COMP9121 Week8 Lab

In this lab, we are now going to use the Wireshark protocol analyser to get a better feeling how TCP operates. We are going to use the provided packet captures (PCAP files).

1. Wiresharking TCP

Load the first capture, week8_capture_1.pcap. Answer a few small questions:

1 What are
- source IP
- destination IP
- source port
- destination port

Easy to know

2 Judging by the destination port, what kind of TCP-based communication is this?

Web or HTTP, since 80 is the port number

3 How long are the fields for source and destination port?

16 bits

4 How long is the sequence number? How long is the acknowledgement?

32 bits

5 What is the largest (smallest) sequence number that can be expressed with this length?

0 and 2^{32}-1 in byte

6 What is the MSS? How does the sender and receiver negotiate MSS?

Max segment size. Negotiate in "Optional" during handshake.

7 What does the option 'SACK permitted' possibly mean?

Allow selected ACK

8 What do the first three packets constitute?

SYN, SYN ACK, ACK

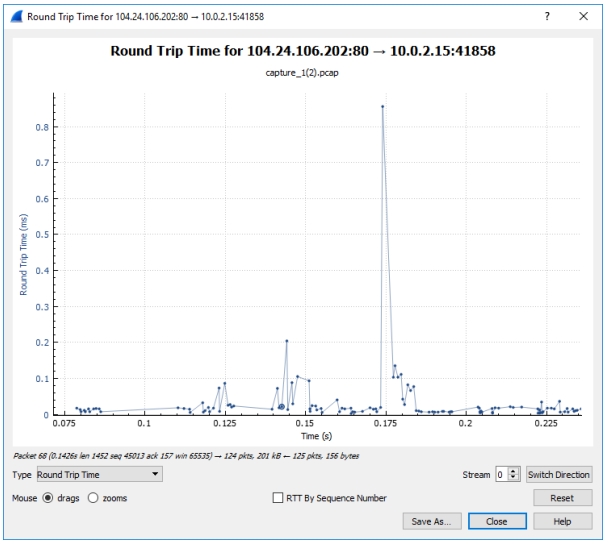
9 Identify sequence number and acknowledgements. Draw a 'swim lane' figure that shows which ACK follows which segment. Inspecting the first 8 packets is enough.

→ SEQ=0
←SEQ=0, ACK=1
→SEQ=1, ACK=1
→SEQ=1, ACK=1
←SEQ=1, ACK=157
←SEQ=1, ACK=157
→SEQ=157, ACK=1453
←SEQ=1453, ACK=157

10 Is the ACK in packet 3 piggybacked? Is the ACK in packet 10 piggybacked?

No. Yes

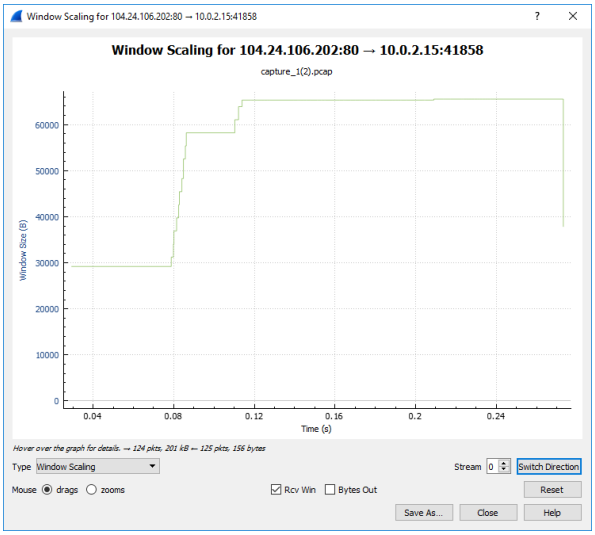
11 Have a look at the RTTs-in which range are they? Compare between a packet and its acknowledgement. You can also use Statistics->TCP Stream Graph->Round Trip Time to plot the RTTs.



12 Inspect packet 3. What is the advertised window size? What does this mean?

29200, received window size. Use for flow control. Advertise available buffer size

13 Use Statistics->TCP Stream Graph->Window Scaling to inspect it over the course of the transmission.



2 telnet

In this task, we are going to inspect week8_capture_2.pcap.

Have a look at the trace. It contains a trace of a telnet conversation—i.e. a login via an unencrypted protocol. The interesting data starts around packet 15.

1 Who is communicating with whom? Where is this communication taking place?

A computer is communicating with itself. One computer. (Use port number to know the direction.)

2 In which packet does the user start to type the username? In which the password?

From packet 20.

From packet 49.

3 How does telnet transmit the typed characters?

One by one. (Echo the user name, but not password)

4 How large are hence the packets? Link layer 16, IP 20, TCP 32, telnet 1, in bytes