Assignment

**Homework 4**

**P4**. Consider the following string of ASCII characters that were captured by Wireshark when the browser sent an HTTP GET message (i.e., this is the actual content of an HTTP GET message). The characters are carriage return and line-feed characters (that is, the italized character string in the text below represents the single carriage-return character that was contained at that point in the HTTP header). Answer the following questions, indicating where in the HTTP GET message below you find the answer.

GET /cs453/index.html HTTP/1.1Host: gai a.cs.umass.eduUser-Agent: Mozilla/5.0 ( Windows;U; Windows NT 5.1; en-US; rv:1.7.2) Gec ko/20040804 Netscape/7.2 (ax) Accept:ex t/xml, application/xml, application/xhtml+xml, text /html;q=0.9, text/plain;q=0.8,image/png,\*/\*;q=0.5 M02\_KURO1557\_08\_SE\_C02.indd 168 12/02/20 4:08 PM PROBLEMS 169 Accept-Language: en-us,en;q=0.5AcceptEncoding: zip,deflateAccept-Charset: ISO -8859-1,utf-8;q=0.7,\*;q=0.7Keep-Alive: 300 Connection:keep-alive

a. What is the URL of the document requested by the browser?

- The URL of the document requested by the browser is “cs453/index.html”.

b. What version of HTTP is the browser running?

- The version of HTTP that the browser is running is HTTP/1.1.

c. Does the browser request a non-persistent or a persistent connection?

- The browser requests a persistent connection because “Connection: keep-alive”.

d. What is the IP address of the host on which the browser is running?

- No, the provided string doesn't contain the IP address

e. What type of browser initiates this message? Why is the browser type needed in an HTTP request message?

- The browser initiating this HTTP request message is Mozilla/5.0, which is common use with Firefox browser. There are several reasons why some browsers are using HTTP request message according to the following:

1) Content Negotiation: The server can use the information about the browser type to determine the appropriate content to send back.

2) Feature Detection: Servers may need to detect the capabilities of the browser to provide appropriate content or functionality. Different browsers support different features or standards, so this information can help tailor the response.

3) Logging and Analytics: Knowing the browser type helps in logging and analytics on the server side. Website owners can analyze the distribution of browsers accessing their site, which can inform decisions about website design and optimization.

4) Compatibility: It helps in ensuring compatibility with various browsers. By knowing the browser type, developers can ensure that the website or web application functions correctly across different browsers and versions.

**Lab 2 HTTP**

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

* HTTP 1.1

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

- The system has not told.

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

- My computer IP: 10.131.165.58

- Website IP: 128.119.245.12

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

- Status Code: 404

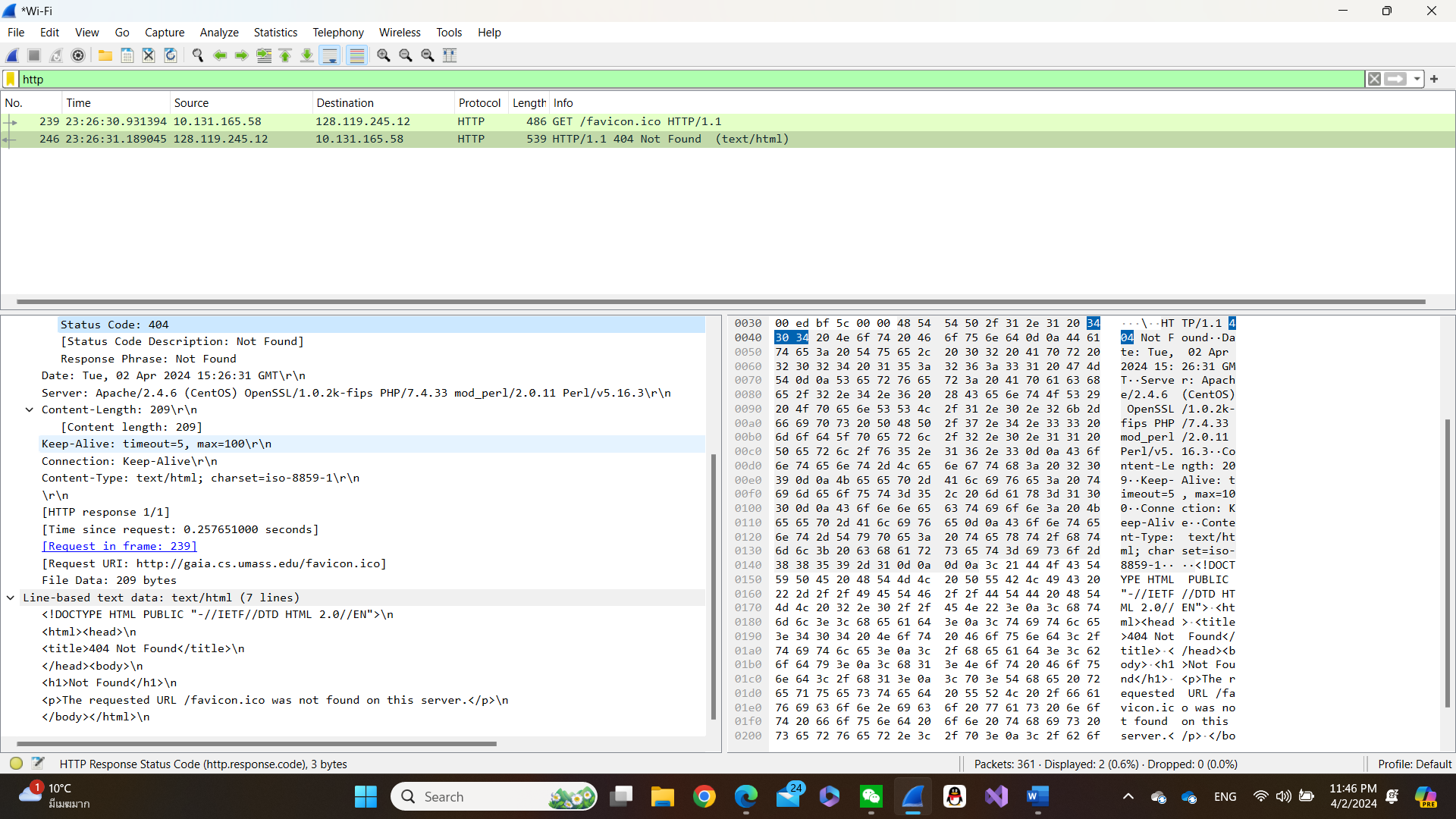
5. When was the HTML file that you are retrieving last modified at the server?

- Date: Tue, 02 Apr 2024 15:26:31 GMT\r\n

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

- File Data: 209 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.

- No, that's all

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?

- In the HTTP GET line I do not see “IF-MODIFIED-SINCE”.

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

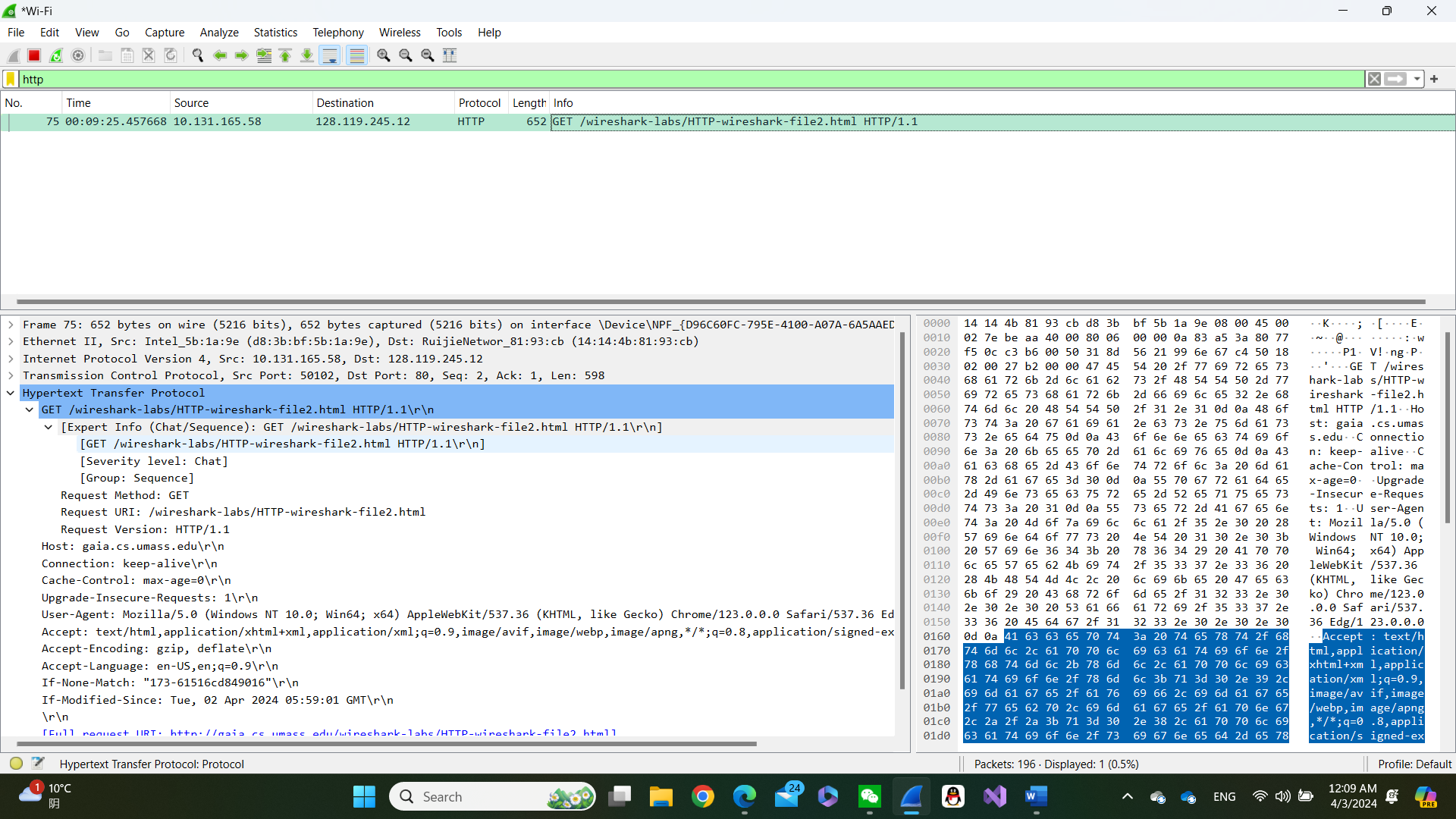
- The contents of the file in the response packet were discovered.

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?

- If-Modified-Since: Tue, 02 Apr 2024 05:59:01 GMT\r\n

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 that is, it has not changed, and the text has not been retransmitted, but the existing text in the cache is directly called. This offloads servers and increases efficiency.



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?

- I saw 1 GET methods and the trace number is 62.

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

- Packet number 638

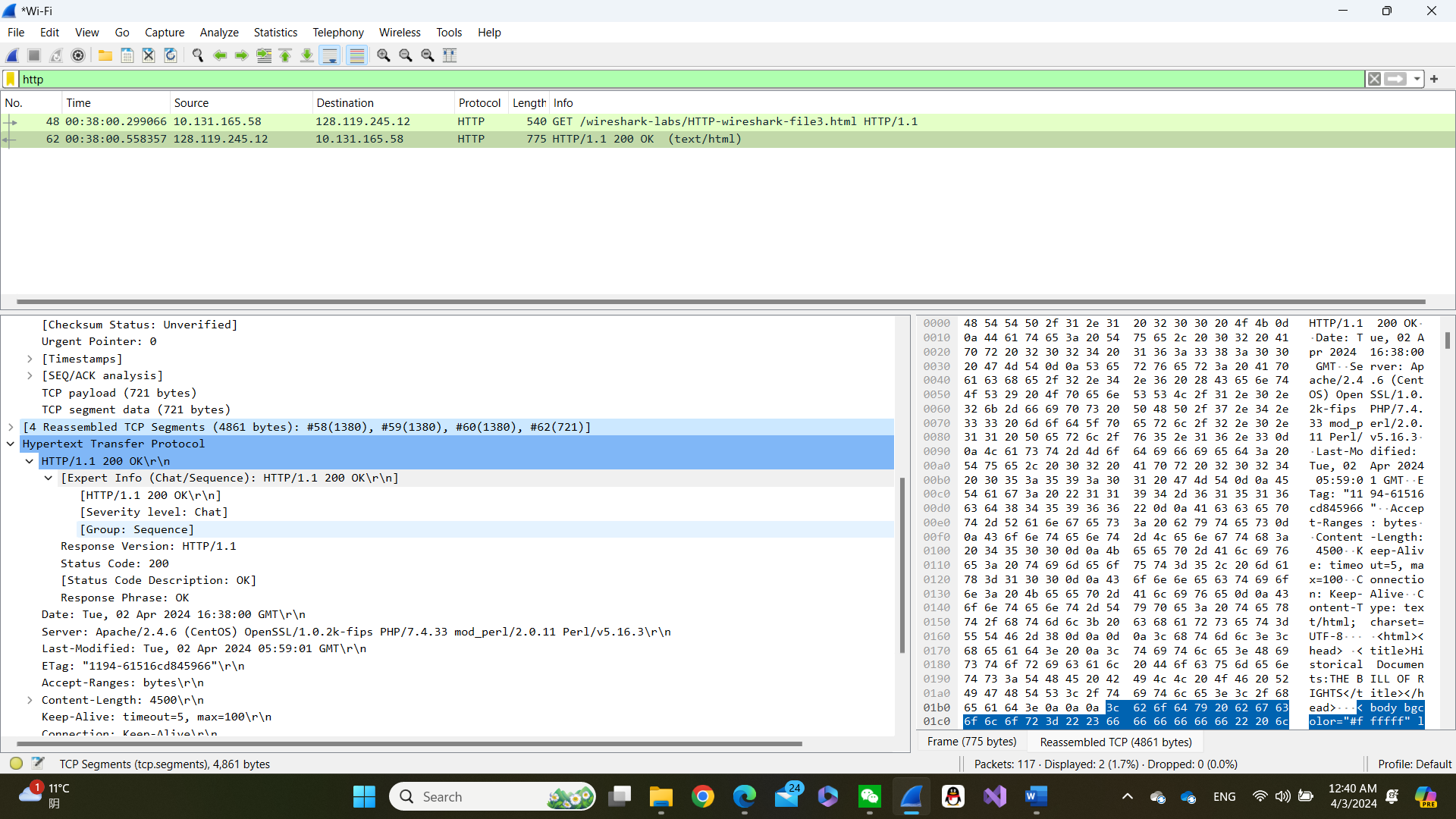
14. What is the status code and phrase in the response?

- Status Code: 200

- [Status Code Description: Not Modified]

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

- [4 Reassembled TCP Segments (4861 bytes): #58(1380), #59(1380), #60(1380), #62(721)]

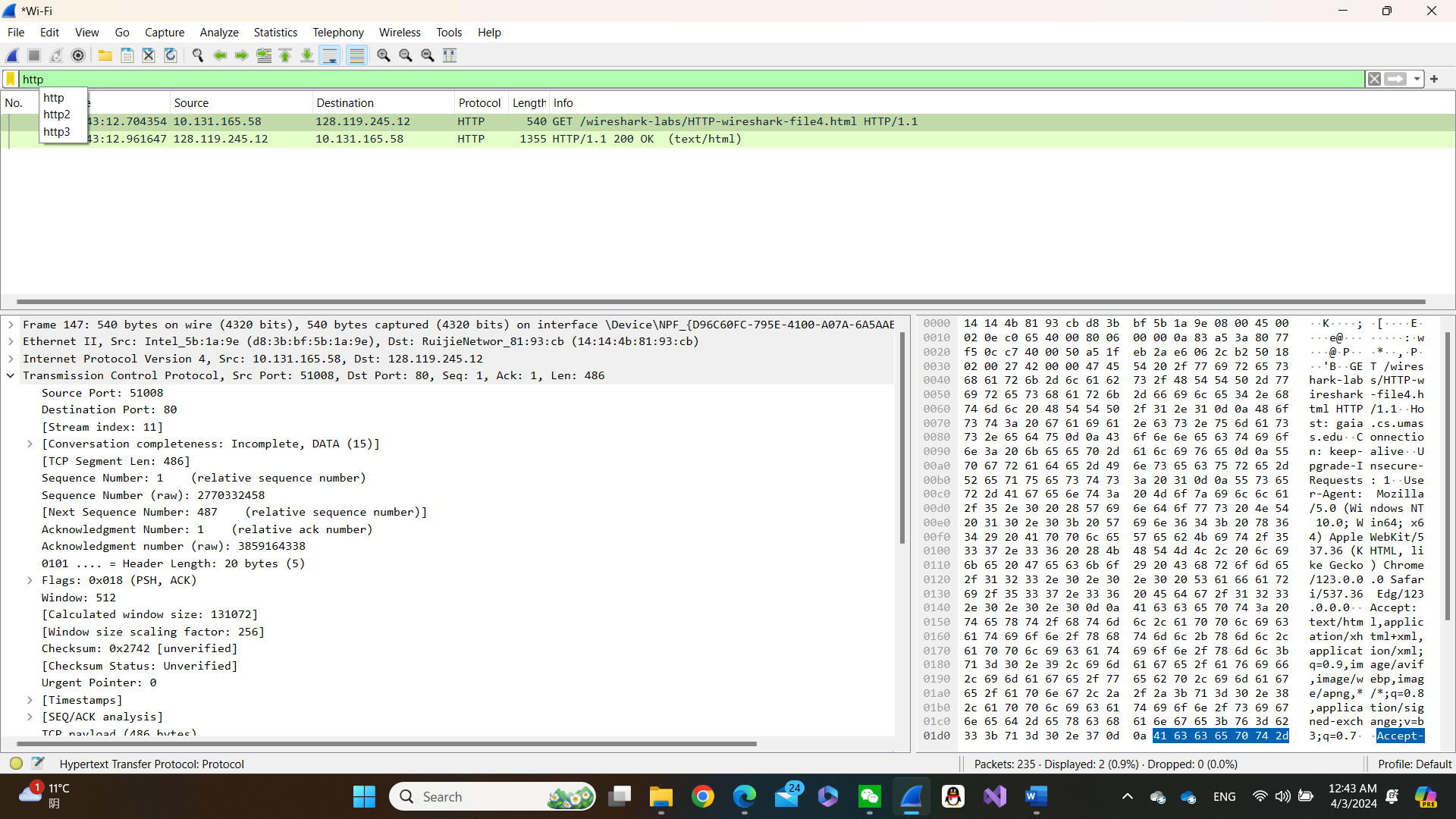


16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

- 1 GET requests

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.

- I'm not sure if this concurrency is really sent at the same time, but GET packets are sent at different times, so I think they should be sent sequential not parallel.

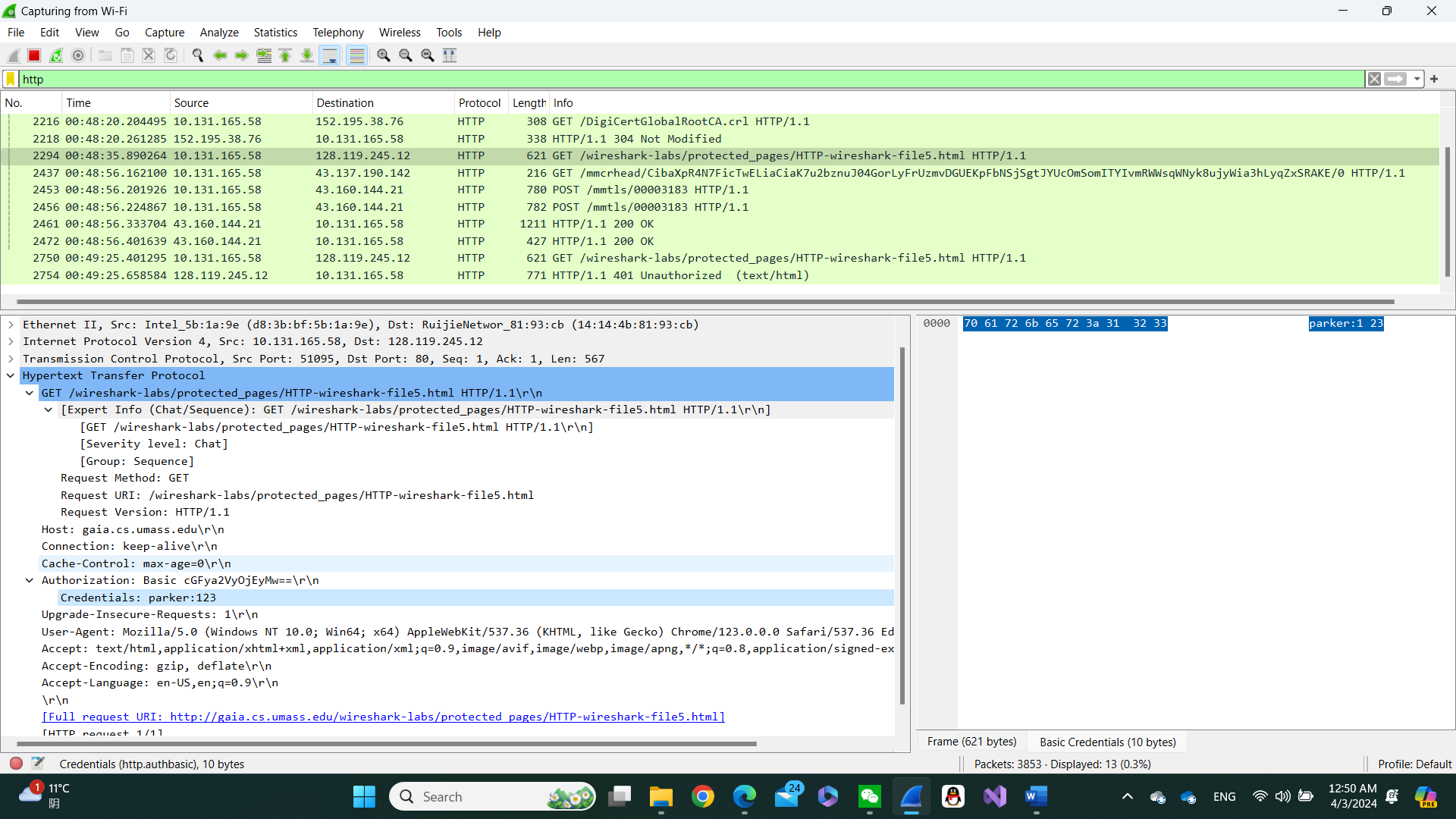


18. What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser?

- [HTTP/1.1 401 Unauthorized\r\n]

- [Severity level: Chat]

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

- Authorization: Basic cGFya2VyOjEyMw==\r\n

- Credentials: parker:123

**Homework 3**

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

* UDP, TCP, ARP

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark *View* pull down menu, then select Time *Display Format*, then select *Time-of-day*.)

- GET message: 21:33:44.066485

- HTTP OK: 21:33:44.070267

Time to send = 0.01 seconds

3. What is the Internet address of the cs.whu.edu.cn? What is the Internet address of your computer?

* Address of cs.whu.ed.cn = 202.114.64.221
* Address of my computer = 10.131.166.249

4. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select *Print* from the Wireshark *File* command menu, and select the “*Selected Packet Only”* and *“Print as displayed”* radial buttons, and then click OK.

