

Ex No:4B

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

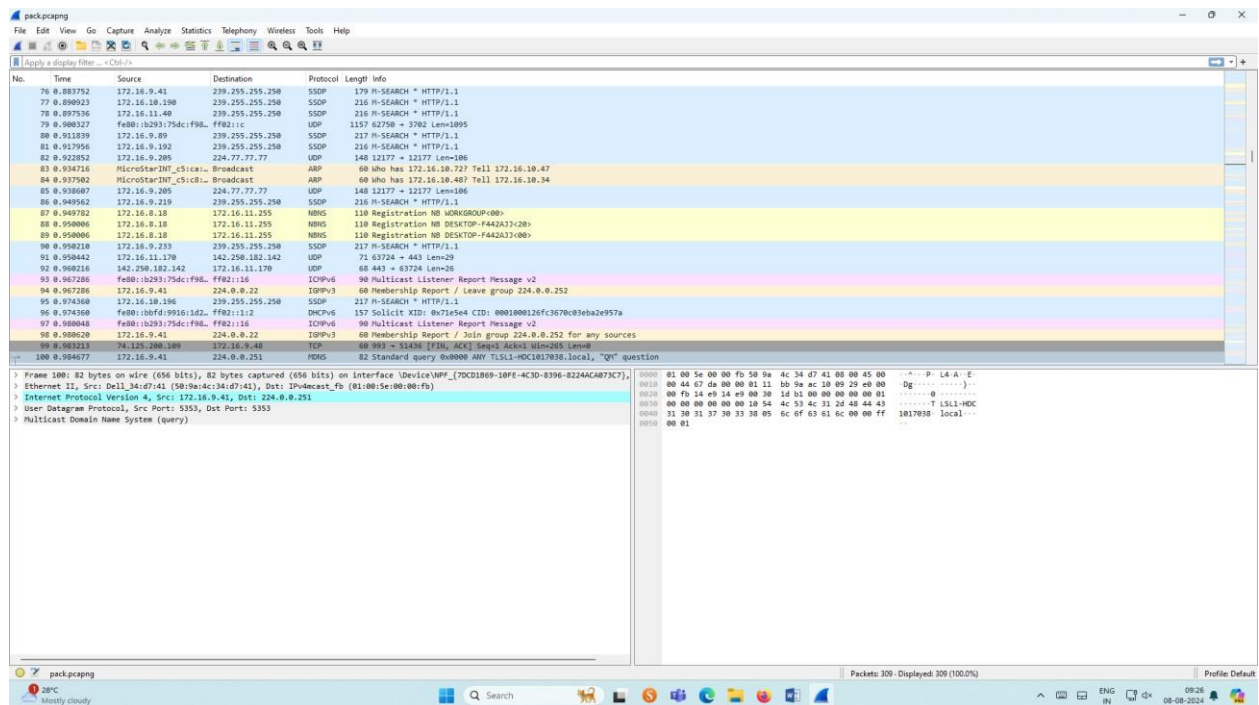
Exercises

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

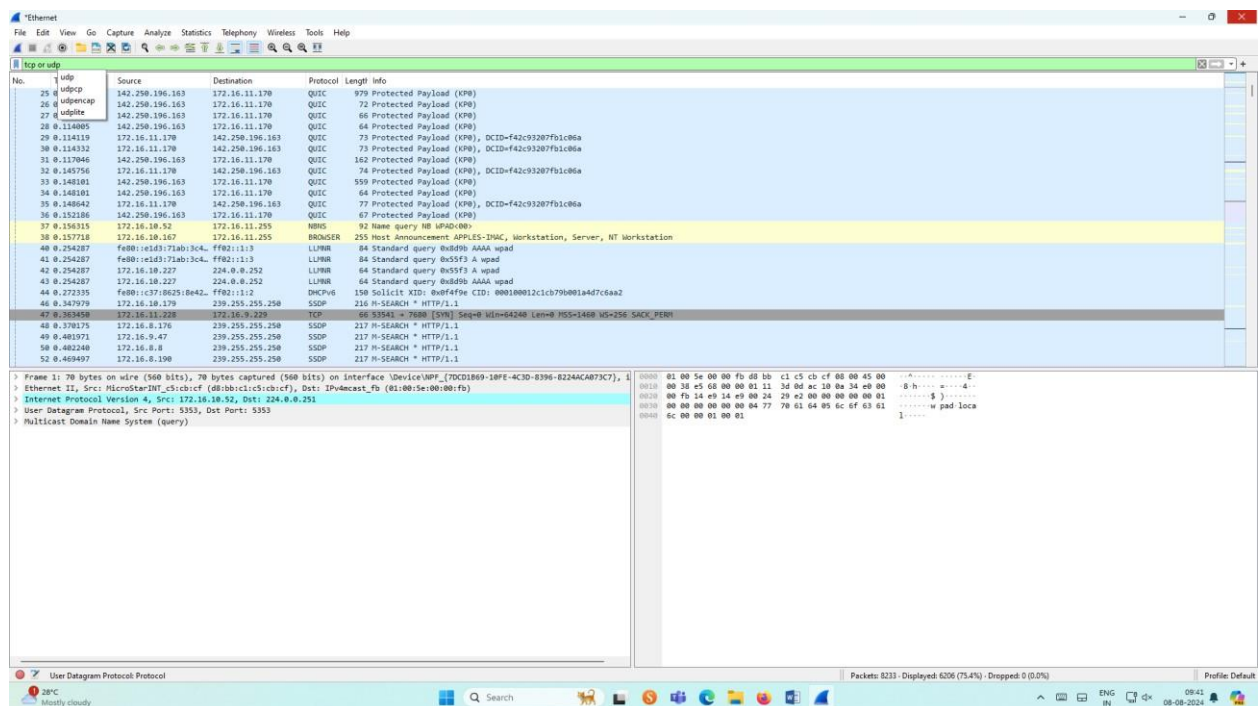


2. Create a Filter to display only TCP/UDP packets, inspect the packets and provide the flow graph.

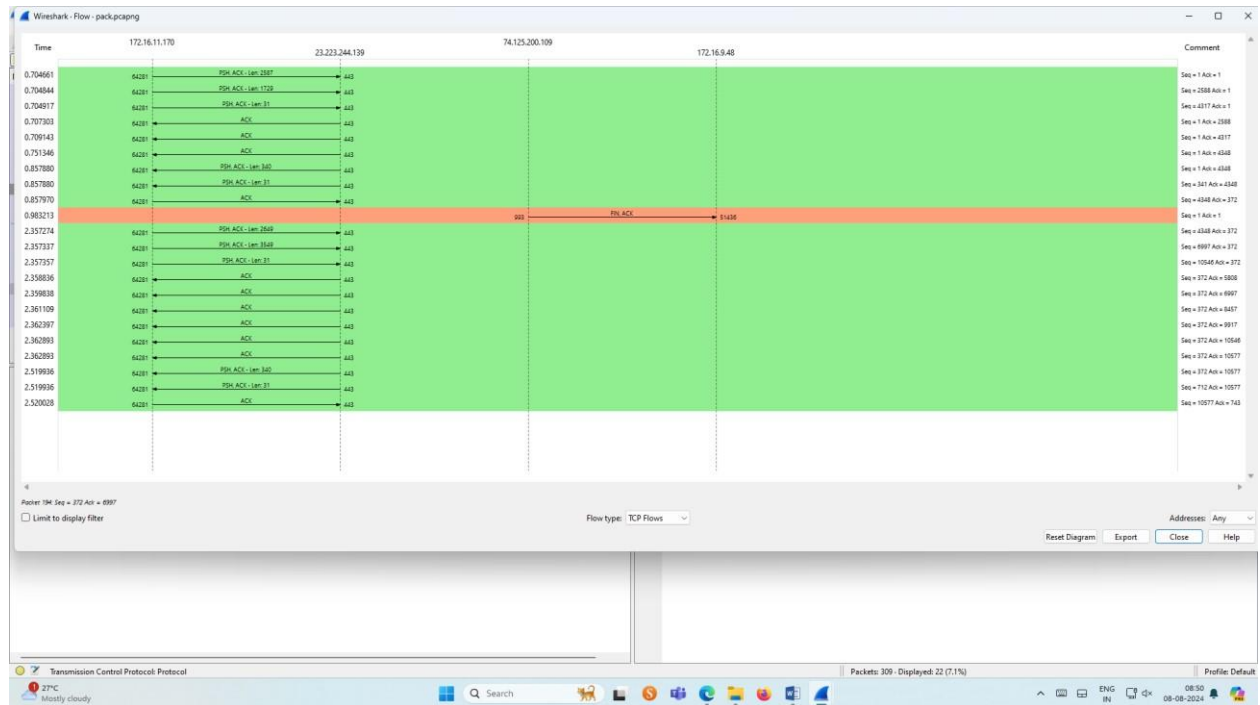
Procedure

- 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.

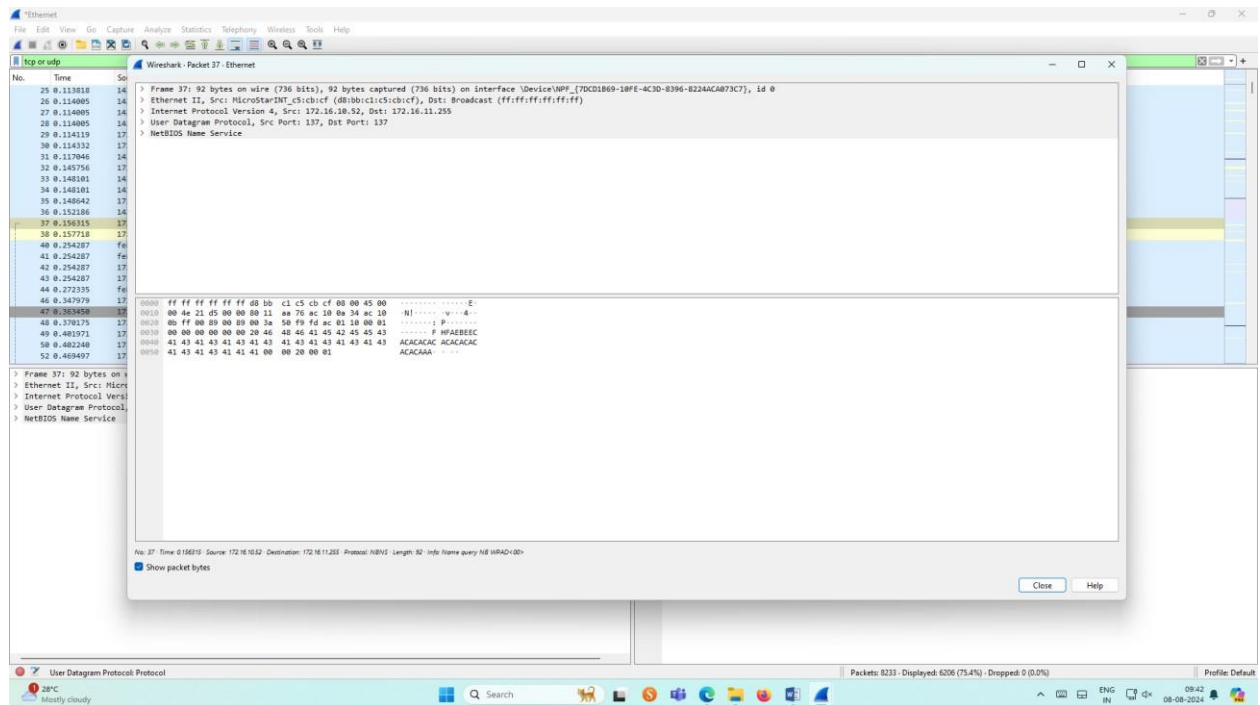
Output:



Flow Graph output




Inspecting the packets

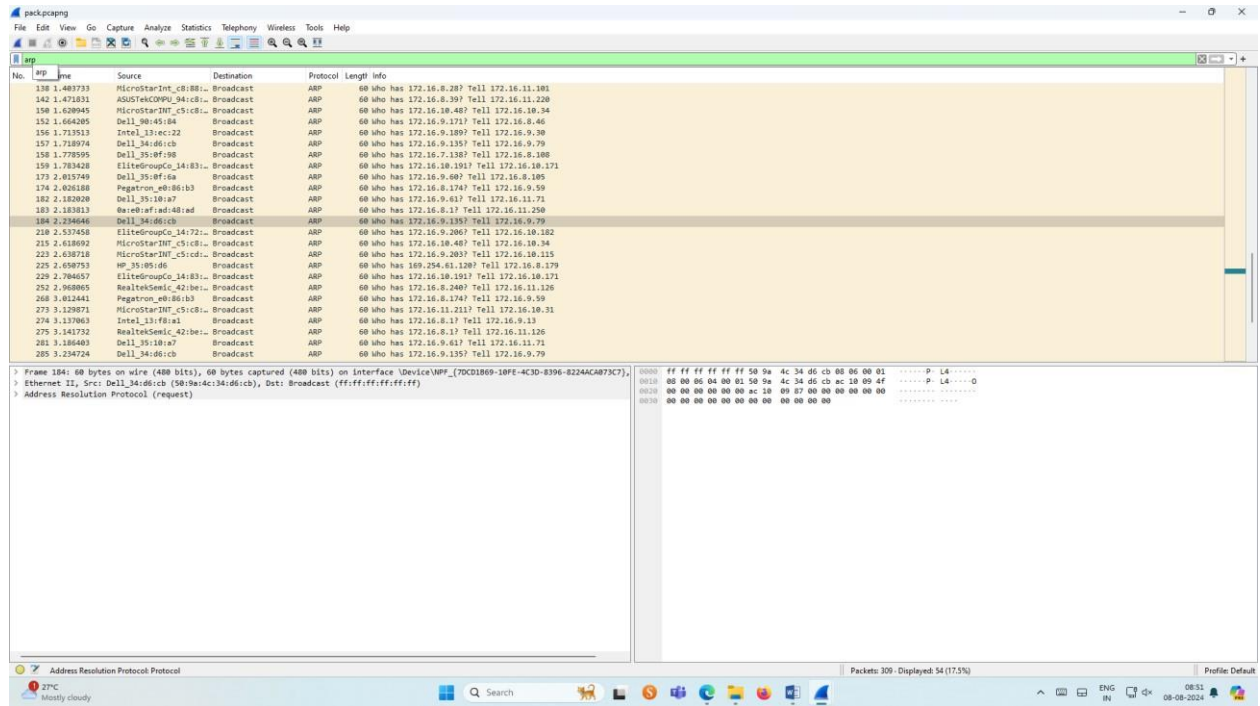


3.Create a Filter to display only ARP packets and inspect the packets.

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

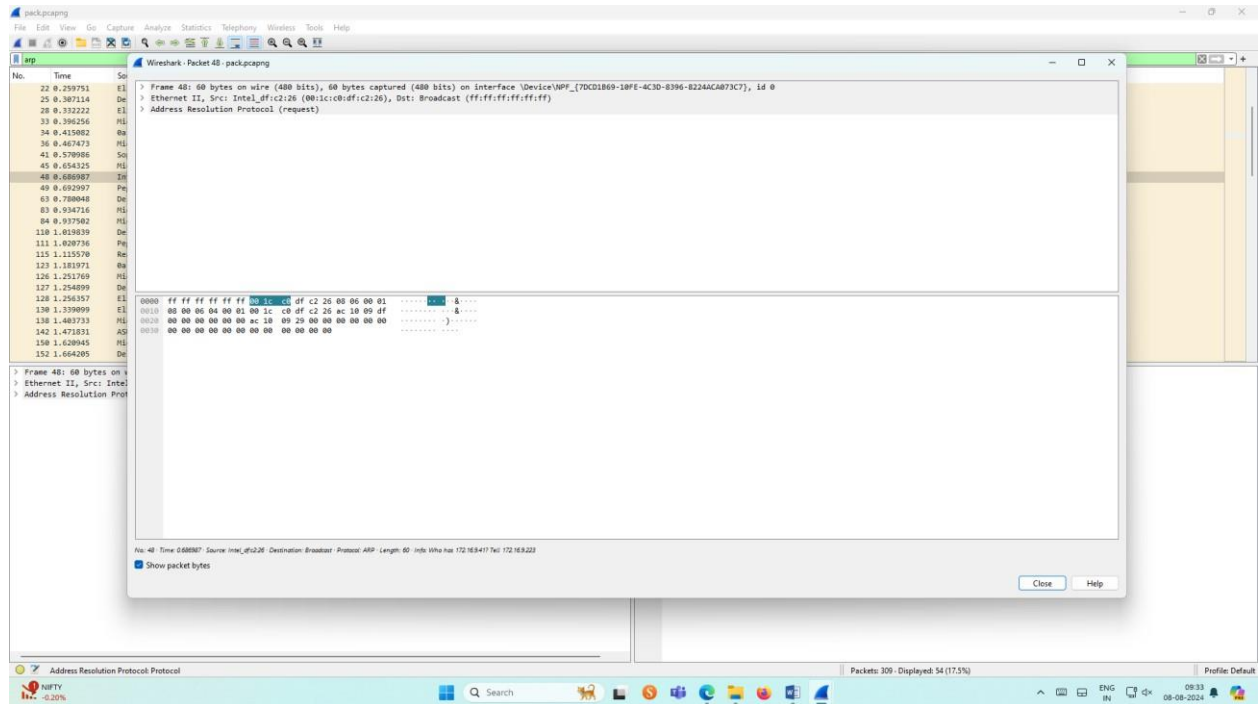


The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains icons for file operations, capture control, and analysis. The main display area is divided into three panes:

- Packet List:** Displays a list of captured packets. The first 100 packets are ARP requests, all with a destination MAC of ff:ff:ff:ff:ff:ff. The list includes columns for No., Time, Source, Destination, Protocol, Length, and Info.
- Packet Details:** Shows the details of the selected packet (No. 100). It includes the Ethernet II header (Source: Dell_34:d6:cb, Destination: Broadcast) and the Address Resolution Protocol (ARP) header (Request).
- Packet Bytes:** Displays the raw packet data in hexadecimal and ASCII format.



The status bar at the bottom indicates that 309 packets are displayed, representing 17.5% of the total capture. The system tray shows the date and time as 08-08-2024.

Inspecting the packets

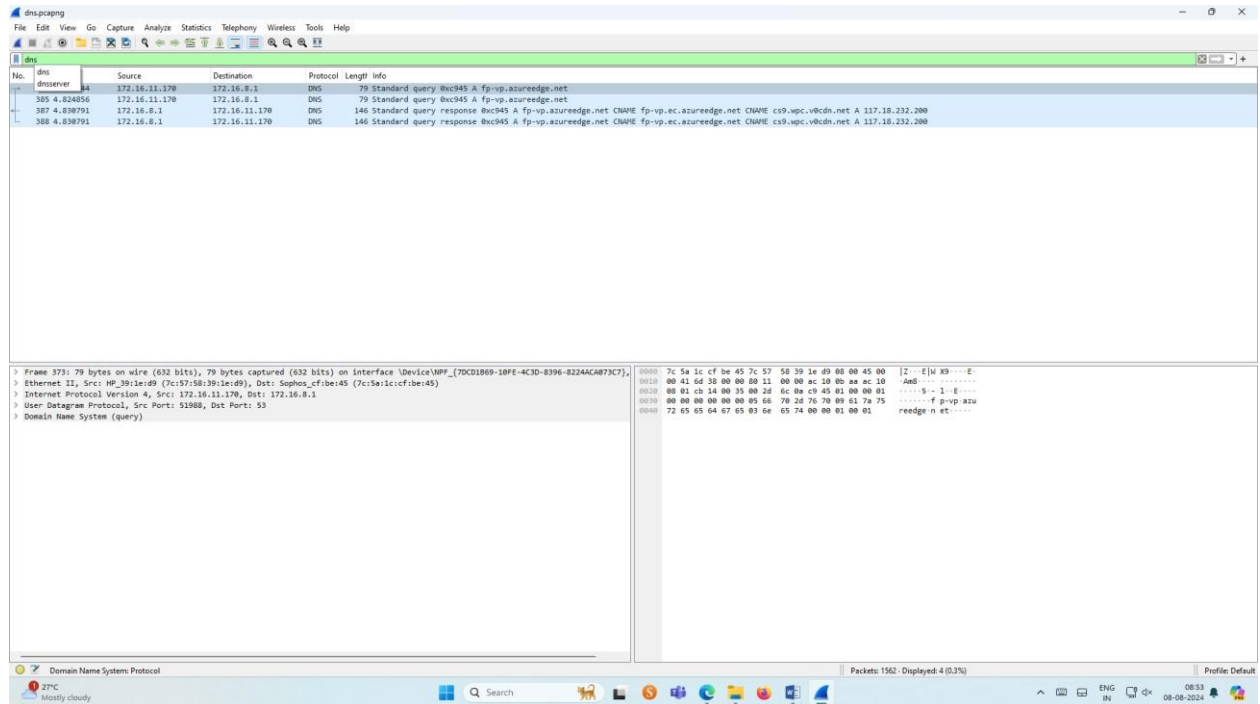


4.Create a Filter to display only DNS packets and provide the flow graph.

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



The image shows a Wireshark packet capture of DNS traffic. The top pane displays a list of packets, with the first three packets selected. The second pane shows the details of the selected packet, including the Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query) fields. The third pane shows the raw packet data in hexadecimal and ASCII.

No.	dns	Source	Destination	Protocol	Length	Info
385	4.824056	172.16.11.170	172.16.8.1	DNS	79	Standard query 8bc945 A fp-vp.azureedge.net
387	4.838791	172.16.8.1	172.16.11.170	DNS	146	Standard query response 8bc945 A fp-vp.azureedge.net CNAME fp-vp.ec.azureedge.net CNAME cs9.wpc.vcdn.net A 117.18.232.200
388	4.838791	172.16.8.1	172.16.11.170	DNS	146	Standard query response 8bc945 A fp-vp.azureedge.net CNAME fp-vp.ec.azureedge.net CNAME cs9.wpc.vcdn.net A 117.18.232.200

Frame 375: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface DeviceMPF_{70C3B69-18FE-4C3D-8396-8224ACAB73C7}, Ethernet II, Src: HP_39:1e:d9 (7c:57:58:39:1e:d9), Dst: Sophos_cf:be:45 (7c:5a:1c:cf:be:45)

Internet Protocol Version 4, Src: 172.16.11.170, Dst: 172.16.8.1

User Datagram Protocol, Src Port: 51988, Dst Port: 53

Domain Name System (query)

10000: 7c 5a 1c cf be 45 7c 57 58 39 1e d9 08 00 45 00 [2...E]u K9...E

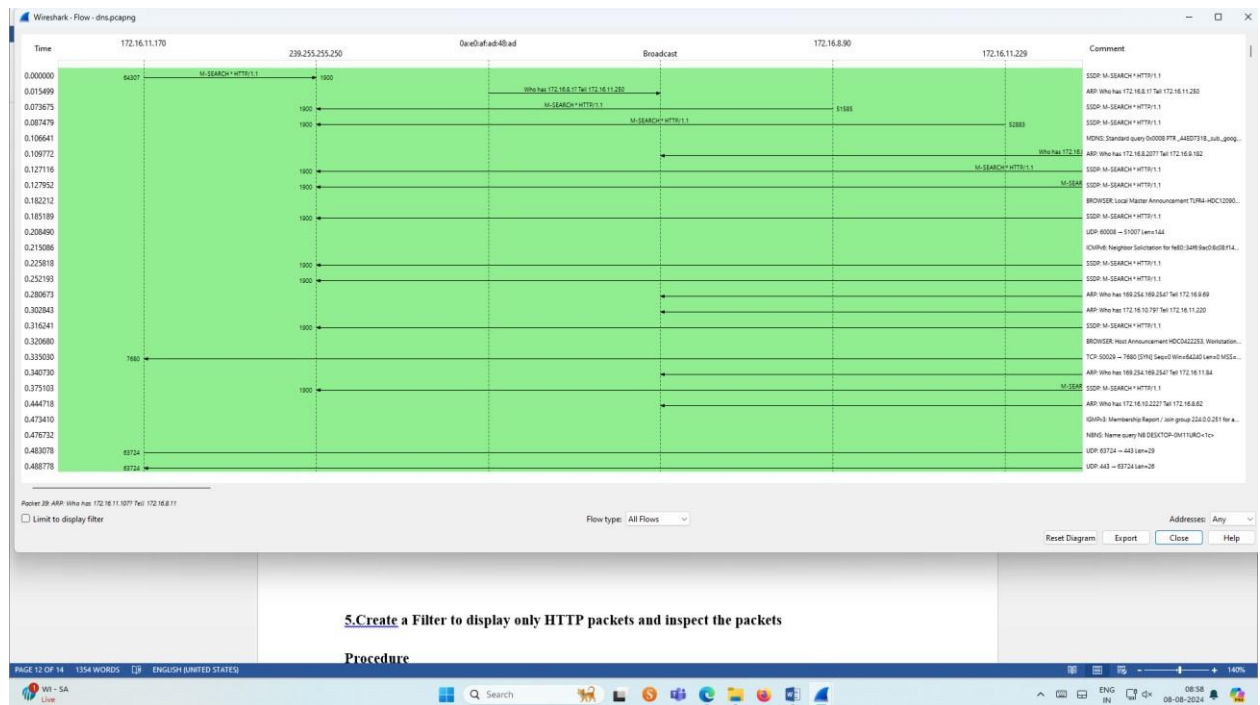
00100: 00 41 6d 38 00 00 00 11 00 00 ac 10 0b aa ac 10 A06... ..

00200: 00 01 c5 14 00 35 00 2d 6c 0a c9 45 01 00 00 01S...1..E...

00300: 00 00 00 00 00 00 65 68 78 2d 76 73 09 51 7a 75f p r p p a z u


00400: 72 65 65 64 67 65 63 6a 65 74 00 00 01 00 01r e e d g e n e t

Graph output

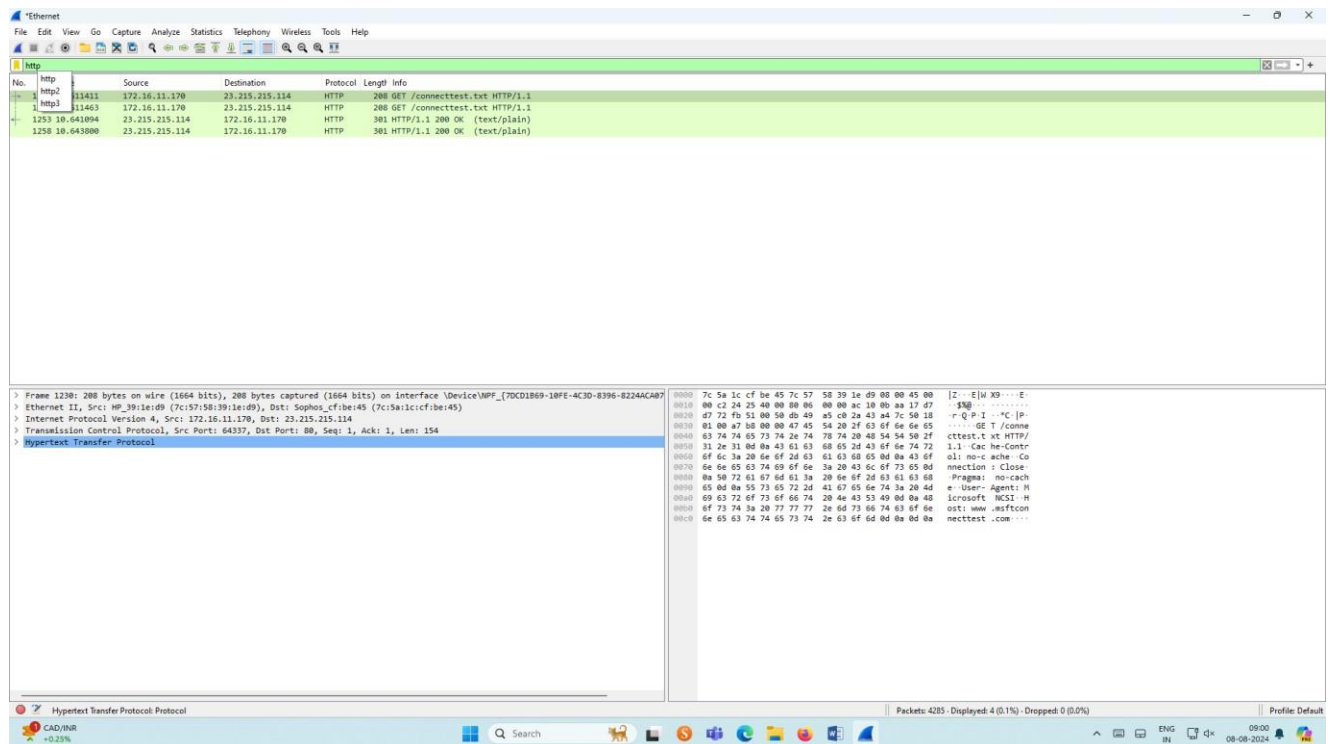


5. Create a Filter to display only HTTP packets and inspect the packets

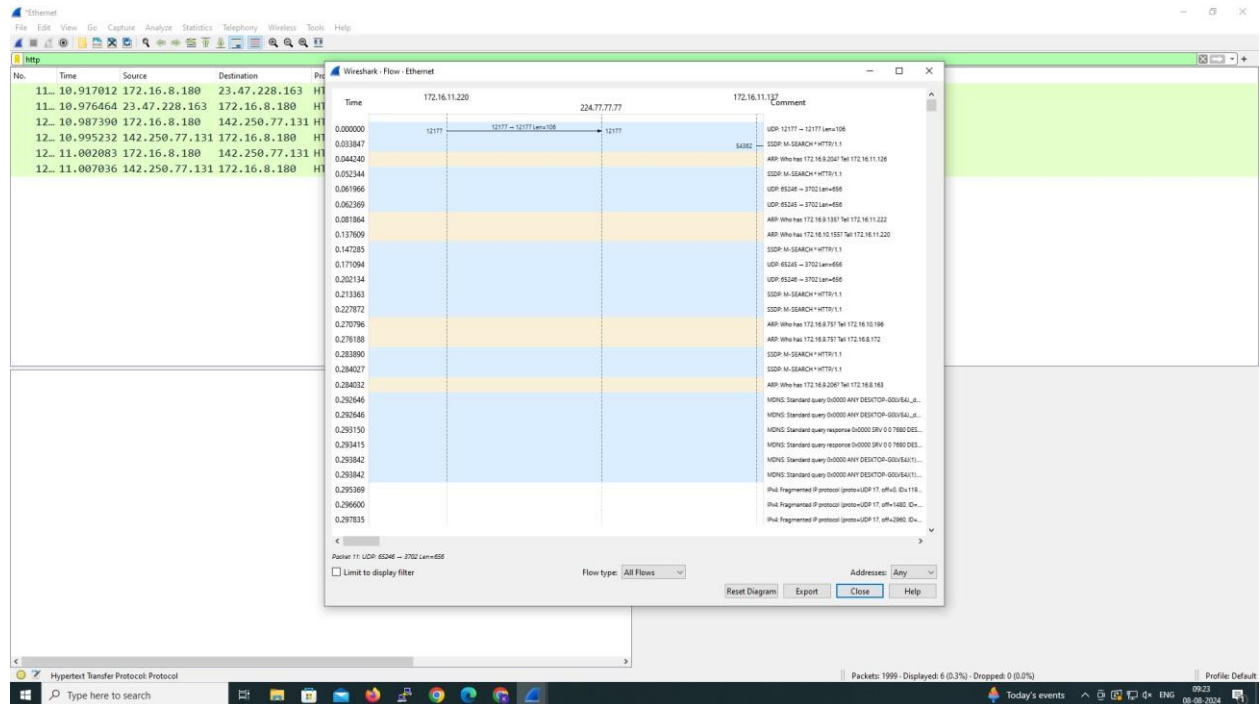
Procedure

- 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.

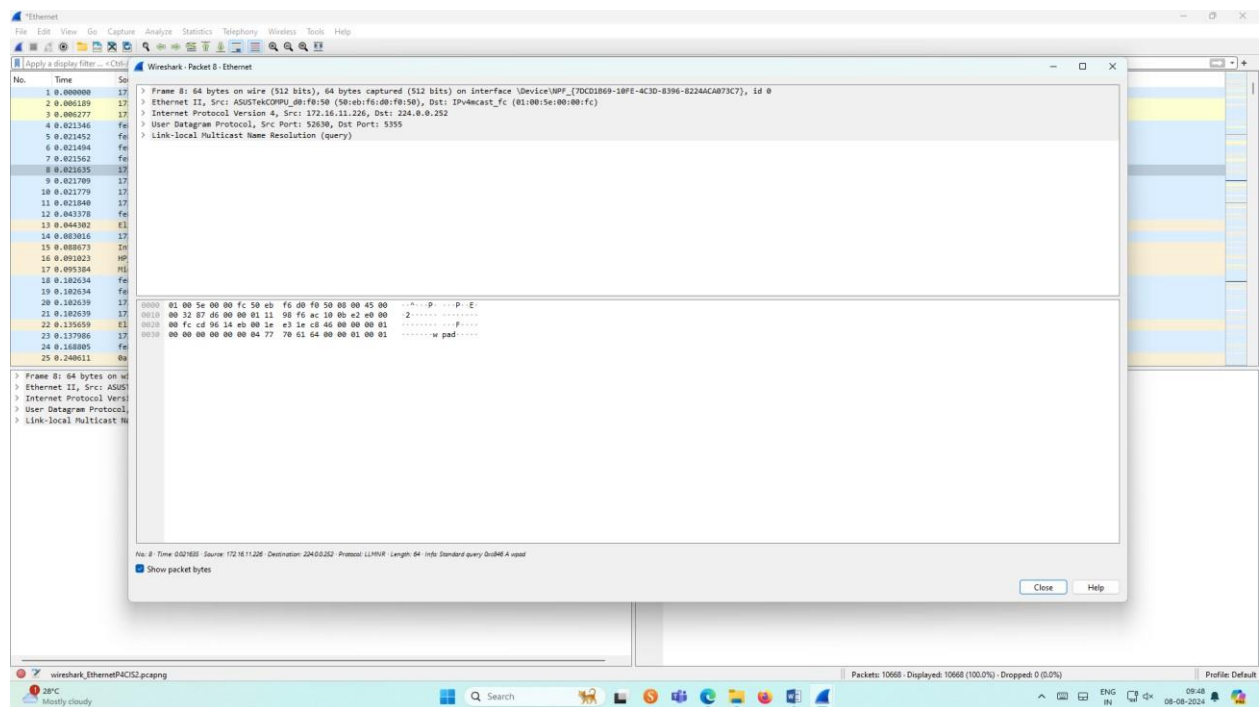
Output



Flow Graph output



Inspecting the packets

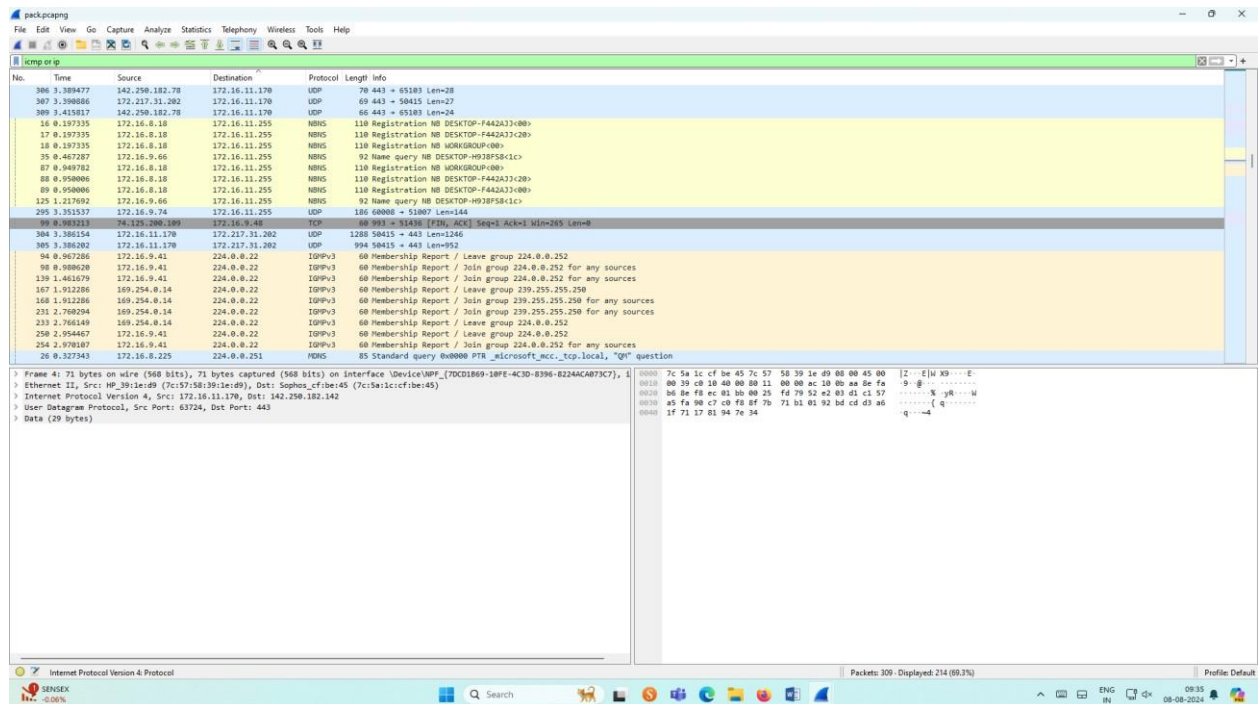


6.Create a Filter to display only IP/ICMP packets and inspect the packets.

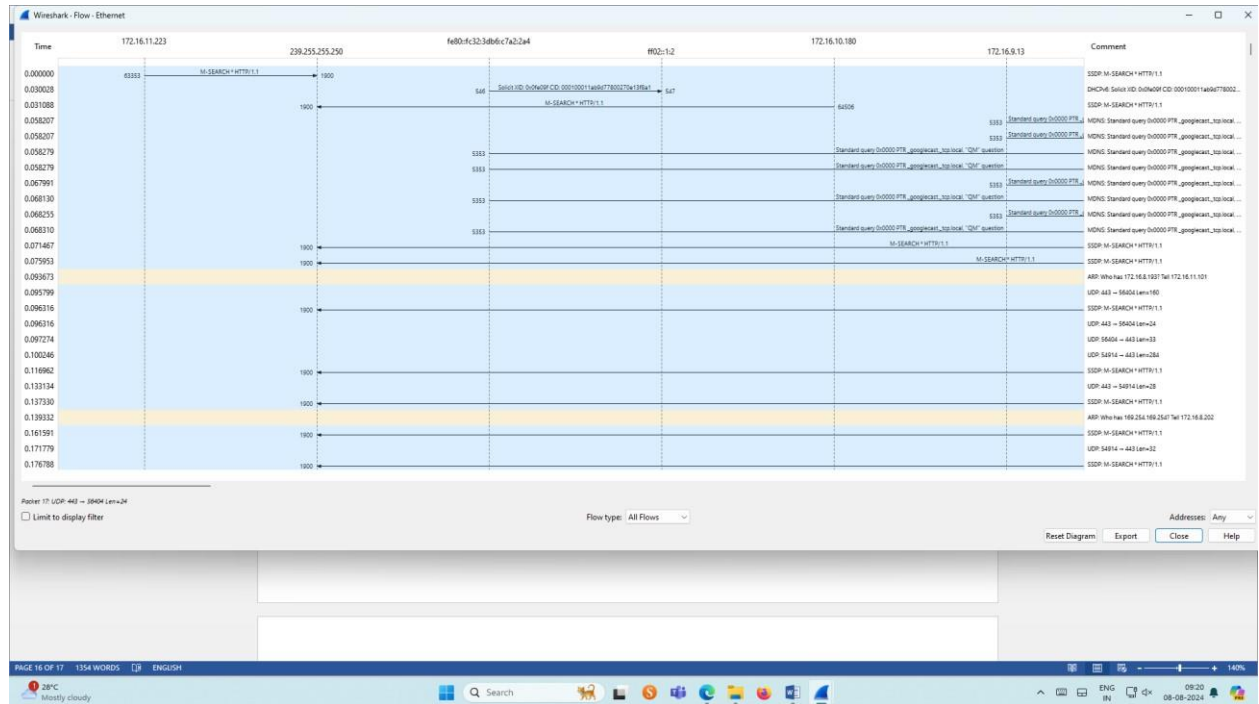
Procedure

- 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

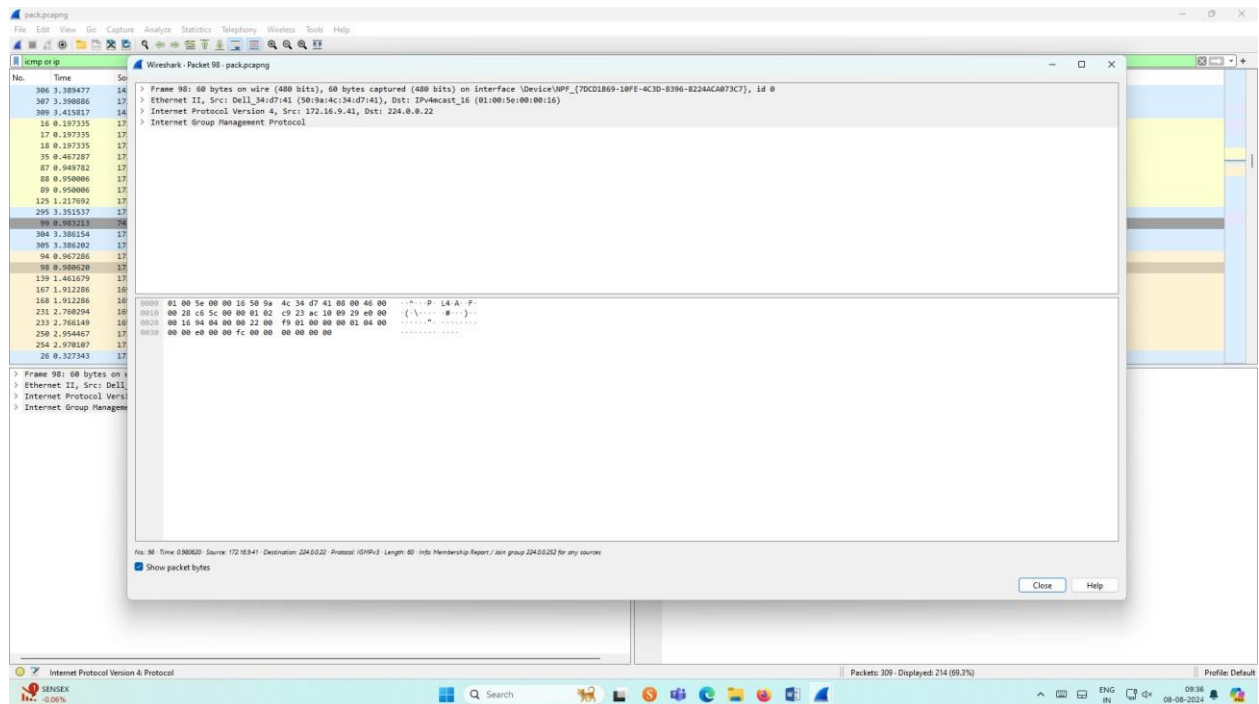
Output



Flow Graph output




Inspecting the packets

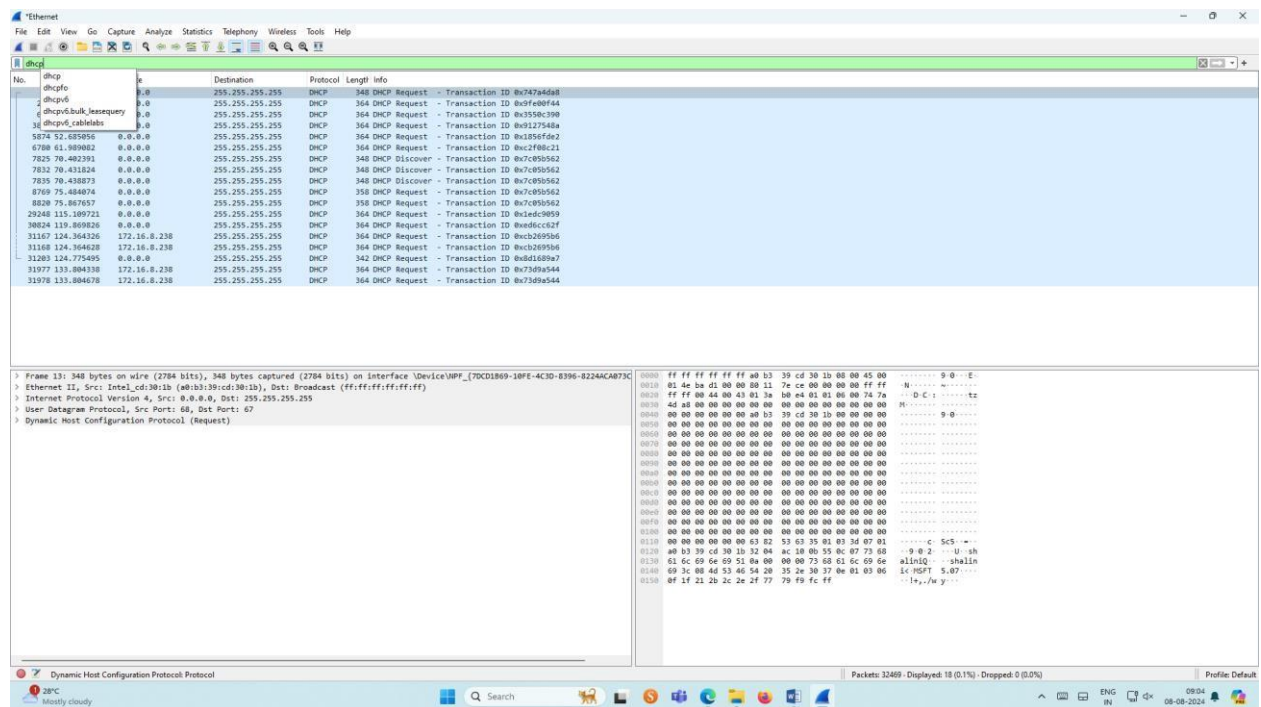


7. Create a Filter to display only DHCP packets and inspect the packets.

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

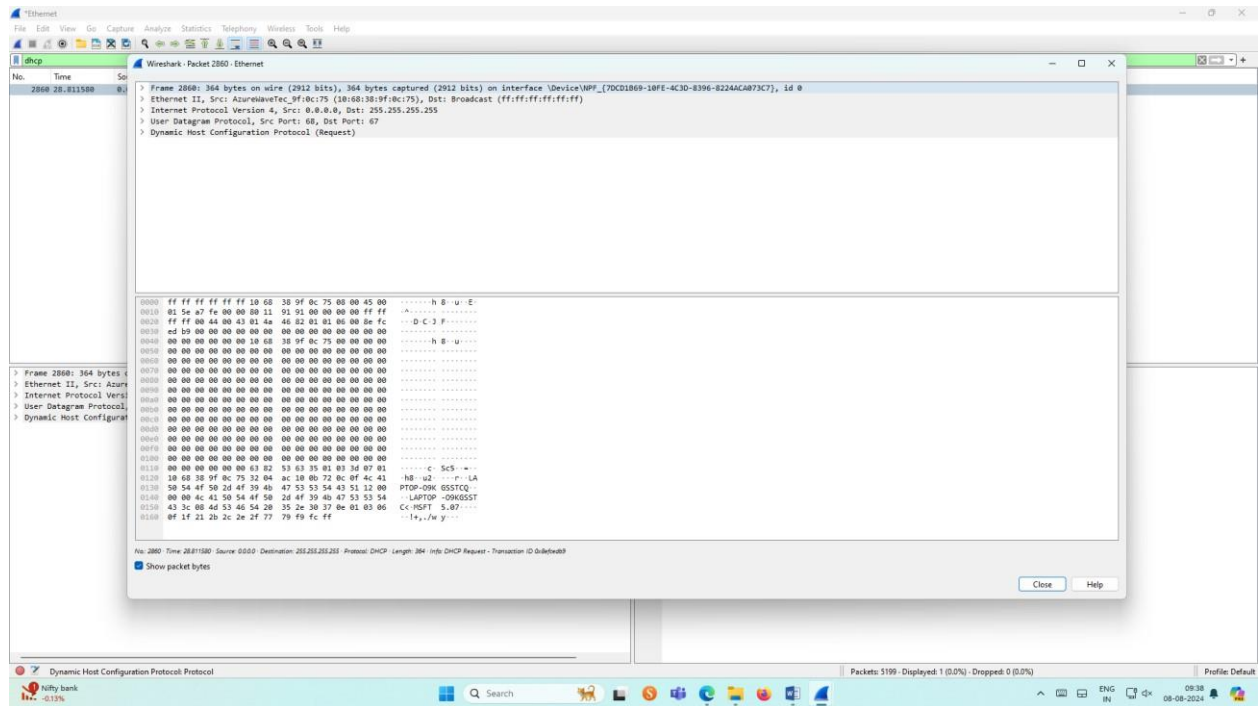


The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, and Tools. The main window is divided into three panes:

- Packet List:** Shows a list of captured packets. The filter bar at the top is set to "dhcp". The list includes packets 1 through 14, all of which are DHCP requests or discoveries. The "Length" column shows the size of each packet in bytes.
- Packet Details:** Shows the hierarchical structure of the selected packet (Packet 13). The layers are: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Dynamic Host Configuration Protocol (Request). The "Dynamic Host Configuration Protocol (Request)" layer is expanded, showing fields like "Transaction ID", "Op", "Xid", "Type", "Length", "Flags", "Magic", "Cookie", "Cookie-Mask", "Server Identifier", "Parameter List", and "Options".
- Packet Bytes:** Shows the raw data of the selected packet in hexadecimal and ASCII. The data is displayed in a hex dump format, with the ASCII representation shown on the right.

The status bar at the bottom indicates that 12489 packets were displayed (0.1%) and 0 packets were dropped (0.0%). The system tray at the bottom shows the date and time as 08-08-2024.

Inspecting the packets



Result:

The filtering, searching and inspecting of packets using wireshark tool has been done successfully.