

YARRA JAISURYA

231901063

CSE CS

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**

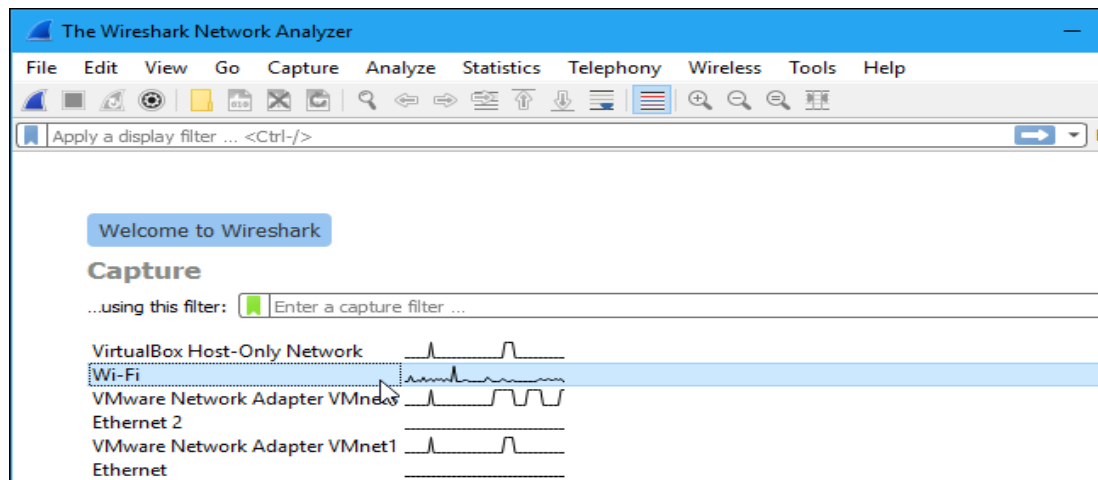
Getting Wireshark

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

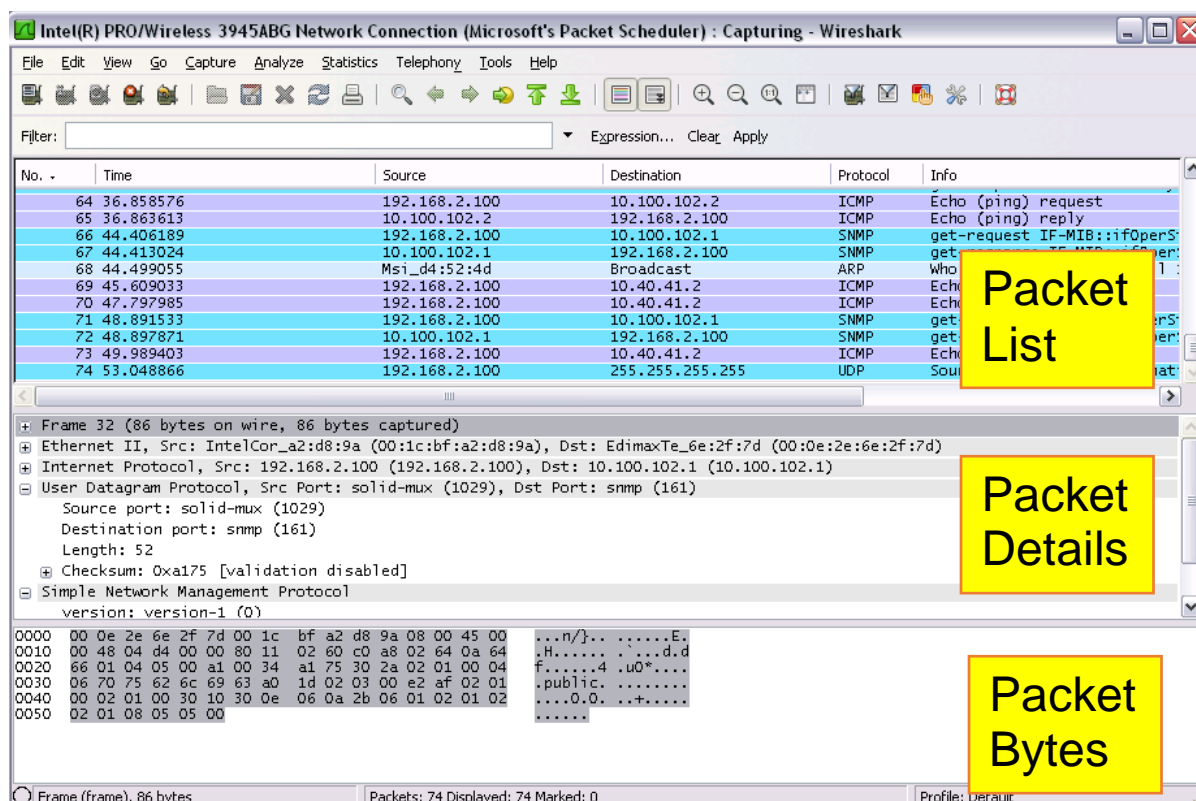
After downloading and installing Wireshark, launch it and double-click the name of a network interface under Capture to start capturing packets on that interface

YARRA JAISURYA
231901063
CSE CS



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.



YARRA JAISURYA

231901063

CSE CS

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

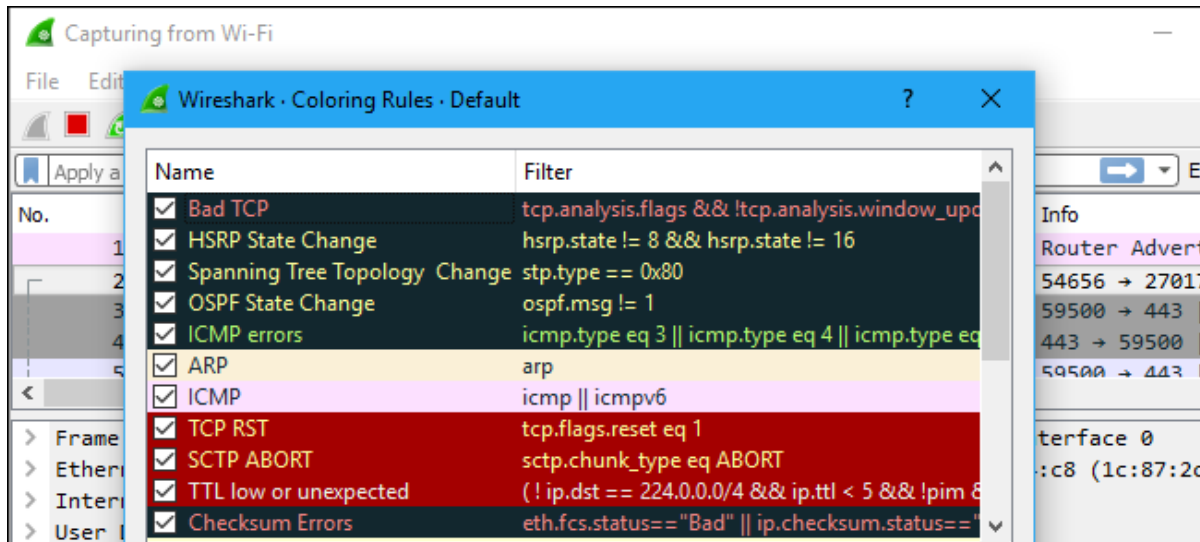
The packet bytes pane shows the data of the current packet (selected in the “Packet List” pane) in a hexdump style.

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.

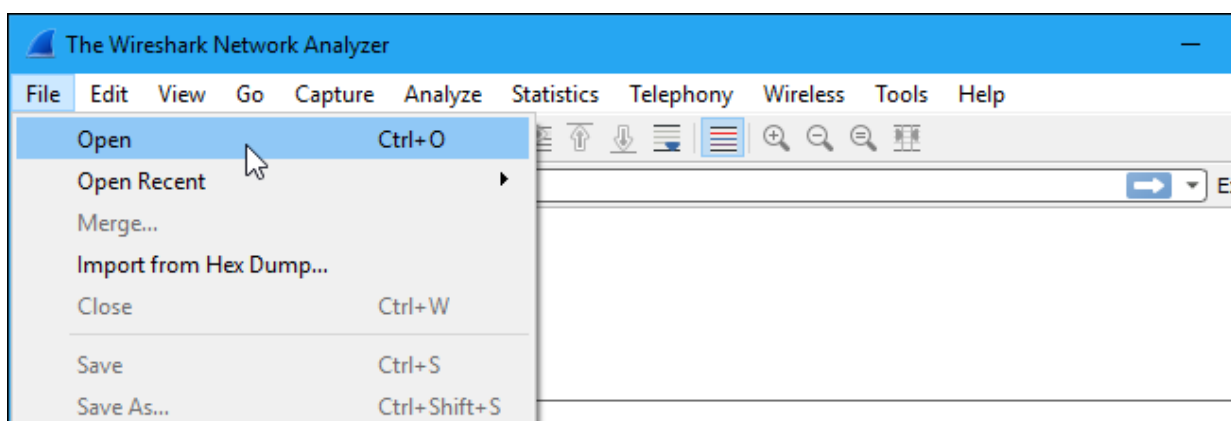
YARRA JAISURYA
231901063
CSE CS



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

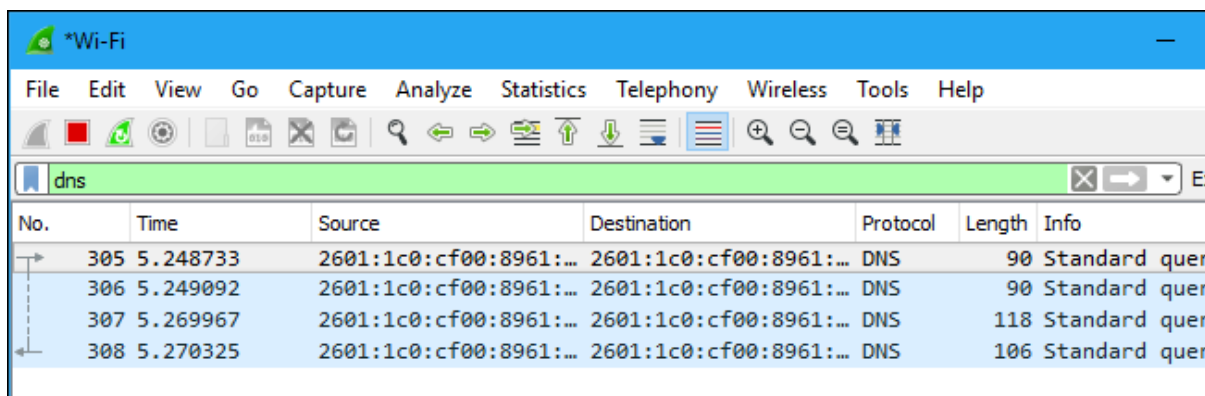
YARRA JAISURYA

231901063

CSE CS

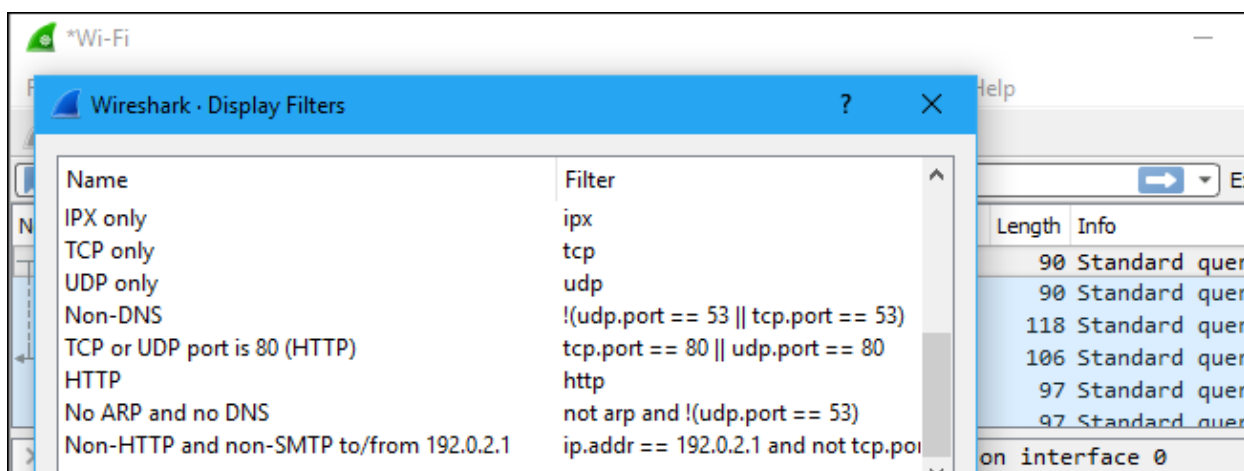
traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark's filters come in.

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.

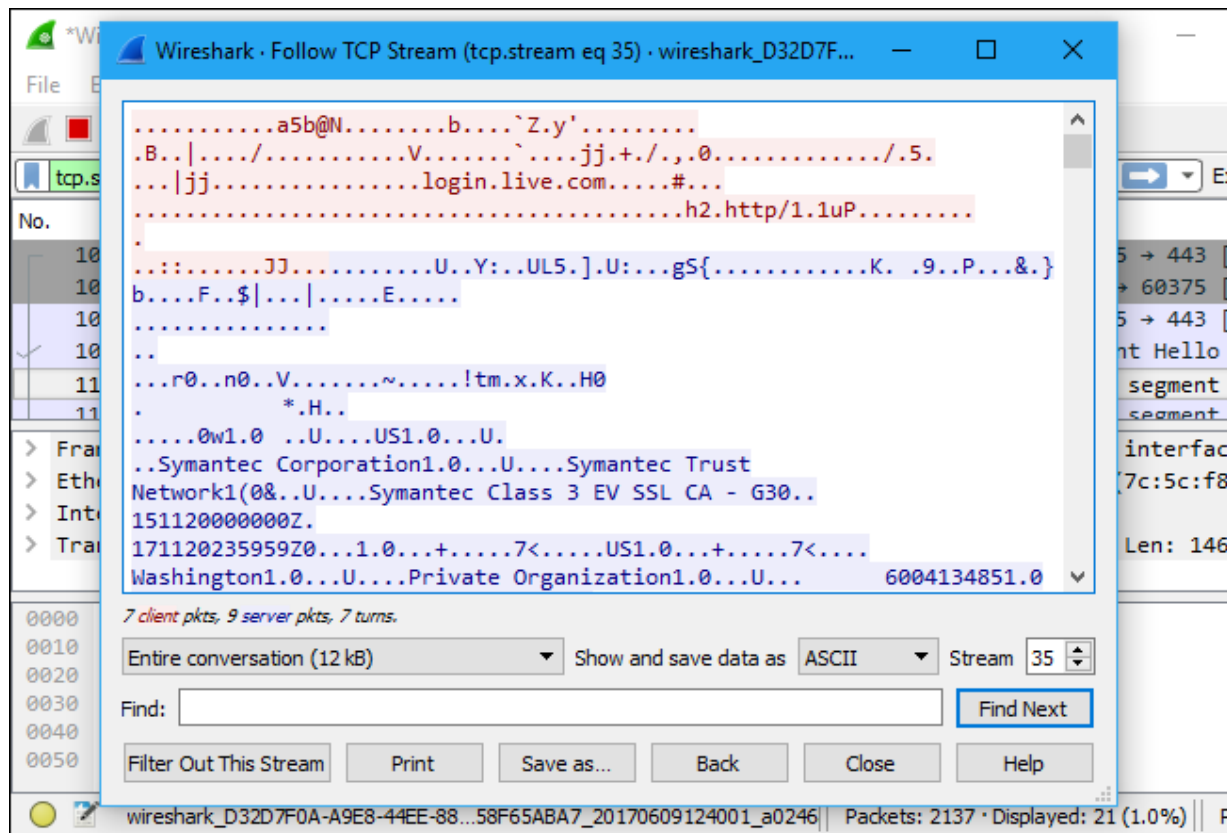
For more information on Wireshark's display filtering language, read the [Building display filter expressions](#) page in the official Wireshark documentation.



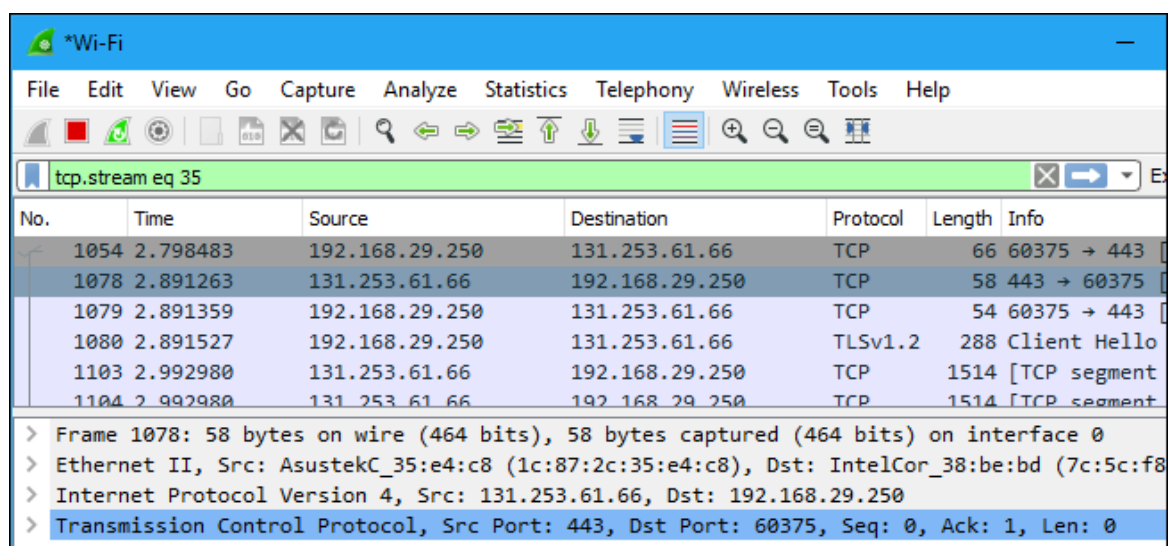
Another interesting thing you can do is right-click a packet and select Follow > TCP Stream.

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.

YARRA JAISURYA
231901063
CSE CS



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.

YARRA JAISURYA

231901063

CSE CS

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 frame 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:

Offset	Hex	ASCII
0000	1c 87 2c 35 e4 c8 7c 5c f8 38 be bd 08 00 45 00	...,5.. \ .8....E.
0010	00 34 0b 5d 40 00 80 06 4f 85 c0 a8 1d fa 83 fd	.4.]@... 0.....
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	..

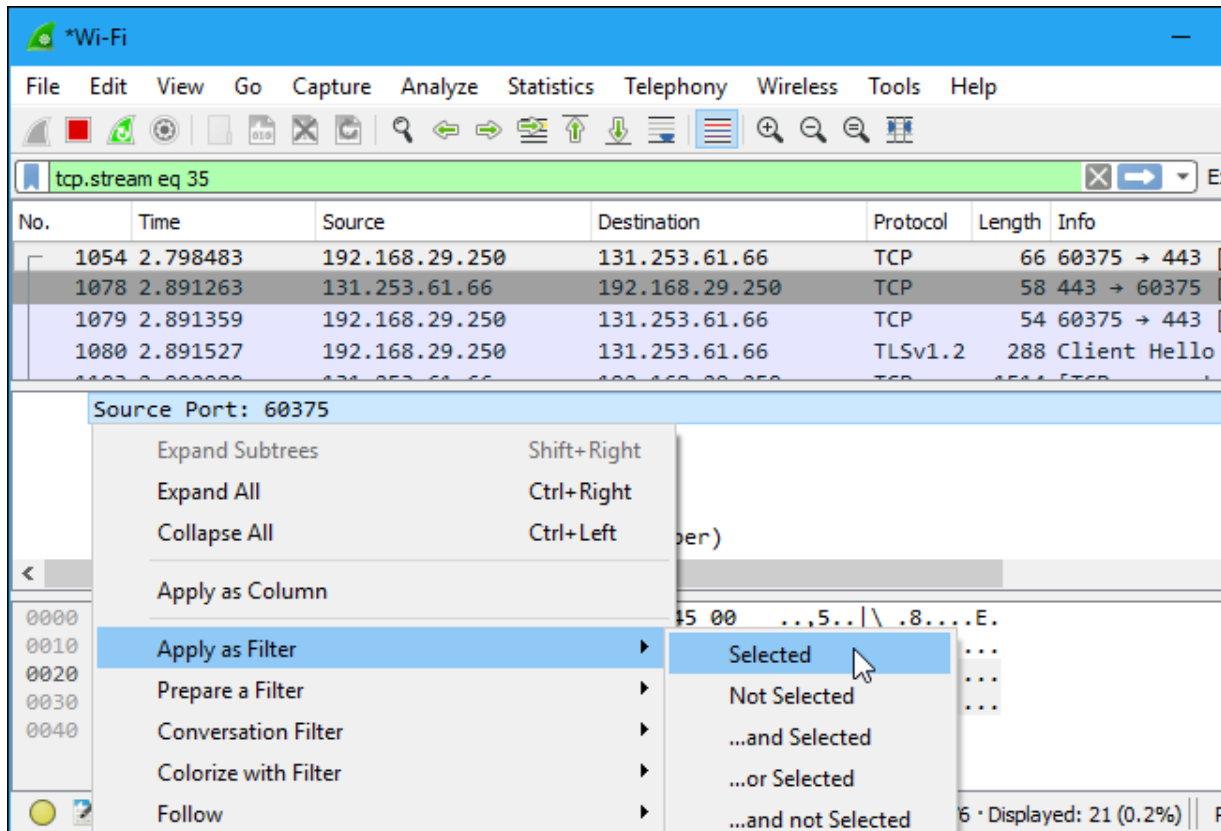
The status bar at the bottom indicates the encapsulation type (frame.encap_type) and the number of packets displayed (21 out of 8136, or 0.3%).

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.

YARRA JAISURYA

231901063

CSE CS



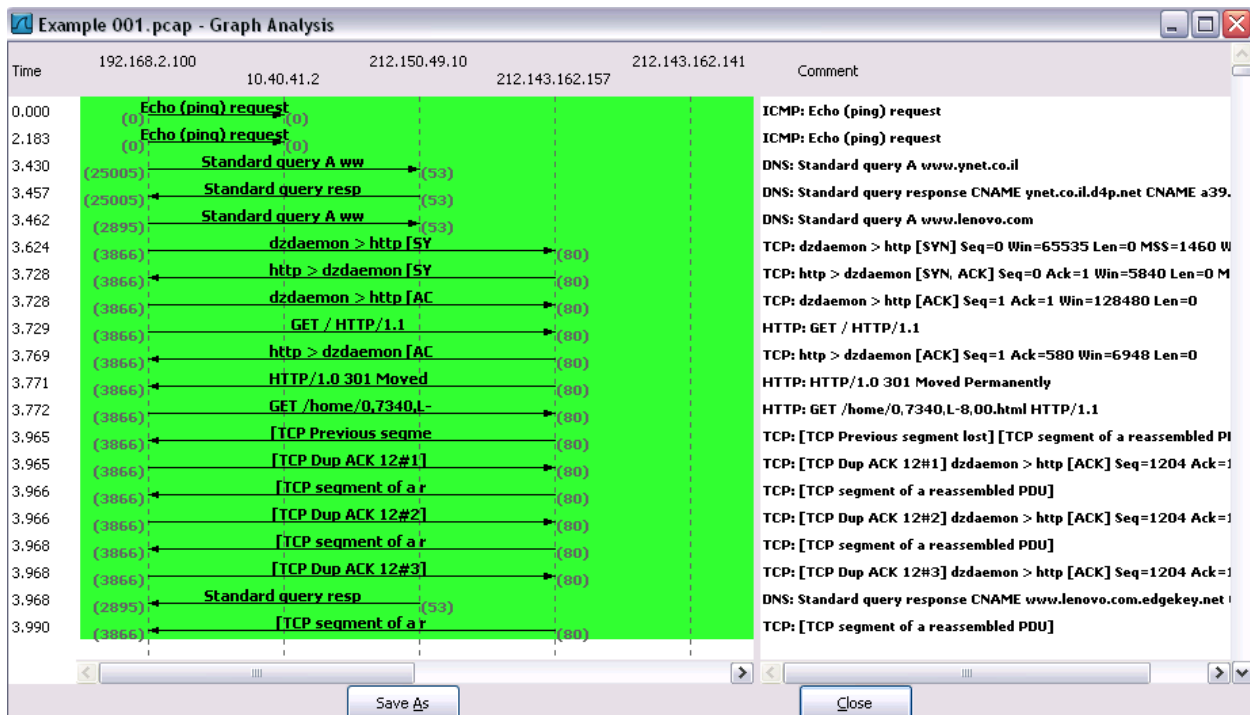
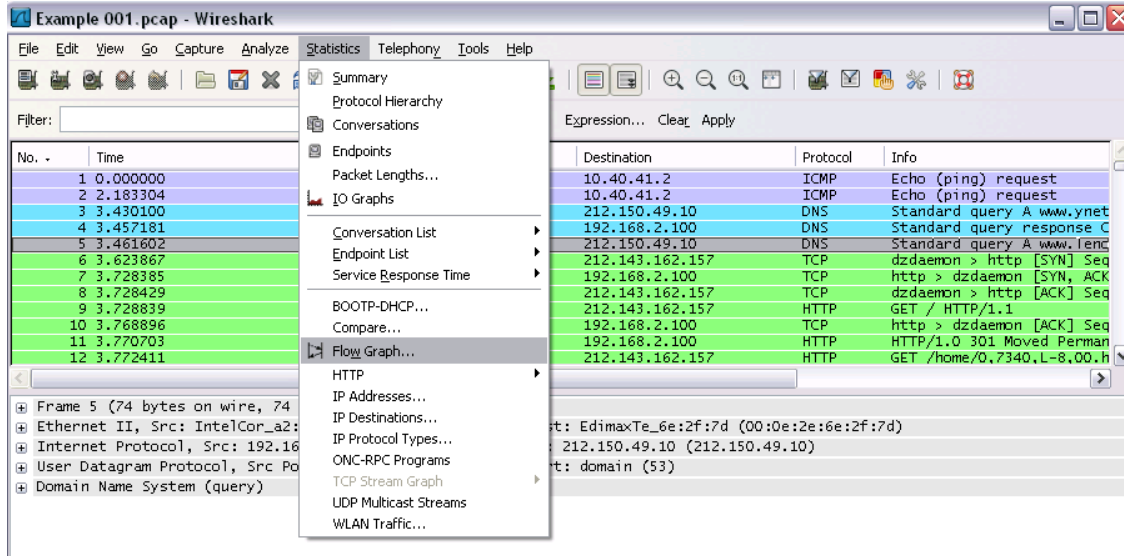
Wireshark is an extremely powerful tool, and this tutorial is just scratching the surface of what you can do with it. Professionals use it to debug network protocol implementations, examine security problems and inspect network protocol internals.

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

YARRA JAISURYA

231901063

CSE CS



YARRA JAISURYA

231901063

CSE CS

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

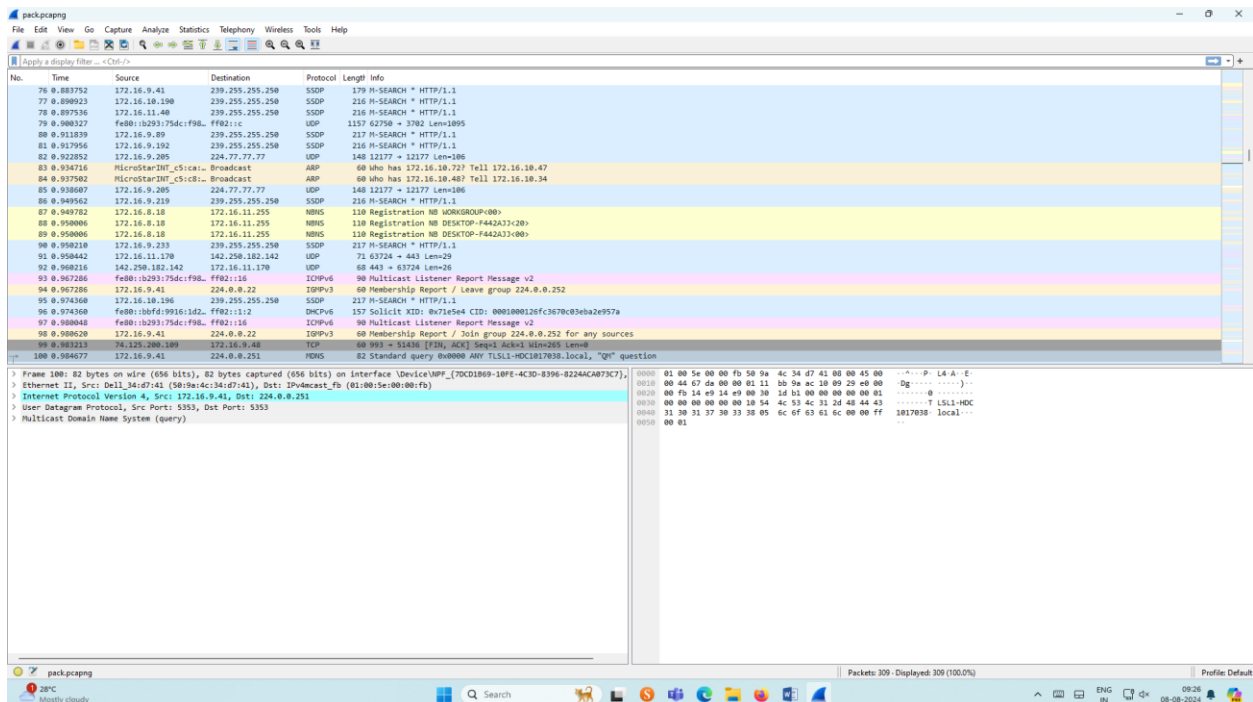
Exercises

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 main window shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, and Length. The selected packet (No. 100) is a Multicast Domain Name System (query) packet. The packet details pane on the right shows the hierarchical structure of the selected packet, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Multicast Domain Name System (query). The packet bytes pane at the bottom shows the raw data of the selected packet.



YARRA JAISURYA

231901063

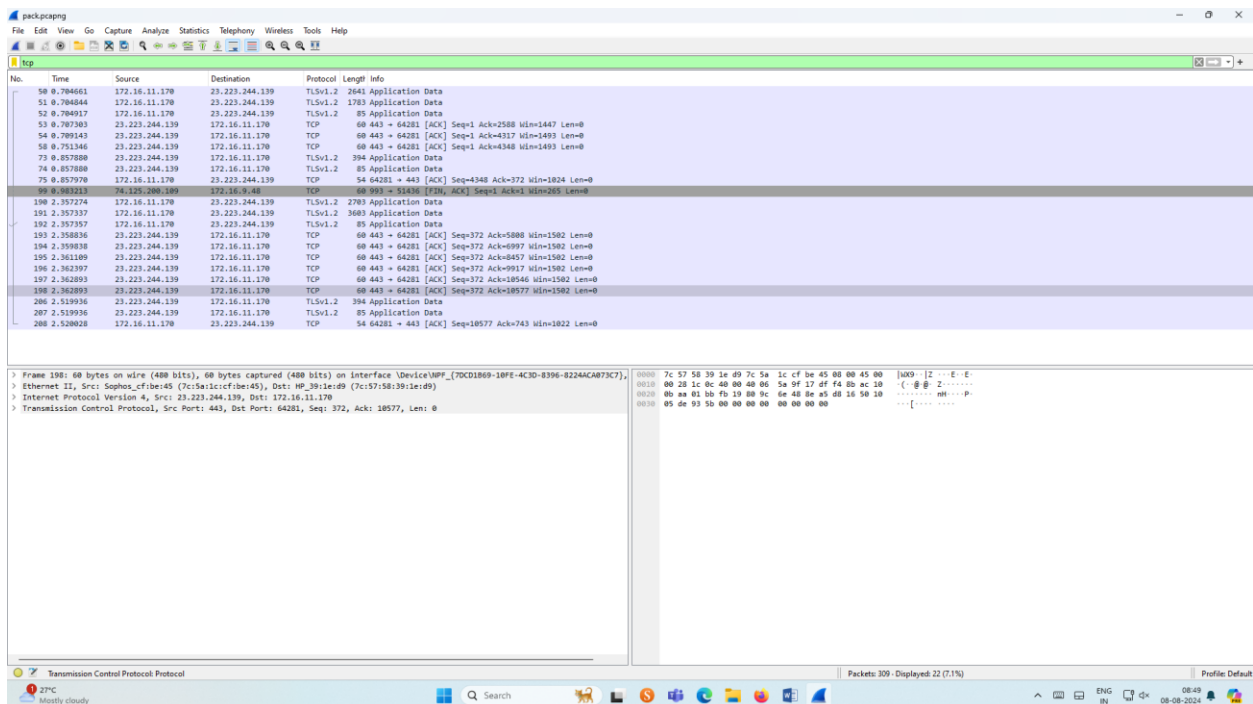
CSE CS

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 StatisticsFlow graph.
- Save the packets.

Output:



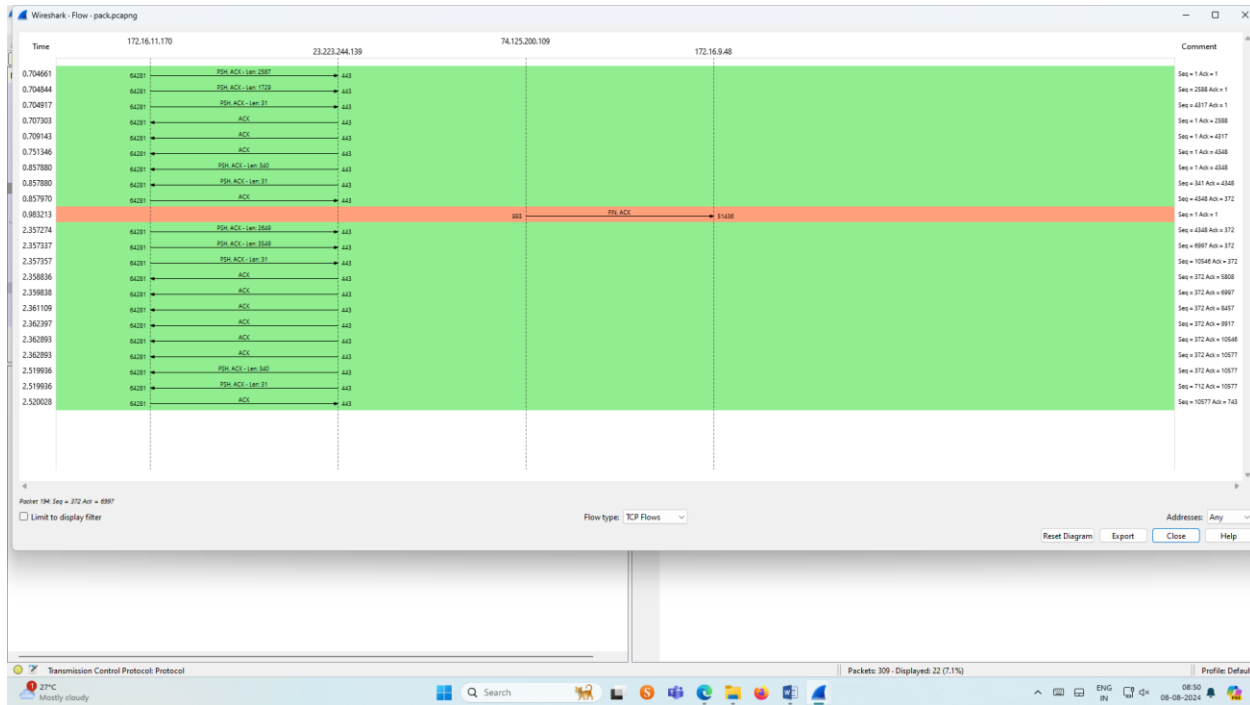
The screenshot displays the Wireshark interface with a packet capture of TCP traffic. The packet list shows several TCP segments from 172.16.11.170 to 23.223.244.139. The packet details pane shows the structure of a TCP segment, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
98	0.794661	172.16.11.170	23.223.244.139	TLSv1.2	2641	Application Data
99	0.796044	172.16.11.170	23.223.244.139	TLSv1.2	1793	Application Data
100	0.796917	172.16.11.170	23.223.244.139	TLSv1.2	85	Application Data
101	0.797303	23.223.244.139	172.16.11.170	TCP	60	443 → 64281 [ACK] Seq=1 Ack=2568 Win=1447 Len=0
102	0.798143	23.223.244.139	172.16.11.170	TCP	60	443 → 64281 [ACK] Seq=1 Ack=4317 Win=1493 Len=0
103	0.751346	23.223.244.139	172.16.11.170	TCP	60	443 → 64281 [ACK] Seq=1 Ack=4348 Win=1493 Len=0
104	0.857888	23.223.244.139	172.16.11.170	TLSv1.2	394	Application Data
105	0.857888	23.223.244.139	172.16.11.170	TLSv1.2	85	Application Data
106	0.857970	172.16.11.170	23.223.244.139	TCP	54	64281 → 443 [ACK] Seq=4348 Ack=372 Win=1824 Len=0
107	0.981213	172.16.11.170	23.223.244.139	TCP	60	443 → 64281 [ACK] Seq=1 Ack=1 Win=205 Len=0
108	2.357274	172.16.11.170	23.223.244.139	TLSv1.2	2789	Application Data
109	2.357337	172.16.11.170	23.223.244.139	TLSv1.2	3683	Application Data
110	2.357357	172.16.11.170	23.223.244.139	TLSv1.2	85	Application Data
111	2.358836	23.223.244.139	172.16.11.170	TCP	60	443 → 64281 [ACK] Seq=372 Ack=5388 Win=1502 Len=0
112	2.359838	23.223.244.139	172.16.11.170	TCP	60	443 → 64281 [ACK] Seq=372 Ack=8997 Win=1502 Len=0
113	2.361109	23.223.244.139	172.16.11.170	TCP	60	443 → 64281 [ACK] Seq=372 Ack=8457 Win=1502 Len=0
114	2.362397	23.223.244.139	172.16.11.170	TCP	60	443 → 64281 [ACK] Seq=372 Ack=8917 Win=1502 Len=0
115	2.362893	23.223.244.139	172.16.11.170	TCP	60	443 → 64281 [ACK] Seq=372 Ack=19546 Win=1502 Len=0
116	2.362893	23.223.244.139	172.16.11.170	TCP	60	443 → 64281 [ACK] Seq=372 Ack=19577 Win=1502 Len=0
117	2.519936	23.223.244.139	172.16.11.170	TLSv1.2	394	Application Data
118	2.519936	23.223.244.139	172.16.11.170	TLSv1.2	85	Application Data
119	2.520028	172.16.11.170	23.223.244.139	TCP	54	64281 → 443 [ACK] Seq=19577 Ack=743 Win=1822 Len=0

Frame 198: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on Interface \Device\NPF_{70CD1869-18FE-4C3D-8396-8224AC873C7},
> Ethernet II, Src: Sophos_cf8e45 (7c:5a:1c:f8:e4:5), Dst: HP_39:1e:d9 (7c:57:58:39:1e:d9)
> Internet Protocol Version 4, Src: 23.223.244.139, Dst: 172.16.11.170
> Transmission Control Protocol, Src Port: 443, Dst Port: 64281, Seq: 372, Len: 0


Packets: 300 - Displayed: 22 (7.1%)

YARRA JAISURYA
231901063
CSE CS
Flow Graph output



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

Procedure

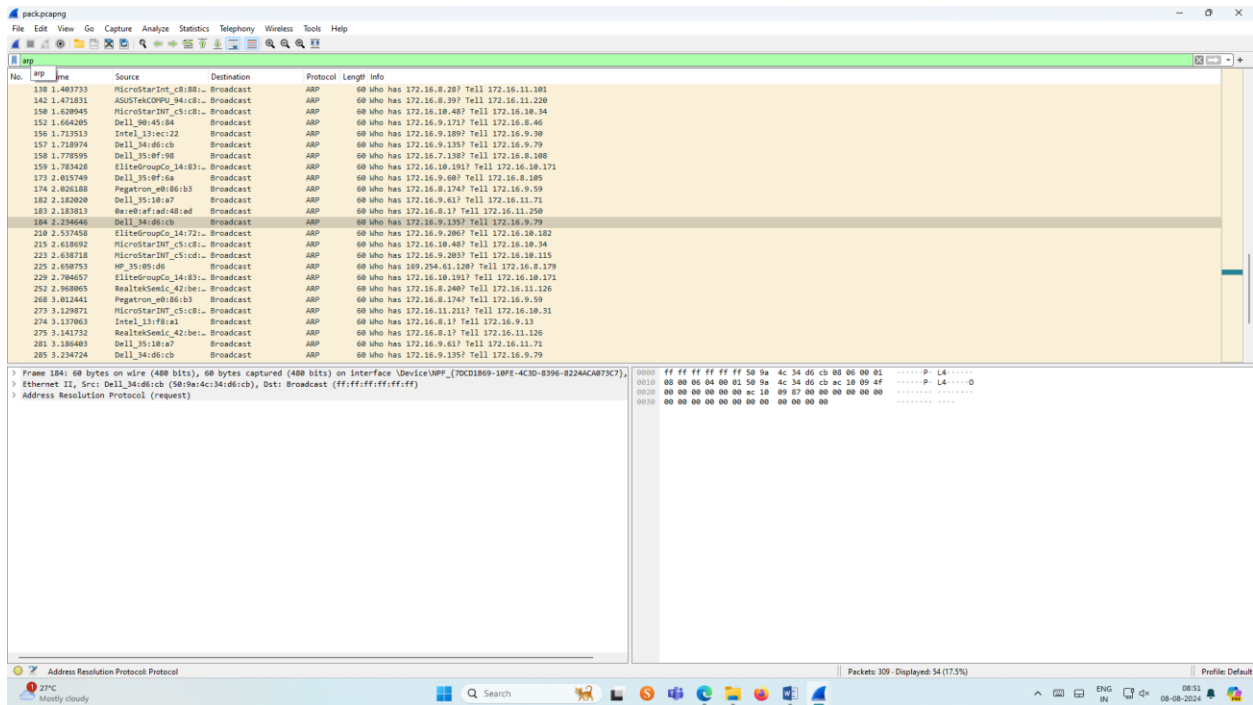
- Select Local Area Connection in Wireshark.
- Go to capture  option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search ARP packets in search bar.
- Save the packets.

YARRA JAISURYA

231901063



CSE CS

Output



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

Procedure

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

YARRA JAISURYA
231901063
CSE CS

Output

Wireshark packet capture showing DNS traffic. The packet list displays three packets:

No.	Time	Source	Destination	Protocol	Length	Info
385	4.824056	172.16.11.170	172.16.8.1	DNS	79	Standard query 8bc945 A fp-vp.azureedge.net
387	4.830791	172.16.8.1	172.16.11.170	DNS	146	Standard query response 8bc945 A fp-vp.azureedge.net CNAME fp-vp.ec.azureedge.net CNAME cs9.xpc.vbcdn.net A 117.18.232.200
388	4.830791	172.16.8.1	172.16.11.170	DNS	146	Standard query response 8bc945 A fp-vp.azureedge.net CNAME fp-vp.ec.azureedge.net CNAME cs9.xpc.vbcdn.net A 117.18.232.200

The packet details pane shows the structure of the first packet (Frame 373):

- Ethernet II, Src: HP_39:1e:d9 (7c:57:58:39:1e:d9), Dst: Sophos_cf-bei: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)

The packet bytes pane shows the raw data in hexadecimal and ASCII:

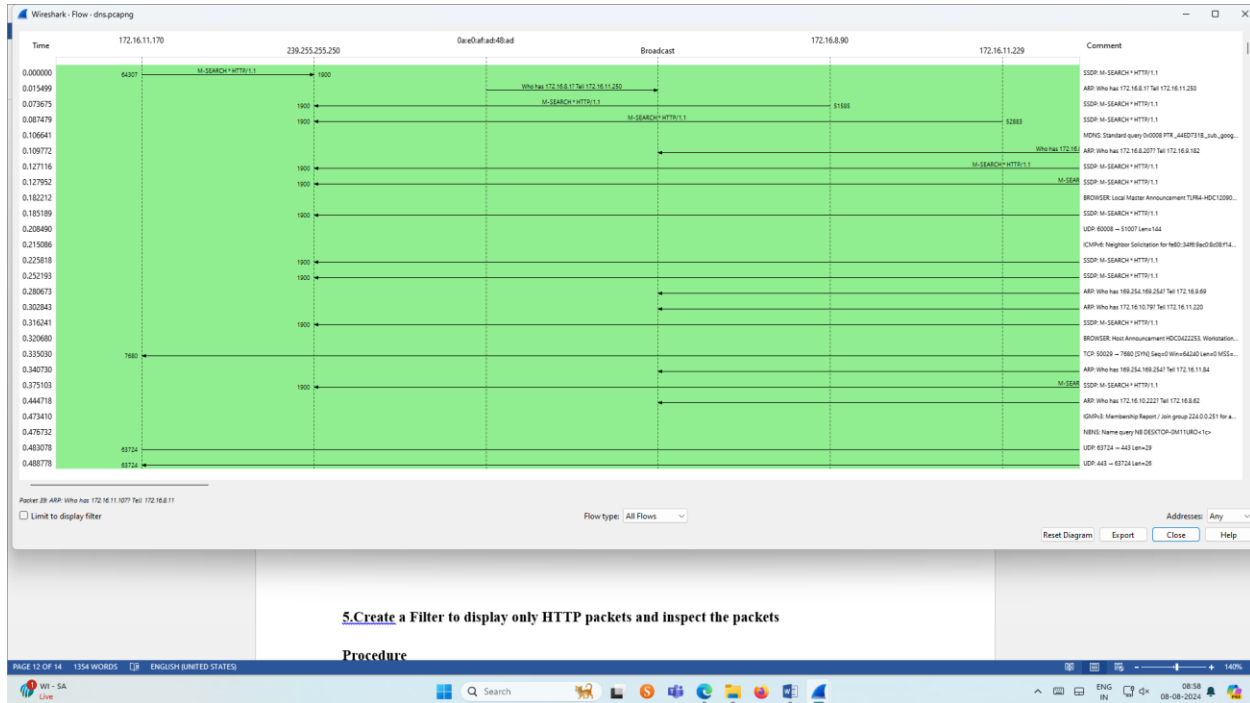
```
0000  7c 5a 1c cf be 45 7c 57 58 39 1e d9 00 00 45 00  [2...E]u X0...E-
0010  00 41 6d 38 00 00 00 11 00 00 ac 10 00 aa ac 10  And .....
0020  08 01 cb 14 00 35 00 2d 6c 0a c9 45 01 00 00 01  ....S- 1-E...
0030  00 00 00 00 00 00 05 66 70 2d 76 70 09 61 7a 75  ....f p-vp.azu
0040  72 65 65 64 67 65 63 64 65 74 00 00 01 00 01  reedge-n et....
```

Graph output

YARRA JAISURYA

231901063

CSE CS



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

Procedure

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

Output

YARRA JAISURYA

231901063

CSE CS

The image shows a Wireshark network traffic capture. The top pane displays a list of captured packets. The second pane shows the details of the selected packet (No. 1238), which is an HTTP GET request. The third pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.11.170	23.215.215.114	HTTP	208	GET /connecttest.txt HTTP/1.1
2	0.000000	172.16.11.170	23.215.215.114	HTTP	208	GET /connecttest.txt HTTP/1.1
3	0.000000	23.215.215.114	172.16.11.170	HTTP	381	HTTP/1.1 200 OK (text/plain)
4	0.000000	23.215.215.114	172.16.11.170	HTTP	381	HTTP/1.1 200 OK (text/plain)

Frame 1238: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interface \Device\NPF_{70CD1869-18FE-4C3D-B396-8224ACA07} (7c9a1c1cfbe45)

Ethernet II, Src: HP_39:1e:1d:9 (7c9a1c1cfbe45), Dst: Sophos_cf1be45 (7c9a1c1cfbe45)

Internet Protocol Version 4, Src: 172.16.11.170, Dst: 23.215.215.114

Transmission Control Protocol, Src Port: 64327, Dst Port: 80, Seq: 1, Ack: 1, Len: 154

Hypertext Transfer Protocol

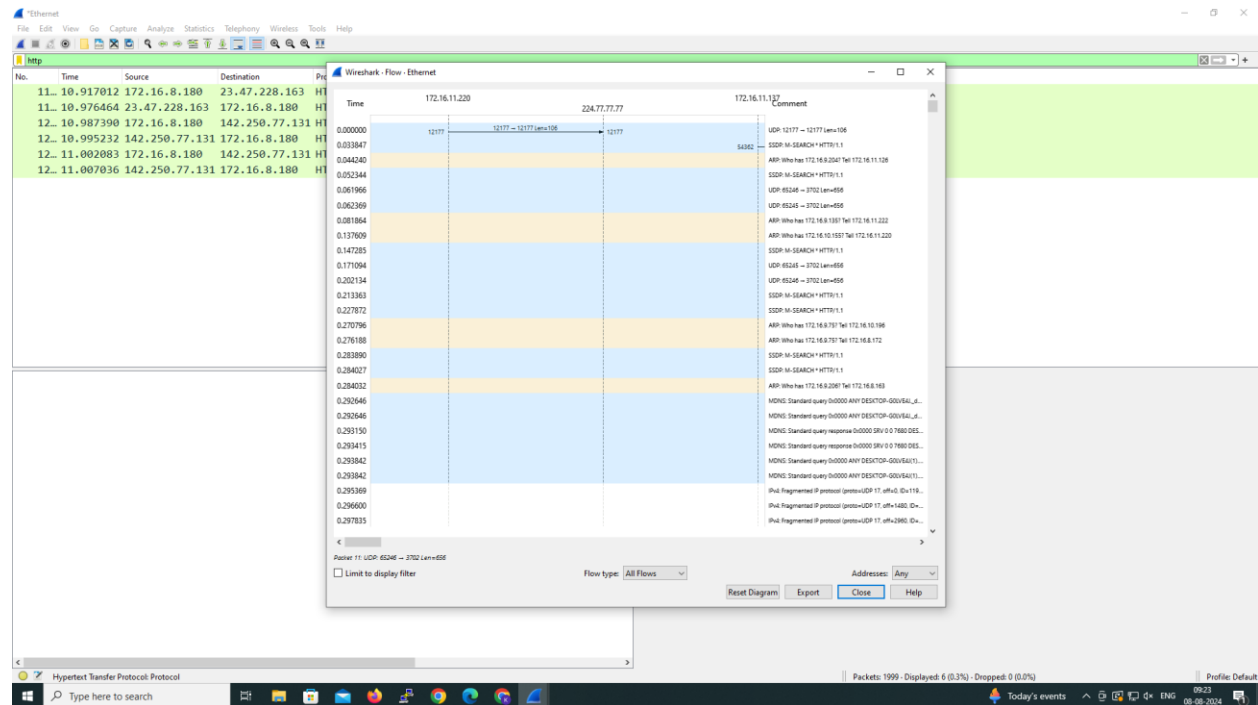
0000 7c 5a 1c cf be 45 7c 57 58 39 1e d9 00 00 45 00 [Z...E]w Xp...E
0010 00 c2 24 25 40 00 00 06 00 00 ac 10 00 aa 17 d7 . \$N\$
0020 d7 72 fb 51 00 50 db 49 a5 20 2f 63 6f 6e 6e 65 --r Q P I --C |P.
0030 01 00 a7 b8 00 00 47 45 54 20 2f 63 6f 6e 6e 65GE T /conne
0040 63 74 74 65 73 74 2e 74 78 74 20 40 54 54 50 2f ccttest.txt HTTP/
0050 31 2e 31 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 72 1.1 .Cac he-Contr
0060 6f 6c 3a 20 6e 6f 2d 63 61 63 68 65 00 0a 43 6f ol: no-c ache-Co
0070 6e 6e 65 63 74 69 6f 6e 3a 20 43 6c 6f 73 65 6d nnection : Close
0080 0a 50 72 61 67 6d 61 3a 20 6e 6f 2d 63 61 63 68 .Pragma: no-cach
0090 65 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d e-User- Agent: H
00a0 69 63 72 6f 73 6f 66 74 20 6e 43 53 40 0d 0a 40 Scrouff. NCSS: H
00b0 6f 73 74 3a 20 77 77 77 2e 6d 73 66 74 63 6f 6e ost: www.msftcon
00c0 6e 65 63 74 74 65 73 74 2e 63 6f 6d 0d 0a 0d 0a necttest.com....

Flow Graph output

YARRA JAISURYA


231901063

CSE CS



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

Procedure

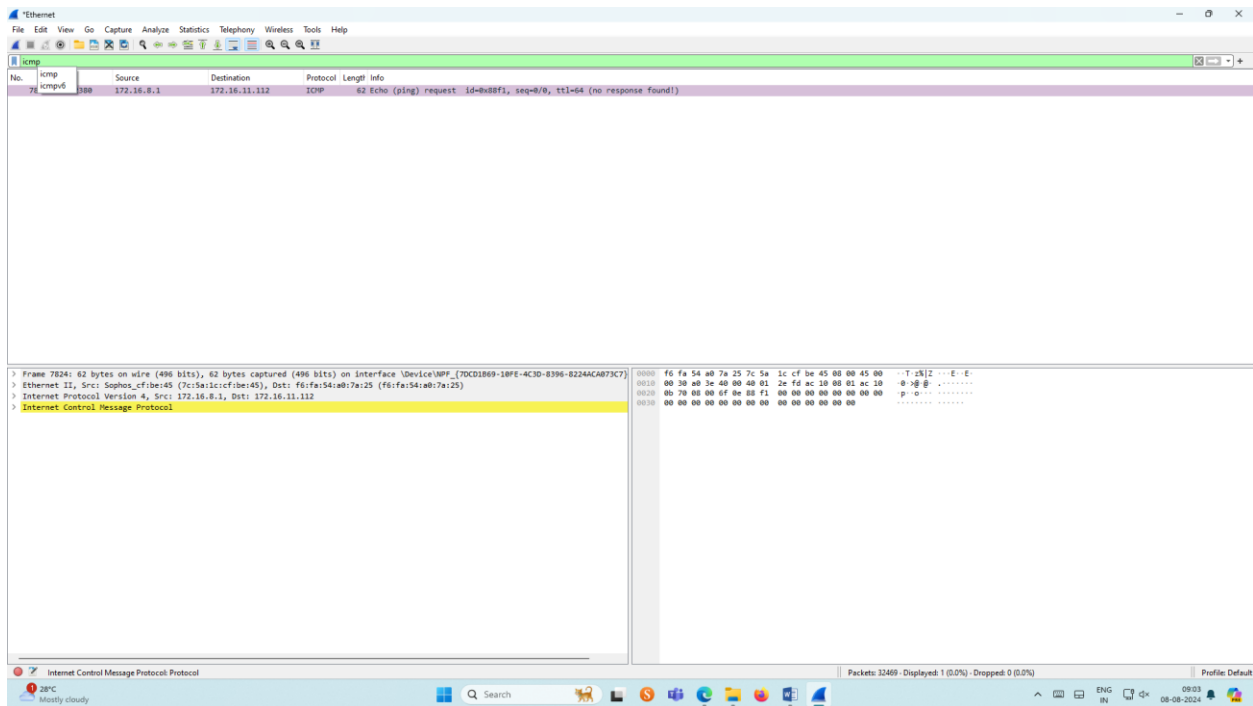
- Select Local Area Connection in Wireshark.
- Go to capture  option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search ICMP/IP packets in search bar.
- Save the packets

Output

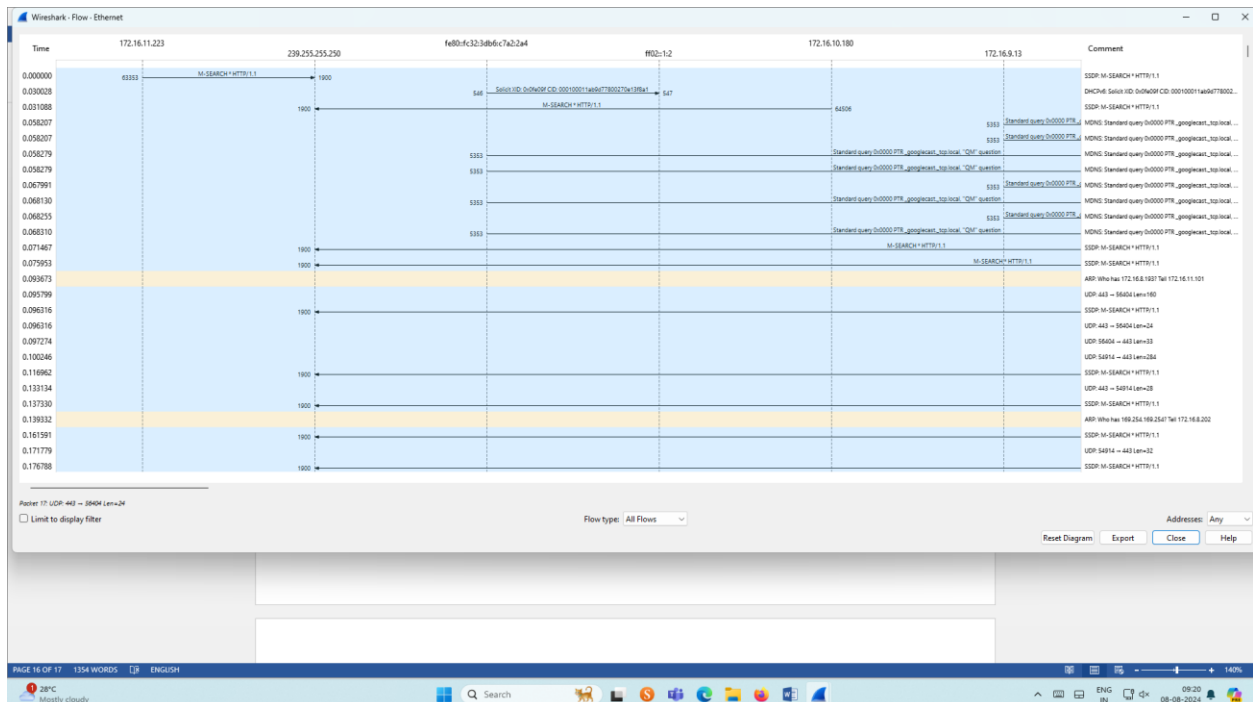
YARRA JAISURYA

231901063

CSE CS



Flow Graph output




YARRA JAISURYA

231901063

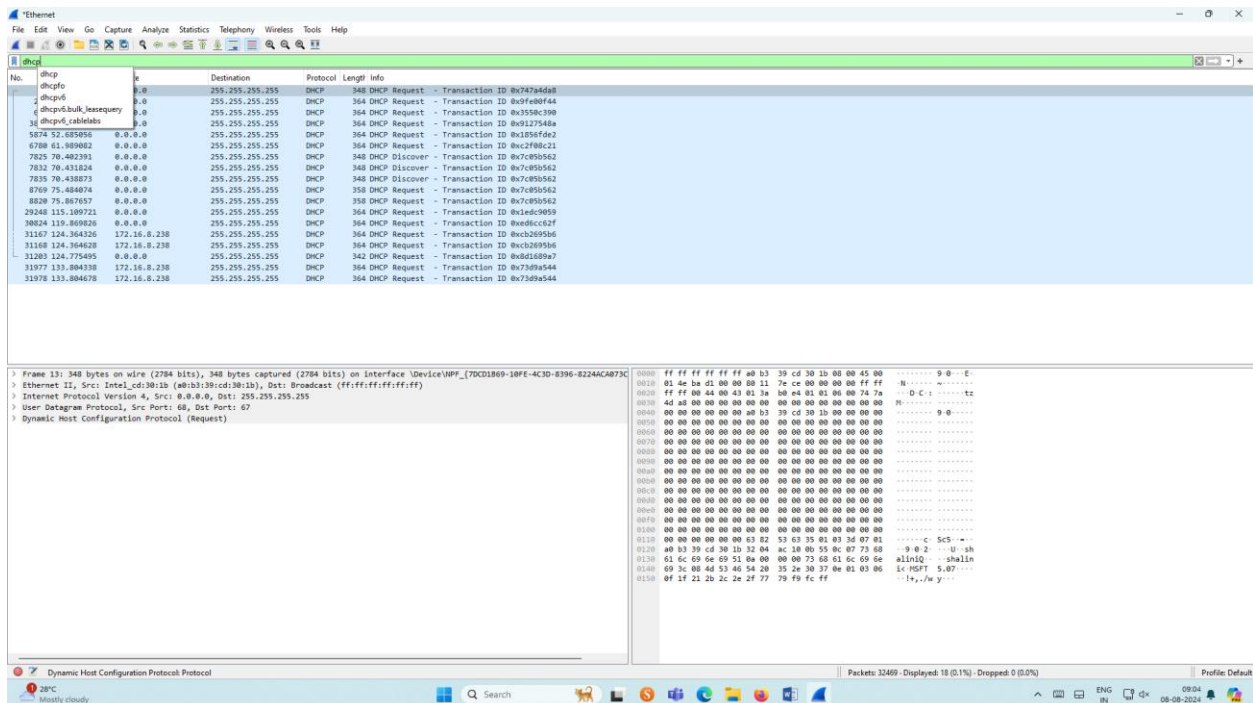
CSE CS

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 filter 'dhcp' applied. The packet details pane on the right shows the structure of the selected packet (Frame 13), which is a DHCP Request. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x7474d4d8
2	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x9fe80f44
3	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x9550c390
4	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x9127548a
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 0xc2f86c21
7	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
8	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
9	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
10	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
11	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
12	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
13	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
14	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
15	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
16	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
17	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
18	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
19	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
20	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
21	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
22	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
23	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
24	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
25	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
26	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
27	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
28	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
29	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
30	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
31	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
32	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
33	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
34	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
35	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
36	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
37	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
38	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
39	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
40	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
41	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
42	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
43	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
44	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
45	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
46	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
47	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
48	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
49	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
50	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
51	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
52	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
53	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
54	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
55	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
56	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
57	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
58	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
59	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
60	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
61	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
62	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
63	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
64	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
65	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
66	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
67	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
68	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
69	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
70	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
71	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
72	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
73	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
74	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
75	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
76	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
77	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
78	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
79	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
80	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
81	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
82	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
83	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
84	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
85	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
86	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
87	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
88	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
89	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
90	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
91	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
92	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
93	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
94	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
95	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
96	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
97	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
98	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
99	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662
100	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Discover - Transaction ID 0x7c805662

Frame 13: 348 bytes on wire (2784 bits), 348 bytes captured (2784 bits) on interface \Device\NPF_{70CD1869-18FE-4C3D-8396-8224ACAB3C} on 0.0.0.0
Ethernet II, Src: Intel_i350 (80:00:00:00:00:00), 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 ff ff 39 cd 30 10 00 00 45 009.0.E
0010 02 4e 1a c0 00 00 11 7c ce 00 00 00 ff ff
0020 ff ff 00 44 00 43 01 3a b0 e4 01 01 00 74 7aD.E.z
0030 4d a8 00 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 a0 31 39 cd 10 10 00 00 00
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 52 63 55 01 01 36 07 01C.ScS
0120 a0 b3 39 cd 30 10 32 04 ac 18 05 55 0c 07 73 689.0.2...h
0130 61 5c 69 6a 69 51 6a 00 00 73 65 c1 6c 69 6aaLinIQ...h
0140 69 3c 08 4d 53 46 54 20 35 2e 30 37 0e 01 03 06h.RSPT.5.07
0150 0f 1f 21 20 2c 2e 2f 77 79 f9 fc ffs...w.y

YARRA JAISURYA

231901063

CSE CS