Wireshark Lab: TCP v7.0

Supplement to Computer Networking: A Top-Down

Approach, 7th ed., J.F. Kurose and K.W. Ross

Start up your web browser. Go the http://gaia.cs.umass.edu/wireshark-

labs/alice.txt and retrieve an ASCII copy of Alice in Wonderland.

• Next go to http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html.

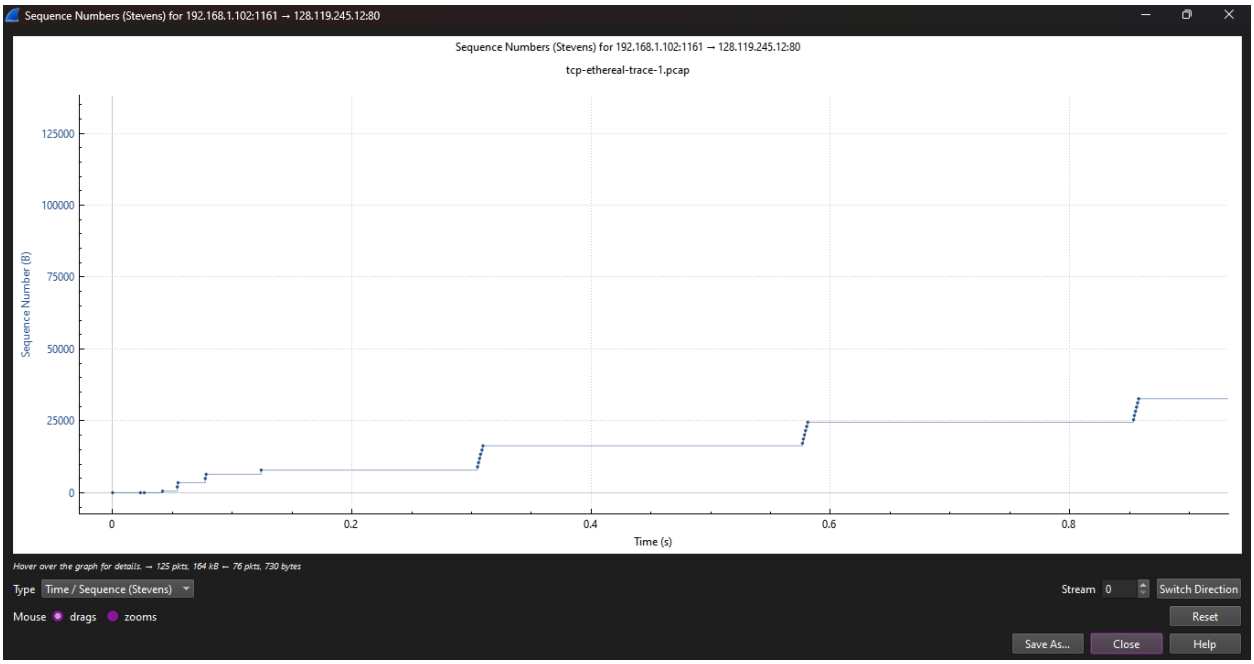
• Press the "Upload alice.txt file" button to upload the

file to the gaia.cs.umass.edu server. Once the file has been uploaded, a short

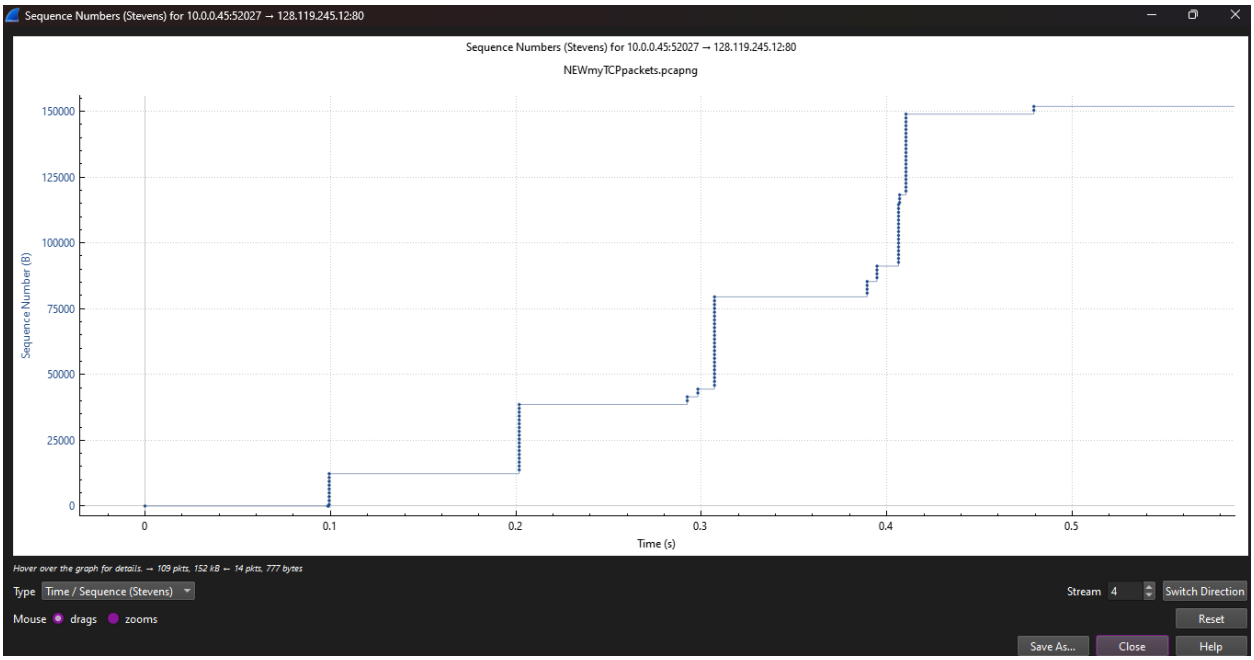
congratulations message will be displayed in your browser window.

1. In using my personal trace file, the TCP source port used is 52027 and the IP address of the source computer is 10.0.0.45 (my computer).
2. The IP address of the gaia.cs.umass.edu server is 128.119.245.12. The port number sending and receiving TCP segments for this connection is port 80.
3. The IP address and TCP port number used by my client computer is IP 10.0.0.45 and port number 52027.
4. The sequence number for the TCP SYN segment that initiated the connection between the client and server was: 3,735,224,050. The 0x002 flag within the connection shows that this is a SYN segment.
5. The sequence number for the SYN+ACK segment sent by gaia.cs.umass.edu to the client in response to the SYN was: 1,575,408,095. The value in the Acknowledgement field for this segment was 3,735,224,051. This value is the next expected sequence number, since sequence number of the segment it is acknowledging was 3,735,224,050. The 0x012 flag identifies this as an ACK segment.
6. The sequence number of the TCP segment containing the HTTP POST command was: 3,428,947,769.
7. The first six sequence numbers of the TCP segment starting with the HTTP POST command were:
   3,428,947,769
   3,428,948,389
   3428949849
   3428951309
   3428952769
   3428954229
   Each segment was received at 4.487-4.488 seconds. The ACK for each segment was received at 4.590 (the ACK for segments 1-10). The RTT value was 0.10235 seconds according to Wireshark's analysis.
   The EstimatedRTT value after the receipt of each ACK was 0.0986 seconds.
8. The length of each of the first six segments were a length of 1,460.

9. In using the given trace file, the minimum amount of available buffer space advertised at the received for the entire trace is 17,520. No throttle would occur since the length of the segments are smaller than the minimum buffer.
10. There were no seen retransmissions in the provided trace or in my personal trace. I used “tcp.analysis.retransmission” to see any retransmitted packets. Also, the sequence numbers were always increasing, never repeating or out of order, so that proves there were no retransmissions.
11. The receiver typically acknowledges 1460 bytes in an ACK. I could not identify a case where the receiver is ACKing every other received segment in the provided trace file. In my personal trace file, I was able to identify this pattern, from segments 3428984889-3428992189, this pattern occurred.
12. Using my personal trace file, the throughput was calculated to be 267,275.69 bytes/sec. Since the total transfer size was 160kB, the first packet in the connection was sent at 4.487382, and the final packet in the connection was sent at 5.721340, the throughput for my transmission was calculated to be 267,275.69 bytes/sec.
13. In using the provided trace, it is a bit harder to tell where exactly the congestion avoidance and where slow start stops because the packets are not being sent in a very consistent manner. But from what I can see, slow start begins at time=0s and slow start ends roughly at time=0.31s. The measured data here differs from the idealized behavior of TCP because this is a real situation where packets can be lost, networks can be latent, and many other factors outside of congestion take a role in how the data is gathered.



14. In my personal transmission trace file, I was able to see that slow start begins at time=0s and it ends roughly at time=0.41s, where congestion avoidance begins to take over.


Sequence Numbers (Stevens) for 10.0.0.45:52027 → 128.119.245.12:80
Sequence Numbers (Stevens) for 10.0.0.45:52027 → 128.119.245.12:80
NEWmyTCPpackets.pcapng
Sequence Number (B)
150000
125000
100000
75000
50000
25000
0
0
0.1
0.2
0.3
0.4
0.5
Time (s)
Hover over the graph for details. → 109 pkts, 152 kB ← 14 pkts, 777 bytes
Type
Time / Sequence (Stevens)
Stream
4
Switch Direction
Mouse
drags
zooms
Reset
Save As...
Close
Help