

NAME:KEERTHIKA.S

ROLL.NO:231901024

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:

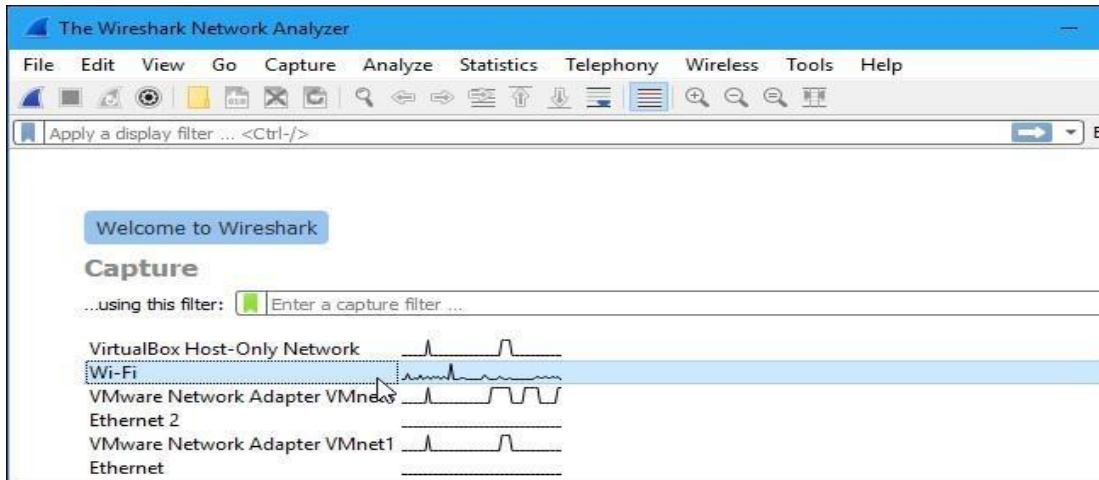
- Network administrators: troubleshoot network problems
- Network security engineers: examine security problems
- Developers: debug protocol implementations
- People: learn **network protocol internals**

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.

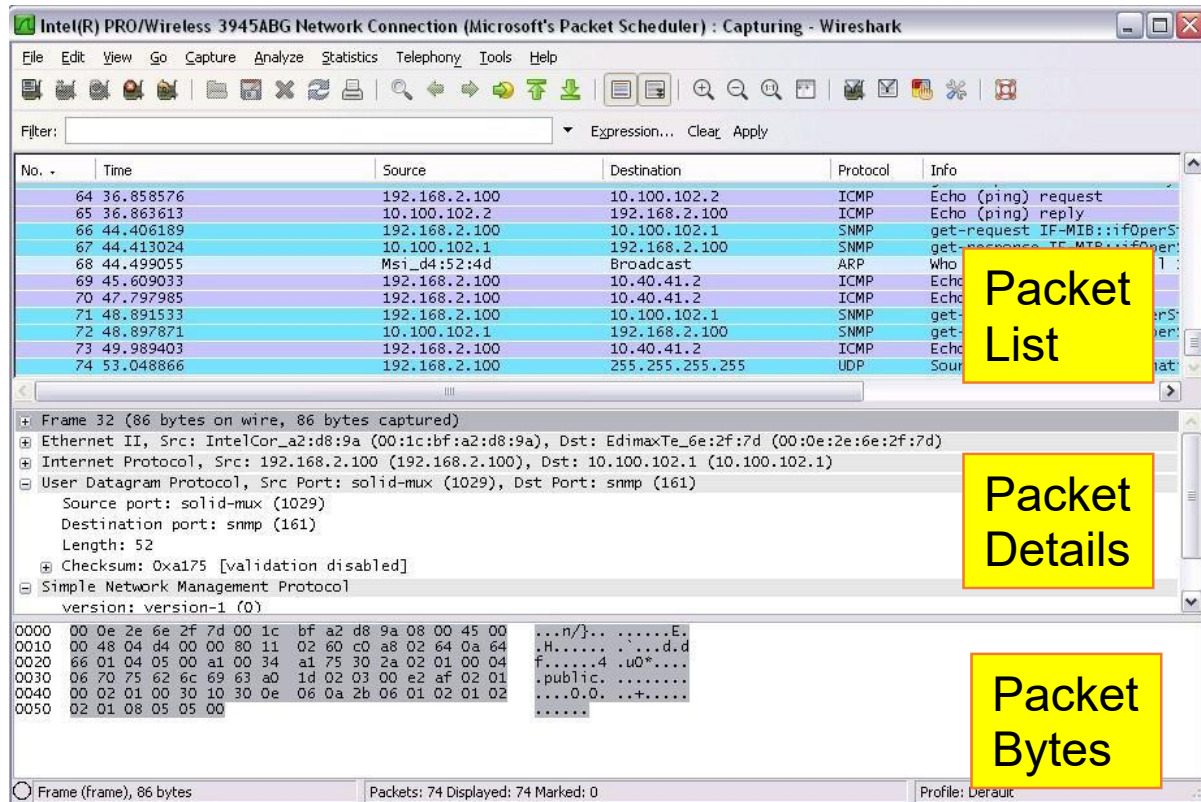
Capturing Packets

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.



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 pane and —Packet Bytes pane.

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.

NAME:KEERTHIKA.S

ROLL.NO:231901024

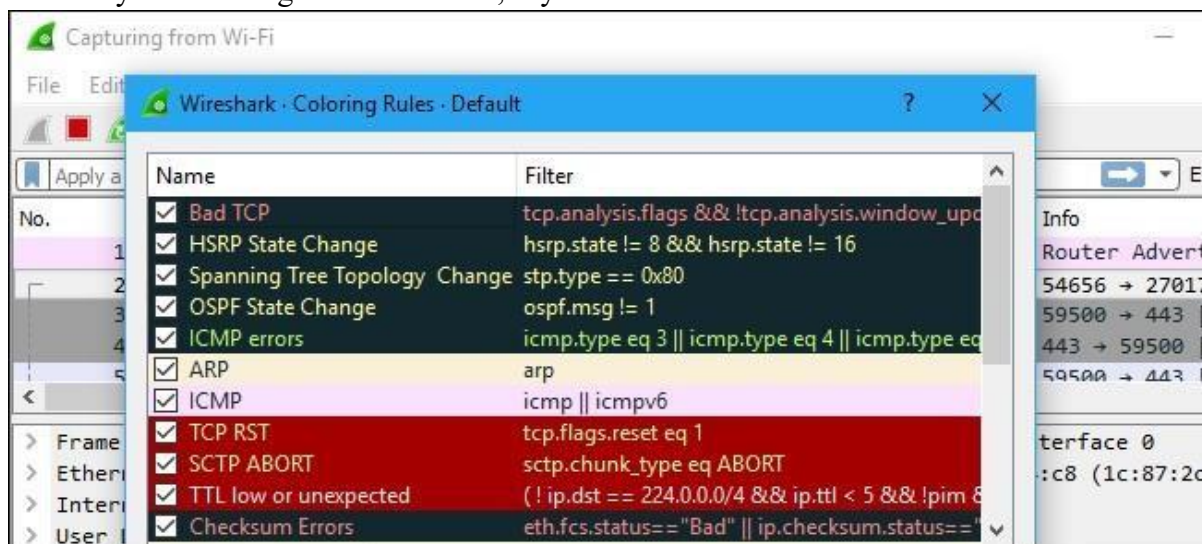
The “Packet Bytes” Pane

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.



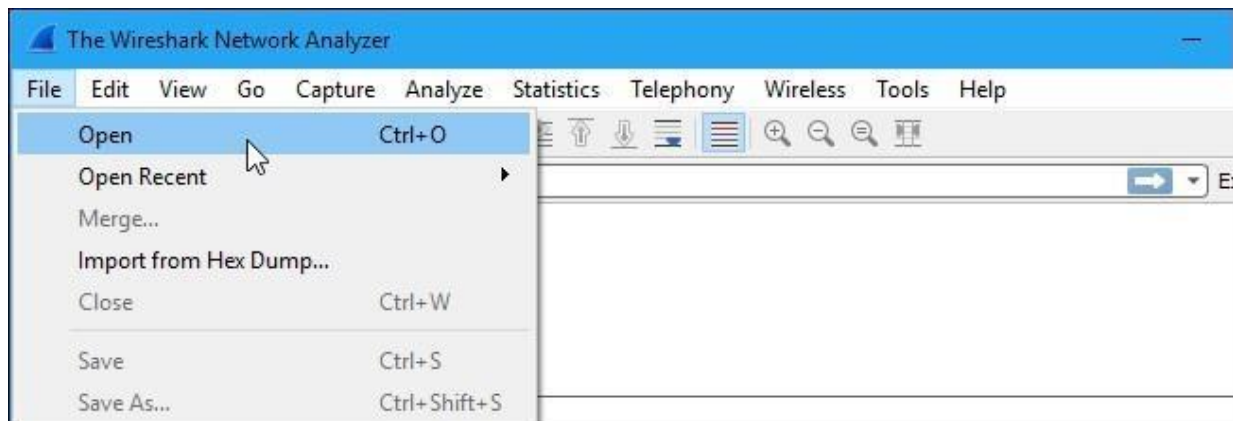
Sample Captures

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.

NAME:KEERTHIKA.S

ROLL.NO:231901024

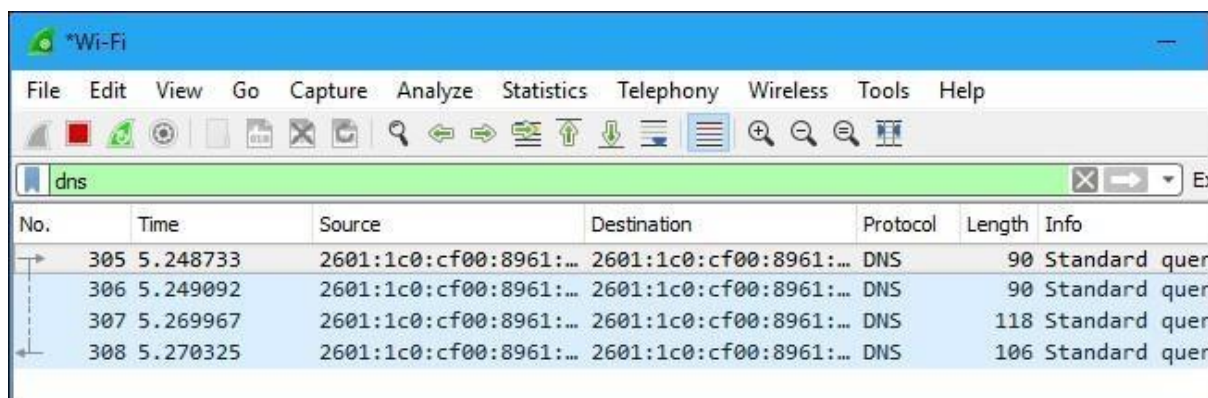
You can also save your own captures in Wireshark and open them later. Click File > Save to save your captured packets.



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.

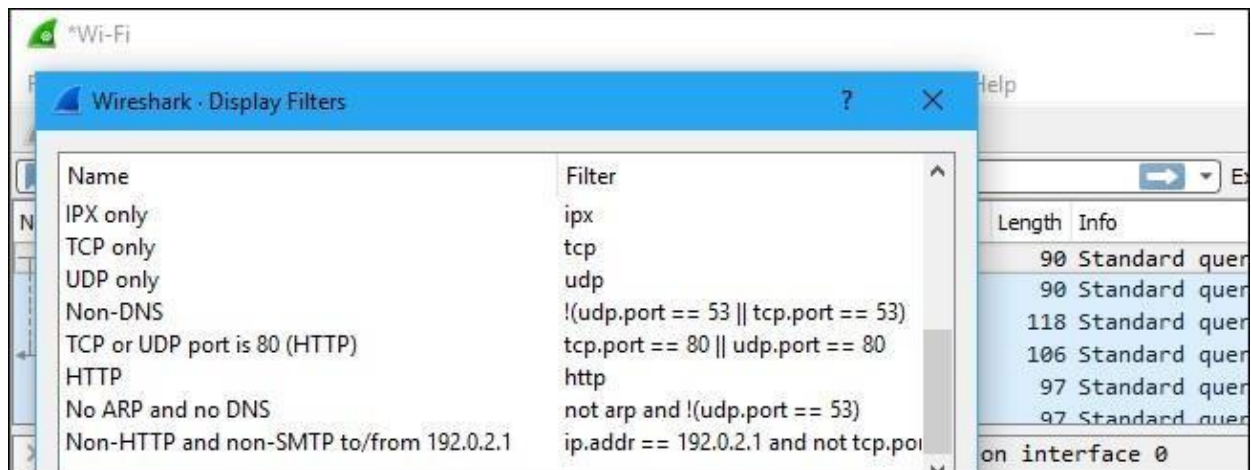


You can also click Analyze > Display Filters to choose a filter from among the default filters included in Wireshark. From here, you can add your own custom filters and save them to easily access them in the future.

NAME:KEERTHIKA.S

ROLL.NO:231901024

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

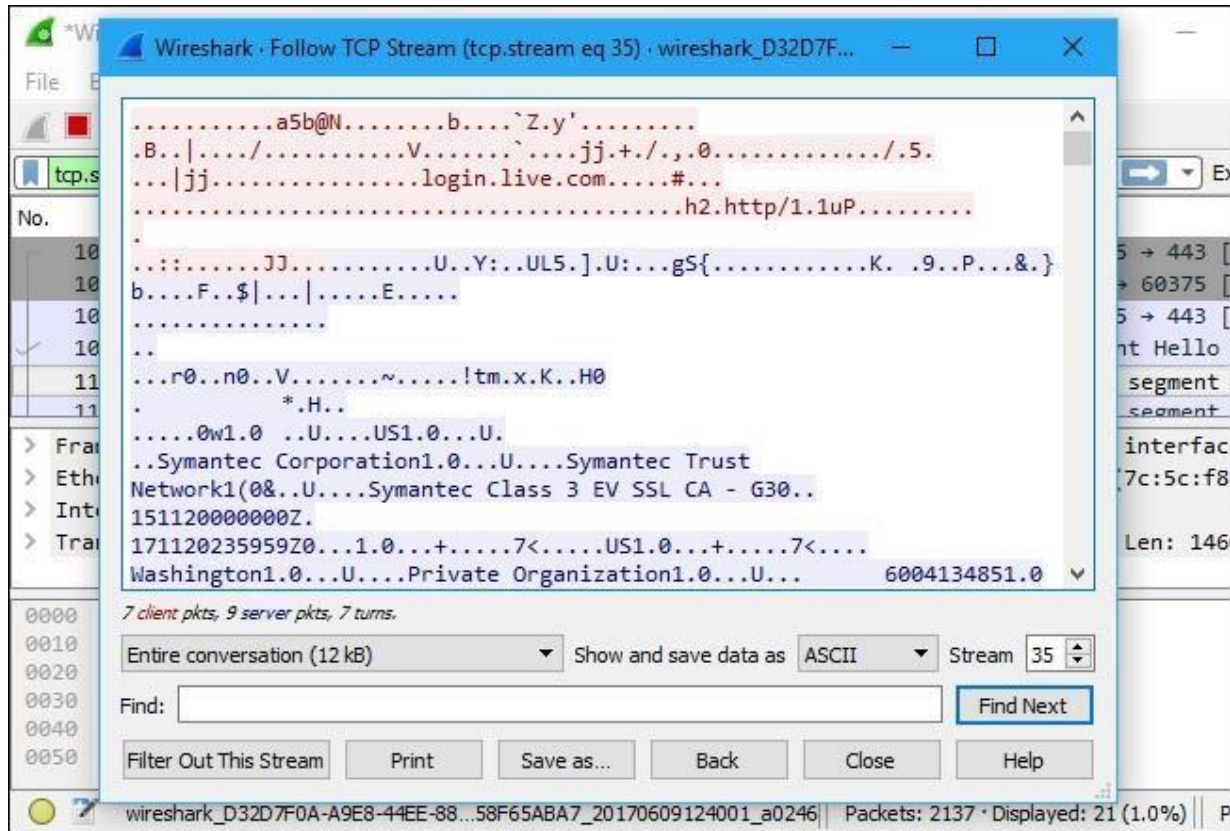


Another interesting thing you can do is right-click a packet and select Follow > TCP Stream.

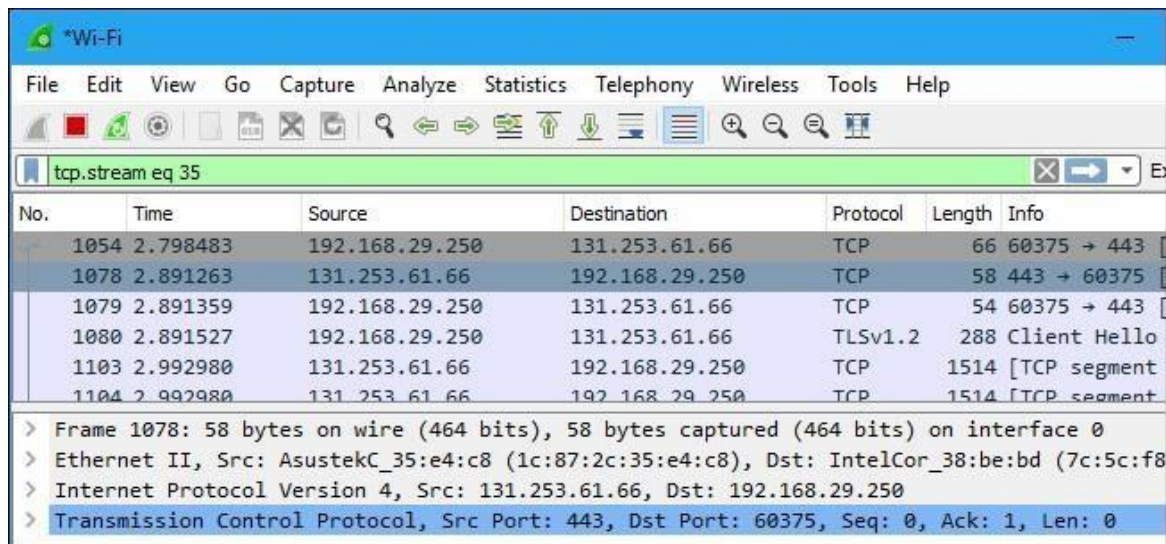
You'll see the full TCP conversation between the client and the server. You can also click other protocols in the Follow menu to see the full conversations for other protocols, if applicable.

NAME:KEERTHIKA.S

ROLL.NO:231901024



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



CSE(CYBER SECURITY)

NAME:KEERTHIKA.S

ROLL.NO:231901024

Inspecting Packets

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

The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for packet capture and analysis. The packet list pane shows a table of captured packets:

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

The packet details pane for the selected packet (No. 1054) shows the following information:

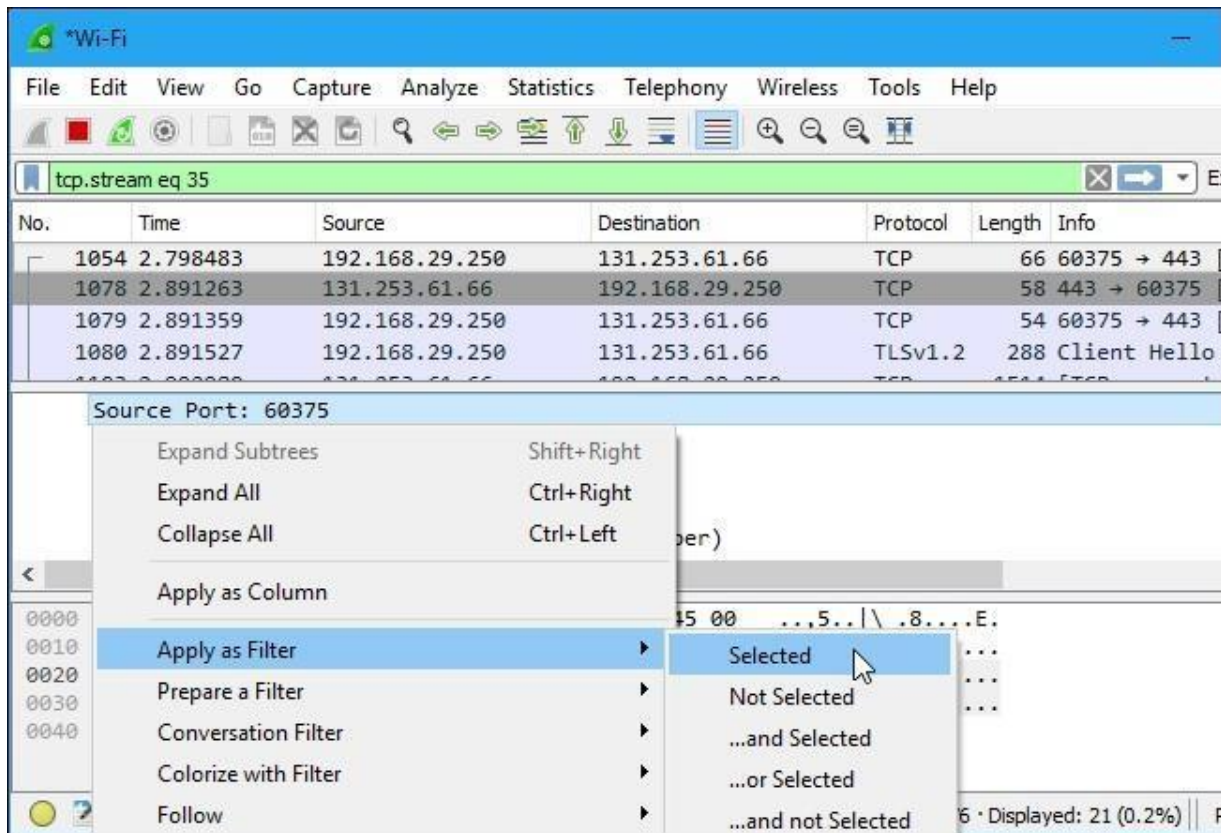
- Frame 1054: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
- Interface id: 0 (\Device\NPF_{D32D7F0A-A9E8-44EE-88DC-DFD58F65ABA7})
- Encapsulation type: Ethernet (1)
- Arrival Time: Jun 9, 2017 12:40:04.140141000 Pacific Daylight Time
- [Time shift for this packet: 0.000000000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

The packet bytes pane shows the raw data in hexadecimal and 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 ..
```

The status bar at the bottom indicates the filter is 'Encapsulation type (frame.encap_type)' and shows '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.

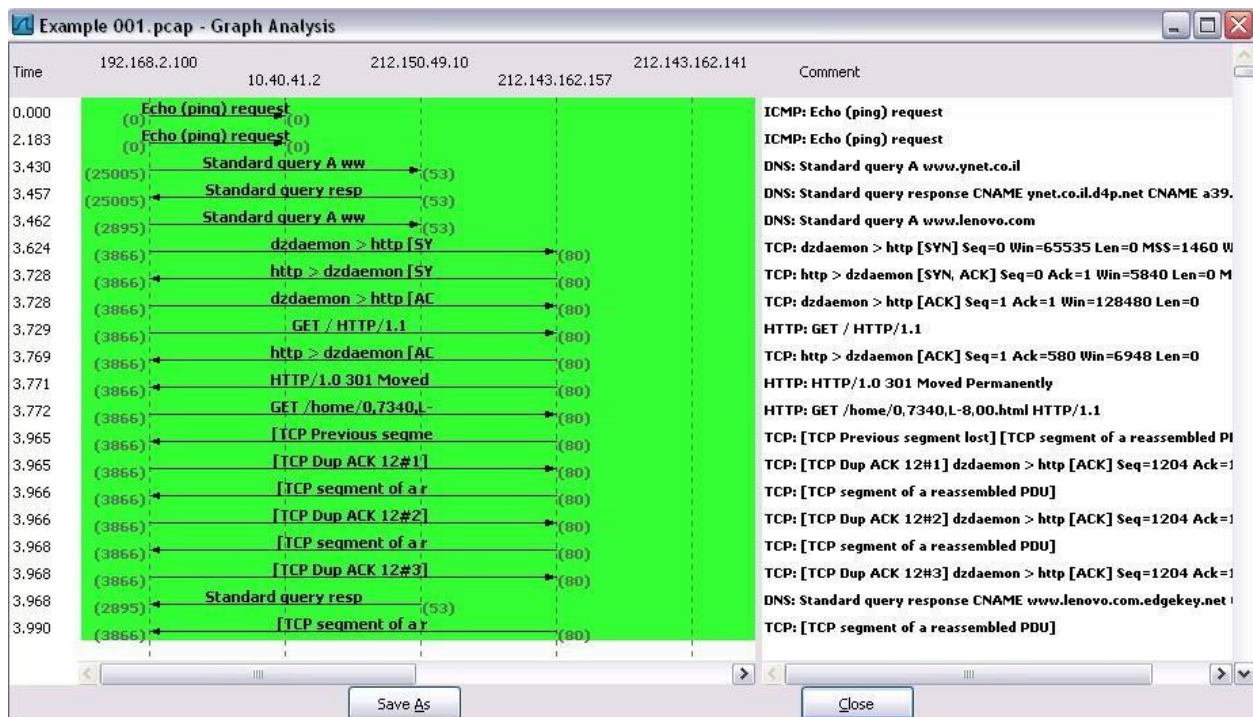
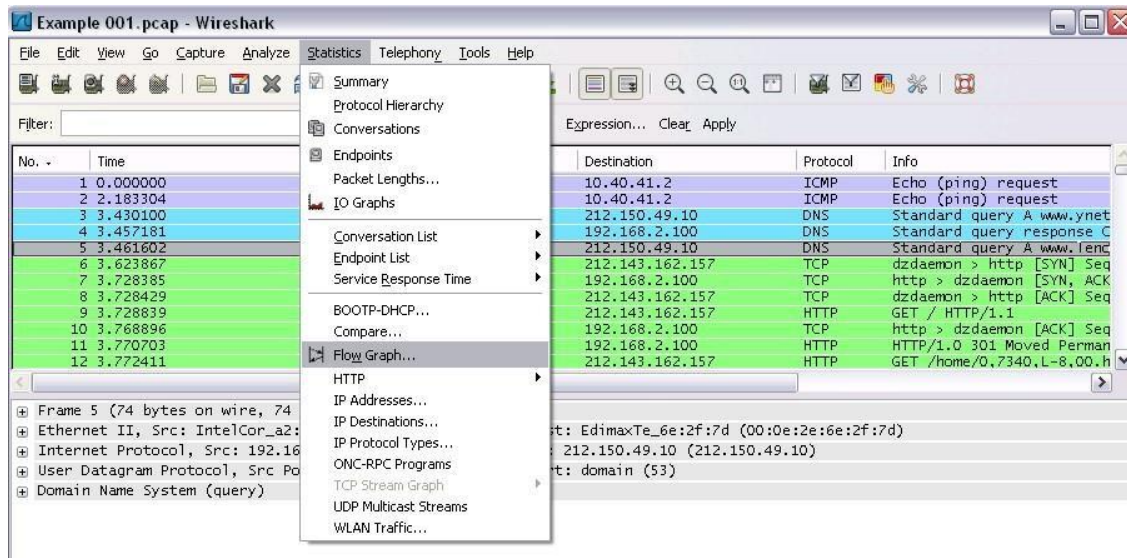


Wireshark is an extremely powerful tool, and this tutorial is just scratching the surface of what you can do with it. Professionals use it to debug network protocol implementations, examine security problems and inspect network protocol internals.

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

NAME:KEERTHIKA.S

ROLL.NO:231901024



CSE(CYBER SECURITY)

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.

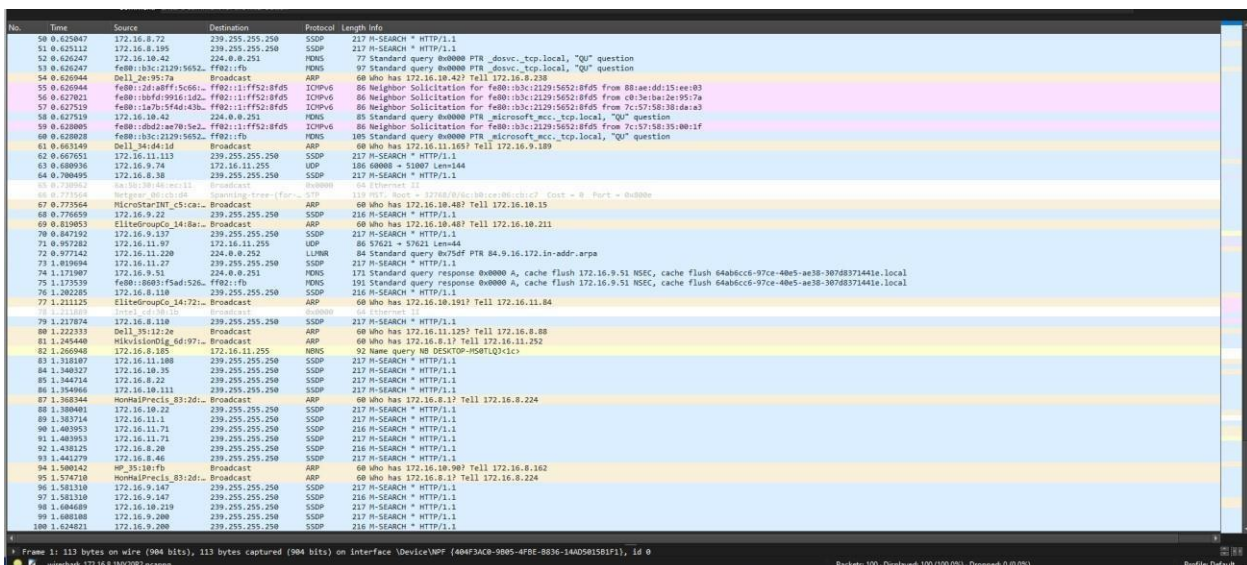
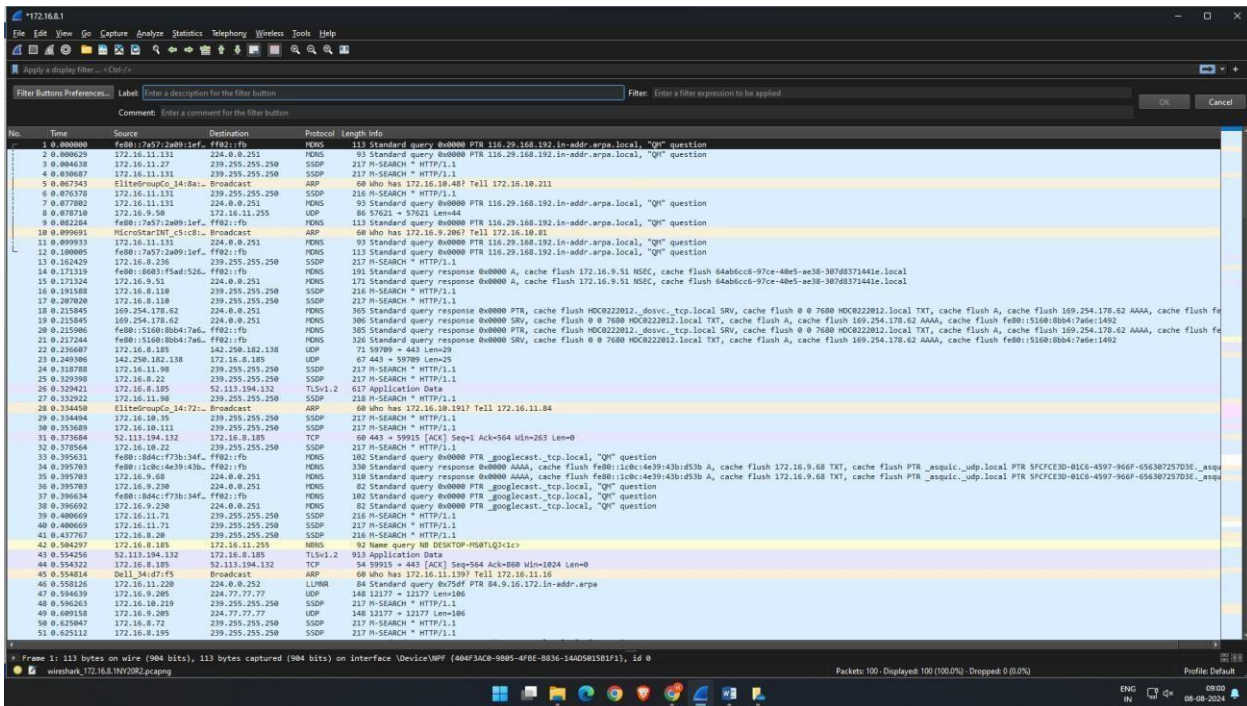
Procedure

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

NAME:KEERTHIKA.S

Output

ROLL.NO:231901024



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

CSE(CYBER SECURITY)

NAME:KEERTHIKA.S

ROLL.NO:231901024

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:udp

No.	Time	Source	Destination	Protocol	Length	Info
915	12.358257	172.16.8.105	52.113.194.132	TCP	54	59968 → 443 [FIN, ACK] Seq=1 Ack=1 Win=0 Len=0
916	12.359399	52.113.194.132	172.16.8.185	TCP	60	443 → 59968 [ACK] Seq=1 Ack=2 Win=205 Len=0
1425	22.431631	172.16.8.185	172.217.167.138	TCP	55	59969 → 443 [ACK] Seq=1 Ack=1 Win=1821 Len=1 [TCP segment of a reassembled PDU]
1426	22.432531	172.217.167.138	172.16.8.185	TCP	66	443 → 59969 [ACK] Seq=1 Ack=2 Win=257 Len=0 SLE=1 SRE=2
1996	26.932929	172.216.8.11	172.216.8.105	TCP	60	49447 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1945	27.313511	172.16.8.11	172.16.9.65	TCP	66	[TCP Retransmission] 49447 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1966	27.727258	172.16.8.185	142.251.18.188	TLShv1.2	88	Application Data
1971	27.763773	142.251.18.188	172.16.8.185	TCP	68	526 → 59078 [ACK] Seq=1 Ack=27 Win=290 Len=0
1976	27.765175	142.251.18.188	172.16.8.185	TLShv1.2	88	Application Data
1982	27.806326	172.16.8.185	142.251.18.188	TCP	64	59078 → 5228 [ACK] Seq=27 Ack=27 Win=1821 Len=0
2063	29.168766	172.16.8.11	172.16.9.65	TCP	66	[TCP Retransmission] 49447 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2132	31.327088	172.16.8.11	172.16.9.65	TCP	66	[TCP Retransmission] 49447 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2408	34.924438	172.16.8.208	172.16.11.48	TCP	66	[TCP Retransmission] 64979 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2611	36.939966	172.16.8.208	172.16.11.48	TCP	66	[TCP Retransmission] 64979 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2838	48.931561	172.16.8.208	172.16.11.48	TCP	66	[TCP Retransmission] 64979 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
3788	56.783918	172.16.9.173	172.16.11.48	TCP	66	52637 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
3748	57.762848	172.16.8.173	172.16.11.48	TCP	66	[TCP Retransmission] 52637 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
5862	59.714261	172.16.9.173	172.16.11.48	TCP	66	[TCP Retransmission] 52637 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
5118	63.772224	172.16.8.173	172.16.11.48	TCP	66	[TCP Retransmission] 52637 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
6354	67.444533	172.16.8.185	172.217.167.138	TCP	55	[TCP Keep-Alive] 59969 → 443 [ACK] Seq=1 Ack=1 Win=1821 Len=1
6355	67.444139	172.217.167.138	172.16.8.185	TCP	66	[TCP Keep-Alive ACK] 443 → 59969 [ACK] Seq=1 Ack=2 Win=257 Len=0 SLE=1 SRE=2
6631	72.774735	172.16.8.185	142.251.18.188	TCP	55	[TCP Keep-Alive] 59078 → 5228 [ACK] Seq=28 Ack=27 Win=1821 Len=1
6634	72.820888	142.251.18.188	172.16.8.185	TCP	66	[TCP Keep-Alive ACK] 5228 → 59078 [ACK] Seq=27 Ack=27 Win=290 Len=0 SLE=26 SRE=27

Inspecting the packets

Wireshark - Packet 2352 - 172.16.8.1

Frame 2352: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF{404F3AC0-98B5-4F8E-B836-14A0501581F1}, id 0

Ethernet II, Src: MicroStarInt, addr:36:ad:36:7e:ad:a3:78, Dst: 36:d2:b3:ccd:d1:03 (36:d2:b3:ccd:d1:03)

Internet Protocol Version 4, Src: 172.16.8.11, Dst: 172.16.9.65

Transmission Control Protocol, Src Port: 49447, Dst Port: 7680, Seq: 0, Len: 0

0000 36 d2 b3 cc d1 03 d4 3d 7e ad 43 78 08 00 45 00 6 ~ Cx ~ E

0010 00 34 52 29 40 00 00 06 3f 2e ac 10 08 0b ac 10 4R @ ~ ? ~

0020 09 41 c1 27 1e 00 3b f3 85 b3 00 00 00 00 02 .. A ~ ~ ~

0030 fa f8 69 e4 00 00 02 04 05 b4 01 03 00 01 01 .. l ~ ~ ~

0040 04 02 ..

No: 2352, Time: 33.327080, Source: 172.16.8.11 - Destination: 172.16.9.65 - Protocol: TCP - Length: 66 - Info: [TCP Retransmission] 49447 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

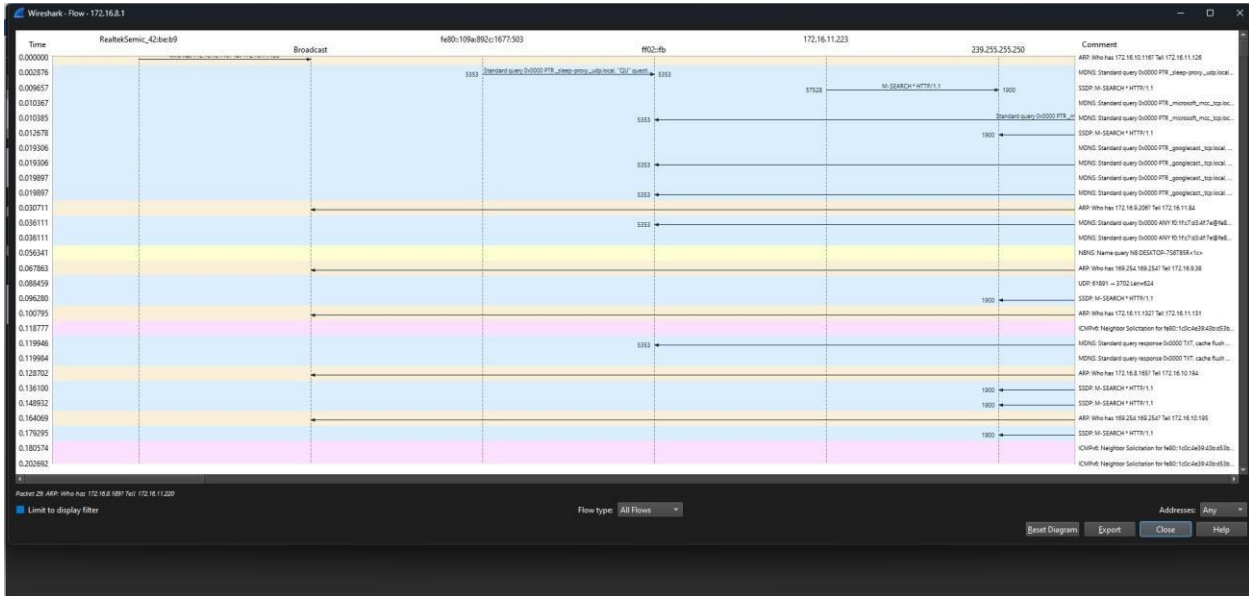
Show packet bytes

Close Help

NAME:KEERTHIKA.S

ROLL.NO:231901024

Flow Graph output



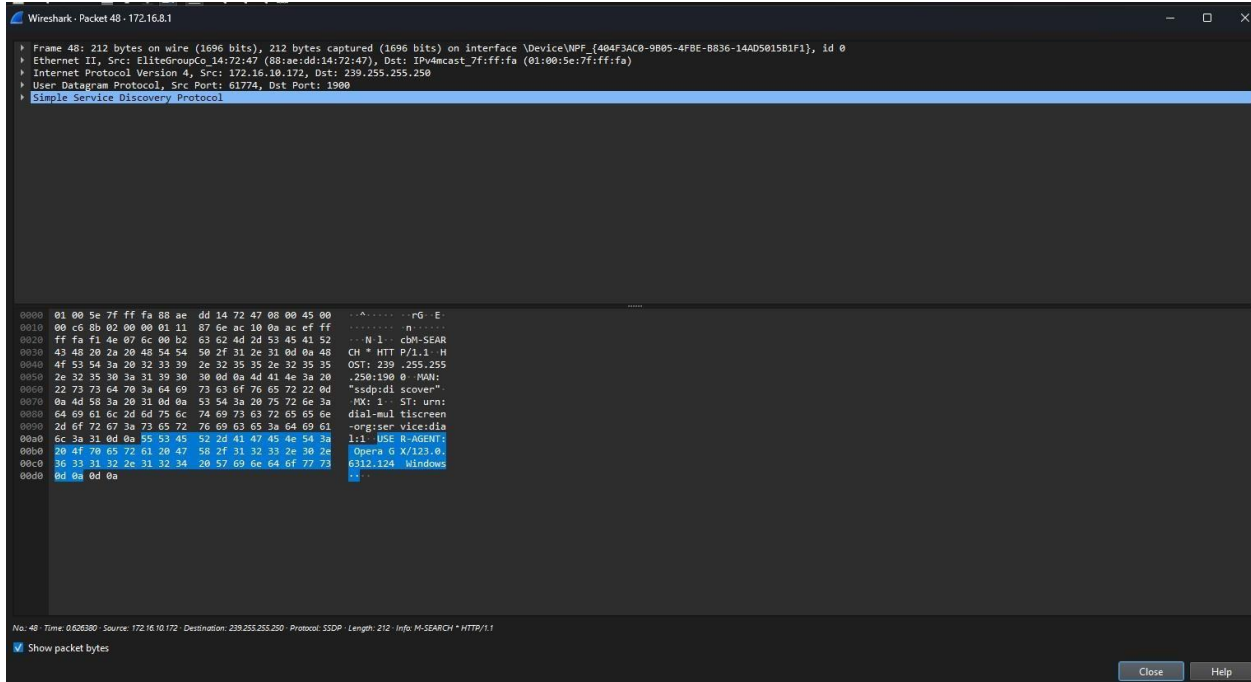
Output:tcp

No.	Time	Source	Destination	Protocol	Length	Info
0	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
1	0.000000	172.16.11.123	239.255.255.250	SSDP	71	63346 + 443 Len=29
2	0.000000	172.16.11.123	239.255.255.250	SSDP	68	443 + 63346 Len=26
3	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
4	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
5	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
6	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
7	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
8	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
9	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
10	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
11	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
12	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
13	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
14	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
15	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
16	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
17	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
18	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
19	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
20	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
21	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
22	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
23	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
24	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
25	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
26	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
27	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
28	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
29	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
30	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
31	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
32	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
33	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
34	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
35	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
36	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
37	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
38	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
39	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
40	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
41	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
42	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
43	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
44	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
45	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
46	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
47	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
48	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
49	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
50	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
51	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
52	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
53	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
54	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
55	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
56	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
57	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
58	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
59	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
60	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
61	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
62	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
63	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
64	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
65	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
66	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
67	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
68	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
69	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
70	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
71	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
72	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
73	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
74	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
75	0.000000	172.16.11.123	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1

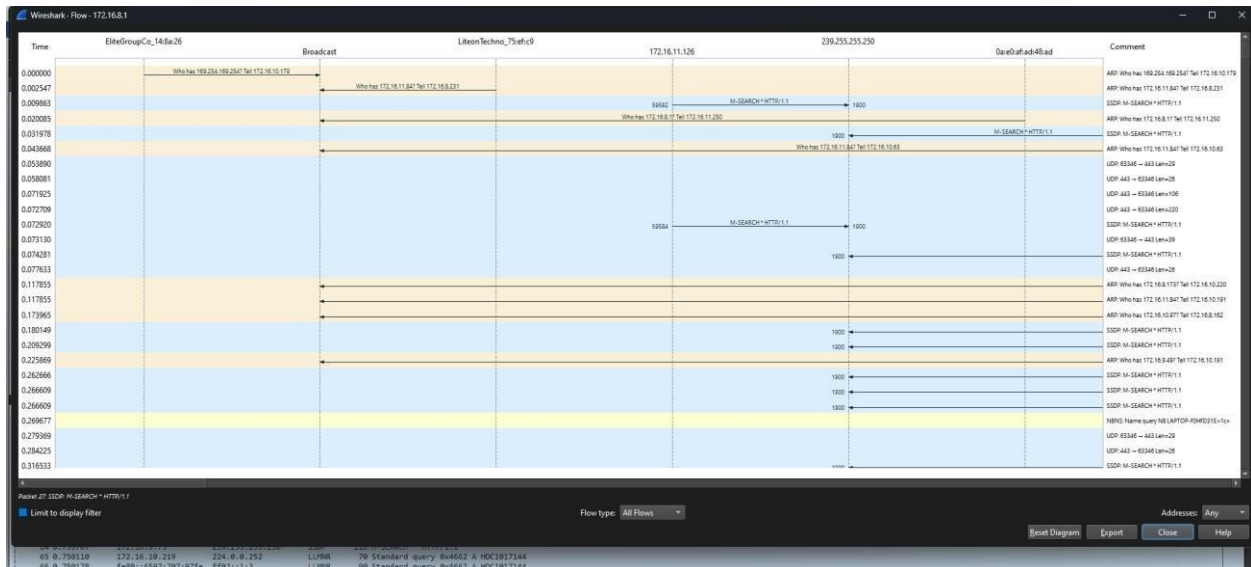
CSE(CYBER SECURITY)

Inspecting the packets

ROLL.NO:231901024



Flow chart output



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

CSE(CYBER SECURITY)

NAME:KEERTHIKA.S

ROLL.NO:231901024

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.

NAME:KEERTHIKA.S

ROLL.NO:231901024

Output

No.	Time	Source	Destination	Protocol	Length	Info
3	0.825842	61gabytech_8c184...	Broadcast	ARP	60	who has 172.16.11.218? Tell 172.16.11.222
15	0.12076	EliteGroupCo_35ee...	Broadcast	ARP	60	who has 169.254.169.254? Tell 172.16.10.178
16	0.236807	HP_3510bf2	Broadcast	ARP	60	who has 172.16.10.97? Tell 172.16.8.189
17	0.278549	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.9.63? Tell 172.16.10.118
19	0.319883	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.9.208? Tell 172.16.10.49
20	0.364115	Dell_3510ff98	Broadcast	ARP	60	who has 172.16.25.108? Tell 172.16.8.188
21	0.364115	Dell_3510ff98	Broadcast	ARP	60	who has 172.16.6.183? Tell 172.16.8.188
22	0.388779	Dell_3510ff98	Broadcast	ARP	60	who has 172.16.8.179? Tell 172.16.8.238
23	0.488227	HP_3510bf2	Broadcast	ARP	60	who has 172.16.10.97? Tell 172.16.8.162
24	0.453338	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.10.48? Tell 172.16.10.43
26	0.47771	EliteGroupCo_1472...	Broadcast	ARP	60	who has 169.254.169.254? Tell 172.16.10.190
28	0.494587	RealtekSemio_4218...	Broadcast	ARP	60	who has 172.16.9.57? Tell 172.16.9.235
30	0.533843	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.9.208? Tell 172.16.10.115
32	0.564951	Dell_3510ff98	Broadcast	ARP	60	who has 172.16.10.51? Tell 172.16.8.289
33	0.569354	MicroStarINT_ad18a...	Broadcast	ARP	60	who has 172.16.9.63? Tell 172.16.10.224
35	0.750917	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.8.165? Tell 172.16.10.31
36	0.750917	Dell_3510bf2	Broadcast	ARP	60	who has 172.16.8.117? Tell 172.16.11.8
38	0.752825	61gabytech_8c184...	Broadcast	ARP	60	Gratuitous ARP For 172.16.11.194 (Reply)
39	0.768795	RealtekSemio_4218...	Broadcast	ARP	60	who has 172.16.8.17? Tell 172.16.11.250
47	0.898024	Dell_3510ff98	Broadcast	ARP	60	who has 172.16.10.39? Tell 172.16.10.238
51	1.626436	Intel_772519f	Broadcast	ARP	60	who has 172.16.8.17? Tell 172.16.9.214
52	1.626436	Intel_772519f	Broadcast	ARP	60	who has 172.16.8.17? Tell 172.16.9.214
53	1.678841	HonHaiPrecis_8313...	Broadcast	ARP	60	who has 172.16.9.173? Tell 172.16.11.229
54	1.688086	Intel_772519f	Broadcast	ARP	60	who has 172.16.8.17? Tell 172.16.9.214
63	1.239511	HP_3510bf2	Broadcast	ARP	60	who has 172.16.10.97? Tell 172.16.8.189
64	1.255270	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.9.208? Tell 172.16.10.49
65	1.255270	EliteGroupCo_1472...	Broadcast	ARP	60	who has 169.254.169.254? Tell 172.16.10.190
66	1.427223	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.10.48? Tell 172.16.10.31
74	1.575648	MicroStarINT_ad18a...	Broadcast	ARP	60	who has 172.16.9.63? Tell 172.16.10.224
79	1.751140	Dell_3510bf2	Broadcast	ARP	60	who has 172.16.8.117? Tell 172.16.11.8
83	1.852802	Intel_772519f	Broadcast	ARP	60	who has 172.16.8.17? Tell 172.16.9.214
84	1.854562	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.10.72? Tell 172.16.11.120
85	1.864562	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.10.93? Tell 172.16.11.120
87	1.872726	RealtekSemio_4218...	Broadcast	ARP	60	who has 172.16.8.17? Tell 172.16.11.126
100	2.463908	Dell_3510bf2	Broadcast	ARP	60	who has 172.16.8.117? Tell 172.16.11.295
115	2.239519	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.10.48? Tell 172.16.10.31
117	2.259638	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.9.208? Tell 172.16.10.49
118	2.252190	EliteGroupCo_1472...	Broadcast	ARP	60	who has 169.254.169.254? Tell 172.16.10.190
124	2.405188	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.10.48? Tell 172.16.10.43
125	2.409718	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.11.48? Tell 172.16.10.39
131	2.645240	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.10.72? Tell 172.16.11.120
132	2.645240	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.10.93? Tell 172.16.11.120
135	2.718374	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.10.48? Tell 172.16.10.20
140	2.825589	EliteGroupCo_1472...	Broadcast	ARP	60	who has 169.254.169.254? Tell 172.16.10.211
153	2.830549	ASUSTeKCOMP_94icb...	Broadcast	ARP	60	who has 172.16.8.155? Tell 172.16.11.229
155	3.459889	HP_3510bf2	Broadcast	ARP	60	who has 172.16.10.97? Tell 172.16.8.162
162	3.239662	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.10.48? Tell 172.16.10.31
164	3.237749	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.8.165? Tell 172.16.10.31
167	3.374858	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.10.48? Tell 172.16.10.20
179	3.408773	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.10.48? Tell 172.16.10.43
171	3.470618	HonHaiPrecis_8313...	Broadcast	ARP	60	who has 172.16.8.17? Tell 172.16.11.229
174	3.497988	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.9.75? Tell 172.16.10.42
178	5.529211	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.9.208? Tell 172.16.10.115
189	5.645025	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.10.72? Tell 172.16.11.120
190	5.645025	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.10.93? Tell 172.16.11.120

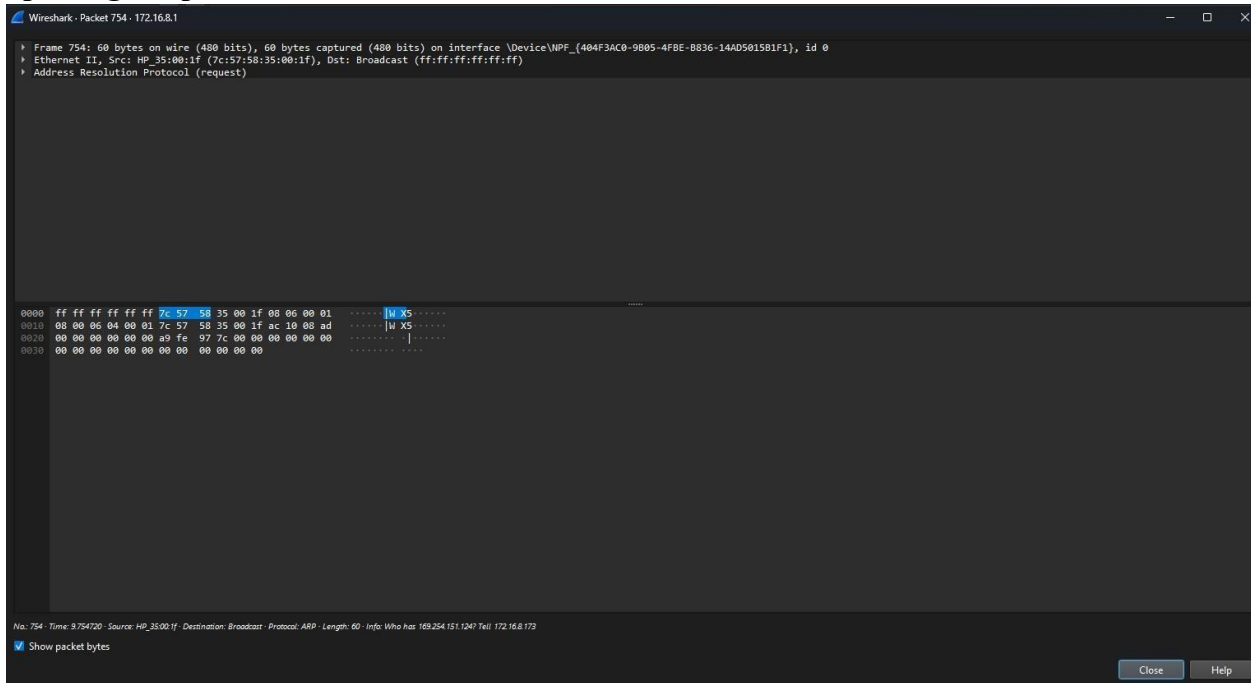
No.	Time	Source	Destination	Protocol	Length	Info
197	5.762228	EliteGroupCo_1472...	Broadcast	ARP	60	who has 169.254.169.254? Tell 172.16.10.211
204	5.900941	RealtekSemio_4218...	Broadcast	ARP	60	who has 172.16.8.17? Tell 172.16.11.126
205	5.912085	HP_3510bf2	Broadcast	ARP	60	who has 172.16.10.97? Tell 172.16.8.162
206	5.915868	Dell_3510bf2	Broadcast	ARP	60	who has 172.16.8.117? Tell 172.16.11.8
209	6.053199	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.9.208? Tell 172.16.10.115
210	6.040408	ASUSTeKCOMP_94icb...	Broadcast	ARP	60	who has 172.16.11.48? Tell 172.16.11.208
212	6.069574	ASUSTeKCOMP_94icb...	Broadcast	ARP	60	who has 172.16.8.155? Tell 172.16.11.220
214	6.107784	767a1651ff7f40	Broadcast	ARP	60	who has 172.16.9.78? Tell 172.16.11.79
215	6.107784	767a1651ff7f40	Broadcast	ARP	60	who has 172.16.11.97? Tell 172.16.11.79
217	6.239982	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.8.165? Tell 172.16.10.31
220	6.268068	RealtekSemio_4218...	Broadcast	ARP	60	who has 172.16.9.133? Tell 172.16.11.126
222	6.318414	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.9.75? Tell 172.16.10.42
226	6.374085	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.10.48? Tell 172.16.10.20
243	6.748716	Dell_3510bf2	Broadcast	ARP	60	who has 172.16.8.117? Tell 172.16.11.8
247	6.773297	EliteGroupCo_1472...	Broadcast	ARP	60	who has 169.254.169.254? Tell 172.16.10.211
253	6.907484	HP_3510bf2	Broadcast	ARP	60	who has 172.16.10.97? Tell 172.16.8.162
258	5.051300	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.9.208? Tell 172.16.10.115
259	5.961841	ASUSTeKCOMP_94icb...	Broadcast	ARP	60	who has 172.16.11.48? Tell 172.16.11.220
267	5.151623	ASUSTeKCOMP_94icb...	Broadcast	ARP	60	who has 172.16.10.20? Tell 172.16.11.120
268	5.151623	ASUSTeKCOMP_94icb...	Broadcast	ARP	60	who has 172.16.8.39? Tell 172.16.11.220
269	5.295554	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.8.165? Tell 172.16.10.31
274	5.318075	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.9.75? Tell 172.16.10.42
284	5.420839	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.10.48? Tell 172.16.10.31
293	5.508057	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.10.48? Tell 172.16.10.43
294	5.595780	767a1651ff7f40	Broadcast	ARP	60	who has 172.16.9.78? Tell 172.16.11.79
305	5.747521	Dell_3510bf2	Broadcast	ARP	60	who has 172.16.8.117? Tell 172.16.11.8
313	5.878880	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.10.72? Tell 172.16.11.120
314	5.878880	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.10.93? Tell 172.16.11.120
320	5.924552	RealtekSemio_4218...	Broadcast	ARP	60	who has 172.16.8.17? Tell 172.16.11.126
326	6.055884	ASUSTeKCOMP_94icb...	Broadcast	ARP	60	who has 172.16.11.48? Tell 172.16.11.220
335	6.142793	767a1651ff7f40	Broadcast	ARP	60	who has 172.16.9.78? Tell 172.16.11.79
337	6.261325	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.10.48? Tell 172.16.10.31
343	6.318075	EliteGroupCo_1472...	Broadcast	ARP	60	who has 169.254.169.254? Tell 172.16.10.171
344	6.342561	RealtekSemio_4218...	Broadcast	ARP	60	who has 172.16.8.42? Tell 172.16.11.126
351	6.489550	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.9.63? Tell 172.16.10.118
354	6.440725	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.10.48? Tell 172.16.10.43
370	6.644242	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.10.72? Tell 172.16.11.120
371	6.644242	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.10.93? Tell 172.16.11.120
392	6.818591	HP_3510bf2	Broadcast	ARP	60	who has 172.16.8.165? Tell 172.16.8.166
396	6.842067	Dell_3510ff98	Broadcast	ARP	60	who has 172.16.25.108? Tell 172.16.8.188
397	6.842067	Dell_3510ff98	Broadcast	ARP	60	who has 172.16.6.183? Tell 172.16.8.188
428	7.054344	HP_3510bf2	Broadcast	ARP	60	who has 172.16.10.97? Tell 172.16.8.162
441	7.195416	RealtekSemio_4218...	Broadcast	ARP	60	who has 172.16.8.17? Tell 172.16.11.250
442	7.242090	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.10.48? Tell 172.16.10.31
449	7.273779	EliteGroupCo_1472...	Broadcast	ARP	60	who has 169.254.169.254? Tell 172.16.10.171
450	7.273775	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.9.63? Tell 172.16.10.118
452	7.321413	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.8.165? Tell 172.16.10.31
453	7.356848	Dell_3510ff98	Broadcast	ARP	60	who has 172.16.25.108? Tell 172.16.8.188
454	7.356848	Dell_3510ff98	Broadcast	ARP	60	who has 172.16.6.183? Tell 172.16.8.188
464	7.449409	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.10.48? Tell 172.16.10.43
480	7.518140	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.9.208? Tell 172.16.10.115
480	7.643612	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.10.72? Tell 172.16.11.120
487	7.643612	MicroStarINT_c5icb...	Broadcast	ARP	60	who has 172.16.10.93? Tell 172.16.11.120
497	7.69678	RealtekSemio_4218...	Broadcast	ARP	60	who has 172.16.8.17? Tell 172.16.11.250
506	7.903718	HP_3510bf2	Broadcast	ARP	60	who has 172.16.10.97? Tell 172.16.8.162
508	7.933862	Payatton_eb14:32	Broadcast	ARP	60	who has 172.16.10.69? Tell 172.16.9.147

CSE(CYBER SECURITY)

NAME:KEERTHIKA.S

ROLL.NO:231901024

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.

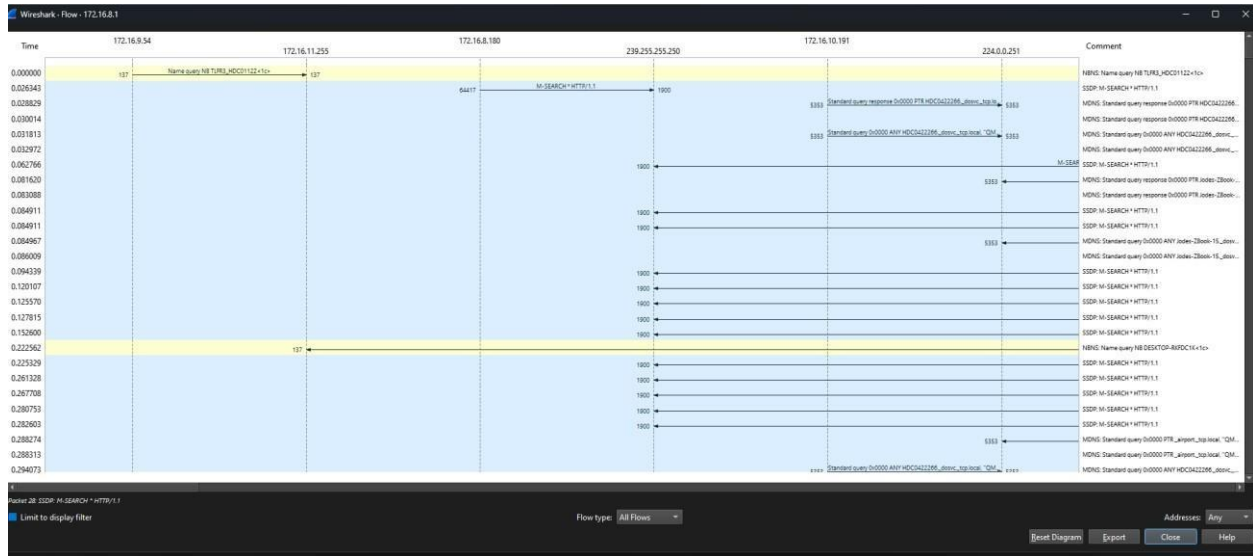
Output

dns					
No.	Time	Source	Destination	Protocol	Length Info
805	5.920690	172.16.8.185	172.16.8.1	DNS	74 Standard query 0xd1ca A www.google.com
806	5.920859	172.16.8.185	172.16.8.1	DNS	74 Standard query 0xdcea HTTPS www.google.com
807	5.922217	172.16.8.1	172.16.8.185	DNS	90 Standard query response 0xd1ca A www.google.com A 142.250.196.36
808	5.922217	172.16.8.1	172.16.8.185	DNS	99 Standard query response 0xdcea HTTPS www.google.com HTTPS

NAME:KEERTHIKA.S


ROLL.NO:231901024

Flow 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.

NAME:KEERTHIKA.S

ROLL.NO:231901024

Output

Io.	Time	Source	Destination	Protocol	Length	Info
614	7.685024	172.16.8.184	34.104.35.123	HTTP	520	GET /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e...
617	7.698858	34.104.35.123	172.16.8.184	HTTP	731	HTTP/1.1 416 Requested range not satisfiable
618	7.700353	172.16.8.184	34.104.35.123	HTTP	500	HEAD /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e...
619	7.709986	34.104.35.123	172.16.8.184	HTTP	667	HTTP/1.1 200 OK
624	7.742844	172.16.8.184	34.104.35.123	HTTP	520	GET /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e...
626	7.752652	34.104.35.123	172.16.8.184	HTTP	731	HTTP/1.1 416 Requested range not satisfiable
627	7.754181	172.16.8.184	34.104.35.123	HTTP	500	HEAD /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e...
630	7.764711	34.104.35.123	172.16.8.184	HTTP	706	HTTP/1.1 200 OK
634	7.790436	172.16.8.184	34.104.35.123	HTTP	520	GET /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e...
635	7.799887	34.104.35.123	172.16.8.184	HTTP	731	HTTP/1.1 416 Requested range not satisfiable
636	7.801361	172.16.8.184	34.104.35.123	HTTP	500	HEAD /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e...
637	7.809151	34.104.35.123	172.16.8.184	HTTP	667	HTTP/1.1 200 OK
639	7.838248	172.16.8.184	34.104.35.123	HTTP	520	GET /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e...
642	7.852555	34.104.35.123	172.16.8.184	HTTP	692	HTTP/1.1 416 Requested range not satisfiable
643	7.854134	172.16.8.184	34.104.35.123	HTTP	500	HEAD /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e...
645	7.871249	34.104.35.123	172.16.8.184	HTTP	706	HTTP/1.1 200 OK
648	7.901837	172.16.8.184	34.104.35.123	HTTP	520	GET /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e...
649	7.912361	34.104.35.123	172.16.8.184	HTTP	731	HTTP/1.1 416 Requested range not satisfiable
650	7.914442	172.16.8.184	34.104.35.123	HTTP	500	HEAD /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e...
651	7.922388	34.104.35.123	172.16.8.184	HTTP	667	HTTP/1.1 200 OK
652	7.949279	172.16.8.184	34.104.35.123	HTTP	520	GET /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e...
654	7.961780	34.104.35.123	172.16.8.184	HTTP	731	HTTP/1.1 416 Requested range not satisfiable
655	7.963277	172.16.8.184	34.104.35.123	HTTP	500	HEAD /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e...
658	7.973876	34.104.35.123	172.16.8.184	HTTP	706	HTTP/1.1 200 OK
5969	68.003432	172.16.8.184	34.104.35.123	HTTP	520	GET /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e...
5975	68.021813	34.104.35.123	172.16.8.184	HTTP	692	HTTP/1.1 416 Requested range not satisfiable
5977	68.022279	172.16.8.184	34.104.35.123	HTTP	500	HEAD /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e...
5982	68.037182	34.104.35.123	172.16.8.184	HTTP	706	HTTP/1.1 200 OK
6000	68.060979	172.16.8.184	34.104.35.123	HTTP	520	GET /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e...
6009	68.075015	34.104.35.123	172.16.8.184	HTTP	731	HTTP/1.1 416 Requested range not satisfiable
6010	68.075735	172.16.8.184	34.104.35.123	HTTP	500	HEAD /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e...
6012	68.095897	34.104.35.123	172.16.8.184	HTTP	706	HTTP/1.1 200 OK
6016	68.113543	172.16.8.184	34.104.35.123	HTTP	520	GET /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e...
6020	68.127351	34.104.35.123	172.16.8.184	HTTP	692	HTTP/1.1 416 Requested range not satisfiable
6022	68.128754	172.16.8.184	34.104.35.123	HTTP	500	HEAD /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e...
6026	68.147978	34.104.35.123	172.16.8.184	HTTP	706	HTTP/1.1 200 OK
6027	68.165225	172.16.8.184	34.104.35.123	HTTP	520	GET /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e...
6031	68.178231	34.104.35.123	172.16.8.184	HTTP	692	HTTP/1.1 416 Requested range not satisfiable
6032	68.179227	172.16.8.184	34.104.35.123	HTTP	500	HEAD /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e...
6033	68.191504	34.104.35.123	172.16.8.184	HTTP	667	HTTP/1.1 200 OK
6036	68.212702	172.16.8.184	34.104.35.123	HTTP	520	GET /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e...
6037	68.221863	34.104.35.123	172.16.8.184	HTTP	731	HTTP/1.1 416 Requested range not satisfiable
6038	68.222707	172.16.8.184	34.104.35.123	HTTP	500	HEAD /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e...
6040	68.232365	34.104.35.123	172.16.8.184	HTTP	667	HTTP/1.1 200 OK
6047	68.260625	172.16.8.184	34.104.35.123	HTTP	520	GET /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e...
6048	68.269573	34.104.35.123	172.16.8.184	HTTP	692	HTTP/1.1 416 Requested range not satisfiable
6049	68.270838	172.16.8.184	34.104.35.123	HTTP	500	HEAD /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e...
6050	68.282851	34.104.35.123	172.16.8.184	HTTP	706	HTTP/1.1 200 OK
13471	128.310870	172.16.8.184	34.104.35.123	HTTP	520	GET /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e...
13475	128.326936	34.104.35.123	172.16.8.184	HTTP	731	HTTP/1.1 416 Requested range not satisfiable

NAME:KEERTHIKA.S

ROLL.NO:231901024

Inspecting the packets

Wireshark · Packet 78794 · Ethernet

> Frame 78794: 692 bytes on wire (5536 bits), 692 bytes captured (5536 bits) on interface 0
> Ethernet II, Src: Sophos_cf:be:45 (7c:5a:1c:cf:be:45), Dst: 7c:57:58:34:fd:06 (7c:57:58:34:fd:06)
> Internet Protocol Version 4, Src: 34.104.35.123, Dst: 172.16.8.184
> Transmission Control Protocol, Src Port: 80, Dst Port: 50274, Seq: 1, Ack: 467, Len: 638
> Hypertext Transfer Protocol

0000	7c 57 58 34 fd 06 7c 5a 1c cf be 45 08 00 45 00	WX4... Z...E..E..
0010	02 a6 c0 46 40 00 40 06 7d 60 22 68 23 7b ac 10	...F@.@...} `h#{...
0020	08 b8 00 50 c4 62 52 16 61 0f aa 0c 2a af 50 18	...P.bR...a...*.P..
0030	00 ed cb 95 00 00 48 54 54 50 2f 31 2e 31 20 34HT TP/1.1 4
0040	31 36 20 52 65 71 75 65 73 74 65 64 20 72 61 6e	16 Reque sted ran
0050	67 65 20 6e 6f 74 20 73 61 74 69 73 66 69 61 62	ge not s atisfiab
0060	6c 65 0d 0a 61 63 63 65 70 74 2d 72 61 6e 67 65	le..acce pt-range
0070	73 3a 20 6e 6f 6e 65 0d 0a 63 6f 6e 74 65 6e 74	s: none..content
0080	2d 64 69 73 70 6f 73 69 74 69 6f 6e 3a 20 61 74	-disposi tion: at
0090	74 61 63 68 6d 65 6e 74 0d 0a 63 6f 6e 74 65 6e	tachment ..conten
00a0	74 2d 73 65 63 75 72 69 74 79 2d 70 6f 6c 69 63	t-securi ty-polici
00b0	79 3a 20 64 65 66 61 75 6c 74 2d 73 72 63 20 27	y: defau lt-src '
00c0	6e 6f 6e 65 27 0d 0a 73 65 72 76 65 72 3a 20 47	none'...s erver: G
00d0	6f 6f 67 6c 65 2d 45 64 67 65 2d 43 61 63 68 65	oogle-Ed ge-Cache
00e0	0d 0a 78 2d 63 6f 6e 74 65 6e 74 2d 74 79 70 65	..x-cont ent-type
00f0	2d 6f 70 74 69 6f 6e 73 3a 20 6e 6f 73 6e 69 66	-options : nosnif
0100	66 0d 0a 78 2d 66 72 61 6d 65 2d 6f 70 74 69 6f	f..x-fra me-optio
0110	6e 73 3a 20 53 41 4d 45 4f 52 49 47 49 4e 0d 0a	ns: SAME ORIGIN..
0120	78 2d 78 73 73 2d 70 72 6f 74 65 63 74 69 6f 6e	x-xss-pr otection
0130	3a 20 30 0d 0a 63 6f 6e 74 65 6e 74 2d 6c 65 6e	: 0..con tent-len
0140	67 74 68 3a 20 30 0d 0a 78 2d 72 65 71 75 65 73	gth: 0..x-reques
0150	74 2d 69 64 3a 20 35 32 64 62 32 34 31 33 2d 61	t-id: 52 db2413-a
0160	65 34 35 2d 34 30 63 66 2d 38 37 30 65 2d 39 61	e45-40cf -870e-9a
0170	30 37 61 32 61 33 38 65 64 39 0d 0a 64 61 74 65	07a2a38e d9..date
0180	3a 20 57 65 64 2c 20 30 37 20 41 75 67 20 32 30	: Wed, 0 7 Aug 20
0190	32 34 20 31 38 3a 30 38 3a 31 36 20 47 4d 54 0d	24 18:08 :16 GMT..
01a0	0a 61 67 65 3a 20 33 35 35 31 31 0d 0a 6c 61 73	age: 35 511..las
01b0	74 2d 6d 6f 64 69 66 69 65 64 3a 20 4d 6f 6e 2c	t-modifi ed: Mon,
01c0	20 30 35 20 41 75 67 20 32 30 32 34 20 31 38 3a	05 Aug 2024 18:
01d0	30 32 3a 31 35 20 47 4d 54 0d 0a 65 74 61 67 3a	02:15 GM T..etag:
01e0	20 22 32 65 65 34 36 31 38 22 0d 0a 63 6f 6e 74	"2ee461 8"..cont
01f0	65 6e 74 2d 74 79 70 65 3a 20 61 70 70 6c 69 63	ent-type : applic
0200	61 74 69 6f 6e 2f 6f 63 74 65 74 2d 73 74 72 65	ation/oc tet-stre
0210	61 6d 0d 0a 61 6c 74 2d 73 76 63 3a 20 68 33 3d	am..alt- svc: h3=
0220	22 3a 34 34 33 22 3b 20 6d 61 3d 32 35 39 32 30	":443"; ma=25920
0230	30 30 2c 20 68 33 2d 32 39 3d 22 3a 34 34 33 22	00, h3-2 9=":443"
0240	3b 20 6d 61 3d 32 35 39 32 30 30 30 0d 0a 63 61	; ma=259 2000..ca
0250	63 68 65 2d 63 6f 6e 74 72 6f 6c 3a 20 70 75 62	che-cont rol: pub
0260	6c 69 63 2c 6d 61 78 2d 61 67 65 3d 38 36 34 30	lic,max- age=8640
0270	30 0d 0a 56 69 61 3a 20 48 54 54 50 2f 31 2e 31	0..Via: HTTP/1.1
0280	20 66 6f 72 77 61 72 64 2e 68 74 74 70 2e 70 72	forward .http.pr
0290	6f 78 79 3a 33 31 32 38 0d 0a 43 6f 6e 6e 65 63	oxy:3128 ..Connec

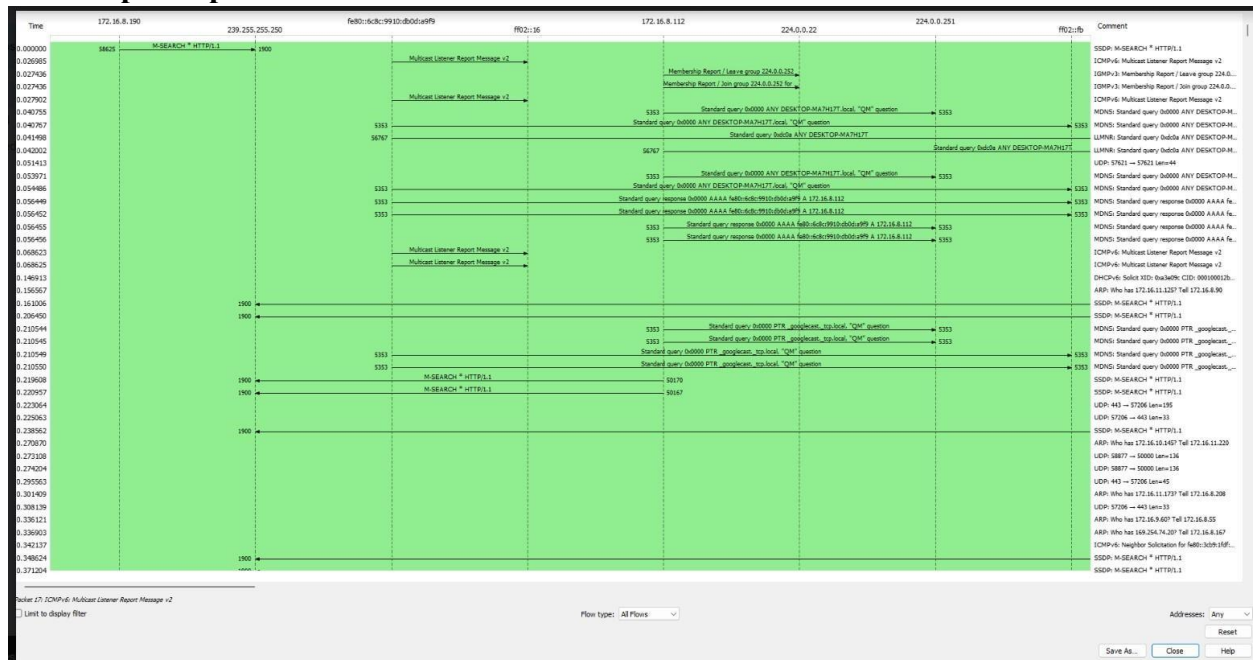
Close Help

CSE(CYBER SECURITY)

NAME:KEERTHIKA.S

ROLL.NO:231901024

Flow Graph output



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

Procedure

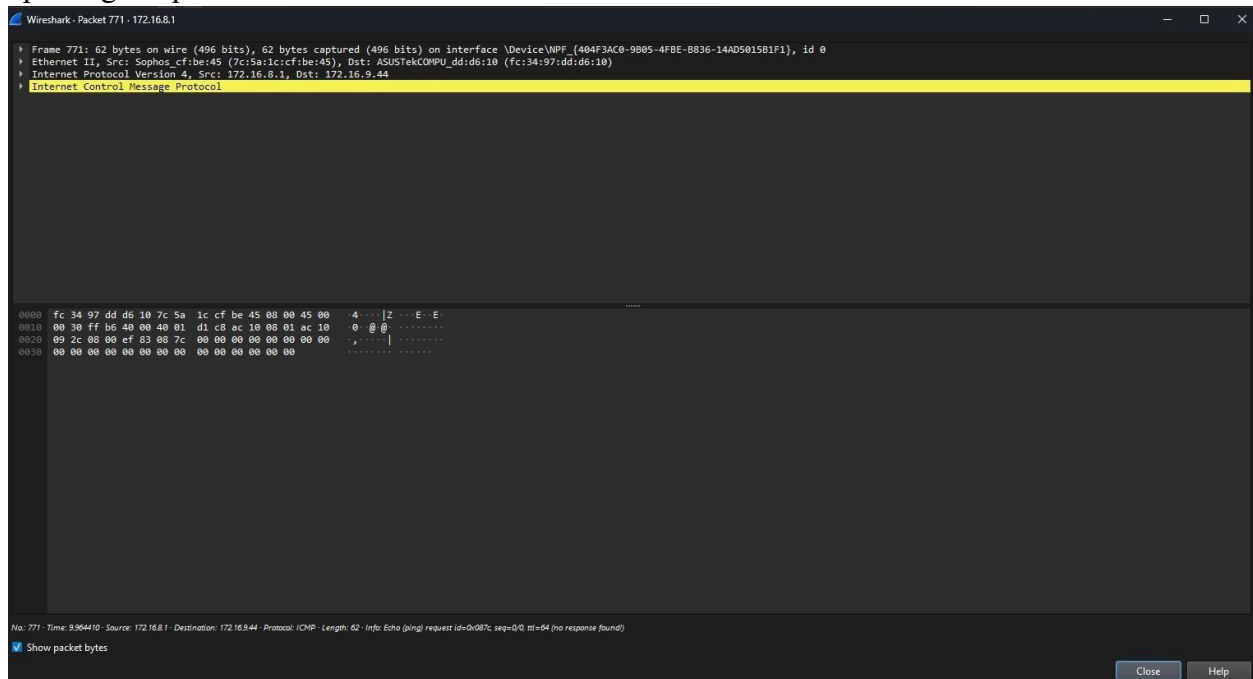
- Select Local Area Connection in Wireshark.
- Go to capture ☹ option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search ICMP/IP packets in search bar.
- Save the packets

Output:icmp

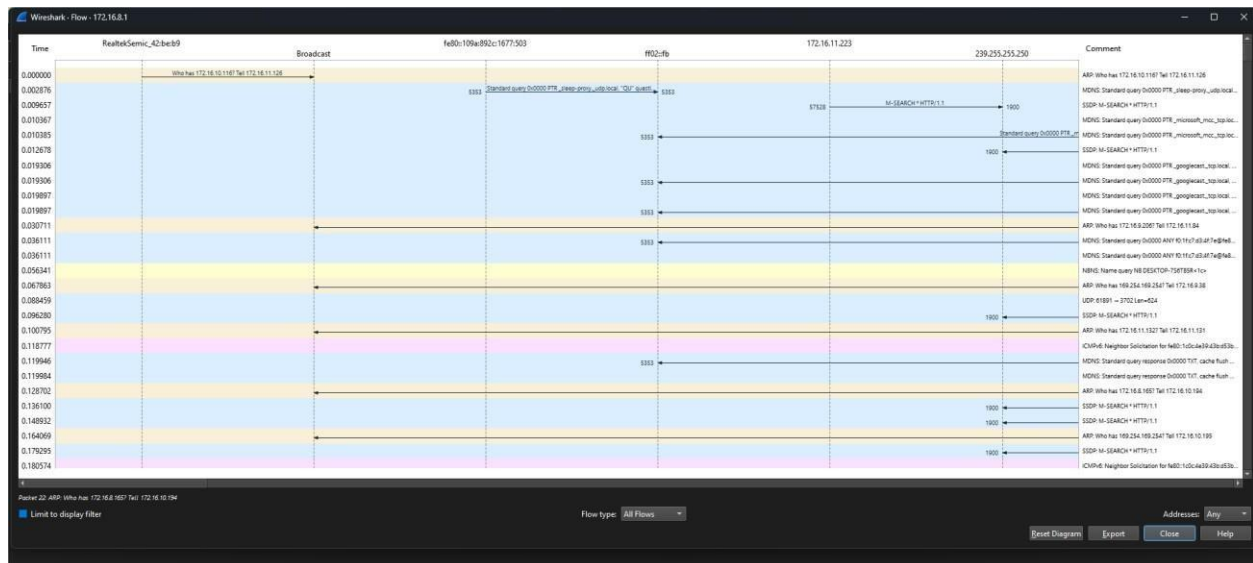
No.	Time	Source	Destination	Protocol	Length	Info
771	9.964410	172.16.9.1	172.16.9.44	ICMP	62	Echo (ping) request id=0x087c, seq=0/0, ttl=64 (no response found!)

Inspecting the packets

ROLL.NO:231901024



Flow Graph output



CSE(CYBER SECURITY)

NAME:KEERTHIKA.S

ROLL.NO:231901024

Output:ip

No.	Time	Source	Destination	Protocol	Length	Info
8	0.050881	142.250.182.142	172.16.8.185	UDP	68	443 → 63346 Len=26
9	0.071925	142.250.182.142	172.16.8.185	UDP	148	443 → 63346 Len=106
10	0.072709	142.250.182.142	172.16.8.185	UDP	262	443 → 63346 Len=200
11	0.072920	172.16.11.126	239.255.255.250	SSDP	217	H-SEARCH * HTTP/1.1
12	0.073130	172.16.8.185	142.250.182.142	UDP	81	63346 → 443 Len=39
13	0.074281	172.16.9.128	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
14	0.077633	142.250.182.142	172.16.8.185	UDP	68	443 → 63346 Len=26
15	0.180149	172.16.8.212	239.255.255.250	SSDP	217	H-SEARCH * HTTP/1.1
19	0.209299	172.16.11.129	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
21	0.262666	172.16.11.239	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
22	0.266689	172.16.8.226	239.255.255.250	SSDP	218	H-SEARCH * HTTP/1.1
23	0.266689	172.16.11.83	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
24	0.269677	172.16.8.231	172.16.11.255	NBNS	92	Name query NB LAPTOP-F0WFD31E1c<*
25	0.279369	172.16.8.185	142.250.182.142	UDP	71	63346 → 443 Len=29
26	0.284225	142.250.182.142	172.16.8.185	UDP	68	443 → 63346 Len=26
27	0.310333	172.16.8.37	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
29	0.342090	172.16.8.169	239.255.255.250	SSDP	217	H-SEARCH * HTTP/1.1
30	0.353355	172.16.9.69	239.255.255.250	SSDP	217	H-SEARCH * HTTP/1.1
31	0.360149	172.16.10.190	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
32	0.367863	172.16.11.4	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
35	0.433642	172.16.9.192	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
36	0.440731	172.16.10.196	239.255.255.250	SSDP	217	H-SEARCH * HTTP/1.1
37	0.442081	172.16.9.219	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
38	0.447140	172.16.8.32	239.255.255.250	SSDP	217	H-SEARCH * HTTP/1.1
39	0.500999	172.16.8.185	142.250.182.142	UDP	71	63346 → 443 Len=29
41	0.505941	142.250.182.142	172.16.8.185	UDP	68	443 → 63346 Len=26
44	0.543334	172.16.10.43	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
46	0.639658	172.16.11.130	239.255.255.250	SSDP	217	H-SEARCH * HTTP/1.1
47	0.639658	172.16.11.132	239.255.255.250	SSDP	217	H-SEARCH * HTTP/1.1
49	0.627664	172.16.8.163	172.16.11.255	NBNS	92	Name query NB DESKTOP-BKFDCK1C1<*
50	0.640564	172.16.8.16	239.255.255.250	SSDP	217	H-SEARCH * HTTP/1.1
51	0.640162	172.16.9.171	239.255.255.250	SSDP	217	H-SEARCH * HTTP/1.1
52	0.631986	172.16.8.112	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
53	0.633616	172.16.8.112	239.255.255.250	SSDP	217	H-SEARCH * HTTP/1.1
54	0.696278	172.16.8.178	239.255.255.250	SSDP	217	H-SEARCH * HTTP/1.1
55	0.696362	172.16.9.6	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
56	0.707188	172.16.8.185	142.250.182.142	UDP	71	63346 → 443 Len=29
57	0.712816	142.250.182.142	172.16.8.185	UDP	68	443 → 63346 Len=26
59	0.731196	172.16.8.238	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
60	0.737464	172.16.10.219	224.0.0.252	LWMR	70	Standard query 0xcff1 A HDC1817144
62	0.739882	172.16.10.219	224.0.0.252	LWMR	70	Standard query 0xcff7 A HDC1817144
64	0.739707	172.16.9.75	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
65	0.750110	172.16.10.219	224.0.0.252	LWMR	70	Standard query 0x4662 A HDC1817144
67	0.751187	172.16.10.219	224.0.0.252	LWMR	70	Standard query 0x604d AAAA HDC1817144
69	0.764152	172.16.10.219	172.16.11.255	BROWSER	220	Request Announcement V1\$FEL2
70	0.769820	172.16.8.218	224.0.0.251	NBNS	220	Standard query response 0xb000 PTR Jodes-ZBook-15_dosvc_tcp.local SRV 0 0 7680 Jodes-ZBook-15.local TXT
71	0.771823	172.16.8.218	224.0.0.251	NBNS	92	Standard query 0xb000 aly Jodes-ZBook-15_dosvc_tcp.local "Q"
74	0.775139	172.16.9.174	172.16.11.255	BROWSER	243	Local Master Announcement HDC1817144, Workstation, Server, NT Workstation, Potential Browser, Backup Browser, Master Browser
75	0.786882	172.16.10.219	224.0.0.252	LWMR	70	Standard query 0x3346 A HDC1817144
76	0.786882	172.16.10.219	224.0.0.252	LWMR	70	Standard query 0x7645 AAAA HDC1817144
77	0.786882	172.16.10.219	224.0.0.252	LWMR	70	Standard query 0xc072 A HDC1817144
78	0.786882	172.16.10.219	224.0.0.252	LWMR	70	Standard query 0x3791 AAAA HDC1817144
79	0.786882	172.16.10.219	224.0.0.252	LWMR	70	Standard query 0x4816 A HDC1817144
80	0.786882	172.16.10.219	224.0.0.252	LWMR	70	Standard query 0xc4cd AAAA HDC1817144
83	0.789964	172.16.8.238	239.255.255.250	SSDP	217	H-SEARCH * HTTP/1.1
88	0.789964	172.16.10.219	172.16.11.255	BROWSER	220	Request Announcement V1\$FEL2

Inspecting the packets

Wireshark - Packet 47 - 172.16.8.1

Frame 47: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface \Device\NPF_{404F3AC0-9805-4FBE-B836-14A05015B1F1}, id 0

Ethernet II, Src: 0a:00:a1:01:9e:0a (0a:00:a1:01:9e:0a), Dst: IP4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)

Internet Protocol Version 4, Src: 172.16.11.130, Dst: 239.255.255.250

User Datagram Protocol, Src Port: 59614, Dst Port: 1900

Simple Service Discovery Protocol

0000 01 00 5c 7f ff fa 0a e0 af ca 01 9e 08 00 45 00E

0010 00 cb c9 88 00 00 01 11 48 05 ac 10 0b 8a ef ffH.....

0020 ff fa e8 de 87 6c 00 b7 c1 fe 4d 2d 53 45 41 52l...M-SEAR

0030 43 4b 20 2a 20 40 64 54 50 2f 31 2e 31 0d 0a 4b C# * HTTP/1.1 H

0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 OST: 239.255.255

0050 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20 .250:190 0 -MAN:

0060 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 2d 8d "ssdp:discover"

0070 0a 4d 50 3a 20 31 0d 0a 53 50 3a 20 75 72 6e 3a RQ: 1 - ST: urn:

0080 64 69 61 6c 2d 6d 75 6c 7a 69 73 63 72 65 65 6e dial-multiscreen

0090 2d 6f 72 67 3a 73 65 72 76 69 63 65 3a 64 69 61 -org:service:dia

00a0 6c 3a 31 0d 0a 55 53 45 52 2d 41 47 45 4e 54 3a l:1 USE R-AGENT:

00b0 20 40 69 63 72 6f 73 6f 66 74 20 45 64 67 65 4f Microsoft Edge/

00c0 31 32 37 2e 30 2e 32 36 35 31 2e 30 36 20 57 69 127.0.20.51:66 bl

00d0 6e 64 6f 77 73 0d 0a 0d 0a ndows 6.1

No. 47: Time: 0.619859 - Source: 172.16.11.130 - Destination: 239.255.255.250 - Protocol: SSDP - Length: 217 - Info: M-SEARCH * HTTP/1.1

Show packet bytes

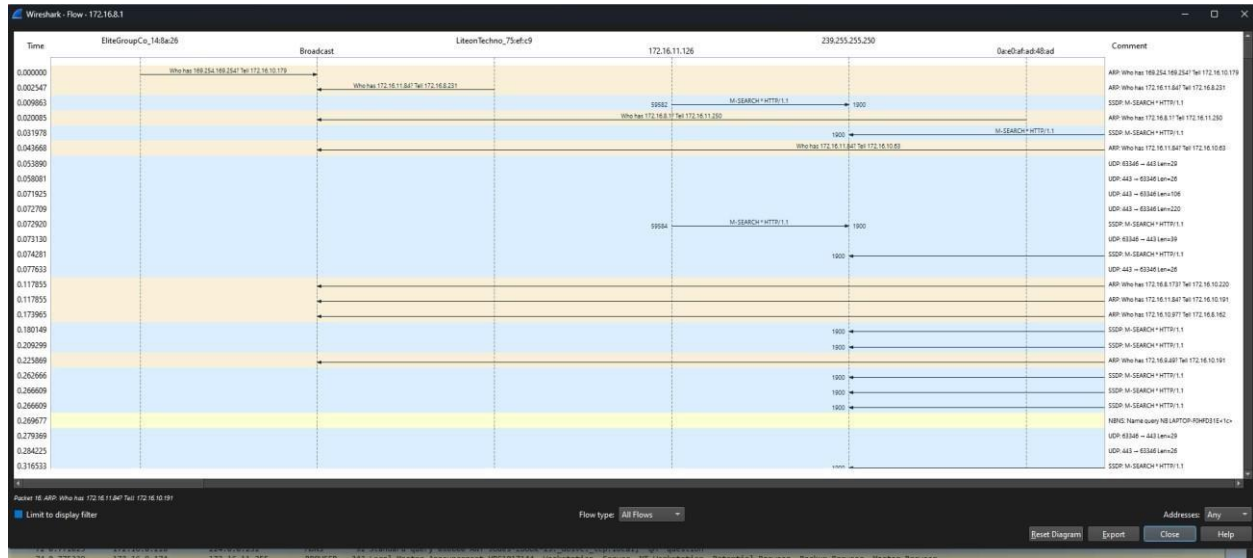
Close Help

CSE(CYBER SECURITY)

NAME:KEERTHIKA.S

ROLL.NO:231901024

Flow chart 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

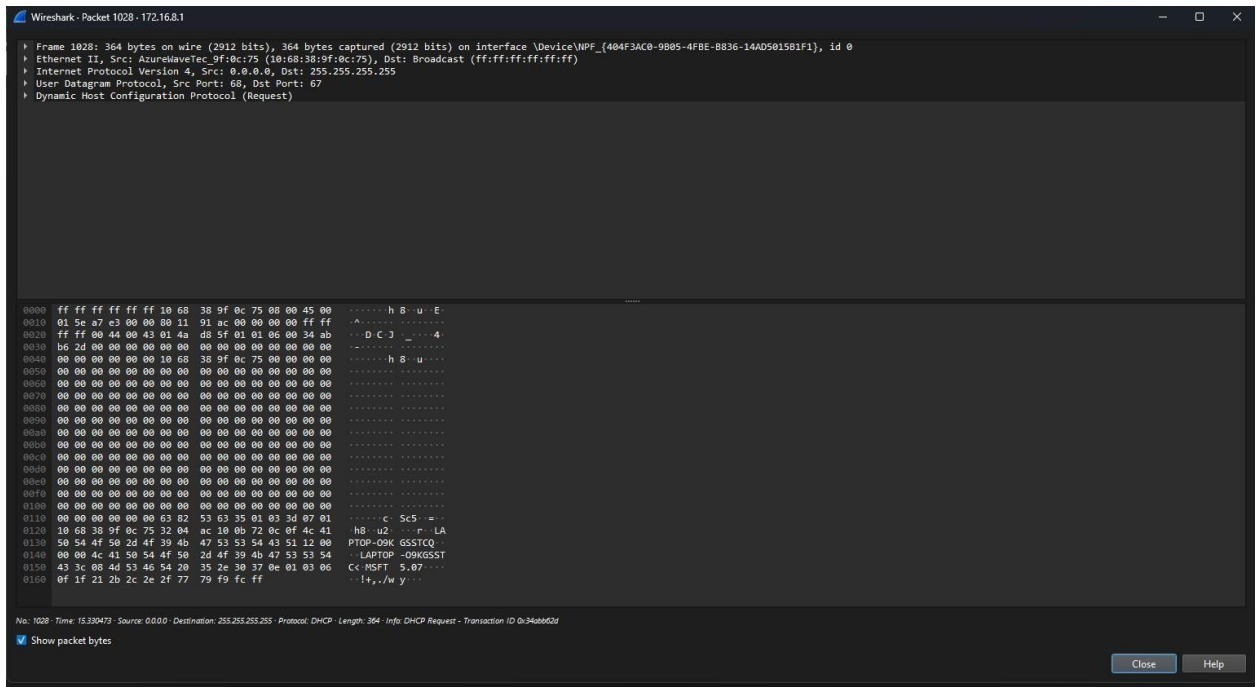
NAME:KEERTHIKA.S

ROLL.NO:231901024

Output

No.	Time	Source	Destination	Protocol	Length	Info
770	9.964499	0.0.0.0	255.255.255.255	DHCP	340	DHCP Discover - Transaction ID 0xf19cf3d1
852	10.003200	0.0.0.0	255.255.255.255	DHCP	350	DHCP Request - Transaction ID 0xf19cf3d1
1028	15.330473	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x34abb62d

Inspecting the packets



Result:

Thus the output was verified successfully.

NAME:KEERTHIKA.S

ROLL.NO:231901024

CSE(CYBER SECURITY)