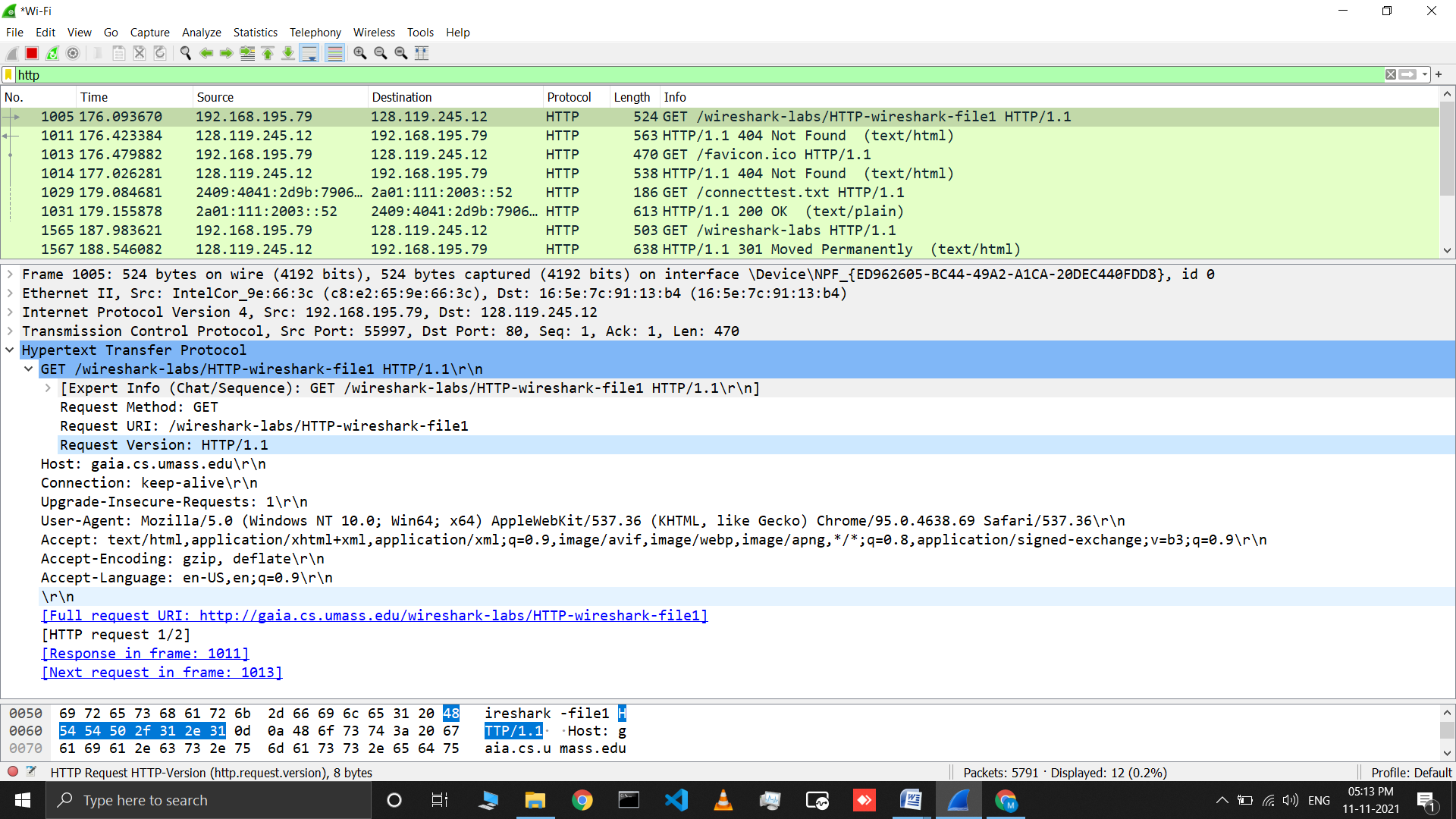
**PRACTICAL-10**

**Aim: HTTP packets -** Understand basic networking concept using Wire shark and capture HTTP Protocol Traffic

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

## Answer: Both of them are version 1.1 (HTTP version information is listed in the item ‘Request Version’)

****

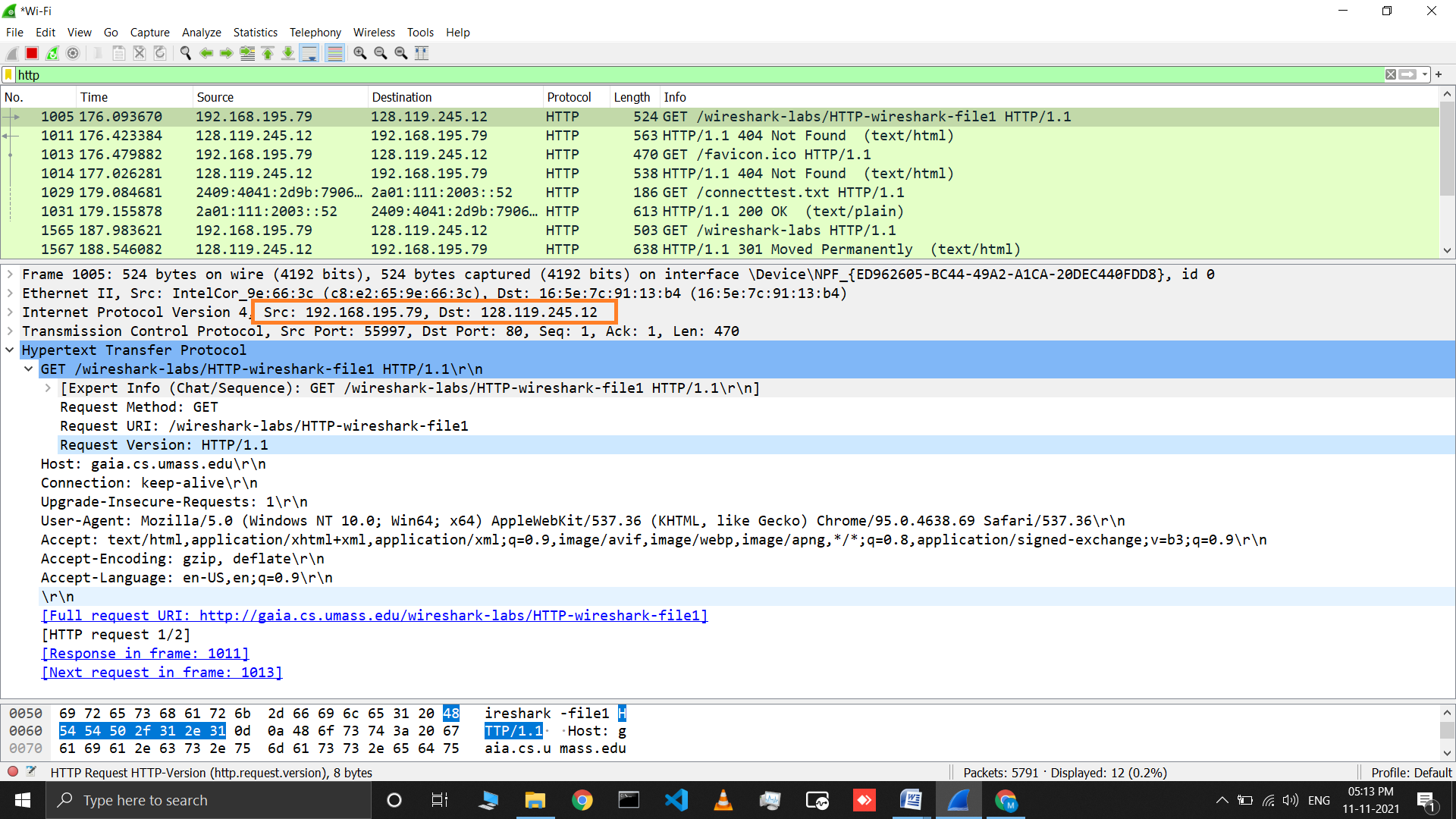
1. What languages (if any) does your browser indicate that it can accept tothe server?

## Answer: en-US (US English) (languages information is listed in the item ‘Accept-Language’ in the HTTP GET message)

## 2.png

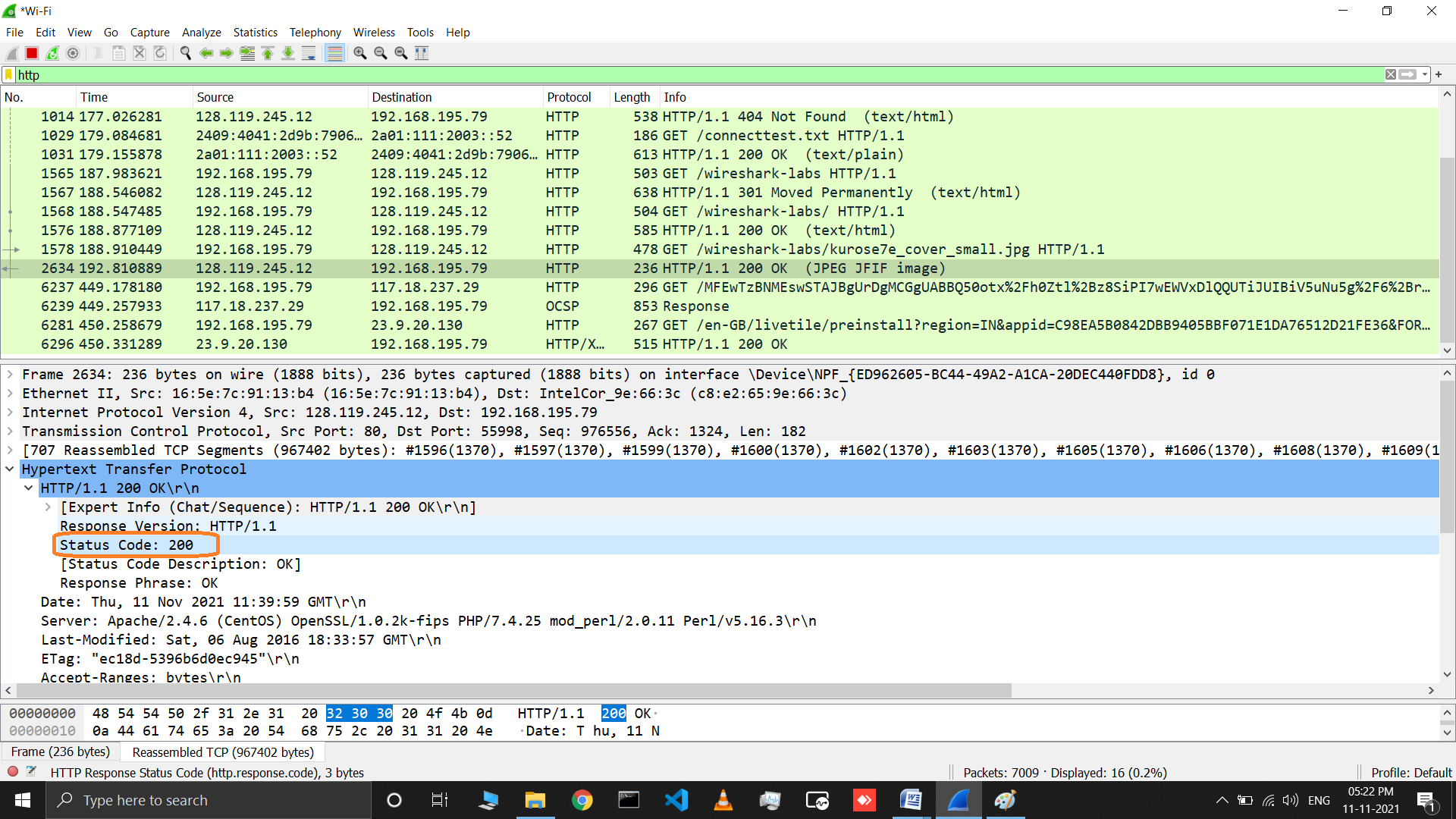
1. What is the IP address of your computer? Of the gaia.cs.umass.eduserver**?**

## Answer: my computer: 192.168.195.79 gaia.cs.umass.edu: 128.119.245.12

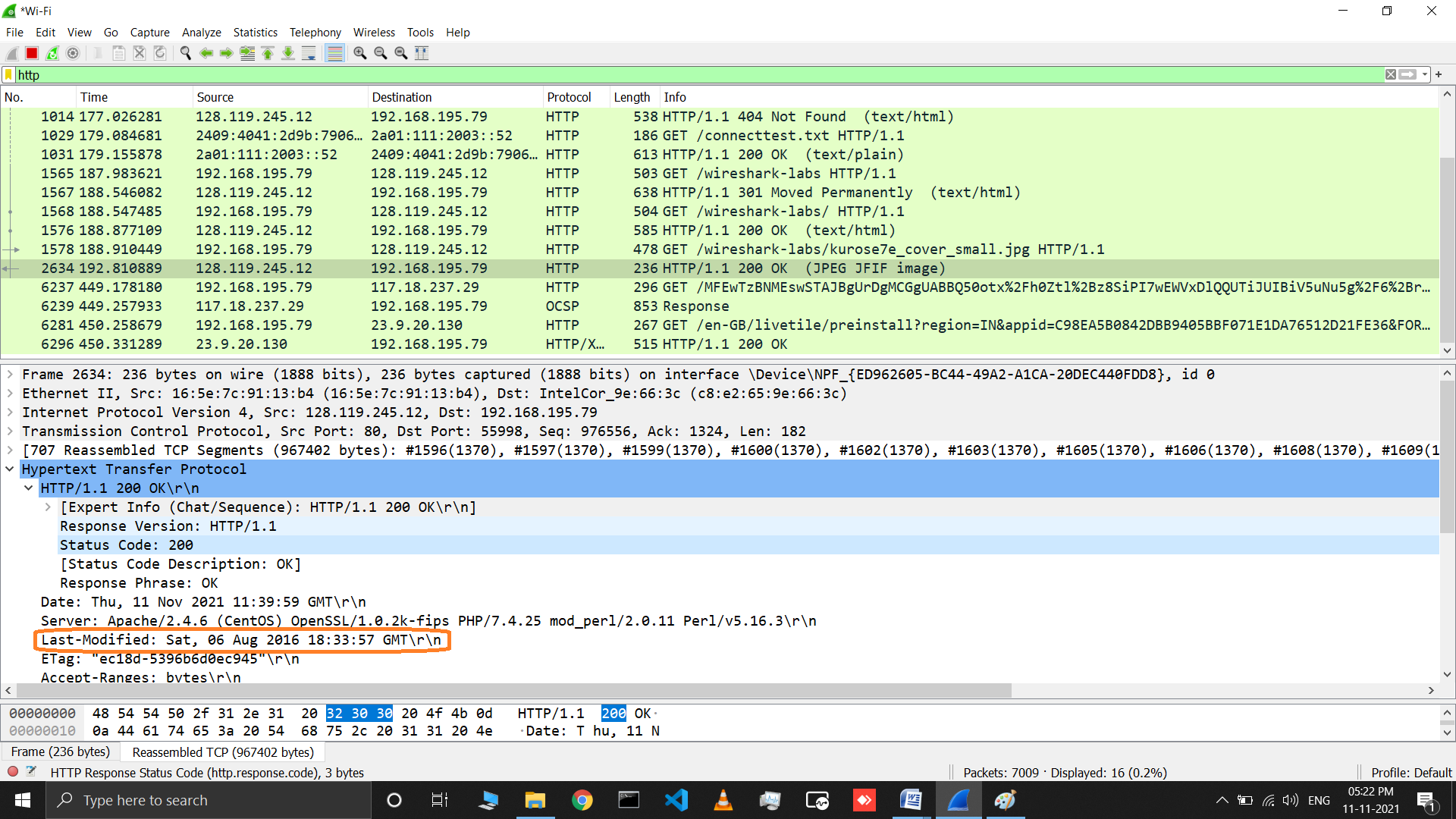
****

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

## Answer: status code:200 (status code information is listed in the HTTP OKmessage)

****

1. When was the HTML file that you are retrieving last modified at theserver? **Answer: Sat, 6 Aug 2016 (last modified information is listed in the item ‘Last- Modified’ in the HTTP OKmessage)**

****

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

## Answer: Solution: Content length: 967053 bytes(Content length information is listed in the item ‘Content-Length’ in the HTTP OK message)

## 6.png

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

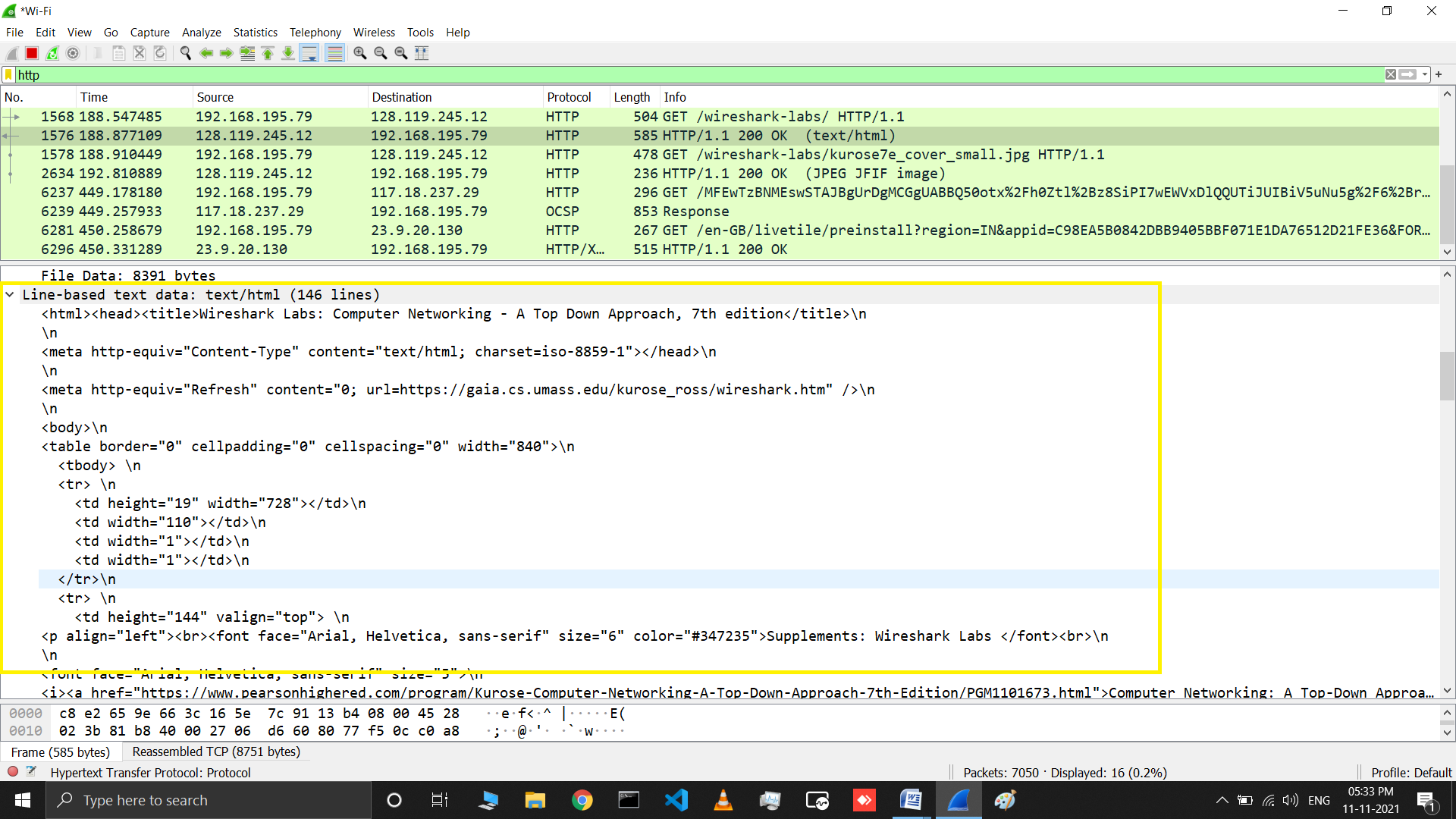
## Answer: I do not see any different headings between the two windows

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

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

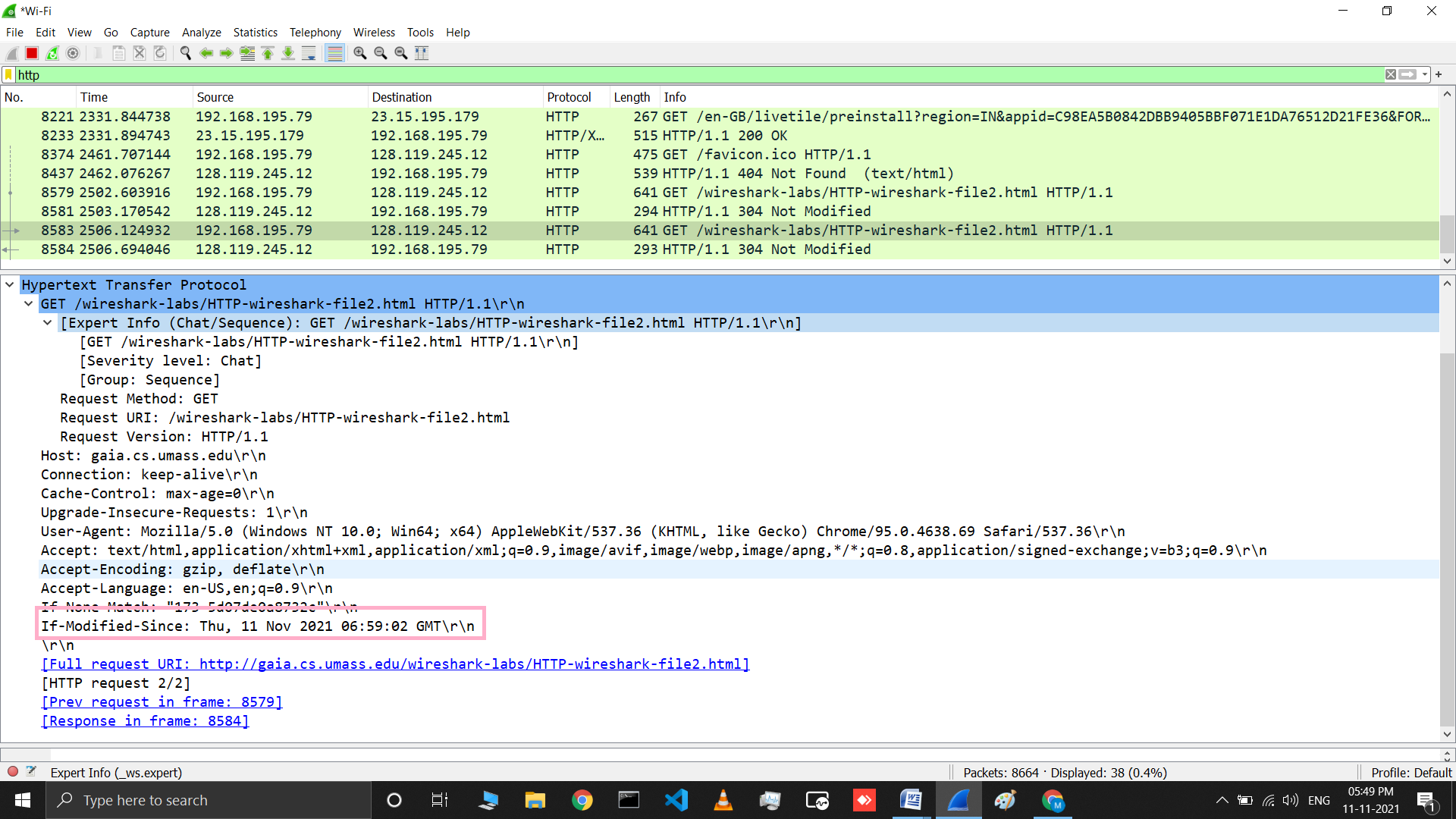
1. Inspect the contents of the server response. Did the server explicitly returnthe contents of the file? How can you tell?

## Answer: The server did explicitly return the contents of the file. 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.

****

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?

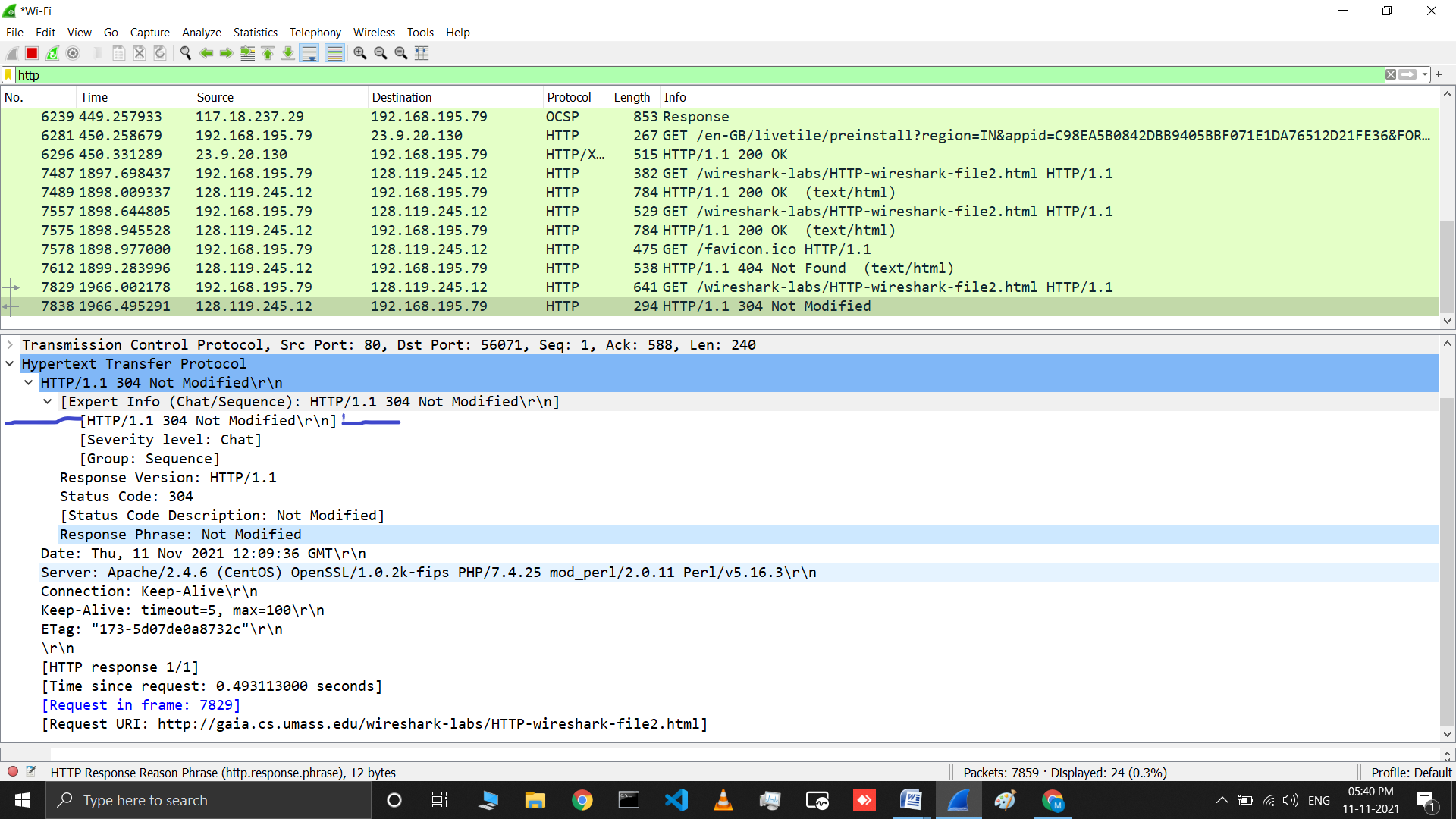
## Answer: Yes in the second HTTP message an IF-MODIFIED-SINCE line is included. The information that follows is the date and time that I last accessed the webpage

****

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.

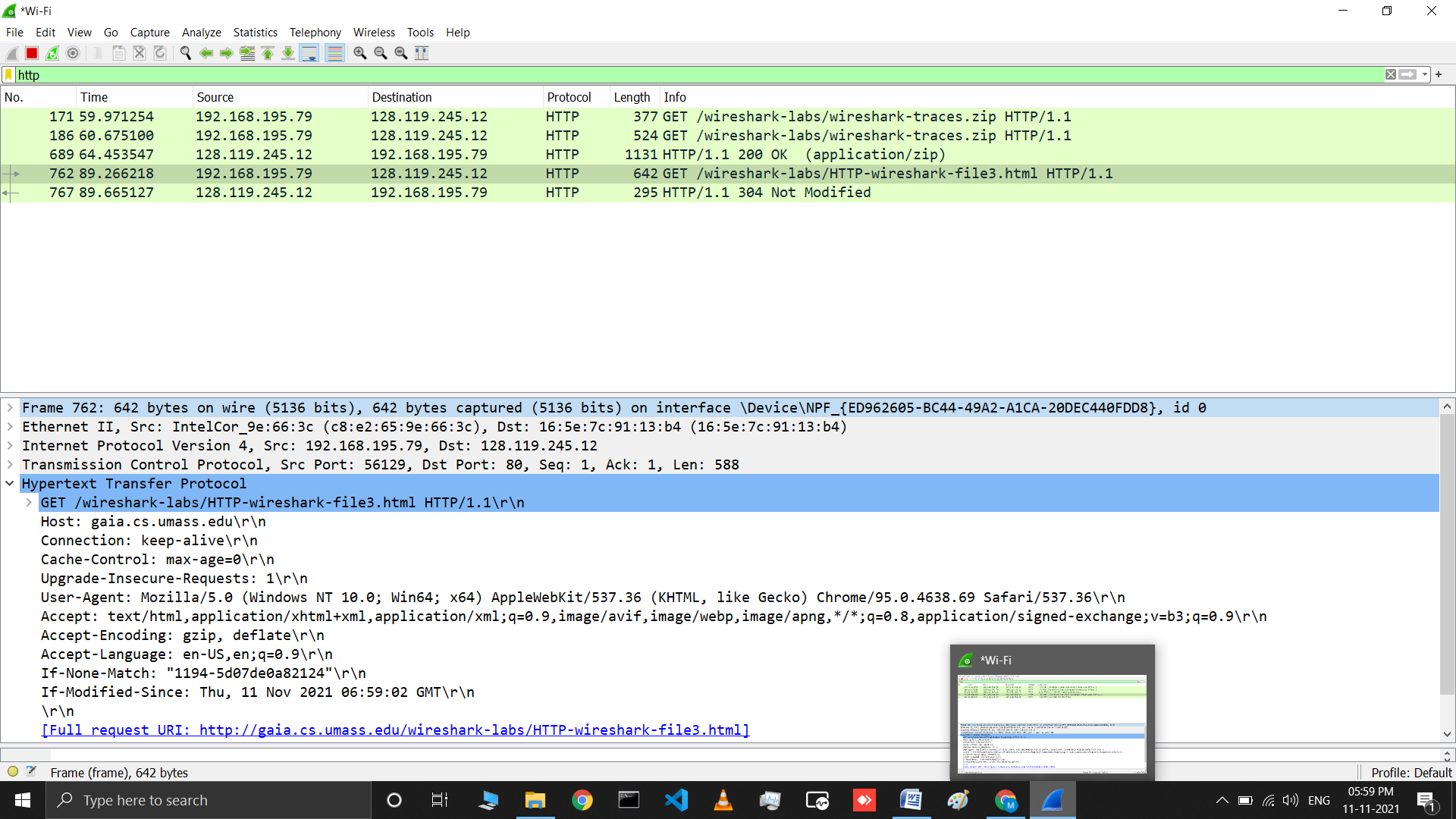
## Answer:

* **The HTTP status code is “304: NotModified”**
* **The server did not return the contents of the file because the browser simply retrieved the contents from its cache. Had the file been modified since it was last accessed, it would have returned the contents of the file, instead itsimply told my browser to retrieve the old file from its cachedmemory.**

****

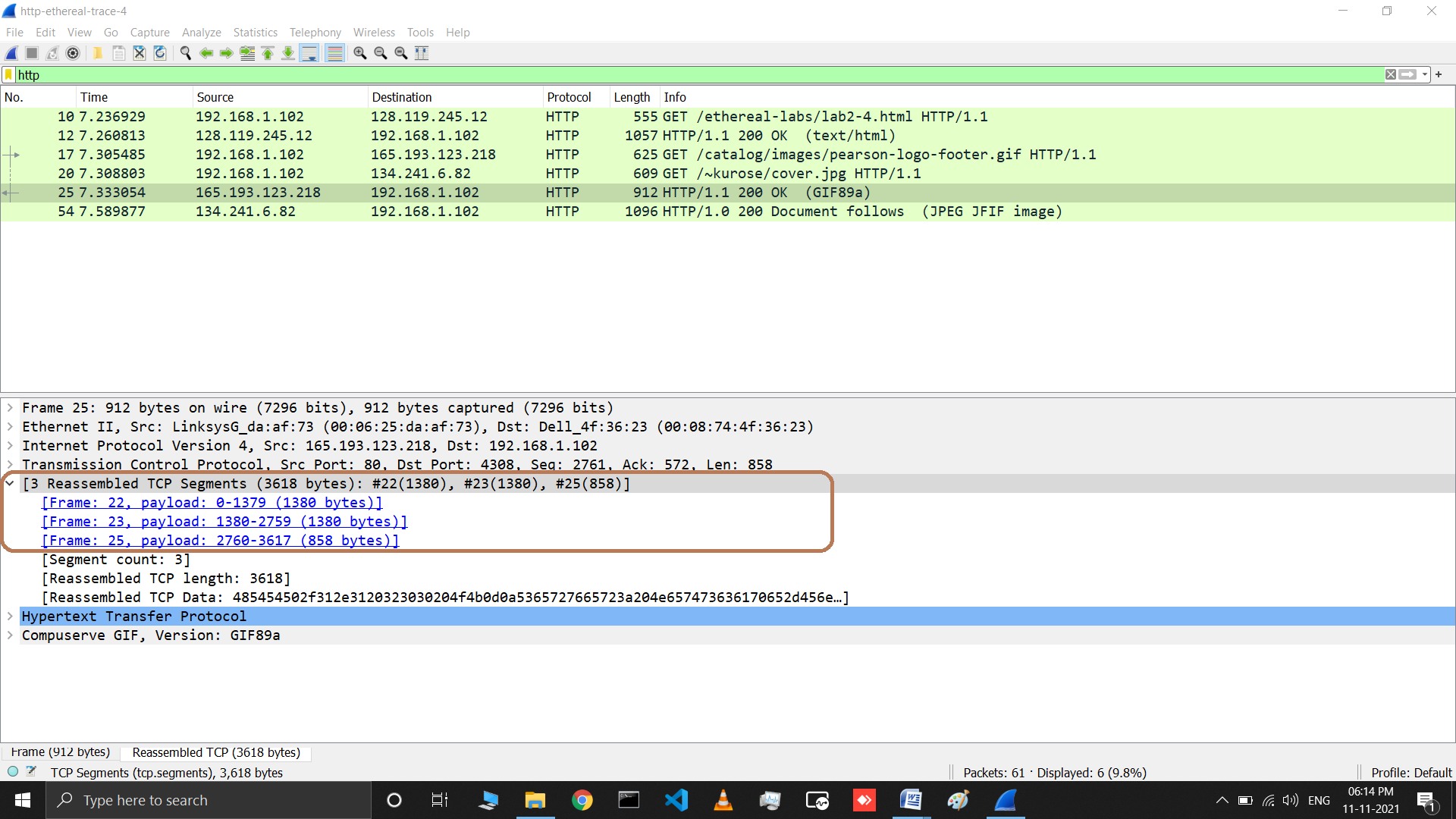
1. How many HTTP GET request messages did your browser send? Whichpacket number in the trace contains the GET message for the Bill orRights?

## Answer: My browser sent 1 HTTP GET request was sent by my browser and the packet 8 in the trace contains the GET message for the Bill of Rights.

****

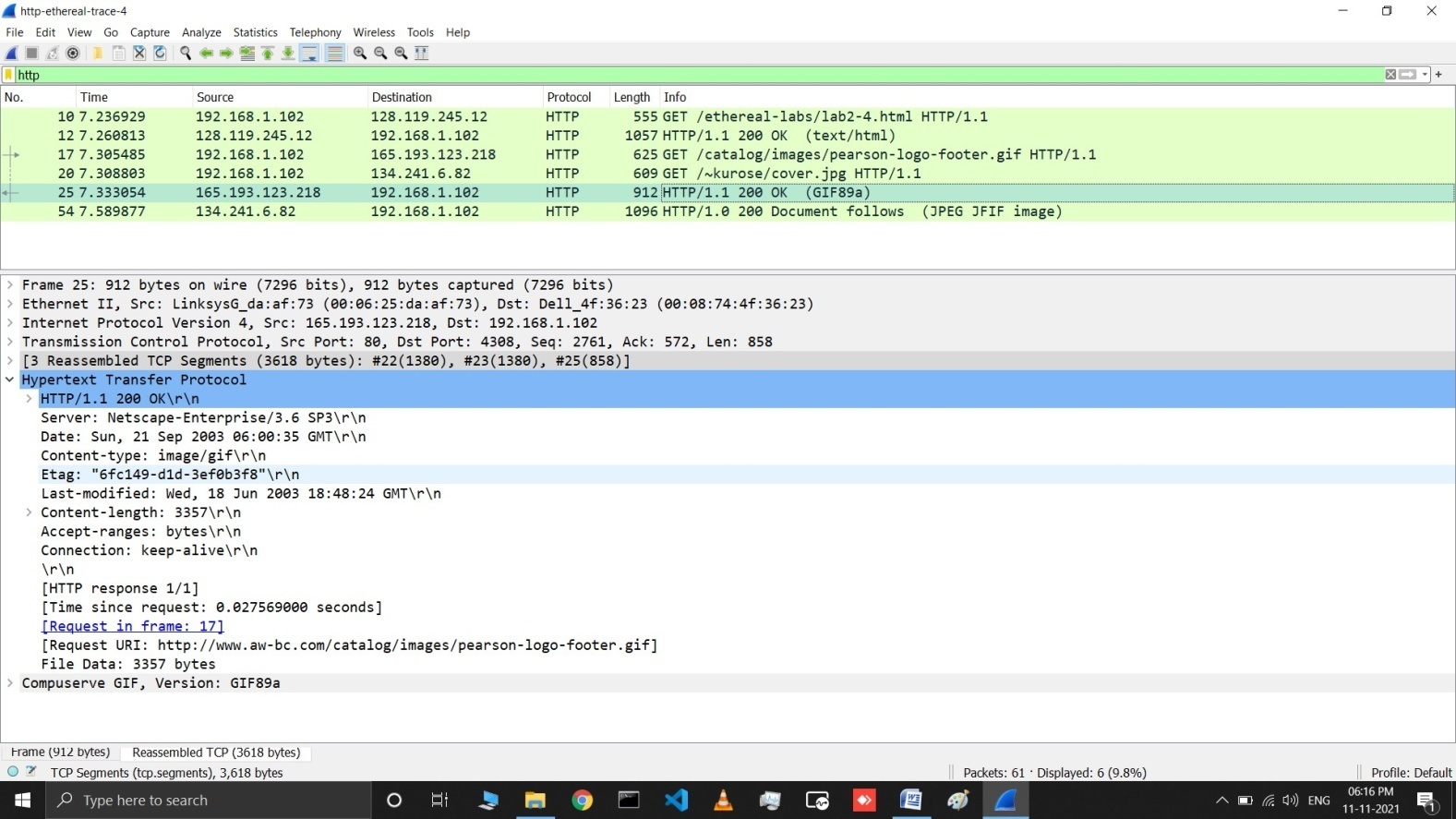
1. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GETrequest?

## Answer: The first response packet (PDU) from the server, packet 10 contains the status code and phrase.

****

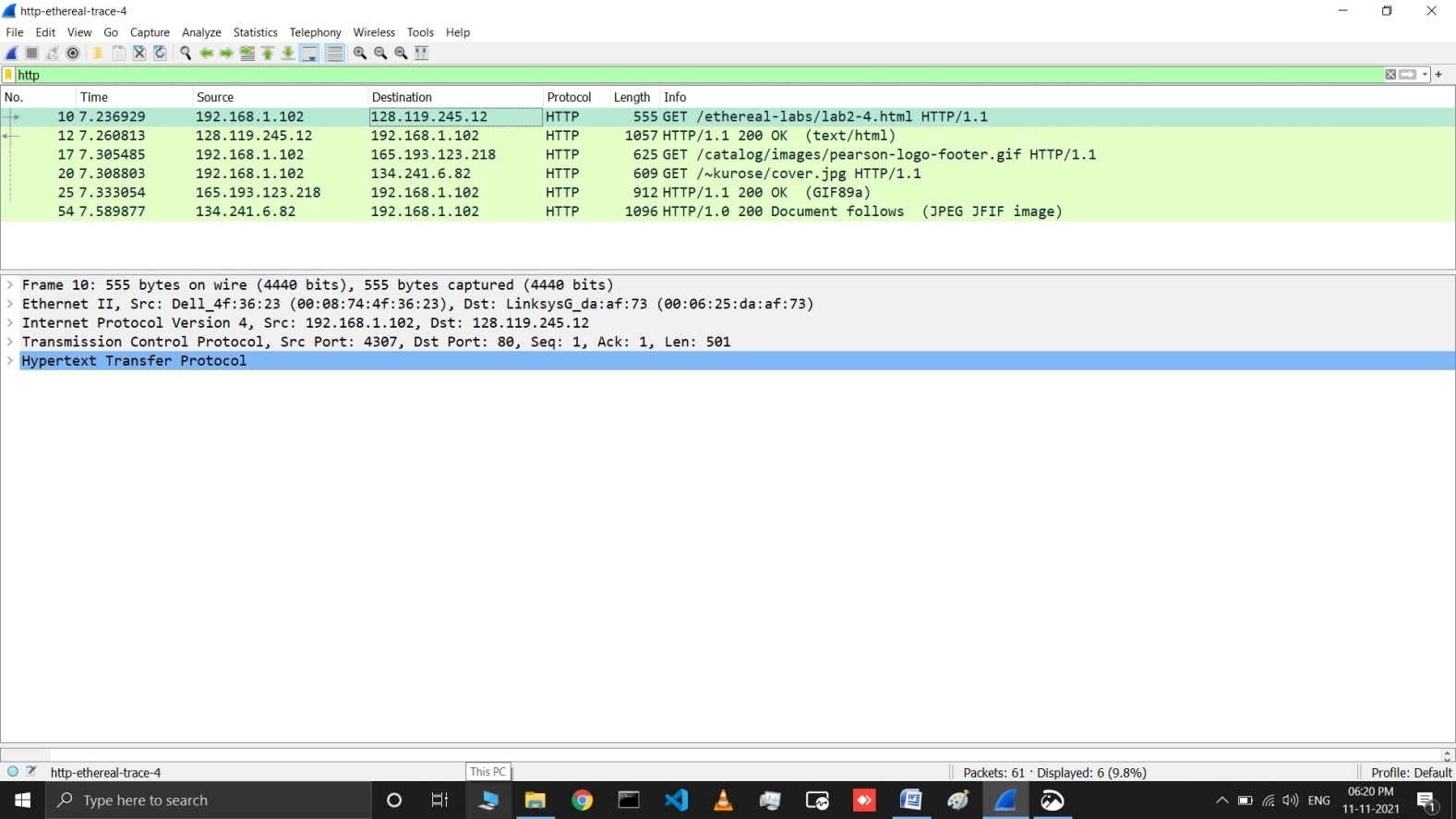
1. What is the status code and phrase in there sponse ?

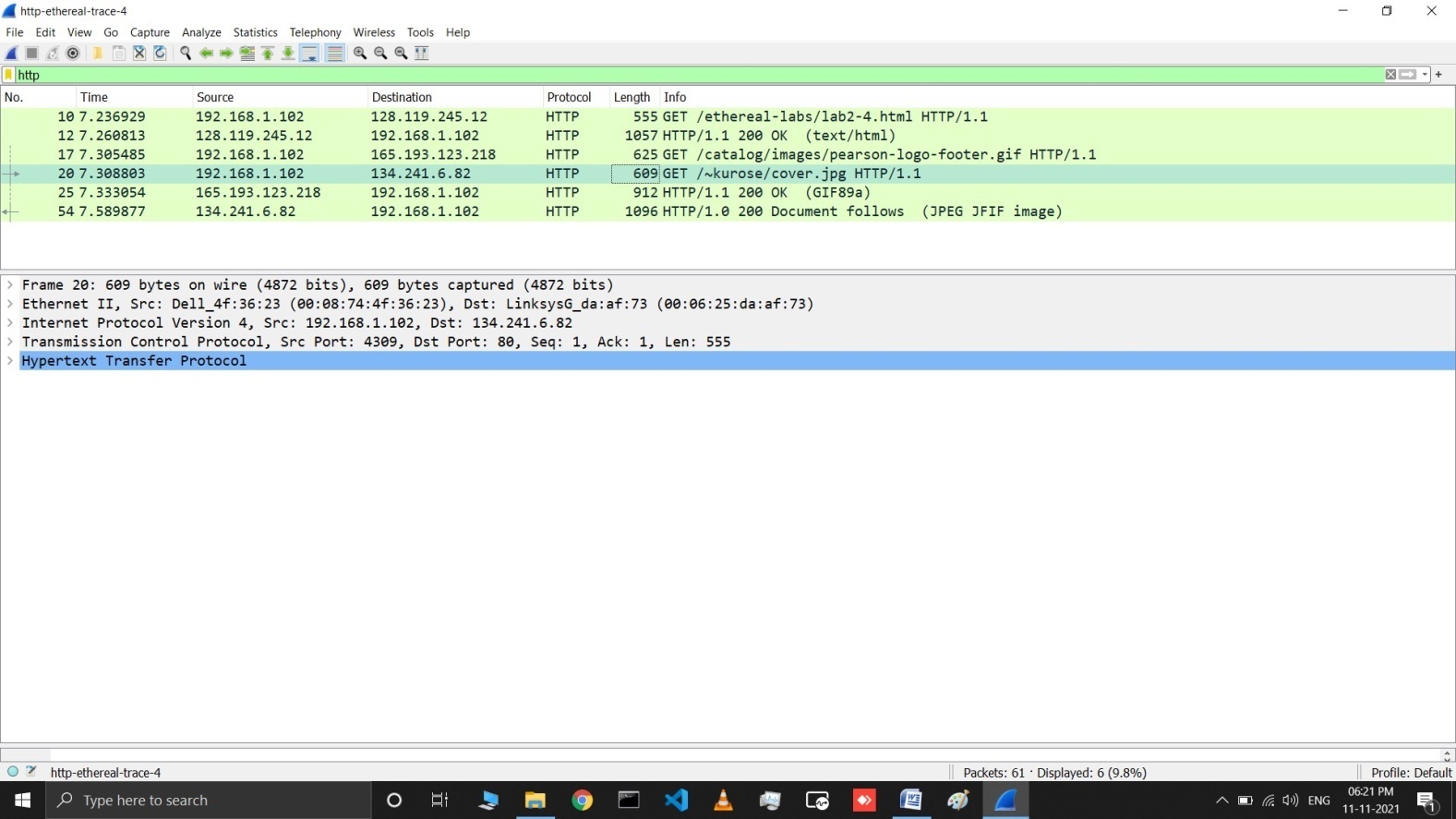
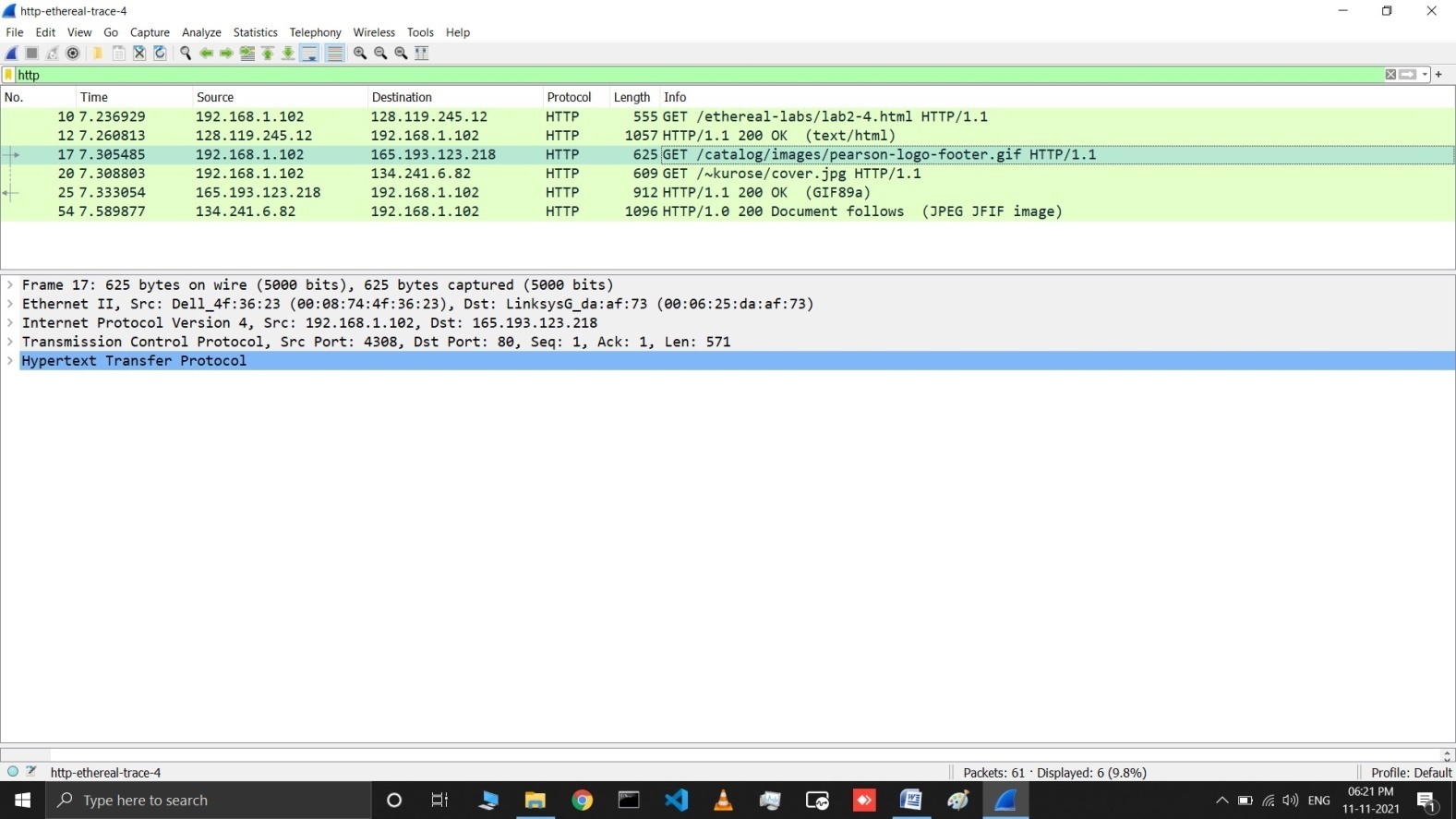
## Answer: Answer: The status code from this packet was a 200, and the phrase was an OK.

****

1. How many data-containing TCP segments were needed to carry the singleHTTP response and the text of the Bill ofRights?

## Answer: There were 4 TCP segments (10, 17 and 20) were needed to carry the single HTTP response and the text of the Bill of Rights.

****

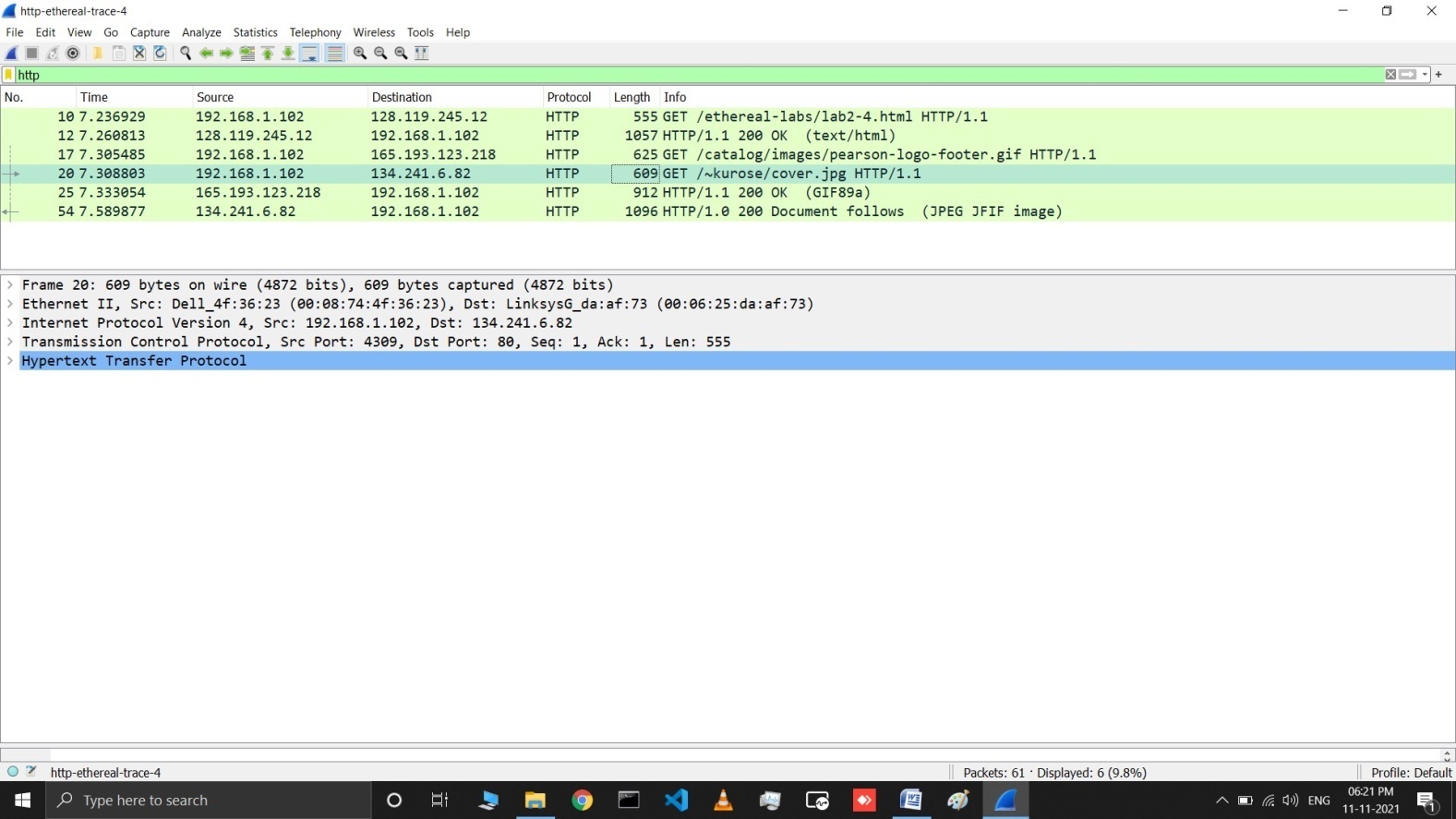
****

1. How many HTTP GET request messages did your browser send? Towhich Internet addresses were these GET requestssent?

## Answer: My browser sent 3 http GET message requests. packet 10 Internet addresses:- 128.119.245.12

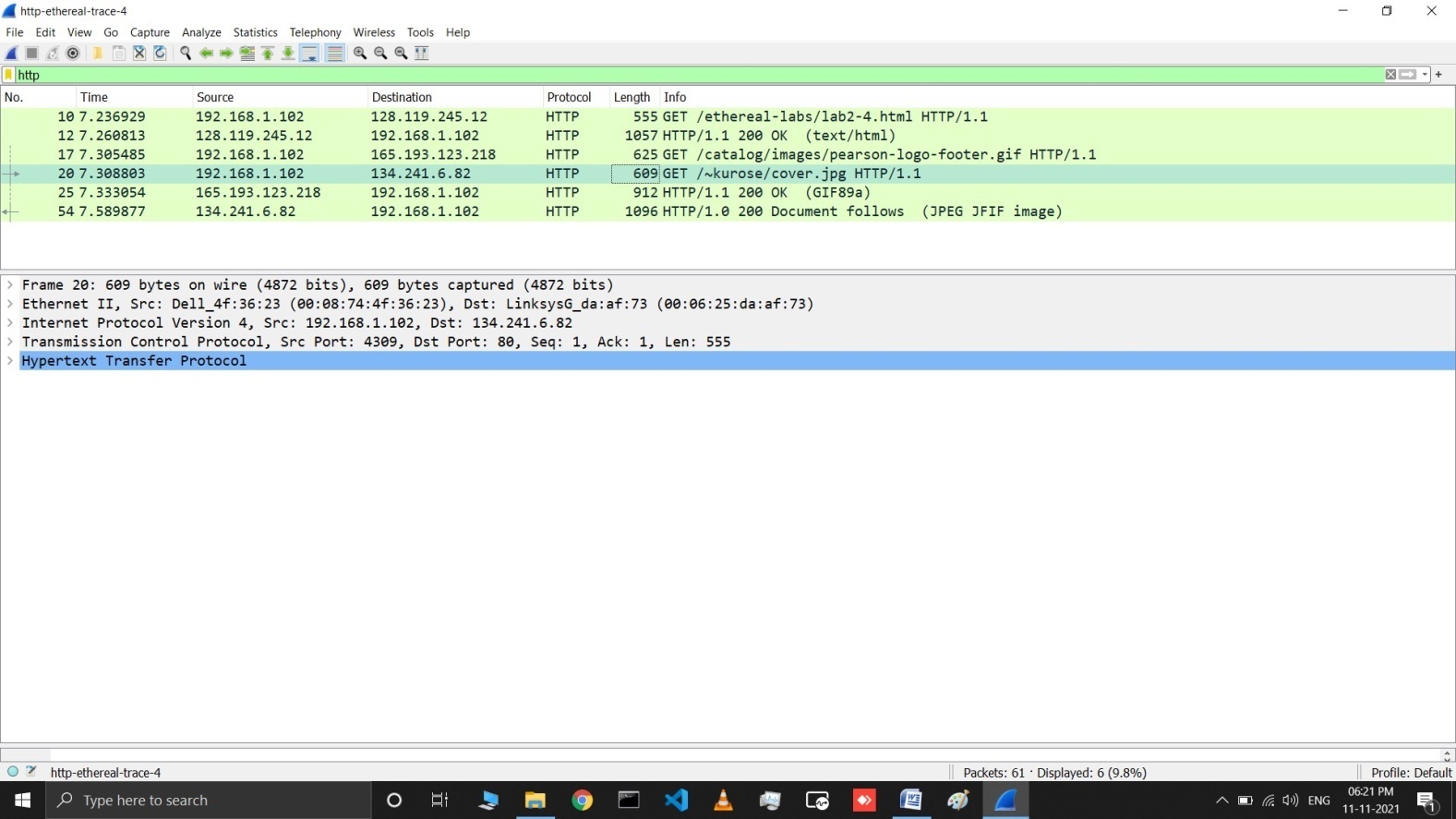
**packet 17 Internet addresses:- 165.193.123.218**

**packet 20 Internet addresses:- 134.241.6.82**

****

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

## Answer: They should have been downloaded parallel. This is because of the way the packets 20 and 25 functioned where the request for packet 20 was made before the request for 25.

****

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

## Answer: This deals with packets 6 and 9. 6 Has the Get and 9 has the Reply. The response is 401 authorization required.

## 16.png

1. When your browser’s sends the HTTP GET message for the second time,what new field is included in the HTTP GETmessage?

## Answer: The new field included is Authorization:Basic:field.