1. Do the Wireshark exercise found here, which will introduce you to the Wireshark tool:
    1. List 3 different protocol s that appear in the protocol column in the unfiltered packet-listing window in step 7 above.
        i. HTTP
        ii. UDP
        iii. ARP
    2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received?
        i. .29384sec
    3. What is the internet address of the gaia.cs.umass.edu? What is the internet address of your computer?
        i. Gaia.cs.umass.edu
            1. 129.119.245.12
        ii. Mine:
            1. 128.61.88.199
    4. Print the two HTTP messages (GET and OK) referred to in question 2 above.

C:\Users\BALKRI~1\AppData\Local\Temp\wireshark_C2084376-19DA-413B-BF6E-CD2464678D80_20190126132839_a06244.pcapng 6257 total packets, 14 shown

```
No.     Time              Source                Destination           Protocol Length Info
   2653 13:28:43.235469    128.61.88.199         128.119.245.12        HTTP     464    GET /wireshark-labs/INTRO-wireshark-
file1.html HTTP/1.1
Frame 2653: 464 bytes on wire (3712 bits), 464 bytes captured (3712 bits) on interface 0
Ethernet II, Src: AsustekC_c7:e1:6d (08:62:66:c7:e1:6d), Dst: Cisco_eb:f1:80 (68:ef:bd:eb:f1:80)
Internet Protocol Version 4, Src: 128.61.88.199, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 56879, Dst Port: 80, Seq: 1, Ack: 1, Len: 410
Hypertext Transfer Protocol
No.     Time              Source                Destination           Protocol Length Info
   2675 13:28:43.264853    128.119.245.12        128.61.88.199         HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 2675: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface 0
Ethernet II, Src: Cisco_eb:f1:80 (68:ef:bd:eb:f1:80), Dst: AsustekC_c7:e1:6d (08:62:66:c7:e1:6d)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 128.61.88.199
Transmission Control Protocol, Src Port: 80, Dst Port: 56879, Seq: 1, Ack: 411, Len: 438
Hypertext Transfer Protocol
Line-based text data: text/html (3 lines)
    <html>\n
    Congratulations!  You've downloaded the first Wireshark lab file!\n
    </html>\n
```

2.

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
    i. My Browser: HTTP 1.1
    ii. Server: HTTP 1.1
    iii. Marked in Red
2. What languages (if any) does your browser indicate that it can accept to the server?
    i. Accept-Language: en-US\r\n
    ii. Marked in Yellow
3. What is the IP address of your computer? Or the gaia.cs.umass.edu server?
    i. Me: 128.61.88.199
    ii. Sever: 128.119.245.12
    iii. Marked in Green
4. What is the status code returned from the server to your browser?
    i. 202 OK
    ii. Marked in Blue
5. When was the HTML file that you are retrieving last modified at the server?
    i. Sat, 26 Jan 2019 06:59:01 GMT\r\n
    ii. Marked in Orange
6. How many bytes of content are being returned to your browser?
    i. File Data: 128 bytes
    ii. Marked in Purple
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.
    i. All the data can be found in the raw data.

```
No.     Time                Source                Destination           Protocol Length Info
  11267 14:07:39.380829     128.61.88.199         128.119.245.12        HTTP     463    GET /wireshark-labs/HTTP-wireshark-file1.html
HTTP/1.1
Frame 11267: 463 bytes on wire (3704 bits), 463 bytes captured (3704 bits) on interface 0
Ethernet II, Src: AsustekC_c7:e1:6d (08:62:66:c7:e1:6d), Dst: Cisco_eb:f1:80 (68:ef:bd:eb:f1:80)
Internet Protocol Version 4, Src: 128.61.88.199, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 57174, Dst Port: 80, Seq: 1, Ack: 1, Len: 409
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
        Request Method: GET
        Request URI: /wireshark-labs/HTTP-wireshark-file1.html
        Request Version: HTTP/1.1
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36
Edge/17.17134\r\n
    Accept-Language: en-US\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept-Encoding: gzip, deflate\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 11293]
No.     Time                Source                Destination           Protocol Length Info
  11293 14:07:39.410214     128.119.245.12        128.61.88.199         HTTP     540    HTTP/1.1 200 OK (text/html)
Frame 11293: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
Ethernet II, Src: Cisco_eb:f1:80 (68:ef:bd:eb:f1:80), Dst: AsustekC_c7:e1:6d (08:62:66:c7:e1:6d)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 128.61.88.199
Transmission Control Protocol, Src Port: 80, Dst Port: 57174, Seq: 1, Ack: 410, Len: 486
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Sat, 26 Jan 2019 19:07:39 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Sat, 26 Jan 2019 06:59:01 GMT\r\n
    ETag: "80-58056fa809ef3"\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 1/1]
    [Time since request: 0.029385000 seconds]
    [Request in frame: 11267]
    File Data: 128 bytes
Line-based text data: text/html (4 lines)
```

8. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?
    i. No
9. Did the server explicitly return the contents of the file? How can you tell?
    i. Yes last line of the server’s first response has the line “Line-based text data”
    ii. Marked in Blue

```
No.     Time              Source                Destination           Protocol Length Info
   2910 16:02:51.235161    128.119.245.12        128.61.88.199         HTTP     784    HTTP/1.1 200 OK  (text/html)
Frame 2910: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface 0
Ethernet II, Src: Cisco_eb:f1:80 (68:ef:bd:eb:f1:80), Dst: AsustekC_c7:e1:6d (08:62:66:c7:e1:6d)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 128.61.88.199
Transmission Control Protocol, Src Port: 80, Dst Port: 57712, Seq: 1, Ack: 410, Len: 730
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Sat, 26 Jan 2019 21:02:51 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Sat, 26 Jan 2019 06:59:01 GMT\r\n
    ETag: "173-58056fa80933b"\r\n
    Accept-Ranges: bytes\r\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
    [HTTP response 1/2]
    [Time since request: 0.029583000 seconds]
    [Request in frame: 2900]
    [Next request in frame: 4021]
    [Next response in frame: 4035]
    File Data: 371 bytes
Line-based text data: text/html (10 lines)
```

10. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so what information follows the “IF-MODIFIED-SINCE:” head?
    i. Yes that follows the header is: Sat, 26 Jan 2019 06:59:01 GMT\r\n
    ii. Marked in Blue

```
No.     Time              Source                Destination           Protocol Length Info
   2704 17:25:30.285957    128.61.88.199         128.119.245.12        HTTP     591    GET /wireshark-labs/HTTP-wireshark-file2.html
HTTP/1.1
Frame 2704: 591 bytes on wire (4728 bits), 591 bytes captured (4728 bits) on interface 0
Ethernet II, Src: AsustekC_c7:e1:6d (08:62:66:c7:e1:6d), Dst: Cisco_eb:f1:80 (68:ef:bd:eb:f1:80)
Internet Protocol Version 4, Src: 128.61.88.199, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 54227, Dst Port: 80, Seq: 426, Ack: 731, Len: 537
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
        Request Method: GET
        Request URI: /wireshark-labs/HTTP-wireshark-file2.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    If-None-Match: "173-58056fa80933b"\r\n
    If-Modified-Since: Sat, 26 Jan 2019 06:59:01 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 2/2]
    [Prev request in frame: 1301]
    [Response in frame: 2722]
```

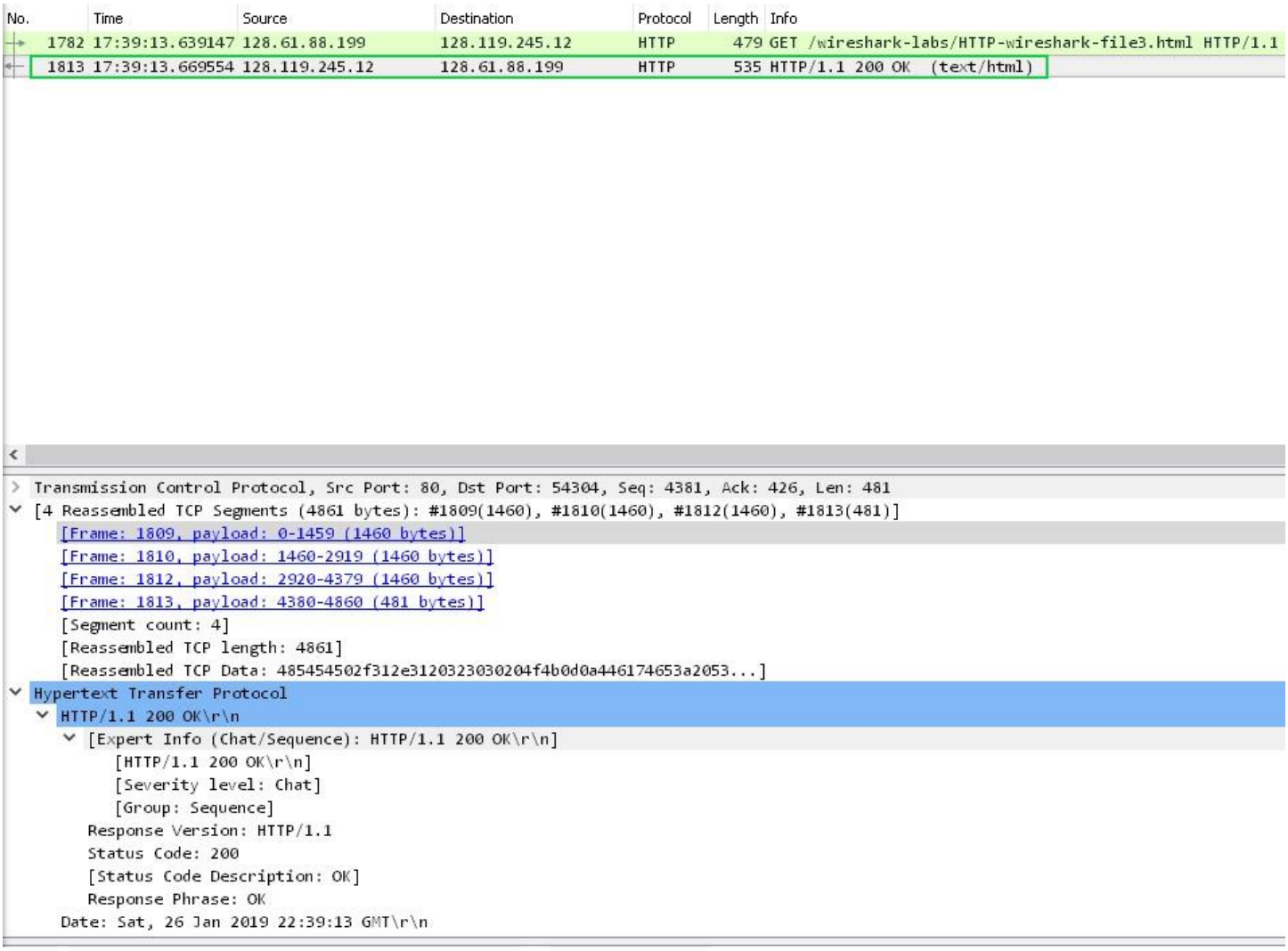
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.
    i. The status code is: 304 Not Modified
    ii. The server did not explicitly return the contents of the files as they were already loaded on to the browser's cache.
    iii. Marked in Green

```
No.     Time              Source                Destination           Protocol Length Info
   2722 17:25:30.314809    128.119.245.12        128.61.88.199         HTTP     293    HTTP/1.1 304 Not Modified
Frame 2722: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface 0
Ethernet II, Src: Cisco_eb:f1:80 (68:ef:bd:eb:f1:80), Dst: AsustekC_c7:e1:6d (08:62:66:c7:e1:6d)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 128.61.88.199
Transmission Control Protocol, Src Port: 80, Dst Port: 54227, Seq: 731, Ack: 963, Len: 239
Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
        Response Version: HTTP/1.1
        Status Code: 304
        [Status Code Description: Not Modified]
        Response Phrase: Not Modified
    Date: Sat, 26 Jan 2019 22:25:30 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=99\r\n
    ETag: "173-58056fa80933b"\r\n
    \r\n
    [HTTP response 2/2]
    [Time since request: 0.028852000 seconds]
    [Prev request in frame: 1301]
    [Prev response in frame: 1320]
    [Request in frame: 2704]
```

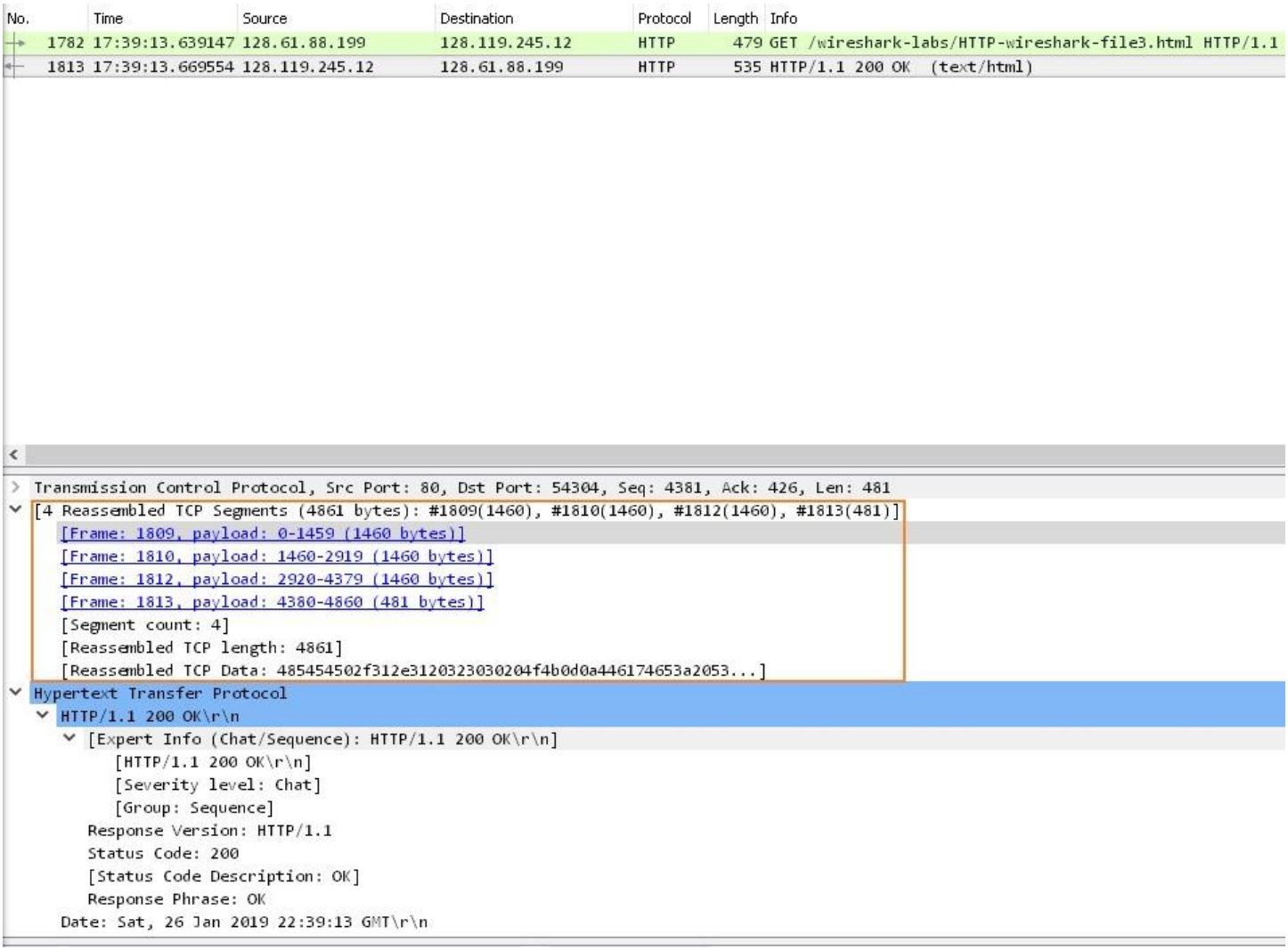
12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the Get message for the Bill of Rights?
    i. One GET request was sent
    ii. Packet no: 1782
    iii. Marked in Red

```
No.     Time              Source          Destination     Protocol Length Info
   1782 17:39:13.639147 128.61.88.199   128.119.245.12  HTTP     479    GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
   1813 17:39:13.669554 128.119.245.12  128.61.88.199   HTTP     535    HTTP/1.1 200 OK  (text/html)
```

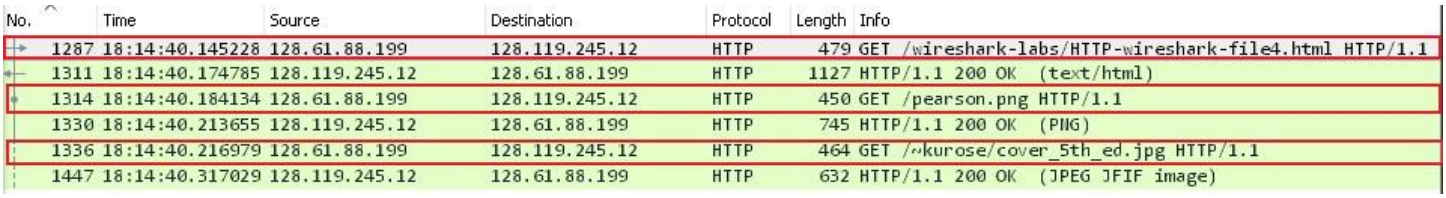
13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?
    i. Packet No. 1813 contains 200 OK
    ii. Marked in Green




14. What is the status code and phrase in the response?
    i. The status code: 200
    ii. Phrase: OK
    iii. The previous screen shot has the status code and phrase marked in green.
15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?
    i. 4 segments were needed
    ii. Marked in Orange



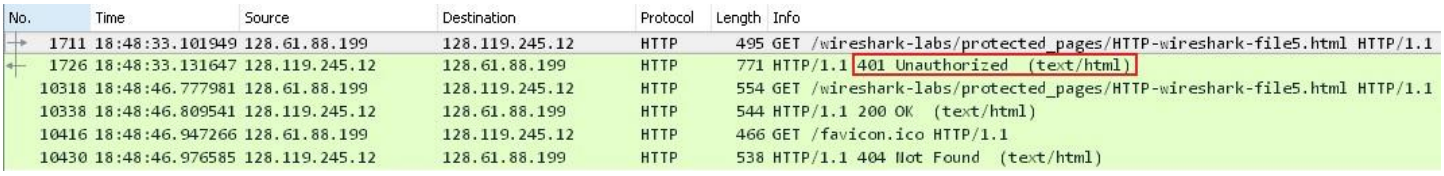

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?
    i. 3 HTTP GET request messages
    ii. All 3 requests were sent to: 128.119.245.12
    iii. Marked in Red




17. Can you tell whether your browser download the two images serially, or whether they were downloaded from the two websites in parallel? Explain.
    i. The images were downloaded serially, because the images were transmitted through two separate TCP connections.
    ii. Marked in Yellow

```
No.     Time              Source                Destination           Protocol Length Info
   2054 18:37:53.295383    128.119.245.12        128.61.88.199         HTTP     745    HTTP/1.1 200 OK  (PNG)
Frame 2054: 745 bytes on wire (5960 bits), 745 bytes captured (5960 bits) on interface 0
Ethernet II, Src: Cisco_eb:f1:80 (68:ef:bd:eb:f1:80), Dst: AsustekC_c7:e1:6d (08:62:66:c7:e1:6d)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 128.61.88.199
Transmission Control Protocol, Src Port: 80, Dst Port: 54637, Seq: 3994, Ack: 822, Len: 691
    Source Port: 80
    Destination Port: 54637
    [Stream index: 19]
    [TCP Segment Len: 691]
    Sequence number: 3994    (relative sequence number)
    [Next sequence number: 4685    (relative sequence number)]
    Acknowledgment number: 822    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window size value: 245
    [Calculated window size: 31360]
    [Window size scaling factor: 128]
    Checksum: 0x9a0a [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
    [Timestamps]
    TCP payload (691 bytes)
    TCP segment data (691 bytes)
[3 Reassembled TCP Segments (3611 bytes): #2052(1460), #2053(1460), #2054(691)]
Hypertext Transfer Protocol
Portable Network Graphics
No.     Time              Source                Destination           Protocol Length Info
   2179 18:37:53.394850    128.119.245.12        128.61.88.199         HTTP     632    HTTP/1.1 200 OK  (JPEG JFIF image)
Frame 2179: 632 bytes on wire (5056 bits), 632 bytes captured (5056 bits) on interface 0
Ethernet II, Src: Cisco_eb:f1:80 (68:ef:bd:eb:f1:80), Dst: AsustekC_c7:e1:6d (08:62:66:c7:e1:6d)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 128.61.88.199
Transmission Control Protocol, Src Port: 80, Dst Port: 54639, Seq: 100741, Ack: 411, Len: 578
    Source Port: 80
    Destination Port: 54639
    [Stream index: 22]
    [TCP Segment Len: 578]
    Sequence number: 100741    (relative sequence number)
    [Next sequence number: 101319    (relative sequence number)]
    Acknowledgment number: 411    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window size value: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
    Checksum: 0x68d0 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
    [Timestamps]
    TCP payload (578 bytes)
    TCP segment data (578 bytes)
[70 Reassembled TCP Segments (101318 bytes): #2074(1460), #2075(1460), #2076(1460), #2077(1460), #2078(1460), #2079(1460), #2080(1460),
#2081(1460), #2083(1460), #2084(1460), #2098(1460), #2099(1460), #2100(1460), #2101(1460), #2102(1460), ]
Hypertext Transfer Protocol
JPEG File Interchange Format
```

18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?
    i. The server's response to the initial GET message is: 401 Unauthorized
    ii. Marked in Red



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1711 | 18:48:33.101949 | 128.61.88.199 | 128.119.245.12 | HTTP | 495 | GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1 |
| 1726 | 18:48:33.131647 | 128.119.245.12 | 128.61.88.199 | HTTP | 771 | HTTP/1.1 401 Unauthorized (text/html) |
| 10318 | 18:48:46.777981 | 128.61.88.199 | 128.119.245.12 | HTTP | 554 | GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1 |
| 10338 | 18:48:46.809541 | 128.119.245.12 | 128.61.88.199 | HTTP | 544 | HTTP/1.1 200 OK (text/html) |
| 10416 | 18:48:46.947266 | 128.61.88.199 | 128.119.245.12 | HTTP | 466 | GET /favicon.ico HTTP/1.1 |
| 10430 | 18:48:46.976585 | 128.119.245.12 | 128.61.88.199 | HTTP | 538 | HTTP/1.1 404 Not Found (text/html) |

19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?
    i. An authorization header is has been included with the Credentials that were inputted
    ii. Marked in Blue

```
No.     Time              Source                Destination           Protocol Length Info
  10318 18:48:46.777981    128.61.88.199         128.119.245.12        HTTP     554    GET /wireshark-labs/protected_pages/HTTP-
wireshark-file5.html HTTP/1.1
Frame 10318: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface 0
Ethernet II, Src: AsustekC_c7:e1:6d (08:62:66:c7:e1:6d), Dst: Cisco_eb:f1:80 (68:ef:bd:eb:f1:80)
Internet Protocol Version 4, Src: 128.61.88.199, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 49507, Dst Port: 80, Seq: 1, Ack: 1, Len: 500
Hypertext Transfer Protocol
    GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
        Credentials: wireshark-students:network
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
    [HTTP request 1/2]
    [Response in frame: 10338]
    [Next request in frame: 10416]
```