Wireshark Lab: TCP

Name(s): ____

It is recommended that you keep RFC 9293 open while working on this lab.

Useful Wireshark features for this lab (activated from popup menu):

- Set / Unset Time Reference (Cmd-T on MacOS)
- Follow ⇒ TCP Stream
- Filter by TCP port number
  - By source port: `tcp.srcport == NNNNN`
  - By destination port: `tcp.dstport == NNNNN`
  - By either port: `tcp.port == NNNNN`

Ideal submission of your report: put your answer directly in the PDF (as a textbox) and upload the edited/annotated PDF to Bb.

General

1. (2 points) HTTP POST for transferring/uploading file `alice.txt` `gaia.cs.umass.edu`
   (a) The IP address of the client computer (source): ________________
   (b) The TCP port number of the client computer (source): __________
2. (2 points) HTTP POST for transferring/uploading file `alice.txt` `gaia.cs.umass.edu`
   (a) The IP address of the `gaia.cs.umass.edu`: ____________________
   (b) The TCP port on `gaia.cs.umass.edu` for sending/receiving TCP segments for this connection is ________

TCP Basics

3. (3 points) Answer the following question for the TCP segments
   (a) What is the **raw** sequence number[1] of the TCP SYN segment that is used to initiate the TCP connection between the client computer and `gaia.cs.umass.edu` __________.
   (b) What is it in this TCP segment that identifies the segment as a SYN segment? ________________
   (c) Will the TCP receiver in this session be able to use Selective ACK? __________
4. (4 points) Sync Acknowledgement
   (a) What is the **raw** *sequence number* of the SYNACK segment sent by `gaia.cs.umass.edu` to the client computer in reply to the SYN? ________
   (b) What is it in the segment that identifies the segment as a SYNACK segment? ________________________
   (c) What is the **raw** value of the ACK field in the SYNACK segment? ____________
   (d) How did `gaia.cs.umass.edu` determine that value? ____________
5. (3 points) TCP segments of HTTP POST
   (a) What is the sequence number of the TCP segment containing the header of the HTTP POST command? Raw: ____________ Relative: ____________
   (b) Number of bytes int the payload of this TCP segment: ________
   (c) Did all the data in `alice.txt` fit into this single segment? ________
6. (5 points) Consider the TCP segment containing the HTTP POST as the first segment in the data transfer:
   (a) At what time was the first segment (the one containing the HTTP POST) ____________

[1] Not the number under the "No" column used by Wireshark. Also the answer is NOT zero

(b) At what time was the ACK for this first segment received? ________________

(c) What is the RTT for this first data-containing segment? ________________

(d) What is the RTT for the second data-containing segment? ________________

(e) **Skip the question about** `EstimatedRTT`

7. (1 point) What is the length (header + payload) of each of the first four data-carrying TCP segments? ______________________________________

8. (2 points) (a) What is the minimum amount of available buffer space advertised to the client by `gaia.cs.umass.edu` among these four segments? ______________________________________

   (b) Does the lack of receiver buffer space ever throttle the sender for these four segments? ____

9. (2 points) (a) Any retransmitted segment in the trace file (from client to server)? __________

   (b) What did you check? ____

10. (2 points) (a) How much data does the receiver typically acknowledge in an ACK among the first ten data-carrying segment sent from the client to `gaia.cs.umass.edu` ________________

    (b) Can you identify cases where the receiver is ACKin every other received segment? Explain ____

11. (2 points) What is the throughput (bytes transferred per unit time) for the TCP connection? Explain your calculation