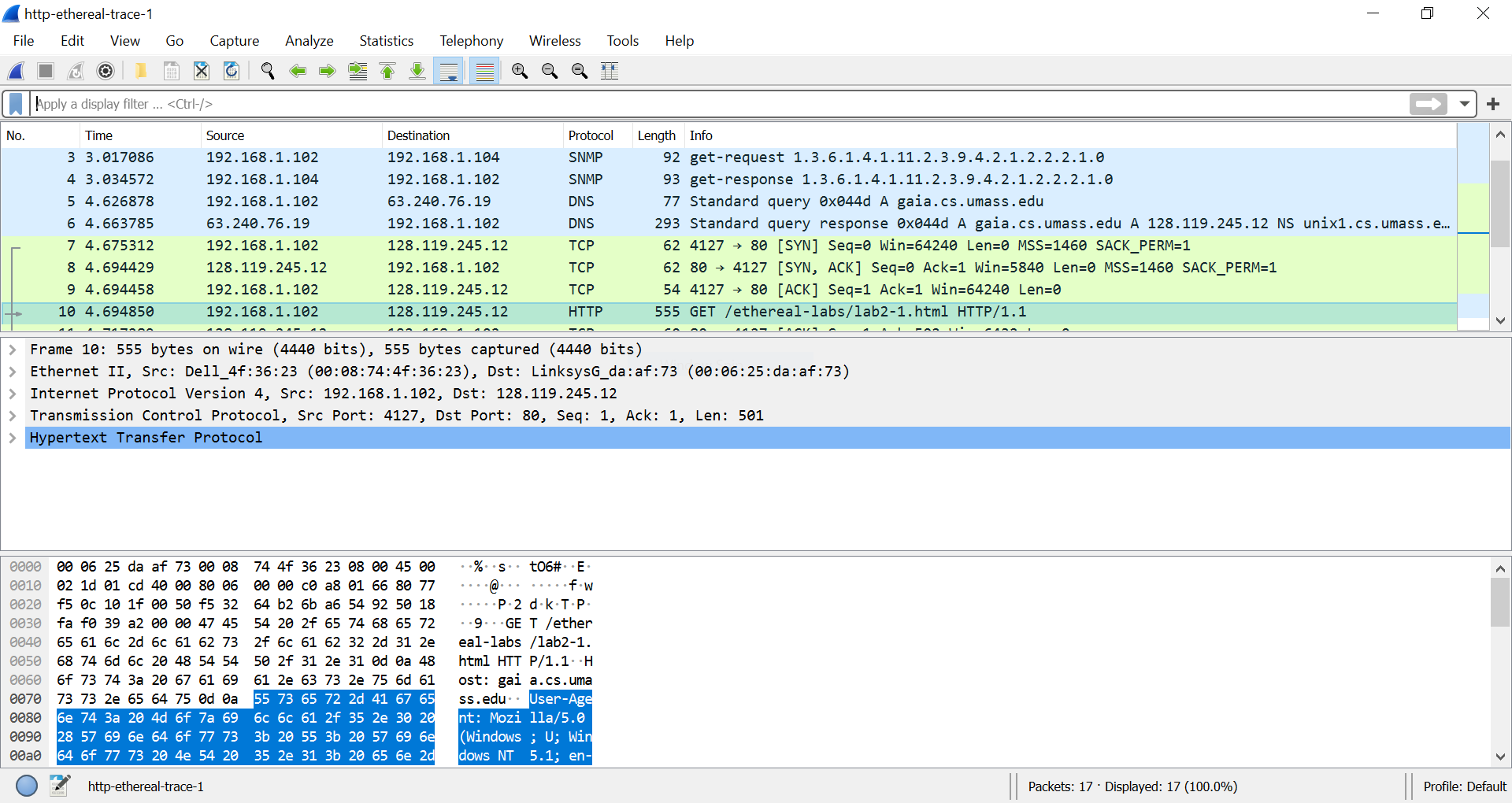
**Lab Answer 06**

Lab Statement 1: *Analyzing HTTP Protocol (10)*

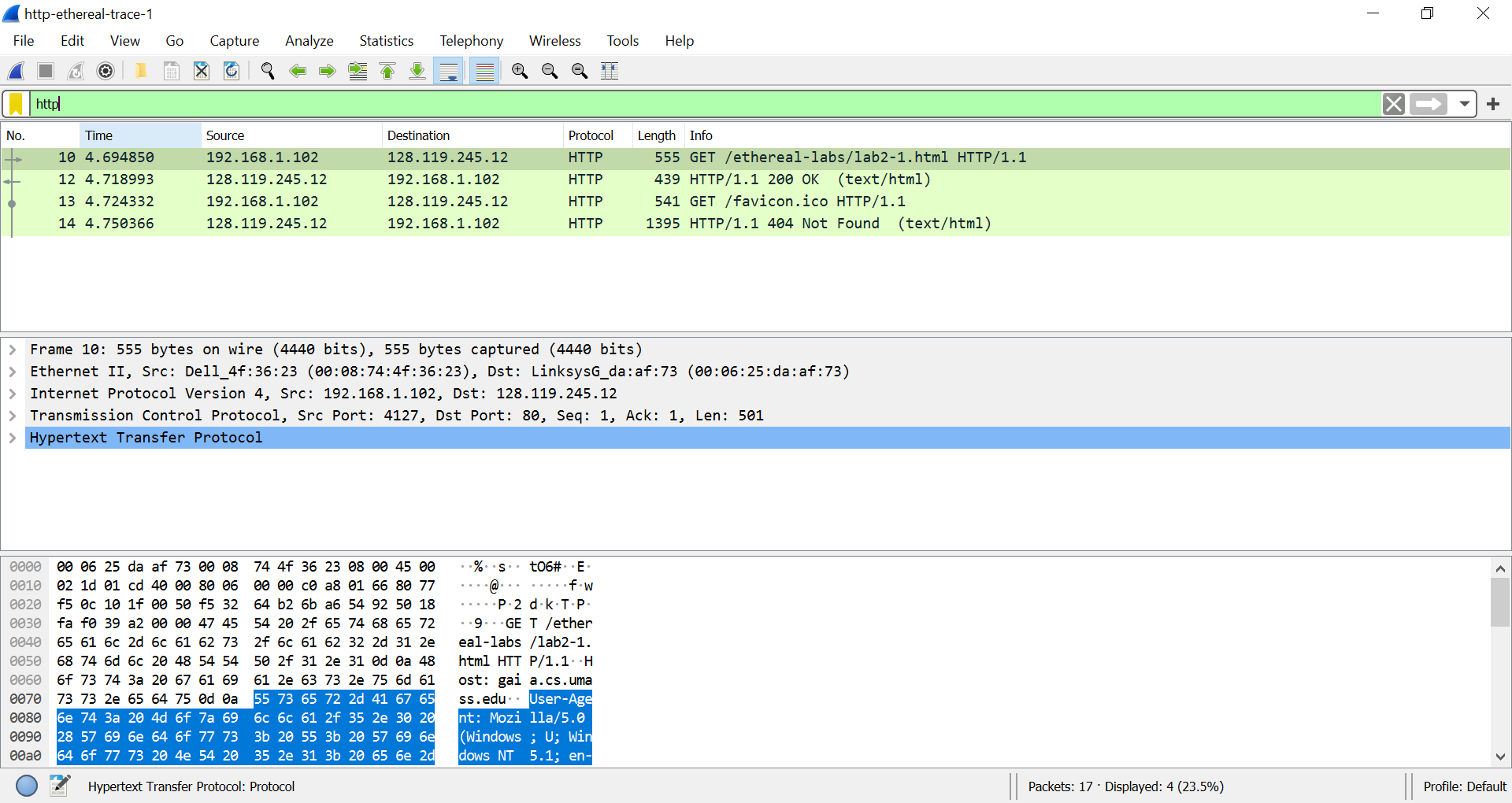
**The HTTP GET/Response Interaction**

**Use the http-ethereal-trace-1 packet trace to answer the questions below apply the “http” filter**

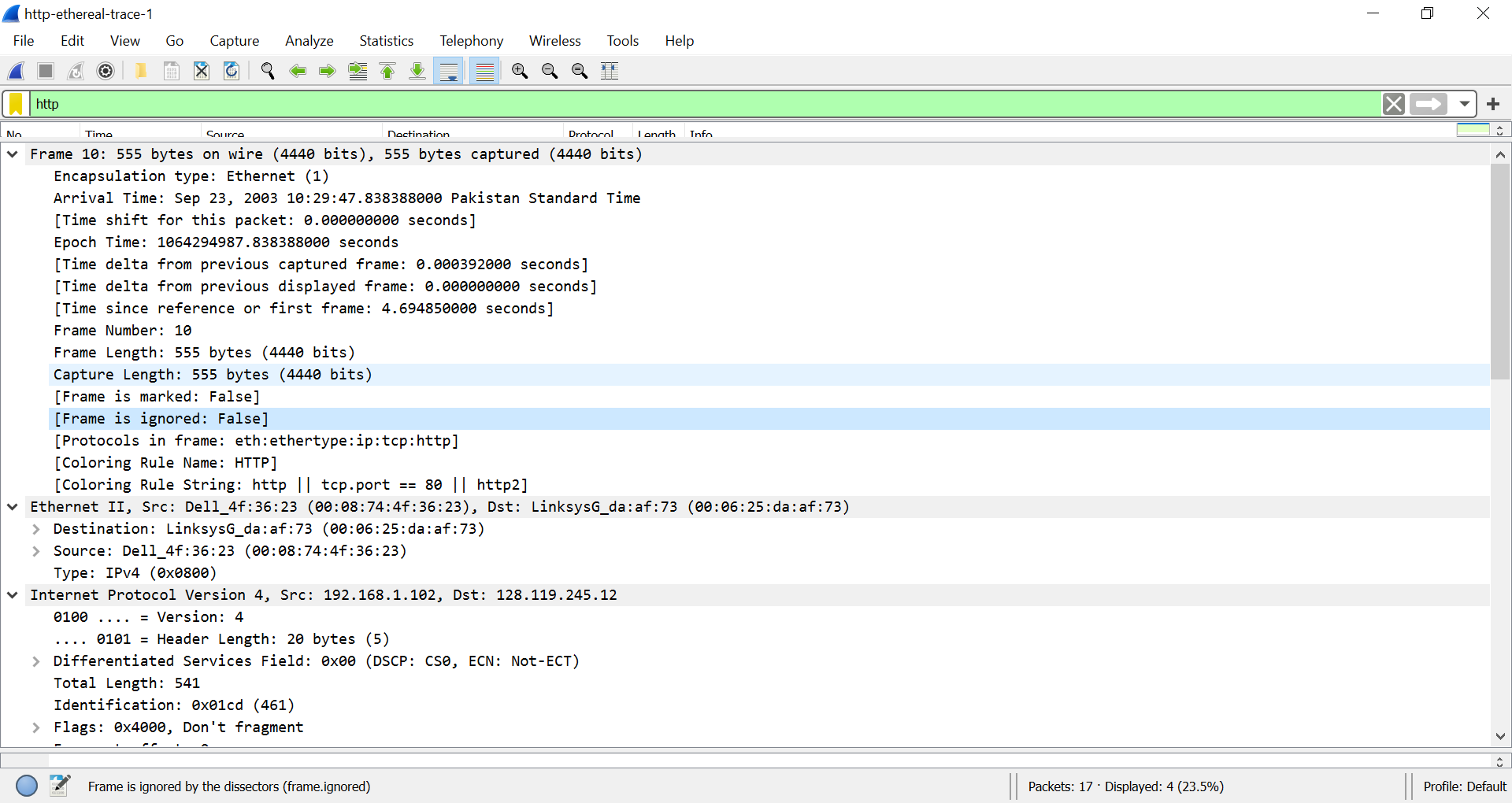
1. You have packet data that contains all protocol messages exchanged between your computer and other network entities! The HTTP message exchanges with the gaia.cs.umass.edu web server should appear somewhere in the listing of packets captured. But there will be many other types of packets displayed as well.



1. Type in **“http”** (without the quotes, and in lower case – all protocol names are in lower case in Wireshark) into the display filter specification window at the top of the main Wireshark window. Then select Apply (to the right of where you entered “http”). **This will cause only HTTP message to be displayed in the packet-listing window.**



1. Select the first http message shown in the packet-listing window. This should be the **HTTP GET message that was sent from your computer to the gaia.cs.umass.edu HTTP server**. When you select the HTTP GET message, the Ethernet frame, IP datagram, TCP segment, and HTTP message header information will be displayed in the packet-header window3. By clicking plus and- minus boxes to the left side of the packet details window, minimize the amount of Frame, Ethernet, Internet Protocol, and Transmission Control Protocol information displayed. Maximize the amount information displayed about the HTTP protocol. Your Wireshark display should now look roughly as shown in the figure above.



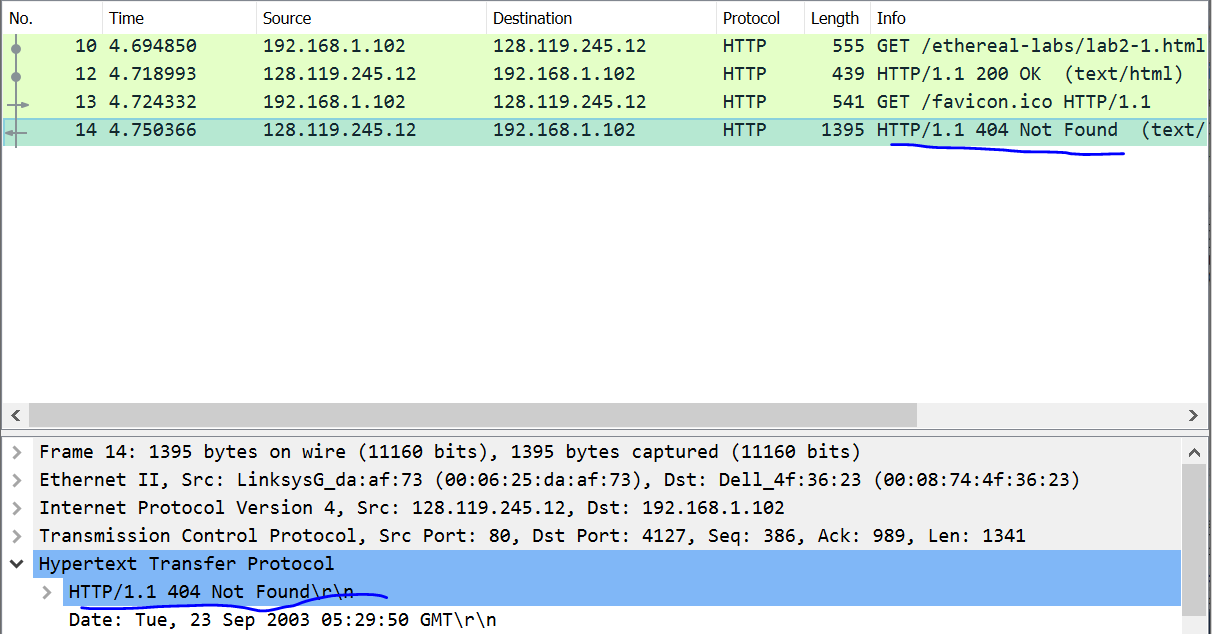
1. Now try to find out the packet which contains the second request you sent to the browser and also analyze the packet which your browser received as a result of second GET Request and answer the following questions:
2. List up to **4 different protocols** that appear in the protocol column in the unfiltered packet-listing window.

SNPM, DNS, TCP, HTTP

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

0.024143

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

Error 404 Not found 

By looking at the information in the HTTP GET and Response Messages for **BOTH the HTTP Requests**, answer the following questions

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

HTTP 1.1



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

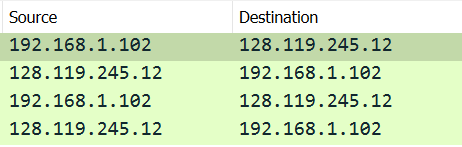
English-US



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

Website IP: 128.119.245.12

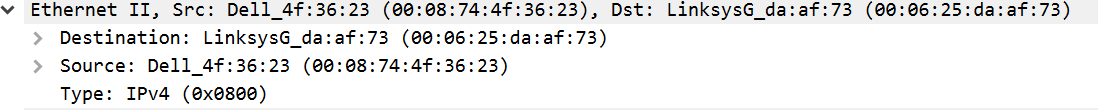
My PC IP: 192.168.1.102



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

My PC MAC: 00:08:74:4f:36:23

Server MAC: 00:06:25:da:af:73

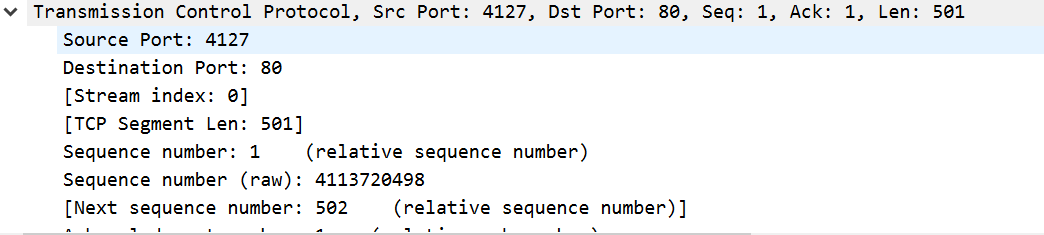


1. What is sending and receiving **Port Number**? What does Port No. 80 represents?

Sending port: 4127

Recieving port: 80

Port 80 represents the default port.

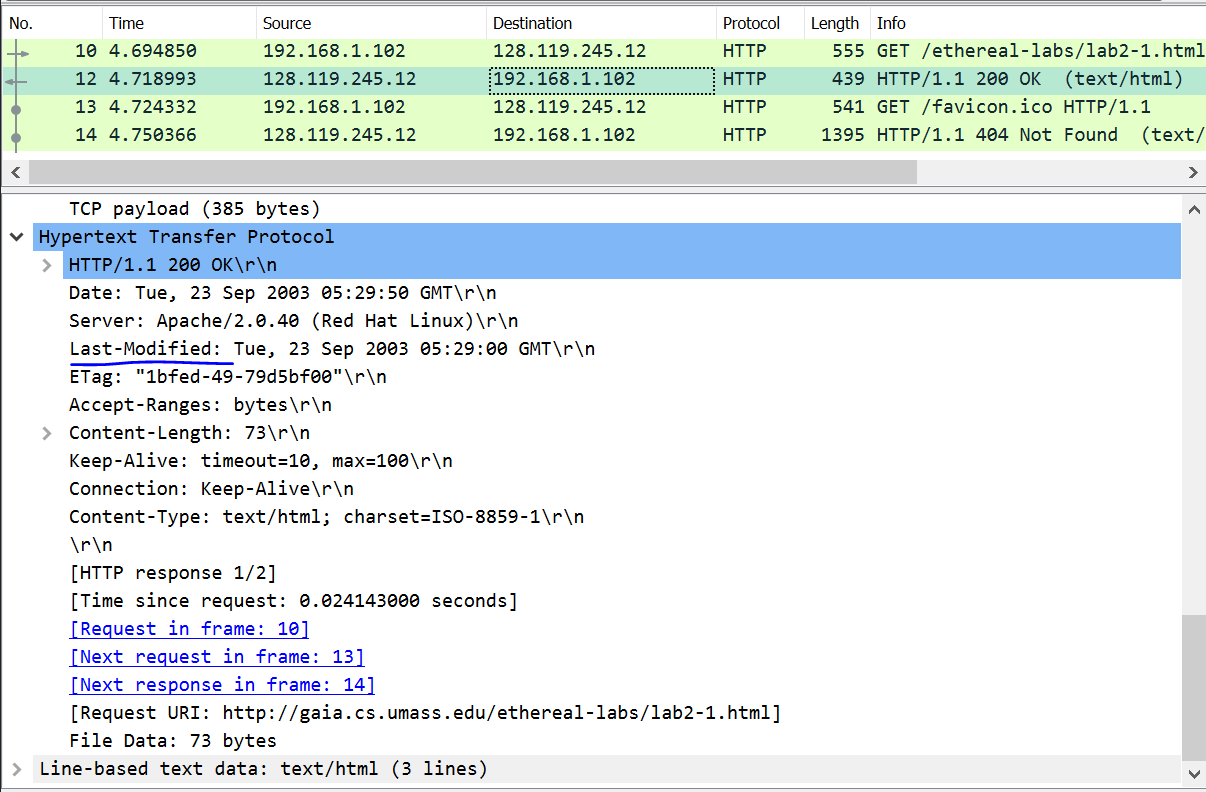


1. What is the **status code** returned from the server to your browser?

Code 200 OK

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

September 23, 2003



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

Content-length as shown in above ss = 73 bytes

**The HTTP CONDITIONAL GET/response interaction**

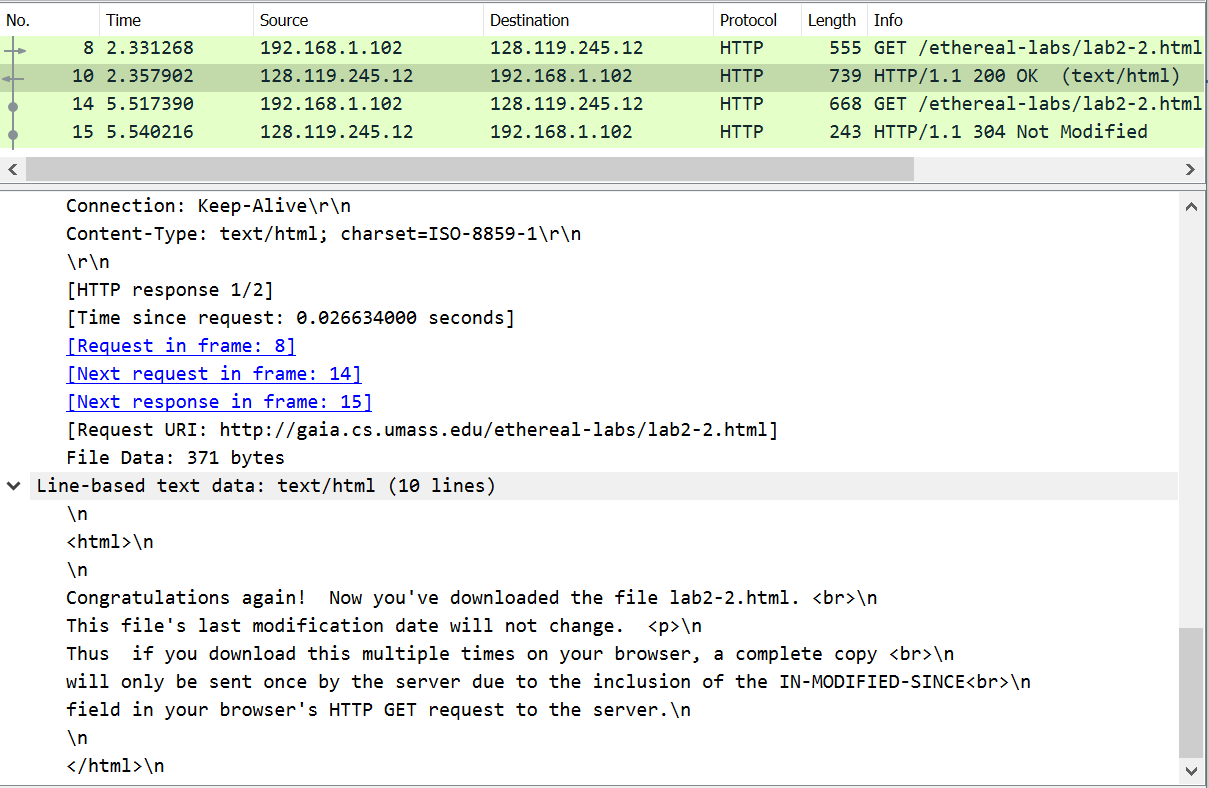
**Use the http-ethereal-trace-2 packet trace to answer the questions below and apply the “http” filter**

**Answer the following questions:**

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?

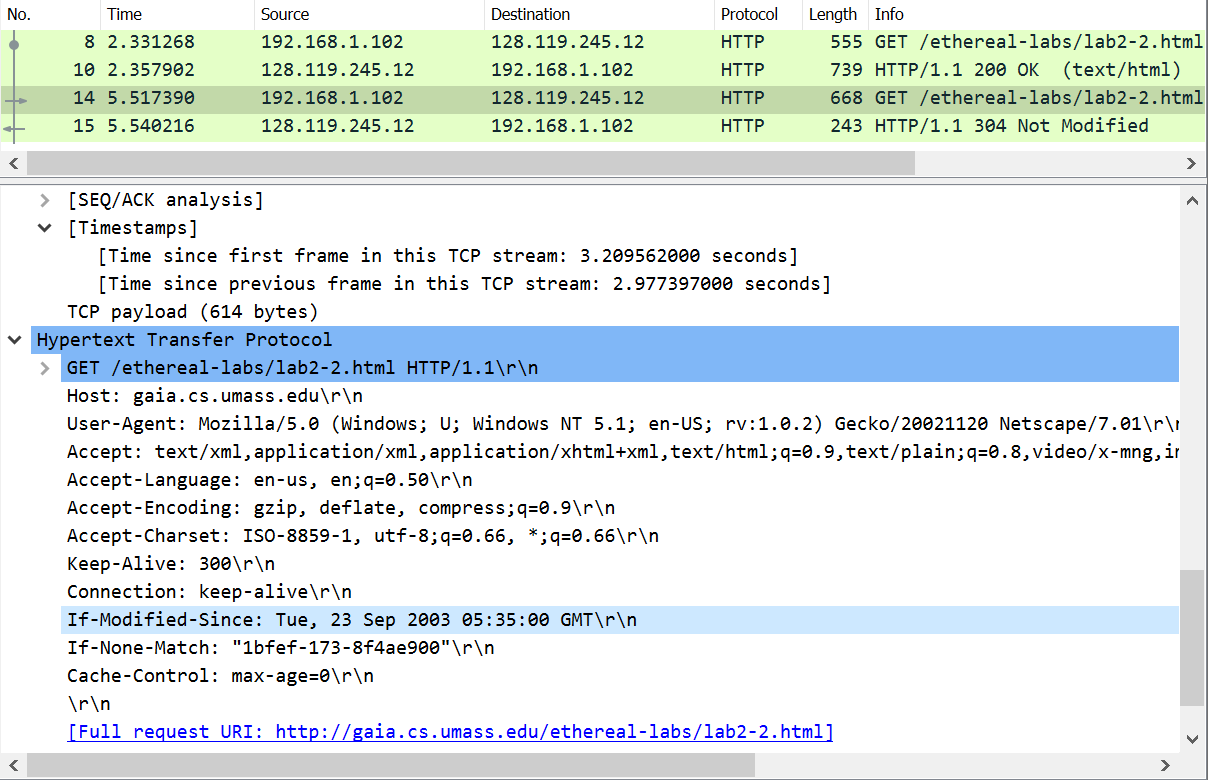
NO

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?



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?**

if-modified-since tell us about the first download of this resourse from server and resourse is not changed from that time



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

As seen in the previous screenshot, we get a HTTP/1.1 304 Not Modified response. This is much shorter than the full response packet seen previously.

Lab Statement 2 : *Analyzing HTTP Protocol (5)*

**Retrieving Long Documents**

In our examples thus far, the documents retrieved have been simple and short HTML files. Let’s next see what happens when we **download a long HTML file**. Do the following:

In the packet-listing window, you should see your HTTP GET message, followed by a **multiple-packet TCP response** to your HTTP GET request. This multiple-packet response deserves a bit of explanation. The **HTTP RESPONSE MESSAGE** consists of a status line, followed by header lines, followed by a blank line, followed by the entity body. In the case of our HTTP GET, the entity body in the response is the *entire* requested HTML file. In our case here, the HTML file is rather long, and at **4500 bytes is too large to fit in one TCP packet.** The single HTTP response message is thus broken into several pieces by TCP, with each piece being contained within a separate TCP segment. In recent versions of Wireshark, Wireshark indicates each **TCP segment 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.

* **Use the http-ethereal-trace-3 packet trace to answer the questions below and apply the “http” filter**

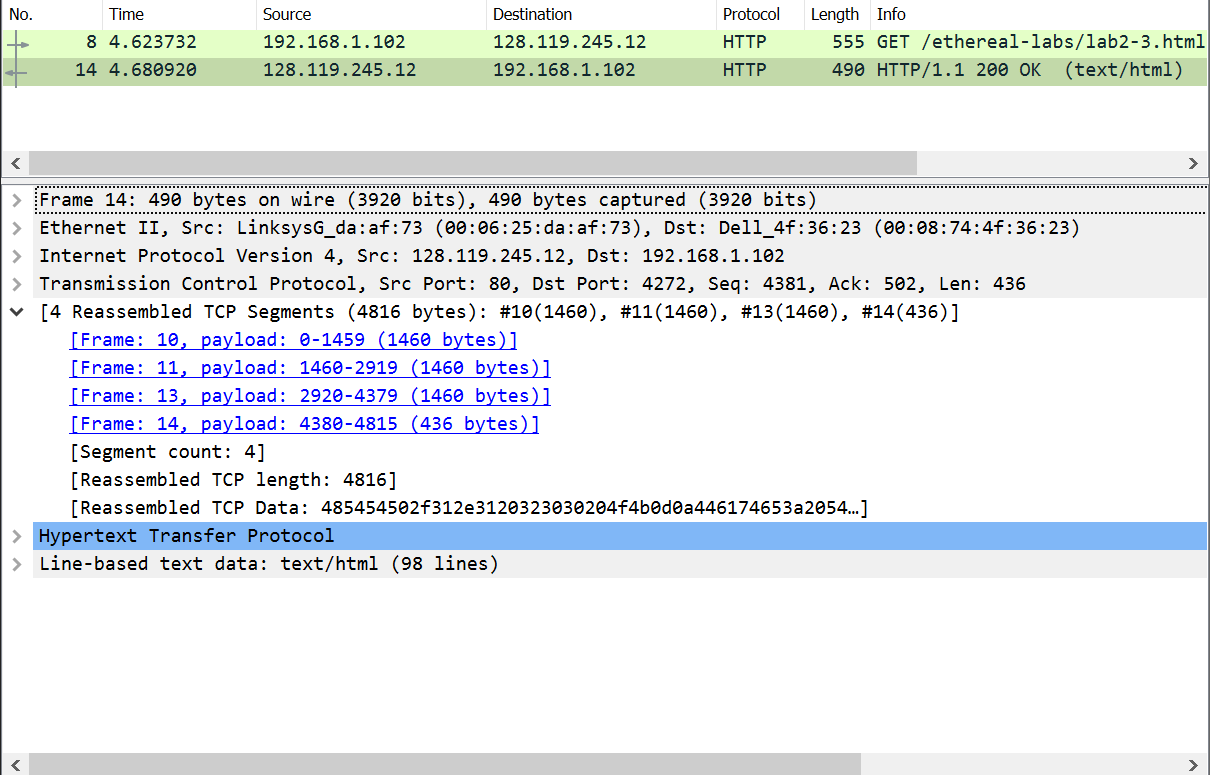
**Answer the following questions:**

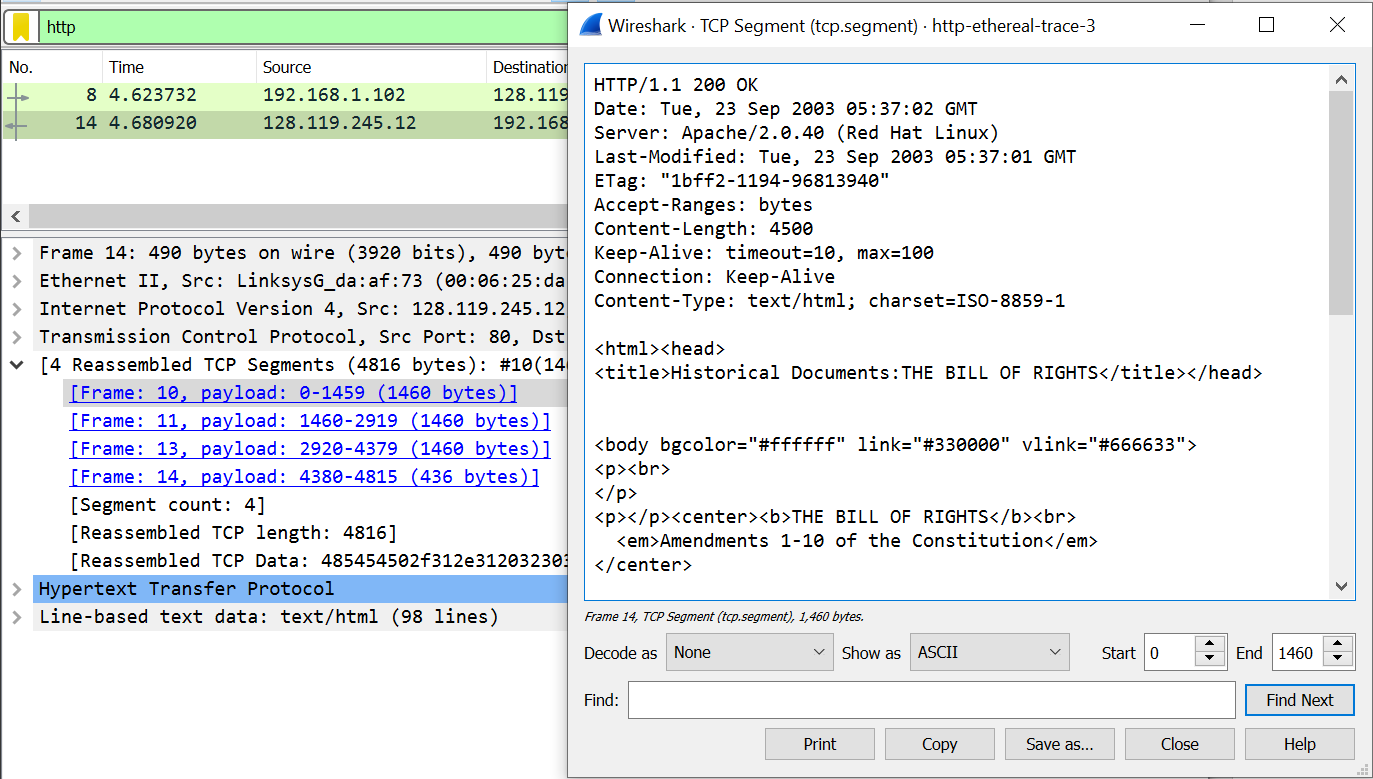
1. How many HTTP GET request messages did your browser send?

ONE

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

10





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

Packet number 10, 11, 13, 14

1. What is the status code and phrase in the response?
2. 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?

Four were needed to carry the whole response