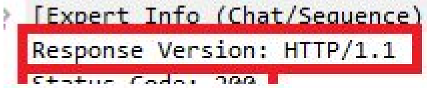
Joel Huffman
CS372-400 Spring 2019

Lab 2

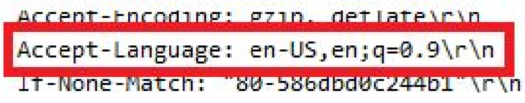
1. **Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?**



```
[Expert Info (Chat/Sequence)
Response Version: HTTP/1.1
Status Code: 200
```

Browser: 1.1
Server: 1.1

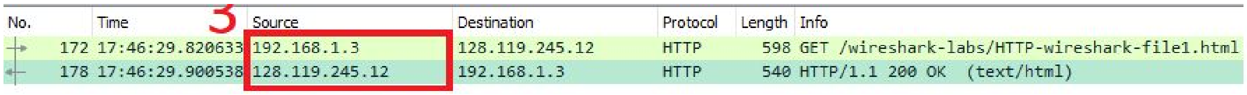
2. **What languages (if any) does your browser indicate that it can accept to the server?**



```
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
If-None-Match: "80-586dbd0c244b1"\r\n
```

English

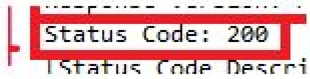
3. **What is the IP address of your computer? Of the gaia.cs.umass.edu server?**



No.	Time	Source	Destination	Protocol	Length	Info
172	17:46:29.820633	192.168.1.3	128.119.245.12	HTTP	598	GET /wireshark-labs/HTTP-wireshark-file1.html
178	17:46:29.900538	128.119.245.12	192.168.1.3	HTTP	540	HTTP/1.1 200 OK (text/html)

My computer: 192.168.1.3
Server: 128.119.245.12

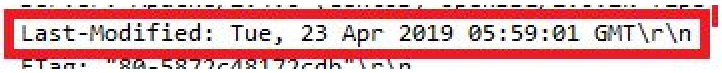
4. **What is the status code returned from the server to your browser?**



```
Status Code: 200
[Status Code Descri
```

200

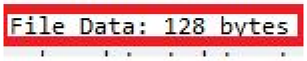
5. **When was the HTML file that you are retrieving last modified at the server?**



```
Last-Modified: Tue, 23 Apr 2019 05:59:01 GMT\r\n
ETag: "80-5872c48172cdb"\r\n
```

Tue, 23 Apr 2019 05:59:01 GMT

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

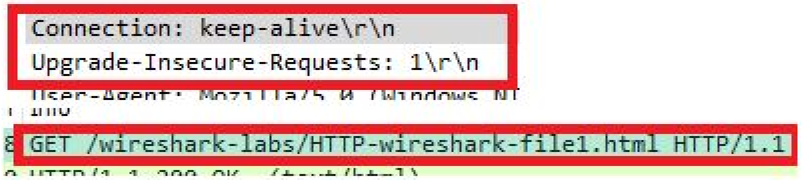


```
File Data: 128 bytes
```

128

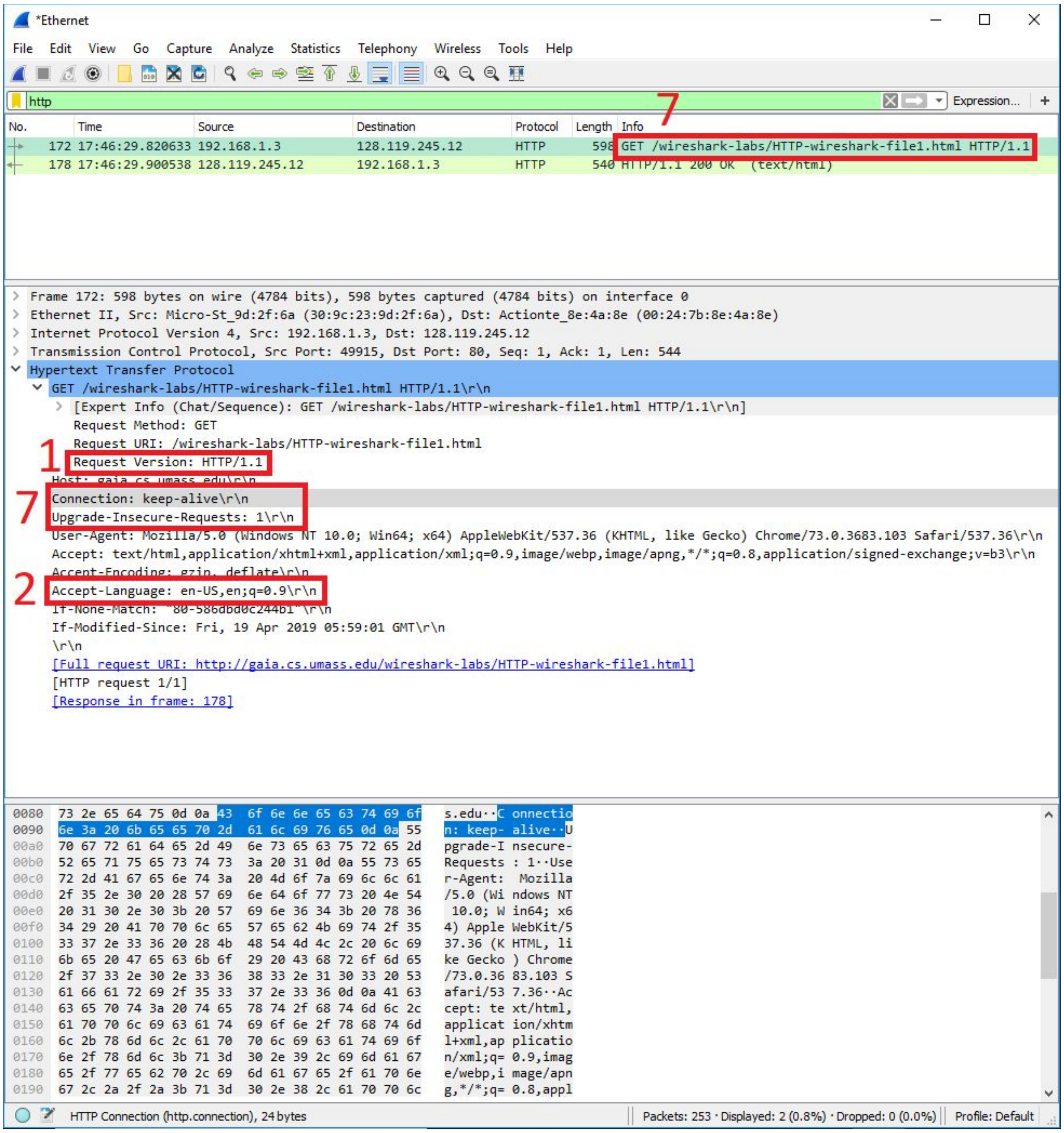
Joel Huffman
CS372-400 Spring 2019

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**



```
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
```

There are bits of header information (“connection: keep-alive”, “Upgrade-Insecure_requests: 1”, etc.) that are not included in the packet-listing window, but not any actual headers.



*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression…
7
1
7
2

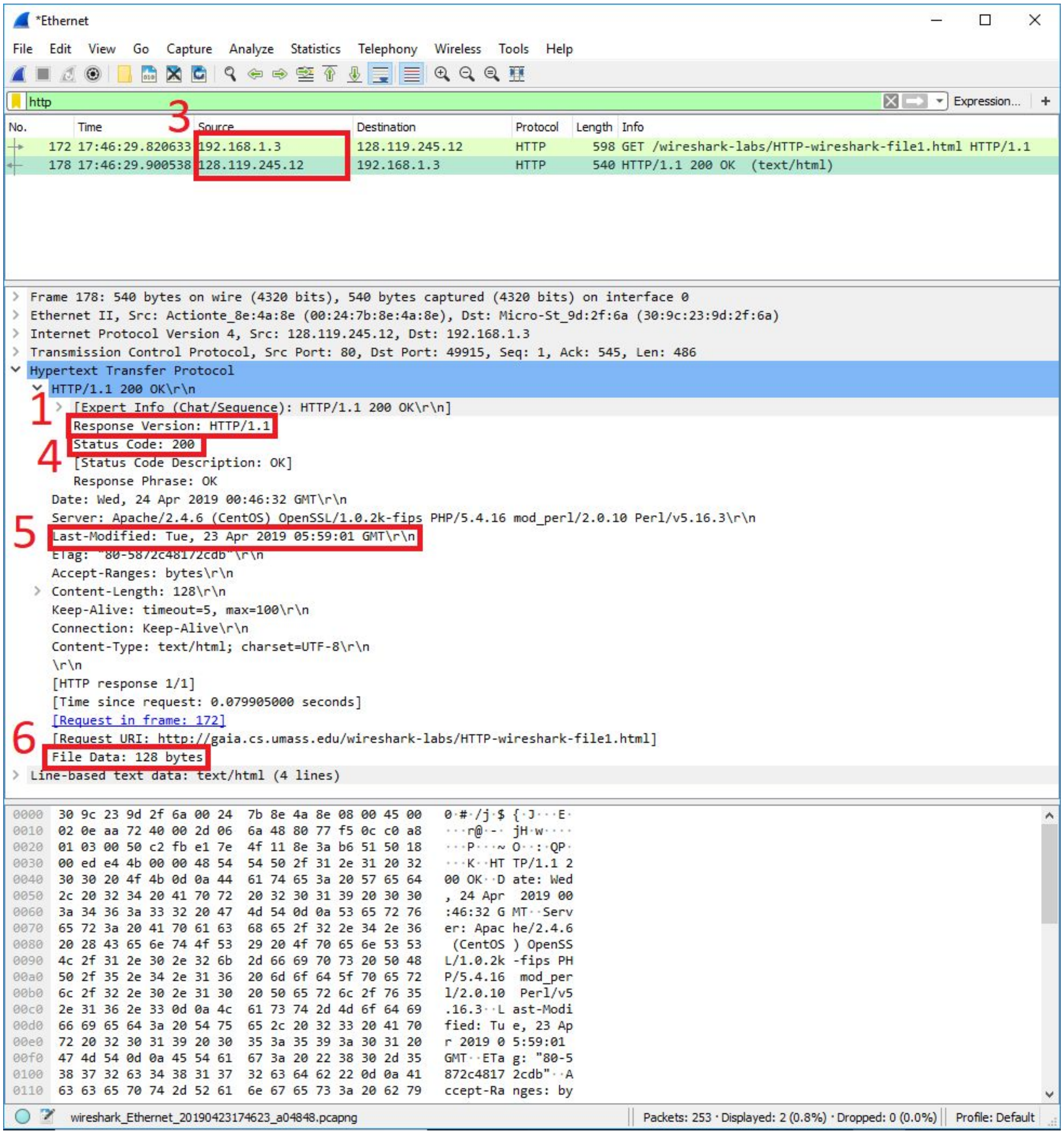
```
No.   Time             Source          Destination      Protocol  Length Info
  172 17:46:29.820633 192.168.1.3     128.119.245.12   HTTP      598    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  178 17:46:29.900538 128.119.245.12  192.168.1.3      HTTP      540    HTTP/1.1 200 OK  (text/html)
```

```
> Frame 172: 598 bytes on wire (4784 bits), 598 bytes captured (4784 bits) on interface 0
> Ethernet II, Src: Micro-St_9d:2f:6a (30:9c:23:9d:2f:6a), Dst: Actionte_8e:4a:8e (00:24:7b:8e:4a:8e)
> Internet Protocol Version 4, Src: 192.168.1.3, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 49915, Dst Port: 80, Seq: 1, Ack: 1, Len: 544
v Hypertext Transfer Protocol
  v 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
    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/73.0.3683.103 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: "80-586dbd0c244b1"\r\n
    If-Modified-Since: Fri, 19 Apr 2019 05:59:01 GMT\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: 178]
```

```
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 55   n: keep- alive··U
00a0  70 67 72 61 64 65 2d 49  6e 73 65 63 75 72 65 2d   pgrade-I nsecure-
00b0  52 65 71 75 65 73 74 73  3a 20 31 0d 0a 55 73 65   Requests : 1··Use
00c0  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a 69 6c 6c 61   r-Agent:  Mozilla
00d0  2f 35 2e 30 20 28 57 69  6e 64 6f 77 73 20 4e 54   /5.0 (Wi ndows NT
00e0  20 31 30 2e 30 3b 20 57  69 6e 36 34 3b 20 78 36    10.0; W in64; x6
00f0  34 29 20 41 70 70 6c 65  57 65 62 4b 69 74 2f 35   4) Apple WebKit/5
0100  33 37 2e 33 36 20 28 4b  48 54 4d 4c 2c 20 6c 69   37.36 (K HTML, li
0110  6b 65 20 47 65 63 6b 6f  29 20 43 68 72 6f 6d 65   ke Gecko ) Chrome
0120  2f 37 33 2e 30 2e 33 36  38 33 2e 31 30 33 20 53   /73.0.36 83.103 S
0130  61 66 61 72 69 2f 35 33  37 2e 33 36 0d 0a 41 63   afari/53 7.36··Ac
0140  63 65 70 74 3a 20 74 65  78 74 2f 68 74 6d 6c 2c   cept: te xt/html,
0150  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 68 74 6d   applicat ion/xhtm
0160  6c 2b 78 6d 6c 2c 61 70  70 6c 69 63 61 74 69 6f   l+xml,ap plicatio
0170  6e 2f 78 6d 6c 3b 71 3d  30 2e 39 2c 69 6d 61 67   n/xml;q= 0.9,imag
0180  65 2f 77 65 62 70 2c 69  6d 61 67 65 2f 61 70 6e   e/webp,i mage/apn
0190  67 2c 2a 2f 2a 3b 71 3d  30 2e 38 2c 61 70 70 6c   g,*/*;q= 0.8,appl
```

```
HTTP Connection (http.connection), 24 bytes    Packets: 253 · Displayed: 2 (0.8%) · Dropped: 0 (0.0%)    Profile: Default
```

Joel Huffman
CS372-400 Spring 2019


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression…
3
1
4
5
6

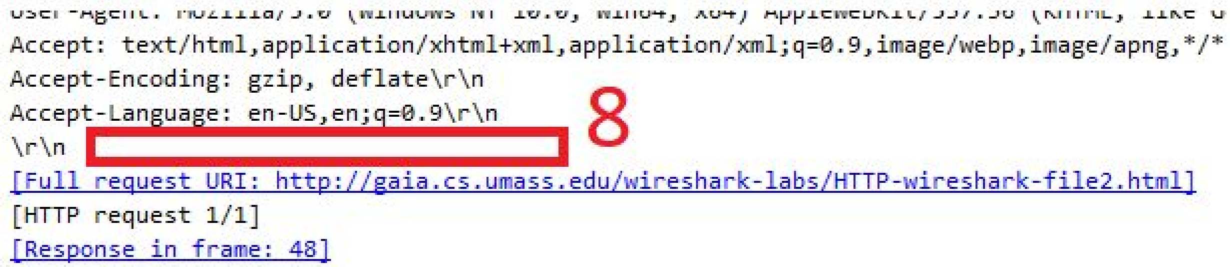
```
No.  Time             Source          Destination     Protocol  Length  Info
 172 17:46:29.820633 192.168.1.3     128.119.245.12  HTTP      598 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
 178 17:46:29.900538 128.119.245.12  192.168.1.3     HTTP      540 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 178: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
> Ethernet II, Src: Actionte_8e:4a:8e (00:24:7b:8e:4a:8e), Dst: Micro-St_9d:2f:6a (30:9c:23:9d:2f:6a)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.3
> Transmission Control Protocol, Src Port: 80, Dst Port: 49915, Seq: 1, Ack: 545, Len: 486
v Hypertext Transfer Protocol
  v 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: Wed, 24 Apr 2019 00:46:32 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: Tue, 23 Apr 2019 05:59:01 GMT\r\n
    ETag: "80-5872c48172cdb"\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: 0.079905000 seconds]
    [Request in frame: 172]
    [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)
```

```
0000  30 9c 23 9d 2f 6a 00 24  7b 8e 4a 8e 08 00 45 00   0·#·/j·$ {·J···E·
0010  02 0e aa 72 40 00 2d 06  6a 48 80 77 f5 0c c0 a8   ···r@·-· jH·w····
0020  01 03 00 50 c2 fb e1 7e  4f 11 8e 3a b6 51 50 18   ···P···~ O··:·QP·
0030  00 ed e4 4b 00 00 48 54  54 50 2f 31 2e 31 20 32   ···K··HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 57 65 64   00 OK··D ate: Wed
0050  2c 20 32 34 20 41 70 72  20 32 30 31 39 20 30 30   , 24 Apr  2019 00
0060  3a 34 36 3a 33 32 20 47  4d 54 0d 0a 53 65 72 76   :46:32 G MT··Serv
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34 2e 36   er: Apac he/2.4.6
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70 65 6e 53 53    (CentOS ) OpenSS
0090  4c 2f 31 2e 30 2e 32 6b  2d 66 69 70 73 20 50 48   L/1.0.2k -fips PH
00a0  50 2f 35 2e 34 2e 31 36  20 6d 6f 64 5f 70 65 72   P/5.4.16  mod_per
00b0  6c 2f 32 2e 30 2e 31 30  20 50 65 72 6c 2f 76 35   l/2.0.10  Perl/v5
00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d 4d 6f 64 69   .16.3··L ast-Modi
00d0  66 69 65 64 3a 20 54 75  65 2c 20 32 33 20 41 70   fied: Tu e, 23 Ap
00e0  72 20 32 30 31 39 20 30  35 3a 35 39 3a 30 31 20   r 2019 0 5:59:01
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 38 30 2d 35   GMT··ETa g: "80-5
0100  38 37 32 63 34 38 31 37  32 63 64 62 22 0d 0a 41   872c4817 2cdb"··A
0110  63 63 65 70 74 2d 52 61  6e 67 65 73 3a 20 62 79   ccept-Ra nges: by
```

wireshark_Ethernet_20190423174623_a04848.pcapng | Packets: 253 · Displayed: 2 (0.8%) · Dropped: 0 (0.0%) | Profile: Default

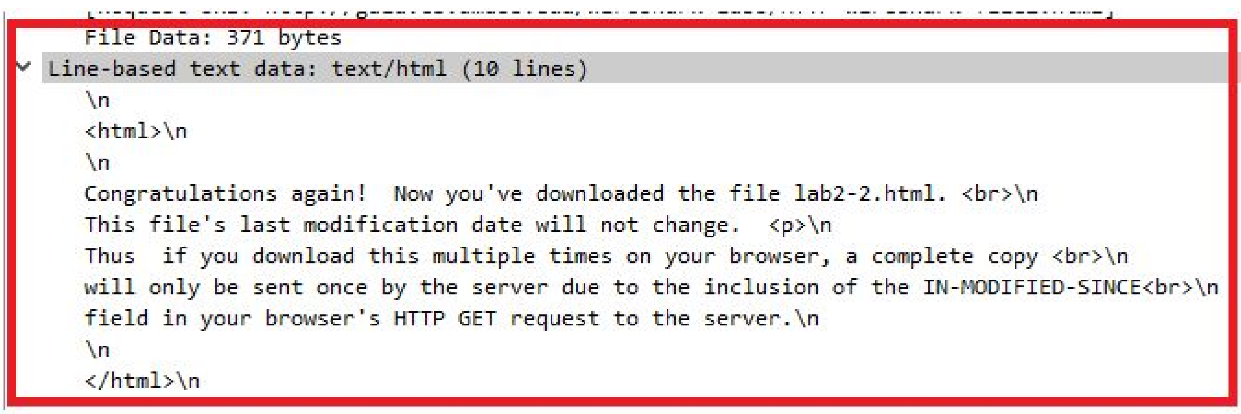
8. **Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?**



```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like G
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*
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 1/1]
[Response in frame: 48]
```

No, if it was it would be in the above area.

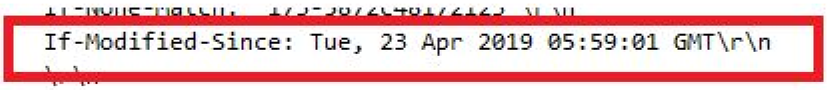
9. **Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?**



```
    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
```

Yes, the text/html sent by the server is included in the response.

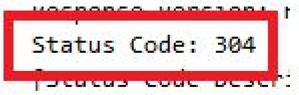
10. **Now inspect the contents of the second and third HTTP GET requests from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in one of the HTTP GETs? If so, what information follows the "IF-MODIFIED-SINCE:" header?**



```
If-Modified-Since: Tue, 23 Apr 2019 05:59:01 GMT\r\n
```

Yes, Tue, 23 Apr 2019 05:59:01 GMT

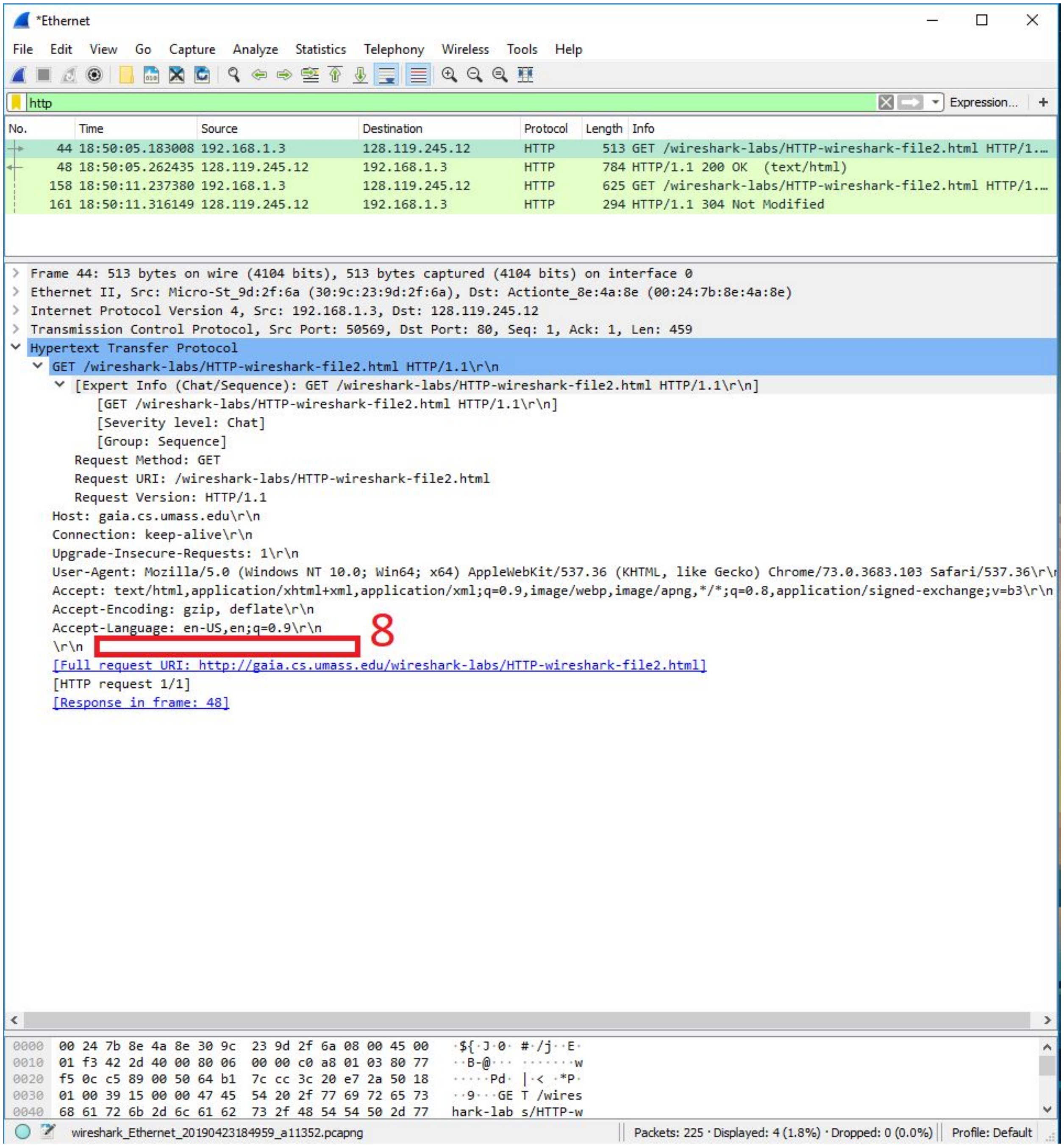
11. **What is the HTTP status code and phrase returned from the server in response to the HTTP GET with IF MODIFIED SINCE (if there is one)? Did the server explicitly return the contents of the file? Explain.**



```
Status Code: 304
```

304 Not Modified. No, the server didn't send the contents of the file because it was determined to have already been sent recently. The page's content can instead be pulled from cache. This is helpful because it limits unnecessary use of both server and client bandwidth.

Joel Huffman
CS372-400 Spring 2019


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

```
No.    Time            Source          Destination     Protocol Length Info
    44 18:50:05.183008 192.168.1.3     128.119.245.12  HTTP      513 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.…
    48 18:50:05.262435 128.119.245.12  192.168.1.3     HTTP      784 HTTP/1.1 200 OK  (text/html)
   158 18:50:11.237380 192.168.1.3     128.119.245.12  HTTP      625 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.…
   161 18:50:11.316149 128.119.245.12  192.168.1.3     HTTP      294 HTTP/1.1 304 Not Modified
```

```
> Frame 44: 513 bytes on wire (4104 bits), 513 bytes captured (4104 bits) on interface 0
> Ethernet II, Src: Micro-St_9d:2f:6a (30:9c:23:9d:2f:6a), Dst: Actionte_8e:4a:8e (00:24:7b:8e:4a:8e)
> Internet Protocol Version 4, Src: 192.168.1.3, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 50569, Dst Port: 80, Seq: 1, Ack: 1, Len: 459
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
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36\r\
    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 1/1]
    [Response in frame: 48]
```

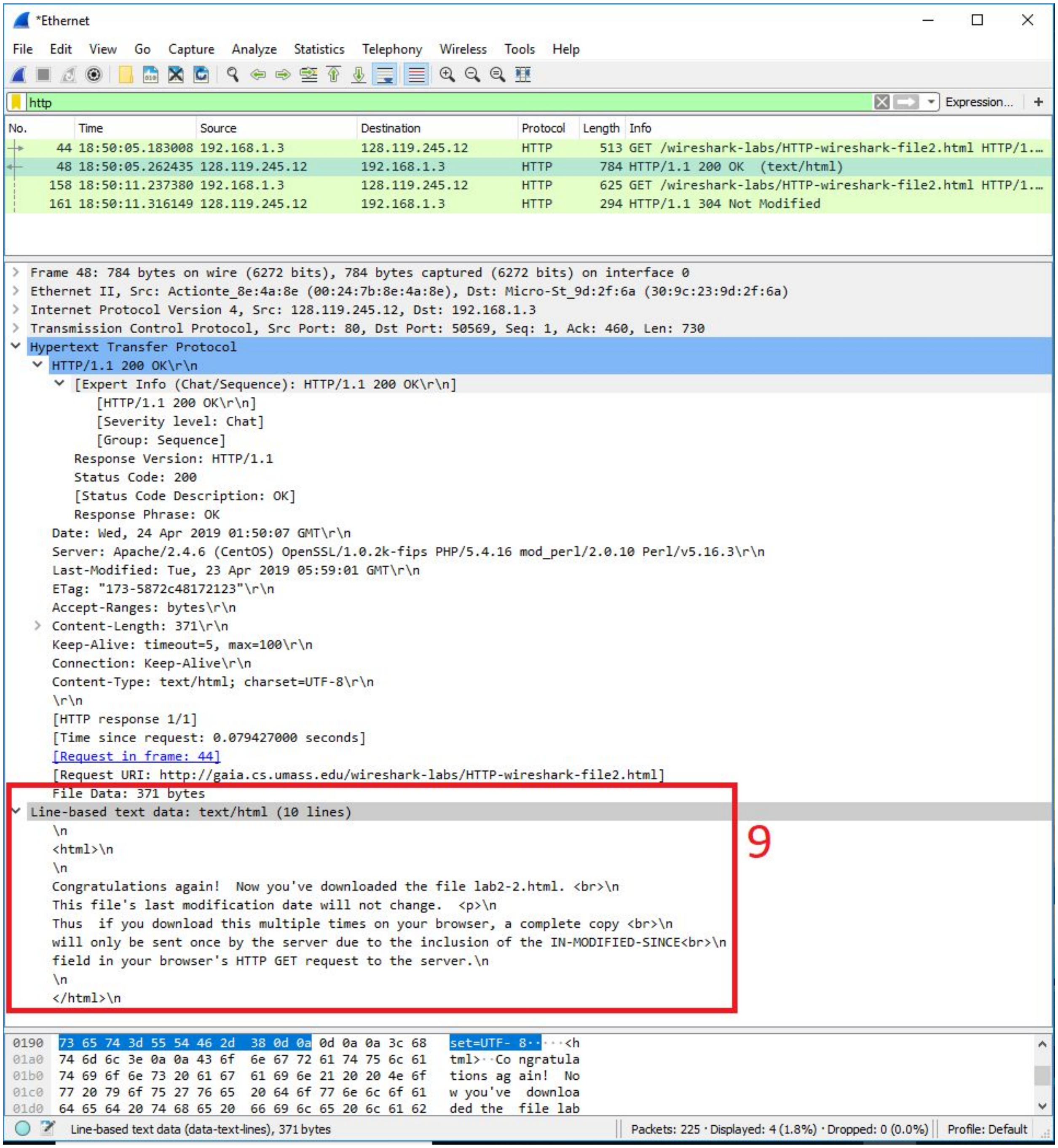
8

```
0000  00 24 7b 8e 4a 8e 30 9c  23 9d 2f 6a 08 00 45 00   ·${·J·0· #·/j··E·
0010  01 f3 42 2d 40 00 80 06  00 00 c0 a8 01 03 80 77   ··B-@··· ·······w
0020  f5 0c c5 89 00 50 64 b1  7c cc 3c 20 e7 2a 50 18   ·····Pd· |·< ·*P·
0030  01 00 39 15 00 00 47 45  54 20 2f 77 69 72 65 73   ··9···GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
```

wireshark_Ethernet_20190423184959_a11352.pcapng

Packets: 225 · Displayed: 4 (1.8%) · Dropped: 0 (0.0%)

Profile: Default


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+
9

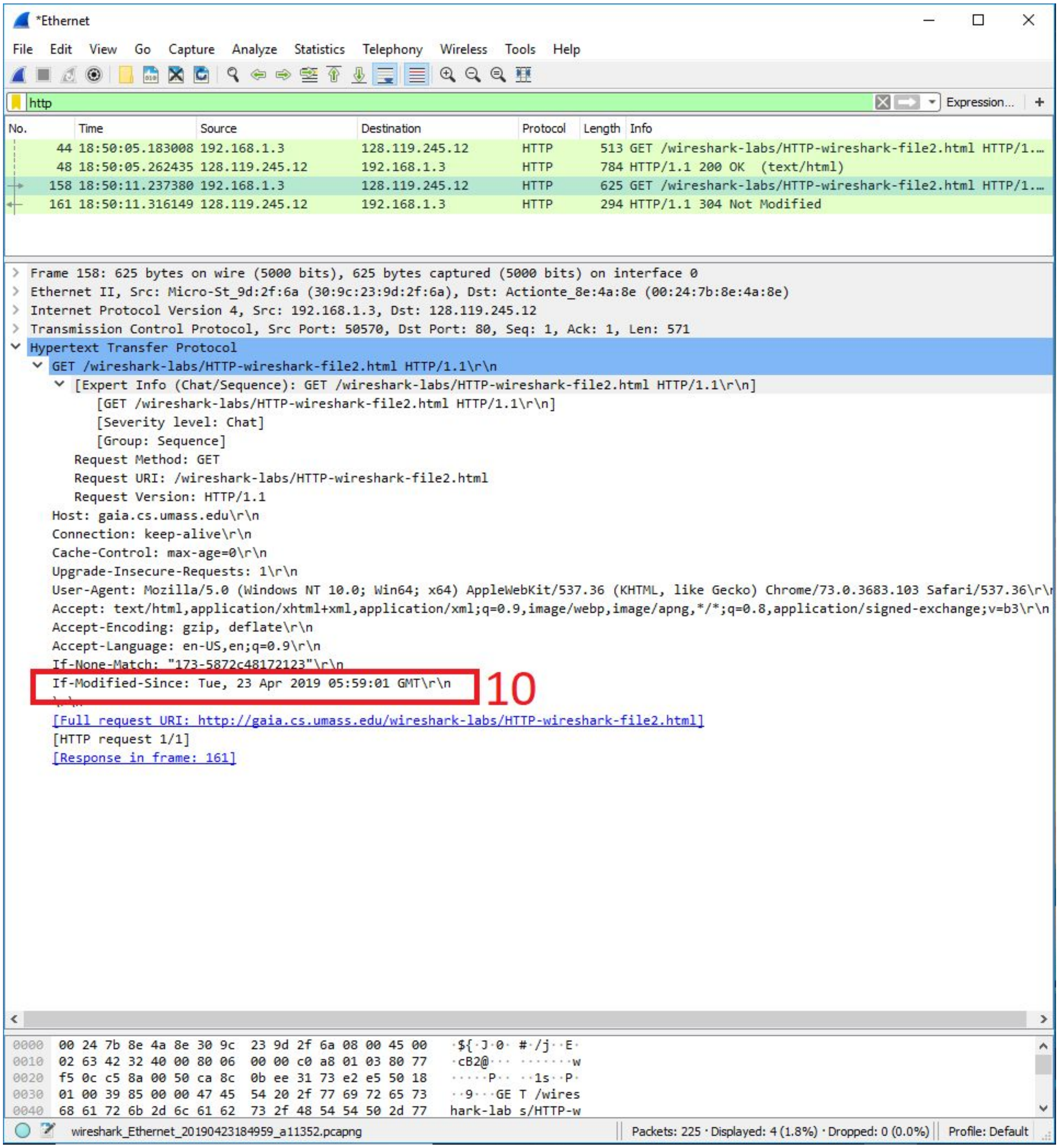
http

```
No.    Time             Source          Destination     Protocol  Length Info
   44 18:50:05.183008 192.168.1.3     128.119.245.12  HTTP        513 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.…
   48 18:50:05.262435 128.119.245.12  192.168.1.3     HTTP        784 HTTP/1.1 200 OK  (text/html)
  158 18:50:11.237380 192.168.1.3     128.119.245.12  HTTP        625 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.…
  161 18:50:11.316149 128.119.245.12  192.168.1.3     HTTP        294 HTTP/1.1 304 Not Modified
```

```
> Frame 48: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface 0
> Ethernet II, Src: Actionte_8e:4a:8e (00:24:7b:8e:4a:8e), Dst: Micro-St_9d:2f:6a (30:9c:23:9d:2f:6a)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.3
> Transmission Control Protocol, Src Port: 80, Dst Port: 50569, Seq: 1, Ack: 460, Len: 730
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: Wed, 24 Apr 2019 01:50:07 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: Tue, 23 Apr 2019 05:59:01 GMT\r\n
    ETag: "173-5872c48172123"\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 1/1]
    [Time since request: 0.079427000 seconds]
    [Request in frame: 44]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    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
```

```
0190  73 65 74 3d 55 54 46 2d  38 0d 0a 0d 0a 0a 3c 68   set=UTF- 8·····<h
01a0  74 6d 6c 3e 0a 0a 43 6f  6e 67 72 61 74 75 6c 61   tml>··Co ngratula
01b0  74 69 6f 6e 73 20 61 67  61 69 6e 21 20 20 4e 6f   tions ag ain!  No
01c0  77 20 79 6f 75 27 76 65  20 64 6f 77 6e 6c 6f 61   w you've  downloa
01d0  64 65 64 20 74 68 65 20  66 69 6c 65 20 6c 61 62   ded the  file lab
```

Line-based text data (data-text-lines), 371 bytes | Packets: 225 · Displayed: 4 (1.8%) · Dropped: 0 (0.0%) | Profile: Default



*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+
10

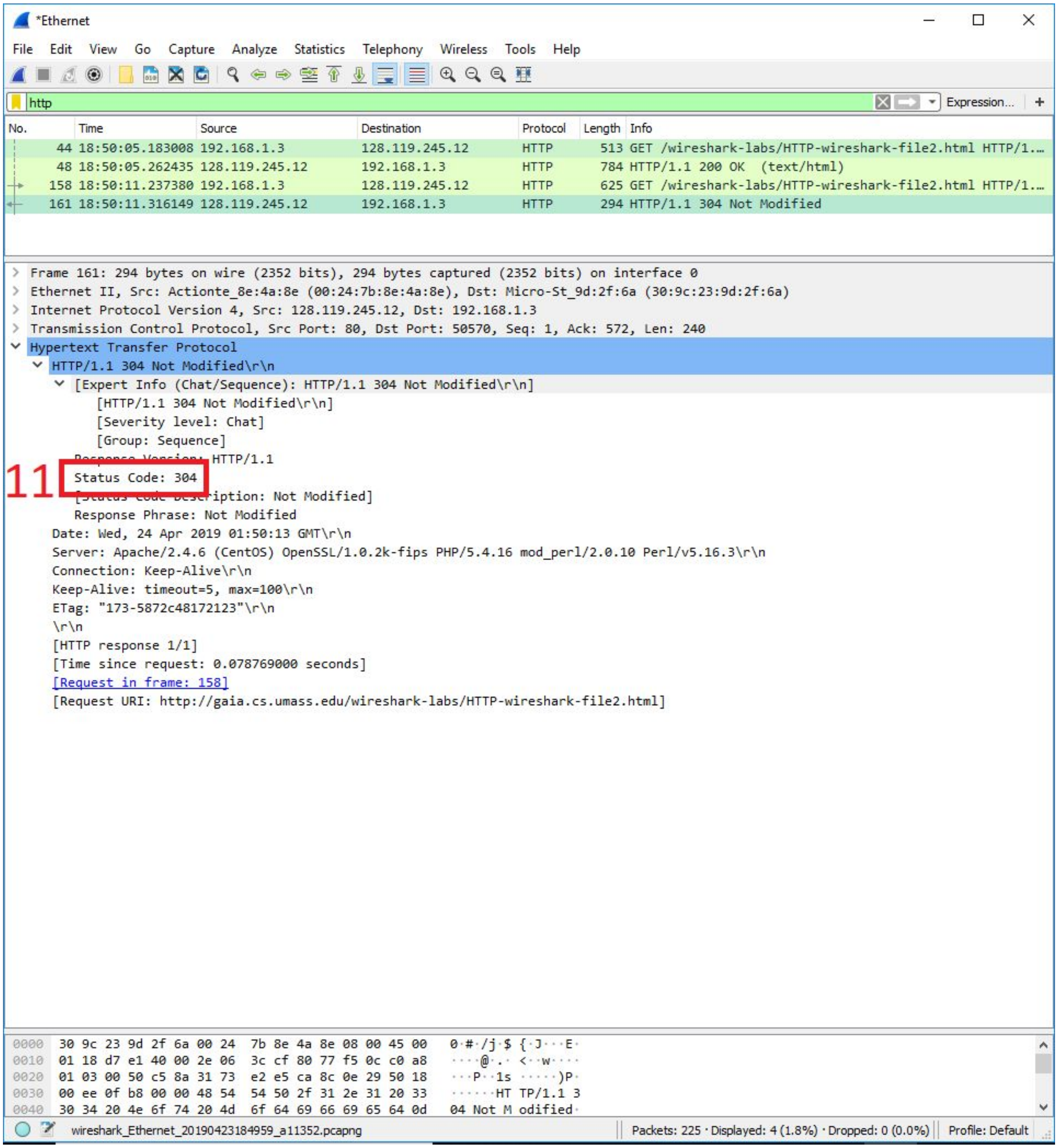
http

```
No.   Time            Source          Destination     Protocol Length Info
   44 18:50:05.183008 192.168.1.3     128.119.245.12  HTTP      513 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.…
   48 18:50:05.262435 128.119.245.12  192.168.1.3     HTTP      784 HTTP/1.1 200 OK  (text/html)
  158 18:50:11.237380 192.168.1.3     128.119.245.12  HTTP      625 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.…
  161 18:50:11.316149 128.119.245.12  192.168.1.3     HTTP      294 HTTP/1.1 304 Not Modified
```

```
> Frame 158: 625 bytes on wire (5000 bits), 625 bytes captured (5000 bits) on interface 0
> Ethernet II, Src: Micro-St_9d:2f:6a (30:9c:23:9d:2f:6a), Dst: Actionte_8e:4a:8e (00:24:7b:8e:4a:8e)
> Internet Protocol Version 4, Src: 192.168.1.3, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 50570, Dst Port: 80, Seq: 1, Ack: 1, Len: 571
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/73.0.3683.103 Safari/537.36\r\
    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: "173-5872c48172123"\r\n
    If-Modified-Since: Tue, 23 Apr 2019 05:59:01 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: 161]
```

```
0000  00 24 7b 8e 4a 8e 30 9c  23 9d 2f 6a 08 00 45 00   ·${·J·0· #·/j··E·
0010  02 63 42 32 40 00 80 06  00 00 c0 a8 01 03 80 77   ·cB2@··· ·······w
0020  f5 0c c5 8a 00 50 ca 8c  0b ee 31 73 e2 e5 50 18   ·····P·· ··1s··P·
0030  01 00 39 85 00 00 47 45  54 20 2f 77 69 72 65 73   ··9···GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
```

wireshark_Ethernet_20190423184959_a11352.pcapng | Packets: 225 · Displayed: 4 (1.8%) · Dropped: 0 (0.0%) | Profile: Default



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

```
http
```

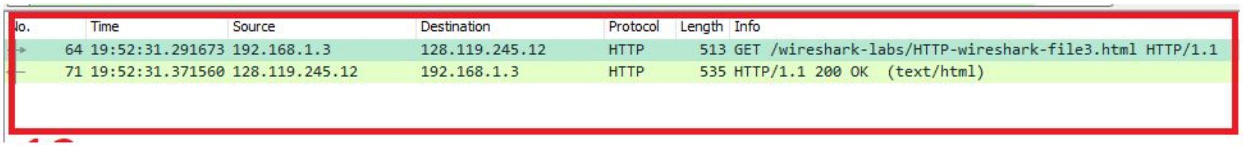
```
No.   Time             Source          Destination     Protocol Length Info
   44 18:50:05.183008 192.168.1.3     128.119.245.12  HTTP       513 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.…
   48 18:50:05.262435 128.119.245.12  192.168.1.3     HTTP       784 HTTP/1.1 200 OK  (text/html)
  158 18:50:11.237380 192.168.1.3     128.119.245.12  HTTP       625 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.…
  161 18:50:11.316149 128.119.245.12  192.168.1.3     HTTP       294 HTTP/1.1 304 Not Modified
```

```
> Frame 161: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface 0
> Ethernet II, Src: Actionte_8e:4a:8e (00:24:7b:8e:4a:8e), Dst: Micro-St_9d:2f:6a (30:9c:23:9d:2f:6a)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.3
> Transmission Control Protocol, Src Port: 80, Dst Port: 50570, Seq: 1, Ack: 572, Len: 240
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
11    Status Code: 304
      [Status Code Description: Not Modified]
      Response Phrase: Not Modified
    Date: Wed, 24 Apr 2019 01:50:13 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: "173-5872c48172123"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.078769000 seconds]
    [Request in frame: 158]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

```
0000  30 9c 23 9d 2f 6a 00 24  7b 8e 4a 8e 08 00 45 00   0·#·/j·$ {·J···E·
0010  01 18 d7 e1 40 00 2e 06  3c cf 80 77 f5 0c c0 a8   ····@·.· <··w····
0020  01 03 00 50 c5 8a 31 73  e2 e5 ca 8c 0e 29 50 18   ···P··1s ·····)P·
0030  00 ee 0f b8 00 00 48 54  54 50 2f 31 2e 31 20 33   ······HT TP/1.1 3
0040  30 34 20 4e 6f 74 20 4d  6f 64 69 66 69 65 64 0d   04 Not M odified·
```

```
wireshark_Ethernet_20190423184959_a11352.pcapng    Packets: 225 · Displayed: 4 (1.8%) · Dropped: 0 (0.0%)    Profile: Default
```

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?

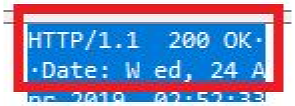


```
No.   Time             Source          Destination     Protocol Length Info
   64 19:52:31.291673 192.168.1.3     128.119.245.12  HTTP       513 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
   71 19:52:31.371560 128.119.245.12  192.168.1.3     HTTP       535 HTTP/1.1 200 OK  (text/html)
```

1 GET request. The first and only packet sent for the GET request contains the GET

message.

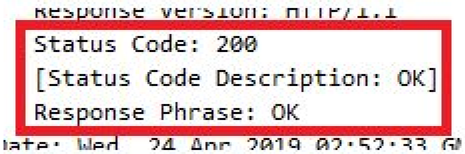
13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?



```
HTTP/1.1  200 OK·
·Date: W ed, 24 A
pr 2019  02:52:33
```

The first packet of the response contains the status code.

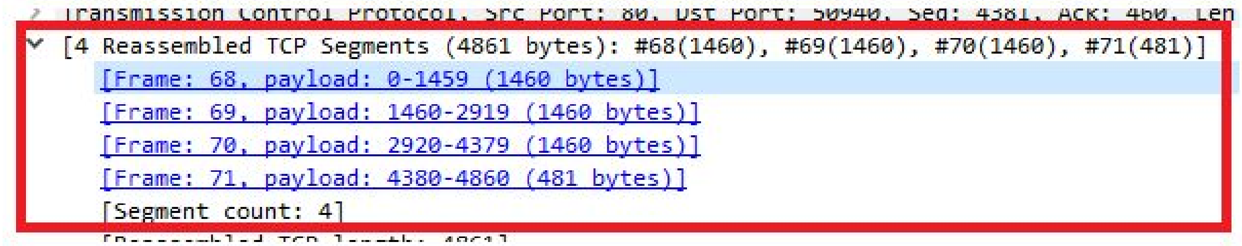
14. What is the status code and phrase in the response?



```
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Date: Wed, 24 Apr 2019 02:52:33 GM
```

200 OK

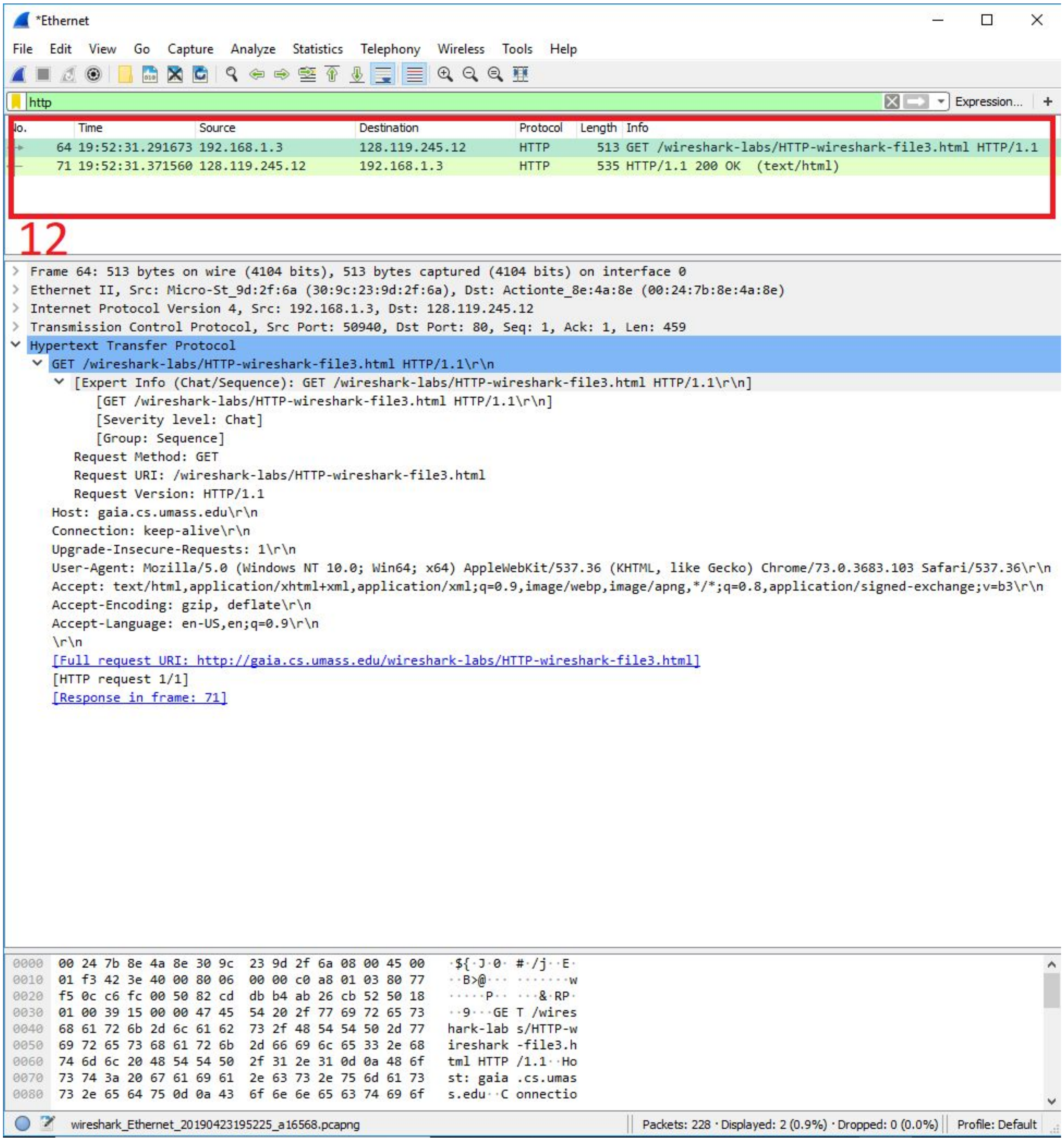
15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?



```
> Transmission Control Protocol, Src Port: 80, Dst Port: 50940, Seq: 4381, Ack: 460, Len
v [4 Reassembled TCP Segments (4861 bytes): #68(1460), #69(1460), #70(1460), #71(481)]
     [Frame: 68, payload: 0-1459 (1460 bytes)]
     [Frame: 69, payload: 1460-2919 (1460 bytes)]
     [Frame: 70, payload: 2920-4379 (1460 bytes)]
     [Frame: 71, payload: 4380-4860 (481 bytes)]
     [Segment count: 4]
     [Reassembled TCP length: 4861]
```

4 segments

Joel Huffman
CS372-400 Spring 2019


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

http

```
No.   Time             Source          Destination     Protocol Length Info
   64 19:52:31.291673 192.168.1.3     128.119.245.12  HTTP      513 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
   71 19:52:31.371560 128.119.245.12  192.168.1.3     HTTP      535 HTTP/1.1 200 OK  (text/html)
```

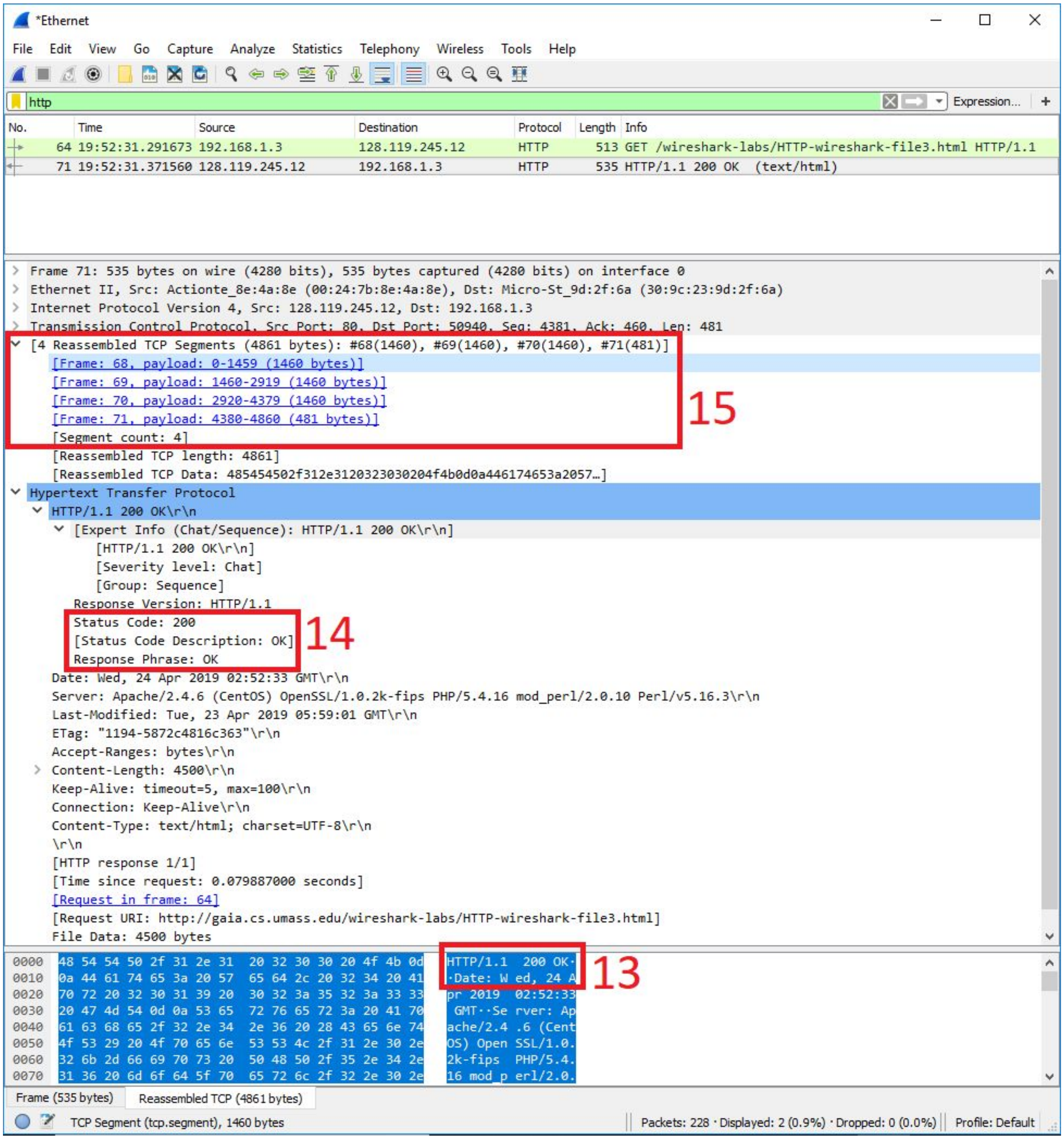
12

```
> Frame 64: 513 bytes on wire (4104 bits), 513 bytes captured (4104 bits) on interface 0
> Ethernet II, Src: Micro-St_9d:2f:6a (30:9c:23:9d:2f:6a), Dst: Actionte_8e:4a:8e (00:24:7b:8e:4a:8e)
> Internet Protocol Version 4, Src: 192.168.1.3, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 50940, Dst Port: 80, Seq: 1, Ack: 1, Len: 459
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
    v [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]
        [GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file3.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/73.0.3683.103 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: 71]
```

```
0000  00 24 7b 8e 4a 8e 30 9c  23 9d 2f 6a 08 00 45 00   ·${·J·0· #·/j··E·
0010  01 f3 42 3e 40 00 80 06  00 00 c0 a8 01 03 80 77   ··B>@··· ·······w
0020  f5 0c c6 fc 00 50 82 cd  db b4 ab 26 cb 52 50 18   ·····P·· ···&·RP·
0030  01 00 39 15 00 00 47 45  54 20 2f 77 69 72 65 73   ··9···GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 33 2e 68   ireshark -file3.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio
```

wireshark_Ethernet_20190423195225_a16568.pcapng | Packets: 228 · Displayed: 2 (0.9%) · Dropped: 0 (0.0%) | Profile: Default

Joel Huffman
CS372-400 Spring 2019


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

```
No.  Time             Source          Destination     Protocol Length Info
  64 19:52:31.291673 192.168.1.3     128.119.245.12  HTTP      513 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  71 19:52:31.371560 128.119.245.12  192.168.1.3     HTTP      535 HTTP/1.1 200 OK  (text/html)
```

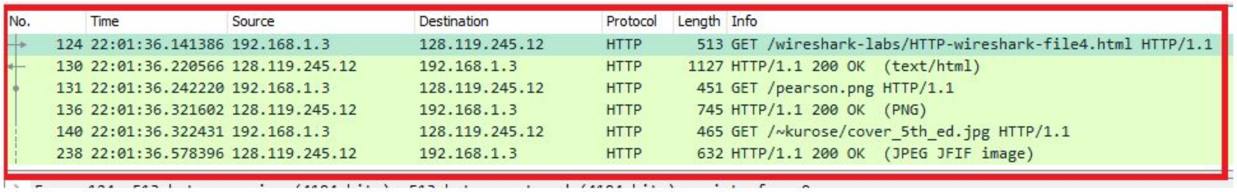
```
> Frame 71: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface 0
> Ethernet II, Src: Actionte_8e:4a:8e (00:24:7b:8e:4a:8e), Dst: Micro-St_9d:2f:6a (30:9c:23:9d:2f:6a)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.3
> Transmission Control Protocol, Src Port: 80, Dst Port: 50940, Seq: 4381, Ack: 460, Len: 481
v [4 Reassembled TCP Segments (4861 bytes): #68(1460), #69(1460), #70(1460), #71(481)]
    [Frame: 68, payload: 0-1459 (1460 bytes)]
    [Frame: 69, payload: 1460-2919 (1460 bytes)]
    [Frame: 70, payload: 2920-4379 (1460 bytes)]
    [Frame: 71, payload: 4380-4860 (481 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2057…]
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: Wed, 24 Apr 2019 02:52:33 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: Tue, 23 Apr 2019 05:59:01 GMT\r\n
    ETag: "1194-5872c4816c363"\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: 0.079887000 seconds]
    [Request in frame: 64]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
    File Data: 4500 bytes
```

```
0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK·
0010  0a 44 61 74 65 3a 20 57  65 64 2c 20 32 34 20 41   ·Date: W ed, 24 A
0020  70 72 20 32 30 31 39 20  30 32 3a 35 32 3a 33 33   pr 2019  02:52:33
0030  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT··Se rver: Ap
0040  61 63 68 65 2f 32 2e 34  2e 36 20 28 43 65 6e 74   ache/2.4 .6 (Cent
0050  4f 53 29 20 4f 70 65 6e  53 53 4c 2f 31 2e 30 2e   OS) Open SSL/1.0.
0060  32 6b 2d 66 69 70 73 20  50 48 50 2f 35 2e 34 2e   2k-fips  PHP/5.4.
0070  31 36 20 6d 6f 64 5f 70  65 72 6c 2f 32 2e 30 2e   16 mod_p erl/2.0.
```

Frame (535 bytes) | Reassembled TCP (4861 bytes)

TCP Segment (tcp.segment), 1460 bytes | Packets: 228 · Displayed: 2 (0.9%) · Dropped: 0 (0.0%) | Profile: Default

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

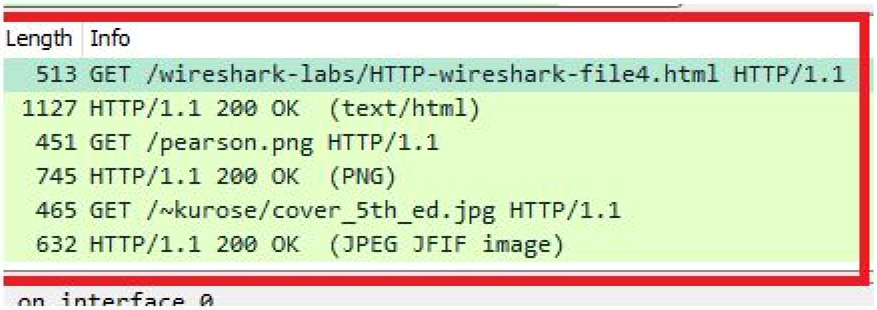


```
No.  Time             Source          Destination     Protocol Length Info
 124 22:01:36.141386 192.168.1.3     128.119.245.12  HTTP      513 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
 130 22:01:36.220566 128.119.245.12  192.168.1.3     HTTP     1127 HTTP/1.1 200 OK  (text/html)
 131 22:01:36.242220 192.168.1.3     128.119.245.12  HTTP      451 GET /pearson.png HTTP/1.1
 136 22:01:36.321602 128.119.245.12  192.168.1.3     HTTP      745 HTTP/1.1 200 OK  (PNG)
 140 22:01:36.322431 192.168.1.3     128.119.245.12  HTTP      465 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
 238 22:01:36.578396 128.119.245.12  192.168.1.3     HTTP      632 HTTP/1.1 200 OK  (JPEG JFIF image)
```

3 GET requests were sent. The messages all went to 128.119.245.12 for the HTML/text,

and two images.

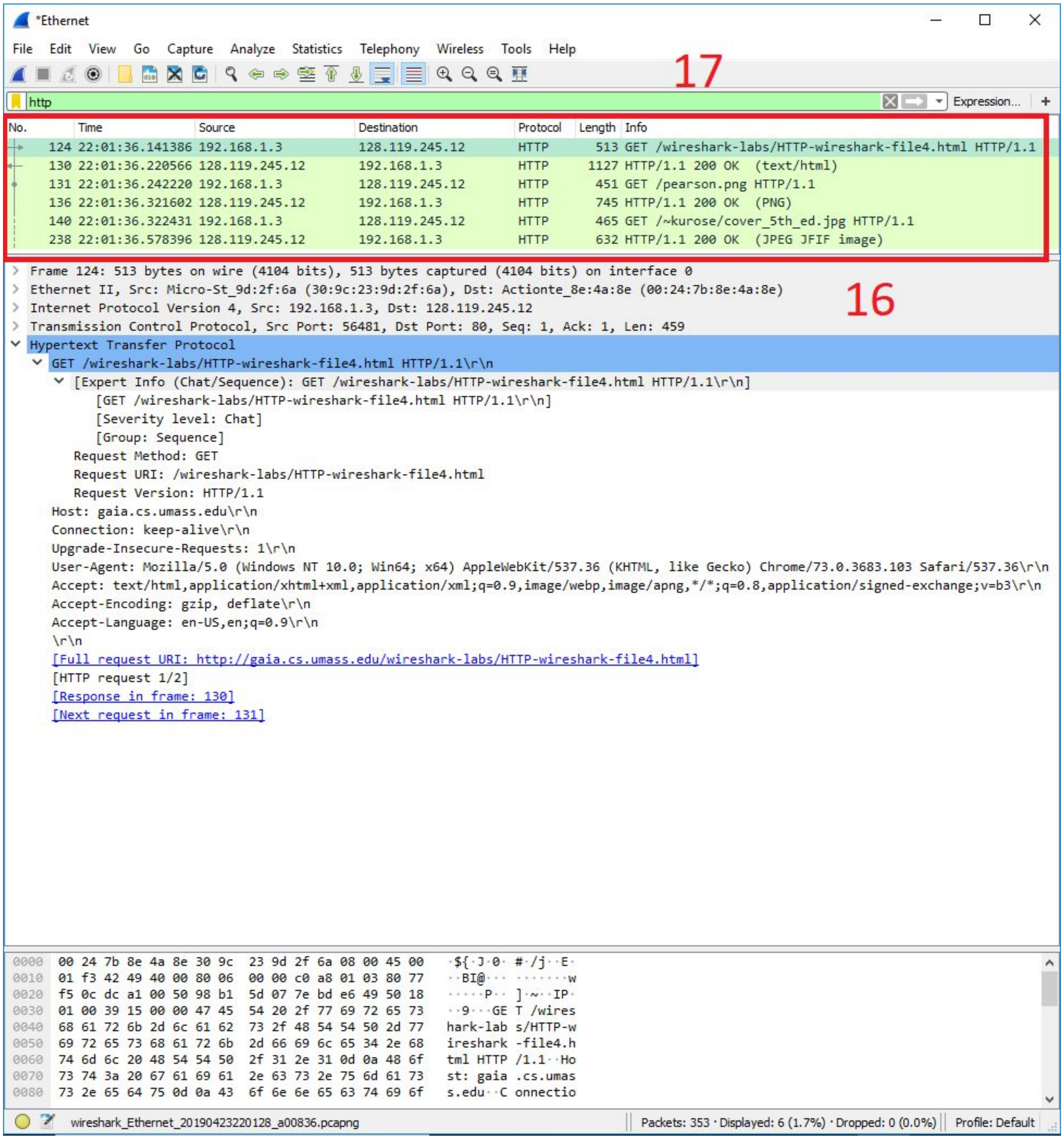
17. **Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.**



```
Length  Info
   513  GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
  1127  HTTP/1.1 200 OK  (text/html)
   451  GET /pearson.png HTTP/1.1
   745  HTTP/1.1 200 OK  (PNG)
   465  GET /~kurose/cover_5th_ed.jpg HTTP/1.1
   632  HTTP/1.1 200 OK  (JPEG JFIF image)
 on interface 0
```

The images were downloaded serially/sequentially because the GET requests were sent sequentially and not at the same time. Furthermore, the timestamps are shown for each response and while they're close to one another, they don't occur at the same time.

Joel Huffman
CS372-400 Spring 2019


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

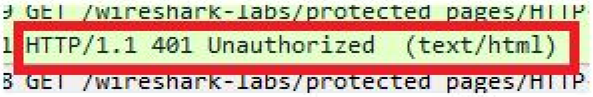
```
No.  Time            Source          Destination     Protocol Length Info
 124 22:01:36.141386 192.168.1.3     128.119.245.12  HTTP      513 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
 130 22:01:36.220566 128.119.245.12  192.168.1.3     HTTP     1127 HTTP/1.1 200 OK  (text/html)
 131 22:01:36.242220 192.168.1.3     128.119.245.12  HTTP      451 GET /pearson.png HTTP/1.1
 136 22:01:36.321602 128.119.245.12  192.168.1.3     HTTP      745 HTTP/1.1 200 OK  (PNG)
 140 22:01:36.322431 192.168.1.3     128.119.245.12  HTTP      465 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
 238 22:01:36.578396 128.119.245.12  192.168.1.3     HTTP      632 HTTP/1.1 200 OK  (JPEG JFIF image)
```

```
> Frame 124: 513 bytes on wire (4104 bits), 513 bytes captured (4104 bits) on interface 0
> Ethernet II, Src: Micro-St_9d:2f:6a (30:9c:23:9d:2f:6a), Dst: Actionte_8e:4a:8e (00:24:7b:8e:4a:8e)
> Internet Protocol Version 4, Src: 192.168.1.3, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 56481, Dst Port: 80, Seq: 1, Ack: 1, Len: 459
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n
    v [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n]
        [GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file4.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/73.0.3683.103 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 1/2]
    [Response in frame: 130]
    [Next request in frame: 131]
```

```
0000  00 24 7b 8e 4a 8e 30 9c  23 9d 2f 6a 08 00 45 00   ·${·J·0· #·/j··E·
0010  01 f3 42 49 40 00 80 06  00 00 c0 a8 01 03 80 77   ··BI@··· ·······w
0020  f5 0c dc a1 00 50 98 b1  5d 07 7e bd e6 49 50 18   ·····P·· ]·~··IP·
0030  01 00 39 15 00 00 47 45  54 20 2f 77 69 72 65 73   ··9···GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 34 2e 68   ireshark -file4.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio
```

wireshark_Ethernet_20190423220128_a00836.pcapng | Packets: 353 · Displayed: 6 (1.7%) · Dropped: 0 (0.0%) | Profile: Default

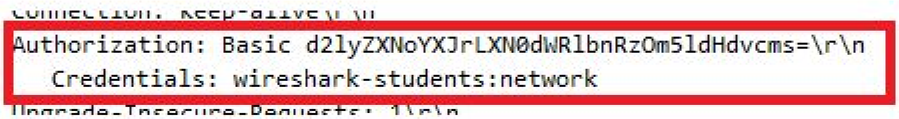
18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?



```
9 GET /wireshark-labs/protected pages/HTTP
1 HTTP/1.1 401 Unauthorized  (text/html)
3 GET /wireshark-labs/protected pages/HTTP
```

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?**



```
Connection: keep-alive\r\n
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
  Credentials: wireshark-students:network
Upgrade-Insecure-Requests: 1\r\n
```

Authorization with the credentials we entered into the username and password fields.