Ex No: 14 b PACKET SNIFFING USING WIRESHARK
DATE:19.8.24
AIM:

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

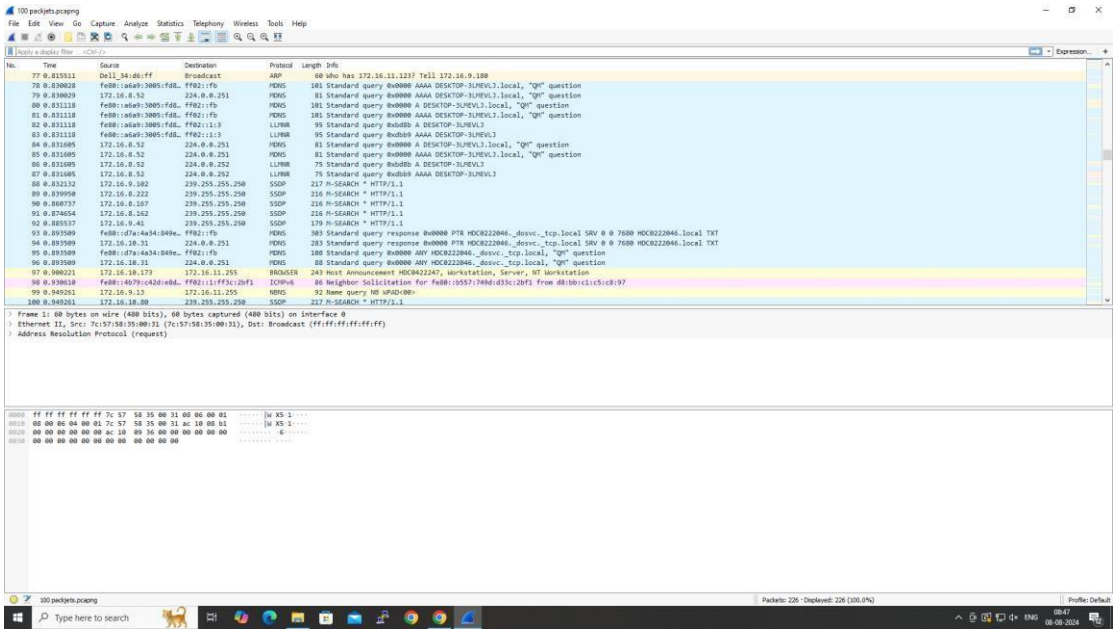
Exercises

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

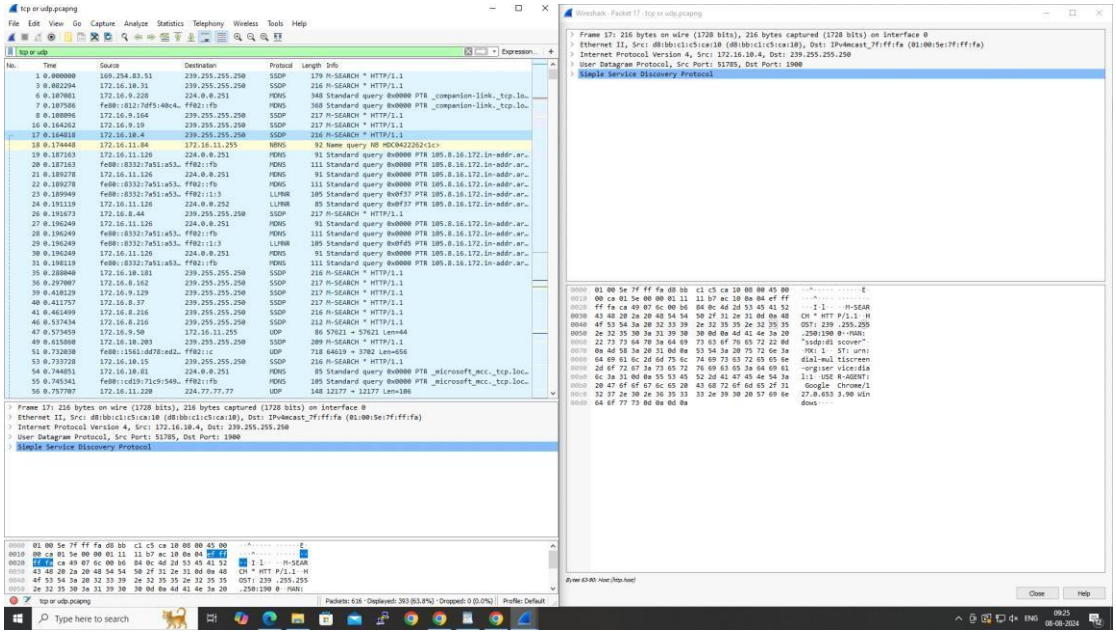


2.Create a Filter to display only TCP/UDP packets, inspect the packets and provide the flow graph.

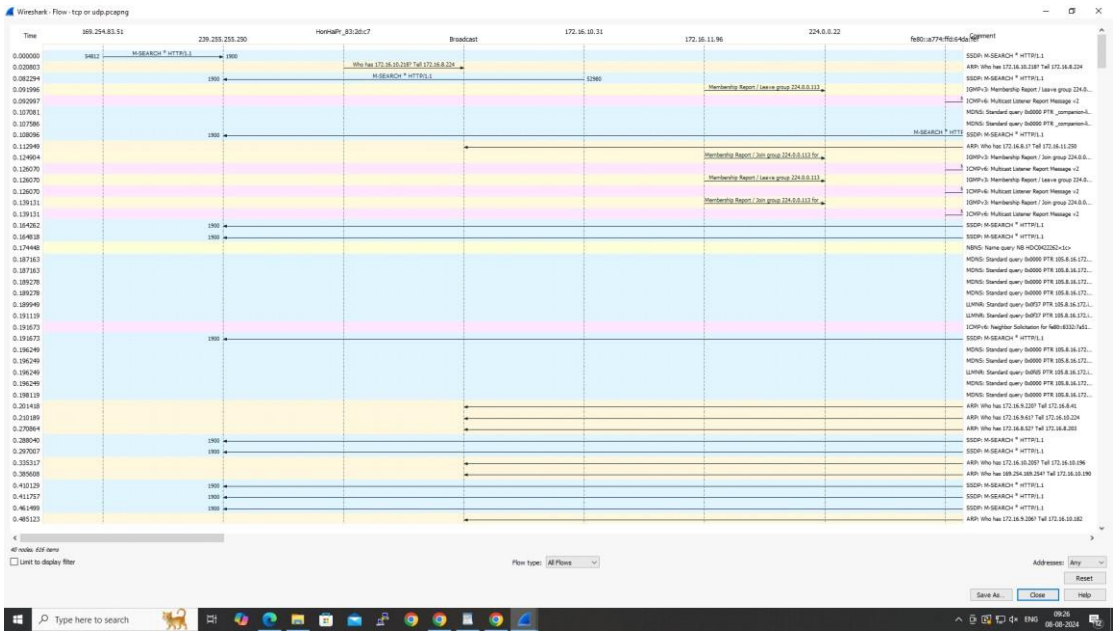
Procedure

- 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:

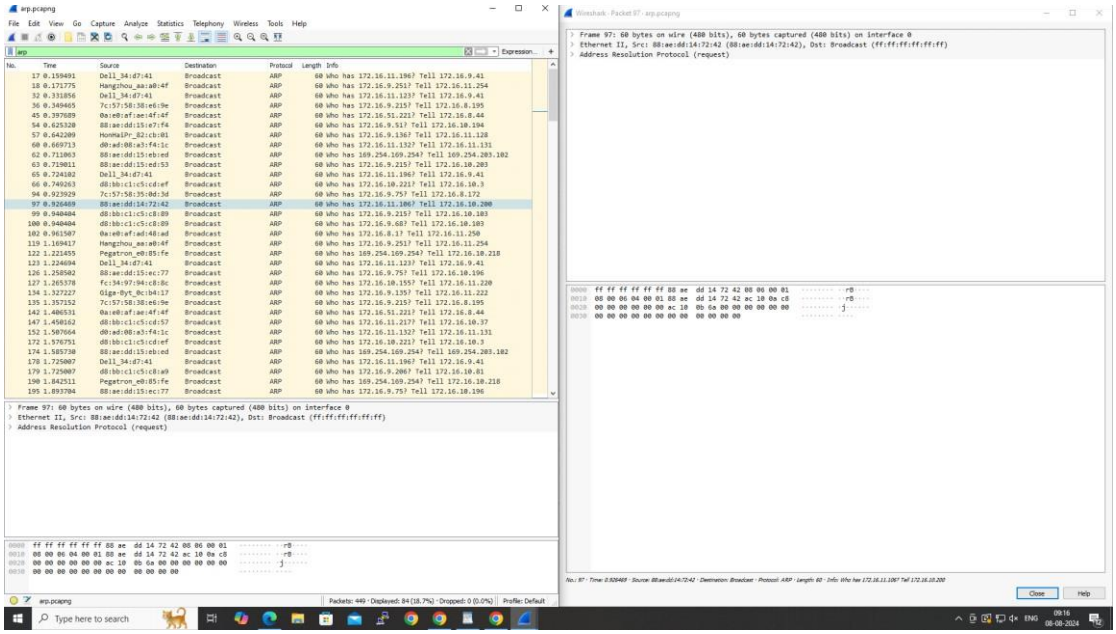


3.Create a Filter to display only ARP packets and inspect the packets.

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

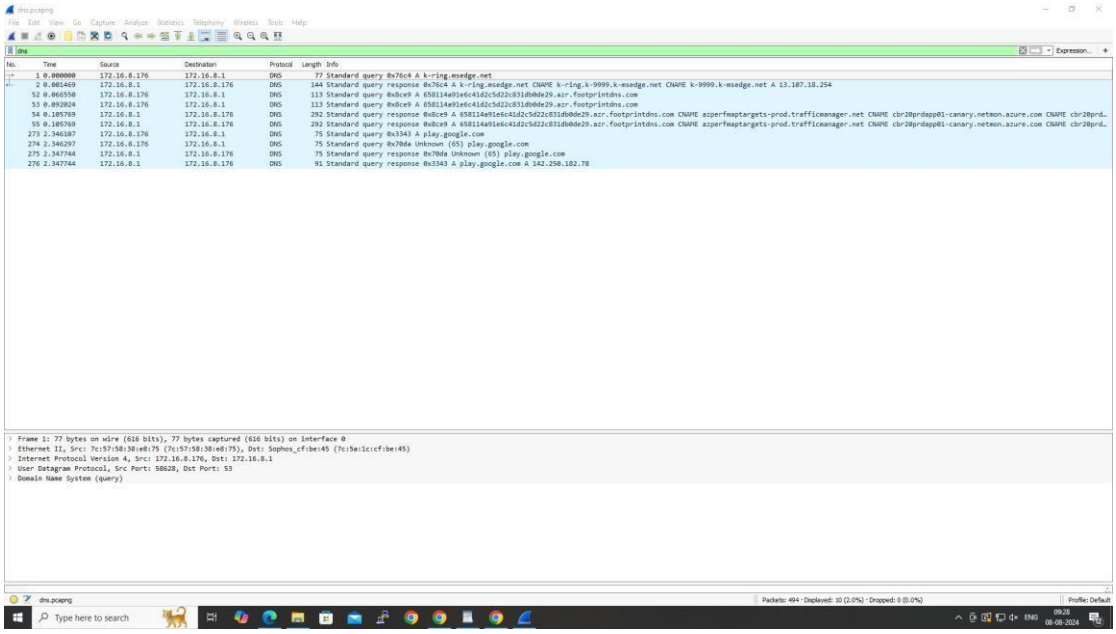


4.Create a Filter to display only DNS packets and provide the flow graph.

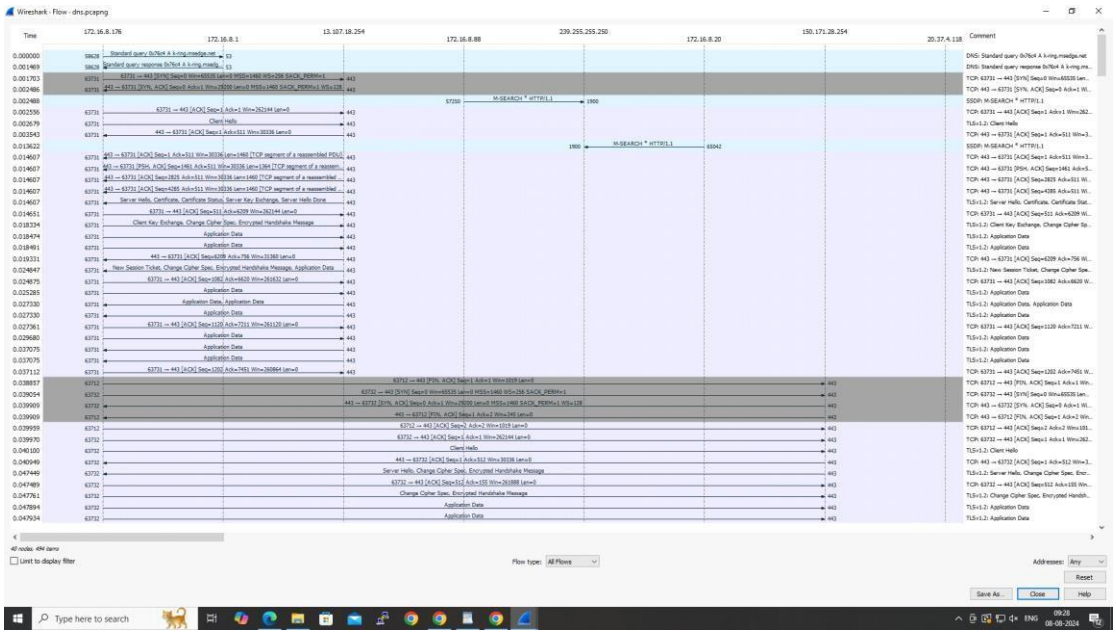
Procedure

- 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



Flow Graph output



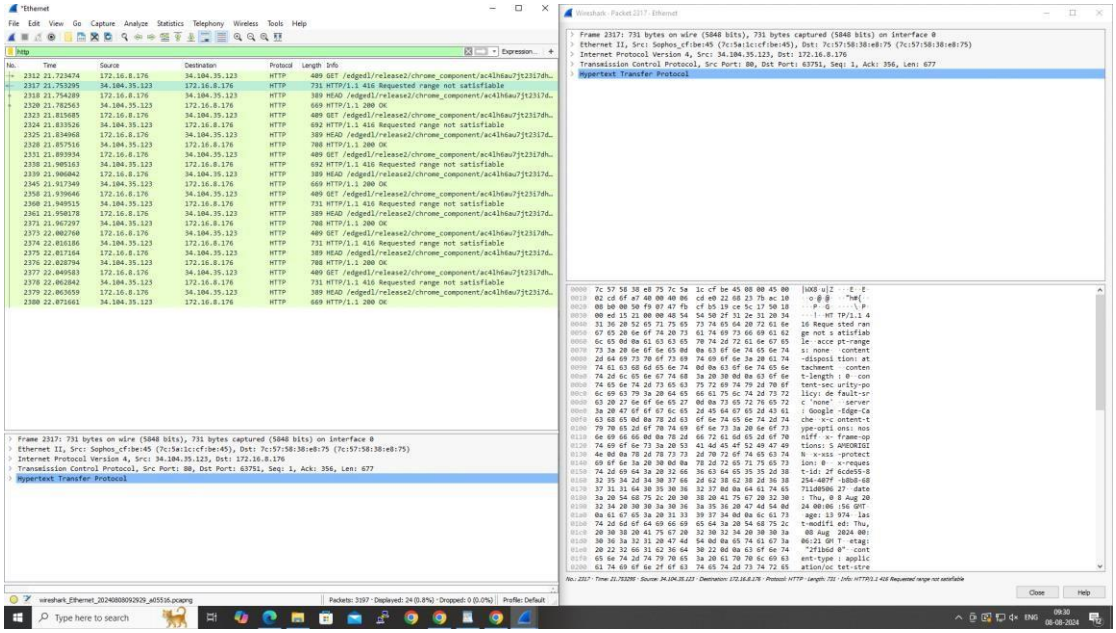
5.Create a Filter to display only HTTP packets and inspect the packets

Procedure

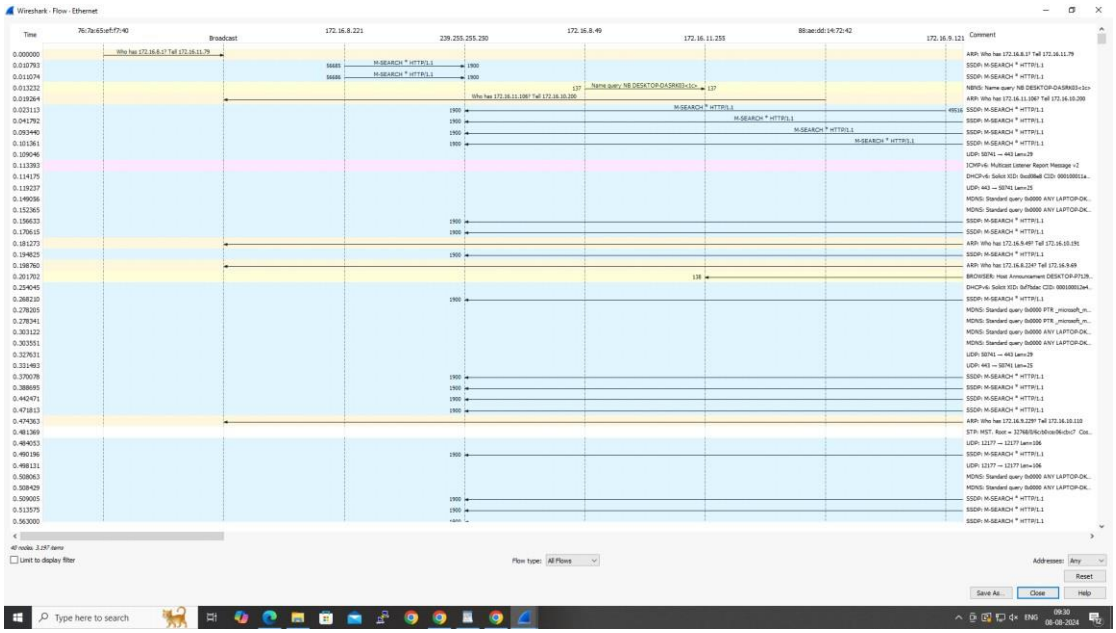
- Select Local Area Connection in Wireshark.

- 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:

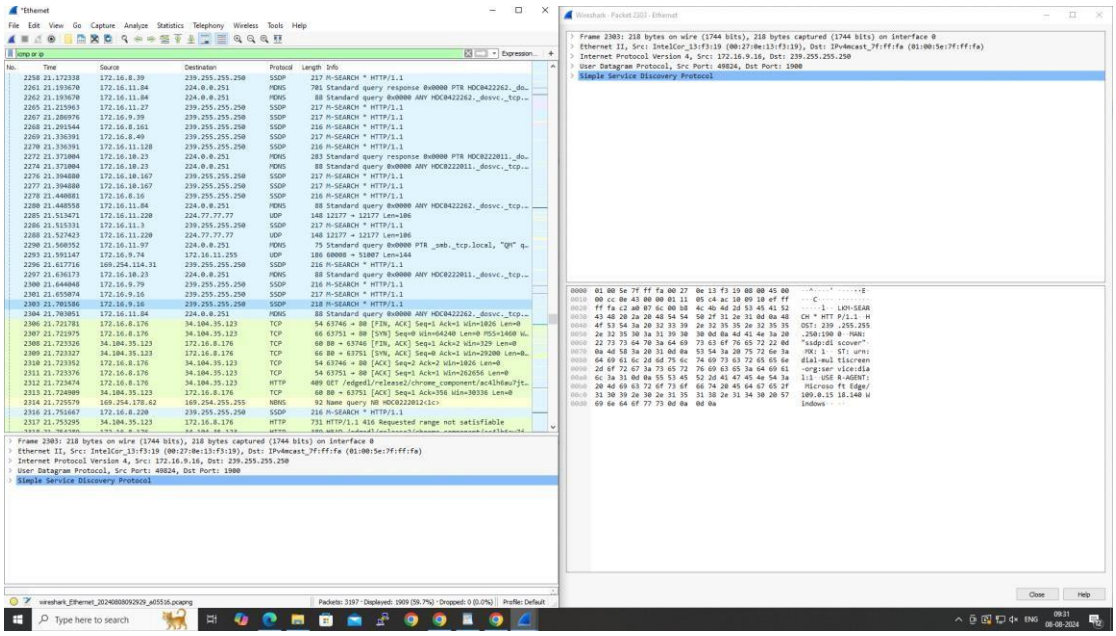


6.Create a Filter to display only IP/ICMP packets and inspect the packets.

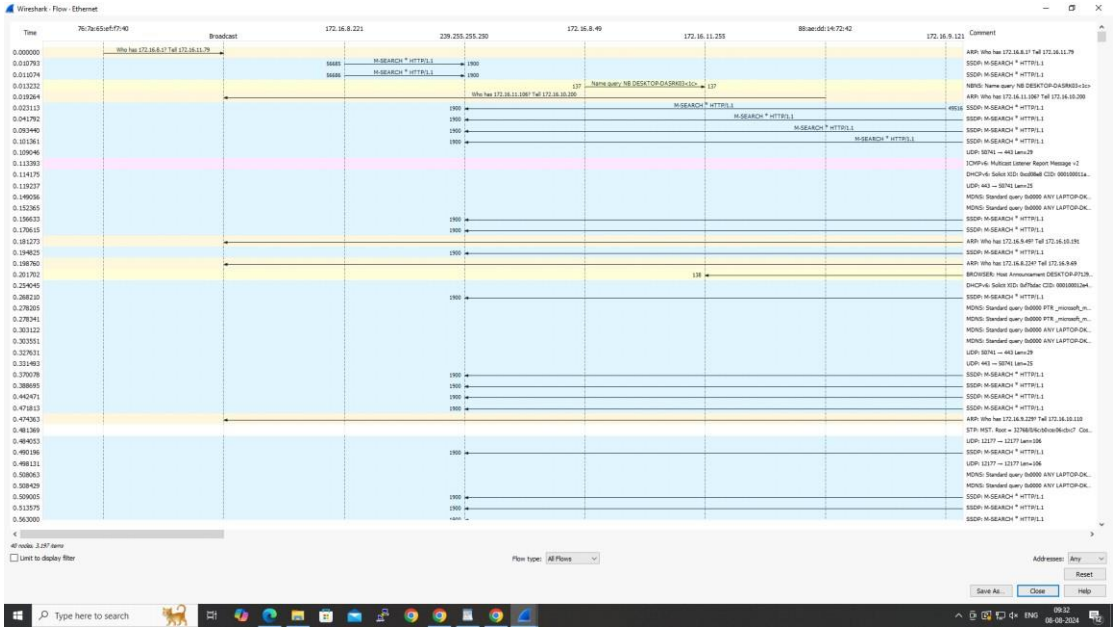
Procedure

- 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:

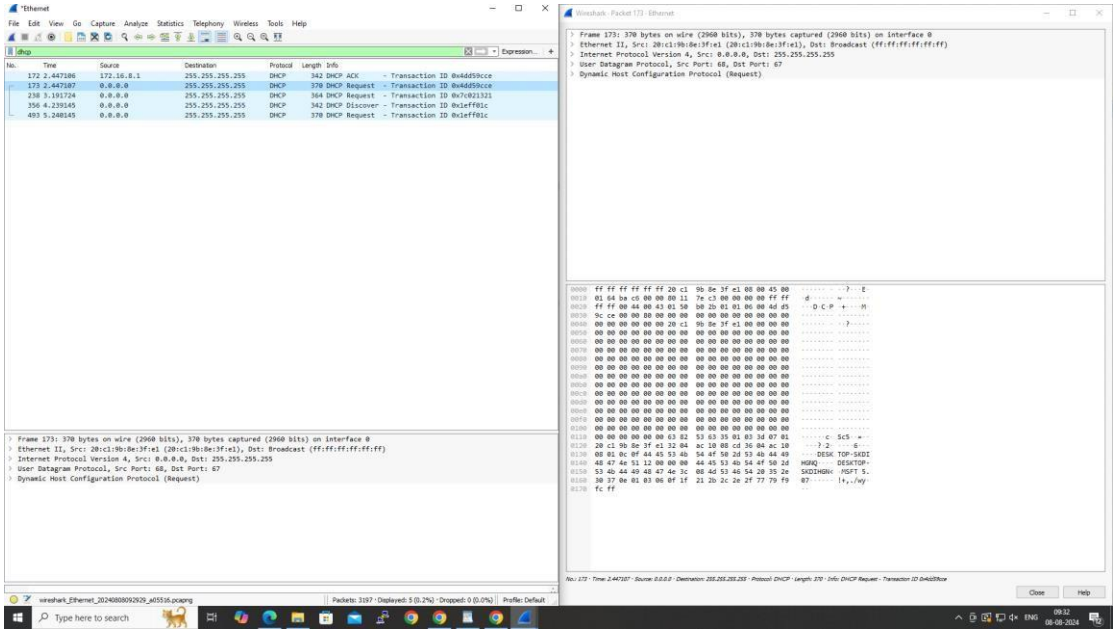


7.Create a Filter to display only DHCP packets and inspect the packets.

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:


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dhcp
Expression...
No. Time Source Destination Protocol Length Info
172 2.447106 172.16.8.1 255.255.255.255 DHCP 342 DHCP ACK - Transaction ID 0x4dd59cce
173 2.447107 0.0.0.0 255.255.255.255 DHCP 370 DHCP Request - Transaction ID 0x4dd59cce
238 3.191724 0.0.0.0 255.255.255.255 DHCP 364 DHCP Request - Transaction ID 0x7c021321
356 4.239145 0.0.0.0 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0x1eff01c
493 5.240145 0.0.0.0 255.255.255.255 DHCP 370 DHCP Request - Transaction ID 0x1eff01c
Frame 173: 370 bytes on wire (2960 bits), 370 bytes captured (2960 bits) on interface 0
Ethernet II, Src: 20:c1:9b:8e:3f:e1 (20:c1:9b:8e:3f:e1), 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)
wireshark_Ethernet_20240808092929_a05516.pcapng
Packets: 3197 · Displayed: 5 (0.2%) · Dropped: 0 (0.0%)
Profile: Default
Wireshark · Packet 173 · Ethernet
Frame 173: 370 bytes on wire (2960 bits), 370 bytes captured (2960 bits) on interface 0
Ethernet II, Src: 20:c1:9b:8e:3f:e1 (20:c1:9b:8e:3f:e1), 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)
No.: 173 · Time: 2.447107 · Source: 0.0.0.0 · Destination: 255.255.255.255 · Protocol: DHCP · Length: 370 · Info: DHCP Request - Transaction ID 0x4dd59cce
Close
Help
Type here to search
ENG
09:32
08-08-2024