1. Capture a TCP connection and identify SYN, SYN-ACK, and ACK.

Tcp.stream eq 0

Questions:

● Which packets are SYN, SYN-ACK, and ACK?

Packet 1,2,3

● What are the source and destination ports?

Src -20000

dst-80

● What is the initial sequence number?

Isn-0

2.Find the size of TCP segments carrying application data.

tcp.port==80 || tcp.port==443

Questions:

● What is the payload length of the first 5 data packets?

435

● Identify any large payload segments.

1538

3.Detects retransmitted segments in a capture.

tcp.analysis.retransmission

Questions:

● Which packet(s) were retransmitted?

Total – 68

Src-10.0.0.1 dst- 10.0.0.100 , isn- 9

● What is the RTT for the retransmission?

4. Identify duplicate ACKs in TCP.

tcp.analysis.duplicate\_ack

Questions:

● How many duplicate ACKs were observed?

28

● What sequence number do they acknowledge?

Sequence number -1

5. Understand flow control in TCP.

Questions:

● What is the advertised window size?

8192

● How does window scaling affect throughput?

-2 (2)^2 = 4

8192 \* 4

6. Measure RTT of TCP segments and estimate using TCP formula.

Statistic-----> flow graph----> screenshot

Questions:

● What is the RTT of the first 5 segments?

screenshot

● Compute Estimated RTT after each ACK.

7. Detects packets received out-of-order.

tcp.analysis.out\_of\_order

Questions:

● Which packets arrived out-of-order?

Total -21

src-10.0.0.1

dst-10.0.0.100

prtocol- TCP

● How did TCP handle them?

theory