NETWORK LAB

LAB ASSIGNMENT for Week # 2

Usirikayala Likhith

20223295, D2

HTTP

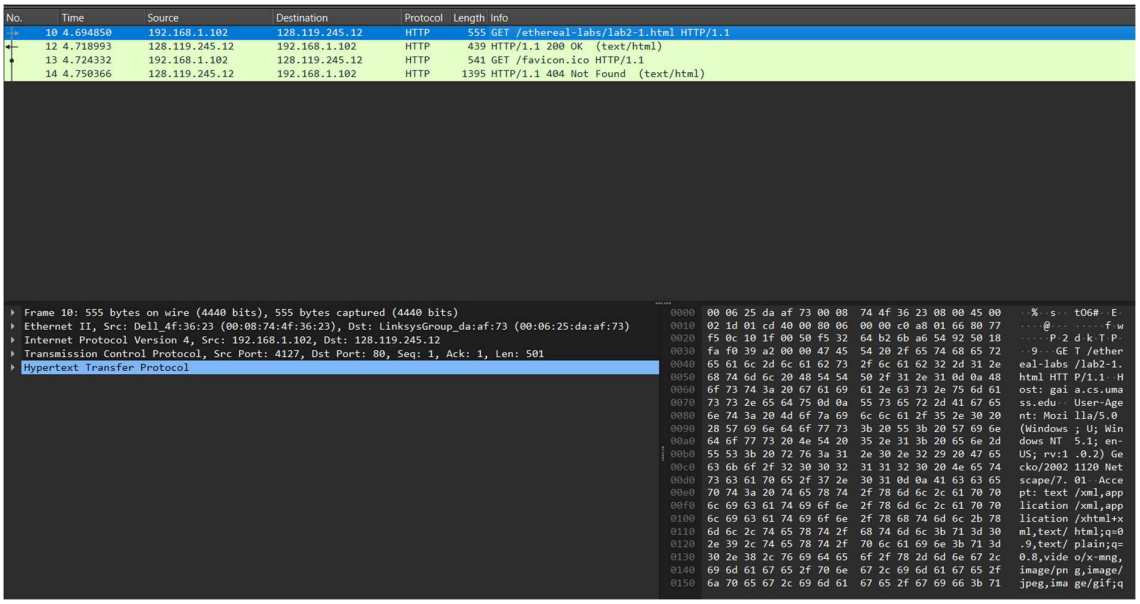
1. The Basic HTTP GET/response interaction

Note: Answer the following questions using the http-ethereal-trace-1 packet trace to answer the

questions below

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

ANS:

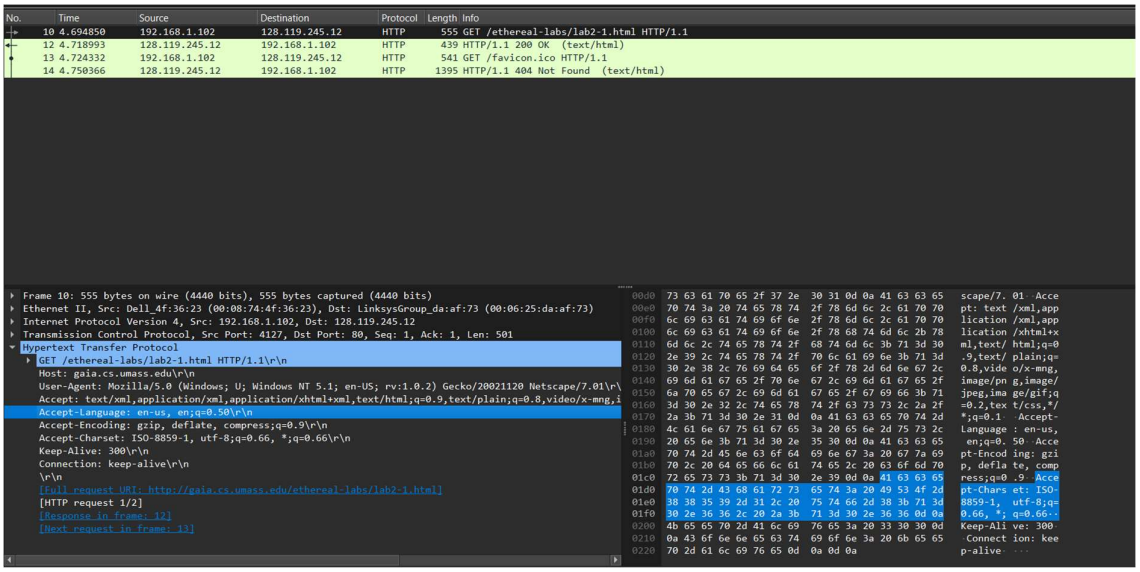


My browser is running HTTP version 1.1 and HTTP version of the server is also 1.1.

2. What languages (if any) does your browser indicate that it can accept to the server?

ANS:

American English and English of weight 0.5 were accepted by the server.



3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

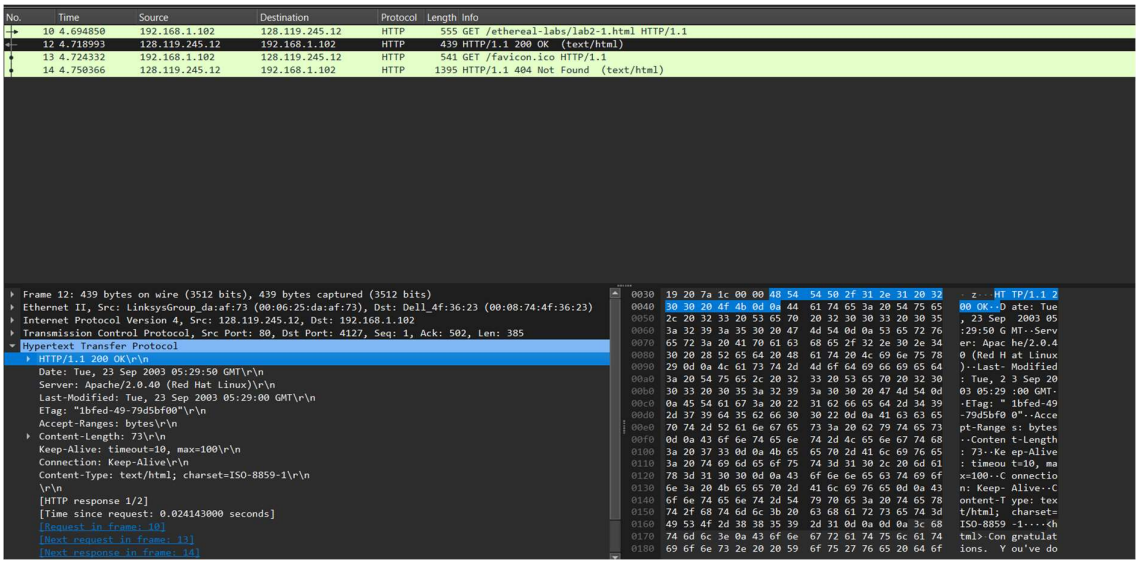
ANS:

The IP address of my computer is 192.168.1.102 and the IP address of the server is 128.119.245.12 .

4. What is the status code returned from the server to your browser?

ANS:

The Status Code returned from the server to browser is 200 OK.



5. When was the HTML file that you are retrieving last modified at the server?

ANS:

The HTML file was last modified on Tuesday , 23 September 2003 05:29:00 GMT.

6. How many bytes of content are being returned to your browser?

ANS:

73 bytes of content are being returned to my browser.

7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

ANS:

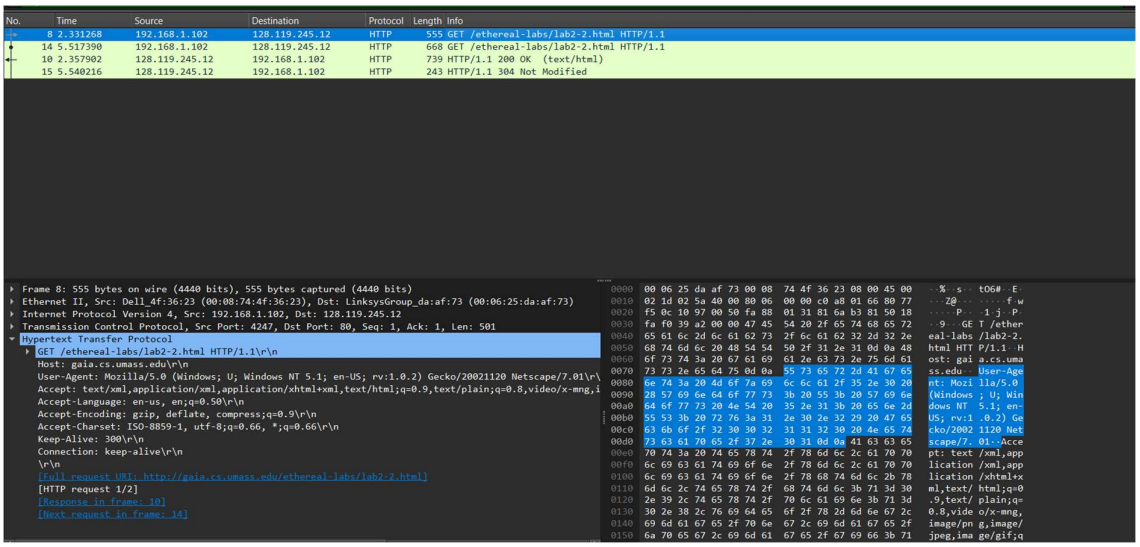
NO Additional headers were listed in raw data window.

2. The HTTP CONDITIONAL GET/response interaction

Note: Answer the following questions using the http-ethereal-trace-2 packet trace to answer the questions below

8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF□MODIFIED-SINCE" line in the HTTP GET?

ANS:

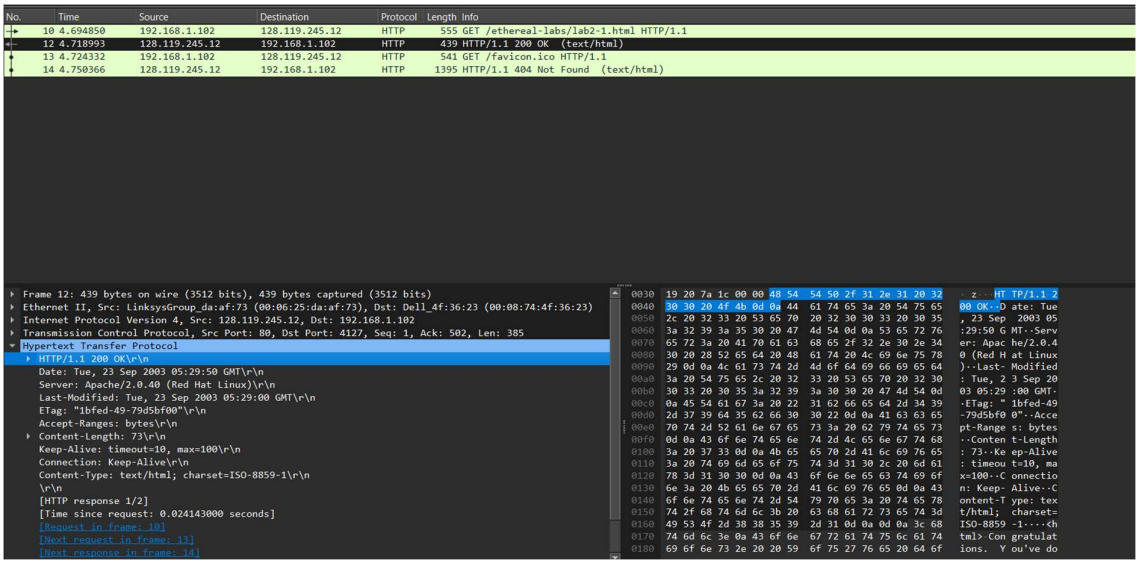


There wasn't any IF-MODIFIED SINCE line in HTTP GET.

9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

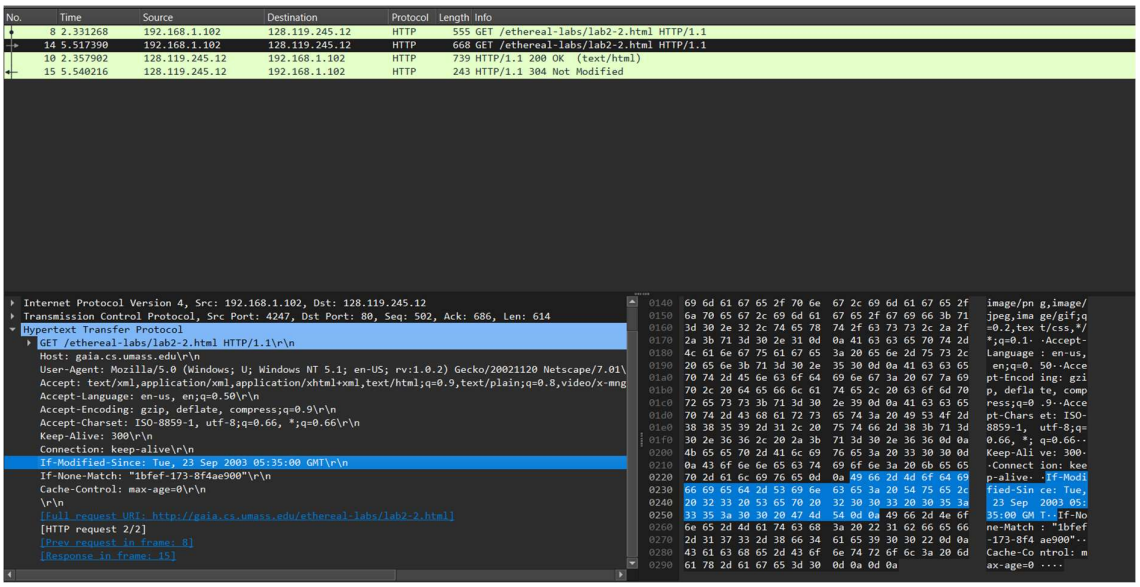
ANS:

Yes the Server explicitly return the contents of the file. The status word of the response message is 200 OK. So the server sent the response for the request that been sent .



10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET? If so, what information follows the "IF-MODIFIED-SINCE:" header?

ANS:



Yes there is an IF-MODIFIED-SINCE header in the HTTP GET. It indicates the last date and time the file has been received a response from the server. For this file the information is

Tue, 23 sep 2003 05:35:00 GMT.

11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

ANS:

The HTTP status code and phrase returned from the server in response is 304 Not Modified.

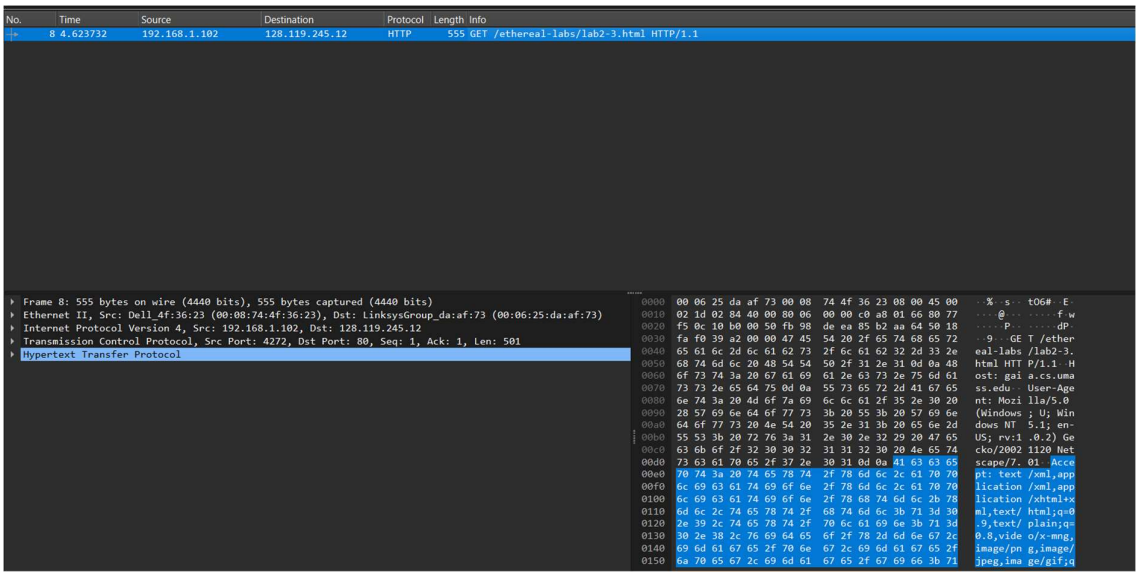
The server doesn't explicitly return the contents of the file because the file wasn't modified since the last response. So server tells to check the cache which is still valid.

3. Retrieving Long Documents

Note: Answer the following questions using the http-ethereal-trace-3 packet trace to answer the questions below

12. 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?

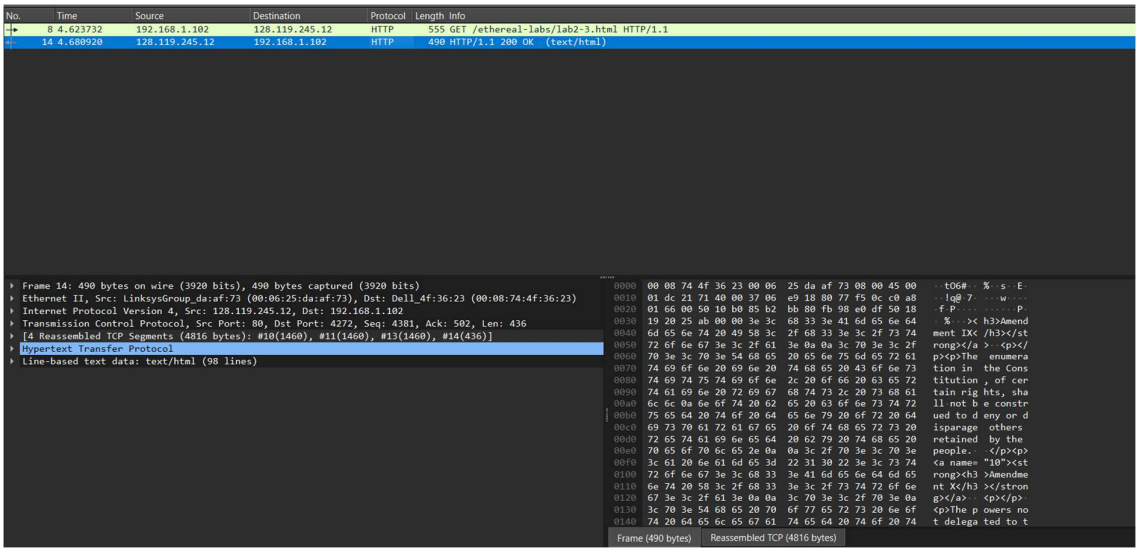
ANS:



Only one HTTP GET request has been send by the browser. The Packet number is 8.

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

ANS:



The packet number is 14 which contains the status code and phrase associated with the response for HTTP GET request

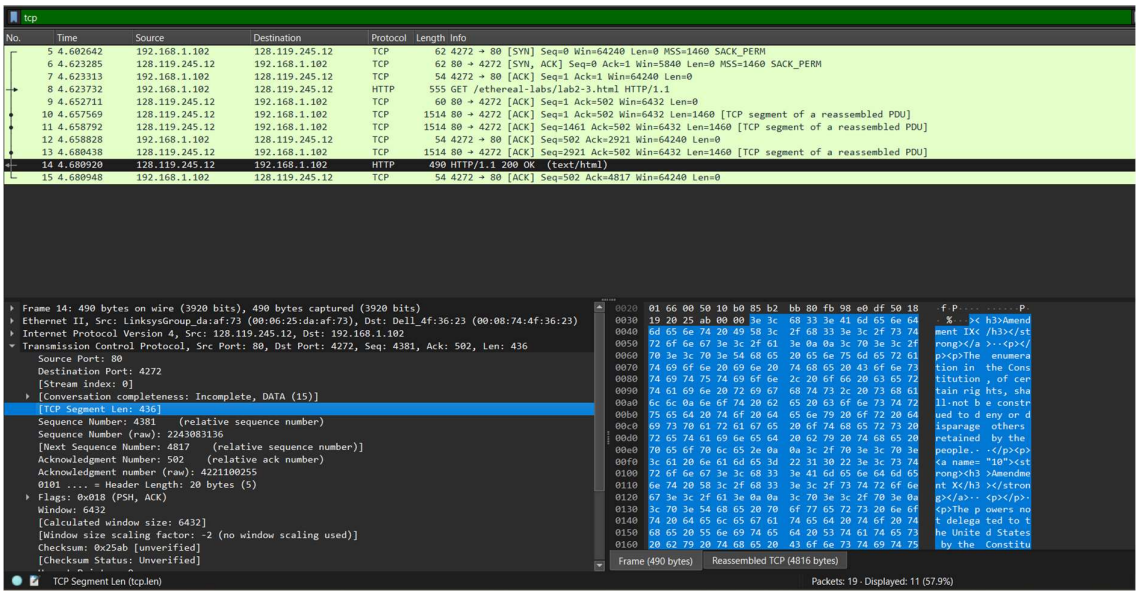
14. What is the status code and phrase in the response?

ANS:

The Status code and phrase in response is 200 OK.

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

ANS:



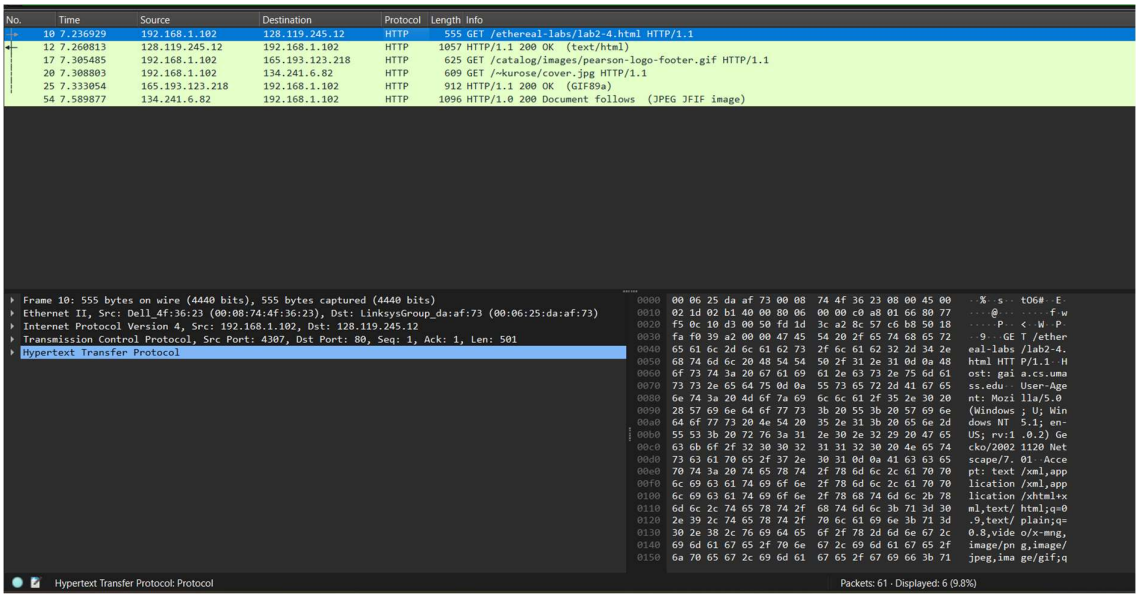
Segement count is 4.

4. HTML Documents with Embedded Objects

Note: Answer the following questions using the http-ethereal-trace-4 packet trace to answer the questions below

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

ANS:



There were 3 HTTP GET request messages that were sent from the browser. The GET requests were sent to three different IP addresses. They are

128.119.245.12, 165.193.123.218, 134.241.6.82

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

ANS:

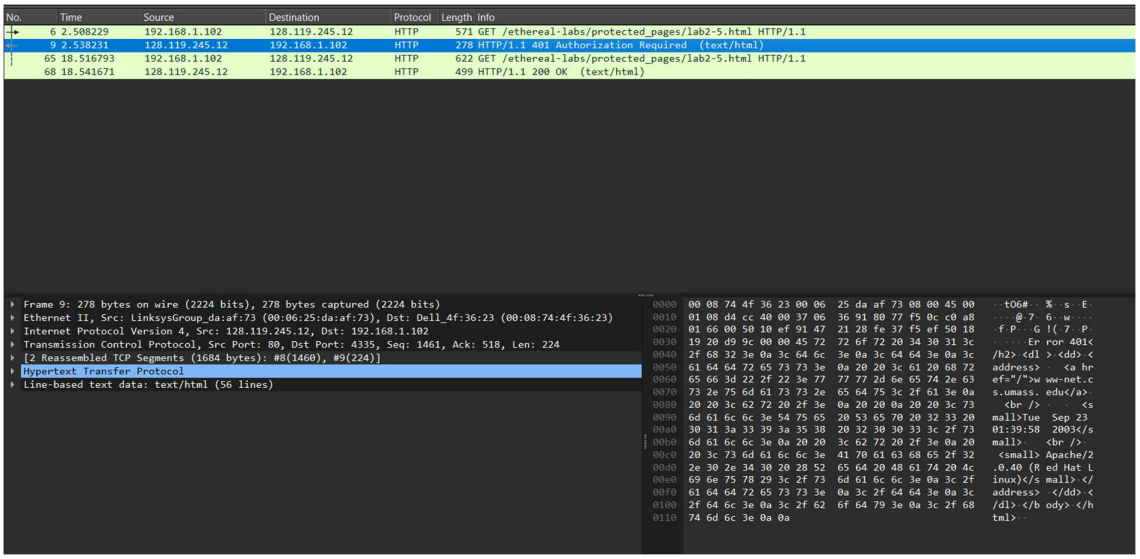
The browser downloaded the two images from the two web sites in parallel. Because the request message for the two images were sent to two different IP addresses. So the response for the two images were sent from two different IP addresses. So we can say they were downloaded from two different web sites in parallel.

5. HTTP Authentications

Note: Answer the following questions using the http-ethereal-trace-5 packet trace to answer the questions below

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

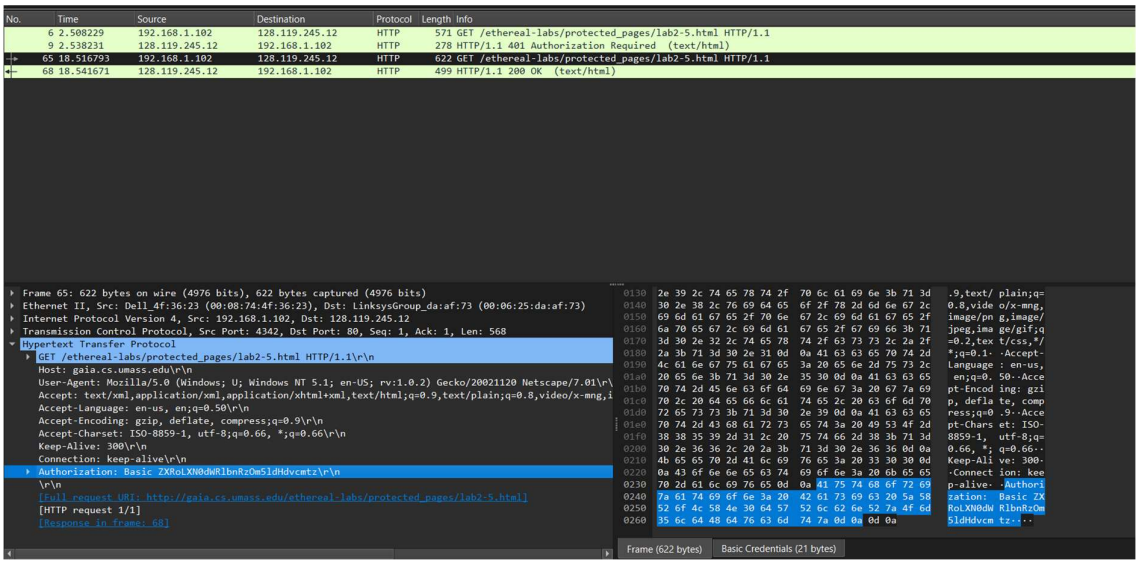
ANS:



The servers response for the initial HTTP GET message from the browser is 401 Authorization Required.

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

ANS:



A new field Authorization was included in the new HTTP GET message.

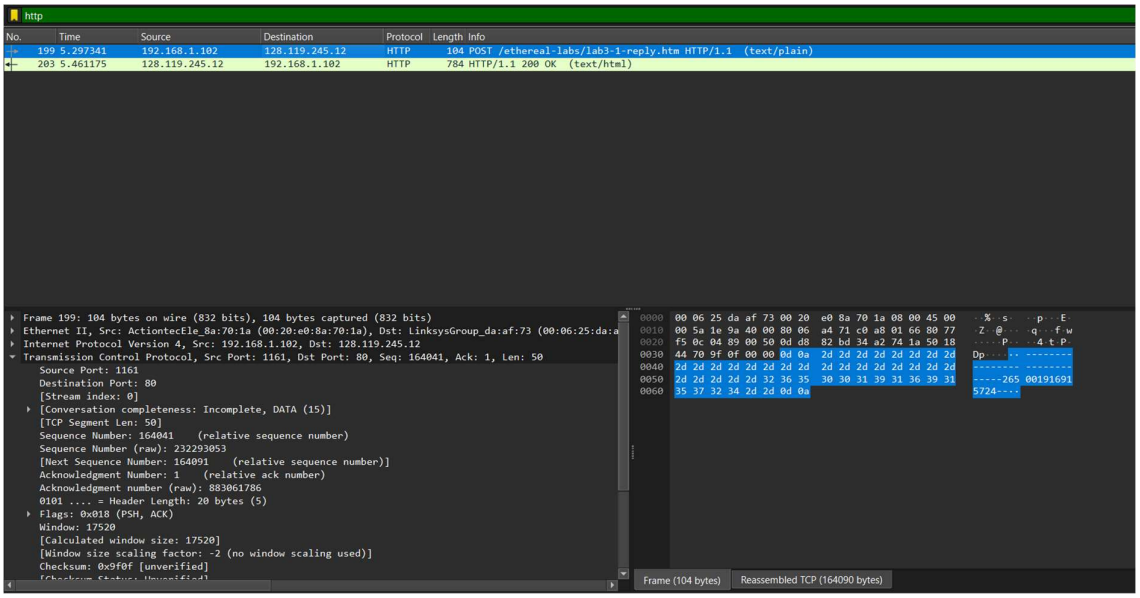
TCP

1. A first look at the captured trace

Note: Answer the following questions using the tcp-ethereal-trace-1 packet trace to answer the questions below

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".

ANS:



The IP address for the source is 192.168.1.102 and source port number is 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?

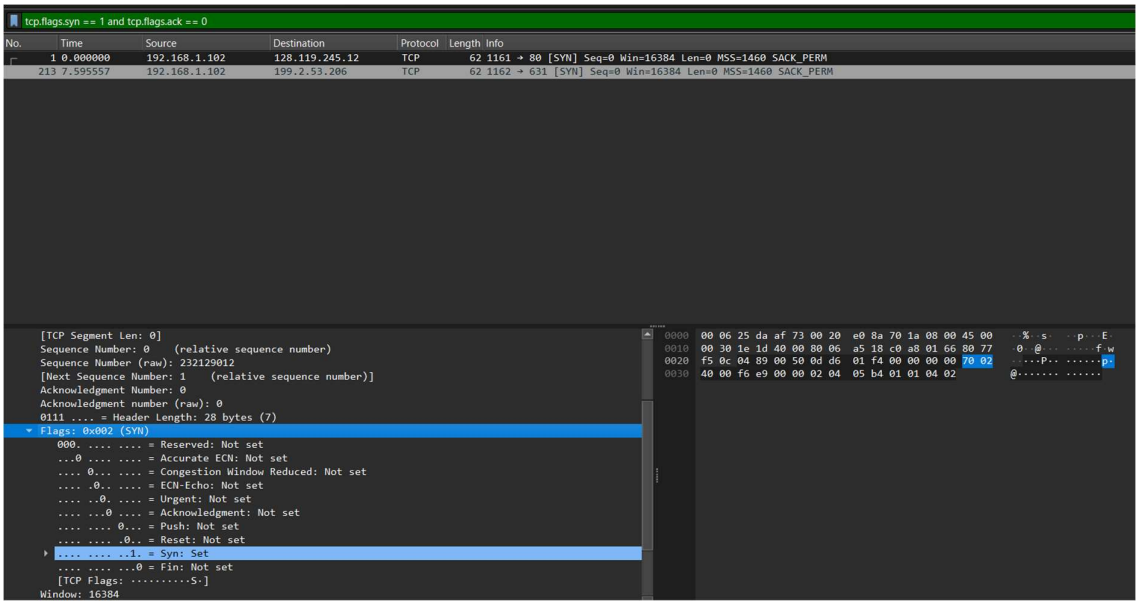
The IP address of the destination is 128.119.245.12 and the destination port number is 80.

2. TCP Basics

Note: Answer the following questions using the tcp-ethereal-trace-1 packet trace to answer the questions below:

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?

ANS:

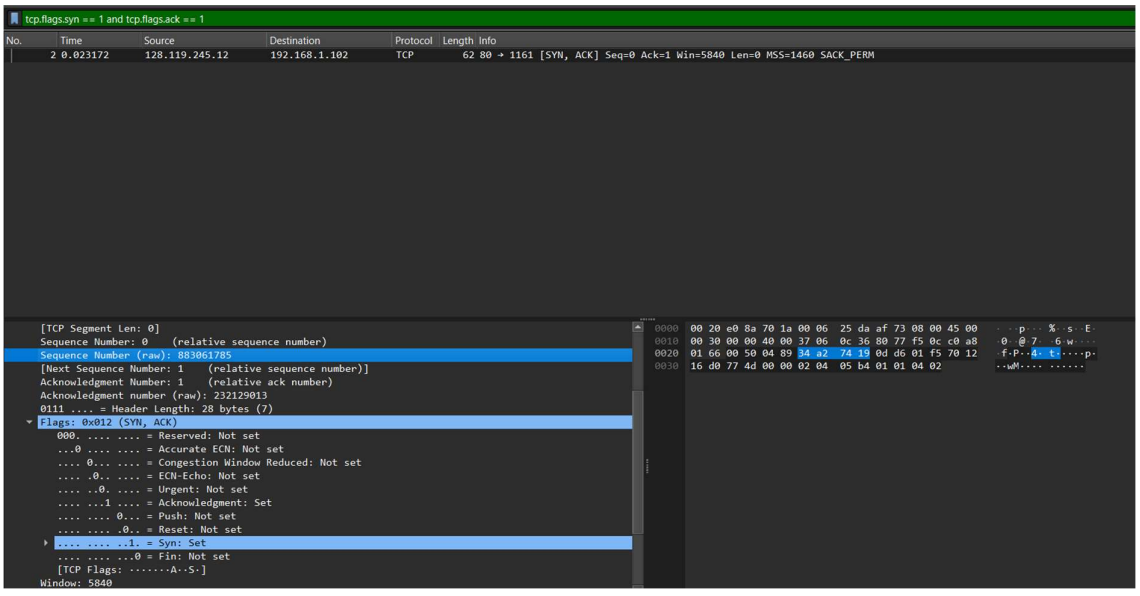


The sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu is 232129012.

BY the flags we can identify the segment as SYN SEGMENT as the SYN flag is set.

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?

ANS:



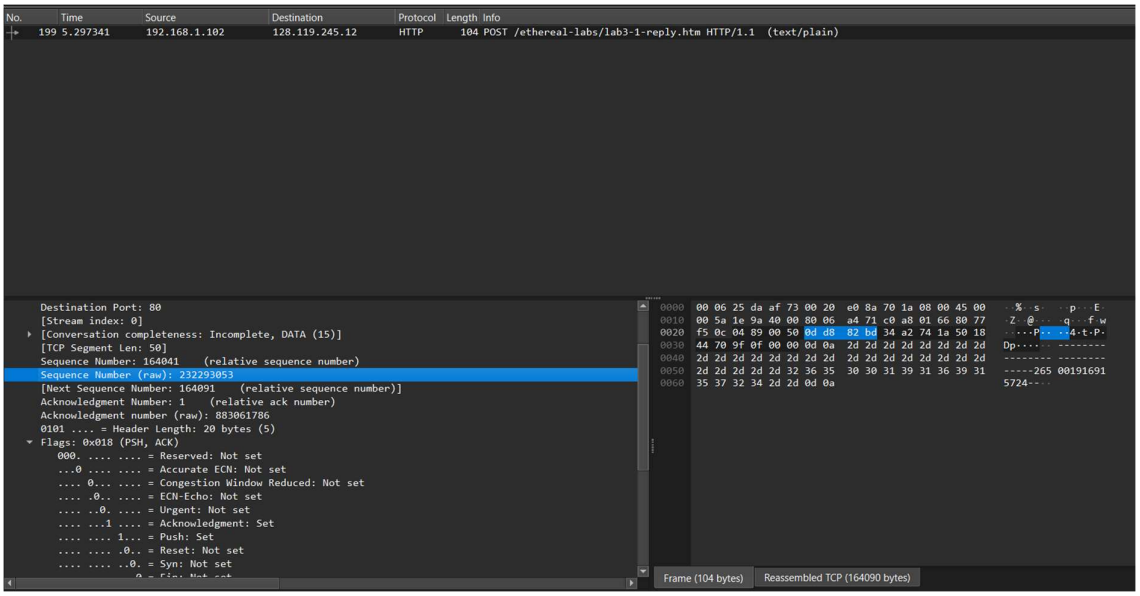
The Sequence number of SYNACK Segment is 883061785.

The Acknowledgment flag is set and the Acknowledge number is 232129013.

Both the SYN flag and Ack flags are set. By the flags we can identify the segment 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.

ANS:



Sequence number is 232293053

6. 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?

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.

ANS:

Sequence Number:

1 t=0.026477 ack= 0.053937 rtt=0.02746

566 t=0.041737 ack=0.077294 rtt=0.035557

2026 t=0.054026 ack=0.124085 rtt=0.070059

3486 t=0.054690 ack=0.169118 rtt=0.114428

4946 t=0.077405 ack=0.217299 rtt=0.139894

6406 t=0.078157 ack=0.267802 rtt=0.189645

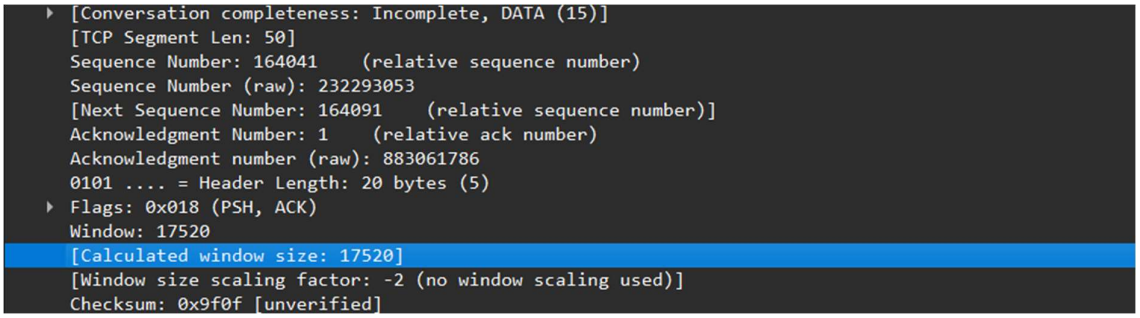
7. What is the length of each of the first six TCP segments?

ANS:

565, 1460, 1460, 1460, 1460

8. What is the minimum amount of available buffer space advertised at the received for the entire trace? Does the lack of receiver buffer space ever throttle the sender?

ANS:



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

ANS:

NO

10. How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment.

ANS:

1460

11. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.