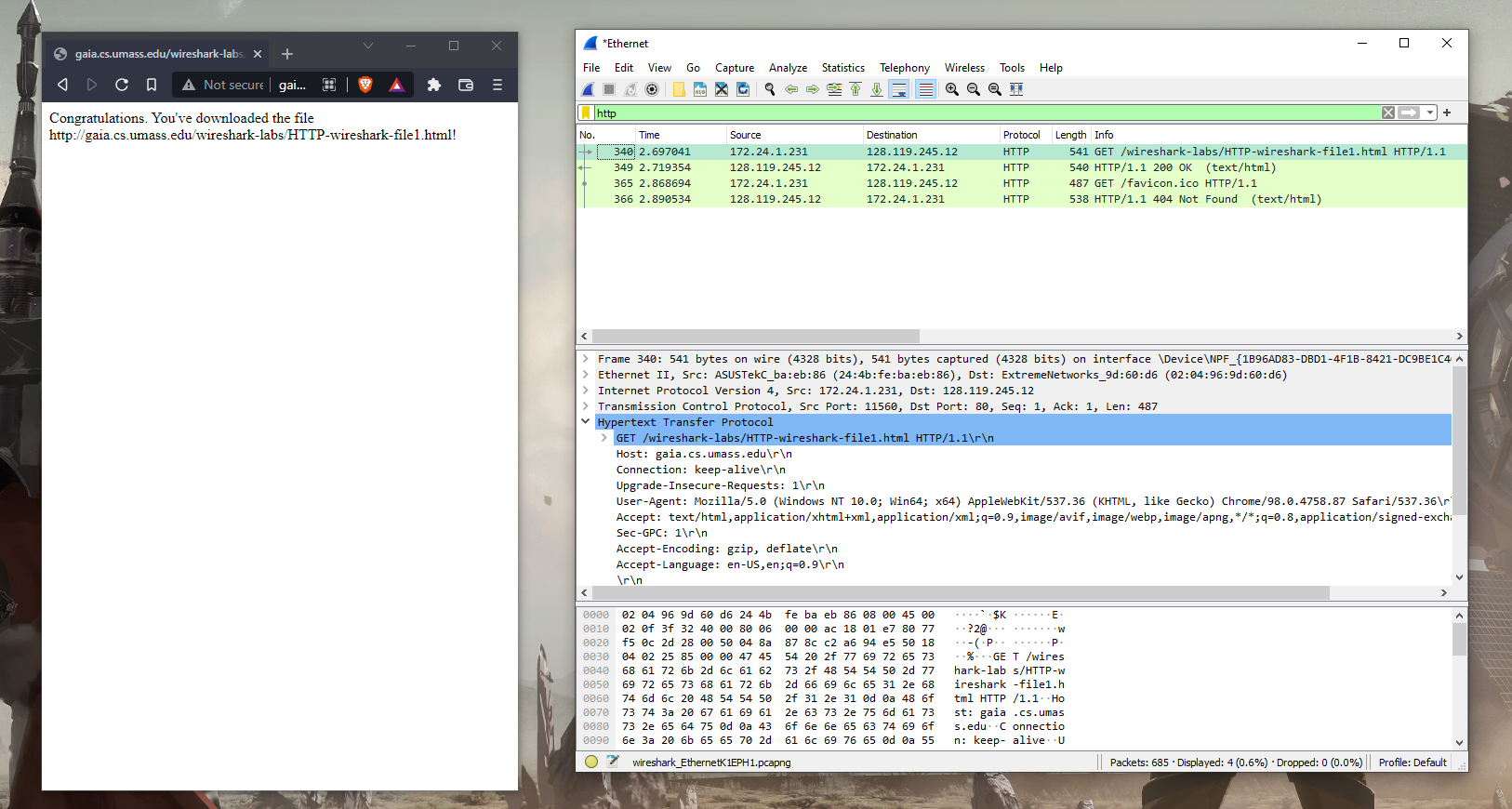
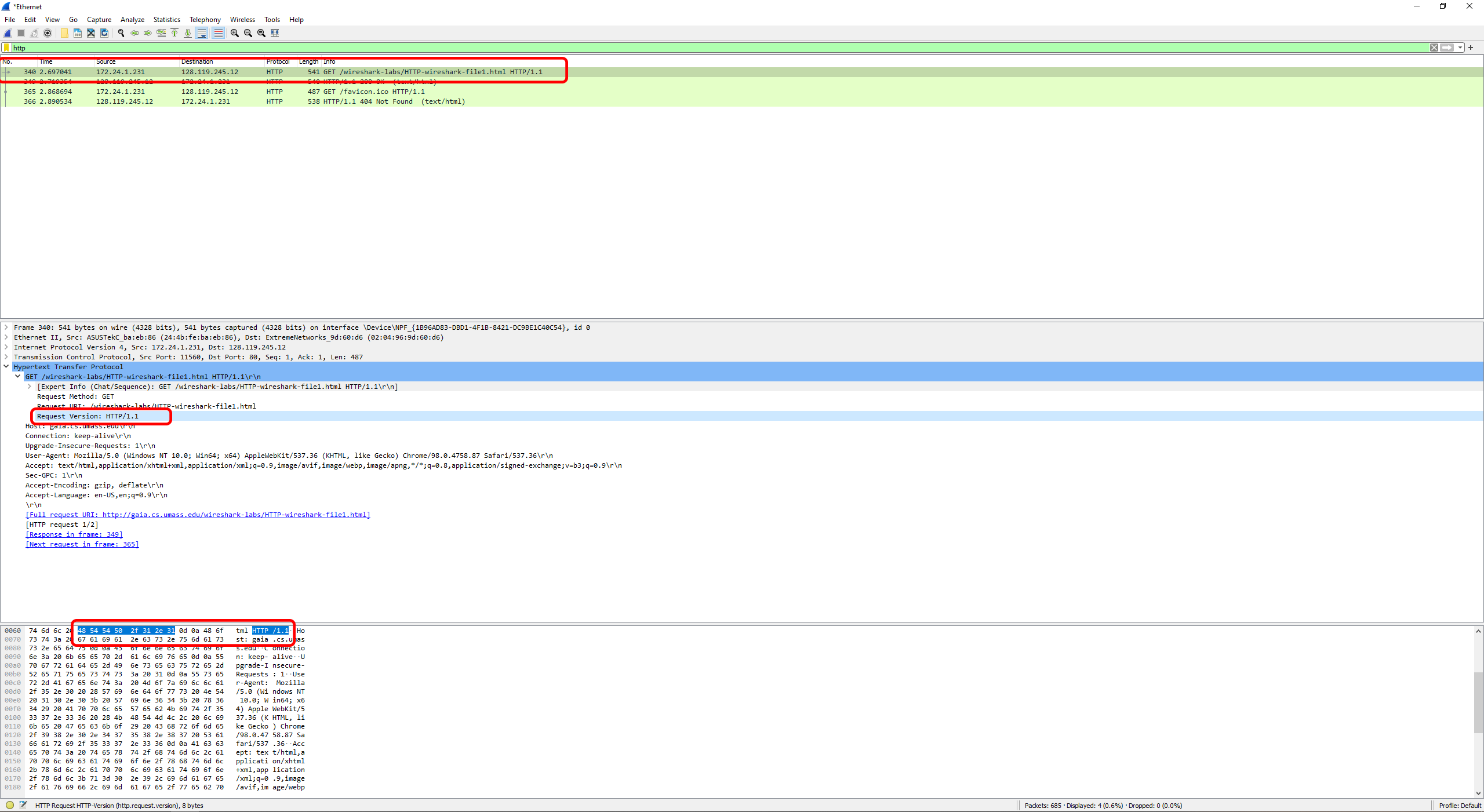
Part 1  
Steps 1-5:



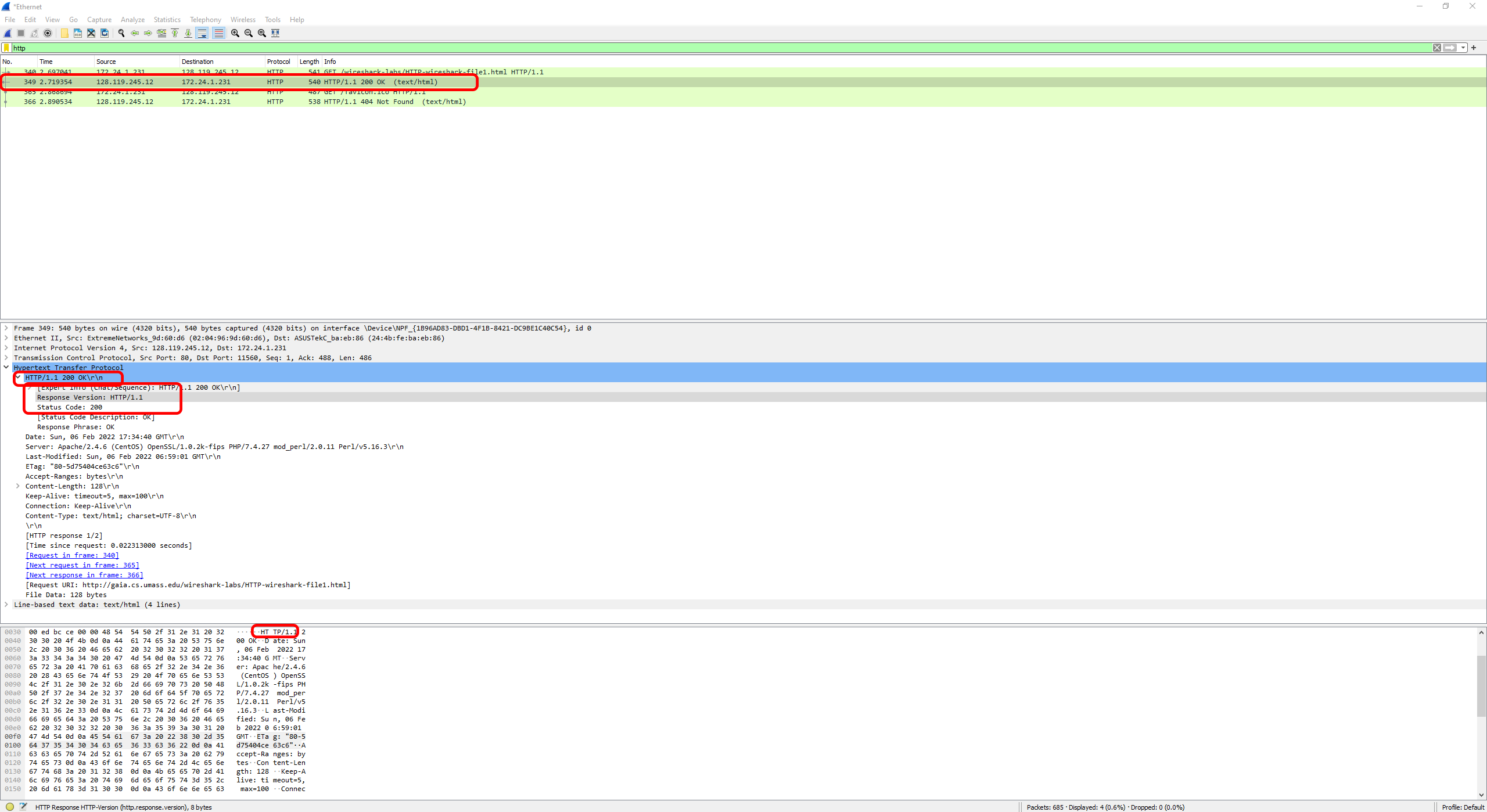
Questions 1-7:

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

Browser is running HTTP 1.1:



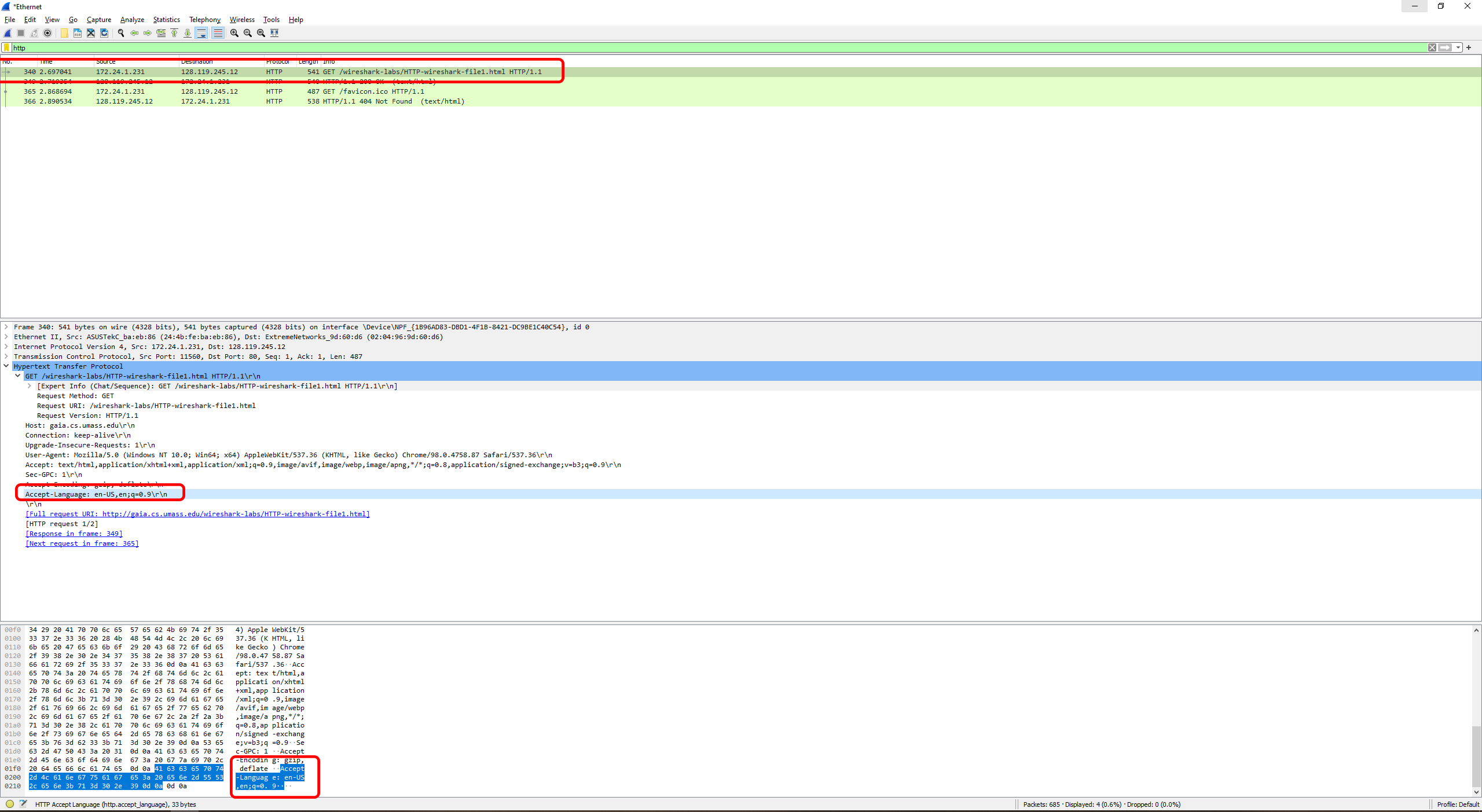
Server is running 1.1:



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

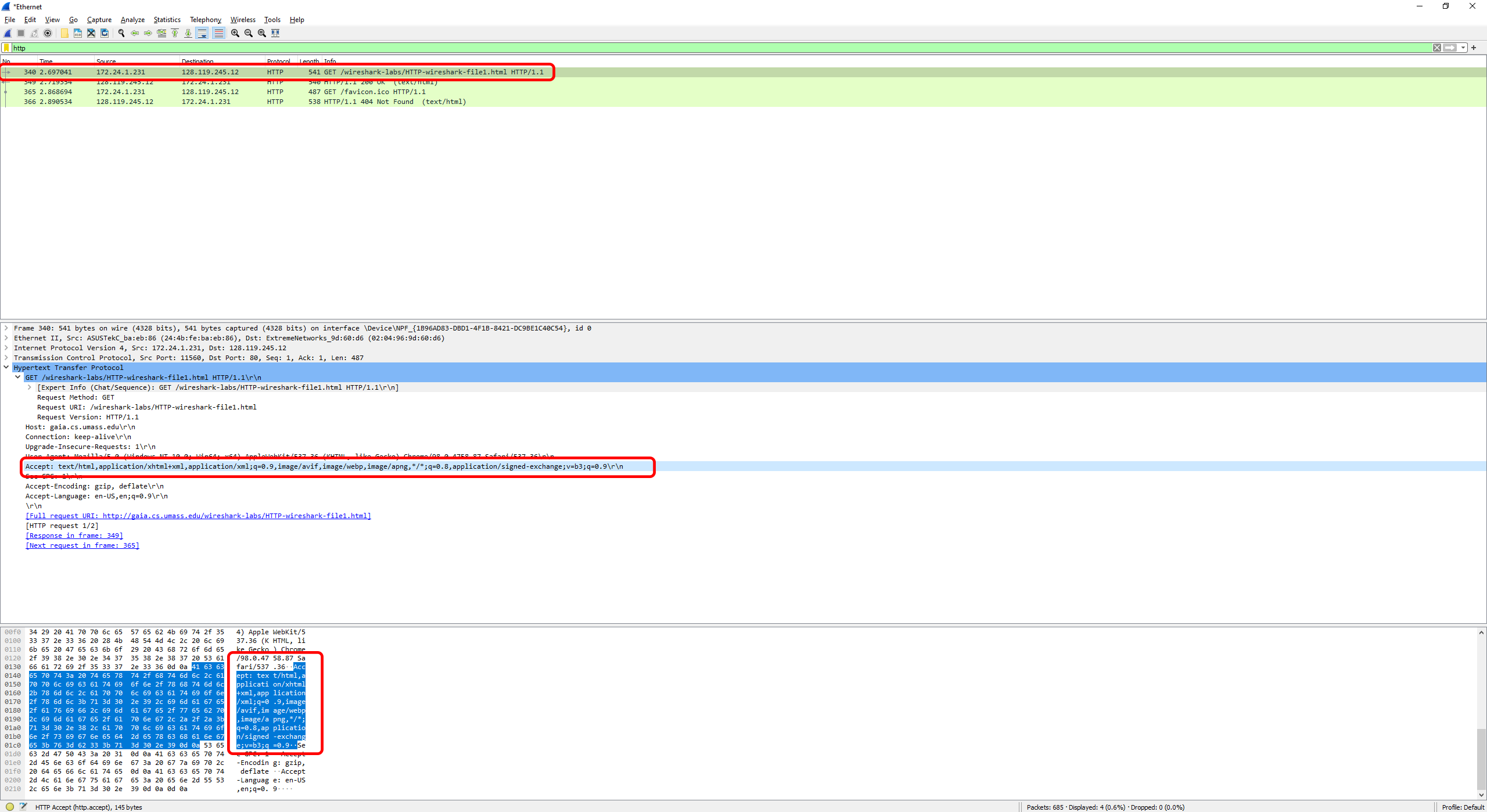
(Spoken languages accepted)

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



(Programming languages accepted)

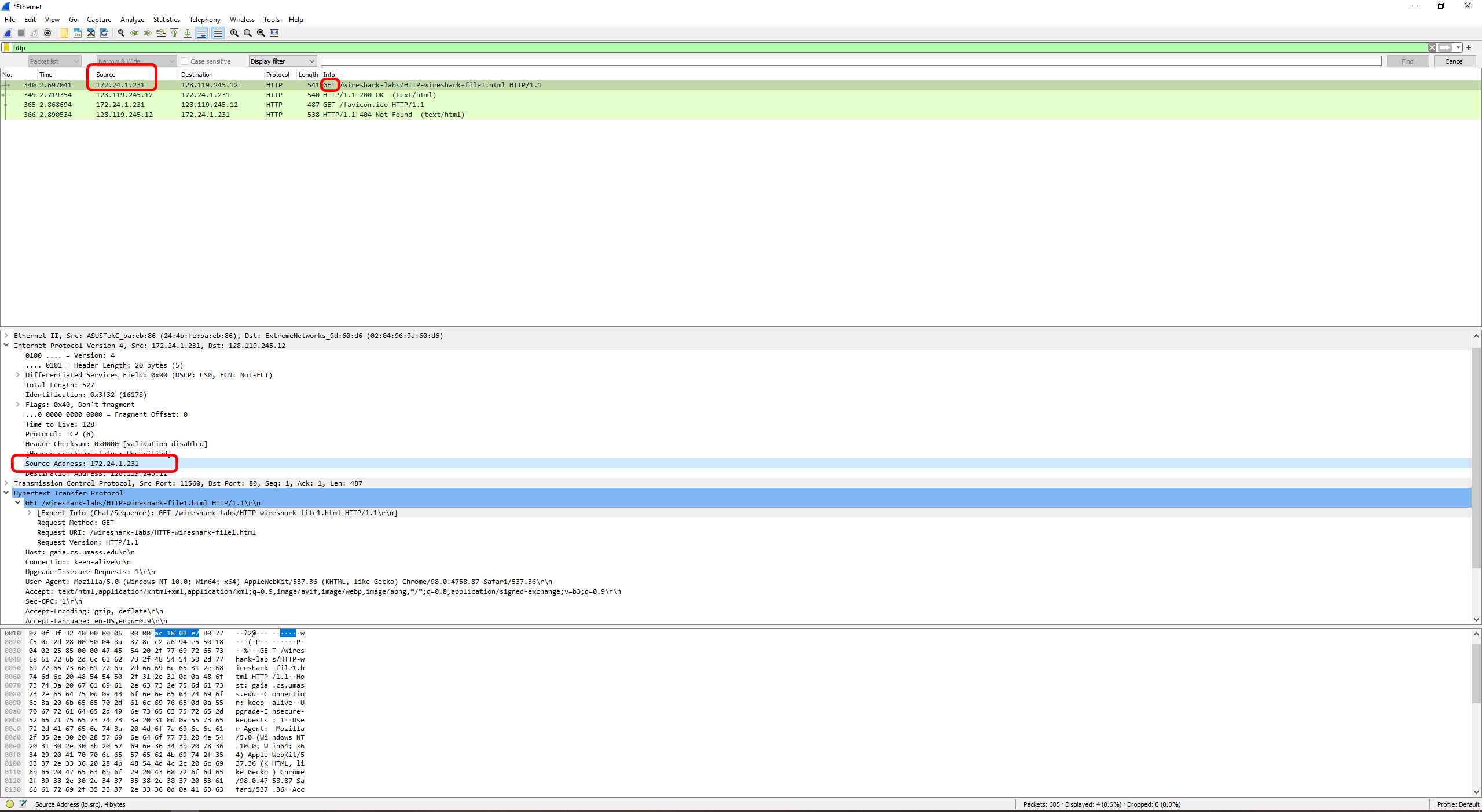
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9



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

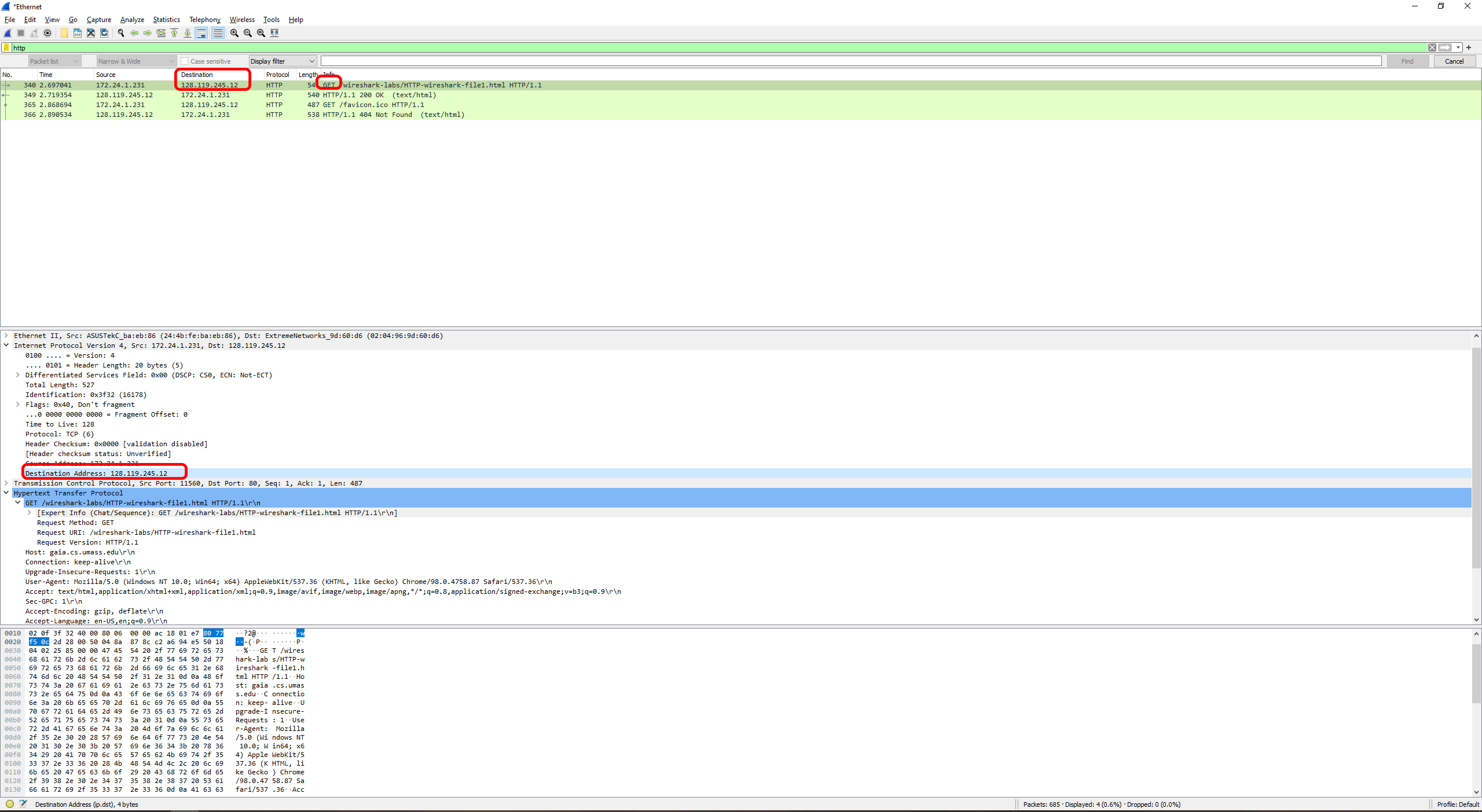
Computer:

172.24.1.231



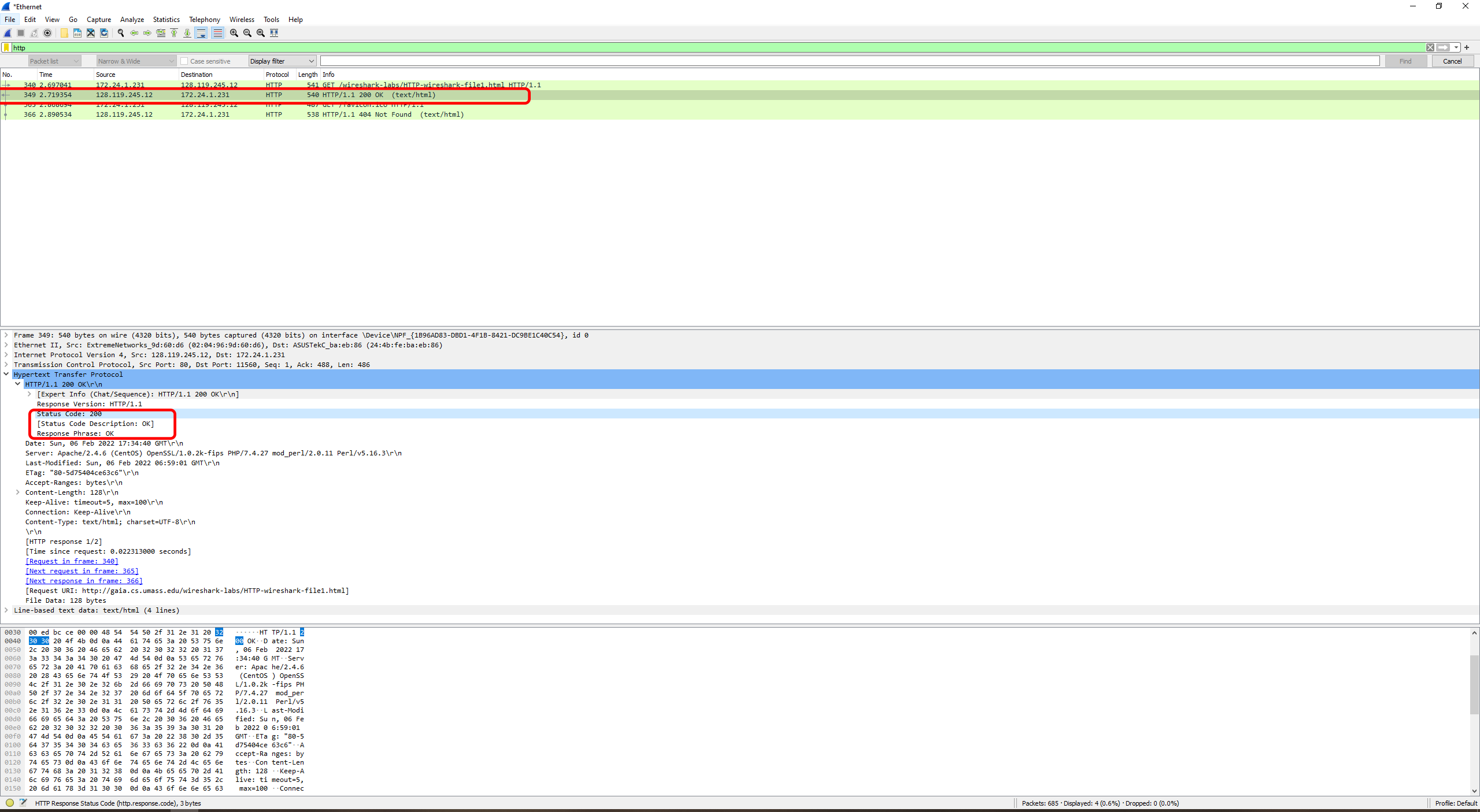
Server:

128.119.245.12



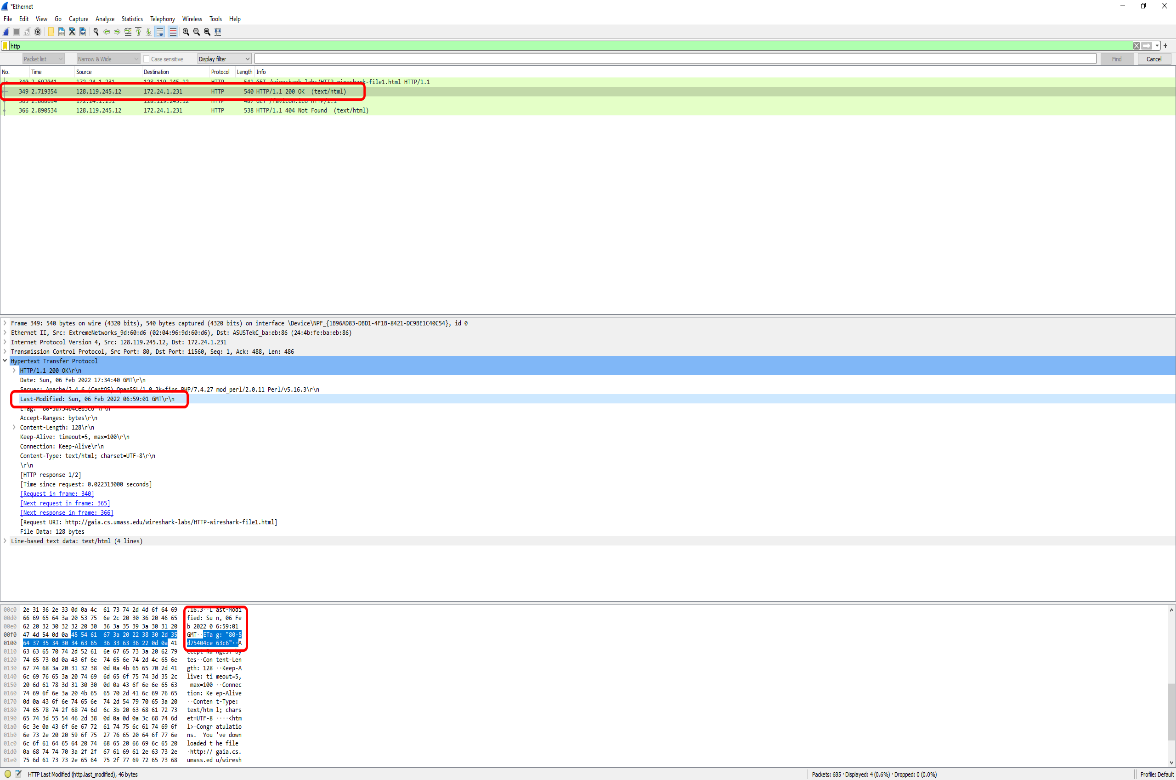
1. What is the status code returned from the server to your browser?

200



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

Last-Modified: Sun, 06 Feb 2022 06:59:01 GMT



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

128 bytes

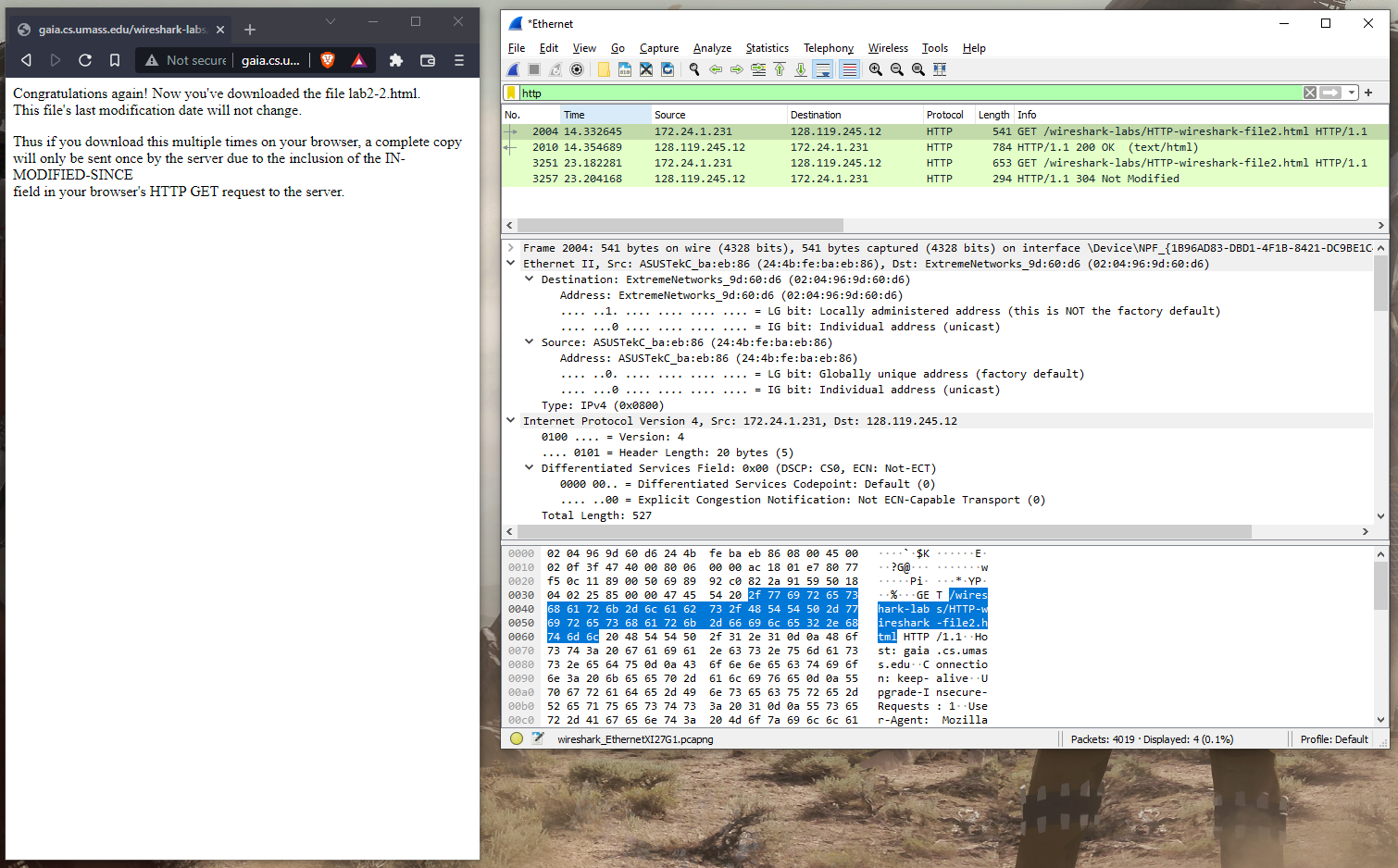


1. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

No, everything within the raw data in the packet content window is available within the packet-listing window.

<https://drive.google.com/file/d/1EYRzQ7xcOkOH101OyTwm21KMzidUZu4e/view?usp=sharing>

Part 2



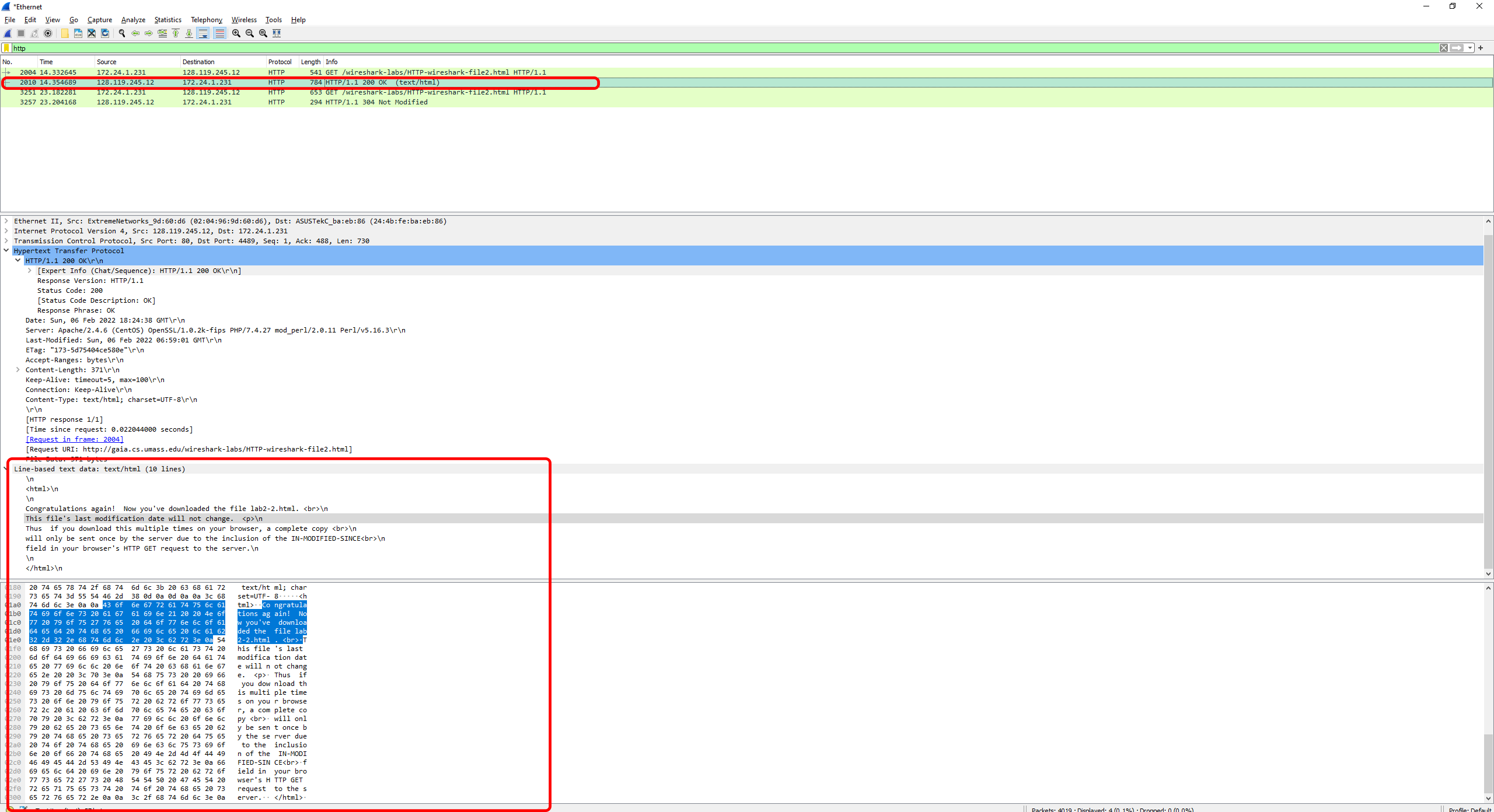
1. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

No, there is no “IF-MODIFIED-SINCE” line



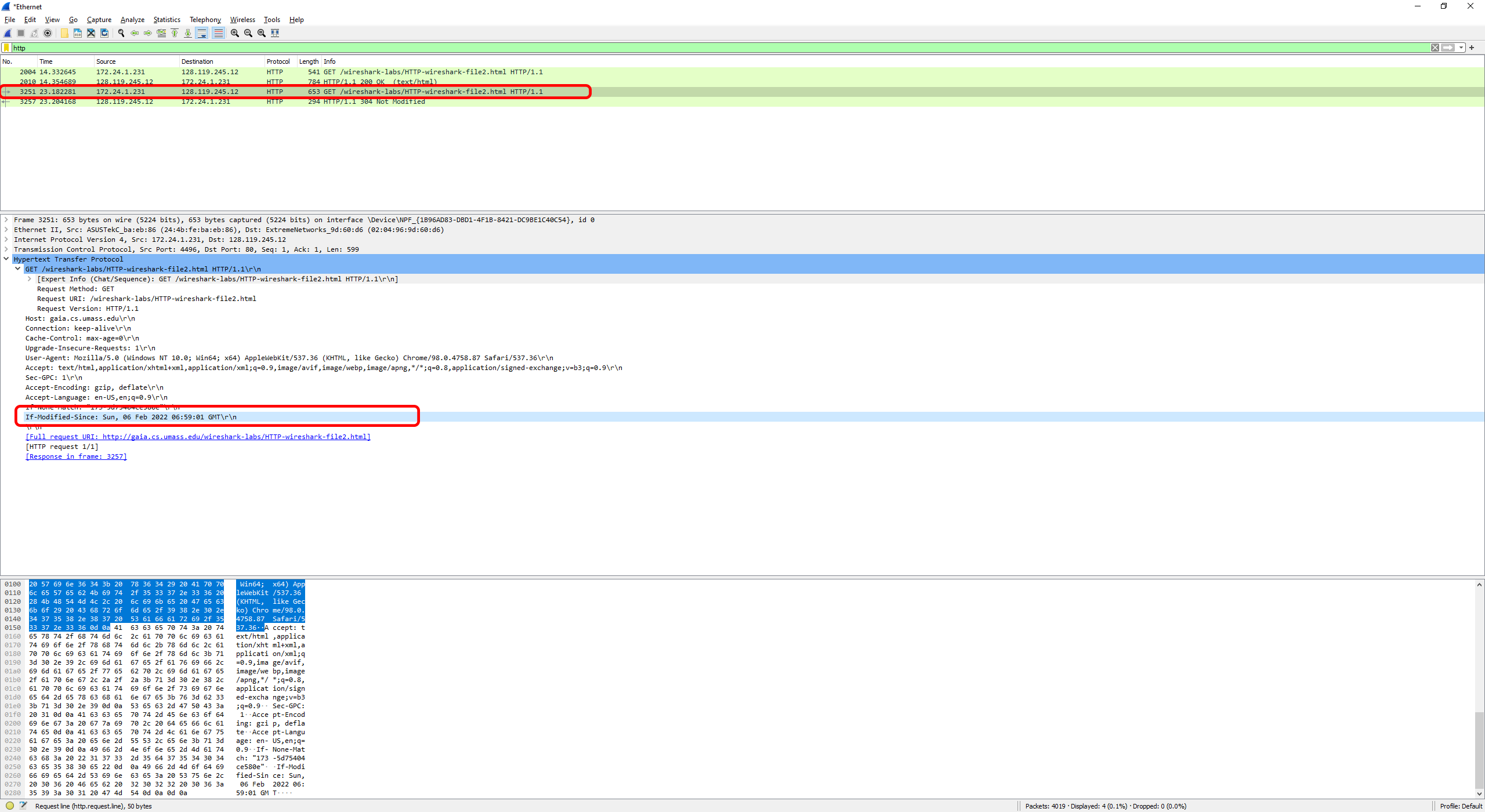
1. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Yes, it explicitly returns the contents of the file. I can tell because all of the data is listed in the line-based text data portion of wireshark, as well, in the raw data viewer I can see all of the data of the page.



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?

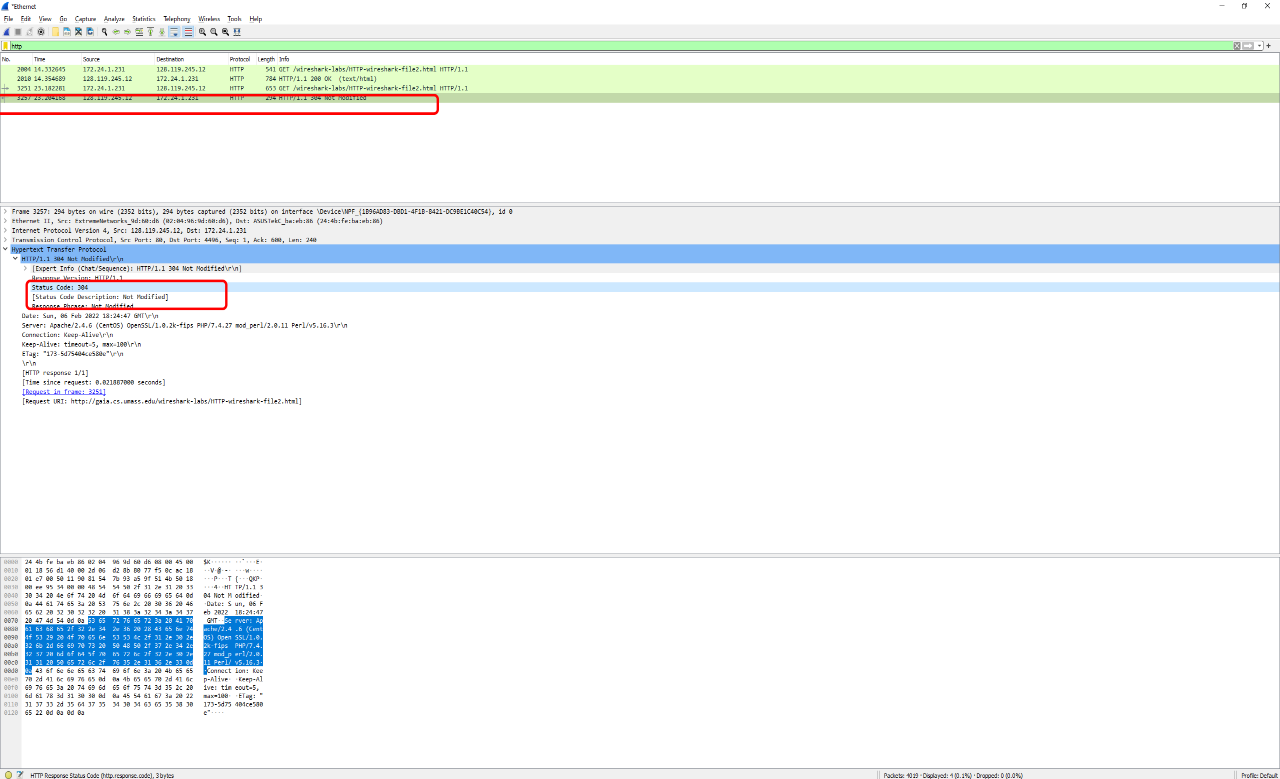
Yes, what follows is the date “If-Modified-Since: Sun, 06 Feb 2022 06:59:01 GMT”



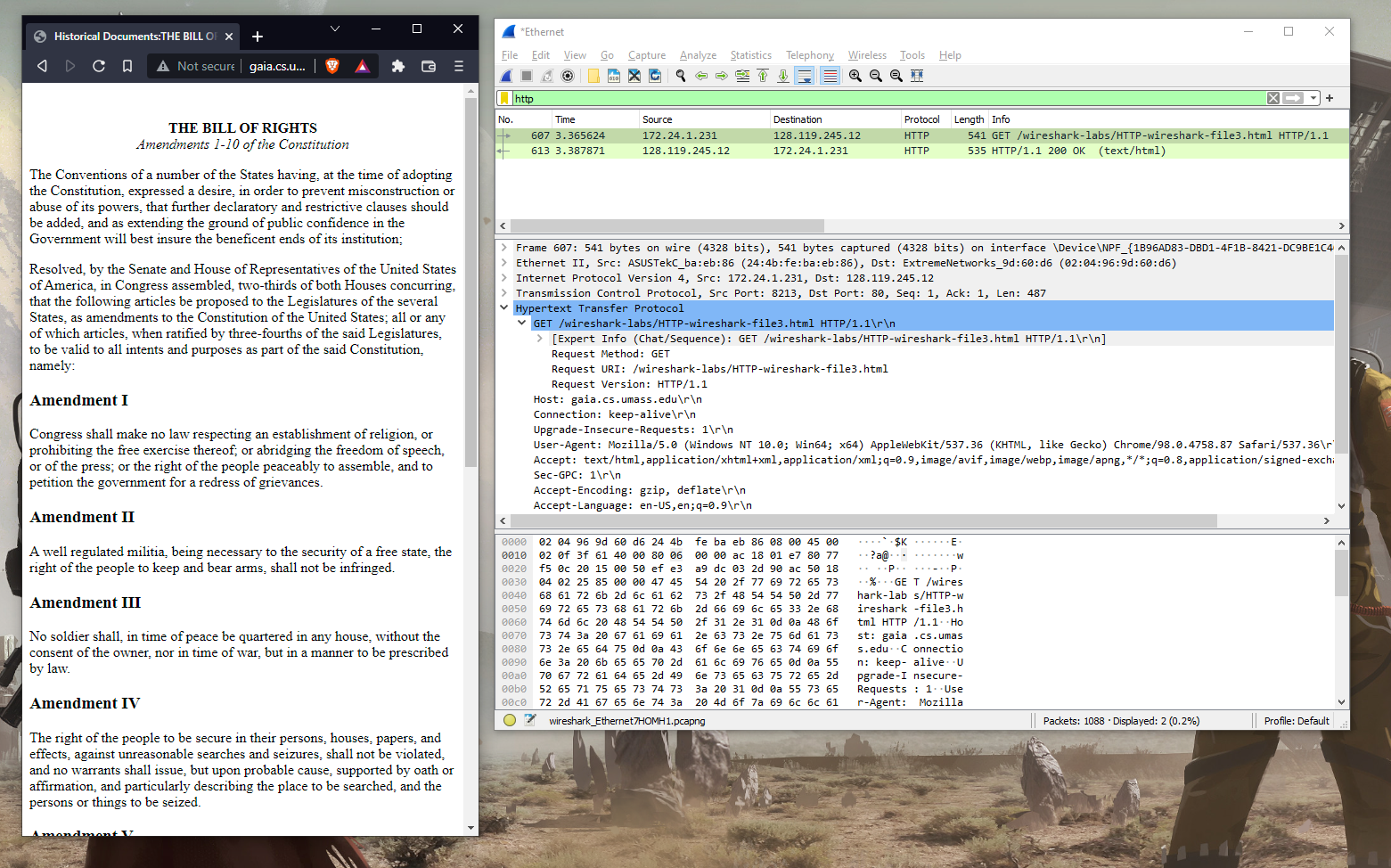
1. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

HTTP Status code: 304

Response: Not modified



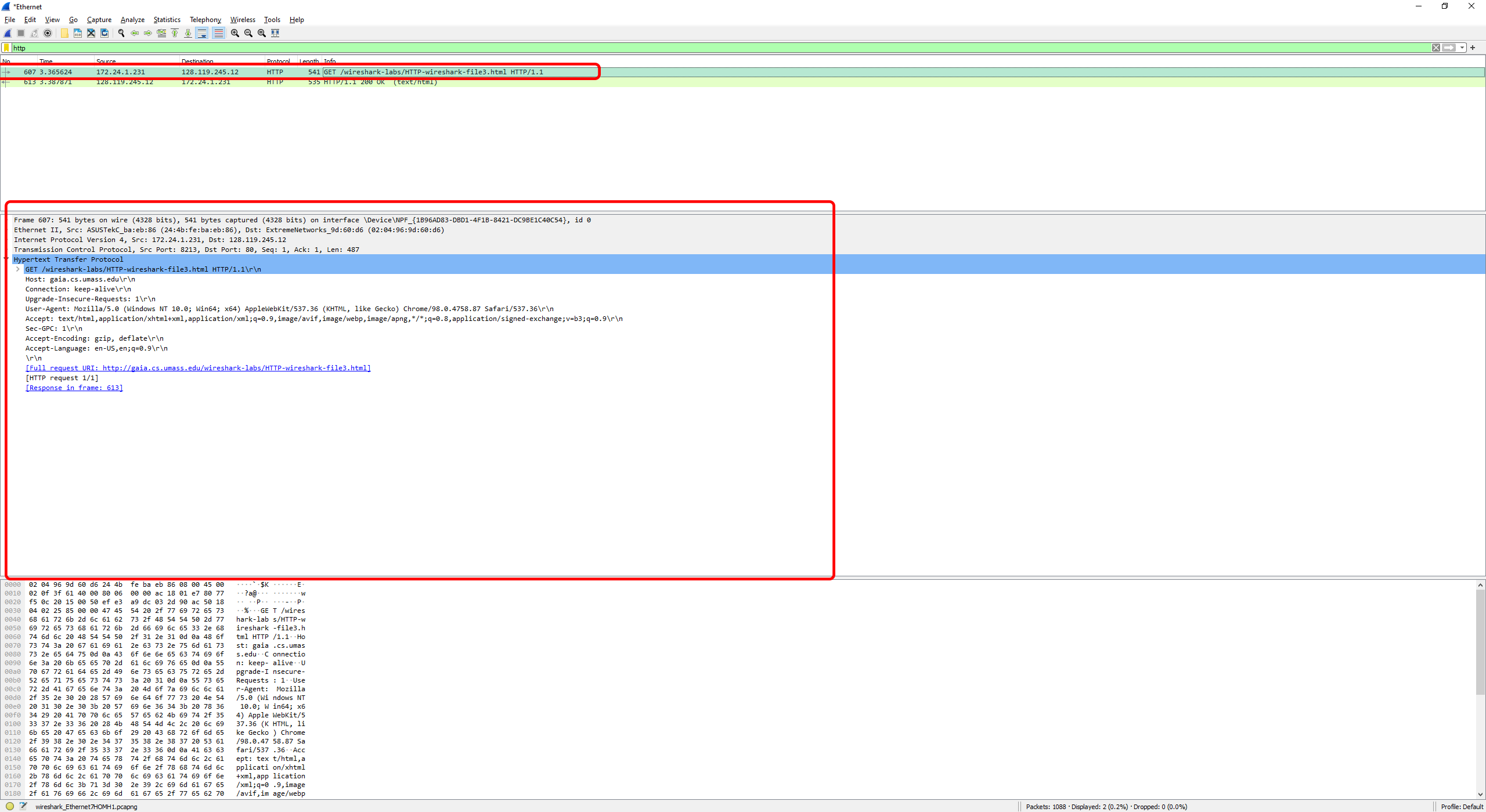
It did not explicitly return the contents of the file because it has detected that it hasn’t been modified since my last visit. There is also no raw data for the content of the page available like there was in question 9

Part 3

(Please note: It appears wireshark has changed since the creation of this lab, so the question and answers as well as information supplied to me is a little off)

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

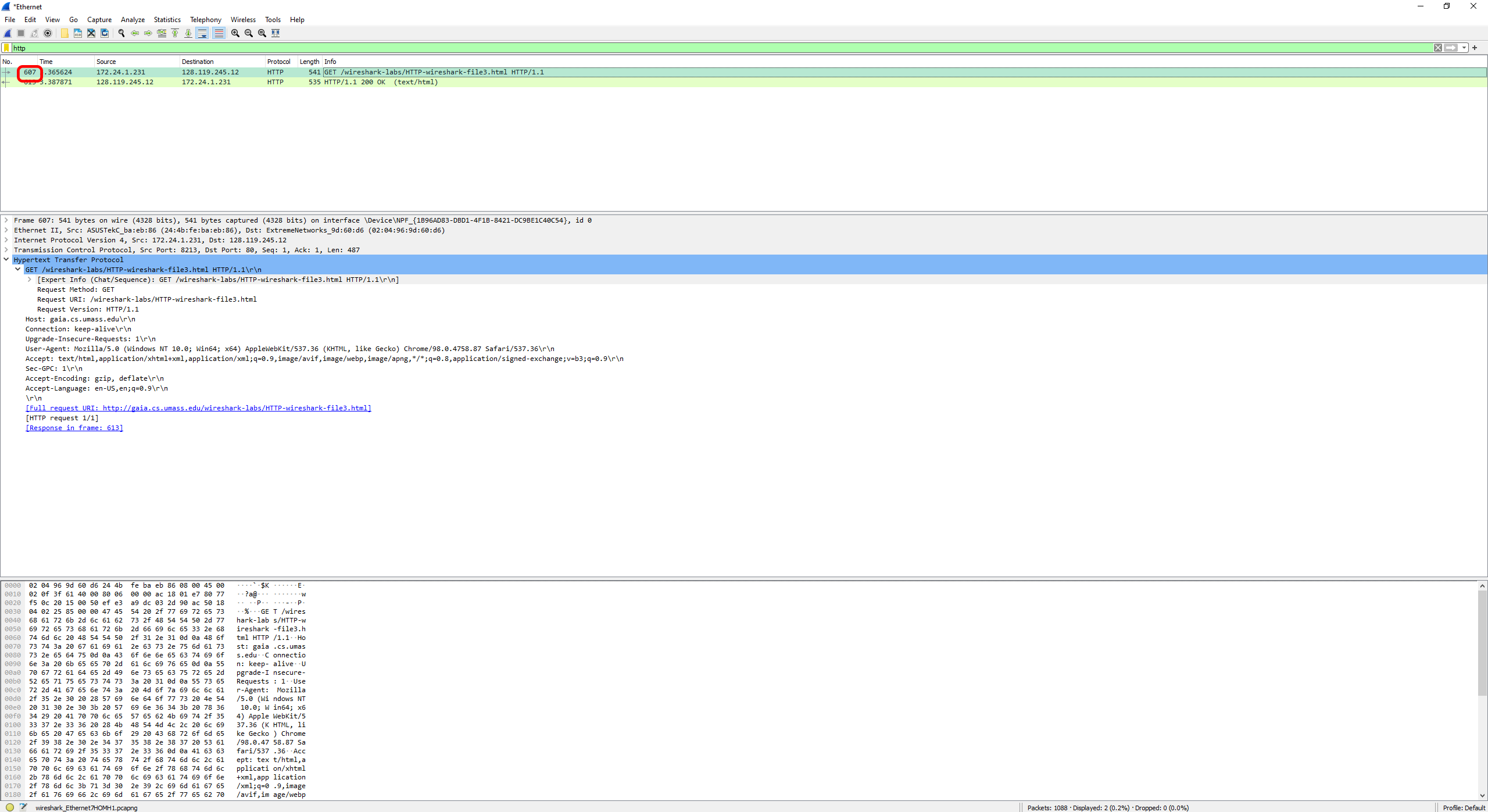
It contains 1 HTTP GET request message which does not contain the TCP segments, the TCP segments are within the server response.



The Bill of Rights is within the first TCP segment of the server response as shown in the picture below. Graphical user interface, application

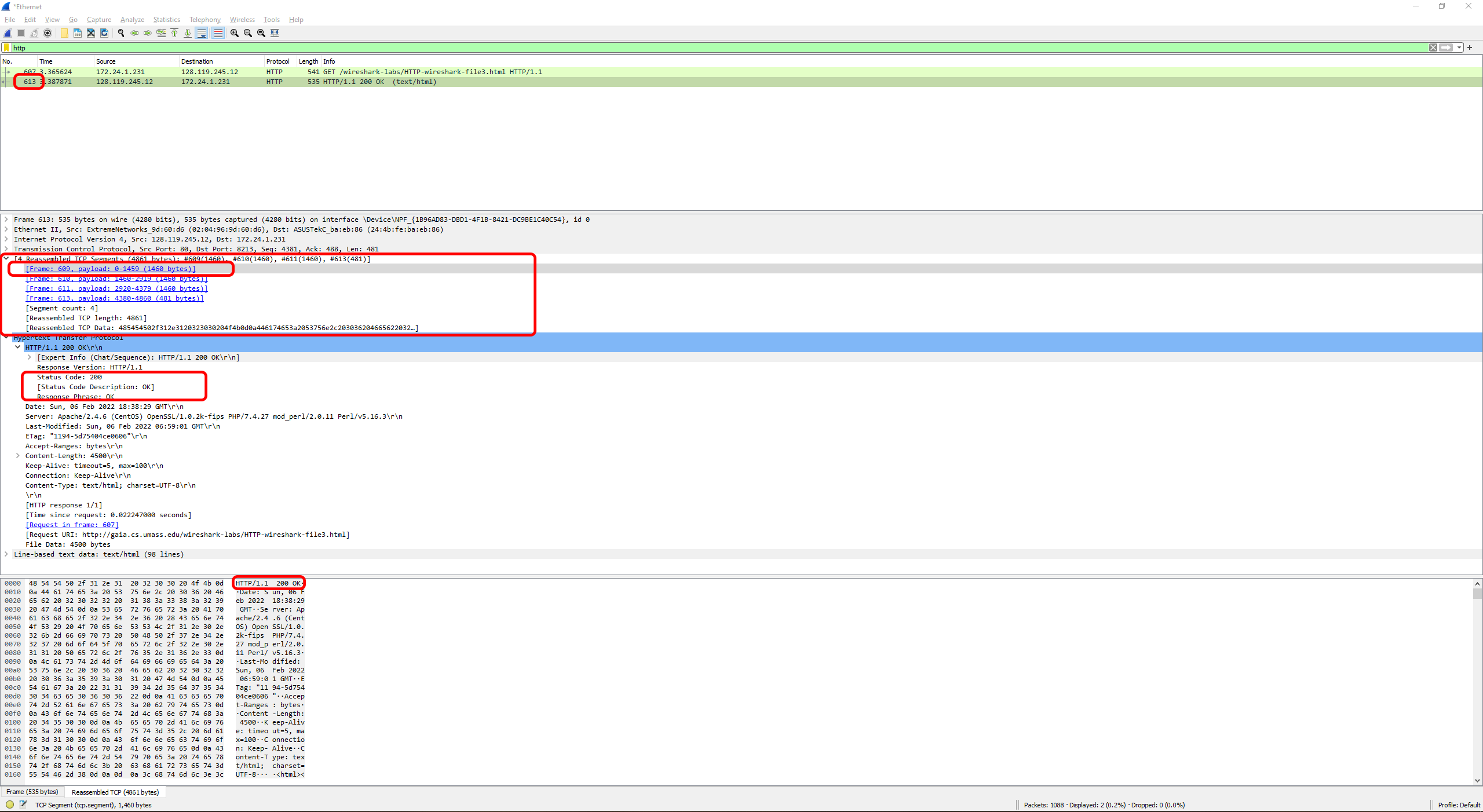
Description automatically generated

The actual Wireshark packet number for the HTTP GET is packet 607.



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

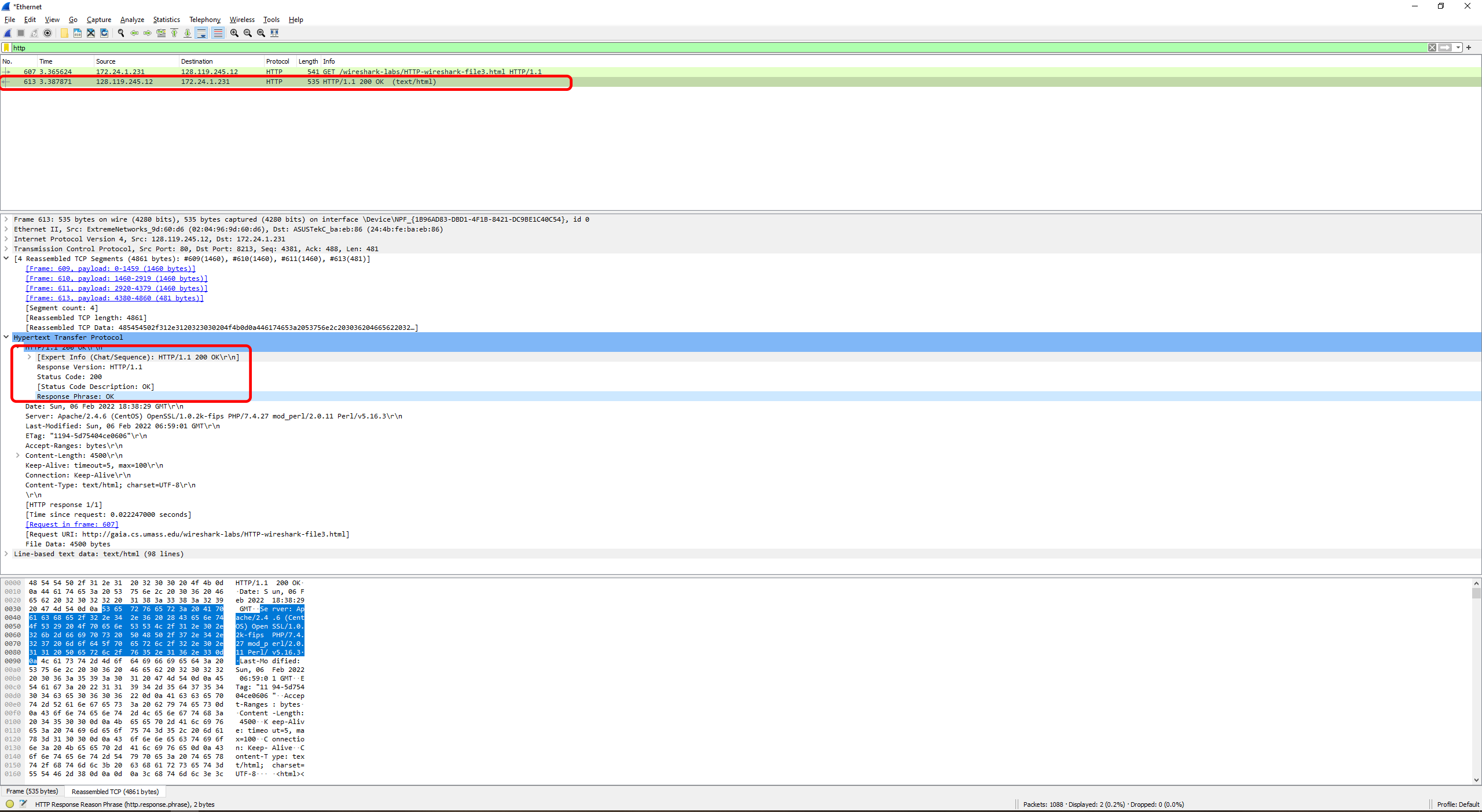
It is TCP segment number 1, however, actual Wireshark packet number 613



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

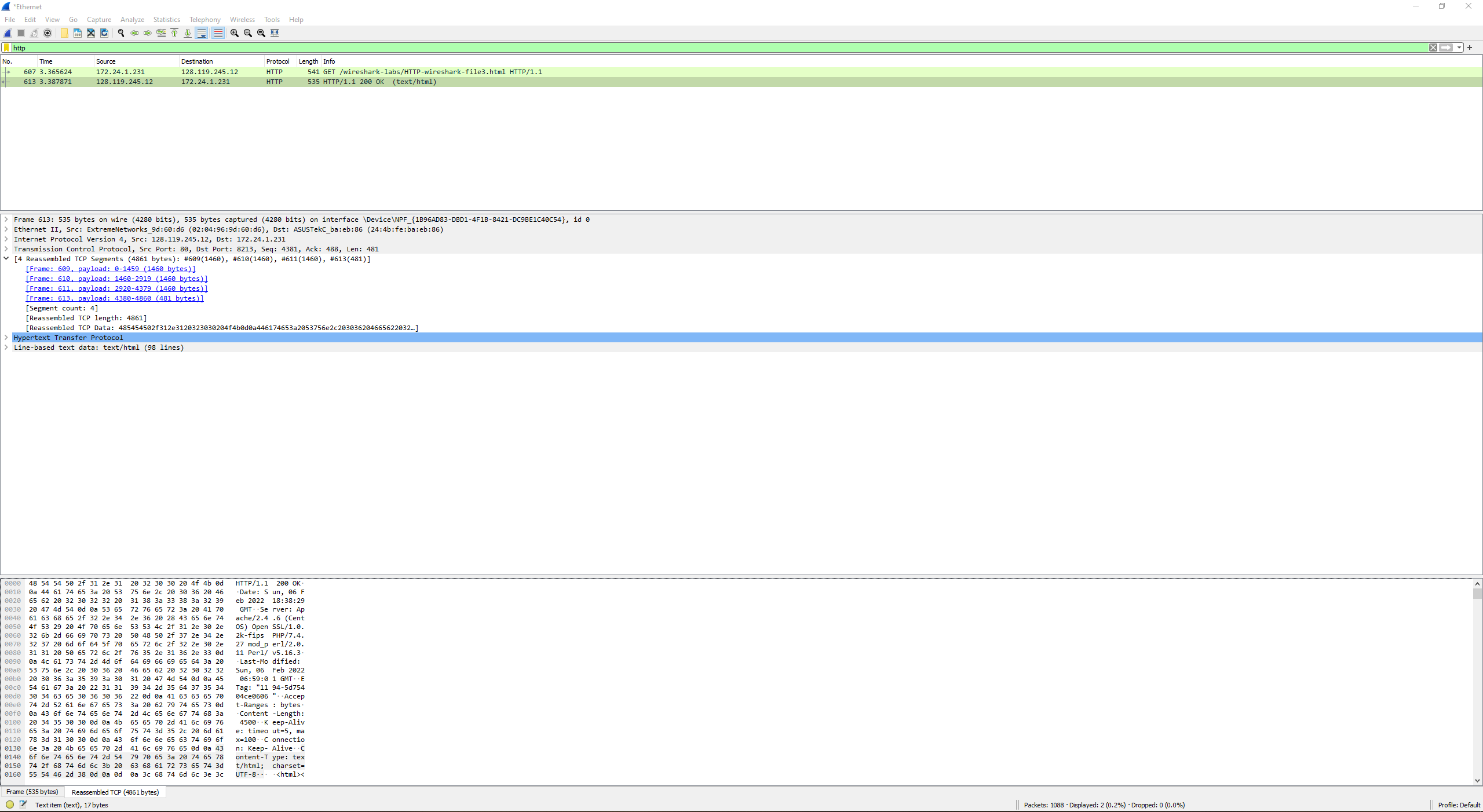
200

OK

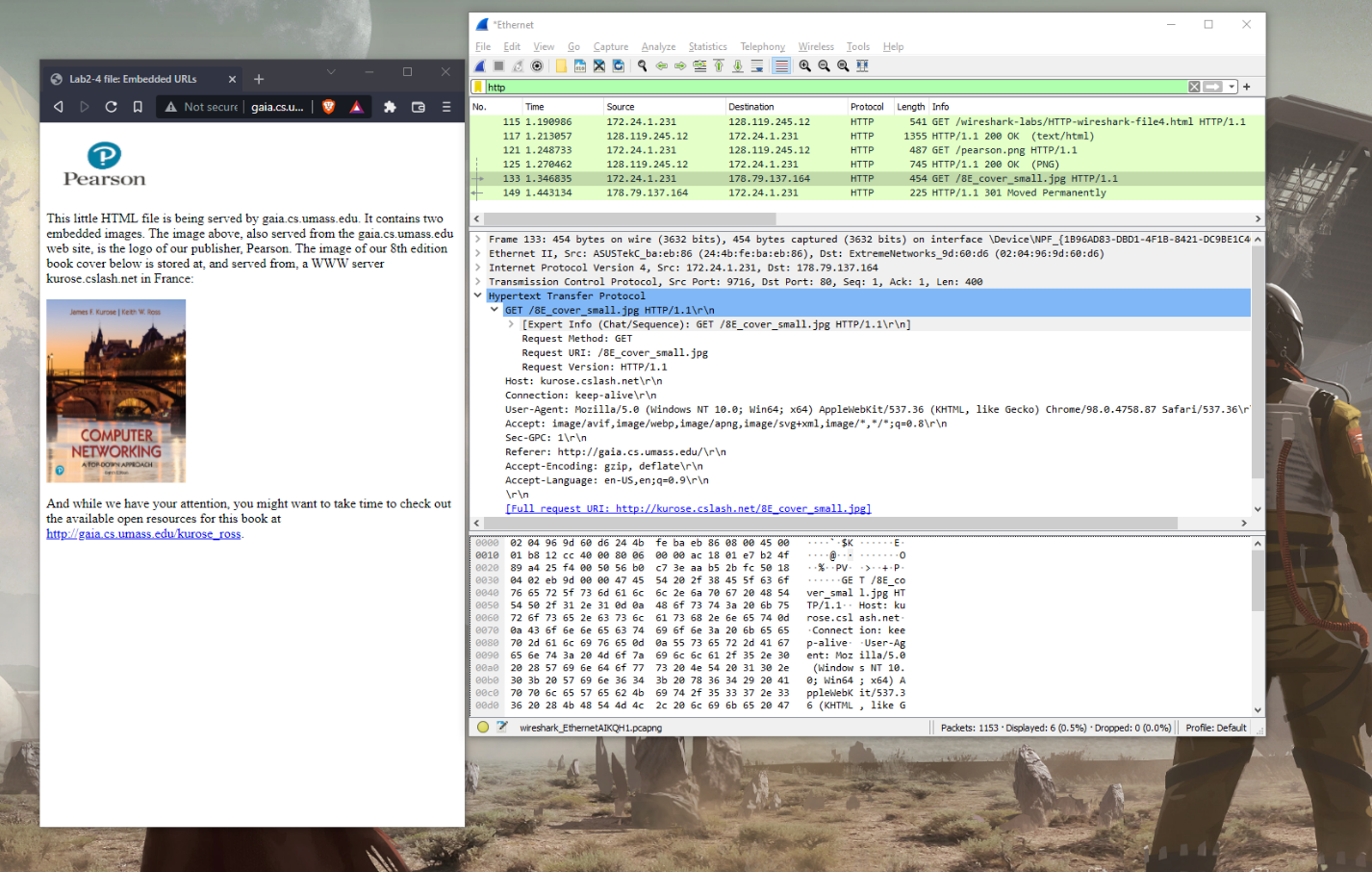


1. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

4 TCP segments



Part 4



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

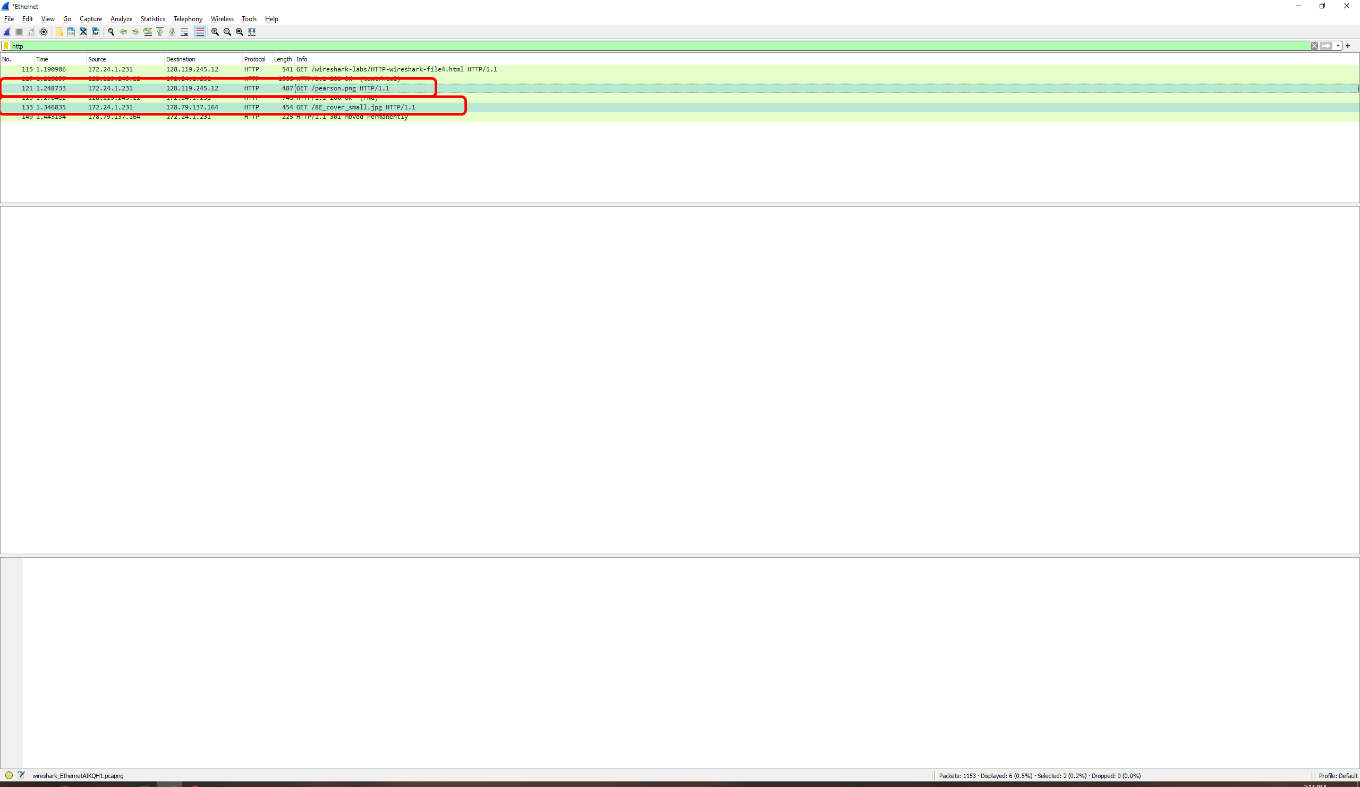
3 GET Request messages sent

1st GET IP: 128.119.245.12

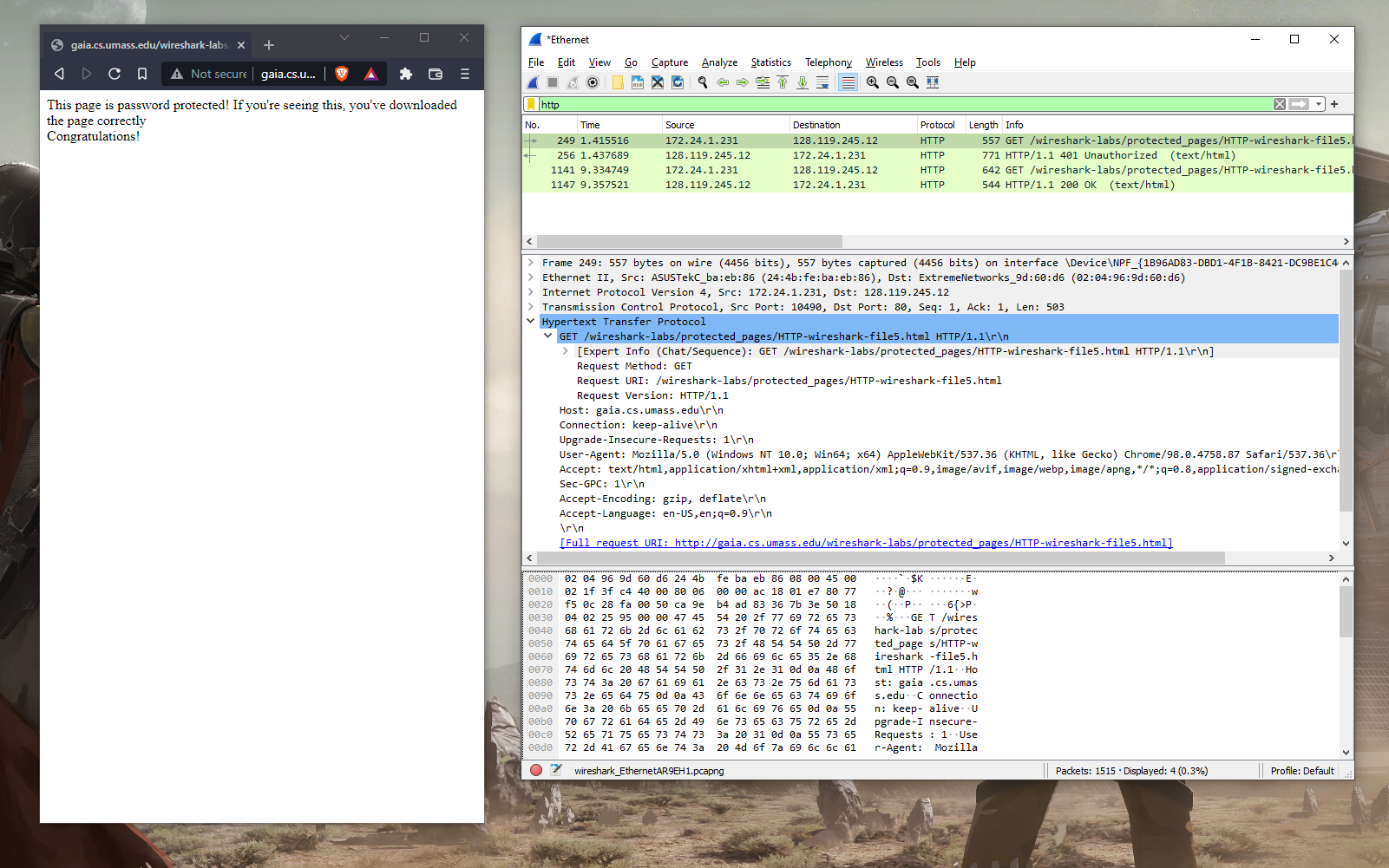
2nd GET IP: 128.119.245.12

3rd GET IP: 178.79.137.164

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.

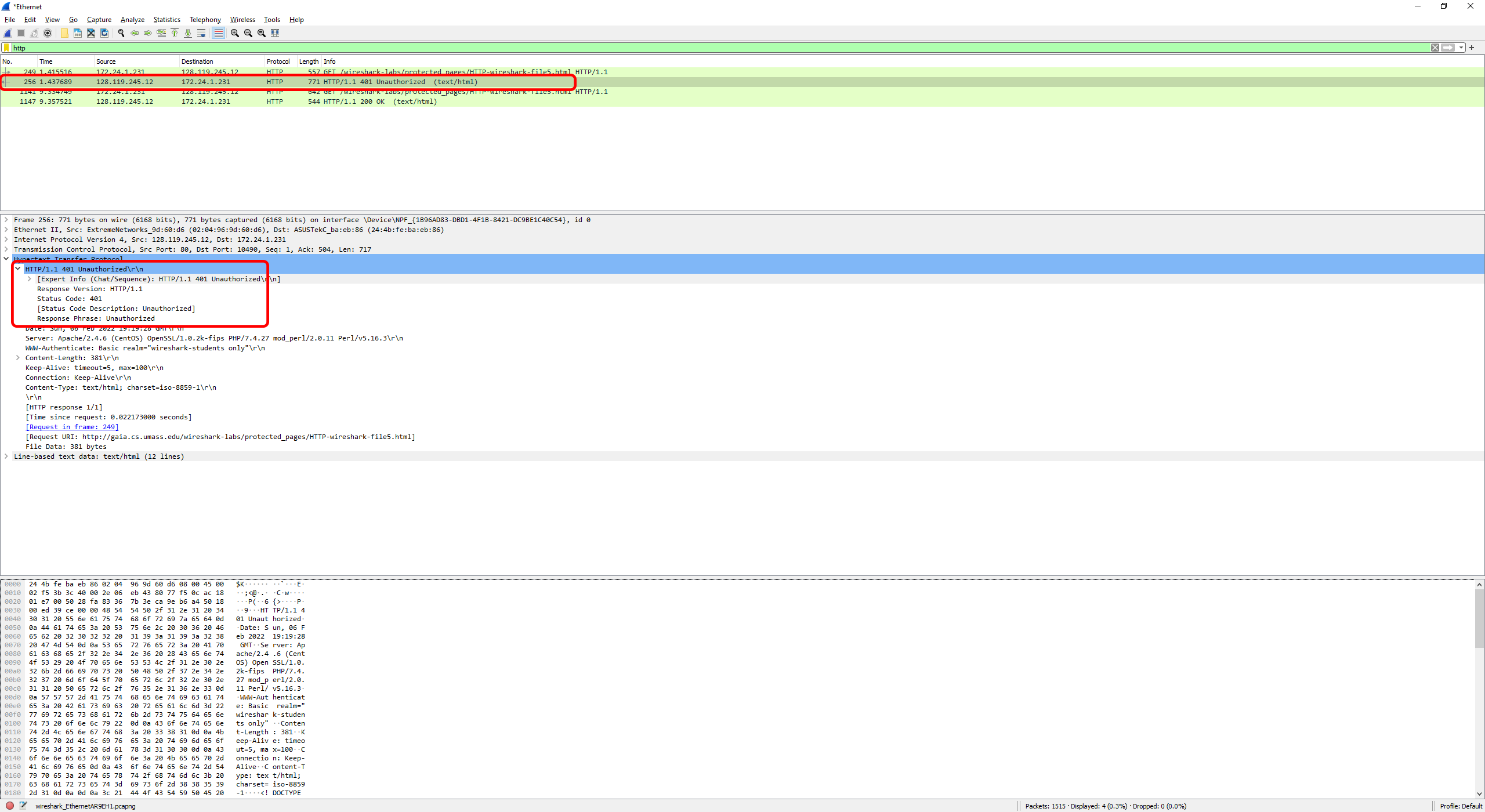
They were downloaded serially as there were two separate GET requests for it, as well they were downloaded within 2 different responses back

Part 5

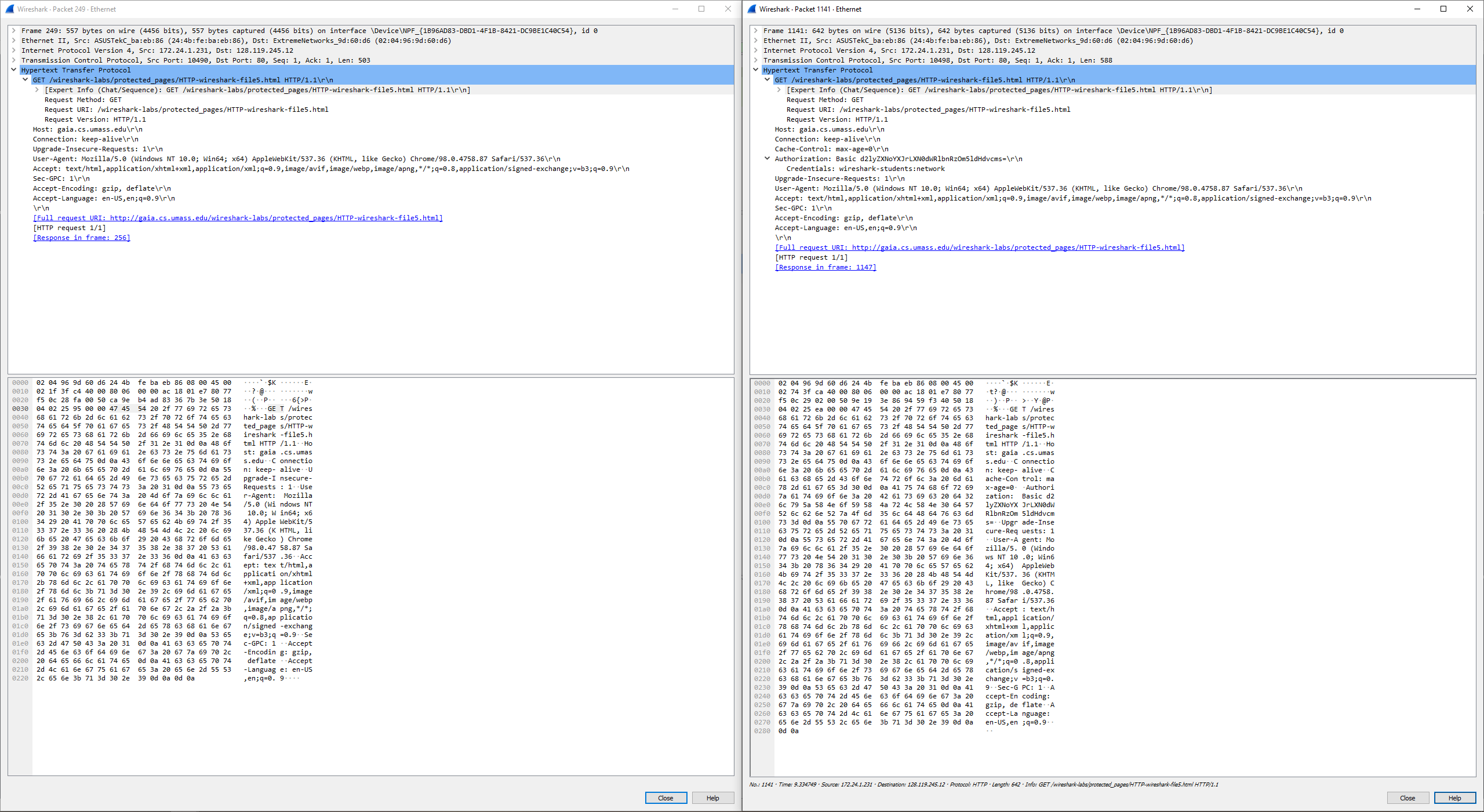


1. What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser?

401

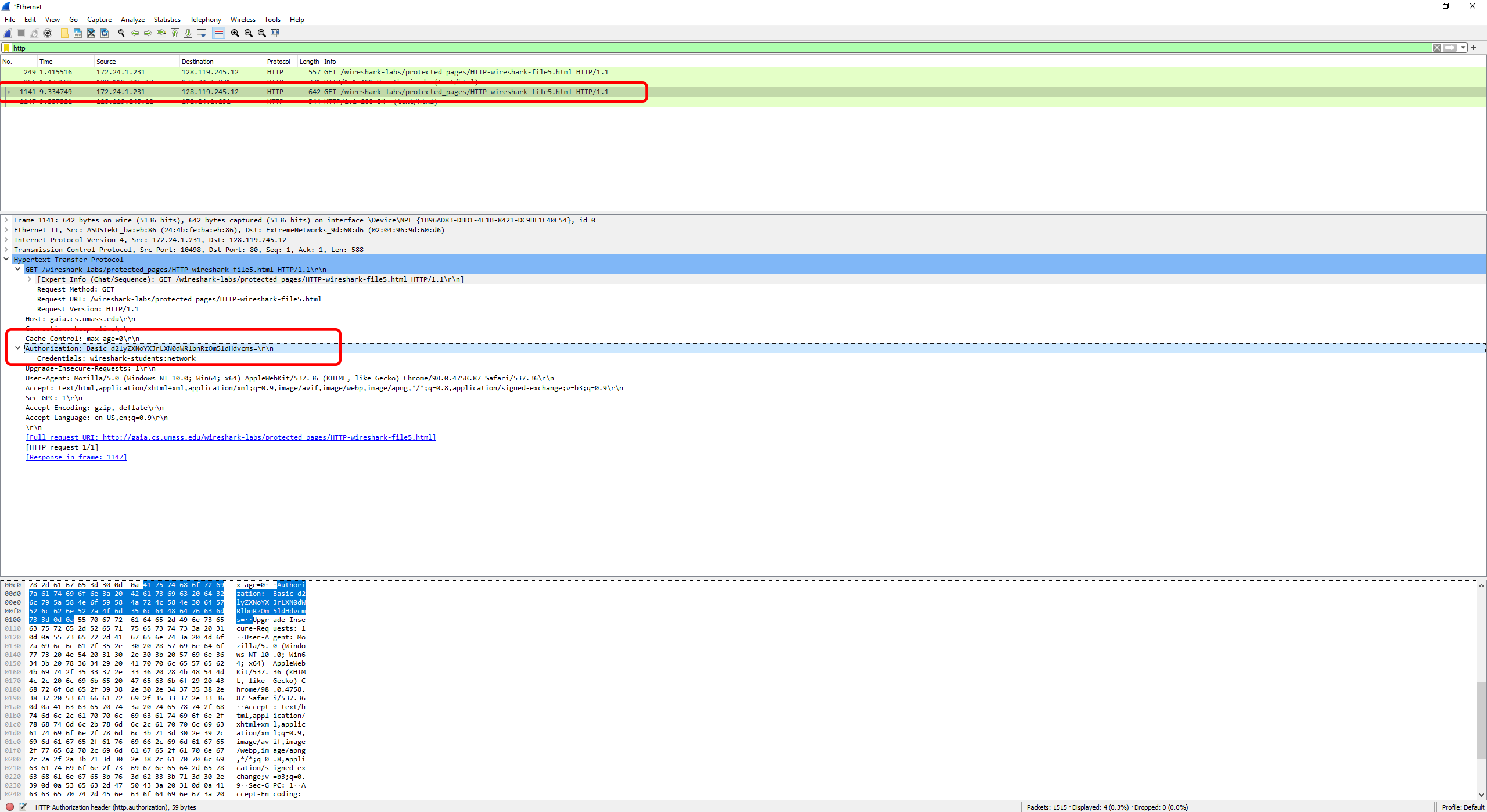
Unauthorized

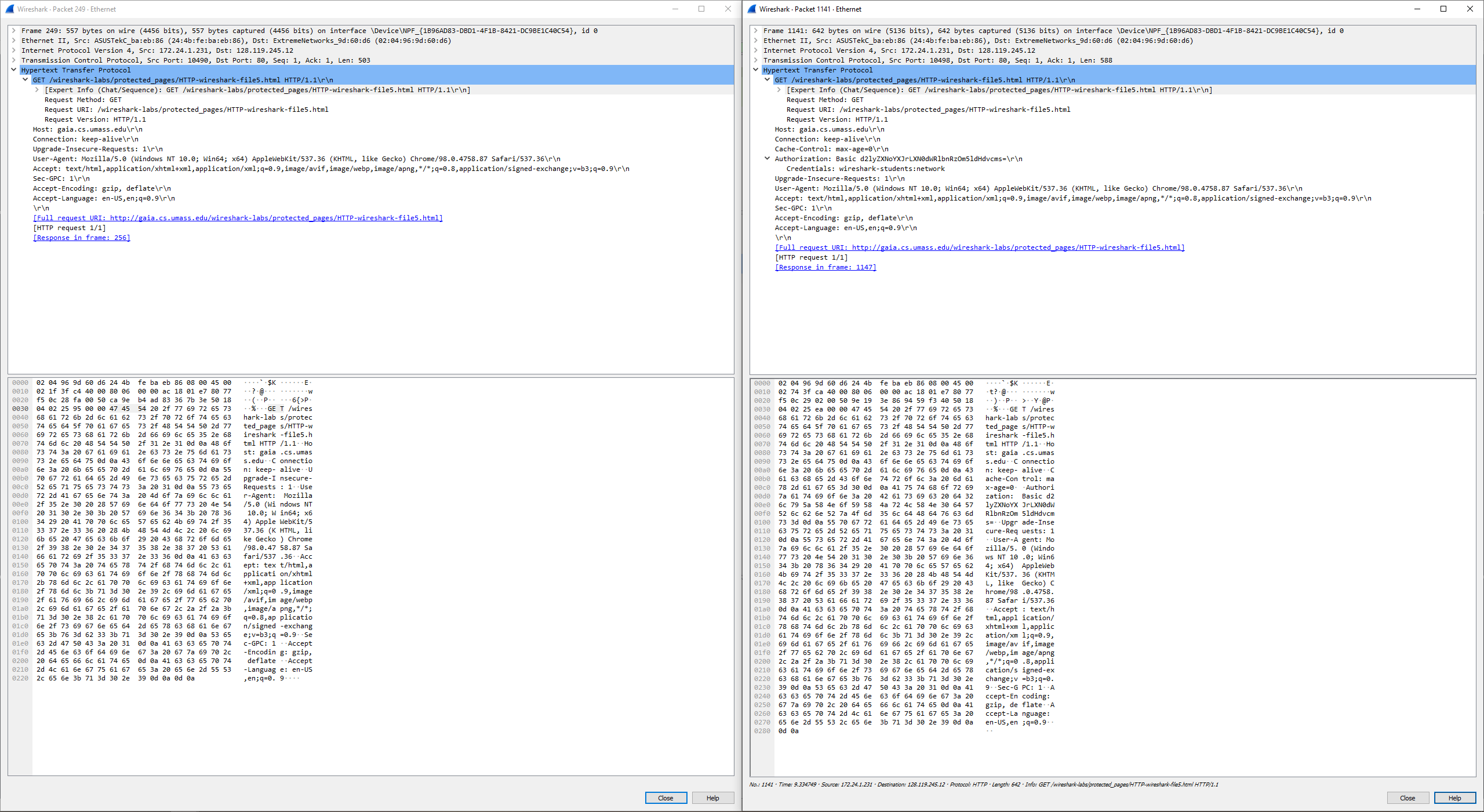
1. When your browser’s sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

Both cache-control and Authorization Basic are new in the second HTTP GET message as well a credentials

Cache-Control: max-age=0

Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=





I pledge that on all academic work that I submit, I will neither give nor receive unauthorized aid, nor will I present another person's work as my own.

Dalton Murray