
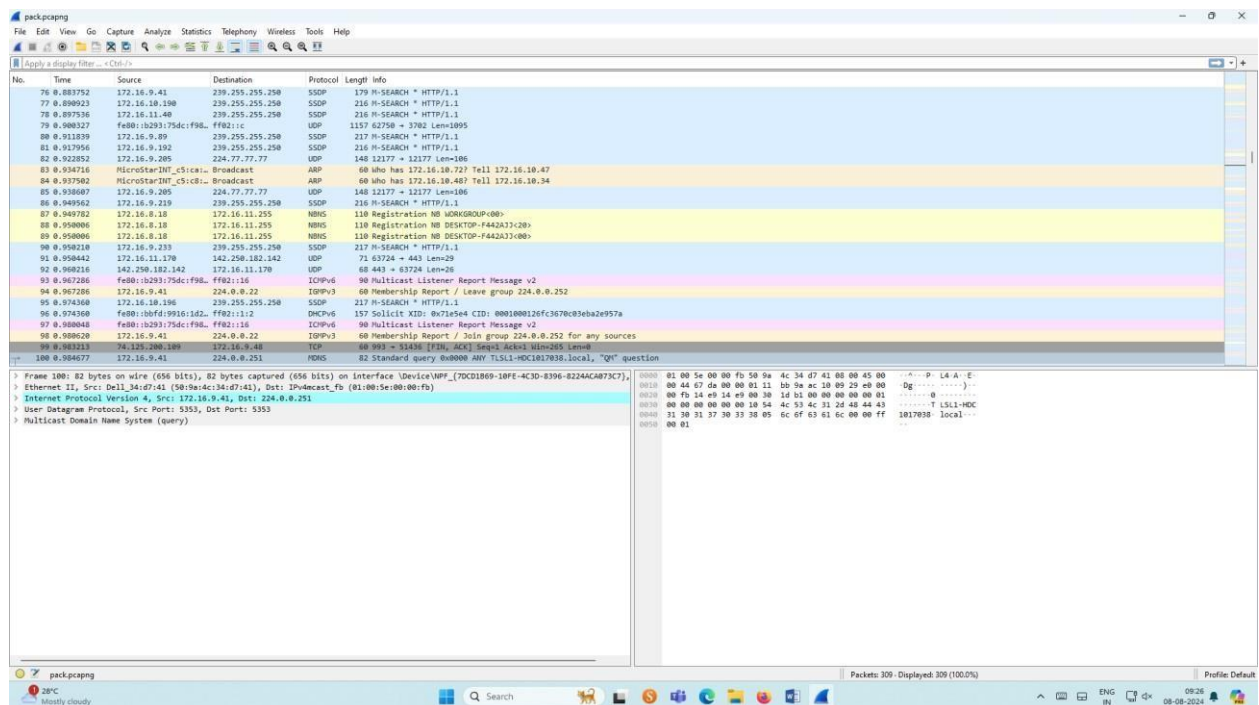


Ex No: 4 b**Date:14:8:24****ANALYZE NETWORK TRAFFIC USING WIRESHARK TOOL****AIM:**

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.

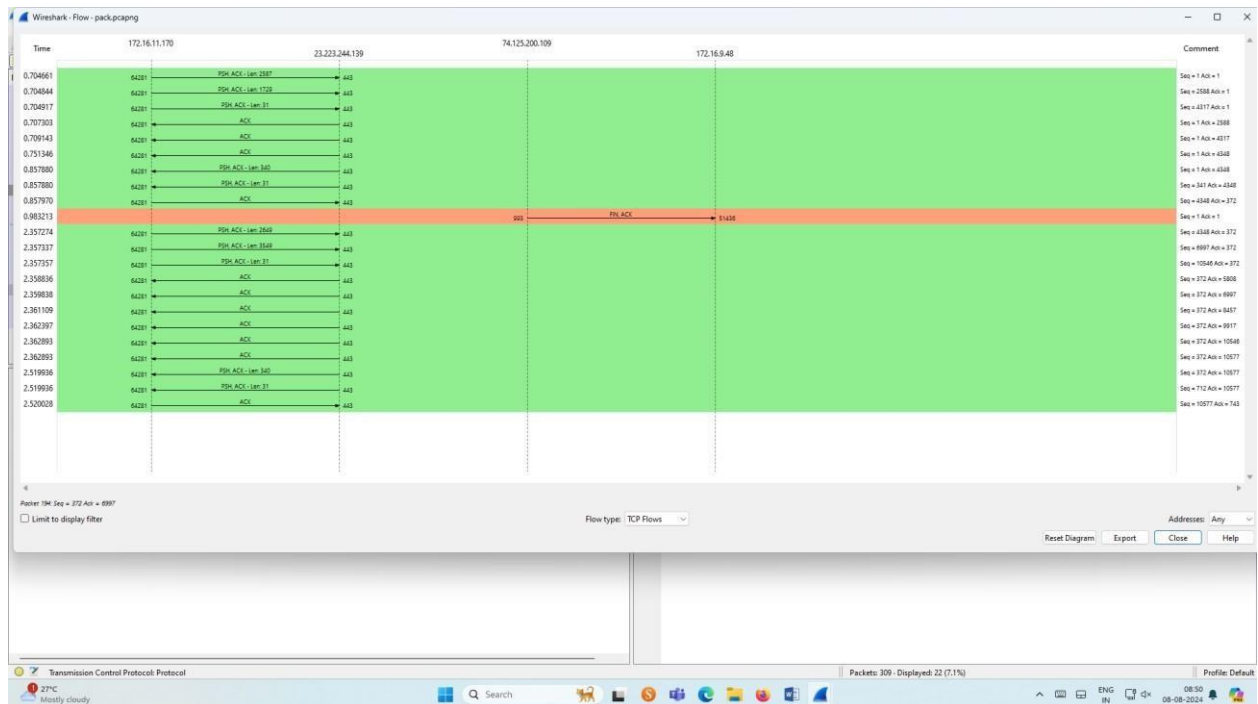
Output:

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 toolbar contains icons for various functions like opening files, capturing, and analyzing. The main window is divided into three panes:

- Packet List:** Shows a list of captured packets. The selected packet is No. 190, a TCP Reset (RST) from 172.16.11.170 to 23.223.244.139.
- Packet Details:** Shows the structure of the selected packet. It is a Transmission Control Protocol (TCP) segment with a Reset flag (RST), Sequence number 372, Acknowledgment number 5088, and Window size 1502.
- Packet Bytes:** Shows the raw data of the selected packet in hexadecimal and ASCII format.


The status bar at the bottom indicates that 309 packets are displayed, representing 7.1% of the total capture. The system tray shows the date and time as 08-08-2024, 08:49.

Flow Graph output

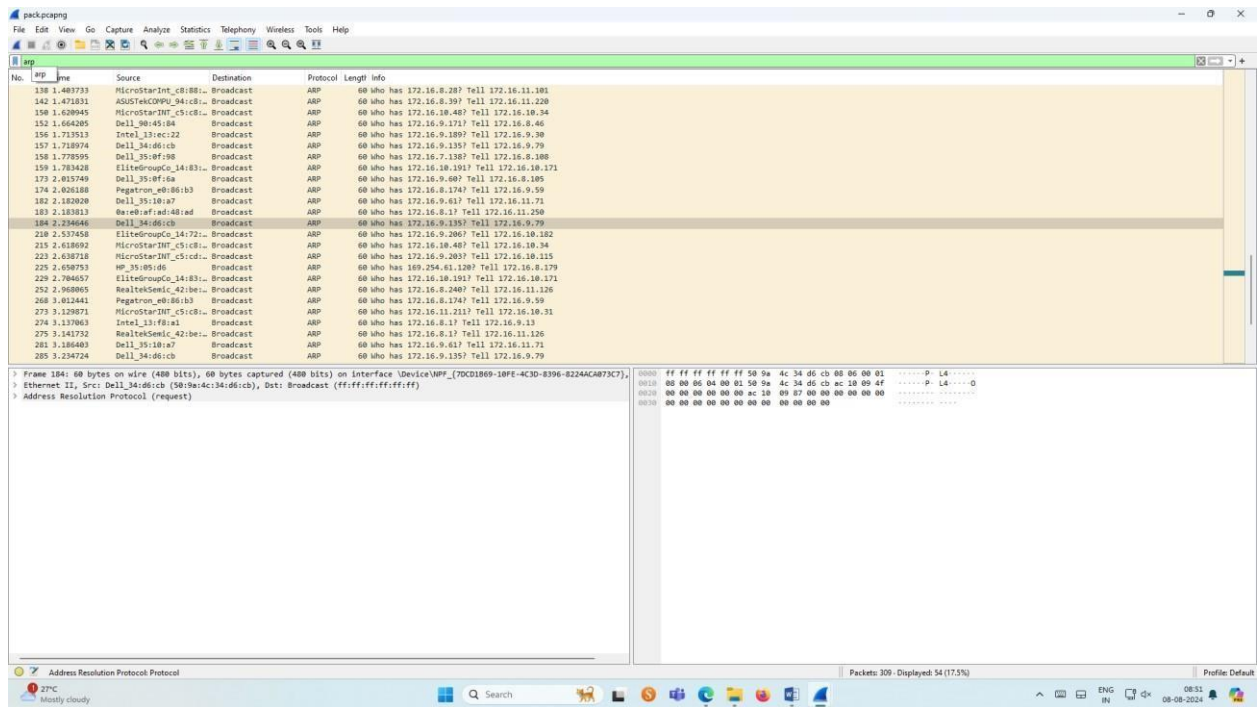


3.Create a Filter to display only ARP packets and inspect the packets.

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



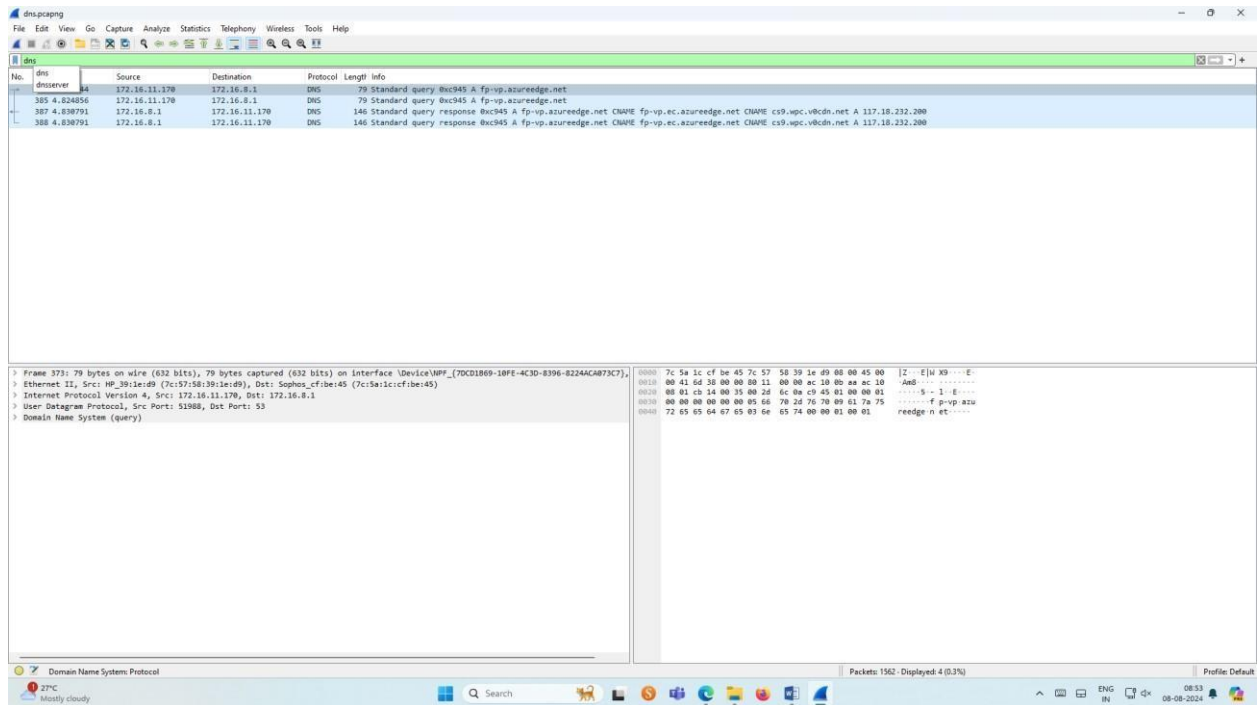
4.Create a Filter to display only DNS packets and provide the flow graph.

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 list of captured DNS packets. The packet list shows four entries, all of which are DNS Standard query responses from 172.16.11.170 to 172.16.8.1. The packet details pane on the right shows the structure of a DNS Standard query response, including the Ethernet II header, Internet Protocol Version 4 header, User Datagram Protocol header, and Domain Name System (query) header. The packet bytes pane on the right shows the raw data of the packet, including the Ethernet II header, Internet Protocol Version 4 header, User Datagram Protocol header, and Domain Name System (query) header.

No.	Time	Source	Destination	Protocol	Length	Info
385	4.824856	172.16.11.170	172.16.8.1	DNS	79	Standard query response 8xc945 A fp-vp.azureedge.net
387	4.838791	172.16.8.1	172.16.11.170	DNS	146	Standard query response 8xc945 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 8xc945 A fp-vp.azureedge.net CNAME fp-vp.ec.azureedge.net CNAME cs9.wpc.vcdn.net A 117.18.232.200

Frame 373: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface \Device\NPF_{70CD1869-10FE-4C3D-8396-8224ACAB73C7} 2

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: 53888, Dst Port: 53

Domain Name System (query)

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 00 11 00 00 ac 10 00 aa ac 10 ...A&... ..

0020 00 01 c9 14 00 15 00 2d cc 00 cf 45 01 00 00 01 ...S...I...E...

0030 00 00 00 00 00 00 05 68 70 2d 76 70 09 61 7a 75f p-vp azu

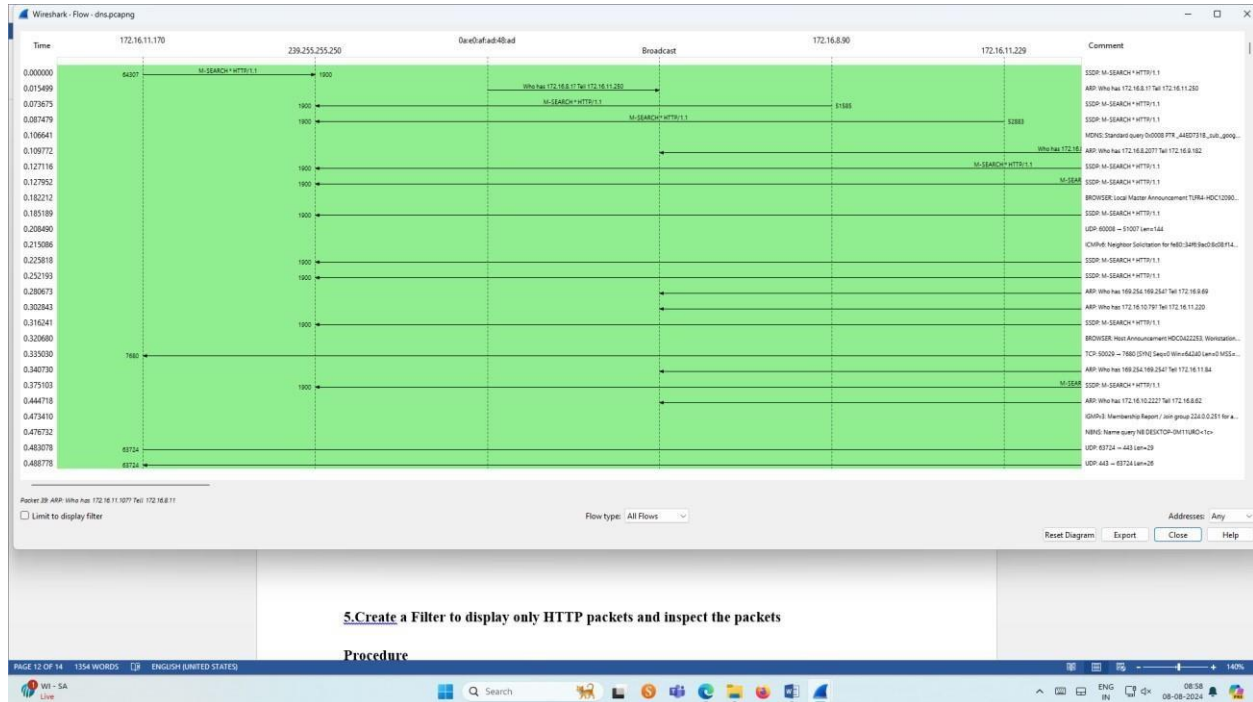
0040 72 65 65 64 67 65 63 6a 65 74 00 00 01 00 01 ...eedge n et:....

Domain Name System Protocol

Packets: 1562 - Displayed: 4 (0.3%)


Profile: Default

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 four packets:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.11.170	23.215.215.114	HTTP	208	GET /connecttest.txt HTTP/1.1
2	0.000000	172.16.11.170	23.215.215.114	HTTP	208	GET /connecttest.txt HTTP/1.1
3	0.000000	23.215.215.114	172.16.11.170	HTTP	301	HTTP/1.1 200 OK (text/plain)
4	0.000000	23.215.215.114	172.16.11.170	HTTP	301	HTTP/1.1 200 OK (text/plain)

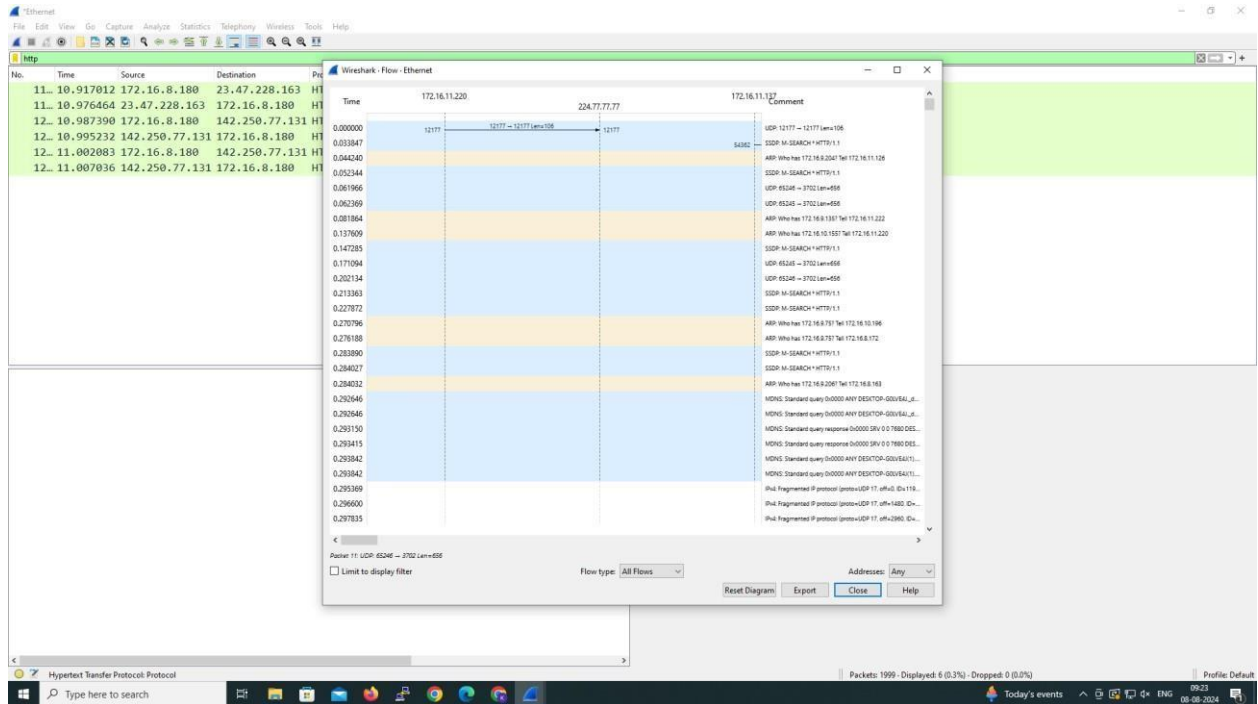
The packet details pane on the right shows the structure of the selected packet (No. 1):

- Frame 1238: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interface \Device\NPF_{70CD1B69-10FE-4C3D-8396-B224ACAB7} Ethernet II, Src: VM_39:1e:d9 (7c:5b:91:1e: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

The packet bytes pane on the right shows the raw data of the selected packet (No. 1):


```
0000 7c 5a 1c cf be 45 7c 57 58 39 1e d9 00 00 45 00 [Z...E]W X0...E-
0010 00 c2 24 25 40 00 00 00 00 00 ac 10 00 aa 17 d7 380 .....
0020 d7 72 fb 51 00 50 d0 49 a5 c0 2a 43 a4 7c 50 18 r-Q P I ...c [p-
0030 01 00 a7 50 00 00 47 45 54 20 2f 63 6f 6e 6e 65 ...GE T /comme
0040 63 74 74 65 73 74 24 74 70 74 20 40 54 54 50 2f cttest.txt HTTP/
0050 31 2e 31 0d 0a 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 0d 0a 43 6f all no-c ache- Co
0070 6e 6e 65 63 74 69 6f 6e 3a 20 43 6c 6f 73 65 0d nnection + Close
0080 0a 50 72 61 67 6d 61 3a 20 6e 6f 2d 63 61 63 68 Pragma: no-cach
0090 65 0d 0a 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 0a 40 icrosoft NCS1.1 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 0a 6d 0a necttest .com...
```

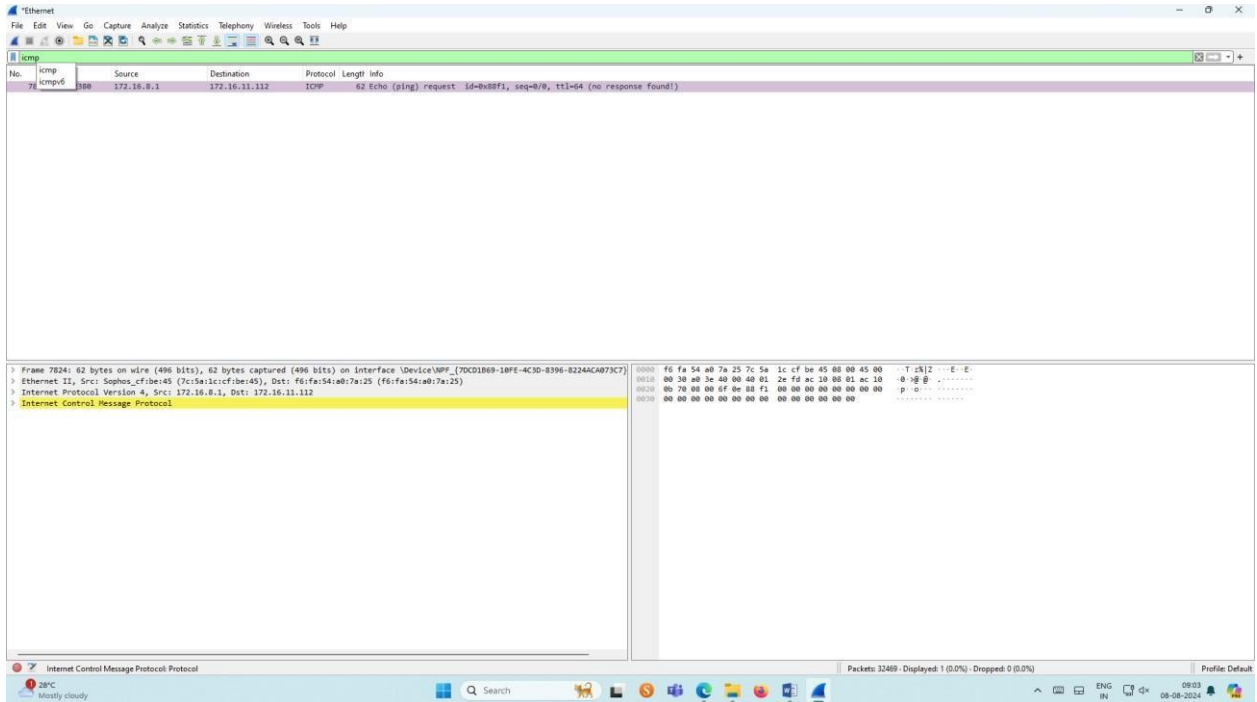
Flow Graph output



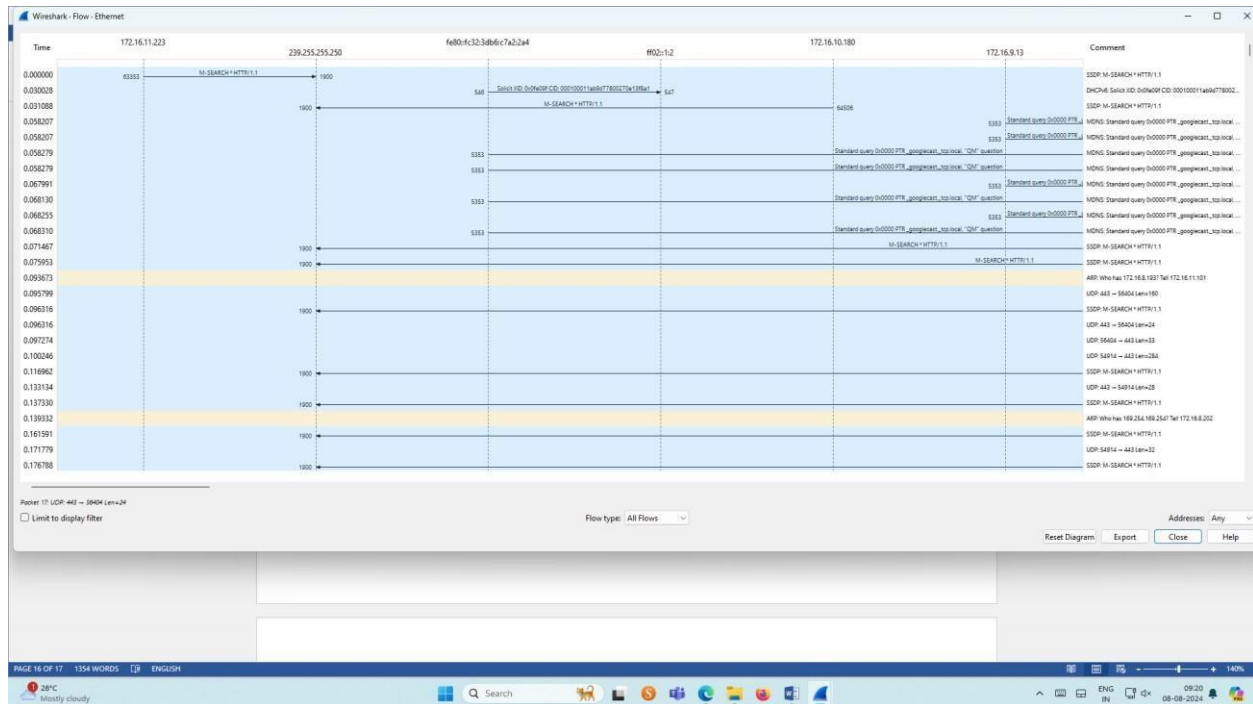
6.Create a Filter to display only IP/ICMP packets and inspect the packets.

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



Flow Graph output

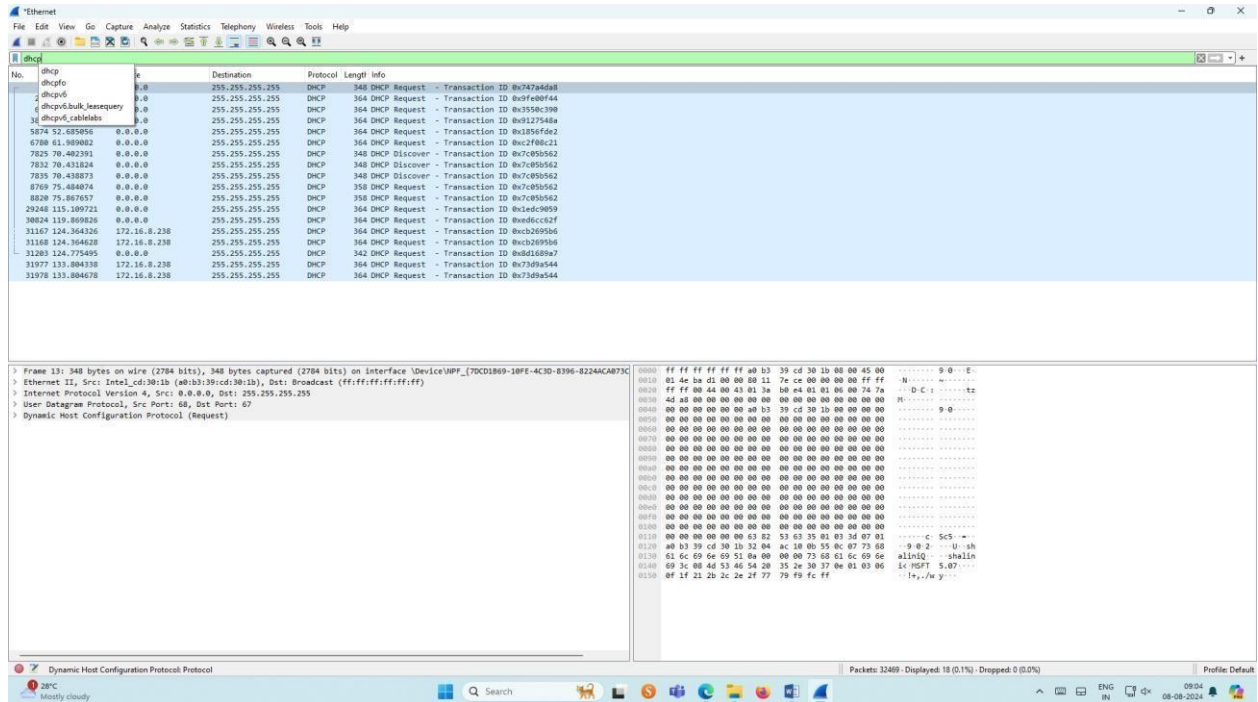


7.Create a Filter to display only DHCP packets and inspect the packets.

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

Output



Result:

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