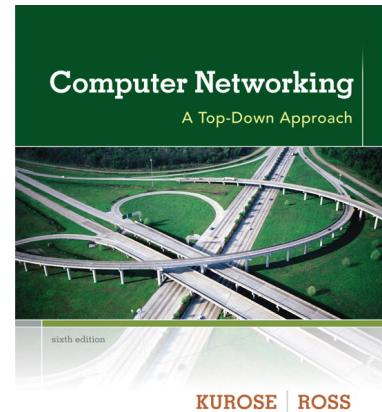


# Wireshark Lab: HTTP v6.1

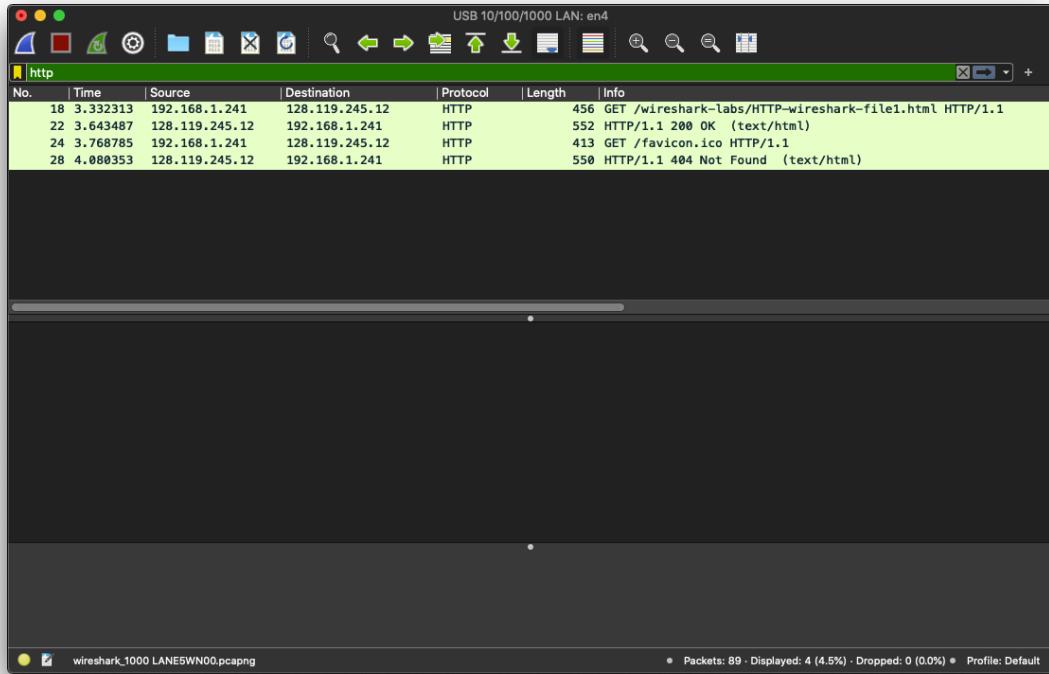
Supplement to *Computer Networking: A Top-Down Approach*, 6<sup>th</sup> ed., J.F. Kurose and K.W. Ross

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

© 2005-21012, J.F Kurose and K.W. Ross, All Rights Reserved



## 1. The Basic HTTP GET/response interaction

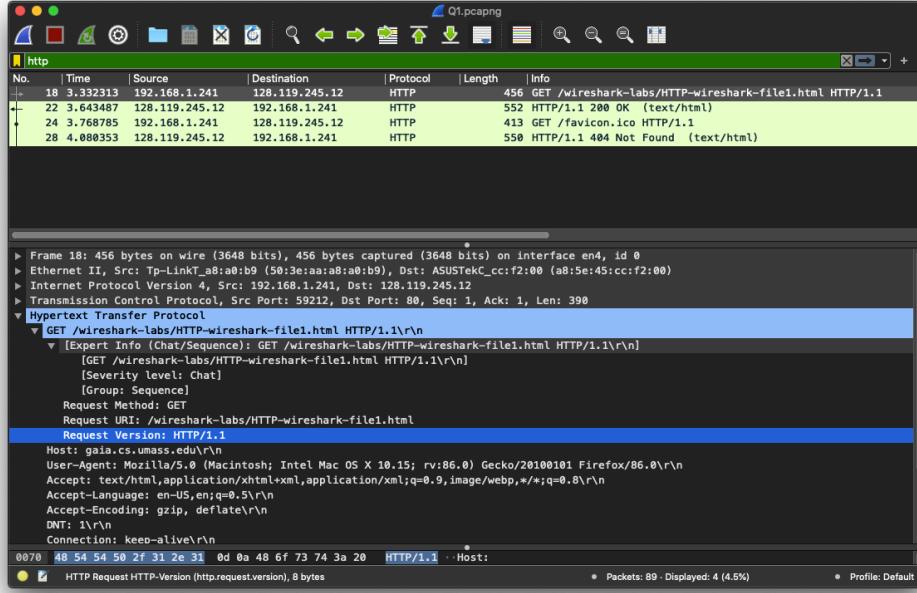


**Figure 1:** Wireshark Display after <http://gaia.cs.umass.edu/wireshark-labs/ HTTP-wireshark-file1.html> has been retrieved by browser

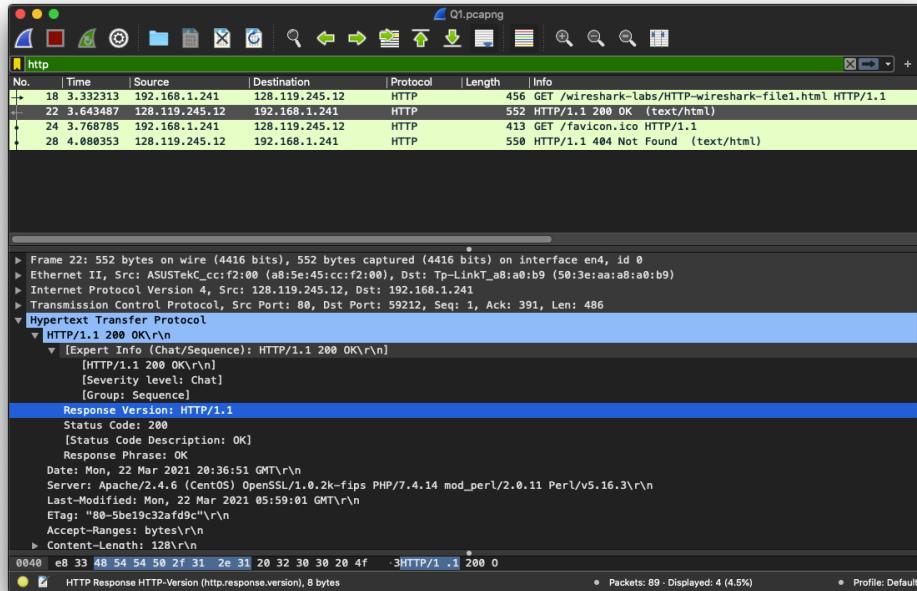
1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

**ANSWER :**

My Browser is running HTTP version 1.1



Server is running on HTTP version 1.1

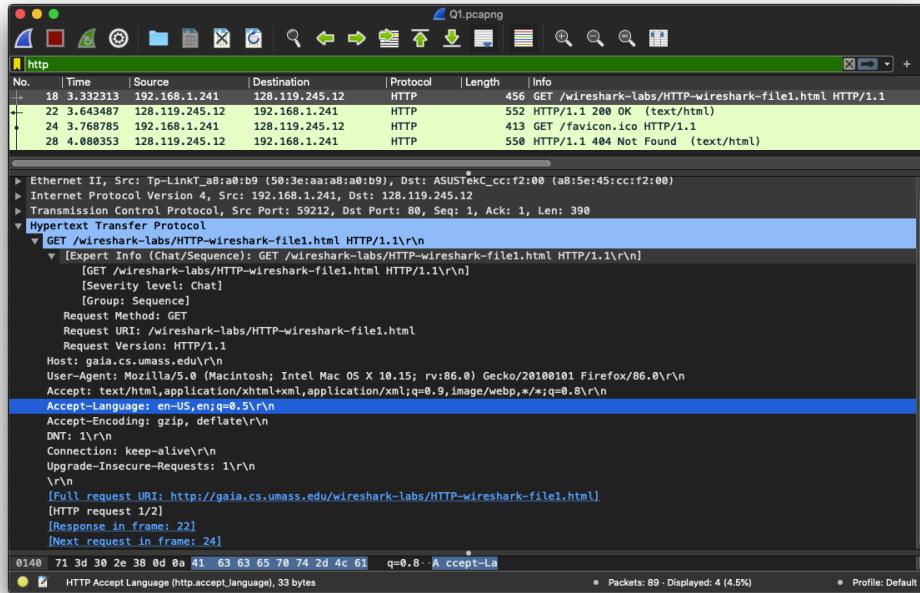


MD. ABU YOUSUF SAJAL

ID : 17.01.04.025

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

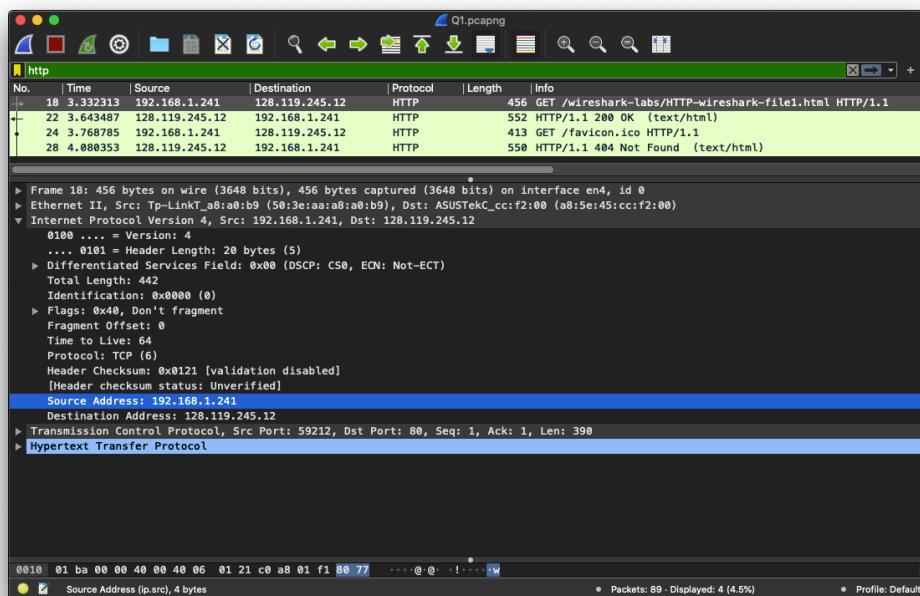
**Answer :** My browser indicates “en-US” Language format. Which is a language code tells Windows operating system to display text as per United States English standards. This is sometimes known as “localizing” content.



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

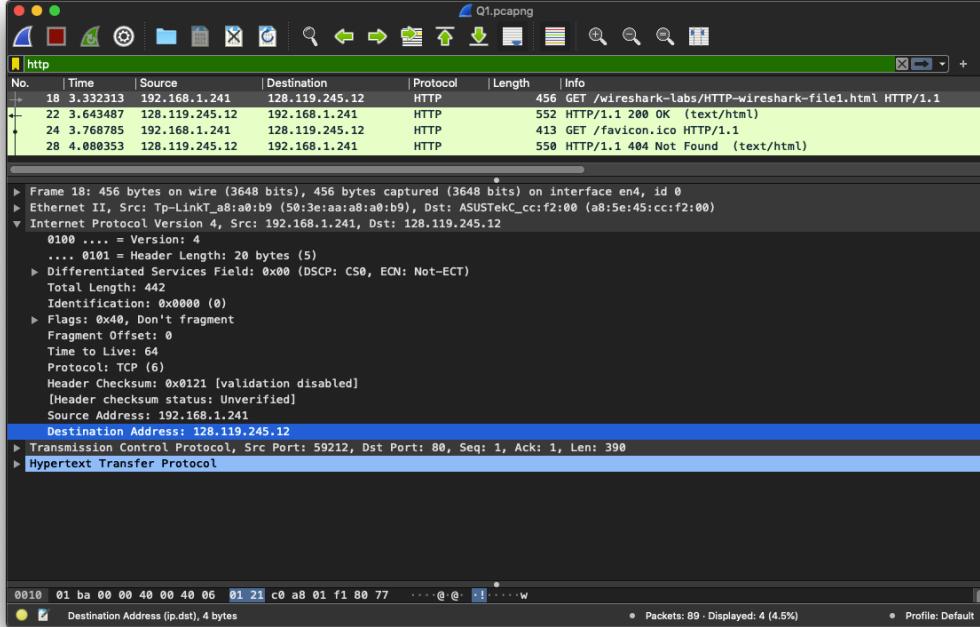
**Answer :**

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)

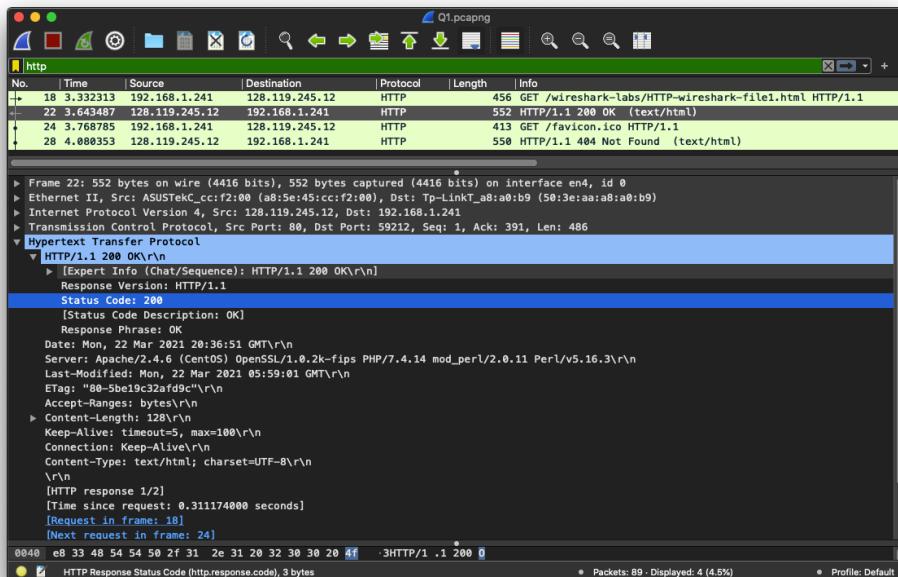


4. What is the status code returned from the server to your browser?

### 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

USB 10/100/1000 LAN: en4

No.	Time	Source	Destination	Protocol	Length	Info
18	3.332313	192.168.1.241	128.119.245.12	HTTP	456	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
22	3.643487	128.119.245.12	192.168.1.241	HTTP	552	HTTP/1.1 200 OK (text/html)
24	3.768785	192.168.1.241	128.119.245.12	HTTP	413	GET /favicon.ico HTTP/1.1
28	4.080353	128.119.245.12	192.168.1.241	HTTP	550	HTTP/1.1 404 Not Found (text/html)

Frame 22: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface en4, id 0  
Ethernet II, Src: ASUSTekC\_cc:f2:00 (a8:5e:45:cc:f2:00), Dst: Tp-LinkT\_a8:a0:b9 (50:3e:aa:a8:a0:b9)  
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.241  
Transmission Control Protocol, Src Port: 80, Dst Port: 59212, Seq: 1, Ack: 391, Len: 486

▼ Hypertext Transfer Protocol  
  ► HTTP/1.1 200 OK\r\n    Date: Mon, 22 Mar 2021 05:36:51 GMT\r\n    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod\_perl/2.0.11 Perl/v5.16.3\r\n    Last-Modified: Mon, 22 Mar 2021 05:59:01 GMT\r\n    ETag: "80-5be19c32af9c"\r\n    Accept-Ranges: bytes\r\n    Content-Length: 128\r\n    Keep-Alive: timeout=5, max=100\r\n    Connection: Keep-Alive\r\n    Content-Type: text/html; charset=UTF-8\r\n\r\n    [HTTP response 1/2]  
    [Time since request: 0.311174000 seconds]

00d0 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64 3 · Last- Modified  
00e0 3a 20 4d 6f 6e 2c 20 32 32 20 4d 61 72 20 32 30 : Mon, 22 Mar 20  
00f0 32 31 20 30 35 3a 30 31 20 47 4d 54 0d 21 05:59:01 GMT.  
0100 0a 45 54 61 67 3a 20 22 38 30 2d 35 62 65 31 39 ETag: " 80-5be19

HTTP Last Modified (http.last\_modified), 46 bytes

Packets: 89 - Displayed: 4 (4.5%) - Dropped: 0 (0.0%) • Profile: Default

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.

USB 10/100/1000 LAN: en4

No.	Time	Source	Destination	Protocol	Length	Info
18	3.332313	192.168.1.241	128.119.245.12	HTTP	456	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
22	3.643487	128.119.245.12	192.168.1.241	HTTP	552	HTTP/1.1 200 OK (text/html)
24	3.768785	192.168.1.241	128.119.245.12	HTTP	413	GET /favicon.ico HTTP/1.1
28	4.080353	128.119.245.12	192.168.1.241	HTTP	550	HTTP/1.1 404 Not Found (text/html)

Frame 22: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface en4, id 0  
Ethernet II, Src: ASUSTekC\_cc:f2:00 (a8:5e:45:cc:f2:00), Dst: Tp-LinkT\_a8:a0:b9 (50:3e:aa:a8:a0:b9)  
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.241  
Transmission Control Protocol, Src Port: 80, Dst Port: 59212, Seq: 1, Ack: 391, Len: 486

▼ Hypertext Transfer Protocol  
  ► HTTP/1.1 200 OK\r\n    Date: Mon, 22 Mar 2021 05:36:51 GMT\r\n    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod\_perl/2.0.11 Perl/v5.16.3\r\n    Last-Modified: Mon, 22 Mar 2021 05:59:01 GMT\r\n    ETag: "80-5be19c32af9c"\r\n    Accept-Ranges: bytes\r\n    Content-Length: 128\r\n    Keep-Alive: timeout=5, max=100\r\n    Connection: Keep-Alive\r\n    Content-Type: text/html; charset=UTF-8\r\n\r\n    [Content length: 128]  
    Keep-Alive: timeout=5, max=100\r\n    Connection: Keep-Alive\r\n    Content-Type: text/html; charset=UTF-8\r\n    \r\n    [HTTP response 1/2]

0130 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a : Content -Length:  
0140 20 31 32 38 0d 0a 4b 65 65 70 2d 41 6c 69 76 65 128 · Ke ep-Alive  
0150 3a 20 74 69 6d 65 6f 75 74 3d 35 2c 20 6d 61 78 : timeou t=5, max  
0160 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e =100 · Co nnection

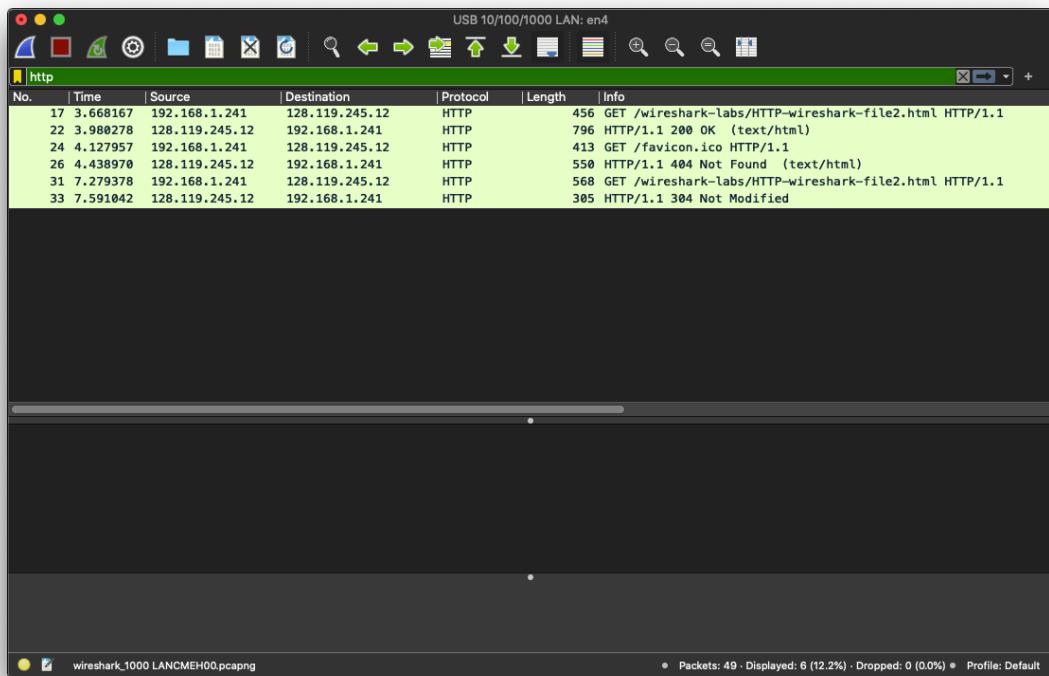
Content length (http.content\_length), 21 bytes

Packets: 89 - Displayed: 4 (4.5%) - Dropped: 0 (0.0%) • Profile: Default

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



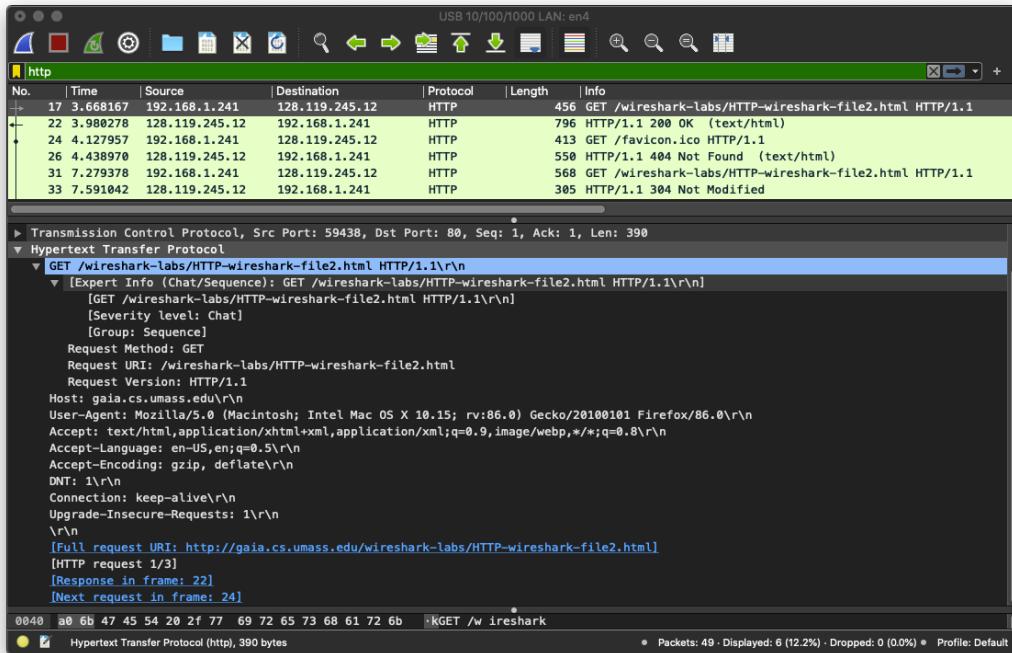
**Figure 2:** Wireshark Display after <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html> has been retrieved by browser

MD. ABU YOUSUF SAJAL

ID : 17.01.04.025

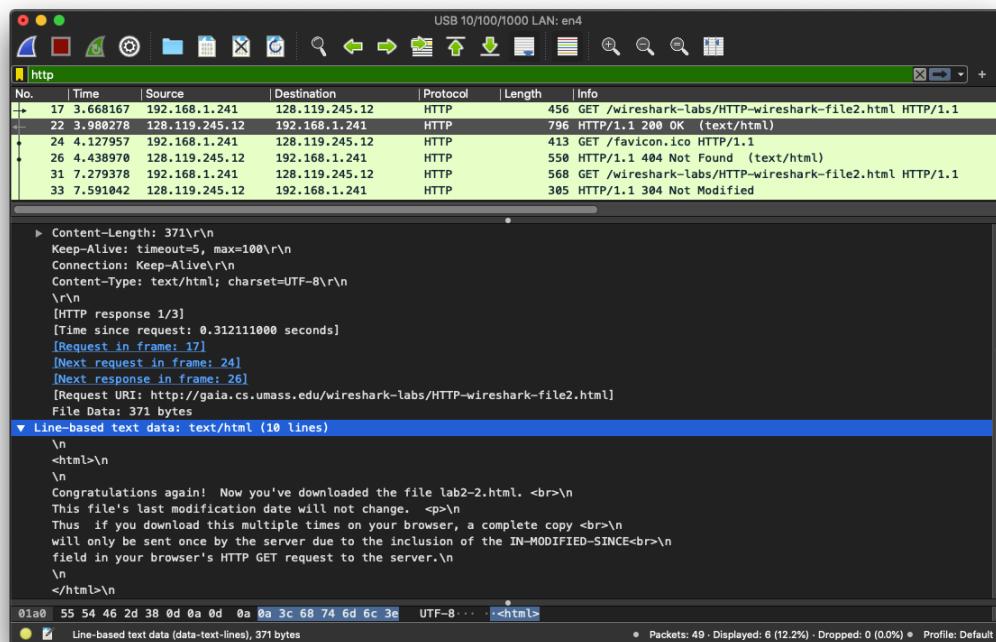
8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

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



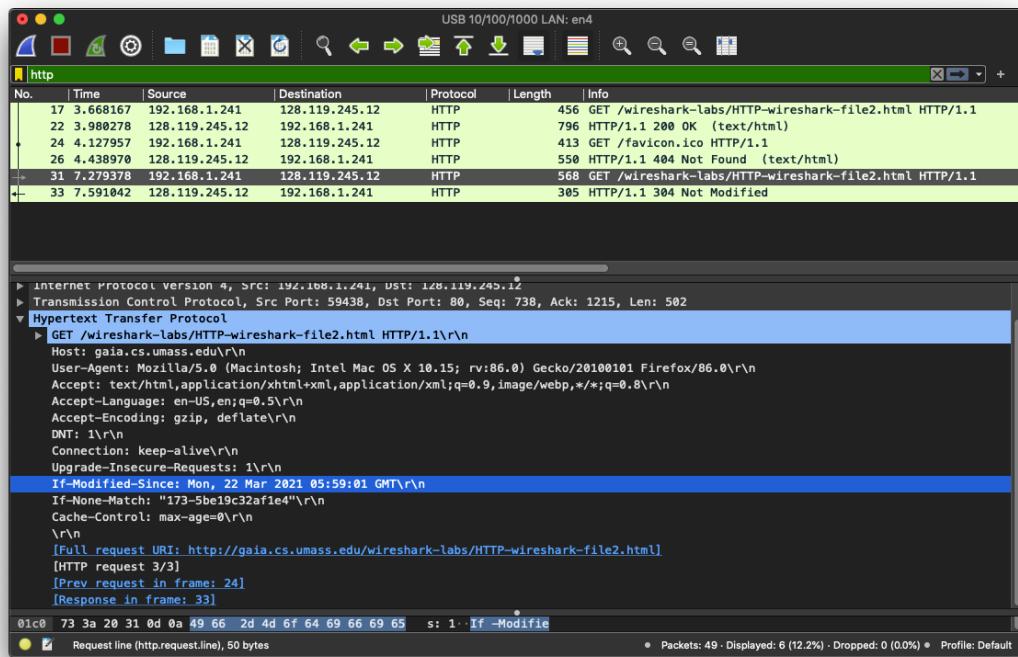
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

**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



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.



The screenshot shows a Wireshark capture window with the following details:

- USB 10/100/1000 LAN: en4** is selected as the interface.
- The **http** protocol is selected in the filter bar.
- The table lists 33 captured frames, with the 33rd frame highlighted in green. The columns include No., Time, Source, Destination, Protocol, Length, and Info.
- The 33rd frame is expanded to show the raw HTTP request:

```
> Internet Protocol Version 4, Src: 192.168.1.241, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 59438, Dst Port: 80, Seq: 738, Ack: 1215, Len: 502
> Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gala.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:86.0) Gecko/20100101 Firefox/86.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    DNT: 1\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    If-Modified-Since: Mon, 22 Mar 2021 05:59:01 GMT\r\n
    If-None-Match: "173-5be19c32af1e4"\r\n
    Cache-Control: max-age=0\r\n
  \r\n
  [Full request URI: http://gala.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
  [HTTP request 3/3]
  [Prev request in frame: 24]
  [Response in frame: 33]
```
- The status bar at the bottom indicates: Request line (http.request.line), 50 bytes, Packets: 49 - Displayed: 6 (12.2%) - Dropped: 0 (0.0%) - Profile: Default.

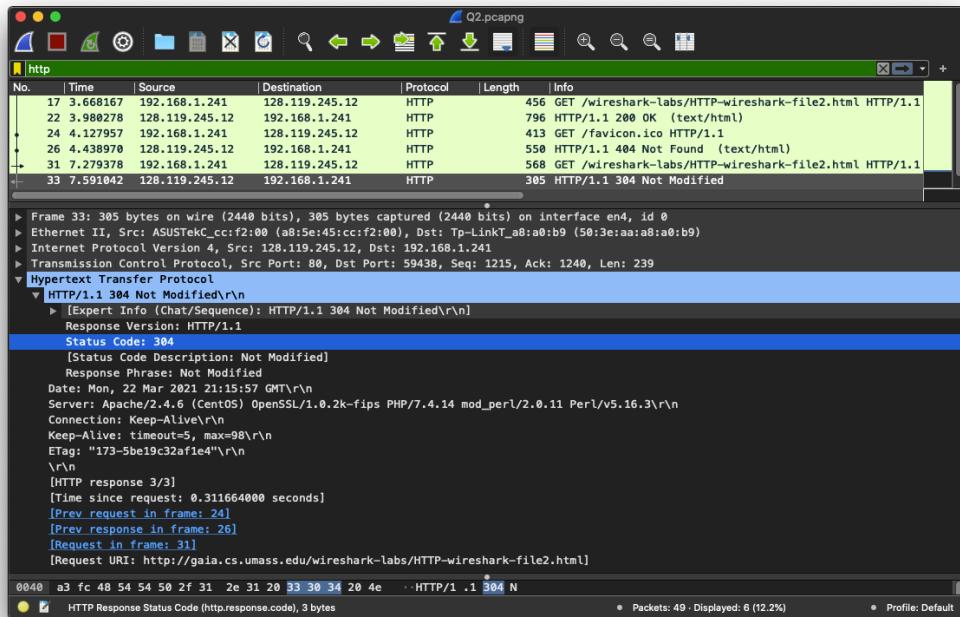
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

**ANSWER :**

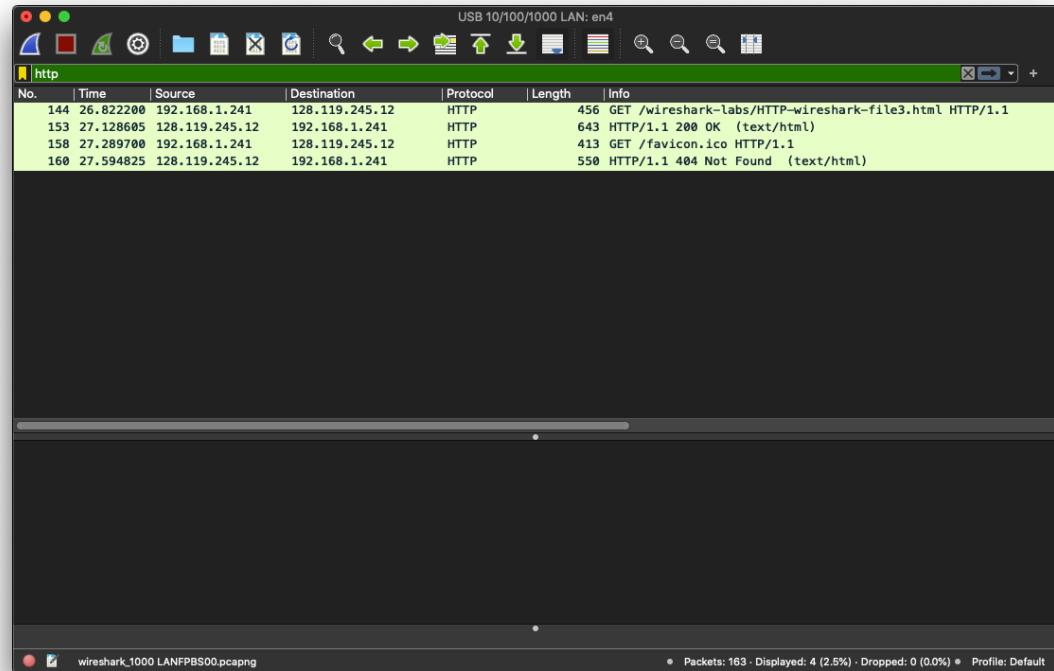
Status Code : **304**

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.



### 3. Retrieving Long Documents



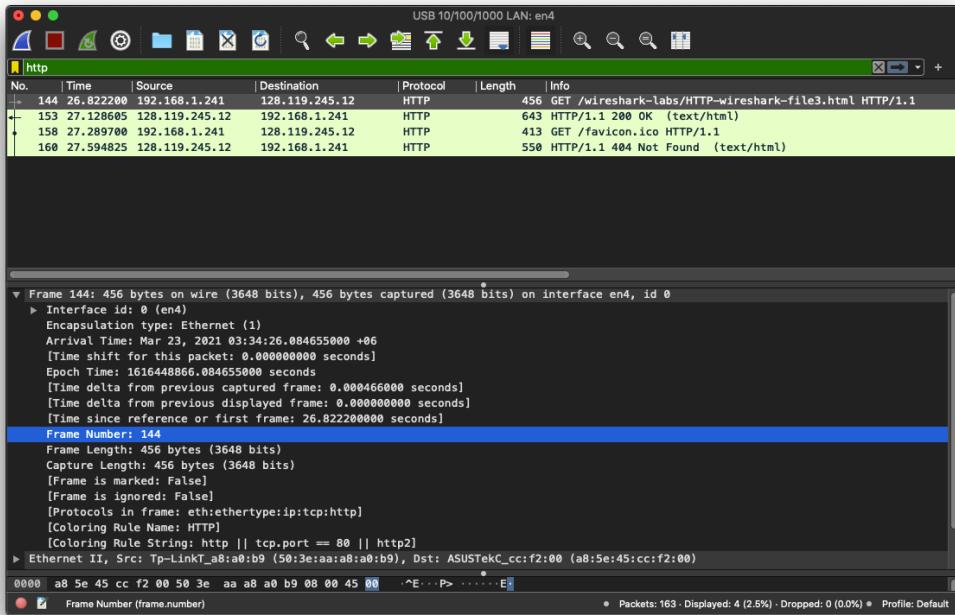
**Figure 3:** Wireshark Display after <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html> has been retrieved by browser

MD. ABU YOUSUF SAJAL

ID : 17.01.04.025

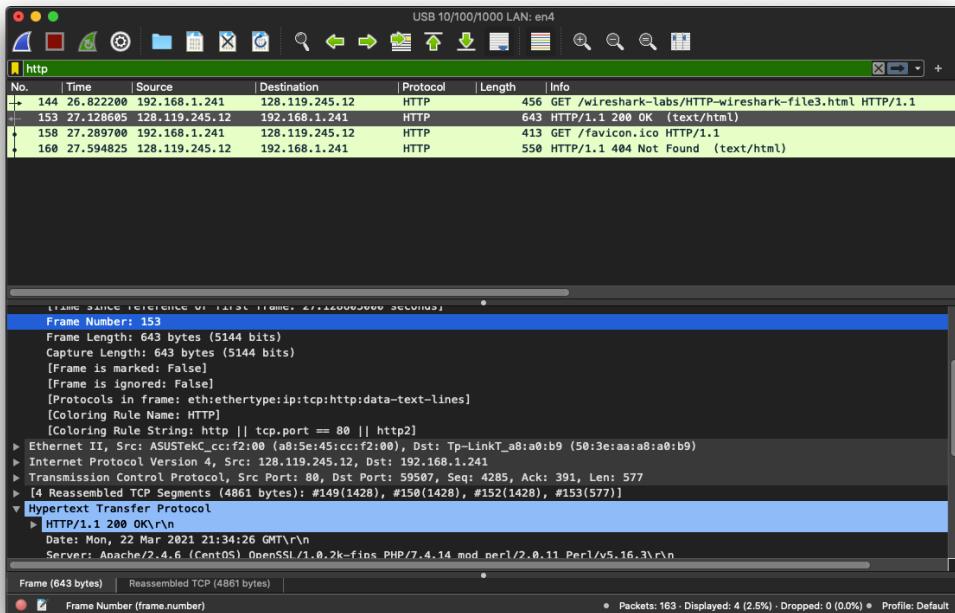
12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

**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

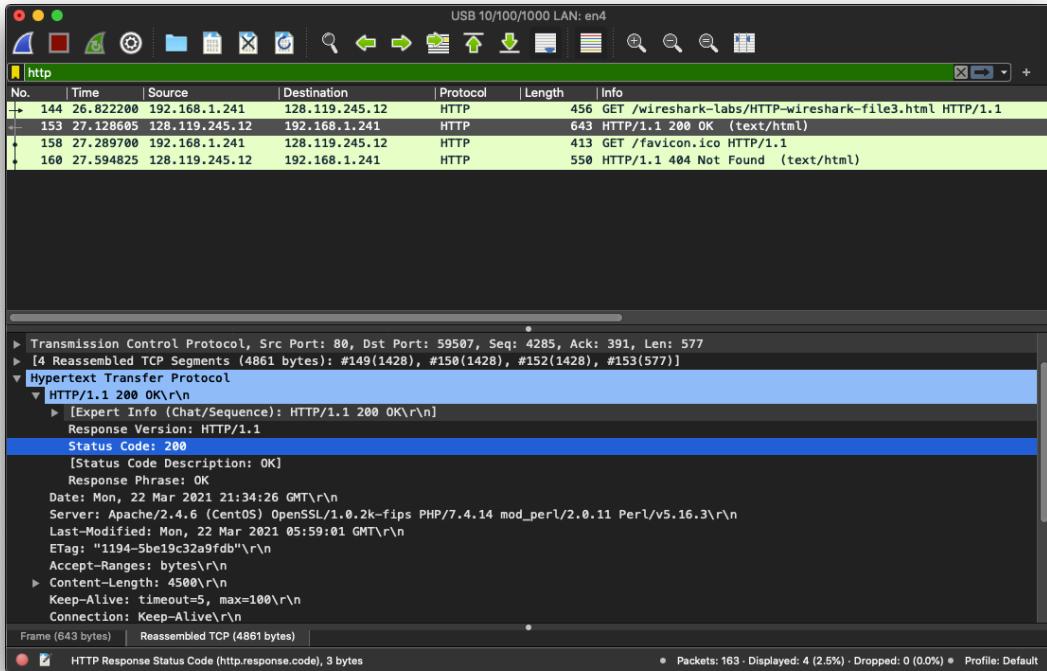
ID : 17.01.04.025

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

**Answer :**

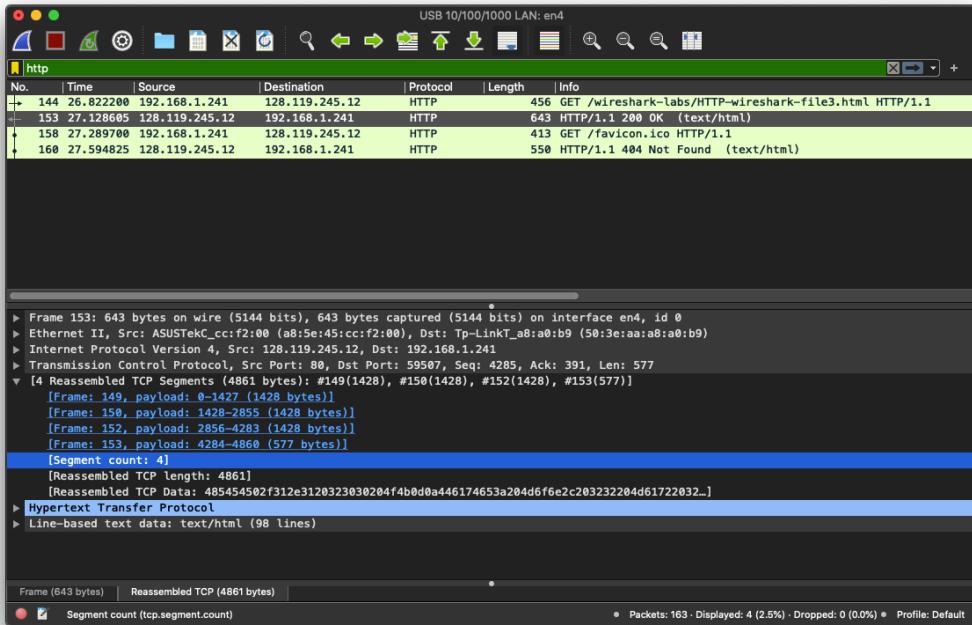
Status Code : **200**

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

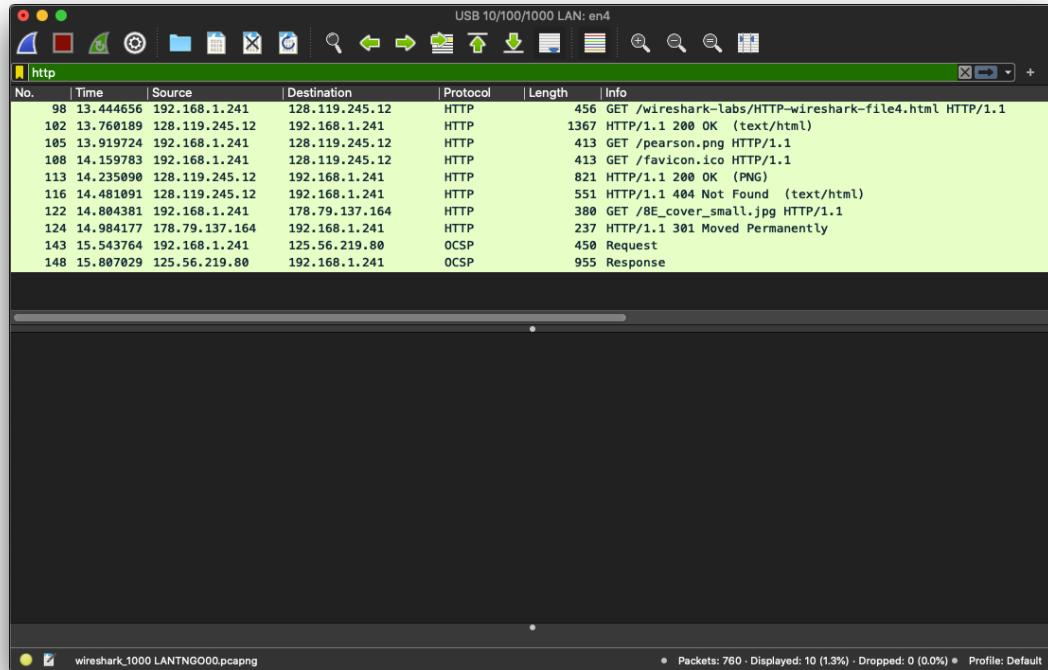


15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

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



## 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

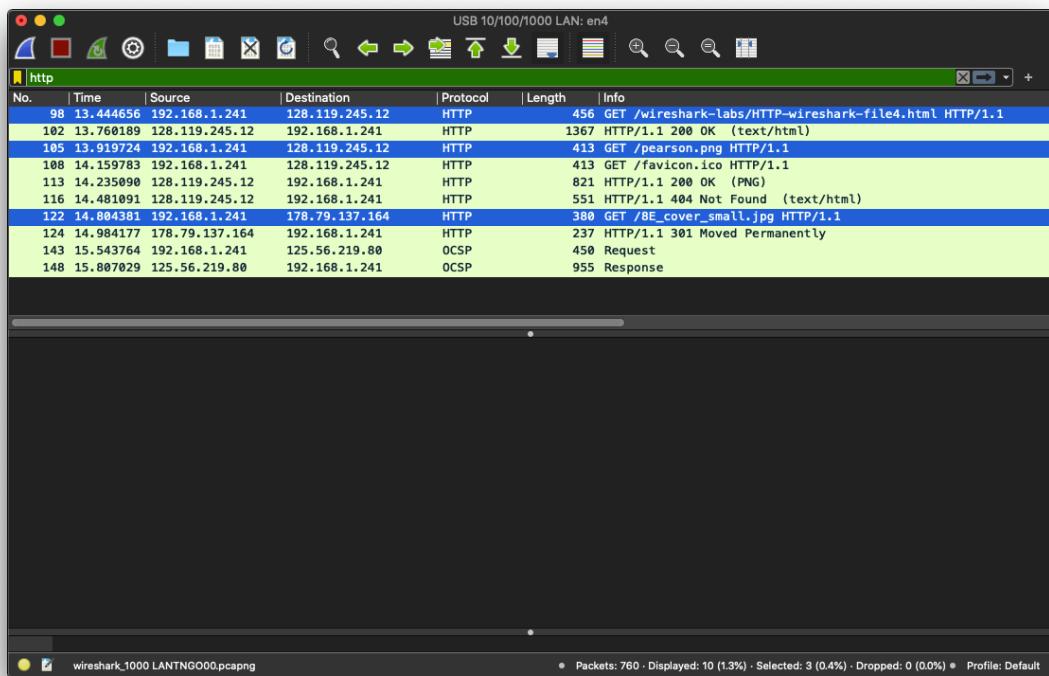
ID : 17.01.04.025

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

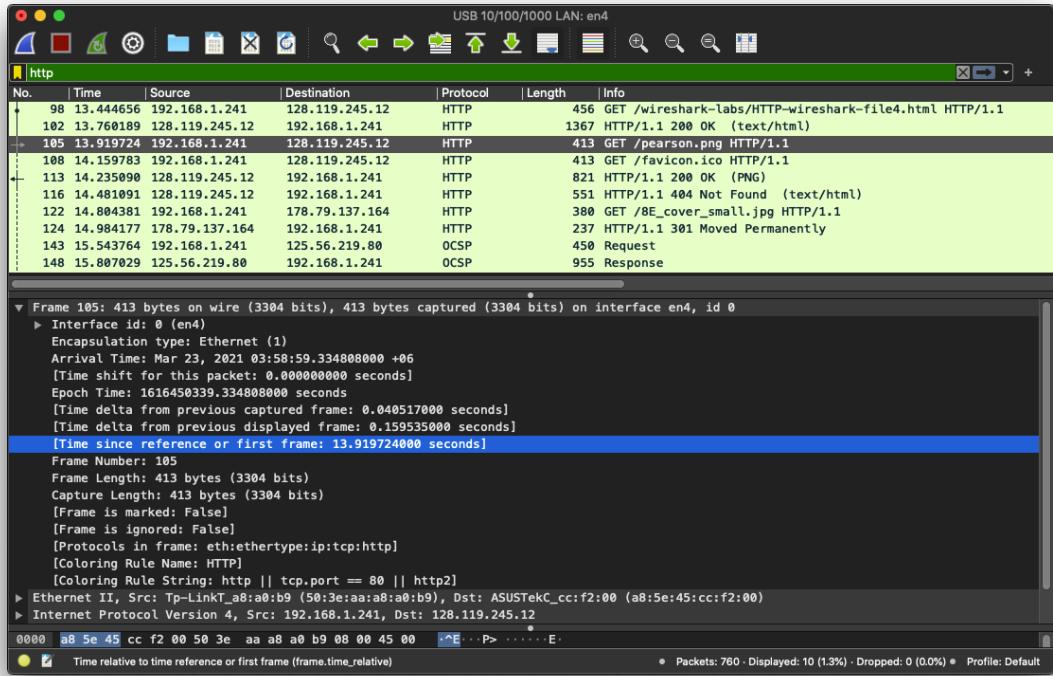


17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

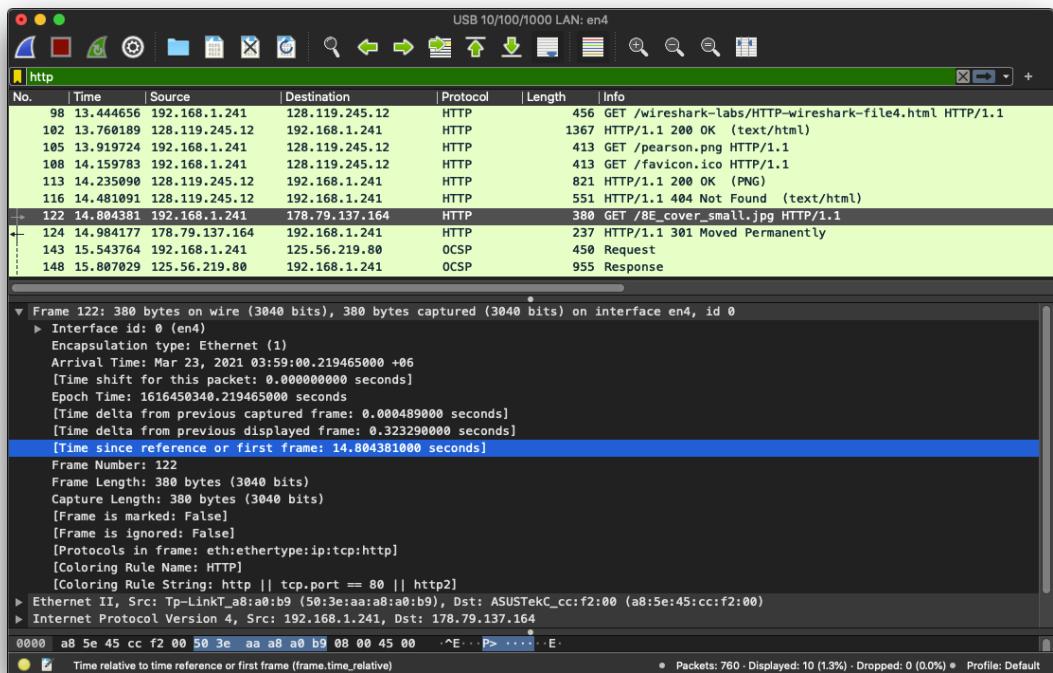
**Answer :** Browser downloaded the two images serially. The first image “*person.png*” was requested at **(13.919724000 sec)** since first frame and the second image “*8E\_cover\_small.jpg*” was requested at **(14.804381000 sec)** since first frame. So, there is a time difference of **(0.0884657 sec)**.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

MD. ABU YOUSUF SAJAL  
ID : 17.01.04.025

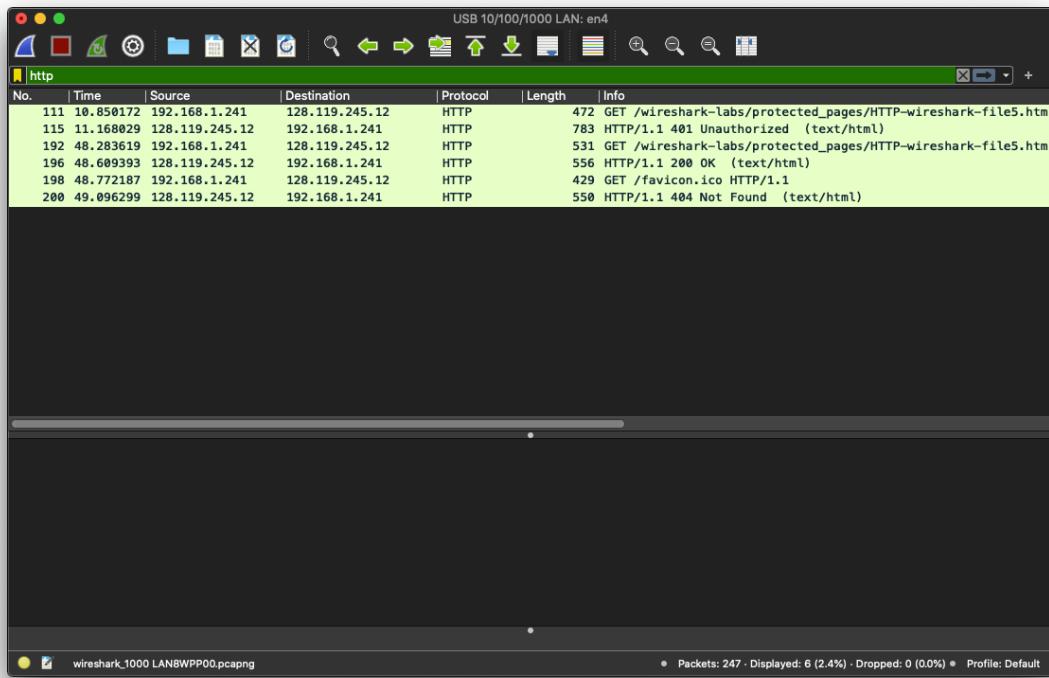
First Image Requested Time : [Mar 23, 2021 03:58:59.334808000 +06]



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



## 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?

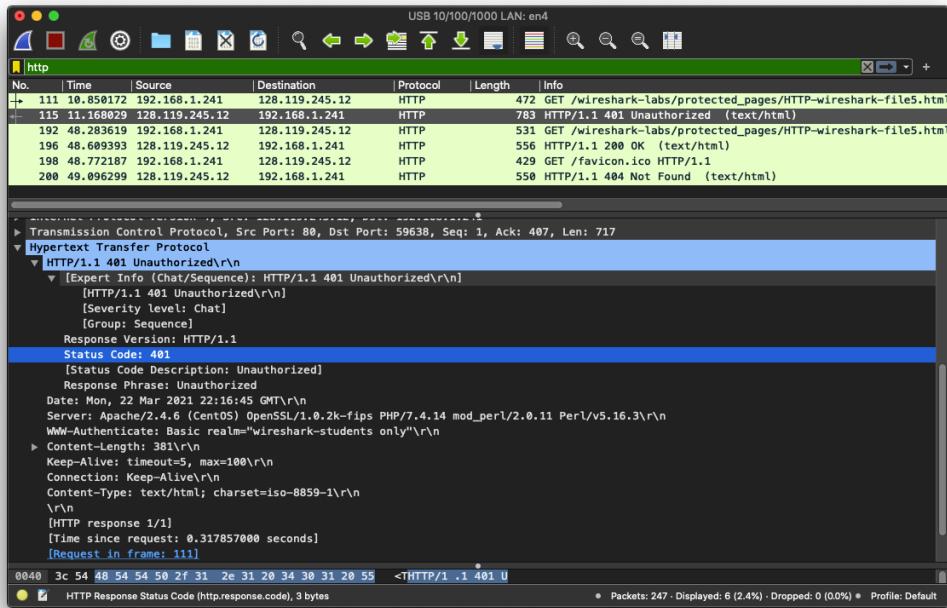
**Answer :**

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

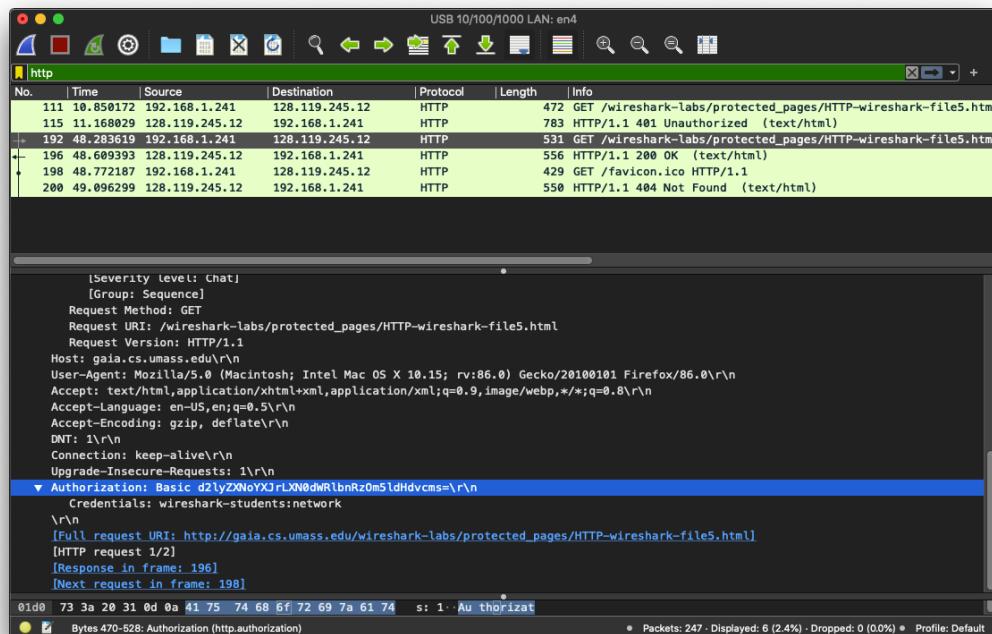
ID : 17.01.04.025



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.



## **Resources :-**

*All the capture packets link given below,*

[Task 1](#)

[Task 2](#)

[Task 3](#)

[Task 4](#)

[Task 5](#)