Questions:

The Basic HTTP GET/response interaction

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

   Ans: 1.1

```
    TCP payload (488 bytes)
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Sat, 30 Jan 2021 21:43:30 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: Sat, 30 Jan 2021 06:59:02 GMT\r\n
```

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

```
User-Agent: Mozilla/5.0 (Macintosh; 
Accept: text/html,application/xhtml+x
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
\r\n
```

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

Source	Destination
128.119.245.12	10.0.0.44
10.0.0.44	128.119.245.12

   Ans :
   10.0.0.44 128.119.245.12
4. What is the status code returned from the server to your browser?
   Ans: 200

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

   Ans: `Last-Modified: Sat, 30 Jan 2021 06:59:02 GMT\r\n`

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

   Ans: `Content-Length: 128\r\n` 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.
   Ans: Yes, there are extra headers in the raw data that are not displayed in the packet-listing window. For example:

   `Connection: Keep-Alive\r\n`

The HTTP CONDITIONAL GET/response interaction

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?
   Ans: There is **no** "If-Modified-Since" line….
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Ans:

```
\n
<html>\n
\n
Congratulations again!  Now you've downloaded the file lab2-2.html. <br>\n
This file's last modification date will not change.  <p>\n
Thus  if you download this multiple times on your browser, a complete copy <br>\n
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
field in your browser's HTTP GET request to the server.\n
\n
</html>\n
```

```
▸ Content-Length: 371\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
  [Request in frame: 56]
  [Time since request: 0.024609000 seconds]
  [Request URI: /wireshark-labs/HTTP-wireshark-file2.html]
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
  File Data: 371 bytes
```

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 GET6? If so, what information follows the “IF-MODIFIED-SINCE:” header?

Ans :

```
If-None-Match: "173-5ba18a7e1ba7e"\r\n
If-Modified-Since: Sat, 30 Jan 2021 06:59:02 GMT\r\n
```

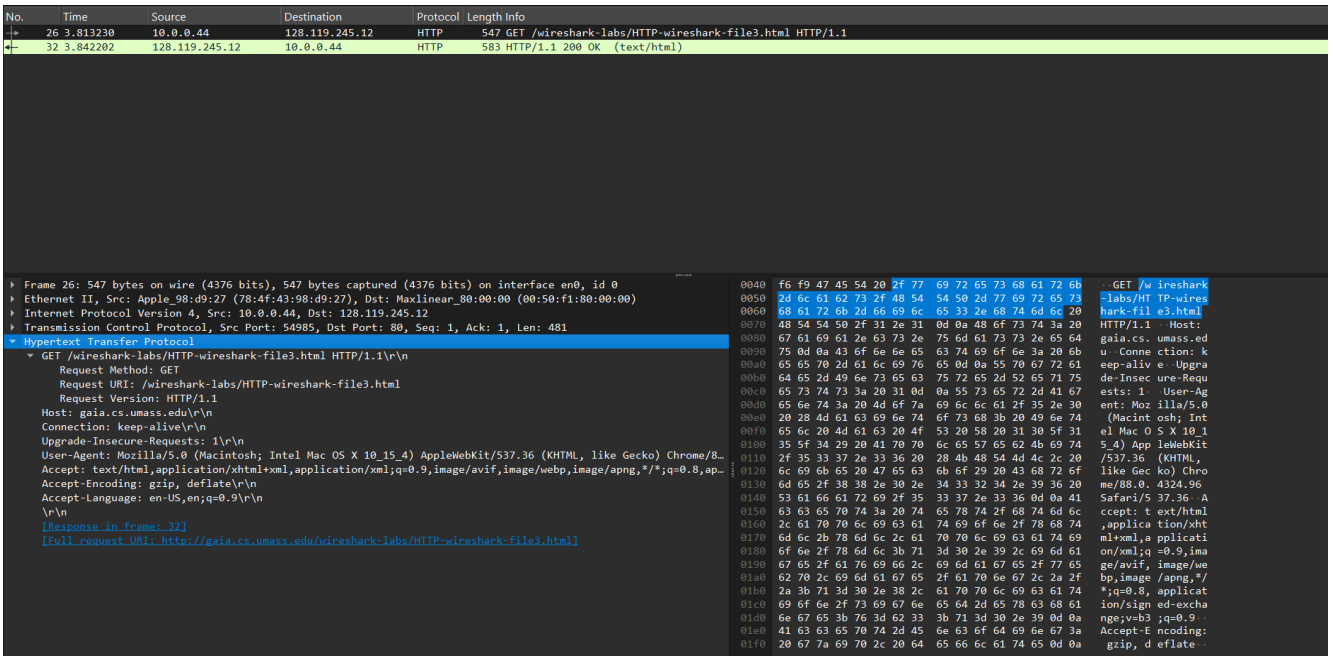
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

Ans:

```
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 304 Not Modified\r\n
    Date: Sat, 30 Jan 2021 18:19:56 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
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=99\r\n
    ETag: "173-5ba18a7e1ba7e"\r\n
    \r\n
    [Request in frame: 555]
    [Time since request: 0.022630000 seconds]
    [Request URI: /wireshark-labs/HTTP-wireshark-file2.html]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

304 Not Modified. The server did **not** return the file contents

Retrieving Long Documents



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?

Ans: 1…..26

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

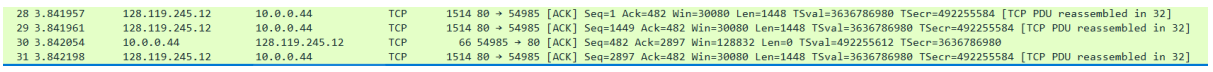
Ans : 32

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

Ans: 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?

Ans: 3(28, 29, 31)



HTML Documents with Embedded Objects

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

Ans: There are 4 HTTP GET request messages. These requests are sent to the IP address :

1. 178.79.137.164
2. 104.98.115.146
3. 128.119.245.12

No.	Time	Source	Destination	Protocol	Length	Info
118	3.309908	10.0.0.44	178.79.137.164	HTTP	500	GET /8E_cover_small.jpg HTTP/1.1
144	3.757683	10.0.0.44	104.98.115.146	HTTP	361	GET /MFgwVqADAgEAME8wTTBLMAkGBSsOAwIaBQAEFEja
99	3.072335	10.0.0.44	128.119.245.12	HTTP	493	GET /pearson.png HTTP/1.1
95	3.018199	10.0.0.44	128.119.245.12	HTTP	547	GET /wireshark-labs/HTTP-wireshark-file4.html

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

Ans:

99	3.072335	10.0.0.44	128.119.245.12	HTTP	493	GET /pearson.png HTTP/1.1
104	3.092770	128.119.245.12	10.0.0.44	HTTP	781	HTTP/1.1 200 OK (PNG)
118	3.309908	10.0.0.44	178.79.137.164	HTTP	500	GET /8E_cover_small.jpg HTTP/1.1
120	3.451822	178.79.137.164	10.0.0.44	HTTP	237	HTTP/1.1 301 Moved Permanently

Serially. As the GET request for the second image (packet 118 at 3.309s) was sent after the 200 OK response for the first image (packet 104 at 3.092s) was received.

HTTP Authentication:

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

Ans: There are two response packets: 482 and 94

The response in packet 482 is:

```
▾ Hypertext Transfer Protocol
  ▾ HTTP/1.1 200 OK\r\n
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
```

Packet 482

The server responded with status code 200 and phrase OK

The response in packet 94 is:

```
▾ Hypertext Transfer Protocol
  ▾ HTTP/1.1 401 Unauthorized\r\n
      Response Version: HTTP/1.1
      Status Code: 401
      [Status Code Description: Unauthorized]
      Response Phrase: Unauthorized
```

Packet 94

The server responded with status code 401 and phrase "Unauthorized"

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

Ans:

```
▾ Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    Credentials: wireshark-students:network
```