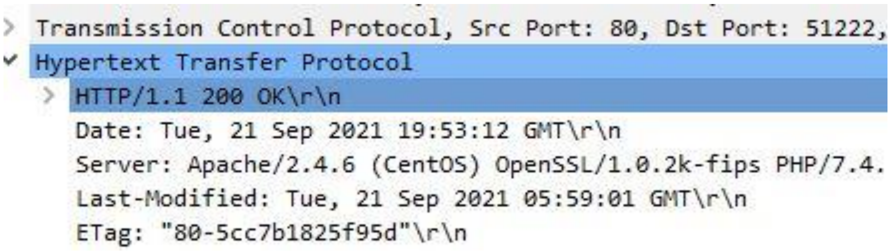
Wireshark 1

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

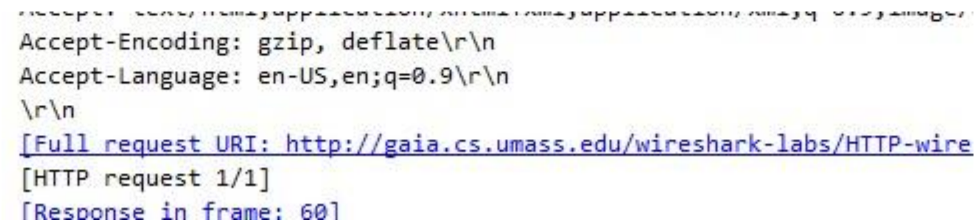
HTTP version 1.1. It is running HTTP version 1.1.



```
> Transmission Control Protocol, Src Port: 80, Dst Port: 51222,
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Tue, 21 Sep 2021 19:53:12 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.
    Last-Modified: Tue, 21 Sep 2021 05:59:01 GMT\r\n
    ETag: "80-5cc7b1825f95d"\r\n
```

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

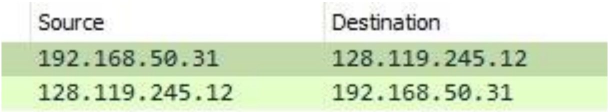
It will accept English-US and English languages.



```
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/HTTP-wire
[HTTP request 1/1]
[Response in frame: 60]
```

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

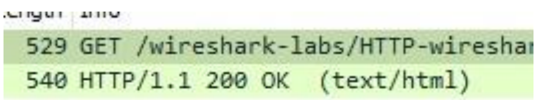
My computer: 192.168.50.31. Gaia.cs.umass.edu server: 128.119.245.12



Source	Destination
192.168.50.31	128.119.245.12
128.119.245.12	192.168.50.31

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

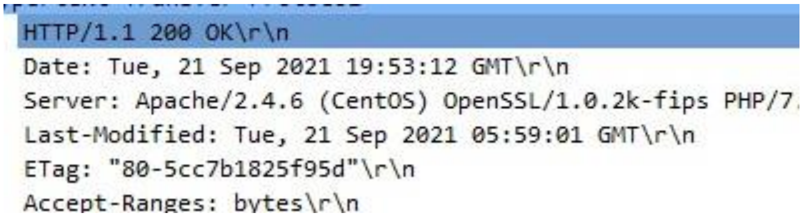
200 OK



```
529 GET /wireshark-labs/HTTP-wireshar
540 HTTP/1.1 200 OK  (text/html)
```

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

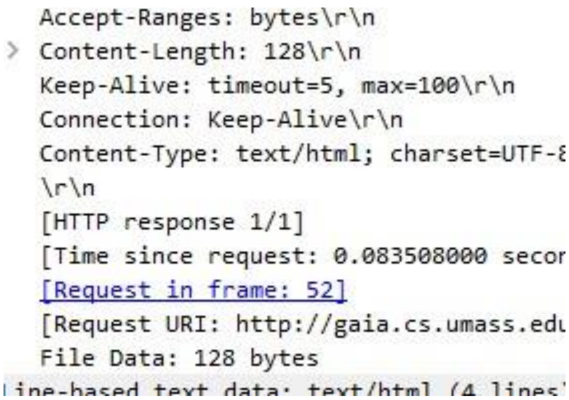
Tue, 21 Sep 2021 05:59:01 GMT



```
HTTP/1.1 200 OK\r\n
Date: Tue, 21 Sep 2021 19:53:12 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.
Last-Modified: Tue, 21 Sep 2021 05:59:01 GMT\r\n
ETag: "80-5cc7b1825f95d"\r\n
Accept-Ranges: bytes\r\n
```

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

128 bytes



```
   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
   [HTTP response 1/1]
   [Time since request: 0.083508000 secor
   [Request in frame: 52]
   [Request URI: http://gaia.cs.umass.edu
   File Data: 128 bytes
Line-based text data: text/html (4 lines
```

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 didn't see any different between the two.

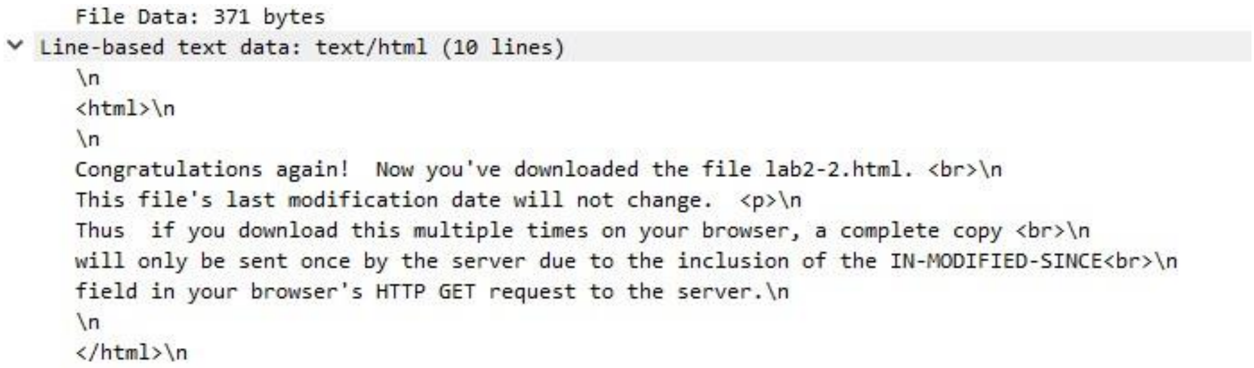
Wireshark 2

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 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?

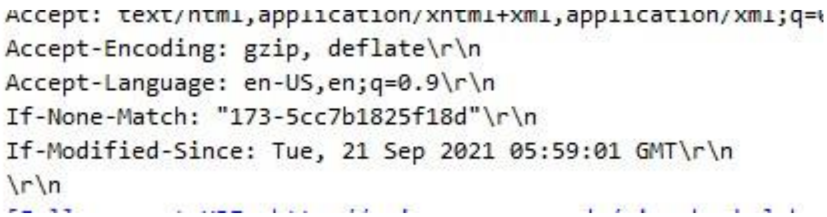
Wireshark has a section called "Line-based Text Data" which shows what the server returned, and which matched from the website I went on.



```
    File Data: 371 bytes
v Line-based text data: text/html (10 lines)
    \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
```

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?

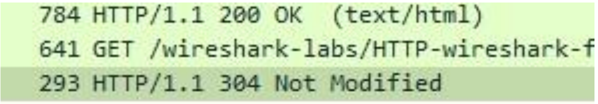
Yes, there is an if-modified-since line in the second HTTP GET request. The information I get is Tue, 21 Sep 2021 05:59:01 GMT.



```
Accept: text/html,application/xhtml+xml,application/xml;q=
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
If-None-Match: "173-5cc7b1825f18d"\r\n
If-Modified-Since: Tue, 21 Sep 2021 05:59:01 GMT\r\n
\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.

The status code is “304: Not Modified”. The server did not return the contents of the file because the browser just retrieved the contents from its cache instead.

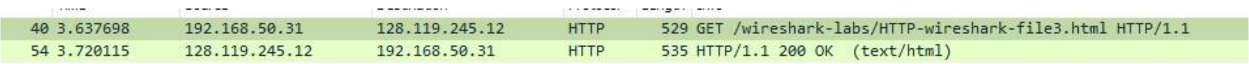


```
784 HTTP/1.1 200 OK  (text/html)
641 GET /wireshark-labs/HTTP-wireshark-f
293 HTTP/1.1 304 Not Modified
```

Wireshark 3

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?

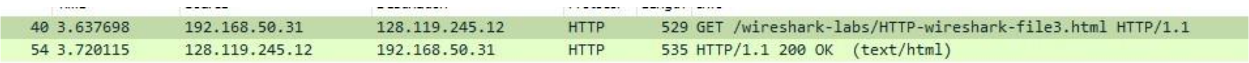
It only sent 1 GET request. The packet number is 40.



```
40 3.637698   192.168.50.31    128.119.245.12   HTTP    529 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
54 3.720115   128.119.245.12   192.168.50.31    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?

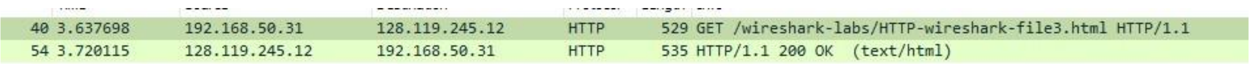
The packet number is 54.



```
40 3.637698   192.168.50.31    128.119.245.12   HTTP    529 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
54 3.720115   128.119.245.12   192.168.50.31    HTTP    535 HTTP/1.1 200 OK  (text/html)
```

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

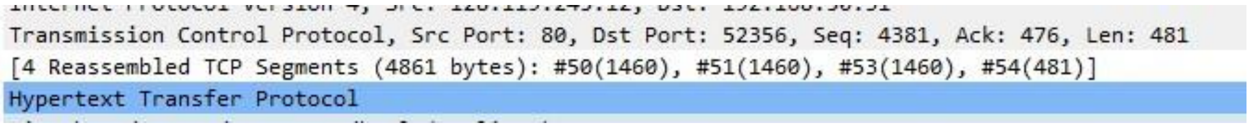
200 OK



```
40 3.637698   192.168.50.31    128.119.245.12   HTTP    529 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
54 3.720115   128.119.245.12   192.168.50.31    HTTP    535 HTTP/1.1 200 OK  (text/html)
```

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

It was sent in 4 Reassembled TCP segments.

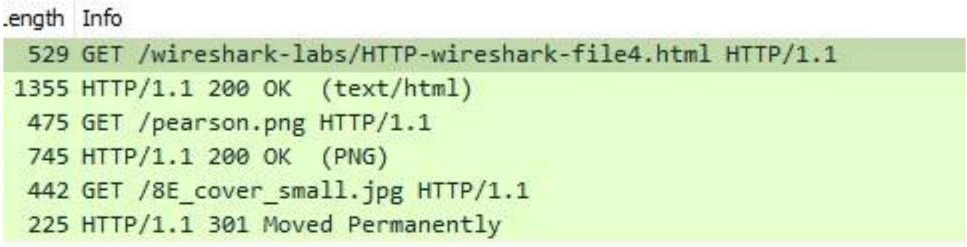


```
Transmission Control Protocol, Src Port: 80, Dst Port: 52356, Seq: 4381, Ack: 476, Len: 481
[4 Reassembled TCP Segments (4861 bytes): #50(1460), #51(1460), #53(1460), #54(481)]
Hypertext Transfer Protocol
```

Wireshark 4

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

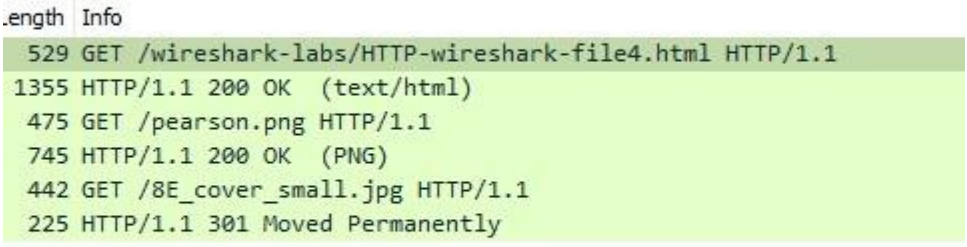
It sent 3 GET request. They were sent to 128.119.245.12, 128.119.245.12, 178.79.137.164.



```
.ength Info
  529 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
 1355 HTTP/1.1 200 OK  (text/html)
  475 GET /pearson.png HTTP/1.1
  745 HTTP/1.1 200 OK  (PNG)
  442 GET /8E_cover_small.jpg HTTP/1.1
  225 HTTP/1.1 301 Moved Permanently
```

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.

The browser downloaded the two images serially because the first images was first requested and sent and then the second one was requested and sent. If there were sent in parallel, they both would have been requested first then both would have sent after.

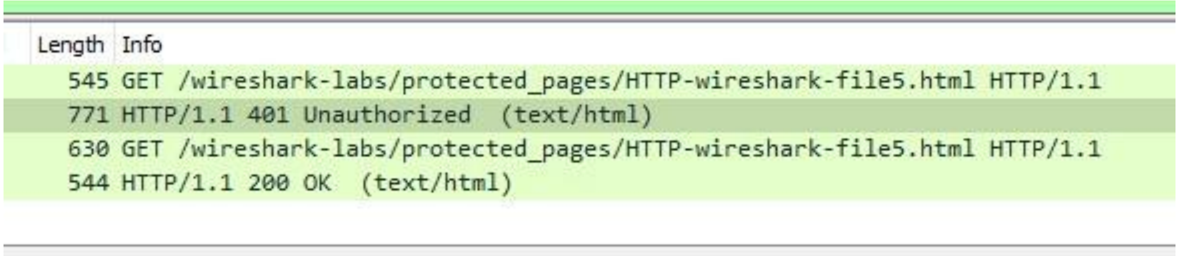


```
.ength Info
  529 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
 1355 HTTP/1.1 200 OK  (text/html)
  475 GET /pearson.png HTTP/1.1
  745 HTTP/1.1 200 OK  (PNG)
  442 GET /8E_cover_small.jpg HTTP/1.1
  225 HTTP/1.1 301 Moved Permanently
```

Wireshark 5

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

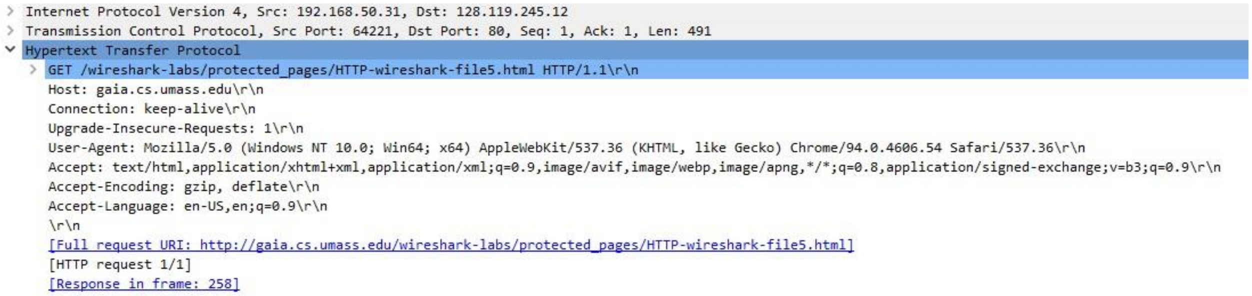
The initial response was “401 Unauthorized”.



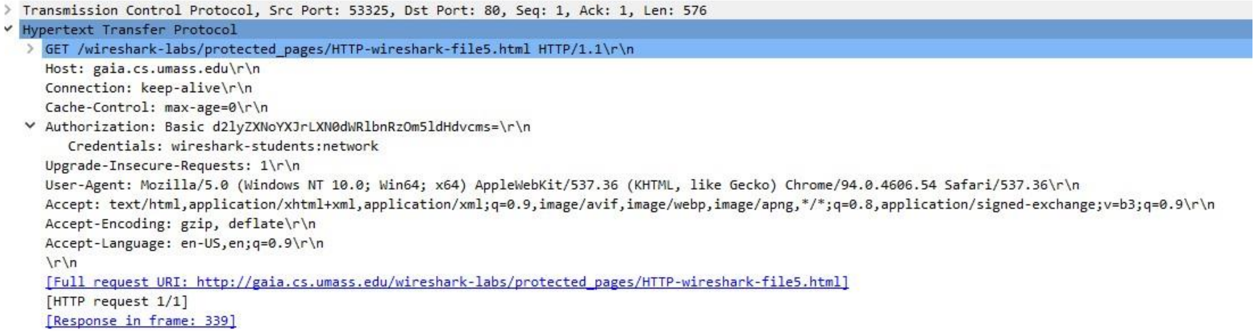
```
Length Info
   545 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
   771 HTTP/1.1 401 Unauthorized  (text/html)
   630 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
   544 HTTP/1.1 200 OK  (text/html)
```

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

The new field included is the Authorization field which contains the username and password. http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html



```
> Internet Protocol Version 4, Src: 192.168.50.31, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 64221, Dst Port: 80, Seq: 1, Ack: 1, Len: 491
v 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
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.54 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\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 1/1]
    [Response in frame: 258]
```



```
> Transmission Control Protocol, Src Port: 53325, Dst Port: 80, Seq: 1, Ack: 1, Len: 576
v 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
    Cache-Control: max-age=0\r\n
  v 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/94.0.4606.54 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\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 1/1]
    [Response in frame: 339]
```