

**Lab Tasks:**

The goal of this section of the lab was primarily to introduce you to Wireshark.

The following questions will demonstrate that you’ve been able to get Wireshark

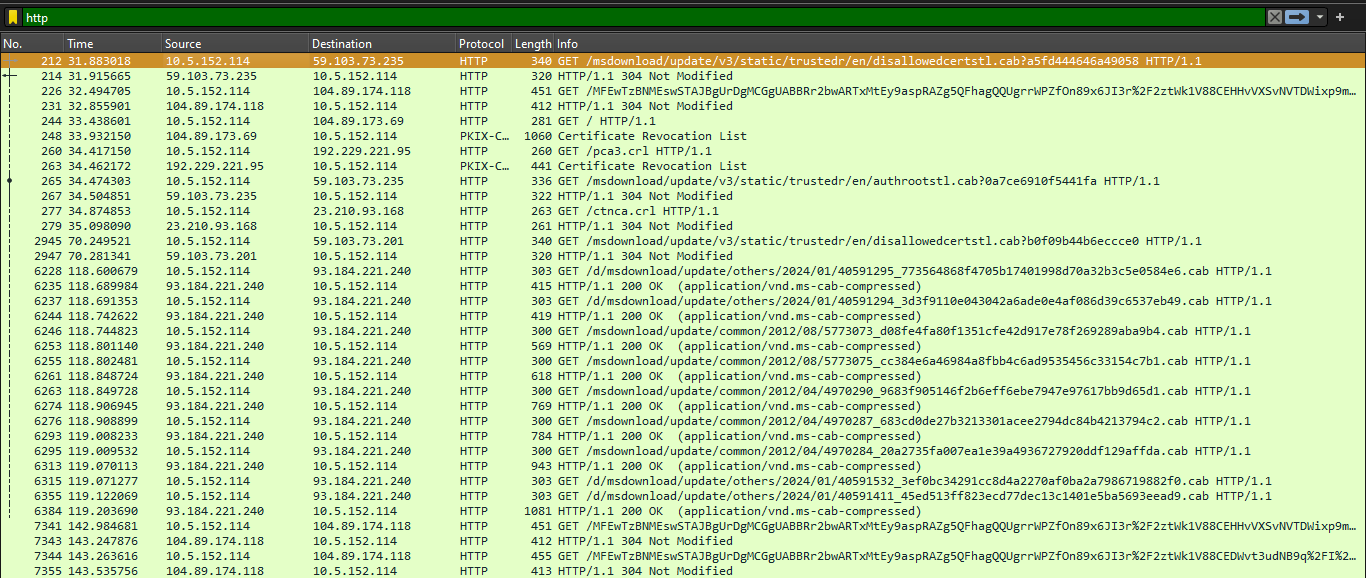
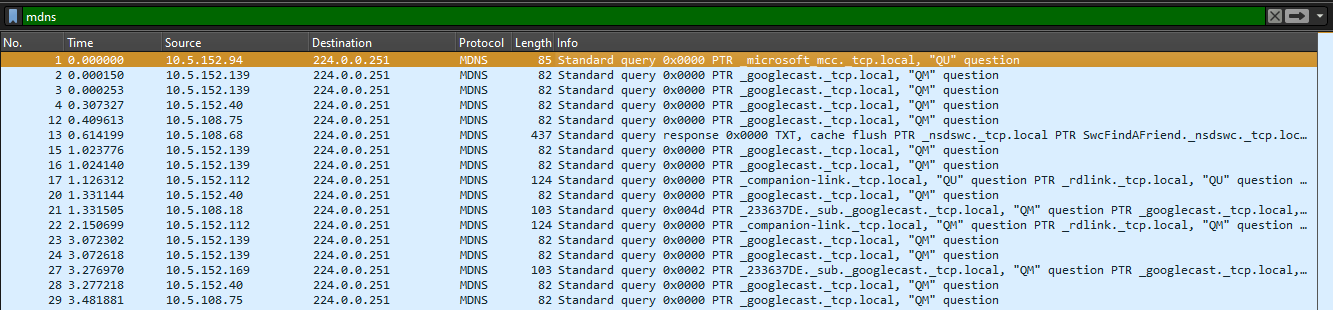
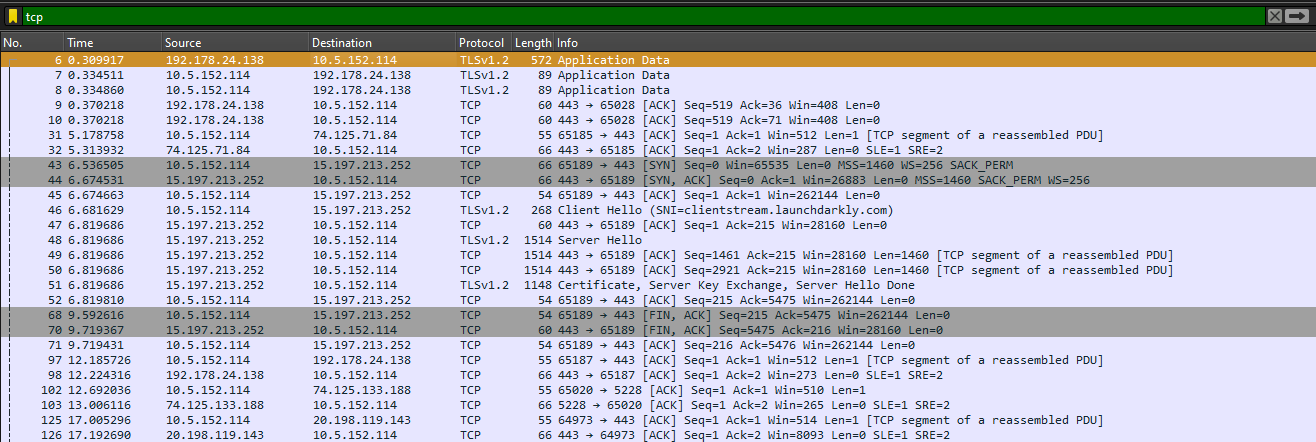
up and running, andhave explored some of its capabilities. Answer the following

questions, based on your Wireshark experimentation:

**1.** **List 3 different protocols that appear in the protocol column in the**

**unfilteredpacket-listing window in step 7 above.**

**Solution:**

1. http:
2. mdns:
3. tcp:

**2. How long did it take from when the HTTP GET message was sent until the**

**HTTPOK reply was received? (By default, the value of the Time column in**

**the packet- listing window is the amount of time, in seconds, since Wireshark**

**tracing began. To display the Time field in time-of-day format, select the**

**Wireshark View pull down menu, then select Time Display Format, then**

**select Time-of-day.)**

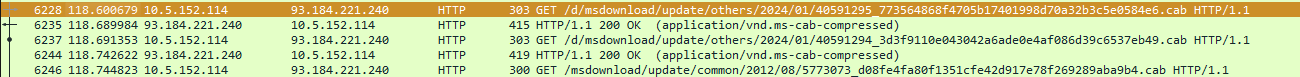
**Solution:**

**-0.089305** time take from when the HTTP GET message was sent until the

HTTPOK reply was received.

**3.** **What is the Internet address of the gaia.cs.umass.edu (also known as**

**www- net.cs.umass.edu)? What is the Internet address of your**

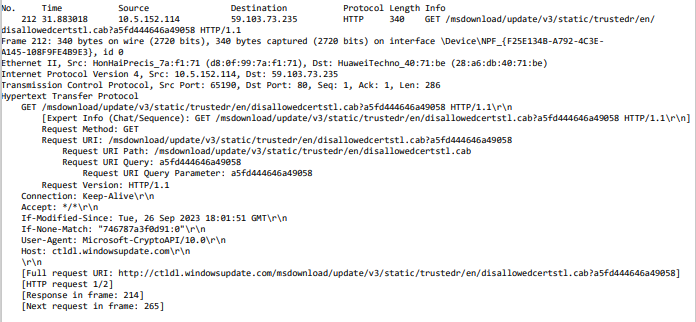
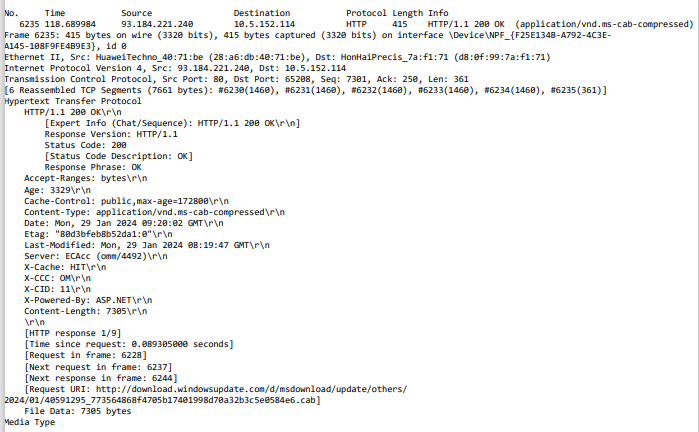
**computer?**

**4.** **Print the two HTTP messages (GET and OK) referred to in question 2 above.**

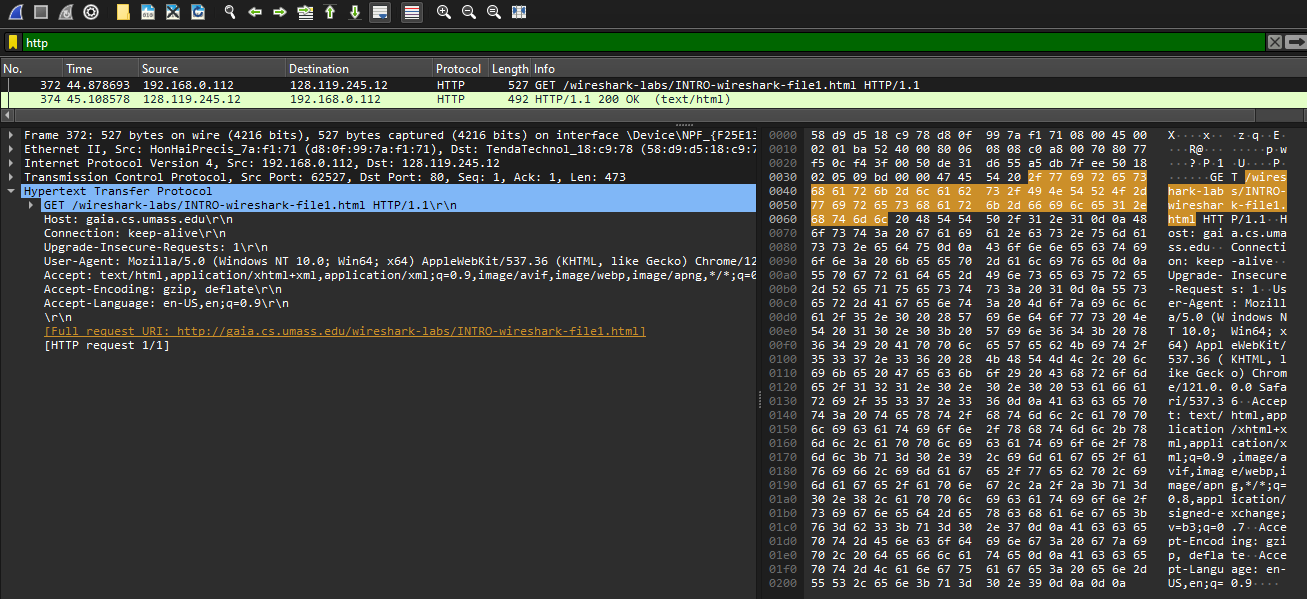
**Todo so, select Print from the Wireshark File command menu, and select**

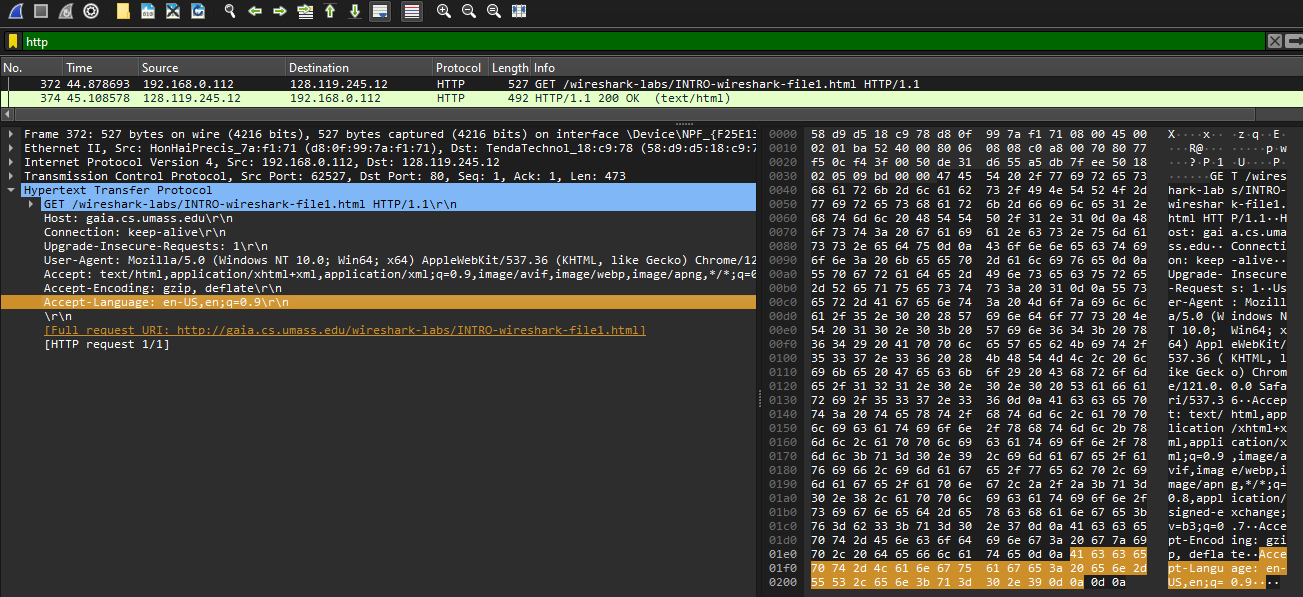
**the “Selected Packet Only” and “Print as displayed” radial buttons, and**

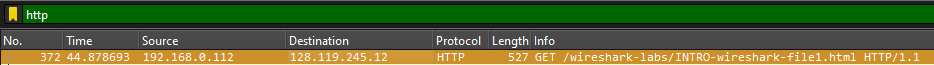
**then click OK.**

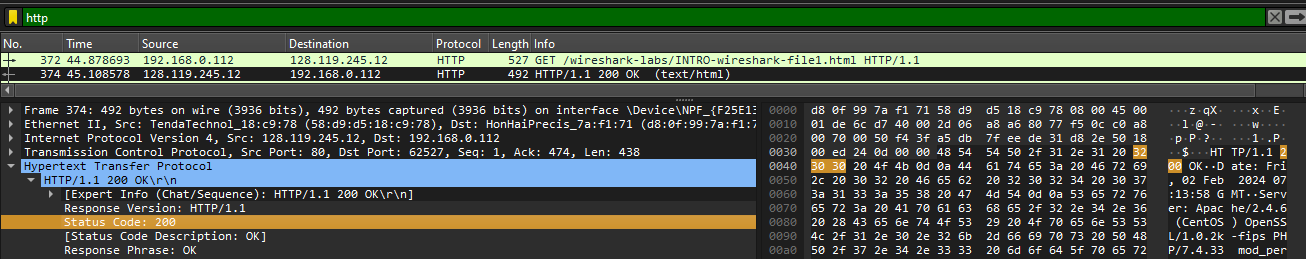
1.  **HTTP message GET:**
2. **HTTP message OK:**

**1. The Basic HTTP GET/response interaction**

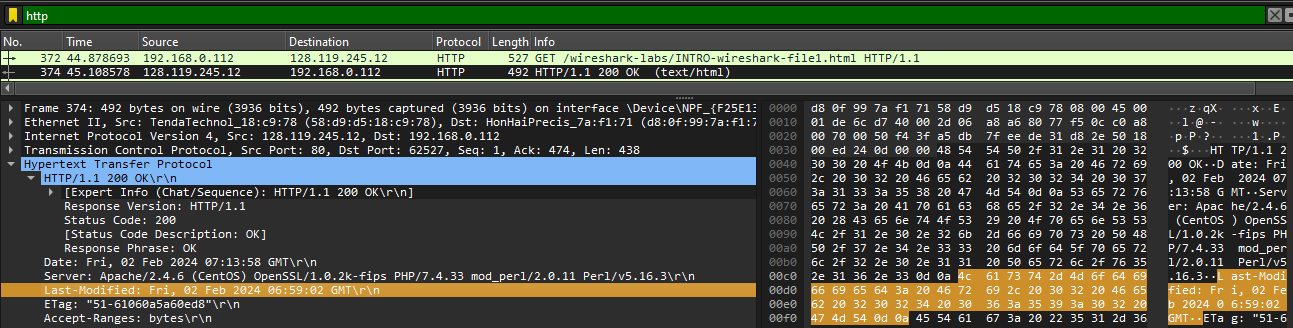
1. **Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?**
2. **What languages (if any) does your browser indicate that it can accept to the server?**

Accept-Language: en-US,en;q=0.9\r\n

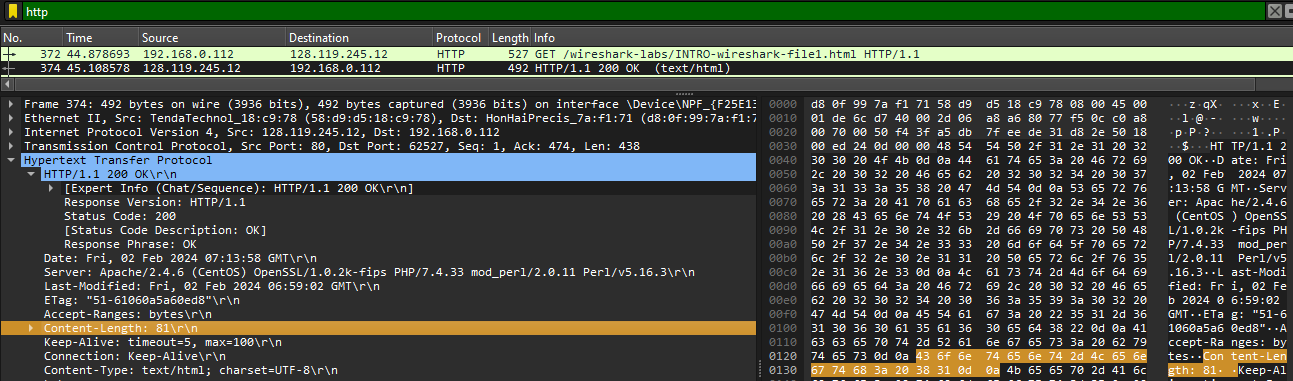
1. **What is the IP address of your computer? Of the gaia.cs.umass.edu server?**
2. **What is the status code returned from the server to your browser?**

Status Code: 200

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

Last-Modified: Fri, 02 Feb 2024 06:59:02 GMT\r\n

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

Content-Length: 81\r\n

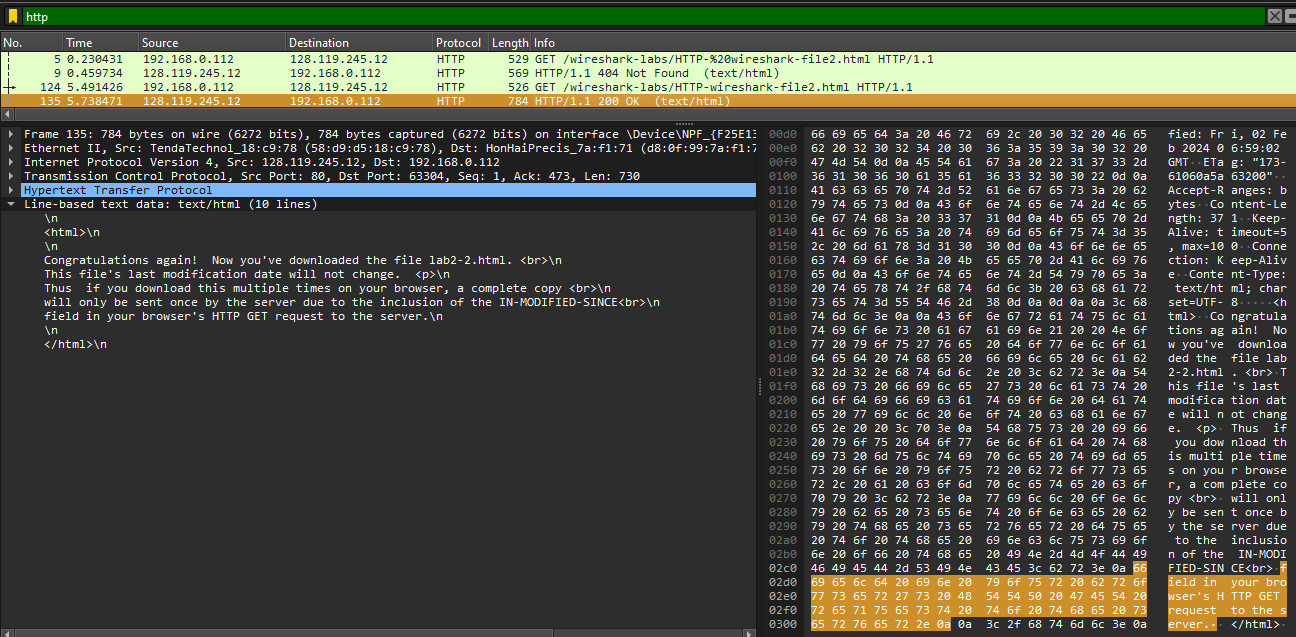
1. **By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.**

No. The raw data appears to match up exactly with what is shown in the packet-listing window.

**2. The HTTP CONDITIONAL GET/response interaction**

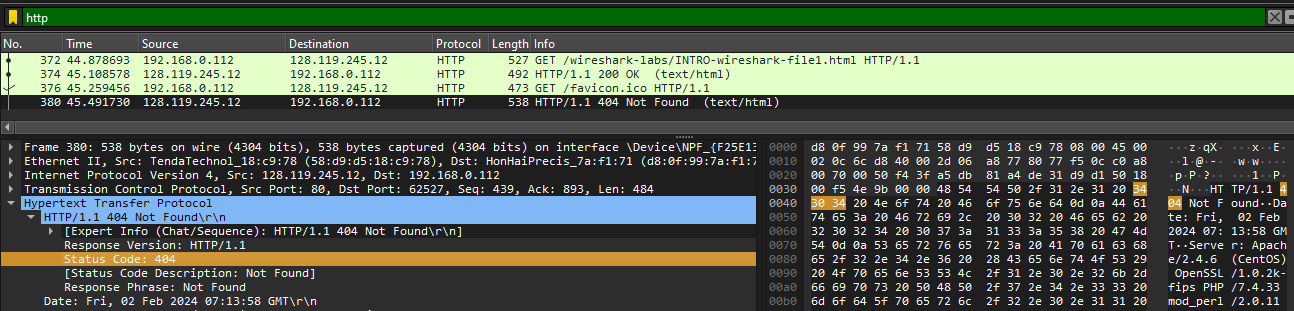
1. **Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?**

No! I can’t see.

1. **Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?**
2. **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?**

No! I can’t see.

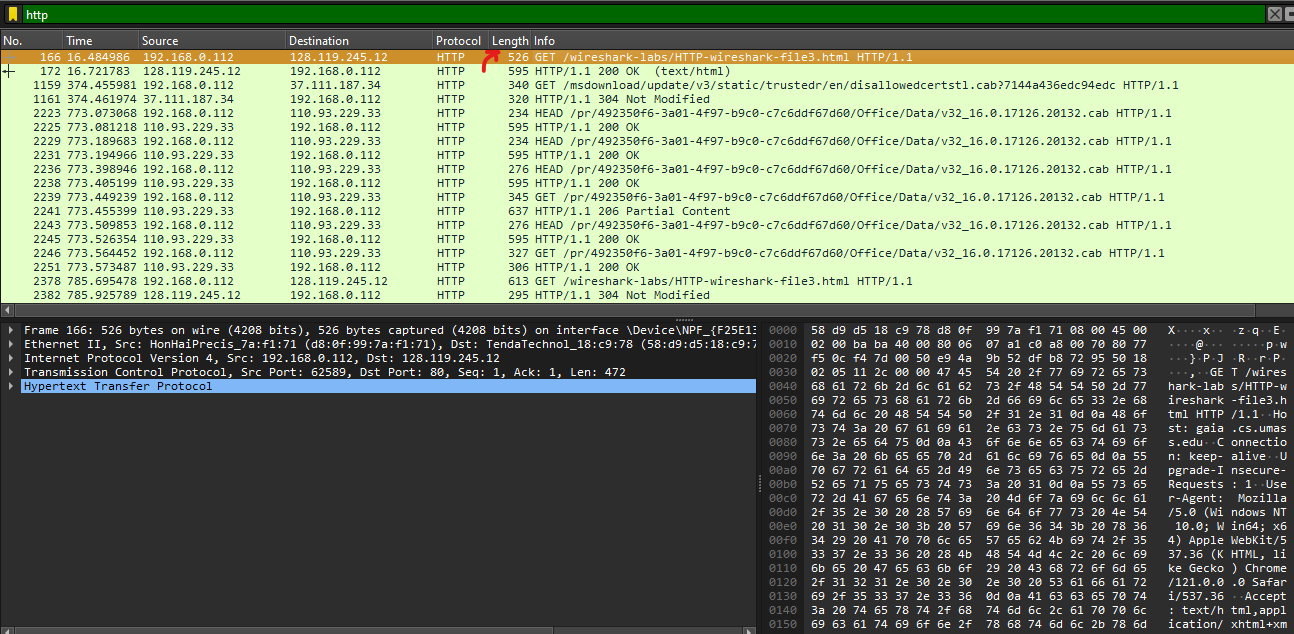
1. **What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.**

****The status code and phrase returned from the server is **HTTP/1.1 404 Not Found\r\n**. The server didn’t return the contents of the file since the browser loaded it from its cache.

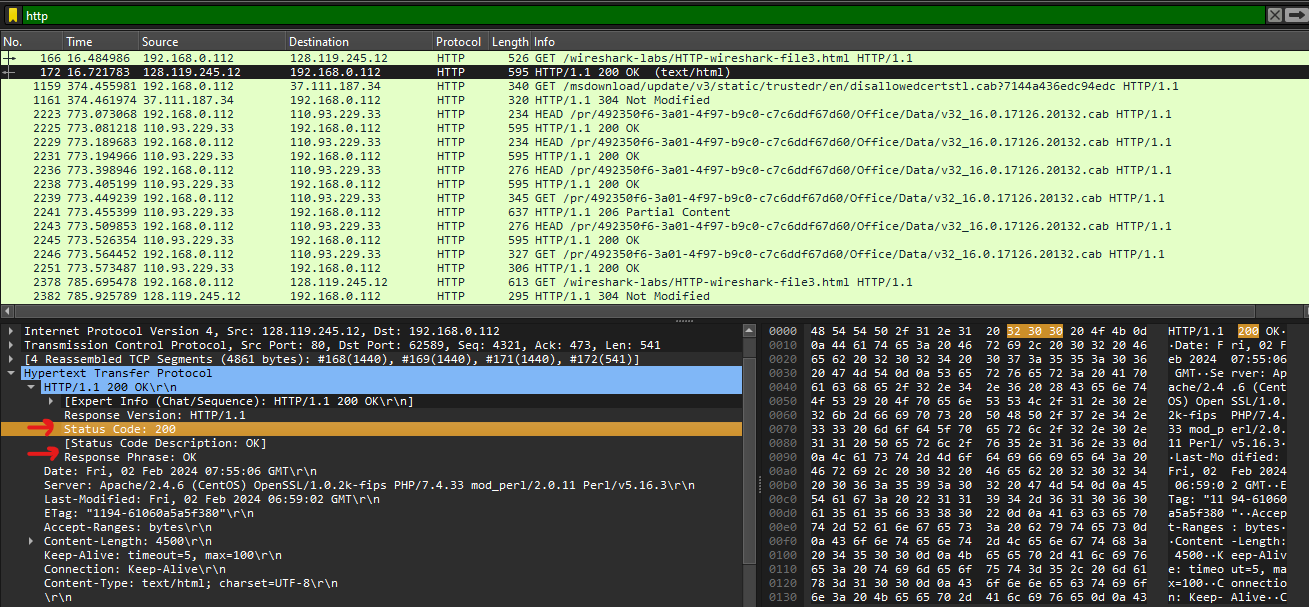
**3. Retrieving Long Documents**

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?**

My browser only sent 1 HTTP GET request to the server. The Packet that contained the GET message was packet number 166.

****

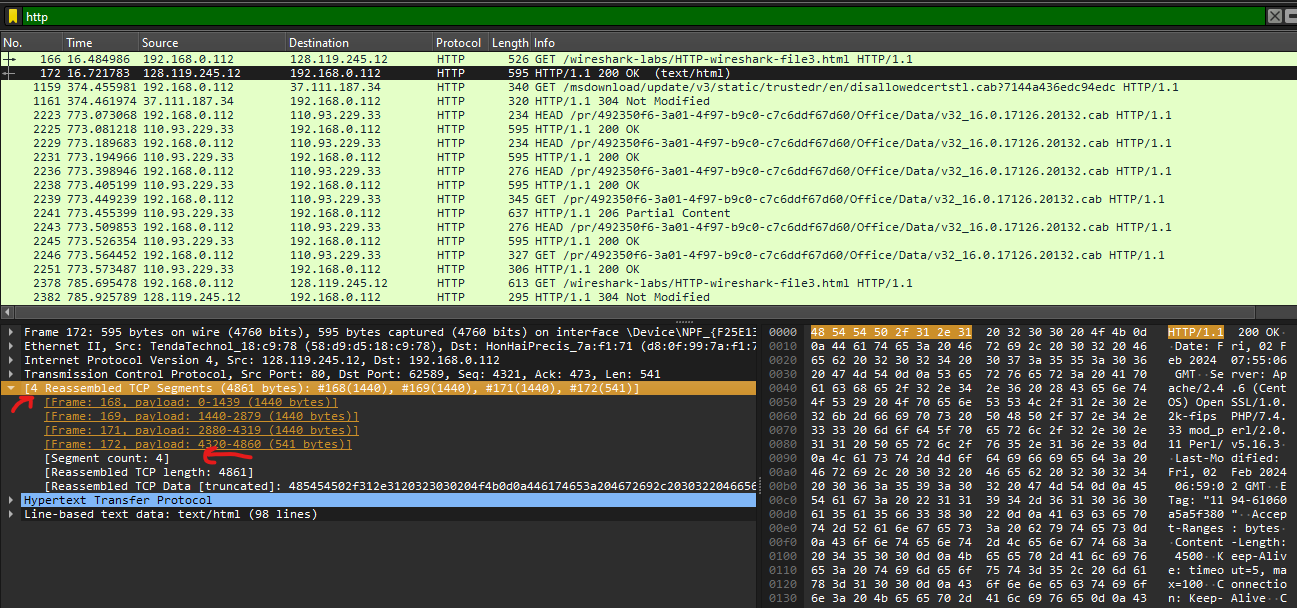
1. **Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?**

The packet that contains the status code and phrase which the server sent in response to the GET message was packet number 172.

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

Status Code: 200, Response Phrase: OK

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

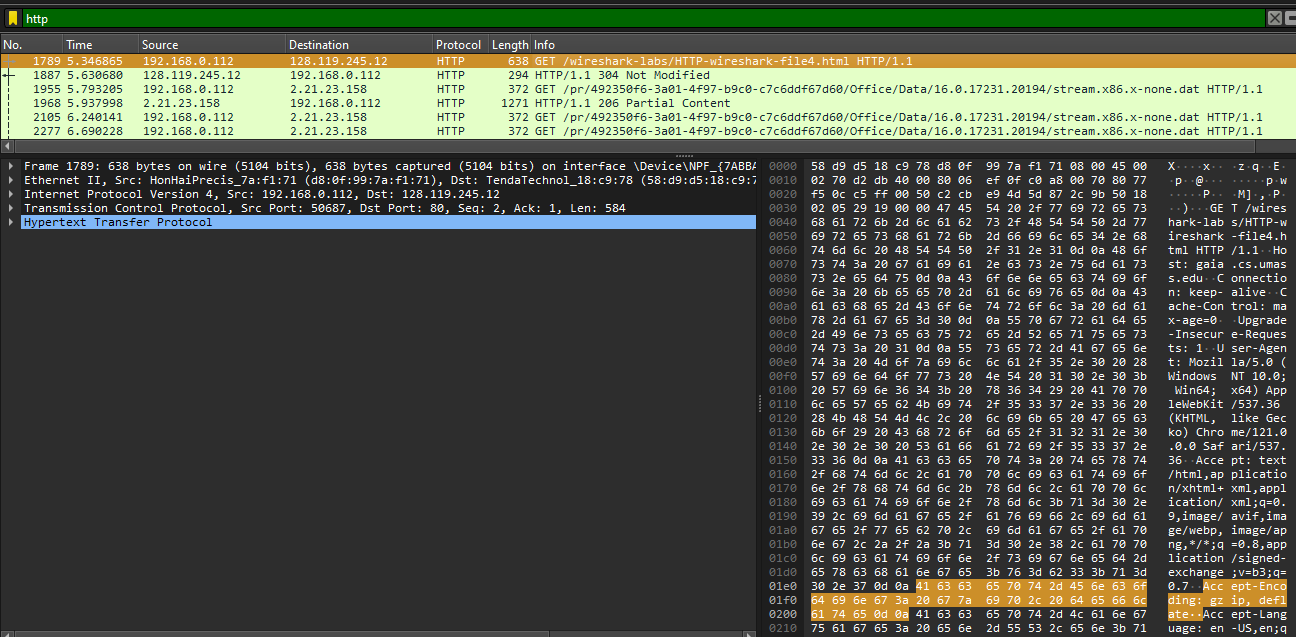
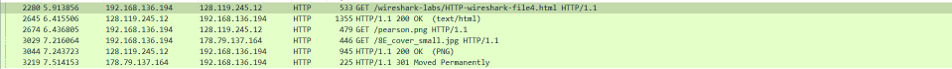
****The data was sent in 4 TCP segments to the browser, then reassembled.

**4. HTML Documents with Embedded Objects**

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

**Solution:**

My browser sent 3 http GET message requests. One each to each for each of the following: The initial page, the Pearson logo, and the cover of the Pearson book, 5th Edition.

****

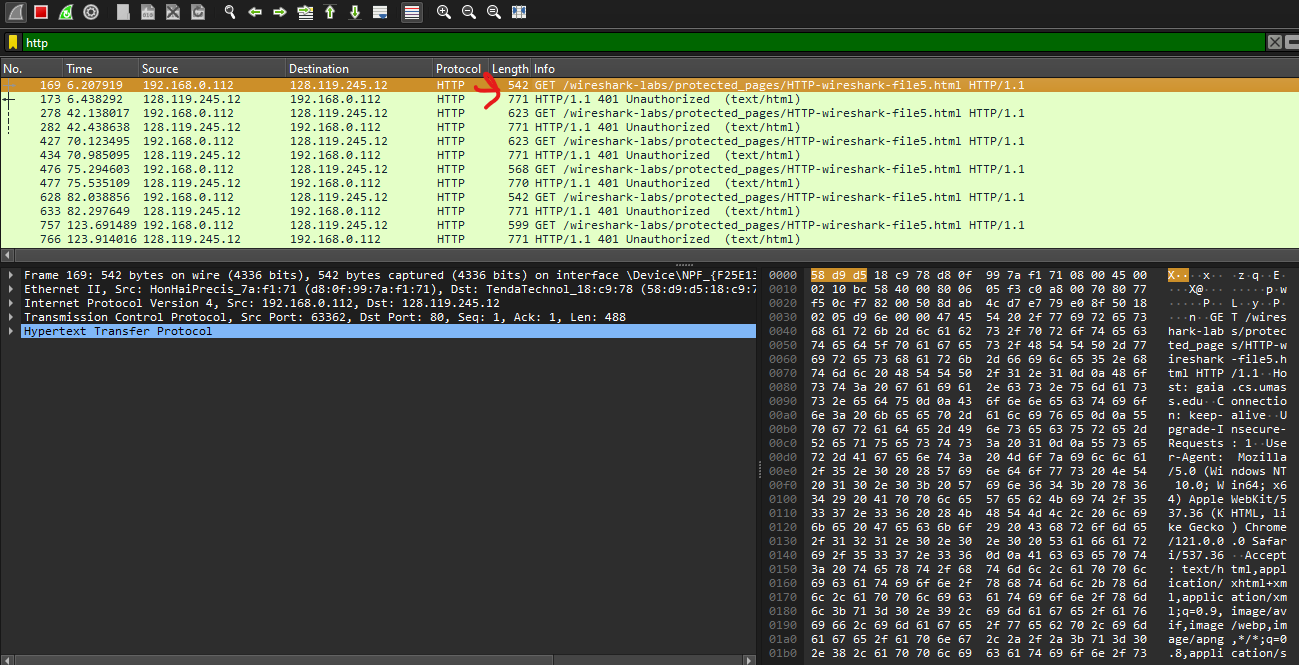
**17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.**

The browser downloaded the two images in serially. I believe this to be the case because the first image was requested and sent before the second image was requested by the browser. Had they been running in parallel, both files would have been requested then would have returned in the same time period. In this case however, the second image was only requested after the first image came back.

**5. HTTP Authentication**

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

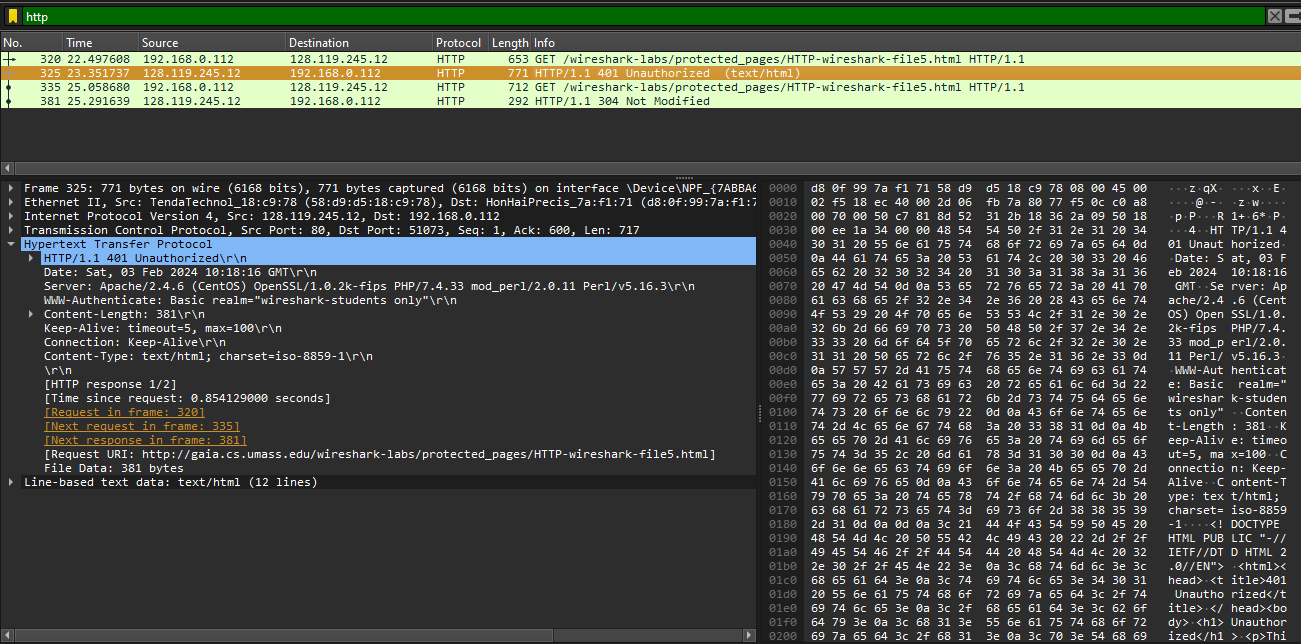
The servers initial response was “401 Authentication Required”

****

**19. When your browser’s sends the HTTP GET message for the second**

**time, what new field is included in the HTTP GET message?**

The new field that is now included is the authorization field. This is included because we sent the server a username and password along with our request stating that we were authorized to receive the page.

****