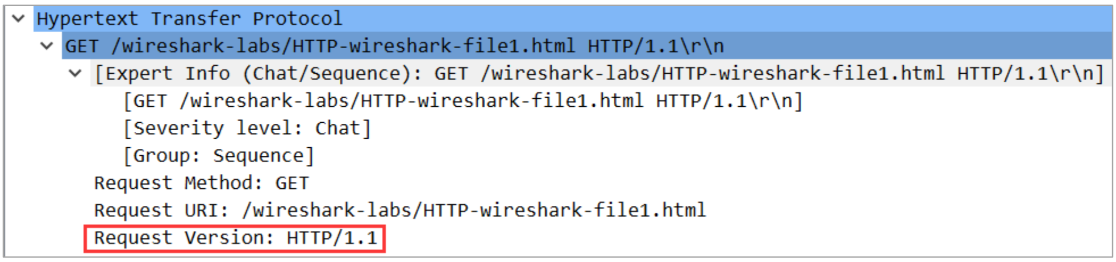
Wireshark Lab 2 – HTTP
Xiaoying Li

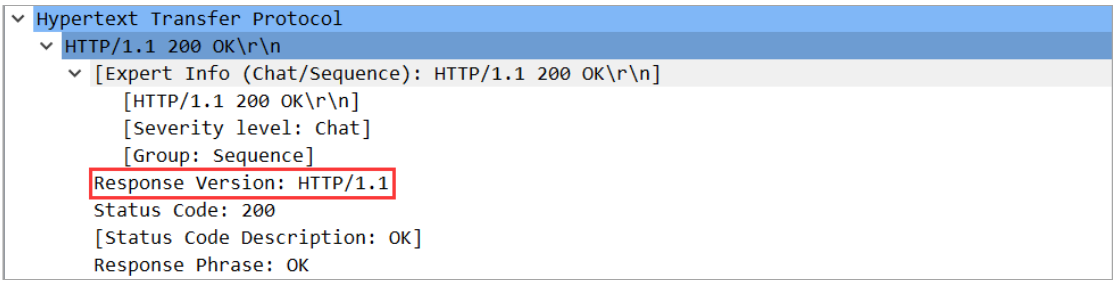
1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

HTTP version my browser is running: HTTP 1.1



```
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    v [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
        [GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
```

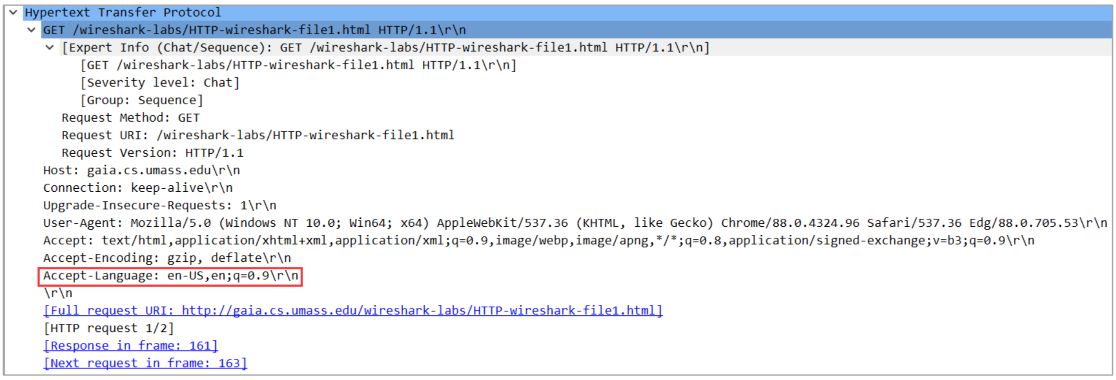
HTTP version the server is running: HTTP 1.1



```
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    v [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        [HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
```

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

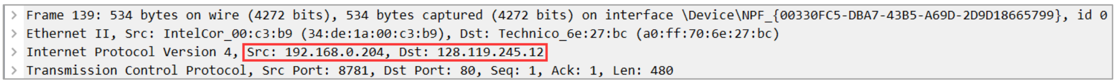
My browser indicates it can accept en-US (US English) and en (English).



```
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    v [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
        [GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
    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/88.0.4324.96 Safari/537.36 Edg/88.0.705.53\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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/HTTP-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 161]
    [Next request in frame: 163]
```

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

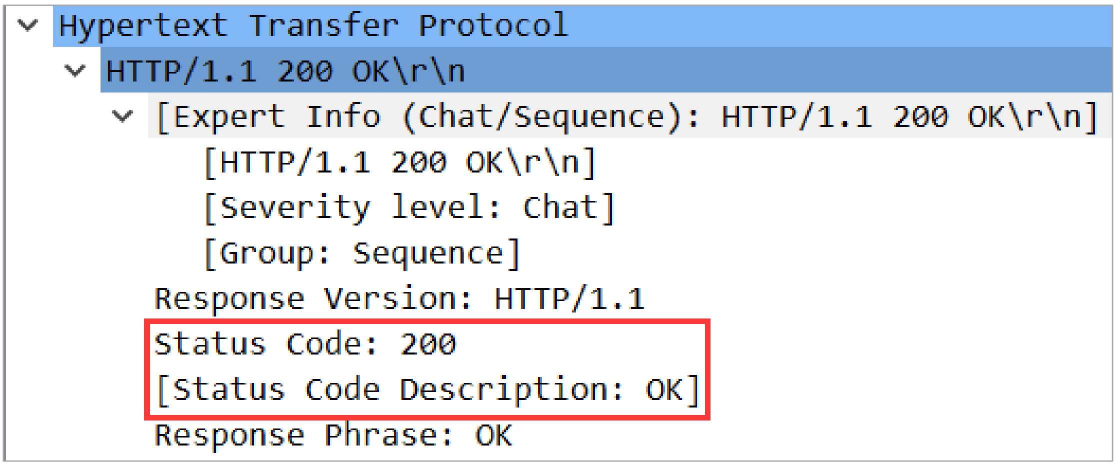
IP address of my computer: 192.168.0.204
IP address of the gaia.cs.umass.edu server: 128. 119.245.12



```
> Frame 139: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface \Device\NPF_{00330FC5-DBA7-43B5-A69D-2D9D18665799}, id 0
> Ethernet II, Src: IntelCor_00:c3:b9 (34:de:1a:00:c3:b9), Dst: Technico_6e:27:bc (a0:ff:70:6e:27:bc)
> Internet Protocol Version 4, Src: 192.168.0.204, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 8781, Dst Port: 80, Seq: 1, Ack: 1, Len: 480
```

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

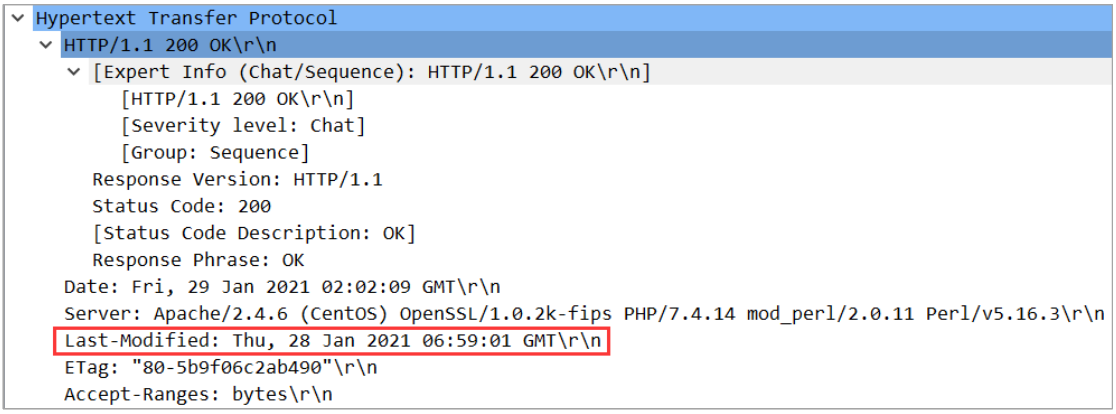
The status code returned from the server to my browser is 200.



```
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    v [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        [HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
```

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

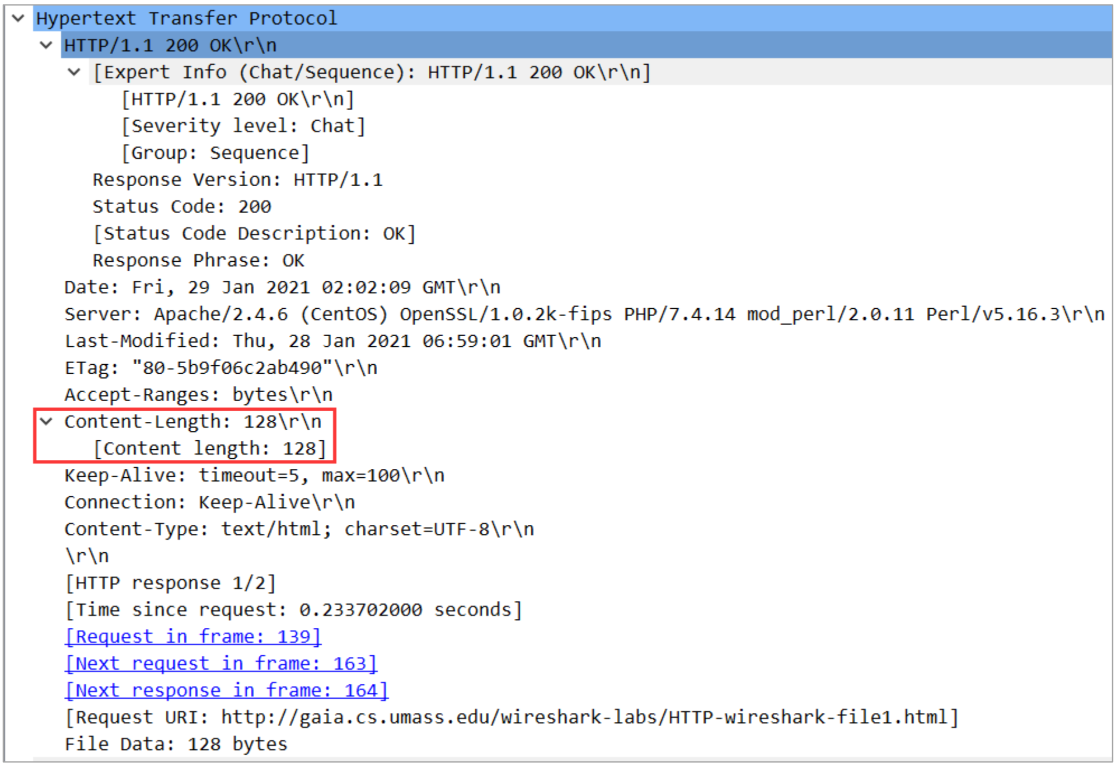
Time of the HTML file last modified at the server: Fri, 28 Jan 2021 06:59:01 GMT



```
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    v [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        [HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Fri, 29 Jan 2021 02:02:09 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: Thu, 28 Jan 2021 06:59:01 GMT\r\n
    ETag: "80-5b9f06c2ab490"\r\n
    Accept-Ranges: bytes\r\n
```

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

Bytes of content returned: 128



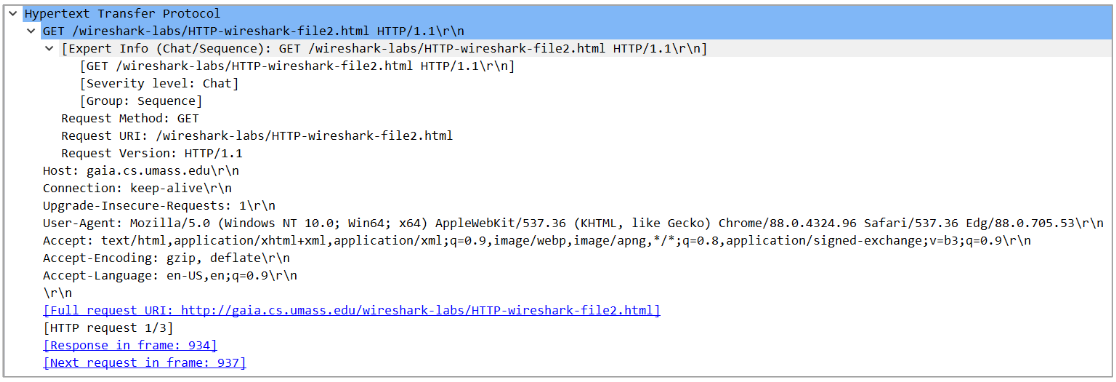
```
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    v [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        [HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Fri, 29 Jan 2021 02:02:09 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: Thu, 28 Jan 2021 06:59:01 GMT\r\n
    ETag: "80-5b9f06c2ab490"\r\n
    Accept-Ranges: bytes\r\n
  v Content-Length: 128\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]
    [Time since request: 0.233702000 seconds]
    [Request in frame: 139]
    [Next request in frame: 163]
    [Next response in frame: 164]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    File Data: 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.

No. I didn’t see any headers within the data that are not displayed in the packet-listing window.

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. I didn’t see an “IF-MODIFIED-SINCE” line in the HTTP GET.

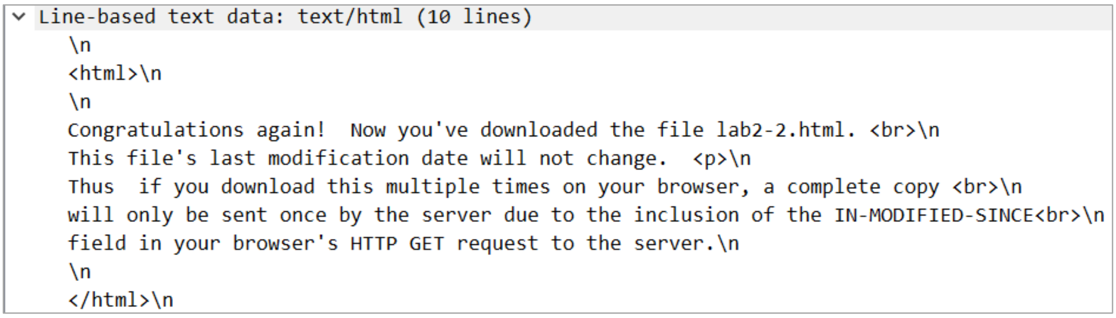


```
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
      [GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    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
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.96 Safari/537.36 Edg/88.0.705.53\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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/HTTP-wireshark-file2.html]
  [HTTP request 1/3]
  [Response in frame: 934]
  [Next request in frame: 937]
```

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

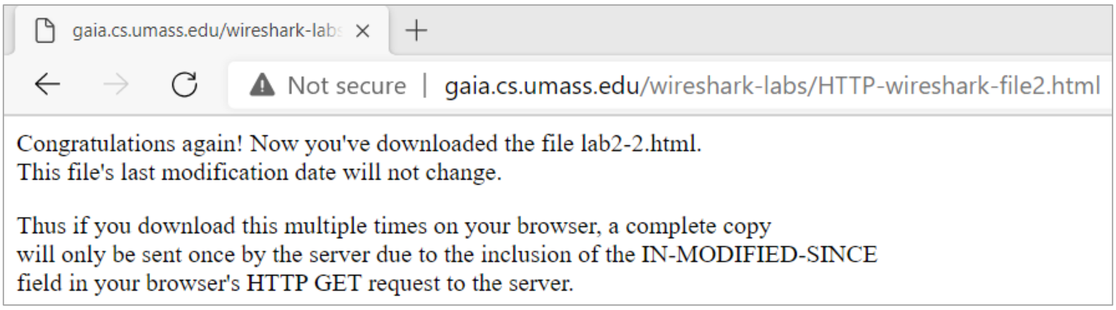
Yes. The server explicitly returned the contents of the file. I can tell this by the line-based text data of the HTTP OK reply to the HTTP GET request, which is same as the contents shown in the browser.

Wireshark:



```
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
```

Browser:

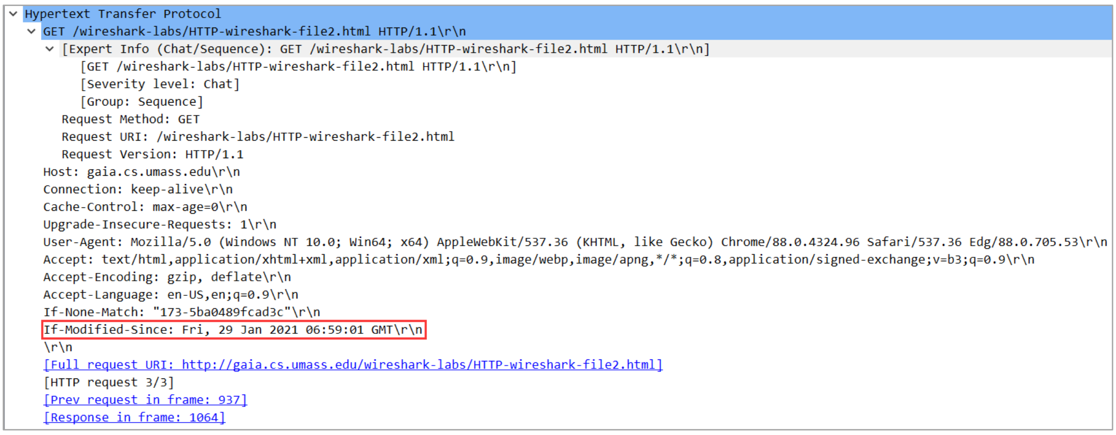

gaia.cs.umass.edu/wireshark-labs
Not secure | gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html

Congratulations again! Now you've downloaded the file lab2-2.html.
This file's last modification date will not change.

Thus if you download this multiple times on your browser, a complete copy
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE
field in your browser's HTTP GET request to the server.

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?

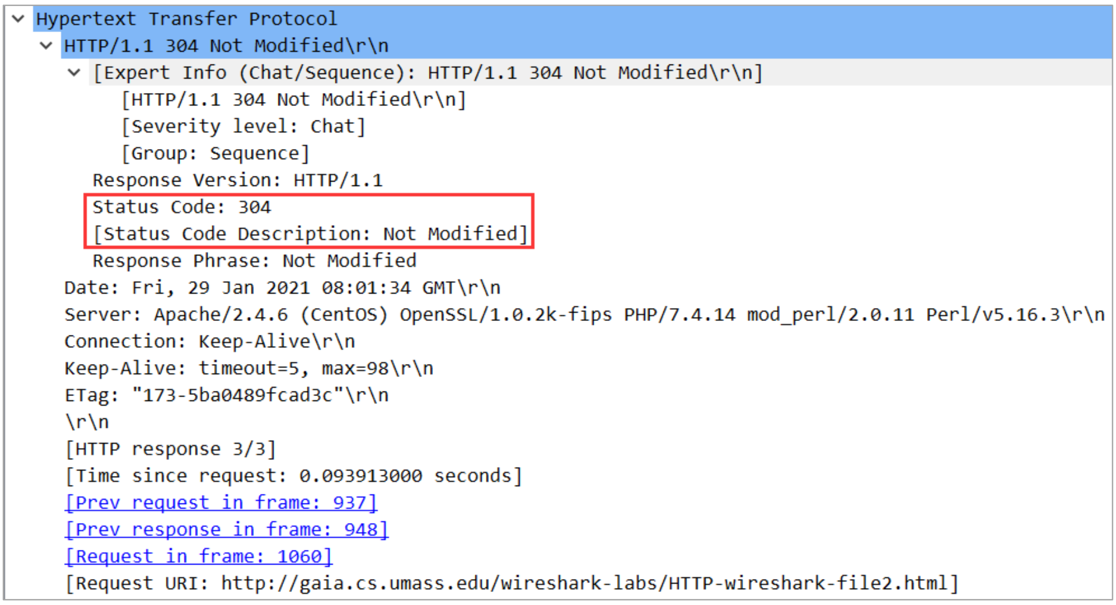
Yes. I see an “IF-MODIFIED-SINCE:” line in the HTTP GET. The information follows the “IF-MODIFIED-SINCE:” header is the last modification time of this file.



```
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    v [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
        [GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      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/88.0.4324.96 Safari/537.36 Edg/88.0.705.53\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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
    If-None-Match: "173-5ba0489fcad3c"\r\n
    If-Modified-Since: Fri, 29 Jan 2021 06:59:01 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 3/3]
    [Prev request in frame: 937]
    [Response in frame: 1064]
```

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.

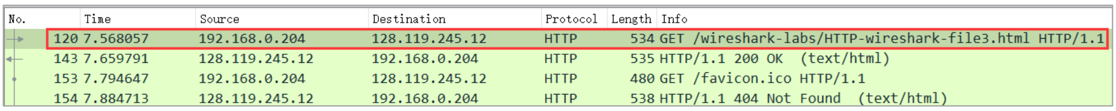
The HTTP status code and phrase returned from the server in response to this second HTTP GET is 304 Not Modified. The server did not explicitly return the contents of the file, because the file hadn’t been modified, so the browser loaded the contents from its cache and thus no content length was specified.



```
v Hypertext Transfer Protocol
  v HTTP/1.1 304 Not Modified\r\n
    v [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
        [HTTP/1.1 304 Not Modified\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 304
      [Status Code Description: Not Modified]
      Response Phrase: Not Modified
    Date: Fri, 29 Jan 2021 08:01:34 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=98\r\n
    ETag: "173-5ba0489fcad3c"\r\n
    \r\n
    [HTTP response 3/3]
    [Time since request: 0.093913000 seconds]
    [Prev request in frame: 937]
    [Prev response in frame: 948]
    [Request in frame: 1060]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

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?

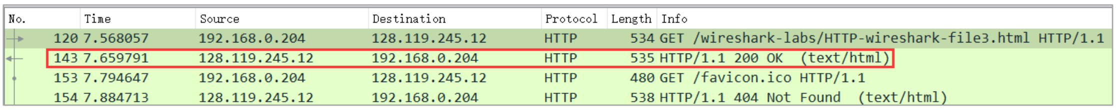
My browser sent only 1 HTTP GET request message. Packet number 120 in the trace contains the GET message for the Bill or Rights.



```
No.   Time        Source          Destination     Protocol Length Info
  120 7.568057    192.168.0.204   128.119.245.12  HTTP       534 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  143 7.659791    128.119.245.12  192.168.0.204   HTTP       535 HTTP/1.1 200 OK  (text/html)
  153 7.794647    192.168.0.204   128.119.245.12  HTTP       480 GET /favicon.ico HTTP/1.1
  154 7.884713    128.119.245.12  192.168.0.204   HTTP       538 HTTP/1.1 404 Not Found  (text/html)
```

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

Packet number 143 in the trace contains the status code and phrase associated with the response to the HTTP GET request.

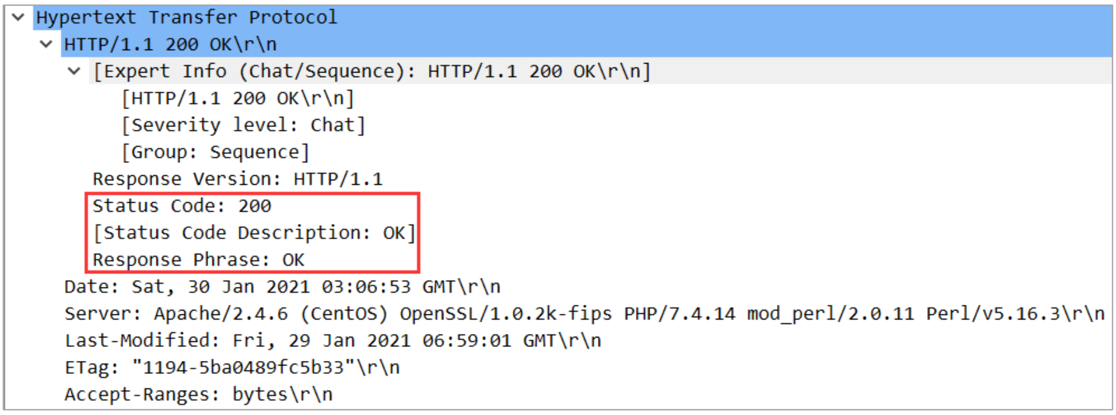


```
No.   Time        Source          Destination     Protocol Length Info
  120 7.568057    192.168.0.204   128.119.245.12  HTTP       534 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  143 7.659791    128.119.245.12  192.168.0.204   HTTP       535 HTTP/1.1 200 OK  (text/html)
  153 7.794647    192.168.0.204   128.119.245.12  HTTP       480 GET /favicon.ico HTTP/1.1
  154 7.884713    128.119.245.12  192.168.0.204   HTTP       538 HTTP/1.1 404 Not Found  (text/html)
```

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

Status code: 200

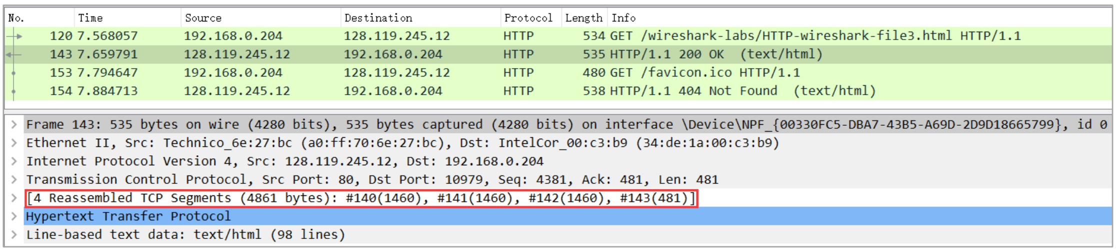
Phrase: OK



```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      [HTTP/1.1 200 OK\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
  Date: Sat, 30 Jan 2021 03:06:53 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: Fri, 29 Jan 2021 06:59:01 GMT\r\n
  ETag: "1194-5ba0489fc5b33"\r\n
  Accept-Ranges: bytes\r\n
```

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

4 data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights.

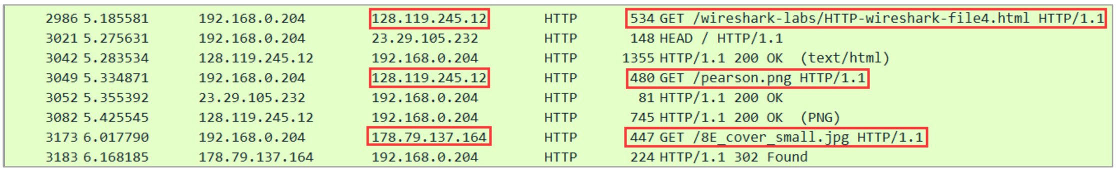


```
No.       Time        Source           Destination      Protocol  Length Info
    120 7.568057    192.168.0.204    128.119.245.12   HTTP        534 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
    143 7.659791    128.119.245.12   192.168.0.204    HTTP        535 HTTP/1.1 200 OK  (text/html)
    153 7.794647    192.168.0.204    128.119.245.12   HTTP        480 GET /favicon.ico HTTP/1.1
    154 7.884713    128.119.245.12   192.168.0.204    HTTP        538 HTTP/1.1 404 Not Found  (text/html)

> Frame 143: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{00330FC5-DBA7-43B5-A69D-2D9D18665799}, id 0
> Ethernet II, Src: Technico_6e:27:bc (a0:ff:70:6e:27:bc), Dst: IntelCor_00:c3:b9 (34:de:1a:00:c3:b9)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.204
> Transmission Control Protocol, Src Port: 80, Dst Port: 10979, Seq: 4381, Ack: 481, Len: 481
> [4 Reassembled TCP Segments (4861 bytes): #140(1460), #141(1460), #142(1460), #143(481)]
> Hypertext Transfer Protocol
> Line-based text data: text/html (98 lines)
```

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

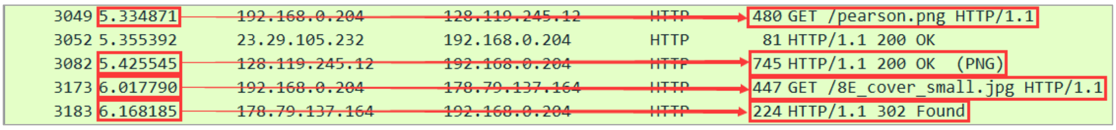
My browser sent 3 HTTP GET request messages. The first two GET requests were sent to 128.119.245.12, and the third one was sent to 178.79.137.164.



```
   2986 5.185581     192.168.0.204     128.119.245.12    HTTP     534 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
   3021 5.275631     192.168.0.204     23.29.105.232     HTTP     148 HEAD / HTTP/1.1
   3042 5.283534     128.119.245.12    192.168.0.204     HTTP    1355 HTTP/1.1 200 OK  (text/html)
   3049 5.334871     192.168.0.204     128.119.245.12    HTTP     480 GET /pearson.png HTTP/1.1
   3052 5.355392     23.29.105.232     192.168.0.204     HTTP      81 HTTP/1.1 200 OK
   3082 5.425545     128.119.245.12    192.168.0.204     HTTP     745 HTTP/1.1 200 OK  (PNG)
   3173 6.017790     192.168.0.204     178.79.137.164    HTTP     447 GET /8E_cover_small.jpg HTTP/1.1
   3183 6.168185     178.79.137.164    192.168.0.204     HTTP     224 HTTP/1.1 302 Found
```

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.

I think my browser downloaded the two images from two web sites serially. The order of two GET request messages and their responses from the server was "GET person.png → OK person.png → GET 8E_cover_small.jpg → OK 8E_cover_small.jpg", which indicated that the two images were downloaded serially.

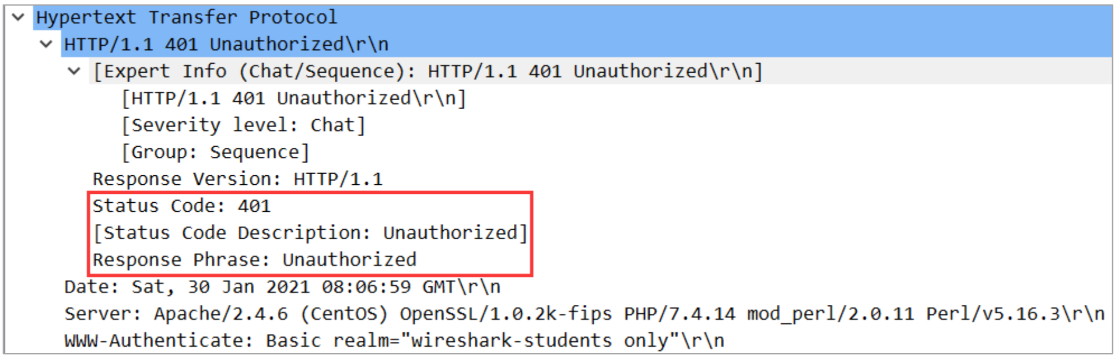


```
   3049 5.334871     192.168.0.204     128.119.245.12    HTTP     480 GET /pearson.png HTTP/1.1
   3052 5.355392     23.29.105.232     192.168.0.204     HTTP      81 HTTP/1.1 200 OK
   3082 5.425545     128.119.245.12    192.168.0.204     HTTP     745 HTTP/1.1 200 OK  (PNG)
   3173 6.017790     192.168.0.204     178.79.137.164    HTTP     447 GET /8E_cover_small.jpg HTTP/1.1
   3183 6.168185     178.79.137.164    192.168.0.204     HTTP     224 HTTP/1.1 302 Found
```

NOTE: The instructor answered in Piazza that the two images were downloaded in parallel and some students used Chrome or Firefox's developer tools to explain it. But I think we should answer this question based on Wireshark's result. If the right answer should be "in parallel", then I can only explain it by that the two GET request messages were sent very simultaneously based on Wireshark's result.

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

The server’s response to the initial HTTP GET message is 401 Unauthorized.

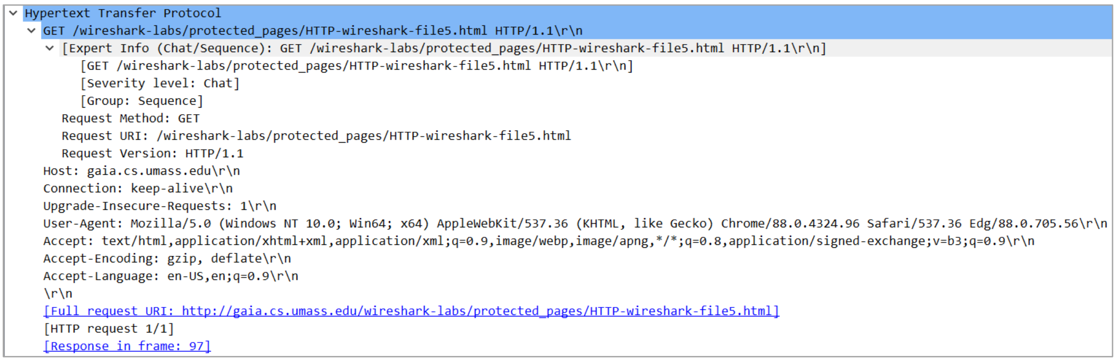


```
Hypertext Transfer Protocol
  HTTP/1.1 401 Unauthorized\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
      [HTTP/1.1 401 Unauthorized\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Response Version: HTTP/1.1
    Status Code: 401
    [Status Code Description: Unauthorized]
    Response Phrase: Unauthorized
  Date: Sat, 30 Jan 2021 08:06:59 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
  WWW-Authenticate: Basic realm="wireshark-students only"\r\n
```

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

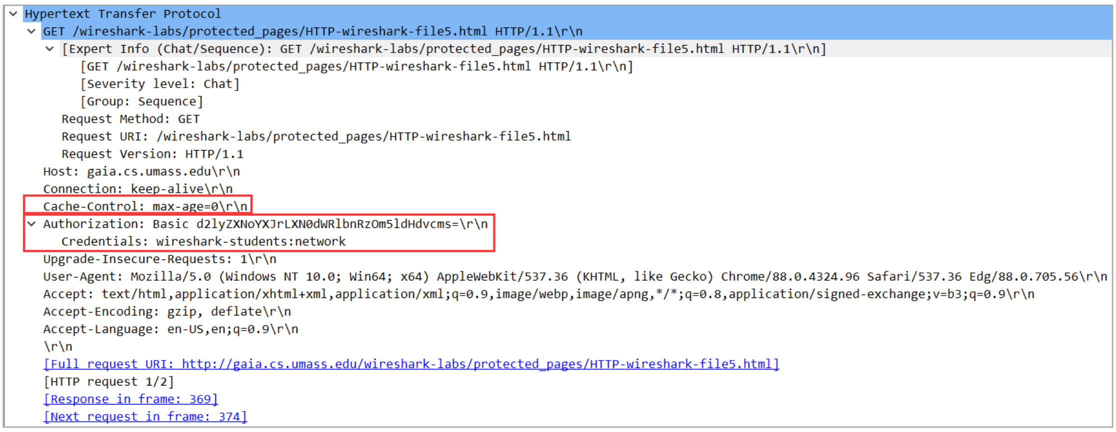
A new field “Authorization” is included in the second HTTP GET message. Also, a new field Cache-Control is included.

First HTTP GET message:



```
Hypertext Transfer Protocol
  GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
      [GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
    Request Version: HTTP/1.1
  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/88.0.4324.96 Safari/537.36 Edg/88.0.705.56\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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: 97]
```

Second HTTP GET message:



```
Hypertext Transfer Protocol
  GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
      [GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.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
  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/88.0.4324.96 Safari/537.36 Edg/88.0.705.56\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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 1/2]
  [Response in frame: 369]
  [Next request in frame: 374]
```