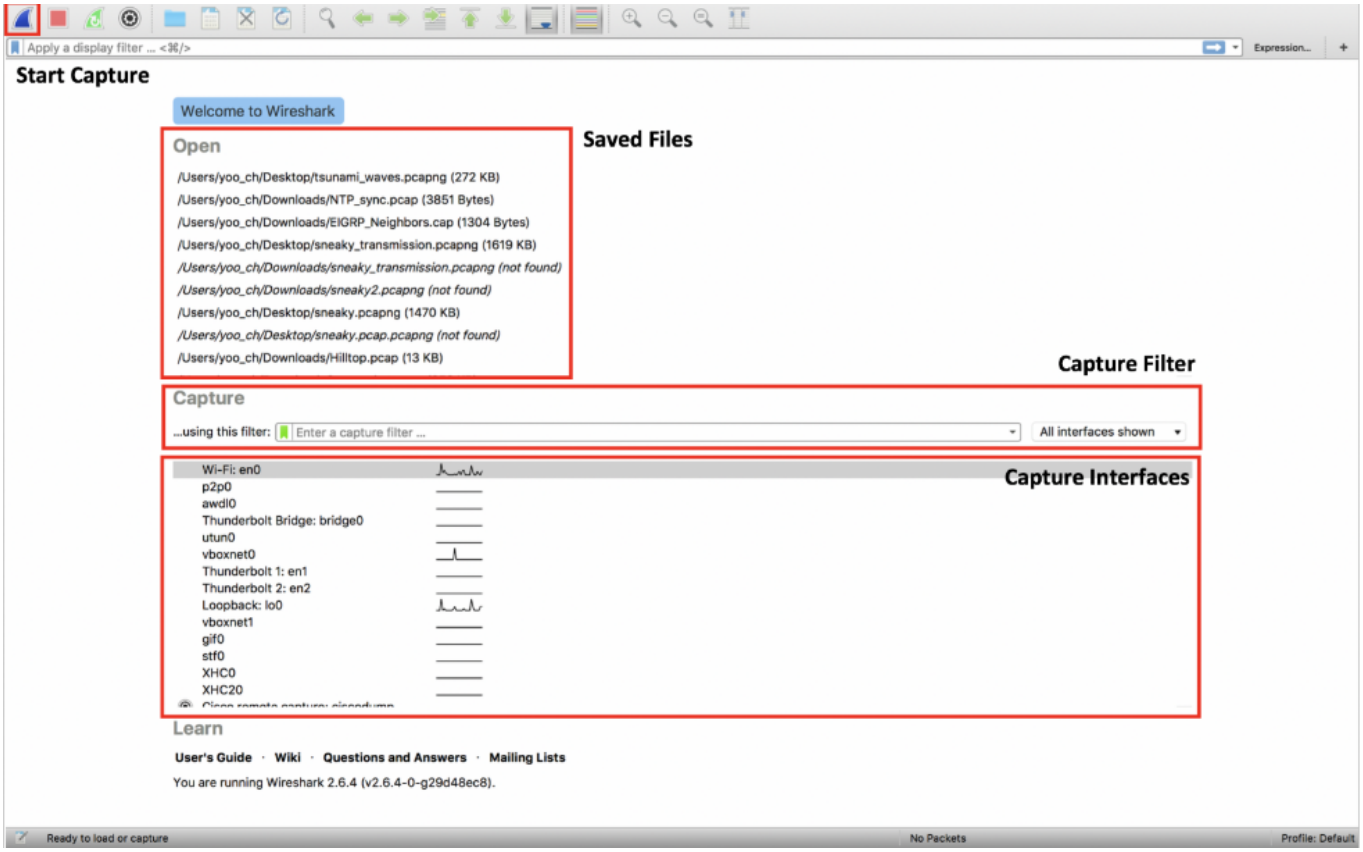
# Analysis with wireshark

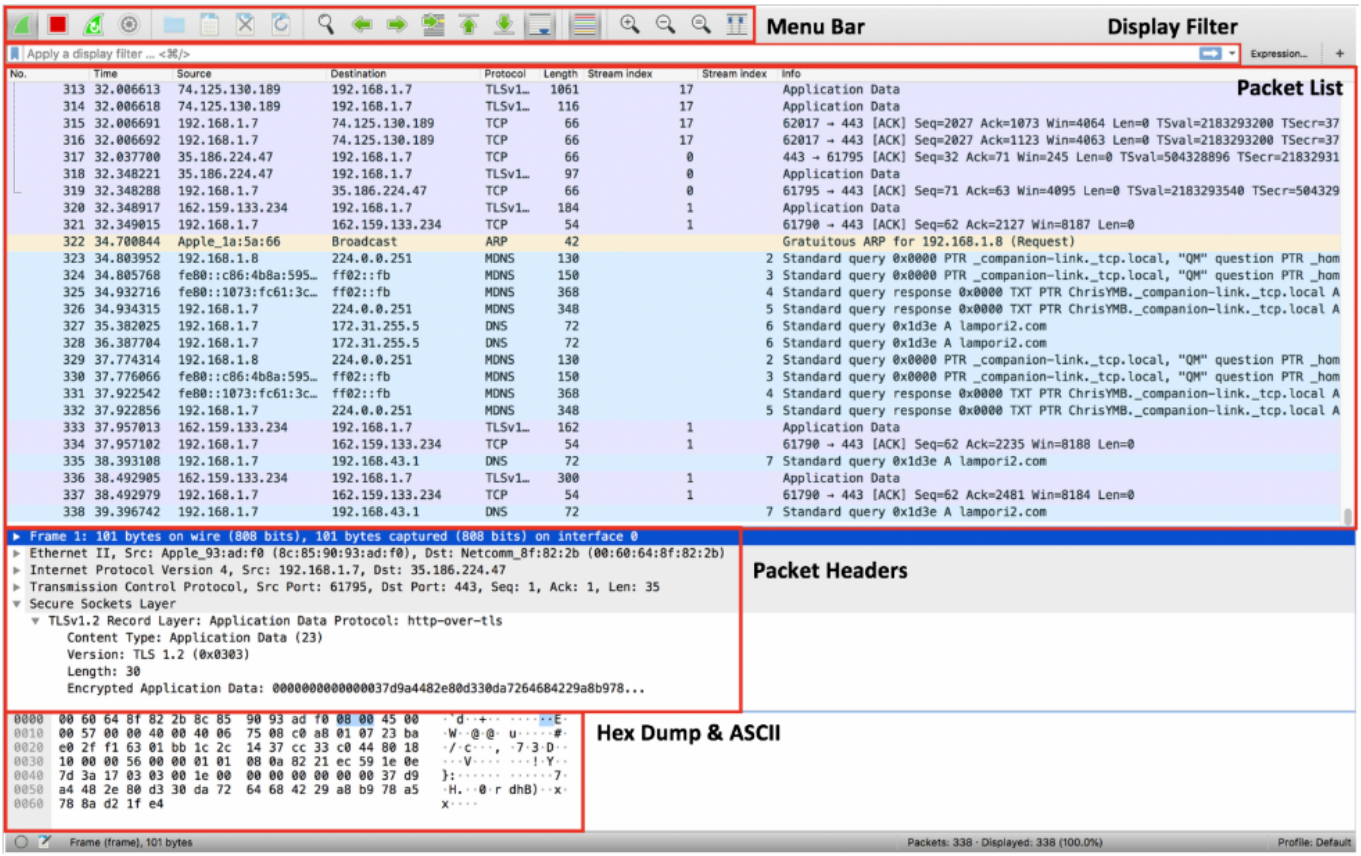
***Resumes done by Tr1h4rd3r***

Wireshark Startup Window:




```
1: Start Capture: The blue button in the top left corner start capturing inbound
and outbound packets.
2: Open saved files
3: Capture filter: You can write expressions in the capture filter to limite the
types of packets that wireshark captures.
4: Capture Interface Selection
```

Wireshark Main Window:




1: Menu bar: The menu bar local at the top of the window is used to manage the capture, in the left section you can start, stop and restart the capture, and manage capture interface settings.
2: Display Filters: The display filter is used to display only specified packets. You can construct an expression by specifying header fields and optionally, the values that they should match. Example: ip.src_host == 192.168.1.7 and tcp.port == 443 and ssl.record.version == 0x0303.
3: Panes: the wireshark main window has 3 main panes: packet list, packet headers and the hex dumps and ascii respresentation of the packets bytes
4: Packet list: This aggregates major information on the packets that wireshark captures, in columns. Generally, the packet list should display the packet number, time since the start of the capture, the source and destionation IP addresses, the protocol, the packet length and a summary of the packet headers or contents.
5: Packets Headers: The packet headers section provides a wealth of information on each individual packet, and organises packet headers fields and values in layers of easy-to-view drop-down menus - from layer 1 frame information to layer 7 protcool contents. On the bottom pane we can see the hexadecimal and ASCII representation of the entire packet.

Applying a display Filter:

```
tcp.port == 80 -> only displays packets that have a source or dstination of port 80
tcp.window_size_value >= 8000 -> displays TCP packets with a window size of 8000
bytes or over.

Logical operator can be used on filters, and (&&) or (||), for example
ip.dst_host==192.168.1.7 && tcp -> only displays tcp port on the dstination host ip
192.168.1.7,  we can use not (!) as a operator.
```

Following streams and costum collumns:

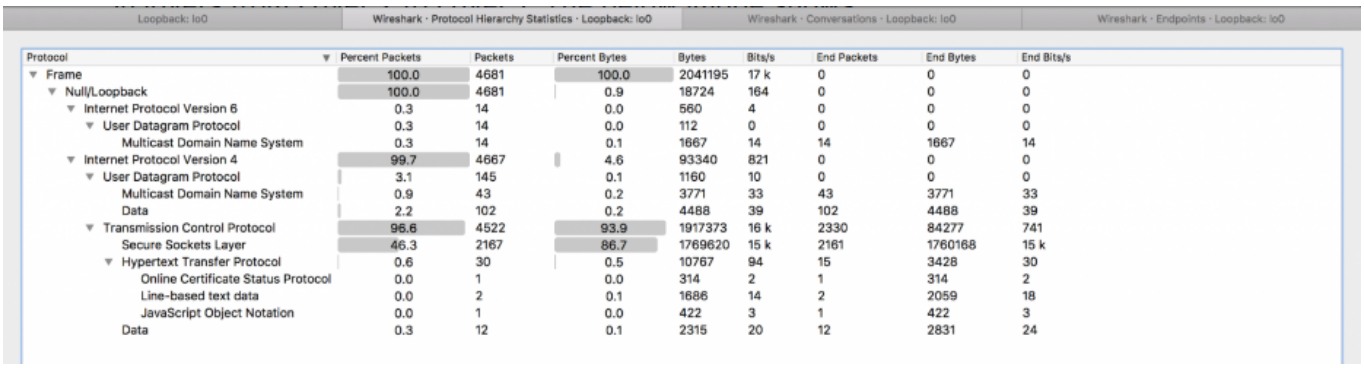
```
To follow a stream on wireshark we go to: right click on packet -> Follow ->
TCP/UDP/SSL/HTTP Stream.
To add a packet header value as a column, right click on the header -> apply as
column.
```

Viewing Capture Statistics:

```
Wireshark collect different statistics about the traffic in the capture file.
This section discuss three of the statistics windows:
        Protocol Hierarchy
        Conversations
        Endpoints
```

Protocol Hierarchy:

```
This window displays the percentages of the number of packets or bytes in a
protocol conversation agains the entire traffic.
```




| Protocol | Percent Packets | Packets | Percent Bytes | Bytes | Bits/s | End Packets | End Bytes | End Bits/s |
|---|---|---|---|---|---|---|---|---|
| Frame | 100.0 | 4681 | 100.0 | 2041195 | 17 k | 0 | 0 | 0 |
| Null/Loopback | 100.0 | 4681 | 0.9 | 18724 | 164 | 0 | 0 | 0 |
| Internet Protocol Version 6 | 0.3 | 14 | 0.0 | 560 | 4 | 0 | 0 | 0 |
| User Datagram Protocol | 0.3 | 14 | 0.0 | 112 | 0 | 0 | 0 | 0 |
| Multicast Domain Name System | 0.3 | 14 | 0.1 | 1667 | 14 | 14 | 1667 | 14 |
| Internet Protocol Version 4 | 99.7 | 4667 | 4.6 | 93340 | 821 | 0 | 0 | 0 |
| User Datagram Protocol | 3.1 | 145 | 0.1 | 1160 | 10 | 0 | 0 | 0 |
| Multicast Domain Name System | 0.9 | 43 | 0.2 | 3771 | 33 | 43 | 3771 | 33 |
| Data | 2.2 | 102 | 0.2 | 4488 | 39 | 102 | 4488 | 39 |
| Transmission Control Protocol | 96.6 | 4522 | 93.9 | 1917373 | 16 k | 2330 | 84277 | 741 |
| Secure Sockets Layer | 46.3 | 2167 | 86.7 | 1769620 | 15 k | 2161 | 1760168 | 15 k |
| Hypertext Transfer Protocol | 0.6 | 30 | 0.5 | 10767 | 94 | 15 | 3428 | 30 |
| Online Certificate Status Protocol | 0.0 | 1 | 0.0 | 314 | 2 | 1 | 314 | 2 |
| Line-based text data | 0.0 | 2 | 0.1 | 1686 | 14 | 2 | 2059 | 18 |
| JavaScript Object Notation | 0.0 | 1 | 0.0 | 422 | 3 | 1 | 422 | 3 |
| Data | 0.3 | 12 | 0.1 | 2315 | 20 | 12 | 2831 | 24 |

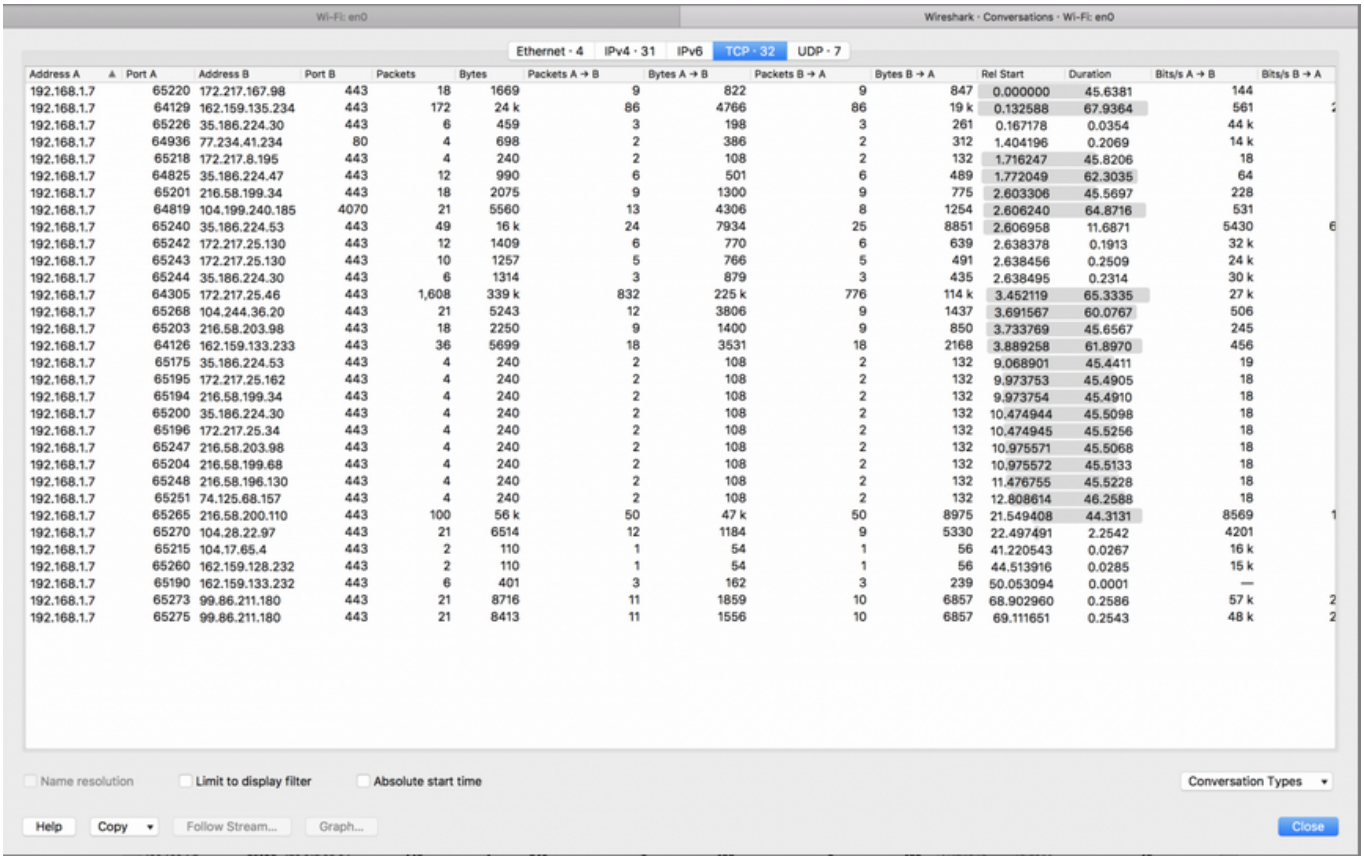
```
Here we can see that:
        99.7 is IPV4 packets
        96.6 is TCP
```

46.3 being ssl

This can be usefull in a example case where we notice a very samll portion of FTP traffic in a large network that doesn´t use FTP. It might be worth it to check out the FTP traffic and make sure is legitimate.

Conversations:

This window also provides good information  on the traffic, including which hosts communicated which hosts, on which ports, and with a total of how many bytes and packets in the conversation. This window is great for identifying the different MAC or IP addresses that a host has communicated with, and the volume of traffic between them.

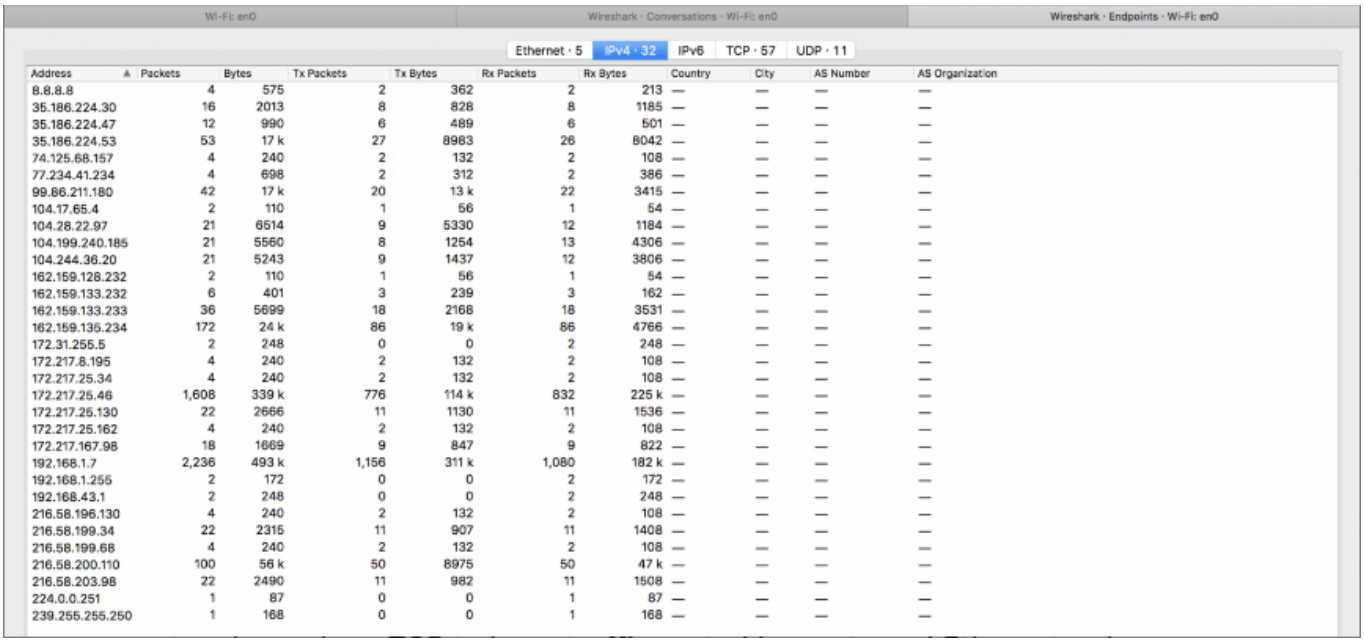



| Address A | Port A | Address B | Port B | Packets | Bytes | Packets A → B | Bytes A → B | Packets B → A | Bytes B → A | Rel Start | Duration | Bits/s A → B | Bits/s B → A |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 192.168.1.7 | 65220 | 172.217.167.98 | 443 | 18 | 1669 | 9 | 822 | 9 | 847 | 0.000000 | 45.6381 | 144 | |
| 192.168.1.7 | 64129 | 162.159.135.234 | 443 | 172 | 24 k | 86 | 4766 | 86 | 19 k | 0.132588 | 67.9364 | 561 | |
| 192.168.1.7 | 65226 | 35.186.224.30 | 443 | 6 | 459 | 3 | 198 | 3 | 261 | 0.167178 | 0.0354 | 44 k | |
| 192.168.1.7 | 64936 | 77.234.41.234 | 80 | 4 | 698 | 2 | 386 | 2 | 312 | 1.404196 | 0.2069 | 14 k | |
| 192.168.1.7 | 65218 | 172.217.8.195 | 443 | 4 | 240 | 2 | 108 | 2 | 132 | 1.716247 | 45.8206 | 18 | |
| 192.168.1.7 | 64825 | 35.186.224.47 | 443 | 12 | 990 | 6 | 501 | 6 | 489 | 1.772049 | 62.3035 | 64 | |
| 192.168.1.7 | 65201 | 216.58.199.34 | 443 | 18 | 2075 | 9 | 1300 | 9 | 775 | 2.603306 | 45.5697 | 228 | |
| 192.168.1.7 | 64819 | 104.199.240.185 | 4070 | 21 | 5560 | 13 | 4306 | 8 | 1254 | 2.606240 | 64.8716 | 531 | |
| 192.168.1.7 | 65240 | 35.186.224.53 | 443 | 49 | 16 k | 24 | 7934 | 25 | 8851 | 2.606958 | 11.6871 | 5430 | |
| 192.168.1.7 | 65242 | 172.217.25.130 | 443 | 12 | 1409 | 6 | 770 | 6 | 639 | 2.638378 | 0.1913 | 32 k | |
| 192.168.1.7 | 65243 | 172.217.25.130 | 443 | 10 | 1257 | 5 | 766 | 5 | 491 | 2.638456 | 0.2509 | 24 k | |
| 192.168.1.7 | 65244 | 35.186.224.30 | 443 | 6 | 1314 | 3 | 879 | 3 | 435 | 2.638495 | 0.2314 | 30 k | |
| 192.168.1.7 | 64305 | 172.217.25.46 | 443 | 1,608 | 339 k | 832 | 225 k | 776 | 114 k | 3.452119 | 65.3335 | 27 k | |
| 192.168.1.7 | 65268 | 104.244.36.20 | 443 | 21 | 5243 | 12 | 3806 | 9 | 1437 | 3.691567 | 60.0767 | 506 | |
| 192.168.1.7 | 65203 | 216.58.203.98 | 443 | 18 | 2250 | 9 | 1400 | 9 | 850 | 3.733769 | 45.6567 | 245 | |
| 192.168.1.7 | 64126 | 162.159.133.233 | 443 | 36 | 5699 | 18 | 3531 | 18 | 2168 | 3.889258 | 61.8970 | 456 | |
| 192.168.1.7 | 65175 | 35.186.224.53 | 443 | 4 | 240 | 2 | 108 | 2 | 132 | 9.068901 | 45.4411 | 19 | |
| 192.168.1.7 | 65195 | 172.217.25.162 | 443 | 4 | 240 | 2 | 108 | 2 | 132 | 9.973753 | 45.4905 | 18 | |
| 192.168.1.7 | 65194 | 216.58.199.34 | 443 | 4 | 240 | 2 | 108 | 2 | 132 | 9.973754 | 45.4910 | 18 | |
| 192.168.1.7 | 65200 | 35.186.224.30 | 443 | 4 | 240 | 2 | 108 | 2 | 132 | 10.474944 | 45.5098 | 18 | |
| 192.168.1.7 | 65196 | 172.217.25.34 | 443 | 4 | 240 | 2 | 108 | 2 | 132 | 10.474945 | 45.5256 | 18 | |
| 192.168.1.7 | 65247 | 216.58.203.98 | 443 | 4 | 240 | 2 | 108 | 2 | 132 | 10.975571 | 45.5068 | 18 | |
| 192.168.1.7 | 65204 | 216.58.199.68 | 443 | 4 | 240 | 2 | 108 | 2 | 132 | 10.975572 | 45.5133 | 18 | |
| 192.168.1.7 | 65248 | 216.58.196.130 | 443 | 4 | 240 | 2 | 108 | 2 | 132 | 11.476755 | 45.5228 | 18 | |
| 192.168.1.7 | 65251 | 74.125.68.157 | 443 | 4 | 240 | 2 | 108 | 2 | 132 | 12.808614 | 46.2588 | 18 | |
| 192.168.1.7 | 65265 | 216.58.200.110 | 443 | 100 | 56 k | 50 | 47 k | 50 | 8975 | 21.549408 | 44.3131 | 8569 | |
| 192.168.1.7 | 65270 | 104.28.22.97 | 443 | 21 | 6514 | 12 | 1184 | 9 | 5330 | 22.497491 | 2.2542 | 4201 | |
| 192.168.1.7 | 65215 | 104.17.65.4 | 443 | 2 | 110 | 1 | 54 | 1 | 56 | 41.220543 | 0.0267 | 16 k | |
| 192.168.1.7 | 65260 | 162.159.128.232 | 443 | 2 | 110 | 1 | 54 | 1 | 56 | 44.513916 | 0.0285 | 15 k | |
| 192.168.1.7 | 65190 | 162.159.133.232 | 443 | 6 | 401 | 3 | 162 | 3 | 239 | 50.053094 | 0.0001 | — | |
| 192.168.1.7 | 65273 | 99.86.211.180 | 443 | 21 | 8716 | 11 | 1859 | 10 | 6857 | 68.902960 | 0.2586 | 57 k | |
| 192.168.1.7 | 65275 | 99.86.211.180 | 443 | 21 | 8413 | 11 | 1556 | 10 | 6857 | 69.111651 | 0.2543 | 48 k | |

In the above image, as shown by the first line, host 192.168.56.17 has been connecting to HTTPS 172.217.167.98 server with port 65220 and has sent and recieve 9 packets.

Endpoints:

The endpoints window shows all of the different hosts that appear in the capture and the ammount of packets/bytes they sent and received. This window is useful in sorting hosts by their network activity, by either transmittion or receiving volume.
For example: If a hosts receive much more traffic then they have been transmitting they are probably downloading a large file. But if its the opossite they might being uploading a file.




| Address | Packets | Bytes | Tx Packets | Tx Bytes | Rx Packets | Rx Bytes | Country | City | AS Number | AS Organization |
|---|---|---|---|---|---|---|---|---|---|---|
| 8.8.8.8 | 4 | 575 | 2 | 362 | 2 | 213 | — | — | — | — |
| 35.186.224.30 | 16 | 2013 | 8 | 828 | 8 | 1185 | — | — | — | — |
| 35.186.224.47 | 12 | 990 | 6 | 489 | 6 | 501 | — | — | — | — |
| 35.186.224.53 | 53 | 17 k | 27 | 8983 | 26 | 8042 | — | — | — | — |
| 74.125.68.157 | 4 | 240 | 2 | 132 | 2 | 108 | — | — | — | — |
| 77.234.41.234 | 4 | 698 | 2 | 312 | 2 | 386 | — | — | — | — |
| 99.86.211.180 | 42 | 17 k | 20 | 13 k | 22 | 3415 | — | — | — | — |
| 104.17.65.4 | 2 | 110 | 1 | 56 | 1 | 54 | — | — | — | — |
| 104.28.22.97 | 21 | 6514 | 9 | 5330 | 12 | 1184 | — | — | — | — |
| 104.199.240.185 | 21 | 5560 | 8 | 1254 | 13 | 4306 | — | — | — | — |
| 104.244.36.20 | 21 | 5243 | 9 | 1437 | 12 | 3806 | — | — | — | — |
| 162.159.128.232 | 2 | 110 | 1 | 56 | 1 | 54 | — | — | — | — |
| 162.159.133.232 | 6 | 401 | 3 | 239 | 3 | 162 | — | — | — | — |
| 162.159.133.233 | 36 | 5699 | 18 | 2168 | 18 | 3531 | — | — | — | — |
| 162.159.135.234 | 172 | 24 k | 86 | 19 k | 86 | 4766 | — | — | — | — |
| 172.31.255.5 | 2 | 248 | 0 | 0 | 2 | 248 | — | — | — | — |
| 172.217.8.195 | 4 | 240 | 2 | 132 | 2 | 108 | — | — | — | — |
| 172.217.25.34 | 4 | 240 | 2 | 132 | 2 | 108 | — | — | — | — |
| 172.217.25.46 | 1,608 | 339 k | 776 | 114 k | 832 | 225 k | — | — | — | — |
| 172.217.25.130 | 22 | 2666 | 11 | 1130 | 11 | 1536 | — | — | — | — |
| 172.217.25.162 | 4 | 240 | 2 | 132 | 2 | 108 | — | — | — | — |
| 172.217.167.98 | 18 | 1669 | 9 | 847 | 9 | 822 | — | — | — | — |
| 192.168.1.7 | 2,236 | 493 k | 1,156 | 311 k | 1,080 | 182 k | — | — | — | — |
| 192.168.1.255 | 2 | 172 | 0 | 0 | 2 | 172 | — | — | — | — |
| 192.168.43.1 | 2 | 248 | 0 | 0 | 2 | 248 | — | — | — | — |
| 216.58.196.130 | 4 | 240 | 2 | 132 | 2 | 108 | — | — | — | — |
| 216.58.199.34 | 22 | 2315 | 11 | 907 | 11 | 1408 | — | — | — | — |
| 216.58.199.68 | 4 | 240 | 2 | 132 | 2 | 108 | — | — | — | — |
| 216.58.200.110 | 100 | 56 k | 50 | 8975 | 50 | 47 k | — | — | — | — |
| 216.58.203.98 | 22 | 2490 | 11 | 982 | 11 | 1508 | — | — | — | — |
| 224.0.0.251 | 1 | 87 | 0 | 0 | 1 | 87 | — | — | — | — |
| 239.255.255.250 | 1 | 168 | 0 | 0 | 1 | 168 | — | — | — | — |

In the above diagram, host 192.168.1.7 has sent 1156 packets, totaling 311kb and received 1080 packets, totaling 182kb.