

Exp No: 5  
DATE: 31.07.25

## Experiment on packet capture tool WIRESHARK

### Aim:

To capture and analyze network packets using Wireshark and apply filters to display specific protocols.

### Packet Sniffer:

⇒ Sniffs messages being sent/received from/by your computer.  
⇒ stores and displays the content of the various protocol fields in the message.

### DESCRIPTION:

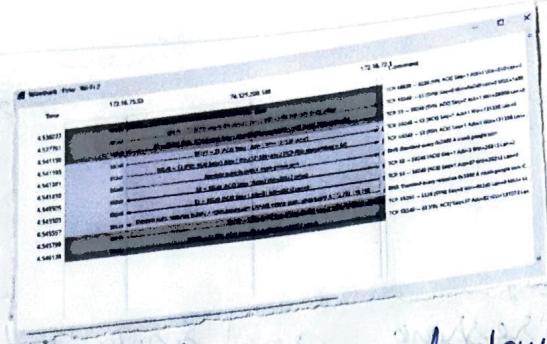
Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real-time and displays them in human-readable form. Wireshark includes filters, color coding, and other features that let you dig deeper into network traffic and inspect individual packets.

### Capturing and Analysing packets using Wireshark

- ⇒ To filter, capture, view packets in Wireshark
- ⇒ capture 100 packets from the Ethernet / IEEE 802.3 LAN interface and save it.

### Procedure:

- ⇒ Select Local area connection in Wireshark
- ⇒ Go to capture → options

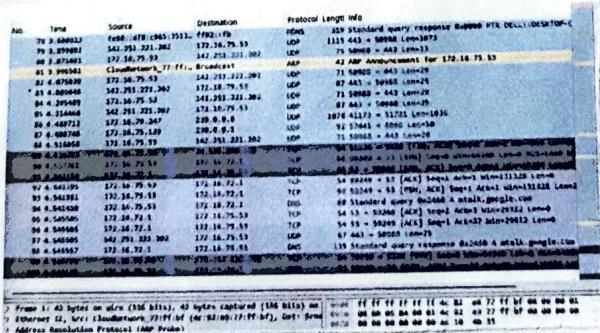


1. Create a filter to display only TCP packets. inspect the Packets and provide the flow graph.

Procedure:

- select LAN in wireshark
- go to Capture → Options
- select Stop Capture automatically after 100 Packets.
- Search TCP packets in search box.
- To see flow graph click static → flowgraph

## Flow Graph



2. Create a filter to display only ARP packets and inspect the packets.

Procedure:

- Search ARP packets in search box
- Save the packets

Output

3. C  
Pack  
Proc

Out

A  
Po  
P

display only TCP, UDP  
and provide the flow graph

procedure:

shark

on

automatically after 100

search box.

click statistic

→ flowgraph

Output: after selecting the statistic, click flowgraph and you will see

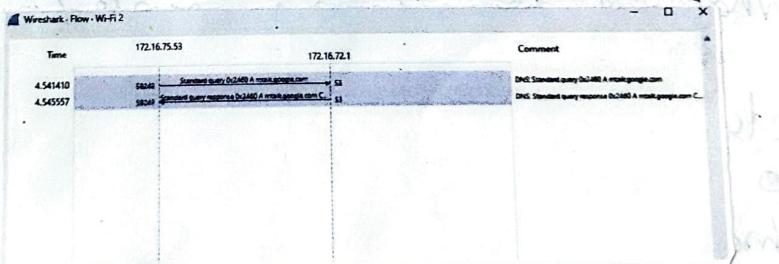
| No. | Time     | Source                | Destination | Protocol Length Info                     |
|-----|----------|-----------------------|-------------|--|
| 2   | 0.000000 | CloudNetwork_77:ff:ff | Broadcast   | ARP 42 who has 172.16.75.53? (ARP Probe) |
| 3   | 0.00075  | CloudNetwork_77:ff:ff | Broadcast   | ARP 42 who has 172.16.75.53? (ARP Probe) |
| 4   | 1.997994 | CloudNetwork_77:ff:ff | Broadcast   | ARP 42 ARP Announcement for 172.16.75.53 |
| 5   | 1.998001 | CloudNetwork_77:ff:ff | Broadcast   | 42 ARP/ANNOUNCEMENT for 172.16.75.53     |

3. create a filter to display only DNS  
packets and provide the flow graph

Procedure:

- search DNS packets in search bar.
- To see flow graph click Statistics → Flow graph
- Save the packets

Output:



4. Create a filter to display only IP/TCP  
packets and inspect the packets.

Procedure:

- search IP packets in search bar
- Save the packets.

| No. | Time     | Source       | Destination     | Protocol Length Info  |
|-----|----------|--------------|-----------------|---|
| 2   | 0.002631 | 172.16.75.53 | 224.0.0.251     | ICMP 1317 Standard query response XIAOMI_PTA_DELLDESKTOP-C  |
| 3   | 0.003664 | 172.16.75.53 | 224.0.0.251     | ICMP 948 Standard query response XIAOMI_PTA_DELLDESKTOP-C   |
| 4   | 0.003964 | 172.16.75.53 | 224.0.0.251     | ICMP 948 Standard query response XIAOMI_PTA_DELLDESKTOP-C   |
| 5   | 0.003973 | 172.16.75.53 | 142.251.229.120 | UDP 71 57362 + 443 Len=29                                   |
| 6   | 0.004622 | 172.16.75.53 | 142.251.229.120 | UDP 71 57362 + 443 Len=29                                   |
| 7   | 0.005038 | 172.16.75.53 | 142.251.229.120 | UDP 72 443 + 57362 Len=30                                   |
| 8   | 0.005042 | 172.16.75.53 | 172.16.75.53    | UDP 73 443 + 57362 Len=30                                   |
| 9   | 0.005052 | 172.16.75.53 | 172.16.75.53    | TCP 54 59545 + 36 [ACK] Seq=1483 Win=1483                   |
| 10  | 0.005471 | 172.16.75.53 | 204.79.197.222  | TCP 54 59522 + 443 [ACK] Seq=1483 Win=1483                  |
| 11  | 0.005493 | 172.16.75.53 | 204.79.197.222  | TCP 54 59522 + 443 [ACK] Seq=1483 Win=1483                  |
| 12  | 0.005494 | 172.16.75.53 | 22.202.229.23   | TCP 54 59522 + 443 [ACK] Seq=1483 Win=1483                  |
| 13  | 0.005495 | 172.16.75.53 | 204.79.197.222  | TCP 54 59522 + 443 [ACK] Seq=1483 Win=1483                  |
| 14  | 0.005497 | 172.16.75.53 | 204.79.197.222  | TCP 54 59522 + 443 [ACK] Seq=1483 Win=1483                  |
| 15  | 0.005498 | 172.16.75.53 | 204.79.197.222  | TCP 54 59522 + 443 [ACK] Seq=1483 Win=1483                  |
| 16  | 0.005814 | 172.16.75.53 | 229.0.0.6       | ICMP 3678 39776 + 53723 Len=1826                            |
| 17  | 0.005814 | 172.16.75.53 | 239.0.0.1       | ICMP 52 65450 + 6646 Len=8                                  |
| 18  | 0.022062 | 172.16.75.53 | 239.0.0.9       | ICMP 3478 56274 + 53723 Len=1826                            |
| 19  | 0.022062 | 172.16.75.53 | 239.0.0.9       | ICMP 3678 49626 + 53723 Len=1826                            |
| 20  | 0.022462 | 172.16.75.53 | 255.259.255.255 | ICMP 92 Name query response, requested name does not exist  |
| 21  | 0.022793 | 172.16.75.53 | 172.16.75.53    | ICMP 128 Name query response, requested name does not exist |
| 22  | 0.028957 | 172.16.75.53 | 239.0.0.6       | ICMP 3678 26893 + 53723 Len=1826                            |
| 23  | 0.041308 | 172.16.75.53 | 172.16.75.53    | ICMP 92 Name query response, requested name does not exist  |

- 5) Create a filter to display only DHCP packets and inspect the packets.
- Procedure:
- search DHCP packets in the search bar
  - Save the packets.

| No. | Time            | Source  | Destination     | Protocol | Length | Info  |
|-----|-----------------|---------|-----------------|----------|--------|---|
| 1   | 12:57:25.110000 | 0.0.0.9 | 255.255.255.255 | DHCP     | 342    | DHCP Request - Transaction ID 0x9797cf      |
| 2   | 12:57:25.110000 | 0.0.0.9 | 255.255.255.255 | DHCP     | 342    | DHCP Request - Transaction ID 0x1dd986cf    |
| 3   | 12:57:25.110000 | 0.0.0.9 | 255.255.255.255 | DHCP     | 342    | DHCP Request - Transaction ID 0x21440000    |
| 4   | 12:57:25.110000 | 0.0.0.9 | 255.255.255.255 | DHCP     | 342    | DHCP Request - Transaction ID 0x1442160     |
| 5   | 12:57:25.110000 | 0.0.0.9 | 255.255.255.255 | DHCP     | 342    | DHCP Request - Transaction ID 0x155776ef    |
| 6   | 12:57:25.110000 | 0.0.0.9 | 255.255.255.255 | DHCP     | 342    | DHCP Request - Transaction ID 0x95dfcb02    |
| 7   | 12:57:25.110000 | 0.0.0.9 | 255.255.255.255 | DHCP     | 342    | DHCP Request - Transaction ID 0x9590fb5d4d  |
| 8   | 12:57:25.110000 | 0.0.0.9 | 255.255.255.255 | DHCP     | 342    | DHCP Request - Transaction ID 0x9590fb5f62  |
| 9   | 12:57:25.110000 | 0.0.0.9 | 255.255.255.255 | DHCP     | 342    | DHCP Request - Transaction ID 0x9590fb5f73  |
| 10  | 12:57:25.110000 | 0.0.0.9 | 255.255.255.255 | DHCP     | 342    | DHCP Request - Transaction ID 0x9590fb5f84d |
| 11  | 12:57:25.110000 | 0.0.0.9 | 255.255.255.255 | DHCP     | 342    | DHCP Request - Transaction ID 0x9590fb5f952 |
| 12  | 12:57:25.110000 | 0.0.0.9 | 255.255.255.255 | DHCP     | 342    | DHCP Request - Transaction ID 0x9590fb5fa60 |
| 13  | 12:57:25.110000 | 0.0.0.9 | 255.255.255.255 | DHCP     | 342    | DHCP Request - Transaction ID 0x9590fb5fb70 |
| 14  | 12:57:25.110000 | 0.0.0.9 | 255.255.255.255 | DHCP     | 342    | DHCP Request - Transaction ID 0x9590fb5fc83 |
| 15  | 12:57:25.110000 | 0.0.0.9 | 255.255.255.255 | DHCP     | 342    | DHCP Request - Transaction ID 0x76a377ec    |

Student observation:

- Q) What is promiscuous mode?

Promiscuous mode is a setting for a network interface card (NIC) that allows it to capture all network packets passing through it regardless of the destination MAC address.

- Q) Does ARP packets have transport layer header? Explain.

No, ARP packets DO NOT have transport layer header. It sits between the network and data link layers - there is NO TCP or UDP involved. So no transport layer existing.

which transport  
it uses UD  
TCP for large

A-

What is a protocol?

It is

What is  
Address  
network: C

RESULT:

The tools:

plays only DHCP packets  
etc in its search for

3. Which transport layer protocol is used by DNS?  
It uses UDP for normal packets and  
TCP for large responses/zone transfers.

4. What is the port number used by HTTP  
protocol?

It uses port 80 by default.

5. What is broadcast IP address?  
Address to reach all hosts in a  
network.

rule?

a setting for a  
DHCP that allows if  
packets are passing  
the destination

transport layer

not have:  
between two  
nodes - there is  
so no transport

RESULT:

From the experiments on packets captured  
tool: WIRESHARK has been done successfully.