

Ex No: 14A
Name:E.MONIKA

Date:13.08.2024

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:

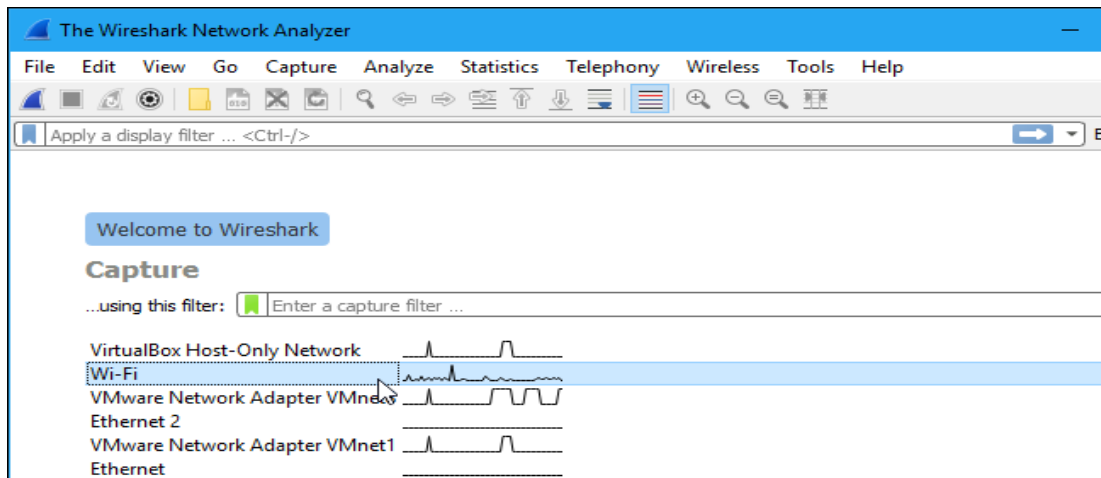
- Network administrators: troubleshoot network problems
- Network security engineers: examine security problems
- Developers: debug protocol implementations
- People: learn **network protocol internals**

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.

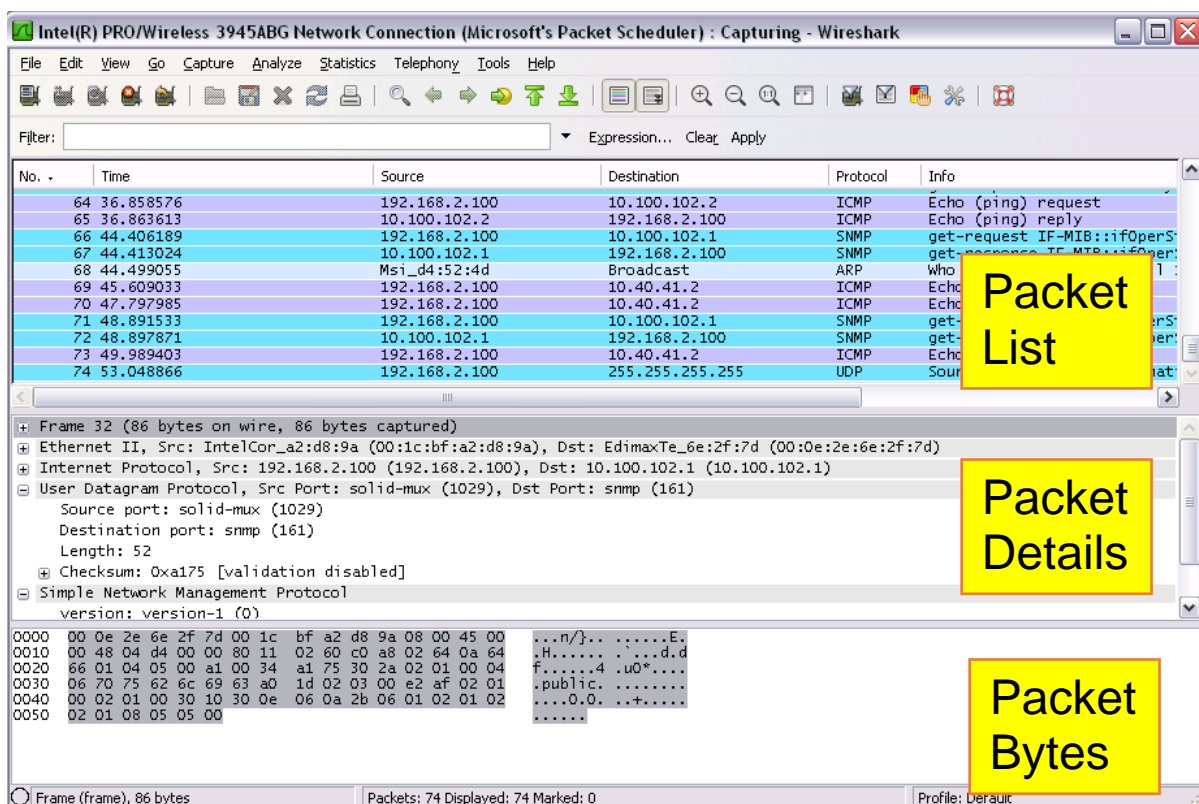
Capturing Packets

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.

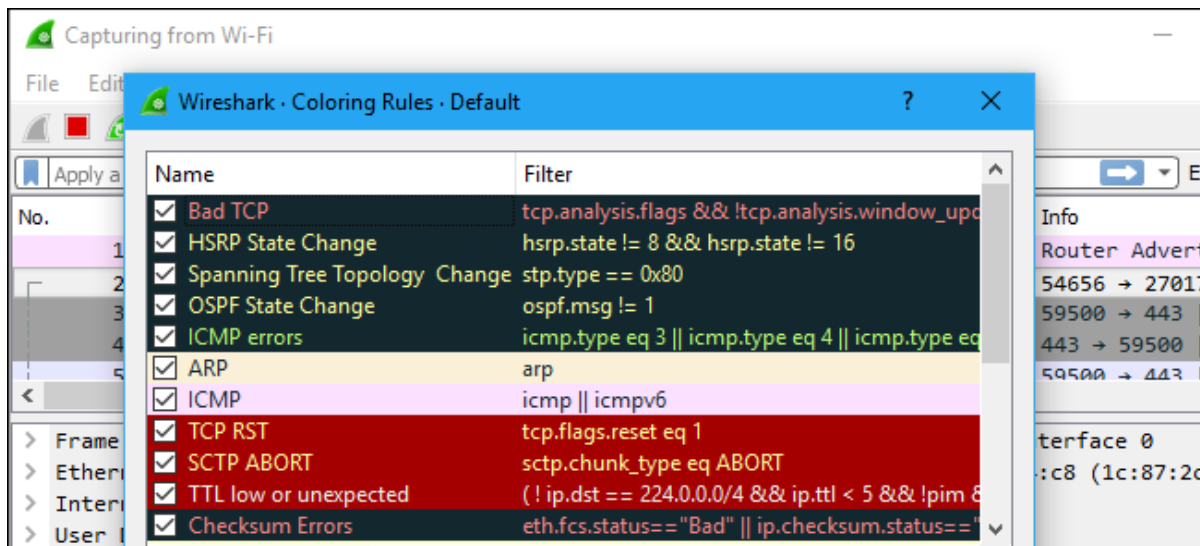
The “Packet Bytes” Pane

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.

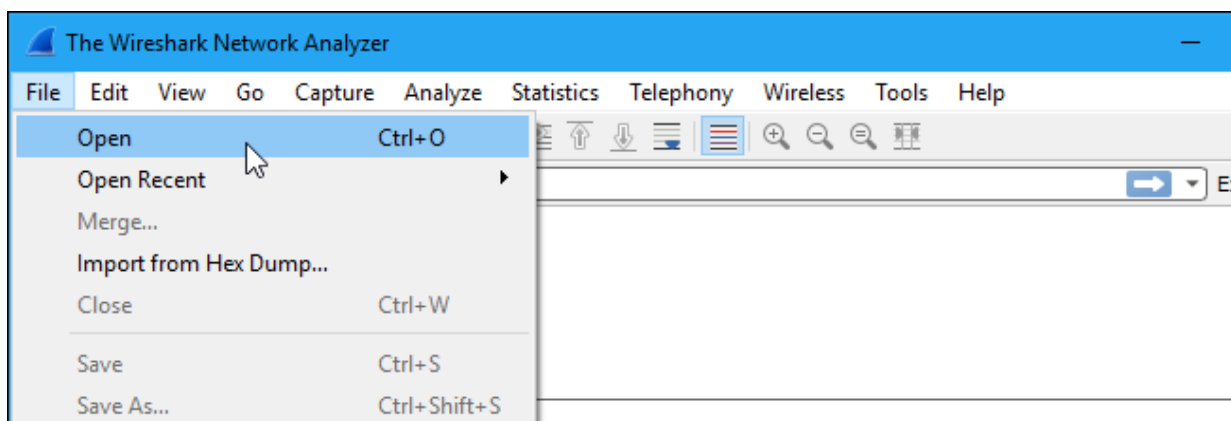
To view exactly what the color codes mean, click View > Coloring Rules. You can also customize and modify the coloring rules from here, if you like.



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.

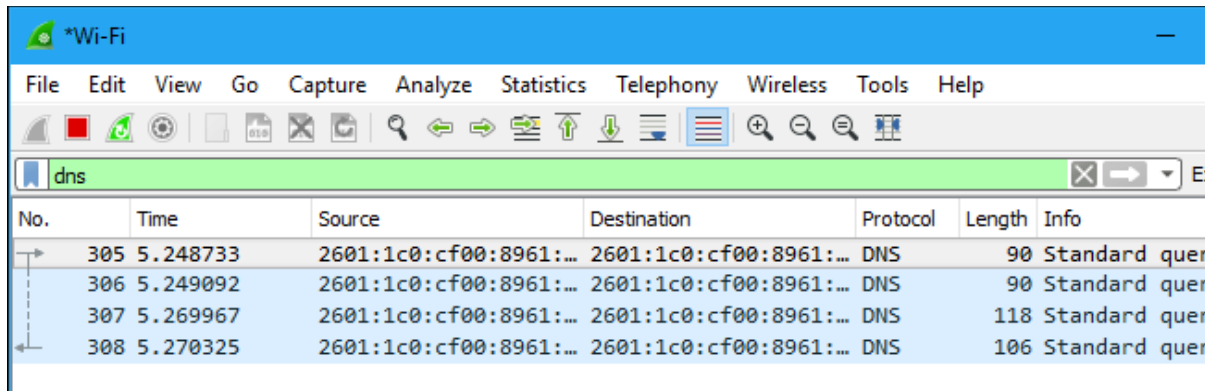


Filtering Packets

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

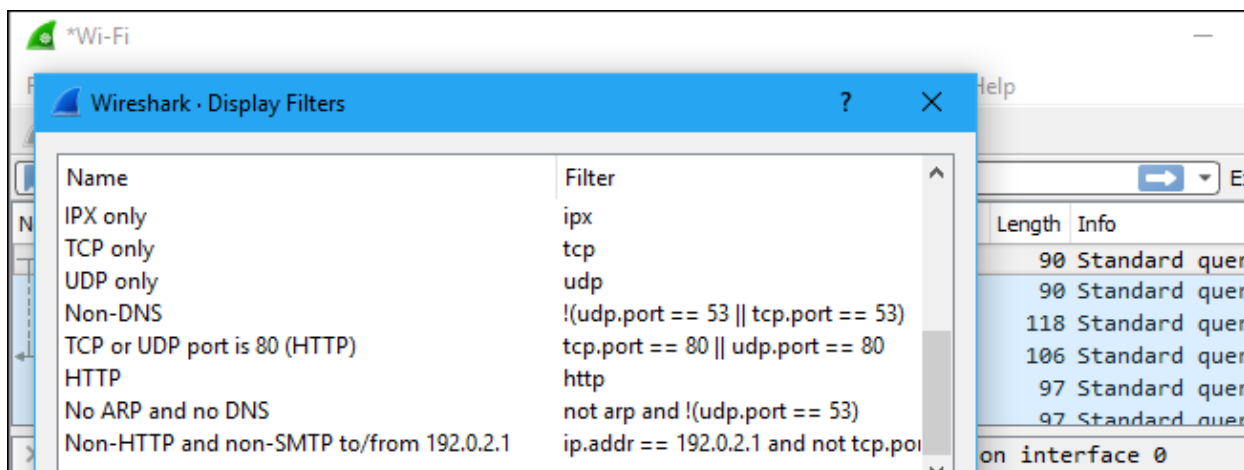
traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark's filters come in.

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.



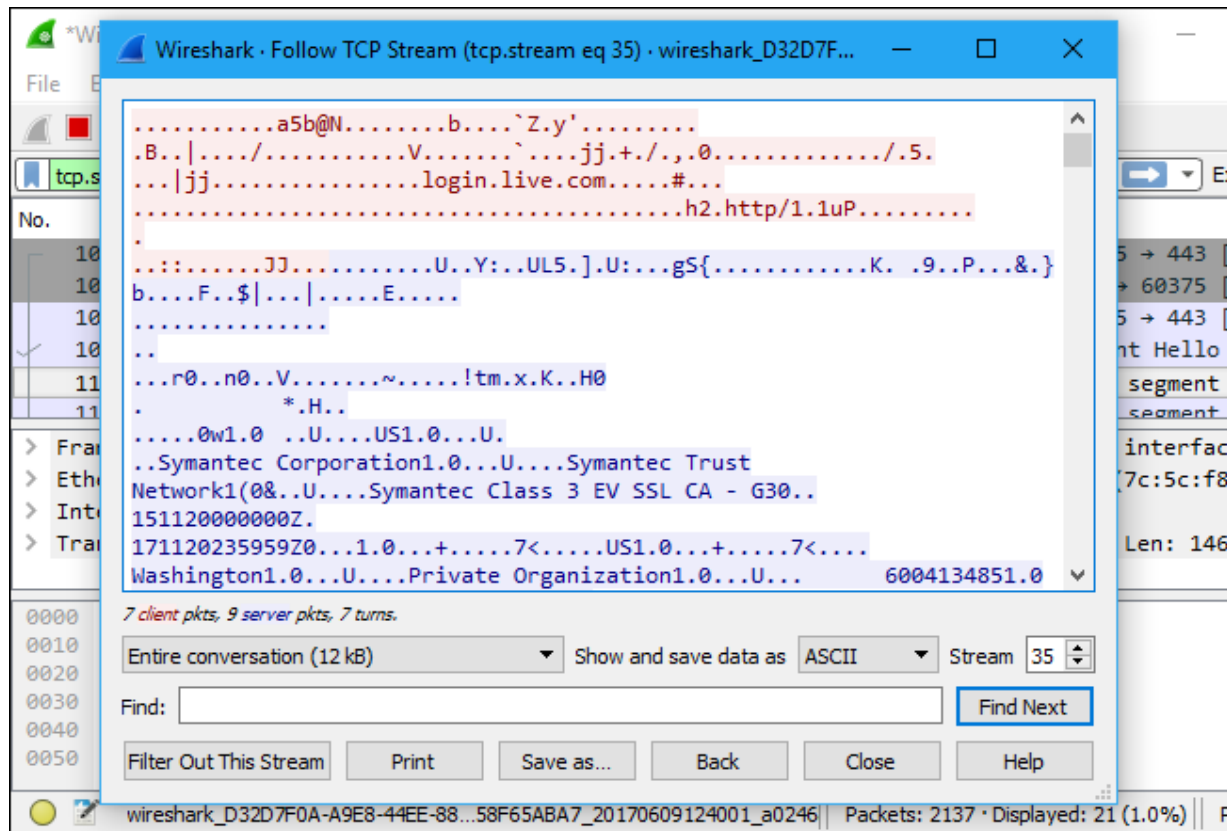
You can also click Analyze > Display Filters to choose a filter from among the default filters included in Wireshark. From here, you can add your own custom filters and save them to easily access them in the future.

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

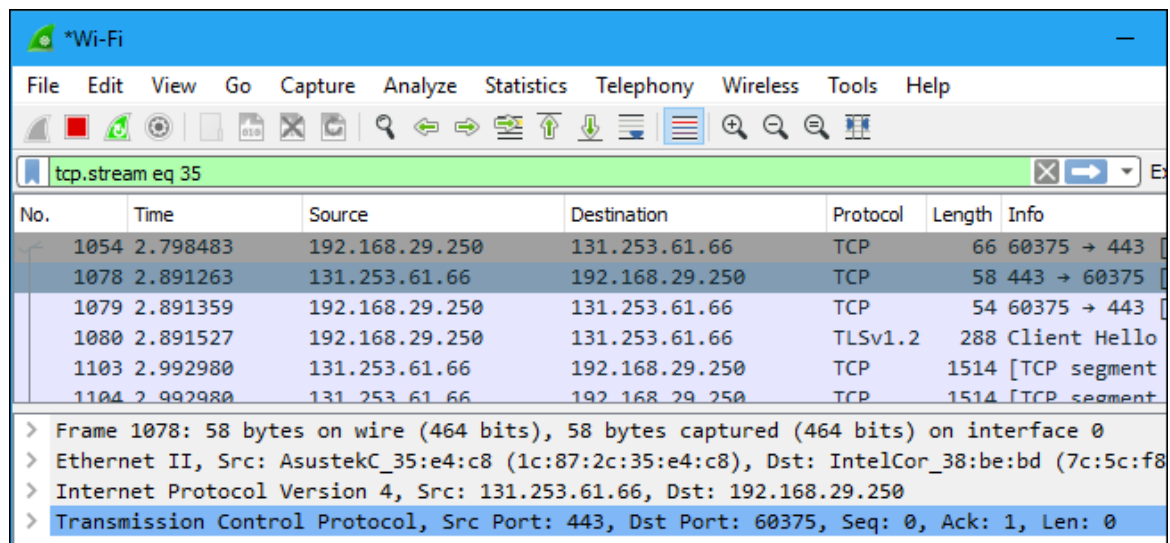


Another interesting thing you can do is right-click a packet and select Follow > TCP Stream.

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 list pane shows several packets, with packet 1054 selected. The packet details pane shows the structure of frame 1054, including the Ethernet II encapsulation type and the arrival time. The packet bytes pane shows the raw data of the frame in hexadecimal and ASCII.

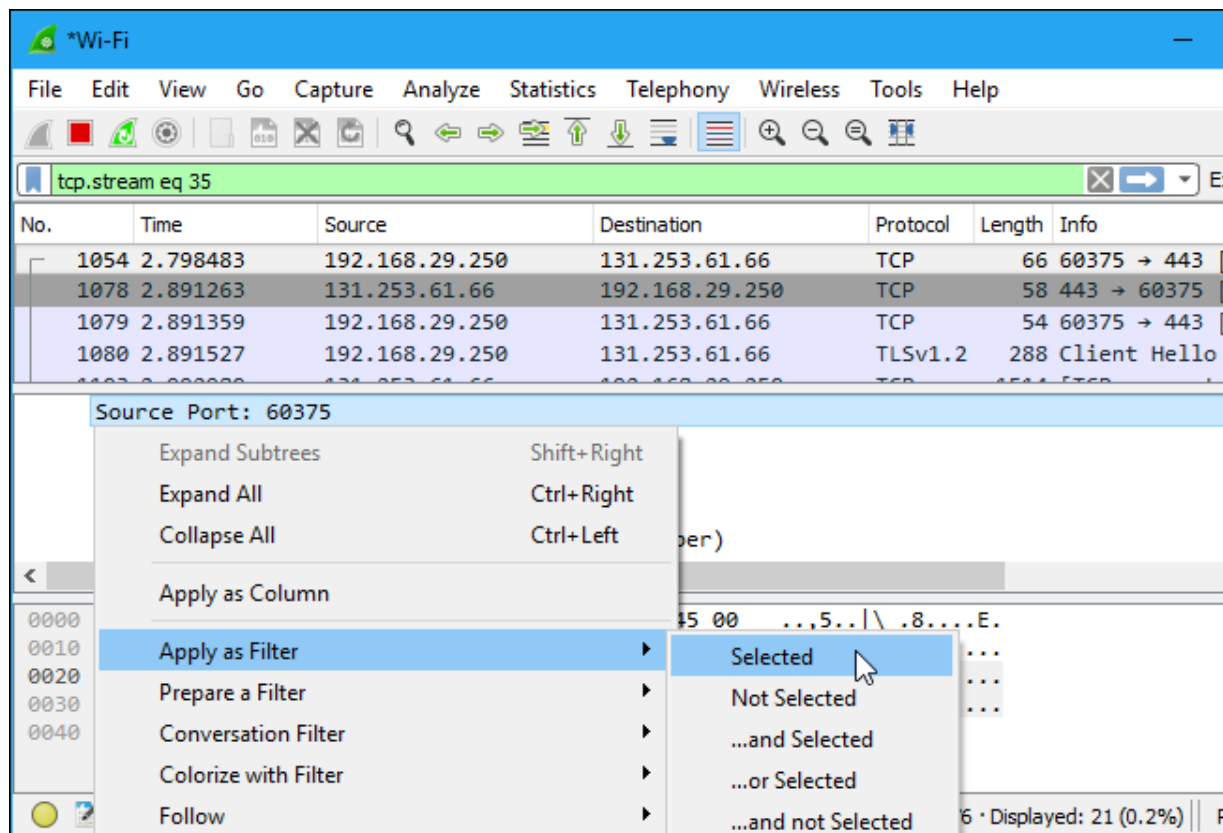
| No. | Time | Source | Destination | Protocol | Length | Info |
|------|----------|----------------|----------------|----------|--------|--------------|
| 1054 | 2.798483 | 192.168.29.250 | 131.253.61.66 | TCP | 66 | 60375 → 443 |
| 1078 | 2.891263 | 131.253.61.66 | 192.168.29.250 | TCP | 58 | 443 → 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

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

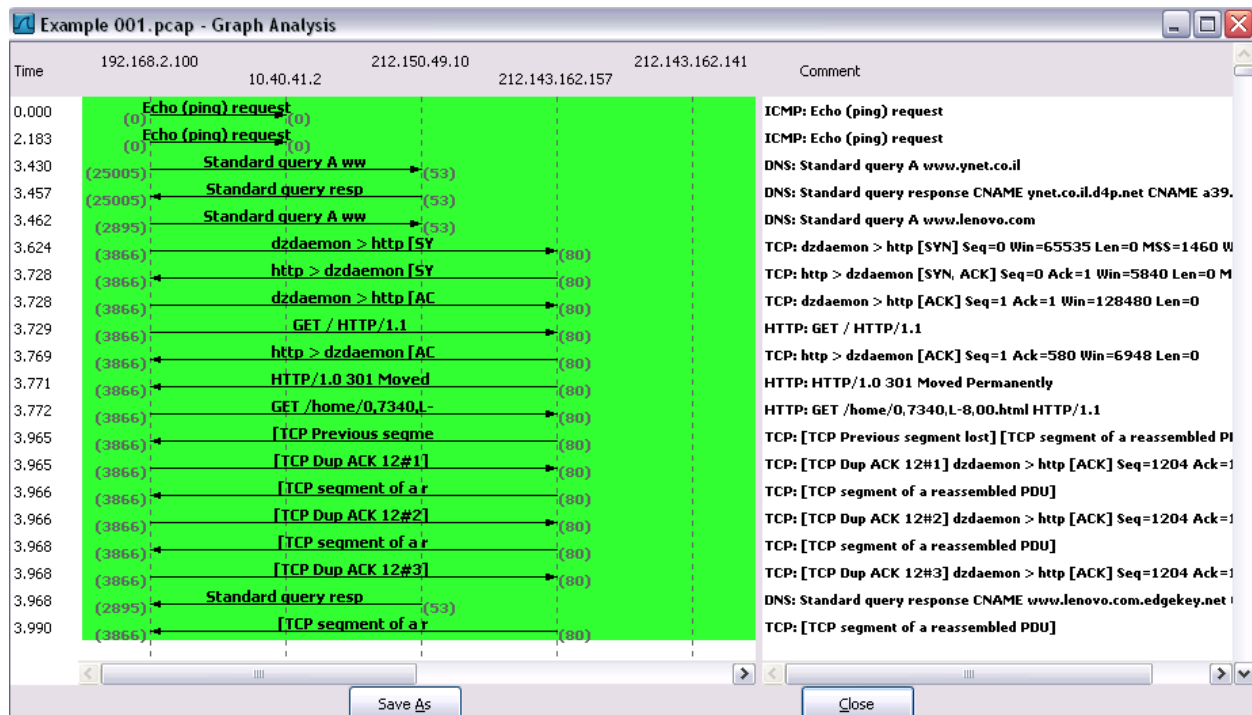
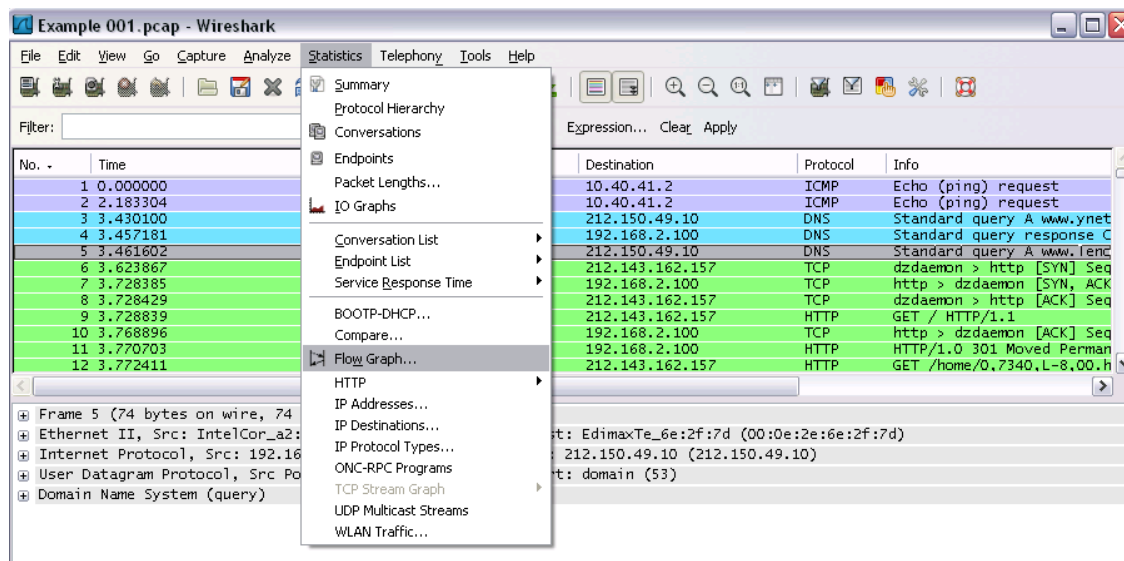
Encapsulation type (frame.encap_type) | Packets: 8136 · Displayed: 21 (0.3%)

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: 14B

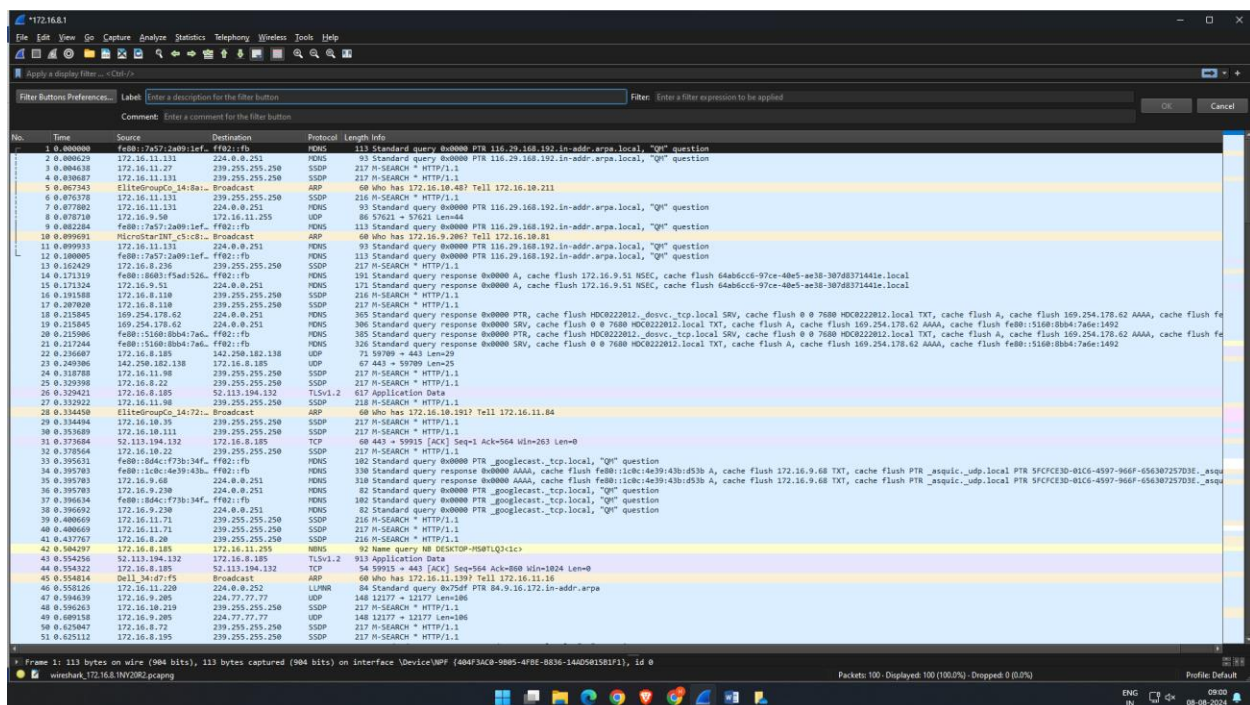
Date:13.08.2024

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

CS23532-COMPUTER NETWORKS

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|---|---------------------------|----------|---|--|
| 50 | 0.625047 | 172.16.8.72 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 51 | 0.625112 | 172.16.8.195 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 52 | 0.626247 | 172.16.10.42 | 224.0.0.251 | PNMS | 97 | Standard query 0x0000 PTR _dssvc_.tcp.local, "Q" question |
| 53 | 0.626247 | fe80::b3c:2129:5652::ff02::fb | | PNMS | 97 | Standard query 0x0000 PTR _dssvc_.tcp.local, "Q" question |
| 54 | 0.626044 | 0e11:3a:95:7a | Broadcast | ARP | 60 | Who has 172.16.10.42? Tell 172.16.8.238 |
| 55 | 0.626044 | fe80::b3c:2129:5652::ff02::fb | ff02::1:ff52:8f:05 | ICMPv6 | 86 | Neighbor Solicitation for fe80::b3c:2129:5652:8f:05 from c81e1ba2e15:ee183 |
| 56 | 0.627821 | fe80::b3c:2129:5652::ff02::fb | ff02::1:ff52:8f:05 | ICMPv6 | 86 | Neighbor Solicitation for fe80::b3c:2129:5652:8f:05 from c81e1ba2e15:7a |
| 57 | 0.627519 | fe80::b3c:2129:5652::ff02::fb | ff02::1:ff52:8f:05 | ICMPv6 | 86 | Neighbor Solicitation for fe80::b3c:2129:5652:8f:05 from 7c157:5b:18:da:3 |
| 58 | 0.627519 | 172.16.10.42 | 224.0.0.251 | PNMS | 85 | Standard query 0x0000 PTR _microsoft_mcc_.tcp.local, "Q" question |
| 59 | 0.628005 | fe80::b3c:2129:5652::ff02::fb | ff02::1:ff52:8f:05 | ICMPv6 | 86 | Neighbor Solicitation for fe80::b3c:2129:5652:8f:05 from 7c157:5b:18:da:3 |
| 60 | 0.628005 | fe80::b3c:2129:5652::ff02::fb | | PNMS | 185 | Standard query 0x0000 PTR _microsoft_mcc_.tcp.local, "Q" question |
| 61 | 0.663149 | 0e11:3a:95:7a | Broadcast | ARP | 60 | Who has 172.16.11.105? Tell 172.16.9.189 |
| 62 | 0.667051 | 172.16.11.113 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 63 | 0.680926 | 172.16.9.74 | 172.16.11.255 | UDP | 186 | 0x0000 = 51007 Len=144 |
| 64 | 0.700495 | 172.16.8.38 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 65 | 0.770661 | 0a:1b:3a:4b:c0cc:11 | Broadcast | 64 | 0x00000000 | 44 Ethernet II |
| 66 | 0.775564 | Wargear-Wi6icb184 | Spanning-tree (for... STP | 118 | Root = 32768/0/0c:1b:3a:4b:c0cc:11 Cost = 0 Port = 0x0000 | |
| 67 | 0.775564 | MicroStar28T-chica... | Broadcast | ARP | 60 | Who has 172.16.10.48? Tell 172.16.10.15 |
| 68 | 0.776059 | 172.16.9.122 | 239.255.255.250 | SSDP | 216 | M-SEARCH * HTTP/1.1 |
| 69 | 0.819053 | ff1e:0000:0000:0000:0000:0000:0000:0000 | Broadcast | ARP | 60 | Who has 172.16.10.48? Tell 172.16.10.211 |
| 70 | 0.847182 | 172.16.9.137 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 71 | 0.957282 | 172.16.11.97 | 172.16.11.255 | UDP | 86 | 57621 = 57621 Len=44 |
| 72 | 0.977142 | 172.16.11.228 | 224.0.0.252 | L1WRR | 84 | Standard query 0x75eff PTR 84.9.16.172.in-addr.arpa |
| 73 | 1.403064 | 172.16.11.27 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 74 | 1.171987 | 172.16.9.51 | 224.0.0.251 | PNMS | 171 | Standard query response 0x0000 A, cache flush 172.16.9.51 H5EC, cache flush 64ab6cc8-97cc-48e5-ae38-307d8371441e.local |
| 75 | 1.173539 | fe80::b3c:2129:5652::ff02::fb | ff02::1:ff52:8f:05 | PNMS | 181 | Standard query response 0x0000 A, cache flush 172.16.9.51 H5EC, cache flush 64ab6cc8-97cc-48e5-ae38-307d8371441e.local |
| 76 | 1.202205 | 172.16.8.110 | 239.255.255.250 | SSDP | 216 | M-SEARCH * HTTP/1.1 |
| 77 | 1.211125 | ff1e:0000:0000:0000:0000:0000:0000:0000 | Broadcast | ARP | 60 | Who has 172.16.10.191? Tell 172.16.11.84 |
| 78 | 1.211125 | ff1e:0000:0000:0000:0000:0000:0000:0000 | Broadcast | ARP | 60 | Who has 172.16.10.191? Tell 172.16.11.84 |
| 79 | 1.212784 | 172.16.8.110 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 80 | 1.222331 | 0e11:3a:95:7a | Broadcast | ARP | 60 | Who has 172.16.11.129? Tell 172.16.8.88 |
| 81 | 1.265440 | 0a:1b:3a:4b:c0cc:11 | Broadcast | ARP | 60 | Who has 172.16.8.17? Tell 172.16.11.252 |
| 82 | 1.266948 | 172.16.8.185 | 172.16.11.255 | PNMS | 92 | Name query 0x DESKTOP-HS8TLQ7-ic |
| 83 | 1.318187 | 172.16.11.240 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 84 | 1.340837 | 172.16.10.35 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 85 | 1.344714 | 172.16.8.122 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 86 | 1.354966 | 172.16.10.111 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 87 | 1.388344 | 0e11:3a:95:7a | Broadcast | ARP | 60 | Who has 172.16.8.17? Tell 172.16.8.224 |
| 88 | 1.389481 | 172.16.10.121 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 89 | 1.383714 | 172.16.11.11 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 90 | 1.403953 | 172.16.11.71 | 239.255.255.250 | SSDP | 216 | M-SEARCH * HTTP/1.1 |
| 91 | 1.403953 | 172.16.11.71 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 92 | 1.418125 | 172.16.8.20 | 239.255.255.250 | SSDP | 216 | M-SEARCH * HTTP/1.1 |
| 93 | 1.441279 | 172.16.8.14 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 94 | 1.500142 | 0e11:3a:95:7a | Broadcast | ARP | 60 | Who has 172.16.10.90? Tell 172.16.8.162 |
| 95 | 1.517410 | 0e11:3a:95:7a | Broadcast | ARP | 60 | Who has 172.16.8.17? Tell 172.16.8.224 |
| 96 | 1.561110 | 172.16.9.147 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 97 | 1.581310 | 172.16.9.147 | 239.255.255.250 | SSDP | 216 | M-SEARCH * HTTP/1.1 |
| 98 | 1.684689 | 172.16.10.219 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 99 | 1.688188 | 172.16.9.200 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 100 | 1.624821 | 172.16.9.200 | 239.255.255.250 | SSDP | 216 | M-SEARCH * HTTP/1.1 |

Frame 1: 113 bytes on wire (904 bits), 113 bytes captured (904 bits) on interface \Device\NPF {40AF3ACB-98B5-4F8E-B836-14D05015B1F1}, id 0

Wireshark 172.16.8.15V20R2.pcapng

Packets: 100 - Displayed: 100 (100.0%) - Dropped: 0 (0.0%)

Profile: Default

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

Procedure

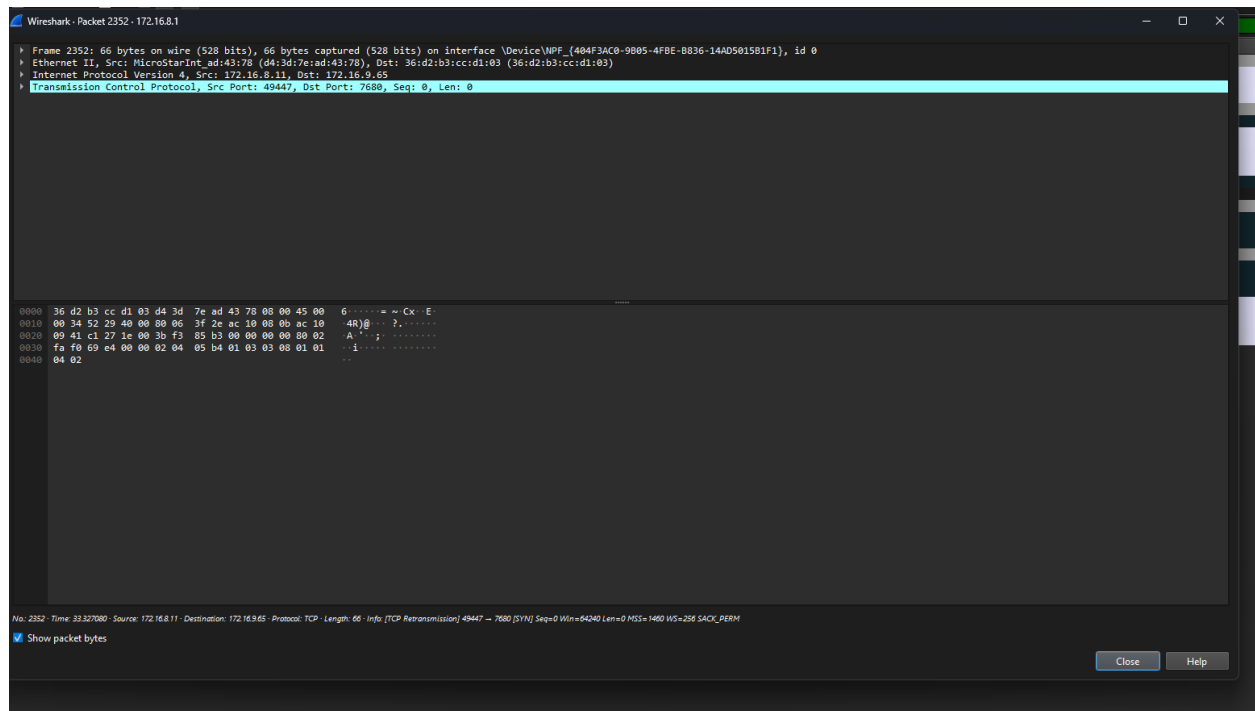
- Select Local Area Connection in Wireshark.
- Go to capture ☐ option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search TCP packets in search bar.
- To see flow graph click Statistics<>Flow graph.
- Save the packets.

Output:udp

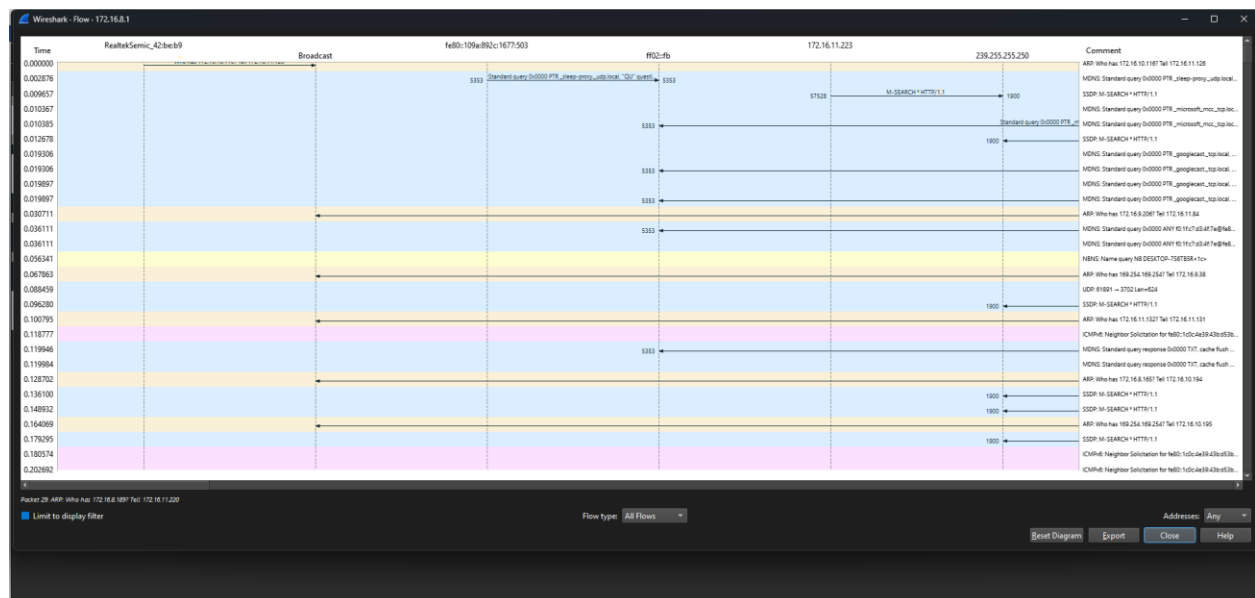
| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------|-----------------|-----------------|----------|--------|--|
| 915 | 12.158257 | 172.16.8.185 | 52.113.194.132 | TCP | 54 | 59968 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1818 Len=0 |
| 916 | 12.159399 | 52.113.194.132 | 172.16.8.185 | TCP | 60 | 443 → 59968 [ACK] Seq=1 Ack=2 Win=205 Len=0 |
| 1425 | 21.431611 | 172.16.8.185 | 172.217.107.138 | TCP | 55 | 59968 → 443 [ACK] Seq=1 Ack=1 Win=1802 Len=1 [TCP segment of a reassembled PDU] |
| 1426 | 21.432511 | 172.217.107.138 | 172.16.8.185 | TCP | 66 | 443 → 59968 [ACK] Seq=1 Ack=2 Win=257 Len=0 SLE=1 SRE=2 |
| 1516 | 26.117217 | 172.16.8.11 | 172.16.9.65 | TCP | 66 | 49447 → 7680 [VIN] Seq=0 Win=64240 Len=0 H5=1408 US=256 SACK PERM |
| 1518 | 26.119111 | 172.16.8.11 | 172.16.9.65 | TCP | 66 | TCP Retransmission 49447 → 7680 [VIN] Seq=0 Win=64240 Len=0 H5=1408 US=256 SACK PERM |
| 1968 | 27.727259 | 172.16.8.185 | 142.251.18.188 | TLSv1.2 | 80 | Application Data |
| 1973 | 27.765773 | 142.251.18.188 | 172.16.8.185 | TCP | 60 | 5228 → 59870 [ACK] Seq=1 Ack=27 Win=290 Len=0 |
| 1976 | 27.765175 | 142.251.18.188 | 172.16.8.185 | TLSv1.2 | 80 | Application Data |
| 3082 | 27.886526 | 172.16.8.185 | 142.251.18.188 | TCP | 54 | 59870 → 5228 [ACK] Seq=27 Ack=27 Win=1823 Len=0 |
| 2015 | 28.102224 | 172.16.8.185 | 172.16.9.65 | TCP | 66 | TCP Retransmission 49447 → 7680 [VIN] Seq=0 Win=64240 Len=0 H5=1408 US=256 SACK PERM |
| 2052 | 31.327808 | 172.16.8.11 | 172.16.9.65 | TCP | 66 | TCP Retransmission 49447 → 7680 [VIN] Seq=0 Win=64240 Len=0 H5=1408 US=256 SACK PERM |
| 2054 | 31.329095 | 172.16.8.11 | 172.16.9.65 | TCP | 66 | TCP Retransmission 49447 → 7680 [VIN] Seq=0 Win=64240 Len=0 H5=1408 US=256 SACK PERM |
| 2804 | 34.204438 | 172.16.8.200 | 172.16.11.40 | TCP | 66 | TCP Retransmission 64979 → 7680 [VIN] Seq=0 Win=64240 Len=0 H5=1408 US=256 SACK PERM |
| 2811 | 36.938966 | 172.16.8.200 | 172.16.11.40 | TCP | 66 | TCP Retransmission 64979 → 7680 [VIN] Seq=0 Win=64240 Len=0 H5=1408 US=256 SACK PERM |
| 2830 | 40.933265 | 172.16.8.200 | 172.16.11.40 | TCP | 66 | TCP Retransmission 64979 → 7680 [VIN] Seq=0 Win=64240 Len=0 H5=1408 US=256 SACK PERM |
| 5704 | 56.703916 | 172.16.9.173 | 172.16.11.40 | TCP | 66 | TCP Retransmission 52637 → 7680 [VIN] Seq=0 Win=64240 Len=0 H5=1408 US=256 SACK PERM |
| 5740 | 57.787881 | 172.16.9.173 | 172.16.11.40 | TCP | 66 | TCP Retransmission 52637 → 7680 [VIN] Seq=0 Win=64240 Len=0 H5=1408 US=256 SACK PERM |
| 5862 | 59.142611 | 172.16.9.173 | 172.16.11.40 | TCP | 66 | TCP Retransmission 52637 → 7680 [VIN] Seq=0 Win=64240 Len=0 H5=1408 US=256 SACK PERM |
| 6313 | 57.203274 | 172.16.8.185 | 172.16.11.40 | TCP | 66 | TCP Retransmission 52637 → 7680 [VIN] Seq=0 Win=64240 Len=0 H5=1408 US=256 SACK PERM |
| 6354 | 67.444413 | 172.16.8.185 | 172.217.107.138 | TCP | 55 | TCP Keep-Alive 59969 → 443 [ACK] Seq=1 Ack=1 Win=1822 Len=1 |
| 6355 | 67.444413 | 172.217.107.138 | 172.16.8.185 | TCP | 66 | TCP Keep-Alive ACK 443 → 59969 [ACK] Seq=1 Ack=2 Win=257 Len=0 SLE=1 SRE=2 |
| 6631 | 72.774755 | 172.16.8.185 | 142.251.18.188 | TCP | 55 | TCP Keep-Alive 59870 → 5228 [ACK] Seq=26 Ack=27 Win=1823 Len=1 |
| 6634 | 72.810898 | 142.251.18.188 | 172.16.8.185 | TCP | 66 | TCP Keep-Alive ACK 5228 → 59870 [ACK] Seq=27 Ack=27 Win=290 Len=0 SLE=26 SRE=27 |

Inspecting the packets

CS23532-COMPUTER NETWORKS



Flow Graph output

**Output:tcp**

CS23532-COMPUTER NETWORKS

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|--------------------------------|-----------------|----------|--------|---|
| 3 | 0.009863 | 172.16.11.126 | 239.255.255.250 | SSDP | 216 | M-SEARCH * HTTP/1.1 |
| 5 | 0.831978 | 172.16.18.211 | 239.255.255.250 | SSDP | 216 | M-SEARCH * HTTP/1.1 |
| 7 | 0.853898 | 172.16.18.185 | 142.250.182.142 | UDP | 71 | 63346 → 443 Len=20 |
| 8 | 0.858881 | 142.250.182.142 | 172.16.18.185 | UDP | 68 | 443 → 63346 Len=20 |
| 9 | 0.871925 | 142.250.182.142 | 172.16.18.185 | UDP | 148 | 443 → 63346 Len=186 |
| 10 | 0.872709 | 142.250.182.142 | 172.16.18.185 | UDP | 262 | 443 → 63346 Len=220 |
| 11 | 0.872920 | 172.16.11.126 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 12 | 0.873138 | 172.16.18.185 | 142.250.182.142 | UDP | 81 | 63346 → 443 Len=30 |
| 13 | 0.874281 | 172.16.9.128 | 239.255.255.250 | SSDP | 216 | M-SEARCH * HTTP/1.1 |
| 14 | 0.877633 | 142.250.182.142 | 172.16.18.185 | UDP | 68 | 443 → 63346 Len=20 |
| 18 | 0.180149 | 172.16.8.212 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 19 | 0.289299 | 172.16.11.129 | 239.255.255.250 | SSDP | 216 | M-SEARCH * HTTP/1.1 |
| 21 | 0.265666 | 172.16.11.238 | 239.255.255.250 | SSDP | 218 | M-SEARCH * HTTP/1.1 |
| 22 | 0.266689 | 172.16.8.226 | 239.255.255.250 | SSDP | 218 | M-SEARCH * HTTP/1.1 |
| 23 | 0.265689 | 172.16.11.83 | 239.255.255.250 | SSDP | 216 | M-SEARCH * HTTP/1.1 |
| 24 | 0.269677 | 172.16.8.231 | 172.16.11.255 | NDNS | 92 | Name query NB LAPTOP-FRHF031E<ic> |
| 25 | 0.279369 | 172.16.8.185 | 142.250.182.142 | UDP | 71 | 63346 → 443 Len=20 |
| 26 | 0.284225 | 142.250.182.142 | 172.16.18.185 | UDP | 68 | 443 → 63346 Len=20 |
| 27 | 0.316533 | 172.16.8.37 | 239.255.255.250 | SSDP | 216 | M-SEARCH * HTTP/1.1 |
| 29 | 0.342098 | 172.16.8.189 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 30 | 0.353555 | 172.16.9.89 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 31 | 0.360149 | 172.16.18.190 | 239.255.255.250 | SSDP | 216 | M-SEARCH * HTTP/1.1 |
| 32 | 0.367863 | 172.16.11.4 | 239.255.255.250 | SSDP | 216 | M-SEARCH * HTTP/1.1 |
| 35 | 0.432822 | 172.16.9.192 | 239.255.255.250 | SSDP | 216 | M-SEARCH * HTTP/1.1 |
| 36 | 0.440731 | 172.16.18.196 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 37 | 0.442881 | 172.16.9.219 | 239.255.255.250 | SSDP | 216 | M-SEARCH * HTTP/1.1 |
| 38 | 0.447340 | 172.16.8.32 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 39 | 0.588999 | 172.16.18.185 | 142.250.182.142 | UDP | 71 | 63346 → 443 Len=20 |
| 41 | 0.589941 | 142.250.182.142 | 172.16.18.185 | UDP | 68 | 443 → 63346 Len=20 |
| 44 | 0.543334 | 172.16.18.43 | 239.255.255.250 | SSDP | 216 | M-SEARCH * HTTP/1.1 |
| 47 | 0.610959 | 172.16.11.138 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 48 | 0.626380 | 172.16.18.172 | 239.255.255.250 | SSDP | 212 | M-SEARCH * HTTP/1.1 |
| 49 | 0.627664 | 172.16.8.163 | 172.16.11.255 | NDNS | 92 | Name query NB DESKTOP-BKFDK1C<ic> |
| 50 | 0.643654 | 172.16.8.16 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 51 | 0.649162 | 172.16.9.171 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 52 | 0.651986 | 172.16.8.112 | 239.255.255.250 | SSDP | 216 | M-SEARCH * HTTP/1.1 |
| 53 | 0.683616 | 172.16.8.112 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 54 | 0.686278 | 172.16.8.178 | 239.255.255.250 | SSDP | 217 | M-SEARCH * HTTP/1.1 |
| 55 | 0.686362 | 172.16.9.6 | 239.255.255.250 | SSDP | 216 | M-SEARCH * HTTP/1.1 |
| 56 | 0.787180 | 172.16.8.185 | 142.250.182.142 | UDP | 71 | 63346 → 443 Len=20 |
| 57 | 0.712818 | 142.250.182.142 | 172.16.18.185 | UDP | 68 | 443 → 63346 Len=20 |
| 59 | 0.731196 | 172.16.8.238 | 239.255.255.250 | SSDP | 216 | M-SEARCH * HTTP/1.1 |
| 60 | 0.737464 | 172.16.18.219 | 224.0.0.252 | LLMNR | 70 | Standard query 0xcdf1 A HDC181744 |
| 61 | 0.737557 | f68b:0597:787:97fe::f682:1:1:3 | | LLMNR | 98 | Standard query 0xcdf1 A HDC181744 |
| 62 | 0.738582 | 172.16.18.219 | 224.0.0.252 | LLMNR | 70 | Standard query 0xcdf1 AAAA HDC181744 |
| 63 | 0.738684 | f68b:0597:787:97fe::f682:1:1:3 | | LLMNR | 98 | Standard query 0xcdf1 AAAA HDC181744 |
| 64 | 0.739707 | 172.16.9.75 | 239.255.255.250 | SSDP | 216 | M-SEARCH * HTTP/1.1 |
| 65 | 0.750110 | 172.16.18.219 | 224.0.0.252 | LLMNR | 70 | Standard query 0x4662 A HDC181744 |
| 66 | 0.750170 | f68b:0597:787:97fe::f682:1:1:3 | | LLMNR | 98 | Standard query 0x4662 A HDC181744 |
| 67 | 0.751187 | 172.16.18.219 | 224.0.0.252 | LLMNR | 70 | Standard query 0x58dd AAAA HDC181744 |
| 68 | 0.751267 | f68b:0597:787:97fe::f682:1:1:3 | | LLMNR | 98 | Standard query 0x58dd AAAA HDC181744 |
| 69 | 0.764152 | 172.16.18.219 | 172.16.11.255 | BROWSER | 230 | Request Announcement VSSFL2 |
| 70 | 0.769820 | 172.16.8.218 | 224.0.0.251 | NDNS | 229 | Standard query response 0x0000 PTR Jodes-ZBook-15_dosvc_tcp.local SRV 0 0 7680 Jodes-ZBook-15.local TXT |
| 71 | 0.771821 | f68b:0597:787:97fe::f682:1:1:3 | | NDNS | 219 | Standard query response 0x0000 PTR Jodes-ZBook-15_dosvc_tcp.local SRV 0 0 7680 Jodes-ZBook-15.local TXT |
| 72 | 0.771823 | 172.16.8.218 | 224.0.0.251 | NDNS | 92 | Standard query 0x0000 ANY Jodes-ZBook-15_dosvc_tcp.local, "Q" question |
| 73 | 0.771629 | f68b:0597:787:97fe::f682:1:1:3 | | NDNS | 112 | Standard query 0x0000 ANY Jodes-ZBook-15_dosvc_tcp.local, "Q" question |

Frame 31: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on Interface \Device\NPF{40AF3AC0-9805-4FBE-8B36-14A0501581F1}, id 0

User Datagram Protocol

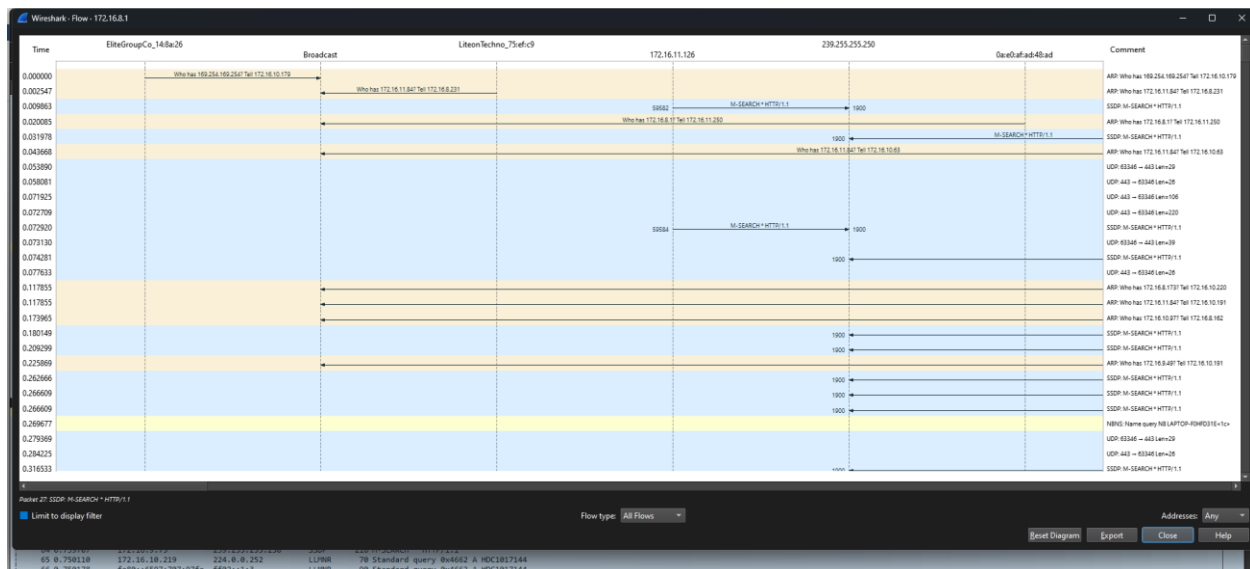
Packets: 845 - Displayed: 619 (73.3%) - Dropped: 0 (0.0%)

Profile: Default

Inspecting the packets

| | |
|--|--|
| Wireshark - Packet 48 - 172.16.8.1 | |
| Frame 48: 212 bytes on wire (1696 bits), 212 bytes captured (1696 bits) on Interface \Device\NPF{40AF3AC0-9805-4FBE-8B36-14A0501581F1}, id 0 | |
| Ethernet II, Src: EliteGroupCo, Id: 72:47:47: (88:acd:14:72:47), Dst: IPv4cast_7f:ff:fa (01:80:5e:7f:ff:fa) | |
| Internet Protocol Version 4, Src: 172.16.10.172, Dst: 239.255.255.250 | |
| User Datagram Protocol, Src Port: 61774, Dst Port: 1900 | |
| Simple Service Discovery Protocol | |
| 0000 01 00 5e 7f ff fa 88 ae dd 14 72 47 08 00 45 00 ...N...rg.E | |
| 0010 00 c6 8b 02 00 00 01 11 87 6e ac 10 0a ac ef ffn..... | |
| 0020 ff fa f1 4e 07 6c 00 b2 63 62 4d 2d 53 45 41 52 ...N.l...cbm-SEAR | |
| 0030 43 48 20 2a 20 40 54 54 50 2f 31 2e 31 0d 0a 48 ...CH * HTTP/1.1 M | |
| 0040 4f 53 54 3a 20 32 33 30 2e 32 35 35 2e 32 35 35 ...OST: 239.255.255 | |
| 0050 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20 ...250:190 0 MAN: | |
| 0060 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d ..."ssdp:discover" | |
| 0070 0a 4d 58 3a 20 31 0d 0a 53 54 3a 20 75 72 6e 3a ...MX: 1, ST: urn: | |
| 0080 64 69 61 6c 2d 6d 76 6c 74 69 73 63 72 65 6e ...dl1:multit screen | |
| 0090 2d 6f 72 67 3a 73 65 72 76 69 63 65 3a 64 69 61 ...-org:ser vice:dia | |
| 00a0 6c 3a 31 0d 0a 55 53 45 52 2d 41 47 45 4e 54 3a ...l:1 USE R-AGENT: | |
| 00b0 20 4f 70 65 72 61 20 47 58 2f 31 32 33 2e 30 2e ...Opera G X/123.0. | |
| 00c0 50 33 31 32 2e 31 32 34 20 57 69 6e 64 6f 77 73 ...8312.124 windows | |
| 00d0 0d 0a 0d 0a | |
| No. 48 - Time: 0.626380 - Source: 172.16.10.172 - Destination: 239.255.255.250 - Protocol: SSDP - Length: 212 - Info: M-SEARCH * HTTP/1.1 | |
| <input checked="" type="checkbox"/> Show packet bytes | |
| Close Help | |

Flow chart output



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

Procedure

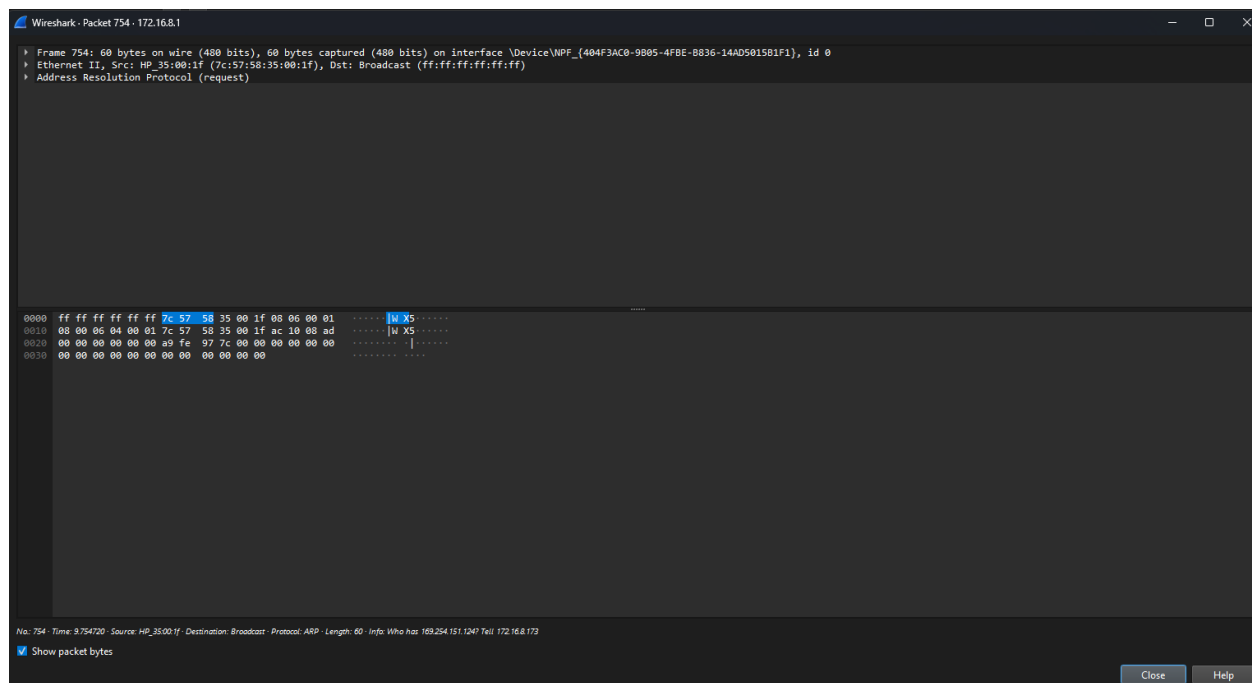
- Select Local Area Connection in Wireshark.
- Go to capture □ option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search ARP packets in search bar.
- Save the packets.

Output

CS23532-COMPUTER NETWORKS



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|----------|-----------------------|-------------------|----------|--------------|---|
| 9 | 0.921542 | GigabyteTech_Bc1b4... | Broadcast | ARP | 60 | Who has 172.16.11.216? Tell 172.16.11.222 |
| 15 | 0.182076 | EliteGroupC_151ee... | Broadcast | ARP | 60 | Who has 169.254.169.254? Tell 172.16.10.178 |
| 16 | 0.236907 | HP_3518ef:f8 | Broadcast | ARP | 60 | Who has 172.16.10.93? Tell 172.16.8.189 |
| 17 | 0.278540 | MicroStarINT_5c1ca... | Broadcast | ARP | 60 | Who has 172.16.9.63? Tell 172.16.10.118 |
| 18 | 0.359883 | MicroStarINT_5c1cf... | Broadcast | ARP | 60 | Who has 172.16.9.280? Tell 172.16.10.49 |
| 20 | 0.364115 | Dell_3518ff:f8 | Broadcast | ARP | 60 | Who has 172.16.9.180? Tell 172.16.8.180 |
| 21 | 0.364115 | Dell_3518ff:f8 | Broadcast | ARP | 60 | Who has 172.16.6.183? Tell 172.16.8.180 |
| 22 | 0.388779 | Dell_2e195f:7a | Broadcast | ARP | 60 | Who has 172.16.6.139? Tell 172.16.8.238 |
| 23 | 0.486227 | HP_3518ff:f8 | Broadcast | ARP | 60 | Who has 172.16.10.97? Tell 172.16.8.162 |
| 24 | 0.451338 | MicroStarINT_5c1cb... | Broadcast | ARP | 60 | Who has 172.16.10.48? Tell 172.16.10.43 |
| 26 | 0.477771 | EliteGroupC_14721... | Broadcast | ARP | 60 | Who has 169.254.169.254? Tell 172.16.10.190 |
| 28 | 0.494357 | 0ae0:afad:ad15 | Broadcast | ARP | 60 | Who has 172.16.9.67? Tell 172.16.9.219 |
| 30 | 0.555043 | MicroStarINT_5c1cd... | Broadcast | ARP | 60 | Who has 172.16.9.283? Tell 172.16.10.115 |
| 32 | 0.564951 | Dell_371b75 | Broadcast | ARP | 60 | Who has 172.16.10.21? Tell 172.16.8.203 |
| 33 | 0.569354 | MicroStarINT_ad13e... | Broadcast | ARP | 60 | Who has 172.16.9.61? Tell 172.16.10.224 |
| 35 | 0.759917 | MicroStarINT_5c1cb... | Broadcast | ARP | 60 | Who has 172.16.10.16? Tell 172.16.10.31 |
| 36 | 0.759917 | Dell_34d31bc | Broadcast | ARP | 60 | Who has 172.16.8.117? Tell 172.16.11.8 |
| 38 | 0.752825 | 06:c7:71:37:4d:7b | 06:1b:ad:56:96:c1 | ARP | 60 | Gratuitous ARP for 172.16.11.184 (Reply) |
| 39 | 0.760795 | 0ae0:afad:ad15 | Broadcast | ARP | 60 | Who has 172.16.8.1? Tell 172.16.9.214 |
| 47 | 0.890624 | Dell_2e195f:7a | Broadcast | ARP | 60 | Who has 172.16.10.39? Tell 172.16.8.238 |
| 51 | 1.026436 | Intel_77125:9f | Broadcast | ARP | 60 | Who has 172.16.8.1? Tell 172.16.9.214 |
| 52 | 1.026436 | Intel_77125:9f | Broadcast | ARP | 60 | Who has 172.16.8.1? Tell 172.16.9.214 |
| 53 | 1.078841 | HomeIprecis_B132i... | Broadcast | ARP | 60 | Who has 172.16.9.171? Tell 172.16.11.229 |
| 54 | 1.080386 | Intel_77125:9f | Broadcast | ARP | 60 | Who has 172.16.8.1? Tell 172.16.9.219 |
| 63 | 1.238551 | HP_381e6:f2 | Broadcast | ARP | 60 | Who has 172.16.10.99? Tell 172.16.8.189 |
| 64 | 1.255278 | MicroStarINT_5c1cf... | Broadcast | ARP | 60 | Who has 172.16.9.280? Tell 172.16.10.49 |
| 65 | 1.255278 | EliteGroupC_14721... | Broadcast | ARP | 60 | Who has 169.254.169.254? Tell 172.16.10.190 |
| 66 | 1.427223 | MicroStarINT_5c1cb... | Broadcast | ARP | 60 | Who has 172.16.10.48? Tell 172.16.10.31 |
| 74 | 1.576548 | MicroStarINT_ad13e... | Broadcast | ARP | 60 | Who has 172.16.9.61? Tell 172.16.10.224 |
| 75 | 1.576548 | MicroStarINT_5c1cb... | Broadcast | ARP | 60 | Who has 172.16.10.48? Tell 172.16.10.43 |
| 79 | 1.751248 | Dell_34d31bc | Broadcast | ARP | 60 | Who has 172.16.8.117? Tell 172.16.11.8 |
| 81 | 1.852082 | Intel_77125:9f | Broadcast | ARP | 60 | Who has 172.16.8.1? Tell 172.16.9.214 |
| 84 | 1.864562 | MicroStarINT_5c1cb... | Broadcast | ARP | 60 | Who has 172.16.10.72? Tell 172.16.11.120 |
| 85 | 1.864562 | MicroStarINT_5c1cb... | Broadcast | ARP | 60 | Who has 172.16.10.93? Tell 172.16.11.120 |
| 87 | 1.872276 | RealtekSemiC_421be... | Broadcast | ARP | 60 | Who has 172.16.8.1? Tell 172.16.11.126 |
| 108 | 2.003928 | Dell_35111f9 | Broadcast | ARP | 60 | Who has 172.16.9.118? Tell 172.16.9.235 |
| 115 | 2.239518 | MicroStarINT_5c1cb... | Broadcast | ARP | 60 | Who has 172.16.10.48? Tell 172.16.10.31 |
| 117 | 2.249588 | MicroStarINT_5c1cf... | Broadcast | ARP | 60 | Who has 172.16.9.280? Tell 172.16.10.49 |
| 118 | 2.251198 | EliteGroupC_14721... | Broadcast | ARP | 60 | Who has 169.254.169.254? Tell 172.16.10.190 |
| 124 | 2.451858 | MicroStarINT_5c1cb... | Broadcast | ARP | 60 | Who has 172.16.10.48? Tell 172.16.10.43 |
| 125 | 2.459718 | MicroStarINT_5c1cd... | Broadcast | ARP | 60 | Who has 172.16.11.80? Tell 172.16.10.30 |
| 131 | 2.645248 | MicroStarINT_5c1cb... | Broadcast | ARP | 60 | Who has 172.16.10.72? Tell 172.16.11.120 |
| 132 | 2.645248 | MicroStarINT_5c1cb... | Broadcast | ARP | 60 | Who has 172.16.10.93? Tell 172.16.11.120 |
| 135 | 2.782874 | MicroStarINT_5c1cd... | Broadcast | ARP | 60 | Who has 172.16.10.48? Tell 172.16.10.20 |
| 148 | 2.825386 | EliteGroupC_1418a... | Broadcast | ARP | 60 | Who has 169.254.169.254? Tell 172.16.10.211 |
| 151 | 2.839549 | ASUSTekCOMP_941c... | Broadcast | ARP | 60 | Who has 172.16.6.5? Tell 172.16.11.220 |
| 155 | 3.059889 | HP_3518ff:f8 | Broadcast | ARP | 60 | Who has 172.16.10.97? Tell 172.16.8.162 |
| 162 | 3.239662 | MicroStarINT_5c1cb... | Broadcast | ARP | 60 | Who has 172.16.10.48? Tell 172.16.10.31 |
| 164 | 3.317749 | MicroStarINT_5c1cd... | Broadcast | ARP | 60 | Who has 172.16.9.165? Tell 172.16.10.31 |
| 167 | 3.374858 | MicroStarINT_5c1cd... | Broadcast | ARP | 60 | Who has 172.16.10.48? Tell 172.16.10.30 |
| 170 | 3.450973 | MicroStarINT_5c1cb... | Broadcast | ARP | 60 | Who has 172.16.10.48? Tell 172.16.10.43 |
| 171 | 3.470818 | HomeIprecis_B132i... | Broadcast | ARP | 60 | Who has 172.16.9.1? Tell 172.16.11.229 |
| 174 | 3.497980 | MicroStarINT_5c1cc... | Broadcast | ARP | 60 | Who has 172.16.9.75? Tell 172.16.10.42 |
| 178 | 3.525921 | MicroStarINT_5c1cd... | Broadcast | ARP | 60 | Who has 172.16.9.283? Tell 172.16.10.115 |
| 189 | 3.648925 | MicroStarINT_5c1cb... | Broadcast | ARP | 60 | Who has 172.16.10.72? Tell 172.16.11.120 |
| 190 | 3.648925 | MicroStarINT_5c1cb... | Broadcast | ARP | 60 | Who has 172.16.10.93? Tell 172.16.11.120 |
| Frame 75: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF {404F3ACB-9805-4F8C-8036-1A4D501501F1}, Id 0 | | | | | | |
| Address Resolution Protocol Protocol | | | | | | |
| | | | | | Packets: 508 | Displayed: 112 (22.0%) - Dropped: 0 (0.0%) |
| Profile: Default | | | | | | |
| No. | Time | Source | Destination | Protocol | Length | Info |
| 197 | 3.782228 | EliteGroupC_1418a... | Broadcast | ARP | 60 | Who has 169.254.169.254? Tell 172.16.10.211 |
| 204 | 3.908041 | RealtekSemiC_421be... | Broadcast | ARP | 60 | Who has 172.16.8.1? Tell 172.16.11.126 |
| 205 | 3.912395 | HP_3518ff:f8 | Broadcast | ARP | 60 | Who has 172.16.10.97? Tell 172.16.8.162 |
| 206 | 3.915866 | Dell_34d31bc | Broadcast | ARP | 60 | Who has 172.16.8.117? Tell 172.16.11.8 |
| 209 | 4.051199 | MicroStarINT_5c1cd... | Broadcast | ARP | 60 | Who has 172.16.9.283? Tell 172.16.10.115 |
| 210 | 4.064088 | ASUSTekCOMP_941c... | Broadcast | ARP | 60 | Who has 172.16.11.48? Tell 172.16.11.220 |
| 212 | 4.069574 | ASUSTekCOMP_941c... | Broadcast | ARP | 60 | Who has 172.16.8.178? Tell 172.16.11.220 |
| 214 | 4.167784 | 7617a:65:ef:f7:40 | Broadcast | ARP | 60 | Who has 172.16.9.78? Tell 172.16.11.79 |
| 215 | 4.167784 | 7617a:65:ef:f7:40 | Broadcast | ARP | 60 | Who has 172.16.11.97? Tell 172.16.11.79 |
| 217 | 4.239862 | MicroStarINT_5c1cb... | Broadcast | ARP | 60 | Who has 172.16.9.165? Tell 172.16.10.31 |
| 220 | 4.268808 | RealtekSemiC_421be... | Broadcast | ARP | 60 | Who has 172.16.9.133? Tell 172.16.11.126 |
| 222 | 4.318414 | MicroStarINT_5c1cc... | Broadcast | ARP | 60 | Who has 172.16.9.75? Tell 172.16.10.42 |
| 226 | 4.374603 | MicroStarINT_5c1cb... | Broadcast | ARP | 60 | Who has 172.16.10.48? Tell 172.16.10.20 |
| 243 | 4.748716 | Dell_34d31bc | Broadcast | ARP | 60 | Who has 172.16.8.117? Tell 172.16.11.8 |
| 247 | 4.773297 | EliteGroupC_1418a... | Broadcast | ARP | 60 | Who has 169.254.169.254? Tell 172.16.10.211 |
| 251 | 4.907494 | HP_3518ff:f8 | Broadcast | ARP | 60 | Who has 172.16.10.97? Tell 172.16.8.162 |
| 258 | 5.051380 | MicroStarINT_5c1cd... | Broadcast | ARP | 60 | Who has 172.16.9.283? Tell 172.16.10.115 |
| 259 | 5.061841 | ASUSTekCOMP_941c... | Broadcast | ARP | 60 | Who has 172.16.11.48? Tell 172.16.11.220 |
| 267 | 5.191623 | ASUSTekCOMP_941c... | Broadcast | ARP | 60 | Who has 172.16.10.28? Tell 172.16.11.220 |
| 268 | 5.191623 | ASUSTekCOMP_941c... | Broadcast | ARP | 60 | Who has 172.16.8.39? Tell 172.16.11.220 |
| 269 | 5.239554 | MicroStarINT_5c1cb... | Broadcast | ARP | 60 | Who has 172.16.9.165? Tell 172.16.10.31 |
| 274 | 5.310875 | MicroStarINT_5c1cc... | Broadcast | ARP | 60 | Who has 172.16.9.75? Tell 172.16.10.42 |
| 284 | 5.428839 | MicroStarINT_5c1cb... | Broadcast | ARP | 60 | Who has 172.16.10.48? Tell 172.16.10.31 |
| 291 | 5.598857 | MicroStarINT_5c1cb... | Broadcast | ARP | 60 | Who has 172.16.10.48? Tell 172.16.10.43 |
| 294 | 5.595780 | 7617a:65:ef:f7:40 | Broadcast | ARP | 60 | Who has 172.16.9.78? Tell 172.16.11.79 |
| 305 | 5.747521 | Dell_34d31bc | Broadcast | ARP | 60 | Who has 172.16.8.117? Tell 172.16.11.8 |
| 313 | 5.878898 | MicroStarINT_5c1cb... | Broadcast | ARP | 60 | Who has 172.16.10.72? Tell 172.16.11.120 |
| 314 | 5.878898 | MicroStarINT_5c1cb... | Broadcast | ARP | 60 | Who has 172.16.10.93? Tell 172.16.11.120 |
| 320 | 5.931452 | RealtekSemiC_421be... | Broadcast | ARP | 60 | Who has 172.16.8.1? Tell 172.16.11.126 |
| 326 | 6.055884 | ASUSTekCOMP_941c... | Broadcast | ARP | 60 | Who has 172.16.11.48? Tell 172.16.11.220 |
| 335 | 6.142793 | 7617a:65:ef:f7:40 | Broadcast | ARP | 60 | Who has 172.16.9.78? Tell 172.16.11.79 |
| 337 | 6.241525 | MicroStarINT_5c1cb... | Broadcast | ARP | 60 | Who has 172.16.10.48? Tell 172.16.10.31 |
| 341 | 6.319075 | EliteGroupC_14183... | Broadcast | ARP | 60 | Who has 169.254.169.254? Tell 172.16.10.171 |
| 344 | 6.342561 | RealtekSemiC_421be... | Broadcast | ARP | 60 | Who has 172.16.8.42? Tell 172.16.11.126 |
| 351 | 6.409550 | MicroStarINT_5c1ca... | Broadcast | ARP | 60 | Who has 172.16.9.63? Tell 172.16.10.118 |
| 354 | 6.449725 | MicroStarINT_5c1cb... | Broadcast | ARP | 60 | Who has 172.16.10.48? Tell 172.16.10.43 |
| 370 | 6.644242 | MicroStarINT_5c1cb... | Broadcast | ARP | 60 | Who has 172.16.10.72? Tell 172.16.11.120 |
| 371 | 6.644242 | MicroStarINT_5c1cb... | Broadcast | ARP | 60 | Who has 172.16.10.93? Tell 172.16.11.120 |
| 392 | 6.818491 | HP_3518ff:f8 | Broadcast | ARP | 60 | Who has 172.16.9.165? Tell 172.16.8.166 |
| 396 | 6.842867 | Dell_3518ff:f8 | Broadcast | ARP | 60 | Who has 172.16.25.180? Tell 172.16.8.180 |
| 397 | 6.842867 | Dell_3518ff:f8 | Broadcast | ARP | 60 | Who has 172.16.6.183? Tell 172.16.8.180 |
| 420 | 7.064344 | HP_3518ff:f8 | Broadcast | ARP | 60 | Who has 172.16.10.97? Tell 172.16.8.162 |
| 441 | 7.195416 | 0ae0:afad:ad15 | Broadcast | ARP | 60 | Who has 172.16.8.1? Tell 172.16.11.200 |
| 442 | 7.242680 | MicroStarINT_5c1cb... | Broadcast | ARP | 60 | Who has 172.16.10.48? Tell 172.16.10.31 |
| 449 | 7.275770 | EliteGroupC_14183... | Broadcast | ARP | 60 | Who has 169.254.169.254? Tell 172.16.10.171 |
| 450 | 7.278715 | MicroStarINT_5c1ca... | Broadcast | ARP | 60 | Who has 172.16.9.63? Tell 172.16.10.118 |
| 452 | 7.321413 | MicroStarINT_5c1cb... | Broadcast | ARP | 60 | Who has 172.16.9.165? Tell 172.16.10.31 |
| 453 | 7.356848 | Dell_3518ff:f8 | Broadcast | ARP | 60 | Who has 172.16.25.180? Tell 172.16.8.180 |
| 454 | 7.356848 | Dell_3518ff:f8 | Broadcast | ARP | 60 | Who has 172.16.6.183? Tell 172.16.8.180 |
| 464 | 7.448499 | MicroStarINT_5c1cb... | Broadcast | ARP | 60 | Who has 172.16.10.48? Tell 172.16.10.43 |
| 480 | 7.538140 | MicroStarINT_5c1cd... | Broadcast | ARP | 60 | Who has 172.16.9.283? Tell 172.16.10.115 |
| 485 | 7.643612 | MicroStarINT_5c1cb... | Broadcast | ARP | 60 | Who has 172.16.10.72? Tell 172.16.11.120 |
| 487 | 7.643612 | MicroStarINT_5c1cb... | Broadcast | ARP | 60 | Who has 172.16.10.93? Tell 172.16.11.120 |
| 492 | 7.769878 | 0ae0:afad:ad15 | Broadcast | ARP | 60 | Who has 172.16.8.1? Tell 172.16.11.200 |
| 506 | 7.983718 | HP_3518ff:f8 | Broadcast | ARP | 60 | Who has 172.16.10.97? Tell 172.16.8.162 |
| 508 | 7.933862 | Pegatron_06:04:32 | Broadcast | ARP | 60 | Who has 172.16.10.69? Tell 172.16.9.147 |
| Frame 75: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF {404F3ACB-9805-4F8C-8036-1A4D501501F1}, Id 0 | | | | | | |
| Address Resolution Protocol Protocol | | | | | | |
| | | | | | Packets: 508 | Displayed: 112 (22.0%) - Dropped: 0 (0.0%) |
| Profile: Default | | | | | | |

Inspecting the packets



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

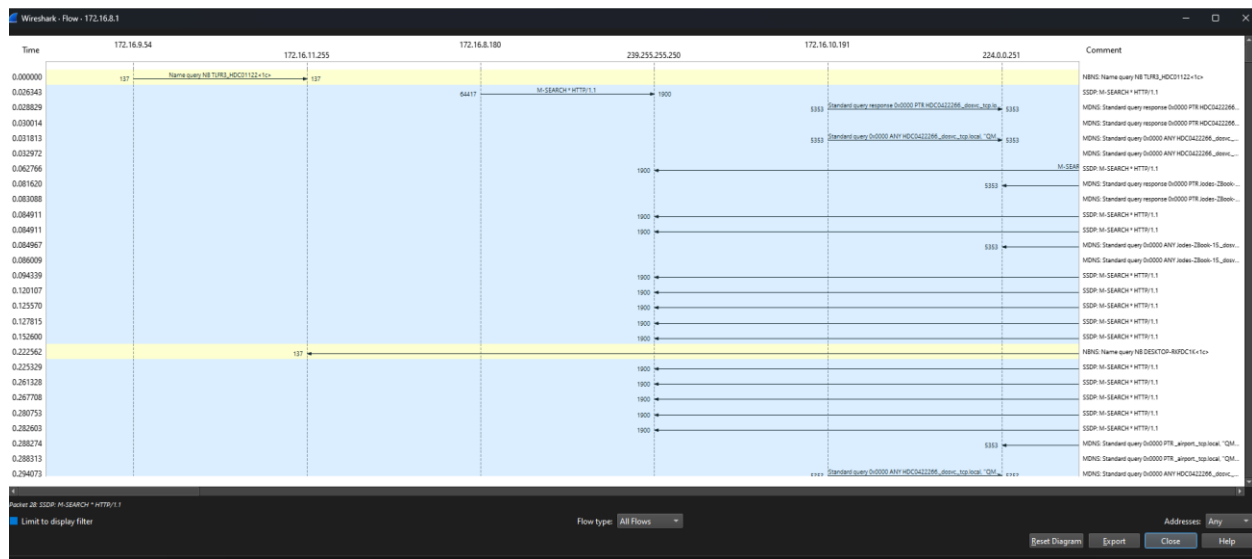
Procedure

- 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


| dns | | | | | |
|-----|----------|--------------|--------------|----------|---|
| No. | Time | Source | Destination | Protocol | Length Info |
| 805 | 5.920690 | 172.16.8.185 | 172.16.8.1 | DNS | 74 Standard query 0x61ca A www.google.com |
| 806 | 5.920859 | 172.16.8.185 | 172.16.8.1 | DNS | 74 Standard query 0xdcea HTTPS www.google.com |
| 807 | 5.922217 | 172.16.8.1 | 172.16.8.185 | DNS | 90 Standard query response 0x61ca A www.google.com A 142.250.196.36 |
| 808 | 5.922217 | 172.16.8.1 | 172.16.8.185 | DNS | 99 Standard query response 0xdcea HTTPS www.google.com HTTPS |

Flow Graph output



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

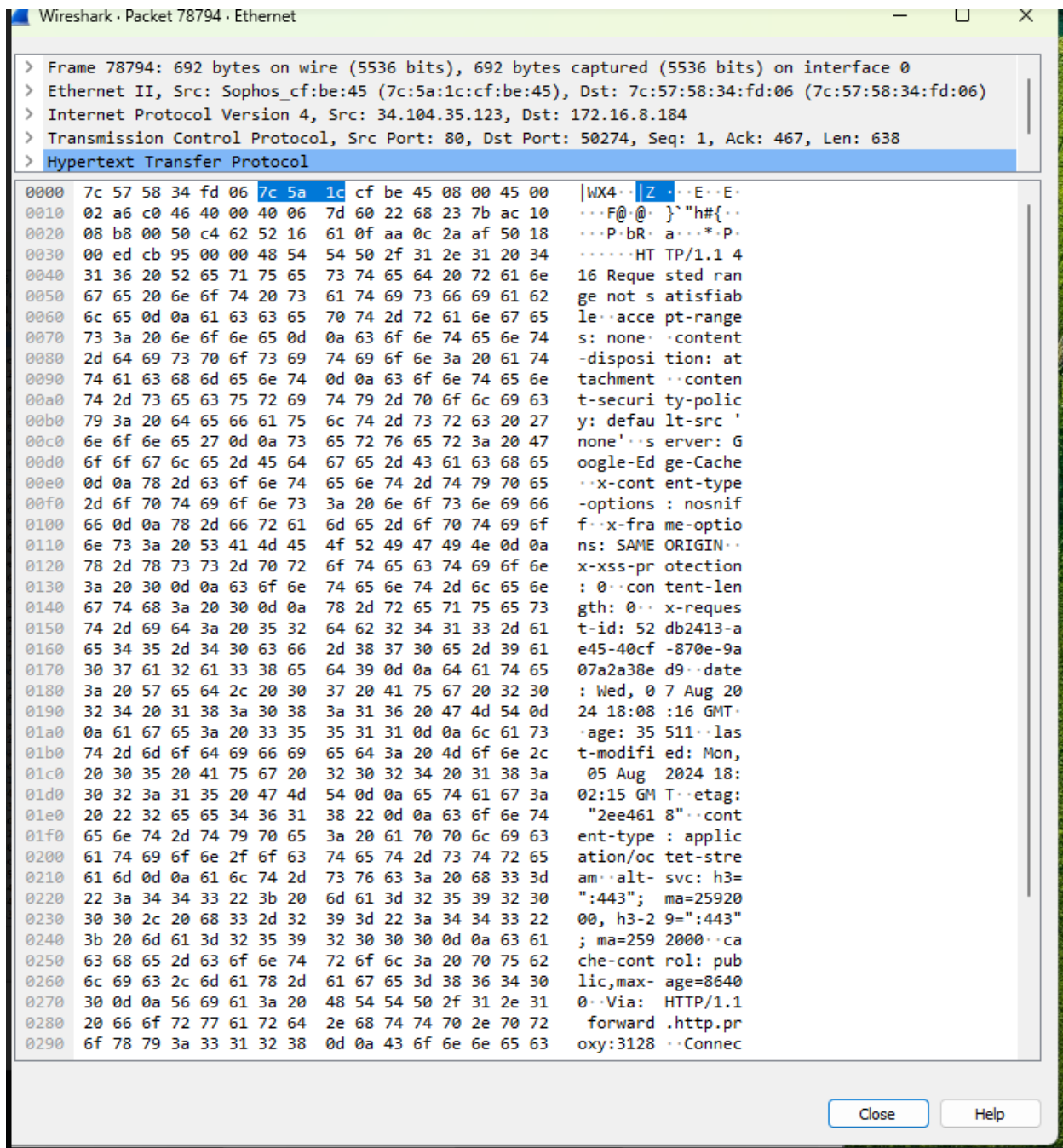
Procedure

- 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.

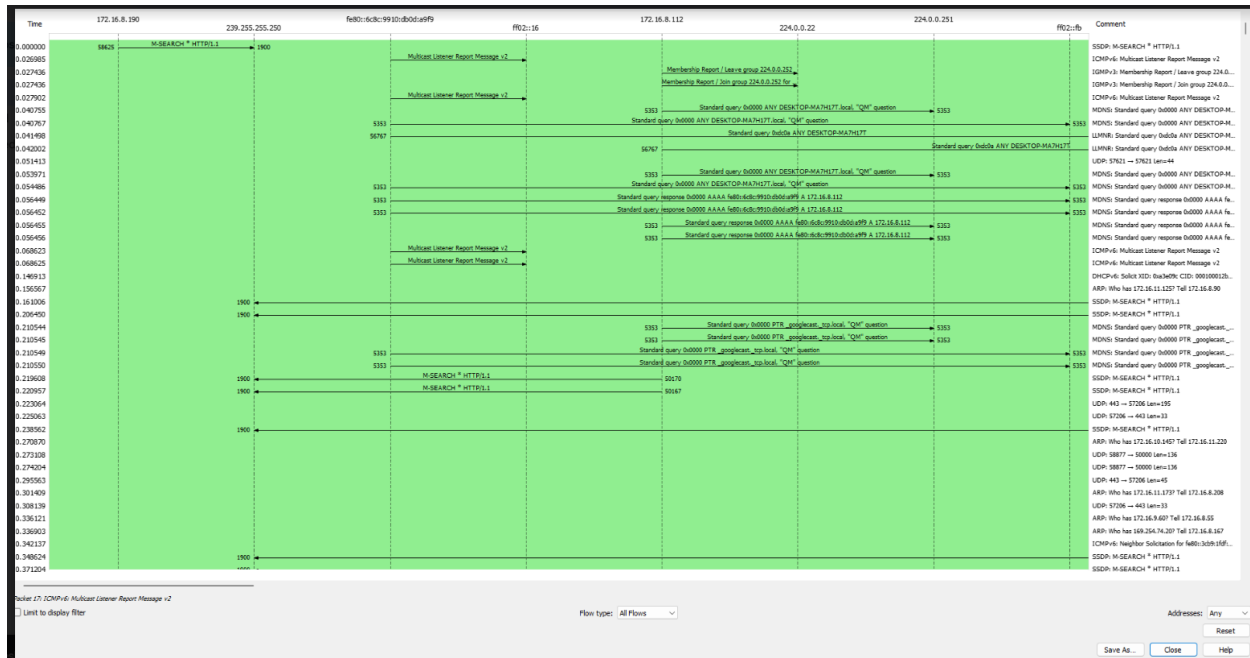
Output

| No. | Time | Source | Destination | Protocol | Length | Info |
|-------|------------|---------------|---------------|----------|--------|---|
| 614 | 7.685024 | 172.16.8.184 | 34.104.35.123 | HTTP | 520 | GET /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e... |
| 617 | 7.698858 | 34.104.35.123 | 172.16.8.184 | HTTP | 731 | HTTP/1.1 416 Requested range not satisfiable |
| 618 | 7.700353 | 172.16.8.184 | 34.104.35.123 | HTTP | 500 | HEAD /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e... |
| 619 | 7.709986 | 34.104.35.123 | 172.16.8.184 | HTTP | 667 | HTTP/1.1 200 OK |
| 624 | 7.742844 | 172.16.8.184 | 34.104.35.123 | HTTP | 520 | GET /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e... |
| 626 | 7.752652 | 34.104.35.123 | 172.16.8.184 | HTTP | 731 | HTTP/1.1 416 Requested range not satisfiable |
| 627 | 7.754181 | 172.16.8.184 | 34.104.35.123 | HTTP | 500 | HEAD /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e... |
| 630 | 7.764711 | 34.104.35.123 | 172.16.8.184 | HTTP | 706 | HTTP/1.1 200 OK |
| 634 | 7.790436 | 172.16.8.184 | 34.104.35.123 | HTTP | 520 | GET /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e... |
| 635 | 7.799887 | 34.104.35.123 | 172.16.8.184 | HTTP | 731 | HTTP/1.1 416 Requested range not satisfiable |
| 636 | 7.801361 | 172.16.8.184 | 34.104.35.123 | HTTP | 500 | HEAD /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e... |
| 637 | 7.809151 | 34.104.35.123 | 172.16.8.184 | HTTP | 667 | HTTP/1.1 200 OK |
| 639 | 7.838248 | 172.16.8.184 | 34.104.35.123 | HTTP | 520 | GET /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e... |
| 642 | 7.852555 | 34.104.35.123 | 172.16.8.184 | HTTP | 692 | HTTP/1.1 416 Requested range not satisfiable |
| 643 | 7.854134 | 172.16.8.184 | 34.104.35.123 | HTTP | 500 | HEAD /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e... |
| 645 | 7.871249 | 34.104.35.123 | 172.16.8.184 | HTTP | 706 | HTTP/1.1 200 OK |
| 648 | 7.901837 | 172.16.8.184 | 34.104.35.123 | HTTP | 520 | GET /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e... |
| 649 | 7.912361 | 34.104.35.123 | 172.16.8.184 | HTTP | 731 | HTTP/1.1 416 Requested range not satisfiable |
| 650 | 7.914442 | 172.16.8.184 | 34.104.35.123 | HTTP | 500 | HEAD /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e... |
| 651 | 7.922388 | 34.104.35.123 | 172.16.8.184 | HTTP | 667 | HTTP/1.1 200 OK |
| 652 | 7.949279 | 172.16.8.184 | 34.104.35.123 | HTTP | 520 | GET /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e... |
| 654 | 7.961780 | 34.104.35.123 | 172.16.8.184 | HTTP | 731 | HTTP/1.1 416 Requested range not satisfiable |
| 655 | 7.963277 | 172.16.8.184 | 34.104.35.123 | HTTP | 500 | HEAD /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e... |
| 658 | 7.973876 | 34.104.35.123 | 172.16.8.184 | HTTP | 706 | HTTP/1.1 200 OK |
| 5969 | 68.003432 | 172.16.8.184 | 34.104.35.123 | HTTP | 520 | GET /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e... |
| 5975 | 68.021813 | 34.104.35.123 | 172.16.8.184 | HTTP | 692 | HTTP/1.1 416 Requested range not satisfiable |
| 5977 | 68.022279 | 172.16.8.184 | 34.104.35.123 | HTTP | 500 | HEAD /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e... |
| 5982 | 68.037182 | 34.104.35.123 | 172.16.8.184 | HTTP | 706 | HTTP/1.1 200 OK |
| 6000 | 68.060979 | 172.16.8.184 | 34.104.35.123 | HTTP | 520 | GET /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e... |
| 6009 | 68.075015 | 34.104.35.123 | 172.16.8.184 | HTTP | 731 | HTTP/1.1 416 Requested range not satisfiable |
| 6010 | 68.075735 | 172.16.8.184 | 34.104.35.123 | HTTP | 500 | HEAD /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e... |
| 6012 | 68.095897 | 34.104.35.123 | 172.16.8.184 | HTTP | 706 | HTTP/1.1 200 OK |
| 6016 | 68.113543 | 172.16.8.184 | 34.104.35.123 | HTTP | 520 | GET /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e... |
| 6020 | 68.127351 | 34.104.35.123 | 172.16.8.184 | HTTP | 692 | HTTP/1.1 416 Requested range not satisfiable |
| 6022 | 68.128754 | 172.16.8.184 | 34.104.35.123 | HTTP | 500 | HEAD /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e... |
| 6026 | 68.147978 | 34.104.35.123 | 172.16.8.184 | HTTP | 706 | HTTP/1.1 200 OK |
| 6027 | 68.165225 | 172.16.8.184 | 34.104.35.123 | HTTP | 520 | GET /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e... |
| 6031 | 68.178231 | 34.104.35.123 | 172.16.8.184 | HTTP | 692 | HTTP/1.1 416 Requested range not satisfiable |
| 6032 | 68.179227 | 172.16.8.184 | 34.104.35.123 | HTTP | 500 | HEAD /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e... |
| 6033 | 68.191504 | 34.104.35.123 | 172.16.8.184 | HTTP | 667 | HTTP/1.1 200 OK |
| 6036 | 68.212702 | 172.16.8.184 | 34.104.35.123 | HTTP | 520 | GET /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e... |
| 6037 | 68.221863 | 34.104.35.123 | 172.16.8.184 | HTTP | 731 | HTTP/1.1 416 Requested range not satisfiable |
| 6038 | 68.222707 | 172.16.8.184 | 34.104.35.123 | HTTP | 500 | HEAD /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e... |
| 6040 | 68.232365 | 34.104.35.123 | 172.16.8.184 | HTTP | 667 | HTTP/1.1 200 OK |
| 6047 | 68.260625 | 172.16.8.184 | 34.104.35.123 | HTTP | 520 | GET /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e... |
| 6048 | 68.269573 | 34.104.35.123 | 172.16.8.184 | HTTP | 692 | HTTP/1.1 416 Requested range not satisfiable |
| 6049 | 68.270838 | 172.16.8.184 | 34.104.35.123 | HTTP | 500 | HEAD /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e... |
| 6050 | 68.282851 | 34.104.35.123 | 172.16.8.184 | HTTP | 706 | HTTP/1.1 200 OK |
| 13471 | 128.310870 | 172.16.8.184 | 34.104.35.123 | HTTP | 520 | GET /edgedl/diffgen-puffin/lmelglejhemejginpboagddgdfbepgmp/1.54491a53303afa6612e... |
| 13475 | 128.326936 | 34.104.35.123 | 172.16.8.184 | HTTP | 731 | HTTP/1.1 416 Requested range not satisfiable |

Inspecting the packets



Flow Graph output



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

Procedure

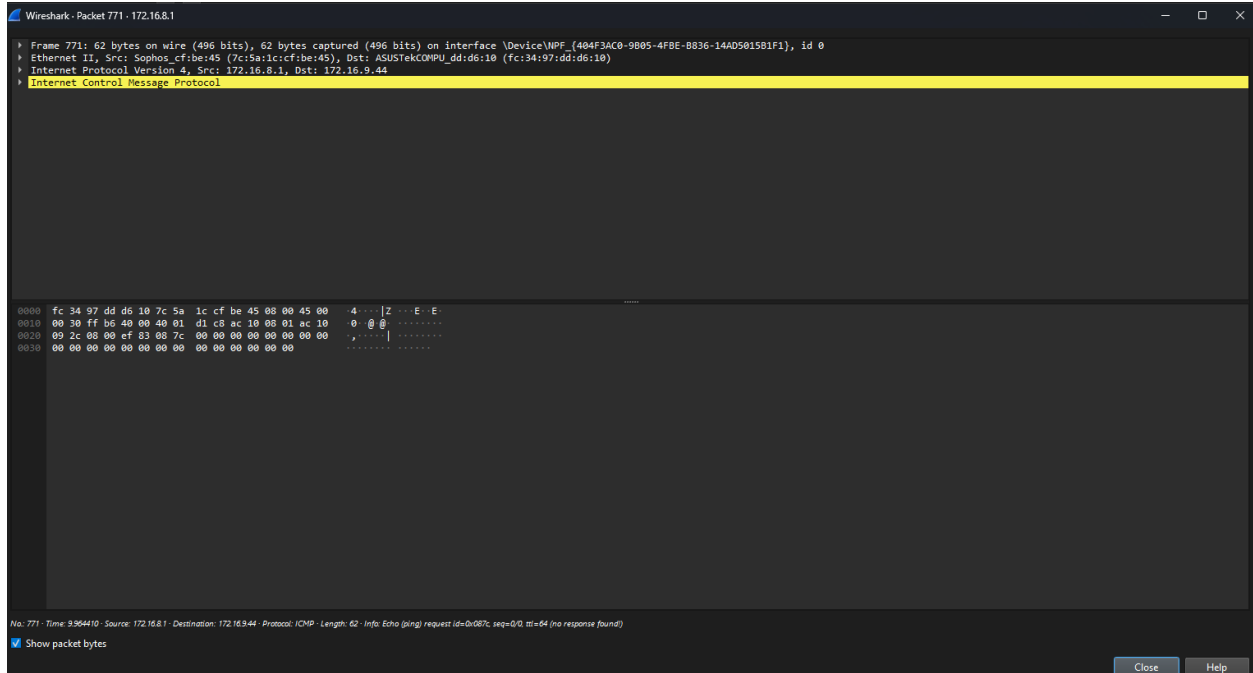
- Select Local Area Connection in Wireshark.
- Go to capture □ option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search ICMP/IP packets in search bar.
- Save the packets

Output:icmp

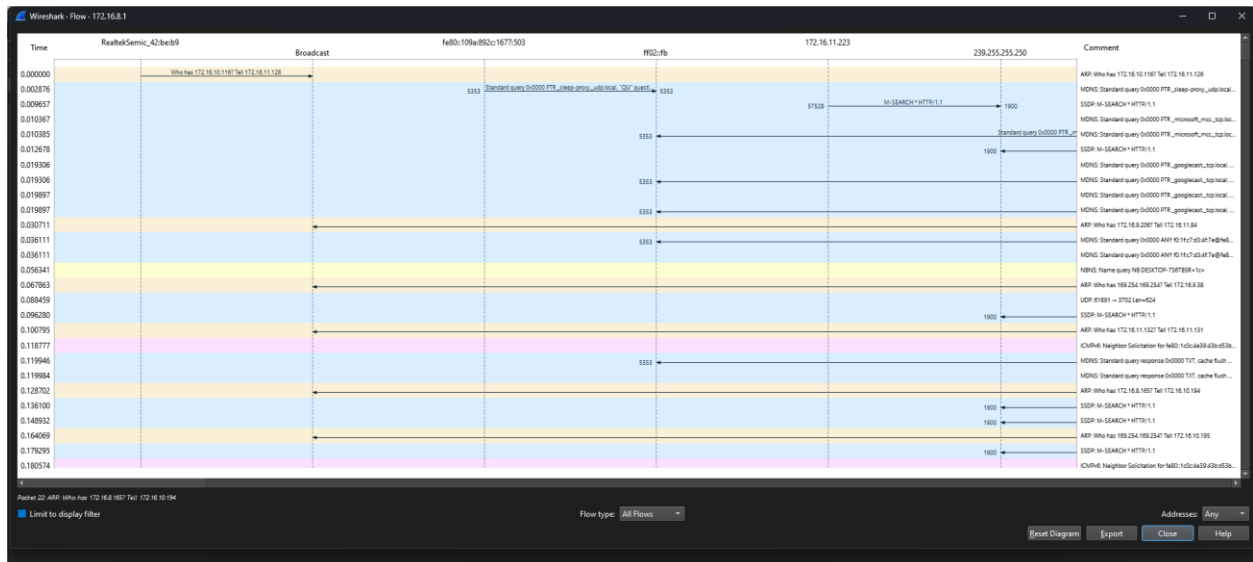
| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|------------|-------------|----------|--------|---|
| 771 | 9.964410 | 172.16.8.1 | 172.16.9.44 | ICMP | 62 | Echo (ping) request id=0x087c, seq=0/0, ttl=64 (no response found!) |

Inspecting the packets

CS23532-COMPUTER NETWORKS



Flow Graph output



Output:ip

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|-----------------|-----------------|-----------|--------|--|
| 8 | 0.850881 | 142.250.182.142 | 172.16.0.185 | UDP | 68 | 443 → 63346 Len=26 |
| 9 | 0.871925 | 142.250.182.142 | 172.16.0.185 | UDP | 140 | 443 → 63346 Len=106 |
| 10 | 0.872709 | 142.250.182.142 | 172.16.0.185 | UDP | 262 | 443 → 63346 Len=230 |
| 11 | 0.872920 | 172.16.11.126 | 239.255.255.250 | SSDP | 217 | N-SEARCH * HTTP/1.1 |
| 12 | 0.873130 | 172.16.0.185 | 142.250.182.142 | UDP | 81 | 63346 → 443 Len=39 |
| 13 | 0.874281 | 172.16.9.128 | 239.255.255.250 | SSDP | 216 | N-SEARCH * HTTP/1.1 |
| 14 | 0.877033 | 142.250.182.142 | 172.16.0.185 | UDP | 68 | 443 → 63346 Len=26 |
| 18 | 0.180149 | 172.16.0.232 | 239.255.255.250 | SSDP | 217 | N-SEARCH * HTTP/1.1 |
| 19 | 0.209299 | 172.16.11.129 | 239.255.255.250 | SSDP | 216 | N-SEARCH * HTTP/1.1 |
| 21 | 0.262665 | 172.16.11.239 | 239.255.255.250 | SSDP | 216 | N-SEARCH * HTTP/1.1 |
| 22 | 0.266689 | 172.16.8.226 | 239.255.255.250 | SSDP | 218 | N-SEARCH * HTTP/1.1 |
| 23 | 0.266689 | 172.16.11.83 | 239.255.255.250 | SSDP | 216 | N-SEARCH * HTTP/1.1 |
| 24 | 0.269077 | 172.16.0.231 | 239.255.255.250 | SSDP | 52 | Name query 00 LARTOP-FHW03151c< |
| 25 | 0.279369 | 172.16.8.185 | 142.250.182.142 | UDP | 71 | 63346 → 443 Len=29 |
| 26 | 0.284225 | 142.250.182.142 | 172.16.0.185 | UDP | 68 | 443 → 63346 Len=26 |
| 27 | 0.316531 | 172.16.0.137 | 239.255.255.250 | SSDP | 216 | N-SEARCH * HTTP/1.1 |
| 29 | 0.342059 | 172.16.8.169 | 239.255.255.250 | SSDP | 217 | N-SEARCH * HTTP/1.1 |
| 30 | 0.353355 | 172.16.9.89 | 239.255.255.250 | SSDP | 217 | N-SEARCH * HTTP/1.1 |
| 31 | 0.360149 | 172.16.10.190 | 239.255.255.250 | SSDP | 216 | N-SEARCH * HTTP/1.1 |
| 32 | 0.367863 | 172.16.11.4 | 239.255.255.250 | SSDP | 216 | N-SEARCH * HTTP/1.1 |
| 35 | 0.419262 | 172.16.0.182 | 239.255.255.250 | SSDP | 216 | N-SEARCH * HTTP/1.1 |
| 36 | 0.440731 | 172.16.10.196 | 239.255.255.250 | SSDP | 217 | N-SEARCH * HTTP/1.1 |
| 37 | 0.442081 | 172.16.0.219 | 239.255.255.250 | SSDP | 216 | N-SEARCH * HTTP/1.1 |
| 38 | 0.447340 | 172.16.8.32 | 239.255.255.250 | SSDP | 217 | N-SEARCH * HTTP/1.1 |
| 39 | 0.500999 | 172.16.0.185 | 142.250.182.142 | UDP | 71 | 63346 → 443 Len=29 |
| 41 | 0.509941 | 142.250.182.142 | 172.16.0.185 | UDP | 68 | 443 → 63346 Len=26 |
| 44 | 0.543334 | 172.16.10.43 | 239.255.255.250 | SSDP | 216 | N-SEARCH * HTTP/1.1 |
| 47 | 0.632959 | 172.16.11.138 | 239.255.255.250 | SSDP | 217 | N-SEARCH * HTTP/1.1 |
| 48 | 0.626380 | 172.16.10.172 | 239.255.255.250 | SSDP | 212 | N-SEARCH * HTTP/1.1 |
| 49 | 0.627654 | 172.16.8.163 | 172.16.11.255 | NRPS | 92 | Name query 00 DESKTOP-RKFD1K1c< |
| 50 | 0.649554 | 172.16.8.16 | 239.255.255.250 | SSDP | 217 | N-SEARCH * HTTP/1.1 |
| 51 | 0.649162 | 172.16.9.171 | 239.255.255.250 | SSDP | 217 | N-SEARCH * HTTP/1.1 |
| 52 | 0.651986 | 172.16.0.112 | 239.255.255.250 | SSDP | 216 | N-SEARCH * HTTP/1.1 |
| 53 | 0.683616 | 172.16.0.112 | 239.255.255.250 | SSDP | 217 | N-SEARCH * HTTP/1.1 |
| 54 | 0.696278 | 172.16.8.178 | 239.255.255.250 | SSDP | 217 | N-SEARCH * HTTP/1.1 |
| 55 | 0.696362 | 172.16.9.6 | 239.255.255.250 | SSDP | 216 | N-SEARCH * HTTP/1.1 |
| 56 | 0.707180 | 172.16.8.185 | 142.250.182.142 | UDP | 71 | 63346 → 443 Len=29 |
| 57 | 0.712836 | 142.250.182.142 | 172.16.0.185 | UDP | 68 | 443 → 63346 Len=26 |
| 59 | 0.721196 | 172.16.0.238 | 239.255.255.250 | SSDP | 216 | N-SEARCH * HTTP/1.1 |
| 60 | 0.737464 | 172.16.10.219 | 224.0.0.252 | LUNMR | 70 | Standard query 0xc6f1 A HDC1817444 |
| 62 | 0.739562 | 172.16.10.219 | 224.0.0.252 | LUNMR | 70 | Standard query 0xc6ff AAAA HDC1817444 |
| 64 | 0.739707 | 172.16.9.75 | 239.255.255.250 | SSDP | 216 | N-SEARCH * HTTP/1.1 |
| 65 | 0.750119 | 172.16.10.219 | 224.0.0.252 | LUNMR | 70 | Standard query 0x4662 A HDC1817444 |
| 67 | 0.751187 | 172.16.10.219 | 224.0.0.252 | LUNMR | 70 | Standard query 0x5666 AAAA HDC1817444 |
| 69 | 0.764152 | 172.16.10.219 | 172.16.11.255 | BROADCAST | 220 | Request Announcement VISFEL2 |
| 70 | 0.769628 | 172.16.0.218 | 224.0.0.251 | PINGS | 220 | Standard query response 0x0000 PTR Jodes-2Book-15_dosvc_tcp.local SRV 0 7680 Jodes-2Book-15.local TXT |
| 72 | 0.771823 | 172.16.8.218 | 224.0.0.251 | PINGS | 82 | Standard query 0x0000 ANY Jodes-2Book-15_dosvc_tcp.local, "QM" question |
| 74 | 0.775339 | 172.16.9.174 | 172.16.11.255 | BROADCAST | 243 | Local Master Announcement HDC1817444, Workstation, Server, NT Workstation, Potential Browser, Backup Browser, Master Browser |
| 75 | 0.786882 | 172.16.10.219 | 224.0.0.252 | LUNMR | 70 | Standard query 0xc244 A HDC1817444 |
| 76 | 0.786882 | 172.16.10.219 | 224.0.0.252 | LUNMR | 70 | Standard query 0x7645 AAAA HDC1817444 |
| 77 | 0.786882 | 172.16.10.219 | 224.0.0.252 | LUNMR | 70 | Standard query 0xc572 A HDC1817444 |
| 78 | 0.786882 | 172.16.10.219 | 224.0.0.252 | LUNMR | 70 | Standard query 0xc791 AAAA HDC1817444 |
| 79 | 0.786882 | 172.16.10.219 | 224.0.0.252 | LUNMR | 70 | Standard query 0x4816 A HDC1817444 |
| 80 | 0.786882 | 172.16.10.219 | 224.0.0.252 | LUNMR | 70 | Standard query 0xc41d AAAA HDC1817444 |
| 83 | 0.786964 | 172.16.8.238 | 239.255.255.250 | SSDP | 217 | N-SEARCH * HTTP/1.1 |
| 88 | 0.786964 | 172.16.10.219 | 172.16.11.255 | BROADCAST | 220 | Request Announcement VISFEL2 |

Inspecting the packets

Wireshark - Packet 47 - 172.16.8.1

Frame 47: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface \Device\NPF{404F3AC0-9B05-4FBE-B836-14A05015B1F1}, id 0

Ethernet II, Src: 0a:00:a1:01:9e:0a (0a:00:a1:01:9e:0a), Dst: IPv4multicast 7f:ff:fa (01:00:5e:7f:ff:fa)

Internet Protocol Version 4, Src: 172.16.11.138, Dst: 239.255.255.250

User Datagram Protocol, Src Port: 59614, Dst Port: 1900

Simple Service Discovery Protocol

```

0000  01 00 5e 7f ff fa 0a e0 af ca 01 9e 08 00 45 00  ..A.....E
0010  00 cb c9 88 00 00 01 11 48 05 ac 10 0b 8a ef ff  ....H.....
0020  ff fa 8e 07 6c 00 b7 e1 fe 4d 2d 53 45 41 52    ...I...N-SEAR
0030  43 45 20 2a 20 42 54 54 50 2f 31 2e 31 0d 0a 4b  CH + HTTP/1.1 N
0040  4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35  OST: 239.255.255
0050  2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20  .250:190 0 MAN:
0060  22 73 73 64 70 3a 64 69 73 6f 76 65 72 22 0d  "ssdpdiscover"
0070  0a 4d 50 3a 20 31 0d 0a 63 64 3a 20 75 72 6e 3a  PKG: 1 ST: urn:
0080  64 69 61 6c 2d 6d 75 6c 74 69 73 63 72 65 65 6e  dial-multiscreen
0090  2d 6f 72 67 3a 73 65 72 76 69 63 65 3a 64 69 61  -org:serviceid:
00a0  6c 3a 31 0d 0a 55 53 45 52 2d 41 47 45 4e 54 3a  I:1 USE-AGENT:
00b0  20 4d 69 63 72 64 72 6f 66 74 20 45 64 67 65 2f  MicrosofEdge/
00c0  31 37 2e 30 2e 32 36 35 31 2e 38 36 20 57 69    127.0.26.51.86 W
00d0  6e 64 6f 77 73 0d 0a 0d 0a                      ndows

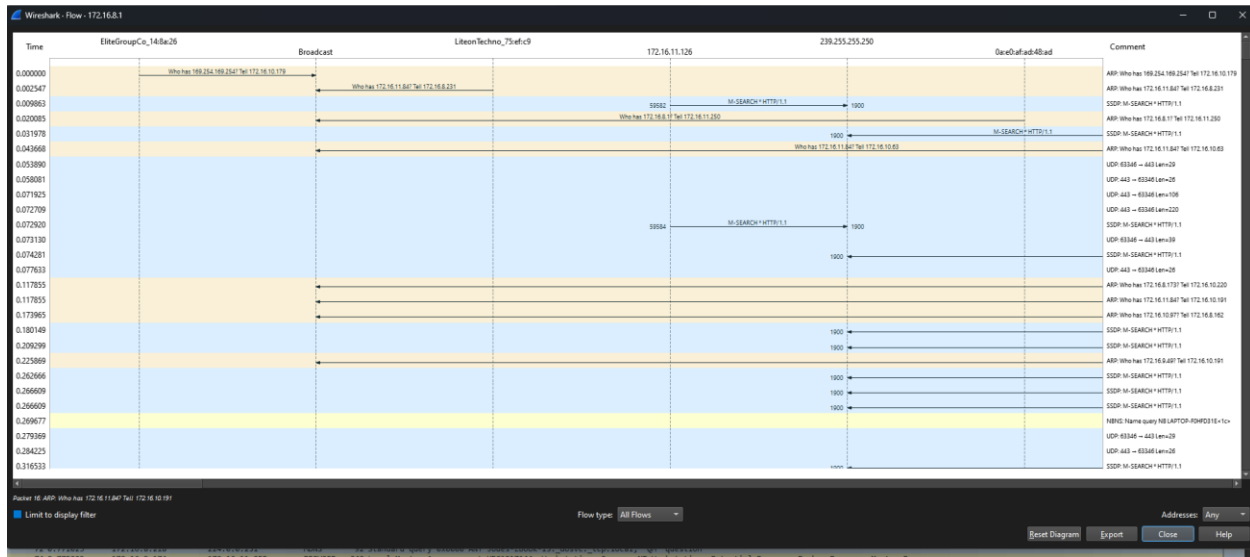
```

No. 47: Time: 0.619969 Source: 172.16.11.138 Destination: 239.255.255.250 Protocol: SSDP Length: 217 Info: N-SEARCH * HTTP/1.1

Show packet bytes

Close Help

Flow chart 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

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------|---------|-----------------|----------|--------|---|
| 770 | 9.964409 | 0.0.0.0 | 255.255.255.255 | DHCP | 340 | DHCP Discover - Transaction ID 0xf19cf3d1 |
| 852 | 10.953009 | 0.0.0.0 | 255.255.255.255 | DHCP | 350 | DHCP Request - Transaction ID 0xf19cf3d1 |
| 1028 | 15.338473 | 0.0.0.0 | 255.255.255.255 | DHCP | 364 | DHCP Request - Transaction ID 0x34abb62d |

Inspecting the packets

