

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:

No.	Time	Source	Destination	Protocol	Length	Info
196	5.201150	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80 [ACK] Seq=16236
197	5.202024	192.168.1.102	128.119.245.12	TCP	326	1161 → 80 [PSH, ACK] Seq=
198	5.297257	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack
199	5.297341	192.168.1.102	128.119.245.12	HTTP	104	POST /ethereal-labs/lab3-
200	5.389471	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack
201	5.447887	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack
202	5.455830	128.119.245.12	192.168.1.102	TCP	60	80 → 1161 [ACK] Seq=1 Ack
203	5.461175	128.119.245.12	192.168.1.102	HTTP	784	HTTP/1.1 200 OK (text/ht
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

▶ 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)
 Sequence number (raw): 232293053
 [Next sequence number: 164091 (relative sequence number)]
 Acknowledgment number: 1 (relative ack number)
 Acknowledgment number (raw): 883061786

The source IP address was 192.168.1.102 using source port 1161.

2. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?

Answer:

The destination IP address is 128.119.245.12 receiving on 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:

The source IP address was 192.168.1.102 using source port 1161.

4. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?

Answer:

1	0.000000	192.168.1.102	128.119.245.12	TCP	62	1161 → 80	[SYN]	Seq=0 Win=16384	L
2	0.023172	128.119.245.12	192.168.1.102	TCP	62	80 → 1161	[SYN, ACK]	Seq=0 Ack=1	
3	0.023265	192.168.1.102	128.119.245.12	TCP	54	1161 → 80	[ACK]	Seq=1 Ack=1 Win=1	
4	0.026477	192.168.1.102	128.119.245.12	TCP	619	1161 → 80	[PSH, ACK]	Seq=1 Ack=1	
5	0.041737	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80	[PSH, ACK]	Seq=566 Ack=	
6	0.053937	128.119.245.12	192.168.1.102	TCP	60	80 → 1161	[ACK]	Seq=1 Ack=566 Win	
7	0.054026	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80	[ACK]	Seq=2026 Ack=1 Wi	
8	0.054690	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80	[ACK]	Seq=3486 Ack=1 Wi	
9	0.077294	128.119.245.12	192.168.1.102	TCP	60	80 → 1161	[ACK]	Seq=1 Ack=2026 Wi	
10	0.077405	192.168.1.102	128.119.245.12	TCP	1514	1161 → 80	[ACK]	Seq=4946 Ack=1 Wi	

Transmission Control Protocol, Src Port: 1161, Dst Port: 80, Seq: 0, Len: 0

Source Port: 1161

Destination Port: 80

[Stream index: 0]

[TCP Segment Len: 0]

Sequence number: 0 (relative sequence number)

Sequence number (raw): 232129012

[Next sequence number: 1 (relative sequence number)]

Acknowledgment number: 0

Acknowledgment number (raw): 0

0111 = Header Length: 28 bytes (7)

Flags: 0x002 (SYN)

Window size value: 16384

[Calculated window size: 16384]

Checksum: 0xf6a9 [unverified]

The sequence number of the segment used to initiate the TCP connection is 0. We can see that the message contains a SYN flag indicating that it is a SYN segment.

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:

1	0.000000	192.168.1.102	128.119.245.12	TCP	62	1161 → 80	[SYN]	Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1	
2	0.023172	128.119.245.12	192.168.1.102	TCP	62	80 → 1161	[SYN, ACK]	Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1	
3	0.023265	192.168.1.102	128.119.245.12	TCP	54	1161 → 80	[ACK]	Seq=1 Ack=1 Win=17520 Len=0	
4	0.026477	192.168.1.102	128.119.245.12	TCP	619	1161 → 80	[PSH, ACK]	Seq=1 Ack=1 Win=17520 Len=565 [TCP segment of	
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 segment	
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 segment of	
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 segment of	
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 segment of	

Frame 2: 62 bytes on wire (496 bits), 62 bytes captured (496 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: 0, Ack: 1, Len: 0

Source Port: 80

Destination Port: 1161

[Stream index: 0]

[TCP Segment Len: 0]

Sequence number: 0 (relative sequence number)

Sequence number (raw): 883061785

[Next sequence number: 1 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

Acknowledgment number (raw): 232129013

0111 = Header Length: 28 bytes (7)

Flags: 0x012 (SYN, ACK)

Window size value: 5840

[Calculated window size: 5840]

Checksum: 0x774d [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

The sequence number of the SYNACK segment is 0.

The value of the acknowledgement field is 1. This value is determined by the initial sequence number +1.

The message carries flags that show it to be a SYN ACK message.

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:

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

Source Port: 1161
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 50]
Sequence number: 164041 (relative sequence number)
Sequence number (raw): 232293053
[Next sequence number: 164091 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Acknowledgment number (raw): 883061786
0101 ... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window size value: 17520
[Calculated window size: 17520]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x9f0f [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
[Timestamps]

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.