

M.VISHWANATH

231901062

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:

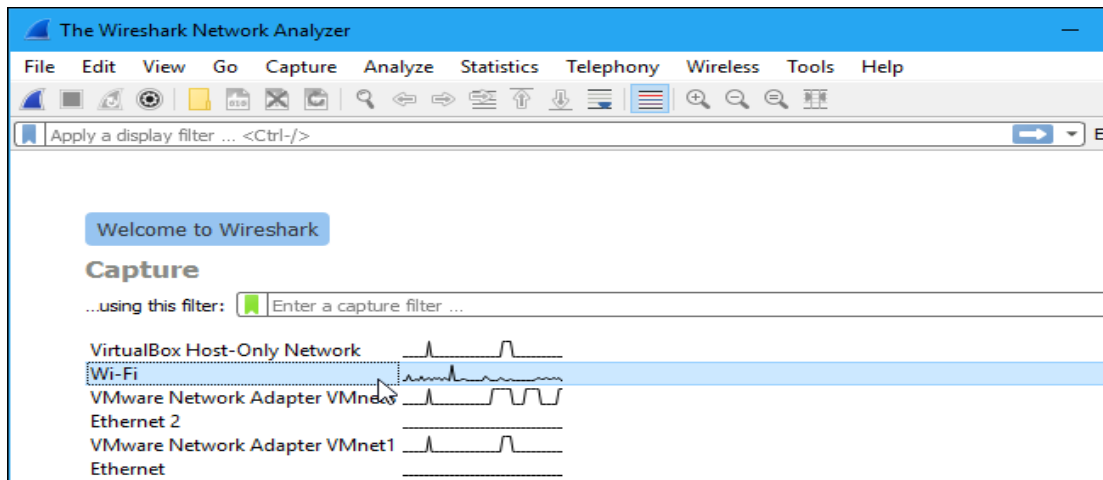
- Network administrators: troubleshoot network problems
- Network security engineers: examine security problems
- Developers: debug protocol implementations
- People: learn **network protocol internals**

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.

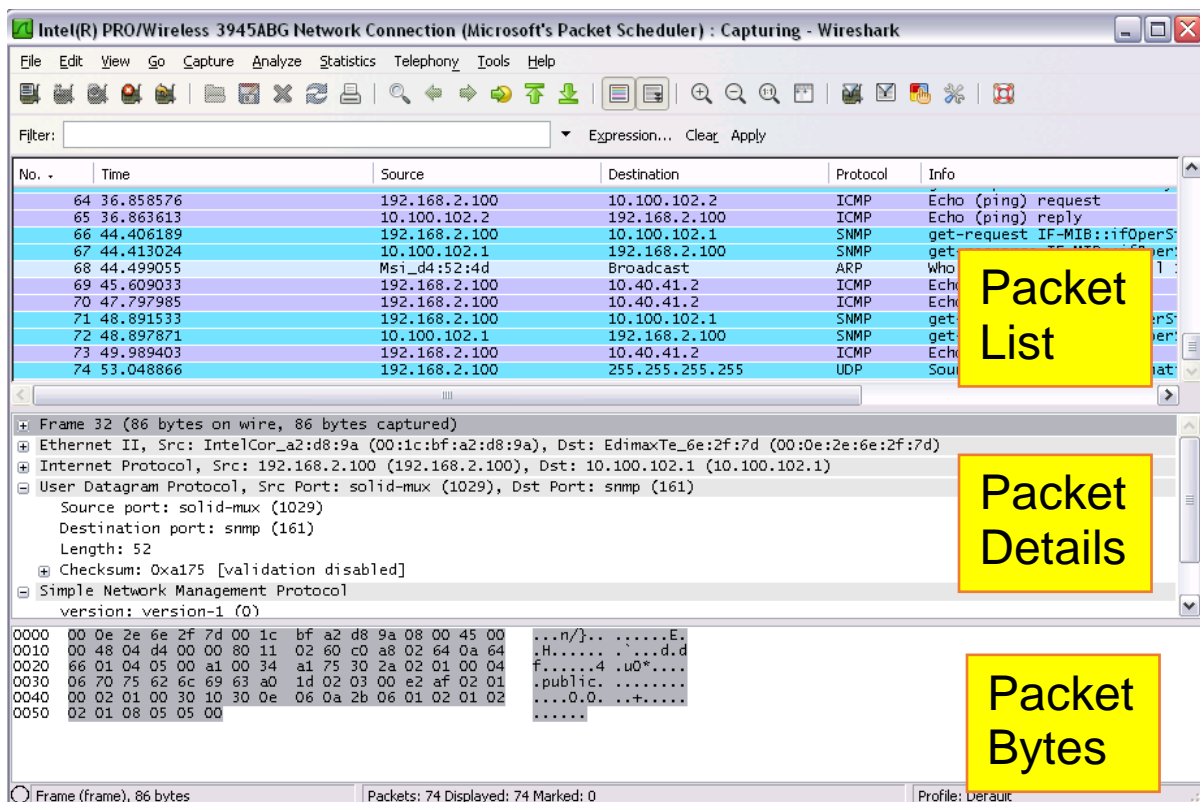
Capturing Packets

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” and “Packet Bytes” panes.

The “Packet Details” Pane

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

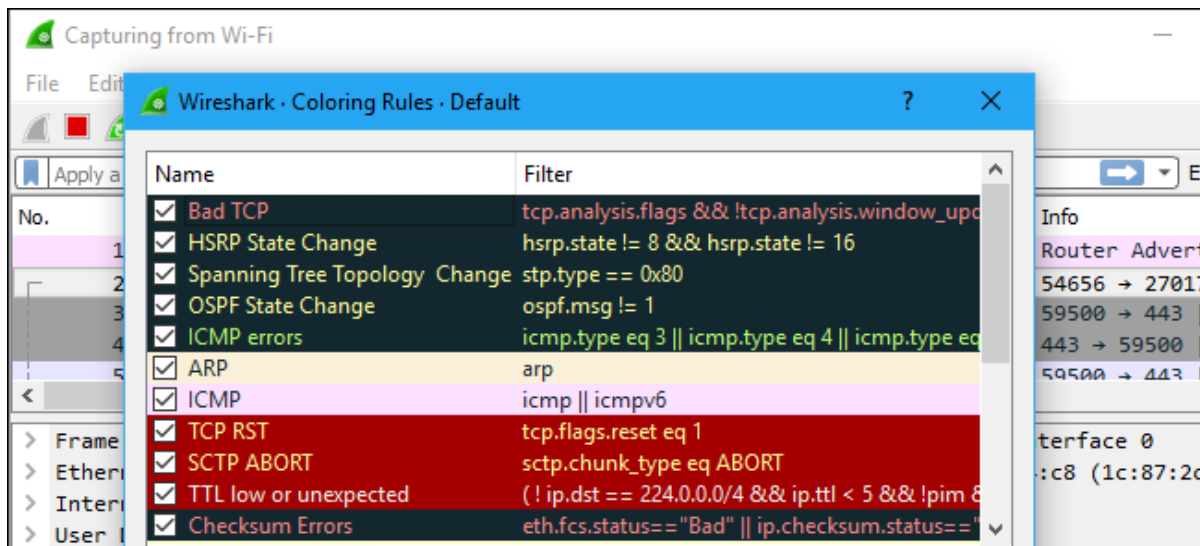
The “Packet Bytes” Pane

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

Color Coding

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

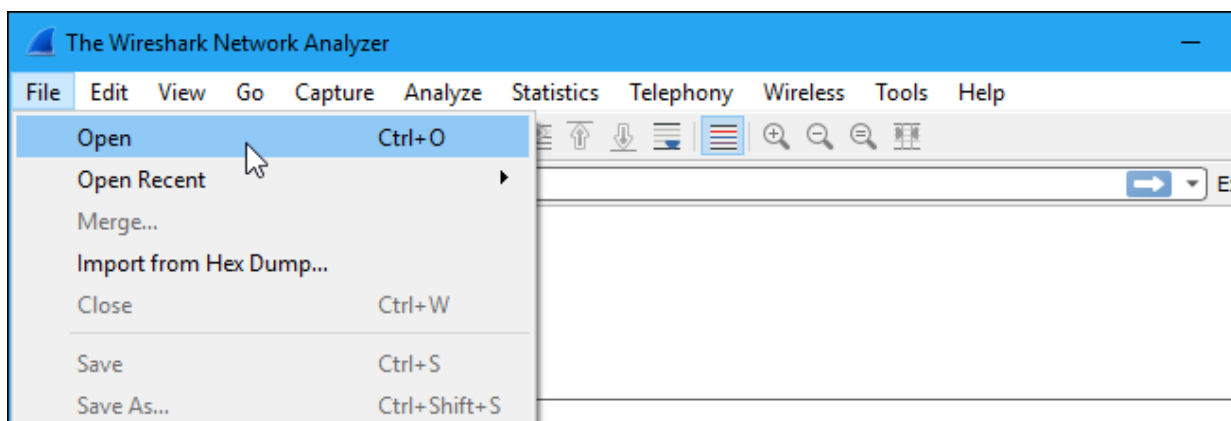
To view exactly what the color codes mean, click View > Coloring Rules. You can also customize and modify the coloring rules from here, if you like.



Sample Captures

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

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

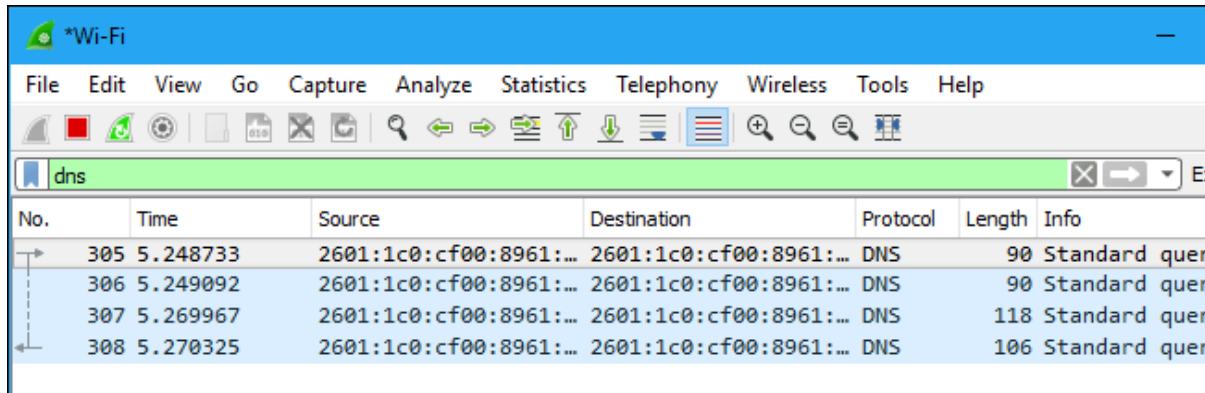


Filtering Packets

If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the

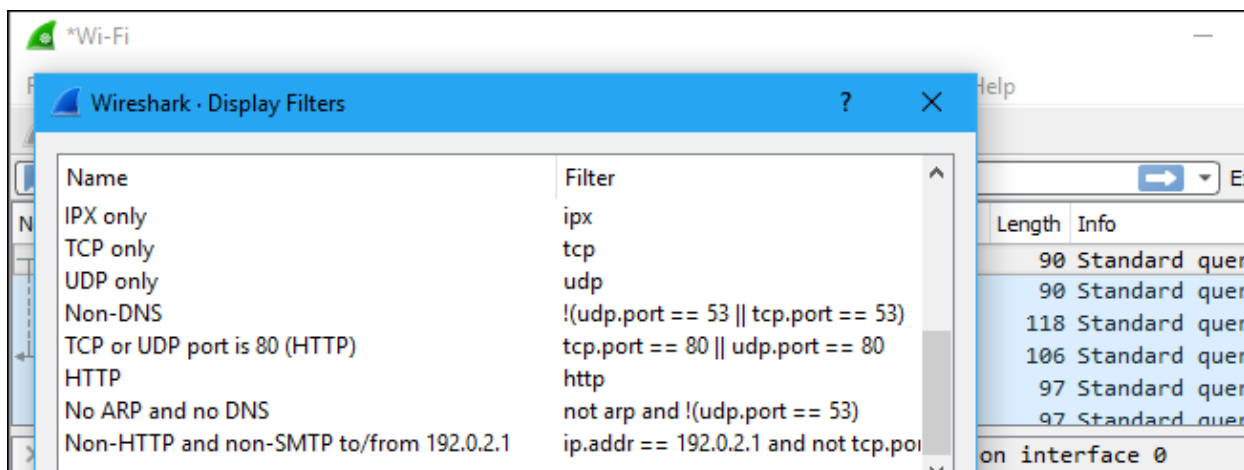
traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark's filters come in.

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



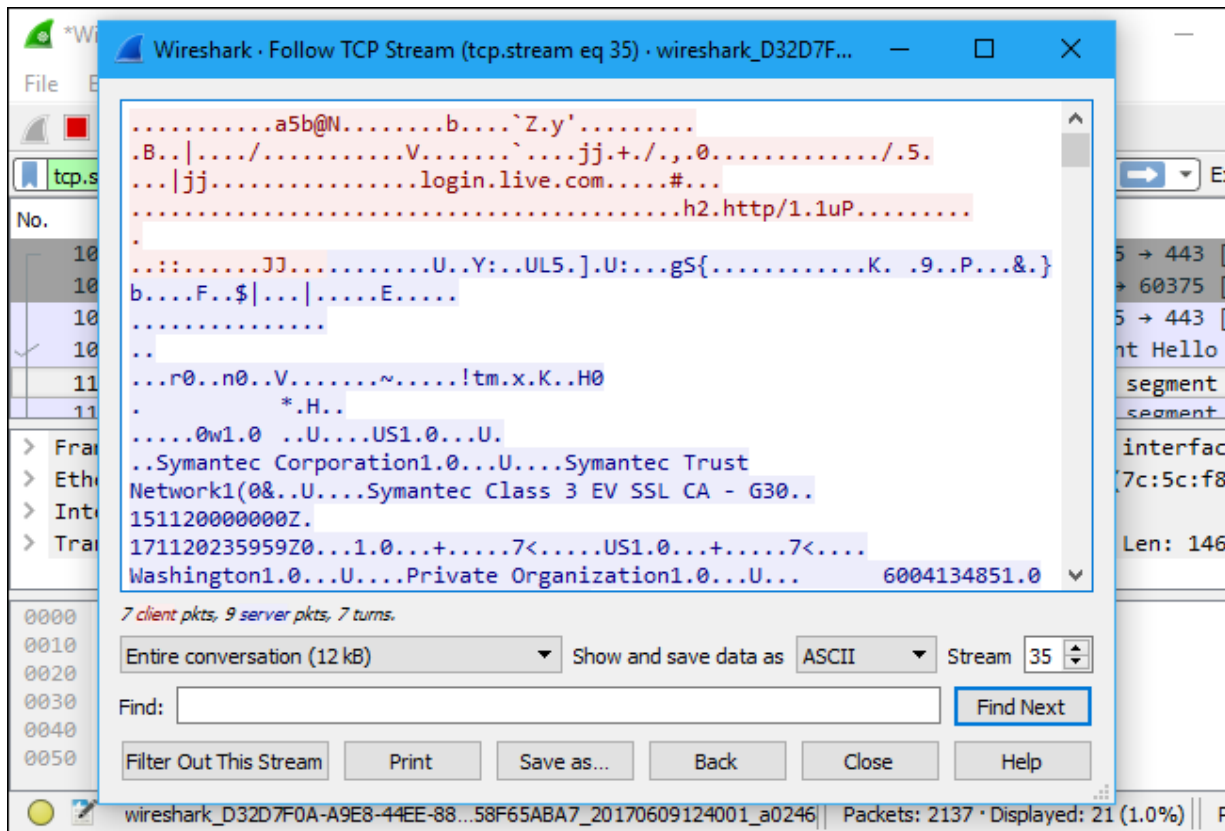
You can also click Analyze > Display Filters to choose a filter from among the default filters included in Wireshark. From here, you can add your own custom filters and save them to easily access them in the future.

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

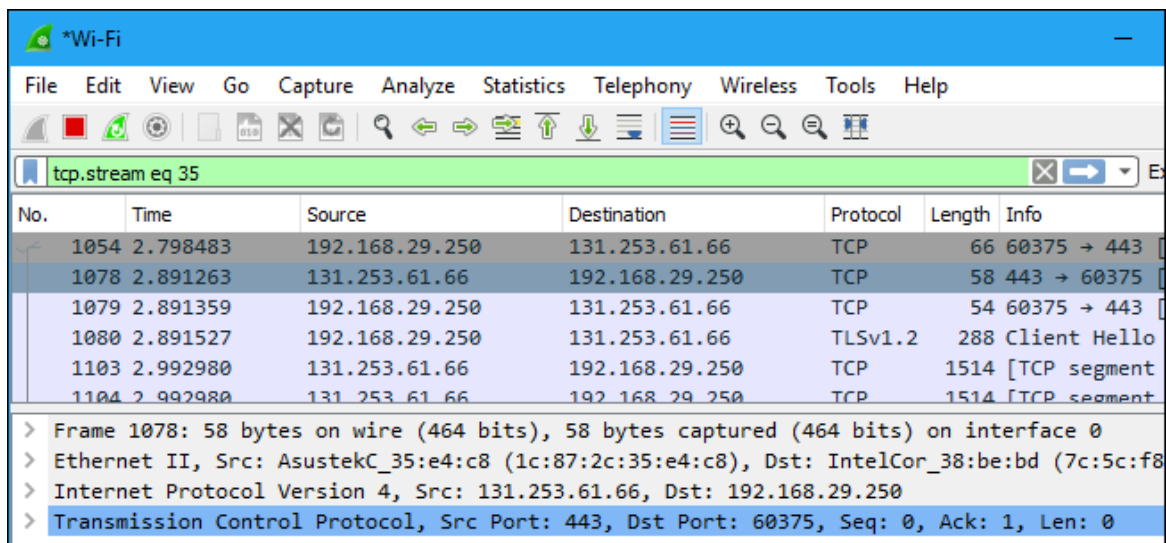


Another interesting thing you can do is right-click a packet and select Follow > TCP Stream.

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



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



Inspecting Packets

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

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 35

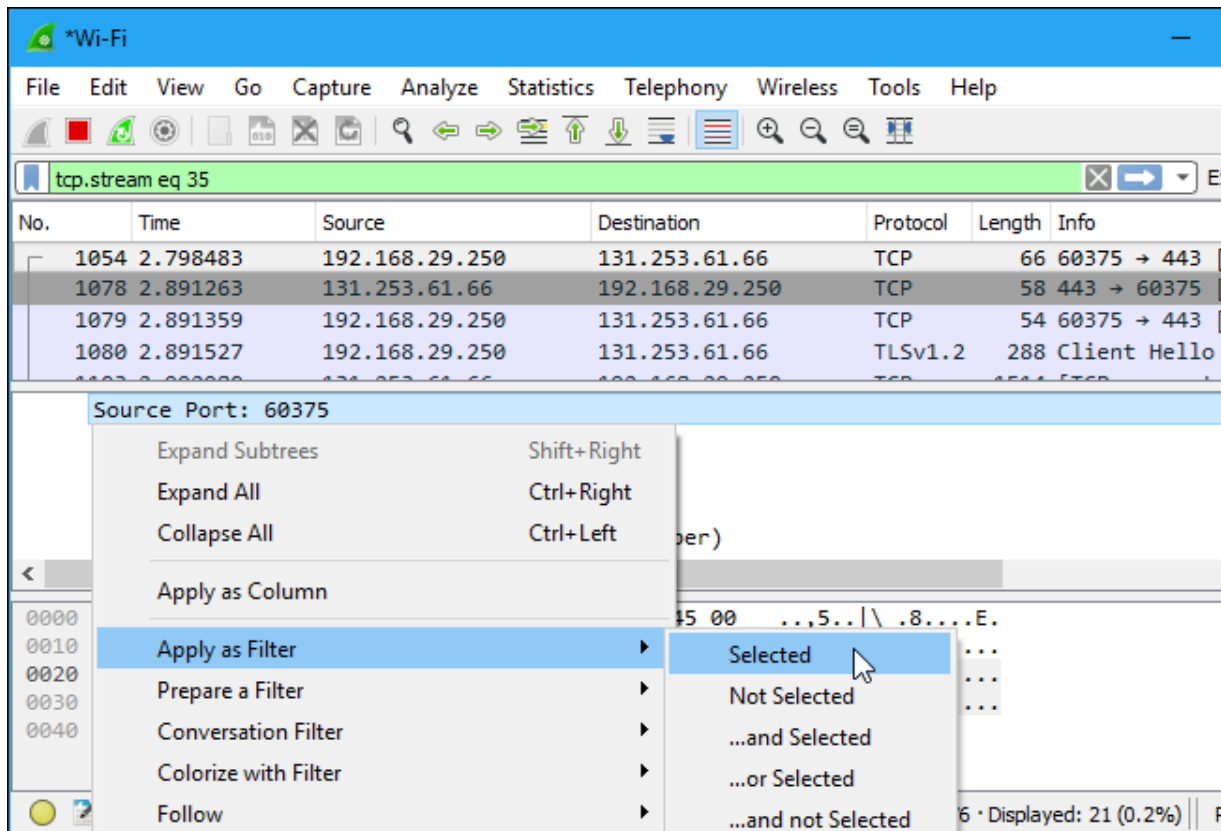
No.	Time	Source	Destination	Protocol	Length	Info
1054	2.798483	192.168.29.250	131.253.61.66	TCP	66	60375 → 443
1078	2.891263	131.253.61.66	192.168.29.250	TCP	58	443 → 60375
1079	2.891359	192.168.29.250	131.253.61.66	TCP	54	60375 → 443
1080	2.891527	192.168.29.250	131.253.61.66	TLSv1.2	288	Client Hello

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

0000	1c 87 2c 35 e4 c8 7c 5c f8 38 be bd 08 00 45 00	..,5.. \ .8....E.
0010	00 34 0b 5d 40 00 80 06 4f 85 c0 a8 1d fa 83 fd	.4.]@... O.....
0020	3d 42 eb d7 01 bb 22 52 7b 69 00 00 00 00 80 02	=B...."R {i.....
0030	fa f0 48 ef 00 00 02 04 05 b4 01 03 03 08 01 01	..H.....
0040	04 02	..

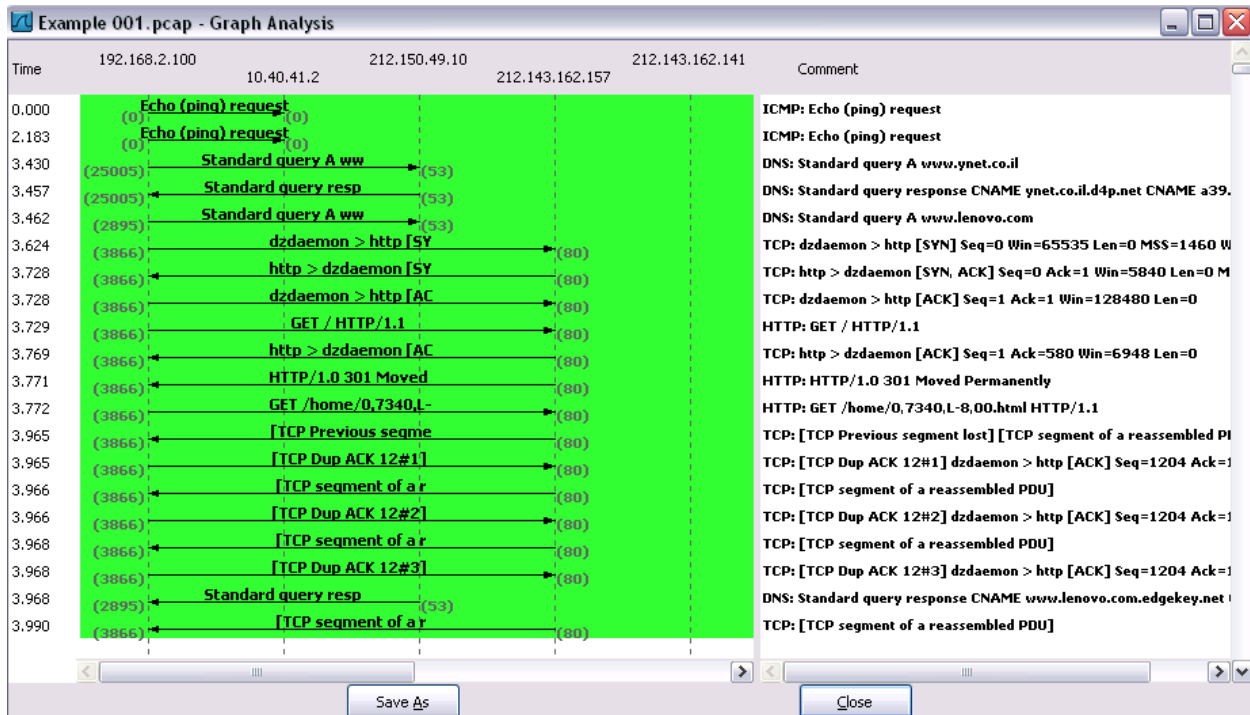
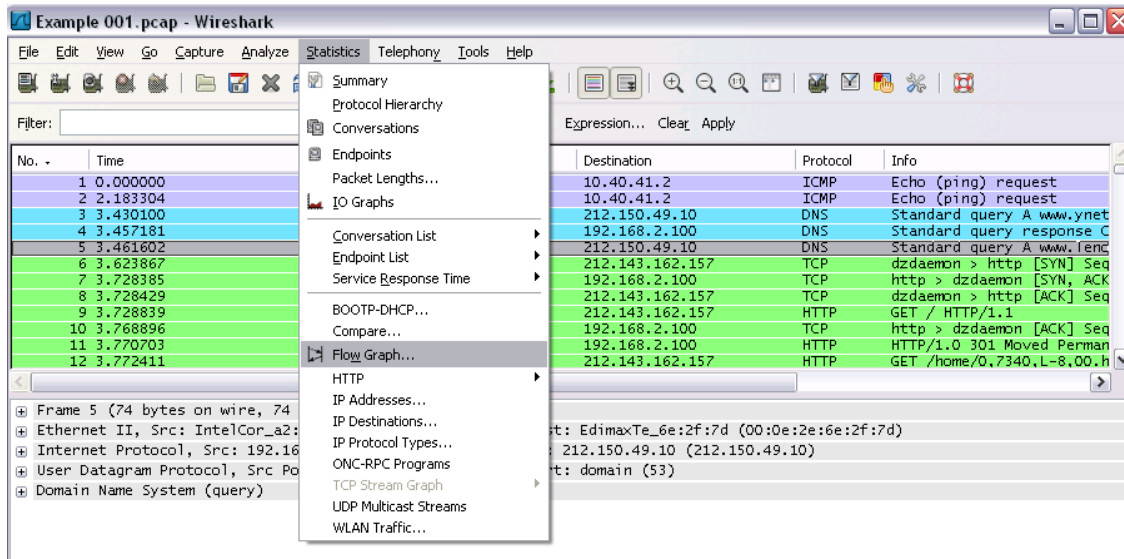
Encapsulation type (frame.encap_type) | Packets: 8136 · Displayed: 21 (0.3%)

You can also create filters from here — just right-click one of the details and use the Apply as Filter submenu to create a filter based on it.



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

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



Ex No: 14 b

PACKET SNIFFING USING WIRESHARK


AIM:

To capture, save, filter and analyze network traffic on TCP / UDP / IP / HTTP / ARP /DHCP /ICMP /DNS using Wireshark Tool

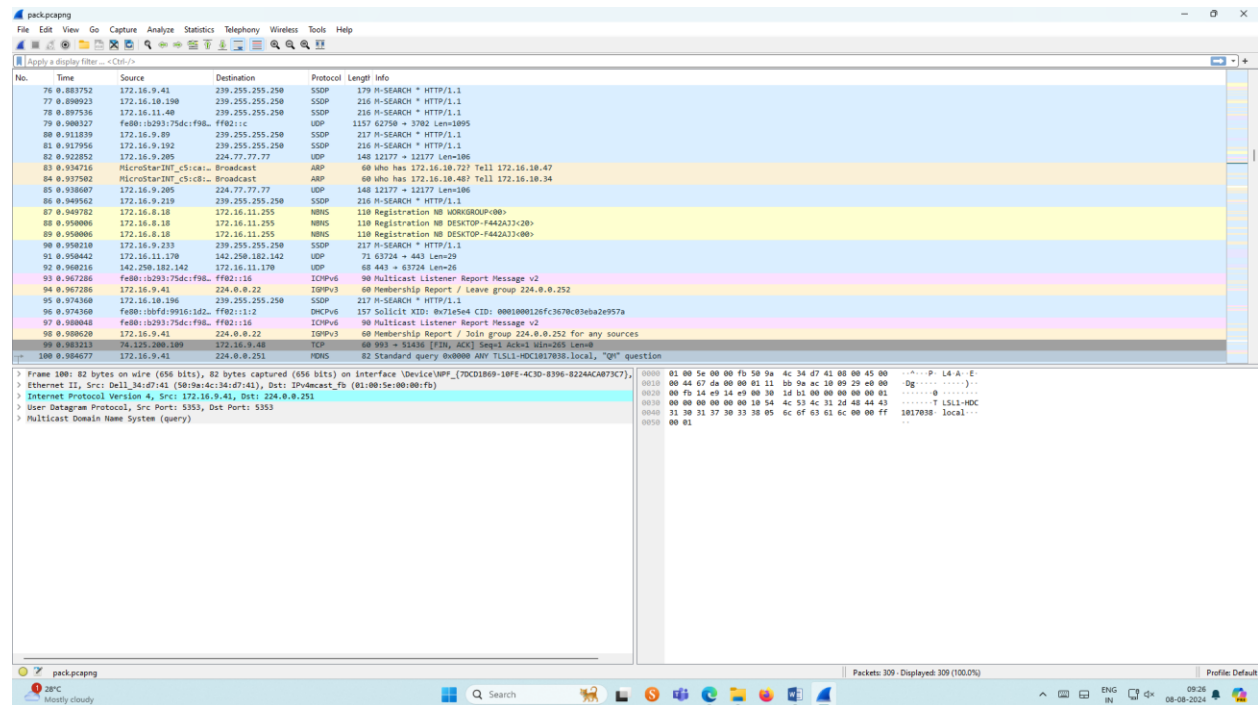
Exercises

1. Capture 100 packets from the Ethernet: IEEE 802.3 LAN Interface and save it.

Procedure

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

Output





The image shows a screenshot of the Wireshark network protocol analyzer. The main window displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The packets are filtered by 'ethernet II, Src: Dell_34d741 (98:9d:4c:34:d7:41), Dst: IP-broadcast (01:00:5e:00:00:fb)'. The packet list shows various protocols including HTTP, UDP, ARP, and DNS. The packet details pane on the right shows the selected packet (No. 100) as an Ethernet II frame, and the packet bytes pane shows the raw data in hexadecimal and ASCII.

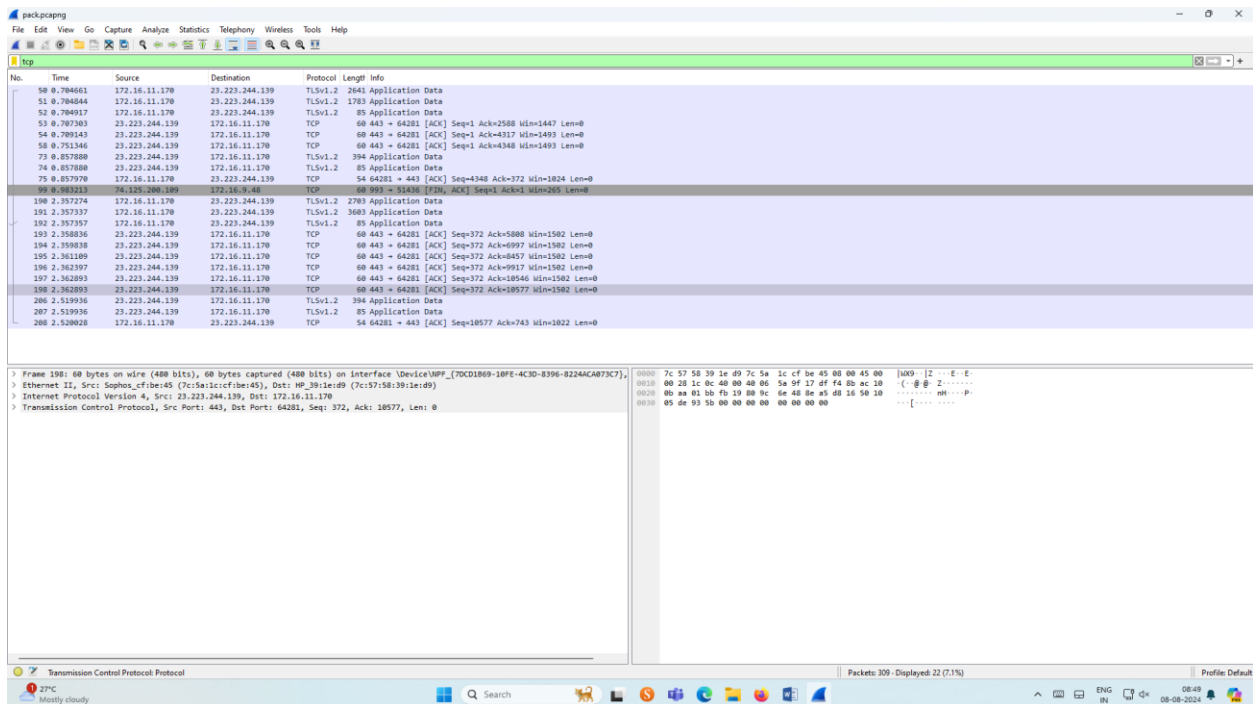
No.	Time	Source	Destination	Protocol	Length	Info
76	0.883752	172.16.9.41	239.255.255.250	SSDP	179	H-SEARCH * HTTP/1.1
77	0.890923	172.16.18.190	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
78	0.897536	172.16.11.40	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
79	0.900327	fe80::b293:75dc:f9b...ff02::1c		UDP	1157	62750 → 3702 Len=1095
80	0.911839	172.16.9.49	239.255.255.250	SSDP	217	H-SEARCH * HTTP/1.1
81	0.917956	172.16.9.192	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
82	0.922852	172.16.9.205	224.77.77.77	UDP	148	12177 → 12177 Len=106
83	0.934716	MicroStarINT_c5:ca...		ARP	60	who has 172.16.18.72? Tell 172.16.18.47
84	0.937592	MicroStarINT_c5:c8...		ARP	60	who has 172.16.18.40? Tell 172.16.18.34
85	0.938607	172.16.9.205	224.77.77.77	UDP	148	12177 → 12177 Len=106
86	0.949562	172.16.9.219	239.255.255.250	SSDP	216	H-SEARCH * HTTP/1.1
87	0.949782	172.16.8.18	172.16.11.255	NBNS	118	Registration NB XDRGROUP=800
88	0.950006	172.16.8.18	172.16.11.255	NBNS	118	Registration NB DESKTOP-F442A33C20
89	0.950006	172.16.8.18	172.16.11.255	NBNS	118	Registration NB DESKTOP-F442A33C20
90	0.950218	172.16.9.231	239.255.255.250	SSDP	217	H-SEARCH * HTTP/1.1
91	0.950442	172.16.11.170	142.250.182.142	UDP	71	63724 → 443 Len=29
92	0.960216	142.250.182.142	172.16.11.170	UDP	68	443 → 63724 Len=26
93	0.967286	fe80::b293:75dc:f9b...ff02::1d		ICMPv6	90	Multicast Listener Report Message v2
94	0.967286	172.16.9.41	224.0.0.22	IGMPv3	60	Membership Report / Leave group 224.0.0.252
95	0.974368	172.16.18.196	239.255.255.250	SSDP	217	H-SEARCH * HTTP/1.1
96	0.974368	fe80::b0fd:9916:1d2...ff02::1d		DHCPv6	157	Solicit XID: 0x71e5e4 CID: 0001000126fc3670c03eba2e957a
97	0.100048	fe80::b293:75dc:f9b...ff02::1d		ICMPv6	90	Multicast Listener Report Message v2
98	0.980620	172.16.9.41	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any sources
99	0.981213	74.125.200.189	172.16.9.48	TCP	60	993 → 51436 [FIN, ACK] Seq=1 Ack=1 Win=285 Len=0
100	0.984677	172.16.9.41	224.0.0.251	MDNS	82	Standard query 0x0000 ANY TL3L1-MC3M17858.local, "Q" question

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

Procedure

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

Output:

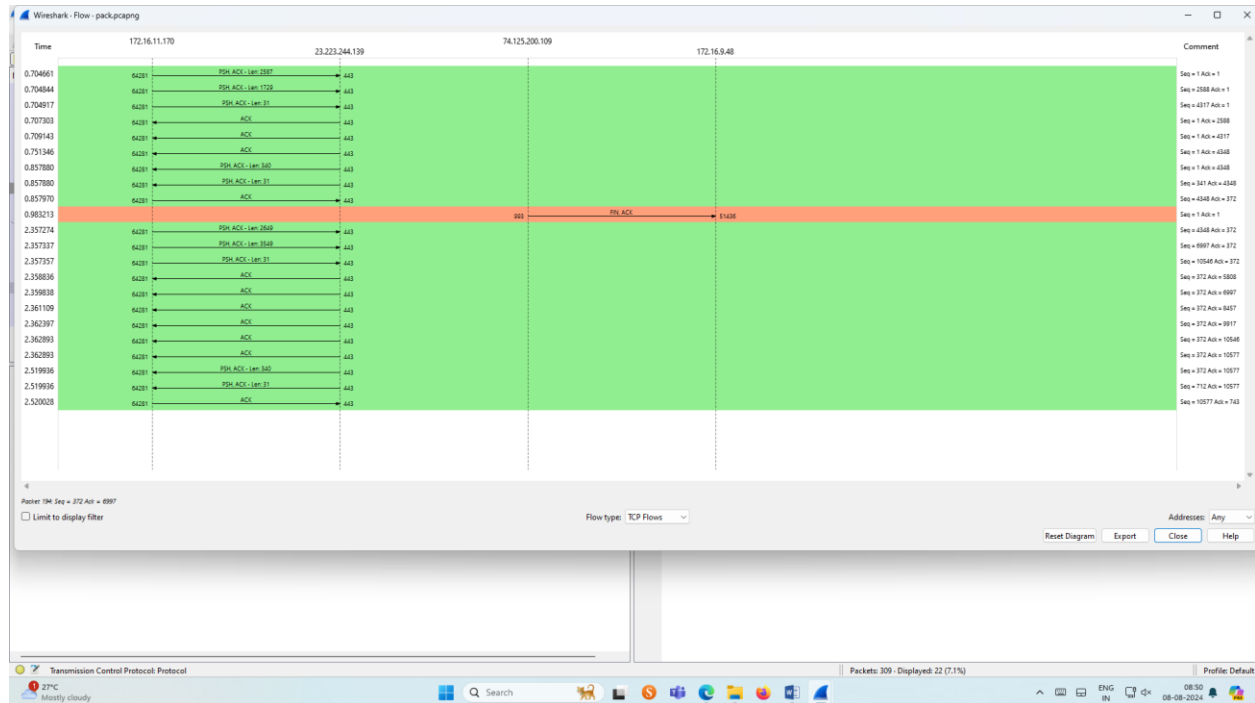


The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The main window is divided into three panes:

- Packet List:** Shows a list of captured packets. The selected packet is 198, which is a TCP segment from 172.16.11.170 to 23.223.244.139. The packet details show it is a SYN packet (Seq=372, Win=1582, Len=0).
- Packet Details:** Provides a hierarchical view of the selected packet's structure. It shows the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header.
- Packet Bytes:** Displays the raw data of the selected packet in hexadecimal and ASCII format.

The bottom status bar indicates that 300 packets were captured and 22 (7.1%) are displayed. The system tray shows the date and time as 08-08-2024.

Flow Graph output

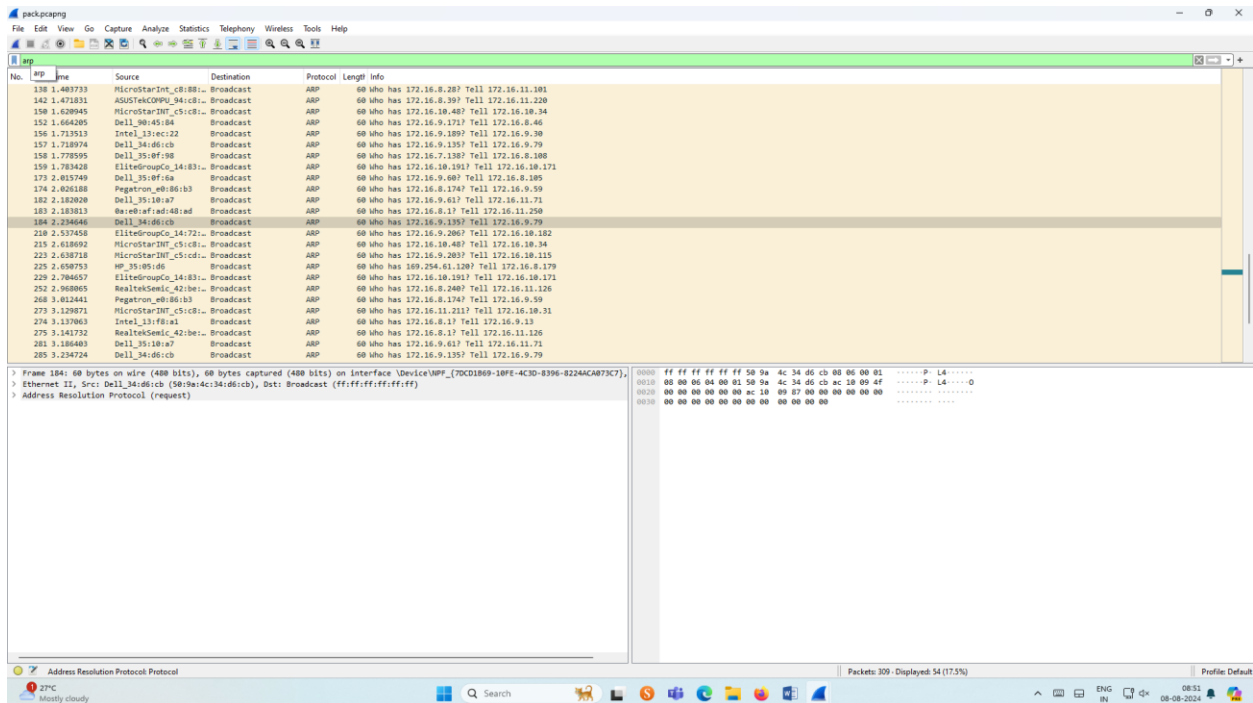


3. Create a Filter to display only ARP packets and inspect the packets.

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.

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.
- Save the packets.

Output

dns

No.	Source	Destination	Protocol	Length	Info
385	172.16.11.170	172.16.8.1	DNS	79	Standard query 8bc945 A fp-vp.azureedge.net
387	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.vpc.vcdn.net A 117.18.232.200
388	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.vpc.vcdn.net A 117.18.232.200

> Frame 373: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on Interface {DeviceNPF_{70CD1869-10FE-4C3D-8396-8224AC873C7}}, Ethernet II, Src: WP_3813e08 (7c:57:58:b3:1e:09), Dst: Sophos_cf1be145 (7c:5a:1c:cf:1b:45)

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

> User Datagram Protocol, Src Port: 51088, Dst Port: 53

> Domain Name System (query)

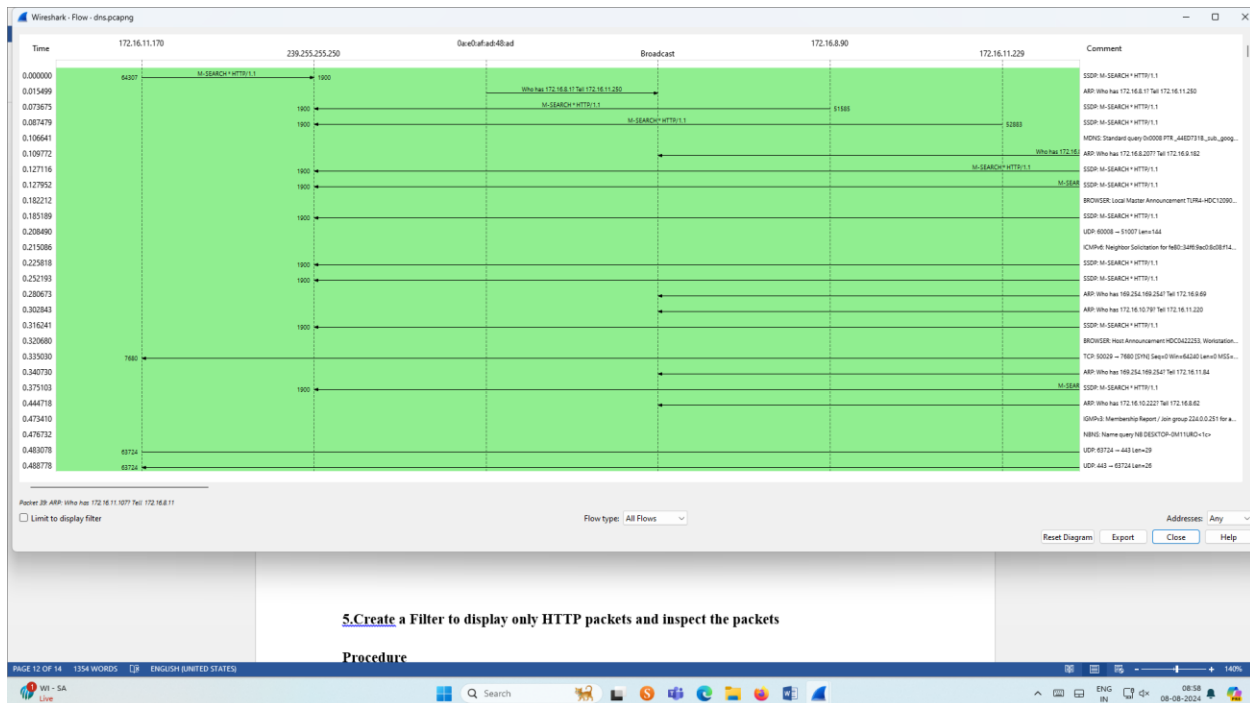
0000 7c 5a 1c cf 1b 45 7c 57 58 39 1e 09 00 00 45 00 |2- [w X0...E-
0010 00 41 6d 38 00 00 11 00 00 ac 10 00 aa ac 10 |AoB...
0020 08 81 cb 14 00 35 00 2d 6c 0a c9 45 01 00 00 01 |.....S- 1-E...
0030 00 00 00 00 00 00 05 66 70 2d 76 70 00 01 7a 75 |.....f p-vp.azu
0040 72 65 65 64 67 65 83 6e 65 74 00 00 01 00 01 |reedge-n et....

Domain Name System Protocol

Packets: 1562 - Displayed: 4 (0.3%)


Profile Default

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

Wireshark Network Analyzer - Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Filter: http

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.11.170	23.215.215.114	HTTP	288	GET /connecttest.txt HTTP/1.1
2	0.000000	172.16.11.170	23.215.215.114	HTTP	288	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 1230: 288 bytes on wire (1664 bits), 288 bytes captured (1664 bits) on interface \Device\NPF_{70CD1869-18FE-4C3D-B396-8224ACA07} [Ethernet II, Src: HP_39:1e:d9 (7c:57:50:39:1e:d9), Dst: Sophos_cf:be:45 (7c:5a:1c:cf:be:45)]

Ethernet II, Src: HP_39:1e:d9 (7c:57:50:39:1e: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

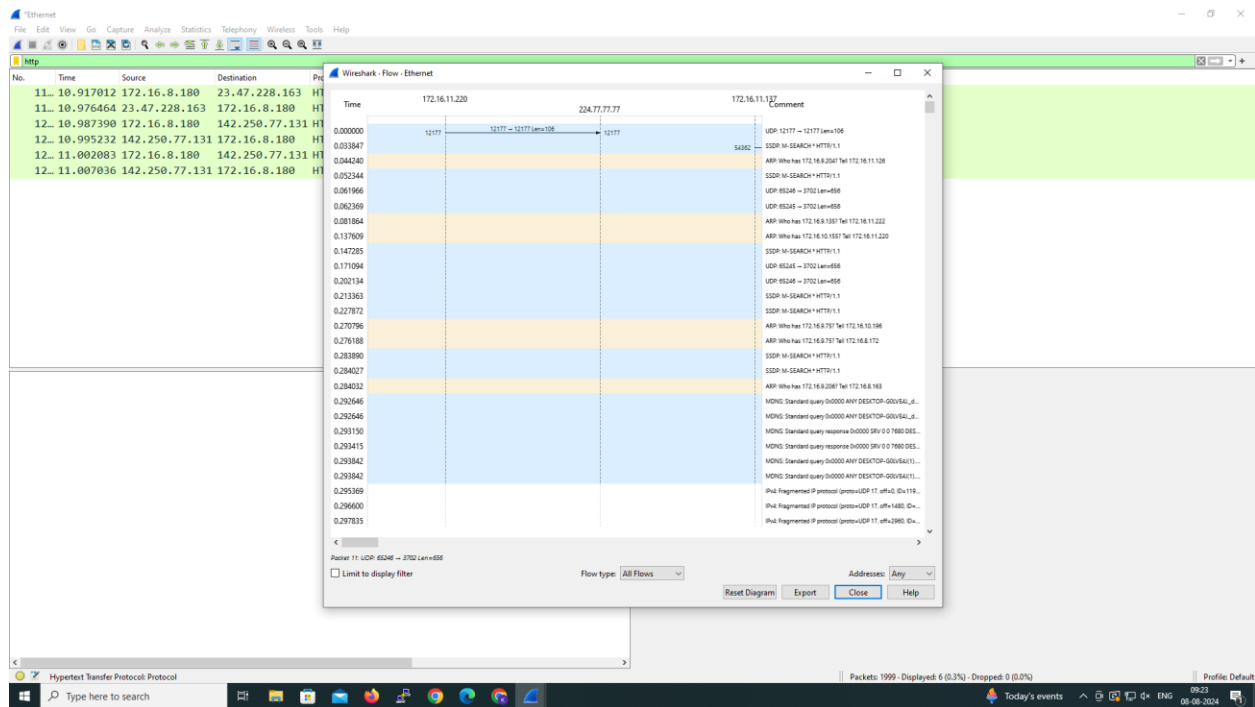
Hypertext Transfer Protocol

0000 7c 5a 1c cf be 45 7c 57 50 39 1e d9 00 00 45 00 | 2 - E | W X9 - - - - - E
0010 00 c2 24 25 40 00 00 00 00 00 ac 10 0b aa 17 d7 | \$B - - - - -
0020 d7 72 fb 51 00 50 db 49 a5 c0 2a 43 a4 7c 50 18 | - r Q P I - - C | P
0030 01 00 47 50 00 00 47 45 54 20 2f 03 0f 6e 6e 65 | - - - - - OE T / come
0040 63 74 74 65 73 74 2e 74 70 74 20 48 54 50 2f | cttest.t xt HTTP/
0050 31 2e 31 0d 0a 43 61 63 68 05 2d 43 0f 6e 74 72 | 1.1 - Cac he-Contr
0060 6f 6c 3a 20 6e 6f 2d 63 61 63 68 05 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 0d | nnection : Close
0080 0a 50 72 61 67 6d 61 3a 20 6e 6f 2d 63 61 63 68 | -Pragmas: 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 48 | icrosoft MCS: 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 0a 0d 0a | necttest .com - - -

Packets: 4285 - Displayed: 4 (0.1%) - Dropped: 0 (0.0%)


Profile: Default

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

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

