Assignment 3

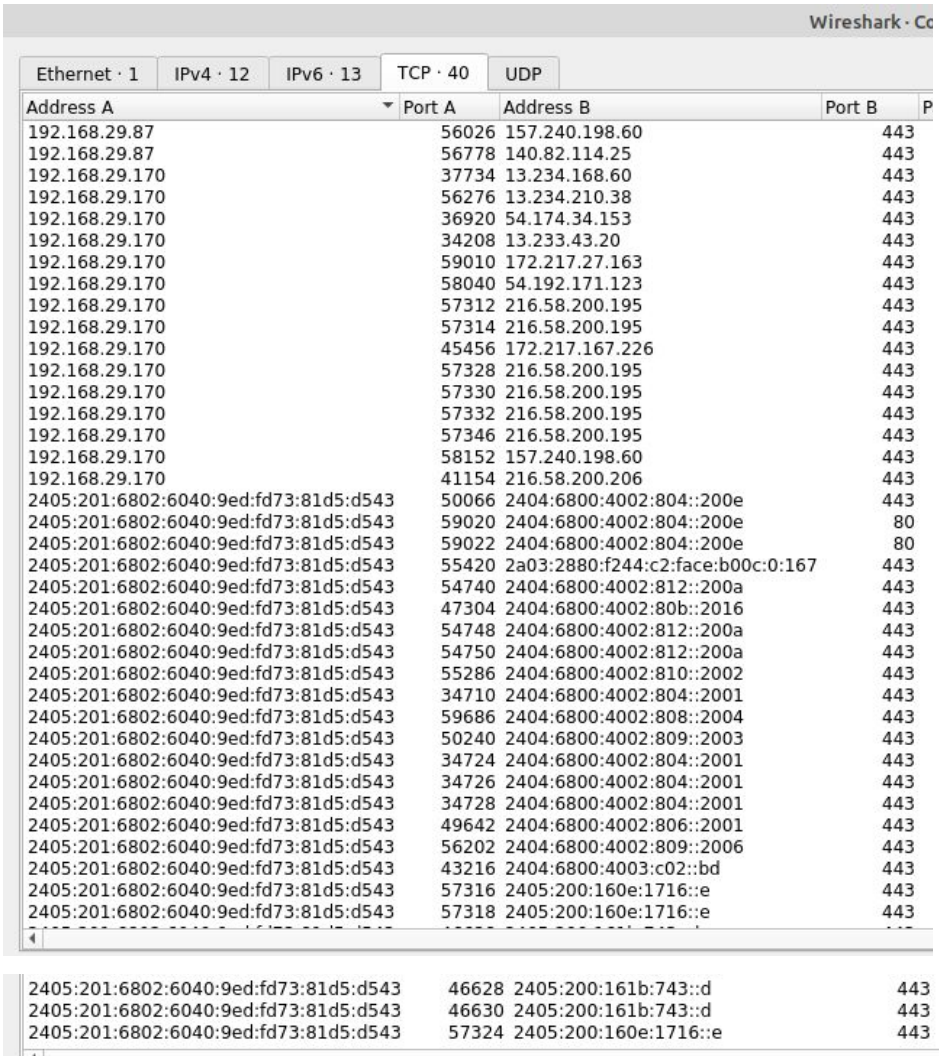
1)

a)

```
navneet@navneet-Inspiron:~$ sudo tshark -i wlx00177c9b1d95 -f tcp -a duration:30 -w /tmp/Capture.pcap
Running as user "root" and group "root". This could be dangerous.
Capturing on 'wlx00177c9b1d95'
46437
```

b)

There are **40 TCP** connections in this packet capture.
The communicating peers can be seen in the attached screenshot.



Wireshark · Cc

Ethernet · 1 | IPv4 · 12 | IPv6 · 13 | TCP · 40 | UDP

Address A	Port A	Address B	Port B
192.168.29.87	56026	157.240.198.60	443
192.168.29.87	56778	140.82.114.25	443
192.168.29.170	37734	13.234.168.60	443
192.168.29.170	56276	13.234.210.38	443
192.168.29.170	36920	54.174.34.153	443
192.168.29.170	34208	13.233.43.20	443
192.168.29.170	59010	172.217.27.163	443
192.168.29.170	58040	54.192.171.123	443
192.168.29.170	57312	216.58.200.195	443
192.168.29.170	57314	216.58.200.195	443
192.168.29.170	45456	172.217.167.226	443
192.168.29.170	57328	216.58.200.195	443
192.168.29.170	57330	216.58.200.195	443
192.168.29.170	57332	216.58.200.195	443
192.168.29.170	57346	216.58.200.195	443
192.168.29.170	58152	157.240.198.60	443
192.168.29.170	41154	216.58.200.206	443
2405:201:6802:6040:9ed:fd73:81d5:d543	50066	2404:6800:4002:804::200e	443
2405:201:6802:6040:9ed:fd73:81d5:d543	59020	2404:6800:4002:804::200e	80
2405:201:6802:6040:9ed:fd73:81d5:d543	59022	2404:6800:4002:804::200e	80
2405:201:6802:6040:9ed:fd73:81d5:d543	55420	2a03:2880:f244:c2:face:b00c:0:167	443
2405:201:6802:6040:9ed:fd73:81d5:d543	54740	2404:6800:4002:812::200a	443
2405:201:6802:6040:9ed:fd73:81d5:d543	47304	2404:6800:4002:80b::2016	443
2405:201:6802:6040:9ed:fd73:81d5:d543	54748	2404:6800:4002:812::200a	443
2405:201:6802:6040:9ed:fd73:81d5:d543	54750	2404:6800:4002:812::200a	443
2405:201:6802:6040:9ed:fd73:81d5:d543	55286	2404:6800:4002:810::2002	443
2405:201:6802:6040:9ed:fd73:81d5:d543	34710	2404:6800:4002:804::2001	443
2405:201:6802:6040:9ed:fd73:81d5:d543	59686	2404:6800:4002:808::2004	443
2405:201:6802:6040:9ed:fd73:81d5:d543	50240	2404:6800:4002:809::2003	443
2405:201:6802:6040:9ed:fd73:81d5:d543	34724	2404:6800:4002:804::2001	443
2405:201:6802:6040:9ed:fd73:81d5:d543	34726	2404:6800:4002:804::2001	443
2405:201:6802:6040:9ed:fd73:81d5:d543	34728	2404:6800:4002:804::2001	443
2405:201:6802:6040:9ed:fd73:81d5:d543	49642	2404:6800:4002:806::2001	443
2405:201:6802:6040:9ed:fd73:81d5:d543	56202	2404:6800:4002:809::2006	443
2405:201:6802:6040:9ed:fd73:81d5:d543	43216	2404:6800:4003:c02::bd	443
2405:201:6802:6040:9ed:fd73:81d5:d543	57316	2405:200:160e:1716::e	443
2405:201:6802:6040:9ed:fd73:81d5:d543	57318	2405:200:160e:1716::e	443
2405:201:6802:6040:9ed:fd73:81d5:d543	46628	2405:200:161b:743::d	443
2405:201:6802:6040:9ed:fd73:81d5:d543	46630	2405:200:161b:743::d	443
2405:201:6802:6040:9ed:fd73:81d5:d543	57324	2405:200:160e:1716::e	443

c) Since address A is the local address of my system, thus we can consider bytes sent from host A to B as **upstream** and bytes sent from host B to A as **downstream**. The upstream and downstream data transfer for each TCP connection can be seen from the screenshot.

Address A	Port A	Address B	Port	Bytes A → B	Bytes B → A
192.168.29.87	56778	140.82.114.25	443	96	0
192.168.29.170	57312	216.58.200.195	443	128	74
192.168.29.170	57314	216.58.200.195	443	128	74
192.168.29.170	57328	216.58.200.195	443	128	74
192.168.29.170	57330	216.58.200.195	443	128	74
192.168.29.170	57332	216.58.200.195	443	128	74
192.168.29.170	57346	216.58.200.195	443	128	74
2405:201:6802:...	54740	2404:6800:40...	443	168	94
2405:201:6802:...	54748	2404:6800:40...	443	168	94
2405:201:6802:...	54750	2404:6800:40...	443	168	94
2405:201:6802:...	34710	2404:6800:40...	443	168	94
2405:201:6802:...	34724	2404:6800:40...	443	168	94
2405:201:6802:...	34726	2404:6800:40...	443	168	94
192.168.29.170	59010	172.217.27.163	443	171	171
192.168.29.170	41154	216.58.200.206	443	171	171
2405:201:6802:...	43216	2404:6800:40...	443	211	211
192.168.29.170	58152	157.240.198.60	443	342	1,477
192.168.29.87	56026	157.240.198.60	443	396	0
2405:201:6802:...	59020	2404:6800:40...	80	352	180
2405:201:6802:...	55420	2a03:2880:f24...	443	469	445
2405:201:6802:...	59022	2404:6800:40...	80	888	1,019
2405:201:6802:...	49642	2404:6800:40...	443	1,692	1,433
192.168.29.170	36920	54.174.34.153	443	2,262	4,763
192.168.29.170	37734	13.234.168.60	443	2,741	5,379
192.168.29.170	58040	54.192.171.123	443	1,893	6,250
2405:201:6802:...	56202	2404:6800:40...	443	2,480	2,256
192.168.29.170	56276	13.234.210.38	443	2,634	7,234
192.168.29.170	45456	172.217.167.226	443	2,358	5,074
2405:201:6802:...	59686	2404:6800:40...	443	3,937	4,172
2405:201:6802:...	50240	2404:6800:40...	443	3,054	3,341
2405:201:6802:...	55286	2404:6800:40...	443	4,535	8,711
2405:201:6802:...	34728	2404:6800:40...	443	9,314	45 k
2405:201:6802:...	46628	2405:200:161...	443	14 k	208 k
2405:201:6802:...	47304	2404:6800:40...	443	29 k	677 k
2405:201:6802:...	50066	2404:6800:40...	443	136 k	635 k
2405:201:6802:...	57318	2405:200:160...	443	67 k	1,067 k
2405:201:6802:...	57324	2405:200:160...	443	70 k	1,341 k
2405:201:6802:...	57316	2405:200:160...	443	111 k	2,754 k
2405:201:6802:...	57316	2405:200:160...	443	111 k	2,754 k
2405:201:6802:...	46630	2405:200:161...	443	143 k	3,924 k
192.168.29.170	34208	13.233.43.20	443	687 k	33 M

Total data transfer in upstream for all the connections = **1302865 bytes**
Total data transfer in downstream for all the connections = **44462455 bytes**

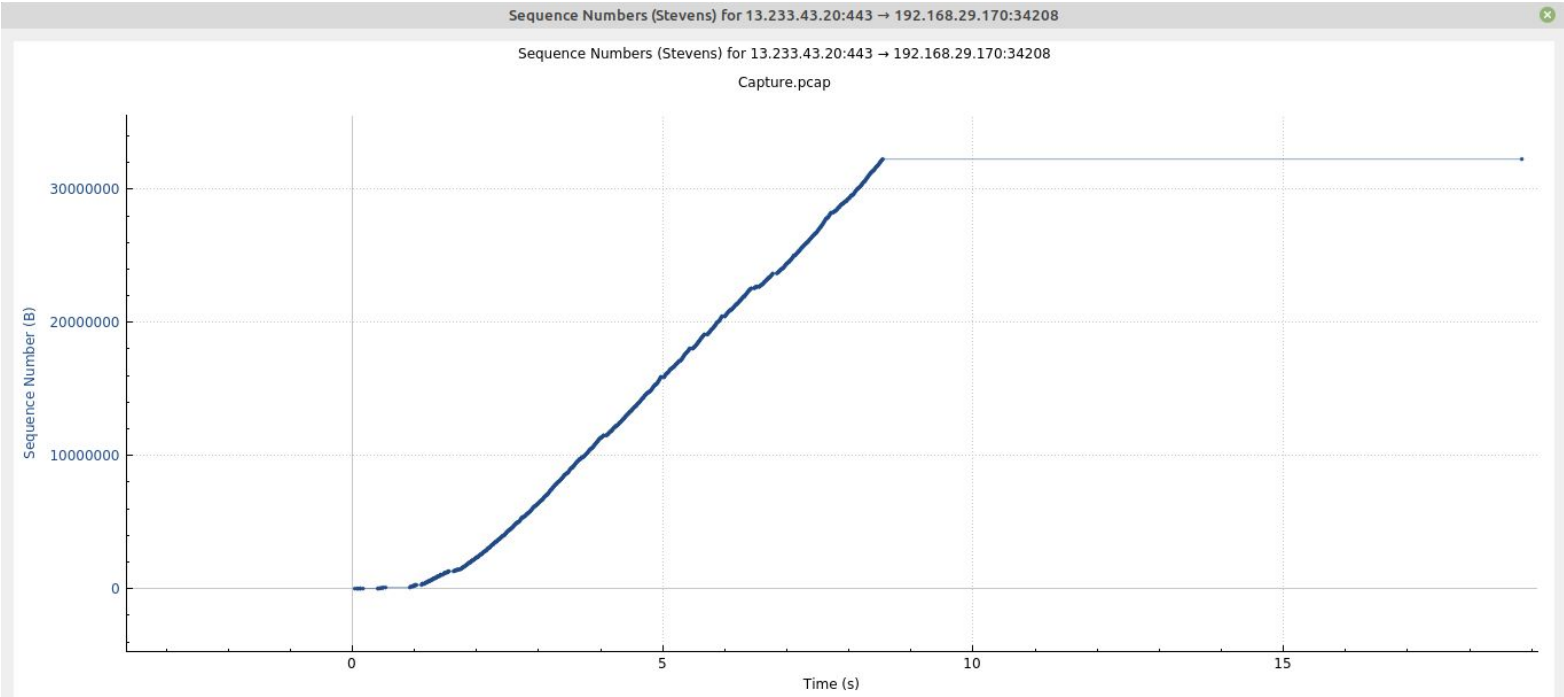
d) The connection for which the bytes transfer was maximum is attached below:

Address A	Port A	Address B	Port B	Bytes
192.168.29.170	34208	13.233.43.20	443	34 M

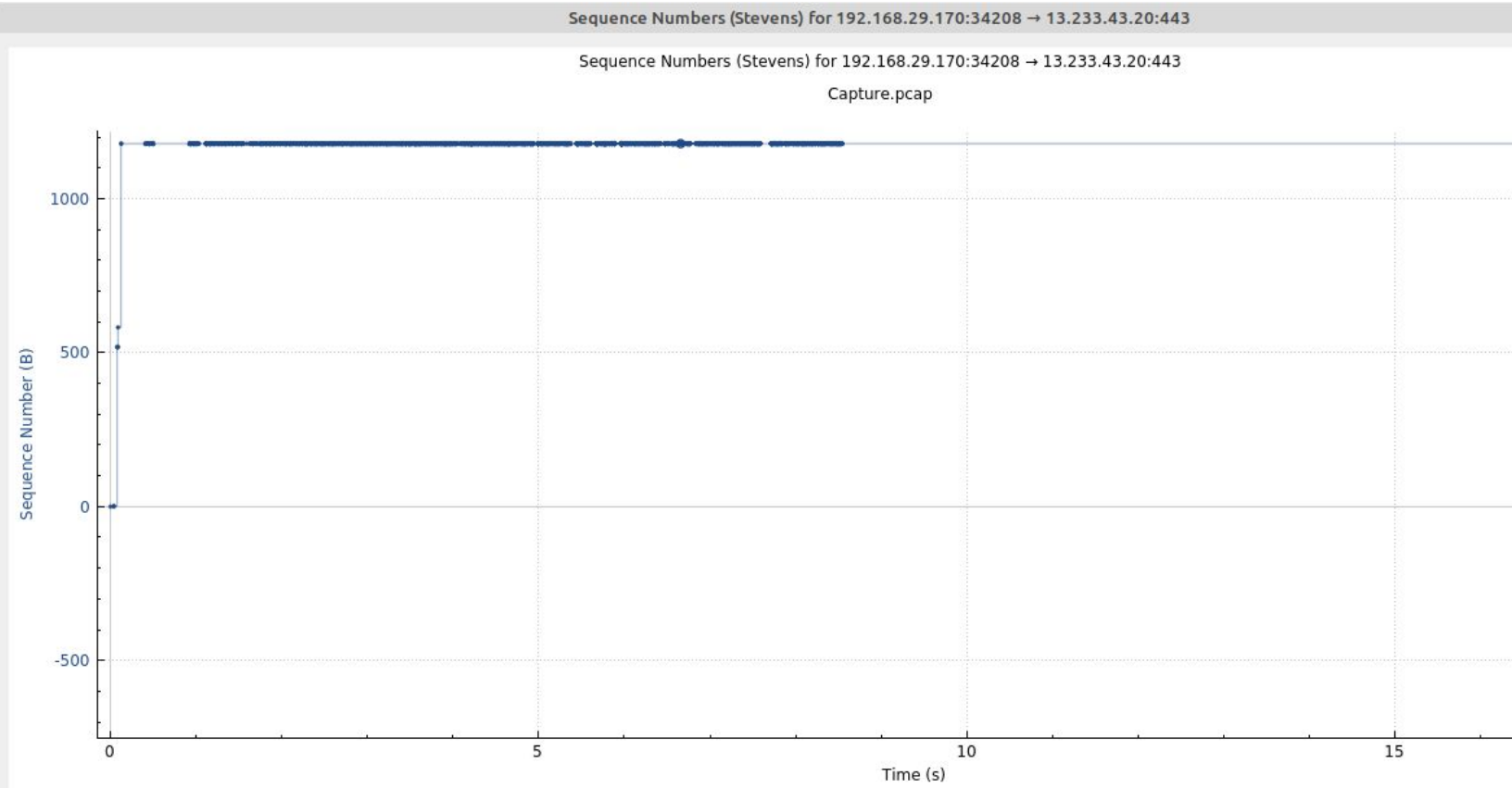
We observe that the sequence number does not get repeated for two different data packets,

this means that the sequence space is sufficient enough to satisfy transmittedsequence numbers .

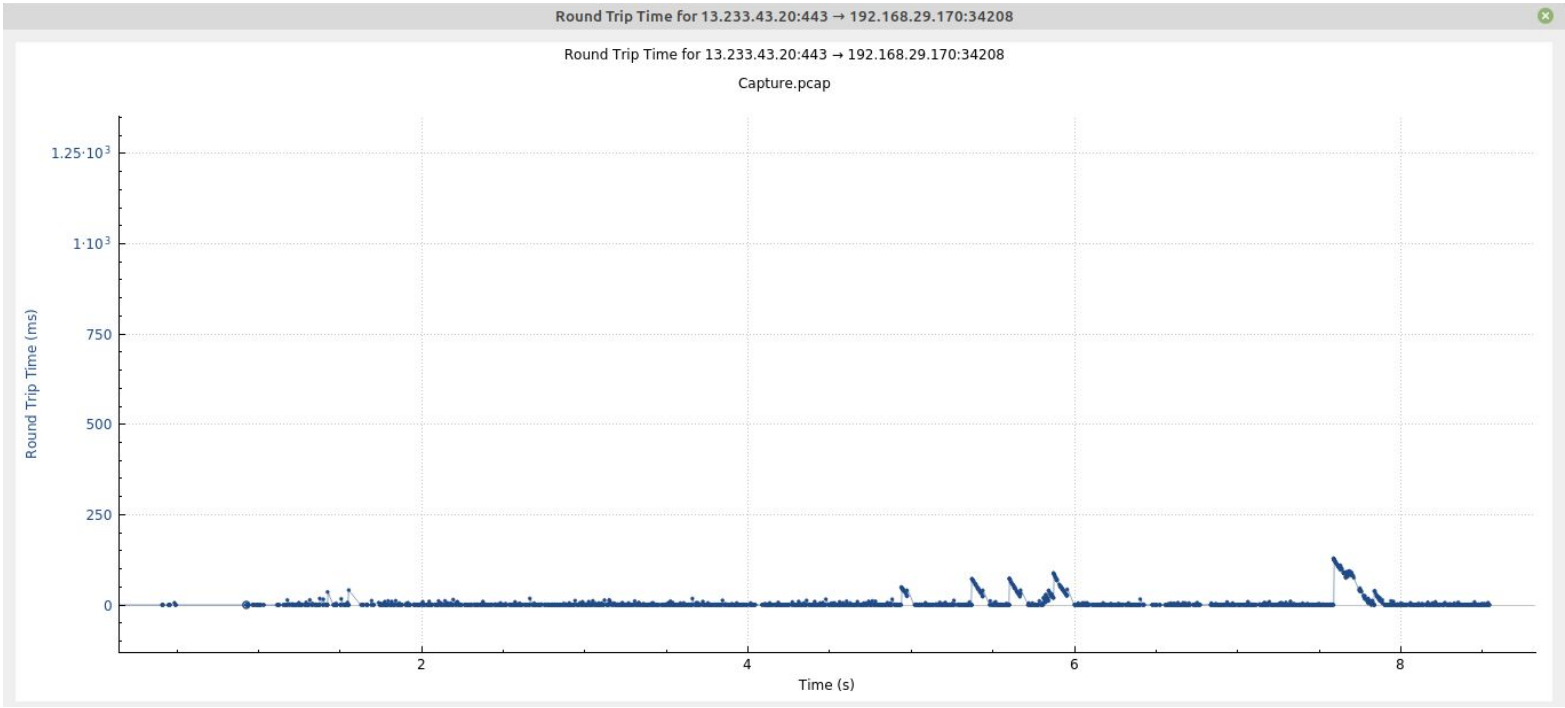
The TCP stream graph for host B to A(my system) is shown below



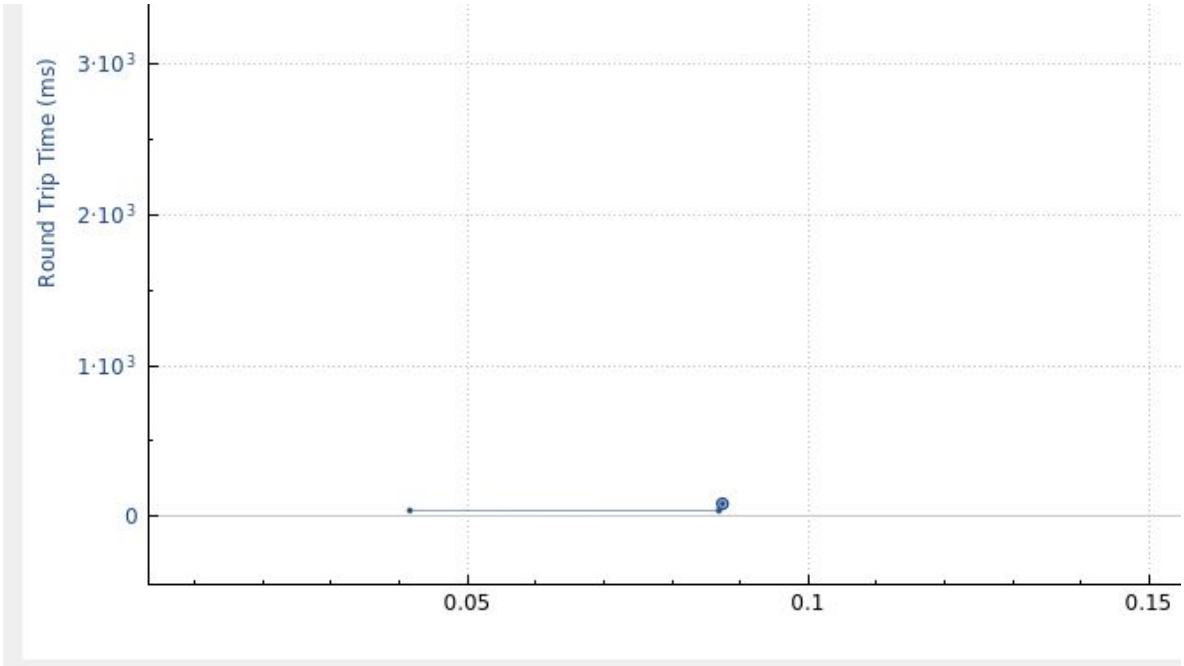
The TCP stream graph for host A(my system) to B is shown below



e) The RTT graph for host B to A(my system) is as follows :



The RTT graph for A(my system) to B is as follows :



f)

Used sample1.pcap for this part

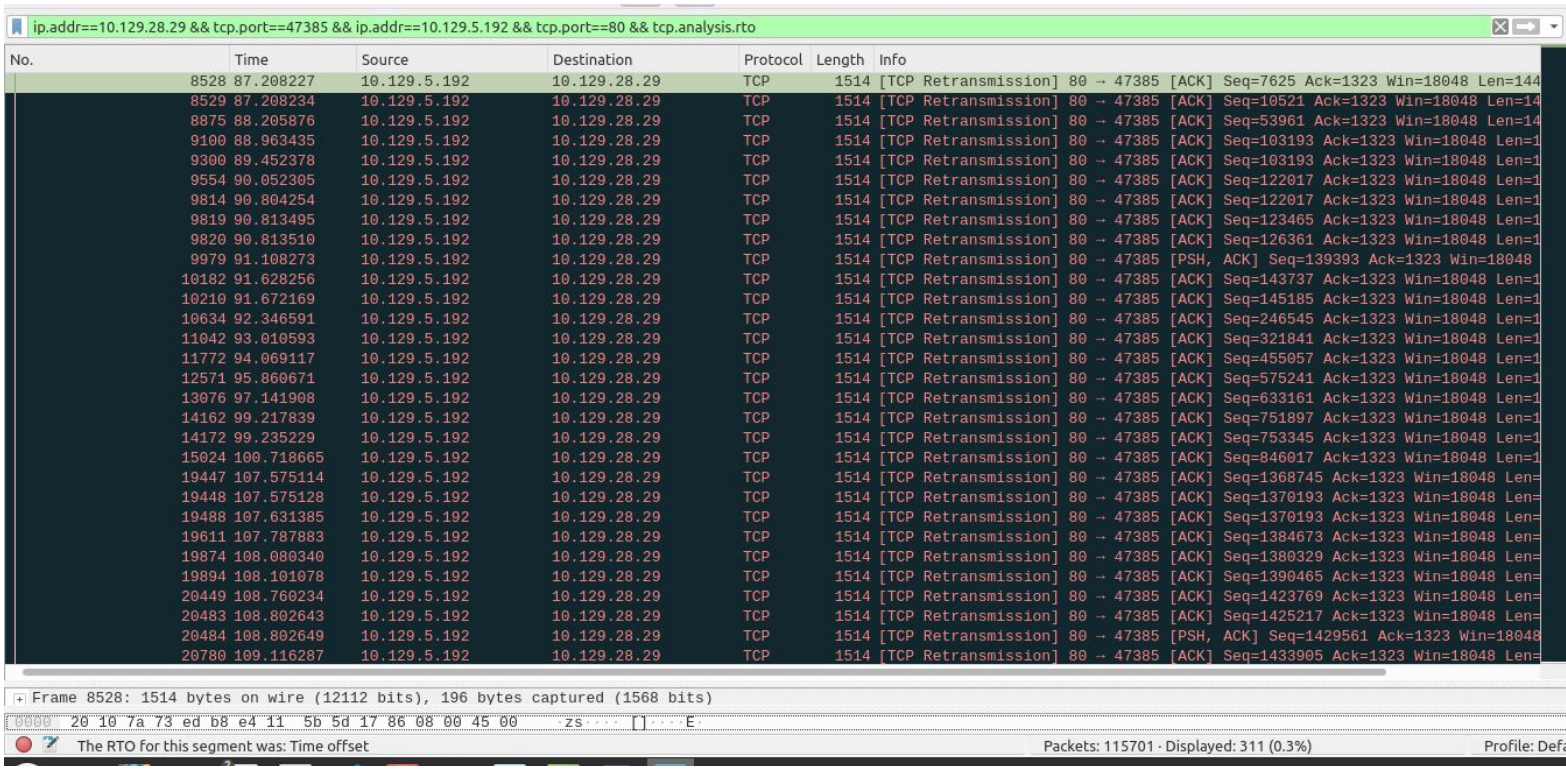
Address A	Port A	Address B	Port B	Packets	Bytes
10.129.28.29	47385	10.129.5.192	80	9,658	11 M

This is the connection for which maximum bytes transfer happens in sample1.pcap

Yes, the timeout instances are there in this case. These can be figured out from the TCP Retransmission packets, these packets are retransmitted because the sender does not receive an ACK for these packets within the timeout period.

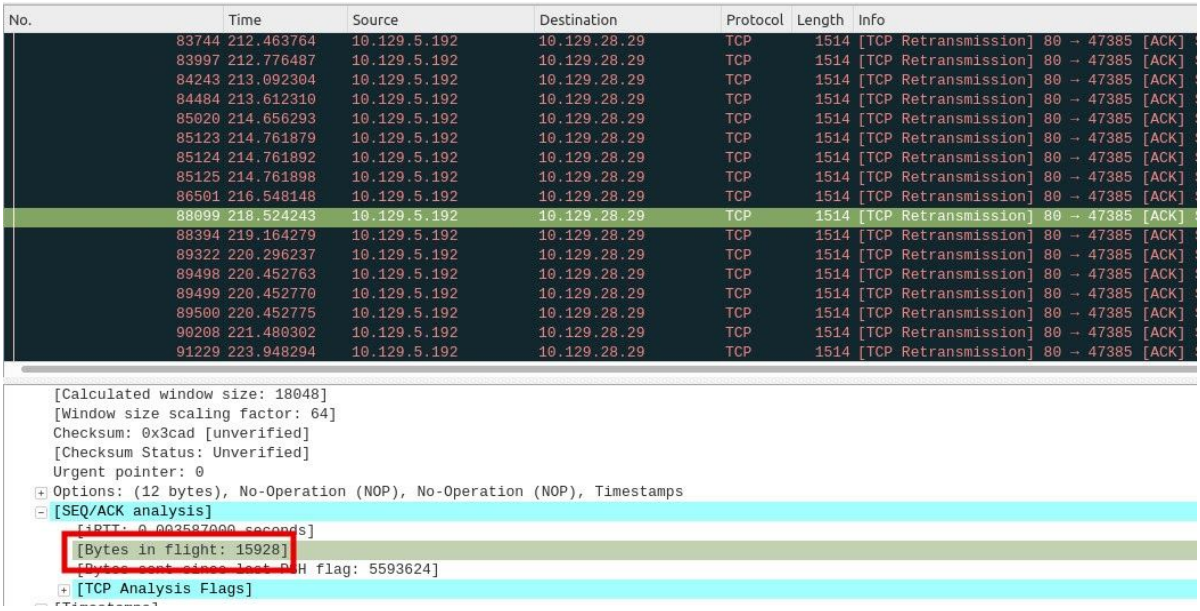
These can be found using **tcp.analysis.rto** filter. It filters the TCP packets that were retransmitted due to timeout. So, for the TCP connection mentioned above we use the following filter to find the timeout instances.

ip.addr==10.129.28.29 && tcp.port==47385 && ip.addr==10.129.5.192 && tcp.port==80 && tcp.analysis.rto



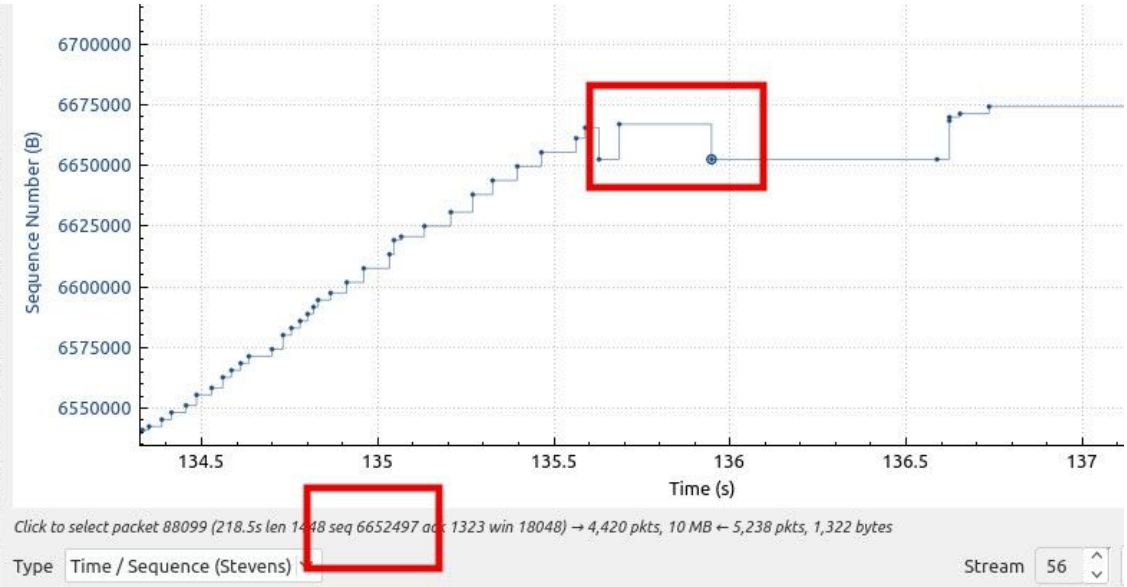
There are **311** such instances for timeout for this connection.

Let's check the congestion window size for the 88099th packet.(It is a Retransmission Packet)

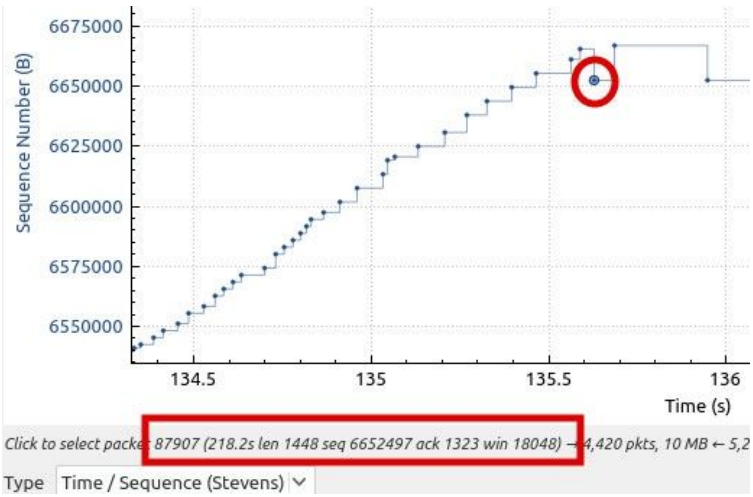


We can calculate the approx congestion window size before the time-out happens from the bytes in flight.So, the congestion window size is **15928 bytes** just before the timeout happens.
After the timeout happens the congestion window size will become **1 M.S.S.**

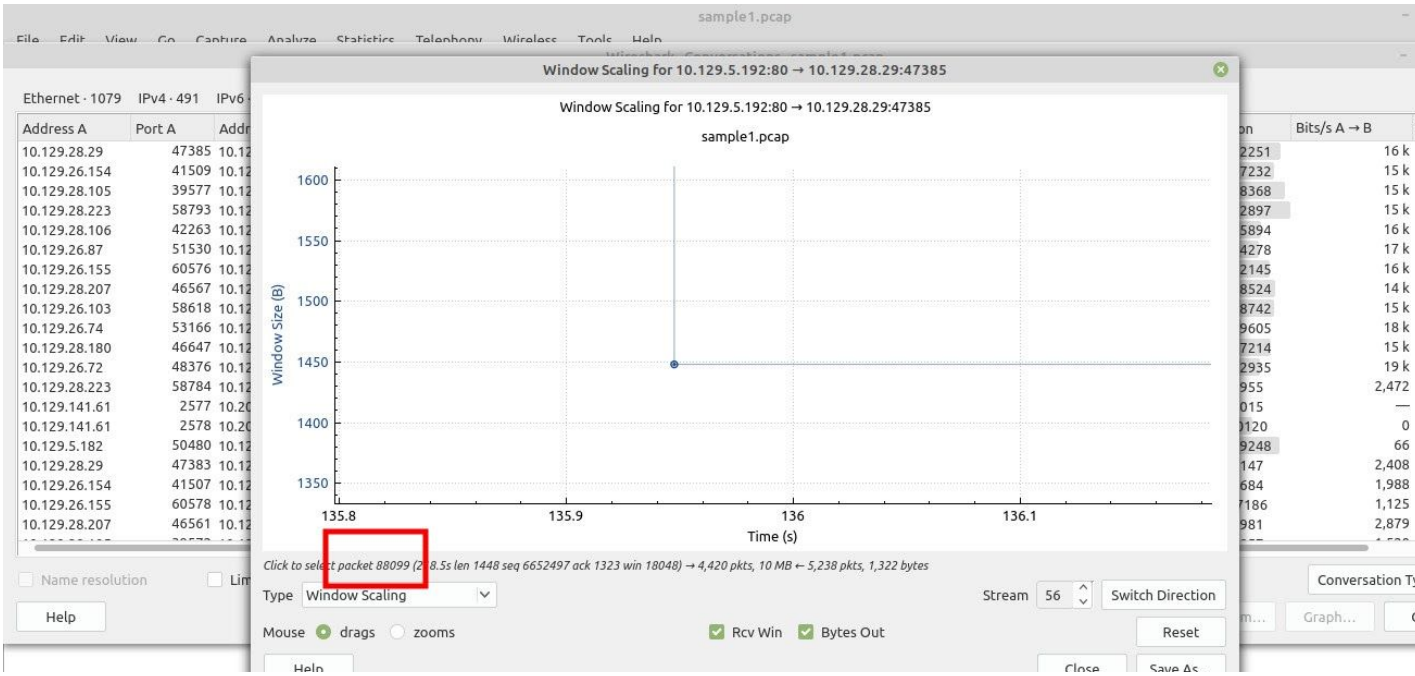
We can see from the graph below that there was a dip in the sequence number just after one packet was transferred, this means that timeout must have happened, and we know this is a retransmission packet.



Considering the packet two packets before this, we observe the same sequence number,this makes sure that the packet 88099 was a retransmission packet.



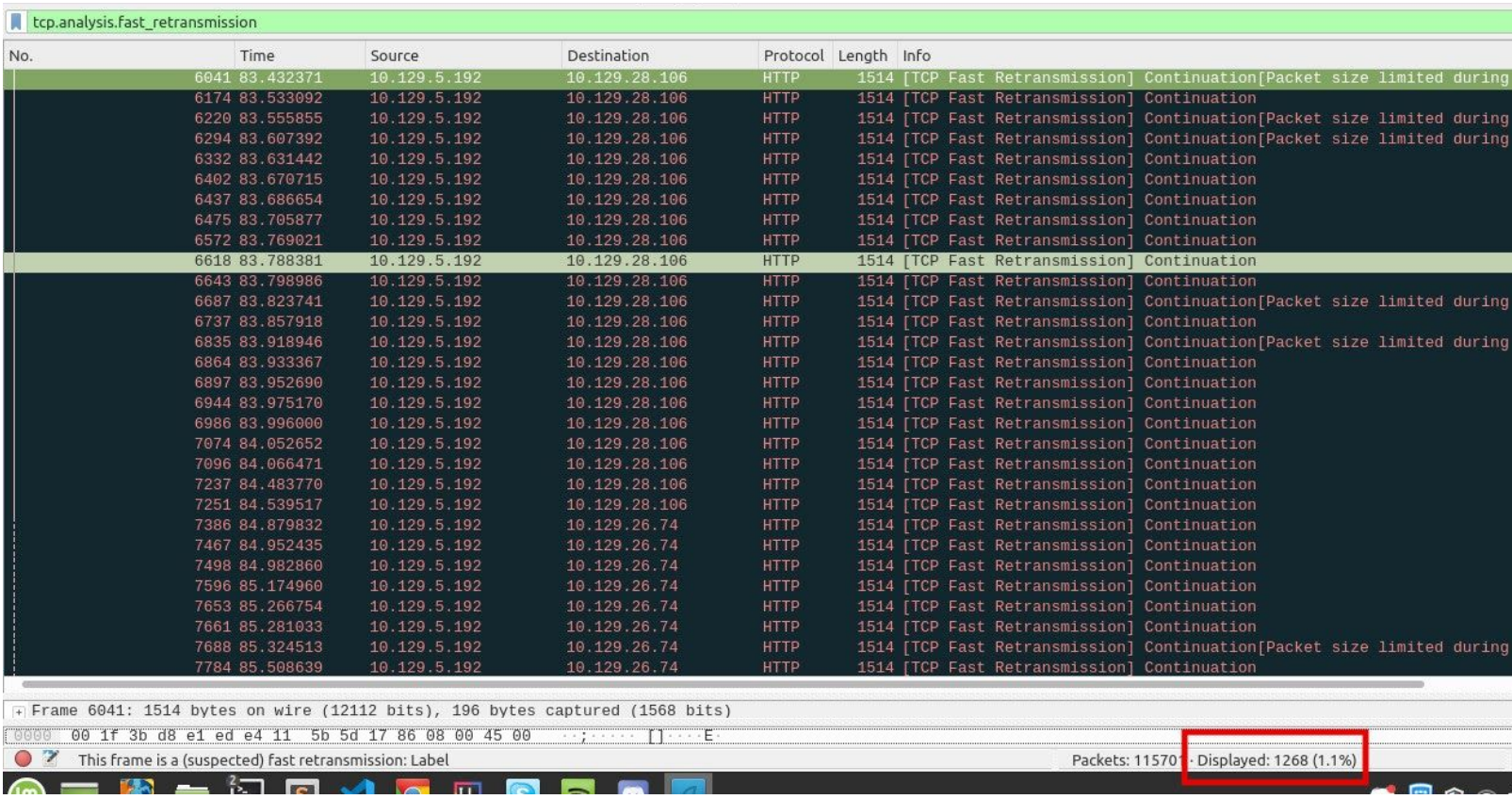
If we observe the window scaling graph for 88099th packet we see this (zoomed in view):



We observe that the Bytes out value is approximately 1450 bytes and we know that congestion window size can be inferred from the bytes out, so the congestion window size will be near this value, which will be almost 1 MSS.

g)

Used sample1.pcap for this part



Number of fast retransmissions are **1268** (for all the TCP connections)

2) Netstat was executed after the execution for tshark was over

a) Netstat displayed 29 connections which does not match with the TCP connections in my captured pcap file. This is because some of the TCP connections might have been closed during those 30 seconds.

```
navneet@navneet-Inspiron:~$ netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 navneet-Inspiron:58796  45.55.41.223:http       CLOSE_WAIT
tcp        0      0 navneet-Inspiron:34208  ec2-13-233-43-20.:https ESTABLISHED
tcp        0      0 navneet-Inspiron:49202  ec2-52-200-53-54.:https ESTABLISHED
tcp        0      0 navneet-Inspiron:45456  del11s04-in-f2.1e:https ESTABLISHED
tcp        0      0 navneet-Inspiron:59010  kix05s07-in-f3.1e:https ESTABLISHED
tcp        0      0 navneet-Inspiron:37024  ec2-18-232-238-10:https ESTABLISHED
tcp        0      0 navneet-Inspiron:56778  lb-140-82-114-25-:https ESTABLISHED
tcp        0      0 navneet-Inspiron:41154  nrt12s12-in-f206.:https ESTABLISHED
tcp        0      0 navneet-Inspiron:56026  whatsapp-cdn-shv-:https ESTABLISHED
tcp        0      0 navneet-Inspiron:37734  ec2-13-234-168-60:https ESTABLISHED
tcp        0      0 navneet-Inspiron:46666  ec2-52-26-249-11.:https ESTABLISHED
tcp        0      0 navneet-Inspiron:36920  ec2-54-174-34-153:https ESTABLISHED
tcp        0      0 navneet-Inspiron:45918  aeab55d76dd13c9bb:https TIME_WAIT
tcp        0      0 navneet-Inspiron:56276  ec2-13-234-210-38:https ESTABLISHED
tcp        0      0 navneet-Inspiron:58040  server-54-192-171:https ESTABLISHED
tcp        0      0 navneet-Inspiron:58152  whatsapp-cdn-shv-:https ESTABLISHED
tcp6       0      0 navneet-Inspiron:50240  del03s14-in-x03.1:https ESTABLISHED
tcp6       0      0 navneet-Inspiron:49642  del03s07-in-x01.1:https ESTABLISHED
tcp6       0      0 navneet-Inspiron:46630  2405:200:161b:743:https ESTABLISHED
tcp6       0      0 navneet-Inspiron:56202  del03s14-in-x06.1:https ESTABLISHED
tcp6       0      0 navneet-Inspiron:46628  2405:200:161b:743:https ESTABLISHED
tcp6       0      0 navneet-Inspiron:59020  del03s09-in-x0e.1e:http TIME_WAIT
tcp6       0      0 navneet-Inspiron:55286  del11s05-in-x02.1:https ESTABLISHED
tcp6       0      0 navneet-Inspiron:47304  del03s16-in-x16.1:https ESTABLISHED
tcp6       0      0 navneet-Inspiron:59022  del03s09-in-x0e.1e:http ESTABLISHED
tcp6       0      0 navneet-Inspiron:50066  del03s09-in-x0e.1:https ESTABLISHED
tcp6       0      0 navneet-Inspiron:34728  del03s09-in-x01.1:https ESTABLISHED
tcp6       0      0 navneet-Inspiron:59686  del03s13-in-x04.1:https ESTABLISHED
tcp6       0      0 navneet-Inspiron:43216  sc-in-xbd.1e100.n:https ESTABLISHED
```

b)

2 of these connections are in Timed-Wait state while 26 of them are in Established state.There is no fin-wait-1 tcp connection.

```
navneet@navneet-Inspiron:~$ netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 navneet-Inspiron:58796  45.55.41.223:http       CLOSE_WAIT
tcp        0      0 navneet-Inspiron:34208  ec2-13-233-43-20.:https ESTABLISHED
tcp        0      0 navneet-Inspiron:49202  ec2-52-200-53-54.:https ESTABLISHED
tcp        0      0 navneet-Inspiron:45456  del11s04-in-f2.1e:https ESTABLISHED
tcp        0      0 navneet-Inspiron:59010  kix05s07-in-f3.1e:https ESTABLISHED
tcp        0      0 navneet-Inspiron:37024  ec2-18-232-238-10:https ESTABLISHED
tcp        0      0 navneet-Inspiron:56778  lb-140-82-114-25-:https ESTABLISHED
tcp        0      0 navneet-Inspiron:41154  nrt12s12-in-f206.:https ESTABLISHED
tcp        0      0 navneet-Inspiron:56026  whatsapp-cdn-shv-:https ESTABLISHED
tcp        0      0 navneet-Inspiron:37734  ec2-13-234-168-60:https ESTABLISHED
tcp        0      0 navneet-Inspiron:46666  ec2-52-26-249-11.:https ESTABLISHED
tcp        0      0 navneet-Inspiron:36920  ec2-54-174-34-153:https ESTABLISHED
tcp        0      0 navneet-Inspiron:45918  aeab55d76dd13c9bb:https TIME_WAIT
tcp        0      0 navneet-Inspiron:56276  ec2-13-234-210-38:https ESTABLISHED
tcp        0      0 navneet-Inspiron:58040  server-54-192-171:https ESTABLISHED
tcp        0      0 navneet-Inspiron:58152  whatsapp-cdn-shv-:https ESTABLISHED
tcp6       0      0 navneet-Inspiron:50240  del03s14-in-x03.1:https ESTABLISHED
tcp6       0      0 navneet-Inspiron:49642  del03s07-in-x01.1:https ESTABLISHED
tcp6       0      0 navneet-Inspiron:46630  2405:200:161b:743:https ESTABLISHED
tcp6       0      0 navneet-Inspiron:56202  del03s14-in-x06.1:https ESTABLISHED
tcp6       0      0 navneet-Inspiron:46628  2405:200:161b:743:https ESTABLISHED
tcp6       0      0 navneet-Inspiron:59020  del03s09-in-x0e.1e:http TIME_WAIT
tcp6       0      0 navneet-Inspiron:55286  del11s05-in-x02.1:https ESTABLISHED
tcp6       0      0 navneet-Inspiron:47304  del03s16-in-x16.1:https ESTABLISHED
tcp6       0      0 navneet-Inspiron:59022  del03s09-in-x0e.1e:http ESTABLISHED
tcp6       0      0 navneet-Inspiron:50066  del03s09-in-x0e.1:https ESTABLISHED
tcp6       0      0 navneet-Inspiron:34728  del03s09-in-x01.1:https ESTABLISHED
tcp6       0      0 navneet-Inspiron:59686  del03s13-in-x04.1:https ESTABLISHED
tcp6       0      0 navneet-Inspiron:43216  sc-in-xbd.1e100.n:https ESTABLISHED
```

c)

```
navneet@navneet-Inspiron:~$ sudo ifconfig wlx00177c9b1d95 down
```

```
navneet@navneet-Inspiron:~$ netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 navneet-Inspiron:58796  45.55.41.223:http       CLOSE_WAIT
tcp        0    124 navneet-Inspiron:49202  ec2-52-200-53-54.:https FIN_WAIT1
tcp        0    103 navneet-Inspiron:45456  del11s04-in-f2.1e:https FIN_WAIT1
tcp        0    103 navneet-Inspiron:59010  kix05s07-in-f3.1e:https FIN_WAIT1
tcp        0    124 navneet-Inspiron:37024  ec2-18-232-238-10:https FIN_WAIT1
tcp        0      0 navneet-Inspiron:56318  whatsapp-cdn-shv-:https ESTABLISHED
tcp        0      0 navneet-Inspiron:56778  lb-140-82-114-25-:https ESTABLISHED
tcp        0    103 navneet-Inspiron:41154  del11s07-in-f14.1:https FIN_WAIT1
tcp        0      0 navneet-Inspiron:56026  whatsapp-cdn-shv-:https ESTABLISHED
tcp        0      0 navneet-Inspiron:46666  ec2-52-26-249-11.:https ESTABLISHED
tcp        0      0 navneet-Inspiron:39152  82.221.107.34.bc.g:http ESTABLISHED
tcp        0    103 navneet-Inspiron:58040  server-54-192-171:https FIN_WAIT1
tcp        0    103 navneet-Inspiron:58152  whatsapp-cdn-shv-:https FIN_WAIT1
tcp6       0    103 2405:201:6802:604:50240 del03s14-in-x03.1:https FIN_WAIT1
tcp6       0    103 2405:201:6802:604:49642 del03s07-in-x01.1:https FIN_WAIT1
tcp6       0      0 navneet-Inspiron:39116  2600:1901:0:38d7:::http ESTABLISHED
tcp6       0    103 2405:201:6802:604:56202 del03s14-in-x06.1:https FIN_WAIT1
tcp6       0      0 navneet-Inspiron:39112  2600:1901:0:38d7:::http ESTABLISHED
tcp6       0    103 2405:201:6802:604:55286 del11s05-in-x02.1:https FIN_WAIT1
tcp6       0    103 2405:201:6802:604:47304 del03s16-in-x16.1:https FIN_WAIT1
tcp6       0    103 2405:201:6802:604:50066 del03s09-in-x0e.1:https FIN_WAIT1
tcp6       0    103 2405:201:6802:604:34728 del03s09-in-x01.1:https FIN_WAIT1
tcp6       0    103 2405:201:6802:604:59686 del03s13-in-x04.1:https FIN_WAIT1
tcp6       0    103 2405:201:6802:604:43216 sc-in-xbd.1e100.n:https FIN_WAIT1
```

The number of TCP connections became 24, this is because some of the connections might have closed.

The Number of FIN_WAIT1 connections increased to 16, this is because the interface is down and we are no longer connected to the network. Putting the interface to downstate triggered this.

Some of them are still in Established state which will eventually get converted to Fin_wait1 state.

Finally, every connection will be closed , since the interface is not active now.