

Author: Jeremy Vuong
Course: CSC 138-03
Professor: Jun Dai
Date: 03/05/2023

Wireshark Lab 2-TCP

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).
 - a. IP address: 10.0.0.96
 - b. TCP port number: 63955
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?
 - a. IP address of gaia.cs.umass.edu: 128.119.245.12
 - b. Port number: 80

```
No.    Time           Source            Destination       Protocol Length Info
63 01:40:49.190214 10.0.0.96         128.119.245.12   HTTP      3455   POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1
(text/plain)
Frame 63: 3455 bytes on wire (27640 bits), 3455 bytes captured (27640 bits) on interface \Device\NPF_{2748DDCA-
E1DE-4281-80C4-430F4323F5A7}, id 0
Ethernet II, Src: Giga-Byt_07:19:d9 (d8:5e:d3:07:19:d9), Dst: Technico_ac:2b:0c (dc:eb:69:ac:2b:0c)
Internet Protocol Version 4, Src: 10.0.0.96, Dst: 128.119.245.12
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
[Total Length: 3441 bytes (reported as 0, presumed to be because of "TCP segmentation offload" (TSO))]
Identification: 0x5a89 (23177)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to live: 128
Protocol: TCP (6)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.0.0.96
Destination Address: 128.119.245.12
Transmission Control Protocol, Src Port: 63955, Dst Port: 80, Seq: 149635, Ack: 1, Len: 3401
Source Port: 63955
Destination Port: 80
[Stream index: 3]
[Conversation completeness: Incomplete (12)]
[TCP Segment Len: 3401]
Sequence Number: 149635 (relative sequence number)
Sequence Number (raw): 3718610710
[Next Sequence Number: 153036 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 161514501
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 1026
[Calculated window size: 1026]
[Window size scaling factor: -1 (unknown)]
Checksum: 0x7fea [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
TCP payload (3401 bytes)
TCP segment data (3401 bytes)
[22 Reassembled TCP Segments (153035 bytes): #5(714), #6(13140), #14(1460), #16(2920), #18(2920), #20(14600), #22(5840), #32(2920),
#34(2920), #36(2920), #38(14600), #40(14600), #42(5840), #44(8760), #46(2920), #51(2920), #53(2920), #55(116)]
```

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?
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?
 - a. 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.
 - b. **Flags: 0x002 (SYN)** identifies the segment as a SYN segment.

```

No.      Time                Source            Destination      Protocol Length Info
 3 01:40:48.890721    10.0.0.96        128.119.245.12   TCP              66      63968 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
WS=256 SACK_PERM
Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{2748DDCA-E1DE-4281-80C4-430F4323F5A7}, id 0
Ethernet II, Src: Giga-Byt_07:19:d9 (d8:5e:d3:07:19:d9), Dst: Technico_ac:2b:0c (dc:eb:69:ac:2b:0c)
Internet Protocol Version 4, Src: 10.0.0.96, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 63968, Dst Port: 80, Seq: 0, Len: 0
  Source Port: 63968
  Destination Port: 80
  [Stream index: 1]
  [Conversation completeness: Incomplete, ESTABLISHED (7)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 871293057
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 0
  Acknowledgment number (raw): 0
  1000 .... = Header Length: 32 bytes (8)
  Flags: 0x002 (SYN)
  Window: 64240
  [Calculated window size: 64240]
  Checksum: 0x800a [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
  [Timestamps]

```

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?
 - a. The sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN is 0.
 - b. The value of the Acknowledgement field in the SYNACK segment is 1.
 - c. gaia.cs.umass.edu determines that value by adding 1 to the initial sequence number of the SYN segment from the client computer.
 - d. The **SYN flag** and the **Acknowledgement flag** being set to 1 identifies the segment as a SYNACK segment.

```

No.    Time           Source             Destination        Protocol Length Info
 7 01:40:48.967190  20.81.51.95       10.0.0.96         TCP                66      443 → 63969 [SYN, ACK] Seq=0 Ack=1 Win=65535
Len=0 MSS=1440 WS=256 SACK_PERM
Frame 7: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{2748DDCA-E1DE-4281-80C4-430F4323F5A7}, id 0
Ethernet II, Src: Technico_ac:2b:0c (dc:eb:69:ac:2b:0c), Dst: Giga-Byt_07:19:d9 (d8:5e:d3:07:19:d9)
Internet Protocol Version 4, Src: 20.81.51.95, Dst: 10.0.0.96
Transmission Control Protocol, Src Port: 443, Dst Port: 63969, Seq: 0, Ack: 1, Len: 0
  Source Port: 443
  Destination Port: 63969
  [Stream index: 2]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 2511713301
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 844849058
  1000 .... = Header Length: 32 bytes (8)
  Flags: 0x012 (SYN, ACK)
    000. .... = Reserved: Not set
    ...0 .... = Accurate ECN: Not set
    ....0... = Congestion Window Reduced: 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: 65535
  [Calculated window size: 65535]
  Checksum: 0x459f [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
  [Timestamps]
  [SEQ/ACK analysis]

```

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.

 - a. The sequence number of the TCP segment containing the HTTP POST command is **1**.

```

No.      Time          Source            Destination      Protocol Length Info
 5 01:40:48.892649  10.0.0.96        128.119.245.12  TCP             768      63955 → 80 [PSH, ACK] Seq=1 Ack=1 Win=1026
Len=714
Frame 5: 768 bytes on wire (6144 bits), 768 bytes captured (6144 bits) on interface \Device\NPF_{2748DDCA-E1DE-4281-80C4-430F4323F5A7},
id 0
Ethernet II, Src: Giga-Byt_07:19:d9 (d8:5e:d3:07:19:d9), Dst: Technico_ac:2b:0c (dc:eb:69:ac:2b:0c)
Internet Protocol Version 4, Src: 10.0.0.96, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 63955, Dst Port: 80, Seq: 1, Ack: 1, Len: 714
  Source Port: 63955
  Destination Port: 80
  [Stream index: 3]
  [Conversation completeness: Incomplete (12)]
  [TCP Segment Len: 714]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 3718461076
  [Next Sequence Number: 715 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 161514501
  0101 .... = Header Length: 20 bytes (5)
  Flags: 0x018 (PSH, ACK)
    000. .... = Reserved: Not set
    ...0 .... = Accurate ECN: Not set
    ....0... = Congestion Window Reduced: Not set
    ....0... = ECN-Echo: Not set
    ....0... = Urgent: Not set
    ....1... = Acknowledgment: Set
    ....1... = Push: Set
    ....0... = Reset: Not set
    ....0... = Syn: Not set
    ....0... = Fin: Not set
  [TCP Flags: .....AP...]
  Window: 1026
  [Calculated window size: 1026]
  [Window size scaling factor: -1 (unknown)]
  Checksum: 0x82c8 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  [Timestamps]
  [SEQ/ACK analysis]
  TCP payload (714 bytes)
Data (714 bytes)
0000  50 4f 53 54 20 2f 77 69 72 65 73 68 61 72 6b 2d  POST /wireshark-
0010  6c 61 62 73 2f 6c 61 62 33 2d 31 2d 72 65 70 6c  labs/lab3-1-repl
0020  79 2e 68 74 6d 20 48 54 50 2f 31 2e 31 0d 0a    y.htm HTTP/1.1..
0030  48 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d  Host: gaia.cs.um
0040  61 73 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74  ass.edu..Connect

```

Note: I needed to create a new trace for the following questions because I noticed that there were some missing packets that I needed in order to complete the following questions.

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 239 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 239 for all subsequent segments.

- a. The first six segments:
 - i. Packet 29, **sequence number: 1;**
Sent at 22:19:10.325873;
 - ii. Packet 34, **sequence number: 14601;**
Sent at 22:19:10.421928; received at 22:19:10.422037
RTT = 0.000109 seconds

- iii. Packet 36, **sequence number: 29201;**
Sent at 22:19:10.422042; received at 22:19:10.520643
RTT = 0.098601 seconds
- iv. Packet 40, **sequence number: 43801;**
Sent at 22:19:10.520654; received at 22:19:10.520911
RTT = 0.000257 seconds
- v. Packet 42, **sequence number: 58401;**
Sent at 22:19:10.520782; received at 22:19:10.615208
RTT = 0.094426 seconds
- vi. Packet 44, **sequence number: 73001;**
Sent at 22:19:10.520852; received at 22:19:10.615786
RTT = 0.094934seconds

No.	Time	Source	Destination	Protocol	Length	Info
10	22:19:09.510868	10.0.0.96	128.119.245.12	TCP	54	53698 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
29	22:19:10.325873	10.0.0.96	128.119.245.12	TCP	14654	53698 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=14600 [TCP segment of a reassembled PDU]
33	22:19:10.421916	128.119.245.12	10.0.0.96	TCP	60	80 → 53698 [ACK] Seq=1 Ack=7301 Win=43904 Len=0
34	22:19:10.421928	10.0.0.96	128.119.245.12	TCP	14654	53698 → 80 [ACK] Seq=14601 Ack=1 Win=262656 Len=14600 [TCP segment of a reassembled PDU]
35	22:19:10.422037	128.119.245.12	10.0.0.96	TCP	60	80 → 53698 [ACK] Seq=1 Ack=14601 Win=58496 Len=0
36	22:19:10.422042	10.0.0.96	128.119.245.12	TCP	14654	53698 → 80 [PSH, ACK] Seq=29201 Ack=1 Win=262656 Len=14600 [TCP segment of a reassembled PDU]
39	22:19:10.520643	128.119.245.12	10.0.0.96	TCP	60	80 → 53698 [ACK] Seq=1 Ack=21901 Win=73088 Len=0
40	22:19:10.520654	10.0.0.96	128.119.245.12	TCP	14654	53698 → 80 [ACK] Seq=43801 Ack=1 Win=262656 Len=14600 [TCP segment of a reassembled PDU]
41	22:19:10.520778	128.119.245.12	10.0.0.96	TCP	60	80 → 53698 [ACK] Seq=1 Ack=29201 Win=87680 Len=0
42	22:19:10.520782	10.0.0.96	128.119.245.12	TCP	14654	53698 → 80 [PSH, ACK] Seq=58401 Ack=1 Win=262656 Len=14600 [TCP segment of a reassembled PDU]
43	22:19:10.520849	128.119.245.12	10.0.0.96	TCP	60	80 → 53698 [ACK] Seq=1 Ack=36501 Win=102272 Len=0
44	22:19:10.520852	10.0.0.96	128.119.245.12	TCP	14654	53698 → 80 [ACK] Seq=73001 Ack=1 Win=262656 Len=14600 [TCP segment of a reassembled PDU]
45	22:19:10.520911	128.119.245.12	10.0.0.96	TCP	60	80 → 53698 [ACK] Seq=1 Ack=43801 Win=116864 Len=0
46	22:19:10.520914	10.0.0.96	128.119.245.12	TCP	14654	53698 → 80 [PSH, ACK] Seq=87601 Ack=1 Win=262656 Len=14600 [TCP segment of a reassembled PDU]
48	22:19:10.614998	128.119.245.12	10.0.0.96	TCP	60	80 → 53698 [ACK] Seq=1 Ack=51101 Win=131456 Len=0
49	22:19:10.615001	10.0.0.96	128.119.245.12	TCP	14654	53698 → 80 [ACK] Seq=102201 Ack=1 Win=262656 Len=14600 [TCP segment of a reassembled PDU]
50	22:19:10.615208	128.119.245.12	10.0.0.96	TCP	60	80 → 53698 [ACK] Seq=1 Ack=58401 Win=146048 Len=0
51	22:19:10.615212	10.0.0.96	128.119.245.12	TCP	14654	53698 → 80 [PSH, ACK] Seq=116801 Ack=1 Win=262656 Len=14600 [TCP segment of a reassembled PDU]
52	22:19:10.615394	128.119.245.12	10.0.0.96	TCP	60	80 → 53698 [ACK] Seq=1 Ack=65701 Win=160640 Len=0
53	22:19:10.615397	10.0.0.96	128.119.245.12	TCP	14654	53698 → 80 [ACK] Seq=131401 Ack=1 Win=262656 Len=14600 [TCP segment of a reassembled PDU]
54	22:19:10.615571	128.119.245.12	10.0.0.96	TCP	60	80 → 53698 [ACK] Seq=1 Ack=68621 Win=166528 Len=0
55	22:19:10.615574	10.0.0.96	128.119.245.12	TCP	5894	53698 → 80 [ACK] Seq=146001 Ack=1 Win=262656 Len=5840 [TCP segment of a reassembled PDU]
56	22:19:10.615786	128.119.245.12	10.0.0.96	TCP	60	80 → 53698 [ACK] Seq=1 Ack=73001 Win=175232 Len=0
57	22:19:10.615789	10.0.0.96	128.119.245.12	HTTP	1189	POST /wreshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)

> Frame 29: 14654 bytes on wire (117232 bits), 14654 bytes captured (117232 bits) on interface	0000	dc eb 69 ac 2b 0c d8 5e d3 07 19 d9 08 00 45 00	..i+...^.....E-
> Ethernet II, Src: Giga-Byt_07:19:d9 (d8:5e:d3:07:19:d9), Dst: Technico_ac:2b:0c (dc:eb:69:ac):	0010	00 00 60 b2 40 00 80 06 00 00 0a 00 00 60 80 77	...@... ..w
> Internet Protocol Version 4, Src: 10.0.0.96, Dst: 128.119.245.12	0020	f5 0c d1 c2 00 50 96 7f ab 61 0c 25 bc 7c 50 10P...a% P-
▼ Transmission Control Protocol, Src Port: 53698, Dst Port: 80, Seq: 1, Ack: 1, Len: 14600	0030	04 02 7f ea 00 00 50 4f 53 54 20 2f 77 69 72 65PO ST/wire
Source Port: 53698	0040	73 68 61 72 6b 2d 6c 61 62 73 2f 6c 61 62 33 2d	shark-la bs/lab3-
Destination Port: 80	0050	31 2d 72 65 70 6c 79 2e 68 74 6d 20 48 54 54 50	l-reply. htm HTTP
[Stream index: 1]	0060	2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 67 61 69 61	/1.1..Ho st: gaia
[Conversation completeness: Complete, WITH_DATA (31)]	0070	2e 63 73 2e 75 6d 61 73 73 2e 65 64 75 0d 0a 55	.s.unas s.edu..U
[TCP Segment Len: 14600]	0080	73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c	ser-Agen t: Mozil
Sequence Number: 1 (relative sequence number)	0090	6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20	la/5.0 (Windows
Sequence Number (raw): 2524949345	00a0	4e 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 30 20	NT 10.0; Win64;
[Next Sequence Number: 14601 (relative sequence number)]	00b0	78 36 34 3b 20 72 76 3a 31 30 39 2e 30 29 20 47	x64; rv: 109.0) G
Acknowledgment Number: 1 (relative ack number)	00c0	65 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 46 69	ecko/201 00101 Fi
Acknowledgment number (raw): 203799676	00d0	72 65 66 6f 78 2f 31 31 31 2e 30 0d 0a 41 63 63	refox/11 1.0..Acc
0101 = Header Length: 20 bytes (5)	00e0	65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61	ept: tex t/html,a
> Flags: 0x010 (ACK)	00f0	70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c	pplicati on/xhtml
Window: 1026	0100	2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e	=xml,app lication
[Calculated window size: 262656]	0110	2f 78 6d 6c 3b 71 3d 30 2e 39 2e 69 6d 61 67 65	/xml;q=0.9,image
[Window size scaling factor: 256]	0120	2f 61 76 69 66 2c 69 6d 61 67 65 2f 77 65 62 70	/avi;f,im age/webp
Checksum: 0x7fea [unverified]	0130	2c 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 41 63 63 65	/*;q=0.8..Acce
[Checksum Status: Unverified]	0140	70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d	pt-Langu age: en-
Urgent Pointer: 0	0150	55 53 2c 65 6e 3b 71 3d 30 2e 35 0d 0a 41 63 63	US,en;q= 0.5..Acc
> [Timestamps]	0160	65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a	ept-Encod ing: gz
> [SEQ/ACK analysis]	0170	69 70 2c 20 64 65 66 6c 61 74 65 0d 0a 43 6f 6e	ip, defl ate..Con
TCP payload (14600 bytes)	0180	74 65 6e 74 2d 54 79 70 65 3a 20 6d 75 6c 74 69	tent-Typ e: multi
[Reassembled PDU in frame: 57]	0190	70 61 72 74 2f 66 6f 72 6d 2d 64 61 74 61 3b 20	part/for m-data;
TCP segment data (14600 bytes)	01a0	62 6f 75 6e 64 61 72 79 3d 2d 2d 2d 2d 2d 2d 2d	boundary =-----
	01b0	2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d	-----
	01c0	2d 2d 2d 2d 33 34 33 30 33 37 31 34 38 30 37 36	-----3430 37148076
	01d0	37 31 35 33 39 30 33 33 30 32 34 37 37 39 32 32	71539033 02477922
	01e0	38 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74	8..Conte nt-Lengt

No.	Time	Source	Destination	Protocol	Length	Info
34	22:19:10.421928	10.0.0.96	128.119.245.12	TCP	14654	53698 → 80 [ACK] Seq=14601 Ack=1 Win=262656

Len=14600 [TCP segment of a reassembled PDU]
 Frame 34: 14654 bytes on wire (117232 bits), 14654 bytes captured (117232 bits) on interface \Device\NPF_{2748DDCA-E1DE-4281-80C4-430F4323F5A7}, id 0
 Ethernet II, Src: Giga-Byt_07:19:d9 (d8:5e:d3:07:19:d9), Dst: Technico_ac:2b:0c (dc:eb:69:ac:2b:0c)
 Internet Protocol Version 4, Src: 10.0.0.96, Dst: 128.119.245.12
 Transmission Control Protocol, Src Port: 53698, Dst Port: 80, Seq: 14601, Ack: 1, Len: 14600
 Source Port: 53698
 Destination Port: 80
 [Stream index: 1]
 [Conversation completeness: Complete, WITH_DATA (31)]
 [TCP Segment Len: 14600]
 Sequence Number: 14601 (relative sequence number)
 Sequence Number (raw): 2524963945
 [Next Sequence Number: 29201 (relative sequence number)]
 Acknowledgment Number: 1 (relative ack number)
 Acknowledgment number (raw): 203799676
 0101 = Header Length: 20 bytes (5)
 Flags: 0x010 (ACK)
 Window: 1026
 [Calculated window size: 262656]

No.	Time	Source	Destination	Protocol	Length	Info
36	22:19:10.422042	10.0.0.96	128.119.245.12	TCP	14654	53698 → 80 [PSH, ACK] Seq=29201 Ack=1 Win=262656

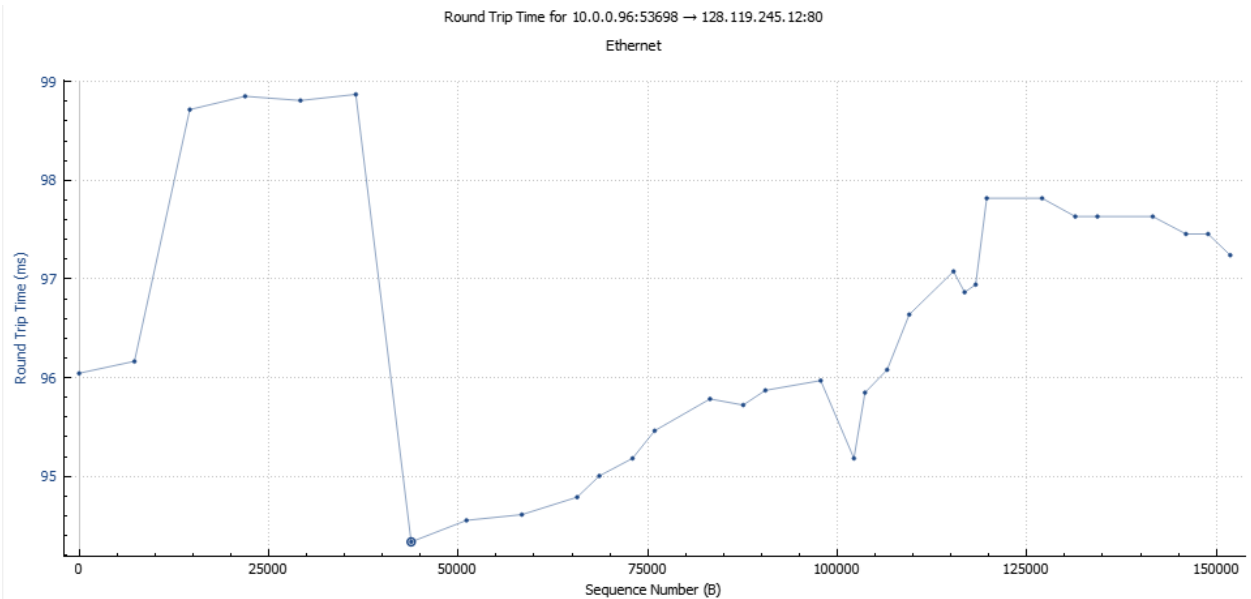
Len=14600 [TCP segment of a reassembled PDU]
 Frame 36: 14654 bytes on wire (117232 bits), 14654 bytes captured (117232 bits) on interface \Device\NPF_{2748DDCA-E1DE-4281-80C4-430F4323F5A7}, id 0
 Ethernet II, Src: Giga-Byt_07:19:d9 (d8:5e:d3:07:19:d9), Dst: Technico_ac:2b:0c (dc:eb:69:ac:2b:0c)
 Internet Protocol Version 4, Src: 10.0.0.96, Dst: 128.119.245.12
 Transmission Control Protocol, Src Port: 53698, Dst Port: 80, Seq: 29201, Ack: 1, Len: 14600
 Source Port: 53698
 Destination Port: 80
 [Stream index: 1]
 [Conversation completeness: Complete, WITH_DATA (31)]
 [TCP Segment Len: 14600]
 Sequence Number: 29201 (relative sequence number)
 Sequence Number (raw): 2524978545
 [Next Sequence Number: 43801 (relative sequence number)]
 Acknowledgment Number: 1 (relative ack number)
 Acknowledgment number (raw): 203799676
 0101 = Header Length: 20 bytes (5)
 Flags: 0x018 (PSH, ACK)
 Window: 1026
 [Calculated window size: 262656]

No.	Time	Source	Destination	Protocol	Length	Info
40	22:19:10.520654	10.0.0.96	128.119.245.12	TCP	14654	53698 → 80 [ACK] Seq=43801 Ack=1 Win=262656

Len=14600 [TCP segment of a reassembled PDU]
 Frame 40: 14654 bytes on wire (117232 bits), 14654 bytes captured (117232 bits) on interface \Device\NPF_{2748DDCA-E1DE-4281-80C4-430F4323F5A7}, id 0
 Ethernet II, Src: Giga-Byt_07:19:d9 (d8:5e:d3:07:19:d9), Dst: Technico_ac:2b:0c (dc:eb:69:ac:2b:0c)
 Internet Protocol Version 4, Src: 10.0.0.96, Dst: 128.119.245.12
 Transmission Control Protocol, Src Port: 53698, Dst Port: 80, Seq: 43801, Ack: 1, Len: 14600
 Source Port: 53698
 Destination Port: 80
 [Stream index: 1]
 [Conversation completeness: Complete, WITH_DATA (31)]
 [TCP Segment Len: 14600]
 Sequence Number: 43801 (relative sequence number)
 Sequence Number (raw): 2524993145
 [Next Sequence Number: 58401 (relative sequence number)]
 Acknowledgment Number: 1 (relative ack number)
 Acknowledgment number (raw): 203799676
 0101 = Header Length: 20 bytes (5)
 Flags: 0x010 (ACK)
 Window: 1026
 [Calculated window size: 262656]

No.	Time	Source	Destination	Protocol	Length	Info
42	22:19:10.520782	10.0.0.96	128.119.245.12	TCP	14654	53698 → 80 [PSH, ACK] Seq=58401 Ack=1 Win=262656 Len=14600 [TCP segment of a reassembled PDU]
Frame 42: 14654 bytes on wire (117232 bits), 14654 bytes captured (117232 bits) on interface \Device\NPF_{2748DDCA-E1DE-4281-80C4-430F4323F5A7}, id 0 Ethernet II, Src: Giga-Byt_07:19:d9 (d8:5e:d3:07:19:d9), Dst: Technico_ac:2b:0c (dc:eb:69:ac:2b:0c) Internet Protocol Version 4, Src: 10.0.0.96, Dst: 128.119.245.12 Transmission Control Protocol, Src Port: 53698, Dst Port: 80, Seq: 58401, Ack: 1, Len: 14600 Source Port: 53698 Destination Port: 80 [Stream index: 1] [Conversation completeness: Complete, WITH_DATA (31)] [TCP Segment Len: 14600] Sequence Number: 58401 (relative sequence number) Sequence Number (raw): 2525007745 [Next Sequence Number: 73001 (relative sequence number)] Acknowledgment Number: 1 (relative ack number) Acknowledgment number (raw): 203799676 0101 = Header Length: 20 bytes (5) Flags: 0x018 (PSH, ACK) Window: 1026 [Calculated window size: 262656]						
44	22:19:10.520852	10.0.0.96	128.119.245.12	TCP	14654	53698 → 80 [ACK] Seq=73001 Ack=1 Win=262656 Len=14600 [TCP segment of a reassembled PDU]
Frame 44: 14654 bytes on wire (117232 bits), 14654 bytes captured (117232 bits) on interface \Device\NPF_{2748DDCA-E1DE-4281-80C4-430F4323F5A7}, id 0 Ethernet II, Src: Giga-Byt_07:19:d9 (d8:5e:d3:07:19:d9), Dst: Technico_ac:2b:0c (dc:eb:69:ac:2b:0c) Internet Protocol Version 4, Src: 10.0.0.96, Dst: 128.119.245.12 Transmission Control Protocol, Src Port: 53698, Dst Port: 80, Seq: 73001, Ack: 1, Len: 14600 Source Port: 53698 Destination Port: 80 [Stream index: 1] [Conversation completeness: Complete, WITH_DATA (31)] [TCP Segment Len: 14600] Sequence Number: 73001 (relative sequence number) Sequence Number (raw): 2525022345 [Next Sequence Number: 87601 (relative sequence number)] Acknowledgment Number: 1 (relative ack number) Acknowledgment number (raw): 203799676 0101 = Header Length: 20 bytes (5) Flags: 0x010 (ACK) Window: 1026 [Calculated window size: 262656]						

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.



8. What is the length of each of the first six TCP segments?
 - a. The length of each of the first six TCP segments are 14600 bytes

No.	Time	Source	Destination	Protocol	Length	Info
3	22:19:09.423577	10.0.0.96	128.119.245.12	TCP	66	53698 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
9	22:19:09.510841	128.119.245.12	10.0.0.96	TCP	66	80 → 53698 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
10	22:19:09.510868	10.0.0.96	128.119.245.12	TCP	54	53698 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
29	22:19:10.325873	10.0.0.96	128.119.245.12	TCP	14654	53698 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=14600 [TCP segment of a reassembled PDU]
33	22:19:10.421916	128.119.245.12	10.0.0.96	TCP	60	80 → 53698 [ACK] Seq=1 Ack=7301 Win=43904 Len=0
34	22:19:10.421928	10.0.0.96	128.119.245.12	TCP	14654	53698 → 80 [ACK] Seq=14601 Ack=1 Win=262656 Len=14600 [TCP segment of a reassembled PDU]
35	22:19:10.422037	128.119.245.12	10.0.0.96	TCP	60	80 → 53698 [ACK] Seq=1 Ack=14601 Win=58496 Len=0
36	22:19:10.422042	10.0.0.96	128.119.245.12	TCP	14654	53698 → 80 [PSH, ACK] Seq=29201 Ack=1 Win=262656 Len=14600 [TCP segment of a reassembled PDU]
39	22:19:10.520643	128.119.245.12	10.0.0.96	TCP	60	80 → 53698 [ACK] Seq=1 Ack=21901 Win=73088 Len=0
40	22:19:10.520654	10.0.0.96	128.119.245.12	TCP	14654	53698 → 80 [ACK] Seq=43801 Ack=1 Win=262656 Len=14600 [TCP segment of a reassembled PDU]
41	22:19:10.520778	128.119.245.12	10.0.0.96	TCP	60	80 → 53698 [ACK] Seq=1 Ack=29201 Win=87680 Len=0
42	22:19:10.520782	10.0.0.96	128.119.245.12	TCP	14654	53698 → 80 [PSH, ACK] Seq=58401 Ack=1 Win=262656 Len=14600 [TCP segment of a reassembled PDU]
43	22:19:10.520849	128.119.245.12	10.0.0.96	TCP	60	80 → 53698 [ACK] Seq=1 Ack=36501 Win=102272 Len=0
44	22:19:10.520852	10.0.0.96	128.119.245.12	TCP	14654	53698 → 80 [ACK] Seq=73001 Ack=1 Win=262656 Len=14600 [TCP segment of a reassembled PDU]

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?
 - a. The minimum amount of available buffer space advertised at the receiver for the entire trace was 29200 bytes.
 - b. No, the lack of receiver buffer space did not ever throttle the sender. The buffer continued to grow.


```

No.      Time           Source           Destination      Protocol Length Info
 9 22:19:09.510841 128.119.245.12 10.0.0.96       TCP              66      80 → 53698 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
MSS=1460 SACK_PERM WS=128
Frame 9: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{2748DDCA-E1DE-4281-80C4-430F4323F5A7}, id 0
Ethernet II, Src: Technico_ac:2b:0c (dc:eb:69:ac:2b:0c), Dst: Giga-Byt_07:19:d9 (d8:5e:d3:07:19:d9)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.96
Transmission Control Protocol, Src Port: 80, Dst Port: 53698, Seq: 0, Ack: 1, Len: 0
  Source Port: 80
  Destination Port: 53698
  [Stream index: 1]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 203799675
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 2524949345
  1000 .... = Header Length: 32 bytes (8)
  Flags: 0x012 (SYN, ACK)
  Window: 29200
  [Calculated window size: 29200]
  Checksum: 0xa078 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted, No-Operation (NOP), Window scale
  [Timestamps]
  [SEQ/ACK analysis]

```

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

- No, there aren't any retransmitted segments. I referred to the RTT graph in order to answer this question.

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 247 in the text).

- The receiver is typically acknowledging 14,592 bytes of data in an ACK. If we observe the first several ACKs, we can see that 14,592 bytes of data are acknowledged each time.
- Yes, the screen shot below shows the receiver ACKing every other received segment.

No.	Time	Source	Destination	Protocol	Length	Info
33	22:19:10.421916	128.119.245.12	10.0.0.96	TCP	60	80 → 53698 [ACK] Seq=1 Ack=7301 Win=43904 Len=0
34	22:19:10.421928	10.0.0.96	128.119.245.12	TCP	14654	53698 → 80 [ACK] Seq=14601 Ack=1 Win=262656 Len=14600 [TCP segment of a reassembled PDU]
35	22:19:10.422037	128.119.245.12	10.0.0.96	TCP	60	80 → 53698 [ACK] Seq=1 Ack=14601 Win=58496 Len=0
36	22:19:10.422042	10.0.0.96	128.119.245.12	TCP	14654	53698 → 80 [PSH, ACK] Seq=29201 Ack=1 Win=262656 Len=14600 [TCP segment of a reassembled PDU]
39	22:19:10.520643	128.119.245.12	10.0.0.96	TCP	60	80 → 53698 [ACK] Seq=1 Ack=21901 Win=73088 Len=0
40	22:19:10.520654	10.0.0.96	128.119.245.12	TCP	14654	53698 → 80 [ACK] Seq=43801 Ack=1 Win=262656 Len=14600 [TCP segment of a reassembled PDU]
41	22:19:10.520778	128.119.245.12	10.0.0.96	TCP	60	80 → 53698 [ACK] Seq=1 Ack=29201 Win=87680 Len=0
42	22:19:10.520782	10.0.0.96	128.119.245.12	TCP	14654	53698 → 80 [PSH, ACK] Seq=58401 Ack=1 Win=262656 Len=14600 [TCP segment of a reassembled PDU]
43	22:19:10.520849	128.119.245.12	10.0.0.96	TCP	60	80 → 53698 [ACK] Seq=1 Ack=36501 Win=102272 Len=0
44	22:19:10.520852	10.0.0.96	128.119.245.12	TCP	14654	53698 → 80 [ACK] Seq=73001 Ack=1 Win=262656 Len=14600 [TCP segment of a reassembled PDU]
45	22:19:10.520911	128.119.245.12	10.0.0.96	TCP	60	80 → 53698 [ACK] Seq=1 Ack=43801 Win=116864 Len=0
46	22:19:10.520914	10.0.0.96	128.119.245.12	TCP	14654	53698 → 80 [PSH, ACK] Seq=87601 Ack=1 Win=262656 Len=14600 [TCP segment of a reassembled PDU]
48	22:19:10.614990	128.119.245.12	10.0.0.96	TCP	60	80 → 53698 [ACK] Seq=1 Ack=51101 Win=131456 Len=0
49	22:19:10.615001	10.0.0.96	128.119.245.12	TCP	14654	53698 → 80 [ACK] Seq=102201 Ack=1 Win=262656 Len=14600 [TCP segment of a reassembled PDU]
50	22:19:10.615208	128.119.245.12	10.0.0.96	TCP	60	80 → 53698 [ACK] Seq=1 Ack=58401 Win=146048 Len=0
51	22:19:10.615212	10.0.0.96	128.119.245.12	TCP	14654	53698 → 80 [PSH, ACK] Seq=116801 Ack=1 Win=262656 Len=14600 [TCP segment of a reassembled PDU]
52	22:19:10.615394	128.119.245.12	10.0.0.96	TCP	60	80 → 53698 [ACK] Seq=1 Ack=65701 Win=160640 Len=0
53	22:19:10.615397	10.0.0.96	128.119.245.12	TCP	14654	53698 → 80 [ACK] Seq=131401 Ack=1 Win=262656 Len=14600 [TCP segment of a reassembled PDU]
54	22:19:10.615571	128.119.245.12	10.0.0.96	TCP	60	80 → 53698 [ACK] Seq=1 Ack=68621 Win=166528 Len=0
55	22:19:10.615574	10.0.0.96	128.119.245.12	TCP	5894	53698 → 80 [ACK] Seq=146001 Ack=1 Win=262656 Len=5840 [TCP segment of a reassembled PDU]
56	22:19:10.615786	128.119.245.12	10.0.0.96	TCP	60	80 → 53698 [ACK] Seq=1 Ack=73001 Win=175232 Len=0

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

Explain how you calculated this value.

- calculated window size final ok = 281856 bytes
time difference: 0.713099 - 0.615789 = 0.09731 seconds
throughput = 281856/0.09731 = 2,896,475.1824067413421025588325969 bps
throughput = ~2.9 Mbps

- b. I figured out the total amount of data transferred and divided it by the time it took to transfer the data.

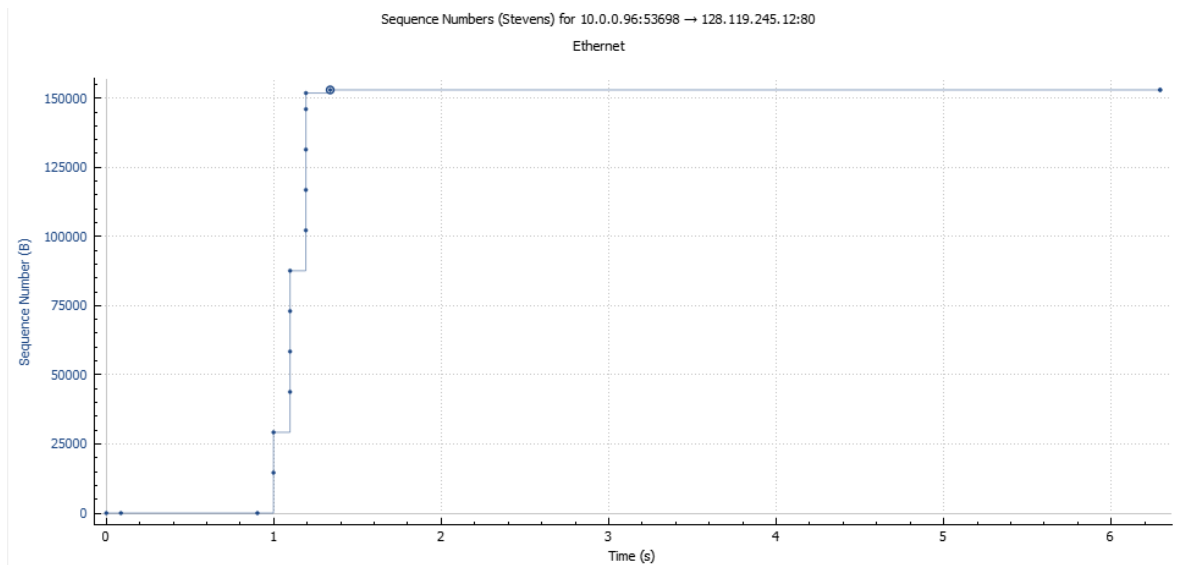
```

57 22:19:10.615789 10.0.0.96 128.119.245.12 HTTP 1189 POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)

No.    Time                Source                Destination            Protocol Length Info
 77    22:19:10.713099    128.119.245.12        10.0.0.96              HTTP      831    HTTP/1.1 200 OK (text/html)
Frame 77: 831 bytes on wire (6648 bits), 831 bytes captured (6648 bits) on interface \Device\NPF_{2748DDCA-E1DE-4281-80C4-430F4323F5A7}, id 0
Ethernet II, Src: Technico_ac:2b:0c (dc:eb:69:ac:2b:0c), Dst: Giga-Byt_07:19:d9 (d8:5e:d3:07:19:d9)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.96
Transmission Control Protocol, Src Port: 80, Dst Port: 53698, Seq: 1, Ack: 152976, Len: 777
  Source Port: 80
  Destination Port: 53698
  [Stream index: 1]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 777]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 203799676
  [Next Sequence Number: 778 (relative sequence number)]
  Acknowledgment Number: 152976 (relative ack number)
  Acknowledgment number (raw): 2525102320
  0101 .... = Header Length: 20 bytes (5)
  Flags: 0x018 (PSH, ACK)
  Window: 2202
  [Calculated window size: 281856]
  [Window size scaling factor: 128]
  Checksum: 0x4691 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  [Timestamps]
  [SEQ/ACK analysis]
  TCP payload (777 bytes)
Hypertext Transfer Protocol
Line-based text data: text/html (11 lines)

```

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.



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`
- a. It looks like TCP's slow start phase begins at around 0-0.1173 seconds and ends at around 0.2 seconds. Congestion avoidance takes over at around 1 second.