

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

The image displays the Wireshark network protocol analyzer interface. The left pane shows the packet list with 258 packets captured on interface enp8s0. The right pane shows the packet details for the selected packet (No. 229), which is a TCP Reset (RST) packet from 192.168.0.105 to 104.124.225.137. The bottom pane shows the raw packet data in hexadecimal and ASCII.

Packet List (Left Pane):

No.	Time	Source	Destination	Protocol	Info
2	0.664276859	192.168.0.105	104.124.225.137	TLSv1.2	Applica
3	0.664356929	192.168.0.105	192.0.77.2	TLSv1.2	Applica
4	0.664394180	192.168.0.105	192.0.73.2	TLSv1.2	Applica
5	0.664442772	192.168.0.105	103.56.230.139	TLSv1.2	Applica
6	0.665835104	103.56.230.139	192.168.0.105	TLSv1.2	Applica
7	0.665874264	192.168.0.105	103.56.230.139	TCP	37326 ->
8	0.628865953	192.0.77.2	192.168.0.105	TLSv1.2	Applica
9	0.628904593	192.168.0.105	192.0.77.2	TCP	33084 ->
10	0.628866689	192.0.73.2	192.168.0.105	TLSv1.2	Applica
11	0.628942846	192.168.0.105	192.0.73.2	TCP	49068 ->
12	0.747887977	104.124.225.137	192.168.0.105	TLSv1.2	Applica
13	0.747921224	192.168.0.105	104.124.225.137	TCP	37774 ->
16	4.058022769	192.168.0.105	172.217.167.238	TLSv1.2	Applica
17	4.059786765	172.217.167.238	192.168.0.105	TCP	443 -> 4
21	5.605183429	192.168.0.105	172.217.161.3	TLSv1.2	Applica
22	5.605274815	192.168.0.105	3.93.255.179	TLSv1.2	Applica
23	5.605316546	192.168.0.105	103.56.230.139	TLSv1.2	Applica
24	5.606952588	103.56.230.139	192.168.0.105	TLSv1.2	Applica
25	5.606955097	192.168.0.105	103.56.230.139	TCP	37348 ->
26	5.607307175	172.217.161.3	192.168.0.105	TCP	443 -> 8
27	5.607307486	172.217.161.3	192.168.0.105	TLSv1.2	Applica
28	5.60724189	192.168.0.105	172.217.161.3	TCP	38242 ->
29	5.823805361	2.02.265.170	102.168.0.105	TLSv1.2	Applica

Packet Details (Right Pane):

Frame 229: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface enp8s0, 1 Ethernet II, Src: HewlettP_de:c5:17 (ec:b1:d7:de:c5:17), Dst: D-LinkIn_0b:10:90 (0c:b6:d2:0), Internet Protocol Version 4, Src: 192.168.0.105, Dst: 104.124.225.137, Transmission Control Protocol, Src Port: 37774, Dst Port: 443, Seq: 182, Len: 0

Raw Data (Bottom Pane):

```
0000  0c b6 d2 0b 10 90 ec b1 d7 de c5 17 08 00 45 20 .....E
0010  00 28 00 00 40 00 40 06 2f 99 c0 a8 00 69 68 7c ..(..@.@:/....ih|
0020  e1 89 93 8e 31 db 41 f9 3c 9f 00 00 00 50 04 ....A<.....P.
0030  00 00 00 e7 00 00 .....
```

c. Upstream: 18783 bytes

Wireshark - Capture File Properties - q1.pcap

Details

Hash (SHA256): bf7cdaab3de8142dbc17bd11fd144c128a8796fe39ed0b02fd4a54b9c24821ad
Hash (RIPEMD160): 3ed2674869e98eb3ecd7c1f5c586287caa5fc077
Hash (SHA1): 26f81afbd4c4b22563c3c003968653bd141b9030
Format: Wireshark/... - pcapng
Encapsulation: Ethernet

Time

First packet: 2020-10-20 19:15:09
Last packet: 2020-10-20 19:15:38
Elapsed: 00:00:28

Capture

Hardware: Intel(R) Core(TM) i3-4005U CPU @ 1.70GHz (with SSE4.2)
OS: Linux 5.8.13-arch1-1
Application: Dumpcap (Wireshark) 3.2.7 (Git commit fb6522d84a3a)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit
enp8s0	0 (0.0%)	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	258	116 (45.0%)	—
Time span, s	28.837	28.232	—
Average pps	8.9	4.1	—
Average packet size, B	162	162	—
Bytes	41806	18783 (44.9%)	0
Average bytes/s	1,449	665	—
Average bits/s	11 k	5,322	—

Capture file comments

Refresh Save Comments Close Copy To Clipboard Help

q1.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp && (ip.src == 192.168.0.105)

No.	Time	Source	Destination	Protocol	Info
2	0.604276850	192.168.0.105	104.124.225.137	TLSv1.2	Applica
3	0.604356929	192.168.0.105	192.0.77.2	TLSv1.2	Applica
4	0.604394180	192.168.0.105	192.0.73.2	TLSv1.2	Applica
5	0.604442772	192.168.0.105	103.56.230.139	TLSv1.2	Applica
7	0.605874264	192.168.0.105	103.56.230.139	TCP	37326 →
9	0.628904593	192.168.0.105	192.0.77.2	TCP	33084 →
11	0.628942846	192.168.0.105	192.0.73.2	TCP	49088 →
13	0.747921224	192.168.0.105	104.124.225.137	TCP	37774 →
14	0.058022769	192.168.0.105	172.217.167.238	TLSv1.2	Applica
21	5.605183429	192.168.0.105	172.217.161.3	TLSv1.2	Applica
22	5.605274815	192.168.0.105	3.93.255.179	TLSv1.2	Applica
23	5.605316546	192.168.0.105	103.56.230.139	TLSv1.2	Applica
25	5.606955097	192.168.0.105	103.56.230.139	TCP	37348 →
28	5.650724189	192.168.0.105	172.217.161.3	TCP	38242 →
30	5.832927150	192.168.0.105	3.93.255.179	TCP	33088 →
36	6.431202790	192.168.0.105	104.26.11.240	TCP	36952 →
39	6.514173789	192.168.0.105	104.26.11.240	TCP	36952 →
40	6.517706255	192.168.0.105	104.26.11.240	TLSv1.3	Client
41	6.539136928	192.168.0.105	104.26.11.240	TCP	36952 →
42	6.539688239	192.168.0.105	104.26.11.240	TCP	36954 →
43	6.553232491	192.168.0.105	104.26.11.240	TCP	54932 →
44	6.569488075	192.168.0.105	172.67.75.39	TCP	41496 →

Frame 28: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface enp8s0, id Ethernet II, Src: HewlettP_de:c5:17 (ec:b1:d7:de:c5:17), Dst: D-LinkIn_0b:10:90 (0c:b6:d2:00:10:90), Internet Protocol Version 4, Src: 192.168.0.105, Dst: 172.217.161.3, Transmission Control Protocol, Src Port: 38242, Dst Port: 443, Seq: 40, Len: 0

Source: IPv4 address Packets: 258 · Displayed: 116 (45.0%) Profile: Default

Downstream: 11611bytes

Wireshark - Capture File Properties - q1.pcap

Details

Hash (SHA256): bf7cdaab3de8142dbc17bd11fd144c128a8796fe39ed0b02fd4a54b9c24821ad
Hash (RIPEMD160): 3ed2674869e98eb3ecd7c1f5c586287caa5fc077
Hash (SHA1): 26f81afbd4c4b22563c3c003968653bd141b9030
Format: Wireshark/... - pcapng
Encapsulation: Ethernet

Time

First packet: 2020-10-20 19:15:09
Last packet: 2020-10-20 19:15:38
Elapsed: 00:00:28

Capture

Hardware: Intel(R) Core(TM) i3-4005U CPU @ 1.70GHz (with SSE4.2)
OS: Linux 5.8.13-arch1-1
Application: Dumpcap (Wireshark) 3.2.7 (Git commit fb6522d84a3a)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit
enp8s0	0 (0.0%)	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	258	74 (28.7%)	—
Time span, s	28.837	28.231	—
Average pps	8.9	2.6	—
Average packet size, B	162	157	—
Bytes	41806	11611 (27.8%)	0
Average bytes/s	1,449	411	—
Average bits/s	11 k	3,290	—

Capture file comments

Refresh Save Comments Close Copy To Clipboard Help

q1.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp && (ip.dst == 192.168.0.105)

No.	Time	Source	Destination	Protocol	Info
98	7.057900448	104.26.11.240	192.168.0.105	TCP	443 → 3
102	7.368647033	104.26.11.240	192.168.0.105	TCP	443 → 3
104	7.528254079	104.26.11.240	192.168.0.105	TCP	443 → 3
26	5.607307175	172.217.161.3	192.168.0.105	TCP	443 → 3
27	5.607307406	172.217.161.3	192.168.0.105	TLSv1.2	Applica
17	4.059760705	172.217.167.238	192.168.0.105	TCP	443 → 4
115	10.7837770	172.217.167.238	192.168.0.105	TLSv1.2	Applica
131	11.4419949	172.217.167.238	192.168.0.105	TCP	443 → 4
66	6.655299640	172.67.75.39	192.168.0.105	TCP	443 → 4
10	0.628866680	192.0.73.2	192.168.0.105	TLSv1.2	Applica
62	6.629846247	192.0.73.2	192.168.0.105	TLSv1.2	Applica
145	12.6398188	192.0.73.2	192.168.0.105	TLSv1.2	Applica
191	16.5481500	192.0.73.2	192.168.0.105	TCP	443 → 4
192	16.5481504	192.0.73.2	192.168.0.105	TCP	443 → 4
8	0.628865953	192.0.77.2	192.168.0.105	TLSv1.2	Applica
60	6.629845893	192.0.77.2	192.168.0.105	TLSv1.2	Applica
143	12.6398182	192.0.77.2	192.168.0.105	TLSv1.2	Applica
220	17.5447838	192.0.77.2	192.168.0.105	TCP	443 → 3
221	17.5447842	192.0.77.2	192.168.0.105	TCP	443 → 3
113	10.7608933	216.58.200.174	192.168.0.105	TCP	443 → 4
114	10.7677482	216.58.200.174	192.168.0.105	TCP	443 → 4
118	10.8427735	216.58.200.174	192.168.0.105	TCP	443 → 4

Frame 29: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface enp8s0, id Ethernet II, Src: D-LinkIn_0b:10:90 (0c:b6:d2:0b:10:90), Dst: HewlettP_de:c5:17 (ec:b1:d7:de:c5:17), Internet Protocol Version 4, Src: 3.93.255.179, Dst: 192.168.0.105, Transmission Control Protocol, Src Port: 443, Dst Port: 33068, Seq: 1, Ack: 47, Len: 46, Transport Layer Security, TLSv1.2 Record Layer: Application Data Protocol: http-over-tls

Source: IPv4 address Packets: 258 · Displayed: 74 (28.7%) Profile: Default

d. Connection with maximum number of bytes: 3.92.255.179

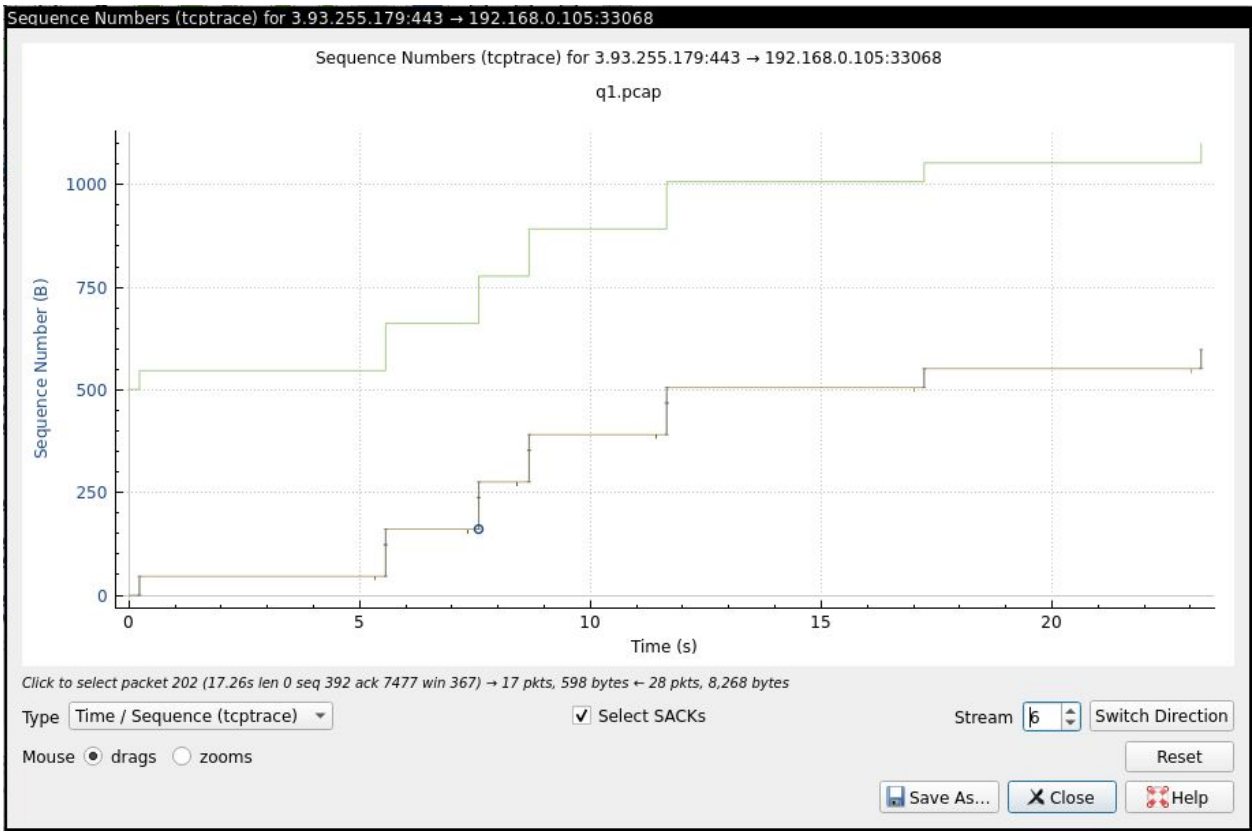
Wireshark · Conversations · q1.pcap

Ethernet · 5		IPv4 · 17		IPv6		TCP · 16		UDP · 11	
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		

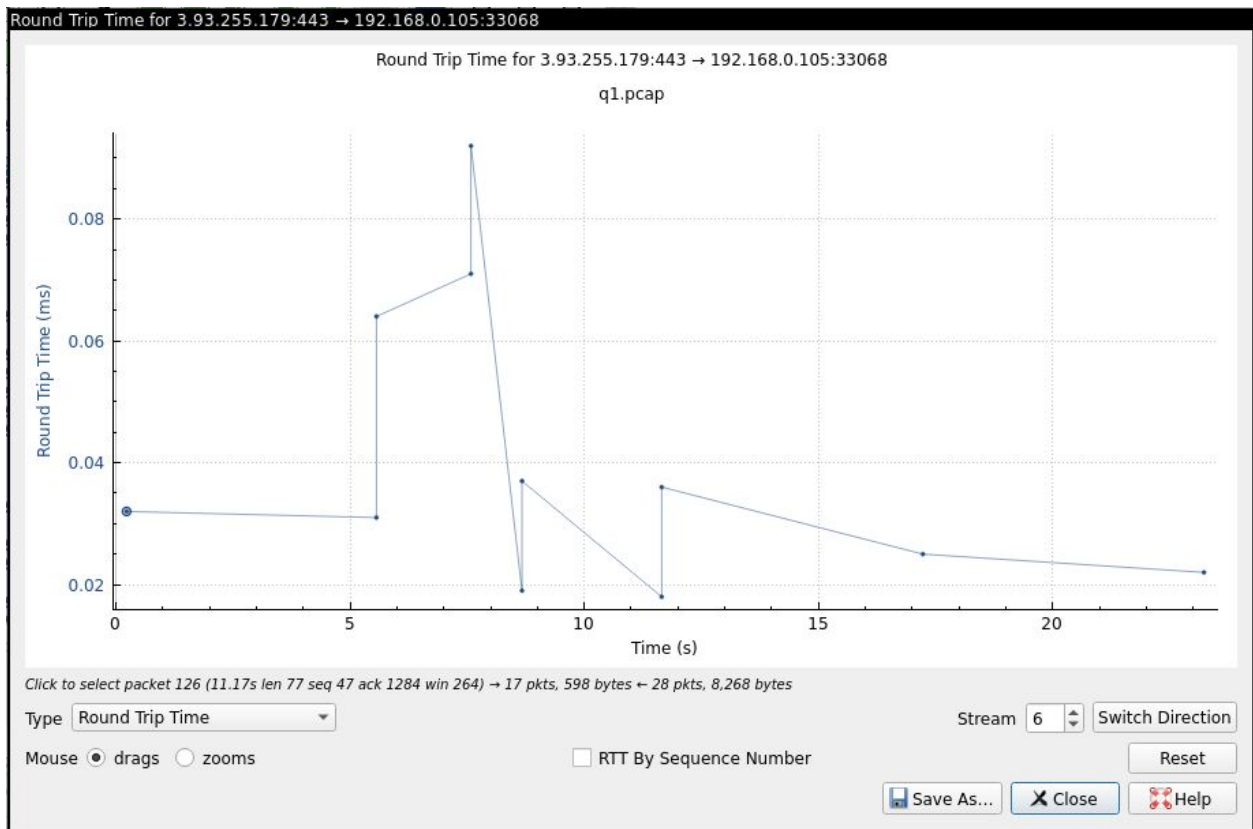
Sequence number progression via flow graph



TCP stream graph



e. RTT graph



f. Source:

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

sample1.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

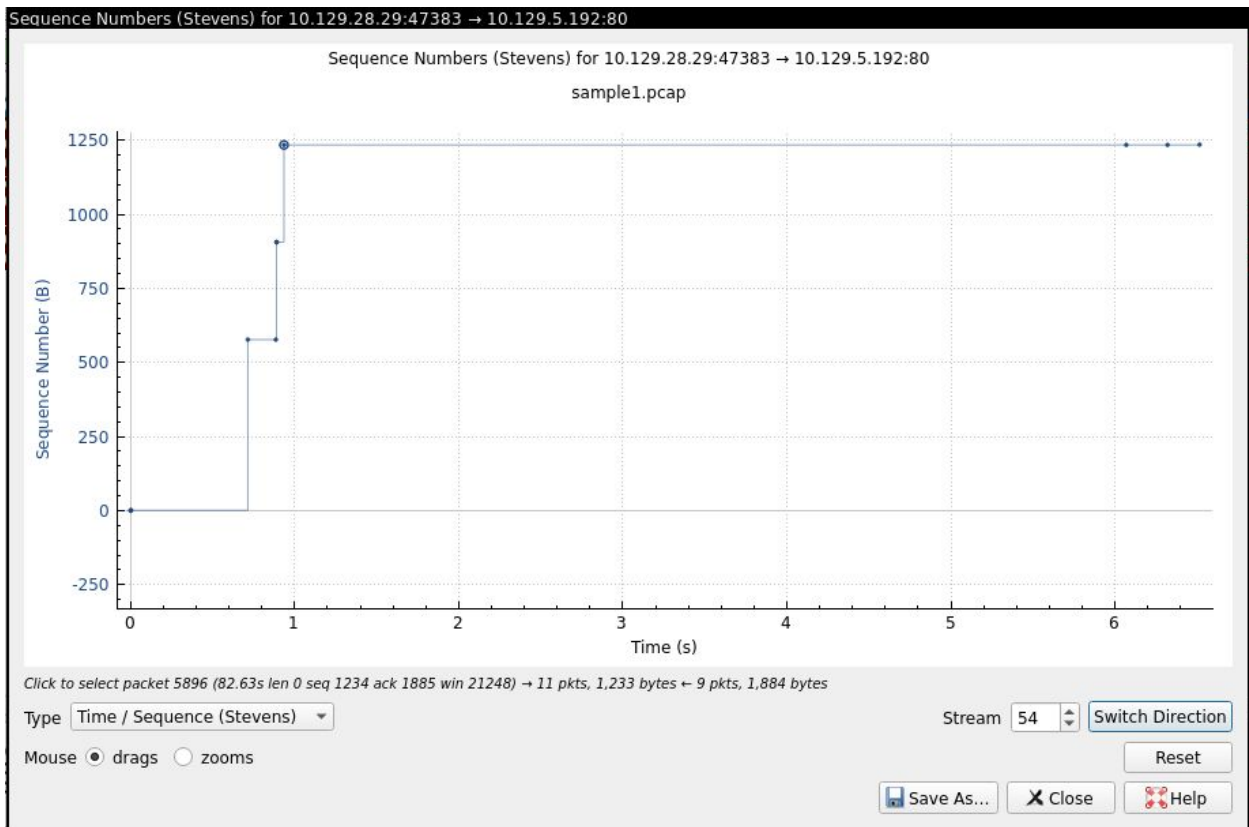
tcp && tcp.flags.reset==1

No.	Time	Source	Destination	Protocol	Info
8885	88.295991	10.129.5.192	10.129.5.192	TCP	47383 → 80 [RST] Seq=1235 Win=0 Len=0
9751	90.561091	10.129.5.192	108.160.162.112	TCP	43946 → 80 [RST, ACK] Seq=547 Ack=1352 Win=16200 Len=0 TSval=3213530 TSecr=3719690194
12358	95.341453	10.129.5.192	108.160.162.51	TCP	45096 → 80 [RST, ACK] Seq=547 Ack=1352 Win=16200 Len=0 TSval=3214725 TSecr=3719694973
21060	109.453841	10.129.28.223	10.129.5.192	TCP	58784 → 80 [RST] Seq=1935 Win=0 Len=0
53518	166.521873	10.105.1.7	10.129.141.61	TCP	80 → 2572 [RST] Seq=1 Win=0 Len=0
90758	223.110708	10.129.5.192	108.160.162.112	TCP	43968 → 80 [RST, ACK] Seq=547 Ack=1352 Win=16200 Len=0 TSval=3246667 TSecr=3719822746
93637	226.536791	10.201.13.50	10.129.141.61	TCP	80 → 2578 [RST] Seq=4232 Win=0 Len=0
119418	258.369234	10.129.5.192	108.160.162.112	TCP	43974 → 80 [RST, ACK] Seq=547 Ack=1352 Win=16200 Len=0 TSval=3255479 TSecr=3719857994
111667	261.891522	10.129.5.192	108.160.162.51	TCP	45126 → 80 [RST, ACK] Seq=547 Ack=1352 Win=16200 Len=0 TSval=3256362 TSecr=3719861527

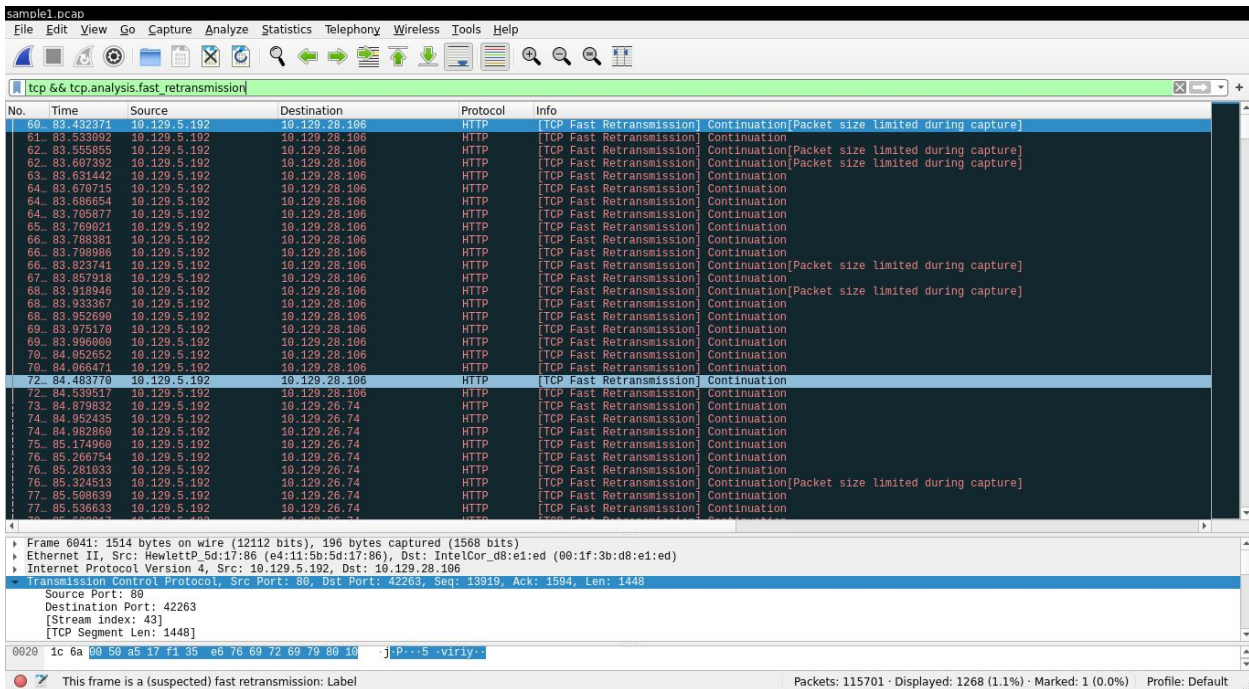
sample1.pcap

Packets: 115701 · Displayed: 9 (0.0%) · Marked: 1 (0.0%) Profile: Default

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
```