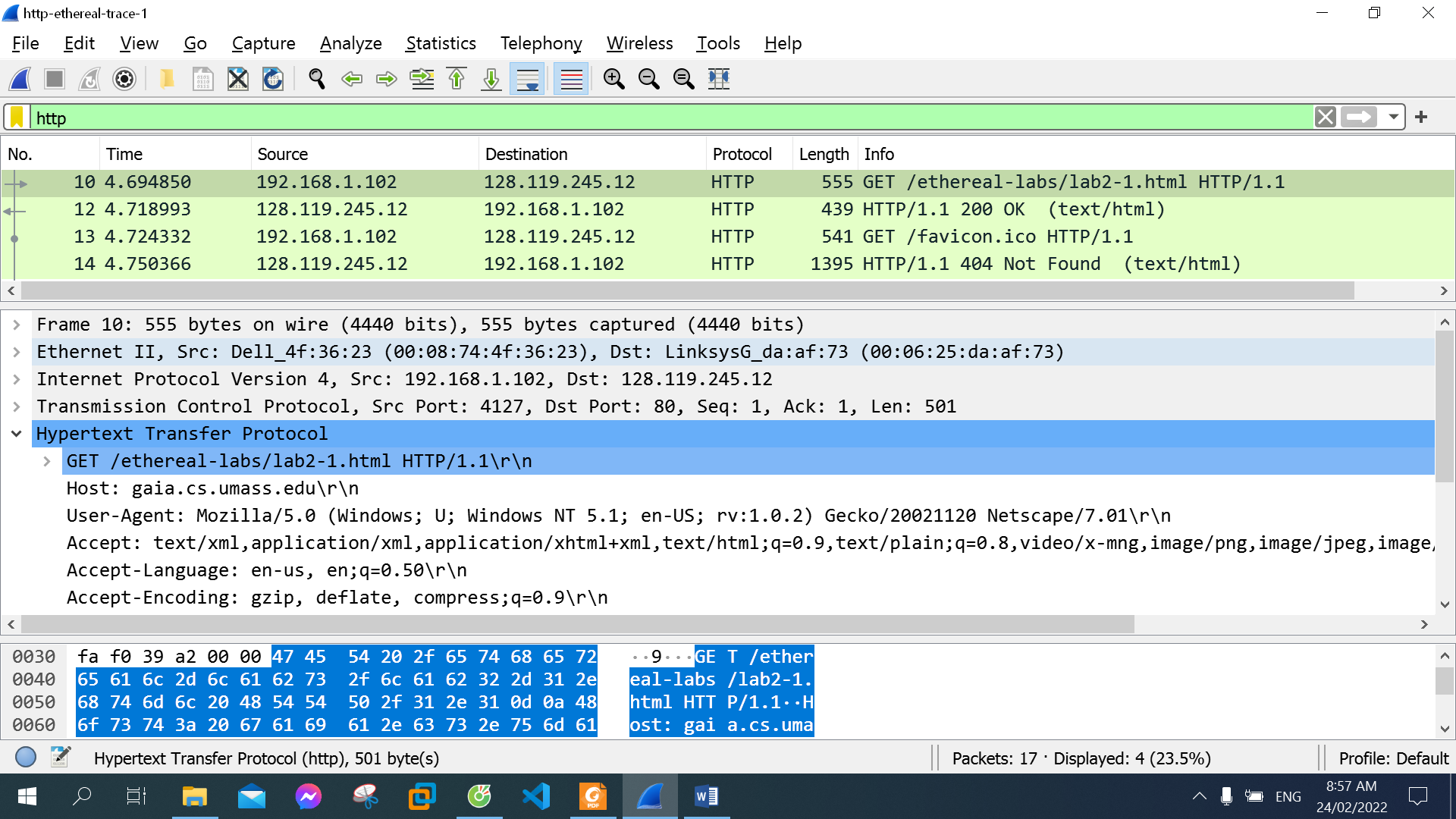
**LAB 2A**

**Wireshark Lab: HTTP v8.0**

**Name: Hồ Đức Trí**

**Student No: 1912288**

I/ The Basic HTTP GET/response interaction

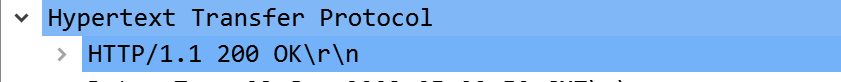


1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

My browser is running HTTP version 1.1:



The server is running HTTP version 1.1:

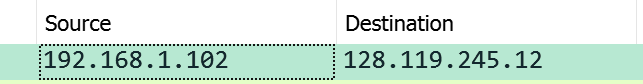


1. What languages (if any) does your browser indicate that it can accept to the server?

en - us



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



Internet address of my computer 192.168.1.102

IP address gaia.cs.umass.edu server is 128.119.245.12

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

OK 200



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



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

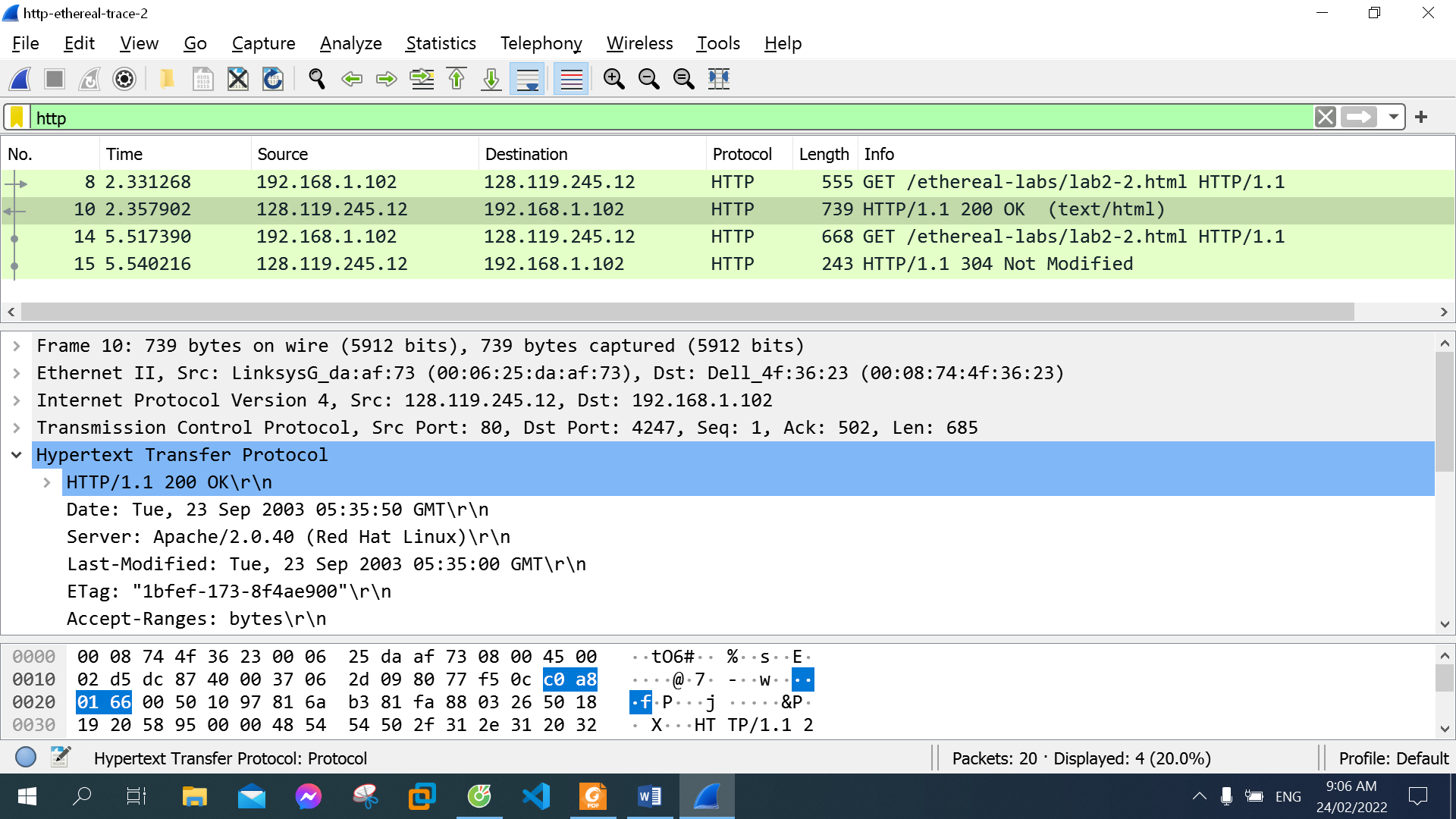


1. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

Date, Server, Last-Modified… in response message

II/ The HTTP CONDITIONAL GET/response interaction

The first GET message



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

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

Yes. Because the Line-based text data in OK message responses to the GET message.

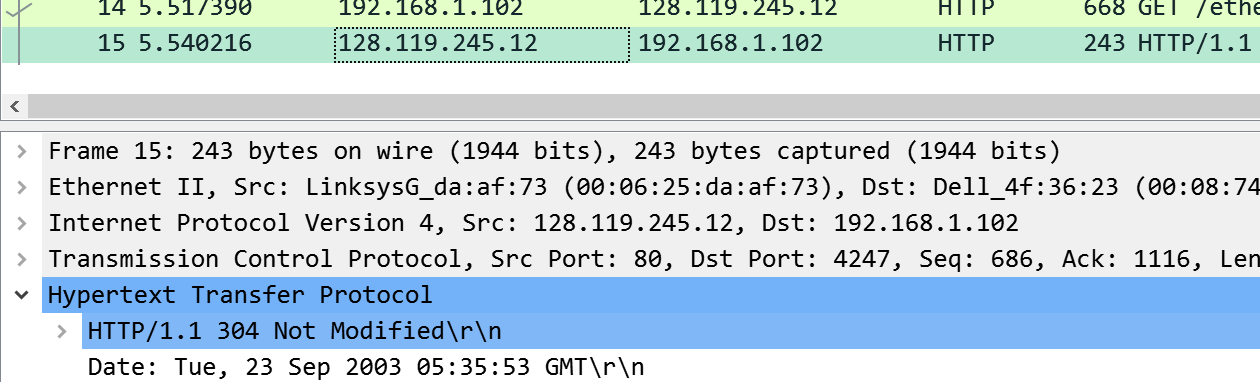
1. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

Yes.



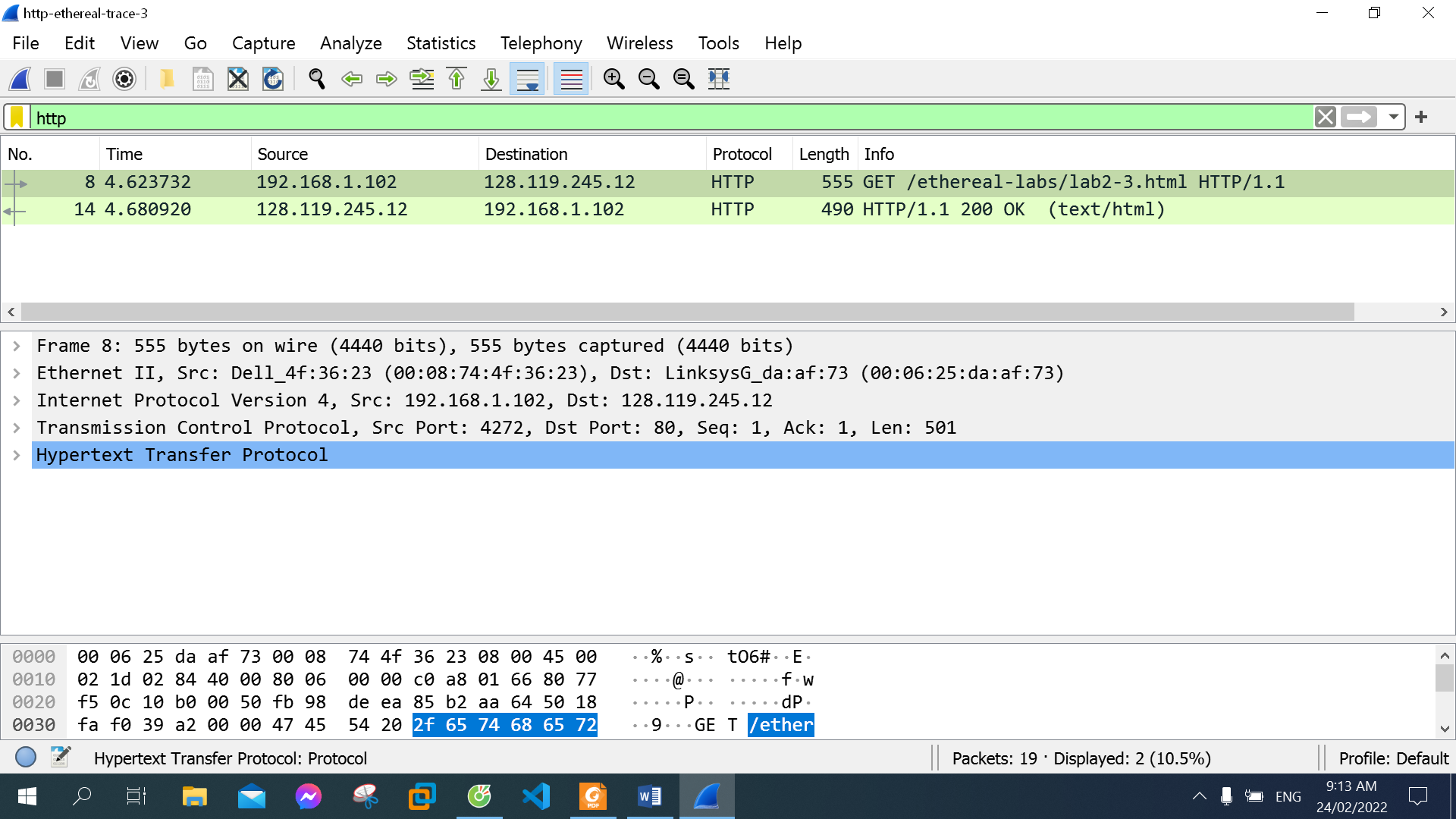
1. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

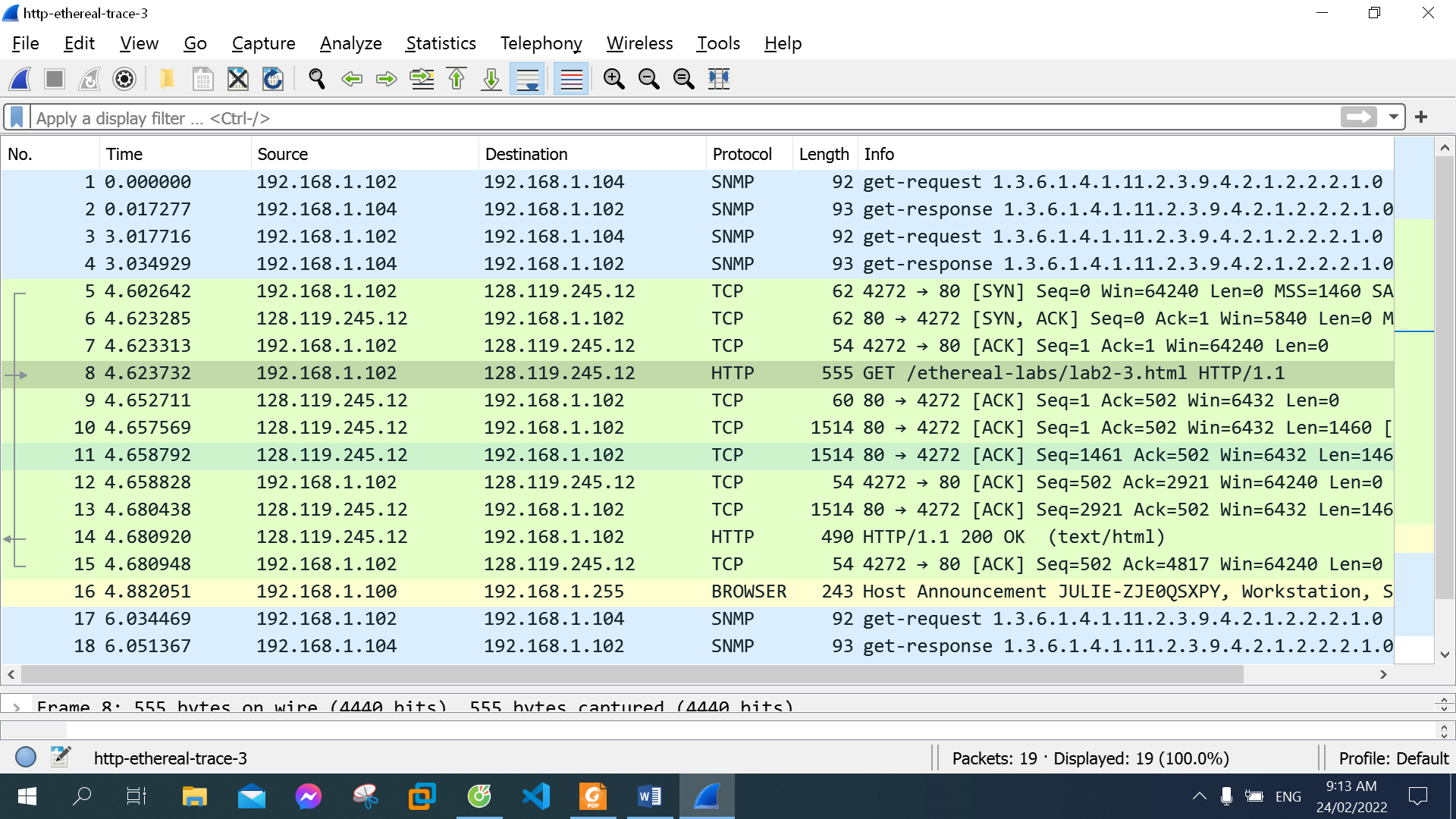
304 Not Modified.



No, the redirection response code server did not return the contents of the file. The HTTP 304 Not Modified client indicates that there is no need to retransmit the requested resources.

III/ 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?

1 messages.

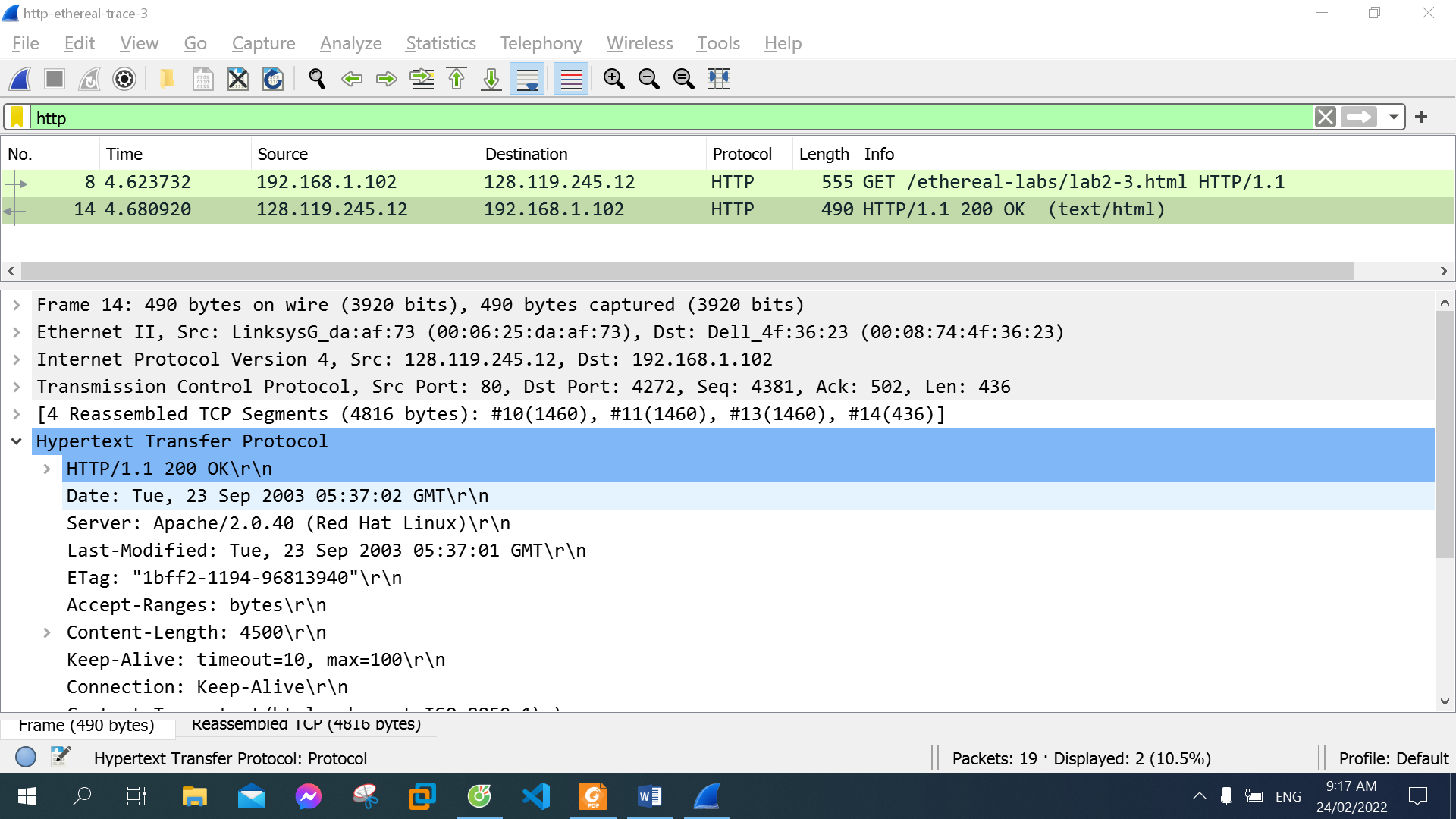
Package number 8.

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

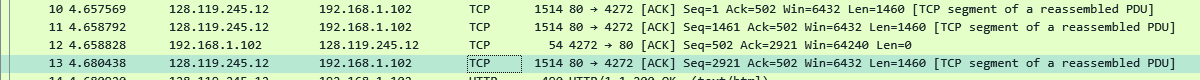
Package number 14.

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

200 OK.



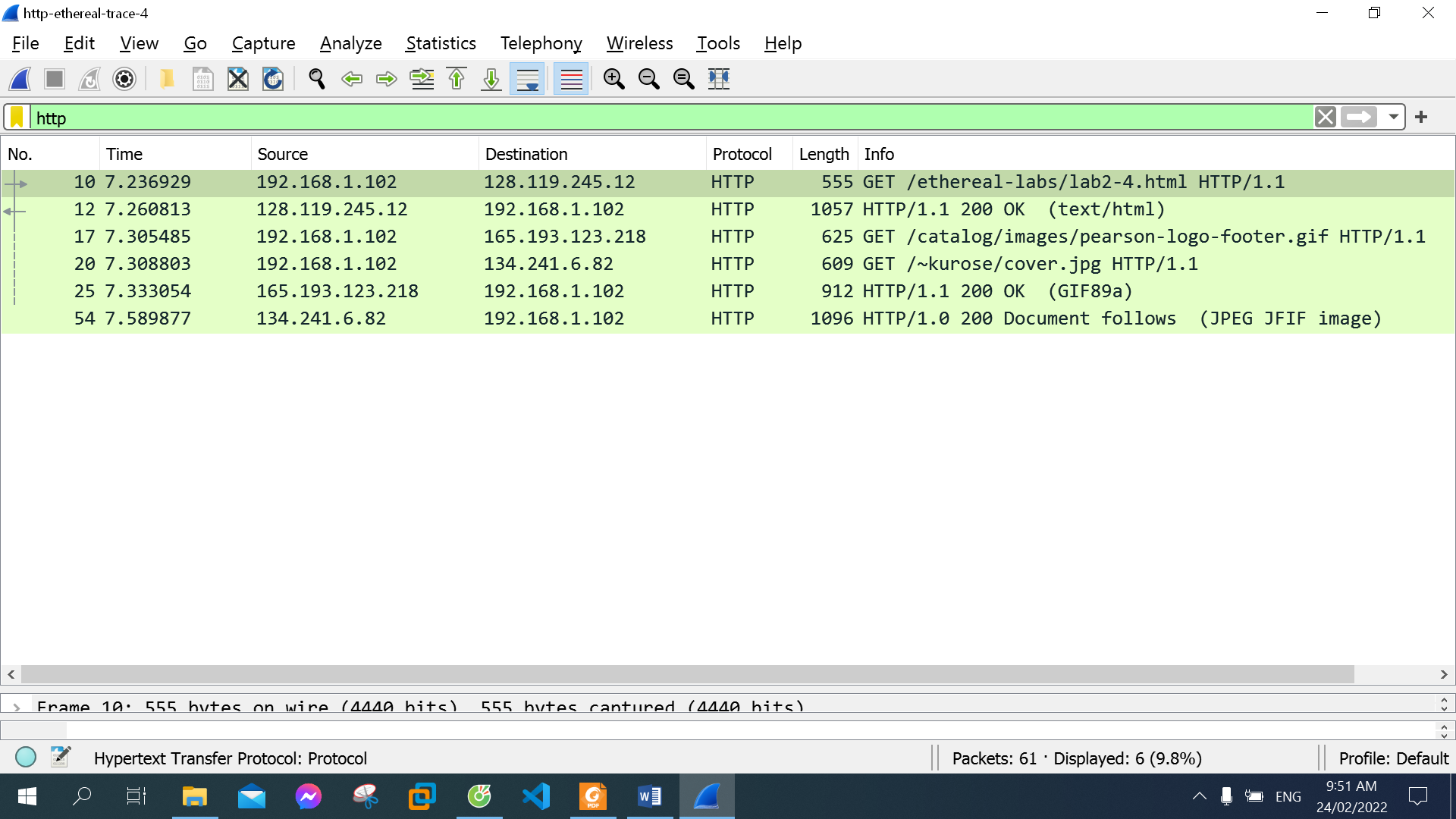
1. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?



3 segments, package number 10, 11, 13.

IV/ 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?



3 messages.

128.119.245.12,

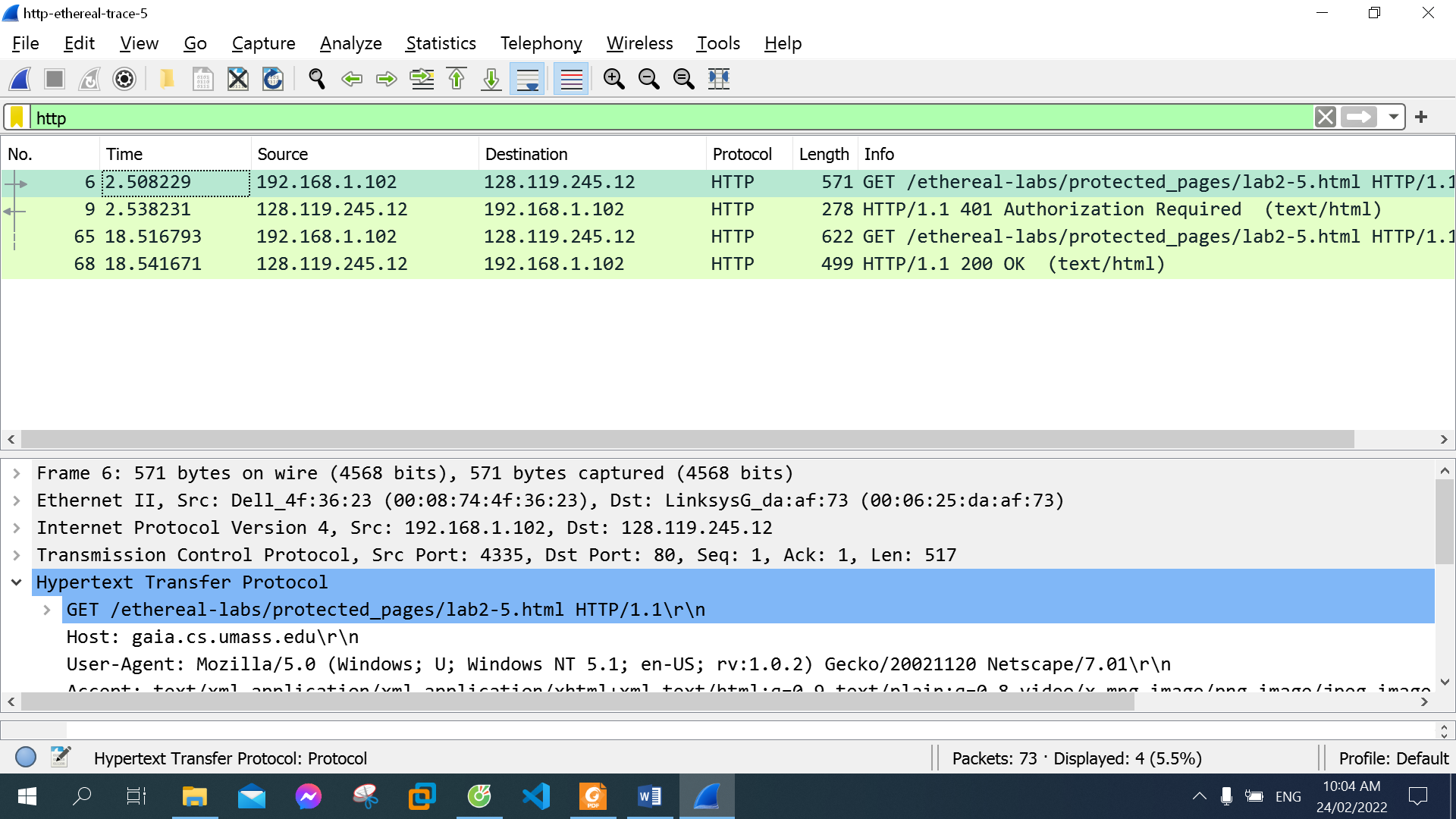
165.193.123.218,

134.241.6.82

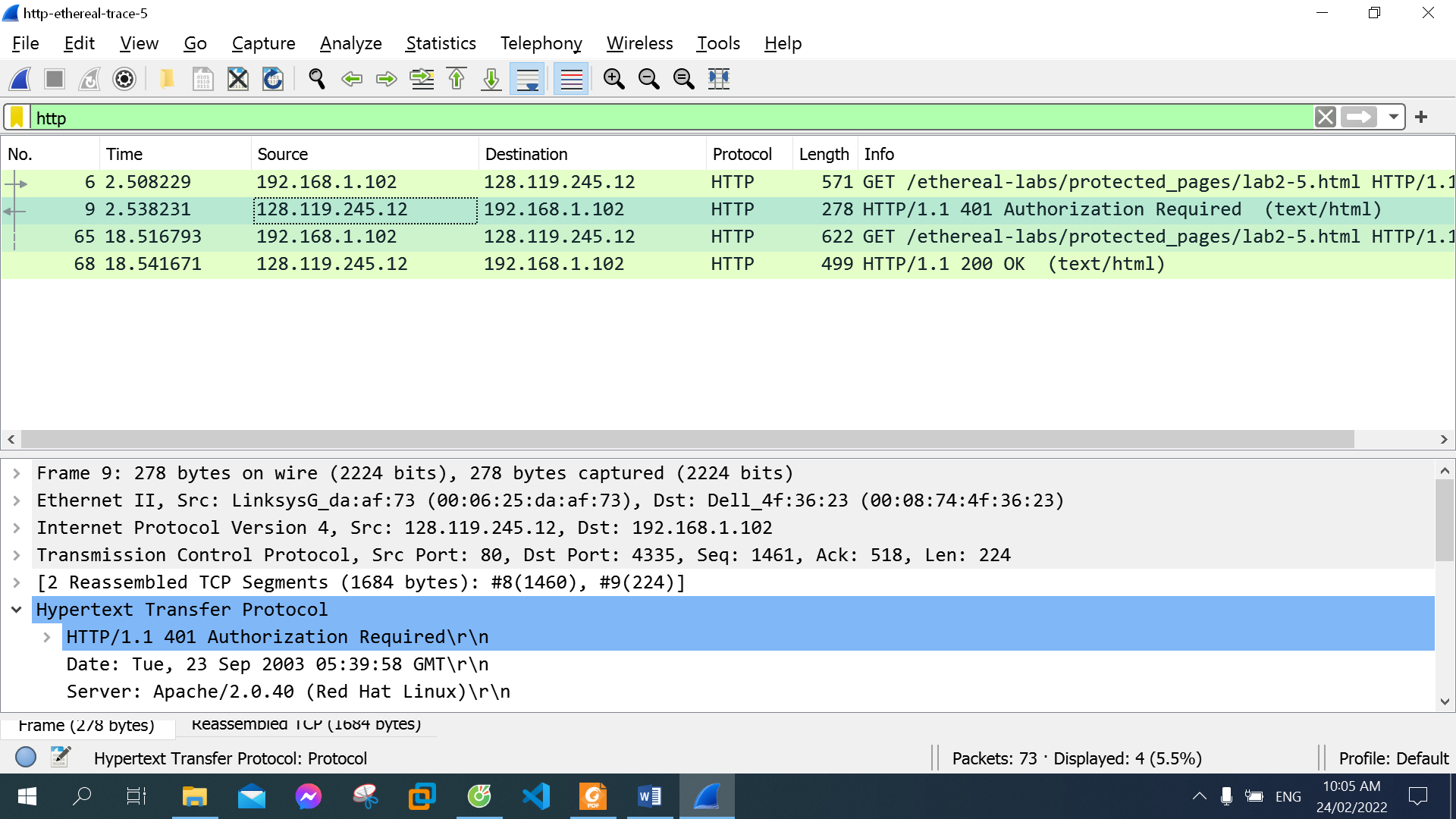
17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

My browser downloaded the two images from the two web sites in parallel. Because the second image sends the request right after the first image's GET command

V/ HTTP Authentication



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



401 Authorization Required

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

The field Authorization

