Karthikeyan Rajamani
UTA ID:1001267157

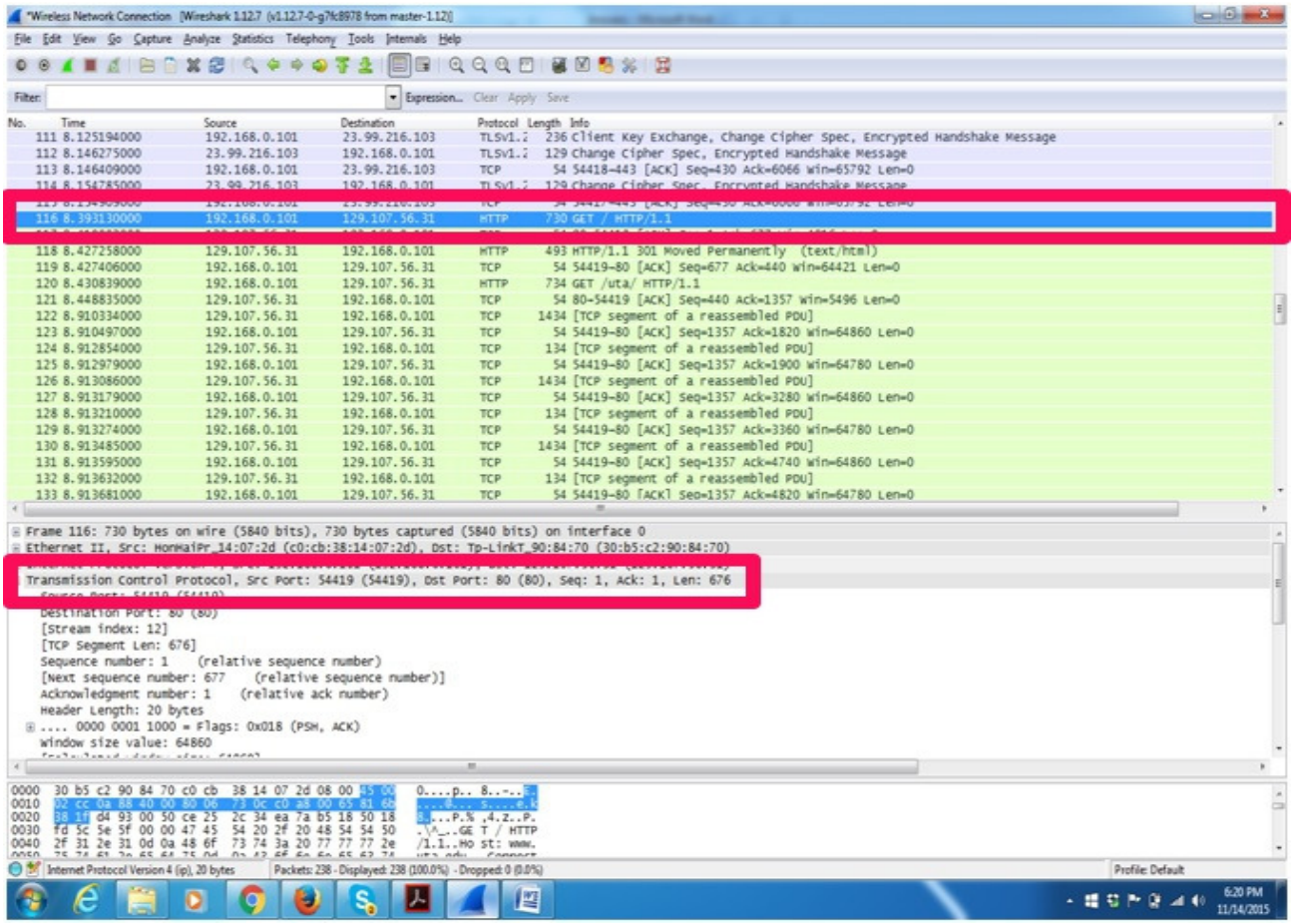
# Computer Networks CSE 5344
# Project 2 TCP Analysis using Wireshark

## Problem Set-1

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

**Client computer(source) IP address: 192.168.0.101**

**Client TCP port number:54419**




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

**IP address of UTA.edu:129.107.56.31 (Above screenshot)**

**TCP port of UTA.edu: 80**

3. What is the IP address and TCP port number used by your client computer (source) to browse the page uta.edu.

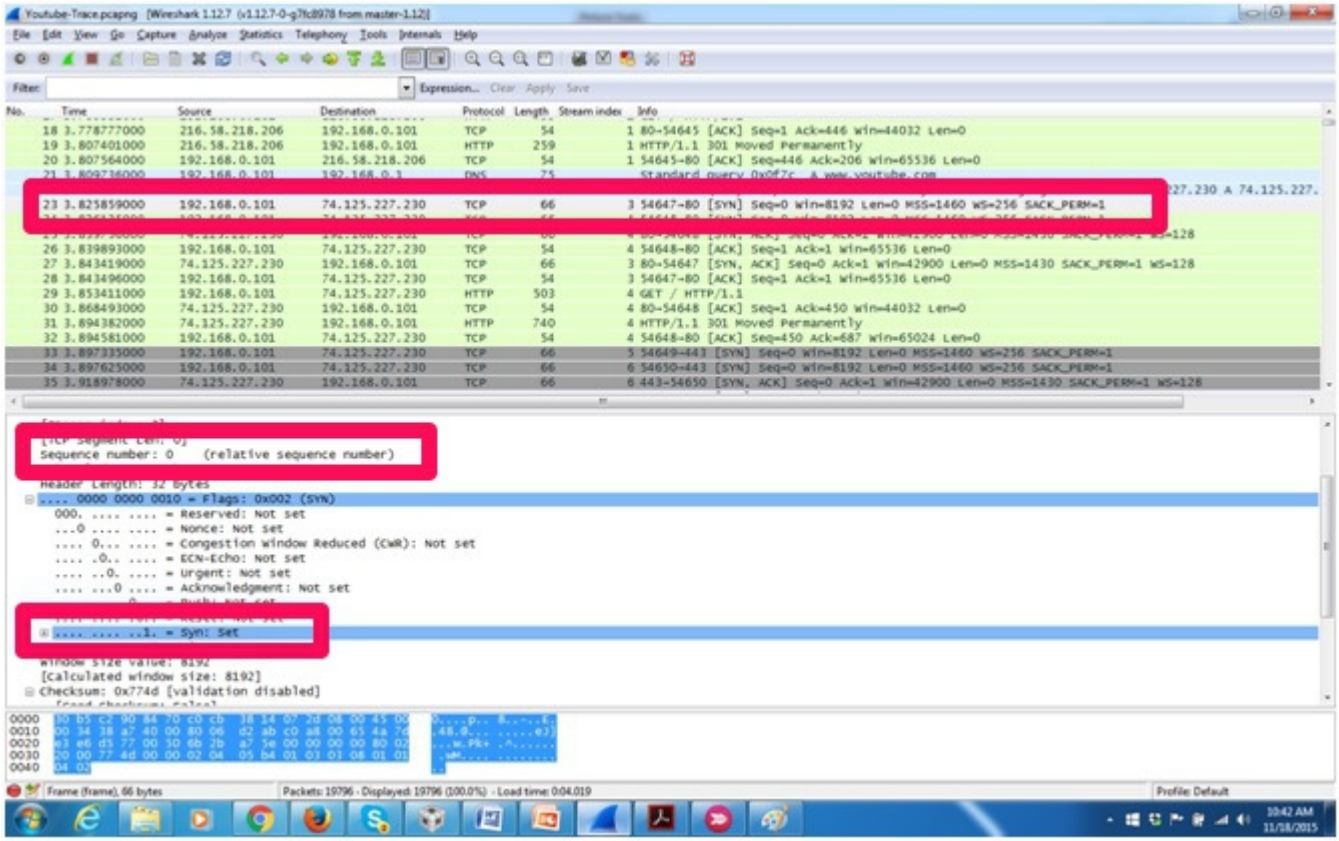
**IP address used by client-192.168.0.101(Above screenshot)**

**TCP port number of the client-54419**

**Problem set-2**

1.What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and youtube.com?

**SYN segment Initiation Relative Sequence  Number: 0**




2.What is it in the segment that identifies the segment as a SYN segment?

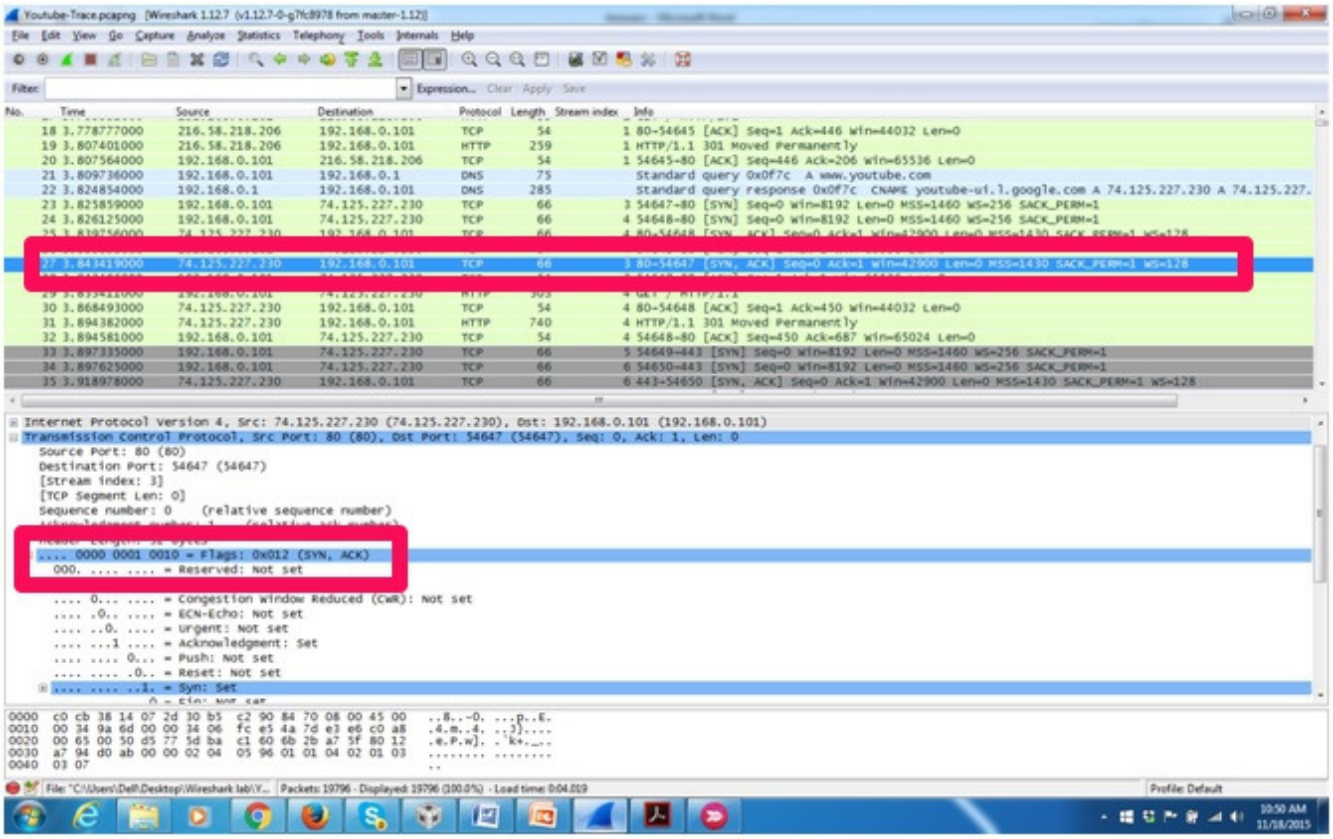
**SYN flag is set (=1) in the segment (Flags 0X02 (SYN)) ---screenshot above**

3.What is the sequence number of the SYNACK segment sent by youtube.com to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment?

**The SYN ACK  relative sequence number from youtube.com is 0**

**The value of Acknowledgment is 1(relative acknowledgement number)**

*(Screenshot below)*

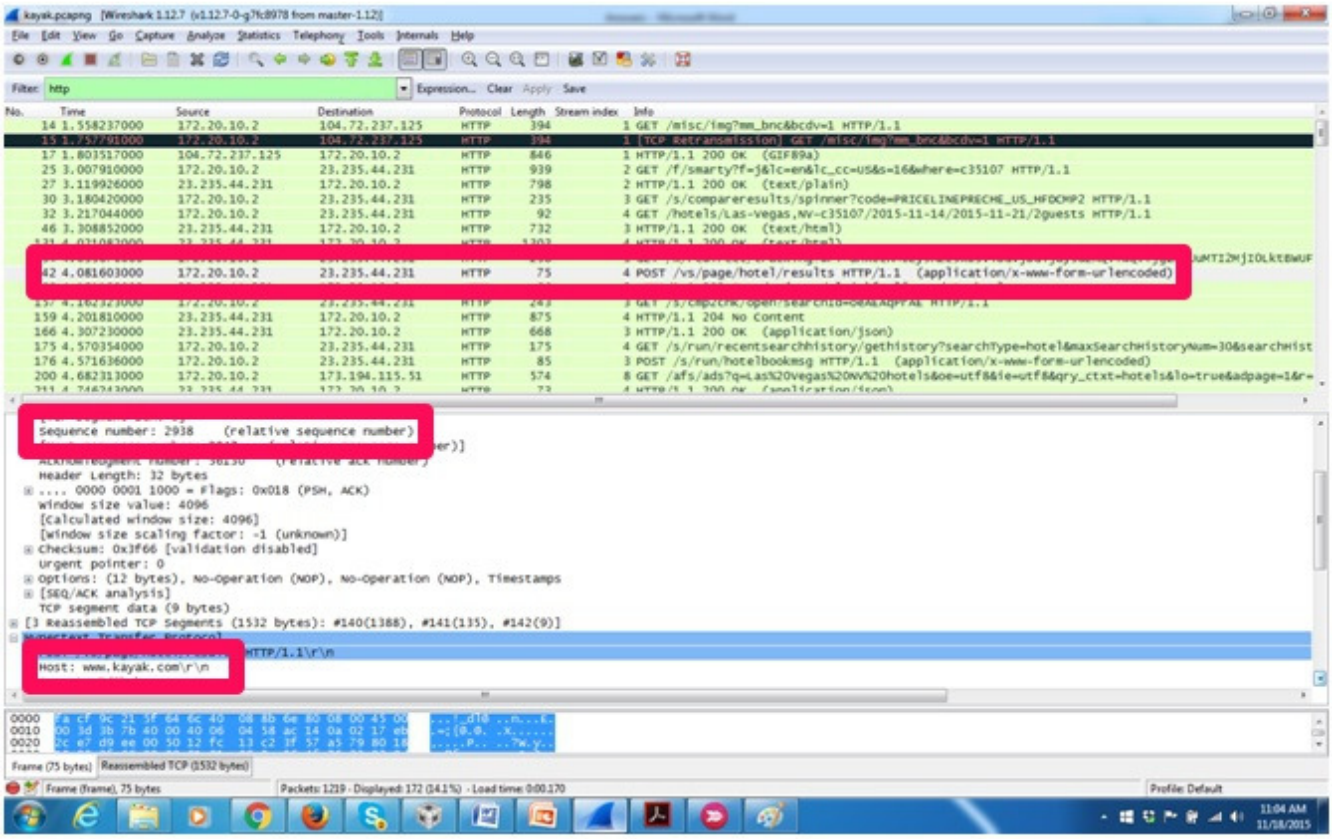



4.How did youtube.com determine that value? What is it in the segment that identifies the segment as a SYNACK segment?
**From the sequence 0 it received for SYN, the acknowledgement was set to 1( 0+1).**
**The SYN & ACK flags are set indicating it is a SYN ACK.**
**Both SYN flag =1& ACK flag=1**

**Problem Set-3**

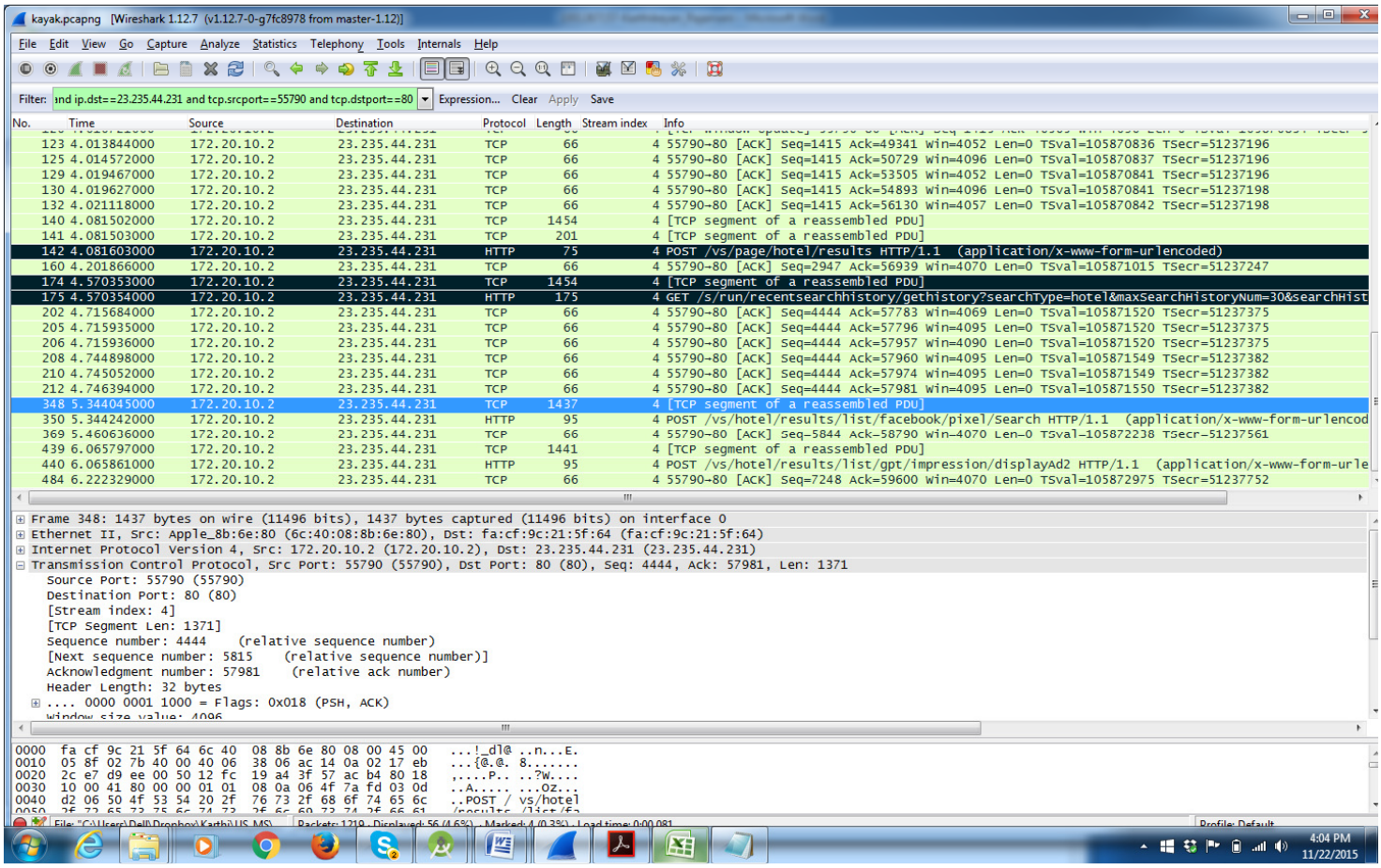
1.What is the sequence number of the TCP segment containing the HTTP POST command?

**Kayak.com-Relative sequence number:2938**




2. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What are the sequence numbers of the first four 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 eachof the four segments? What is the EstimatedRTT value (see Secttion 3.5.3, page 239 in text) after the receipt of each ACK? Assume that the value of the EstimatedRTT is equal to the measured RTT for the _rst segment, and then is computed using the EstimatedRTT equation on page 239 for all subsequent segments

**Filter=ip.src==172.20.10.2 and ip.dst==23.235.44.231 and tcp.srcport==55790 and tcp.dstport==80**




| Segment no | Wireshark Trace no | Rel.Seq. no | Time sent | Next exp seq no | Ack Wireshark Tr no | Ack Recd Time | Sampled RTT | Estimated RTT |
|---|---|---|---|---|---|---|---|---|
| 1st segment- HTTP Post | 142 | 1 | 4.081603 | 2947 | 146 | 4.135716 | 0.05411300 | 0.054113000000000 |
| 2nd segment | 174 | 2947 | 4.570353 | 4335 | 186 | 4.646868 | 0.07651500 | 0.056913250000000 |
| 3rd segment | 175 | 4335 | 4.570354 | 4444 | 188 | 4.649796 | 0.07944200 | 0.059729343750000 |
| 4th segment | 348 | 4444 | 5.344045 | 5815 | 356 | 5.393234 | 0.04918900 | 0.058411800781250 |

**Formula: EstimatedRTT=(1-x)*EstimatedRTT+x*Sample RTT ---- (X=0.125)**

**1st Segment- EstimatedRTT=SampleRTT=0.05411300**

**2nd Segment- = (1-0.125)*0.05411300 +0.125*0.07651500=0.056913250000000**

**3rd segment =(1-0.1250.056913250000000+0.125*0.07944200=0.059729343750000**

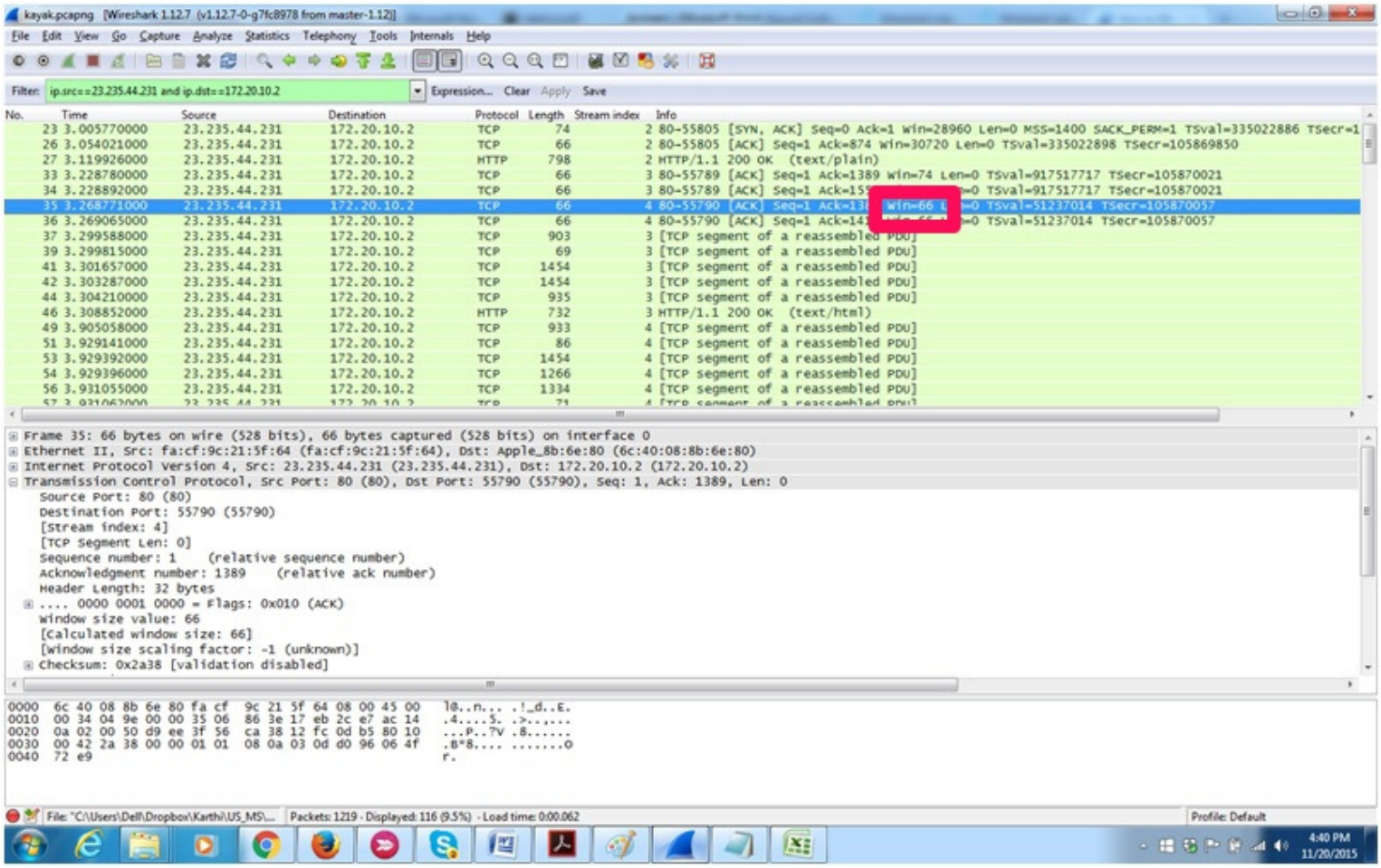
**4th segment =(1-0.125)* 0.059729343750000+0.125*0.04918900=0.058411800781250**

3.What is the length of each of the first four TCP segments?

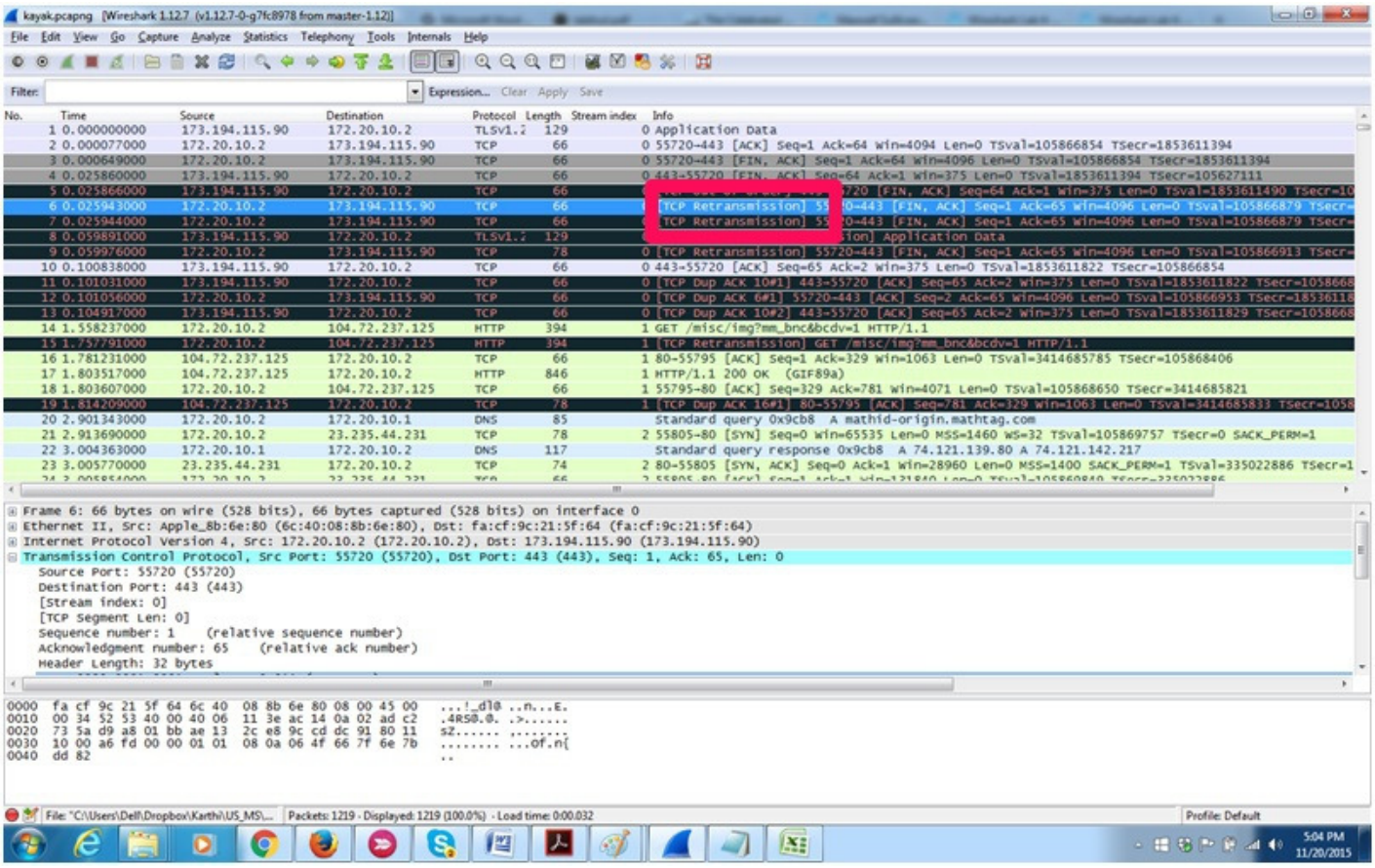
| Segment | Wireshark Trace no | Segment Length |
|---|---|---|
| 1st segment-HTTP Post | 142 | 9 |
| 2nd segment | 174 | 1388 |
| 3rd segment | 175 | 109 |
| 4th segment | 348 | 1371 |

4.What is the minimum amount of available buffer space advertised at the receiver for the entire trace? Does the lack of receiver buffer space ever throttle the sender?

**The minimum buffer size window is 66 in no 35. The study of the trace indicates that the sender is not throttled.**

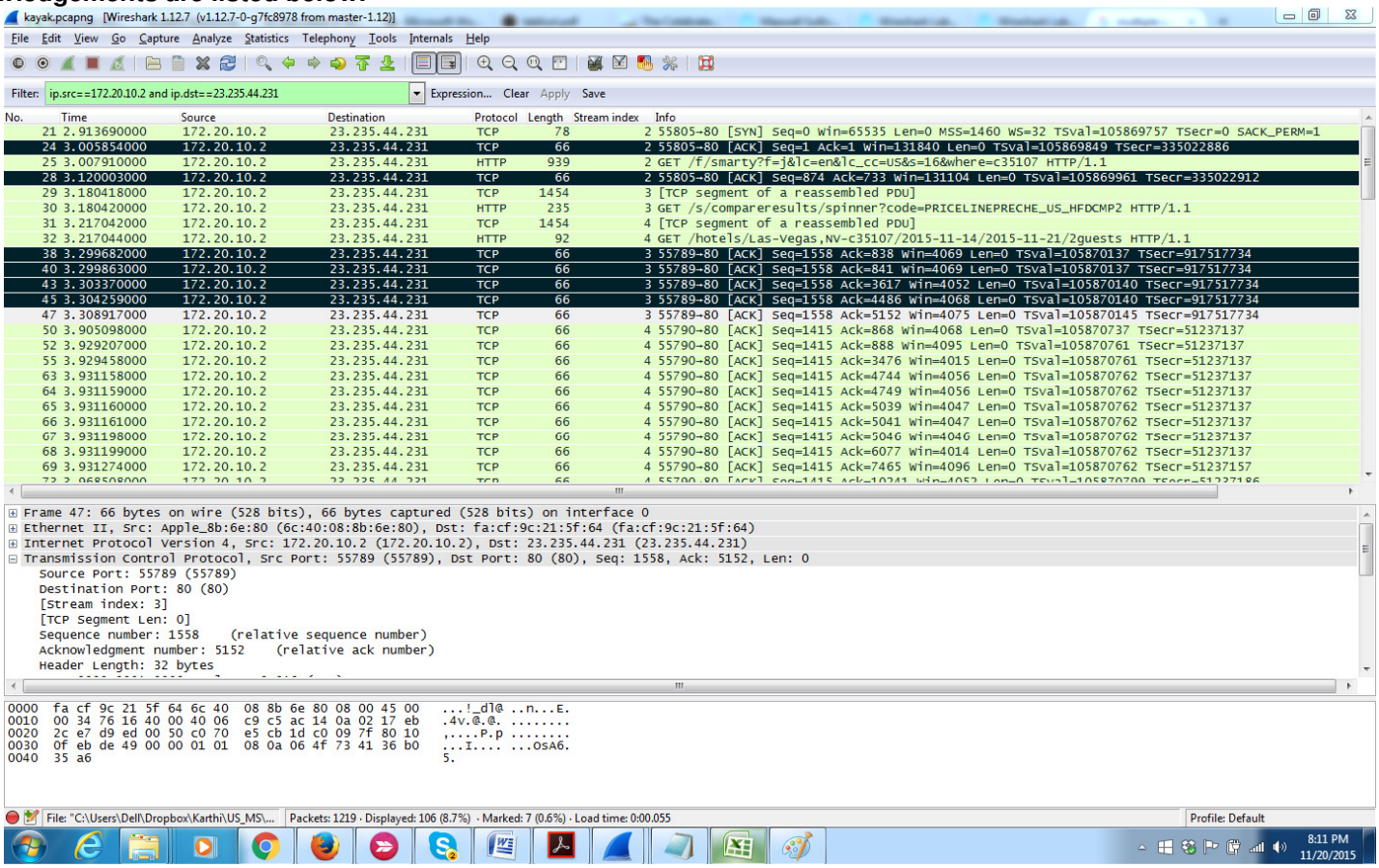



5. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?
**There are retransmissions in the trace file. They have the same sequence numbers. The TCP Retransmission black lines in the trace mark the retransmitted segments.**



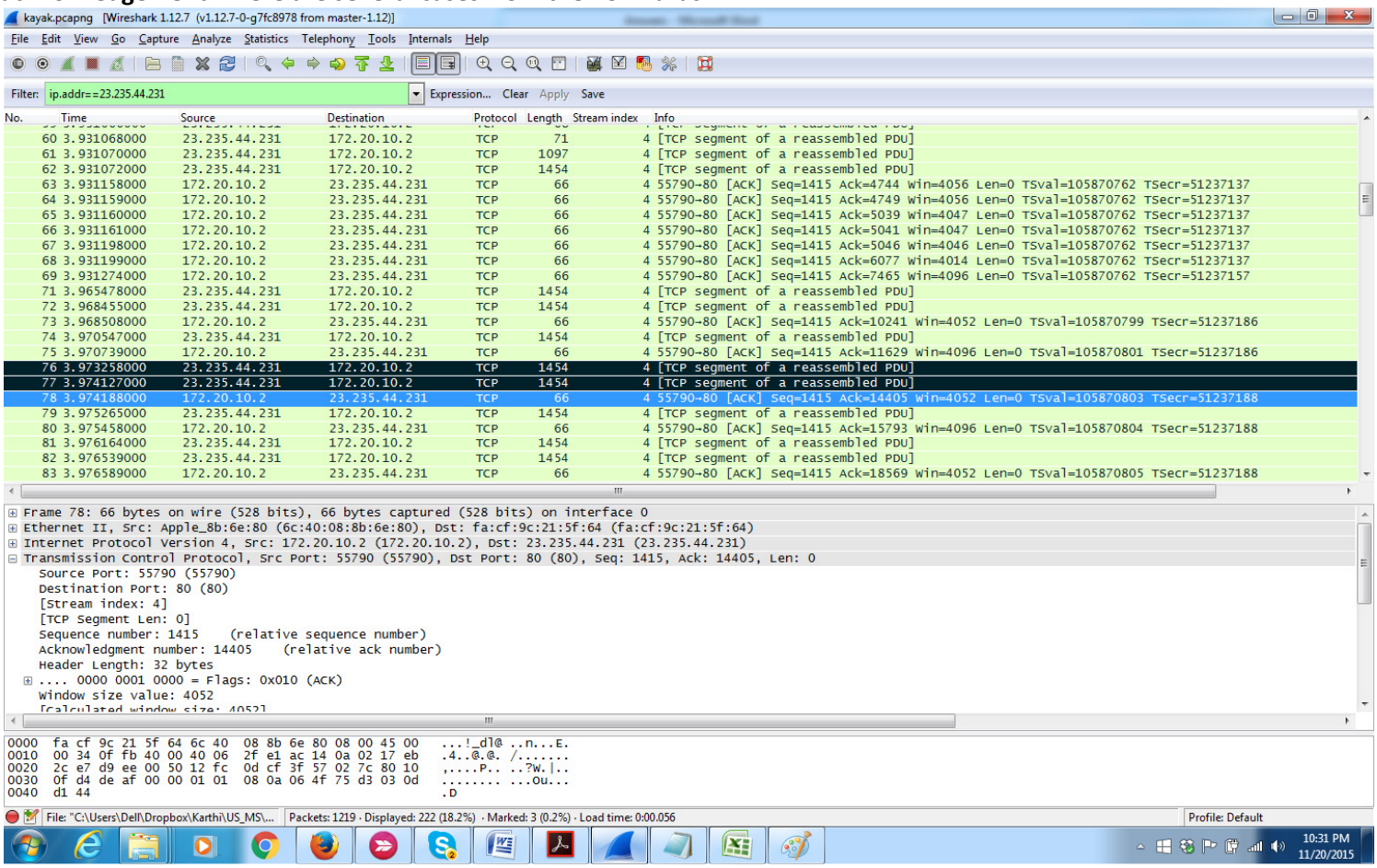

6.How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment (see Table 3.2 on page 247 in the text).

**The difference between successive Ack-numbers gives a measure of the data sent to server. The data from the first seven Acknowledgements are listed below.**



| Wireshark Trace no | ACK No | Ack Data |
|---|---|---|
| 24 | 1 | |
| 28 | 733 | 732 |
| 38 | 838 | 105 |
| 40 | 841 | 3 |
| 43 | 3617 | 2776 |
| 45 | 4486 | 869 |
| 47 | 5152 | 666 |

**Yes, in segment #73, the reciver ACKing ACK=10241 which is for Segment #71 & 72. The receiver is sending cumulative acknowledgement. There are several cases from then onwards.**




7. What is the throughput (bytes transferred per unit time) for the TCP connection?

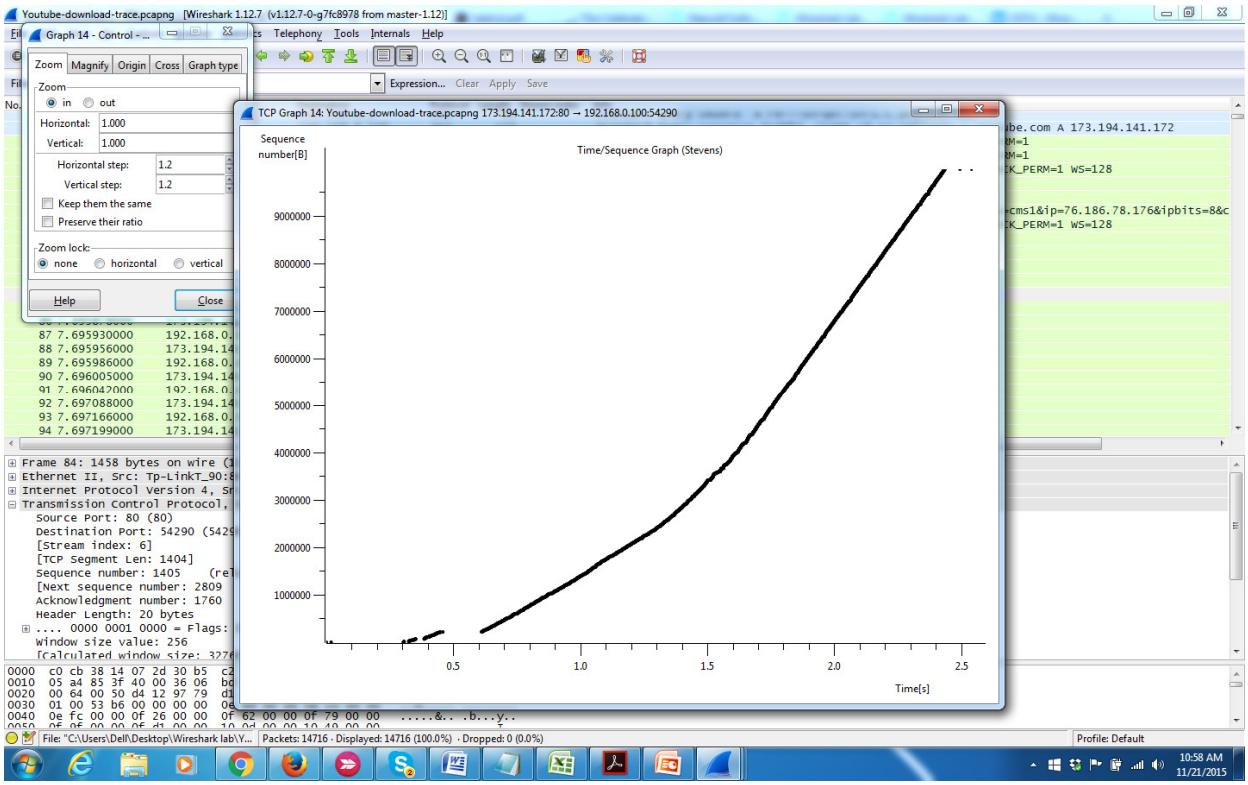
**Throughput=4130.998997Bytes/Sec**

8. Explain how you calculated this value.

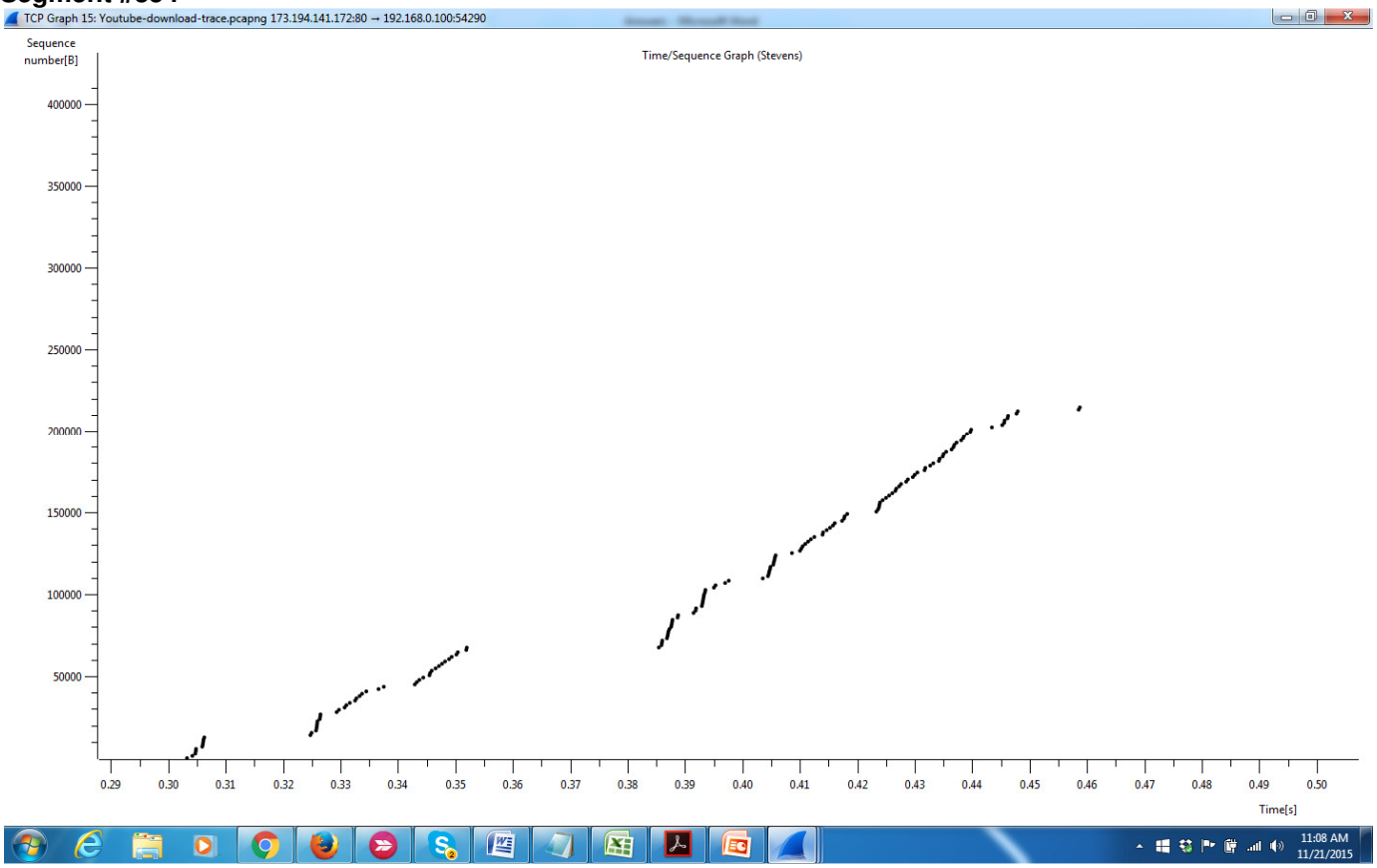
**The first segment Wireshark trace # 25 Time =3.007910000 Segment sequence number=1**
**The last acknowledged sequence number of the current session #447 Time=6.116117000 Segment sequence number =12870**
**Total transmission time=6.116117000 -3.007910000 =3.108207 seconds**
**Last byte no-447- sack no=12841**
**Total no of bytes=12870-1=12869 Bytes**
**Throughput=12869/3.108207=4140.329Bytes/Sec**

## Problem Set-4

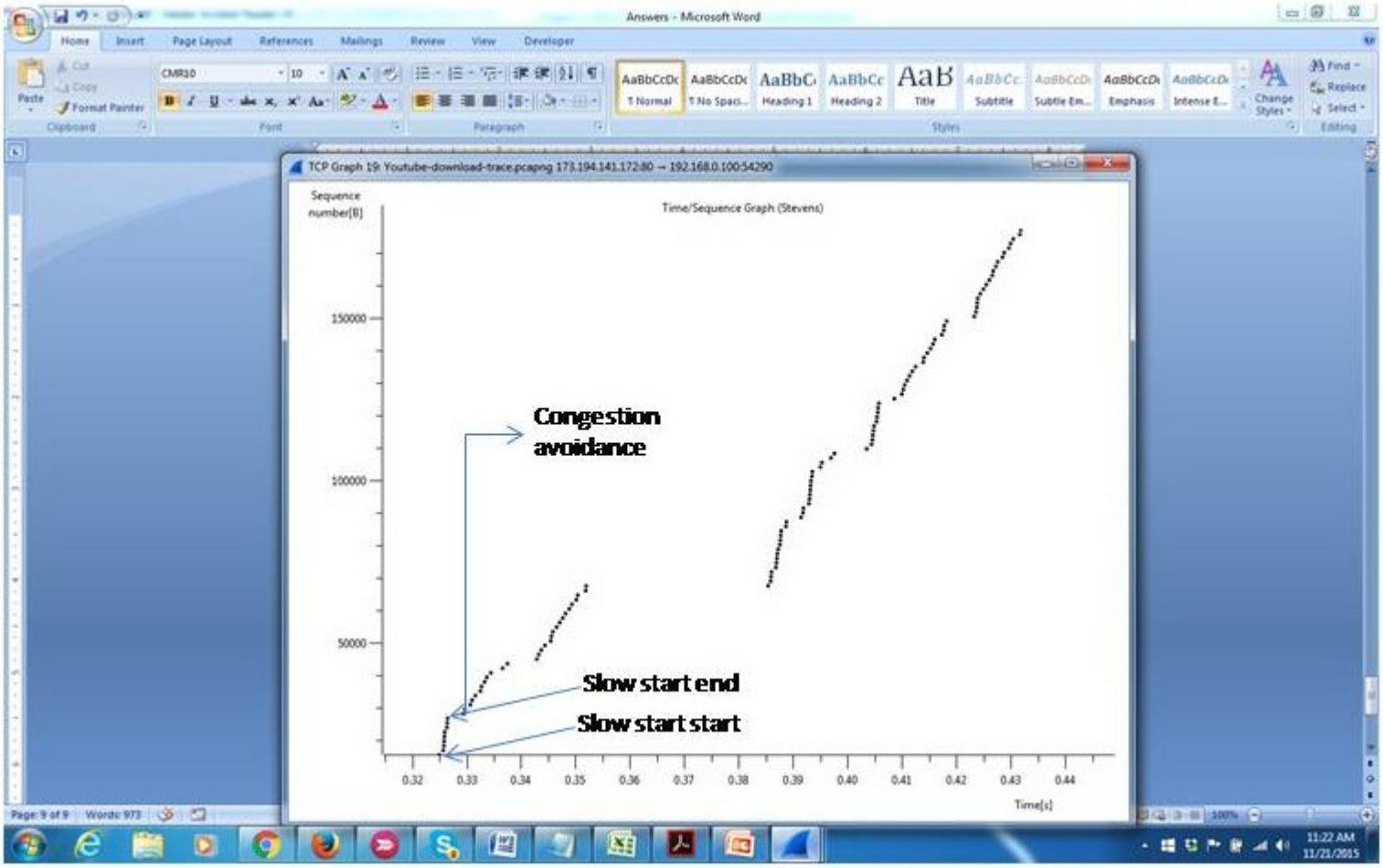
1. Use the Time-Sequence-Graph(Stevens) plotting tool to view the sequence number versus time plot of segments being sent from youtube.com to your computer. Can you identify where TCP's slow-start phase begins and ends, and where congestion avoidance takes over? Highlight these areas . Comment on ways in which the measured data differs from the idealized behavior of TCP that we've studied in the text.




### Segment #354




### Zoomed portions of the graph.




**Further zoomed portions of the graph.**

**Slow start seems to start at 0.325 Seconds and ends at 0.328 approximately.**
**Congestion avoidance seems to start from 0.329 seconds as the data volume is cut down.**
**The text book plots a perfect exponential growth for slow start but the trace graph indicates the slow start is uneven.**
**The congestion avoidance graph in the book indicates a gradual increase after sstresh but the trace graph congestion avoidance is uneven.**

2. Answer each of two questions above for the trace that you have gathered when you transferred a file from your computer from youtube.com.