# CSE4344/5344

# Project 2 (Spring 2021)

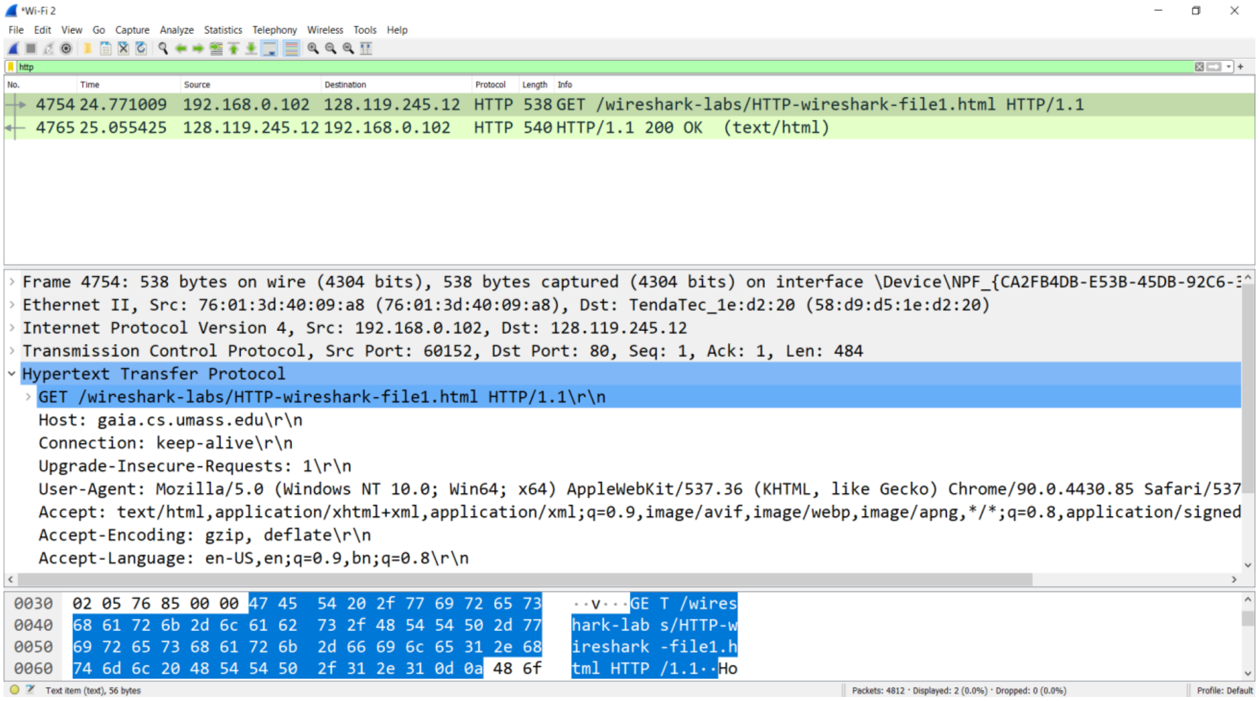
## Wireshark Lab: HTTP

Nudrat Nawal Saber

1001733394

## The Basic HTTP GET/response interaction

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


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info

```
4754 24.771009  192.168.0.102  128.119.245.12  HTTP  538 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
4765 25.055425  128.119.245.12 192.168.0.102   HTTP  540 HTTP/1.1 200 OK  (text/html)
```

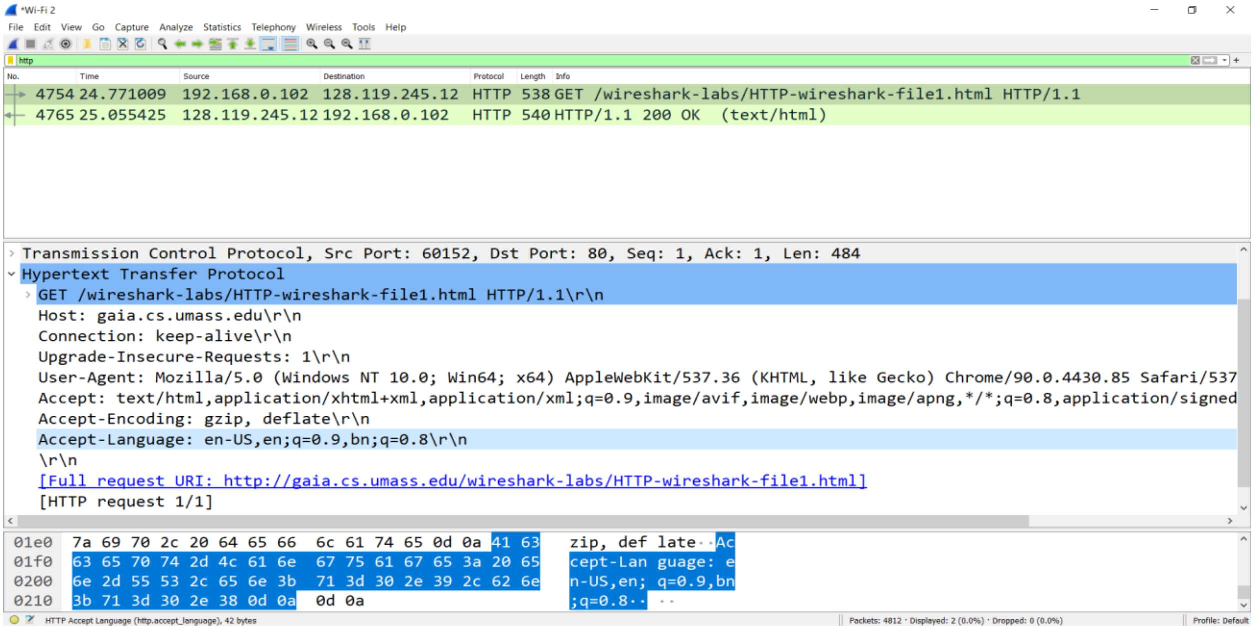
```
> Frame 4754: 538 bytes on wire (4304 bits), 538 bytes captured (4304 bits) on interface \Device\NPF_{CA2FB4DB-E53B-45DB-92C6-3
> Ethernet II, Src: 76:01:3d:40:09:a8 (76:01:3d:40:09:a8), Dst: TendaTec_1e:d2:20 (58:d9:d5:1e:d2:20)
> Internet Protocol Version 4, Src: 192.168.0.102, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 60152, Dst Port: 80, Seq: 1, Ack: 1, Len: 484
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/90.0.4430.85 Safari/537
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,bn;q=0.8\r\n
```

```
0030  02 05 76 85 00 00 47 45  54 20 2f 77 69 72 65 73   ··v···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 31 2e 68   ireshark -file1.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
```

Text item (text), 56 bytes | Packets: 4812 · Displayed: 2 (0.0%) · Dropped: 0 (0.0%) | Profile: Default

**Answer:** Both my browser and the server are running on HTTP 1.1

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


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info

```
4754 24.771009  192.168.0.102  128.119.245.12  HTTP  538 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
4765 25.055425  128.119.245.12 192.168.0.102   HTTP  540 HTTP/1.1 200 OK  (text/html)
```

```
> Transmission Control Protocol, Src Port: 60152, Dst Port: 80, Seq: 1, Ack: 1, Len: 484
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/90.0.4430.85 Safari/537
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,bn;q=0.8\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
```

```
01e0  7a 69 70 2c 20 64 65 66  6c 61 74 65 0d 0a 41 63   zip, def late··Ac
01f0  63 65 70 74 2d 4c 61 6e  67 75 61 67 65 3a 20 65   cept-Lan guage: e
0200  6e 2d 55 53 2c 65 6e 3b  71 3d 30 2e 39 2c 62 6e   n-US,en; q=0.9,bn
0210  3b 71 3d 30 2e 38 0d 0a  0d 0a                     ;q=0.8·· ··
```

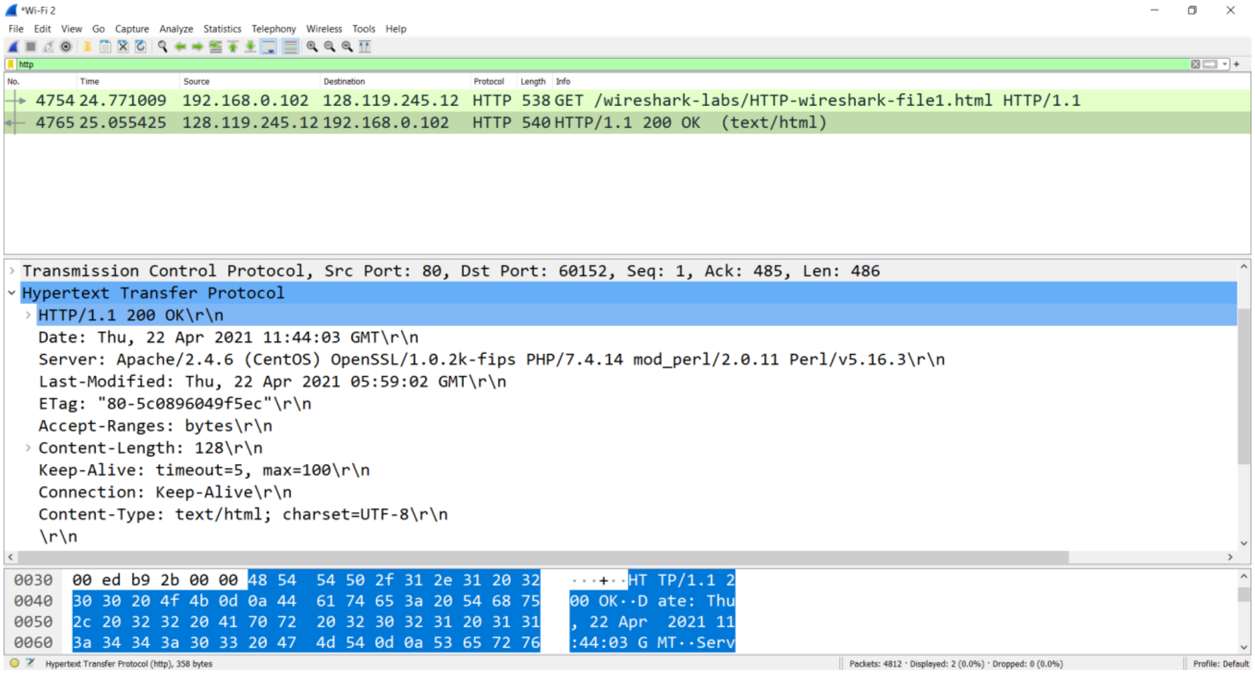
HTTP Accept Language (http.accept_language), 42 bytes | Packets: 4812 · Displayed: 2 (0.0%) · Dropped: 0 (0.0%) | Profile: Default

**Answer:** From the picture we can see the browser will accept en-US language.

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

**Answer**: From the previous picture we can see, My IP address is 192.168.0.102 and IP address of gaia.cs.umass.edu server is 128.119.245.12

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



*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
No.   Time      Source          Destination     Protocol Length Info
4754 24.771009  192.168.0.102   128.119.245.12  HTTP     538    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
4765 25.055425  128.119.245.12  192.168.0.102   HTTP     540    HTTP/1.1 200 OK  (text/html)
```

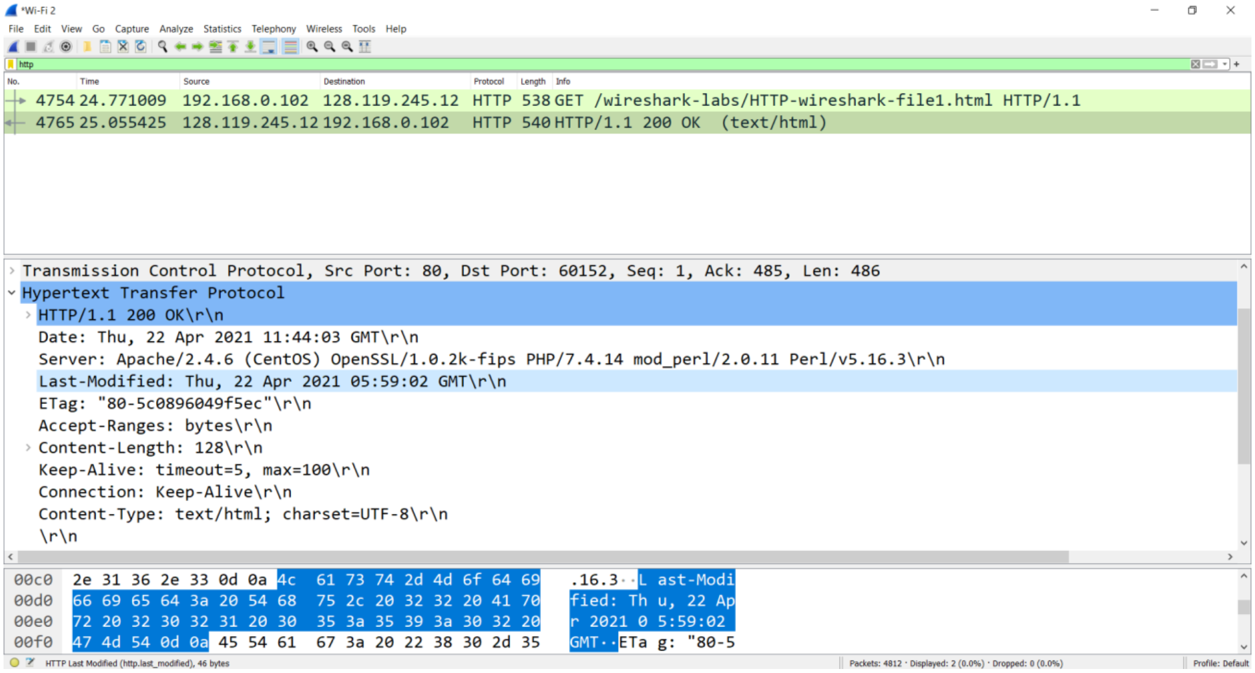
```
> Transmission Control Protocol, Src Port: 80, Dst Port: 60152, Seq: 1, Ack: 485, Len: 486
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Thu, 22 Apr 2021 11:44:03 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Thu, 22 Apr 2021 05:59:02 GMT\r\n
    ETag: "80-5c0896049f5ec"\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
```

```
0030  00 ed b9 2b 00 00 48 54  54 50 2f 31 2e 31 20 32   ···+··HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 54 68 75   00 OK··D ate: Thu
0050  2c 20 32 32 20 41 70 72  20 32 30 32 31 20 31 31   , 22 Apr  2021 11
0060  3a 34 34 3a 30 33 20 47  4d 54 0d 0a 53 65 72 76   :44:03 G MT··Serv
```

```
Hypertext Transfer Protocol (http), 358 bytes    Packets: 4812 · Displayed: 2 (0.0%) · Dropped: 0 (0.0%)    Profile: Default
```

**Answer**: We can see the server returned 200 status code to my browser.

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


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time      Source         Destination    Protocol Length Info
4754 24.771009  192.168.0.102  128.119.245.12  HTTP  538 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
4765 25.055425  128.119.245.12 192.168.0.102   HTTP  540 HTTP/1.1 200 OK  (text/html)
```

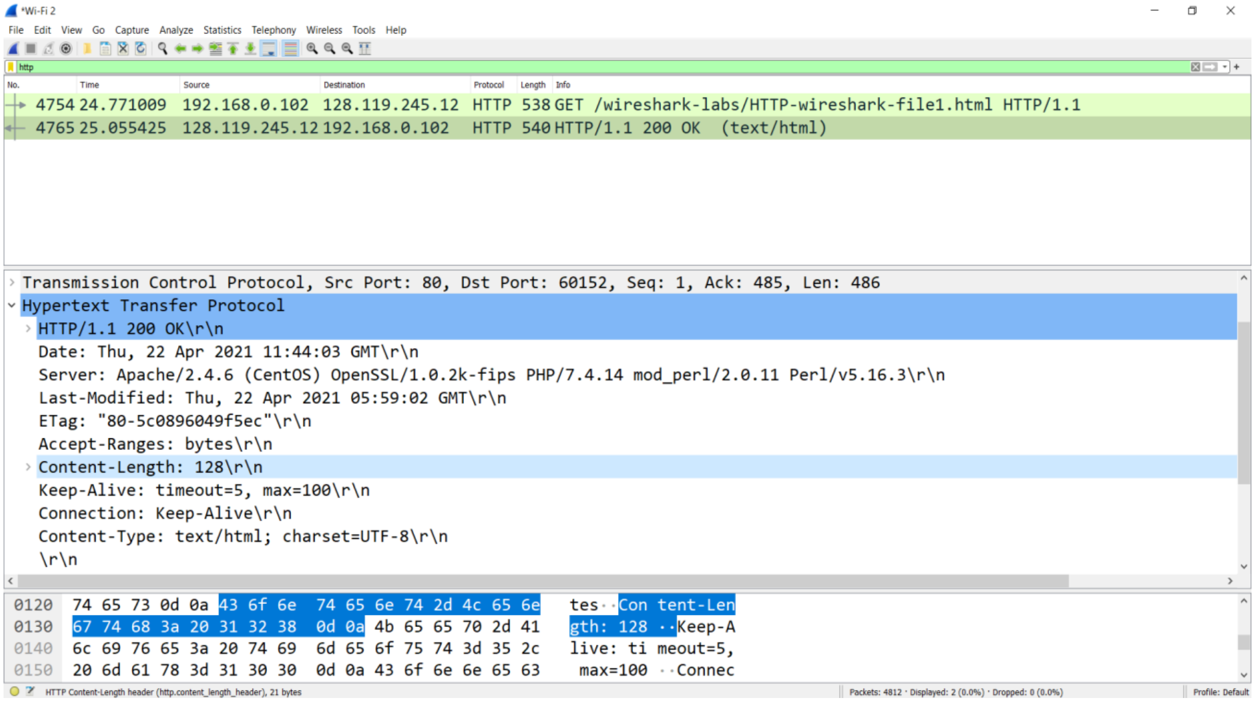
```
> Transmission Control Protocol, Src Port: 80, Dst Port: 60152, Seq: 1, Ack: 485, Len: 486
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Thu, 22 Apr 2021 11:44:03 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Thu, 22 Apr 2021 05:59:02 GMT\r\n
    ETag: "80-5c0896049f5ec"\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
```

```
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 68  75 2c 20 32 32 20 41 70   fied: Th u, 22 Ap
00e0  72 20 32 30 32 31 20 30  35 3a 35 39 3a 30 32 20   r 2021 0 5:59:02
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 38 30 2d 35   GMT··ETa g: "80-5
```

```
HTTP Last Modified (http.last_modified), 46 bytes    Packets: 4812 · Displayed: 2 (0.0%) · Dropped: 0 (0.0%)    Profile: Default
```

**Answer**: From the picture we can see it was last modified on Thu, 22 Apr 2021 05:59:02 GMT

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


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time      Source         Destination    Protocol Length Info
4754 24.771009  192.168.0.102  128.119.245.12  HTTP  538 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
4765 25.055425  128.119.245.12 192.168.0.102   HTTP  540 HTTP/1.1 200 OK  (text/html)
```

```
> Transmission Control Protocol, Src Port: 80, Dst Port: 60152, Seq: 1, Ack: 485, Len: 486
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Thu, 22 Apr 2021 11:44:03 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, 22 Apr 2021 05:59:02 GMT\r\n
    ETag: "80-5c0896049f5ec"\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
```

```
0120  74 65 73 0d 0a 43 6f 6e  74 65 6e 74 2d 4c 65 6e   tes··Con tent-Len
0130  67 74 68 3a 20 31 32 38  0d 0a 4b 65 65 70 2d 41   gth: 128 ··Keep-A
0140  6c 69 76 65 3a 20 74 69  6d 65 6f 75 74 3d 35 2c   live: ti meout=5,
0150  20 6d 61 78 3d 31 30 30  0d 0a 43 6f 6e 6e 65 63    max=100 ··Connec
```

```
HTTP Content-Length header (http.content_length_header), 21 bytes    Packets: 4812 · Displayed: 2 (0.0%) · Dropped: 0 (0.0%)    Profile: Default
```

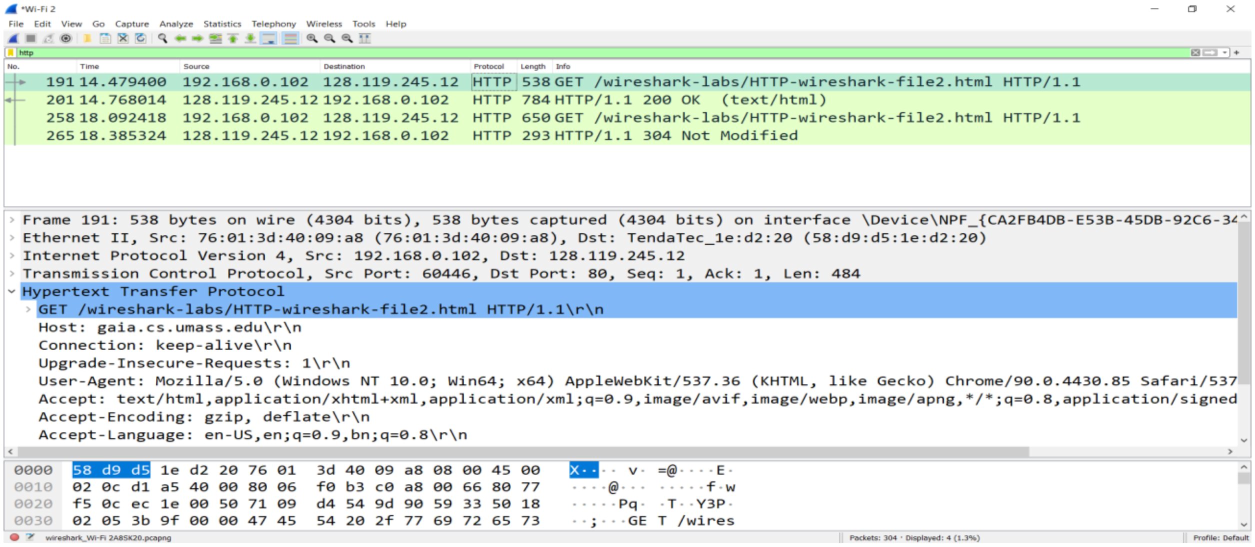
**Answer**: From the Content-Length header we can see 128 bytes of content are being returned to my browser

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.**

**Answer: No**

## The HTTP CONDITIONAL GET/response interaction

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?**


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.  Time       Source          Destination     Protocol Length Info
191  14.479400  192.168.0.102   128.119.245.12  HTTP     538    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
201  14.768014  128.119.245.12  192.168.0.102   HTTP     784    HTTP/1.1 200 OK  (text/html)
258  18.092418  192.168.0.102   128.119.245.12  HTTP     650    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
265  18.385324  128.119.245.12  192.168.0.102   HTTP     293    HTTP/1.1 304 Not Modified
```

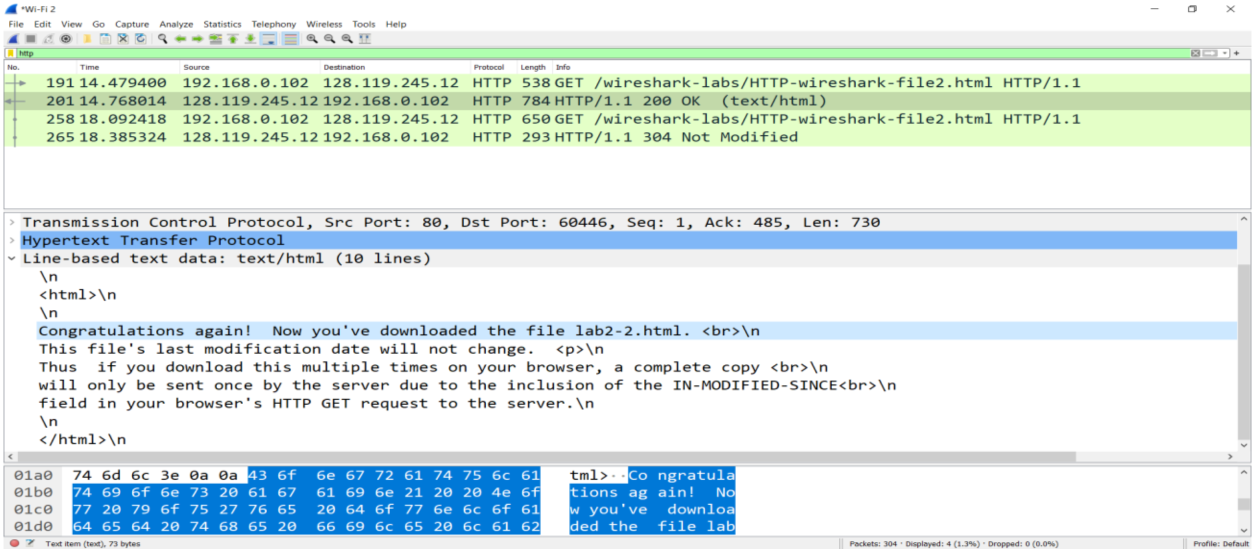
```
> Frame 191: 538 bytes on wire (4304 bits), 538 bytes captured (4304 bits) on interface \Device\NPF_{CA2FB4DB-E53B-45DB-92C6-34
> Ethernet II, Src: 76:01:3d:40:09:a8 (76:01:3d:40:09:a8), Dst: TendaTec_1e:d2:20 (58:d9:d5:1e:d2:20)
> Internet Protocol Version 4, Src: 192.168.0.102, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 60446, Dst Port: 80, Seq: 1, Ack: 1, Len: 484
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/90.0.4430.85 Safari/537
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,bn;q=0.8\r\n
```

```
0000  58 d9 d5 1e d2 20 76 01  3d 40 09 a8 08 00 45 00   X···· v· =@····E·
0010  02 0c d1 a5 40 00 80 06  f0 b3 c0 a8 00 66 80 77   ····@··· ·····f·w
0020  f5 0c ec 1e 00 50 71 09  d4 54 9d 90 59 33 50 18   ·····Pq· ·T··Y3P·
0030  02 05 3b 9f 00 00 47 45  54 20 2f 77 69 72 65 73   ··;···GE T /wires
```

wireshark_Wi-Fi 2A8SK20.pcapng
Packets: 304 · Displayed: 4 (1.3%)
Profile: Default

**Answer**: No

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


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
Text item (text), 73 bytes
Packets: 304 · Displayed: 4 (1.3%) · Dropped: 0 (0.0%)
Profile: Default

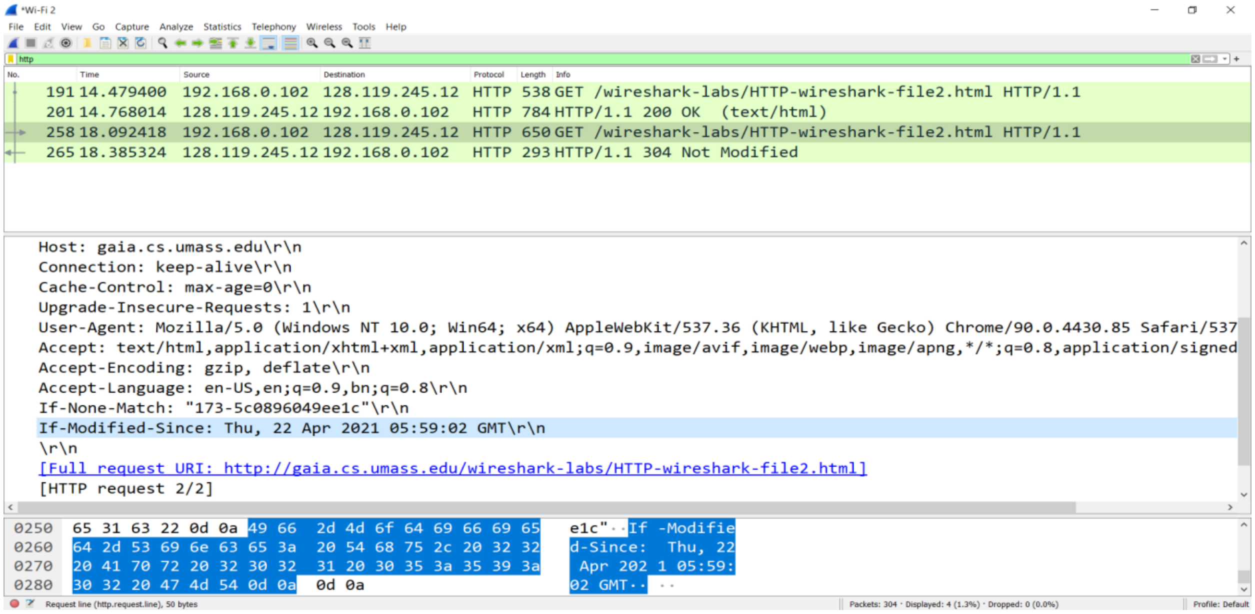
```
191 14.479400  192.168.0.102  128.119.245.12 HTTP 538 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
201 14.768014  128.119.245.12 192.168.0.102  HTTP 784 HTTP/1.1 200 OK  (text/html)
258 18.092418  192.168.0.102  128.119.245.12 HTTP 650 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
265 18.385324  128.119.245.12 192.168.0.102  HTTP 293 HTTP/1.1 304 Not Modified
```

```
> Transmission Control Protocol, Src Port: 80, Dst Port: 60446, Seq: 1, Ack: 485, Len: 730
> Hypertext Transfer Protocol
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
```

```
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
```

**Answer**: Yes. We can see the file contents in Line-base text data field.

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?**


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
Request line (http.request.line), 50 bytes
Packets: 304 · Displayed: 4 (1.3%) · Dropped: 0 (0.0%)
Profile: Default

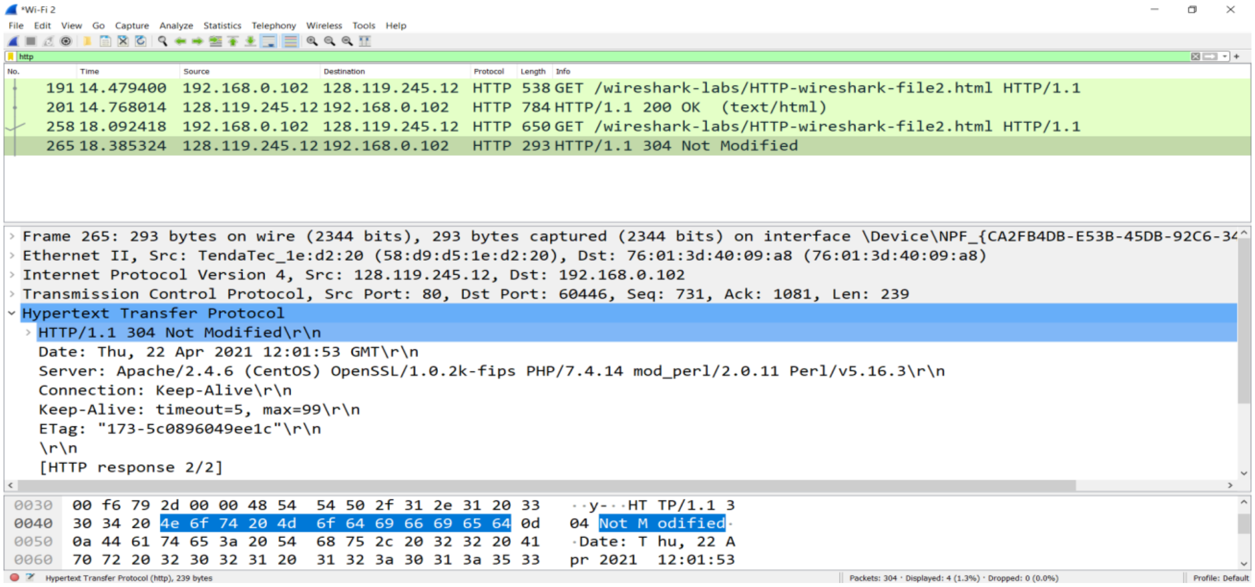
```
191 14.479400  192.168.0.102  128.119.245.12 HTTP 538 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
201 14.768014  128.119.245.12 192.168.0.102  HTTP 784 HTTP/1.1 200 OK  (text/html)
258 18.092418  192.168.0.102  128.119.245.12 HTTP 650 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
265 18.385324  128.119.245.12 192.168.0.102  HTTP 293 HTTP/1.1 304 Not Modified
```

```
    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/90.0.4430.85 Safari/537
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,bn;q=0.8\r\n
    If-None-Match: "173-5c0896049ee1c"\r\n
    If-Modified-Since: Thu, 22 Apr 2021 05:59:02 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 2/2]
```

```
0250  65 31 63 22 0d 0a 49 66  2d 4d 6f 64 69 66 69 65   e1c"··If -Modifie
0260  64 2d 53 69 6e 63 65 3a  20 54 68 75 2c 20 32 32   d-Since:  Thu, 22
0270  20 41 70 72 20 32 30 32  31 20 30 35 3a 35 39 3a    Apr 202 1 05:59:
0280  30 32 20 47 4d 54 0d 0a  0d 0a                     02 GMT·· ··
```

**Answer**: Yes. The information follows the "IF-MODIFIED-SINCE:" header is Thu, 22 Apr 2021 05:59:02 GMT. It indicates the time of the last modification of the file from the previous get request.

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.**



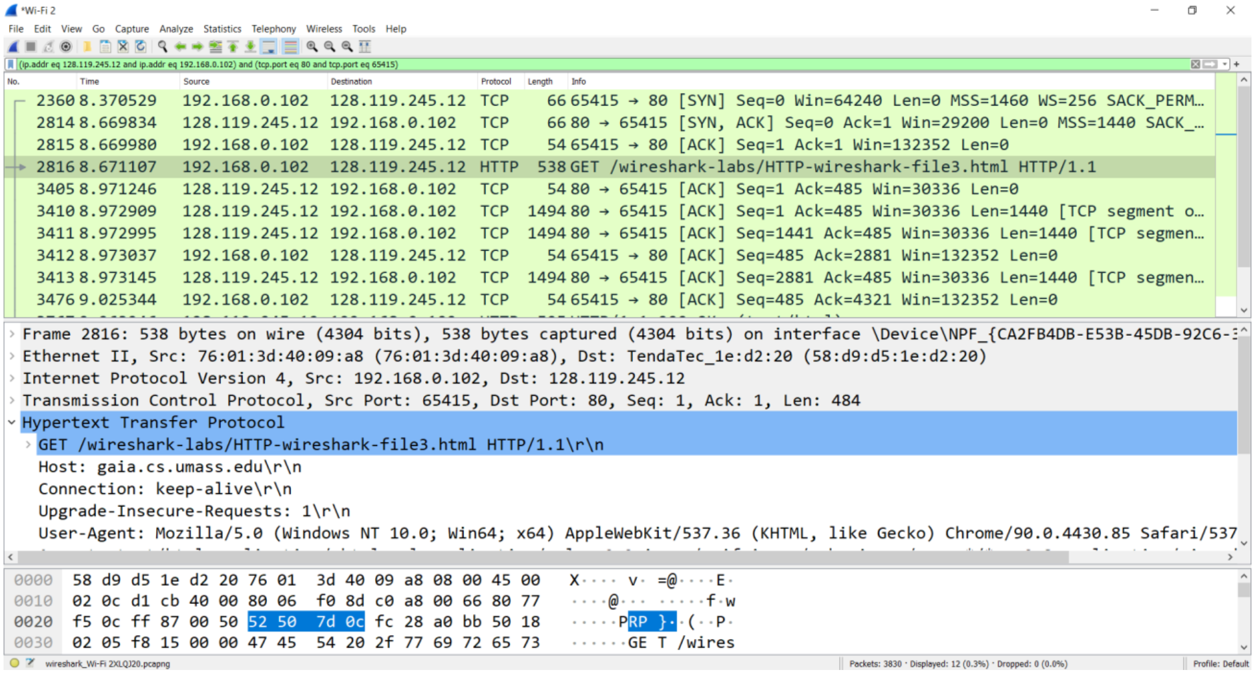
*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
No.  Time      Source         Destination    Protocol Length Info
 191 14.479400 192.168.0.102  128.119.245.12 HTTP  538 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 201 14.768014 128.119.245.12 192.168.0.102  HTTP  784 HTTP/1.1 200 OK  (text/html)
 258 18.092418 192.168.0.102  128.119.245.12 HTTP  650 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 265 18.385324 128.119.245.12 192.168.0.102  HTTP  293 HTTP/1.1 304 Not Modified

> Frame 265: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{CA2FB4DB-E53B-45DB-92C6-34
> Ethernet II, Src: TendaTec_1e:d2:20 (58:d9:d5:1e:d2:20), Dst: 76:01:3d:40:09:a8 (76:01:3d:40:09:a8)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.102
> Transmission Control Protocol, Src Port: 80, Dst Port: 60446, Seq: 731, Ack: 1081, Len: 239
v Hypertext Transfer Protocol
  > HTTP/1.1 304 Not Modified\r\n
    Date: Thu, 22 Apr 2021 12:01:53 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
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=99\r\n
    ETag: "173-5c0896049ee1c"\r\n
    \r\n
    [HTTP response 2/2]

0030  00 f6 79 2d 00 00 48 54  54 50 2f 31 2e 31 20 33   ··y-··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·
0050  0a 44 61 74 65 3a 20 54  68 75 2c 20 32 32 20 41   ·Date: T hu, 22 A
0060  70 72 20 32 30 32 31 20  31 32 3a 30 31 3a 35 33   pr 2021  12:01:53

Hypertext Transfer Protocol (http), 239 bytes    Packets: 304 · Displayed: 4 (1.3%) · Dropped: 0 (0.0%)    Profile: Default
```

**Answer**: The status code and phrase returned from the server is HTTP/1.1 304 Not Modified. Because the server didn't return the contents of file since the browser loaded it from its cache.

## Retrieving Long Documents

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?**

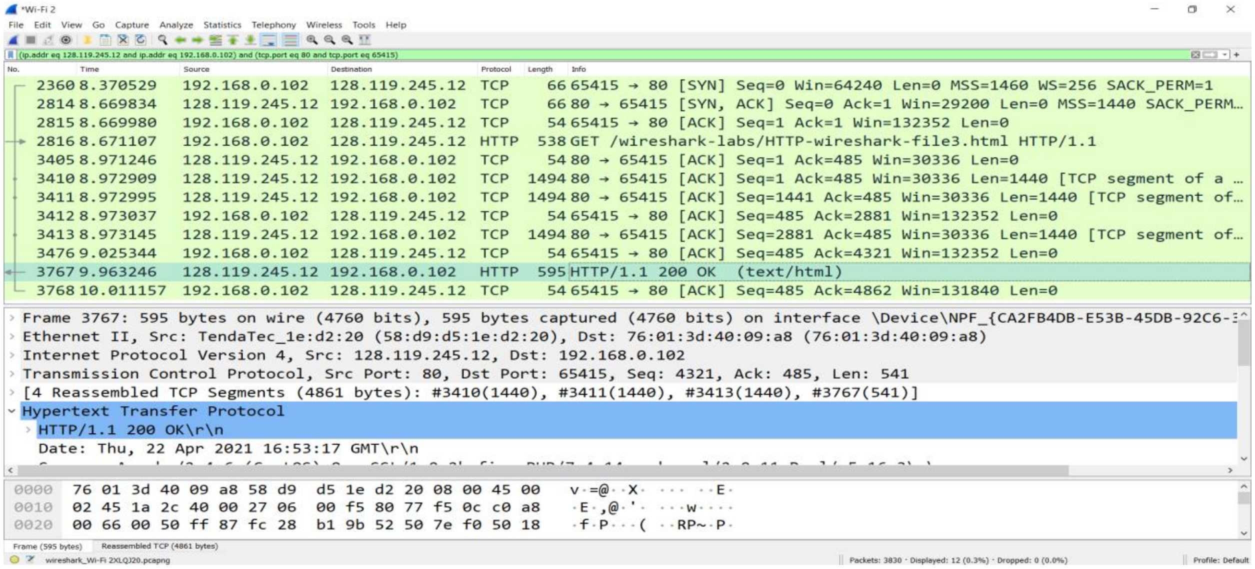


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
(ip.addr eq 128.119.245.12 and ip.addr eq 192.168.0.102) and (tcp.port eq 80 and tcp.port eq 65415)
No.  Time     Source         Destination    Protocol Length Info
2360 8.370529 192.168.0.102  128.119.245.12 TCP    66 65415 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM…
2814 8.669834 128.119.245.12 192.168.0.102  TCP    66 80 → 65415 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_…
2815 8.669980 192.168.0.102  128.119.245.12 TCP    54 65415 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
2816 8.671107 192.168.0.102  128.119.245.12 HTTP  538 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
3405 8.971246 128.119.245.12 192.168.0.102  TCP    54 80 → 65415 [ACK] Seq=1 Ack=485 Win=30336 Len=0
3410 8.972909 128.119.245.12 192.168.0.102  TCP  1494 80 → 65415 [ACK] Seq=1 Ack=485 Win=30336 Len=1440 [TCP segment o…
3411 8.972995 128.119.245.12 192.168.0.102  TCP  1494 80 → 65415 [ACK] Seq=1441 Ack=485 Win=30336 Len=1440 [TCP segmen…
3412 8.973037 192.168.0.102  128.119.245.12 TCP    54 65415 → 80 [ACK] Seq=485 Ack=2881 Win=132352 Len=0
3413 8.973145 128.119.245.12 192.168.0.102  TCP  1494 80 → 65415 [ACK] Seq=2881 Ack=485 Win=30336 Len=1440 [TCP segmen…
3476 9.025344 192.168.0.102  128.119.245.12 TCP    54 65415 → 80 [ACK] Seq=485 Ack=4321 Win=132352 Len=0

> Frame 2816: 538 bytes on wire (4304 bits), 538 bytes captured (4304 bits) on interface \Device\NPF_{CA2FB4DB-E53B-45DB-92C6-3
> Ethernet II, Src: 76:01:3d:40:09:a8 (76:01:3d:40:09:a8), Dst: TendaTec_1e:d2:20 (58:d9:d5:1e:d2:20)
> Internet Protocol Version 4, Src: 192.168.0.102, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 65415, Dst Port: 80, Seq: 1, Ack: 1, Len: 484
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/90.0.4430.85 Safari/537

0000  58 d9 d5 1e d2 20 76 01  3d 40 09 a8 08 00 45 00   X···· v· =@····E·
0010  02 0c d1 cb 40 00 80 06  f0 8d c0 a8 00 66 80 77   ····@··· ·····f·w
0020  f5 0c ff 87 00 50 52 50  7d 0c fc 28 a0 bb 50 18   ·····PRP }··(··P·
0030  02 05 f8 15 00 00 47 45  54 20 2f 77 69 72 65 73   ······GE T /wires

wireshark_Wi-Fi 2XLQJ20.pcapng    Packets: 3830 · Displayed: 12 (0.3%) · Dropped: 0 (0.0%)    Profile: Default
```

**Answer**: From the picture we can see my browser send 1 HTTP GET request message. The packet number 2816 in the trace contains the GET message for the Bill or Rights.

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



*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

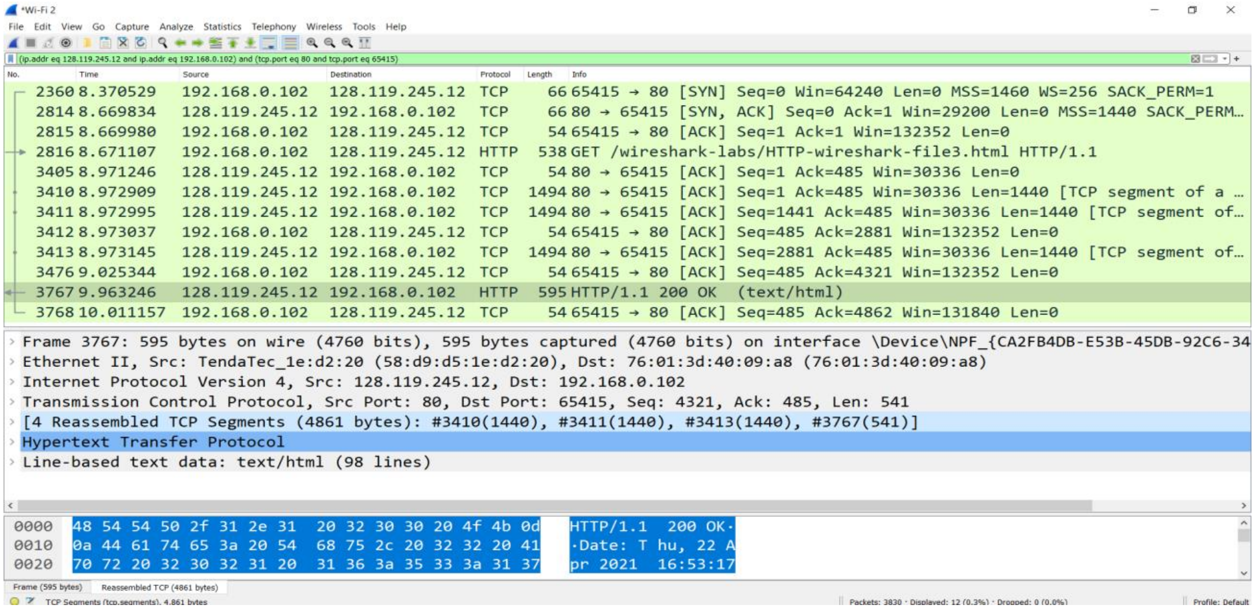
```
(ip.addr eq 128.119.245.12 and ip.addr eq 192.168.0.102) and (tcp.port eq 80 and tcp.port eq 65415)

No.   Time      Source          Destination     Protocol Length Info
2360 8.370529   192.168.0.102   128.119.245.12  TCP      66 65415 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2814 8.669834   128.119.245.12  192.168.0.102   TCP      66 80 → 65415 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM…
2815 8.669980   192.168.0.102   128.119.245.12  TCP      54 65415 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
2816 8.671107   192.168.0.102   128.119.245.12  HTTP    538 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
3405 8.971246   128.119.245.12  192.168.0.102   TCP      54 80 → 65415 [ACK] Seq=1 Ack=485 Win=30336 Len=0
3410 8.972909   128.119.245.12  192.168.0.102   TCP    1494 80 → 65415 [ACK] Seq=1 Ack=485 Win=30336 Len=1440 [TCP segment of a …
3411 8.972995   128.119.245.12  192.168.0.102   TCP    1494 80 → 65415 [ACK] Seq=1441 Ack=485 Win=30336 Len=1440 [TCP segment of…
3412 8.973037   192.168.0.102   128.119.245.12  TCP      54 65415 → 80 [ACK] Seq=485 Ack=2881 Win=132352 Len=0
3413 8.973145   128.119.245.12  192.168.0.102   TCP    1494 80 → 65415 [ACK] Seq=2881 Ack=485 Win=30336 Len=1440 [TCP segment of…
3476 9.025344   192.168.0.102   128.119.245.12  TCP      54 65415 → 80 [ACK] Seq=485 Ack=4321 Win=132352 Len=0
3767 9.963246   128.119.245.12  192.168.0.102   HTTP    595 HTTP/1.1 200 OK  (text/html)
3768 10.011157  192.168.0.102   128.119.245.12  TCP      54 65415 → 80 [ACK] Seq=485 Ack=4862 Win=131840 Len=0

> Frame 3767: 595 bytes on wire (4760 bits), 595 bytes captured (4760 bits) on interface \Device\NPF_{CA2FB4DB-E53B-45DB-92C6-
> Ethernet II, Src: TendaTec_1e:d2:20 (58:d9:d5:1e:d2:20), Dst: 76:01:3d:40:09:a8 (76:01:3d:40:09:a8)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.102
> Transmission Control Protocol, Src Port: 80, Dst Port: 65415, Seq: 4321, Ack: 485, Len: 541
> [4 Reassembled TCP Segments (4861 bytes): #3410(1440), #3411(1440), #3413(1440), #3767(541)]
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Thu, 22 Apr 2021 16:53:17 GMT\r\n

0000  76 01 3d 40 09 a8 58 d9  d5 1e d2 20 08 00 45 00   v·=@··X·  ··· ··E·
0010  02 45 1a 2c 40 00 27 06  00 f5 80 77 f5 0c c0 a8   ·E·,@·'·  ···w····
0020  00 66 00 50 ff 87 fc 28  b1 9b 52 50 7e f0 50 18   ·f·P···(  ··RP~·P·

Frame (595 bytes)   Reassembled TCP (4861 bytes)
wireshark_Wi-Fi 2XLQJ20.pcapng    Packets: 3830 · Displayed: 12 (0.3%) · Dropped: 0 (0.0%)    Profile: Default
```

**Answer**: The packet number 3767 in the trace contains the status code and phrase associated with the response to the HTTP GET request.

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

**Answer**: From the previous picture we can see the status code and phrase was 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?**



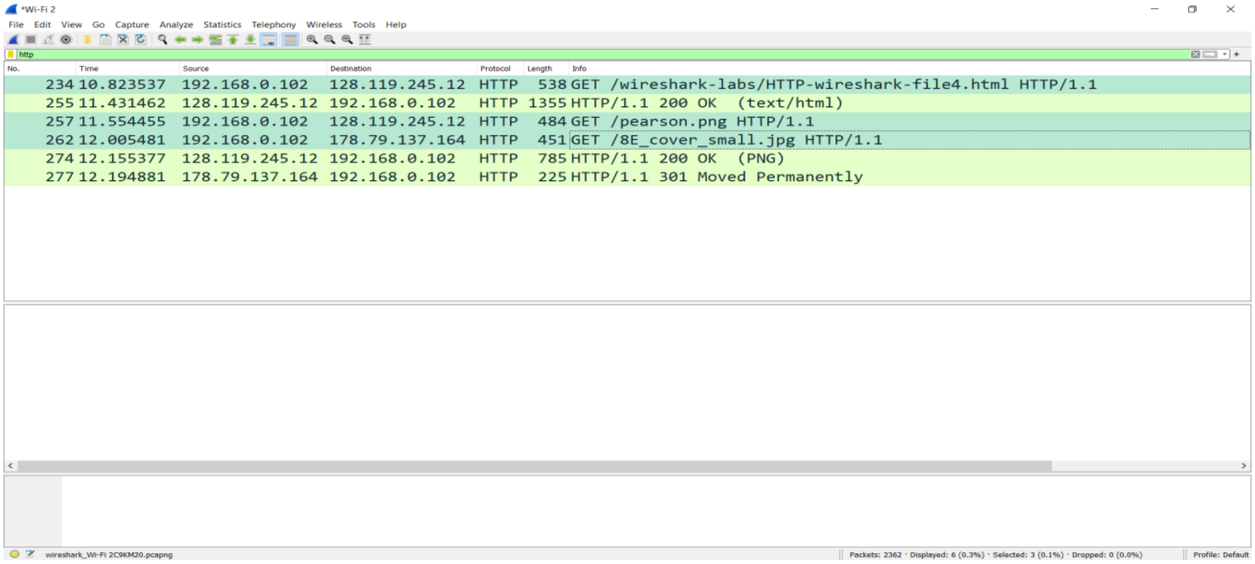
*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
(ip.addr eq 128.119.245.12 and ip.addr eq 192.168.0.102) and (tcp.port eq 80 and tcp.port eq 65415)

No.   Time      Source          Destination     Protocol Length Info
2360 8.370529   192.168.0.102   128.119.245.12  TCP       66 65415 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2814 8.669834   128.119.245.12  192.168.0.102   TCP       66 80 → 65415 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM…
2815 8.669980   192.168.0.102   128.119.245.12  TCP       54 65415 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
2816 8.671107   192.168.0.102   128.119.245.12  HTTP     538 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
3405 8.971246   128.119.245.12  192.168.0.102   TCP       54 80 → 65415 [ACK] Seq=1 Ack=485 Win=30336 Len=0
3410 8.972909   128.119.245.12  192.168.0.102   TCP     1494 80 → 65415 [ACK] Seq=1 Ack=485 Win=30336 Len=1440 [TCP segment of a …
3411 8.972995   128.119.245.12  192.168.0.102   TCP     1494 80 → 65415 [ACK] Seq=1441 Ack=485 Win=30336 Len=1440 [TCP segment of…
3412 8.973037   192.168.0.102   128.119.245.12  TCP       54 65415 → 80 [ACK] Seq=485 Ack=2881 Win=132352 Len=0
3413 8.973145   128.119.245.12  192.168.0.102   TCP     1494 80 → 65415 [ACK] Seq=2881 Ack=485 Win=30336 Len=1440 [TCP segment of…
3476 9.025344   192.168.0.102   128.119.245.12  TCP       54 65415 → 80 [ACK] Seq=485 Ack=4321 Win=132352 Len=0
3767 9.963246   128.119.245.12  192.168.0.102   HTTP     595 HTTP/1.1 200 OK  (text/html)
3768 10.011157  192.168.0.102   128.119.245.12  TCP       54 65415 → 80 [ACK] Seq=485 Ack=4862 Win=131840 Len=0

> Frame 3767: 595 bytes on wire (4760 bits), 595 bytes captured (4760 bits) on interface \Device\NPF_{CA2FB4DB-E53B-45DB-92C6-34
> Ethernet II, Src: TendaTec_1e:d2:20 (58:d9:d5:1e:d2:20), Dst: 76:01:3d:40:09:a8 (76:01:3d:40:09:a8)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.102
> Transmission Control Protocol, Src Port: 80, Dst Port: 65415, Seq: 4321, Ack: 485, Len: 541
> [4 Reassembled TCP Segments (4861 bytes): #3410(1440), #3411(1440), #3413(1440), #3767(541)]
> Hypertext Transfer Protocol
> Line-based text data: text/html (98 lines)

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 54  68 75 2c 20 32 32 20 41   ·Date: T hu, 22 A
0020  70 72 20 32 30 32 31 20  31 36 3a 35 33 3a 31 37   pr 2021  16:53:17

Frame (595 bytes)   Reassembled TCP (4861 bytes)
TCP Segments (tcp.segments), 4,861 bytes        Packets: 3830 · Displayed: 12 (0.3%) · Dropped: 0 (0.0%)        Profile: Default
```

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

## HTML Documents with Embedded Objects

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

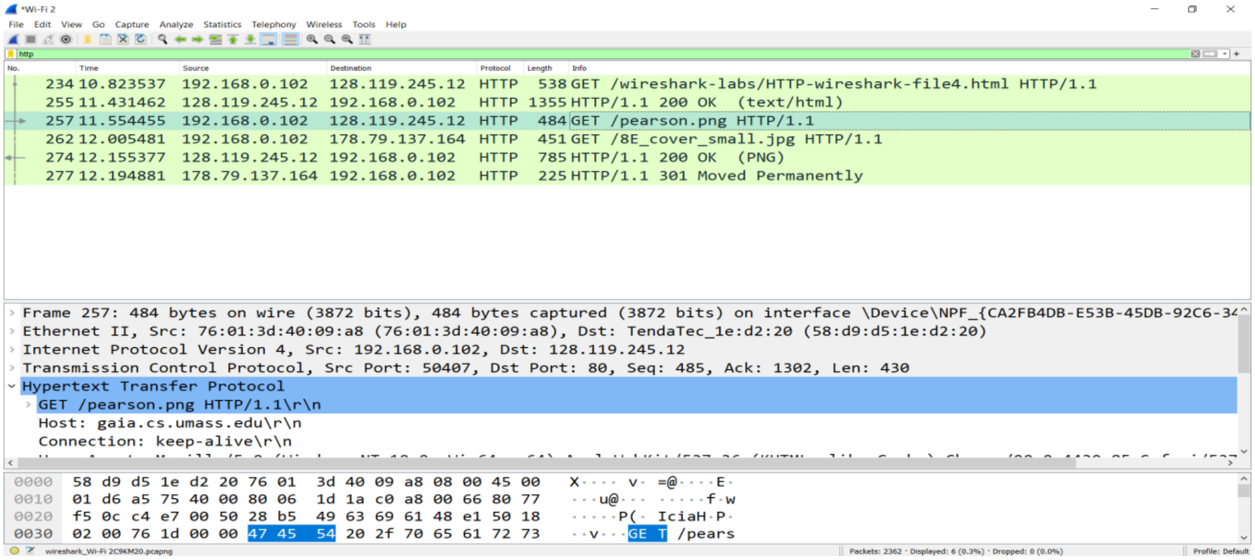


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http

No.   Time       Source          Destination     Protocol Length Info
234  10.823537   192.168.0.102   128.119.245.12  HTTP     538 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
255  11.431462   128.119.245.12  192.168.0.102   HTTP    1355 HTTP/1.1 200 OK  (text/html)
257  11.554455   192.168.0.102   128.119.245.12  HTTP     484 GET /pearson.png HTTP/1.1
262  12.005481   192.168.0.102   178.79.137.164  HTTP     451 GET /8E_cover_small.jpg HTTP/1.1
274  12.155377   128.119.245.12  192.168.0.102   HTTP     785 HTTP/1.1 200 OK  (PNG)
277  12.194881   178.79.137.164  192.168.0.102   HTTP     225 HTTP/1.1 301 Moved Permanently

wireshark_Wi-Fi 2C9KM20.pcapng        Packets: 2362 · Displayed: 6 (0.3%) · Selected: 3 (0.1%) · Dropped: 0 (0.0%)        Profile: Default
```

**Answer**: My browser sent 3 HTTP GET request messages. 2 of them were sent to address 128.119.245.12 and 1 of them were sent to address 178.79.137.164

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.**


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
wireshark_Wi-Fi 2C9KM20.pcapng
Packets: 2362 · Displayed: 6 (0.3%) · Dropped: 0 (0.0%)
Profile: Default

```
No.  Time       Source          Destination     Protocol Length Info
 234 10.823537  192.168.0.102   128.119.245.12  HTTP      538 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
 255 11.431462  128.119.245.12  192.168.0.102   HTTP     1355 HTTP/1.1 200 OK  (text/html)
 257 11.554455  192.168.0.102   128.119.245.12  HTTP      484 GET /pearson.png HTTP/1.1
 262 12.005481  192.168.0.102   178.79.137.164  HTTP      451 GET /8E_cover_small.jpg HTTP/1.1
 274 12.155377  128.119.245.12  192.168.0.102   HTTP      785 HTTP/1.1 200 OK  (PNG)
 277 12.194881  178.79.137.164  192.168.0.102   HTTP      225 HTTP/1.1 301 Moved Permanently
```

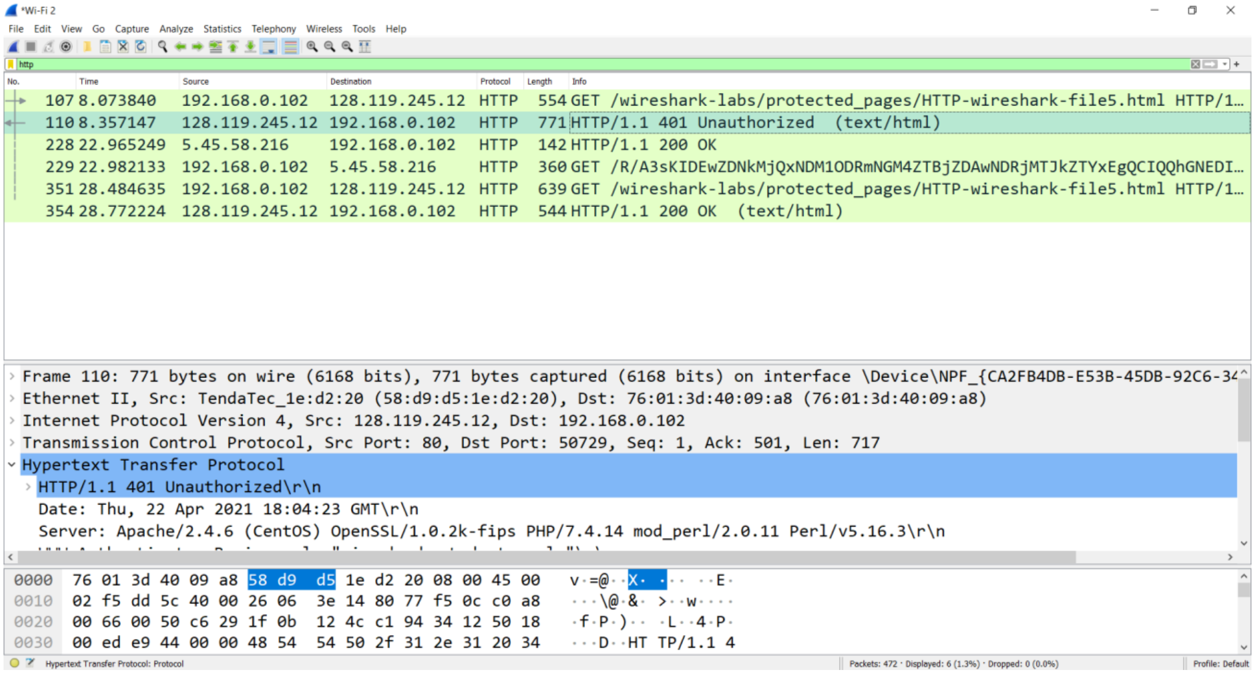
```
> Frame 257: 484 bytes on wire (3872 bits), 484 bytes captured (3872 bits) on interface \Device\NPF_{CA2FB4DB-E53B-45DB-92C6-34
> Ethernet II, Src: 76:01:3d:40:09:a8 (76:01:3d:40:09:a8), Dst: TendaTec_1e:d2:20 (58:d9:d5:1e:d2:20)
> Internet Protocol Version 4, Src: 192.168.0.102, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 50407, Dst Port: 80, Seq: 485, Ack: 1302, Len: 430
v Hypertext Transfer Protocol
  > GET /pearson.png HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
```

```
0000  58 d9 d5 1e d2 20 76 01  3d 40 09 a8 08 00 45 00   X····v· =@····E·
0010  01 d6 a5 75 40 00 80 06  1d 1a c0 a8 00 66 80 77   ···u@··· ·····f·w
0020  f5 0c c4 e7 00 50 28 b5  49 63 69 61 48 e1 50 18   ·····P(· IciaH·P·
0030  02 00 76 1d 00 00 47 45  54 20 2f 70 65 61 72 73   ··v···GE T /pears
```

**Answer**: My browser downloaded two images from the two web sites in parallel. The request for the second image file (Packet number 262) was made before the first image file was received (Packet number 274).

## HTTP Authentication

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


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Hypertext Transfer Protocol: Protocol
Packets: 472 · Displayed: 6 (1.3%) · Dropped: 0 (0.0%)
Profile: Default

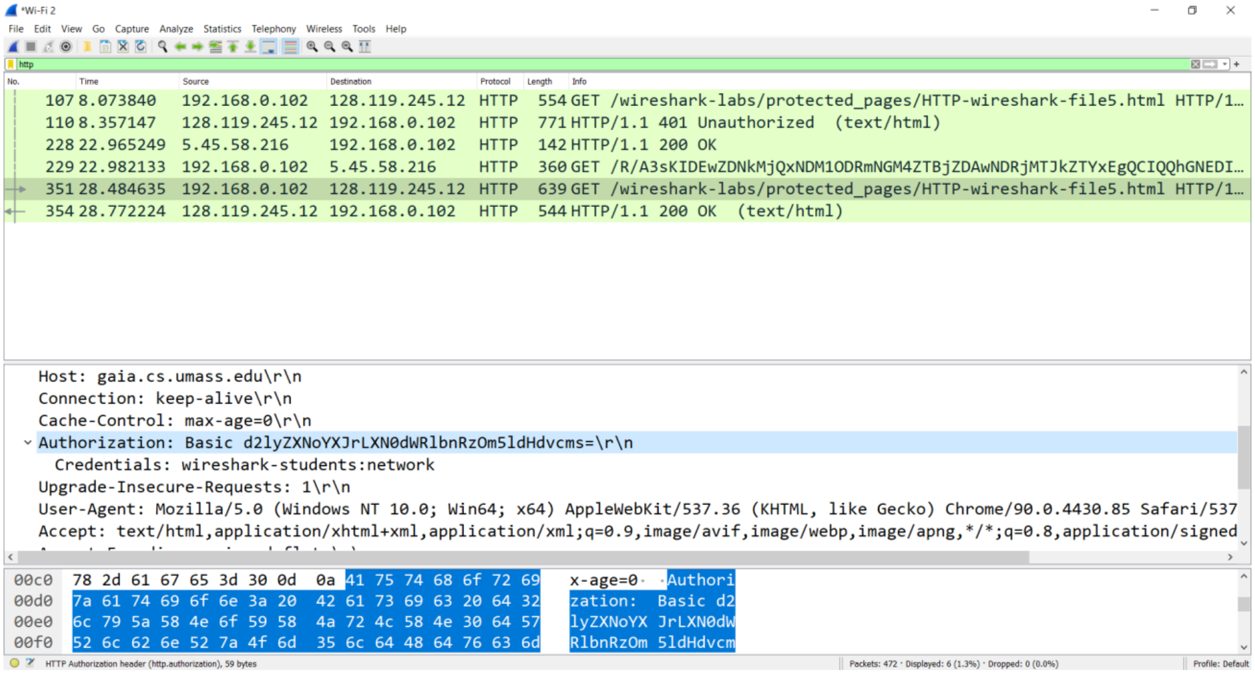
```
No.  Time       Source          Destination     Protocol Length Info
 107 8.073840   192.168.0.102   128.119.245.12  HTTP      554 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1…
 110 8.357147   128.119.245.12  192.168.0.102   HTTP      771 HTTP/1.1 401 Unauthorized  (text/html)
 228 22.965249  5.45.58.216     192.168.0.102   HTTP      142 HTTP/1.1 200 OK
 229 22.982133  192.168.0.102   5.45.58.216     HTTP      360 GET /R/A3sKIDEwZDNkMjQxNDM1ODRmNGM4ZTBjZDAwNDRjMTJkZTYxEgQCIQQhGNEDI…
 351 28.484635  192.168.0.102   128.119.245.12  HTTP      639 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1…
 354 28.772224  128.119.245.12  192.168.0.102   HTTP      544 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 110: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Device\NPF_{CA2FB4DB-E53B-45DB-92C6-34
> Ethernet II, Src: TendaTec_1e:d2:20 (58:d9:d5:1e:d2:20), Dst: 76:01:3d:40:09:a8 (76:01:3d:40:09:a8)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.102
> Transmission Control Protocol, Src Port: 80, Dst Port: 50729, Seq: 1, Ack: 501, Len: 717
v Hypertext Transfer Protocol
  > HTTP/1.1 401 Unauthorized\r\n
    Date: Thu, 22 Apr 2021 18:04:23 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
```

```
0000  76 01 3d 40 09 a8 58 d9  d5 1e d2 20 08 00 45 00   v·=@··X· ·· ··E·
0010  02 f5 dd 5c 40 00 26 06  3e 14 80 77 f5 0c c0 a8   ···\@·&· >··w····
0020  00 66 00 50 c6 29 1f 0b  12 4c c1 94 34 12 50 18   ·f·P·)·· ·L··4·P·
0030  00 ed e9 44 00 00 48 54  54 50 2f 31 2e 31 20 34   ···D··HT TP/1.1 4
```

**Answer**: The server's response in response to the initial HTTP GET message from my browser was 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?**



*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.  Time          Source          Destination     Protocol Length Info
 107 8.073840     192.168.0.102   128.119.245.12  HTTP     554 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1…
 110 8.357147     128.119.245.12  192.168.0.102   HTTP     771 HTTP/1.1 401 Unauthorized  (text/html)
 228 22.965249    5.45.58.216     192.168.0.102   HTTP     142 HTTP/1.1 200 OK
 229 22.982133    192.168.0.102   5.45.58.216     HTTP     360 GET /R/A3sKIDEwZDNkMjQxNDM1ODRmNGM4ZTBjZDAwNDRjMTJkZTYxEgQCIQQhGNEDI…
 351 28.484635    192.168.0.102   128.119.245.12  HTTP     639 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1…
 354 28.772224    128.119.245.12  192.168.0.102   HTTP     544 HTTP/1.1 200 OK  (text/html)
```

```
    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/90.0.4430.85 Safari/537
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed
```

```
00c0  78 2d 61 67 65 3d 30 0d  0a 41 75 74 68 6f 72 69   x-age=0· ·Authori
00d0  7a 61 74 69 6f 6e 3a 20  42 61 73 69 63 20 64 32   zation:  Basic d2
00e0  6c 79 5a 58 4e 6f 59 58  4a 72 4c 58 4e 30 64 57   lyZXNoYX JrLXN0dW
00f0  52 6c 62 6e 52 7a 4f 6d  35 6c 64 48 64 76 63 6d   RlbnRzOm 5ldHdvcm
```

HTTP Authorization header (http.authorization), 59 bytes | Packets: 472 · Displayed: 6 (1.3%) · Dropped: 0 (0.0%) | Profile: Default

**Answer**: The new field is included in the HTTP GET message is Authorization field.