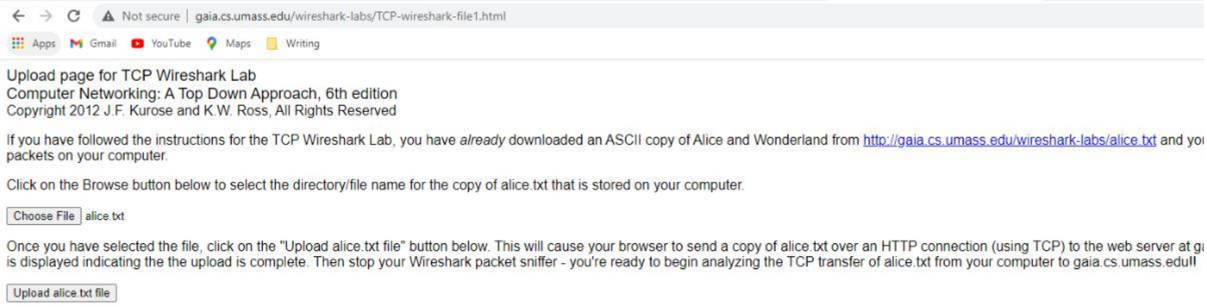
TCP Protocol Analysis

- After installing the wireshark on the machine.

1. Capturing a bulk TCP transfer from your computer to a remote server

- Browsed http://gaia.cs.umass.edu/wiresharklabs/alice.txt on chrome browser and then saved this file on the computer.
- Then browsed http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html on chrome browser.
- Using browse button, selected the saved file (alice.txt) on computer.


Not secure | gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html
Apps
Gmail
YouTube
Maps
Writing

Upload page for TCP Wireshark Lab
Computer Networking: A Top Down Approach, 6th edition
Copyright 2012 J.F. Kurose and K.W. Ross, All Rights Reserved

If you have followed the instructions for the TCP Wireshark Lab, you have *already* downloaded an ASCII copy of Alice and Wonderland from http://gaia.cs.umass.edu/wireshark-labs/alice.txt and yo packets on your computer.

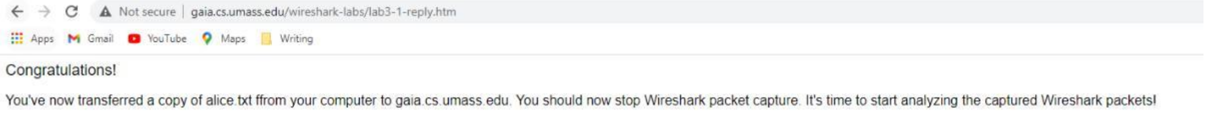
Click on the Browse button below to select the directory/file name for the copy of alice.txt that is stored on your computer.

Choose File alice.txt

Once you have selected the file, click on the "Upload alice.txt file" button below. This will cause your browser to send a copy of alice.txt over an HTTP connection (using TCP) to the web server at g is displayed indicating the the upload is complete. Then stop your Wireshark packet sniffer - you're ready to begin analyzing the TCP transfer of alice.txt from your computer to gaia.cs.umass.edu!!

Upload alice.txt file

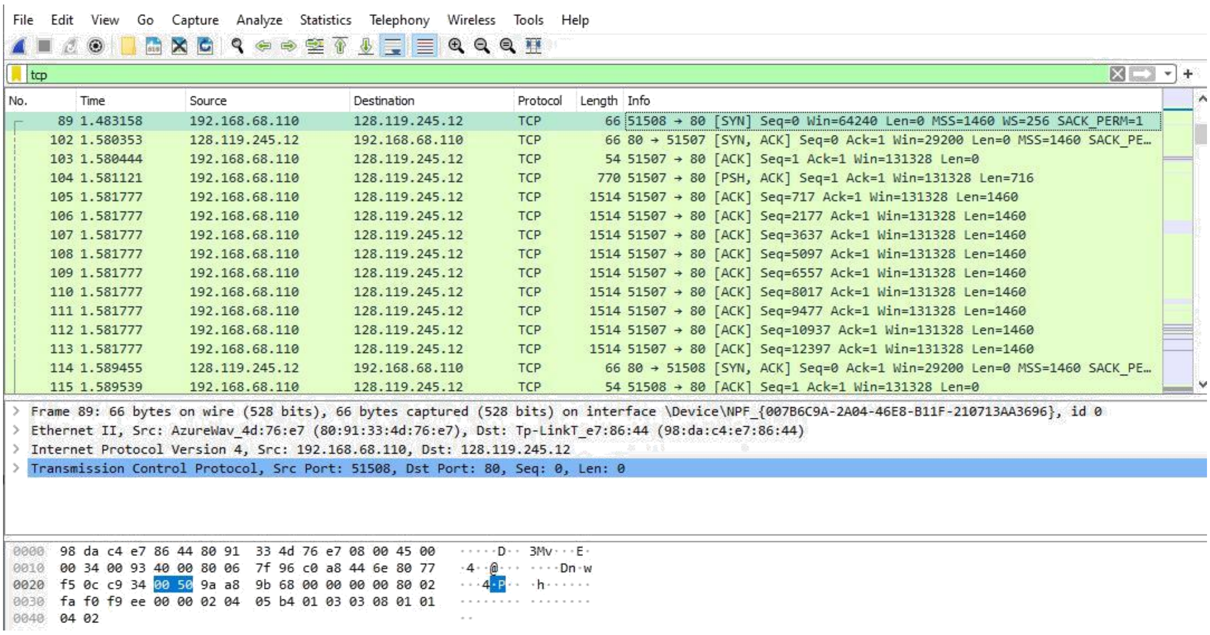
- Then opened wireshark and then clicked on upload button on chrome browser. Below congratulation message displayed on browser (as shown in snaphot).


Not secure | gaia.cs.umass.edu/wireshark-labs/lab3-1-reply.htm
Apps
Gmail
YouTube
Maps
Writing

Congratulations!

You've now transferred a copy of alice.txt ffrom your computer to gaia.cs.umass.edu. You should now stop Wireshark packet capture. It's time to start analyzing the captured Wireshark packets!

- Captured packet while uploading the file (alice.txt) on wireshark. After filtering the TCP protocol in wireshark, packets are shown as given in below snapshot:



tcp

```
No.     Time        Source           Destination      Protocol  Length  Info
     89 1.483158    192.168.68.110   128.119.245.12   TCP           66  51508 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
    102 1.580353    128.119.245.12   192.168.68.110   TCP           66  80 → 51507 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PE…
    103 1.580444    192.168.68.110   128.119.245.12   TCP           54  51507 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
    104 1.581121    192.168.68.110   128.119.245.12   TCP          770  51507 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=716
    105 1.581777    192.168.68.110   128.119.245.12   TCP         1514  51507 → 80 [ACK] Seq=717 Ack=1 Win=131328 Len=1460
    106 1.581777    192.168.68.110   128.119.245.12   TCP         1514  51507 → 80 [ACK] Seq=2177 Ack=1 Win=131328 Len=1460
    107 1.581777    192.168.68.110   128.119.245.12   TCP         1514  51507 → 80 [ACK] Seq=3637 Ack=1 Win=131328 Len=1460
    108 1.581777    192.168.68.110   128.119.245.12   TCP         1514  51507 → 80 [ACK] Seq=5097 Ack=1 Win=131328 Len=1460
    109 1.581777    192.168.68.110   128.119.245.12   TCP         1514  51507 → 80 [ACK] Seq=6557 Ack=1 Win=131328 Len=1460
    110 1.581777    192.168.68.110   128.119.245.12   TCP         1514  51507 → 80 [ACK] Seq=8017 Ack=1 Win=131328 Len=1460
    111 1.581777    192.168.68.110   128.119.245.12   TCP         1514  51507 → 80 [ACK] Seq=9477 Ack=1 Win=131328 Len=1460
    112 1.581777    192.168.68.110   128.119.245.12   TCP         1514  51507 → 80 [ACK] Seq=10937 Ack=1 Win=131328 Len=1460
    113 1.581777    192.168.68.110   128.119.245.12   TCP         1514  51507 → 80 [ACK] Seq=12397 Ack=1 Win=131328 Len=1460
    114 1.589455    128.119.245.12   192.168.68.110   TCP           66  80 → 51508 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PE…
    115 1.589539    192.168.68.110   128.119.245.12   TCP           54  51508 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
```

```
> Frame 89: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{007B6C9A-2A04-46E8-B11F-210713AA3696}, id 0
> Ethernet II, Src: AzureWav_4d:76:e7 (80:91:33:4d:76:e7), Dst: Tp-LinkT_e7:86:44 (98:da:c4:e7:86:44)
> Internet Protocol Version 4, Src: 192.168.68.110, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 51508, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  98 da c4 e7 86 44 80 91  33 4d 76 e7 08 00 45 00   ·····D·· 3Mv···E·
0010  00 34 00 93 40 00 80 06  7f 96 c0 a8 44 6e 80 77   ·4··@··· ····Dn·w
0020  f5 0c c9 34 00 50 9a a8  9b 68 00 00 00 00 80 02   ···4·P·· ·h······
0030  fa f0 f9 ee 00 00 02 04  05 b4 01 03 03 08 01 01   ········ ········
0040  04 02                                              ··
```

Since, below questions are required to answer based on wireshark captured packet file **tcpethereal-trace-1**

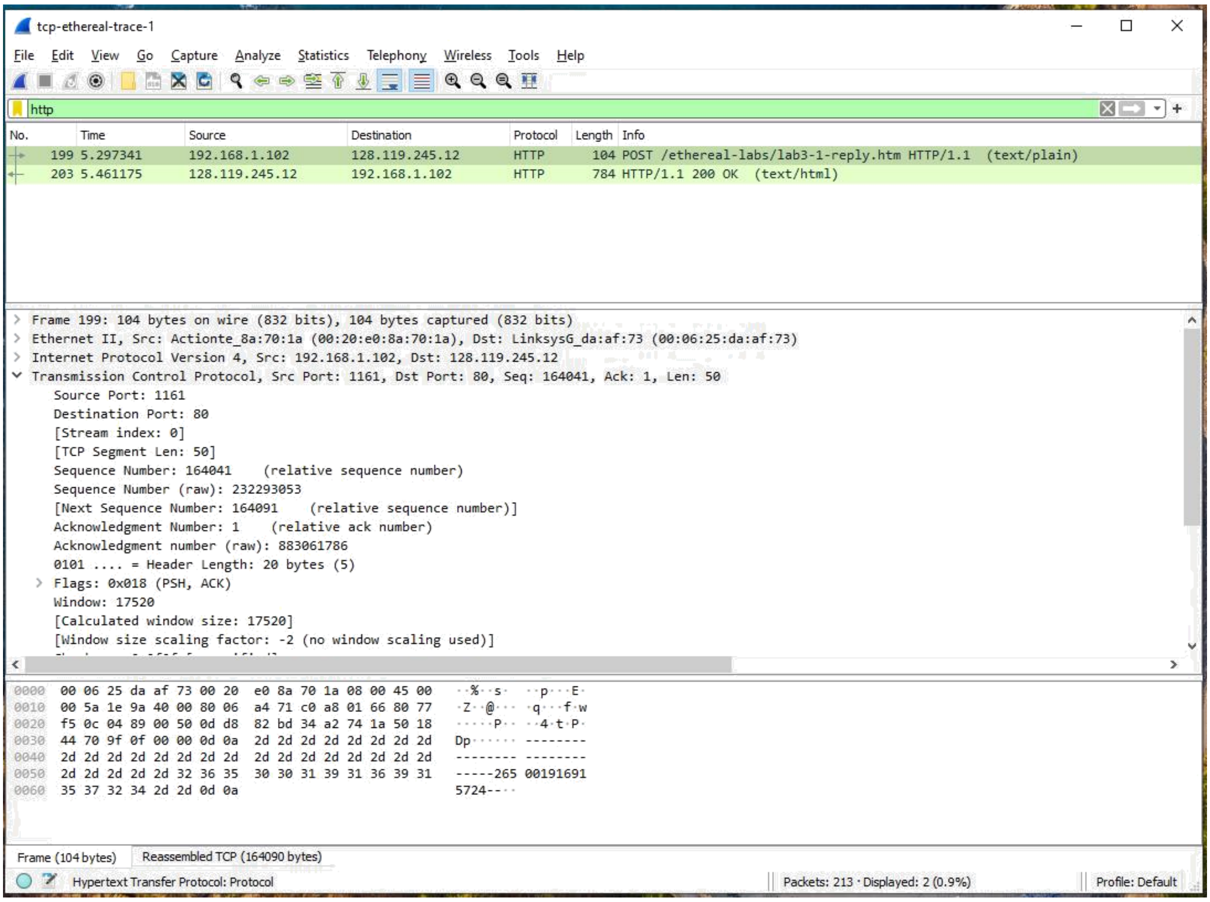
So, opened this trace file in wireshark tool.

2. **A first look at the captured trace**

    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".**

    Answer:1

    IP address used by the client computer(source) is **192.168.1.102**
    TCP port number used by the client computer(source) is **1161**


tcp-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
```

```
No.   Time       Source          Destination     Protocol  Length Info
  199 5.297341   192.168.1.102   128.119.245.12  HTTP         104 POST /ethereal-labs/lab3-1-reply.htm HTTP/1.1  (text/plain)
  203 5.461175   128.119.245.12  192.168.1.102   HTTP         784 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 199: 104 bytes on wire (832 bits), 104 bytes captured (832 bits)
> Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 164041, Ack: 1, Len: 50
    Source Port: 1161
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 50]
    Sequence Number: 164041    (relative sequence number)
    Sequence Number (raw): 232293053
    [Next Sequence Number: 164091    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 883061786
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 17520
    [Calculated window size: 17520]
    [Window size scaling factor: -2 (no window scaling used)]
```

```
0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ··%··s·  ··p···E·
0010  00 5a 1e 9a 40 00 80 06  a4 71 c0 a8 01 66 80 77   ·Z··@···  ·q···f·w
0020  f5 0c 04 89 00 50 0d d8  82 bd 34 a2 74 1a 50 18   ·····P··  ··4·t·P·
0030  44 70 9f 0f 00 00 0d 0a  2d 2d 2d 2d 2d 2d 2d 2d   Dp······  --------
0040  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   --------  --------
0050  2d 2d 2d 2d 2d 32 36 35  30 30 31 39 31 36 39 31   -----265  00191691
0060  35 37 32 34 2d 2d 0d 0a                            5724--··
```

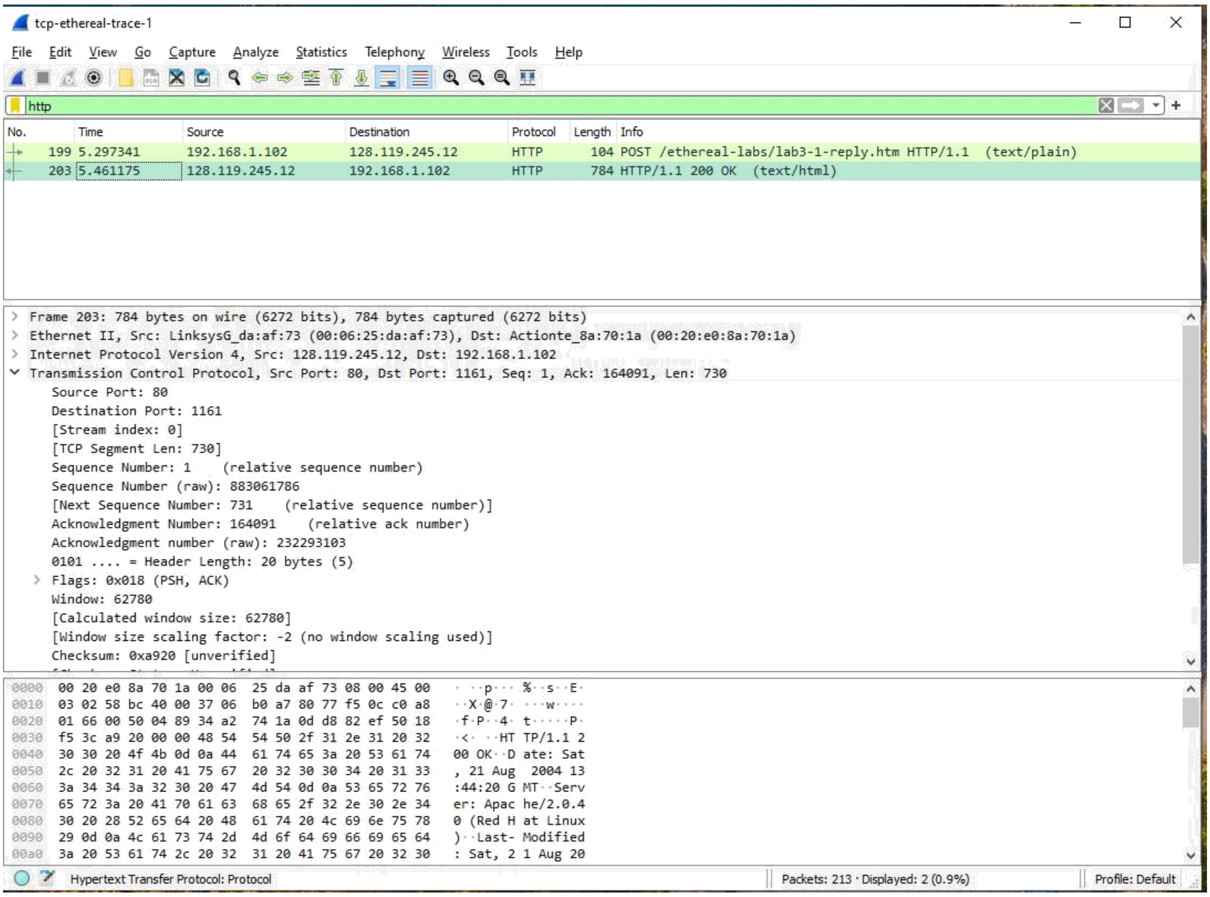
Frame (104 bytes)
Reassembled TCP (164090 bytes)
Hypertext Transfer Protocol: Protocol
Packets: 213 · Displayed: 2 (0.9%)
Profile: Default

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:2

IP address of gaia.cs.umass.edu is **128.119.245.12**

Port number for sending and receiving TCP segment is **80** and **1161**


tcp-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

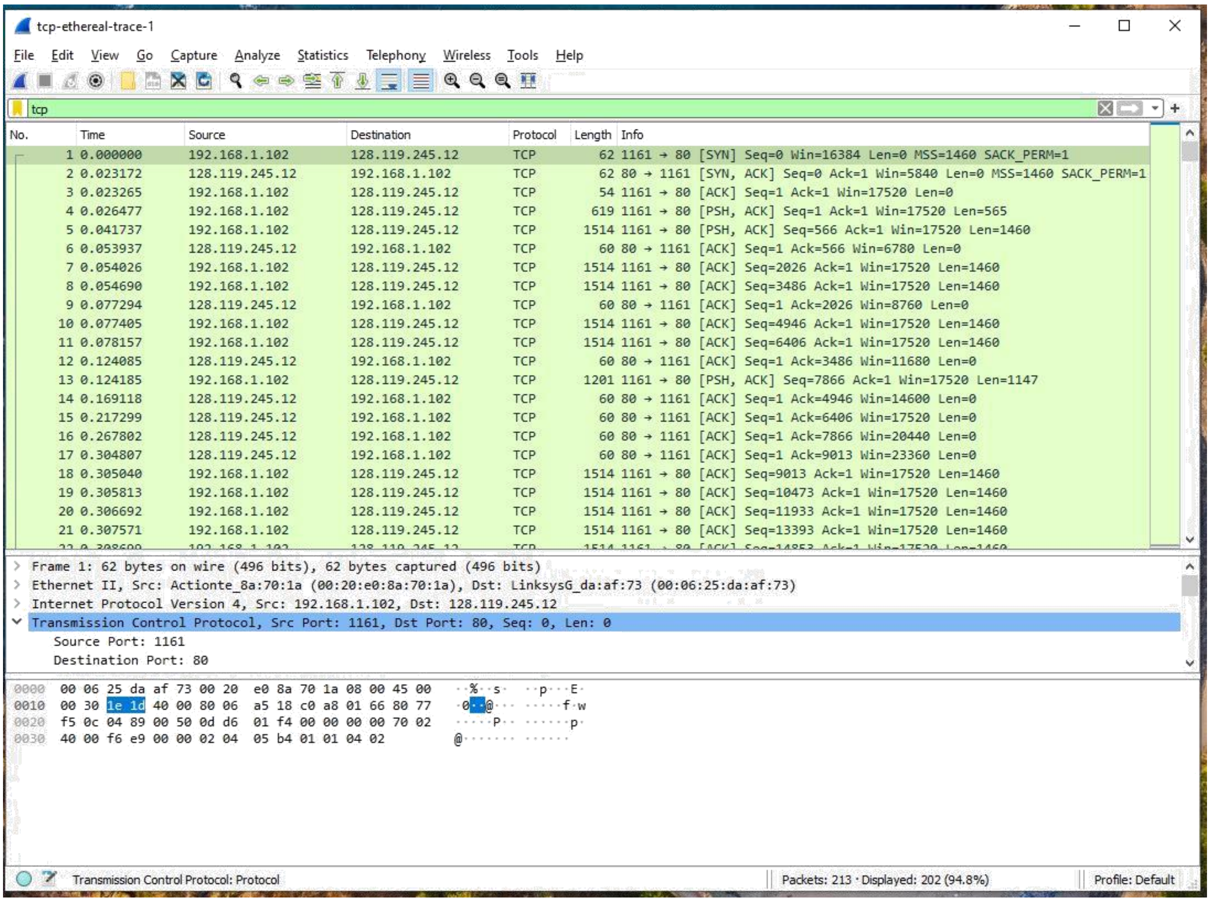
No.	Time	Source	Destination	Protocol	Length	Info
199	5.297341	192.168.1.102	128.119.245.12	HTTP	104	POST /ethereal-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
203	5.461175	128.119.245.12	192.168.1.102	HTTP	784	HTTP/1.1 200 OK (text/html)

```
> Frame 203: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
v Transmission Control Protocol, Src Port: 80, Dst Port: 1161, Seq: 1, Ack: 164091, Len: 730
     Source Port: 80
     Destination Port: 1161
     [Stream index: 0]
     [TCP Segment Len: 730]
     Sequence Number: 1    (relative sequence number)
     Sequence Number (raw): 883061786
     [Next Sequence Number: 731    (relative sequence number)]
     Acknowledgment Number: 164091    (relative ack number)
     Acknowledgment number (raw): 232293103
     0101 .... = Header Length: 20 bytes (5)
   > Flags: 0x018 (PSH, ACK)
     Window: 62780
     [Calculated window size: 62780]
     [Window size scaling factor: -2 (no window scaling used)]
     Checksum: 0xa920 [unverified]
```

```
0000  00 20 e0 8a 70 1a 00 06  25 da af 73 08 00 45 00   · ··p··· %··s··E·
0010  03 02 58 bc 40 00 37 06  b0 a7 80 77 f5 0c c0 a8   ··X·@·7· ···w····
0020  01 66 00 50 04 89 34 a2  74 1a 0d d8 82 ef 50 18   ·f·P··4· t·····P·
0030  f5 3c a9 20 00 00 48 54  54 50 2f 31 2e 31 20 32   ·<· ··HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 53 61 74   00 OK··D ate: Sat
0050  2c 20 32 31 20 41 75 67  20 32 30 30 34 20 31 33   , 21 Aug  2004 13
0060  3a 34 34 3a 32 30 20 47  4d 54 0d 0a 53 65 72 76   :44:20 G MT··Serv
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 30 2e 34   er: Apac he/2.0.4
0080  30 20 28 52 65 64 20 48  61 74 20 4c 69 6e 75 78   0 (Red H at Linux
0090  29 0d 0a 4c 61 73 74 2d  4d 6f 64 69 66 69 65 64   )··Last- Modified
00a0  3a 20 53 61 74 2c 20 32  31 20 41 75 67 20 32 30   : Sat, 2 1 Aug 20
```

Hypertext Transfer Protocol: Protocol | Packets: 213 · Displayed: 2 (0.9%) | Profile: Default

Now uncheck the HTTP box from wireshark by doing this, select Analyze->Enabled Protocols->uncheck HTTP box->select OK
Wireshark screen will look as shown in below snapshot:


tcp-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

```
No.   Time      Source          Destination     Protocol Length Info
    1 0.000000  192.168.1.102   128.119.245.12  TCP        62 1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
    2 0.023172  128.119.245.12  192.168.1.102   TCP        62 80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
    3 0.023265  192.168.1.102   128.119.245.12  TCP        54 1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
    4 0.026477  192.168.1.102   128.119.245.12  TCP       619 1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565
    5 0.041737  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460
    6 0.053937  128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
    7 0.054026  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460
    8 0.054690  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460
    9 0.077294  128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
   10 0.077405  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460
   11 0.078157  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460
   12 0.124085  128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0
   13 0.124185  192.168.1.102   128.119.245.12  TCP      1201 1161 → 80 [PSH, ACK] Seq=7866 Ack=1 Win=17520 Len=1147
   14 0.169118  128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=4946 Win=14600 Len=0
   15 0.217299  128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=6406 Win=17520 Len=0
   16 0.267802  128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=7866 Win=20440 Len=0
   17 0.304807  128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=9013 Win=23360 Len=0
   18 0.305040  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=9013 Ack=1 Win=17520 Len=1460
   19 0.305813  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=10473 Ack=1 Win=17520 Len=1460
   20 0.306692  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=11933 Ack=1 Win=17520 Len=1460
   21 0.307571  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=13393 Ack=1 Win=17520 Len=1460
   22 0.308699  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=14853 Ack=1 Win=17520 Len=1460
```

```
> Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
> Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 1161
    Destination Port: 80
```

```
0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ··%··s·  ··p···E·
0010  00 30 1e 1d 40 00 80 06  a5 18 c0 a8 01 66 80 77   ·0··@···  ·····f·w
0020  f5 0c 04 89 00 50 0d d6  01 f4 00 00 00 00 70 02   ·····P··  ······p·
0030  40 00 f6 e9 00 00 02 04  05 b4 01 01 04 02         @·······  ······
```

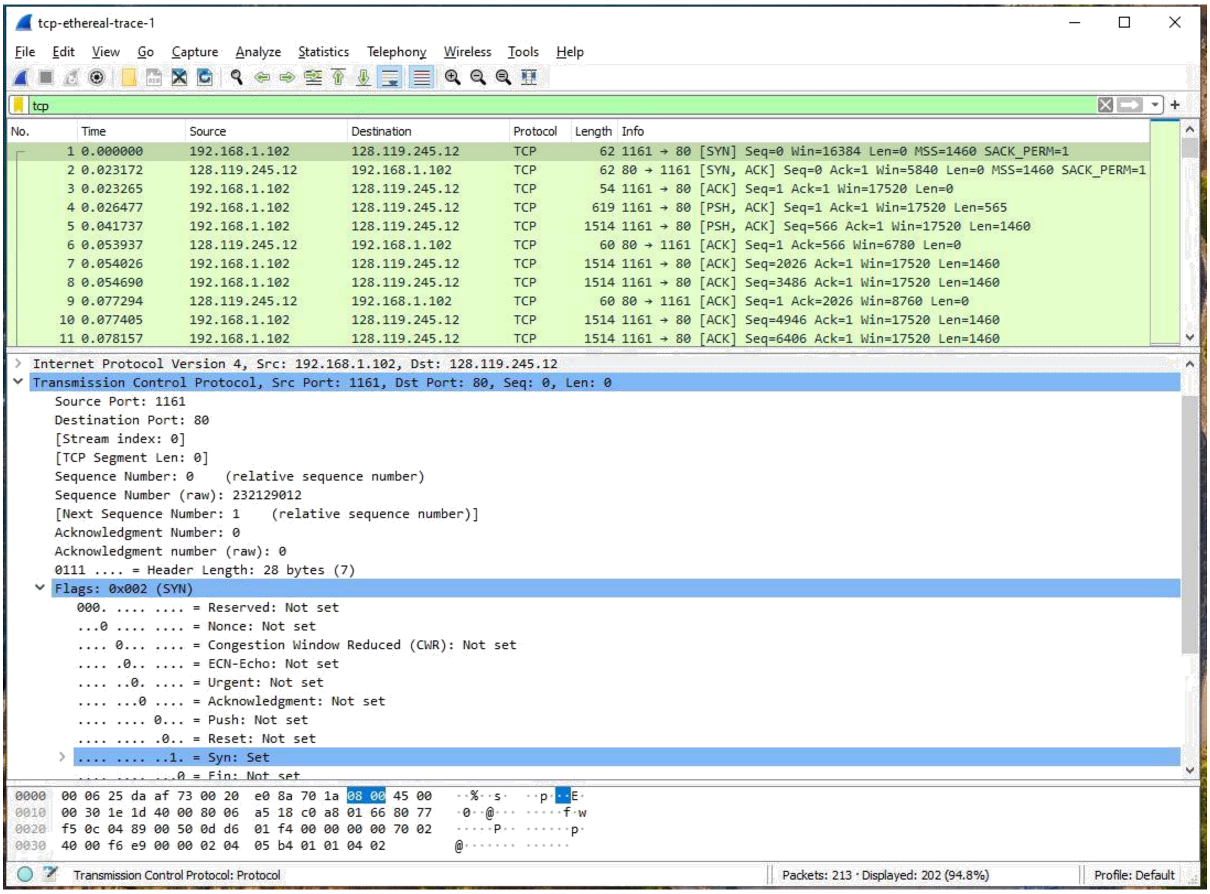
Transmission Control Protocol: Protocol | Packets: 213 · Displayed: 202 (94.8%) | Profile: Default

3. **TCP Basics**
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:1

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 is **0** as found in trace file.

The SYN flag has set to 1 which identifies the segment as SYN segment.
Refer below snapshot:



tcp

```
No.   Time       Source           Destination      Protocol  Length Info
    1 0.000000   192.168.1.102    128.119.245.12   TCP         62 1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
    2 0.023172   128.119.245.12   192.168.1.102    TCP         62 80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
    3 0.023265   192.168.1.102    128.119.245.12   TCP         54 1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
    4 0.026477   192.168.1.102    128.119.245.12   TCP        619 1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565
    5 0.041737   192.168.1.102    128.119.245.12   TCP       1514 1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460
    6 0.053937   128.119.245.12   192.168.1.102    TCP         60 80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
    7 0.054026   192.168.1.102    128.119.245.12   TCP       1514 1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460
    8 0.054690   192.168.1.102    128.119.245.12   TCP       1514 1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460
    9 0.077294   128.119.245.12   192.168.1.102    TCP         60 80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
   10 0.077405   192.168.1.102    128.119.245.12   TCP       1514 1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460
   11 0.078157   192.168.1.102    128.119.245.12   TCP       1514 1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460
```

```
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 0, Len: 0
     Source Port: 1161
     Destination Port: 80
     [Stream index: 0]
     [TCP Segment Len: 0]
     Sequence Number: 0    (relative sequence number)
     Sequence Number (raw): 232129012
     [Next Sequence Number: 1    (relative sequence number)]
     Acknowledgment Number: 0
     Acknowledgment number (raw): 0
     0111 .... = Header Length: 28 bytes (7)
  v  Flags: 0x002 (SYN)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...0 .... = Acknowledgment: Not set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
     >  .... .... ..1. = Syn: Set
        .... .... ...0 = Fin: Not set
```

```
0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ··%··s·  ··p···E·
0010  00 30 1e 1d 40 00 80 06  a5 18 c0 a8 01 66 80 77   ·0··@···  ·····f·w
0020  f5 0c 04 89 00 50 0d d6  01 f4 00 00 00 00 70 02   ·····P··  ······p·
0030  40 00 f6 e9 00 00 02 04  05 b4 01 01 04 02         @·······  ······
```

Transmission Control Protocol: Protocol | Packets: 213 · Displayed: 202 (94.8%) | 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:5

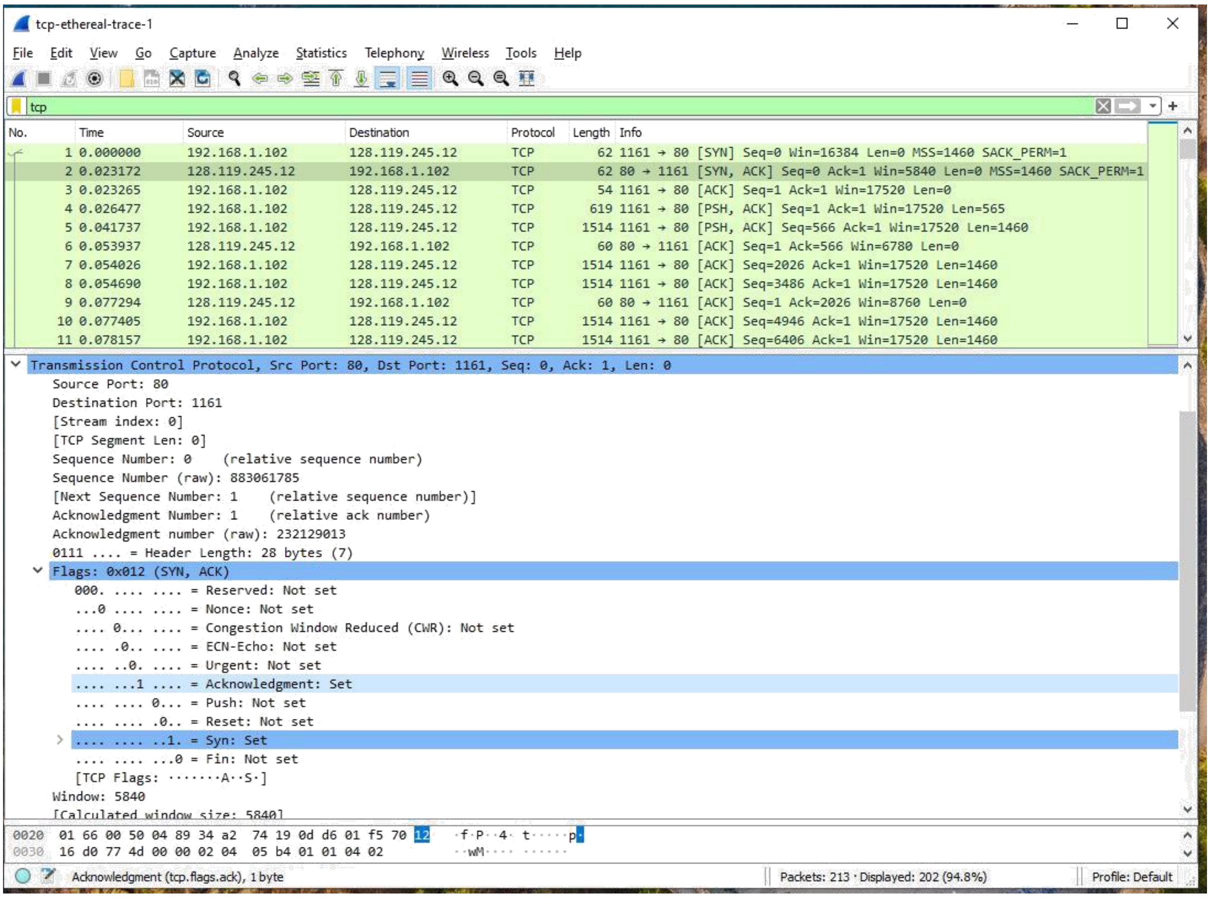
The sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN is **0** in the trace file.

Value of acknowledgment number in trace file is **1**.

gaia.cs.umass.edu determined the acknowledgment field value in the SYNACK segment by adding 1 to the initial sequence number (0) of SYN segment that was initiated by the client computer.

Initial sequence number of SYN segment (0) + 1 = Acknowledgment number of SYNACK (1)

The flag of SYN and Acknowledgement in the segment are set to 1 and they indicate that this segment is a SYNACK segment. Refer snapshot below:


tcp-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp
```

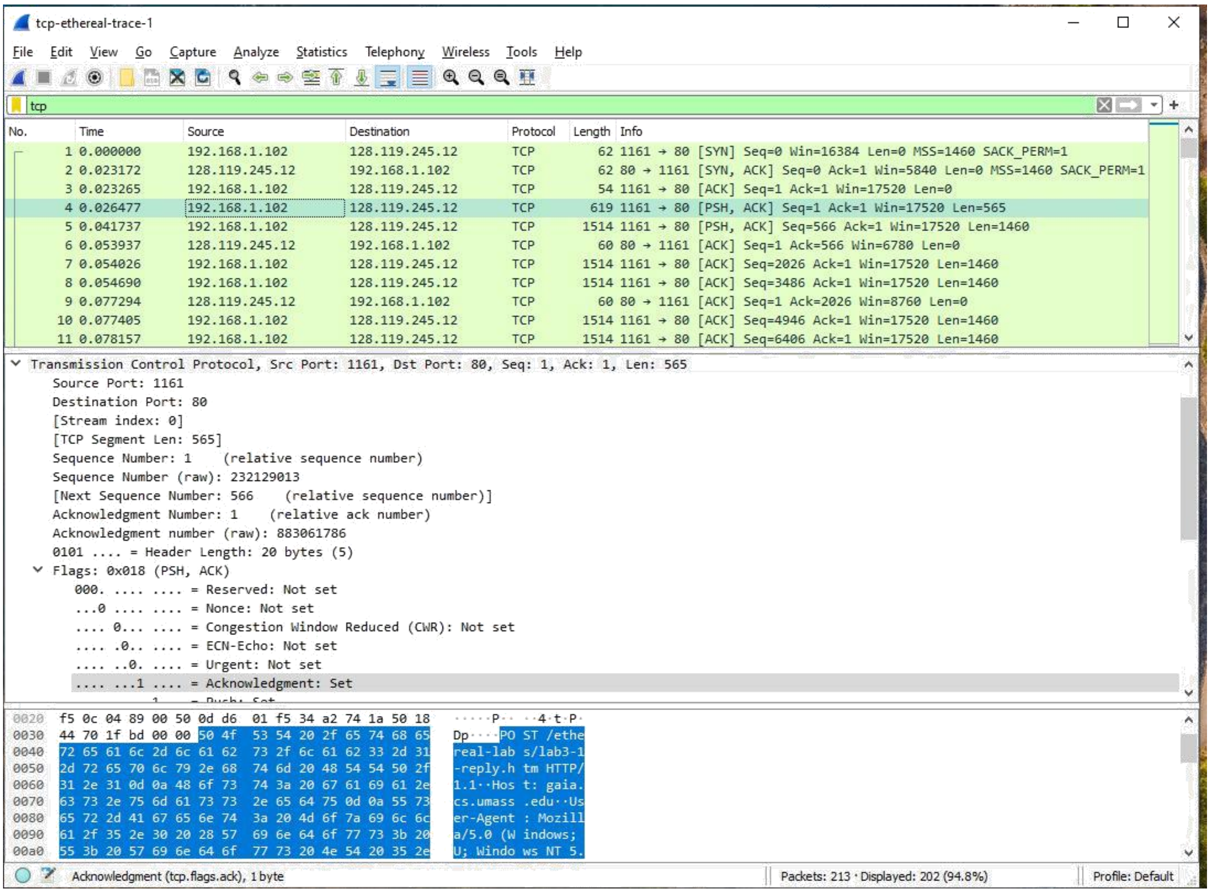
```
No.  Time       Source          Destination     Protocol Length Info
   1 0.000000   192.168.1.102   128.119.245.12  TCP        62 1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
   2 0.023172   128.119.245.12  192.168.1.102   TCP        62 80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
   3 0.023265   192.168.1.102   128.119.245.12  TCP        54 1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
   4 0.026477   192.168.1.102   128.119.245.12  TCP       619 1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565
   5 0.041737   192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460
   6 0.053937   128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
   7 0.054026   192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460
   8 0.054690   192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460
   9 0.077294   128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
  10 0.077405   192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460
  11 0.078157   192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460
```

```
Transmission Control Protocol, Src Port: 80, Dst Port: 1161, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 1161
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 883061785
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 232129013
    0111 .... = Header Length: 28 bytes (7)
    Flags: 0x012 (SYN, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 0... = Push: Not set
        .... .... .0.. = Reset: Not set
        .... .... ..1. = Syn: Set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·······A··S·]
    Window: 5840
    [Calculated window size: 5840]
```

```
0020  01 66 00 50 04 89 34 a2  74 19 0d d6 01 f5 70 12   ·f·P··4· t·····p·
0030  16 d0 77 4d 00 00 02 04  05 b4 01 01 04 02         ··wM···· ······
```

Acknowledgment (tcp.flags.ack), 1 byte | Packets: 213 · Displayed: 202 (94.8%) | Profile: Default

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:6
   The sequence number of the TCP segment containing the HTTP POST command is **1**



```
No.    Time      Source          Destination     Protocol Length Info
     1 0.000000  192.168.1.102   128.119.245.12  TCP        62 1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
     2 0.023172  128.119.245.12  192.168.1.102   TCP        62 80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
     3 0.023265  192.168.1.102   128.119.245.12  TCP        54 1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
     4 0.026477  192.168.1.102   128.119.245.12  TCP       619 1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565
     5 0.041737  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460
     6 0.053937  128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
     7 0.054026  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460
     8 0.054690  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460
     9 0.077294  128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
    10 0.077405  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460
    11 0.078157  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460
```

```
Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 1, Ack: 1, Len: 565
    Source Port: 1161
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 565]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 232129013
    [Next Sequence Number: 566    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 883061786
    0101 .... = Header Length: 20 bytes (5)
  Flags: 0x018 (PSH, ACK)
       000. .... .... = Reserved: Not set
       ...0 .... .... = Nonce: Not set
       .... 0... .... = Congestion Window Reduced (CWR): Not set
       .... .0.. .... = ECN-Echo: Not set
       .... ..0. .... = Urgent: Not set
       .... ...1 .... = Acknowledgment: Set
```

```
0020  f5 0c 04 89 00 50 0d d6  01 f5 34 a2 74 1a 50 18   ·····P·· ··4·t·P·
0030  44 70 1f bd 00 00 50 4f  53 54 20 2f 65 74 68 65   Dp····PO ST /ethe
0040  72 65 61 6c 2d 6c 61 62  73 2f 6c 61 62 33 2d 31   real-lab s/lab3-1
0050  2d 72 65 70 6c 79 2e 68  74 6d 20 48 54 54 50 2f   -reply.h tm HTTP/
0060  31 2e 31 0d 0a 48 6f 73  74 3a 20 67 61 69 61 2e   1.1··Hos t: gaia.
0070  63 73 2e 75 6d 61 73 73  2e 65 64 75 0d 0a 55 73   cs.umass .edu··Us
0080  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
0090  61 2f 35 2e 30 20 28 57  69 6e 64 6f 77 73 3b 20   a/5.0 (W indows; 
00a0  55 3b 20 57 69 6e 64 6f  77 73 20 4e 54 20 35 2e   U; Windo ws NT 5.
```

Acknowledgment (tcp.flags.ack), 1 byte | Packets: 213 · Displayed: 202 (94.8%) | 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?**

Answer:7

The sequence number of first six segments in the TCP connections are taken from segment-4,5,7,8,10,11 in this trace file:

First segment in the TCP connection containing HTTP POST: **1**

Second segment sequence number: **566**

Third segment sequence number: **2026**

Fourth segment sequence number: **3486**

Fifth segment sequence number: **4946**

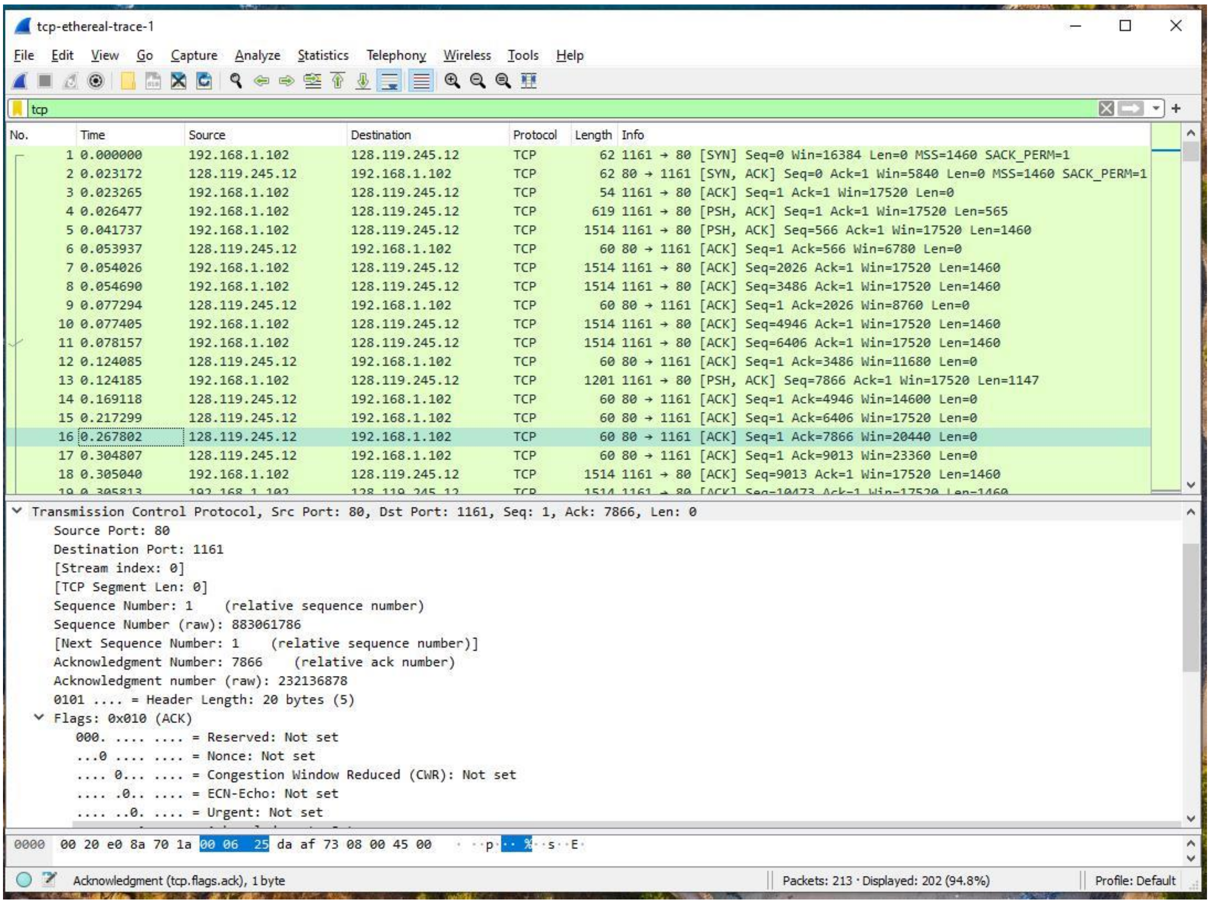
Sixth segment sequence number: **6406**

Time at which each segment was sent:

TCP segment	Sent time (seconds)
Segment 1	0.026477
Segment 2	0.041737
Segment 3	0.054026
Segment 4	0.05469
Segment 5	0.077405
Segment 6	0.078157

Time when ACK for each segment received:

TCP segment	Received time (seconds)
Segment 1	0.053937
Segment 2	0.077294
Segment 3	0.124085
Segment 4	0.169118
Segment 5	0.217299
Segment 6	0.267802


tcp-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

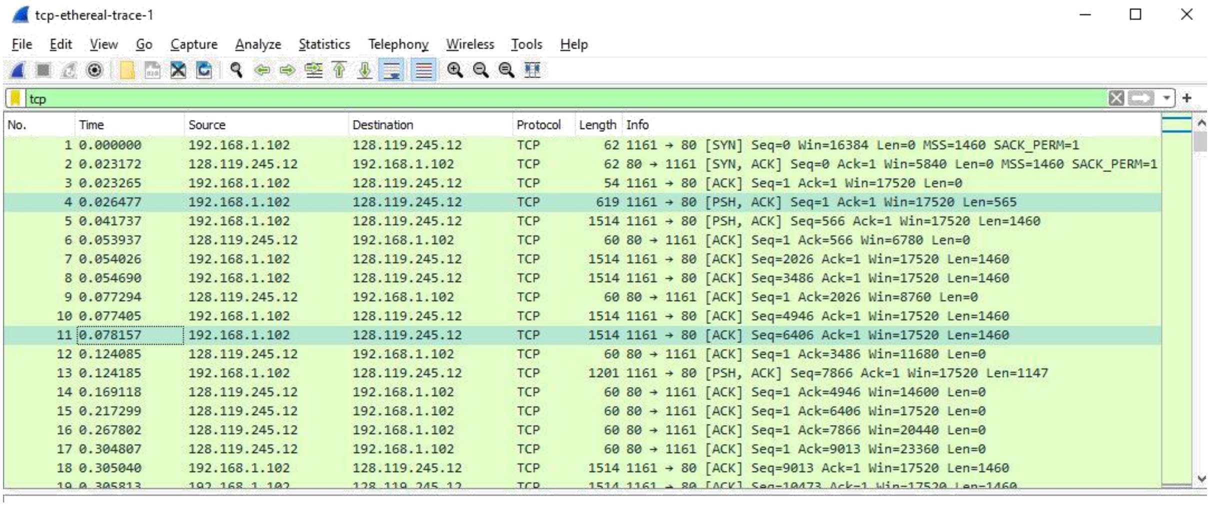
```
No.   Time      Source          Destination     Protocol Length Info
    1 0.000000  192.168.1.102   128.119.245.12  TCP        62 1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
    2 0.023172  128.119.245.12  192.168.1.102   TCP        62 80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
    3 0.023265  192.168.1.102   128.119.245.12  TCP        54 1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
    4 0.026477  192.168.1.102   128.119.245.12  TCP       619 1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565
    5 0.041737  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460
    6 0.053937  128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
    7 0.054026  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460
    8 0.054690  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460
    9 0.077294  128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
   10 0.077405  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460
   11 0.078157  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460
   12 0.124085  128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0
   13 0.124185  192.168.1.102   128.119.245.12  TCP      1201 1161 → 80 [PSH, ACK] Seq=7866 Ack=1 Win=17520 Len=1147
   14 0.169118  128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=4946 Win=14600 Len=0
   15 0.217299  128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=6406 Win=17520 Len=0
   16 0.267802  128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=7866 Win=20440 Len=0
   17 0.304807  128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=9013 Win=23360 Len=0
   18 0.305040  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=9013 Ack=1 Win=17520 Len=1460
   19 0.305813  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=10473 Ack=1 Win=17520 Len=1460
```

```
Transmission Control Protocol, Src Port: 80, Dst Port: 1161, Seq: 1, Ack: 7866, Len: 0
    Source Port: 80
    Destination Port: 1161
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 883061786
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 7866    (relative ack number)
    Acknowledgment number (raw): 232136878
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x010 (ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
```

```
0000  00 20 e0 8a 70 1a 00 06  25 da af 73 08 00 45 00   · ··p·· %··s··E·
```

Acknowledgment (tcp.flags.ack), 1 byte
Packets: 213 · Displayed: 202 (94.8%)
Profile: Default

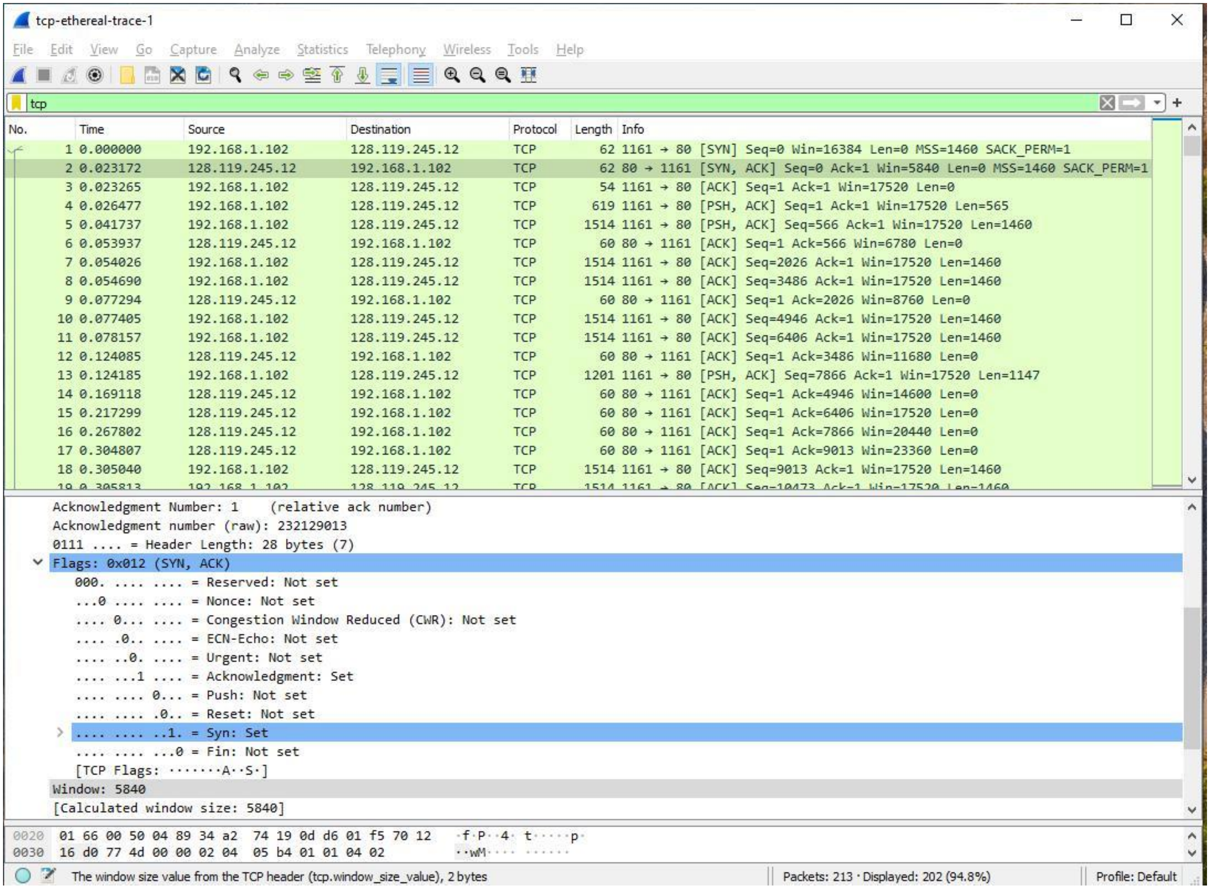
8. **What is the length of each of the first six TCP segments?**
   Answer:8
   The first TCP segment (containing the HTTP POST) has length: 565 bytes
   Other five TCP segments are of length: 1460 bytes (each)


tcp-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

```
No.     Time          Source            Destination       Protocol  Length  Info
      1 0.000000      192.168.1.102     128.119.245.12    TCP         62 1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
      2 0.023172      128.119.245.12    192.168.1.102     TCP         62 80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
      3 0.023265      192.168.1.102     128.119.245.12    TCP         54 1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
      4 0.026477      192.168.1.102     128.119.245.12    TCP        619 1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565
      5 0.041737      192.168.1.102     128.119.245.12    TCP       1514 1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460
      6 0.053937      128.119.245.12    192.168.1.102     TCP         60 80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
      7 0.054026      192.168.1.102     128.119.245.12    TCP       1514 1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460
      8 0.054690      192.168.1.102     128.119.245.12    TCP       1514 1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460
      9 0.077294      128.119.245.12    192.168.1.102     TCP         60 80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
     10 0.077405      192.168.1.102     128.119.245.12    TCP       1514 1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460
     11 0.078157      192.168.1.102     128.119.245.12    TCP       1514 1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460
     12 0.124085      128.119.245.12    192.168.1.102     TCP         60 80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0
     13 0.124185      192.168.1.102     128.119.245.12    TCP       1201 1161 → 80 [PSH, ACK] Seq=7866 Ack=1 Win=17520 Len=1147
     14 0.169118      128.119.245.12    192.168.1.102     TCP         60 80 → 1161 [ACK] Seq=1 Ack=4946 Win=14600 Len=0
     15 0.217299      128.119.245.12    192.168.1.102     TCP         60 80 → 1161 [ACK] Seq=1 Ack=6406 Win=17520 Len=0
     16 0.267802      128.119.245.12    192.168.1.102     TCP         60 80 → 1161 [ACK] Seq=1 Ack=7866 Win=20440 Len=0
     17 0.304807      128.119.245.12    192.168.1.102     TCP         60 80 → 1161 [ACK] Seq=1 Ack=9013 Win=23360 Len=0
     18 0.305040      192.168.1.102     128.119.245.12    TCP       1514 1161 → 80 [ACK] Seq=9013 Ack=1 Win=17520 Len=1460
     19 0.305813      192.168.1.102     128.119.245.12    TCP       1514 1161 → 80 [ACK] Seq=10473 Ack=1 Win=17520 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?**
   Answer:9

   The minimum amount of available buffer space advertised at the received for the entire trace is 5840 bytes. It is shown in segment 2 of the first acknowledgement from the server. This receiver window grows steadily until a maximum receiver buffer size is of 62780 bytes. No, the lack of receiver buffer space doesn't throttle the sender.


tcp-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

```
No.     Time          Source            Destination       Protocol  Length  Info
      1 0.000000      192.168.1.102     128.119.245.12    TCP         62 1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
      2 0.023172      128.119.245.12    192.168.1.102     TCP         62 80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
      3 0.023265      192.168.1.102     128.119.245.12    TCP         54 1161 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
      4 0.026477      192.168.1.102     128.119.245.12    TCP        619 1161 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=565
      5 0.041737      192.168.1.102     128.119.245.12    TCP       1514 1161 → 80 [PSH, ACK] Seq=566 Ack=1 Win=17520 Len=1460
      6 0.053937      128.119.245.12    192.168.1.102     TCP         60 80 → 1161 [ACK] Seq=1 Ack=566 Win=6780 Len=0
      7 0.054026      192.168.1.102     128.119.245.12    TCP       1514 1161 → 80 [ACK] Seq=2026 Ack=1 Win=17520 Len=1460
      8 0.054690      192.168.1.102     128.119.245.12    TCP       1514 1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460
      9 0.077294      128.119.245.12    192.168.1.102     TCP         60 80 → 1161 [ACK] Seq=1 Ack=2026 Win=8760 Len=0
     10 0.077405      192.168.1.102     128.119.245.12    TCP       1514 1161 → 80 [ACK] Seq=4946 Ack=1 Win=17520 Len=1460
     11 0.078157      192.168.1.102     128.119.245.12    TCP       1514 1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460
     12 0.124085      128.119.245.12    192.168.1.102     TCP         60 80 → 1161 [ACK] Seq=1 Ack=3486 Win=11680 Len=0
     13 0.124185      192.168.1.102     128.119.245.12    TCP       1201 1161 → 80 [PSH, ACK] Seq=7866 Ack=1 Win=17520 Len=1147
     14 0.169118      128.119.245.12    192.168.1.102     TCP         60 80 → 1161 [ACK] Seq=1 Ack=4946 Win=14600 Len=0
     15 0.217299      128.119.245.12    192.168.1.102     TCP         60 80 → 1161 [ACK] Seq=1 Ack=6406 Win=17520 Len=0
     16 0.267802      128.119.245.12    192.168.1.102     TCP         60 80 → 1161 [ACK] Seq=1 Ack=7866 Win=20440 Len=0
     17 0.304807      128.119.245.12    192.168.1.102     TCP         60 80 → 1161 [ACK] Seq=1 Ack=9013 Win=23360 Len=0
     18 0.305040      192.168.1.102     128.119.245.12    TCP       1514 1161 → 80 [ACK] Seq=9013 Ack=1 Win=17520 Len=1460
     19 0.305813      192.168.1.102     128.119.245.12    TCP       1514 1161 → 80 [ACK] Seq=10473 Ack=1 Win=17520 Len=1460
```

```
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 232129013
    0111 .... = Header Length: 28 bytes (7)
  ∨ Flags: 0x012 (SYN, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    > .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·······A··S·]
    Window: 5840
    [Calculated window size: 5840]

0020  01 66 00 50 04 89 34 a2  74 19 0d d6 01 f5 70 12   ·f·P··4· t·····p·
0030  16 d0 77 4d 00 00 02 04  05 b4 01 01 04 02         ··wM···· ······

The window size value from the TCP header (tcp.window_size_value), 2 bytes    Packets: 213 · Displayed: 202 (94.8%)    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:10

There are no retransmitted segments in the trace file. To verify this in the trace file, check the sequence numbers of the TCP segments in the trace file. All sequence numbers from the source (192.168.1.102) to the destination (128.119.245.12) are increasing with respect to time.