

**Step 1. Capture a trace**

- 1) Find a URL, I am using this one, <http://conferences.sigcomm.org/sigcomm/2011/papers/sigcomm/p14.pdf>, Which size is about 900KB.
- 2) Fetch the URL with wget command.

```

➔ ~ wget http://conferences.sigcomm.org/sigcomm/2011/papers/sigcomm/p14.pdf
--2019-10-25 09:30:22-- http://conferences.sigcomm.org/sigcomm/2011/papers/sigcomm/p14.pdf
Resolving conferences.sigcomm.org (conferences.sigcomm.org)... 162.249.4.107
Connecting to conferences.sigcomm.org (conferences.sigcomm.org)|162.249.4.107|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 964684 (942K) [application/pdf]
Saving to: 'p14.pdf'

p14.pdf          100%[=====>] 942.07K  1.36MB/s   in 0.7s

2019-10-25 09:30:24 (1.36 MB/s) - 'p14.pdf' saved [964684/964684]

```

- 3) Set up the filter to be 'tcp and host conferences.sigcomm.org', then repeat the wget command in 2) step.

The image shows a Wireshark packet capture of a TCP SYN packet. The packet list shows a packet from 10.120.19.73 to 162.249.4.107 on port 80. The packet details show the TCP header with sequence number 0, window size 65535, and flags SYN. The packet bytes are shown in hexadecimal and ASCII.

**Step 2 & 3. Inspect the Trace and TCP Segment Structure**

Expand a segment of trace, I find out the detailed structure of a tcp header, it looks like this:

Source port	Dest Port	Sequence Number	Ack Number	Header Length + Flags	Window size	Checksum	Urgent pointer	options	payloads
2 bytes	2 bytes	4 bytes	4 bytes	2 bytes	2 bytes	2 bytes	2 bytes	12 bytes	1424 bytes

Apply a display filter ... <filter>

No.	Time	Source	Destination	Protocol	Length	Info
7	0.129851	162.249.4.107	10.120.19.73	TCP	66	(TCP Dup ACK 6#1) 80 → 63211 [ACK] Seq=1 Ack=189 Win=66912 Len=0 TSval=3523
8	0.637636	162.249.4.107	10.120.19.73	TCP	1490	80 → 63211 [ACK] Seq=1 Ack=189 Win=66912 Len=1424 TSval=3523789507 TSecr=628
9	0.637643	162.249.4.107	10.120.19.73	TCP	1490	80 → 63211 [ACK] Seq=1425 Ack=189 Win=66912 Len=1424 TSval=3523789507 TSecr=
10	0.637742	10.120.19.73	162.249.4.107	TCP	66	63211 → 80 [ACK] Seq=189 Ack=2849 Win=129536 Len=0 TSval=628297730 TSecr=352378950

Transmission Control Protocol, Src Port: 80, Dst Port: 63211, Seq: 1, Ack: 189, Len: 1424

Source Port: 80  
Destination Port: 63211  
[Stream index: 0]  
[TCP Segment Len: 1424]  
Sequence number: 1 (relative sequence number)  
[Next sequence number: 1425 (relative sequence number)]  
Acknowledgment number: 189 (relative ack number)  
1000 .... = Header Length: 32 bytes (8)  
Flags: 0x010 (ACK)  
Window size value: 2091  
[Calculated window size: 66912]  
[Window size scaling factor: 32]  
Checksum: 0x80a6 [unverified]  
[Checksum Status: Unverified]  
Urgent pointer: 0  
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps  
TCP Option - No-Operation (NOP)  
TCP Option - No-Operation (NOP)  
TCP Option - Timestamps: TSval 3523789507, TSecr 628297204  
Kind: Time Stamp Option (8)  
Length: 10  
Timestamp value: 3523789507  
Timestamp echo reply: 628297204  
[SEQ/ACK analysis]  
[Timestamps]  
TCP payload (1424 bytes)  
TCP segment data (1424 bytes)

0020 13 49 00 50 f6 eb 54 6e aa 43 84 da 9e bb 80 10 .I.P..Tn..C.....  
0030 08 2b 80 a6 00 00 01 01 08 0a d2 08 c2 c3 25 73 +.....+.....%s  
0040 0d f4 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f .HTTP/1.1 200 0  
0050 4b 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b K..Conne ction: K  
0060 65 65 70 2d 41 6c 69 76 65 0d 0a 43 6f 6e 74 65 eep-Alive..Conte  
0070 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 61 nt-Type: applica  
0080 74 69 6f 6e 2f 70 64 66 0d 0a 4c 61 73 74 2d 4d tion/pdf..Last-M  
0090 6f 64 69 66 69 65 64 3a 20 54 75 65 2c 20 30 32 odified: Tue, 02  
00a0 20 41 75 67 20 32 30 31 31 20 30 32 3a 34 39 3a Aug 201 1 02:49:  
00b0 32 33 20 47 4d 54 0d 0a 45 74 61 67 3a 20 22 65 23 GMT- Etag: "e  
00c0 62 38 34 63 2d 34 65 33 37 36 35 62 33 2d 33 38 b84c-4e3 765b3-38

Transmission Control Protocol (tcp), 32 bytes

Packets: 1234 · Displayed: 1234 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

## Step 4. TCP Connection Setup and Teardown

### 1. Filter the syn packets with filter 'tcp.flags.syn==1'

tcp.flags.syn==1

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.120.19.73	162.249.4.107	TCP	78	63211 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=628297804 TSecr=0 SACK
2	0.020171	162.249.4.107	10.120.19.73	TCP	74	80 → 63211 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1436 WS=32 SACK_PERM=1 TSval

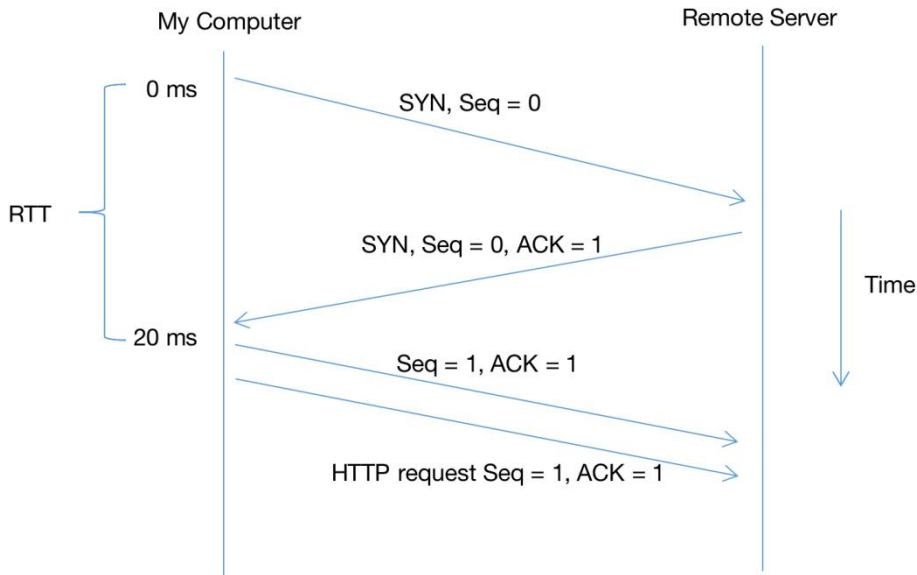
Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0  
Ethernet II, Src: Apple\_85:d7:85 (04:83:e7:85:d7:85), Dst: Cisco\_9f:f3:3f (08:00:0c:9f:f3:3f)  
Internet Protocol Version 4, Src: 10.120.19.73, Dst: 162.249.4.107  
Transmission Control Protocol, Src Port: 63211, Dst Port: 80, Seq: 0, Len: 0  
Source Port: 63211  
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  
1011 .... = Header Length: 44 bytes (11)  
Flags: 0x002 (SYN)  
0000 .... = Reserved: Not set  
...0 .... = Nonce: Not set  
...0 .... = Congestion Window Reduced (CWR): Not set  
...0 .... = ECH-Echo: Not set  
...0 .... = Urgent: Not set  
...0 .... = Acknowledgment: Not set  
...0 .... = Push: Not set  
...0 .... = Reset: Not set  
...0 .... = Syn: Set  
...0 .... = Fin: Not set  
[TCP Flags: .....S.]

0000 00 00 0c 9f f3 3f a4 83 e7 05 d7 85 08 00 45 00 .....?.....E  
0010 00 40 00 00 40 00 00 75 93 0a 78 13 49 a2 f9 @ @ @ u..x.I  
0020 04 6b f6 eb 00 50 84 da 9d fe 00 00 00 b0 02 k..P.....  
0030 ff ff 24 c9 00 00 02 04 05 b4 01 03 03 06 01 01 \$.....  
0040 00 0a 25 73 0d 06 00 00 00 04 02 00 00 .....\$

Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0  
Ethernet II, Src: Cisco\_9f:f3:3f (08:00:0c:9f:f3:3f), Dst: Apple\_85:d7:85 (04:83:e7:85:d7:85)  
Internet Protocol Version 4, Src: 162.249.4.107, Dst: 10.120.19.73  
Transmission Control Protocol, Src Port: 80, Dst Port: 63211, Seq: 0, Ack: 1, Len: 0  
Source Port: 80  
Destination Port: 63211  
[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)  
1010 .... = Header Length: 40 bytes (10)  
Flags: 0x012 (SYN, ACK)  
0000 .... = Reserved: Not set  
...0 .... = Nonce: Not set  
...0 .... = Congestion Window Reduced (CWR): Not set  
...0 .... = ECH-Echo: Not set  
...0 .... = Urgent: Not set  
...0 .... = Acknowledgment: Set  
...0 .... = Push: Not set  
...0 .... = Reset: Not set  
...0 .... = Syn: Set  
...0 .... = Fin: Not set  
[TCP Flags: .....A.S.]

0000 04 83 e7 05 d7 85 04 c5 a0 ea c7 42 00 00 45 00 .....@..E  
0010 00 3c 31 9d 40 00 3e 06 45 fa a2 f9 04 0b 0a 78 <1 @> ..E...k.x  
0020 13 49 00 50 f6 eb 54 6e aa 42 84 da 9d ff aa 32 .I.P..Tn..B.....  
0030 ff ff a2 9d 00 00 02 04 05 9c 01 03 03 05 04 02 .....\$  
0040 00 0a d2 08 c2 7e 25 73 0d 06 .....

2. Draw a time sequence diagram for the three-way handshake.



### Step 5. Connection Options

1. What TCP Options are carried on the SYN packets for your trace?

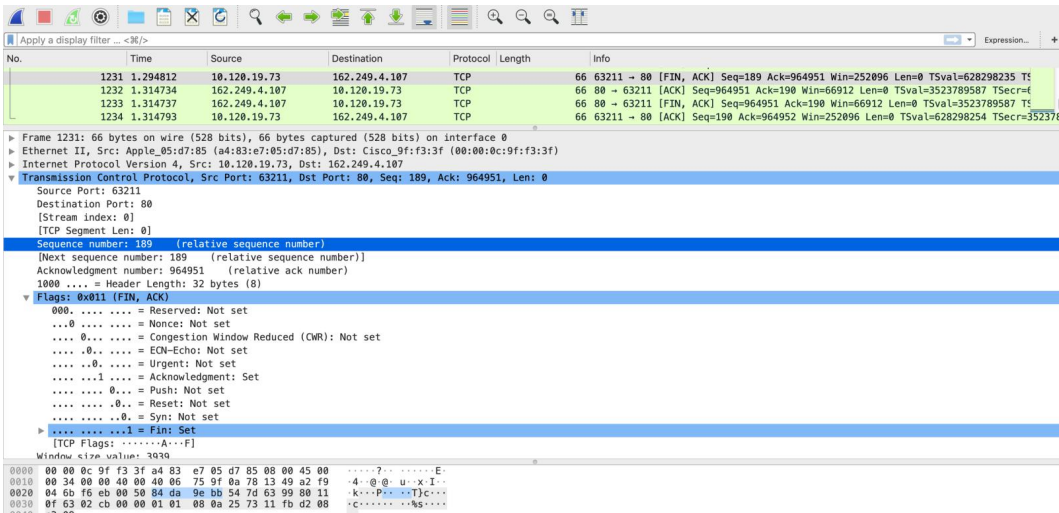
The tcp options are Maximum segment size, No-Operation(NOP), Window scale, No-Operation(NOP), Timestamps, SACK permitted, End of Option List(EOL).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.120.19.73	162.249.4.107	TCP	78	63211 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=628297094 TSecr=
2	0.020171	162.249.4.107	10.120.19.73	TCP	74	80 → 63211 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1436 WS=32 SACK_PERM=1
3	0.020266	10.120.19.73	162.249.4.107	TCP	66	63211 → 80 [ACK] Seq=1 Ack=1 Win=132416 Len=0 TSval=628297114 TSecr=35237894
4	0.020481	10.120.19.73	162.249.4.107	HTTP	254	GET /sigcomm/2011/papers/sigcomm/p14.pdf HTTP/1.1
5	0.110474	10.120.19.73	162.249.4.107	TCP	254	[TCP Retransmission] 63211 → 80 [PSH, ACK] Seq=1 Ack=1 Win=132416 Len=188 TS
6	0.118615	162.249.4.107	10.120.19.73	TCP	66	80 → 63211 [ACK] Seq=1 Ack=189 Win=66912 Len=0 TSval=3523789450 TSecr=628297

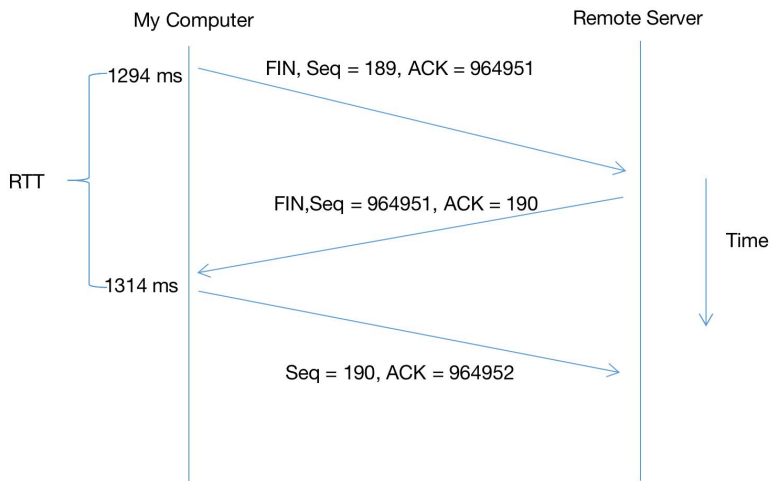
▶ Ethernet II, Src: Apple\_05:d7:85 (a4:83:e7:05:d7:85), Dst: Cisco\_9f:f3:3f (00:00:0c:9f:f3:3f)  
 ▶ Internet Protocol Version 4, Src: 10.120.19.73, Dst: 162.249.4.107  
 ▼ Transmission Control Protocol, Src Port: 63211, Dst Port: 80, Seq: 0, Len: 0  
   Source Port: 63211  
   Destination Port: 80  
   [Stream index: 0]  
   [TCP Segment Len: 0]  
   Sequence number: 0 (relative sequence number)  
   [Next sequence number: 0 (relative sequence number)]  
   Acknowledgment number: 0  
   1011 .... = Header Length: 44 bytes (11)  
   ▶ Flags: 0x002 (SYN)  
     Window size value: 65535  
     [Calculated window size: 65535]  
     Checksum: 0x24c9 [unverified]  
     [Checksum Status: Unverified]  
     Urgent pointer: 0  
   ▼ Options: (24 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), Timestamps, SACK permitted, End of Option List (EOL)  
     ▶ TCP Option - Maximum segment size: 1460 bytes  
     ▶ TCP Option - No-Operation (NOP)  
     ▶ TCP Option - Window scale: 6 (multiply by 64)  
     ▶ TCP Option - No-Operation (NOP)  
     ▶ TCP Option - No-Operation (NOP)  
     ▼ TCP Option - Timestamps: TSval 628297094, TSecr 0  
       Kind: Time Stamp Option (8)  
       Length: 10  
       Timestamp value: 628297094  
       Timestamp echo reply: 0  
     ▶ TCP Option - SACK permitted  
     ▶ TCP Option - End of Option List (EOL)

### Step 6. FIN/RST Tear down

1. Check the FIN packets

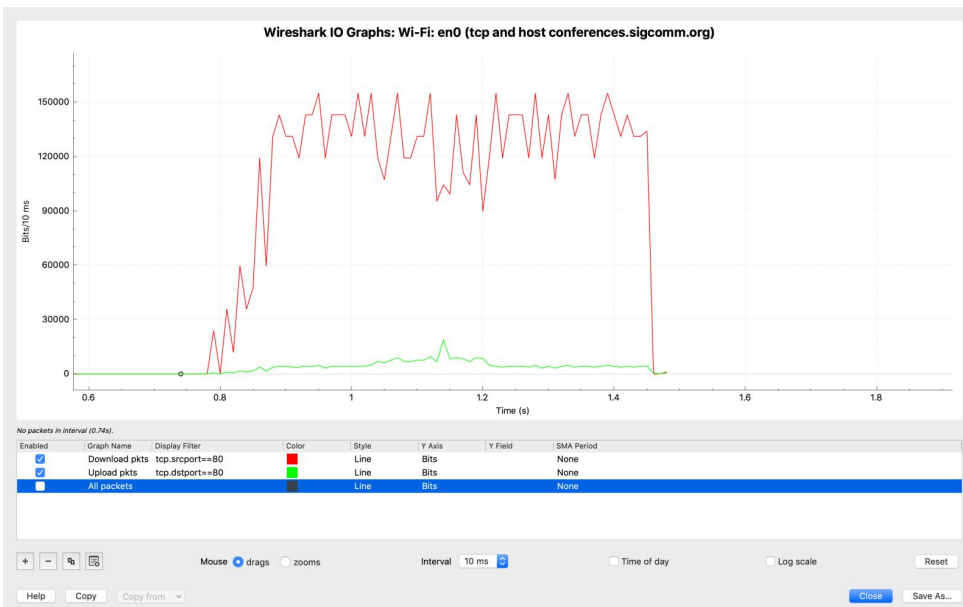


2. Draw a diagram for the tear down.



## Step 7. TCP Data Transfer

1. TCP Stream Graph.



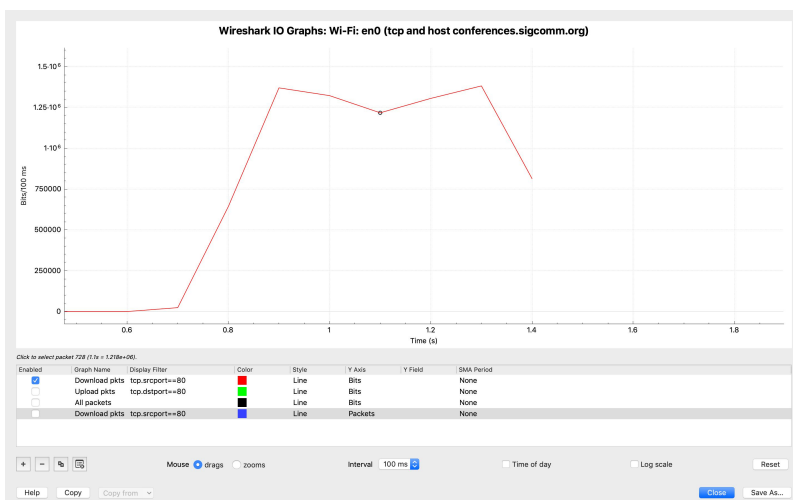
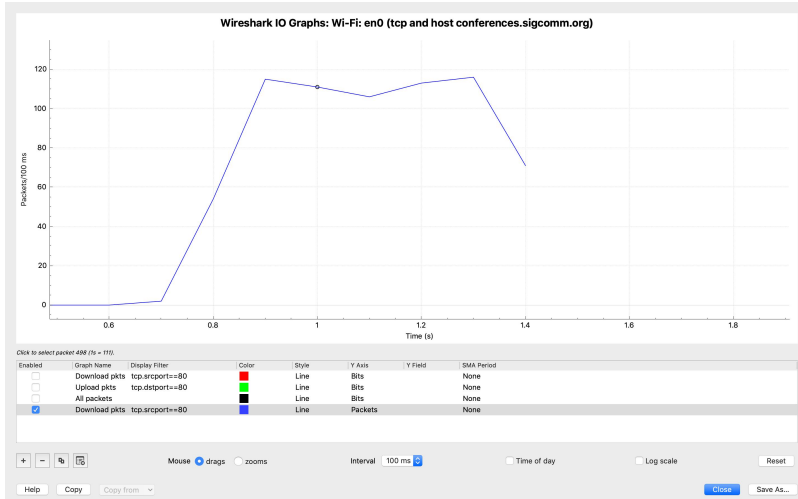


## 2. Answer the following questions to show your understanding of the data transfer:

- 1) What is the rough data rate in the download direction in packets/second and bits/second once the TCP connection is running well?

Download rate in packets/s is around  $100 \text{ (pkts/100ms)} * 10 = 1000 \text{ pkts.}$

in bits/s is around  $1.25 * 10^6 \text{ (bits/100ms)} * 10 = 12.5 * 10^6 \text{ bits}$



- 2) What percentage of this download rate is content?

The packet is 1490 bytes and payload is 1424 bytes, thus the content percentage is  $1424 / 1490 = 95\%$ .

No.	Time	Source	Destination	Protocol	Length	Info
14	0.819132	162.249.4.107	10.120.19.73	TCP	1490	80 → 64189 [ACK] Seq=5697 Ack=189 Win=66912 Len=1424 TSval=1922858773 TSecr=66 64189 → 80 [ACK] Seq=7121 Win=129600 Len=8 TSval=636616104 TSecr=1922858773
15	0.819284	10.120.19.73	162.249.4.107	TCP	66	64189 → 80 [ACK] Seq=7121 Win=129600 Len=8 TSval=636616104 TSecr=1922858773

Frame 14: 1490 bytes on wire (11920 bits), 1490 bytes captured (11920 bits) on interface 0  
 Ethernet II, Src: Cisco\_ea:c7:42 (04:c5:a4:ea:c7:42), Dst: Apple\_05:d7:85 (04:83:e7:05:d7:85)  
 Internet Protocol Version 4, Src: 162.249.4.107, Dst: 10.120.19.73  
 Transmission Control Protocol, Src Port: 80, Dst Port: 64189, Seq: 5697, Ack: 189, Len: 1424

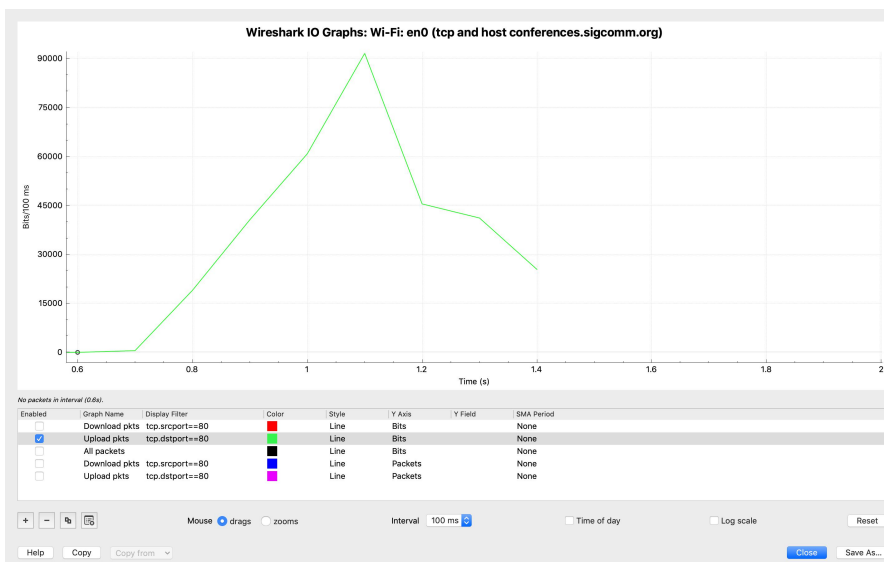
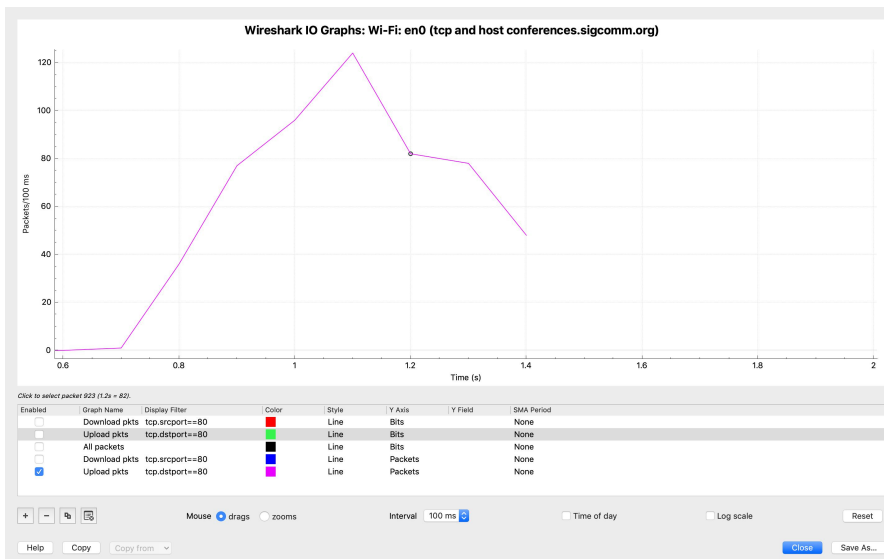
Source Port: 80  
 Destination Port: 64189  
 [Stream index: 0]  
 [TCP Segment Len: 1424]  
 Sequence number: 5697 (relative sequence number)  
 [Next sequence number: 7121 (relative sequence number)]  
 Acknowledgment number: 189 (relative ack number)  
 1000 .... = Header Length: 32 bytes (8)  
 Flags: 0x010 (ACK)  
 Window size value: 2091  
 [Calculated window size: 66912]  
 [Window size scaling factor: 32]  
 Checksum: 0x46ed [unverified]  
 [Checksum Status: Unverified]  
 Urgent pointer: 0  
 Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps  
 [SEQ/ACK analysis]  
 [Timestamps]

TCP payload (1424 bytes)  
 TCP segment data (1424 bytes)

- 3) What is the rough data rate in the upload direction in packets/second and bits/second due to the ACK packets?

Download rate in packets/s is around  $85 \text{ (pkts/100ms)} * 10 = 850 \text{ pkts.}$

in bits/s is around  $0.06 * 10^6 \text{ (bits/100ms)} * 10 = 0.6 * 10^6 \text{ bits}$



- 4) If the most recently received TCP segment from the server has a sequence number of X, then what ACK number does the next transmitted TCP segment carry?

As is shown below, the segment from the server has seq num 239233, and the next transmitted segment has an ACK of 240657, we could see that  $240657 - 239233 = 1424$ , which is the payload bytes number. Thus if the seq num is X, then the next transmitted ACK will be X plus the payload bytes.

No.	Time	Source	Destination	Protocol	Length	Info
287	0.997436	162.249.4.107	10.120.19.73	TCP	1490	80 → 64189 [ACK] Seq=237809 Ack=189 Win=66912 Len=1424 TSval=1922858788 TSecr=1922858788
288	0.998458	162.249.4.107	10.120.19.73	TCP	1490	80 → 64189 [ACK] Seq=239233 Ack=189 Win=66912 Len=1424 TSval=1922858788 TSecr=1922858788
289	0.998480	10.120.19.73	162.249.4.107	TCP	66	64189 → 80 [ACK] Seq=189 Ack=240657 Win=162368 Len=0 TSval=636616246 TSecr=1922858788

Frame 288: 1490 bytes on wire (11920 bits), 1490 bytes captured (11920 bits) on interface 0

Ethernet II, Src: Cisco\_ea:c7:42 (04:c5:a4:ea:c7:42), Dst: Apple\_05:d7:85 (a4:83:e7:05:d7:85)

Internet Protocol Version 4, Src: 162.249.4.107, Dst: 10.120.19.73

Transmission Control Protocol, Src Port: 80, Dst Port: 64189, Seq: 239233, Ack: 189, Len: 1424

Source Port: 80

Destination Port: 64189

[Stream index: 0]

[TCP Segment Len: 1424]

Sequence number: 239233 (relative sequence number)

[Next sequence number: 240657 (relative sequence number)]

Acknowledgment number: 189 (relative ack number)

## Lab 4 – Yuanjie Yue 10/30/2019

Apply a display filter ...							Expression...	
No.	Time	Source	Destination	Protocol	Length	Info		
287	0.997436	162.1	10.120.19.73	TCP	1490	80 → 64189 [ACK] Seq=237809 Ack=189 Win=66912 Len=1424 TSval=1922858788 TSecr=1922858788		
288	0.998458	162.1	10.120.19.73	TCP	1490	80 → 64189 [ACK] Seq=239233 Ack=189 Win=66912 Len=1424 TSval=1922858788 TSecr=1922858788		
289	0.998480	10.1	162.249.4.107	TCP	66	64189 → 80 [ACK] Seq=189 Ack=240657 Win=162368 Len=0 TSval=636616246 TSecr=1922858788		
▶ Frame 289: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0								
▶ Ethernet II, Src: Apple 08:00:0e:00:00:00, Dst: Cisco 9f:f3:3f (00:00:0c:9f:f3:3f)								
▶ Internet Protocol Version 4, Src: 10.120.19.73, Dst: 162.249.4.107								
▼ Transmission Control Protocol, Src Port: 64189, Dst Port: 80, Seq: 189, Ack: 240657, Len: 0								
Source Port: 64189								
Destination Port: 80								
[Stream index: 0]								
[TCP Segment Len: 0]								
Sequence number: 189 (relative sequence number)								
[Next sequence number: 189 (relative sequence number)]								
Acknowledgment number: 240657 (relative ack number)								