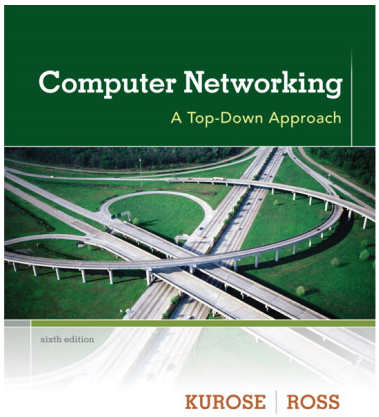
MD. ABU YOUSUF SAJAL
ID : 17.01.04.025

Wireshark Lab: HTTP v6.1

Supplement to *Computer Networking: A Top-Down Approach, 6th ed.,* J.F. Kurose and K.W. Ross



"Tell me and I forget. Show me and I remember. Involve me and I understand." Chinese proverb

---

1. The Basic HTTP GET/response interaction

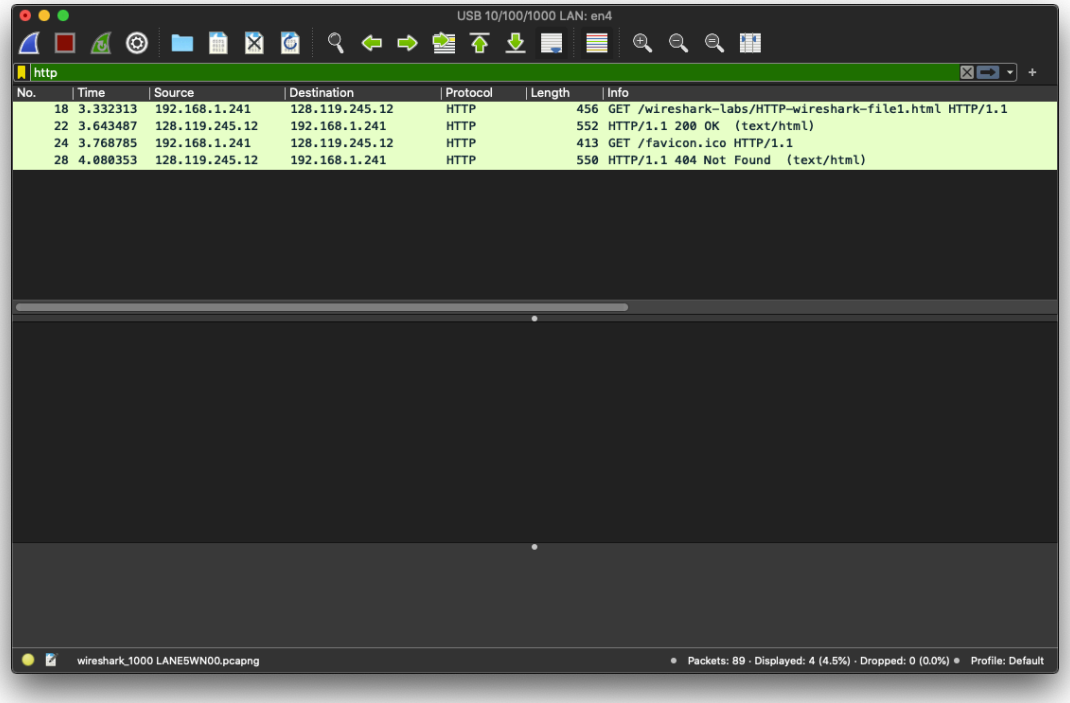


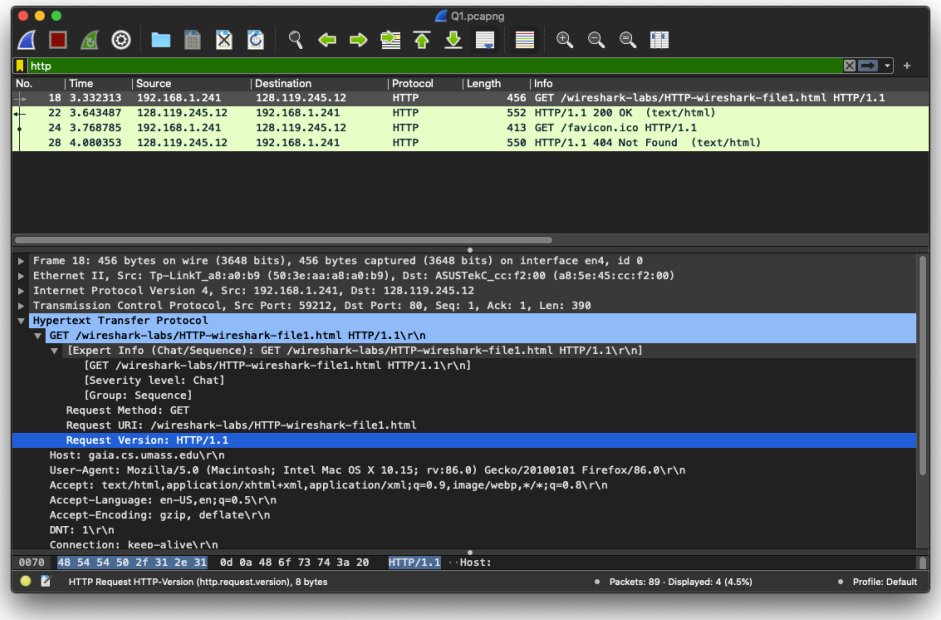
Figure 1: Wireshark Display after http://gaia.cs.umass.edu/wireshark-labs/ HTTP-wireshark-file1.html has been retrieved by browser

MD. ABU YOUSUF SAJAL
ID : 17.01.04.025

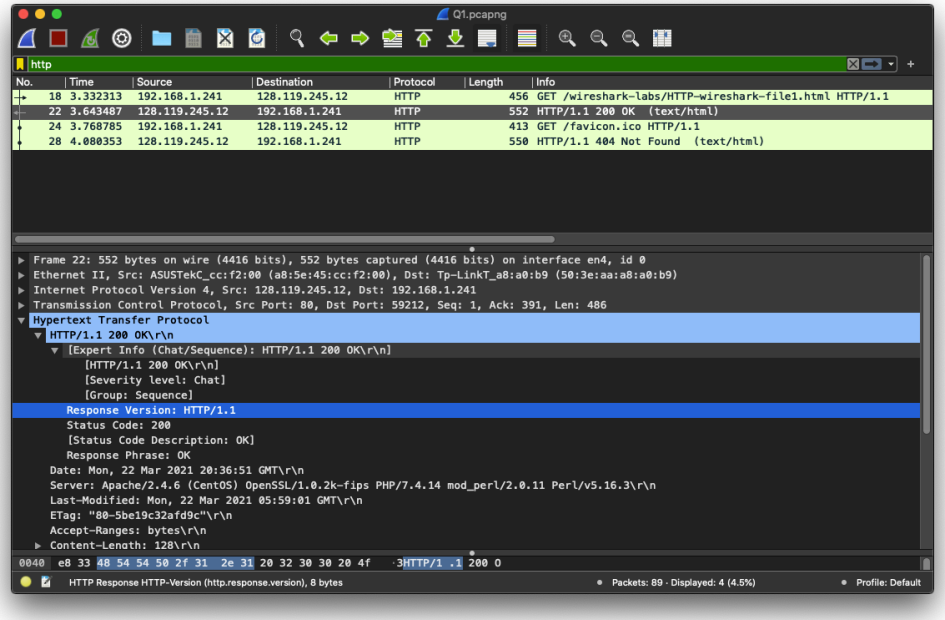
1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

ANSWER :

My Browser is running HTTP version 1.1



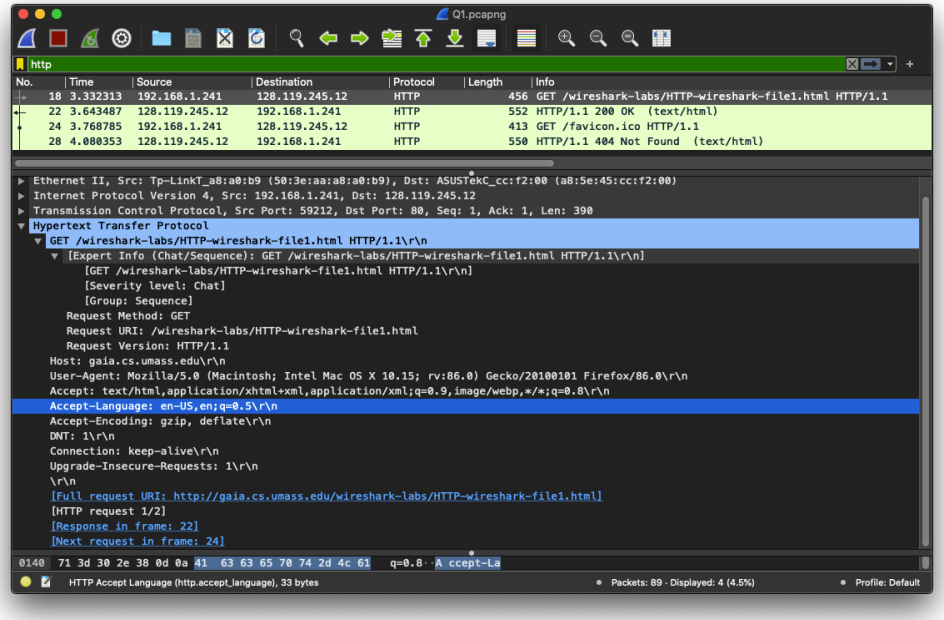
Server is running on HTTP version 1.1



MD. ABU YOUSUF SAJAL
ID : 17.01.04.025

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

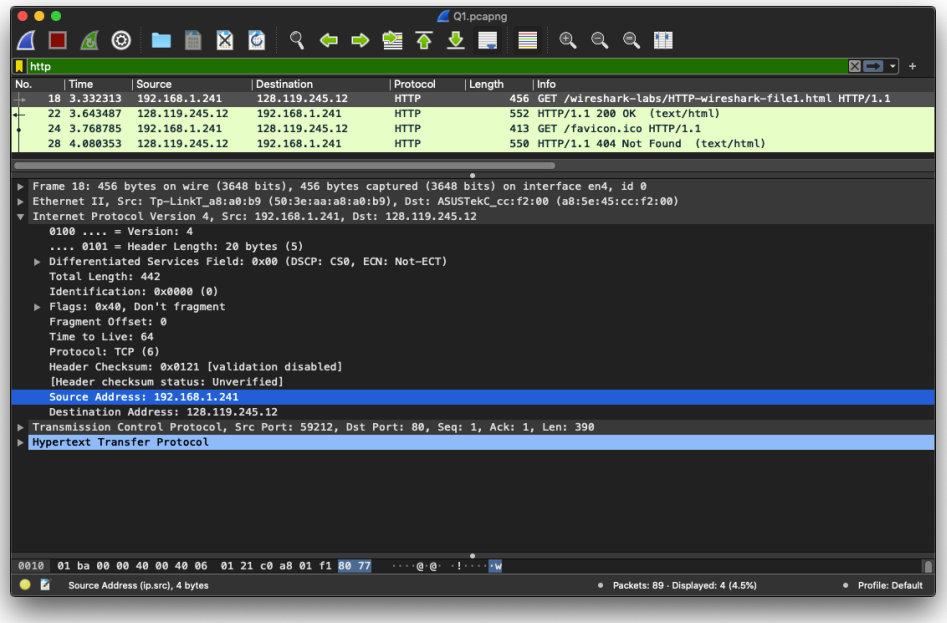
Answer : My browser indicates "**en-US**" Language format. Which is a language code tells Windows operating system to display text as per United States English standards. This is sometimes known as "localizing" content.



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

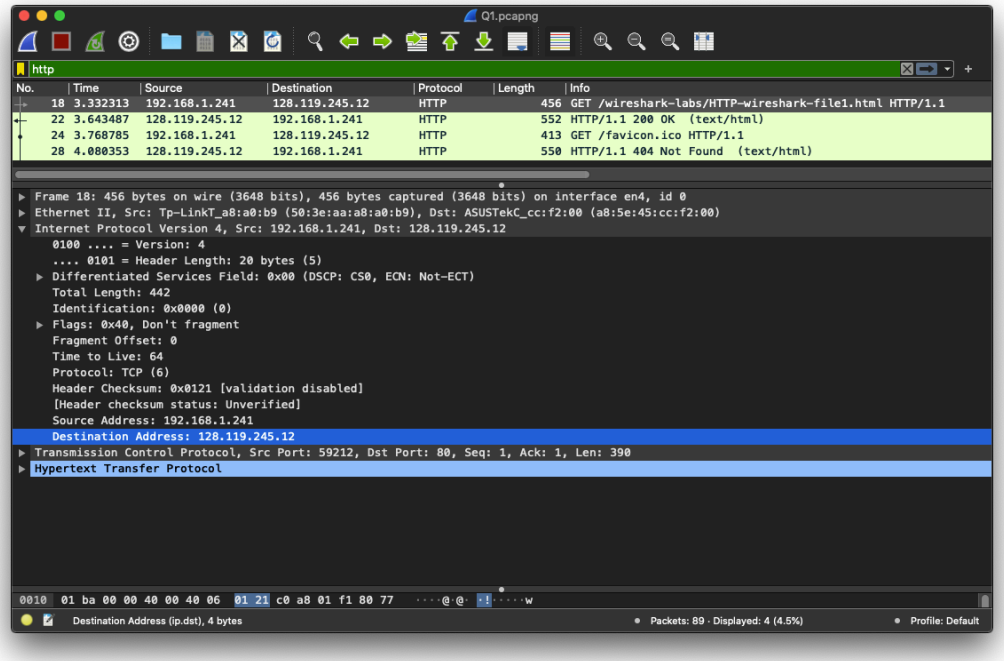
Answer :

My IP Address : *192.168.1.241* (Source Address)



MD. ABU YOUSUF SAJAL
ID : 17.01.04.025

Source IP Address : *128.119.245.12* (Destination Address)

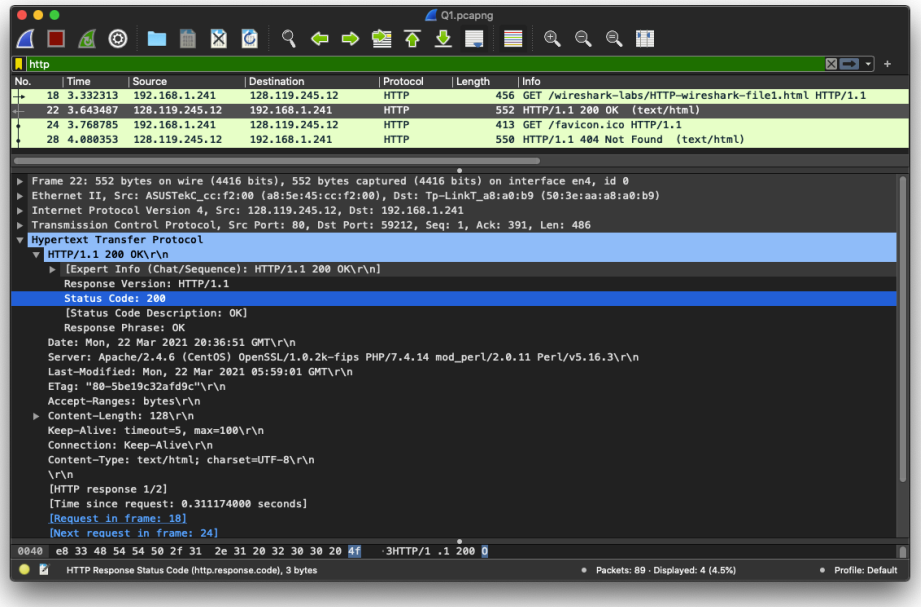


4. What is the status code returned from the server to your browser?

Answer :

Status Code : **200**

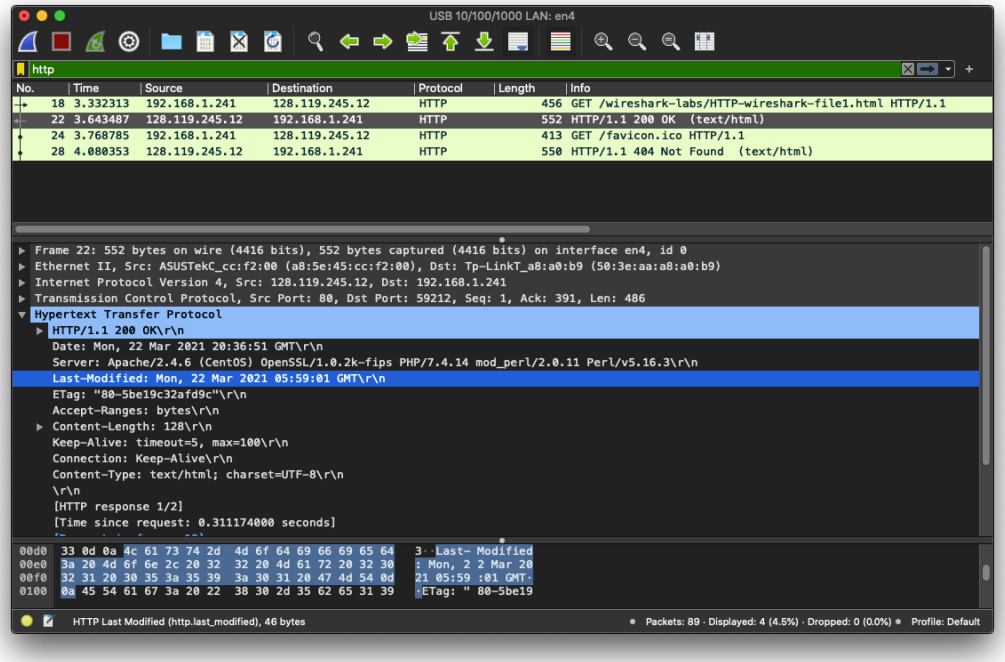
Status Code Description : OK . Success status response code indicates that the request has succeeded



MD. ABU YOUSUF SAJAL
ID : 17.01.04.025

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

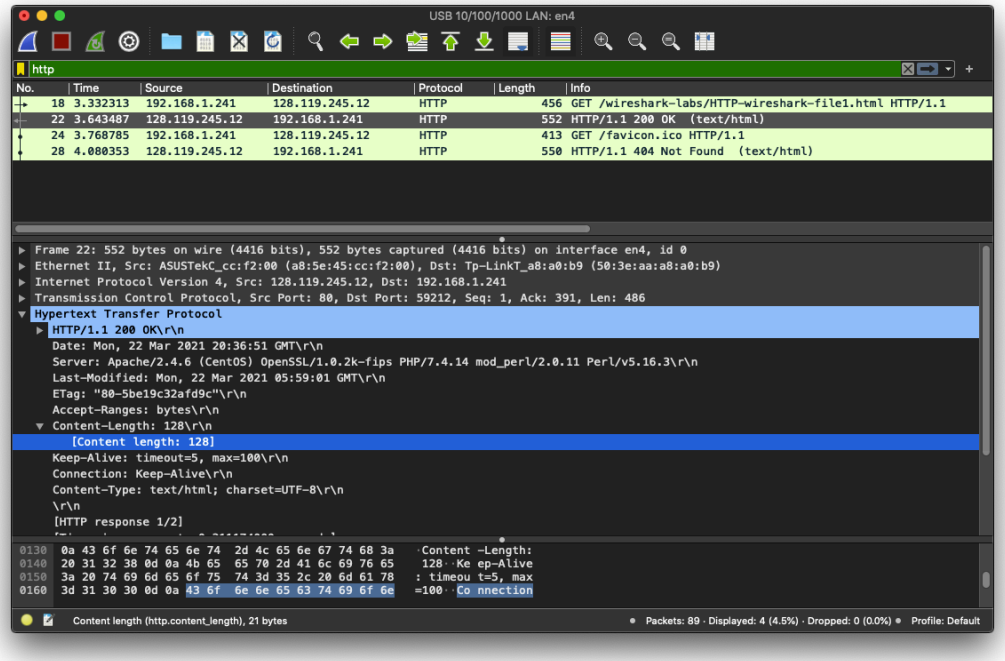
Answer : Last Modified : 22, Mar, 2021 at 05:59:01 GMT



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

Answer : Content Length : **128**

128 bytes of data are being returned to my browser.



MD. ABU YOUSUF SAJAL
ID : 17.01.04.025

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 : There have no difference in heading information between packet content and packet listing window.

2. The HTTP CONDITIONAL GET/response interaction

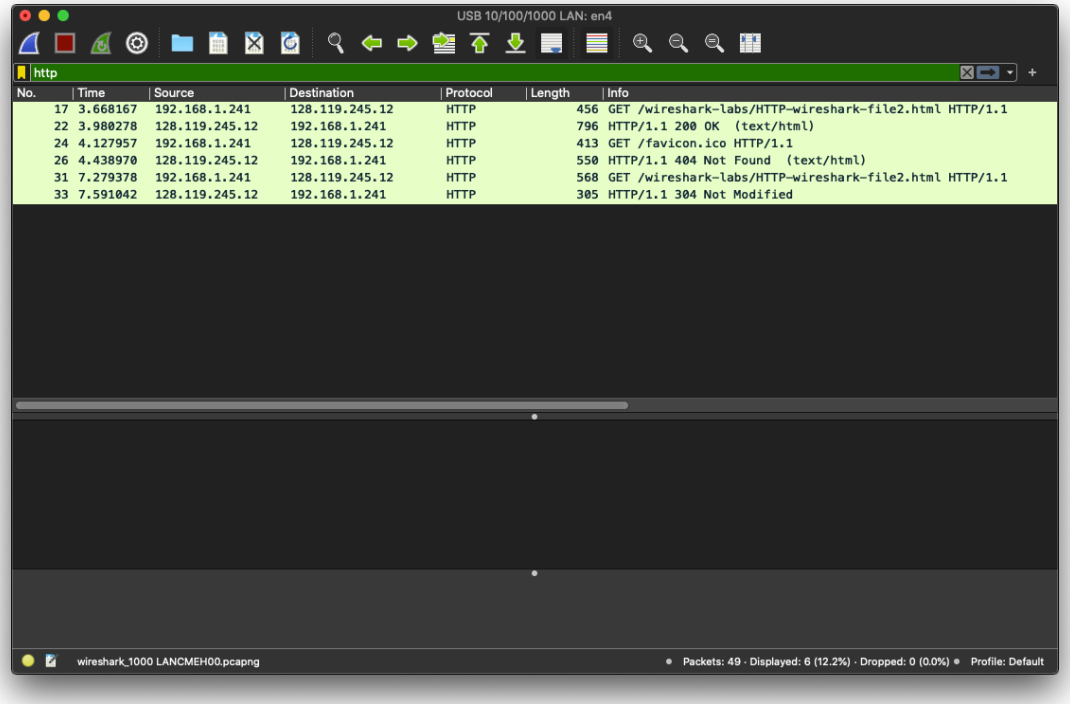
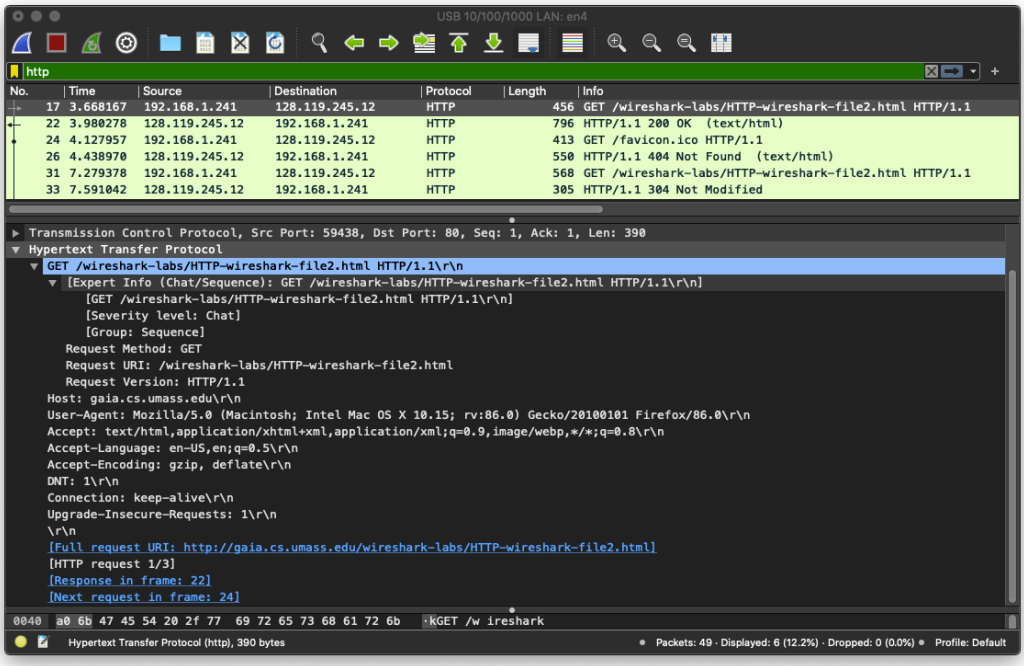


Figure 2: Wireshark Display after http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html has been retrieved by browser

MD. ABU YOUSUF SAJAL
ID : 17.01.04.025

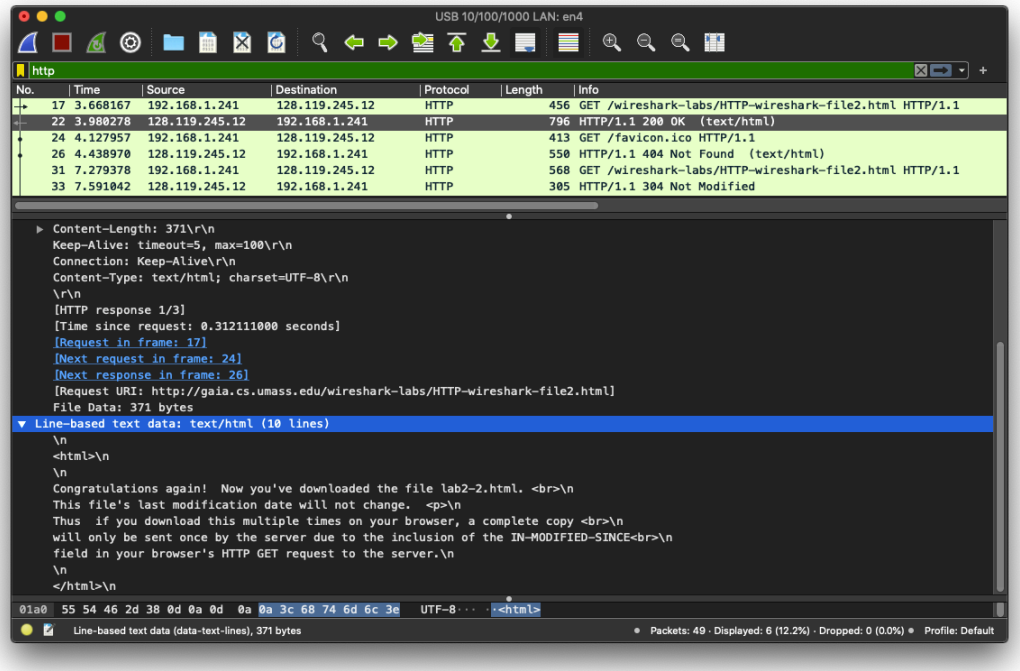
8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

Answer : There is no “IF-MODIFIED-SINCE” line in HTTP GET



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

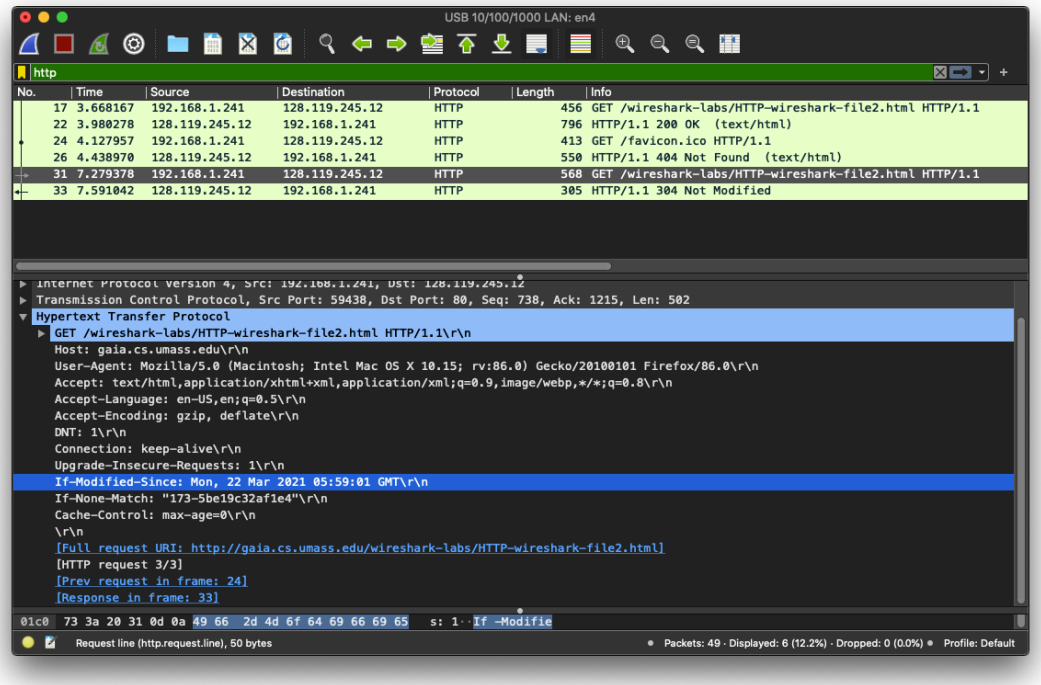
Answer : YES, The Server explicitly returned the contents of the file. Under “Line-Based Text Data” section we can see HTML contents of the file



MD. ABU YOUSUF SAJAL
ID : 17.01.04.025

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, there is an “IF-MODIFIED-SINCE” line in the HTTP GET. It contains information about last modified Date and Time of the server.



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.

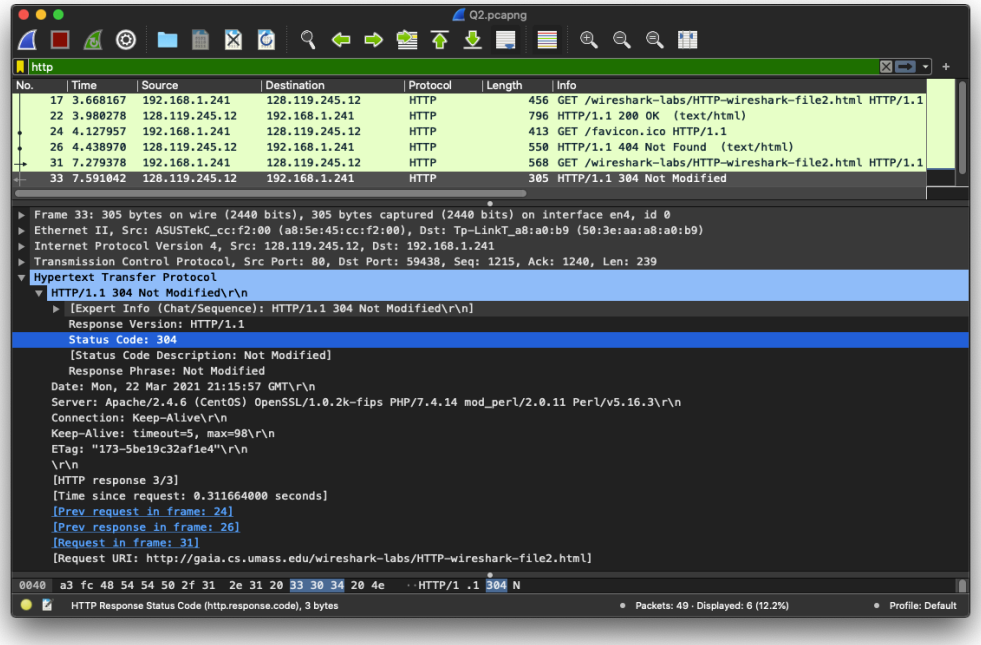
ANSWER :

Status Code : **304**

Status Code Description : The HTTP 304 Not Modified client redirection response code indicates that there is no need to retransmit the requested resources. It is an implicit redirection to a cached resource.

No, The server did not explicitly returned the contains of the file. Instead it simply commanded the browser to retrieve data from its cached memory.

MD. ABU YOUSUF SAJAL
ID : 17.01.04.025



3. Retrieving Long Documents

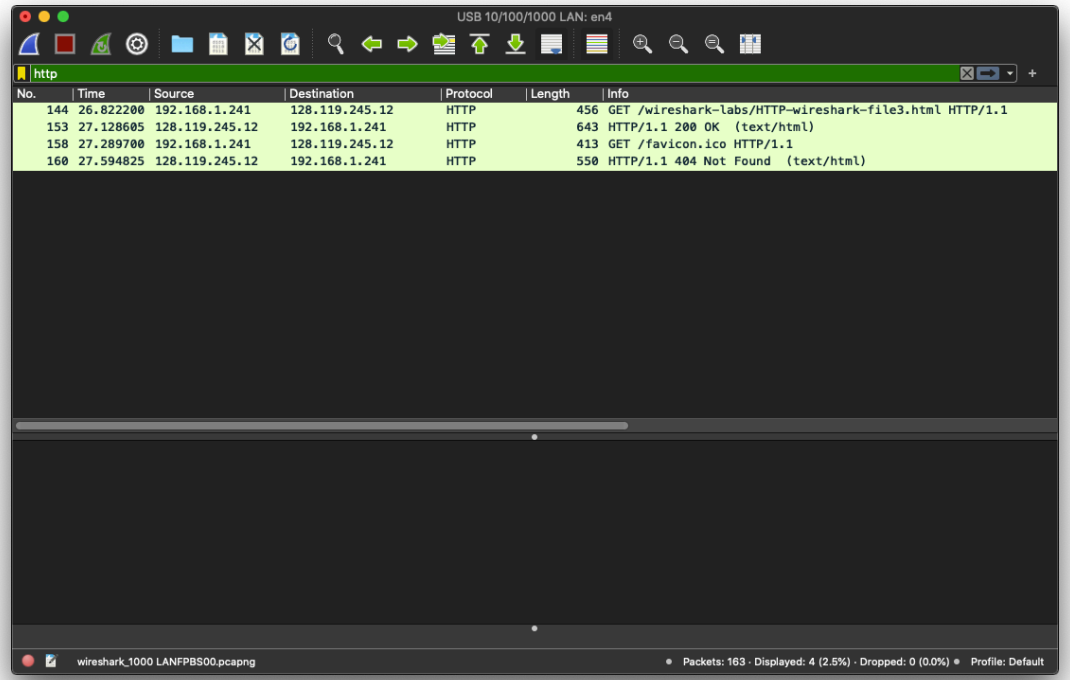
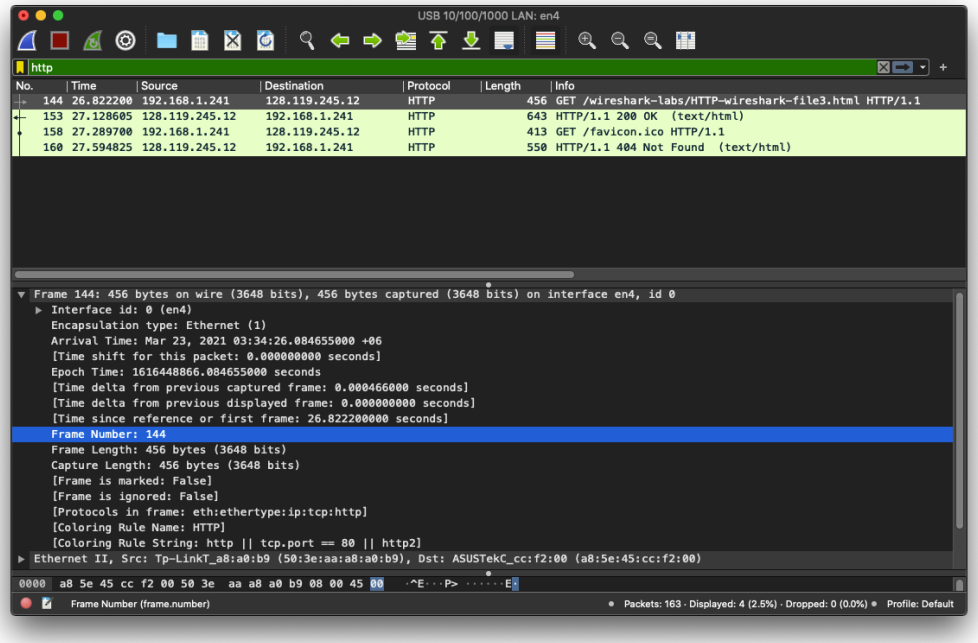


Figure 3: Wireshark Display after http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html has been retrieved by browser

MD. ABU YOUSUF SAJAL
ID : 17.01.04.025

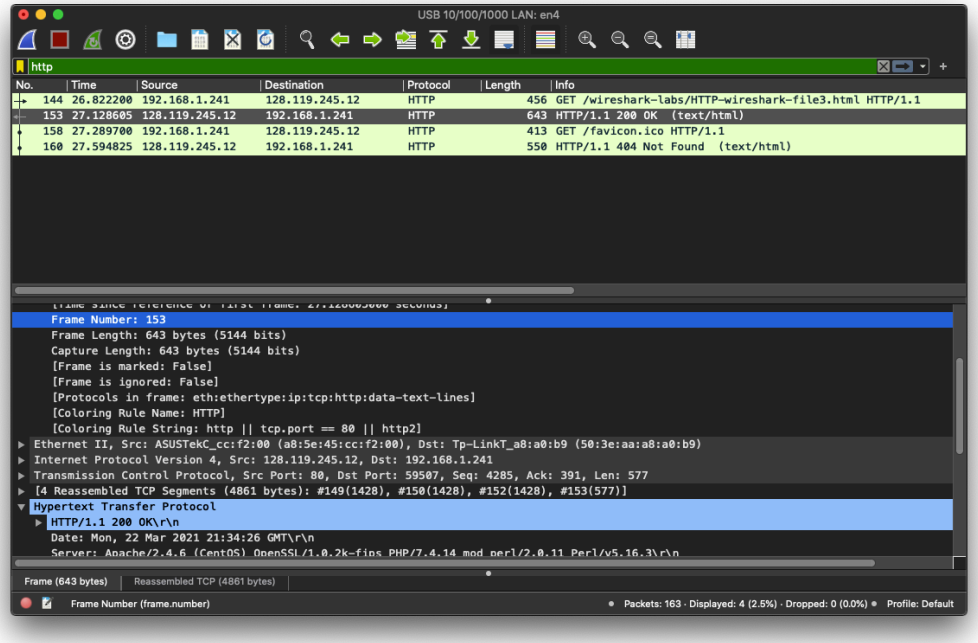
12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

Answer: My browser sent only one HTTP GET request message to the server .
The packet number was **144**.



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

Answer : 153, is the packet number which was sent by server contains the status code and phrase associated with the response to the HTTP GET request.



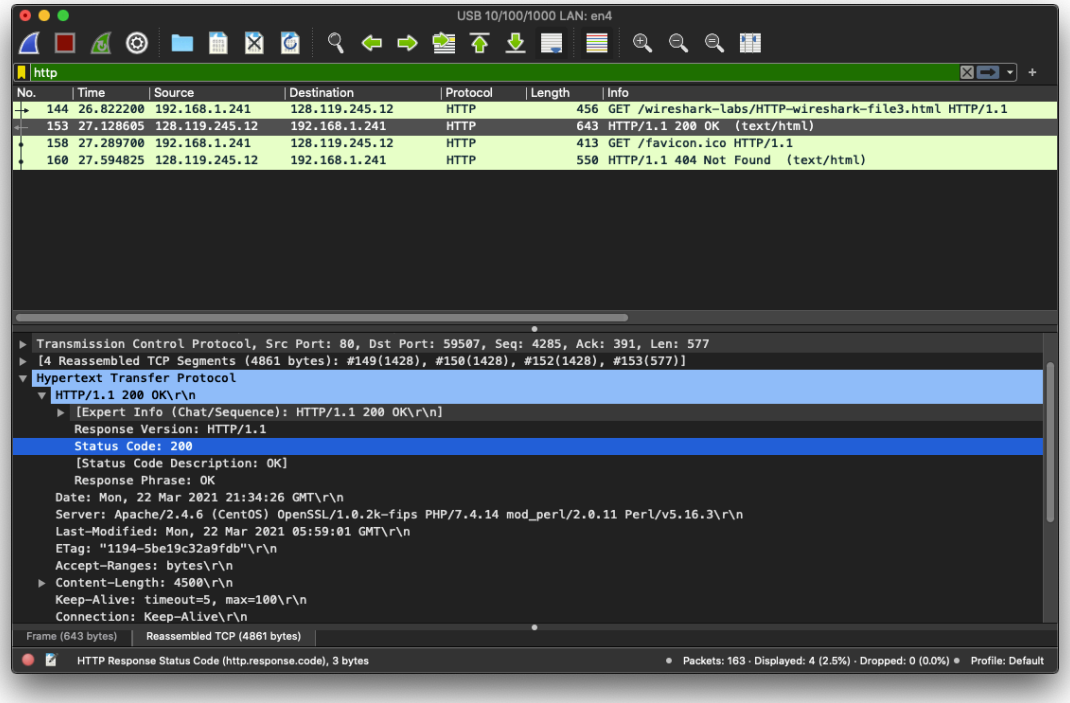
MD. ABU YOUSUF SAJAL
ID : 17.01.04.025

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

Answer :

Status Code : **200**

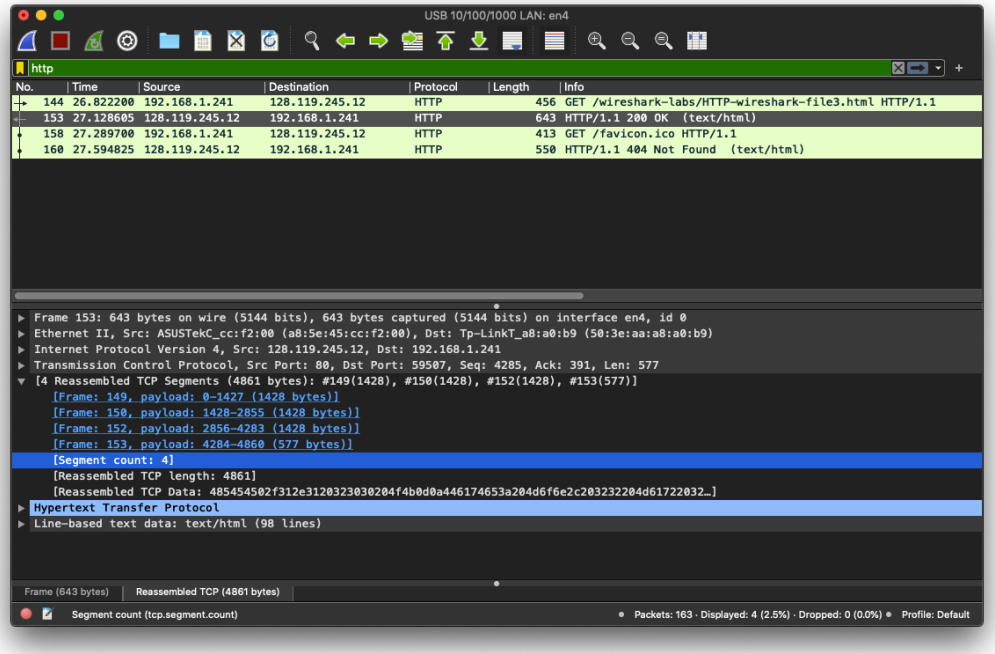
Status Code Description : The HTTP 200 OK success status response code indicates that the request has succeeded. A 200 response is cacheable by default.



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

Answer : There was **5** data-containing TCP segments needed to carry the single HTTP response and the text of the “BILL OF RIGHTS”.

MD. ABU YOUSUF SAJAL
ID : 17.01.04.025



4. HTML Documents with Embedded Objects

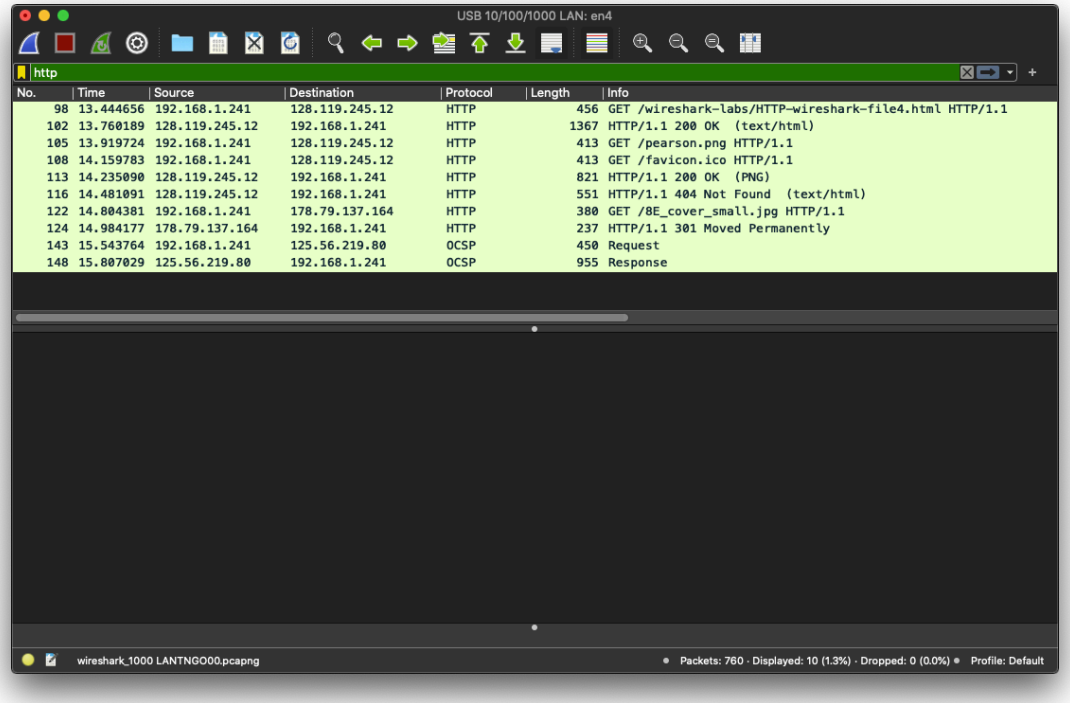


Figure 3: Wireshark Display after http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html has been retrieved by browser

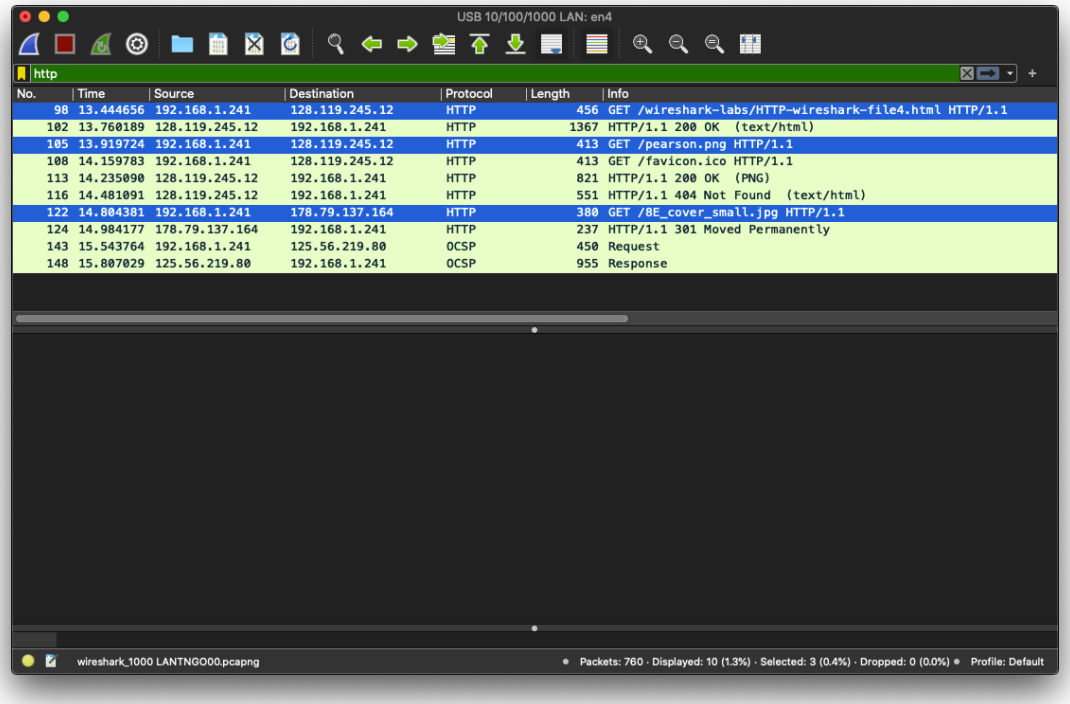
MD. ABU YOUSUF SAJAL
ID : 17.01.04.025

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

Answer : My browser sent **3** HTTP GET request messages.

Internet Addresses are given below,

URL	IP ADDRESS
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html	*128.119.245.12*
http://gaia.cs.umass.edu/pearson.png	*128.119.245.12*
http://kurose.cslash.net/8E_cover_small.jpg	*178.79.137.164*

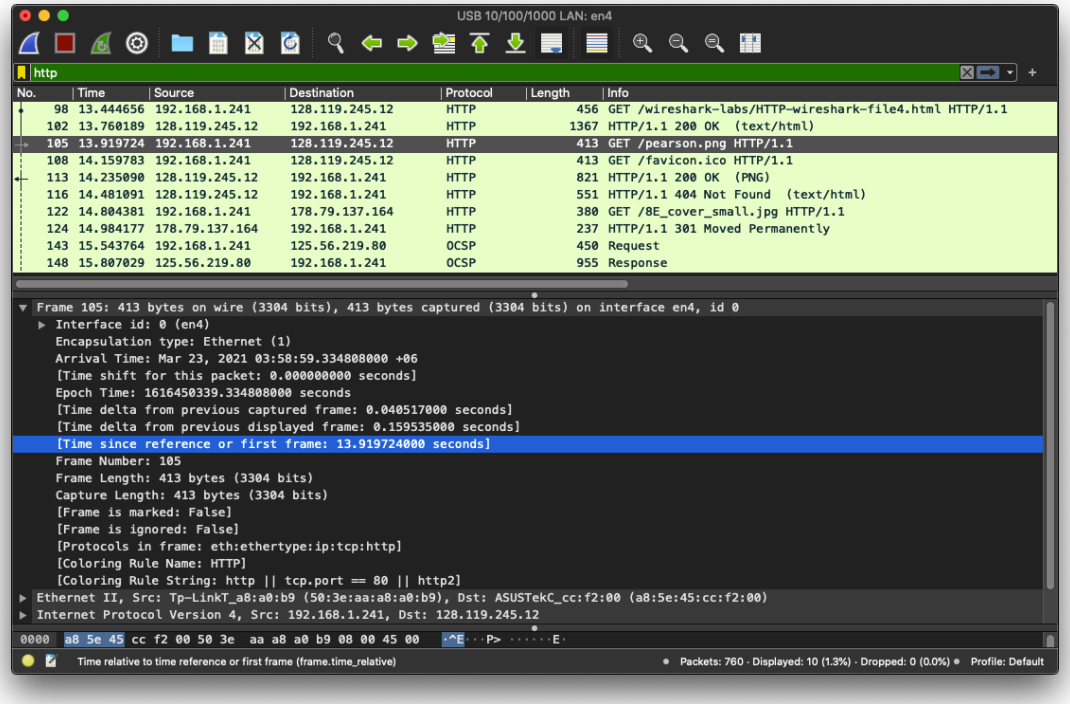


17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

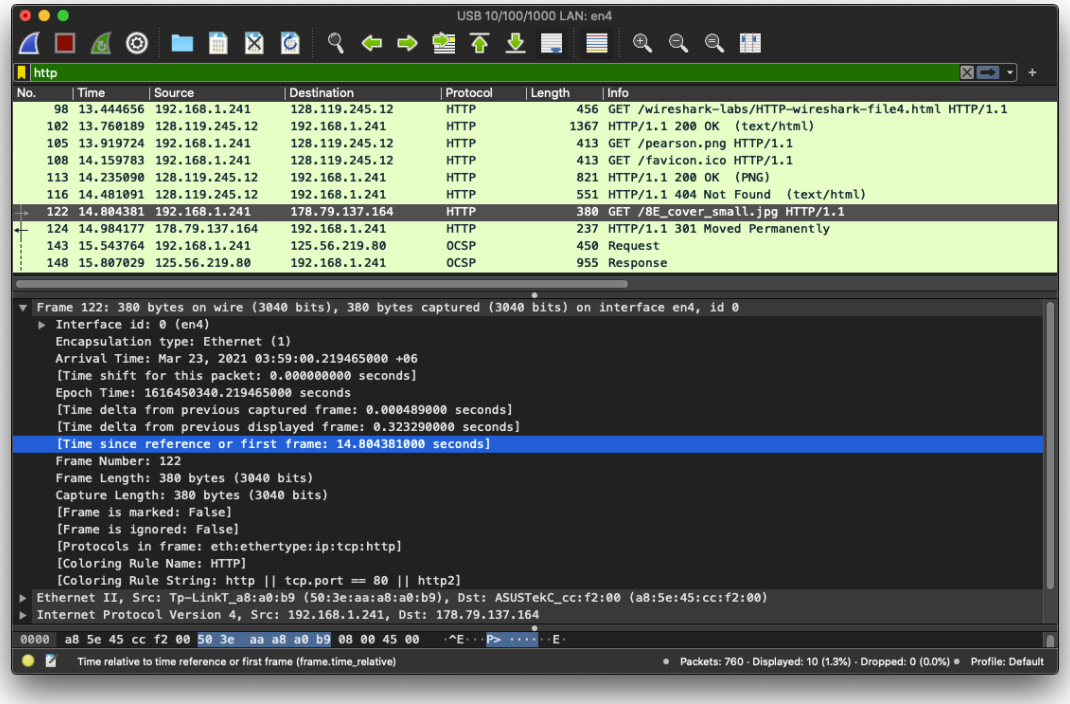
Answer : Browser downloaded the two images serially. The first image "*person.png*" was requested at **(13.919724000 sec)** since first frame and the second image "*8E_cover_small.jpg*" was requested at **(14.804381000 sec)** since first frame. So, there is a time difference of **(0.0884657 sec)**. If the were downloaded from the websites in parallel there would have no time difference.

MD. ABU YOUSUF SAJAL
ID : 17.01.04.025

First Image Requested Time : [Mar 23, 2021 **03:58:59.334808000** +06]



Second Image Requested Time : [Mar 23, 2021 **03:59:00.219465000** +06]



MD. ABU YOUSUF SAJAL
ID : 17.01.04.025

5. HTTP Authentication

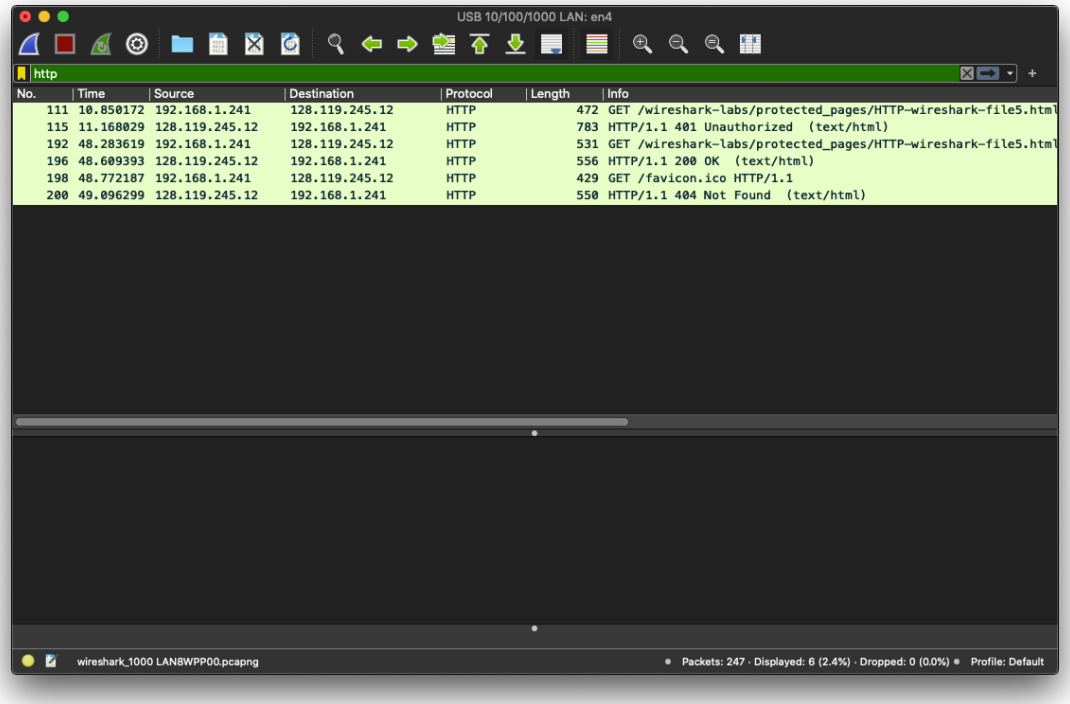


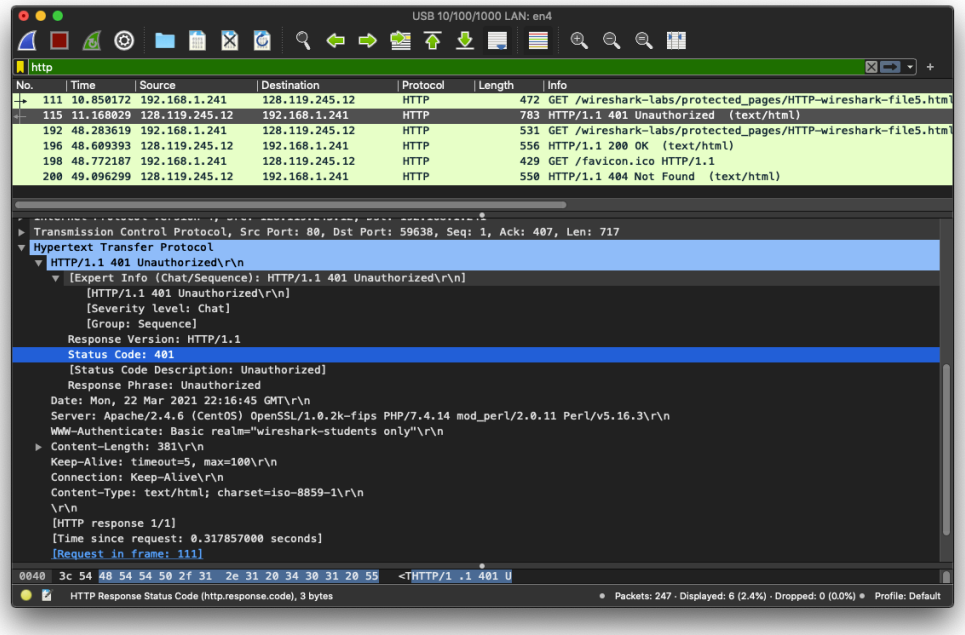
Figure 5: Wireshark Display after http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file5.html has been retrieved by browser

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

Answer :

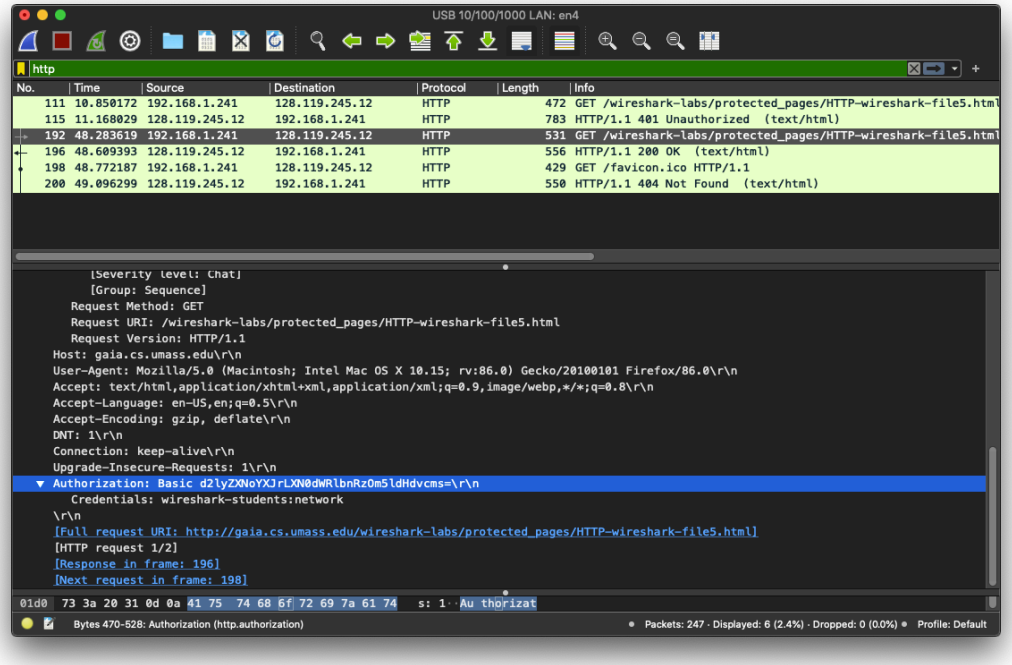
Status Code : **401**
Status Code Description : The HTTP 401 Unauthorized client error status response code indicates that the request has not been applied because it lacks valid authentication credentials for the target resource.

MD. ABU YOUSUF SAJAL
ID : 17.01.04.025



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 : When my browser sends the HTTP GET message for the second time a filed named "***Authorization***" is included.
The field contains information of login credentials in Base64 format and Plain Text which we provided as 'username' & 'password' along with our request to login to the server.



MD. ABU YOUSUF SAJAL
ID : 17.01.04.025

Resources :-

All the capture packets link given below,

Task 1

Task 2

Task 3

Task 4

Task 5