LAPORAN KONSEP JARINGAN

TCP Header Analysis using wireshark

Iwan Syarif S.Kom., M.Kom., M.Sc., Ph.D.

Dzikri Mutawakkil

3121600041

2 D4 Teknik Informatika B

TEKNIK INFORMATIKA
DEPARTEMEN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK ELEKTRONIKA NEGERI SURABAYA
2021/2022

1. **What is the IP address and TCP port number used by the client computer (source) that is transferring 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.**

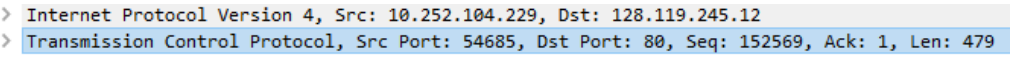
   IP Source : 10.252.104.229
   Source Port Number : 54685

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

   IP Destination : 128.119.245.12
   Destination Port Number : 80

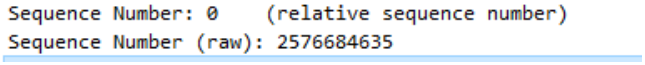
3. **What is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu?**

   IP Source : 10.252.104.229
   Source Port Number : 54685



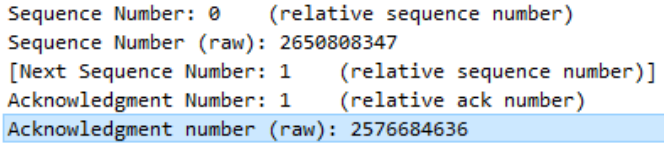
4. **What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?**

   Sequence Number: 0 (relative sequence number)
   Sequence Number (raw): 2576684635



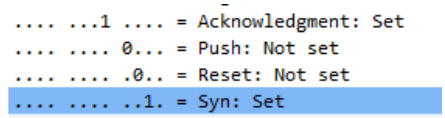
5. **What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?**

   Sequence Number: 0 (relative sequence number)
   Sequence Number (raw): 2650808347
   Acknowledgment Number: 1 (relative ack number)
   Acknowledgment number (raw): 2576684636



   Ack number didapat dari Syn number + 1
   Sequence Ack Number: 0 + 1 = 1

Sequence Ack Number (raw): 2576684635 + 1 = 2576684636

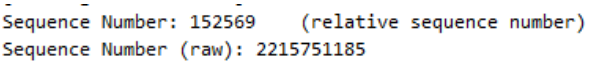


Acknowledgement dan syn flag diset bernilai 1 untuk mengindikasikan SynAck segment.

6. **What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.**

Sequence Number: 152569 (relative sequence number)

Sequence Number (raw): 2215751185



7. **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 segments in the TCP connection (including the segment containing the HTTP POST)? 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 when its acknowledgement 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 the receipt of 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.**

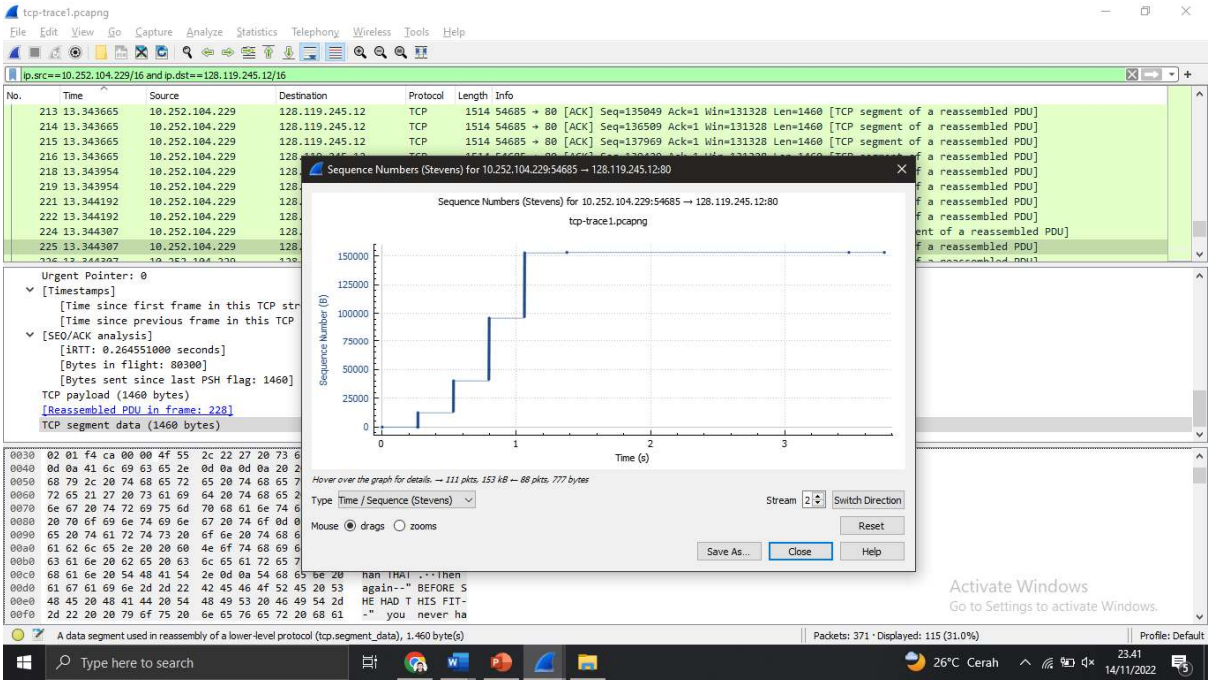
Note: Wireshark has a nice feature that allows you to plot the RTT for each of the TCP segments sent. Select a TCP segment in the "listing of captured packets" window that is being sent from the client to the gaia.cs.umass.edu server. Then select: Statistics->TCP Stream Graph- >Round Trip Time Graph.

Http post 6 segment pertama ada pada nomor 50,53,54,55,56,57. Sedangkan untuk Ack segment nya berada pada nomor 75,77,80,83,86,89. Dan dapat disimpulkan seperti tabel dibawah ini

	Sent Time	**Ack Received Time**	**RTT**
Segment 1	12.547951	12.812449	0.264498000 seconds
Segment 2	12.548668	12.813168	0.264500000 seconds
Segment 3	12.548668	12.813285	0.264617000 seconds
Segment 4	12.548668	12.813388	0.264720000 seconds
Segment 5	12.548668	12.813517	0.264849000 seconds
Segment 6	12.548668	12.813641	0.264973000 seconds

EstimatedRTT after the receipt of the ACK of segment 1:
EstimatedRTT : RTT for Segment 1 = 0.264498 second
EstimatedRTT after the receipt of the ACK of segment 2:
EstimatedRTT : 0.875 * 0.264498 + 0.125 * 0.2645 = 0.26449825
EstimatedRTT after the receipt of the ACK of segment 3:
EstimatedRTT : 0.875 * 0. 26449825+ 0.125 * 0.264617 = 0.26451309375
EstimatedRTT after the receipt of the ACK of segment 4:

EstimatedRTT : 0.875 * 0. 26451309375+ 0.125 * 0. 26472= 0.26453895703125
EstimatedRTT after the receipt of the ACK of segment 5:
EstimatedRTT : 0.875 * 0. 26453895703125+ 0.125 * 0. 264849 = 0.26457771240234375
EstimatedRTT after the receipt of the ACK of segment 6:
EstimatedRTT : 0.875 * 0. 26457771240234375+ 0.125 * 0. 264973= 0.2642712335205078125



8. **What is the length of each of the first six TCP segments?**
   First TCP Length
   [TCP Segment Len: 728]
   Sixth TCP Length
   [TCP Segment Len: 1460]

9. **What is the minimum amount of available buffer space advertised at the received for the entire trace? Does the lack of receiver buffer space ever throttle the sender?**
   Minimum nya adalah 29200 sesuai pada ACK pertama yang diterima.

   Sampai terakhir di ukuran 204672 dan pengirim tidak akan pernah memenuhi penyimpanan untuk menerima dengan memeriksanya.

10. **Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?**
    Tidak ada, Ini terlihat dari trace file sequence number terhadap waktu (Stevens). Tiap sequence number hanya memiliki 1 time, artinya tidak ada retransmisi segmen.

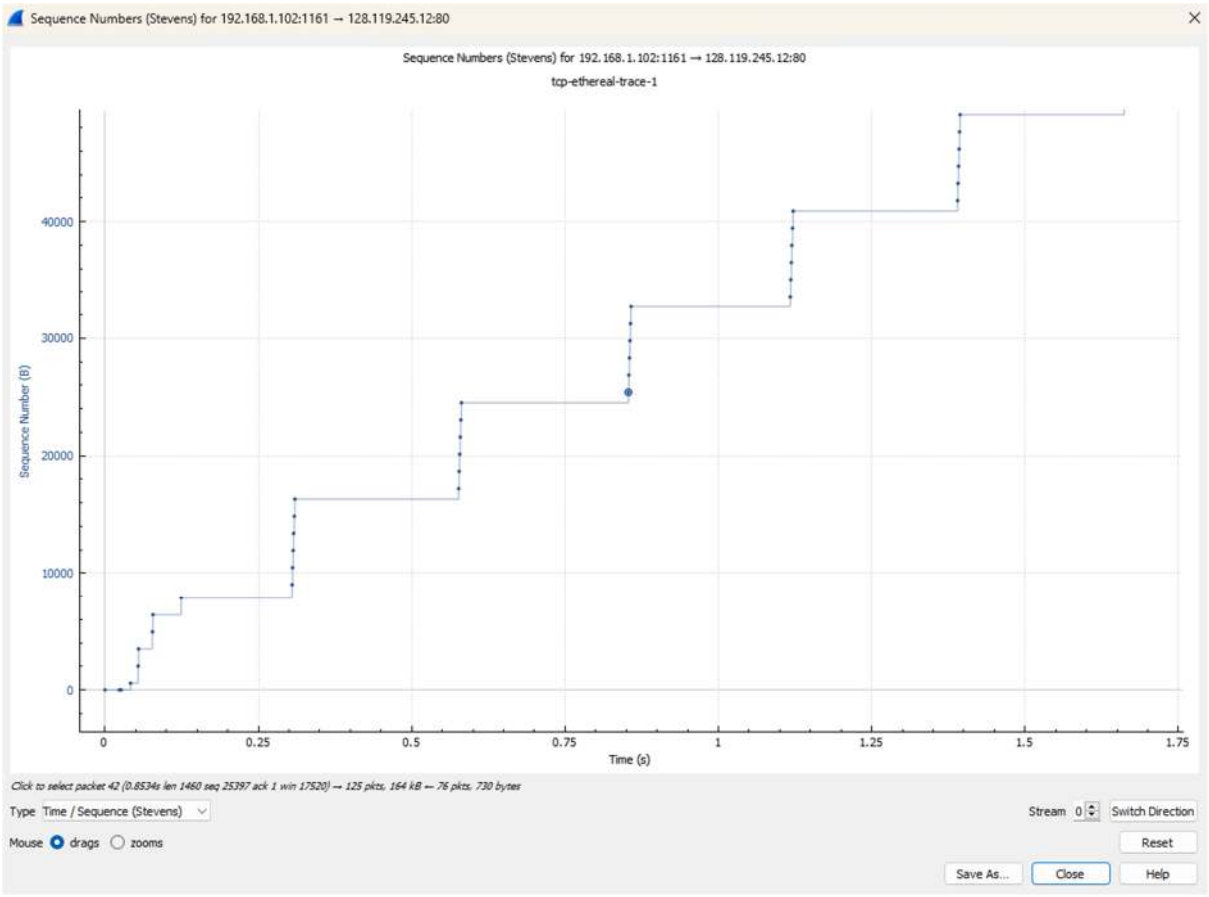
11. **How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment (see Table 3.2 on page 250 in the text).**

	acknowledged sequence number	acknowledged data
ACK 1	566	566
ACK 2	2026	1460
ACK 3	3486	1460
ACK 4	4946	1460
ACK 5	6406	1460
ACK 6	7866	1460
ACK 7	9013	1147
ACK 8	10473	1460
ACK 9	11933	1460
ACK 10	13393	1460
ACK 11	14853	1460
ACK 12	16313	1460

12. **What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value**

- The computation of TCP throughput largely depends on the selection of averaging time period. As a common throughput computation, in this question, we select the average time period as the whole connection time. Then, the average throughput for this TCP connection is computed as the ratio between the total amount data and the total transmission time. The total amount data transmitted can be computed by the difference between the sequence number of the first TCP segment (i.e. 1 byte for No. 4 segment) and the acknowledged sequence number of the last ACK (164091 bytes for No. 202 segment). Therefore, the total data are 164091 - 1 = 164090 bytes. The whole transmission time is the difference of the time instant of the first TCP segment (i.e., 0.026477 second for No.4 segment) and the time instant of the last ACK (i.e., 5.455830 second for No. 202 segment). Therefore, the total transmission time is 5.455830 - 0.026477 = 5.4294 seconds. Hence, the throughput for the TCP connection is computed as 164090/5.4294 = 30.222 KByte/sec.

13. **Use the Time-Sequence-Graph(Stevens) plotting tool to view the sequence number versus time plot of segments being sent from the client to the gaia.cs.umass.edu server. Can you identify where TCP's slowstart phase begins and ends, and where congestion avoidance takes over? Comment on ways in which the measured data differs from the idealized behavior of TCP that we've studied in the text**



14. Answer each of two questions above for the trace that you have gathered when you transferred a file from your computer to gaia.cs.umass.edu