EX NO:4b **Analyze Network traffic using Wireshark tool**
DATE:07.08.24

AIM:

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

Exercises

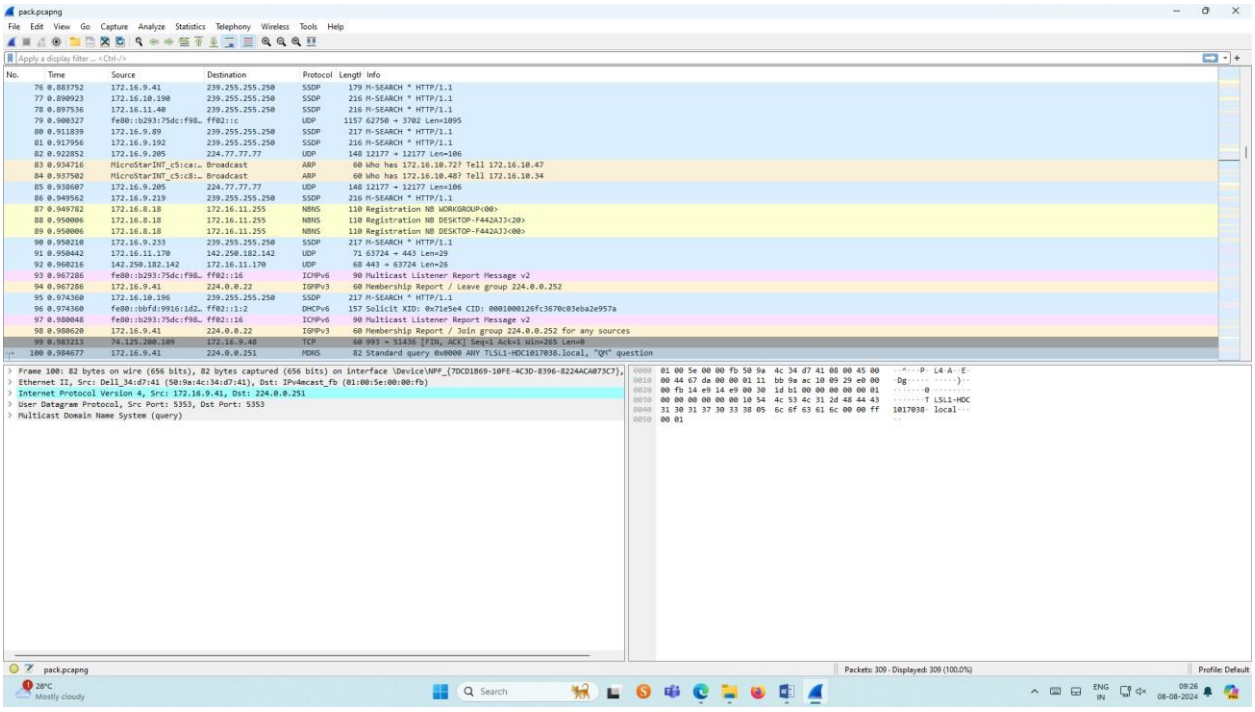
1. Capture 100 packets from the Ethernet: IEEE 802.3 LAN Interface and save it.

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

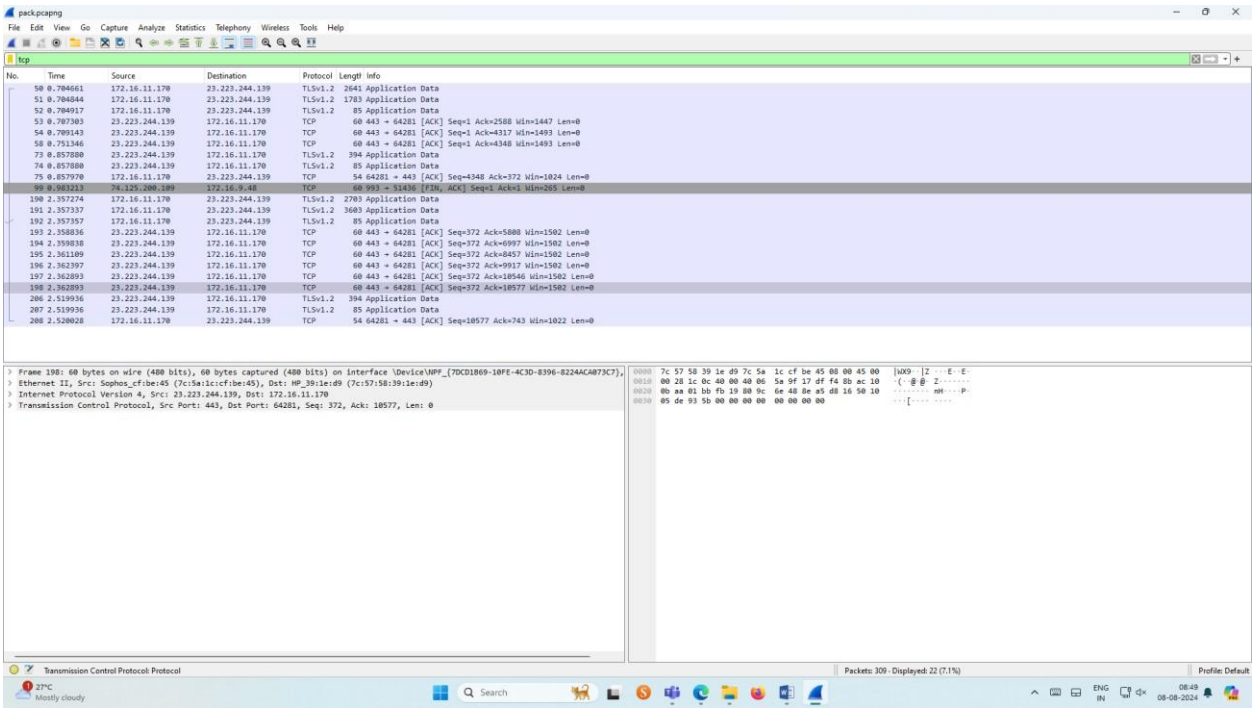


2.Create a Filter to display only TCP/UDP packets, inspect the packets and provide the flow graph.

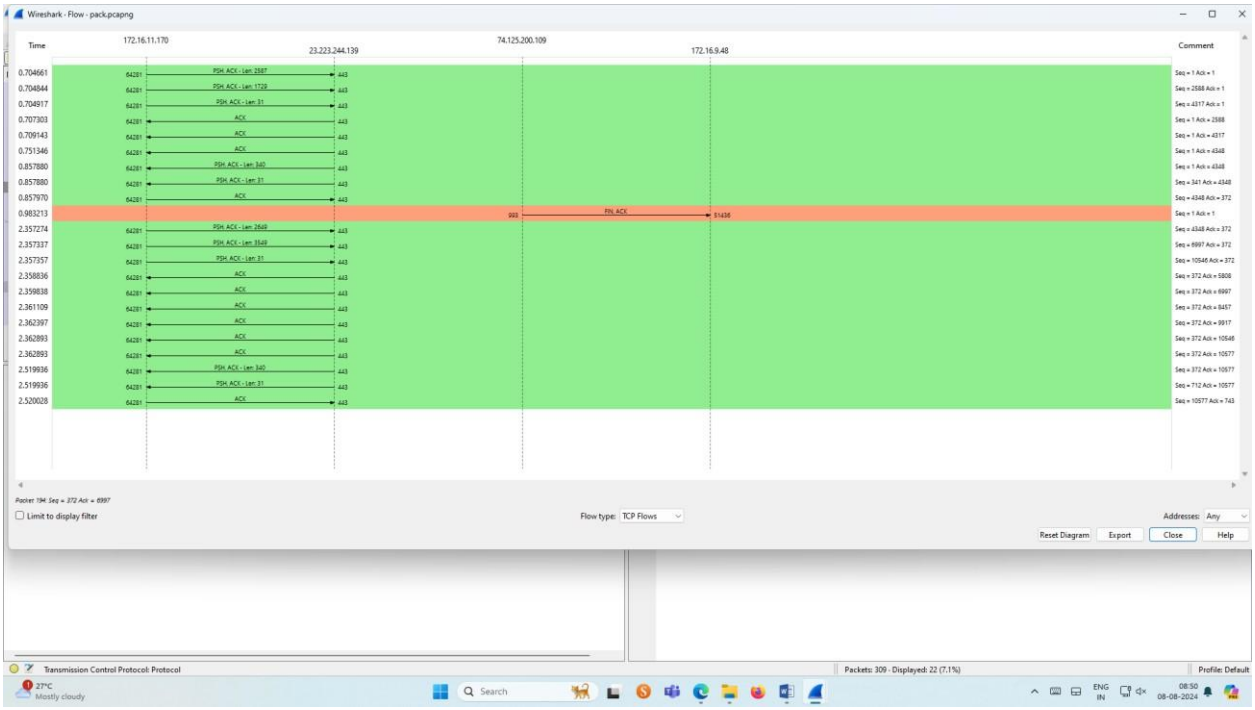
Procedure

- 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:



Flow Graph output

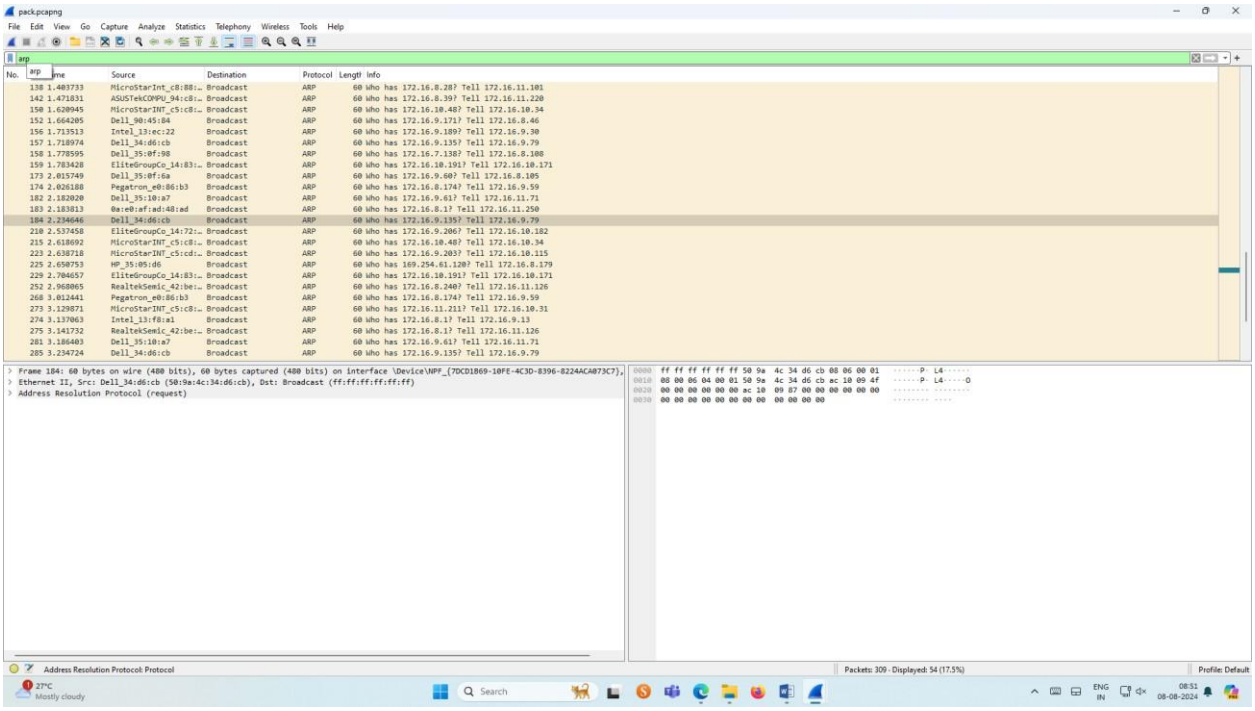


3.Create a Filter to display only ARP packets and inspect the packets.

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



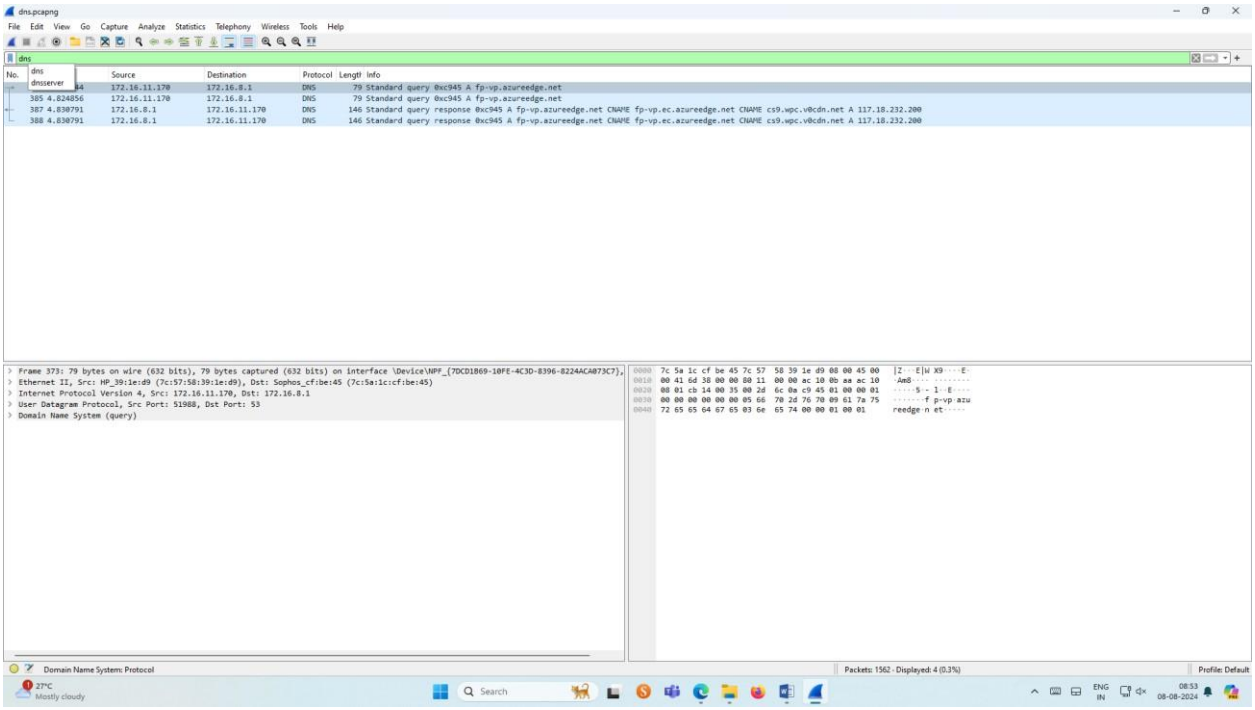
4.Create a Filter to display only DNS packets and provide the flow graph.

Procedure

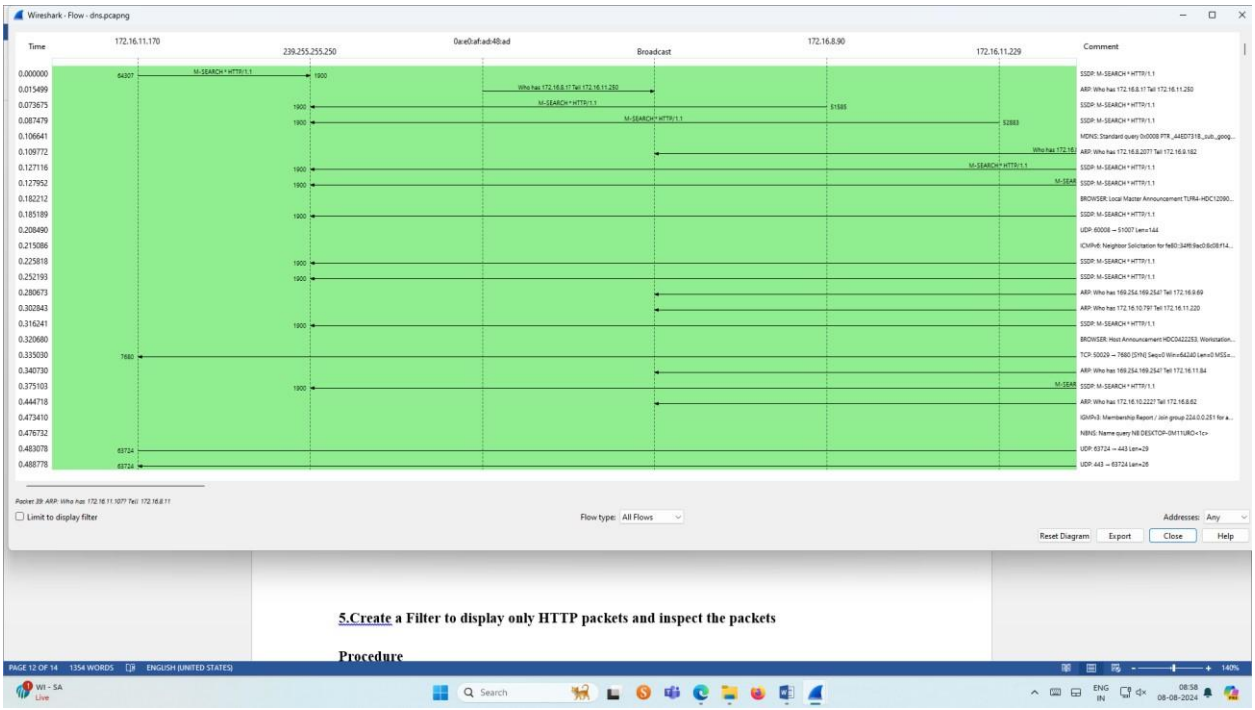
- Select Local Area Connection in Wireshark.
- Go to capture option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search DNS packets in search bar.

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

Output



Graph output



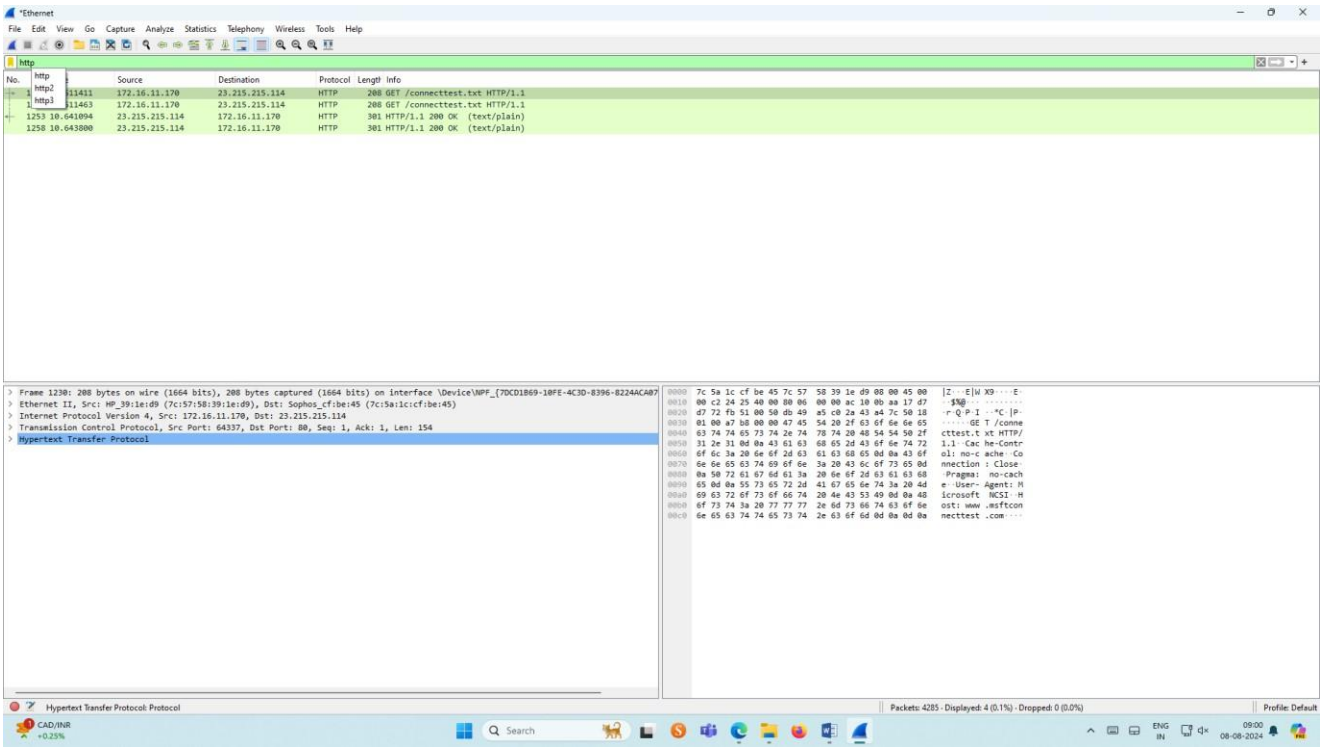
5.Create a Filter to display only HTTP packets and inspect the packets

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.

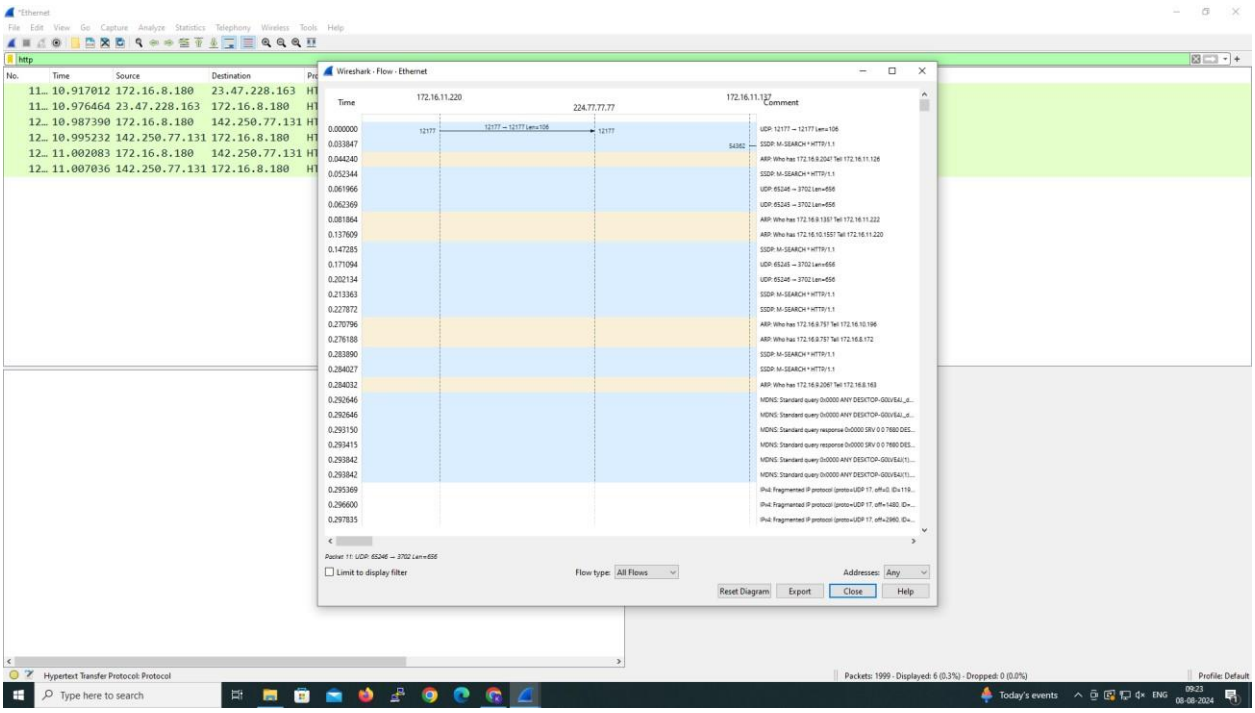
Output

NAME:PRIYANKA.E ROLL NO:231901038



CSE(CYBER SECURITY)

Flow Graph output

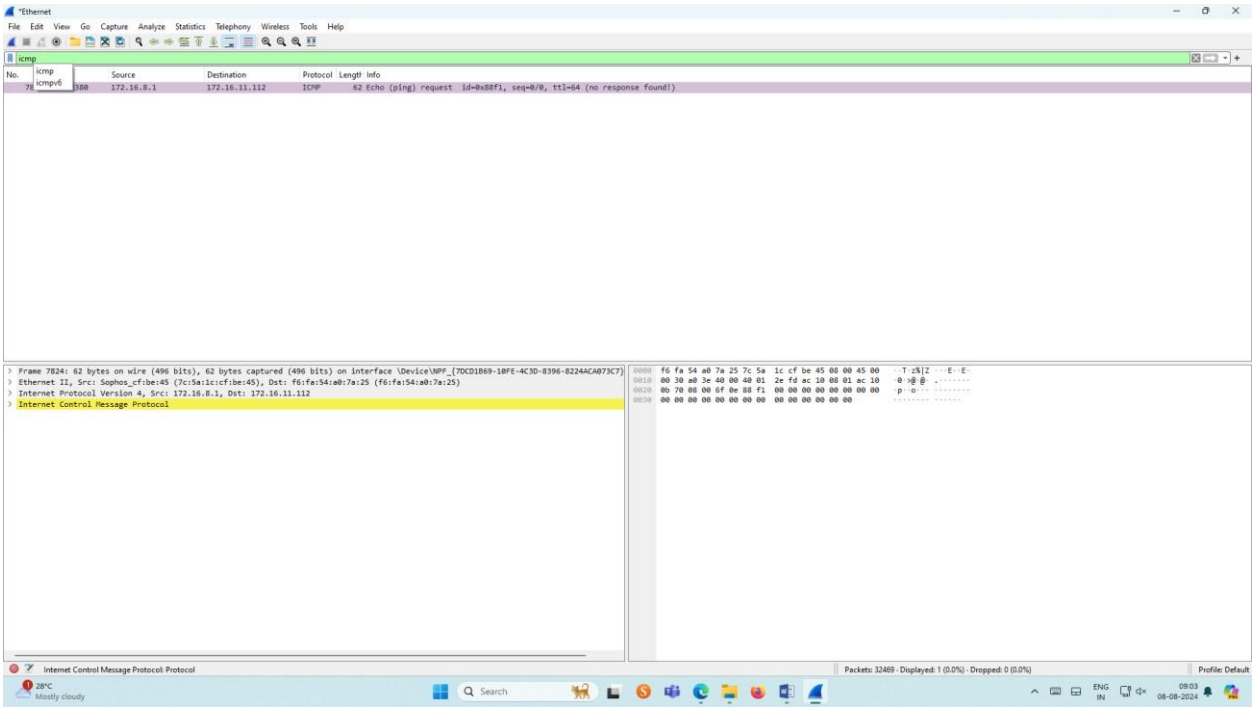


6.Create a Filter to display only IP/ICMP packets and inspect the packets.

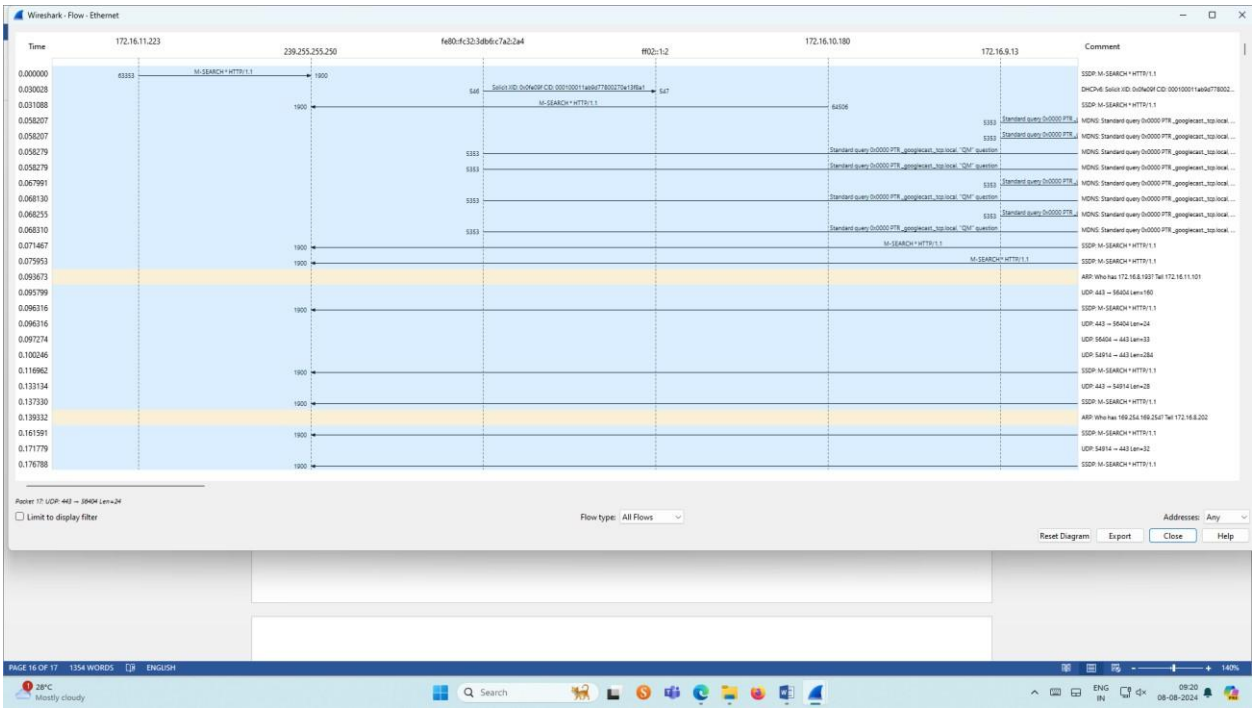
Procedure

- 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


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Source Destination Protocol Length Info
172.16.8.1 172.16.11.112 ICMP 62 Echo (ping) request id=0x88f1, seq=0/0, ttl=64 (no response found!)
Frame 7824: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface \Device\NPF_{7DCD1B69-10FE-4C3D-8396-8224ACA073C7}
Ethernet II, Src: Sophos_cf:be:45 (7c:5a:1c:cf:be:45), Dst: f6:fa:54:a0:7a:25 (f6:fa:54:a0:7a:25)
Internet Protocol Version 4, Src: 172.16.8.1, Dst: 172.16.11.112
Internet Control Message Protocol
Internet Control Message Protocol: Protocol
Packets: 32469 · Displayed: 1 (0.0%) · Dropped: 0 (0.0%)
Profile: Default
Search

Flow Graph output

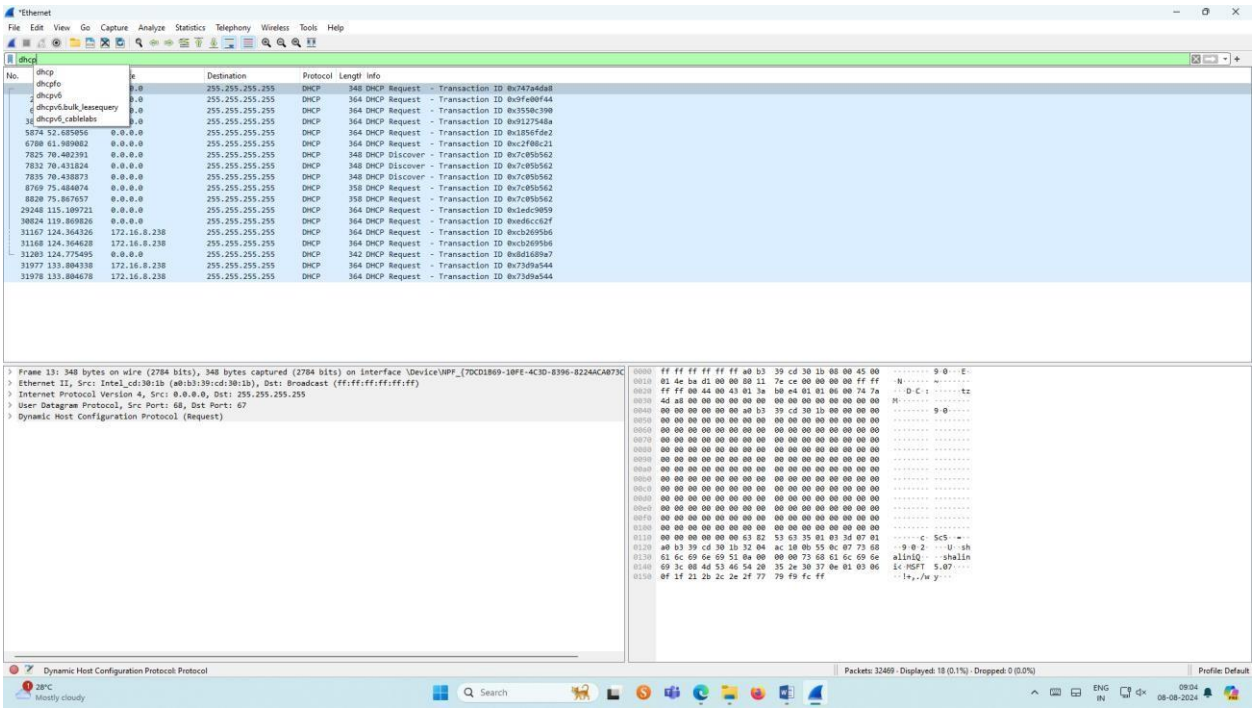


7.Create a Filter to display only DHCP packets and inspect the packets.

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.