**LAPORAN KONSEP JARINGAN**

**[Teori 05] Wireshark: TCPv8.0**



Disusun Oleh:

Aldow Fan Dzikri (NRP. 3121500022)

2 D3 ITA

Dosen Pengampu:

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

**PROGRAM STUDI D3 TEKNIK INFORMATIKA**

**DEPARTEMEN TEKNIK INFORMATIKA DAN KOMPUTER**

**POLITEKNIK ELEKTRONIKA NEGERI SURABAYA**

**2022**

Questions:

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?



Pada gambar diatas IP address Client Computer yang mentransfer ke gaia.cs.umass.edu adalah 192.168.1.102 dengan TPC Port 1161.

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



Pada gambar diatas IP address dari gaia.cs.umass.edu yang menerima transfer dari Client Computer adalah 128.119.245.12 dengan TCP Port number 80.

If you have been able to create your own trace, answer the following question:

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



Pada gambar diatas IP address yang digunakan komputer saya yang melakukan transfer file ke gaia.cs.umass.edu adalah 128.119.245.12 dengan TCP Port number 9051

1. 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?

Nomor urut segmen TCP SYN adalah 0 karena digunakan untuk meniru koneksi TCP antara komputer klien dan gaia.cs.umass.edu. Berdasarkan gambar di atas, pada bagian Flags, flag Syn diatur ke 1 yang menunjukkan bahwa segmen ini adalah segmen SYN.

1. 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?



Berdasarkan gambar diatas urutan segmen SYNACK yang dikirim oleh gaia.cs.umass.edu ke clien computer yang membalas ke syn adalah 0.

Nilai acknowledgement di segmen SYNACK adalah 1. Nilai acknowledgement di segmen SYNACK ditentukan oleh server gaia.cs.umass.edu. Server menambahkan 1 ke nomor urut awal segmen SYN dari komputer klien. Untuk kasus ini, nomor urut awal segmen SYN dari komputer klien adalah 0, sehingga nilai bidang acknowlegement di segmen SYNACK adalah 1. Segmen akan diidentifikasi sebagai segmen SYNACK jika flag SYN dan acknowledgmenent di segmen disetel ke 1.

1. 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?



Terlihat seperti gambar diatas bahwa isi segmentnya HTTP Post dan sequence number segmentnya adalah 1.

1. 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.



According to above figures, the segments 1‐6 are No. 6, 7, 8, 9, 11 and 14. The ACK of segments 1‐6 are No. 10, 12, 13, 16, 19 and 22.

Segment 1 sequence number is 1

Segment 2 sequence number is 579

Segment 3 sequence number is 716

Segment 4 sequence number is 2164

Segment 5 sequence number is 3612

Segment 6 sequence number is 5060

Recording the sending time and received time of ACKs:



According to the formula:

EstimatedRTT = 0.875 \* EstimatedRTT + 0.125 \* SampleRTT

EstimatedRTT after the receipt of the ACK of segment 1: EstimatedRTT = RTT for Segment 1 = 0.095674 s EstimatedRTT after the receipt of the ACK of segment 2: EstimatedRTT = 0.875 \* 0.095674 + 0.125 \* 0.095864= 0.09569775 s EstimatedRTT after the receipt of the ACK of segment 3: EstimatedRTT = 0.875 \* 0.09569775 + 0.125 \* 0.09682= 0.09583803125 s EstimatedRTT after the receipt of the ACK of segment 4: EstimatedRTT = 0.875 \* 0.09583803125 + 0.125 \* 0.098154= 0.09612752734 s EstimatedRTT after the receipt of the ACK of segment 5: EstimatedRTT = 0.875 \* 0.09612752734 + 0.125 \* 0.112884= 0.09822208642

EstimatedRTT after the receipt of the ACK of segment 6: EstimatedRTT = 0.875 \*0.09822208642 + 0.125 \* 0.113781= 0.10016695061 s



1. What is the length of each of the first six TCP segments?



The length of the first TCP segment is 578 bytes, the length of the second TCP segment is 137 bytes. The length of each of the following five TCP segments is 1448 bytes

1. 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?



The minimum amount of available buffer space advertised at the received for the entire trace is indicated first ACK from the server, its value is 5792 bytes (shown in above figure). This reviver window grows until it reaches the maximum receiver buffer size of 62780 bytes. According to the trace, the sender is never throttled due to lacking of receiver buffer space.

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



There is no retransmitted segments in the trace file since in the time sequence graph (stevens), all sequence numbers are monotonically increasing.

1. 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).
2. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value

Answer the following questions for the TCP segments the packet trace tcp-etherealtrace-1 in http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip

1. 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



The slow start of the TCP seems to begin at about 0.27 seconds and then ends at about 0.35 seconds.    Congestion avoidance takes over at about 0.7 seconds because it cut down the amount being sent

1. 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.ed ?

The questions had been answered .