

Ex No: 4 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

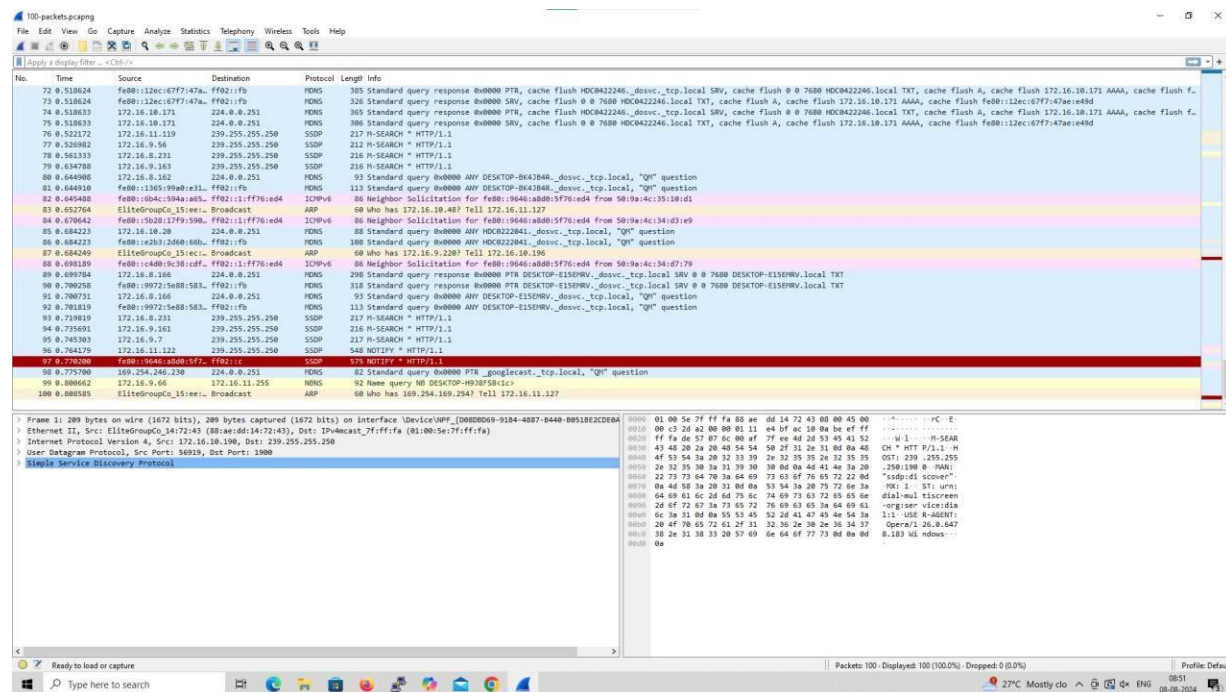
Exercises

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





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

- Packet List:** Shows 100 captured packets. The first few packets are DNS queries and responses. Packet 97 is a DHCP Discover message.
- Packet Details:** Shows the hierarchical structure of the selected packet (Frame 1: 289 bytes on wire). It includes Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Simple Network Management Protocol.
- Packet Bytes:** Shows the raw data of the selected packet in hexadecimal and ASCII.

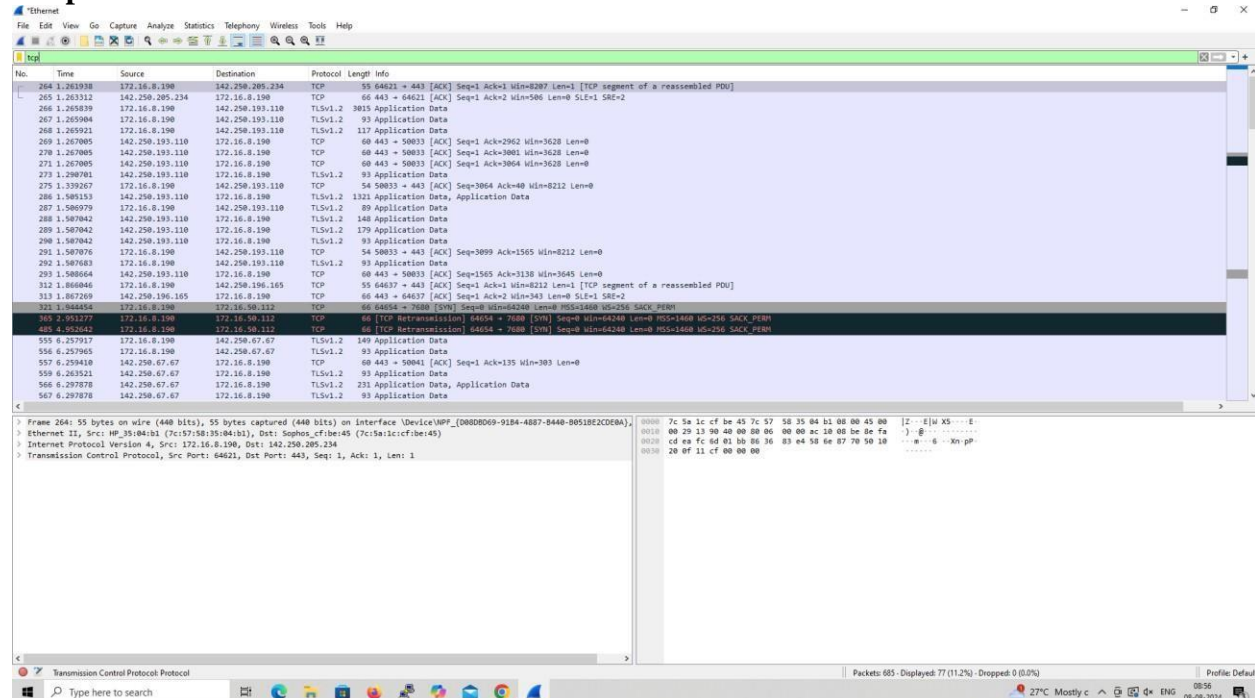
The status bar at the bottom indicates that 100 packets are displayed and 0 are dropped. The system clock shows 08:31 on 08-08-2024.

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:



The image shows a Wireshark packet capture analysis of a UDP stream. The top pane displays a list of packets, with packet 1196 selected. The middle pane shows the packet details for the selected packet, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Data (186 bytes). The bottom pane shows the raw packet data in hexadecimal and ASCII format.

Packet 1196 details:

- Frame 1196: 186 bytes on wire (1488 bits), 186 bytes captured (1488 bits) on interface \Device\NPF_{D080B069-91B4-4887-B440-B051BE2C0A}, id 0
- Ethernet II, Src: ASUSTekCPU_e2:ee:ab (20:7b:d2:e2:ee:ab), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 172.16.9.205, Dst: 172.16.11.255
- User Datagram Protocol, Src Port: 60008, Dst Port: 51007
- Data (144 bytes)

Raw packet data (hex):

```
0000 ff ff ff ff ff ff 20 7b d2 e2 ee ab 08 00 45 00 .....f.....E
0010 80 ac 58 1c 00 00 74 ab ac 10 09 4a ac 10 ....X.....t...
0020 0b ff ea 68 c7 3f 00 98 f3 cc 4a b5 7f e5 21 43 ...h?.....IC
0030 bd f3 2d 9e da ff f9 b6 b3 37 0a 18 c3 30 e2 91 .....7.....
0040 86 88 24 65 99 2c 29 6c 00 4b 10 19 83 16 c2 2b ...$e...lK...+
0050 22 c2 a1 a6 f6 32 42 e8 1a cf 22 da 07 cc 60 75 ...2B.....u
0060 53 7d 25 a5 3e aa 85 7f db 31 d7 a3 2e cd 60 9b ...S%>...1...
0070 3d 1f 12 0c 73 87 30 25 0c ca f9 0d 6c 84 92 fc ...s%0%.....
0080 6b 19 e2 ba be aa 37 7f d2 02 c9 01 4e c3 80 k...7X.....N
0090 9e 01 96 f2 ff a1 05 9b 9c 67 17 de c2 20 ed 95 .....g...c
00a0 29 15 a1 cb 99 3e 1a 4f 68 12 70 0f 43 d5 b0 fb )A->O h p C...
00b0 46 02 78 94 8e 9c d6 bc ba 66 F-x.....f
```

The image shows a Wireshark packet capture analysis of a UDP stream. The top pane displays a list of packets, with packet 1196 selected. The middle pane shows the packet details for the selected packet, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Data (144 bytes). The bottom pane shows the raw packet data in hexadecimal and ASCII format.

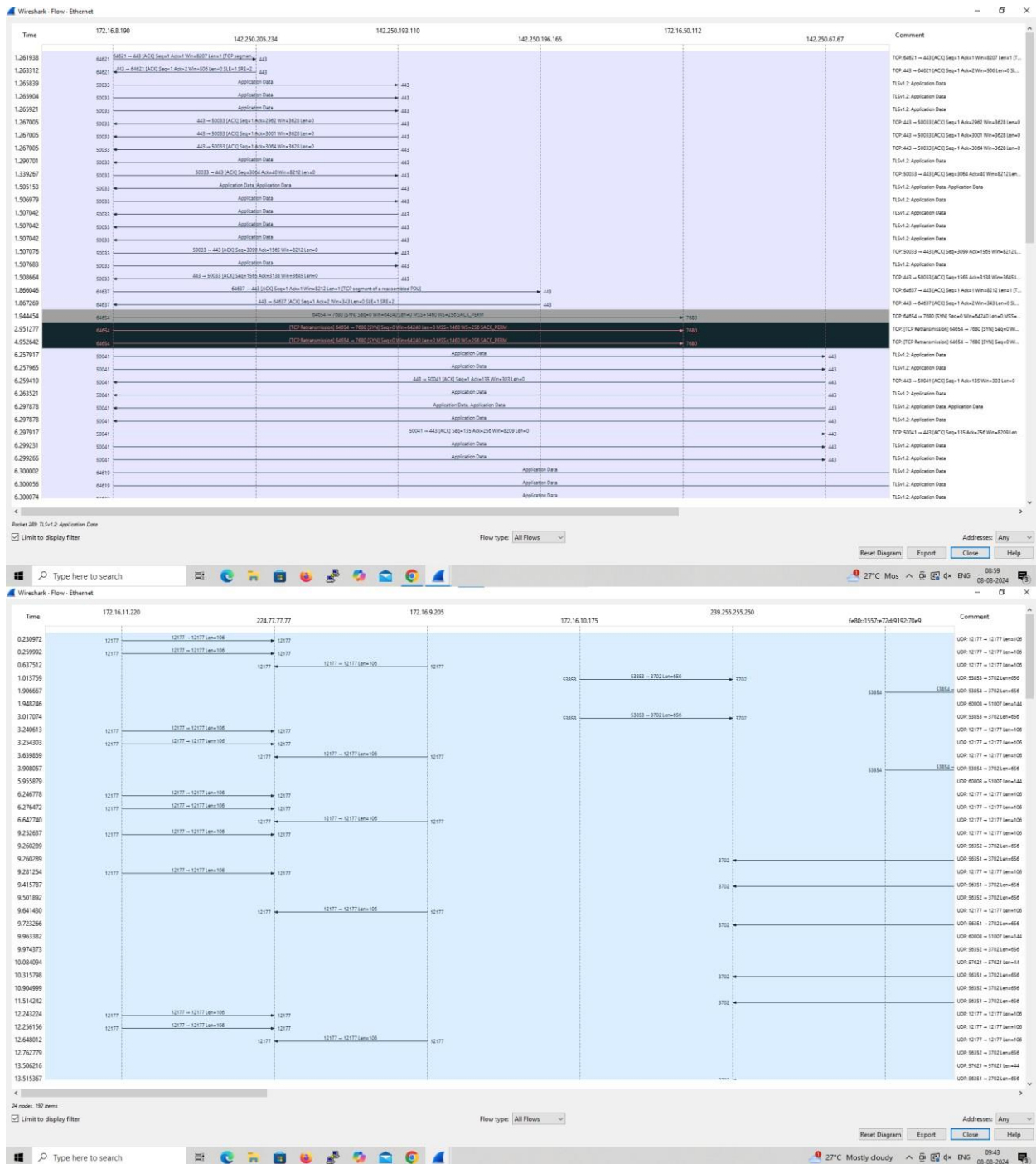
Packet 1196 details:

- Frame 1196: 186 bytes on wire (1488 bits), 186 bytes captured (1488 bits) on interface \Device\NPF_{D080B069-91B4-4887-B440-B051BE2C0A}, id 0
- Ethernet II, Src: ASUSTekCPU_e2:ee:ab (20:7b:d2:e2:ee:ab), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 172.16.9.205, Dst: 172.16.11.255
- User Datagram Protocol, Src Port: 60008, Dst Port: 51007
- Data (144 bytes)

Raw packet data (hex):


```
0000 ff ff ff ff ff ff 20 7b d2 e2 ee ab 08 00 45 00 .....f.....E
0010 80 ac 58 1c 00 00 74 ab ac 10 09 4a ac 10 ....X.....t...
0020 0b ff ea 68 c7 3f 00 98 f3 cc 4a b5 7f e5 21 43 ...h?.....IC
0030 bd f3 2d 9e da ff f9 b6 b3 37 0a 18 c3 30 e2 91 .....7.....
0040 86 88 24 65 99 2c 29 6c 00 4b 10 19 83 16 c2 2b ...$e...lK...+
0050 22 c2 a1 a6 f6 32 42 e8 1a cf 22 da 07 cc 60 75 ...2B.....u
0060 53 7d 25 a5 3e aa 85 7f db 31 d7 a3 2e cd 60 9b ...S%>...1...
0070 3d 1f 12 0c 73 87 30 25 0c ca f9 0d 6c 84 92 fc ...s%0%.....
0080 6b 19 e2 ba be aa 37 7f d2 02 c9 01 4e c3 80 k...7X.....N
0090 9e 01 96 f2 ff a1 05 9b 9c 67 17 de c2 20 ed 95 .....g...c
00a0 29 15 a1 cb 99 3e 1a 4f 68 12 70 0f 43 d5 b0 fb )A->O h p C...
00b0 46 02 78 94 8e 9c d6 bc ba 66 F-x.....f
```

Flow Graph output

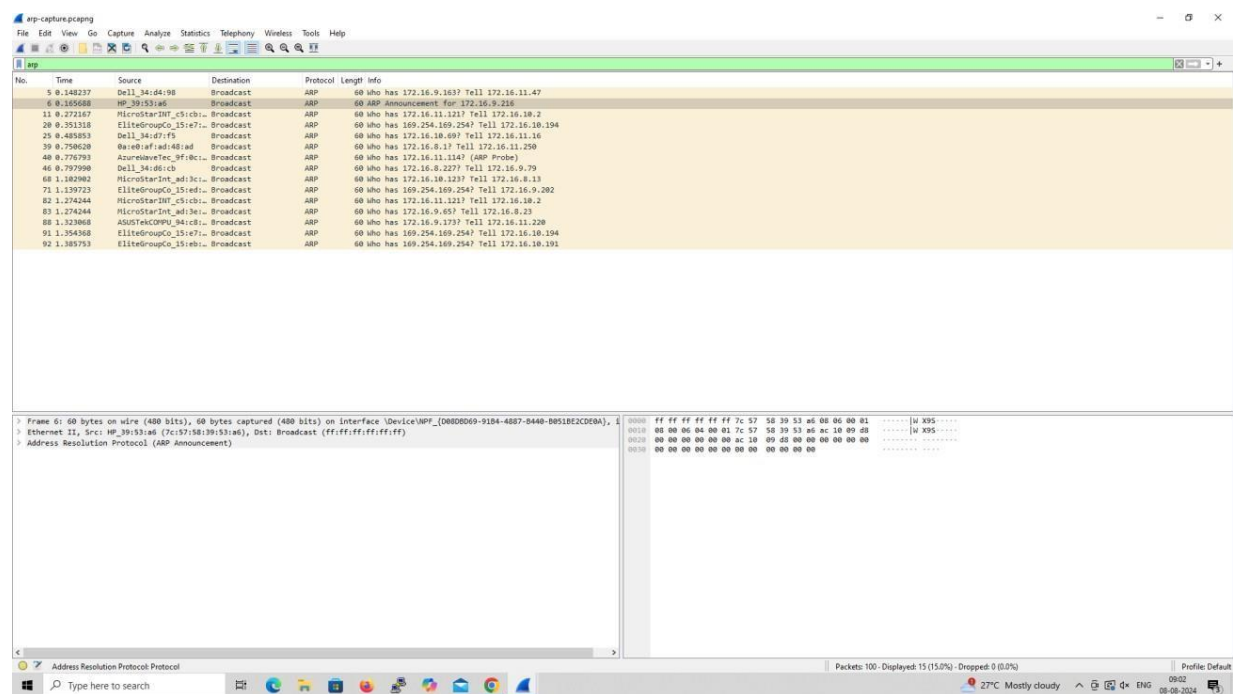


3. Create a Filter to display only ARP packets and inspect the packets.

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

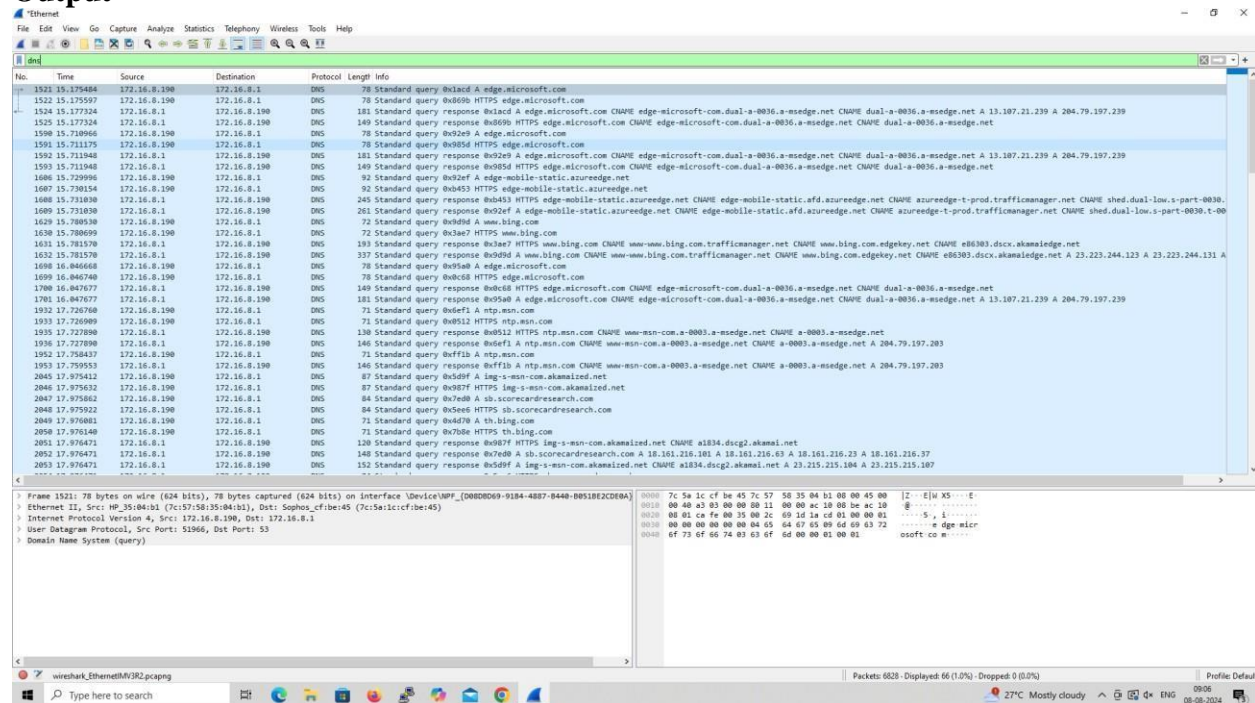


4. Create a Filter to display only DNS packets and provide the flow graph.

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



Weschak - Flow - Ethernet

Time	Source IP	Destination IP	Comment
18.175404	Standard query 0-1e4d A edge.microsoft.com	53	DNS: Standard query 0-1e4d A edge.microsoft.com
18.175997	Standard query 0-b086 HTTP/1.5 edge.microsoft.com	53	DNS: Standard query 0-b086 HTTP/1.5 edge.microsoft.com
18.177324	Standard query response 0-1e4d A edge.microsoft.com	53	DNS: Standard query response 0-1e4d A edge.microsoft.com
18.177324	Standard query response 0-b086 HTTP/1.5 edge.microsoft.com	53	DNS: Standard query response 0-b086 HTTP/1.5 edge.microsoft.com
18.177966	Standard query 0-1e4d A edge.microsoft.com	53	DNS: Standard query 0-1e4d A edge.microsoft.com
18.171175	Standard query 0-b086 HTTP/1.5 edge.microsoft.com	53	DNS: Standard query 0-b086 HTTP/1.5 edge.microsoft.com
18.171948	Standard query response 0-1e4d A edge.microsoft.com	53	DNS: Standard query response 0-1e4d A edge.microsoft.com
18.171948	Standard query response 0-b086 HTTP/1.5 edge.microsoft.com	53	DNS: Standard query response 0-b086 HTTP/1.5 edge.microsoft.com
18.172996	Standard query 0-1e4d A edge-mobile.static.edgekey.net	53	DNS: Standard query 0-1e4d A edge-mobile.static.edgekey.net
18.173014	Standard query 0-b086 HTTP/1.5 edge-mobile.static.edgekey.net	53	DNS: Standard query 0-b086 HTTP/1.5 edge-mobile.static.edgekey.net
18.173103	Standard query response 0-b086 HTTP/1.5 edge-mobile.static.edgekey.net	53	DNS: Standard query response 0-b086 HTTP/1.5 edge-mobile.static.edgekey.net
18.173103	Standard query response 0-1e4d A edge-mobile.static.edgekey.net	53	DNS: Standard query response 0-1e4d A edge-mobile.static.edgekey.net
18.176050	Standard query 0-b086 A www.bing.com	53	DNS: Standard query 0-b086 A www.bing.com
18.176099	Standard query 0-1e4d HTTP/1.5 www.bing.com	53	DNS: Standard query 0-1e4d HTTP/1.5 www.bing.com
18.176150	Standard query response 0-1e4d HTTP/1.5 www.bing.com	53	DNS: Standard query response 0-1e4d HTTP/1.5 www.bing.com
18.176150	Standard query response 0-b086 A www.bing.com	53	DNS: Standard query response 0-b086 A www.bing.com
18.046668	Standard query 0-b086 A edge.microsoft.com	53	DNS: Standard query 0-b086 A edge.microsoft.com
18.046740	Standard query 0-b086 HTTP/1.5 edge.microsoft.com	53	DNS: Standard query 0-b086 HTTP/1.5 edge.microsoft.com
18.047677	Standard query response 0-b086 HTTP/1.5 edge.microsoft.com	53	DNS: Standard query response 0-b086 HTTP/1.5 edge.microsoft.com
18.047677	Standard query response 0-1e4d A edge.microsoft.com	53	DNS: Standard query response 0-1e4d A edge.microsoft.com
17.726760	Standard query 0-b086 A img.msn.com	53	DNS: Standard query 0-b086 A img.msn.com
17.726909	Standard query 0-b086 HTTP/1.5 img.msn.com	53	DNS: Standard query 0-b086 HTTP/1.5 img.msn.com
17.727890	Standard query response 0-b086 HTTP/1.5 img.msn.com	53	DNS: Standard query response 0-b086 HTTP/1.5 img.msn.com
17.727890	Standard query response 0-1e4d A img.msn.com	53	DNS: Standard query response 0-1e4d A img.msn.com
17.758437	Standard query 0-b086 A img.msn.com	53	DNS: Standard query 0-b086 A img.msn.com
17.759553	Standard query response 0-b086 A img.msn.com	53	DNS: Standard query response 0-b086 A img.msn.com
17.975412	Standard query 0-b086 A img-m-msn-com.alicdn.com	53	DNS: Standard query 0-b086 A img-m-msn-com.alicdn.com
17.975632	Standard query 0-b086 HTTP/1.5 img-m-msn-com.alicdn.com	53	DNS: Standard query 0-b086 HTTP/1.5 img-m-msn-com.alicdn.com
17.975862	Standard query 0-1e4d A js.cdnresearch.com	53	DNS: Standard query 0-1e4d A js.cdnresearch.com
17.975862	Standard query 0-1e4d HTTP/1.5 js.cdnresearch.com	53	DNS: Standard query 0-1e4d HTTP/1.5 js.cdnresearch.com
17.976081	Standard query 0-b086 A js.cdnresearch.com	53	DNS: Standard query 0-b086 A js.cdnresearch.com
17.976140	Standard query 0-b086 HTTP/1.5 js.cdnresearch.com	53	DNS: Standard query 0-b086 HTTP/1.5 js.cdnresearch.com
17.976471	Standard query response 0-b086 HTTP/1.5 img-m-msn-com.alicdn.com	53	DNS: Standard query response 0-b086 HTTP/1.5 img-m-msn-com.alicdn.com
17.976471	Standard query response 0-1e4d A js.cdnresearch.com	53	DNS: Standard query response 0-1e4d A js.cdnresearch.com
17.976471	Standard query response 0-b086 A img-m-msn-com.alicdn.com	53	DNS: Standard query response 0-b086 A img-m-msn-com.alicdn.com

Active: 162 DNS: Standard query response 0-b086 A www.bing.com CHNAME www.bing.com trafficmanager.net CHNAME www.bing.com edgekey.net CHNAME edgekey.net alicdn.com A 23.232.244.123 A 23.232.244.131 A 23.232.244.113 A 23.232.244.147 A 23.232.244.138 A 23.232.244.128 A 23.232.244.111 A 23.232.244.128 A 23.232.244.146


☒ Limit to display filter

Flow type: All Flows

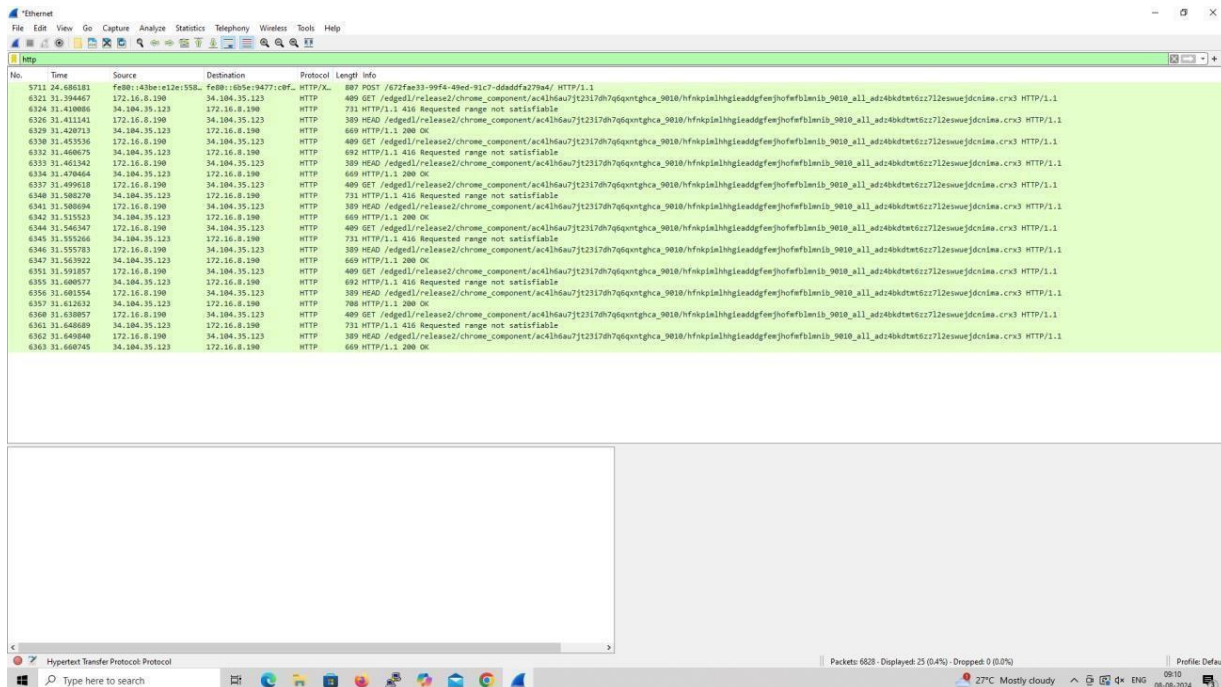
Buttons: Reset Diagram, Export, Address: Any, Help

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

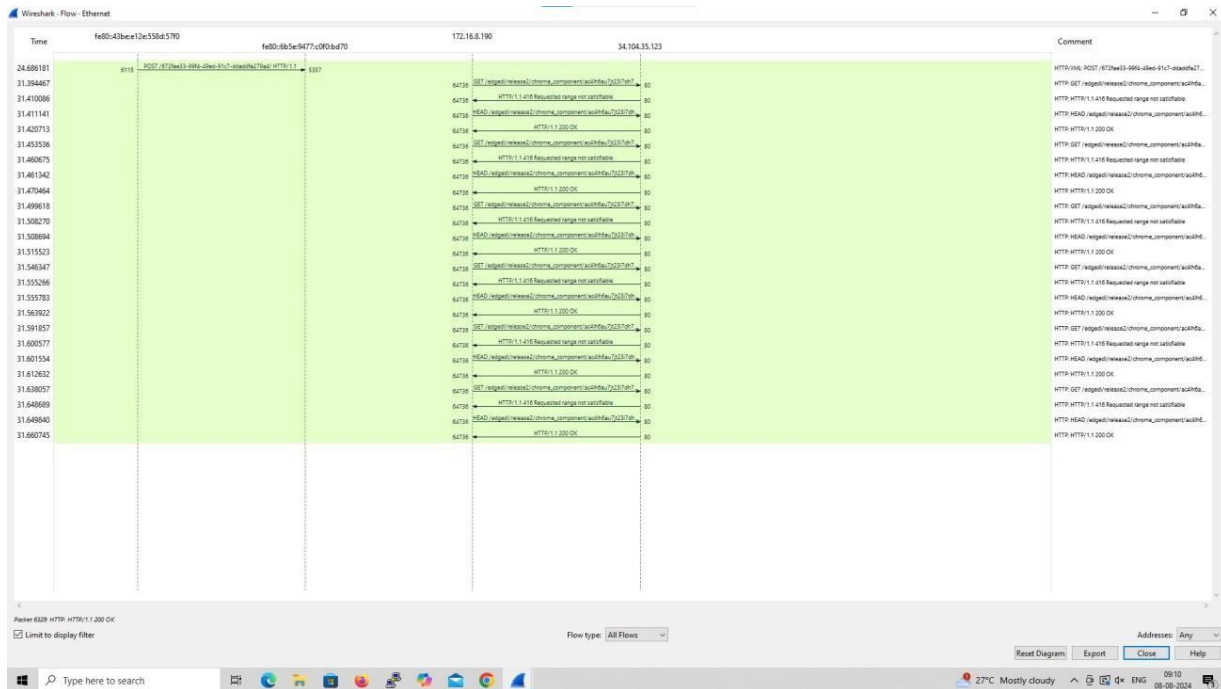
Procedure

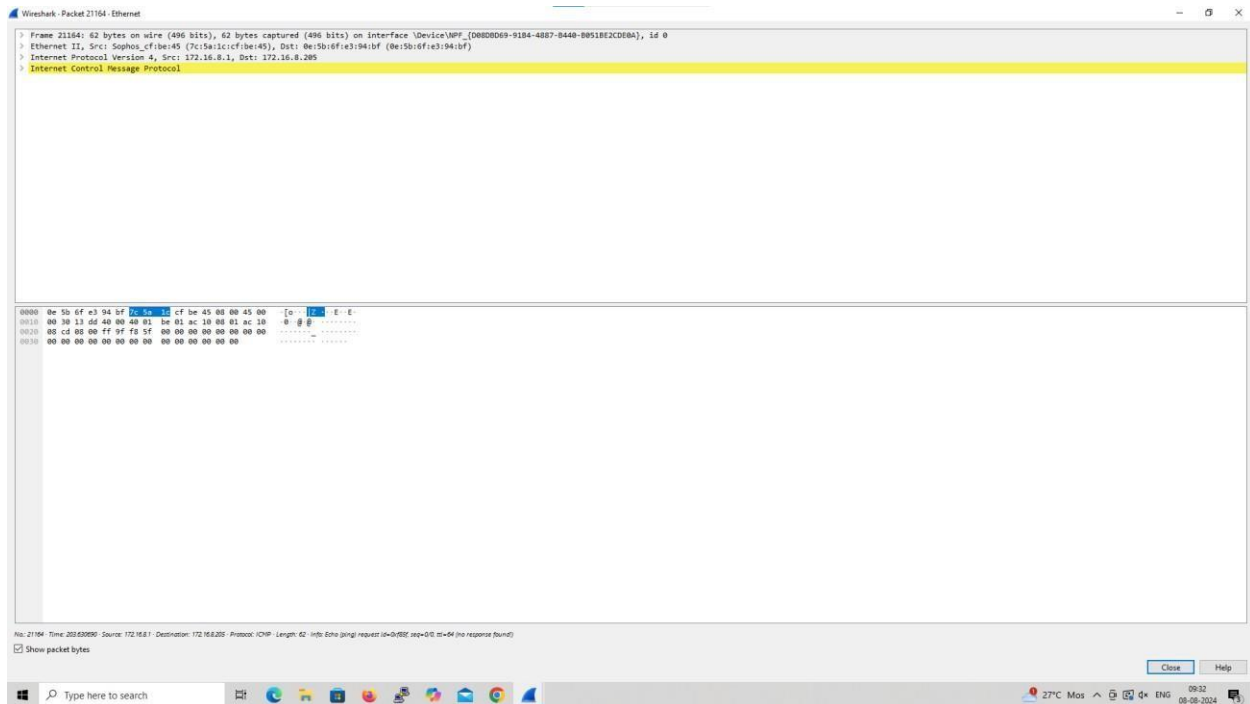
- Select Local Area Connection in Wireshark.
- Go to capture  option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search HTTP packets in the search bar.
- Save the packets.

Output

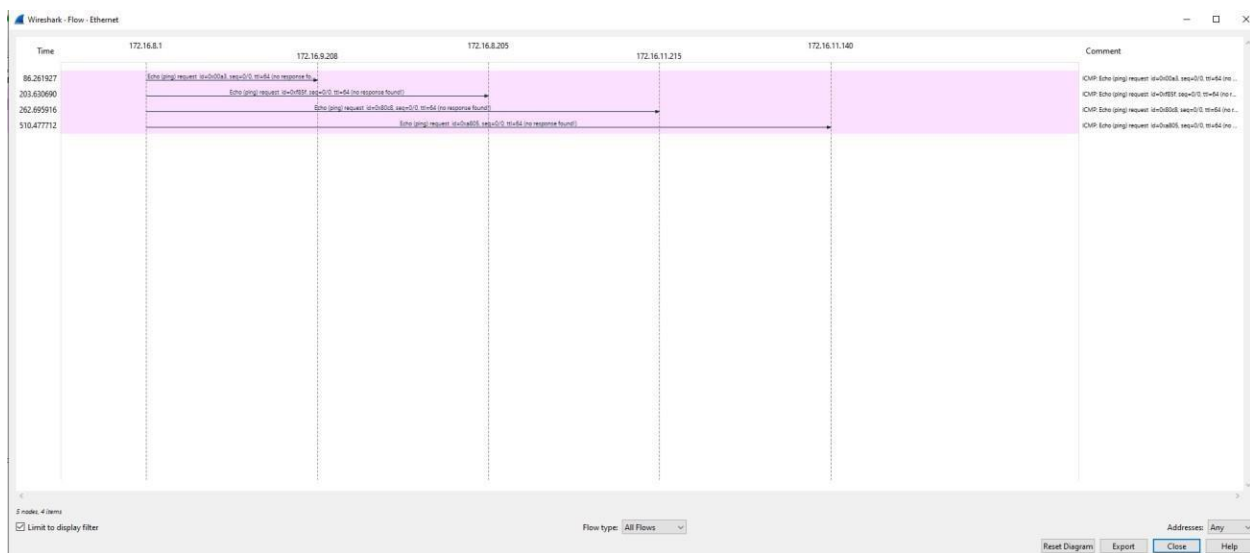


Flow Graph output






Flow Graph output

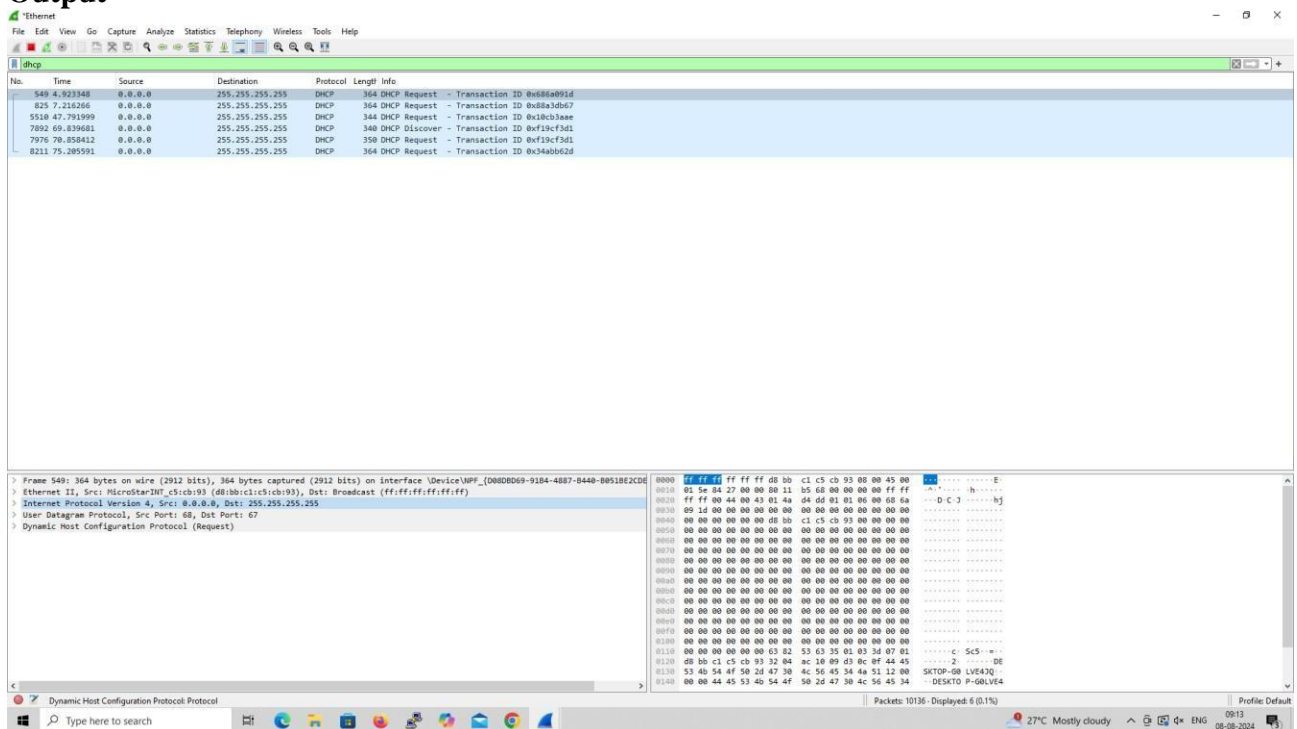


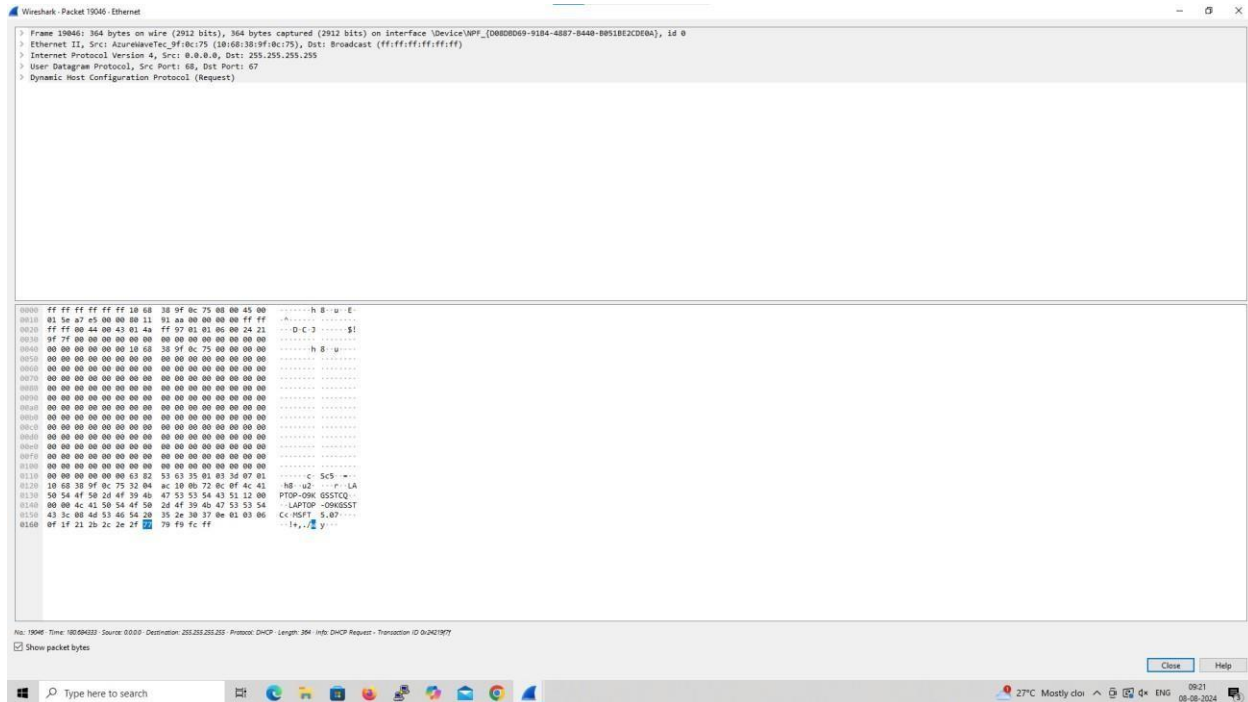
7. Create a Filter to display only DHCP packets and inspect the packets.

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 packets are captured, saved, filtered and analyzed for various protocols like TCP / UDP / IP / HTTP / ARP /DHCP/ICMP /DNS using Wireshark Tool.