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:

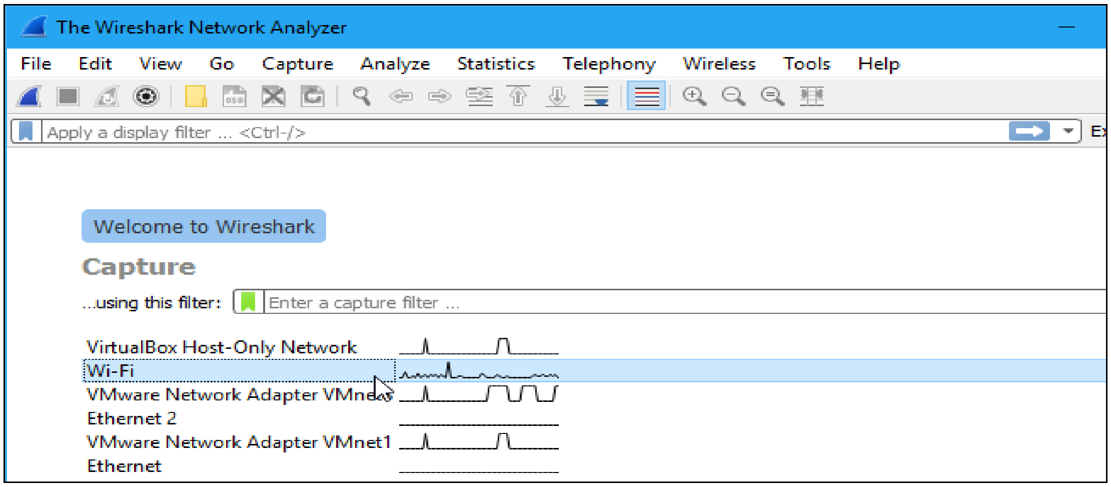
- Network administrators: troubleshoot network problems
- Network security engineers: examine security problems
- Developers: debug protocol implementations
- People: learn **network protocol internals**

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

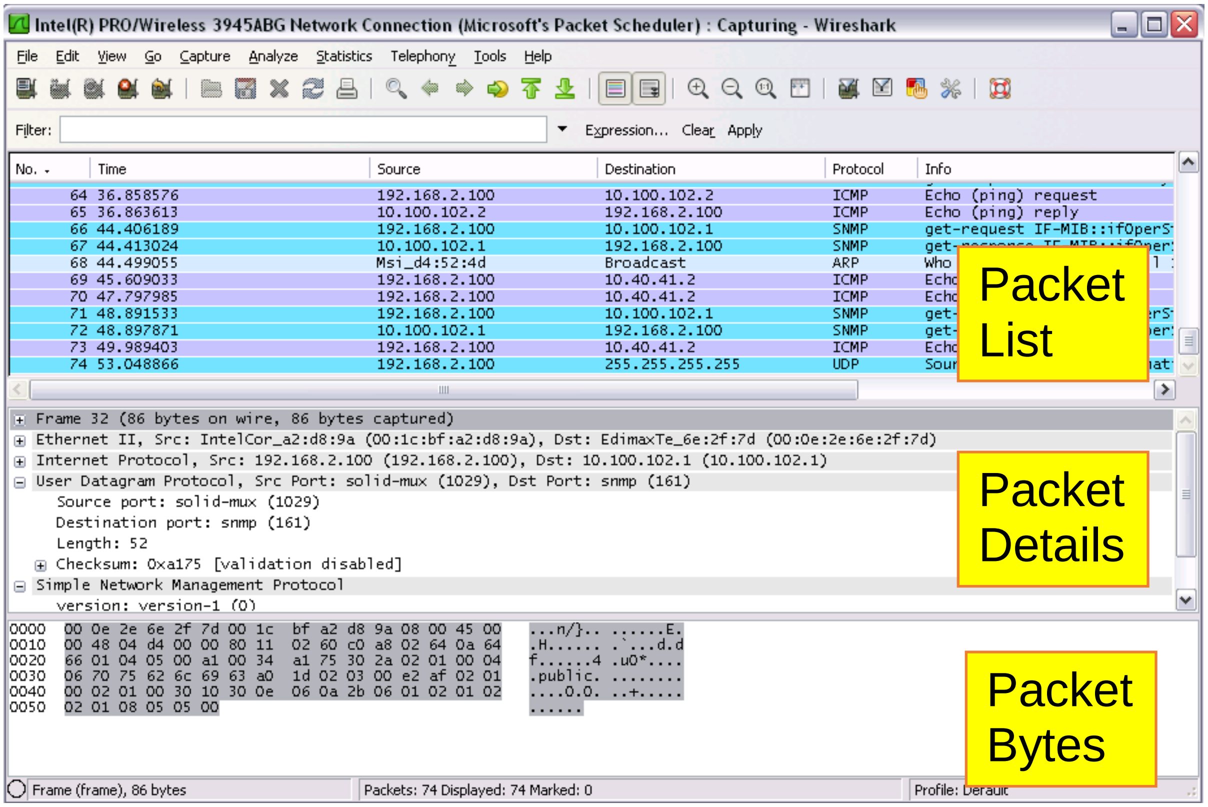
After downloading and installing Wireshark, launch it and double-click the name of a network interface under Capture to start capturing packets on that interface



```
VirtualBox Host-Only Network
Wi-Fi
VMware Network Adapter VMnet
Ethernet 2
VMware Network Adapter VMnet1
Ethernet
```

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.



```
No. -   Time        Source            Destination        Protocol  Info
     64 36.858576   192.168.2.100     10.100.102.2       ICMP      Echo (ping) request
     65 36.863613   10.100.102.2      192.168.2.100      ICMP      Echo (ping) reply
     66 44.406189   192.168.2.100     10.100.102.1       SNMP      get-request IF-MIB::ifOperS
     67 44.413024   10.100.102.1      192.168.2.100      SNMP      get-response IF-MIB::ifOper
     68 44.499055   Msi_d4:52:4d      Broadcast          ARP       Who
     69 45.609033   192.168.2.100     10.40.41.2         ICMP      Echo
     70 47.797985   192.168.2.100     10.40.41.2         ICMP      Echo
     71 48.891533   192.168.2.100     10.100.102.1       SNMP      get-
     72 48.897871   10.100.102.1      192.168.2.100      SNMP      get-
     73 49.989403   192.168.2.100     10.40.41.2         ICMP      Echo
     74 53.048866   192.168.2.100     255.255.255.255    UDP       Sour
```

```
+ Frame 32 (86 bytes on wire, 86 bytes captured)
+ Ethernet II, Src: IntelCor_a2:d8:9a (00:1c:bf:a2:d8:9a), Dst: EdimaxTe_6e:2f:7d (00:0e:2e:6e:2f:7d)
+ Internet Protocol, Src: 192.168.2.100 (192.168.2.100), Dst: 10.100.102.1 (10.100.102.1)
- User Datagram Protocol, Src Port: solid-mux (1029), Dst Port: snmp (161)
    Source port: solid-mux (1029)
    Destination port: snmp (161)
    Length: 52
  + Checksum: 0xa175 [validation disabled]
- Simple Network Management Protocol
    version: version-1 (0)
```

```
0000  00 0e 2e 6e 2f 7d 00 1c  bf a2 d8 9a 08 00 45 00   ...n/}.. ......E.
0010  00 48 04 d4 00 00 80 11  02 60 c0 a8 02 64 0a 64   .H...... .`...d.d
0020  66 01 04 05 00 a1 00 34  a1 75 30 2a 02 01 00 04   f......4 .u0*....
0030  06 70 75 62 6c 69 63 a0  1d 02 03 00 e2 af 02 01   .public. ........
0040  00 02 01 00 30 10 30 0e  06 0a 2b 06 01 02 01 02   ....0.0. ..+.....
0050  02 01 08 05 05 00                                  ......
```

```
Frame (frame), 86 bytes    Packets: 74 Displayed: 74 Marked: 0    Profile: Default
```

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.

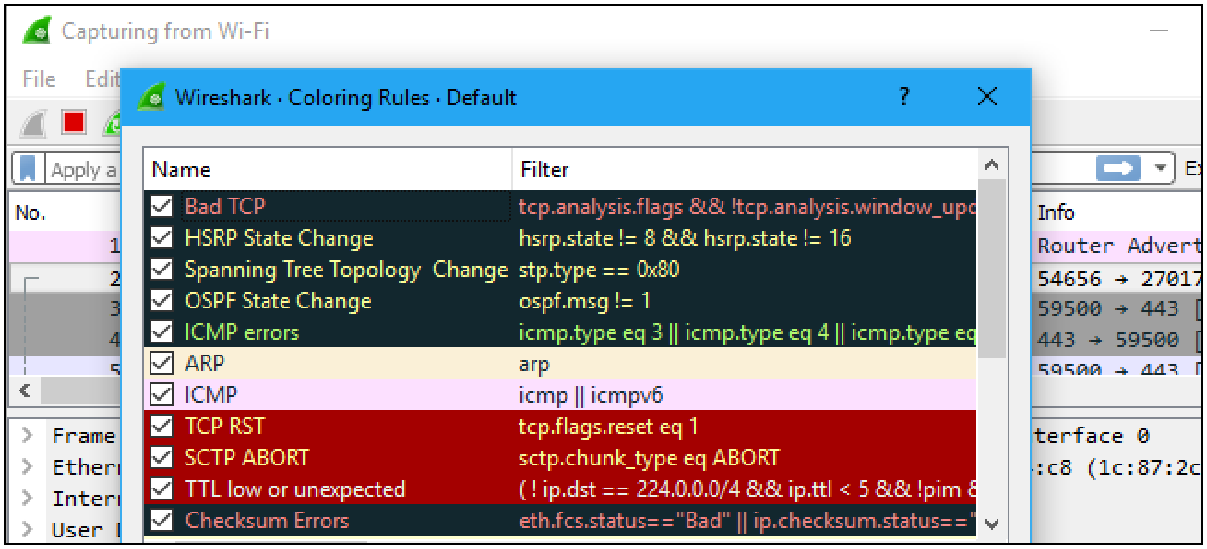
The “Packet Bytes” Pane

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.

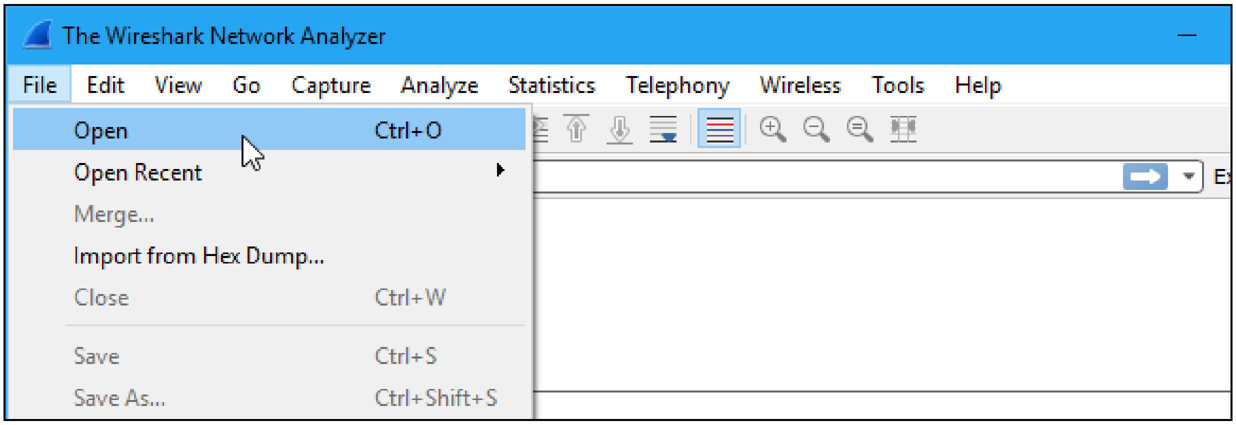


Name	Filter
☑ Bad TCP	tcp.analysis.flags && !tcp.analysis.window_upd
☑ HSRP State Change	hsrp.state != 8 && hsrp.state != 16
☑ Spanning Tree Topology Change	stp.type == 0x80
☑ OSPF State Change	ospf.msg != 1
☑ ICMP errors	icmp.type eq 3 || icmp.type eq 4 || icmp.type eq
☑ ARP	arp
☑ ICMP	icmp || icmpv6
☑ TCP RST	tcp.flags.reset eq 1
☑ SCTP ABORT	sctp.chunk_type eq ABORT
☑ TTL low or unexpected	(! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim &
☑ Checksum Errors	eth.fcs.status=="Bad" || ip.checksum.status=="

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.

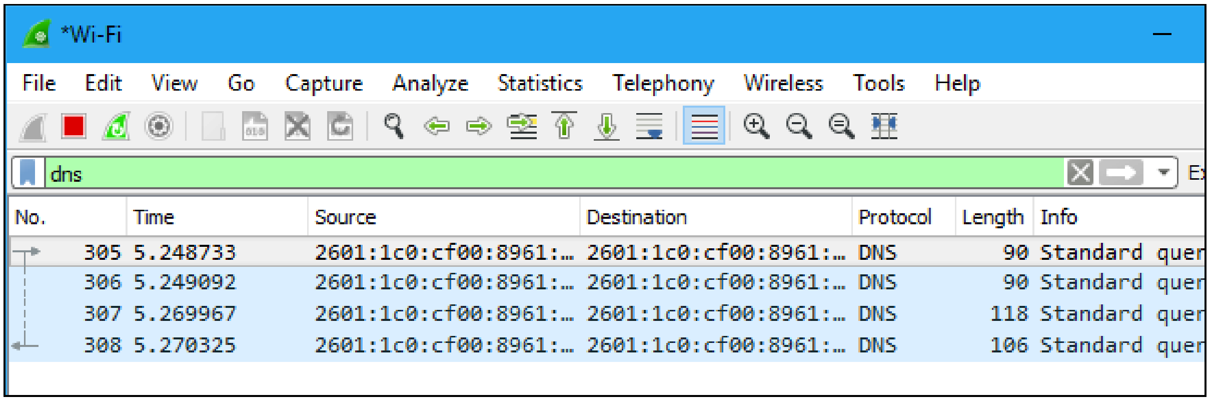
You can also save your own captures in Wireshark and open them later. Click File > Save to save your captured packets.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Open Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Ctrl+Shift+S
Ex

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.

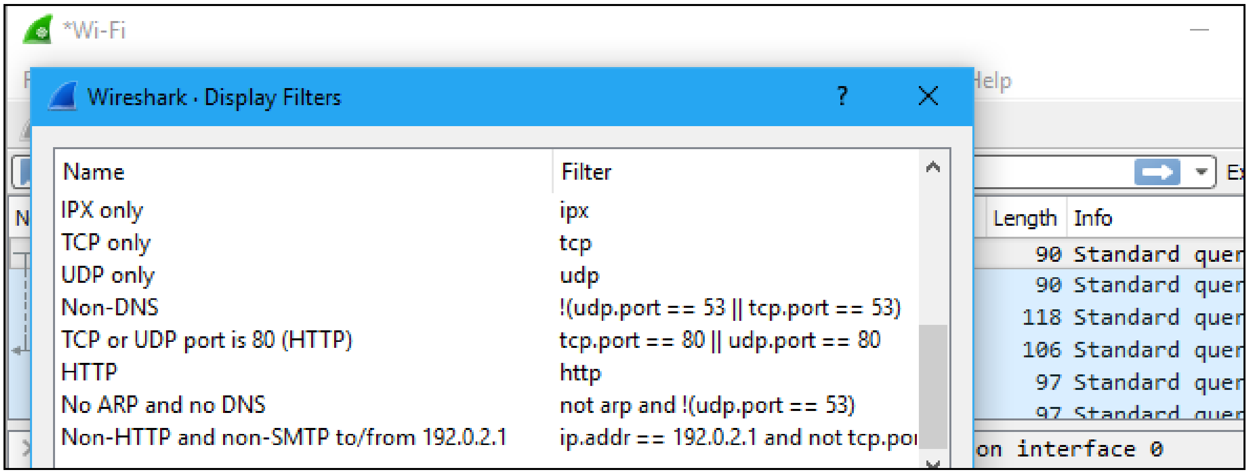
The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type “dns” and you’ll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.



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

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

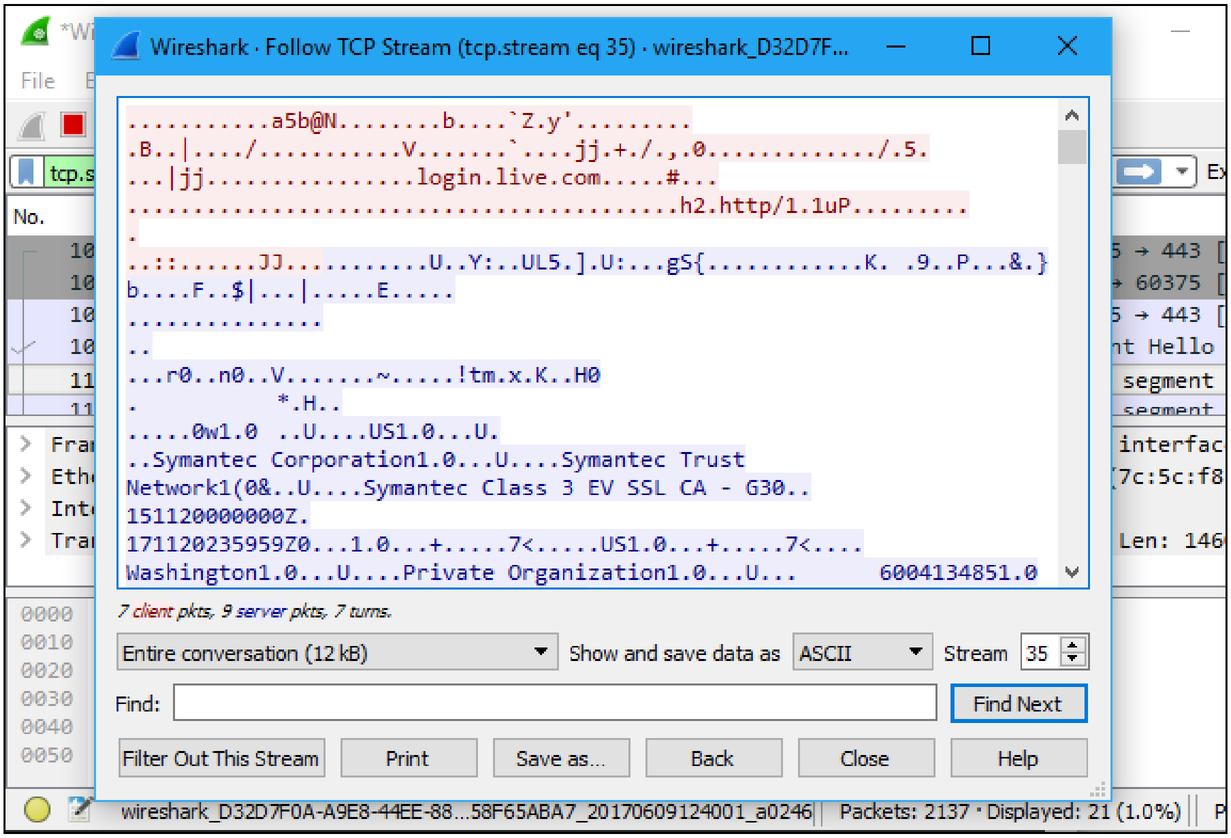
For more information on Wireshark’s display filtering language, read the Building display filter expressions page in the official Wireshark documentation.



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

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

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



Wireshark · Follow TCP Stream (tcp.stream eq 35) · wireshark_D32D7F...
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

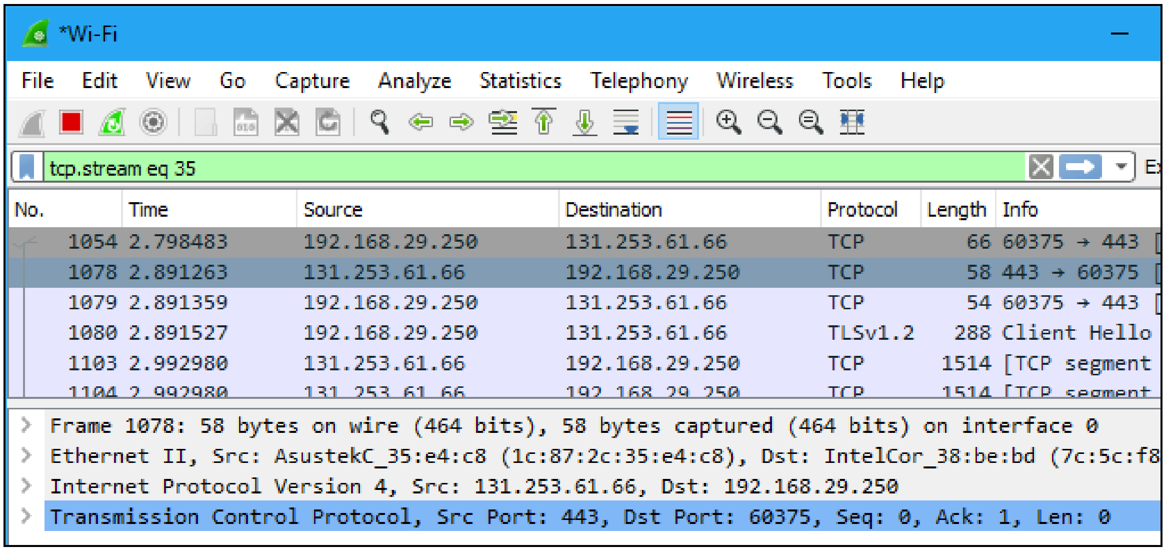
```
...........a5b@N........b....`Z.y'.........
.B..|..../...........V........`....jj.+./.,.0.............../.5.
...|jj................login.live.com.....#...
.........................................h2.http/1.1uP.........
.
..::......JJ.............U..Y:..UL5.].U:...gS{............K. .9..P...&.}
b....F..$|...|.....E.....
...............
..
...r0..n0..V.......~.....!tm.x.K..H0
.          *.H..
.....0w1.0  ..U....US1.0...U.
..Symantec Corporation1.0...U....Symantec Trust
Network1(0&..U....Symantec Class 3 EV SSL CA - G30..
151120000000Z.
171120235959Z0...1.0...+.....7<.....US1.0...+.....7<....
Washington1.0...U....Private Organization1.0...U...      6004134851.0
```

7 client pkts, 9 server pkts, 7 turns.

Entire conversation (12 kB) · Show and save data as ASCII · Stream 35

wireshark_D32D7F0A-A9E8-44EE-88...58F65ABA7_20170609124001_a0246 | Packets: 2137 · Displayed: 21 (1.0%)

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



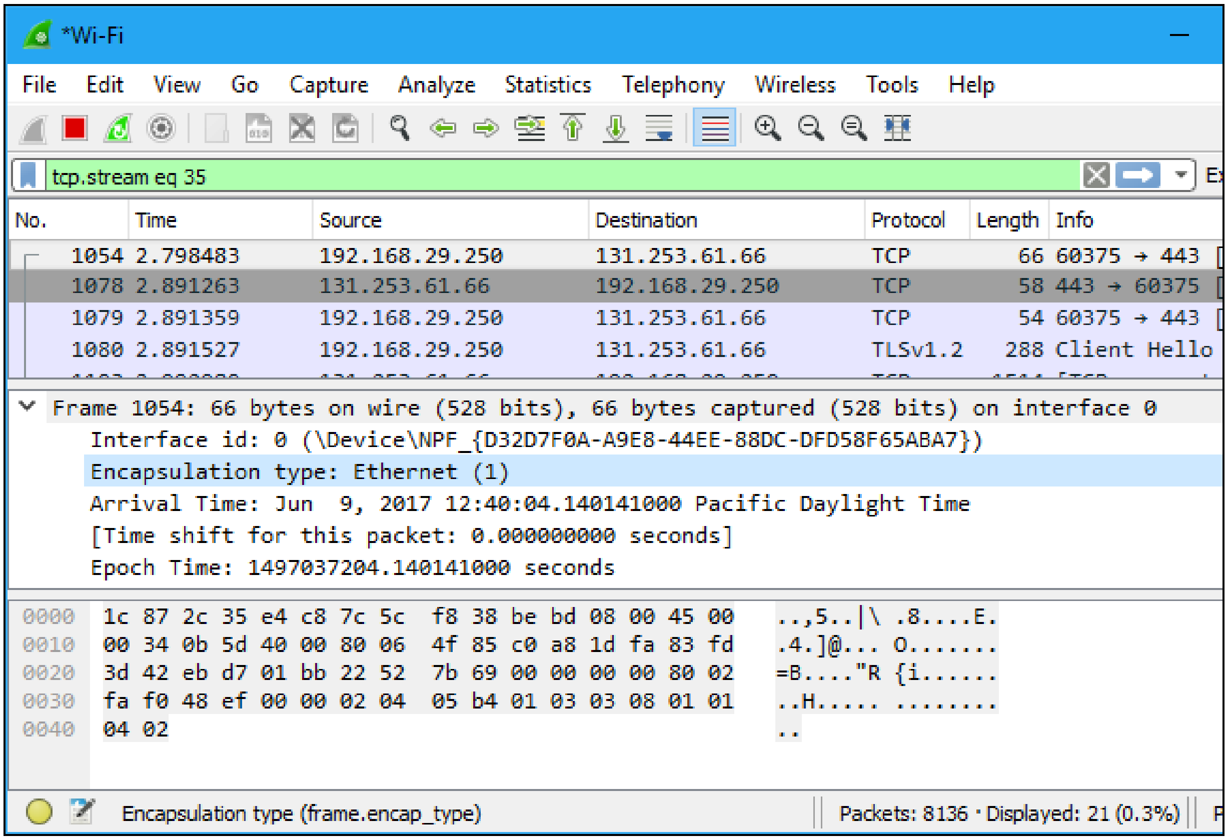
tcp.stream eq 35

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

```
> 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.



tcp.stream eq 35

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

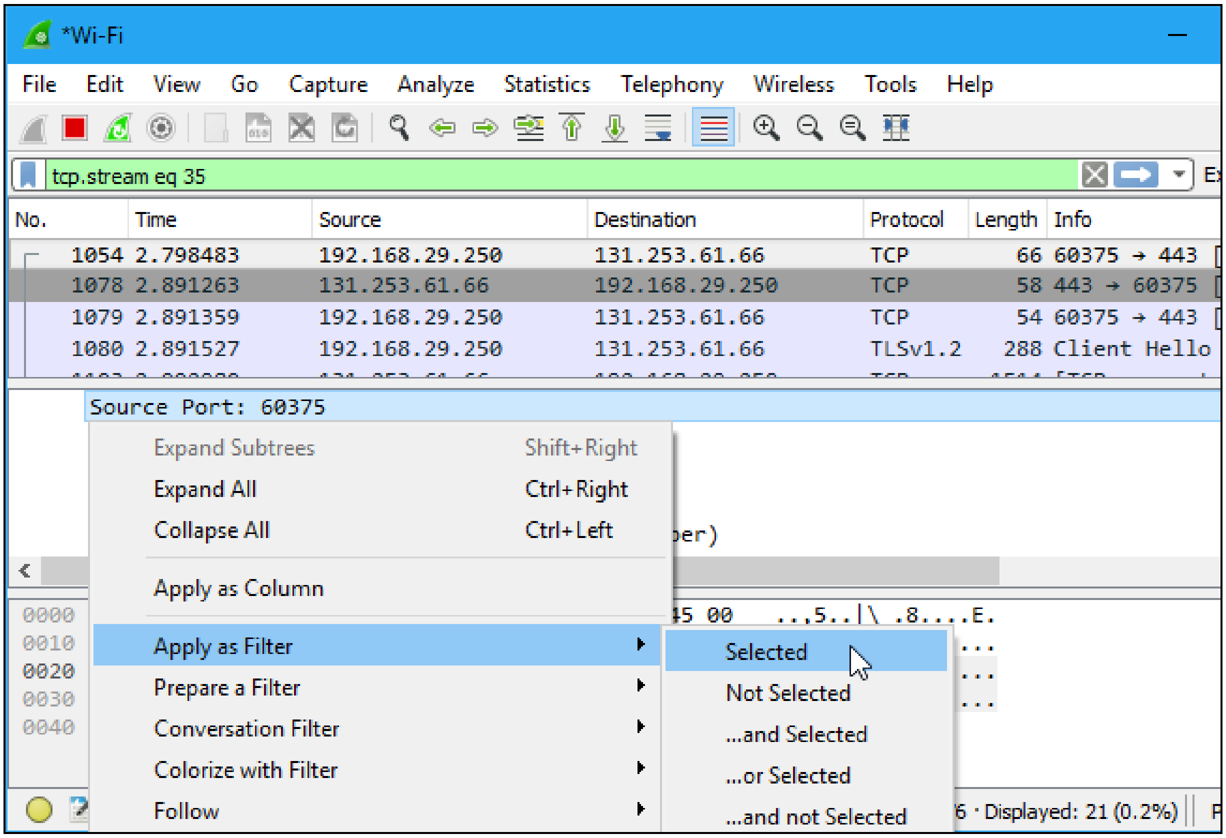
```
Frame 1054: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
    Interface id: 0 (\Device\NPF_{D32D7F0A-A9E8-44EE-88DC-DFD58F65ABA7})
    Encapsulation type: Ethernet (1)
    Arrival Time: Jun  9, 2017 12:40:04.140141000 Pacific Daylight Time
    [Time shift for this packet: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

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

Encapsulation type (frame.encap_type)

Packets: 8136 · Displayed: 21 (0.3%)

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



tcp.stream eq 35

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

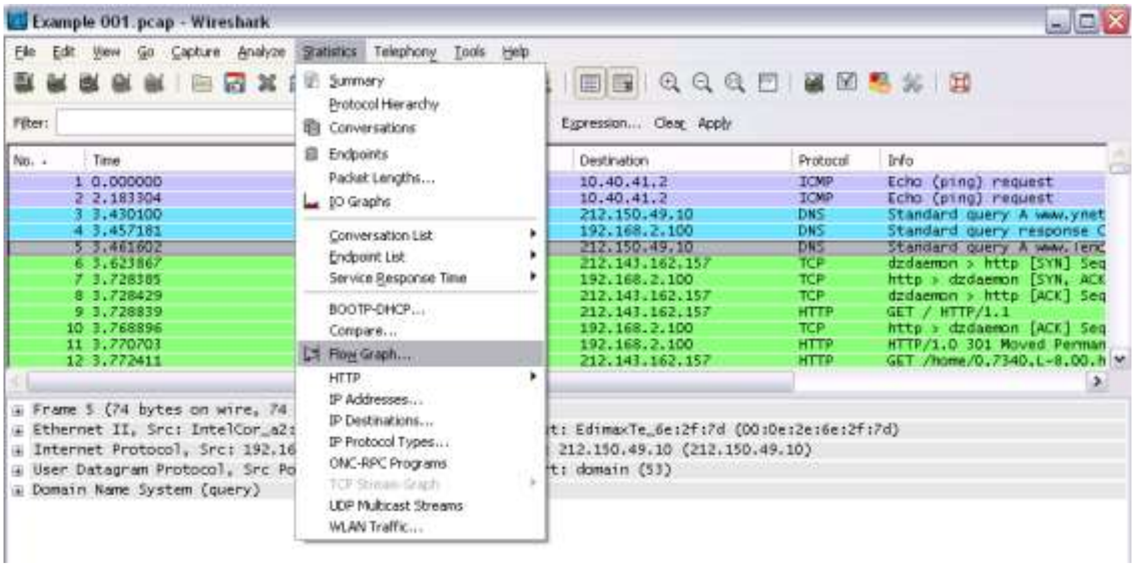
```
Source Port: 60375
```

```
0000                45 00   ...5..|\ .8....E.
0010
0020
0030
0040
```

Displayed: 21 (0.2%)

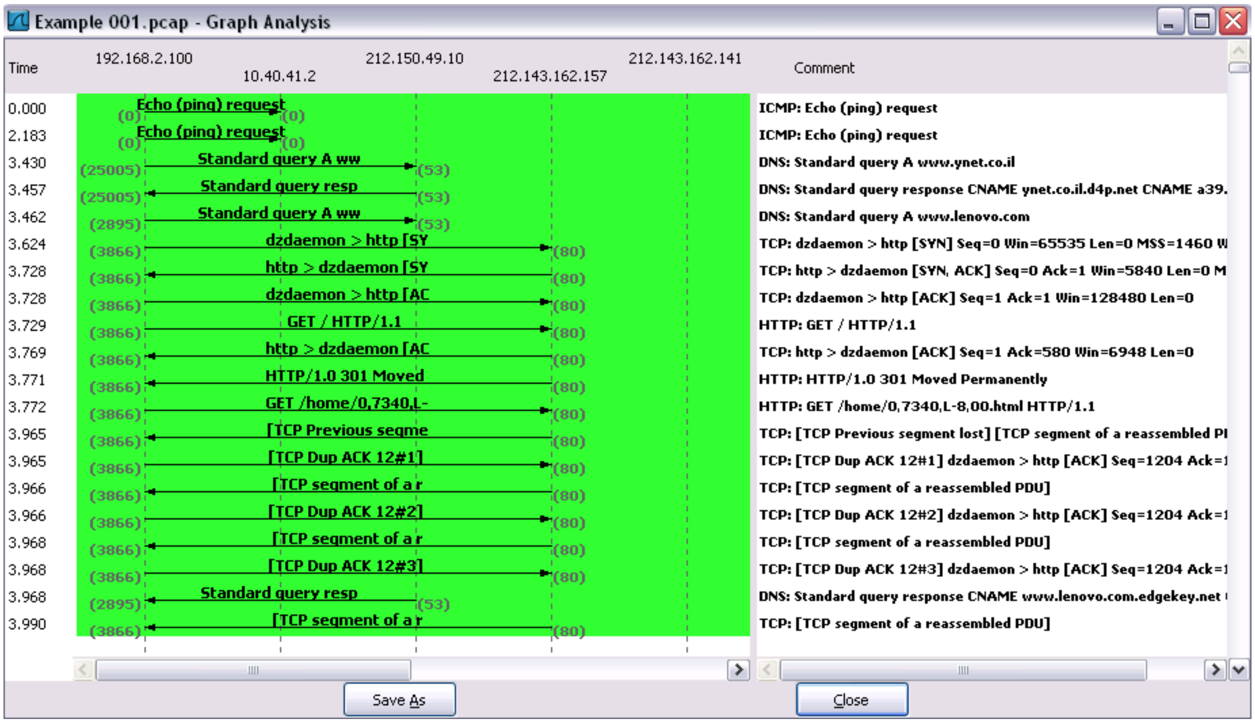
Wireshark is an extremely powerful tool, and this tutorial is just scratching the surface of what you can do with it. Professionals use it to debug network protocol implementations, examine security problems and inspect network protocol internals.

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



No.	Time	Destination	Protocol	Info
1	0.000000	10.40.41.2	ICMP	Echo (ping) request
2	2.183304	10.40.41.2	ICMP	Echo (ping) request
3	3.430100	212.150.49.10	DNS	Standard query A www.ynet
4	3.457181	192.168.2.100	DNS	Standard query response C
5	3.461602	212.150.49.10	DNS	Standard query A www.lenc
6	3.623867	212.143.162.157	TCP	dzdaemon > http [SYN] Seq
7	3.728385	192.168.2.100	TCP	http > dzdaemon [SYN, ACK
8	3.728429	212.143.162.157	TCP	dzdaemon > http [ACK] Seq
9	3.728839	212.143.162.157	HTTP	GET / HTTP/1.1
10	3.768896	192.168.2.100	TCP	http > dzdaemon [ACK] Seq
11	3.770703	192.168.2.100	HTTP	HTTP/1.0 301 Moved Perman
12	3.772411	212.143.162.157	HTTP	GET /home/0,7340,L-8,00.h

```
⊞ Frame 5 (74 bytes on wire, 74
⊞ Ethernet II, Src: IntelCor_a2:                    t: EdimaxTe_6e:2f:7d (00:0e:2e:6e:2f:7d)
⊞ Internet Protocol, Src: 192.16                     212.150.49.10 (212.150.49.10)
⊞ User Datagram Protocol, Src Po                    t: domain (53)
⊞ Domain Name System (query)
```



Time	Comment
0.000	ICMP: Echo (ping) request
2.183	ICMP: Echo (ping) request
3.430	DNS: Standard query A www.ynet.co.il
3.457	DNS: Standard query response CNAME ynet.co.il.d4p.net CNAME a39.
3.462	DNS: Standard query A www.lenovo.com
3.624	TCP: dzdaemon > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 W
3.728	TCP: http > dzdaemon [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 M
3.728	TCP: dzdaemon > http [ACK] Seq=1 Ack=1 Win=128480 Len=0
3.729	HTTP: GET / HTTP/1.1
3.769	TCP: http > dzdaemon [ACK] Seq=1 Ack=580 Win=6948 Len=0
3.771	HTTP: HTTP/1.0 301 Moved Permanently
3.772	HTTP: GET /home/0,7340,L-8,00.html HTTP/1.1
3.965	TCP: [TCP Previous segment lost] [TCP segment of a reassembled PI
3.965	TCP: [TCP Dup ACK 12#1] dzdaemon > http [ACK] Seq=1204 Ack=1
3.966	TCP: [TCP segment of a reassembled PDU]
3.966	TCP: [TCP Dup ACK 12#2] dzdaemon > http [ACK] Seq=1204 Ack=1
3.968	TCP: [TCP segment of a reassembled PDU]
3.968	TCP: [TCP Dup ACK 12#3] dzdaemon > http [ACK] Seq=1204 Ack=1
3.968	DNS: Standard query response CNAME www.lenovo.com.edgekey.net
3.990	TCP: [TCP segment of a reassembled PDU]

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

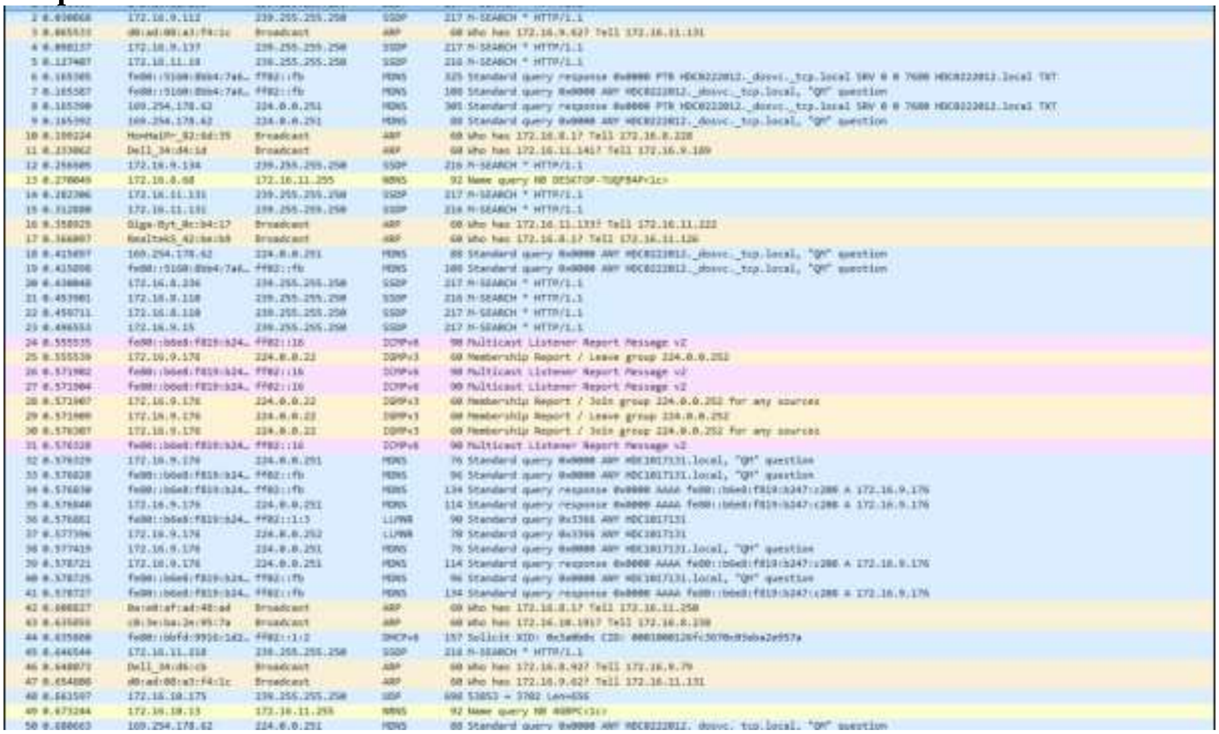
Exercises

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

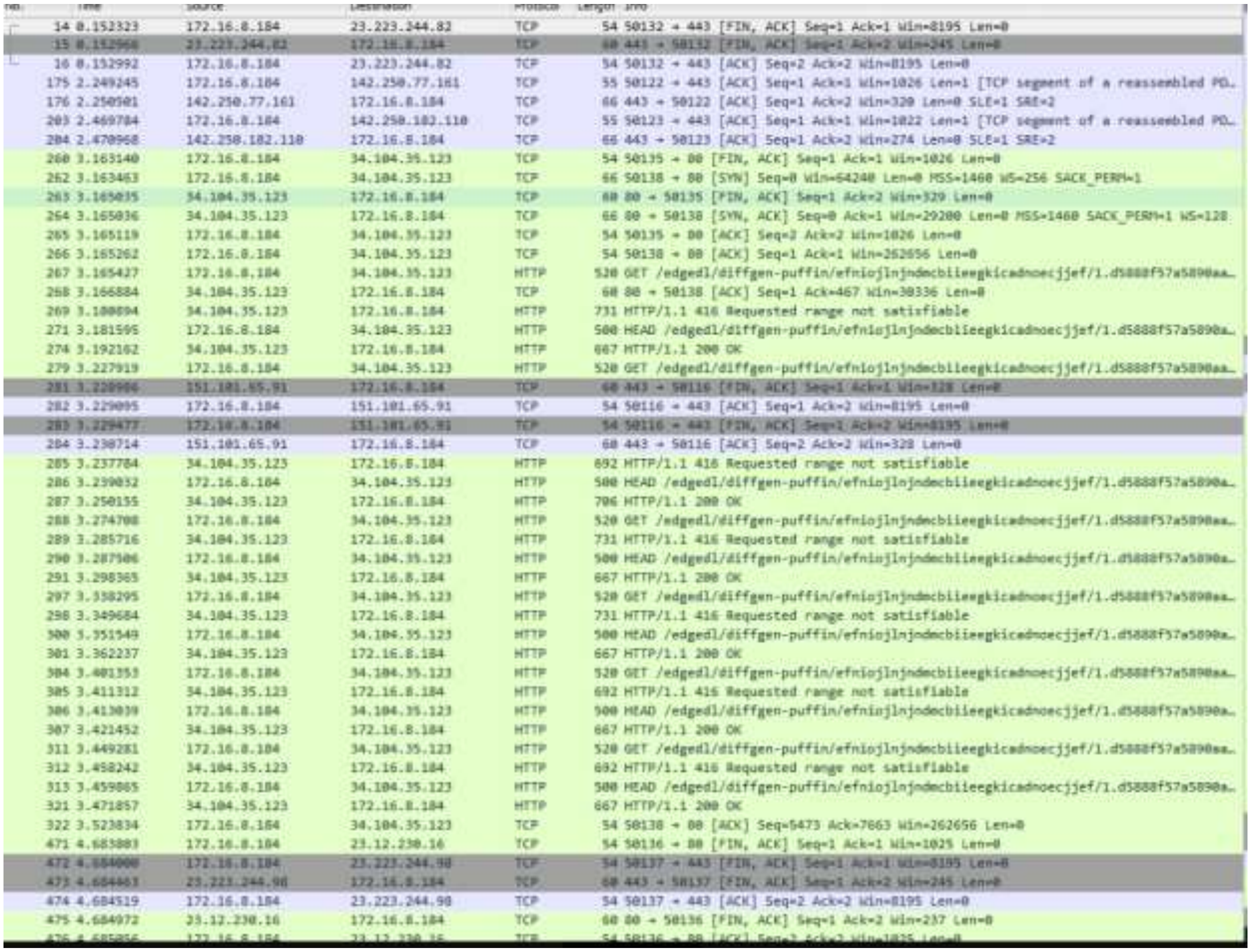


```
 2 0.030068  172.16.9.112          239.255.255.250  SSDP    217 M-SEARCH * HTTP/1.1
 3 0.065533  d0:ad:08:a3:f4:1c     Broadcast        ARP      60 Who has 172.16.9.62? Tell 172.16.11.131
 4 0.090137  172.16.9.137          239.255.255.250  SSDP    217 M-SEARCH * HTTP/1.1
 5 0.127407  172.16.11.18          239.255.255.250  SSDP    216 M-SEARCH * HTTP/1.1
 6 0.165305  fe80::5100:8bb4:7a6…  ff02::fb         MDNS    325 Standard query response 0x0000 PTR HDC0222012._dosvc._tcp.local SRV 0 0 7680 HDC0222012.local TXT
 7 0.165307  fe80::5100:8bb4:7a6…  ff02::fb         MDNS    100 Standard query 0x0000 ANY HDC0222012._dosvc._tcp.local, "QM" question
 8 0.165390  169.254.178.62        224.0.0.251      MDNS    305 Standard query response 0x0000 PTR HDC0222012._dosvc._tcp.local SRV 0 0 7680 HDC0222012.local TXT
 9 0.165392  169.254.178.62        224.0.0.251      MDNS     80 Standard query 0x0000 ANY HDC0222012._dosvc._tcp.local, "QM" question
10 0.190224  HonHaiPr_82:6d:35     Broadcast        ARP      60 Who has 172.16.8.1? Tell 172.16.8.228
11 0.233062  Dell_34:d4:1d         Broadcast        ARP      60 Who has 172.16.11.141? Tell 172.16.9.189
12 0.256505  172.16.9.134          239.255.255.250  SSDP    216 M-SEARCH * HTTP/1.1
13 0.270049  172.16.8.68           172.16.11.255    NBNS     92 Name query NB DESKTOP-TUQP84P<1c>
14 0.282306  172.16.11.131         239.255.255.250  SSDP    217 M-SEARCH * HTTP/1.1
15 0.312080  172.16.11.131         239.255.255.250  SSDP    216 M-SEARCH * HTTP/1.1
16 0.358925  Giga-Byt_8c:b4:17     Broadcast        ARP      60 Who has 172.16.11.133? Tell 172.16.11.222
17 0.366007  RealtekS_42:be:b8     Broadcast        ARP      60 Who has 172.16.8.1? Tell 172.16.11.126
18 0.415097  169.254.178.62        224.0.0.251      MDNS     80 Standard query 0x0000 ANY HDC0222012._dosvc._tcp.local, "QM" question
19 0.415098  fe80::5100:8bb4:7a6…  ff02::fb         MDNS    100 Standard query 0x0000 ANY HDC0222012._dosvc._tcp.local, "QM" question
20 0.430048  172.16.8.236          239.255.255.250  SSDP    217 M-SEARCH * HTTP/1.1
21 0.453901  172.16.8.118          239.255.255.250  SSDP    216 M-SEARCH * HTTP/1.1
22 0.450711  172.16.8.118          239.255.255.250  SSDP    217 M-SEARCH * HTTP/1.1
23 0.496553  172.16.9.15           239.255.255.250  SSDP    217 M-SEARCH * HTTP/1.1
24 0.555535  fe80::b6e8:f819:b24…  ff02::16         ICMPv6   90 Multicast Listener Report Message v2
25 0.555539  172.16.9.176          224.0.0.22       IGMPv3   60 Membership Report / Leave group 224.0.0.252
26 0.571902  fe80::b6e8:f819:b24…  ff02::16         ICMPv6   90 Multicast Listener Report Message v2
27 0.571904  fe80::b6e8:f819:b24…  ff02::16         ICMPv6   90 Multicast Listener Report Message v2
28 0.571907  172.16.9.176          224.0.0.22       IGMPv3   60 Membership Report / Join group 224.0.0.252 for any sources
29 0.571909  172.16.9.176          224.0.0.22       IGMPv3   60 Membership Report / Leave group 224.0.0.252
30 0.576307  172.16.9.176          224.0.0.22       IGMPv3   60 Membership Report / Join group 224.0.0.252 for any sources
31 0.576328  fe80::b6e8:f819:b24…  ff02::16         ICMPv6   90 Multicast Listener Report Message v2
32 0.576329  172.16.9.176          224.0.0.251      MDNS     76 Standard query 0x0000 ANY HDC1017131.local, "QM" question
33 0.576828  fe80::b6e8:f819:b24…  ff02::fb         MDNS     96 Standard query 0x0000 ANY HDC1017131.local, "QM" question
34 0.576830  fe80::b6e8:f819:b24…  ff02::fb         MDNS    134 Standard query response 0x0000 AAAA fe80::b6e8:f819:b247:c288 A 172.16.9.176
35 0.576840  172.16.9.176          224.0.0.251      MDNS    114 Standard query response 0x0000 AAAA fe80::b6e8:f819:b247:c288 A 172.16.9.176
36 0.576881  fe80::b6e8:f819:b24…  ff02::1:3        LLMNR    90 Standard query 0x3366 ANY HDC1017131
37 0.577396  172.16.9.176          224.0.0.252      LLMNR    70 Standard query 0x3366 ANY HDC1017131
38 0.577419  172.16.9.176          224.0.0.251      MDNS     76 Standard query 0x0000 ANY HDC1017131.local, "QM" question
39 0.578721  172.16.9.176          224.0.0.251      MDNS    114 Standard query response 0x0000 AAAA fe80::b6e8:f819:b247:c288 A 172.16.9.176
40 0.578725  fe80::b6e8:f819:b24…  ff02::fb         MDNS     96 Standard query 0x0000 ANY HDC1017131.local, "QM" question
41 0.578727  fe80::b6e8:f819:b24…  ff02::fb         MDNS    134 Standard query response 0x0000 AAAA fe80::b6e8:f819:b247:c288 A 172.16.9.176
42 0.600827  8a:e0:af:ad:48:ad     Broadcast        ARP      60 Who has 172.16.8.1? Tell 172.16.11.250
43 0.635059  c8:3e:ba:2e:95:7a     Broadcast        ARP      60 Who has 172.16.10.191? Tell 172.16.8.230
44 0.635060  fe80::bbfd:9916:1d2…  ff02::1:2        DHCPv6  157 Solicit XID: 0x3a0b0c CID: 0001000126fc3070c05eba2e957a
45 0.646544  172.16.11.218         239.255.255.250  SSDP    216 M-SEARCH * HTTP/1.1
46 0.648071  Dell_34:d6:cb         Broadcast        ARP      60 Who has 172.16.8.92? Tell 172.16.9.79
47 0.654086  d0:ad:08:a3:f4:1c     Broadcast        ARP      60 Who has 172.16.9.62? Tell 172.16.11.131
48 0.663597  172.16.10.175         239.255.255.250  UDP     698 53853 → 3702 Len=656
49 0.673244  172.16.10.13          172.16.11.255    NBNS     92 Name query NB 408PC<1c>
50 0.680663  169.254.178.62        224.0.0.251      MDNS     80 Standard query 0x0000 ANY HDC0222012._dosvc._tcp.local, "QM" question
```

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

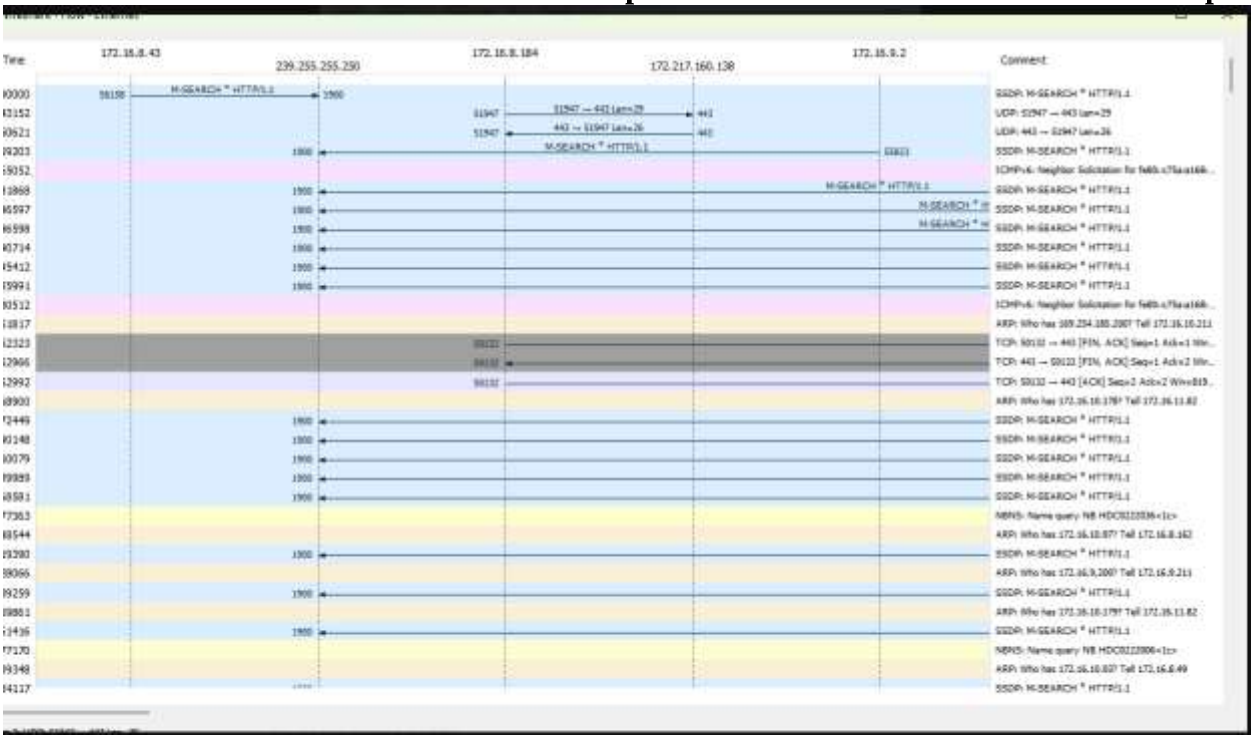
Procedure

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

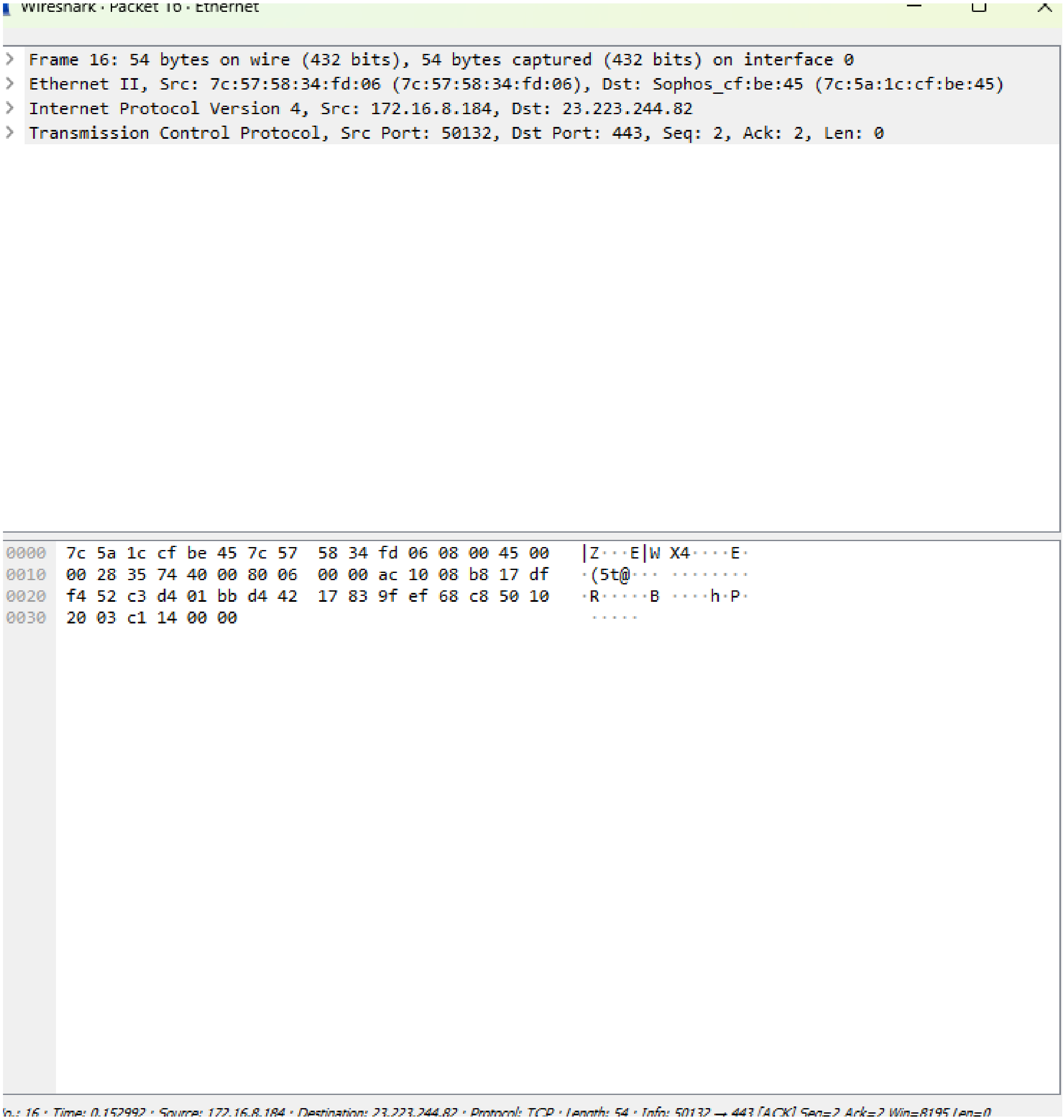


```
No.     Time         Source            Destination       Protocol  Length Info
     14 0.152323     172.16.8.184      23.223.244.82     TCP         54 50132 → 443 [FIN, ACK] Seq=1 Ack=1 Win=8195 Len=0
     15 0.152966     23.223.244.82     172.16.8.184      TCP         60 443 → 50132 [FIN, ACK] Seq=1 Ack=2 Win=245 Len=0
     16 0.152992     172.16.8.184      23.223.244.82     TCP         54 50132 → 443 [ACK] Seq=2 Ack=2 Win=8195 Len=0
    175 2.249245     172.16.8.184      142.250.77.161    TCP         55 50122 → 443 [ACK] Seq=1 Ack=1 Win=1026 Len=1 [TCP segment of a reassembled PD…
    176 2.250501     142.250.77.161    172.16.8.184      TCP         66 443 → 50122 [ACK] Seq=1 Ack=2 Win=320 Len=0 SLE=1 SRE=2
    203 2.469784     172.16.8.184      142.250.182.110   TCP         55 50123 → 443 [ACK] Seq=1 Ack=1 Win=1022 Len=1 [TCP segment of a reassembled PD…
    204 2.470968     142.250.182.110   172.16.8.184      TCP         66 443 → 50123 [ACK] Seq=1 Ack=2 Win=274 Len=0 SLE=1 SRE=2
    260 3.163140     172.16.8.184      34.104.35.123     TCP         54 50135 → 80 [FIN, ACK] Seq=1 Ack=1 Win=1026 Len=0
    262 3.163463     172.16.8.184      34.104.35.123     TCP         66 50138 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
    263 3.165035     34.104.35.123     172.16.8.184      TCP         60 80 → 50135 [FIN, ACK] Seq=1 Ack=2 Win=329 Len=0
    264 3.165036     34.104.35.123     172.16.8.184      TCP         66 80 → 50138 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
    265 3.165119     172.16.8.184      34.104.35.123     TCP         54 50135 → 80 [ACK] Seq=2 Ack=2 Win=1026 Len=0
    266 3.165262     172.16.8.184      34.104.35.123     TCP         54 50138 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
    267 3.165427     172.16.8.184      34.104.35.123     HTTP       520 GET /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890aa…
    268 3.166884     34.104.35.123     172.16.8.184      TCP         60 80 → 50138 [ACK] Seq=1 Ack=467 Win=30336 Len=0
    269 3.180894     34.104.35.123     172.16.8.184      HTTP       731 HTTP/1.1 416 Requested range not satisfiable
    271 3.181595     172.16.8.184      34.104.35.123     HTTP       500 HEAD /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890a…
    274 3.192162     34.104.35.123     172.16.8.184      HTTP       667 HTTP/1.1 200 OK
    279 3.227919     172.16.8.184      34.104.35.123     HTTP       520 GET /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890aa…
    281 3.228986     151.101.65.91     172.16.8.184      TCP         60 443 → 50116 [FIN, ACK] Seq=1 Ack=1 Win=328 Len=0
    282 3.229095     172.16.8.184      151.101.65.91     TCP         54 50116 → 443 [ACK] Seq=1 Ack=2 Win=8195 Len=0
    283 3.229477     172.16.8.184      151.101.65.91     TCP         54 50116 → 443 [FIN, ACK] Seq=1 Ack=2 Win=8195 Len=0
    284 3.230714     151.101.65.91     172.16.8.184      TCP         60 443 → 50116 [ACK] Seq=2 Ack=2 Win=328 Len=0
    285 3.237784     34.104.35.123     172.16.8.184      HTTP       692 HTTP/1.1 416 Requested range not satisfiable
    286 3.239032     172.16.8.184      34.104.35.123     HTTP       500 HEAD /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890a…
    287 3.250155     34.104.35.123     172.16.8.184      HTTP       706 HTTP/1.1 200 OK
    288 3.274708     172.16.8.184      34.104.35.123     HTTP       520 GET /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890aa…
    289 3.285716     34.104.35.123     172.16.8.184      HTTP       731 HTTP/1.1 416 Requested range not satisfiable
    290 3.287506     172.16.8.184      34.104.35.123     HTTP       500 HEAD /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890a…
    291 3.298365     34.104.35.123     172.16.8.184      HTTP       667 HTTP/1.1 200 OK
    297 3.338295     172.16.8.184      34.104.35.123     HTTP       520 GET /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890aa…
    298 3.349684     34.104.35.123     172.16.8.184      HTTP       731 HTTP/1.1 416 Requested range not satisfiable
    300 3.351549     172.16.8.184      34.104.35.123     HTTP       500 HEAD /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890a…
    301 3.362237     34.104.35.123     172.16.8.184      HTTP       667 HTTP/1.1 200 OK
    304 3.401353     172.16.8.184      34.104.35.123     HTTP       520 GET /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890aa…
    305 3.411312     34.104.35.123     172.16.8.184      HTTP       692 HTTP/1.1 416 Requested range not satisfiable
    306 3.413039     172.16.8.184      34.104.35.123     HTTP       500 HEAD /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890a…
    307 3.421452     34.104.35.123     172.16.8.184      HTTP       667 HTTP/1.1 200 OK
    311 3.449281     172.16.8.184      34.104.35.123     HTTP       520 GET /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890aa…
    312 3.458242     34.104.35.123     172.16.8.184      HTTP       692 HTTP/1.1 416 Requested range not satisfiable
    313 3.459865     172.16.8.184      34.104.35.123     HTTP       500 HEAD /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890a…
    321 3.471857     34.104.35.123     172.16.8.184      HTTP       667 HTTP/1.1 200 OK
    322 3.523834     172.16.8.184      34.104.35.123     TCP         54 50138 → 80 [ACK] Seq=5473 Ack=7663 Win=262656 Len=0
    471 4.683883     172.16.8.184      23.12.230.16      TCP         54 50136 → 80 [FIN, ACK] Seq=1 Ack=1 Win=1025 Len=0
    472 4.684000     172.16.8.184      23.223.244.98     TCP         54 50137 → 443 [FIN, ACK] Seq=1 Ack=1 Win=8195 Len=0
    473 4.684463     23.223.244.98     172.16.8.184      TCP         60 443 → 50137 [FIN, ACK] Seq=1 Ack=2 Win=245 Len=0
    474 4.684519     172.16.8.184      23.223.244.98     TCP         54 50137 → 443 [ACK] Seq=2 Ack=2 Win=8195 Len=0
    475 4.684972     23.12.230.16      172.16.8.184      TCP         60 80 → 50136 [FIN, ACK] Seq=1 Ack=2 Win=237 Len=0
    476 4.685056     172.16.8.184      23.12.230.16      TCP         54 50136 → 80 [ACK] Seq=2 Ack=2 Win=1025 Len=0
```

Flow Graph output



```
Time    172.16.8.43   239.255.255.250   172.16.8.184   172.217.160.138   172.16.9.2   Comment
00000                                                                                SSDP: M-SEARCH * HTTP/1.1
43152                                                                                UDP: 51947 → 443 Len=29
60621                                                                                UDP: 443 → 51947 Len=26
19203                                                                                SSDP: M-SEARCH * HTTP/1.1
59052                                                                                ICMPv6: Neighbor Solicitation for fe80::c75a:a16b...
11868                                                                                SSDP: M-SEARCH * HTTP/1.1
46597                                                                                SSDP: M-SEARCH * HTTP/1.1
46598                                                                                SSDP: M-SEARCH * HTTP/1.1
40714                                                                                SSDP: M-SEARCH * HTTP/1.1
45412                                                                                SSDP: M-SEARCH * HTTP/1.1
15991                                                                                SSDP: M-SEARCH * HTTP/1.1
80512                                                                                ICMPv6: Neighbor Solicitation for fe80::c75a:a16b...
51817                                                                                ARP: Who has 169.254.185.200? Tell 172.16.10.211
52323                                                                                TCP: 50132 → 443 [FIN, ACK] Seq=1 Ack=1 Win...
52966                                                                                TCP: 443 → 50132 [FIN, ACK] Seq=1 Ack=2 Win...
52992                                                                                TCP: 50132 → 443 [ACK] Seq=2 Ack=2 Win=819...
68900                                                                                ARP: Who has 172.16.10.178? Tell 172.16.11.82
72446                                                                                SSDP: M-SEARCH * HTTP/1.1
80148                                                                                SSDP: M-SEARCH * HTTP/1.1
00079                                                                                SSDP: M-SEARCH * HTTP/1.1
19989                                                                                SSDP: M-SEARCH * HTTP/1.1
18581                                                                                SSDP: M-SEARCH * HTTP/1.1
77383                                                                                NBNS: Name query NB HDC0122036<1c>
18544                                                                                ARP: Who has 172.16.10.87? Tell 172.16.8.162
19390                                                                                SSDP: M-SEARCH * HTTP/1.1
39066                                                                                ARP: Who has 172.16.9.200? Tell 172.16.9.211
19259                                                                                SSDP: M-SEARCH * HTTP/1.1
19881                                                                                ARP: Who has 172.16.10.179? Tell 172.16.11.82
51436                                                                                SSDP: M-SEARCH * HTTP/1.1
77170                                                                                NBNS: Name query NB HDC0122006<1c>
19348                                                                                ARP: Who has 172.16.10.83? Tell 172.16.8.49
84117                                                                                SSDP: M-SEARCH * HTTP/1.1
```



```
> Frame 16: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
> Ethernet II, Src: 7c:57:58:34:fd:06 (7c:57:58:34:fd:06), Dst: Sophos_cf:be:45 (7c:5a:1c:cf:be:45)
> Internet Protocol Version 4, Src: 172.16.8.184, Dst: 23.223.244.82
> Transmission Control Protocol, Src Port: 50132, Dst Port: 443, Seq: 2, Ack: 2, Len: 0
```

```
0000  7c 5a 1c cf be 45 7c 57  58 34 fd 06 08 00 45 00   |Z···E|W X4····E·
0010  00 28 35 74 40 00 80 06  00 00 ac 10 08 b8 17 df   ·(5t@··· ········
0020  f4 52 c3 d4 01 bb d4 42  17 83 9f ef 68 c8 50 10   ·R·····B ····h·P·
0030  20 03 c1 14 00 00                                   ······
```

```
lo.: 16 · Time: 0.152992 · Source: 172.16.8.184 · Destination: 23.223.244.82 · Protocol: TCP · Length: 54 · Info: 50132 → 443 [ACK] Seq=2 Ack=2 Win=8195 Len=0
```

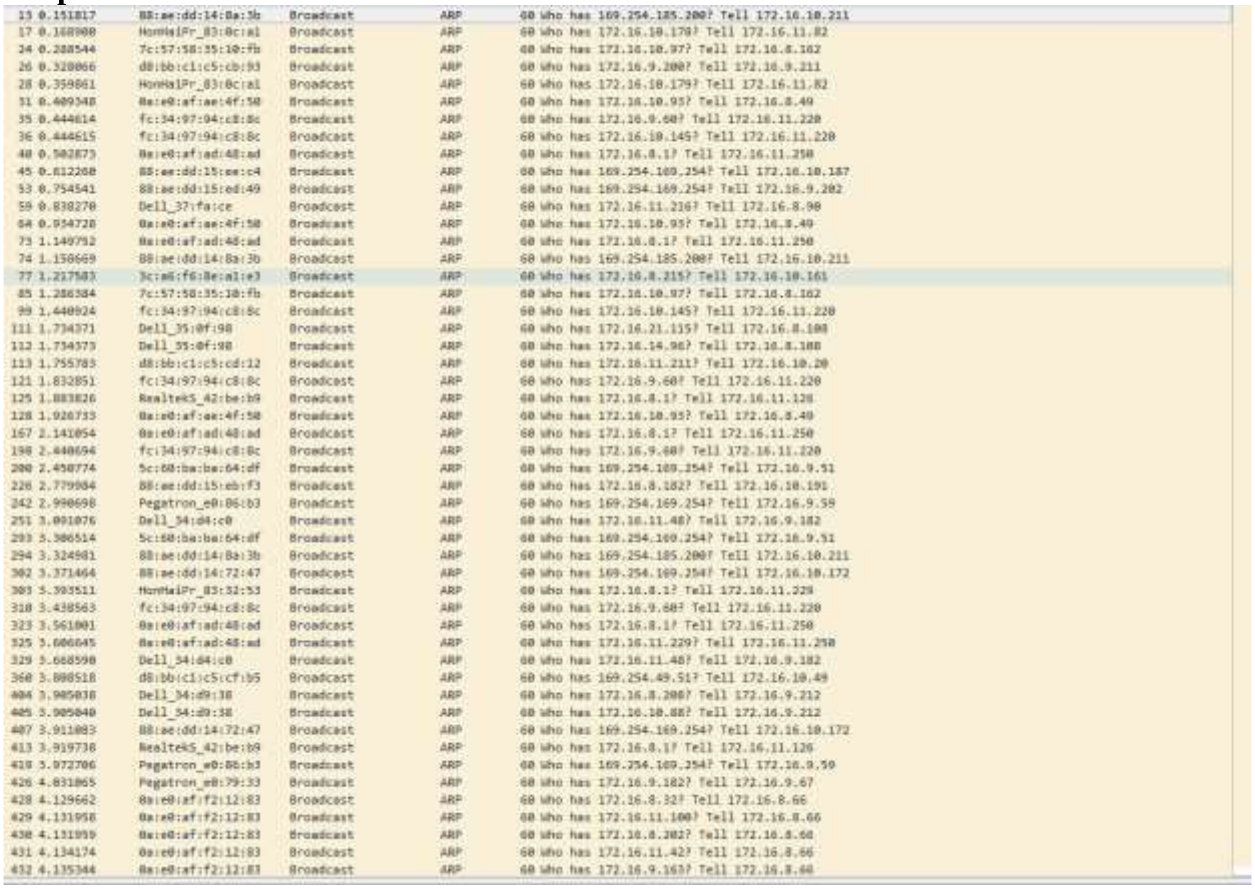
3.Create a Filter to display only ARP packets and inspect the packets.

Procedure

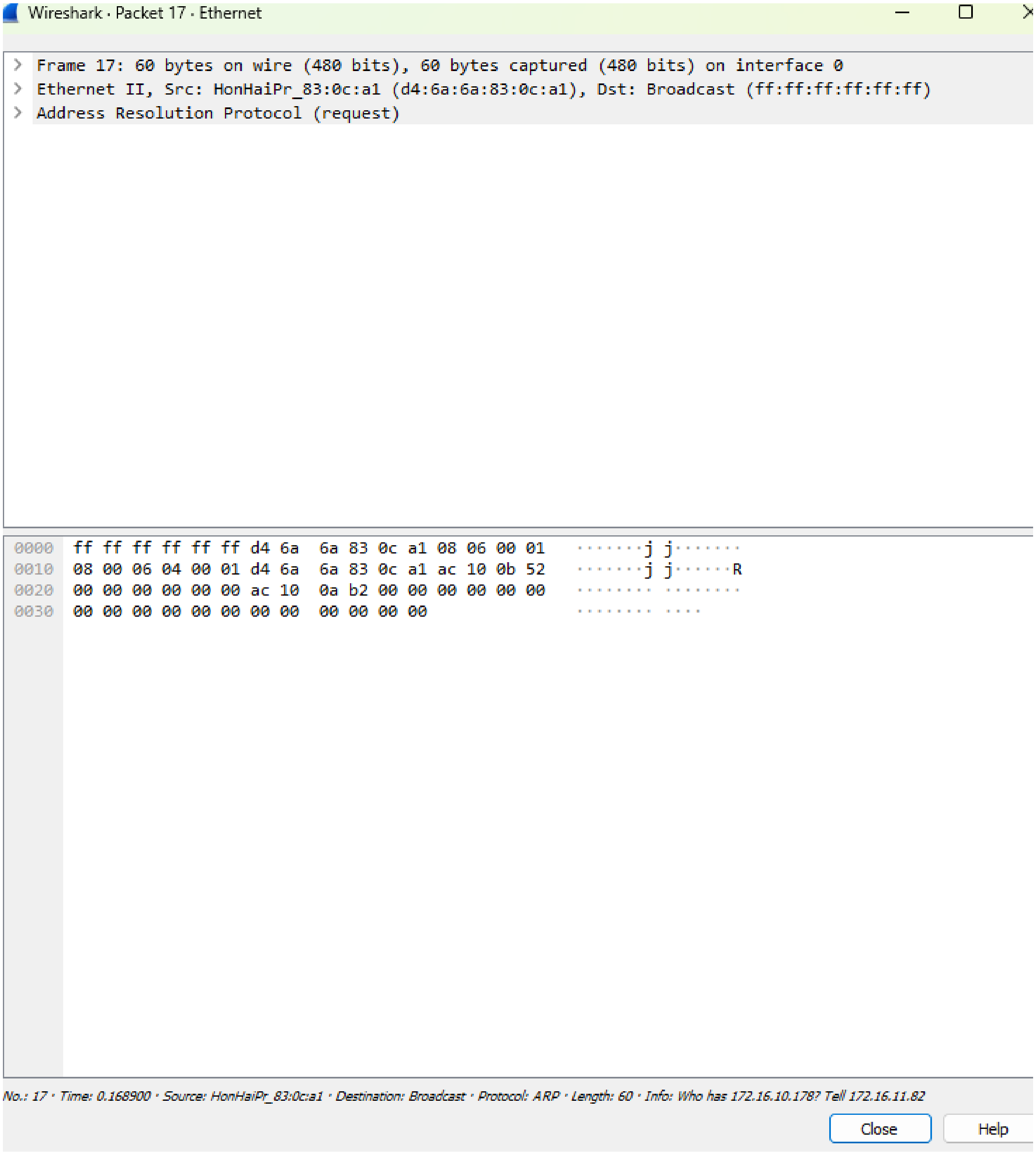
- Select Local Area Connection in Wireshark.
- Go to capture ⚇option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search ARP packets in search bar.

- □ Save the packets.

Output



```
 13 0.151817   88:ae:dd:14:8a:3b    Broadcast   ARP   60 Who has 169.254.185.200? Tell 172.16.10.211
 17 0.168908   HonHaiPr_83:8c:a1    Broadcast   ARP   60 Who has 172.16.10.179? Tell 172.16.11.82
 24 0.288544   7c:57:58:35:10:fb    Broadcast   ARP   60 Who has 172.16.10.97? Tell 172.16.8.162
 26 0.328066   d8:bb:c1:c5:cb:93    Broadcast   ARP   60 Who has 172.16.9.200? Tell 172.16.9.211
 28 0.359861   HonHaiPr_83:8c:a1    Broadcast   ARP   60 Who has 172.16.10.179? Tell 172.16.11.82
 31 0.409348   8a:e0:af:ae:4f:58    Broadcast   ARP   60 Who has 172.16.10.93? Tell 172.16.8.49
 35 0.444614   fc:34:97:94:c8:8c    Broadcast   ARP   60 Who has 172.16.9.60? Tell 172.16.11.220
 36 0.444615   fc:34:97:94:c8:8c    Broadcast   ARP   60 Who has 172.16.10.145? Tell 172.16.11.220
 40 0.502873   8a:e0:af:ad:48:ad    Broadcast   ARP   60 Who has 172.16.8.1? Tell 172.16.11.250
 45 0.612260   88:ae:dd:15:ee:c4    Broadcast   ARP   60 Who has 169.254.169.254? Tell 172.16.10.187
 53 0.754541   88:ae:dd:15:ed:49    Broadcast   ARP   60 Who has 169.254.169.254? Tell 172.16.9.202
 59 0.838270   Dell_37:fa:ce        Broadcast   ARP   60 Who has 172.16.11.216? Tell 172.16.8.98
 64 0.934728   8a:e0:af:ae:4f:58    Broadcast   ARP   60 Who has 172.16.10.93? Tell 172.16.8.49
 73 1.149752   8a:e0:af:ad:48:ad    Broadcast   ARP   60 Who has 172.16.8.1? Tell 172.16.11.250
 74 1.150669   88:ae:dd:14:8a:3b    Broadcast   ARP   60 Who has 169.254.185.200? Tell 172.16.10.211
 77 1.217583   3c:a6:f6:8e:a1:e3    Broadcast   ARP   60 Who has 172.16.8.215? Tell 172.16.10.161
 85 1.286384   7c:57:58:35:10:fb    Broadcast   ARP   60 Who has 172.16.10.97? Tell 172.16.8.162
 99 1.440924   fc:34:97:94:c8:8c    Broadcast   ARP   60 Who has 172.16.10.145? Tell 172.16.11.220
111 1.734371   Dell_35:0f:98        Broadcast   ARP   60 Who has 172.16.21.115? Tell 172.16.8.108
112 1.734373   Dell_35:0f:98        Broadcast   ARP   60 Who has 172.16.14.96? Tell 172.16.8.108
113 1.755783   d8:bb:c1:c5:cd:12    Broadcast   ARP   60 Who has 172.16.11.211? Tell 172.16.10.20
121 1.832851   fc:34:97:94:c8:8c    Broadcast   ARP   60 Who has 172.16.9.60? Tell 172.16.11.220
125 1.883826   RealtekS_42:be:b9    Broadcast   ARP   60 Who has 172.16.8.1? Tell 172.16.11.126
128 1.920733   8a:e0:af:ae:4f:58    Broadcast   ARP   60 Who has 172.16.10.93? Tell 172.16.8.49
167 2.141054   8a:e0:af:ad:48:ad    Broadcast   ARP   60 Who has 172.16.8.1? Tell 172.16.11.250
198 2.440694   fc:34:97:94:c8:8c    Broadcast   ARP   60 Who has 172.16.9.60? Tell 172.16.11.220
200 2.450774   5c:60:ba:be:64:df    Broadcast   ARP   60 Who has 169.254.169.254? Tell 172.16.9.51
226 2.779984   88:ae:dd:15:eb:f3    Broadcast   ARP   60 Who has 172.16.8.182? Tell 172.16.10.191
242 2.990698   Pegatron_e0:86:b3    Broadcast   ARP   60 Who has 169.254.169.254? Tell 172.16.9.59
251 3.001076   Dell_34:d4:c0        Broadcast   ARP   60 Who has 172.16.11.48? Tell 172.16.9.182
293 3.306514   5c:60:ba:be:64:df    Broadcast   ARP   60 Who has 169.254.169.254? Tell 172.16.9.51
294 3.324981   88:ae:dd:14:8a:3b    Broadcast   ARP   60 Who has 169.254.185.200? Tell 172.16.10.211
302 3.371464   88:ae:dd:14:72:47    Broadcast   ARP   60 Who has 169.254.169.254? Tell 172.16.10.172
303 3.393511   HonHaiPr_83:32:53    Broadcast   ARP   60 Who has 172.16.8.1? Tell 172.16.11.229
318 3.438563   fc:34:97:94:c8:8c    Broadcast   ARP   60 Who has 172.16.9.60? Tell 172.16.11.220
323 3.561001   8a:e0:af:ad:48:ad    Broadcast   ARP   60 Who has 172.16.8.1? Tell 172.16.11.250
325 3.606645   8a:e0:af:ad:48:ad    Broadcast   ARP   60 Who has 172.16.11.229? Tell 172.16.11.250
329 3.668590   Dell_34:d4:c0        Broadcast   ARP   60 Who has 172.16.11.48? Tell 172.16.9.182
360 3.808518   d8:bb:c1:c5:cf:b5    Broadcast   ARP   60 Who has 169.254.49.51? Tell 172.16.10.49
404 3.905038   Dell_34:d9:38        Broadcast   ARP   60 Who has 172.16.8.200? Tell 172.16.9.212
405 3.905040   Dell_34:d9:38        Broadcast   ARP   60 Who has 172.16.10.88? Tell 172.16.9.212
407 3.911083   88:ae:dd:14:72:47    Broadcast   ARP   60 Who has 169.254.169.254? Tell 172.16.10.172
413 3.919738   RealtekS_42:be:b9    Broadcast   ARP   60 Who has 172.16.8.1? Tell 172.16.11.126
418 3.972706   Pegatron_e0:86:b3    Broadcast   ARP   60 Who has 169.254.169.254? Tell 172.16.9.59
426 4.031065   Pegatron_e0:79:33    Broadcast   ARP   60 Who has 172.16.9.182? Tell 172.16.9.67
428 4.129662   8a:e0:af:f2:12:83    Broadcast   ARP   60 Who has 172.16.8.32? Tell 172.16.8.66
429 4.131958   8a:e0:af:f2:12:83    Broadcast   ARP   60 Who has 172.16.11.100? Tell 172.16.8.66
430 4.131959   8a:e0:af:f2:12:83    Broadcast   ARP   60 Who has 172.16.8.202? Tell 172.16.8.66
431 4.134174   8a:e0:af:f2:12:83    Broadcast   ARP   60 Who has 172.16.11.42? Tell 172.16.8.66
432 4.135344   8a:e0:af:f2:12:83    Broadcast   ARP   60 Who has 172.16.9.163? Tell 172.16.8.66
```



```
> Frame 17: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: HonHaiPr_83:0c:a1 (d4:6a:6a:83:0c:a1), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff d4 6a  6a 83 0c a1 08 06 00 01   ·······j j·······
0010  08 00 06 04 00 01 d4 6a  6a 83 0c a1 ac 10 0b 52   ·······j j······R
0020  00 00 00 00 00 00 ac 10  0a b2 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

No.: 17 · Time: 0.168900 · Source: HonHaiPr_83:0c:a1 · Destination: Broadcast · Protocol: ARP · Length: 60 · Info: Who has 172.16.10.178? Tell 172.16.11.82

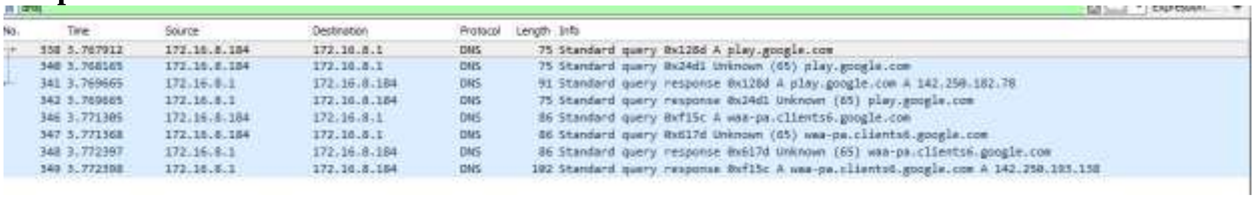
4.Create a Filter to display only DNS packets and provide the flow graph.

Procedure

- Select Local Area Connection in Wireshark.

- Go to capture option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search DNS packets in search bar.
- To see flow graph click StatisticsFlow graph.
- Save the packets.

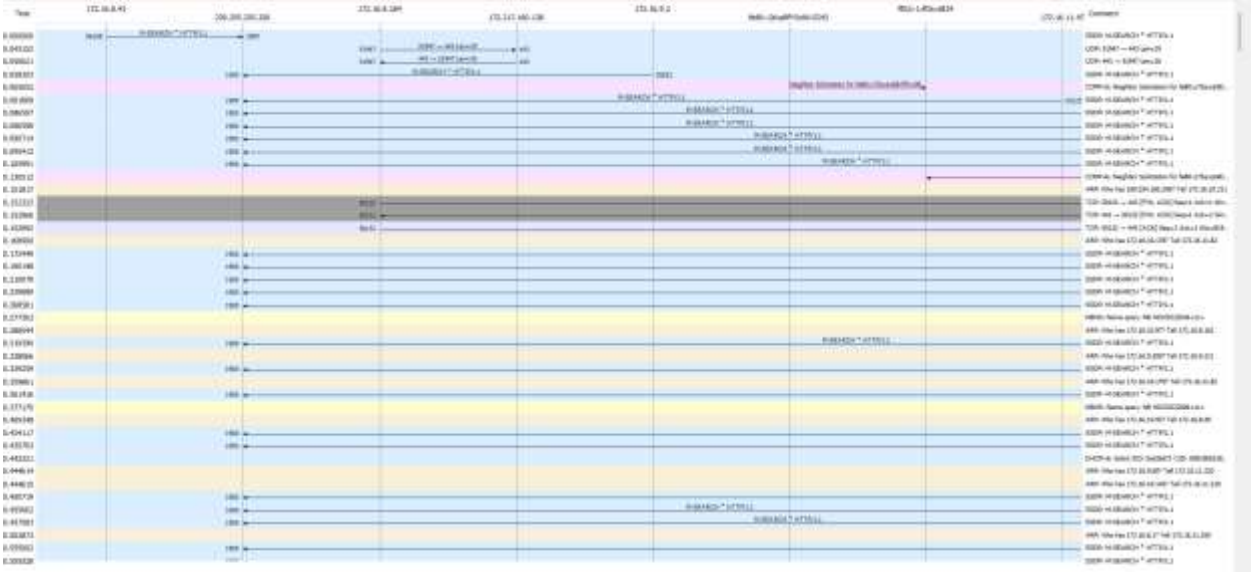
Output



dns

No.	Time	Source	Destination	Protocol	Length	Info
338	3.767912	172.16.8.184	172.16.8.1	DNS	75	Standard query 0x128d A play.google.com
340	3.768165	172.16.8.184	172.16.8.1	DNS	75	Standard query 0x24d1 Unknown (65) play.google.com
341	3.769665	172.16.8.1	172.16.8.184	DNS	91	Standard query response 0x128d A play.google.com A 142.250.182.78
342	3.769685	172.16.8.1	172.16.8.184	DNS	75	Standard query response 0x24d1 Unknown (65) play.google.com
346	3.771305	172.16.8.184	172.16.8.1	DNS	86	Standard query 0xf15c A waa-pa.clients6.google.com
347	3.771368	172.16.8.184	172.16.8.1	DNS	86	Standard query 0x617d Unknown (65) waa-pa.clients6.google.com
348	3.772397	172.16.8.1	172.16.8.184	DNS	86	Standard query response 0x617d Unknown (65) waa-pa.clients6.google.com
349	3.772308	172.16.8.1	172.16.8.184	DNS	102	Standard query response 0xf15c A waa-pa.clients6.google.com A 142.250.183.158

Flow Graph output

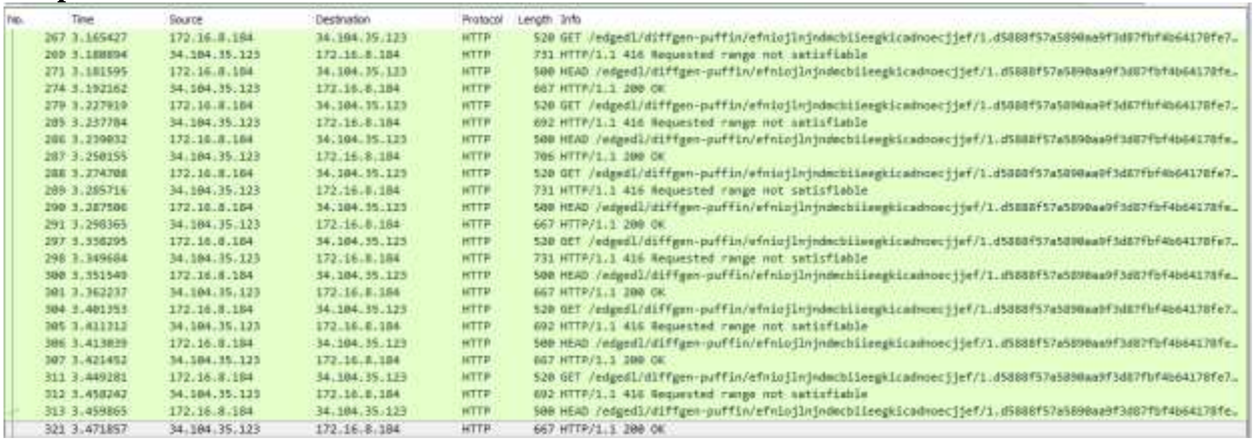


5.Create a Filter to display only HTTP packets and inspect the packets

Procedure

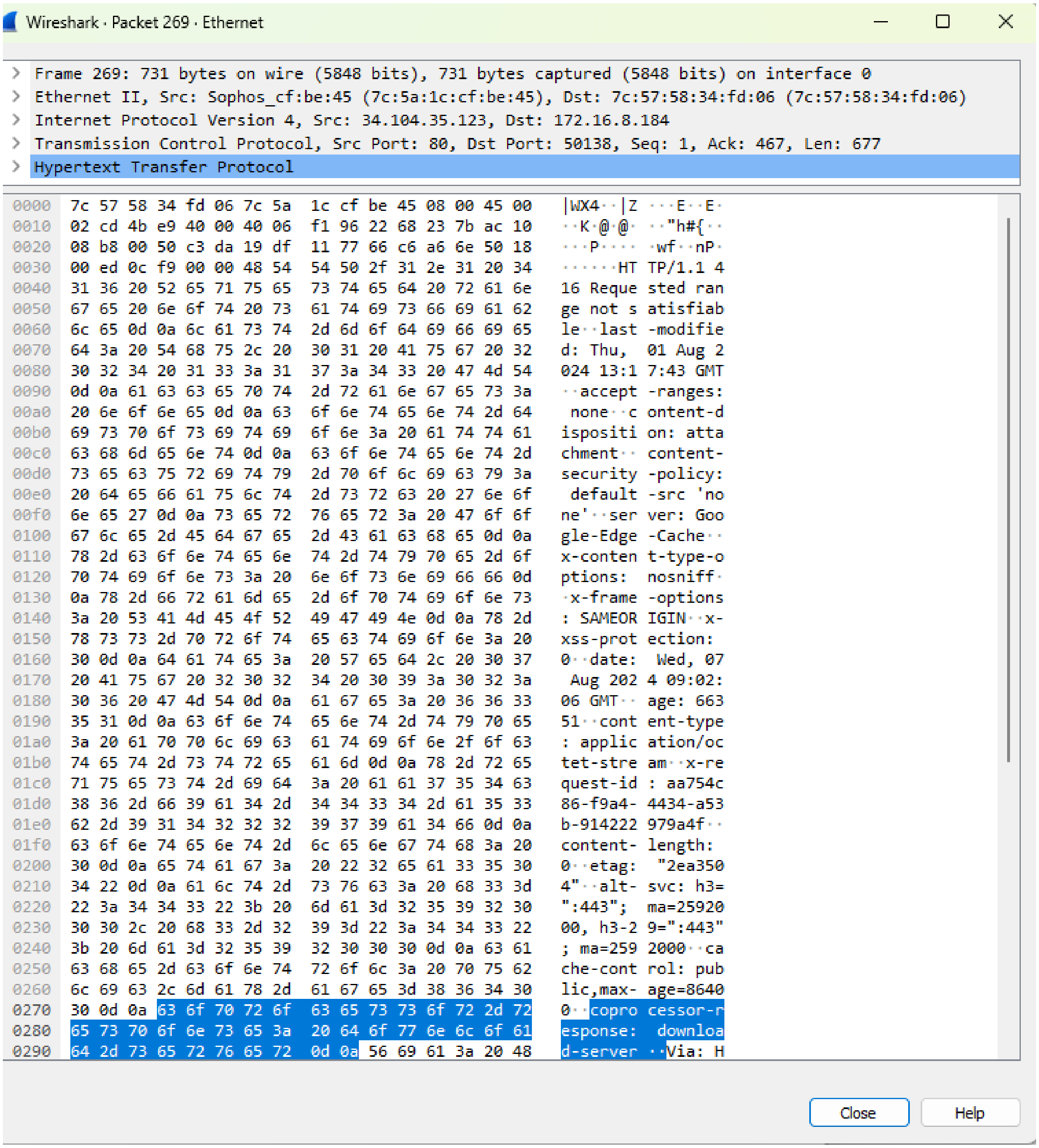
- □ Select Local Area Connection in Wireshark.
- □ Go to capture ⚇option
- □ Select stop capture automatically after 100 packets.
- □ Then click Start capture.
- □ Search HTTP packets in the search bar.
- □ Save the packets.

Output



```
No.   Time       Source          Destination     Protocol  Length Info
  267 3.165427   172.16.8.184    34.104.35.123   HTTP        520 GET /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890aa9f3d87fbf4b64178fe7…
  269 3.180894   34.104.35.123   172.16.8.184    HTTP        731 HTTP/1.1 416 Requested range not satisfiable
  271 3.181595   172.16.8.184    34.104.35.123   HTTP        500 HEAD /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890aa9f3d87fbf4b64178fe…
  274 3.192162   34.104.35.123   172.16.8.184    HTTP        667 HTTP/1.1 200 OK
  279 3.227919   172.16.8.184    34.104.35.123   HTTP        520 GET /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890aa9f3d87fbf4b64178fe7…
  285 3.237784   34.104.35.123   172.16.8.184    HTTP        692 HTTP/1.1 416 Requested range not satisfiable
  286 3.239032   172.16.8.184    34.104.35.123   HTTP        500 HEAD /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890aa9f3d87fbf4b64178fe…
  287 3.250155   34.104.35.123   172.16.8.184    HTTP        706 HTTP/1.1 200 OK
  288 3.274708   172.16.8.184    34.104.35.123   HTTP        520 GET /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890aa9f3d87fbf4b64178fe7…
  289 3.285716   34.104.35.123   172.16.8.184    HTTP        731 HTTP/1.1 416 Requested range not satisfiable
  290 3.287506   172.16.8.184    34.104.35.123   HTTP        500 HEAD /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890aa9f3d87fbf4b64178fe…
  291 3.298365   34.104.35.123   172.16.8.184    HTTP        667 HTTP/1.1 200 OK
  297 3.338295   172.16.8.184    34.104.35.123   HTTP        520 GET /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890aa9f3d87fbf4b64178fe7…
  298 3.349684   34.104.35.123   172.16.8.184    HTTP        731 HTTP/1.1 416 Requested range not satisfiable
  300 3.351549   172.16.8.184    34.104.35.123   HTTP        500 HEAD /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890aa9f3d87fbf4b64178fe…
  301 3.362237   34.104.35.123   172.16.8.184    HTTP        667 HTTP/1.1 200 OK
  304 3.401353   172.16.8.184    34.104.35.123   HTTP        520 GET /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890aa9f3d87fbf4b64178fe7…
  305 3.411312   34.104.35.123   172.16.8.184    HTTP        692 HTTP/1.1 416 Requested range not satisfiable
  306 3.413839   172.16.8.184    34.104.35.123   HTTP        500 HEAD /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890aa9f3d87fbf4b64178fe…
  307 3.421452   34.104.35.123   172.16.8.184    HTTP        667 HTTP/1.1 200 OK
  311 3.449281   172.16.8.184    34.104.35.123   HTTP        520 GET /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890aa9f3d87fbf4b64178fe7…
  312 3.458242   34.104.35.123   172.16.8.184    HTTP        692 HTTP/1.1 416 Requested range not satisfiable
  313 3.459865   172.16.8.184    34.104.35.123   HTTP        500 HEAD /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890aa9f3d87fbf4b64178fe…
  321 3.471857   34.104.35.123   172.16.8.184    HTTP        667 HTTP/1.1 200 OK
```

Flow Graph output



```
> Frame 269: 731 bytes on wire (5848 bits), 731 bytes captured (5848 bits) on interface 0
> Ethernet II, Src: Sophos_cf:be:45 (7c:5a:1c:cf:be:45), Dst: 7c:57:58:34:fd:06 (7c:57:58:34:fd:06)
> Internet Protocol Version 4, Src: 34.104.35.123, Dst: 172.16.8.184
> Transmission Control Protocol, Src Port: 80, Dst Port: 50138, Seq: 1, Ack: 467, Len: 677
> Hypertext Transfer Protocol

0000  7c 57 58 34 fd 06 7c 5a  1c cf be 45 08 00 45 00   |WX4··|Z ···E··E·
0010  02 cd 4b e9 40 00 40 06  f1 96 22 68 23 7b ac 10   ··K·@·@· ··"h#{··
0020  08 b8 00 50 c3 da 19 df  11 77 66 c6 a6 6e 50 18   ···P···· ·wf··nP·
0030  00 ed 0c f9 00 00 48 54  54 50 2f 31 2e 31 20 34   ······HT TP/1.1 4
0040  31 36 20 52 65 71 75 65  73 74 65 64 20 72 61 6e   16 Reque sted ran
0050  67 65 20 6e 6f 74 20 73  61 74 69 73 66 69 61 62   ge not s atisfiab
0060  6c 65 0d 0a 6c 61 73 74  2d 6d 6f 64 69 66 69 65   le··last -modifie
0070  64 3a 20 54 68 75 2c 20  30 31 20 41 75 67 20 32   d: Thu,  01 Aug 2
0080  30 32 34 20 31 33 3a 31  37 3a 34 33 20 47 4d 54   024 13:1 7:43 GMT
0090  0d 0a 61 63 63 65 70 74  2d 72 61 6e 67 65 73 3a   ··accept -ranges:
00a0  20 6e 6f 6e 65 0d 0a 63  6f 6e 74 65 6e 74 2d 64    none··c ontent-d
00b0  69 73 70 6f 73 69 74 69  6f 6e 3a 20 61 74 74 61   ispositi on: atta
00c0  63 68 6d 65 6e 74 0d 0a  63 6f 6e 74 65 6e 74 2d   chment·· content-
00d0  73 65 63 75 72 69 74 79  2d 70 6f 6c 69 63 79 3a   security -policy:
00e0  20 64 65 66 61 75 6c 74  2d 73 72 63 20 27 6e 6f    default -src 'no
00f0  6e 65 27 0d 0a 73 65 72  76 65 72 3a 20 47 6f 6f   ne'··ser ver: Goo
0100  67 6c 65 2d 45 64 67 65  2d 43 61 63 68 65 0d 0a   gle-Edge -Cache··
0110  78 2d 63 6f 6e 74 65 6e  74 2d 74 79 70 65 2d 6f   x-conten t-type-o
0120  70 74 69 6f 6e 73 3a 20  6e 6f 73 6e 69 66 66 0d   ptions:  nosniff·
0130  0a 78 2d 66 72 61 6d 65  2d 6f 70 74 69 6f 6e 73   ·x-frame -options
0140  3a 20 53 41 4d 45 4f 52  49 47 49 4e 0d 0a 78 2d   : SAMEOR IGIN··x-
0150  78 73 73 2d 70 72 6f 74  65 63 74 69 6f 6e 3a 20   xss-prot ection: 
0160  30 0d 0a 64 61 74 65 3a  20 57 65 64 2c 20 30 37   0··date:  Wed, 07
0170  20 41 75 67 20 32 30 32  34 20 30 39 3a 30 32 3a    Aug 202 4 09:02:
0180  30 36 20 47 4d 54 0d 0a  61 67 65 3a 20 36 36 33   06 GMT·· age: 663
0190  35 31 0d 0a 63 6f 6e 74  65 6e 74 2d 74 79 70 65   51··cont ent-type
01a0  3a 20 61 70 70 6c 69 63  61 74 69 6f 6e 2f 6f 63   : applic ation/oc
01b0  74 65 74 2d 73 74 72 65  61 6d 0d 0a 78 2d 72 65   tet-stre am··x-re
01c0  71 75 65 73 74 2d 69 64  3a 20 61 61 37 35 34 63   quest-id : aa754c
01d0  38 36 2d 66 39 61 34 2d  34 34 33 34 2d 61 35 33   86-f9a4- 4434-a53
01e0  62 2d 39 31 34 32 32 32  39 37 39 61 34 66 0d 0a   b-914222 979a4f··
01f0  63 6f 6e 74 65 6e 74 2d  6c 65 6e 67 74 68 3a 20   content- length: 
0200  30 0d 0a 65 74 61 67 3a  20 22 32 65 61 33 35 30   0··etag:  "2ea350
0210  34 22 0d 0a 61 6c 74 2d  73 76 63 3a 20 68 33 3d   4"··alt- svc: h3=
0220  22 3a 34 34 33 22 3b 20  6d 61 3d 32 35 39 32 30   ":443";  ma=25920
0230  30 30 2c 20 68 33 2d 32  39 3d 22 3a 34 34 33 22   00, h3-2 9=":443"
0240  3b 20 6d 61 3d 32 35 39  32 30 30 30 0d 0a 63 61   ; ma=259 2000··ca
0250  63 68 65 2d 63 6f 6e 74  72 6f 6c 3a 20 70 75 62   che-cont rol: pub
0260  6c 69 63 2c 6d 61 78 2d  61 67 65 3d 38 36 34 30   lic,max- age=8640
0270  30 0d 0a 63 6f 70 72 6f  63 65 73 73 6f 72 2d 72   0··copro cessor-r
0280  65 73 70 6f 6e 73 65 3a  20 64 6f 77 6e 6c 6f 61   esponse:  downloa
0290  64 2d 73 65 72 76 65 72  0d 0a 56 69 61 3a 20 48   d-server ··Via: H
```

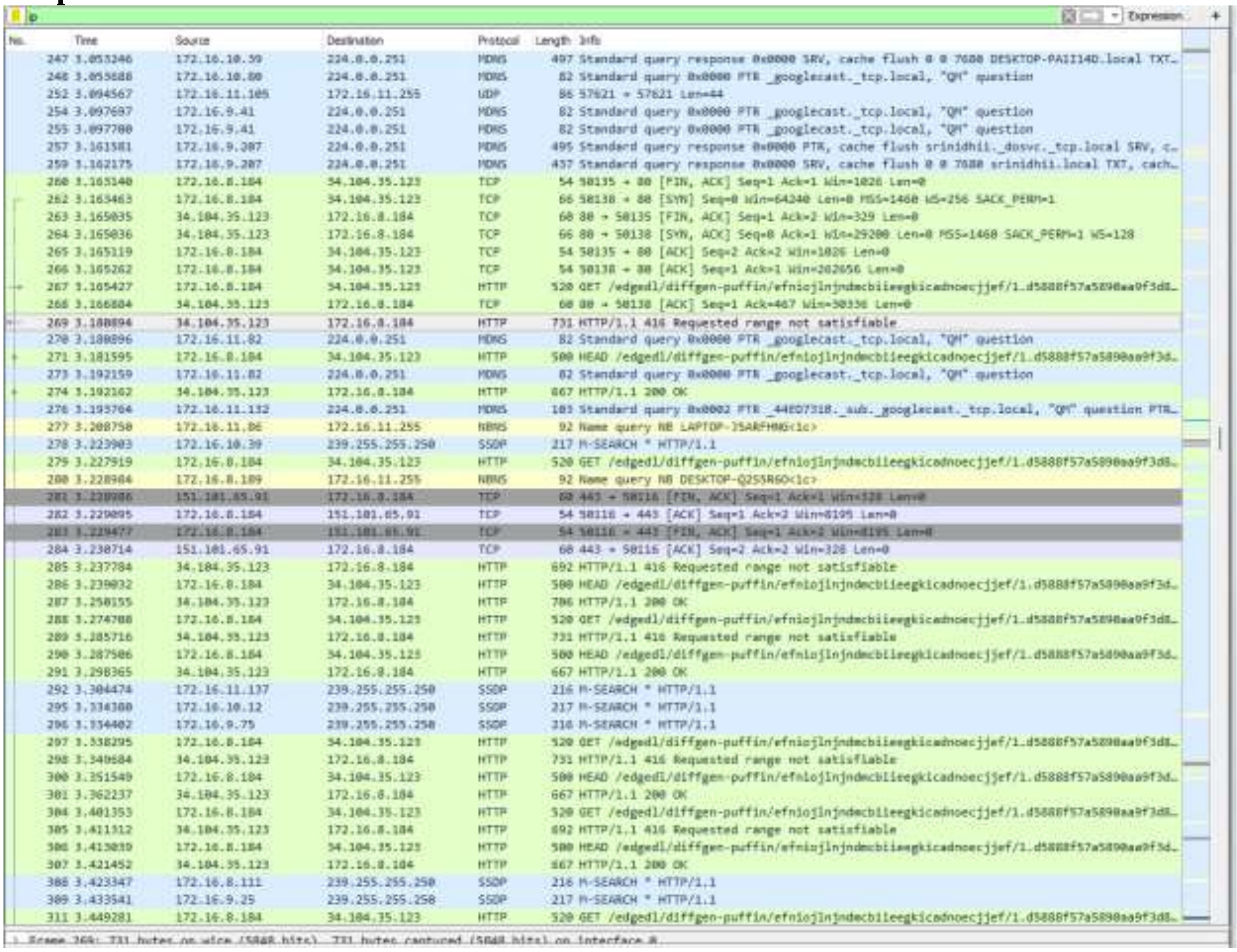
6.Create a Filter to display only IP/ICMP packets and inspect the packets.

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

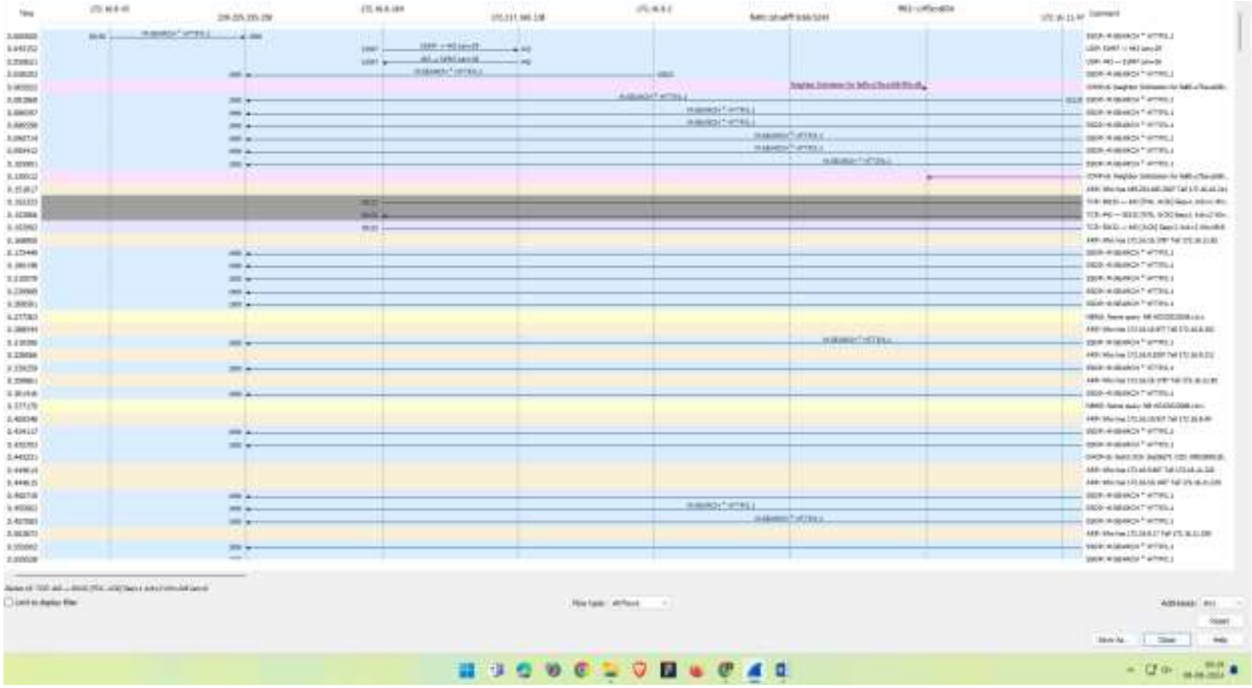


ip

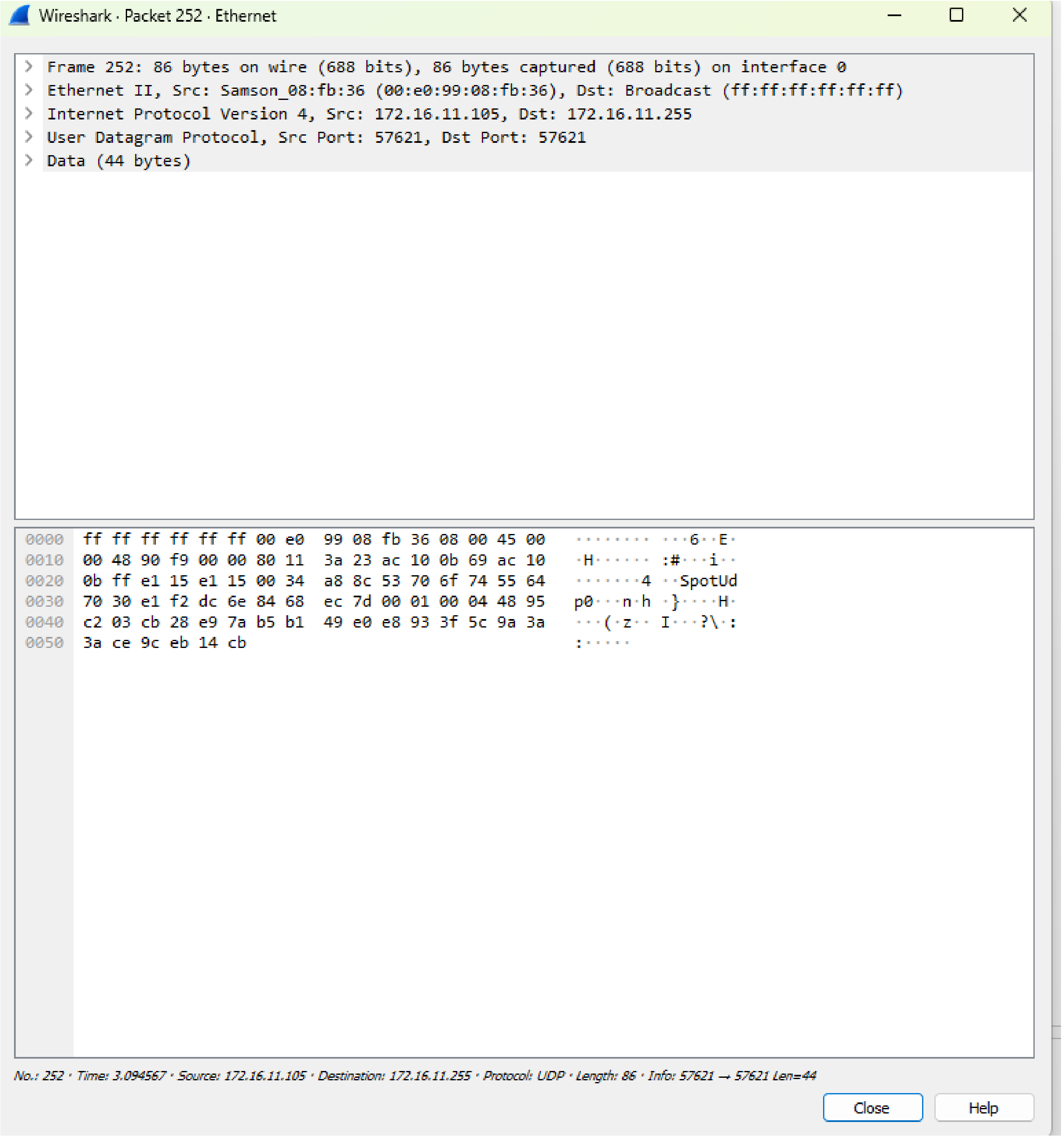
No.	Time	Source	Destination	Protocol	Length	Info
247	3.053246	172.16.10.39	224.0.0.251	MDNS	497	Standard query response 0x0000 SRV, cache flush 0 0 7680 DESKTOP-PAII14D.local TXT…
248	3.053688	172.16.10.80	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
252	3.094567	172.16.11.105	172.16.11.255	UDP	86	57621 → 57621 Len=44
254	3.097697	172.16.9.41	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
255	3.097700	172.16.9.41	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
257	3.161581	172.16.9.207	224.0.0.251	MDNS	495	Standard query response 0x0000 PTR, cache flush srinidhii._dosvc._tcp.local SRV, c…
259	3.162175	172.16.9.207	224.0.0.251	MDNS	437	Standard query response 0x0000 SRV, cache flush 0 0 7680 srinidhii.local TXT, cach…
260	3.163140	172.16.8.184	34.104.35.123	TCP	54	50135 → 80 [FIN, ACK] Seq=1 Ack=1 Win=1026 Len=0
262	3.163463	172.16.8.184	34.104.35.123	TCP	66	50138 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
263	3.165035	34.104.35.123	172.16.8.184	TCP	60	80 → 50135 [FIN, ACK] Seq=1 Ack=2 Win=329 Len=0
264	3.165036	34.104.35.123	172.16.8.184	TCP	66	80 → 50138 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
265	3.165119	172.16.8.184	34.104.35.123	TCP	54	50135 → 80 [ACK] Seq=2 Ack=2 Win=1026 Len=0
266	3.165262	172.16.8.184	34.104.35.123	TCP	54	50138 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
267	3.165427	172.16.8.184	34.104.35.123	HTTP	520	GET /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890aa9f3d8…
268	3.166804	34.104.35.123	172.16.8.184	TCP	60	80 → 50138 [ACK] Seq=1 Ack=467 Win=30336 Len=0
269	3.180894	34.104.35.123	172.16.8.184	HTTP	731	HTTP/1.1 416 Requested range not satisfiable
270	3.180896	172.16.11.82	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
271	3.181595	172.16.8.184	34.104.35.123	HTTP	500	HEAD /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890aa9f3d…
273	3.192159	172.16.11.82	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
274	3.192162	34.104.35.123	172.16.8.184	HTTP	667	HTTP/1.1 200 OK
276	3.193764	172.16.11.132	224.0.0.251	MDNS	103	Standard query 0x0002 PTR _44ED7318._sub._googlecast._tcp.local, "QM" question PTR…
277	3.208758	172.16.11.86	172.16.11.255	NBNS	92	Name query NB LAPTOP-J5ARFHNG<1c>
278	3.223903	172.16.10.39	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
279	3.227919	172.16.8.184	34.104.35.123	HTTP	520	GET /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890aa9f3d8…
280	3.228984	172.16.8.189	172.16.11.255	NBNS	92	Name query NB DESKTOP-Q2S5R6O<1c>
281	3.228986	151.101.65.91	172.16.8.184	TCP	60	443 → 50116 [FIN, ACK] Seq=1 Ack=1 Win=328 Len=0
282	3.229095	172.16.8.184	151.101.65.91	TCP	54	50116 → 443 [ACK] Seq=1 Ack=2 Win=8195 Len=0
283	3.229477	172.16.8.184	151.101.65.91	TCP	54	50116 → 443 [FIN, ACK] Seq=1 Ack=2 Win=8195 Len=0
284	3.230714	151.101.65.91	172.16.8.184	TCP	60	443 → 50116 [ACK] Seq=2 Ack=2 Win=328 Len=0
285	3.237784	34.104.35.123	172.16.8.184	HTTP	692	HTTP/1.1 416 Requested range not satisfiable
286	3.239032	172.16.8.184	34.104.35.123	HTTP	500	HEAD /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890aa9f3d…
287	3.250155	34.104.35.123	172.16.8.184	HTTP	706	HTTP/1.1 200 OK
288	3.274708	172.16.8.184	34.104.35.123	HTTP	520	GET /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890aa9f3d8…
289	3.285716	34.104.35.123	172.16.8.184	HTTP	731	HTTP/1.1 416 Requested range not satisfiable
290	3.287506	172.16.8.184	34.104.35.123	HTTP	500	HEAD /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5d90aa9f3d…
291	3.298365	34.104.35.123	172.16.8.184	HTTP	667	HTTP/1.1 200 OK
292	3.304474	172.16.11.137	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
295	3.334380	172.16.10.12	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
296	3.334402	172.16.9.75	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
297	3.338295	172.16.8.184	34.104.35.123	HTTP	520	GET /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890aa9f3d8…
298	3.340684	34.104.35.123	172.16.8.184	HTTP	731	HTTP/1.1 416 Requested range not satisfiable
300	3.351540	172.16.8.184	34.104.35.123	HTTP	500	HEAD /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890aa9f3d…
301	3.362237	34.104.35.123	172.16.8.184	HTTP	667	HTTP/1.1 200 OK
304	3.401353	172.16.8.184	34.104.35.123	HTTP	520	GET /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890aa9f3d8…
305	3.411312	34.104.35.123	172.16.8.184	HTTP	692	HTTP/1.1 416 Requested range not satisfiable
306	3.413030	172.16.8.184	34.104.35.123	HTTP	500	HEAD /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890aa9f3d…
307	3.421452	34.104.35.123	172.16.8.184	HTTP	667	HTTP/1.1 200 OK
308	3.423347	172.16.8.111	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
309	3.433541	172.16.9.25	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
311	3.449281	172.16.8.184	34.104.35.123	HTTP	520	GET /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.d5888f57a5890aa9f3d8…

Frame 269: 731 bytes on wire (5848 bits), 731 bytes captured (5848 bits) on interface 0

Flow Graph output



```
Time                                                                  Comment
[illegible]                                                           SSDP: M-SEARCH * HTTP/1.1
[illegible]                                                           [illegible]
```



```
> Frame 252: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
> Ethernet II, Src: Samson_08:fb:36 (00:e0:99:08:fb:36), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 172.16.11.105, Dst: 172.16.11.255
> User Datagram Protocol, Src Port: 57621, Dst Port: 57621
> Data (44 bytes)
```

```
0000  ff ff ff ff ff ff 00 e0  99 08 fb 36 08 00 45 00   ········ ···6··E·
0010  00 48 90 f9 00 00 80 11  3a 23 ac 10 0b 69 ac 10   ·H······ :#···i··
0020  0b ff e1 15 e1 15 00 34  a8 8c 53 70 6f 74 55 64   ·······4 ··SpotUd
0030  70 30 e1 f2 dc 6e 84 68  ec 7d 00 01 00 04 48 95   p0···n·h ·}····H·
0040  c2 03 cb 28 e9 7a b5 b1  49 e0 e8 93 3f 5c 9a 3a   ···(·z·· I···?\·:
0050  3a ce 9c eb 14 cb                                  :·····
```

No.: 252 · Time: 3.094567 · Source: 172.16.11.105 · Destination: 172.16.11.255 · Protocol: UDP · Length: 86 · Info: 57621 → 57621 Len=44

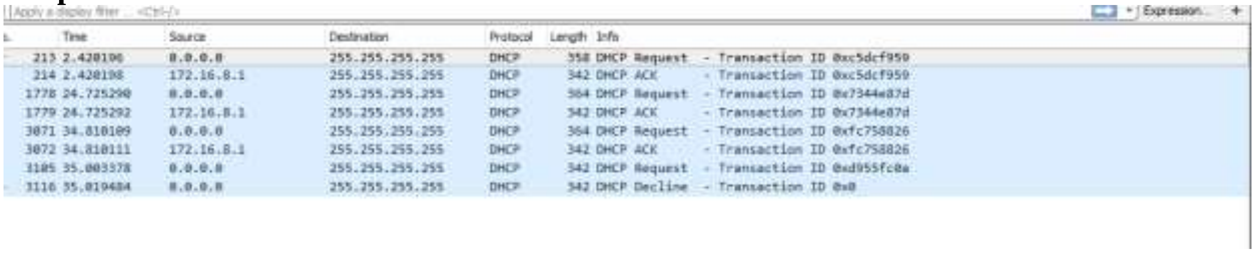
7.Create a Filter to display only DHCP packets and inspect the packets.

Procedure

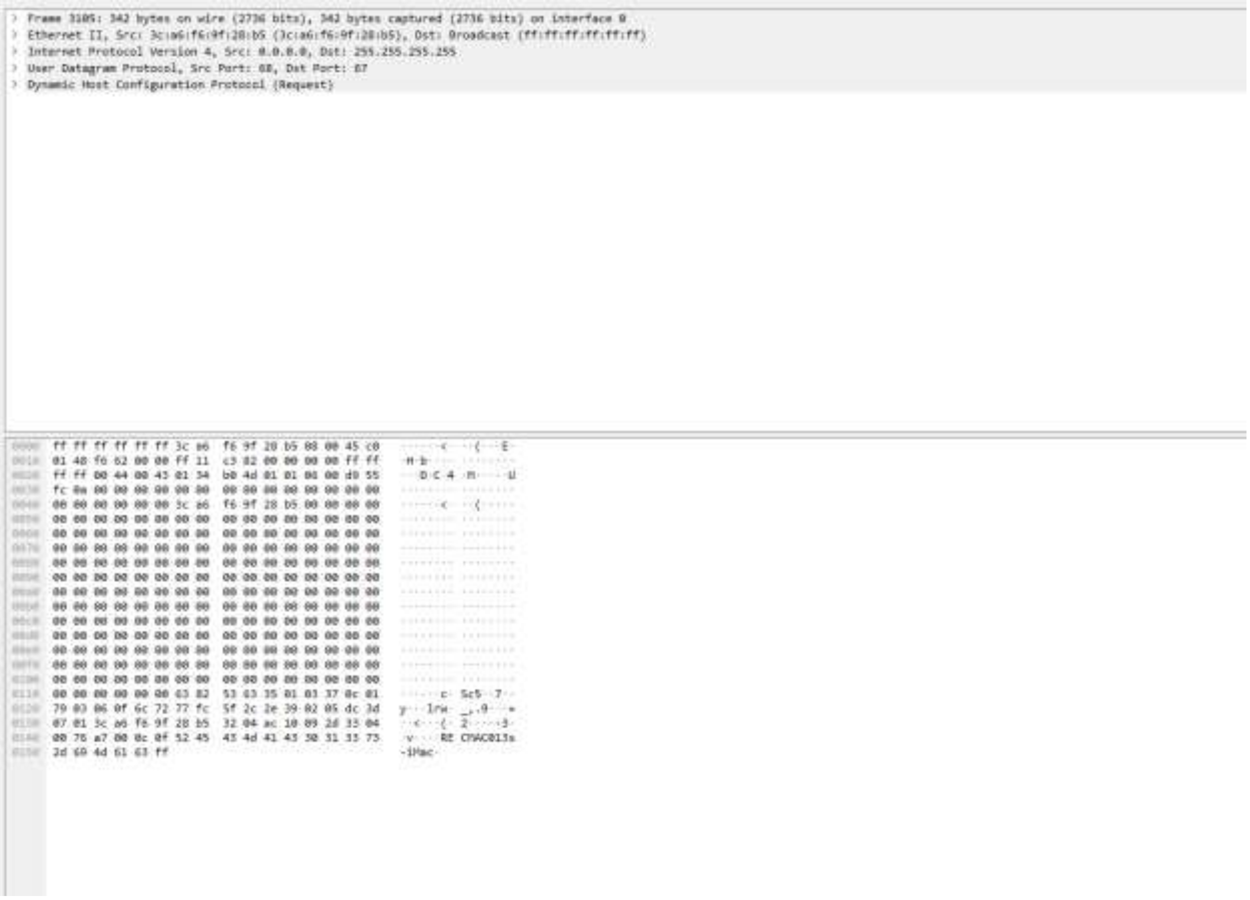
- □ Select Local Area Connection in Wireshark.
- □ Go to capture ⚇option
- □ Select stop capture automatically after 100 packets.
- □ Then click Start capture.

- □ Search DHCP packets in search bar.
- □ Save the packets

Output



.	Time	Source	Destination	Protocol	Length	Info
213	2.420106	0.0.0.0	255.255.255.255	DHCP	358	DHCP Request - Transaction ID 0xc5dcf959
214	2.420198	172.16.8.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xc5dcf959
1778	24.725290	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x7344e87d
1779	24.725292	172.16.8.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x7344e87d
3071	34.810109	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0xfc758826
3072	34.810111	172.16.8.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xfc758826
3105	35.003378	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xd955fc0a
3116	35.019484	0.0.0.0	255.255.255.255	DHCP	342	DHCP Decline - Transaction ID 0x0



```
> Frame 3105: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
> Ethernet II, Src: 3c:a6:f6:9f:28:b5 (3c:a6:f6:9f:28:b5), 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 3c a6  f6 9f 28 b5 08 00 45 c0   ······<· ··(···E·
0010  01 48 f6 62 00 00 ff 11  c3 82 00 00 00 00 ff ff   ·H·b···· ········
0020  ff ff 00 44 00 43 01 34  b0 4d 01 01 00 00 d0 55   ···D·C·4 ·M·····U
0030  fc 0a 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 3c a6  f6 9f 28 b5 00 00 00 00   ······<· ··(·····
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 37 0c 01   ······c· Sc5··7··
0120  79 03 06 0f 6c 72 77 fc  5f 2c 2e 39 02 05 dc 3d   y···lrw· _,.9···=
0130  07 01 3c a6 f6 9f 28 b5  32 04 ac 10 09 2d 33 04   ··<···(· 2····-3·
0140  00 76 a7 00 0c 0f 52 45  43 4d 41 43 30 31 33 73   ·v····RE CMAC013s
0150  3d 69 4d 61 63 ff                                  =iMac·
```