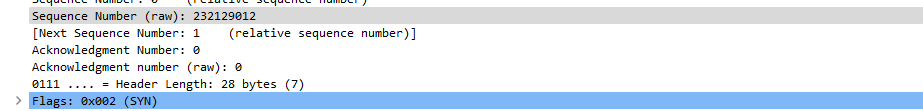
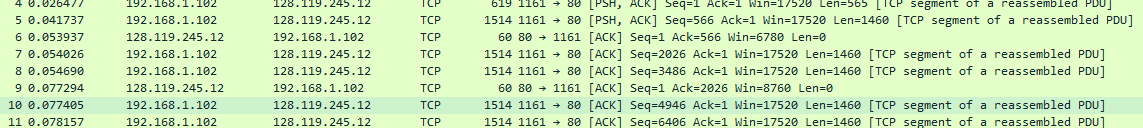
Astrid Delestine

Wireshark\_TCP\_v8 Lab 2

2/9/2023

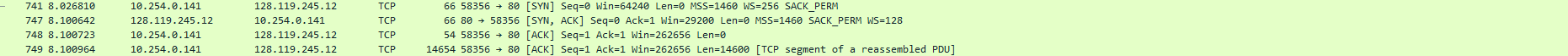
1. 192.168.1.102, Port:1161
   1. 
2. IP: 128.119.245.12, Port:80
   1. 
3. IP: 10.254.0.141 port:58356
   1. 
4. (using the given trace) sequence number = 0 (relative) 232129012 (raw). We know that it is the SYN segment because it has a SYN flag passed. 0x002 These bytes were 46 and 47 Text

   Description automatically generated
5. Sequence number = 0, The acknowledgement field was set to a relative 1, This number is the same as the raw sequence number sent in the SYN segment in question 4 plus 1. Bytes 46 and 47 identify the segment as a SYNACK segment.
   1. 
6. The sequence number for the HTTP POST command was: 164041. The Sequence Number (raw) was: 232293053.
   1. Text

      Description automatically generated
7. For this analysis the first six sequence numbers are [4,5,7,8,10,11], The time these packets were sent is [0.026477,0.041737,0.0540690,0.054690,0.077405,0.078157] in seconds sense initial capture. The time each ACK was received was [0.053937, 0.077294, 0.124085, 0.169118, 0.217299, 0.306692] in seconds sense initial capture, I was also unable to find the acknowledgement for the fourth segment. The RTT values are [0.02746, 0.035557, 0.070059, 0.114428, 0.139894, 0.189645] in seconds. The estimated RTT follows the equation, EstimatedRTT = 0.875 \* EstimatedRTT + 0.125 \* SampleRTT  
   [0.02746, 0.0285, 0.0337, 0.0438, 0.0558,0.0 725]
   1. 
8. The first segment size was 565 bytes, then the others were all 1460 bytes.
   1. 
9. The minimum amount of data space, also known as the calculated window size, is 5840 bytes. For this reason, the sender is never throttled.
   1. Text

      Description automatically generated
10. There are no incomplete segments. To find an incomplete segment, you would need to check for each ACK. See the first graph on problem 13.
11. 60 bytes are used to acknowledge a typical amount of 1460 bytes in an ACK. We know that if the data is doubled then the sender is only acknowledging every other sequence.
    1. 
12. All data bytes 164090 bytes, I calculated 31.132Kbps from total time of the transmission, and the total amount of data.
    1. Text

       Description automatically generated with medium confidence
13. Slow start begins at time 0 and switches at 0.1242 seconds to congestion avoidance. The measured data
    1. Chart

       Description automatically generated
14. The throughput of the packets is 152975 bytes for all data and it was completed in 0.410917 seconds, thus I have 2.97821696mbps as the throughput. It is hard to tell when slow start begins as my packets are so large, thus I believe my system is in congestion avoidance for most of the TCP operation.
    1. Chart

       Description automatically generated