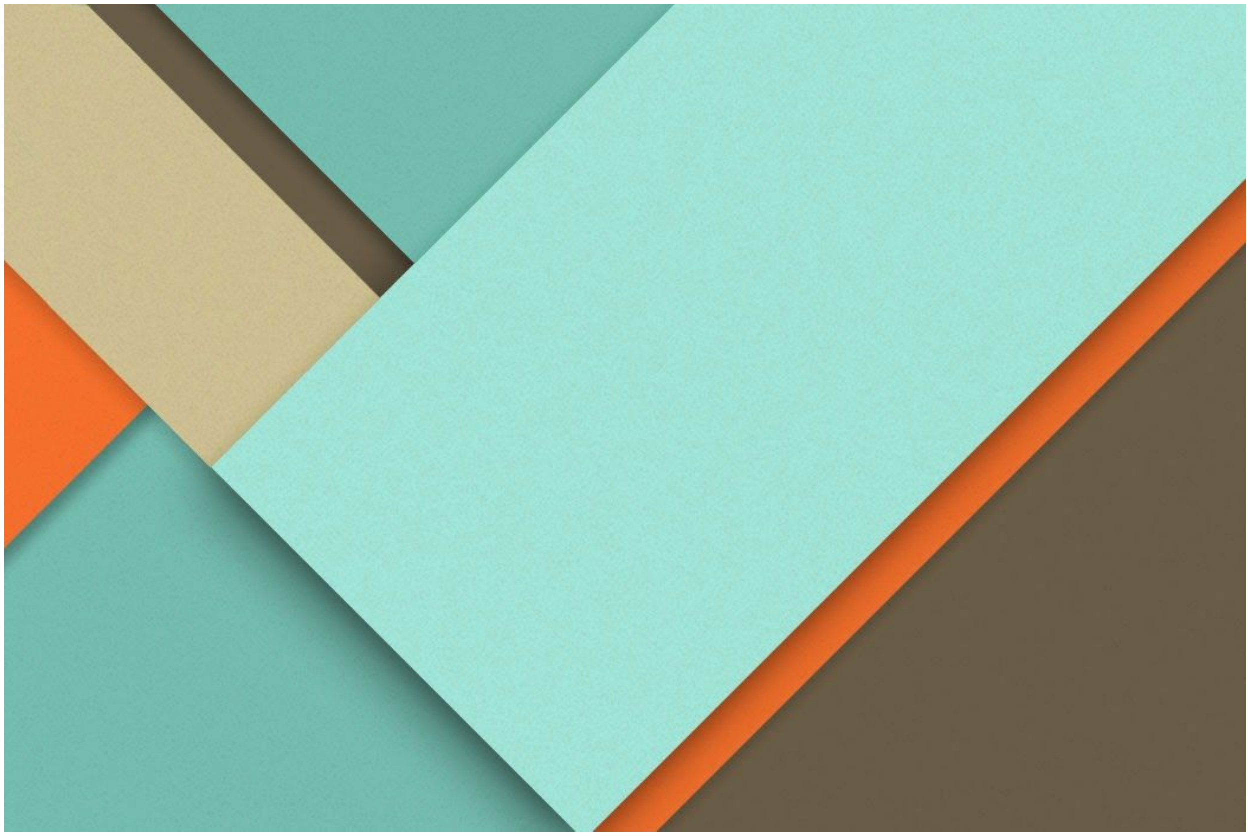


# Computer Networks Lab

ASSIGNMENT 5

SAMARPAN CHAKRAVARTY
BCSE - III
001810501026

26/12/2020

## 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.

## Goals:

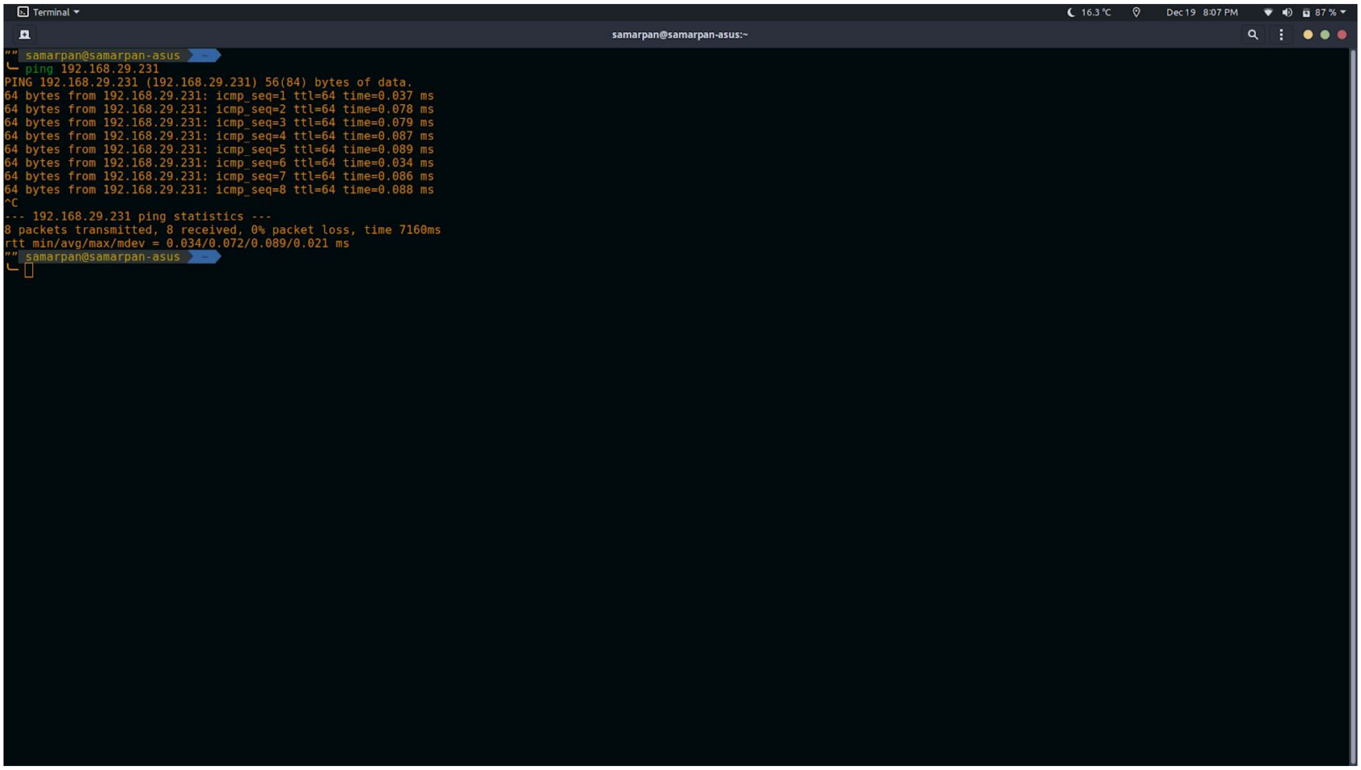
Install wireshark in the local machine and capture and analyse various packets according to the given questions.

## Specifications:

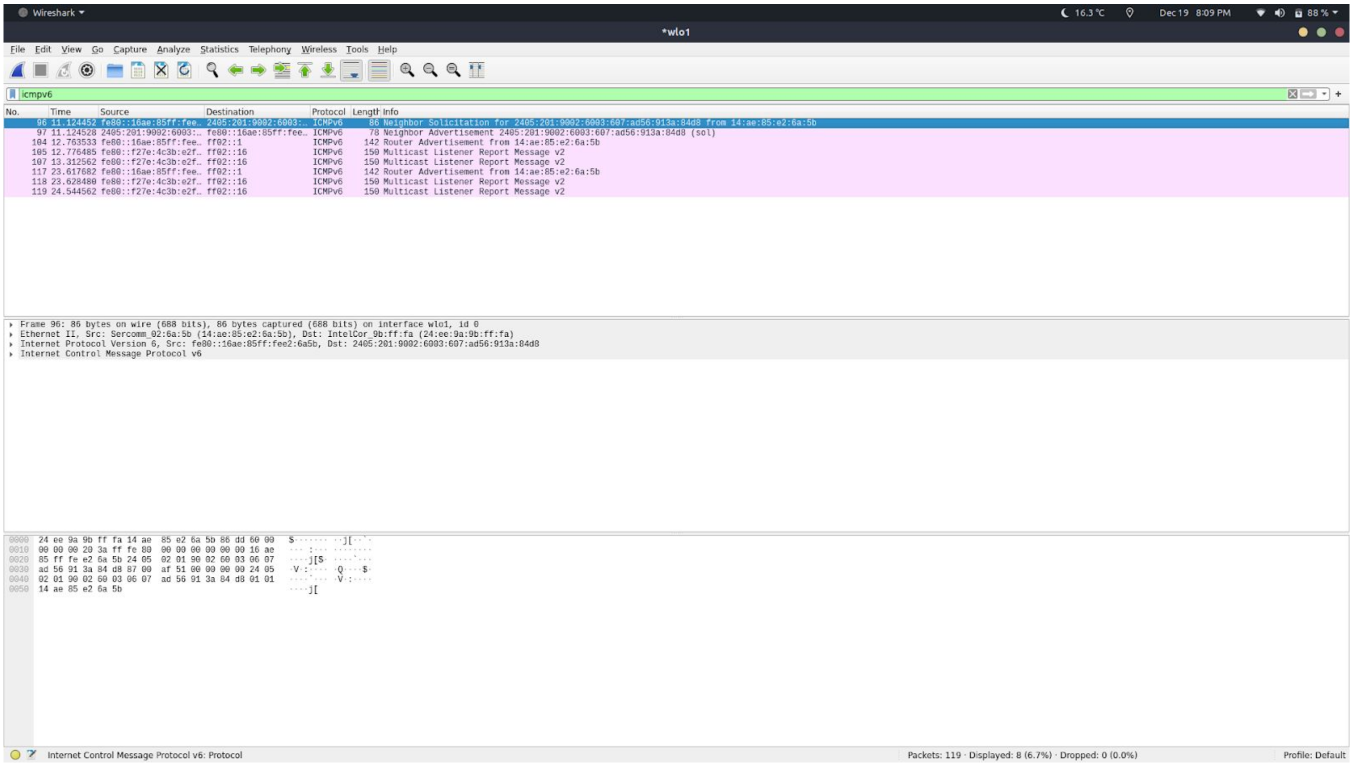
1. System- Linux
2. OS- Ubuntu 20.10
3. Wireshark-3.2.7
4. Network- Wireless network(WIFI)

# 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 neighbouring system. After the ARP request, the pings (ICMP echo request and replies) can be seen.**



```
"" samarpan@samarpan-asus ~
╰ ping 192.168.29.231
PING 192.168.29.231 (192.168.29.231) 56(84) bytes of data.
64 bytes from 192.168.29.231: icmp_seq=1 ttl=64 time=0.037 ms
64 bytes from 192.168.29.231: icmp_seq=2 ttl=64 time=0.078 ms
64 bytes from 192.168.29.231: icmp_seq=3 ttl=64 time=0.079 ms
64 bytes from 192.168.29.231: icmp_seq=4 ttl=64 time=0.087 ms
64 bytes from 192.168.29.231: icmp_seq=5 ttl=64 time=0.089 ms
64 bytes from 192.168.29.231: icmp_seq=6 ttl=64 time=0.034 ms
64 bytes from 192.168.29.231: icmp_seq=7 ttl=64 time=0.086 ms
64 bytes from 192.168.29.231: icmp_seq=8 ttl=64 time=0.088 ms
^C
--- 192.168.29.231 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7160ms
rtt min/avg/max/mdev = 0.034/0.072/0.089/0.021 ms
"" samarpan@samarpan-asus ~
╰
```



icmpv6

```
No.      Time       Source               Destination          Protocol Length Info
     96 11.124452 fe80::16ae:85ff:fee… 2405:201:9002:6003:… ICMPv6     86 Neighbor Solicitation for 2405:201:9002:6003:607:ad56:913a:84d8 from 14:ae:85:e2:6a:5b
     97 11.124528 2405:201:9002:6003:… fe80::16ae:85ff:fee… ICMPv6     78 Neighbor Advertisement 2405:201:9002:6003:607:ad56:913a:84d8 (sol)
    104 12.763533 fe80::16ae:85ff:fee… ff02::1              ICMPv6    142 Router Advertisement from 14:ae:85:e2:6a:5b
    105 12.776485 fe80::f27e:4c3b:e2f… ff02::16             ICMPv6    150 Multicast Listener Report Message v2
    107 13.312562 fe80::f27e:4c3b:e2f… ff02::16             ICMPv6    150 Multicast Listener Report Message v2
    117 23.617682 fe80::16ae:85ff:fee… ff02::1              ICMPv6    142 Router Advertisement from 14:ae:85:e2:6a:5b
    118 23.628480 fe80::f27e:4c3b:e2f… ff02::16             ICMPv6    150 Multicast Listener Report Message v2
    119 24.544562 fe80::f27e:4c3b:e2f… ff02::16             ICMPv6    150 Multicast Listener Report Message v2
```

```
▸ Frame 96: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface wlo1, id 0
▸ Ethernet II, Src: Sercomm_02:6a:5b (14:ae:85:e2:6a:5b), Dst: IntelCor_9b:ff:fa (24:ee:9a:9b:ff:fa)
▸ Internet Protocol Version 6, Src: fe80::16ae:85ff:fee2:6a5b, Dst: 2405:201:9002:6003:607:ad56:913a:84d8
▸ Internet Control Message Protocol v6
```

```
0000  24 ee 9a 9b ff fa 14 ae  85 e2 6a 5b 86 dd 60 00   $······· ··j[··`·
0010  00 00 00 20 3a ff fe 80  00 00 00 00 00 00 16 ae   ··· :··· ········
0020  85 ff fe e2 6a 5b 24 05  02 01 90 02 60 03 06 07   ····j[$· ····`···
0030  ad 56 91 3a 84 d8 87 00  af 51 00 00 00 00 24 05   ·V·:···· ·Q····$·
0040  02 01 90 02 60 03 06 07  ad 56 91 3a 84 d8 01 01   ····`··· ·V·:····
0050  14 ae 85 e2 6a 5b                                  ····j[
```

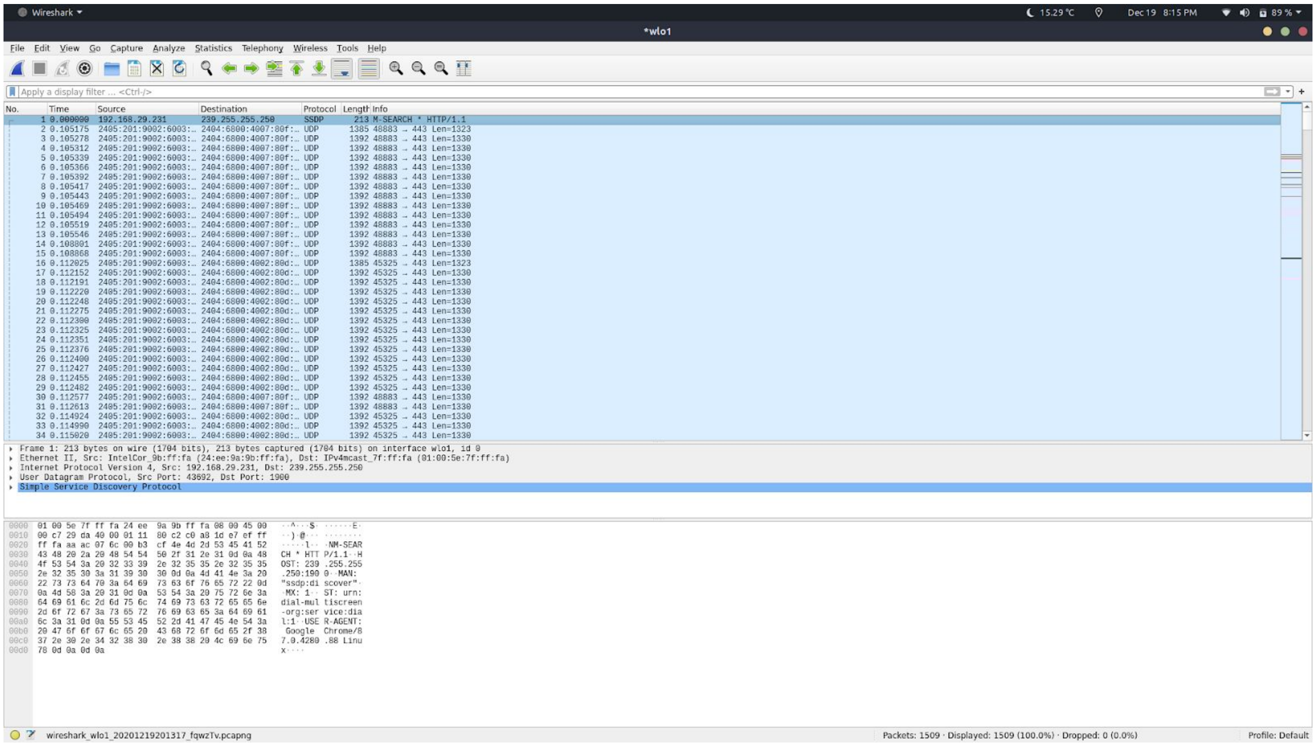
Internet Control Message Protocol v6: Protocol

Packets: 119 · Displayed: 8 (6.7%) · Dropped: 0 (0.0%)

Profile: Default

## Q2. Generate some web traffic and

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


Wireshark
15.29 °C
Dec 19 8:15 PM
89 %
*wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.    Time      Source               Destination          Protocol Length Info
     1 0.000000  192.168.29.231       239.255.255.250      SSDP      213 M-SEARCH * HTTP/1.1
     2 0.105175  2405:201:9002:6003:… 2404:6800:4007:80f:… UDP      1385 48883 → 443 Len=1323
     3 0.105278  2405:201:9002:6003:… 2404:6800:4007:80f:… UDP      1392 48883 → 443 Len=1330
     4 0.105312  2405:201:9002:6003:… 2404:6800:4007:80f:… UDP      1392 48883 → 443 Len=1330
     5 0.105339  2405:201:9002:6003:… 2404:6800:4007:80f:… UDP      1392 48883 → 443 Len=1330
     6 0.105366  2405:201:9002:6003:… 2404:6800:4007:80f:… UDP      1392 48883 → 443 Len=1330
     7 0.105392  2405:201:9002:6003:… 2404:6800:4007:80f:… UDP      1392 48883 → 443 Len=1330
     8 0.105417  2405:201:9002:6003:… 2404:6800:4007:80f:… UDP      1392 48883 → 443 Len=1330
     9 0.105443  2405:201:9002:6003:… 2404:6800:4007:80f:… UDP      1392 48883 → 443 Len=1330
    10 0.105469  2405:201:9002:6003:… 2404:6800:4007:80f:… UDP      1392 48883 → 443 Len=1330
    11 0.105494  2405:201:9002:6003:… 2404:6800:4007:80f:… UDP      1392 48883 → 443 Len=1330
    12 0.105519  2405:201:9002:6003:… 2404:6800:4007:80f:… UDP      1392 48883 → 443 Len=1330
    13 0.105546  2405:201:9002:6003:… 2404:6800:4007:80f:… UDP      1392 48883 → 443 Len=1330
    14 0.108801  2405:201:9002:6003:… 2404:6800:4007:80f:… UDP      1392 48883 → 443 Len=1330
    15 0.108868  2405:201:9002:6003:… 2404:6800:4007:80f:… UDP      1392 48883 → 443 Len=1330
    16 0.112025  2405:201:9002:6003:… 2404:6800:4002:80d:… UDP      1385 45325 → 443 Len=1323
    17 0.112152  2405:201:9002:6003:… 2404:6800:4002:80d:… UDP      1392 45325 → 443 Len=1330
    18 0.112191  2405:201:9002:6003:… 2404:6800:4002:80d:… UDP      1392 45325 → 443 Len=1330
    19 0.112220  2405:201:9002:6003:… 2404:6800:4002:80d:… UDP      1392 45325 → 443 Len=1330
    20 0.112248  2405:201:9002:6003:… 2404:6800:4002:80d:… UDP      1392 45325 → 443 Len=1330
    21 0.112275  2405:201:9002:6003:… 2404:6800:4002:80d:… UDP      1392 45325 → 443 Len=1330
    22 0.112300  2405:201:9002:6003:… 2404:6800:4002:80d:… UDP      1392 45325 → 443 Len=1330
    23 0.112325  2405:201:9002:6003:… 2404:6800:4002:80d:… UDP      1392 45325 → 443 Len=1330
    24 0.112351  2405:201:9002:6003:… 2404:6800:4002:80d:… UDP      1392 45325 → 443 Len=1330
    25 0.112376  2405:201:9002:6003:… 2404:6800:4002:80d:… UDP      1392 45325 → 443 Len=1330
    26 0.112400  2405:201:9002:6003:… 2404:6800:4002:80d:… UDP      1392 45325 → 443 Len=1330
    27 0.112427  2405:201:9002:6003:… 2404:6800:4002:80d:… UDP      1392 45325 → 443 Len=1330
    28 0.112455  2405:201:9002:6003:… 2404:6800:4002:80d:… UDP      1392 45325 → 443 Len=1330
    29 0.112482  2405:201:9002:6003:… 2404:6800:4002:80d:… UDP      1392 45325 → 443 Len=1330
    30 0.112577  2405:201:9002:6003:… 2404:6800:4007:80f:… UDP      1392 48883 → 443 Len=1330
    31 0.112613  2405:201:9002:6003:… 2404:6800:4007:80f:… UDP      1392 48883 → 443 Len=1330
    32 0.114924  2405:201:9002:6003:… 2404:6800:4002:80d:… UDP      1392 45325 → 443 Len=1330
    33 0.114990  2405:201:9002:6003:… 2404:6800:4002:80d:… UDP      1392 45325 → 443 Len=1330
    34 0.115020  2405:201:9002:6003:… 2404:6800:4002:80d:… UDP      1392 45325 → 443 Len=1330
```

```
▸ Frame 1: 213 bytes on wire (1704 bits), 213 bytes captured (1704 bits) on interface wlo1, id 0
▸ Ethernet II, Src: IntelCor_9b:ff:fa (24:ee:9a:9b:ff:fa), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
▸ Internet Protocol Version 4, Src: 192.168.29.231, Dst: 239.255.255.250
▸ User Datagram Protocol, Src Port: 43692, Dst Port: 1900
▸ Simple Service Discovery Protocol
```

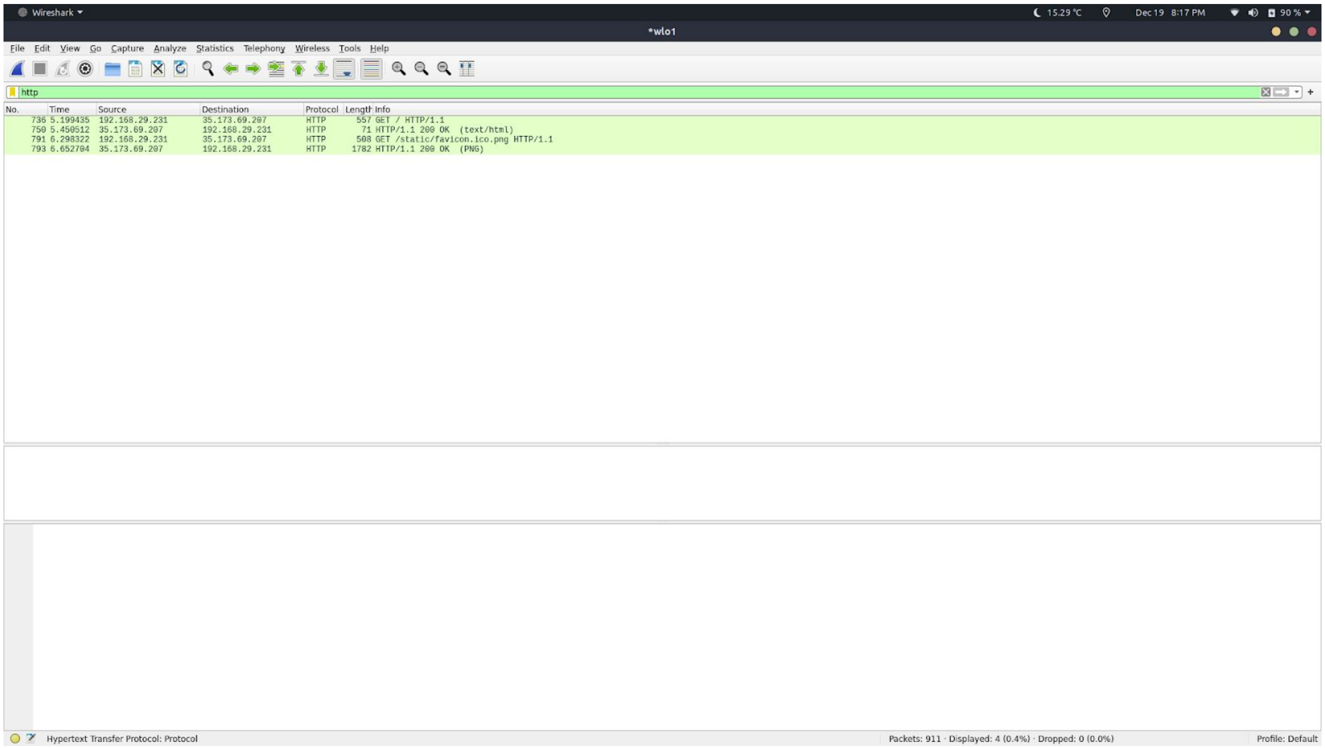
```
0000  01 00 5e 7f ff fa 24 ee  9a 9b ff fa 08 00 45 00   ··^···$· ······E·
0010  00 c7 29 da 40 00 01 11  80 c2 c0 a8 1d e7 ef ff   ··)·@··· ········
0020  ff fa aa ac 07 6c 00 b3  cf 4e 4d 2d 53 45 41 52   ·····l·· ·NM-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/1.1··H
0040  4f 53 54 3a 20 32 33 39  2e 32 35 35 2e 32 35 35   OST: 239 .255.255
0050  2e 32 35 30 3a 31 39 30  30 0d 0a 4d 41 4e 3a 20   .250:190 0··MAN:
0060  22 73 73 64 70 3a 64 69  73 63 6f 76 65 72 22 0d   "ssdp:di scover"·
0070  0a 4d 58 3a 20 31 0d 0a  53 54 3a 20 75 72 6e 3a   ·MX: 1·· ST: urn:
0080  64 69 61 6c 2d 6d 75 6c  74 69 73 63 72 65 65 6e   dial-mul tiscreen
0090  2d 6f 72 67 3a 73 65 72  76 69 63 65 3a 64 69 61   -org:ser vice:dia
00a0  6c 3a 31 0d 0a 55 53 45  52 2d 41 47 45 4e 54 3a   l:1··USE R-AGENT:
00b0  20 47 6f 6f 67 6c 65 20  43 68 72 6f 6d 65 2f 38    Google  Chrome/8
00c0  37 2e 30 2e 34 32 38 30  2e 38 38 20 4c 69 6e 75   7.0.4280 .88 Linu
00d0  78 0d 0a 0d 0a                                     x····
```

wireshark_wlo1_20201219201317_fqwzTv.pcapng

Packets: 1509 · Displayed: 1509 (100.0%) · Dropped: 0 (0.0%)

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.**

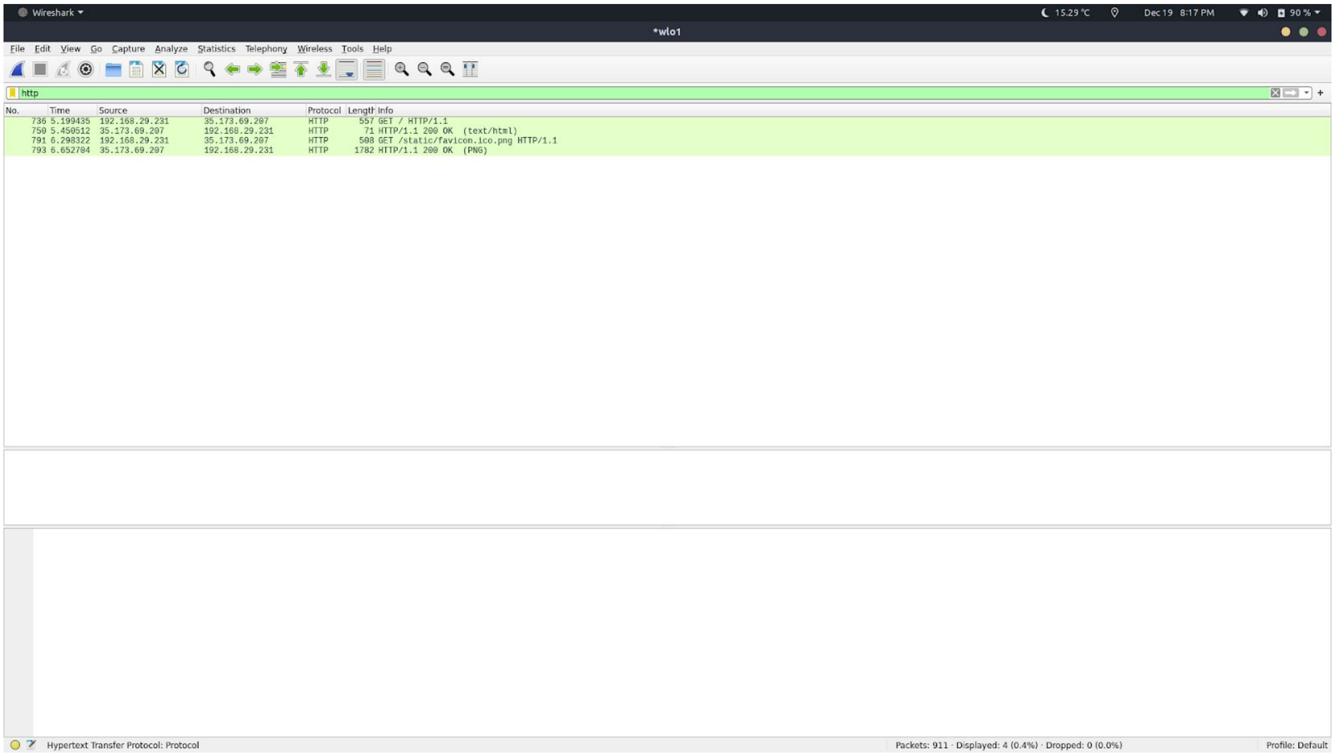

Wireshark
15.29 °C
Dec 19 8:17 PM
90 %
*wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.    Time     Source           Destination      Protocol Length Info
   736 5.199435 192.168.29.231   35.173.69.207    HTTP      557 GET / HTTP/1.1
   750 5.450512 35.173.69.207    192.168.29.231   HTTP       71 HTTP/1.1 200 OK  (text/html)
   791 6.298322 192.168.29.231   35.173.69.207    HTTP      508 GET /static/favicon.ico.png HTTP/1.1
   793 6.652704 35.173.69.207    192.168.29.231   HTTP     1782 HTTP/1.1 200 OK  (PNG)
```

Hypertext Transfer Protocol: Protocol | Packets: 911 · Displayed: 4 (0.4%) · Dropped: 0 (0.0%) | Profile: Default

As shown in the screenshot above the GET(736) was sent at 5.199435 second and the reply OK(750) was received at 5.450512 second. Thus the delay is (5.450512-5.199435) seconds which is 251.077 milliseconds.

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


Wireshark
15.29 °C
Dec 19 8:17 PM
90 %
*wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

```
No.      Time      Source          Destination     Protocol Length Info
    736 5.199435  192.168.29.231  35.173.69.207   HTTP       557 GET / HTTP/1.1
    750 5.450512  35.173.69.207   192.168.29.231  HTTP        71 HTTP/1.1 200 OK  (text/html)
    791 6.298322  192.168.29.231  35.173.69.207   HTTP       508 GET /static/favicon.ico.png HTTP/1.1
    793 6.652704  35.173.69.207   192.168.29.231  HTTP      1782 HTTP/1.1 200 OK  (PNG)
```

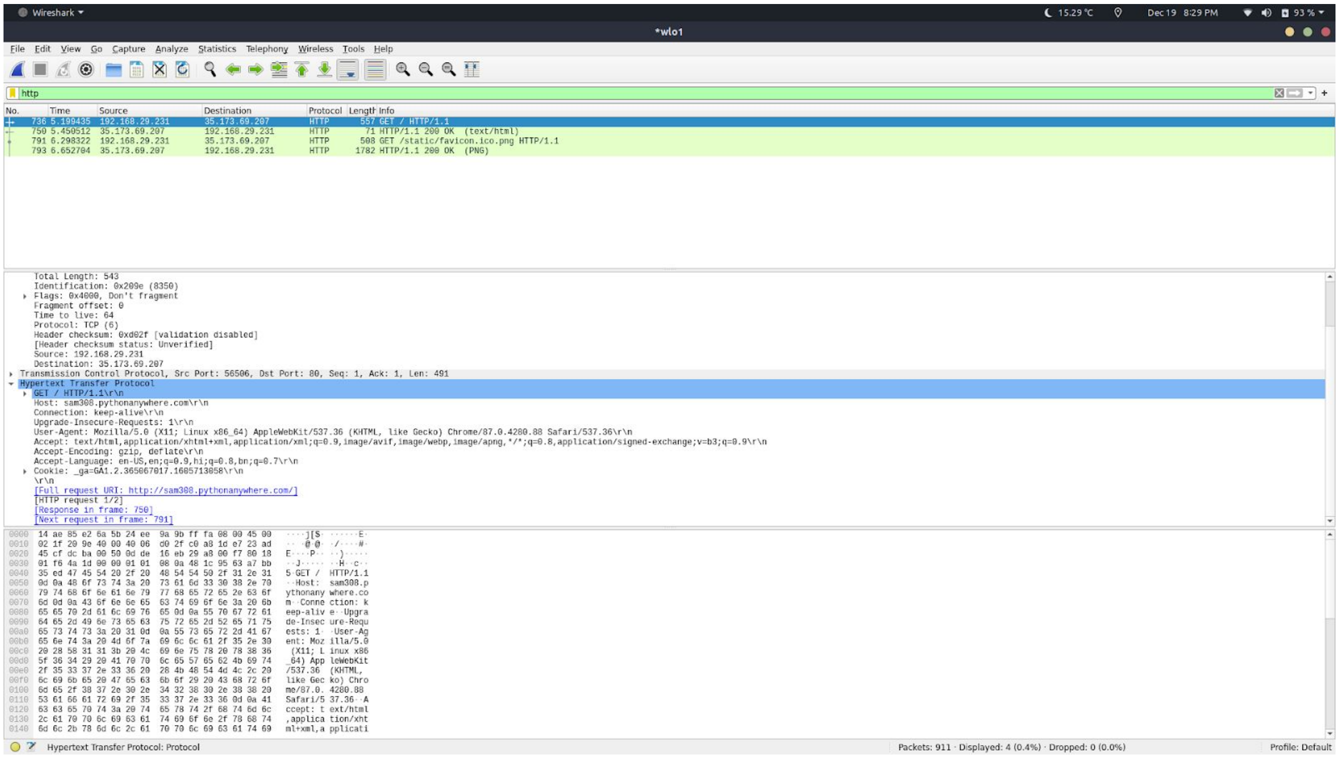
Hypertext Transfer Protocol: Protocol

Packets: 911 · Displayed: 4 (0.4%) · Dropped: 0 (0.0%)

Profile: Default

As shown in the screenshot above, the IP address of the website is **35.173.69.207** and the IP address of my laptop is **192.168.29.231**

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.**


Wireshark
15.29 °C
Dec 19 8:29 PM
93 %
*wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
+
Hypertext Transfer Protocol: Protocol
Profile: Default

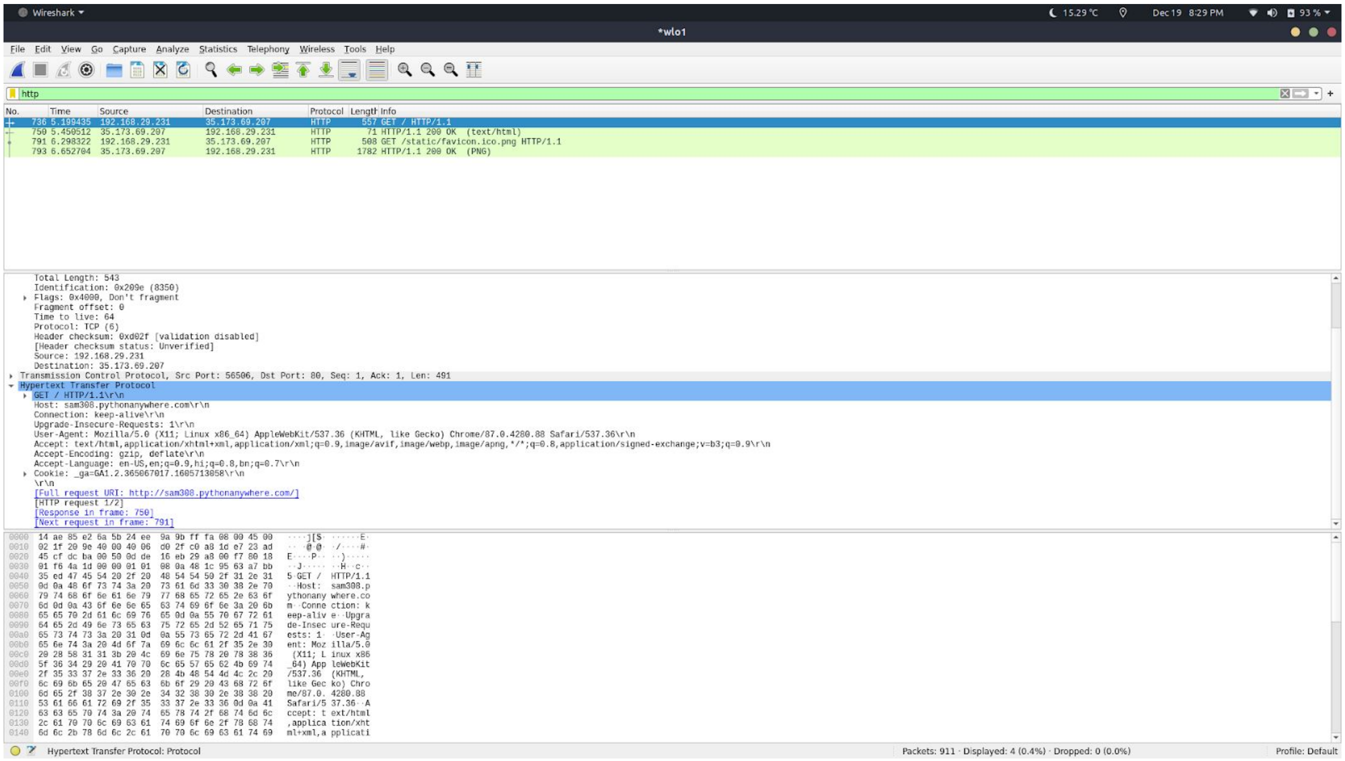
```
No.   Time       Source          Destination     Protocol Length Info
  736 5.199435   192.168.29.231  35.173.69.207   HTTP      557 GET / HTTP/1.1
  750 5.450512   35.173.69.207   192.168.29.231  HTTP       71 HTTP/1.1 200 OK  (text/html)
  791 6.298322   192.168.29.231  35.173.69.207   HTTP      508 GET /static/favicon.ico.png HTTP/1.1
  793 6.652704   35.173.69.207   192.168.29.231  HTTP     1782 HTTP/1.1 200 OK  (PNG)
```

```
    Total Length: 543
    Identification: 0x209e (8350)
  ▸ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0xd02f [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.29.231
    Destination: 35.173.69.207
▸ Transmission Control Protocol, Src Port: 56506, Dst Port: 80, Seq: 1, Ack: 1, Len: 491
▾ Hypertext Transfer Protocol
  ▸ GET / HTTP/1.1\r\n
    Host: sam308.pythonanywhere.com\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,hi;q=0.8,bn;q=0.7\r\n
  ▸ Cookie: _ga=GA1.2.365067017.1605713058\r\n
    \r\n
    [Full request URI: http://sam308.pythonanywhere.com/]
    [HTTP request 1/2]
    [Response in frame: 750]
    [Next request in frame: 791]
```

```
0000  14 ae 85 e2 6a 5b 24 ee  9a 9b ff fa 08 00 45 00   ····j[$· ······E·
0010  02 1f 20 9e 40 00 40 06  d0 2f c0 a8 1d e7 23 ad   ·· ·@·@· ·/····#·
0020  45 cf dc ba 00 50 0d de  16 eb 29 a8 00 f7 80 18   E····P·· ··)·····
0030  01 f6 4a 1d 00 00 01 01  08 0a 48 1c 95 63 a7 bb   ··J····· ··H··c··
0040  35 ed 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 31   5·GET /  HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20  73 61 6d 33 30 38 2e 70   ··Host:  sam308.p
0060  79 74 68 6f 6e 61 6e 79  77 68 65 72 65 2e 63 6f   ythonany where.co
0070  6d 0d 0a 43 6f 6e 6e 65  63 74 69 6f 6e 3a 20 6b   m··Conne ction: k
0080  65 65 70 2d 61 6c 69 76  65 0d 0a 55 70 67 72 61   eep-aliv e··Upgra
0090  64 65 2d 49 6e 73 65 63  75 72 65 2d 52 65 71 75   de-Insec ure-Requ
00a0  65 73 74 73 3a 20 31 0d  0a 55 73 65 72 2d 41 67   ests: 1· ·User-Ag
00b0  65 6e 74 3a 20 4d 6f 7a  69 6c 6c 61 2f 35 2e 30   ent: Moz illa/5.0
00c0  20 28 58 31 31 3b 20 4c  69 6e 75 78 20 78 38 36    (X11; L inux x86
00d0  5f 36 34 29 20 41 70 70  6c 65 57 65 62 4b 69 74   _64) App leWebKit
00e0  2f 35 33 37 2e 33 36 20  28 4b 48 54 4d 4c 2c 20   /537.36  (KHTML,
00f0  6c 69 6b 65 20 47 65 63  6b 6f 29 20 43 68 72 6f   like Gec ko) Chro
0100  6d 65 2f 38 37 2e 30 2e  34 32 38 30 2e 38 38 20   me/87.0. 4280.88
0110  53 61 66 61 72 69 2f 35  33 37 2e 33 36 0d 0a 41   Safari/5 37.36··A
0120  63 63 65 70 74 3a 20 74  65 78 74 2f 68 74 6d 6c   ccept: t ext/html
0130  2c 61 70 70 6c 69 63 61  74 69 6f 6e 2f 78 68 74   ,applica tion/xht
0140  6d 6c 2b 78 6d 6c 2c 61  70 70 6c 69 63 61 74 69   ml+xml,a pplicati
```

Packets: 911 · Displayed: 4 (0.4%) · Dropped: 0 (0.0%)

## e. Find out the value of the Host from the Packet Details Panel, within the GET command.


Wireshark
15.29 °C
Dec 19 8:29 PM
93 %
*wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

```
No.    Time      Source          Destination     Protocol Length Info
   736 5.199435  192.168.29.231  35.173.69.207   HTTP      557 GET / HTTP/1.1
   750 5.450512  35.173.69.207   192.168.29.231  HTTP       71 HTTP/1.1 200 OK  (text/html)
   791 6.298322  192.168.29.231  35.173.69.207   HTTP      508 GET /static/favicon.ico.png HTTP/1.1
   793 6.652704  35.173.69.207   192.168.29.231  HTTP     1782 HTTP/1.1 200 OK  (PNG)
```

```
    Total Length: 543
    Identification: 0x209e (8350)
  ▸ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0xd02f [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.29.231
    Destination: 35.173.69.207
▸ Transmission Control Protocol, Src Port: 56506, Dst Port: 80, Seq: 1, Ack: 1, Len: 491
▾ Hypertext Transfer Protocol
  ▸ GET / HTTP/1.1\r\n
    Host: sam308.pythonanywhere.com\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,hi;q=0.8,bn;q=0.7\r\n
  ▸ Cookie: _ga=GA1.2.365067017.1605713058\r\n
    \r\n
    [Full request URI: http://sam308.pythonanywhere.com/]
    [HTTP request 1/2]
    [Response in frame: 750]
    [Next request in frame: 791]
```

```
0000  14 ae 85 e2 6a 5b 24 ee  9a 9b ff fa 08 00 45 00   ····j[$· ······E·
0010  02 1f 20 9e 40 00 40 06  d0 2f c0 a8 1d e7 23 ad   ·· ·@·@· ·/····#·
0020  45 cf dc ba 00 50 0d de  16 eb 29 a8 00 f7 80 18   E····P·· ··)·····
0030  01 f6 4a 1d 00 00 01 01  08 0a 48 1c 95 63 a7 bb   ··J····· ··H··c··
0040  35 ed 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 31   5·GET /  HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20  73 61 6d 33 30 38 2e 70   ··Host:  sam308.p
0060  79 74 68 6f 6e 61 6e 79  77 68 65 72 65 2e 63 6f   ythonany where.co
0070  6d 0d 0a 43 6f 6e 6e 65  63 74 69 6f 6e 3a 20 6b   m··Conne ction: k
0080  65 65 70 2d 61 6c 69 76  65 0d 0a 55 70 67 72 61   eep-aliv e··Upgra
0090  64 65 2d 49 6e 73 65 63  75 72 65 2d 52 65 71 75   de-Insec ure-Requ
00a0  65 73 74 73 3a 20 31 0d  0a 55 73 65 72 2d 41 67   ests: 1· ·User-Ag
00b0  65 6e 74 3a 20 4d 6f 7a  69 6c 6c 61 2f 35 2e 30   ent: Moz illa/5.0
00c0  20 28 58 31 31 3b 20 4c  69 6e 75 78 20 78 38 36    (X11; L inux x86
00d0  5f 36 34 29 20 41 70 70  6c 65 57 65 62 4b 69 74   _64) App leWebKit
00e0  2f 35 33 37 2e 33 36 20  28 4b 48 54 4d 4c 2c 20   /537.36  (KHTML,
00f0  6c 69 6b 65 20 47 65 63  6b 6f 29 20 43 68 72 6f   like Gec ko) Chro
0100  6d 65 2f 38 37 2e 30 2e  34 32 38 30 2e 38 38 20   me/87.0. 4280.88
0110  53 61 66 61 72 69 2f 35  33 37 2e 33 36 0d 0a 41   Safari/5 37.36··A
0120  63 63 65 70 74 3a 20 74  65 78 74 2f 68 74 6d 6c   ccept: t ext/html
0130  2c 61 70 70 6c 69 63 61  74 69 6f 6e 2f 78 68 74   ,applica tion/xht
0140  6d 6c 2b 78 6d 6c 2c 61  70 70 6c 69 63 61 74 69   ml+xml,a pplicati
```

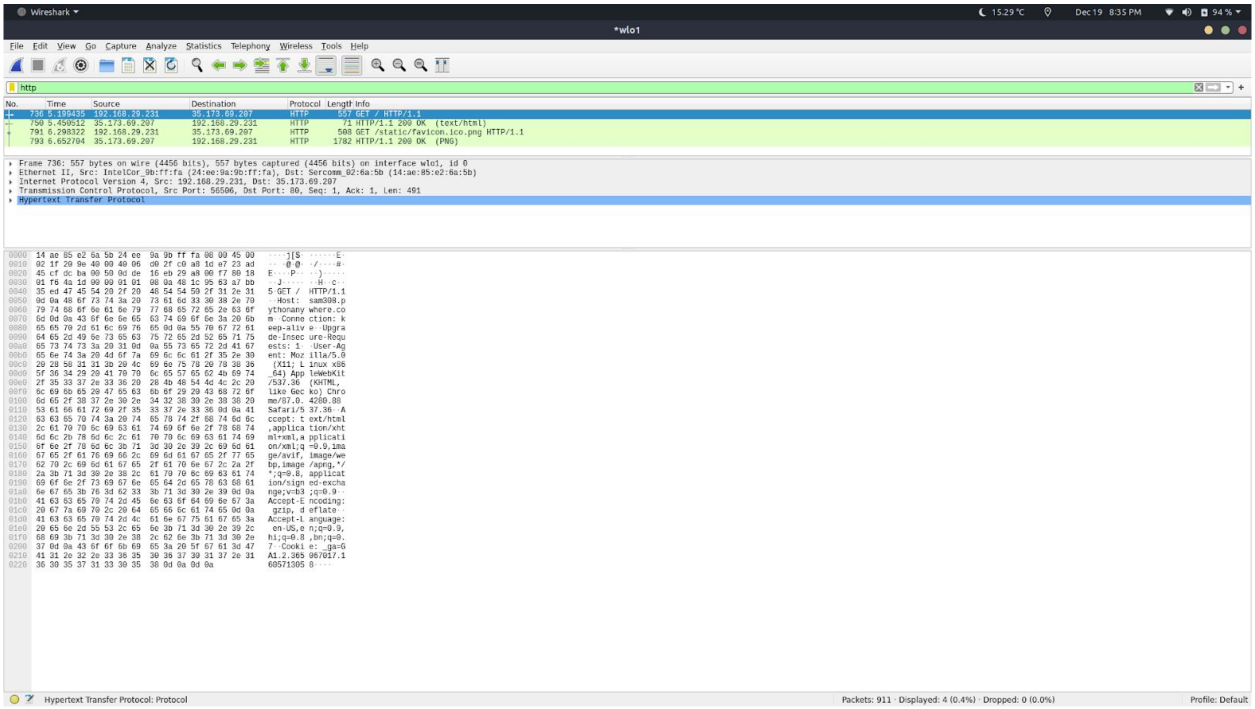
Hypertext Transfer Protocol: Protocol

Packets: 911 · Displayed: 4 (0.4%) · Dropped: 0 (0.0%)

Profile: Default

As shown in the screenshot above, the Host is: **sam308.pythonanywhere.com\r\n**

## Q3. Highlight the Hex and ASCII representations of the packet in the Packet Bytes Panel.


Wireshark
*wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time      Source          Destination     Protocol Length Info
  736 5.199435  192.168.29.231  35.173.69.207   HTTP      557 GET / HTTP/1.1
  750 5.450512  35.173.69.207   192.168.29.231  HTTP       71 HTTP/1.1 200 OK  (text/html)
  791 6.298322  192.168.29.231  35.173.69.207   HTTP      508 GET /static/favicon.ico.png HTTP/1.1
  793 6.652704  35.173.69.207   192.168.29.231  HTTP     1782 HTTP/1.1 200 OK  (PNG)
```

```
▸ Frame 736: 557 bytes on wire (4456 bits), 557 bytes captured (4456 bits) on interface wlo1, id 0
▸ Ethernet II, Src: IntelCor_9b:ff:fa (24:ee:9a:9b:ff:fa), Dst: Sercomm_02:6a:5b (14:ae:85:e2:6a:5b)
▸ Internet Protocol Version 4, Src: 192.168.29.231, Dst: 35.173.69.207
▸ Transmission Control Protocol, Src Port: 56506, Dst Port: 80, Seq: 1, Ack: 1, Len: 491
▸ Hypertext Transfer Protocol
```

```
0000  14 ae 85 e2 6a 5b 24 ee  9a 9b ff fa 08 00 45 00   ····j[$· ······E·
0010  02 1f 20 9e 40 00 40 06  d0 2f c0 a8 1d e7 23 ad   ·· ·@·@· ·/····#·
0020  45 cf dc ba 00 50 0d de  16 eb 29 a8 00 f7 80 18   E····P·· ··)·····
0030  01 f6 4a 1d 00 00 01 01  08 0a 48 1c 95 63 a7 bb   ··J····· ··H··c··
0040  35 ed 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 31   5·GET /  HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20  73 61 6d 33 30 38 2e 70   ··Host:  sam308.p
0060  79 74 68 6f 6e 61 6e 79  77 68 65 72 65 2e 63 6f   ythonany where.co
0070  6d 0d 0a 43 6f 6e 6e 65  63 74 69 6f 6e 3a 20 6b   m··Conne ction: k
0080  65 65 70 2d 61 6c 69 76  65 0d 0a 55 70 67 72 61   eep-aliv e··Upgra
0090  64 65 2d 49 6e 73 65 63  75 72 65 2d 52 65 71 75   de-Insec ure-Requ
00a0  65 73 74 73 3a 20 31 0d  0a 55 73 65 72 2d 41 67   ests: 1· ·User-Ag
00b0  65 6e 74 3a 20 4d 6f 7a  69 6c 6c 61 2f 35 2e 30   ent: Moz illa/5.0
00c0  20 28 58 31 31 3b 20 4c  69 6e 75 78 20 78 38 36    (X11; L inux x86
00d0  5f 36 34 29 20 41 70 70  6c 65 57 65 62 4b 69 74   _64) App leWebKit
00e0  2f 35 33 37 2e 33 36 20  28 4b 48 54 4d 4c 2c 20   /537.36  (KHTML,
00f0  6c 69 6b 65 20 47 65 63  6b 6f 29 20 43 68 72 6f   like Gec ko) Chro
0100  6d 65 2f 38 37 2e 30 2e  34 32 38 30 2e 38 38 20   me/87.0. 4280.88
0110  53 61 66 61 72 69 2f 35  33 37 2e 33 36 0d 0a 41   Safari/5 37.36··A
0120  63 63 65 70 74 3a 20 74  65 78 74 2f 68 74 6d 6c   ccept: t ext/html
0130  2c 61 70 70 6c 69 63 61  74 69 6f 6e 2f 78 68 74   ,applica tion/xht
0140  6d 6c 2b 78 6d 6c 2c 61  70 70 6c 69 63 61 74 69   ml+xml,a pplicati
0150  6f 6e 2f 78 6d 6c 3b 71  3d 30 2e 39 2c 69 6d 61   on/xml;q =0.9,ima
0160  67 65 2f 61 76 69 66 2c  69 6d 61 67 65 2f 77 65   ge/avif, image/we
0170  62 70 2c 69 6d 61 67 65  2f 61 70 6e 67 2c 2a 2f   bp,image /apng,*/
0180  2a 3b 71 3d 30 2e 38 2c  61 70 70 6c 69 63 61 74   *;q=0.8, applicat
0190  69 6f 6e 2f 73 69 67 6e  65 64 2d 65 78 63 68 61   ion/sign ed-excha
01a0  6e 67 65 3b 76 3d 62 33  3b 71 3d 30 2e 39 0d 0a   nge;v=b3 ;q=0.9··
01b0  41 63 63 65 70 74 2d 45  6e 63 6f 64 69 6e 67 3a   Accept-E ncoding:
01c0  20 67 7a 69 70 2c 20 64  65 66 6c 61 74 65 0d 0a    gzip, d eflate··
01d0  41 63 63 65 70 74 2d 4c  61 6e 67 75 61 67 65 3a   Accept-L anguage:
01e0  20 65 6e 2d 55 53 2c 65  6e 3b 71 3d 30 2e 39 2c    en-US,e n;q=0.9,
01f0  68 69 3b 71 3d 30 2e 38  2c 62 6e 3b 71 3d 30 2e   hi;q=0.8 ,bn;q=0.
0200  37 0d 0a 43 6f 6f 6b 69  65 3a 20 5f 67 61 3d 47   7··Cooki e: _ga=G
0210  41 31 2e 32 2e 33 36 35  30 36 37 30 31 37 2e 31   A1.2.365 067017.1
0220  36 30 35 37 31 33 30 35  38 0d 0a 0d 0a            60571305 8····
```

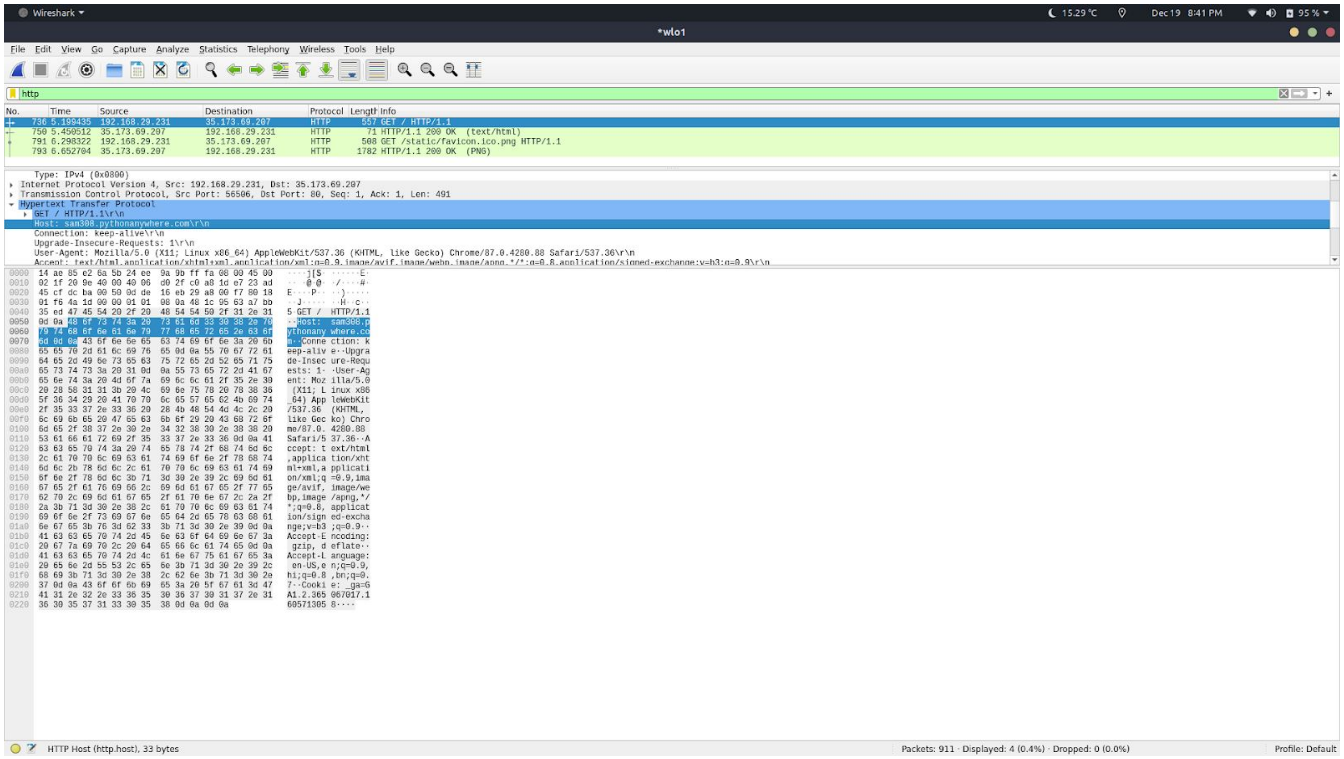
```
Hypertext Transfer Protocol: Protocol     Packets: 911 · Displayed: 4 (0.4%) · Dropped: 0 (0.0%)     Profile: Default
```

The HEX and ASCII representations of the packet is:

```
0000   14 ae 85 e2 6a 5b 24 ee 9a 9b ff fa 08 00 45 00   ....j[$.......E.
0010   02 1f 20 9e 40 00 40 06 d0 2f c0 a8 1d e7 23 ad   .. .@.@../....#.
0020   45 cf dc ba 00 50 0d de 16 eb 29 a8 00 f7 80 18   E....P....).....
0030   01 f6 4a 1d 00 00 01 01 08 0a 48 1c 95 63 a7 bb   ..J.......H..c..
0040   35 ed 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31   5.GET / HTTP/1.1
0050   0d 0a 48 6f 73 74 3a 20 73 61 6d 33 30 38 2e 70   ..Host: sam308.p
0060   79 74 68 6f 6e 61 6e 79 77 68 65 72 65 2e 63 6f   ythonanywhere.co
0070   6d 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b   m..Connection: k
0080   65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 67 72 61   eep-alive..Upgra
```

```
0090   64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75   de-Insecure-Requ    (Continued....)
00a0   65 73 74 73 3a 20 31 0d 0a 55 73 65 72 2d 41 67   ests: 1..User-Ag
00b0   65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30   ent: Mozilla/5.0
00c0   20 28 58 31 31 3b 20 4c 69 6e 75 78 20 78 38 36    (X11; Linux x86
00d0   5f 36 34 29 20 41 70 70 6c 65 57 65 62 4b 69 74   _64) AppleWebKit
00e0   2f 35 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20   /537.36 (KHTML,
00f0   6c 69 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f   like Gecko) Chro
0100   6d 65 2f 38 37 2e 30 2e 34 32 38 30 2e 38 38 20   me/87.0.4280.88
0110   53 61 66 61 72 69 2f 35 33 37 2e 33 36 0d 0a 41   Safari/537.36..A
0120   63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c   ccept: text/html
0130   2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74   ,application/xht
0140   6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69   ml+xml,applicati
0150   6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61   on/xml;q=0.9,ima
0160   67 65 2f 61 76 69 66 2c 69 6d 61 67 65 2f 77 65   ge/avif,image/we
0170   62 70 2c 69 6d 61 67 65 2f 61 70 6e 67 2c 2a 2f   bp,image/apng,*/
0180   2a 3b 71 3d 30 2e 38 2c 61 70 70 6c 69 63 61 74   *;q=0.8,applicat
0190   69 6f 6e 2f 73 69 67 6e 65 64 2d 65 78 63 68 61   ion/signed-excha
01a0   6e 67 65 3b 76 3d 62 33 3b 71 3d 30 2e 39 0d 0a   nge;v=b3;q=0.9..
01b0   41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a   Accept-Encoding:
01c0   20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a    gzip, deflate..
01d0   41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a   Accept-Language:
01e0   20 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e 39 2c    en-US,en;q=0.9,
01f0   68 69 3b 71 3d 30 2e 38 2c 62 6e 3b 71 3d 30 2e   hi;q=0.8,bn;q=0.
0200   37 0d 0a 43 6f 6f 6b 69 65 3a 20 5f 67 61 3d 47   7..Cookie: _ga=G
0210   41 31 2e 32 2e 33 36 35 30 36 37 30 31 37 2e 31   A1.2.365067017.1
0220   36 30 35 37 31 33 30 35 38 0d 0a 0d 0a            605713058....
```

## Q4. Find out the first 4 bytes of the Hex value of the Host parameter from the Packet Bytes Panel.


Wireshark
15.29 °C
Dec 19 8:41 PM
95 %
*wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.    Time      Source          Destination     Protocol Length Info
   736 5.199435  192.168.29.231  35.173.69.207   HTTP      557 GET / HTTP/1.1
   750 5.450512  35.173.69.207   192.168.29.231  HTTP       71 HTTP/1.1 200 OK  (text/html)
   791 6.298322  192.168.29.231  35.173.69.207   HTTP      508 GET /static/favicon.ico.png HTTP/1.1
   793 6.652704  35.173.69.207   192.168.29.231  HTTP     1782 HTTP/1.1 200 OK  (PNG)
```

```
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 192.168.29.231, Dst: 35.173.69.207
▸ Transmission Control Protocol, Src Port: 56506, Dst Port: 80, Seq: 1, Ack: 1, Len: 491
▾ Hypertext Transfer Protocol
  ▸ GET / HTTP/1.1\r\n
    Host: sam308.pythonanywhere.com\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
```

```
0000  14 ae 85 e2 6a 5b 24 ee  9a 9b ff fa 08 00 45 00   ····j[$· ······E·
0010  02 1f 20 9e 40 00 40 06  d0 2f c0 a8 1d e7 23 ad   ·· ·@·@· ·/····#·
0020  45 cf dc ba 00 50 0d de  16 eb 29 a8 00 f7 80 18   E····P·· ··)·····
0030  01 f6 4a 1d 00 00 01 01  08 0a 48 1c 95 63 a7 bb   ··J····· ··H··c··
0040  35 ed 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 31   5·GET /  HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20  73 61 6d 33 30 38 2e 70   ··Host:  sam308.p
0060  79 74 68 6f 6e 61 6e 79  77 68 65 72 65 2e 63 6f   ythonany where.co
0070  6d 0d 0a 43 6f 6e 6e 65  63 74 69 6f 6e 3a 20 6b   m··Conne ction: k
0080  65 65 70 2d 61 6c 69 76  65 0d 0a 55 70 67 72 61   eep-aliv e··Upgra
0090  64 65 2d 49 6e 73 65 63  75 72 65 2d 52 65 71 75   de-Insec ure-Requ
00a0  65 73 74 73 3a 20 31 0d  0a 55 73 65 72 2d 41 67   ests: 1· ·User-Ag
00b0  65 6e 74 3a 20 4d 6f 7a  69 6c 6c 61 2f 35 2e 30   ent: Moz illa/5.0
00c0  20 28 58 31 31 3b 20 4c  69 6e 75 78 20 78 38 36    (X11; L inux x86
00d0  5f 36 34 29 20 41 70 70  6c 65 57 65 62 4b 69 74   _64) App leWebKit
00e0  2f 35 33 37 2e 33 36 20  28 4b 48 54 4d 4c 2c 20   /537.36  (KHTML,
00f0  6c 69 6b 65 20 47 65 63  6b 6f 29 20 43 68 72 6f   like Gec ko) Chro
0100  6d 65 2f 38 37 2e 30 2e  34 32 38 30 2e 38 38 20   me/87.0. 4280.88
0110  53 61 66 61 72 69 2f 35  33 37 2e 33 36 0d 0a 41   Safari/5 37.36··A
0120  63 63 65 70 74 3a 20 74  65 78 74 2f 68 74 6d 6c   ccept: t ext/html
0130  2c 61 70 70 6c 69 63 61  74 69 6f 6e 2f 78 68 74   ,applica tion/xht
0140  6d 6c 2b 78 6d 6c 2c 61  70 70 6c 69 63 61 74 69   ml+xml,a pplicati
0150  6f 6e 2f 78 6d 6c 3b 71  3d 30 2e 39 2c 69 6d 61   on/xml;q =0.9,ima
0160  67 65 2f 61 76 69 66 2c  69 6d 61 67 65 2f 77 65   ge/avif, image/we
0170  62 70 2c 69 6d 61 67 65  2f 61 70 6e 67 2c 2a 2f   bp,image /apng,*/
0180  2a 3b 71 3d 30 2e 38 2c  61 70 70 6c 69 63 61 74   *;q=0.8, applicat
0190  69 6f 6e 2f 73 69 67 6e  65 64 2d 65 78 63 68 61   ion/sign ed-excha
01a0  6e 67 65 3b 76 3d 62 33  3b 71 3d 30 2e 39 0d 0a   nge;v=b3 ;q=0.9··
01b0  41 63 63 65 70 74 2d 45  6e 63 6f 64 69 6e 67 3a   Accept-E ncoding:
01c0  20 67 7a 69 70 2c 20 64  65 66 6c 61 74 65 0d 0a    gzip, d eflate··
01d0  41 63 63 65 70 74 2d 4c  61 6e 67 75 61 67 65 3a   Accept-L anguage:
01e0  20 65 6e 2d 55 53 2c 65  6e 3b 71 3d 30 2e 39 2c    en-US,e n;q=0.9,
01f0  68 69 3b 71 3d 30 2e 38  2c 62 6e 3b 71 3d 30 2e   hi;q=0.8 ,bn;q=0.
0200  37 0d 0a 43 6f 6f 6b 69  65 3a 20 5f 67 61 3d 47   7··Cooki e: _ga=G
0210  41 31 2e 32 2e 33 36 35  30 36 37 30 31 37 2e 31   A1.2.365 067017.1
0220  36 30 35 37 31 33 30 35  38 0d 0a 0d 0a            60571305 8····
```

HTTP Host (http.host), 33 bytes

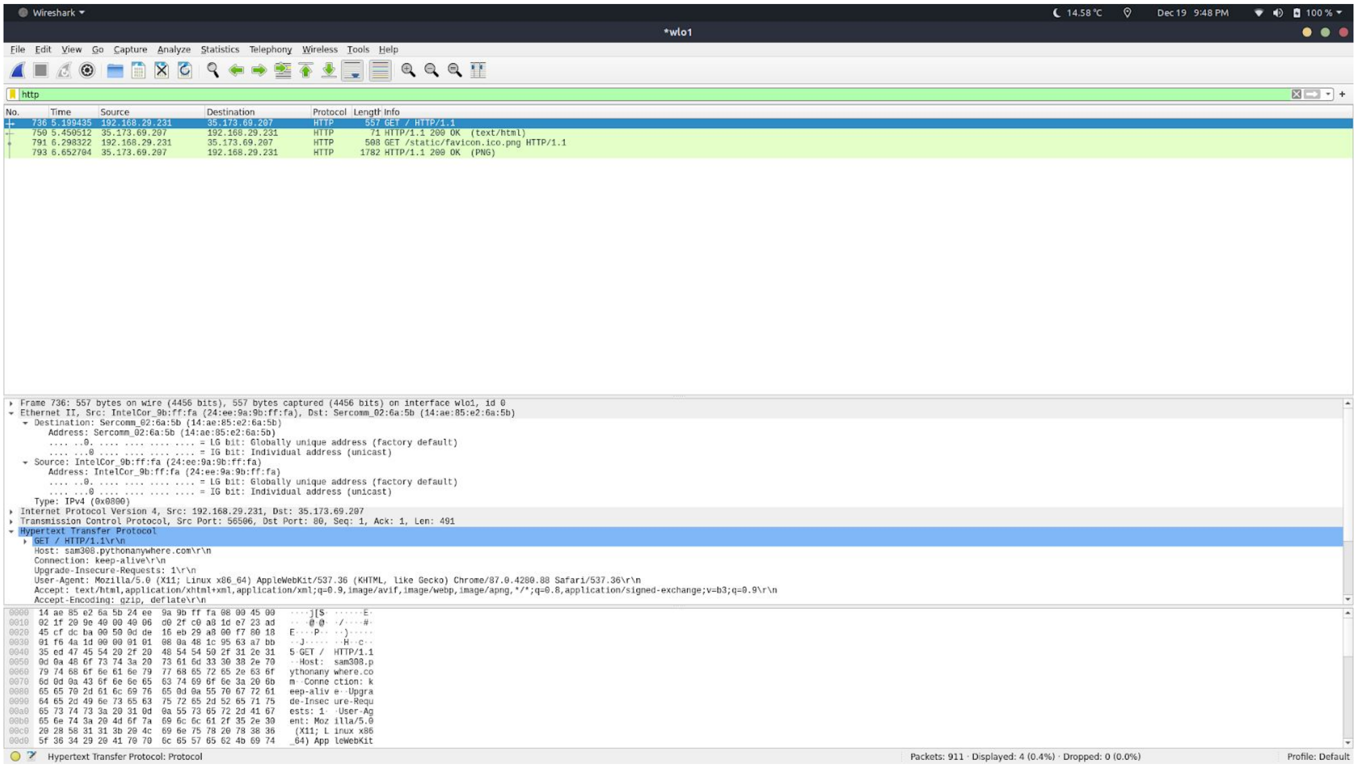
Packets: 911 · Displayed: 4 (0.4%) · Dropped: 0 (0.0%)

Profile: Default

The first four bytes of the Hex value of the Host parameter from the Packet Bytes Panel are: **48 cf 73 74**

## Q5. Filter packets with http, TCP, DNS and other protocols. Find out what 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.

## HTTP:


Wireshark
14.58 °C
Dec 19 9:48 PM
100 %
*wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

```
No.   Time      Source          Destination     Protocol Length Info
  736 5.199435  192.168.29.231  35.173.69.207   HTTP      557 GET / HTTP/1.1
  750 5.450512  35.173.69.207   192.168.29.231  HTTP       71 HTTP/1.1 200 OK  (text/html)
  791 6.298322  192.168.29.231  35.173.69.207   HTTP      508 GET /static/favicon.ico.png HTTP/1.1
  793 6.652704  35.173.69.207   192.168.29.231  HTTP     1782 HTTP/1.1 200 OK  (PNG)
```

```
▸ Frame 736: 557 bytes on wire (4456 bits), 557 bytes captured (4456 bits) on interface wlo1, id 0
▾ Ethernet II, Src: IntelCor_9b:ff:fa (24:ee:9a:9b:ff:fa), Dst: Sercomm_02:6a:5b (14:ae:85:e2:6a:5b)
  ▾ Destination: Sercomm_02:6a:5b (14:ae:85:e2:6a:5b)
      Address: Sercomm_02:6a:5b (14:ae:85:e2:6a:5b)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: IntelCor_9b:ff:fa (24:ee:9a:9b:ff:fa)
      Address: IntelCor_9b:ff:fa (24:ee:9a:9b:ff:fa)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 192.168.29.231, Dst: 35.173.69.207
▸ Transmission Control Protocol, Src Port: 56506, Dst Port: 80, Seq: 1, Ack: 1, Len: 491
▾ Hypertext Transfer Protocol
  ▸ GET / HTTP/1.1\r\n
    Host: sam308.pythonanywhere.com\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
```

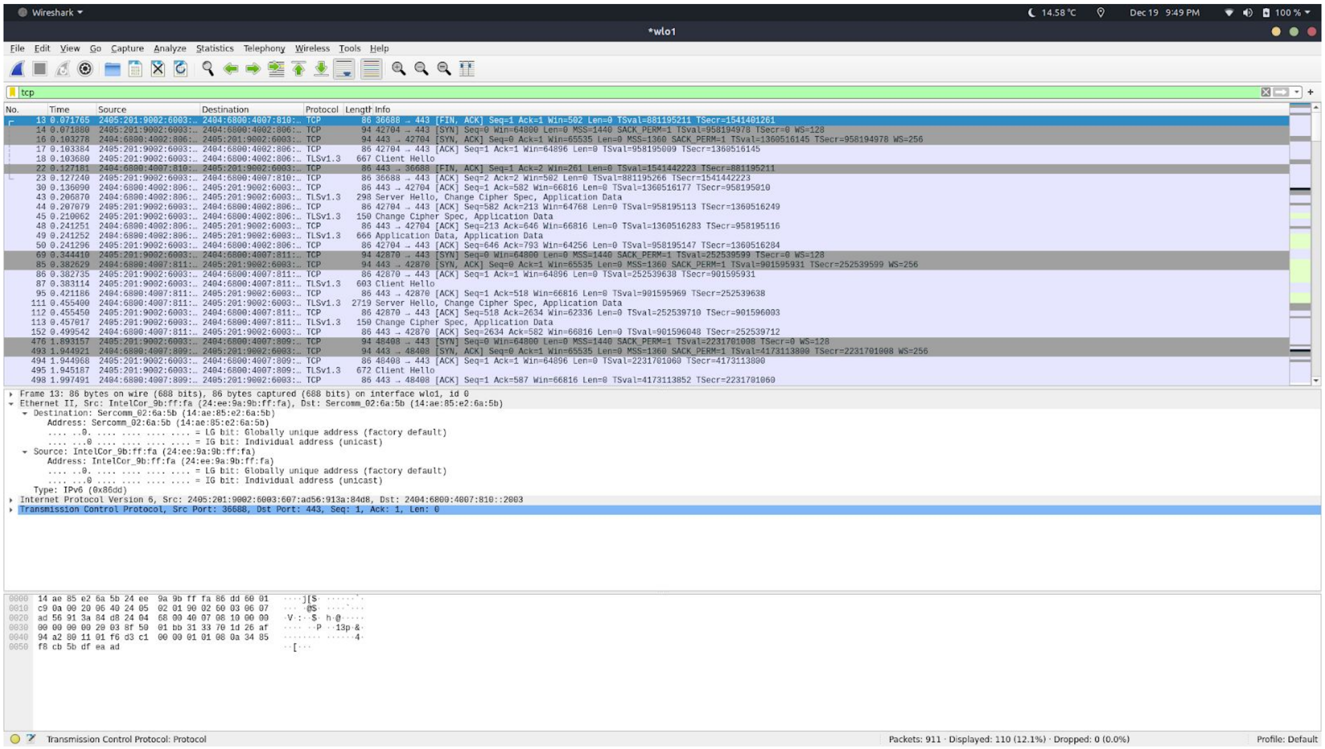
```
0000  14 ae 85 e2 6a 5b 24 ee  9a 9b ff fa 08 00 45 00   ····j[$· ······E·
0010  02 1f 20 9e 40 00 40 06  d0 2f c0 a8 1d e7 23 ad   ·· ·@·@· ·/····#·
0020  45 cf dc ba 00 50 0d de  16 eb 29 a8 00 f7 80 18   E····P·· ··)·····
0030  01 f6 4a 1d 00 00 01 01  08 0a 48 1c 95 63 a7 bb   ··J····· ··H··c··
0040  35 ed 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 31   5·GET /  HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20  73 61 6d 33 30 38 2e 70   ··Host:  sam308.p
0060  79 74 68 6f 6e 61 6e 79  77 68 65 72 65 2e 63 6f   ythonany where.co
0070  6d 0d 0a 43 6f 6e 6e 65  63 74 69 6f 6e 3a 20 6b   m··Conne ction: k
0080  65 65 70 2d 61 6c 69 76  65 0d 0a 55 70 67 72 61   eep-aliv e··Upgra
0090  64 65 2d 49 6e 73 65 63  75 72 65 2d 52 65 71 75   de-Insec ure-Requ
00a0  65 73 74 73 3a 20 31 0d  0a 55 73 65 72 2d 41 67   ests: 1· ·User-Ag
00b0  65 6e 74 3a 20 4d 6f 7a  69 6c 6c 61 2f 35 2e 30   ent: Moz illa/5.0
00c0  20 28 58 31 31 3b 20 4c  69 6e 75 78 20 78 38 36    (X11; L inux x86
00d0  5f 36 34 29 20 41 70 70  6c 65 57 65 62 4b 69 74   _64) App leWebKit
```

Hypertext Transfer Protocol: Protocol

Packets: 911 · Displayed: 4 (0.4%) · Dropped: 0 (0.0%)

Profile: Default

## TCP:


Wireshark
14.58 °C
Dec 19 9:49 PM
100 %
*wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

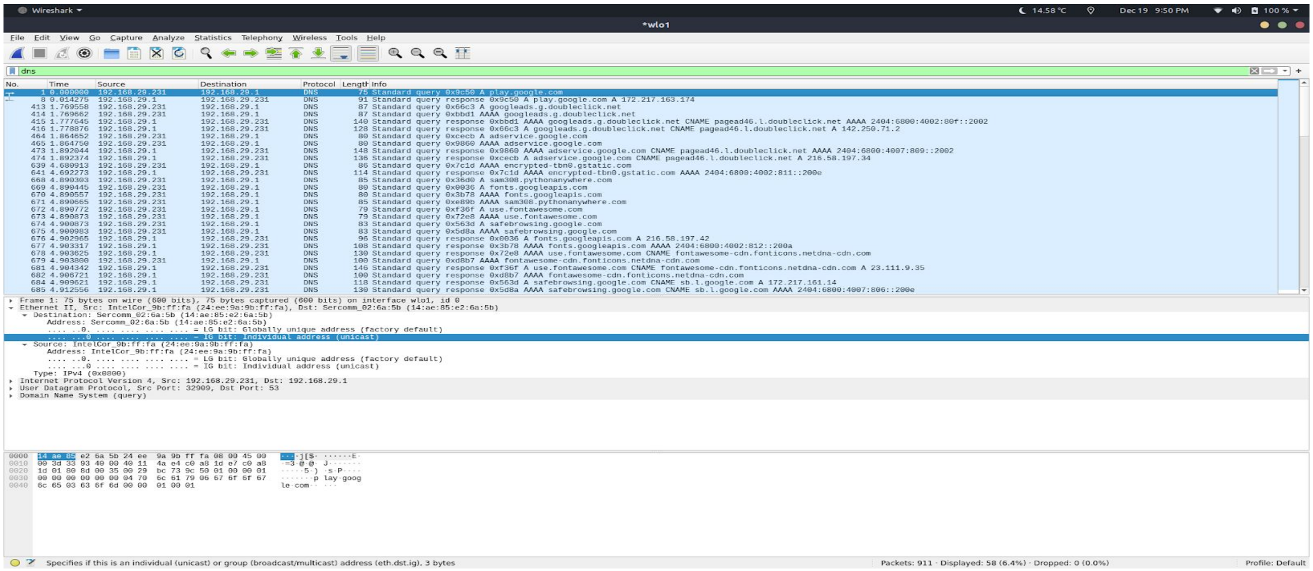
```
No.  Time      Source                Destination           Protocol Length Info
  13 0.071765  2405:201:9002:6003:…  2404:6800:4007:810:…  TCP        86 36688 → 443 [FIN, ACK] Seq=1 Ack=1 Win=502 Len=0 TSval=881195211 TSecr=1541401261
  14 0.071880  2405:201:9002:6003:…  2404:6800:4002:806:…  TCP        94 42704 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM=1 TSval=958194978 TSecr=0 WS=128
  16 0.103278  2404:6800:4002:806:…  2405:201:9002:6003:…  TCP        94 443 → 42704 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1360 SACK_PERM=1 TSval=1360516145 TSecr=958194978 WS=256
  17 0.103384  2405:201:9002:6003:…  2404:6800:4002:806:…  TCP        86 42704 → 443 [ACK] Seq=1 Ack=1 Win=64896 Len=0 TSval=958195009 TSecr=1360516145
  18 0.103680  2405:201:9002:6003:…  2404:6800:4002:806:…  TLSv1.3   667 Client Hello
  22 0.127181  2404:6800:4007:810:…  2405:201:9002:6003:…  TCP        86 443 → 36688 [FIN, ACK] Seq=1 Ack=2 Win=261 Len=0 TSval=1541442223 TSecr=881195211
  23 0.127240  2405:201:9002:6003:…  2404:6800:4007:810:…  TCP        86 36688 → 443 [ACK] Seq=2 Ack=2 Win=502 Len=0 TSval=881195266 TSecr=1541442223
  30 0.136090  2404:6800:4002:806:…  2405:201:9002:6003:…  TCP        86 443 → 42704 [ACK] Seq=1 Ack=582 Win=66816 Len=0 TSval=1360516177 TSecr=958195010
  43 0.206870  2404:6800:4002:806:…  2405:201:9002:6003:…  TLSv1.3   298 Server Hello, Change Cipher Spec, Application Data
  44 0.207079  2405:201:9002:6003:…  2404:6800:4002:806:…  TCP        86 42704 → 443 [ACK] Seq=582 Ack=213 Win=64768 Len=0 TSval=958195113 TSecr=1360516249
  45 0.210062  2405:201:9002:6003:…  2404:6800:4002:806:…  TLSv1.3   150 Change Cipher Spec, Application Data
  48 0.241251  2404:6800:4002:806:…  2405:201:9002:6003:…  TCP        86 443 → 42704 [ACK] Seq=213 Ack=646 Win=66816 Len=0 TSval=1360516283 TSecr=958195116
  49 0.241252  2404:6800:4002:806:…  2405:201:9002:6003:…  TLSv1.3   666 Application Data, Application Data
  50 0.241296  2405:201:9002:6003:…  2404:6800:4002:806:…  TCP        86 42704 → 443 [ACK] Seq=646 Ack=793 Win=64256 Len=0 TSval=958195147 TSecr=1360516284
  69 0.344410  2405:201:9002:6003:…  2404:6800:4007:811:…  TCP        94 42870 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM=1 TSval=252539599 TSecr=0 WS=128
  85 0.382629  2404:6800:4007:811:…  2405:201:9002:6003:…  TCP        94 443 → 42870 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1360 SACK_PERM=1 TSval=901595931 TSecr=252539599 WS=256
  86 0.382735  2405:201:9002:6003:…  2404:6800:4007:811:…  TCP        86 42870 → 443 [ACK] Seq=1 Ack=1 Win=64896 Len=0 TSval=252539638 TSecr=901595931
  87 0.383114  2405:201:9002:6003:…  2404:6800:4007:811:…  TLSv1.3   603 Client Hello
  95 0.421186  2404:6800:4007:811:…  2405:201:9002:6003:…  TCP        86 443 → 42870 [ACK] Seq=1 Ack=518 Win=66816 Len=0 TSval=901595969 TSecr=252539638
 111 0.455400  2404:6800:4007:811:…  2405:201:9002:6003:…  TLSv1.3  2719 Server Hello, Change Cipher Spec, Application Data
 112 0.455450  2405:201:9002:6003:…  2404:6800:4007:811:…  TCP        86 42870 → 443 [ACK] Seq=518 Ack=2634 Win=62336 Len=0 TSval=252539710 TSecr=901596003
 113 0.457017  2405:201:9002:6003:…  2404:6800:4007:811:…  TLSv1.3   150 Change Cipher Spec, Application Data
 152 0.499542  2404:6800:4007:811:…  2405:201:9002:6003:…  TCP        86 443 → 42870 [ACK] Seq=2634 Ack=582 Win=66816 Len=0 TSval=901596048 TSecr=252539712
 476 1.893157  2405:201:9002:6003:…  2404:6800:4007:809:…  TCP        94 48408 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM=1 TSval=2231701008 TSecr=0 WS=128
 493 1.944921  2404:6800:4007:809:…  2405:201:9002:6003:…  TCP        94 443 → 48408 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1360 SACK_PERM=1 TSval=4173113800 TSecr=2231701008 WS=256
 494 1.944968  2405:201:9002:6003:…  2404:6800:4007:809:…  TCP        86 48408 → 443 [ACK] Seq=1 Ack=1 Win=64896 Len=0 TSval=2231701060 TSecr=4173113800
 495 1.945187  2405:201:9002:6003:…  2404:6800:4007:809:…  TLSv1.3   672 Client Hello
 498 1.997491  2404:6800:4007:809:…  2405:201:9002:6003:…  TCP        86 443 → 48408 [ACK] Seq=1 Ack=587 Win=66816 Len=0 TSval=4173113852 TSecr=2231701060
```

```
▸ Frame 13: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface wlo1, id 0
▾ Ethernet II, Src: IntelCor_9b:ff:fa (24:ee:9a:9b:ff:fa), Dst: Sercomm_02:6a:5b (14:ae:85:e2:6a:5b)
  ▾ Destination: Sercomm_02:6a:5b (14:ae:85:e2:6a:5b)
      Address: Sercomm_02:6a:5b (14:ae:85:e2:6a:5b)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: IntelCor_9b:ff:fa (24:ee:9a:9b:ff:fa)
      Address: IntelCor_9b:ff:fa (24:ee:9a:9b:ff:fa)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv6 (0x86dd)
▸ Internet Protocol Version 6, Src: 2405:201:9002:6003:607:ad56:913a:84d8, Dst: 2404:6800:4007:810::2003
▸ Transmission Control Protocol, Src Port: 36688, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
```

```
0000  14 ae 85 e2 6a 5b 24 ee  9a 9b ff fa 86 dd 60 01   ····j[$· ······`·
0010  c9 0a 00 20 06 40 24 05  02 01 90 02 60 03 06 07   ··· ·@$· ····`···
0020  ad 56 91 3a 84 d8 24 04  68 00 40 07 08 10 00 00   ·V·:··$· h·@·····
0030  00 00 00 00 20 03 8f 50  01 bb 31 33 70 1d 26 af   ···· ··P ··13p·&·
0040  94 a2 80 11 01 f6 d3 c1  00 00 01 01 08 0a 34 85   ········ ······4·
0050  f8 cb 5b df ea ad                                  ··[···
```

Transmission Control Protocol: Protocol    Packets: 911 · Displayed: 110 (12.1%) · Dropped: 0 (0.0%)    Profile: Default

## DNS:


Wireshark
14.58 °C
Dec 19 9:50 PM
100 %
*wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

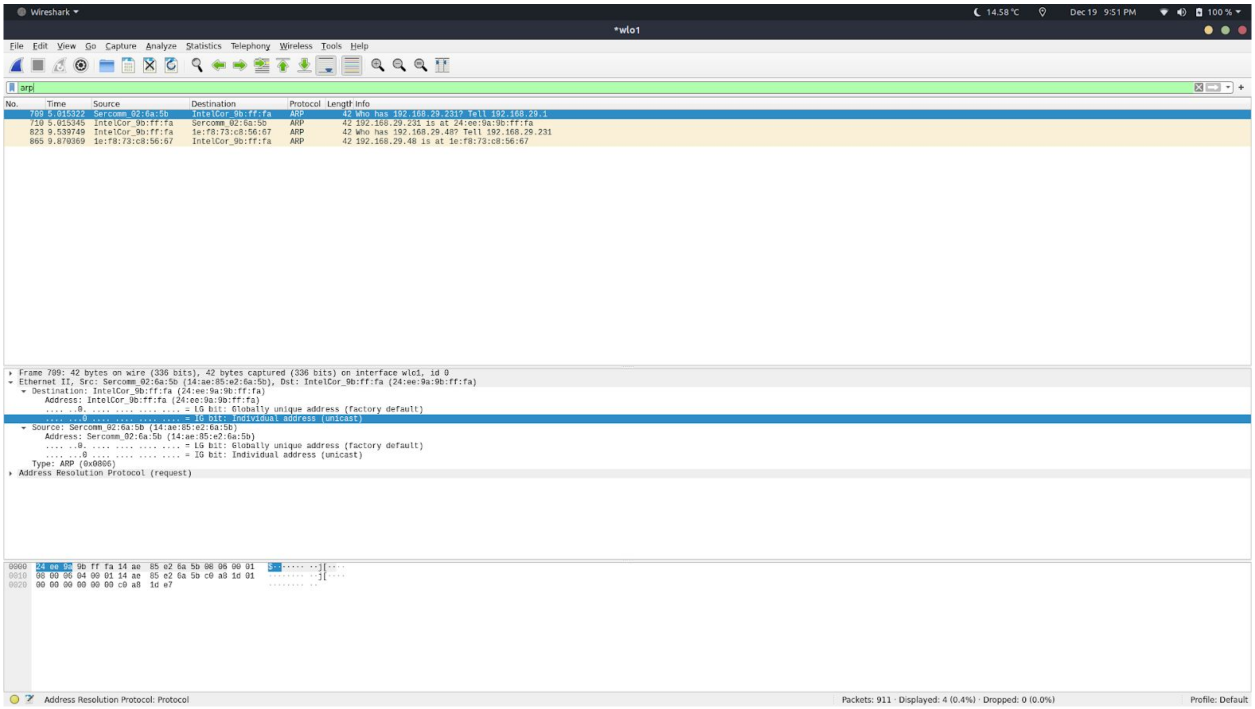
```
No.  Time      Source          Destination     Protocol Length Info
   1 0.000000  192.168.29.231  192.168.29.1    DNS       75 Standard query 0x9c50 A play.google.com
   8 0.014275  192.168.29.1    192.168.29.231  DNS       91 Standard query response 0x9c50 A play.google.com A 172.217.163.174
 413 1.769558  192.168.29.231  192.168.29.1    DNS       87 Standard query 0x66c3 A googleads.g.doubleclick.net
 414 1.769662  192.168.29.231  192.168.29.1    DNS       87 Standard query 0xbbd1 AAAA googleads.g.doubleclick.net
 415 1.777645  192.168.29.1    192.168.29.231  DNS      140 Standard query response 0xbbd1 AAAA googleads.g.doubleclick.net CNAME pagead46.l.doubleclick.net AAAA 2404:6800:4002:80f::2002
 416 1.778876  192.168.29.1    192.168.29.231  DNS      128 Standard query response 0x66c3 A googleads.g.doubleclick.net CNAME pagead46.l.doubleclick.net A 142.250.71.2
 464 1.864652  192.168.29.231  192.168.29.1    DNS       80 Standard query 0xcecb A adservice.google.com
 465 1.864750  192.168.29.231  192.168.29.1    DNS       80 Standard query 0x9860 AAAA adservice.google.com
 473 1.892044  192.168.29.1    192.168.29.231  DNS      148 Standard query response 0x9860 AAAA adservice.google.com CNAME pagead46.l.doubleclick.net AAAA 2404:6800:4007:809::2002
 474 1.892374  192.168.29.1    192.168.29.231  DNS      136 Standard query response 0xcecb A adservice.google.com CNAME pagead46.l.doubleclick.net A 216.58.197.34
 639 4.680913  192.168.29.231  192.168.29.1    DNS       86 Standard query 0x7c1d AAAA encrypted-tbn0.gstatic.com
 641 4.692273  192.168.29.1    192.168.29.231  DNS      114 Standard query response 0x7c1d AAAA encrypted-tbn0.gstatic.com AAAA 2404:6800:4002:811::200e
 668 4.890303  192.168.29.231  192.168.29.1    DNS       85 Standard query 0x36d0 A sam308.pythonanywhere.com
 669 4.890445  192.168.29.231  192.168.29.1    DNS       80 Standard query 0x0036 A fonts.googleapis.com
 670 4.890557  192.168.29.231  192.168.29.1    DNS       80 Standard query 0x3b78 AAAA fonts.googleapis.com
 671 4.890665  192.168.29.231  192.168.29.1    DNS       85 Standard query 0xe89b AAAA sam308.pythonanywhere.com
 672 4.890772  192.168.29.231  192.168.29.1    DNS       79 Standard query 0xf36f A use.fontawesome.com
 673 4.890873  192.168.29.231  192.168.29.1    DNS       79 Standard query 0x72e8 AAAA use.fontawesome.com
 674 4.900873  192.168.29.231  192.168.29.1    DNS       83 Standard query 0x563d A safebrowsing.google.com
 675 4.900983  192.168.29.231  192.168.29.1    DNS       83 Standard query 0x5d8a AAAA safebrowsing.google.com
 676 4.902965  192.168.29.1    192.168.29.231  DNS       96 Standard query response 0x0036 A fonts.googleapis.com A 216.58.197.42
 677 4.903317  192.168.29.1    192.168.29.231  DNS      108 Standard query response 0x3b78 AAAA fonts.googleapis.com AAAA 2404:6800:4002:812::200a
 678 4.903625  192.168.29.1    192.168.29.231  DNS      130 Standard query response 0x72e8 AAAA use.fontawesome.com CNAME fontawesome-cdn.fonticons.netdna-cdn.com
 679 4.903800  192.168.29.231  192.168.29.1    DNS      100 Standard query 0xd8b7 AAAA fontawesome-cdn.fonticons.netdna-cdn.com
 681 4.904342  192.168.29.1    192.168.29.231  DNS      146 Standard query response 0xf36f A use.fontawesome.com CNAME fontawesome-cdn.fonticons.netdna-cdn.com A 23.111.9.35
 682 4.906721  192.168.29.1    192.168.29.231  DNS      100 Standard query response 0xd8b7 AAAA fontawesome-cdn.fonticons.netdna-cdn.com
 684 4.909621  192.168.29.1    192.168.29.231  DNS      118 Standard query response 0x563d A safebrowsing.google.com CNAME sb.l.google.com A 172.217.161.14
 685 4.912556  192.168.29.1    192.168.29.231  DNS      130 Standard query response 0x5d8a AAAA safebrowsing.google.com CNAME sb.l.google.com AAAA 2404:6800:4007:806::200e
```

```
▸ Frame 1: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface wlo1, id 0
▾ Ethernet II, Src: IntelCor_9b:ff:fa (24:ee:9a:9b:ff:fa), Dst: Sercomm_02:6a:5b (14:ae:85:e2:6a:5b)
  ▾ Destination: Sercomm_02:6a:5b (14:ae:85:e2:6a:5b)
      Address: Sercomm_02:6a:5b (14:ae:85:e2:6a:5b)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: IntelCor_9b:ff:fa (24:ee:9a:9b:ff:fa)
      Address: IntelCor_9b:ff:fa (24:ee:9a:9b:ff:fa)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 192.168.29.231, Dst: 192.168.29.1
▸ User Datagram Protocol, Src Port: 32909, Dst Port: 53
▸ Domain Name System (query)
```

```
0000  14 ae 85 e2 6a 5b 24 ee  9a 9b ff fa 08 00 45 00   ····j[$· ······E·
0010  00 3d 33 93 40 00 40 11  4a e4 c0 a8 1d e7 c0 a8   ·=3·@·@· J·······
0020  1d 01 80 8d 00 35 00 29  bc 73 9c 50 01 00 00 01   ·····5·) ·s·P····
0030  00 00 00 00 00 00 04 70  6c 61 79 06 67 6f 6f 67   ·······p lay·goog
0040  6c 65 03 63 6f 6d 00 00  01 00 01                  le·com·· ···
```

Specifies if this is an individual (unicast) or group (broadcast/multicast) address (eth.dst.ig), 3 bytes    Packets: 911 · Displayed: 58 (6.4%) · Dropped: 0 (0.0%)    Profile: Default

## ARP:


Wireshark
14.58 °C
Dec 19 9:51 PM
100 %
*wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

```
No.   Time     Source             Destination        Protocol Length Info
  709 5.015322 Sercomm_02:6a:5b   IntelCor_9b:ff:fa  ARP        42 Who has 192.168.29.231? Tell 192.168.29.1
  710 5.015345 IntelCor_9b:ff:fa  Sercomm_02:6a:5b   ARP        42 192.168.29.231 is at 24:ee:9a:9b:ff:fa
  823 9.539749 IntelCor_9b:ff:fa  1e:f8:73:c8:56:67  ARP        42 Who has 192.168.29.48? Tell 192.168.29.231
  865 9.870369 1e:f8:73:c8:56:67  IntelCor_9b:ff:fa  ARP        42 192.168.29.48 is at 1e:f8:73:c8:56:67
```

```
▸ Frame 709: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface wlo1, id 0
▾ Ethernet II, Src: Sercomm_02:6a:5b (14:ae:85:e2:6a:5b), Dst: IntelCor_9b:ff:fa (24:ee:9a:9b:ff:fa)
  ▾ Destination: IntelCor_9b:ff:fa (24:ee:9a:9b:ff:fa)
      Address: IntelCor_9b:ff:fa (24:ee:9a:9b:ff:fa)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: Sercomm_02:6a:5b (14:ae:85:e2:6a:5b)
      Address: Sercomm_02:6a:5b (14:ae:85:e2:6a:5b)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
▸ Address Resolution Protocol (request)
```

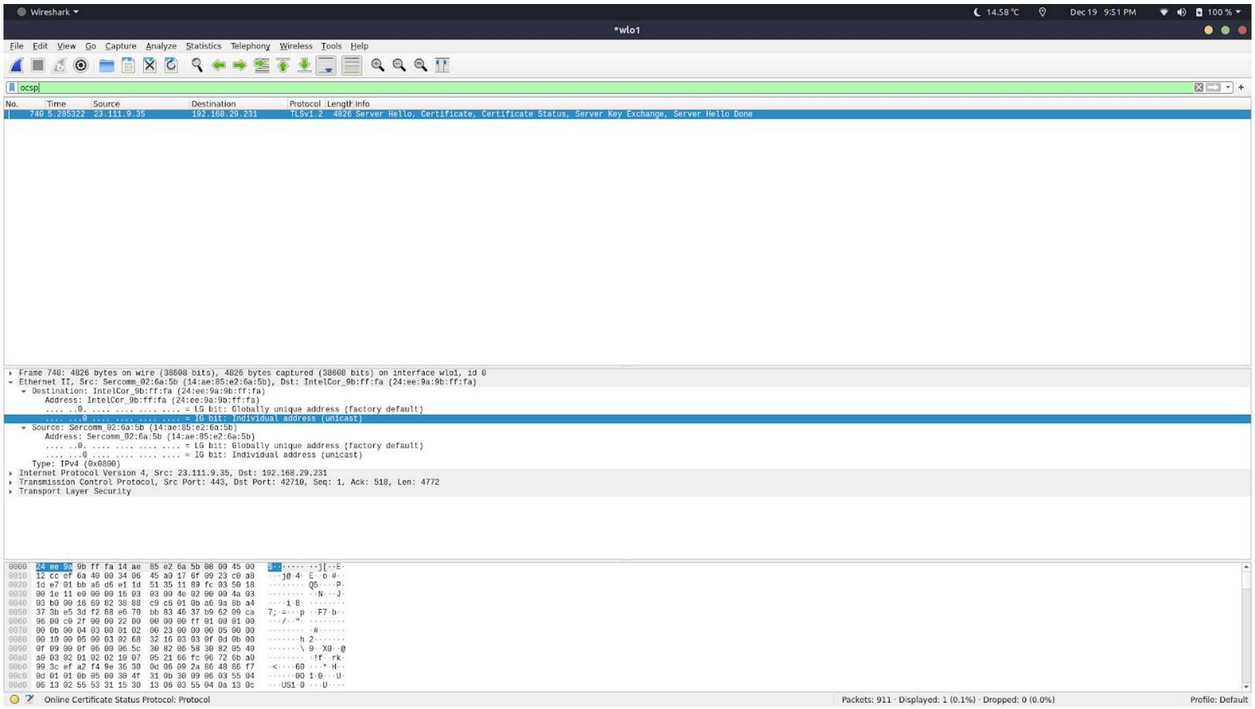
```
0000  24 ee 9a 9b ff fa 14 ae  85 e2 6a 5b 08 06 00 01   $······ ··j[····
0010  08 00 06 04 00 01 14 ae  85 e2 6a 5b c0 a8 1d 01   ········ ··j[····
0020  00 00 00 00 00 00 c0 a8  1d e7                     ········ ··
```

Address Resolution Protocol: Protocol

Packets: 911 · Displayed: 4 (0.4%) · Dropped: 0 (0.0%)

Profile: Default

## OCSP:


Wireshark
14.58 °C
Dec 19 9:51 PM
100 %
*wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ocsp

```
No.   Time     Source       Destination     Protocol Length Info
  740 5.285322 23.111.9.35  192.168.29.231  TLSv1.2  4826 Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
```

```
▸ Frame 740: 4826 bytes on wire (38608 bits), 4826 bytes captured (38608 bits) on interface wlo1, id 0
▾ Ethernet II, Src: Sercomm_02:6a:5b (14:ae:85:e2:6a:5b), Dst: IntelCor_9b:ff:fa (24:ee:9a:9b:ff:fa)
  ▾ Destination: IntelCor_9b:ff:fa (24:ee:9a:9b:ff:fa)
      Address: IntelCor_9b:ff:fa (24:ee:9a:9b:ff:fa)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: Sercomm_02:6a:5b (14:ae:85:e2:6a:5b)
      Address: Sercomm_02:6a:5b (14:ae:85:e2:6a:5b)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 23.111.9.35, Dst: 192.168.29.231
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 42710, Seq: 1, Ack: 518, Len: 4772
▸ Transport Layer Security
```

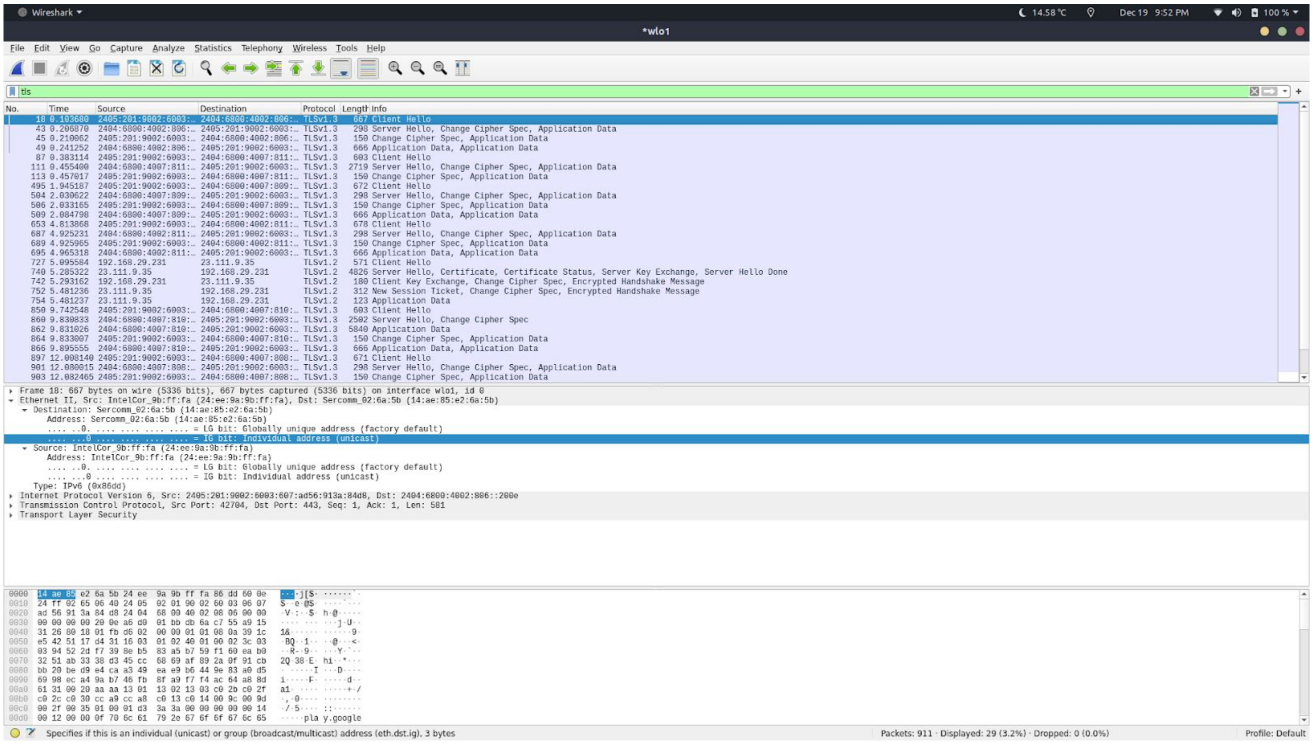
```
0000  24 ee 9a 9b ff fa 14 ae  85 e2 6a 5b 08 00 45 00   $······ ··j[··E·
0010  12 cc ef 6a 40 00 34 06  45 a0 17 6f 09 23 c0 a8   ···j@·4· E··o·#··
0020  1d e7 01 bb a6 d6 e1 1d  51 35 11 89 fc 03 50 18   ········ Q5····P·
0030  00 1e 11 e0 00 00 16 03  03 00 4e 02 00 00 4a 03   ········ ··N···J·
0040  03 b0 00 16 69 82 38 88  c9 c6 01 0b a6 9a 8b a4   ····i·8· ········
0050  37 3b e5 3d f2 88 e6 70  bb 83 46 37 b9 62 09 ca   7;·=···p ··F7·b··
0060  96 00 c0 2f 00 00 22 00  00 00 00 ff 01 00 01 00   ···/··"· ········
0070  00 0b 00 04 03 00 01 02  00 23 00 00 00 05 00 00   ········ ·#······
0080  00 10 00 05 00 03 02 68  32 16 03 03 0f 0d 0b 00   ·······h 2·······
0090  0f 09 00 0f 06 00 06 5c  30 82 06 58 30 82 05 40   ·······\ 0··X0··@
00a0  a0 03 02 01 02 02 10 07  05 21 66 fc 96 72 6b a0   ········ ·!f··rk·
00b0  99 3c ef a2 f4 9e 36 30  0d 06 09 2a 86 48 86 f7   ·<····60 ···*·H··
00c0  0d 01 01 0b 05 00 30 4f  31 0b 30 09 06 03 55 04   ······0O 1·0···U·
00d0  06 13 02 55 53 31 15 30  13 06 03 55 04 0a 13 0c   ···US1·0 ···U····
```

Online Certificate Status Protocol: Protocol

Packets: 911 · Displayed: 1 (0.1%) · Dropped: 0 (0.0%)

Profile: Default

## TLS:


Wireshark
14.58 °C
Dec 19 9:52 PM
100 %
*wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tls
```

```
No.  Time       Source               Destination          Protocol Length Info
  18 0.103680  2405:201:9002:6003:… 2404:6800:4002:806:… TLSv1.3   667 Client Hello
  43 0.206870  2404:6800:4002:806:… 2405:201:9002:6003:… TLSv1.3   298 Server Hello, Change Cipher Spec, Application Data
  45 0.210062  2405:201:9002:6003:… 2404:6800:4002:806:… TLSv1.3   150 Change Cipher Spec, Application Data
  49 0.241252  2404:6800:4002:806:… 2405:201:9002:6003:… TLSv1.3   666 Application Data, Application Data
  87 0.383114  2405:201:9002:6003:… 2404:6800:4007:811:… TLSv1.3   603 Client Hello
 111 0.455400  2404:6800:4007:811:… 2405:201:9002:6003:… TLSv1.3  2719 Server Hello, Change Cipher Spec, Application Data
 113 0.457017  2405:201:9002:6003:… 2404:6800:4007:811:… TLSv1.3   150 Change Cipher Spec, Application Data
 495 1.945187  2405:201:9002:6003:… 2404:6800:4007:809:… TLSv1.3   672 Client Hello
 504 2.030622  2404:6800:4007:809:… 2405:201:9002:6003:… TLSv1.3   298 Server Hello, Change Cipher Spec, Application Data
 506 2.033165  2405:201:9002:6003:… 2404:6800:4007:809:… TLSv1.3   150 Change Cipher Spec, Application Data
 509 2.084798  2404:6800:4007:809:… 2405:201:9002:6003:… TLSv1.3   666 Application Data, Application Data
 653 4.813868  2405:201:9002:6003:… 2404:6800:4002:811:… TLSv1.3   678 Client Hello
 687 4.925231  2404:6800:4002:811:… 2405:201:9002:6003:… TLSv1.3   298 Server Hello, Change Cipher Spec, Application Data
 689 4.925965  2405:201:9002:6003:… 2404:6800:4002:811:… TLSv1.3   150 Change Cipher Spec, Application Data
 695 4.965318  2404:6800:4002:811:… 2405:201:9002:6003:… TLSv1.3   666 Application Data, Application Data
 727 5.095584  192.168.29.231       23.111.9.35          TLSv1.2   571 Client Hello
 740 5.285322  23.111.9.35          192.168.29.231       TLSv1.2  4826 Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
 742 5.293162  192.168.29.231       23.111.9.35          TLSv1.2   180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
 752 5.481236  23.111.9.35          192.168.29.231       TLSv1.2   312 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
 754 5.481237  23.111.9.35          192.168.29.231       TLSv1.2   123 Application Data
 850 9.742548  2405:201:9002:6003:… 2404:6800:4007:810:… TLSv1.3   603 Client Hello
 860 9.830833  2404:6800:4007:810:… 2405:201:9002:6003:… TLSv1.3  2502 Server Hello, Change Cipher Spec
 862 9.831026  2404:6800:4007:810:… 2405:201:9002:6003:… TLSv1.3  5840 Application Data
 864 9.833007  2405:201:9002:6003:… 2404:6800:4007:810:… TLSv1.3   150 Change Cipher Spec, Application Data
 866 9.895555  2404:6800:4007:810:… 2405:201:9002:6003:… TLSv1.3   666 Application Data, Application Data
 897 12.008140 2405:201:9002:6003:… 2404:6800:4007:808:… TLSv1.3   671 Client Hello
 901 12.080015 2404:6800:4007:808:… 2405:201:9002:6003:… TLSv1.3   298 Server Hello, Change Cipher Spec, Application Data
 903 12.082465 2405:201:9002:6003:… 2404:6800:4007:808:… TLSv1.3   150 Change Cipher Spec, Application Data
```

```
▸ Frame 18: 667 bytes on wire (5336 bits), 667 bytes captured (5336 bits) on interface wlo1, id 0
▾ Ethernet II, Src: IntelCor_9b:ff:fa (24:ee:9a:9b:ff:fa), Dst: Sercomm_02:6a:5b (14:ae:85:e2:6a:5b)
  ▾ Destination: Sercomm_02:6a:5b (14:ae:85:e2:6a:5b)
      Address: Sercomm_02:6a:5b (14:ae:85:e2:6a:5b)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: IntelCor_9b:ff:fa (24:ee:9a:9b:ff:fa)
      Address: IntelCor_9b:ff:fa (24:ee:9a:9b:ff:fa)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv6 (0x86dd)
▸ Internet Protocol Version 6, Src: 2405:201:9002:6003:607:ad56:913a:84d8, Dst: 2404:6800:4002:806::200e
▸ Transmission Control Protocol, Src Port: 42704, Dst Port: 443, Seq: 1, Ack: 1, Len: 581
▸ Transport Layer Security
```

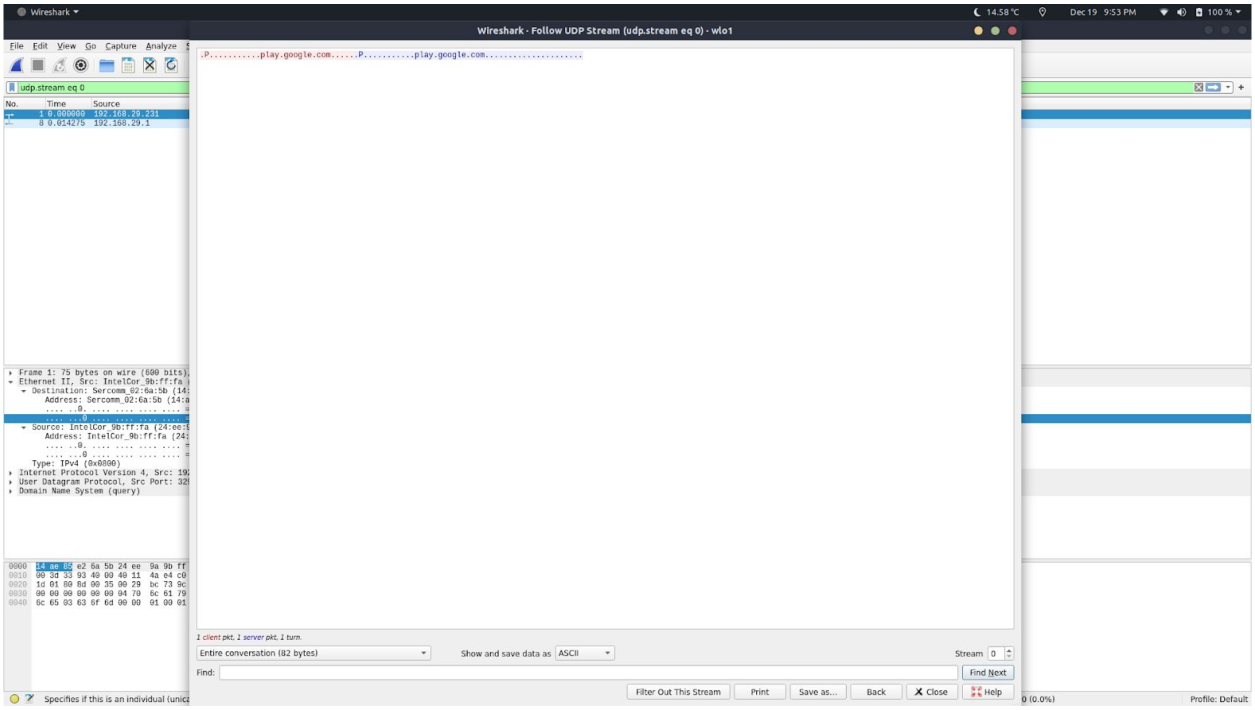
```
0000  14 ae 85 e2 6a 5b 24 ee  9a 9b ff fa 86 dd 60 0e   ····j[$· ······`·
0010  24 ff 02 65 06 40 24 05  02 01 90 02 60 03 06 07   $··e·@$· ····`···
0020  ad 56 91 3a 84 d8 24 04  68 00 40 02 08 06 00 00   ·V·:··$· h·@·····
0030  00 00 00 00 20 0e a6 d0  01 bb db 6a c7 55 a9 15   ···· ··· ···j·U··
0040  31 26 80 18 01 fb d6 02  00 00 01 01 08 0a 39 1c   1&······ ······9·
0050  e5 42 51 17 d4 31 16 03  01 02 40 01 00 02 3c 03   ·BQ··1·· ··@···<·
0060  03 94 52 2d f7 39 8e b5  83 a5 b7 59 f1 60 ea b0   ··R-·9·· ···Y·`··
0070  32 51 ab 33 38 d3 45 cc  68 69 af 89 2a 0f 91 cb   2Q·38·E· hi··*···
0080  bb 20 be d9 e4 ca a3 49  ea e9 b6 44 9e 83 a0 d5   · ·····I ···D····
0090  69 98 ec a4 9a b7 46 fb  8f a9 f7 f4 ac 64 a8 8d   i·····F· ·····d··
00a0  61 31 00 20 aa aa 13 01  13 02 13 03 c0 2b c0 2f   a1· ···· ·····+·/
00b0  c0 2c c0 30 cc a9 cc a8  c0 13 c0 14 00 9c 00 9d   ·,·0···· ········
00c0  00 2f 00 35 01 00 01 d3  3a 3a 00 00 00 00 00 14   ·/·5···· ::······
00d0  00 12 00 00 0f 70 6c 61  79 2e 67 6f 6f 67 6c 65   ·····pla y.google
```

Specifies if this is an individual (unicast) or group (broadcast/multicast) address (eth.dst.ig), 3 bytes

Packets: 911 · Displayed: 29 (3.2%) · Dropped: 0 (0.0%)

Profile: Default

On selecting a packet of DNS protocol, and on selecting follow UDP Stream for this paket, the following result was obtained:



```
udp.stream eq 0
```

```
No.  Time      Source
   1 0.000000  192.168.29.231
   8 0.014275  192.168.29.1
```

```
.P..........play.google.com......P..........play.google.com....................
```

```
▸ Frame 1: 75 bytes on wire (600 bits),
▾ Ethernet II, Src: IntelCor_9b:ff:fa (
  ▾ Destination: Sercomm_02:6a:5b (14:
      Address: Sercomm_02:6a:5b (14:a
      .... ..0. .... .... .... .... =
      .... ...0 .... .... .... .... =
  ▾ Source: IntelCor_9b:ff:fa (24:ee:9
      Address: IntelCor_9b:ff:fa (24:
      .... ..0. .... .... .... .... =
      .... ...0 .... .... .... .... =
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 192
▸ User Datagram Protocol, Src Port: 329
▸ Domain Name System (query)
```

```
0000  14 ae 85 e2 6a 5b 24 ee  9a 9b ff
0010  00 3d 33 93 40 00 40 11  4a e4 c0
0020  1d 01 80 8d 00 35 00 29  bc 73 9c
0030  00 00 00 00 00 00 04 70  6c 61 79
0040  6c 65 03 63 6f 6d 00 00  01 00 01
```

*1 client pkt, 1 server pkt, 1 turn.*

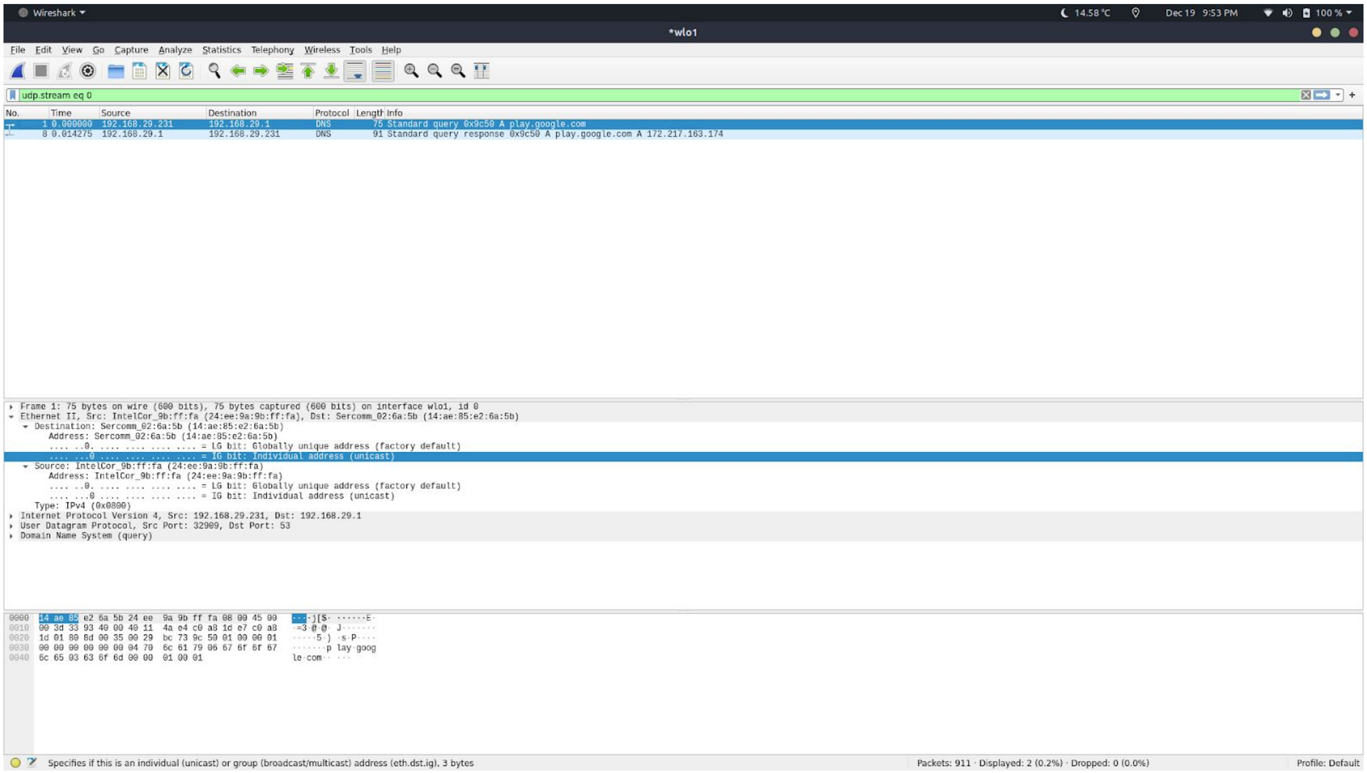
Entire conversation (82 bytes) — Show and save data as: ASCII — Stream: 0

Find:

Specifies if this is an individual (unica

0 (0.0%)

Profile: Default


Wireshark
14.58 °C
Dec 19 9:53 PM
100 %
*wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.stream eq 0

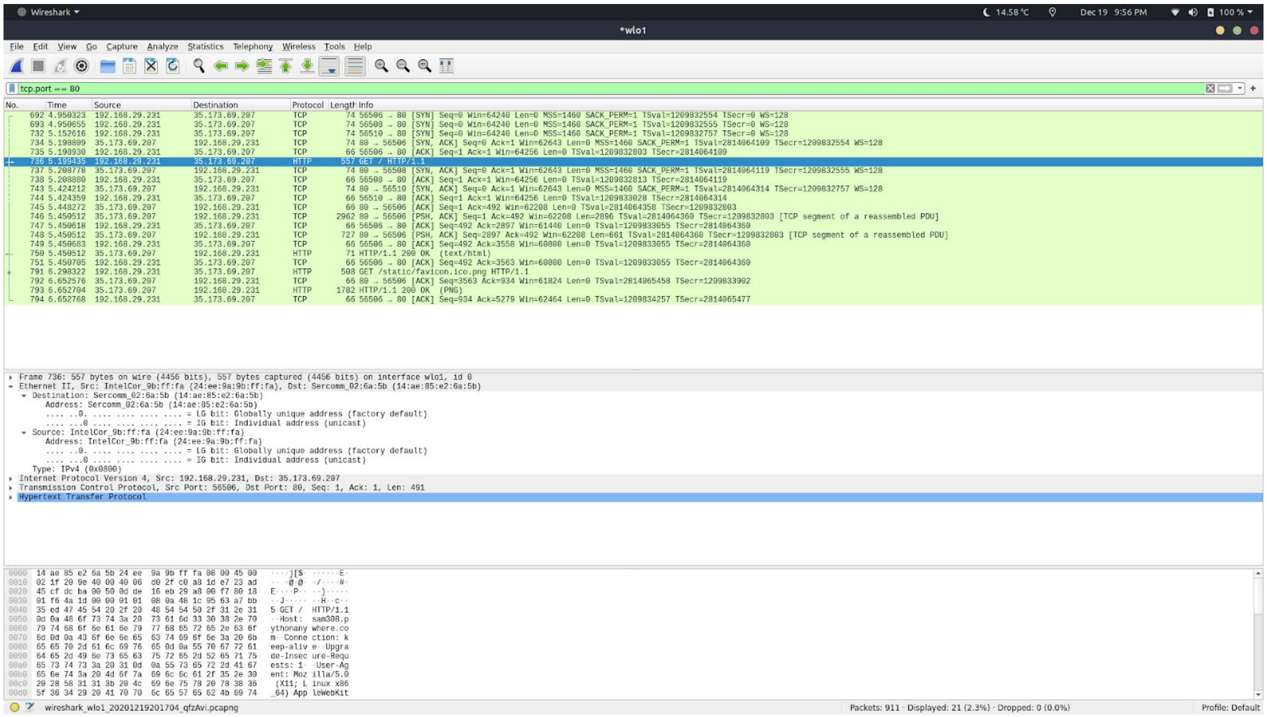
```
No.  Time      Source          Destination     Protocol Length Info
   1 0.000000  192.168.29.231  192.168.29.1    DNS      75 Standard query 0x9c50 A play.google.com
   8 0.014275  192.168.29.1    192.168.29.231  DNS      91 Standard query response 0x9c50 A play.google.com A 172.217.163.174
```

```
▸ Frame 1: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface wlo1, id 0
▾ Ethernet II, Src: IntelCor_9b:ff:fa (24:ee:9a:9b:ff:fa), Dst: Sercomm_02:6a:5b (14:ae:85:e2:6a:5b)
  ▾ Destination: Sercomm_02:6a:5b (14:ae:85:e2:6a:5b)
      Address: Sercomm_02:6a:5b (14:ae:85:e2:6a:5b)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: IntelCor_9b:ff:fa (24:ee:9a:9b:ff:fa)
      Address: IntelCor_9b:ff:fa (24:ee:9a:9b:ff:fa)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 192.168.29.231, Dst: 192.168.29.1
▸ User Datagram Protocol, Src Port: 32909, Dst Port: 53
▸ Domain Name System (query)
```

```
0000  14 ae 85 e2 6a 5b 24 ee  9a 9b ff fa 08 00 45 00   ····j[$· ······E·
0010  00 3d 33 93 40 00 40 11  4a e4 c0 a8 1d e7 c0 a8   ·=3·@·@· J·······
0020  1d 01 80 8d 00 35 00 29  bc 73 9c 50 01 00 00 01   ·····5·) ·s·P····
0030  00 00 00 00 00 00 04 70  6c 61 79 06 67 6f 6f 67   ·······p lay·goog
0040  6c 65 03 63 6f 6d 00 00  01 00 01                  le·com·· ···
```

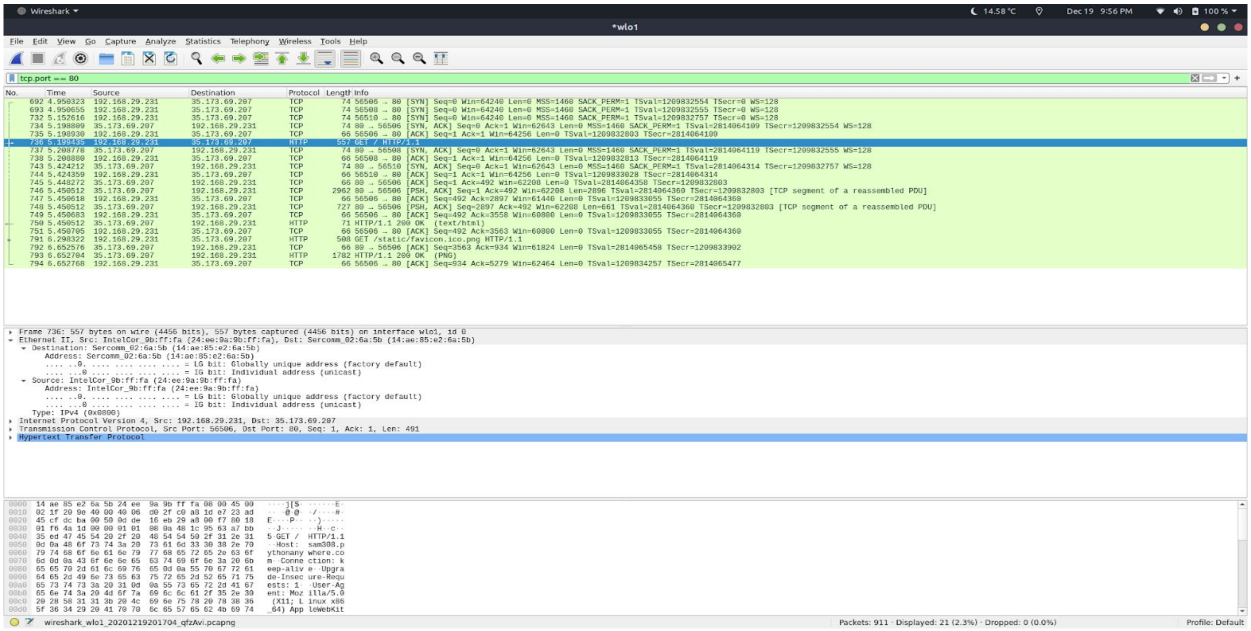
Specifies if this is an individual (unicast) or group (broadcast/multicast) address (eth.dst.ig), 3 bytes | Packets: 911 · Displayed: 2 (0.2%) · Dropped: 0 (0.0%) | Profile: Default

## Q6. 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.



```
tcp.port == 80

No.  Time     Source         Destination    Protocol Length Info
 692 4.950323 192.168.29.231 35.173.69.207  TCP        74 56506 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1209832554 TSecr=0 WS=128
 693 4.950655 192.168.29.231 35.173.69.207  TCP        74 56508 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1209832555 TSecr=0 WS=128
 732 5.152616 192.168.29.231 35.173.69.207  TCP        74 56510 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1209832757 TSecr=0 WS=128
 734 5.198809 35.173.69.207  192.168.29.231 TCP        74 80 → 56506 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=1460 SACK_PERM=1 TSval=2814064109 TSecr=1209832554 WS=128
 735 5.198930 192.168.29.231 35.173.69.207  TCP        66 56506 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1209832803 TSecr=2814064109
 736 5.199435 192.168.29.231 35.173.69.207  HTTP      557 GET / HTTP/1.1
 737 5.208778 35.173.69.207  192.168.29.231 TCP        74 80 → 56508 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=1460 SACK_PERM=1 TSval=2814064119 TSecr=1209832555 WS=128
 738 5.208880 192.168.29.231 35.173.69.207  TCP        66 56508 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1209832813 TSecr=2814064119
 743 5.424212 35.173.69.207  192.168.29.231 TCP        74 80 → 56510 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=1460 SACK_PERM=1 TSval=2814064314 TSecr=1209832757 WS=128
 744 5.424359 192.168.29.231 35.173.69.207  TCP        66 56510 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1209833028 TSecr=2814064314
 745 5.448272 35.173.69.207  192.168.29.231 TCP        66 80 → 56506 [ACK] Seq=1 Ack=492 Win=62208 Len=0 TSval=2814064358 TSecr=1209832803
 746 5.450512 35.173.69.207  192.168.29.231 TCP      2962 80 → 56506 [PSH, ACK] Seq=1 Ack=492 Win=62208 Len=2896 TSval=2814064360 TSecr=1209832803 [TCP segment of a reassembled PDU]
 747 5.450618 192.168.29.231 35.173.69.207  TCP        66 56506 → 80 [ACK] Seq=492 Ack=2897 Win=61440 Len=0 TSval=1209833055 TSecr=2814064360
 748 5.450512 35.173.69.207  192.168.29.231 TCP       727 80 → 56506 [PSH, ACK] Seq=2897 Ack=492 Win=62208 Len=661 TSval=2814064360 TSecr=1209832803 [TCP segment of a reassembled PDU]
 749 5.450683 192.168.29.231 35.173.69.207  TCP        66 56506 → 80 [ACK] Seq=492 Ack=3558 Win=60800 Len=0 TSval=1209833055 TSecr=2814064360
 750 5.450512 35.173.69.207  192.168.29.231 HTTP       71 HTTP/1.1 200 OK  (text/html)
 751 5.450705 192.168.29.231 35.173.69.207  TCP        66 56506 → 80 [ACK] Seq=492 Ack=3563 Win=60800 Len=0 TSval=1209833055 TSecr=2814064360
 791 6.298322 192.168.29.231 35.173.69.207  HTTP      508 GET /static/favicon.ico.png HTTP/1.1
 792 6.652576 35.173.69.207  192.168.29.231 TCP        66 80 → 56506 [ACK] Seq=3563 Ack=934 Win=61824 Len=0 TSval=2814065458 TSecr=1209833902
 793 6.652704 35.173.69.207  192.168.29.231 HTTP     1782 HTTP/1.1 200 OK  (PNG)
 794 6.652768 192.168.29.231 35.173.69.207  TCP        66 56506 → 80 [ACK] Seq=934 Ack=5279 Win=62464 Len=0 TSval=1209834257 TSecr=2814065477

▸ Frame 736: 557 bytes on wire (4456 bits), 557 bytes captured (4456 bits) on interface wlo1, id 0
▾ Ethernet II, Src: IntelCor_9b:ff:fa (24:ee:9a:9b:ff:fa), Dst: Sercomm_02:6a:5b (14:ae:85:e2:6a:5b)
  ▾ Destination: Sercomm_02:6a:5b (14:ae:85:e2:6a:5b)
      Address: Sercomm_02:6a:5b (14:ae:85:e2:6a:5b)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: IntelCor_9b:ff:fa (24:ee:9a:9b:ff:fa)
      Address: IntelCor_9b:ff:fa (24:ee:9a:9b:ff:fa)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 192.168.29.231, Dst: 35.173.69.207
▸ Transmission Control Protocol, Src Port: 56506, Dst Port: 80, Seq: 1, Ack: 1, Len: 491
▸ Hypertext Transfer Protocol

0000  14 ae 85 e2 6a 5b 24 ee  9a 9b ff fa 08 00 45 00   ····j[$· ······E·
0010  02 1f 20 9e 40 00 40 06  d0 2f c0 a8 1d e7 23 ad   ·· ·@·@· ·/····#·
0020  45 cf dc ba 00 50 0d de  16 eb 29 a8 00 f7 80 18   E····P·· ··)·····
0030  01 f6 4a 1d 00 00 01 01  08 0a 48 1c 95 63 a7 bb   ··J····· ··H··c··
0040  35 ed 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 31   5·GET /  HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20  73 61 6d 33 30 38 2e 70   ··Host:  sam308.p
0060  79 74 68 6f 6e 61 6e 79  77 68 65 72 65 2e 63 6f   ythonany where.co
0070  6d 0d 0a 43 6f 6e 6e 65  63 74 69 6f 6e 3a 20 6b   m··Conne ction: k
0080  65 65 70 2d 61 6c 69 76  65 0d 0a 55 70 67 72 61   eep-aliv e··Upgra
0090  64 65 2d 49 6e 73 65 63  75 72 65 2d 52 65 71 75   de-Insec ure-Requ
00a0  65 73 74 73 3a 20 31 0d  0a 55 73 65 72 2d 41 67   ests: 1· ·User-Ag
00b0  65 6e 74 3a 20 4d 6f 7a  69 6c 6c 61 2f 35 2e 30   ent: Moz illa/5.0
00c0  20 28 58 31 31 3b 20 4c  69 6e 75 78 20 78 38 36    (X11; L inux x86
00d0  5f 36 34 29 20 41 70 70  6c 65 57 65 62 4b 69 74   _64) App leWebKit

wireshark_wlo1_20201219201704_qfzAvi.pcapng   Packets: 911 · Displayed: 21 (2.3%) · Dropped: 0 (0.0%)   Profile: Default
```

On expanding Ethernet layer of the packet 736 in Packet Details Panel, the following result is obtained:



```
tcp.port == 80

No.  Time     Source         Destination    Protocol Length Info
 692 4.950323 192.168.29.231 35.173.69.207  TCP        74 56506 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1209832554 TSecr=0 WS=128
 693 4.950655 192.168.29.231 35.173.69.207  TCP        74 56508 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1209832555 TSecr=0 WS=128
 732 5.152616 192.168.29.231 35.173.69.207  TCP        74 56510 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1209832757 TSecr=0 WS=128
 734 5.198809 35.173.69.207  192.168.29.231 TCP        74 80 → 56506 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=1460 SACK_PERM=1 TSval=2814064109 TSecr=1209832554 WS=128
 735 5.198930 192.168.29.231 35.173.69.207  TCP        66 56506 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1209832803 TSecr=2814064109
 736 5.199435 192.168.29.231 35.173.69.207  HTTP      557 GET / HTTP/1.1
 737 5.208778 35.173.69.207  192.168.29.231 TCP        74 80 → 56508 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=1460 SACK_PERM=1 TSval=2814064119 TSecr=1209832555 WS=128
 738 5.208880 192.168.29.231 35.173.69.207  TCP        66 56508 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1209832813 TSecr=2814064119
 743 5.424212 35.173.69.207  192.168.29.231 TCP        74 80 → 56510 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=1460 SACK_PERM=1 TSval=2814064314 TSecr=1209832757 WS=128
 744 5.424359 192.168.29.231 35.173.69.207  TCP        66 56510 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1209833028 TSecr=2814064314
 745 5.448272 35.173.69.207  192.168.29.231 TCP        66 80 → 56506 [ACK] Seq=1 Ack=492 Win=62208 Len=0 TSval=2814064358 TSecr=1209832803
 746 5.450512 35.173.69.207  192.168.29.231 TCP      2962 80 → 56506 [PSH, ACK] Seq=1 Ack=492 Win=62208 Len=2896 TSval=2814064360 TSecr=1209832803 [TCP segment of a reassembled PDU]
 747 5.450618 192.168.29.231 35.173.69.207  TCP        66 56506 → 80 [ACK] Seq=492 Ack=2897 Win=61440 Len=0 TSval=1209833055 TSecr=2814064360
 748 5.450512 35.173.69.207  192.168.29.231 TCP       727 80 → 56506 [PSH, ACK] Seq=2897 Ack=492 Win=62208 Len=661 TSval=2814064360 TSecr=1209832803 [TCP segment of a reassembled PDU]
 749 5.450683 192.168.29.231 35.173.69.207  TCP        66 56506 → 80 [ACK] Seq=492 Ack=3558 Win=60800 Len=0 TSval=1209833055 TSecr=2814064360
 750 5.450512 35.173.69.207  192.168.29.231 HTTP       71 HTTP/1.1 200 OK  (text/html)
 751 5.450705 192.168.29.231 35.173.69.207  TCP        66 56506 → 80 [ACK] Seq=492 Ack=3563 Win=60800 Len=0 TSval=1209833055 TSecr=2814064360
 791 6.298322 192.168.29.231 35.173.69.207  HTTP      508 GET /static/favicon.ico.png HTTP/1.1
 792 6.652576 35.173.69.207  192.168.29.231 TCP        66 80 → 56506 [ACK] Seq=3563 Ack=934 Win=61824 Len=0 TSval=2814065458 TSecr=1209833902
 793 6.652704 35.173.69.207  192.168.29.231 HTTP     1782 HTTP/1.1 200 OK  (PNG)
 794 6.652768 192.168.29.231 35.173.69.207  TCP        66 56506 → 80 [ACK] Seq=934 Ack=5279 Win=62464 Len=0 TSval=1209834257 TSecr=2814065477

▸ Frame 736: 557 bytes on wire (4456 bits), 557 bytes captured (4456 bits) on interface wlo1, id 0
▾ Ethernet II, Src: IntelCor_9b:ff:fa (24:ee:9a:9b:ff:fa), Dst: Sercomm_02:6a:5b (14:ae:85:e2:6a:5b)
  ▾ Destination: Sercomm_02:6a:5b (14:ae:85:e2:6a:5b)
      Address: Sercomm_02:6a:5b (14:ae:85:e2:6a:5b)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: IntelCor_9b:ff:fa (24:ee:9a:9b:ff:fa)
      Address: IntelCor_9b:ff:fa (24:ee:9a:9b:ff:fa)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 192.168.29.231, Dst: 35.173.69.207
▸ Transmission Control Protocol, Src Port: 56506, Dst Port: 80, Seq: 1, Ack: 1, Len: 491
▸ Hypertext Transfer Protocol

0000  14 ae 85 e2 6a 5b 24 ee  9a 9b ff fa 08 00 45 00   ····j[$· ······E·
0010  02 1f 20 9e 40 00 40 06  d0 2f c0 a8 1d e7 23 ad   ·· ·@·@· ·/····#·
0020  45 cf dc ba 00 50 0d de  16 eb 29 a8 00 f7 80 18   E····P·· ··)·····
0030  01 f6 4a 1d 00 00 01 01  08 0a 48 1c 95 63 a7 bb   ··J····· ··H··c··
0040  35 ed 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 31   5·GET /  HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20  73 61 6d 33 30 38 2e 70   ··Host:  sam308.p
0060  79 74 68 6f 6e 61 6e 79  77 68 65 72 65 2e 63 6f   ythonany where.co
0070  6d 0d 0a 43 6f 6e 6e 65  63 74 69 6f 6e 3a 20 6b   m··Conne ction: k
0080  65 65 70 2d 61 6c 69 76  65 0d 0a 55 70 67 72 61   eep-aliv e··Upgra
0090  64 65 2d 49 6e 73 65 63  75 72 65 2d 52 65 71 75   de-Insec ure-Requ
00a0  65 73 74 73 3a 20 31 0d  0a 55 73 65 72 2d 41 67   ests: 1· ·User-Ag
00b0  65 6e 74 3a 20 4d 6f 7a  69 6c 6c 61 2f 35 2e 30   ent: Moz illa/5.0
00c0  20 28 58 31 31 3b 20 4c  69 6e 75 78 20 78 38 36    (X11; L inux x86
00d0  5f 36 34 29 20 41 70 70  6c 65 57 65 62 4b 69 74   _64) App leWebKit

wireshark_wlo1_20201219201704_qfzAvi.pcapng   Packets: 911 · Displayed: 21 (2.3%) · Dropped: 0 (0.0%)   Profile: Default
```

### Q7. What are the manufacturers of your PC’s Network Interface Card (NIC), and the servers NIC?

Manufacturer of my Laptop’s Network Interface Card (NIC) is:

**IntelCor_9b:ff:fa (24:ee:9a:9b:ff:fa)**

Manufacturer of the server’s Network Interface Card (NIC) is:

**Sercomm_02:6a:5b (14:ae:85:e2:6a:5b)**

### Q8. What are the Hex values (shown the raw bytes panel) of the two NICs Manufacturers OUIs?

For my Laptop’s manufacturer: **24:ee:9a:9b:ff:fa**

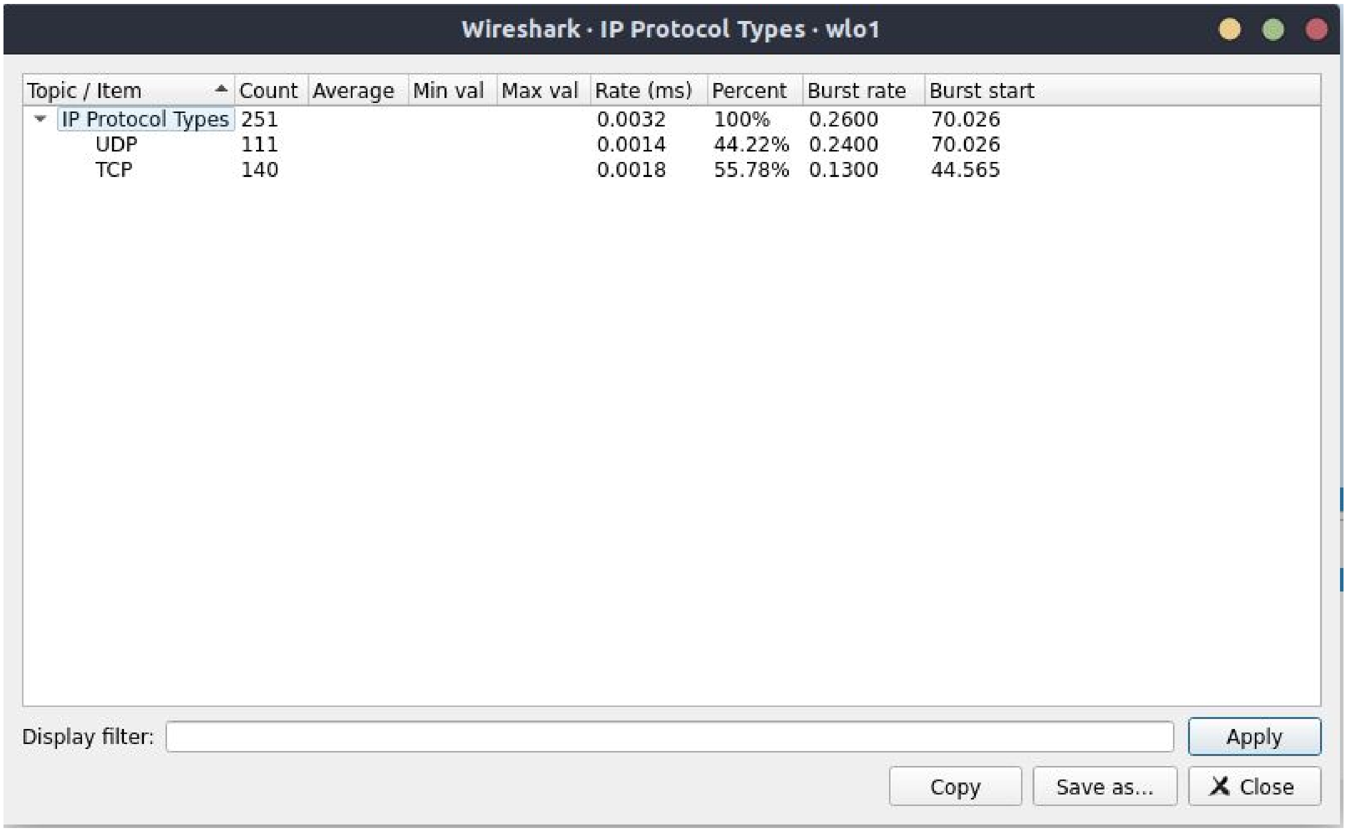
For server’s manufacturer: **14:ae:85:e2:6a:5b**

**Q9. 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?**

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

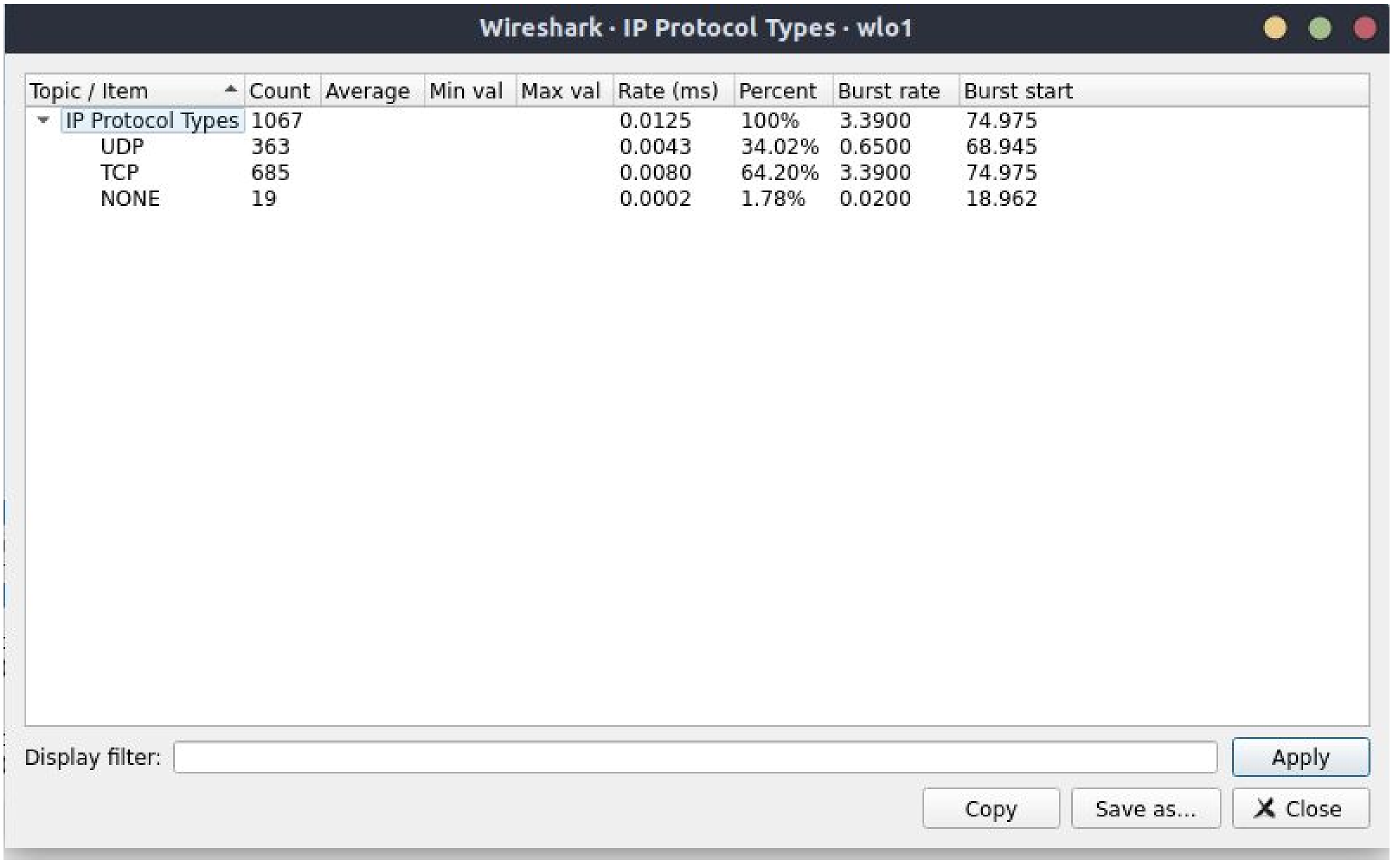
The IPv4 statistics of the packet capture:



Wireshark · IP Protocol Types · wlo1

| Topic / Item | Count | Average | Min val | Max val | Rate (ms) | Percent | Burst rate | Burst start |
|---|---|---|---|---|---|---|---|---|
| IP Protocol Types | 251 | | | | 0.0032 | 100% | 0.2600 | 70.026 |
| UDP | 111 | | | | 0.0014 | 44.22% | 0.2400 | 70.026 |
| TCP | 140 | | | | 0.0018 | 55.78% | 0.1300 | 44.565 |

The IPv6 statistics of the packet capture:



| Topic / Item | Count | Average | Min val | Max val | Rate (ms) | Percent | Burst rate | Burst start |
|---|---|---|---|---|---|---|---|---|
| IP Protocol Types | 1067 | | | | 0.0125 | 100% | 3.3900 | 74.975 |
| UDP | 363 | | | | 0.0043 | 34.02% | 0.6500 | 68.945 |
| TCP | 685 | | | | 0.0080 | 64.20% | 3.3900 | 74.975 |
| NONE | 19 | | | | 0.0002 | 1.78% | 0.0200 | 18.962 |

Higher level protocols which use **TCP**:

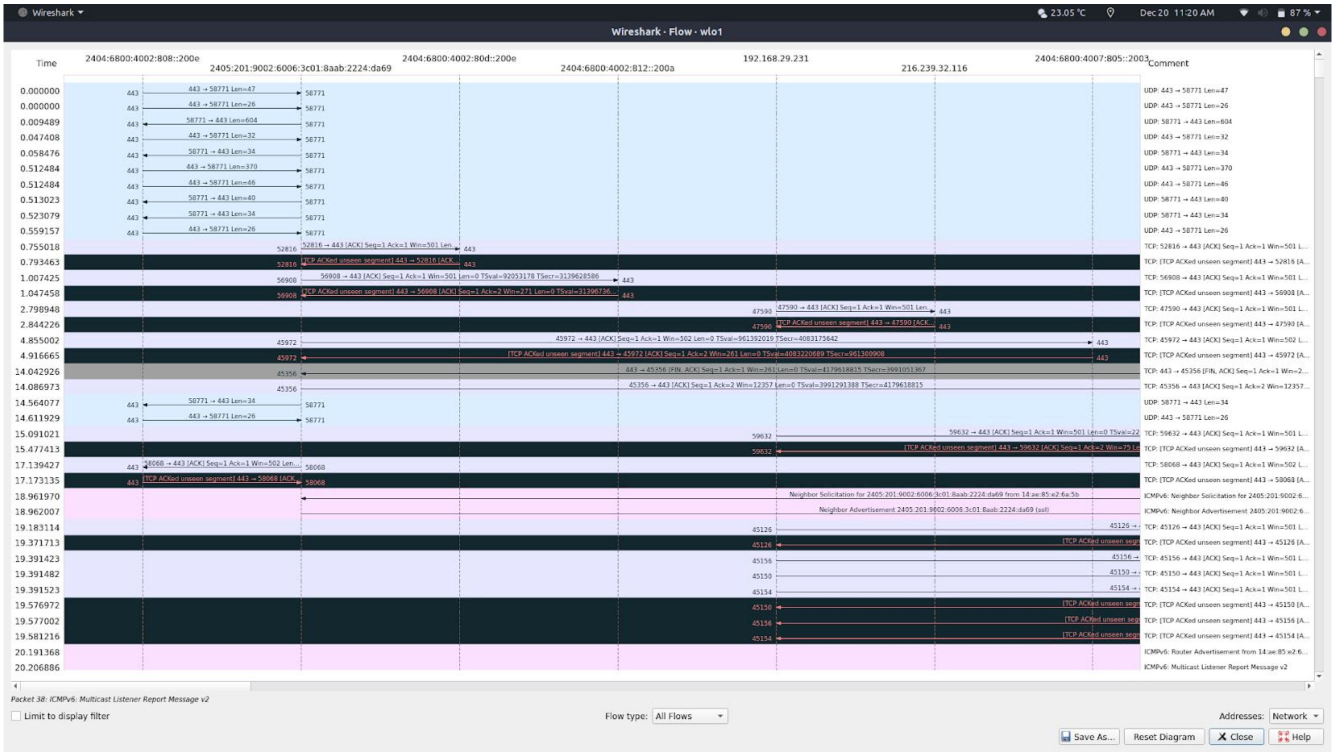
1. **HTTPS** - HyperText Transfer Protocol Secure
2. **FTP** - File Transfer Protocol

Higher level protocols which use **UDP**:

1. **SNMP** - Simple Network Management Protocol
2. **RIP** - Routing Information Protocol

## Q10. 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 for General flow and network source:



```
Time        Comment
0.000000    UDP: 443 → 58771 Len=47
0.000000    UDP: 443 → 58771 Len=26
0.009489    UDP: 58771 → 443 Len=604
0.047408    UDP: 443 → 58771 Len=32
0.058476    UDP: 58771 → 443 Len=34
0.512484    UDP: 443 → 58771 Len=370
0.512484    UDP: 443 → 58771 Len=46
0.513023    UDP: 58771 → 443 Len=40
0.523079    UDP: 58771 → 443 Len=34
0.559157    UDP: 443 → 58771 Len=26
0.755018    TCP: 52816 → 443 [ACK] Seq=1 Ack=1 Win=501 L...
0.793463    TCP: [TCP ACKed unseen segment] 443 → 52816 [A...
1.007425    TCP: 56908 → 443 [ACK] Seq=1 Ack=1 Win=501 L...
1.047458    TCP: [TCP ACKed unseen segment] 443 → 56908 [A...
2.798948    TCP: 47590 → 443 [ACK] Seq=1 Ack=1 Win=501 L...
2.844226    TCP: [TCP ACKed unseen segment] 443 → 47590 [A...
4.855002    TCP: 45972 → 443 [ACK] Seq=1 Ack=1 Win=502 L...
4.916665    TCP: [TCP ACKed unseen segment] 443 → 45972 [A...
14.042926   TCP: 443 → 45356 [FIN, ACK] Seq=1 Ack=1 Win=2...
14.086973   TCP: 45356 → 443 [ACK] Seq=1 Ack=2 Win=12357...
14.564077   UDP: 58771 → 443 Len=34
14.611929   UDP: 443 → 58771 Len=26
15.091021   TCP: 59632 → 443 [ACK] Seq=1 Ack=1 Win=501 L...
15.477413   TCP: [TCP ACKed unseen segment] 443 → 59632 [A...
17.139427   TCP: 58068 → 443 [ACK] Seq=1 Ack=1 Win=502 L...
17.173135   TCP: [TCP ACKed unseen segment] 443 → 58068 [A...
18.961970   ICMPv6: Neighbor Solicitation for 2405:201:9002:6...
18.962007   ICMPv6: Neighbor Advertisement 2405:201:9002:6...
19.183114   TCP: 45126 → 443 [ACK] Seq=1 Ack=1 Win=501 L...
19.371713   TCP: [TCP ACKed unseen segment] 443 → 45126 [A...
19.391423   TCP: 45156 → 443 [ACK] Seq=1 Ack=1 Win=501 L...
19.391482   TCP: 45150 → 443 [ACK] Seq=1 Ack=1 Win=501 L...
19.391523   TCP: 45154 → 443 [ACK] Seq=1 Ack=1 Win=501 L...
19.576972   TCP: [TCP ACKed unseen segment] 443 → 45150 [A...
19.577002   TCP: [TCP ACKed unseen segment] 443 → 45156 [A...
19.581216   TCP: [TCP ACKed unseen segment] 443 → 45154 [A...
20.191368   ICMPv6: Router Advertisement from 14:ae:85:e2:6...
20.206886   ICMPv6: Multicast Listener Report Message v2
```

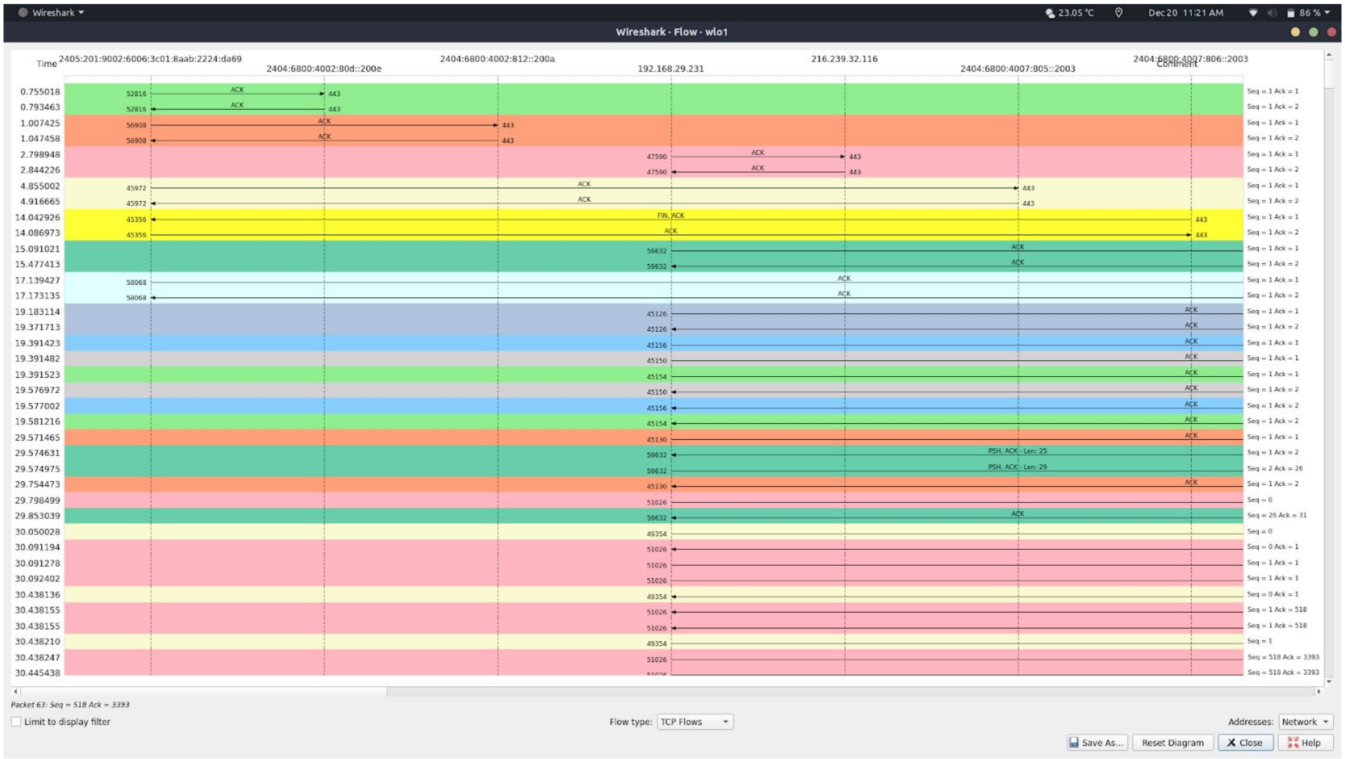
Packet 38: ICMPv6: Multicast Listener Report Message v2

☐ Limit to display filter

Flow type: All Flows

Addresses: Network

Graph obtained for TCP flow and network source:



| Time | | | | Comment |
|---|---|---|---|---|
| 0.755018 | 52816 | ACK | 443 | Seq = 1 Ack = 1 |
| 0.793463 | 52816 | ACK | 443 | Seq = 1 Ack = 2 |
| 1.007425 | 56908 | ACK | 443 | Seq = 1 Ack = 1 |
| 1.047458 | 56908 | ACK | 443 | Seq = 1 Ack = 2 |
| 2.798948 | 47590 | ACK | 443 | Seq = 1 Ack = 1 |
| 2.844226 | 47590 | ACK | 443 | Seq = 1 Ack = 2 |
| 4.855002 | 45972 | ACK | 443 | Seq = 1 Ack = 1 |
| 4.916665 | 45972 | ACK | 443 | Seq = 1 Ack = 2 |
| 14.042926 | 45356 | FIN, ACK | 443 | Seq = 1 Ack = 1 |
| 14.086973 | 45356 | ACK | 443 | Seq = 1 Ack = 2 |
| 15.091021 | 59632 | ACK | | Seq = 1 Ack = 1 |
| 15.477413 | 59632 | ACK | | Seq = 1 Ack = 2 |
| 17.139427 | 58068 | ACK | | Seq = 1 Ack = 1 |
| 17.173135 | 58068 | ACK | | Seq = 1 Ack = 2 |
| 19.183114 | 45126 | ACK | | Seq = 1 Ack = 1 |
| 19.371713 | 45126 | ACK | | Seq = 1 Ack = 2 |
| 19.391423 | 45156 | ACK | | Seq = 1 Ack = 1 |
| 19.391482 | 45150 | ACK | | Seq = 1 Ack = 1 |
| 19.391523 | 45154 | ACK | | Seq = 1 Ack = 1 |
| 19.576972 | 45150 | ACK | | Seq = 1 Ack = 2 |
| 19.577002 | 45156 | ACK | | Seq = 1 Ack = 2 |
| 19.581216 | 45154 | ACK | | Seq = 1 Ack = 2 |
| 29.571465 | 45130 | ACK | | Seq = 1 Ack = 1 |
| 29.574631 | 59632 | PSH, ACK - Len: 25 | | Seq = 1 Ack = 2 |
| 29.574975 | 59632 | PSH, ACK - Len: 29 | | Seq = 2 Ack = 26 |
| 29.754473 | 45130 | ACK | | Seq = 1 Ack = 2 |
| 29.798499 | 51026 | | | Seq = 0 |
| 29.853039 | 59632 | ACK | | Seq = 26 Ack = 31 |
| 30.050028 | 49354 | | | Seq = 0 |
| 30.091194 | 51026 | | | Seq = 0 Ack = 1 |
| 30.091278 | 51026 | | | Seq = 1 Ack = 1 |
| 30.092402 | 51026 | | | Seq = 1 Ack = 1 |
| 30.438136 | 49354 | | | Seq = 0 Ack = 1 |
| 30.438155 | 51026 | | | Seq = 1 Ack = 518 |
| 30.438155 | 51026 | | | Seq = 1 Ack = 518 |
| 30.438210 | 49354 | | | Seq = 1 |
| 30.438247 | 51026 | | | Seq = 518 Ack = 3393 |
| 30.445438 | 51026 | | | Seq = 518 Ack = 3393 |

*Packet 63: Seq = 518 Ack = 3393*

☐ Limit to display filter

Flow type: TCP Flows

Addresses: Network

## Comments:

This was a very interesting and unique assignment. It led me to learn using a new utility tool Wireshark. The packets were captured and analysed as per the requirements and helped me get a clear knowledge about how the protocols work in the real world.