Zachodniopomorski
Uniwersytet Technologiczny
w Szczecinie

Network Systems Administration

Report 4 - Analysis of TCP packages with Wireshark

dr inż. Piotr Lech

Abdurrahman Karaoluk

ka46312

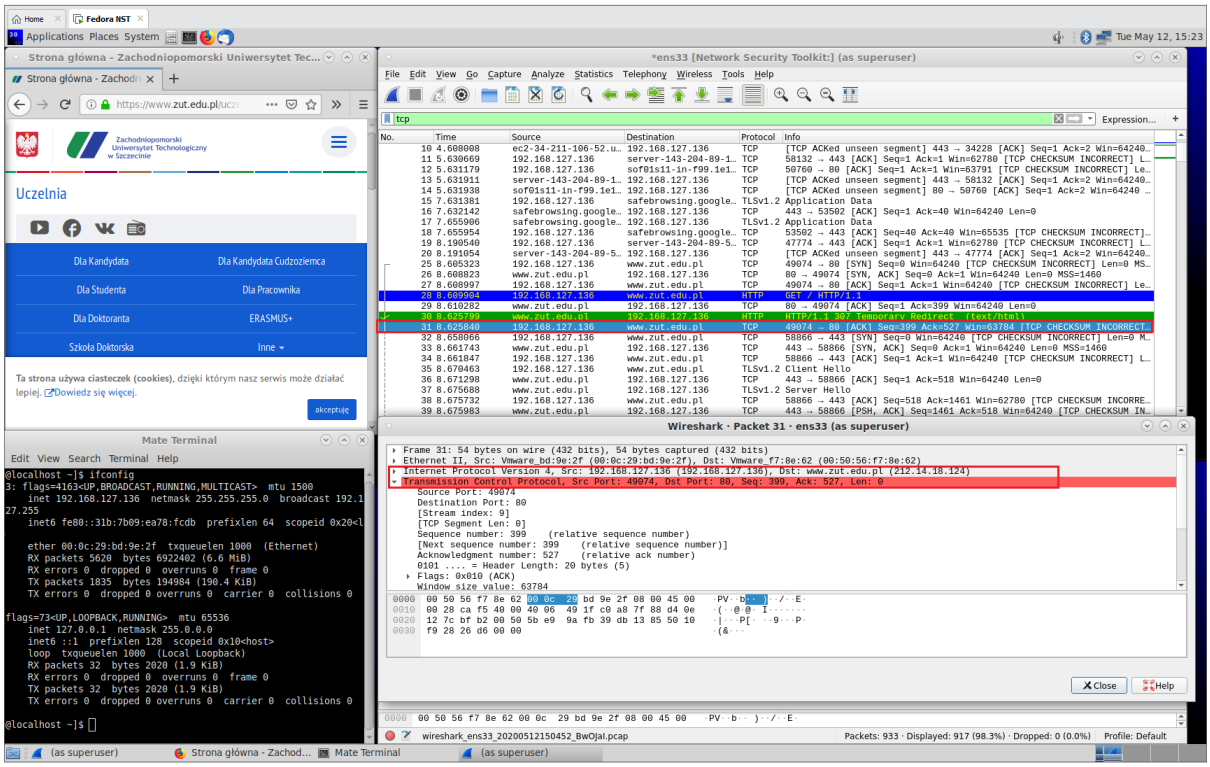
Method : "www.zut.ed.pl" address was visited on the virtual machine. The packet traffic generated was analyzed with Wireshark.

Q1- What are IP address and TCP port number used by the client computer (source) and destination address with visit to “www.zut.edu.pl” ?

A1-

	Source	Destination
IP	192.168.127.136	212.14.18.124
Port Number	49074	80

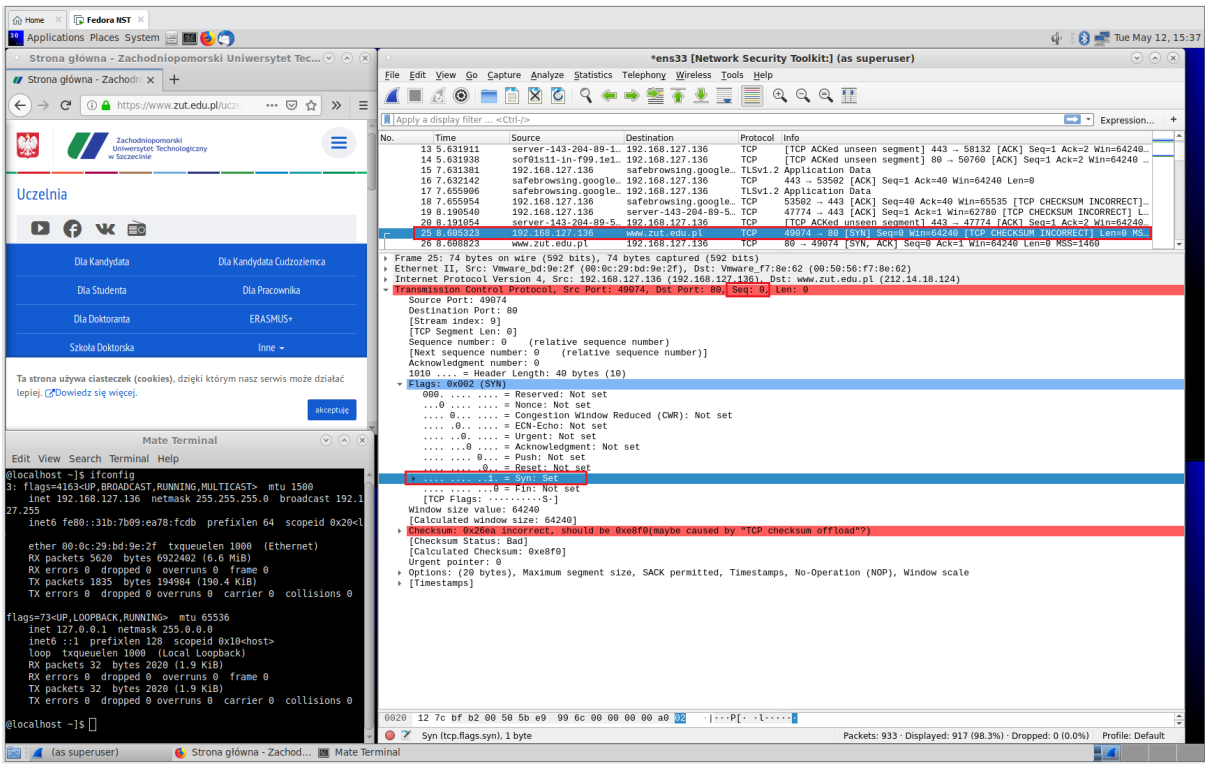
Ss1-



Q2-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?

A2- The sequence number of the TCP SYN segment is 0 since it is used to imitate the TCP connection between the client computer and “www.zut.edu.pl”. According to the screenshot below, in the Flags section, the SYN flag is set to 1 which indicates that this segment is a SYN segment.

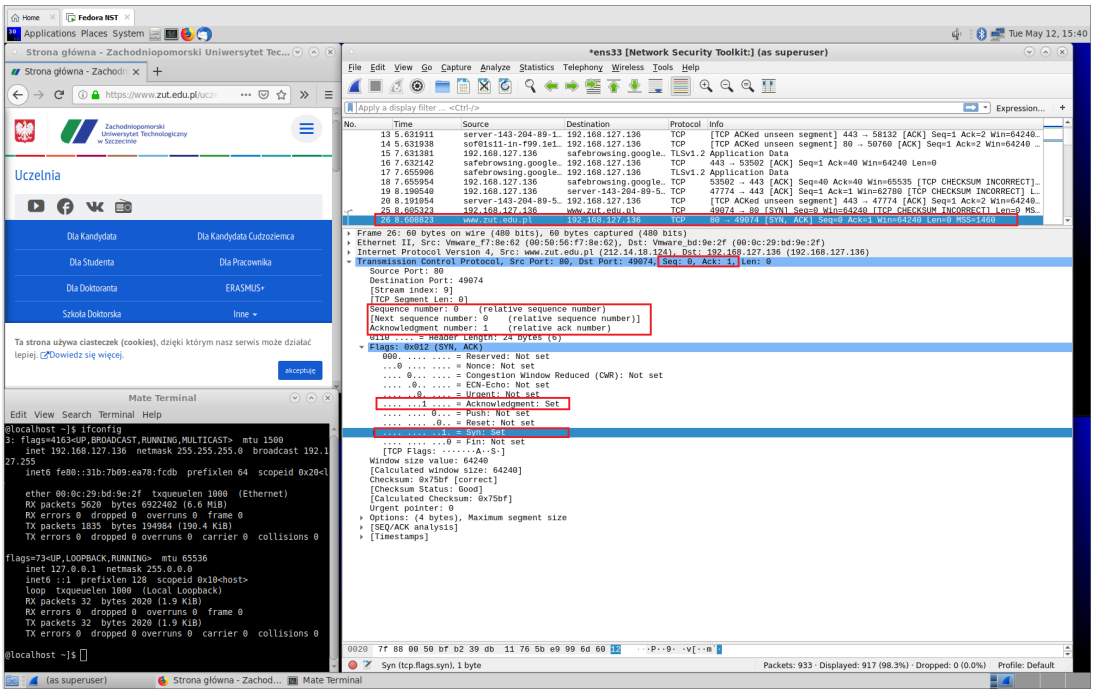
Ss2-



Q3- 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 “www.zut.edu.pl” determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

A3- The sequence number of the SYN_ACK segment sent by “www.zut.edu.pl” to the client computer in reply to the SYN is 0. The value of the acknowledgement field in the SYN_ACK segment is determined by the server “www.zut.edu.pl” The server adds 1 to the initial sequence number of the SYN segment from the client computer. For this case, the initial sequence number of the SYN segment from the client computer is 0, thus the value of the acknowledgement field in the SYN_ACK segment is 1. A segment will be identified as a SYN_ACK segment if both SYN flag and ACKnowledgement flag in the segment are set to 1.

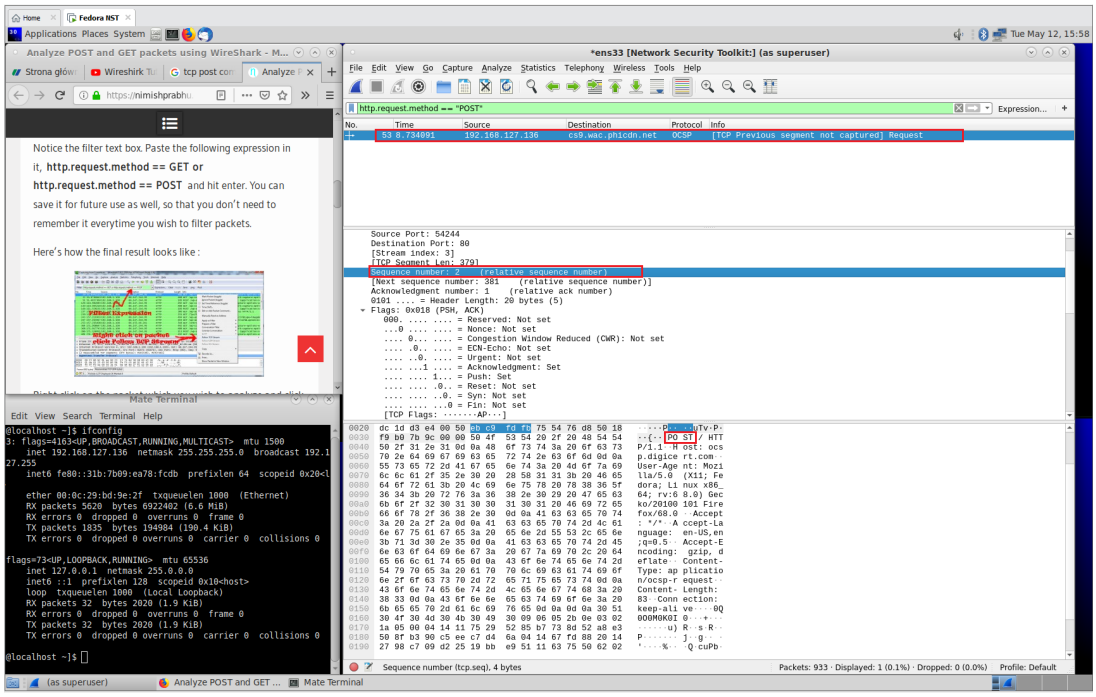
Ss3-



Q4- 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.

A4- The sequence number of the TCP segment containing the HTTP Post command is 2.

Ss4-



Q5- Consider the TCP connection.

Q1- What are the sequence numbers of two segments in the TCP connection?

A1- Sequence number for segment 1 is 1, sequence number for segment 2 is 399.

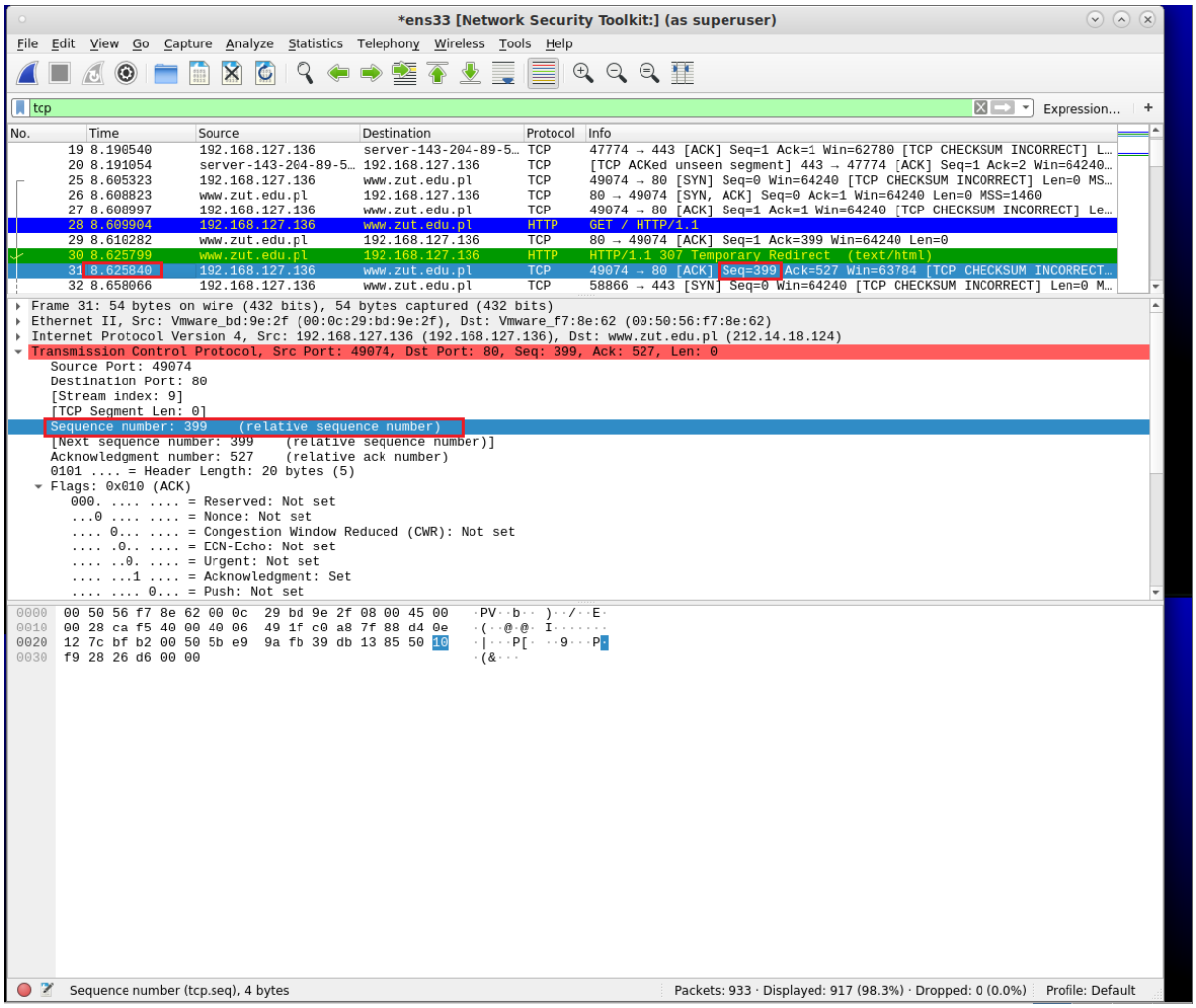
Q2- At what time was each segment sent?

A2- 9.608997 s for segment 1 and 8.625840 s for segment 2.

Q3- When was the ACK for each segment received?

A3- ACK for segment 1 was received at 9.608997 s and ACK for segment 2 is received at 8.625840 s.

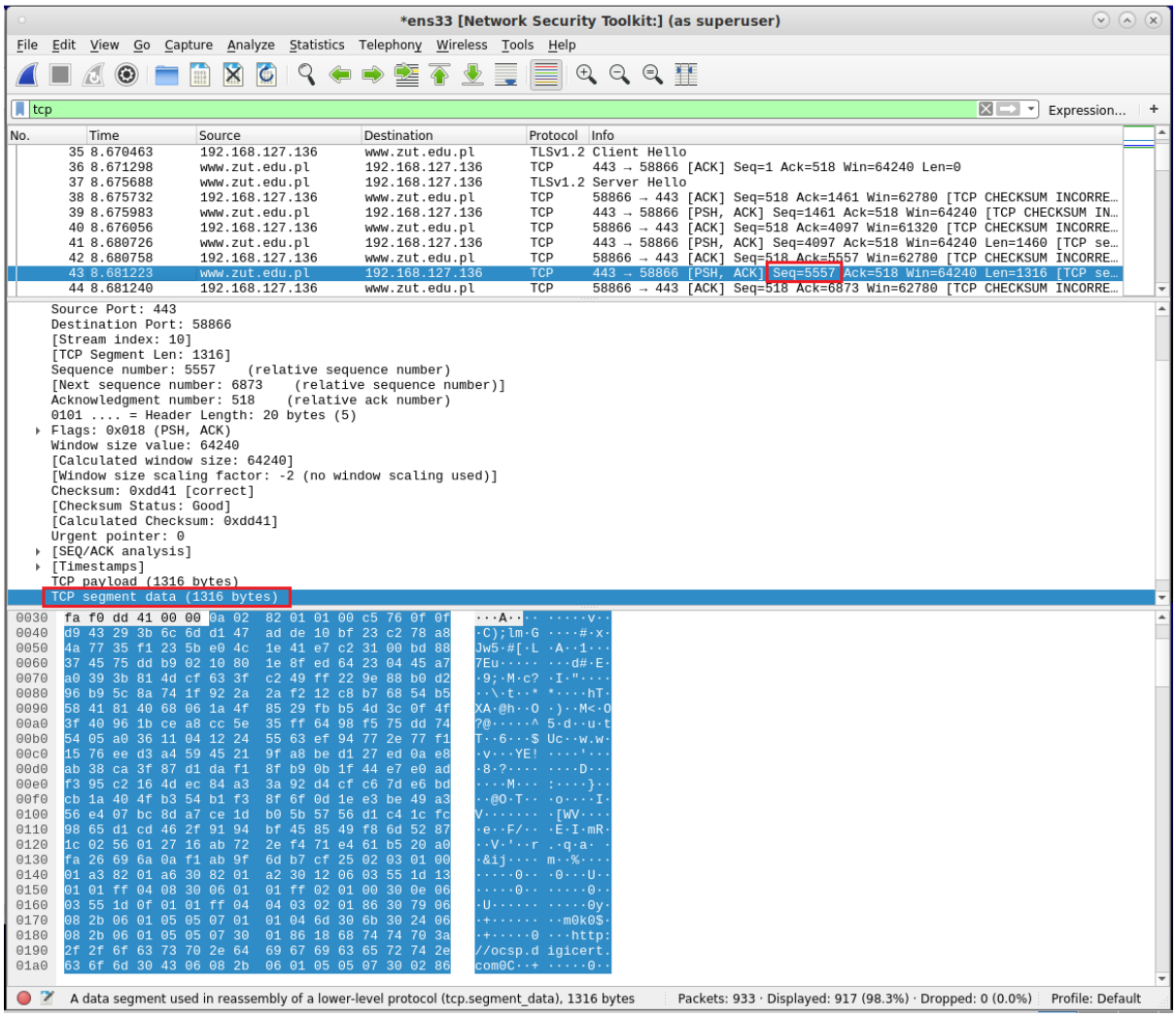
Ss5-



Q6- What is the length of any TCP segment?

A6- The length of TCP segment is 1316 bytes.

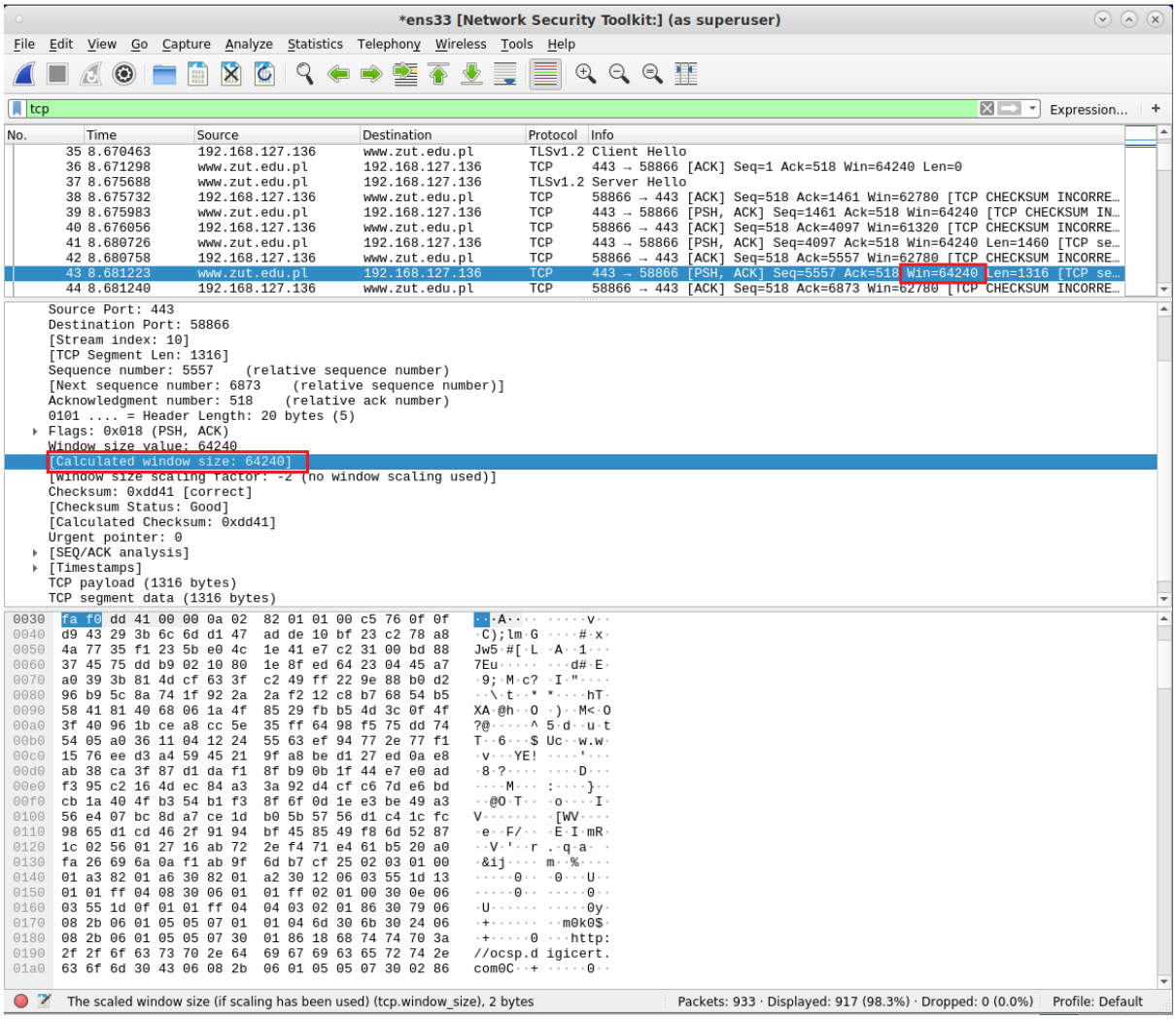
Ss6-



Q7- 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?

A7- The minimum amount of available buffer space advertised at the received is 6440 bytes.

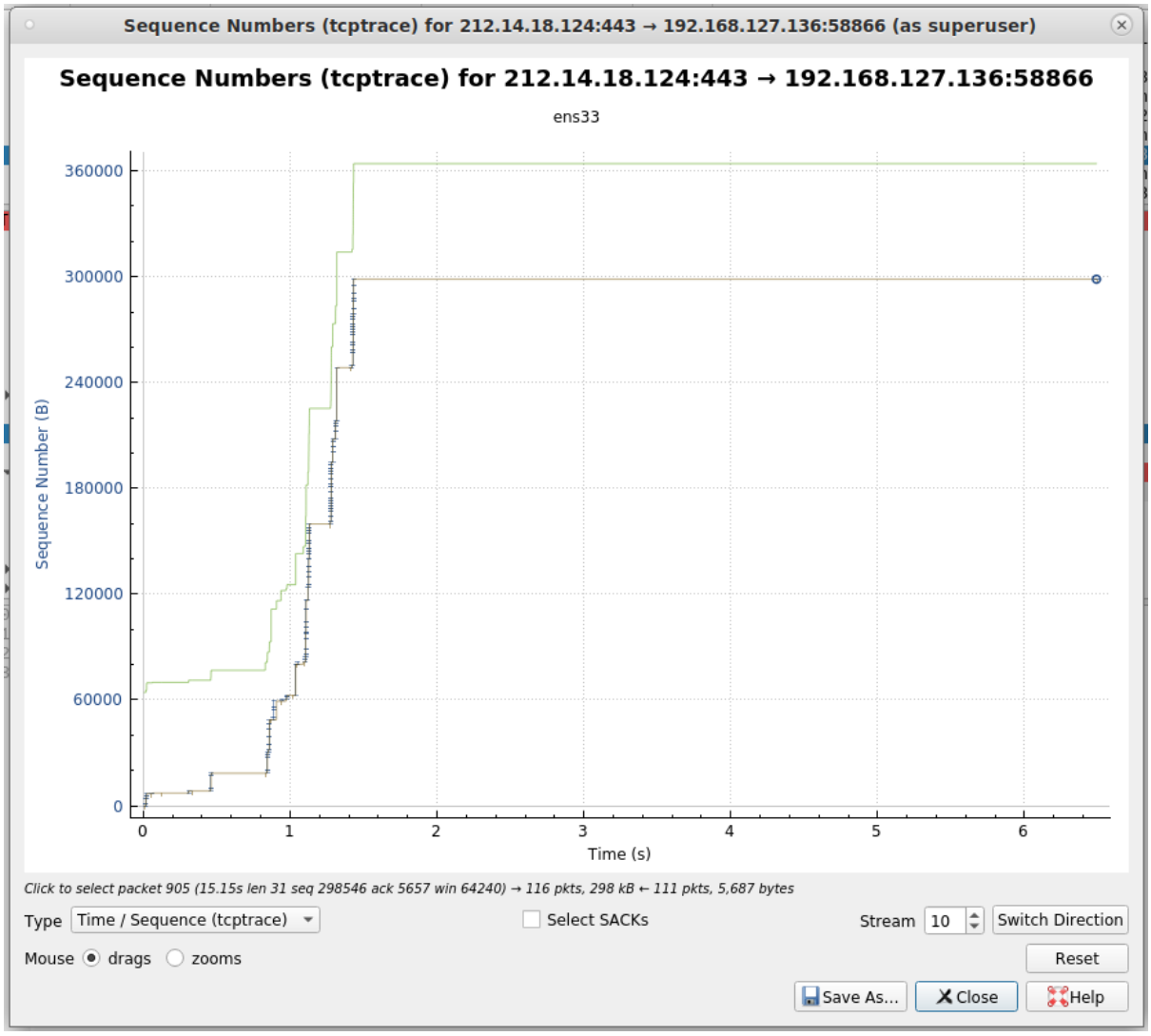
Ss7-



Q8- Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?

A8- Yes there are retransmitted segments in the trace file. This can be explained by packets with same sequence number at different time is found.

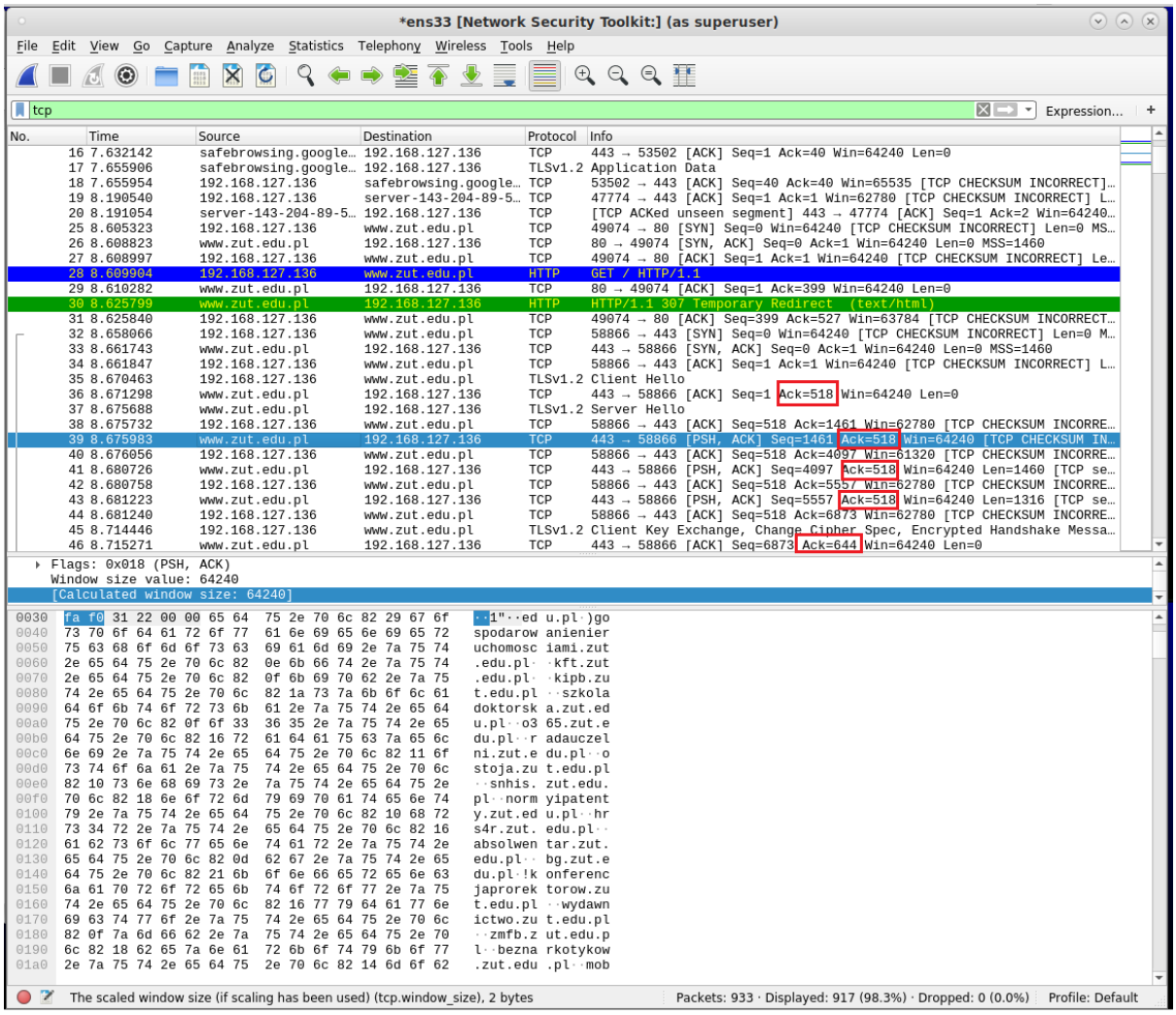
Ss8-



Q9- How much data does the receiver typically acknowledge in an ACK?

A9-
According to the screenshot below, we can see that the ACK numbers increase in the sequence of 518 and 644.

Ss9-



Q10- What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.

A10-

Throughput = (Amount of data transmitted) / (Time incurred)
Amount of data transmitted = 326,646 bytes
Time incurred = 17,491128 – 8.610282 = 8.880846
Throughput = 326646 / 8,880846
Throughput = 36.780,9553

Ss10-