

CS23532  
NAME:B.MADHAN KUMAR  
ROLL NO:231901028

## **Ex No:4A      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:**

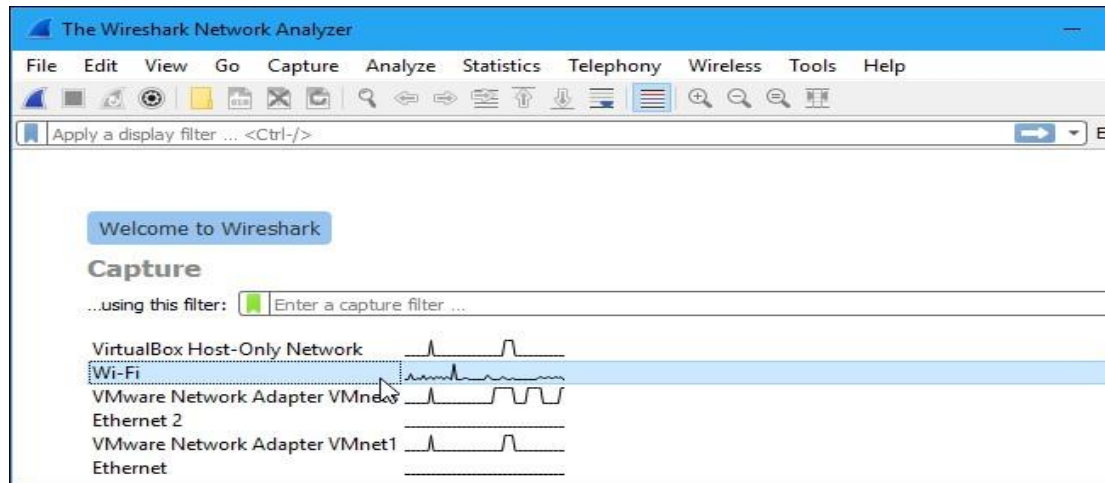
- Network administrators: troubleshoot network problems
- Network security engineers: examine security problems
- Developers: debug protocol implementations
- People: learn **network protocol internals**

### **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**

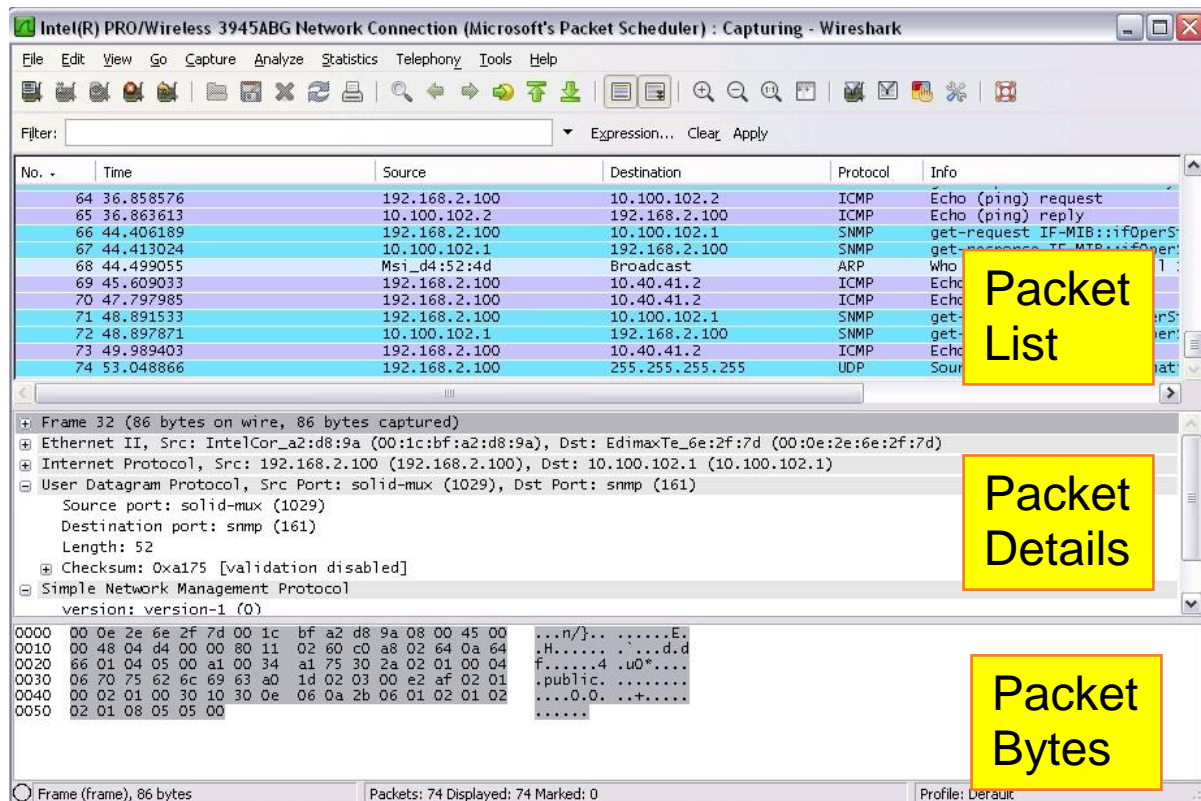
After downloading and installing Wireshark, launch it and double-click the name of a network interface under Capture to start capturing packets on that interface



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.

CS23532  
NAME:B.MADHAN KUMAR  
ROLL NO:231901028



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.

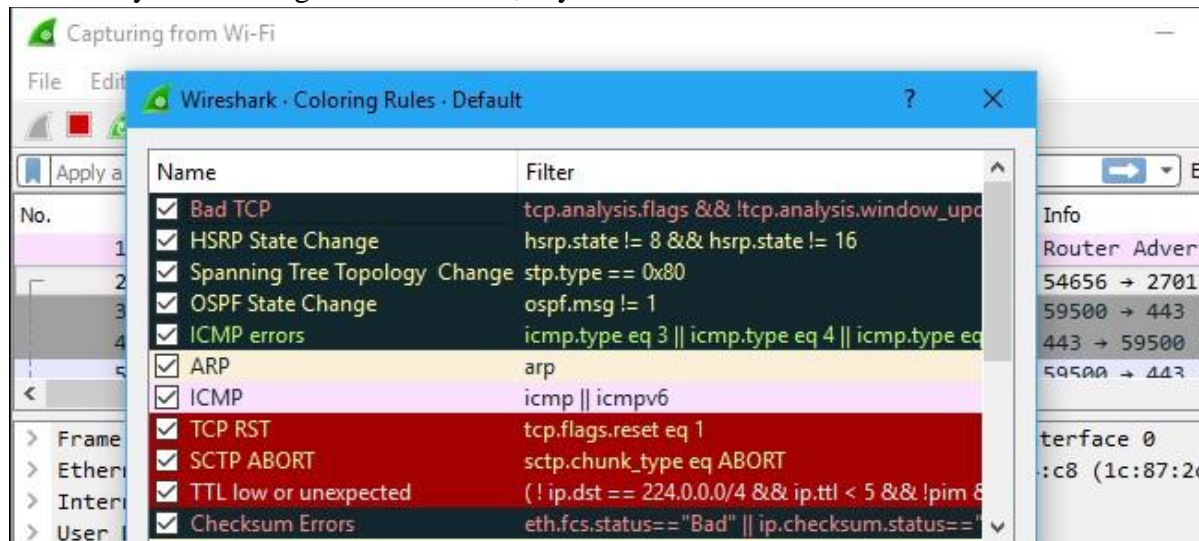
## The “Packet Bytes” Pane

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.

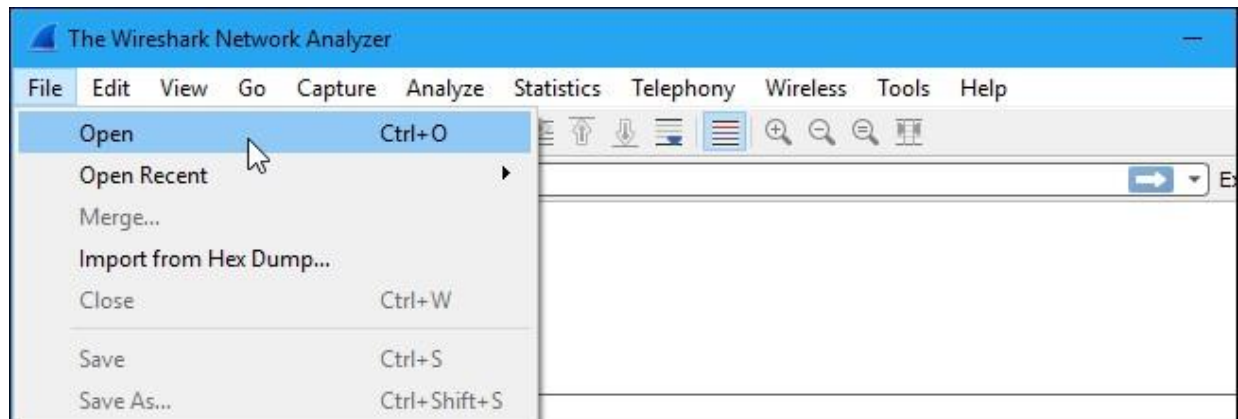


## Sample Captures

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.

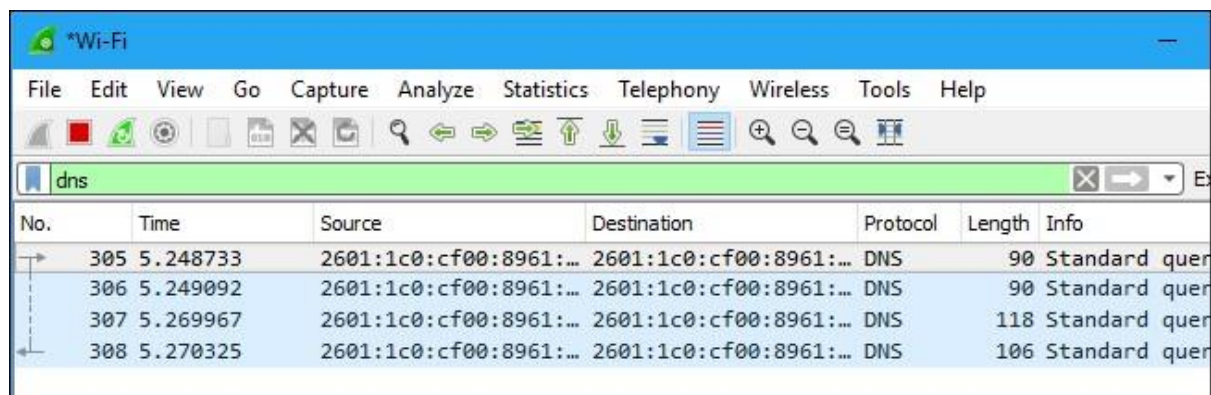
CS23532  
NAME:B.MADHAN KUMAR  
ROLL NO:231901028



## 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.

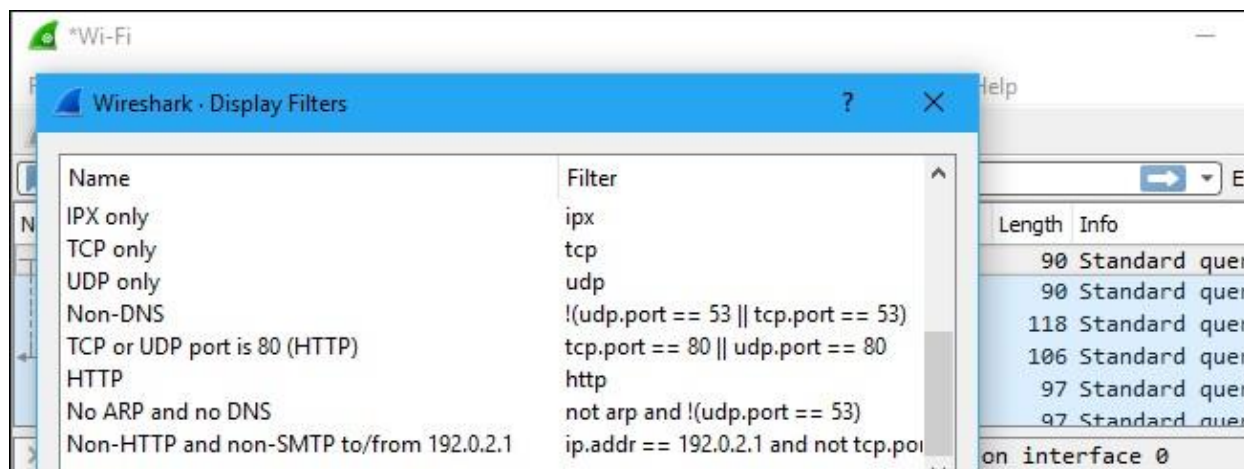
The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type `—dns` and you'll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.



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.

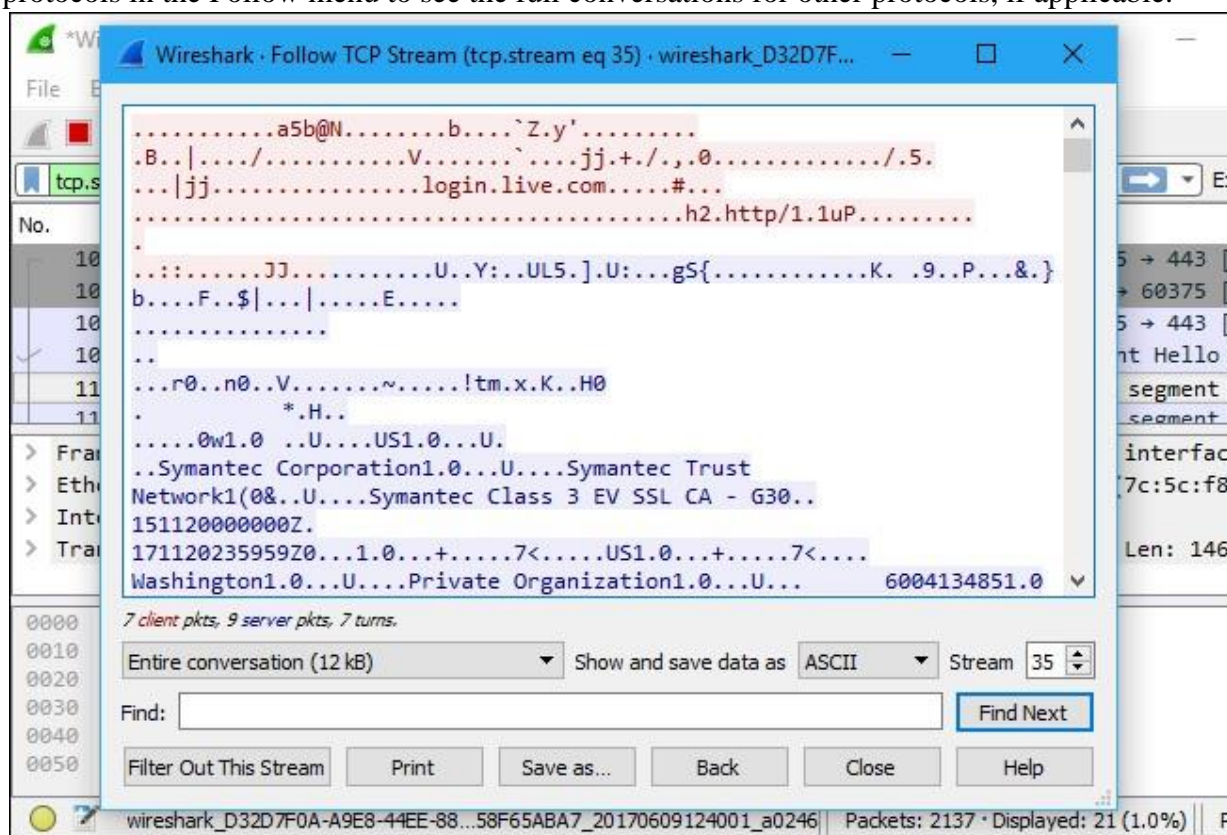
For more information on Wireshark's display filtering language, read the [Building display filter expressions](#) page in the official Wireshark documentation.





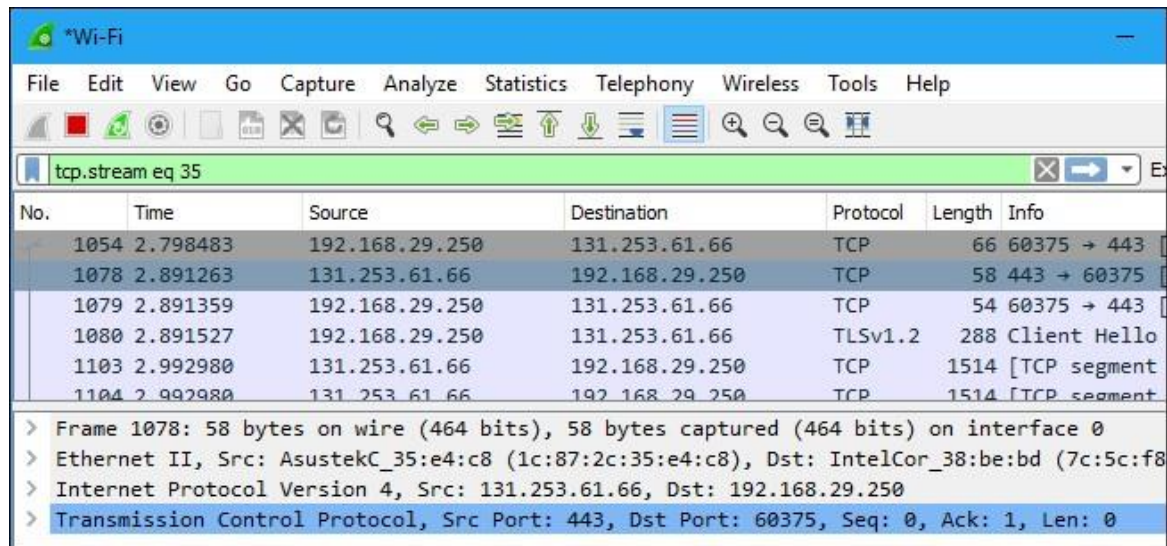
Another interesting thing you can do is right-click a packet and select Follow > TCP Stream.

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.

CS23532  
NAME: B.MADHAN KUMAR  
ROLL NO: 231901028



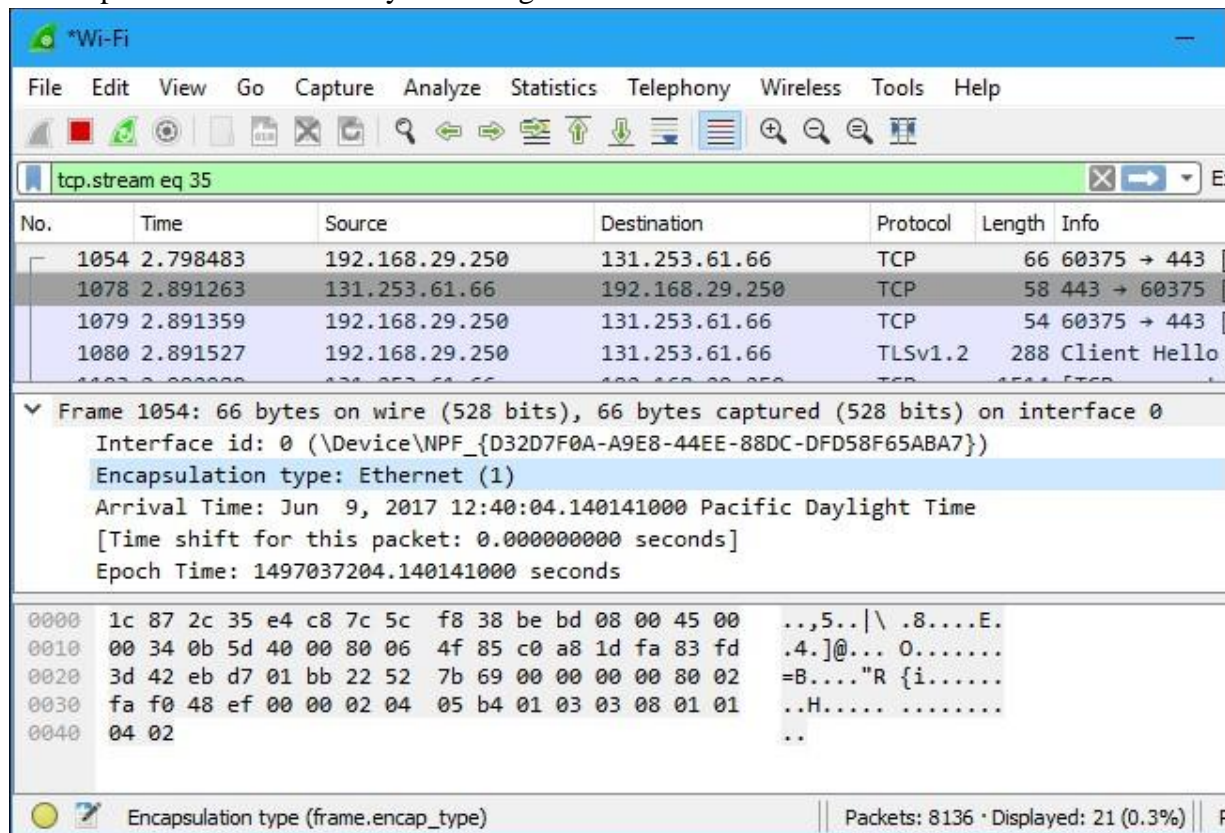
Wireshark packet capture window showing a list of packets. The selected packet (1078) details are expanded below the list.

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
1103	2.992980	131.253.61.66	192.168.29.250	TCP	1514	[TCP segment
1104	2.992980	131.253.61.66	192.168.29.250	TCP	1514	[TCP segment

Frame 1078: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface 0  
Ethernet II, Src: AsustekC\_35:e4:c8 (1c:87:2c:35:e4:c8), Dst: IntelCor\_38:be:bd (7c:5c:f8  
Internet Protocol Version 4, Src: 131.253.61.66, Dst: 192.168.29.250  
Transmission Control Protocol, Src Port: 443, Dst Port: 60375, Seq: 0, Ack: 1, Len: 0

## Inspecting Packets

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



Wireshark packet capture window showing details of packet 1054. The details pane shows the encapsulation type, arrival time, and epoch time. The packet bytes are displayed in hexadecimal and ASCII.

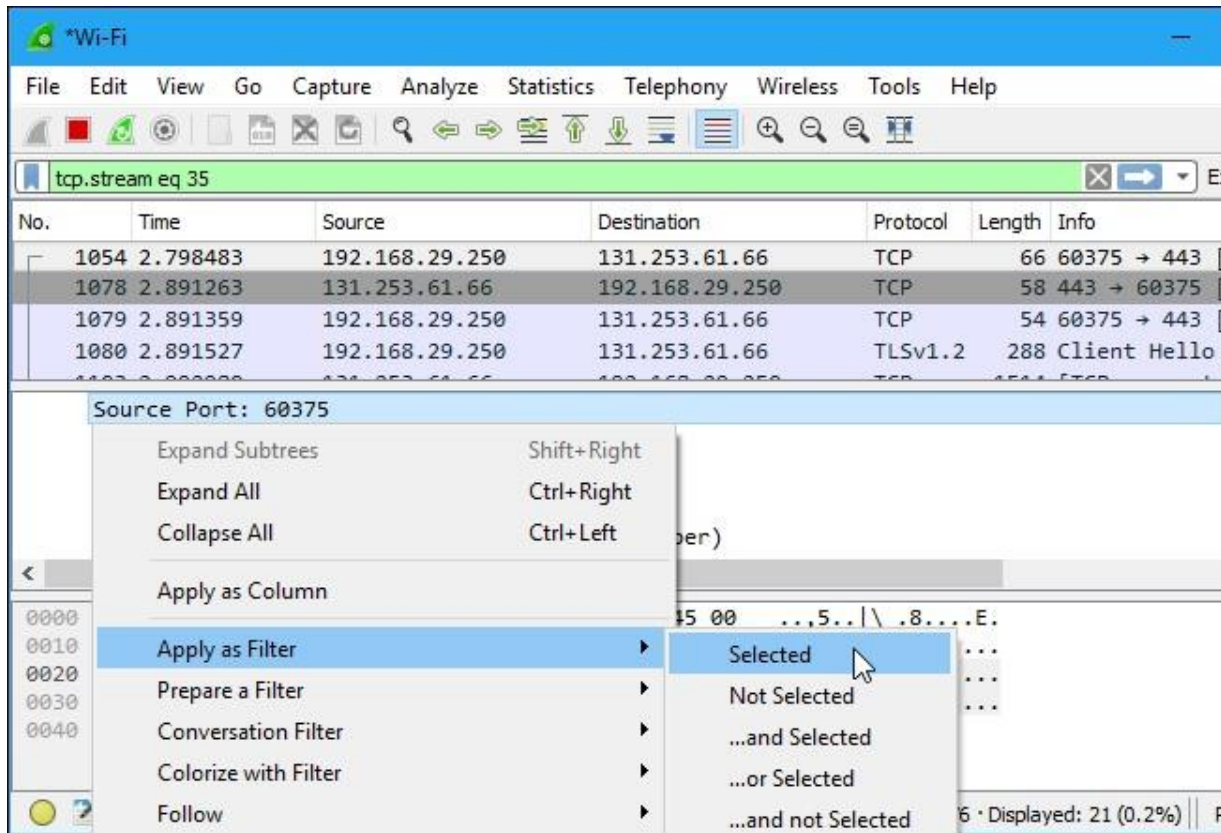
No.	Time	Source	Destination	Protocol	Length	Info
1054	2.798483	192.168.29.250	131.253.61.66	TCP	66	60375 → 443
1078	2.891263	131.253.61.66	192.168.29.250	TCP	58	443 → 60375
1079	2.891359	192.168.29.250	131.253.61.66	TCP	54	60375 → 443
1080	2.891527	192.168.29.250	131.253.61.66	TLSv1.2	288	Client Hello

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

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.

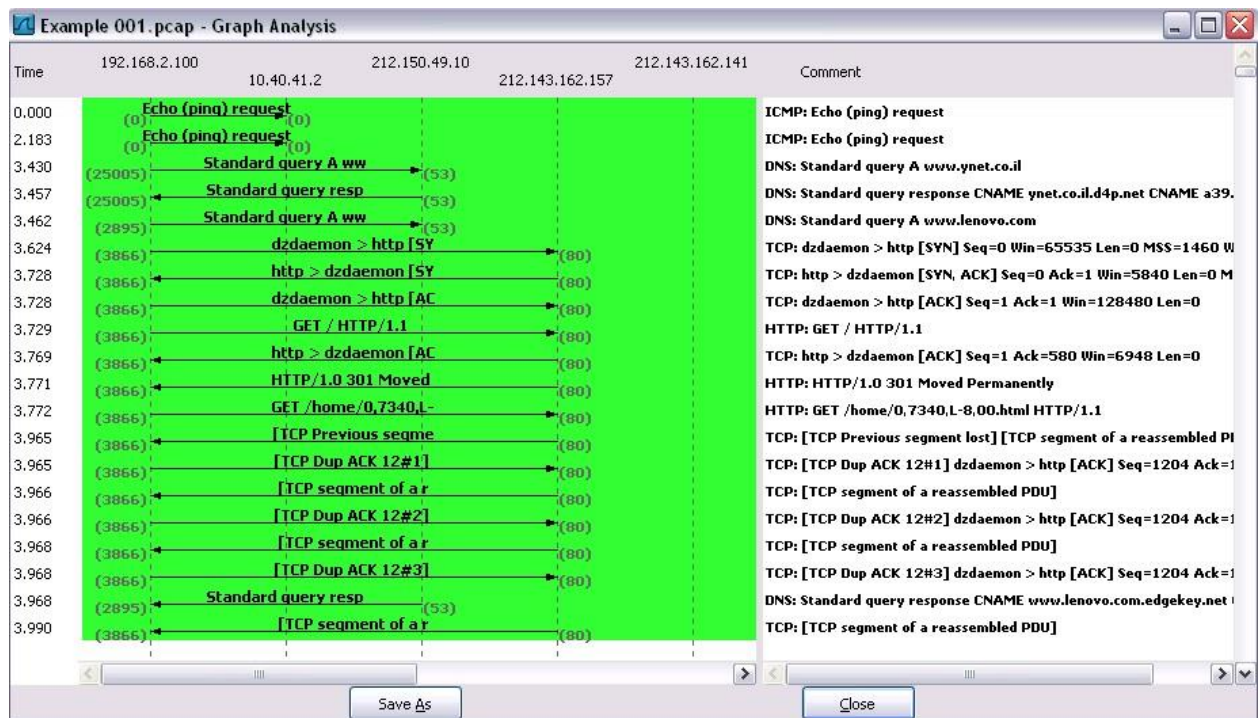
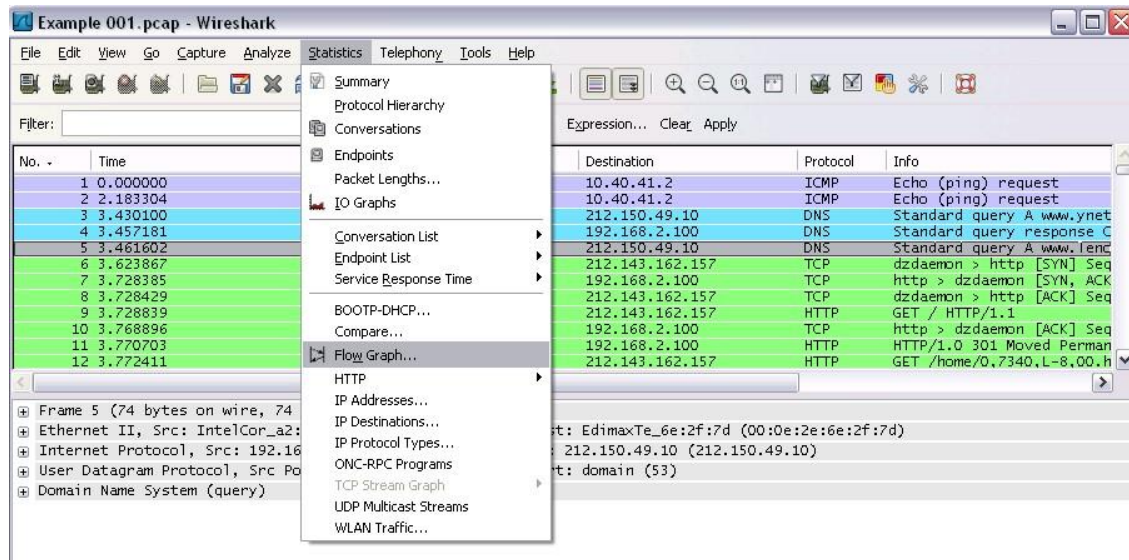
**Flow Graph:** Gives a better understanding of what we see.



CS23532

NAME: B. MADHAN KUMAR


ROLL NO: 231901028

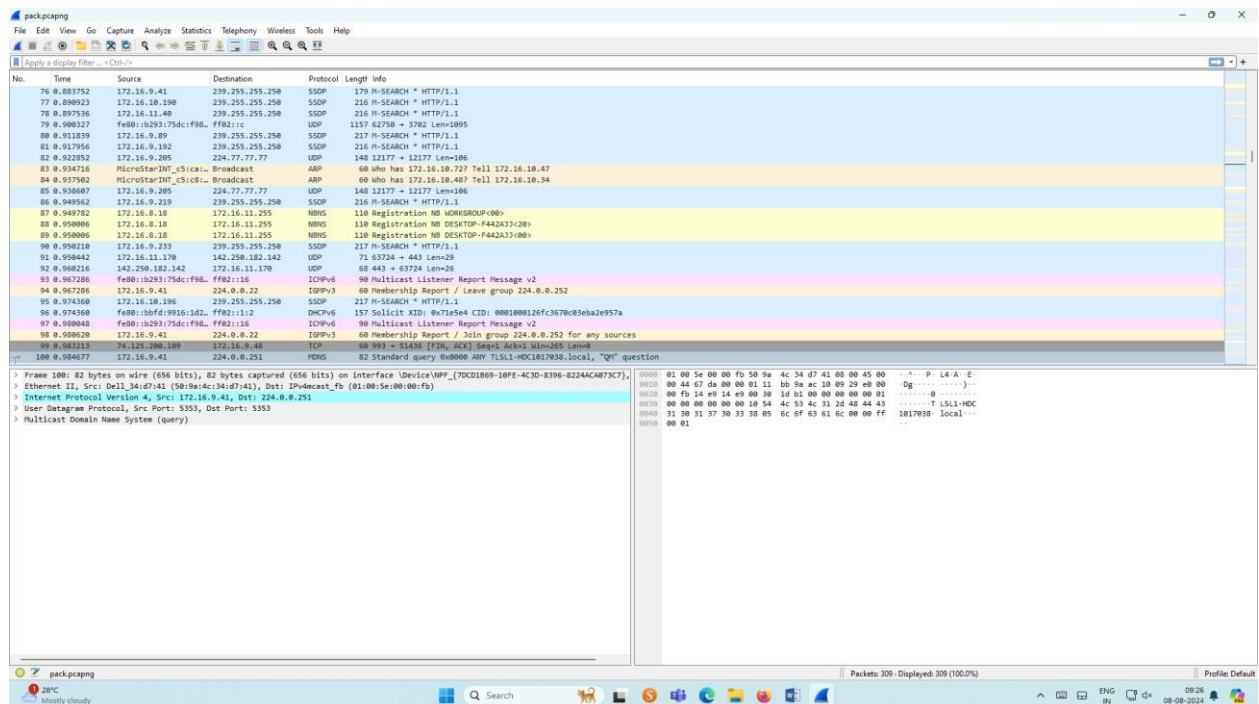


**Ex No: 4B****PACKET SNIFFING USING WIRESHARK****AIM:**

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 file operations, capture control, and analysis. The main window is divided into three panes:

- Packet List:** Shows a list of 100 captured packets. The first few packets are HTTP GET requests. Packet 83 is an ARP request. Packet 84 is an ARP response. Packet 85 is a DHCP request. Packet 86 is a DHCP response. Packet 87 is a DHCP request. Packet 88 is a DHCP response. Packet 89 is a DHCP request. Packet 90 is a DHCP response. Packet 91 is a DHCP request. Packet 92 is a DHCP response. Packet 93 is a DHCP request. Packet 94 is a DHCP response. Packet 95 is a DHCP request. Packet 96 is a DHCP response. Packet 97 is a DHCP request. Packet 98 is a DHCP response. Packet 99 is a DHCP request. Packet 100 is a DHCP response.
- Packet Details:** Shows the hierarchical structure of the selected packet (Packet 100). It includes Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Multicast Domain Name System (query).
- Packet Bytes:** Shows the raw data of the selected packet in hexadecimal and ASCII format.

The status bar at the bottom indicates that 100 packets are displayed (100.0%).



CS23532

NAME: B. MADHAN KUMAR

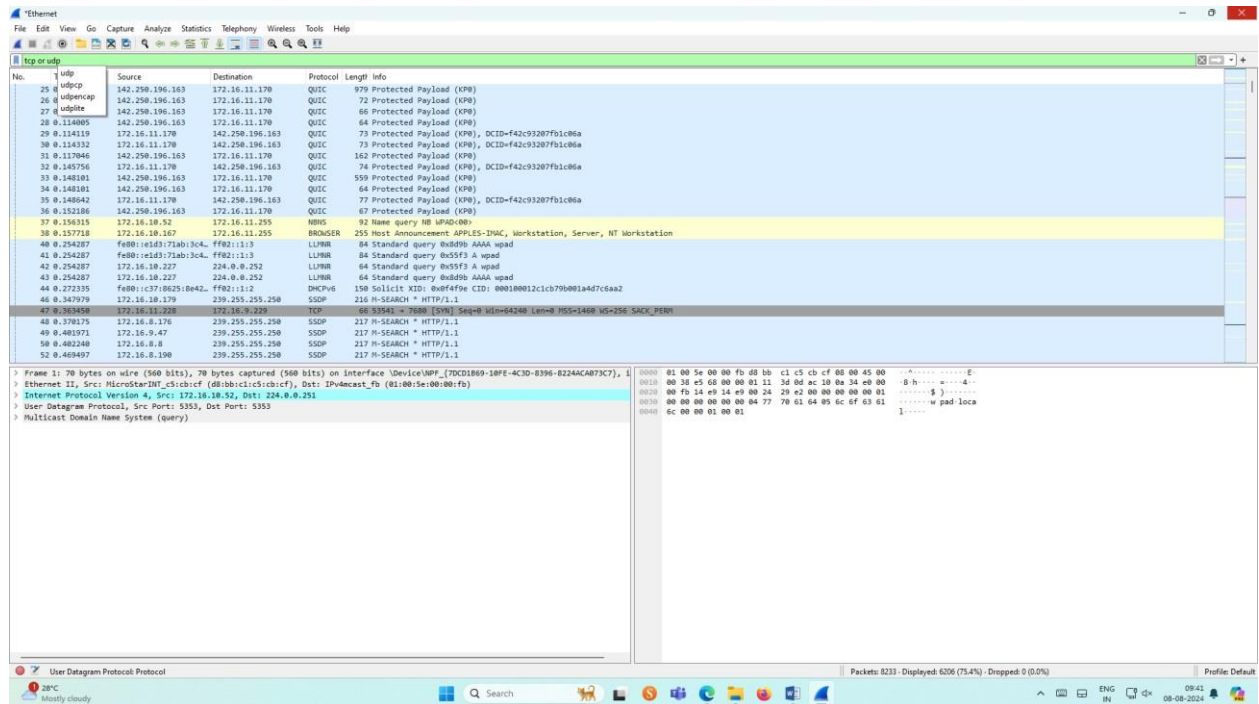
ROLL NO: 231901028

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

### Procedure

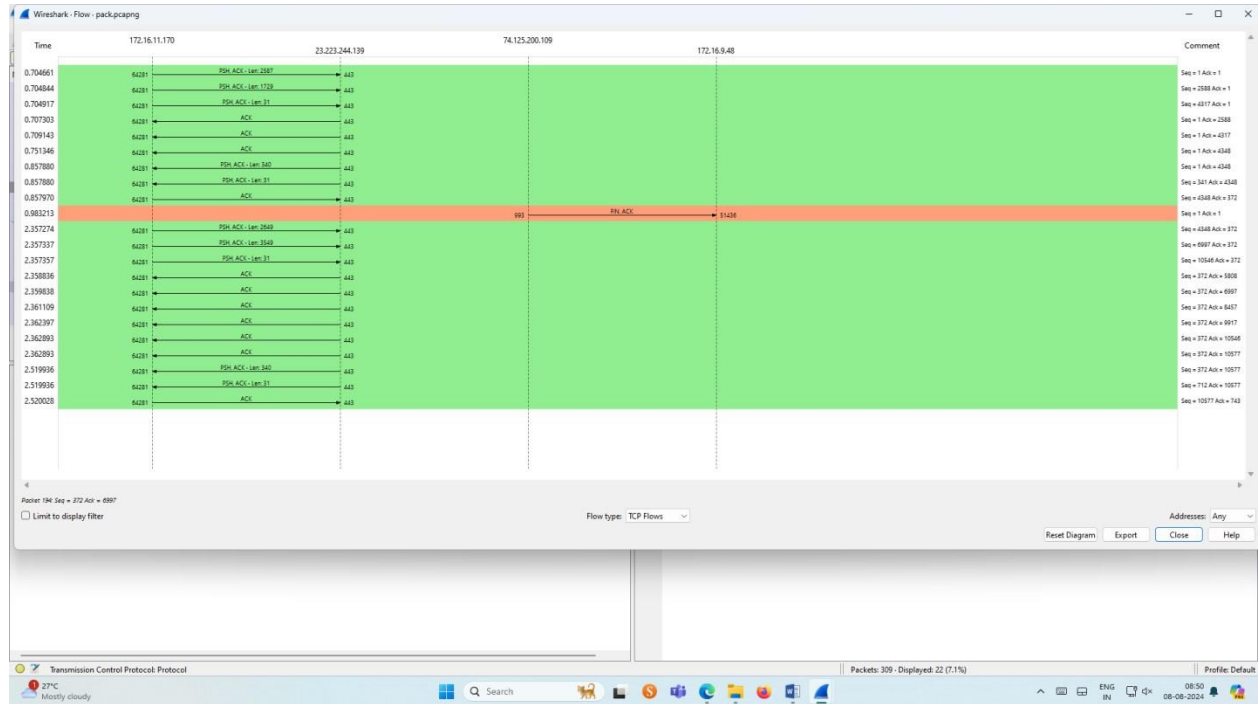
- Select Local Area Connection in Wireshark.
- Go to capture  option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search TCP packets in search bar.
- To see flow graph click Statistics  Flow graph. ➤ Save the packets.

### Output:

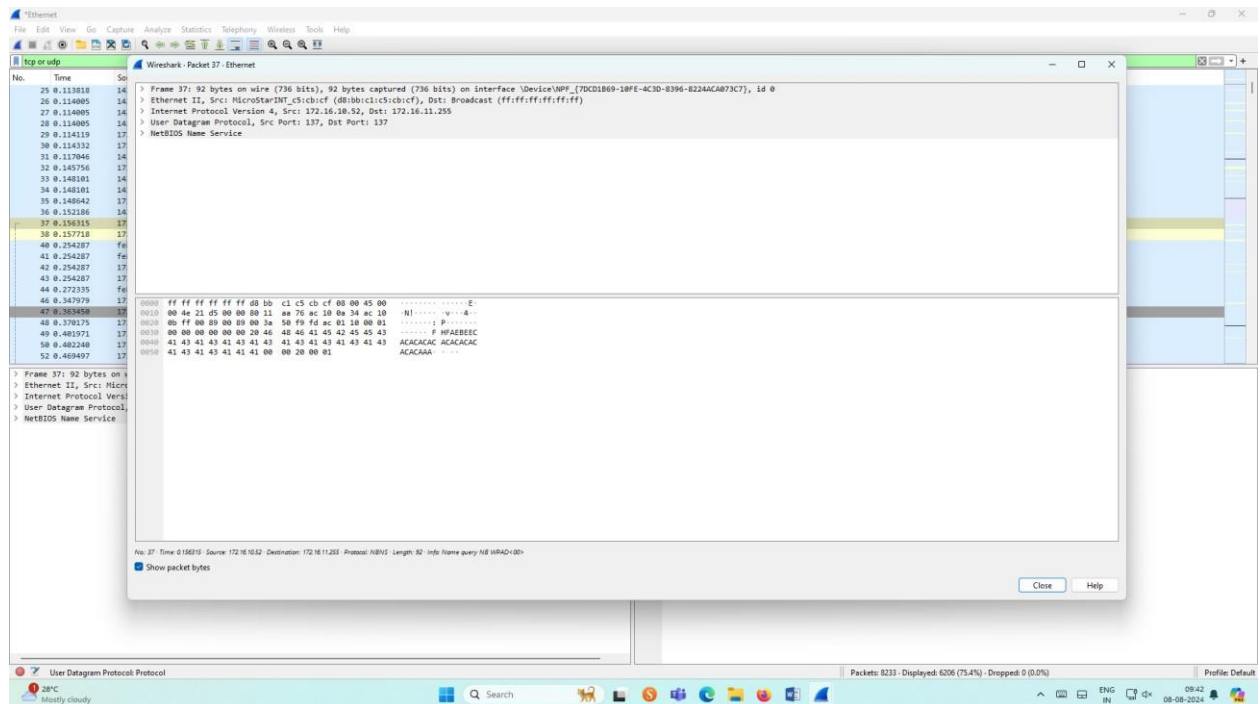


CS23532

### Flow Graph output



## Inspecting the packets






CS23532

NAME: B. MADHAN KUMAR

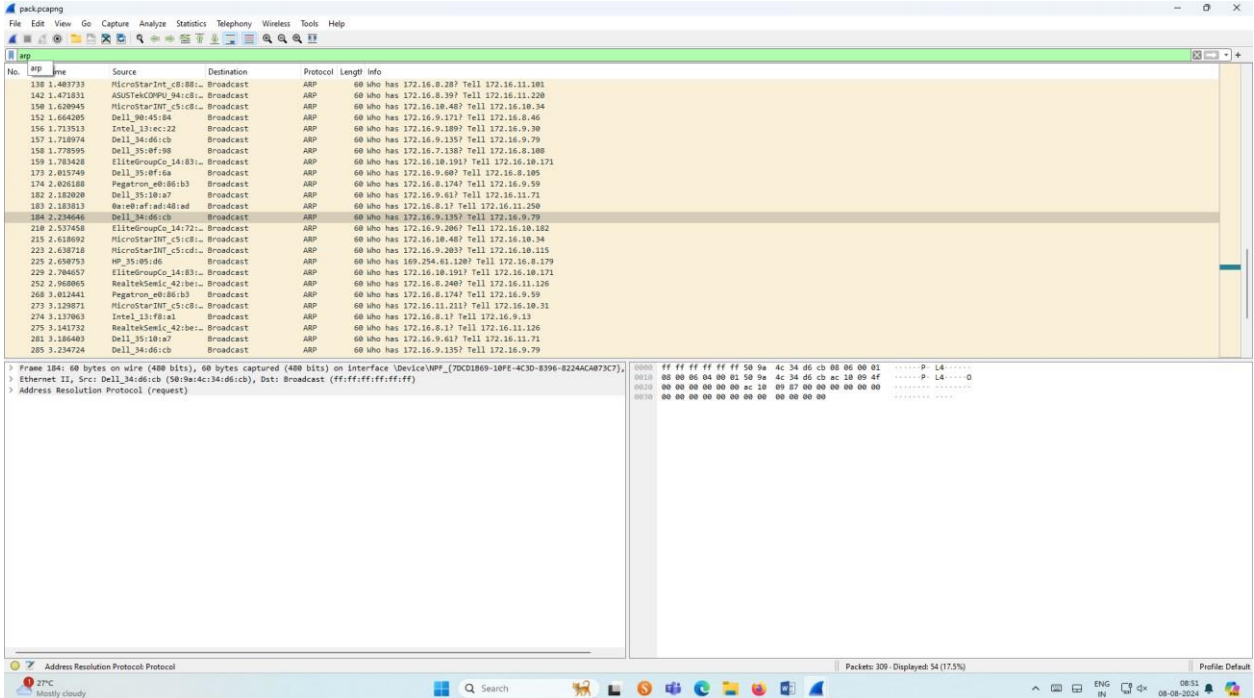
ROLL NO: 231901028

### 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



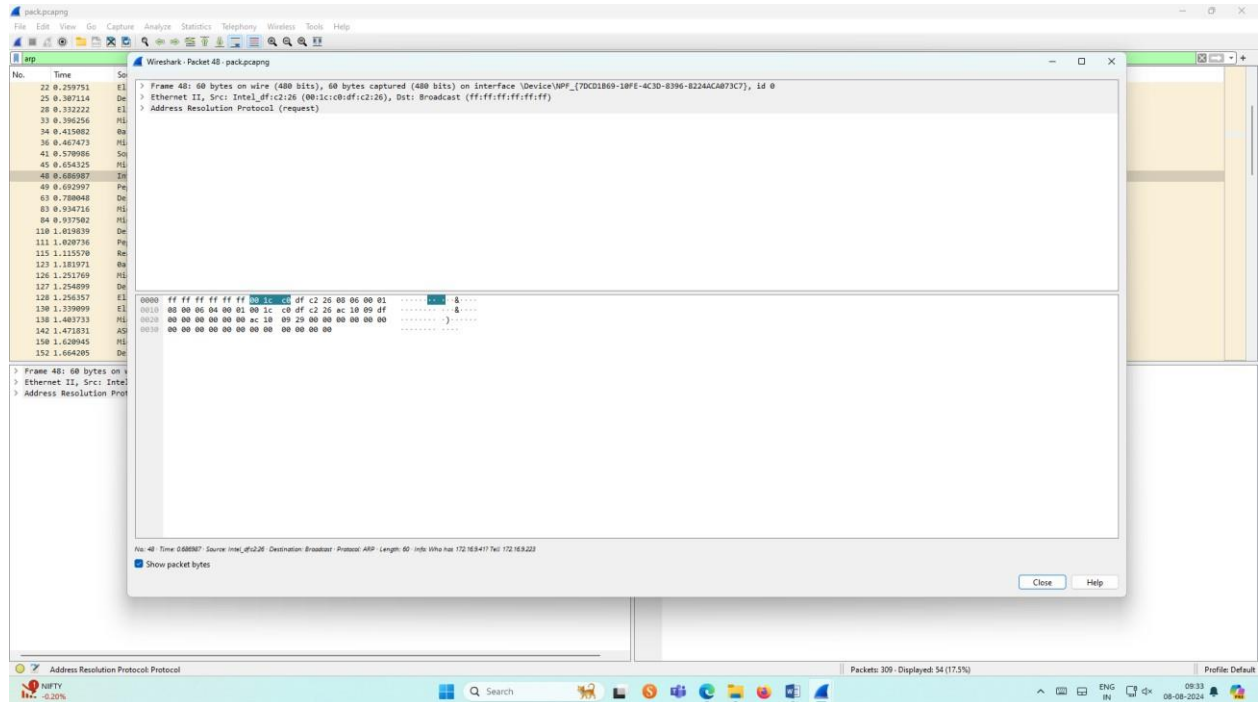
The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains icons for opening files, saving, capturing, and analyzing. The main window is divided into three panes:

- Filter Bar:** Displays the filter `arp`.
- Packet List:** A table showing captured packets. The first 20 packets are ARP requests and responses. The table has columns: No., Time, Source, Destination, Protocol, Length, and Info.
- Packet Details:** Shows the details of the selected packet (No. 184). It includes the Ethernet II header, Internet Protocol (IP) header, and ARP (Address Resolution Protocol) section.

The bottom status bar indicates the current capture status: "Packets: 309 - Displayed: 54 (17.5%)".



CS23532

## 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.

CS23532  
NAME:B.MADHAN KUMAR  
ROLL NO:231901028

## Output

Wireshark packet capture showing DNS traffic. The packet list shows a standard query and a standard query response. The packet details pane shows the structure of the query, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query). The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
34	0.000000	172.16.11.170	172.16.8.1	DNS	79	Standard query 0xc945 A fp-yp.azureedge.net
35	0.000000	172.16.11.170	172.16.8.1	DNS	79	Standard query 0xc945 A fp-yp.azureedge.net
36	0.000000	172.16.8.1	172.16.11.170	DNS	146	Standard query response 0xc945 A fp-yp.azureedge.net CNAME fp-yp.ec.azureedge.net CNAME cs9.wpc.vcdn.net A 117.18.232.200
37	0.000000	172.16.8.1	172.16.11.170	DNS	146	Standard query response 0xc945 A fp-yp.azureedge.net CNAME fp-yp.ec.azureedge.net CNAME cs9.wpc.vcdn.net A 117.18.232.200

Frame 37: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface \Device\NPF\_{70CD1869-18FE-4C3D-8396-8224ACAB73C7}, Ethernet II, Src: WP\_301e4d9 (7c:57:58:39:1e:4d9), Dst: Sophos\_cf:be:45 (7c:5a:1c:cf:be:45)

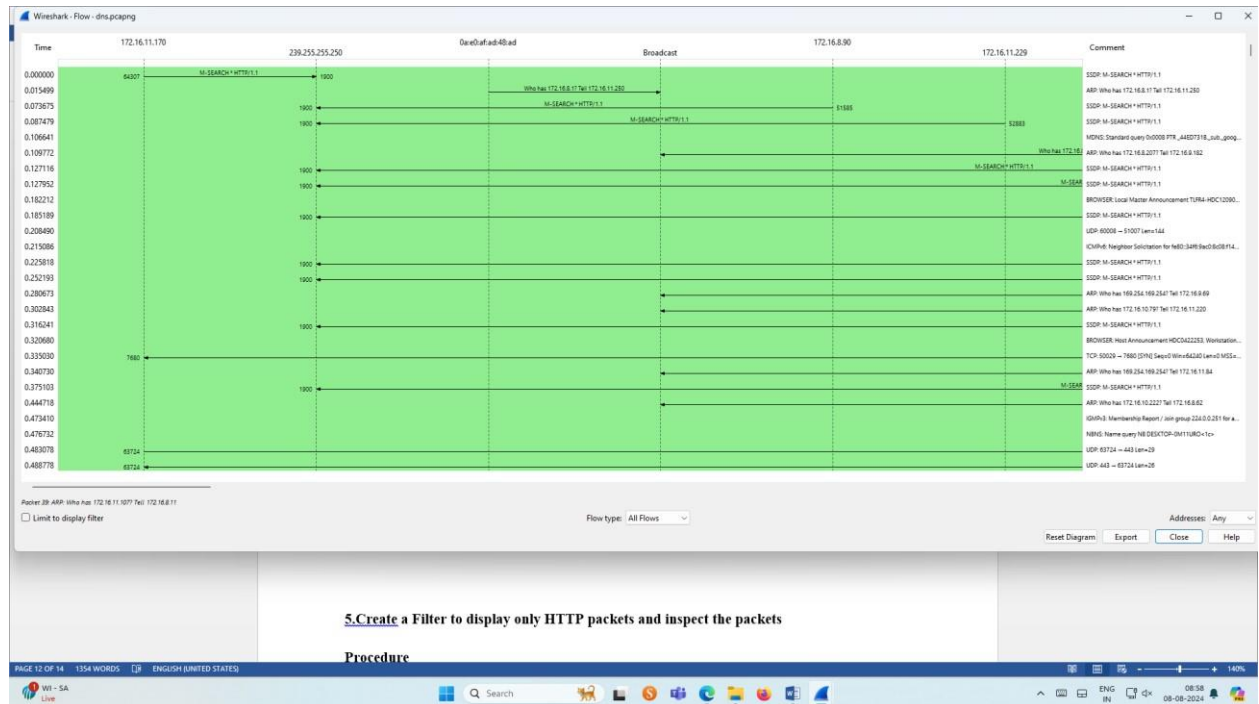
Internet Protocol Version 4, Src: 172.16.11.170, Dst: 172.16.8.1

User Datagram Protocol, Src Port: 51988, Dst Port: 53

Domain Name System (query)

0000 7c 5a 1c cf be 45 7c 57 58 39 1e 4d 00 00 45 00 [Z...E]W X9...E  
0010 00 41 6d 38 00 00 00 11 00 00 0c 10 00 00 00 00 JAd  
0020 00 01 c0 14 00 35 00 28 6c 0a c9 45 01 00 00 01 .....S-1...E....  
0030 00 00 00 00 00 00 05 66 70 2d 70 09 01 7a 75 .....f p-yp.azu  
0040 72 65 65 64 67 65 63 66 65 74 00 00 01 00 01 reedge n.ec...

## Graph output



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

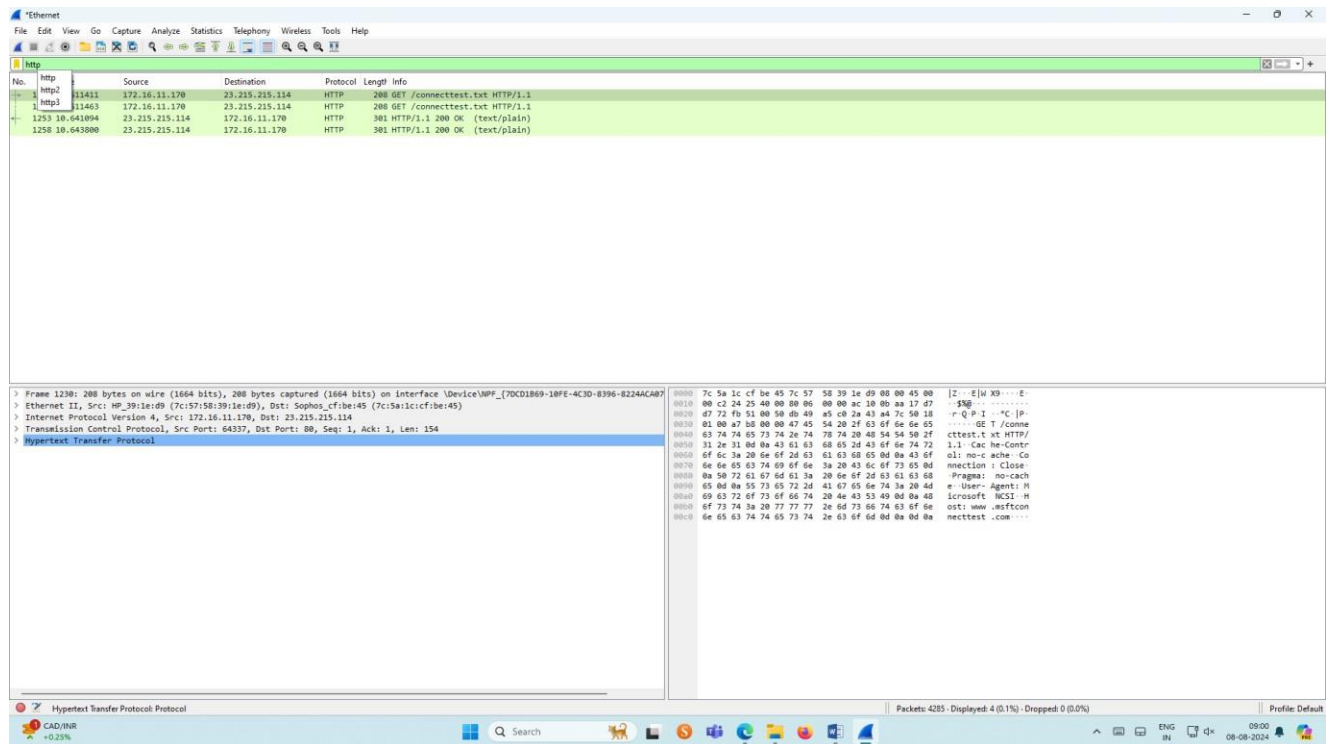


## Select Local Area Connection in Wireshark.

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.

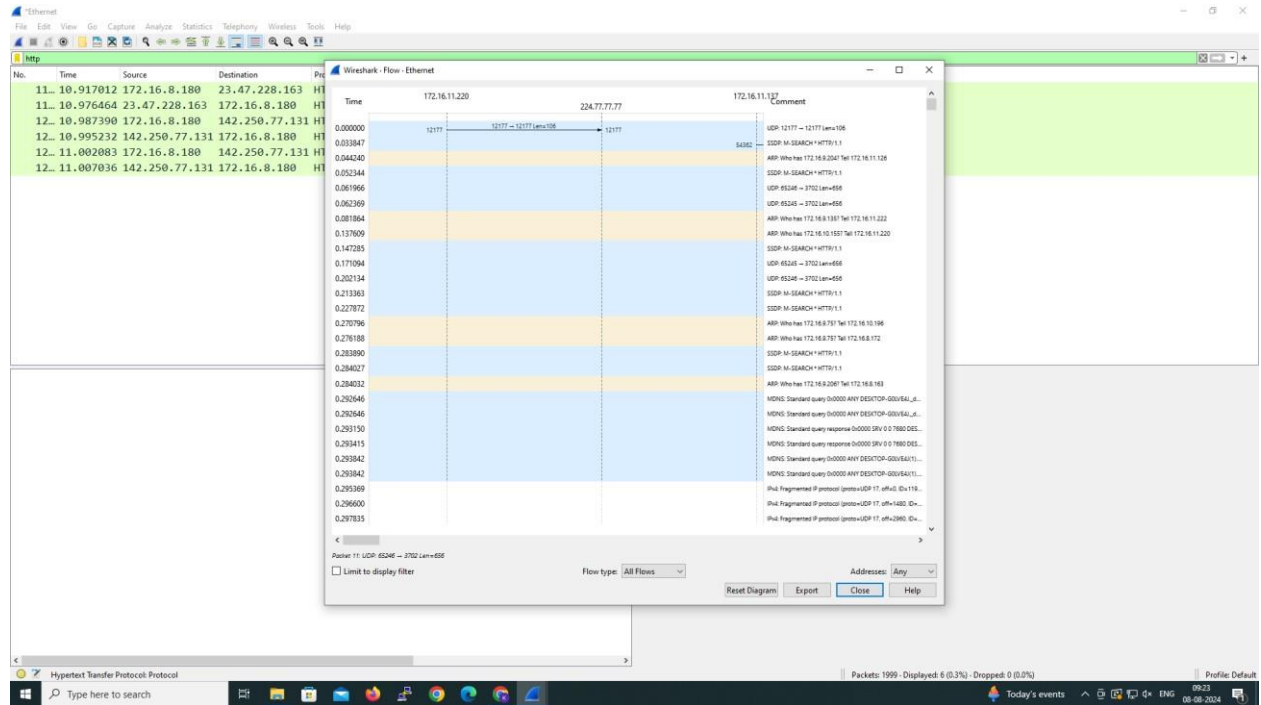
## Output



## Procedure

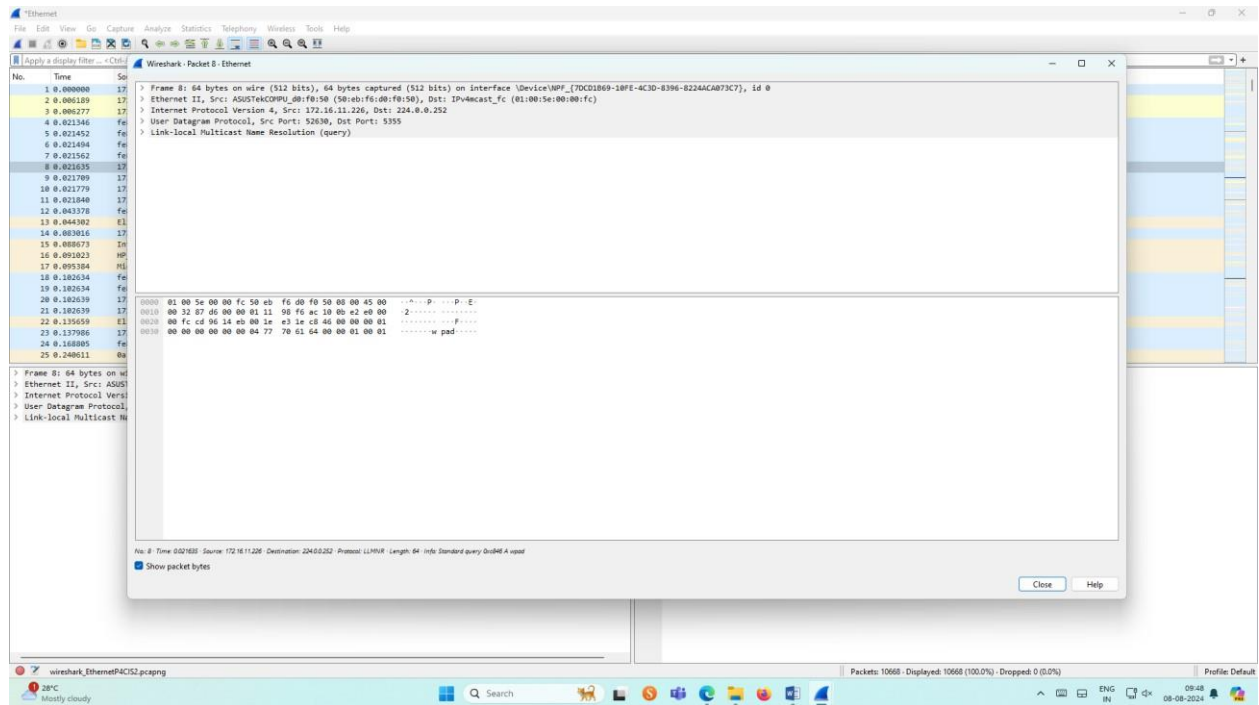


### Flow Graph output



CS23532

## Inspecting the packets



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

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

CS23532

## Procedure

The image shows a Wireshark packet capture analysis. The main pane displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The filter bar at the top is set to 'icmp or igmp'. The packet list shows several ICMP Registration and Name query messages, followed by a large block of IGMP Membership Reports and Leave group messages. The packet details pane on the right shows the structure of the selected packet (No. 309), including Ethernet II, Internet Protocol Version 4, and User Datagram Protocol fields. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
306	3.389477	142.250.182.78	172.16.11.170	UDP	70	443 → 65183 Len=28
307	3.399886	172.16.11.170	172.16.11.170	UDP	69	443 → 65183 Len=27
309	3.415817	142.250.182.78	172.16.11.170	UDP	66	443 → 65183 Len=24
16	0.197335	172.16.8.18	172.16.11.255	NBNS	110	Registration NB DESKTOP-F442A33<00>
17	0.197335	172.16.8.18	172.16.11.255	NBNS	110	Registration NB DESKTOP-F442A33<20>
18	0.197335	172.16.8.18	172.16.11.255	NBNS	110	Registration NB WORKGROUP<00>
35	0.467287	172.16.9.66	172.16.11.255	NBNS	92	Name query NB DESKTOP-H938F58<1c>
87	0.940782	172.16.8.18	172.16.11.255	NBNS	110	Registration NB WORKGROUP<00>
88	0.950086	172.16.8.18	172.16.11.255	NBNS	110	Registration NB DESKTOP-F442A33<20>
89	0.950086	172.16.8.18	172.16.11.255	NBNS	110	Registration NB DESKTOP-F442A33<00>
125	1.217692	172.16.9.66	172.16.11.255	NBNS	92	Name query NB DESKTOP-H938F58<1c>
295	3.351537	172.16.9.74	172.16.11.255	UDP	106	60000 → 51807 Len=144
99	0.983213	74.125.200.149	172.16.9.48	TCP	60	993 → 81458 [FIN, ACK] Seq=1 Ack=3 Win=285 Len=0
304	3.386154	172.16.11.170	172.16.11.252	UDP	1280	50415 → 443 Len=1246
305	3.386282	172.16.11.170	172.16.11.252	UDP	994	50415 → 443 Len=952
94	0.967286	172.16.9.41	224.0.0.22	IGMPv3	60	Membership Report / Leave group 224.0.0.252
98	0.988620	172.16.9.41	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any sources
139	1.461679	172.16.9.41	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any sources
167	1.912286	169.254.0.14	224.0.0.22	IGMPv3	60	Membership Report / Leave group 239.255.255.250
168	1.912286	169.254.0.14	224.0.0.22	IGMPv3	60	Membership Report / Join group 239.255.255.250 for any sources
231	2.768294	169.254.0.14	224.0.0.22	IGMPv3	60	Membership Report / Join group 239.255.255.250 for any sources
233	2.766148	169.254.0.14	224.0.0.22	IGMPv3	60	Membership Report / Leave group 224.0.0.252
250	2.954467	172.16.9.41	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any sources
254	2.978107	172.16.9.41	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any sources
26	0.327543	172.16.8.255	224.0.0.251	NBNS	85	Standard query 0x0000 PTR _mscrosft_mccc_tcp_local, "qm" question

Packet 309 - Displayed: 214 (69.3%)

Internet Protocol Version 4 - Protocol

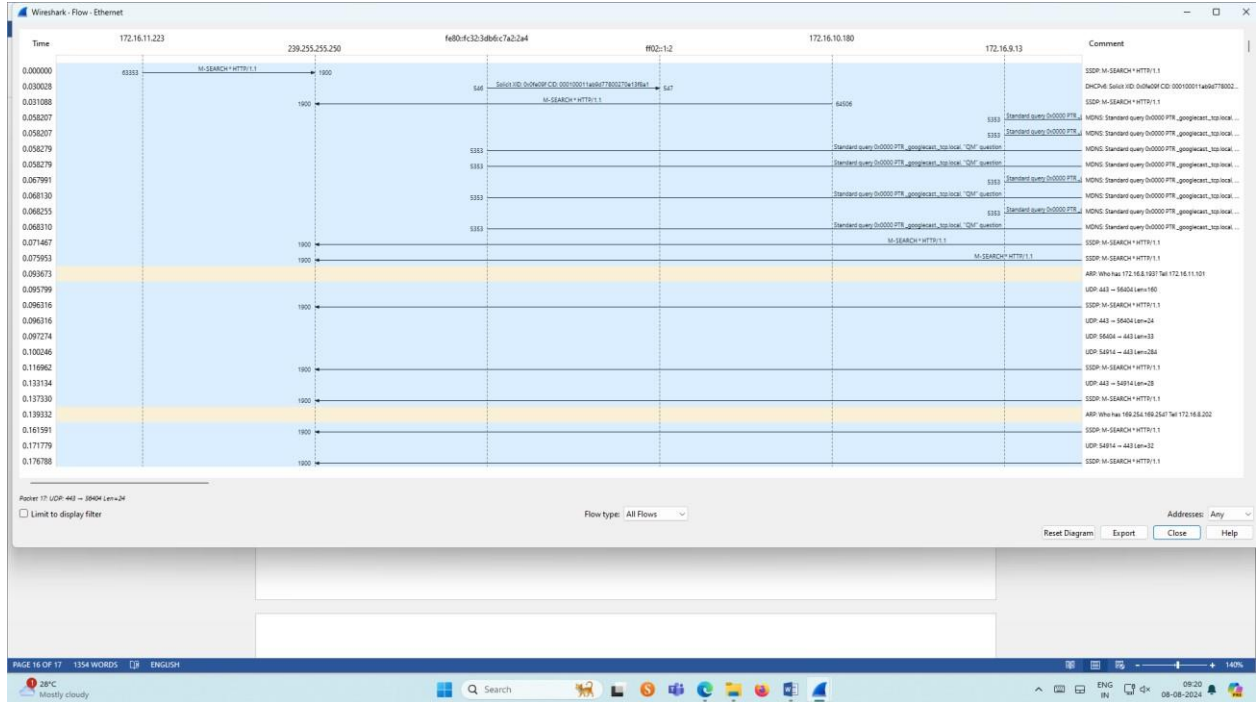
Frame 4: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on Interface Vmnic0\NPF\_{70CD1869-18FE-4C30-8396-B224AC873C7}, 1  
> Ethernet II, Src: HP\_361c:d9 (7c:57:18:19:1e:d9), Dst: Sophos\_cf:be:45 (7c:5a:1c:cf:be:45)  
> Internet Protocol Version 4, Src: 172.16.11.170, Dst: 142.250.182.142  
> User Datagram Protocol, Src Port: 63724, Dst Port: 443  
> Data (29 bytes)

0000 7c 5a 1c cf be 45 7c 57 58 39 1e d9 00 00 45 00 |Z...E|u X9...E|  
0010 00 39 c0 10 40 00 00 11 00 00 ac 10 0b aa be fa |9...  
0020 b6 be f8 ec 81 b0 00 25 fd 79 52 e2 03 d1 c1 57 |.....X y8...W|  
0030 a5 fa 98 c7 c0 f8 bf 7b 71 b1 01 92 bd cd d3 96 |.....{ q.....|  
0040 1f 71 17 81 94 7e 34 |q...4

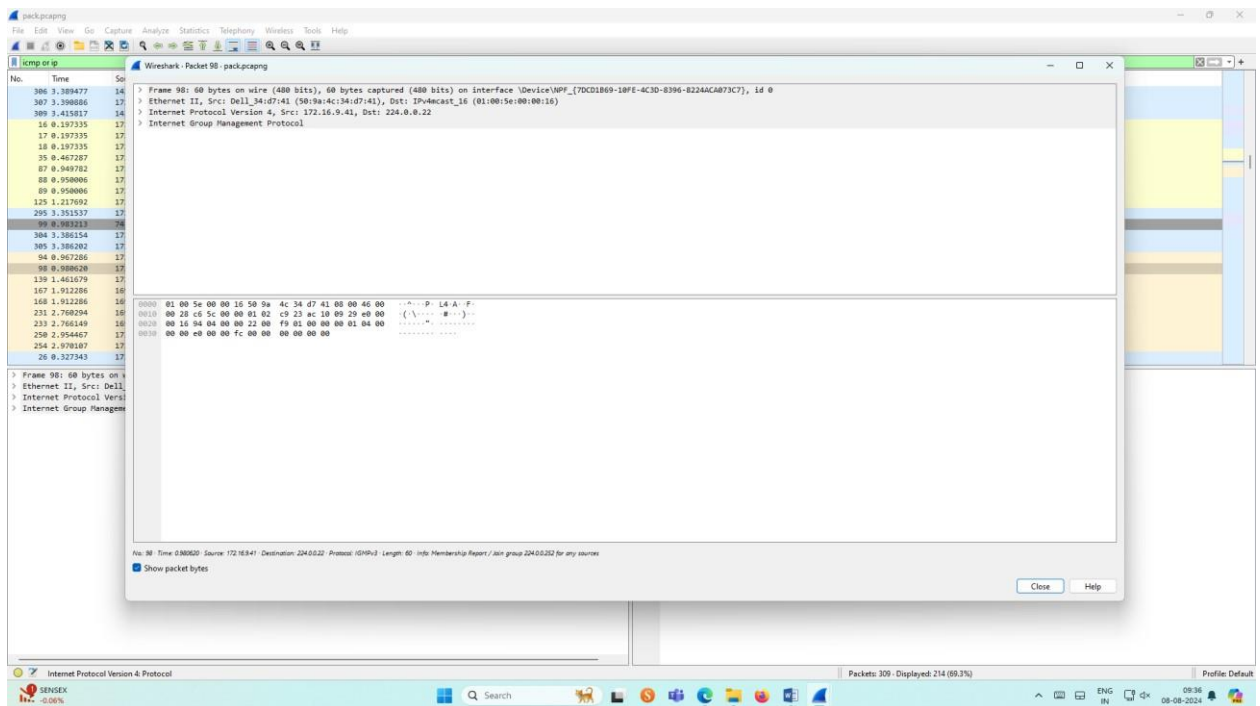


CS23532

## Flow Graph output



## Inspecting the packets



CS23532

## Procedure



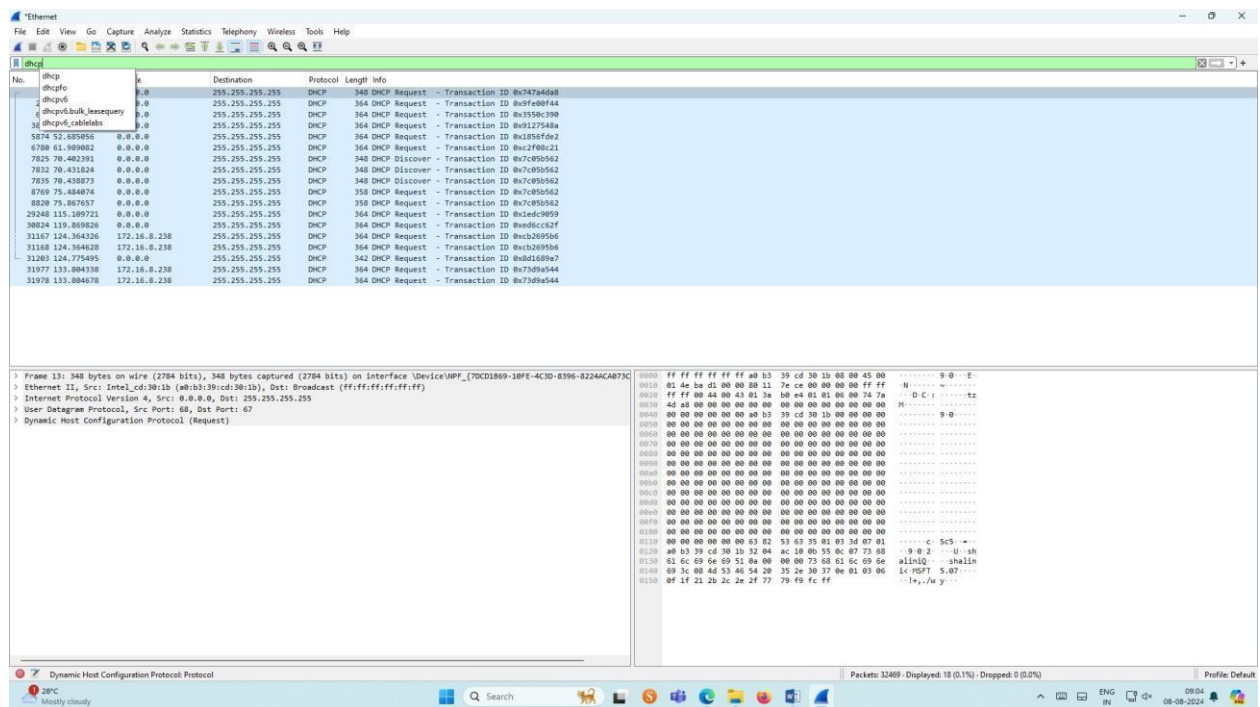
## 7. Create a Filter to display only DHCP packets and inspect the packets.

## 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



## Inspecting the packets

