

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:

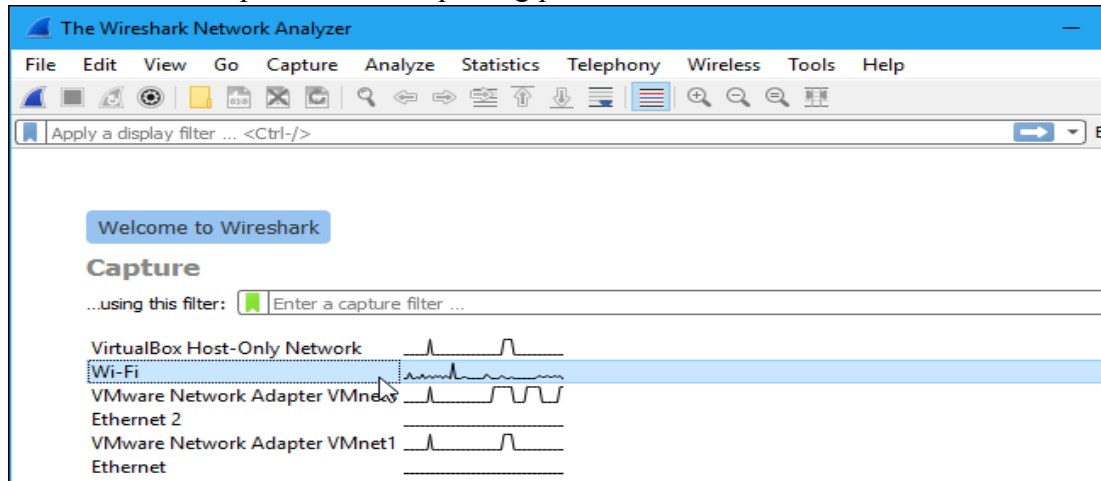
- Network administrators: troubleshoot network problems
- Network security engineers: examine security problems
- Developers: debug protocol implementations
- People: learn **network protocol internals**

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.

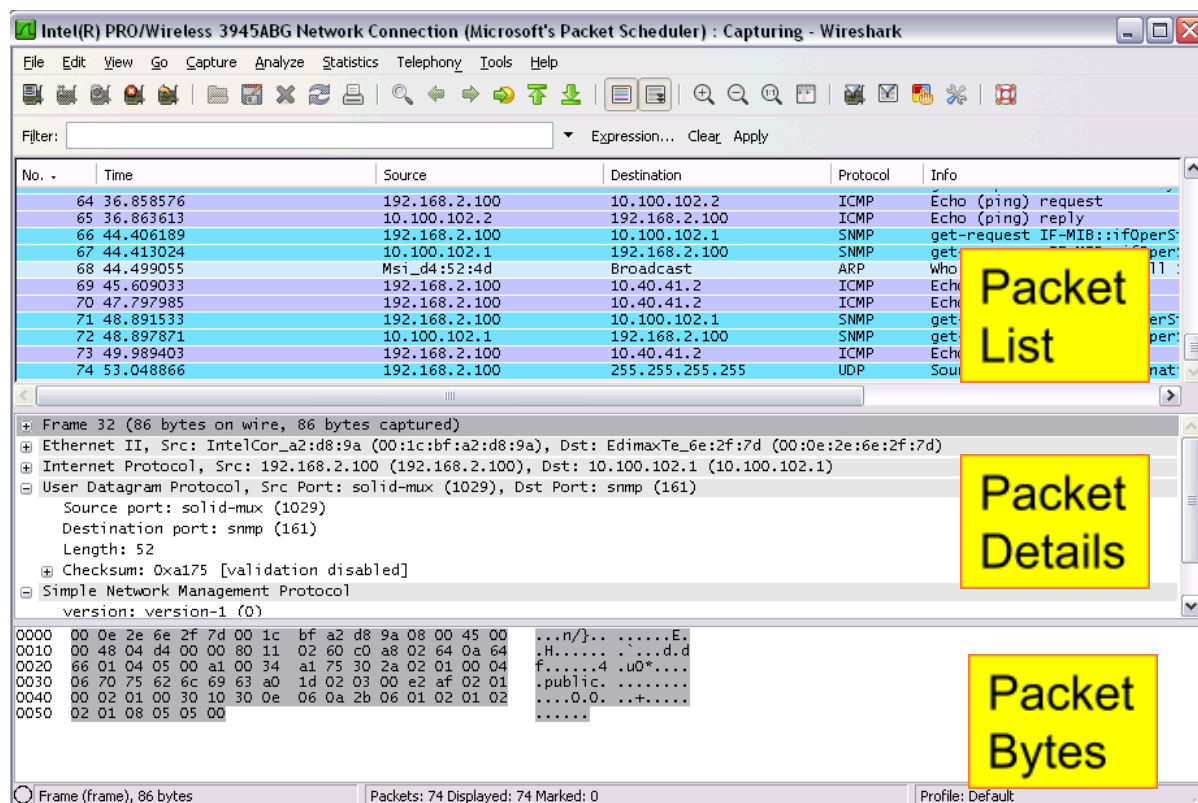
Capturing Packets

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



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.

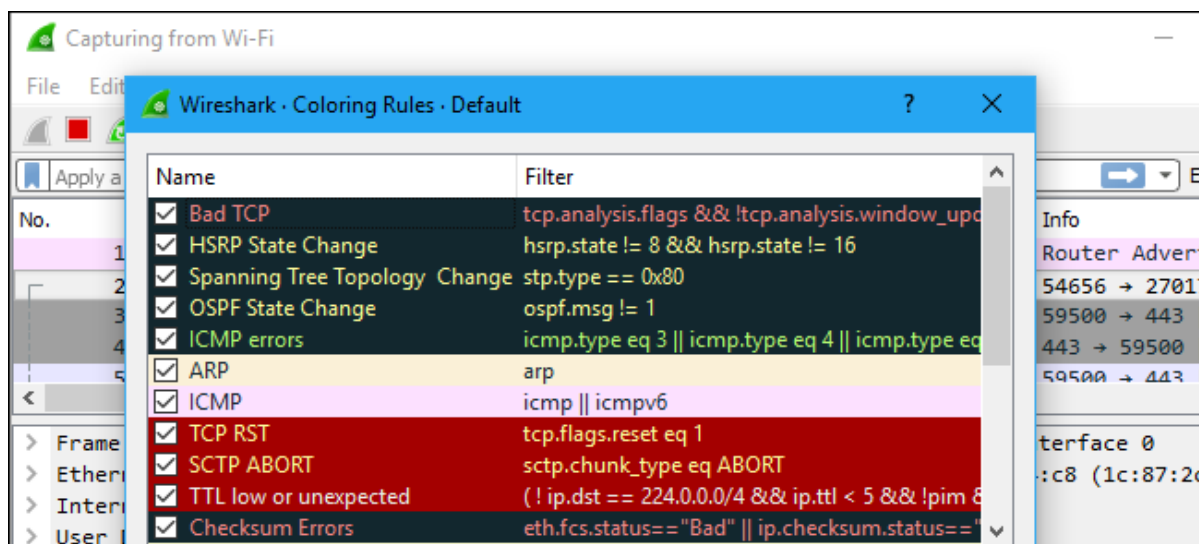
The “Packet Bytes” Pane

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.

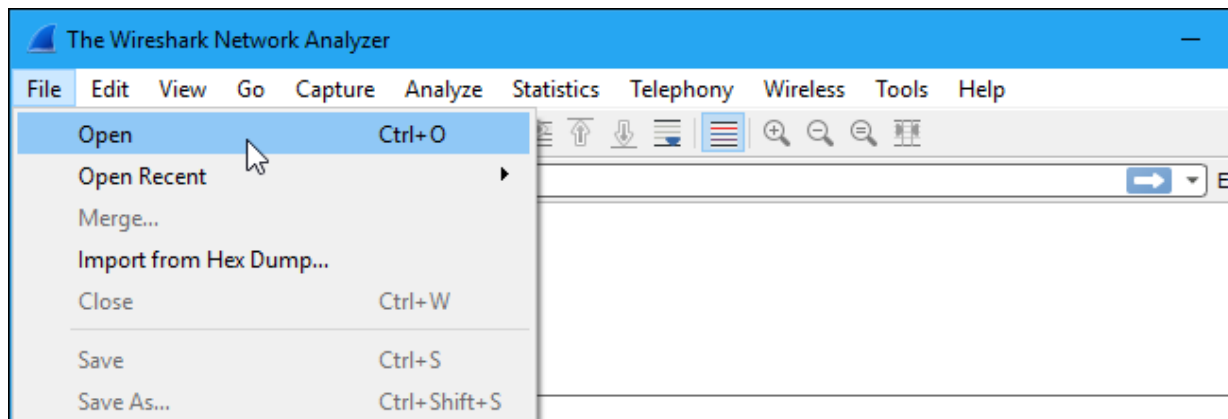
To view exactly what the color codes mean, click View > Coloring Rules. You can also customize and modify the coloring rules from here, if you like.



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.

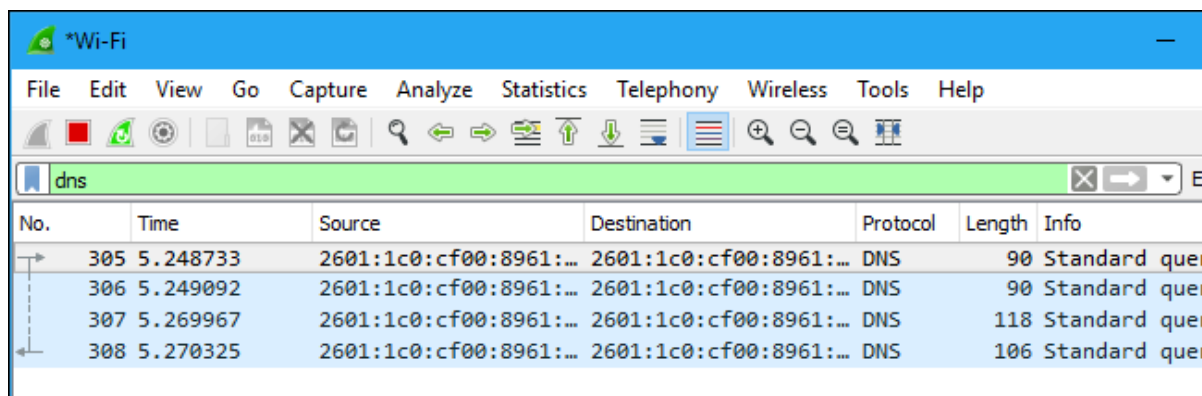
You can also save your own captures in Wireshark and open them later. Click File > Save to save your captured packets.



Filtering Packets

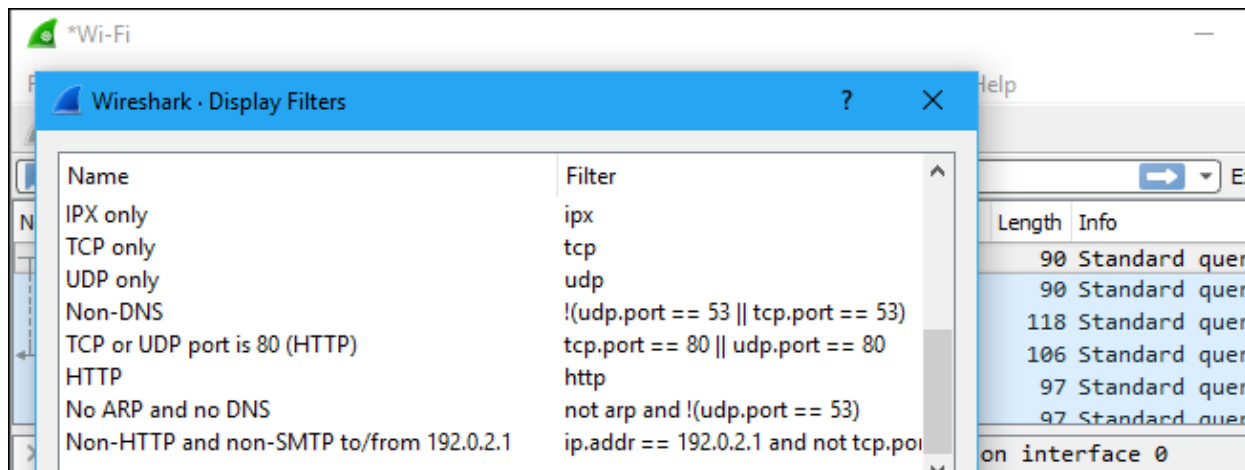
If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark's filters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



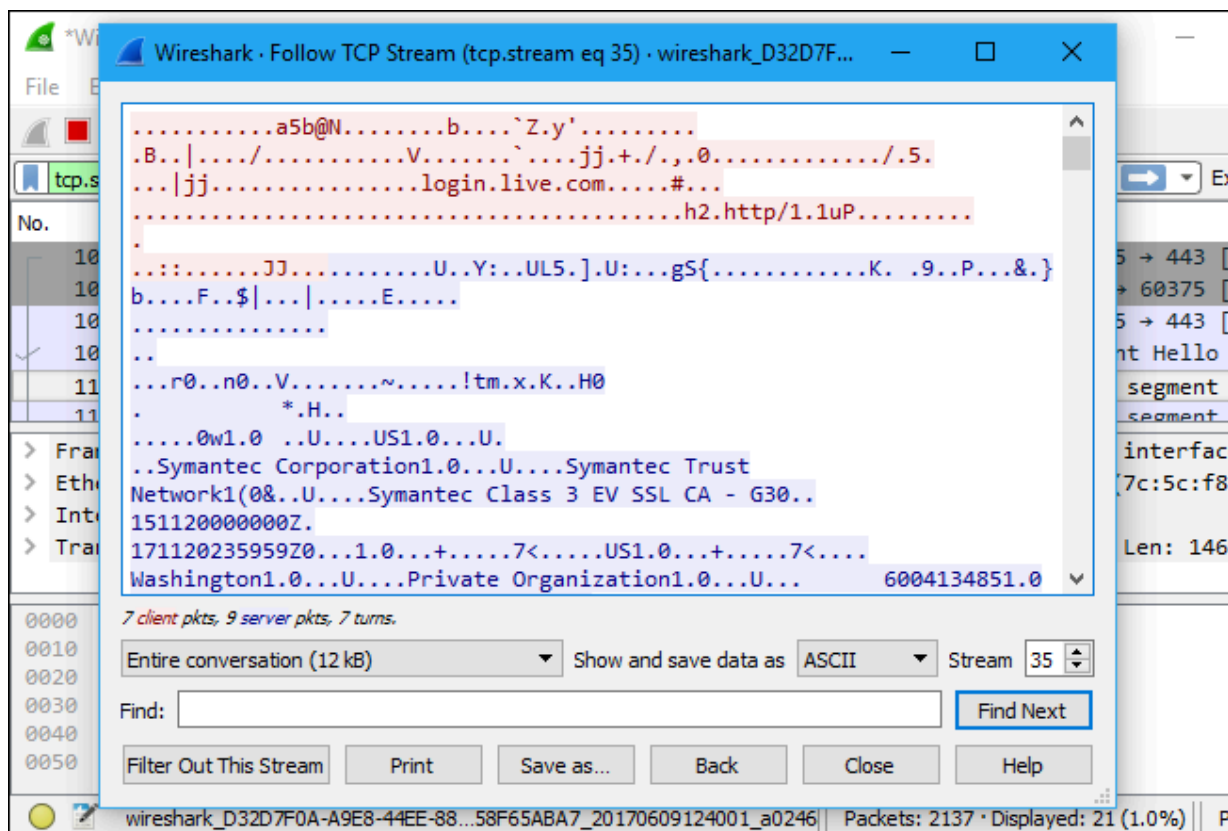
You can also click Analyze > Display Filters to choose a filter from among the default filters included in Wireshark. From here, you can add your own custom filters and save them to easily access them in the future.

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

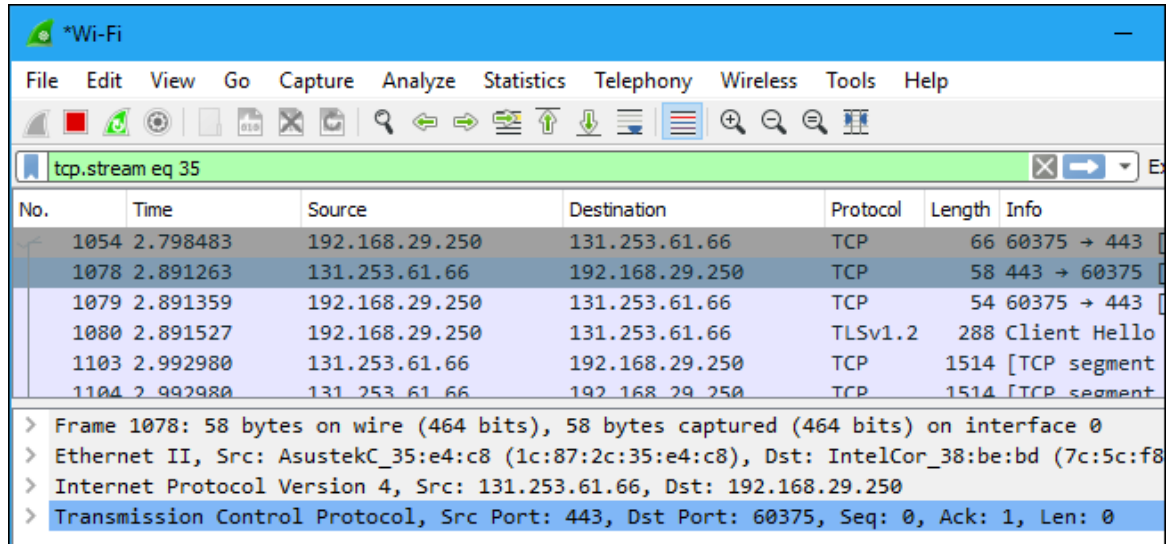


Another interesting thing you can do is right-click a packet and select Follow > TCP Stream.

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.



The image shows a Wireshark packet capture window titled '*Wi-Fi'. The filter bar at the top contains the text 'tcp.stream eq 35'. Below the filter bar is a table of captured packets. The table has columns for No., Time, Source, Destination, Protocol, Length, and Info. The following table represents the data shown in the packet list:

No.	Time	Source	Destination	Protocol	Length	Info
1054	2.798483	192.168.29.250	131.253.61.66	TCP	66	60375 → 443
1078	2.891263	131.253.61.66	192.168.29.250	TCP	58	443 → 60375
1079	2.891359	192.168.29.250	131.253.61.66	TCP	54	60375 → 443
1080	2.891527	192.168.29.250	131.253.61.66	TLSv1.2	288	Client Hello
1103	2.992980	131.253.61.66	192.168.29.250	TCP	1514	[TCP segment
1104	2.992980	131.253.61.66	192.168.29.250	TCP	1514	[TCP segment

Below the packet list, the details pane for packet 1078 is expanded, showing the following information:

- > Frame 1078: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface 0
- > Ethernet II, Src: AsustekC_35:e4:c8 (1c:87:2c:35:e4:c8), Dst: IntelCor_38:be:bd (7c:5c:f8)
- > Internet Protocol Version 4, Src: 131.253.61.66, Dst: 192.168.29.250
- > Transmission Control Protocol, Src Port: 443, Dst Port: 60375, Seq: 0, Ack: 1, Len: 0

Inspecting Packets

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

The image shows a Wireshark packet capture window titled "*Wi-Fi". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains 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 details pane for frame 1054 shows the following information:

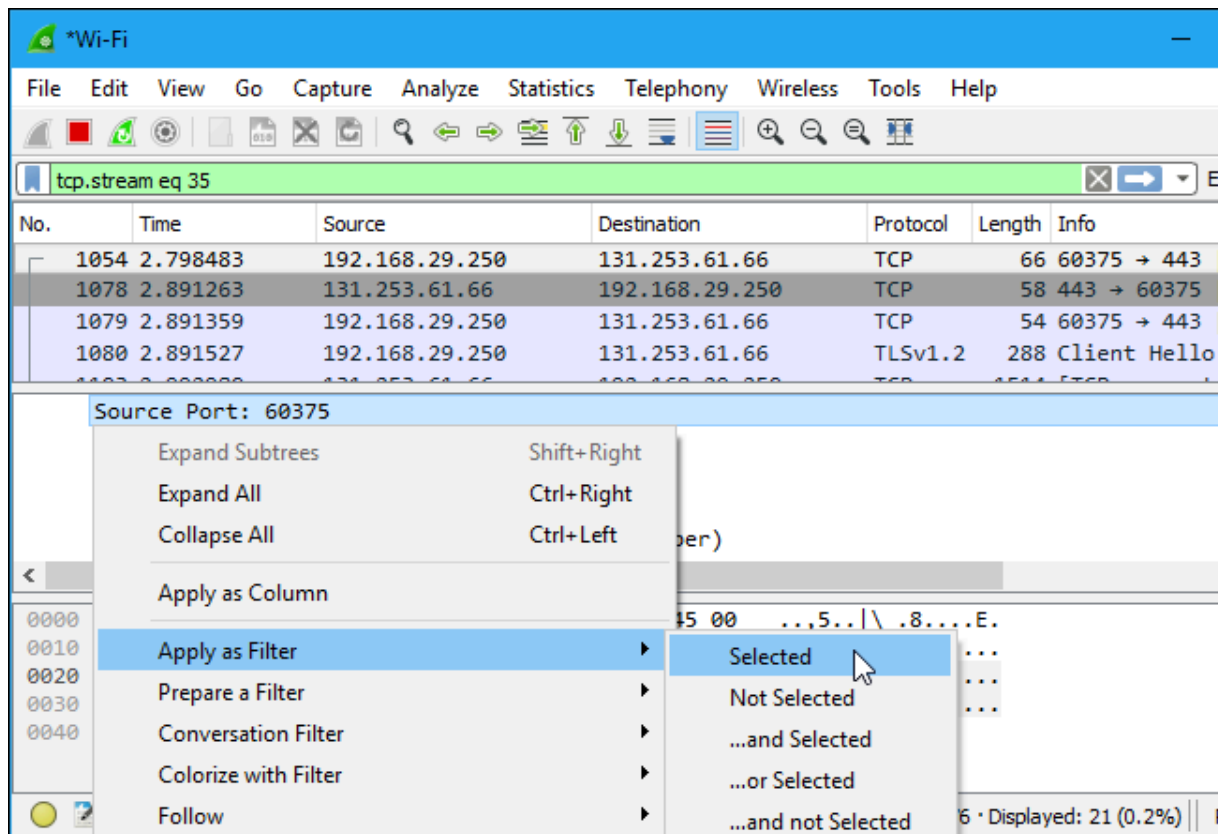
- Frame 1054: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
- Interface id: 0 (\Device\NPF_{D32D7F0A-A9E8-44EE-88DC-DFD58F65ABA7})
- Encapsulation type: Ethernet (1)
- Arrival Time: Jun 9, 2017 12:40:04.140141000 Pacific Daylight Time
- [Time shift for this packet: 0.000000000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

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

```
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 ..
```

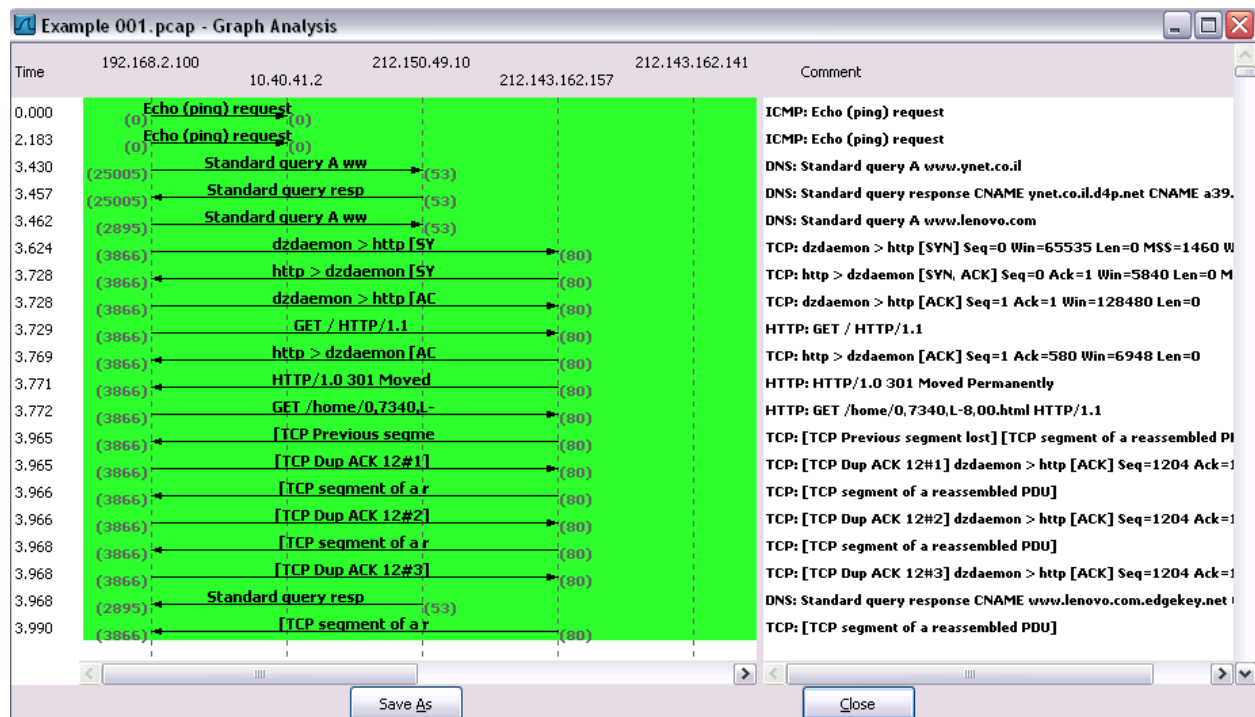
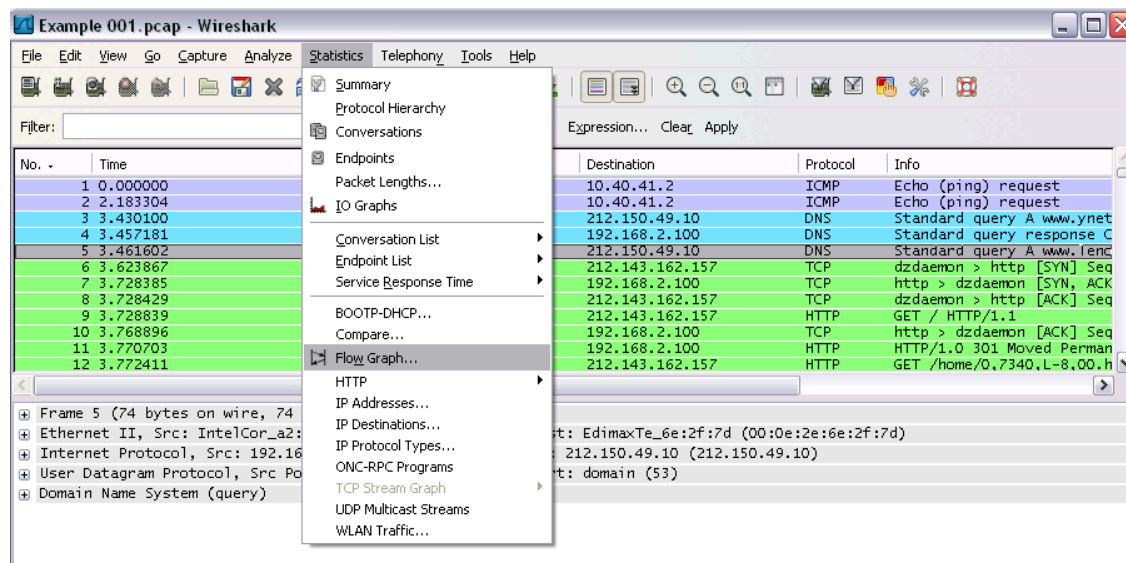
The status bar at the bottom indicates "Encapsulation type (frame.encap_type)" and "Packets: 8136 · Displayed: 21 (0.3%)".

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 screenshot displays the Wireshark network protocol analyzer interface. At the top, the status bar indicates '100 packets captured'. The main window is divided into three panes: the packet list, packet details, and packet bytes.

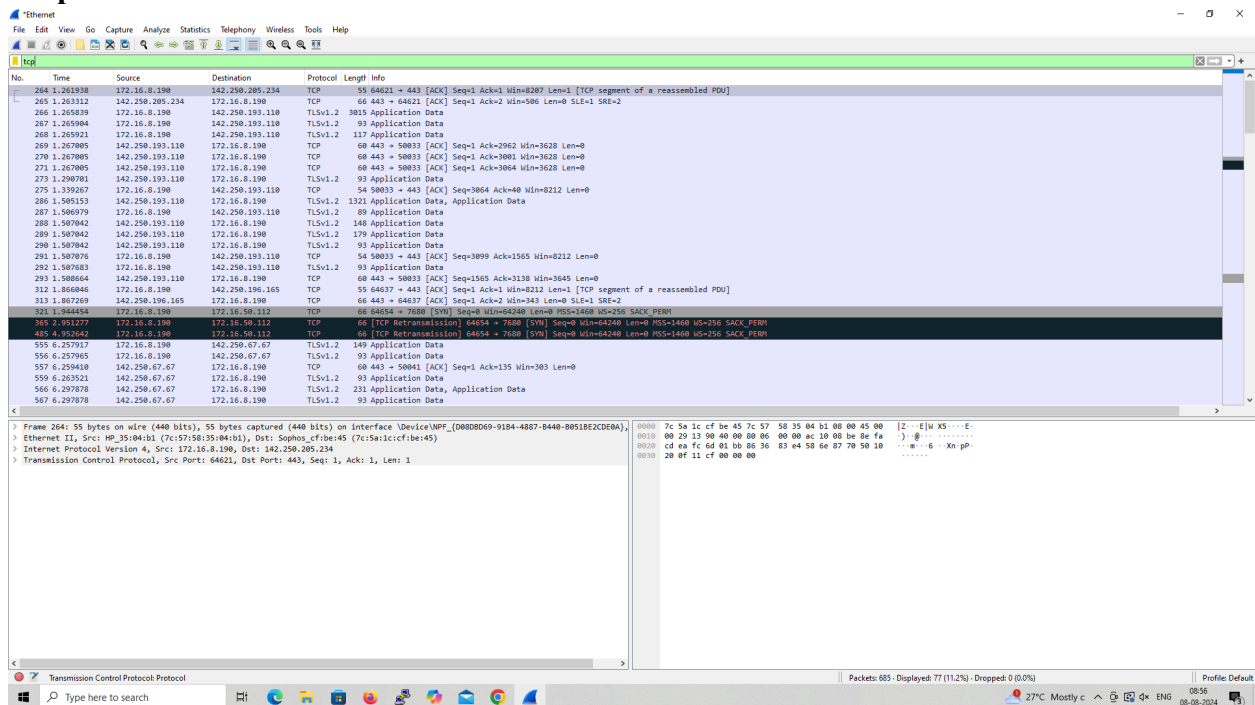
Packet List: This pane shows a list of 100 captured packets. The columns include No., Time, Source, Destination, Protocol, Length, and Info. The packets are filtered by 'ethernet II, Src: ElitedropCo_14:72:43 (80:0e:dd:14:72:43), Dst: 192.16.10.190 (81:00:5e:7f:ff:fa)'. The list shows various protocols such as ICMP, DNS, and HTTP.

Packet Details: This pane shows the hierarchical structure of the selected packet (No. 100). It includes fields like Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Simple Service Discovery Protocol.

Packet Bytes: This pane shows the raw data of the selected packet in hexadecimal and ASCII format. The data is displayed in a hex dump view, showing the raw bytes of the packet.

Procedure

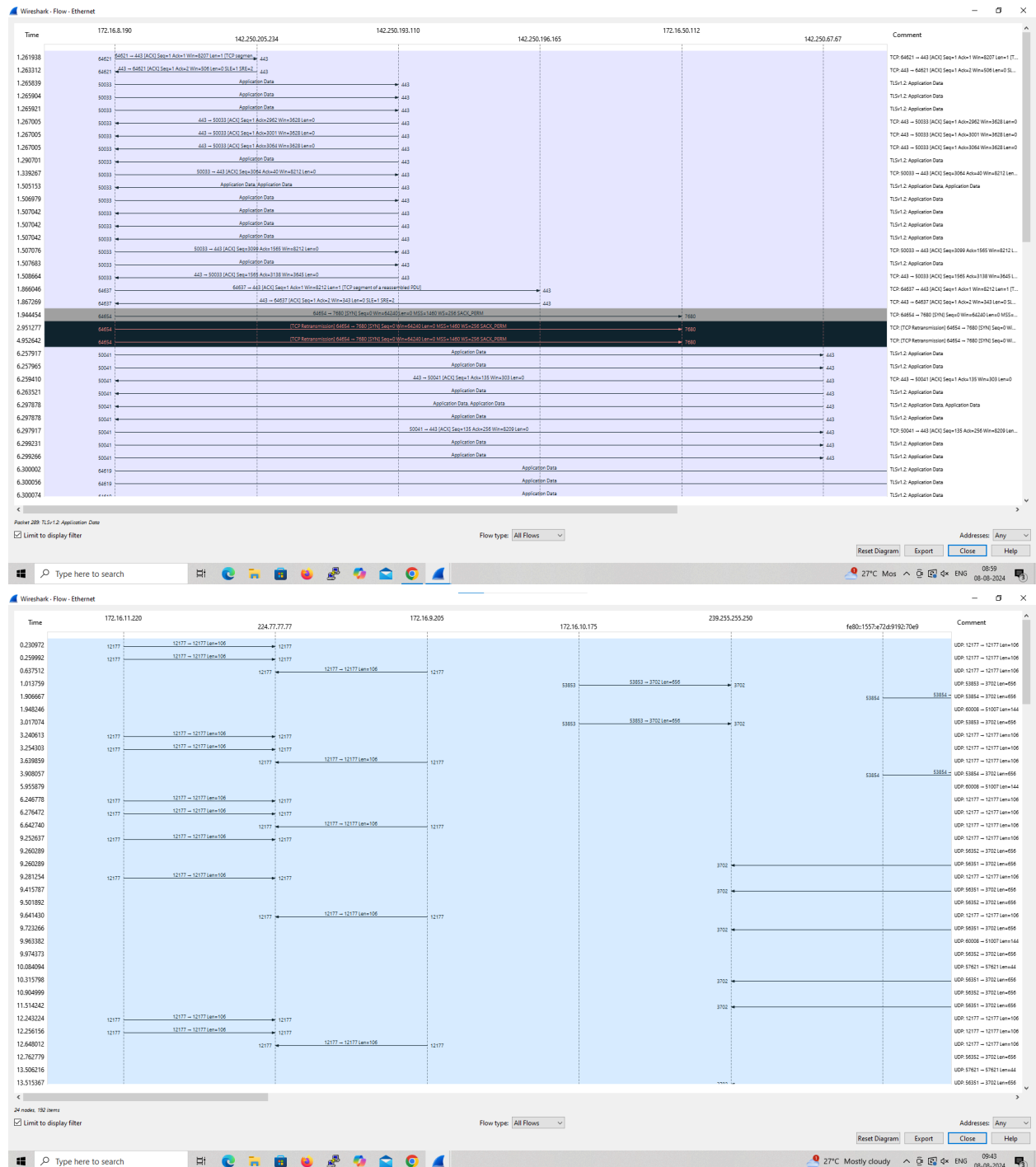
- Output:**



Wireshark packet capture analysis of a UDP packet. The packet list shows a UDP packet from 172.16.11.220 to 172.16.11.255. The packet details show the Ethernet II, Internet Protocol Version 4, and User Datagram Protocol layers. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Wireshark packet capture analysis of a UDP packet. The packet list shows a UDP packet from 172.16.11.220 to 172.16.11.255. The packet details show the Ethernet II, Internet Protocol Version 4, and User Datagram Protocol layers. The packet bytes pane shows the raw data in hexadecimal and ASCII.

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

The screenshot shows the Wireshark interface with a filter applied to display only ARP packets. The packet list shows 15 ARP packets, all of which are broadcasts from various sources to the destination ff:ff:ff:ff:ff:ff. The packet details pane shows the structure of an ARP Announcement packet, including Ethernet II, Internet Protocol Version 4, and Address Resolution Protocol (ARP Announcement) fields. The packet bytes pane shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
5	0.148237	Dell_34:d4:98	Broadcast	ARP	60	who has 172.16.9.163? Tell 172.16.11.47
6	0.165688	VP_39:53:ad	Broadcast	ARP	60	ARP Announcement for 172.16.9.216
11	0.272167	MicroStarINT_c5:ch...	Broadcast	ARP	60	who has 172.16.11.121? Tell 172.16.10.2
20	0.351318	EliteGroupCo_15:e7...	Broadcast	ARP	60	who has 169.254.169.254? Tell 172.16.10.194
25	0.485053	Dell_34:d7:f5	Broadcast	ARP	60	who has 172.16.10.69? Tell 172.16.11.16
39	0.750620	0a:e8:af:ad:48:ad	Broadcast	ARP	60	who has 172.16.8.1? Tell 172.16.11.250
40	0.776793	AzureWaveTec_9f:0c...	Broadcast	ARP	60	who has 172.16.11.114? (ARP Probe)
46	0.797990	Dell_34:d6:cb	Broadcast	ARP	60	who has 172.16.8.227? Tell 172.16.9.79
68	1.102902	MicroStarInt_ad:3c...	Broadcast	ARP	60	who has 172.16.10.123? Tell 172.16.8.13
71	1.139723	EliteGroupCo_15:ed...	Broadcast	ARP	60	who has 169.254.169.254? Tell 172.16.9.202
82	1.274244	MicroStarINT_c5:ch...	Broadcast	ARP	60	who has 172.16.11.121? Tell 172.16.10.2
83	1.274244	MicroStarInt_ad:3e...	Broadcast	ARP	60	who has 172.16.9.65? Tell 172.16.8.23
88	1.323068	ASUSTeKCOMPU_94:cd...	Broadcast	ARP	60	who has 172.16.9.173? Tell 172.16.11.220
91	1.354368	EliteGroupCo_15:e7...	Broadcast	ARP	60	who has 169.254.169.254? Tell 172.16.10.194
92	1.385753	EliteGroupCo_15:eb...	Broadcast	ARP	60	who has 169.254.169.254? Tell 172.16.10.194

Frame 6: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface UDeviceVFP_08080D69-9184-4807-8440-B051BECDE0A0, 1
> Ethernet II, Src: HP_39:53:ad (7c:57:58:39:53:ad), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (ARP Announcement)

0000 ff ff ff ff ff ff 7c 57 58 39 53 ad 00 00 01 [M] XPS:....
0010 00 00 06 04 00 01 7c 57 58 39 53 ad ac 10 00 05 [M] XPS:....
0020 00 00 00 00 00 00 ac 10 00 d8 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040

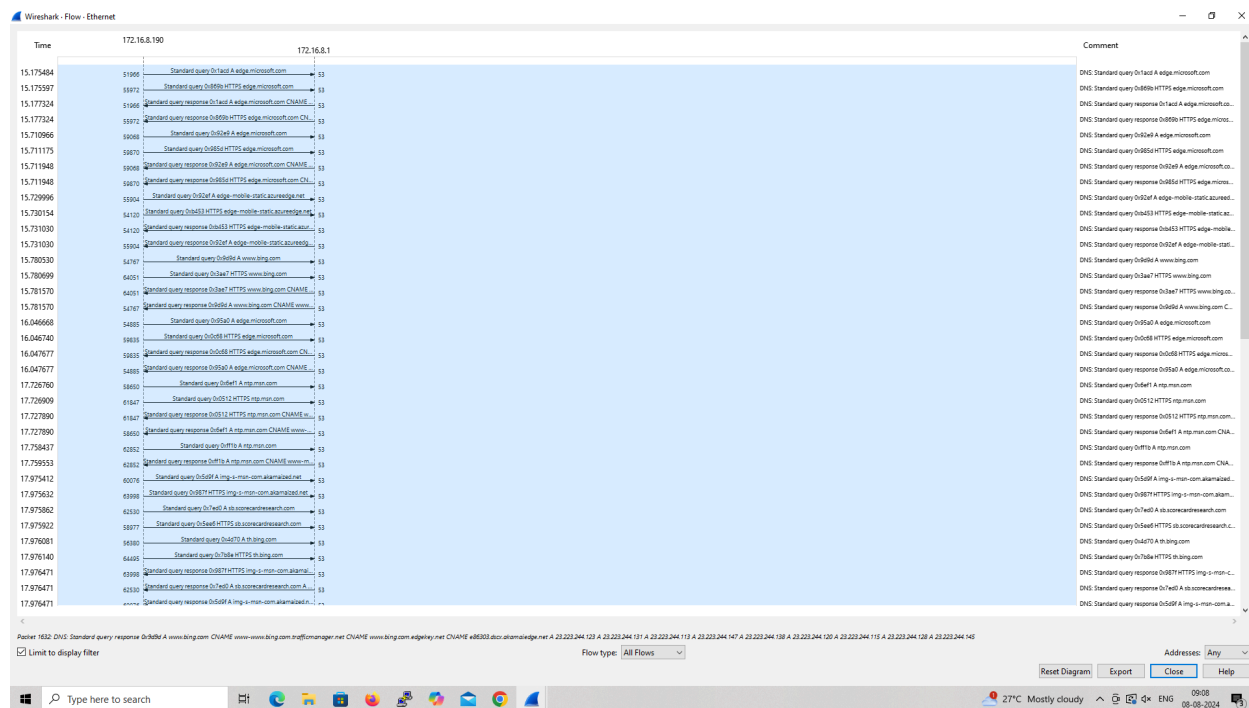
Procedure

- ☐ 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.

File Edit View Go Capture Statistics Telephony Wireless Tools Help
15.775464

No.	Time	Source	Destination	Protocol	Length	Info
1521	15.175464	172.16.8.190	172.16.8.1	DNS	78	Standard query 0x1ad2 A edge.microsoft.com
1522	15.175597	172.16.8.190	172.16.8.1	DNS	78	Standard query 0x0600 HTTPS edge.microsoft.com
1524	15.177324	172.16.8.1	172.16.8.190	DNS	181	Standard query response 0x1ad2 A edge.microsoft.com CNAME edge-microsoft.com.dual-a-0036-a.sedge.net A 13.107.21.239 A 204.79.197.239
1525	15.177324	172.16.8.1	172.16.8.190	DNS	149	Standard query response 0x0600 HTTPS edge.microsoft.com CNAME edge-microsoft.com.dual-a-0036-a.sedge.net CNAME dual-a-0036-a.sedge.net
1590	15.178966	172.16.8.190	172.16.8.1	DNS	78	Standard query 0x02e9 A edge.microsoft.com
1591	15.171175	172.16.8.190	172.16.8.1	DNS	78	Standard query 0x058d HTTPS edge.microsoft.com
1592	15.171184	172.16.8.1	172.16.8.190	DNS	181	Standard query response 0x02e9 A edge.microsoft.com CNAME edge-microsoft.com.dual-a-0036-a.sedge.net CNAME dual-a-0036-a.sedge.net A 13.107.21.239 A 204.79.197.239
1593	15.171184	172.16.8.1	172.16.8.190	DNS	149	Standard query response 0x058d HTTPS edge.microsoft.com CNAME edge-microsoft.com.dual-a-0036-a.sedge.net CNAME dual-a-0036-a.sedge.net
1606	15.172996	172.16.8.190	172.16.8.1	DNS	92	Standard query 0x02ef A edge-mobile-static.azureedge.net
1607	15.173004	172.16.8.190	172.16.8.1	DNS	92	Standard query 0x0453 HTTPS edge-mobile-static.azureedge.net
1608	15.173180	172.16.8.1	172.16.8.190	DNS	245	Standard query response 0x0453 HTTPS edge-mobile-static.azureedge.net CNAME edge-mobile-static.afd.azureedge.net CNAME azureedge-t-prod.trafficmanager.net CNAME shed.dual-lw-s-part-0030-
1609	15.173180	172.16.8.1	172.16.8.190	DNS	205	Standard query response 0x02ef A edge-mobile-static.azureedge.net CNAME edge-mobile-static.afd.azureedge.net CNAME azureedge-t-prod.trafficmanager.net CNAME shed.dual-lw-s-part-0030-
1610	15.173030	172.16.8.1	172.16.8.1	DNS	72	Standard query 0x00d4 A www.bing.com
1610	15.178069	172.16.8.190	172.16.8.1	DNS	72	Standard query 0x03e7 HTTPS www.bing.com
1611	15.1781570	172.16.8.1	172.16.8.190	DNS	193	Standard query response 0x03e7 HTTPS www.bing.com CNAME www-www.bing.com.trafficmanager.net CNAME www.bing.com.edgekey.net CNAME e0303.dscw.akamaiedge.net
1612	15.1781570	172.16.8.1	172.16.8.190	DNS	337	Standard query response 0x00d4 A www.bing.com CNAME www-www.bing.com.trafficmanager.net CNAME www.bing.com.edgekey.net CNAME e0303.dscw.akamaiedge.net A 23.223.244.123 A 23.223.244.131 A
1616	16.046668	172.16.8.190	172.16.8.1	DNS	78	Standard query 0x05b0 A edge.microsoft.com
1619	16.046740	172.16.8.190	172.16.8.1	DNS	78	Standard query 0x00c8 HTTPS edge.microsoft.com
1790	16.047677	172.16.8.1	172.16.8.190	DNS	149	Standard query response 0x00c8 HTTPS edge.microsoft.com CNAME edge-microsoft.com.dual-a-0036-a.sedge.net CNAME dual-a-0036-a.sedge.net
1791	16.047677	172.16.8.1	172.16.8.190	DNS	181	Standard query response 0x05b0 A edge.microsoft.com CNAME edge-microsoft.com.dual-a-0036-a.sedge.net CNAME dual-a-0036-a.sedge.net A 13.107.21.239 A 204.79.197.239
1912	17.727870	172.16.8.190	172.16.8.1	DNS	71	Standard query 0x0ef1 A ntp.ssn.com
1913	17.727899	172.16.8.190	172.16.8.1	DNS	71	Standard query 0x0512 HTTPS ntp.ssn.com
1915	17.727899	172.16.8.1	172.16.8.190	DNS	138	Standard query response 0x0512 HTTPS ntp.ssn.com CNAME www-ssn.com-a-0003-a.sedge.net CNAME a-0003-a.sedge.net
1916	17.727899	172.16.8.1	172.16.8.190	DNS	146	Standard query response 0x0ef1 A ntp.ssn.com CNAME www-ssn.com-a-0003-a.sedge.net CNAME a-0003-a.sedge.net A 204.79.197.203
1952	17.758437	172.16.8.190	172.16.8.1	DNS	71	Standard query 0x0f1d A ntp.ssn.com
1953	17.759553	172.16.8.1	172.16.8.190	DNS	146	Standard query response 0x0f1d A ntp.ssn.com CNAME www-ssn.com-a-0003-a.sedge.net CNAME a-0003-a.sedge.net A 204.79.197.203
2045	17.975412	172.16.8.190	172.16.8.1	DNS	87	Standard query 0x509f A img-s-snn.com.akamaized.net
2046	17.975632	172.16.8.190	172.16.8.1	DNS	87	Standard query 0x007f HTTPS img-s-snn.com.akamaized.net
2047	17.975632	172.16.8.190	172.16.8.1	DNS	84	Standard query 0x0ebd A sb.scorecardresearch.com
2048	17.975922	172.16.8.190	172.16.8.1	DNS	84	Standard query 0x0ee6 HTTPS sb.scorecardresearch.com
2049	17.976081	172.16.8.190	172.16.8.1	DNS	71	Standard query 0x0d70 A th.bing.com
2049	17.976164	172.16.8.190	172.16.8.1	DNS	71	Standard query 0x07be HTTPS th.bing.com
2051	17.976471	172.16.8.1	172.16.8.190	DNS	128	Standard query response 0x007f HTTPS img-s-snn.com.akamaized.net CNAME a1834.dscg2.akamai.net

Flow Graph output

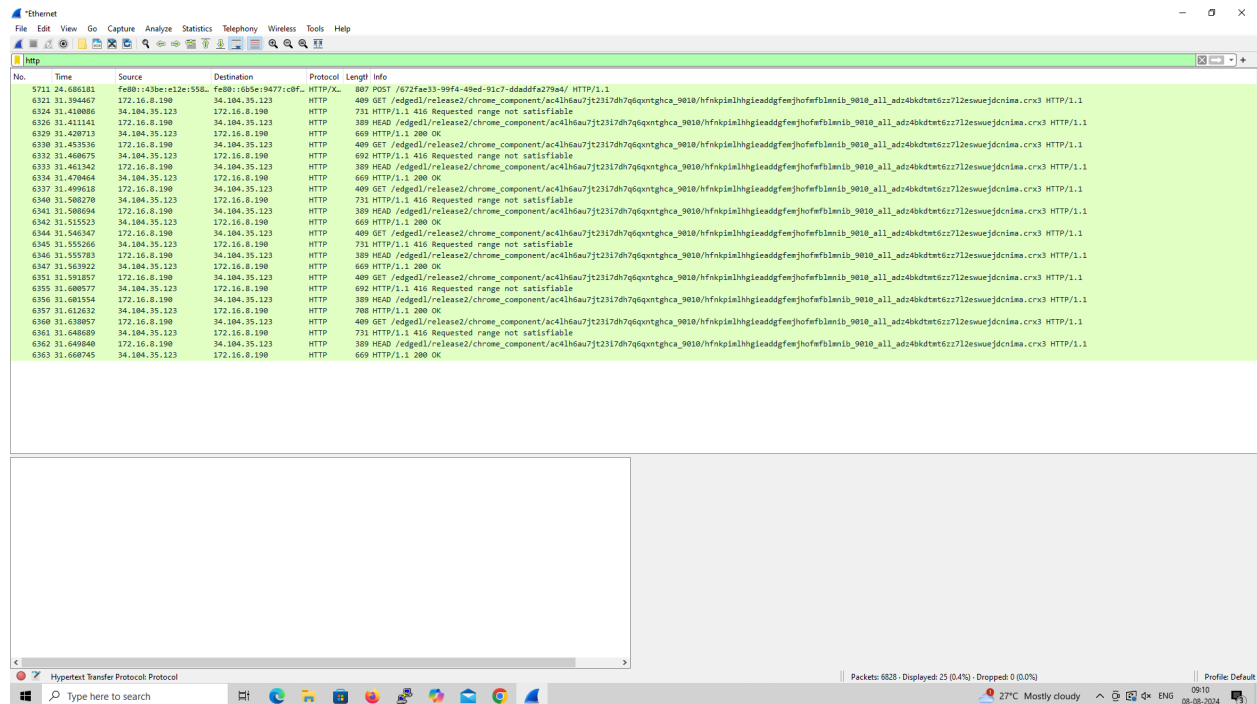


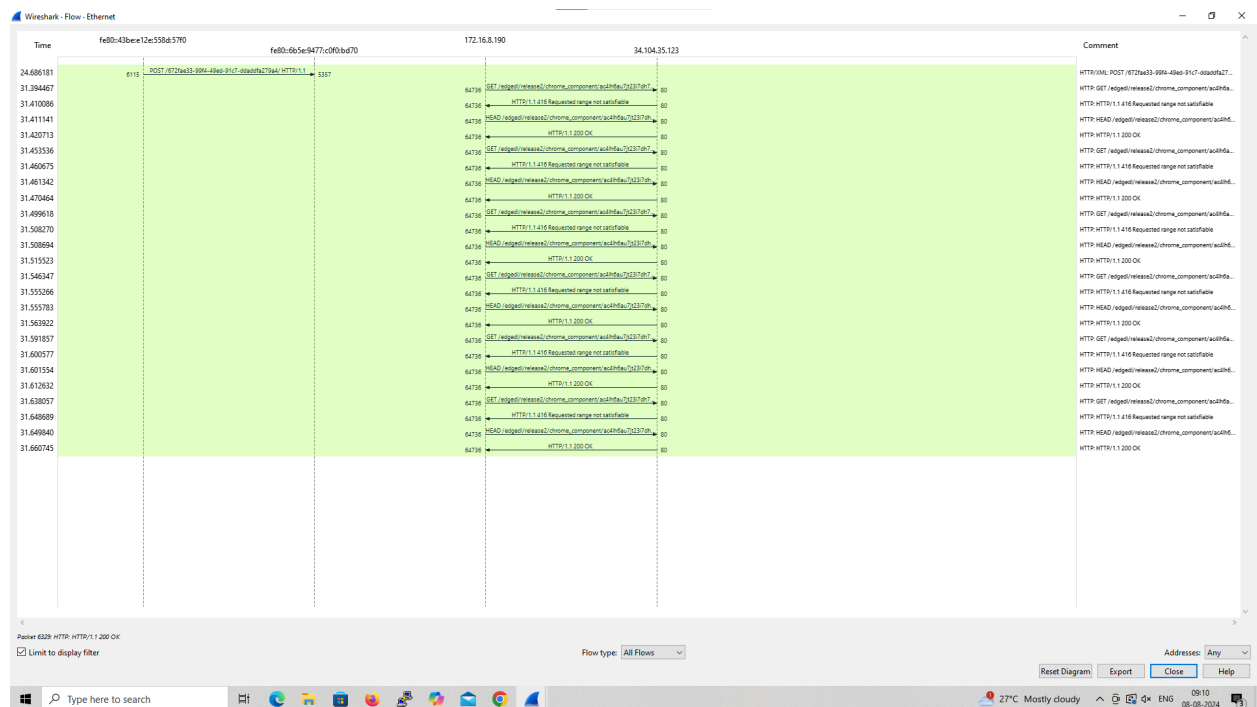
5.Create a Filter to display only HTTP packets and inspect the packets

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.

Output



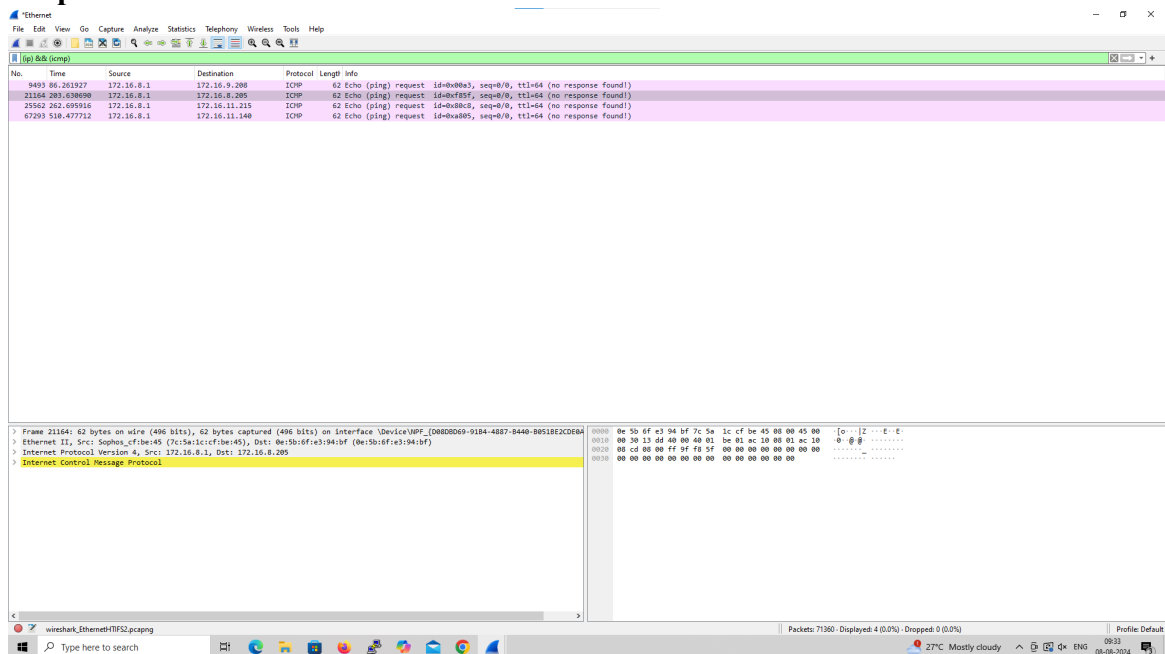


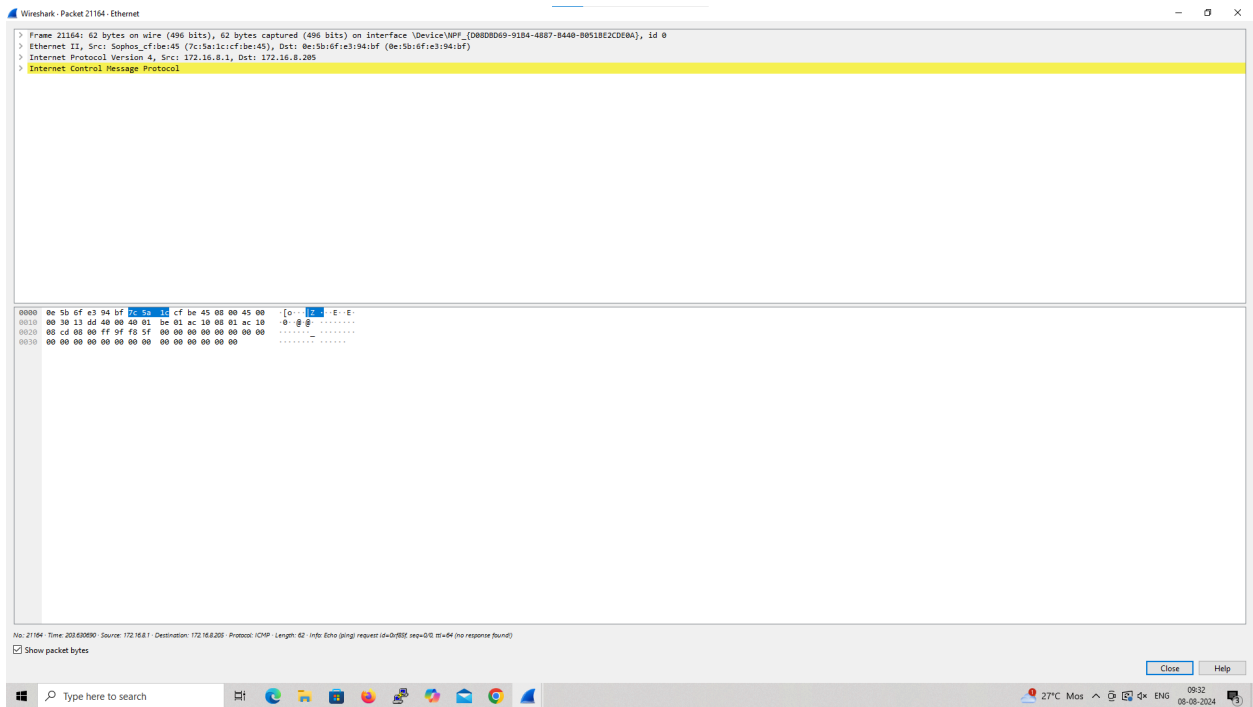
6. Create a Filter to display only IP/ICMP packets and inspect the packets.

Procedure

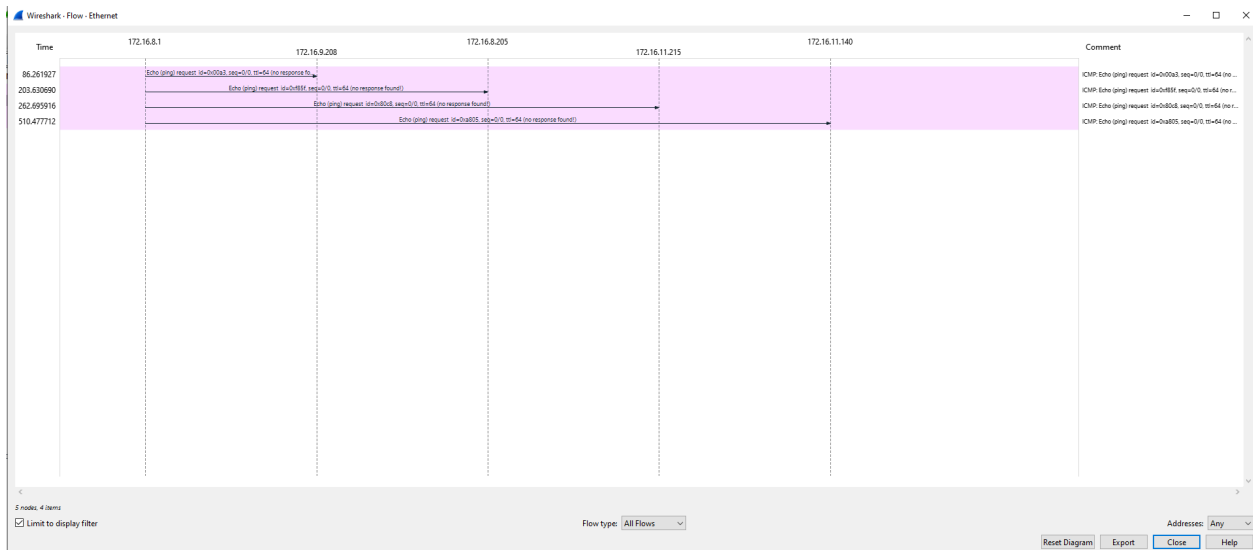
- ☐ Select Local Area Connection in Wireshark.
- ☐ Go to capture ☐ option
- ☐ Select stop capture automatically after 100 packets.
- ☐ Then click Start capture.
- ☐ Search ICMP/IP packets in search bar.
- ☐ Save the packets

Output





Flow Graph 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

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 various functions like opening files, saving, and capturing. The main window is divided into three panes:

- Packet List:** Shows a list of captured packets. The filter bar at the top is set to 'dhcp'. The list includes packets 549, 825, 5510, 7992, 7976, and 8211, all of which are DHCP requests or discoveries.
- Packet Details:** Shows the hierarchical structure of the selected packet (No. 549). It includes Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Dynamic Host Configuration Protocol (Request).
- Packet Bytes:** Shows the raw data of the selected packet in hexadecimal and ASCII format.

The status bar at the bottom indicates that 10136 packets were captured and 6 are currently displayed. The system clock shows 09:13 on 08-08-2024.

Wireshark - Packet 19046 - Ethernet

> Frame 19046: 364 bytes on wire (2912 bits), 364 bytes captured (2912 bits) on interface \Device\NPF_{D080B069-91B4-4887-B440-B051BE2CDE0A}, id 0
> Ethernet II, Src: AzureWaveTec_9f:8c:75 (10:60:38:9f:8c:75), 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 10 08 00 9f 8c 75 00 00 45 00  .....h B-ig-E-
0010  01 5e a7 e5 00 00 11 91 aa 00 00 00 00 ff ff  .....A.....
0020  ff ff 00 44 00 43 01 4a ff 97 01 01 00 24 21  ....D-C-J.....$!
0030  9f 7f 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0040  00 00 00 00 00 10 68 35 9f 8c 75 00 00 00 00  .....h B-ig-....
0050  00 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 00  .....
0070  00 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 00  .....
0090  00 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 00  .....
00b0  00 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 00  .....
00d0  00 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 00  .....
00f0  00 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 00  .....
0110  00 00 00 00 00 63 82 53 63 35 01 03 3d 07 01  ....C-ScS-....
0120  10 68 35 9f 8c 75 32 04 ac 18 00 72 0c 0f 4c 41  ..NB-g2--p-LA
0130  50 54 4f 50 2d 4f 39 4b 47 53 53 54 43 51 12 00  ..PTOP-09K-ESSTCQ
0140  00 00 4c 41 50 54 4f 50 2d 4f 39 4b 47 53 53 54  ..LAPTOP -09K05ST
0150  43 3c 05 4d 53 46 54 20 35 2e 30 37 0e 01 83 06  ..C-HOST- 5-87
0160  0f 1f 21 2b 2c 2e 2f 79 79 fc ff  ..-!+,,y-..
```

No: 19046 Time: 180.694333 Source: 0.0.0.0 Destination: 255.255.255.255 Protocol: DHCP Length: 364 Info: DHCP Request - Transaction ID 0x2421967

☒ Show packet bytes

Close Help

Windows taskbar: 27°C Mostly clear 09:21 08-08-2024