Ex No: 14 b **PACKET SNIFFING USING WIRESHARK**

Date : 14.8.2024

AIM:

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

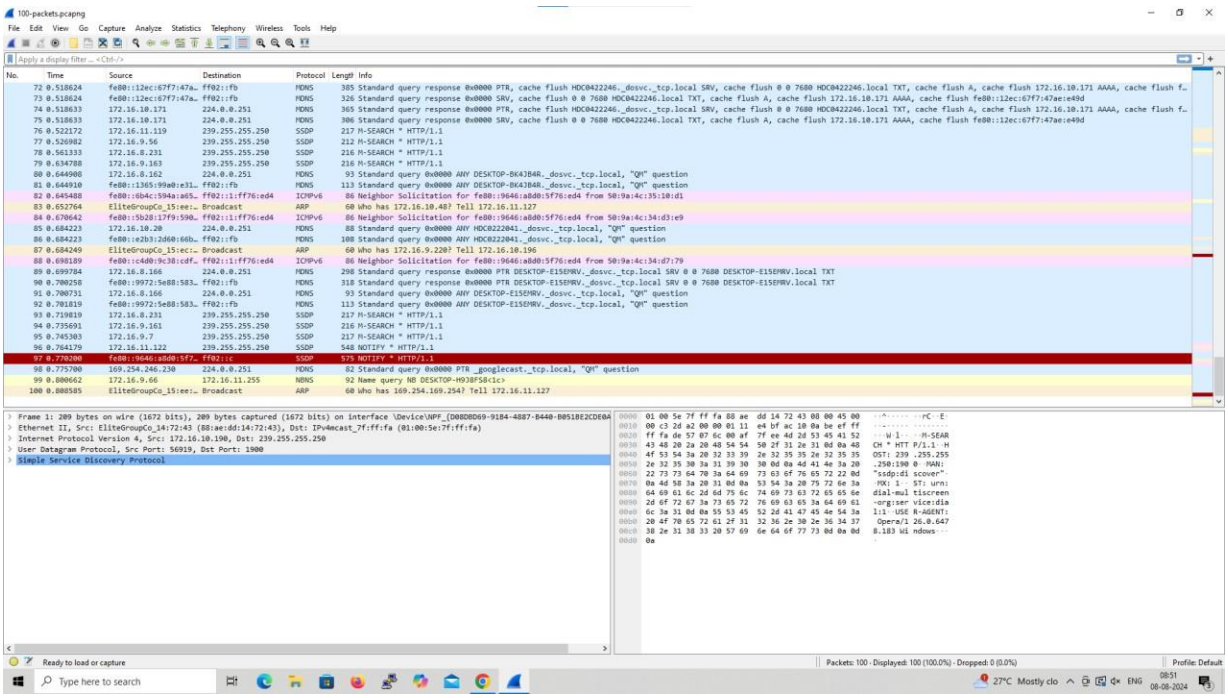
Exercises

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

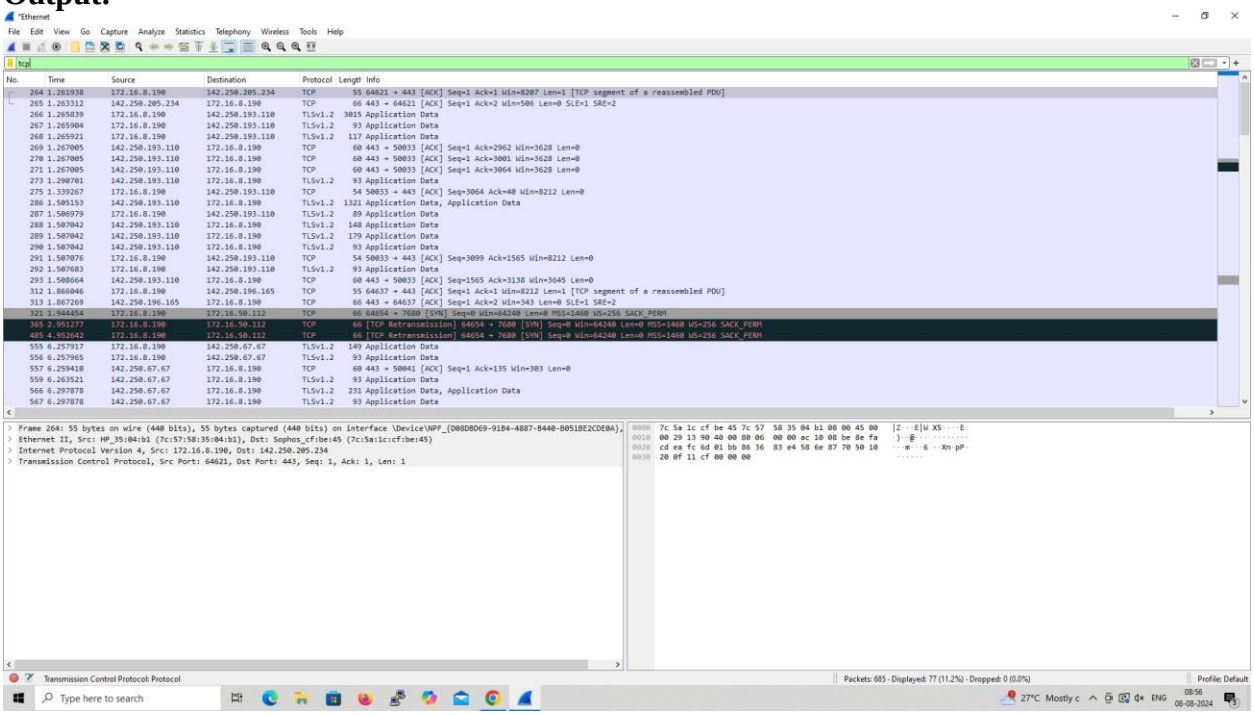


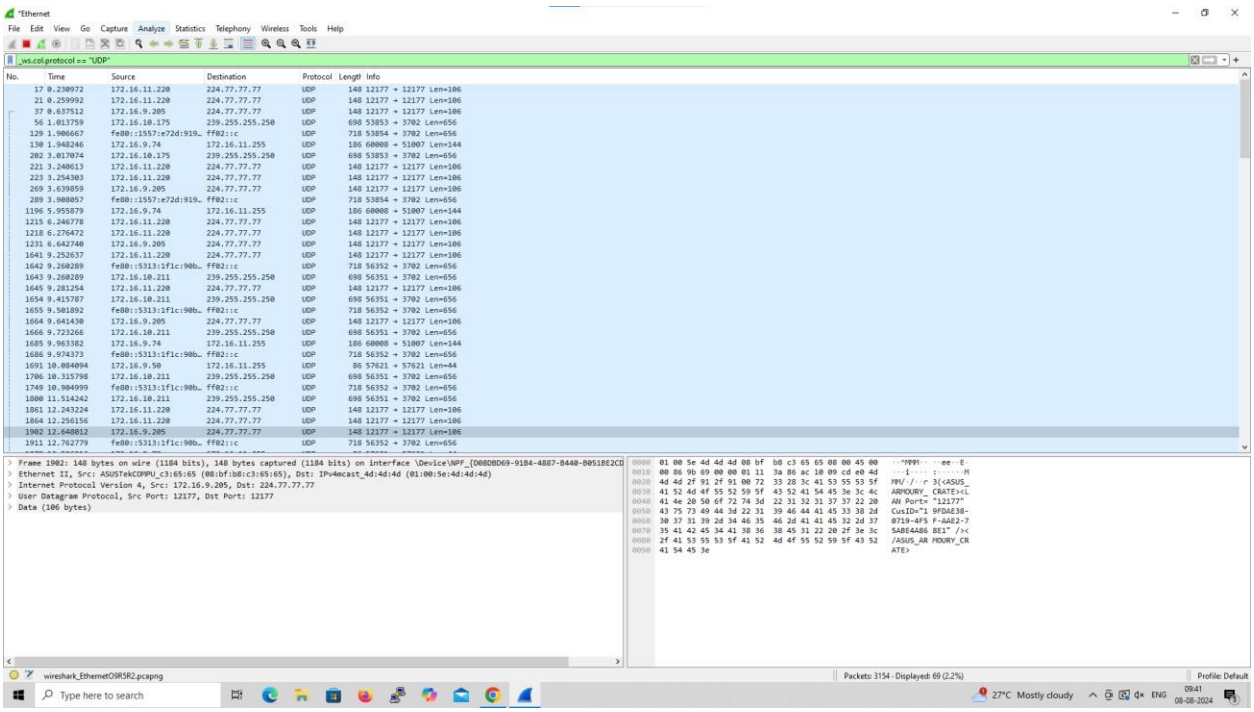
2. Create a Filter to display only TCP/UDP packets, inspect the packets and provide the flow graph.

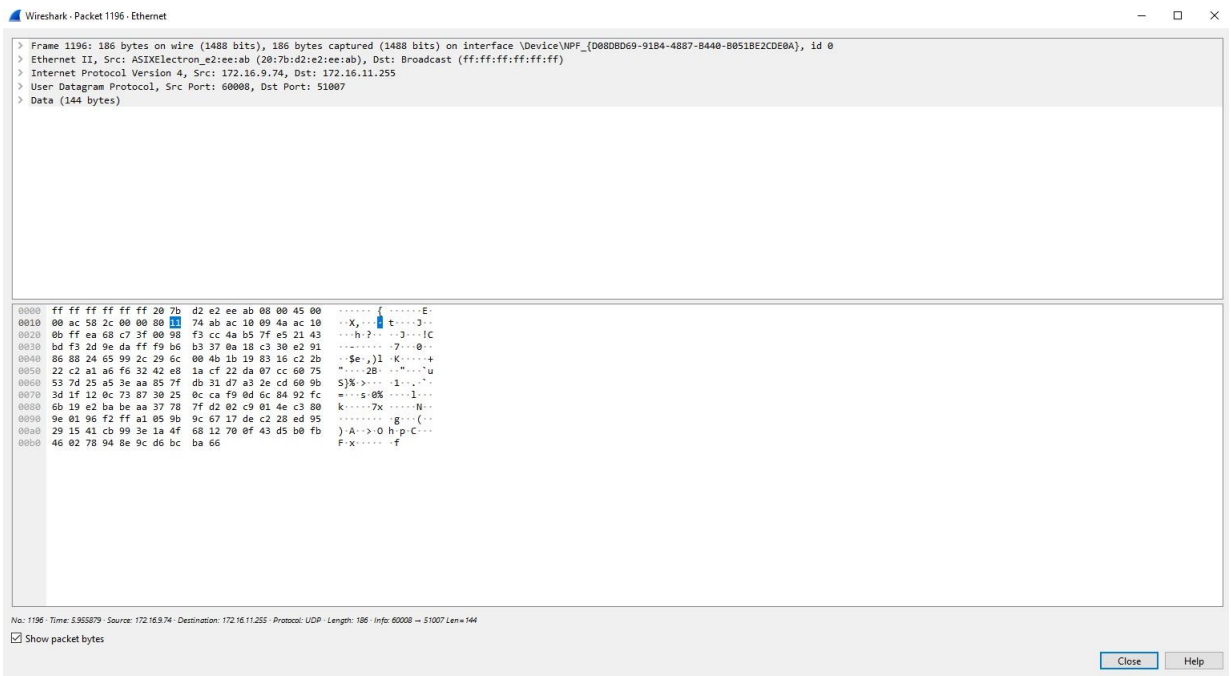
Procedure

- 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.

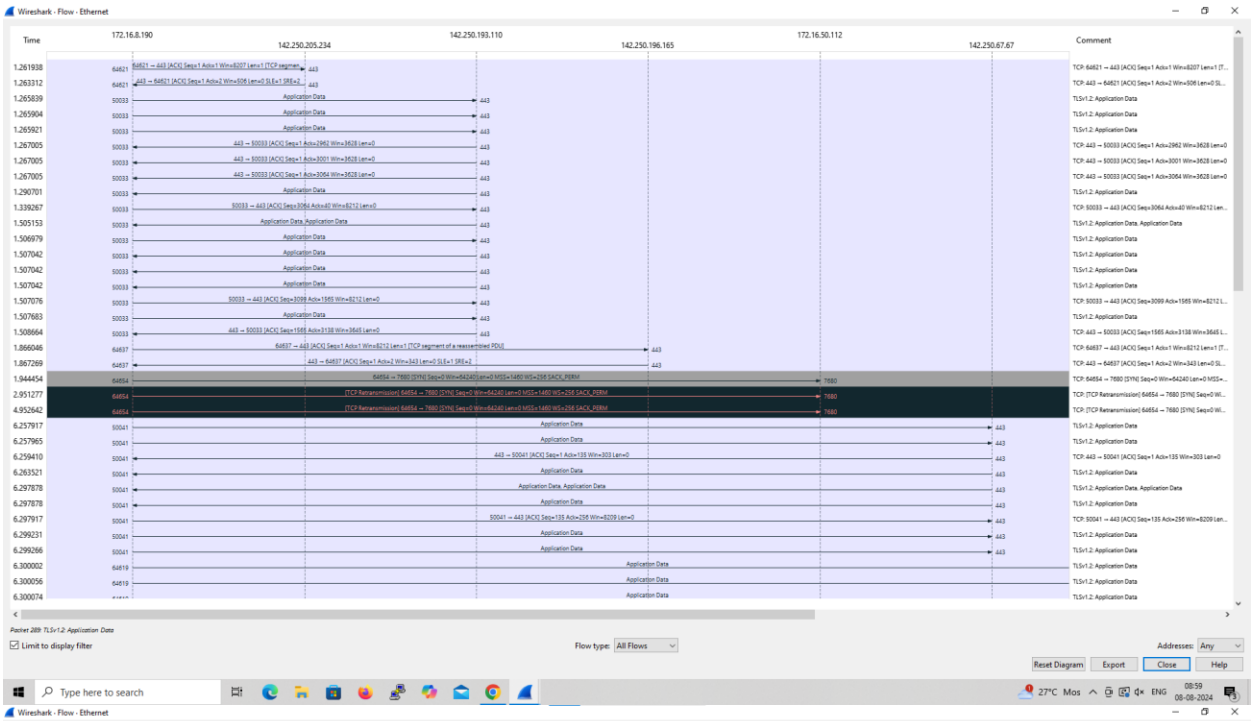
Output:

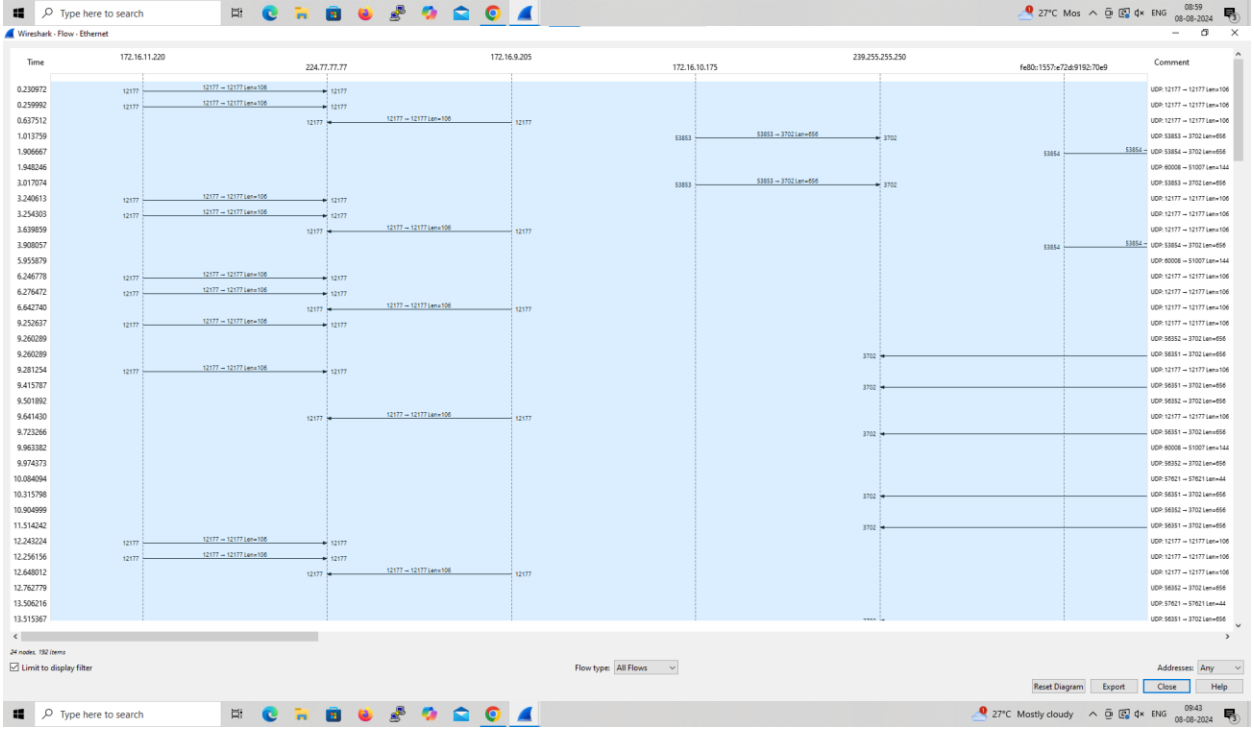



*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
_ws.col.protocol == "UDP"
No. Time Source Destination Protocol Length Info
17 0.230972 172.16.11.220 224.77.77.77 UDP 148 12177 → 12177 Len=106
21 0.259992 172.16.11.220 224.77.77.77 UDP 148 12177 → 12177 Len=106
37 0.637512 172.16.9.205 224.77.77.77 UDP 148 12177 → 12177 Len=106
56 1.013759 172.16.10.175 239.255.255.250 UDP 698 53853 → 3702 Len=656
129 1.906667 fe80::1557:e72d:919… ff02::c UDP 718 53854 → 3702 Len=656
130 1.948246 172.16.9.74 172.16.11.255 UDP 186 60008 → 51007 Len=144
202 3.017074 172.16.10.175 239.255.255.250 UDP 698 53853 → 3702 Len=656
221 3.240613 172.16.11.220 224.77.77.77 UDP 148 12177 → 12177 Len=106
223 3.254303 172.16.11.220 224.77.77.77 UDP 148 12177 → 12177 Len=106
269 3.639859 172.16.9.205 224.77.77.77 UDP 148 12177 → 12177 Len=106
289 3.980857 fe80::1557:e72d:919… ff02::c UDP 718 53854 → 3702 Len=656
1196 5.955879 172.16.9.74 172.16.11.255 UDP 186 60008 → 51007 Len=144
1215 6.246778 172.16.11.220 224.77.77.77 UDP 148 12177 → 12177 Len=106
1218 6.276472 172.16.11.220 224.77.77.77 UDP 148 12177 → 12177 Len=106
1231 6.642740 172.16.9.205 224.77.77.77 UDP 148 12177 → 12177 Len=106
1641 9.252637 172.16.11.220 224.77.77.77 UDP 148 12177 → 12177 Len=106
1642 9.260289 fe80::5313:1f1c:90b… ff02::c UDP 718 56352 → 3702 Len=656
1643 9.260289 172.16.10.211 239.255.255.250 UDP 698 56351 → 3702 Len=656
1645 9.281254 172.16.11.220 224.77.77.77 UDP 148 12177 → 12177 Len=106
1654 9.415787 172.16.10.211 239.255.255.250 UDP 698 56351 → 3702 Len=656
1655 9.501892 fe80::5313:1f1c:90b… ff02::c UDP 718 56352 → 3702 Len=656
1664 9.641430 172.16.9.205 224.77.77.77 UDP 148 12177 → 12177 Len=106
1666 9.723266 172.16.10.211 239.255.255.250 UDP 698 56351 → 3702 Len=656
1685 9.963382 172.16.9.74 172.16.11.255 UDP 186 60008 → 51007 Len=144
1686 9.974373 fe80::5313:1f1c:90b… ff02::c UDP 718 56352 → 3702 Len=656
1691 10.084094 172.16.9.50 172.16.11.255 UDP 86 57621 → 57621 Len=44
1706 10.315798 172.16.10.211 239.255.255.250 UDP 698 56351 → 3702 Len=656
1749 10.904999 fe80::5313:1f1c:90b… ff02::c UDP 718 56352 → 3702 Len=656
1800 11.514242 172.16.10.211 239.255.255.250 UDP 698 56351 → 3702 Len=656
1861 12.243224 172.16.11.220 224.77.77.77 UDP 148 12177 → 12177 Len=106
1864 12.256156 172.16.11.220 224.77.77.77 UDP 148 12177 → 12177 Len=106
1902 12.648012 172.16.9.205 224.77.77.77 UDP 148 12177 → 12177 Len=106
1911 12.762779 fe80::5313:1f1c:90b… ff02::c UDP 718 56352 → 3702 Len=656
Frame 1902: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface \Device\NPF_{D08DBD69-91B4-4887-B440-B051BE2CD
Ethernet II, Src: ASUSTekCOMPU_c3:65:65 (08:bf:b8:c3:65:65), Dst: IPv4mcast_4d:4d:4d (01:00:5e:4d:4d:4d)
Internet Protocol Version 4, Src: 172.16.9.205, Dst: 224.77.77.77
User Datagram Protocol, Src Port: 12177, Dst Port: 12177
Data (106 bytes)
wireshark_EthernetO9R5R2.pcapng
Packets: 3154 · Displayed: 69 (2.2%)
Profile: Default
Type here to search
27°C Mostly cloudy
ENG
09:41
08-08-2024


Wireshark · Packet 1196 · Ethernet
Frame 1196: 186 bytes on wire (1488 bits), 186 bytes captured (1488 bits) on interface \Device\NPF_{D08DBD69-91B4-4887-B440-B051BE2CDE0A}, id 0
Ethernet II, Src: ASIXElectron_e2:ee:ab (20:7b:d2:e2:ee:ab), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 172.16.9.74, Dst: 172.16.11.255
User Datagram Protocol, Src Port: 60008, Dst Port: 51007
Data (144 bytes)
0000 ff ff ff ff ff ff 20 7b d2 e2 ee ab 08 00 45 00
0010 00 ac 58 2c 00 00 80 11 74 ab ac 10 09 4a ac 10
0020 0b ff ea 68 c7 3f 00 98 f3 cc 4a b5 7f e5 21 43
0030 bd f3 2d 9e da ff f9 b6 b3 37 0a 18 c3 30 e2 91
0040 86 88 24 65 99 2c 29 6c 00 4b 1b 19 83 16 c2 2b
0050 22 c2 a1 a6 f6 32 42 e8 1a cf 22 da 07 cc 60 75
0060 53 7d 25 a5 3e aa 85 7f db 31 d7 a3 2e cd 60 9b
0070 3d 1f 12 0c 73 87 30 25 0c ca f9 0d 6c 84 92 fc
0080 6b 19 e2 ba be aa 37 78 7f d2 02 c9 01 4e c3 80
0090 9e 01 96 f2 ff a1 05 9b 9c 67 17 de c2 28 ed 95
00a0 29 15 41 cb 99 3e 1a 4f 68 12 70 0f 43 d5 b0 fb
00b0 46 02 78 94 8e 9c d6 bc ba 66
No.: 1196 · Time: 5.955879 · Source: 172.16.9.74 · Destination: 172.16.11.255 · Protocol: UDP · Length: 186 · Info: 60008 → 51007 Len=144
Show packet bytes
Close
Help

Flow Graph output



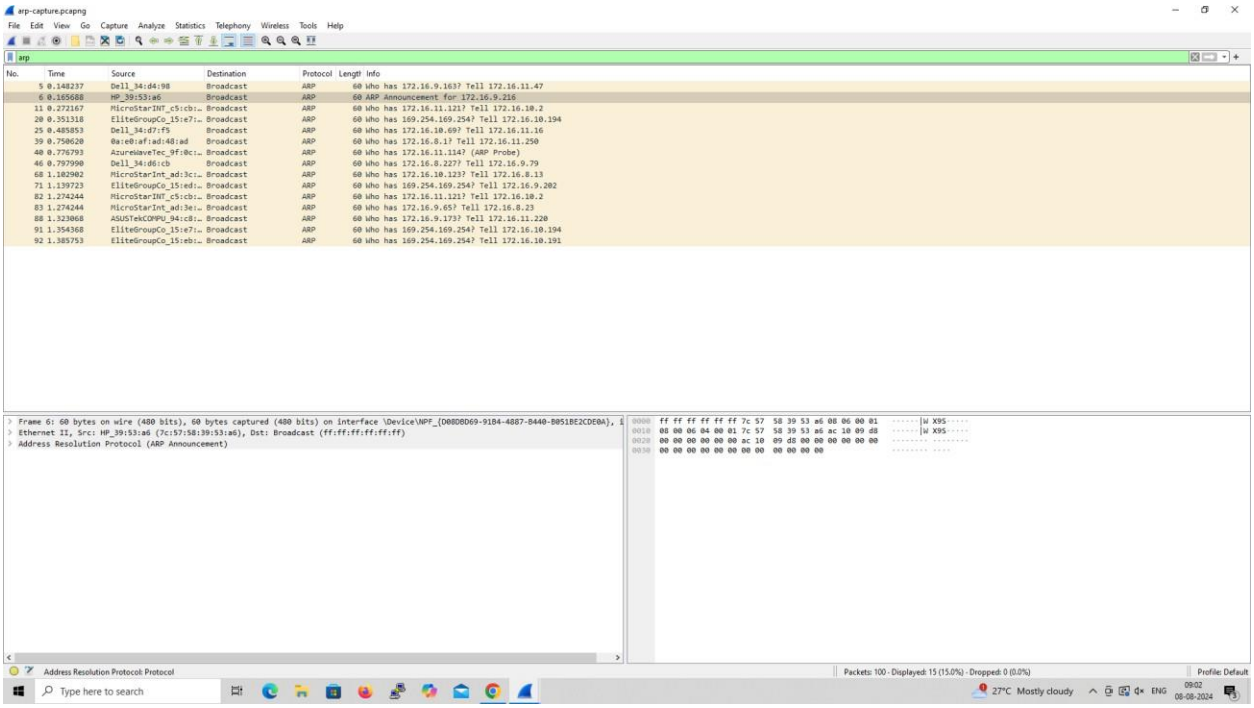


3. Create a Filter to display only ARP packets and inspect the packets.

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

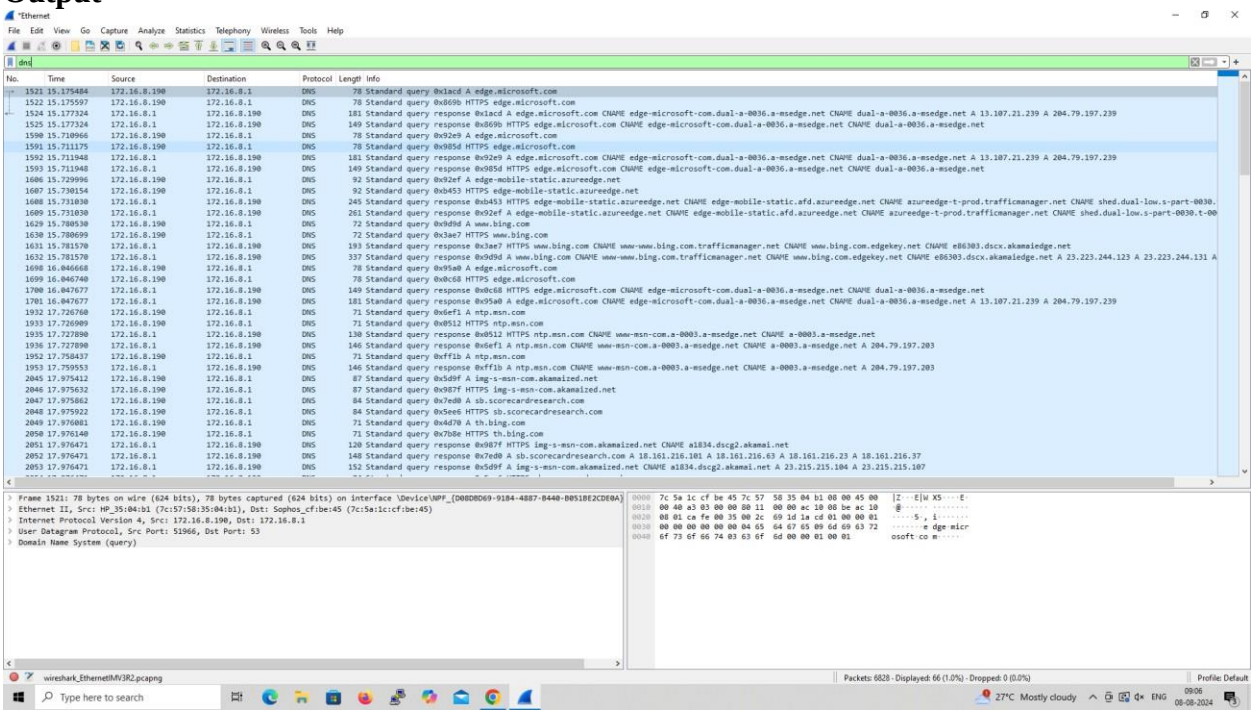


4. Create a Filter to display only DNS packets and provide the flow graph.

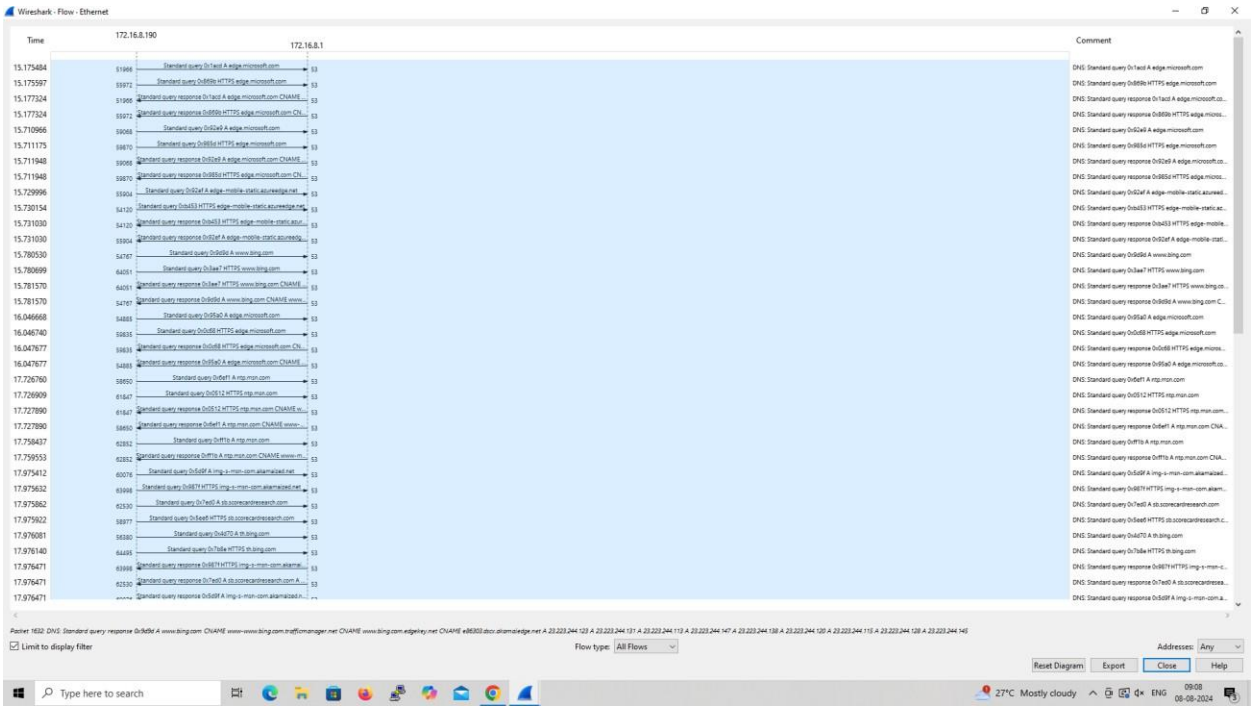
Procedure

- 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



Flow Graph output

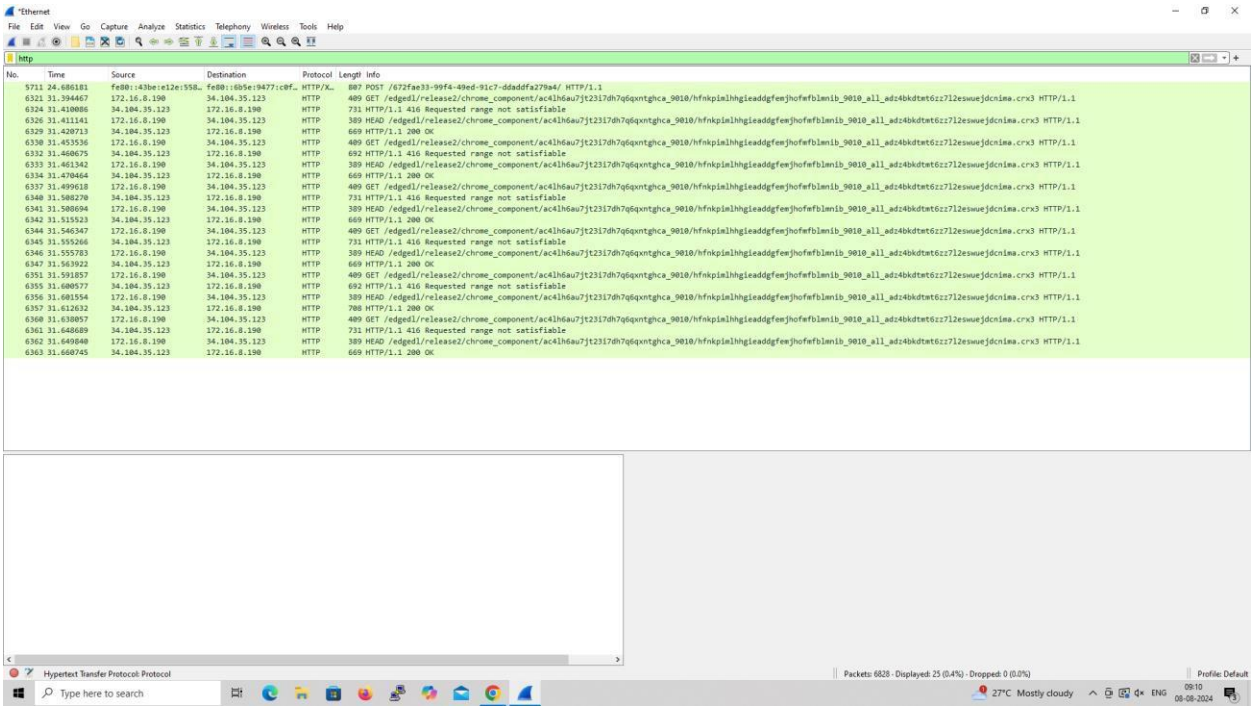


5. Create a Filter to display only HTTP packets and inspect the packets

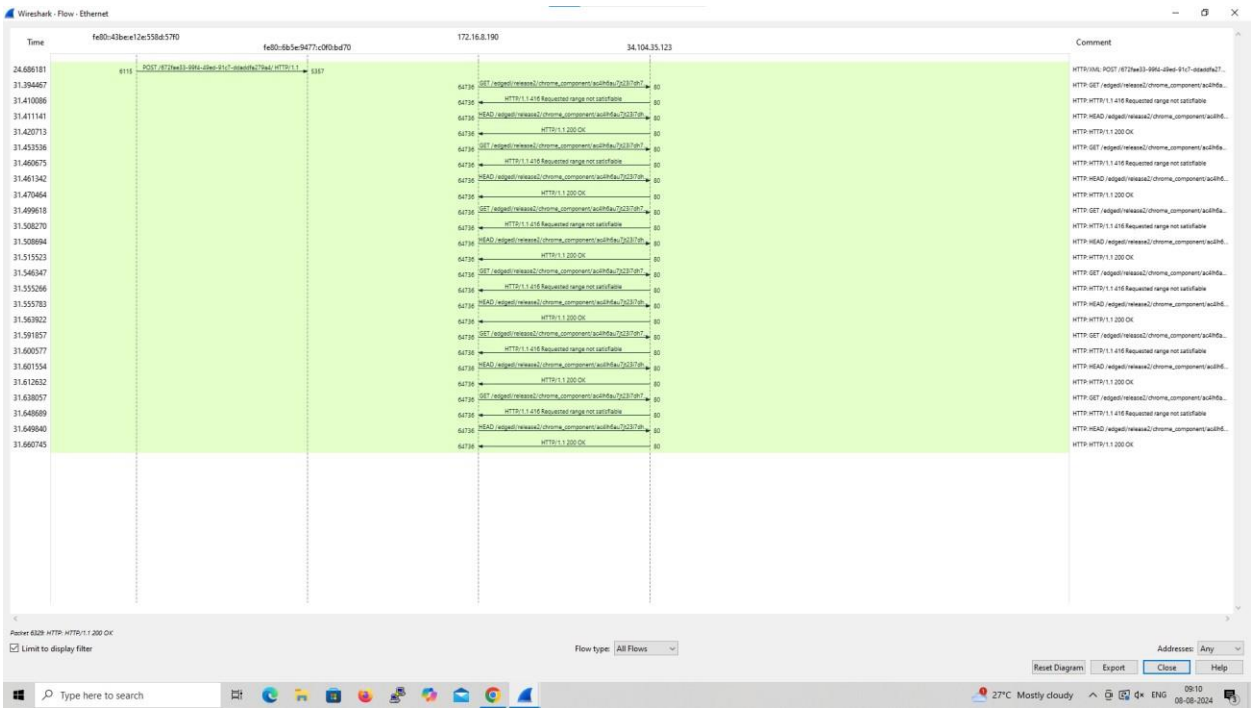
Procedure

- 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

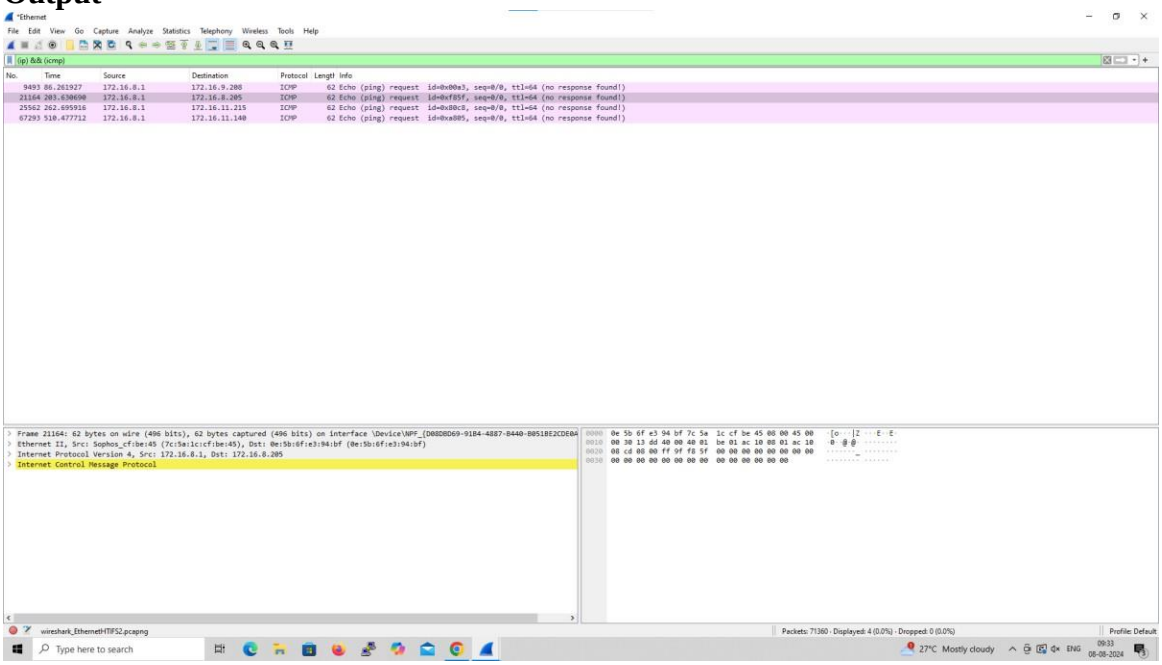


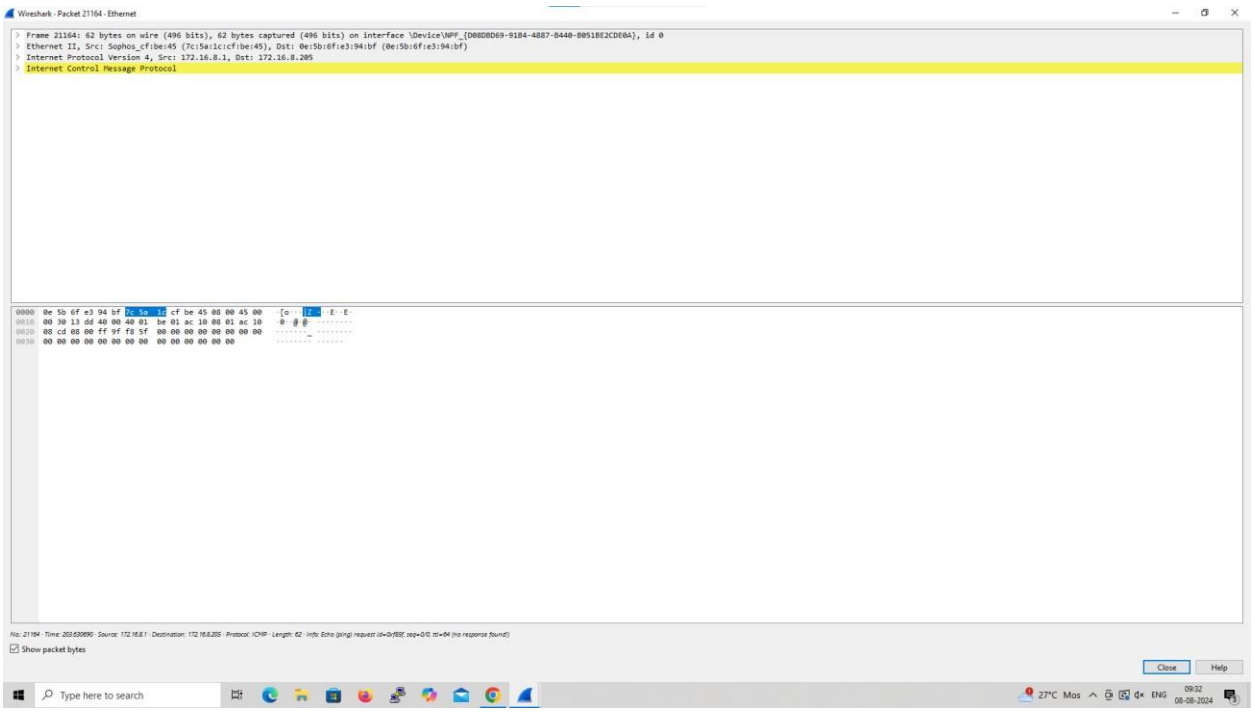
6. Create a Filter to display only IP/ICMP packets and inspect the packets.

Procedure

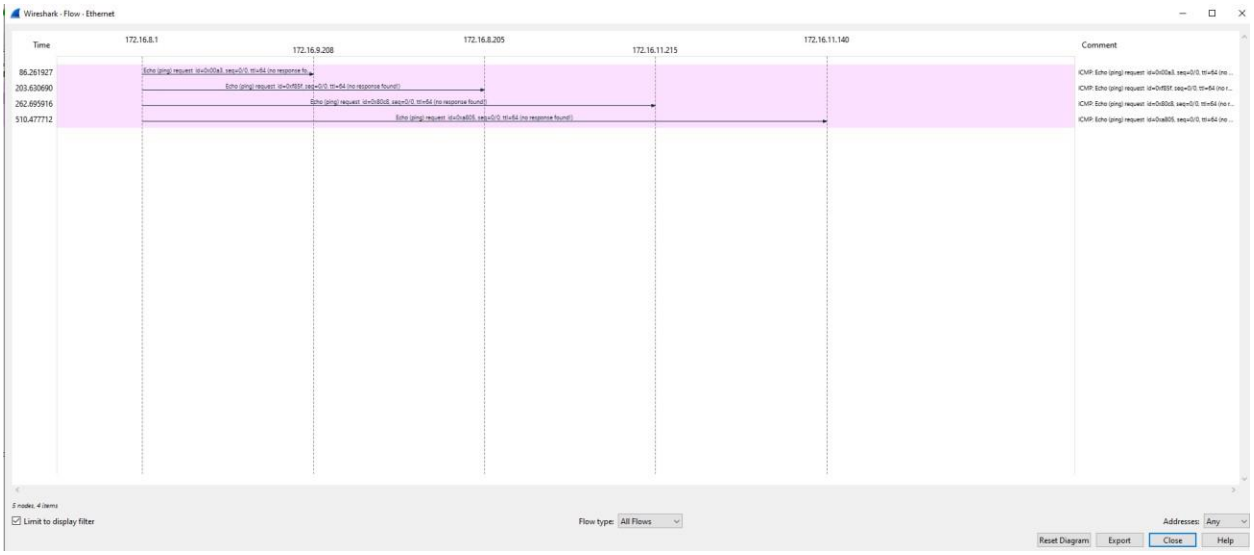
- Select Local Area Connection in Wireshark.
- Go to capture option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search ICMP/IP packets in search bar.
- Save the packets

Output :





Flow Graph output

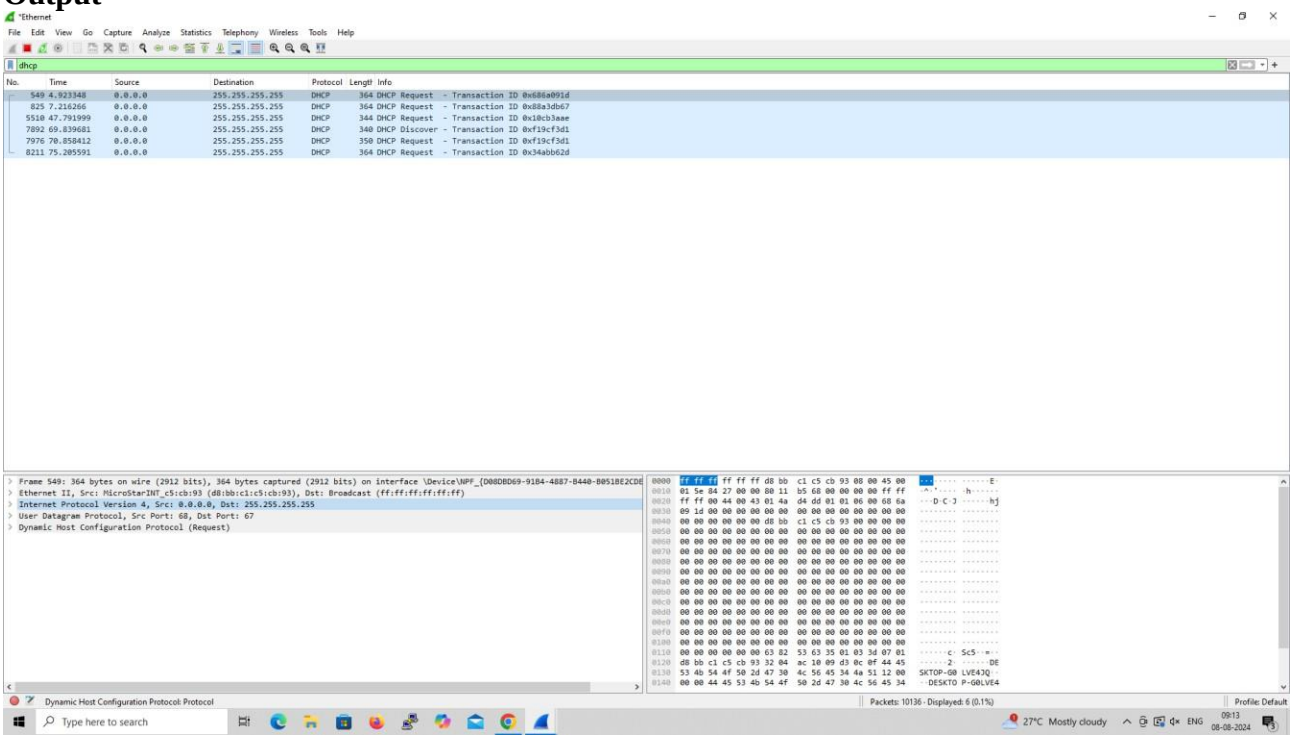


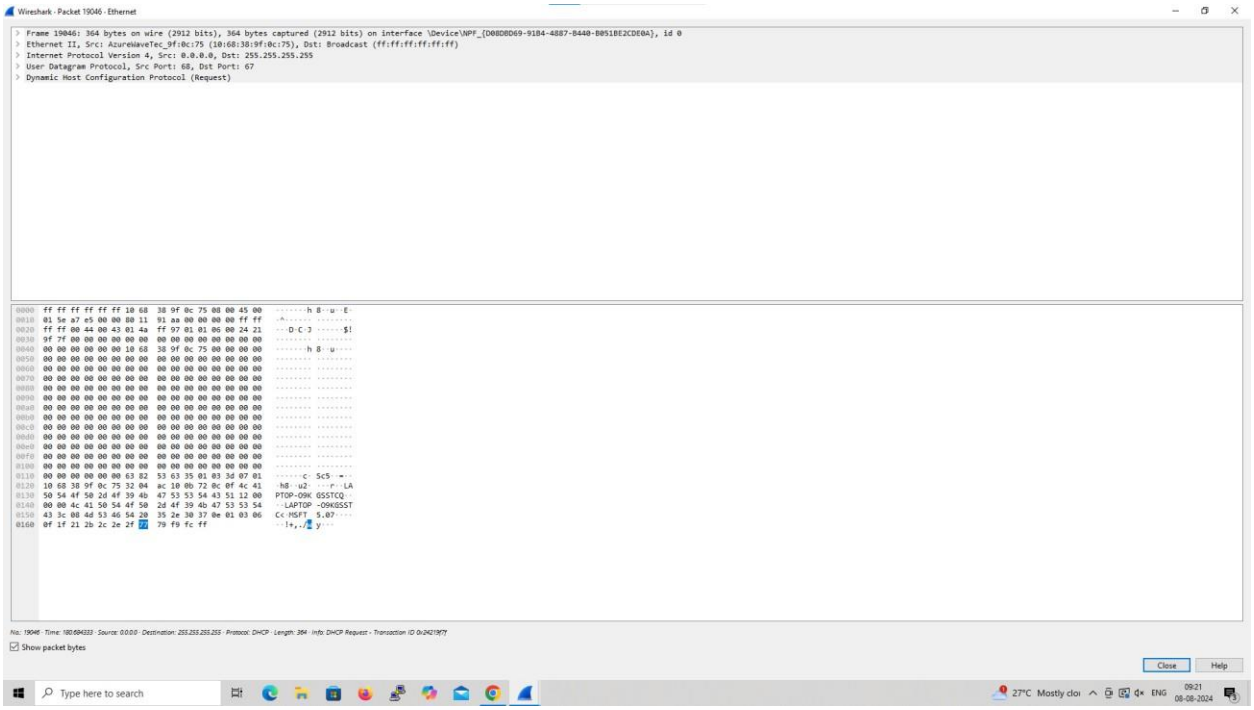
7. Create a Filter to display only DHCP packets and inspect the packets.

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 :

Hence the packet sniffing concepts using wireshark tool is completed.