CSCE 47503 Computer Networks – Wireshark TCP

Name: Blake Williams

ID: 010974718

35 points

11 questions

# Instructions

* Type your work, print it to a **single** PDF, and upload it to Blackboard before the due date and time. It is strongly suggested that you use the given document.
* Show all of your work. Correct answers alone may not carry full credit without proper justification and details of steps.
* -2 points if you do not insert your name and ID at the top of the document.
* -5 points if it is not typed or legible. For this homework, you may scan it with something like the CamScanner app, but just make sure it is a legible PDF.
* -5 points if it is not a PDF file.
* -5 points if it is not a single PDF file. Submit one PDF file. Do not submit zip files containing one or more files.
* -5 points if you present the worked problems out of order. In other words, please present the problems in the order assigned, 1, 2, 3, …

Please use the *tcp-ethereal-trace-1* pcap file provided to youto answer all the questions **except for question 3.**

1. [2 pts.] What is the IP address and TCP port number used by the client computer (source) that transfers the file to gaia.cs.umass.edu? To answer this question, it’s probably easiest to select an HTTP message and explore the details of the TCP packet used to carry this HTTP message using the “details of the selected packet header window” (refer to Figure 2 in the “Getting Started with Wireshark” Lab if you’re uncertain about the Wireshark windows).

IP ADDR = 192.168.1.102

PORT = 1161

1. [2 pts.] What is the IP address of gaia.cs.umass.edu? What port number is it sending and receiving TCP segments for this connection?

IP ADDR = 128.119.245.12

PORT = 80

1. [3 pts.] For your own trace, what is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu? Please attach a screenshot or a picture, e.g., to print a packet, use File->Print, choose Selected packet only, choose Packet summary line, and select the minimum amount of packet detail you need to answer the question.



Client IP = 192.168.0.188

Port = 36692

1. [3 pts.] What is the sequence number of the TCP SYN segment used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies it as an SYN segment? Please attach a screenshot with the corresponding packet(s) highlighted.
   1. Sequence = 0
   2. You know it is a SYN because the SYN flag is set

A screenshot of a computer

Description automatically generated

1. [3 pts.] What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment? Please attach a screenshot with the corresponding packet(s) highlighted.
   1. Sequence = 0
   2. You know It is a SYNACK because the SYN and ACK flags are set

A screenshot of a computer

Description automatically generated

1. [2 pts.] What is the sequence number of the TCP segment containing the HTTP POST command? To find the POST command, dig into the packet content field at the bottom of the Wireshark window and look for a segment with a “POST” within its DATA field. Please attach a screenshot with the corresponding packet(s) highlighted.
   1. Sequence = 1
   2. A screenshot of a computer

      Description automatically generated
2. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What are the sequence numbers of the first six TCP connection segments (including the HTTP POST segment)? At what time was each segment sent? When was the ACK for each segment received? Given the difference between when each TCP segment was sent and its acknowledgment was received, what is the RTT value for each of the six segments? What is the EstimatedRTT value (see Section 3.5.3, page 242 in text) after receiving each ACK? Assume that the value of the EstimatedRTT is equal to the measured RTT for the first segment and then is computed using the EstimatedRTT equation on page 242 for all subsequent segments.

*Note:* Wireshark has a nice feature that allows you to plot the RTT for each TCP segment sent. Select a TCP segment in the “listing of captured packets” window sent from the client to the gaia.cs.umass.edu server. Then select *Statistics->TCP Stream Graph->Round Trip Time Graph.*

Answer:

[2 pts.] The HTTP POST segment is considered as the first segment. Segments 1 – 6 are No. 4\_\_, \_5\_, \_7\_, \_8\_, \_10\_, and \_11\_ in this trace respectively. The ACKs of segments 1 – 6 are No. \_6\_, \_9\_, \_12\_, \_14\_, \_15\_, and \_16\_ in this trace.

[2 pts.] Fill in the sequence number for Segments 1– 6 (use relative sequence# instead of raw sequence#).

Segment 1 sequence number: \_\_1\_\_  
Segment 2 sequence number: \_\_566\_\_   
Segment 3 sequence number: \_2026\_\_\_   
Segment 4 sequence number: \_3486\_\_\_  
Segment 5 sequence number: \_4946\_\_\_   
Segment 6 sequence number: \_\_6406\_\_

[3 pts.] The sending time and the received time of ACKs are tabulated in the following table.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Sent time** | **ACK received time** | **RTT (seconds)** |
| Segment 1 | 08:44:20.596858000 | 08:44:20.624318000 | 0.027460000 |
| Segment 2 | 08:44:20.612118000 | 08:44:20.647675000 | 0.035557000 |
| Segment 3 | 08:44:20.624407000 | 08:44:20.694466000 | 0.070059000 |
| Segment 4 | 08:44:20.625071000 | 08:44:20.739499000 | 0.114428000 |
| Segment 5 | 08:44:20.647786000 | 08:44:20.787680000 | 0.139894000 |
| Segment 6 | 08:44:20.648538000 | 08:44:20.838183000 | 0.189645000 |

[3 pts.] EstimatedRTT = 0.875 \* EstimatedRTT + 0.125 \* SampleRTT

EstimatedRTT after the receipt of the ACK of segment 1:   
EstimatedRTT = RTT for Segment 1 = \_0.02746\_\_\_\_\_\_\_ second

EstimatedRTT after the receipt of the ACK of segment 2:  
EstimatedRTT = \_\_\_\_\_\_\_\_0.28594625\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

EstimatedRTT after the receipt of the ACK of segment 3:  
EstimatedRTT = \_\_\_\_\_\_\_\_\_ 0.0294649219\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

EstimatedRTT after the receipt of the ACK of segment 4:  
EstimatedRTT = \_\_\_\_\_\_\_\_\_\_\_\_\_ .0345391816\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

EstimatedRTT after the receipt of the ACK of segment 5:  
EstimatedRTT = \_\_\_\_\_\_\_\_\_\_\_\_ 0.0445252839\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

EstimatedRTT after the receipt of the ACK of segment 6:  
EstimatedRTT = \_\_\_\_\_\_\_\_\_\_ 0.0564463734\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. [3 pts.] What is the length of each of the first six TCP segments? Please attach a screenshot with the corresponding packet(s) highlighted.

A screenshot of a computer

Description automatically generated

First TCP = 619

2-6 TCP = 1514

1. [3 pts.] What is the minimum available buffer space advertised at the receiver for the entire trace? Does the lack of receiver buffer space ever throttle the sender? Please attach a screenshot with the corresponding packet(s) highlighted.
   1. 5840 is the minimum available buffer space advertised.
   2. No, because the advertised window sizes are larger than the lower threshold. Therefore the sender is not limited by the receiver buffer size.

A screenshot of a computer

Description automatically generated

1. [2 pts.] Are there any retransmitted segments in the trace file? What did you check for (in the trace) to answer this question?
   * 1. No, you can check ack values for duplicate values and there are not any.
2. [2 pts.] What is the TCP connection's throughput (bytes transferred per unit time)? Explain how you calculated this value.
   1. 164091/(26.026211 –20.596858)
   2. 30222.9381659