EX NO: 5 EXPERIMENT ON PACKET CAPTURE TOOL: WIRESHARK

DATE: 14.08.2025

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.

=) Store and display the contents of the various protocol fields in the message.

Description:

Wireshark, a network analysis tool formerly known as Ethereal, captures packet in real time and display them in human-readable format. 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 tool:

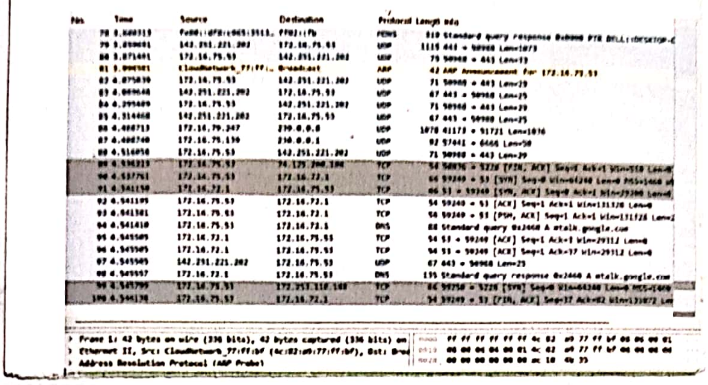
=) To filter, capture, view packets in Wireshark Tool.

=) Capture 100 packets from the Ethernet: IEEE 802.3 LAN Interface and save it.

Procedure:

- Select Local Area Connection in wireshark.
- Go to capture → option
- Select stop capture automatically after 100 packets
- Then click Start capture.
- Save the packets.

Output:



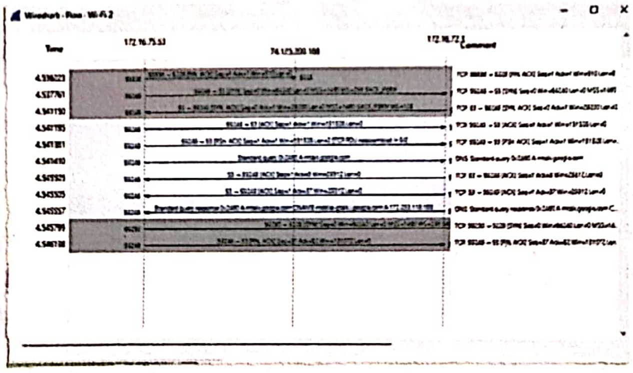
```
No.   Time      Source                    Destination       Protocol Length Info
  78 3.680319   fe80::df8:c065:5513…      ff02::fb          MDNS     519 Standard query response 0x0000 PTR DELL::DESKTOP-…
  79 3.890601   142.251.221.202           172.16.75.53      UDP     1115 443 → 50900 Len=1073
  80 3.871491   172.16.75.53              142.251.221.202   UDP       75 50900 → 443 Len=33
  81 3.990581   CloudNetwork_77:ff:…      Broadcast         ARP       42 ARP Announcement for 172.16.75.53
  82 4.075030   172.16.75.53              142.251.221.202   UDP       71 50900 → 443 Len=29
  83 4.089648   142.251.221.202           172.16.75.53      UDP       67 443 → 50900 Len=25
  84 4.295409   172.16.75.53              142.251.221.202   UDP       71 50900 → 443 Len=29
  85 4.314468   142.251.221.202           172.16.75.53      UDP       67 443 → 50900 Len=25
  86 4.400713   172.16.79.247             239.0.0.0         UDP     1070 41173 → 51721 Len=1076
  87 4.400740   172.16.75.130             230.0.0.1         UDP       92 57441 → 6666 Len=50
  88 4.516050   172.16.75.53              142.251.221.202   UDP       71 50900 → 443 Len=29
  89 4.536223   172.16.75.53              74.125.200.188    TCP       54 50836 → 5228 [FIN, ACK] Seq=1 Ack=1 Win=510 Len=0
  90 4.537761   172.16.75.53              172.16.72.1       TCP       66 59240 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 …
  91 4.541150   172.16.72.1               172.16.75.53      TCP       66 53 → 59240 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
  92 4.541195   172.16.75.53              172.16.72.1       TCP       54 59240 → 53 [ACK] Seq=1 Ack=1 Win=131328 Len=0
  93 4.541381   172.16.75.53              172.16.72.1       TCP       54 59240 → 53 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=…
  94 4.541410   172.16.75.53              172.16.72.1       DNS       88 Standard query 0x2460 A mtalk.google.com
  95 4.545505   172.16.72.1               172.16.75.53      TCP       54 53 → 59240 [ACK] Seq=1 Ack=1 Win=29312 Len=0
  96 4.545505   172.16.72.1               172.16.75.53      TCP       54 53 → 59240 [ACK] Seq=1 Ack=37 Win=29312 Len=0
  97 4.545505   142.251.221.202           172.16.75.53      UDP       67 443 → 50900 Len=25
  98 4.545557   172.16.72.1               172.16.75.53      DNS      135 Standard query response 0x2460 A mtalk.google.com
  99 4.545799   172.16.75.53              172.253.118.188   TCP       66 59250 → 5228 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
 100 4.546129   172.16.75.53              172.16.72.1       TCP       54 59240 → 53 [FIN, ACK] Seq=37 Ack=82 Win=131072 Len…

> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on
> Ethernet II, Src: CloudNetwork_77:ff:bf (4c:82:a9:77:ff:bf), Dst: Broa
> Address Resolution Protocol (ARP Probe)

0000  ff ff ff ff ff ff 4c 82  a9 77 ff bf 08 06 00 01
0010  08 00 06 04 00 01 4c 82  a9 77 ff bf 00 00 00 00
0020  00 00 00 00 00 00 ac 10  4b 35
```

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

Procedure:

- o Select LAN in wireshark.
- o Go to capture → option.
- o Select stop capture automatically after 100 packets.
- o Then click start capture.
- o Search TCP packets in search bar.
- o To see flow graph click Statistics → Flow graph.
- o Save the packets.

Flow Graph:

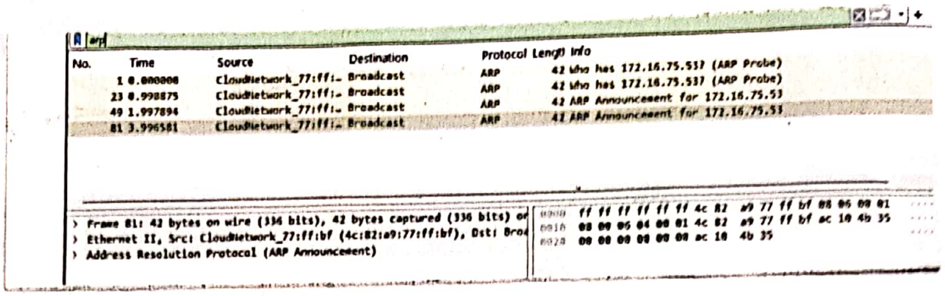


2. Create a Filter to display only ARP packets and inspect the packets.

Procedure:

- o Search ARP packets in search bar.
- o Save the packets.

Output :



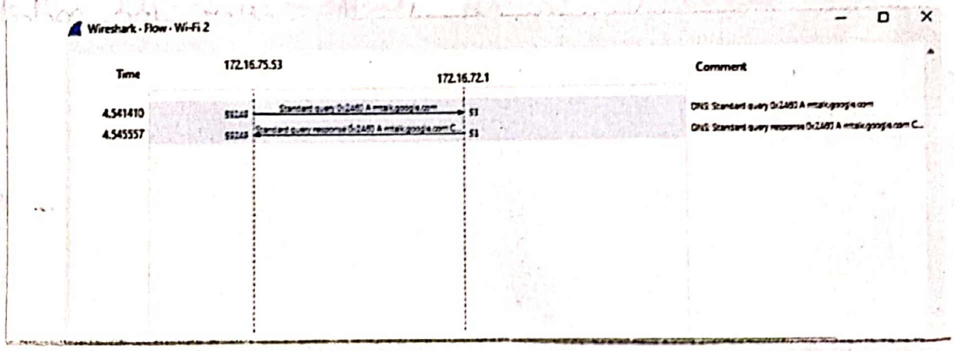
```
arp
No.   Time       Source                   Destination   Protocol Length Info
    1 0.000000   CloudNetwork_77:ff:…     Broadcast     ARP      42 Who has 172.16.75.53? (ARP Probe)
   23 0.998875   CloudNetwork_77:ff:…     Broadcast     ARP      42 Who has 172.16.75.53? (ARP Probe)
   49 1.997894   CloudNetwork_77:ff:…     Broadcast     ARP      42 ARP Announcement for 172.16.75.53
   81 3.996581   CloudNetwork_77:ff:…     Broadcast     ARP      42 ARP Announcement for 172.16.75.53

> Frame 81: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) o
> Ethernet II, Src: CloudNetwork_77:ff:bf (4c:82:a9:77:ff:bf), Dst: Bro
> Address Resolution Protocol (ARP Announcement)

0000  ff ff ff ff ff ff 4c 82  a9 77 ff bf 08 06 00 01
0010  08 00 06 04 00 01 4c 82  a9 77 ff bf ac 10 4b 35
0020  00 00 00 00 00 00 ac 10  4b 35
```

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 :



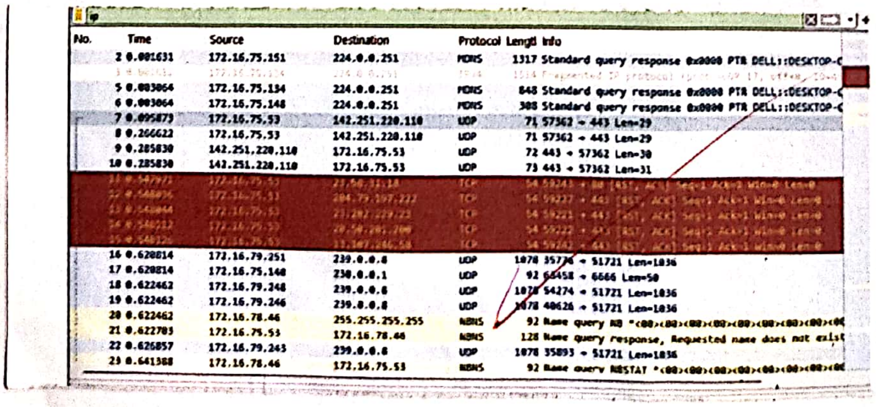
```
Wireshark · Flow · Wi-Fi 2

Time        172.16.75.53                                  172.16.72.1    Comment
4.541410    59248  Standard query 0x2480 A mtalk.google.com  →  53      DNS: Standard query 0x2480 A mtalk.google.com
4.545557    59248  ←  Standard query response 0x2480 A mtalk.google.com C…  53   DNS: Standard query response 0x2480 A mtalk.google.com C…
```

4. Create a Filter to display only IP/ICMP packets and inspect the packets.

Procedure :

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

Output :



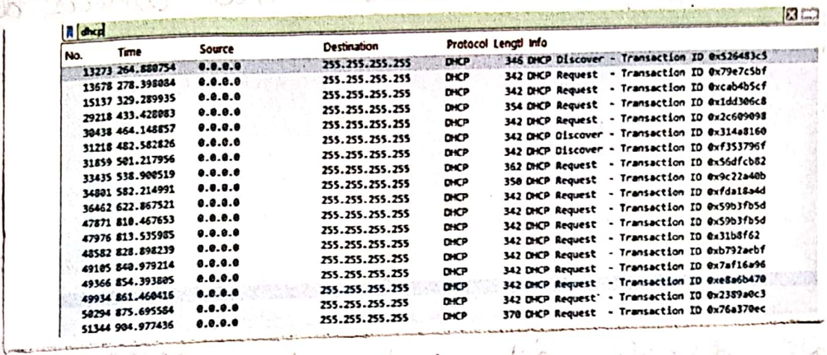
```
ip
No.   Time       Source            Destination        Protocol Length Info
    2 0.001631   172.16.75.151     224.0.0.251        MDNS     1317 Standard query response 0x0000 PTR DELL::DESKTOP-C
    3 0.001631   172.16.75.134     224.0.0.251        IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=
    5 0.003064   172.16.75.134     224.0.0.251        MDNS      848 Standard query response 0x0000 PTR DELL::DESKTOP-C
    6 0.003064   172.16.75.148     224.0.0.251        MDNS      308 Standard query response 0x0000 PTR DELL::DESKTOP-C
    7 0.095873   172.16.75.53      142.251.220.110    UDP        71 57362 → 443 Len=29
    8 0.266622   172.16.75.53      142.251.220.110    UDP        71 57362 → 443 Len=29
    9 0.285830   142.251.220.110   172.16.75.53       UDP        72 443 → 57362 Len=30
   10 0.285830   142.251.220.110   172.16.75.53       UDP        73 443 → 57362 Len=31
   11 0.547971   172.16.75.53      23.56.31.18        TCP        54 59243 → 80 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
   12 0.548036   172.16.75.53      204.79.197.222     TCP        54 59227 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   13 0.548044   172.16.75.53      23.202.229.23      TCP        54 59221 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   14 0.548212   172.16.75.53      20.50.201.200      TCP        54 59222 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   15 0.548126   172.16.75.53      13.107.246.58      TCP        54 59242 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   16 0.620814   172.16.79.251     239.0.0.8          UDP      1078 35776 → 51721 Len=1036
   17 0.620814   172.16.75.148     230.0.0.1          UDP        92 64458 → 6666 Len=50
   18 0.622462   172.16.79.248     239.0.0.8          UDP      1078 54274 → 51721 Len=1036
   19 0.622462   172.16.79.246     239.0.0.8          UDP      1078 40626 → 51721 Len=1036
   20 0.622462   172.16.78.46      255.255.255.255    NBNS       92 Name query NB "<00><00><00><00><00><00><00><00><0
   21 0.622703   172.16.75.53      172.16.78.46       NBNS      128 Name query response, Requested name does not exist
   22 0.626857   172.16.79.243     239.0.0.8          UDP      1078 35893 → 51721 Len=1036
   23 0.641388   172.16.78.46      172.16.75.53       NBNS       92 Name query NBSTAT "<00><00><00><00><00><00><00><0
```

5. Create a Filter to display only DHCP packets and inspect the packets

Procedure:

- Search DHCP packets in search bar
- Save the packets.

Output:



dhcp

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 13273 | 264.880754 | 0.0.0.0 | 255.255.255.255 | DHCP | 346 | DHCP Discover - Transaction ID 0x526483c5 |
| 13678 | 278.398084 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Request - Transaction ID 0x79e7c5bf |
| 15137 | 329.289935 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Request - Transaction ID 0xcab4b5cf |
| 29218 | 433.428083 | 0.0.0.0 | 255.255.255.255 | DHCP | 354 | DHCP Request - Transaction ID 0x1dd306c8 |
| 30438 | 464.148857 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Request - Transaction ID 0x2c609098 |
| 31218 | 482.582826 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Discover - Transaction ID 0x314a8160 |
| 31859 | 501.217956 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Discover - Transaction ID 0xf353796f |
| 33435 | 538.900519 | 0.0.0.0 | 255.255.255.255 | DHCP | 362 | DHCP Request - Transaction ID 0x56dfcb82 |
| 34801 | 582.214991 | 0.0.0.0 | 255.255.255.255 | DHCP | 350 | DHCP Request - Transaction ID 0x9c22a40b |
| 36462 | 622.867521 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Request - Transaction ID 0xfda18a4d |
| 47871 | 810.467653 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Request - Transaction ID 0x59b3fb5d |
| 47976 | 813.535985 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Request - Transaction ID 0x59b3fb5d |
| 48582 | 828.898239 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Request - Transaction ID 0x31b8f62 |
| 49105 | 840.979214 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Request - Transaction ID 0xb792aebf |
| 49366 | 854.393805 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Request - Transaction ID 0x7af16a96 |
| 49934 | 861.460416 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Request - Transaction ID 0xe8a6b470 |
| 50294 | 875.695584 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Request - Transaction ID 0x2389a0c3 |
| 51344 | 904.977436 | 0.0.0.0 | 255.255.255.255 | DHCP | 370 | DHCP Request - Transaction ID 0x76a370ec |

Student Observation:

1. What is promiscuous mode?

Ans: 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.

2. Does ARP packets has transport layer header? Explain.

Ans: No, ARP packets do not have a transport layer header. It sits between the network and data link layers - there is no TCP or UDP involved, so no transport layer header exists.

3. Which transport layer protocol is used by DNS?

Ans: It uses UDP for normal queries and TCP for large responses / zone transfers.

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

Ans: It uses port 80 by default.

5. What is broadcast IP address?

Ans: Address to reach all hosts in a network (192.168.1.255/24

4/9/2

Result:

Thus the experiments on packet capture tool: Wireshark has been done successfully.