
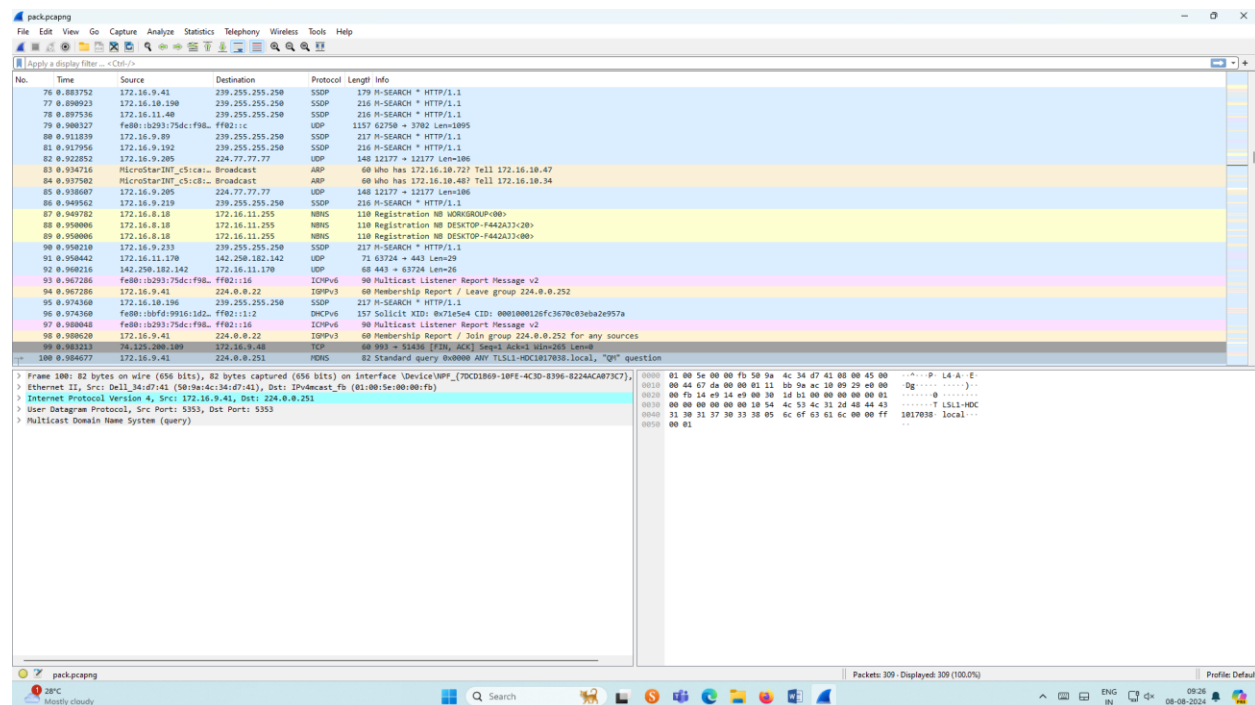


Ex No: 4 b PACKET SNIFFING USING WIRESHARK**AIM:**

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:

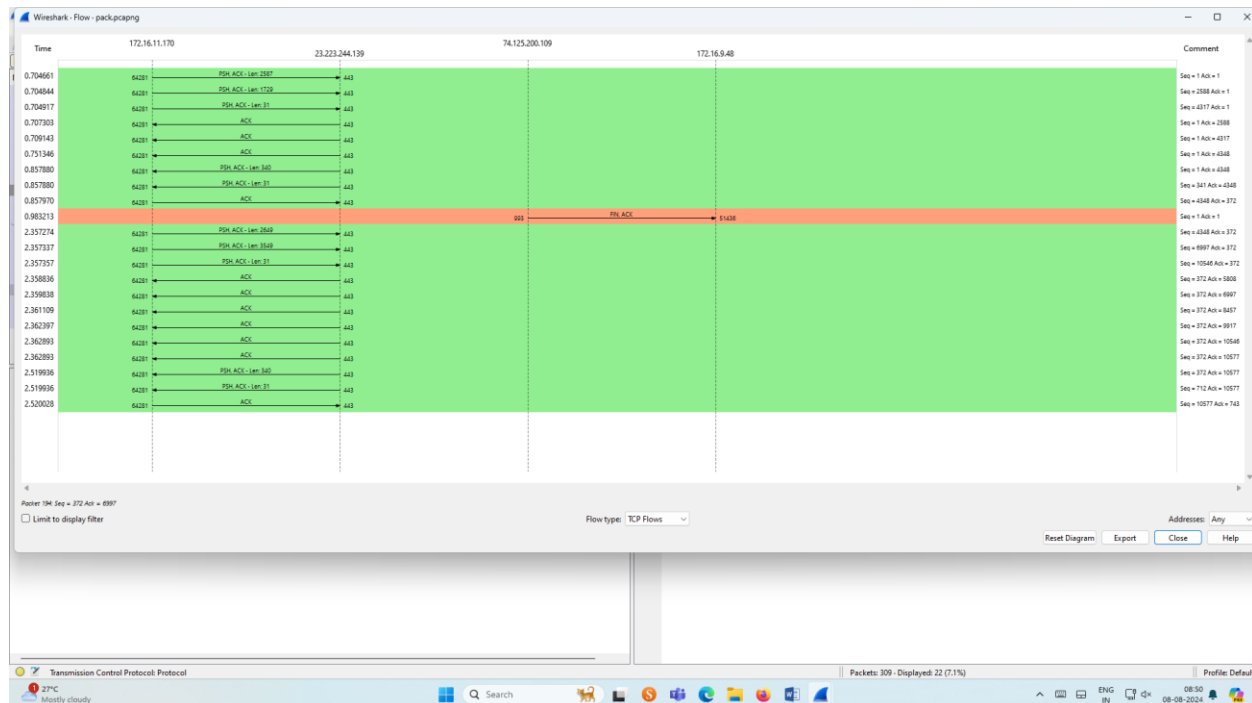
The screenshot displays the Wireshark interface with a capture of network traffic. The packet list pane shows several TCP packets, including application data and acknowledgments (ACK). The packet details pane for the selected packet (No. 190) shows the Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (TCP) layers. The packet bytes pane shows the raw data in hexadecimal and ASCII. The status bar at the bottom indicates that 309 packets were captured, and 22 packets are currently displayed (7.1%).

No.	Time	Source	Destination	Protocol	Length	Info
90	0.794661	172.16.11.170	23.223.244.139	TLSv1.2	2641	Application Data
91	0.794664	172.16.11.170	23.223.244.139	TLSv1.2	1703	Application Data
92	0.794917	172.16.11.170	23.223.244.139	TLSv1.2	85	Application Data
93	0.797303	23.223.244.139	172.16.11.170	TCP	60	443 → 64281 [ACK] Seq=1 Ack=2588 Win=1447 Len=0
94	0.799143	23.223.244.139	172.16.11.170	TCP	60	443 → 64281 [ACK] Seq=1 Ack=4317 Win=1493 Len=0
95	0.751346	23.223.244.139	172.16.11.170	TCP	60	443 → 64281 [ACK] Seq=1 Ack=4348 Win=1493 Len=0
96	0.857888	23.223.244.139	172.16.11.170	TLSv1.2	394	Application Data
97	0.857888	23.223.244.139	172.16.11.170	TLSv1.2	85	Application Data
98	0.857978	172.16.11.170	23.223.244.139	TCP	54	64281 → 443 [ACK] Seq=4348 Ack=372 Win=1824 Len=0
99	0.983213	78.125.200.189	172.16.9.48	TCP	60	993 → 51436 [FIN, ACK] Seq=1 Ack=1 Win=295 Len=0
100	2.357274	172.16.11.170	23.223.244.139	TLSv1.2	2783	Application Data
101	2.357337	172.16.11.170	23.223.244.139	TLSv1.2	3603	Application Data
102	2.357357	172.16.11.170	23.223.244.139	TLSv1.2	85	Application Data
103	2.358836	23.223.244.139	172.16.11.170	TCP	60	443 → 64281 [ACK] Seq=372 Ack=5088 Win=1502 Len=0
104	2.358838	23.223.244.139	172.16.11.170	TCP	60	443 → 64281 [ACK] Seq=372 Ack=9997 Win=1502 Len=0
105	2.362189	23.223.244.139	172.16.11.170	TCP	60	443 → 64281 [ACK] Seq=372 Ack=9457 Win=1502 Len=0
106	2.362397	23.223.244.139	172.16.11.170	TCP	60	443 → 64281 [ACK] Seq=372 Ack=9917 Win=1502 Len=0
107	2.362393	23.223.244.139	172.16.11.170	TCP	60	443 → 64281 [ACK] Seq=372 Ack=10546 Win=1502 Len=0
108	2.362393	23.223.244.139	172.16.11.170	TCP	60	443 → 64281 [ACK] Seq=372 Ack=10577 Win=1502 Len=0
206	2.519936	23.223.244.139	172.16.11.170	TLSv1.2	394	Application Data
207	2.519936	23.223.244.139	172.16.11.170	TLSv1.2	85	Application Data
208	2.520028	172.16.11.170	23.223.244.139	TCP	54	64281 → 443 [ACK] Seq=10577 Ack=743 Win=1822 Len=0

Frame 190: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on Interface \Device\NPF_{70CD1869-18FE-4C3D-8396-B224AC873C7},
 > Ethernet II, Src: Sophos_cf:be:e45 (7c:5a:1c:f1:b1:e45), Dst: HP_39:1e:d9 (7c:57:58:39:1e:d9)
 > Internet Protocol Version 4, Src: 23.223.244.139, Dst: 172.16.11.170
 > Transmission Control Protocol, Src Port: 443, Dst Port: 64281, Seq: 372, Ack: 10577, Len: 0


0000 7c 57 58 39 1e d9 7c 5a 1c f1 b1 e45 00 00 00 00 [X]...E...
 0010 00 28 1c 0c 40 00 40 06 5a 9f 17 df f4 8b ac 10Z.....
 0020 8b aa 01 b0 f9 19 88 9c 6e 48 8e a5 d5 16 5b 10m...P...
 0030 95 de 93 5b 00 00 00 00 00 00 00 00[.....

Flow Graph output

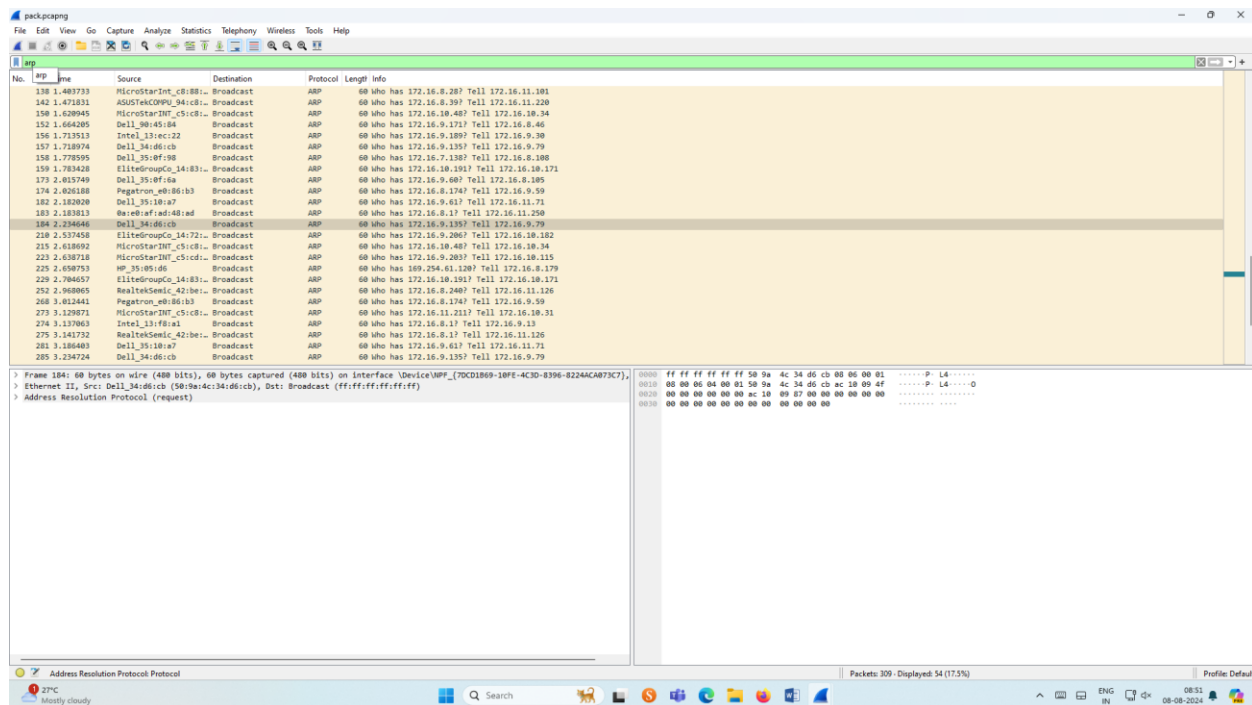


3.Create a Filter to display only ARP packets and inspect the packets.

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

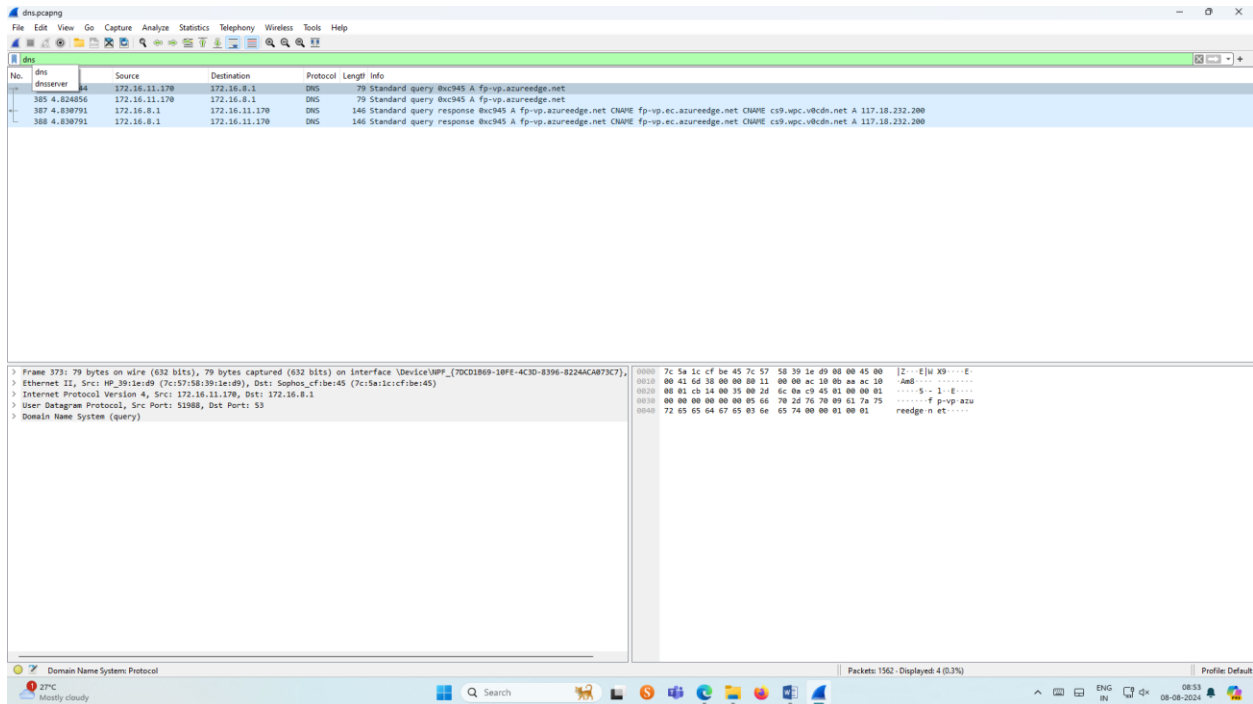


4.Create a Filter to display only DNS packets and provide the flow graph.

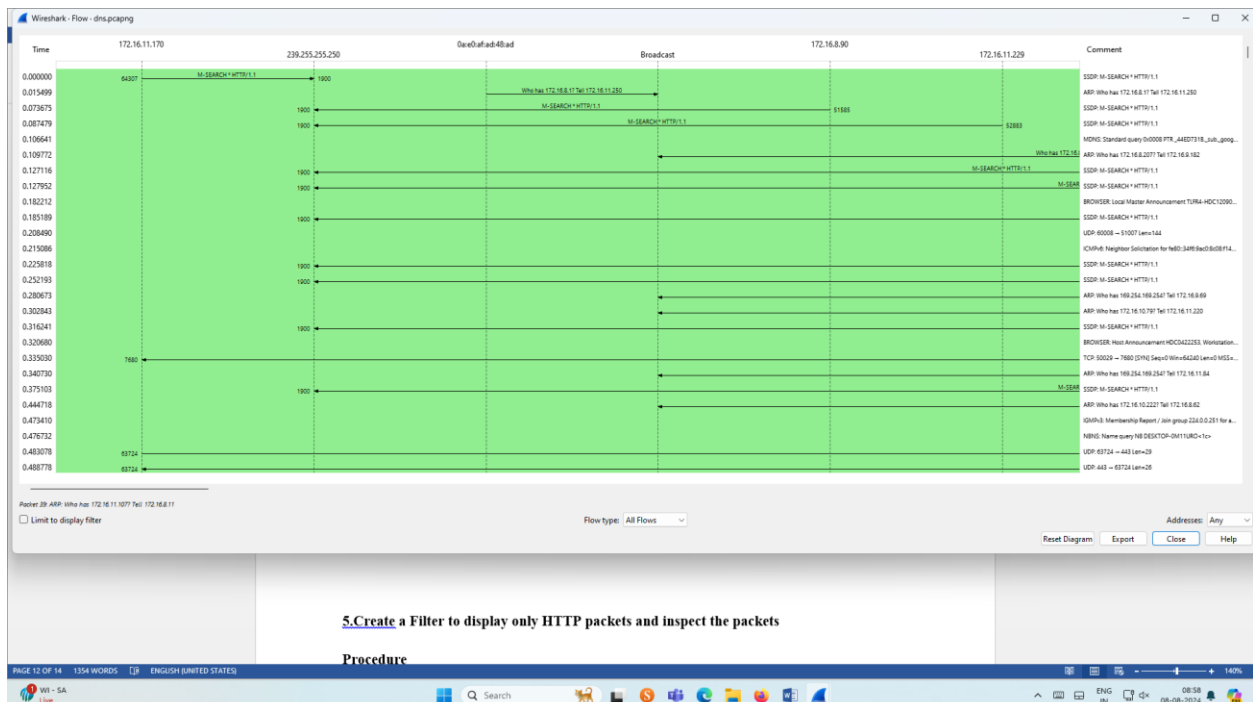
Procedure

- 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




Graph output

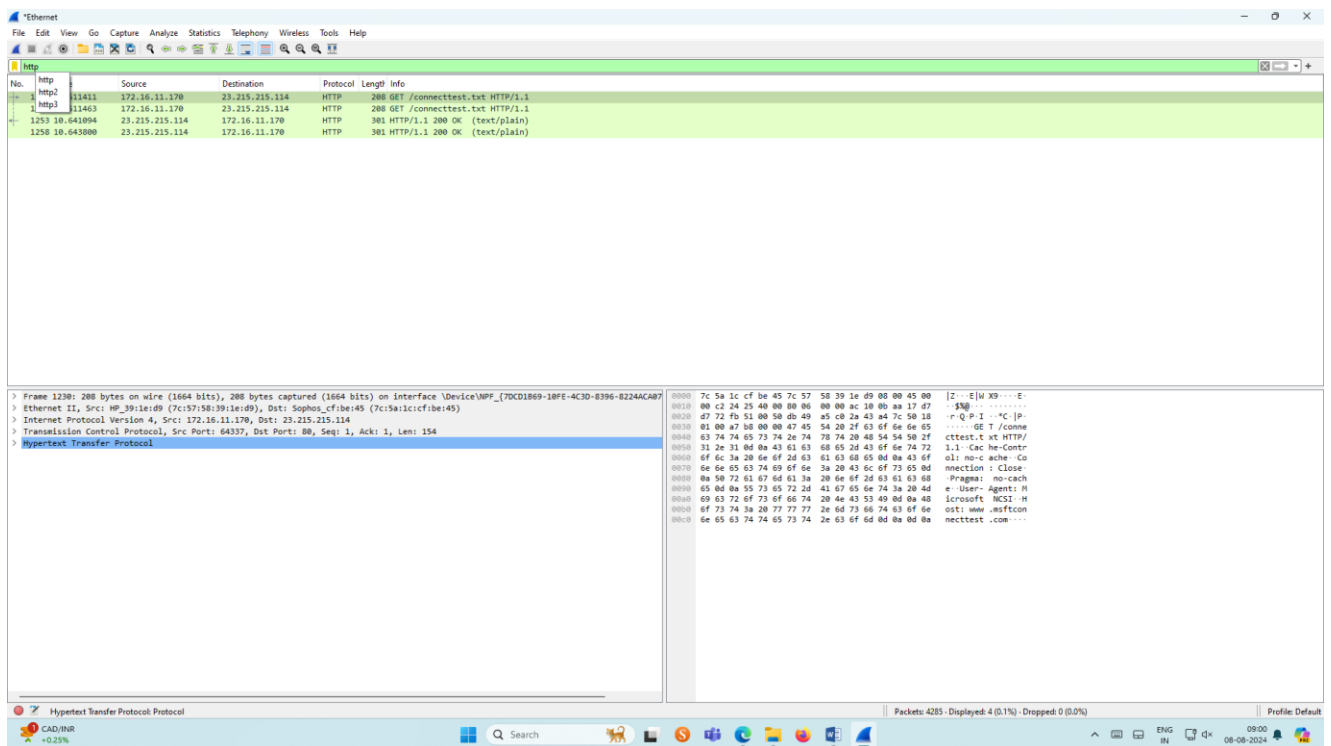


5.Create a Filter to display only HTTP packets and inspect the packets

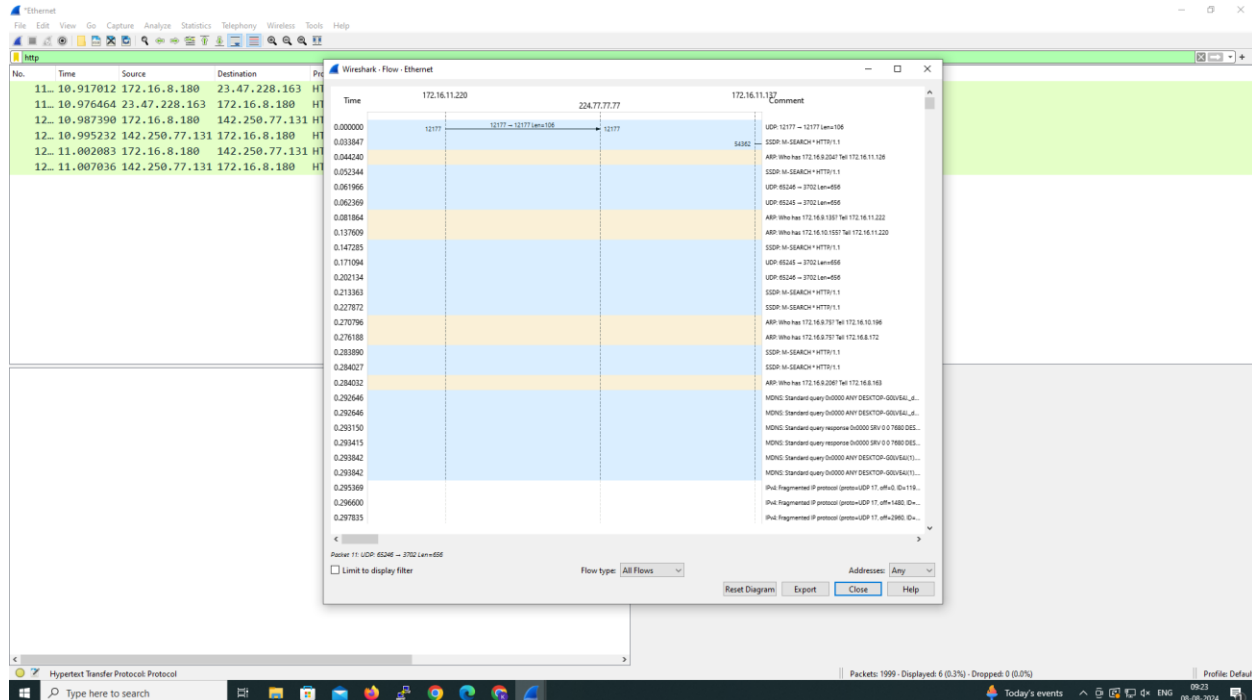
Procedure

- 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



Flow Graph output

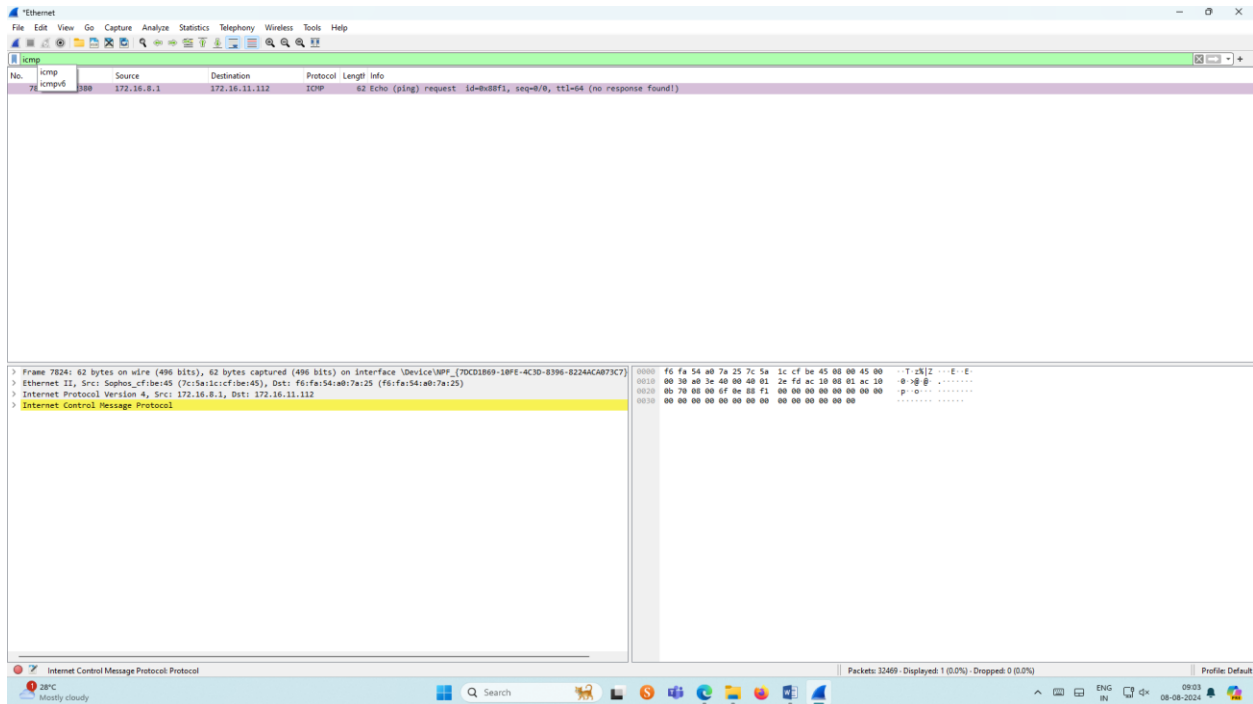


6.Create a Filter to display only IP/ICMP packets and inspect the packets.

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

