

SUDHARSAN S

231901054

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.

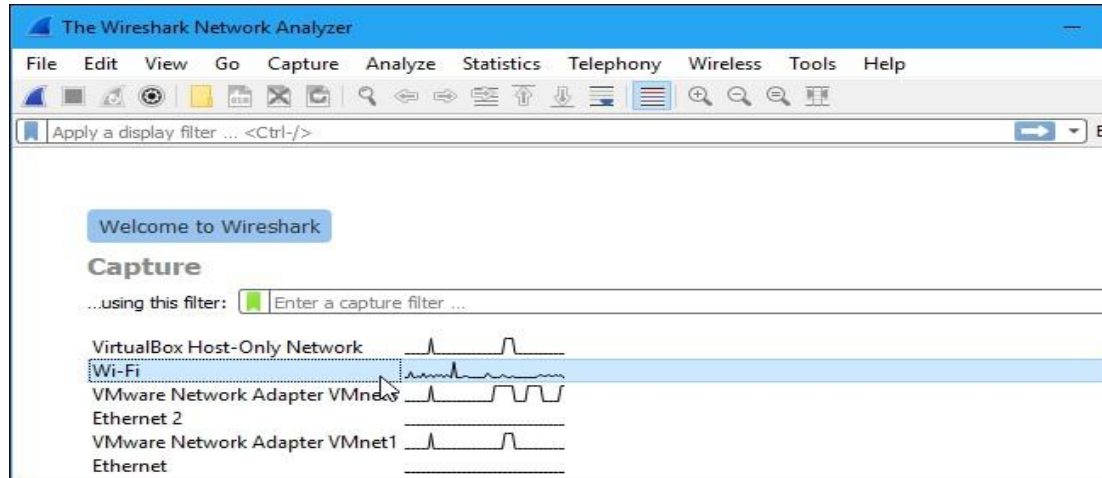
Capturing Packets

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

SUDHARSAN S

231901054

CSE CS



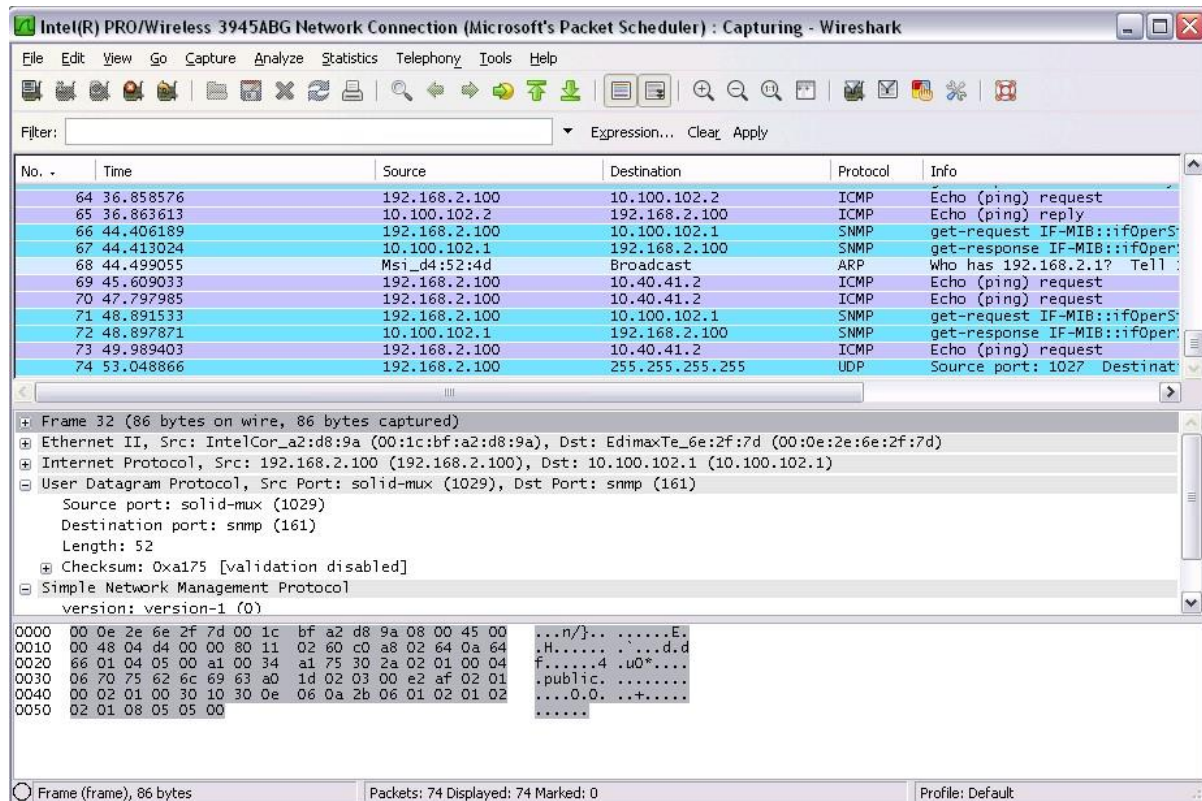
As soon as you click the interface's name, you'll see the packets start to appear in real time. Wireshark captures each packet sent to or from your system.

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.

SUDHARSAN S

231901054

CSE CS



Packet
List

Packet
Details

Packet Bytes

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

SUDHARSAN S

231901054

CSE CS

The “Packet List” Pane

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

The “Packet Details” Pane

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

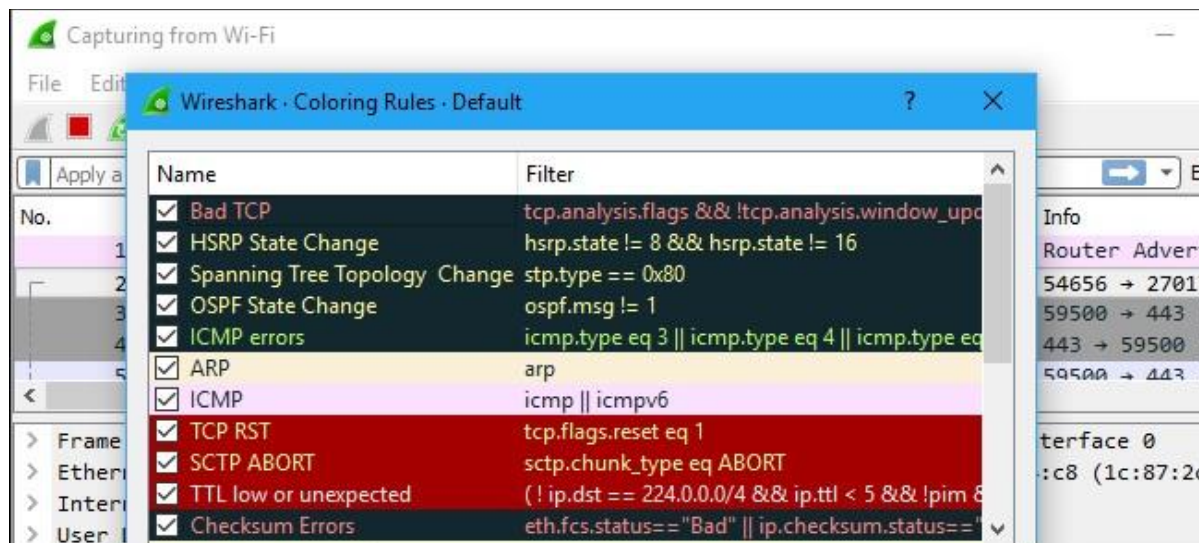
The “Packet Bytes” Pane

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

Color Coding

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

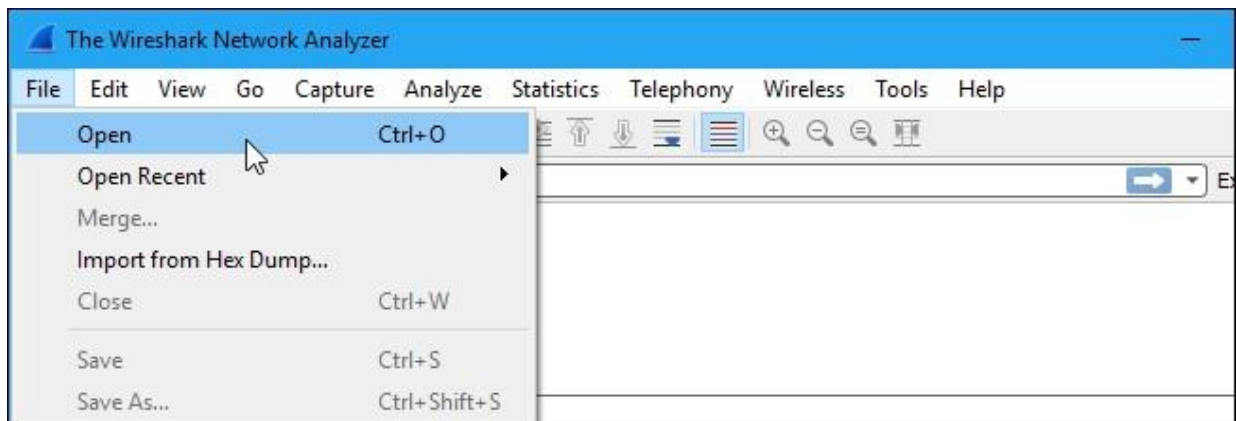
To view exactly what the color codes mean, click View > Coloring Rules. You can also customize and modify the coloring rules from here, if you like.



Sample Captures

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

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

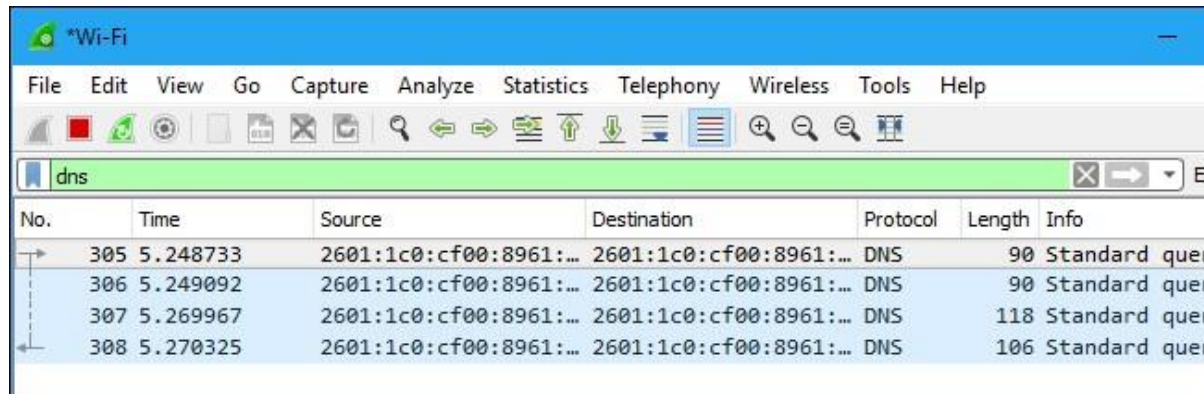


Filtering Packets

If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark's filters come in.

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

SUDHARSAN S
231901054
CSE CS

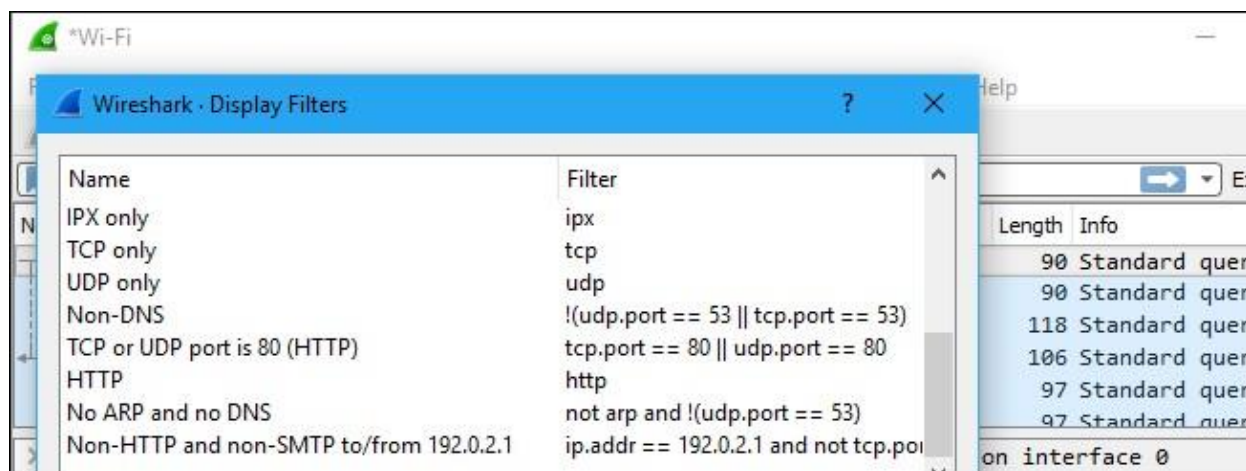


The image shows the Wireshark interface with a packet capture window titled '*Wi-Fi'. The packet list pane shows four DNS packets (No. 305, 306, 307, 308) with their respective times, source and destination IP addresses, and protocols. The packet details pane shows the selected packet's details, including the protocol and length.

No.	Time	Source	Destination	Protocol	Length	Info
305	5.248733	2601:1c0:cf00:8961:...	2601:1c0:cf00:8961:...	DNS	90	Standard quer
306	5.249092	2601:1c0:cf00:8961:...	2601:1c0:cf00:8961:...	DNS	90	Standard quer
307	5.269967	2601:1c0:cf00:8961:...	2601:1c0:cf00:8961:...	DNS	118	Standard quer
308	5.270325	2601:1c0:cf00:8961:...	2601:1c0:cf00:8961:...	DNS	106	Standard quer

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.



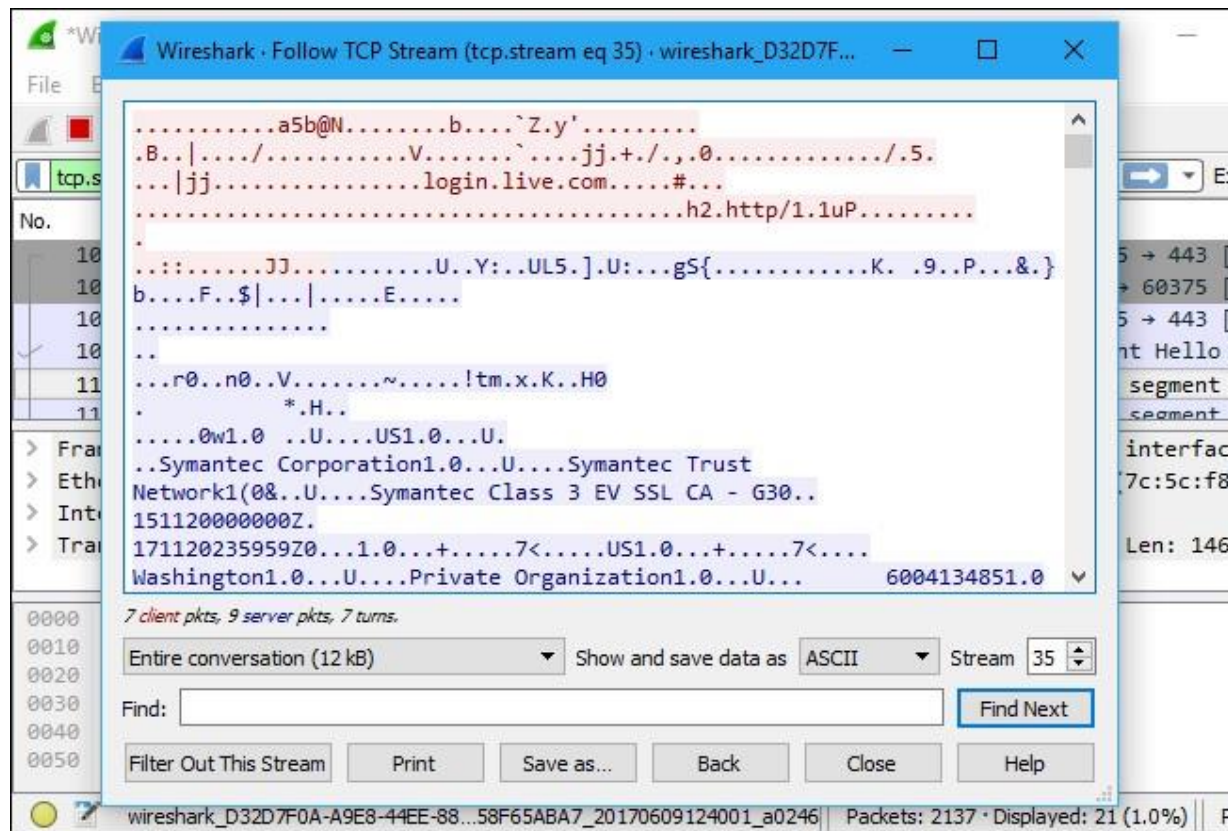
The image shows the 'Wireshark · Display Filters' dialog box. It contains a list of filters with their names and corresponding filter expressions. The filters are: IPX only (ipx), TCP only (tcp), UDP only (udp), Non-DNS (!(udp.port == 53 || tcp.port == 53)), TCP or UDP port is 80 (HTTP) (tcp.port == 80 || udp.port == 80), HTTP (http), No ARP and no DNS (not arp and !(udp.port == 53)), and Non-HTTP and non-SMTP to/from 192.0.2.1 (ip.addr == 192.0.2.1 and not tcp.por).

Name	Filter
IPX only	ipx
TCP only	tcp
UDP only	udp
Non-DNS	!(udp.port == 53 tcp.port == 53)
TCP or UDP port is 80 (HTTP)	tcp.port == 80 udp.port == 80
HTTP	http
No ARP and no DNS	not arp and !(udp.port == 53)
Non-HTTP and non-SMTP to/from 192.0.2.1	ip.addr == 192.0.2.1 and not tcp.por

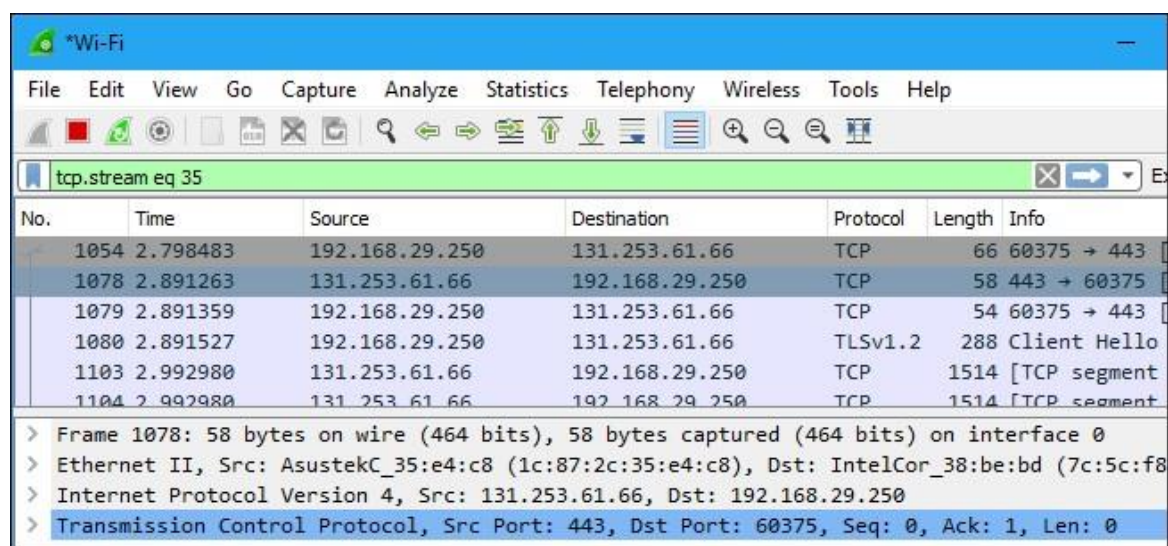
Another interesting thing you can do is right-click a packet and select Follow > TCP Stream.

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.

SUDHARSAN S
231901054
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.

SUDHARSAN S
231901054
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. A filter bar at the top shows the filter 'tcp.stream eq 35'. The packet list pane displays several packets, with packet 1054 selected. The packet details pane shows the structure of frame 1054, including the interface ID, encapsulation type (Ethernet), arrival time, and epoch time. The packet bytes pane shows the raw data 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

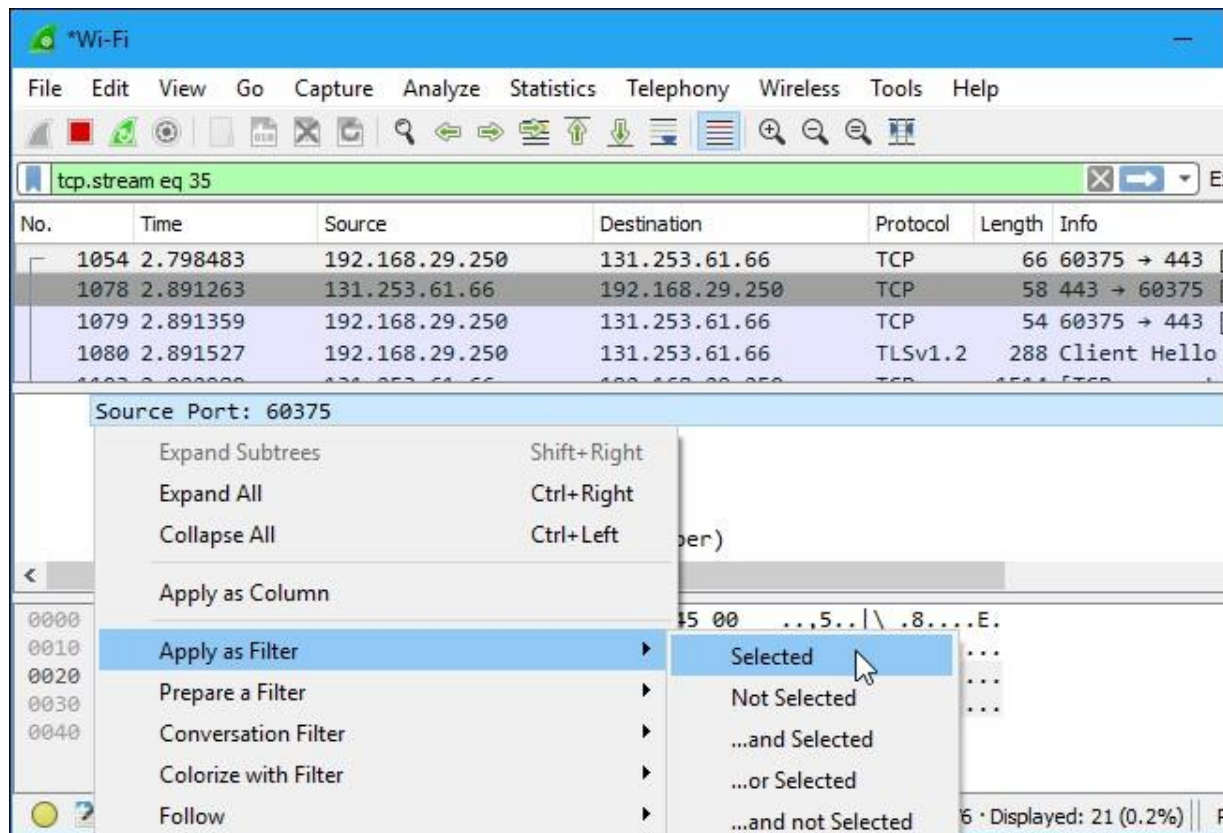
▼ Frame 1054: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Interface id: 0 (\Device\NPF_{D32D7F0A-A9E8-44EE-88DC-DFD58F65ABA7})
Encapsulation type: Ethernet (1)
Arrival Time: Jun 9, 2017 12:40:04.140141000 Pacific Daylight Time
[Time shift for this packet: 0.000000000 seconds]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

SUDHARSAN S
231901054
CSE CS



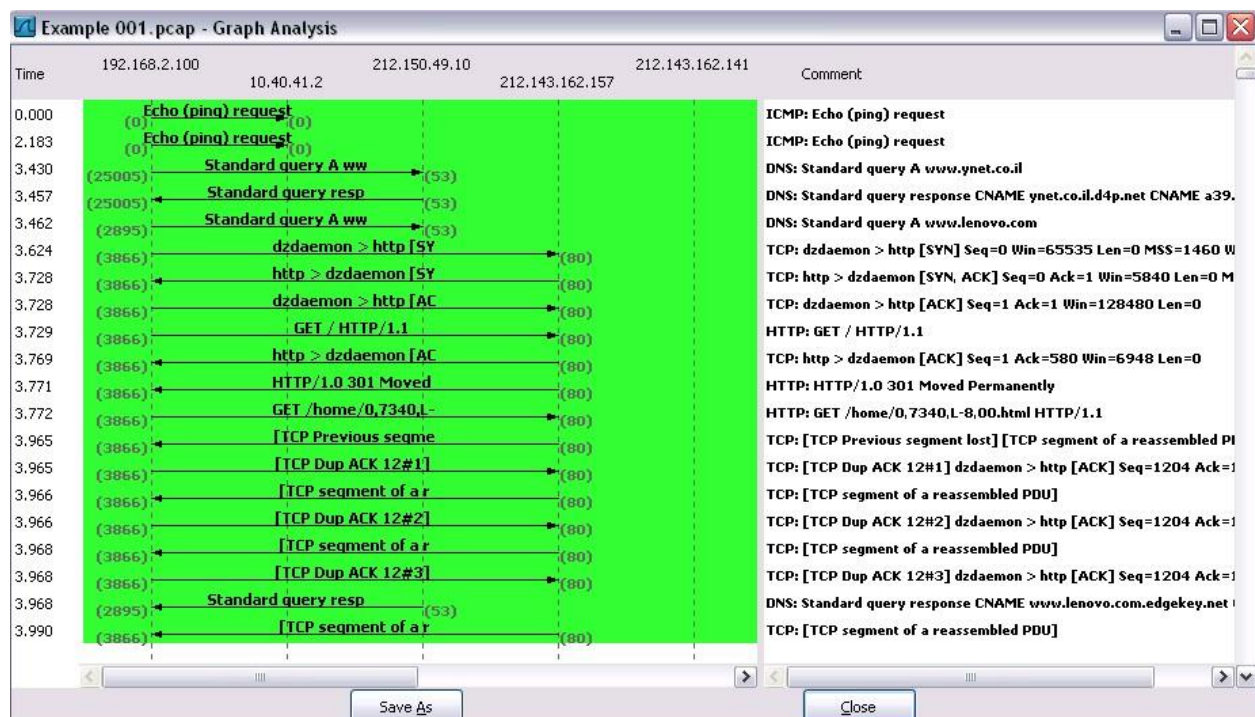
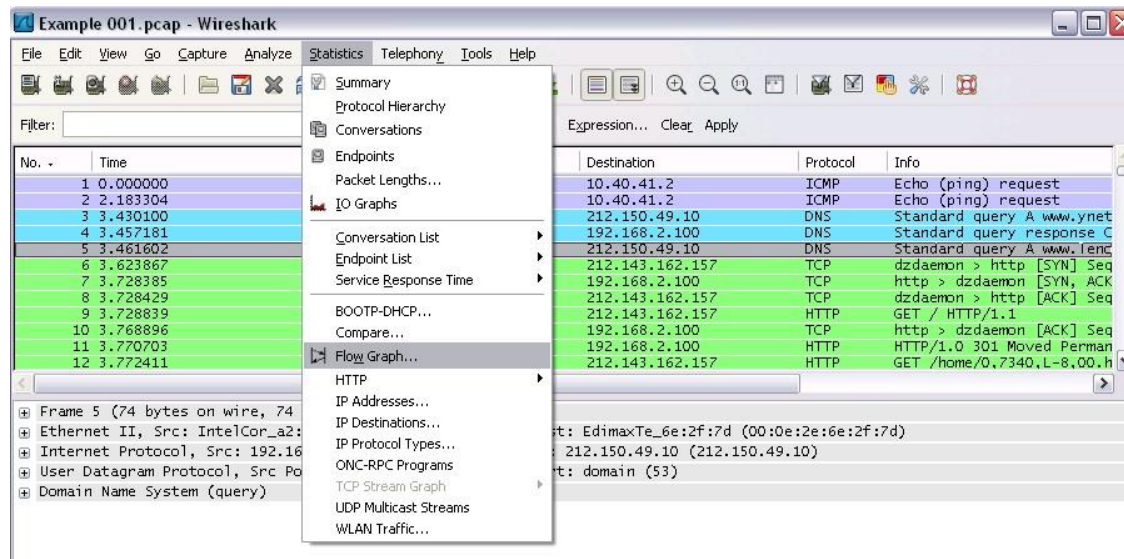
Wireshark is an extremely powerful tool, and this tutorial is just scratching the surface of what you can do with it. Professionals use it to debug network protocol implementations, examine security problems and inspect network protocol internals.

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

SUDHARSAN S

231901054

CSE CS



SUDHARSAN S

231901054

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

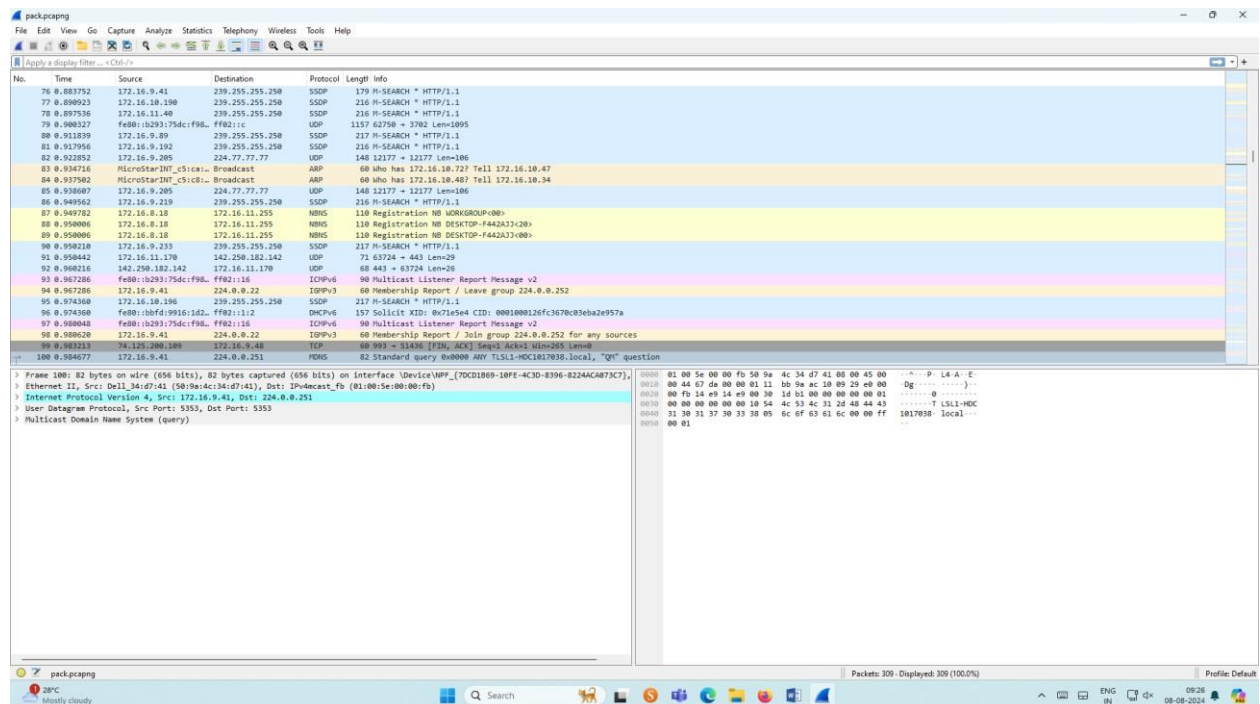
Exercises

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





SUDHARSAN S

231901054

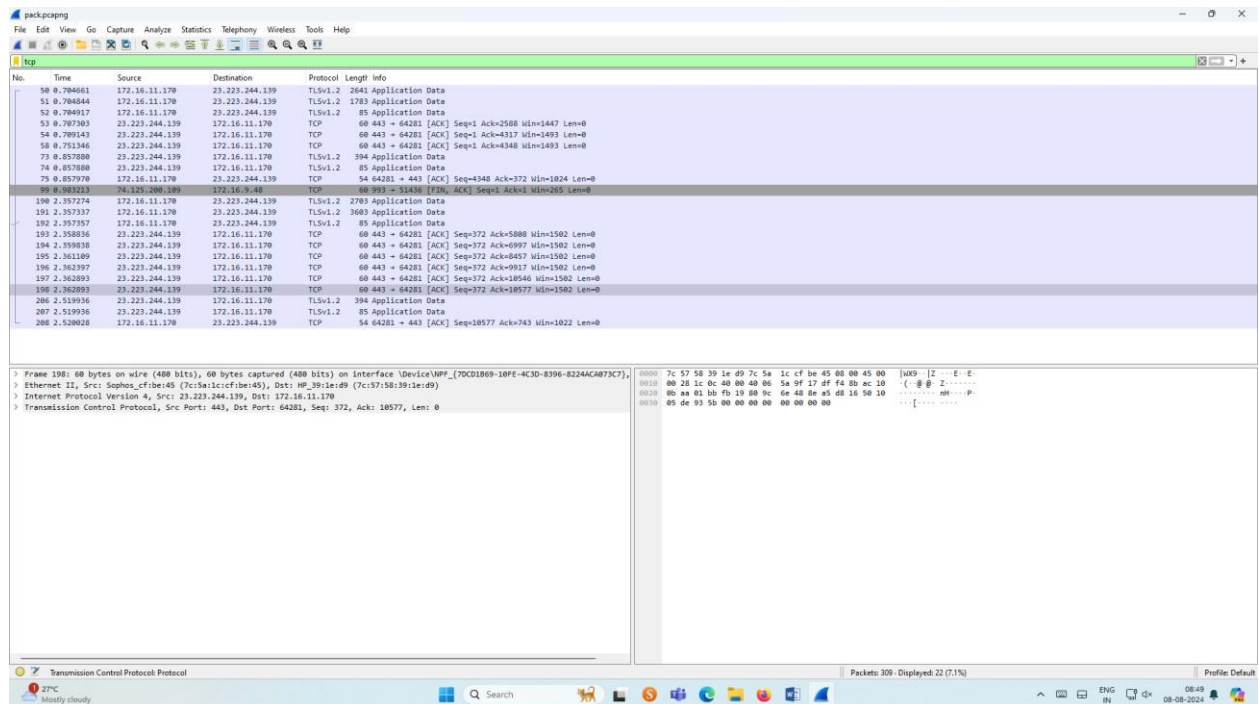
CSE CS

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:

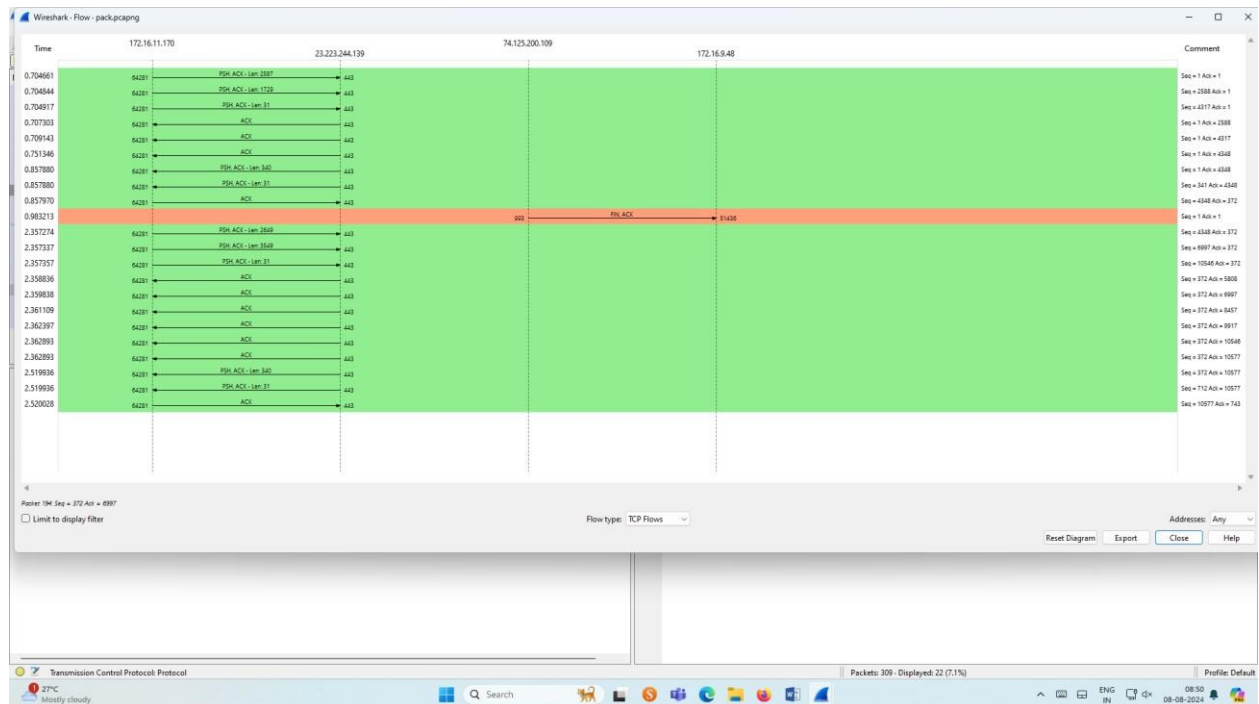


SUDHARSAN S

231901054


CSE CS

Flow Graph output



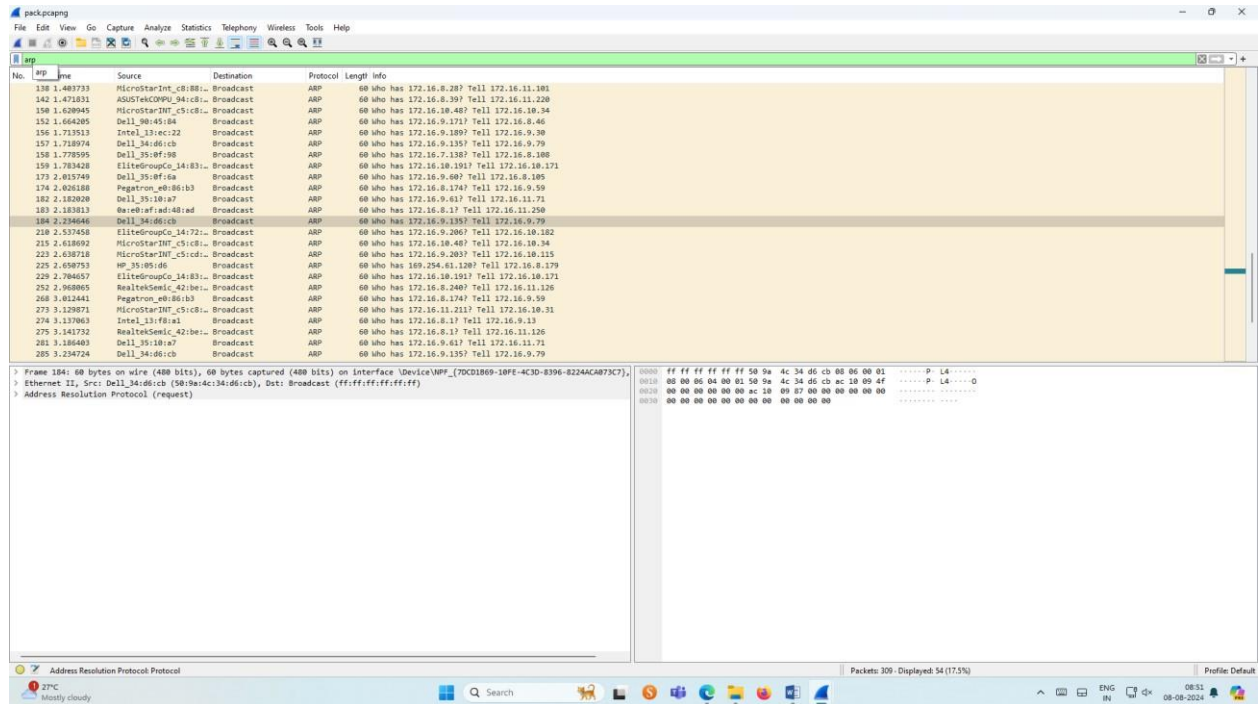
3.Create a Filter to display only ARP packets and inspect the packets.

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.



SUDHARSAN S
231901054
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 StatisticsFlow graph.

SUDHARSAN S

231901054

CSE CS

➤ Save the packets.

Output

The image shows a Wireshark packet capture window titled 'dns.pcapng'. The main pane displays a list of four captured packets, all of which are DNS messages. The first two are standard queries, and the next two are standard query responses. The packet details pane on the left shows the hierarchical structure of the selected packet (No. 377), including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query). The packet bytes pane on the right shows the raw data in hexadecimal and ASCII format.

No.	Time	Source	Destination	Protocol	Length	Info
375	4.824856	172.16.11.170	172.16.8.1	DNS	79	Standard query 8xc945 A fp-vp.azureedge.net
377	4.838791	172.16.8.1	172.16.11.170	DNS	146	Standard query response 8xc945 A fp-vp.azureedge.net CNAME fp-vp.ec.azureedge.net CNAME cs9-wpc.vcdn.net A 117.18.232.200
378	4.838791	172.16.8.1	172.16.11.170	DNS	146	Standard query response 8xc945 A fp-vp.azureedge.net CNAME fp-vp.ec.azureedge.net CNAME cs9-wpc.vcdn.net A 117.18.232.200

Frame 377: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface \Device\NPF_{70CD1869-10FE-4C3D-8396-822AAC873C7}, Ethernet II, Src: HP_39:1a:d9 (7c:57:18:39:1a:d9), Dst: Suphas_cfb6e45 (7c:5a:1c:cf:b6:e4:5), 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)

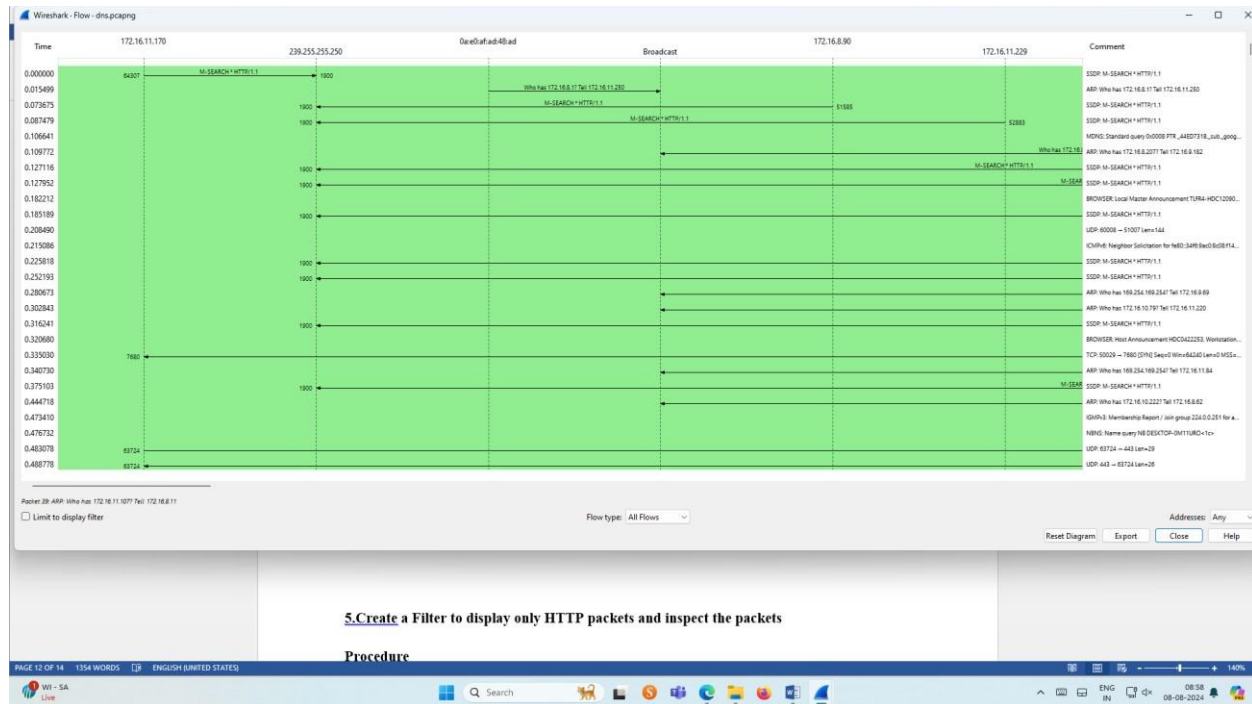
0000 7c 5a 1c cf b6 e4 57 58 39 1a d9 00 00 45 00 [2] Eja X9...E
0010 00 43 6d 38 00 00 00 11 00 00 0c 18 00 0a ac 10 And
0020 00 01 cb 14 00 35 00 2d 6c 0a e9 45 01 00 00 01S- 1-E....
0030 00 00 00 00 00 05 66 70 2d 70 70 09 61 7a 75f p-vp.azu
0040 72 15 65 64 67 65 63 64 65 74 00 00 01 00 01 reedge n et....

SUDHARSAN S

231901054


CSE CS

Graph output



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

Procedure

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

Output

SUDHARSAN S

231901054

CSE CS

Wireshark interface showing a packet capture of an HTTP GET request and response. The packet list on the left shows four packets, with the selected packet (No. 4) being an HTTP 200 OK response. The packet details pane on the right shows the structure of the HTTP response, including the status bar, headers (Content-Type: text/plain), and the body (connecttest.txt).

Packet List:

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	301	HTTP/1.1 200 OK (text/plain)
4	0.000000	23.215.215.114	172.16.11.170	HTTP	301	HTTP/1.1 200 OK (text/plain)

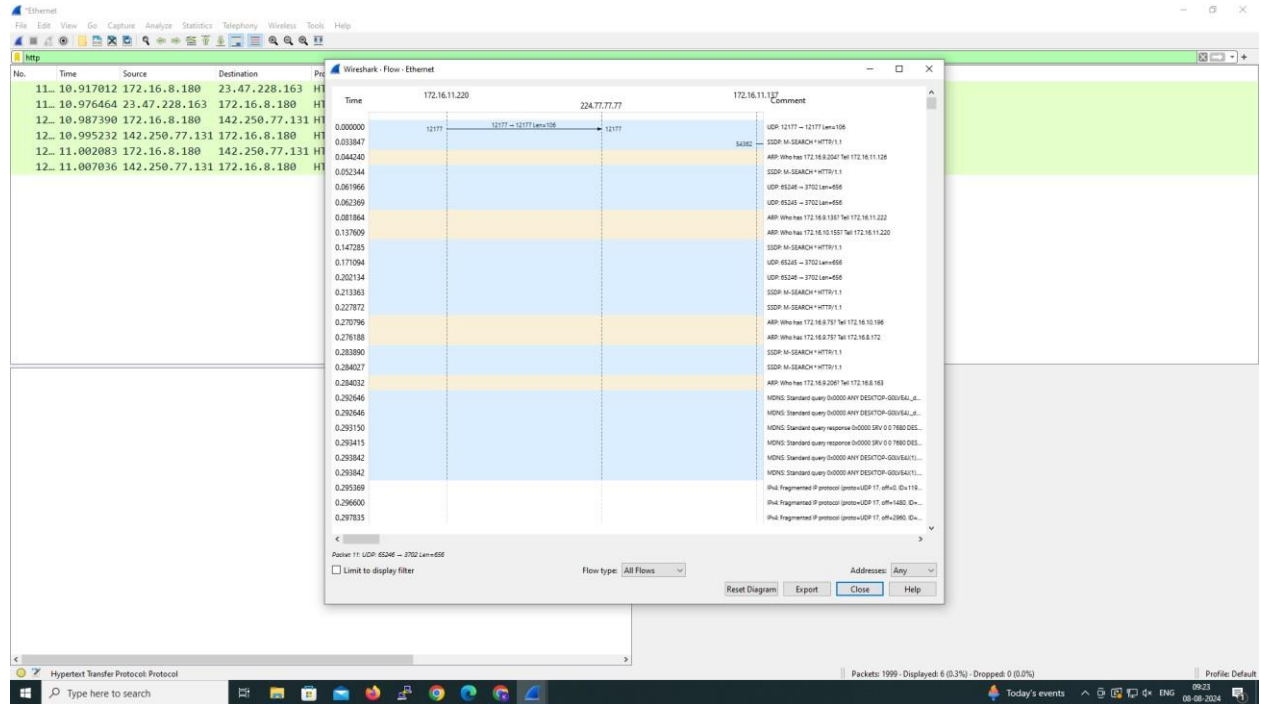
Packet Details (Selected Packet 4):

- Frame 1230: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interface \Device\NPF_{7DCD1B69-18FE-4C3D-8396-B224ACAB7}
- Ethernet II, Src: HP_39:1e:d9 (7c:57:58:39:1e:d9), Dst: Sophos_cf:be:45 (7c:5a:1c:cf:be:45)
- Internet Protocol Version 4, Src: 172.16.11.170, Dst: 23.215.215.114
- Transmission Control Protocol, Src Port: 64337, Dst Port: 80, Seq: 1, Ack: 1, Len: 154
- Hypertext Transfer Protocol

HTTP Response Structure:


```
0000 7c 5a 1c cf be 45 7c 57 58 39 1e d9 00 00 45 00 |Z...E|W X9...E-
0010 00 c2 24 25 40 00 00 00 00 00 ac 10 00 aa 17 07 |S&...
0020 47 72 f9 51 00 50 db 49 a5 c0 2a 43 a4 7c 50 18 |r Q P I ~c [p-
0030 01 00 a7 b0 00 00 47 45 54 20 2f 63 6f 6e 6e 65 |...GE T /conne
0040 63 74 74 65 73 74 2e 74 70 74 20 40 54 54 50 2f |cttest.t xt HTTP/
0050 31 2e 31 0d 0a 43 01 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 0d 0a 43 6f |oli: 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: M
00a0 69 63 72 6f 73 6f 66 74 20 4e 43 53 49 0d 0a 40 |icrosoft .NET: 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:~:~
```

SUDHARSAN S
231901054
CSE CS
Flow Graph output



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

Procedure

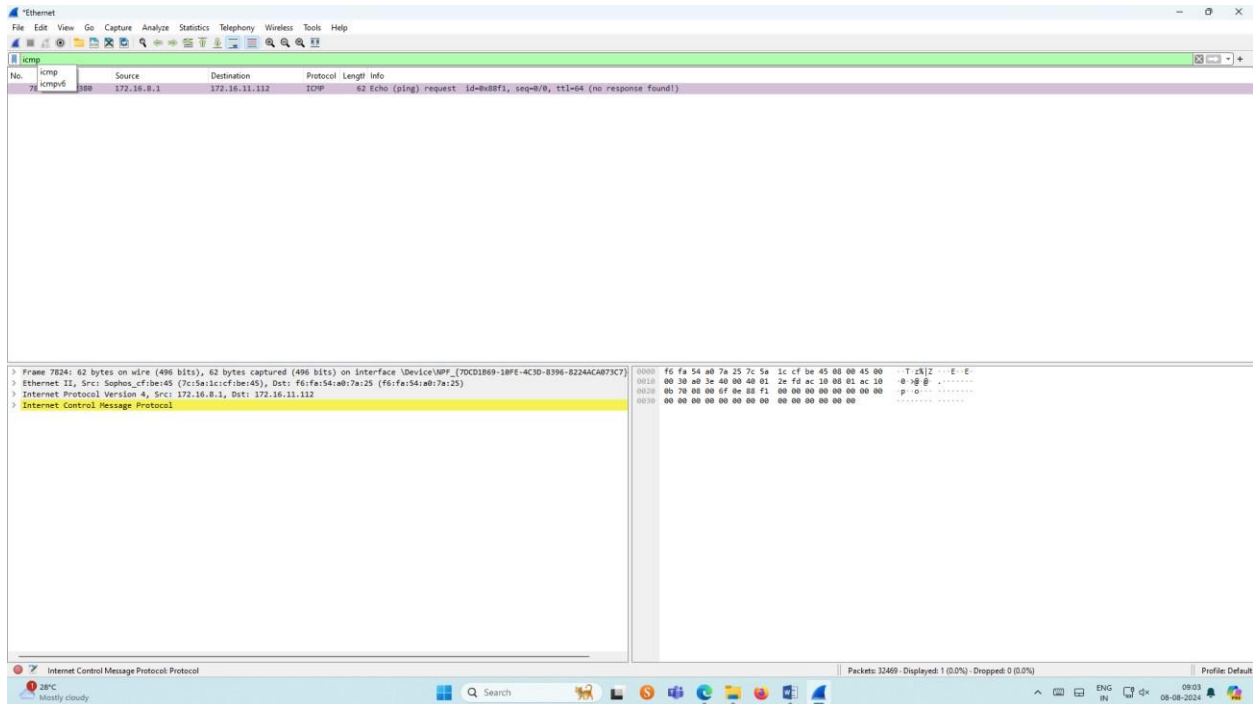
- Select Local Area Connection in Wireshark.
- Go to capture  option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search ICMP/IP packets in search bar.
- Save the packets

SUDHARSAN S

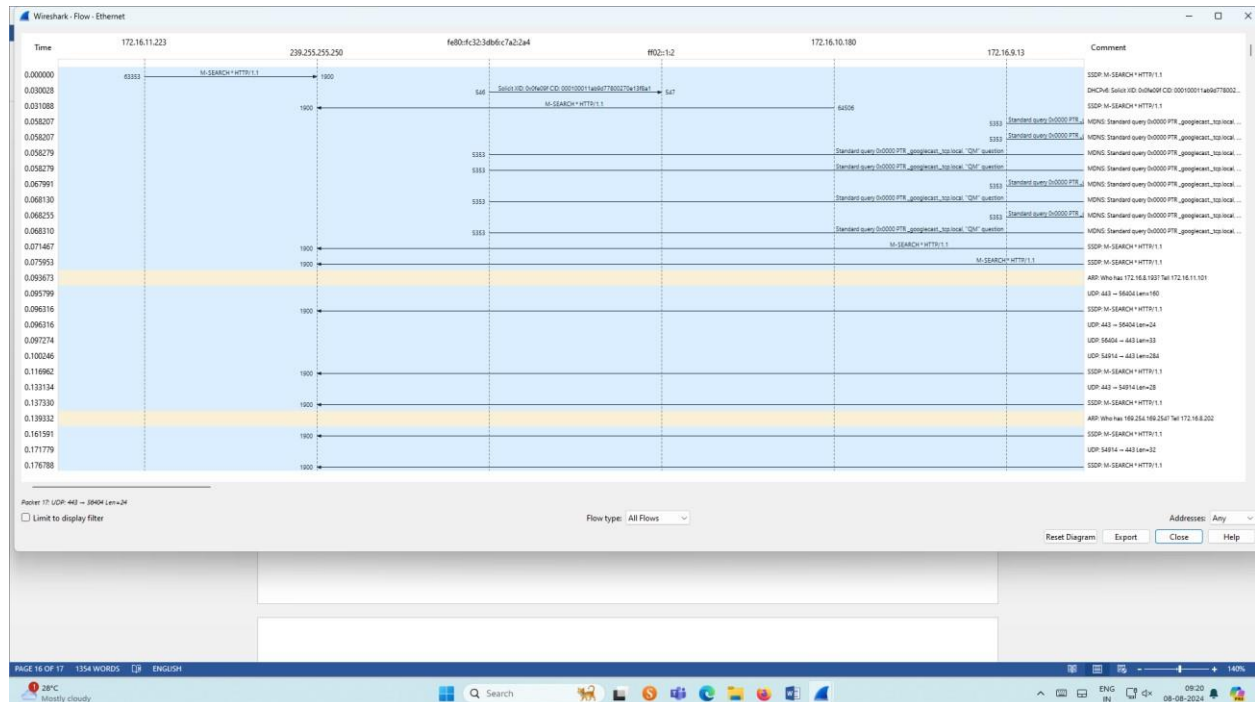
231901054

CSE CS

Output



Flow Graph output




SUDHARSAN S

231901054

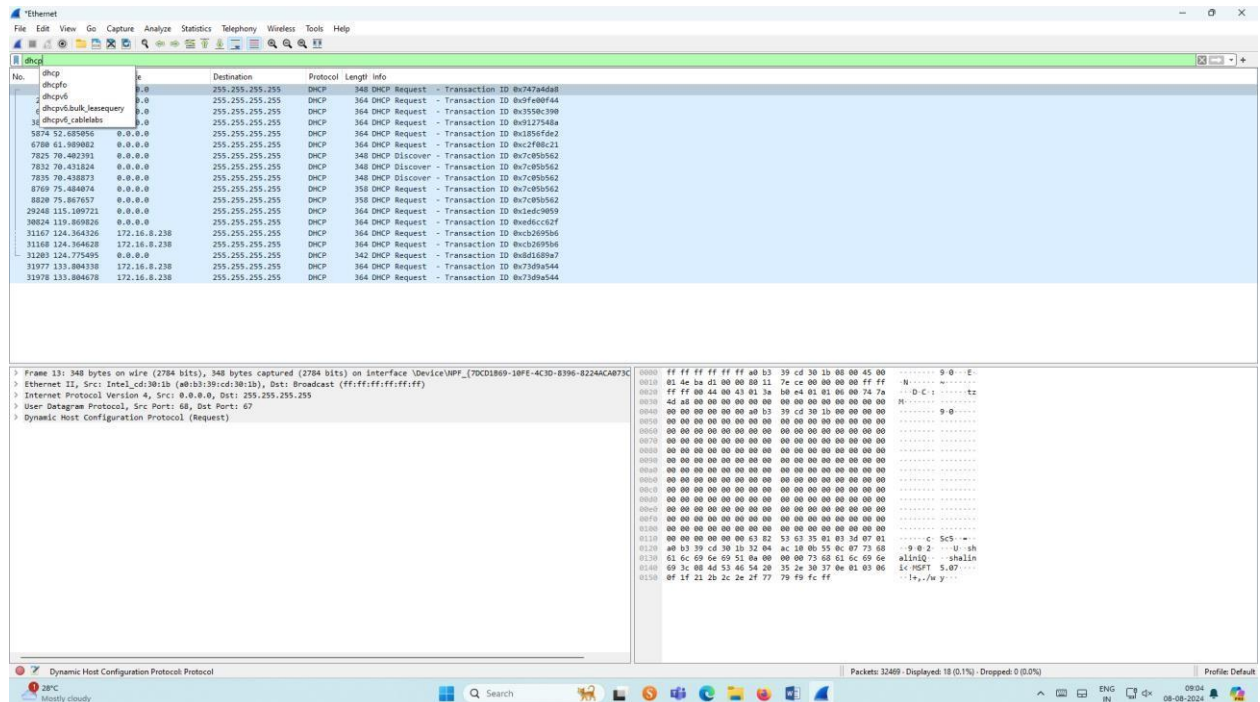
CSE CS

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 toolbar contains icons for opening files, saving, capturing, and analyzing. The main window is divided into three panes:

- Packet List Pane:** Shows a list of captured packets. A filter 'dhcp' is applied in the top right. The list includes packets 1 through 31, all of which are DHCP requests or discoveries. The selected packet is number 31, a DHCP Request from 172.16.8.238 to 255.255.255.255.
- Packet Details Pane:** Displays the structure of the selected packet (No. 31). It shows the Ethernet II header, Internet Protocol Version 4 header, and User Datagram Protocol header. The selected packet is a DHCP Request (Transaction ID: 0x73d89a54).
- Packet Bytes Pane:** Shows the raw data of the selected packet in hexadecimal and ASCII. The data starts with 'ff ff ff ff ff ff ff ff' and ends with '79 f5 fc ff'.

The status bar at the bottom indicates that 32489 packets were displayed (0.1%) and 0 packets were dropped (0.0%). The system tray shows the date and time as 08-08-2024, 08:04.

SUDHARSAN S
231901054
CSE CS