Lachlan Sinclair

Lab 02

10/23/2019

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

My browser is running HTTP 1.1

The server is running HTTP 1.1

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

en-US and en (US English and English).

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

192.168.0.19 is my computers IP.

128.119.245.12 is the servers IP.

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

Status code 200 OK

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

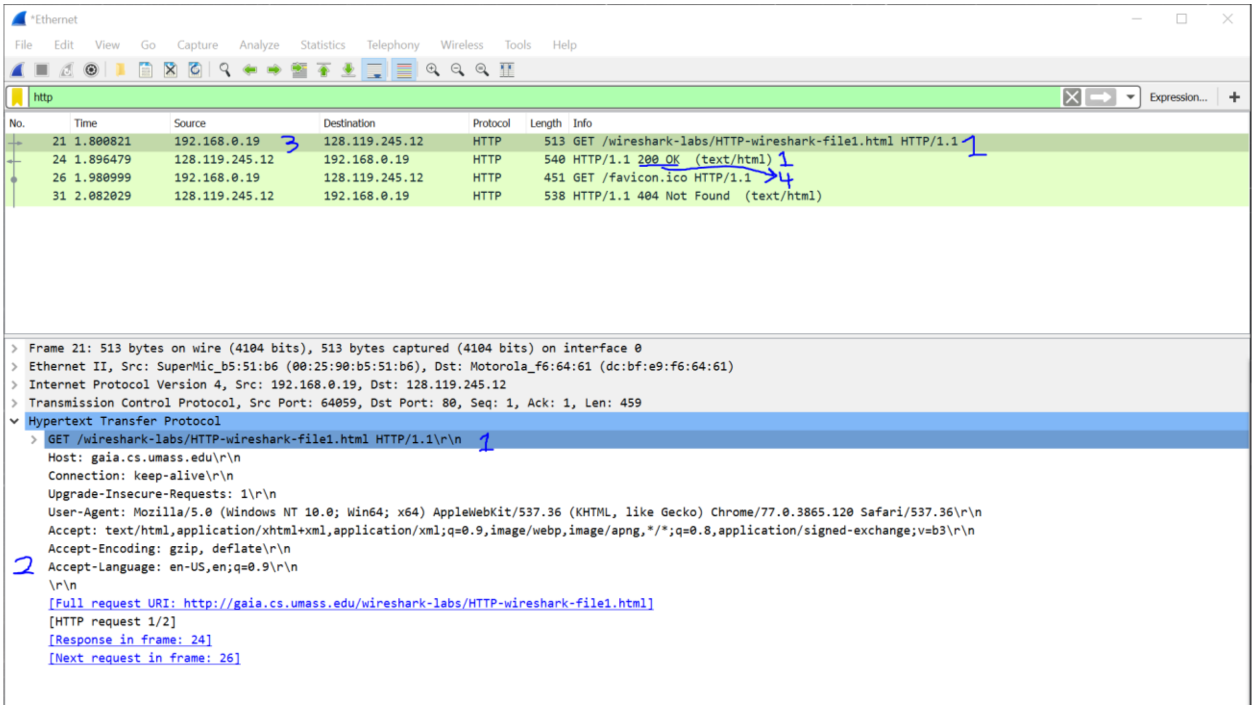
Last modified Thursday, 27 Oct 2019 05:59:02 GMT

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

128 bytes

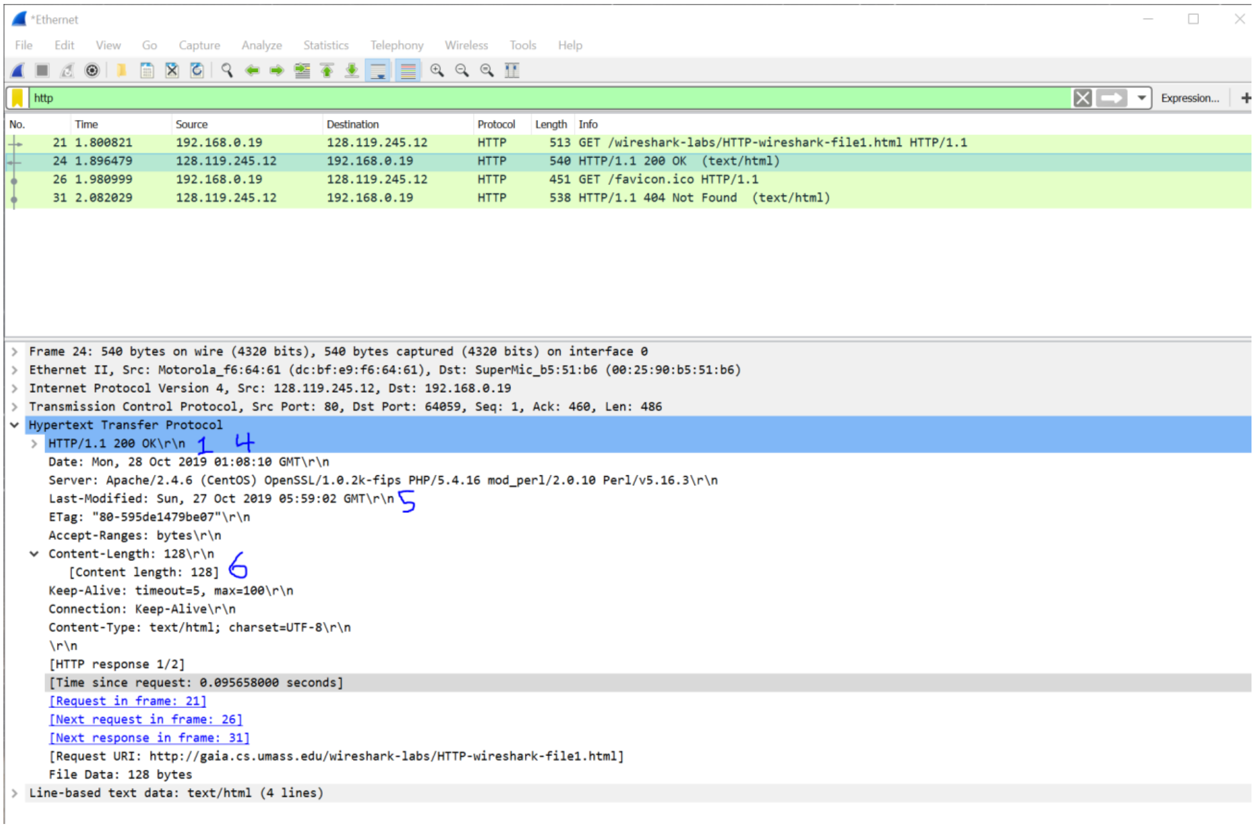
7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

No, I do not, all the headers within the data are displayed in the packet listing window.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
3
1
1
4
1
2

```
No.   Time        Source          Destination     Protocol  Length  Info
   21 1.800821    192.168.0.19    128.119.245.12  HTTP       513  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
   24 1.896479    128.119.245.12  192.168.0.19    HTTP       540  HTTP/1.1 200 OK  (text/html)
   26 1.980999    192.168.0.19    128.119.245.12  HTTP       451  GET /favicon.ico HTTP/1.1
   31 2.082029    128.119.245.12  192.168.0.19    HTTP       538  HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 21: 513 bytes on wire (4104 bits), 513 bytes captured (4104 bits) on interface 0
> Ethernet II, Src: SuperMic_b5:51:b6 (00:25:90:b5:51:b6), Dst: Motorola_f6:64:61 (dc:bf:e9:f6:64:61)
> Internet Protocol Version 4, Src: 192.168.0.19, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 64059, Dst Port: 80, Seq: 1, Ack: 1, Len: 459
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file1.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/77.0.3865.120 Safari/537.36\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\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: 24]
    [Next request in frame: 26]
```

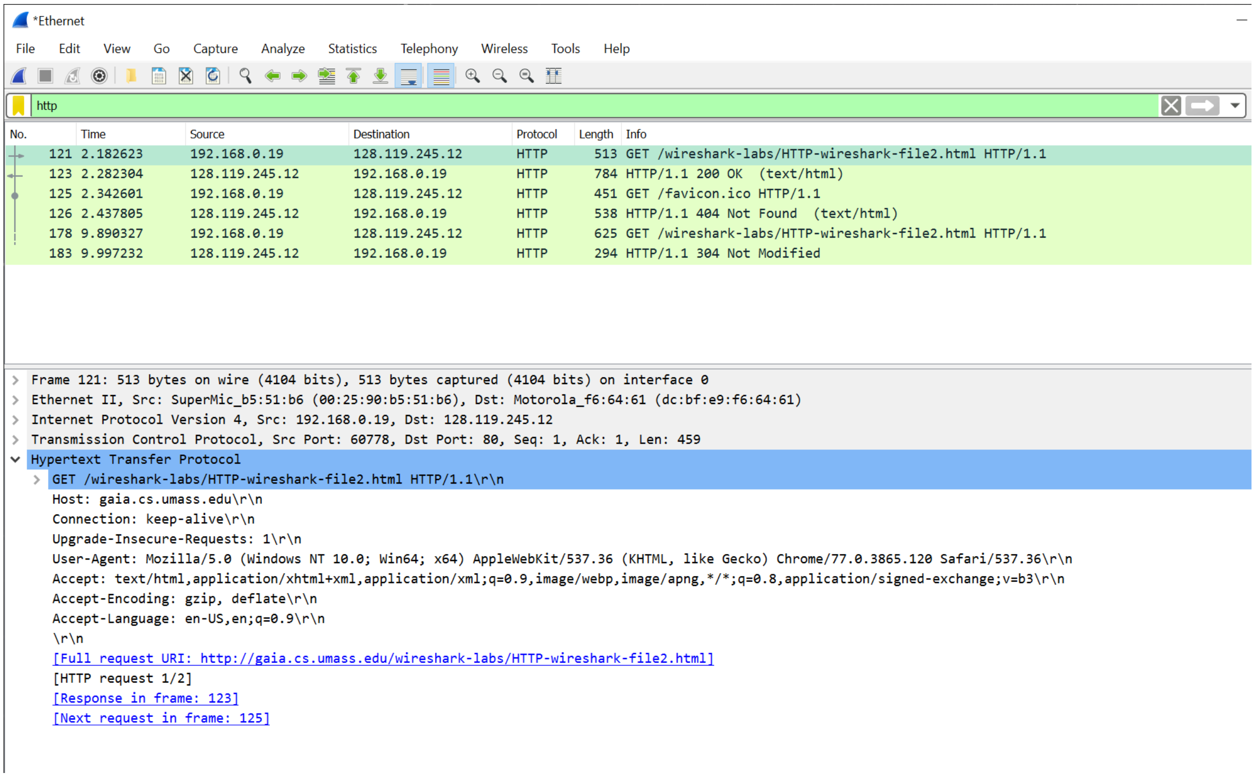

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
1
4
5
6

```
No.   Time        Source          Destination     Protocol  Length  Info
   21 1.800821    192.168.0.19    128.119.245.12  HTTP       513  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
   24 1.896479    128.119.245.12  192.168.0.19    HTTP       540  HTTP/1.1 200 OK  (text/html)
   26 1.980999    192.168.0.19    128.119.245.12  HTTP       451  GET /favicon.ico HTTP/1.1
   31 2.082029    128.119.245.12  192.168.0.19    HTTP       538  HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 24: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
> Ethernet II, Src: Motorola_f6:64:61 (dc:bf:e9:f6:64:61), Dst: SuperMic_b5:51:b6 (00:25:90:b5:51:b6)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.19
> Transmission Control Protocol, Src Port: 80, Dst Port: 64059, Seq: 1, Ack: 460, Len: 486
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Mon, 28 Oct 2019 01:08:10 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: Sun, 27 Oct 2019 05:59:02 GMT\r\n
    ETag: "80-595de1479be07"\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: 0.095658000 seconds]
    [Request in frame: 21]
    [Next request in frame: 26]
    [Next response in frame: 31]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    File Data: 128 bytes
> Line-based text data: text/html (4 lines)
```

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 not an IF-MODIFIED-SINCE line.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

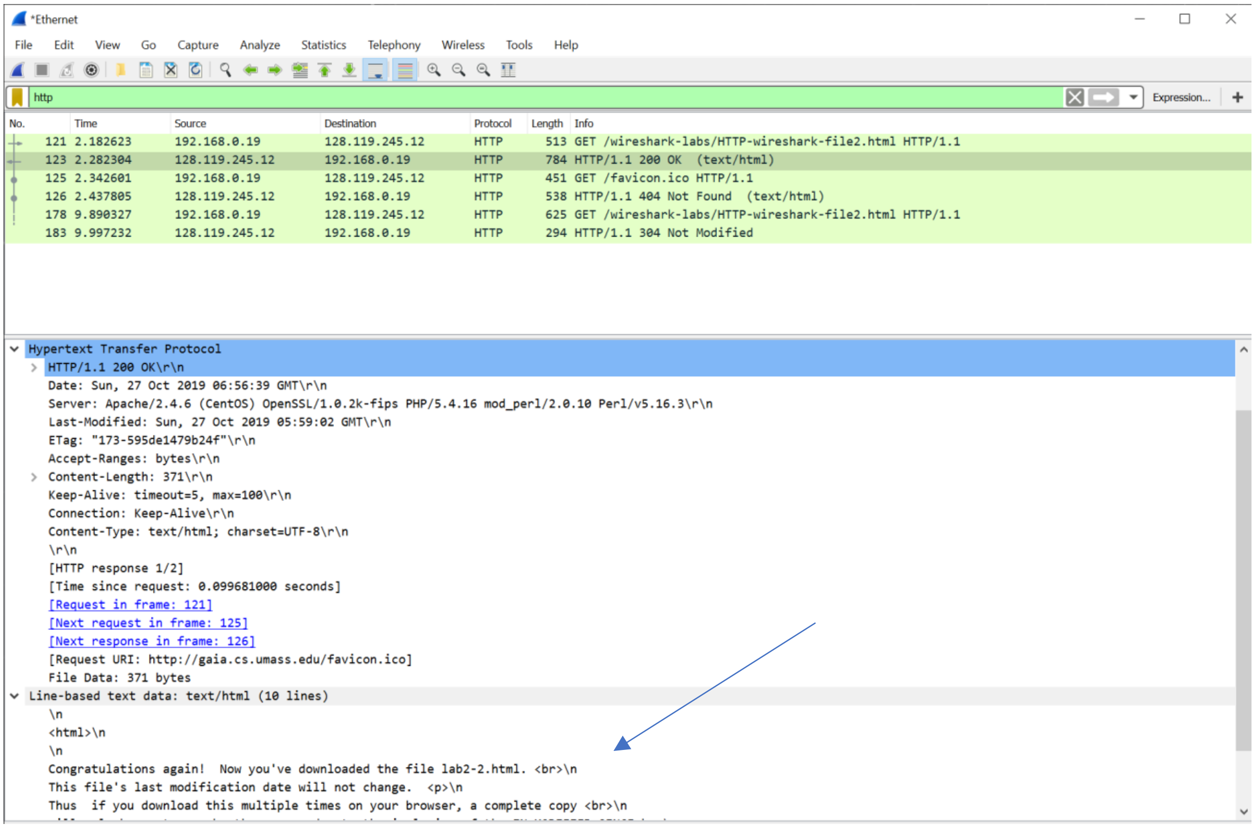
http

```
No.   Time       Source          Destination     Protocol  Length  Info
  121 2.182623   192.168.0.19    128.119.245.12  HTTP        513 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  123 2.282304   128.119.245.12  192.168.0.19    HTTP        784 HTTP/1.1 200 OK  (text/html)
  125 2.342601   192.168.0.19    128.119.245.12  HTTP        451 GET /favicon.ico HTTP/1.1
  126 2.437805   128.119.245.12  192.168.0.19    HTTP        538 HTTP/1.1 404 Not Found  (text/html)
  178 9.890327   192.168.0.19    128.119.245.12  HTTP        625 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  183 9.997232   128.119.245.12  192.168.0.19    HTTP        294 HTTP/1.1 304 Not Modified
```

```
> Frame 121: 513 bytes on wire (4104 bits), 513 bytes captured (4104 bits) on interface 0
> Ethernet II, Src: SuperMic_b5:51:b6 (00:25:90:b5:51:b6), Dst: Motorola_f6:64:61 (dc:bf:e9:f6:64:61)
> Internet Protocol Version 4, Src: 192.168.0.19, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 60778, Dst Port: 80, Seq: 1, Ack: 1, Len: 459
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file2.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/77.0.3865.120 Safari/537.36\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\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 1/2]
    [Response in frame: 123]
    [Next request in frame: 125]
```

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

Yes, below the HTTP information section you can see the line-based text data: text/html section that contains the file returned by the server.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

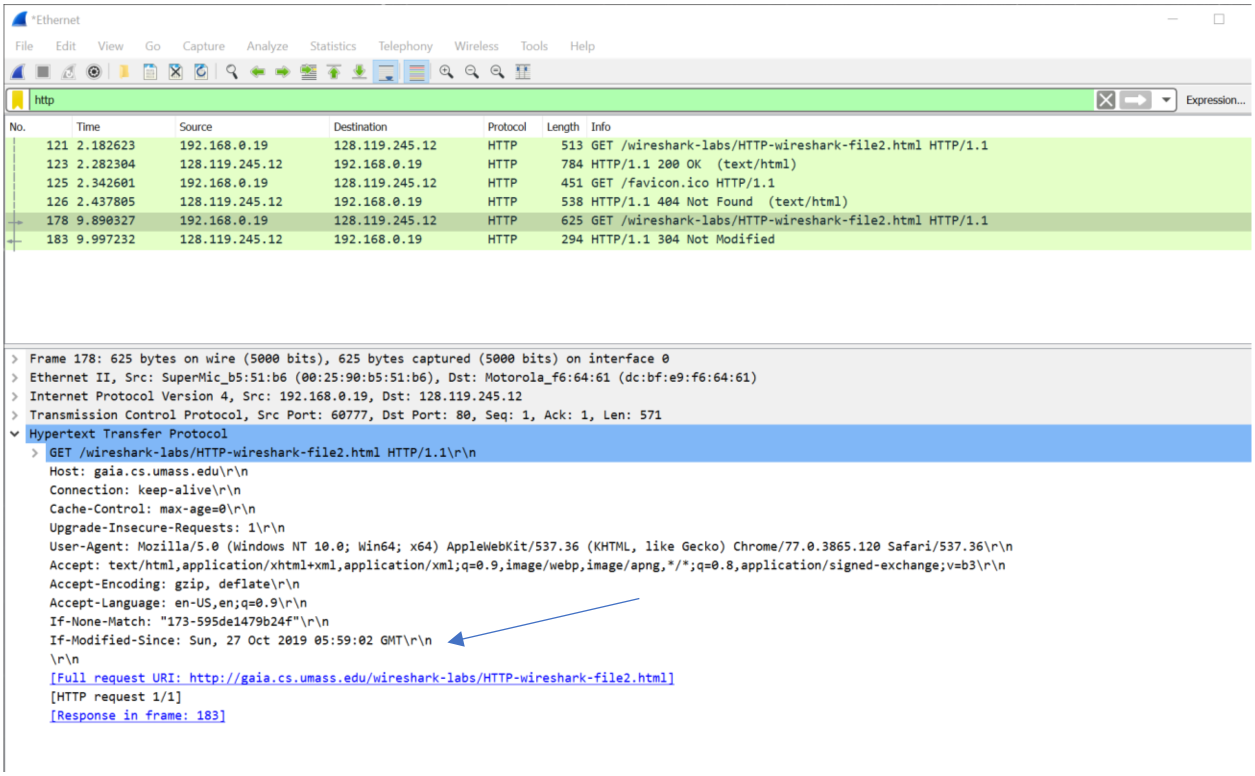
```
http
```

```
No.     Time      Source          Destination     Protocol  Length  Info
  121 2.182623  192.168.0.19    128.119.245.12  HTTP       513 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  123 2.282304  128.119.245.12  192.168.0.19    HTTP       784 HTTP/1.1 200 OK  (text/html)
  125 2.342601  192.168.0.19    128.119.245.12  HTTP       451 GET /favicon.ico HTTP/1.1
  126 2.437805  128.119.245.12  192.168.0.19    HTTP       538 HTTP/1.1 404 Not Found  (text/html)
  178 9.890327  192.168.0.19    128.119.245.12  HTTP       625 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  183 9.997232  128.119.245.12  192.168.0.19    HTTP       294 HTTP/1.1 304 Not Modified
```

```
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Sun, 27 Oct 2019 06:56:39 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: Sun, 27 Oct 2019 05:59:02 GMT\r\n
    ETag: "173-595de1479b24f"\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: 0.099681000 seconds]
    [Request in frame: 121]
    [Next request in frame: 125]
    [Next response in frame: 126]
    [Request URI: http://gaia.cs.umass.edu/favicon.ico]
    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
```

10. Now inspect the contents of the second and third HTTP GET requests from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in one of the HTTP GETs? If so, what information follows the "IF-MODIFIED-SINCE:" header?

The third get request contains an IF-MODIFIED-SINCE line. A date follows the header, it reads: Sun, 27 October 2019 5:59:02 GMT



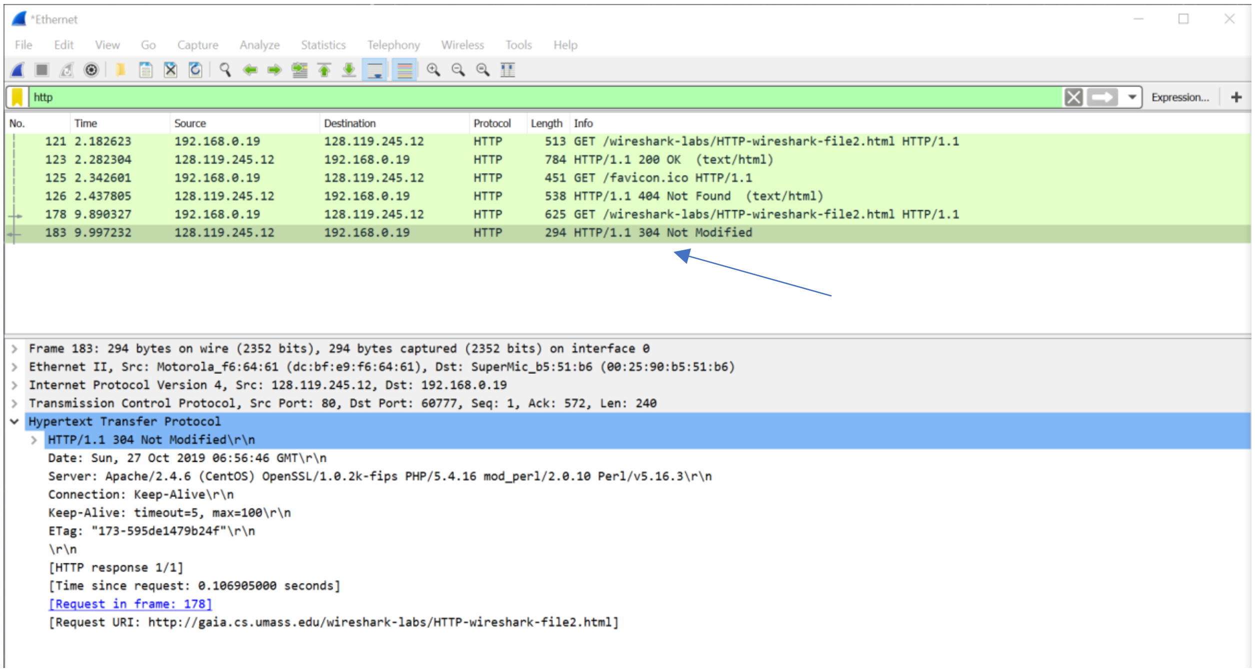
http

```
No.       Time       Source            Destination       Protocol  Length  Info
     121 2.182623    192.168.0.19      128.119.245.12    HTTP         513  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
     123 2.282304    128.119.245.12    192.168.0.19      HTTP         784  HTTP/1.1 200 OK  (text/html)
     125 2.342601    192.168.0.19      128.119.245.12    HTTP         451  GET /favicon.ico HTTP/1.1
     126 2.437805    128.119.245.12    192.168.0.19      HTTP         538  HTTP/1.1 404 Not Found  (text/html)
     178 9.890327    192.168.0.19      128.119.245.12    HTTP         625  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
     183 9.997232    128.119.245.12    192.168.0.19      HTTP         294  HTTP/1.1 304 Not Modified
```

```
> Frame 178: 625 bytes on wire (5000 bits), 625 bytes captured (5000 bits) on interface 0
> Ethernet II, Src: SuperMic_b5:51:b6 (00:25:90:b5:51:b6), Dst: Motorola_f6:64:61 (dc:bf:e9:f6:64:61)
> Internet Protocol Version 4, Src: 192.168.0.19, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 60777, Dst Port: 80, Seq: 1, Ack: 1, Len: 571
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file2.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
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.120 Safari/537.36\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\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    If-None-Match: "173-595de1479b24f"\r\n
    If-Modified-Since: Sun, 27 Oct 2019 05:59:02 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/1]
    [Response in frame: 183]
```

11. What is the HTTP status code and phrase returned from the server in response to the HTTP GET with IF MODIFIED SINCE (if there is one)? Did the server explicitly return the contents of the file? Explain.

It returned a status of 304 Not Modified and didn't explicitly send contents of the file. This is because the file had not been changed since it was last accessed so it did not return the file, the file was loaded from the cache.



```
No.   Time      Source          Destination     Protocol Length Info
  121 2.182623  192.168.0.19    128.119.245.12  HTTP      513 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  123 2.282304  128.119.245.12  192.168.0.19    HTTP      784 HTTP/1.1 200 OK  (text/html)
  125 2.342601  192.168.0.19    128.119.245.12  HTTP      451 GET /favicon.ico HTTP/1.1
  126 2.437805  128.119.245.12  192.168.0.19    HTTP      538 HTTP/1.1 404 Not Found  (text/html)
  178 9.890327  192.168.0.19    128.119.245.12  HTTP      625 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  183 9.997232  128.119.245.12  192.168.0.19    HTTP      294 HTTP/1.1 304 Not Modified
```

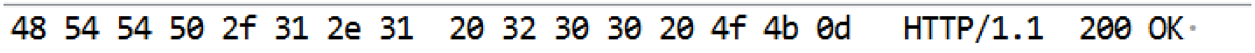
```
> Frame 183: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface 0
> Ethernet II, Src: Motorola_f6:64:61 (dc:bf:e9:f6:64:61), Dst: SuperMic_b5:51:b6 (00:25:90:b5:51:b6)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.19
> Transmission Control Protocol, Src Port: 80, Dst Port: 60777, Seq: 1, Ack: 572, Len: 240
v Hypertext Transfer Protocol
  > HTTP/1.1 304 Not Modified\r\n
    Date: Sun, 27 Oct 2019 06:56:46 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=100\r\n
    ETag: "173-595de1479b24f"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.106905000 seconds]
    [Request in frame: 178]
    [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?

Just one HTTP GET was sent by my browser. Packet 30 contains the GET message.

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

Packet number 34 contains the status code associated with the response. Clicking on the link by 13 in the image below opens that packet in the packet content window and the first line is:



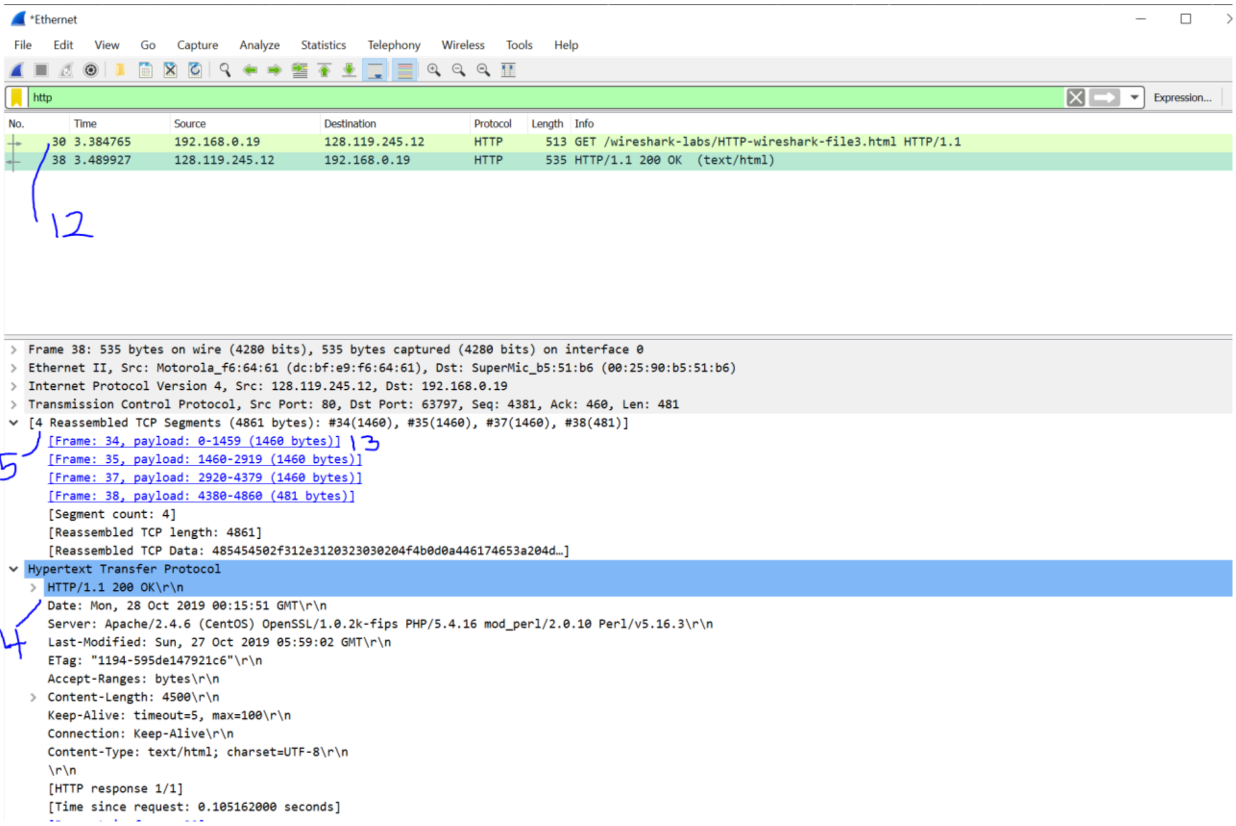
```
48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK·
```

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

Status code: 200 OK

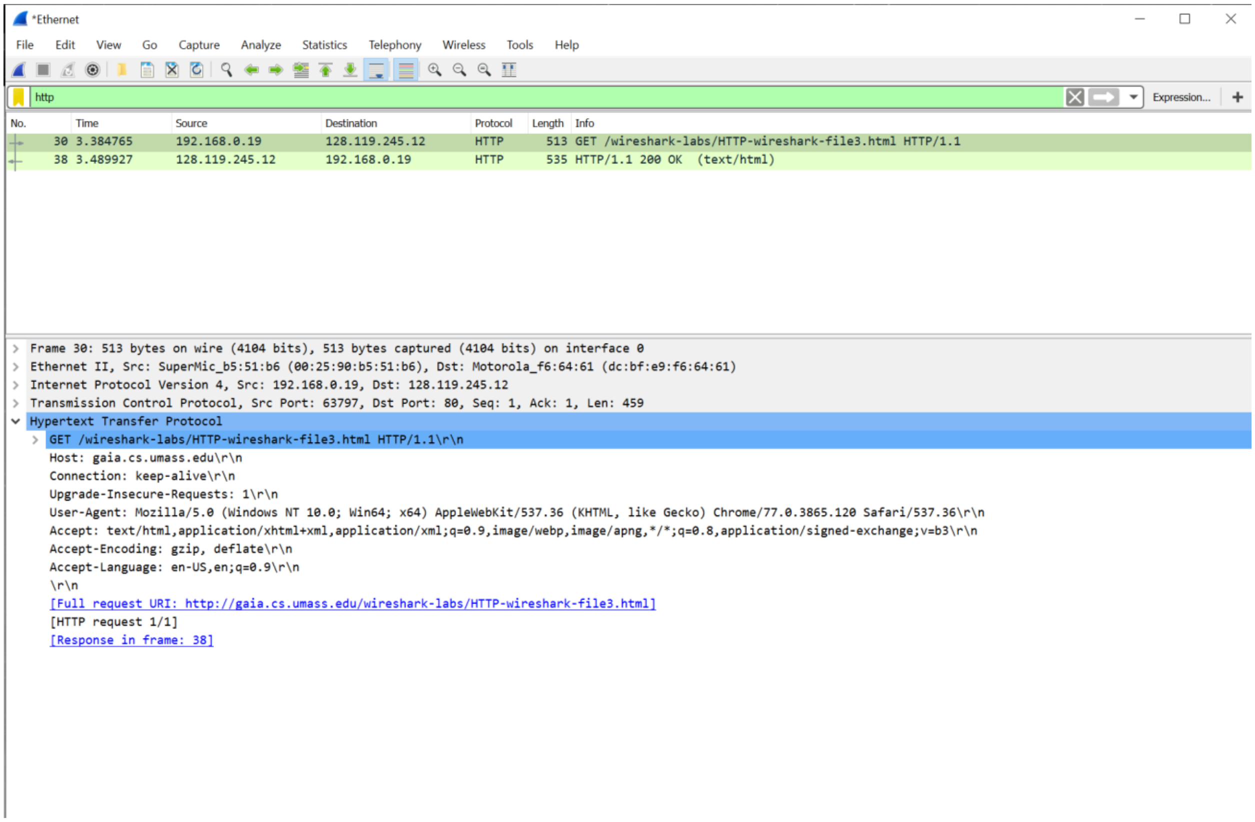
15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

4 TCP segments were used to carry the response.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
12
13
15
14

```
No.  Time      Source           Destination      Protocol  Length  Info
  30 3.384765  192.168.0.19     128.119.245.12   HTTP        513   GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  38 3.489927  128.119.245.12   192.168.0.19     HTTP        535   HTTP/1.1 200 OK  (text/html)
```

```
> Frame 38: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface 0
> Ethernet II, Src: Motorola_f6:64:61 (dc:bf:e9:f6:64:61), Dst: SuperMic_b5:51:b6 (00:25:90:b5:51:b6)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.19
> Transmission Control Protocol, Src Port: 80, Dst Port: 63797, Seq: 4381, Ack: 460, Len: 481
v [4 Reassembled TCP Segments (4861 bytes): #34(1460), #35(1460), #37(1460), #38(481)]
    [Frame: 34, payload: 0-1459 (1460 bytes)]
    [Frame: 35, payload: 1460-2919 (1460 bytes)]
    [Frame: 37, payload: 2920-4379 (1460 bytes)]
    [Frame: 38, payload: 4380-4860 (481 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a204d…]
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Mon, 28 Oct 2019 00:15:51 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: Sun, 27 Oct 2019 05:59:02 GMT\r\n
    ETag: "1194-595de147921c6"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 4500\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: 0.105162000 seconds]
```


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
+

```
No.  Time      Source           Destination      Protocol  Length  Info
  30 3.384765  192.168.0.19     128.119.245.12   HTTP        513   GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  38 3.489927  128.119.245.12   192.168.0.19     HTTP        535   HTTP/1.1 200 OK  (text/html)
```

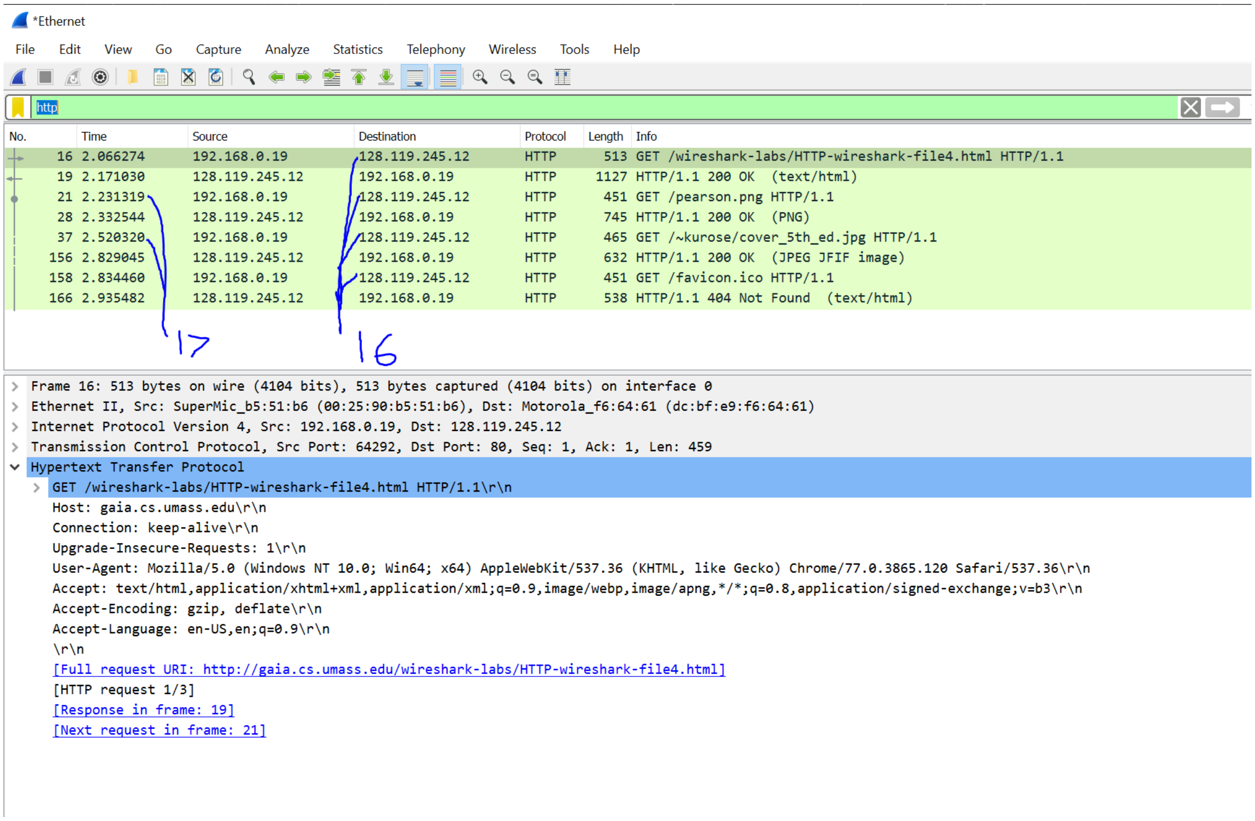
```
> Frame 30: 513 bytes on wire (4104 bits), 513 bytes captured (4104 bits) on interface 0
> Ethernet II, Src: SuperMic_b5:51:b6 (00:25:90:b5:51:b6), Dst: Motorola_f6:64:61 (dc:bf:e9:f6:64:61)
> Internet Protocol Version 4, Src: 192.168.0.19, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 63797, Dst Port: 80, Seq: 1, Ack: 1, Len: 459
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file3.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/77.0.3865.120 Safari/537.36\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\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-file3.html]
    [HTTP request 1/1]
    [Response in frame: 38]
```

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

My browser sent 4 get requests. All 4 were to the IP 128.119.245.12.

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.

They were downloaded serially, the request for the second image was made after the response for the first image was received, therefor they were retrieved serially. I ran this test 5 times, and every time there was a delay between the first images response and the second images get request being sent.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
17
16

```
No.     Time       Source          Destination     Protocol  Length  Info
   16  2.066274   192.168.0.19    128.119.245.12  HTTP       513  GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
   19  2.171030   128.119.245.12  192.168.0.19    HTTP      1127  HTTP/1.1 200 OK  (text/html)
   21  2.231319   192.168.0.19    128.119.245.12  HTTP       451  GET /pearson.png HTTP/1.1
   28  2.332544   128.119.245.12  192.168.0.19    HTTP       745  HTTP/1.1 200 OK  (PNG)
   37  2.520320   192.168.0.19    128.119.245.12  HTTP       465  GET /~kurose/cover_5th_ed.jpg HTTP/1.1
  156  2.829045   128.119.245.12  192.168.0.19    HTTP       632  HTTP/1.1 200 OK  (JPEG JFIF image)
  158  2.834460   192.168.0.19    128.119.245.12  HTTP       451  GET /favicon.ico HTTP/1.1
  166  2.935482   128.119.245.12  192.168.0.19    HTTP       538  HTTP/1.1 404 Not Found  (text/html)
```

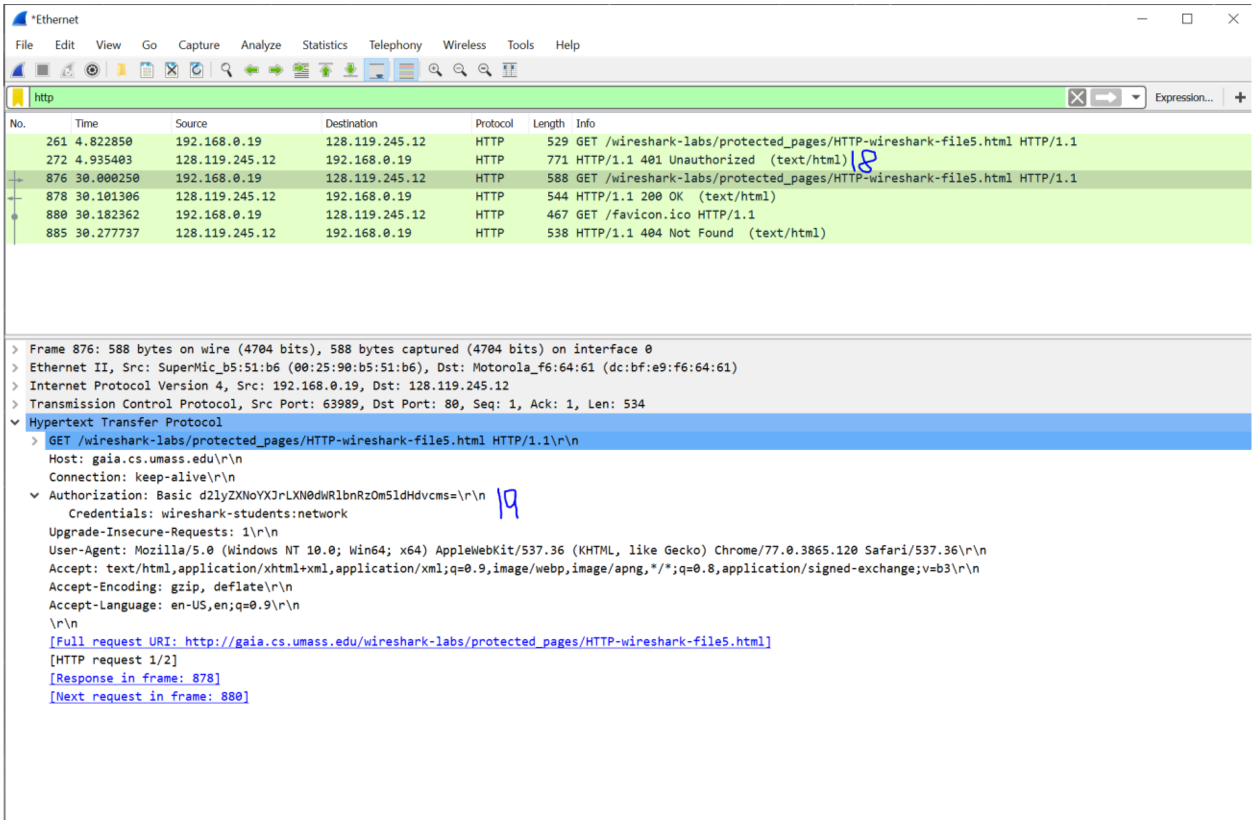
```
> Frame 16: 513 bytes on wire (4104 bits), 513 bytes captured (4104 bits) on interface 0
> Ethernet II, Src: SuperMic_b5:51:b6 (00:25:90:b5:51:b6), Dst: Motorola_f6:64:61 (dc:bf:e9:f6:64:61)
> Internet Protocol Version 4, Src: 192.168.0.19, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 64292, Dst Port: 80, Seq: 1, Ack: 1, Len: 459
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file4.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/77.0.3865.120 Safari/537.36\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\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-file4.html]
    [HTTP request 1/3]
    [Response in frame: 19]
    [Next request in frame: 21]
```

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

401 Unauthorized

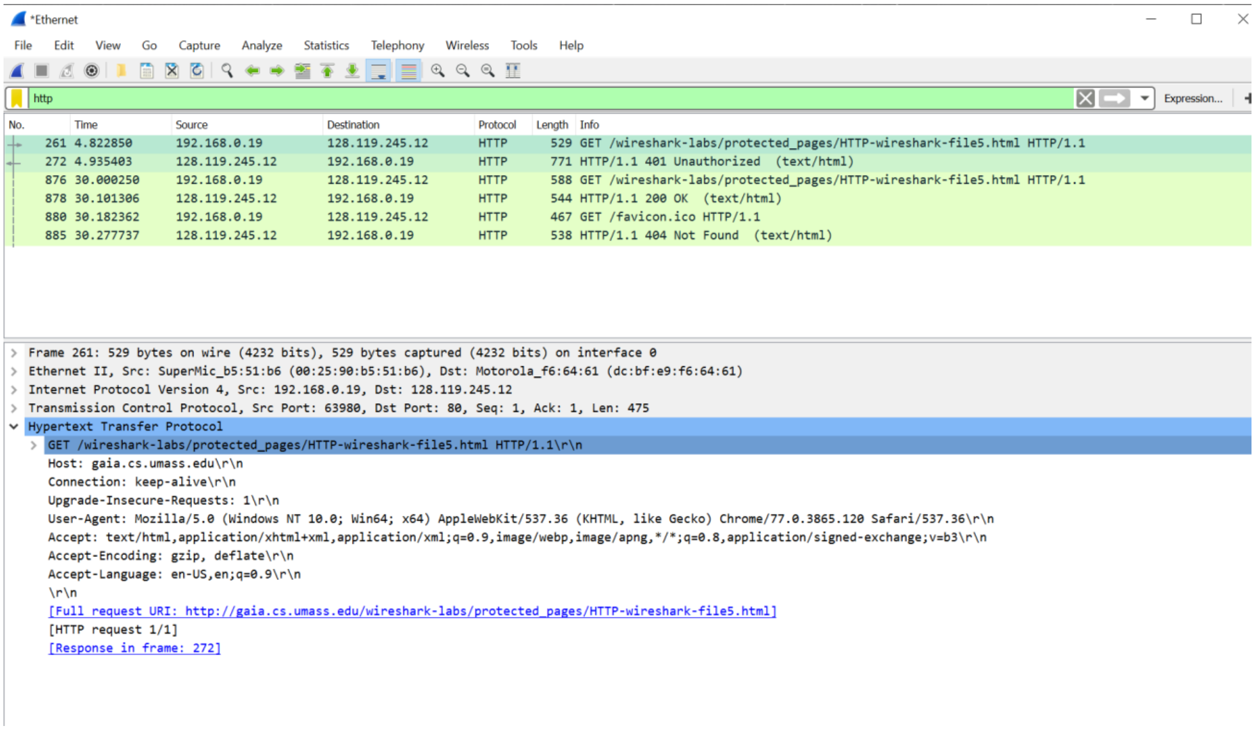
19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

An authorization field was included in the second Get message.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...

```
No.   Time        Source          Destination     Protocol  Length  Info
  261 4.822850    192.168.0.19    128.119.245.12  HTTP       529 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
  272 4.935403    128.119.245.12  192.168.0.19    HTTP       771 HTTP/1.1 401 Unauthorized  (text/html) 18
  876 30.000250   192.168.0.19    128.119.245.12  HTTP       588 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
  878 30.101306   128.119.245.12  192.168.0.19    HTTP       544 HTTP/1.1 200 OK  (text/html)
  880 30.182362   192.168.0.19    128.119.245.12  HTTP       467 GET /favicon.ico HTTP/1.1
  885 30.277737   128.119.245.12  192.168.0.19    HTTP       538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 876: 588 bytes on wire (4704 bits), 588 bytes captured (4704 bits) on interface 0
> Ethernet II, Src: SuperMic_b5:51:b6 (00:25:90:b5:51:b6), Dst: Motorola_f6:64:61 (dc:bf:e9:f6:64:61)
> Internet Protocol Version 4, Src: 192.168.0.19, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 63989, Dst Port: 80, Seq: 1, Ack: 1, Len: 534
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
  v Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n   19
      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/77.0.3865.120 Safari/537.36\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\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: 878]
    [Next request in frame: 880]
```


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...

```
No.   Time        Source          Destination     Protocol  Length  Info
  261 4.822850    192.168.0.19    128.119.245.12  HTTP       529 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
  272 4.935403    128.119.245.12  192.168.0.19    HTTP       771 HTTP/1.1 401 Unauthorized  (text/html)
  876 30.000250   192.168.0.19    128.119.245.12  HTTP       588 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
  878 30.101306   128.119.245.12  192.168.0.19    HTTP       544 HTTP/1.1 200 OK  (text/html)
  880 30.182362   192.168.0.19    128.119.245.12  HTTP       467 GET /favicon.ico HTTP/1.1
  885 30.277737   128.119.245.12  192.168.0.19    HTTP       538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 261: 529 bytes on wire (4232 bits), 529 bytes captured (4232 bits) on interface 0
> Ethernet II, Src: SuperMic_b5:51:b6 (00:25:90:b5:51:b6), Dst: Motorola_f6:64:61 (dc:bf:e9:f6:64:61)
> Internet Protocol Version 4, Src: 192.168.0.19, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 63980, Dst Port: 80, Seq: 1, Ack: 1, Len: 475
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/77.0.3865.120 Safari/537.36\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\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: 272]
```