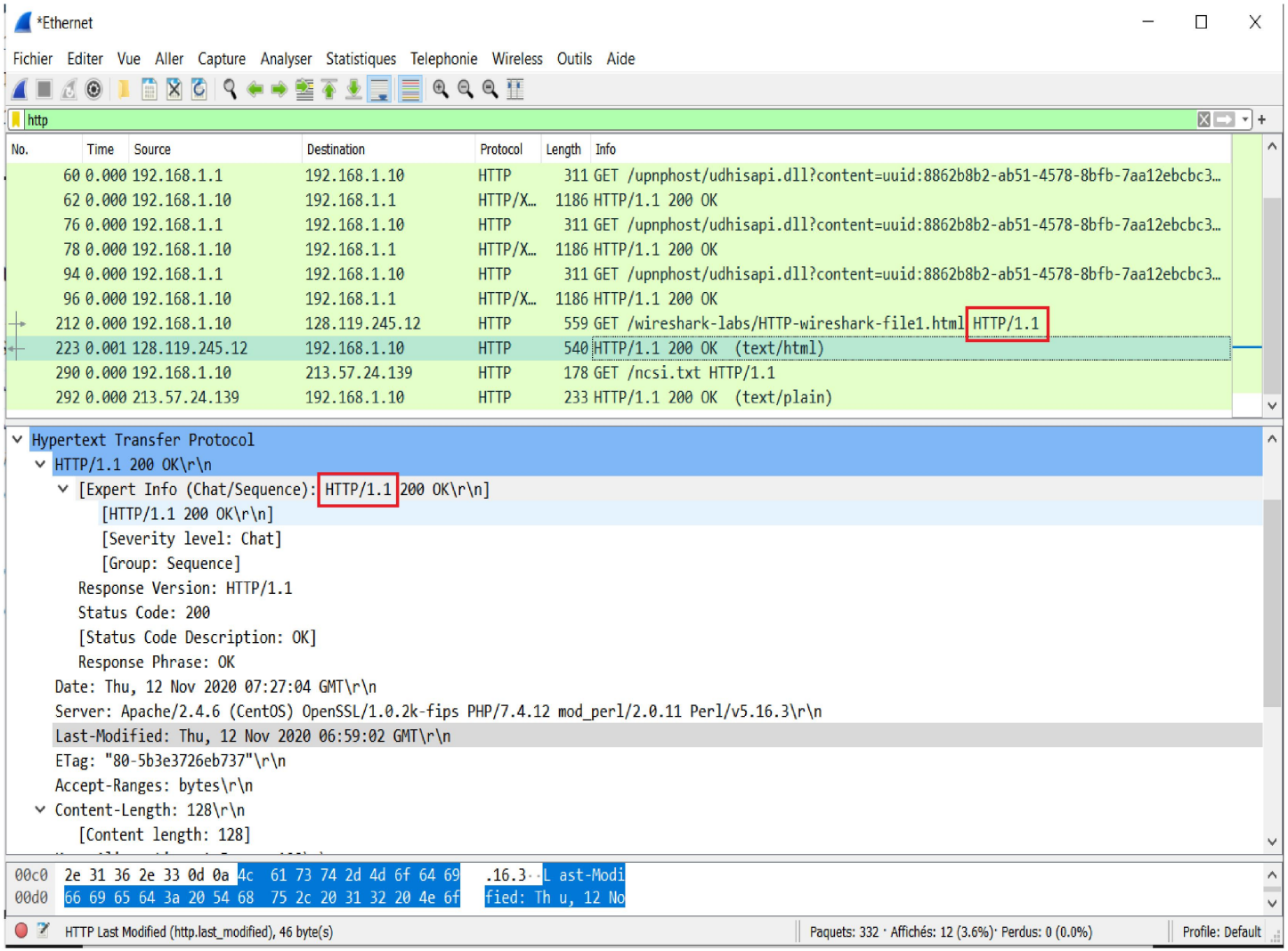
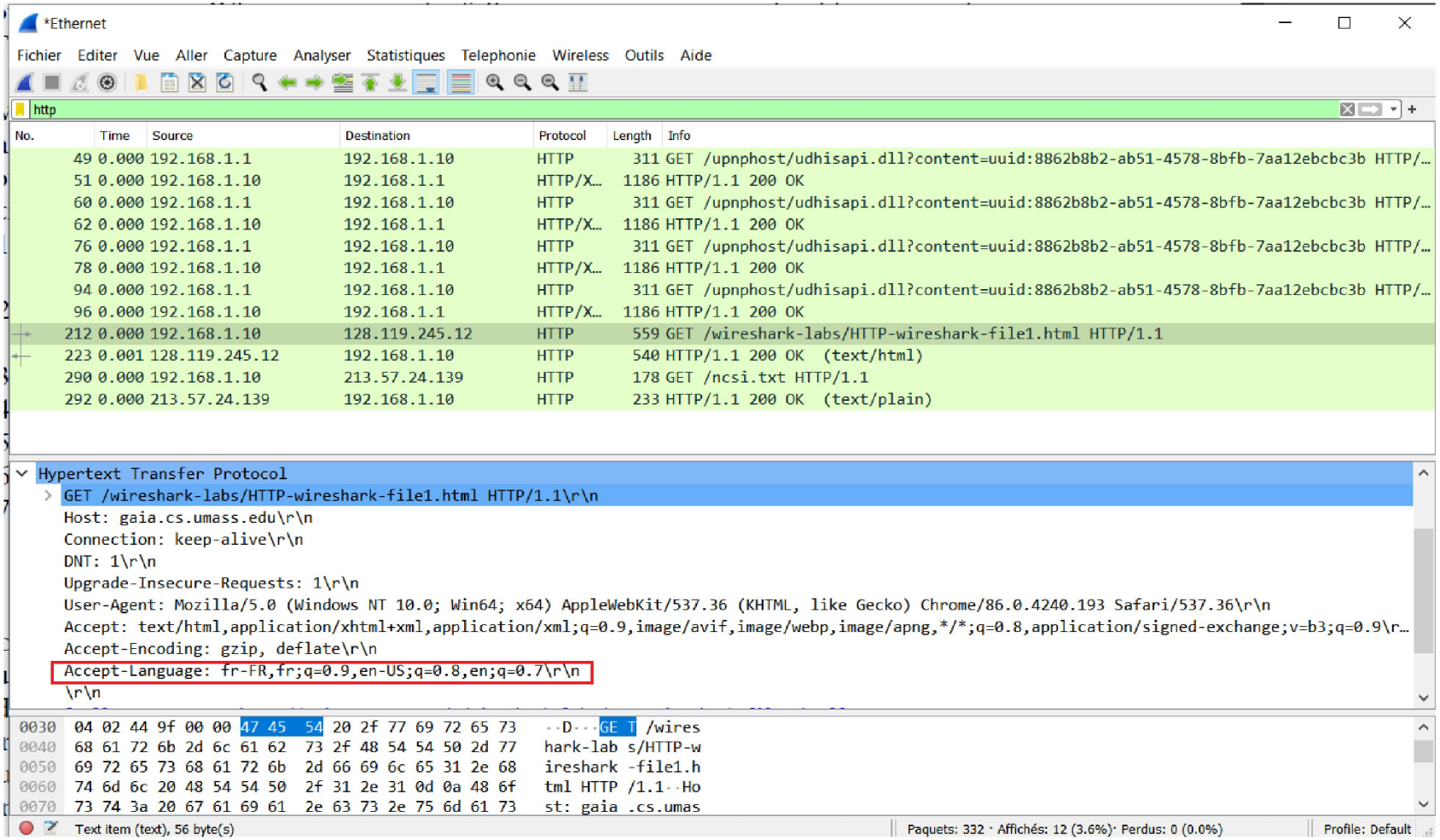


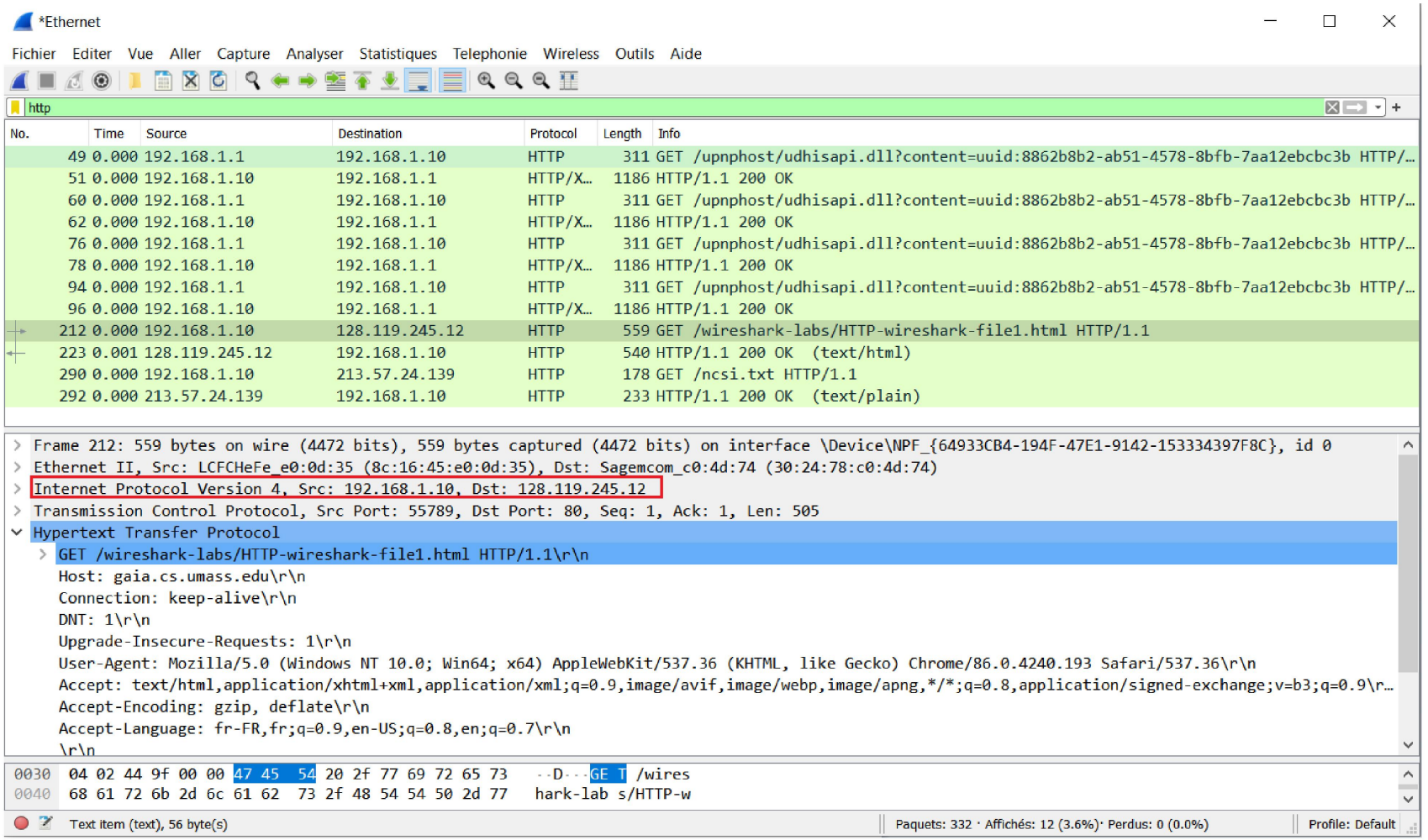
1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

Answer: HTTP 1.1



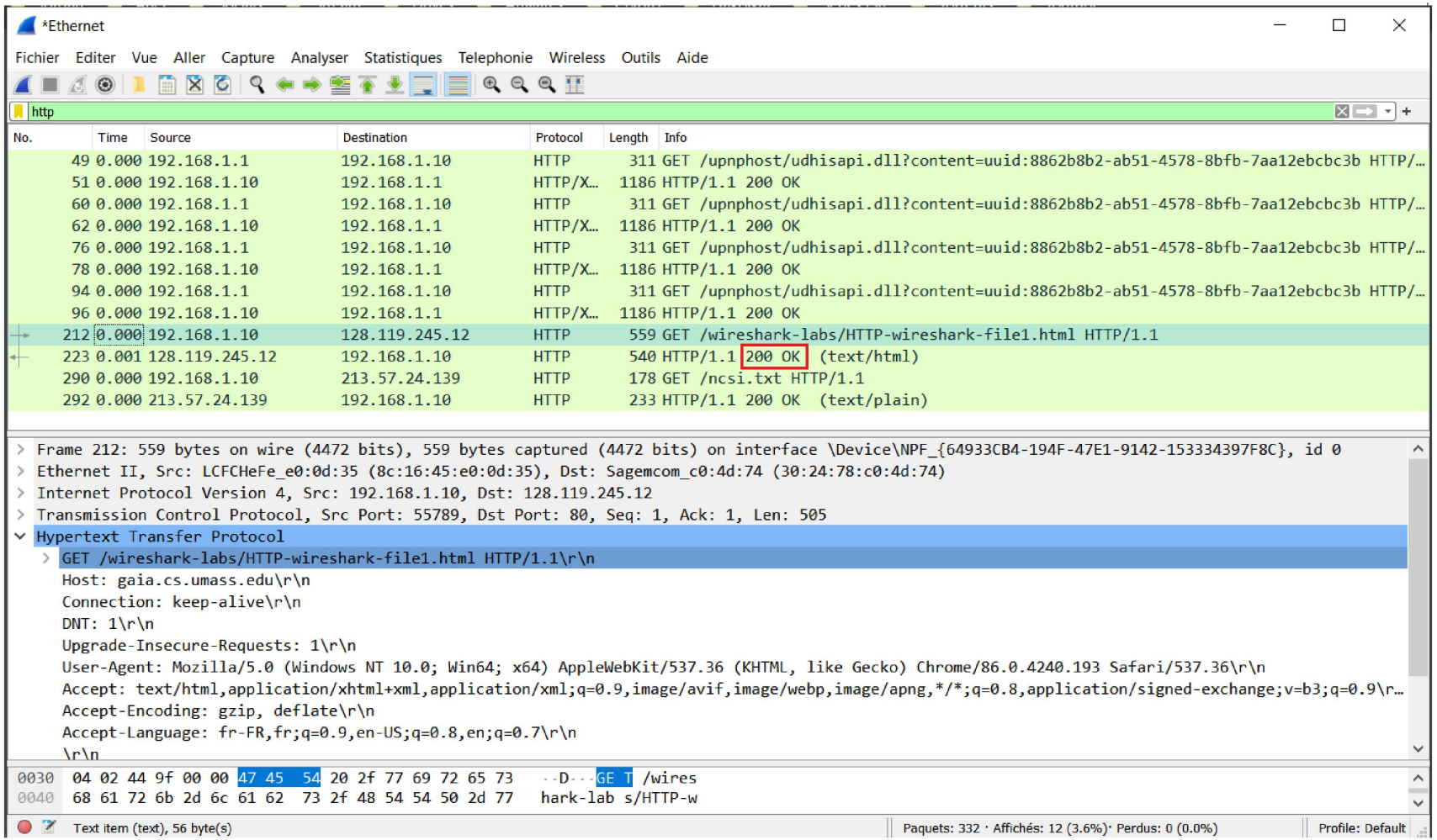
2. What languages (if any) does your browser indicate that it can accept to the server?

Answer: fr-FR (FR French) and en-US (US English)



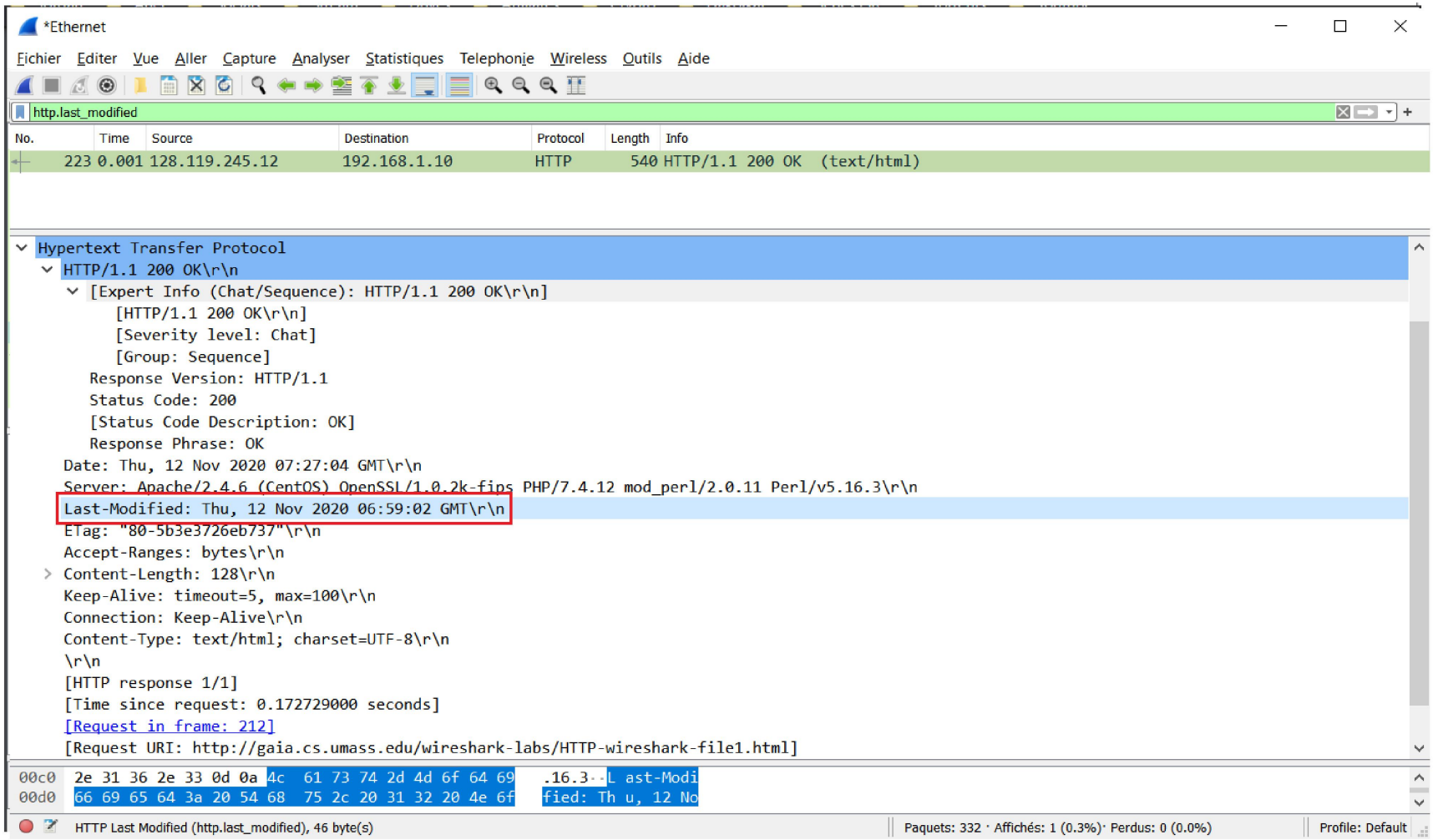
3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

Answer: -My IP is 192.168.1.10 and gaia.cs.umass.edu server's IP is 128.119.245.12



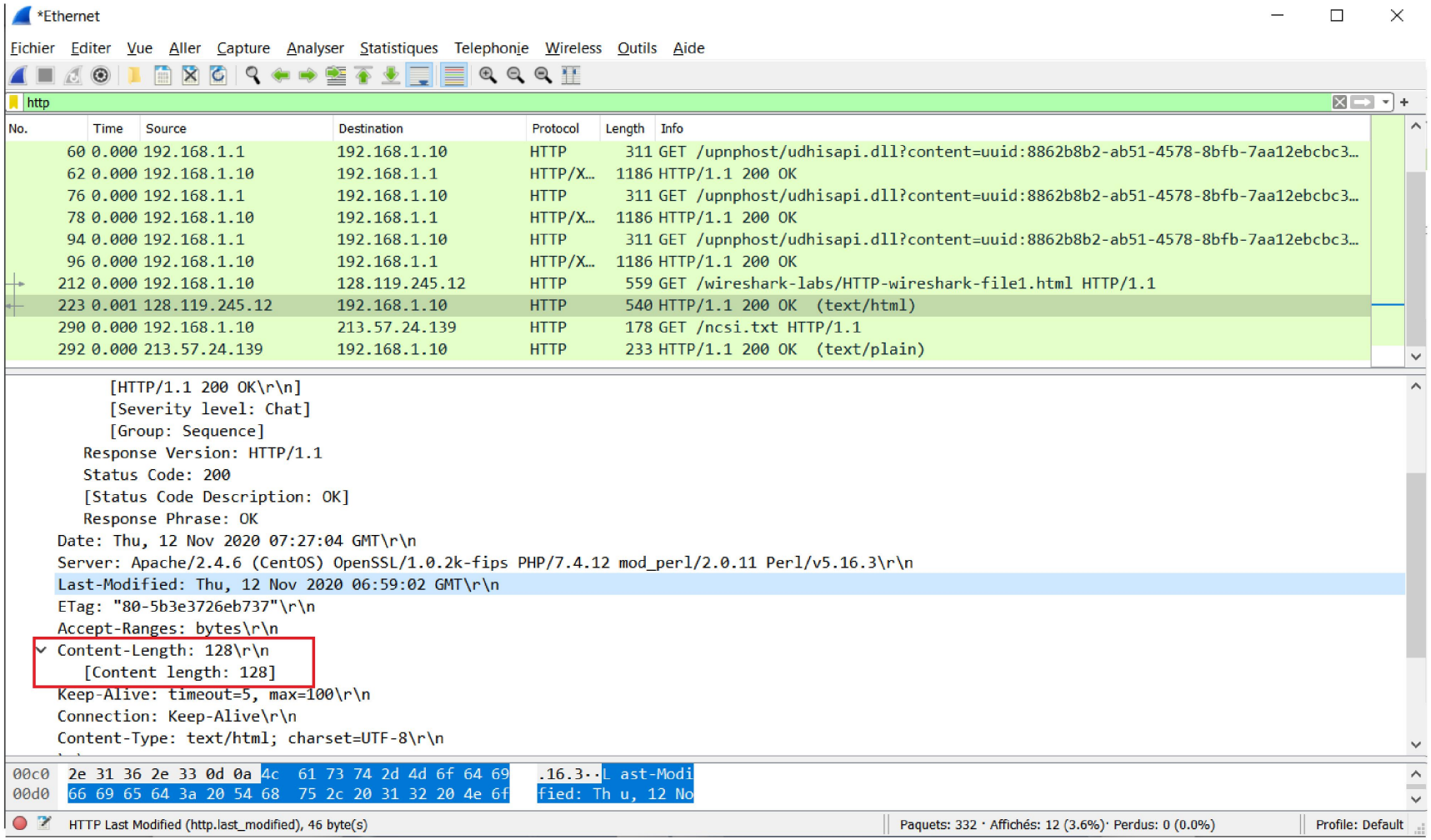
4. What is the status code returned from the server to your browser?

Answer: 200 OK



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

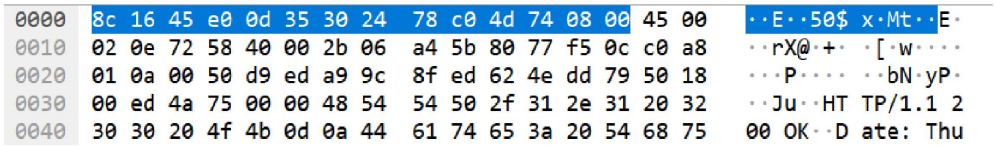
Answer : Using "http.last_modified" filter we can see that the last modified was on Thu, 12 Nov 2020 at 06:59:02 GMT



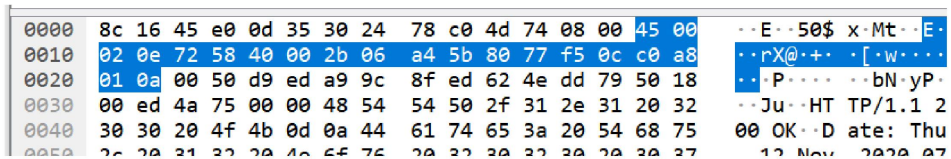
6. How many bytes of content are being returned to your browser?

Answer: 128 bytes

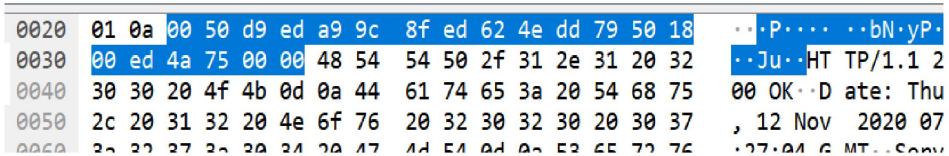
Ethernet :



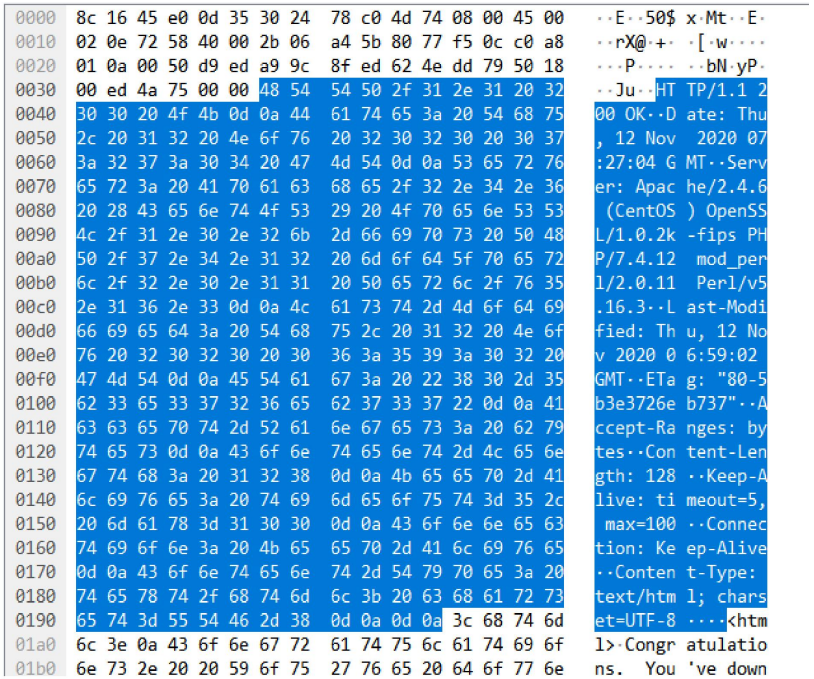
Internet:



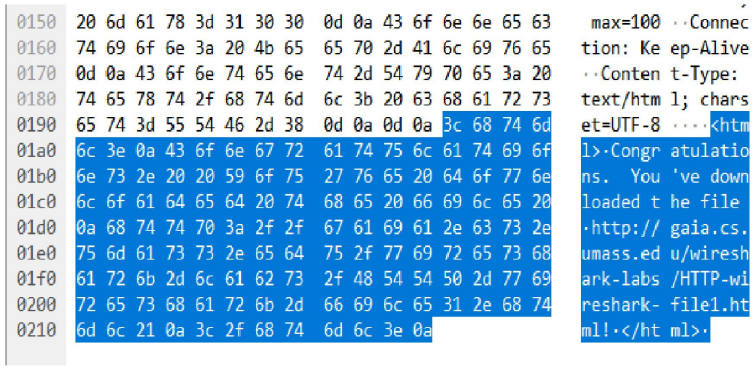
Transmission:



HTTP:



Application:

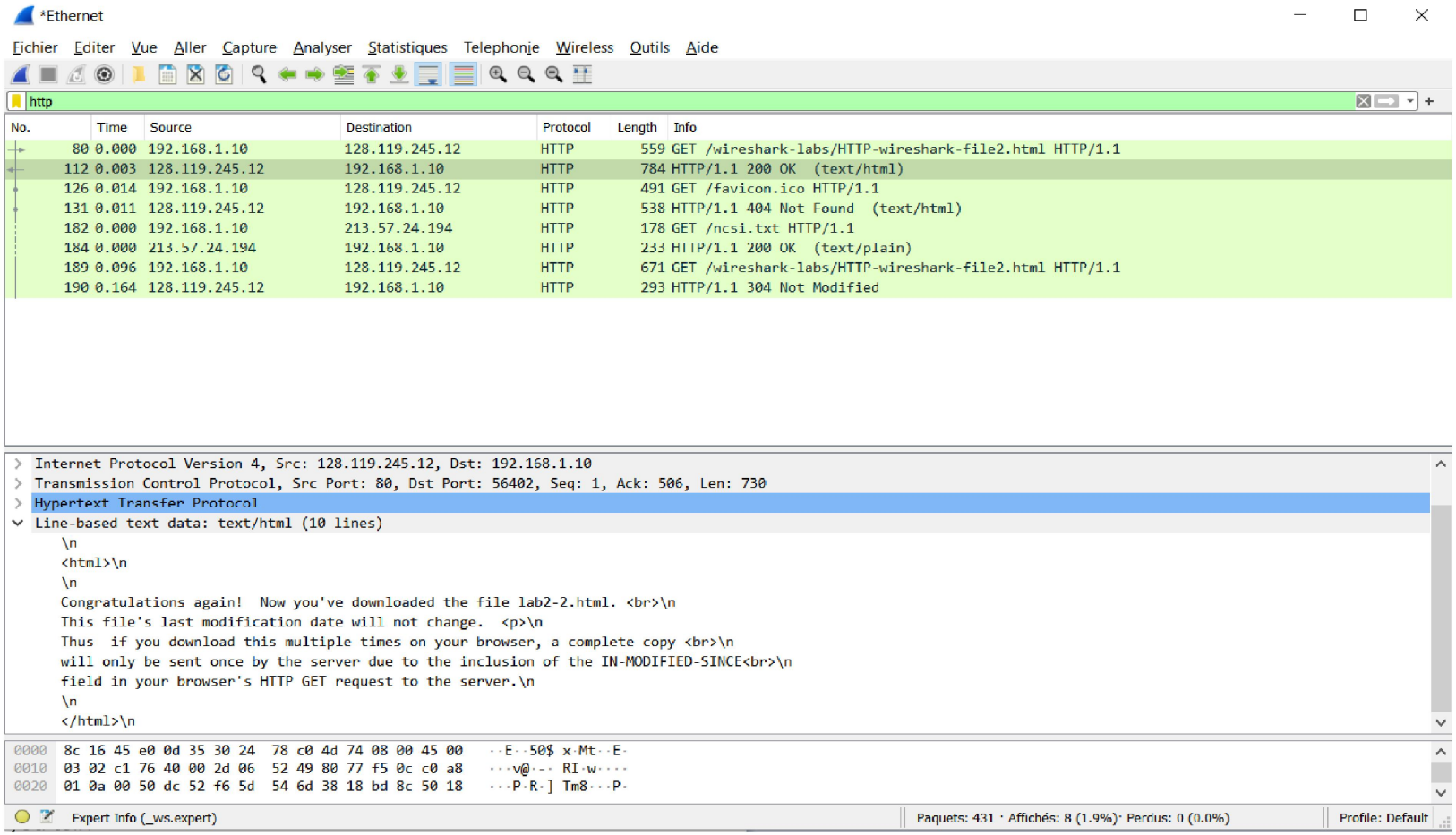


7. By inspecting the raw data in the packet content window, do you see any headers
within the data that are not displayed in the packet-listing window? If so, name one.

Answer: No, everything appears on the packet-listing window (everything is covered)

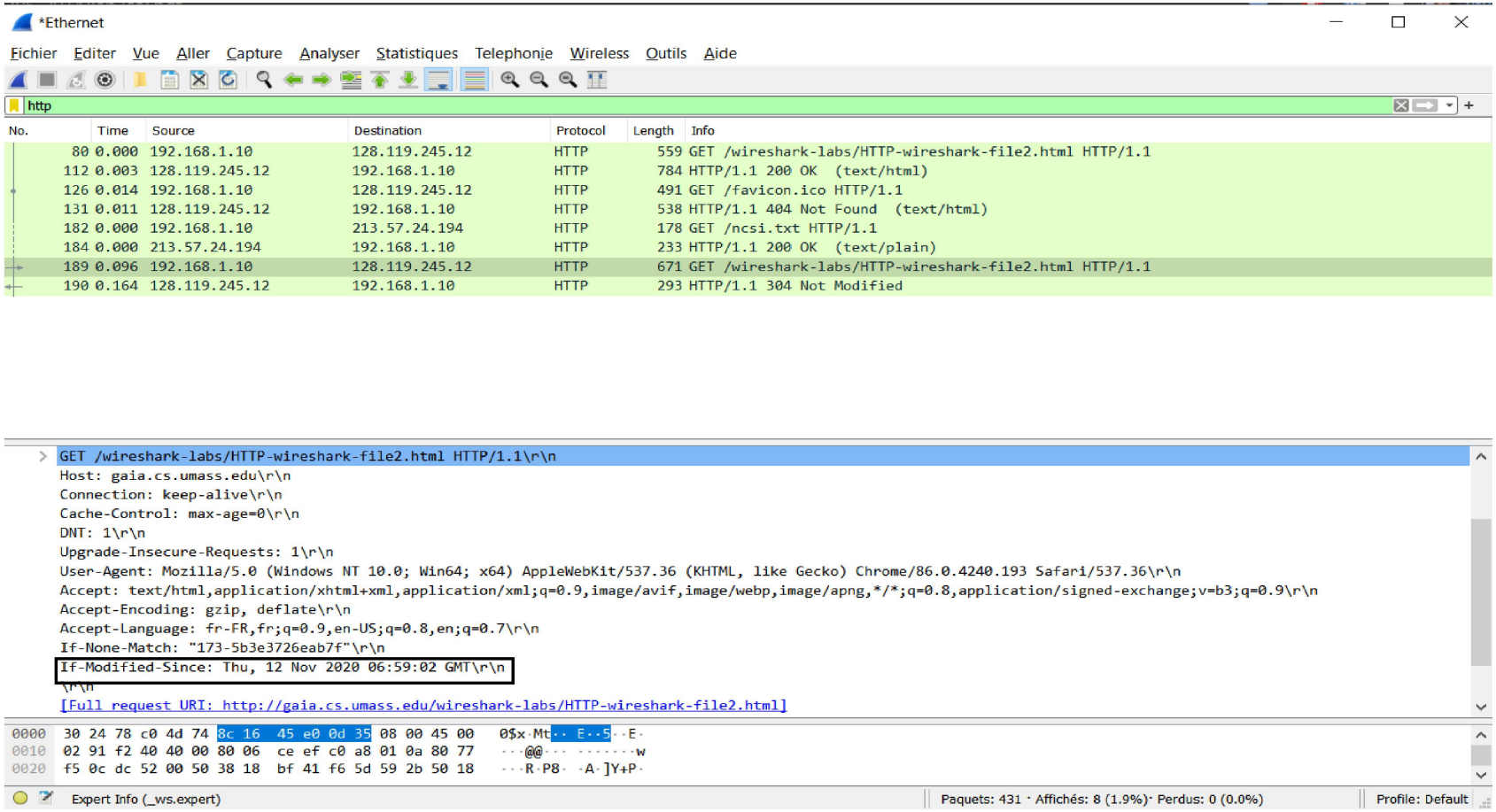
8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

Answer: No



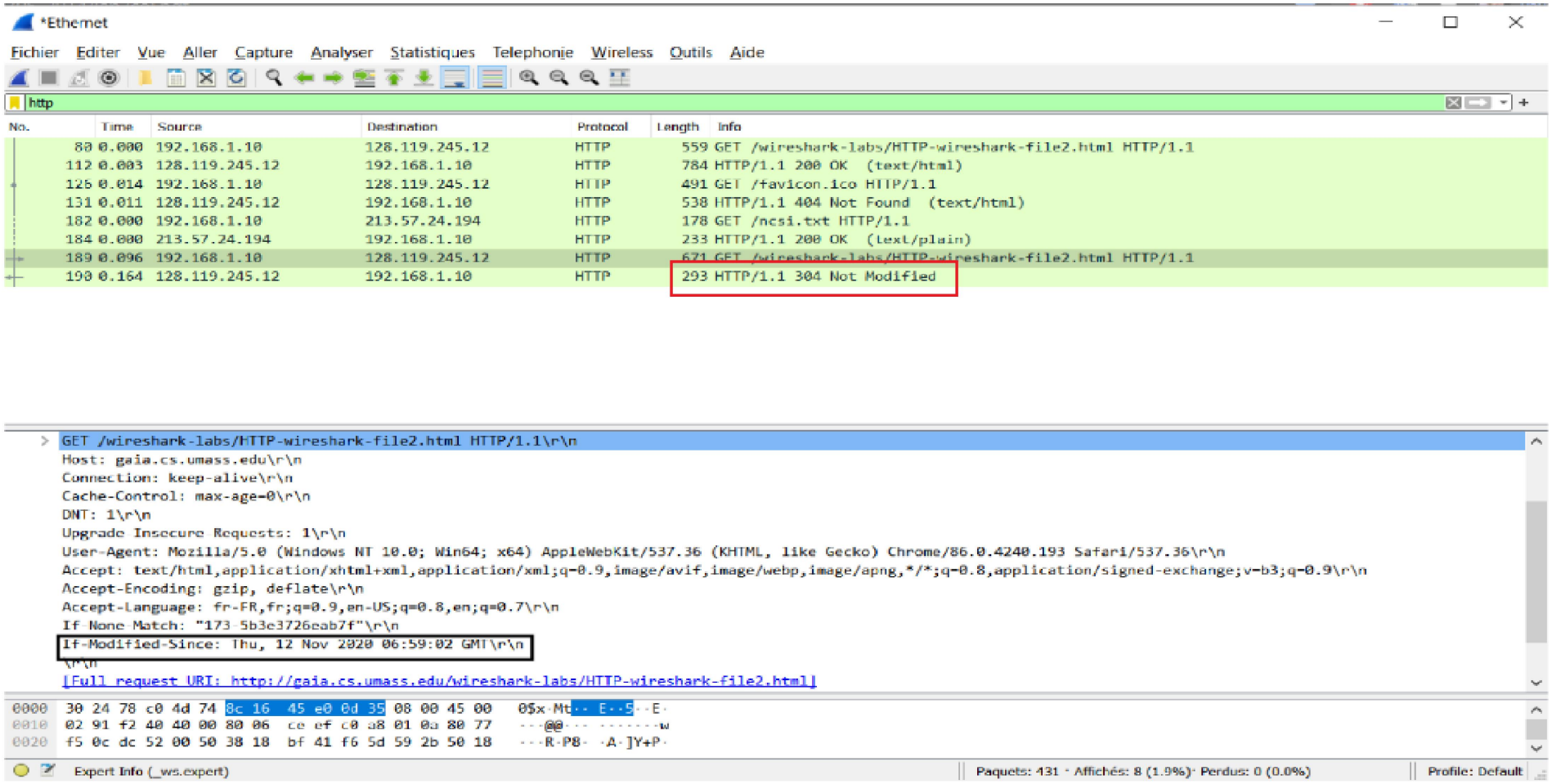
9. Inspect the contents of the server response. Did the server explicitly return the
contents of the file? How can you tell?

Answer: Yes it did. We can tell by reading the file on the Line-based text data protocol



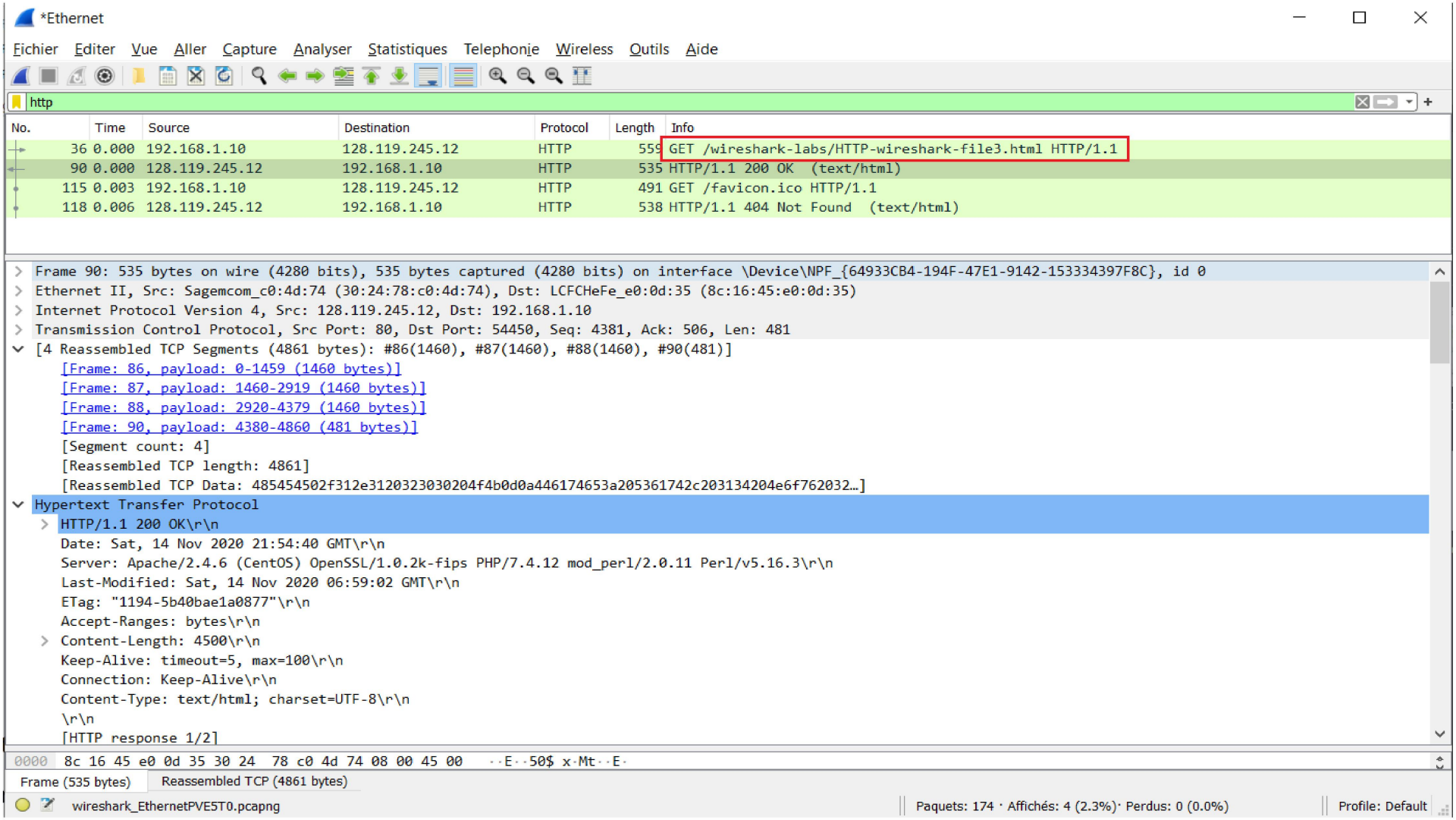
10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

Answer: Yes. It says: IF-MODIFIED-SINCE: Thu, 12 Nov 2020 06:59:02 GMT



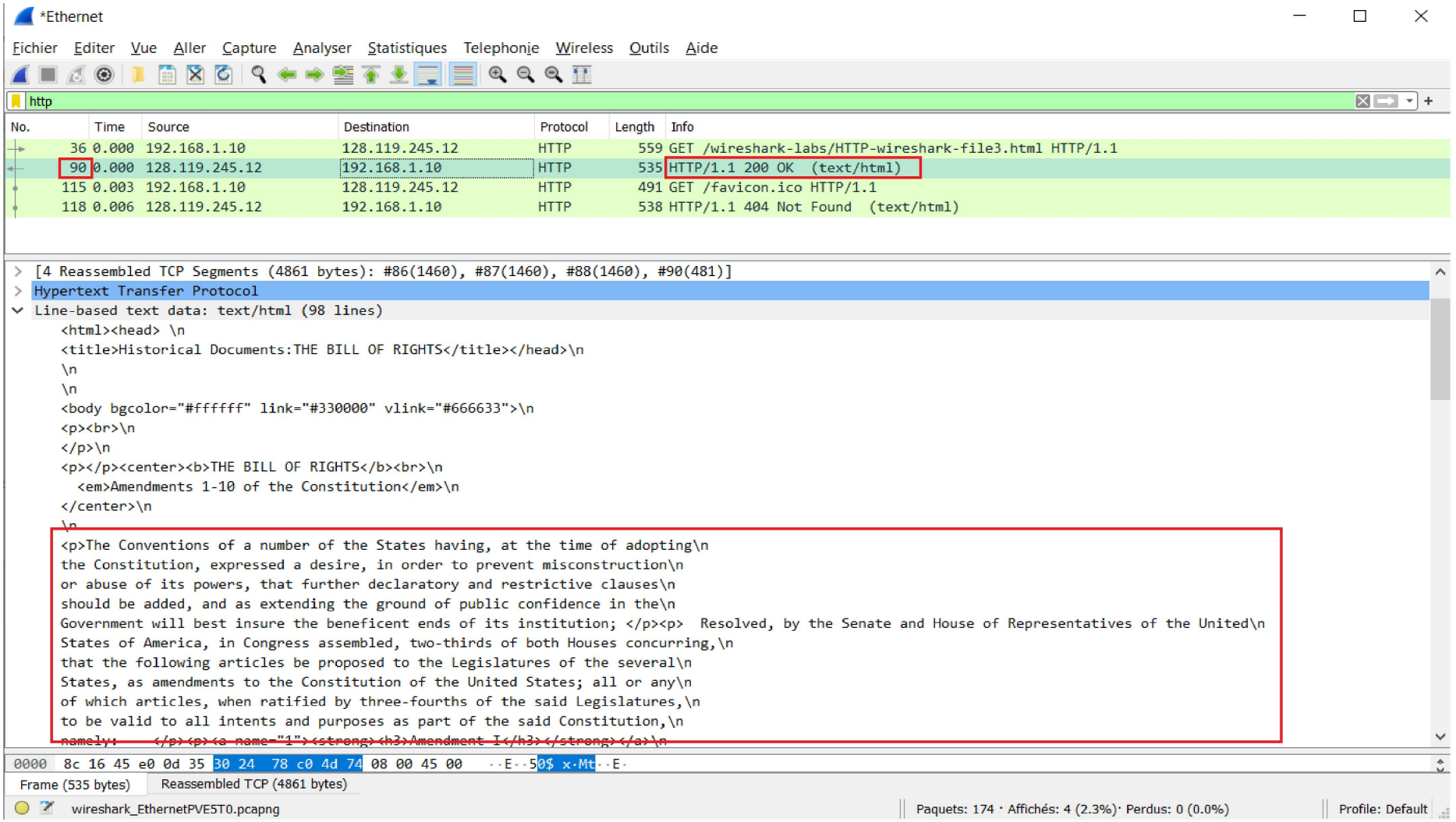
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

Answer: The response from the server is HTTP/1.1 304 Not Modied Response.
The server didn't explicitly returned the contents of the file since it already was stored in cache. It means our web browser (Chrome) performed an object caching and
thus performed a conditional GET, which resulted in finding the object already stored in cache.



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?

Answer: Ignoring the favicon the browser sent only one request. The packet containing the GET message for the Bill or Rights is packet 36

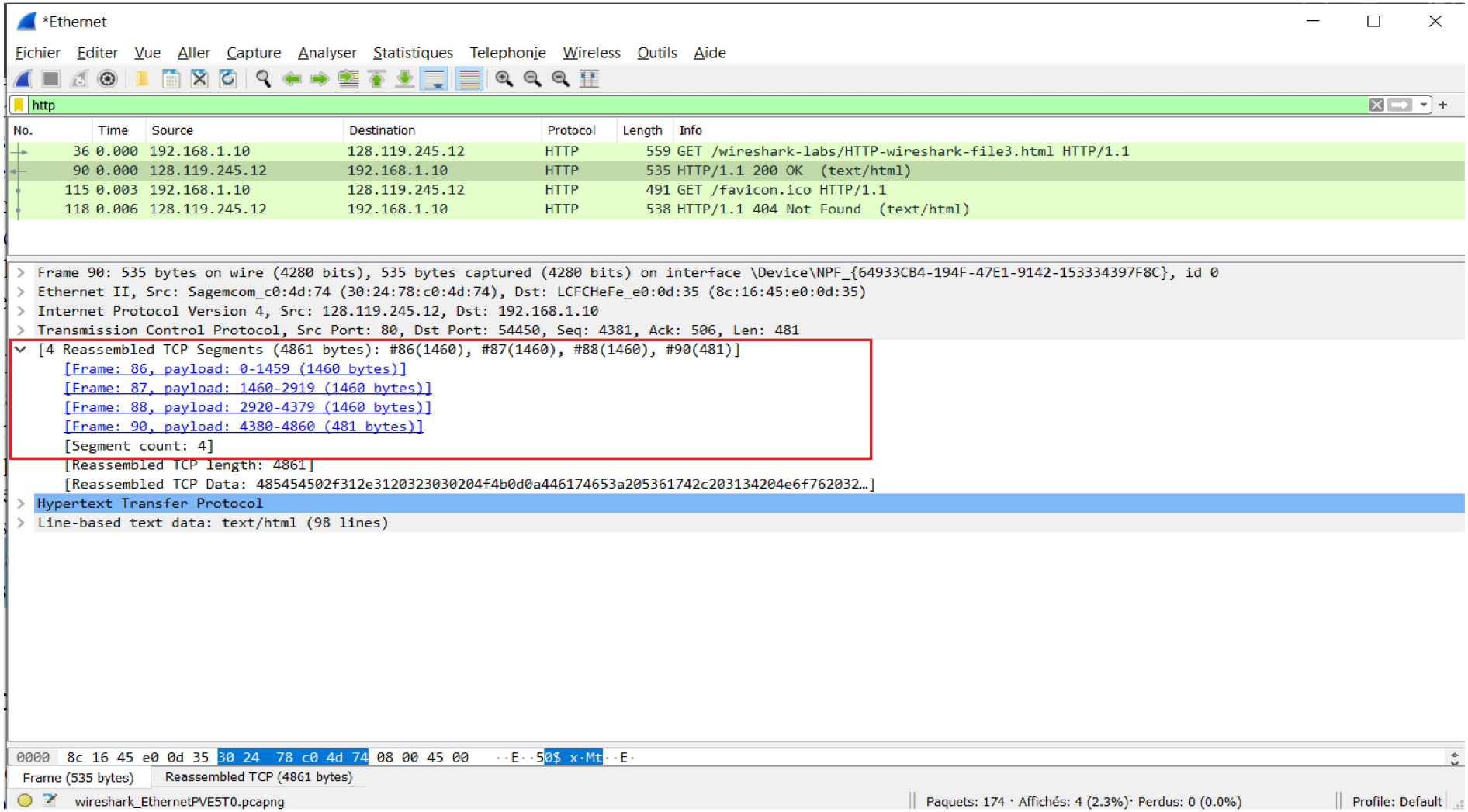


13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

Answer: Packet 90

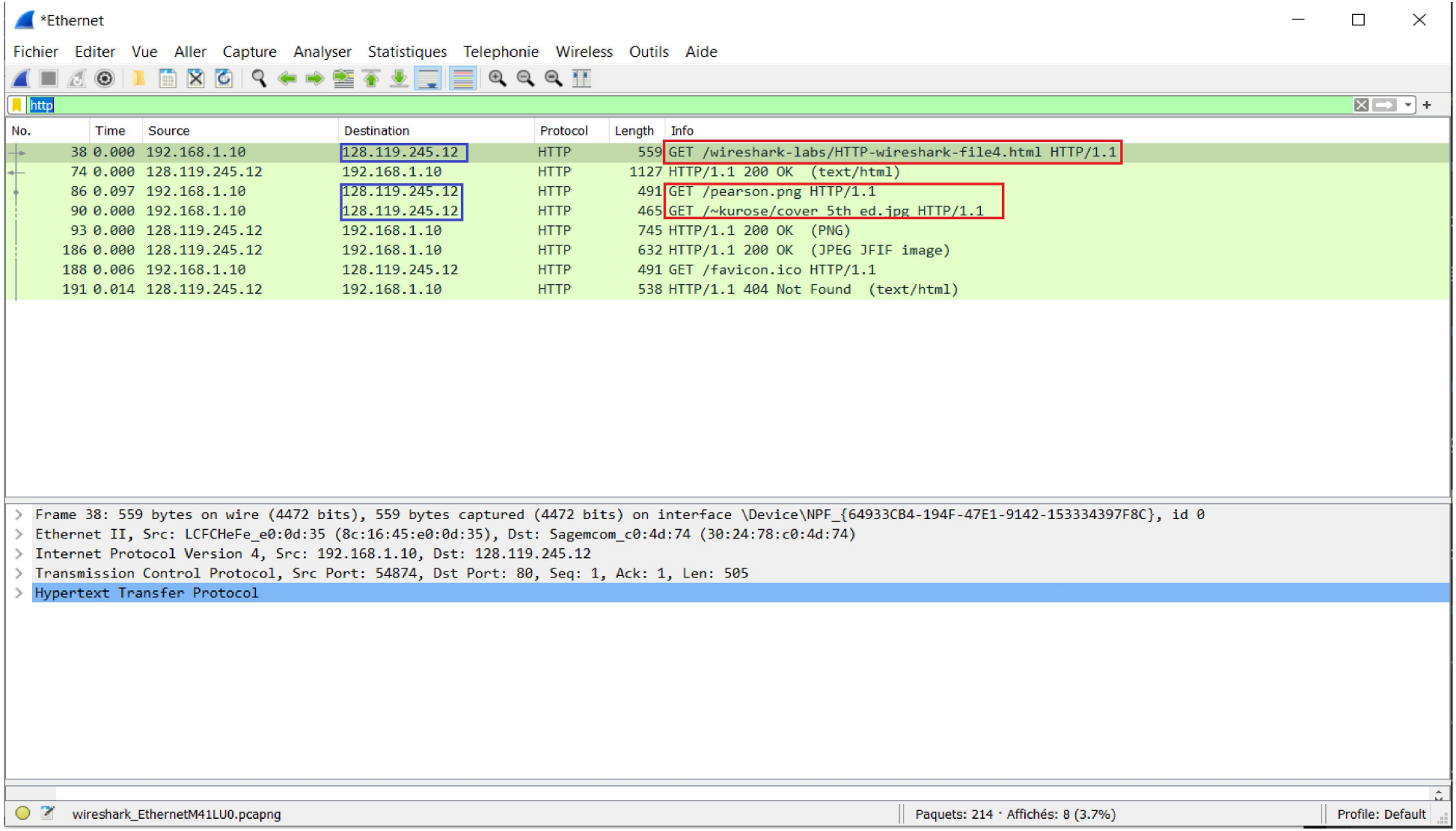
14. What is the status code and phrase in the response?

Answer: HTTP/1.1 200 OK (text/html)



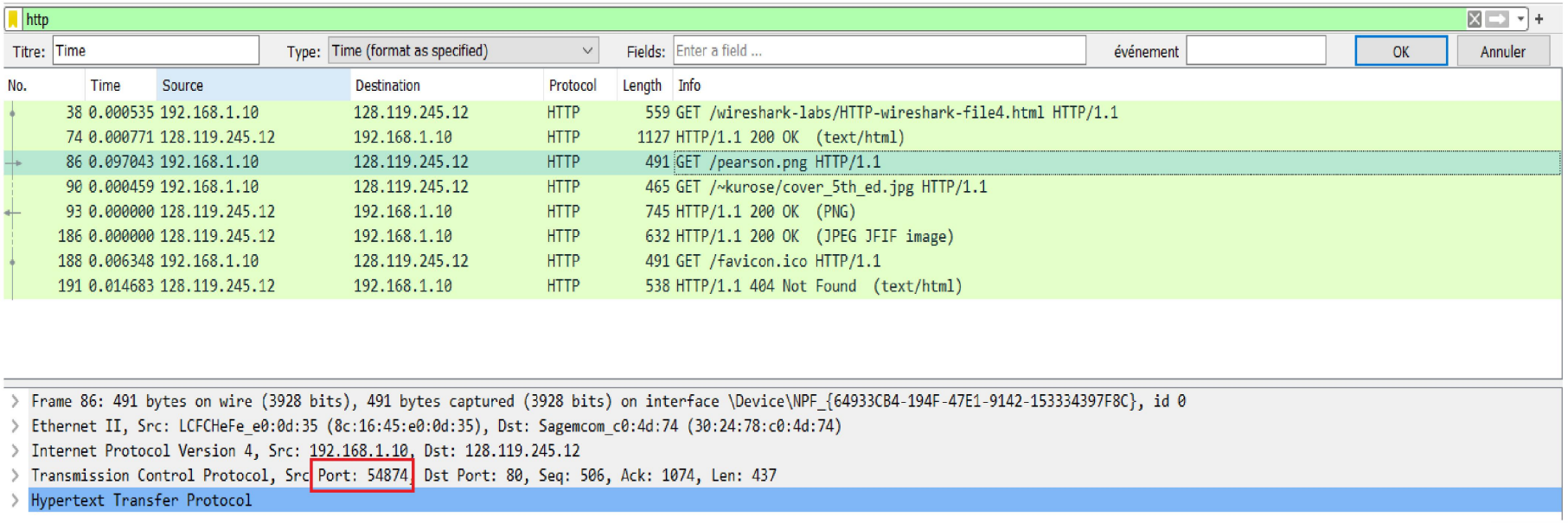
15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

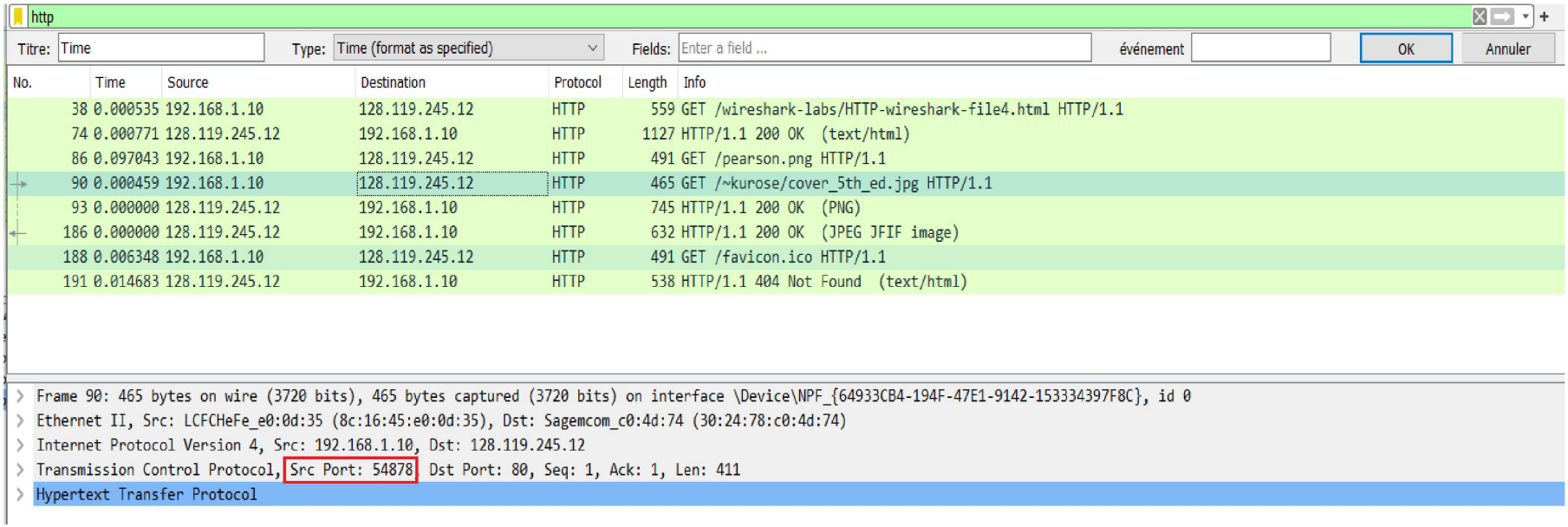
Answer: 4 segments



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

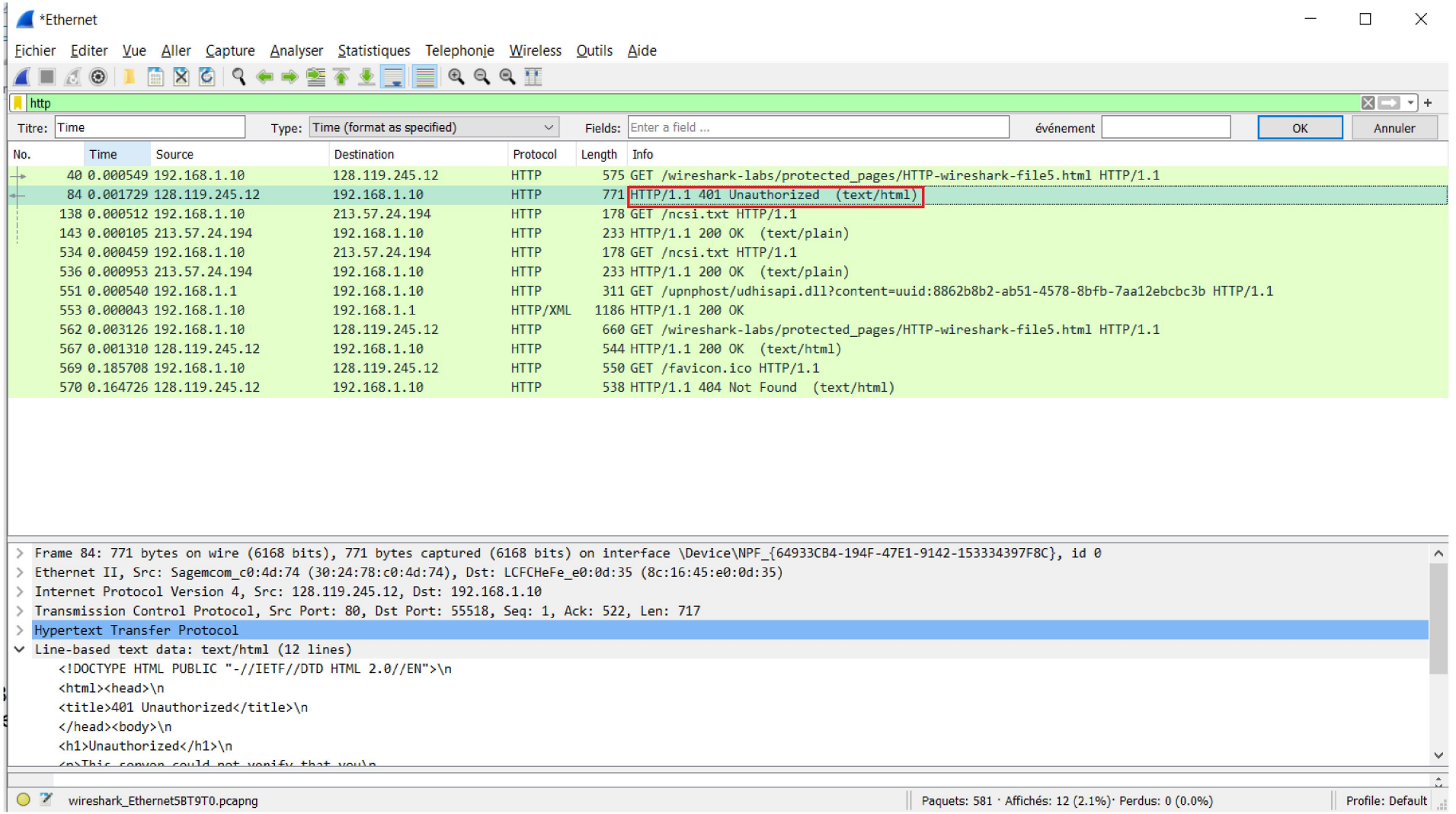
Answer: Ignoring the favicon, the browser sent 3 HTTP GET requests (in red)
Internet addresses are in blue.





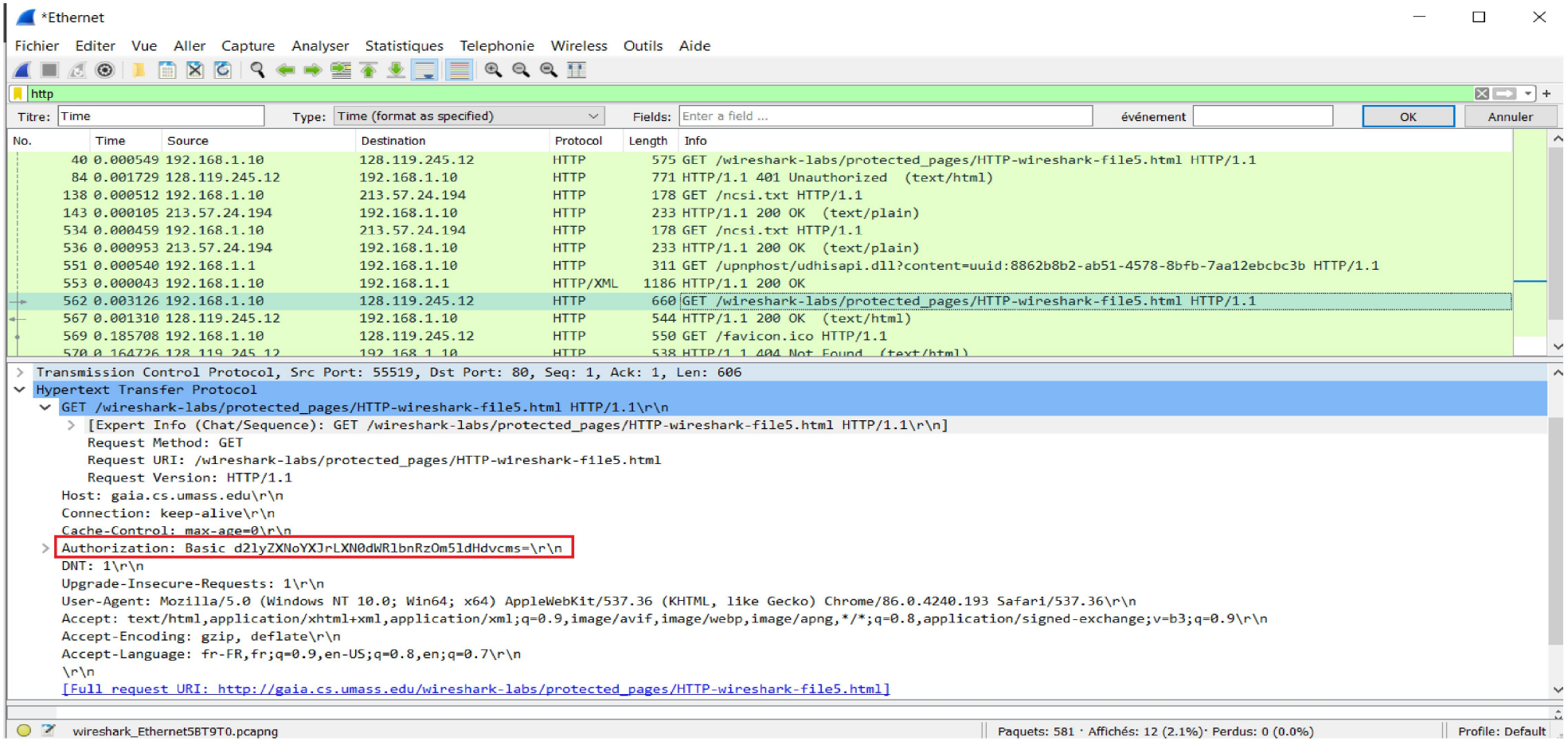
17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

Answer: : By checking the TCP ports(54874 and 54878) we can see that the 2 images were transmitted over two different TCP connections. Therefore they were downloaded serially.



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

Answer: HTTP/1 401 Unauthorized (text/html)



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

Answer: Authorization : Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=

(wireshark-students:network in Base64 encryption)