שם תז

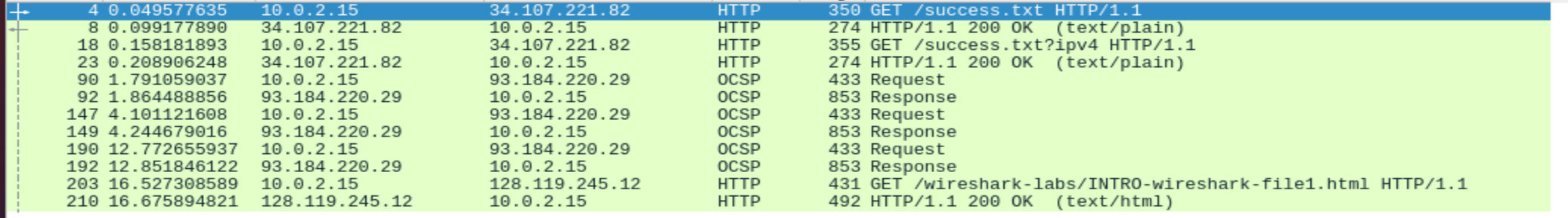
List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

Ans: DNS, HTTP, TCP

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packetlisting 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

Ans:

the time interval between the HTTP GET message and HTTP OK message is 0.1485863



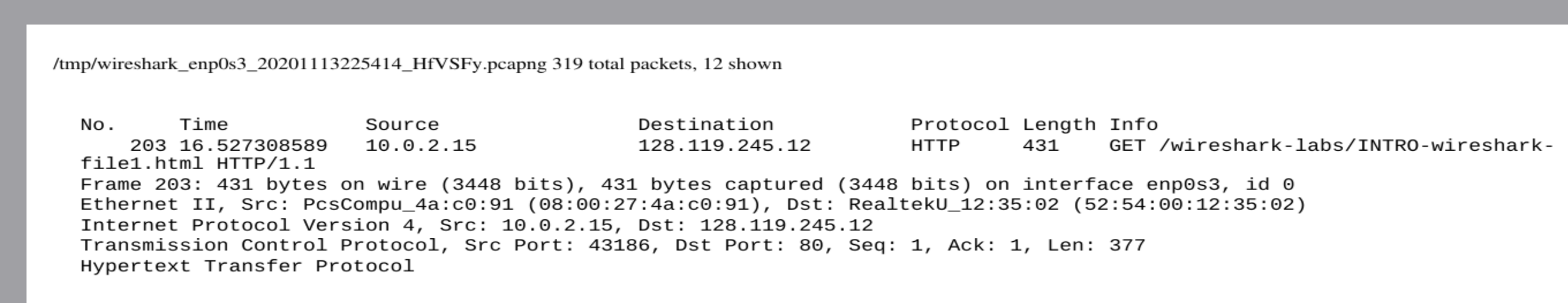
3. What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)? What is the Internet address of your computer?

Ans: Internet address of the gaia.cs.umass.edu: 128.119.245.12

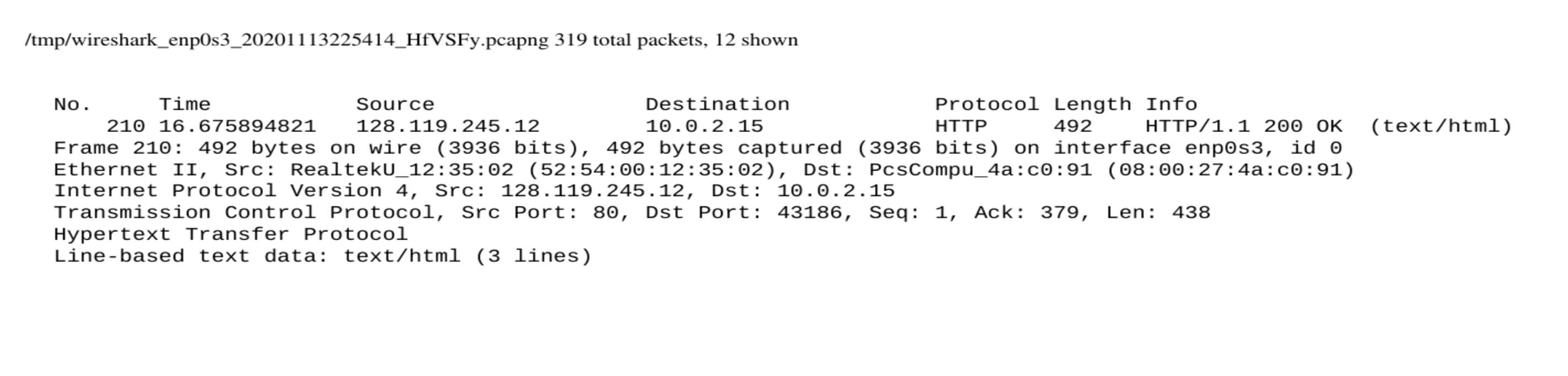
the Internet address of my computer: 192.168.56.1

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

Ans: Get message



OK message



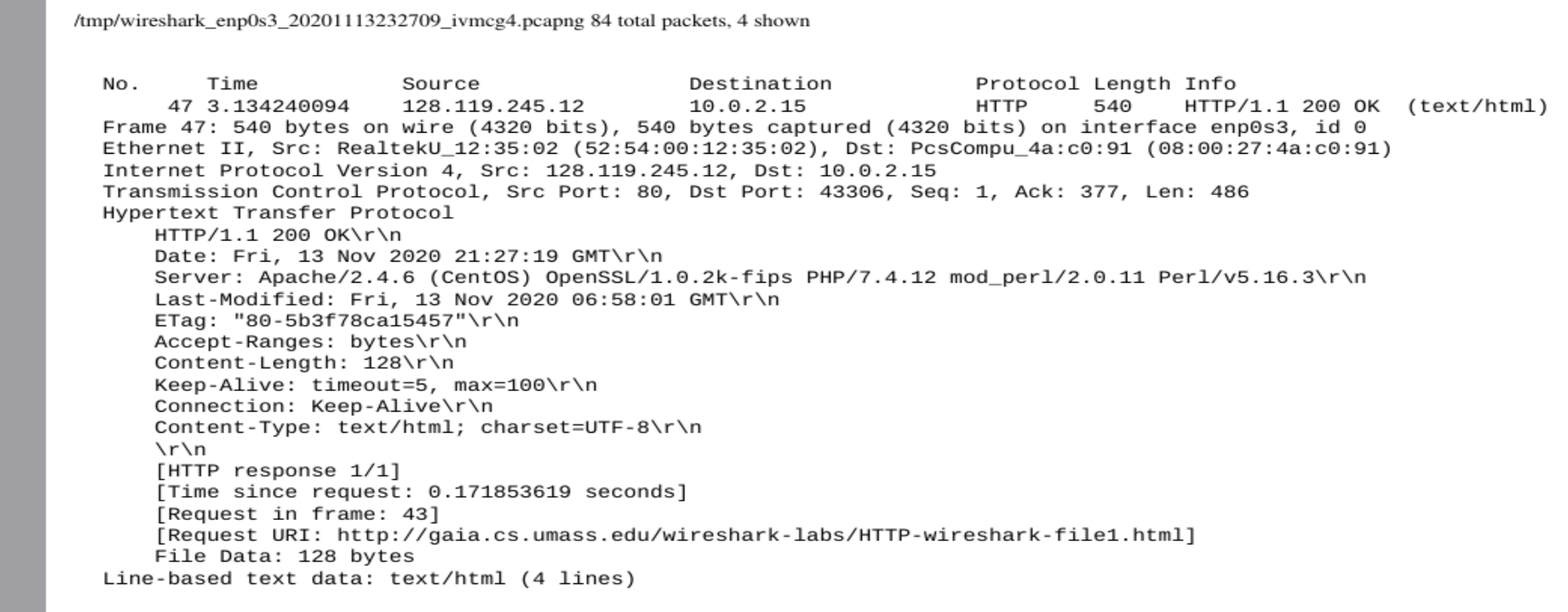
PART 2

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

Ansmy : browser running HTTP version 1.1.







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

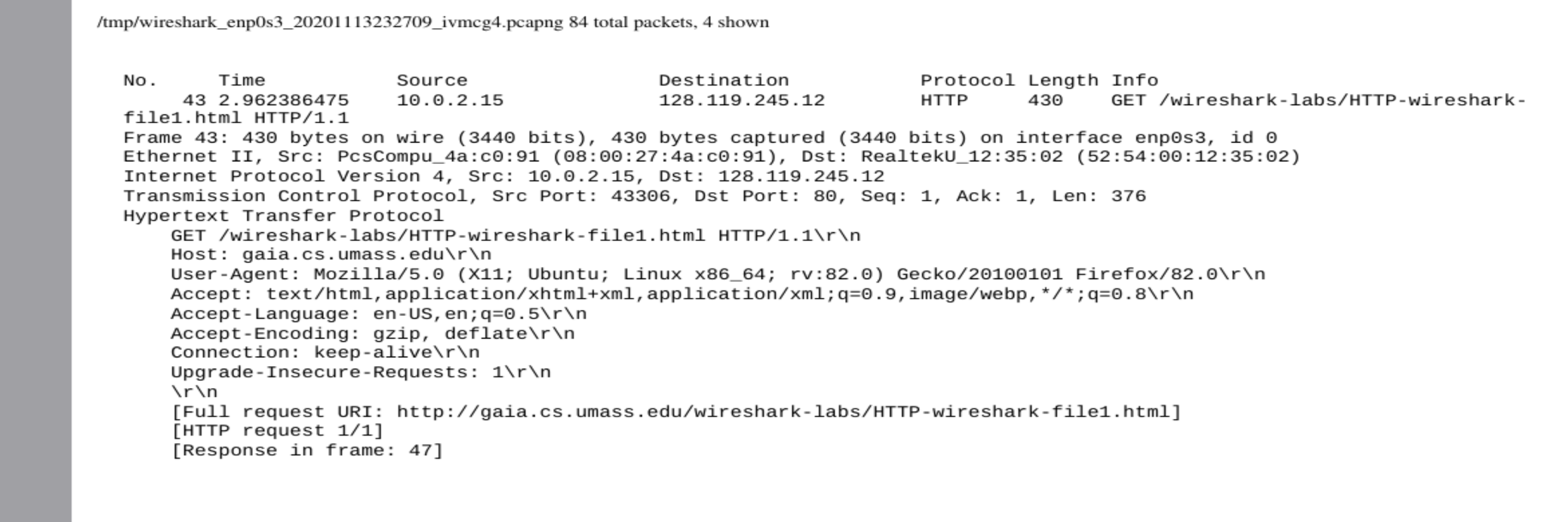
ans: my browser accept – langugge is en-US



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

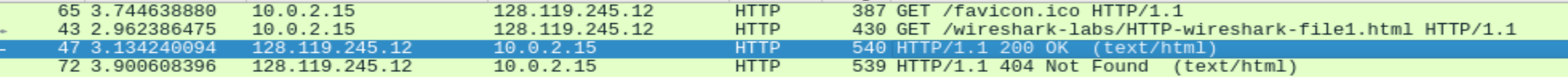
Ans: the IP address of my computer is: 10.0.2.15

the IP address of gaia.cs.umass.edu server is:128.119.245.12



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

Ans: is the status code returned from the server is HTTP/1.1 200 OK



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

Ans: the HTML file that i retrieving last modified at the server is at fri,13 NOV 2020

At 06:58:01



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

Ans: 128 bytes



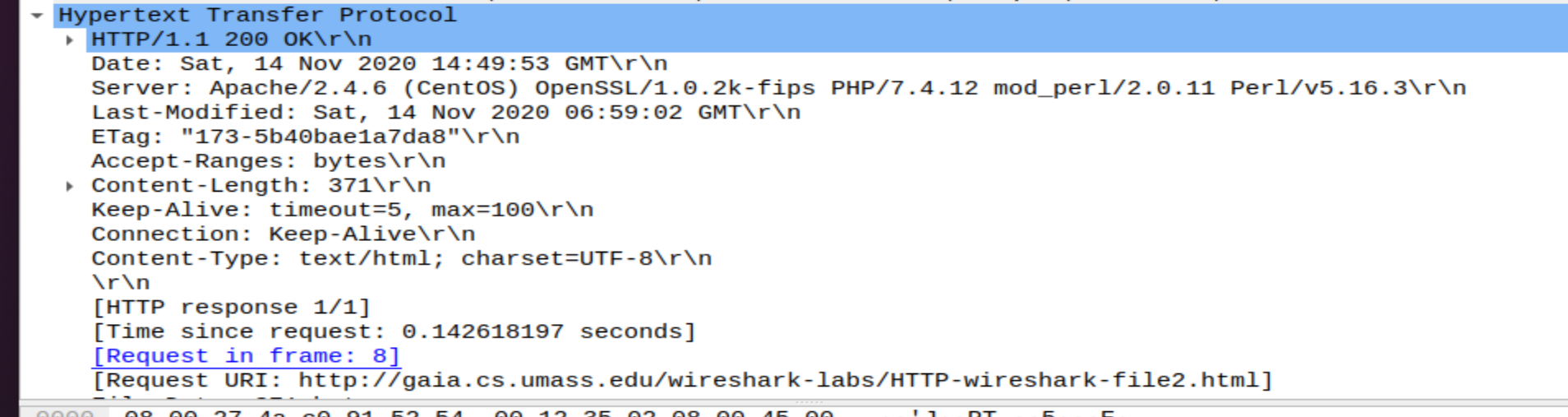
1. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one

Ans:No I could not find

Ans:

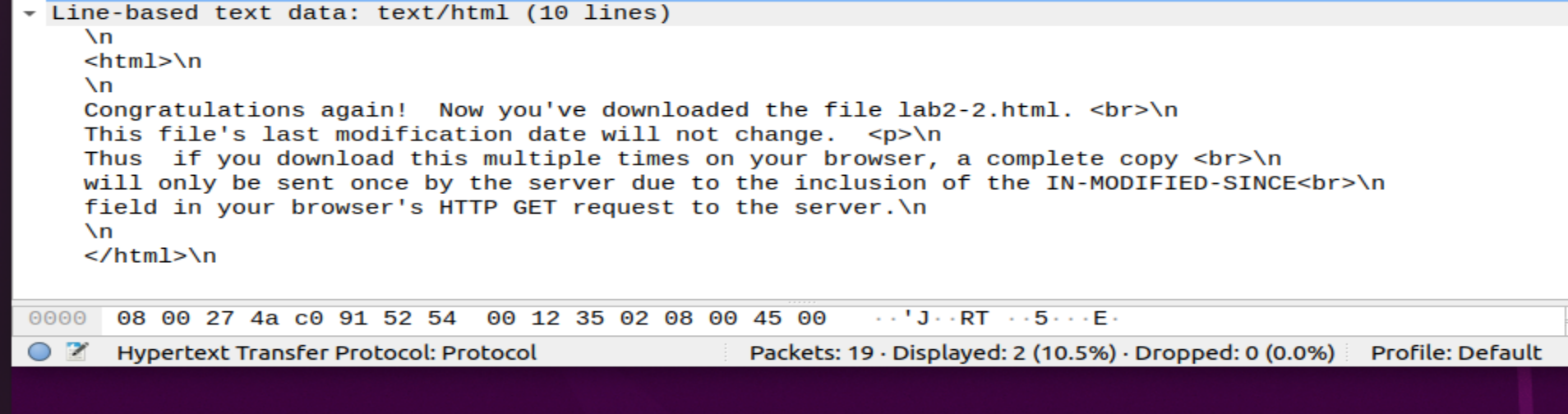
8 . . Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

Ans: No there is no IF-MODIFIED-SINCE line in the GET message.



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

Ans:  Wireshark includes a section titled “Line-Based Text Data” which shows what the server sent back to my browser which is specifically what the website showed when I brought it up on my browser.

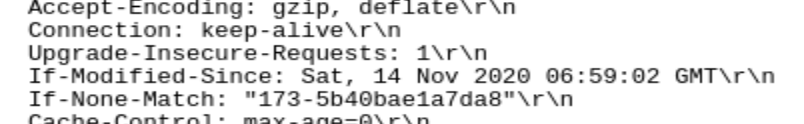


10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

Ans: Yes in the second HTTP message an IF-MODIFIED-SINCE line is included. The information that follows is the date and time that I last accessed the webpage

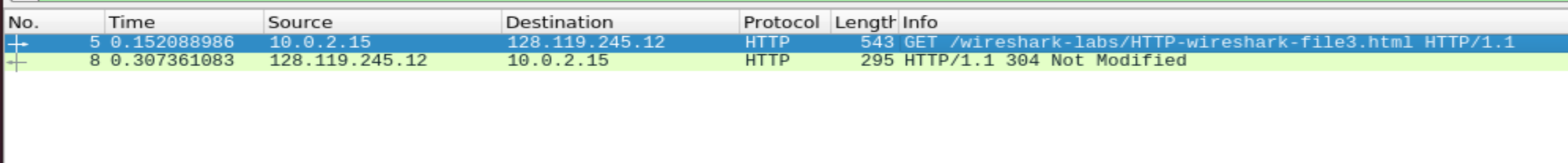
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain

Ans: Yes in the second HTTP message an IF-MODIFIED-SINCE line is included. The information that follows is the date and time that I last accessed the webpage



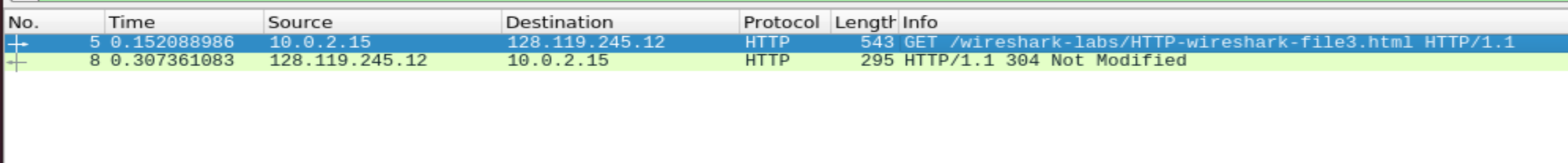
12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

Ans: My browser only sent 1 HTTP GET request to the server the Packet that contained the GET message was packet number 5.



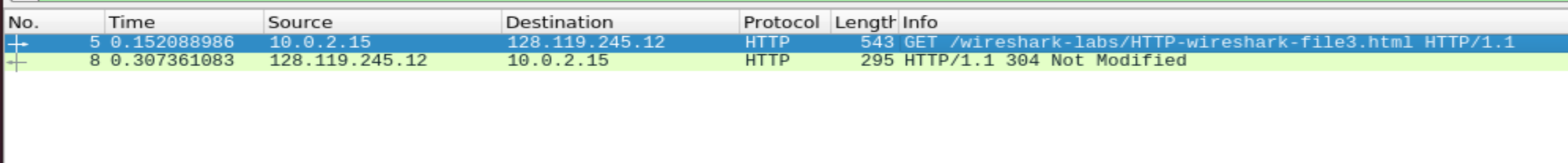
13**. *Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?***

***Ans:*** The packet that contains the status code and phrase which the server sent in response to the GET message was packet number 8.



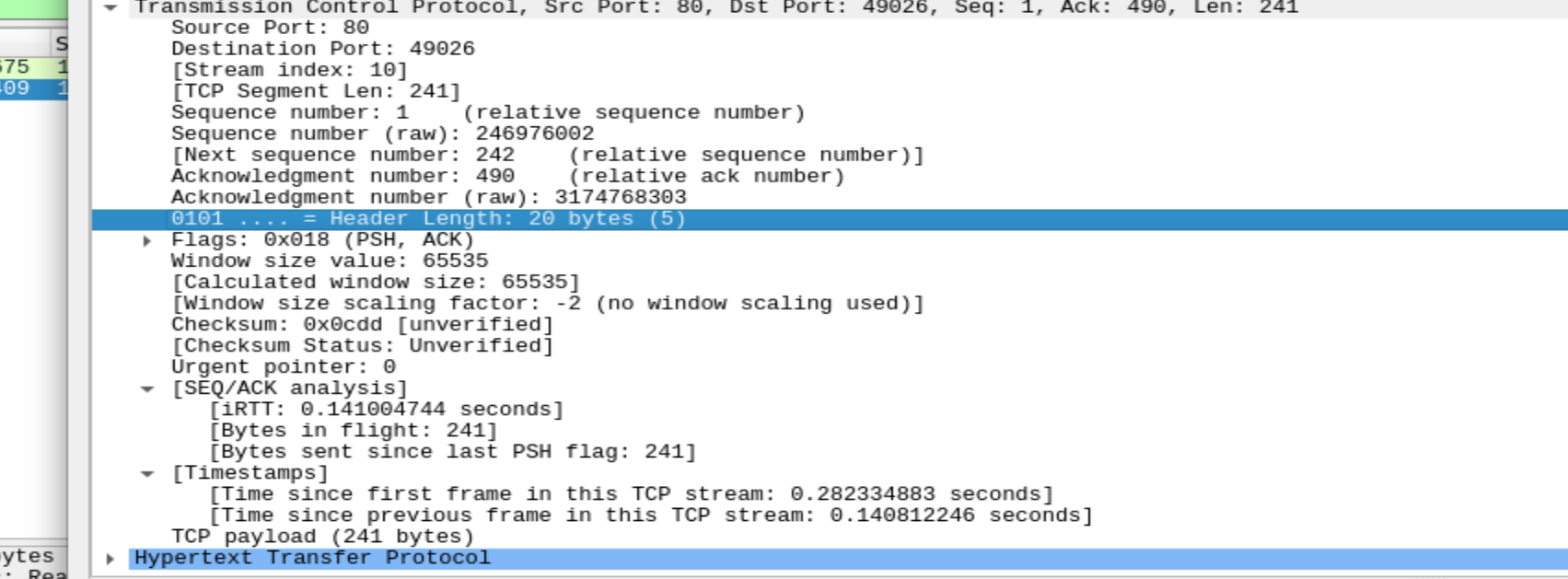
**14. What is the status code and phrase in the response?**

Ans: The code and phrase in the response was 304 Not Modified.



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

Ans: The data was sent in 5 TCP segments to the browser, then reassembled.



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

Ans:

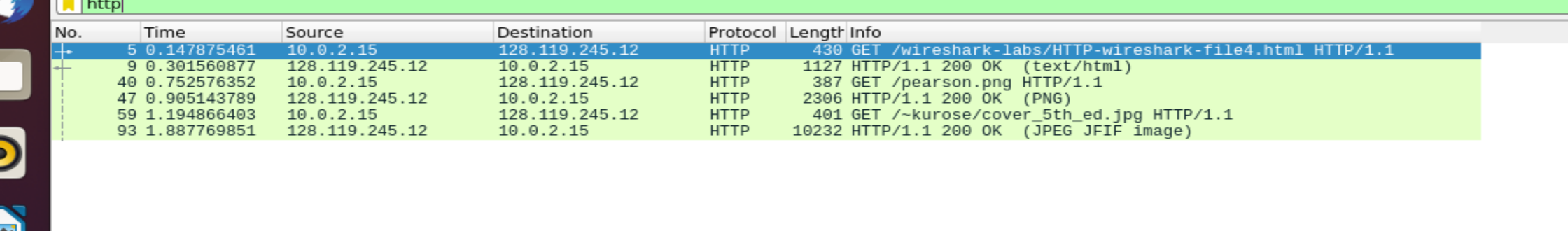
My browser sent 3 http GET message requests. One each to each for each of the following: The

initial page, the Pearson logo, and the cover of the Pearson book, 5th Edition.

Initial Page address: 128.119.245.12

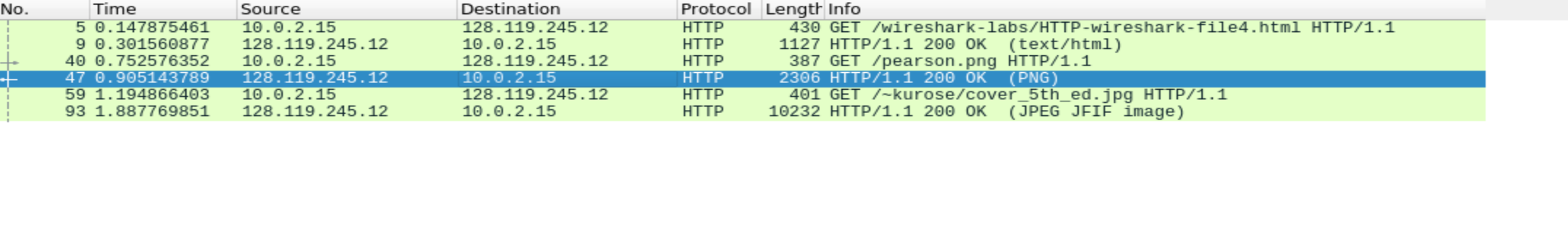
Pearson Logo: 128.119.245.12

Pearson book, 5th Edition: 128.119.245.12



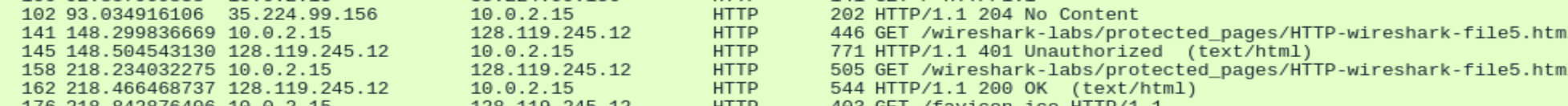
**17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.**

Ans: This is because the first image was requested and sent before the second image was requested by the browser. If they were running in parallel, both files would be prompted and then returned in the same amount of time.



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

Ans: The servers intial response was “401 unauthorized”



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:

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.

