CSC 265 Lab Assignment 4

Due on 11/24/2017 11:59pm

1. UDP Packages

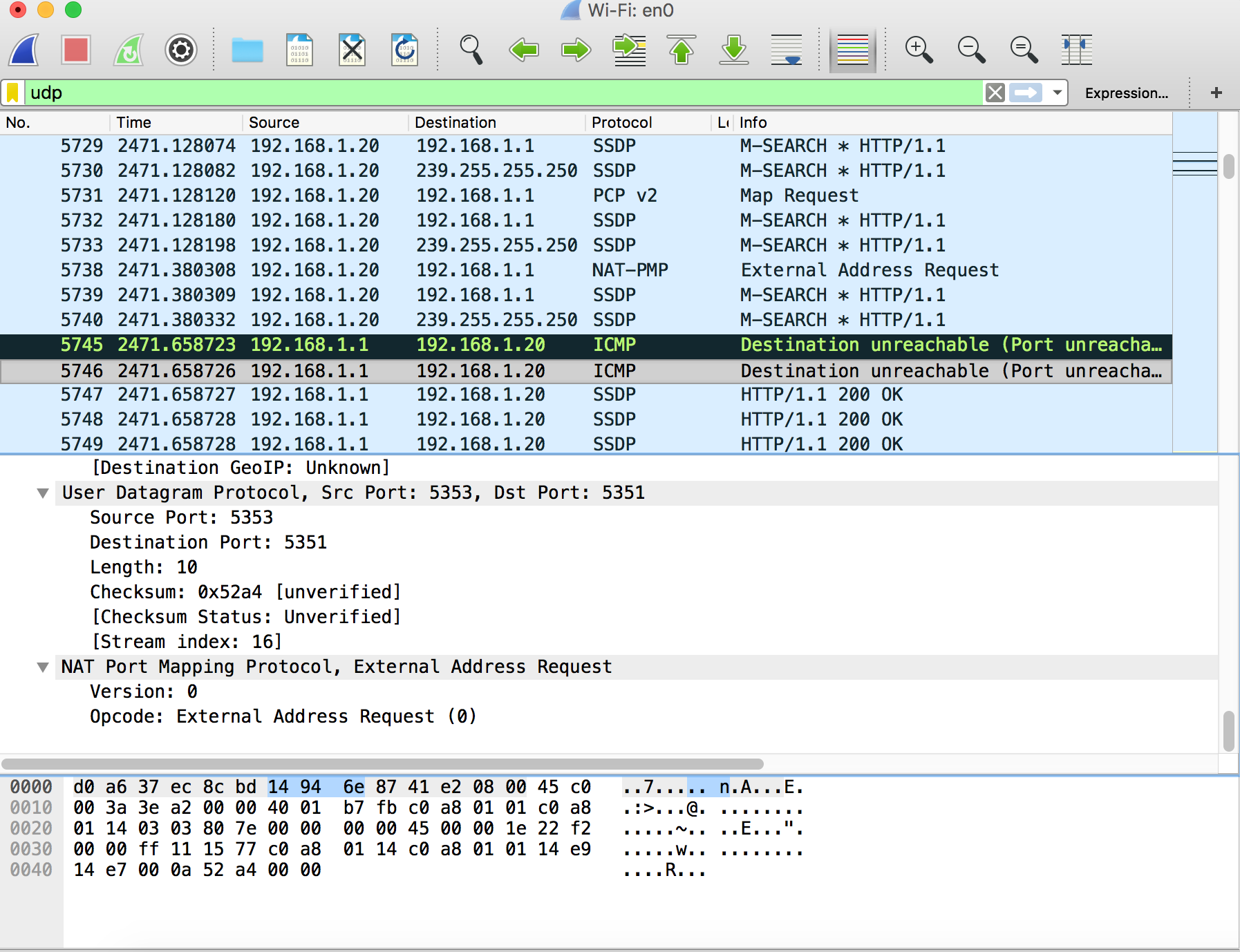
Start capturing packets in Wireshark and then do something that will cause your host to send and receive several UDP packets. (You can run the simple UDP client/server program we did in class). It’s also likely that just by doing nothing (except capturing packets via Wireshark) that some UDP packets sent by others will appear in your trace.

After stopping packet capture, set your packet filter so that Wireshark only displays the UDP packets sent and received at your host. Pick one of these UDP packets and expand the UDP fields in the details window.

Answering the following questions. NOTE: YOU NEED TO PROVIDE YOUR SCREENSHOTS

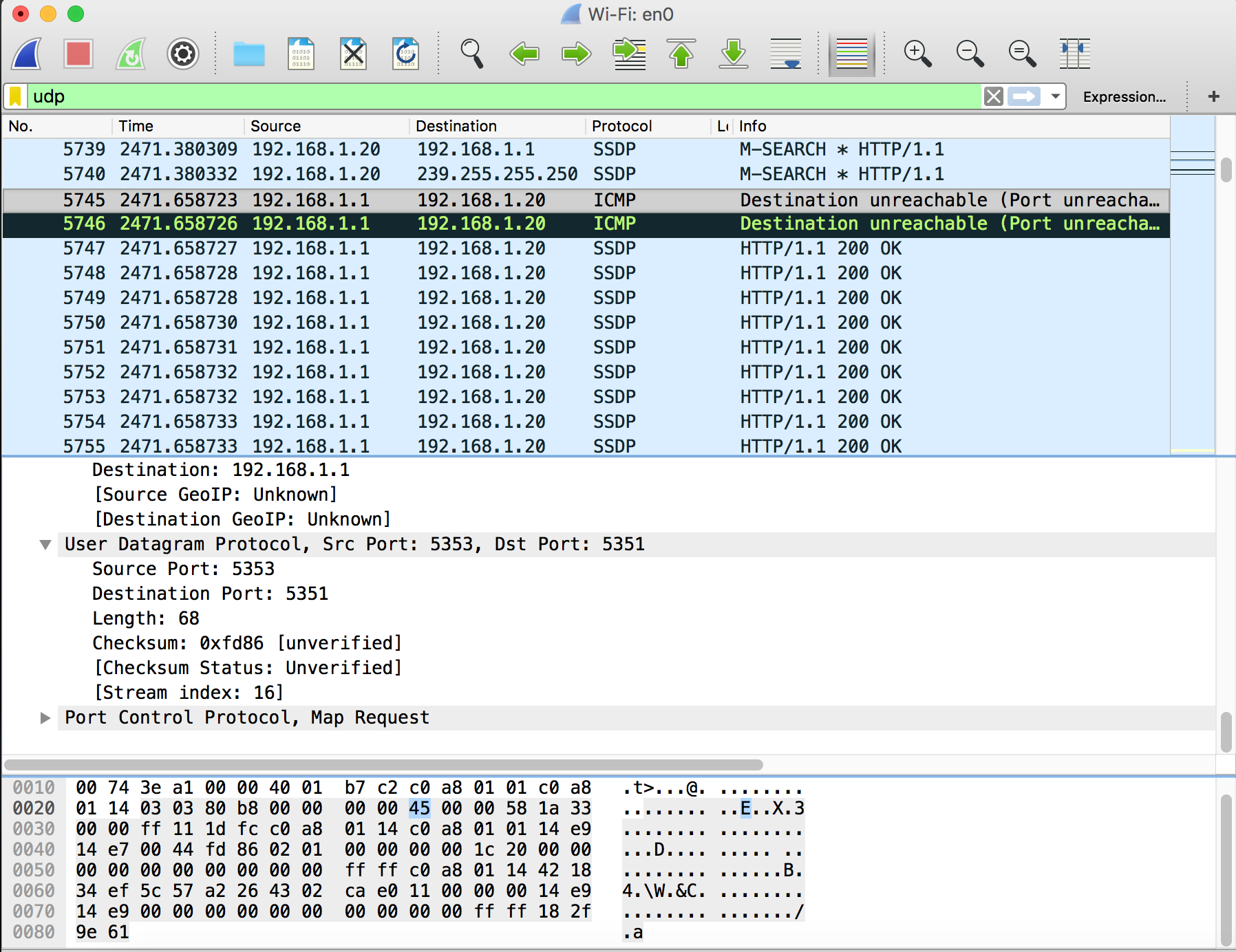
1. Select *one* UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. (You shouldn’t look in the textbook! Answer these questions directly from what you observe in the packet trace.) Name these fields.

The four headers are: source port, destination port, length and checksum.



1. By consulting the displayed information in Wireshark’s packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.

The length of each of the UDP header fields are 20 bytes long.



1. The value in the Length field is the length of what? (You can consult the text for this answer). Verify your claim with your captured UDP packet.

The value in the length field is the length of 4 and is the sum of the UDP header field.

1. What is the maximum number of bytes that can be included in a UDP payload? (Hint: the answer to this question can be determined by your answer to 2. above)

The maximum number of bytes that can be included in a UDP payload is 65535 minus the header bytes. Which would be 65535 - 8 = 65527 bytes .

1. What is the largest possible source port number? (Hint: see the hint in 4.)

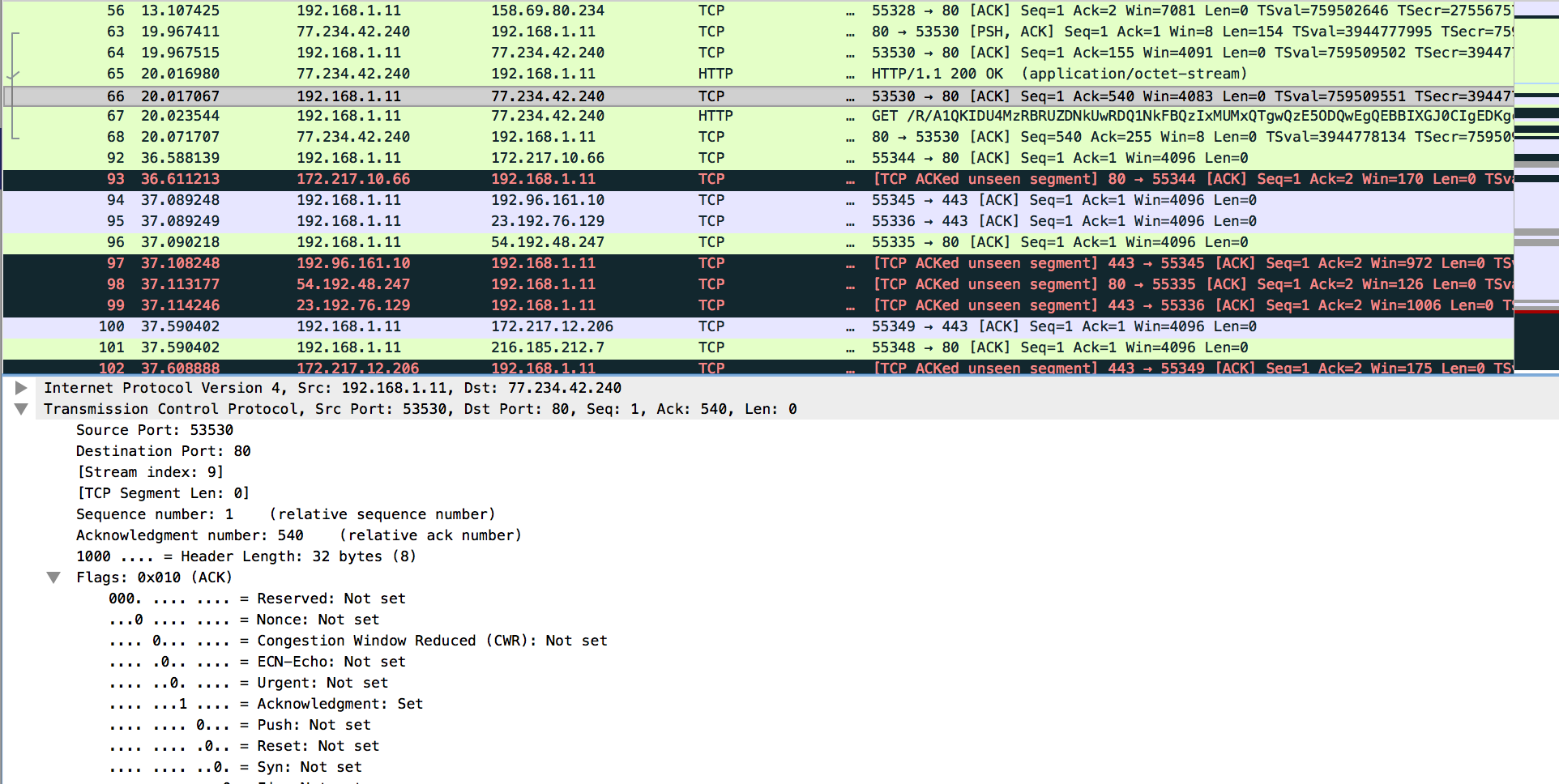
Largest possible source port number is 65535 .

2. TCP Packages

Start capturing packets in Wireshark. Run the simple TCP client/server program we did in class. Send some messages from your client to server. After stopping packet capture, set your packet filter so that Wireshark only displays the TCP packets sent and received at your host. Pick one of these TCP packets and expand the TCP fields in the details window.

Answer the following questions for the TCP segments:

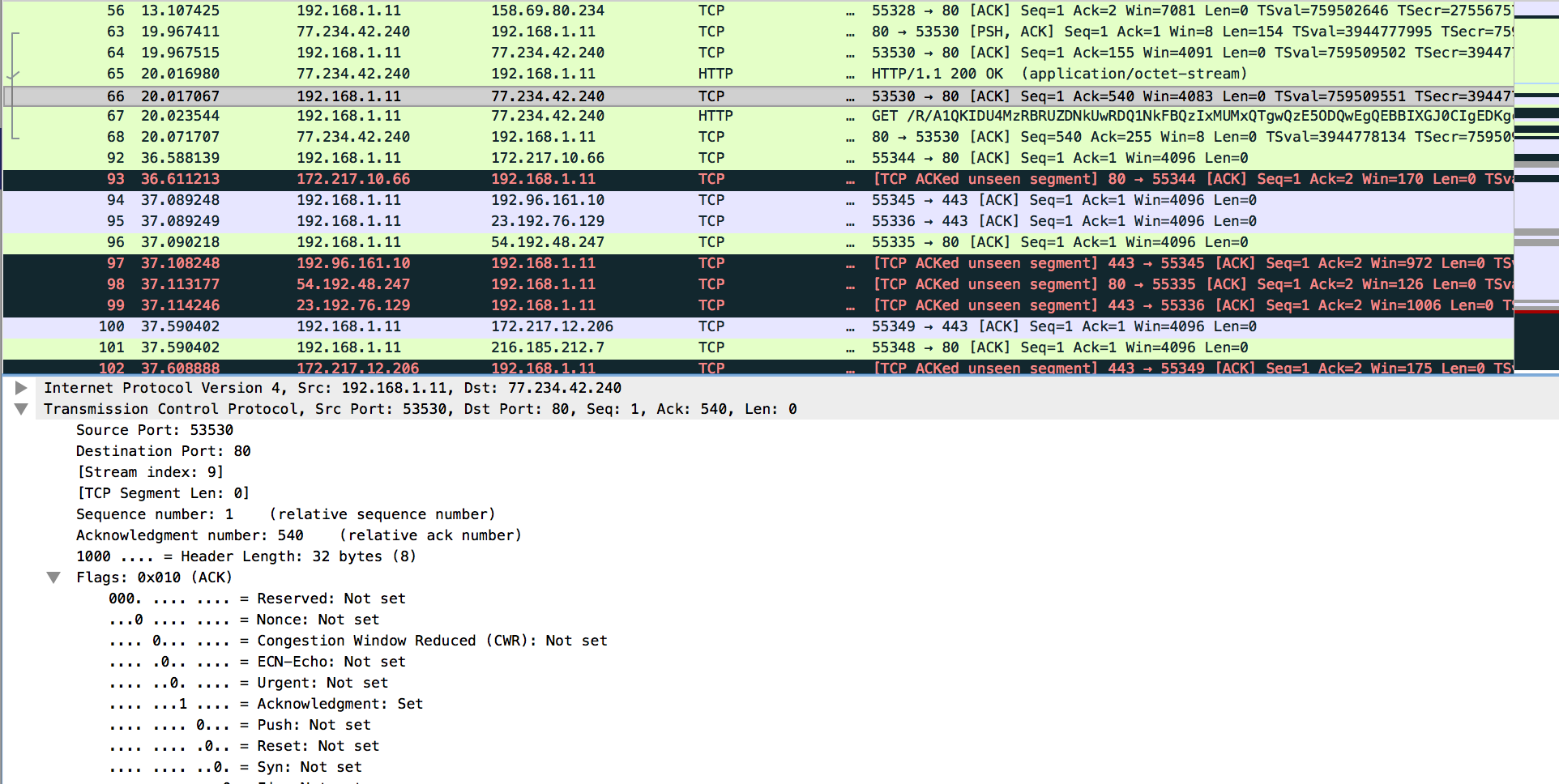
1. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client and server? What is it in the segment that identifies the segment as a SYN segment?



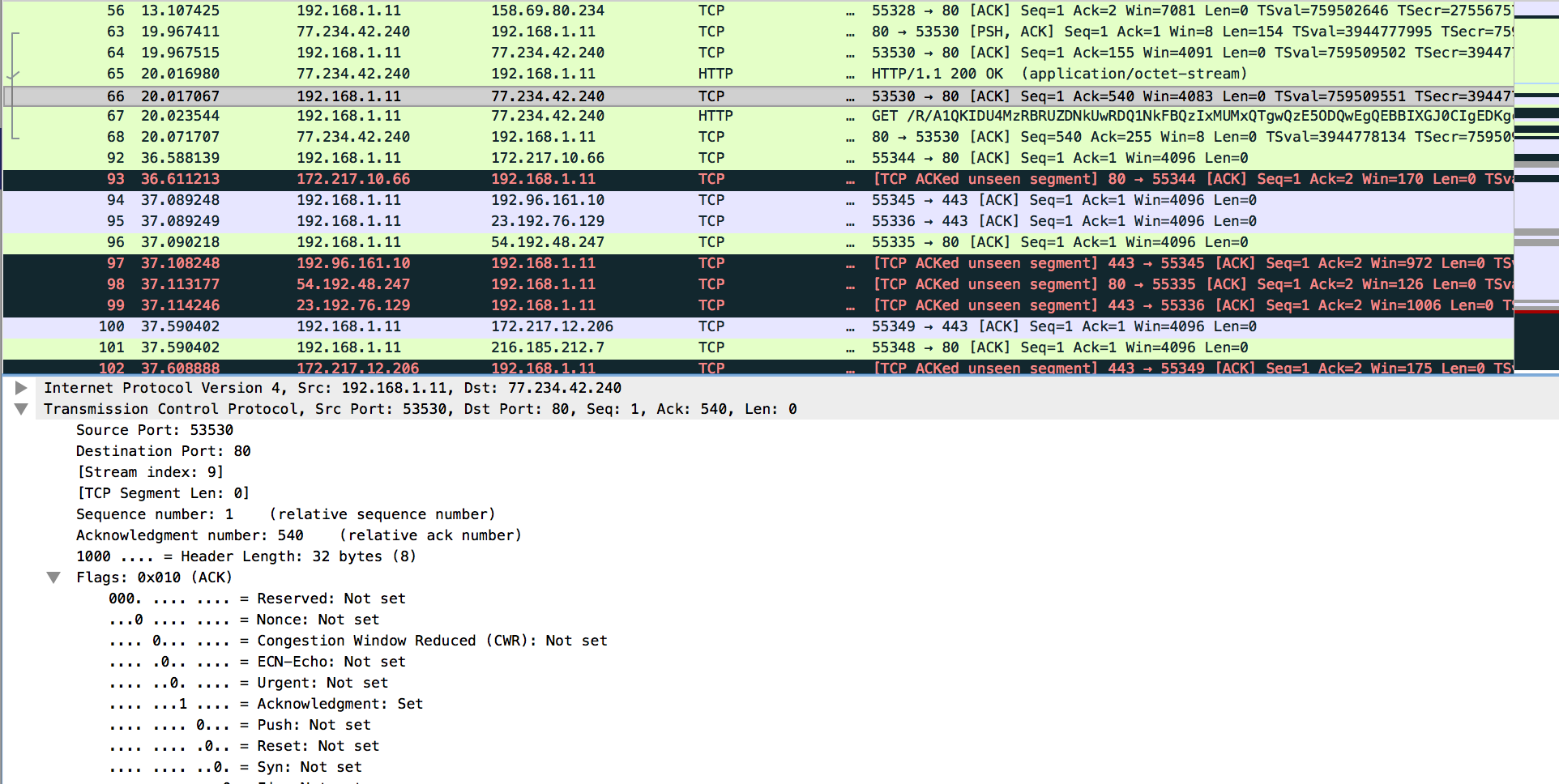
The sequence number of the TCP SYN segment that is 0. Since the initiate the TCP Connection between the client computer and www.lensdiscounters.com. The SYN flag is set to be 0 that identifies that the segment as a SYN segment.

1. What is the sequence number of the SYNACK segment sent by server to the client computer in reply to the SYN?

The Sequence number of the SYNACK segment sent by www.lensdiscounters.com to the client’s computer and the reply to the SYN is 1.



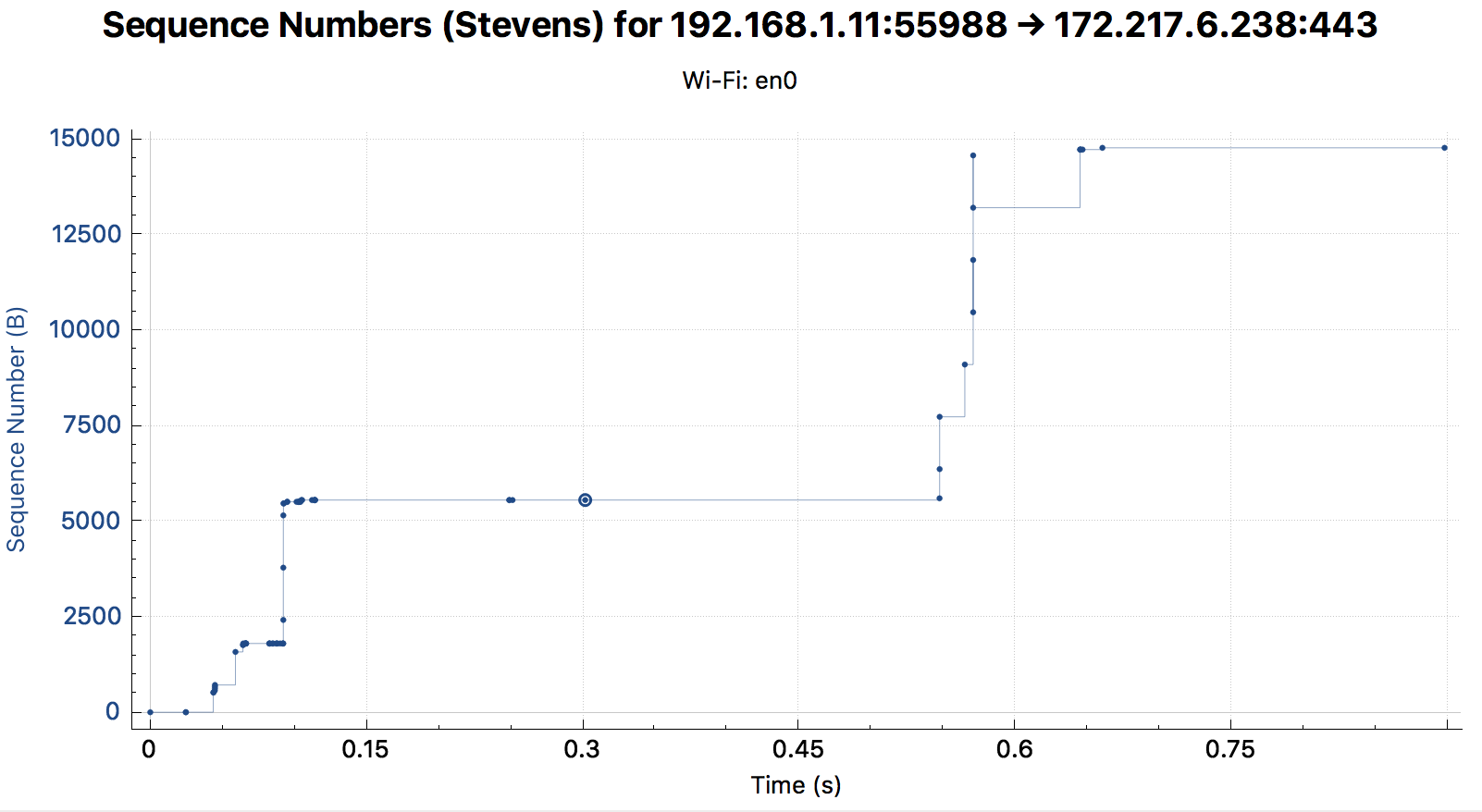
1. What is the value of the Acknowledgement field in the SYNACK segment? How did server determine that value?



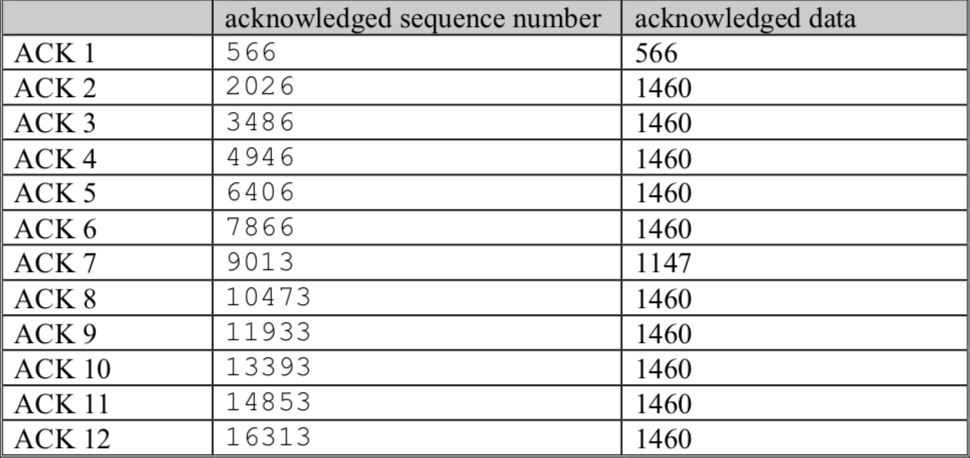
The value of the acknowledgement field is the SYNACK segment is determined by www.lensdiscounters.com .

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

There is not retransmitted segment in the trace file. The way to verify is to check the sequence of the number in Time-Sequence-Graph (stevens). A Trace the graph that sequence number from (192.168.1.11) to the destination (172.217.6.238) it increases with the change to time. The retransmitted segment is sequence by the retransmitted segment should get smaller then any other closest segment.



1. 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 Amount data that the receiver typically acknowledge in an ACK is indicate by the data received by the server betwee­­­n acknowledged sequence number and acknowledged data. The way to check the amount of acknowledged data by each ACK’s is to cases where the receiver is ACKs every other segment.­

