

EX NO:4b
DATE:07.08.24

Analyze Network traffic using Wireshark tool

AIM:

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

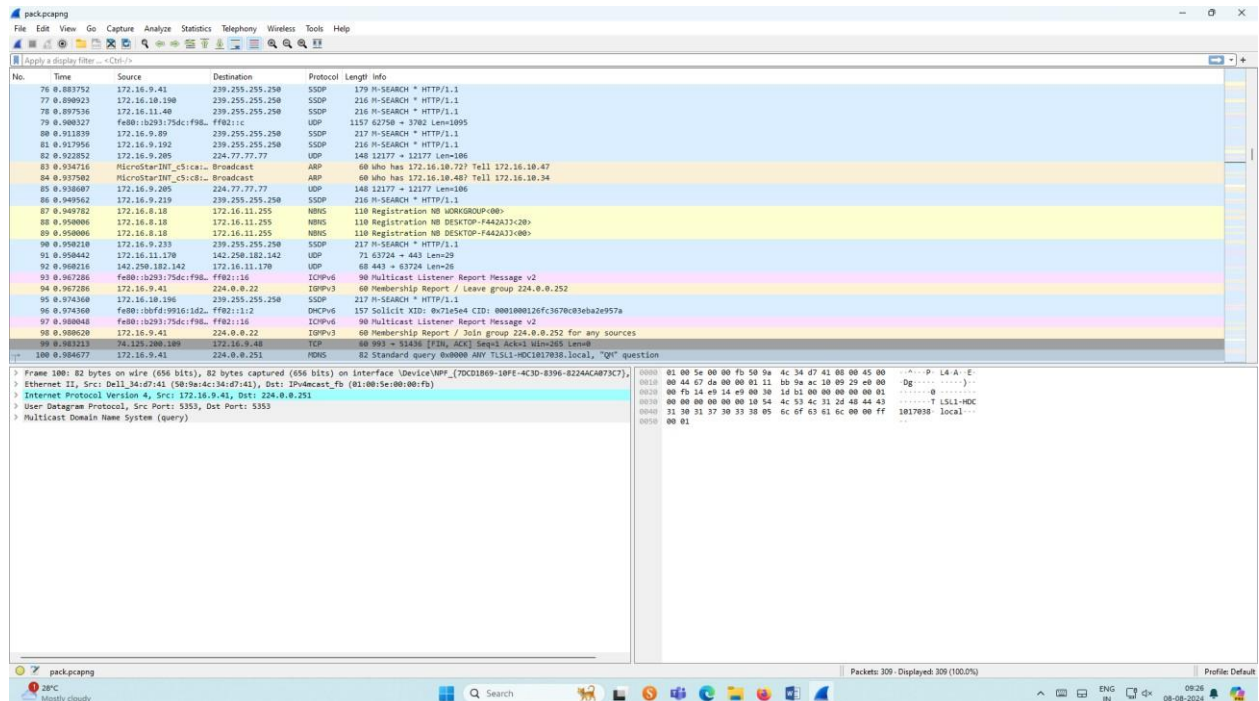
Exercises

1. 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



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

Procedure

- Select Local Area Connection in Wireshark.
- Go to capture ☐ option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search TCP packets in search bar.
- To see flow graph click Statistics ☐ Flow graph. ➤ Save the packets.

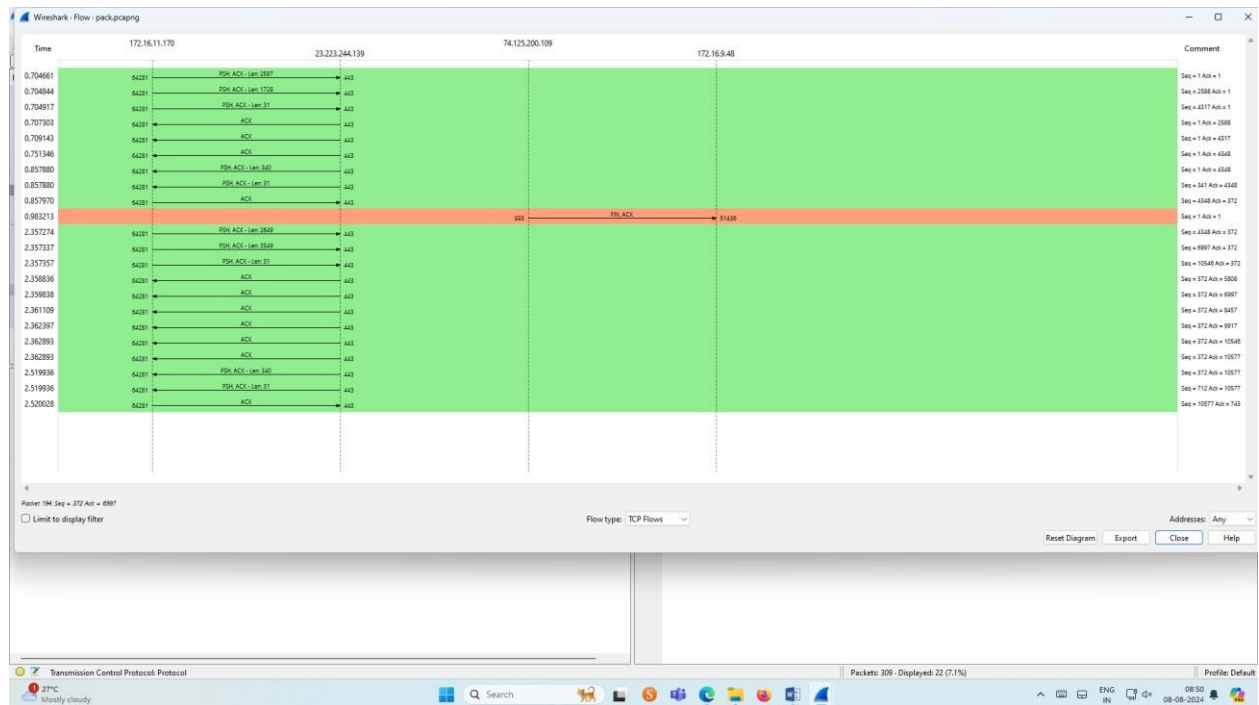
Output:

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The main window is divided into three panes:

- Packet List:** Shows a list of captured packets. The selected packet (No. 198) is a TCP segment from 172.16.11.170 to 23.223.244.139, with sequence number 60443 and acknowledgment number 64281.
- Packet Details:** Shows the structure of the selected packet. It is an Ethernet II frame, an Internet Protocol Version 4 packet, and a Transmission Control Protocol (TCP) segment. The TCP segment details show the source port as 443 and the destination port as 64281.
- Packet Bytes:** Shows the raw data of the packet in hexadecimal and ASCII format.

The status bar at the bottom indicates that 22 packets are displayed (7.1% of the total capture).

Flow Graph output

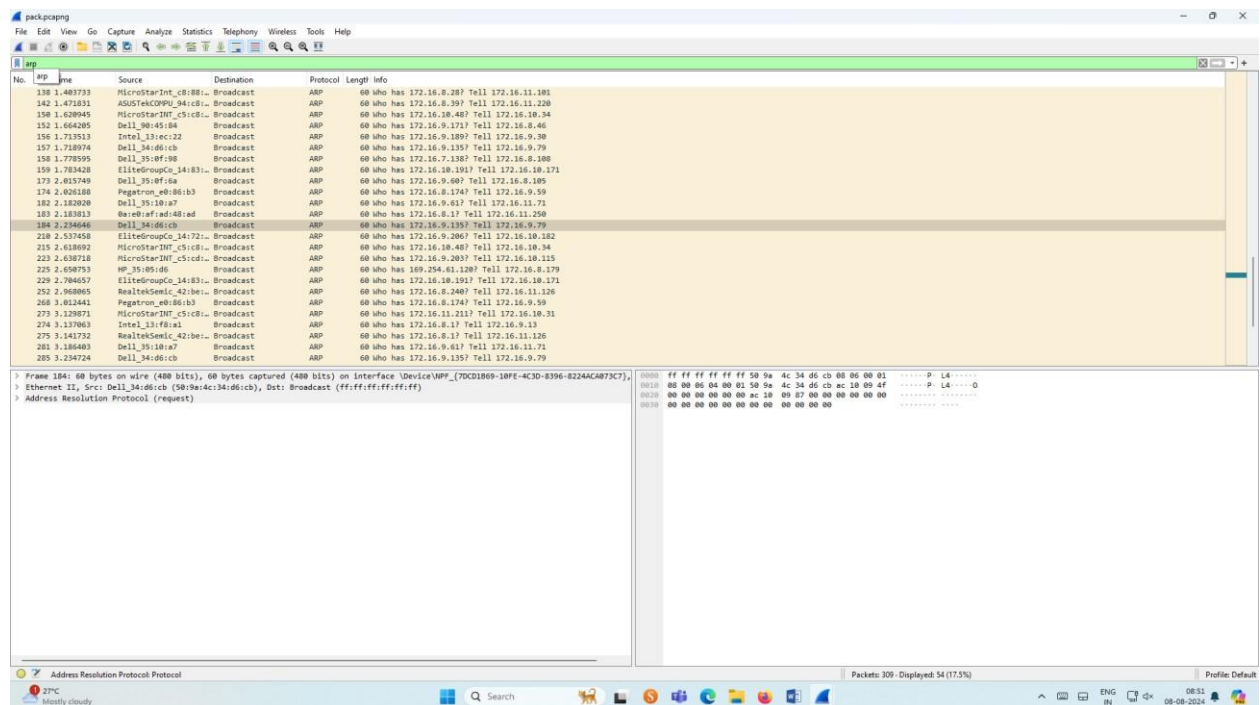


3.Create a Filter to display only ARP packets and inspect the packets.

Procedure

- Select Local Area Connection in Wireshark.
- Go to capture ☐ option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search ARP packets in search bar.
- Save the packets.

Output



4.Create a Filter to display only DNS packets and provide the flow graph.

Procedure

- Select Local Area Connection in Wireshark.
- Go to capture ☐ option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search DNS packets in search bar.

- To see flow graph click Statistics □ Flow graph.
- Save the packets.

Output

The screenshot displays the Wireshark interface with a packet capture of DNS traffic. The packet list on the left shows four packets:

No.	Time	Source	Destination	Protocol	Length	Info
385	4.824856	172.16.11.170	172.16.8.1	DNS	79	Standard query 0xc945 A fp-vp.azureedge.net
387	4.838791	172.16.8.1	172.16.11.170	DNS	146	Standard query response 0xc945 A fp-vp.azureedge.net CNAME fp-vp.ec.azureedge.net CNAME cs9.wpc.vcdn.net A 117.18.232.200
388	4.838791	172.16.8.1	172.16.11.170	DNS	146	Standard query response 0xc945 A fp-vp.azureedge.net CNAME fp-vp.ec.azureedge.net CNAME cs9.wpc.vcdn.net A 117.18.232.200

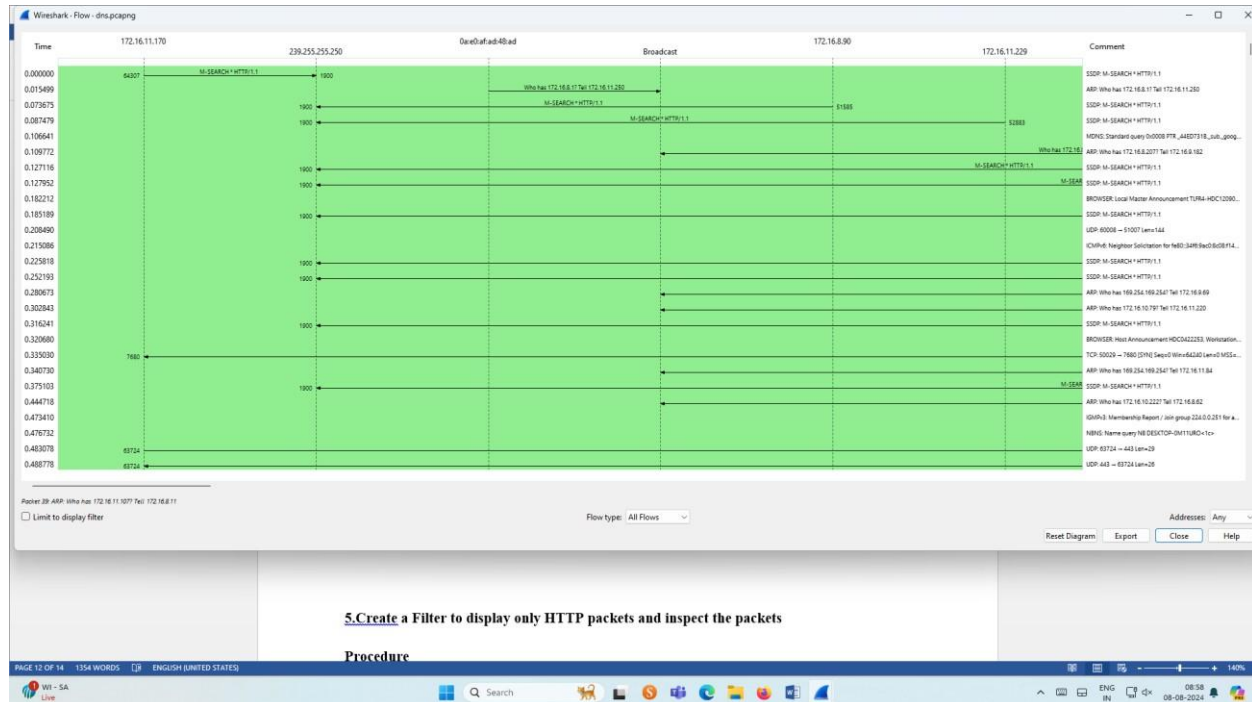
The packet details pane on the right shows the structure of the selected packet (No. 387):

- Frame 373: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface \Device\NPF_{70CD1869-10FE-4C3D-8396-8224ACAB73C7}...
- Ethernet II, Src: HP_39:1e:d9 (7c:57:58:39:1e:d9), Dst: Sophos_cf:be:45 (7c:5a:1c:cf:be:45)
- Internet Protocol Version 4, Src: 172.16.11.170, Dst: 172.16.8.1
- User Datagram Protocol, Src Port: 53868, Dst Port: 53
- Domain Name System (query)

The packet bytes pane on the right shows the raw data in hexadecimal and ASCII:

```
0000  7c 5a 1c cf be 45 7c 57 58 39 1e d9 00 00 45 00  |Z- E|u X9...E|
0010  00 41 6d 38 00 00 11 00 00 ac 10 00 aa ac 10     |AmS...|
0020  00 01 c0 14 00 00 2d 6c 00 c9 45 01 00 00 01     |S- 1-E...|
0030  00 00 00 00 00 05 68 70 2d 76 70 09 61 7a 75     |.....f p-vp.az|
0040  72 65 65 64 67 65 83 6a 65 74 00 00 01 00 01     |reeedge n et...|
```

Graph output



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

Procedure

- Select Local Area Connection in Wireshark.
- Go to capture ☐ option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search HTTP packets in the search bar.
- Save the packets.

Output

The image shows a Wireshark packet capture of an HTTP transaction. The packet list on the left shows three packets: a GET request (No. 1238), a 200 OK response (No. 1253), and a 301 redirect response (No. 1258). The selected packet (No. 1238) is expanded in the packet details pane, showing the Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol layers. The packet bytes pane on the right displays the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1238	0.000000	172.16.11.170	23.215.215.114	HTTP	208	GET /connecttest.txt HTTP/1.1
1253	0.000000	23.215.215.114	172.16.11.170	HTTP	301	HTTP/1.1 200 OK (text/plain)
1258	0.000000	23.215.215.114	172.16.11.170	HTTP	301	HTTP/1.1 200 OK (text/plain)

Frame 1238: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interface \Device\NPF_{70CD1869-18FE-4C3D-8396-B224ACAB7} Ethernet II, Src: WP_39:1e:d9 (7c:57:58:39:1e:d9), Dst: Sophos_cf:be:45 (7c:5a:1c:cf:be:45)

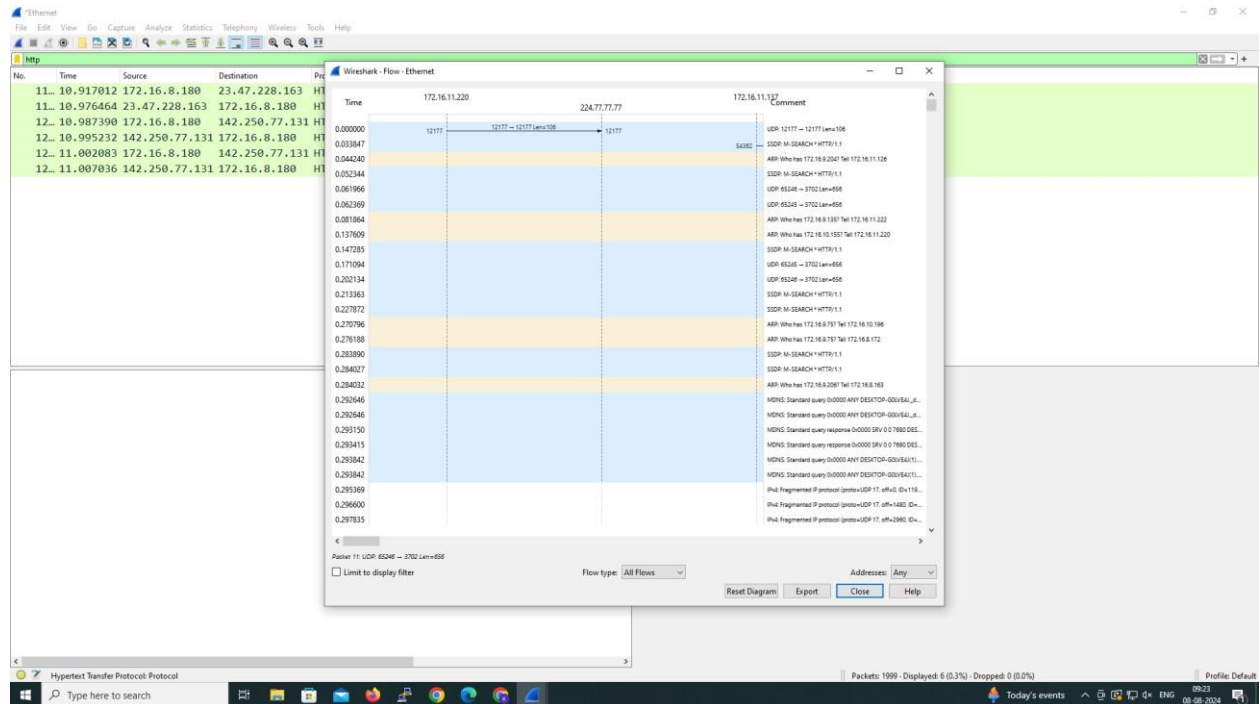
Internet Protocol Version 4, Src: 172.16.11.170, Dst: 23.215.215.114

Transmission Control Protocol, Src Port: 64337, Dst Port: 80, Seq: 1, Ack: 1, Len: 154

Hypertext Transfer Protocol

7c 5a 1c cf be 45 7c 57 58 39 1e d9 08 00 45 00 [Z...E]W X9...E-
0010 08 c2 24 25 48 08 08 00 00 00 ac 18 80 aa 17 d7 580
0020 d7 72 f0 51 08 58 db 49 a5 c0 2a 43 a4 7c 58 18 r-Q P I ...c |p-
0030 81 80 a7 b8 00 00 47 45 54 20 2f 63 6f 6e 6e 65 ...-GE T /conne
0040 63 74 74 65 73 74 2e 74 78 74 20 48 54 54 50 2f cttest.txt HTTP/
0050 31 2e 31 0d 8a 43 61 63 68 65 2d 43 6f 6e 74 72 1:1-Cac he-Contr
0060 6f 6c 3a 20 6e 6f 2d 63 61 63 68 65 8d 8a 43 6f all no-c ache- Co
0070 6e 6e 65 63 74 69 6f 6e 3a 20 43 6c 6f 73 65 0d nection + Close
0080 8a 58 72 61 67 6d 61 3a 20 6e 6f 2d 63 61 63 68 Pragma: no-cach
0090 65 8d 8a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d e User-Agent: H
00a0 69 63 72 6f 73 6f 66 74 20 4e 43 53 49 0d 8a 48 icrosoft MCS1 H
00b0 6f 73 74 3a 20 77 77 77 2e 6d 73 66 74 63 6f 6e ost: www .sftcon
00c0 6e 65 63 74 74 65 73 74 2e 63 6f 6d 6d 8a 6d 8a mectest .com...

Flow Graph output

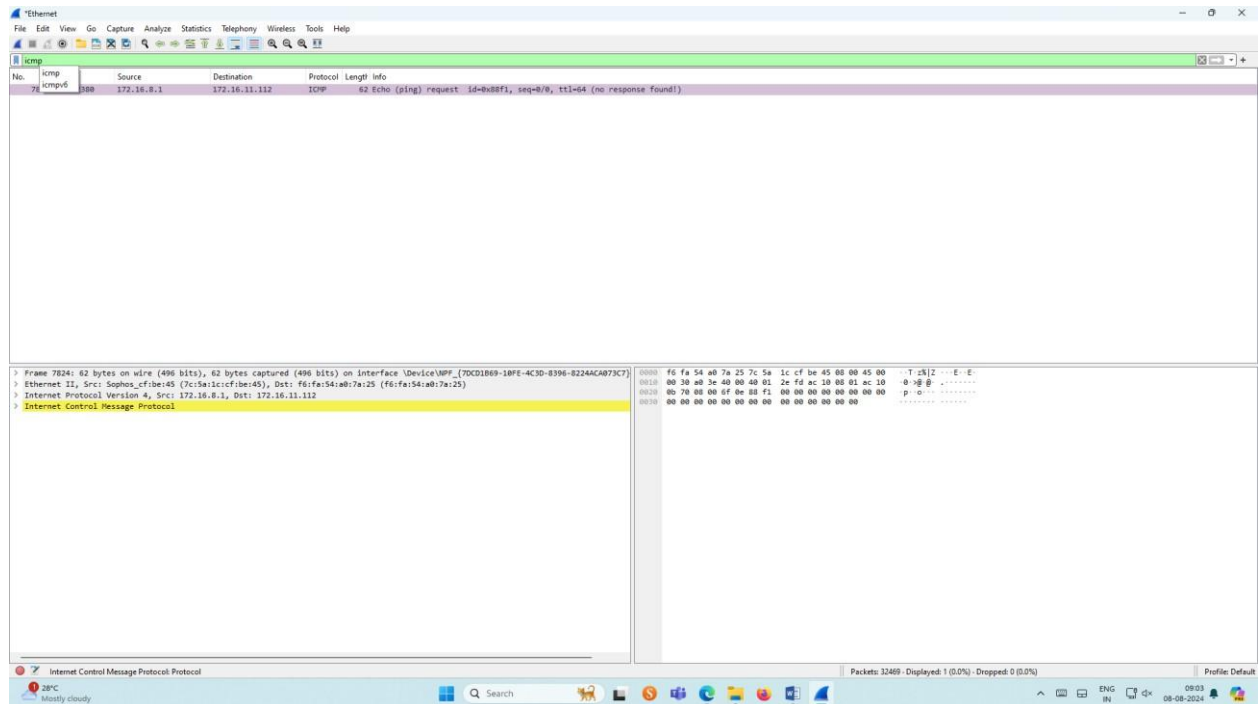


6.Create a Filter to display only IP/ICMP packets and inspect the packets.

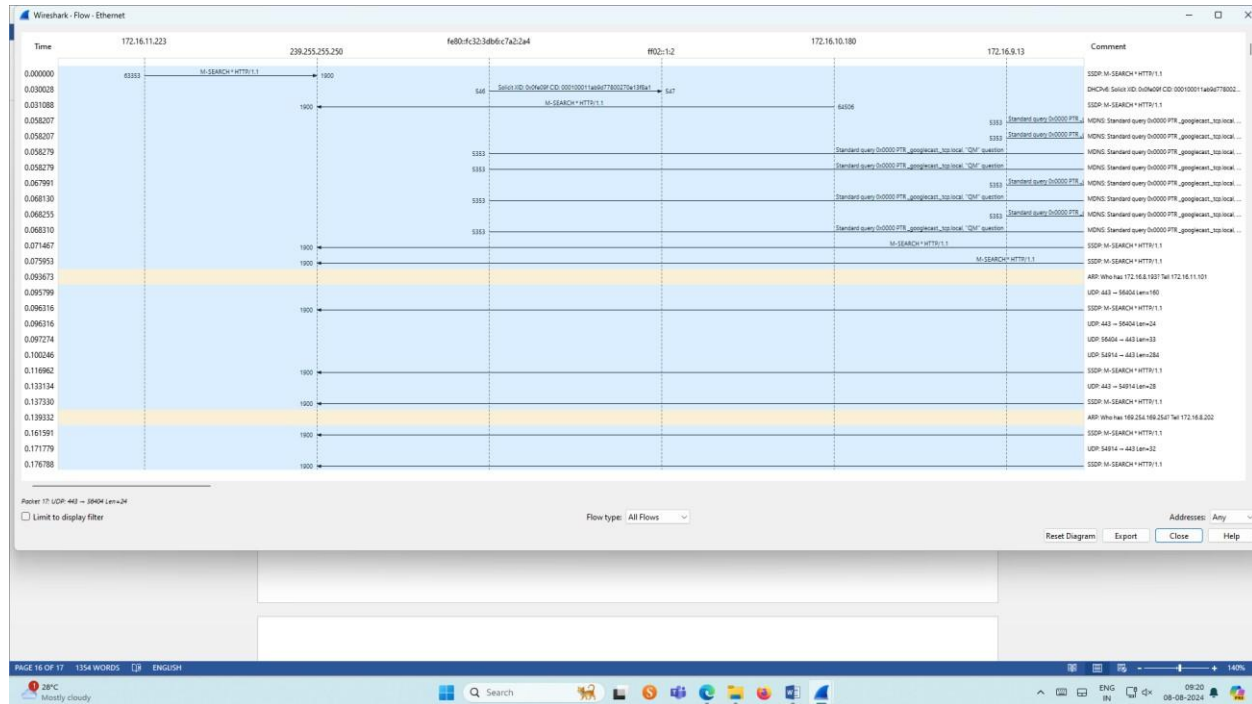
Procedure

- Select Local Area Connection in Wireshark.
- Go to capture ☐ option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search ICMP/IP packets in search bar.
- Save the packets

Output



Flow Graph output



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

Procedure

- Select Local Area Connection in Wireshark.
- Go to capture ☐ option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search DHCP packets in search bar.
- Save the packets

[illegible]

Thus, the study of packet sniffing using Wireshark has been verified.