# 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 10.0.2.15
- – destination IP 104.26.10b.202
- – source port 41858
- – destination port 80

Syn 1st handshake?

2 Judging by the destination port, what kind of TCP-based communication is this?
3 How long are the fields for source and destination port?
4 How long is the sequence number? How long is the acknowledgement? 8 bits
5 What is the largest (smallest) sequence number that can be expressed with this length? 0
6 What is the MSS? How does the sender and receiver negotiate MSS?
7 What does the option 'SACK permitted' possibly mean? maximum segment size
8 What do the first three packets constitute? Establish connection
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.
10 Is the ACK in packet 3 piggybacked? Is the ACK in packet 10 piggybacked?
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?
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.

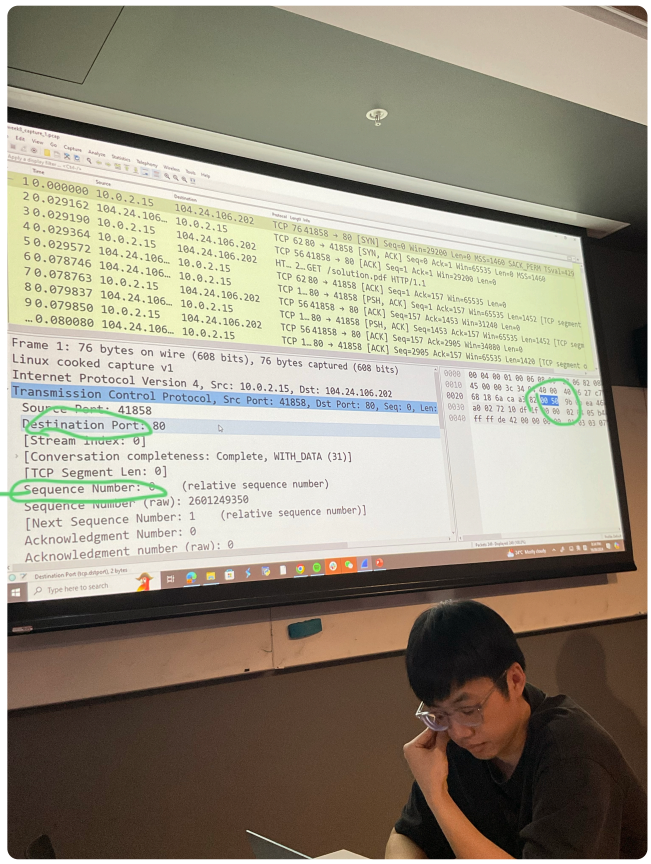
1 Who is communicating with whom? Where is this communication taking place?
2 In which packet does the user start to type the username? In which the password?
3 How does telnet transmit the typed characters?
4 How large are hence the packets?

1. Source IP 10.0.2.15
Dest IP 104.24.106.202
source port 41858
dest port 80

2. Http or Web for Tcp

Hex number
↓
2x8=16 bits

3. 点击 "Source Port" 看右下 Highlight




4. 4x8=32 bits

5. $0 \to 2^{32}-1 \Rightarrow 2^{32}-1$ is the largest number

6. max segment size.

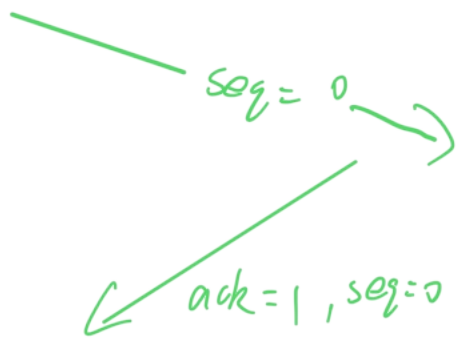
① sender 问 receiver
② receiver 提供给 sender
选 $\min\{①, ②\}$

7. select ack

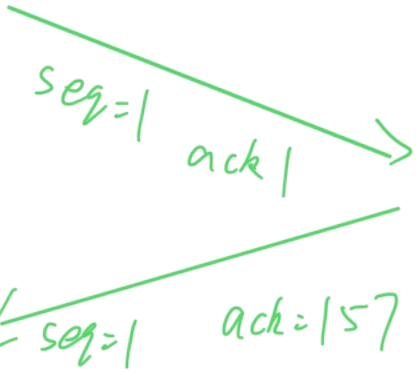
8. Establish connection ?

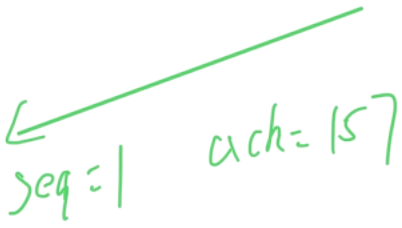
104.24.106.202

9.

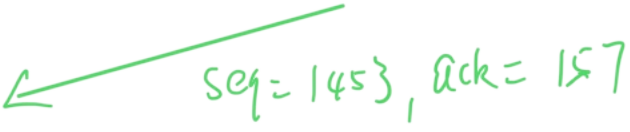


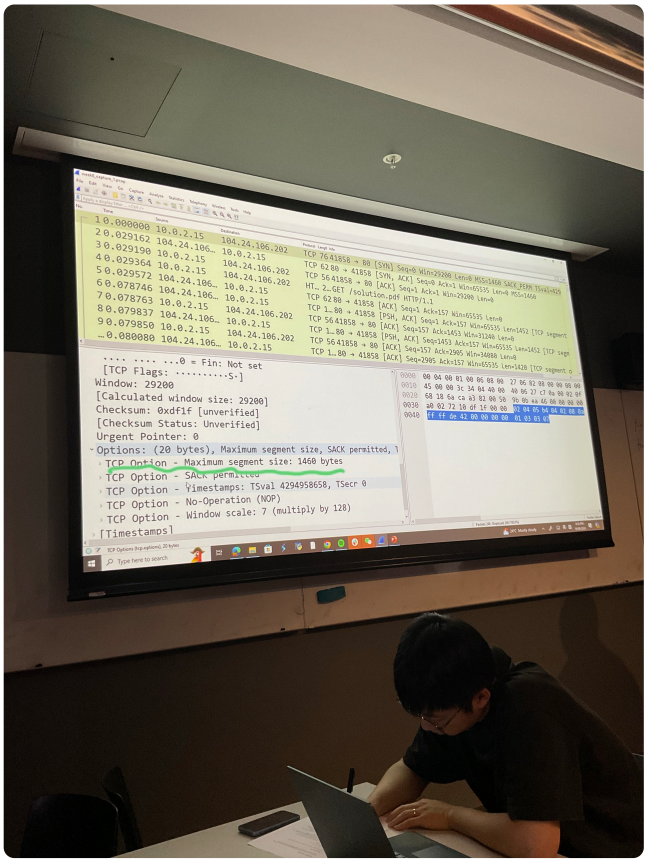








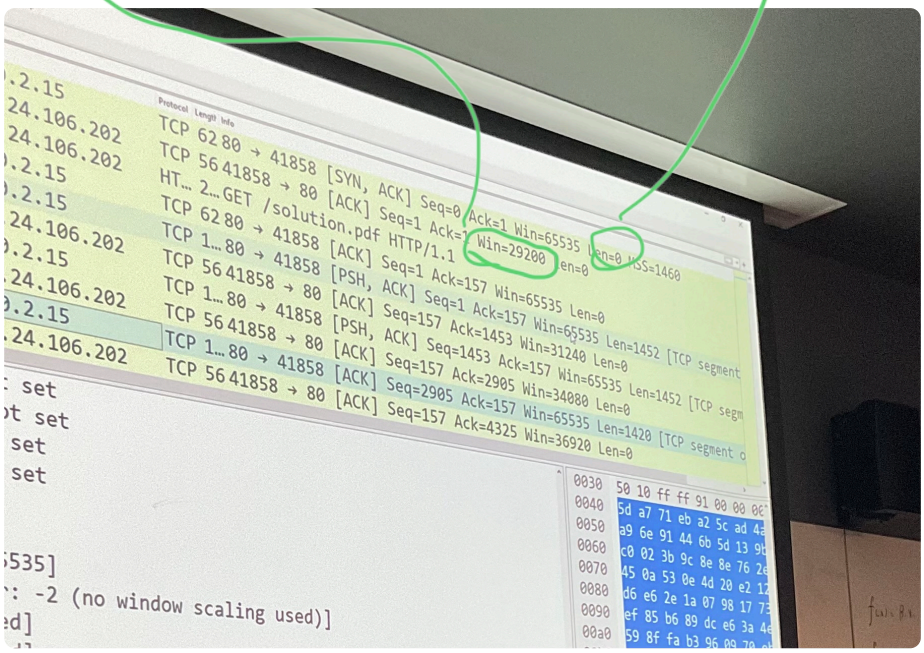
10. Len=0 ⇒ not piggy bank

"len=1420" ⇒ piggy bank

11. Follow instruction

12. "Win" = 29200

window size

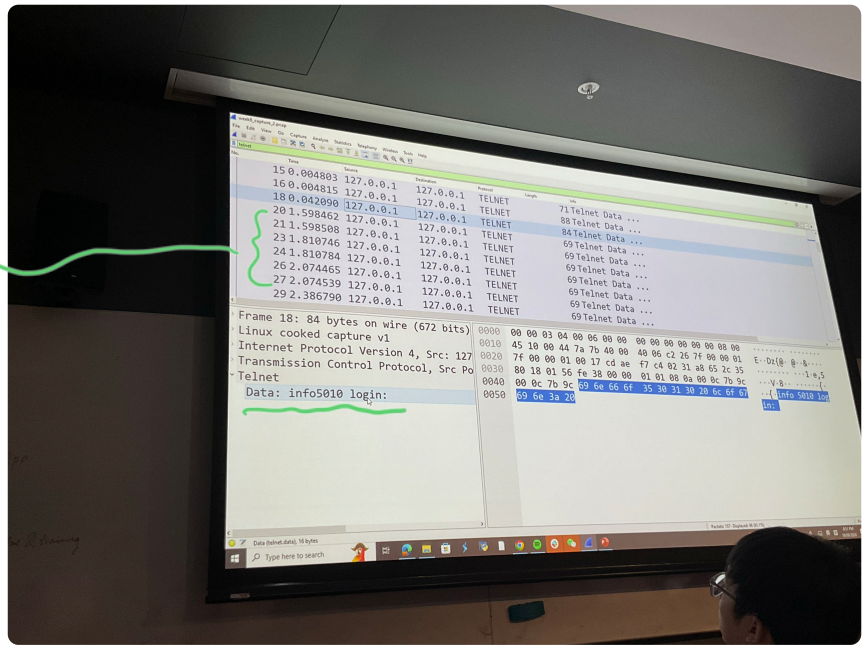



13. Follow instruction

1. self → self

port 23 port 52654

2. Telnet:



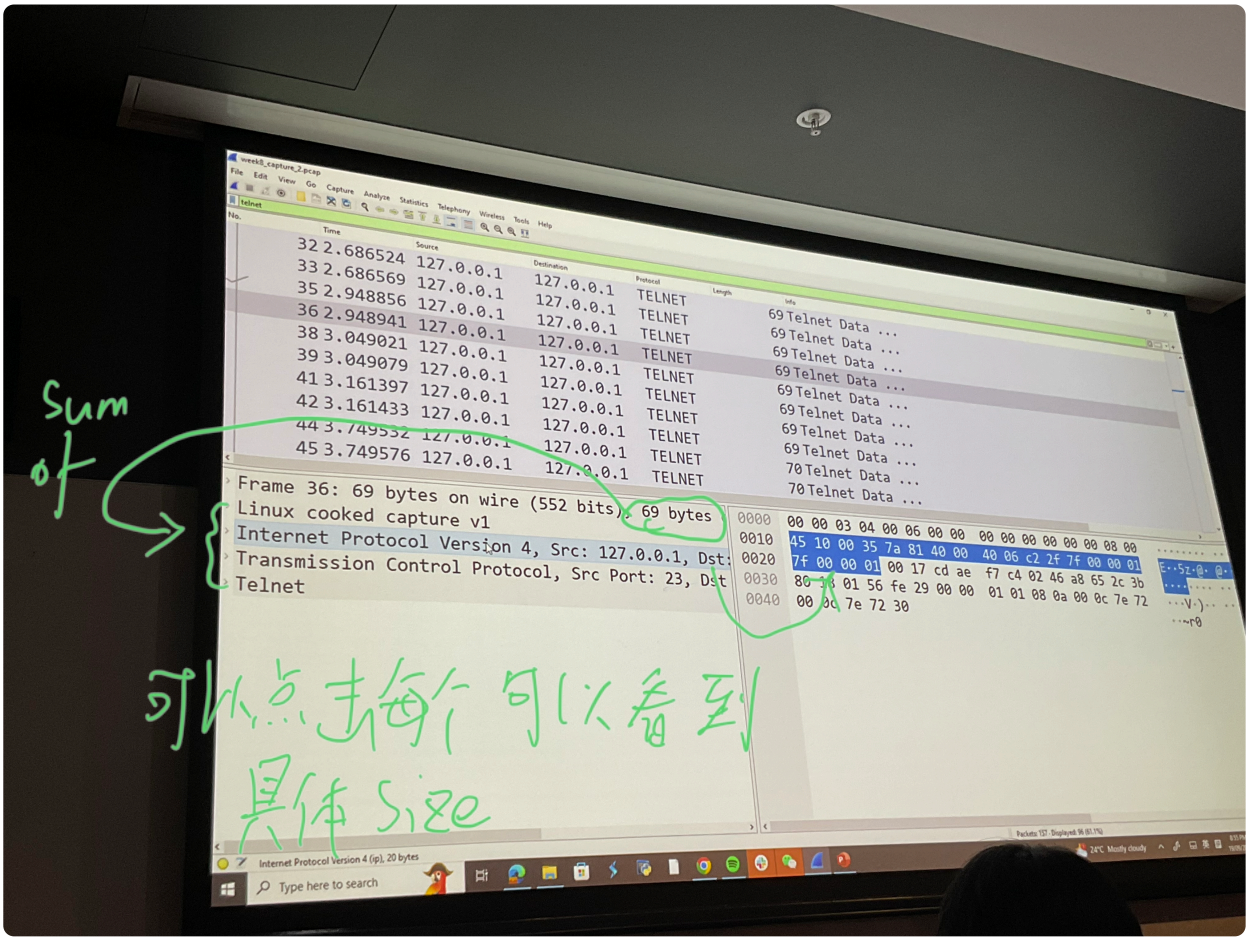

捕捉后面这些

from packet 20 username 重复的

49 password 不重复的

3. transmit one-by-one

4.


Sum of
Frame 36: 69 bytes on wire (552 bits), 69 bytes
Linux cooked capture v1
Internet Protocol Version 4, Src: 127.0.0.1, Dst:
Transmission Control Protocol, Src Port: 23, Dst
Telnet
可以点击每个可以看到
具体size