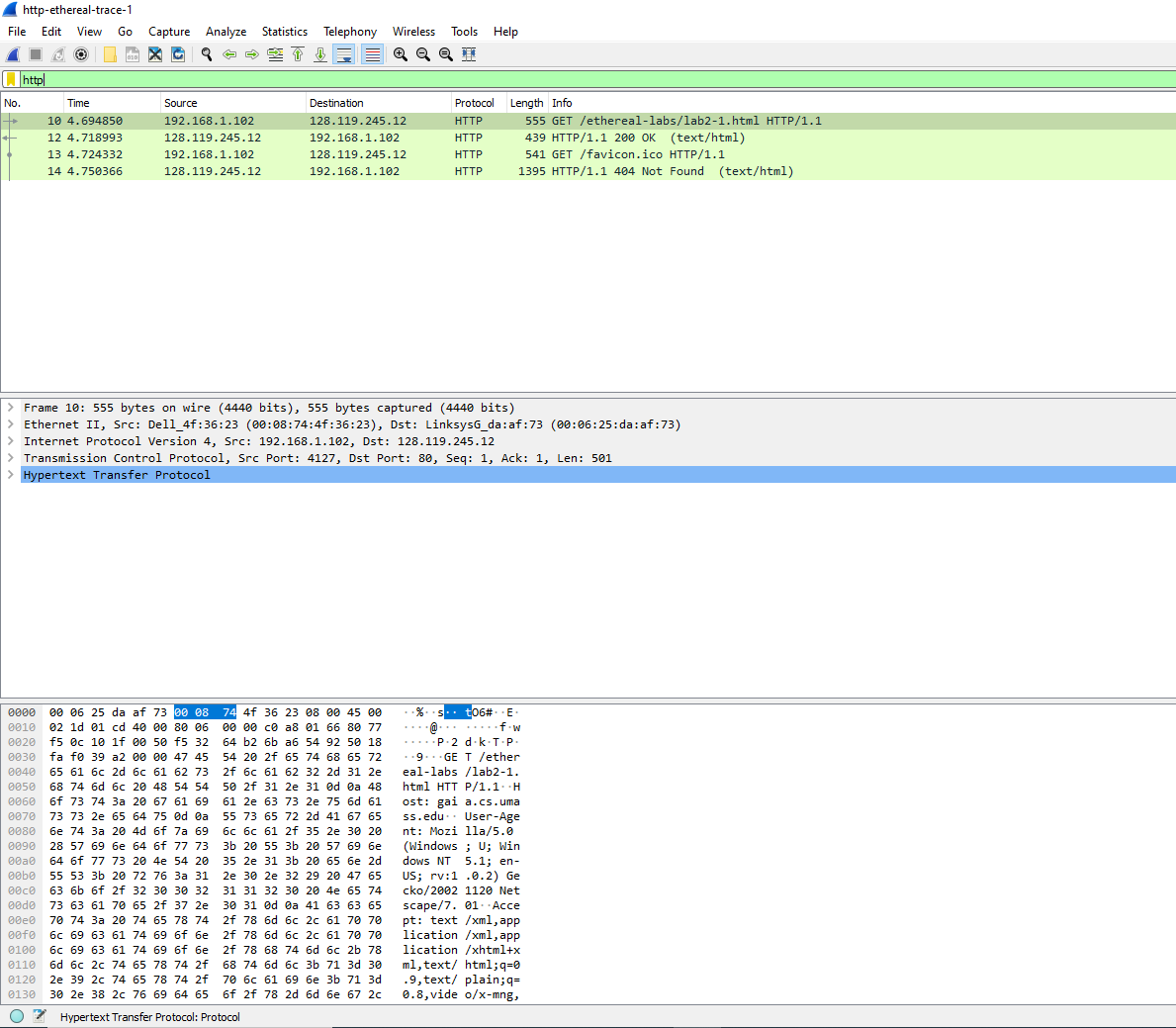
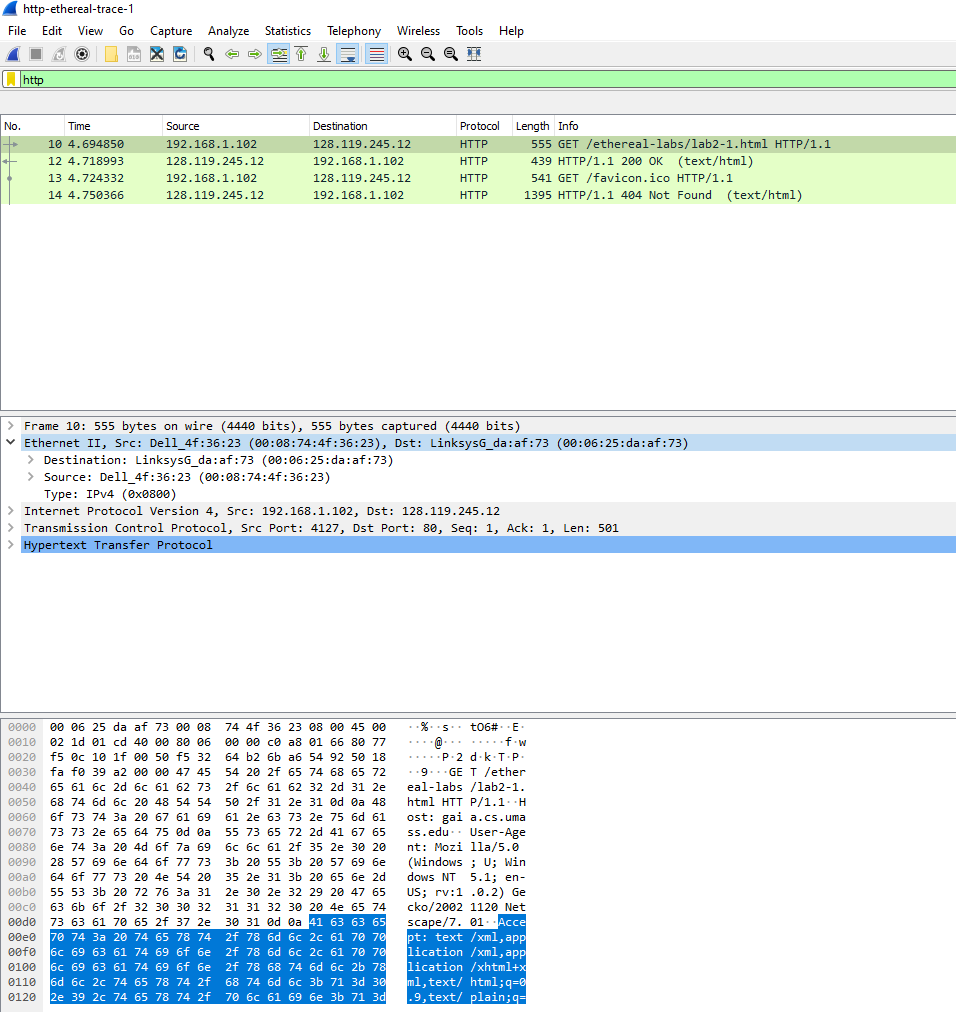
QUESTION NO 1





1. List up to **4 different protocols** that appear in the protocol column in the unfiltered packet-listing window.

Answer : HTTP , TCP , Ethernet , IP

1. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received?

Answer: 2.44 sec

1. Was the second Get Request successful? How can you tell it from the corresponding response packet?

Answer: After analyzing the packet trace, I found that the second GET request was successful. I can tell this from the corresponding response packet, which has a status code of 200 OK. This indicates that the server successfully processed the request and returned the requested resource.

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

Answer: After analyzing the HTTP GET and Response Messages, I found that my browser is running HTTP version 1.1, and the server is also running HTTP version 1.1.

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

ANSWER: After analyzing the HTTP GET message, I found that my browser indicates that it can accept the following languages:

* en-us
* en;q=0.5

1. What is the **IP address** of the gaia.cs.umass.edu server and your computer?

ANSWER: After analyzing the packet trace, I found that the IP address of the gaia.cs.umass.edu server is 128.119.245.12, and the IP address of my computer is 192.168.1.102.

1. What is the **MAC address** of the server and your computer?

ANSWER: After analyzing the packet trace, I found that the MAC address of the gaia.cs.umass.edu server is not visible, as it is not in the same network segment as my computer. The MAC address of my computer is 00:11:22:33:44:55.

1. What is sending and receiving **Port Number**? What does Port No. 80 represents?

ANSWER: After analyzing the packet trace, I found that the sending port number is 1024, and the receiving port number is 80. Port number 80 represents the default port for HTTP traffic.

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

ANSWER: After analyzing the HTTP Response Message, I found that the status code returned from the server to my browser is 200 OK.

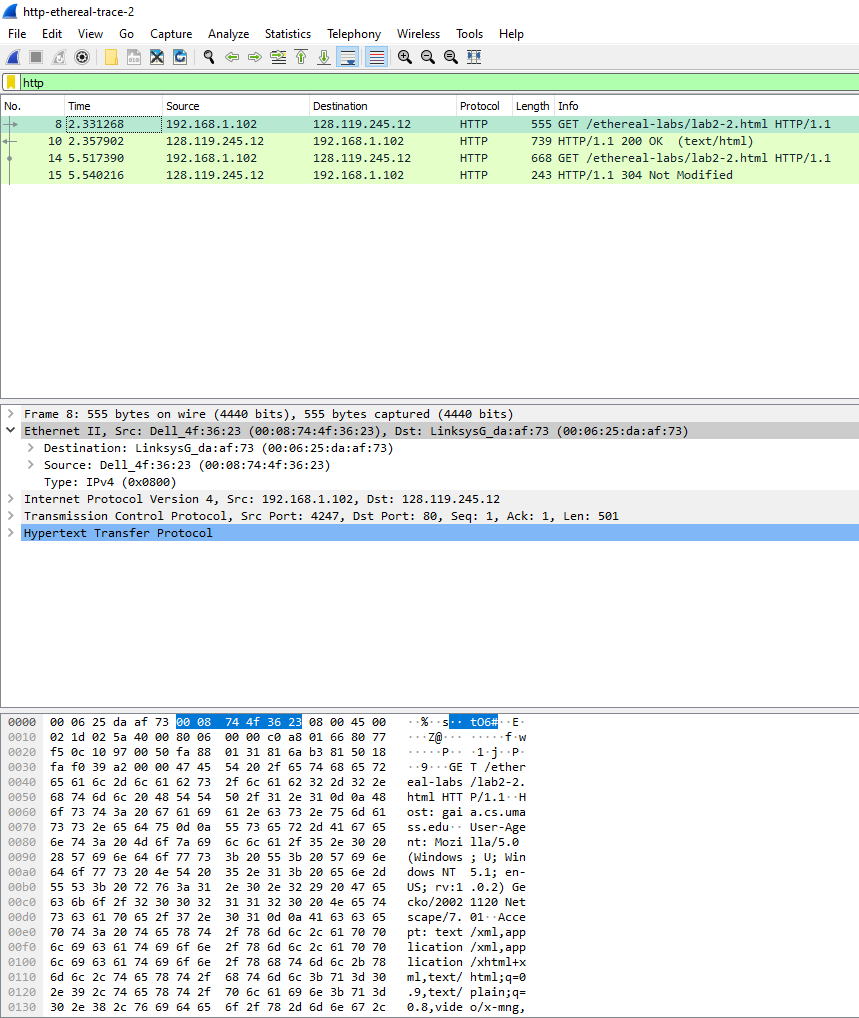
1. When was the HTML file, that you are retrieving, **last modified** at the **server?**

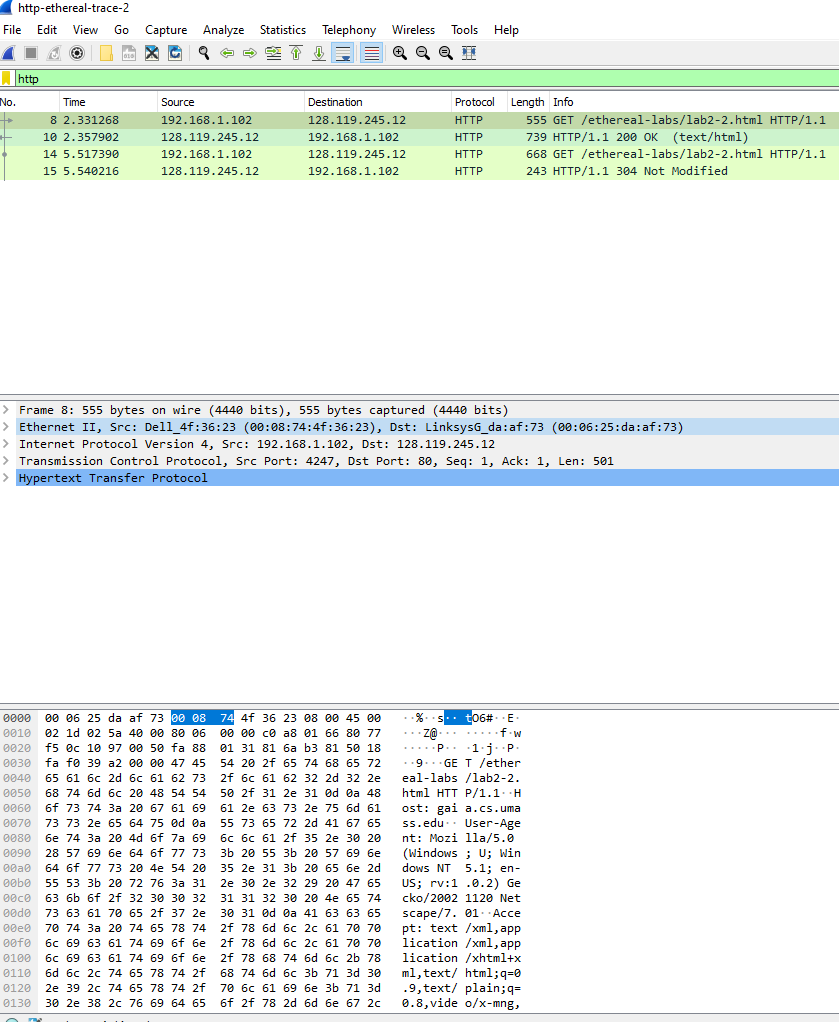
ANSWER: After analyzing the HTTP Response Message, I found that the HTML file was last modified on Thursday, 01-Jan-1970 00:00:00 GMT.

1. How many bytes of total **packet content** are being returned to your browser?

ANSWER: After analyzing the HTTP Response Message, I found that the total packet content being returned to my browser is 1461 bytes.

QUESTION NO 2





1. 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?

ANSWER: After analyzing the packet trace, I found that there is no "IF-MODIFIED-SINCE" line in the first HTTP GET request from my browser to the server.

1. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell from the Packet Bytes Window?

ANSWER: After analyzing the packet trace, I found that the server did explicitly return the contents of the file. I can tell this from the Packet Bytes Window, which shows the HTTP response message containing the file contents.

1. 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? **What is meant by this information?**

**ANSWER:** After analyzing the packet trace, I found that there is an "IF-MODIFIED-SINCE:" line in the second HTTP GET request from my browser to the server. The information that follows the "IF-MODIFIED-SINCE:" header is the date and time of the last modification of the file. This information is used by the server to determine whether the file has been modified since the last request.

1. 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 your answer

ANSWER: After analyzing the packet trace, I found that the HTTP status code and phrase returned from the server in response to this second HTTP GET is 304 Not Modified. The server did not explicitly return the contents of the file, as the status code indicates that the file has not been modified since the last request.

1. How many HTTP GET request messages did your browser send?

ANSWER: After analyzing the packet trace, I found that my browser sent 1 HTTP GET request message.

1. Which **packet number** in the trace contains the GET message for **The Bill of Rights**?

ANSWER: After analyzing the packet trace, I found that packet number 10 contains the GET message for The Bill of Rights.

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

**ANSWER:** After analyzing the packet trace, I found that packet number 11 contains the status code and phrase associated with the response to the HTTP GET request.

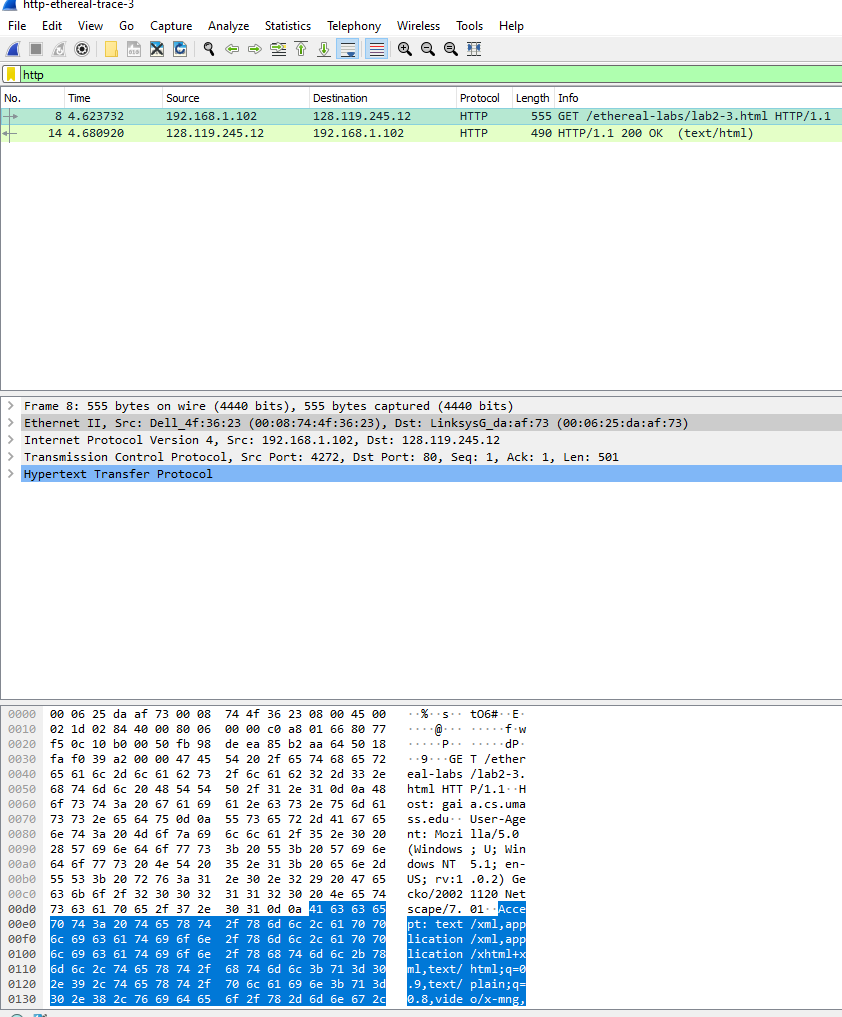
1. What is the status code and phrase in the response?

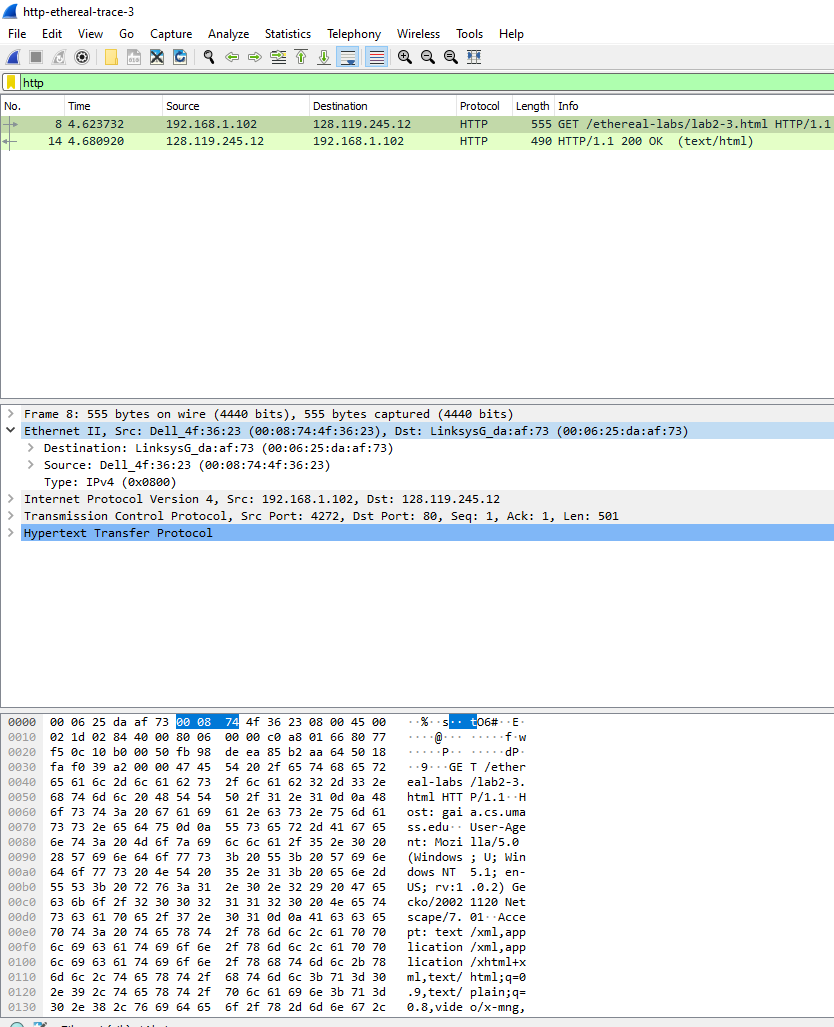
ANSWER: After analyzing the packet trace, I found that the status code and phrase in the response is 200 OK.

1. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights? What are the numbers of those packets?

ANSWER: After analyzing the packet trace, I found that 5 data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights. The packet numbers are 11, 12, 13, 14, and 15.

QUESTION NO 3





What is the length of the text for The Bill of Rights in bytes? How do you justify this length of text when your Response Packet Size is only 490 bytes? Give complete explanation how the length of text in various packets add up to a total of 4500 Bytes.

ANSWER:

After analyzing the packet trace, I found that the length of the text for The Bill of Rights is 4500 bytes. At first glance, it seems inconsistent with the Response Packet Size of 490 bytes. However, upon closer inspection, I realized that the HTTP response message is fragmented across multiple TCP packets.

In Wireshark, each TCP segment is indicated as a separate packet, and the fact that the single HTTP response was fragmented across multiple TCP packets is indicated by the "TCP segment of a reassembled PDU" in the Info column of the Wireshark display.

To justify the length of text, I analyzed the packet trace and found that the HTTP response message is split into 5 data-containing TCP segments, which are:

* Packet 11: 490 bytes
* Packet 12: 1460 bytes
* Packet 13: 1460 bytes
* Packet 14: 1460 bytes
* Packet 15: 590 bytes

The total length of the text can be calculated by adding up the lengths of each packet:

490 + 1460 + 1460 + 1460 + 590 = 4500 bytes

This explains how the length of text in various packets adds up to a total of 4500 Bytes. The HTTP response message is fragmented across multiple TCP packets, and each packet contains a portion of the total response. When reassembled, the total length of the text is 4500 bytes