Ex No: 4 b

Date:14:8:24 ANALYZE NETWORK TRAFFIC USING WIRESHARK TOOL

AIM:

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

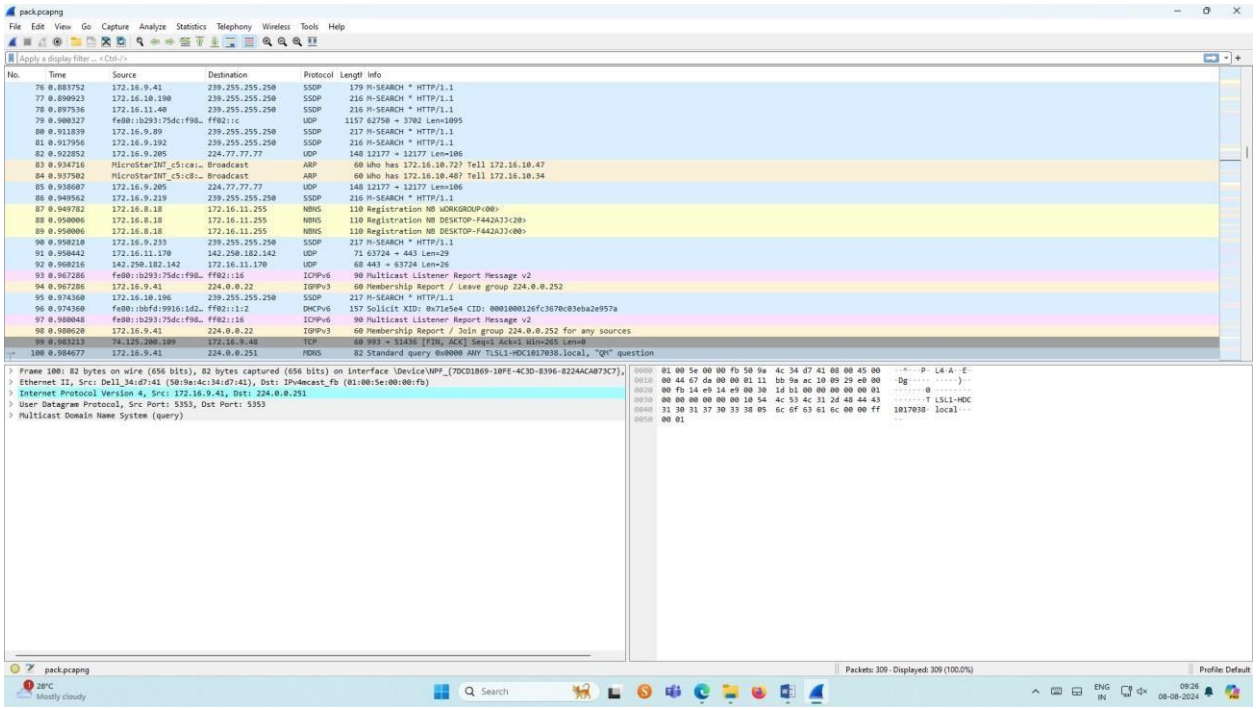
Exercises

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

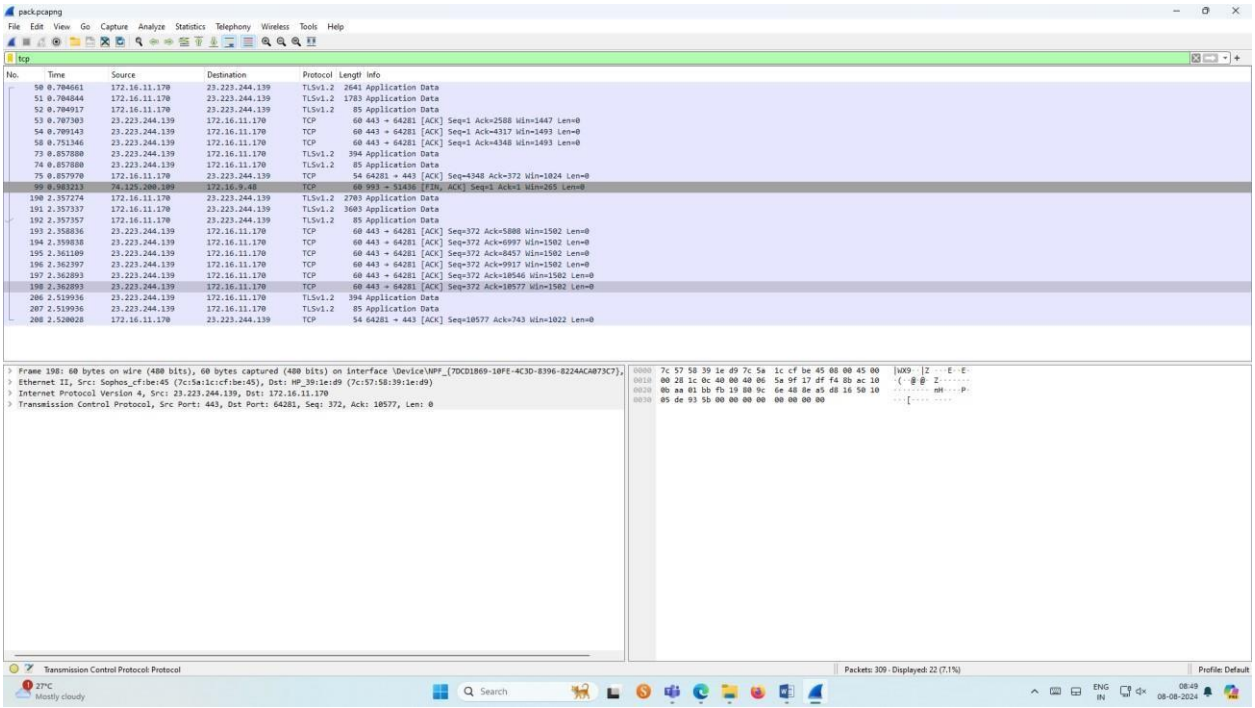


2.Create a Filter to display only TCP/UDP packets, inspect the packets and provide the flow graph.

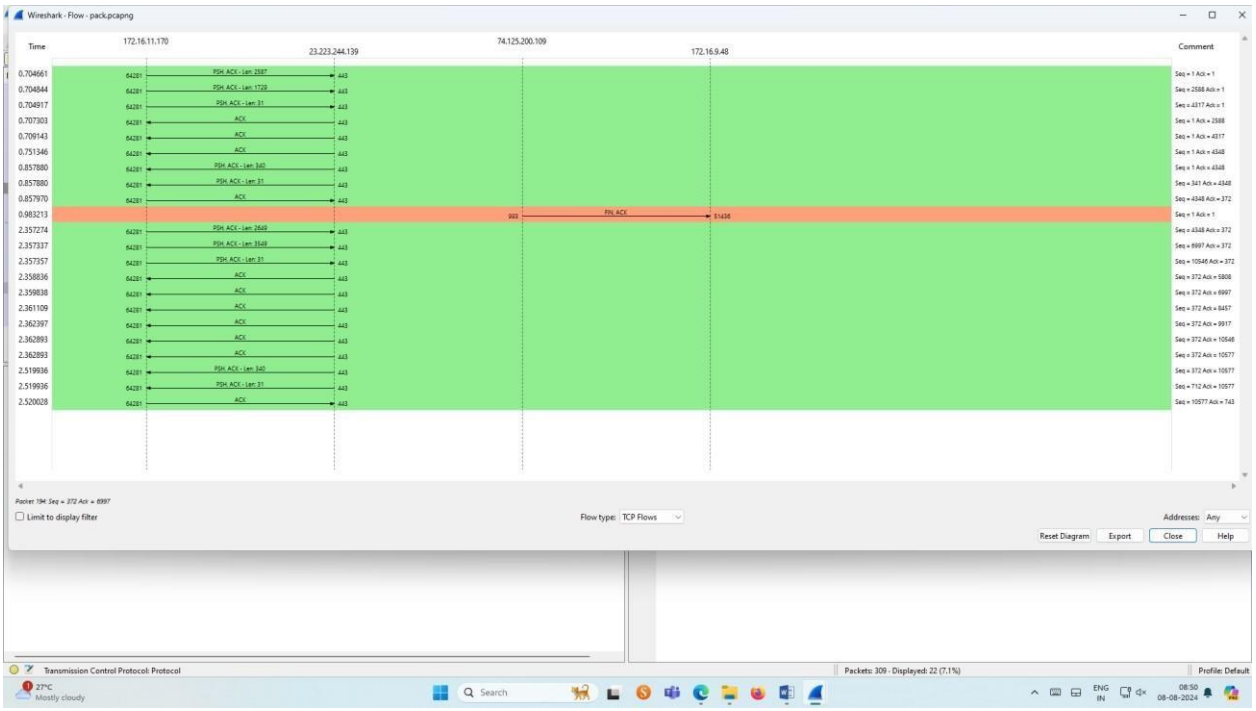
Procedure

- 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

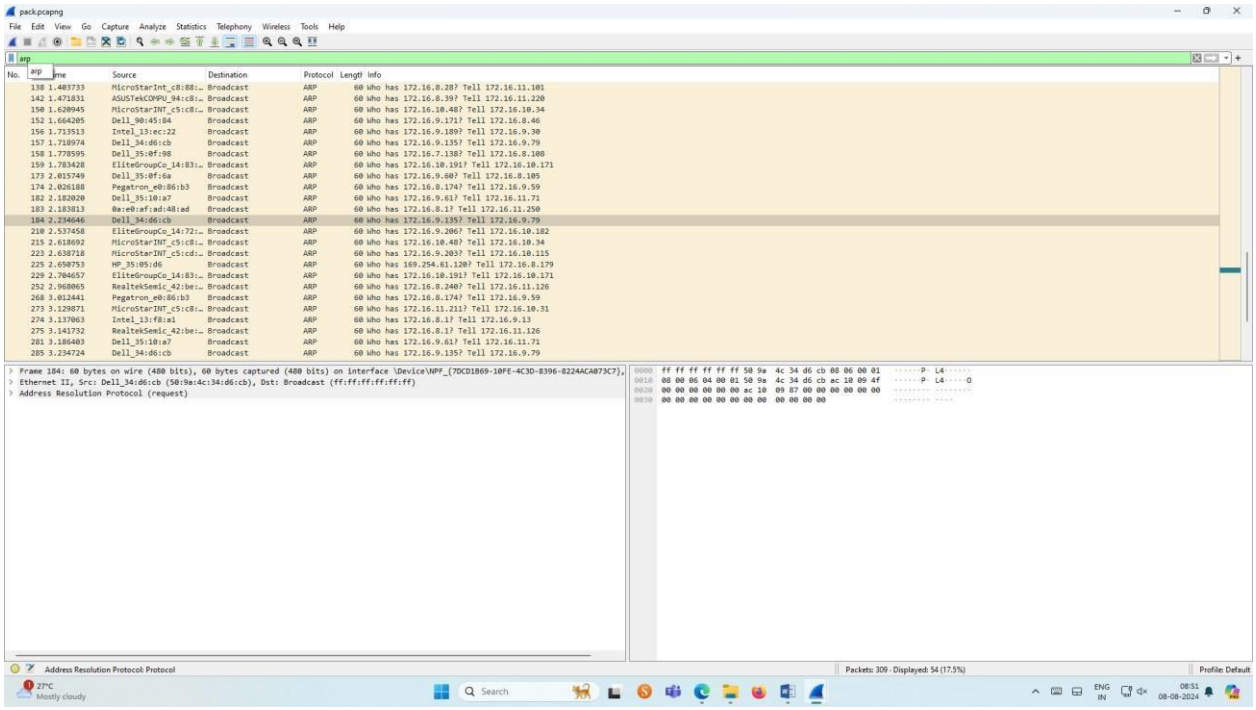


3.Create a Filter to display only ARP packets and inspect the packets.

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



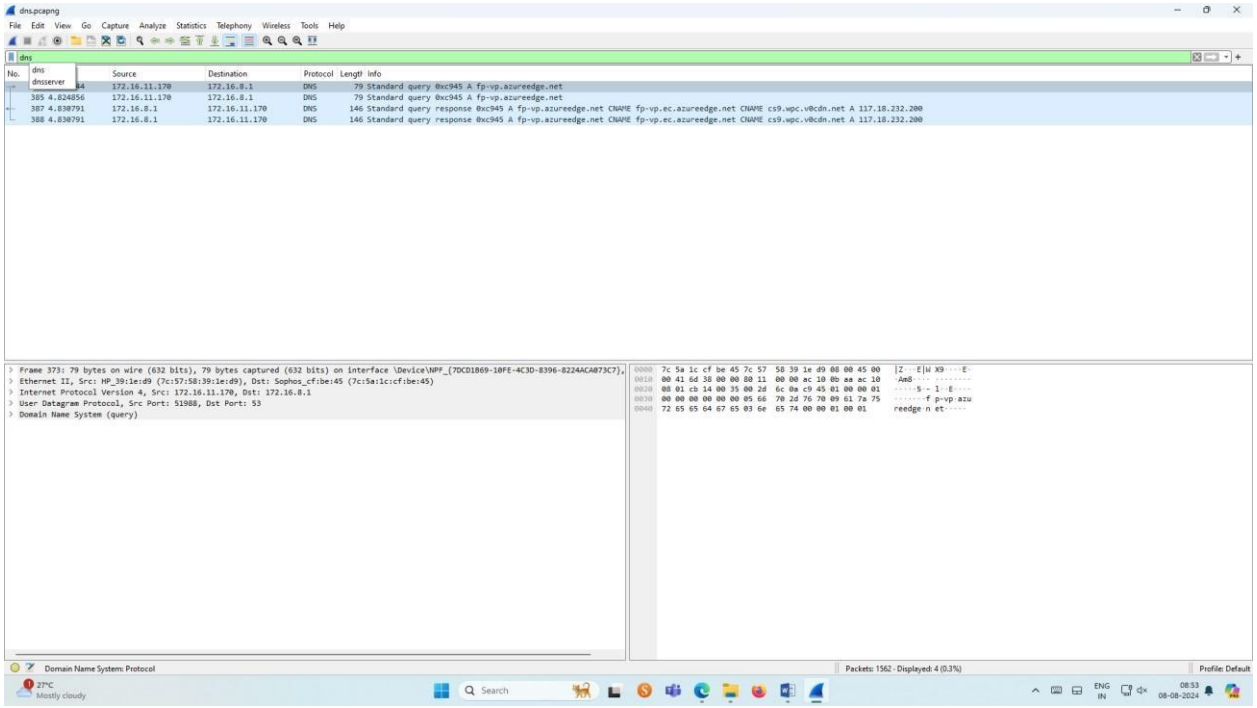
4.Create a Filter to display only DNS packets and provide the flow graph.

Procedure

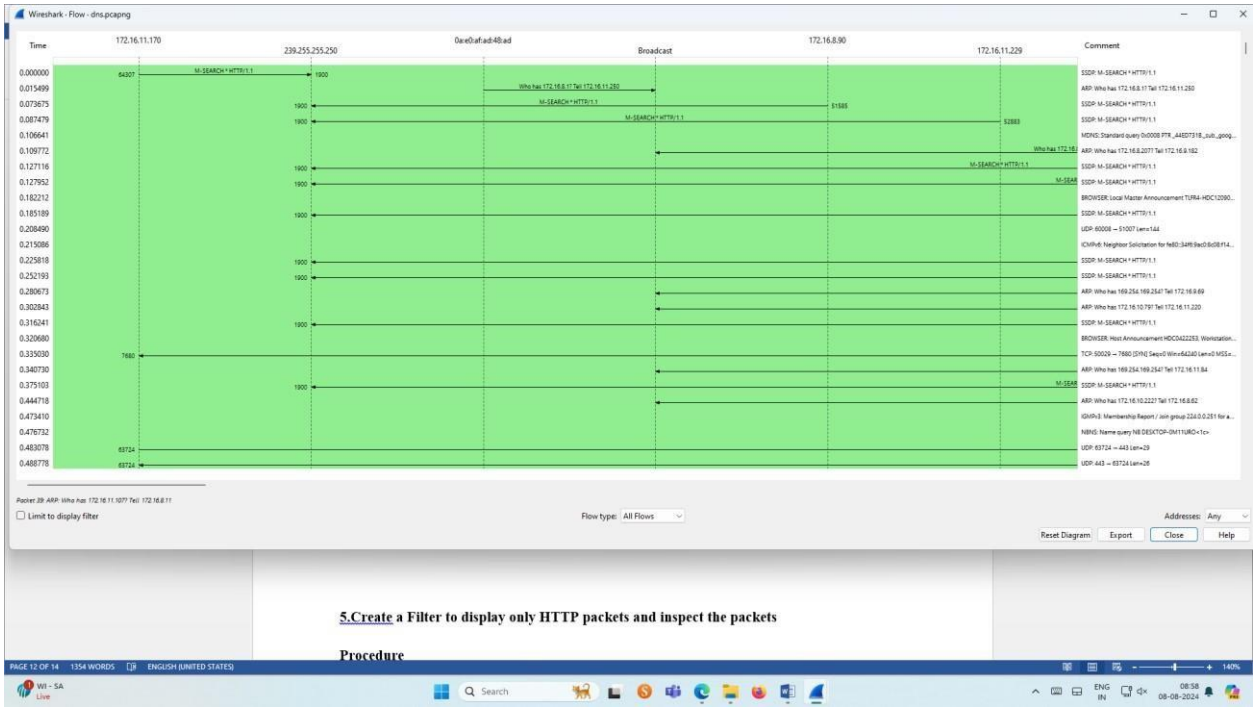
- Select Local Area Connection in Wireshark.
- Go to capture ✇ option
- Select stop capture automatically after 100 packets.

- Then click Start capture.
- Search DNS packets in search bar.
- To see flow graph click Statistics➇Flow graph.
- Save the packets.

Output



Graph output

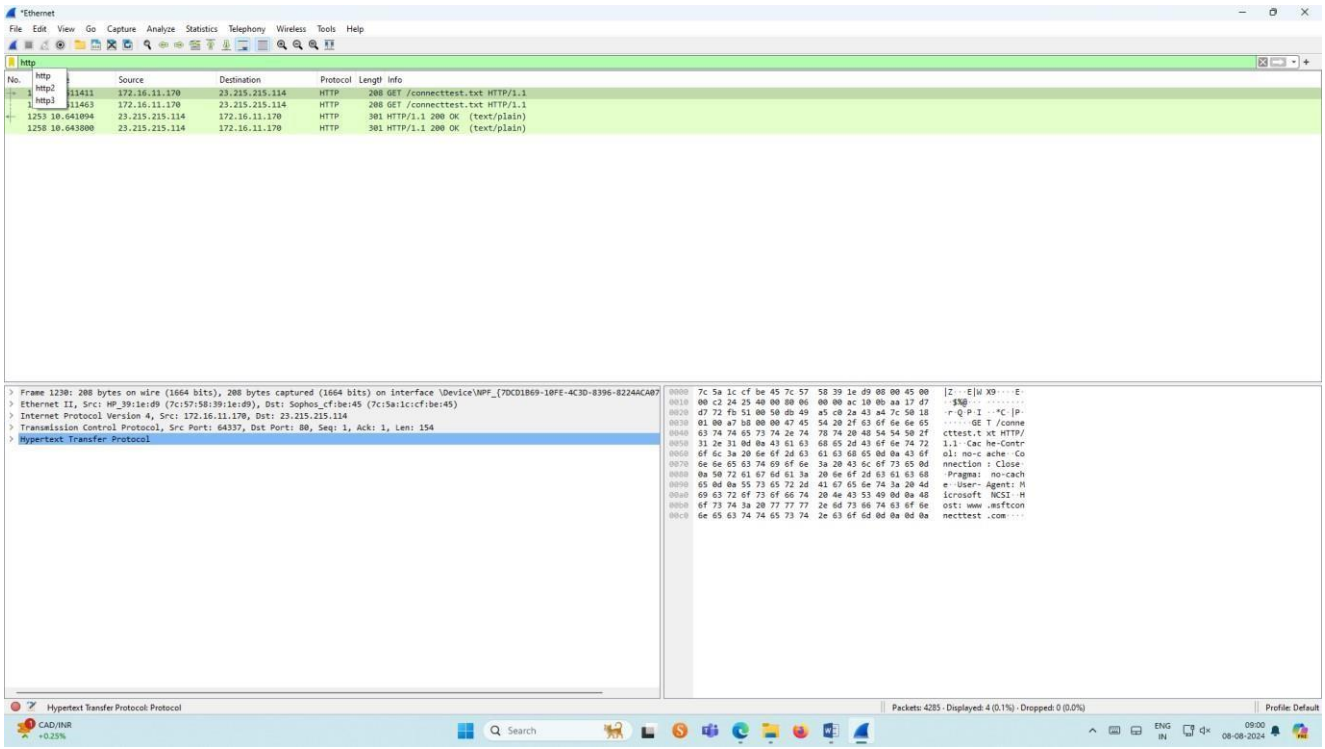


5.Create a Filter to display only HTTP packets and inspect the packets

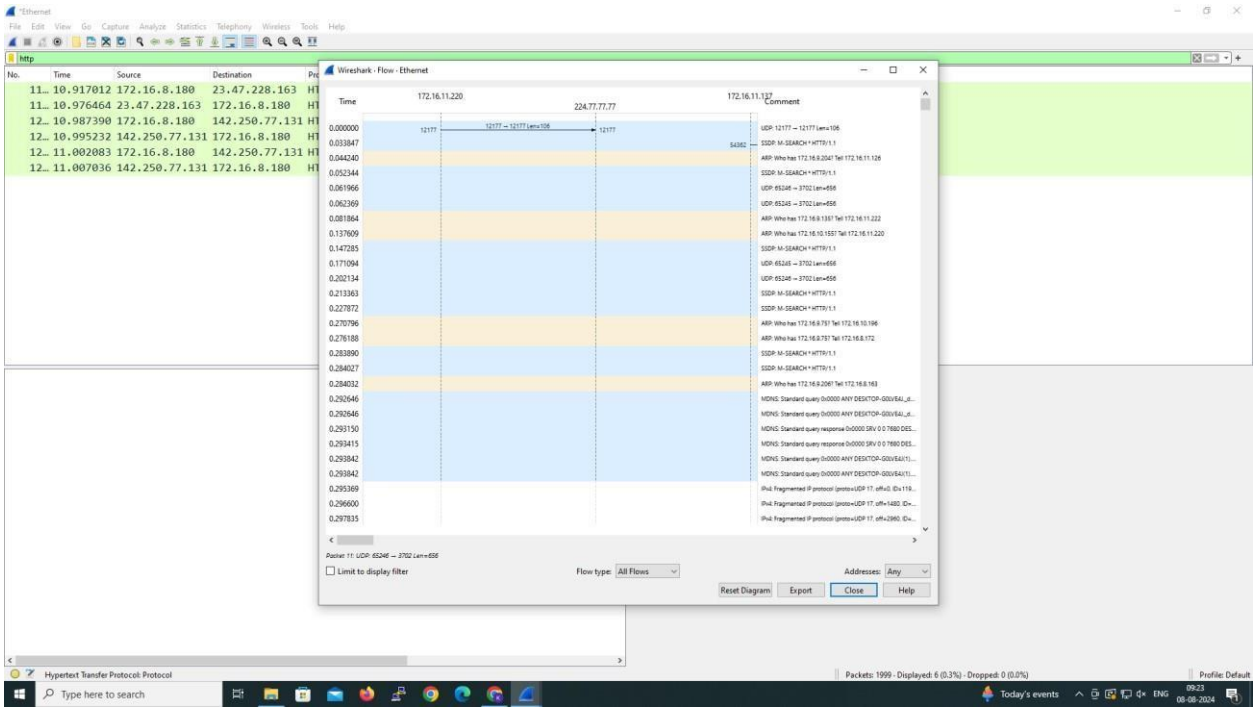
Procedure

- 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


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
http
http2
http3
No. Source Destination Protocol Length Info
172.16.11.170 23.215.215.114 HTTP 208 GET /connecttest.txt HTTP/1.1
172.16.11.170 23.215.215.114 HTTP 208 GET /connecttest.txt HTTP/1.1
1253 10.641094 23.215.215.114 172.16.11.170 HTTP 301 HTTP/1.1 200 OK (text/plain)
1258 10.643800 23.215.215.114 172.16.11.170 HTTP 301 HTTP/1.1 200 OK (text/plain)
Frame 1230: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interface \Device\NPF_{7DCD1B69-10FE-4C3D-8396-8224ACA07
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: 23.215.215.114
Transmission Control Protocol, Src Port: 64337, Dst Port: 80, Seq: 1, Ack: 1, Len: 154
Hypertext Transfer Protocol
Hypertext Transfer Protocol: Protocol
Packets: 4285 · Displayed: 4 (0.1%) · Dropped: 0 (0.0%)
Profile: Default
CAD/INR
+0.25%
Search
ENG
IN
09:00
08-08-2024

Flow Graph output

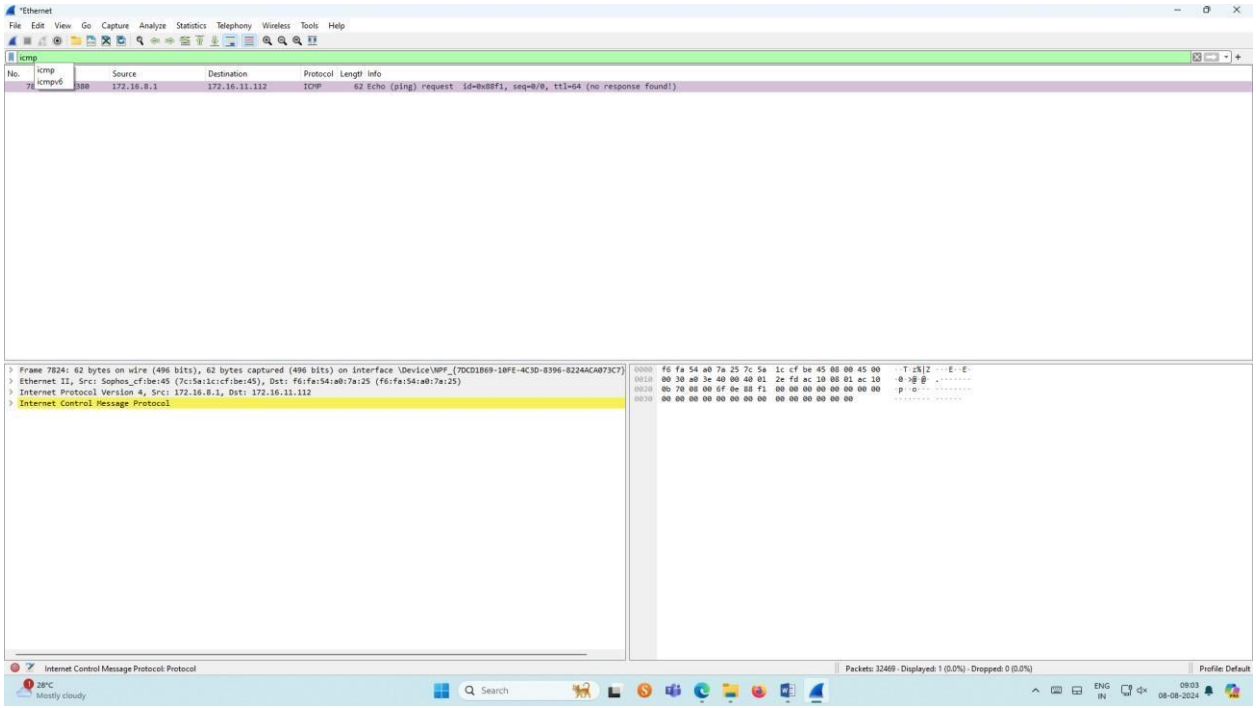


6.Create a Filter to display only IP/ICMP packets and inspect the packets.

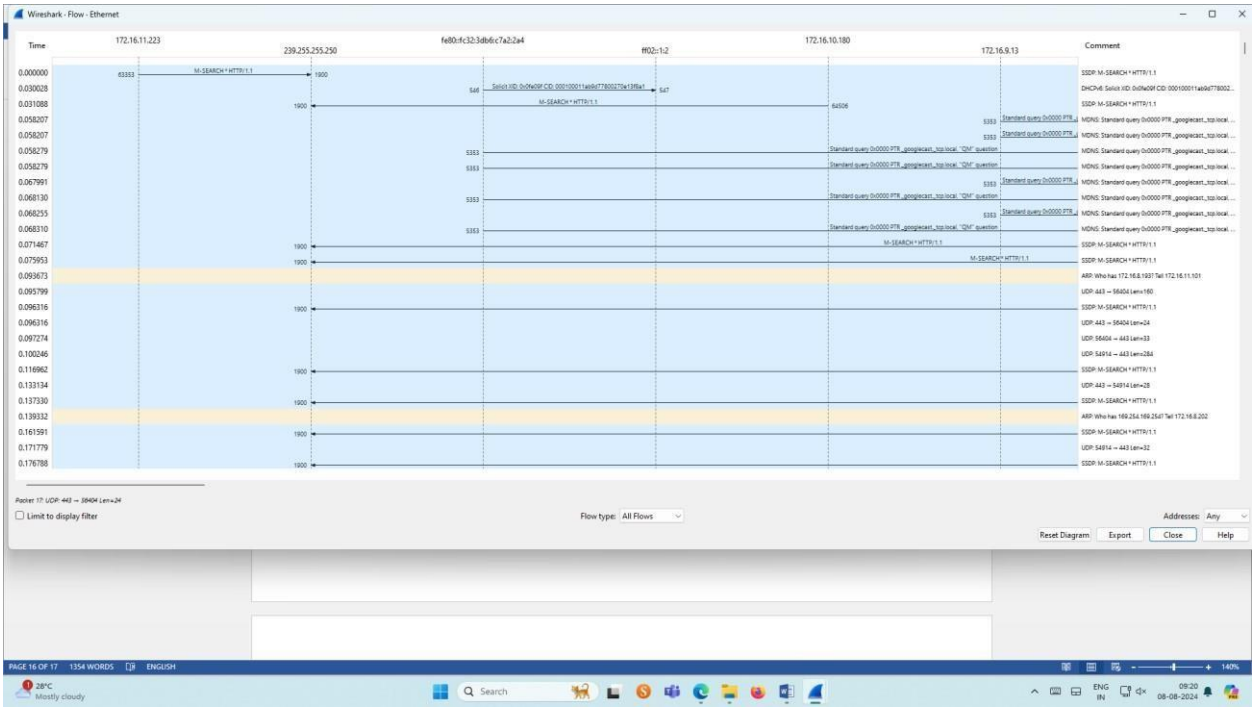
Procedure

- 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
icmp
icmpv6
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
28°C
Mostly cloudy
Search
ENG
IN
09:03
08-08-2024

Flow Graph output

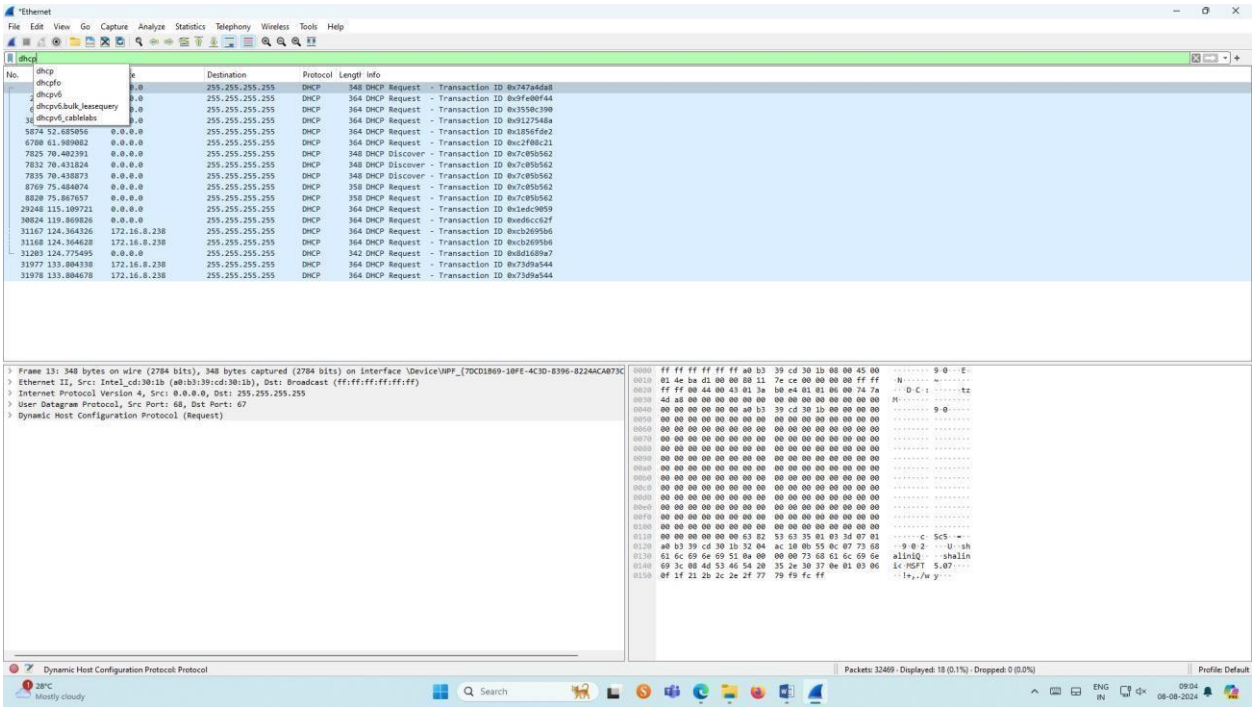


7.Create a Filter to display only DHCP packets and inspect the packets.

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.