Wireshark Project-2

Answers

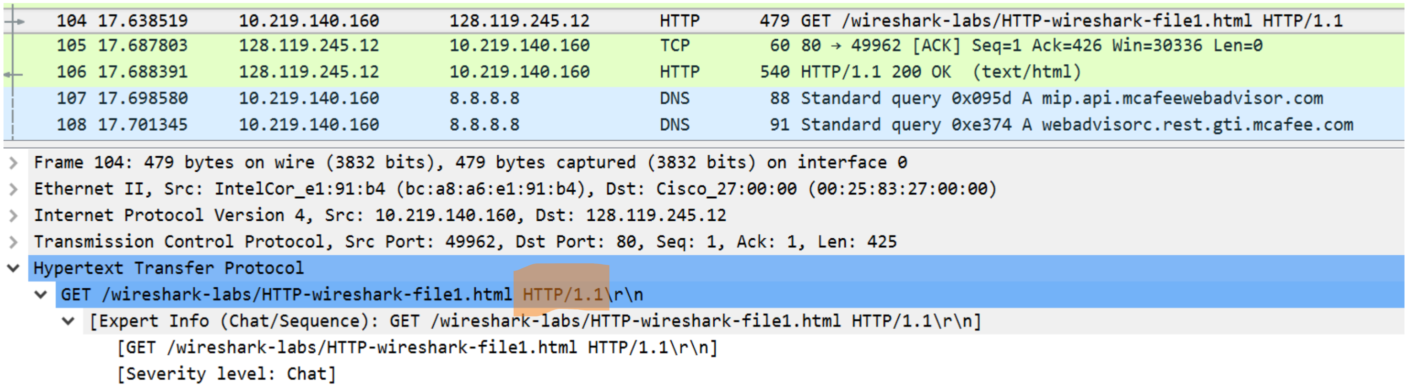
Name: Sagar Sharma
UTA ID: 1001626958

Note: Every answer is highlighted in the related snapshot with orange color.

The Basic HTTP GET/response interaction

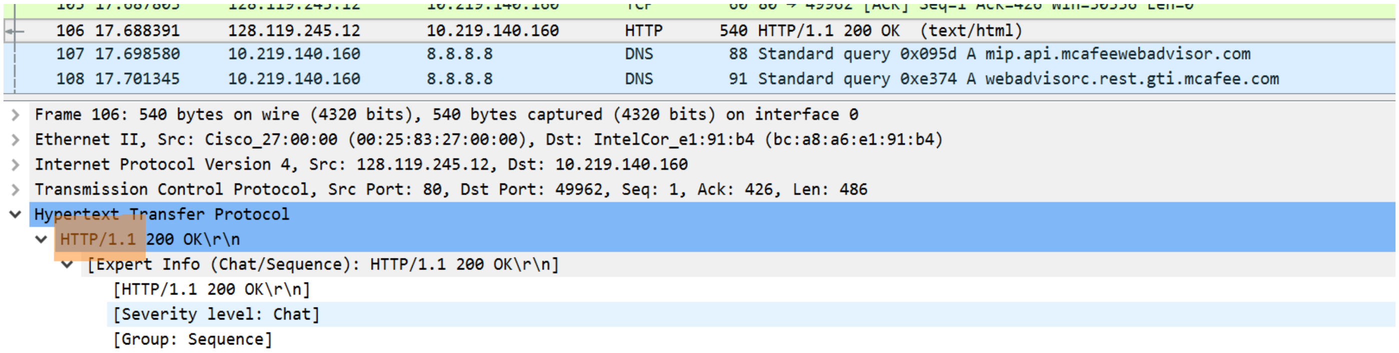
1. The server and the browser both are running **http version 1.1**
   The related snapshots are attached below:

   This snapshot is of *GET request from browser*



```
104 17.638519   10.219.140.160    128.119.245.12    HTTP    479 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
105 17.687803   128.119.245.12    10.219.140.160    TCP      60 80 → 49962 [ACK] Seq=1 Ack=426 Win=30336 Len=0
106 17.688391   128.119.245.12    10.219.140.160    HTTP    540 HTTP/1.1 200 OK  (text/html)
107 17.698580   10.219.140.160    8.8.8.8           DNS      88 Standard query 0x095d A mip.api.mcafeewebadvisor.com
108 17.701345   10.219.140.160    8.8.8.8           DNS      91 Standard query 0xe374 A webadvisorc.rest.gti.mcafee.com

> Frame 104: 479 bytes on wire (3832 bits), 479 bytes captured (3832 bits) on interface 0
> Ethernet II, Src: IntelCor_e1:91:b4 (bc:a8:a6:e1:91:b4), Dst: Cisco_27:00:00 (00:25:83:27:00:00)
> Internet Protocol Version 4, Src: 10.219.140.160, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 49962, Dst Port: 80, Seq: 1, Ack: 1, Len: 425
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]
```

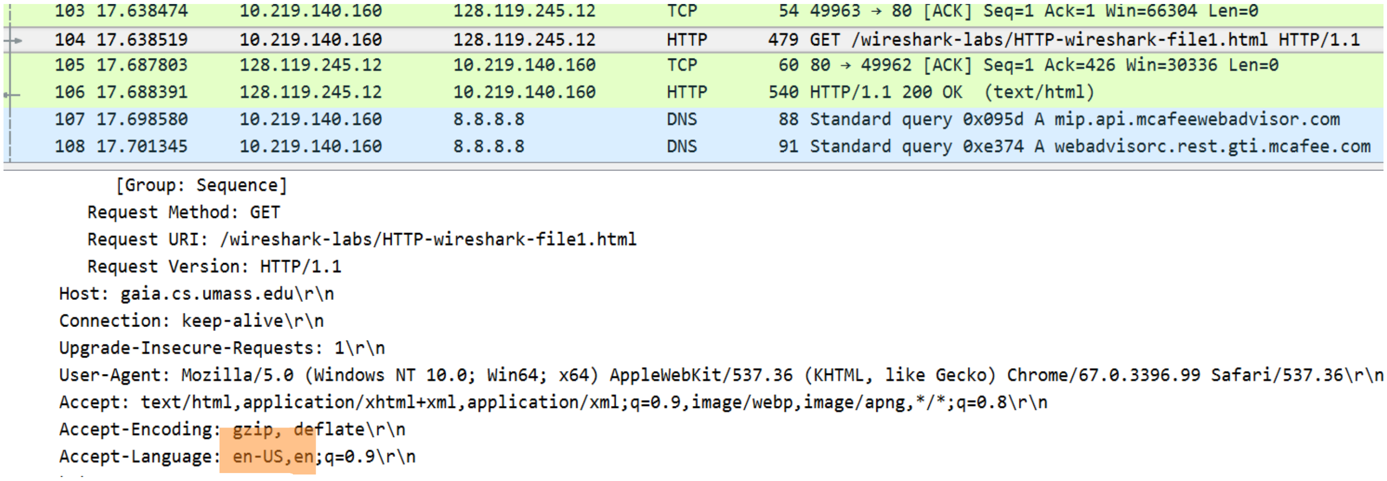
   This snapshot is *response msg from server*



```
105 17.687803   128.119.245.12    10.219.140.160    TCP      60 80 → 49962 [ACK] Seq=1 Ack=426 Win=30336 Len=0
106 17.688391   128.119.245.12    10.219.140.160    HTTP    540 HTTP/1.1 200 OK  (text/html)
107 17.698580   10.219.140.160    8.8.8.8           DNS      88 Standard query 0x095d A mip.api.mcafeewebadvisor.com
108 17.701345   10.219.140.160    8.8.8.8           DNS      91 Standard query 0xe374 A webadvisorc.rest.gti.mcafee.com

> Frame 106: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
> Ethernet II, Src: Cisco_27:00:00 (00:25:83:27:00:00), Dst: IntelCor_e1:91:b4 (bc:a8:a6:e1:91:b4)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.219.140.160
> Transmission Control Protocol, Src Port: 80, Dst Port: 49962, Seq: 1, Ack: 426, 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]
```

2. The browser can accept **US English**, **English** to the server.
   The related snapshots are attached below:

   This snapshot is the *request from browser and includes which language it can accept.*

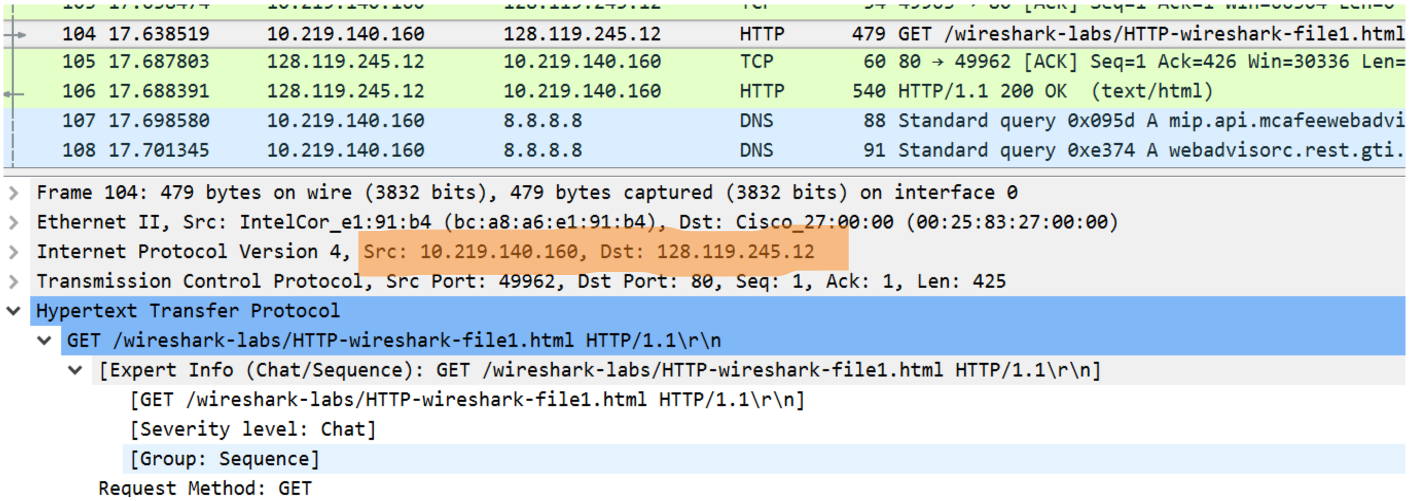


```
103 17.638474   10.219.140.160     128.119.245.12     TCP      54 49963 → 80 [ACK] Seq=1 Ack=1 Win=66304 Len=0
104 17.638519   10.219.140.160     128.119.245.12     HTTP    479 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
105 17.687803   128.119.245.12     10.219.140.160     TCP      60 80 → 49962 [ACK] Seq=1 Ack=426 Win=30336 Len=0
106 17.688391   128.119.245.12     10.219.140.160     HTTP    540 HTTP/1.1 200 OK  (text/html)
107 17.698580   10.219.140.160     8.8.8.8            DNS      88 Standard query 0x095d A mip.api.mcafeewebadvisor.com
108 17.701345   10.219.140.160     8.8.8.8            DNS      91 Standard query 0xe374 A webadvisorc.rest.gti.mcafee.com

        [Group: Sequence]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
   Host: gaia.cs.umass.edu\r\n
   Connection: keep-alive\r\n
   Upgrade-Insecure-Requests: 1\r\n
   User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36\r\n
   Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
   Accept-Encoding: gzip, deflate\r\n
   Accept-Language: en-US,en;q=0.9\r\n
```

3. The **IP address** of the **computer is 10.219.140.160**
   The **IP address** of the gaia.cs.umass.edu **server is 128.119.245.12**

   The related snapshots are attached below:

   Src is computer's IP address and dst is server's IP address

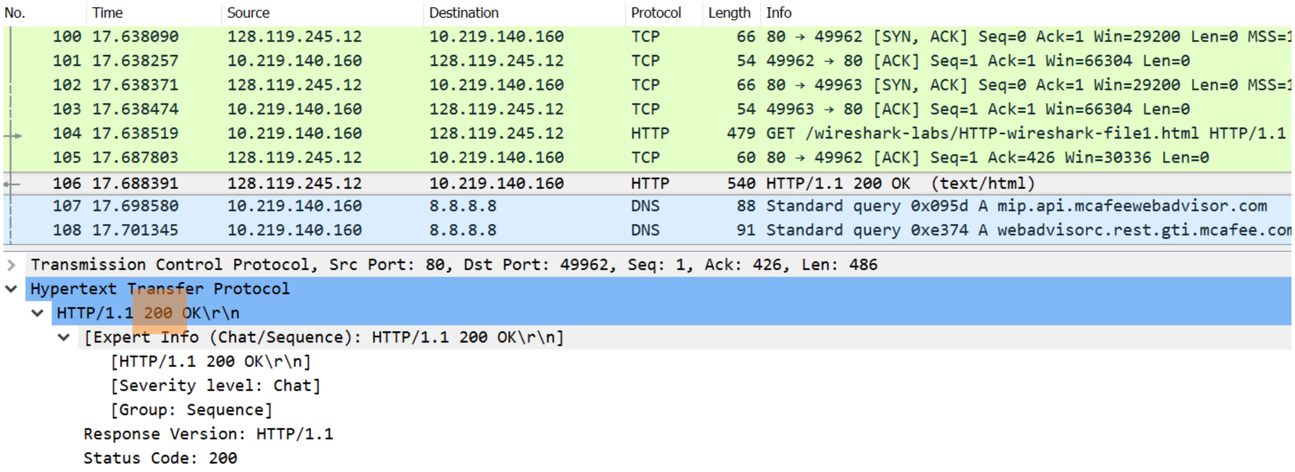


```
104 17.638519   10.219.140.160    128.119.245.12    HTTP    479 GET /wireshark-labs/HTTP-wireshark-file1.html
105 17.687803   128.119.245.12    10.219.140.160    TCP      60 80 → 49962 [ACK] Seq=1 Ack=426 Win=30336 Len=
106 17.688391   128.119.245.12    10.219.140.160    HTTP    540 HTTP/1.1 200 OK  (text/html)
107 17.698580   10.219.140.160    8.8.8.8           DNS      88 Standard query 0x095d A mip.api.mcafeewebadvi
108 17.701345   10.219.140.160    8.8.8.8           DNS      91 Standard query 0xe374 A webadvisorc.rest.gti.

> Frame 104: 479 bytes on wire (3832 bits), 479 bytes captured (3832 bits) on interface 0
> Ethernet II, Src: IntelCor_e1:91:b4 (bc:a8:a6:e1:91:b4), Dst: Cisco_27:00:00 (00:25:83:27:00:00)
> Internet Protocol Version 4, Src: 10.219.140.160, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 49962, Dst Port: 80, Seq: 1, Ack: 1, Len: 425
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
```

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

   The related snapshots are attached below:

   The status code is highlighted

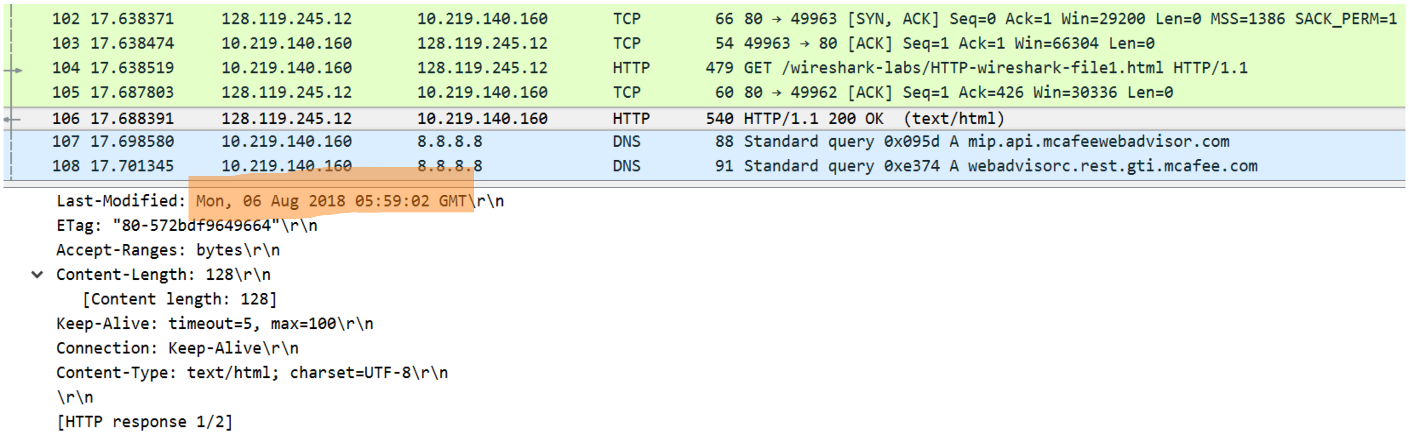


```
No.     Time        Source          Destination     Protocol  Length  Info
    100 17.638090   128.119.245.12  10.219.140.160  TCP         66 80 → 49962 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1
    101 17.638257   10.219.140.160  128.119.245.12  TCP         54 49962 → 80 [ACK] Seq=1 Ack=1 Win=66304 Len=0
    102 17.638371   128.119.245.12  10.219.140.160  TCP         66 80 → 49963 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1
    103 17.638474   10.219.140.160  128.119.245.12  TCP         54 49963 → 80 [ACK] Seq=1 Ack=1 Win=66304 Len=0
    104 17.638519   10.219.140.160  128.119.245.12  HTTP       479 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
    105 17.687803   128.119.245.12  10.219.140.160  TCP         60 80 → 49962 [ACK] Seq=1 Ack=426 Win=30336 Len=0
    106 17.688391   128.119.245.12  10.219.140.160  HTTP       540 HTTP/1.1 200 OK  (text/html)
    107 17.698580   10.219.140.160  8.8.8.8         DNS         88 Standard query 0x095d A mip.api.mcafeewebadvisor.com
    108 17.701345   10.219.140.160  8.8.8.8         DNS         91 Standard query 0xe374 A webadvisorc.rest.gti.mcafee.com

> Transmission Control Protocol, Src Port: 80, Dst Port: 49962, Seq: 1, Ack: 426, 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
```

5. The html file was last modified at **Mon, 06 Aug 2018 05:59:02 GMT** at the server.

   The related snapshots are attached below:

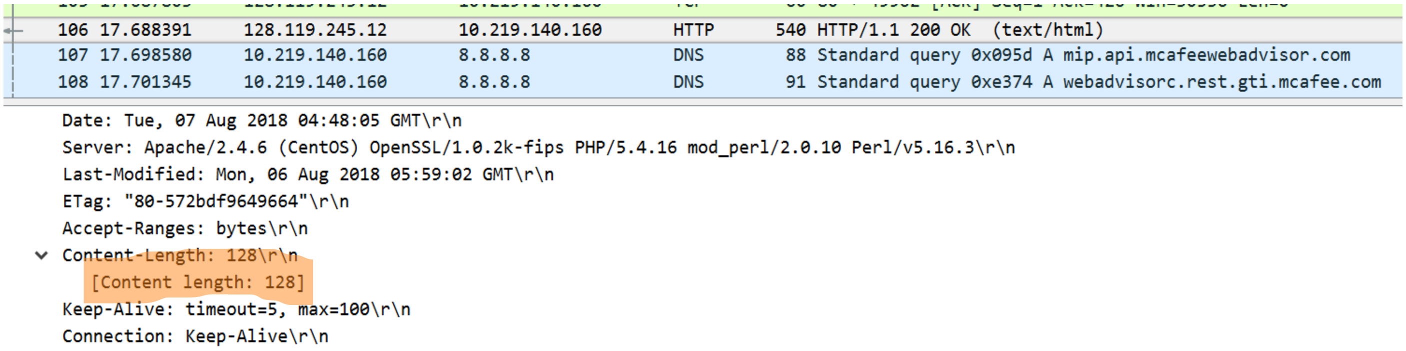
   Modified date is highlighted



```
    102 17.638371   128.119.245.12  10.219.140.160  TCP         66 80 → 49963 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1386 SACK_PERM=1
    103 17.638474   10.219.140.160  128.119.245.12  TCP         54 49963 → 80 [ACK] Seq=1 Ack=1 Win=66304 Len=0
    104 17.638519   10.219.140.160  128.119.245.12  HTTP       479 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
    105 17.687803   128.119.245.12  10.219.140.160  TCP         60 80 → 49962 [ACK] Seq=1 Ack=426 Win=30336 Len=0
    106 17.688391   128.119.245.12  10.219.140.160  HTTP       540 HTTP/1.1 200 OK  (text/html)
    107 17.698580   10.219.140.160  8.8.8.8         DNS         88 Standard query 0x095d A mip.api.mcafeewebadvisor.com
    108 17.701345   10.219.140.160  8.8.8.8         DNS         91 Standard query 0xe374 A webadvisorc.rest.gti.mcafee.com

    Last-Modified: Mon, 06 Aug 2018 05:59:02 GMT\r\n
    ETag: "80-572bdf9649664"\r\n
    Accept-Ranges: bytes\r\n
  v Content-Length: 128\r\n
      [Content length: 128]
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/2]
```

6. The content-length is **128 bytes**.
   The related snapshots are attached below:

Content-length is highlighted



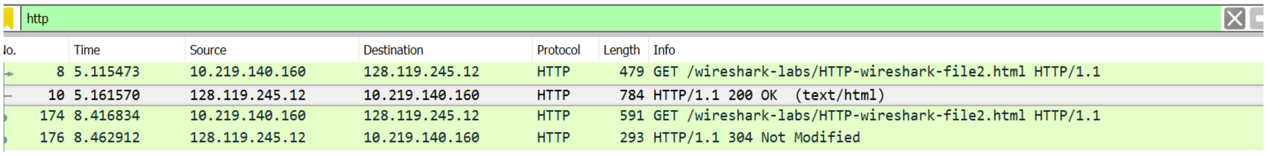
```
 106 17.688391   128.119.245.12   10.219.140.160   HTTP   540 HTTP/1.1 200 OK  (text/html)
 107 17.698580   10.219.140.160   8.8.8.8          DNS     88 Standard query 0x095d A mip.api.mcafeewebadvisor.com
 108 17.701345   10.219.140.160   8.8.8.8          DNS     91 Standard query 0xe374 A webadvisorc.rest.gti.mcafee.com

    Date: Tue, 07 Aug 2018 04:48:05 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: Mon, 06 Aug 2018 05:59:02 GMT\r\n
    ETag: "80-572bdf9649664"\r\n
    Accept-Ranges: bytes\r\n
  ⌄ Content-Length: 128\r\n
        [Content length: 128]
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
```

7. **No**, the raw data is exactly same for the header content of the packet content window as displayed in the packet listing window.

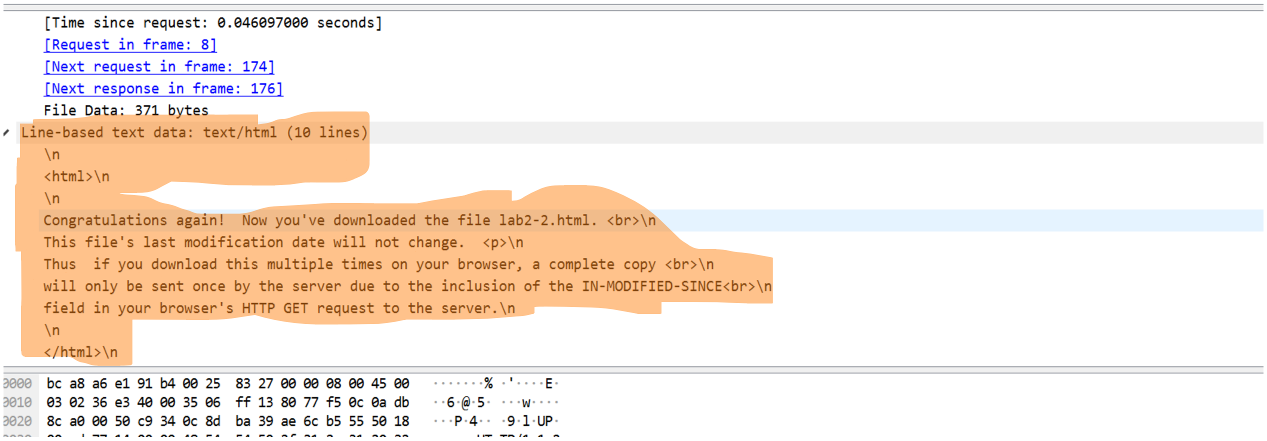
The HTTP CONDITIONAL GET/response interaction

8. **No**, there is no *if modified by* in the *first http get request*.

9. **Yes**, the server did return the contents of the file. The contents of the returned file are highlighted in the snapshot attached below:



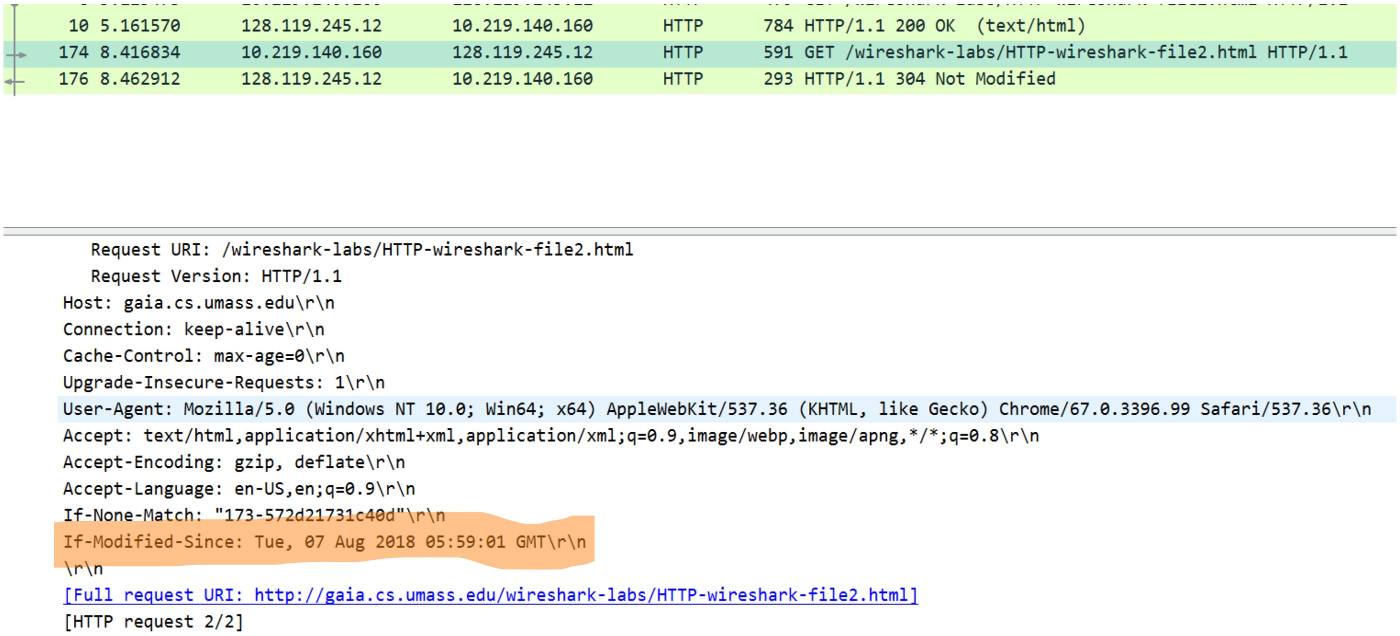
```
No.    Time       Source            Destination       Protocol  Length  Info
   8   5.115473   10.219.140.160    128.119.245.12    HTTP        479   GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  10   5.161570   128.119.245.12    10.219.140.160    HTTP        784   HTTP/1.1 200 OK  (text/html)
 174   8.416834   10.219.140.160    128.119.245.12    HTTP        591   GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 176   8.462912   128.119.245.12    10.219.140.160    HTTP        293   HTTP/1.1 304 Not Modified
```



```
    [Time since request: 0.046097000 seconds]
    [Request in frame: 8]
    [Next request in frame: 174]
    [Next response in frame: 176]
    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

0000  bc a8 a6 e1 91 b4 00 25  83 27 00 00 08 00 45 00   ·······% ·'····E·
0010  03 02 36 e3 40 00 35 06  ff 13 80 77 f5 0c 0a db   ··6·@·5· ···w····
0020  8c a0 00 50 c9 34 0c 8d  ba 39 ae 6c b5 55 50 18   ···P·4·· ·9·l·UP·
```

10. **Yes**, there is an IF MODIFIED SINCE header in the second Get http request. The contents are **Tue, 07 Aug 2018 05:59:01 GMT**

<u>The highlighted part shows if modified since header</u>.

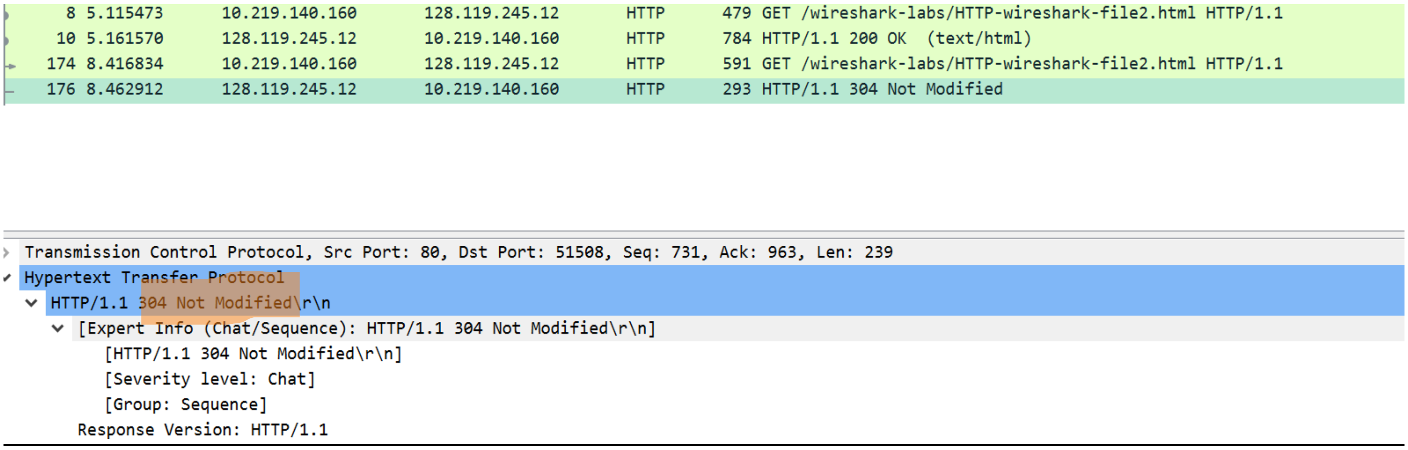


```
 10 5.161570   128.119.245.12   10.219.140.160   HTTP   784 HTTP/1.1 200 OK  (text/html)
174 8.416834   10.219.140.160   128.119.245.12   HTTP   591 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
176 8.462912   128.119.245.12   10.219.140.160   HTTP   293 HTTP/1.1 304 Not Modified
```

```
      Request URI: /wireshark-labs/HTTP-wireshark-file2.html
      Request Version: HTTP/1.1
   Host: gaia.cs.umass.edu\r\n
   Connection: keep-alive\r\n
   Cache-Control: max-age=0\r\n
   Upgrade-Insecure-Requests: 1\r\n
   User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36\r\n
   Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
   Accept-Encoding: gzip, deflate\r\n
   Accept-Language: en-US,en;q=0.9\r\n
   If-None-Match: "173-572d21731c40d"\r\n
   If-Modified-Since: Tue, 07 Aug 2018 05:59:01 GMT\r\n
   \r\n
   [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
   [HTTP request 2/2]
```

11. The status code and phrase returned by server is **304 Not Modified**. The file has not been modified, therefore the contents are **not resent by the server**.

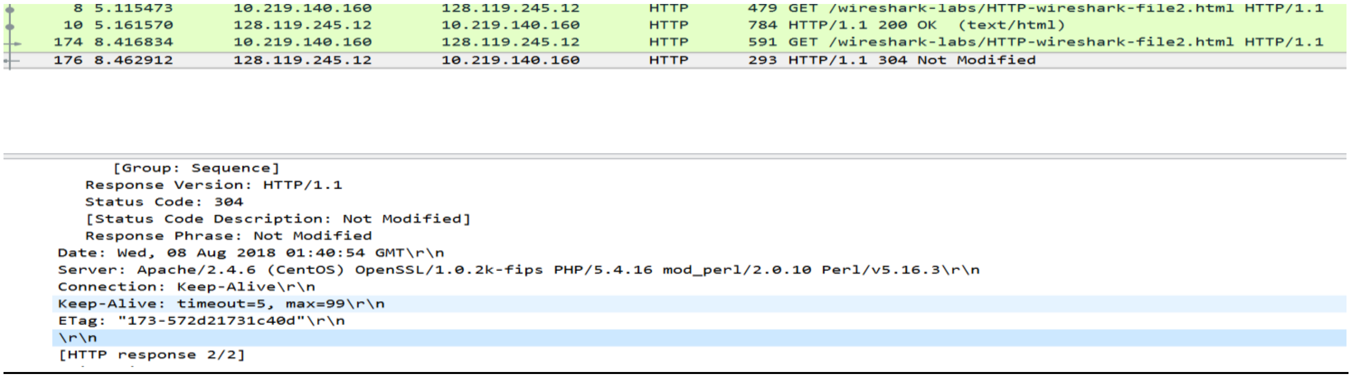
<u>The highlighted parts of the snapshot support the answer:</u>



```
  8 5.115473   10.219.140.160   128.119.245.12   HTTP   479 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 10 5.161570   128.119.245.12   10.219.140.160   HTTP   784 HTTP/1.1 200 OK  (text/html)
174 8.416834   10.219.140.160   128.119.245.12   HTTP   591 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
176 8.462912   128.119.245.12   10.219.140.160   HTTP   293 HTTP/1.1 304 Not Modified
```

```
> Transmission Control Protocol, Src Port: 80, Dst Port: 51508, Seq: 731, Ack: 963, Len: 239
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
```

<u>There is no file content after the E-tag header line and the http response header ends.</u>



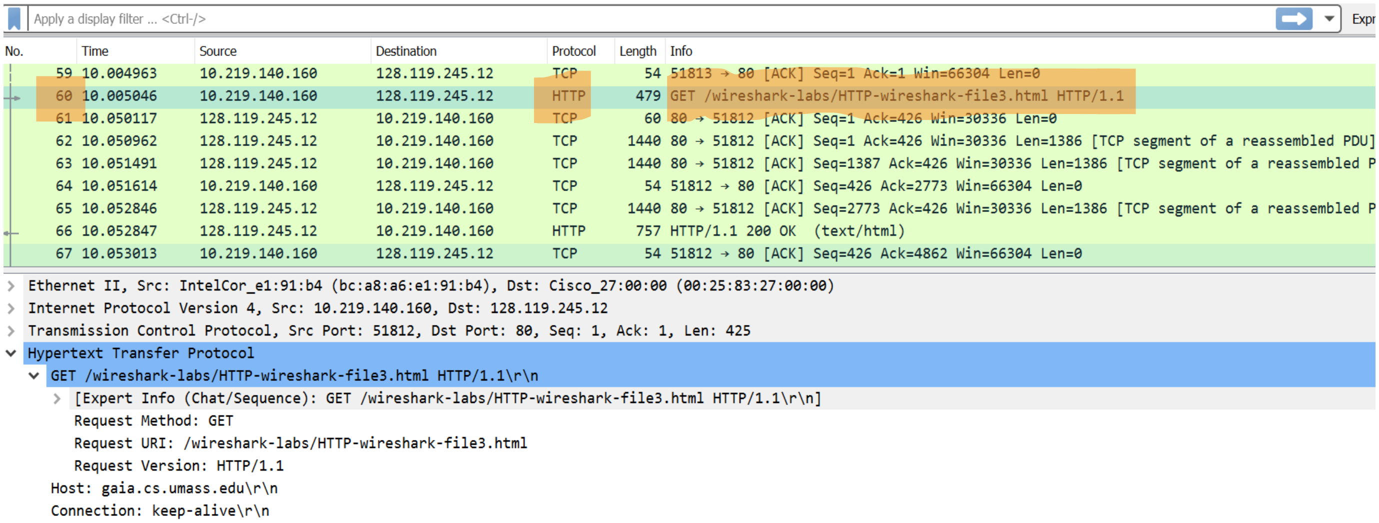
```
  8 5.115473   10.219.140.160   128.119.245.12   HTTP   479 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 10 5.161570   128.119.245.12   10.219.140.160   HTTP   784 HTTP/1.1 200 OK  (text/html)
174 8.416834   10.219.140.160   128.119.245.12   HTTP   591 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
176 8.462912   128.119.245.12   10.219.140.160   HTTP   293 HTTP/1.1 304 Not Modified
```

```
        [Group: Sequence]
     Response Version: HTTP/1.1
     Status Code: 304
     [Status Code Description: Not Modified]
     Response Phrase: Not Modified
  Date: Wed, 08 Aug 2018 01:40:54 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=99\r\n
  ETag: "173-572d21731c40d"\r\n
  \r\n
  [HTTP response 2/2]
```

Retrieving Long Documents

12. The browser sent **only one** *get http request*. **Packet 60** contains the *get message for the Bill of Rights*.

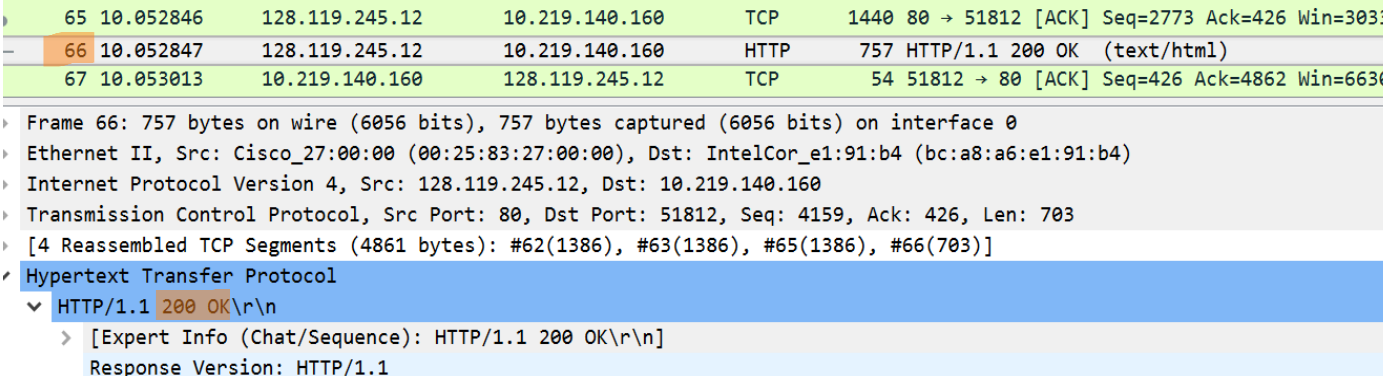
    The snapshot supports the answer:



```
No.  Time       Source          Destination     Protocol Length Info
59   10.004963  10.219.140.160  128.119.245.12  TCP        54  51813 → 80 [ACK] Seq=1 Ack=1 Win=66304 Len=0
60   10.005046  10.219.140.160  128.119.245.12  HTTP      479  GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
61   10.050117  128.119.245.12  10.219.140.160  TCP        60  80 → 51812 [ACK] Seq=1 Ack=426 Win=30336 Len=0
62   10.050962  128.119.245.12  10.219.140.160  TCP      1440  80 → 51812 [ACK] Seq=1 Ack=426 Win=30336 Len=1386 [TCP segment of a reassembled PDU]
63   10.051491  128.119.245.12  10.219.140.160  TCP      1440  80 → 51812 [ACK] Seq=1387 Ack=426 Win=30336 Len=1386 [TCP segment of a reassembled P
64   10.051614  10.219.140.160  128.119.245.12  TCP        54  51812 → 80 [ACK] Seq=426 Ack=2773 Win=66304 Len=0
65   10.052846  128.119.245.12  10.219.140.160  TCP      1440  80 → 51812 [ACK] Seq=2773 Ack=426 Win=30336 Len=1386 [TCP segment of a reassembled P
66   10.052847  128.119.245.12  10.219.140.160  HTTP      757  HTTP/1.1 200 OK  (text/html)
67   10.053013  10.219.140.160  128.119.245.12  TCP        54  51812 → 80 [ACK] Seq=426 Ack=4862 Win=66304 Len=0

> Ethernet II, Src: IntelCor_e1:91:b4 (bc:a8:a6:e1:91:b4), Dst: Cisco_27:00:00 (00:25:83:27:00:00)
> Internet Protocol Version 4, Src: 10.219.140.160, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 51812, Dst Port: 80, Seq: 1, Ack: 1, Len: 425
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file3.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
```

13. **Packet 66** contains the status code and phrase associated with the http get request.

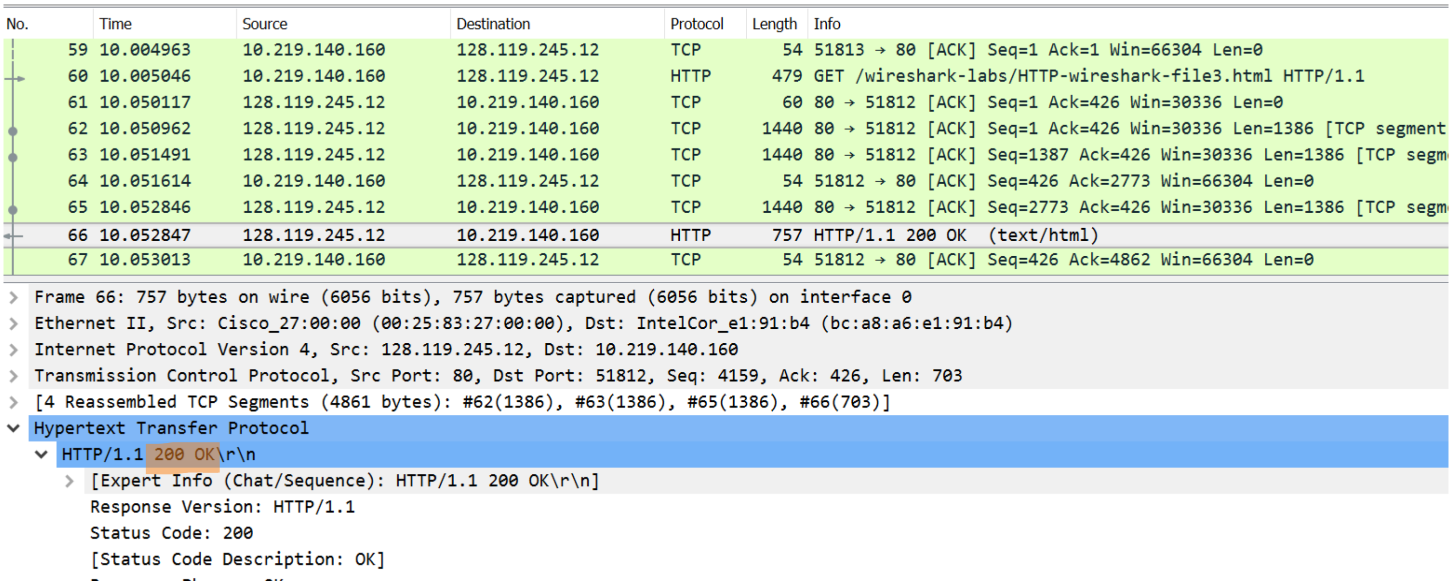
    The snapshot shows the **header lines** of packet 66 which uses HTTP response, *has the status code and phrase associated with get http request sent by the browser*.



```
65 10.052846  128.119.245.12  10.219.140.160  TCP   1440 80 → 51812 [ACK] Seq=2773 Ack=426 Win=303
66 10.052847  128.119.245.12  10.219.140.160  HTTP   757 HTTP/1.1 200 OK  (text/html)
67 10.053013  10.219.140.160  128.119.245.12  TCP     54 51812 → 80 [ACK] Seq=426 Ack=4862 Win=663

> Frame 66: 757 bytes on wire (6056 bits), 757 bytes captured (6056 bits) on interface 0
> Ethernet II, Src: Cisco_27:00:00 (00:25:83:27:00:00), Dst: IntelCor_e1:91:b4 (bc:a8:a6:e1:91:b4)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.219.140.160
> Transmission Control Protocol, Src Port: 80, Dst Port: 51812, Seq: 4159, Ack: 426, Len: 703
> [4 Reassembled TCP Segments (4861 bytes): #62(1386), #63(1386), #65(1386), #66(703)]
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
```

14. Status code and phrase: **200 OK**

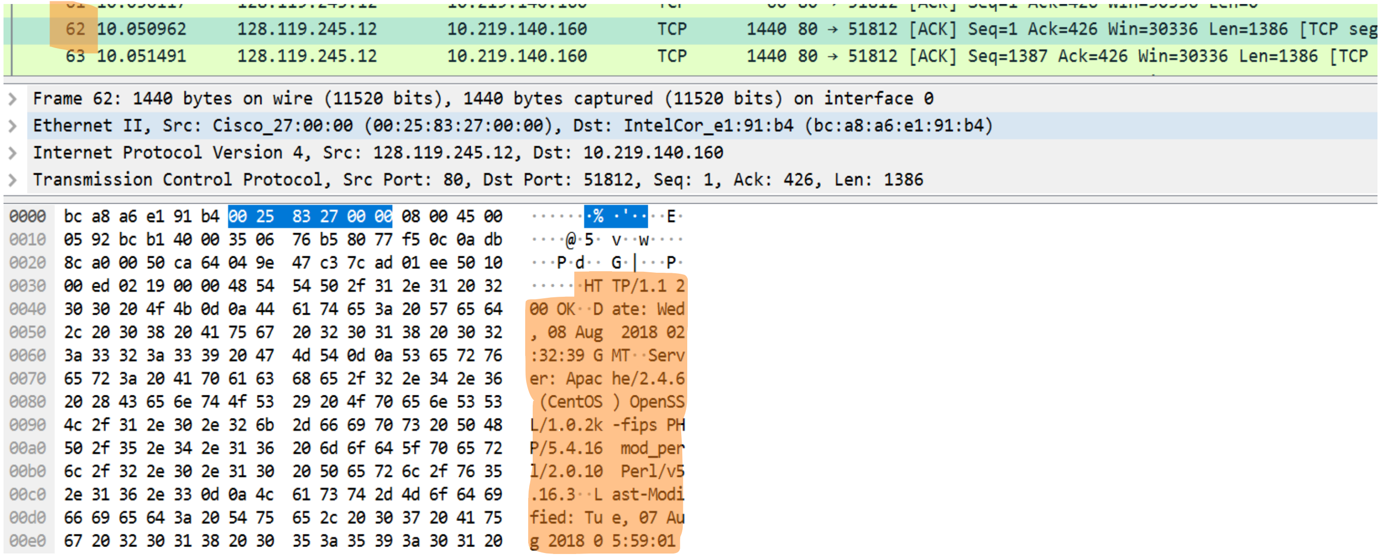
The status code and phrase are highlighted



```
No.  Time       Source          Destination     Protocol Length Info
  59 10.004963  10.219.140.160  128.119.245.12  TCP        54 51813 → 80 [ACK] Seq=1 Ack=1 Win=66304 Len=0
  60 10.005046  10.219.140.160  128.119.245.12  HTTP      479 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  61 10.050117  128.119.245.12  10.219.140.160  TCP        60 80 → 51812 [ACK] Seq=1 Ack=426 Win=30336 Len=0
  62 10.050962  128.119.245.12  10.219.140.160  TCP      1440 80 → 51812 [ACK] Seq=1 Ack=426 Win=30336 Len=1386 [TCP segment
  63 10.051491  128.119.245.12  10.219.140.160  TCP      1440 80 → 51812 [ACK] Seq=1387 Ack=426 Win=30336 Len=1386 [TCP segm
  64 10.051614  10.219.140.160  128.119.245.12  TCP        54 51812 → 80 [ACK] Seq=426 Ack=2773 Win=66304 Len=0
  65 10.052846  128.119.245.12  10.219.140.160  TCP      1440 80 → 51812 [ACK] Seq=2773 Ack=426 Win=30336 Len=1386 [TCP segm
  66 10.052847  128.119.245.12  10.219.140.160  HTTP      757 HTTP/1.1 200 OK  (text/html)
  67 10.053013  10.219.140.160  128.119.245.12  TCP        54 51812 → 80 [ACK] Seq=426 Ack=4862 Win=66304 Len=0

> Frame 66: 757 bytes on wire (6056 bits), 757 bytes captured (6056 bits) on interface 0
> Ethernet II, Src: Cisco_27:00:00 (00:25:83:27:00:00), Dst: IntelCor_e1:91:b4 (bc:a8:a6:e1:91:b4)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.219.140.160
> Transmission Control Protocol, Src Port: 80, Dst Port: 51812, Seq: 4159, Ack: 426, Len: 703
> [4 Reassembled TCP Segments (4861 bytes): #62(1386), #63(1386), #65(1386), #66(703)]
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]
```

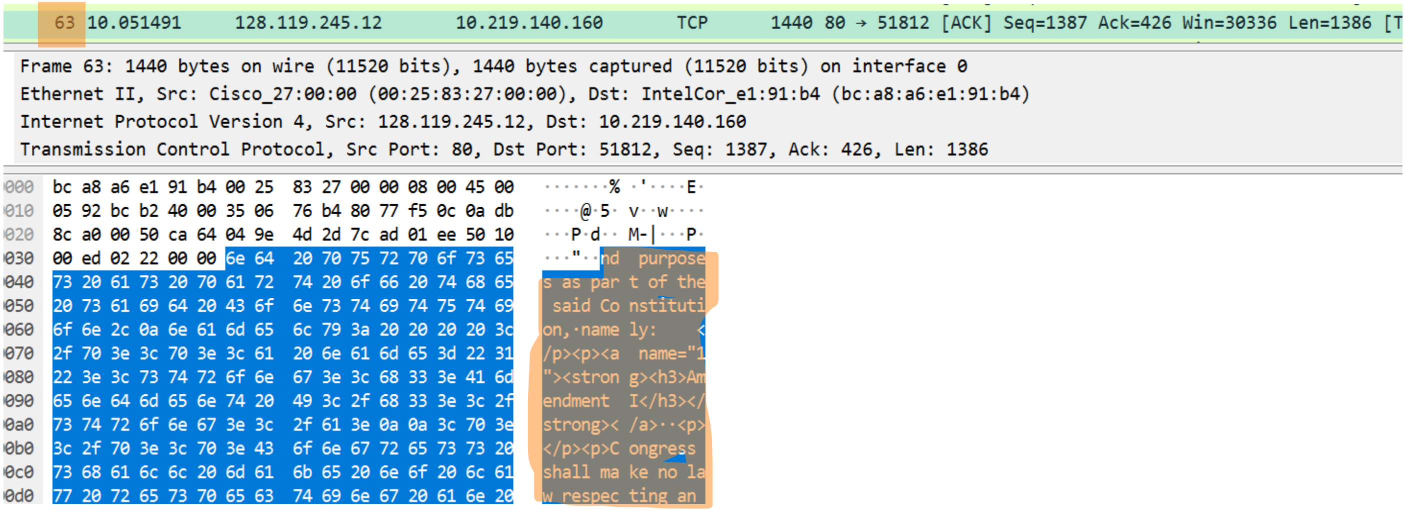
15. **Packet 62,63 and 65** were required to carry the response. *The ASCII contents of the packets are shown below in snapshots carrying the response of the get request*.

Packet 62 with ASCII contents



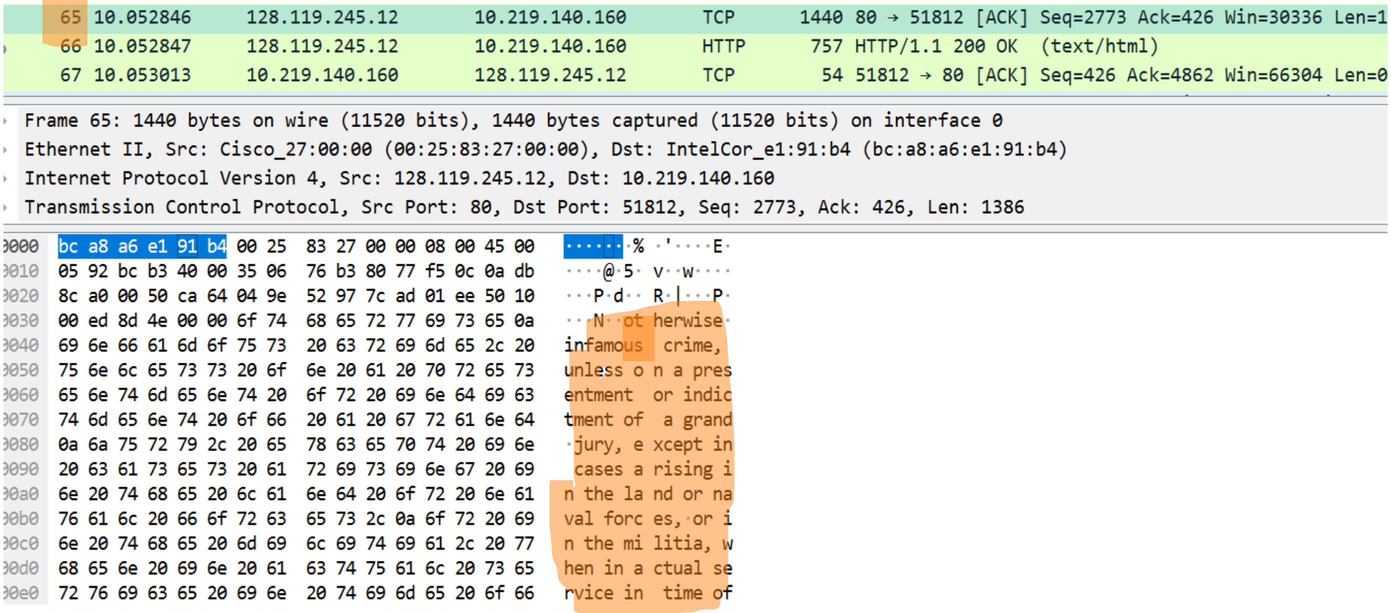
```
  61 10.050117  128.119.245.12  10.219.140.160  TCP   60 80 → 51812 [ACK] Seq=1 Ack=426 Win=30336 Len=0
  62 10.050962  128.119.245.12  10.219.140.160  TCP 1440 80 → 51812 [ACK] Seq=1 Ack=426 Win=30336 Len=1386 [TCP seg
  63 10.051491  128.119.245.12  10.219.140.160  TCP 1440 80 → 51812 [ACK] Seq=1387 Ack=426 Win=30336 Len=1386 [TCP

> Frame 62: 1440 bytes on wire (11520 bits), 1440 bytes captured (11520 bits) on interface 0
> Ethernet II, Src: Cisco_27:00:00 (00:25:83:27:00:00), Dst: IntelCor_e1:91:b4 (bc:a8:a6:e1:91:b4)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.219.140.160
> Transmission Control Protocol, Src Port: 80, Dst Port: 51812, Seq: 1, Ack: 426, Len: 1386

0000  bc a8 a6 e1 91 b4 00 25  83 27 00 00 08 00 45 00   ······%  ·'····E·
0010  05 92 bc b1 40 00 35 06  76 b5 80 77 f5 0c 0a db   ····@·5·  v··w····
0020  8c a0 00 50 ca 64 04 9e  47 c3 7c ad 01 ee 50 10   ···P·d··  G·|···P·
0030  00 ed 02 19 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 57 65 64   00 OK··D  ate: Wed
0050  2c 20 30 38 20 41 75 67  20 32 30 31 38 20 30 32   , 08 Aug   2018 02
0060  3a 33 32 3a 33 39 20 47  4d 54 0d 0a 53 65 72 76   :32:39 G  MT··Serv
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34 2e 36   er: Apac  he/2.4.6
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70 65 6e 53 53    (CentOS  ) OpenSS
0090  4c 2f 31 2e 30 2e 32 6b  2d 66 69 70 73 20 50 48   L/1.0.2k  -fips PH
00a0  50 2f 35 2e 34 2e 31 36  20 6d 6f 64 5f 70 65 72   P/5.4.16   mod_per
00b0  6c 2f 32 2e 30 2e 31 30  20 50 65 72 6c 2f 76 35   l/2.0.10   Perl/v5
00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d 4d 6f 64 69   .16.3··L  ast-Modi
00d0  66 69 65 64 3a 20 54 75  65 2c 20 30 37 20 41 75   fied: Tu  e, 07 Au
00e0  67 20 32 30 31 38 20 30  35 3a 35 39 3a 30 31 20   g 2018 0  5:59:01
```

Packet 63 with ASCII contents



```
63 10.051491    128.119.245.12    10.219.140.160    TCP    1440 80 → 51812 [ACK] Seq=1387 Ack=426 Win=30336 Len=1386 [T

Frame 63: 1440 bytes on wire (11520 bits), 1440 bytes captured (11520 bits) on interface 0
Ethernet II, Src: Cisco_27:00:00 (00:25:83:27:00:00), Dst: IntelCor_e1:91:b4 (bc:a8:a6:e1:91:b4)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.219.140.160
Transmission Control Protocol, Src Port: 80, Dst Port: 51812, Seq: 1387, Ack: 426, Len: 1386

0000  bc a8 a6 e1 91 b4 00 25  83 27 00 00 08 00 45 00   ·······% ·'····E·
0010  05 92 bc b2 40 00 35 06  76 b4 80 77 f5 0c 0a db   ····@·5· v··w····
0020  8c a0 00 50 ca 64 04 9e  4d 2d 7c ad 01 ee 50 10   ···P·d·· M-|···P·
0030  00 ed 02 22 00 00 6e 64  20 70 75 72 70 6f 73 65   ···"··nd  purpose
0040  73 20 61 73 20 70 61 72  74 20 6f 66 20 74 68 65   s as par t of the
0050  20 73 61 69 64 20 43 6f  6e 73 74 69 74 75 74 69    said Co nstituti
0060  6f 6e 2c 0a 6e 61 6d 65  6c 79 3a 20 20 20 20 3c   on,·name ly:    <
0070  2f 70 3e 3c 70 3e 3c 61  20 6e 61 6d 65 3d 22 31   /p><p><a  name="1
0080  22 3e 3c 73 74 72 6f 6e  67 3e 3c 68 33 3e 41 6d   "><stron g><h3>Am
0090  65 6e 64 6d 65 6e 74 20  49 3c 2f 68 33 3e 3c 2f   endment  I</h3></
00a0  73 74 72 6f 6e 67 3e 3c  2f 61 3e 0a 0a 3c 70 3e   strong>< /a>··<p>
00b0  3c 2f 70 3e 3c 70 3e 43  6f 6e 67 72 65 73 73 20   </p><p>C ongress 
00c0  73 68 61 6c 6c 20 6d 61  6b 65 20 6e 6f 20 6c 61   shall ma ke no la
00d0  77 20 72 65 73 70 65 63  74 69 6e 67 20 61 6e 20   w respec ting an 
```

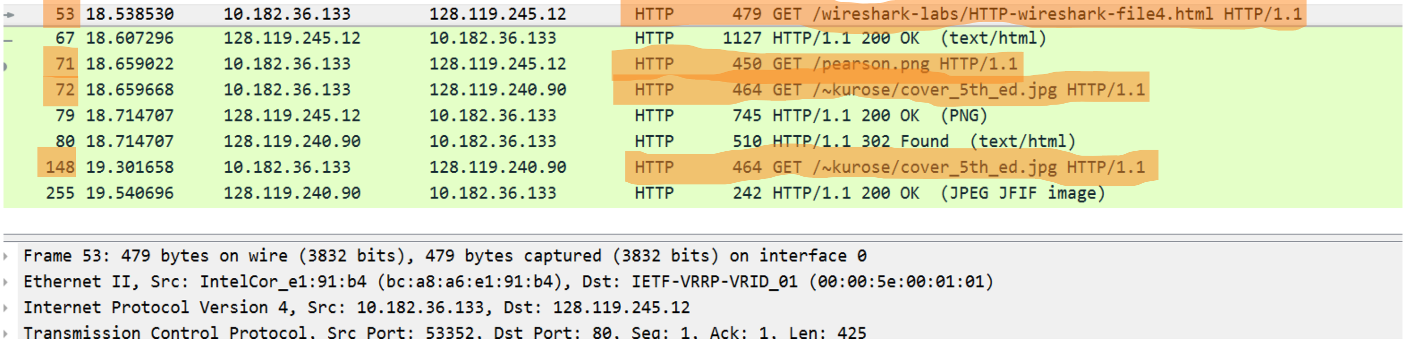
Packet 65 with ASCII contents



```
65 10.052846    128.119.245.12    10.219.140.160    TCP     1440 80 → 51812 [ACK] Seq=2773 Ack=426 Win=30336 Len=1
66 10.052847    128.119.245.12    10.219.140.160    HTTP     757 HTTP/1.1 200 OK  (text/html)
67 10.053013    10.219.140.160    128.119.245.12    TCP       54 51812 → 80 [ACK] Seq=426 Ack=4862 Win=66304 Len=0

Frame 65: 1440 bytes on wire (11520 bits), 1440 bytes captured (11520 bits) on interface 0
Ethernet II, Src: Cisco_27:00:00 (00:25:83:27:00:00), Dst: IntelCor_e1:91:b4 (bc:a8:a6:e1:91:b4)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.219.140.160
Transmission Control Protocol, Src Port: 80, Dst Port: 51812, Seq: 2773, Ack: 426, Len: 1386

0000  bc a8 a6 e1 91 b4 00 25  83 27 00 00 08 00 45 00   ······% ·'····E·
0010  05 92 bc b3 40 00 35 06  76 b3 80 77 f5 0c 0a db   ····@·5· v··w····
0020  8c a0 00 50 ca 64 04 9e  52 97 7c ad 01 ee 50 10   ···P·d·· R·|···P·
0030  00 ed 8d 4e 00 00 6f 74  68 65 72 77 69 73 65 0a   ···N··ot herwise·
0040  69 6e 66 61 6d 6f 75 73  20 63 72 69 6d 65 2c 20   infamous  crime, 
0050  75 6e 6c 65 73 73 20 6f  6e 20 61 20 70 72 65 73   unless o n a pres
0060  65 6e 74 6d 65 6e 74 20  6f 72 20 69 6e 64 69 63   entment  or indic
0070  74 6d 65 6e 74 20 6f 66  20 61 20 67 72 61 6e 64   tment of  a grand
0080  0a 6a 75 72 79 2c 20 65  78 63 65 70 74 20 69 6e   ·jury, e xcept in
0090  20 63 61 73 65 73 20 61  72 69 73 69 6e 67 20 69    cases a rising i
00a0  6e 20 74 68 65 20 6c 61  6e 64 20 6f 72 20 6e 61   n the la nd or na
00b0  76 61 6c 20 66 6f 72 63  65 73 2c 0a 6f 72 20 69   val forc es,·or i
00c0  6e 20 74 68 65 20 6d 69  6c 69 74 69 61 2c 20 77   n the mi litia, w
00d0  68 65 6e 20 69 6e 20 61  63 74 75 61 6c 20 73 65   hen in a ctual se
00e0  72 76 69 63 65 20 69 6e  20 74 69 6d 65 20 6f 66   rvice in  time of
```

16. The browser sent **4 http Get request messages**. **Packet 53** to get the *base html file*. **Packet 71** to get the *Pearson logo*. **Packet 72 and Packet 148** to get the *fifth edition textbook image*.
Packet 53 was sent to **128.119.245.12**
Packet 71 was sent to **128.119.245.12**
Packet 72 and Packet 148 was sent to **128.119.240.90**

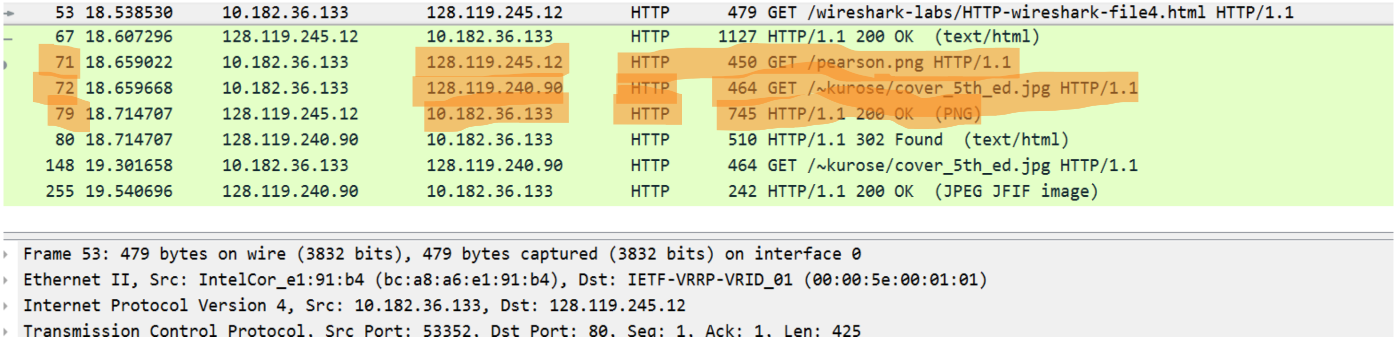
All the get packets are highlighted. Packet 99 and packet 137 will be considered as same get request for the same file.



```
 53 18.538530    10.182.36.133     128.119.245.12    HTTP    479 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
 67 18.607296    128.119.245.12    10.182.36.133     HTTP   1127 HTTP/1.1 200 OK  (text/html)
 71 18.659022    10.182.36.133     128.119.245.12    HTTP    450 GET /pearson.png HTTP/1.1
 72 18.659668    10.182.36.133     128.119.240.90    HTTP    464 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
 79 18.714707    128.119.245.12    10.182.36.133     HTTP    745 HTTP/1.1 200 OK  (PNG)
 80 18.714707    128.119.240.90    10.182.36.133     HTTP    510 HTTP/1.1 302 Found  (text/html)
148 19.301658    10.182.36.133     128.119.240.90    HTTP    464 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
255 19.540696    128.119.240.90    10.182.36.133     HTTP    242 HTTP/1.1 200 OK  (JPEG JFIF image)

Frame 53: 479 bytes on wire (3832 bits), 479 bytes captured (3832 bits) on interface 0
Ethernet II, Src: IntelCor_e1:91:b4 (bc:a8:a6:e1:91:b4), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
Internet Protocol Version 4, Src: 10.182.36.133, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 53352, Dst Port: 80, Seq: 1, Ack: 1, Len: 425
```

17. The images were downloaded **parallelly** by the browser. Since the get request for Pearson logo was sent in packet 71 and the get request for fifth edition textbook image was sent in packet 72. Then, the response 200 OK for Pearson logo was received in packet 79. Therefore, the images were downloaded parallelly.

The associated packets are highlighted below:



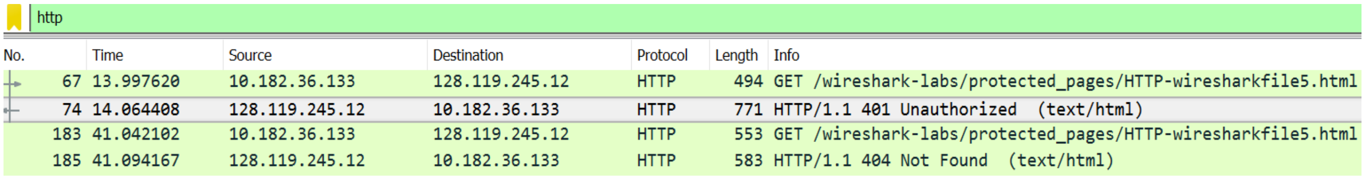
```
 53 18.538530   10.182.36.133    128.119.245.12   HTTP    479 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
 67 18.607296   128.119.245.12   10.182.36.133    HTTP   1127 HTTP/1.1 200 OK  (text/html)
 71 18.659022   10.182.36.133    128.119.245.12   HTTP    450 GET /pearson.png HTTP/1.1
 72 18.659668   10.182.36.133    128.119.240.90   HTTP    464 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
 79 18.714707   128.119.245.12   10.182.36.133    HTTP    745 HTTP/1.1 200 OK  (PNG)
 80 18.714707   128.119.240.90   10.182.36.133    HTTP    510 HTTP/1.1 302 Found  (text/html)
148 19.301658   10.182.36.133    128.119.240.90   HTTP    464 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
255 19.540696   128.119.240.90   10.182.36.133    HTTP    242 HTTP/1.1 200 OK  (JPEG JFIF image)
```

```
Frame 53: 479 bytes on wire (3832 bits), 479 bytes captured (3832 bits) on interface 0
Ethernet II, Src: IntelCor_e1:91:b4 (bc:a8:a6:e1:91:b4), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
Internet Protocol Version 4, Src: 10.182.36.133, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 53352, Dst Port: 80, Seq: 1, Ack: 1, Len: 425
```

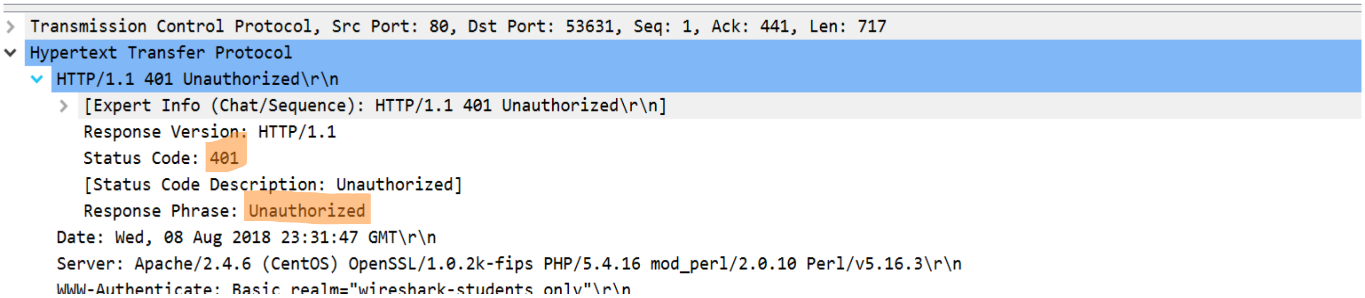
HTTP AUTHENTICATION

18. The *status code and response phrase* from the server for the response message for the initial get request are **401** and **Unauthorized**.

The status code and response message are highlighted below:



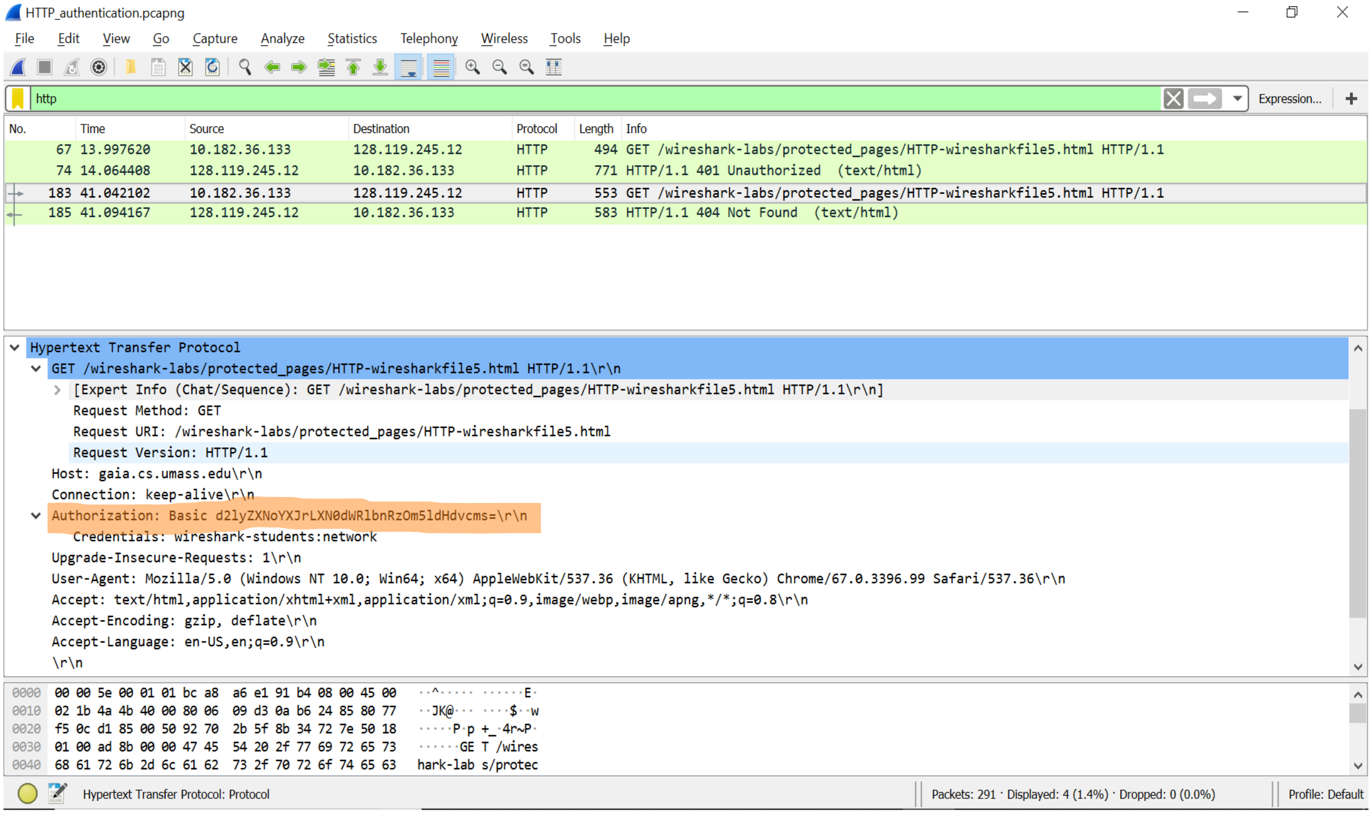
```
http

No.  Time        Source          Destination     Protocol Length Info
 67  13.997620   10.182.36.133   128.119.245.12  HTTP     494 GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html
 74  14.064408   128.119.245.12  10.182.36.133   HTTP     771 HTTP/1.1 401 Unauthorized  (text/html)
183  41.042102   10.182.36.133   128.119.245.12  HTTP     553 GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html
185  41.094167   128.119.245.12  10.182.36.133   HTTP     583 HTTP/1.1 404 Not Found  (text/html)
```



```
> Transmission Control Protocol, Src Port: 80, Dst Port: 53631, Seq: 1, Ack: 441, 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: Wed, 08 Aug 2018 23:31:47 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
```

19. The new field included in the second http Get request is **Authorization: Basic**

The associated line is highlighted:


HTTP_authentication.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression…
+

```
No.   Time        Source          Destination     Protocol  Length  Info
   67 13.997620   10.182.36.133   128.119.245.12  HTTP       494 GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
   74 14.064408   128.119.245.12  10.182.36.133   HTTP       771 HTTP/1.1 401 Unauthorized  (text/html)
  183 41.042102   10.182.36.133   128.119.245.12  HTTP       553 GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
  185 41.094167   128.119.245.12  10.182.36.133   HTTP       583 HTTP/1.1 404 Not Found  (text/html)
```

```
Hypertext Transfer Protocol
  GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html
    Request Version: HTTP/1.1
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    Credentials: wireshark-students:network
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9\r\n
  \r\n
```

```
0000  00 00 5e 00 01 01 bc a8  a6 e1 91 b4 08 00 45 00   ··^····· ······E·
0010  02 1b 4a 4b 40 00 80 06  09 d3 0a b6 24 85 80 77   ··JK@··· ····$··w
0020  f5 0c d1 85 00 50 92 70  2b 5f 8b 34 72 7e 50 18   ·····P·p +_·4r~P·
0030  01 00 ad 8b 00 00 47 45  54 20 2f 77 69 72 65 73   ······GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 70 72 6f 74 65 63   hark-lab s/protec
```

Hypertext Transfer Protocol: Protocol

Packets: 291 · Displayed: 4 (1.4%) · Dropped: 0 (0.0%)

Profile: Default