CSC 138

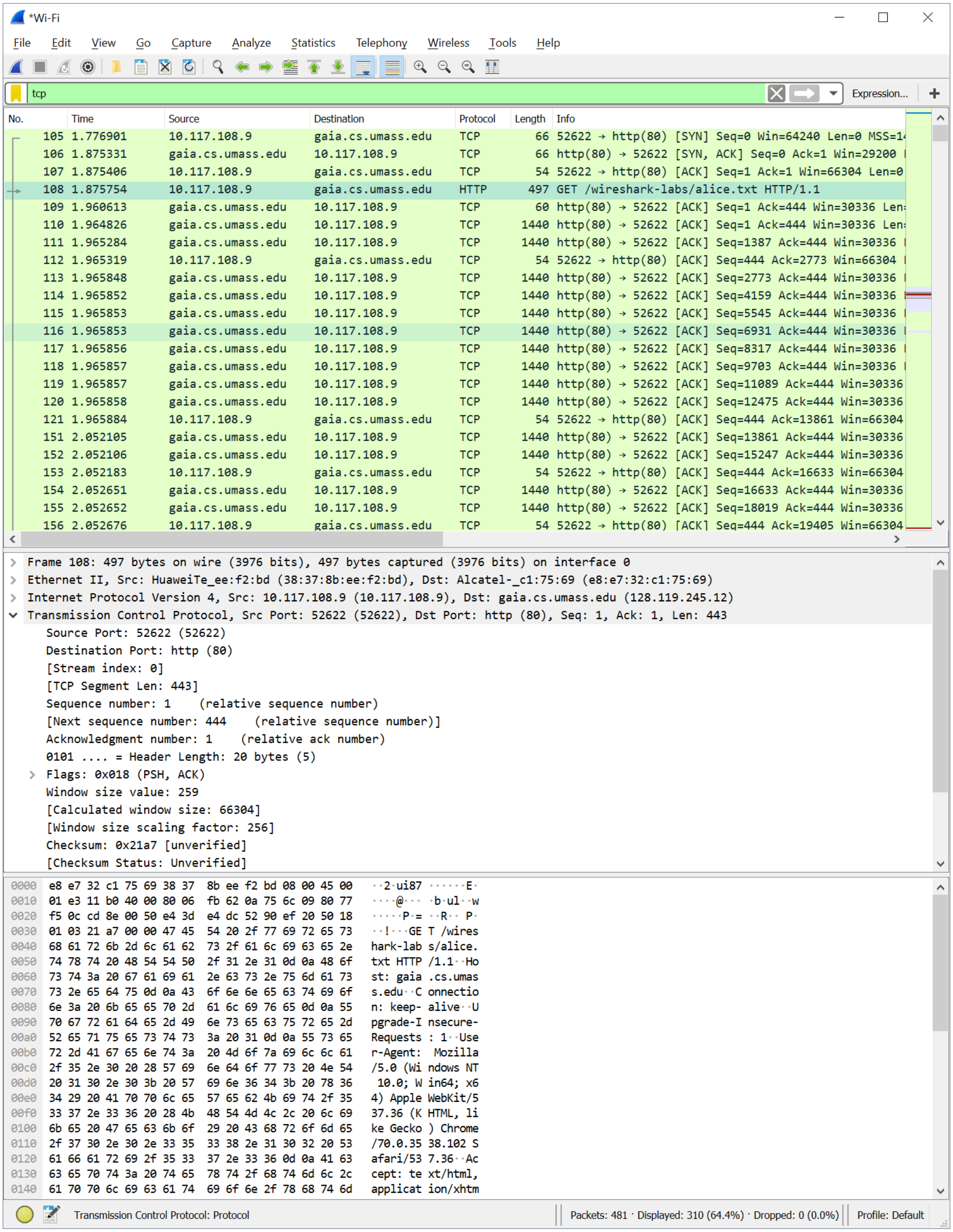
Talal Jawaid

Wireshark Lab 3

12/2/18

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.**

   Answer: The IP Address is 10.117.108.9 and the TCP port is 52662



tcp

```
No.     Time        Source              Destination         Protocol  Length  Info
    105 1.776901    10.117.108.9        gaia.cs.umass.edu   TCP         66 52622 → http(80) [SYN] Seq=0 Win=64240 Len=0 MSS=14
    106 1.875331    gaia.cs.umass.edu   10.117.108.9        TCP         66 http(80) → 52622 [SYN, ACK] Seq=0 Ack=1 Win=29200 
    107 1.875406    10.117.108.9        gaia.cs.umass.edu   TCP         54 52622 → http(80) [ACK] Seq=1 Ack=1 Win=66304 Len=0
    108 1.875754    10.117.108.9        gaia.cs.umass.edu   HTTP       497 GET /wireshark-labs/alice.txt HTTP/1.1
    109 1.960613    gaia.cs.umass.edu   10.117.108.9        TCP         60 http(80) → 52622 [ACK] Seq=1 Ack=444 Win=30336 Len=
    110 1.964826    gaia.cs.umass.edu   10.117.108.9        TCP       1440 http(80) → 52622 [ACK] Seq=1 Ack=444 Win=30336 Len=
    111 1.965284    gaia.cs.umass.edu   10.117.108.9        TCP       1440 http(80) → 52622 [ACK] Seq=1387 Ack=444 Win=30336 
    112 1.965319    10.117.108.9        gaia.cs.umass.edu   TCP         54 52622 → http(80) [ACK] Seq=444 Ack=2773 Win=66304 
    113 1.965848    gaia.cs.umass.edu   10.117.108.9        TCP       1440 http(80) → 52622 [ACK] Seq=2773 Ack=444 Win=30336 
    114 1.965852    gaia.cs.umass.edu   10.117.108.9        TCP       1440 http(80) → 52622 [ACK] Seq=4159 Ack=444 Win=30336 
    115 1.965853    gaia.cs.umass.edu   10.117.108.9        TCP       1440 http(80) → 52622 [ACK] Seq=5545 Ack=444 Win=30336 
    116 1.965853    gaia.cs.umass.edu   10.117.108.9        TCP       1440 http(80) → 52622 [ACK] Seq=6931 Ack=444 Win=30336 
    117 1.965856    gaia.cs.umass.edu   10.117.108.9        TCP       1440 http(80) → 52622 [ACK] Seq=8317 Ack=444 Win=30336 
    118 1.965857    gaia.cs.umass.edu   10.117.108.9        TCP       1440 http(80) → 52622 [ACK] Seq=9703 Ack=444 Win=30336 
    119 1.965857    gaia.cs.umass.edu   10.117.108.9        TCP       1440 http(80) → 52622 [ACK] Seq=11089 Ack=444 Win=30336
    120 1.965858    gaia.cs.umass.edu   10.117.108.9        TCP       1440 http(80) → 52622 [ACK] Seq=12475 Ack=444 Win=30336
    121 1.965884    10.117.108.9        gaia.cs.umass.edu   TCP         54 52622 → http(80) [ACK] Seq=444 Ack=13861 Win=66304
    151 2.052105    gaia.cs.umass.edu   10.117.108.9        TCP       1440 http(80) → 52622 [ACK] Seq=13861 Ack=444 Win=30336
    152 2.052106    gaia.cs.umass.edu   10.117.108.9        TCP       1440 http(80) → 52622 [ACK] Seq=15247 Ack=444 Win=30336
    153 2.052183    10.117.108.9        gaia.cs.umass.edu   TCP         54 52622 → http(80) [ACK] Seq=444 Ack=16633 Win=66304
    154 2.052651    gaia.cs.umass.edu   10.117.108.9        TCP       1440 http(80) → 52622 [ACK] Seq=16633 Ack=444 Win=30336
    155 2.052652    gaia.cs.umass.edu   10.117.108.9        TCP       1440 http(80) → 52622 [ACK] Seq=18019 Ack=444 Win=30336
    156 2.052676    10.117.108.9        gaia.cs.umass.edu   TCP         54 52622 → http(80) [ACK] Seq=444 Ack=19405 Win=66304
```

```
> Frame 108: 497 bytes on wire (3976 bits), 497 bytes captured (3976 bits) on interface 0
> Ethernet II, Src: HuaweiTe_ee:f2:bd (38:37:8b:ee:f2:bd), Dst: Alcatel-_c1:75:69 (e8:e7:32:c1:75:69)
> Internet Protocol Version 4, Src: 10.117.108.9 (10.117.108.9), Dst: gaia.cs.umass.edu (128.119.245.12)
v Transmission Control Protocol, Src Port: 52622 (52622), Dst Port: http (80), Seq: 1, Ack: 1, Len: 443
    Source Port: 52622 (52622)
    Destination Port: http (80)
    [Stream index: 0]
    [TCP Segment Len: 443]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 444    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window size value: 259
    [Calculated window size: 66304]
    [Window size scaling factor: 256]
    Checksum: 0x21a7 [unverified]
    [Checksum Status: Unverified]
```

```
0000  e8 e7 32 c1 75 69 38 37  8b ee f2 bd 08 00 45 00   ··2·ui87 ······E·
0010  01 e3 11 b0 40 00 80 06  fb 62 0a 75 6c 09 80 77   ····@··· ·b·ul··w
0020  f5 0c cd 8e 00 50 e4 3d  e4 dc 52 90 ef 20 50 18   ·····P·= ··R·· P·
0030  01 03 21 a7 00 00 47 45  54 20 2f 77 69 72 65 73   ··!···GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 61 6c 69 63 65 2e   hark-lab s/alice.
0050  74 78 74 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   txt HTTP /1.1··Ho
0060  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0070  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio
0080  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 55   n: keep- alive··U
0090  70 67 72 61 64 65 2d 49  6e 73 65 63 75 72 65 2d   pgrade-I nsecure-
00a0  52 65 71 75 65 73 74 73  3a 20 31 0d 0a 55 73 65   Requests : 1··Use
00b0  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a 69 6c 6c 61   r-Agent:  Mozilla
00c0  2f 35 2e 30 20 28 57 69  6e 64 6f 77 73 20 4e 54   /5.0 (Wi ndows NT
00d0  20 31 30 2e 30 3b 20 57  69 6e 36 34 3b 20 78 36    10.0; W in64; x6
00e0  34 29 20 41 70 70 6c 65  57 65 62 4b 69 74 2f 35   4) Apple WebKit/5
00f0  33 37 2e 33 36 20 28 4b  48 54 4d 4c 2c 20 6c 69   37.36 (K HTML, li
0100  6b 65 20 47 65 63 6b 6f  29 20 43 68 72 6f 6d 65   ke Gecko ) Chrome
0110  2f 37 30 2e 30 2e 33 35  33 38 2e 31 30 32 20 53   /70.0.35 38.102 S
0120  61 66 61 72 69 2f 35 33  37 2e 33 36 0d 0a 41 63   afari/53 7.36··Ac
0130  63 65 70 74 3a 20 74 65  78 74 2f 68 74 6d 6c 2c   cept: te xt/html,
0140  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 68 74 6d   applicat ion/xhtm
```

Transmission Control Protocol: Protocol | Packets: 481 · Displayed: 310 (64.4%) · Dropped: 0 (0.0%) | Profile: Default

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?**

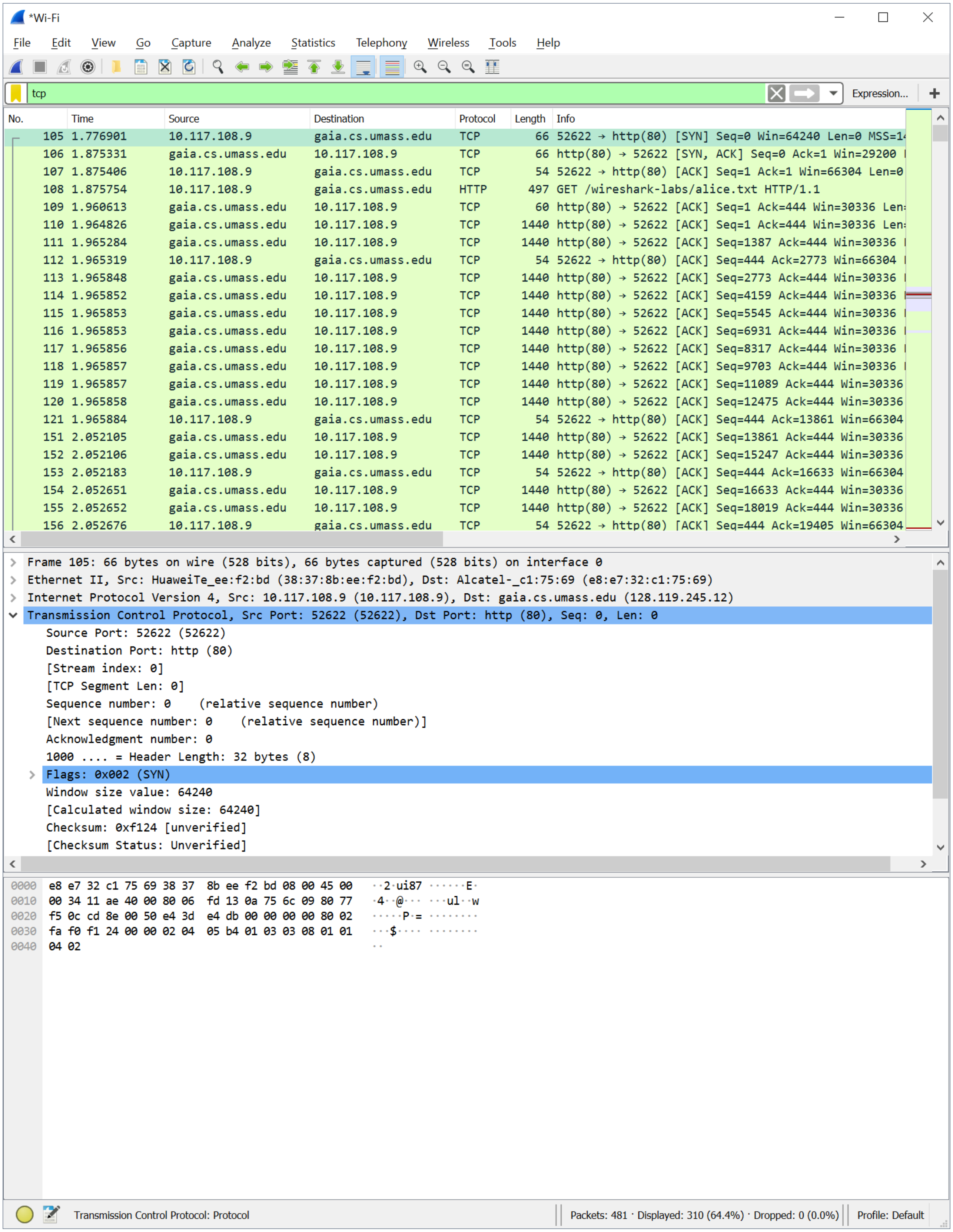
   Answer: The IP address is 128.119.245.12 and the TCP port is 80 for both sending and receiving

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?**

   Answer: The IP Address is 10.117.108.9 and the TCP port is 52662

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?**

   Answer: The sequence number is 0, the flag 0x002 identifies it as a SYN segment



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

tcp

```
No.  Time      Source            Destination       Protocol Length Info
 105 1.776901  10.117.108.9      gaia.cs.umass.edu TCP        66 52622 → http(80) [SYN] Seq=0 Win=64240 Len=0 MSS=14
 106 1.875331  gaia.cs.umass.edu 10.117.108.9      TCP        66 http(80) → 52622 [SYN, ACK] Seq=0 Ack=1 Win=29200
 107 1.875406  10.117.108.9      gaia.cs.umass.edu TCP        54 52622 → http(80) [ACK] Seq=1 Ack=1 Win=66304 Len=0
 108 1.875754  10.117.108.9      gaia.cs.umass.edu HTTP      497 GET /wireshark-labs/alice.txt HTTP/1.1
 109 1.960613  gaia.cs.umass.edu 10.117.108.9      TCP        60 http(80) → 52622 [ACK] Seq=1 Ack=444 Win=30336 Len
 110 1.964826  gaia.cs.umass.edu 10.117.108.9      TCP      1440 http(80) → 52622 [ACK] Seq=1 Ack=444 Win=30336 Len
 111 1.965284  gaia.cs.umass.edu 10.117.108.9      TCP      1440 http(80) → 52622 [ACK] Seq=1387 Ack=444 Win=30336
 112 1.965319  10.117.108.9      gaia.cs.umass.edu TCP        54 52622 → http(80) [ACK] Seq=444 Ack=2773 Win=66304
 113 1.965848  gaia.cs.umass.edu 10.117.108.9      TCP      1440 http(80) → 52622 [ACK] Seq=2773 Ack=444 Win=30336
 114 1.965852  gaia.cs.umass.edu 10.117.108.9      TCP      1440 http(80) → 52622 [ACK] Seq=4159 Ack=444 Win=30336
 115 1.965853  gaia.cs.umass.edu 10.117.108.9      TCP      1440 http(80) → 52622 [ACK] Seq=5545 Ack=444 Win=30336
 116 1.965853  gaia.cs.umass.edu 10.117.108.9      TCP      1440 http(80) → 52622 [ACK] Seq=6931 Ack=444 Win=30336
 117 1.965856  gaia.cs.umass.edu 10.117.108.9      TCP      1440 http(80) → 52622 [ACK] Seq=8317 Ack=444 Win=30336
 118 1.965857  gaia.cs.umass.edu 10.117.108.9      TCP      1440 http(80) → 52622 [ACK] Seq=9703 Ack=444 Win=30336
 119 1.965857  gaia.cs.umass.edu 10.117.108.9      TCP      1440 http(80) → 52622 [ACK] Seq=11089 Ack=444 Win=30336
 120 1.965858  gaia.cs.umass.edu 10.117.108.9      TCP      1440 http(80) → 52622 [ACK] Seq=12475 Ack=444 Win=30336
 121 1.965884  10.117.108.9      gaia.cs.umass.edu TCP        54 52622 → http(80) [ACK] Seq=444 Ack=13861 Win=66304
 151 2.052105  gaia.cs.umass.edu 10.117.108.9      TCP      1440 http(80) → 52622 [ACK] Seq=13861 Ack=444 Win=30336
 152 2.052106  gaia.cs.umass.edu 10.117.108.9      TCP      1440 http(80) → 52622 [ACK] Seq=15247 Ack=444 Win=30336
 153 2.052183  10.117.108.9      gaia.cs.umass.edu TCP        54 52622 → http(80) [ACK] Seq=444 Ack=16633 Win=66304
 154 2.052651  gaia.cs.umass.edu 10.117.108.9      TCP      1440 http(80) → 52622 [ACK] Seq=16633 Ack=444 Win=30336
 155 2.052652  gaia.cs.umass.edu 10.117.108.9      TCP      1440 http(80) → 52622 [ACK] Seq=18019 Ack=444 Win=30336
 156 2.052676  10.117.108.9      gaia.cs.umass.edu TCP        54 52622 → http(80) [ACK] Seq=444 Ack=19405 Win=66304
```

```
> Frame 105: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: HuaweiTe_ee:f2:bd (38:37:8b:ee:f2:bd), Dst: Alcatel-_c1:75:69 (e8:e7:32:c1:75:69)
> Internet Protocol Version 4, Src: 10.117.108.9 (10.117.108.9), Dst: gaia.cs.umass.edu (128.119.245.12)
v Transmission Control Protocol, Src Port: 52622 (52622), Dst Port: http (80), Seq: 0, Len: 0
    Source Port: 52622 (52622)
    Destination Port: http (80)
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 0
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
    Window size value: 64240
    [Calculated window size: 64240]
    Checksum: 0xf124 [unverified]
    [Checksum Status: Unverified]
```

```
0000  e8 e7 32 c1 75 69 38 37  8b ee f2 bd 08 00 45 00   ··2·ui87 ······E·
0010  00 34 11 ae 40 00 80 06  fd 13 0a 75 6c 09 80 77   ·4··@··· ···ul··w
0020  f5 0c cd 8e 00 50 e4 3d  e4 db 00 00 00 00 80 02   ·····P·= ········
0030  fa f0 f1 24 00 00 02 04  05 b4 01 03 03 08 01 01   ···$···· ········
0040  04 02                                              ··
```

Transmission Control Protocol: Protocol

Packets: 481 · Displayed: 310 (64.4%) · Dropped: 0 (0.0%)

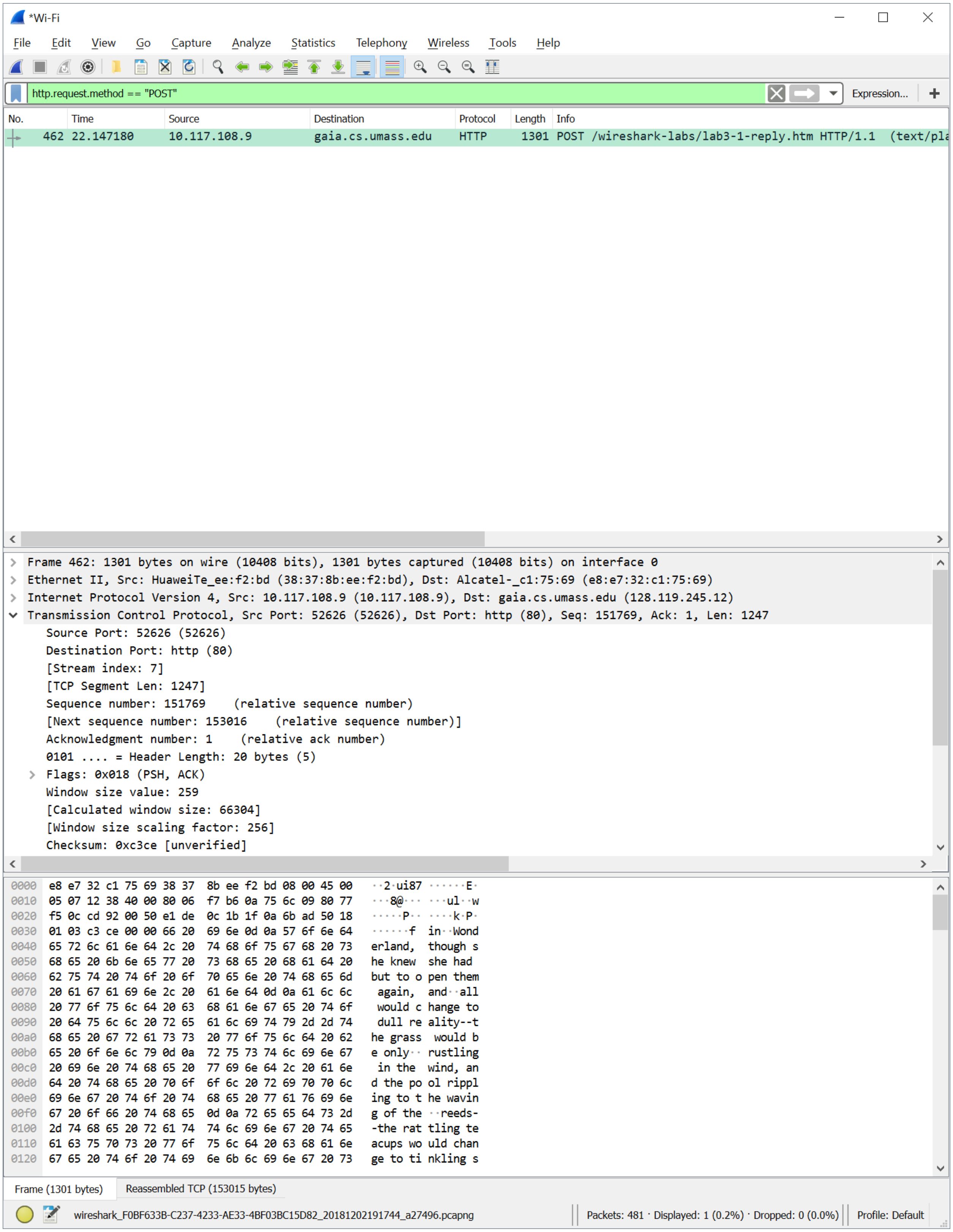
Profile: Default

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?**

   Answer: The sequence number is 0 and the acknowledgement number is 1. The flag 0x012 identifies it as a 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.**

   Answer: The sequence number is 151769



```
http.request.method == "POST"
```

No.	Time	Source	Destination	Protocol	Length	Info
462	22.147180	10.117.108.9	gaia.cs.umass.edu	HTTP	1301	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/pla

```
> Frame 462: 1301 bytes on wire (10408 bits), 1301 bytes captured (10408 bits) on interface 0
> Ethernet II, Src: HuaweiTe_ee:f2:bd (38:37:8b:ee:f2:bd), Dst: Alcatel-_c1:75:69 (e8:e7:32:c1:75:69)
> Internet Protocol Version 4, Src: 10.117.108.9 (10.117.108.9), Dst: gaia.cs.umass.edu (128.119.245.12)
v Transmission Control Protocol, Src Port: 52626 (52626), Dst Port: http (80), Seq: 151769, Ack: 1, Len: 1247
    Source Port: 52626 (52626)
    Destination Port: http (80)
    [Stream index: 7]
    [TCP Segment Len: 1247]
    Sequence number: 151769    (relative sequence number)
    [Next sequence number: 153016    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window size value: 259
    [Calculated window size: 66304]
    [Window size scaling factor: 256]
    Checksum: 0xc3ce [unverified]
```

```
0000  e8 e7 32 c1 75 69 38 37  8b ee f2 bd 08 00 45 00   ··2·ui87 ······E·
0010  05 07 12 38 40 00 80 06  f7 b6 0a 75 6c 09 80 77   ···8@··· ···ul··w
0020  f5 0c cd 92 00 50 e1 de  0c 1b 1f 0a 6b ad 50 18   ·····P·· ····k·P·
0030  01 03 c3 ce 00 00 66 20  69 6e 0d 0a 57 6f 6e 64   ······f  in··Wond
0040  65 72 6c 61 6e 64 2c 20  74 68 6f 75 67 68 20 73   erland,  though s
0050  68 65 20 6b 6e 65 77 20  73 68 65 20 68 61 64 20   he knew  she had
0060  62 75 74 20 74 6f 20 6f  70 65 6e 20 74 68 65 6d   but to o pen them
0070  20 61 67 61 69 6e 2c 20  61 6e 64 0d 0a 61 6c 6c    again,  and··all
0080  20 77 6f 75 6c 64 20 63  68 61 6e 67 65 20 74 6f    would c hange to
0090  20 64 75 6c 6c 20 72 65  61 6c 69 74 79 2d 2d 74    dull re ality--t
00a0  68 65 20 67 72 61 73 73  20 77 6f 75 6c 64 20 62   he grass  would b
00b0  65 20 6f 6e 6c 79 0d 0a  72 75 73 74 6c 69 6e 67   e only·· rustling
00c0  20 69 6e 20 74 68 65 20  77 69 6e 64 2c 20 61 6e    in the  wind, an
00d0  64 20 74 68 65 20 70 6f  6f 6c 20 72 69 70 70 6c   d the po ol rippl
00e0  69 6e 67 20 74 6f 20 74  68 65 20 77 61 76 69 6e   ing to t he wavin
00f0  67 20 6f 66 20 74 68 65  0d 0a 72 65 65 64 73 2d   g of the ··reeds-
0100  2d 74 68 65 20 72 61 74  74 6c 69 6e 67 20 74 65   -the rat tling te
0110  61 63 75 70 73 20 77 6f  75 6c 64 20 63 68 61 6e   acups wo uld chan
0120  67 65 20 74 6f 20 74 69  6e 6b 6c 69 6e 67 20 73   ge to ti nkling s
```

wireshark_F0BF633B-C237-4233-AE33-4BF03BC15D82_20181202191744_a27496.pcapng

Packets: 481 · Displayed: 1 (0.2%) · Dropped: 0 (0.0%)

Profile: Default

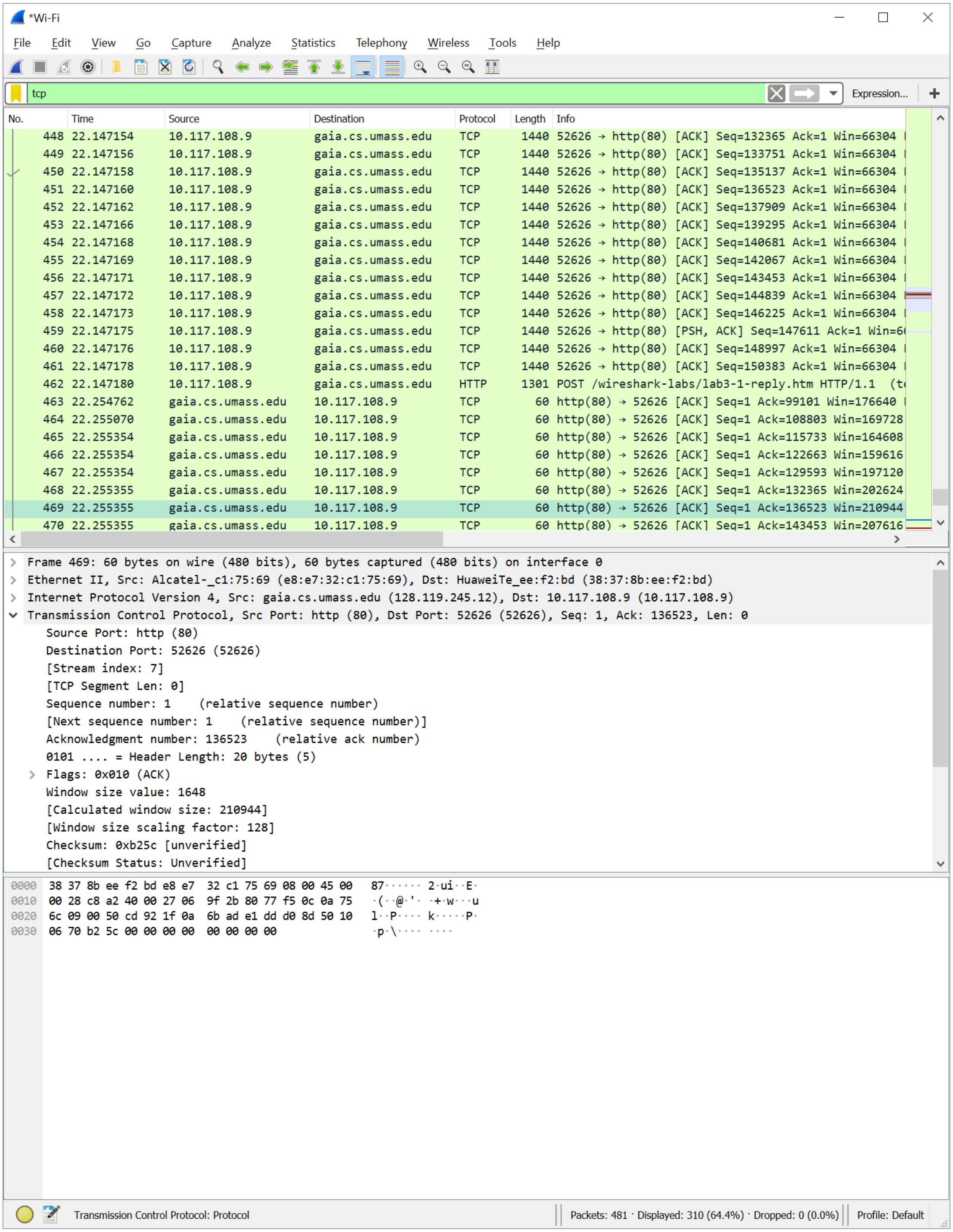
7. **Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What are the sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST)? At what time was each segment sent? When was the ACK for each segment received? 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.

   Answer: The sequence number for the first six segments are all 1 except for the HTTP post which is 151769

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

   Answer: The TCP segment length for the first sex segments is listed as 0



```
tcp
```

```
No.  Time       Source             Destination        Protocol Length Info
 448 22.147154  10.117.108.9       gaia.cs.umass.edu  TCP      1440 52626 → http(80) [ACK] Seq=132365 Ack=1 Win=66304 L
 449 22.147156  10.117.108.9       gaia.cs.umass.edu  TCP      1440 52626 → http(80) [ACK] Seq=133751 Ack=1 Win=66304 L
 450 22.147158  10.117.108.9       gaia.cs.umass.edu  TCP      1440 52626 → http(80) [ACK] Seq=135137 Ack=1 Win=66304 L
 451 22.147160  10.117.108.9       gaia.cs.umass.edu  TCP      1440 52626 → http(80) [ACK] Seq=136523 Ack=1 Win=66304 L
 452 22.147162  10.117.108.9       gaia.cs.umass.edu  TCP      1440 52626 → http(80) [ACK] Seq=137909 Ack=1 Win=66304 L
 453 22.147166  10.117.108.9       gaia.cs.umass.edu  TCP      1440 52626 → http(80) [ACK] Seq=139295 Ack=1 Win=66304 L
 454 22.147168  10.117.108.9       gaia.cs.umass.edu  TCP      1440 52626 → http(80) [ACK] Seq=140681 Ack=1 Win=66304 L
 455 22.147169  10.117.108.9       gaia.cs.umass.edu  TCP      1440 52626 → http(80) [ACK] Seq=142067 Ack=1 Win=66304 L
 456 22.147171  10.117.108.9       gaia.cs.umass.edu  TCP      1440 52626 → http(80) [ACK] Seq=143453 Ack=1 Win=66304 L
 457 22.147172  10.117.108.9       gaia.cs.umass.edu  TCP      1440 52626 → http(80) [ACK] Seq=144839 Ack=1 Win=66304 L
 458 22.147173  10.117.108.9       gaia.cs.umass.edu  TCP      1440 52626 → http(80) [ACK] Seq=146225 Ack=1 Win=66304 L
 459 22.147175  10.117.108.9       gaia.cs.umass.edu  TCP      1440 52626 → http(80) [PSH, ACK] Seq=147611 Ack=1 Win=66
 460 22.147176  10.117.108.9       gaia.cs.umass.edu  TCP      1440 52626 → http(80) [ACK] Seq=148997 Ack=1 Win=66304 L
 461 22.147178  10.117.108.9       gaia.cs.umass.edu  TCP      1440 52626 → http(80) [ACK] Seq=150383 Ack=1 Win=66304 L
 462 22.147180  10.117.108.9       gaia.cs.umass.edu  HTTP     1301 POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1  (te
 463 22.254762  gaia.cs.umass.edu  10.117.108.9       TCP        60 http(80) → 52626 [ACK] Seq=1 Ack=99101 Win=176640 L
 464 22.255070  gaia.cs.umass.edu  10.117.108.9       TCP        60 http(80) → 52626 [ACK] Seq=1 Ack=108803 Win=169728
 465 22.255354  gaia.cs.umass.edu  10.117.108.9       TCP        60 http(80) → 52626 [ACK] Seq=1 Ack=115733 Win=164608
 466 22.255354  gaia.cs.umass.edu  10.117.108.9       TCP        60 http(80) → 52626 [ACK] Seq=1 Ack=122663 Win=159616
 467 22.255354  gaia.cs.umass.edu  10.117.108.9       TCP        60 http(80) → 52626 [ACK] Seq=1 Ack=129593 Win=197120
 468 22.255355  gaia.cs.umass.edu  10.117.108.9       TCP        60 http(80) → 52626 [ACK] Seq=1 Ack=132365 Win=202624
 469 22.255355  gaia.cs.umass.edu  10.117.108.9       TCP        60 http(80) → 52626 [ACK] Seq=1 Ack=136523 Win=210944
 470 22.255355  gaia.cs.umass.edu  10.117.108.9       TCP        60 http(80) → 52626 [ACK] Seq=1 Ack=143453 Win=207616
```

```
> Frame 469: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: Alcatel-_c1:75:69 (e8:e7:32:c1:75:69), Dst: HuaweiTe_ee:f2:bd (38:37:8b:ee:f2:bd)
> Internet Protocol Version 4, Src: gaia.cs.umass.edu (128.119.245.12), Dst: 10.117.108.9 (10.117.108.9)
v Transmission Control Protocol, Src Port: http (80), Dst Port: 52626 (52626), Seq: 1, Ack: 136523, Len: 0
    Source Port: http (80)
    Destination Port: 52626 (52626)
    [Stream index: 7]
    [TCP Segment Len: 0]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 136523    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window size value: 1648
    [Calculated window size: 210944]
    [Window size scaling factor: 128]
    Checksum: 0xb25c [unverified]
    [Checksum Status: Unverified]
```

```
0000  38 37 8b ee f2 bd e8 e7  32 c1 75 69 08 00 45 00   87······ 2·ui··E·
0010  00 28 c8 a2 40 00 27 06  9f 2b 80 77 f5 0c 0a 75   ·(··@·'· ·+·w···u
0020  6c 09 00 50 cd 92 1f 0a  6b ad e1 dd d0 8d 50 10   l··P···· k·····P·
0030  06 70 b2 5c 00 00 00 00  00 00 00 00               ·p·\···· ····
```

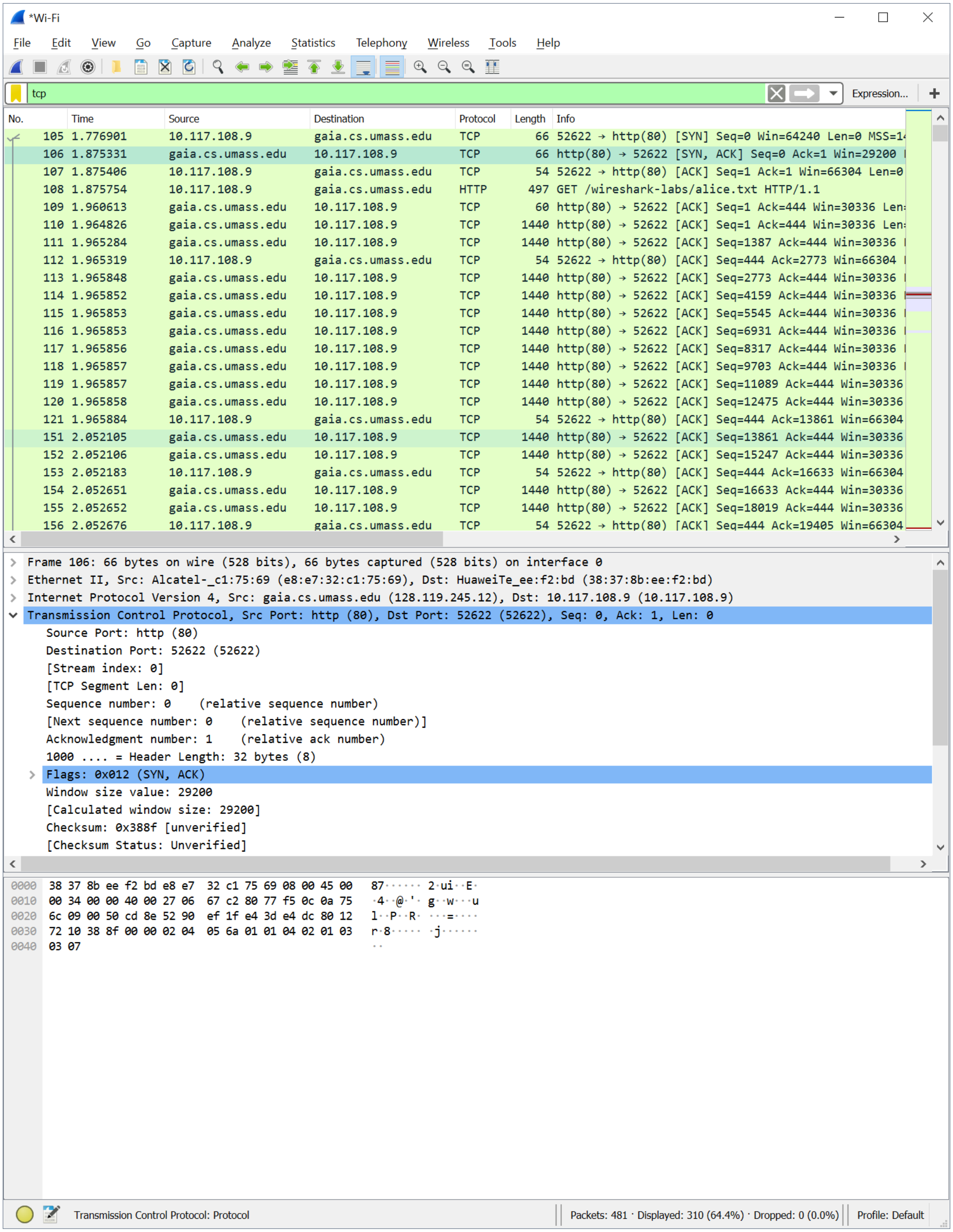
Transmission Control Protocol: Protocol

Packets: 481 · Displayed: 310 (64.4%) · Dropped: 0 (0.0%)

Profile: Default

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?**

   Answer: The minimum amount of available buffer space is 29200 bytes


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
Expression...
+

```
No.   Time      Source              Destination         Protocol  Length Info
  105 1.776901  10.117.108.9        gaia.cs.umass.edu   TCP          66 52622 → http(80) [SYN] Seq=0 Win=64240 Len=0 MSS=14
  106 1.875331  gaia.cs.umass.edu   10.117.108.9        TCP          66 http(80) → 52622 [SYN, ACK] Seq=0 Ack=1 Win=29200
  107 1.875406  10.117.108.9        gaia.cs.umass.edu   TCP          54 52622 → http(80) [ACK] Seq=1 Ack=1 Win=66304 Len=0
  108 1.875754  10.117.108.9        gaia.cs.umass.edu   HTTP        497 GET /wireshark-labs/alice.txt HTTP/1.1
  109 1.960613  gaia.cs.umass.edu   10.117.108.9        TCP          60 http(80) → 52622 [ACK] Seq=1 Ack=444 Win=30336 Len=
  110 1.964826  gaia.cs.umass.edu   10.117.108.9        TCP        1440 http(80) → 52622 [ACK] Seq=1 Ack=444 Win=30336 Len=
  111 1.965284  gaia.cs.umass.edu   10.117.108.9        TCP        1440 http(80) → 52622 [ACK] Seq=1387 Ack=444 Win=30336
  112 1.965319  10.117.108.9        gaia.cs.umass.edu   TCP          54 52622 → http(80) [ACK] Seq=444 Ack=2773 Win=66304
  113 1.965848  gaia.cs.umass.edu   10.117.108.9        TCP        1440 http(80) → 52622 [ACK] Seq=2773 Ack=444 Win=30336
  114 1.965852  gaia.cs.umass.edu   10.117.108.9        TCP        1440 http(80) → 52622 [ACK] Seq=4159 Ack=444 Win=30336
  115 1.965853  gaia.cs.umass.edu   10.117.108.9        TCP        1440 http(80) → 52622 [ACK] Seq=5545 Ack=444 Win=30336
  116 1.965853  gaia.cs.umass.edu   10.117.108.9        TCP        1440 http(80) → 52622 [ACK] Seq=6931 Ack=444 Win=30336
  117 1.965856  gaia.cs.umass.edu   10.117.108.9        TCP        1440 http(80) → 52622 [ACK] Seq=8317 Ack=444 Win=30336
  118 1.965857  gaia.cs.umass.edu   10.117.108.9        TCP        1440 http(80) → 52622 [ACK] Seq=9703 Ack=444 Win=30336
  119 1.965857  gaia.cs.umass.edu   10.117.108.9        TCP        1440 http(80) → 52622 [ACK] Seq=11089 Ack=444 Win=30336
  120 1.965858  gaia.cs.umass.edu   10.117.108.9        TCP        1440 http(80) → 52622 [ACK] Seq=12475 Ack=444 Win=30336
  121 1.965884  10.117.108.9        gaia.cs.umass.edu   TCP          54 52622 → http(80) [ACK] Seq=444 Ack=13861 Win=66304
  151 2.052105  gaia.cs.umass.edu   10.117.108.9        TCP        1440 http(80) → 52622 [ACK] Seq=13861 Ack=444 Win=30336
  152 2.052106  gaia.cs.umass.edu   10.117.108.9        TCP        1440 http(80) → 52622 [ACK] Seq=15247 Ack=444 Win=30336
  153 2.052183  10.117.108.9        gaia.cs.umass.edu   TCP          54 52622 → http(80) [ACK] Seq=444 Ack=16633 Win=66304
  154 2.052651  gaia.cs.umass.edu   10.117.108.9        TCP        1440 http(80) → 52622 [ACK] Seq=16633 Ack=444 Win=30336
  155 2.052652  gaia.cs.umass.edu   10.117.108.9        TCP        1440 http(80) → 52622 [ACK] Seq=18019 Ack=444 Win=30336
  156 2.052676  10.117.108.9        gaia.cs.umass.edu   TCP          54 52622 → http(80) [ACK] Seq=444 Ack=19405 Win=66304
```

```
> Frame 106: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: Alcatel-_c1:75:69 (e8:e7:32:c1:75:69), Dst: HuaweiTe_ee:f2:bd (38:37:8b:ee:f2:bd)
> Internet Protocol Version 4, Src: gaia.cs.umass.edu (128.119.245.12), Dst: 10.117.108.9 (10.117.108.9)
v Transmission Control Protocol, Src Port: http (80), Dst Port: 52622 (52622), Seq: 0, Ack: 1, Len: 0
    Source Port: http (80)
    Destination Port: 52622 (52622)
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x012 (SYN, ACK)
    Window size value: 29200
    [Calculated window size: 29200]
    Checksum: 0x388f [unverified]
    [Checksum Status: Unverified]
```

```
0000  38 37 8b ee f2 bd e8 e7  32 c1 75 69 08 00 45 00   87······ 2·ui··E·
0010  00 34 00 00 40 00 27 06  67 c2 80 77 f5 0c 0a 75   ·4··@·'· g··w···u
0020  6c 09 00 50 cd 8e 52 90  ef 1f e4 3d e4 dc 80 12   l··P··R· ···=····
0030  72 10 38 8f 00 00 02 04  05 6a 01 01 04 02 01 03   r·8····· ·j······
0040  03 07                                              ··
```

Transmission Control Protocol: Protocol

Packets: 481 · Displayed: 310 (64.4%) · Dropped: 0 (0.0%)

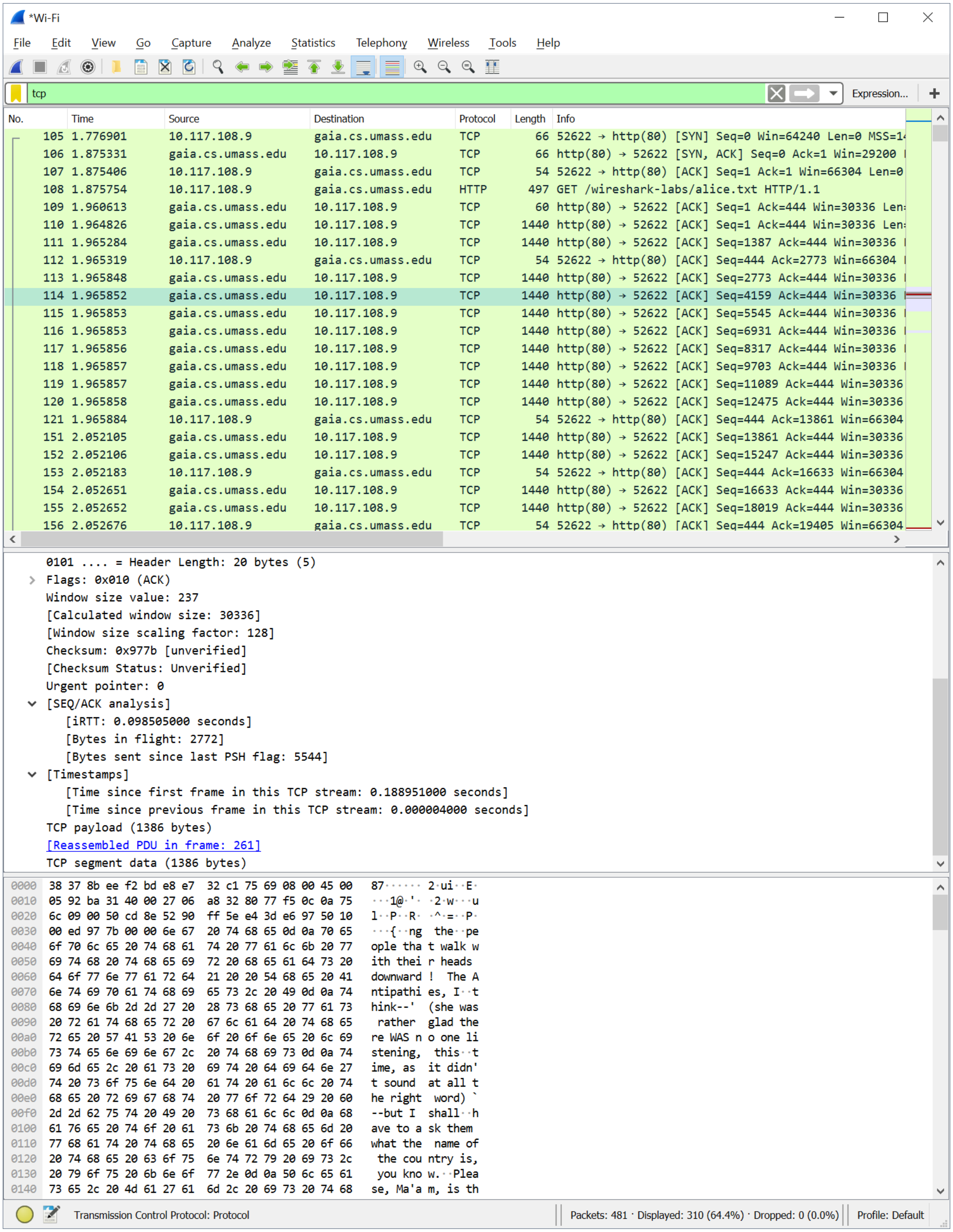
Profile: Default

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

    Answer: I checked sequence numbers of the packets and there were no repeating ones, so there aren't any retransmitted segments in the trace file

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).**

    Answer: On average it acknowledges about 2772 bytes



tcp

```
No.    Time      Source             Destination        Protocol  Length Info
   105 1.776901  10.117.108.9       gaia.cs.umass.edu  TCP         66 52622 → http(80) [SYN] Seq=0 Win=64240 Len=0 MSS=14
   106 1.875331  gaia.cs.umass.edu  10.117.108.9       TCP         66 http(80) → 52622 [SYN, ACK] Seq=0 Ack=1 Win=29200 I
   107 1.875406  10.117.108.9       gaia.cs.umass.edu  TCP         54 52622 → http(80) [ACK] Seq=1 Ack=1 Win=66304 Len=0
   108 1.875754  10.117.108.9       gaia.cs.umass.edu  HTTP       497 GET /wireshark-labs/alice.txt HTTP/1.1
   109 1.960613  gaia.cs.umass.edu  10.117.108.9       TCP         60 http(80) → 52622 [ACK] Seq=1 Ack=444 Win=30336 Len:
   110 1.964826  gaia.cs.umass.edu  10.117.108.9       TCP       1440 http(80) → 52622 [ACK] Seq=1 Ack=444 Win=30336 Len:
   111 1.965284  gaia.cs.umass.edu  10.117.108.9       TCP       1440 http(80) → 52622 [ACK] Seq=1387 Ack=444 Win=30336 I
   112 1.965319  10.117.108.9       gaia.cs.umass.edu  TCP         54 52622 → http(80) [ACK] Seq=444 Ack=2773 Win=66304 I
   113 1.965848  gaia.cs.umass.edu  10.117.108.9       TCP       1440 http(80) → 52622 [ACK] Seq=2773 Ack=444 Win=30336 I
   114 1.965852  gaia.cs.umass.edu  10.117.108.9       TCP       1440 http(80) → 52622 [ACK] Seq=4159 Ack=444 Win=30336 I
   115 1.965853  gaia.cs.umass.edu  10.117.108.9       TCP       1440 http(80) → 52622 [ACK] Seq=5545 Ack=444 Win=30336 I
   116 1.965853  gaia.cs.umass.edu  10.117.108.9       TCP       1440 http(80) → 52622 [ACK] Seq=6931 Ack=444 Win=30336 I
   117 1.965856  gaia.cs.umass.edu  10.117.108.9       TCP       1440 http(80) → 52622 [ACK] Seq=8317 Ack=444 Win=30336 I
   118 1.965857  gaia.cs.umass.edu  10.117.108.9       TCP       1440 http(80) → 52622 [ACK] Seq=9703 Ack=444 Win=30336 I
   119 1.965857  gaia.cs.umass.edu  10.117.108.9       TCP       1440 http(80) → 52622 [ACK] Seq=11089 Ack=444 Win=30336
   120 1.965858  gaia.cs.umass.edu  10.117.108.9       TCP       1440 http(80) → 52622 [ACK] Seq=12475 Ack=444 Win=30336
   121 1.965884  10.117.108.9       gaia.cs.umass.edu  TCP         54 52622 → http(80) [ACK] Seq=444 Ack=13861 Win=66304
   151 2.052105  gaia.cs.umass.edu  10.117.108.9       TCP       1440 http(80) → 52622 [ACK] Seq=13861 Ack=444 Win=30336
   152 2.052106  gaia.cs.umass.edu  10.117.108.9       TCP       1440 http(80) → 52622 [ACK] Seq=15247 Ack=444 Win=30336
   153 2.052183  10.117.108.9       gaia.cs.umass.edu  TCP         54 52622 → http(80) [ACK] Seq=444 Ack=16633 Win=66304
   154 2.052651  gaia.cs.umass.edu  10.117.108.9       TCP       1440 http(80) → 52622 [ACK] Seq=16633 Ack=444 Win=30336
   155 2.052652  gaia.cs.umass.edu  10.117.108.9       TCP       1440 http(80) → 52622 [ACK] Seq=18019 Ack=444 Win=30336
   156 2.052676  10.117.108.9       gaia.cs.umass.edu  TCP         54 52622 → http(80) [ACK] Seq=444 Ack=19405 Win=66304
```

```
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window size value: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
    Checksum: 0x977b [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  v [SEQ/ACK analysis]
       [iRTT: 0.098505000 seconds]
       [Bytes in flight: 2772]
       [Bytes sent since last PSH flag: 5544]
  v [Timestamps]
       [Time since first frame in this TCP stream: 0.188951000 seconds]
       [Time since previous frame in this TCP stream: 0.000004000 seconds]
    TCP payload (1386 bytes)
    [Reassembled PDU in frame: 261]
    TCP segment data (1386 bytes)
```

```
0000  38 37 8b ee f2 bd e8 e7  32 c1 75 69 08 00 45 00   87······ 2·ui··E·
0010  05 92 ba 31 40 00 27 06  a8 32 80 77 f5 0c 0a 75   ···1@·'· ·2·w···u
0020  6c 09 00 50 cd 8e 52 90  ff 5e e4 3d e6 97 50 10   l··P··R· ·^·=··P·
0030  00 ed 97 7b 00 00 6e 67  20 74 68 65 0d 0a 70 65   ···{··ng  the··pe
0040  6f 70 6c 65 20 74 68 61  74 20 77 61 6c 6b 20 77   ople tha t walk w
0050  69 74 68 20 74 68 65 69  72 20 68 65 61 64 73 20   ith thei r heads 
0060  64 6f 77 6e 77 61 72 64  21 20 20 54 68 65 20 41   downward !  The A
0070  6e 74 69 70 61 74 68 69  65 73 2c 20 49 0d 0a 74   ntipathi es, I··t
0080  68 69 6e 6b 2d 2d 27 20  28 73 68 65 20 77 61 73   hink--'  (she was
0090  20 72 61 74 68 65 72 20  67 6c 61 64 20 74 68 65    rather  glad the
00a0  72 65 20 57 41 53 20 6e  6f 20 6f 6e 65 20 6c 69   re WAS n o one li
00b0  73 74 65 6e 69 6e 67 2c  20 74 68 69 73 0d 0a 74   stening,  this··t
00c0  69 6d 65 2c 20 61 73 20  69 74 20 64 69 64 6e 27   ime, as  it didn'
00d0  74 20 73 6f 75 6e 64 20  61 74 20 61 6c 6c 20 74   t sound  at all t
00e0  68 65 20 72 69 67 68 74  20 77 6f 72 64 29 20 60   he right  word) `
00f0  2d 2d 62 75 74 20 49 20  73 68 61 6c 6c 0d 0a 68   --but I  shall··h
0100  61 76 65 20 74 6f 20 61  73 6b 20 74 68 65 6d 20   ave to a sk them 
0110  77 68 61 74 20 74 68 65  20 6e 61 6d 65 20 6f 66   what the  name of
0120  20 74 68 65 20 63 6f 75  6e 74 72 79 20 69 73 2c    the cou ntry is,
0130  20 79 6f 75 20 6b 6e 6f  77 2e 0d 0a 50 6c 65 61    you kno w.··Plea
0140  73 65 2c 20 4d 61 27 61  6d 2c 20 69 73 20 74 68   se, Ma'a m, is th
```

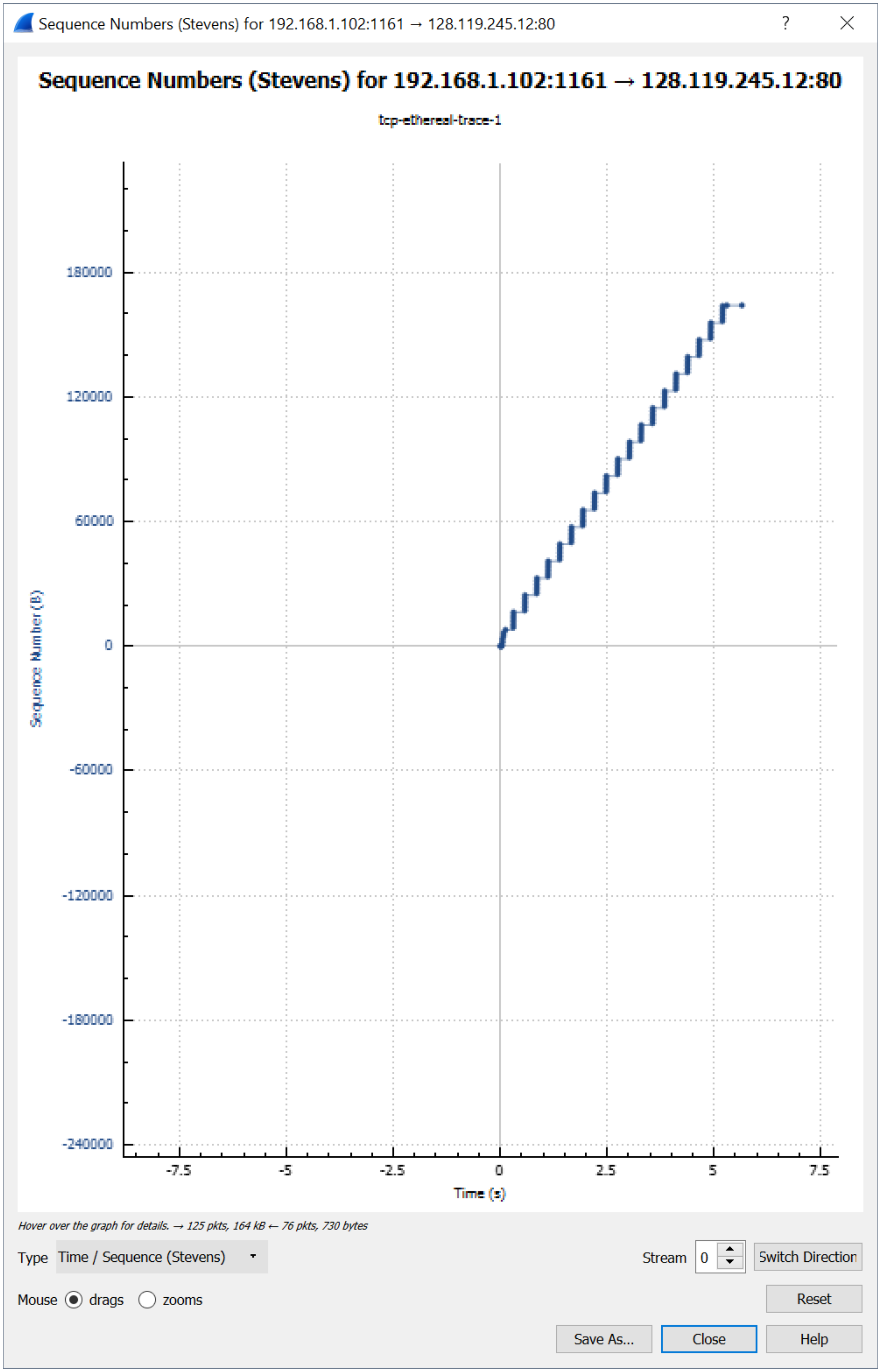
Transmission Control Protocol: Protocol | Packets: 481 · Displayed: 310 (64.4%) · Dropped: 0 (0.0%) | Profile: Default

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

    Answer: By using the file size of the alice file (155,648 bytes) and dividing it by the time spent total for the TCP connection, which was 1.16 seconds, I got a throughput of 133,458 bytes/second.

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**

    Answer: From packet 0 to packet 5 is where the slow start phase of the tCP connection lasts. After that, congestion avoidance takes over



Sequence Numbers (Stevens) for 192.168.1.102:1161 → 128.119.245.12:80

Sequence Numbers (Stevens) for 192.168.1.102:1161 → 128.119.245.12:80

tcp-ethereal-trace-1

Hover over the graph for details. → 125 pkts, 164 kB ← 76 pkts, 730 bytes

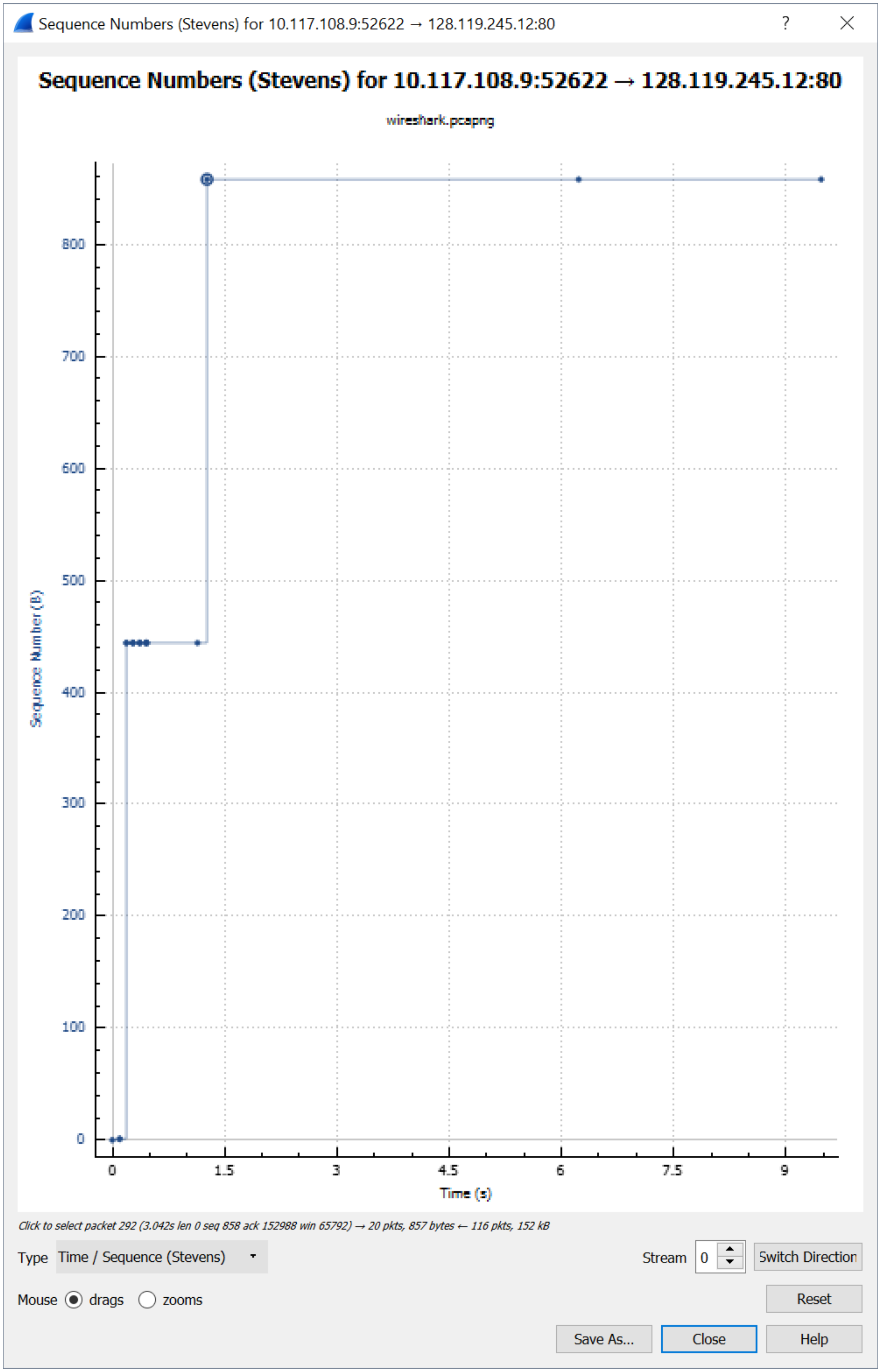
Type Time / Sequence (Stevens)

Stream 0

Mouse ● drags ○ zooms

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**

    Answer: There is a major difference in the way my stevens graph looks compared to the one made from the capture file. I suspect this is due to large number of other packets that were captured unrelated to the lab



Sequence Numbers (Stevens) for 10.117.108.9:52622 → 128.119.245.12:80

Click to select packet 292 (3.042s len 0 seq 858 ack 152988 win 65792) → 20 pkts, 857 bytes ← 116 pkts, 152 kB

Type Time / Sequence (Stevens)

Stream 0

Mouse ● drags ○ zooms