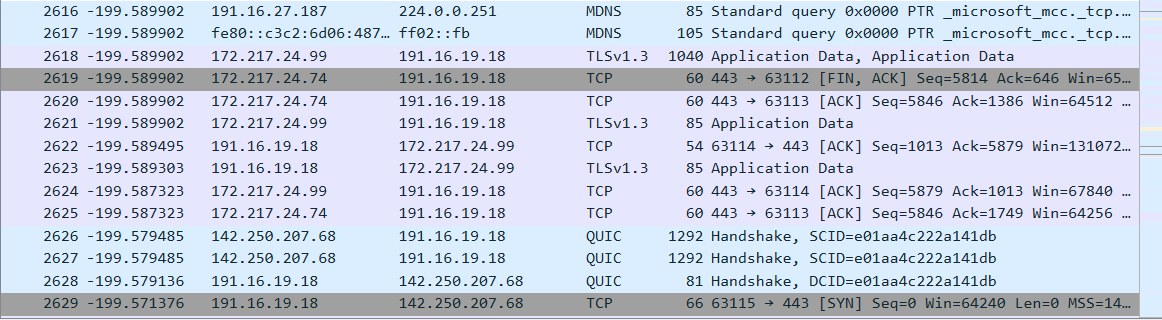
Name: Nguyen Minh Hieu

Class: CC01

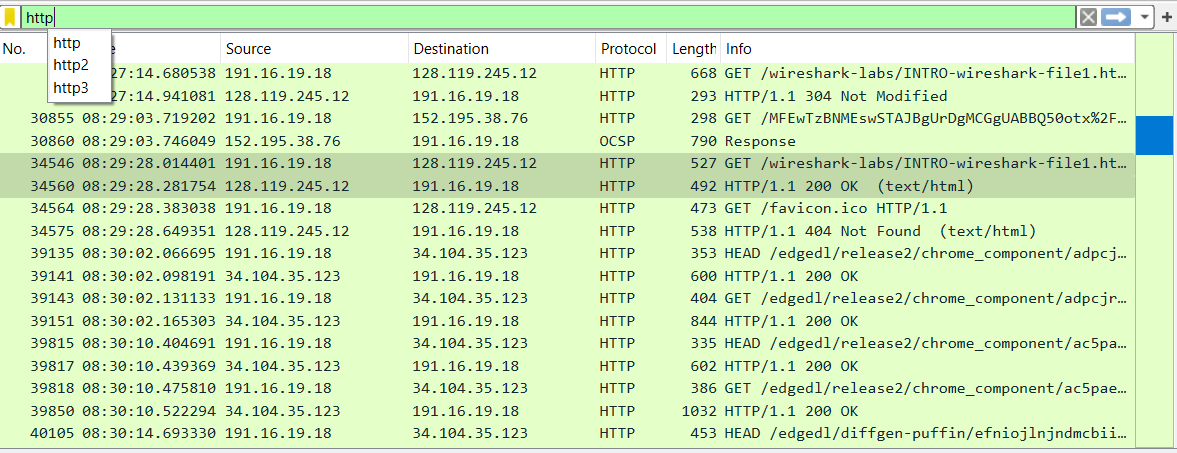
**Lab1a: Introduction to Wireshark Packet Sniffer Tool**

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



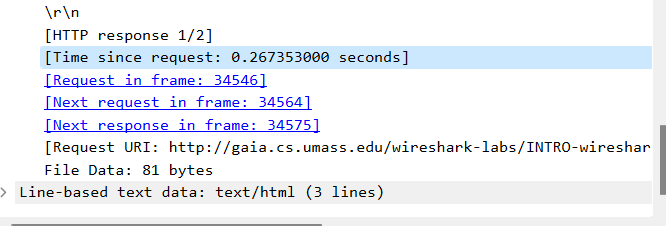
Three different protocols are: MDNS, TCP, QUIC

**Q.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 packetlisting 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.)**



Amount of time for the HTTP GET message was sent until the HTTP OK reply was received:

From 8:29:28.014401 to 8:29:28.281754: 0.267353 s



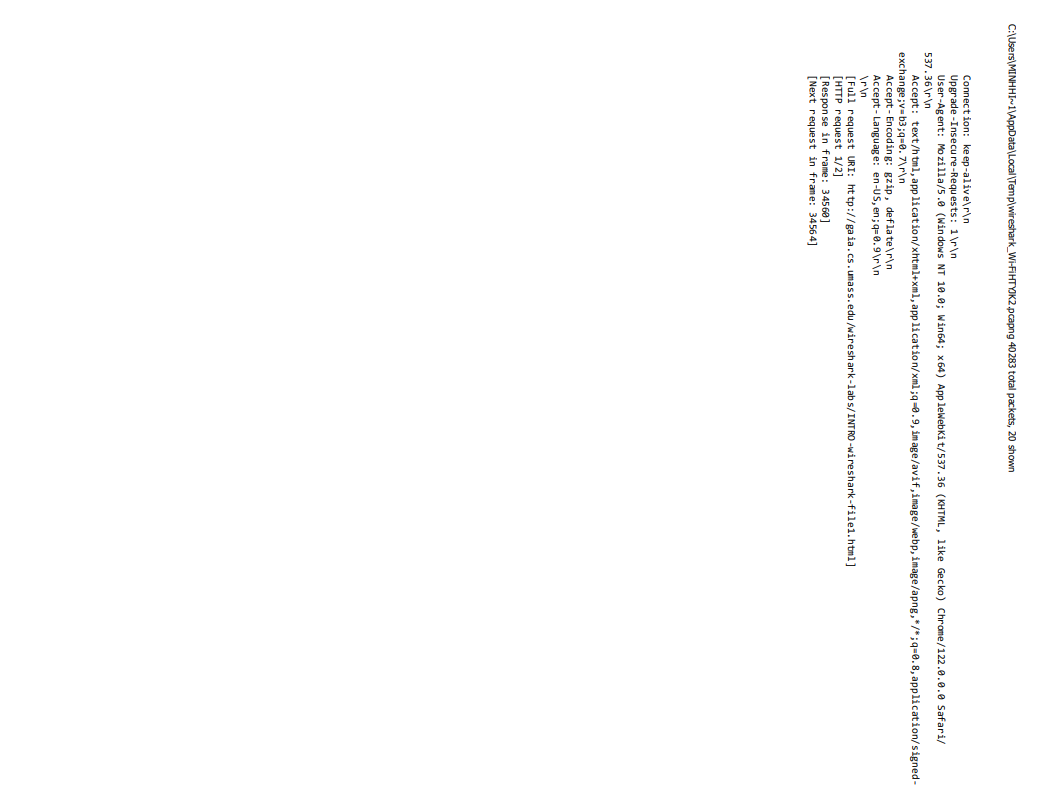
**Q.3: What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)? What is the Internet address of your computer?**

Internet address of the gaia.cs.umass.edu: 128.119.245.1

Internet address of my computer: 191.16.19.18

**Q.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.**





GET message



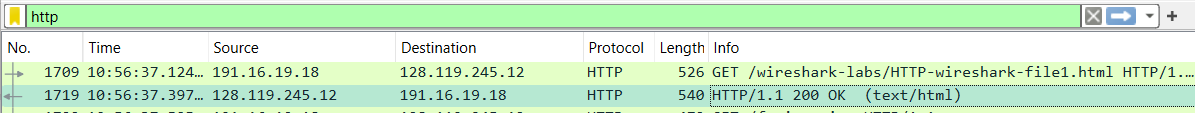


OK message

**LAB3a: Wireshark Lab: HTTP**

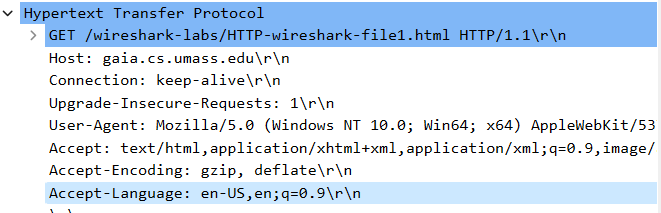
**Q1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the**

server running?



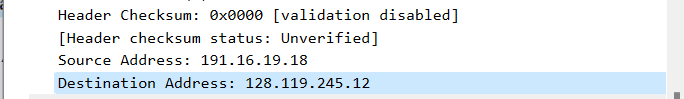
Version 1.1

**Q2. What languages (if any) does your browser indicate that it can accept to the server?**



Accept language” en-US, en

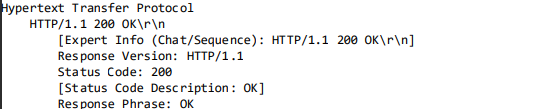
**Q3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?**



IP address of my computer: 191.16.19.18

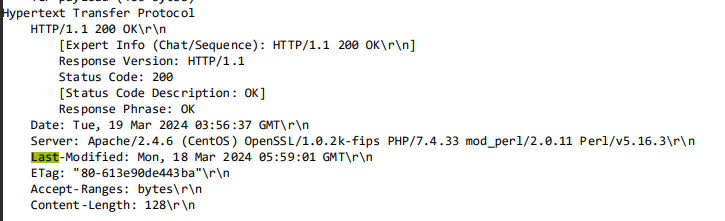
IP address of gaia.cs.umass.edu server: 128.119.245.12

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

****

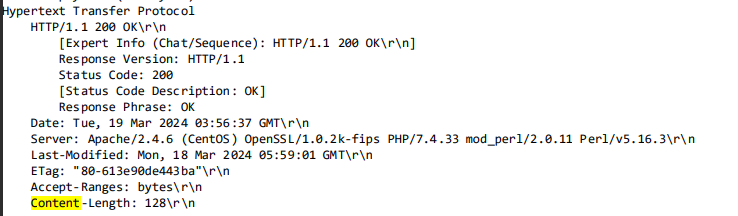
Status code: 200

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

****

Last modified: Monday, 18 March 2024 5:59:01 GMT

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

****

128 bytes

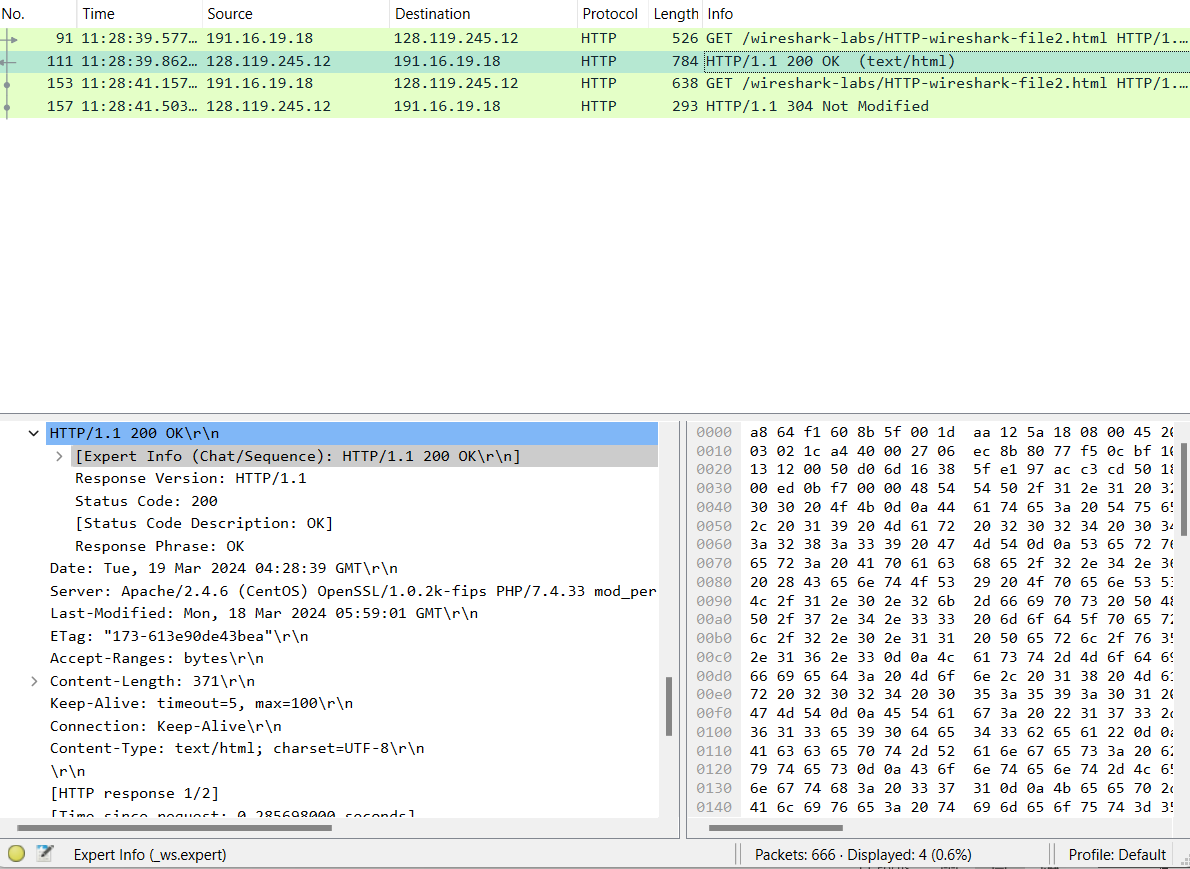
**7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one**

According to the packet data given in the prior discussion, there are no headers present in the data that are not shown in the packet-listing window.

**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?**

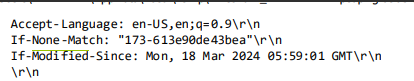
No, there isn’t exist this parameter

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

****

Indeed, the server did purposefully send back the file’s contents. This is evident from the HTTP response status “200 OK”, signifying that the server has successfully handled the request and is now transmitting the data.

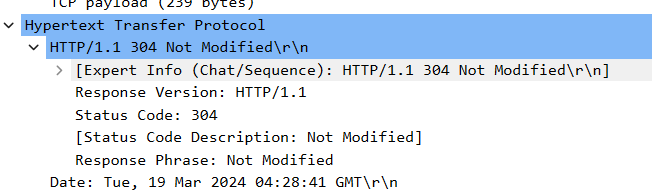
**10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?**

****

If-Modified-Since: Mon, 18 Mar 2024 05:59:01 GMT\r\n

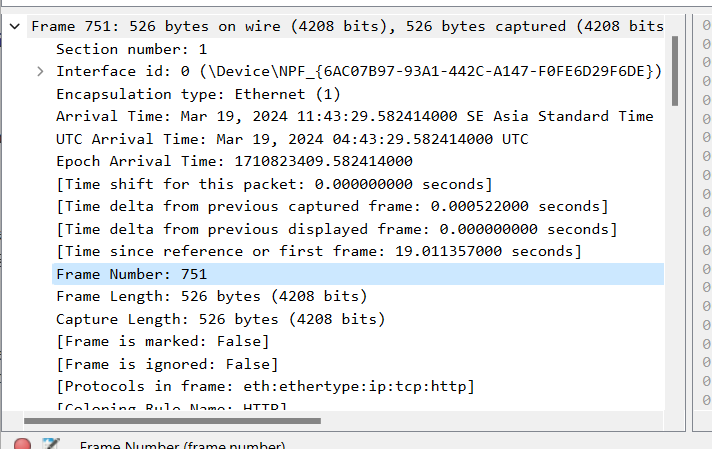
The server utilizes this data to ascertain if the browser’s cached file version is the most recent one. If there have been no modifications to the file on the server since that time, the server responds with a “304 Not Modified” status code, as demonstrated in the response you supplied.

**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.**

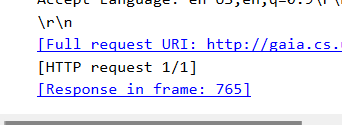
****

**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?**

Only one: Frame 751



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

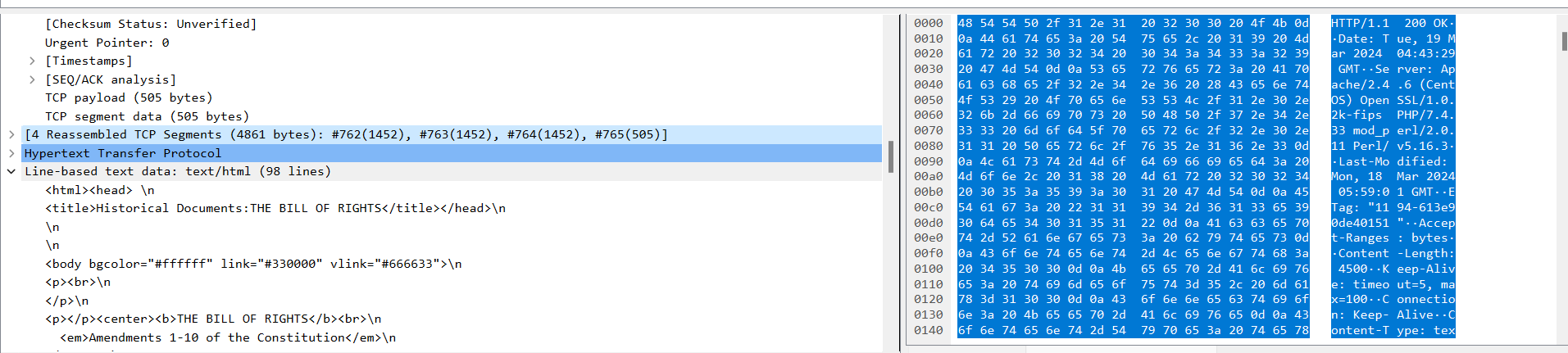
****

Frame: 765

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

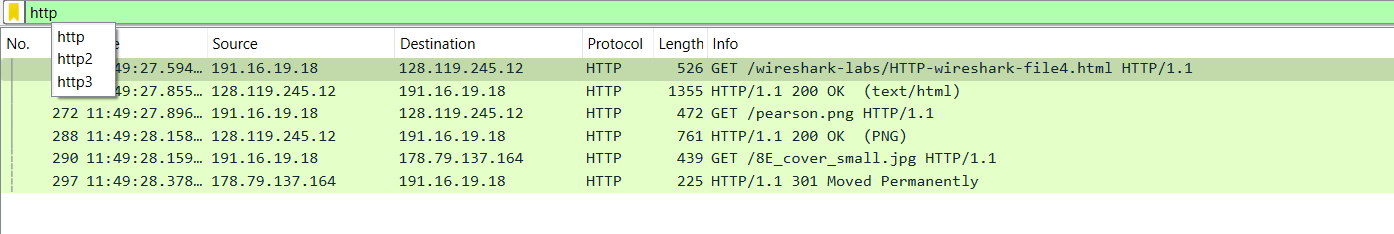
The code and phrase in the response was 200 OK

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

****

There are 4 reassembled TCP segments.

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

****

My Brower send 3 requests:

- The initial page : 128.119.245.12

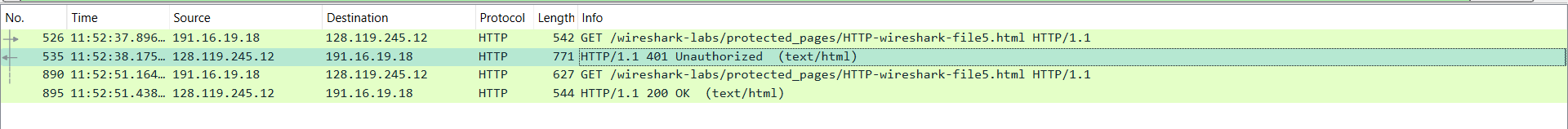
Pearson logo: 128.119.245.12

Pearson book : 178.79.137.164

**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**

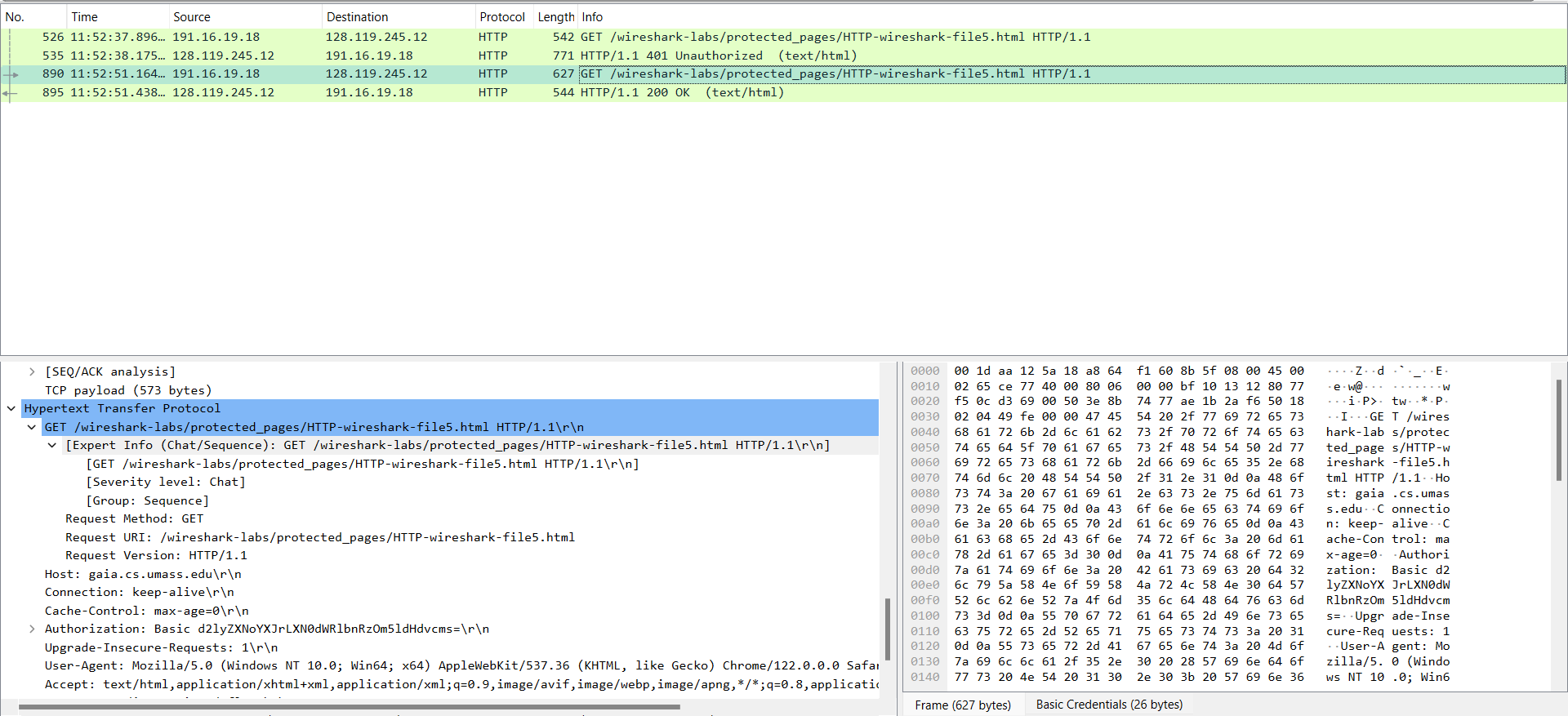
It’s observable that the second request was dispatched following the completion of the first one. Therefore, I’m under the impression that these files were downloaded in a sequential manner.

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

****

The first respond was 401 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?**

****

Itis Authorization