Pulakesh Bag

Roll No: 120CS0131

Computer Science & Engineering
(2020-24)

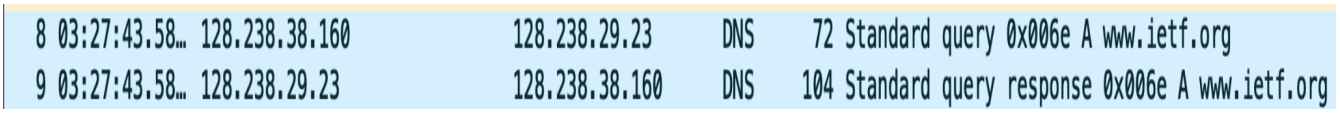
Data Communications & Computer Network Laboratory-3

Q1: Answer the following questions for captured file dns1.pcap (DNS Protocol)

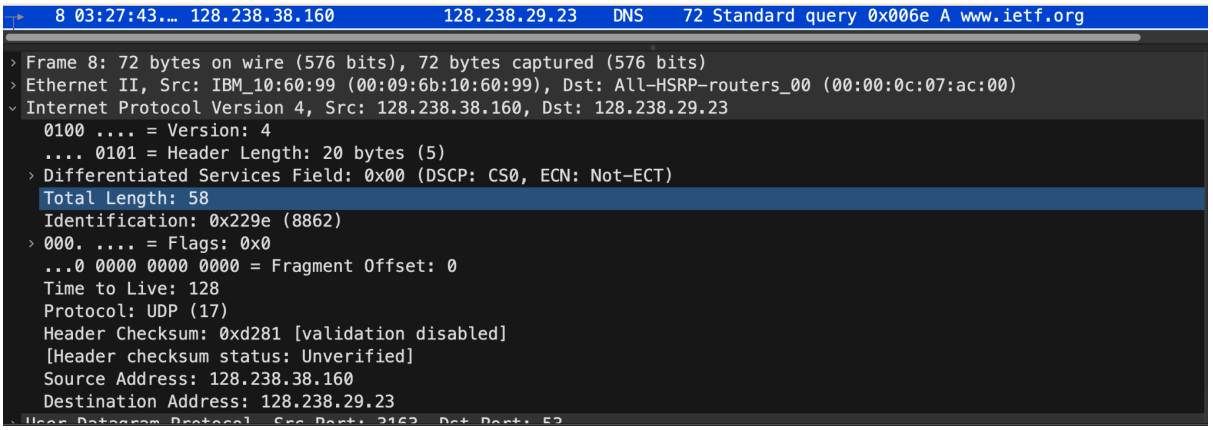
Ans:

1.1. Locate the DNS query and response messages. Are they sent over UDP or TCP?

->



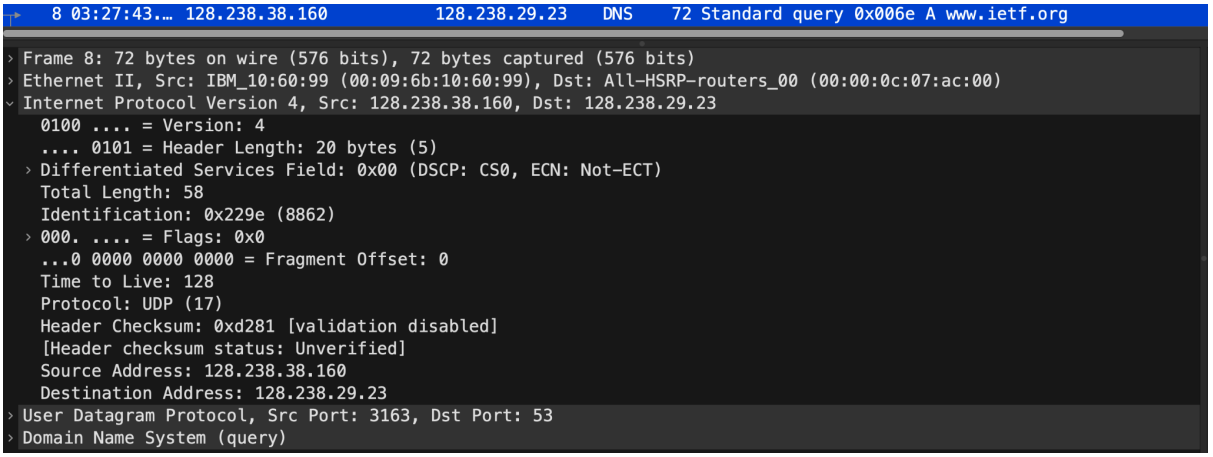
They are sent over ***UDP***



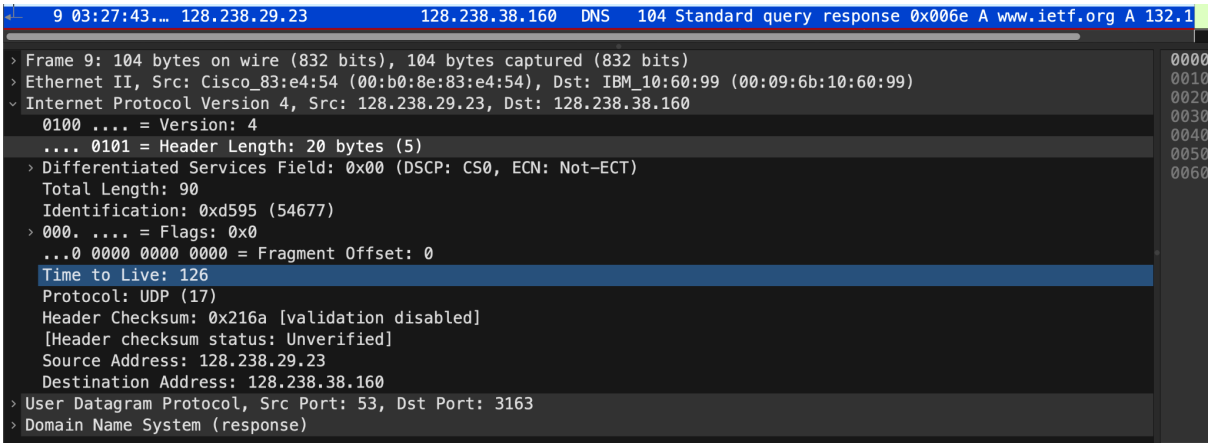
1.2. What is the destination port for the DNS query message? What is the source port of DNS response message?

->

Destination port for the DNS query message is ***53***



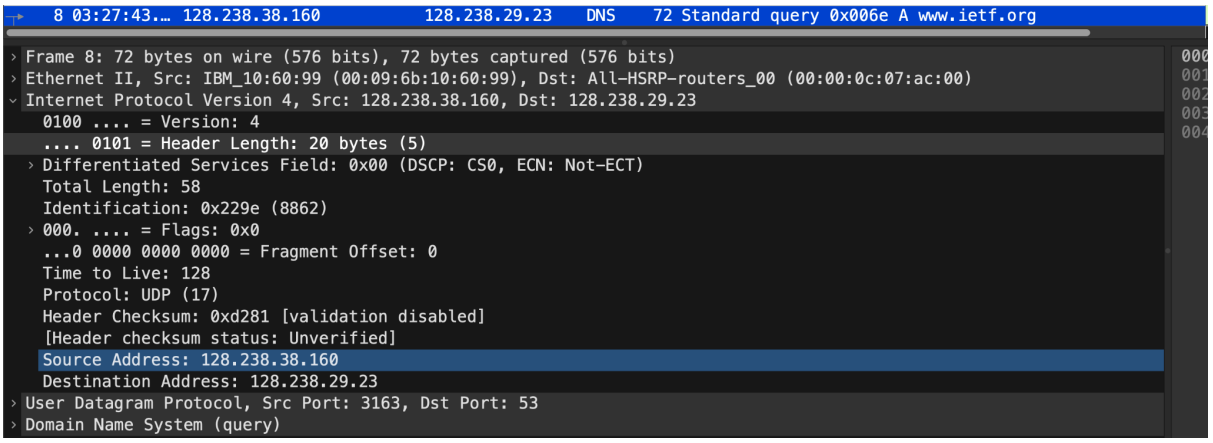
source port of DNS response message is ***53***



1.3. To what IP address is the DNS query message sent? Use nm-tool command to determine the IP address of your local DNS server. Are these two IP addresses the same?

->

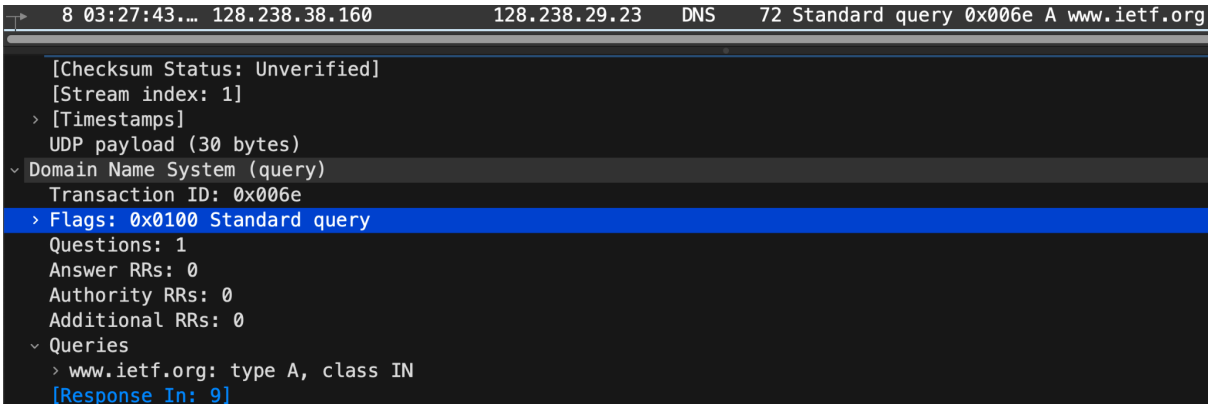
DNS query message sent is sent out to IP address ***128.238.29.23***



1.4. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

->

The DNS query is of type ***Standard query(0x0100)***

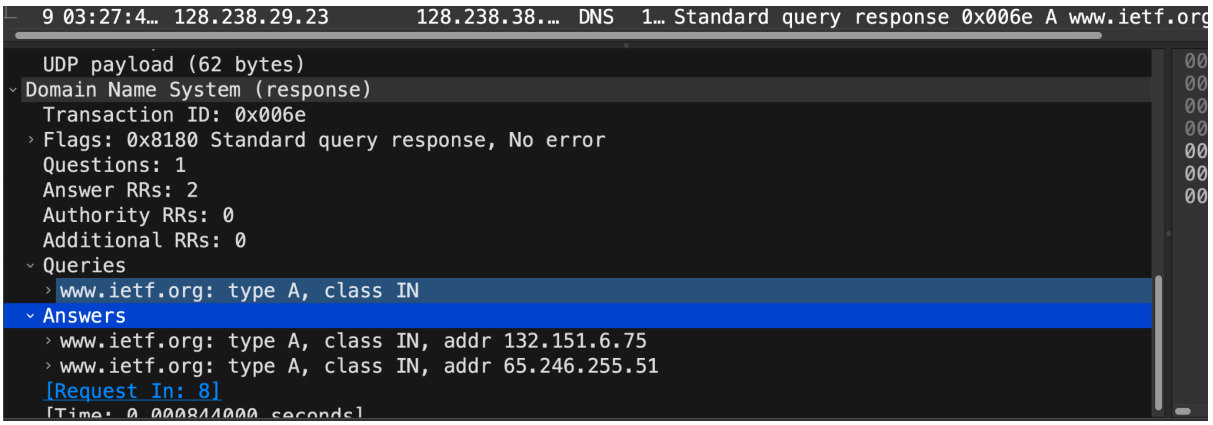


The query message contains ***no answers*** because Answer RRs: 0.

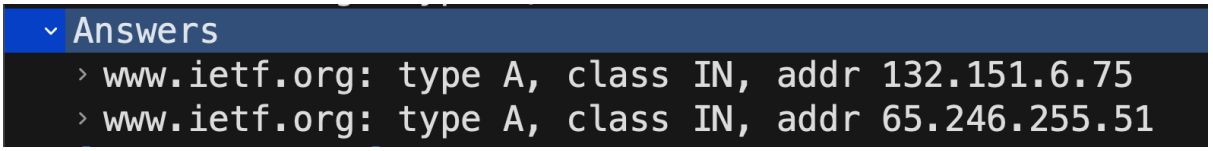
1.5. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

->

2 answers are provided in the response message.



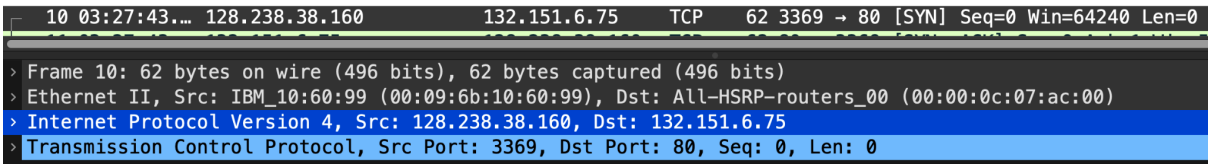
The answers contain data regarding local DNS servers.



1.6. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

->

Destination IP address of the TCP SYN packet correspond to the IP address ***132.151.6.75*** which is also provided in the DNS response message.



1.7. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

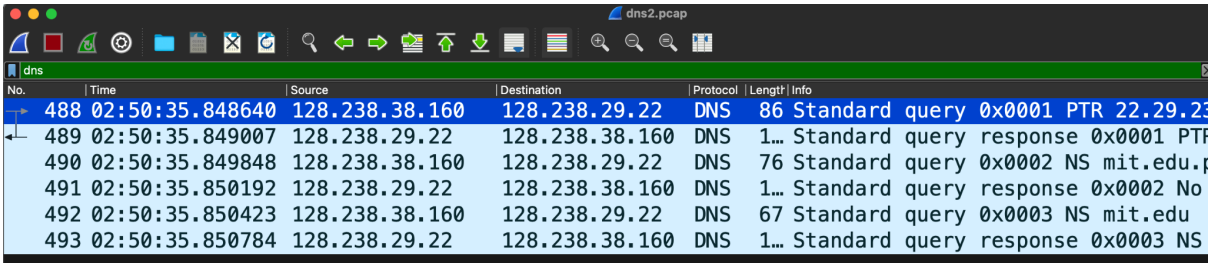
->

No, DNS location is retrieved once and then used in future until it expires, so we don’t see

1.8. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

->

DNS query message is sent to the IP address ***128.238.29.22***



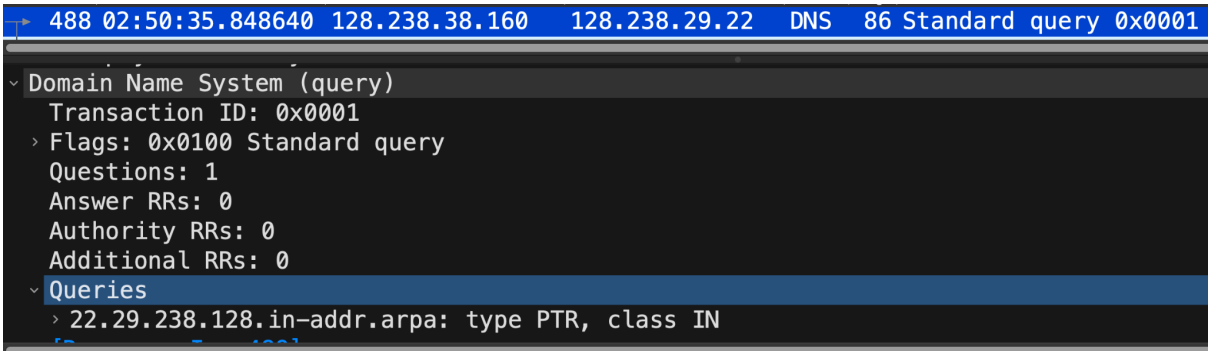
No, this is not the IP address of my default local DNS server(192.168.1.250).

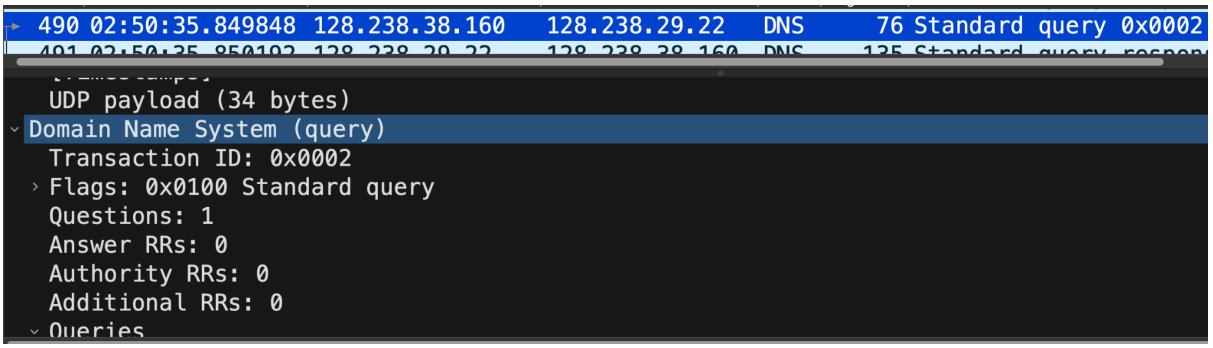
1.9. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

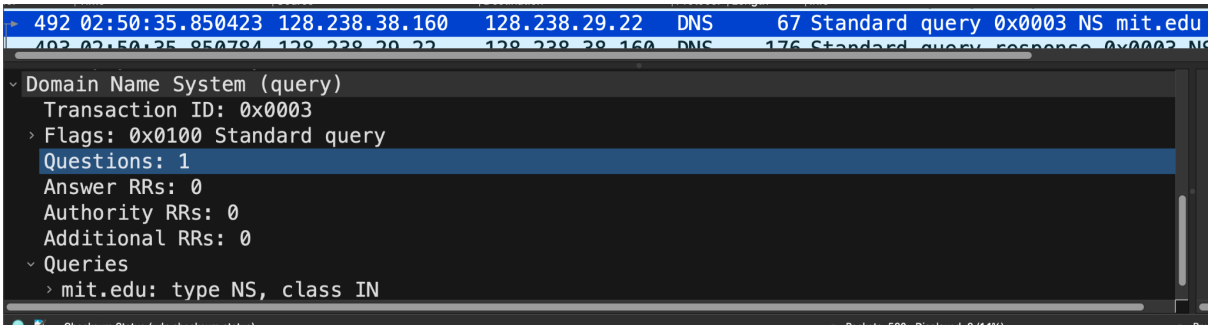
->

The three DNS query is of type ***PTR***.

Query messages of the three queries contains ***0*** answer.

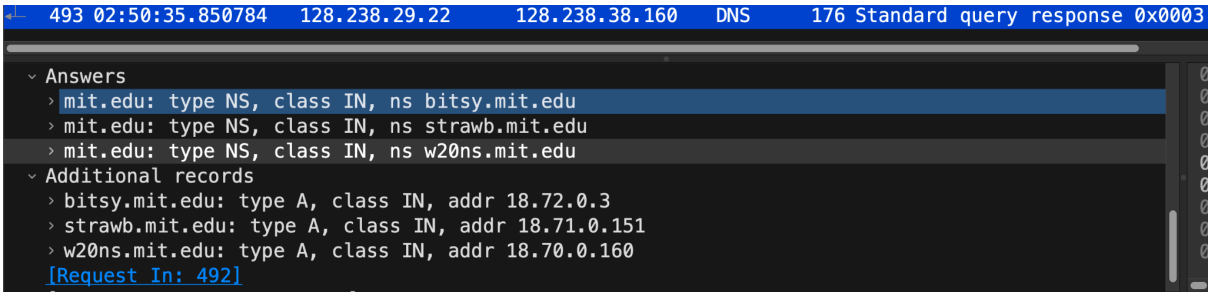






1.10. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT nameservers?
->

This message provide IP addresses of the MIT nameservers bitsy.mit.edu(18.72.0.3), strawb.mit.edu(18.71.0.151), w20ns.mit.edu(18.70.0.160)

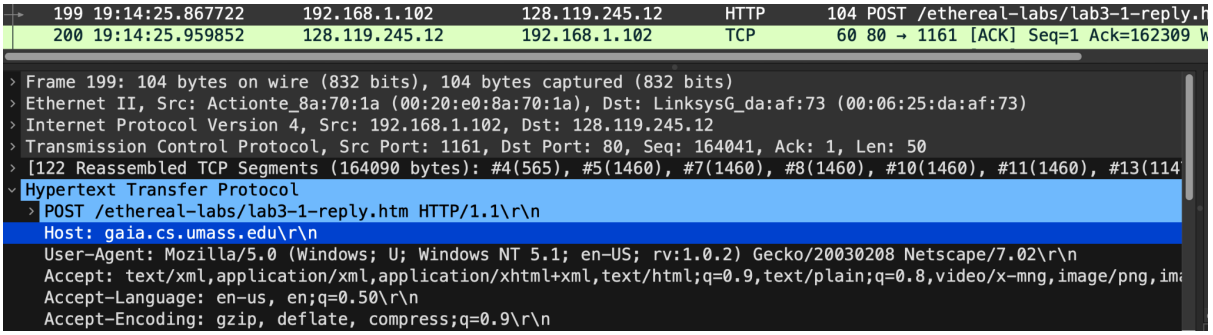


Q2. **Answer the following questions for captured file tcp.pcap (TCP Protocol)**

2.1. 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.

->

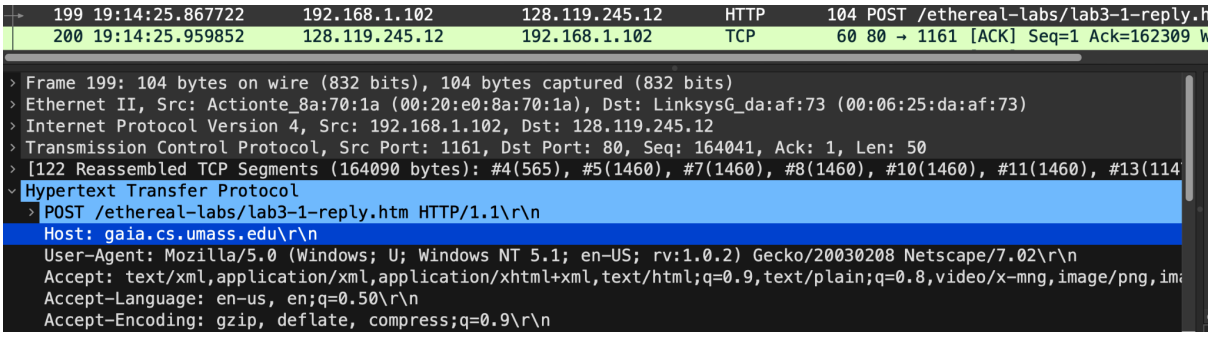
IP address is 192.168.1.102 and port number is 1161, that is used by the client computer (source) that is transferring the file to gaia.cs.umass.edu.



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

->

IP address of gaia.cs.umass.edu is ***128.119.245.12.***



It is sending and receiving TCP segments for this connection on port number ***80.***

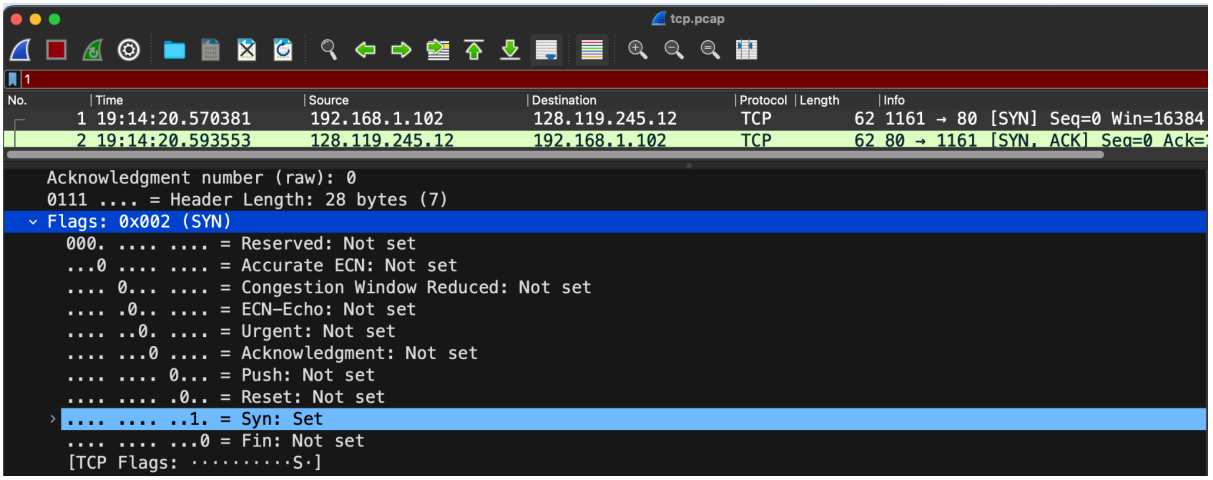
2.3. What is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu?

->

IP address and TCP port number used by my client computer (source) to transfer the file to gaia.cs.umass.edu is ***192.168.1.102*** and ***1161*** respectively.

2.4. 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?
->
Sequence number of the TCP SYN segment is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu. The value is 0 in this trace. The SYN flag is set to 1 and it indicates that this segment is a SYN segment.

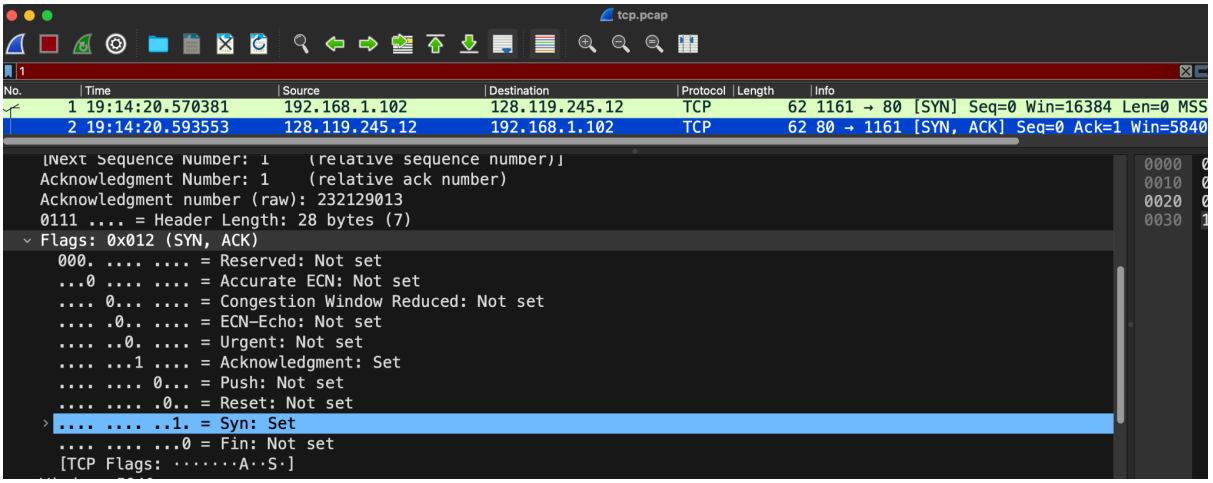
The SYN flag is set to 1 and it indicates that this segment is a SYN segment.



2.5. 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?
->
Sequence number of the SYNACK segment from gaia.cs.umass.edu to the client computer in reply to the SYN has the value of 0 in this trace.

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 gaia.cs.umass.edu by adding 1 to the initial sequence number of SYN segment from the client computer (i.e. the sequence number of the SYN segment initiated by the client computer is 0.).

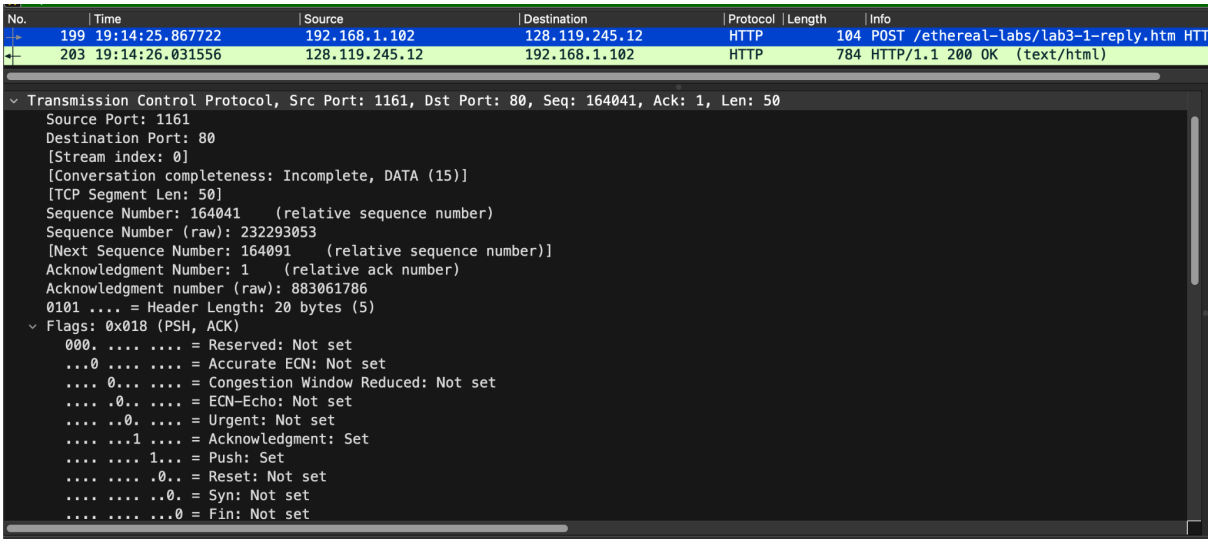
The SYN flag and Acknowledgement flag in the segment are set to 1 and they indicate that this segment is a SYNACK segment.



2.6. 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.

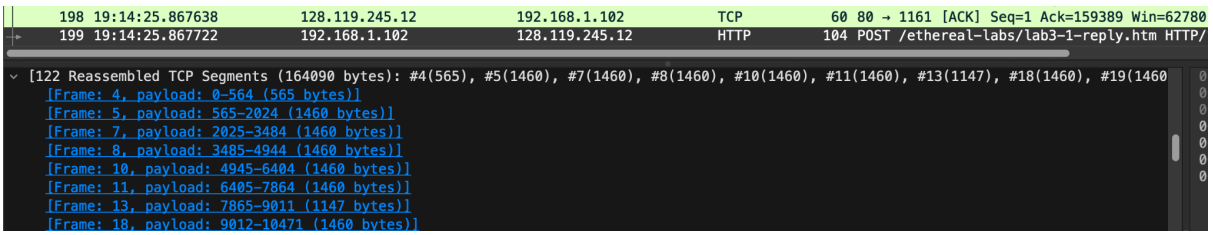
->

No. 199 segment is the TCP segment containing the HTTP POST command. The sequence number of this segment has the value of ***164041***.



2.7. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What is the length of each of the first six TCP segments?

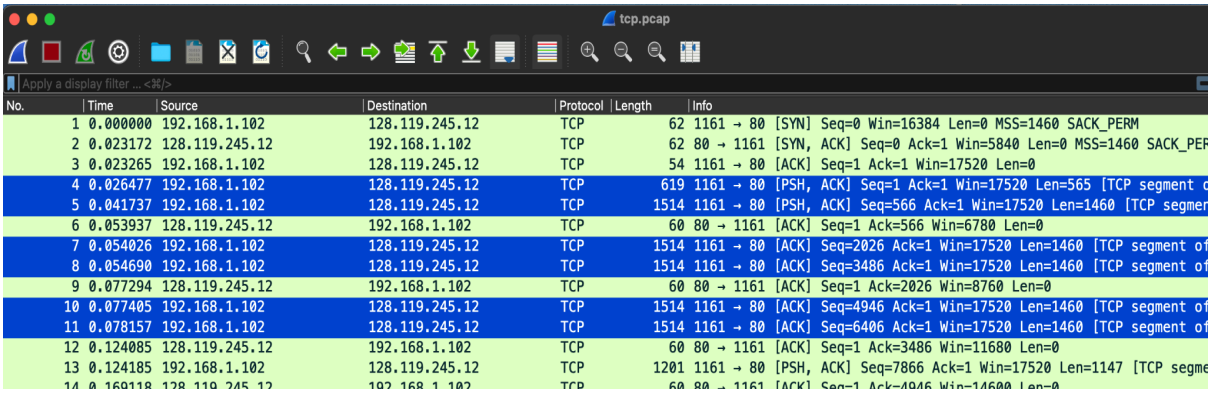
->Length of the first segment is 565 Bytes and the next 5 packet contains 1460 Bytes each.



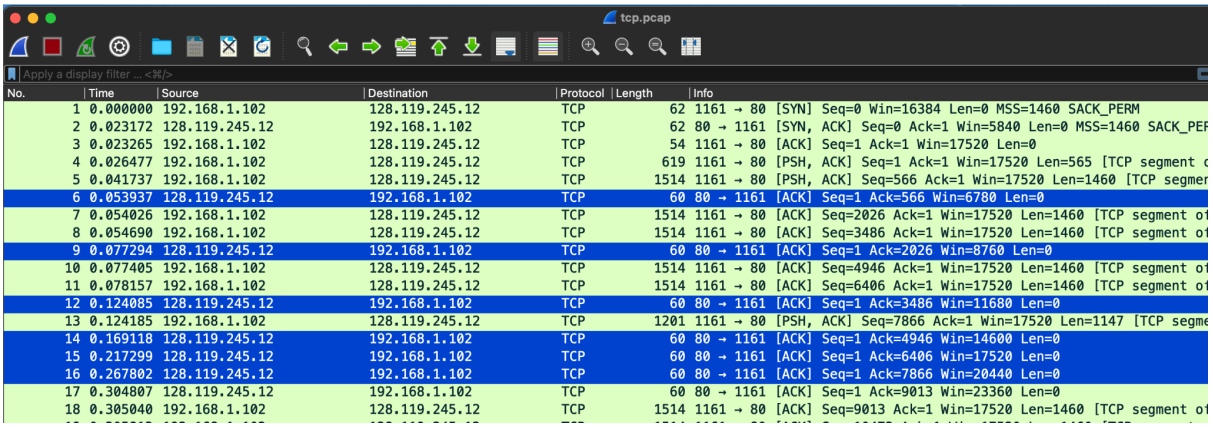
2.8. What is the EstimatedRTT value (see Section 3.5.3, page 239 in text from Kurose Book) after the receipt of each ACK? Assume that the value of the EstimatedRTT is equal to the measured RTT for the first segment. [Hint: Wireshark has a nice feature that allows you to plot the RTT for each of the TCP 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. Select as Statistics->TCP Stream Graph->Round Trip Time Graph.]
->
The HTTP POST segment is considered as the first segment. Segments 1 – 6 are No. 4, 5, 7, 8, 10, and 11 in this trace respectively. The ACKs of segments 1 – 6 are No. 6, 9, 12, 14, 15, and 16 in this trace.

	Sent time	ACK Received time	RTT (seconds)
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 second
EstimatedRTT after the receipt of the ACK of segment 2:
EstimatedRTT = 0.875 * 0.02746 + 0.125 * 0.035557 = 0.0285
EstimatedRTT after the receipt of the ACK of segment 3:
EstimatedRTT = 0.875 * 0.0285 + 0.125 * 0.070059 = 0.0337
EstimatedRTT after the receipt of the ACK of segment 4:
EstimatedRTT = 0.875 * 0.0337+ 0.125 * 0.11443 = 0.0438
EstimatedRTT after the receipt of the ACK of segment 5:
EstimatedRTT = 0.875 * 0.0438 + 0.125 * 0.13989 = 0.0558
EstimatedRTT after the receipt of the ACK of segment 6:
EstimatedRTT = 0.875 * 0.0558 + 0.125 * 0.18964 = 0.0725 second



Segments 1-6



ACK of Segments 1-6