**HỌ TÊN : NGUYỄN XUÂN TRỰC**

**MSSV : 1513804**

======================o0o======================

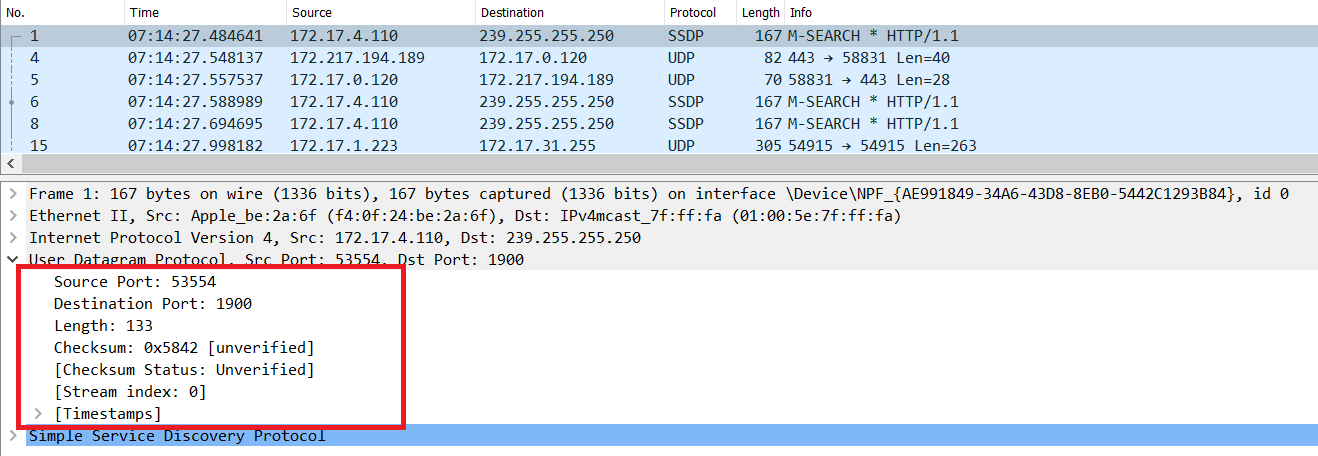
**LAB\_3A**

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.

**SOLUTION**

UDP header contains 4 fields:

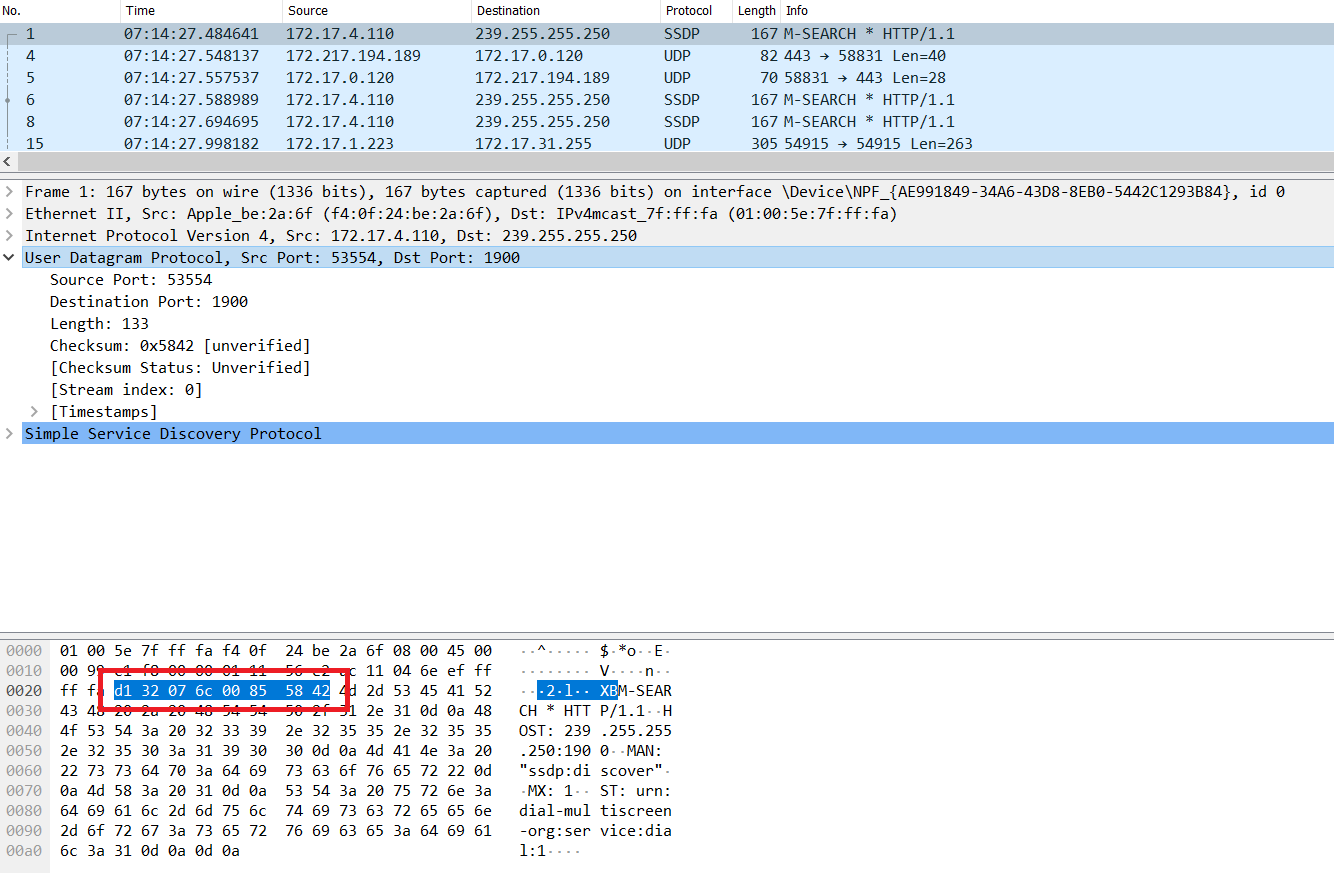
* Source Port
* Destination Port
* Length
* Checksum



2) 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.

**SOLUTION**

The UDP header has a fixed length of 8 bytes. Each of these 4 header fields is 2 bytes long.

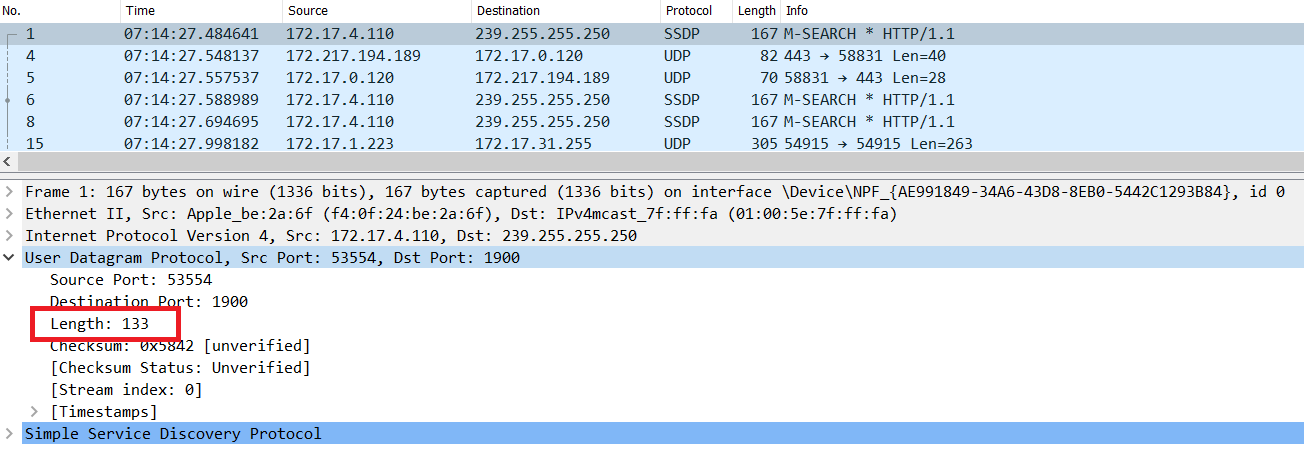


3) The value in the Length field is the length of what? (You can consult the text for this answer). Verify your claim with your captured UDP packet.

**SOLUTION**

The length field specifies the number of bytes in the UDP segment (header plus data). An explicit length value is needed since the size of the data field may differ from one UDP segment to the next.

The length of UDP payload for selected packet is 125 bytes. (133 bytes - 8 bytes = 125 bytes).



4) What is the maximum number of bytes that can be included in a UDP payload?

**SOLUTION**

The maximum number of bytes that can be included in a UDP payload is (2^16 – 1) bytes plus the header bytes. This gives 65535 bytes – 8 bytes = 65527 bytes.

5) What is the largest possible source port number?

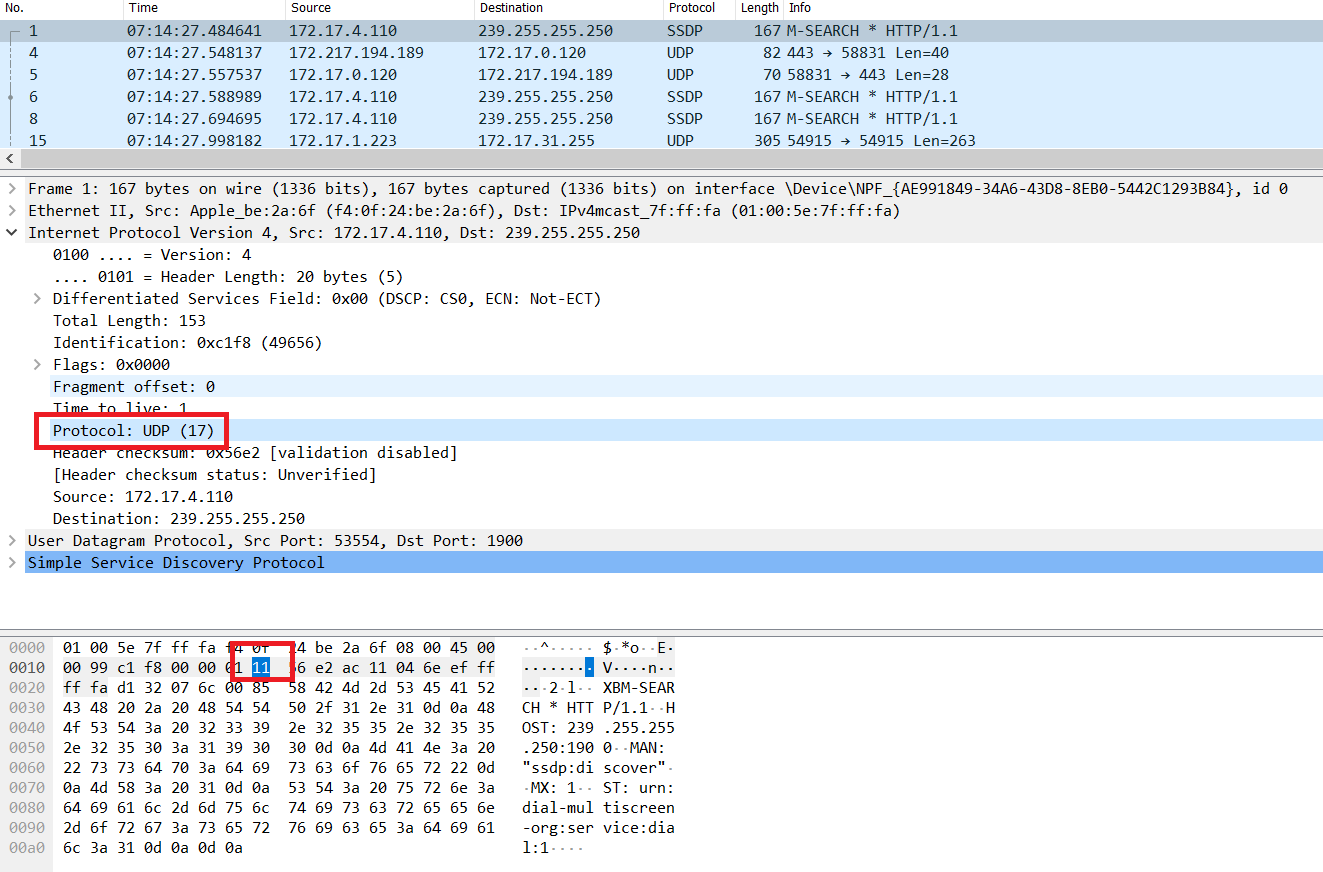
**SOLUTION**

The largest possible source port number is (2^16 – 1) = 65535.

6) What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation.

**SOLUTION**

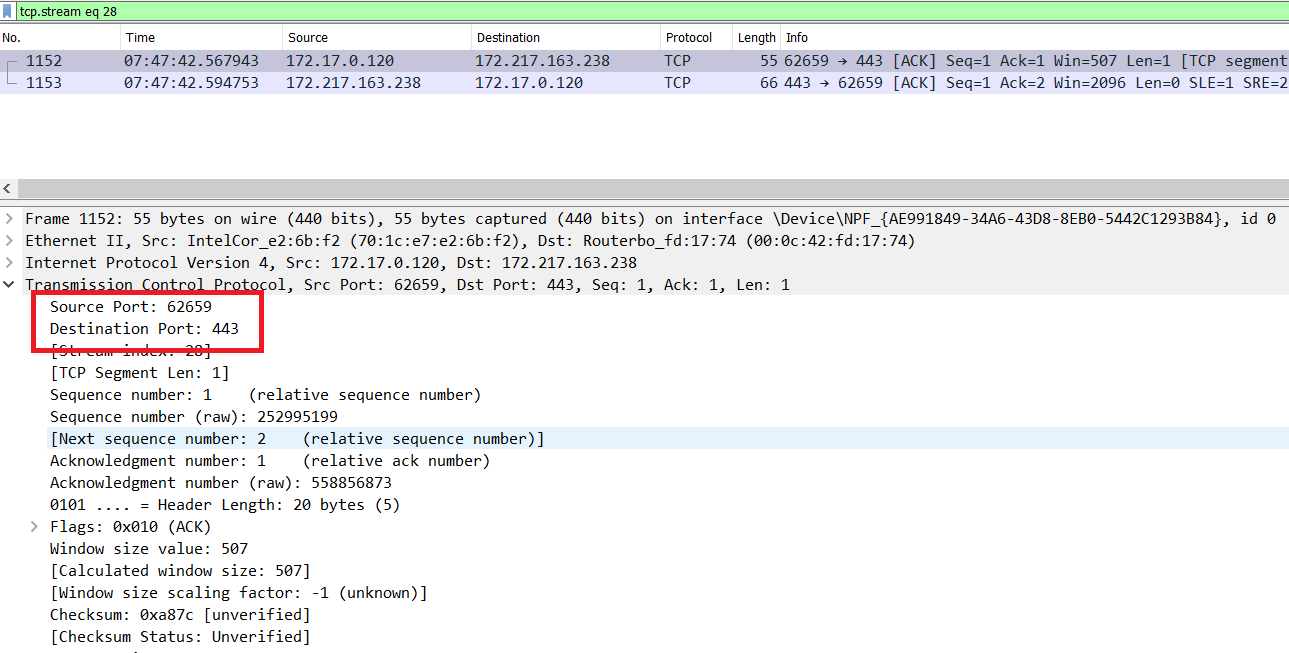
The IP protocol number for UDP is 0x11 hex, which is 17 in decimal value.

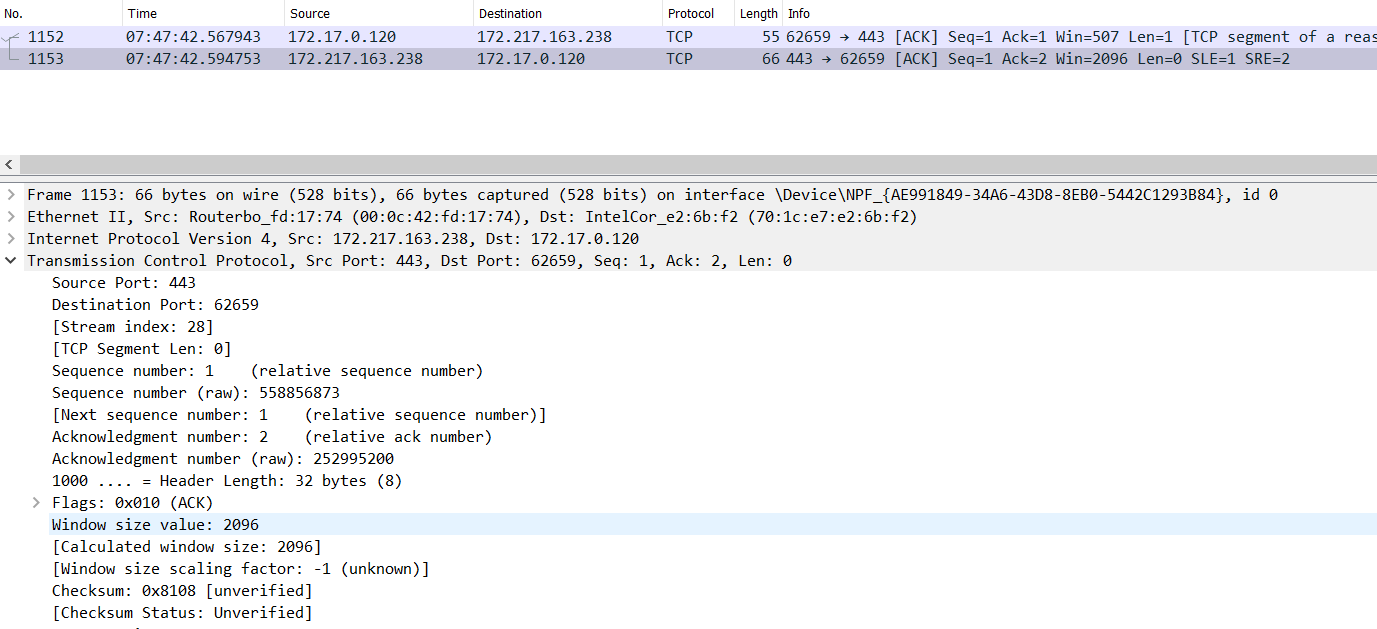


7) Examine a pair of UDP packets in which your host sends the first UDP packet and the second UDP packet is a reply to this first UDP packet.

**SOLUTION**

The source port of the UDP packet sent by the host is the same as the destination port of the reply packet, and conversely the destination port of the UDP packet sent by the host is the same as the source port of the reply packet.



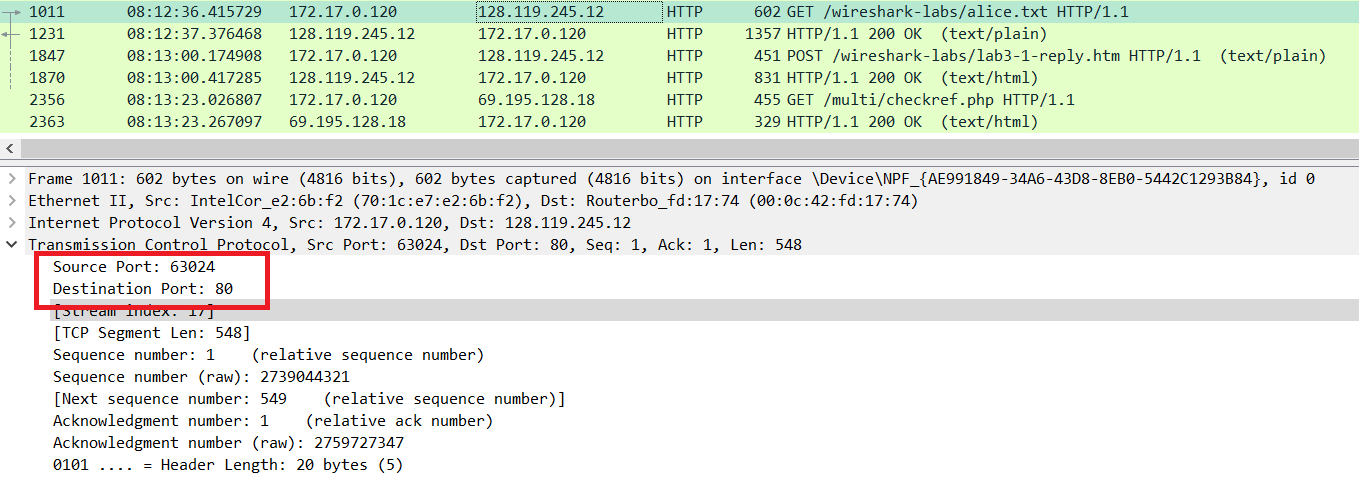


**LAB\_3B**

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.

**SOLUTION**

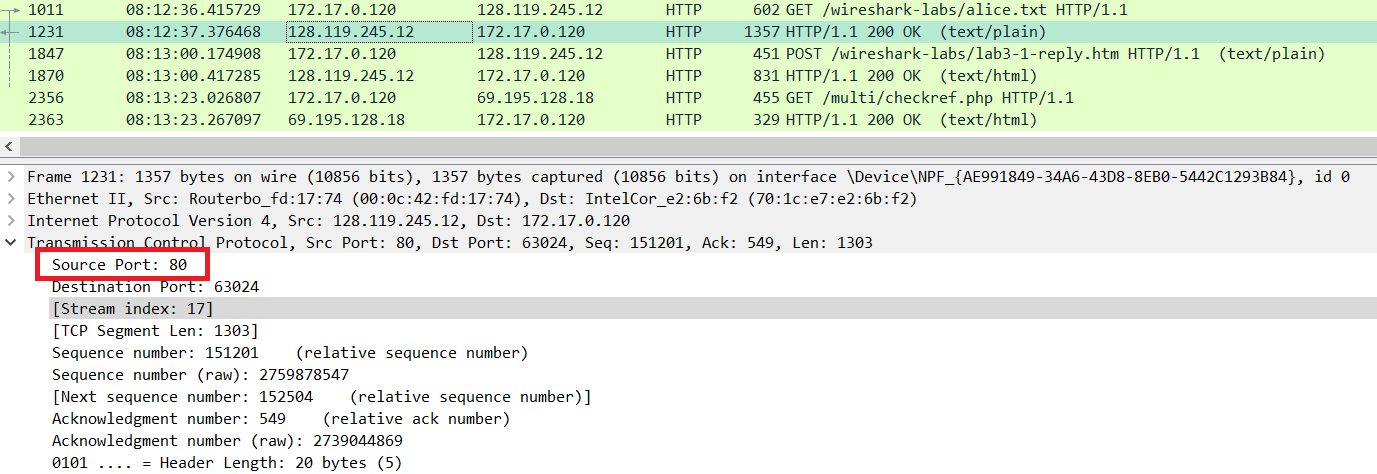
According to above figure, the client computer (source)’s IP address is 172.17.0.120.



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?

**SOLUTION**

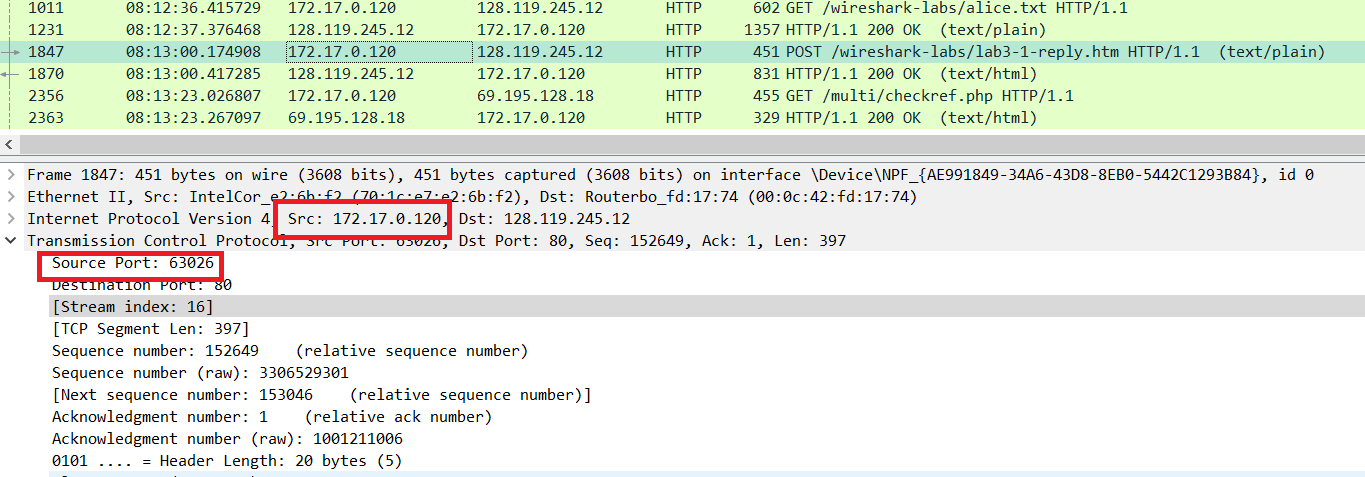
According to above figure, the IP address of gaia.cs.umass.edu is 128.119.245.12 and the TCP port number is 80.



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?

**SOLUTION**

According to above figure, my client computer’s IP address is 172.17.0.120 and the TCP port is 63026.

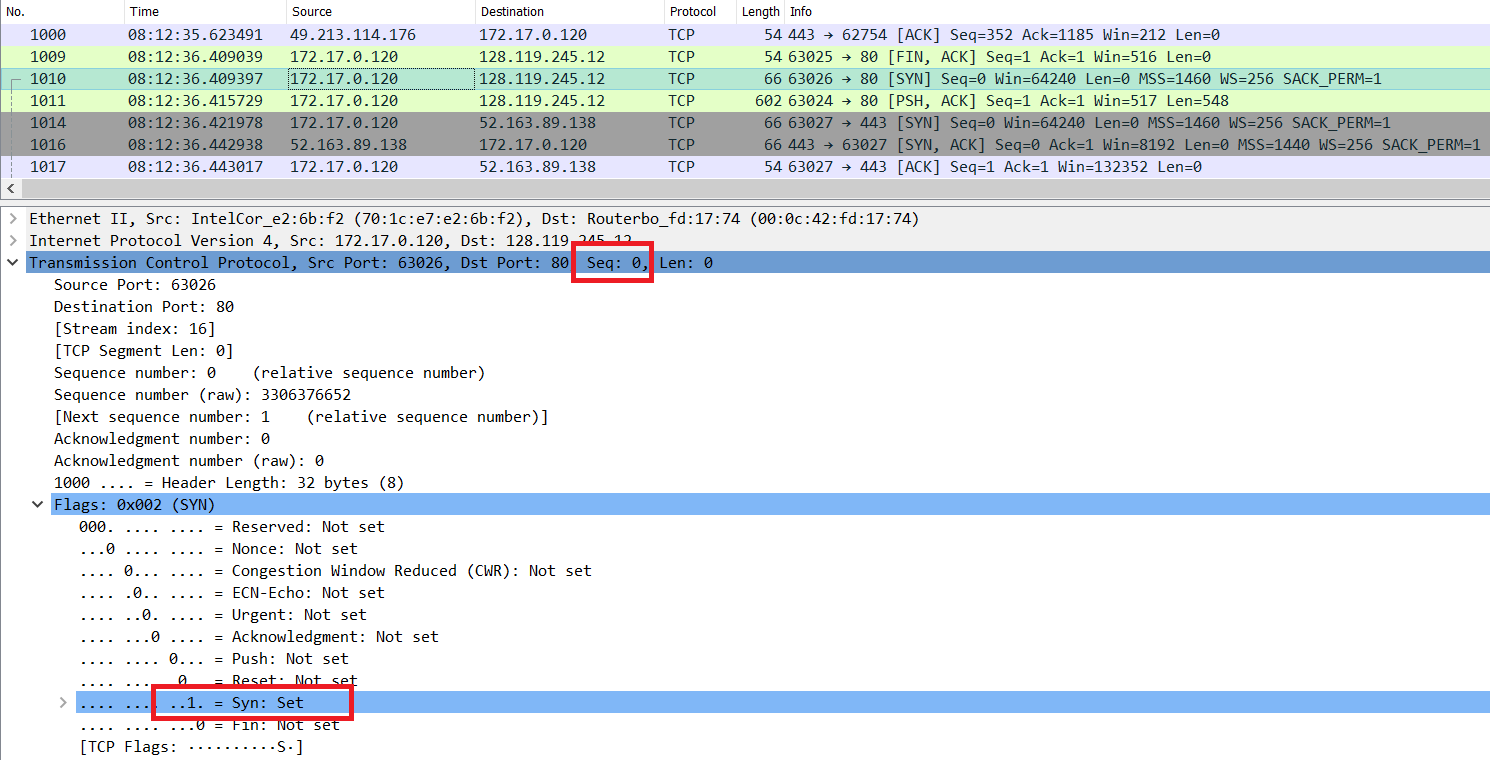


4) What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?

**SOLUTION**

The sequence number of the TCP SYN segment is 0 since it is used to imitate the TCP connection between the client computer and gaia.cs.umass.edu.

According to above figure, in the Flags section, the Syn flag is set to 1 which indicates that this segment is a SYN segment.



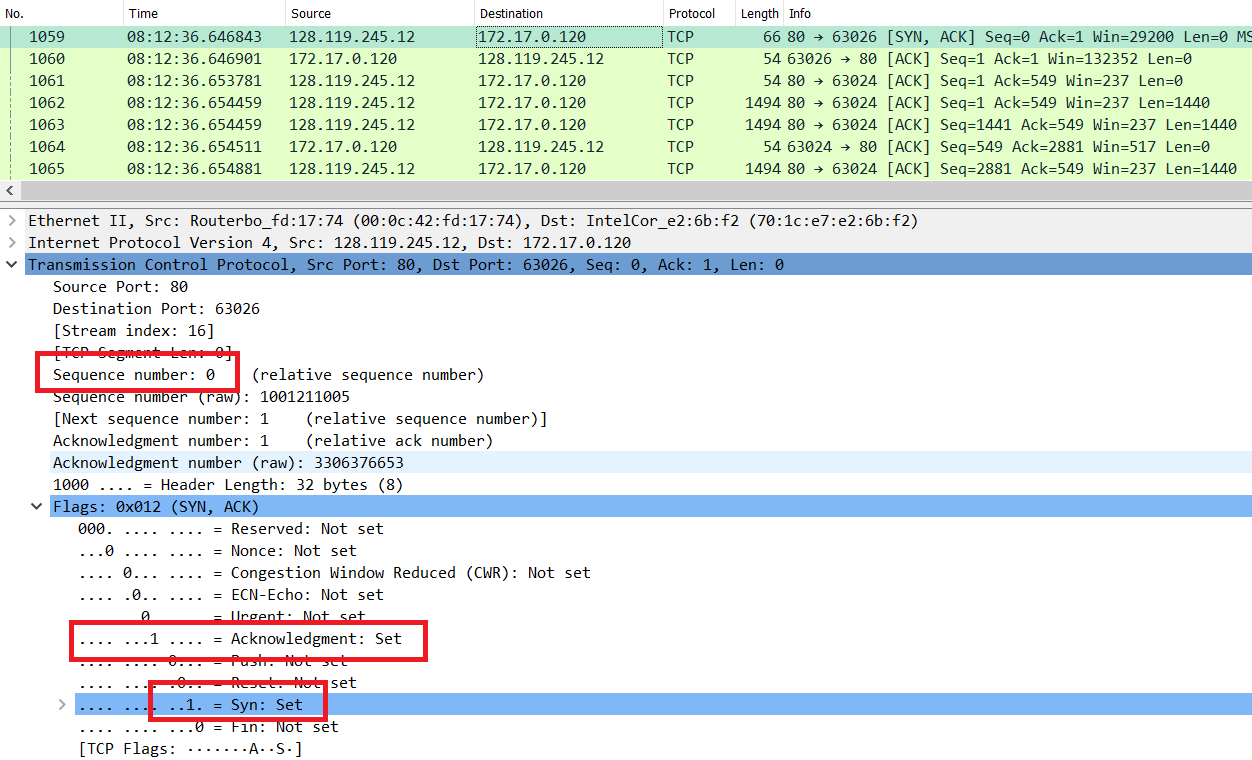
5) What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK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

**SOLUTION**

According to the above figure, the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN is 0.

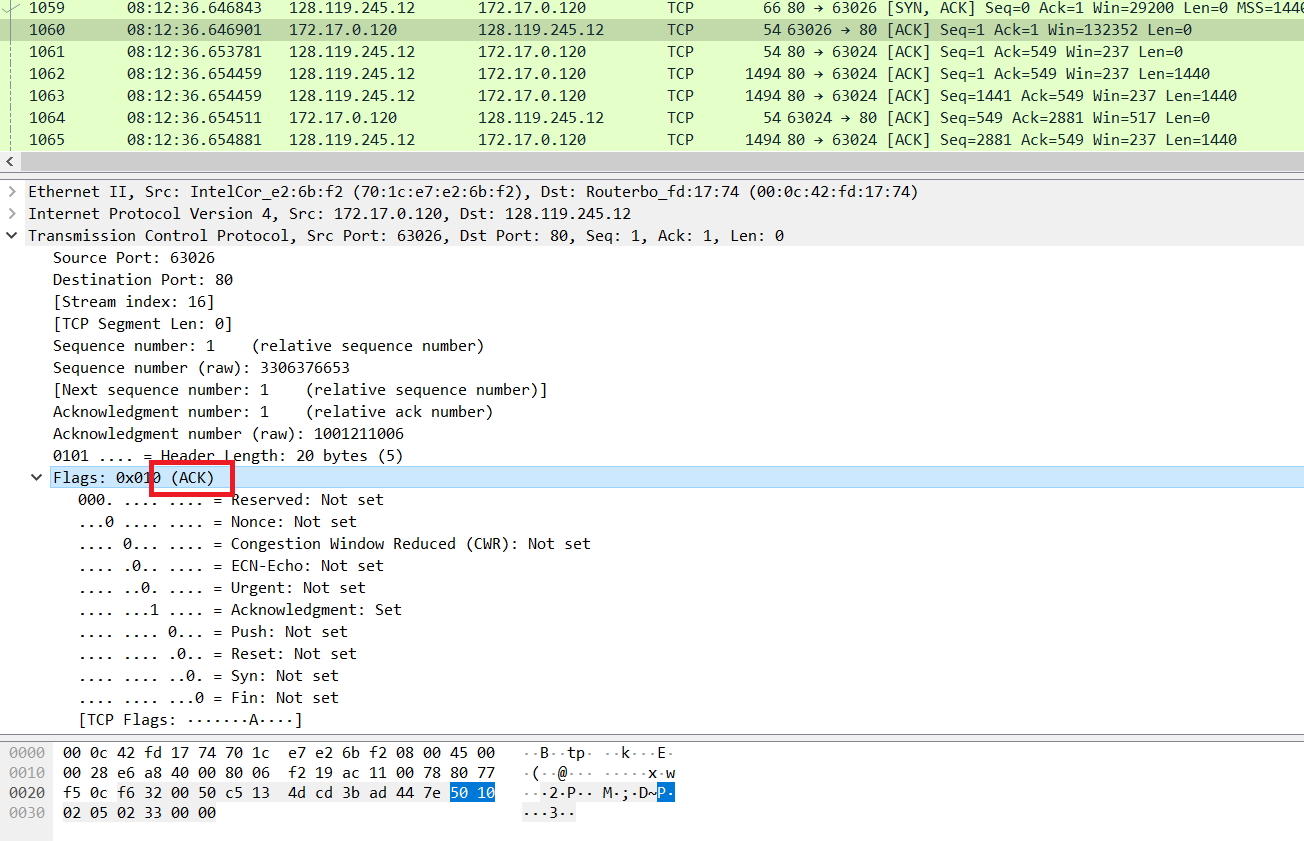
The value of the acknowledgement field in the SYNACK segment is 1. The value of the ACKnowledgement field in the SYNACK segment is determined by the server gaia.cs.umass.edu. The server adds 1 to the initial sequence number of SYN segment form the client computer. For this case, the initial sequence number of SYN segment from the client computer is 0, thus the value of the ACKnowledgement field in the SYNACK segment is 1.

A segment will be identified as a SYNACK segment if both SYN flag and Acknowledgement in the segment are set to 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.

**SOLUTION**



According to above figure, the segment No.1060 contains the HTTP POST command, the sequence number of this segment is 1.