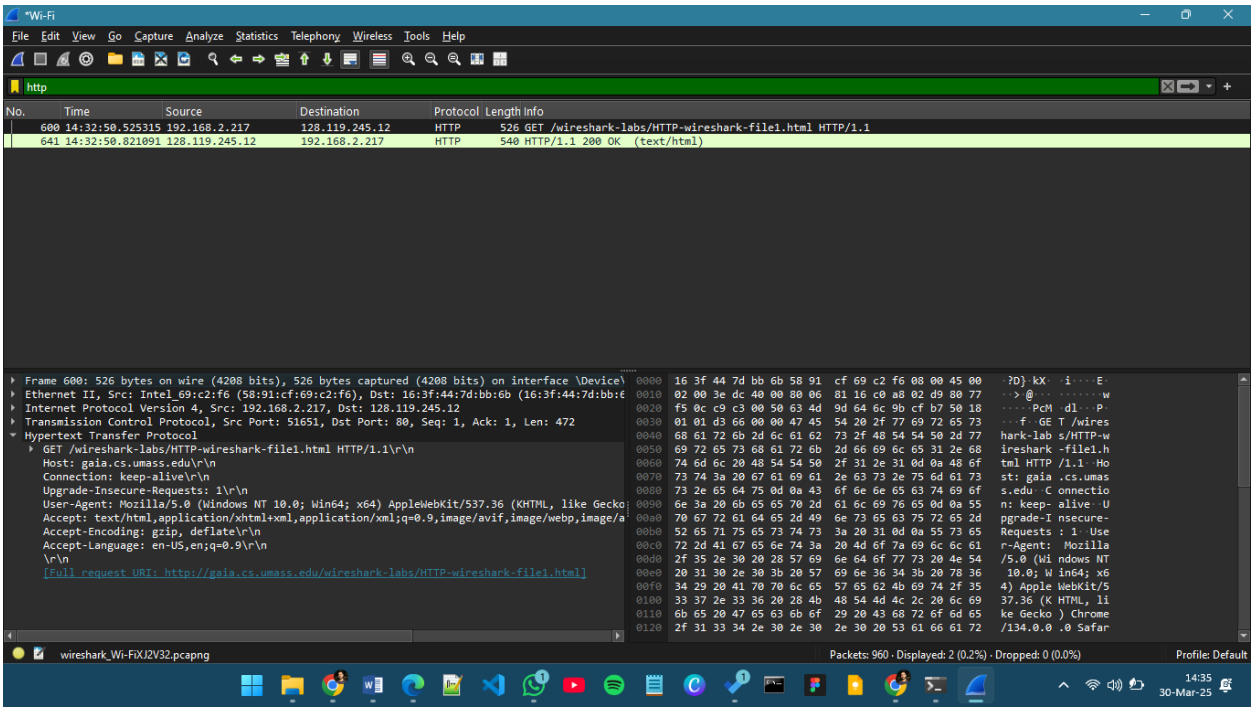
Wireshark Task 2

Part 1:



Questions:

1. **Is your browser running HTTP version 1.0, 1.1, or 2? What version of HTTP is the server running?**
   1.1

2. **What languages (if any) does your browser indicate that it can accept to the server?**
   Accept-Language: en-us,en;q=0.9

3. **What is the IP address of your computer? What is the IP address of the gaia.cs.umass.edu server?**
   My Computer's IP Address: 192.168.2.217
   Gaia.cs.umass.edu Server's IP Address: 128.119.245.12

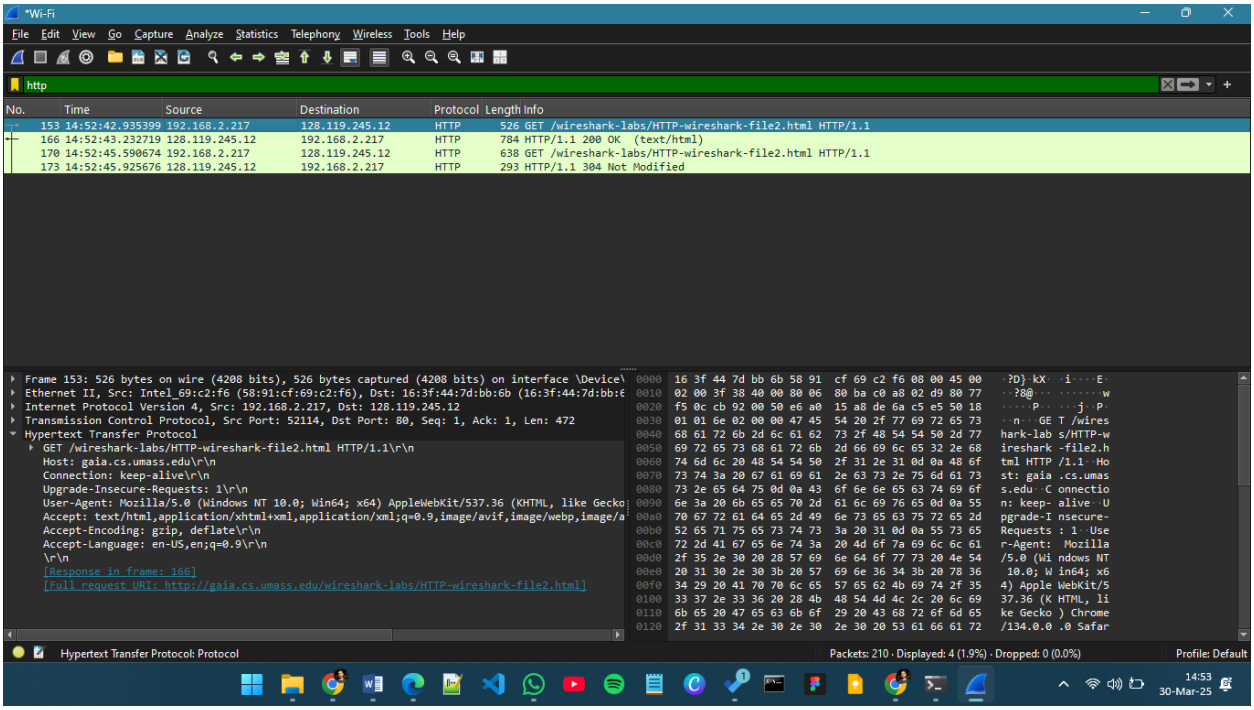
4. **What is the status code returned from the server to your browser?**
   200 OK, which indicates a successful request.

5. **When was the HTML file that you are retrieving last modified at the server?**
   Sun, 30 Mar 2025 05:59:01 GMT

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

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.**
   Date

Part 2



Questions:

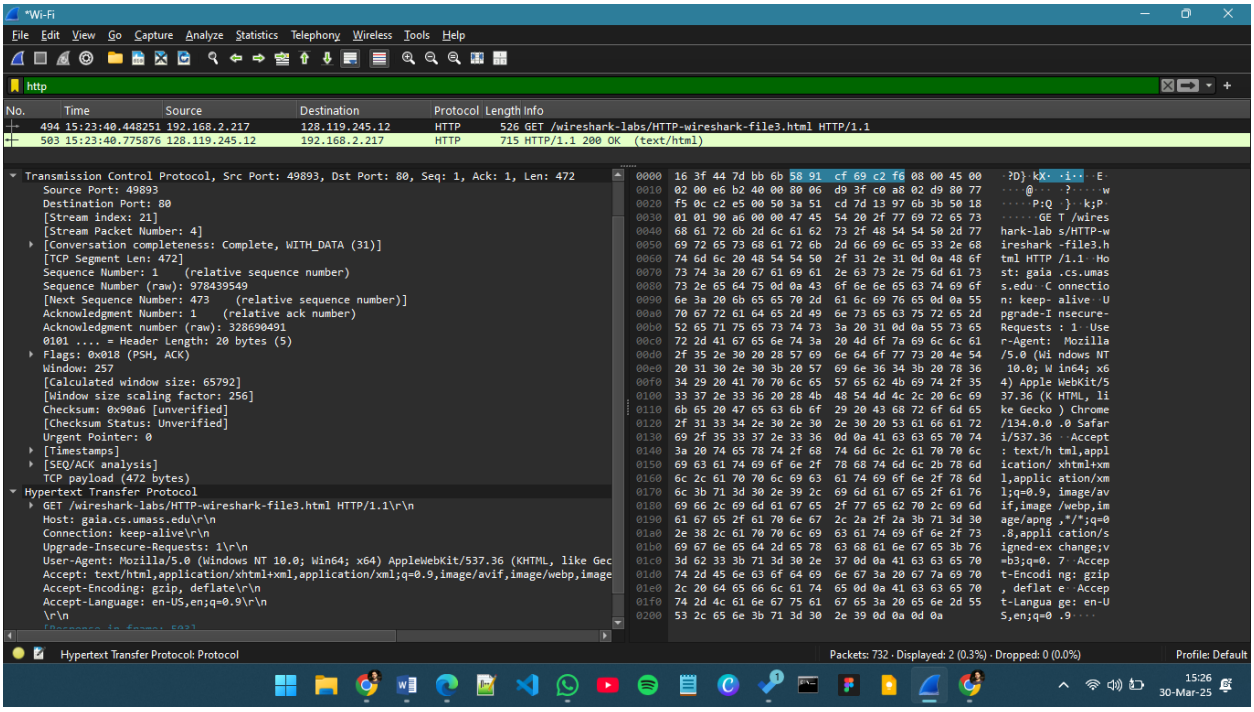
8. **Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF MODIFIED-SINCE" line in the HTTP GET?**
   No

9. **Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?**
   Yes, because the status code is followed by the return type, which says text/html

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 GET2? If so, what information follows the "IF MODIFIED-SINCE:" header?**
    Yes, it contains the same time and date of modification as previous request

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.**
    Status Code: 304 Not modified. There is not any return type that follows the status code, thus server is not explicitly returning the content.

Part 3



Questions:

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?**
    1, Packet 494

13. **Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?**
    Packet 503, Status code 200 OK (text/html)

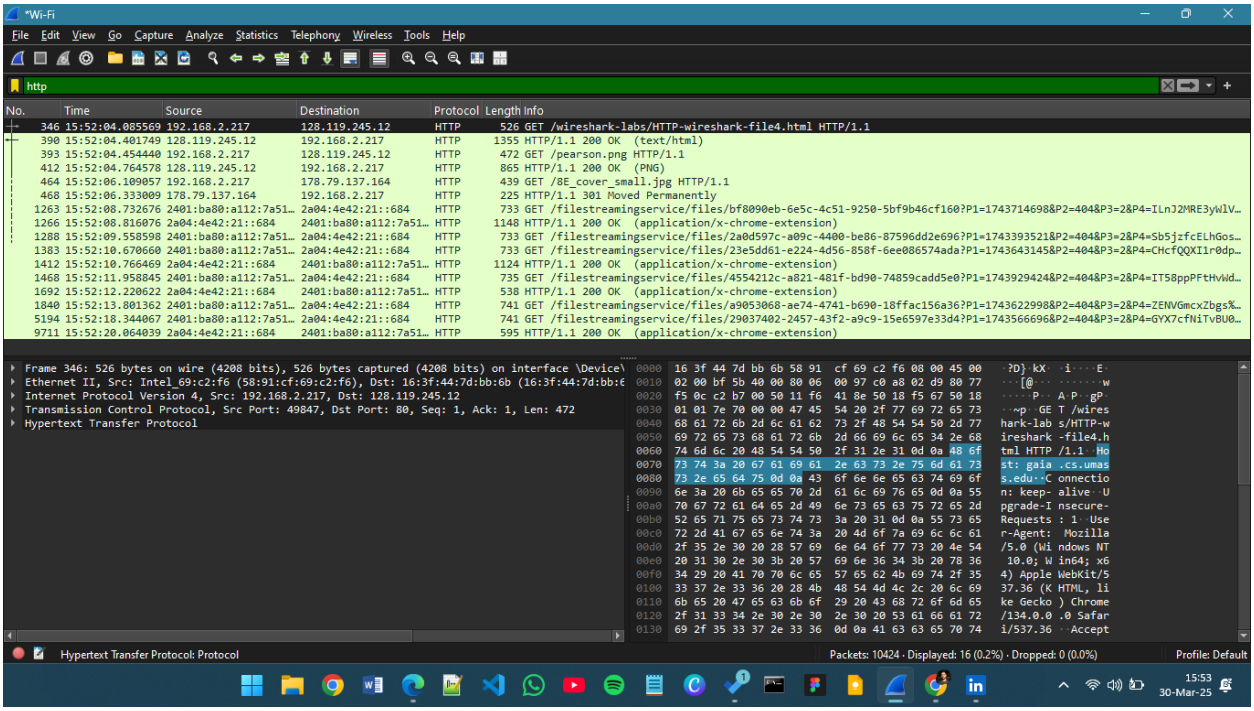
14. What is the status code and phrase in the response?

Status code 200 OK

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

3

Part 4



Questions:

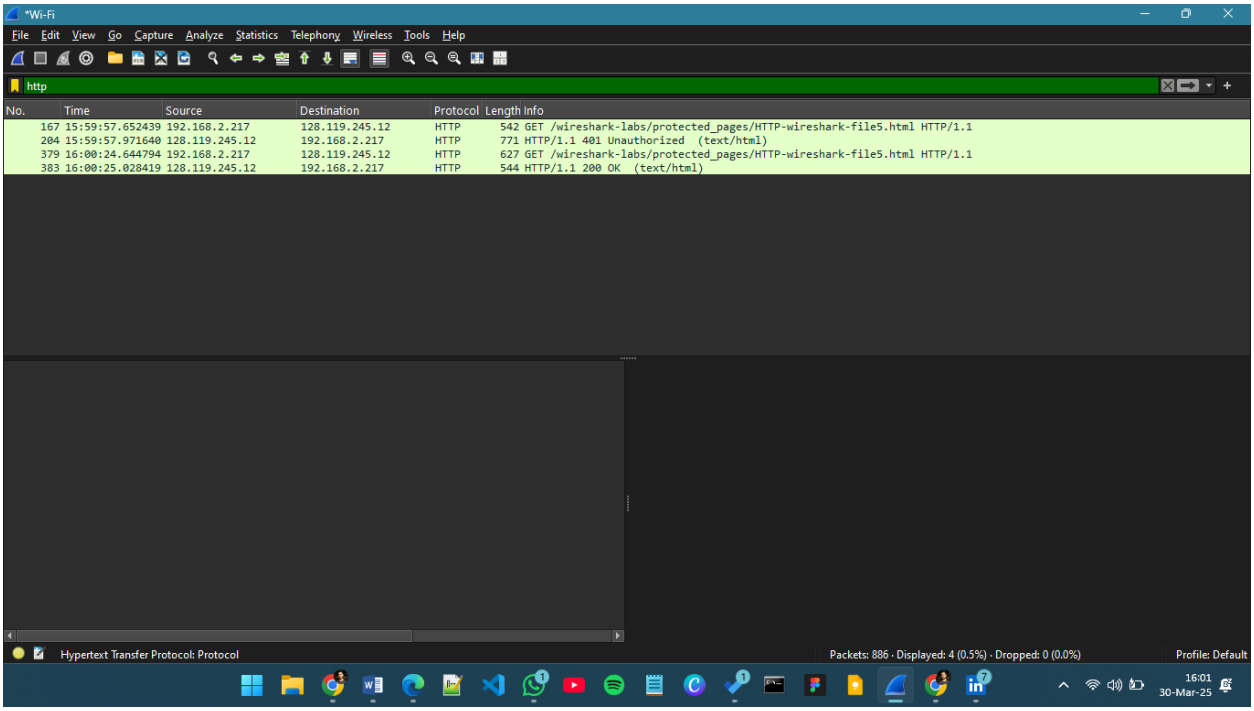
16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

8

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.

Serially, because the request timestamp of second image is after the first image request is completed.

Part 5



Questions:

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