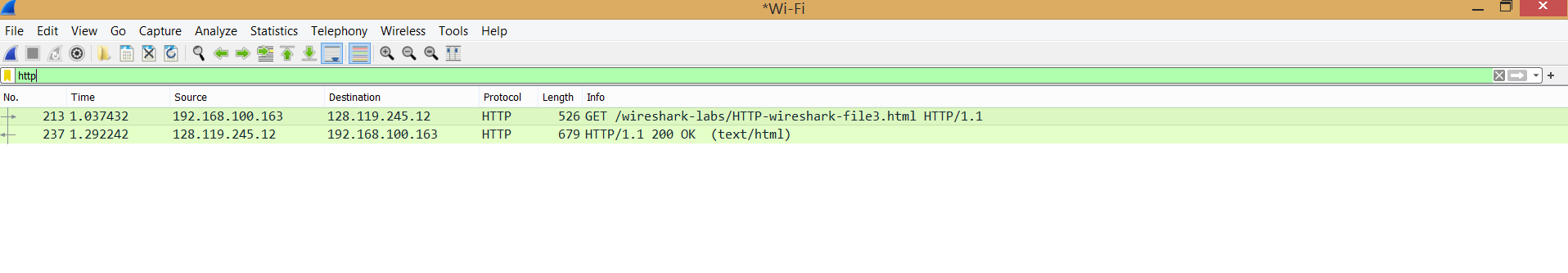
**CN LAB 06**

**SUBMITTED BY: AYESHA ZIA(20K-0414)**

**LAB TASK#1**

**Answer the following questions:**

**1. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?**

1 GET Message was sent by the browser. The packet number is 213.

**2. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?**

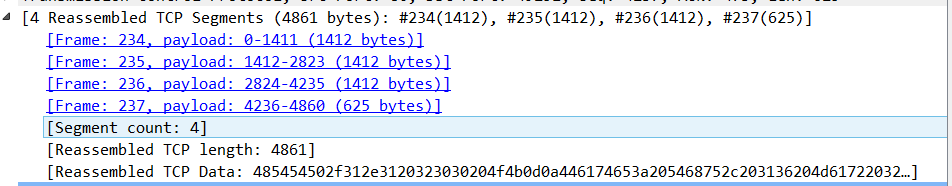
The packet 237 contains the status code and response

**3. What is the status code and phrase in the response?**

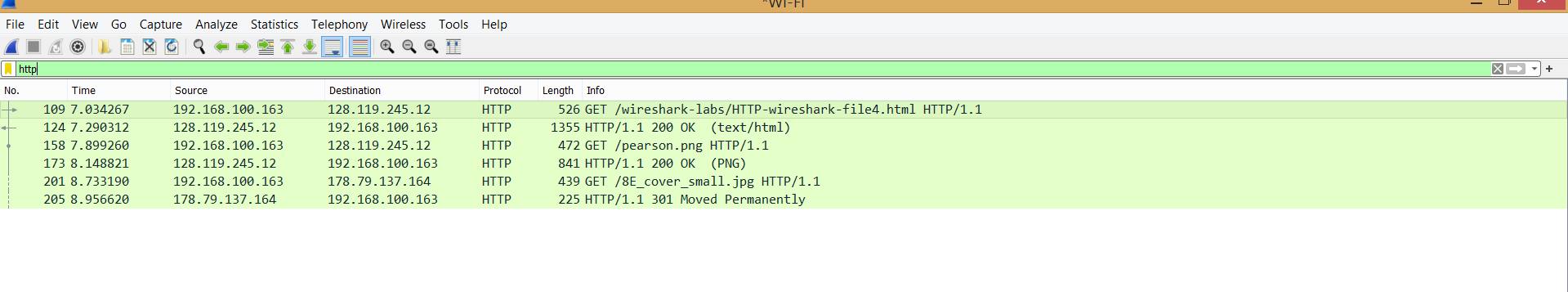
The status code is HTTP/1.1 200 OK

**4. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?**

4 segments



**LAB TASK#2**



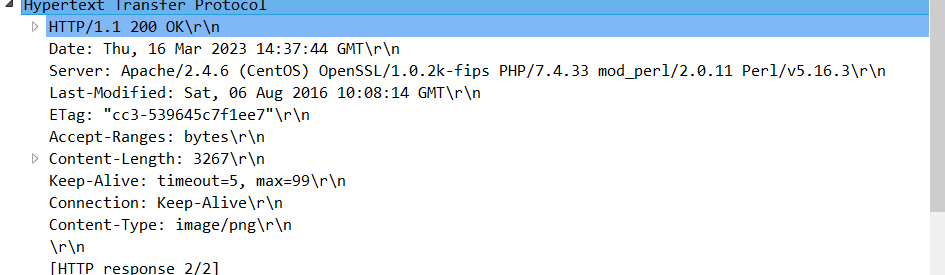
**Answer the following questions:**

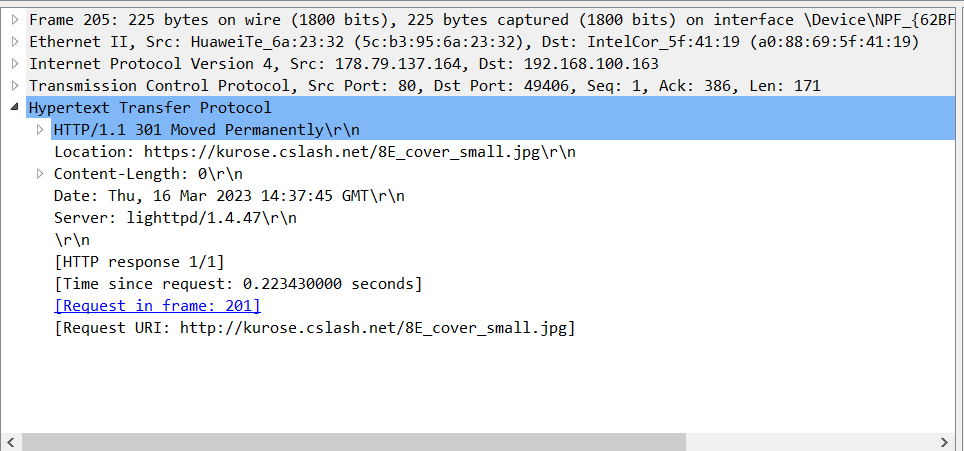
**1. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?**

3 HTTP GET request messages were sent. These were the addresses:

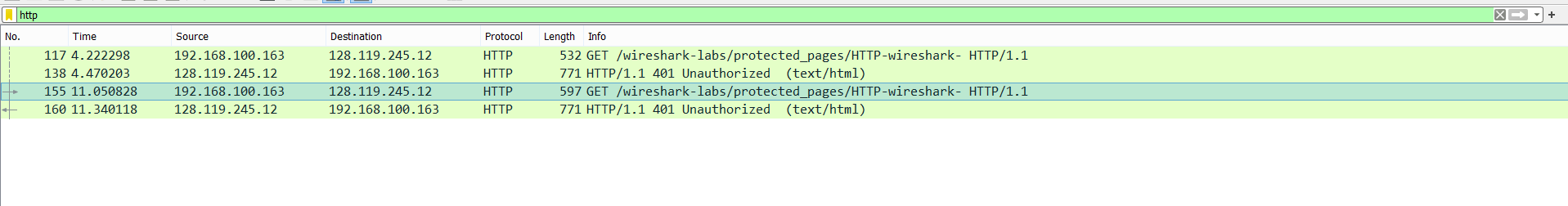
* /wireshark-labs/HTTP-wireshark-file4.html
* /pearson.png
* /BE\_cover\_small.jpefg

**2. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.**





Since the response for both the images is at nearly the same timestamp, we can say that the browser downloaded the websites in parallel.

 **LAB TASK#3**

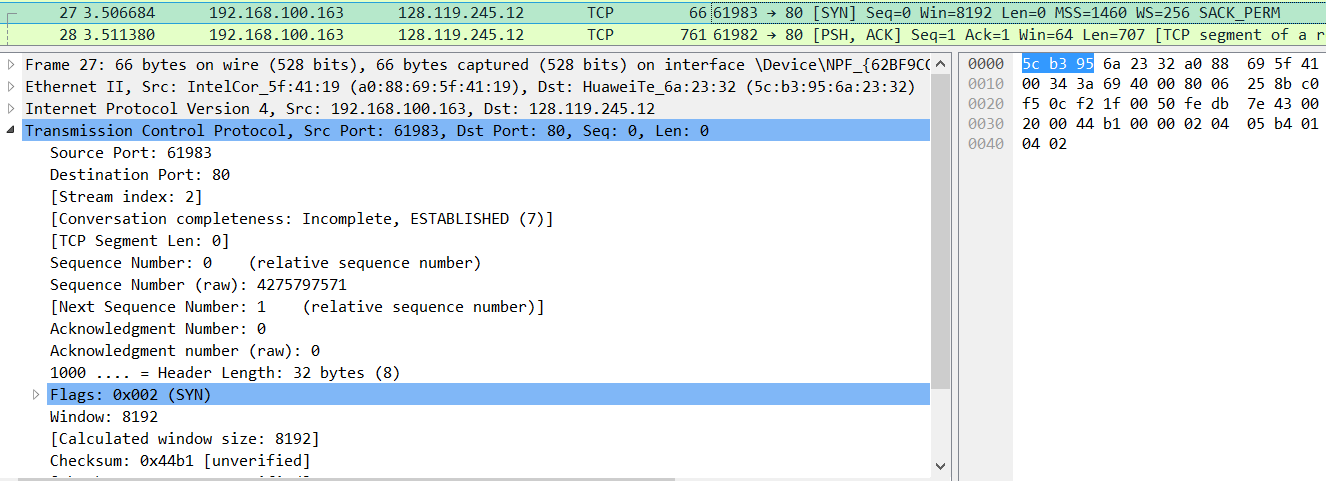
**16. What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser?**

The status code and phrase is HTTP/1.1 Unauthorized

**17. When your browser’s sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?**

No new field is included as the username and password entered in incorrect

**LAB TASK#4**



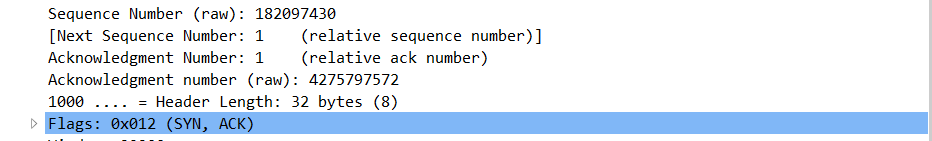
**3. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?**

The sequence number(relative) is 1 while raw sequence number is 4275797571. The following flag identifies the SYN segment

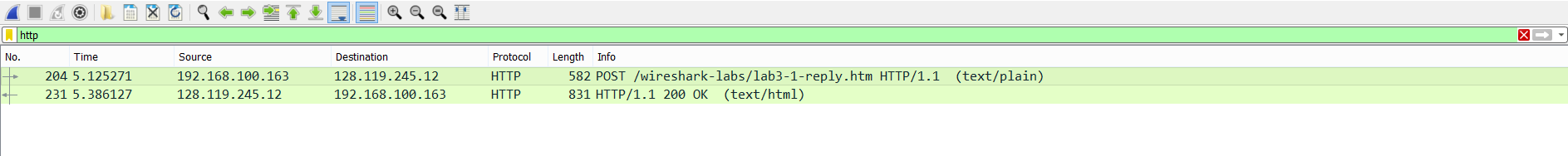


**4. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a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

The sequence number(relative) is 1 while raw sequence number is 182097430. The acknowledgement value is 4275797572. The flag(SYN,ACK) identifies it as SYNACK segment.

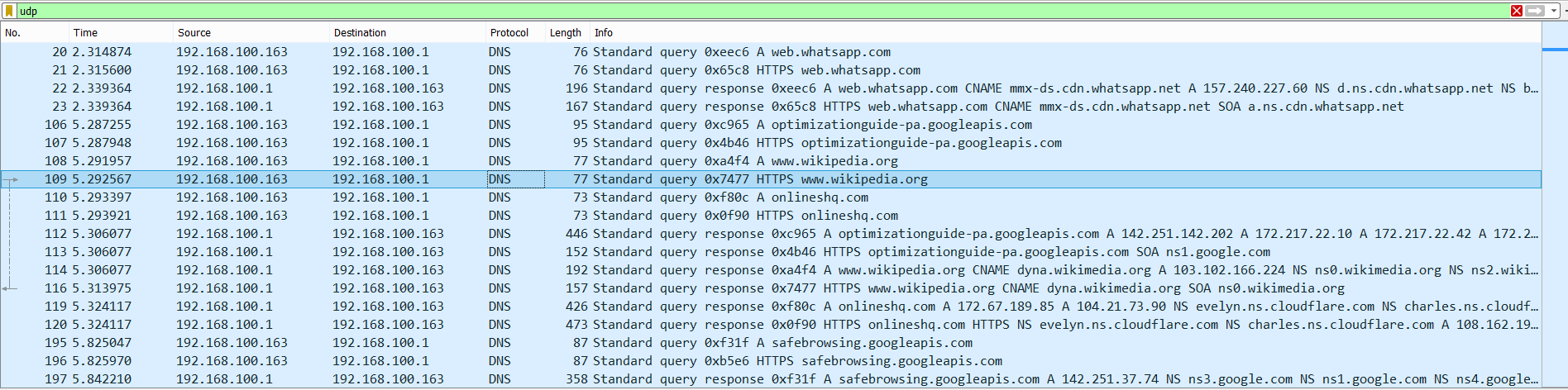


**5. What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command, you’ll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a “POST” within its DATA field.**



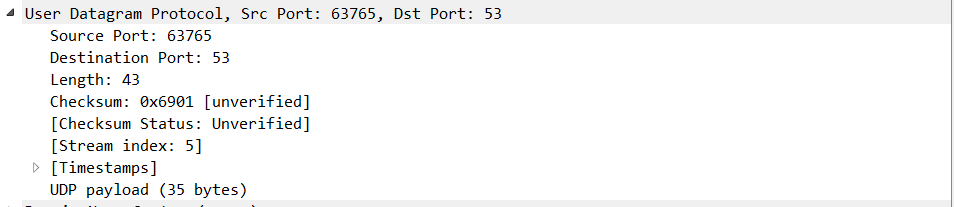


The sequence number(relative) is 152499 while raw sequence number is 197222267.

**LAB TASK#5**

**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 fields made are:

* 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.**

The length of each of the header fields in the UDP header field is 2 bytes.

**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.**

It is the length of the captured packet.



**4. 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 size of the UDP payload can be the maximum size of an IP packet, which is 65,535 bytes.

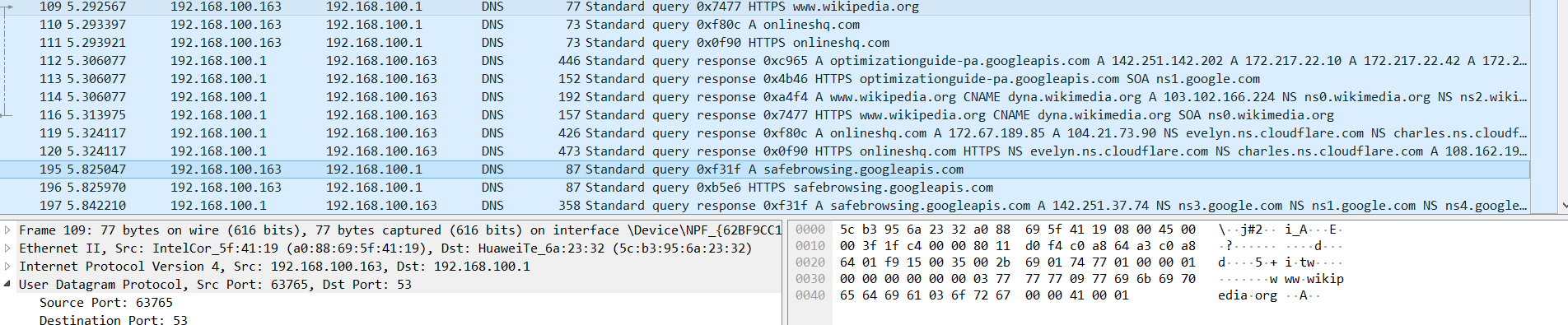
**5. What is the largest possible source port number? (Hint: see the hint in 4.)**

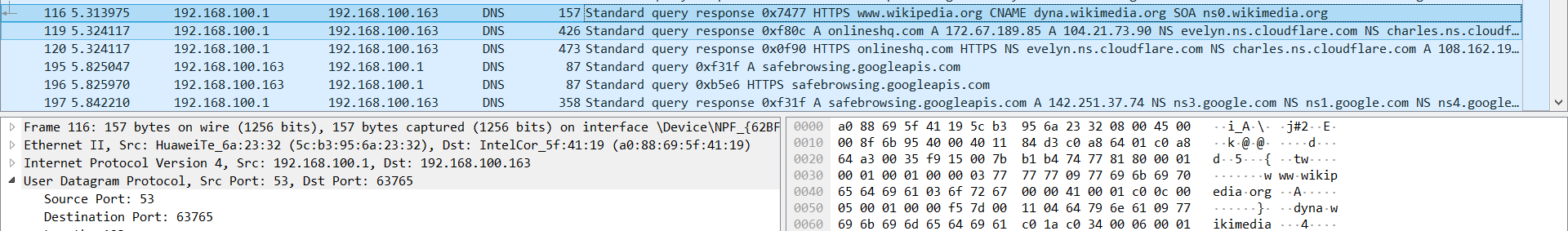
65,535 bytes can be the largest possible source port number.

**6. What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation. To answer this question, you’ll need to look into the Protocol field of the IP datagram containing this UDP segment (see Figure 4.13 in the text, and the discussion of IP header fields).**



In decimal notation, the protocol number is 17 while in hexadecimal notation, the protocol number for UDP is 0x11.

**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. (Hint: for a second packet to be sent in response to a first packet, the sender of the first packet should be the destination of the second packet). Describe the relationship between the port numbers in the two packets.**

The relation between the port numbers is that the source port of the first request packet becomes the destination port of the second packet in response. While the destination port of the requested first packet becomes the source port in response.