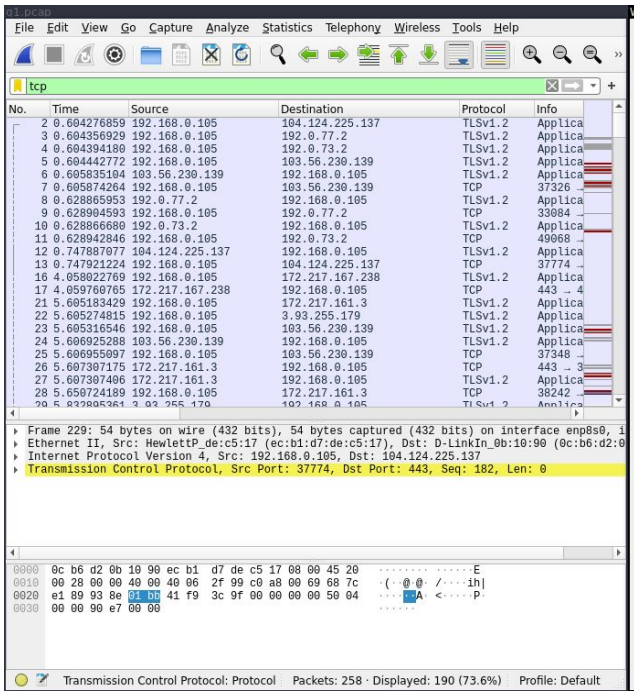
Computer Networks

Setu Gupta (2018190)

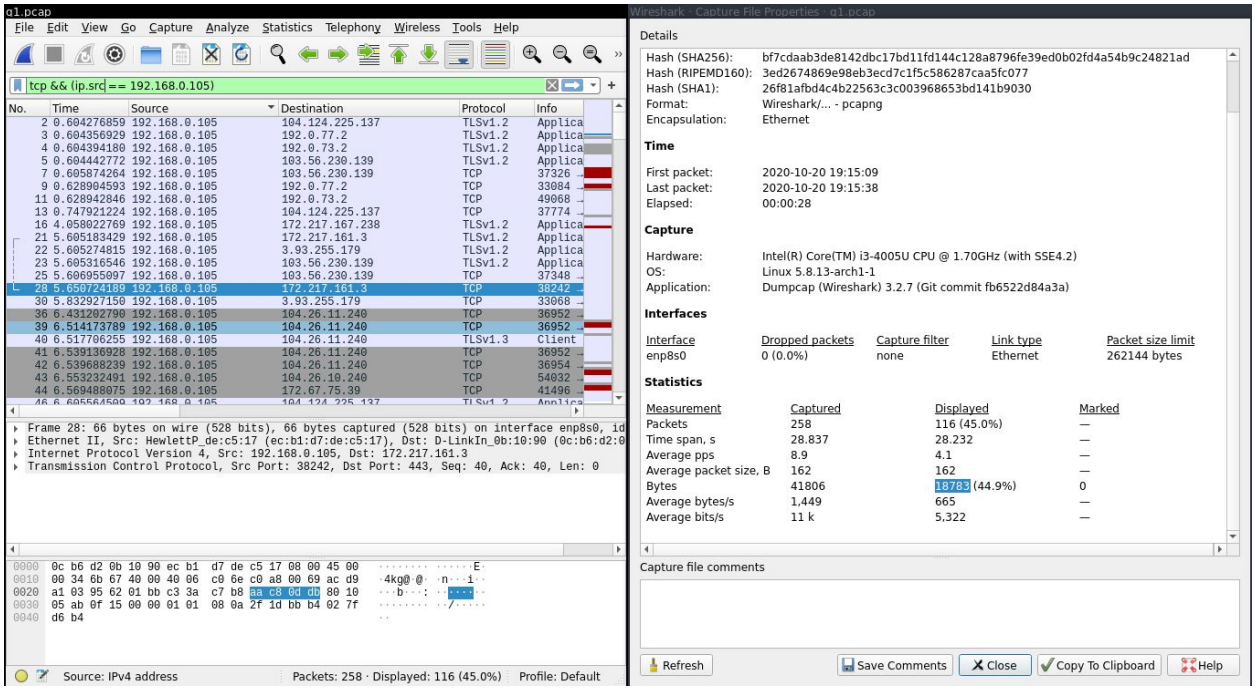
1. Capturing packets and analysing them
    a. Command used: `sudo tshark -i 1 -w q1.pcap -a duration:30`
    Note that 1st interface listed by `sudo tshark -D` is the ethernet port

```
~/Desktop/CN/hw3  master ?3  sudo tshark -i 1 -w q1.pcap -a duration:30
Running as user "root" and group "root". This could be dangerous.
Capturing on 'enp8s0'
258
```

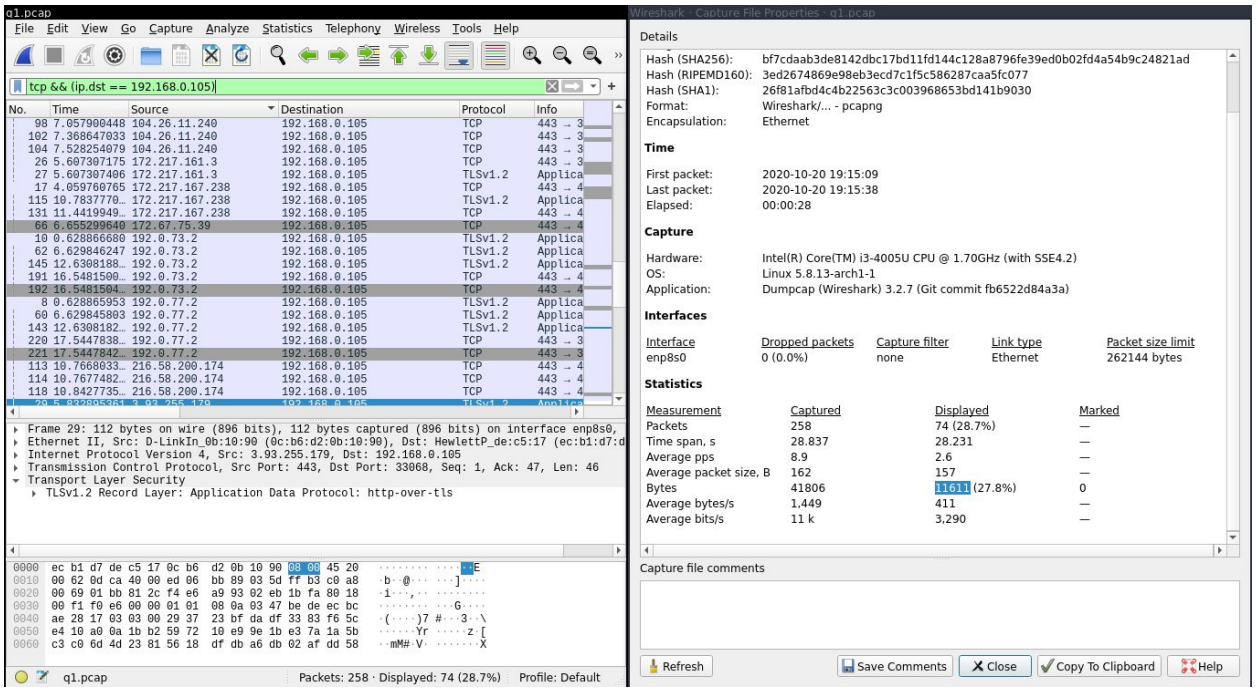
    b. There are 16 TCP connections



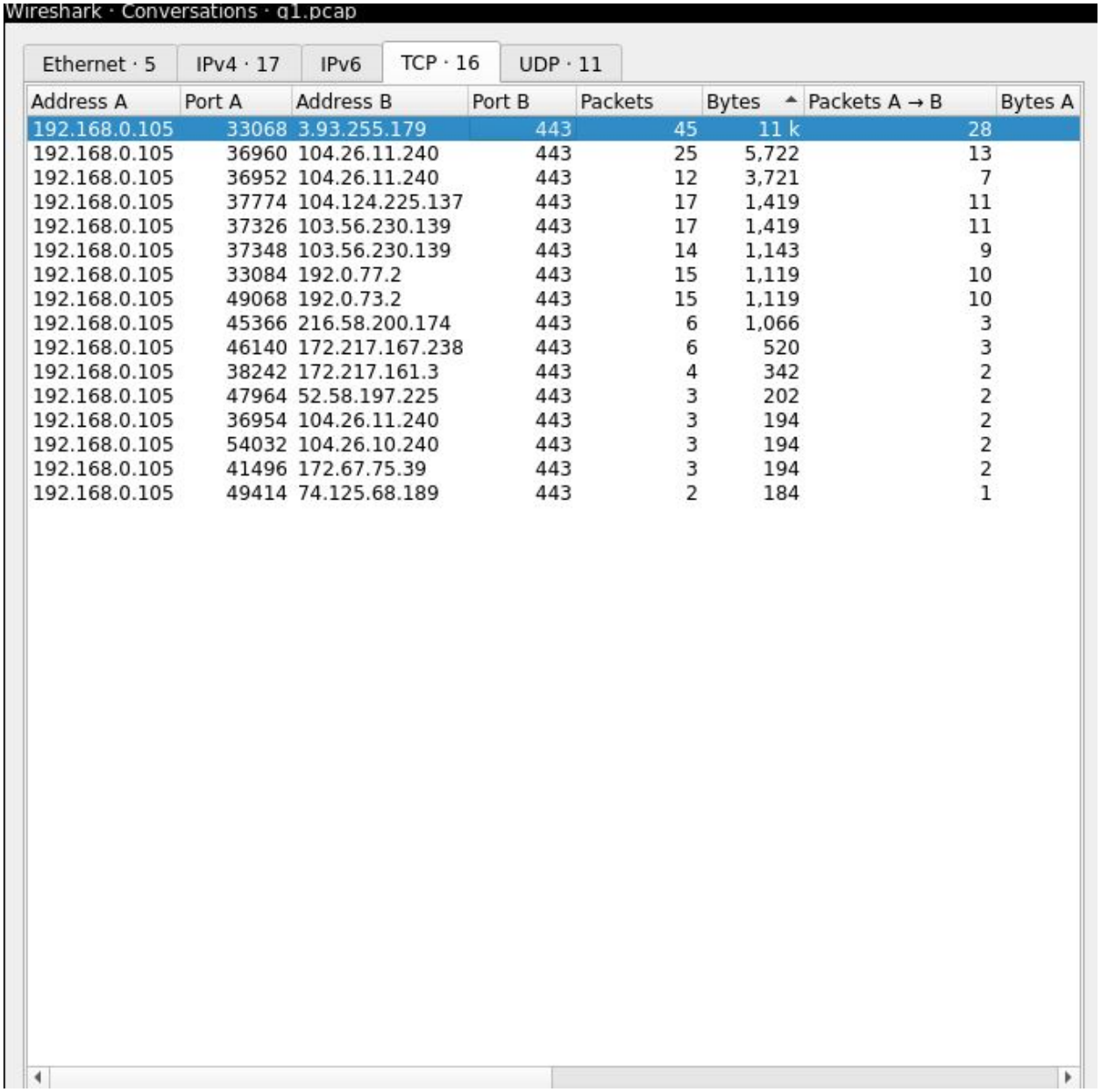
c. Upstream: 18783 bytes



Downstream: 11611bytes

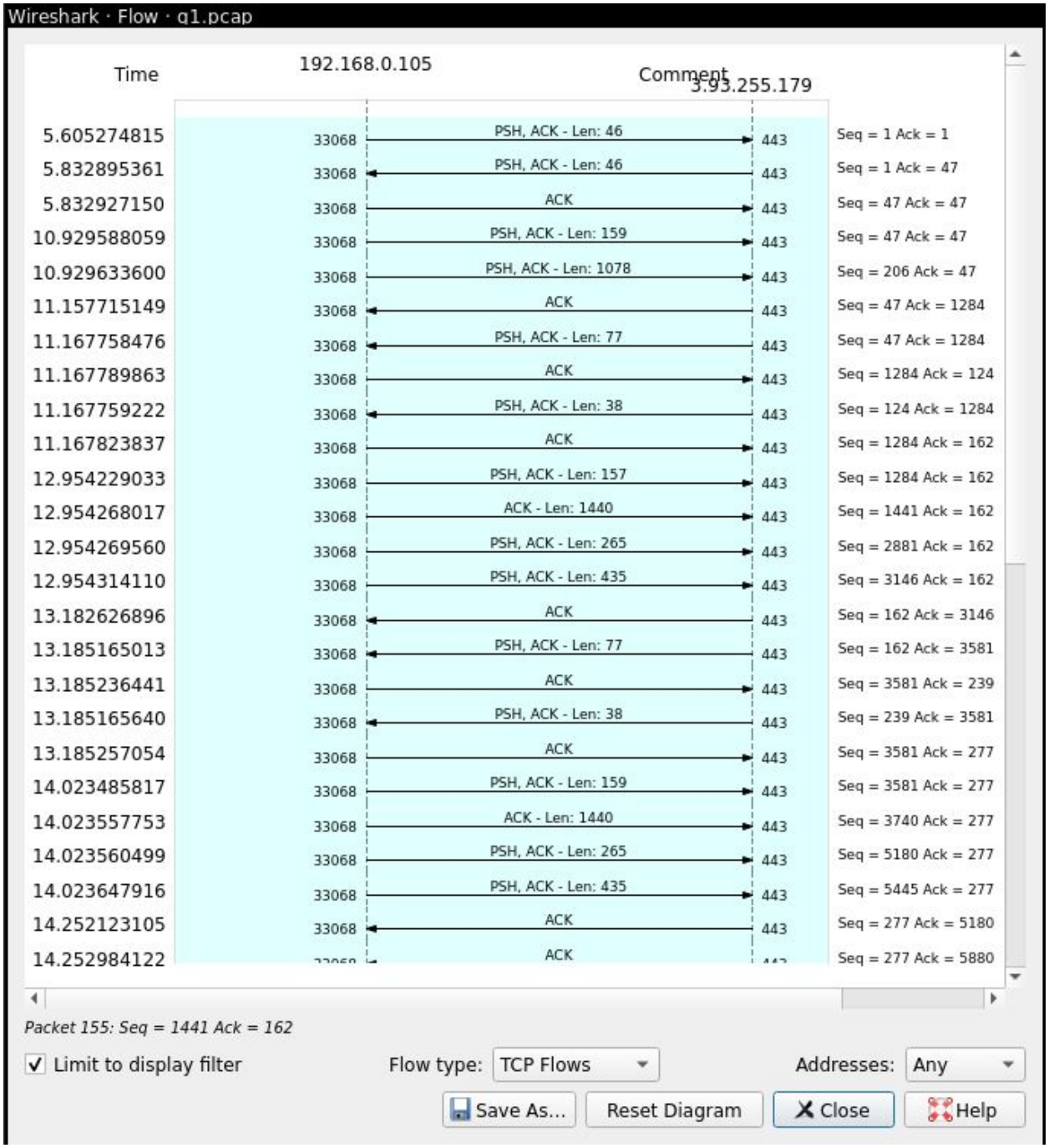


d. Connection with maximum number of bytes: 3.92.255.179

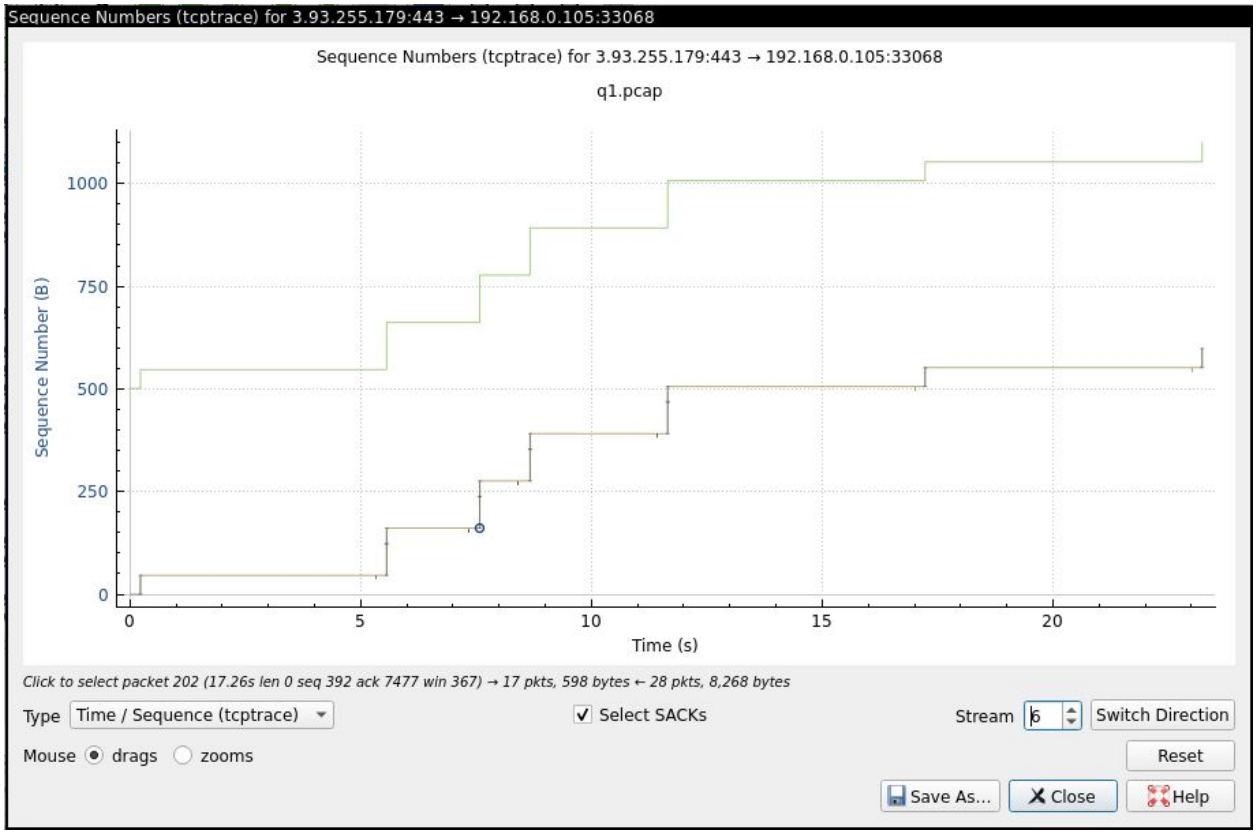


Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A
192.168.0.105	33068	3.93.255.179	443	45	11 k	28	
192.168.0.105	36960	104.26.11.240	443	25	5,722	13	
192.168.0.105	36952	104.26.11.240	443	12	3,721	7	
192.168.0.105	37774	104.124.225.137	443	17	1,419	11	
192.168.0.105	37326	103.56.230.139	443	17	1,419	11	
192.168.0.105	37348	103.56.230.139	443	14	1,143	9	
192.168.0.105	33084	192.0.77.2	443	15	1,119	10	
192.168.0.105	49068	192.0.73.2	443	15	1,119	10	
192.168.0.105	45366	216.58.200.174	443	6	1,066	3	
192.168.0.105	46140	172.217.167.238	443	6	520	3	
192.168.0.105	38242	172.217.161.3	443	4	342	2	
192.168.0.105	47964	52.58.197.225	443	3	202	2	
192.168.0.105	36954	104.26.11.240	443	3	194	2	
192.168.0.105	54032	104.26.10.240	443	3	194	2	
192.168.0.105	41496	172.67.75.39	443	3	194	2	
192.168.0.105	49414	74.125.68.189	443	2	184	1	

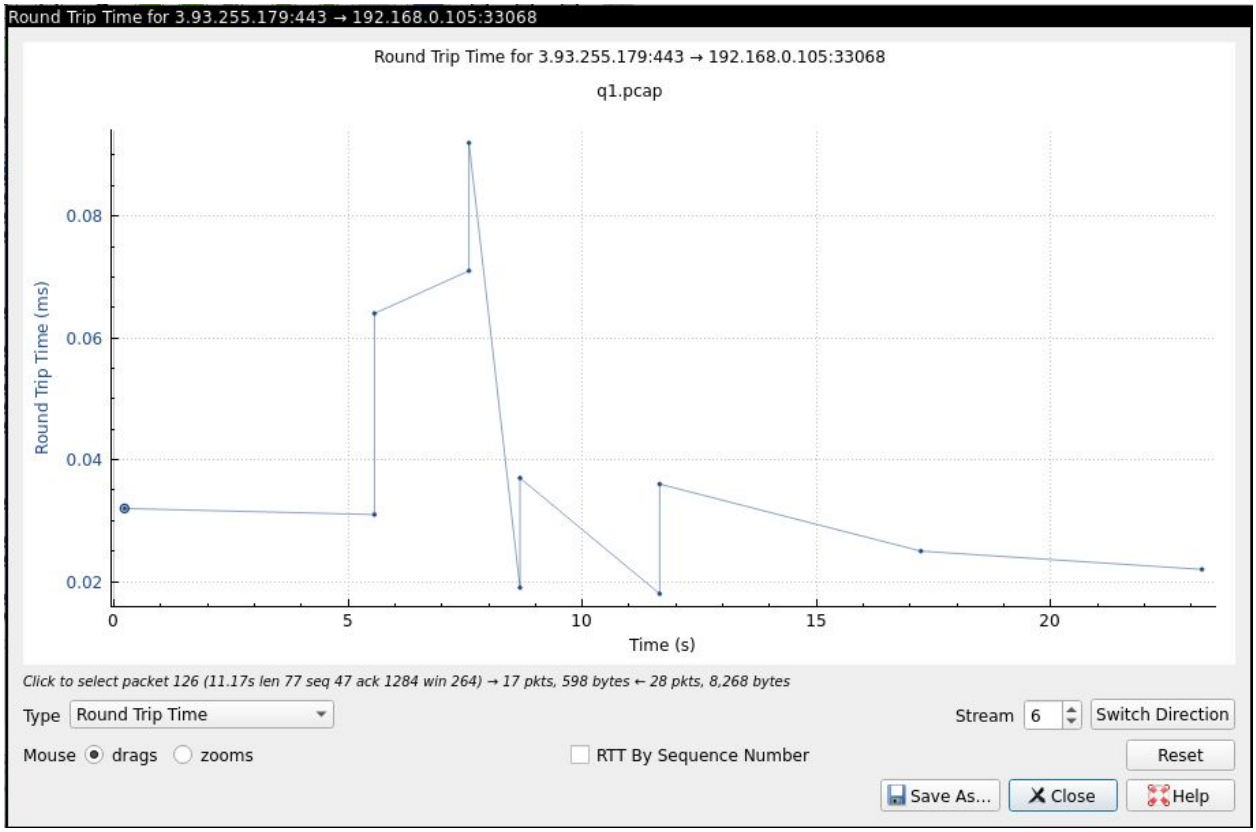
Sequence number progression via flow graph



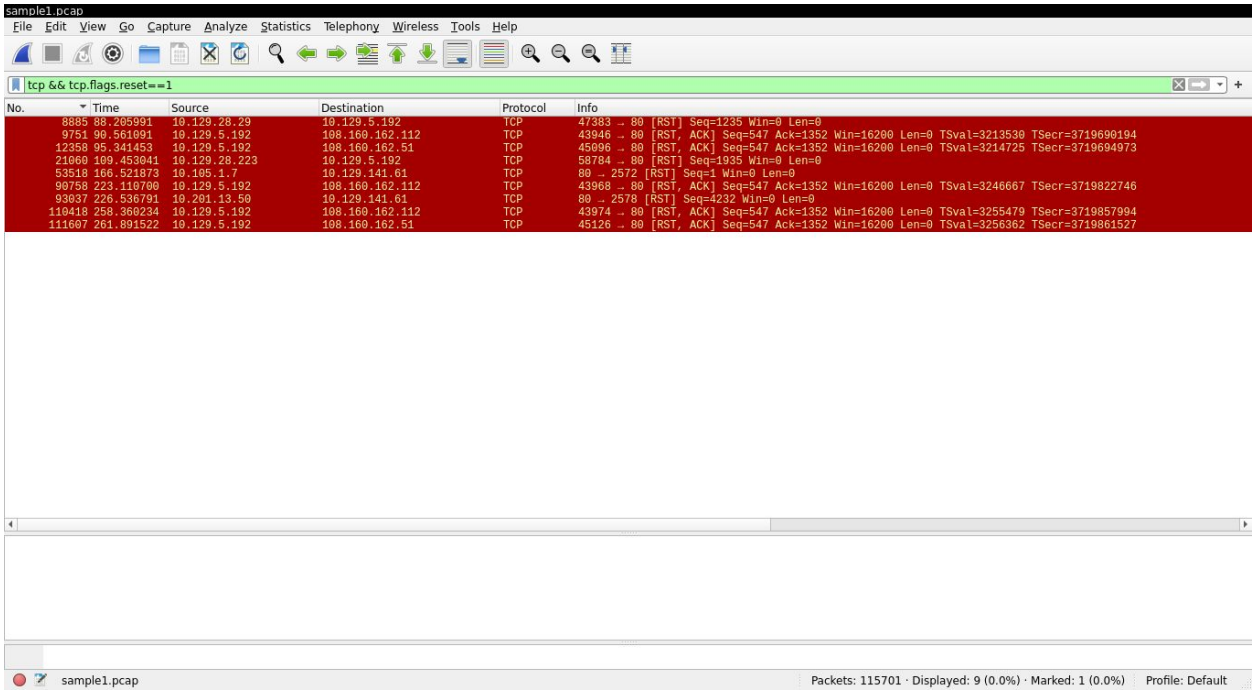
TCP stream graph



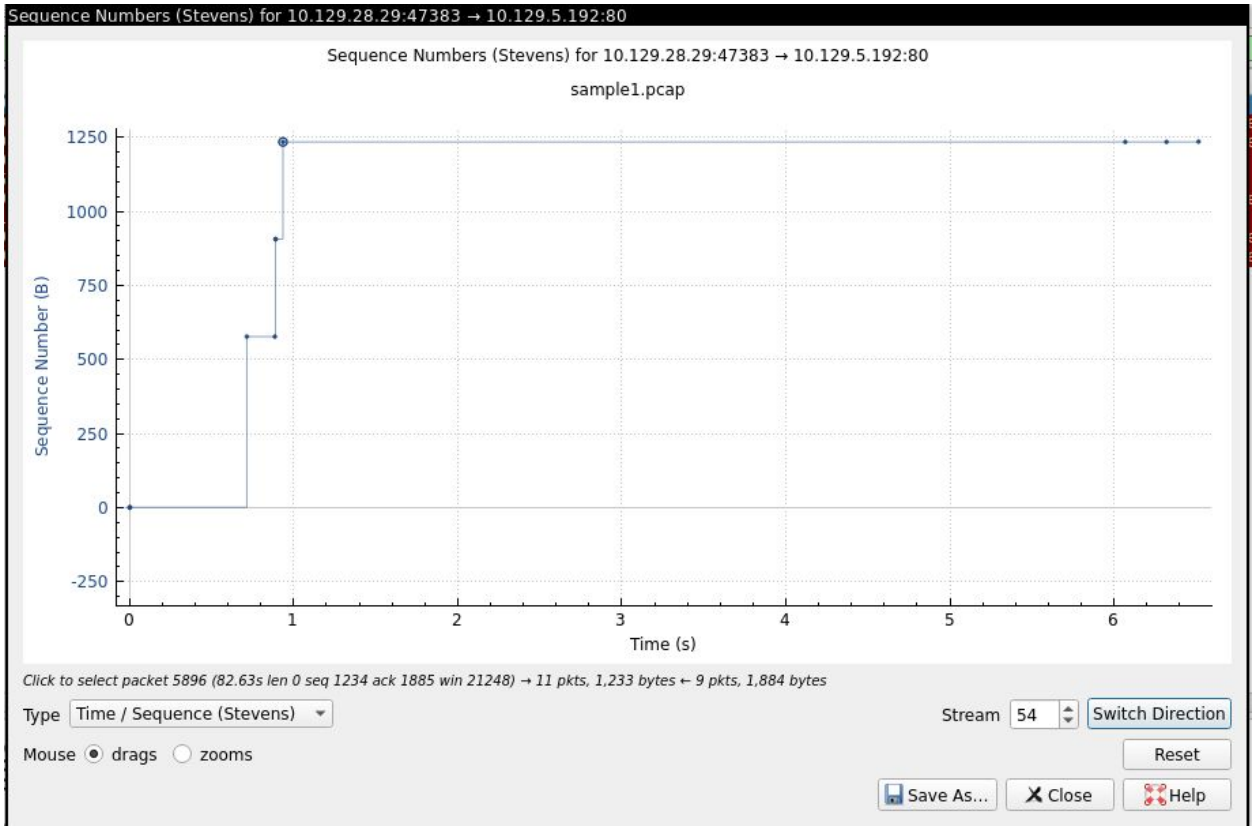
e. RTT graph



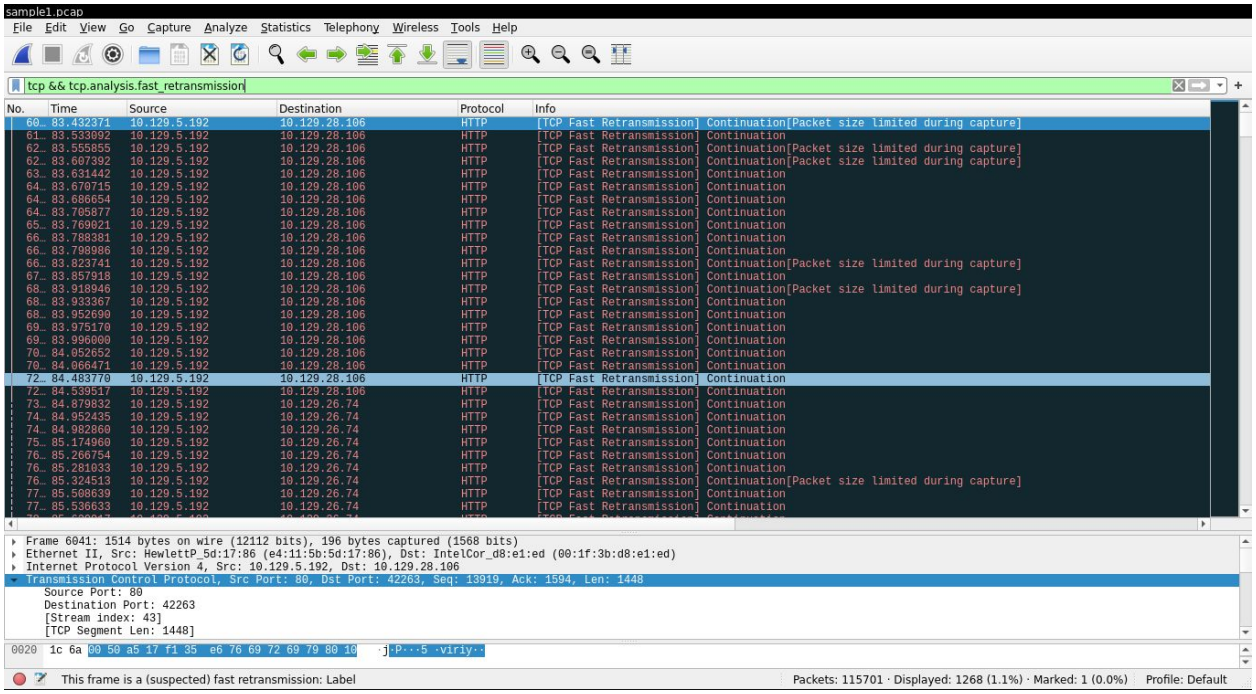
f. Source: https://osqa-ask.wireshark.org/questions/25727/how-to-apply-filter-to-view-tcp-connection-timeout



In TCP stream graph, this can be seen as the sequence number not increasing for a long time.



g. 1268 fast retransmission packets



2. netstat
    a. Not matching exactly as by the time netstat runs, the connections may change.

```
~/Desktop/CN/hw3  master ?3  netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 unknown:36960           104.26.11.240:https     ESTABLISHED
tcp        0      0 unknown:45364           nrt12s11-in-f174.:https ESTABLISHED
tcp        0      0 unknown:42350           del03s13-in-f1.1e:https ESTABLISHED
tcp        0      0 unknown:55576           ec2-54-71-45-57.u:https ESTABLISHED
tcp        0      0 unknown:39040           del11s05-in-f14.1:https ESTABLISHED
tcp        0      0 unknown:38374           del11s03-in-f4.1e:https ESTABLISHED
tcp        0      0 unknown:39158           maa03s19-in-f99.1:https ESTABLISHED
tcp        0      0 unknown:49068           192.0.73.2:https        TIME_WAIT
tcp        0      0 unknown:56428           82.221.107.34.:www-http TIME_WAIT
tcp        0      0 unknown:55152           del11s05-in-f13.1:https ESTABLISHED
tcp        0      0 unknown:45366           nrt12s11-in-f174.:https ESTABLISHED
tcp        0      0 unknown:41088           del03s16-in-f14.1:https ESTABLISHED
tcp        0      0 unknown:56426           82.221.107.34.:www-http TIME_WAIT
tcp        0      0 unknown:39106           del11s05-in-f14.1:https ESTABLISHED
tcp        0      0 unknown:33084           i2.wp.com:https         TIME_WAIT
tcp        0      0 unknown:36566           nrt12s11-in-f170.:https ESTABLISHED
tcp        0      0 unknown:38242           del03s10-in-f3.1e:https ESTABLISHED
tcp        0      0 unknown:49414           sc-in-f189.1e100.:https ESTABLISHED
tcp        0      0 unknown:46140           del11s04-in-f14.1:https ESTABLISHED
tcp        0      0 unknown:33068           ec2-3-93-255-179.:https ESTABLISHED
```

    b. 2 in TIME_WAIT, 6 in ESTABLISHED and 1 in FIN_WAIT1

```
~/Desktop/CN/hw3  master ?3  netstat -at | grep tcp | grep TIME_WAIT
tcp        0      0 unknown:43688           82.221.107.34.:www-http TIME_WAIT
tcp        0      0 unknown:43692           82.221.107.34.:www-http TIME_WAIT
```

```
~/Desktop/CN/hw3  master ?3  netstat -at | grep tcp | grep ESTABLISHED
tcp        0      0 unknown:46338           nrt12s11-in-f174.:https ESTABLISHED
tcp        0      0 unknown:46340           nrt12s11-in-f174.:https ESTABLISHED
tcp        0      0 unknown:35060           ec2-34-216-9-227.:https ESTABLISHED
tcp        0      0 unknown:43708           82.221.107.34.:www-http ESTABLISHED
tcp        0      0 unknown:43710           82.221.107.34.:www-http ESTABLISHED
tcp        0      0 unknown:54290           sc-in-f189.1e100.:https ESTABLISHED
```

```
~/Desktop/CN/hw3  master ?3  netstat -at | grep tcp | grep FIN_WAIT1
tcp        0    294 192.168.0.105:44304     82.221.107.34.:www-http FIN_WAIT1
```

c. The connections go to FIN_WAIT1

Before:

```
~/Desktop/CN/hw3  master ?3  netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 unknown:52062           ec2-54-213-36-182:https ESTABLISHED
tcp        0      0 unknown:45196           nrt12s11-in-f174.:https ESTABLISHED
tcp        0    103 192.168.0.158:54930     sc-in-f189.1e100.:https FIN_WAIT1
tcp        0      0 unknown:45960           del11s04-in-f14.1:https ESTABLISHED
tcp        0     67 192.168.0.158:35478     ec2-54-200-0-167.:https FIN_WAIT1
tcp        0      0 unknown:56404           82.221.107.34.:www-http ESTABLISHED
tcp        0      0 unknown:40760           del03s10-in-f10.1:https ESTABLISHED
tcp        0      0 unknown:49250           sc-in-f189.1e100.:https ESTABLISHED
tcp        0      0 unknown:40762           del03s10-in-f10.1:https ESTABLISHED
tcp        0    124 192.168.0.158:39718     ec2-52-45-85-77.c:https FIN_WAIT1
tcp        0    294 192.168.0.158:44354     82.221.107.34.:www-http FIN_WAIT1
tcp        0      0 unknown:45194           nrt12s11-in-f174.:https ESTABLISHED
tcp        0      0 unknown:56406           82.221.107.34.:www-http ESTABLISHED
~/Desktop/CN/hw3  master ?3  sudo ifconfig enp8s0 down
```

After:

```
~/Desktop/CN/hw3  master ?3  netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0     67 192.168.0.107:52062     54.213.36.182:https     FIN_WAIT1
tcp        0    103 192.168.0.105:45196     216.58.200.174:https    FIN_WAIT1
tcp        0    103 192.168.0.158:54930     74.125.68.189:https     FIN_WAIT1
tcp        0  47971 192.168.0.105:45960     172.217.167.238:https   FIN_WAIT1
tcp        0     67 192.168.0.158:35478     54.200.0.167:https      FIN_WAIT1
tcp        0    103 192.168.0.105:40760     172.217.161.10:https    FIN_WAIT1
tcp        0    103 192.168.0.105:49250     74.125.68.189:https     FIN_WAIT1
tcp        0    103 192.168.0.105:40762     172.217.161.10:https    FIN_WAIT1
tcp        0    124 192.168.0.158:39718     52.45.85.77:https       FIN_WAIT1
tcp        0    103 192.168.0.105:45194     216.58.200.174:https    FIN_WAIT1
tcp        0    294 192.168.0.107:56406     34.107.221.82:www-http  FIN_WAIT1
```