

LAB: 3

The image shows a Wireshark packet capture window titled "*Wi-Fi". The packet list on the left shows a series of packets. Packet 9 is selected, which is a TCP SYN packet from 192.168.1.19 to 128.119.245.12, source port 59707, destination port 80. The packet details pane on the right shows the following information:

```

Frame 9: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: Shenzhen_c3:62:bd (bc:ec:23:c3:62:bd), Dst: Netgear_21:66:a4 (b0:39:56:21:66:a4)
Internet Protocol Version 4, Src: 192.168.1.19, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 59707, Dst Port: 80, Seq: 0, Len: 0
  Source Port: 59707
  Destination Port: 80
  [Stream index: 3]
  [TCP Segment Len: 0]
  Sequence number: 0 (relative sequence number)
  [Next sequence number: 0 (relative sequence number)]
  Acknowledgment number: 0
  1000 .... = Header Length: 32 bytes (8)

```

The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII:

```

0000 b0 39 56 21 66 a4 bc ec 23 c3 62 bd 08 00 45 00 9V!f...#b...E-
0010 00 34 50 2a 40 00 80 06 73 5a c0 a8 01 13 80 77 4P*...sZ.....w
0020 f5 0c e9 3b 00 50 60 02 68 f0 00 00 00 00 80 02 ...;P'h.....
0030 fa f0 8a 61 00 00 02 04 05 b4 01 03 03 08 01 01 ...a.....
0040 04 02 ..

```

1. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu? To answer this question, it's probably easiest to select an HTTP message and explore the details of the TCP packet used to carry this HTTP message, using the "details of the selected packet header window" (refer to Figure 2 in the "Getting Started with Wireshark" Lab if you're uncertain about the Wireshark windows).

Answer: IP address 192.168.1.19 using port 59707

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? If you have been able to create your own trace, answer the following question:

Answer: IP address 128.119.245.12 using port 80

3. What is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu?

Answer: In this case I am the client so IP address 192.168.1.19 using port 59707

162	2.263822	192.168.1.19	128.119.245.12	HTTP	533	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (te
163	2.265780	128.119.245.12	192.168.1.19	TCP	60	80 → 59707 [ACK] Seq=1 Ack=73662 Win=176640 Len=0
164	2.265781	128.119.245.12	192.168.1.19	TCP	60	80 → 59707 [ACK] Seq=1 Ack=75122 Win=179456 Len=0
165	2.265810	128.119.245.12	192.168.1.19	TCP	60	80 → 59707 [ACK] Seq=1 Ack=76582 Win=182400 Len=0
166	2.270370	128.119.245.12	192.168.1.19	TCP	60	80 → 59707 [ACK] Seq=1 Ack=79502 Win=182528 Len=0
167	2.270370	128.119.245.12	192.168.1.19	TCP	60	80 → 59707 [ACK] Seq=1 Ack=82422 Win=180608 Len=0
168	2.270371	128.119.245.12	192.168.1.19	TCP	60	80 → 59707 [ACK] Seq=1 Ack=83882 Win=183296 Len=0
169	2.270371	128.119.245.12	192.168.1.19	TCP	60	80 → 59707 [ACK] Seq=1 Ack=88262 Win=180608 Len=0
170	2.270371	128.119.245.12	192.168.1.19	TCP	60	80 → 59707 [ACK] Seq=1 Ack=91182 Win=182528 Len=0
171	2.270430	128.119.245.12	192.168.1.19	TCP	60	80 → 59707 [ACK] Seq=1 Ack=92642 Win=183296 Len=0
172	2.270431	128.119.245.12	192.168.1.19	TCP	60	80 → 59707 [ACK] Seq=1 Ack=94102 Win=183296 Len=0
173	2.271970	128.119.245.12	192.168.1.19	TCP	60	80 → 59707 [ACK] Seq=1 Ack=95562 Win=183296 Len=0
174	2.271970	128.119.245.12	192.168.1.19	TCP	60	80 → 59707 [ACK] Seq=1 Ack=97022 Win=182528 Len=0
175	2.339010	128.119.245.12	192.168.1.19	TCP	60	80 → 59707 [ACK] Seq=1 Ack=99942 Win=182528 Len=0

> Frame 162: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits) on interface 0
> Ethernet II, Src: Shenzhen_c3:62:bd (bc:ec:23:c3:62:bd), Dst: Netgear_21:66:a4 (b0:39:56:21:66:a4)
> Internet Protocol Version 4, Src: 192.168.1.19, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 59707, Dst Port: 80, Seq: 152502, Ack: 1, Len: 479
> [106 Reassembled TCP Segments (152980 bytes): #13(661), #14(1460), #15(1460), #16(1460), #17(1460), #18(1460), #19(1460), #20(1460),
> Hypertext Transfer Protocol
> MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "--WebKitFormBoundaryrfAzHAQoZw9Ep0FU"

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: Sequence number is 1 and the Flag is what identifies the connection as you can see in the picture below stating if SYN is set.

9	1.764602	192.168.1.19	128.119.245.12	TCP	66	59707 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=
---	----------	--------------	----------------	-----	----	---

> Internet Protocol Version 4, Src: 192.168.1.19, Dst: 128.119.245.12
✓ Transmission Control Protocol, Src Port: 59707, Dst Port: 80, Seq: 0, Len: 0
Source Port: 59707
Destination Port: 80
[Stream index: 3]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
[Next sequence number: 0 (relative sequence number)]
Acknowledgment number: 0
1000 = Header Length: 32 bytes (8)
✓ Flags: 0x002 (SYN)
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

5. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

Answer: The sequence number is 0 for [SYN,ACK] and the Acknowledgement is 1 which determined by the sequence number. Looking at the flag field you can see the acknowledgment field and syn is set to 1 stating it is an SYN ACK message,

11	1.877957	128.119.245.12	192.168.1.19	TCP	66 80 → 59707 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
12	1.878027	192.168.1.19	128.119.245.12	TCP	54 59707 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
13	1.878381	192.168.1.19	128.119.245.12	TCP	715 59707 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=661
14	1.878482	192.168.1.19	128.119.245.12	TCP	1514 59707 → 80 [ACK] Seq=662 Ack=1 Win=65536 Len=1460
15	1.878484	192.168.1.19	128.119.245.12	TCP	1514 59707 → 80 [ACK] Seq=2122 Ack=1 Win=65536 Len=1460
16	1.878486	192.168.1.19	128.119.245.12	TCP	1514 59707 → 80 [ACK] Seq=3582 Ack=1 Win=65536 Len=1460
17	1.878492	192.168.1.19	128.119.245.12	TCP	1514 59707 → 80 [ACK] Seq=5042 Ack=1 Win=65536 Len=1460
18	1.878493	192.168.1.19	128.119.245.12	TCP	1514 59707 → 80 [ACK] Seq=6502 Ack=1 Win=65536 Len=1460
19	1.878495	192.168.1.19	128.119.245.12	TCP	1514 59707 → 80 [ACK] Seq=7962 Ack=1 Win=65536 Len=1460
20	1.878496	192.168.1.19	128.119.245.12	TCP	1514 59707 → 80 [ACK] Seq=9422 Ack=1 Win=65536 Len=1460

> Frame 11: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
 > Ethernet II, Src: Netgear_21:66:a4 (b0:39:56:21:66:a4), Dst: Shenzhen_c3:62:bd (bc:ec:23:c3:62:bd)
 > Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.19
 > Transmission Control Protocol, Src Port: 80, Dst Port: 59707, Seq: 0, Ack: 1, Len: 0

Source Port: 80
 Destination Port: 59707
 [Stream index: 3]
 [TCP Segment Len: 0]
 Sequence number: 0 (relative sequence number)
 [Next sequence number: 0 (relative sequence number)]
 Acknowledgment number: 1 (relative ack number)
 1000 = Header Length: 32 bytes (8)
 > Flags: 0x012 (SYN, ACK)
 Window size value: 29200

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 C 1

6. What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.

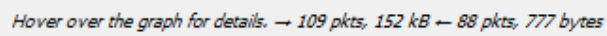

Answer: The sequence number of the TCP containing Post Command is 152502

161	2.263820	192.168.1.19	128.119.245.12	TCP	59707 → 80 [ACK] Seq=151042 Ack=1 Win=65536 Len=146
162	2.263822	192.168.1.19	128.119.245.12	HTTP	533 POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (te
163	2.265780	128.119.245.12	192.168.1.19	TCP	60 80 → 59707 [ACK] Seq=1 Ack=73662 Win=176640 Len=0
164	2.265781	128.119.245.12	192.168.1.19	TCP	60 80 → 59707 [ACK] Seq=1 Ack=75122 Win=179456 Len=0
165	2.265810	128.119.245.12	192.168.1.19	TCP	60 80 → 59707 [ACK] Seq=1 Ack=76582 Win=182400 Len=0
166	2.270370	128.119.245.12	192.168.1.19	TCP	60 80 → 59707 [ACK] Seq=1 Ack=79502 Win=182528 Len=0
167	2.270370	128.119.245.12	192.168.1.19	TCP	60 80 → 59707 [ACK] Seq=1 Ack=82422 Win=180608 Len=0

>	Frame 162: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits) on interface 0
>	Ethernet II, Src: Shenzhen_c3:62:bd (bc:ec:23:c3:62:bd), Dst: Netgear_21:66:a4 (b0:39:56:21:66:a4)
>	Internet Protocol Version 4, Src: 192.168.1.19, Dst: 128.119.245.12
▼	Transmission Control Protocol, Src Port: 59707, Dst Port: 80, Seq: 152502, Ack: 1, Len: 479
	Source Port: 59707
	Destination Port: 80
	[Stream index: 3]
	[TCP Segment Len: 479]
	Sequence number: 152502 (relative sequence number)
	[Next sequence number: 152981 (relative sequence number)]
	Acknowledgment number: 1 (relative ack number)
	0101 = Header Length: 20 bytes (5)
>	Flags: 0x018 (PSH, ACK)

7. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What are the sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST)? At what time was each segment sent? When was the ACK for each segment received? Given the difference between when each TCP segment was sent, and when its acknowledgement was received, what is the RTT value for each of the six segments? What is the EstimatedRTT value (see Section 3.5.3, page 242 in text) after the receipt of each ACK? Assume that the value of the EstimatedRTT is equal to the measured RTT for the first segment, and then is computed using the EstimatedRTT equation on page 242 for all subsequent segments.

Note: Wireshark has a nice feature that allows you to plot the RTT for each of the TCP segments sent. Select a TCP segment in the "listing of captured packets" window that is being sent from the client to the gaia.cs.umass.edu server. Then select: Statistics->TCP Stream Graph- >Round Trip Time Graph.

Stream 3  Switch Direction☐ RTT By Sequence Number

Save As...

Close

Help

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

Answer: The length is 54 and 66 for the TCP segment.

9. What is the minimum amount of available buffer space advertised at the receiver for the entire trace? Does the lack of receiver buffer space ever throttle the sender?

Answer: The minimum buffer space is determined by the calculated window which is 65536 bytes. In the HTTP POST, the SEQ/ACK analysis indicates Bytes sent last was 4859 which is nowhere near the minimum buffer size therefore there should be no throttling.

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: There aren't any retransmissions based on the Sequence numbers and ACK number. If there were then the ack number would have reset

11. How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment (see Table 3.2 on page 250 in the text).

Answer: Typical size is 432 bits for acknowledge in an ACK.

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

204	2.378620	128.119.245.12	192.168.1.19	TCP	60 80 → 59707 [ACK] Seq=1 Ack=152981 Win=289280 Len=0
-----	----------	----------------	--------------	-----	---

Answer: Last Ack – First Sequence Number / time (last-first frame) = $(152981 - 1) / (2.378620) = 63,314.6$
= 63Kbyte/sec.

13. Use the Time-Sequence-Graph(Stevens) plotting tool to view the sequence number versus time plot of segments being sent from the client to the gaia.cs.umass.edu server. Can you identify where TCP's slowstart phase begins and ends, and where congestion avoidance takes over? Comment on ways in which the measured data differs from the idealized behavior of TCP that we've studied in the text.

Answer: Slow start phase begins around 8000 and ends before 18000. Congestion avoidance takes over at 18000. This graph assumes TCP senders are aggressive and cause a lot of traffic. It is also important to understand that TCP depends on application which affects the flow of traffic.

