

Ex No:5A STUDY OF WIRESHARK TOOL FOR PACKET SNIFFING

AIM:

To study packet sniffing concepts using Wireshark Tool.

DESCRIPTION:

Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format. Wireshark includes filters, color coding, and other features that let you dig deep into network traffic and inspect individual packets. You can use Wireshark to inspect a suspicious program's network traffic, analyze the traffic flow on your network, or troubleshoot network problems.

What we can do with Wireshark:

- Capture network traffic
- Decode packet protocols using dissectors
- Define filters – capture and display
- Watch smart statistics
- Analyze problems
- Interactively browse that traffic

Wireshark used for:

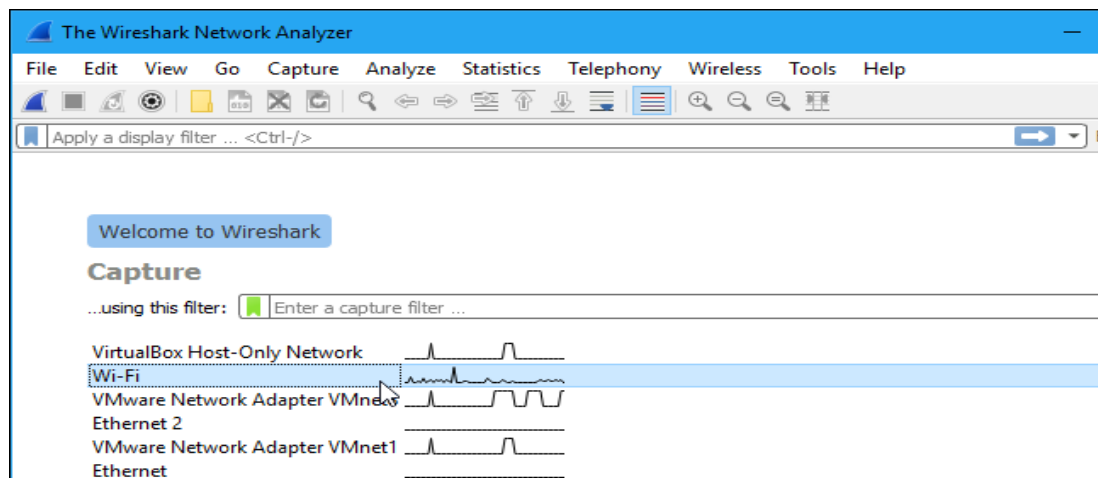
- Network administrators: troubleshoot network problems
- Network security engineers: examine security problems
- Developers: debug protocol implementations
- People: learn **network protocol internals**

Getting Wireshark

Wireshark can be downloaded for Windows or macOS from [its official website](#). For Linux or another UNIX-like system, Wireshark will be found in its package repositories. For Ubuntu, Wireshark will be found in the Ubuntu Software Center.

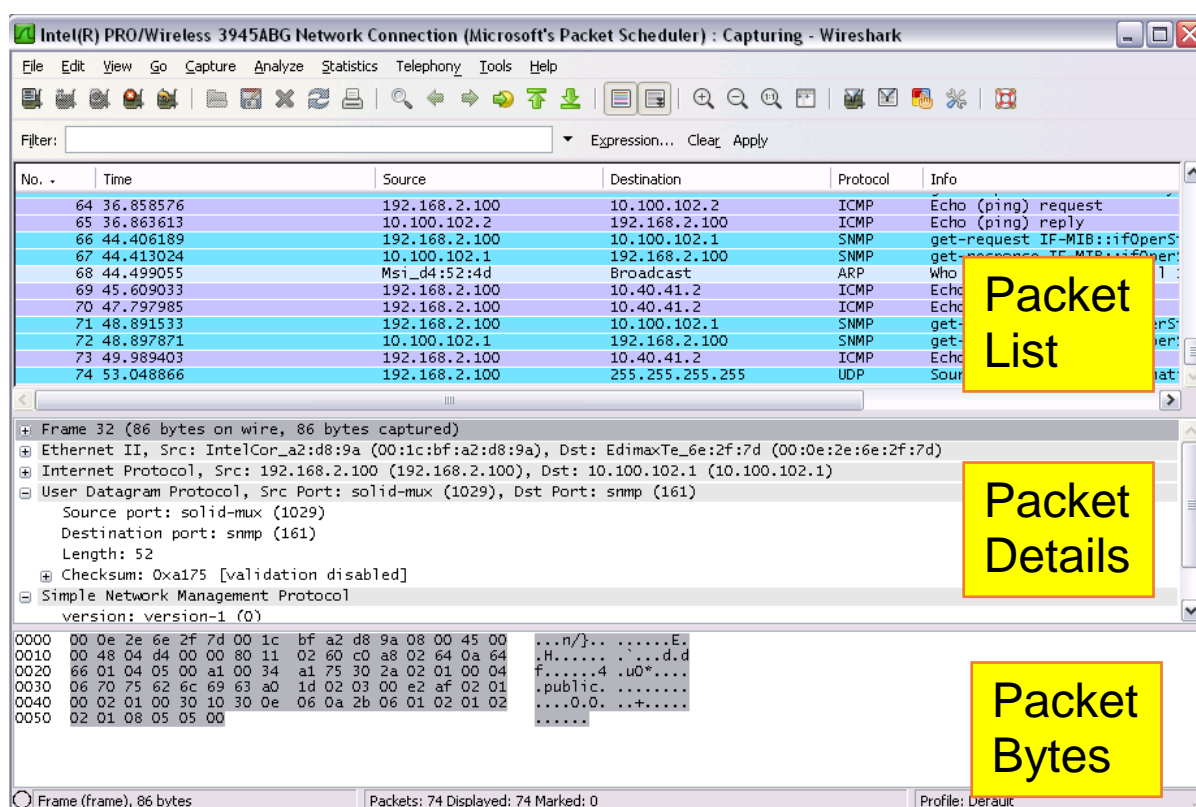
Capturing Packets

After downloading and installing Wireshark, launch it and double-click the name of a network interface under Capture to start capturing packets on that interface



As soon as you click the interface's name, you'll see the packets start to appear in real time. Wireshark captures each packet sent to or from your system.

If you have promiscuous mode enabled—it's enabled by default—you'll also see all the other packets on the network instead of only packets addressed to your network adapter. To check if promiscuous mode is enabled, click Capture > Options and verify the "Enable promiscuous mode on all interfaces" checkbox is activated at the bottom of this window.



Click the red “Stop” button near the top left corner of the window when you want to stop capturing traffic.

The “Packet List” Pane

The packet list pane displays all the packets in the current capture file. The “Packet List” pane Each line in the packet list corresponds to one packet in the capture file. If you select a line in this pane, more details will be displayed in the “Packet Details” and “Packet Bytes” panes.

The “Packet Details” Pane

The packet details pane shows the current packet (selected in the “Packet List” pane) in a more detailed form. This pane shows the protocols and protocol fields of the packet selected in the “Packet List” pane. The protocols and fields of the packet shown in a tree which can be expanded and collapsed.

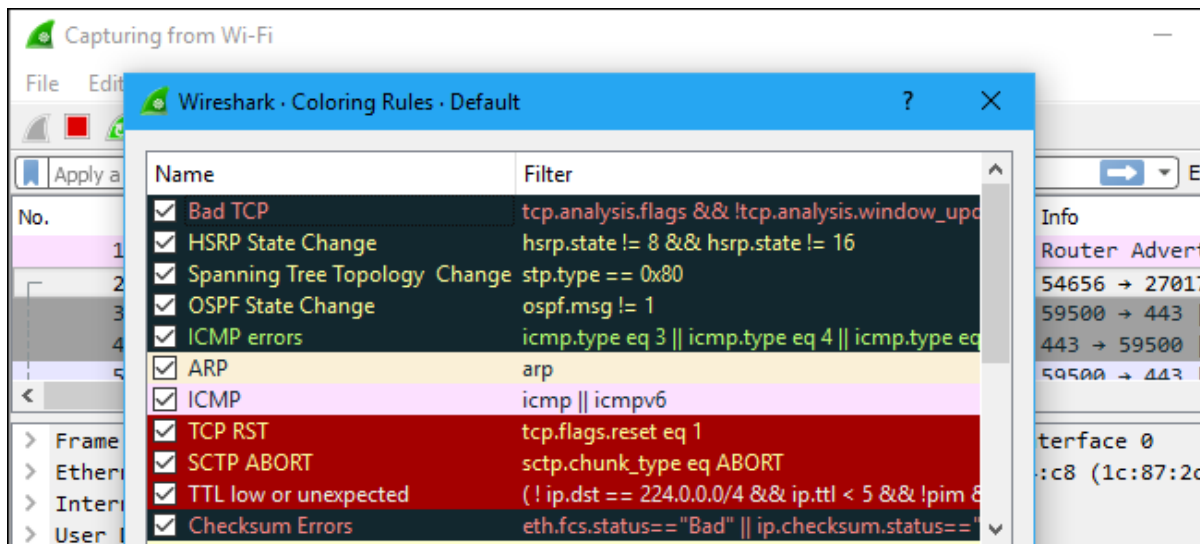
The “Packet Bytes” Pane

The packet bytes pane shows the data of the current packet (selected in the “Packet List” pane) in a hexdump style.

Color Coding

You’ll probably see packets highlighted in a variety of different colors. Wireshark uses colors to help you identify the types of traffic at a glance. By default, light purple is TCP traffic, light blue is UDP traffic, and black identifies packets with errors—for example, they could have been delivered out of order.

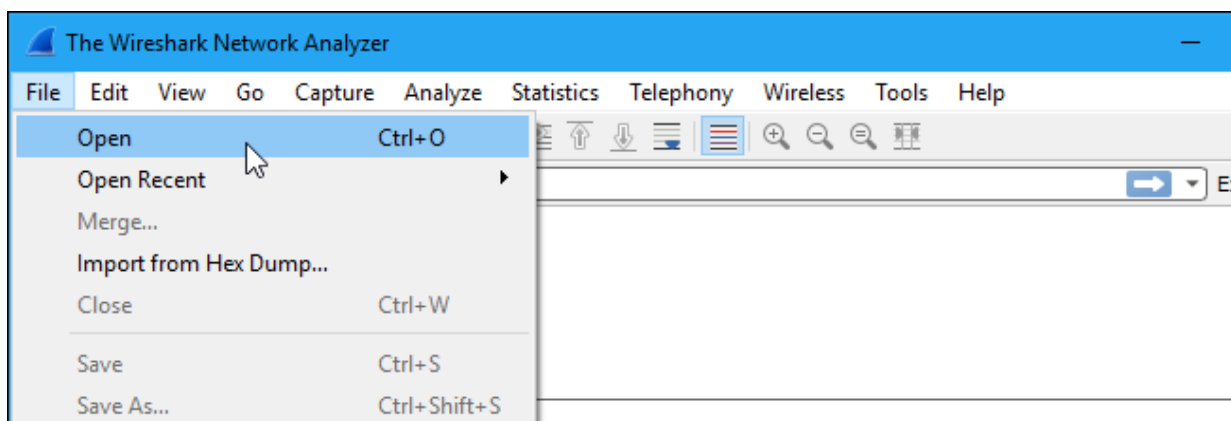
To view exactly what the color codes mean, click View > Coloring Rules. You can also customize and modify the coloring rules from here, if you like.



Sample Captures

If there's nothing interesting on your own network to inspect, Wireshark's wiki has you covered. The wiki contains a [page of sample capture files](#) that you can load and inspect. Click File > Open in Wireshark and browse for your downloaded file to open one.

You can also save your own captures in Wireshark and open them later. Click File > Save to save your captured packets.

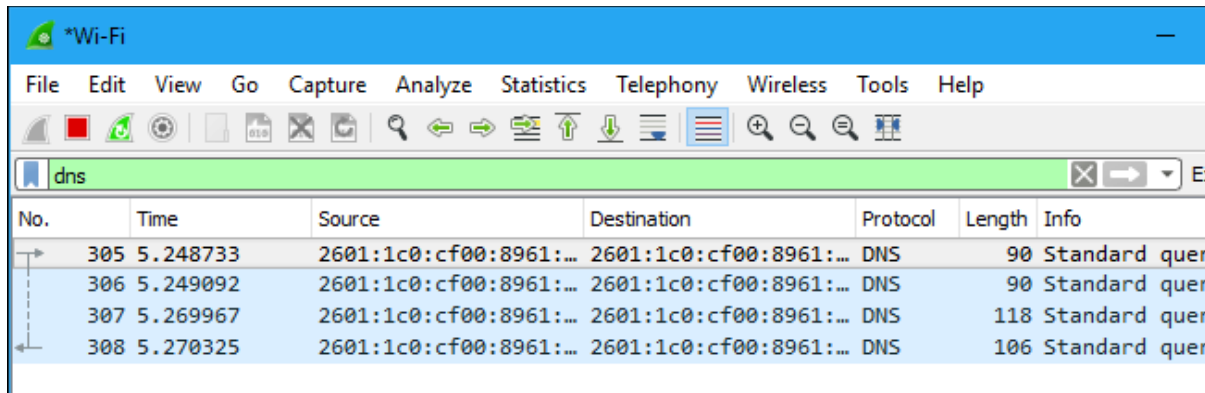


Filtering Packets

If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down

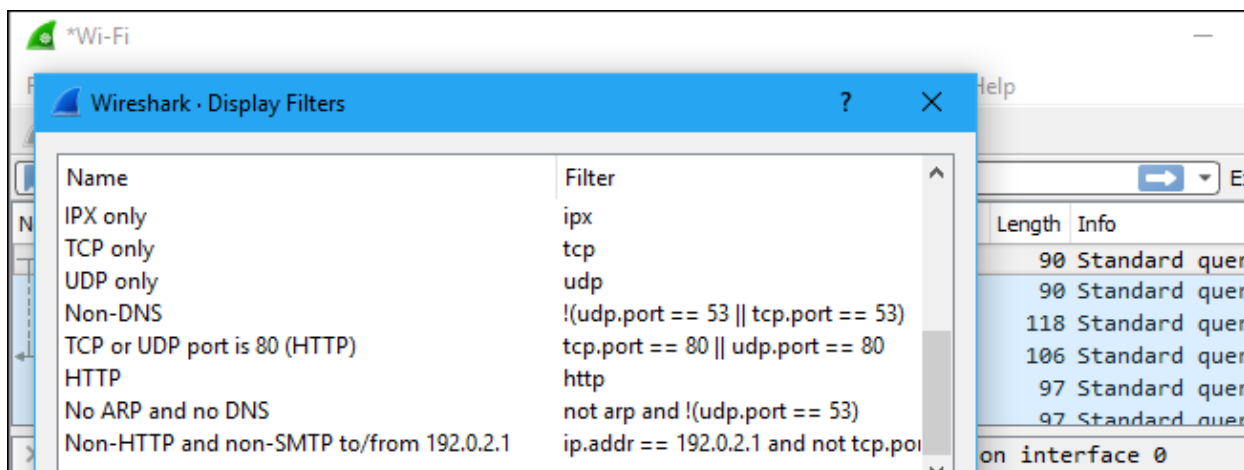
the traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark's filters come in.

The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type "dns" and you'll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.



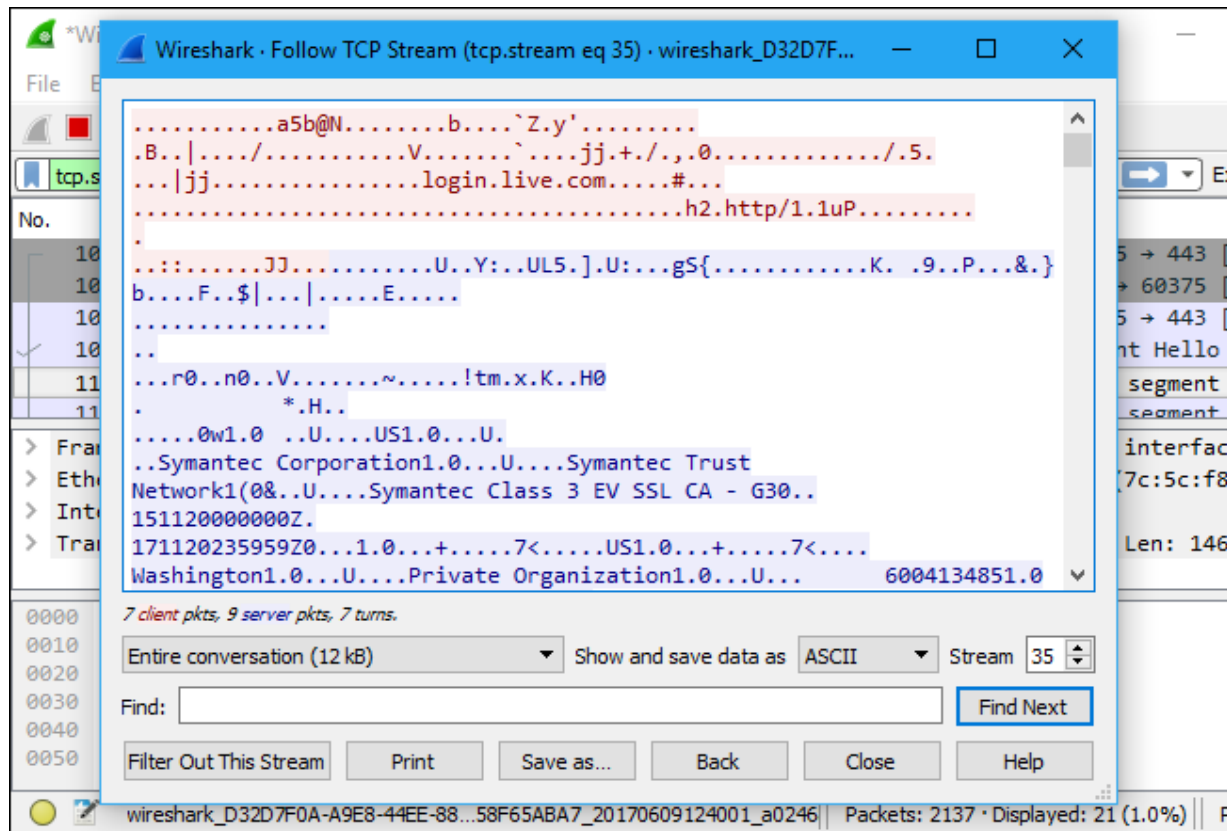
You can also click Analyze > Display Filters to choose a filter from among the default filters included in Wireshark. From here, you can add your own custom filters and save them to easily access them in the future.

For more information on Wireshark's display filtering language, read the [Building display filter expressions](#) page in the official Wireshark documentation.

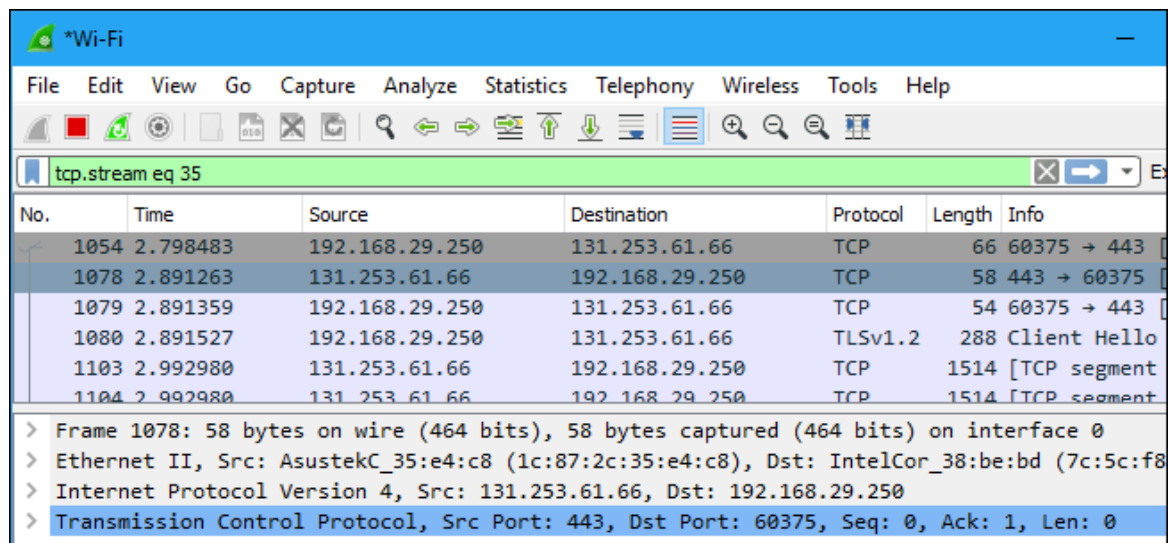


Another interesting thing you can do is right-click a packet and select Follow > TCP Stream.

You'll see the full TCP conversation between the client and the server. You can also click other protocols in the Follow menu to see the full conversations for other protocols, if applicable.



Close the window and you'll find a filter has been applied automatically. Wireshark is showing you the packets that make up the conversation.



Inspecting Packets

Click a packet to select it and you can dig down to view its details.

Wireshark interface showing a packet capture on a Wi-Fi interface. The packet list shows several TCP and TLSv1.2 packets. The selected packet (1054) is expanded, showing details like Interface id, Encapsulation type, Arrival Time, and Epoch Time. The packet bytes are displayed in hexadecimal and ASCII.

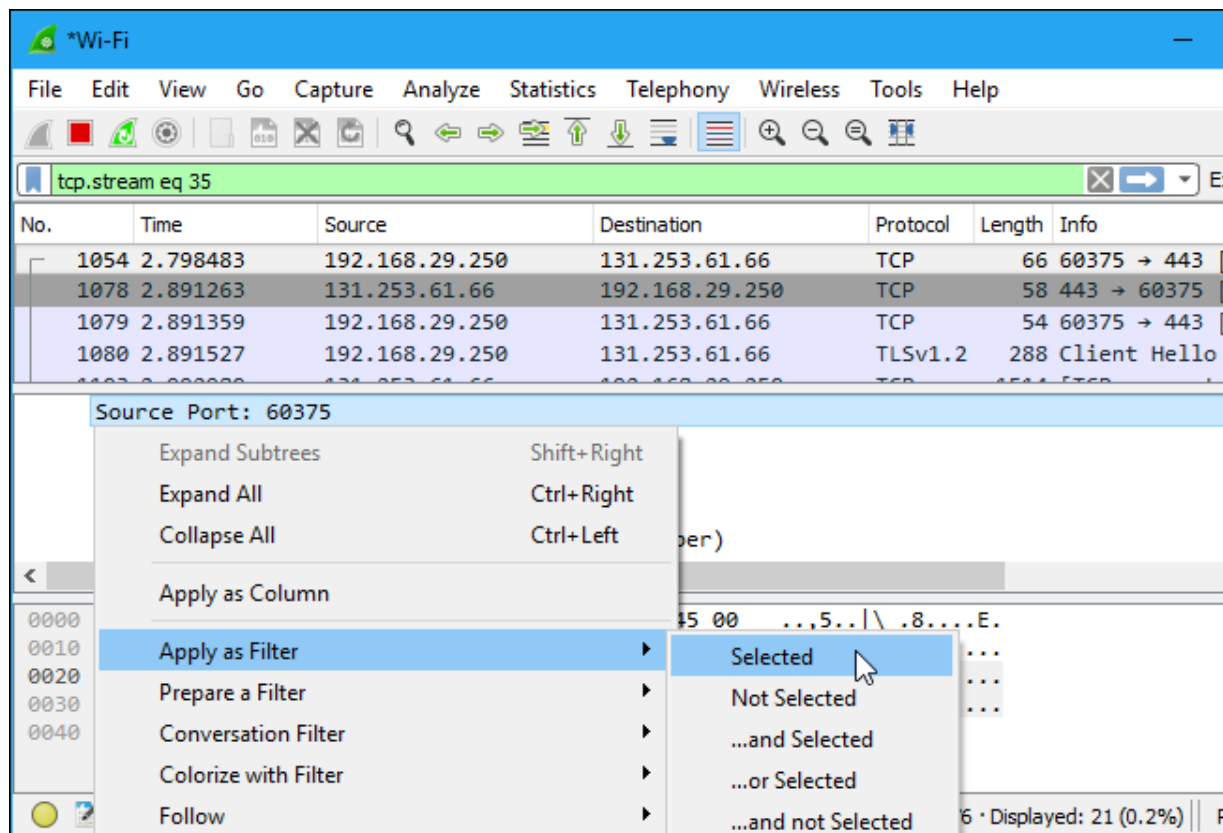
No.	Time	Source	Destination	Protocol	Length	Info
1054	2.798483	192.168.29.250	131.253.61.66	TCP	66	60375 → 443
1078	2.891263	131.253.61.66	192.168.29.250	TCP	58	443 → 60375
1079	2.891359	192.168.29.250	131.253.61.66	TCP	54	60375 → 443
1080	2.891527	192.168.29.250	131.253.61.66	TLSv1.2	288	Client Hello

Frame 1054: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
 Interface id: 0 (\Device\NPF_{D32D7F0A-A9E8-44EE-88DC-DFD58F65ABA7})
 Encapsulation type: Ethernet (1)
 Arrival Time: Jun 9, 2017 12:40:04.140141000 Pacific Daylight Time
 [Time shift for this packet: 0.000000000 seconds]
 Epoch Time: 1497037204.140141000 seconds

Offset	Hex	ASCII
0000	1c 87 2c 35 e4 c8 7c 5c f8 38 be bd 08 00 45 00	..,5.. \ .8....E.
0010	00 34 0b 5d 40 00 80 06 4f 85 c0 a8 1d fa 83 fd	.4.]@... O.....
0020	3d 42 eb d7 01 bb 22 52 7b 69 00 00 00 00 80 02	=B...."R {i.....
0030	fa f0 48 ef 00 00 02 04 05 b4 01 03 03 08 01 01	..H.....
0040	04 02	..

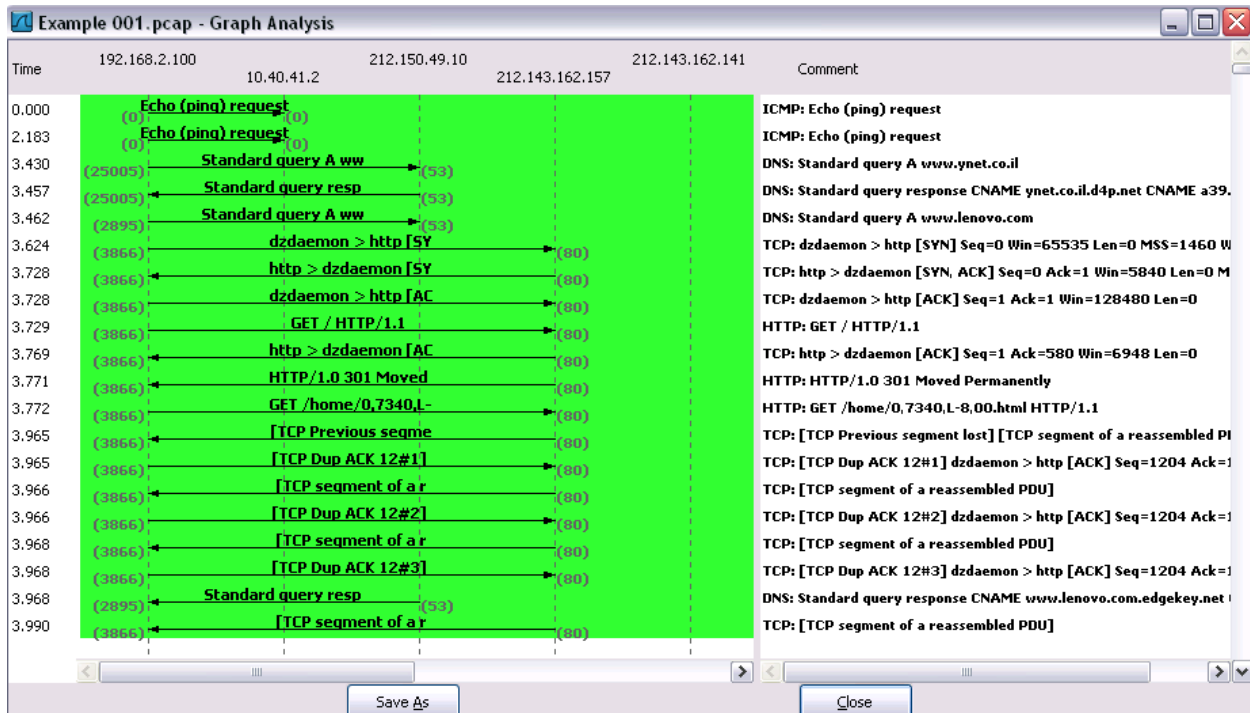
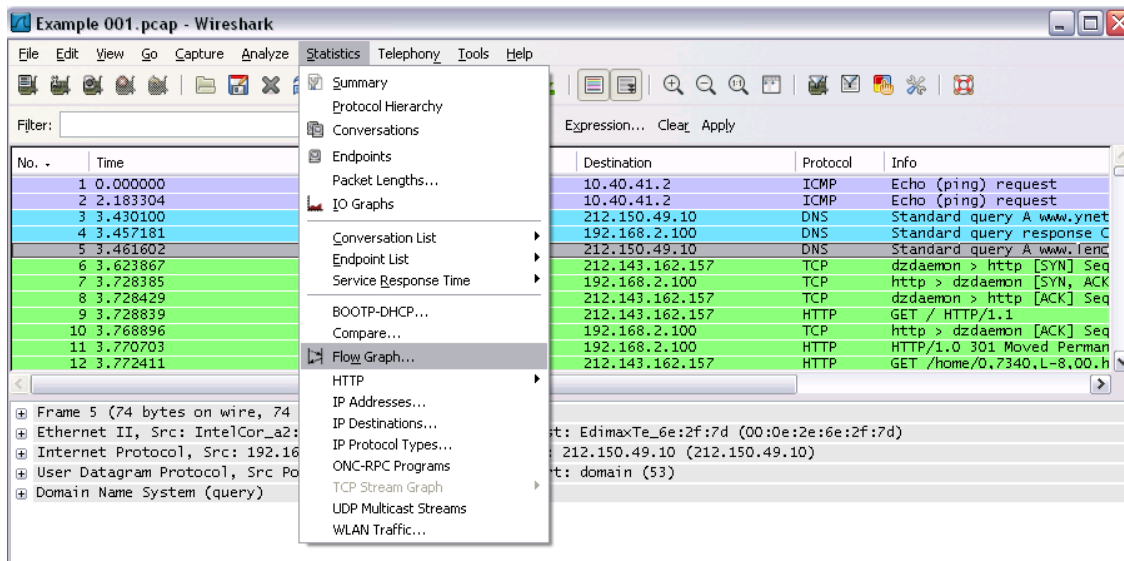
Encapsulation type (frame.encap_type) | Packets: 8136 · Displayed: 21 (0.3%)

You can also create filters from here — just right-click one of the details and use the Apply as Filter submenu to create a filter based on it.



Wireshark is an extremely powerful tool, and this tutorial is just scratching the surface of what you can do with it. Professionals use it to debug network protocol implementations, examine security problems and inspect network protocol internals.


Flow Graph: Gives a better understanding of what we see.

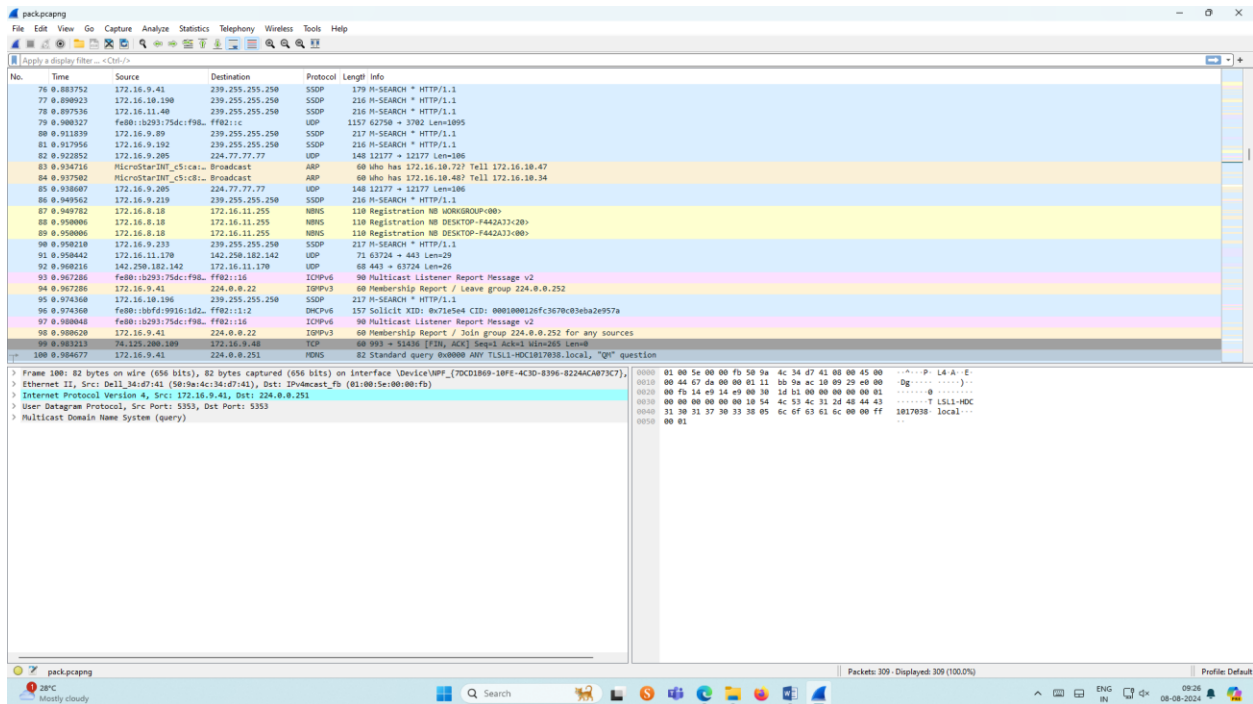


Ex No: 5B**PACKET SNIFFING USING WIRESHARK****AIM:**



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**

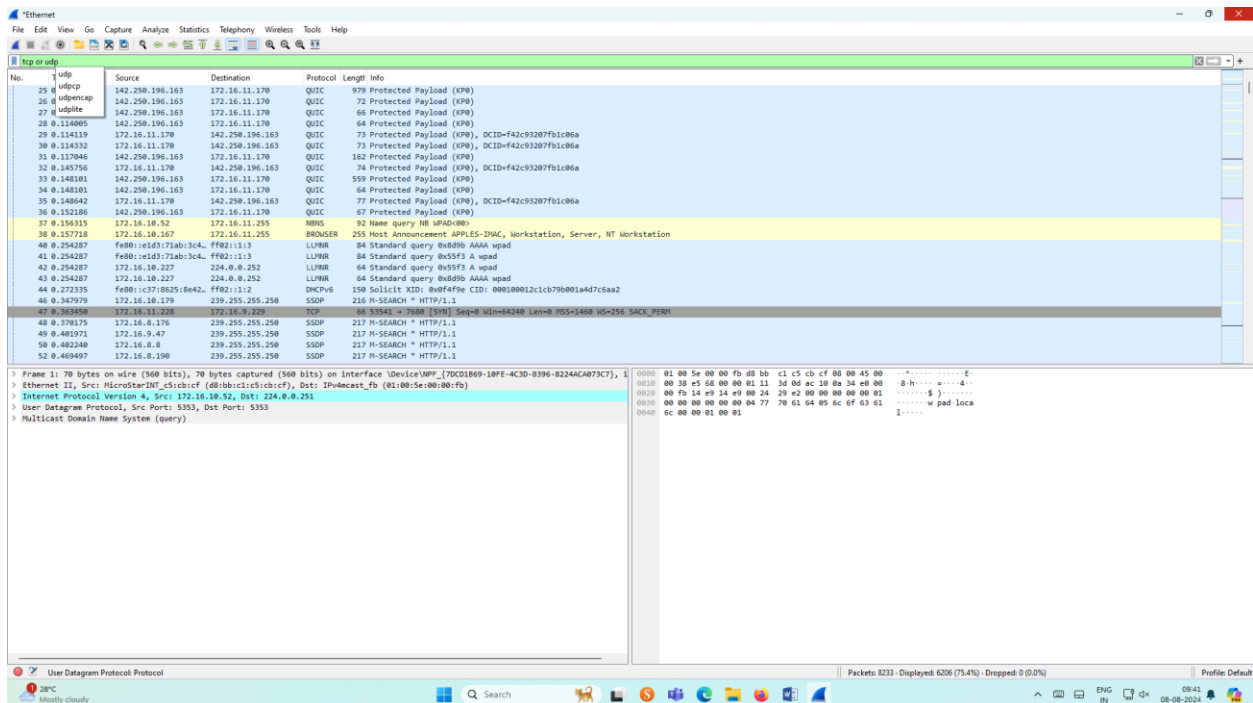
- ☐ Select Local Area Connection in Wireshark.
- ☐ Go to capture  option
- ☐ Select stop capture automatically after 100 packets.
- ☐ Then click Start capture.
- ☐ Save the packets.

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

Procedure

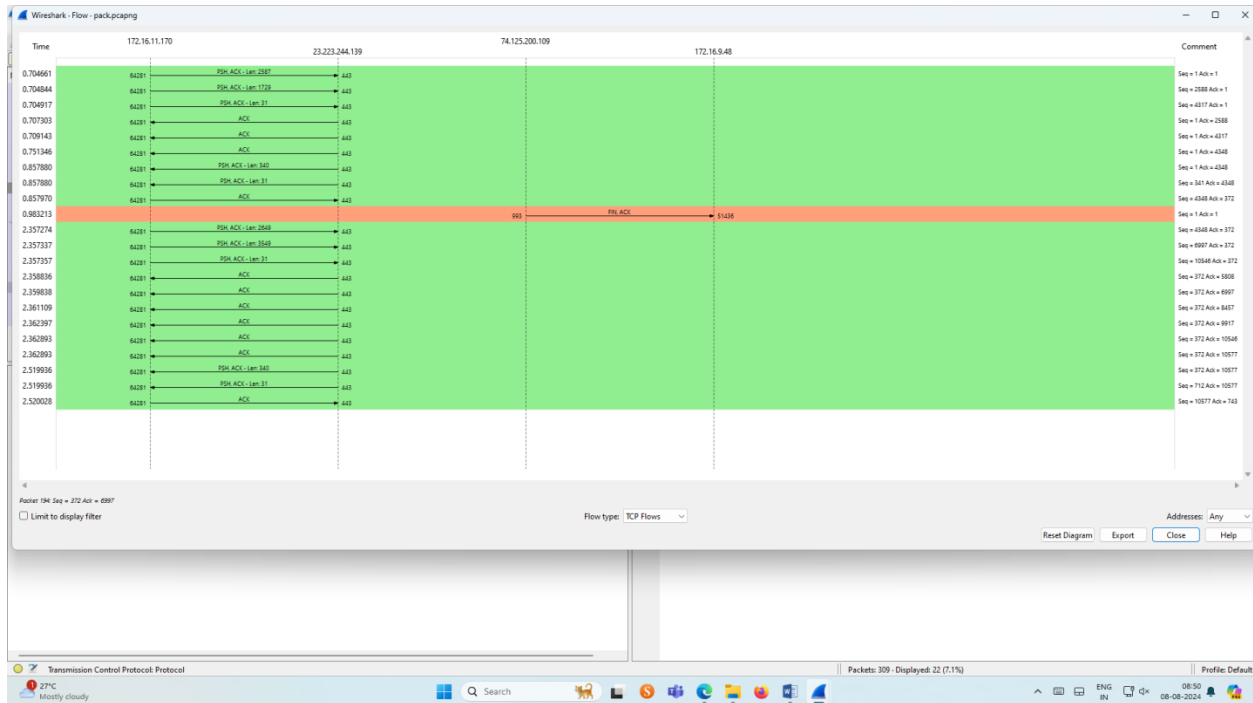
- ☐ Select Local Area Connection in Wireshark.
- ☐ Go to capture  Option
- ☐ Select stop capture automatically after 100 packets.
- ☐ Then click Start capture.
- ☐ Search TCP packets in search bar.
- ☐ To see flow graph click Statistics  Flow graph.
- ☐ Save the packets.

Output:

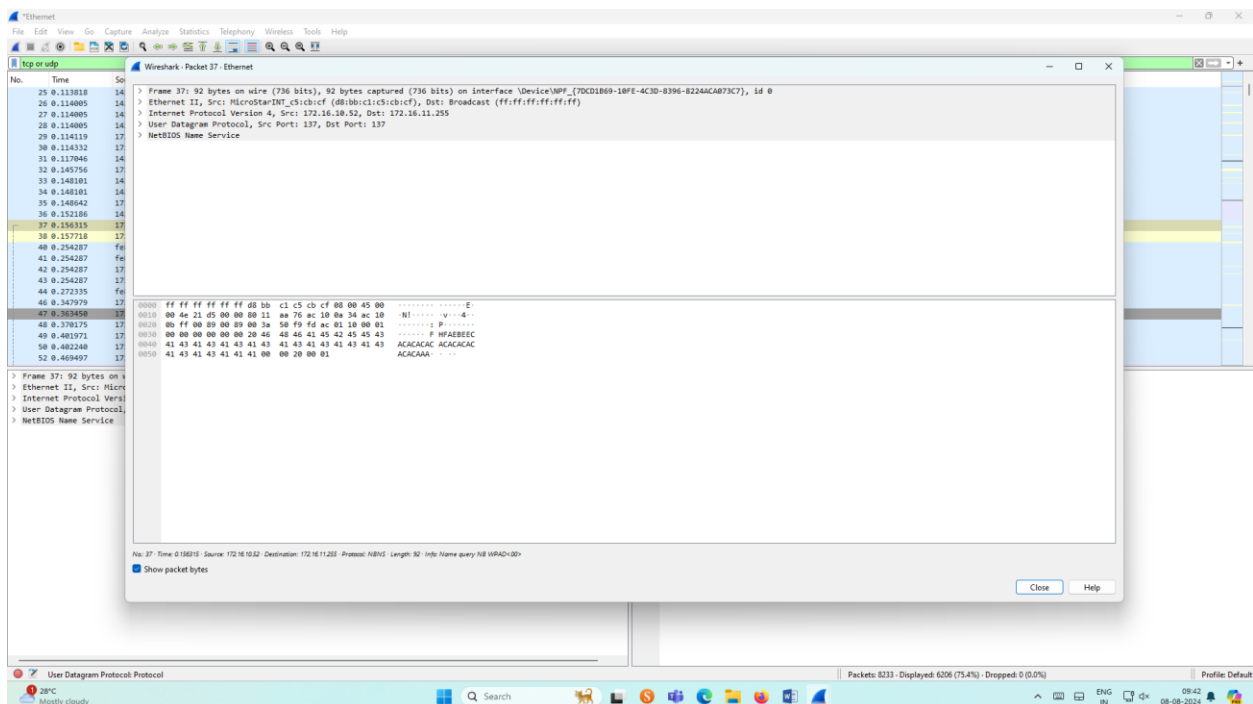


Flow Graph output

CS23532




Inspecting the packets

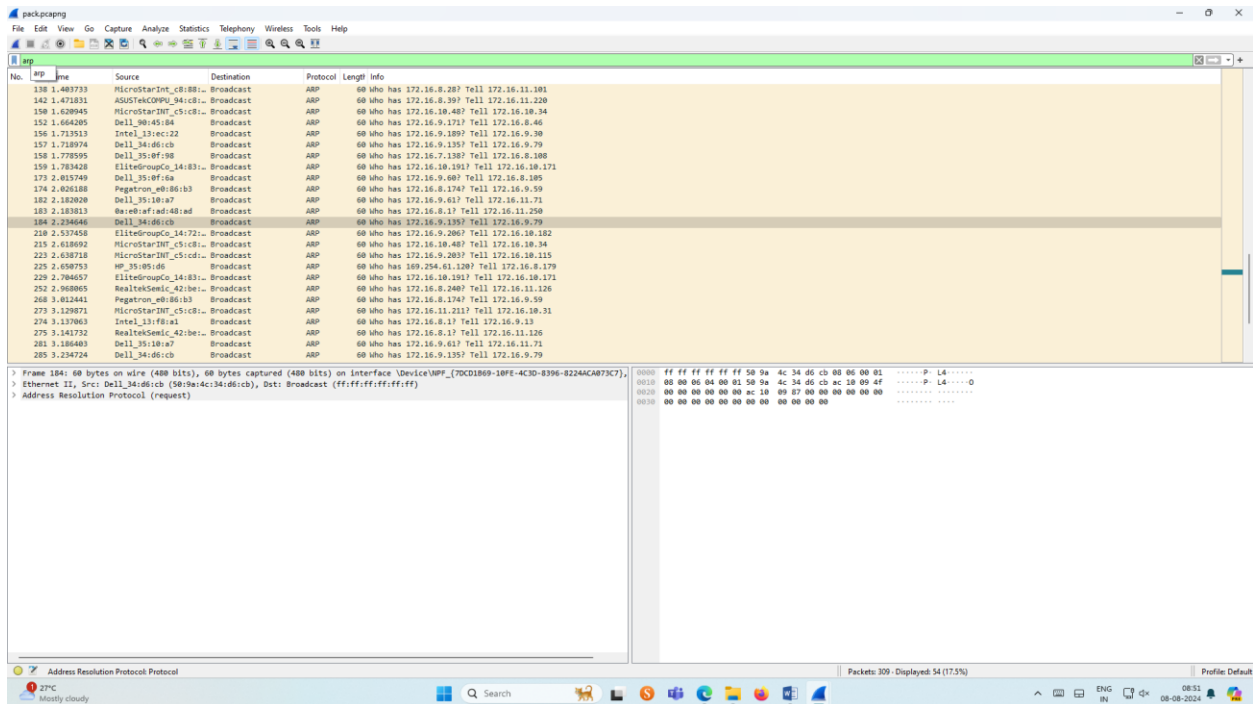


3.Create a Filter to display only ARP packets and inspect the packets.

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 interface with a packet capture of ARP traffic. The packet list pane displays the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
138	1.483733	MicroStarInt_c8:08:...	Broadcast	ARP	60	who has 172.16.8.28? Tell 172.16.11.101
142	1.471831	ASUSTekCOMPU_94:c8:...	Broadcast	ARP	60	who has 172.16.8.39? Tell 172.16.11.220
150	1.620945	MicroStarINT_c8:08:...	Broadcast	ARP	60	who has 172.16.10.40? Tell 172.16.10.34
152	1.664205	Dell_90:45:04	Broadcast	ARP	60	who has 172.16.9.171? Tell 172.16.8.46
156	1.713513	Intel_13:ec:22	Broadcast	ARP	60	who has 172.16.9.189? Tell 172.16.9.30
157	1.718974	Dell_34:06:cb	Broadcast	ARP	60	who has 172.16.9.135? Tell 172.16.9.79
158	1.778595	Dell_35:0f:98	Broadcast	ARP	60	who has 172.16.7.138? Tell 172.16.8.100
159	1.783428	EliteGroupCo_14:83:...	Broadcast	ARP	60	who has 172.16.10.191? Tell 172.16.10.171
173	2.015749	Dell_35:0f:0a	Broadcast	ARP	60	who has 172.16.9.40? Tell 172.16.8.195
174	2.026180	Pegatron_eb:06:b3	Broadcast	ARP	60	who has 172.16.8.174? Tell 172.16.9.59
182	2.182820	Dell_35:10:a7	Broadcast	ARP	60	who has 172.16.9.61? Tell 172.16.11.71
183	2.183813	Basebfraad:48:ad	Broadcast	ARP	60	who has 172.16.8.1? Tell 172.16.11.250
184	2.234646	Dell_34:06:cb	Broadcast	ARP	60	who has 172.16.9.135? Tell 172.16.9.79
210	2.537458	EliteGroupCo_14:72:...	Broadcast	ARP	60	who has 172.16.9.206? Tell 172.16.10.182
215	2.618692	MicroStarINT_c8:08:...	Broadcast	ARP	60	who has 172.16.10.40? Tell 172.16.10.34
223	2.638718	MicroStarINT_c8:08:...	Broadcast	ARP	60	who has 172.16.9.203? Tell 172.16.10.115
225	2.650753	HP_35:05:d6	Broadcast	ARP	60	who has 169.254.61.120? Tell 172.16.8.179
229	2.704657	EliteGroupCo_14:83:...	Broadcast	ARP	60	who has 172.16.10.191? Tell 172.16.10.171
232	2.908065	RealtekSemi_42:be:...	Broadcast	ARP	60	who has 172.16.9.240? Tell 172.16.11.126
268	3.012441	Pegatron_eb:06:b3	Broadcast	ARP	60	who has 172.16.8.174? Tell 172.16.9.59
273	3.120871	MicroStarINT_c8:08:...	Broadcast	ARP	60	who has 172.16.11.211? Tell 172.16.10.31
274	3.137063	Intel_13:ec:a1	Broadcast	ARP	60	who has 172.16.8.1? Tell 172.16.9.13
275	3.141732	RealtekSemi_42:be:...	Broadcast	ARP	60	who has 172.16.8.1? Tell 172.16.11.126
281	3.186483	Dell_35:10:a7	Broadcast	ARP	60	who has 172.16.9.61? Tell 172.16.11.71
285	3.234724	Dell_34:06:cb	Broadcast	ARP	60	who has 172.16.9.135? Tell 172.16.9.79

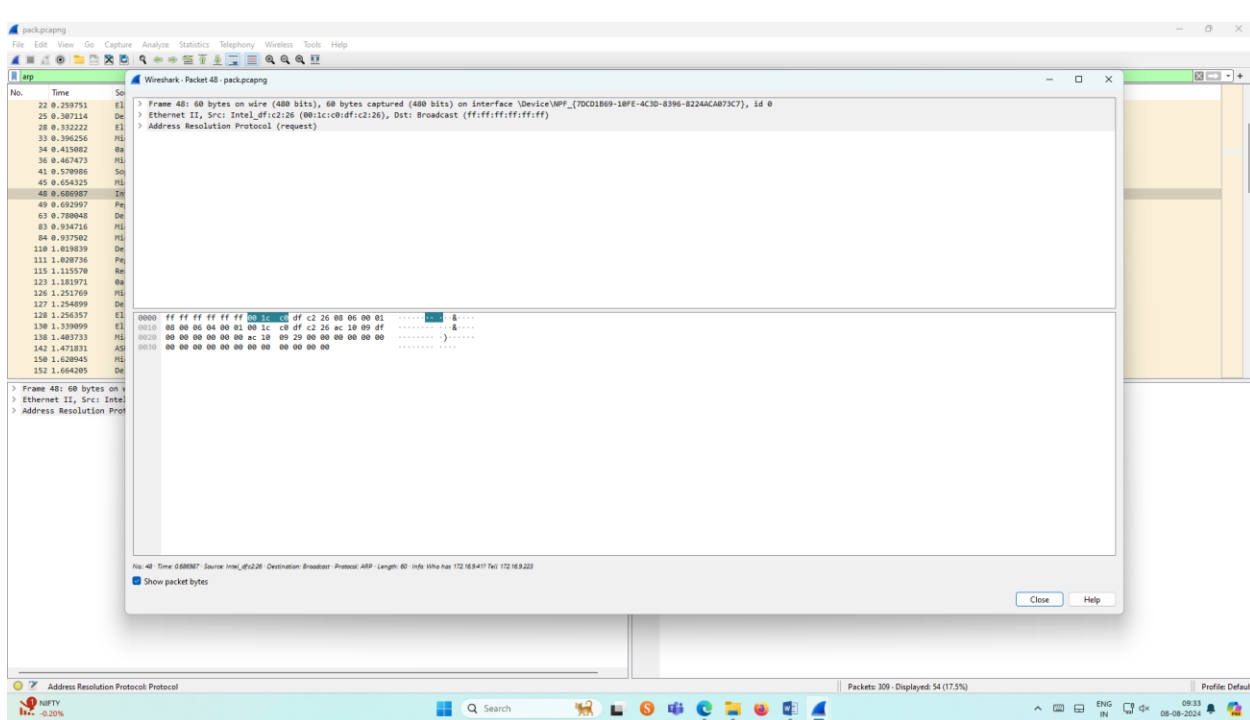
The packet details pane for the selected packet (Frame 184) shows the following structure:

```

> Frame 184: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on Interface \Device\NPF_{70CD1869-10FE-4C3D-8396-8224ACAB73C7}
> Ethernet II, Src: Dell_34:06:cb (98:9e:4c:34:06:cb), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)
  0000  ff ff ff ff ff ff 50 9a 4c 34 06 cb 00 00 01  .....P L4.....
  0010  00 00 00 00 00 01 50 9a 4c 34 06 cb ac 10 00 4f  .....P L4.....Q
  0020  00 00 00 00 00 00 ac 10 09 07 00 00 00 00 00 00  .....
  0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
  
```

Inspecting the packets

CS23532



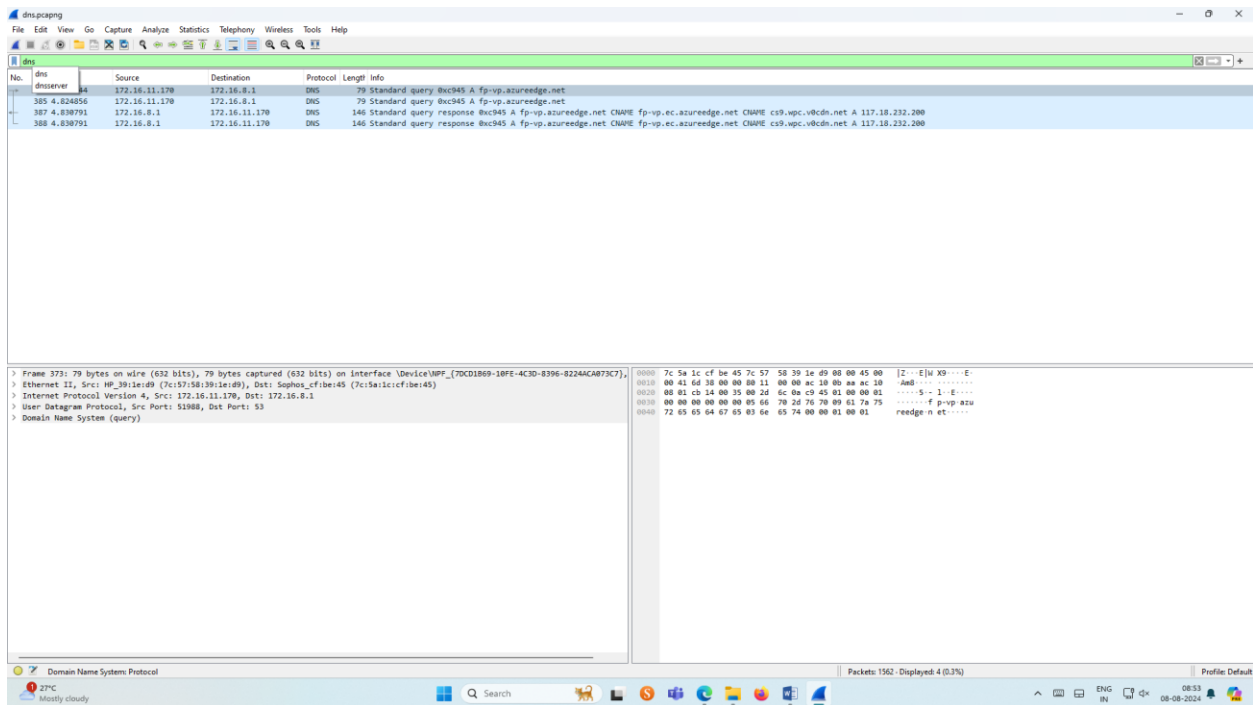
4.Create a Filter to display only DNS packets and provide the flow graph.

Procedure

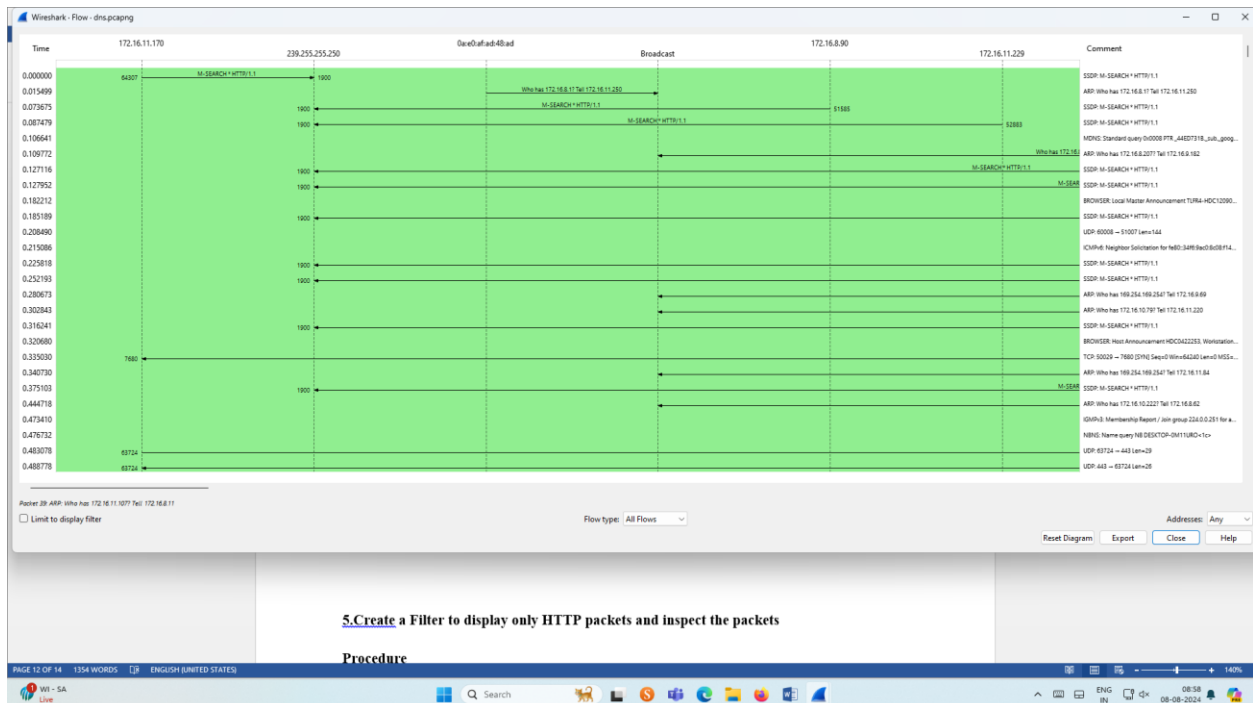
- ☐ Select Local Area Connection in Wireshark.
- ☐ Go to capture Option
- ☐ Select stop capture automatically after 100 packets.
- ☐ Then click Start capture.
- ☐ Search DNS packets in search bar.
- ☐ To see flow graph click Statistics > Flow graph.
- ☐ Save the packets.

Output

CS23532




Graph output

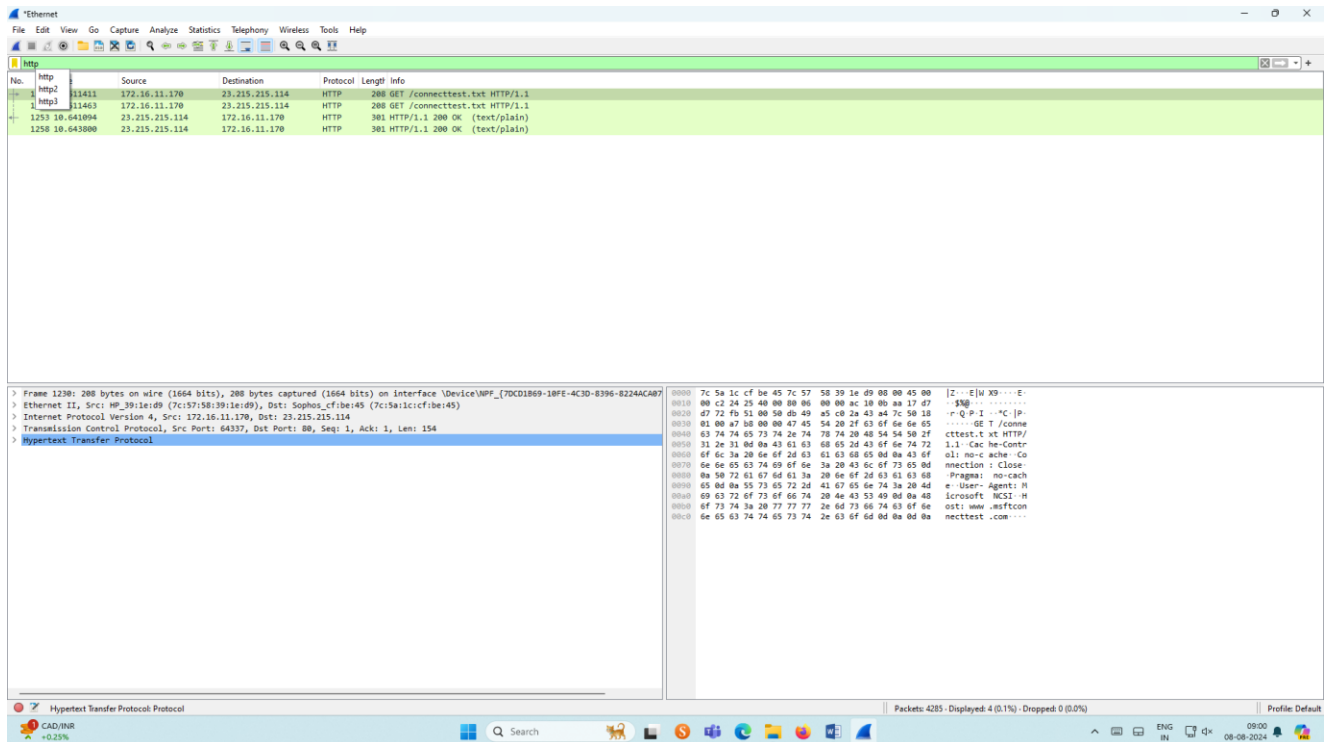


5.Create a Filter to display only HTTP packets and inspect the packets

Procedure

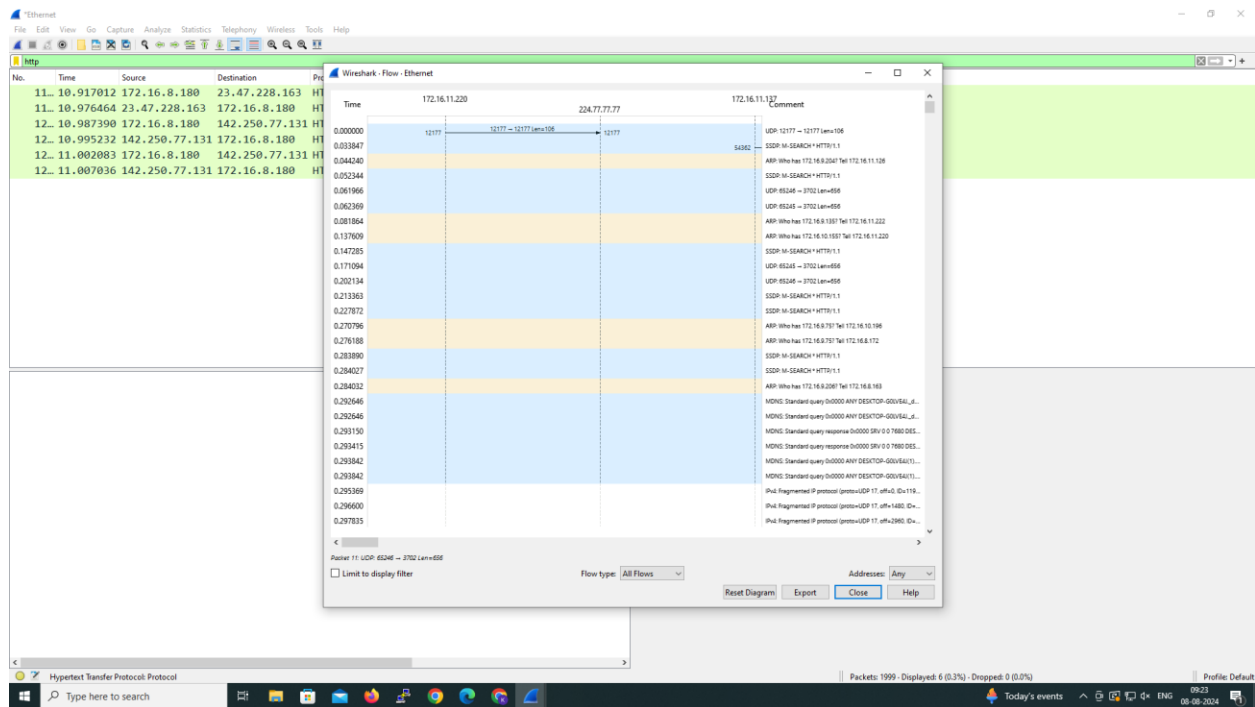
- ☐ Select Local Area Connection in Wireshark.
- ☐ Go to capture  option
- ☐ Select stop capture automatically after 100 packets.
- ☐ Then click Start capture.
- ☐ Search HTTP packets in the search bar.
- ☐ Save the packets.

Output

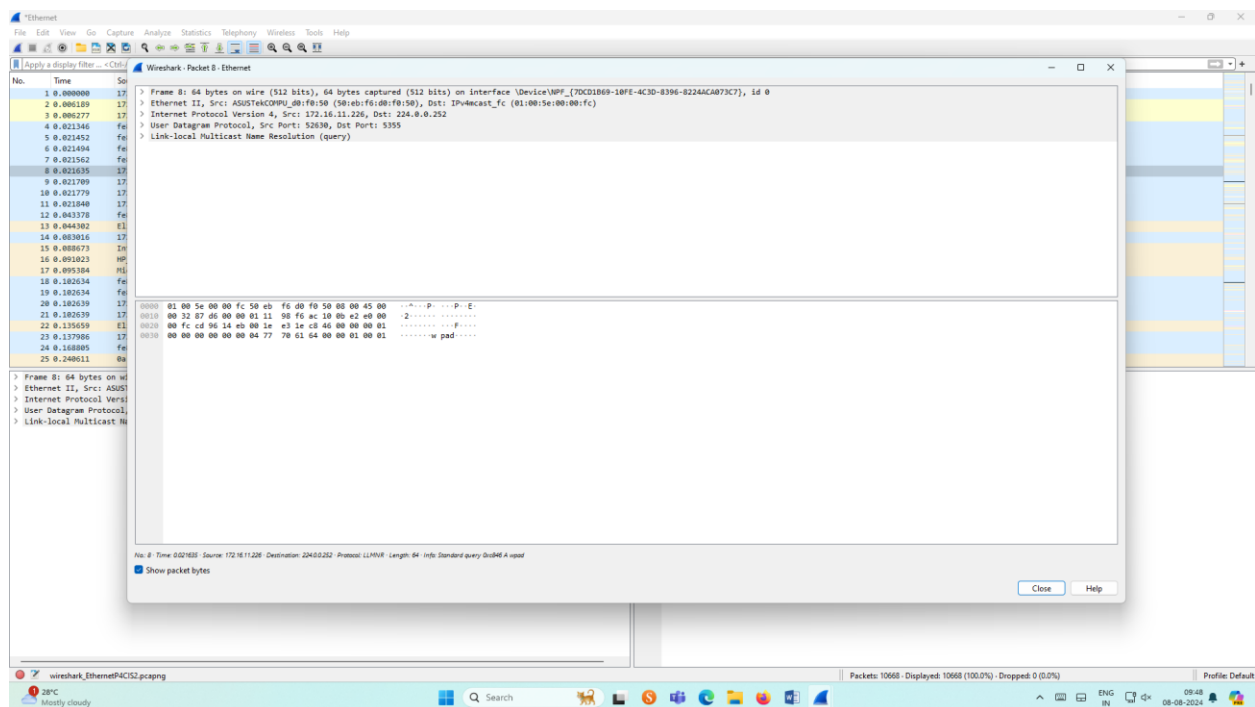


Flow Graph output

CS23532




Inspecting the packets



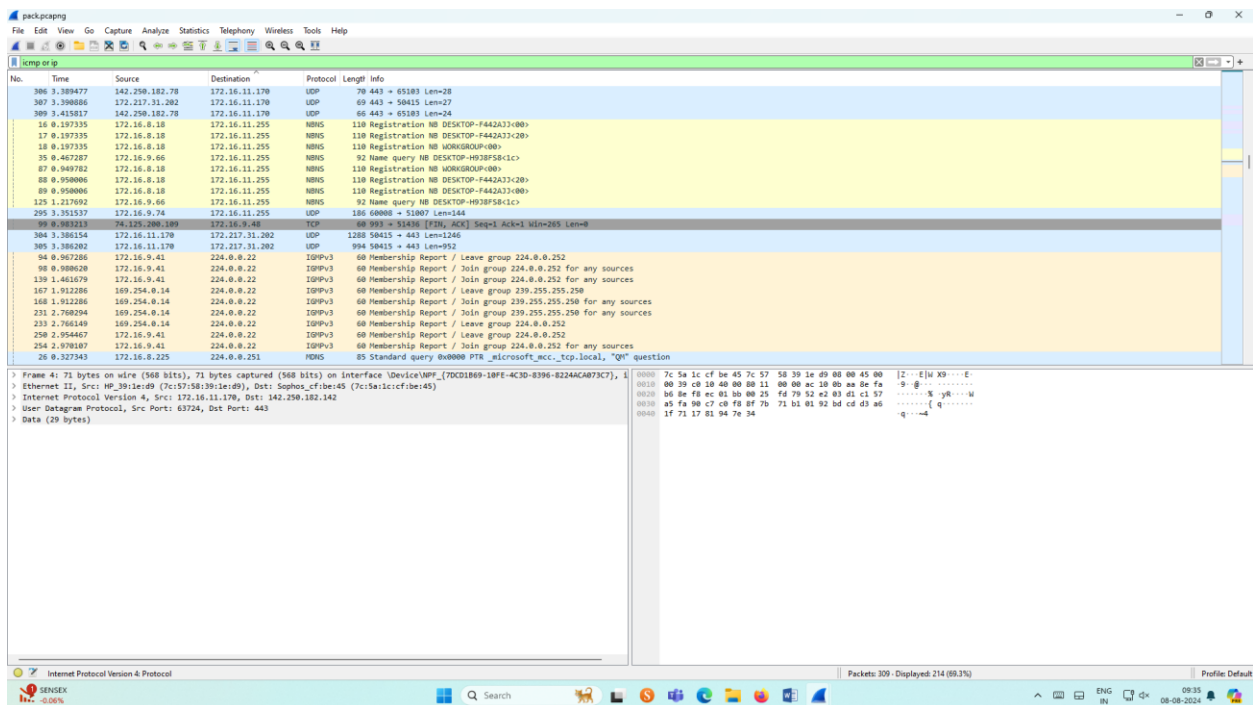
6.Create a Filter to display only IP/ICMP packets and inspect the packets.

CS23532

Procedure

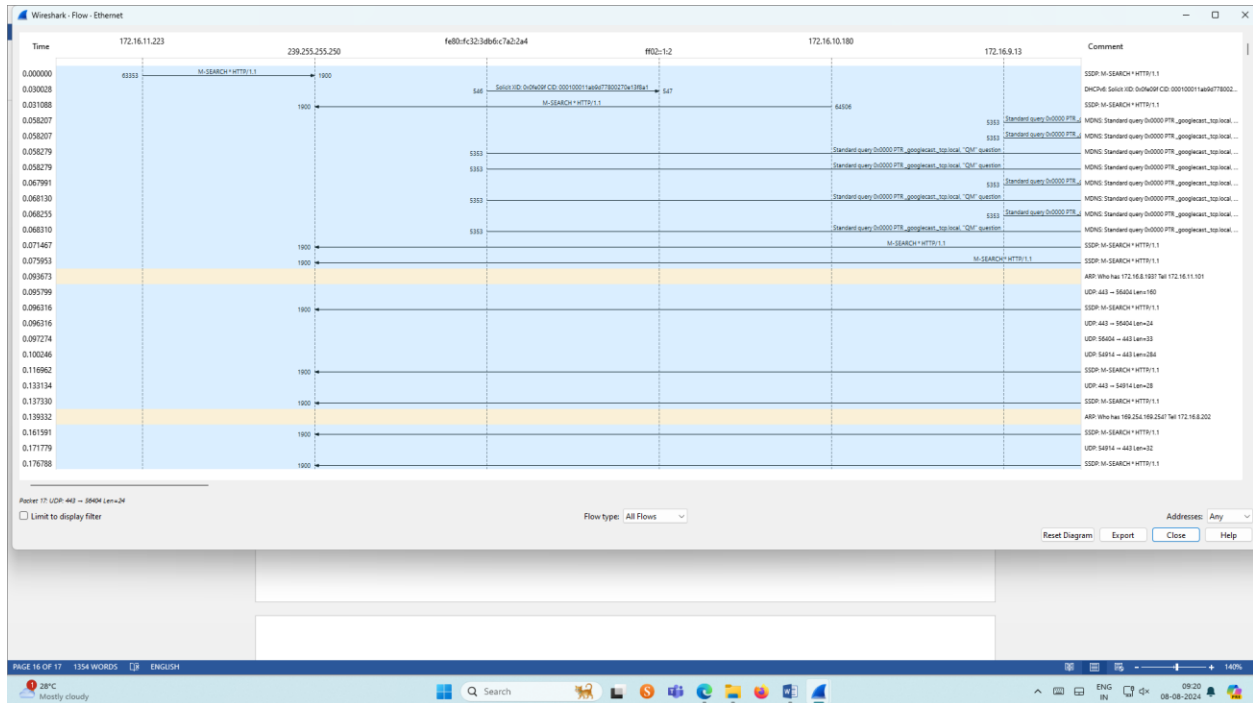
- ☐ Select Local Area Connection in Wireshark.
- ☐ Go to capture  option
- ☐ Select stop capture automatically after 100 packets.
- ☐ Then click Start capture.
- ☐ Search ICMP/IP packets in search bar.
- ☐ Save the packets

Output

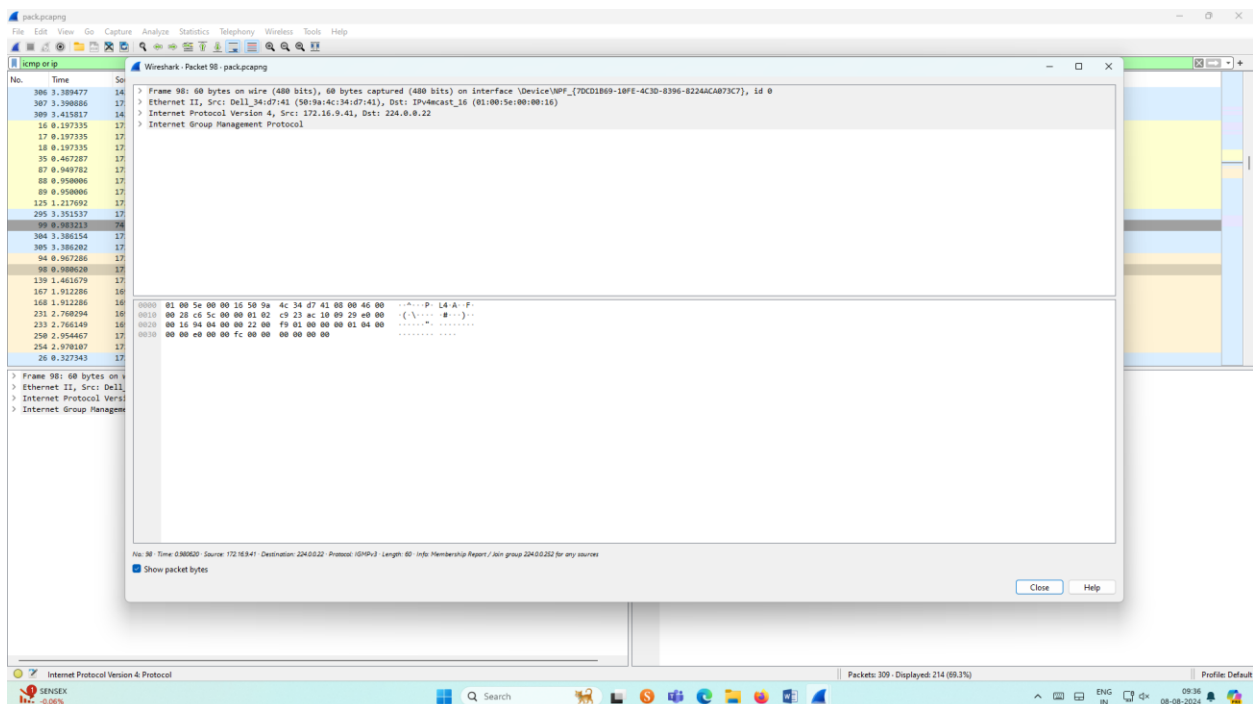


Flow Graph output

CS23532




Inspecting the packets

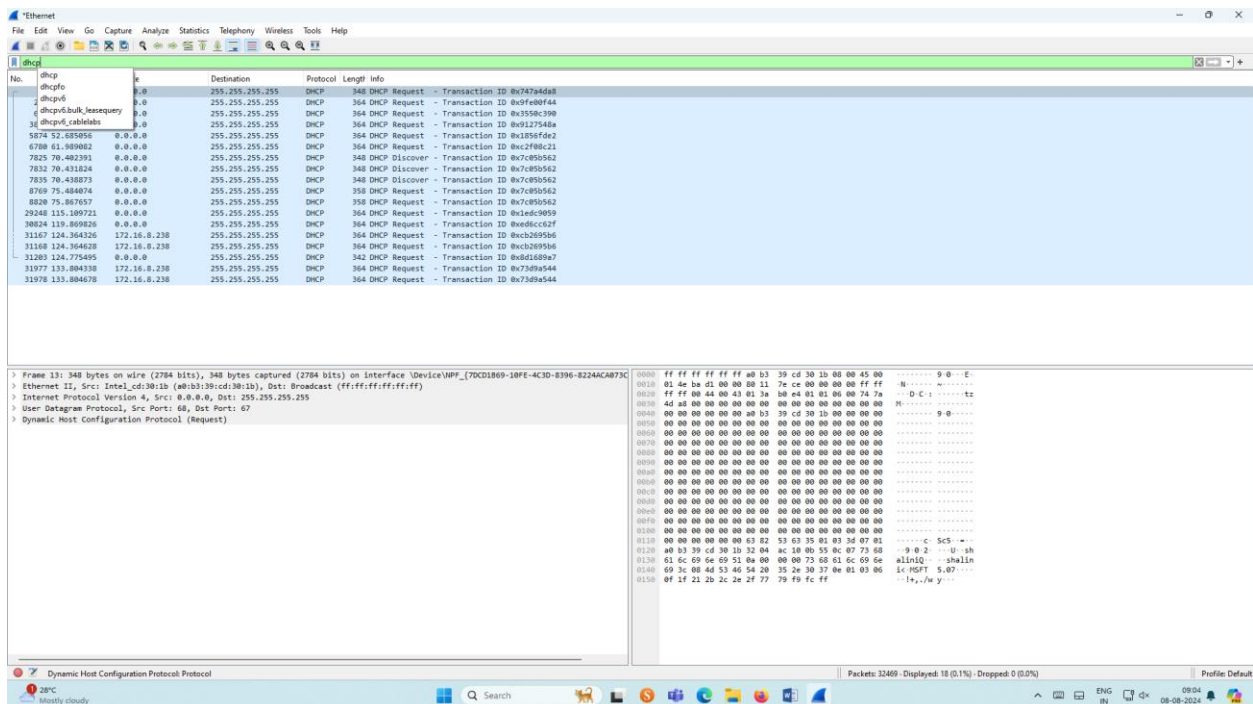


7.Create a Filter to display only DHCP packets and inspect the packets.

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 interface with a DHCP traffic capture. The packet list pane shows several DHCP packets, including requests and discoveries. The packet details pane for the selected packet (Frame 13) shows the following structure:

- Frame 13: 348 bytes on wire (2784 bits), 348 bytes captured (2784 bits) on interface \Device\NPF_{70CD1869-10FE-4C3D-8396-8224AC873C}
- Ethernet II, Src: Intel_c6:30:1b (a8:bb:39:cd:30:1b), 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)

The packet bytes pane shows the raw data of the packet, including the Ethernet II header, IP header, UDP header, and DHCP request payload.

Inspecting the packets

CS23532

