**Aaron Koli**

**1001777604**

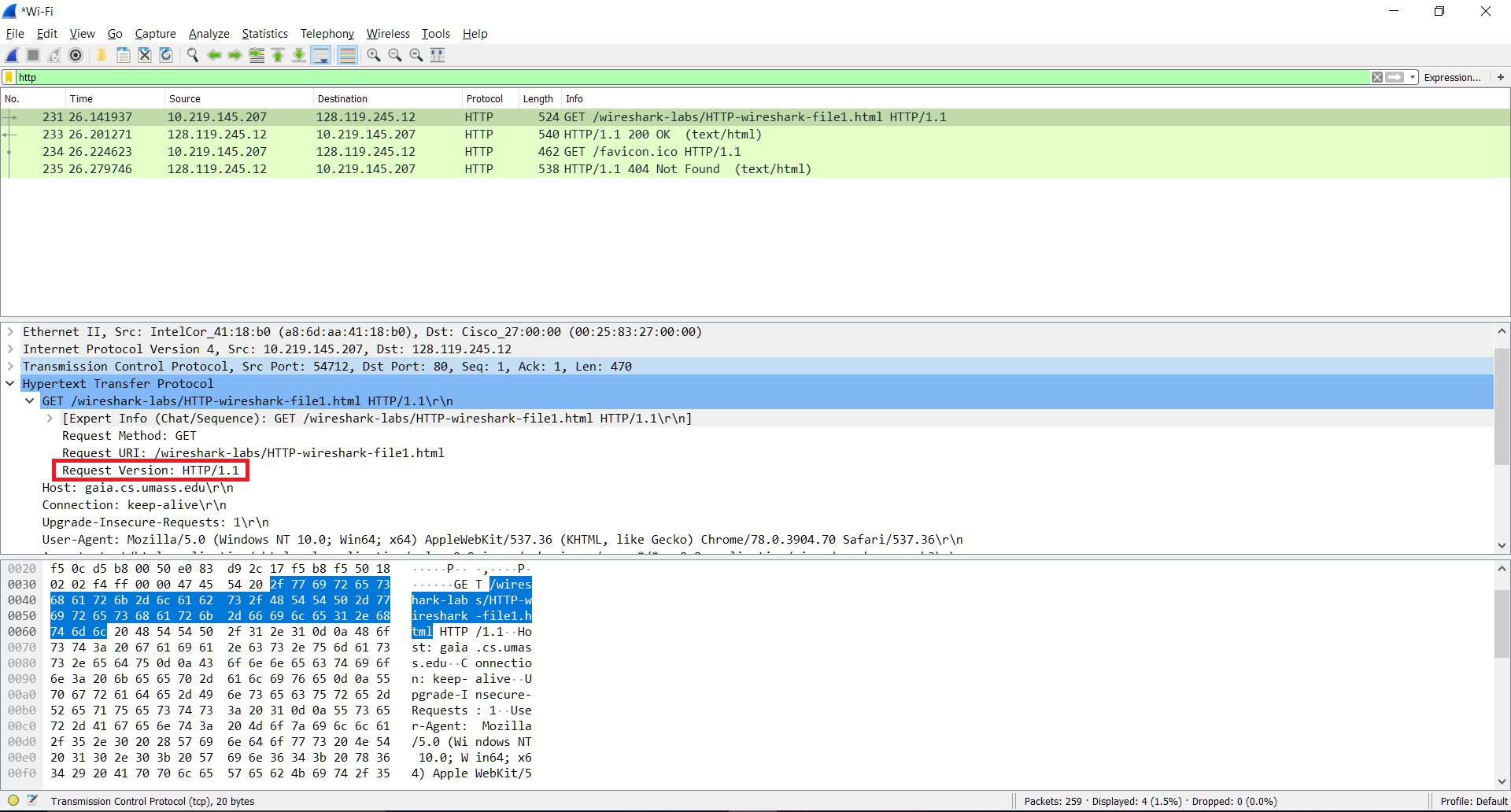
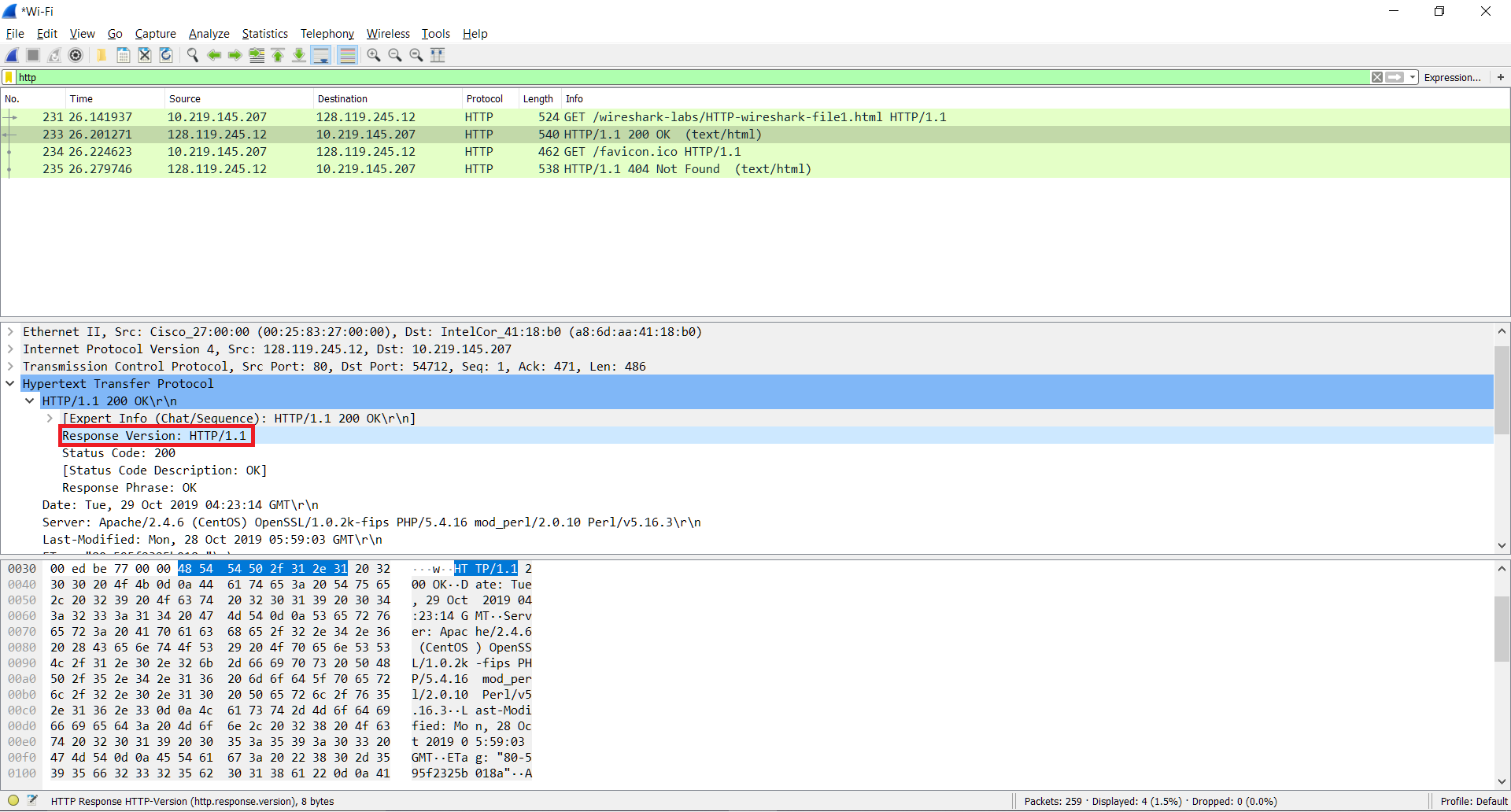
**CSE4344/5344 – Project 2 (Fall 2019)**

**Wireshark Lab: HTTP**

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?

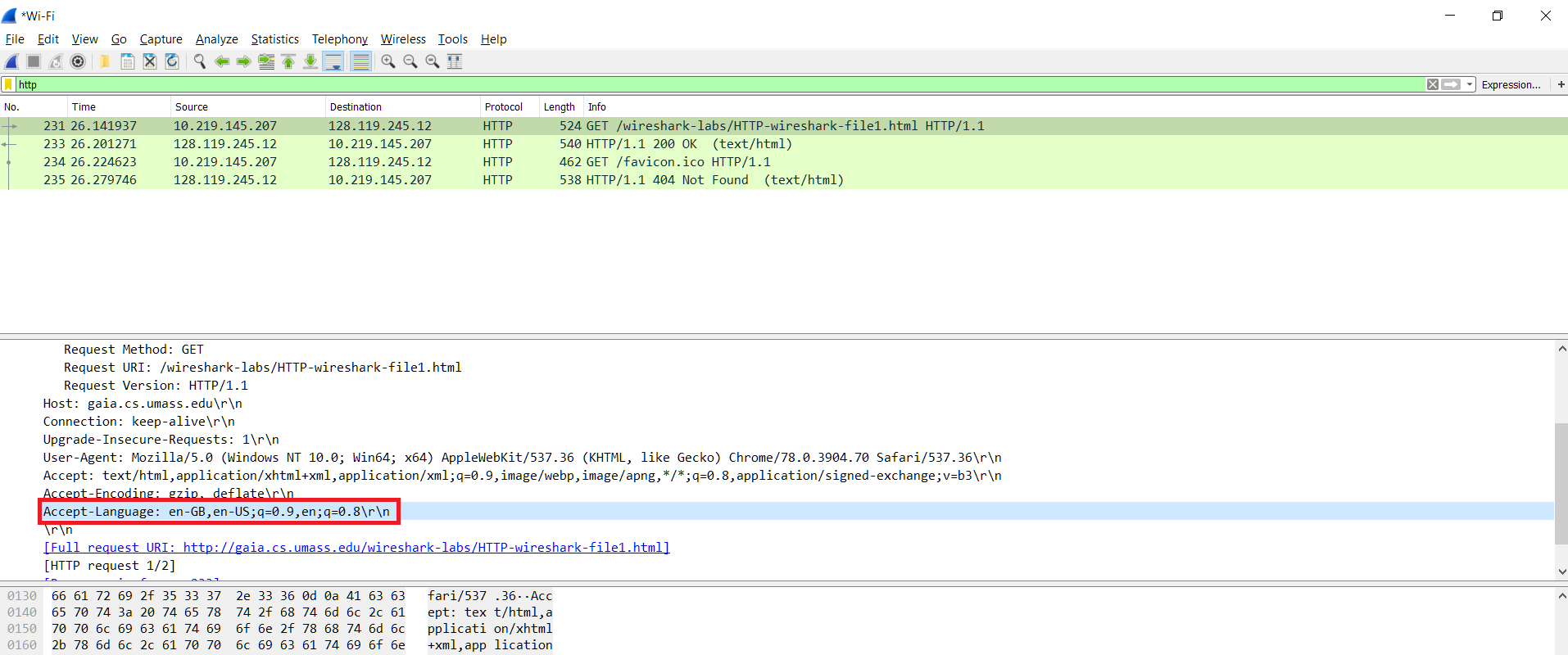
Ans. My browser is running HTTP version 1.1. The Server is also running HTTP version 1.1.

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

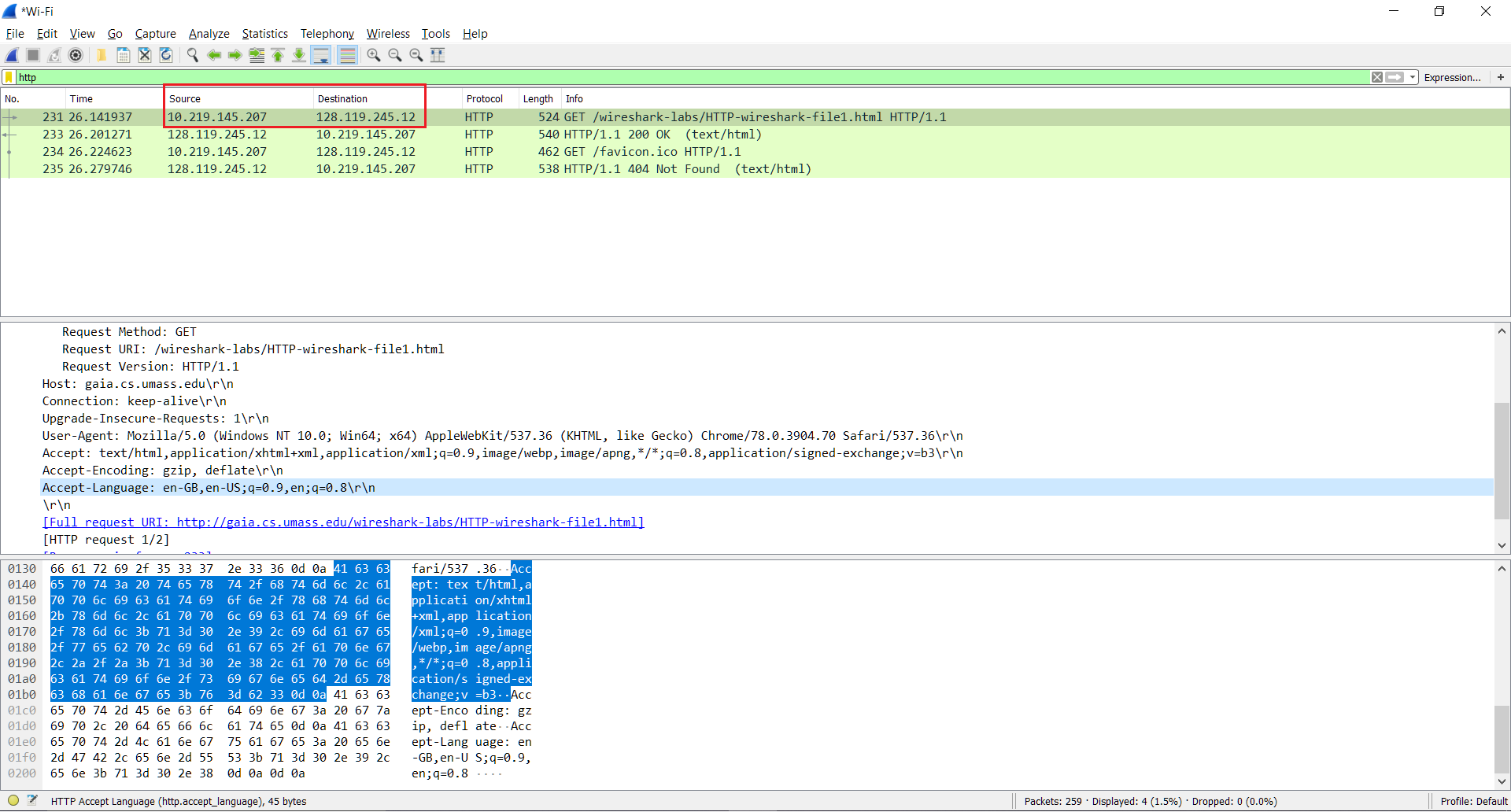
Ans. The browser indicates that it can accept an en-US means American English and en-GB means British English.

Accept-Language: en-GB,en-US;q=0.9,en;q=0.8



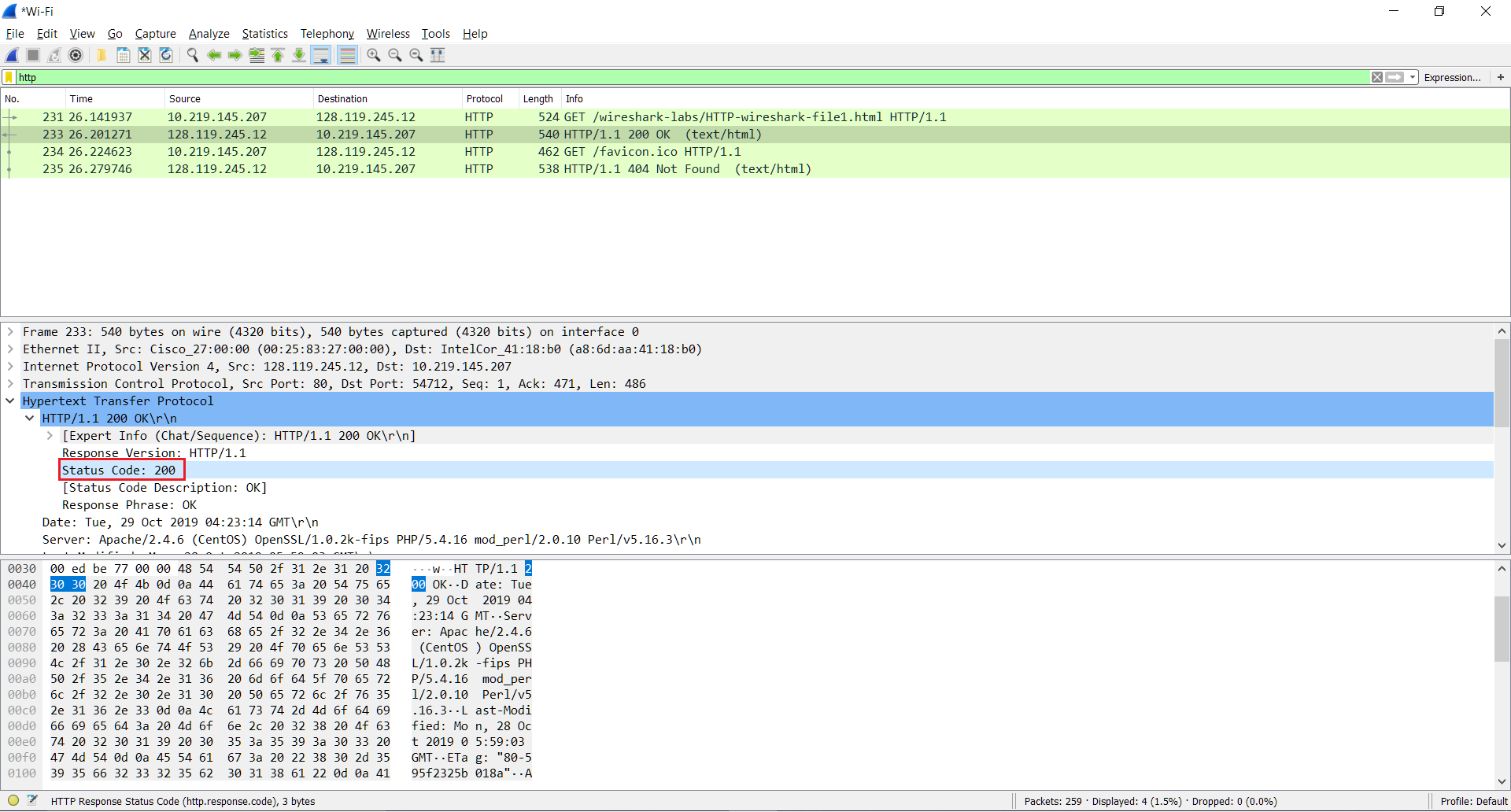
3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

Ans. The IP address of my computer is10.219.145.207 and the server IP is 128.119.245.12



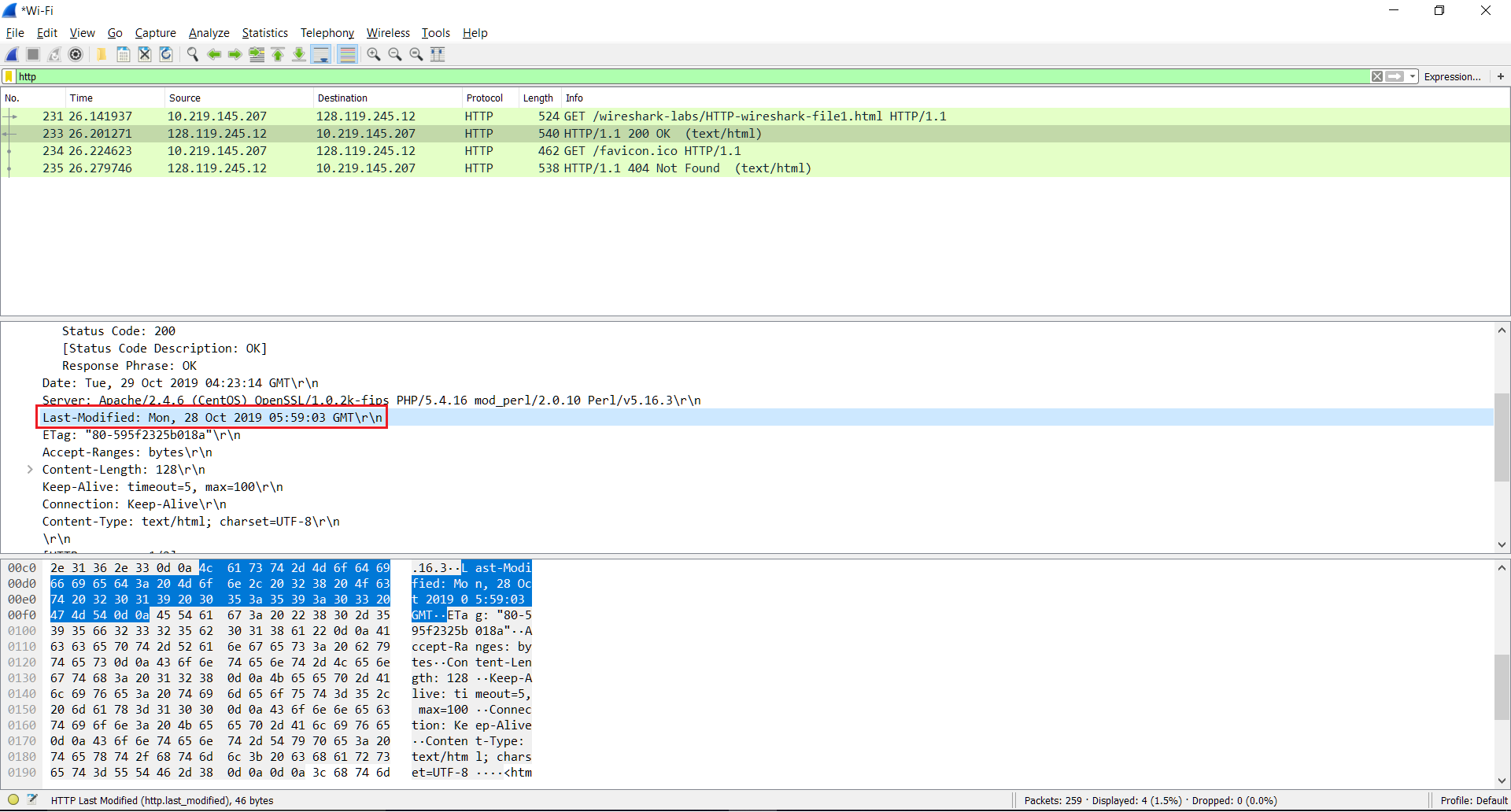
4. What is the status code returned from the server to your browser?

Ans. 200 OK is the status code returned to the browser.



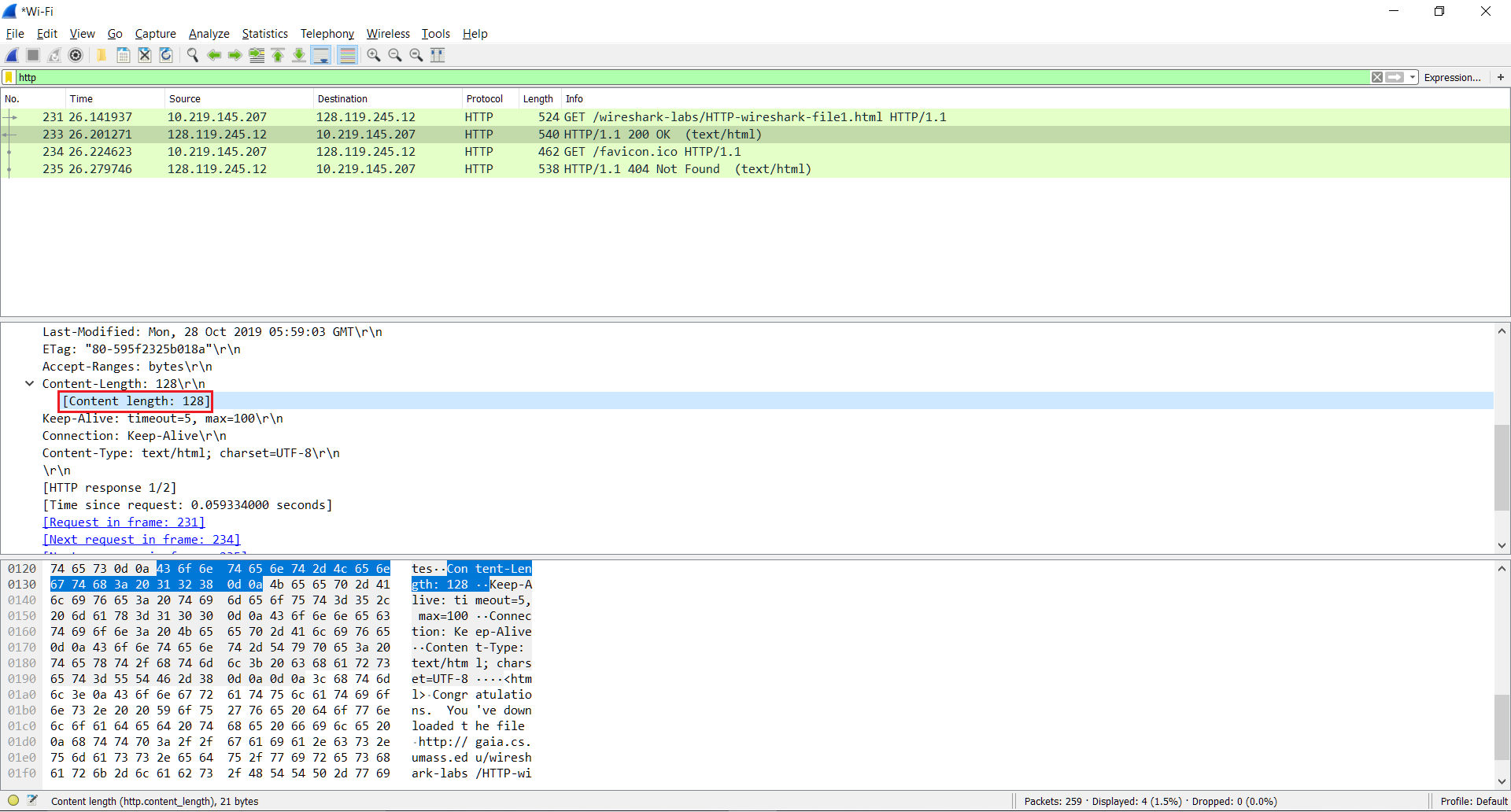
5. When was the HTML file that you are retrieving last modified at the server?

Ans. The HTML file was last modified on Monday, 28 Oct 2019 05:59:03 GMT



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

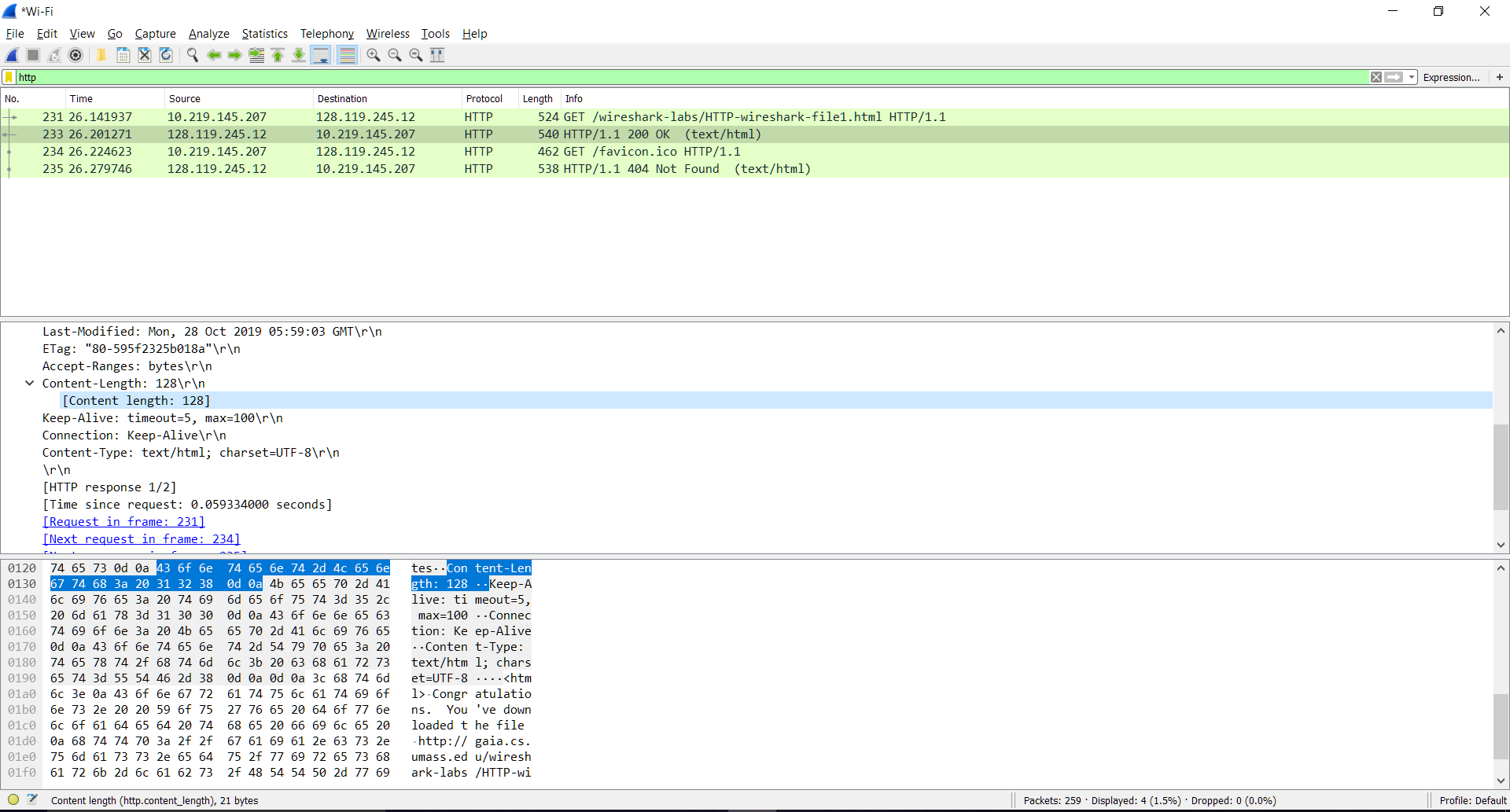
Ans. 128 bytes of content is being returned to the browser.



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. Yes, we do see headers within the packet content window that are not displayed in the packet-listing window.

File Data, Status Code, Response Phrase, Accept Language, Date are some of them.



2. The HTTP CONDITIONAL GET/response interaction

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?

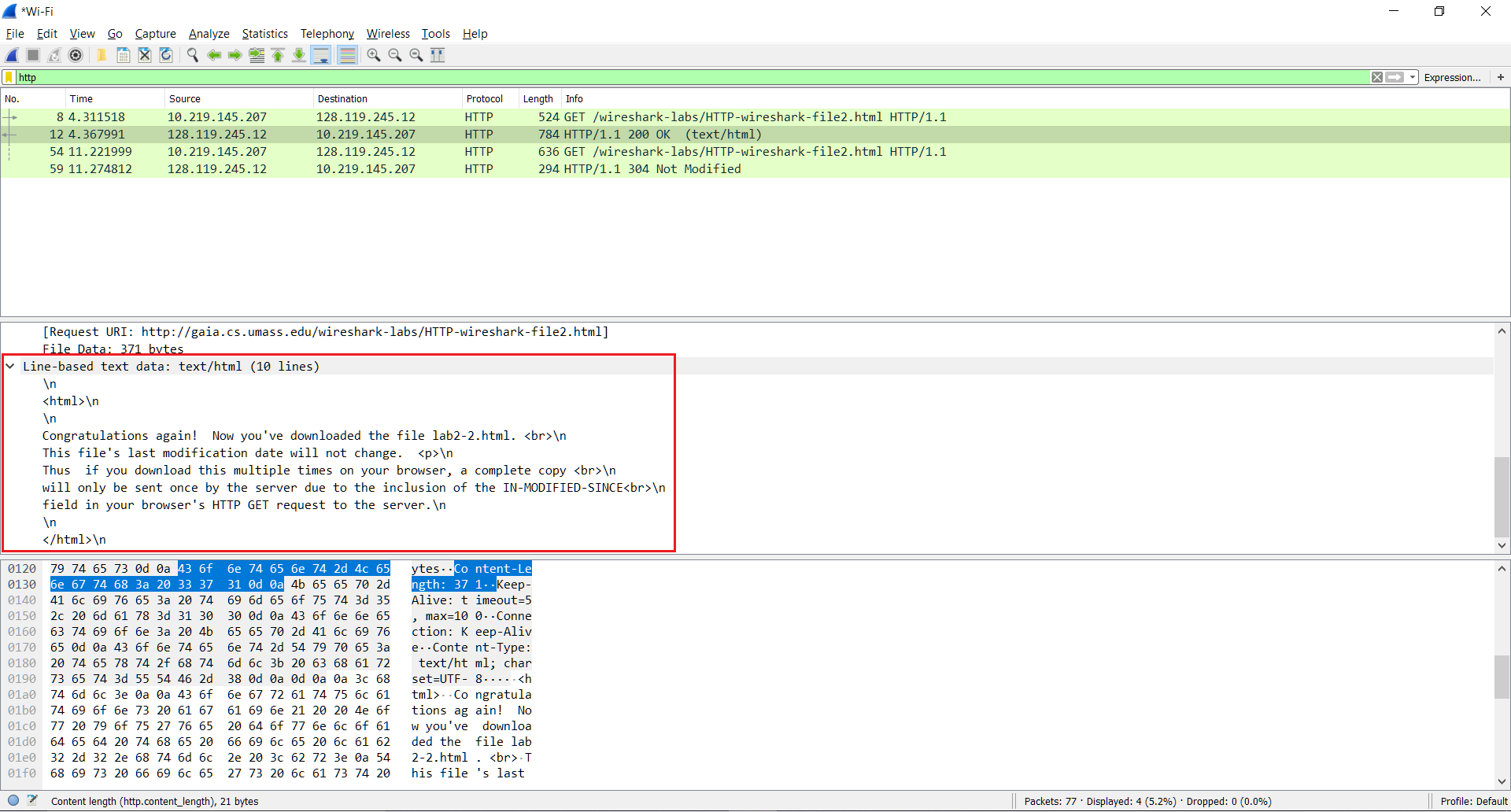
Ans. No, there is no IF-MODIFIED-SINCE line in the first HTTP GET.

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 did return the contents of the file as there is a “Line-based text data” line and under it is the text.

Yes, the server did return the contents of the file as there is a “Line-based text

data” line and under it is the tex



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:” line in the second HTTP GET request and it has a date of Tuesday, 29 Oct 2019 05:59:01 GMT.

Yes, there is an “IF-MODIFIED-SINCE” line in the second GET request and

it follows with a date of Monday September 25, 2017 05:59:01

Yes, there is an “IF-MODIFIED-SINCE” line in the second GET request and

it follows with a date of Monday September 25, 2017 05:59:01

Yes, there is an “IF-MODIFIED-SINCE” line in the second GET request and

it follows with a date of Monday September 25, 2017 05:59:01

Yes, there is an “IF-MODIFIED-SINCE” line in the second GET request and

it follows with a date of Monday September 25, 2017 05:59:01

Yes, there is an “IF-MODIFIED-SINCE” line in the second GET request and

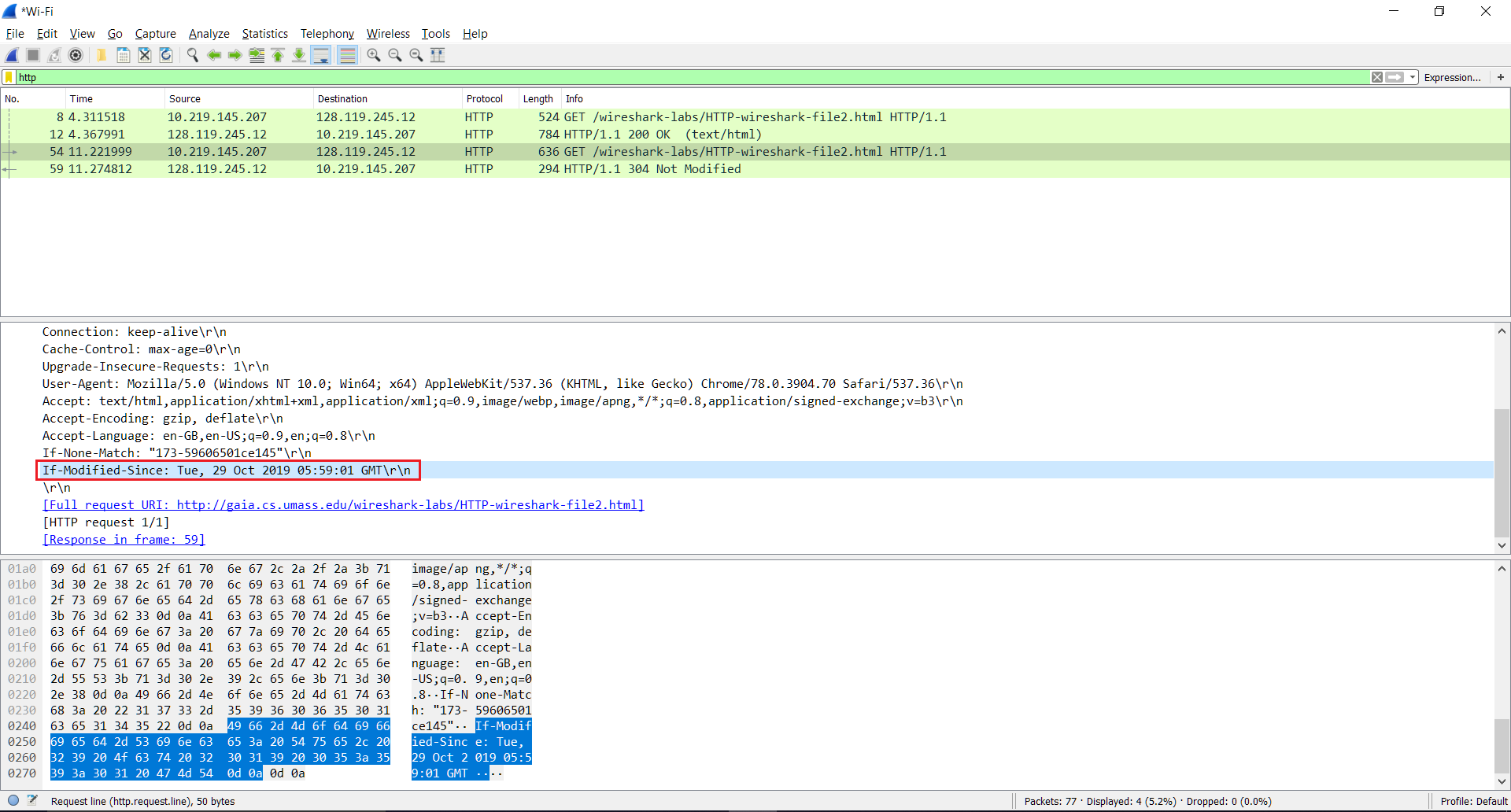
it follows with a date of Monday September 25, 2017 05:59:01

Yes, there is an “IF-MODIFIED-SINCE” line in the second GET request and

it follows with a date of Monday September 25, 2017 05:59:01

Yes, there is an “IF-MODIFIED-SINCE” line in the second GET request and

it follows with a date of Monday September 25, 2017 05:59:01

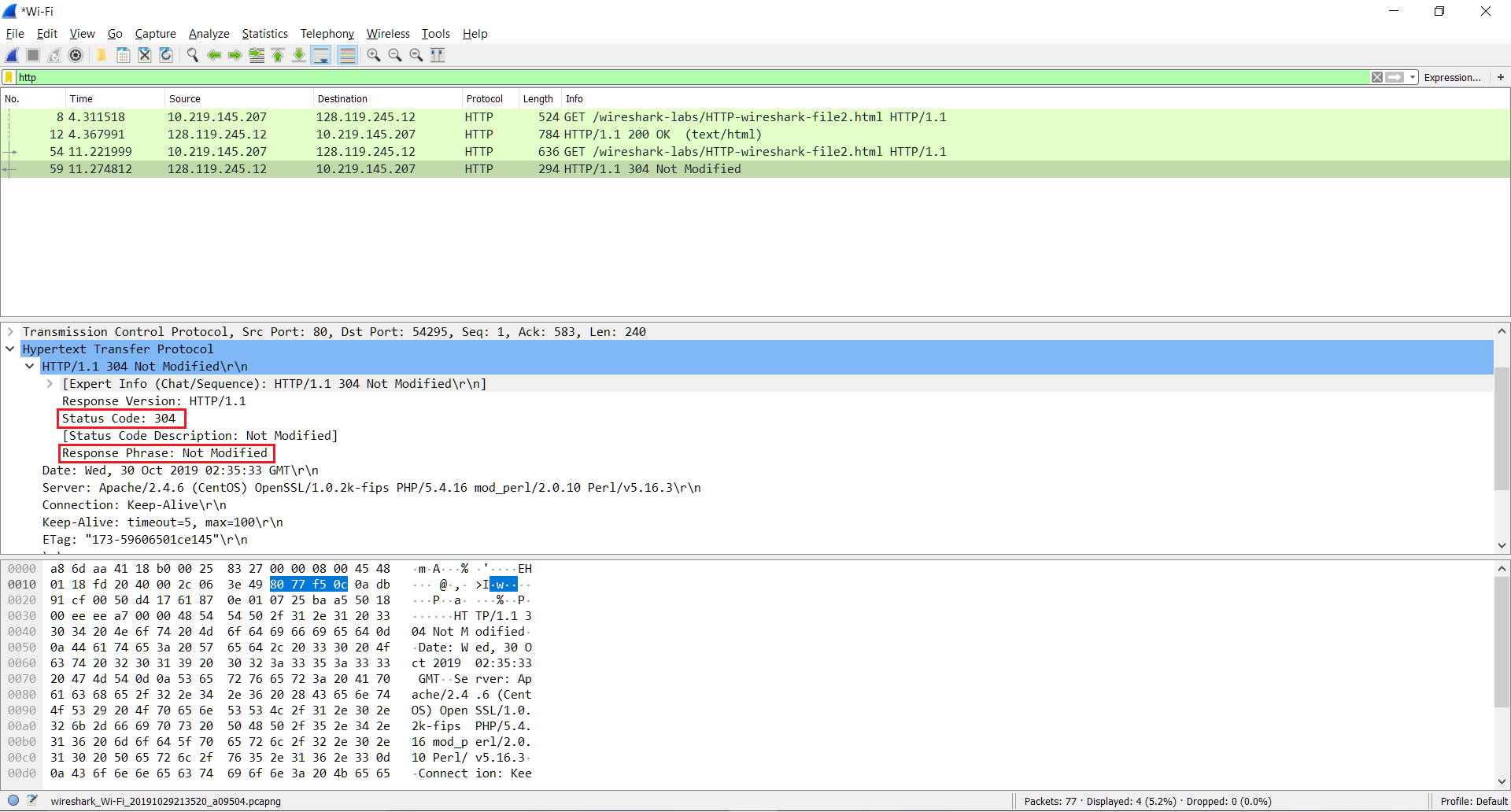


11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

Ans. Status Code – 304

Phrase returned – Not Modified

No, the server explicitly did not return the contents of the file. In the image below as we can see we got a GET request, then a HTTP response, then a GET request and lastly a HTTP response. Because, in the first response the server did return the contents of the file and since the contents of the file have not been modified, it returned the status code as 304 and phrase as not modified.



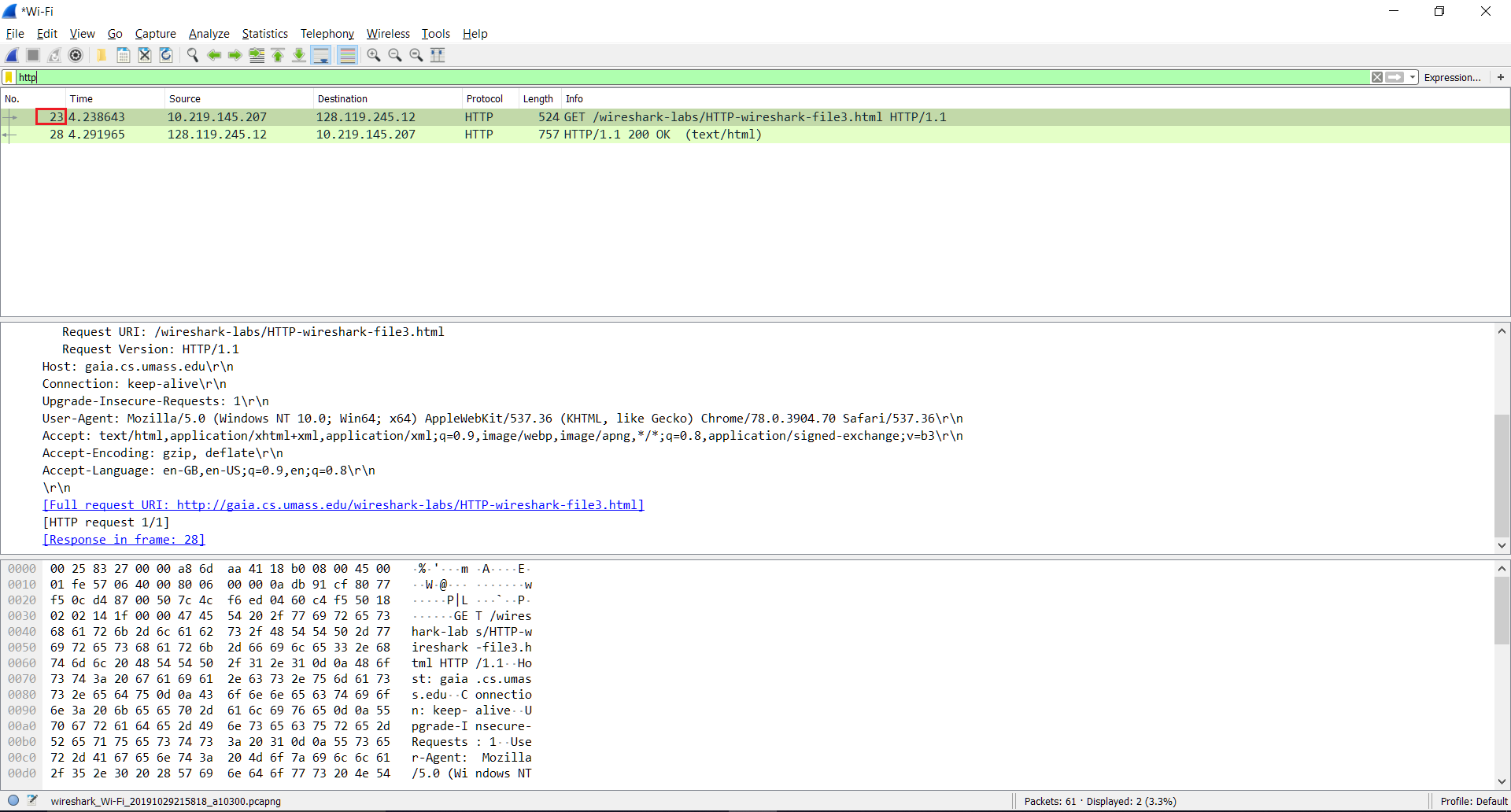
3. Retrieving Long Documents

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?

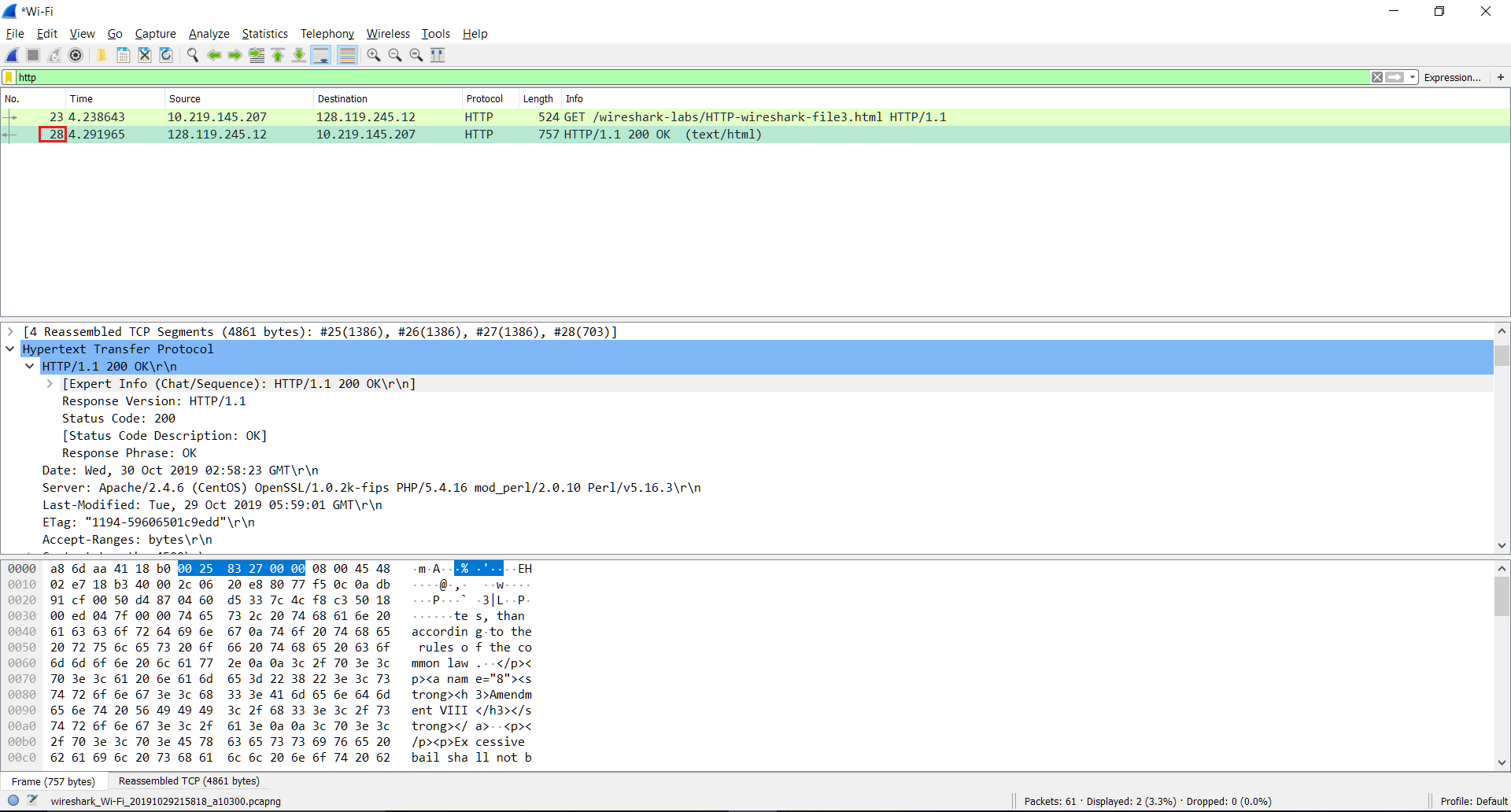
Ans. The browser sent only one HTTP GET request message.

Packet number containing the GET message for the Bill of Rights is 23.



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

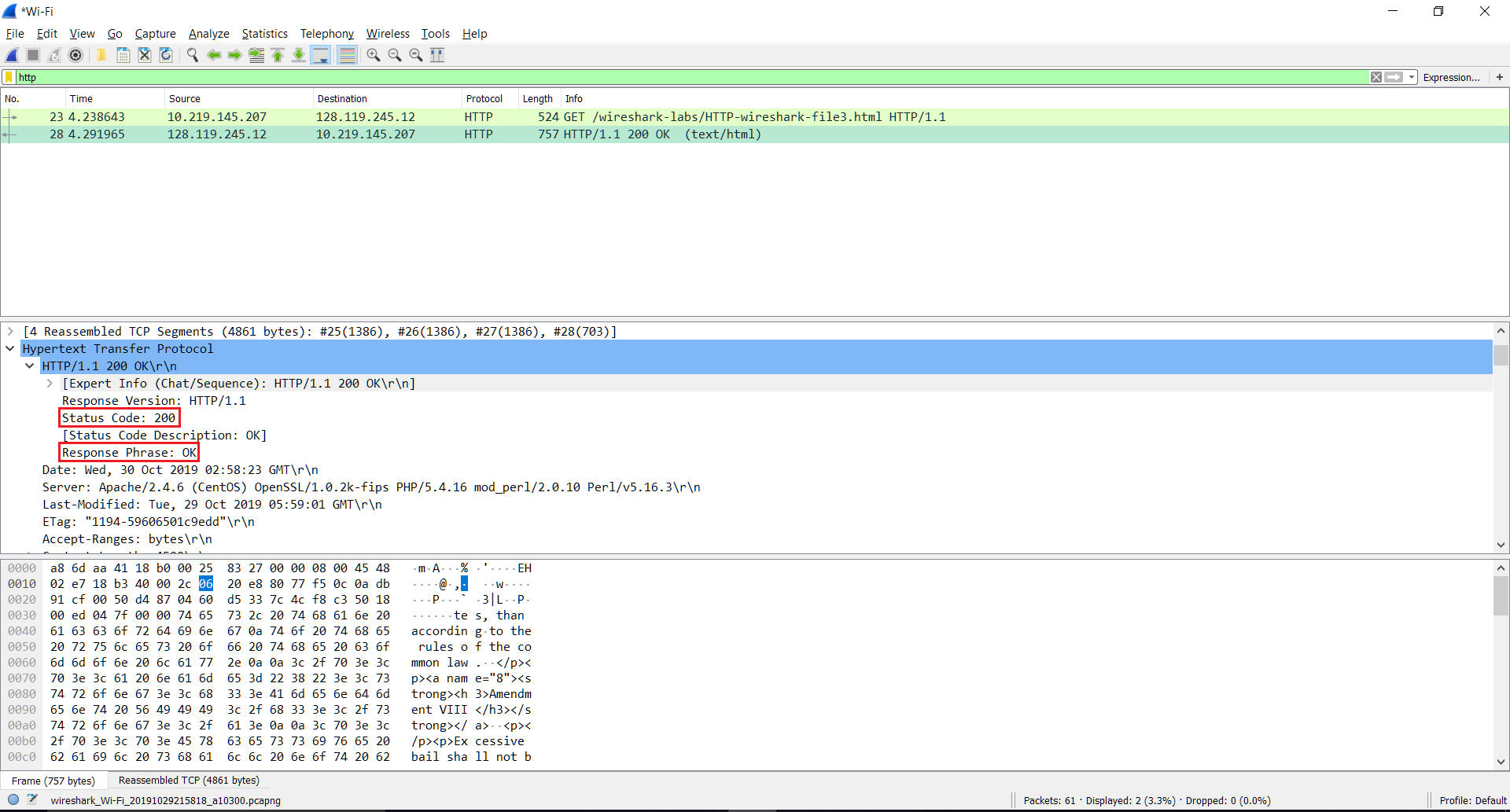
Ans. Packet number 28 in the trace contains the status code and phrase associated with the response to the HTTP GET request.



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

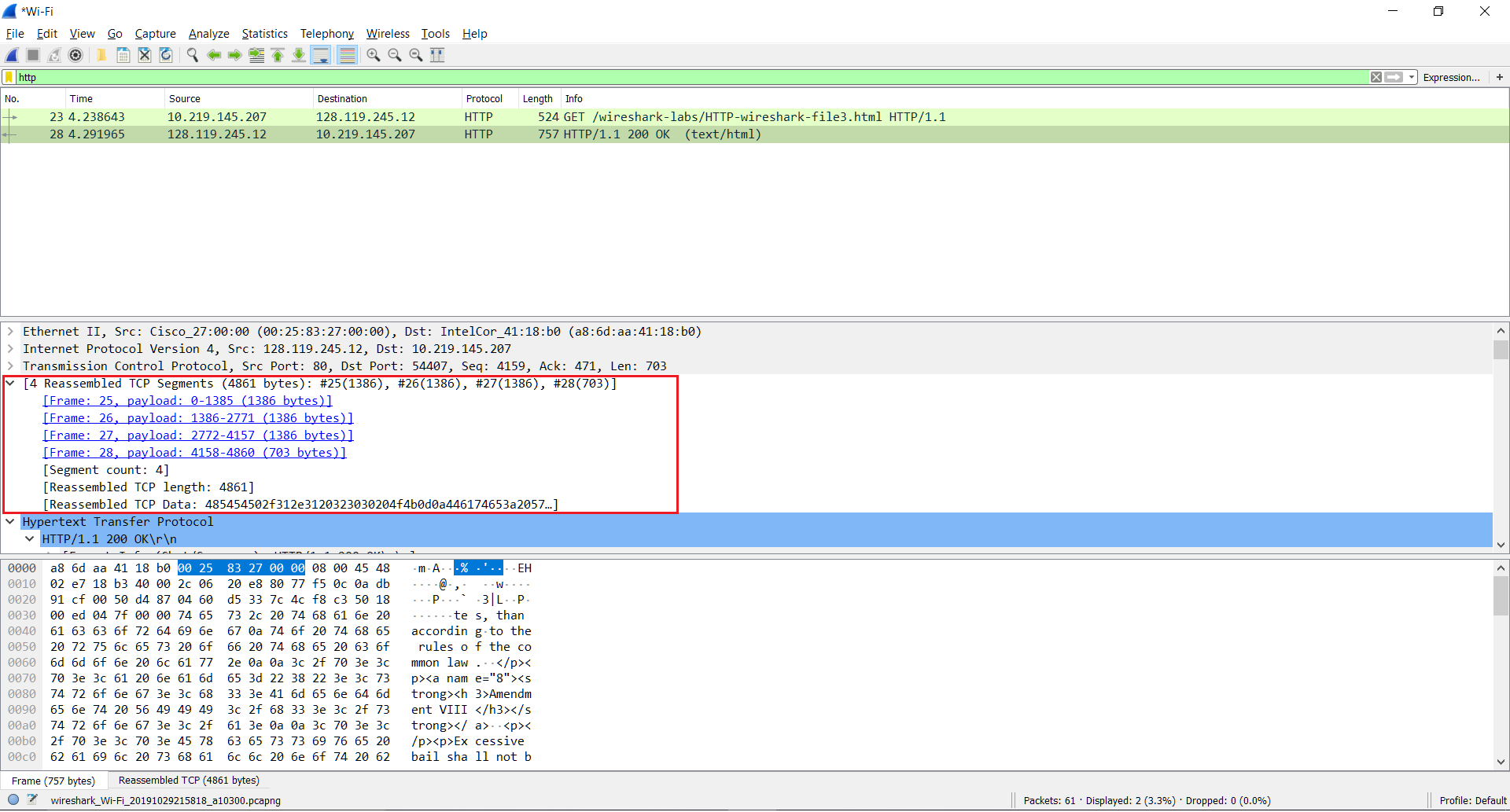
Ans. Status Code – 200

Response Phrase - 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. 4 data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights.

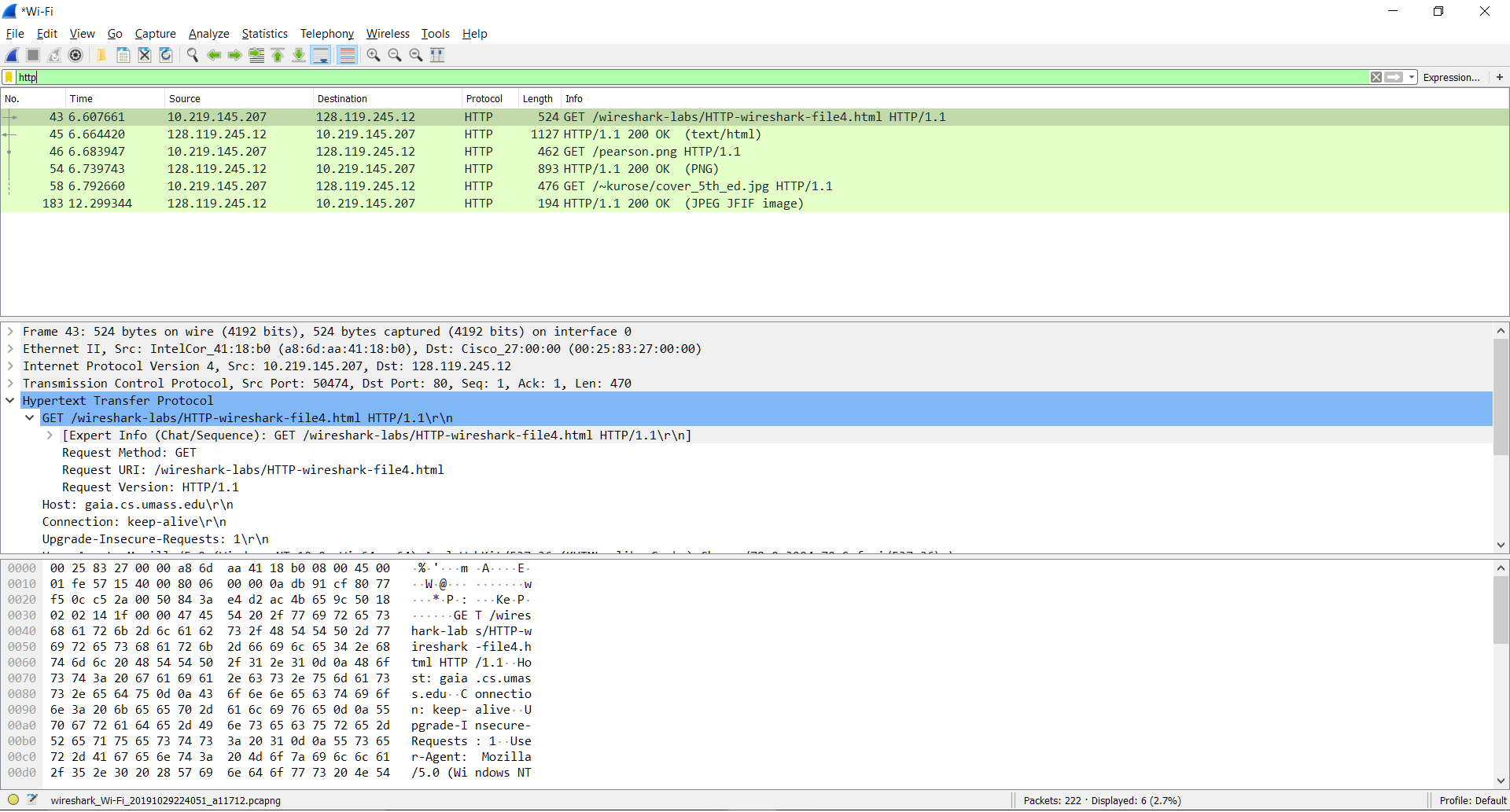


4. HTML Documents with Embedded Objects

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

Ans. The browser sent 3 HTTP GET request messages

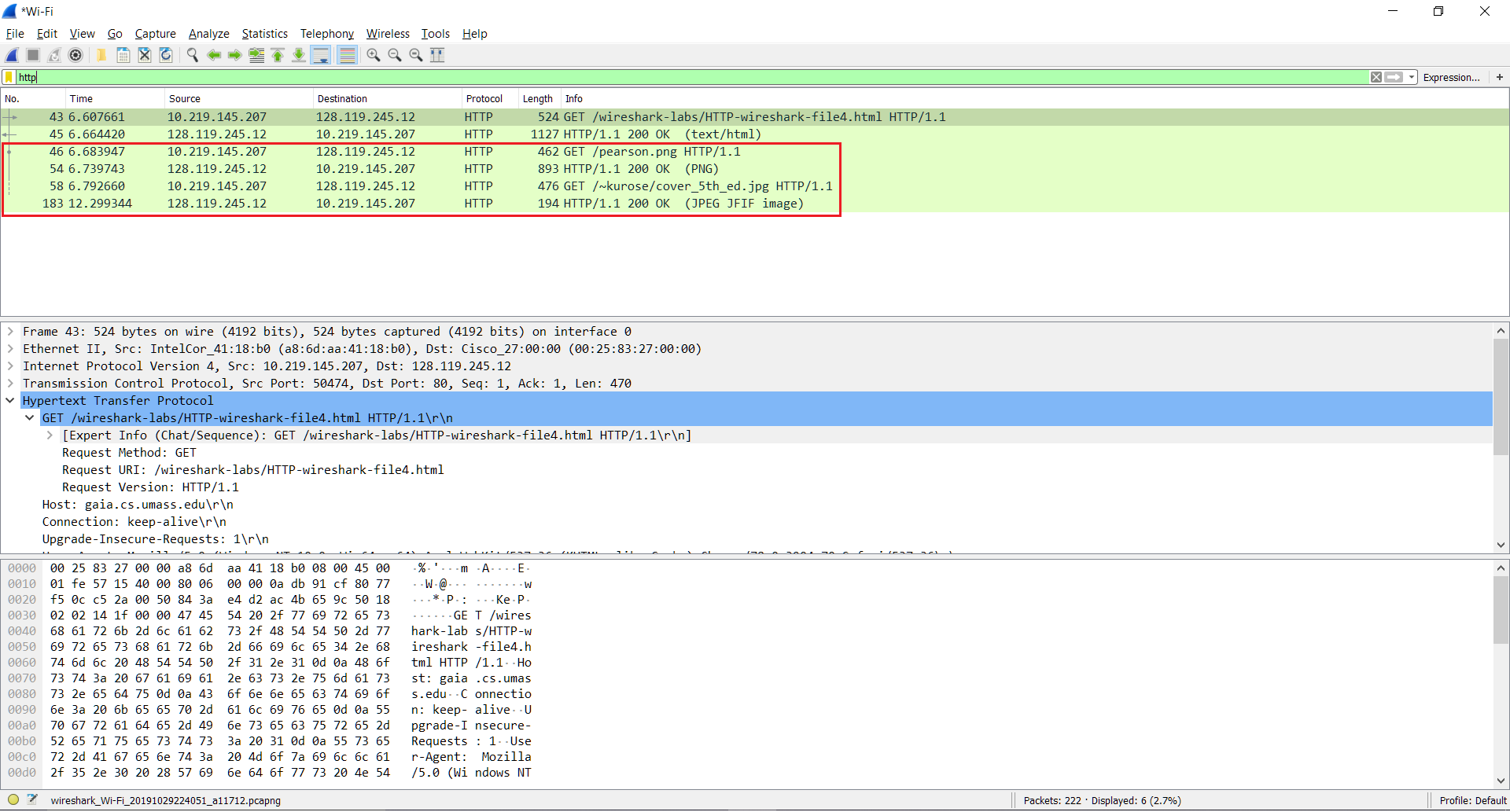
The Internet address to which these GET requests were sent is 128.119.245.12



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. The browser downloaded the two images ‘serially’ from the web.

By looking at this packet content window we can say that the contents were downloaded the following order : First the text message, then the pearson.png image and at last ~kurose/cover\_5th\_ed.jpg image.

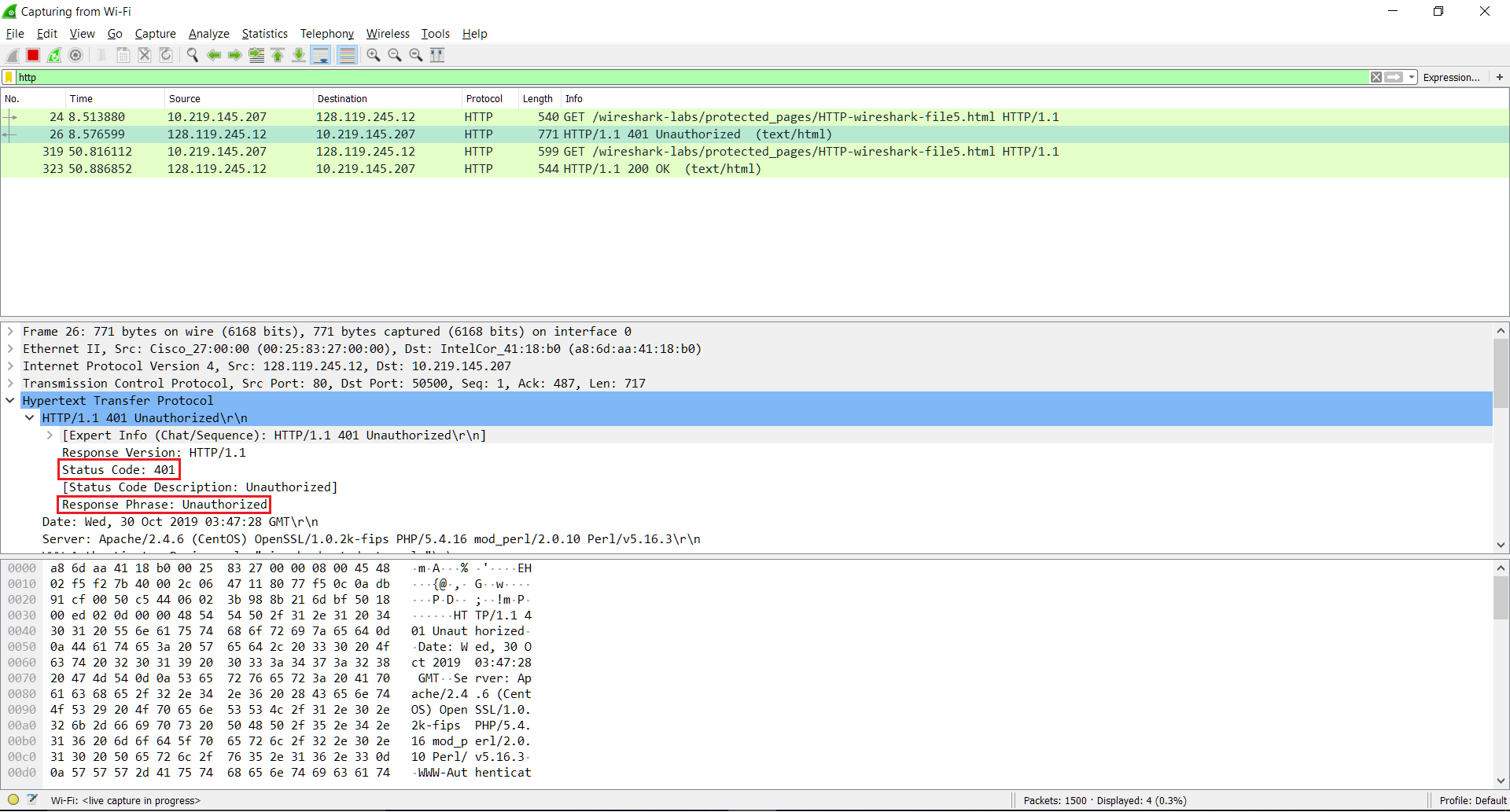


5 HTTP Authentication

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

Ans. Status Code – 401

Phrase – 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. When the browser’s sends the HTTP GET message for the second time, the new field that is included in the HTTP GET message is the ‘Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=’ which contains the Credentials when you expand it.

