

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:

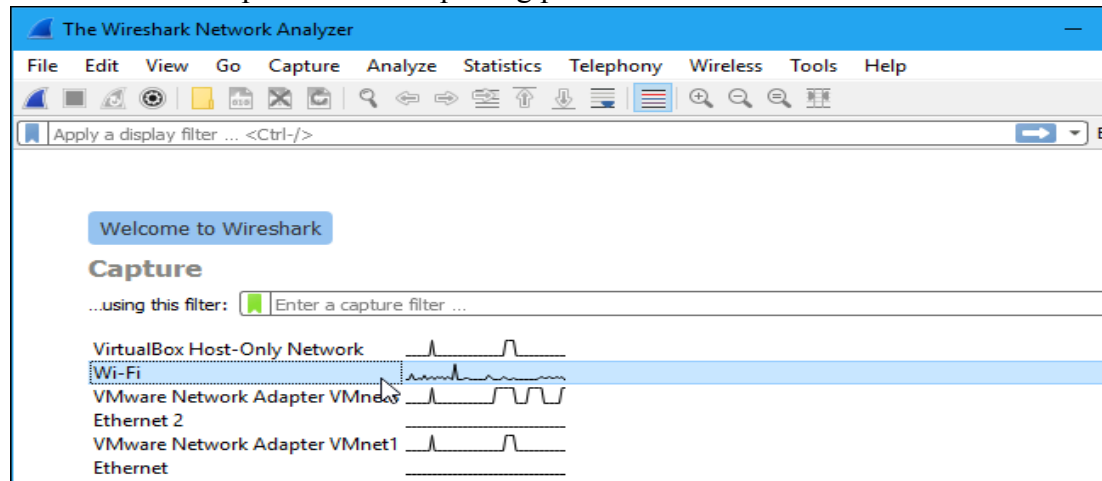
- Network administrators: troubleshoot network problems
- Network security engineers: examine security problems
- Developers: debug protocol implementations
- People: learn **network protocol internals**

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.

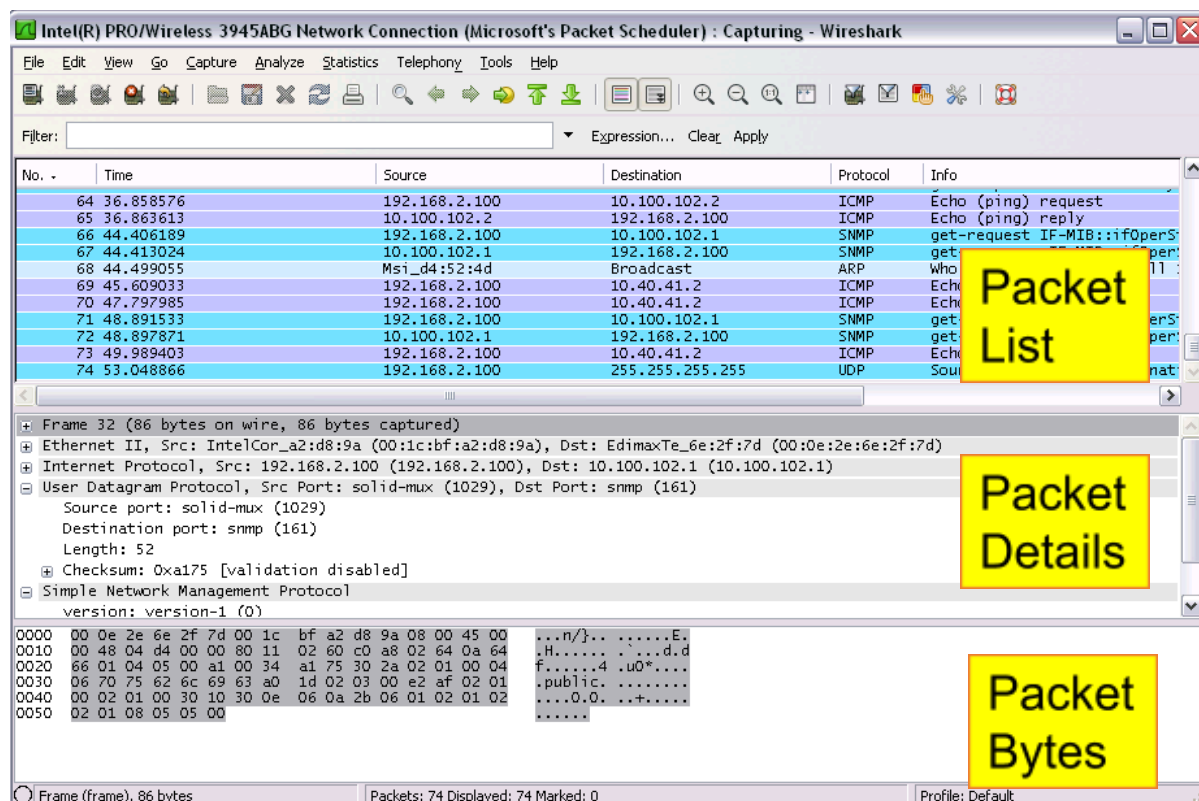
Capturing Packets

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.

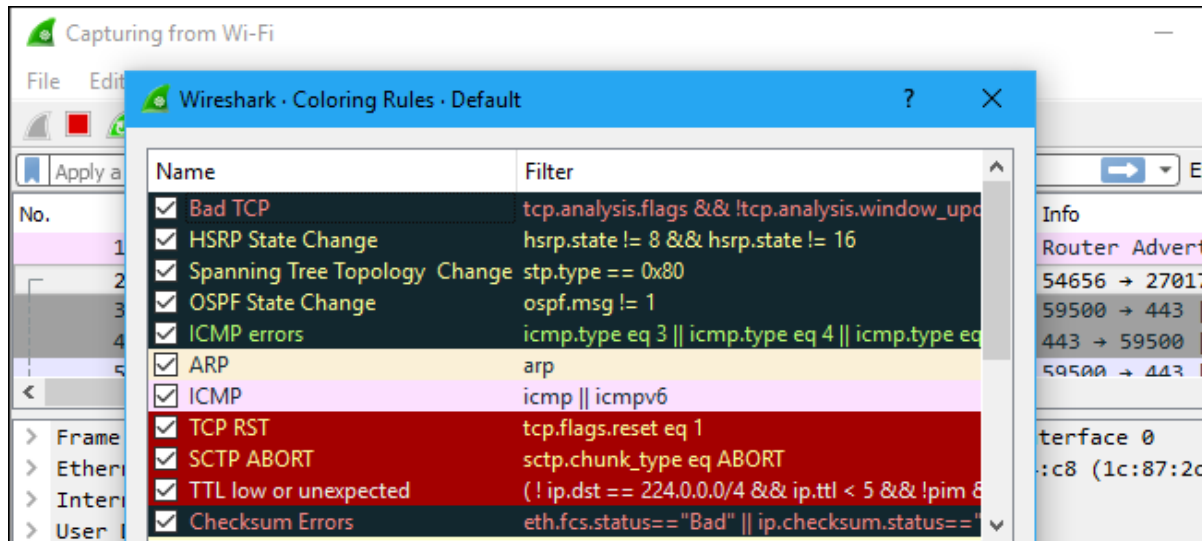
The “Packet Bytes” Pane

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.

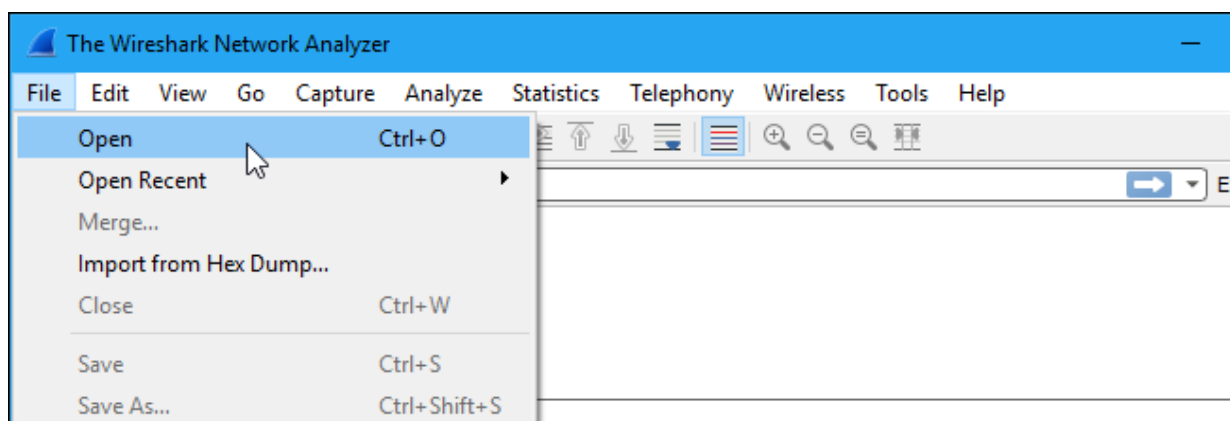
To view exactly what the color codes mean, click View > Coloring Rules. You can also customize and modify the coloring rules from here, if you like.



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.

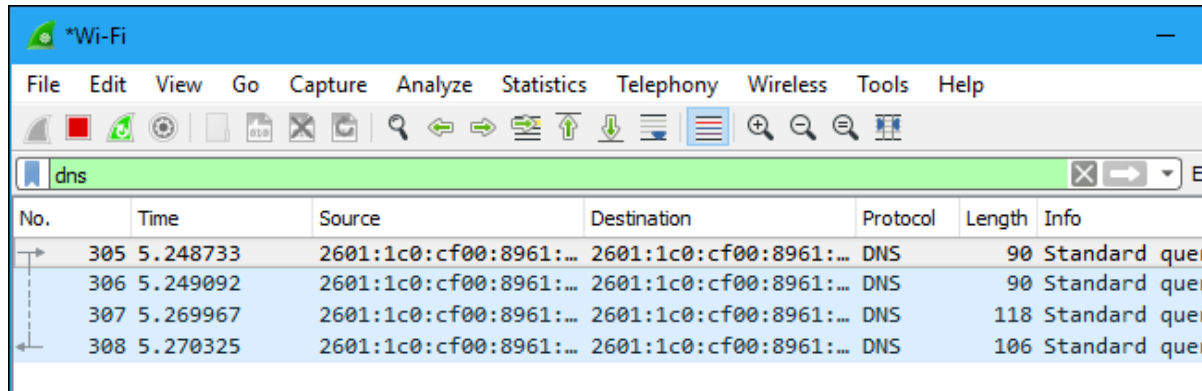


Filtering Packets

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

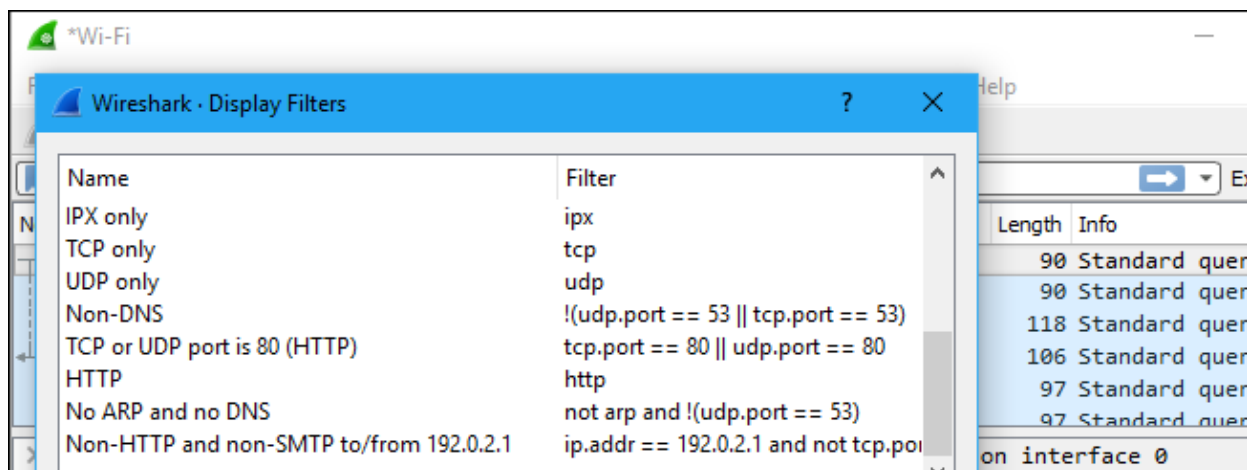
the traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark's filters come in.

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.



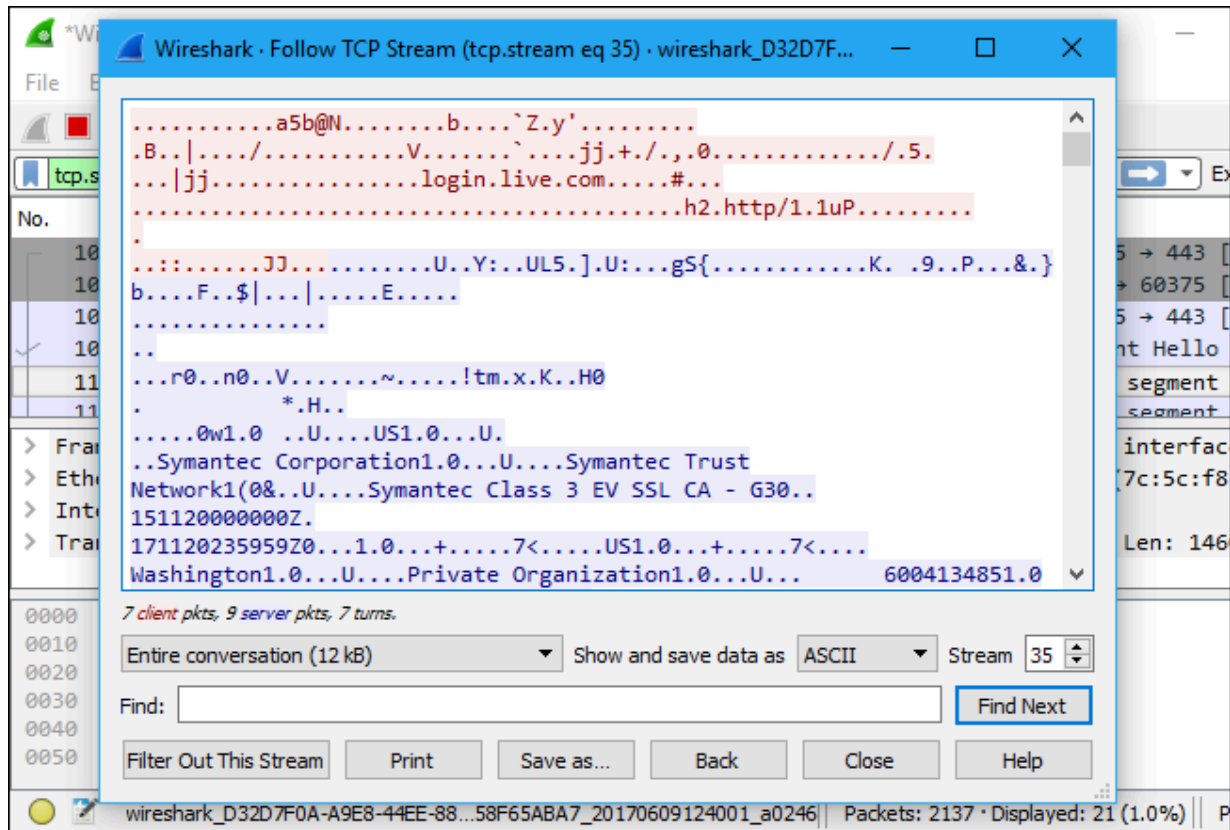
You can also click Analyze > Display Filters to choose a filter from among the default filters included in Wireshark. From here, you can add your own custom filters and save them to easily access them in the future.

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

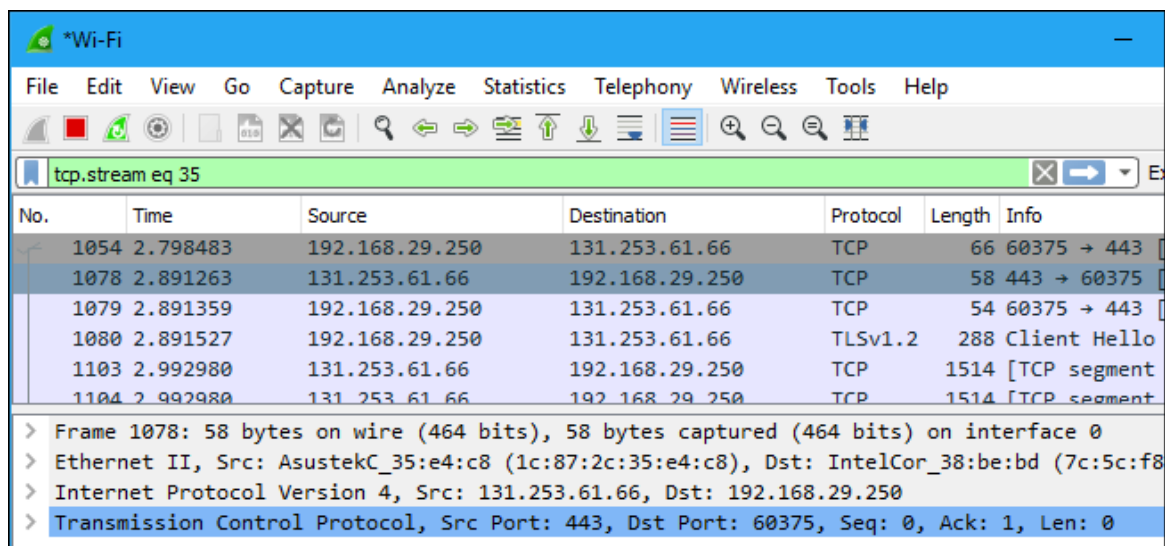


Another interesting thing you can do is right-click a packet and select Follow > TCP Stream.

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.



Inspecting Packets

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

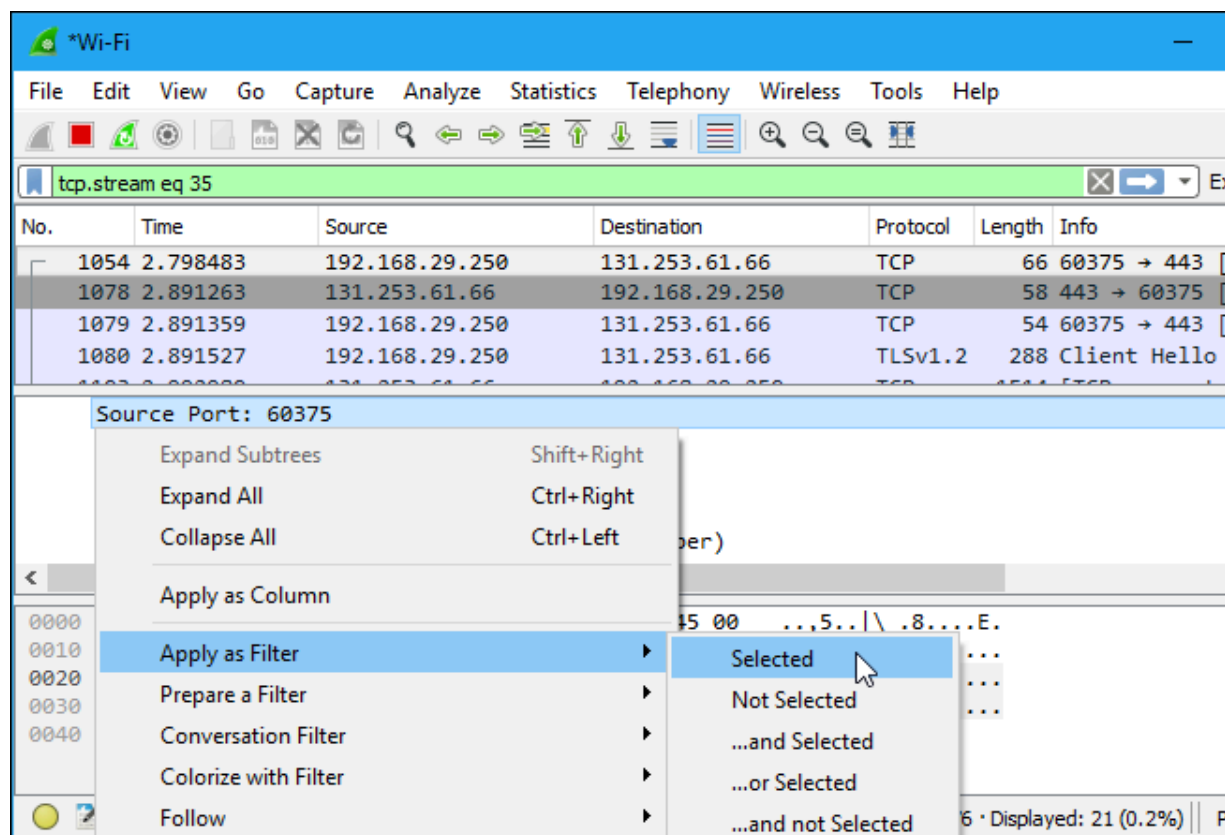
The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for packet capture and analysis. The packet capture filter is set to 'tcp.stream eq 35'. The packet list pane shows several packets, with packet 1054 selected. The details pane for packet 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 of the packet, with the first 40 bytes displayed in hexadecimal and ASCII. The ASCII column shows the text '...5..|\ .8....E.'.

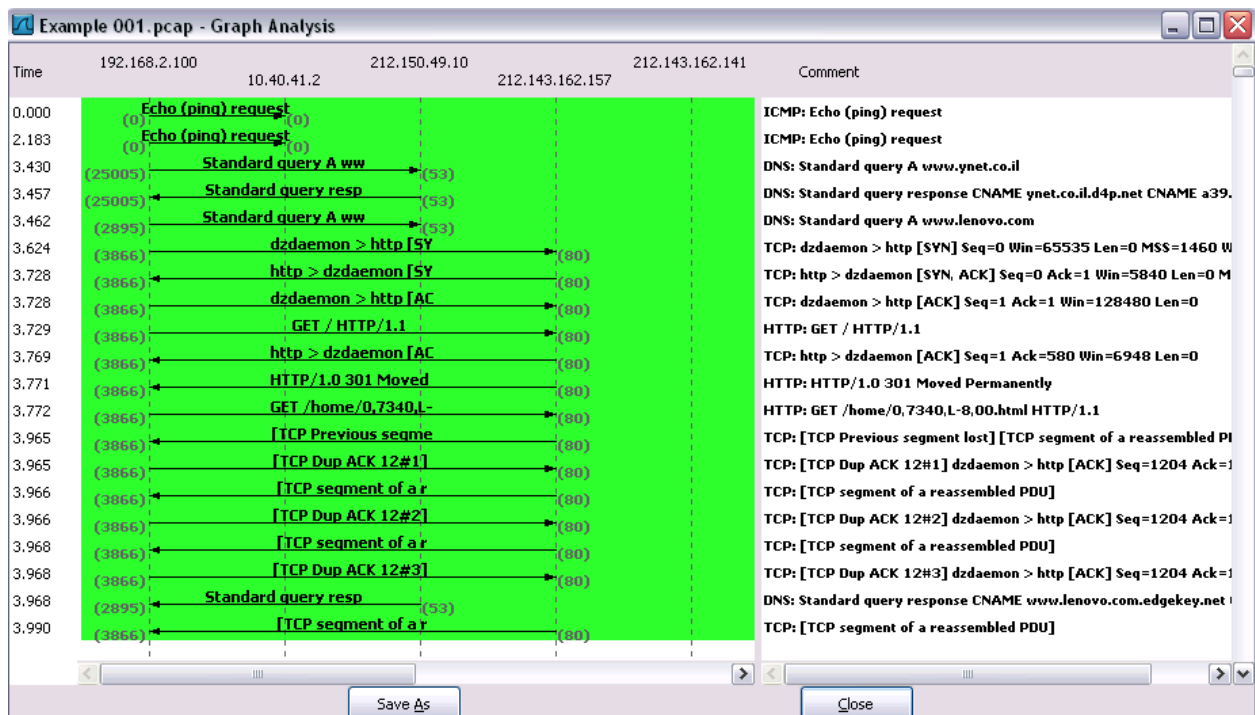
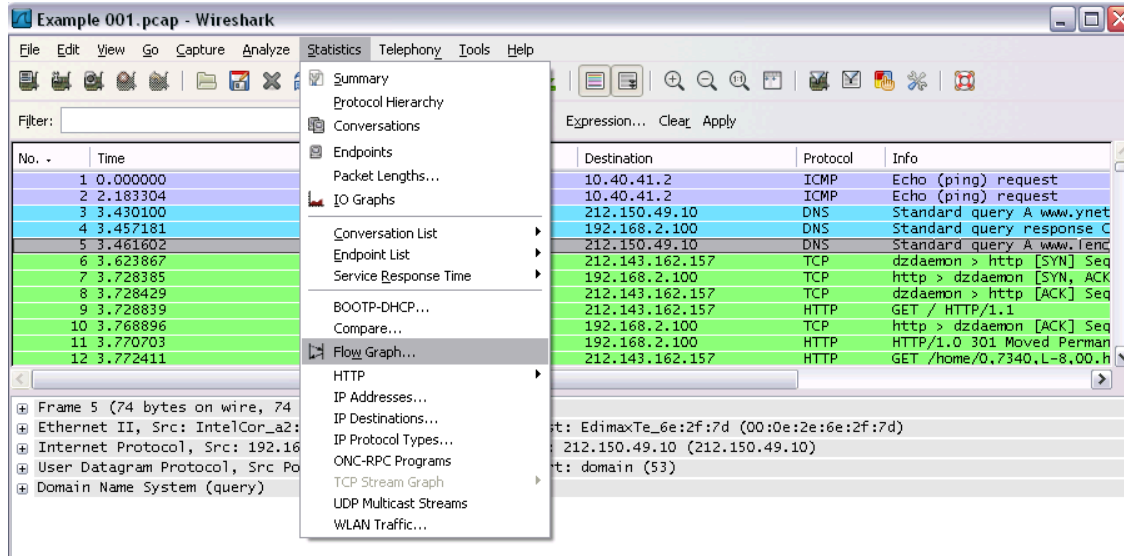
At the bottom of the interface, the status bar shows 'Encapsulation type (frame.encap_type)' and 'Packets: 8136 · Displayed: 21 (0.3%)'.

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

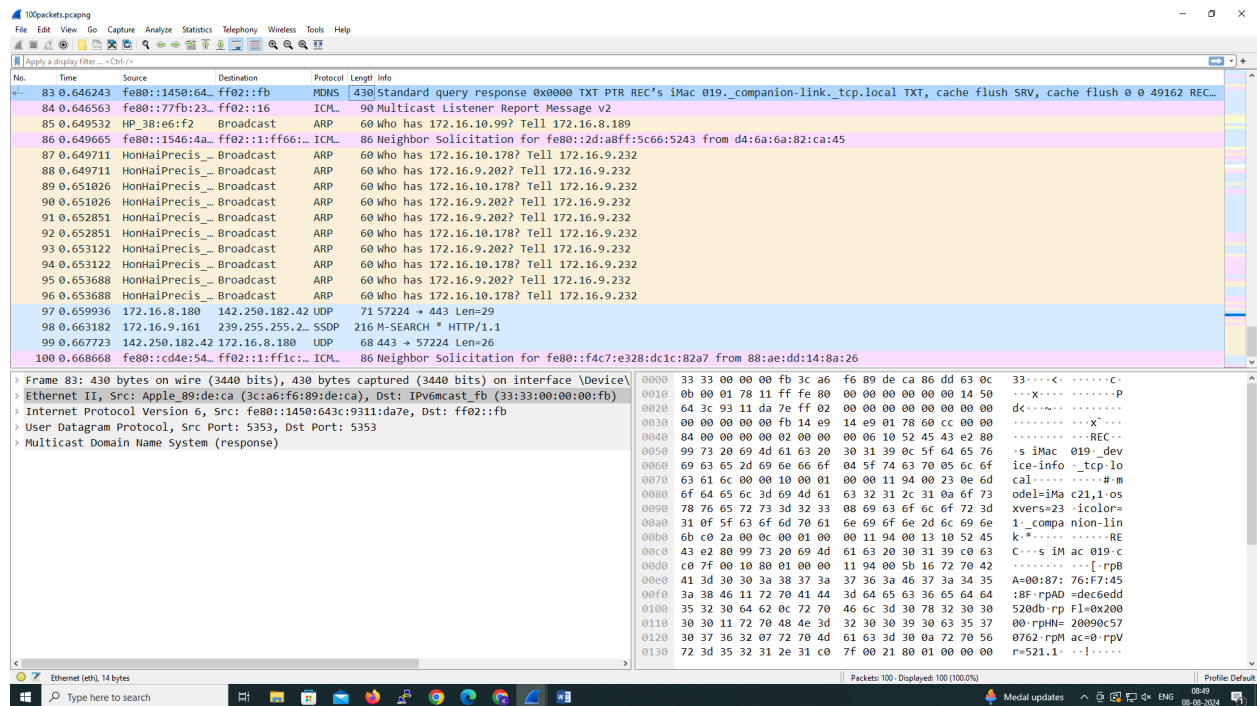
Exercises

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



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<input type="checkbox"/>Flow graph.
- ☐ Save the packets.

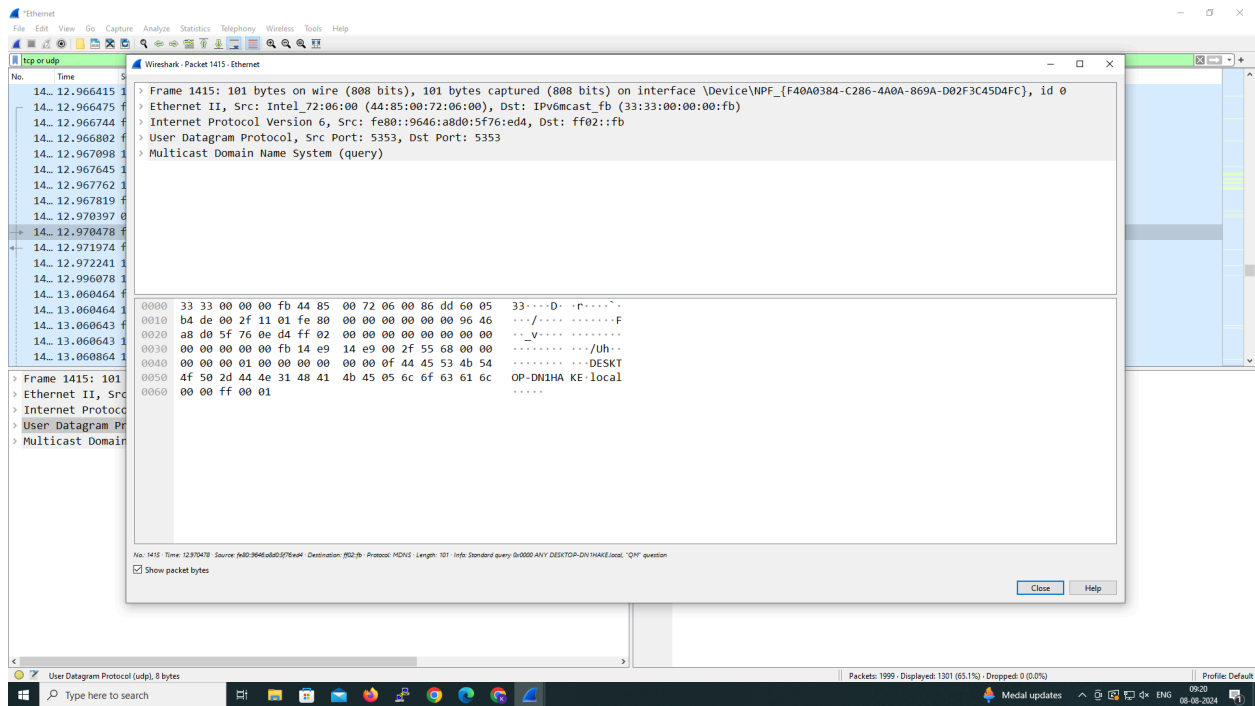
Output:

The image shows a Wireshark network traffic capture. The top pane displays a list of captured packets. The bottom pane shows the details of the selected packet (No. 1415), which is a Multicast Domain Name System (MDNS) query. The packet is 101 bytes long and is captured on the Ethernet II interface. The details pane shows the following information:

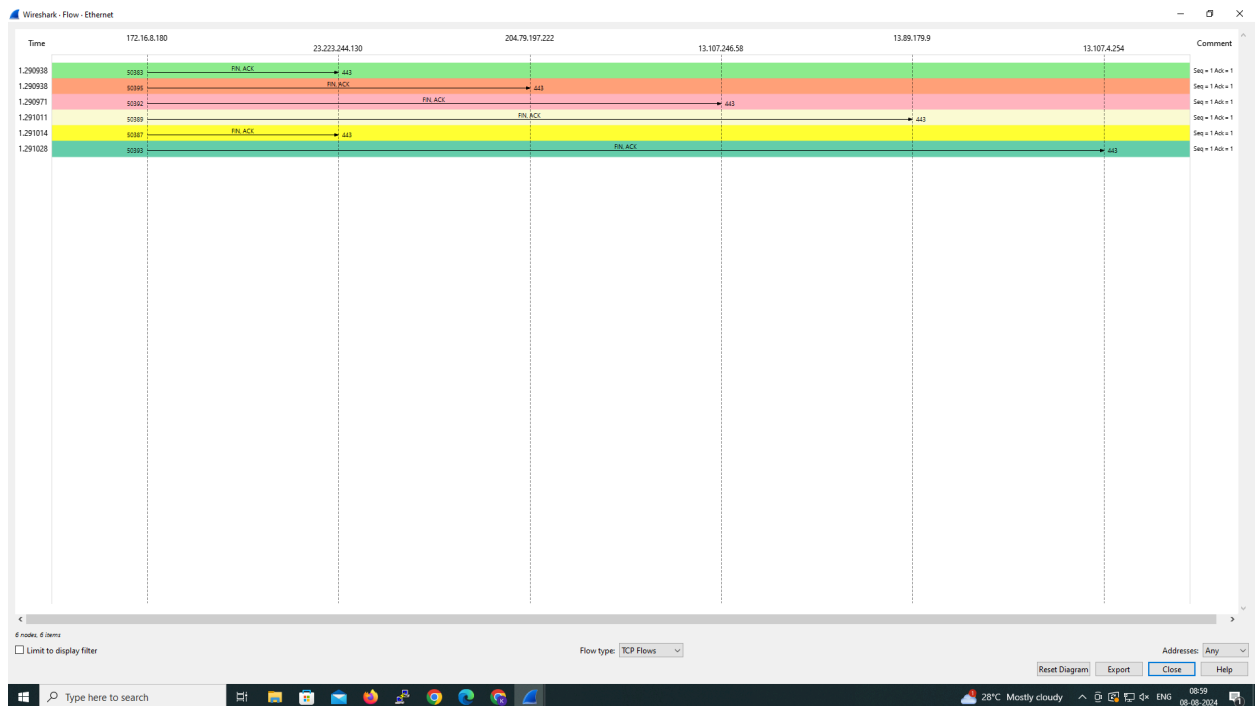
- Frame 1415: 101 bytes on wire (808 bits), 101 bytes captured (808 bits) on interface \Device\NPF{...}
- Ethernet II, Src: Intel_72:06:00 (44:85:00:72:06:00), Dst: IPv6mcast_fb (33:33:00:00:00:fb)
- Internet Protocol Version 6, Src: fe80::9646:a800:ff02::c, Dst: ff02::fb
- User Datagram Protocol, Src Port: 5353, Dst Port: 5353
- Multicast Domain Name System (query)

The packet data is displayed in hexadecimal and ASCII format. The ASCII column shows the following text:

```
33 33 00 00 00 fb 44 85 00 72 06 00 86 dd 60 05 33 33 00 00 00 fb 44 85 00 72 06 00 86 dd 60 05
b4 de 00 2f 11 01 fe 80 00 00 00 00 00 96 46 ..../.....F
a8 d0 5f 76 0e d4 ff 02 00 00 00 00 00 00 00 .._V.....
00 00 00 00 00 fb 11 01 fe 80 00 00 00 00 00 00 ....fe80::9646/a800:ff02::c
00 00 00 01 00 00 00 00 0f 44 45 53 4b 54 .....DESKT
4f 50 2d 44 4e 31 48 41 4b 45 05 6c 6f 63 61 6c OP-DN1HA KE-local
00 00 ff 00 01 .....
```



Flow Graph output

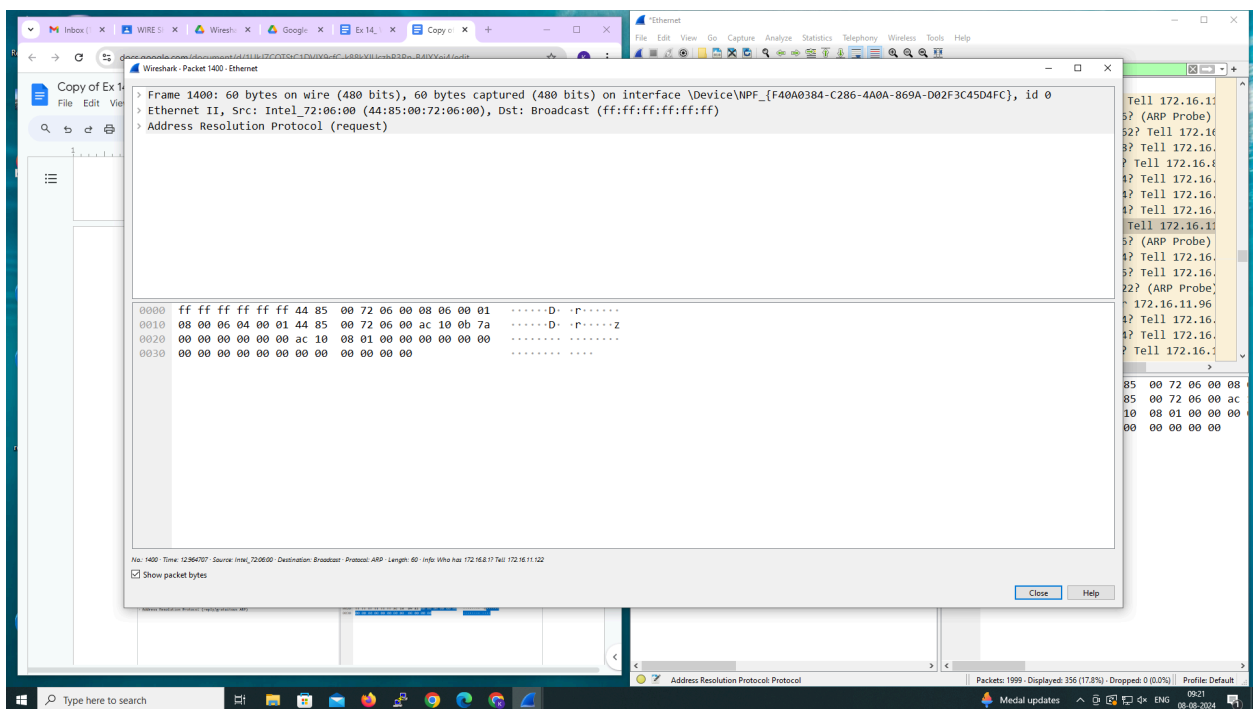


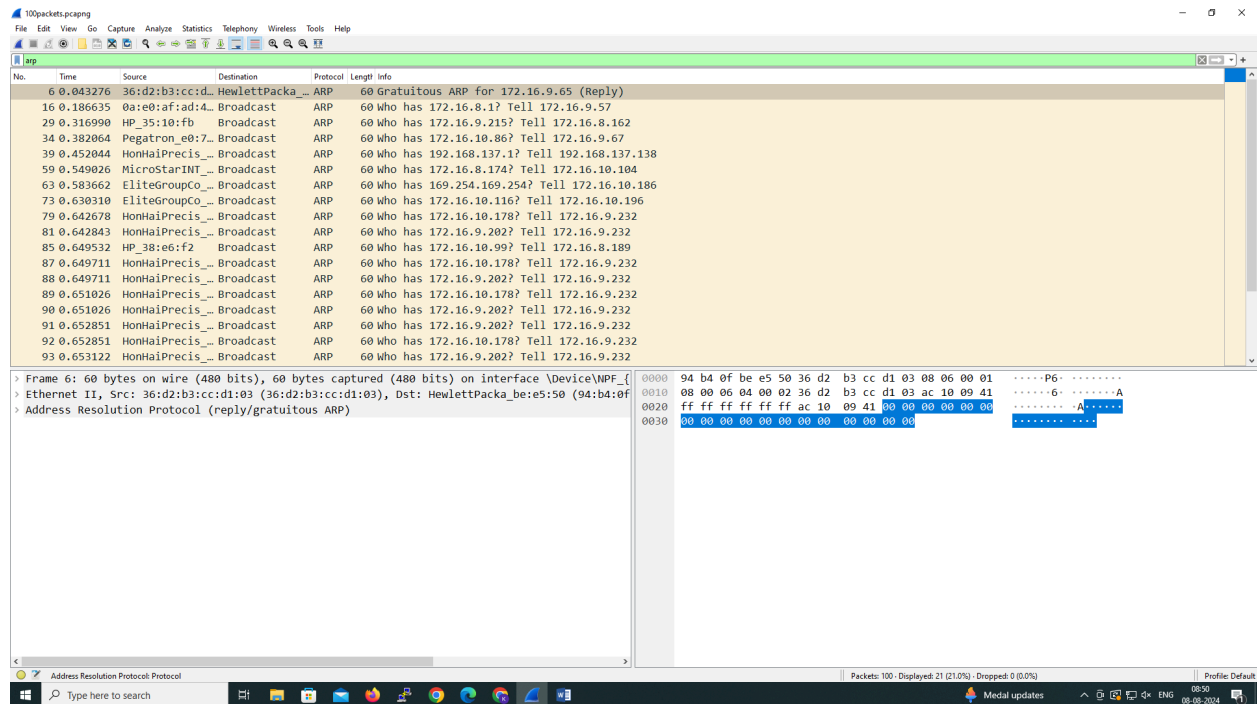
3. Create a Filter to display only ARP packets and inspect the packets.

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 Statistics ☐ Flow graph.
- ☐ Save the packets.

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

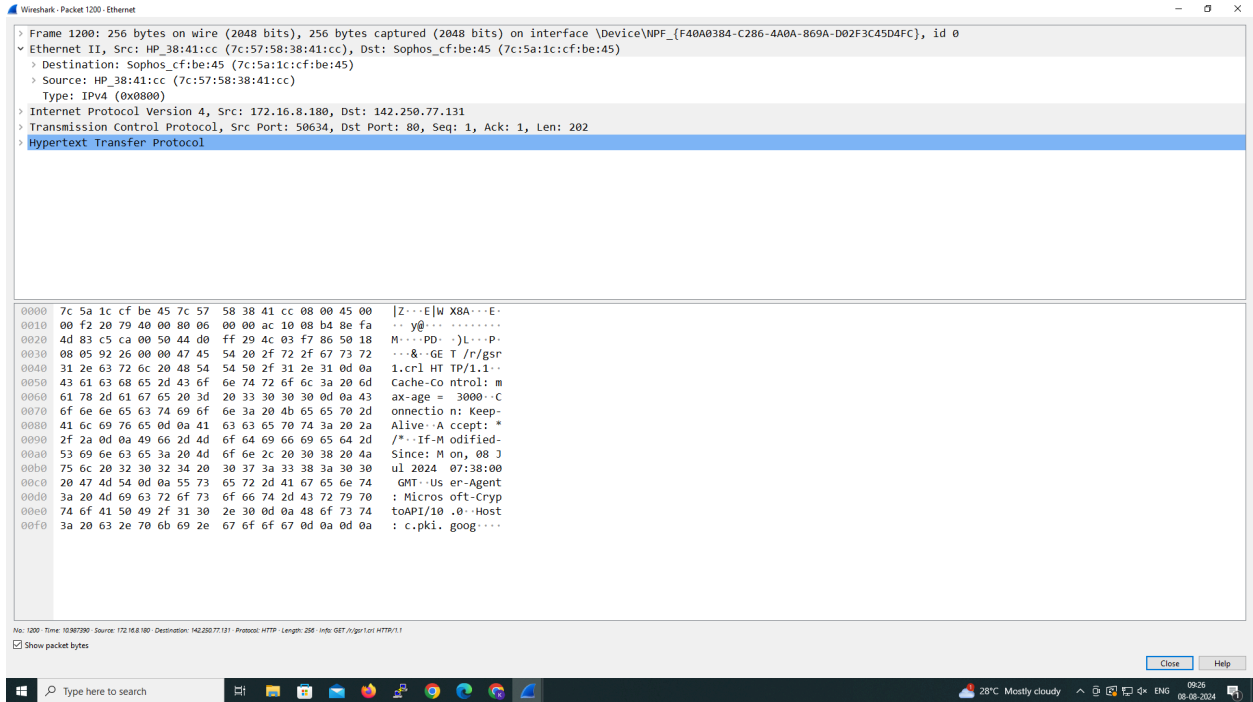
The screenshot displays the Wireshark interface with a network capture of HTTP traffic. The packet list on the left shows three captured packets:

No.	Time	Source	Destination	Protocol	Length	Info
36	0.102656	172.16.8.180	23.215.215.112	HTTP	445	GET /roots/dstrootcax3.p7c HTTP/1.1
71	0.225487	23.215.215.112	172.16.8.180	HTTP	382	HTTP/1.1 304 Not Modified
91	0.281038	172.16.8.180	23.47.228.163	HTTP	415	GET / HTTP/1.1

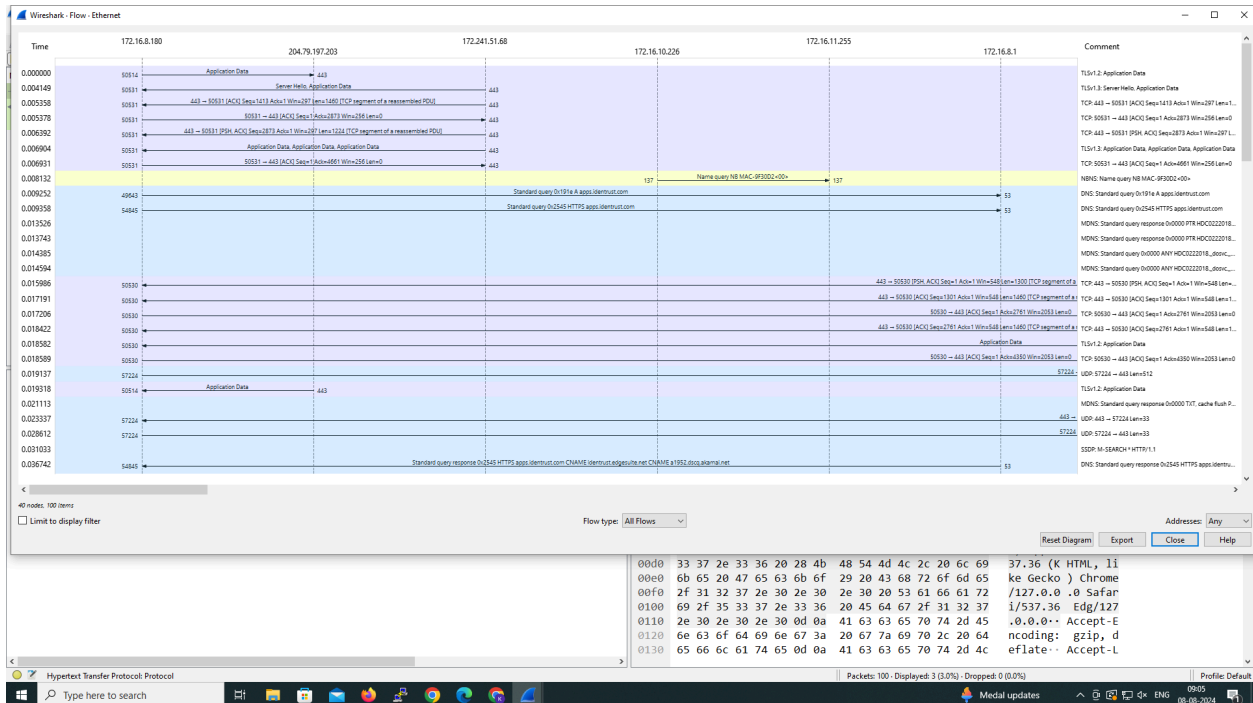
The packet details pane on the right shows the structure of the selected packet (No. 36):

- Frame 36: 445 bytes on wire (3560 bits), 445 bytes captured (3560 bits) on interface \Device\NPF...
- Ethernet II, Src: HP_38:41:cc (7c:57:58:38:41:cc), Dst: Sophos_cf:be:45 (7c:5a:1c:cf:be:45)
- Internet Protocol Version 4, Src: 172.16.8.180, Dst: 23.215.215.112
- Transmission Control Protocol, Src Port: 50533, Dst Port: 80, Seq: 1, Ack: 1, Len: 391
- Hypertext Transfer Protocol

The packet bytes pane on the right shows the raw data of the selected packet, including the HTTP request line and headers.



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

The image shows a Wireshark network traffic capture. The top pane displays a list of captured packets. The bottom pane shows the details of the selected packet (No. 28), which is an Internet Control Message Protocol (ICMP) packet. The packet is a Standard query response from 172.16.10.102 to 172.16.10.178, with a length of 106 bytes. The packet is fragmented into three parts, each 35 bytes long. The packet is captured on the Ethernet II interface, with source address 172.16.10.102 and destination address 172.16.10.178. The packet is captured on the Ethernet II interface, with source address 172.16.10.102 and destination address 172.16.10.178. The packet is captured on the Ethernet II interface, with source address 172.16.10.102 and destination address 172.16.10.178.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.11.220	224.77.77.77	UDP	148	12177 → 12177 Len=106
2	0.033847	172.16.11.137	239.255.255.2	SSDP	216	M-SEARCH * HTTP/1.1
4	0.052344	172.16.10.12	239.255.255.2	SSDP	217	M-SEARCH * HTTP/1.1
6	0.062369	172.16.10.64	239.255.255.2	UDP	698	65245 → 3702 Len=656
9	0.147285	172.16.10.8	239.255.255.2	SSDP	217	M-SEARCH * HTTP/1.1
10	0.171094	172.16.10.64	239.255.255.2	UDP	698	65245 → 3702 Len=656
12	0.213363	172.16.11.33	239.255.255.2	SSDP	217	M-SEARCH * HTTP/1.1
13	0.227872	172.16.11.33	239.255.255.2	SSDP	216	M-SEARCH * HTTP/1.1
16	0.283890	172.16.8.218	239.255.255.2	SSDP	217	M-SEARCH * HTTP/1.1
17	0.284027	172.16.8.218	239.255.255.2	SSDP	216	M-SEARCH * HTTP/1.1
19	0.292646	172.16.10.109	224.0.0.251	MDNS	93	Standard query 0x0000 ANY DESKTOP-G0LVE4J._dosvc._tcp.local, "QM" question
21	0.293150	172.16.10.102	224.0.0.251	MDNS	299	Standard query response 0x0000 SRV 0 0 7680 DESKTOP-G0LVE4J.local TXT A 172.16.10.102 AAAA fe80::233e:43aa:17dc:a750
23	0.293842	172.16.10.109	224.0.0.251	MDNS	96	Standard query 0x0000 ANY DESKTOP-G0LVE4J(1)._dosvc._tcp.local, "QM" question
25	0.295369	172.16.10.109	224.0.0.251	IPv4	15	Fragmented IP protocol (proto=UDP 17, off=0, ID=1194) [Reassembled in #28]
26	0.296600	172.16.10.109	224.0.0.251	IPv4	15	Fragmented IP protocol (proto=UDP 17, off=1480, ID=1194) [Reassembled in #28]
27	0.297835	172.16.10.109	224.0.0.251	IPv4	15	Fragmented IP protocol (proto=UDP 17, off=2960, ID=1194) [Reassembled in #28]
28	0.299067	172.16.10.109	224.0.0.251	MDNS	15	Standard query response 0x0000 SRV 0 0 7680 DESKTOP-G0LVE4J(2)._dosvc._tcp.local PTR DESKTOP-G0LVE4J(3...
33	0.304010	172.16.10.178	224.0.0.22	IGMP	60	Membership Report / Leave group 224.0.0.113

Frame 1: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface \Device\NPF{...} Ethernet II, Src: ASUSTekCOMPU_94:c8:8c (fc:34:97:94:c8:8c), Dst: IPv4mcast_4d:4d:4d (01:00:5e:00:00:00) Internet Protocol Version 4, Src: 172.16.11.220, Dst: 224.77.77.77 User Datagram Protocol, Src Port: 12177, Dst Port: 12177 Data (106 bytes)

0000 01 00 5e 4d 4d 4d fc 34 97 94 c8 8c 08 0e 45 00 ...MM1-4E:
0010 00 86 ca 03 00 00 01 11 09 dd ac 10 0b dc e0 4dM
0020 4d 4d 2f 91 2f 91 00 72 44 46 3c 41 53 55 53 5f MM/-...P DF<ASUS_
0030 41 52 4d 4f 55 52 59 5f 43 52 41 54 45 3e 3c 4c ARMOURY_ CRATE><L
0040 41 4e 20 50 6f 72 74 3d 22 31 32 31 37 37 22 20 AN Port= "12177"
0050 43 75 73 49 44 3d 22 31 34 30 38 32 38 41 44 2d CUSID="1 40828AD-
0060 33 31 34 45 2d 34 45 37 38 2d 39 41 43 31 2d 35 314E-AE7 8-9AC1-5
0070 37 32 43 45 36 39 44 44 32 33 38 22 20 2f 3e 3c 72CE6900 238" /><
0080 2f 41 53 55 53 5f 41 52 4d 4f 55 52 59 5f 43 52 /ASUS_AR MOURY_CR
0090 41 54 45 3e ATE>

Wireshark - Packet 1193 - Ethernet

> Frame 1193: 375 bytes on wire (3000 bits), 375 bytes captured (3000 bits) on interface \Device\NPF_{F40A0384-C286-4A0A-869A-D02F3C45D4FC}, id 0

> Ethernet II, Src: Sophos_cf:be:45 (7c:5a:1c:cf:be:45), Dst: HP_38:41:cc (7c:57:58:38:41:cc)

> Destination: HP_38:41:cc (7c:57:58:38:41:cc)

> Source: Sophos_cf:be:45 (7c:5a:1c:cf:be:45)

Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 23.47.228.163, Dst: 172.16.8.100

> Transmission Control Protocol, Src Port: 80, Dst Port: 50633, Seq: 1, Ack: 228, Len: 321

> Hypertext Transfer Protocol

0000 7c 57 58 38 41 cc 7c 5a 1c cf be 45 00 00 45 00 |WX8A-|Z...E...E...
0010 01 69 5d 05 40 00 00 06 2b f3 17 2f e4 a3 ac 10 |i|@.@. +.../....
0020 08 b4 00 50 c5 c9 2b 6a 50 52 aa be eb c5 50 18 |...P...+j PR...P...
0030 00 ed 65 9f 00 00 48 54 54 50 2f 31 2e 31 20 33 |...e...HT TP/1.1 3
0040 30 34 20 4e 6f 74 20 4d 6f 64 69 66 69 65 64 0d |0d Not Modified-
0050 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 |Content-Type: a
0060 70 70 6c 69 63 61 74 69 6f 6e 2f 70 6b 69 78 2d |pplicati on/pkix-
0070 63 72 6c 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 |crl- Las t-Modifi
0080 65 64 3a 20 4d 6f 6e 2c 20 31 32 20 46 65 62 20 |ed: Mon, 12 Feb
0090 32 30 32 3a 20 32 32 3a 30 37 3a 32 37 20 47 4d |2024 22: 07:27 GM
00a0 54 0d 0a 45 54 61 67 3a 20 22 36 35 63 61 39 36 |T-ETag: "65Ca96
00b0 39 66 2d 32 63 64 2d 0d 0a 43 61 63 68 65 2d 43 |9f-2cd"- Cache-C
00c0 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d 61 67 65 3d |ontrol: max-age=
00d0 33 36 30 30 0d 0a 45 78 70 69 72 65 73 3a 20 54 |3600-Expires: T
00e0 68 75 2c 20 30 38 20 41 75 67 20 32 30 32 3a 20 |hu, 08 Aug 2024
00f0 30 34 3a 3a 36 3a 30 37 20 47 4d 54 0d 0a 44 61 |04:46:07 GMT-da
0100 74 65 3a 20 54 68 75 2c 20 30 38 20 41 75 67 20 |te: Thu, 08 Aug
0110 32 30 32 3a 20 30 33 3a 3a 36 3a 30 37 20 47 4d |2024 03: 46:07 GM
0120 54 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 |T-Conte nt-Lengt
0130 68 3a 20 30 0d 0a 56 69 61 3a 20 48 54 54 50 2f |h: 0-Vi a: HTTP/
0140 31 2e 31 20 66 6f 72 77 61 72 64 2e 68 74 74 70 |1.1 forw ard.http
0150 2e 70 72 6f 78 79 3a 33 31 32 38 0d 0a 43 6f 6e |.proxy:3 128-Con

No: 1193 Time: 10.879004 Source: 23.47.228.163 Destination: 172.16.8.100 Protocol: HTTP Length: 375 Info: HTTP/1.1 304 Not Modified

Show packet bytes

Close Help

Flow Graph output

Wireshark - Flow - Ethernet

Time 172.16.11.220 224.71.71.77 172.16.11.137 239.255.255.250 RealtekSemic_A2beb9 Broadcast Comment

0.318333 IGMPv3 Membership Report / Leave group 224.0.0.113
0.318400 ICMPv6 Multicast Listener Report Message v2
0.318497 IGMPv3 Membership Report / Join group 224.0.0.113 for a...
0.318508 IGMPv3 Membership Report / Join group 224.0.0.113 for a...
0.318555 ICMPv6 Multicast Listener Report Message v2
0.319026 MDNS Standard query response 0x0000 SRV 0 0 7860 DES...
0.320033 IPv6 IPv6 Fragment (off=1488 memory idem=0x00003d m...
0.322080 IPv6 IPv6 Fragment (off=1488 memory idem=0x00003d m...
0.322299 SSDP M-SEARCH * HTTP/1.1
0.322345 IGMPv3 Membership Report / Leave group 224.0.0.113
0.322405 ICMPv6 Multicast Listener Report Message v2
0.323638 IPv6 IPv6 Fragment (off=2884 memory idem=0x00003d m...
0.324679 MDNS Standard query response 0x0000 SRV 0 0 7860 DES...
0.324788 MDNS Standard query 0x0000 ANY DESKTOP-020V6A...
0.324881 MDNS Standard query 0x0000 ANY DESKTOP-020V6A...
0.326159 IPv6 Fragmented IP protocol (proto=UDP 17 off=0, len=118...
0.326205 IGMPv3 Membership Report / Join group 224.0.0.113 for a...
0.326270 ICMPv6 Multicast Listener Report Message v2
0.327531 IPv6 Fragmented IP protocol (proto=UDP 17 off=1480, len...
0.328762 IPv6 Fragmented IP protocol (proto=UDP 17 off=2860, len...
0.329551 MDNS Standard query response 0x0000 SRV 0 0 7860 DES...
0.329637 IGMPv3 Membership Report / Leave group 224.0.0.113
0.329686 ICMPv6 Multicast Listener Report Message v2
0.329746 IGMPv3 Membership Report / Leave group 224.0.0.113
0.329839 ICMPv6 Multicast Listener Report Message v2
0.329906 IGMPv3 Membership Report / Join group 224.0.0.113 for a...
0.329997 ICMPv6 Multicast Listener Report Message v2
0.330261 MDNS Standard query 0x0000 PTR _alljyn_._ldns.local. "Q...
0.330502 MDNS Standard query 0x0000 PTR _alljyn_._ldns.local. "Q...
0.330766 MDNS Standard query 0x0000 PTR _alljyn_._ldns.local. "Q...
0.331007 MDNS Standard query 0x0000 PTR _alljyn_._ldns.local. "Q...
0.331272 MDNS Standard query 0x0000 PTR _alljyn_._ldns.local. "Q...
0.331336 MDNS Standard query 0x0000 PTR _alljyn_._ldns.local. "Q...
0.331602 ICMPv6 Multicast Listener Report Message v2
0.331793 SSDP M-SEARCH * HTTP/1.1
0.333046 IPv6 IPv6 Fragment (off=0 memory idem=0x00003d m...

Packet 70 IPv6 Fragmented IP protocol (proto=UDP 17 off=0, len=118) (Reassembled in #70)

Limit to display filter

Flow type: All Flows

Addresses: Any

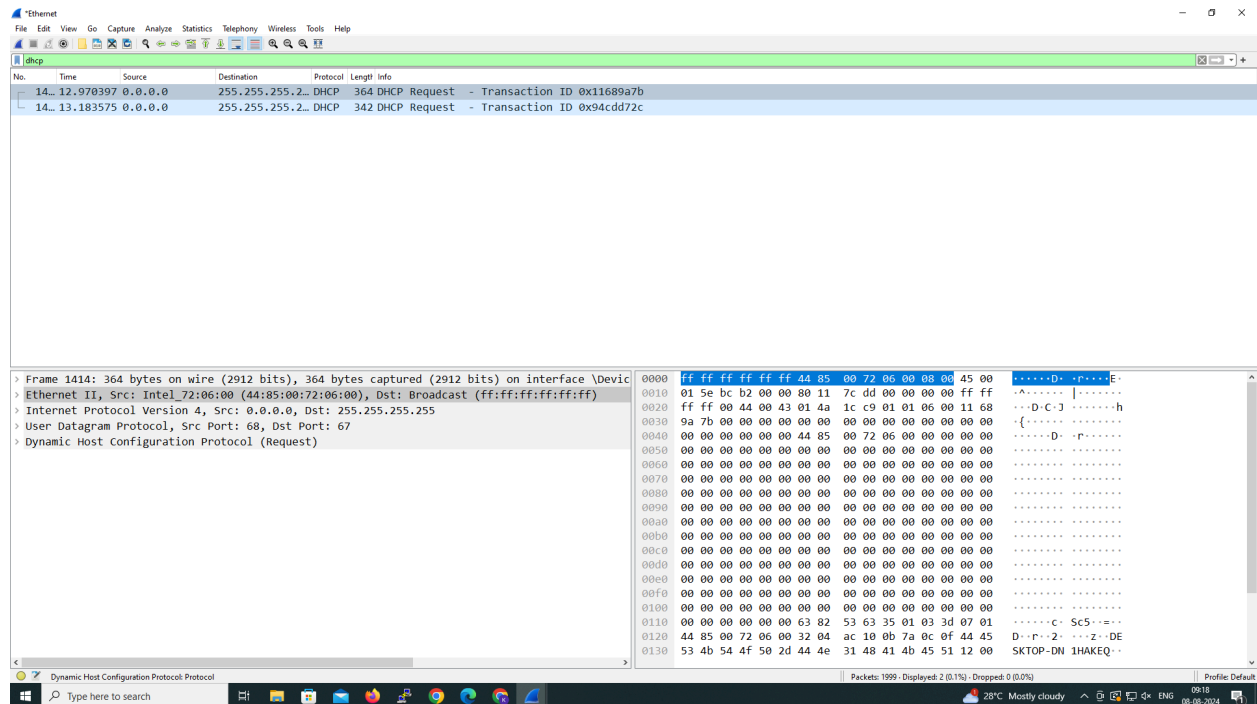
Reset Diagram Export Close Help

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



Wireshark - Packet 1479 - Ethernet

> Frame 1479: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{F40A0384-C286-4A0A-869A-D02F3C45D4FC}, id 0

▼ Ethernet II, Src: Intel_85:d3:6f (4c:5f:70:85:d3:6f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Destination: Broadcast (ff:ff:ff:ff:ff:ff)> Source: Intel_85:d3:6f (4c:5f:70:85:d3:6f)> Type: IPv4 (0x0800)

> 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 4c 5f	70 85 d3 6f 08 00 45 00L_p...E..
0010	01 48 16 ea 00 00 00 11	22 bc 00 00 00 00 ff ff	.H.....".....
0020	ff ff 00 44 00 00 43 01	34 d3 40 01 01 06 00 94	...D.C.4_@.....
0030	d7 2c 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.,.....
0040	00 00 00 00 00 4c 5f	70 85 d3 6f 00 00 00 00L_p...E..
0050	00 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 00
0070	00 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 00
0090	00 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 00
00b0	00 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 00
00d0	00 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 00
00f0	00 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 00
0110	00 00 00 00 00 00 63 82	53 63 35 01 03 3d 07 01C_ Sc5...=...
0120	4c 5f 70 85 d3 6f 32 04	ac 10 0b 60 0c 04 4f 4d	L_p...o2_ ...OM
0130	45 4e 51 07 00 00 00 4f	4d 45 4e 3c 08 4d 53 46	ENQ...O MENC<MSF
0140	54 20 35 2e 30 37 0e 01	03 06 0f 1f 21 2b 2c 2e	T 5.07... ..!+,,
0150	2f 77 79 f9 fc ff		/wy...

No: 1479 Time: 13.188079 Source: 0.0.0.0 Destination: 255.255.255.255 Protocol: DHCP Length: 342 Info: DHCP Request - Transaction ID 0x04a072c

☒ Show packet bytes

Close

Help

Windows Start Button

Type here to search

Taskbar Icons: File Explorer, Calendar, Mail, Photos, Edge, Chrome, etc.

System Tray: Athletics, Network, Volume, Date/Time (09:27 08-08-2024)