Network Assignment 5

Name :- Debargha Mukherjee Roll :- 001910501067

Overview : Wireshark is an open source cross-platform packet capture and analysis tool, with versions for Windows and Linux. The GUI window gives a detailed breakdown of the network protocol stack for each packet, colorizing packet details based on protocol, as well as having functionality to filter and search the traffic, and pick out TCP streams. Wireshark can also save packet data to files for offline analysis and export/import packet captures to/from other tools. Statistics can also be generated for packet capture files.

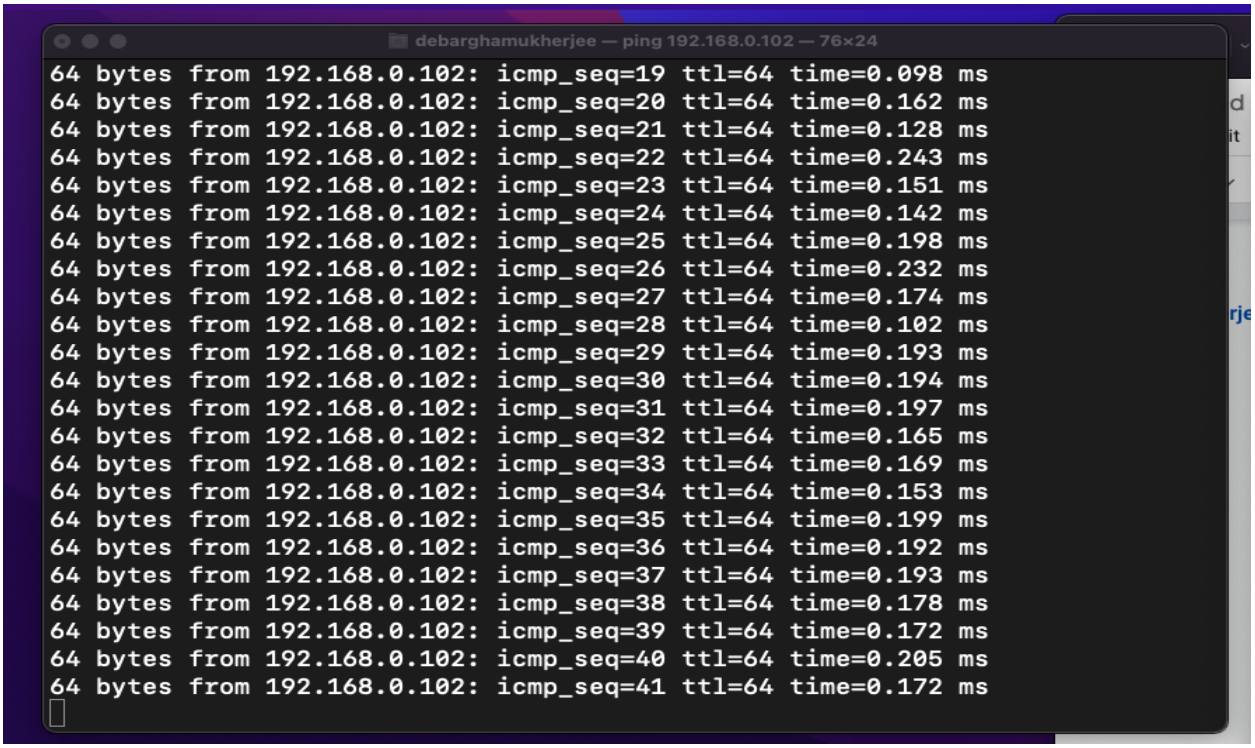
Problem Statement : Install wireshark in local machine and capture and analyse various packets according to the given questions.

System Specifications:

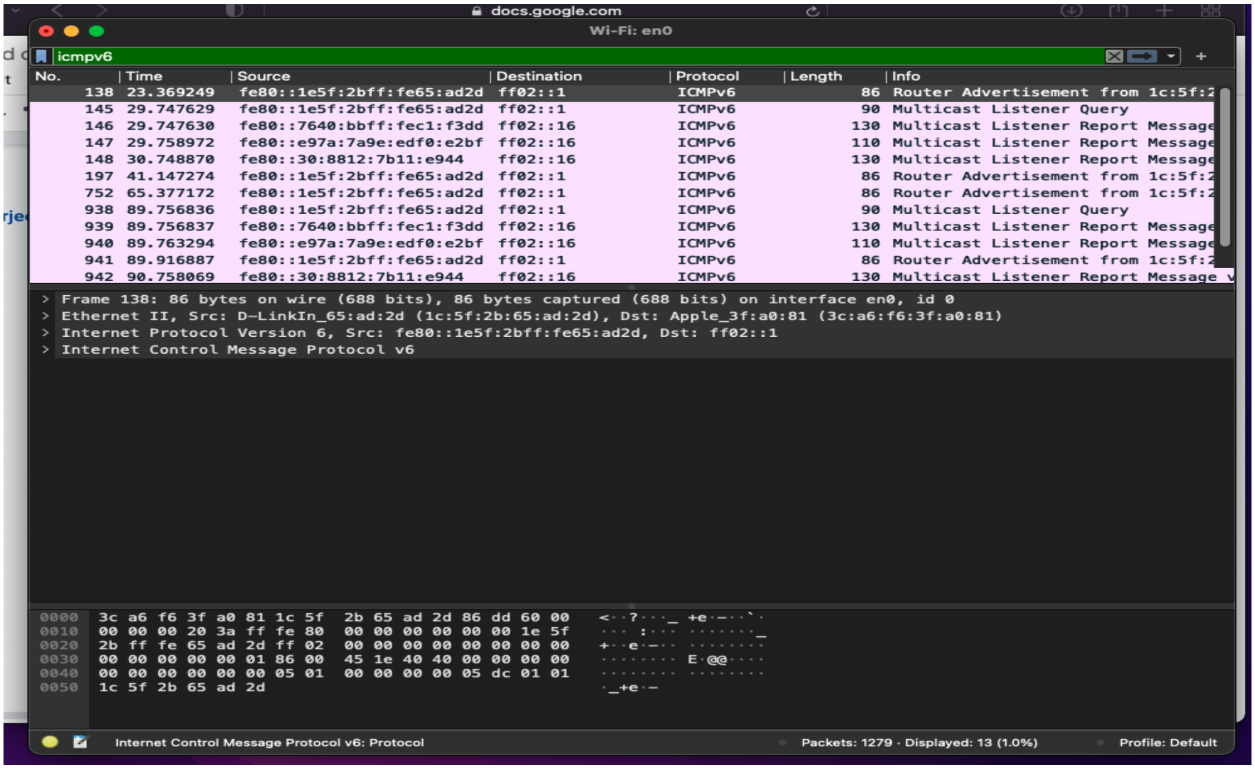
1. System OS Type :- Linux
2. System OS :- Mac OS Monterey
3. wireshark :- 3.2.7
4. Network :- Wireless Network (WIFI)

Questions and Solutions :

Q1. Generate some ICMP traffic by using the Ping command line tool to check the connectivity of a neighbouring machine (or router). Note the results in Wireshark. The initial ARP request broadcast from your PC determines the physical MAC address of the network IP Address, and the ARP reply from the neighboring system. After the ARP request, the pings (ICMP echo request and replies) can be seen.



```
64 bytes from 192.168.0.102: icmp_seq=19 ttl=64 time=0.098 ms
64 bytes from 192.168.0.102: icmp_seq=20 ttl=64 time=0.162 ms
64 bytes from 192.168.0.102: icmp_seq=21 ttl=64 time=0.128 ms
64 bytes from 192.168.0.102: icmp_seq=22 ttl=64 time=0.243 ms
64 bytes from 192.168.0.102: icmp_seq=23 ttl=64 time=0.151 ms
64 bytes from 192.168.0.102: icmp_seq=24 ttl=64 time=0.142 ms
64 bytes from 192.168.0.102: icmp_seq=25 ttl=64 time=0.198 ms
64 bytes from 192.168.0.102: icmp_seq=26 ttl=64 time=0.232 ms
64 bytes from 192.168.0.102: icmp_seq=27 ttl=64 time=0.174 ms
64 bytes from 192.168.0.102: icmp_seq=28 ttl=64 time=0.102 ms
64 bytes from 192.168.0.102: icmp_seq=29 ttl=64 time=0.193 ms
64 bytes from 192.168.0.102: icmp_seq=30 ttl=64 time=0.194 ms
64 bytes from 192.168.0.102: icmp_seq=31 ttl=64 time=0.197 ms
64 bytes from 192.168.0.102: icmp_seq=32 ttl=64 time=0.165 ms
64 bytes from 192.168.0.102: icmp_seq=33 ttl=64 time=0.169 ms
64 bytes from 192.168.0.102: icmp_seq=34 ttl=64 time=0.153 ms
64 bytes from 192.168.0.102: icmp_seq=35 ttl=64 time=0.199 ms
64 bytes from 192.168.0.102: icmp_seq=36 ttl=64 time=0.192 ms
64 bytes from 192.168.0.102: icmp_seq=37 ttl=64 time=0.193 ms
64 bytes from 192.168.0.102: icmp_seq=38 ttl=64 time=0.178 ms
64 bytes from 192.168.0.102: icmp_seq=39 ttl=64 time=0.172 ms
64 bytes from 192.168.0.102: icmp_seq=40 ttl=64 time=0.205 ms
64 bytes from 192.168.0.102: icmp_seq=41 ttl=64 time=0.172 ms
```



```
No.    | Time      | Source                    | Destination | Protocol | Length | Info
   138 23.369249  fe80::1e5f:2bff:fe65:ad2d  ff02::1      ICMPv6         86 Router Advertisement from 1c:5f:2
   145 29.747629  fe80::1e5f:2bff:fe65:ad2d  ff02::1      ICMPv6         90 Multicast Listener Query
   146 29.747630  fe80::7640:bbff:fec1:f3dd  ff02::16     ICMPv6        130 Multicast Listener Report Message
   147 29.758972  fe80::e97a:7a9e:edf0:e2bf  ff02::16     ICMPv6        110 Multicast Listener Report Message
   148 30.748870  fe80::30:8812:7b11:e944    ff02::16     ICMPv6        130 Multicast Listener Report Message
   197 41.147274  fe80::1e5f:2bff:fe65:ad2d  ff02::1      ICMPv6         86 Router Advertisement from 1c:5f:2
   752 65.377172  fe80::1e5f:2bff:fe65:ad2d  ff02::1      ICMPv6         86 Router Advertisement from 1c:5f:2
   938 89.756836  fe80::1e5f:2bff:fe65:ad2d  ff02::1      ICMPv6         90 Multicast Listener Query
   939 89.756837  fe80::7640:bbff:fec1:f3dd  ff02::16     ICMPv6        130 Multicast Listener Report Message
   940 89.763294  fe80::e97a:7a9e:edf0:e2bf  ff02::16     ICMPv6        110 Multicast Listener Report Message
   941 89.916887  fe80::1e5f:2bff:fe65:ad2d  ff02::1      ICMPv6         86 Router Advertisement from 1c:5f:2
   942 90.758069  fe80::30:8812:7b11:e944    ff02::16     ICMPv6        130 Multicast Listener Report Message v
```

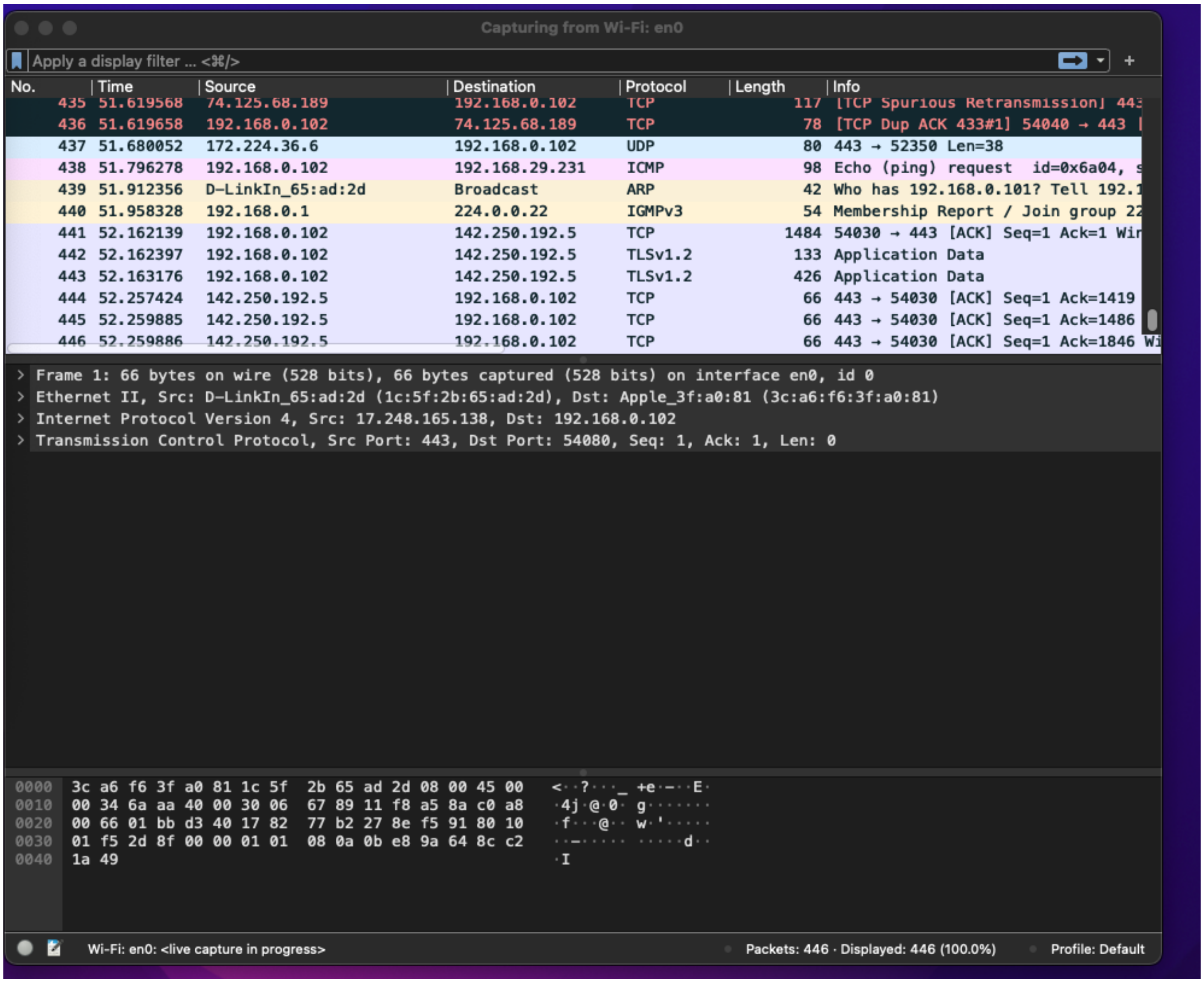
```
> Frame 138: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface en0, id 0
> Ethernet II, Src: D-LinkIn_65:ad:2d (1c:5f:2b:65:ad:2d), Dst: Apple_3f:a0:81 (3c:a6:f6:3f:a0:81)
> Internet Protocol Version 6, Src: fe80::1e5f:2bff:fe65:ad2d, Dst: ff02::1
> Internet Control Message Protocol v6
```

```
0000  3c a6 f6 3f a0 81 1c 5f  2b 65 ad 2d 86 dd 60 00   <··?···_ +e·-··`·
0010  00 00 00 20 3a ff fe 80  00 00 00 00 00 00 1e 5f   ··· :··· ·······_
0020  2b ff fe 65 ad 2d ff 02  00 00 00 00 00 00 00 00   +··e·-·· ········
0030  00 00 00 00 00 01 86 00  45 1e 40 40 00 00 00 00   ········ E·@@····
0040  00 00 00 00 00 00 05 01  00 00 00 00 05 dc 01 01   ········ ········
0050  1c 5f 2b 65 ad 2d                                  ·_+e·-
```

```
Internet Control Message Protocol v6: Protocol          Packets: 1279 · Displayed: 13 (1.0%)          Profile: Default
```

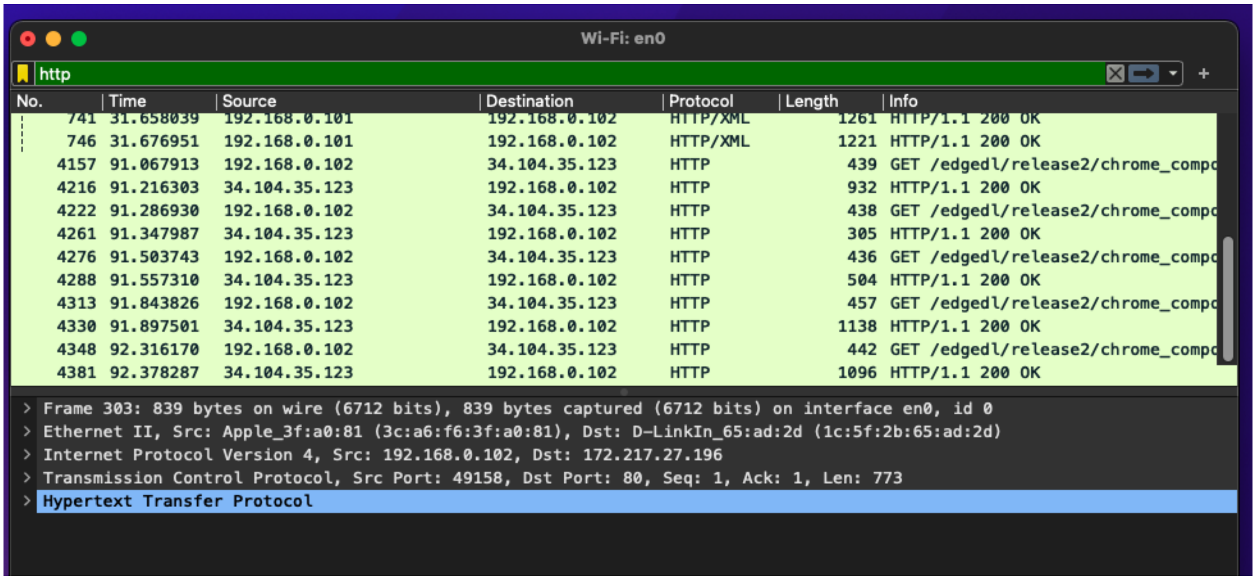
2. Generate some web traffic and

a. find the list the different protocols that appear in the protocol column in the unfiltered packet-listing window of Wireshark.



```
No.   | Time      | Source            | Destination    | Protocol | Length | Info
  435 51.619568  74.125.68.189       192.168.0.102    TCP         117 [TCP Spurious Retransmission] 443
  436 51.619658  192.168.0.102       74.125.68.189    TCP          78 [TCP Dup ACK 433#1] 54040 → 443 [
  437 51.680052  172.224.36.6        192.168.0.102    UDP          80 443 → 52350 Len=38
  438 51.796278  192.168.0.102       192.168.29.231   ICMP         98 Echo (ping) request  id=0x6a04, s
  439 51.912356  D-LinkIn_65:ad:2d   Broadcast        ARP          42 Who has 192.168.0.101? Tell 192.1
  440 51.958328  192.168.0.1         224.0.0.22       IGMPv3       54 Membership Report / Join group 22
  441 52.162139  192.168.0.102       142.250.192.5    TCP        1484 54030 → 443 [ACK] Seq=1 Ack=1 Wir
  442 52.162397  192.168.0.102       142.250.192.5    TLSv1.2     133 Application Data
  443 52.163176  192.168.0.102       142.250.192.5    TLSv1.2     426 Application Data
  444 52.257424  142.250.192.5       192.168.0.102    TCP          66 443 → 54030 [ACK] Seq=1 Ack=1419
  445 52.259885  142.250.192.5       192.168.0.102    TCP          66 443 → 54030 [ACK] Seq=1 Ack=1486
  446 52.259886  142.250.192.5       192.168.0.102    TCP          66 443 → 54030 [ACK] Seq=1 Ack=1846 Wi

> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en0, id 0
> Ethernet II, Src: D-LinkIn_65:ad:2d (1c:5f:2b:65:ad:2d), Dst: Apple_3f:a0:81 (3c:a6:f6:3f:a0:81)
> Internet Protocol Version 4, Src: 17.248.165.138, Dst: 192.168.0.102
> Transmission Control Protocol, Src Port: 443, Dst Port: 54080, Seq: 1, Ack: 1, Len: 0

0000  3c a6 f6 3f a0 81 1c 5f  2b 65 ad 2d 08 00 45 00   <··?···_ +e·–··E·
0010  00 34 6a aa 40 00 30 06  67 89 11 f8 a5 8a c0 a8   ·4j·@·0· g·······
0020  00 66 01 bb d3 40 17 82  77 b2 27 8e f5 91 80 10   ·f···@·· w·'·····
0030  01 f5 2d 8f 00 00 01 01  08 0a 0b e8 9a 64 8c c2   ··–····· ·····d··
0040  1a 49                                              ·I

Wi-Fi: en0: <live capture in progress>          Packets: 446 · Displayed: 446 (100.0%)     Profile: Default
```

b. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)



No.	Time	Source	Destination	Protocol	Length	Info
741	31.658039	192.168.0.101	192.168.0.102	HTTP/XML	1261	HTTP/1.1 200 OK
746	31.676951	192.168.0.101	192.168.0.102	HTTP/XML	1221	HTTP/1.1 200 OK
4157	91.067913	192.168.0.102	34.104.35.123	HTTP	439	GET /edgedl/release2/chrome_compo
4216	91.216303	34.104.35.123	192.168.0.102	HTTP	932	HTTP/1.1 200 OK
4222	91.286930	192.168.0.102	34.104.35.123	HTTP	438	GET /edgedl/release2/chrome_compo
4261	91.347987	34.104.35.123	192.168.0.102	HTTP	305	HTTP/1.1 200 OK
4276	91.503743	192.168.0.102	34.104.35.123	HTTP	436	GET /edgedl/release2/chrome_compo
4288	91.557310	34.104.35.123	192.168.0.102	HTTP	504	HTTP/1.1 200 OK
4313	91.843826	192.168.0.102	34.104.35.123	HTTP	457	GET /edgedl/release2/chrome_compo
4330	91.897501	34.104.35.123	192.168.0.102	HTTP	1138	HTTP/1.1 200 OK
4348	92.316170	192.168.0.102	34.104.35.123	HTTP	442	GET /edgedl/release2/chrome_compo
4381	92.378287	34.104.35.123	192.168.0.102	HTTP	1096	HTTP/1.1 200 OK

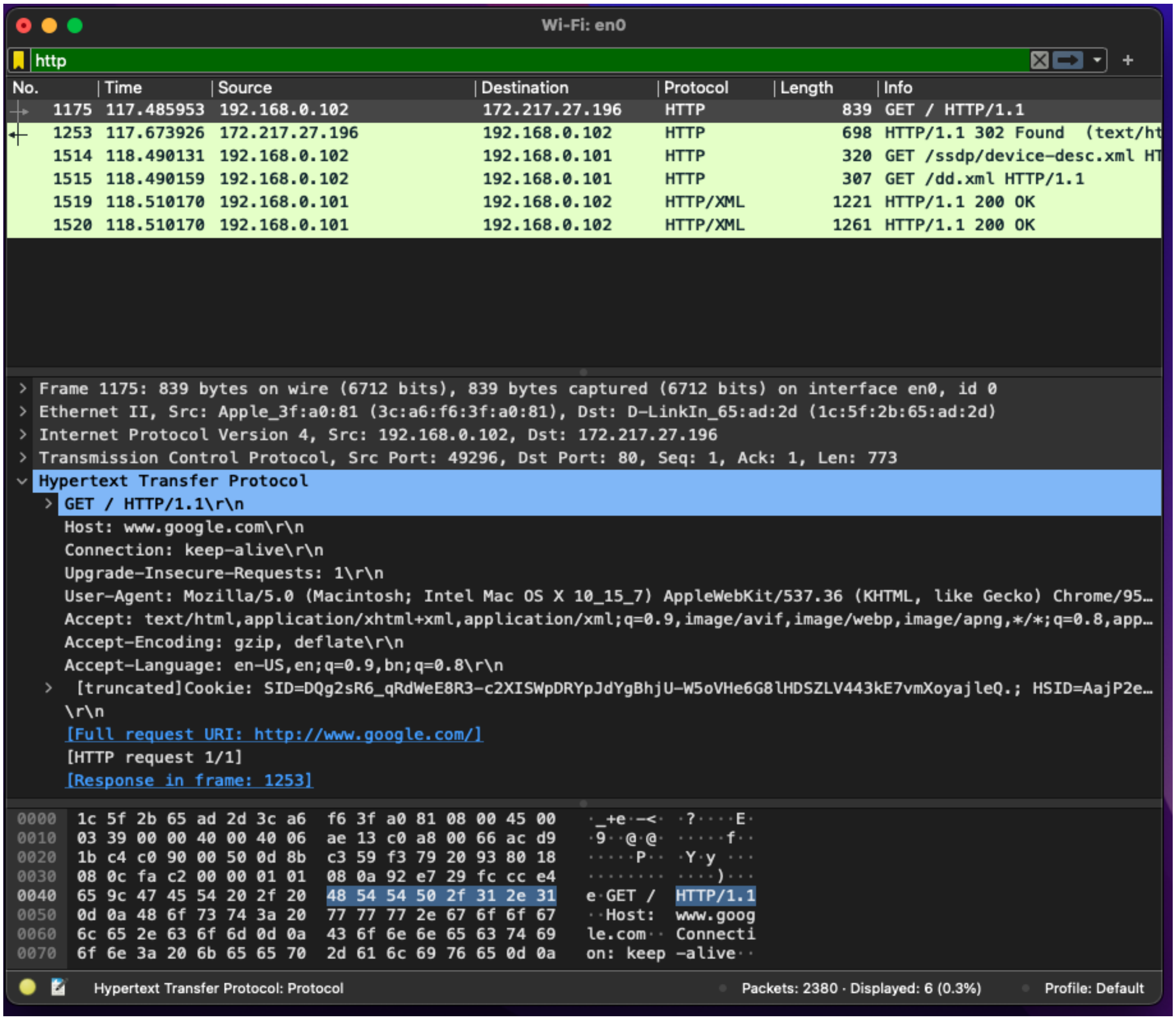
```
> Frame 303: 839 bytes on wire (6712 bits), 839 bytes captured (6712 bits) on interface en0, id 0
> Ethernet II, Src: Apple_3f:a0:81 (3c:a6:f6:3f:a0:81), Dst: D-LinkIn_65:ad:2d (1c:5f:2b:65:ad:2d)
> Internet Protocol Version 4, Src: 192.168.0.102, Dst: 172.217.27.196
> Transmission Control Protocol, Src Port: 49158, Dst Port: 80, Seq: 1, Ack: 1, Len: 773
> Hypertext Transfer Protocol
```

As shown in the screenshot above the GET(4157) was sent at 91.067913 and the OK was received at 91.216303 second. Thus the total delay (91.216303 - 91.067913) = 0.1483 seconds.

c. What is the Internet address of the website? What is the Internet address of your computer?

From the above ss it is clearly visible that the ip address of my computer is 192.168.0.102 and the ip address of the website is 34.104.35.123

d. Search back through your capture, and find an HTTP packet containing a GET command. Click on the packet in the Packet List Panel. Then expand the HTTP layer in the Packet Details Panel, from the packet.



```
No.     Time        Source          Destination     Protocol  Length  Info
1175    117.485953  192.168.0.102   172.217.27.196  HTTP         839  GET / HTTP/1.1
1253    117.673926  172.217.27.196  192.168.0.102   HTTP         698  HTTP/1.1 302 Found  (text/ht
1514    118.490131  192.168.0.102   192.168.0.101   HTTP         320  GET /ssdp/device-desc.xml HT
1515    118.490159  192.168.0.102   192.168.0.101   HTTP         307  GET /dd.xml HTTP/1.1
1519    118.510170  192.168.0.101   192.168.0.102   HTTP/XML    1221  HTTP/1.1 200 OK
1520    118.510170  192.168.0.101   192.168.0.102   HTTP/XML    1261  HTTP/1.1 200 OK
```

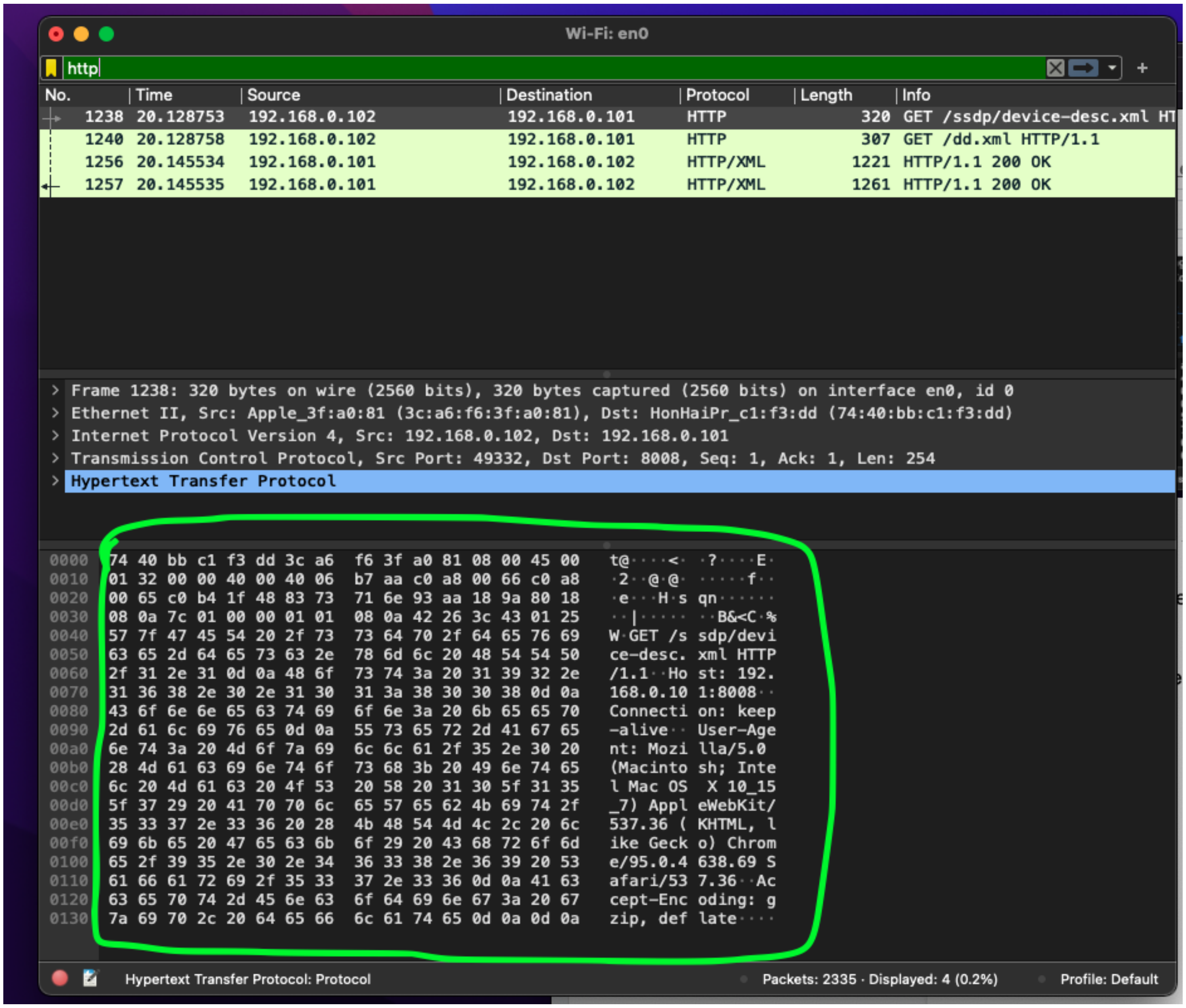
```
> Frame 1175: 839 bytes on wire (6712 bits), 839 bytes captured (6712 bits) on interface en0, id 0
> Ethernet II, Src: Apple_3f:a0:81 (3c:a6:f6:3f:a0:81), Dst: D-LinkIn_65:ad:2d (1c:5f:2b:65:ad:2d)
> Internet Protocol Version 4, Src: 192.168.0.102, Dst: 172.217.27.196
> Transmission Control Protocol, Src Port: 49296, Dst Port: 80, Seq: 1, Ack: 1, Len: 773
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: www.google.com\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95…
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,app…
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,bn;q=0.8\r\n
  >  [truncated]Cookie: SID=DQg2sR6_qRdWeE8R3-c2XISWpDRYpJdYgBhjU-W5oVHe6G8lHDSZLV443kE7vmXoyajleQ.; HSID=AajP2e…
    \r\n
    [Full request URI: http://www.google.com/]
    [HTTP request 1/1]
    [Response in frame: 1253]
```

```
0000  1c 5f 2b 65 ad 2d 3c a6  f6 3f a0 81 08 00 45 00   ·_+e·-<· ·?····E·
0010  03 39 00 00 40 00 40 06  ae 13 c0 a8 00 66 ac d9   ·9··@·@· ·····f··
0020  1b c4 c0 90 00 50 0d 8b  c3 59 f3 79 20 93 80 18   ·····P·· ·Y·y ···
0030  08 0c fa c2 00 00 01 01  08 0a 92 e7 29 fc cc e4   ········ ····)···
0040  65 9c 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 31   e·GET /  HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20  77 77 77 2e 67 6f 6f 67   ··Host:  www.goog
0060  6c 65 2e 63 6f 6d 0d 0a  43 6f 6e 6e 65 63 74 69   le.com·· Connecti
0070  6f 6e 3a 20 6b 65 65 70  2d 61 6c 69 76 65 0d 0a   on: keep -alive··
```

```
Hypertext Transfer Protocol: Protocol          Packets: 2380 · Displayed: 6 (0.3%)     Profile: Default
```

e. Find out the value of the Host from the Packet Details Panel, within the GET command.
The above screenshot shows that the host name is www.google.com

3. Highlight the Hex and ASCII representations of the packet in the Packet Bytes Panel.



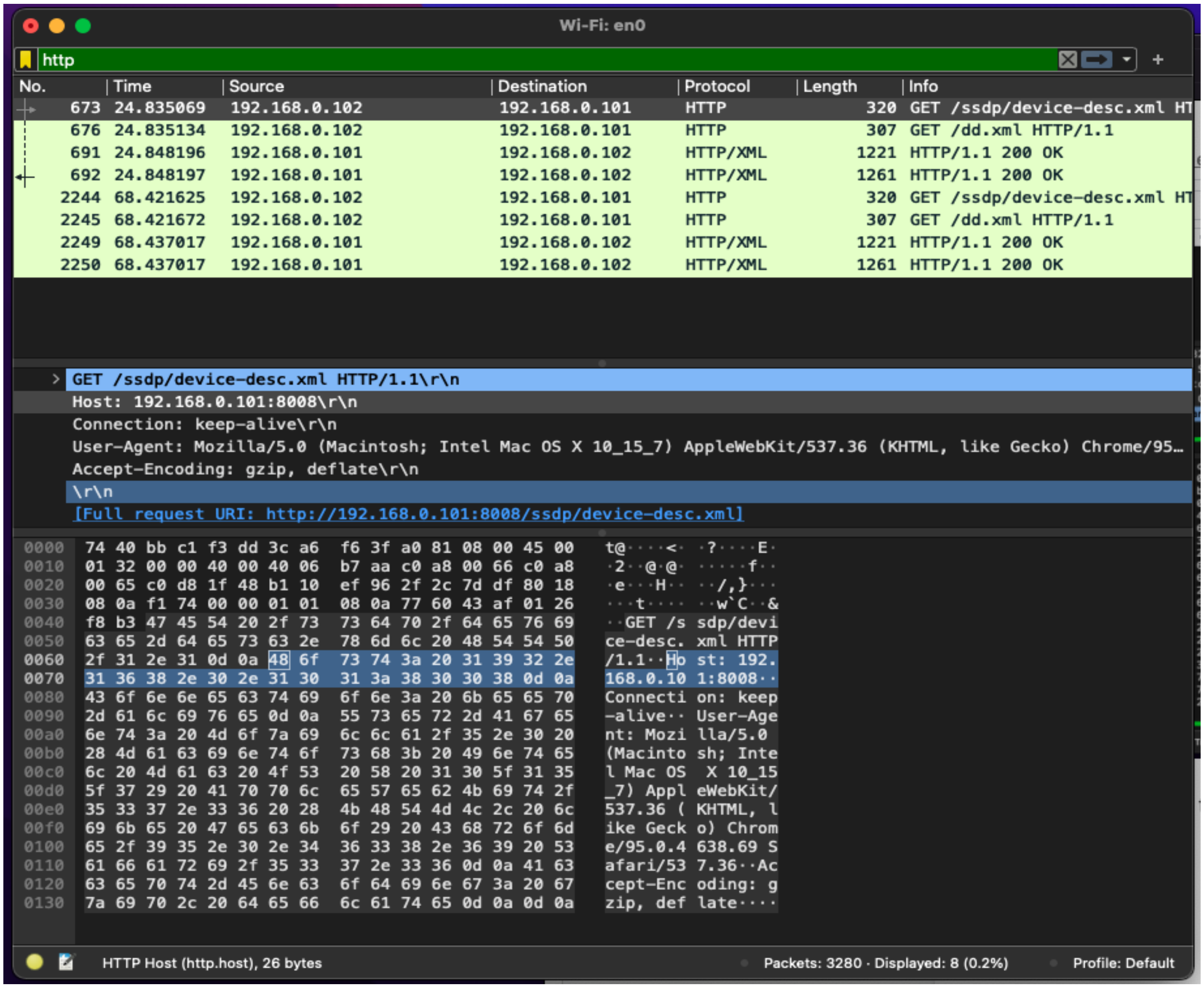
```
No.     Time       Source          Destination     Protocol  Length  Info
  1238  20.128753  192.168.0.102   192.168.0.101   HTTP         320  GET /ssdp/device-desc.xml HT
  1240  20.128758  192.168.0.102   192.168.0.101   HTTP         307  GET /dd.xml HTTP/1.1
  1256  20.145534  192.168.0.101   192.168.0.102   HTTP/XML    1221  HTTP/1.1 200 OK
  1257  20.145535  192.168.0.101   192.168.0.102   HTTP/XML    1261  HTTP/1.1 200 OK
```

```
> Frame 1238: 320 bytes on wire (2560 bits), 320 bytes captured (2560 bits) on interface en0, id 0
> Ethernet II, Src: Apple_3f:a0:81 (3c:a6:f6:3f:a0:81), Dst: HonHaiPr_c1:f3:dd (74:40:bb:c1:f3:dd)
> Internet Protocol Version 4, Src: 192.168.0.102, Dst: 192.168.0.101
> Transmission Control Protocol, Src Port: 49332, Dst Port: 8008, Seq: 1, Ack: 1, Len: 254
> Hypertext Transfer Protocol
```

```
0000  74 40 bb c1 f3 dd 3c a6  f6 3f a0 81 08 00 45 00   t@····<· ·?····E·
0010  01 32 00 00 40 00 40 06  b7 aa c0 a8 00 66 c0 a8   ·2··@·@· ·····f··
0020  00 65 c0 b4 1f 48 83 73  71 6e 93 aa 18 9a 80 18   ·e···H·s qn······
0030  08 0a 7c 01 00 00 01 01  08 0a 42 26 3c 43 01 25   ··|····· ··B&<C·%
0040  57 7f 47 45 54 20 2f 73  73 64 70 2f 64 65 76 69   W·GET /s sdp/devi
0050  63 65 2d 64 65 73 63 2e  78 6d 6c 20 48 54 54 50   ce-desc. xml HTTP
0060  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 31 39 32 2e   /1.1··Ho st: 192.
0070  31 36 38 2e 30 2e 31 30  31 3a 38 30 30 38 0d 0a   168.0.10 1:8008··
0080  43 6f 6e 6e 65 63 74 69  6f 6e 3a 20 6b 65 65 70   Connecti on: keep
0090  2d 61 6c 69 76 65 0d 0a  55 73 65 72 2d 41 67 65   -alive·· User-Age
00a0  6e 74 3a 20 4d 6f 7a 69  6c 6c 61 2f 35 2e 30 20   nt: Mozi lla/5.0
00b0  28 4d 61 63 69 6e 74 6f  73 68 3b 20 49 6e 74 65   (Macinto sh; Inte
00c0  6c 20 4d 61 63 20 4f 53  20 58 20 31 30 5f 31 35   l Mac OS  X 10_15
00d0  5f 37 29 20 41 70 70 6c  65 57 65 62 4b 69 74 2f   _7) Appl eWebKit/
00e0  35 33 37 2e 33 36 20 28  4b 48 54 4d 4c 2c 20 6c   537.36 ( KHTML, l
00f0  69 6b 65 20 47 65 63 6b  6f 29 20 43 68 72 6f 6d   ike Geck o) Chrom
0100  65 2f 39 35 2e 30 2e 34  36 33 38 2e 36 39 20 53   e/95.0.4 638.69 S
0110  61 66 61 72 69 2f 35 33  37 2e 33 36 0d 0a 41 63   afari/53 7.36··Ac
0120  63 65 70 74 2d 45 6e 63  6f 64 69 6e 67 3a 20 67   cept-Enc oding: g
0130  7a 69 70 2c 20 64 65 66  6c 61 74 65 0d 0a 0d 0a   zip, def late····
```

Hypertext Transfer Protocol: Protocol
Packets: 2335 · Displayed: 4 (0.2%)
Profile: Default

4. Find out the first 4 bytes of the Hex value of the Host parameter from the Packet Bytes Panel.



```
No.  | Time      | Source      | Destination | Protocol | Length | Info
 673  24.835069  192.168.0.102  192.168.0.101  HTTP       320  GET /ssdp/device-desc.xml HT
 676  24.835134  192.168.0.102  192.168.0.101  HTTP       307  GET /dd.xml HTTP/1.1
 691  24.848196  192.168.0.101  192.168.0.102  HTTP/XML  1221  HTTP/1.1 200 OK
 692  24.848197  192.168.0.101  192.168.0.102  HTTP/XML  1261  HTTP/1.1 200 OK
2244  68.421625  192.168.0.102  192.168.0.101  HTTP       320  GET /ssdp/device-desc.xml HT
2245  68.421672  192.168.0.102  192.168.0.101  HTTP       307  GET /dd.xml HTTP/1.1
2249  68.437017  192.168.0.101  192.168.0.102  HTTP/XML  1221  HTTP/1.1 200 OK
2250  68.437017  192.168.0.101  192.168.0.102  HTTP/XML  1261  HTTP/1.1 200 OK
```

```
> GET /ssdp/device-desc.xml HTTP/1.1\r\n
  Host: 192.168.0.101:8008\r\n
  Connection: keep-alive\r\n
  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95…
  Accept-Encoding: gzip, deflate\r\n
  \r\n
  [Full request URI: http://192.168.0.101:8008/ssdp/device-desc.xml]
```

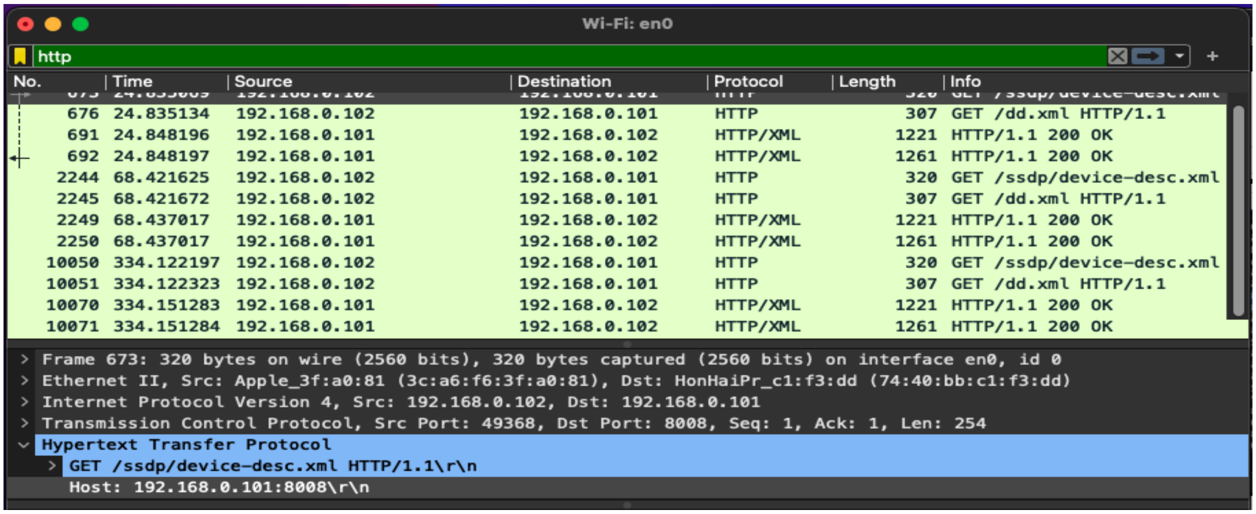
```
0000  74 40 bb c1 f3 dd 3c a6  f6 3f a0 81 08 00 45 00   t@····<· ·?····E·
0010  01 32 00 00 40 00 40 06  b7 aa c0 a8 00 66 c0 a8   ·2··@·@· ·····f··
0020  00 65 c0 d8 1f 48 b1 10  ef 96 2f 2c 7d df 80 18   ·e···H·· ··/,}···
0030  08 0a f1 74 00 00 01 01  08 0a 77 60 43 af 01 26   ···t···· ··w`C··&
0040  f8 b3 47 45 54 20 2f 73  73 64 70 2f 64 65 76 69   ··GET /s sdp/devi
0050  63 65 2d 64 65 73 63 2e  78 6d 6c 20 48 54 54 50   ce-desc. xml HTTP
0060  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 31 39 32 2e   /1.1··Ho st: 192.
0070  31 36 38 2e 30 2e 31 30  31 3a 38 30 30 38 0d 0a   168.0.10 1:8008··
0080  43 6f 6e 6e 65 63 74 69  6f 6e 3a 20 6b 65 65 70   Connecti on: keep
0090  2d 61 6c 69 76 65 0d 0a  55 73 65 72 2d 41 67 65   -alive·· User-Age
00a0  6e 74 3a 20 4d 6f 7a 69  6c 6c 61 2f 35 2e 30 20   nt: Mozi lla/5.0 
00b0  28 4d 61 63 69 6e 74 6f  73 68 3b 20 49 6e 74 65   (Macinto sh; Inte
00c0  6c 20 4d 61 63 20 4f 53  20 58 20 31 30 5f 31 35   l Mac OS  X 10_15
00d0  5f 37 29 20 41 70 70 6c  65 57 65 62 4b 69 74 2f   _7) Appl eWebKit/
00e0  35 33 37 2e 33 36 20 28  4b 48 54 4d 4c 2c 20 6c   537.36 ( KHTML, l
00f0  69 6b 65 20 47 65 63 6b  6f 29 20 43 68 72 6f 6d   ike Geck o) Chrom
0100  65 2f 39 35 2e 30 2e 34  36 33 38 2e 36 39 20 53   e/95.0.4 638.69 S
0110  61 66 61 72 69 2f 35 33  37 2e 33 36 0d 0a 41 63   afari/53 7.36··Ac
0120  63 65 70 74 2d 45 6e 63  6f 64 69 6e 67 3a 20 67   cept-Enc oding: g
0130  7a 69 70 2c 20 64 65 66  6c 61 74 65 0d 0a 0d 0a   zip, def late····
```

```
HTTP Host (http.host), 26 bytes        Packets: 3280 · Displayed: 8 (0.2%)        Profile: Default
```

From the above screen shot it is visible that the first four bytes of the Host parameter from the packets byte panel are : 48 6f 73 74

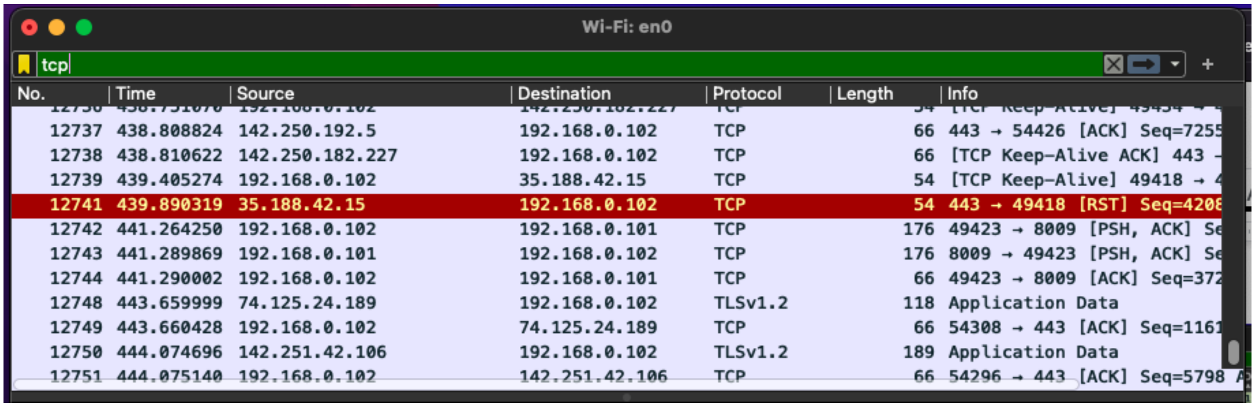
5. Filter packets with http, TCP, DNS and other protocols.
a. Find out what are those packets contain by following one of the conversations (also called network flows), select one of the packets and press the right mouse button..click on follow.

TCP:



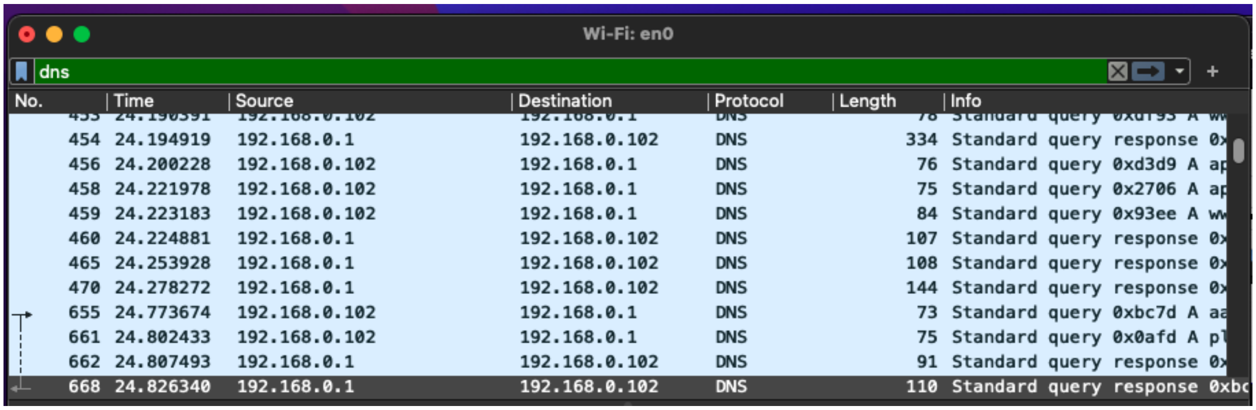
```
Wi-Fi: en0
http
No.     | Time       | Source        | Destination   | Protocol | Length | Info
  673  24.835009  192.168.0.102  192.168.0.101  HTTP       320  GET /ssdp/device-desc.xml
  676  24.835134  192.168.0.102  192.168.0.101  HTTP       307  GET /dd.xml HTTP/1.1
  691  24.848196  192.168.0.101  192.168.0.102  HTTP/XML  1221  HTTP/1.1 200 OK
  692  24.848197  192.168.0.101  192.168.0.102  HTTP/XML  1261  HTTP/1.1 200 OK
 2244  68.421625  192.168.0.102  192.168.0.101  HTTP       320  GET /ssdp/device-desc.xml
 2245  68.421672  192.168.0.102  192.168.0.101  HTTP       307  GET /dd.xml HTTP/1.1
 2249  68.437017  192.168.0.101  192.168.0.102  HTTP/XML  1221  HTTP/1.1 200 OK
 2250  68.437017  192.168.0.101  192.168.0.102  HTTP/XML  1261  HTTP/1.1 200 OK
10050 334.122197  192.168.0.102  192.168.0.101  HTTP       320  GET /ssdp/device-desc.xml
10051 334.122323  192.168.0.102  192.168.0.101  HTTP       307  GET /dd.xml HTTP/1.1
10070 334.151283  192.168.0.101  192.168.0.102  HTTP/XML  1221  HTTP/1.1 200 OK
10071 334.151284  192.168.0.101  192.168.0.102  HTTP/XML  1261  HTTP/1.1 200 OK

> Frame 673: 320 bytes on wire (2560 bits), 320 bytes captured (2560 bits) on interface en0, id 0
> Ethernet II, Src: Apple_3f:a0:81 (3c:a6:f6:3f:a0:81), Dst: HonHaiPr_c1:f3:dd (74:40:bb:c1:f3:dd)
> Internet Protocol Version 4, Src: 192.168.0.102, Dst: 192.168.0.101
> Transmission Control Protocol, Src Port: 49368, Dst Port: 8008, Seq: 1, Ack: 1, Len: 254
v Hypertext Transfer Protocol
  > GET /ssdp/device-desc.xml HTTP/1.1\r\n
    Host: 192.168.0.101:8008\r\n
```

TCP:



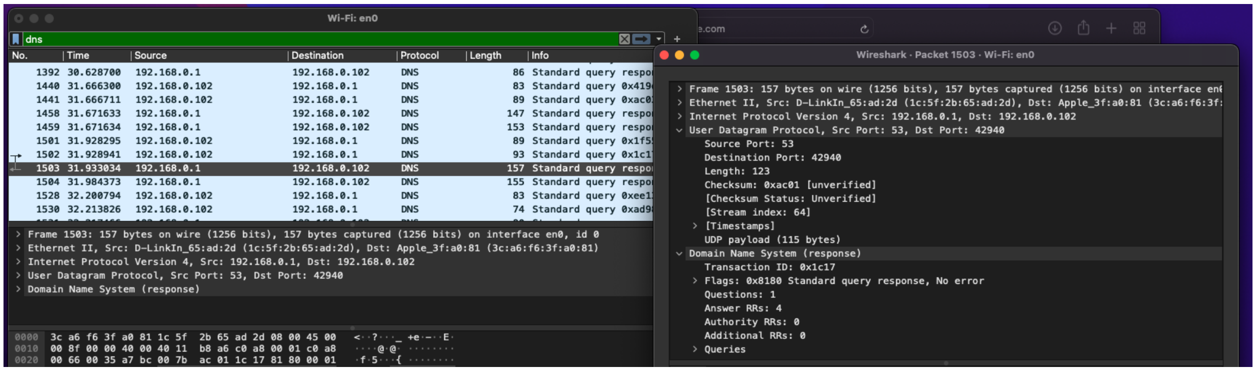
```
Wi-Fi: en0
tcp
No.     | Time       | Source          | Destination     | Protocol | Length | Info
12736 438.751070  192.168.0.102    142.250.182.227  TCP        54  [TCP Keep-Alive] 49434 → 4
12737 438.808824  142.250.192.5    192.168.0.102    TCP        66  443 → 54426 [ACK] Seq=7255
12738 438.810622  142.250.182.227  192.168.0.102    TCP        66  [TCP Keep-Alive ACK] 443 →
12739 439.405274  192.168.0.102    35.188.42.15     TCP        54  [TCP Keep-Alive] 49418 → 4
12741 439.890319  35.188.42.15     192.168.0.102    TCP        54  443 → 49418 [RST] Seq=4208
12742 441.264250  192.168.0.102    192.168.0.101    TCP       176  49423 → 8009 [PSH, ACK] Se
12743 441.289869  192.168.0.101    192.168.0.102    TCP       176  8009 → 49423 [PSH, ACK] Se
12744 441.290002  192.168.0.102    192.168.0.101    TCP        66  49423 → 8009 [ACK] Seq=372
12748 443.659999  74.125.24.189    192.168.0.102    TLSv1.2   118  Application Data
12749 443.660428  192.168.0.102    74.125.24.189    TCP        66  54308 → 443 [ACK] Seq=1161
12750 444.074696  142.251.42.106   192.168.0.102    TLSv1.2   189  Application Data
12751 444.075140  192.168.0.102    142.251.42.106   TCP        66  54296 → 443 [ACK] Seq=5798 A
```

DNS:



```
Wi-Fi: en0
dns
No.  | Time      | Source        | Destination   | Protocol | Length | Info
453  24.190391  192.168.0.102  192.168.0.1    DNS       78  Standard query 0xd193 A ww
454  24.194919  192.168.0.1    192.168.0.102  DNS      334  Standard query response 0x
456  24.200228  192.168.0.102  192.168.0.1    DNS       76  Standard query 0xd3d9 A ap
458  24.221978  192.168.0.102  192.168.0.1    DNS       75  Standard query 0x2706 A ap
459  24.223183  192.168.0.102  192.168.0.1    DNS       84  Standard query 0x93ee A ww
460  24.224881  192.168.0.1    192.168.0.102  DNS      107  Standard query response 0x
465  24.253928  192.168.0.1    192.168.0.102  DNS      108  Standard query response 0x
470  24.278272  192.168.0.1    192.168.0.102  DNS      144  Standard query response 0x
655  24.773674  192.168.0.102  192.168.0.1    DNS       73  Standard query 0xbc7d A aa
661  24.802433  192.168.0.102  192.168.0.1    DNS       75  Standard query 0x0afd A pl
662  24.807493  192.168.0.1    192.168.0.102  DNS       91  Standard query response 0x
668  24.826340  192.168.0.1    192.168.0.102  DNS      110  Standard query response 0xbc
```

On selecting the packet of dns protocol, and on selecting follow UDP Stream for this packet, the following results are obtained.



Wi-Fi: en0

dns

```
No.   Time       Source          Destination     Protocol  Length  Info
 1392 30.628700  192.168.0.1     192.168.0.102   DNS           86  Standard query respo
 1440 31.666300  192.168.0.102   192.168.0.1     DNS           83  Standard query 0x419
 1441 31.666711  192.168.0.102   192.168.0.1     DNS           89  Standard query 0xac0
 1458 31.671633  192.168.0.1     192.168.0.102   DNS          147  Standard query respo
 1459 31.671634  192.168.0.1     192.168.0.102   DNS          153  Standard query respo
 1501 31.928295  192.168.0.102   192.168.0.1     DNS           89  Standard query 0x1f5
 1502 31.928941  192.168.0.102   192.168.0.1     DNS           93  Standard query 0x1c1
 1503 31.933034  192.168.0.1     192.168.0.102   DNS          157  Standard query respo
 1504 31.984373  192.168.0.1     192.168.0.102   DNS          155  Standard query respo
 1528 32.200794  192.168.0.102   192.168.0.1     DNS           83  Standard query 0xee1
 1530 32.213826  192.168.0.102   192.168.0.1     DNS           74  Standard query 0xad9
```

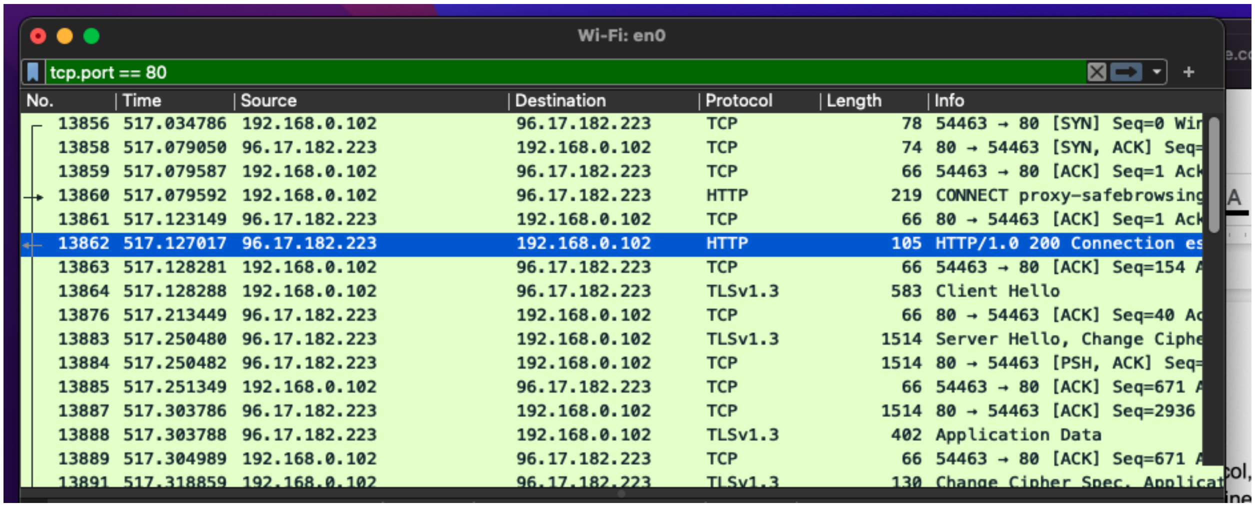
```
> Frame 1503: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits) on interface en0, id 0
> Ethernet II, Src: D-LinkIn_65:ad:2d (1c:5f:2b:65:ad:2d), Dst: Apple_3f:a0:81 (3c:a6:f6:3f:a0:81)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.102
> User Datagram Protocol, Src Port: 53, Dst Port: 42940
> Domain Name System (response)
```

```
0000  3c a6 f6 3f a0 81 1c 5f  2b 65 ad 2d 08 00 45 00   <··?···_ +e·–··E·
0010  00 8f 00 00 40 00 40 11  b8 a6 c0 a8 00 01 c0 a8   ····@·@· ········
0020  00 66 00 35 a7 bc 00 7b  ac 01 1c 17 81 80 00 01   ·f·5···{ ········
```

Wireshark · Packet 1503 · Wi-Fi: en0

```
> Frame 1503: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits) on interface en0
> Ethernet II, Src: D-LinkIn_65:ad:2d (1c:5f:2b:65:ad:2d), Dst: Apple_3f:a0:81 (3c:a6:f6:3f:
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.102
v User Datagram Protocol, Src Port: 53, Dst Port: 42940
    Source Port: 53
    Destination Port: 42940
    Length: 123
    Checksum: 0xac01 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 64]
  > [Timestamps]
    UDP payload (115 bytes)
v Domain Name System (response)
    Transaction ID: 0x1c17
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 0
    Additional RRs: 0
  > Queries
```

6. Search through your capture, and find an HTTP packet coming back from the server (TCP Source Port == 80). Expand the Ethernet layer in the Packet Details Panel.

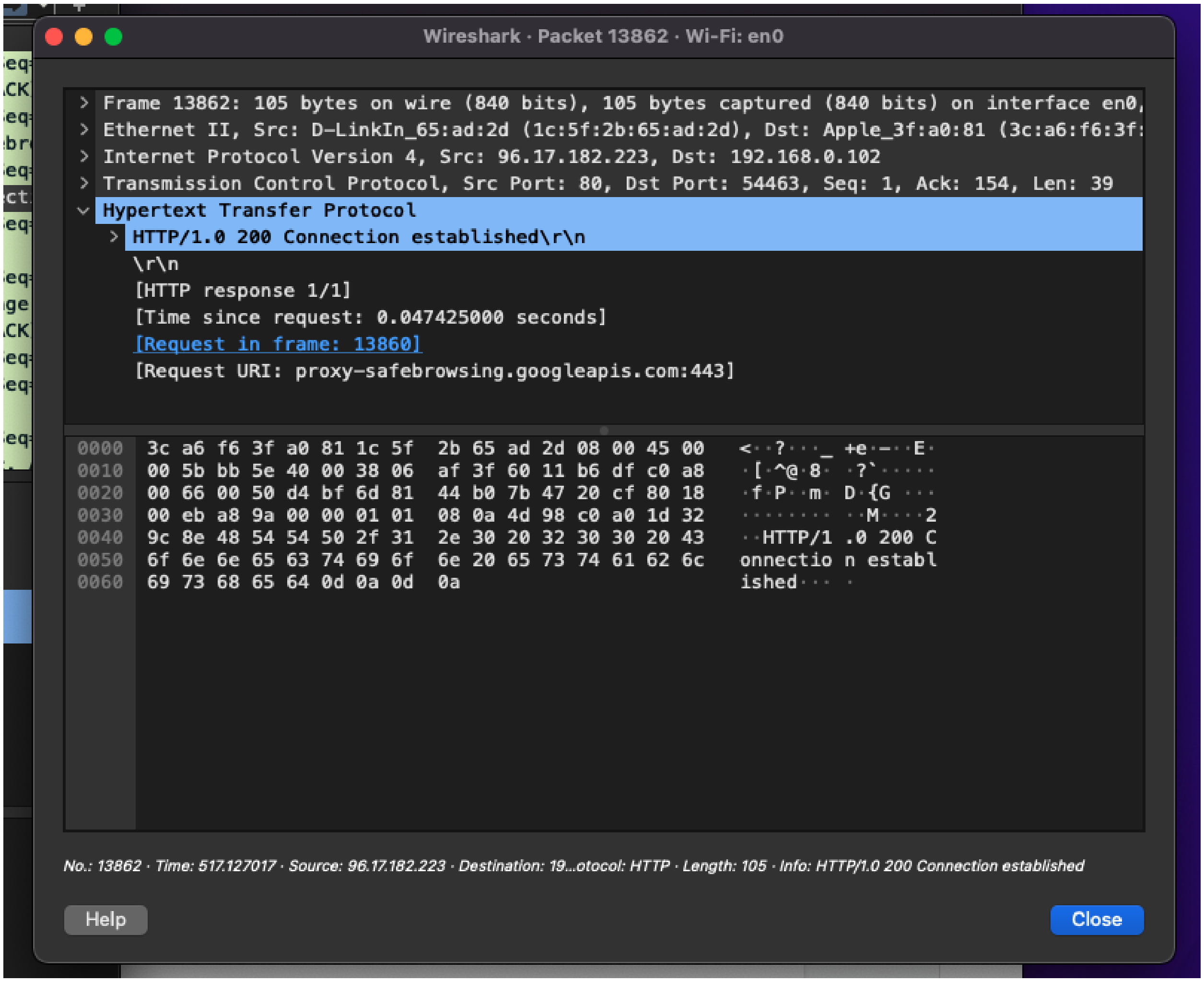


Wi-Fi: en0

tcp.port == 80

```
No.    Time        Source          Destination     Protocol  Length  Info
13856  517.034786  192.168.0.102   96.17.182.223   TCP           78  54463 → 80 [SYN] Seq=0 Wir
13858  517.079050  96.17.182.223   192.168.0.102   TCP           74  80 → 54463 [SYN, ACK] Seq=
13859  517.079587  192.168.0.102   96.17.182.223   TCP           66  54463 → 80 [ACK] Seq=1 Ack
13860  517.079592  192.168.0.102   96.17.182.223   HTTP         219  CONNECT proxy-safebrowsing
13861  517.123149  96.17.182.223   192.168.0.102   TCP           66  80 → 54463 [ACK] Seq=1 Ack
13862  517.127017  96.17.182.223   192.168.0.102   HTTP         105  HTTP/1.0 200 Connection es
13863  517.128281  192.168.0.102   96.17.182.223   TCP           66  54463 → 80 [ACK] Seq=154 A
13864  517.128288  192.168.0.102   96.17.182.223   TLSv1.3      583  Client Hello
13876  517.213449  96.17.182.223   192.168.0.102   TCP           66  80 → 54463 [ACK] Seq=40 Ac
13883  517.250480  96.17.182.223   192.168.0.102   TLSv1.3     1514  Server Hello, Change Ciphe
13884  517.250482  96.17.182.223   192.168.0.102   TCP         1514  80 → 54463 [PSH, ACK] Seq=
13885  517.251349  192.168.0.102   96.17.182.223   TCP           66  54463 → 80 [ACK] Seq=671 A
13887  517.303786  96.17.182.223   192.168.0.102   TCP         1514  80 → 54463 [ACK] Seq=2936
13888  517.303788  96.17.182.223   192.168.0.102   TLSv1.3      402  Application Data
13889  517.304989  192.168.0.102   96.17.182.223   TCP           66  54463 → 80 [ACK] Seq=671 A
13891  517.318859  192.168.0.102   96.17.182.223   TLSv1.3      130  Change Cipher Spec, Applicat
```

On expanding packet number 13862 in the Packet Details Panel, the following results are obtained.



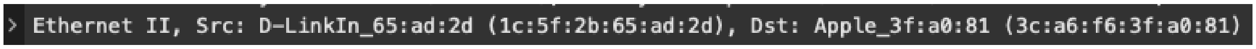
Wireshark · Packet 13862 · Wi-Fi: en0

```
> Frame 13862: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface en0,
> Ethernet II, Src: D-LinkIn_65:ad:2d (1c:5f:2b:65:ad:2d), Dst: Apple_3f:a0:81 (3c:a6:f6:3f:
> Internet Protocol Version 4, Src: 96.17.182.223, Dst: 192.168.0.102
> Transmission Control Protocol, Src Port: 80, Dst Port: 54463, Seq: 1, Ack: 154, Len: 39
v Hypertext Transfer Protocol
  > HTTP/1.0 200 Connection established\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.047425000 seconds]
    [Request in frame: 13860]
    [Request URI: proxy-safebrowsing.googleapis.com:443]
```

```
0000  3c a6 f6 3f a0 81 1c 5f  2b 65 ad 2d 08 00 45 00   <··?···_ +e·-··E·
0010  00 5b bb 5e 40 00 38 06  af 3f 60 11 b6 df c0 a8   ·[·^@·8· ·?`·····
0020  00 66 00 50 d4 bf 6d 81  44 b0 7b 47 20 cf 80 18   ·f·P··m· D·{G ···
0030  00 eb a8 9a 00 00 01 01  08 0a 4d 98 c0 a0 1d 32   ········ ··M····2
0040  9c 8e 48 54 54 50 2f 31  2e 30 20 32 30 30 20 43   ··HTTP/1 .0 200 C
0050  6f 6e 6e 65 63 74 69 6f  6e 20 65 73 74 61 62 6c   onnectio n establ
0060  69 73 68 65 64 0d 0a 0d  0a                        ished··· ·
```

No.: 13862 · Time: 517.127017 · Source: 96.17.182.223 · Destination: 19...otocol: HTTP · Length: 105 · Info: HTTP/1.0 200 Connection established

7. What are the manufacturers of your PC's Network Interface Card (NIC), and the servers NIC?



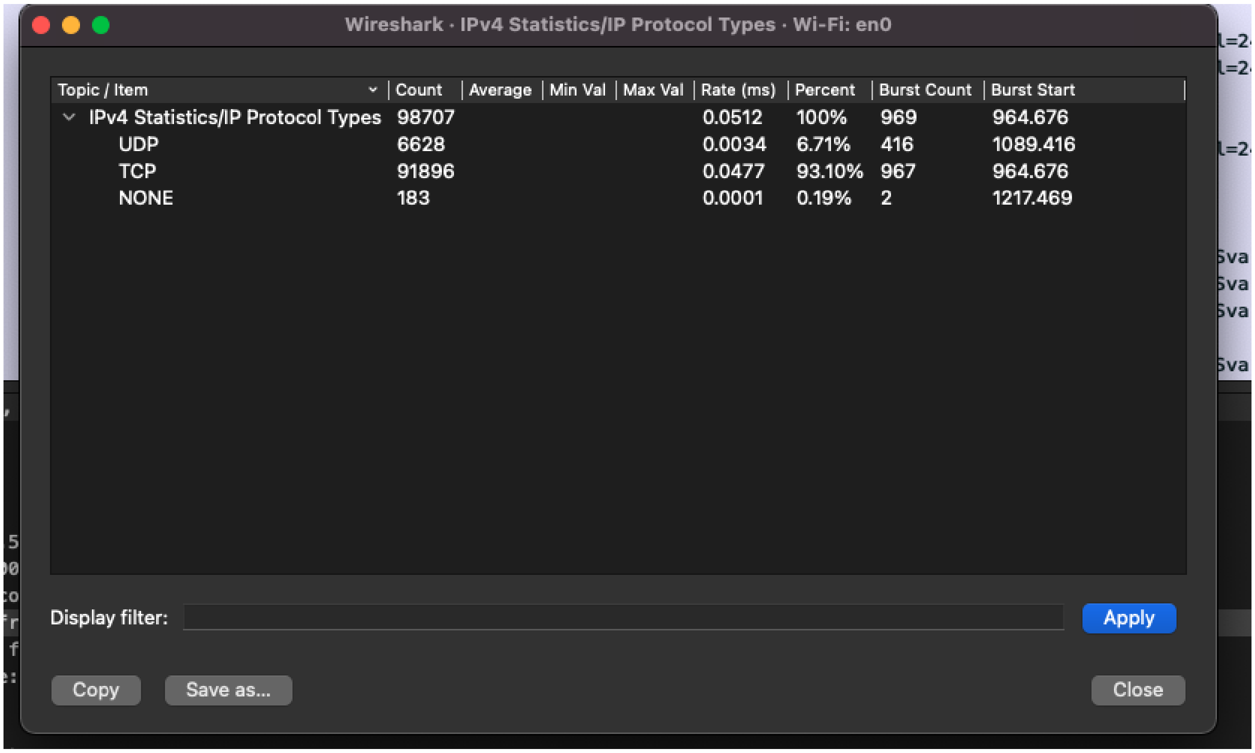
```
> Ethernet II, Src: D-LinkIn_65:ad:2d (1c:5f:2b:65:ad:2d), Dst: Apple_3f:a0:81 (3c:a6:f6:3f:a0:81)
```

Manufacturer's NIC :- D-LinIn_65:ad:2d (1c:5f:2b:65:ad:2d)
server's NIC :- Apple_3f:a0:81 (3c:a6:f6:3f:a0:81)

8. What are the Hex values (shown in the raw bytes panel) of the two NICS Manufacturers OUIs?

For Laptop's Manufacturer :- 1c:5f:2b:65:ad:2d
For server's Manufacturer :- 3c:a6:f6:3f:a0:81

9. Find the following statistics:
a. What percentage of packets in your capture are TCP, and give an example of the higher level protocol which uses TCP?

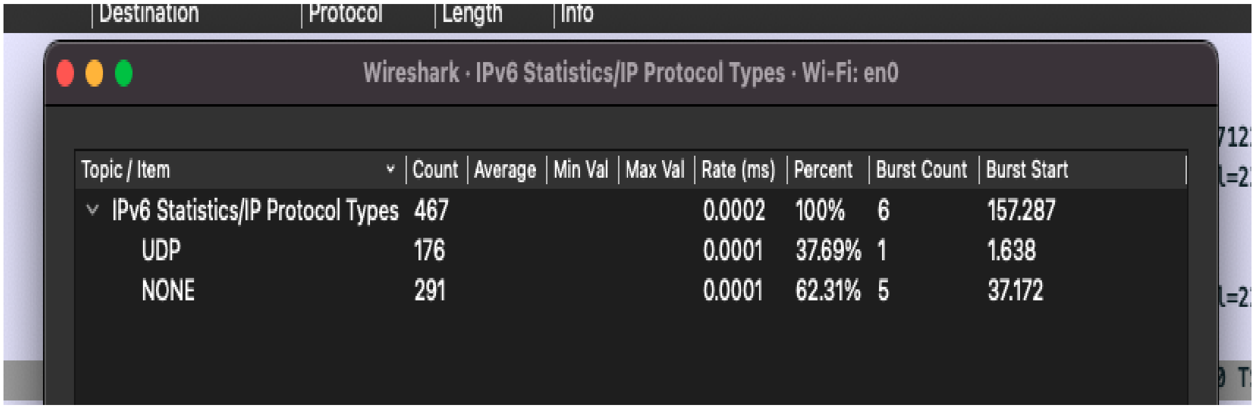


Wireshark · IPv4 Statistics/IP Protocol Types · Wi-Fi: en0

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Count	Burst Start
IPv4 Statistics/IP Protocol Types	98707				0.0512	100%	969	964.676
UDP	6628				0.0034	6.71%	416	1089.416
TCP	91896				0.0477	93.10%	967	964.676
NONE	183				0.0001	0.19%	2	1217.469

Display filter:

b. What percentage of packets in your capture are UDP, and give an example of the higher level protocol which uses UDP?

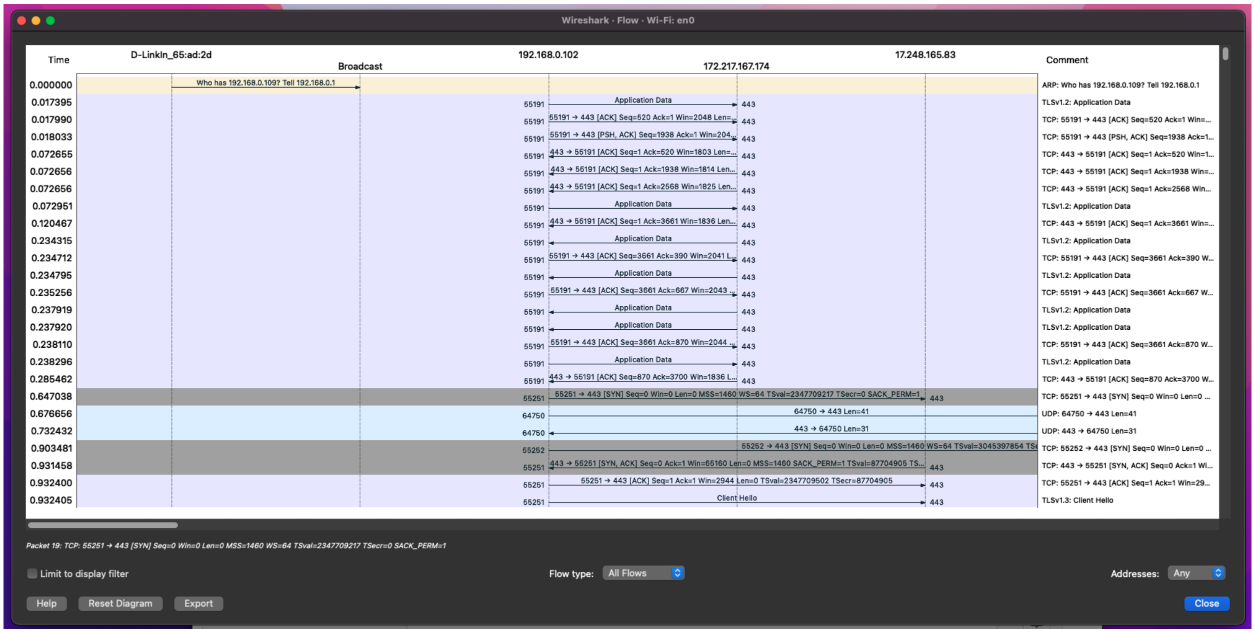


Wireshark · IPv6 Statistics/IP Protocol Types · Wi-Fi: en0

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Count	Burst Start
IPv6 Statistics/IP Protocol Types	467				0.0002	100%	6	157.287
UDP	176				0.0001	37.69%	1	1.638
NONE	291				0.0001	62.31%	5	37.172

10. Find the traffic flow Select the Statistics->Flow Graph menu option. Choose General Flow and Network Source options, and click the OK button.

Graph Obtained from General Flow and network source option of flow graphs:



```
Time      D-LinkIn_65:ad:2d   Broadcast   192.168.0.102   172.217.167.174   17.248.165.83   Comment

0.000000  Who has 192.168.0.109? Tell 192.168.0.1                                         ARP: Who has 192.168.0.109? Tell 192.168.0.1
0.017395  55191  Application Data  443                                                    TLSv1.2: Application Data
0.017990  55191  55191 → 443 [ACK] Seq=520 Ack=1 Win=2048 Len=...  443                    TCP: 55191 → 443 [ACK] Seq=520 Ack=1 Win=...
0.018033  55191  55191 → 443 [PSH, ACK] Seq=1938 Ack=1 Win=204...  443                    TCP: 55191 → 443 [PSH, ACK] Seq=1938 Ack=1...
0.072655  55191  443 → 55191 [ACK] Seq=1 Ack=520 Win=1803 Len=...  443                    TCP: 443 → 55191 [ACK] Seq=1 Ack=520 Win=1...
0.072656  55191  443 → 55191 [ACK] Seq=1 Ack=1938 Win=1814 Len...  443                    TCP: 443 → 55191 [ACK] Seq=1 Ack=1938 Win=...
0.072656  55191  443 → 55191 [ACK] Seq=1 Ack=2568 Win=1825 Len...  443                    TCP: 443 → 55191 [ACK] Seq=1 Ack=2568 Win...
0.072951  55191  Application Data  443                                                    TLSv1.2: Application Data
0.120467  55191  443 → 55191 [ACK] Seq=1 Ack=3661 Win=1836 Len...  443                    TCP: 443 → 55191 [ACK] Seq=1 Ack=3661 Win=...
0.234315  55191  Application Data  443                                                    TLSv1.2: Application Data
0.234712  55191  55191 → 443 [ACK] Seq=3661 Ack=390 Win=2041 L...  443                    TCP: 55191 → 443 [ACK] Seq=3661 Ack=390 W...
0.234795  55191  Application Data  443                                                    TLSv1.2: Application Data
0.235256  55191  55191 → 443 [ACK] Seq=3661 Ack=667 Win=2043 ...  443                     TCP: 55191 → 443 [ACK] Seq=3661 Ack=667 W...
0.237919  55191  Application Data  443                                                    TLSv1.2: Application Data
0.237920  55191  Application Data  443                                                    TLSv1.2: Application Data
0.238110  55191  55191 → 443 [ACK] Seq=3661 Ack=870 Win=2044 ...  443                     TCP: 55191 → 443 [ACK] Seq=3661 Ack=870 W...
0.238296  55191  Application Data  443                                                    TLSv1.2: Application Data
0.285462  55191  443 → 55191 [ACK] Seq=870 Ack=3700 Win=1836 L...  443                    TCP: 443 → 55191 [ACK] Seq=870 Ack=3700 W...
0.647038  55251  55251 → 443 [SYN] Seq=0 Win=0 Len=0 MSS=1460 WS=64 TSval=2347709217 TSecr=0 SACK_PERM=1  443   TCP: 55251 → 443 [SYN] Seq=0 Win=0 Len=0 ...
0.676656  64750  64750 → 443 Len=41                                                       UDP: 64750 → 443 Len=41
0.732432  64750  443 → 64750 Len=31                                                       UDP: 443 → 64750 Len=31
0.903481  55252  55252 → 443 [SYN] Seq=0 Win=0 Len=0 MSS=1460 WS=64 TSval=3045397854 TS   TCP: 55252 → 443 [SYN] Seq=0 Win=0 Len=0 ...
0.931458  55251  443 → 55251 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=87704905 TS...  443   TCP: 443 → 55251 [SYN, ACK] Seq=0 Ack=1 Wi...
0.932400  55251  55251 → 443 [ACK] Seq=1 Ack=1 Win=2944 Len=0 TSval=2347709502 TSecr=87704905  443   TCP: 55251 → 443 [ACK] Seq=1 Ack=1 Win=29...
0.932405  55251  Client Hello  443                                                        TLSv1.3: Client Hello
```

Packet 19: TCP: 55251 → 443 [SYN] Seq=0 Win=0 Len=0 MSS=1460 WS=64 TSval=2347709217 TSecr=0 SACK_PERM=1

□ Limit to display filter

Flow type: All Flows

Addresses: Any

Comments:

The entire assignment focuses on discovering the utility of the tool wireshark. It helped in tracing and analysing packets and packet transfer respectively. Also helped to understand how packet transfer takes place following protocols like TCP, UDP, ARP etc. Looking forward to learning more tools like this.