CS23532

EXP NO : 4B **SOMILA.SA**
DATE: 19/08/24 **231901052**

PACKET SNIFFING USING WIRESHARK

AIM:

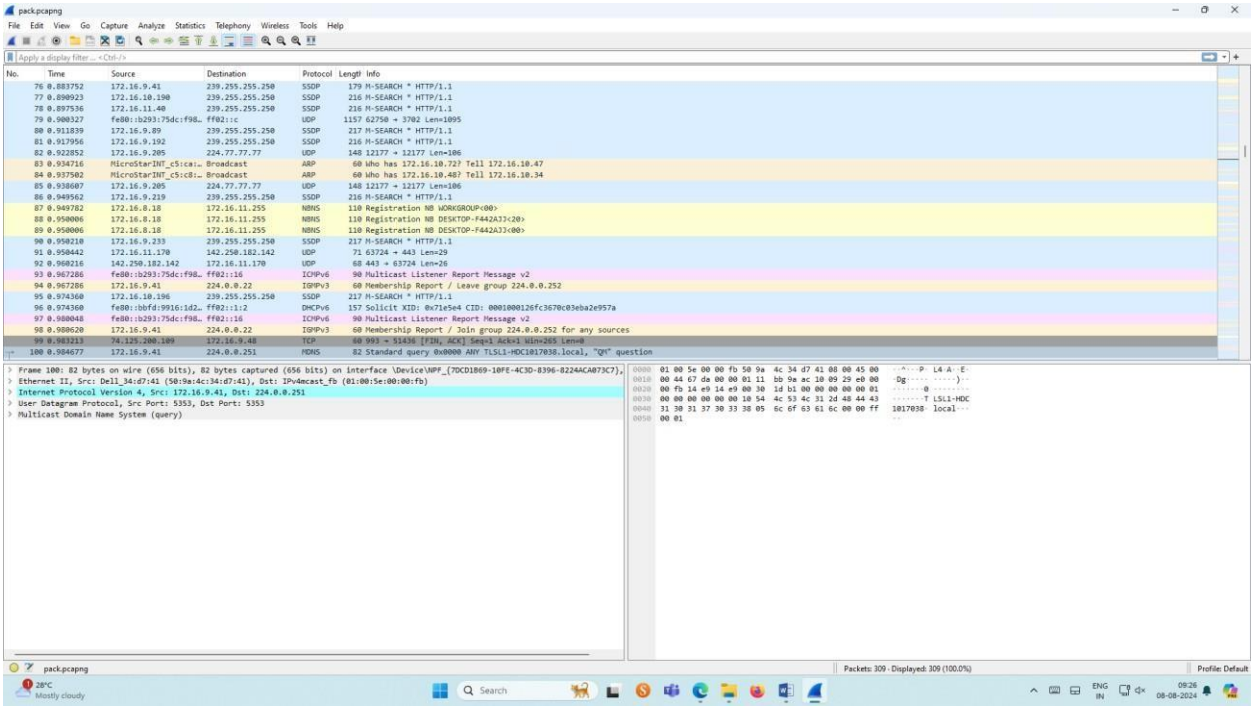
Exercises

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



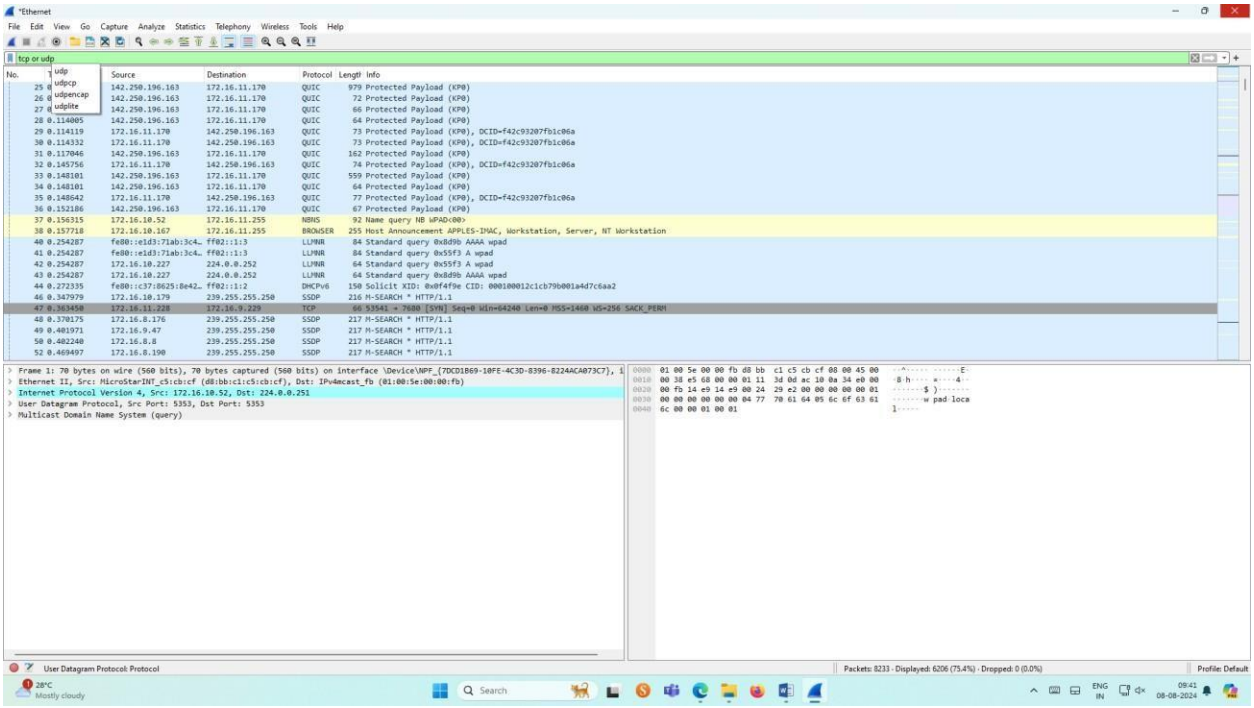
2. Create a Filter to display only TCP/UDP packets, inspect the packets and provide the flow graph.

CS23532

Procedure

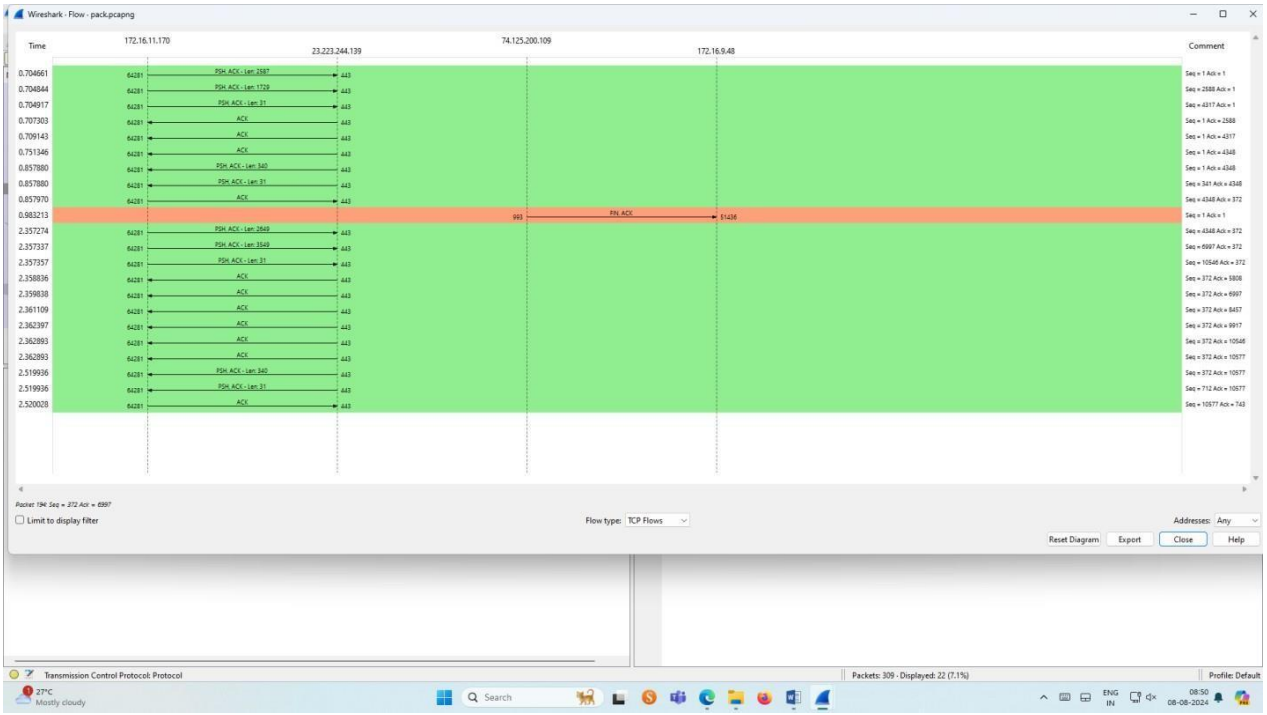
- Select Local Area Connection in Wireshark.
- Go to capture ✇option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search TCP packets in search bar.
- To see flow graph click Statistics✇Flow graph.
- Save the packets.

Output:

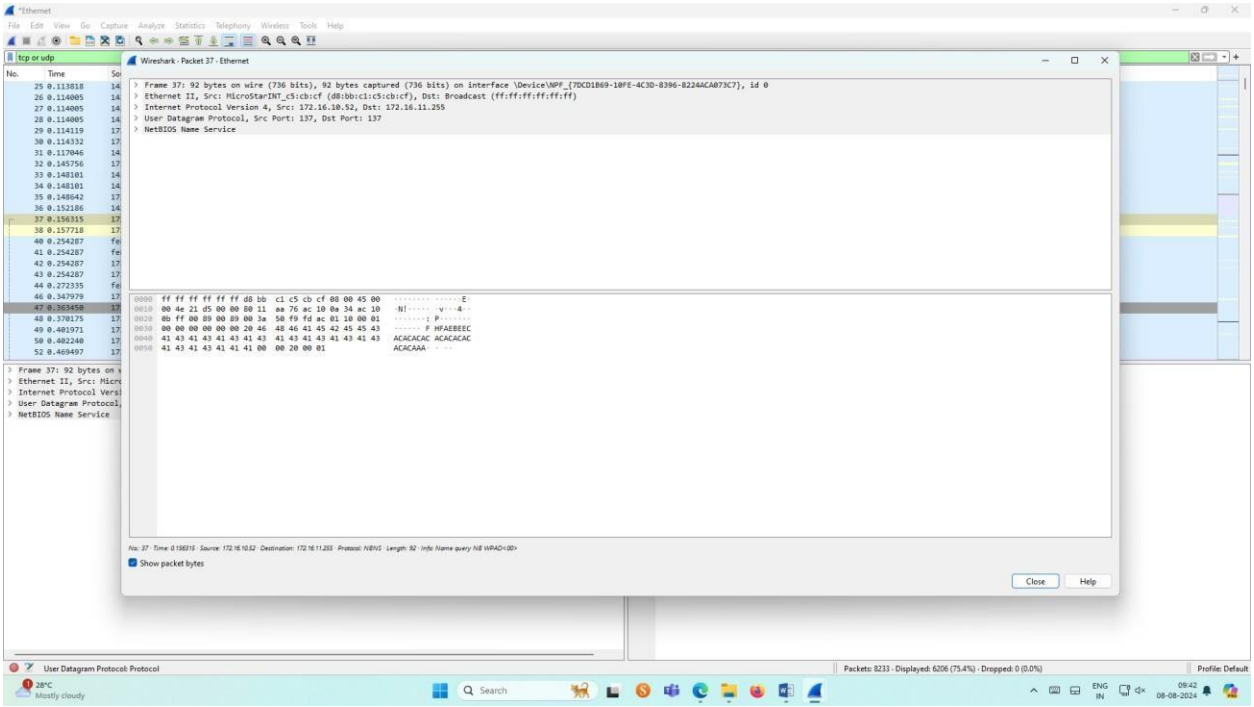


Flow Graph output

CS23532



Inspecting the packets



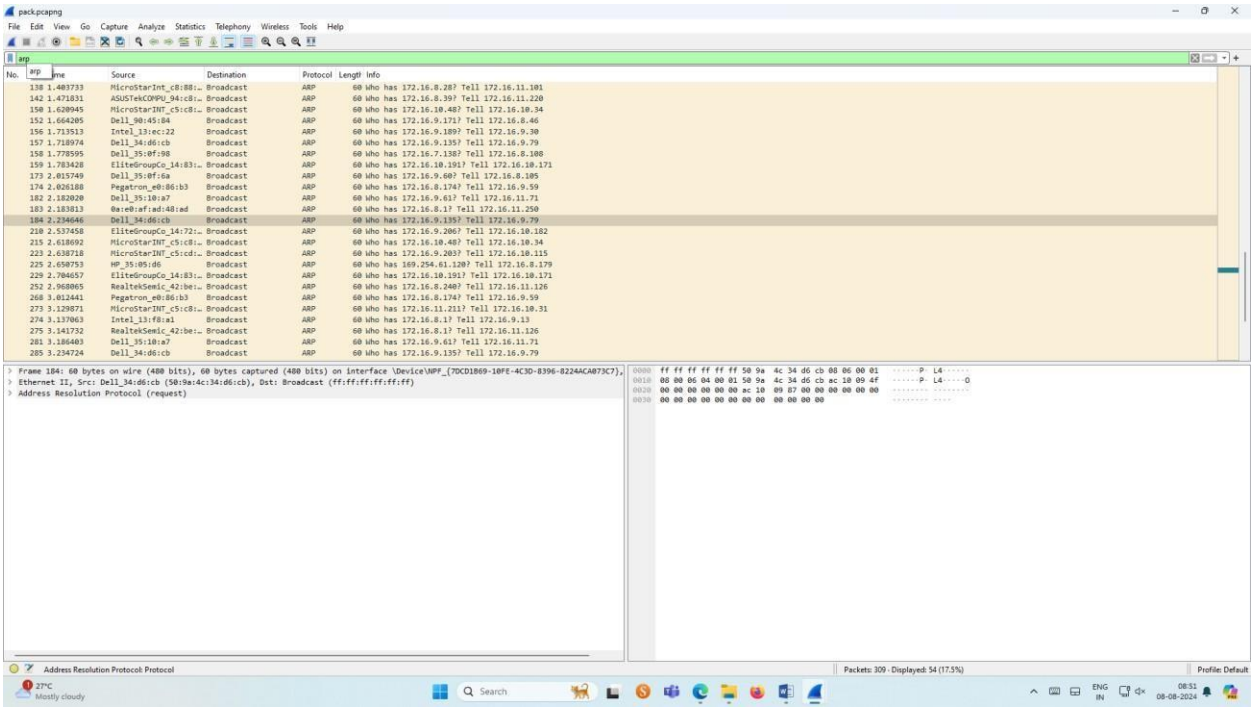
3. Create a Filter to display only ARP packets and inspect the packets.

CS23532

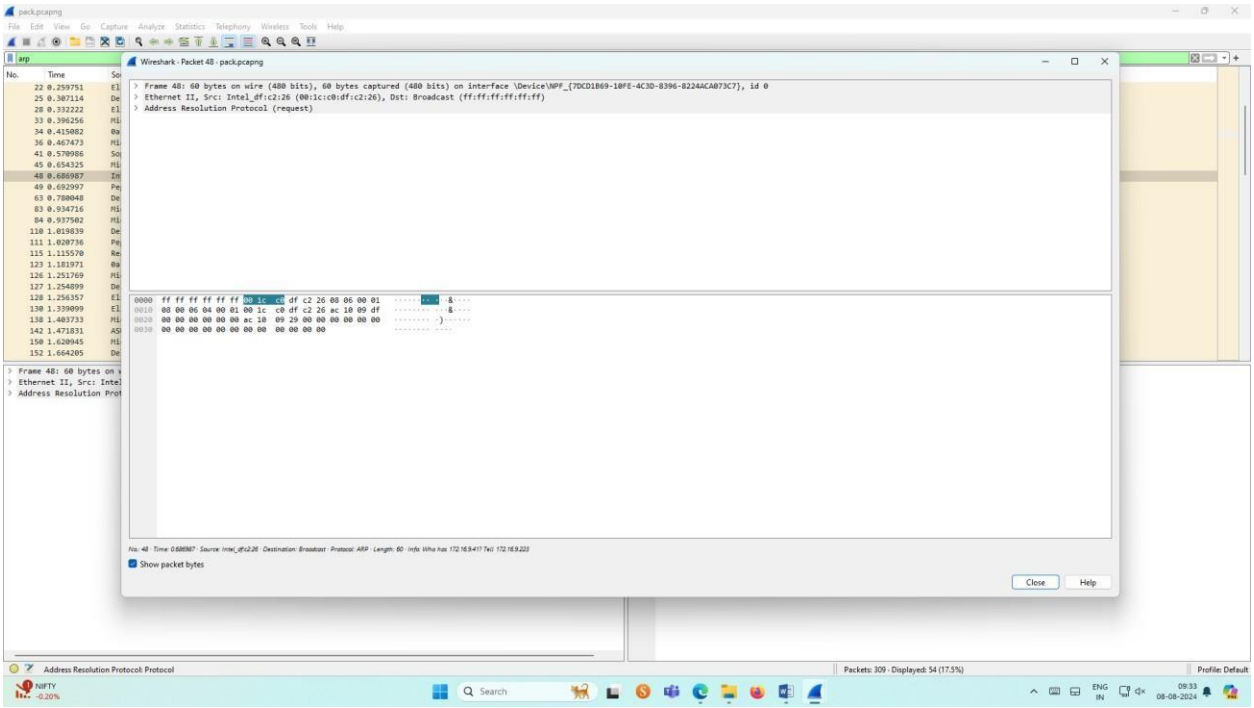
Procedure

- 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



Inspecting the packets



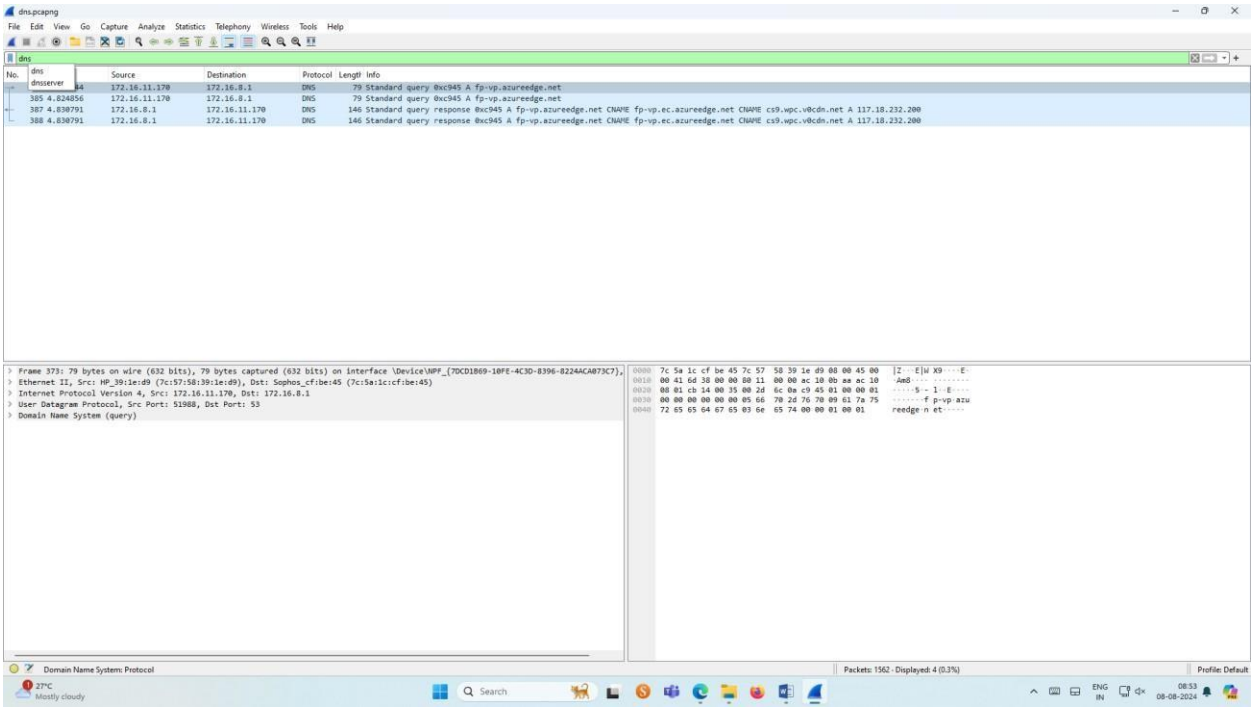
4. Create a Filter to display only DNS packets and provide the flow graph.

Procedure

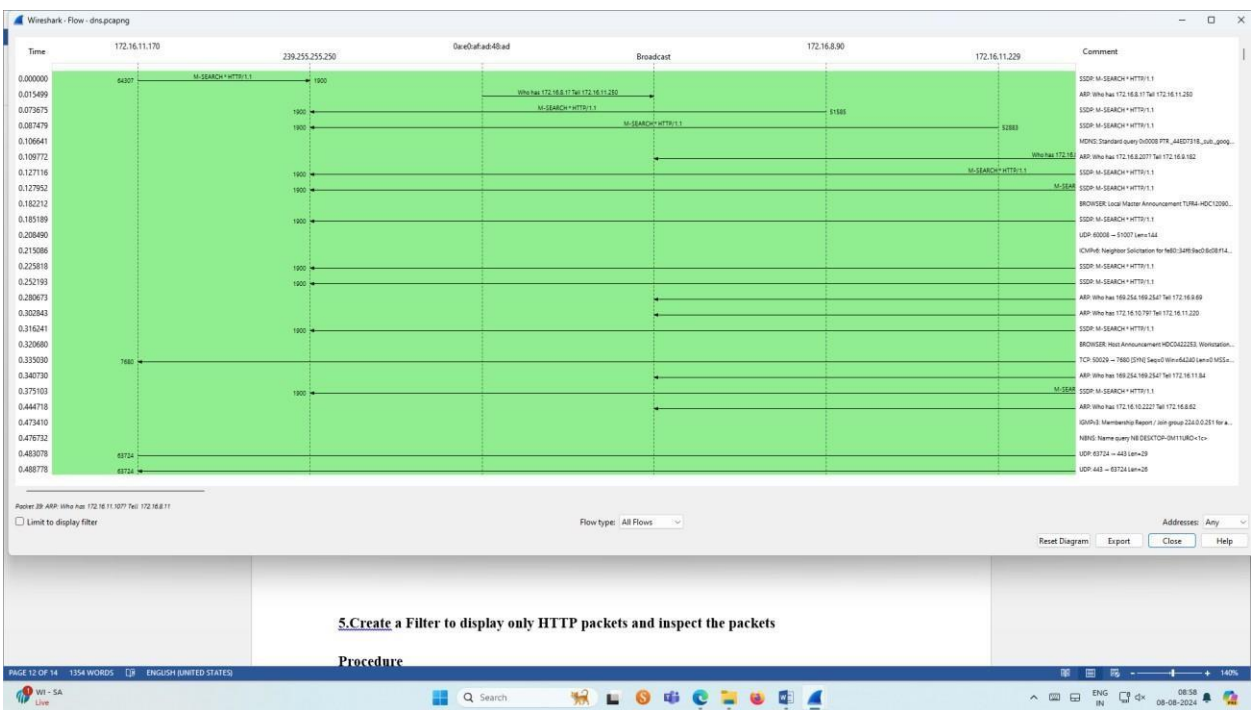
- Select Local Area Connection in Wireshark.
- Go to capture ⚙option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search DNS packets in search bar.
- To see flow graph click Statistics⚙Flow graph.
- Save the packets.

Output

CS23532



Graph output



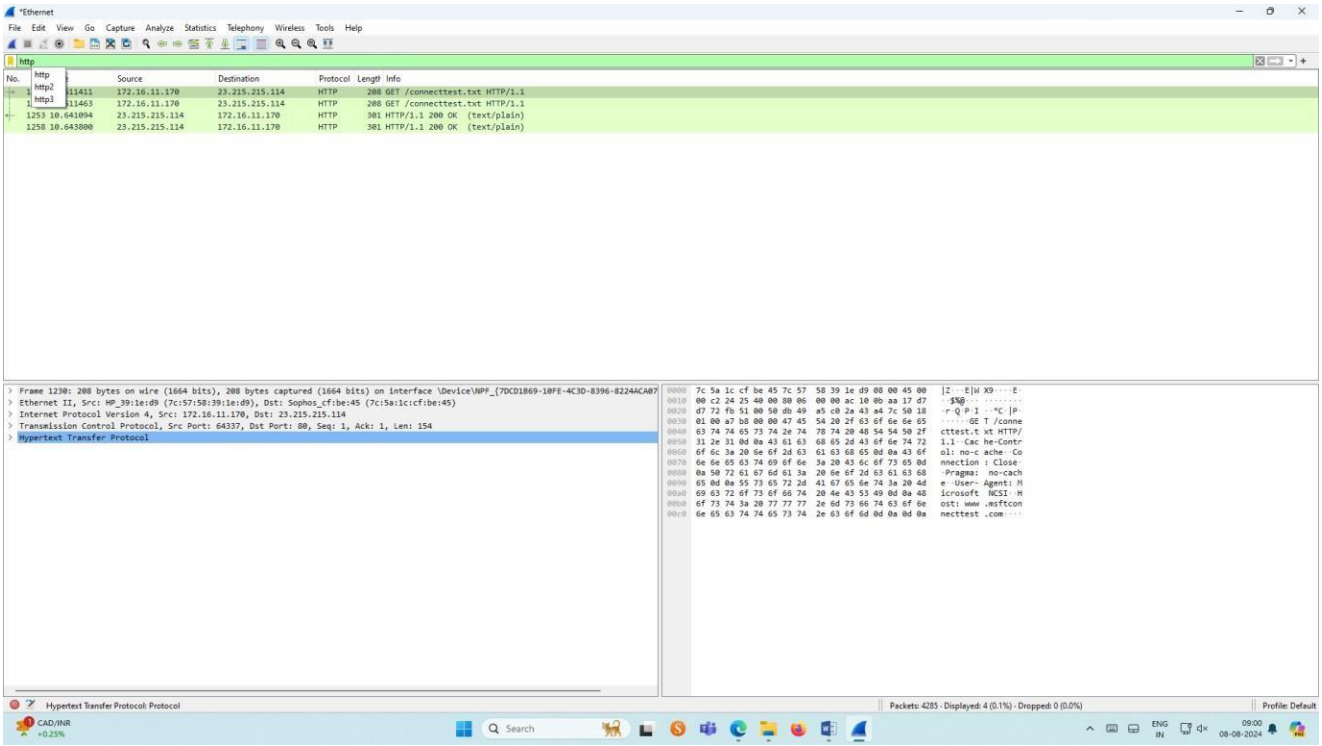
5. Create a Filter to display only HTTP packets and inspect the packets

CS23532

Procedure

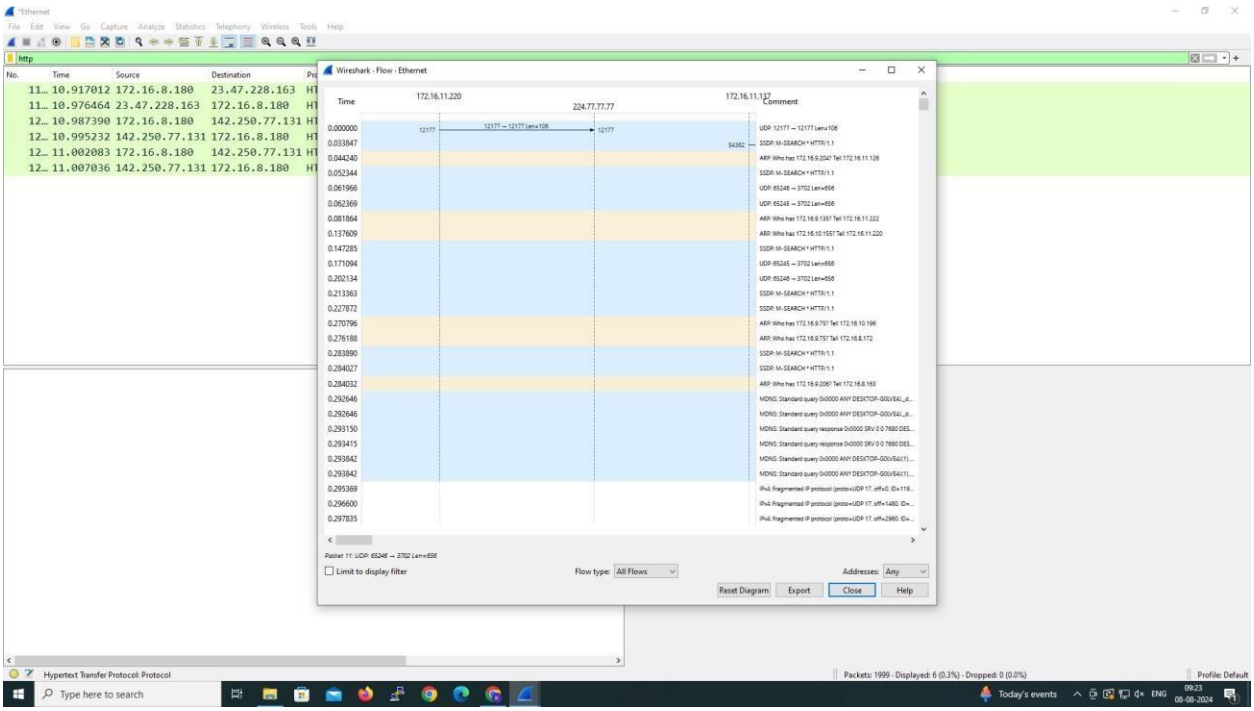
- Select Local Area Connection in Wireshark.
- Go to capture option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search HTTP packets in the search bar.
- Save the packets.

Output

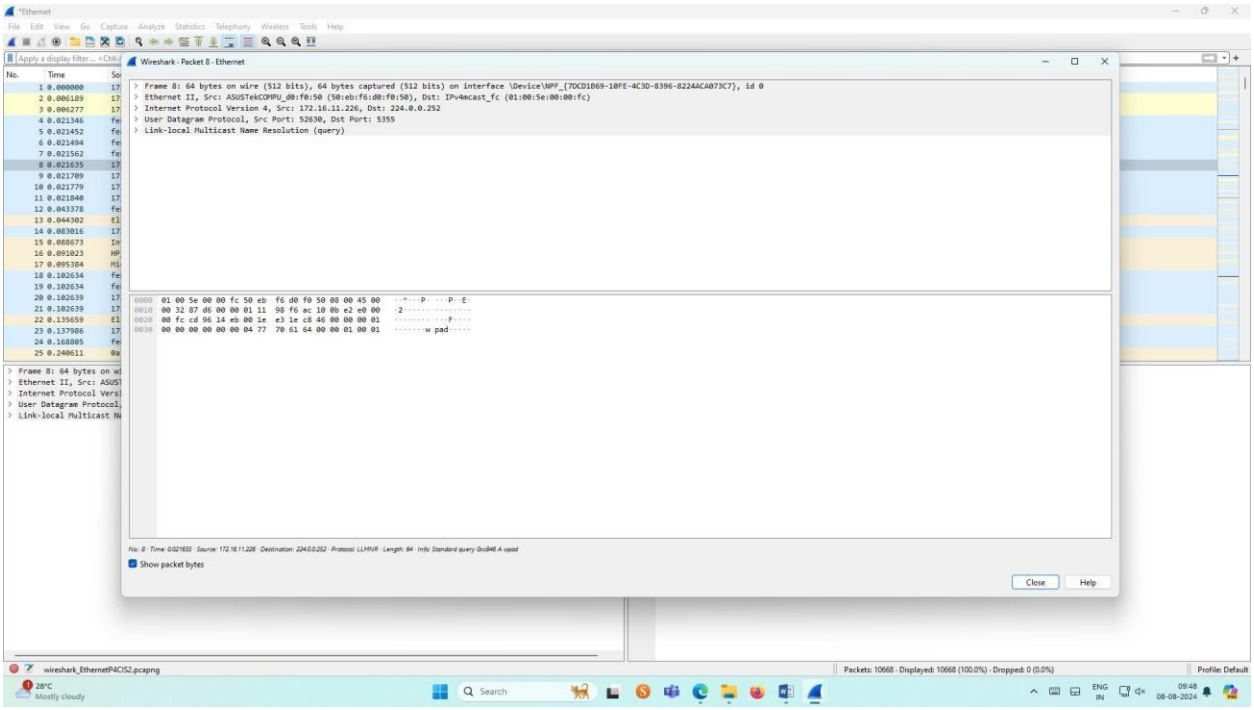


Flow Graph output

CS23532



Inspecting the packets



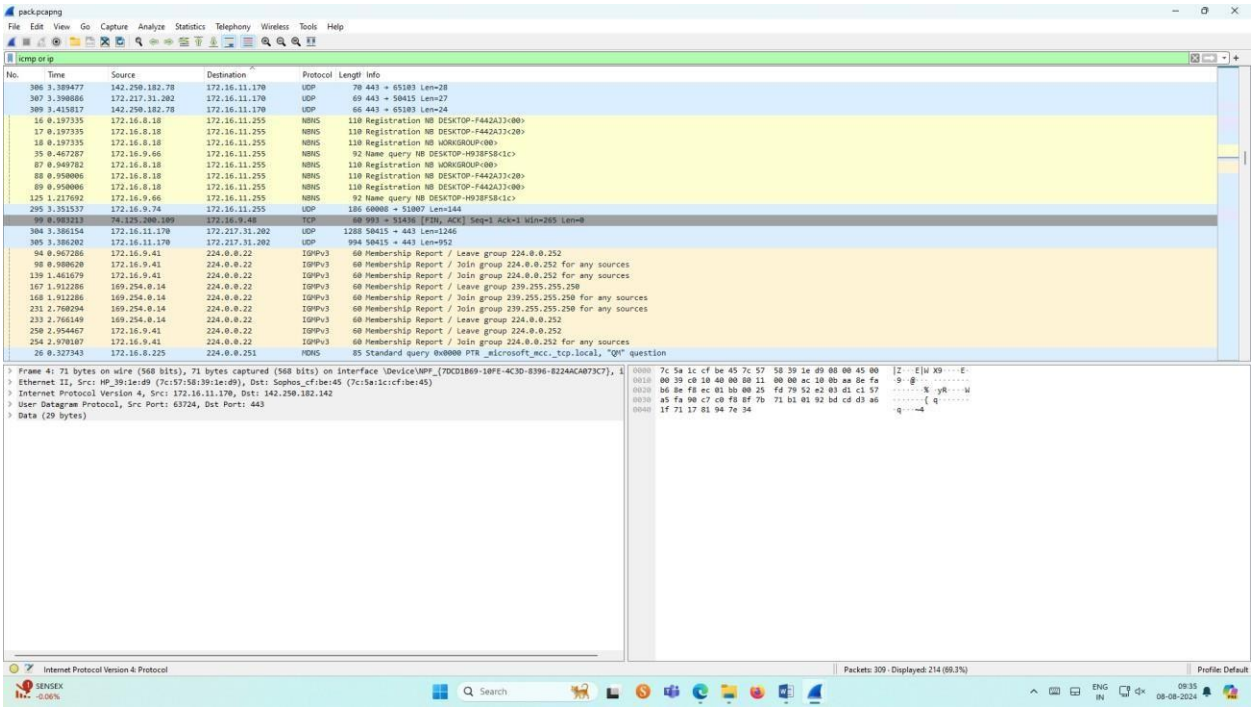
6. Create a Filter to display only IP/ICMP packets and inspect the packets.

CS23532

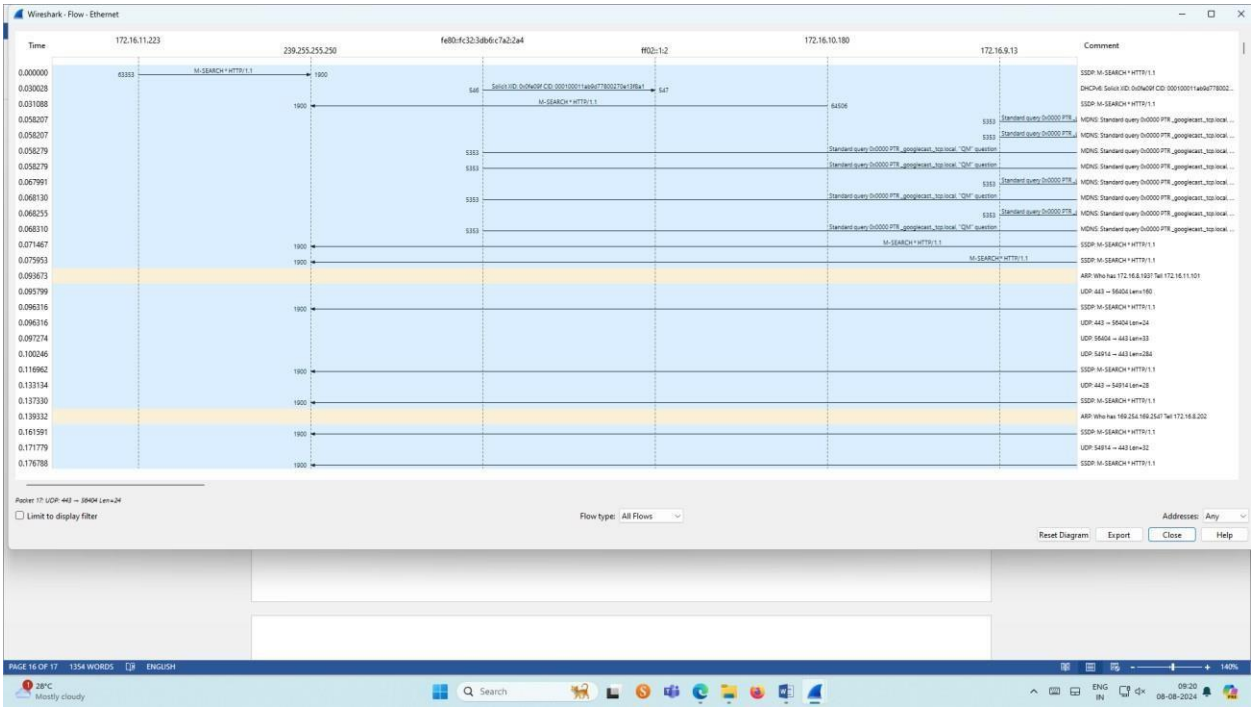
Procedure

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

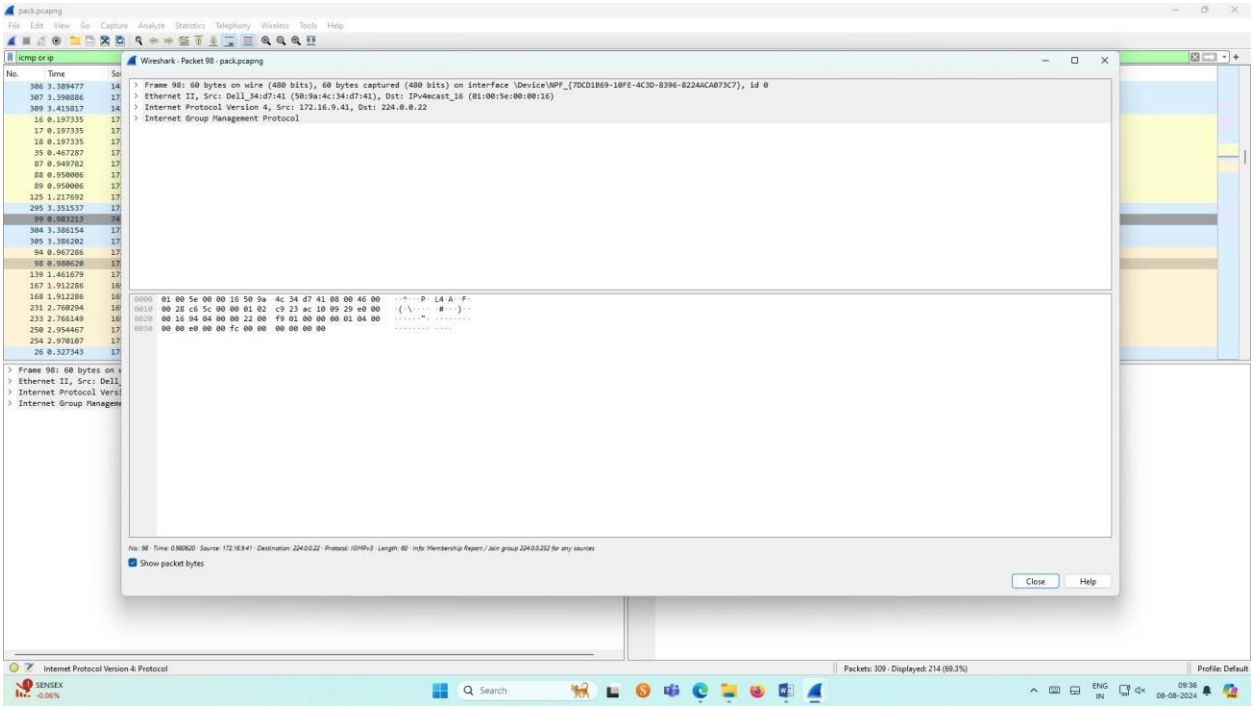
Output



Flow Graph output



Inspecting the packets



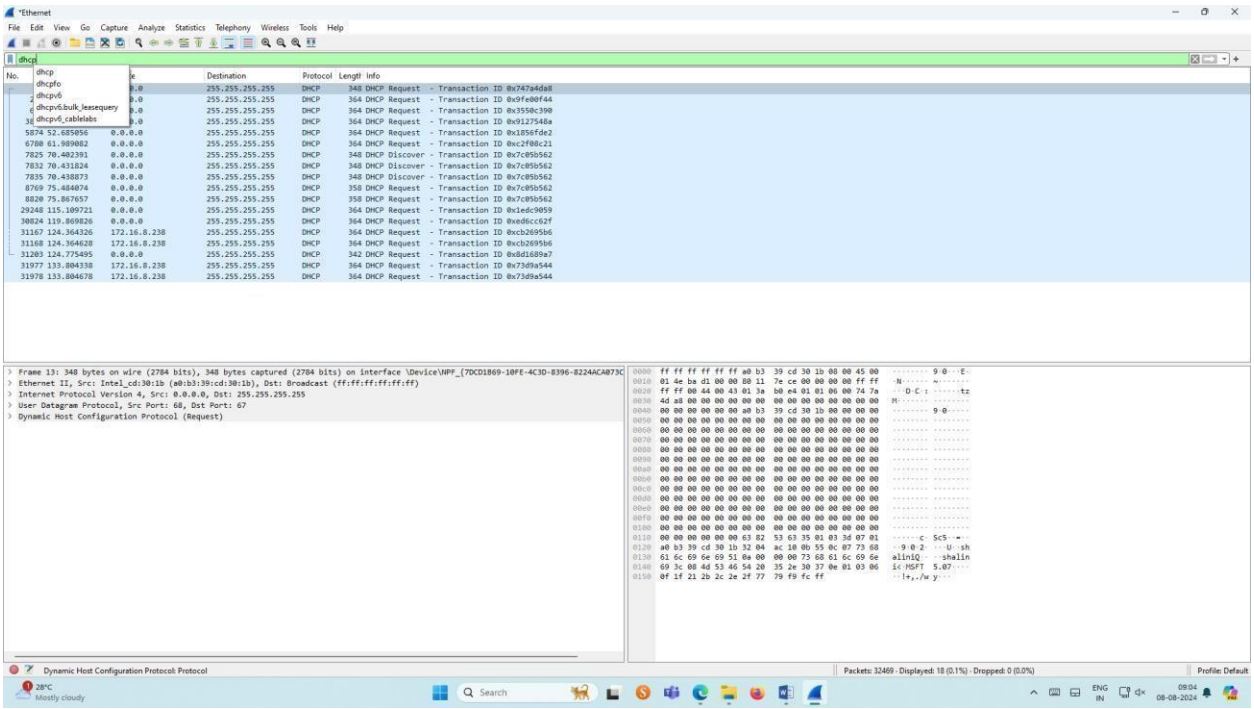
7. Create a Filter to display only DHCP packets and inspect the packets.

CS23532

Procedure

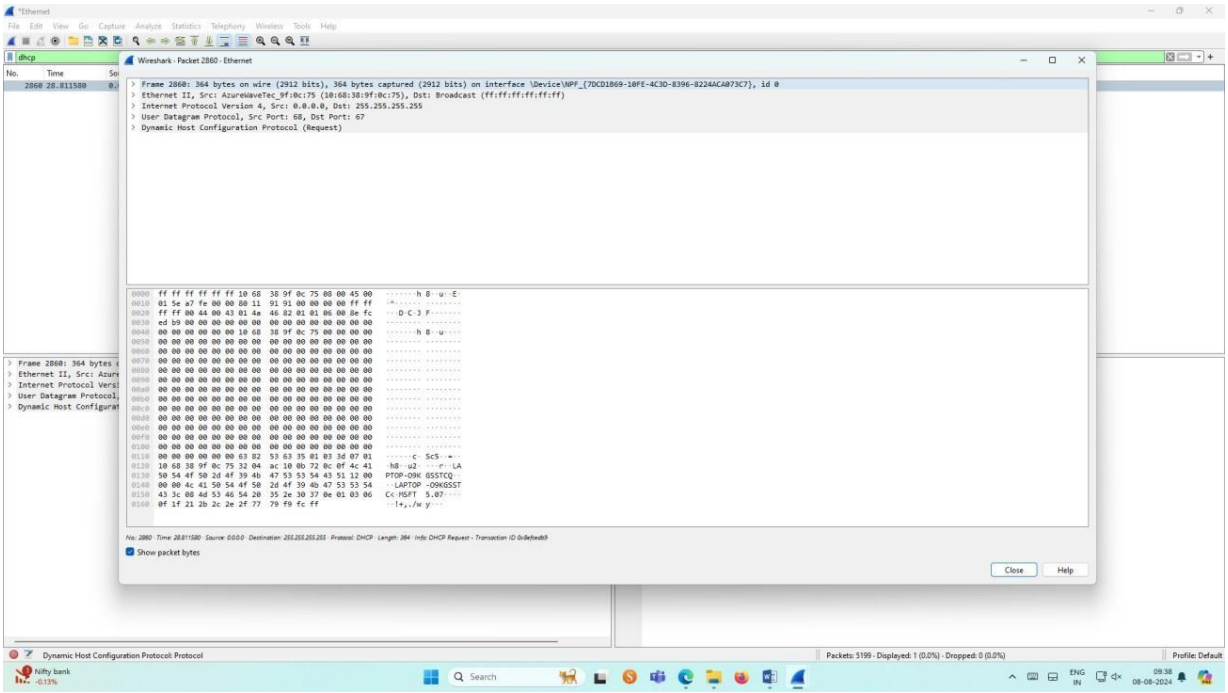
- Select Local Area Connection in Wireshark.
- Go to capture option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search DHCP packets in search bar.
- Save the packets

Output



Inspecting the packets

CS23532


Wireshark · Packet 2860 · Ethernet
Frame 2860: 364 bytes on wire (2912 bits), 364 bytes captured (2912 bits) on interface \Device\NPF_{7DCD1869-10FE-4C3D-8396-8224ACA073C7}, id 0
Ethernet II, Src: AzureWaveTec_9f:0c:75 (10:68:38:9f:0c:75), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Request)
Show packet bytes
Close
Help