
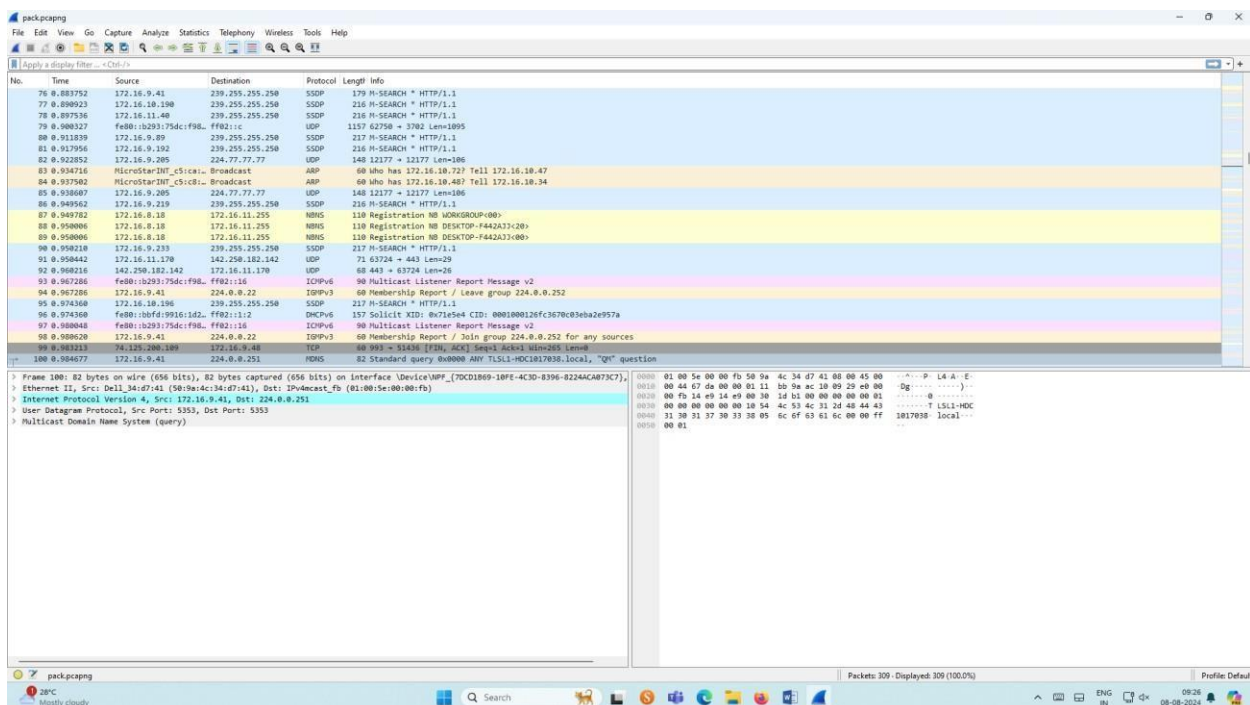


PACKET SNIFFING USING WIRESHARK**AIM:****Exercises****1. Capture 100 packets from the Ethernet: IEEE 802.3 LAN Interface and save it.****Procedure**

- 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


The screenshot shows the Wireshark interface with a packet capture of 100 packets. The packet list on the left shows various protocols including HTTP, ARP, NDIS, ICMPv6, DHCPv6, and TCP. The packet details pane on the right shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Multicast Domain Name System.

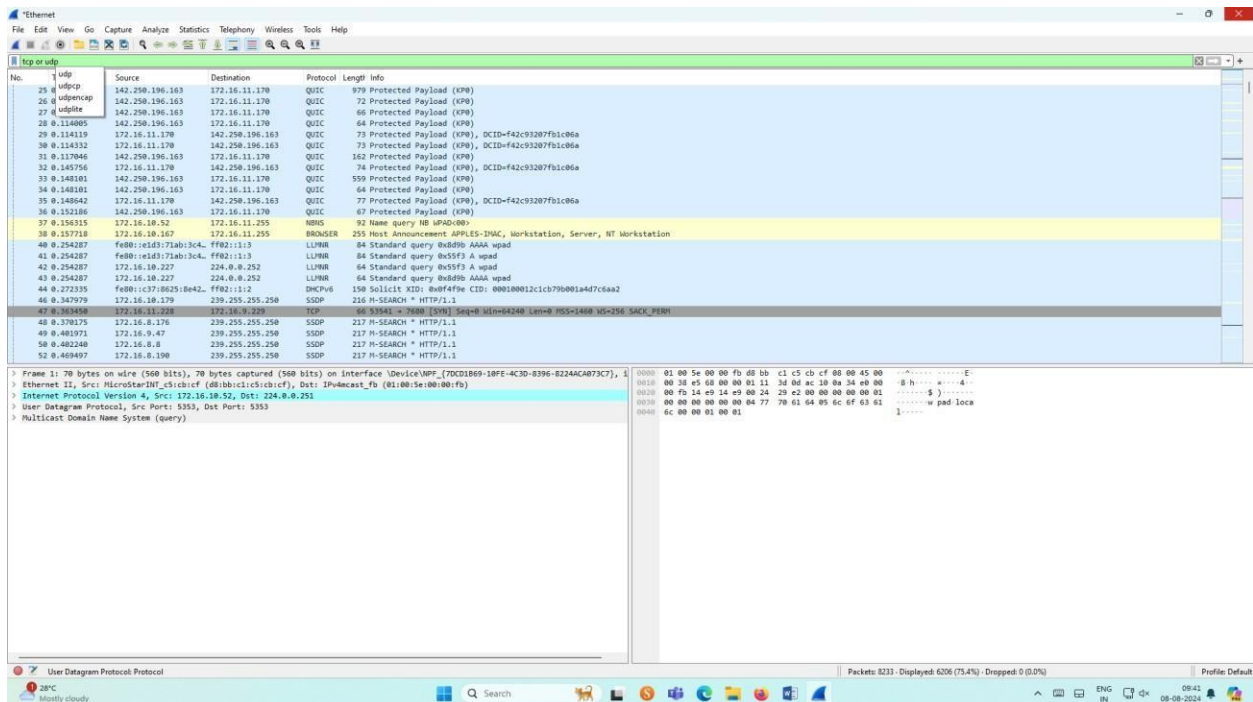
2. Create a Filter to display only TCP/UDP packets, inspect the packets and provide the flow graph.

CS23532

Procedure

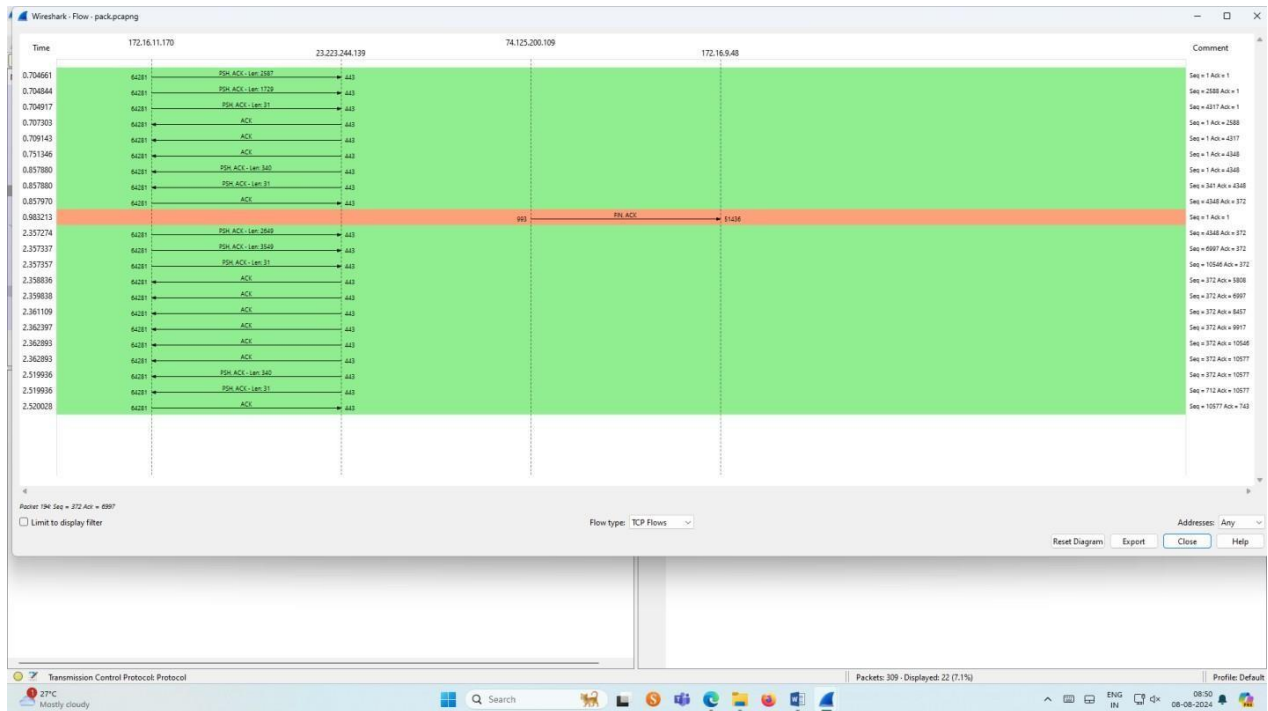
- Select Local Area Connection in Wireshark.
- Go to capture  option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search TCP packets in search bar.
- To see flow graph click Statistics  Flow graph.
- Save the packets.

Output:

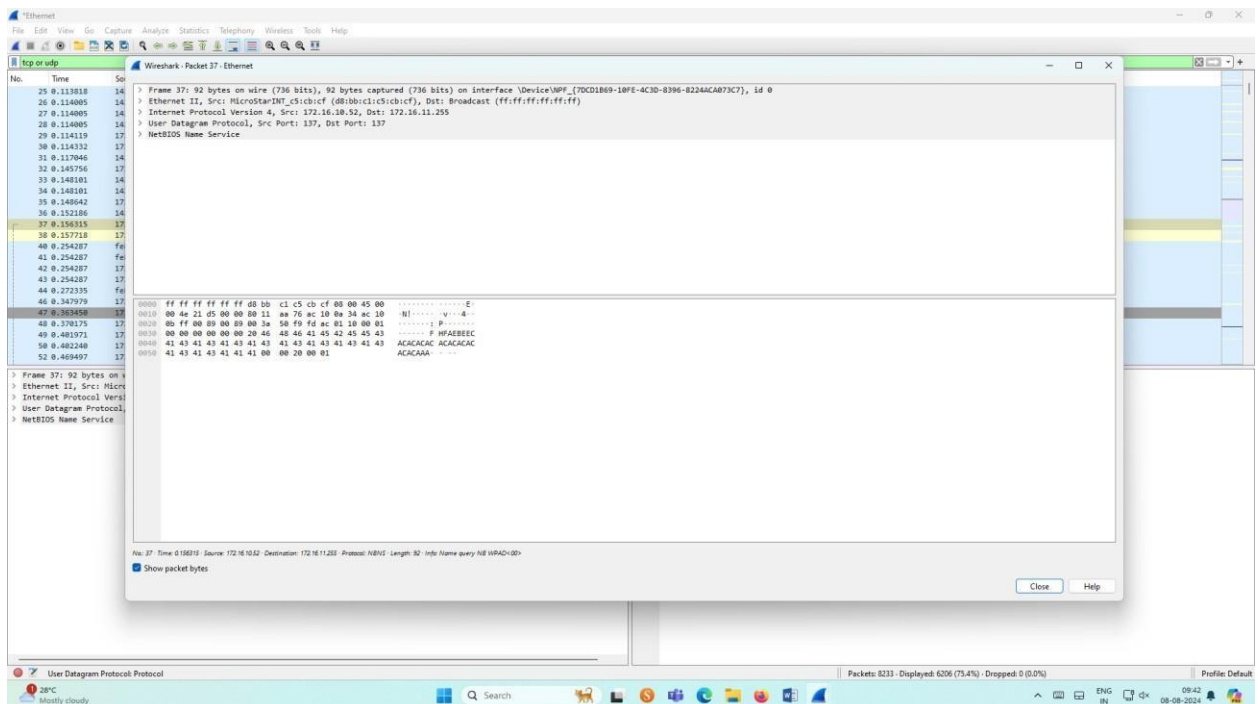


Flow Graph output

CS23532




Inspecting the packets



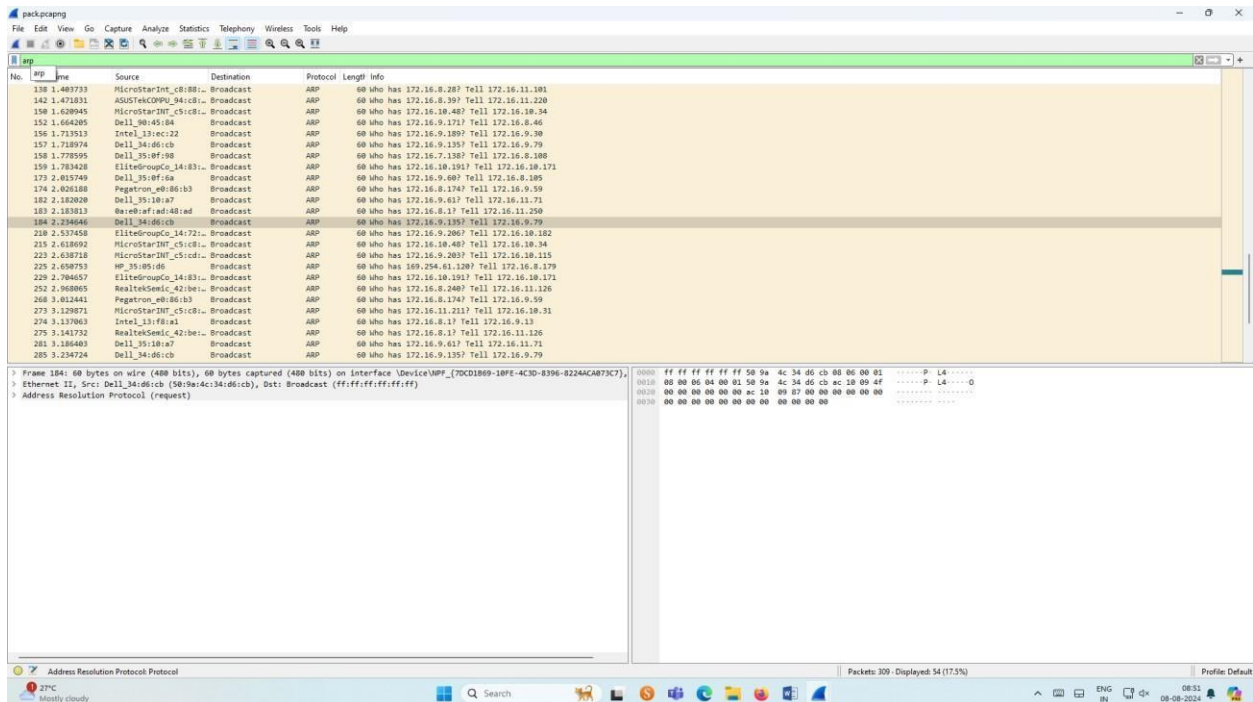
3. Create a Filter to display only ARP packets and inspect the packets.

CS23532

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

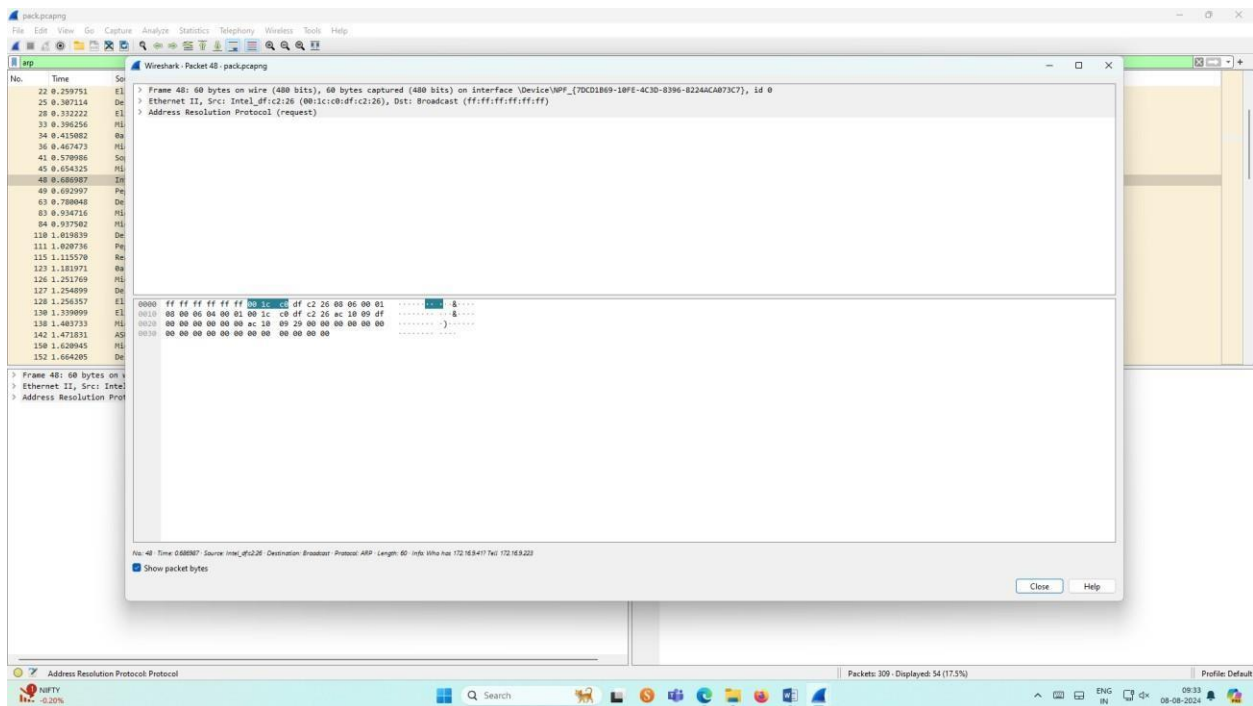


The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The main window is divided into three panes:

- Packet List:** Shows a list of captured packets. The first 100 packets are ARP requests. The columns are No., Time, Source, Destination, Protocol, Length, and Info. The source addresses are various MAC addresses, and the destination is the broadcast address ff:ff:ff:ff:ff:ff.
- Packet Details:** Shows the hierarchical structure of the selected packet (No. 100). It includes Ethernet II, Internet Protocol Version 4, and Address Resolution Protocol (request).
- Packet Bytes:** Shows the raw hex and ASCII data of the selected packet. The hex data is displayed in a table format.



The bottom status bar indicates the current capture status: Address Resolution Protocol Protocol, Packets: 300 - Displayed: 54 (17.5%).

Inspecting the packets



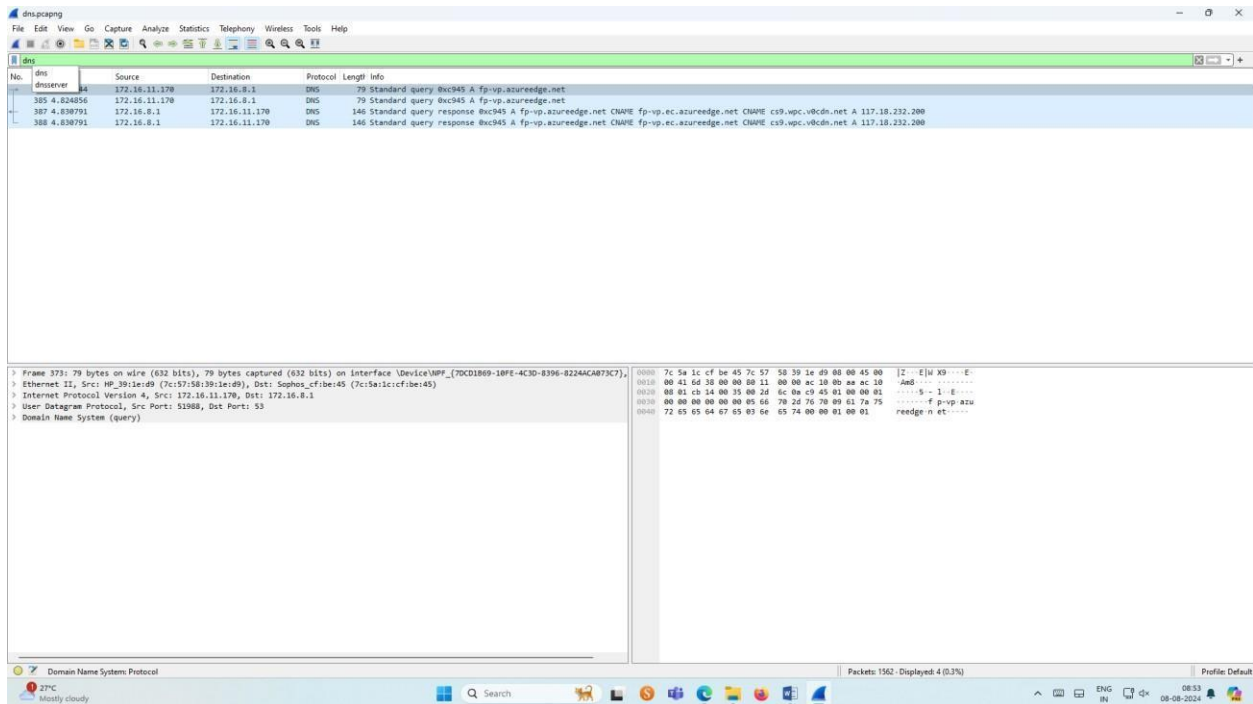
4. Create a Filter to display only DNS packets and provide the flow graph.

Procedure

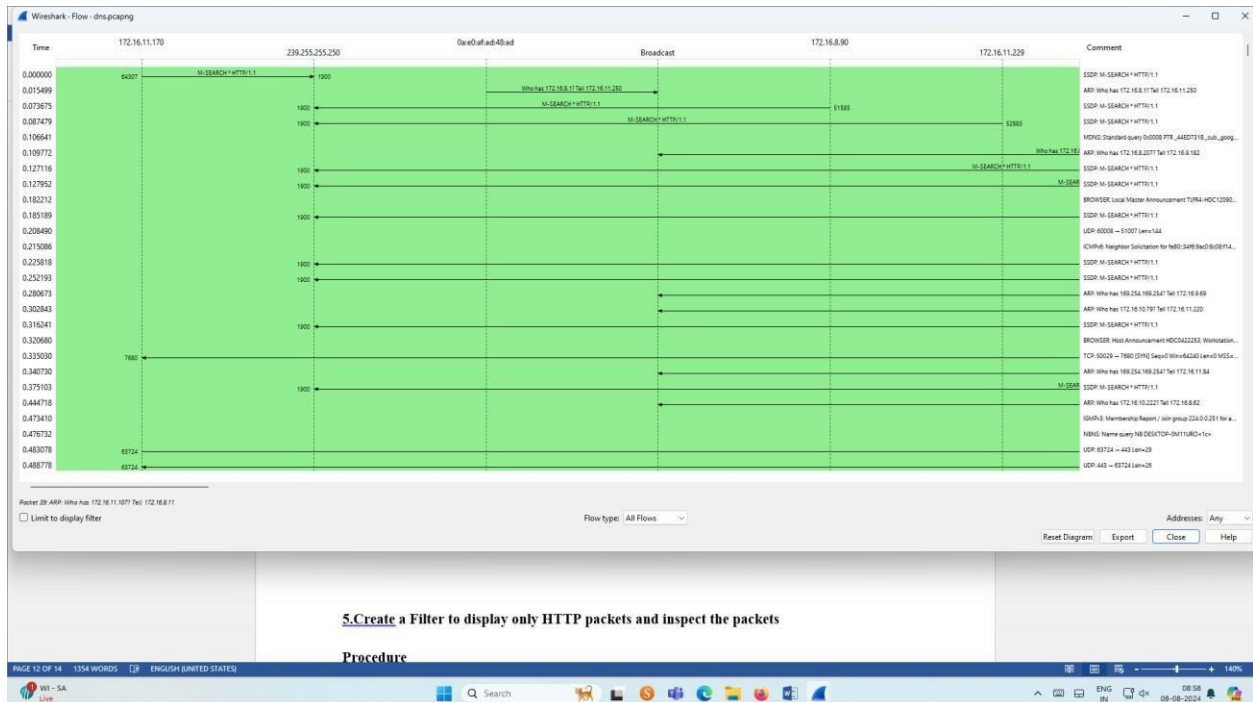
- Select Local Area Connection in Wireshark.
- Go to capture  option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search DNS packets in search bar.
- To see flow graph click Statistics  Flow graph.
- Save the packets.

Output

CS23532




Graph output

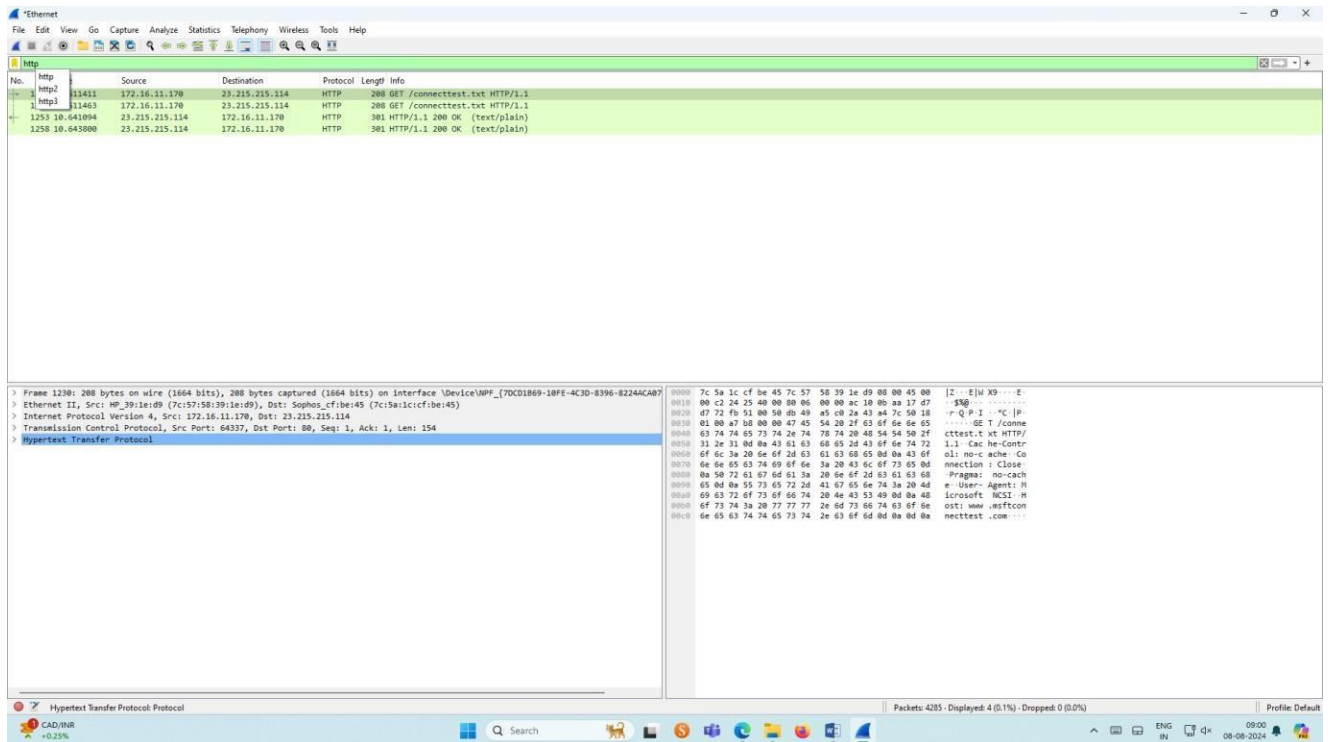


5. Create a Filter to display only HTTP packets and inspect the packets

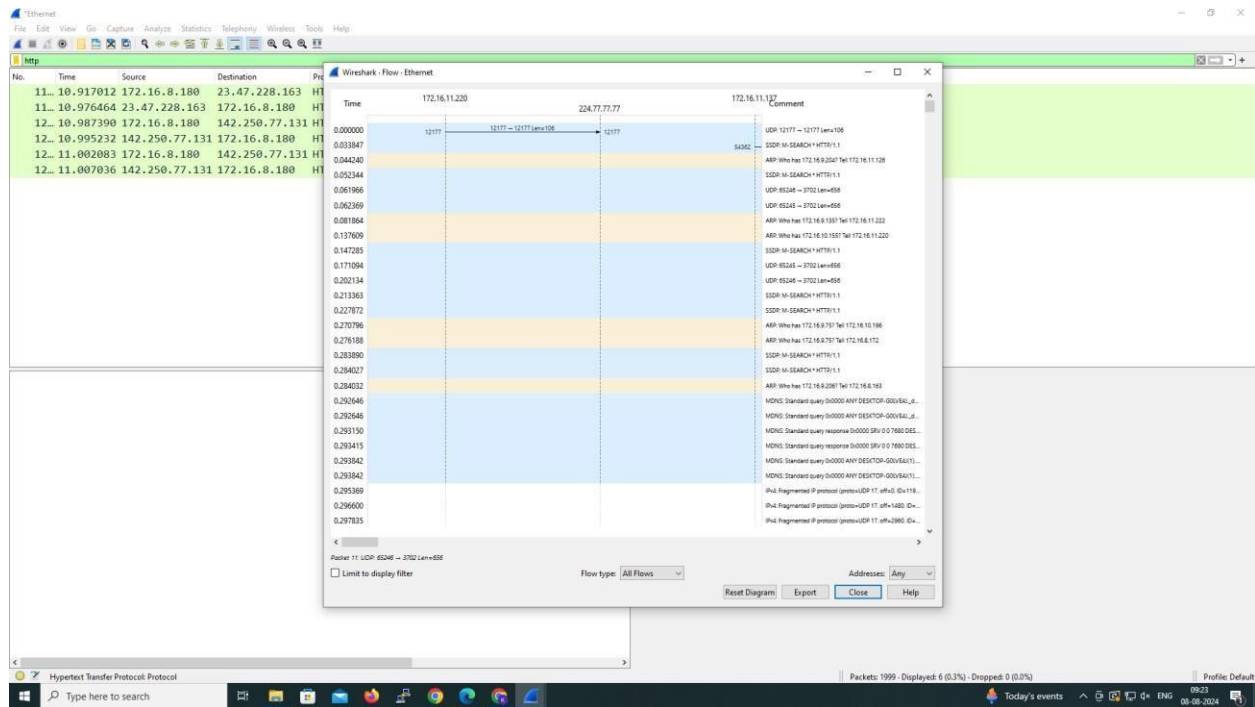
Procedure

- 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.

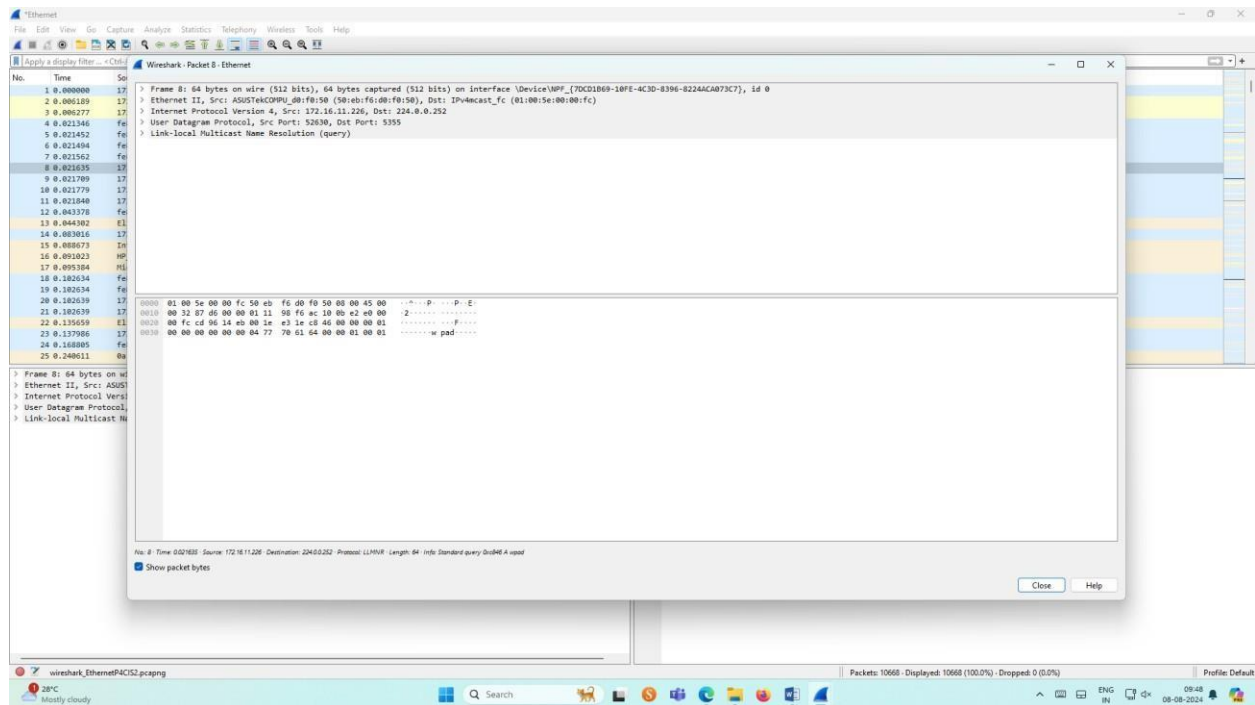
Output



Flow Graph output




Inspecting the packets

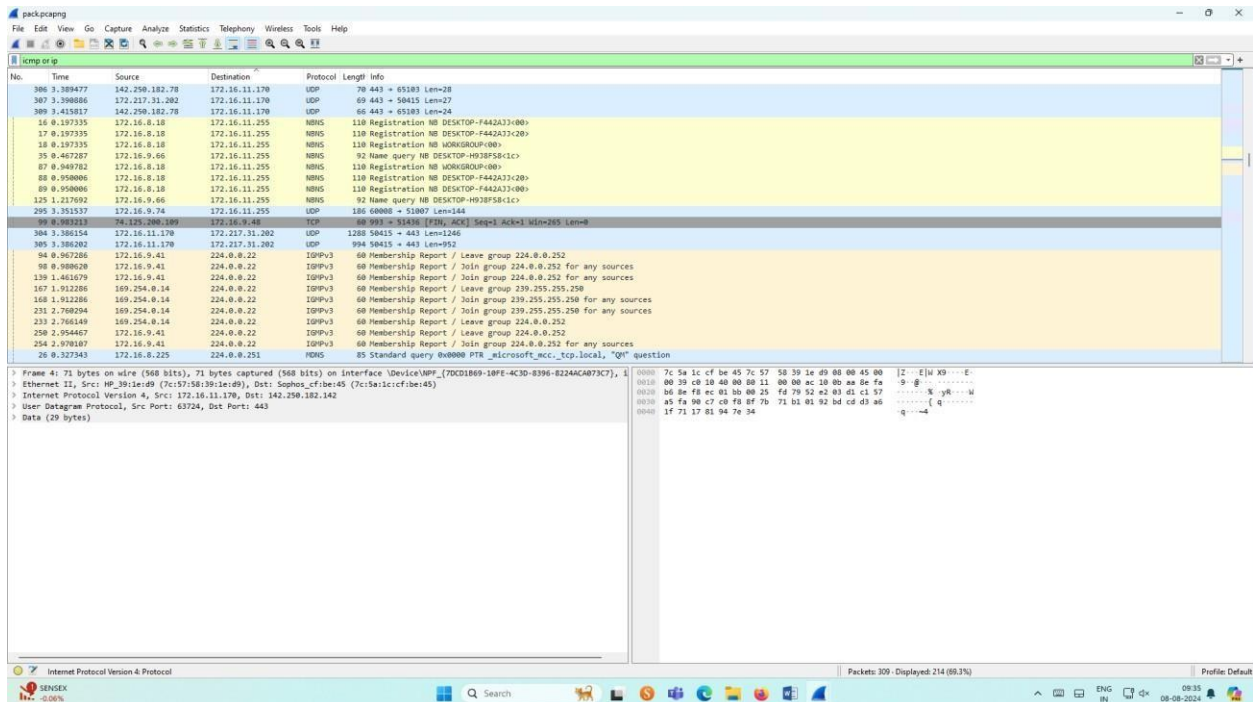


6. Create a Filter to display only IP/ICMP packets and inspect the packets.

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



The screenshot shows the Wireshark interface with a packet capture of ICMP and IP traffic. The packet list pane displays the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
306	1.388477	142.250.182.78	172.16.11.170	UDP	70	443 → 65183 Len=28
307	3.398086	172.217.31.202	172.16.11.170	UDP	69	443 → 50415 Len=27
309	3.415817	142.250.182.78	172.16.11.170	UDP	66	443 → 65183 Len=24
16	0.197335	172.16.8.18	172.16.11.255	NBNS	110	Registration NB DESKTOP-F442A31C2B>
17	0.197335	172.16.8.18	172.16.11.255	NBNS	110	Registration NB DESKTOP-F442A31C2B>
18	0.197335	172.16.8.18	172.16.11.255	NBNS	110	Registration NB WORKGROUP>
35	0.407207	172.16.9.66	172.16.11.255	NBNS	92	Name query NB DESKTOP-H03P581C1>
87	0.940782	172.16.8.18	172.16.11.255	NBNS	110	Registration NB WORKGROUP>
88	0.950006	172.16.8.18	172.16.11.255	NBNS	110	Registration NB DESKTOP-F442A31C2B>
89	0.950006	172.16.8.18	172.16.11.255	NBNS	110	Registration NB DESKTOP-F442A31C2B>
129	1.217692	172.16.9.66	172.16.11.255	NBNS	92	Name query NB DESKTOP-H03P581C1>
295	3.351537	172.16.9.74	172.16.11.255	UDP	186	60000 → 51007 Len=144
98	0.983213	74.125.240.189	172.16.0.48	TCP	60	9931 → 51436 [FIN, ACK] Seq=1 ACK=1 Win=255 Len=0
304	3.386154	172.16.11.170	172.217.31.202	UDP	1288	50415 → 443 Len=1246
305	3.386282	172.16.11.170	172.217.31.202	UDP	994	50415 → 443 Len=952
94	0.967286	172.16.9.41	224.0.0.22	IGMPv3	60	Membership Report / Leave group 224.0.0.252
96	0.988628	172.16.9.41	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any sources
139	1.461679	172.16.9.41	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any sources
167	1.912286	169.254.0.14	224.0.0.22	IGMPv3	60	Membership Report / Leave group 239.255.255.250
168	1.912286	169.254.0.14	224.0.0.22	IGMPv3	60	Membership Report / Join group 239.255.255.250 for any sources
231	2.769294	169.254.0.14	224.0.0.22	IGMPv3	60	Membership Report / Join group 239.255.255.250 for any sources
233	2.766149	169.254.0.14	224.0.0.22	IGMPv3	60	Membership Report / Leave group 224.0.0.252
258	2.954467	172.16.9.41	224.0.0.22	IGMPv3	60	Membership Report / Leave group 224.0.0.252
259	2.978187	172.16.9.41	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any sources
26	0.327543	172.16.8.225	224.0.0.251	NBNS	85	Standard query 0x0000 PTR _microsoft_mcc_tcp.local, "QM" question

The packet details pane for the selected packet (Frame 4) shows the following structure:

- Frame 4: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{70C01B69-10FE-4C3D-8396-E224ACAB73C7}, 1
- Ethernet II, Src: HP_39:1e:d9 (7c:57:58:39:1e:d9), Dst: Sophos_fibe:45 (7c:5a:1c:cf:be:45)
- Internet Protocol Version 4, Src: 172.16.11.170, Dst: 142.250.182.142
- User Datagram Protocol, Src Port: 63724, Dst Port: 443
- Data (29 bytes)

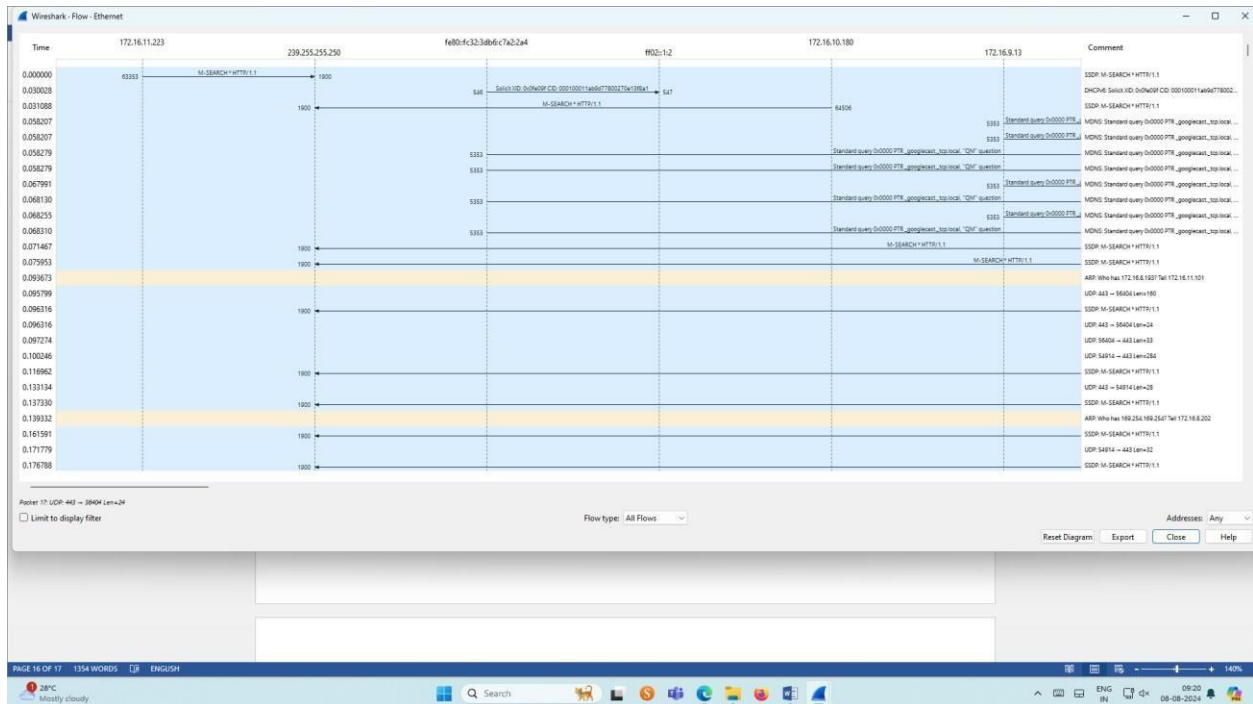
The packet bytes pane shows the raw data in hexadecimal and ASCII:

```

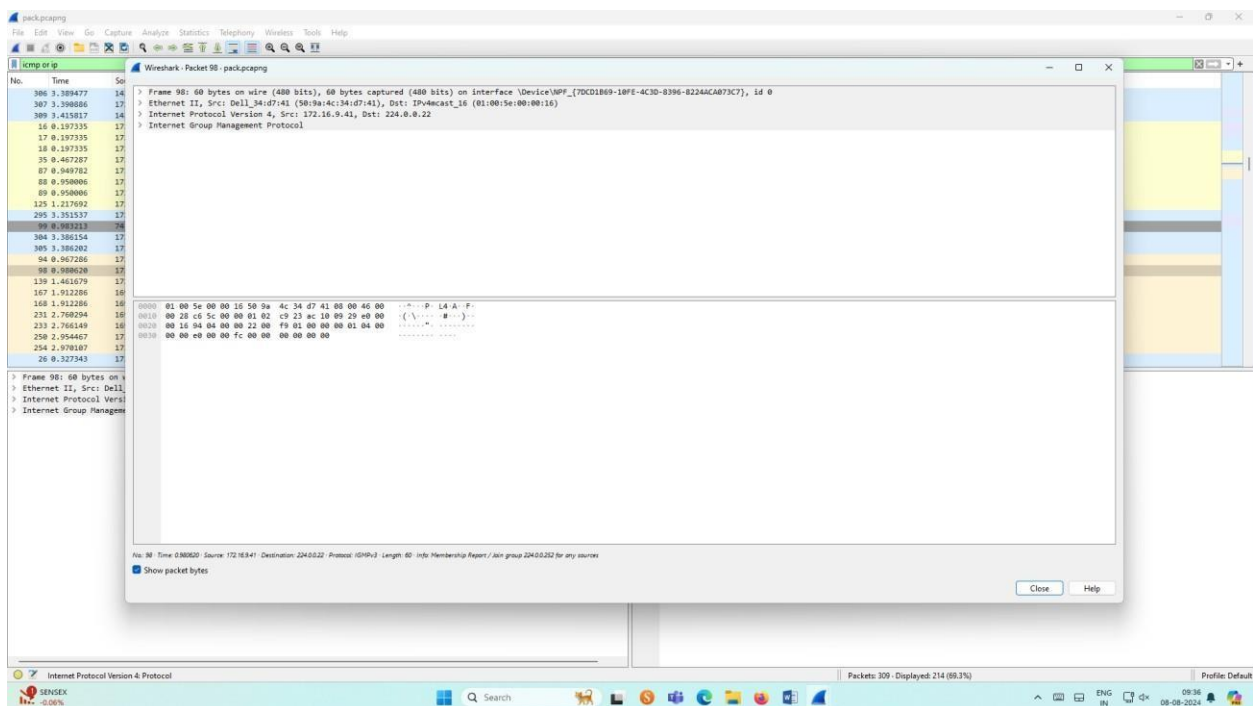
0000  7c 5a 1c cf be 45 7c 57 58 39 1e d9 00 00 45 00 |2...E|u X9....E:
0010  00 39 c8 10 40 00 08 11 00 00 ac 10 00 aa be fa |9.8.....Xp....
0020  80 be f8 ec 01 3b 00 25 fd 79 52 e2 01 d1 c1 97 |.....q.....
0030  a5 fa 90 c7 c0 f8 bf 7b 71 b1 01 92 bd cd d3 a6 |.....q.....
0040  1f 71 17 81 94 7e 34 |q.....4
  
```

Flow Graph output

CS23532




Inspecting the packets



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

CS23532

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

[illegible]

Inspecting the packets

CS23532

