

Lab 4: Step-by-Step Instruction

Kui Wu

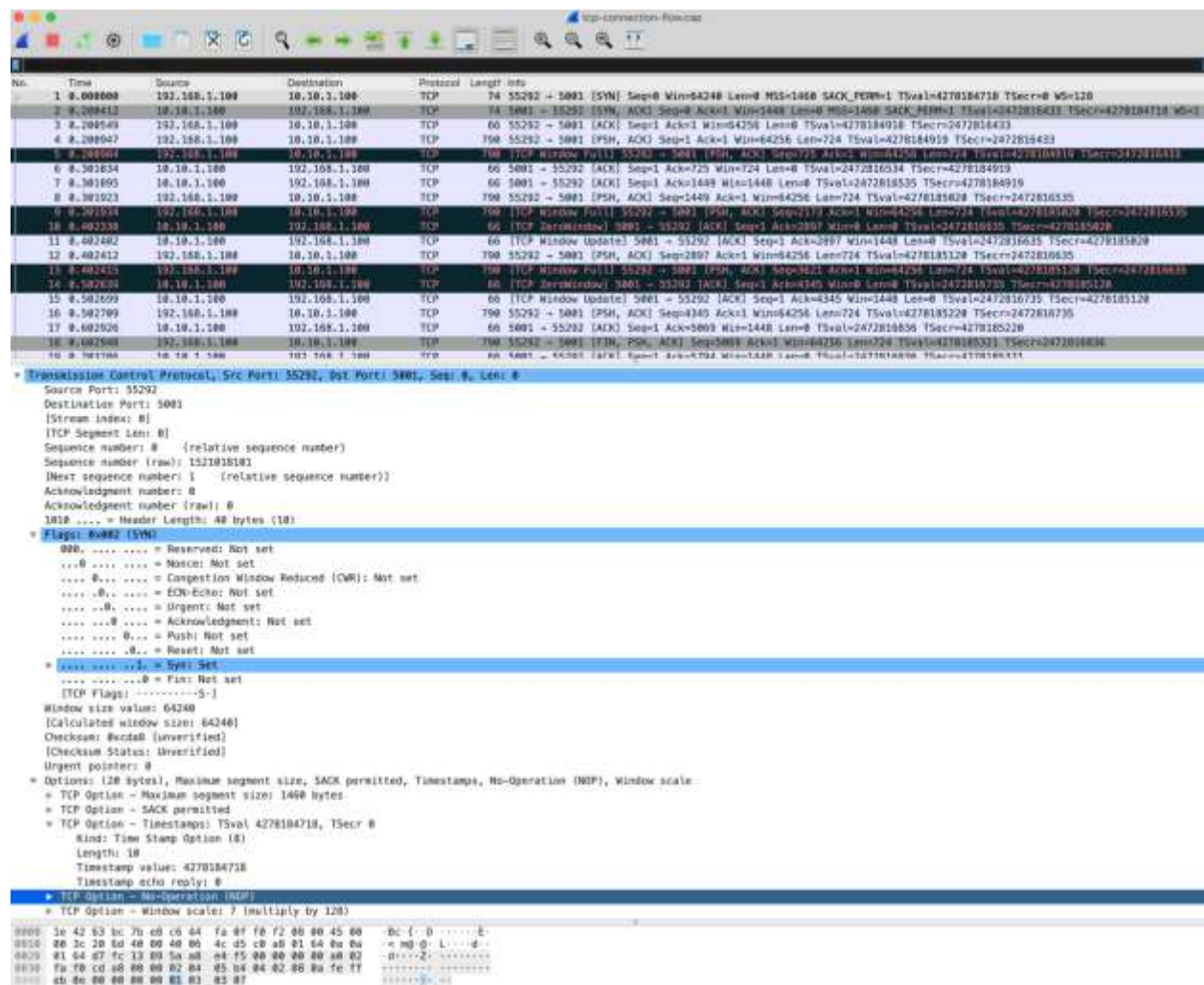
Objective: Understand TCP connection management and flow control

Note: This lab can be done at home using your local machine or at the ECS 360 virtual lab.

Step 1: If you have not installed wireshark (<https://www.wireshark.org/>) in your local computer, download and install wireshark in your local computer.

Step 2: Download *tcp-connection-flow.cap* from brightspace to your local computer and open it with WireShark. The file *TracefileDescription.pdf* in brightspace explains how the tcp trace file was captured.

Click on each individual packet. The information included in the TCP header of this packet is described at the bottom. Click on the “Flags” field (8 bits) to find out the value of each bit in this field.



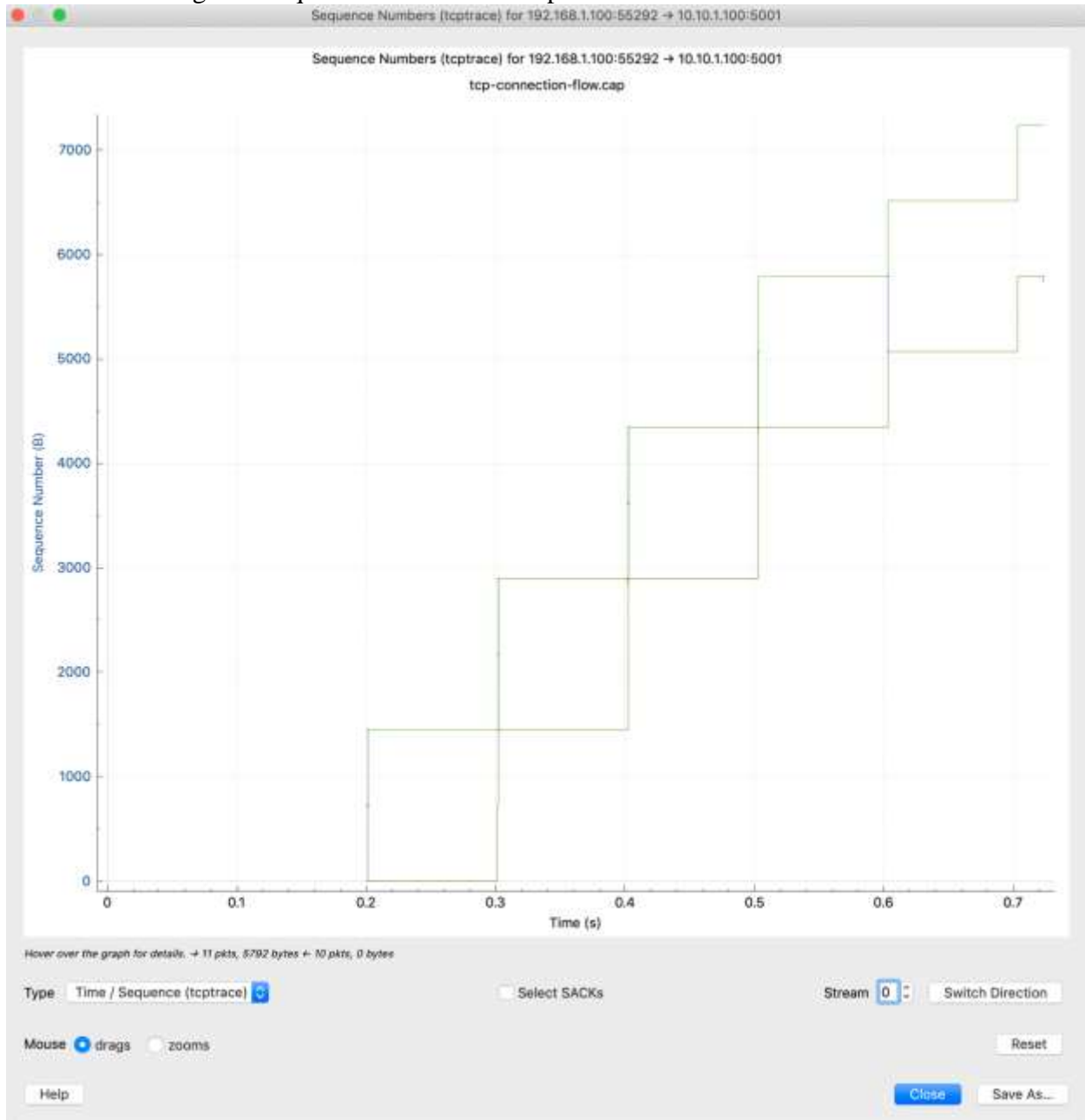
The screenshot shows the Wireshark interface with a packet capture of a TCP connection. The packet list at the top shows several packets, and the packet details pane is expanded for packet 1, showing the TCP header and options.

Packet 1 Details:

- Transmission Control Protocol, Src Port: 55292, Dst Port: 5801, Seq: 0, Len: 0**
 - Source Port: 55292
 - Destination Port: 5801
 - Stream index: 0
 - TCP Segment Len: 0
 - Sequence number: 0 (relative sequence number)
 - Sequence number (raw): 1521038101
 - Next sequence number: 1 (relative sequence number)
 - Acknowledgment number: 0
 - Acknowledgment number (raw): 0
 - 1010 = Header Length: 40 bytes (10)
- Flags: 0x0002 (SYN)**
 - 000. = Reserved: Not set
 - ...0 = Reset: Not set
 -0... = Congestion Window Reduced (CWR): Not set
 -0... = ECN-Echo: Not set
 -0... = Urgent: Not set
 -0... = Acknowledgment: Not set
 -0... = Push: Not set
 -0... = Reset: Not set
- Window size value: 64240**
 - Calculated window size: 64240
 - Checksum: 0xcda8 [unverified]
 - Checksum Status: Unverified
 - Urgent pointer: 0
- Options: 120 bytes, Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale**
 - TCP Option - Maximum segment size: 1460 bytes
 - TCP Option - SACK permitted
 - TCP Option - Timestamps: TSval: 4278184718, Tsecr: 0
 - Kind: Time Stamp Option (8)
 - Length: 10
 - Timestamp value: 4278184718
 - Timestamp echo reply: 0
 - TCP Option - No-operation (NOP)
 - TCP Option - Window scale: 7 (multiply by 128)

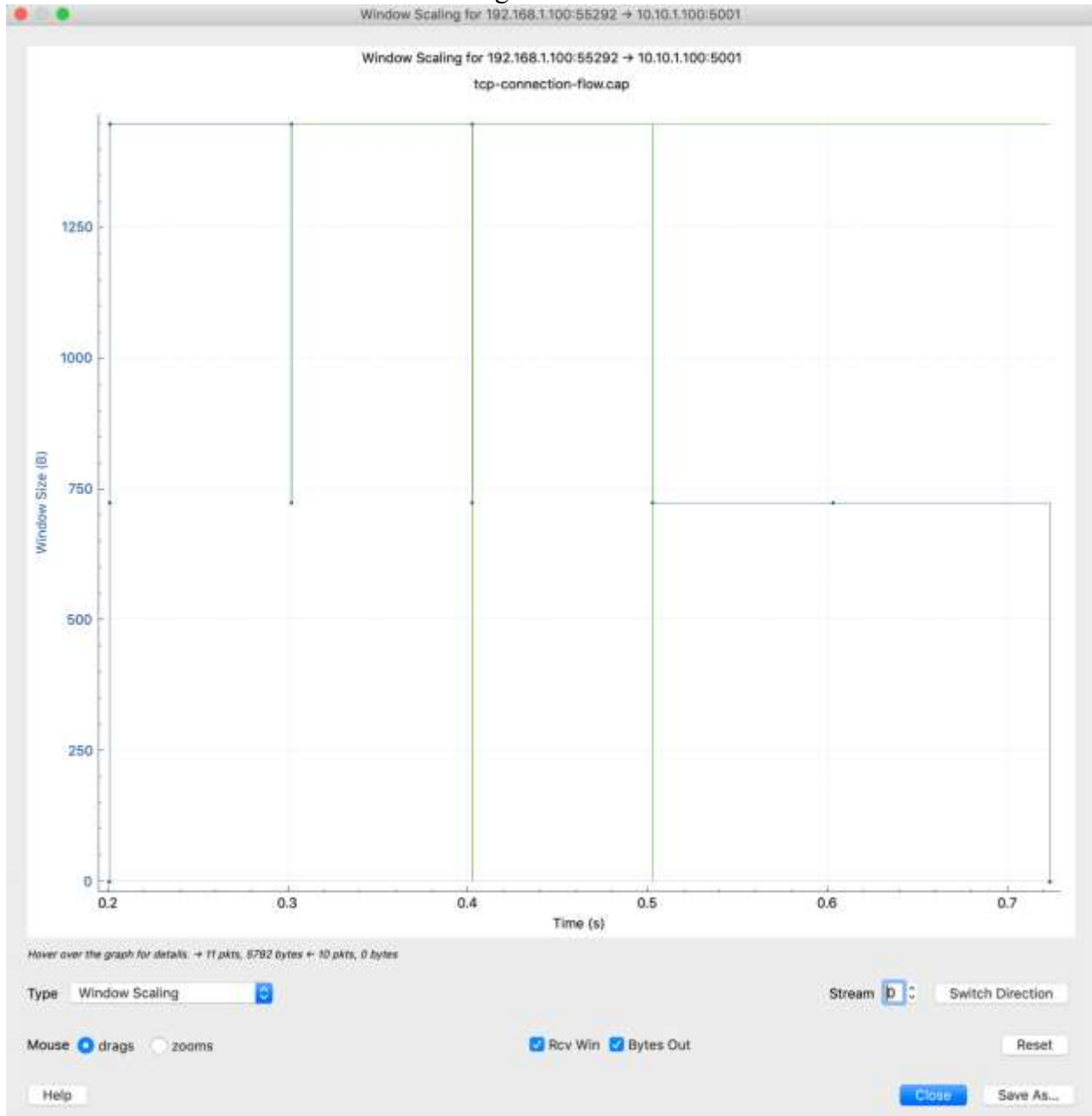
Step 3: Understand the changes of sequence numbers.

Statistics -> TCP Stream Graphs -> Time Sequence (tcptrace), Click “Switch Direction” to observe the changes of sequence numbers in the packets.



Step 4: Understand TCP flow control.

Statistics -> TCP Stream Graphs -> Window Scaling (Flow control). Click on “Switch Direction” to observe the window size changes on each side.



Step 5: Based on your analysis of the TCP trace, finish Homework 4 (posted in brightspace).