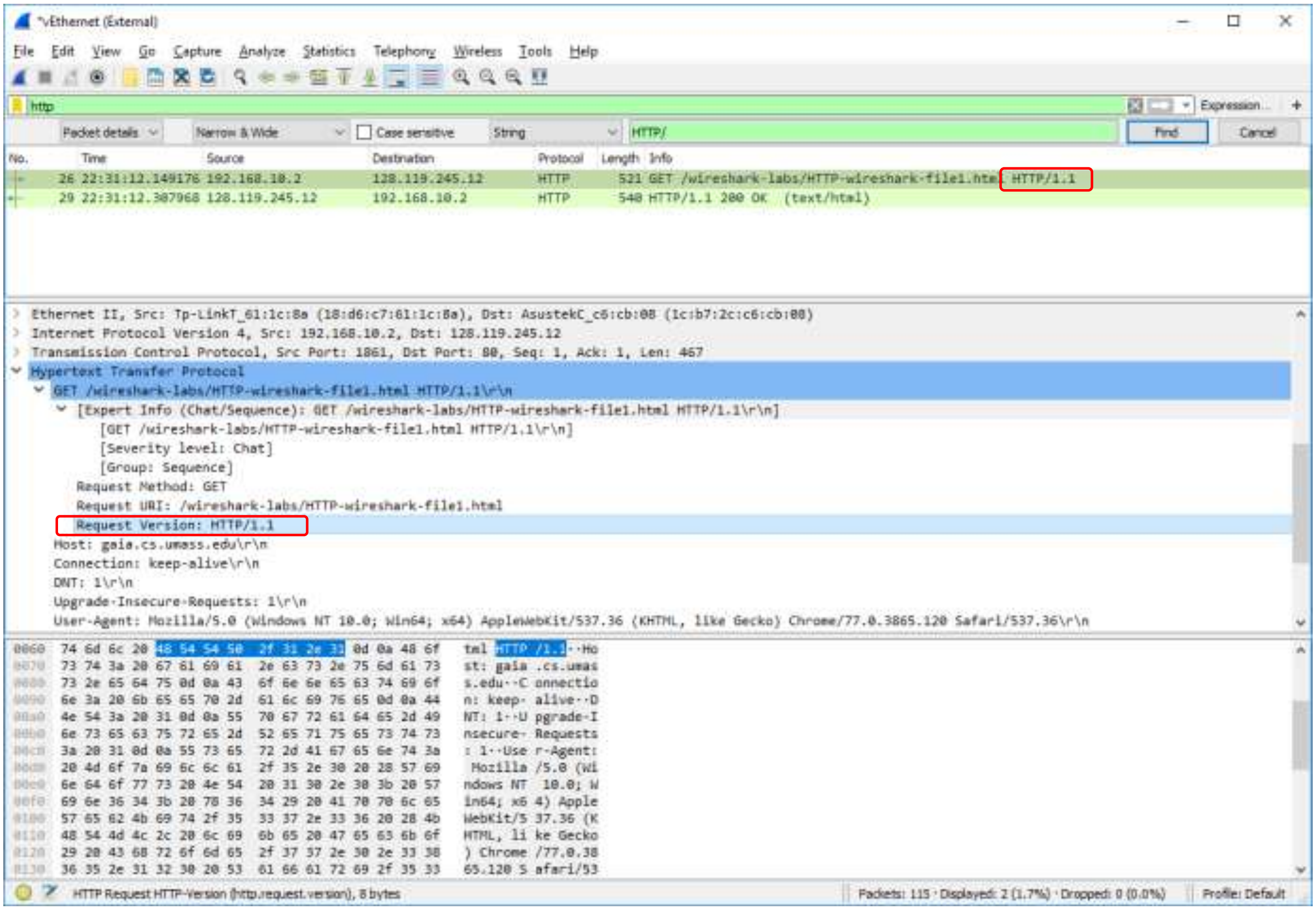
CS372-400
10/13/2019

Edmund Dea
ID# 933280343

Lab 2: Wireshark

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.



http

□ Case sensitive

HTTP/

```
No.   Time                Source           Destination      Protocol  Length  Info
   26 22:31:12.149176     192.168.10.2     128.119.245.12   HTTP         521  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
   29 22:31:12.387968     128.119.245.12   192.168.10.2     HTTP         540  HTTP/1.1 200 OK  (text/html)
```

```
> Ethernet II, Src: Tp-LinkT_61:1c:8a (18:d6:c7:61:1c:8a), Dst: AsustekC_c6:cb:08 (1c:b7:2c:c6:cb:08)
> Internet Protocol Version 4, Src: 192.168.10.2, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 1861, Dst Port: 80, Seq: 1, Ack: 1, Len: 467
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    v [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
        [GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    DNT: 1\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
```

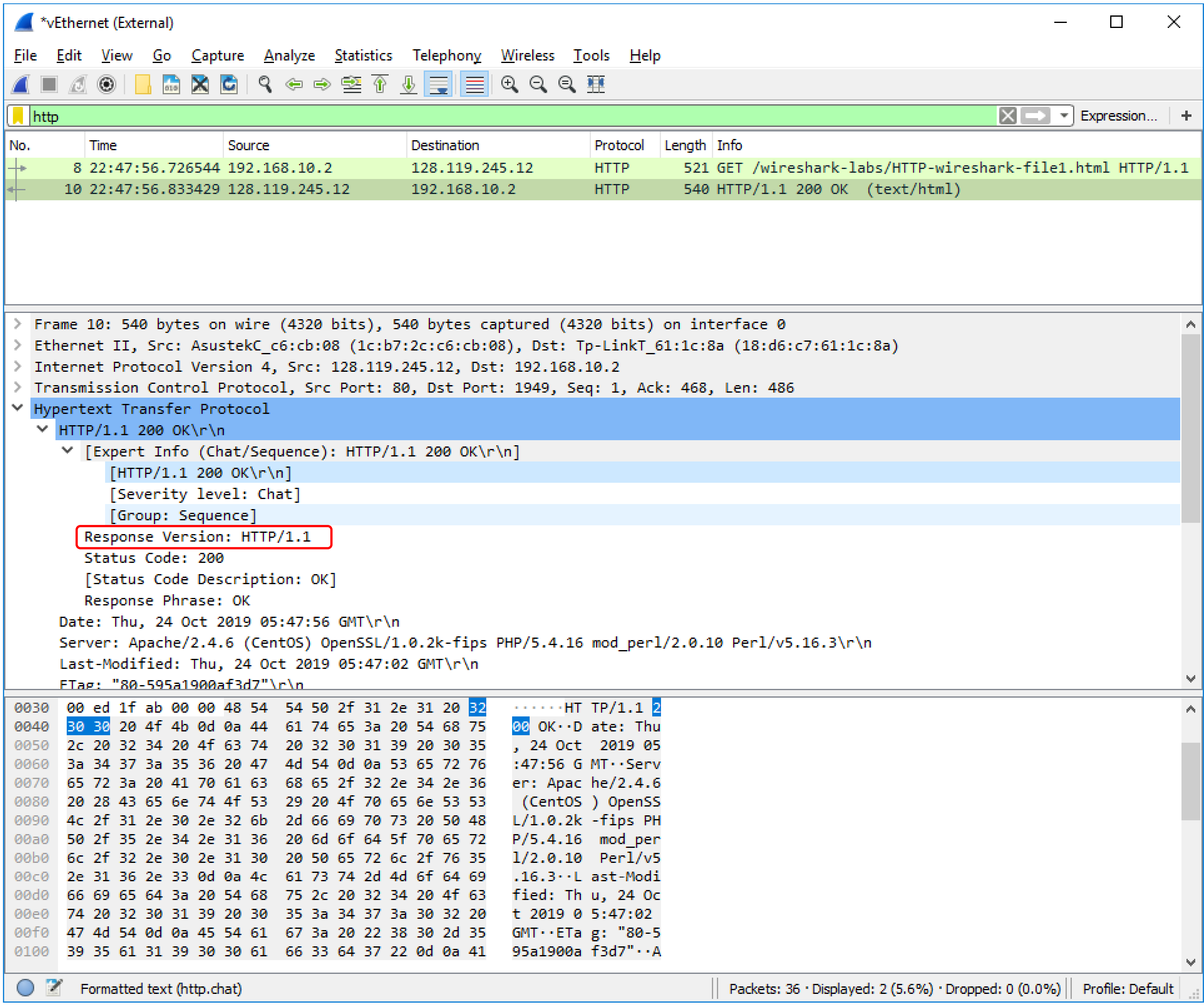
```
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 44   n: keep- alive··D
00a0  4e 54 3a 20 31 0d 0a 55  70 67 72 61 64 65 2d 49   NT: 1··U pgrade-I
00b0  6e 73 65 63 75 72 65 2d  52 65 71 75 65 73 74 73   nsecure- Requests
00c0  3a 20 31 0d 0a 55 73 65  72 2d 41 67 65 6e 74 3a   : 1··Use r-Agent:
00d0  20 4d 6f 7a 69 6c 6c 61  2f 35 2e 30 20 28 57 69    Mozilla /5.0 (Wi
00e0  6e 64 6f 77 73 20 4e 54  20 31 30 2e 30 3b 20 57   ndows NT  10.0; W
00f0  69 6e 36 34 3b 20 78 36  34 29 20 41 70 70 6c 65   in64; x6 4) Apple
0100  57 65 62 4b 69 74 2f 35  33 37 2e 33 36 20 28 4b   WebKit/5 37.36 (K
0110  48 54 4d 4c 2c 20 6c 69  6b 65 20 47 65 63 6b 6f   HTML, li ke Gecko
0120  29 20 43 68 72 6f 6d 65  2f 37 37 2e 30 2e 33 38   ) Chrome /77.0.38
0130  36 35 2e 31 32 30 20 53  61 66 61 72 69 2f 35 33   65.120 S afari/53
```

HTTP Request HTTP-Version (http.request.version), 8 bytes

Packets: 115 · Displayed: 2 (1.7%) · Dropped: 0 (0.0%)

Profile: Default

   The server is also running HTTP 1.1.


*vEthernet (External)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

http

```
No.  Time            Source          Destination     Protocol Length Info
   8 22:47:56.726544 192.168.10.2    128.119.245.12  HTTP        521 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  10 22:47:56.833429 128.119.245.12  192.168.10.2    HTTP        540 HTTP/1.1 200 OK  (text/html)
```

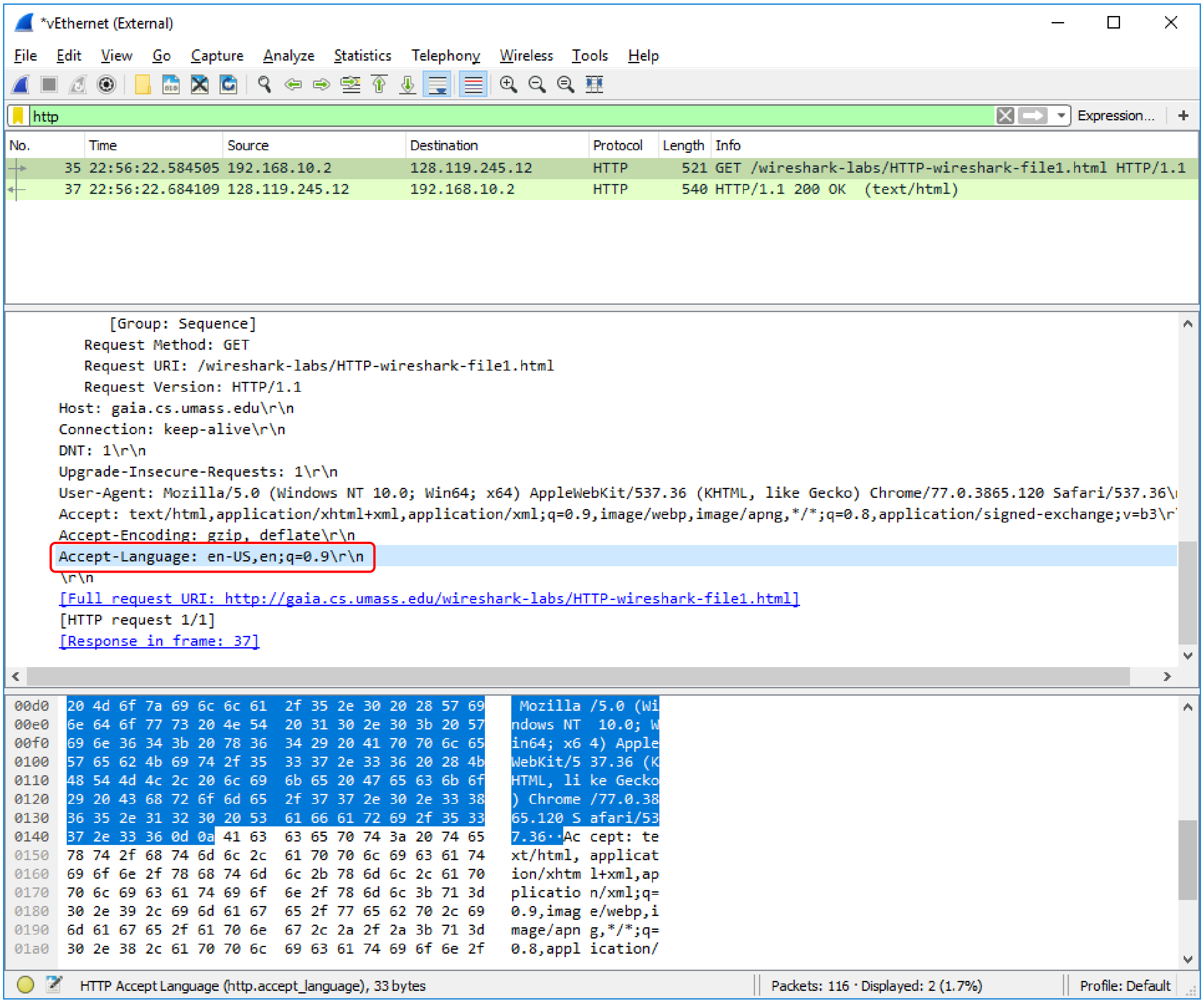
```
> Frame 10: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
> Ethernet II, Src: AsustekC_c6:cb:08 (1c:b7:2c:c6:cb:08), Dst: Tp-LinkT_61:1c:8a (18:d6:c7:61:1c:8a)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.10.2
> Transmission Control Protocol, Src Port: 80, Dst Port: 1949, Seq: 1, Ack: 468, Len: 486
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: Thu, 24 Oct 2019 05:47:56 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: Thu, 24 Oct 2019 05:47:02 GMT\r\n
    ETag: "80-595a1900af3d7"\r\n
```

```
0030  00 ed 1f ab 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 34 20 4f 63 74  20 32 30 31 39 20 30 35   , 24 Oct  2019 05
0060  3a 34 37 3a 35 36 20 47  4d 54 0d 0a 53 65 72 76   :47:56 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 68  75 2c 20 32 34 20 4f 63   fied: Th u, 24 Oc
00e0  74 20 32 30 31 39 20 30  35 3a 34 37 3a 30 32 20   t 2019 0 5:47:02
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 38 30 2d 35   GMT··ETa g: "80-5
0100  39 35 61 31 39 30 30 61  66 33 64 37 22 0d 0a 41   95a1900a f3d7"··A
```

Formatted text (http.chat) | Packets: 36 · Displayed: 2 (5.6%) · Dropped: 0 (0.0%) | Profile: Default

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

My browser indicates that it can accept “en-US, en; q=0.9\r\n”, which means that my browser can accept English US or English language with a q-factor weighting of 0.9.


*vEthernet (External)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

http

```
No.  Time             Source          Destination     Protocol Length Info
  35 22:56:22.584505 192.168.10.2    128.119.245.12  HTTP        521 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  37 22:56:22.684109 128.119.245.12  192.168.10.2    HTTP        540 HTTP/1.1 200 OK  (text/html)
```

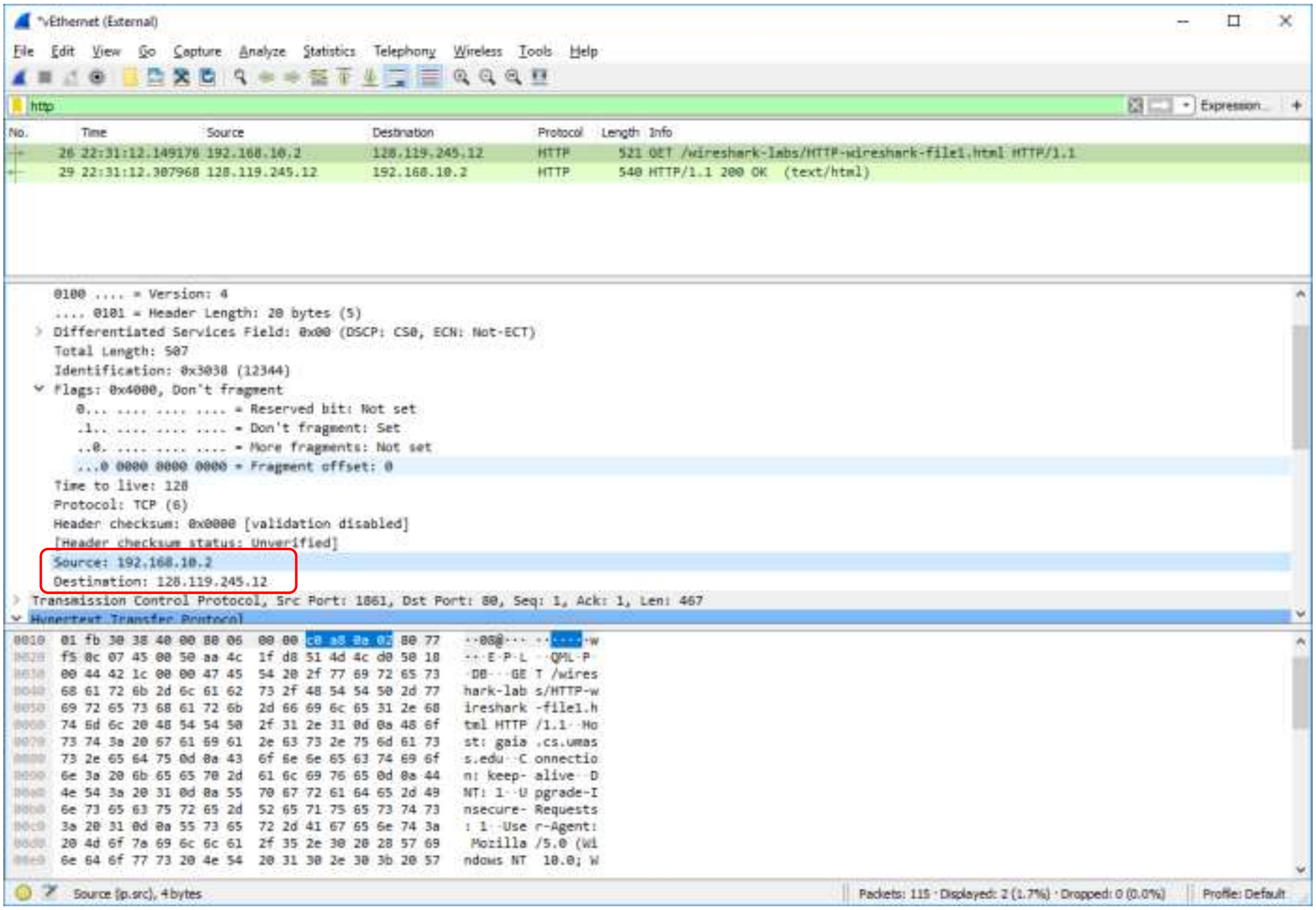
```
            [Group: Sequence]
         Request Method: GET
         Request URI: /wireshark-labs/HTTP-wireshark-file1.html
         Request Version: HTTP/1.1
      Host: gaia.cs.umass.edu\r\n
      Connection: keep-alive\r\n
      DNT: 1\r\n
      Upgrade-Insecure-Requests: 1\r\n
      User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.120 Safari/537.36\
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r
      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 1/1]
      [Response in frame: 37]
```

```
00d0  20 4d 6f 7a 69 6c 6c 61  2f 35 2e 30 20 28 57 69    Mozilla /5.0 (Wi
00e0  6e 64 6f 77 73 20 4e 54  20 31 30 2e 30 3b 20 57   ndows NT  10.0; W
00f0  69 6e 36 34 3b 20 78 36  34 29 20 41 70 70 6c 65   in64; x6 4) Apple
0100  57 65 62 4b 69 74 2f 35  33 37 2e 33 36 20 28 4b   WebKit/5 37.36 (K
0110  48 54 4d 4c 2c 20 6c 69  6b 65 20 47 65 63 6b 6f   HTML, li ke Gecko
0120  29 20 43 68 72 6f 6d 65  2f 37 37 2e 30 2e 33 38   ) Chrome /77.0.38
0130  36 35 2e 31 32 30 20 53  61 66 61 72 69 2f 35 33   65.120 S afari/53
0140  37 2e 33 36 0d 0a 41 63  63 65 70 74 3a 20 74 65   7.36··Ac cept: te
0150  78 74 2f 68 74 6d 6c 2c  61 70 70 6c 69 63 61 74   xt/html, applicat
0160  69 6f 6e 2f 78 68 74 6d  6c 2b 78 6d 6c 2c 61 70   ion/xhtm l+xml,ap
0170  70 6c 69 63 61 74 69 6f  6e 2f 78 6d 6c 3b 71 3d   plicatio n/xml;q=
0180  30 2e 39 2c 69 6d 61 67  65 2f 77 65 62 70 2c 69   0.9,imag e/webp,i
0190  6d 61 67 65 2f 61 70 6e  67 2c 2a 2f 2a 3b 71 3d   mage/apn g,*/*;q=
01a0  30 2e 38 2c 61 70 70 6c  69 63 61 74 69 6f 6e 2f   0.8,appl ication/
```

HTTP Accept Language (http.accept_language), 33 bytes | Packets: 116 · Displayed: 2 (1.7%) | Profile: Default

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

The IP address of my computer is 192.168.10.2, which is the source address. The IP address of gaia.cs.umass.edu is 128.119.245.12, which is the destination address.


*vEthernet (External)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

```
http
```

```
No.    Time                Source           Destination      Protocol  Length  Info
    26 22:31:12.149176 192.168.10.2     128.119.245.12   HTTP       521 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
    29 22:31:12.307968 128.119.245.12   192.168.10.2     HTTP       540 HTTP/1.1 200 OK  (text/html)
```

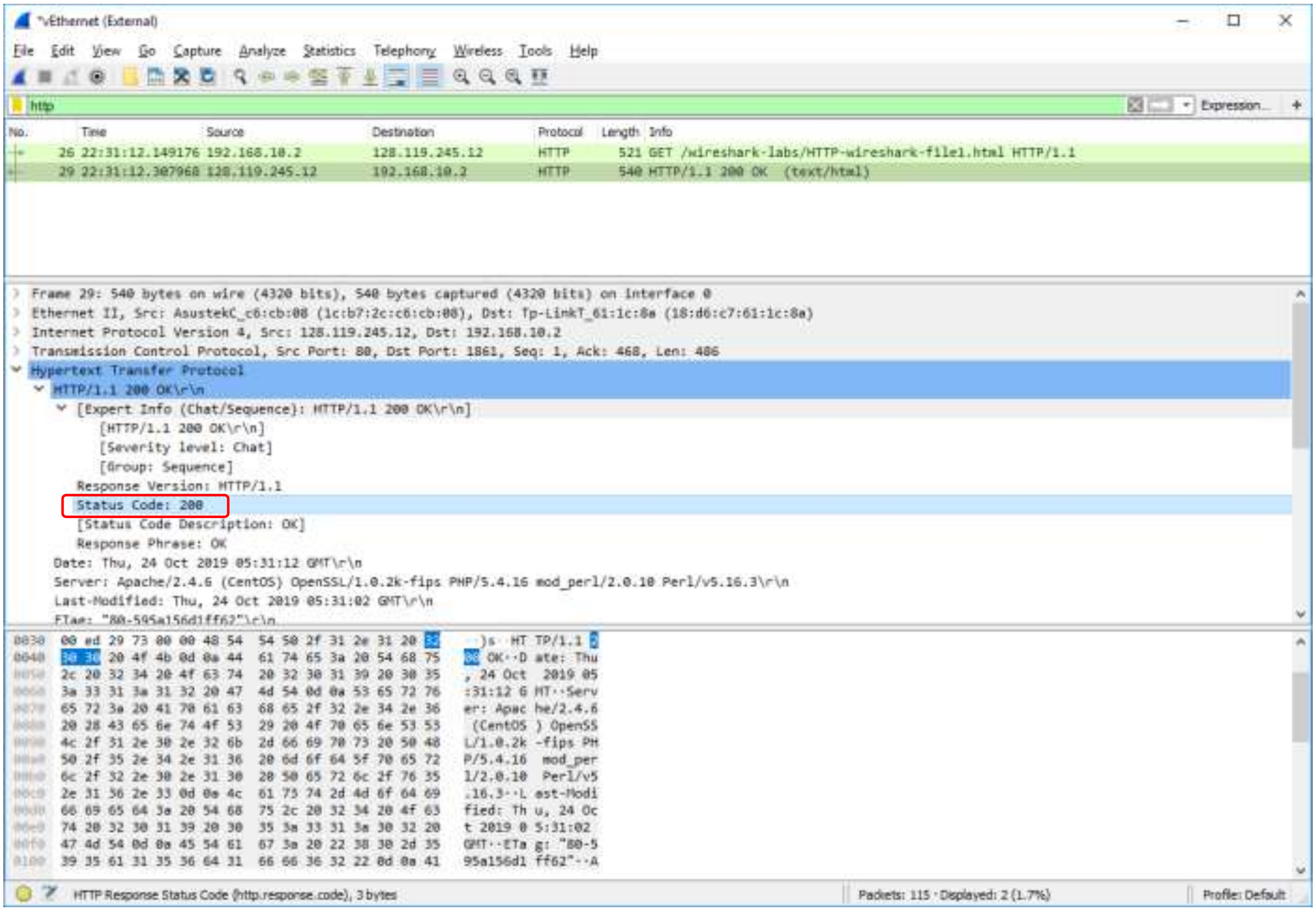
```
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 507
    Identification: 0x3038 (12344)
  v Flags: 0x4000, Don't fragment
      0... .... .... .... = Reserved bit: Not set
      .1.. .... .... .... = Don't fragment: Set
      ..0. .... .... .... = More fragments: Not set
      ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.10.2
    Destination: 128.119.245.12
> Transmission Control Protocol, Src Port: 1061, Dst Port: 80, Seq: 1, Ack: 1, Len: 467
v Hypertext Transfer Protocol
```

```
0010  01 fb 30 38 40 00 80 06  00 00 c0 a8 0a 02 80 77   ··08@··· ······w
0020  f5 8c 07 45 00 50 aa 4c  1f d8 51 4d 4c d0 50 18   ···E·P·L ··QML·P·
0030  00 44 42 1c 00 00 47 45  54 20 2f 77 69 72 65 73   ·DB···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
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
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 44   n: keep- alive··D
00a0  4e 54 3a 20 31 0d 0a 55  70 67 72 61 64 65 2d 49   NT: 1··U pgrade-I
00b0  6e 73 65 63 75 72 65 2d  52 65 71 75 65 73 74 73   nsecure- Requests
00c0  3a 20 31 0d 0a 55 73 65  72 2d 41 67 65 6e 74 3a   : 1··Use r-Agent:
00d0  20 4d 6f 7a 69 6c 6c 61  2f 35 2e 30 20 28 57 69    Mozilla /5.0 (Wi
00e0  6e 64 6f 77 73 20 4e 54  20 31 30 2e 30 3b 20 57   ndows NT  10.0; W
```

```
Source (ip.src), 4 bytes          Packets: 115 · Displayed: 2 (1.7%) · Dropped: 0 (0.0%)          Profile: Default
```

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

Status code 200 OK was returned from the server to my browser.


*vEthernet (External)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
+

```
No.     Time               Source           Destination      Protocol  Length  Info
     26 22:31:12.149176 192.168.10.2     128.119.245.12     HTTP        521 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
     29 22:31:12.307968 128.119.245.12   192.168.10.2       HTTP        540 HTTP/1.1 200 OK  (text/html)
```

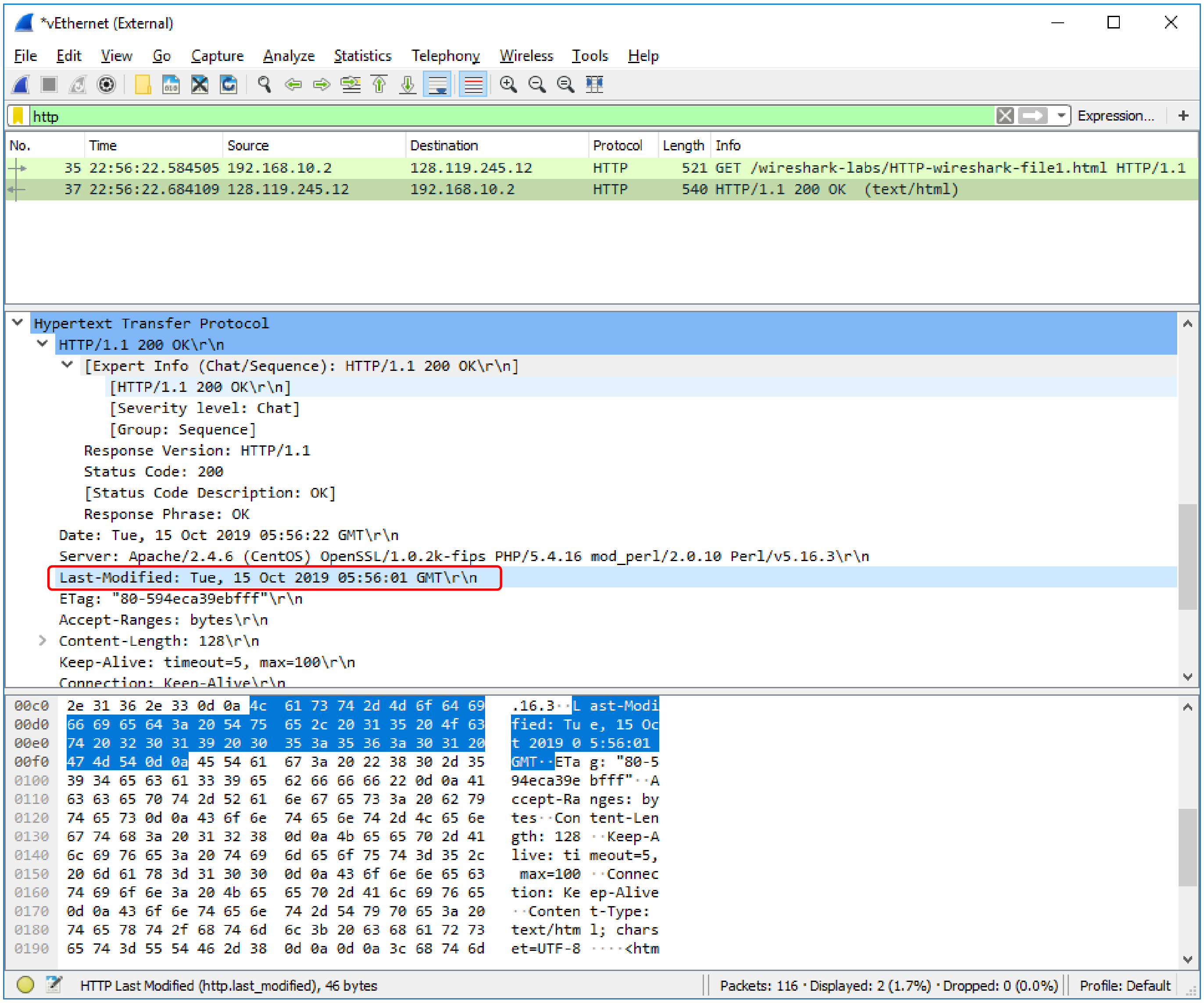
```
> Frame 29: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
> Ethernet II, Src: AsustekC_c6:cb:08 (1c:b7:2c:c6:cb:08), Dst: Tp-LinkT_61:1c:8a (18:d6:c7:61:1c:8a)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.10.2
> Transmission Control Protocol, Src Port: 80, Dst Port: 1861, Seq: 1, Ack: 468, Len: 486
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: Thu, 24 Oct 2019 05:31:12 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: Thu, 24 Oct 2019 05:31:02 GMT\r\n
    ETag: "80-595a156d1ff62"\r\n
```

```
0030  00 ed 29 73 00 00 48 54  54 50 2f 31 2e 31 20 32   ··)s··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 34 20 4f 63 74  20 32 30 31 39 20 30 35   , 24 Oct  2019 05
0060  3a 33 31 3a 31 32 20 47  4d 54 0d 0a 53 65 72 76   :31:12 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 68  75 2c 20 32 34 20 4f 63   fied: Th u, 24 Oc
00e0  74 20 32 30 31 39 20 30  35 3a 33 31 3a 30 32 20   t 2019 0 5:31:02
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 38 30 2d 35   GMT··ETa g: "80-5
0100  39 35 61 31 35 36 64 31  66 66 36 32 22 0d 0a 41   95a156d1 ff62"··A
```

HTTP Response Status Code (http.response.code), 3 bytes

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

The HTML file that I am retrieving was last modified at the server on “Tue, 15 Oct 2019 05:56:01 GMT”.



*vEthernet (External)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

```
http
```

```
No.   Time             Source          Destination     Protocol  Length Info
  35 22:56:22.584505 192.168.10.2    128.119.245.12  HTTP        521 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  37 22:56:22.684109 128.119.245.12  192.168.10.2    HTTP        540 HTTP/1.1 200 OK  (text/html)
```

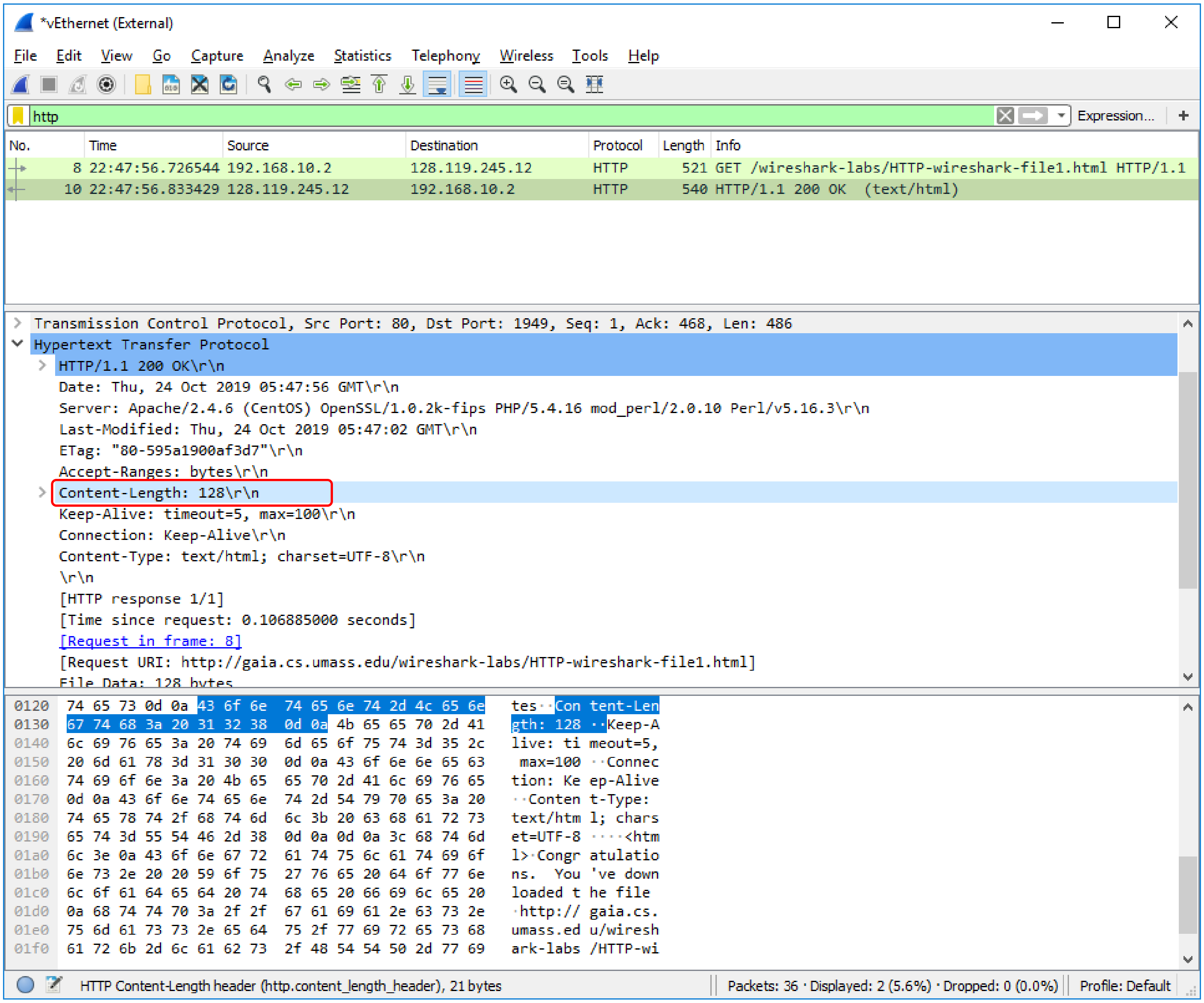
```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        [HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
  Date: Tue, 15 Oct 2019 05:56:22 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, 15 Oct 2019 05:56:01 GMT\r\n
  ETag: "80-594eca39ebfff"\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
```

```
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 31 35 20 4f 63   fied: Tu e, 15 Oc
00e0  74 20 32 30 31 39 20 30  35 3a 35 36 3a 30 31 20   t 2019 0 5:56:01 
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 38 30 2d 35   GMT··ETa g: "80-5
0100  39 34 65 63 61 33 39 65  62 66 66 66 22 0d 0a 41   94eca39e bfff"··A
0110  63 63 65 70 74 2d 52 61  6e 67 65 73 3a 20 62 79   ccept-Ra nges: by
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
0160  74 69 6f 6e 3a 20 4b 65  65 70 2d 41 6c 69 76 65   tion: Ke ep-Alive
0170  0d 0a 43 6f 6e 74 65 6e  74 2d 54 79 70 65 3a 20   ··Conten t-Type: 
0180  74 65 78 74 2f 68 74 6d  6c 3b 20 63 68 61 72 73   text/htm l; chars
0190  65 74 3d 55 54 46 2d 38  0d 0a 0d 0a 3c 68 74 6d   et=UTF-8 ····<htm
```

HTTP Last Modified (http.last_modified), 46 bytes | Packets: 116 · Displayed: 2 (1.7%) · Dropped: 0 (0.0%) | Profile: Default

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

128 bytes of content were returned to my browser.



*vEthernet (External)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

http

```
No.   Time              Source          Destination     Protocol Length Info
    8 22:47:56.726544 192.168.10.2    128.119.245.12  HTTP        521 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
   10 22:47:56.833429 128.119.245.12  192.168.10.2    HTTP        540 HTTP/1.1 200 OK  (text/html)
```

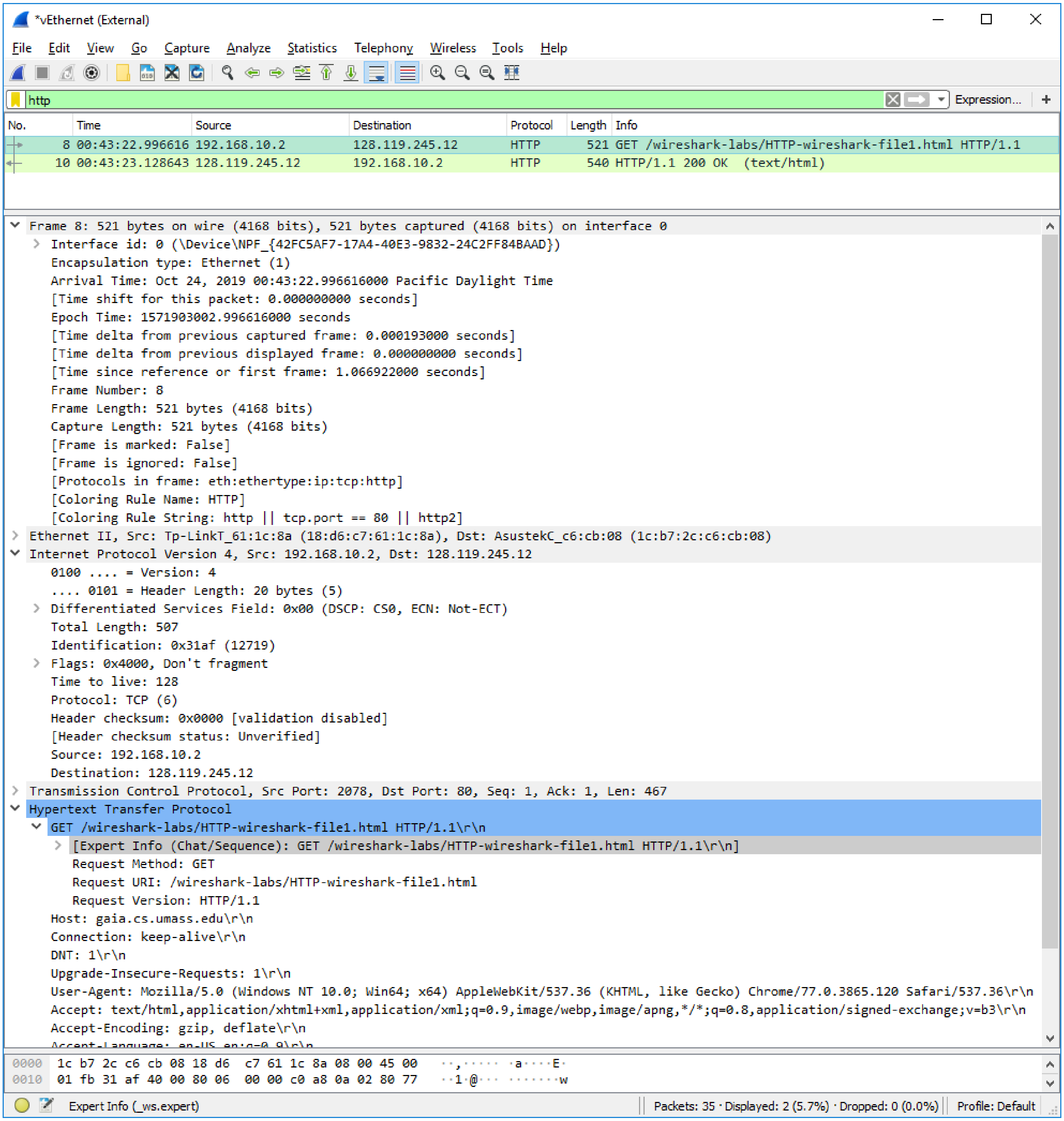
```
> Transmission Control Protocol, Src Port: 80, Dst Port: 1949, Seq: 1, Ack: 468, Len: 486
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Thu, 24 Oct 2019 05:47:56 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Thu, 24 Oct 2019 05:47:02 GMT\r\n
    ETag: "80-595a1900af3d7"\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: 0.106885000 seconds]
    [Request in frame: 8]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    File Data: 128 bytes
```

```
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
0160  74 69 6f 6e 3a 20 4b 65  65 70 2d 41 6c 69 76 65   tion: Ke ep-Alive
0170  0d 0a 43 6f 6e 74 65 6e  74 2d 54 79 70 65 3a 20   ··Conten t-Type: 
0180  74 65 78 74 2f 68 74 6d  6c 3b 20 63 68 61 72 73   text/htm l; chars
0190  65 74 3d 55 54 46 2d 38  0d 0a 0d 0a 3c 68 74 6d   et=UTF-8 ····<htm
01a0  6c 3e 0a 43 6f 6e 67 72  61 74 75 6c 61 74 69 6f   l>·Congr atulatio
01b0  6e 73 2e 20 20 59 6f 75  27 76 65 20 64 6f 77 6e   ns.  You 've down
01c0  6c 6f 61 64 65 64 20 74  68 65 20 66 69 6c 65 20   loaded t he file 
01d0  0a 68 74 74 70 3a 2f 2f  67 61 69 61 2e 63 73 2e   ·http:// gaia.cs.
01e0  75 6d 61 73 73 2e 65 64  75 2f 77 69 72 65 73 68   umass.ed u/wiresh
01f0  61 72 6b 2d 6c 61 62 73  2f 48 54 54 50 2d 77 69   ark-labs /HTTP-wi
```

HTTP Content-Length header (http.content_length_header), 21 bytes | Packets: 36 · Displayed: 2 (5.6%) · Dropped: 0 (0.0%) | Profile: Default

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, all of the headers in the packet content window are displayed in the packet-listing window, as shown below. The No header is shown in the Frame field, the Time header is displayed in the Frame Arrival Time field, the Source/Destination headers are displayed in the Internet Protocol Source/Destination fields, and Protocol header is displayed in the Hypertext Transfer Protocol field, the Length is displayed in the Frame field's Frame Length subfield, and the Info header is displayed in the Hypertext Transfer Protocol field's GET subfield.



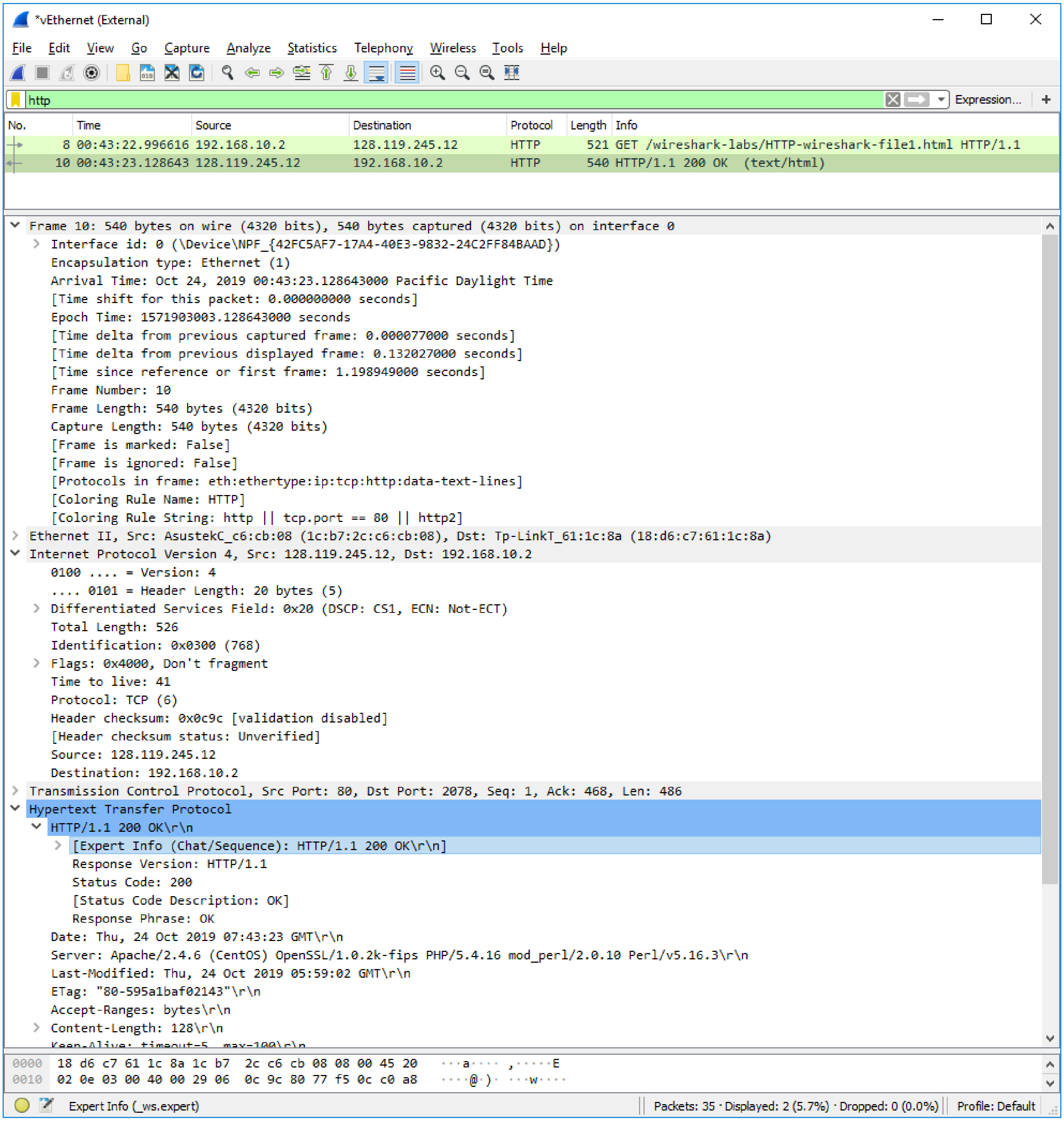
*vEthernet (External)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression…
+

No.	Time	Source	Destination	Protocol	Length	Info
8	00:43:22.996616	192.168.10.2	128.119.245.12	HTTP	521	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
10	00:43:23.128643	128.119.245.12	192.168.10.2	HTTP	540	HTTP/1.1 200 OK (text/html)

```
Frame 8: 521 bytes on wire (4168 bits), 521 bytes captured (4168 bits) on interface 0
  > Interface id: 0 (\Device\NPF_{42FC5AF7-17A4-40E3-9832-24C2FF84BAAD})
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 24, 2019 00:43:22.996616000 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1571903002.996616000 seconds
    [Time delta from previous captured frame: 0.000193000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 1.066922000 seconds]
    Frame Number: 8
    Frame Length: 521 bytes (4168 bits)
    Capture Length: 521 bytes (4168 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
> Ethernet II, Src: Tp-LinkT_61:1c:8a (18:d6:c7:61:1c:8a), Dst: AsustekC_c6:cb:08 (1c:b7:2c:c6:cb:08)
Internet Protocol Version 4, Src: 192.168.10.2, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 507
    Identification: 0x31af (12719)
  > Flags: 0x4000, Don't fragment
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.10.2
    Destination: 128.119.245.12
> Transmission Control Protocol, Src Port: 2078, Dst Port: 80, Seq: 1, Ack: 1, Len: 467
Hypertext Transfer Protocol
    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
    DNT: 1\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
```

```
0000  1c b7 2c c6 cb 08 18 d6  c7 61 1c 8a 08 00 45 00   ··,····· ·a····E·
0010  01 fb 31 af 40 00 80 06  00 00 c0 a8 0a 02 80 77   ··1·@··· ·······w
```

Expert Info (_ws.expert)   Packets: 35 · Displayed: 2 (5.7%) · Dropped: 0 (0.0%)   Profile: Default


*vEthernet (External)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression…
+

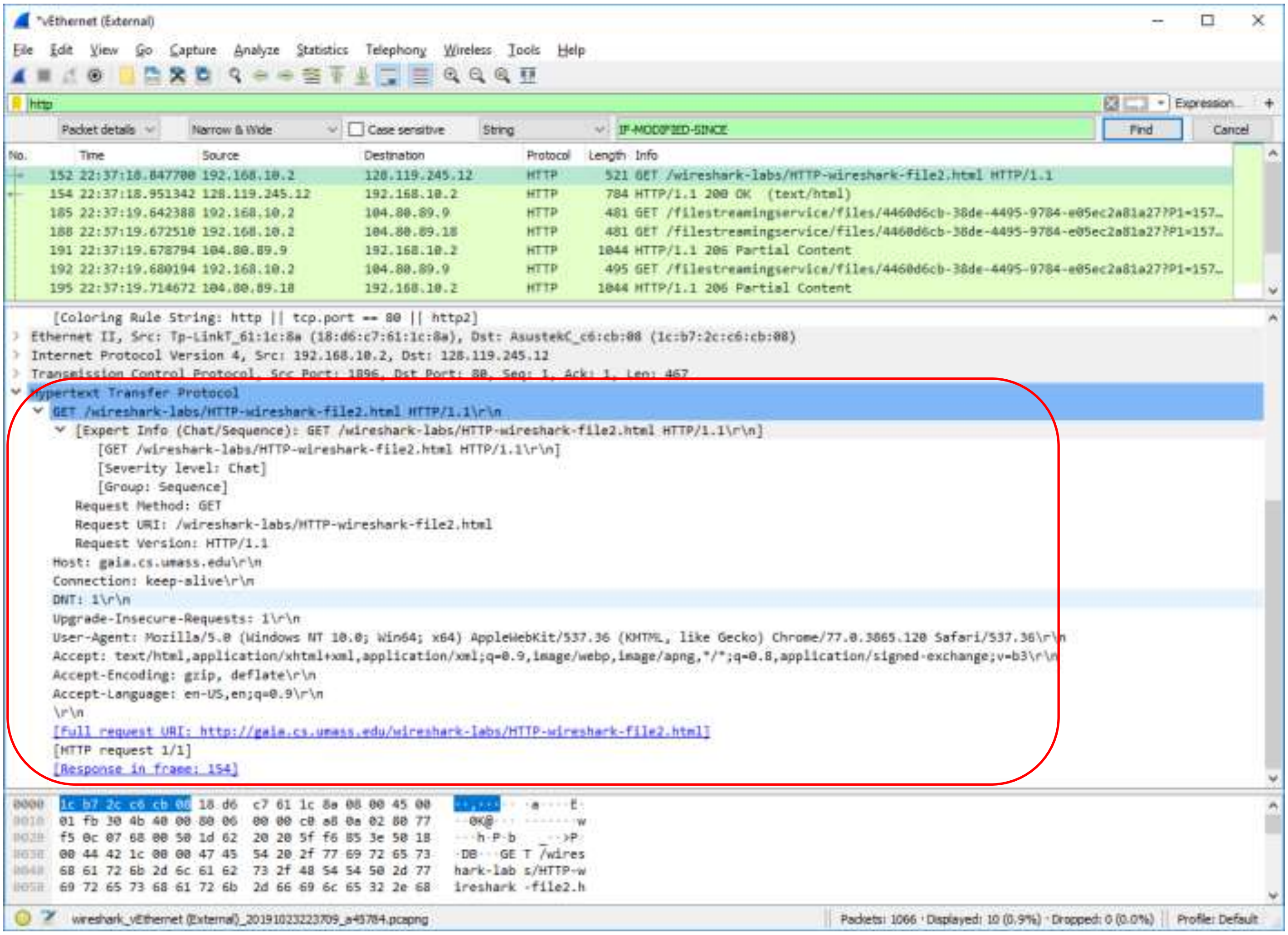
```
No.   Time             Source          Destination     Protocol Length Info
    8 00:43:22.996616  192.168.10.2    128.119.245.12  HTTP        521 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
   10 00:43:23.128643  128.119.245.12  192.168.10.2    HTTP        540 HTTP/1.1 200 OK  (text/html)
```

```
v Frame 10: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
  > Interface id: 0 (\Device\NPF_{42FC5AF7-17A4-40E3-9832-24C2FF84BAAD})
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 24, 2019 00:43:23.128643000 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1571903003.128643000 seconds
    [Time delta from previous captured frame: 0.000077000 seconds]
    [Time delta from previous displayed frame: 0.132027000 seconds]
    [Time since reference or first frame: 1.198949000 seconds]
    Frame Number: 10
    Frame Length: 540 bytes (4320 bits)
    Capture Length: 540 bytes (4320 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
> Ethernet II, Src: AsustekC_c6:cb:08 (1c:b7:2c:c6:cb:08), Dst: Tp-LinkT_61:1c:8a (18:d6:c7:61:1c:8a)
v Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.10.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
    Total Length: 526
    Identification: 0x0300 (768)
  > Flags: 0x4000, Don't fragment
    Time to live: 41
    Protocol: TCP (6)
    Header checksum: 0x0c9c [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.119.245.12
    Destination: 192.168.10.2
> Transmission Control Protocol, Src Port: 80, Dst Port: 2078, Seq: 1, Ack: 468, 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: Thu, 24 Oct 2019 07:43:23 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: Thu, 24 Oct 2019 05:59:02 GMT\r\n
    ETag: "80-595a1baf02143"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
```

```
0000  18 d6 c7 61 1c 8a 1c b7  2c c6 cb 08 08 00 45 20   ···a···· ,·····E 
0010  02 0e 03 00 40 00 29 06  0c 9c 80 77 f5 0c c0 a8   ····@·)· ···w····
```

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

No, there is no IF-MODIFIED-SINCE line in the first HTTP GET message, as shown below.



```
No.   Time              Source          Destination     Protocol Length Info
  152 22:37:18.847700 192.168.10.2    128.119.245.12  HTTP      521 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  154 22:37:18.951342 128.119.245.12  192.168.10.2    HTTP      784 HTTP/1.1 200 OK  (text/html)
  185 22:37:19.642388 192.168.10.2    104.80.89.9     HTTP      481 GET /filestreamingservice/files/4460d6cb-38de-4495-9784-e05ec2a81a27?P1=157…
  188 22:37:19.672510 192.168.10.2    104.80.89.18    HTTP      481 GET /filestreamingservice/files/4460d6cb-38de-4495-9784-e05ec2a81a27?P1=157…
  191 22:37:19.678794 104.80.89.9     192.168.10.2    HTTP     1044 HTTP/1.1 206 Partial Content
  192 22:37:19.680194 192.168.10.2    104.80.89.9     HTTP      495 GET /filestreamingservice/files/4460d6cb-38de-4495-9784-e05ec2a81a27?P1=157…
  195 22:37:19.714672 104.80.89.18    192.168.10.2    HTTP     1044 HTTP/1.1 206 Partial Content
```

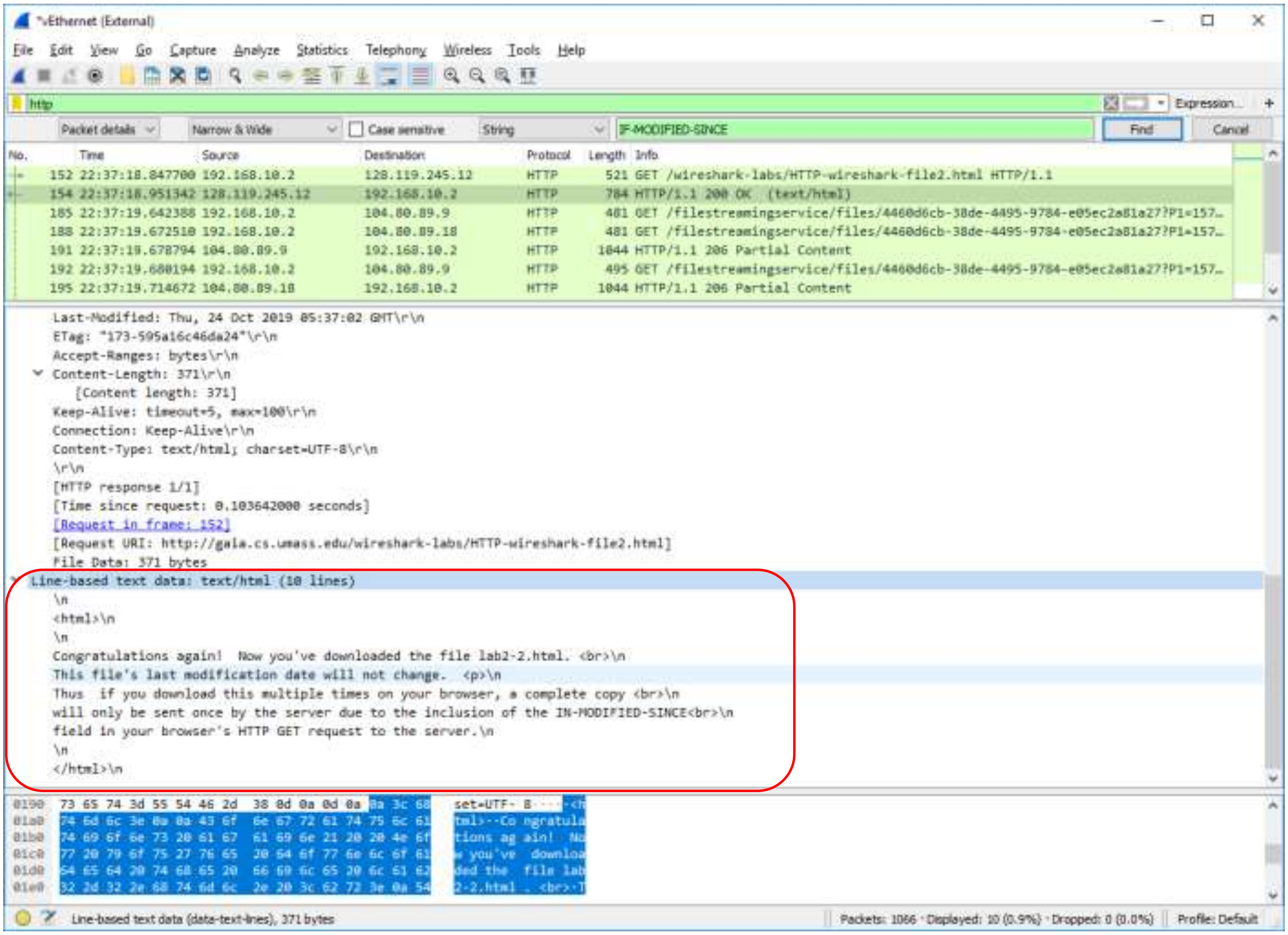
```
    [Coloring Rule String: http || tcp.port == 80 || http2]
> Ethernet II, Src: Tp-LinkT_61:1c:8a (18:d6:c7:61:1c:8a), Dst: AsustekC_c6:cb:08 (1c:b7:2c:c6:cb:08)
> Internet Protocol Version 4, Src: 192.168.10.2, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 1896, Dst Port: 80, Seq: 1, Ack: 1, Len: 467
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
    DNT: 1\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 1/1]
    [Response in frame: 154]
```

```
0000  1c b7 2c c6 cb 08 18 d6  c7 61 1c 8a 08 00 45 00   ··,····· ·a····E·
0010  01 fb 30 4b 40 00 80 06  00 00 c0 a8 0a 02 80 77   ··0K@··· ·······w
0020  f5 0c 07 68 00 50 1d 62  20 20 5f f6 85 3e 50 18   ···h·P·b   _··>P·
0030  00 44 42 1c 00 00 47 45  54 20 2f 77 69 72 65 73   ·DB···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 32 2e 68   ireshark -file2.h
```

wireshark_vEthernet (External)_20191023223709_a45784.pcapng
Packets: 1066 · Displayed: 10 (0.9%) · Dropped: 0 (0.0%)
Profile: Default

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

Yes, the server explicitly returned the contents of the file. The server response message contains a "line-based text data" field that displays the raw text of the file contents.



```
No.   Time                Source           Destination      Protocol  Length  Info
 152 22:37:18.847700 192.168.10.2     128.119.245.12   HTTP       521 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 154 22:37:18.951342 128.119.245.12   192.168.10.2     HTTP       784 HTTP/1.1 200 OK  (text/html)
 185 22:37:19.642388 192.168.10.2     104.80.89.9      HTTP       481 GET /filestreamingservice/files/4460d6cb-38de-4495-9784-e05ec2a81a27?P1=157…
 188 22:37:19.672510 192.168.10.2     104.80.89.18     HTTP       481 GET /filestreamingservice/files/4460d6cb-38de-4495-9784-e05ec2a81a27?P1=157…
 191 22:37:19.678794 104.80.89.9      192.168.10.2     HTTP      1044 HTTP/1.1 206 Partial Content
 192 22:37:19.680194 192.168.10.2     104.80.89.9      HTTP       495 GET /filestreamingservice/files/4460d6cb-38de-4495-9784-e05ec2a81a27?P1=157…
 195 22:37:19.714672 104.80.89.18     192.168.10.2     HTTP      1044 HTTP/1.1 206 Partial Content
```

```
    Last-Modified: Thu, 24 Oct 2019 05:37:02 GMT\r\n
    ETag: "173-595a16c46da24"\r\n
    Accept-Ranges: bytes\r\n
  ˅ Content-Length: 371\r\n
        [Content length: 371]
    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: 0.103642000 seconds]
    [Request in frame: 152]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    File Data: 371 bytes
˅ 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
```

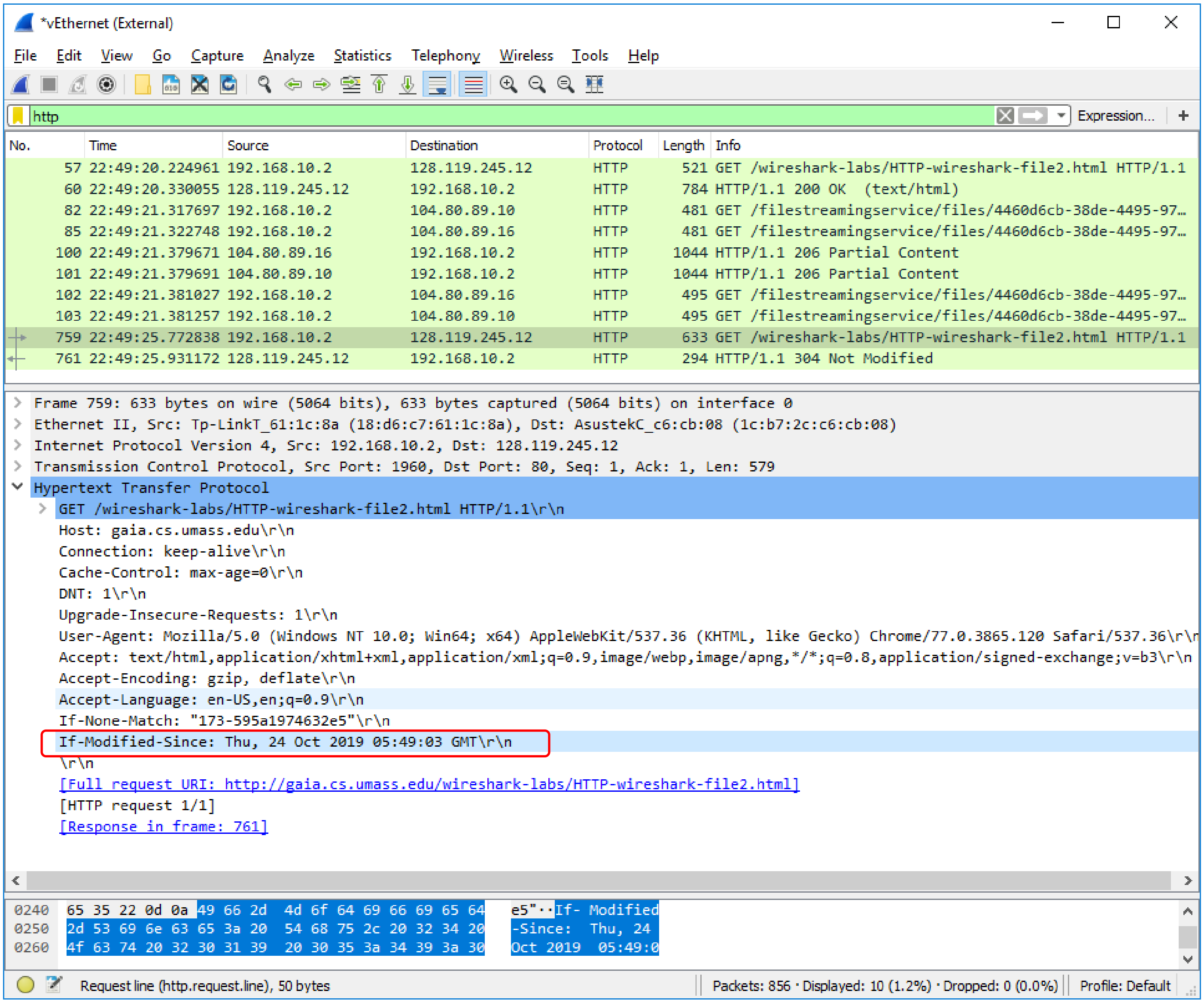
```
0190  73 65 74 3d 55 54 46 2d  38 0d 0a 0d 0a 0a 3c 68   set=UTF- 8·····<h
01a0  74 6d 6c 3e 0a 0a 43 6f  6e 67 72 61 74 75 6c 61   tml>··Co ngratula
01b0  74 69 6f 6e 73 20 61 67  61 69 6e 21 20 20 4e 6f   tions ag ain!  No
01c0  77 20 79 6f 75 27 76 65  20 64 6f 77 6e 6c 6f 61   w you've  downloa
01d0  64 65 64 20 74 68 65 20  66 69 6c 65 20 6c 61 62   ded the  file lab
01e0  32 2d 32 2e 68 74 6d 6c  2e 20 3c 62 72 3e 0a 54   2-2.html . <br>·T
```

Line-based text data (data-text-lines), 371 bytes

Packets: 1066 · Displayed: 10 (0.9%) · Dropped: 0 (0.0%) | Profile: Default

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?

Yes, the second and third HTTP GET requests do contain an IF-MODIFIED-SINCE line. The If-Modified-Since header displays the date "Thu, 24 Oct 2019 05:49:03 GMT", which is the date of the server's response to the last HTTP GET request for the file HTTP-wireshark-file2.html.


*vEthernet (External)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression…
+

```
No.   Time            Source          Destination     Protocol Length Info
   57 22:49:20.224961 192.168.10.2    128.119.245.12  HTTP      521 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   60 22:49:20.330055 128.119.245.12  192.168.10.2    HTTP      784 HTTP/1.1 200 OK  (text/html)
   82 22:49:21.317697 192.168.10.2    104.80.89.10    HTTP      481 GET /filestreamingservice/files/4460d6cb-38de-4495-97…
   85 22:49:21.322748 192.168.10.2    104.80.89.16    HTTP      481 GET /filestreamingservice/files/4460d6cb-38de-4495-97…
  100 22:49:21.379671 104.80.89.16    192.168.10.2    HTTP     1044 HTTP/1.1 206 Partial Content
  101 22:49:21.379691 104.80.89.10    192.168.10.2    HTTP     1044 HTTP/1.1 206 Partial Content
  102 22:49:21.381027 192.168.10.2    104.80.89.16    HTTP      495 GET /filestreamingservice/files/4460d6cb-38de-4495-97…
  103 22:49:21.381257 192.168.10.2    104.80.89.10    HTTP      495 GET /filestreamingservice/files/4460d6cb-38de-4495-97…
  759 22:49:25.772838 192.168.10.2    128.119.245.12  HTTP      633 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  761 22:49:25.931172 128.119.245.12  192.168.10.2    HTTP      294 HTTP/1.1 304 Not Modified
```

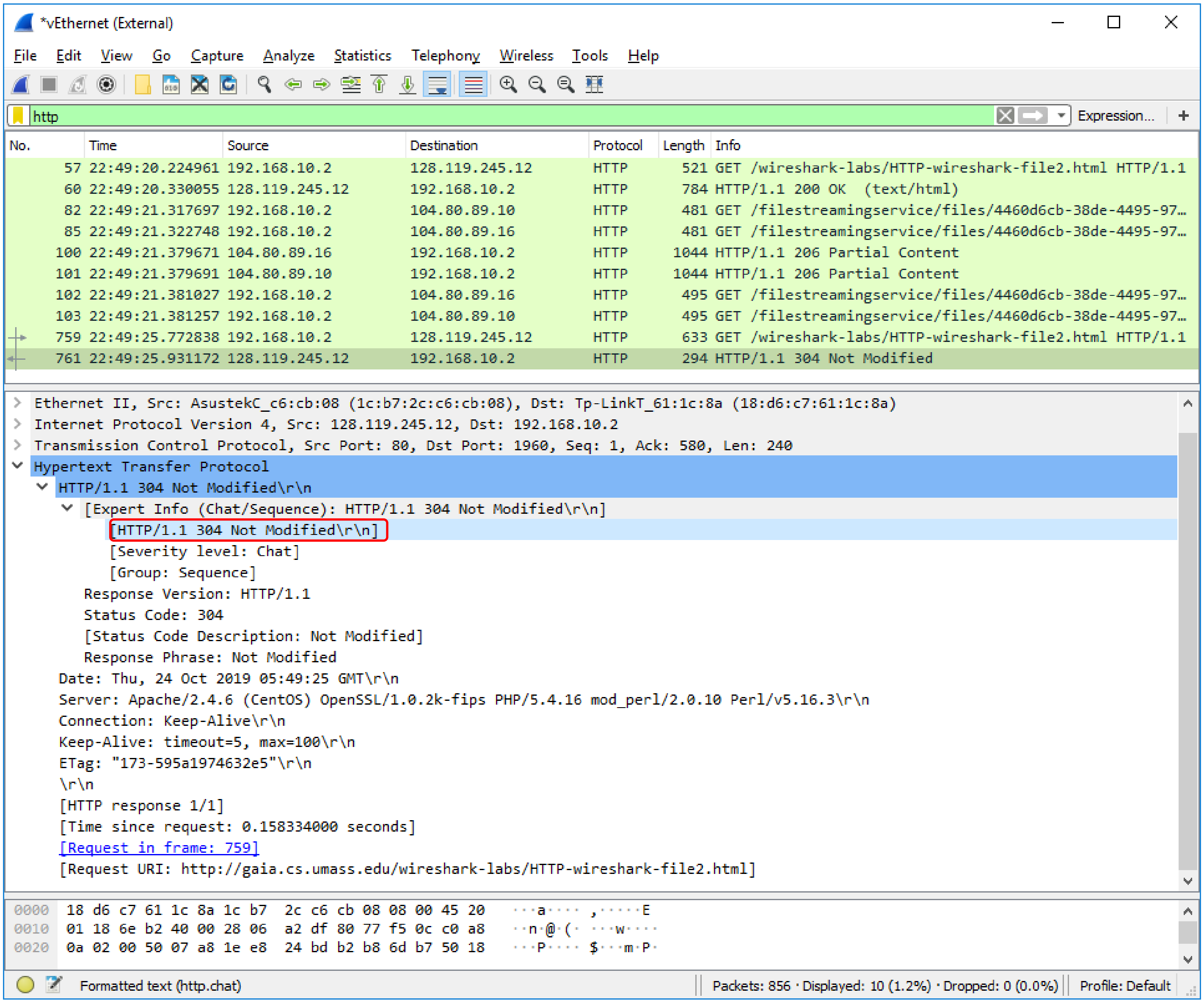
```
> Frame 759: 633 bytes on wire (5064 bits), 633 bytes captured (5064 bits) on interface 0
> Ethernet II, Src: Tp-LinkT_61:1c:8a (18:d6:c7:61:1c:8a), Dst: AsustekC_c6:cb:08 (1c:b7:2c:c6:cb:08)
> Internet Protocol Version 4, Src: 192.168.10.2, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 1960, Dst Port: 80, Seq: 1, Ack: 1, Len: 579
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
    DNT: 1\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\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: "173-595a1974632e5"\r\n
    If-Modified-Since: Thu, 24 Oct 2019 05:49:03 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: 761]
```

```
0240  65 35 22 0d 0a 49 66 2d  4d 6f 64 69 66 69 65 64   e5"··If- Modified
0250  2d 53 69 6e 63 65 3a 20  54 68 75 2c 20 32 34 20   -Since:  Thu, 24
0260  4f 63 74 20 32 30 31 39  20 30 35 3a 34 39 3a 30   Oct 2019  05:49:0
```

Request line (http.request.line), 50 bytes
Packets: 856 · Displayed: 10 (1.2%) · Dropped: 0 (0.0%)
Profile: Default

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.

The HTTP status code is 304 (Not Modified). No, the server did not explicitly return the contents of the file, which is apparent in the image below since the "Line-based text data" header is missing. This implies that the server's version of the file has not been modified more recently than the browser's version of the file stored in cache, so the server did not need to send the file.


*vEthernet (External)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

http

```
No.   Time            Source          Destination     Protocol Length Info
   57 22:49:20.224961 192.168.10.2    128.119.245.12  HTTP      521 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   60 22:49:20.330055 128.119.245.12  192.168.10.2    HTTP      784 HTTP/1.1 200 OK  (text/html)
   82 22:49:21.317697 192.168.10.2    104.80.89.10    HTTP      481 GET /filestreamingservice/files/4460d6cb-38de-4495-97…
   85 22:49:21.322748 192.168.10.2    104.80.89.16    HTTP      481 GET /filestreamingservice/files/4460d6cb-38de-4495-97…
  100 22:49:21.379671 104.80.89.16    192.168.10.2    HTTP     1044 HTTP/1.1 206 Partial Content
  101 22:49:21.379691 104.80.89.10    192.168.10.2    HTTP     1044 HTTP/1.1 206 Partial Content
  102 22:49:21.381027 192.168.10.2    104.80.89.16    HTTP      495 GET /filestreamingservice/files/4460d6cb-38de-4495-97…
  103 22:49:21.381257 192.168.10.2    104.80.89.10    HTTP      495 GET /filestreamingservice/files/4460d6cb-38de-4495-97…
  759 22:49:25.772838 192.168.10.2    128.119.245.12  HTTP      633 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  761 22:49:25.931172 128.119.245.12  192.168.10.2    HTTP      294 HTTP/1.1 304 Not Modified
```

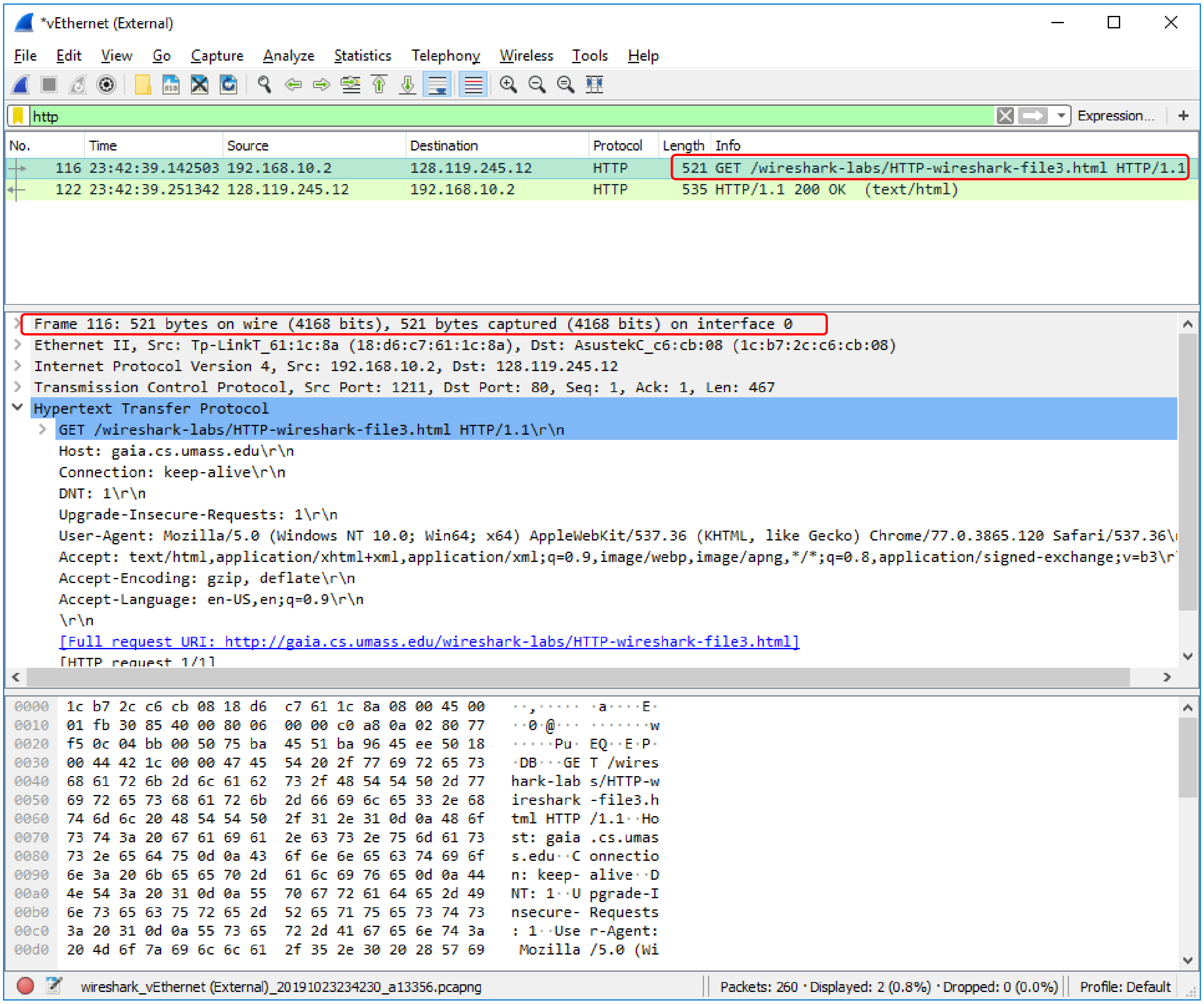
```
> Ethernet II, Src: AsustekC_c6:cb:08 (1c:b7:2c:c6:cb:08), Dst: Tp-LinkT_61:1c:8a (18:d6:c7:61:1c:8a)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.10.2
> Transmission Control Protocol, Src Port: 80, Dst Port: 1960, Seq: 1, Ack: 580, Len: 240
v Hypertext Transfer Protocol
  v HTTP/1.1 304 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
      Status Code: 304
      [Status Code Description: Not Modified]
      Response Phrase: Not Modified
    Date: Thu, 24 Oct 2019 05:49:25 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: "173-595a1974632e5"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.158334000 seconds]
    [Request in frame: 759]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

```
0000  18 d6 c7 61 1c 8a 1c b7  2c c6 cb 08 08 00 45 20   ···a···· ,·····E
0010  01 18 6e b2 40 00 28 06  a2 df 80 77 f5 0c c0 a8   ··n·@·(· ···w····
0020  0a 02 00 50 07 a8 1e e8  24 bd b2 b8 6d b7 50 18   ···P···· $···m·P·
```

Formatted text (http.chat) | Packets: 856 · Displayed: 10 (1.2%) · 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?

My browser sent 1 HTTP GET request message. Frame 116 contains the GET message for the Bill of Rights.


*vEthernet (External)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

```
http
```

```
No.   Time              Source          Destination     Protocol  Length  Info
  116 23:42:39.142503 192.168.10.2    128.119.245.12  HTTP       521 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  122 23:42:39.251342 128.119.245.12  192.168.10.2    HTTP       535 HTTP/1.1 200 OK  (text/html)
```

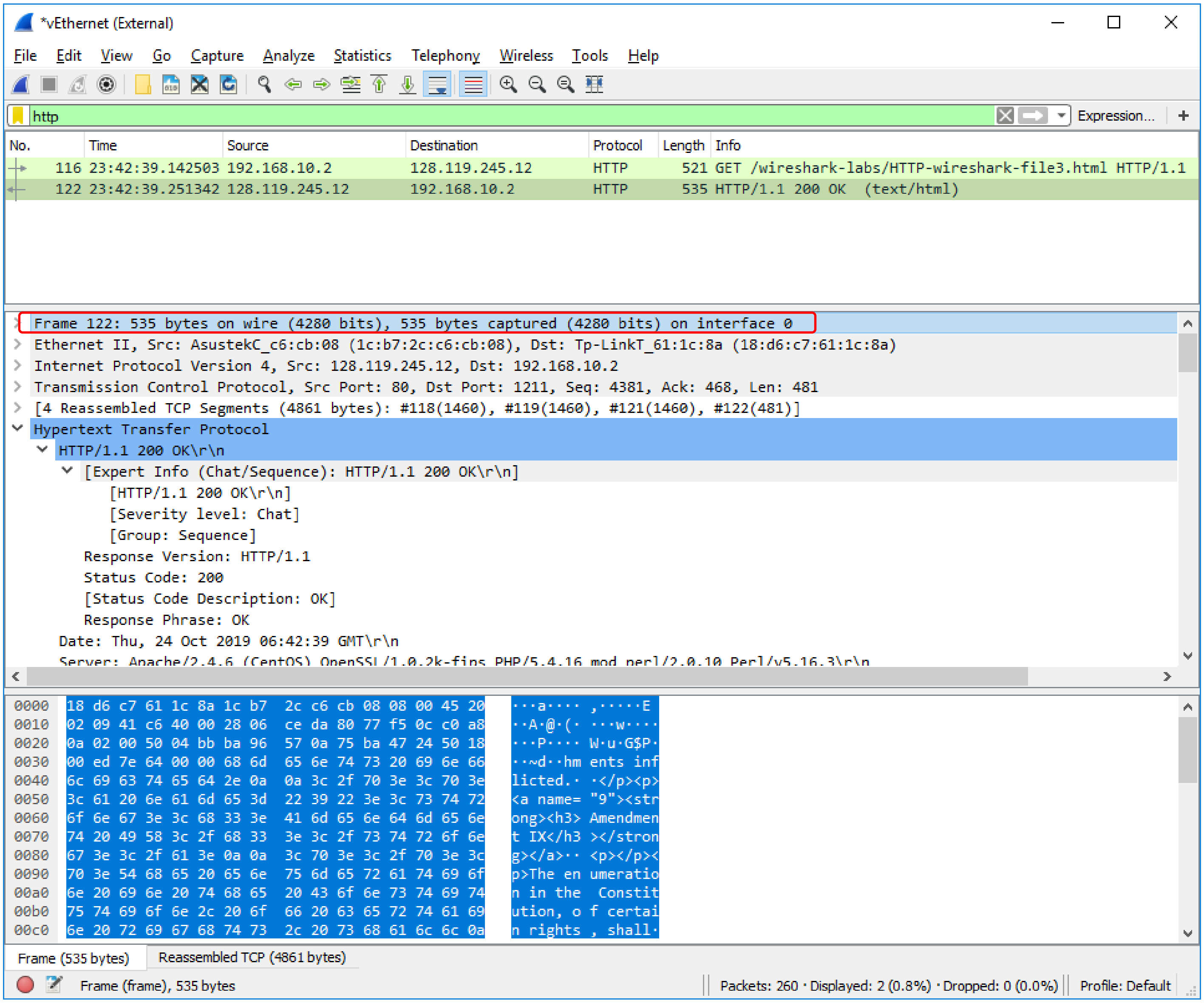
```
> Frame 116: 521 bytes on wire (4168 bits), 521 bytes captured (4168 bits) on interface 0
> Ethernet II, Src: Tp-LinkT_61:1c:8a (18:d6:c7:61:1c:8a), Dst: AsustekC_c6:cb:08 (1c:b7:2c:c6:cb:08)
> Internet Protocol Version 4, Src: 192.168.10.2, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 1211, Dst Port: 80, Seq: 1, Ack: 1, Len: 467
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
    DNT: 1\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\
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r
    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]
```

```
0000  1c b7 2c c6 cb 08 18 d6  c7 61 1c 8a 08 00 45 00   ··,····· ·a····E·
0010  01 fb 30 85 40 00 80 06  00 00 c0 a8 0a 02 80 77   ··0·@··· ·······w
0020  f5 0c 04 bb 00 50 75 ba  45 51 ba 96 45 ee 50 18   ·····Pu· EQ··E·P·
0030  00 44 42 1c 00 00 47 45  54 20 2f 77 69 72 65 73   ·DB···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
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 44   n: keep- alive··D
00a0  4e 54 3a 20 31 0d 0a 55  70 67 72 61 64 65 2d 49   NT: 1··U pgrade-I
00b0  6e 73 65 63 75 72 65 2d  52 65 71 75 65 73 74 73   nsecure- Requests
00c0  3a 20 31 0d 0a 55 73 65  72 2d 41 67 65 6e 74 3a   : 1··Use r-Agent:
00d0  20 4d 6f 7a 69 6c 6c 61  2f 35 2e 30 20 28 57 69    Mozilla /5.0 (Wi
```

```
wireshark_vEthernet (External)_20191023234230_a13356.pcapng    Packets: 260 · Displayed: 2 (0.8%) · Dropped: 0 (0.0%)    Profile: Default
```

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

Frame 122 contains the response to the HTTP GET request.



*vEthernet (External)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression…
+

```
No.  Time             Source          Destination     Protocol Length Info
116  23:42:39.142503  192.168.10.2    128.119.245.12  HTTP     521    GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
122  23:42:39.251342  128.119.245.12  192.168.10.2    HTTP     535    HTTP/1.1 200 OK  (text/html)
```

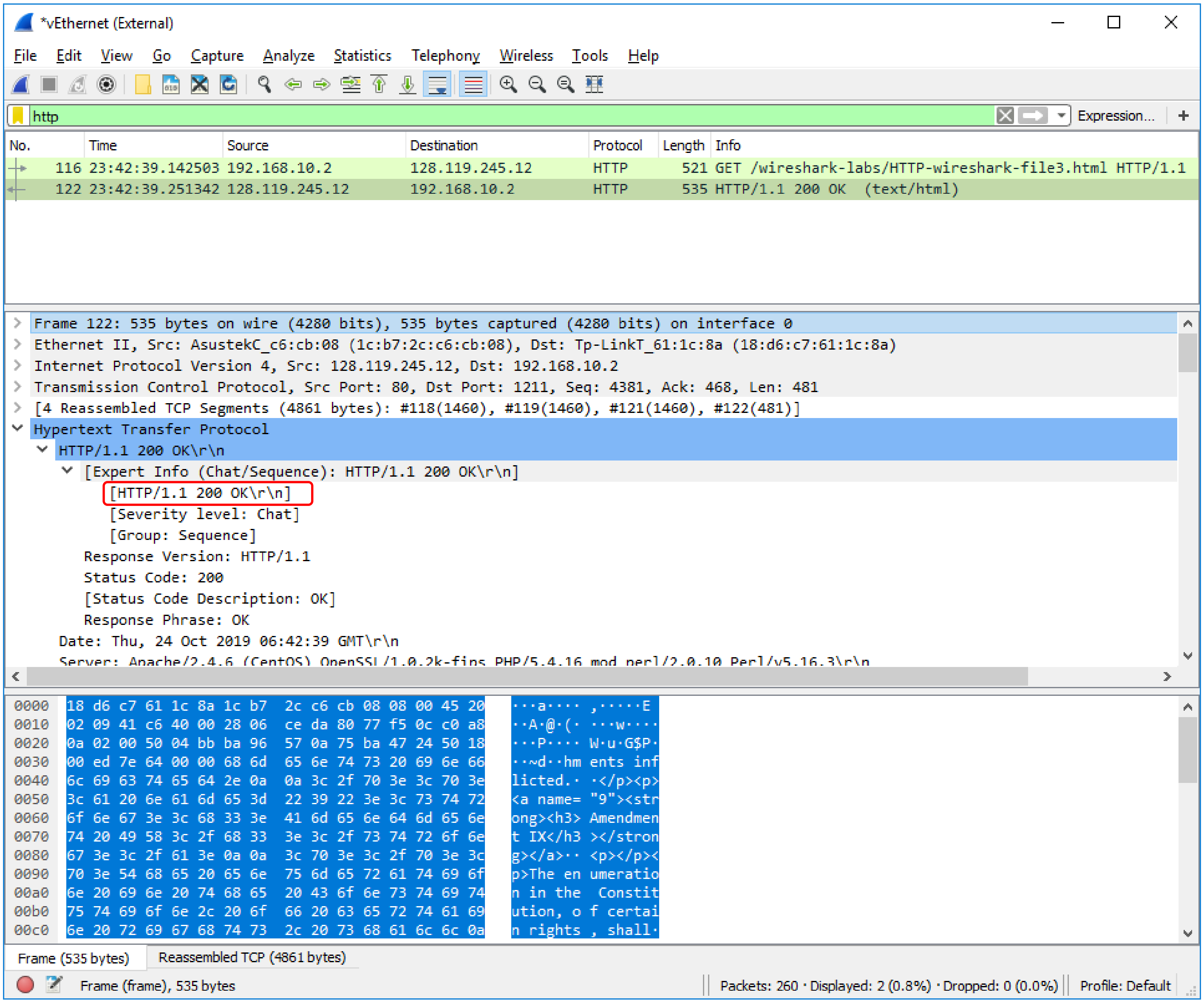
```
> Frame 122: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface 0
> Ethernet II, Src: AsustekC_c6:cb:08 (1c:b7:2c:c6:cb:08), Dst: Tp-LinkT_61:1c:8a (18:d6:c7:61:1c:8a)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.10.2
> Transmission Control Protocol, Src Port: 80, Dst Port: 1211, Seq: 4381, Ack: 468, Len: 481
> [4 Reassembled TCP Segments (4861 bytes): #118(1460), #119(1460), #121(1460), #122(481)]
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: Thu, 24 Oct 2019 06:42:39 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
```

```
0000  18 d6 c7 61 1c 8a 1c b7  2c c6 cb 08 08 00 45 20   ···a···· ,·····E
0010  02 09 41 c6 40 00 28 06  ce da 80 77 f5 0c c0 a8   ··A·@·(· ···w····
0020  0a 02 00 50 04 bb ba 96  57 0a 75 ba 47 24 50 18   ···P···· W·u·G$P·
0030  00 ed 7e 64 00 00 68 6d  65 6e 74 73 20 69 6e 66   ··~d··hm ents inf
0040  6c 69 63 74 65 64 2e 0a  0a 3c 2f 70 3e 3c 70 3e   licted.· ·</p><p>
0050  3c 61 20 6e 61 6d 65 3d  22 39 22 3e 3c 73 74 72   <a name= "9"><str
0060  6f 6e 67 3e 3c 68 33 3e  41 6d 65 6e 64 6d 65 6e   ong><h3> Amendmen
0070  74 20 49 58 3c 2f 68 33  3e 3c 2f 73 74 72 6f 6e   t IX</h3 ></stron
0080  67 3e 3c 2f 61 3e 0a 0a  3c 70 3e 3c 2f 70 3e 3c   g></a>·· <p></p><
0090  70 3e 54 68 65 20 65 6e  75 6d 65 72 61 74 69 6f   p>The en umeratio
00a0  6e 20 69 6e 20 74 68 65  20 43 6f 6e 73 74 69 74   n in the  Constit
00b0  75 74 69 6f 6e 2c 20 6f  66 20 63 65 72 74 61 69   ution, o f certai
00c0  6e 20 72 69 67 68 74 73  2c 20 73 68 61 6c 6c 0a   n rights , shall·
```

Frame (535 bytes)
Reassembled TCP (4861 bytes)
Frame (frame), 535 bytes
Packets: 260 · Displayed: 2 (0.8%) · Dropped: 0 (0.0%)
Profile: Default

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

The response's status code is 200 and the phrase is "OK".



*vEthernet (External)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression…
+

```
No.  Time             Source          Destination     Protocol  Length Info
116 23:42:39.142503 192.168.10.2    128.119.245.12  HTTP       521 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
122 23:42:39.251342 128.119.245.12  192.168.10.2    HTTP       535 HTTP/1.1 200 OK  (text/html)
```

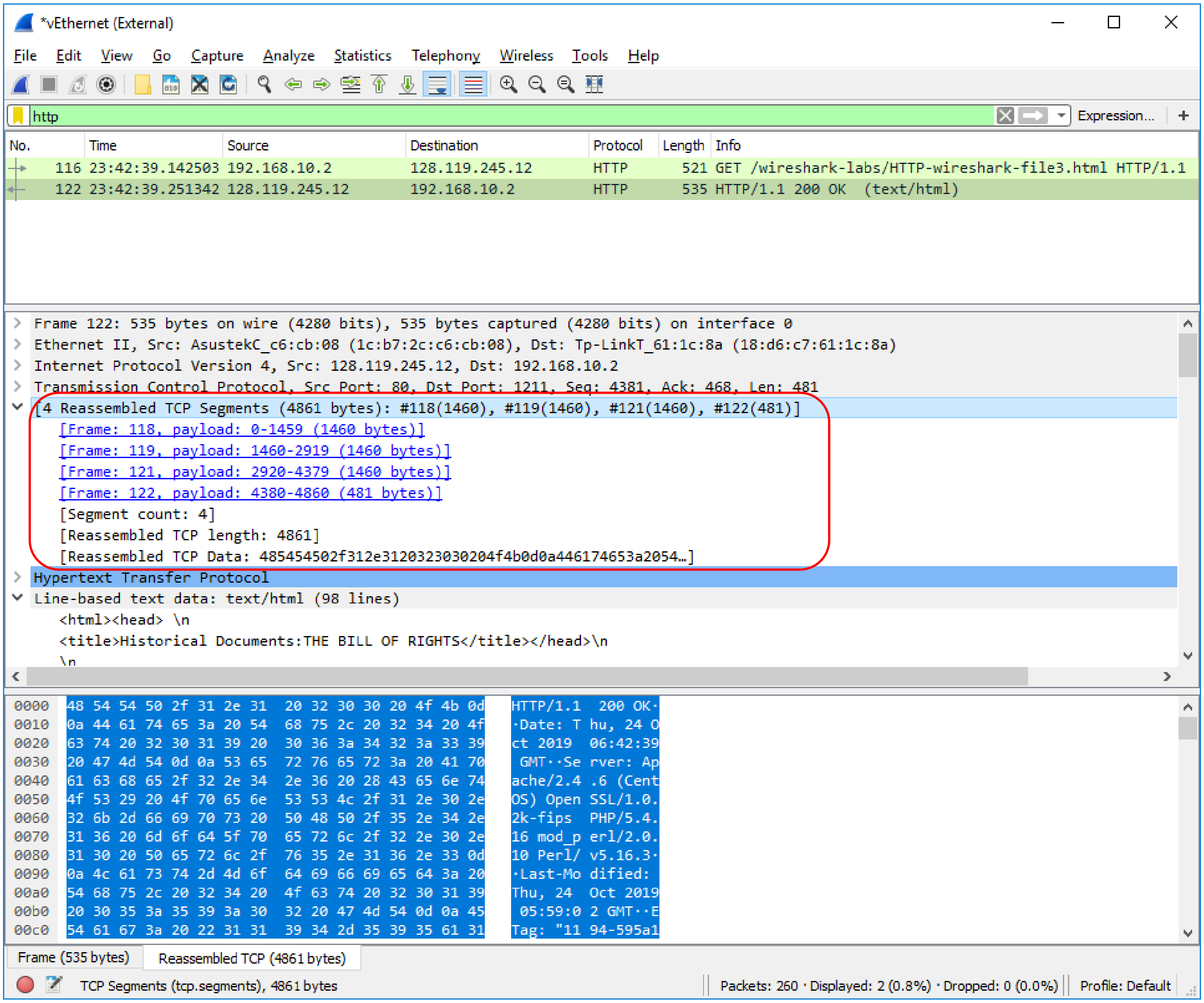
```
> Frame 122: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface 0
> Ethernet II, Src: AsustekC_c6:cb:08 (1c:b7:2c:c6:cb:08), Dst: Tp-LinkT_61:1c:8a (18:d6:c7:61:1c:8a)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.10.2
> Transmission Control Protocol, Src Port: 80, Dst Port: 1211, Seq: 4381, Ack: 468, Len: 481
> [4 Reassembled TCP Segments (4861 bytes): #118(1460), #119(1460), #121(1460), #122(481)]
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: Thu, 24 Oct 2019 06:42:39 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
```

```
0000  18 d6 c7 61 1c 8a 1c b7  2c c6 cb 08 08 00 45 20   ···a···· ,·····E 
0010  02 09 41 c6 40 00 28 06  ce da 80 77 f5 0c c0 a8   ··A·@·(· ···w····
0020  0a 02 00 50 04 bb ba 96  57 0a 75 ba 47 24 50 18   ···P···· W·u·G$P·
0030  00 ed 7e 64 00 00 68 6d  65 6e 74 73 20 69 6e 66   ··~d··hm ents inf
0040  6c 69 63 74 65 64 2e 0a  0a 3c 2f 70 3e 3c 70 3e   licted.· ·</p><p>
0050  3c 61 20 6e 61 6d 65 3d  22 39 22 3e 3c 73 74 72   <a name= "9"><str
0060  6f 6e 67 3e 3c 68 33 3e  41 6d 65 6e 64 6d 65 6e   ong><h3> Amendmen
0070  74 20 49 58 3c 2f 68 33  3e 3c 2f 73 74 72 6f 6e   t IX</h3 ></stron
0080  67 3e 3c 2f 61 3e 0a 0a  3c 70 3e 3c 2f 70 3e 3c   g></a>·· <p></p><
0090  70 3e 54 68 65 20 65 6e  75 6d 65 72 61 74 69 6f   p>The en umeratio
00a0  6e 20 69 6e 20 74 68 65  20 43 6f 6e 73 74 69 74   n in the  Constit
00b0  75 74 69 6f 6e 2c 20 6f  66 20 63 65 72 74 61 69   ution, o f certai
00c0  6e 20 72 69 67 68 74 73  2c 20 73 68 61 6c 6c 0a   n rights , shall·
```

Frame (535 bytes)
Reassembled TCP (4861 bytes)
Frame (frame), 535 bytes
Packets: 260 · Displayed: 2 (0.8%) · Dropped: 0 (0.0%)
Profile: Default

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

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


*vEthernet (External)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression… +

```
http
```

```
No.   Time            Source          Destination     Protocol Length Info
  116 23:42:39.142503 192.168.10.2    128.119.245.12  HTTP      521 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  122 23:42:39.251342 128.119.245.12  192.168.10.2    HTTP      535 HTTP/1.1 200 OK  (text/html)
```

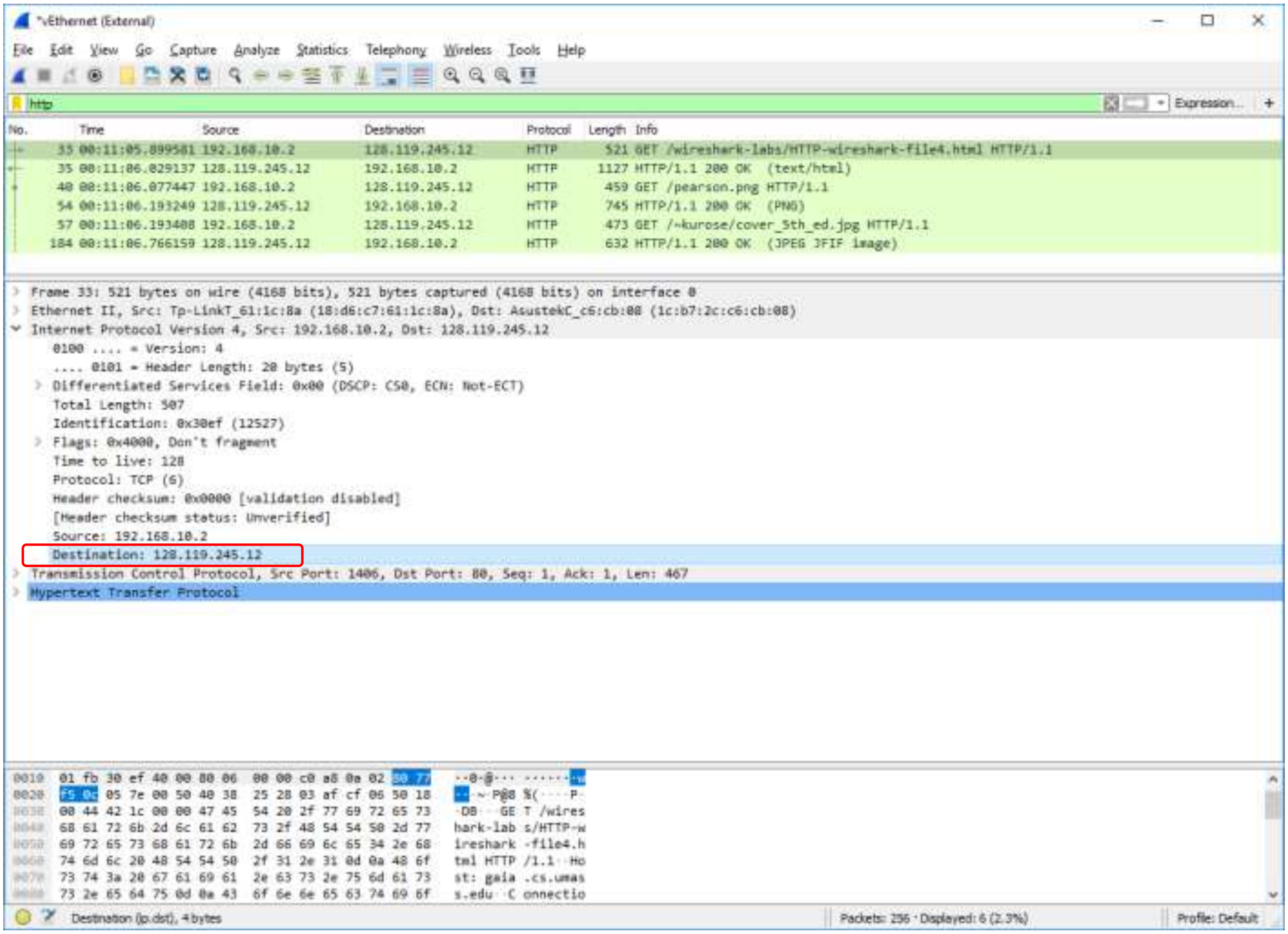
```
> Frame 122: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface 0
> Ethernet II, Src: AsustekC_c6:cb:08 (1c:b7:2c:c6:cb:08), Dst: Tp-LinkT_61:1c:8a (18:d6:c7:61:1c:8a)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.10.2
> Transmission Control Protocol, Src Port: 80, Dst Port: 1211, Seq: 4381, Ack: 468, Len: 481
v [4 Reassembled TCP Segments (4861 bytes): #118(1460), #119(1460), #121(1460), #122(481)]
    [Frame: 118, payload: 0-1459 (1460 bytes)]
    [Frame: 119, payload: 1460-2919 (1460 bytes)]
    [Frame: 121, payload: 2920-4379 (1460 bytes)]
    [Frame: 122, payload: 4380-4860 (481 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2054…]
> Hypertext Transfer Protocol
v Line-based text data: text/html (98 lines)
    <html><head> \n
    <title>Historical Documents:THE BILL OF RIGHTS</title></head>\n
    \n
```

```
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 34 20 4f   ·Date: T hu, 24 O
0020  63 74 20 32 30 31 39 20  30 36 3a 34 32 3a 33 39   ct 2019  06:42:39
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.
0080  31 30 20 50 65 72 6c 2f  76 35 2e 31 36 2e 33 0d   10 Perl/ v5.16.3·
0090  0a 4c 61 73 74 2d 4d 6f  64 69 66 69 65 64 3a 20   ·Last-Mo dified: 
00a0  54 68 75 2c 20 32 34 20  4f 63 74 20 32 30 31 39   Thu, 24  Oct 2019
00b0  20 30 35 3a 35 39 3a 30  32 20 47 4d 54 0d 0a 45    05:59:0 2 GMT··E
00c0  54 61 67 3a 20 22 31 31  39 34 2d 35 39 35 61 31   Tag: "11 94-595a1
```

```
TCP Segments (tcp.segments), 4861 bytes    Packets: 260 · Displayed: 2 (0.8%) · 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?

My browser sent 3 HTTP GET request messages to 128.119.245.12.


*vEthernet (External)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

```
http
```

```
No.    Time               Source          Destination     Protocol Length Info
    33 00:11:05.899581 192.168.10.2     128.119.245.12   HTTP      521 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
    35 00:11:06.029137 128.119.245.12   192.168.10.2     HTTP     1127 HTTP/1.1 200 OK  (text/html)
    40 00:11:06.077447 192.168.10.2     128.119.245.12   HTTP      459 GET /pearson.png HTTP/1.1
    54 00:11:06.193249 128.119.245.12   192.168.10.2     HTTP      745 HTTP/1.1 200 OK  (PNG)
    57 00:11:06.193408 192.168.10.2     128.119.245.12   HTTP      473 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
   184 00:11:06.766159 128.119.245.12   192.168.10.2     HTTP      632 HTTP/1.1 200 OK  (JPEG JFIF image)
```

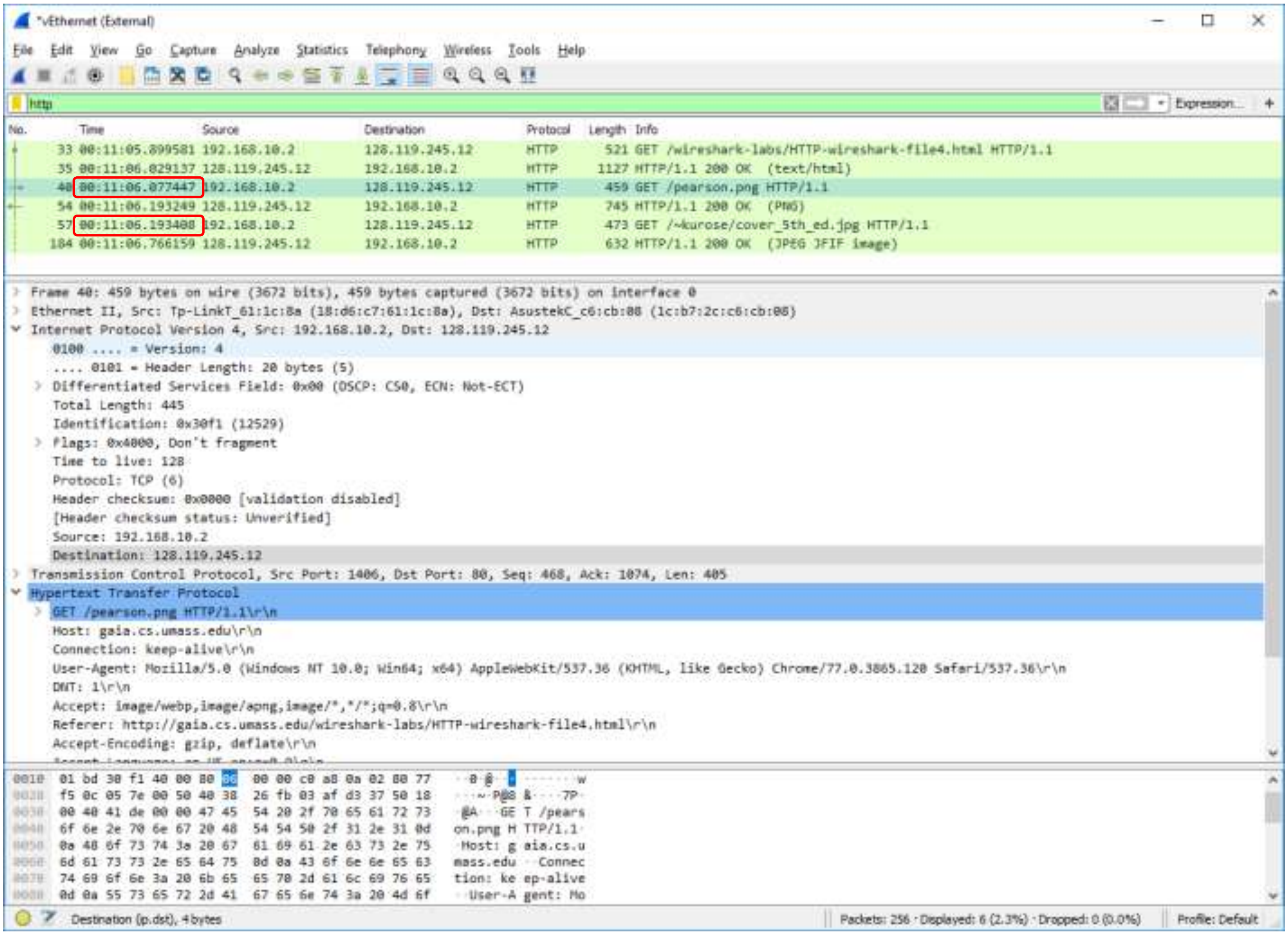
```
> Frame 33: 521 bytes on wire (4168 bits), 521 bytes captured (4168 bits) on interface 0
> Ethernet II, Src: Tp-LinkT_61:1c:8a (18:d6:c7:61:1c:8a), Dst: AsustekC_c6:cb:08 (1c:b7:2c:c6:cb:08)
v Internet Protocol Version 4, Src: 192.168.10.2, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 507
    Identification: 0x30ef (12527)
  > Flags: 0x4000, Don't fragment
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.10.2
    Destination: 128.119.245.12
> Transmission Control Protocol, Src Port: 1406, Dst Port: 80, Seq: 1, Ack: 1, Len: 467
> Hypertext Transfer Protocol
```

```
0010  01 fb 30 ef 40 00 80 06  00 00 c0 a8 0a 02 80 77   ··0·@··· ······.w
0020  f5 0c 05 7e 00 50 40 38  25 28 03 af cf 06 50 18   ··~·P@8 %(····P·
0030  00 44 42 1c 00 00 47 45  54 20 2f 77 69 72 65 73   ·DB···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
```

```
Destination (ip.dst), 4 bytes        Packets: 256 · Displayed: 6 (2.3%)        Profile: Default
```

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

The two images were downloaded serially because pearson.png was downloaded after the second HTTP GET message and cover_5th_ed.jpg was downloaded after the third HTTP GET message. There were 2 HTTP GET requests to download each of the 2 images, and the timestamps for the HTTP GET request messages do not match, so these images must not have been downloaded in parallel.



http

```
No.     Time            Source          Destination     Protocol Length Info
    33 00:11:05.899581 192.168.10.2    128.119.245.12  HTTP      521 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
    35 00:11:06.029137 128.119.245.12  192.168.10.2    HTTP     1127 HTTP/1.1 200 OK  (text/html)
    40 00:11:06.077447 192.168.10.2    128.119.245.12  HTTP      459 GET /pearson.png HTTP/1.1
    54 00:11:06.193249 128.119.245.12  192.168.10.2    HTTP      745 HTTP/1.1 200 OK  (PNG)
    57 00:11:06.193408 192.168.10.2    128.119.245.12  HTTP      473 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
   184 00:11:06.766159 128.119.245.12  192.168.10.2    HTTP      632 HTTP/1.1 200 OK  (JPEG JFIF image)
```

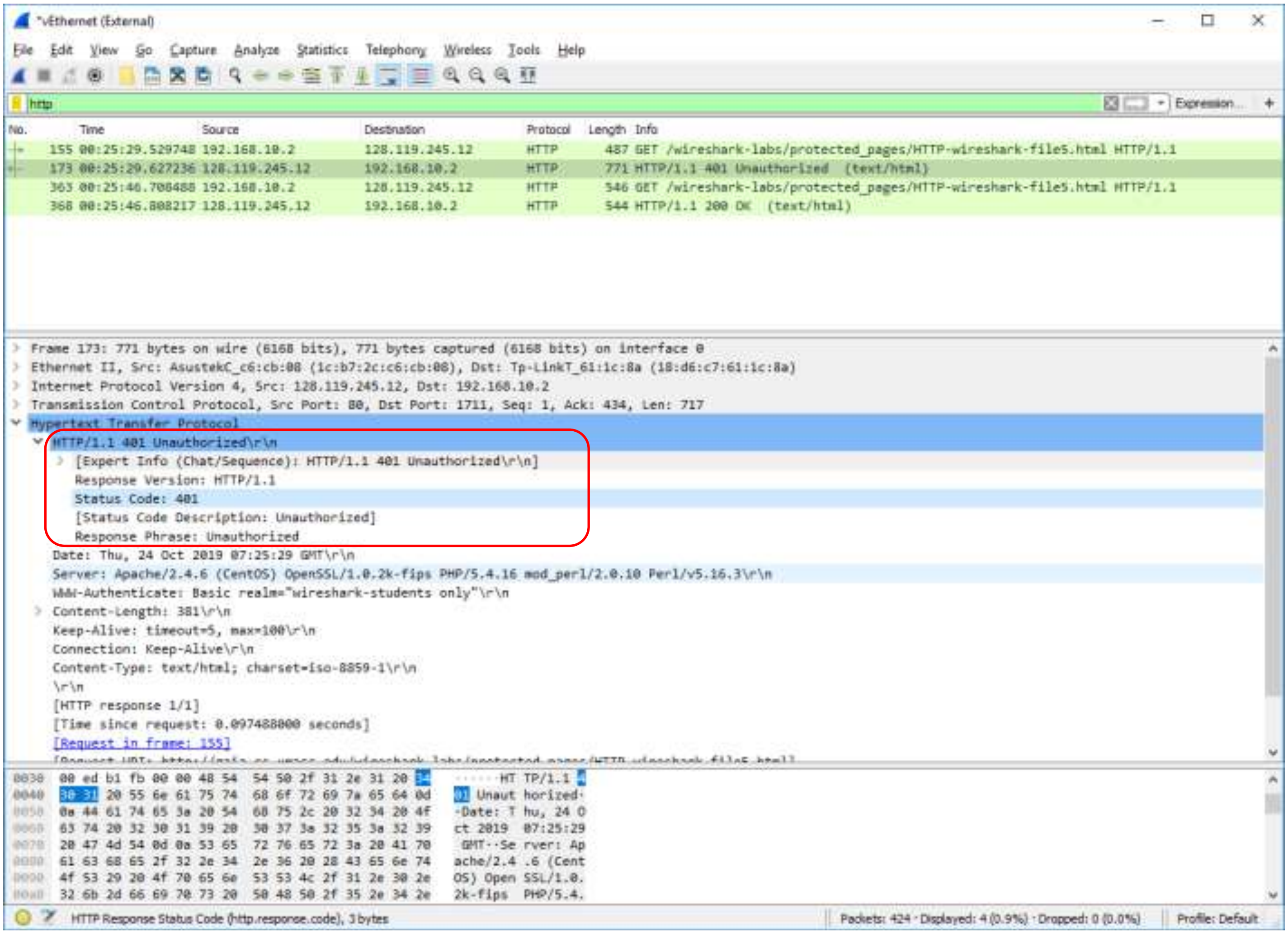
```
> Frame 40: 459 bytes on wire (3672 bits), 459 bytes captured (3672 bits) on interface 0
> Ethernet II, Src: Tp-LinkT_61:1c:8a (18:d6:c7:61:1c:8a), Dst: AsustekC_c6:cb:08 (1c:b7:2c:c6:cb:08)
v Internet Protocol Version 4, Src: 192.168.10.2, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 445
    Identification: 0x30f1 (12529)
  > Flags: 0x4000, Don't fragment
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.10.2
    Destination: 128.119.245.12
> Transmission Control Protocol, Src Port: 1406, Dst Port: 80, Seq: 468, Ack: 1074, Len: 405
v Hypertext Transfer Protocol
  > GET /pearson.png HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\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
    DNT: 1\r\n
    Accept: image/webp,image/apng,image/*,*/*;q=0.8\r\n
    Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html\r\n
    Accept-Encoding: gzip, deflate\r\n
```

```
0010  01 bd 30 f1 40 00 80 06  00 00 c0 a8 0a 02 80 77   ··0·@·········w
0020  f5 0c 05 7e 00 50 40 38  26 fb 03 af d3 37 50 18   ···~·P@8 &····7P·
0030  00 40 41 de 00 00 47 45  54 20 2f 70 65 61 72 73   ·@A···GE T /pears
0040  6f 6e 2e 70 6e 67 20 48  54 54 50 2f 31 2e 31 0d   on.png H TTP/1.1·
0050  0a 48 6f 73 74 3a 20 67  61 69 61 2e 63 73 2e 75   ·Host: g aia.cs.u
0060  6d 61 73 73 2e 65 64 75  0d 0a 43 6f 6e 6e 65 63   mass.edu ··Connec
0070  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: ke ep-alive
0080  0d 0a 55 73 65 72 2d 41  67 65 6e 74 3a 20 4d 6f   ··User-A gent: Mo
```

Destination (ip.dst), 4 bytes | Packets: 256 · Displayed: 6 (2.3%) · 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?

The server's first response to the initial HTTP GET message is status code 401 and phrase "Unauthorized".



*vEthernet (External)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
+

```
No.  Time            Source          Destination     Protocol Length Info
155  00:25:29.529748 192.168.10.2    128.119.245.12  HTTP     487 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
173  00:25:29.627236 128.119.245.12  192.168.10.2    HTTP     771 HTTP/1.1 401 Unauthorized  (text/html)
363  00:25:46.708488 192.168.10.2    128.119.245.12  HTTP     546 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
368  00:25:46.808217 128.119.245.12  192.168.10.2    HTTP     544 HTTP/1.1 200 OK  (text/html)
```

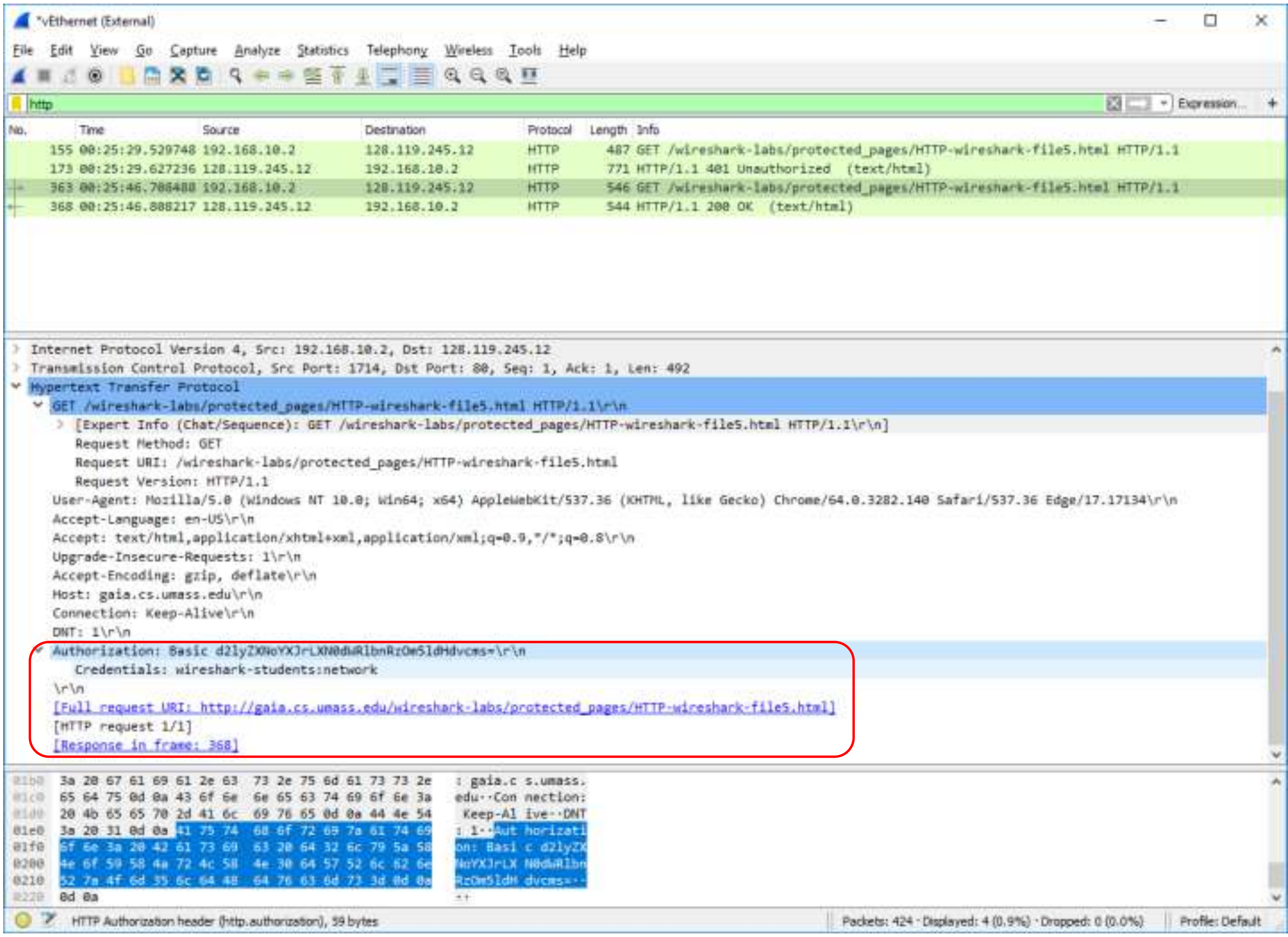
```
> Frame 173: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface 0
> Ethernet II, Src: AsustekC_c6:cb:08 (1c:b7:2c:c6:cb:08), Dst: Tp-LinkT_61:1c:8a (18:d6:c7:61:1c:8a)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.10.2
> Transmission Control Protocol, Src Port: 80, Dst Port: 1711, Seq: 1, Ack: 434, Len: 717
v Hypertext Transfer Protocol
  v HTTP/1.1 401 Unauthorized\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
      Response Version: HTTP/1.1
      Status Code: 401
      [Status Code Description: Unauthorized]
      Response Phrase: Unauthorized
    Date: Thu, 24 Oct 2019 07:25:29 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
    WWW-Authenticate: Basic realm="wireshark-students only"\r\n
  > Content-Length: 381\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.097488000 seconds]
    [Request in frame: 155]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
```

```
0030  00 ed b1 fb 00 00 48 54  54 50 2f 31 2e 31 20 34   ......HT TP/1.1 4
0040  30 31 20 55 6e 61 75 74  68 6f 72 69 7a 65 64 0d   01 Unaut horized·
0050  0a 44 61 74 65 3a 20 54  68 75 2c 20 32 34 20 4f   ·Date: T hu, 24 O
0060  63 74 20 32 30 31 39 20  30 37 3a 32 35 3a 32 39   ct 2019  07:25:29
0070  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT··Se rver: Ap
0080  61 63 68 65 2f 32 2e 34  2e 36 20 28 43 65 6e 74   ache/2.4 .6 (Cent
0090  4f 53 29 20 4f 70 65 6e  53 53 4c 2f 31 2e 30 2e   OS) Open SSL/1.0.
00a0  32 6b 2d 66 69 70 73 20  50 48 50 2f 35 2e 34 2e   2k-fips  PHP/5.4.
```

HTTP Response Status Code (http.response.code), 3 bytes | Packets: 424 · Displayed: 4 (0.9%) · Dropped: 0 (0.0%) | Profile: Default

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

The Authorization: Basic field is the new field that is included in the second HTTP GET message.


*vEthernet (External)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression…

```
No.     Time            Source          Destination     Protocol Length Info
    155 00:25:29.529748 192.168.10.2    128.119.245.12  HTTP     487 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
    173 00:25:29.627236 128.119.245.12  192.168.10.2    HTTP     771 HTTP/1.1 401 Unauthorized  (text/html)
    363 00:25:46.788488 192.168.10.2    128.119.245.12  HTTP     546 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
    368 00:25:46.888217 128.119.245.12  192.168.10.2    HTTP     544 HTTP/1.1 200 OK  (text/html)
```

```
> Internet Protocol Version 4, Src: 192.168.10.2, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 1714, Dst Port: 80, Seq: 1, Ack: 1, Len: 492
v Hypertext Transfer Protocol
  v GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
      Request Version: HTTP/1.1
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134\r\n
    Accept-Language: en-US\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept-Encoding: gzip, deflate\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: Keep-Alive\r\n
    DNT: 1\r\n
  v Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
      Credentials: wireshark-students:network
    \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: 368]
```

```
01b0  3a 20 67 61 69 61 2e 63  73 2e 75 6d 61 73 73 2e   : gaia.c s.umass.
01c0  65 64 75 0d 0a 43 6f 6e  6e 65 63 74 69 6f 6e 3a   edu··Con nection:
01d0  20 4b 65 65 70 2d 41 6c  69 76 65 0d 0a 44 4e 54    Keep-Al ive··DNT
01e0  3a 20 31 0d 0a 41 75 74  68 6f 72 69 7a 61 74 69   : 1··Aut horizati
01f0  6f 6e 3a 20 42 61 73 69  63 20 64 32 6c 79 5a 58   on: Basi c d2lyZX
0200  4e 6f 59 58 4a 72 4c 58  4e 30 64 57 52 6c 62 6e   NoYXJrLX N0dWRlbn
0210  52 7a 4f 6d 35 6c 64 48  64 76 63 6d 73 3d 0d 0a   RzOm5ldH dvcms=··
0220  0d 0a                                              ··
```

HTTP Authorization header (http.authorization), 59 bytes | Packets: 424 · Displayed: 4 (0.9%) · Dropped: 0 (0.0%) | Profile: Default