

Ex No: 14a 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:

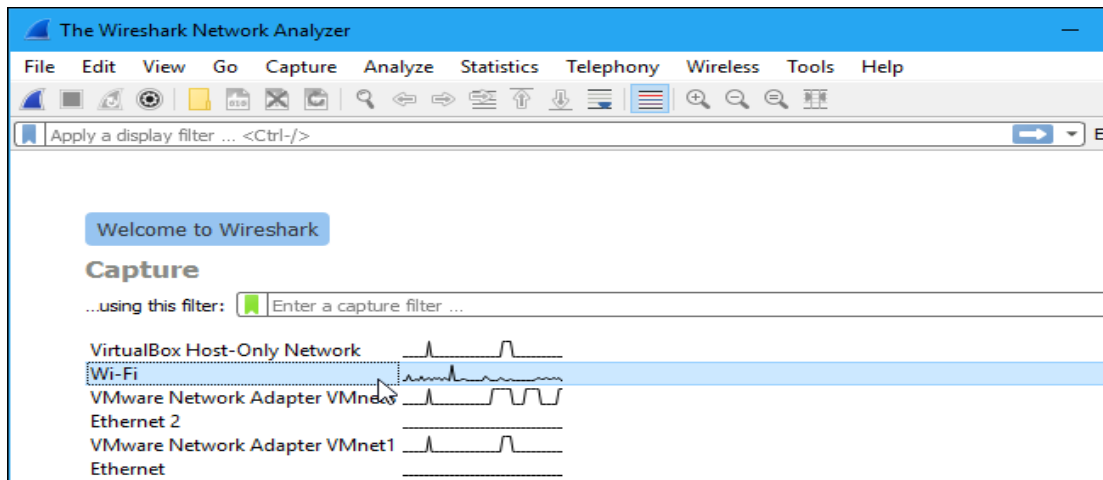
- Network administrators: troubleshoot network problems
- Network security engineers: examine security problems
- Developers: debug protocol implementations
- People: learn **network protocol internals**

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.

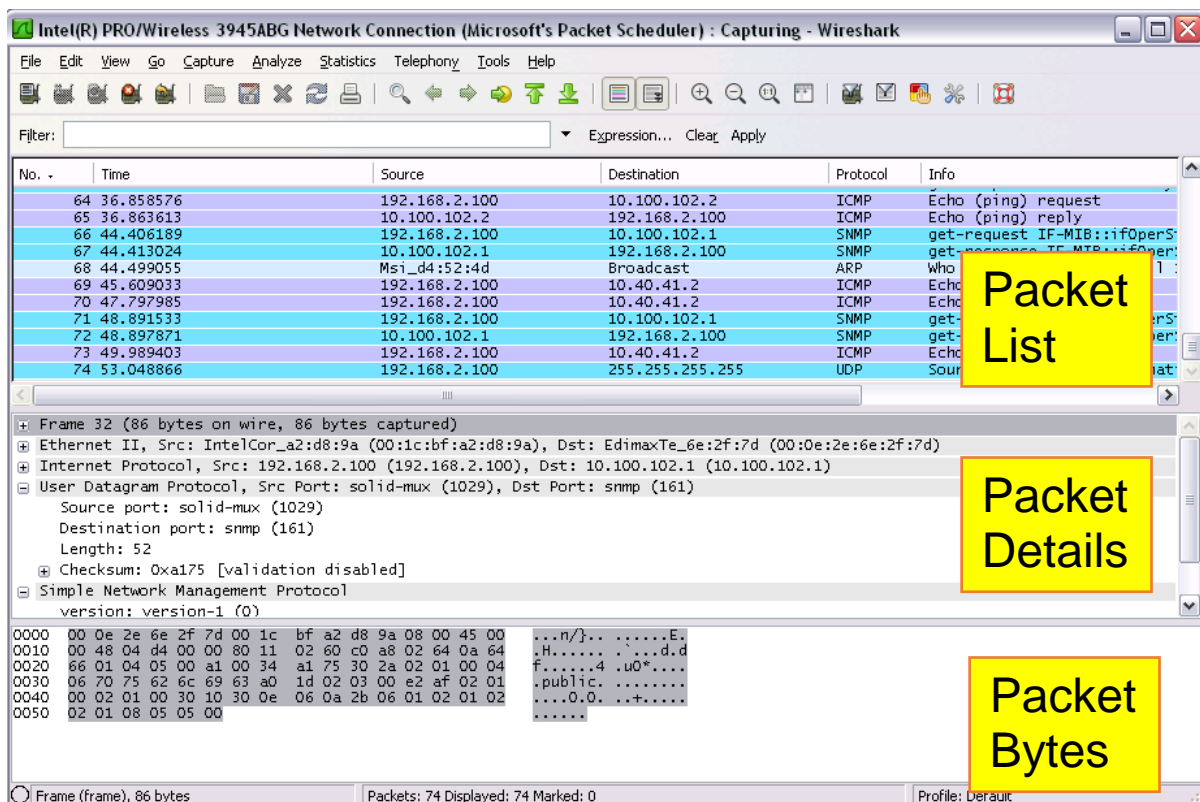
Capturing Packets

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.

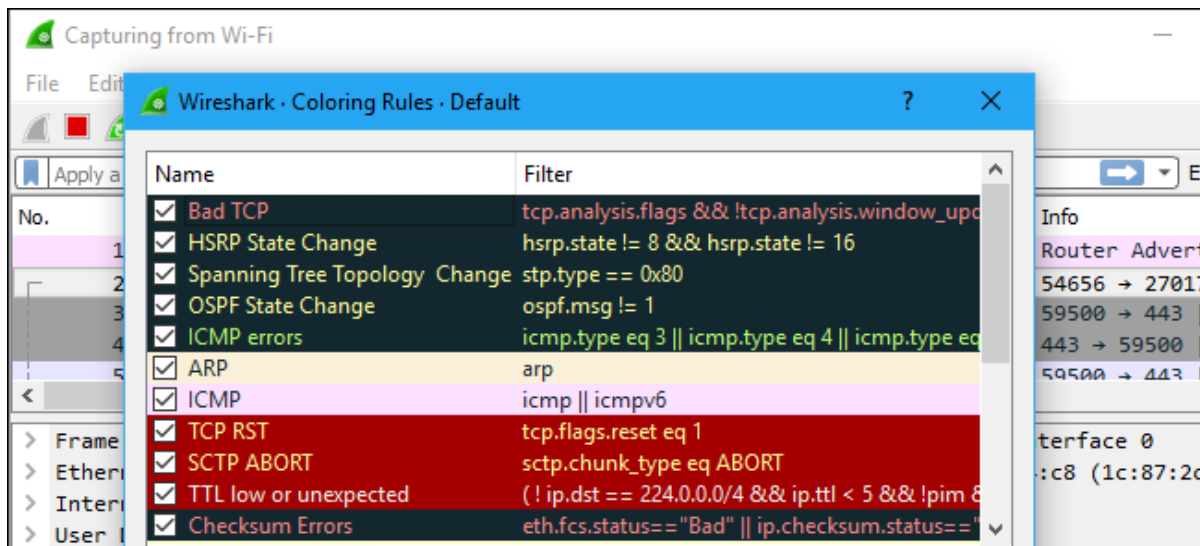
The “Packet Bytes” Pane

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.

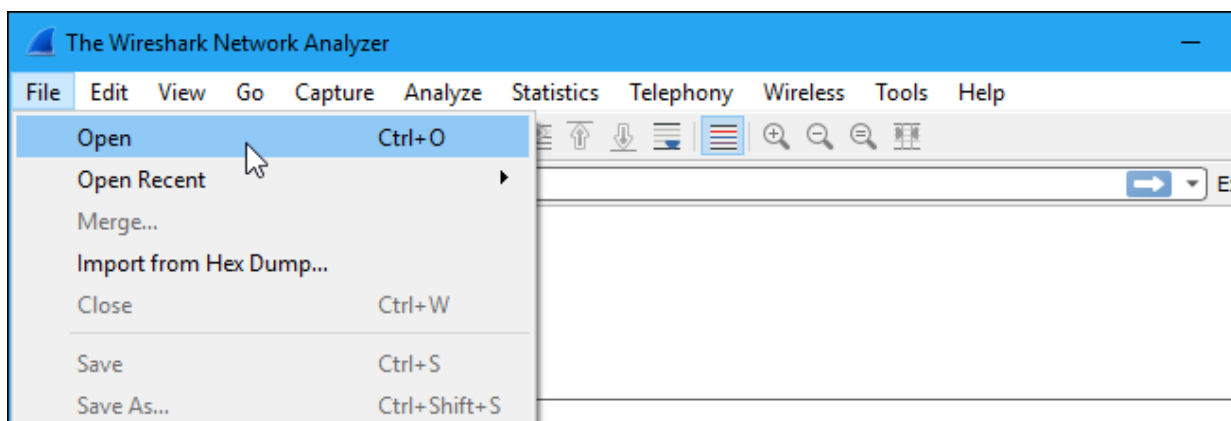
To view exactly what the color codes mean, click View > Coloring Rules. You can also customize and modify the coloring rules from here, if you like.



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.

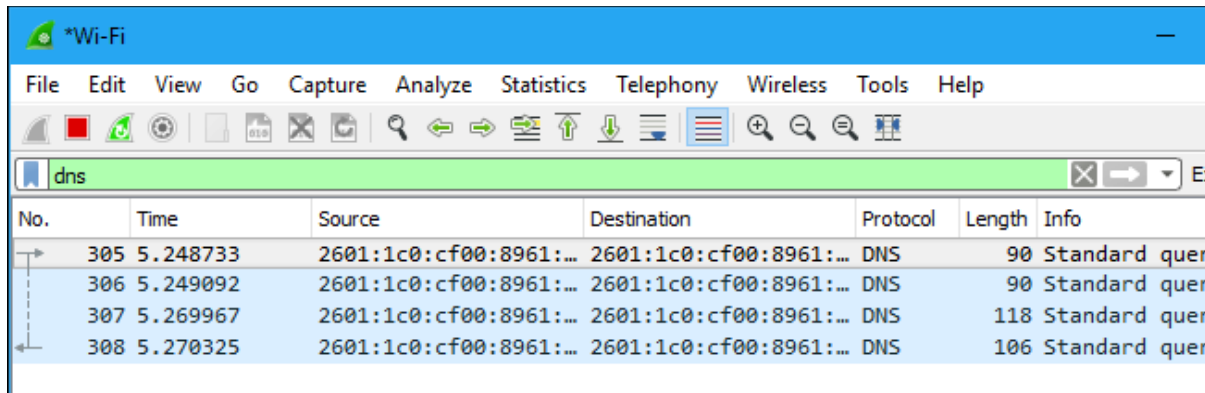


Filtering Packets

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

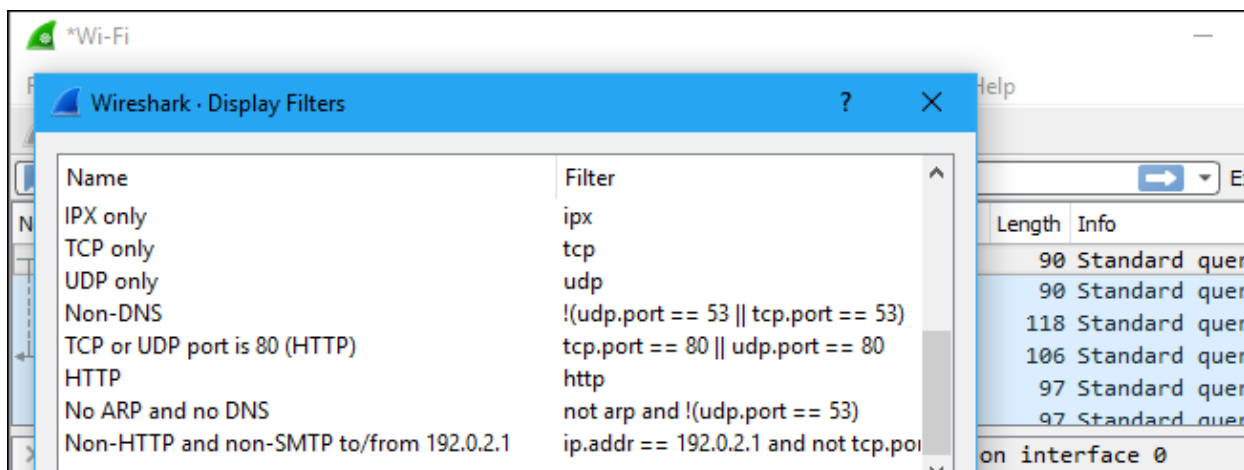
the traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark's filters come in.

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.



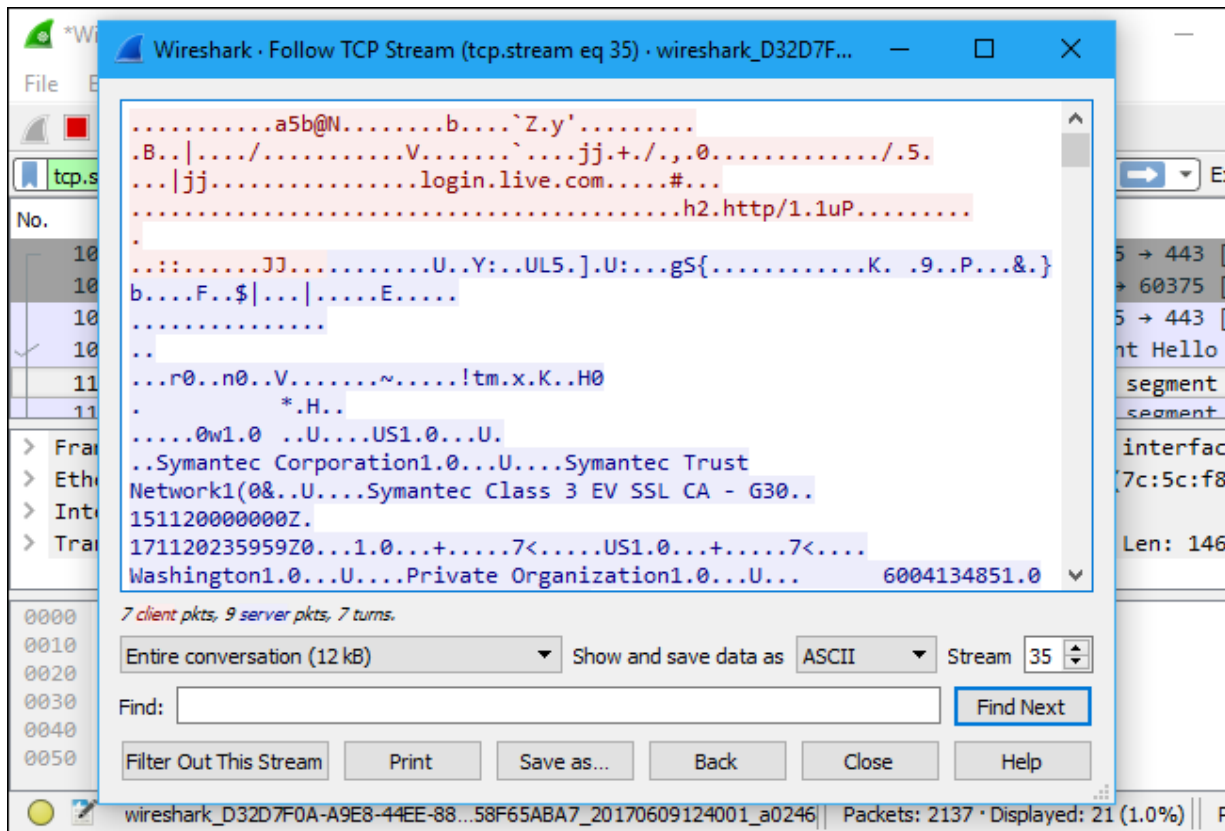
You can also click Analyze > Display Filters to choose a filter from among the default filters included in Wireshark. From here, you can add your own custom filters and save them to easily access them in the future.

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

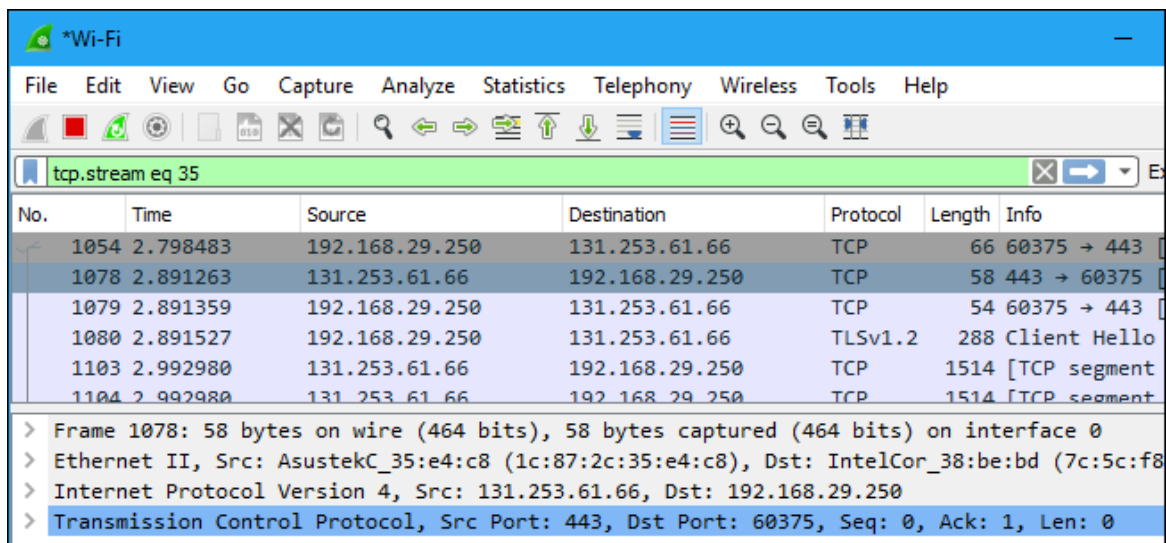


Another interesting thing you can do is right-click a packet and select Follow > TCP Stream.

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.

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 35

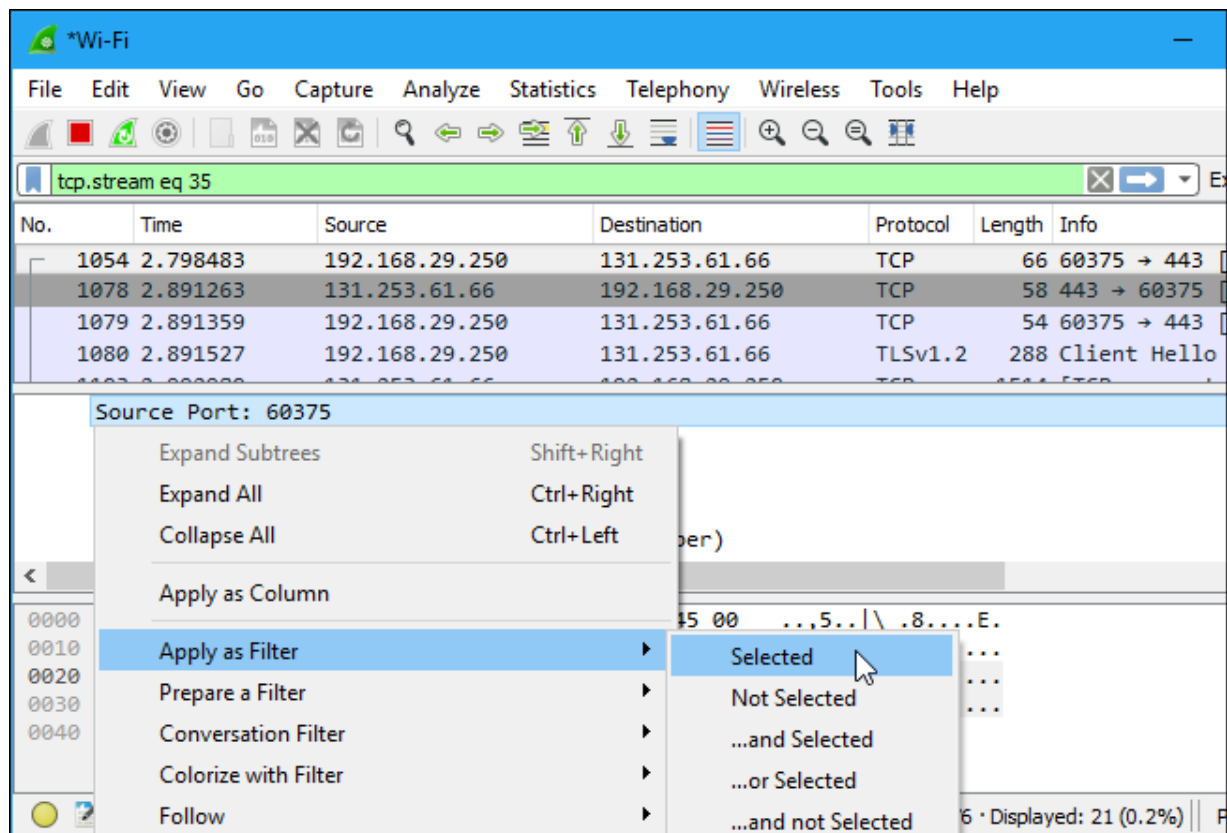
No.	Time	Source	Destination	Protocol	Length	Info
1054	2.798483	192.168.29.250	131.253.61.66	TCP	66	60375 → 443
1078	2.891263	131.253.61.66	192.168.29.250	TCP	58	443 → 60375
1079	2.891359	192.168.29.250	131.253.61.66	TCP	54	60375 → 443
1080	2.891527	192.168.29.250	131.253.61.66	TLSv1.2	288	Client Hello

▼ 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

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	..

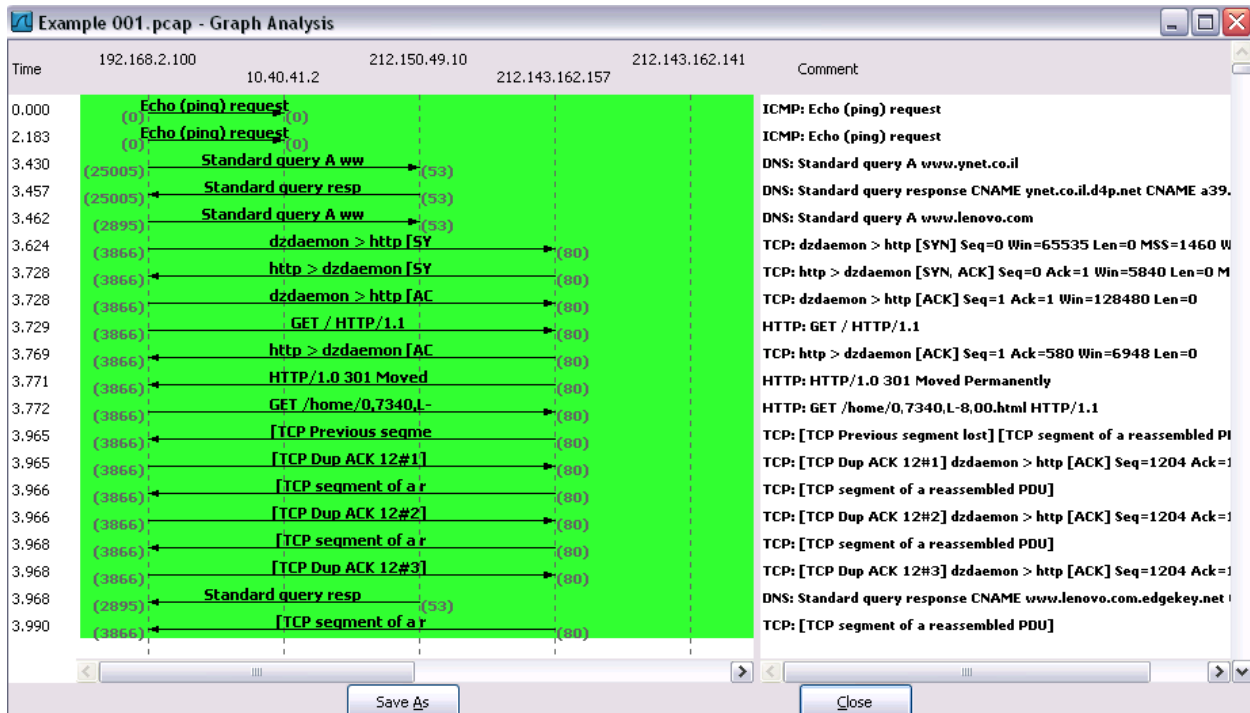
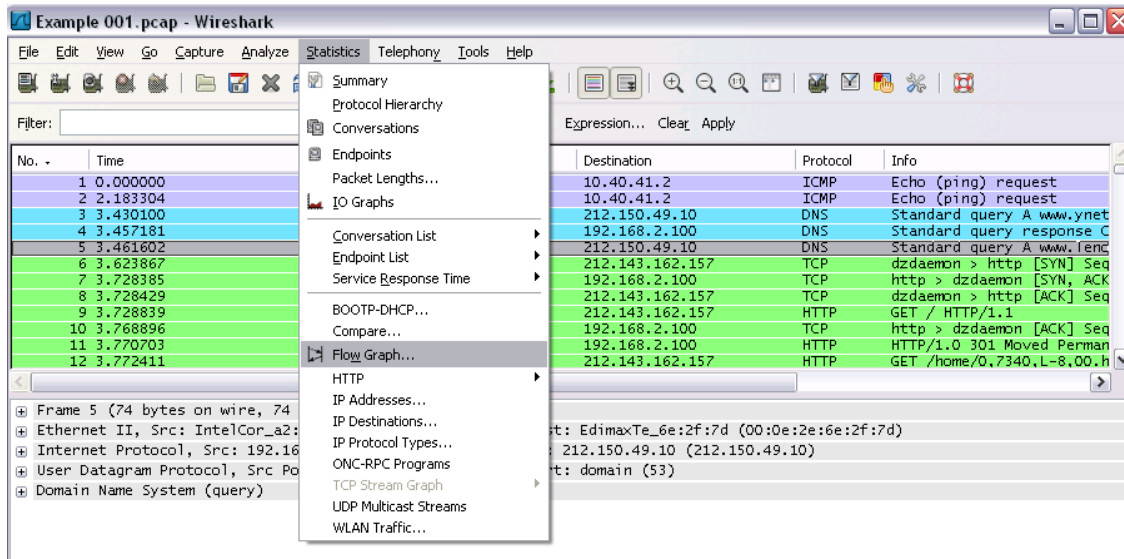
Encapsulation type (frame.encap_type) | Packets: 8136 · Displayed: 21 (0.3%)

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: 14 b

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

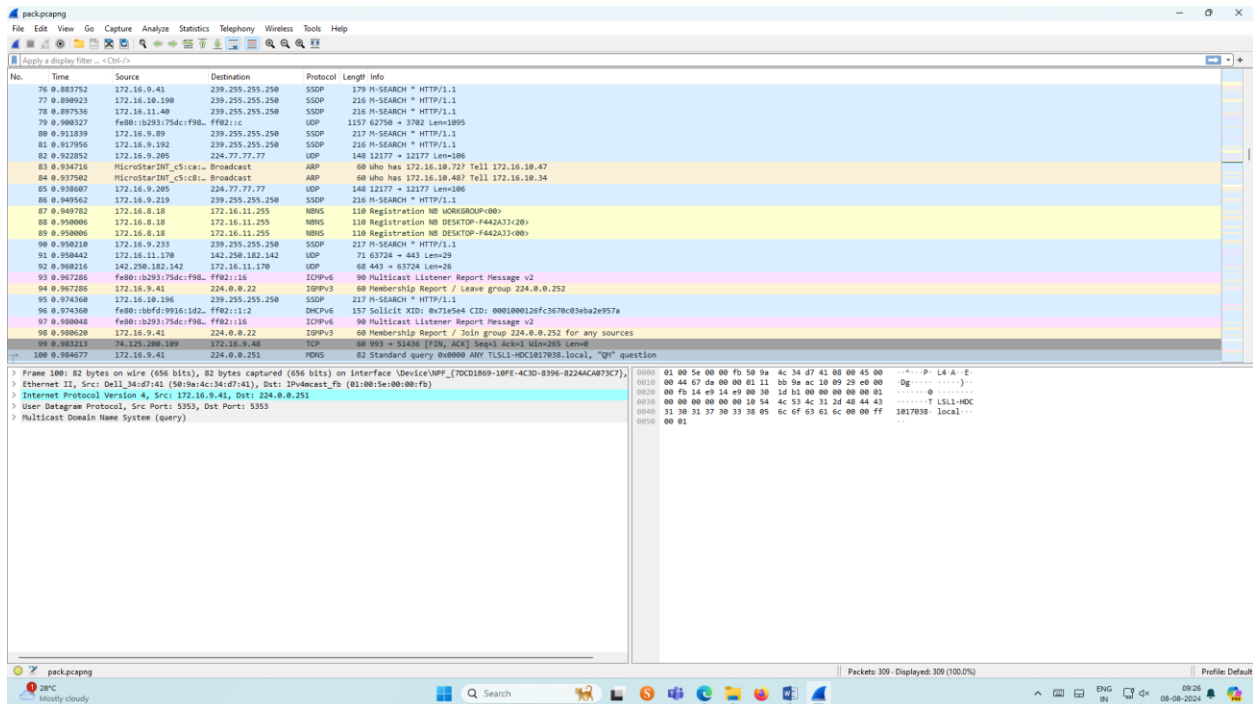
Exercises

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





The screenshot displays 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 opening files, saving, capturing, and analyzing. The main window is divided into three panes:

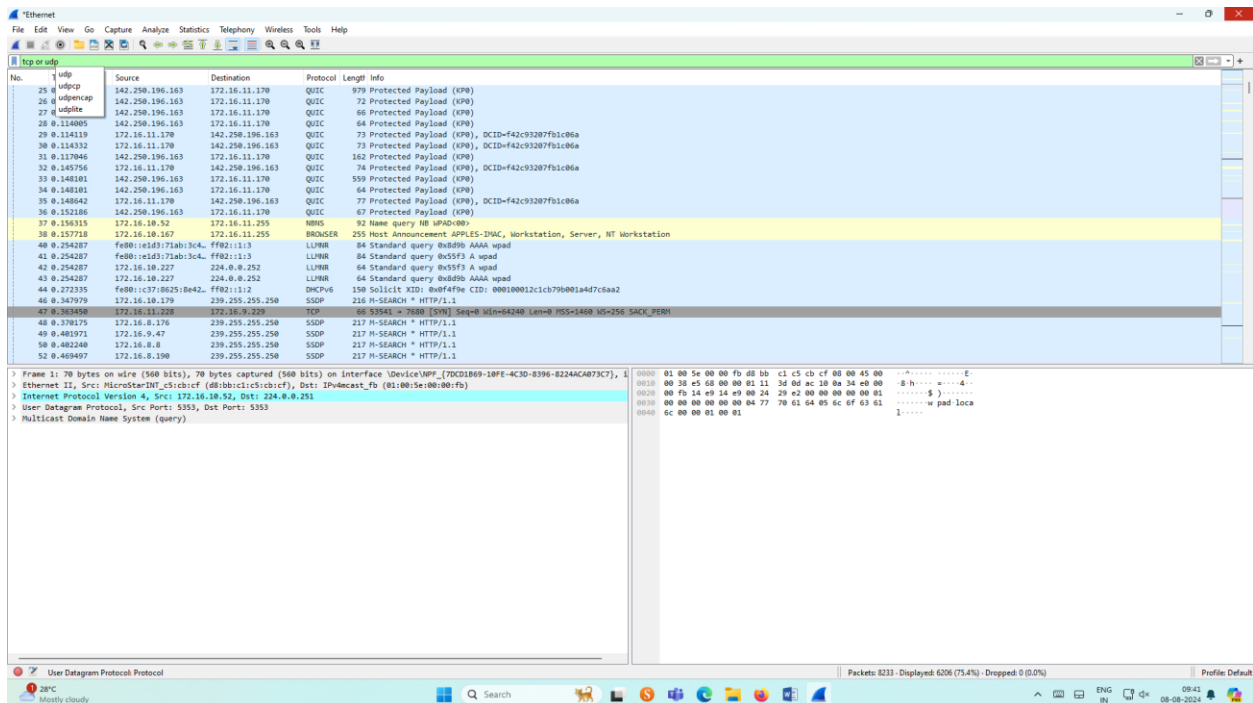
- Packet List:** Shows a list of 100 captured packets. The selected packet (No. 100) is highlighted in blue. The list includes columns for No., Time, Source, Destination, Protocol, Length, and Info.
- Packet Details:** Shows the hierarchical structure of the selected packet. The selected packet (No. 100) is expanded, showing the following layers:
 - Ethernet II, Src: Dell (08:00:27:00:00:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 - Internet Protocol Version 4, Src: 172.16.9.41, Dst: 224.0.0.251
 - User Datagram Protocol, Src Port: 5555, Dst Port: 5555
 - Multicast Domain Name System (query)
- Packet Bytes:** Shows the raw data of the selected packet in hexadecimal and ASCII format.

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

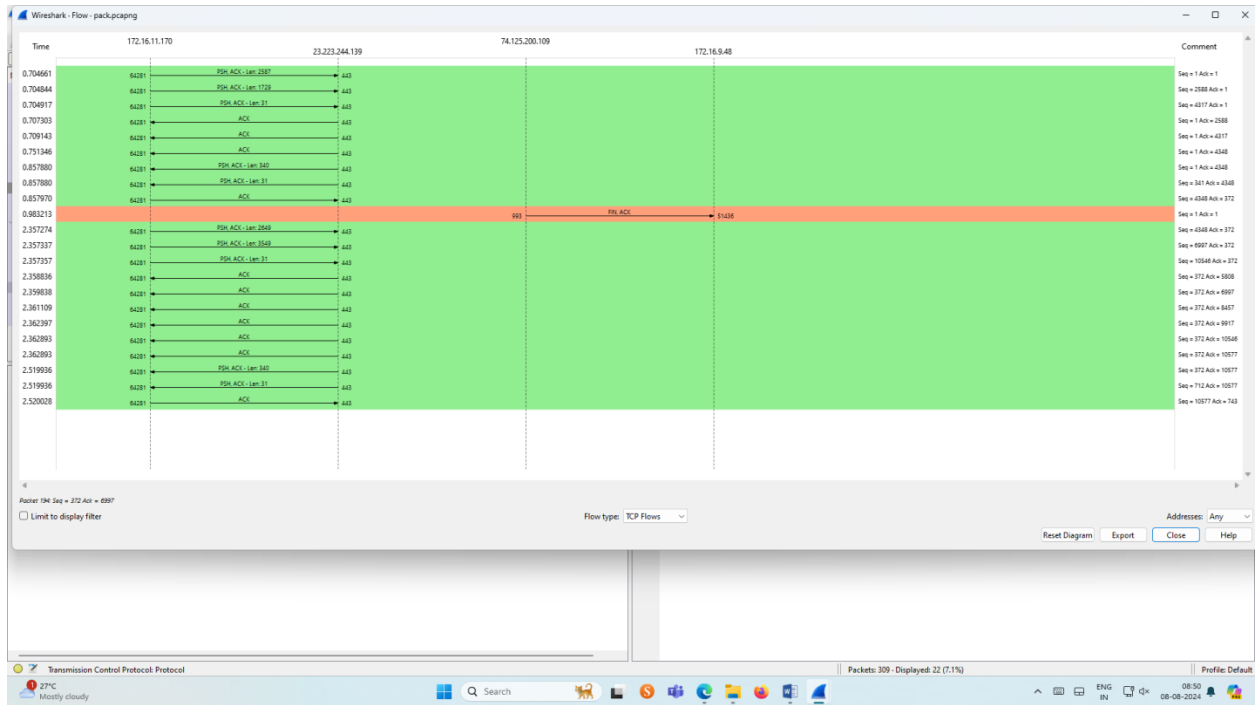
Procedure

- ☐ 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.

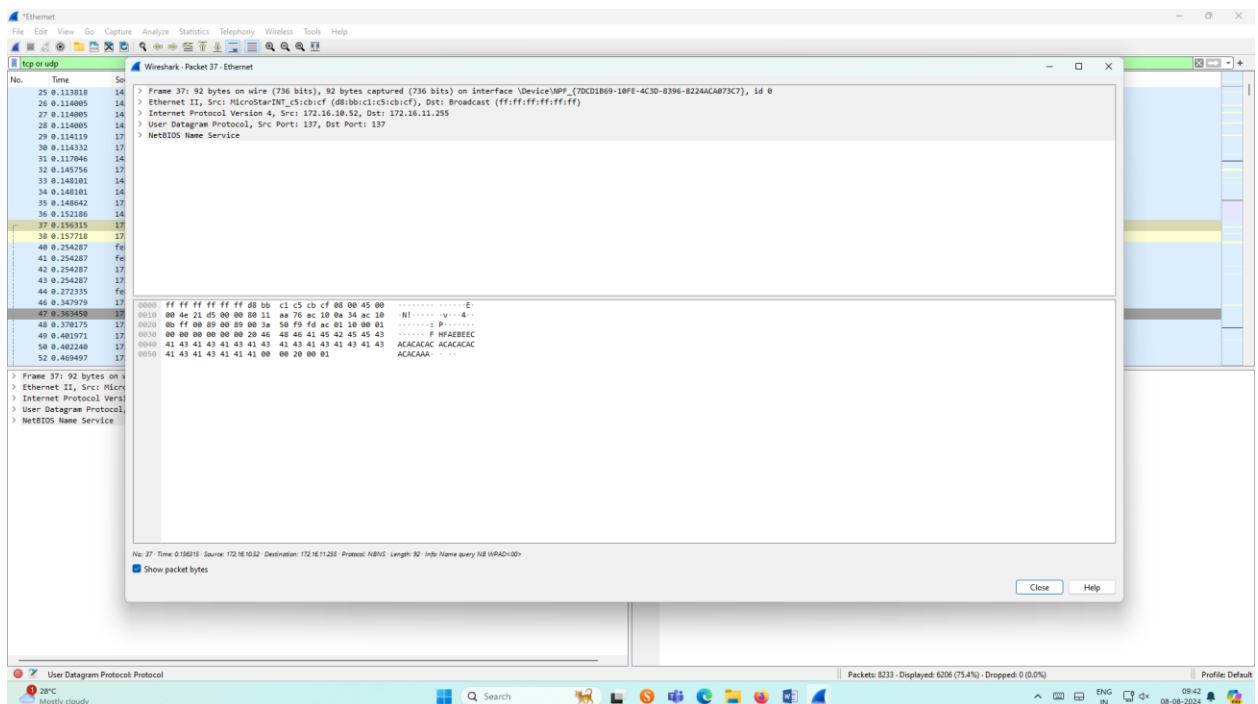
Output:



Flow Graph output




Inspecting the packets

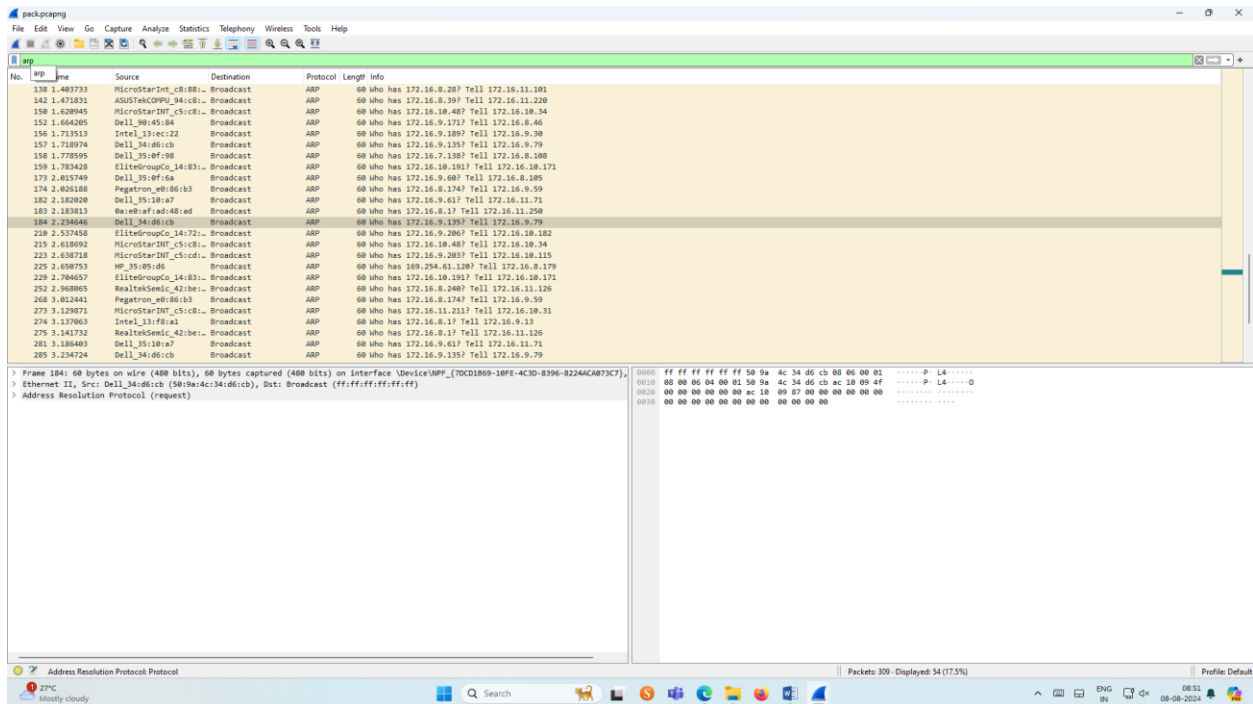


3.Create a Filter to display only ARP packets and inspect the packets.

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



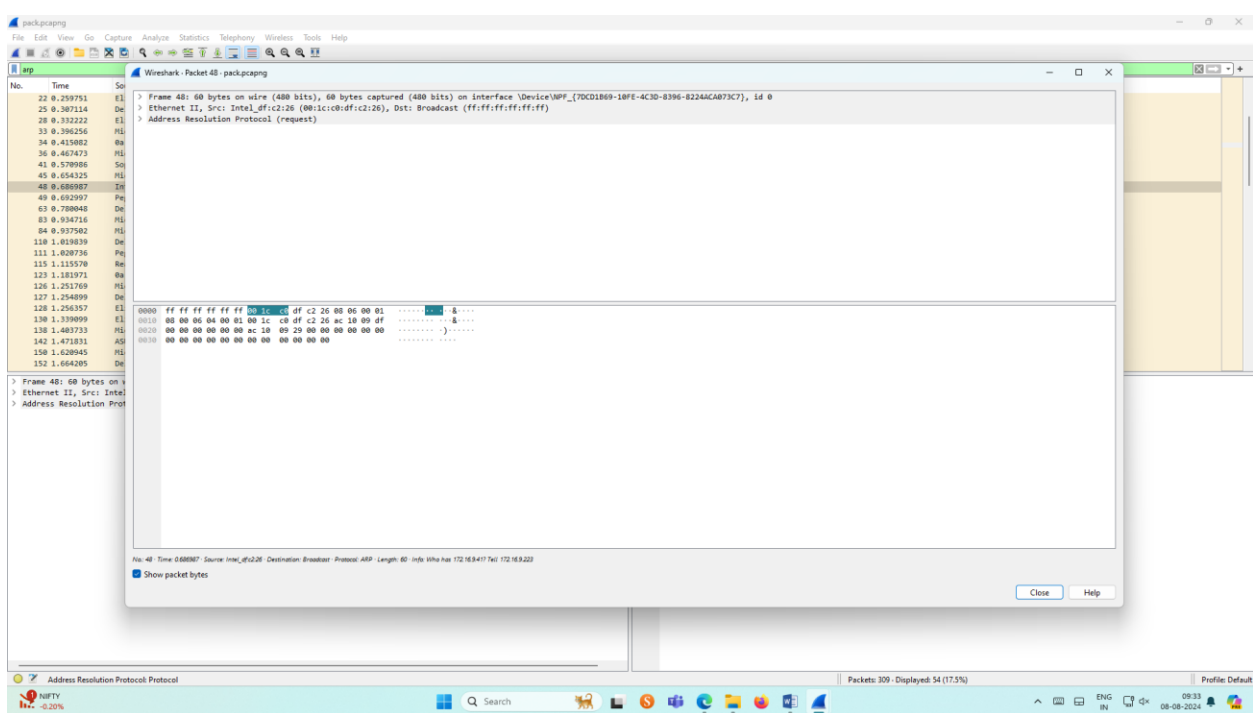
The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The main window is divided into three panes: Packet List, Packet Details, and Packet Bytes.

Packet List Pane: Shows a list of 309 captured packets. The selected packet is number 184, an ARP request from Dell_34:6b:cb to ff:ff:ff:ff:ff:ff. The list includes columns for No., Time, Source, Destination, Protocol, Length, and Info.

Packet Details Pane: Shows the structure of the selected packet. It is an Ethernet II frame, type I, Src: Dell_34:6b:cb (98:9e:4c:34:6b:cb), Dst: Broadcast (ff:ff:ff:ff:ff:ff). The packet is an Address Resolution Protocol (request) packet.



Packet Bytes Pane: Shows the raw data of the packet in hexadecimal and ASCII. The data starts with ff ff ff ff ff ff 50 9a 4c 34 6b cb 00 00 01, which corresponds to the Ethernet II header.

Inspecting the packets




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

Procedure

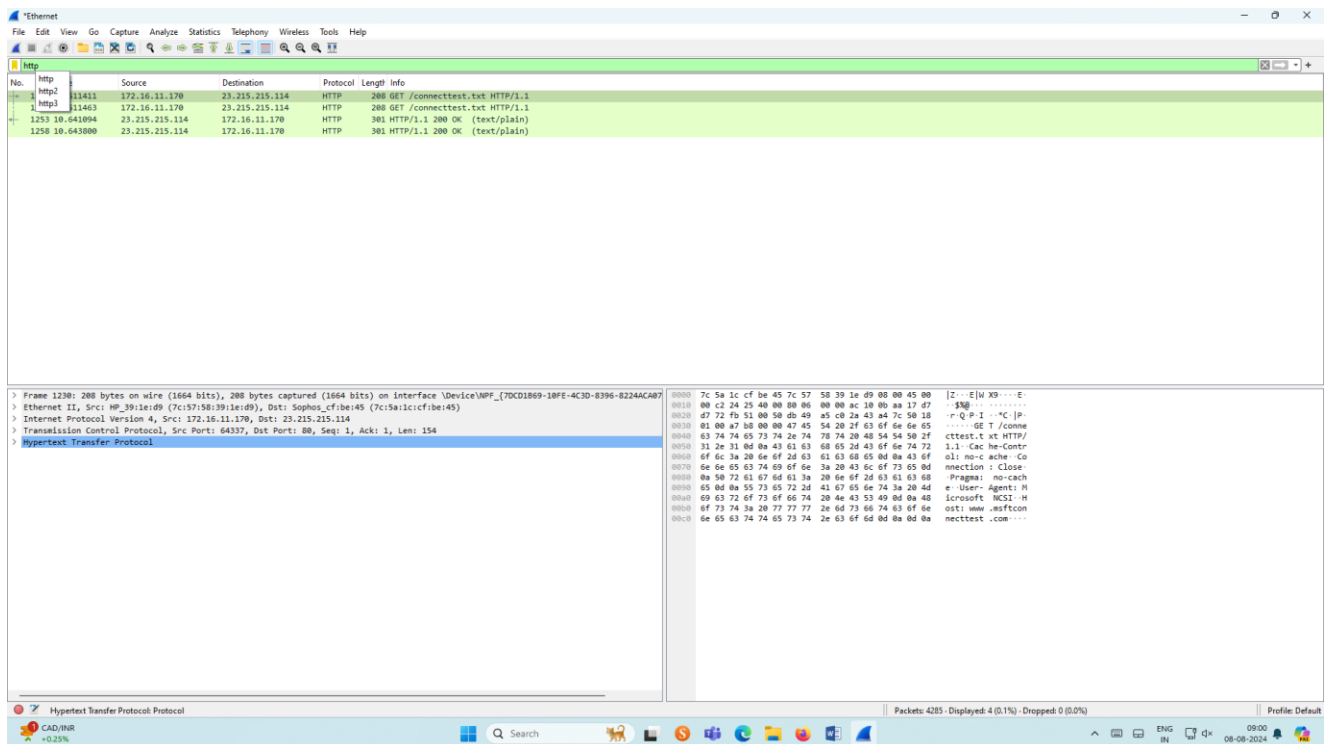
- ☐ Select Local Area Connection in Wireshark.
- ☐ Go to capture  Option
- ☐ Select stop capture automatically after 100 packets.
- ☐ Then click Start capture.
- ☐ Search DNS packets in search bar.
- ☐ To see flow graph click Statistics  Flow graph.
- ☐ Save the packets.

Output

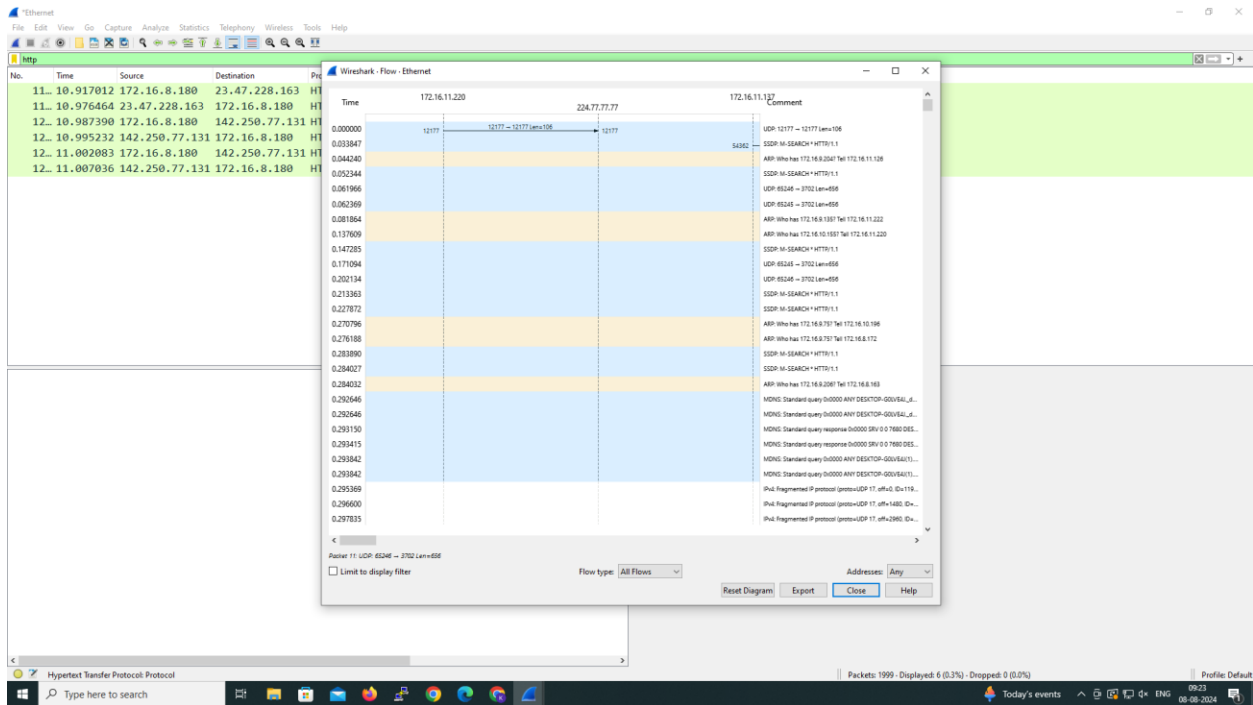
Procedure

- ☐ 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.

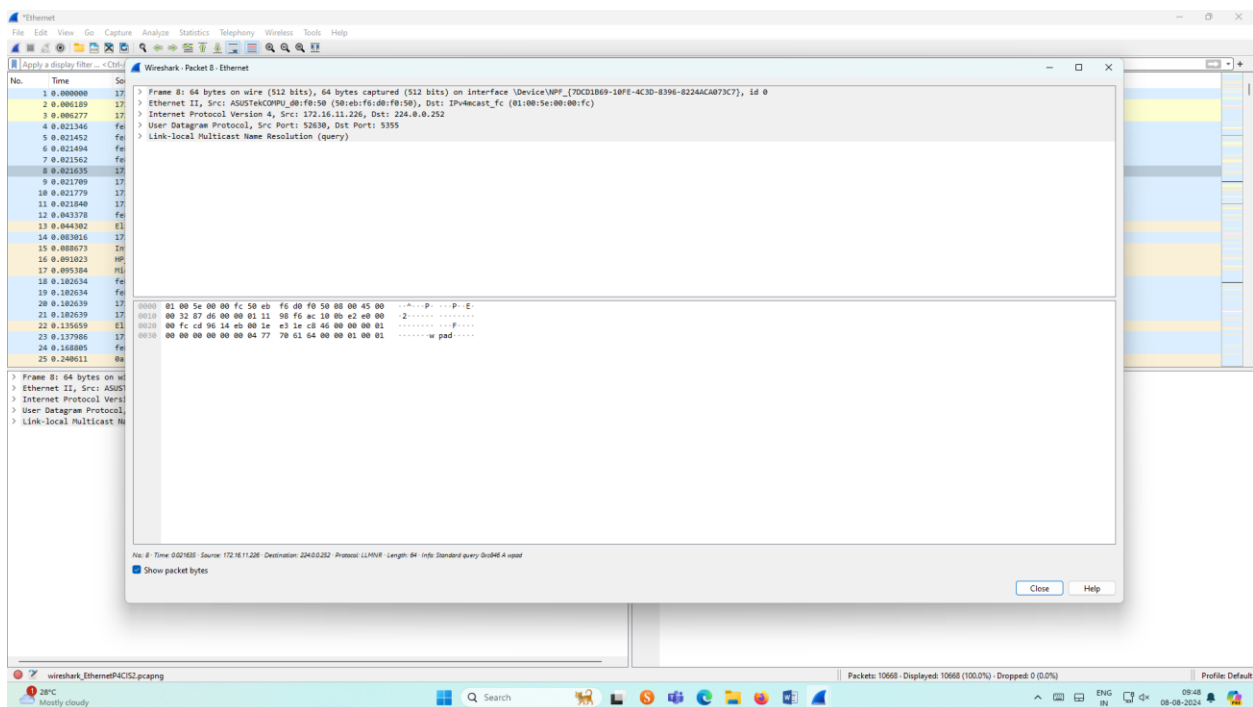
Output



Flow Graph output




Inspecting the packets

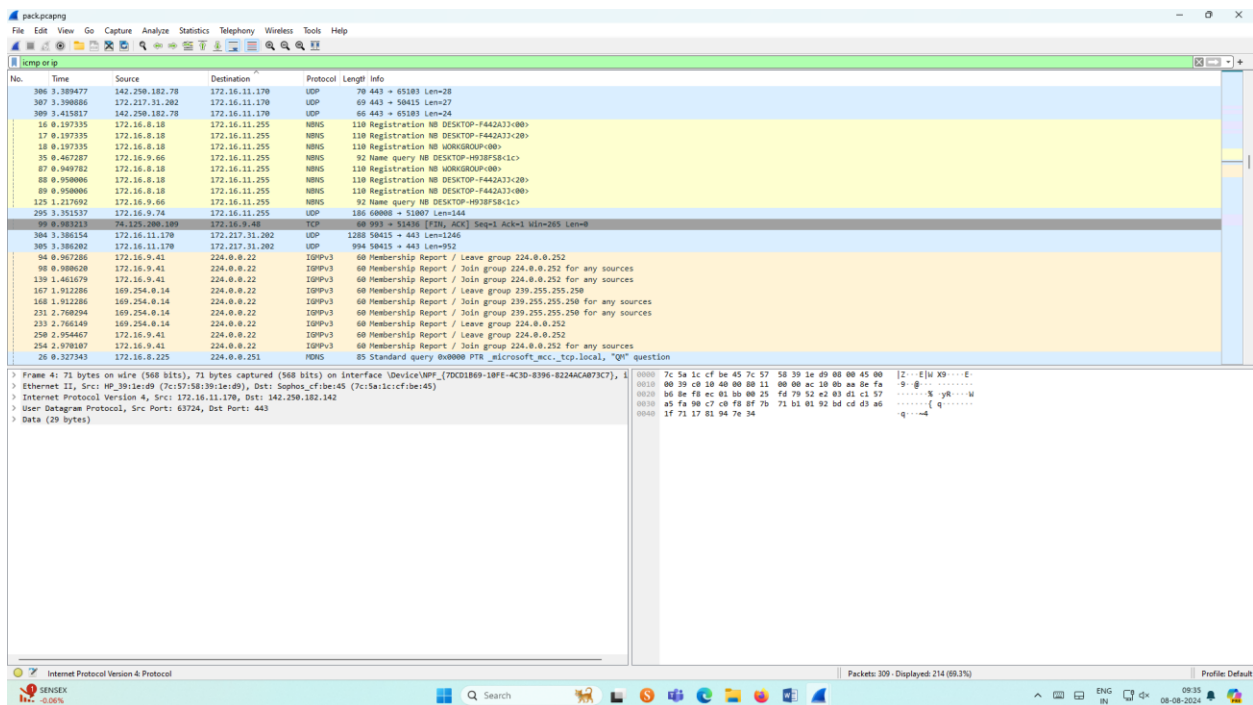


6.Create a Filter to display only IP/ICMP packets and inspect the packets.

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

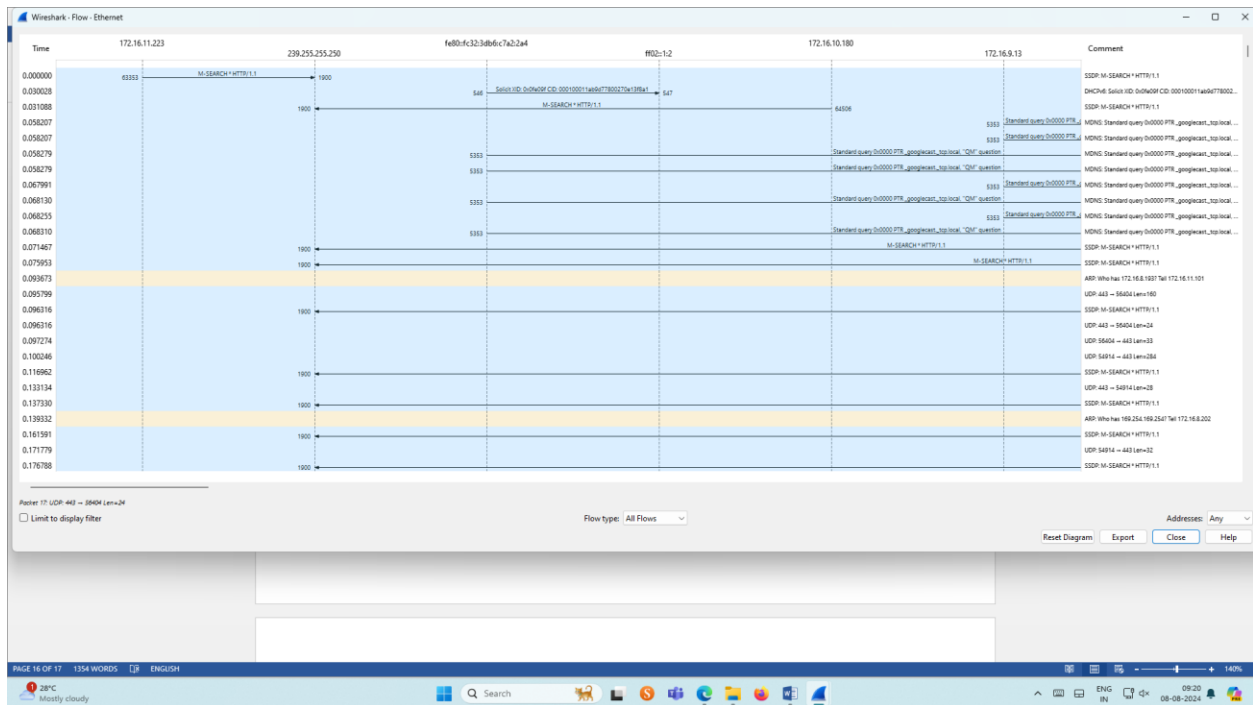


The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains icons for file operations, capture control, and analysis. The main packet list pane shows a table of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The selected packet (No. 4) is an ICMP Echo (ping) request from 172.16.11.178 to 172.16.11.255. The packet details pane on the right shows the structure of the ICMP Echo request, including the type (8), code (0), and identifier (0). The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

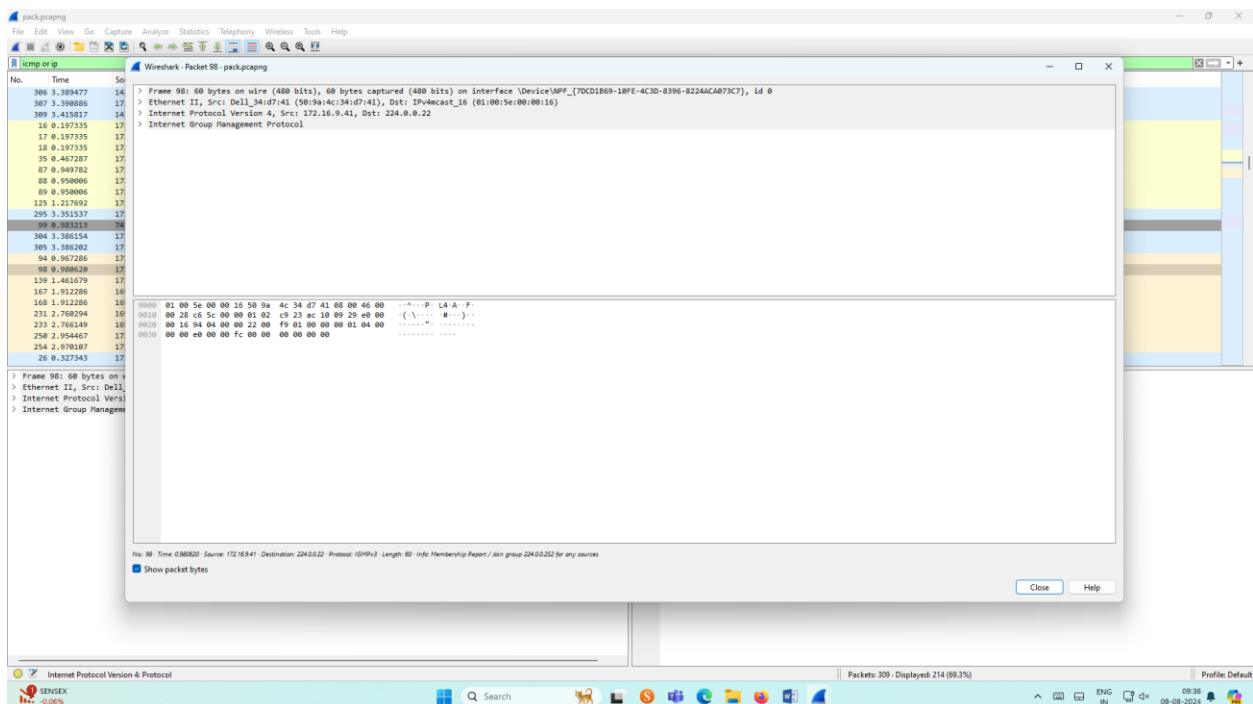
No.	Time	Source	Destination	Protocol	Length	Info
386	3.388477	142.250.182.78	172.16.11.178	UDP	78	443 → 55183 Len=28
387	3.398886	172.16.11.178	172.16.11.178	UDP	68	443 → 50415 Len=27
389	3.415817	142.250.182.78	172.16.11.178	UDP	66	443 → 55183 Len=24
16	0.197335	172.16.8.18	172.16.11.255	NBNS	118	Registration NB DESKTOP-F442A312B0
17	0.197335	172.16.8.18	172.16.11.255	NBNS	118	Registration NB DESKTOP-F442A312B0
18	0.197335	172.16.8.18	172.16.11.255	NBNS	118	Registration NB WORKGROUP000
35	0.467287	172.16.9.66	172.16.11.255	NBNS	92	Name query NB DESKTOP-H93P581C1
87	0.940782	172.16.8.18	172.16.11.255	NBNS	118	Registration NB WORKGROUP000
88	0.950006	172.16.8.18	172.16.11.255	NBNS	118	Registration NB DESKTOP-F442A312B0
89	0.950006	172.16.8.18	172.16.11.255	NBNS	118	Registration NB DESKTOP-F442A312B0
125	1.217092	172.16.9.66	172.16.11.255	NBNS	92	Name query NB DESKTOP-H93P581C1
295	3.351537	172.16.9.74	172.16.11.255	UDP	186	60088 → 51807 Len=144
99	0.981213	74.125.200.189	172.16.0.48	TCP	60	893 → 51436 [FIN, ACK] Seq=1 Win=285 Len=0
384	3.386154	172.16.11.178	172.16.11.252	UDP	128	50415 → 443 Len=146
385	3.386182	172.16.11.178	172.16.11.252	UDP	94	50415 → 443 Len=92
94	0.967286	172.16.9.41	224.0.0.252	IGMPv3	60	Membership Report / Leave group 224.0.0.252
98	0.980620	172.16.9.41	224.0.0.252	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any sources
119	1.461679	172.16.9.41	224.0.0.252	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any sources
167	1.912286	169.254.0.14	224.0.0.252	IGMPv3	60	Membership Report / Leave group 239.255.255.250
168	1.912286	169.254.0.14	224.0.0.252	IGMPv3	60	Membership Report / Join group 239.255.255.250 for any sources
231	2.760294	169.254.0.14	224.0.0.252	IGMPv3	60	Membership Report / Join group 239.255.255.250 for any sources
233	2.760149	169.254.0.14	224.0.0.252	IGMPv3	60	Membership Report / Leave group 224.0.0.252
250	2.954467	172.16.9.41	224.0.0.252	IGMPv3	60	Membership Report / Leave group 224.0.0.252
254	2.970187	172.16.9.41	224.0.0.252	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any sources
26	0.327343	172.16.0.225	224.0.0.251	NBNS	85	Standard query 8x0000 PTR_microsoft_mcc_tcp_local, "QM" question

Frame 4: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{70C1D869-18FE-4C3D-B396-8224AC4073C7}, 1
> Ethernet II, Src: HP_39:1e:d9 (7c:57:58:39:1e:d9), Dst: Sophos_fc:be:a5 (7c:5a:1c:cf:be:a5)
> Internet Protocol Version 4, Src: 172.16.11.178, Dst: 142.250.182.142
> User Datagram Protocol, Src Port: 63724, Dst Port: 443
> Data (29 bytes)
0000 7c 5a 1c cf be a5 7c 57 58 39 1e d9 00 00 45 00 | 2...E|H X3...E:
0010 00 39 c8 10 40 00 88 11 00 00 ac 10 00 aa be fa | 9:8...-...
0020 b6 be f8 ac 00 b0 00 25 fd 79 52 a2 00 d1 c1 57 |X yb...W
0030 a5 fa 08 cf c8 f8 ff 7b 71 b1 01 92 bf cd d3 a0 |{ q.....
0040 1f 71 17 81 94 7e 34 | q.....4

Flow Graph output




Inspecting the packets

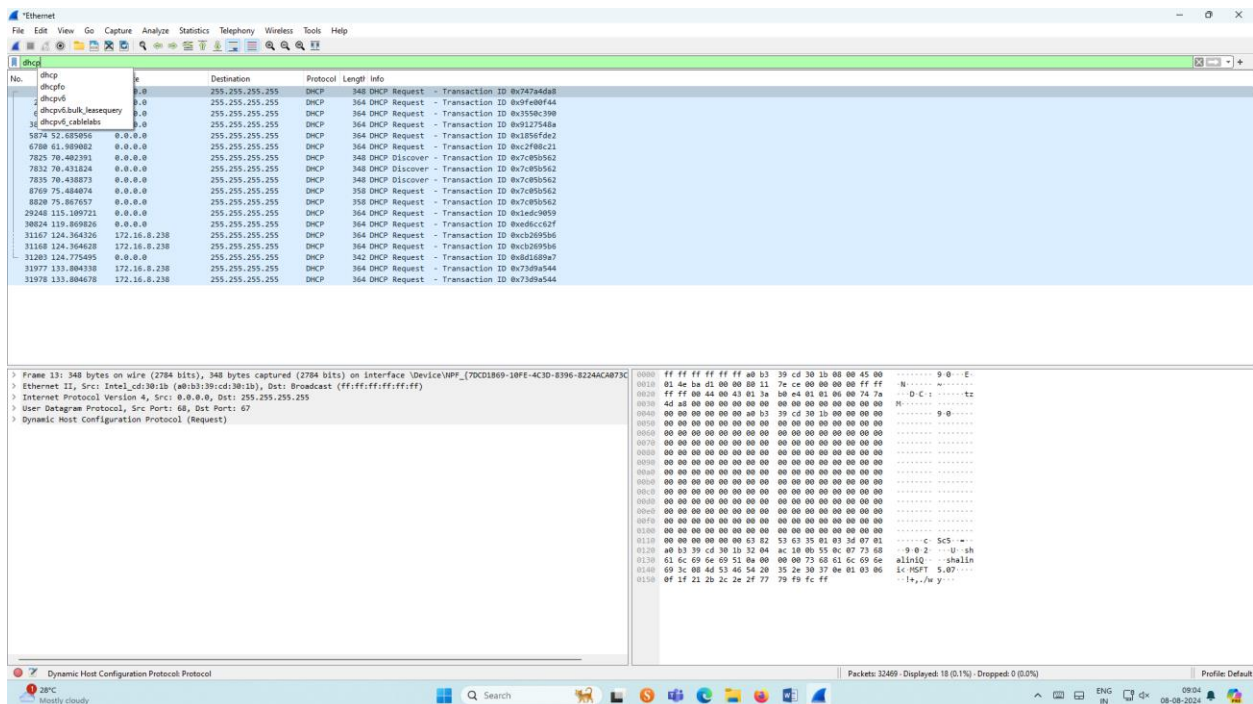


7.Create a Filter to display only DHCP packets and inspect the packets.

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, Tools, and Help. The packet list pane on the left shows a list of captured packets, with the first few being DHCP-related. The packet details pane on the right shows the structure of a DHCP request packet, including the Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Dynamic Host Configuration Protocol (Request) layers. The packet bytes pane at the bottom shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x7474d4d4
2	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x9f80f444
3	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x358c3900
4	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x8127444a
5	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x1856fde2
6	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0xc2f80c21
7	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
8	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
9	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
10	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
11	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
12	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
13	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
14	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
15	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
16	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
17	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
18	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
19	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
20	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
21	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
22	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
23	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
24	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
25	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
26	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
27	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
28	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
29	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
30	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
31	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
32	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
33	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
34	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
35	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
36	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
37	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
38	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
39	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
40	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
41	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
42	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
43	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
44	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
45	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
46	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
47	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
48	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
49	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
50	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
51	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
52	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
53	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
54	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
55	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
56	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
57	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
58	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
59	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
60	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
61	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
62	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
63	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
64	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
65	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
66	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
67	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
68	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
69	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
70	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
71	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
72	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
73	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
74	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
75	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
76	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
77	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
78	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
79	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
80	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
81	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
82	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
83	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
84	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
85	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
86	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
87	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
88	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
89	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
90	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
91	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
92	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
93	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
94	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
95	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
96	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
97	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
98	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
99	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562
100	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c80562

Frame 13: 348 bytes on wire (2784 bits), 348 bytes captured (2784 bits) on interface \Device\NPF_{70CD1869-10FE-4C3D-8396-8224AC873C} (0.0.0.0) on interface 0.0.0.0
Ethernet II, Src: Intel_c8:30:1b (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)

0000 ff ff ff ff ff ff a8 b3 39 cd 30 1b 00 00 45 009.0.E
0010 01 4e be d1 00 00 08 11 7e ce 00 00 00 ff ffM.C.....
0020 ff ff 00 4a 00 43 01 1a 1b e4 01 00 00 74 7aQ.C.....
0030 4d a8 00 00 00 00 00 00 00 00 00 00 00 00M.....
0040 00 00 00 00 00 00 a8 b3 39 cd 30 1b 00 00 009.....
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0110 00 00 00 00 00 00 63 82 53 63 75 01 34 07 01C.S.....
0120 a8 b3 39 cd 30 1b 32 04 ac 18 0b 55 0c 07 73 689.0.2...U..sh
0130 61 5c 69 6e 69 51 0a 00 00 00 73 68 61 6c 09 6ealiniq...shalin
0140 69 3c 08 4d 53 46 54 20 35 24 30 77 00 01 03 00[.HOST.5.87
0150 0f 1f 21 2b 2c 2e 2f 77 79 79 fc ff[.y..y.....

Inspecting the packets

