Collin Easley

Tasks:
Please in your submission, only include the following questions and your answers under each corresponding question. DO NOT HAND IN THE ABOVE LAB INSTRUCTIONS! And again, like assignment 1,
you can choose to type in or submit through hand-written.
1. (10 points) What is the IP address and TCP port number used by the client computer (source) that is transferring the alice.txt 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 3 if you're uncertain about the Wireshark windows).

The IP address for the trace file for the client is 128.119.245.12 and the source port for the client is 80

2. (10 points) What is the IP address of gaia.cs.umass.edu? On what port number is it sending and
receiving TCP segments for this connection?

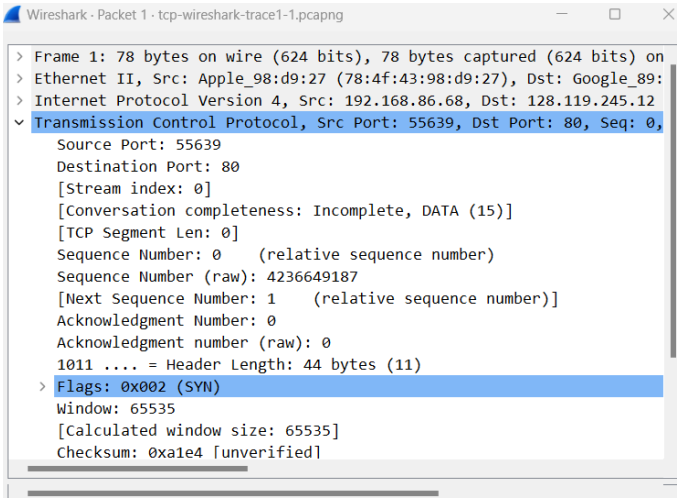
The IP address for the url is 192.168.86.68. Where the URL for sending and receiving 55639

now change Wireshark's "listing of captured packets" window so that it shows information about the
TCP segments containing the HTTP messages, rather than about the HTTP messages, as in Figure 8.
Answer the following questions for the TCP segments:

3. (10 points) (also include the screenshot(s) highlight the packet that proves your answer) What is
the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? (Note: this is the "raw" sequence number carried in the TCP segment itself; it is NOT the packet # in the "No." column in the Wireshark window. Remember there is no such thing as a "packet number" in TCP or UDP; as you know, there are sequence numbers in TCP and that's what we're after here. Also note that this is not the relative sequence number with respect to the starting sequence number of this TCP session.). What is it in this TCP segment that identifies the segment as a SYN segment?

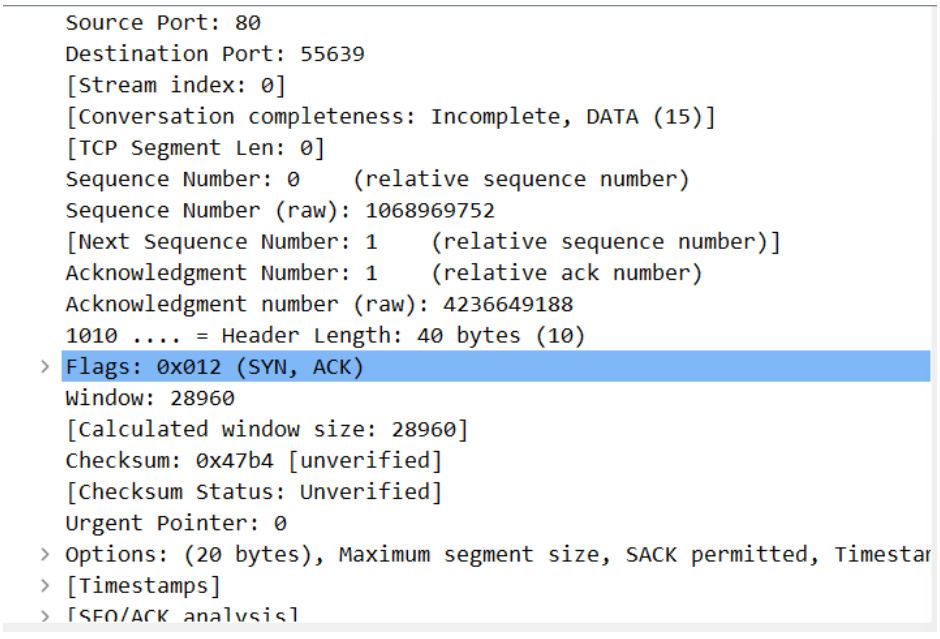
The sequence number is 0 because it is the initial

The presence of SYN in the flags field is what identifies this as a SYN segment



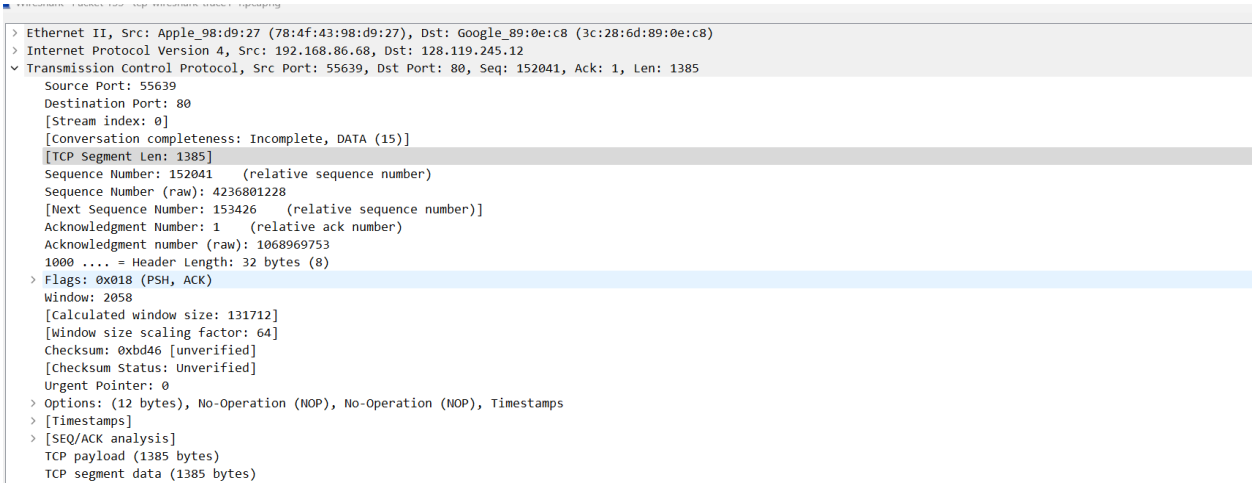
4. (10 points) (also include the screenshot(s) highlight the packet that proves your answer) What is
the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer
in reply to the SYN? What is it in the segment that identifies the segment as a SYNACK segment?
What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value?

The sequence number of the SYN-ACK segment is 1068969752 (raw).
The segment is identified as a SYN-ACK segment because the "SYN" and "ACK" flags are set in the Flags field
The value of the Acknowledgment field in the SYN-ACK segment is 1
The URL determined the value of the acknowledgement field by acknowledging the intial SYN packet sent by the client. The acknowledgment number is set to one more than the sequence number of the received SYN packet. So the URL is ready to receive the data that starts at sequence one.



5. (10 points) (also include the screenshot(s) highlight the packet that proves your answer) What is
the sequence number of the TCP segment containing the header of the HTTP POST command?
Note that in order to find the POST message header, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with the ASCII text "POST" within its DATA field2,3. How many bytes of data are contained in the payload (data) field of this TCP segment? Did all of the data in the transferred file alice.txt fit into this single segment?

Sequence number of the TCP segment containing the header of the HTTP POST is 4236801228 (raw).
Payload field is 1385 bytes of data
Not all the data in the txt file fit in a single segment. The file size indicated in the content length is 152359 bytes which is larger than the payload field. Therefore can not fit into a single segment.



6. (10 points)Are there any retransmitted segments in the trace file? What did you check for (in the
trace) in order to answer this question?

I could not find any i looked at the info column for the trace file looking for retransmission and came up empty

7. (40 points+20 extra points) Consider the TCP segment containing the HTTP “POST” as the first
segment in the data transfer part of the TCP connection.
At what time was the first segment (the one containing the HTTP POST) in the data-transfer part of the TCP connection sent? (10 points)
At what time was the ACK for this first data-containing segment received? (10 points)
What is the RTT for this first data-containing segment? (10 points)
What is the RTT value the second data-carrying TCP segment and its ACK? (10 points)
What is the EstimatedRTT value (see slides) after the ACK for the second data-carrying segment is received? Assume that in making this calculation after the received of the ACK for the second segment, that the initial value of EstimatedRTT is equal to the measured RTT for the first segment, and then is computed using the EstimatedRTT equation on the slides given, and a value of = 0.125. (20 extra points, to get full points, please show equations and details, as well as the screenshots of the Round Trip Time Graph)
Note: Wireshark has a nice feature that allows you to plot the RTT for each of the TCP segments sent. Select a TCP segment in the “listing of captured packets” window that is being sent from the client to the gaia.cs.umass.edu server. Then select: Statistics->TCP Stream Graph->Round Trip Time Graph.
2 Hint: this TCP segment is sent by the client soon (but not always immediately) after the SYNACK segment is
received from the server.
3 Note that if you filter to only show “http” messages, you’ll see that the TCP segment that Wireshark associates
with the HTTP POST message is the last TCP segment in the connection (which contains the text at the end of

1. The timestamp for HTTP post is Feb 2, 2021 21:43:26.840557000 Eastern Standard Time
2. The timestamp for the ACK Feb 2, 2021 21:43:26.840555000 Eastern Standard Time
3. So we solve the RTT
   RTT = time of ACK - time of segment transmission
   So RTT = Feb 2, 2021 21:43:26.840555) - (Feb 2, 2021 21:43:26.840557) = -0.000002 seconds

So its an extremely small delay

4. So we plug it in again
   RTT = (Feb 2, 2021 21:43:26.840557) - (Feb 2, 2021 21:43:26.840555) = 0.000002 seconds
5. EstimatedRTT = (1 - α) * EstimatedRTT + α * SampleRTT
   Estimate is measured RTT for first segment so .000048 seconds
   Alpha is .125
   So
   EstamatedRTT = (1-.125) *.000048 + .125 *0.000002
   EstamatedRTT = (.875*0.000048) + (0.125 * 0.000002)
   estimatedRtt = 0.000042 seconds