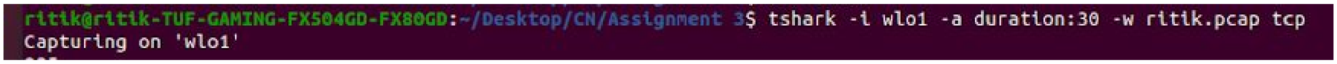
Assignment 3
Ritik Garg | 2018305

Answer 1.

(a). I am using tshark for capturing the packets.

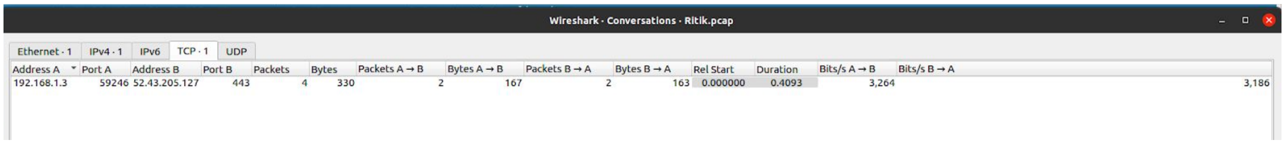
Command: **tshark -i wlo1 -a duration:30 -w Ritik.pcap tcp**



```
ritik@ritik-TUF-GAMING-FX504GD-FX80GD:~/Desktop/CN/Assignment 3$ tshark -i wlo1 -a duration:30 -w ritik.pcap tcp
Capturing on 'wlo1'
```

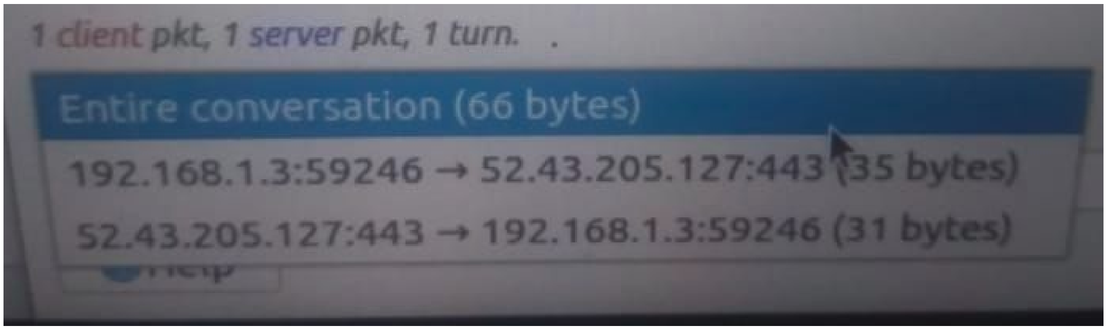
(b). Analysing the packets using wireshark.

Number of TCP connections: Under the Statistics and Conversation section. 1 TCP connections are there. Address A and B are the communicating peers to which it is trying to communicate.



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
192.168.1.3	59246	52.43.205.127	443	4	330	2	167	2	163	0.000000	0.4093	3,264	3,186

(c). Individual data transferred is there in the TCP section. We can check the overall data transmission under the TCP stream section by right clicking the packet.



1 client pkt, 1 server pkt, 1 turn.

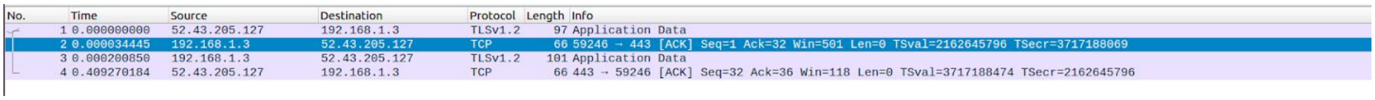
Entire conversation (66 bytes)

192.168.1.3:59246 → 52.43.205.127:443 (35 bytes)

52.43.205.127:443 → 192.168.1.3:59246 (31 bytes)

Entire communication was 66 bytes.

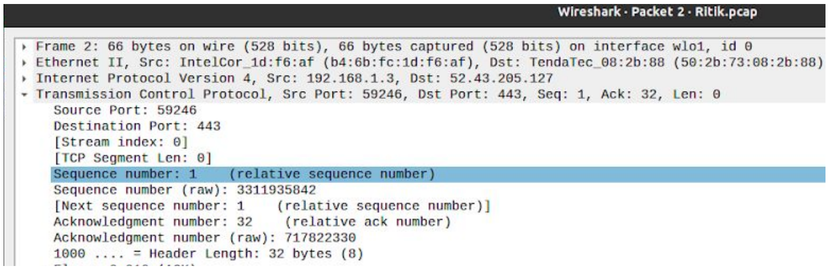
(d). For this double click the length section and it will arrange them in descending order. Check the connection with max length in TCP.



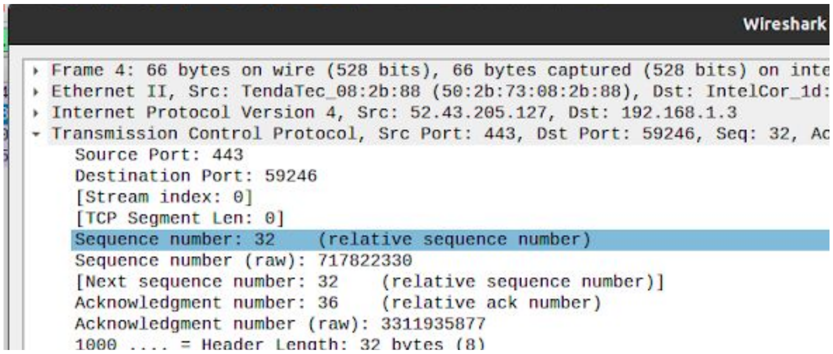
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	52.43.205.127	192.168.1.3	TLSv1.2	97	Application Data
2	0.000034445	192.168.1.3	52.43.205.127	TCP	66	59246 → 443 [ACK] Seq=1 Ack=32 Win=501 Len=0 TSval=2162645796 TSecr=3717188069
3	0.000200850	192.168.1.3	52.43.205.127	TLSv1.2	101	Application Data
4	0.409270184	52.43.205.127	192.168.1.3	TCP	66	443 → 59246 [ACK] Seq=32 Ack=36 Win=118 Len=0 TSval=3717188474 TSecr=2162645796

The one selected is the connection with max length.

To view the sequence number progress in the mid tab.
Apply the filter for that connection (by right clicking or by filter). Now check the sequence number.



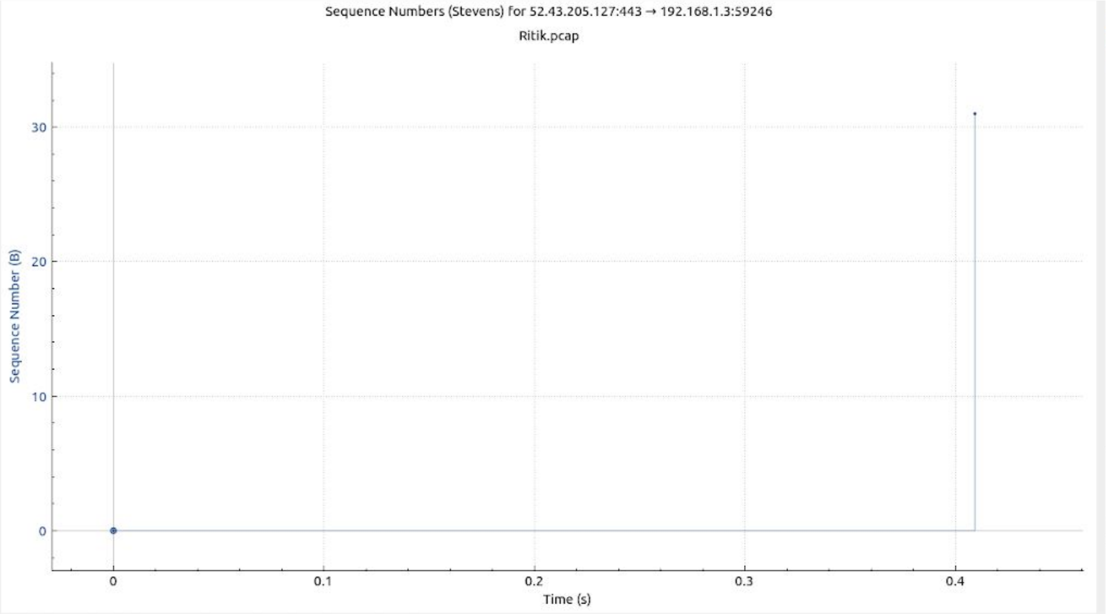
```
▸ Frame 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface wlo1, id 0
▸ Ethernet II, Src: IntelCor_1d:f6:af (b4:6b:fc:1d:f6:af), Dst: TendaTec_08:2b:88 (50:2b:73:08:2b:88)
▸ Internet Protocol Version 4, Src: 192.168.1.3, Dst: 52.43.205.127
▾ Transmission Control Protocol, Src Port: 59246, Dst Port: 443, Seq: 1, Ack: 32, Len: 0
    Source Port: 59246
    Destination Port: 443
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 1    (relative sequence number)
    Sequence number (raw): 3311935842
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 32    (relative ack number)
    Acknowledgment number (raw): 717822330
    1000 .... = Header Length: 32 bytes (8)
```



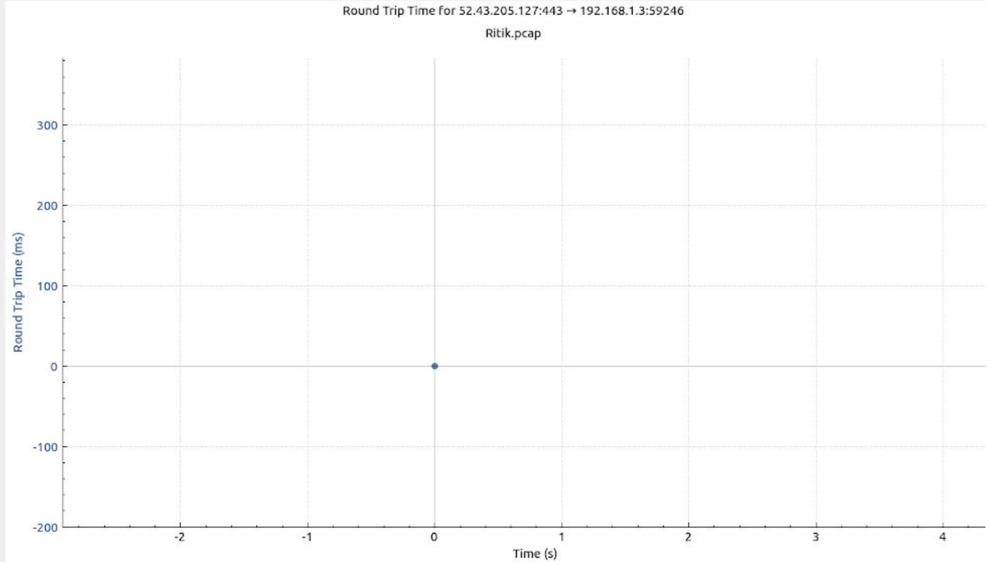
```
▸ Frame 4: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on inte
▸ Ethernet II, Src: TendaTec_08:2b:88 (50:2b:73:08:2b:88), Dst: IntelCor_1d:
▸ Internet Protocol Version 4, Src: 52.43.205.127, Dst: 192.168.1.3
▾ Transmission Control Protocol, Src Port: 443, Dst Port: 59246, Seq: 32, Ac
    Source Port: 443
    Destination Port: 59246
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 32    (relative sequence number)
    Sequence number (raw): 717822330
    [Next sequence number: 32    (relative sequence number)]
    Acknowledgment number: 36    (relative ack number)
    Acknowledgment number (raw): 3311935877
    1000 .... = Header Length: 32 bytes (8)
```

Initially it was 1 after that it changed to 32.

Now click on the Statistics and TCP stream to view the TCP stream graph.

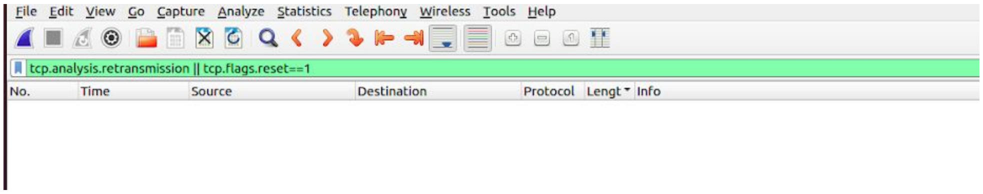


(e). Click on the Statistics tab and under TCP sections, RTT graph .

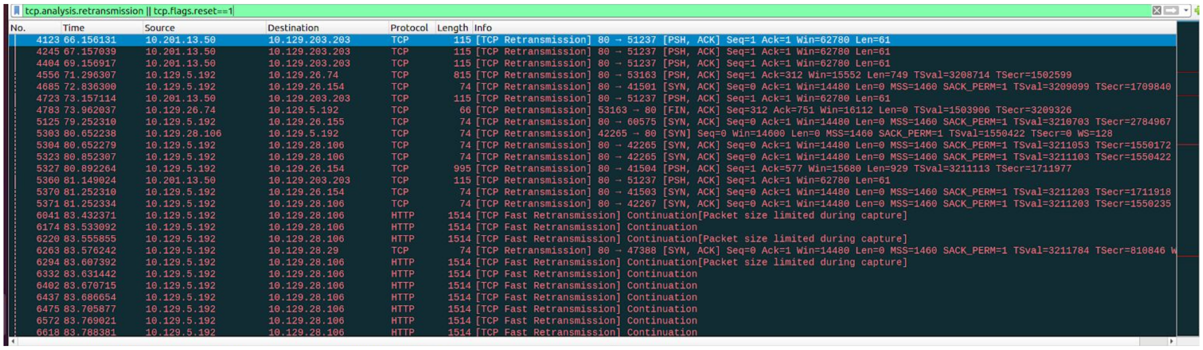


(f).For checking the timeout sessions, apply filter: **tcp.reset.flags==1 || tcp.analyse.retransmission**

Here we can view the timeout sessions are empty, Hence we need to use the file provided.

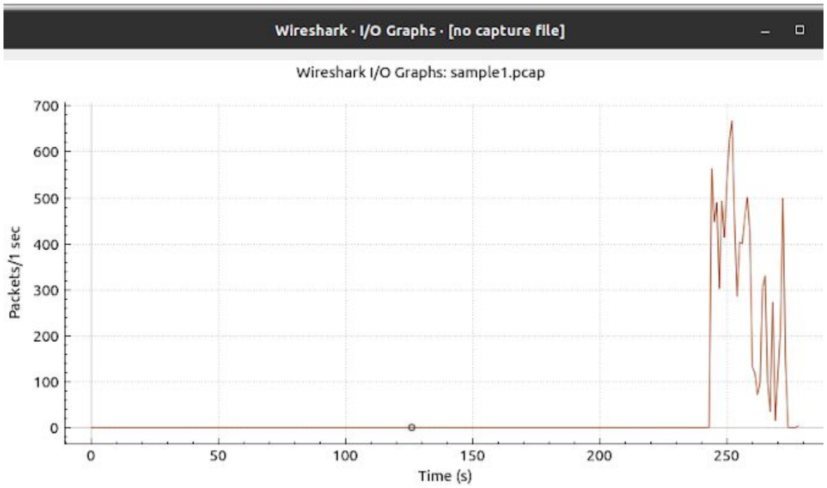

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.analysis.retransmission || tcp.flags.reset==1
No.    Time    Source    Destination    Protocol    Lengt    Info
```

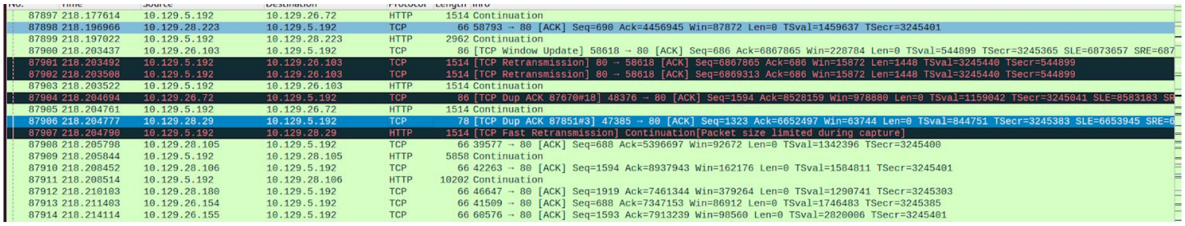


```
tcp.analysis.retransmission || tcp.flags.reset==1
No.  Time        Source          Destination       Protocol  Length Info
4123 66.156131   10.201.13.50    10.129.203.203    TCP        115 [TCP Retransmission] 80 → 51237 [PSH, ACK] Seq=1 Ack=1 Win=62780 Len=61
4245 67.157039   10.201.13.50    10.129.203.203    TCP        115 [TCP Retransmission] 80 → 51237 [PSH, ACK] Seq=1 Ack=1 Win=62780 Len=61
4404 69.156917   10.201.13.50    10.129.203.203    TCP        115 [TCP Retransmission] 80 → 51237 [PSH, ACK] Seq=1 Ack=1 Win=62780 Len=61
4556 71.296307   10.129.5.192    10.129.26.74      TCP        815 [TCP Retransmission] 80 → 53163 [PSH, ACK] Seq=1 Ack=312 Win=15552 Len=749 TSval=3208714 TSecr=1502599
4685 72.836300   10.129.5.192    10.129.26.154     TCP         74 [TCP Retransmission] 80 → 41501 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=3209099 TSecr=1709840
4723 73.157114   10.201.13.50    10.129.203.203    TCP        115 [TCP Retransmission] 80 → 51237 [PSH, ACK] Seq=1 Ack=1 Win=62780 Len=61
4783 73.962037   10.129.26.74    10.129.5.192      TCP         66 [TCP Retransmission] 53163 → 80 [FIN, ACK] Seq=312 Ack=751 Win=16112 Len=0 TSval=1503906 TSecr=3209326
5125 79.252310   10.129.5.192    10.129.26.155     TCP         74 [TCP Retransmission] 80 → 60575 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=3210703 TSecr=2784967
5303 80.652238   10.129.28.106   10.129.5.192      TCP         74 [TCP Retransmission] 42265 → 80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=1550422 TSecr=0 WS=128
5304 80.652279   10.129.5.192    10.129.28.106     TCP         74 [TCP Retransmission] 80 → 42265 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=3211053 TSecr=1550172
5323 80.852307   10.129.5.192    10.129.28.106     TCP         74 [TCP Retransmission] 80 → 42265 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=3211103 TSecr=1550422
5327 80.892264   10.129.5.192    10.129.26.154     TCP        995 [TCP Retransmission] 80 → 41504 [PSH, ACK] Seq=1 Ack=577 Win=15680 Len=929 TSval=3211113 TSecr=1711977
5360 81.149024   10.201.13.50    10.129.203.203    TCP        115 [TCP Retransmission] 80 → 51237 [PSH, ACK] Seq=1 Ack=1 Win=62780 Len=61
5370 81.252310   10.129.5.192    10.129.26.154     TCP         74 [TCP Retransmission] 80 → 41503 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=3211203 TSecr=1711918
5371 81.252334   10.129.5.192    10.129.28.106     TCP         74 [TCP Retransmission] 80 → 42267 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=3211203 TSecr=1550235
6041 83.432371   10.129.5.192    10.129.28.106     HTTP      1514 [TCP Fast Retransmission] Continuation[Packet size limited during capture]
6174 83.533092   10.129.5.192    10.129.28.106     HTTP      1514 [TCP Fast Retransmission] Continuation
6220 83.555855   10.129.5.192    10.129.28.106     HTTP      1514 [TCP Fast Retransmission] Continuation[Packet size limited during capture]
6263 83.576242   10.129.5.192    10.129.28.29      TCP         74 [TCP Retransmission] 80 → 47388 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=3211784 TSecr=810846 W
6294 83.607392   10.129.5.192    10.129.28.106     HTTP      1514 [TCP Fast Retransmission] Continuation[Packet size limited during capture]
6332 83.631442   10.129.5.192    10.129.28.106     HTTP      1514 [TCP Fast Retransmission] Continuation
6402 83.670715   10.129.5.192    10.129.28.106     HTTP      1514 [TCP Fast Retransmission] Continuation
6437 83.686654   10.129.5.192    10.129.28.106     HTTP      1514 [TCP Fast Retransmission] Continuation
6475 83.705877   10.129.5.192    10.129.28.106     HTTP      1514 [TCP Fast Retransmission] Continuation
6572 83.769021   10.129.5.192    10.129.28.106     HTTP      1514 [TCP Fast Retransmission] Continuation
6618 83.788381   10.129.5.192    10.129.28.106     HTTP      1514 [TCP Fast Retransmission] Continuation
```

The congestion window size should remain the same i.e equal to 1 (reset).



We can see the drop for the packets. This shows there was time out.

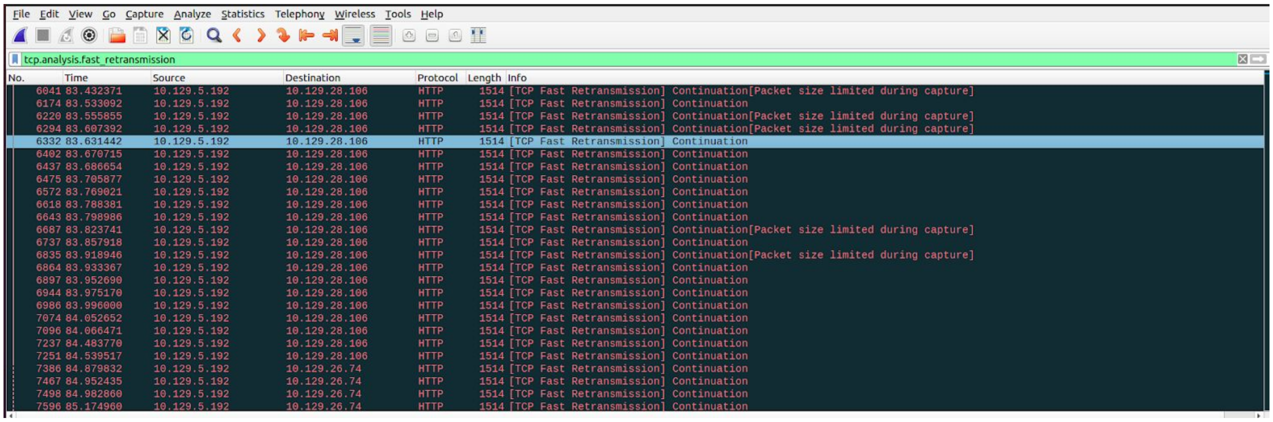


```
87897 218.177614  10.129.5.192     10.129.26.72     HTTP     1514 Continuation
87898 218.196966  10.129.28.223    10.129.5.192     TCP        66 58793 → 80 [ACK] Seq=690 Ack=4456945 Win=87872 Len=0 TSval=1459637 TSecr=3245401
87899 218.197022  10.129.5.192     10.129.28.223    HTTP     2962 Continuation
87900 218.203437  10.129.26.103    10.129.5.192     TCP        86 [TCP Window Update] 58618 → 80 [ACK] Seq=686 Ack=6867865 Win=228784 Len=0 TSval=544899 TSecr=3245365 SLE=6873657 SRE=687
87901 218.203492  10.129.5.192     10.129.26.103    TCP      1514 [TCP Retransmission] 80 → 58618 [ACK] Seq=6867865 Ack=686 Win=15872 Len=1448 TSval=3245440 TSecr=544899
87902 218.203508  10.129.5.192     10.129.26.103    TCP      1514 [TCP Retransmission] 80 → 58618 [ACK] Seq=6869313 Ack=686 Win=15872 Len=1448 TSval=3245440 TSecr=544899
87903 218.203522  10.129.5.192     10.129.26.103    HTTP     1514 Continuation
87904 218.204694  10.129.26.72     10.129.5.192     TCP        86 [TCP Dup ACK 87670#18] 48376 → 80 [ACK] Seq=1594 Ack=8528159 Win=978880 Len=0 TSval=1159042 TSecr=3245041 SLE=8583183 SR
87905 218.204761  10.129.5.192     10.129.26.72     HTTP     1514 Continuation
87906 218.204777  10.129.28.29     10.129.5.192     TCP        78 [TCP Dup ACK 87851#3] 47385 → 80 [ACK] Seq=1323 Ack=6652497 Win=63744 Len=0 TSval=844751 TSecr=3245383 SLE=6653945 SRE=6
87907 218.204790  10.129.5.192     10.129.28.29     HTTP     1514 [TCP Fast Retransmission] Continuation[Packet size limited during capture]
87908 218.205798  10.129.28.105    10.129.5.192     TCP        66 39577 → 80 [ACK] Seq=688 Ack=5396697 Win=92672 Len=0 TSval=1342396 TSecr=3245400
87909 218.205844  10.129.5.192     10.129.28.105    HTTP     5858 Continuation
87910 218.208452  10.129.28.106    10.129.5.192     TCP        66 42263 → 80 [ACK] Seq=1594 Ack=8937943 Win=162176 Len=0 TSval=1584811 TSecr=3245401
87911 218.208514  10.129.5.192     10.129.28.106    HTTP    10202 Continuation
87912 218.210103  10.129.28.180    10.129.5.192     TCP        66 46647 → 80 [ACK] Seq=1919 Ack=7461344 Win=379264 Len=0 TSval=1290741 TSecr=3245303
87913 218.211403  10.129.26.154    10.129.5.192     TCP        66 41509 → 80 [ACK] Seq=688 Ack=7347153 Win=86912 Len=0 TSval=1746483 TSecr=3245385
87914 218.214114  10.129.26.155    10.129.5.192     TCP        66 60576 → 80 [ACK] Seq=1593 Ack=7913239 Win=98560 Len=0 TSval=2820006 TSecr=3245401
```

Also we can see the selected packet has been colored, showing it has been timeout and confirms the timeout.

(g). For fast retransmission: apply filter: **tcp.analyse.fast_retransmission**

Here there is a fast retransmission.



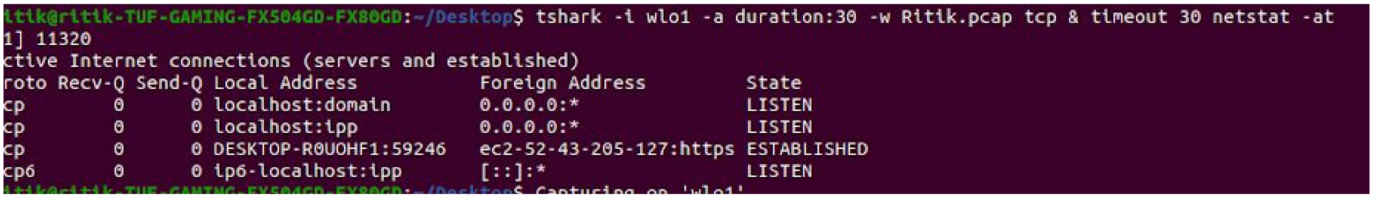
tcp.analysis.fast_retransmission

```
No.   Time       Source          Destination     Protocol Length Info
 6041 83.432371  10.129.5.192    10.129.28.106   HTTP     1514 [TCP Fast Retransmission] Continuation[Packet size limited during capture]
 6174 83.533092  10.129.5.192    10.129.28.106   HTTP     1514 [TCP Fast Retransmission] Continuation
 6220 83.555855  10.129.5.192    10.129.28.106   HTTP     1514 [TCP Fast Retransmission] Continuation[Packet size limited during capture]
 6294 83.607392  10.129.5.192    10.129.28.106   HTTP     1514 [TCP Fast Retransmission] Continuation[Packet size limited during capture]
 6332 83.631442  10.129.5.192    10.129.28.106   HTTP     1514 [TCP Fast Retransmission] Continuation
 6402 83.670715  10.129.5.192    10.129.28.106   HTTP     1514 [TCP Fast Retransmission] Continuation
 6437 83.686654  10.129.5.192    10.129.28.106   HTTP     1514 [TCP Fast Retransmission] Continuation
 6475 83.705877  10.129.5.192    10.129.28.106   HTTP     1514 [TCP Fast Retransmission] Continuation
 6572 83.769021  10.129.5.192    10.129.28.106   HTTP     1514 [TCP Fast Retransmission] Continuation
 6618 83.788381  10.129.5.192    10.129.28.106   HTTP     1514 [TCP Fast Retransmission] Continuation
 6643 83.798986  10.129.5.192    10.129.28.106   HTTP     1514 [TCP Fast Retransmission] Continuation
 6687 83.823741  10.129.5.192    10.129.28.106   HTTP     1514 [TCP Fast Retransmission] Continuation[Packet size limited during capture]
 6737 83.857918  10.129.5.192    10.129.28.106   HTTP     1514 [TCP Fast Retransmission] Continuation
 6835 83.918946  10.129.5.192    10.129.28.106   HTTP     1514 [TCP Fast Retransmission] Continuation[Packet size limited during capture]
 6864 83.933367  10.129.5.192    10.129.28.106   HTTP     1514 [TCP Fast Retransmission] Continuation
 6897 83.952690  10.129.5.192    10.129.28.106   HTTP     1514 [TCP Fast Retransmission] Continuation
 6944 83.975170  10.129.5.192    10.129.28.106   HTTP     1514 [TCP Fast Retransmission] Continuation
 6986 83.996000  10.129.5.192    10.129.28.106   HTTP     1514 [TCP Fast Retransmission] Continuation
 7074 84.052652  10.129.5.192    10.129.28.106   HTTP     1514 [TCP Fast Retransmission] Continuation
 7096 84.066471  10.129.5.192    10.129.28.106   HTTP     1514 [TCP Fast Retransmission] Continuation
 7237 84.483770  10.129.5.192    10.129.28.106   HTTP     1514 [TCP Fast Retransmission] Continuation
 7251 84.539517  10.129.5.192    10.129.28.106   HTTP     1514 [TCP Fast Retransmission] Continuation
 7386 84.879832  10.129.5.192    10.129.26.74    HTTP     1514 [TCP Fast Retransmission] Continuation
 7467 84.952435  10.129.5.192    10.129.26.74    HTTP     1514 [TCP Fast Retransmission] Continuation
 7498 84.982860  10.129.5.192    10.129.26.74    HTTP     1514 [TCP Fast Retransmission] Continuation
 7596 85.174960  10.129.5.192    10.129.26.74    HTTP     1514 [TCP Fast Retransmission] Continuation
```

Answer 2.

(a).Using netstat for validating.

Command: **tshark -i wlo1 -a duration:30 -w ritik12.pcap tcp & timeout 30 netstat -at;**



```
itik@ritik-TUF-GAMING-FX504GD-FX80GD:~/Desktop$ tshark -i wlo1 -a duration:30 -w Ritik.pcap tcp & timeout 30 netstat -at
1] 11320
ctive Internet connections (servers and established)
roto Recv-Q Send-Q Local Address           Foreign Address         State
cp         0      0 localhost:domain        0.0.0.0:*               LISTEN
cp         0      0 localhost:ipp           0.0.0.0:*               LISTEN
cp         0      0 DESKTOP-R0UOHF1:59246   ec2-52-43-205-127:https ESTABLISHED
cp6        0      0 ip6-localhost:ipp       [::]:*                  LISTEN
itik@ritik-TUF-GAMING-FX504GD-FX80GD:~/Desktop$ Capturing on 'wlo1'
```

Now counting the number of tcp connections: 1, they are the same as in the above example.

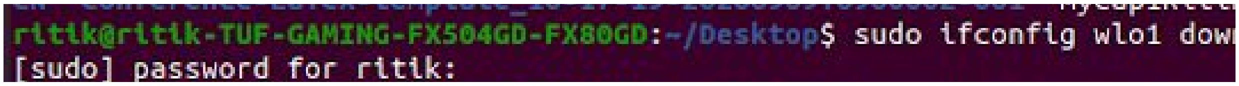
(b).Timed_wait: 0

Listen:3

Established: 1

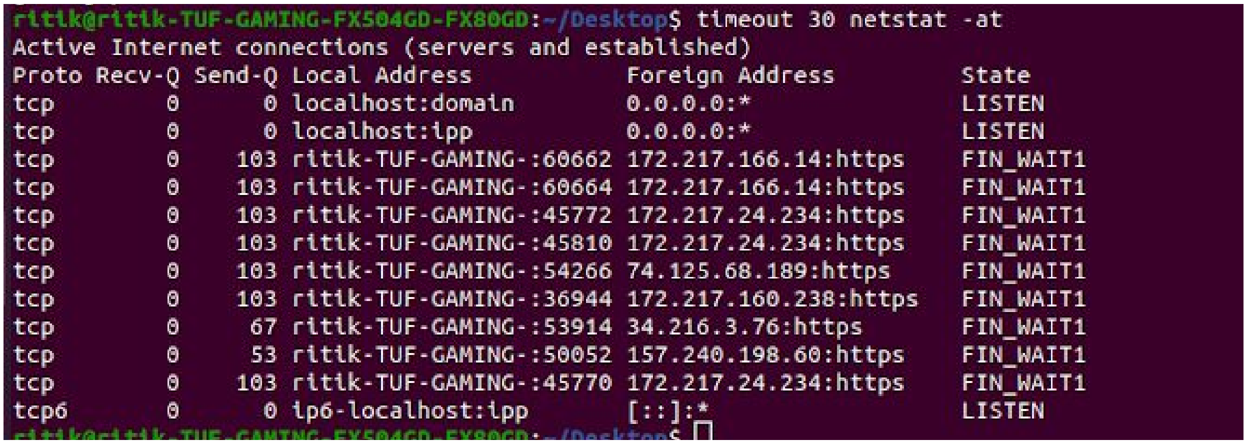
Fin-wait 1: 0

(c). Changing the ifcong wlo1 to down.



```
ritik@ritik-TUF-GAMING-FX504GD-FX80GD:~/Desktop$ sudo ifconfig wlo1 dow
[sudo] password for ritik:
```

Run : **timeout 30 netstat -at**



```
ritik@ritik-TUF-GAMING-FX504GD-FX80GD:~/Desktop$ timeout 30 netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0    103 ritik-TUF-GAMING-:60662 172.217.166.14:https    FIN_WAIT1
tcp        0    103 ritik-TUF-GAMING-:60664 172.217.166.14:https    FIN_WAIT1
tcp        0    103 ritik-TUF-GAMING-:45772 172.217.24.234:https    FIN_WAIT1
tcp        0    103 ritik-TUF-GAMING-:45810 172.217.24.234:https    FIN_WAIT1
tcp        0    103 ritik-TUF-GAMING-:54266 74.125.68.189:https     FIN_WAIT1
tcp        0    103 ritik-TUF-GAMING-:36944 172.217.160.238:https   FIN_WAIT1
tcp        0     67 ritik-TUF-GAMING-:53914 34.216.3.76:https       FIN_WAIT1
tcp        0     53 ritik-TUF-GAMING-:50052 157.240.198.60:https    FIN_WAIT1
tcp        0    103 ritik-TUF-GAMING-:45770 172.217.24.234:https    FIN_WAIT1
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
ritik@ritik-TUF-GAMING-FX504GD-FX80GD:~/Desktop$
```

Timed_wait: 0

Listen: 3

Established: 0

Fin-wait 1:9

Yes they have changed, Now the number of TCP connections has changed and fin-wait state has been increased.