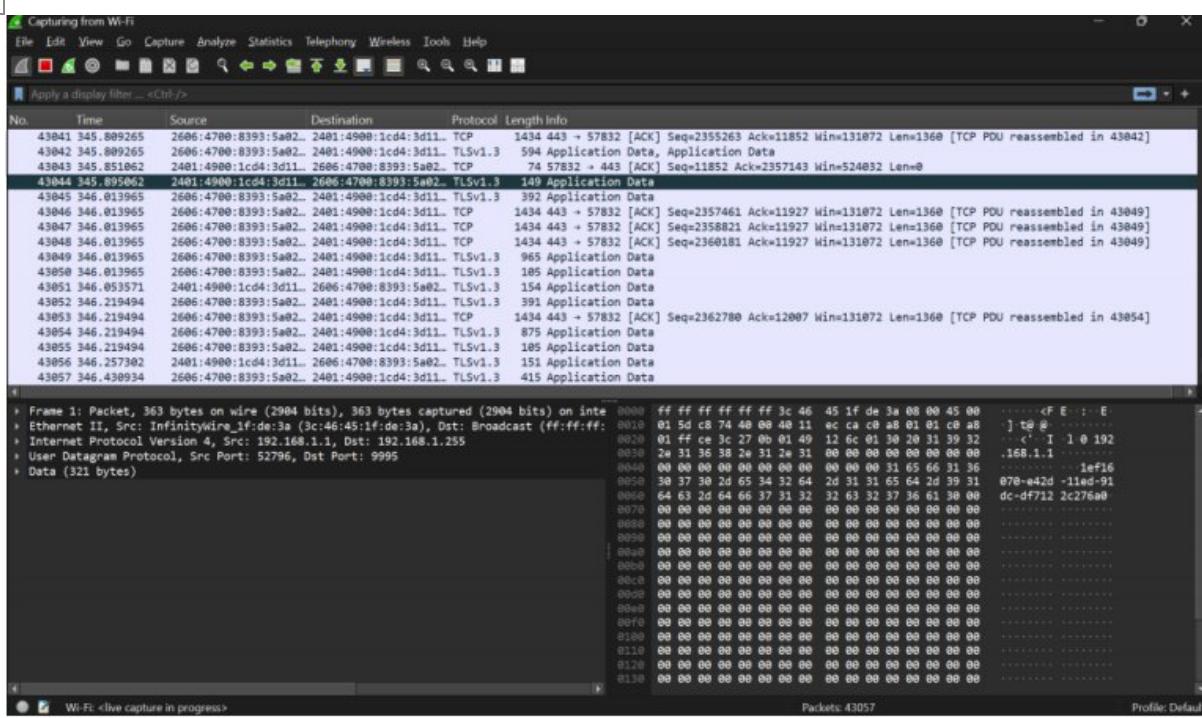
Procedure:

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`

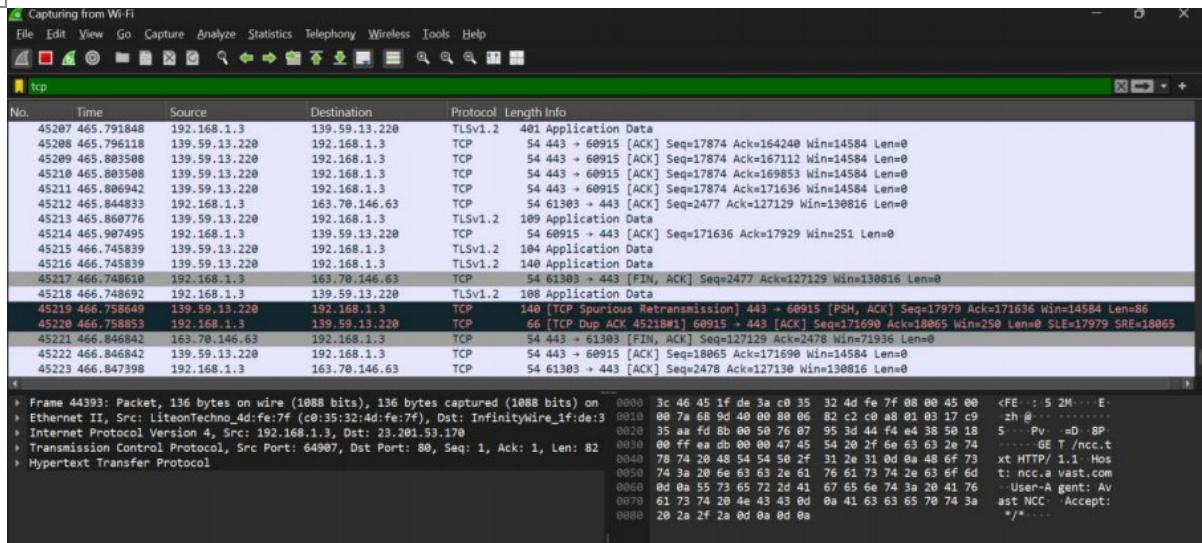
UDP only: `udp`

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

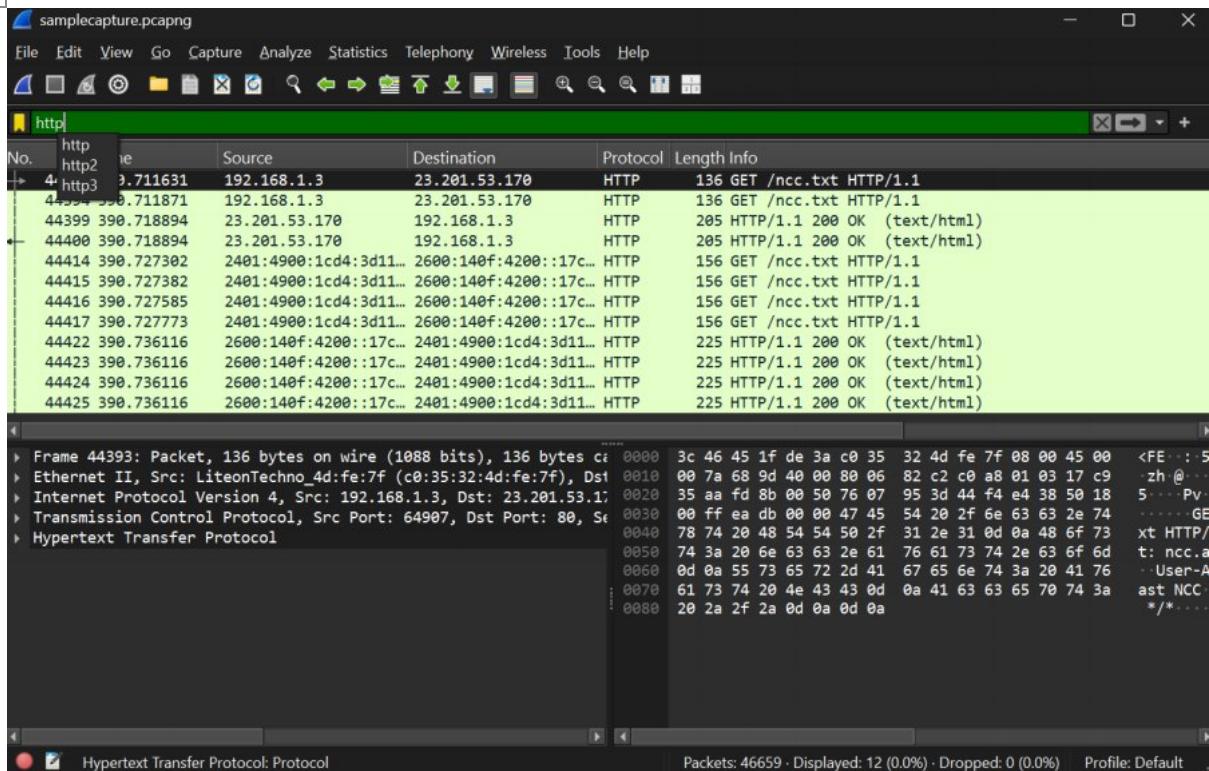
HTTP: http

ARP: arp

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

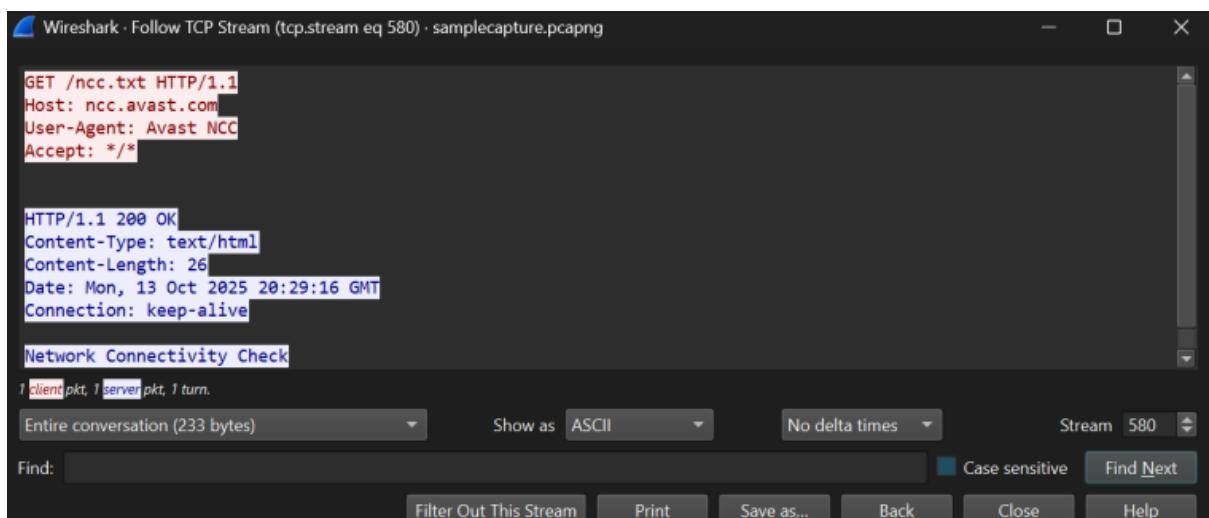
ICMP: icmp

DNS: dns



Follow Streams:

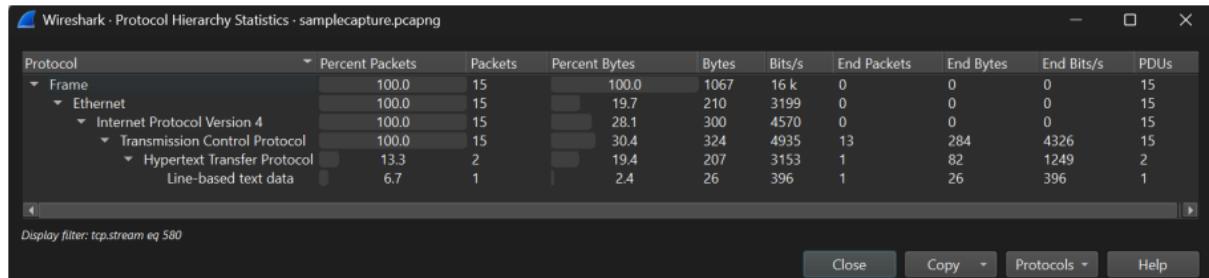
For TCP or UDP conversations, right-click a packet and select Follow > TCP Stream or Follow > UDP Stream to see the conversation in readable form.



Protocol Hierarchy:

Use Statistics > Protocol Hierarchy to get an overview of protocols

present.



Packet Details:

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

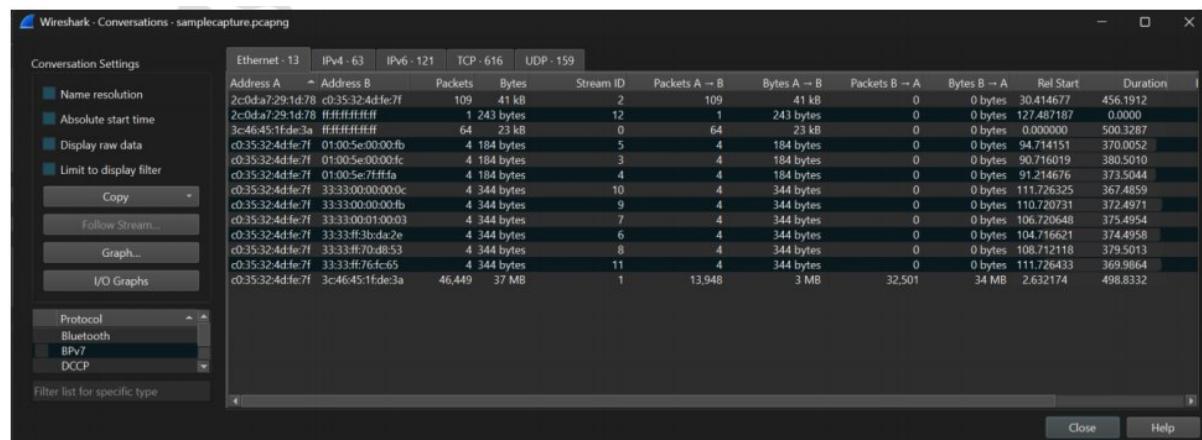
headers and payload details

```
> Frame 43824: Packet, 630 bytes on wire (5040 bits), 630 bytes captured (5040 bits) on
  0000  c0 35 32 4d fe 7f 3c 46 45 1f de 3a 86 dd 60 0a 52M <F E : ' '
> Ethernet II, Src: InfinityWire_1f:de:3a (3c:46:45:1f:de:3a), Dst: LiteonTechno_4d:fe:7
  0010  dd 63 02 40 06 36 26 03 10 46 14 00 00 00 00 00 c @ 68... F ...
  0020  00 00 00 00 00 07 24 01 49 00 1c d4 3d 11 d8 9c ...$ I ...
  0030  79 9b 20 7d 53 01 b1 fd 7d 74 cc 41 11 12 a9 y p S pt A
  0040  cd ed 50 18 3f ff 3a 7d 00 00 67 2b 56 43 90 df ..P ? : g+VC
  0050  26 62 6d 2b 64 9b e3 7f 28 7b 99 2c f7 72 6d 16 &mdm { , rm
  0060  77 50 b4 ea ca df 2c 36 f8 b3 cd c2 f9 f9 4b fc wP...6 K...
  0070  14 b2 73 73 26 c1 79 d0 5f fd 62 21 60 bd 37 d2 ss& y { bl! 7
  0080  5b 8b a4 d8 17 5a 65 d1 28 0d 7b b8 e5 ec 03 e3 [ ^e { {
  0090  dc 0e d7 c6 bc 54 94 c2 16 0a 28 88 cd 04 fa 4e T { N
  00a0  35 76 18 3b 06 22 3b ca 15 4b 49 7b d2 bb b3 e6 5v ; K{ ...
  00b0  21 05 dd 73 89 bb 83 5d a3 e8 bb 13 62 98 ee 46 l s ] b F
  00c0  62 0e 3e 01 ea 45 88 36 b8 11 8a 55 e2 04 e9 75 b > E 6 U u
  00d0  2b 54 3f 96 ed 2a 46 34 14 03 e7 10 e1 ff b2 +? F 4 ...
  00e0  f3 c5 02 20 69 ab 95 b1 cc b0 f0 ba 8b 8b 39 aa i ... 9
  00f0  6e 01 28 7e 1d 43 a5 5e 3e 7b 00 d9 28 e9 97 ba n ~ C ^ > ( (
  0100  89 6f 44 e8 3e 0e 00 01 69 03 00 18 61 04 a2 e2 oO > i a
  0110  b7 c3 f3 d3 37 cc ef 5b 0b df 2c 44 4a 17 79 59 7 [ ,D yY
  0120  9e c1 98 e7 b5 fe ae 8b 66 31 dd f3 57 af 83 29 f1 W )
  0130  48 c2 e8 a6 33 17 0a fd b8 18 f5 b9 42 8b 56 fa H -3 B V
```

Conversations:

Use Statistics > Conversations to analyze communication between source

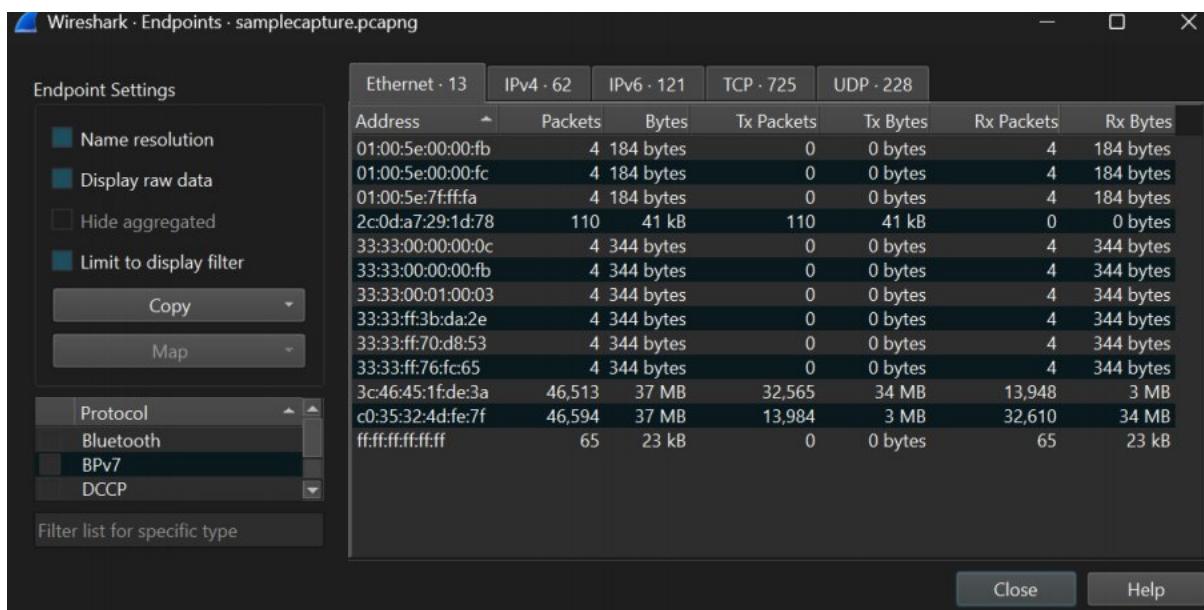
and destination hosts.



Endpoints:

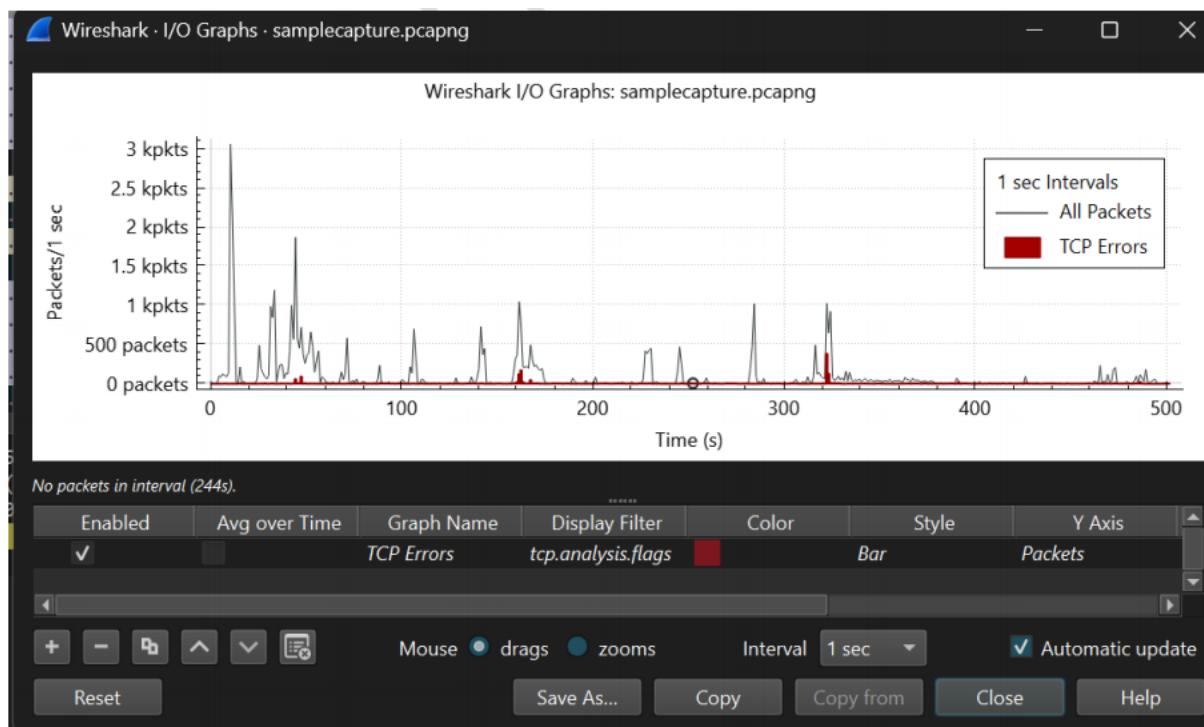
Go to Statistics > Endpoints to list all active IP/MAC addresses involved

in the capture.



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	QUIC	
Note	This QUIC frame has a reused stream offset (retransmission?)	Sequence	TCP	
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.