Lab Assignment-9

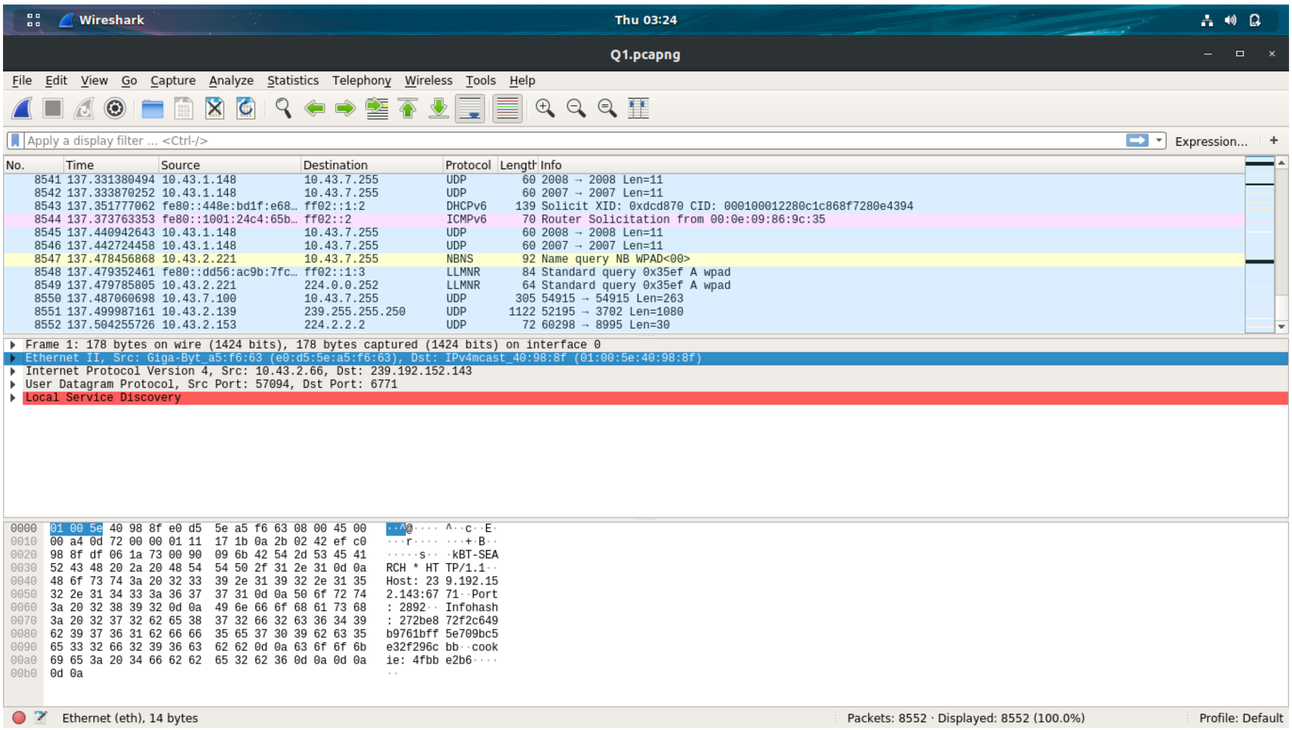
Indian Institute of Technology Roorkee Department of Computer Science and Engineering

CSN-361: Computer Networks Laboratory (Autumn 2019-2020)

Aman jaiswal
Enrollment No:-17114008
B.tech CSE 3rd Year.

Problem Statement 1:

Install Wireshark and explore its uses to capture network traffic. You have to capture normal internet traffic for 20-30 minutes from your system using Wireshark. You need to copy this data in CSV / TXT file.



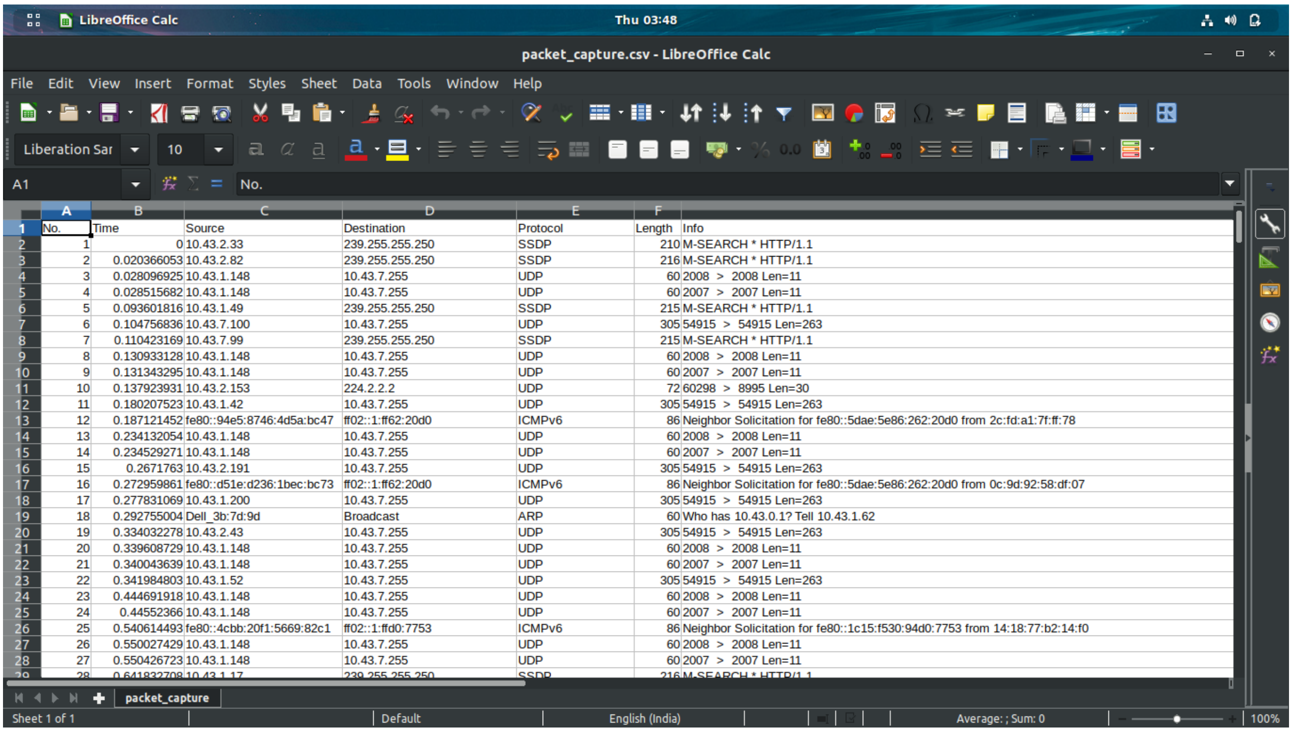
Wireshark
Thu 03:24
Q1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.   Time           Source                Destination      Protocol Length Info
 8541 137.331380494 10.43.1.148            10.43.7.255      UDP        60 2008 → 2008 Len=11
 8542 137.333870252 10.43.1.148            10.43.7.255      UDP        60 2007 → 2007 Len=11
 8543 137.351777062 fe80::448e:bd1f:e68…   ff02::1:2        DHCPv6    139 Solicit XID: 0xdcd870 CID: 000100012280c1c868f7280e4394
 8544 137.373763353 fe80::1001:24c4:65b…   ff02::2          ICMPv6     70 Router Solicitation from 00:0e:09:86:9c:35
 8545 137.440942643 10.43.1.148            10.43.7.255      UDP        60 2008 → 2008 Len=11
 8546 137.442724458 10.43.1.148            10.43.7.255      UDP        60 2007 → 2007 Len=11
 8547 137.478456868 10.43.2.221            10.43.7.255      NBNS       92 Name query NB WPAD<00>
 8548 137.479352461 fe80::dd56:ac9b:7fc…   ff02::1:3        LLMNR      84 Standard query 0x35ef A wpad
 8549 137.479785805 10.43.2.221            224.0.0.252      LLMNR      64 Standard query 0x35ef A wpad
 8550 137.487060698 10.43.7.100            10.43.7.255      UDP       305 54915 → 54915 Len=263
 8551 137.499987161 10.43.2.139            239.255.255.250  UDP      1122 52195 → 3702 Len=1080
 8552 137.504255726 10.43.2.153            224.2.2.2        UDP        72 60298 → 8995 Len=30
```

```
▸ Frame 1: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits) on interface 0
▸ Ethernet II, Src: Giga-Byt_a5:f6:63 (e0:d5:5e:a5:f6:63), Dst: IPv4mcast_40:98:8f (01:00:5e:40:98:8f)
▸ Internet Protocol Version 4, Src: 10.43.2.66, Dst: 239.192.152.143
▸ User Datagram Protocol, Src Port: 57094, Dst Port: 6771
▸ Local Service Discovery
```

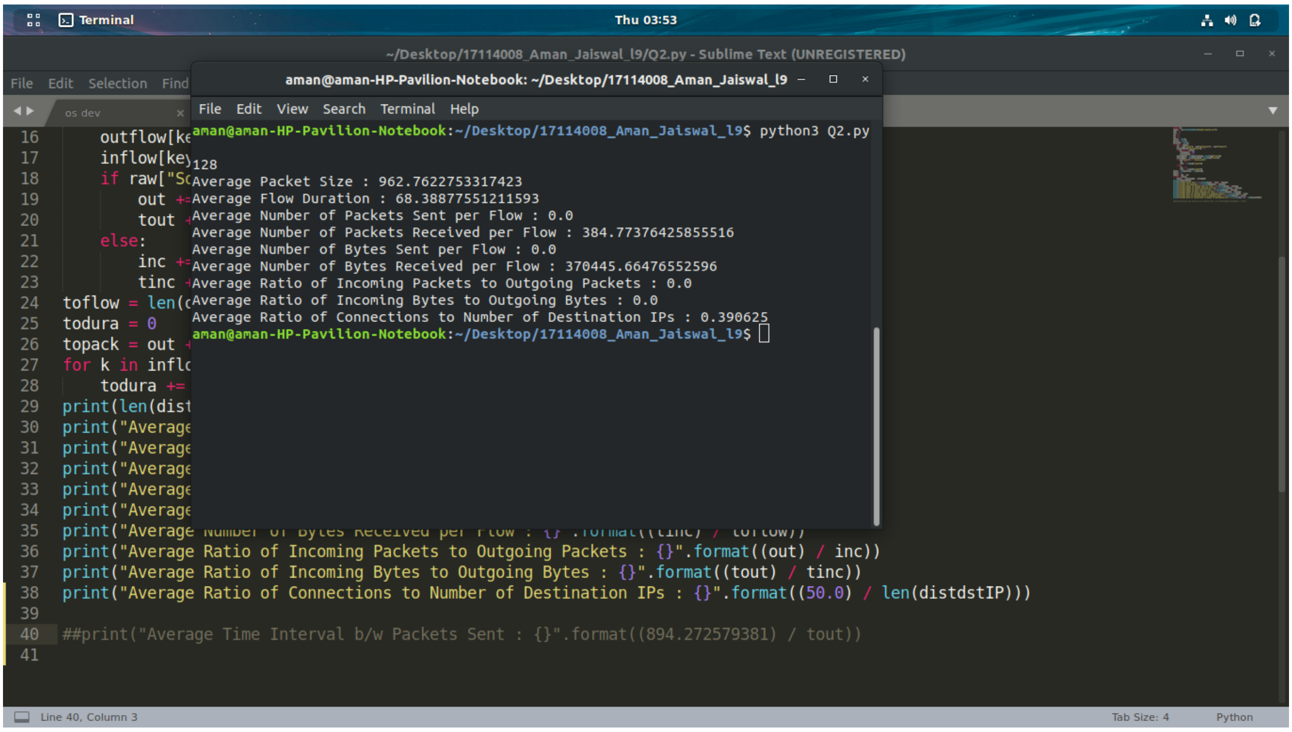
```
0000  01 00 5e 40 98 8f e0 d5  5e a5 f6 63 08 00 45 00   ··^@···· ^··c··E·
0010  00 a4 0d 72 00 00 01 11  17 1b 0a 2b 02 42 ef c0   ···r···· ···+·B··
0020  98 8f df 06 1a 73 00 90  09 6b 42 54 2d 53 45 41   ·····s·· ·kBT-SEA
0030  52 43 48 20 2a 20 48 54  54 50 2f 31 2e 31 0d 0a   RCH * HT TP/1.1··
0040  48 6f 73 74 3a 20 32 33  39 2e 31 39 32 2e 31 35   Host: 23 9.192.15
0050  32 2e 31 34 33 3a 36 37  37 31 0d 0a 50 6f 72 74   2.143:67 71··Port
0060  3a 20 32 38 39 32 0d 0a  49 6e 66 6f 68 61 73 68   : 2892·· Infohash
0070  3a 20 32 37 32 62 65 38  37 32 66 32 63 36 34 39   : 272be8 72f2c649
0080  62 39 37 36 31 62 66 66  35 65 37 30 39 62 63 35   b9761bff 5e709bc5
0090  65 33 32 66 32 39 36 63  62 62 0d 0a 63 6f 6f 6b   e32f296c bb··cook
00a0  69 65 3a 20 34 66 62 62  65 32 62 36 0d 0a 0d 0a   ie: 4fbb e2b6····
00b0  0d 0a                                              ··
```

Ethernet (eth), 14 bytes   Packets: 8552 · Displayed: 8552 (100.0%)   Profile: Default



No.	Time	Source	Destination	Protocol	Length	Info
1	0	10.43.2.33	239.255.255.250	SSDP	210	M-SEARCH * HTTP/1.1
2	0.020366053	10.43.2.82	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
3	0.028096925	10.43.1.148	10.43.7.255	UDP	60	2008 > 2008 Len=11
4	0.028515682	10.43.1.148	10.43.7.255	UDP	60	2007 > 2007 Len=11
5	0.093601816	10.43.1.49	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
6	0.104756836	10.43.7.100	10.43.7.255	UDP	305	54915 > 54915 Len=263
7	0.110423169	10.43.7.99	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
8	0.130933128	10.43.1.148	10.43.7.255	UDP	60	2008 > 2008 Len=11
9	0.131343295	10.43.1.148	10.43.7.255	UDP	60	2007 > 2007 Len=11
10	0.137923931	10.43.2.153	224.2.2.2	UDP	72	60298 > 8995 Len=30
11	0.180207523	10.43.1.42	10.43.7.255	UDP	305	54915 > 54915 Len=263
12	0.187121452	fe80::94e5:8746:4d5a:bc47	ff02::1:ff62:20d0	ICMPv6	86	Neighbor Solicitation for fe80::5dae:5e86:262:20d0 from 2c:fd:a1:7f:ff:78
13	0.234132054	10.43.1.148	10.43.7.255	UDP	60	2008 > 2008 Len=11
14	0.234529271	10.43.1.148	10.43.7.255	UDP	60	2007 > 2007 Len=11
15	0.2671763	10.43.2.191	10.43.7.255	UDP	305	54915 > 54915 Len=263
16	0.272959861	fe80::d51e:d236:1bec:bc73	ff02::1:ff62:20d0	ICMPv6	86	Neighbor Solicitation for fe80::5dae:5e86:262:20d0 from 0c:9d:92:58:df:07
17	0.277831069	10.43.1.200	10.43.7.255	UDP	305	54915 > 54915 Len=263
18	0.292755004	Dell_3b:7d:9d	Broadcast	ARP	60	Who has 10.43.0.1? Tell 10.43.1.62
19	0.334032278	10.43.2.43	10.43.7.255	UDP	305	54915 > 54915 Len=263
20	0.339608729	10.43.1.148	10.43.7.255	UDP	60	2008 > 2008 Len=11
21	0.340043639	10.43.1.148	10.43.7.255	UDP	60	2007 > 2007 Len=11
22	0.341984803	10.43.1.52	10.43.7.255	UDP	305	54915 > 54915 Len=263
23	0.444691918	10.43.1.148	10.43.7.255	UDP	60	2008 > 2008 Len=11
24	0.44552366	10.43.1.148	10.43.7.255	UDP	60	2007 > 2007 Len=11
25	0.540614493	fe80::4cbb:20f1:5669:82c1	ff02::1:ffd0:7753	ICMPv6	86	Neighbor Solicitation for fe80::1c15:f530:94d0:7753 from 14:18:77:b2:14:f0
26	0.550027429	10.43.1.148	10.43.7.255	UDP	60	2008 > 2008 Len=11
27	0.550426723	10.43.1.148	10.43.7.255	UDP	60	2007 > 2007 Len=11
28	0.641832708	10.43.1.17	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1

Problem Statement 2:
Take the CSV / TXT, which is generated in Problem Statement 1 as an input. Write a code (in any programming language of your choice) to extract the following 11 features given below in the table:


Terminal
Thu 03:53
~/Desktop/17114008_Aman_Jaiswal_l9/Q2.py - Sublime Text (UNREGISTERED)
File Edit Selection Find
os dev
aman@aman-HP-Pavilion-Notebook: ~/Desktop/17114008_Aman_Jaiswal_l9
File Edit View Search Terminal Help
Line 40, Column 3
Tab Size: 4
Python

```
    outflow[ke
    inflow[key
    if raw["Sc
        out +=
        tout +
    else:
        inc +=
        tinc +
toflow = len(c
todura = 0
topack = out +
for k in inflo
    todura +=
print(len(dist
print("Average
print("Average
print("Average
print("Average
print("Average
print("Average Number of Bytes Received per Flow : {}".format((tinc) / toflow))
print("Average Ratio of Incoming Packets to Outgoing Packets : {}".format((out) / inc))
print("Average Ratio of Incoming Bytes to Outgoing Bytes : {}".format((tout) / tinc))
print("Average Ratio of Connections to Number of Destination IPs : {}".format((50.0) / len(distdstIP)))

##print("Average Time Interval b/w Packets Sent : {}".format((894.272579381) / tout))

```

```
aman@aman-HP-Pavilion-Notebook:~/Desktop/17114008_Aman_Jaiswal_l9$ python3 Q2.py

128
Average Packet Size : 962.7622753317423
Average Flow Duration : 68.38877551211593
Average Number of Packets Sent per Flow : 0.0
Average Number of Packets Received per Flow : 384.77376425855516
Average Number of Bytes Sent per Flow : 0.0
Average Number of Bytes Received per Flow : 370445.66476552596
Average Ratio of Incoming Packets to Outgoing Packets : 0.0
Average Ratio of Incoming Bytes to Outgoing Bytes : 0.0
Average Ratio of Connections to Number of Destination IPs : 0.390625
aman@aman-HP-Pavilion-Notebook:~/Desktop/17114008_Aman_Jaiswal_l9$ 
```

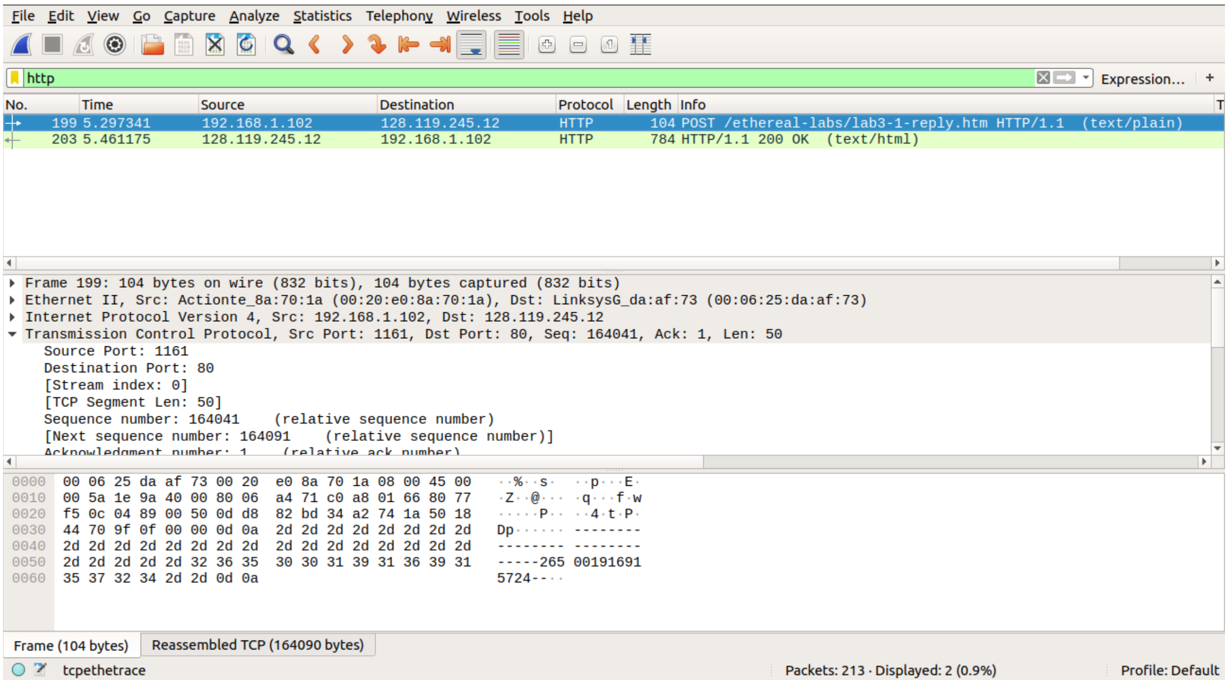
Problem Statement 3:

In this problem, the behavior of TCP protocol will be studied using Wireshark. For this assignment download the Wireshark captured trace file named as tcpethe-trace from Piazza,which is a packet trace of TCP transfer of a file from a client system to a remote server (named as ser1), obtained by running Wireshark on the client machine. Open tcpethe-trace file in Wireshark and answer the following question:

a. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to server (ser1)?

Sol->

The client computer (source)'s IP address is 192.168.1.102 and the TCP port number is 1161.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression…
+
Frame (104 bytes)
Reassembled TCP (164090 bytes)
tcpethetrace
Packets: 213 · Displayed: 2 (0.9%)
Profile: Default

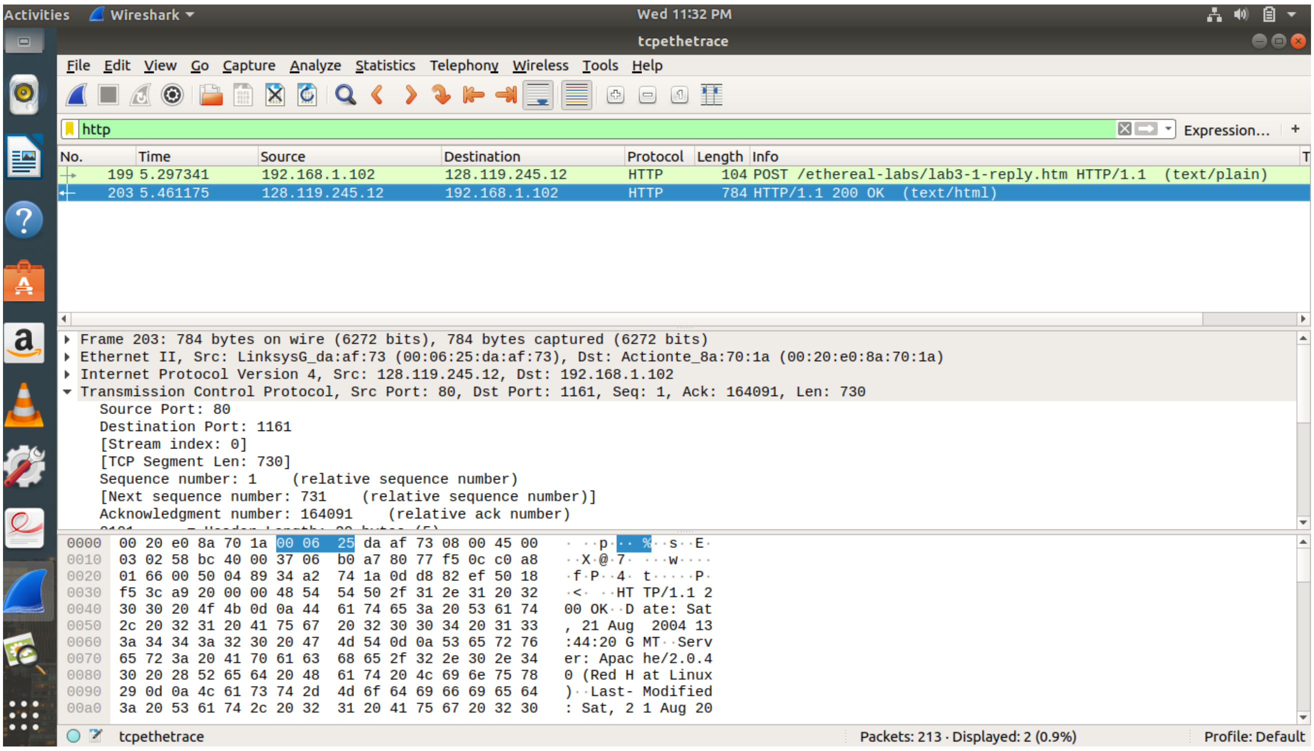
```
No.   Time        Source          Destination     Protocol Length Info
  199 5.297341    192.168.1.102   128.119.245.12  HTTP        104 POST /ethereal-labs/lab3-1-reply.htm HTTP/1.1  (text/plain)
  203 5.461175    128.119.245.12  192.168.1.102   HTTP        784 HTTP/1.1 200 OK  (text/html)
```

```
▸ 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
▾ 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)
    [Next sequence number: 164091    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
```

```
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--··
```

b. What is the IP address of server (ser1)? On what port number it is sending and receiving the TCP segments for this connection?

Sol-> The IP address of ser1 is 128.119.245.12 and the TCP port number is 80.

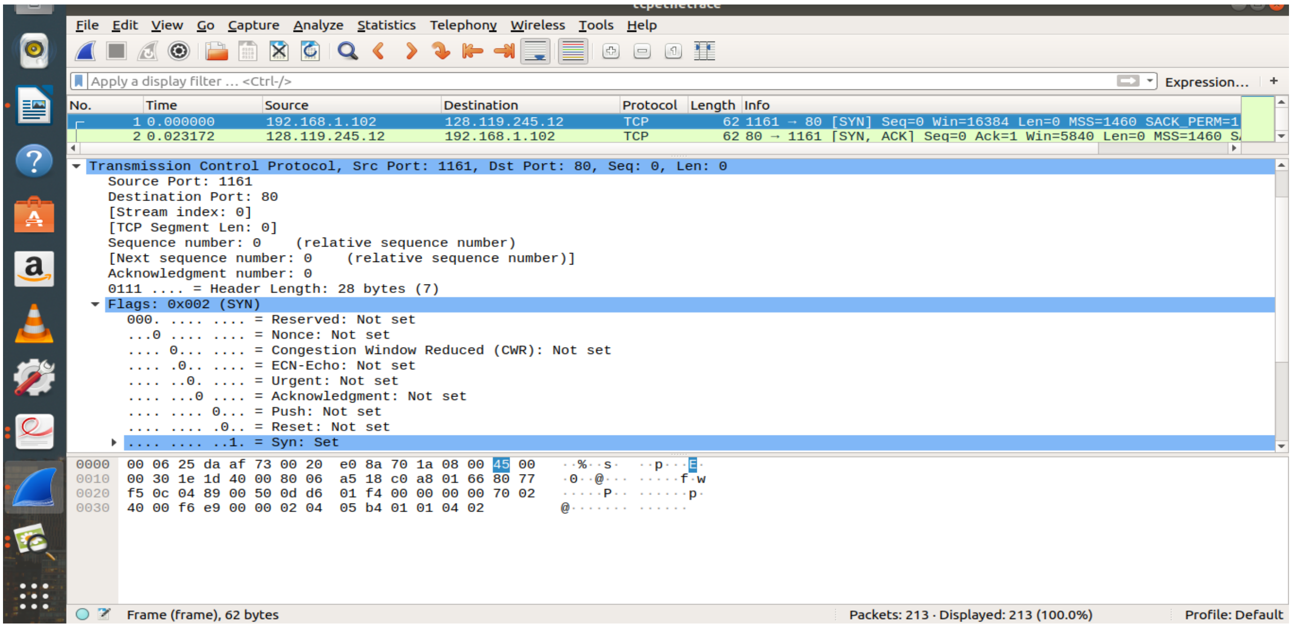


Activities
Wireshark ▾
Wed 11:32 PM
tcpethetrace
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…

```
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
▾ 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)
    [Next sequence number: 731    (relative sequence number)]
    Acknowledgment number: 164091    (relative ack number)

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

tcpethetrace                          Packets: 213 · Displayed: 2 (0.9%)        Profile: Default
```

c. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and ser1? What is it in the segment that identifies the segment as a SYN segment?

Sol-> The sequence number of the TCP SYN segment is 0 since it is used to imitate the TCP connection between the client computer and ser1.
In the Flags section, the Syn flag is set to 1 which indicates that this segment is a SYN segment.



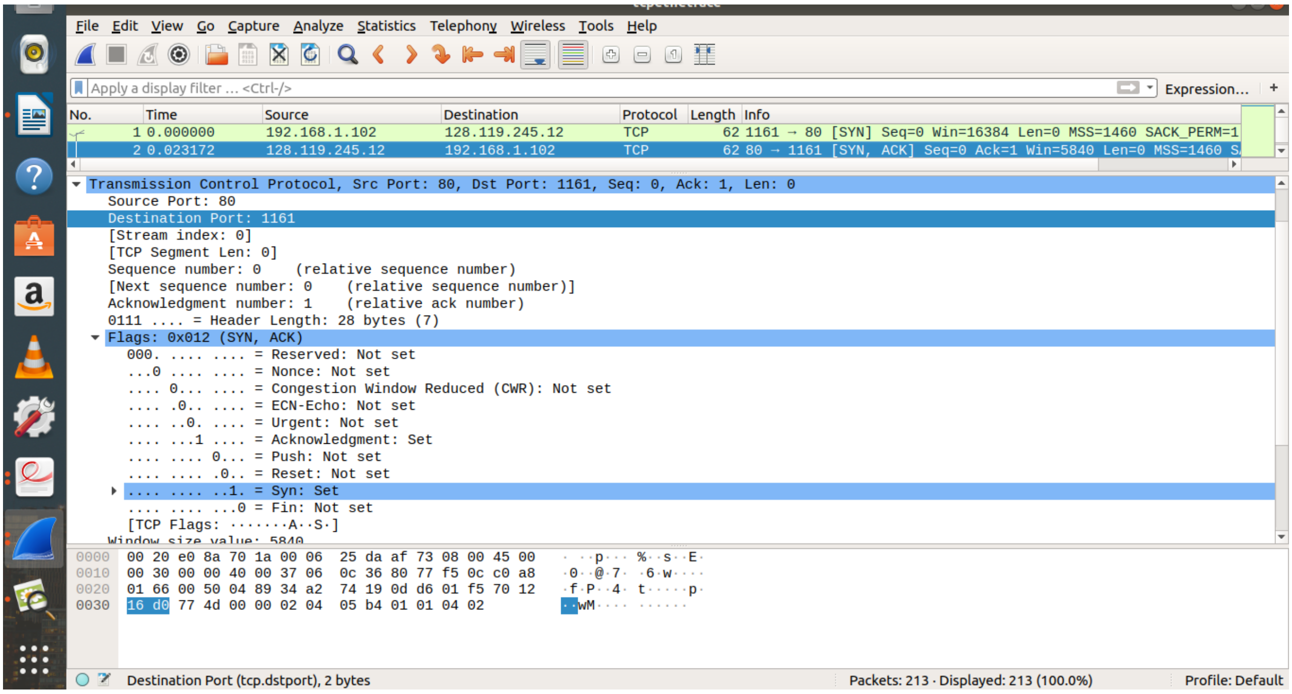
tcpethetrace
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…

```
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 S

▾ 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)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 0
    0111 .... = Header Length: 28 bytes (7)
  ▾ 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

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         @·······  ······

Frame (frame), 62 bytes               Packets: 213 · Displayed: 213 (100.0%)      Profile: Default
```

d. What is the sequence number of the SYNACK segment sent by ser1 to the client

computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did ser1 determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

Sol-> The sequence number of the SYNACK segment sent by ser1 to the client computer in reply to the SYN is 0.
The value of the acknowledgement field in the SYNACK segment is 1. The value of the ACKnowledgement field in the SYNACK segment is determined by the server ser1
The server adds 1 to the initial sequence number of SYN segment form the client computer. For this case, the initial sequence number of SYN segment from the client computer is 0, thus the value of the ACKnowledgement field in the SYNACK segment is 1.
A segment will be identified as a SYNACK segment if both SYN flag and Acknowledgement in the segment are set to 1.

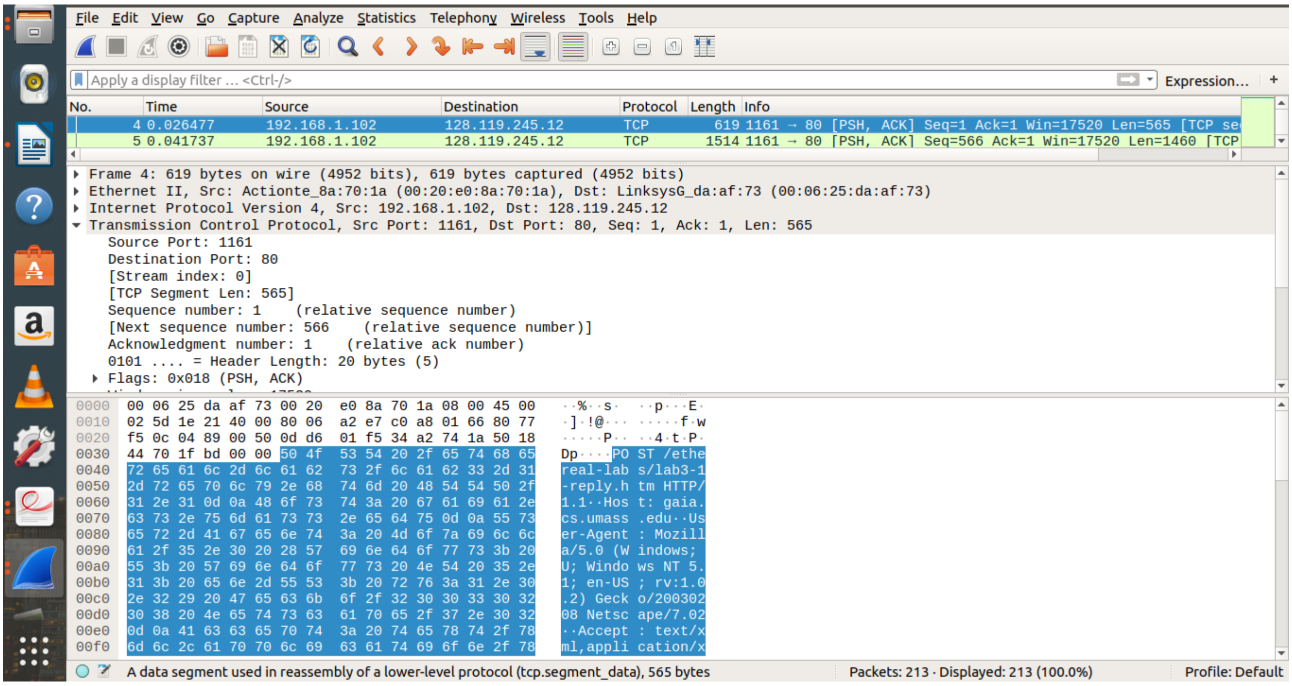


```
No.     Time        Source          Destination     Protocol Length Info
      1 0.000000    192.168.1.102   128.119.245.12  TCP          62 1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
      2 0.023172    128.119.245.12  192.168.1.102   TCP          62 80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 S

▾ 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)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    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 size value: 5840

0000  00 20 e0 8a 70 1a 00 06  25 da af 73 08 00 45 00   · ··p··· %··s··E·
0010  00 30 00 00 40 00 37 06  0c 36 80 77 f5 0c c0 a8   ·0··@·7· ·6·w····
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···· ······
```

Destination Port (tcp.dstport), 2 bytes   Packets: 213 · Displayed: 213 (100.0%)   Profile: Default

e. 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.

Sol-> The segment No. 4 contains the HTTP POST command, the sequence number of this segment is 1.



```
No.    Time        Source          Destination     Protocol  Length Info
     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 [TCP se
     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 [TCP
```

```
▸ Frame 4: 619 bytes on wire (4952 bits), 619 bytes captured (4952 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
▾ 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)
    [Next sequence number: 566    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x018 (PSH, ACK)
```

```
0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ··%··s·  ··p···E·
0010  02 5d 1e 21 40 00 80 06  a2 e7 c0 a8 01 66 80 77   ·]·!@···  ·····f·w
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.
00b0  31 3b 20 65 6e 2d 55 53  3b 20 72 76 3a 31 2e 30   1; en-US ; rv:1.0
00c0  2e 32 29 20 47 65 63 6b  6f 2f 32 30 30 33 30 32   .2) Geck o/200302
00d0  30 38 20 4e 65 74 73 63  61 70 65 2f 37 2e 30 32   08 Netsc ape/7.02
00e0  0d 0a 41 63 63 65 70 74  3a 20 74 65 78 74 2f 78   ··Accept : text/x
00f0  6d 6c 2c 61 70 70 6c 69  63 61 74 69 6f 6e 2f 78   ml,appli cation/x
```

A data segment used in reassembly of a lower-level protocol (tcp.segment_data), 565 bytes

Packets: 213 · Displayed: 213 (100.0%)

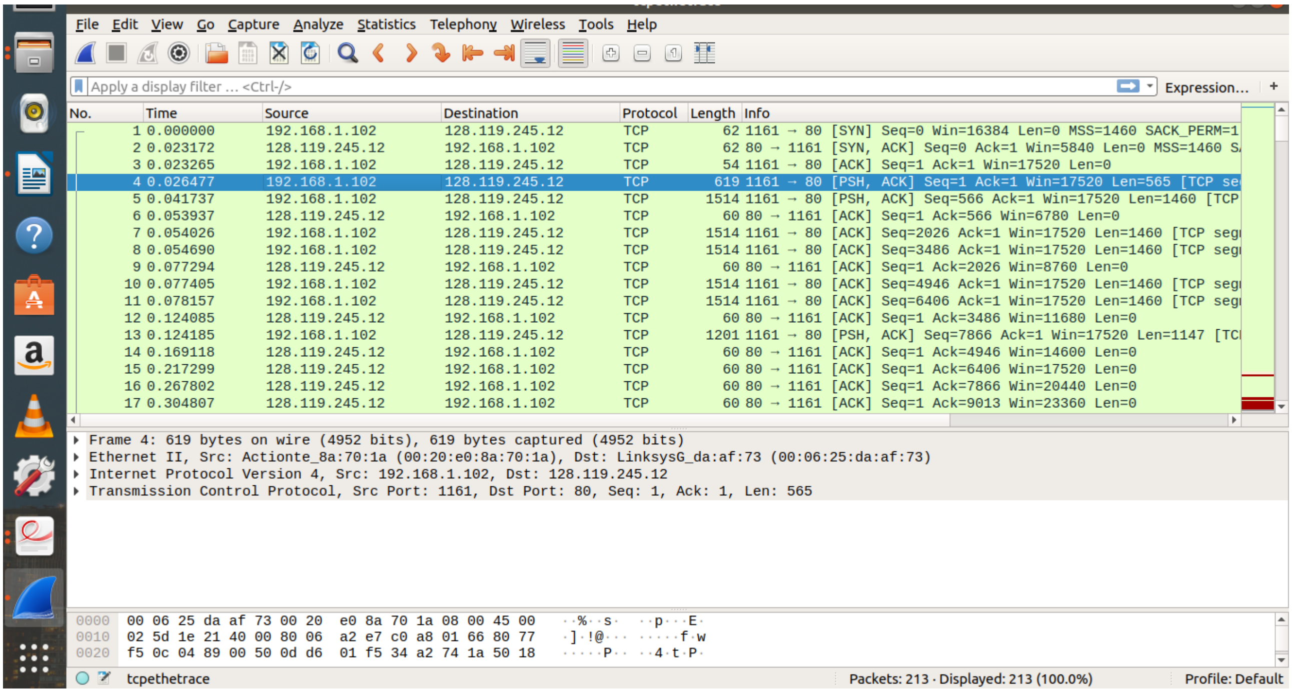
Profile: Default

f. 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 Round Trip Time (RTT) value for each of the six segments? What is the Estimated RTT value after the receipt of each ACK? Assume that the value of the Estimated RTT is equal to the measured RTT for the first segment, and then is computed using the following Estimated RTT equation for all subsequent segments.

Estimated RTT = (1 – α) * Estimated RTT + α * SampleRTT

where, the new value of Estimated RTT is a weighted combination of the previous value of Estimated RTT and the new value for SampleRTT. The recommended value of α = 0.125.

Sol->


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…

```
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 S
    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 [TCP se
    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 [TCP
    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 [TCP seg
    8 0.054690   192.168.1.102     128.119.245.12    TCP       1514 1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP seg
    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 [TCP seg
   11 0.078157   192.168.1.102     128.119.245.12    TCP       1514 1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460 [TCP seg
   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 [TC
   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

▸ Frame 4: 619 bytes on wire (4952 bits), 619 bytes captured (4952 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
▸ Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 1, Ack: 1, Len: 565

0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ··%··s·  ··p···E·
0010  02 5d 1e 21 40 00 80 06  a2 e7 c0 a8 01 66 80 77   ·]·!@···  ·····f·w
0020  f5 0c 04 89 00 50 0d d6  01 f5 34 a2 74 1a 50 18   ·····P··  ··4·t·P·

tcpethetrace          Packets: 213 · Displayed: 213 (100.0%)          Profile: Default
```

According to above figures, the segments 1-6 are No. 4, 5, 7, 8, 10 and 11. The ACK of segments 1-6 are No. 6, 9, 12, 14, 15 and 16.

Segment 1 sequence number is 1
Segment 2 sequence number is 566
Segment 3 sequence number is 2026
Segment 4 sequence number is 3486
Segment 5 sequence number is 4946
Segment 6 sequence number is 6406

	Sent time	**ACK received time**	**RTT**
Segment 1	0.026477	0.053937	0.02746
Segment 2	0.041737	0.077294	0.035557
Segment 3	0.054026	0.124085	0.070059
Segment 4	0.054690	0.169118	0.11443
Segment 5	0.077405	0.217299	0.13989
Segment 6	0.078157	0.267802	0.18964

EstimatedRTT = 0.875 * EstimatedRTT + 0.125 * SampleRTT

EstimatedRTT after the receipt of the ACK of segment 1:
EstimatedRTT = RTT for Segment 1 = 0.02746 s

EstimatedRTT after the receipt of the ACK of segment 2:
EstimatedRTT = 0.875 * 0.02746 + 0.125 * 0.035557 = 0.0285 s

EstimatedRTT after the receipt of the ACK of segment 3:

EstimatedRTT = 0.875 * 0.0285 + 0.125 * 0.070059 = 0.0337 s

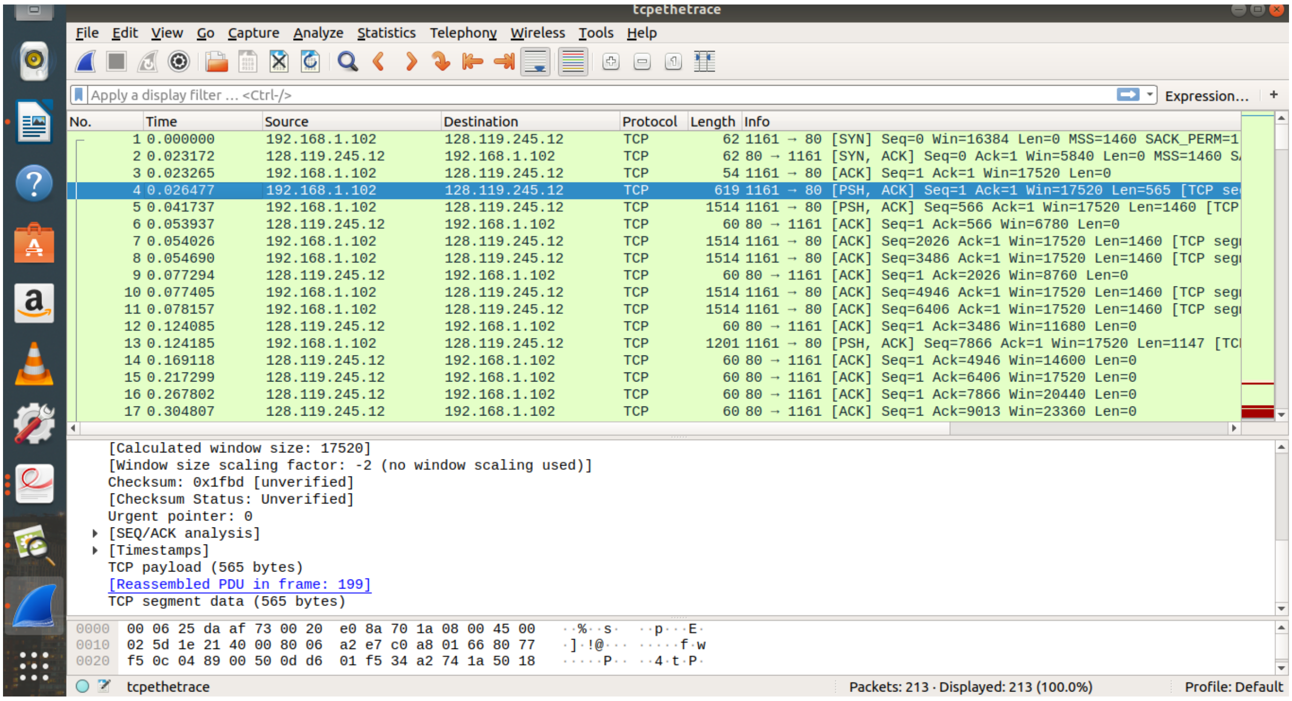
EstimatedRTT after the receipt of the ACK of segment 4:
EstimatedRTT = 0.875 * 0.0337+ 0.125 * 0.11443 = 0.0438 s

EstimatedRTT after the receipt of the ACK of segment 5:
EstimatedRTT = 0.875 * 0.0438 + 0.125 * 0.13989 = 0.0558 s

EstimatedRTT after the receipt of the ACK of segment 6:
EstimatedRTT = 0.875 * 0.0558 + 0.125 * 0.18964 = 0.0725 s

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

Length of the first TCP segment (containing the HTTP POST): 565 bytes
Length of each of the other five TCP segments: 1460 bytes


tcpethetrace
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

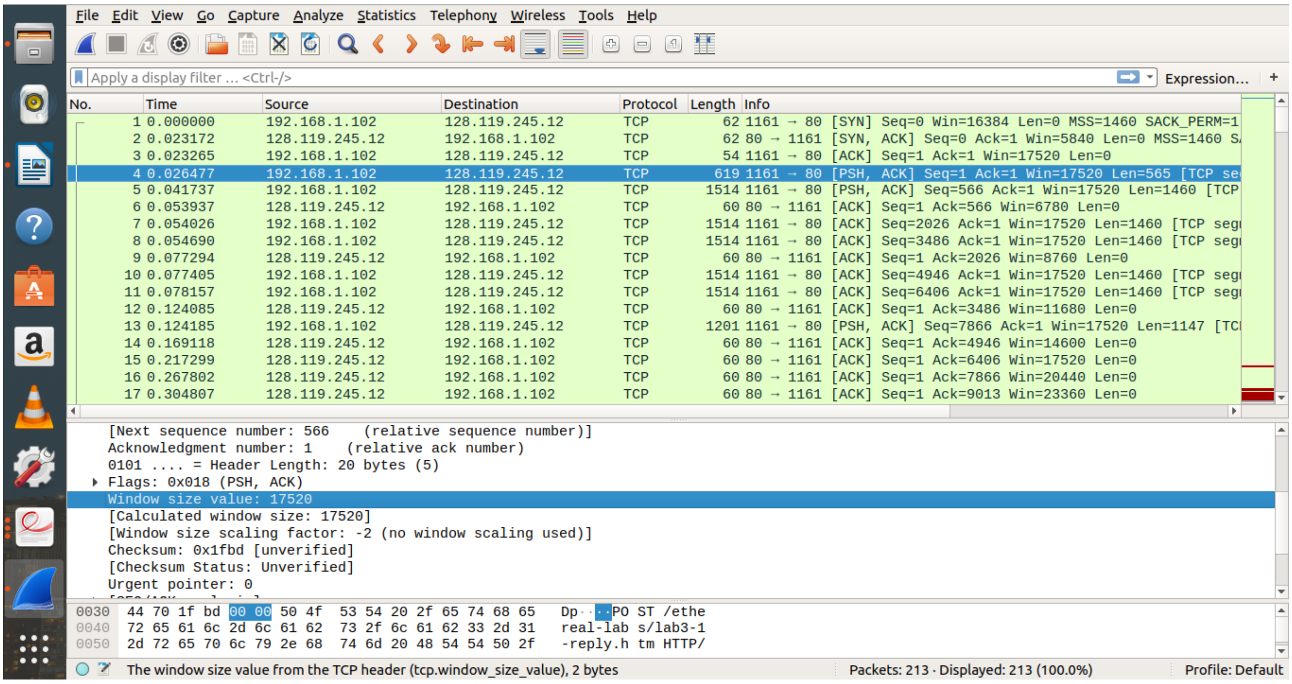
```
No.  Time       Source          Destination     Protocol Length Info
   1 0.000000   192.168.1.102   128.119.245.12  TCP        62 1161 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
   2 0.023172   128.119.245.12  192.168.1.102   TCP        62 80 → 1161 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 S
   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 [TCP se
   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 [TCP
   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 [TCP seg
   8 0.054690   192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP seg
   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 [TCP seg
  11 0.078157   192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460 [TCP seg
  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 [TC
  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
```

```
    [Calculated window size: 17520]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x1fbd [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ [SEQ/ACK analysis]
  ▸ [Timestamps]
    TCP payload (565 bytes)
    [Reassembled PDU in frame: 199]
    TCP segment data (565 bytes)
```

```
0000  00 06 25 da af 73 00 20  e0 8a 70 1a 08 00 45 00   ··%··s·  ··p···E·
0010  02 5d 1e 21 40 00 80 06  a2 e7 c0 a8 01 66 80 77   ·]·!@···  ·····f·w
0020  f5 0c 04 89 00 50 0d d6  01 f5 34 a2 74 1a 50 18   ·····P··  ··4·t·P·
```

h. 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 buffer space (receiver window) advertised at
ser1 for the entire trace is 17520 bytes, which shows in the first acknowledgement from the server. This receiver window grows steadily until a maximum receiver buffer size of 62780 bytes. The sender is never throttled due to lacking of receiver buffer space by inspecting this trace.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

```
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 S
   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 [TCP se
   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 [TCP
   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 [TCP seg
   8 0.054690  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=3486 Ack=1 Win=17520 Len=1460 [TCP seg
   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 [TCP seg
  11 0.078157  192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=6406 Ack=1 Win=17520 Len=1460 [TCP seg
  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 [TC
  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
```

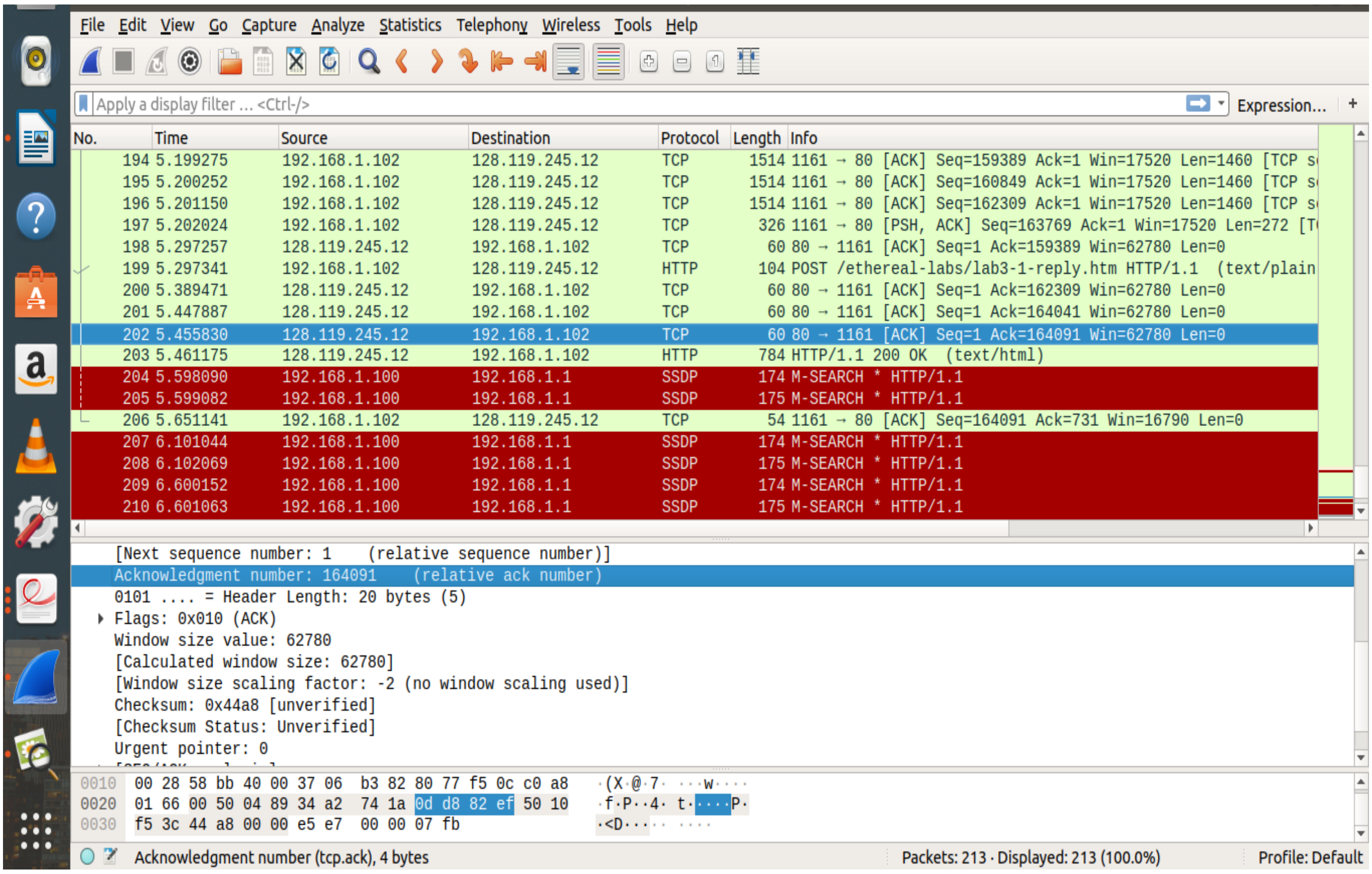
```
    [Next sequence number: 566    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x018 (PSH, ACK)
    Window size value: 17520
    [Calculated window size: 17520]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x1fbd [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
```

```
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/
```

The window size value from the TCP header (tcp.window_size_value), 2 bytes   Packets: 213 · Displayed: 213 (100.0%)   Profile: Default

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

The computation of TCP throughput largely depends on the selection of averaging time period. As a common throughput computation, in this question, we select the average time period as the whole connection time. Then, the average throughput for this TCP connection is computed as the ratio between the total amount data and the total transmission time. The total amount data transmitted can be computed by the difference between the sequence number of the first TCP segment (i.e. 1 byte for No. 4 segment) and the acknowledged sequence number of the last ACK (164091 bytes for No. 202 segment). Therefore, the total data are 164091 - 1 = 164090 bytes. The whole transmission time is the difference of the time instant of the first TCP segment (i.e., 0.026477 second for No.4 segment) and the time instant of the last ACK (i.e., 5.455830 second for No. 202 segment). Therefore, the total transmission time is 5.455830 - 0.026477 = 5.4294 seconds. Hence, the throughput for the TCP connection is computed as 164090/5.4294 = 30.222 Kbyte/sec



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

```
No.  Time        Source          Destination     Protocol Length Info
 194 5.199275    192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=159389 Ack=1 Win=17520 Len=1460 [TCP s
 195 5.200252    192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=160849 Ack=1 Win=17520 Len=1460 [TCP s
 196 5.201150    192.168.1.102   128.119.245.12  TCP      1514 1161 → 80 [ACK] Seq=162309 Ack=1 Win=17520 Len=1460 [TCP s
 197 5.202024    192.168.1.102   128.119.245.12  TCP       326 1161 → 80 [PSH, ACK] Seq=163769 Ack=1 Win=17520 Len=272 [T
 198 5.297257    128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=159389 Win=62780 Len=0
 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
 200 5.389471    128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=162309 Win=62780 Len=0
 201 5.447887    128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=164041 Win=62780 Len=0
 202 5.455830    128.119.245.12  192.168.1.102   TCP        60 80 → 1161 [ACK] Seq=1 Ack=164091 Win=62780 Len=0
 203 5.461175    128.119.245.12  192.168.1.102   HTTP      784 HTTP/1.1 200 OK  (text/html)
 204 5.598090    192.168.1.100   192.168.1.1     SSDP      174 M-SEARCH * HTTP/1.1
 205 5.599082    192.168.1.100   192.168.1.1     SSDP      175 M-SEARCH * HTTP/1.1
 206 5.651141    192.168.1.102   128.119.245.12  TCP        54 1161 → 80 [ACK] Seq=164091 Ack=731 Win=16790 Len=0
 207 6.101044    192.168.1.100   192.168.1.1     SSDP      174 M-SEARCH * HTTP/1.1
 208 6.102069    192.168.1.100   192.168.1.1     SSDP      175 M-SEARCH * HTTP/1.1
 209 6.600152    192.168.1.100   192.168.1.1     SSDP      174 M-SEARCH * HTTP/1.1
 210 6.601063    192.168.1.100   192.168.1.1     SSDP      175 M-SEARCH * HTTP/1.1
```

```
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 164091    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x010 (ACK)
    Window size value: 62780
    [Calculated window size: 62780]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x44a8 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
```

```
0010  00 28 58 bb 40 00 37 06  b3 82 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 10   ·f·P··4· t·····P·
0030  f5 3c 44 a8 00 00 e5 e7  00 00 07 fb               ·<D····· ····
```

Acknowledgment number (tcp.ack), 4 bytes   Packets: 213 · Displayed: 213 (100.0%)   Profile: Default