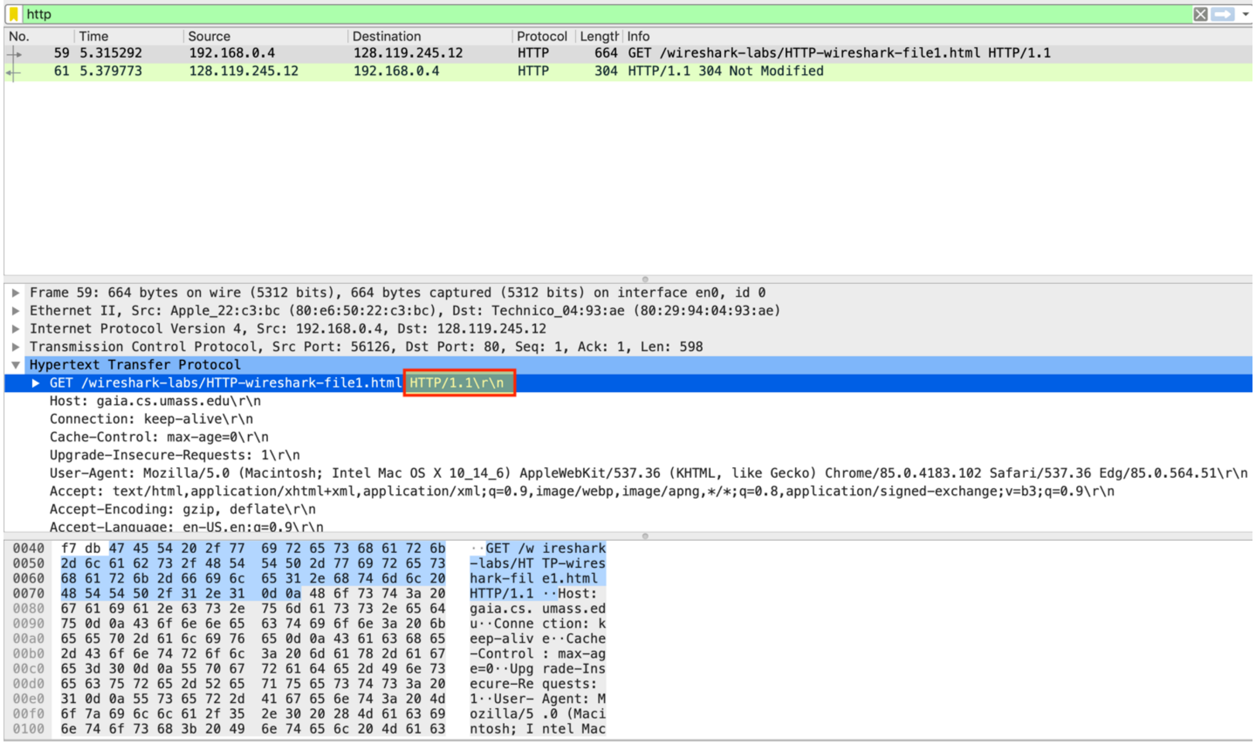
Dorian Benitez
drb160130

CS 4390.001
September 11, 2020

Wireshark Lab: HTTP

PART 1: The Basic HTTP GET/response interaction

1. The browser is running HTTP version 1.1.

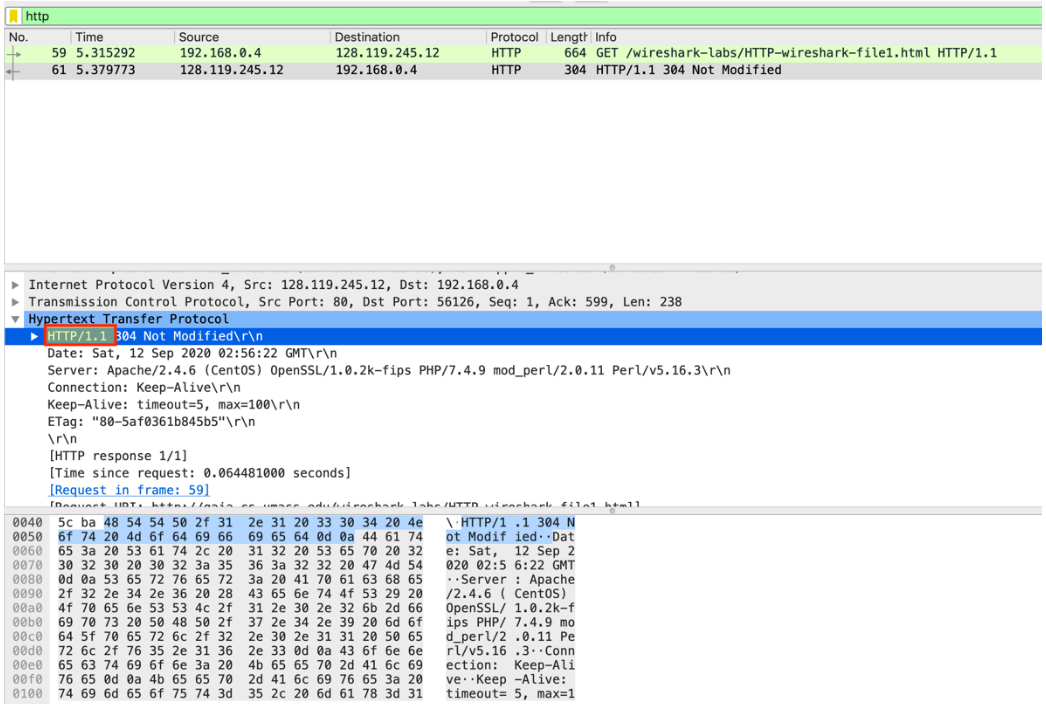


```
http
No.   Time       Source          Destination     Protocol Length Info
  59  5.315292   192.168.0.4     128.119.245.12  HTTP      664  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  61  5.379773   128.119.245.12  192.168.0.4     HTTP      304  HTTP/1.1 304 Not Modified

▶ Frame 59: 664 bytes on wire (5312 bits), 664 bytes captured (5312 bits) on interface en0, id 0
▶ Ethernet II, Src: Apple_22:c3:bc (80:e6:50:22:c3:bc), Dst: Technico_04:93:ae (80:29:94:04:93:ae)
▶ Internet Protocol Version 4, Src: 192.168.0.4, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 56126, Dst Port: 80, Seq: 1, Ack: 1, Len: 598
▼ Hypertext Transfer Protocol
  ▶ GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.102 Safari/537.36 Edg/85.0.564.51\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;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n

0040  f7 db 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   ··GET /w ireshark
0050  2d 6c 61 62 73 2f 48 54  54 50 2d 77 69 72 65 73   -labs/HT TP-wires
0060  68 61 72 6b 2d 66 69 6c  65 31 2e 68 74 6d 6c 20   hark-fil e1.html 
0070  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.1 ··Host: 
0080  67 61 69 61 2e 63 73 2e  75 6d 61 73 73 2e 65 64   gaia.cs. umass.ed
0090  75 0d 0a 43 6f 6e 6e 65  63 74 69 6f 6e 3a 20 6b   u··Conne ction: k
00a0  65 65 70 2d 61 6c 69 76  65 0d 0a 43 61 63 68 65   eep-aliv e··Cache
00b0  2d 43 6f 6e 74 72 6f 6c  3a 20 6d 61 78 2d 61 67   -Control : max-ag
00c0  65 3d 30 0d 0a 55 70 67  72 61 64 65 2d 49 6e 73   e=0··Upg rade-Ins
00d0  65 63 75 72 65 2d 52 65  71 75 65 73 74 73 3a 20   ecure-Re quests: 
00e0  31 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   1··User- Agent: M
00f0  6f 7a 69 6c 6c 61 2f 35  2e 30 20 28 4d 61 63 69   ozilla/5 .0 (Maci
0100  6e 74 6f 73 68 3b 20 49  6e 74 65 6c 20 4d 61 63   ntosh; I ntel Mac
```

The server is also running HTTP version 1.1.

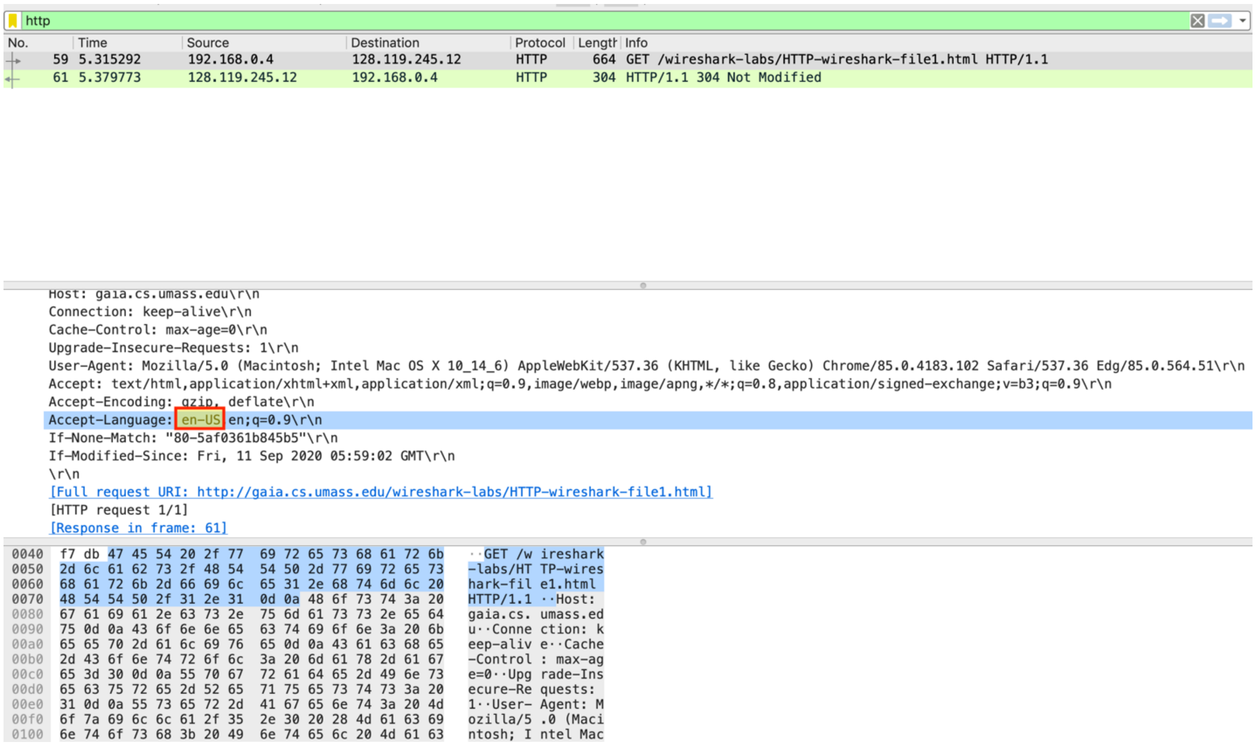


```
http
No.   Time       Source          Destination     Protocol Length Info
  59  5.315292   192.168.0.4     128.119.245.12  HTTP      664  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  61  5.379773   128.119.245.12  192.168.0.4     HTTP      304  HTTP/1.1 304 Not Modified

▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.4
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 56126, Seq: 1, Ack: 599, Len: 238
▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 304 Not Modified\r\n
    Date: Sat, 12 Sep 2020 02:56:22 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.9 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "80-5af0361b845b5"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.064481000 seconds]
    [Request in frame: 59]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]

0040  5c ba 48 54 54 50 2f 31  2e 31 20 33 30 34 20 4e   \·HTTP/1 .1 304 N
0050  6f 74 20 4d 6f 64 69 66  69 65 64 0d 0a 44 61 74   ot Modif ied··Dat
0060  65 3a 20 53 61 74 2c 20  31 32 20 53 65 70 20 32   e: Sat,  12 Sep 2
0070  30 32 30 20 30 32 3a 35  36 3a 32 32 20 47 4d 54   020 02:5 6:22 GMT
0080  0d 0a 53 65 72 76 65 72  3a 20 41 70 61 63 68 65   ··Server : Apache
0090  2f 32 2e 34 2e 36 20 28  43 65 6e 74 4f 53 29 20   /2.4.6 ( CentOS) 
00a0  4f 70 65 6e 53 53 4c 2f  31 2e 30 2e 32 6b 2d 66   OpenSSL/ 1.0.2k-f
00b0  69 70 73 20 50 48 50 2f  37 2e 34 2e 39 20 6d 6f   ips PHP/ 7.4.9 mo
00c0  64 5f 70 65 72 6c 2f 32  2e 30 2e 31 31 20 50 65   d_perl/2 .0.11 Pe
00d0  72 6c 2f 76 35 2e 31 36  2e 33 0d 0a 43 6f 6e 6e   rl/v5.16 .3··Conn
00e0  65 63 74 69 6f 6e 3a 20  4b 65 65 70 2d 41 6c 69   ection:  Keep-Ali
00f0  76 65 0d 0a 4b 65 65 70  2d 41 6c 69 76 65 3a 20   ve··Keep -Alive: 
0100  74 69 6d 65 6f 75 74 3d  35 2c 20 6d 61 78 3d 31   timeout= 5, max=1
```

2. The browser accepts en-US language.



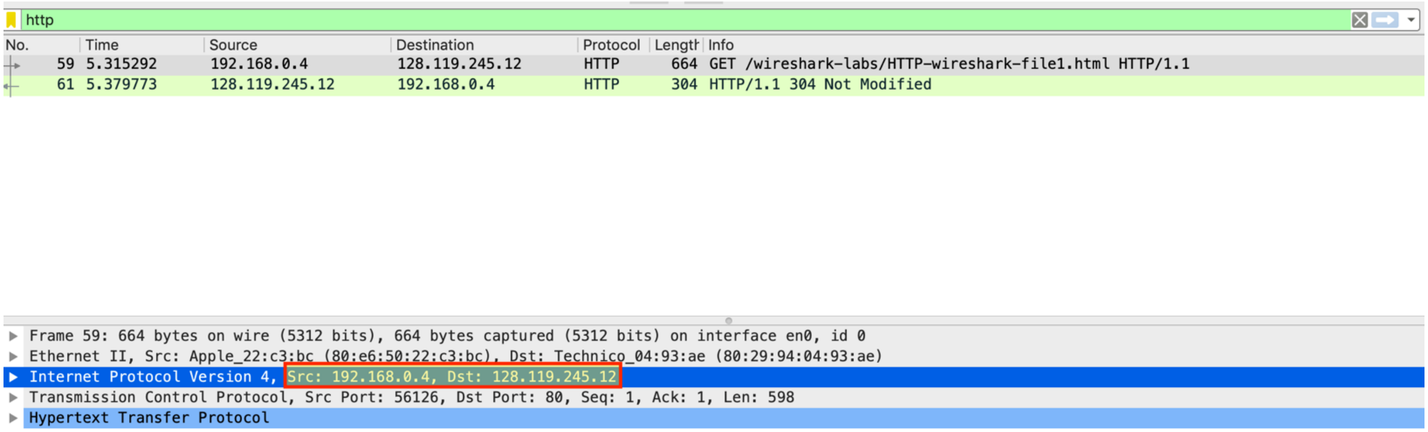
http

```
No.   Time       Source          Destination     Protocol  Length  Info
 59  5.315292   192.168.0.4     128.119.245.12  HTTP       664  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
 61  5.379773   128.119.245.12  192.168.0.4     HTTP       304  HTTP/1.1 304 Not Modified
```

```
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.102 Safari/537.36 Edg/85.0.564.51\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;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US en;q=0.9\r\n
    If-None-Match: "80-5af0361b845b5"\r\n
    If-Modified-Since: Fri, 11 Sep 2020 05:59:02 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 61]
```

```
0040  f7 db 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   ··GET /w ireshark
0050  2d 6c 61 62 73 2f 48 54  54 50 2d 77 69 72 65 73   -labs/HT TP-wires
0060  68 61 72 6b 2d 66 69 6c  65 31 2e 68 74 6d 6c 20   hark-fil e1.html 
0070  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.1 ··Host: 
0080  67 61 69 61 2e 63 73 2e  75 6d 61 73 73 2e 65 64   gaia.cs. umass.ed
0090  75 0d 0a 43 6f 6e 6e 65  63 74 69 6f 6e 3a 20 6b   u··Conne ction: k
00a0  65 65 70 2d 61 6c 69 76  65 0d 0a 43 61 63 68 65   eep-aliv e··Cache
00b0  2d 43 6f 6e 74 72 6f 6c  3a 20 6d 61 78 2d 61 67   -Control : max-ag
00c0  65 3d 30 0d 0a 55 70 67  72 61 64 65 2d 49 6e 73   e=0··Upg rade-Ins
00d0  65 63 75 72 65 2d 52 65  71 75 65 73 74 73 3a 20   ecure-Re quests: 
00e0  31 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   1··User- Agent: M
00f0  6f 7a 69 6c 6c 61 2f 35  2e 30 20 28 4d 61 63 69   ozilla/5 .0 (Maci
0100  6e 74 6f 73 68 3b 20 49  6e 74 65 6c 20 4d 61 63   ntosh; I ntel Mac
```

3. Computer IP address is: 192.168.0.4
Server IP address is: 128.119.245.12

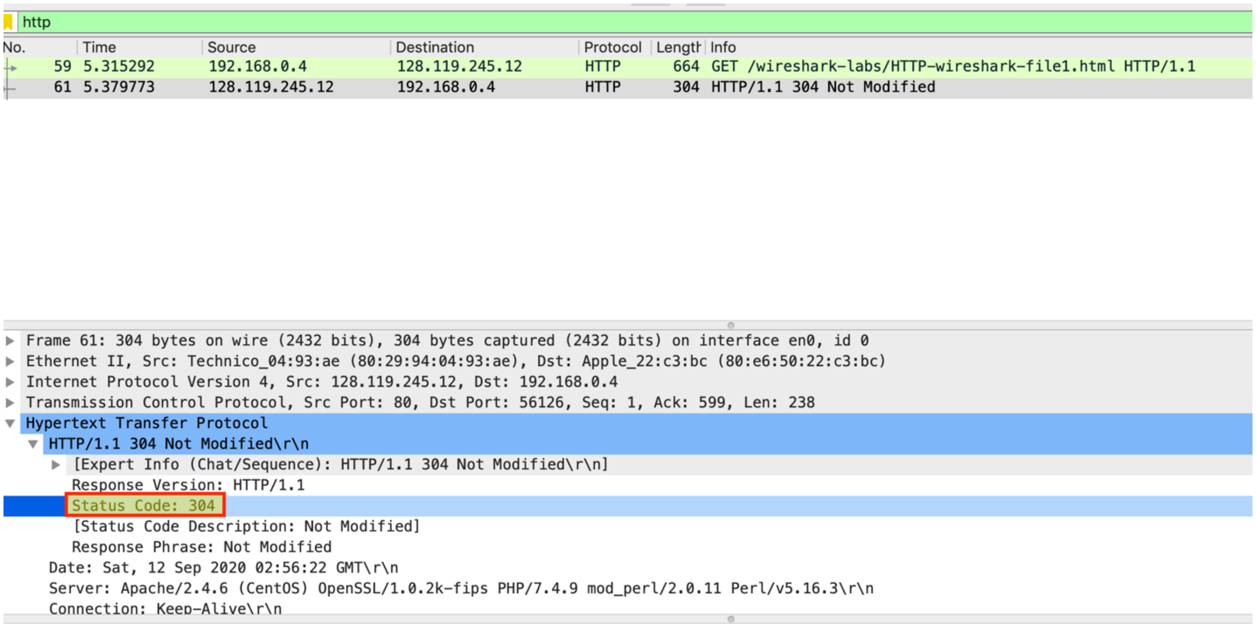


http

```
No.   Time       Source          Destination     Protocol  Length  Info
 59  5.315292   192.168.0.4     128.119.245.12  HTTP       664  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
 61  5.379773   128.119.245.12  192.168.0.4     HTTP       304  HTTP/1.1 304 Not Modified
```

```
▶ Frame 59: 664 bytes on wire (5312 bits), 664 bytes captured (5312 bits) on interface en0, id 0
▶ Ethernet II, Src: Apple_22:c3:bc (80:e6:50:22:c3:bc), Dst: Technico_04:93:ae (80:29:94:04:93:ae)
▶ Internet Protocol Version 4, Src: 192.168.0.4, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 56126, Dst Port: 80, Seq: 1, Ack: 1, Len: 598
▶ Hypertext Transfer Protocol
```

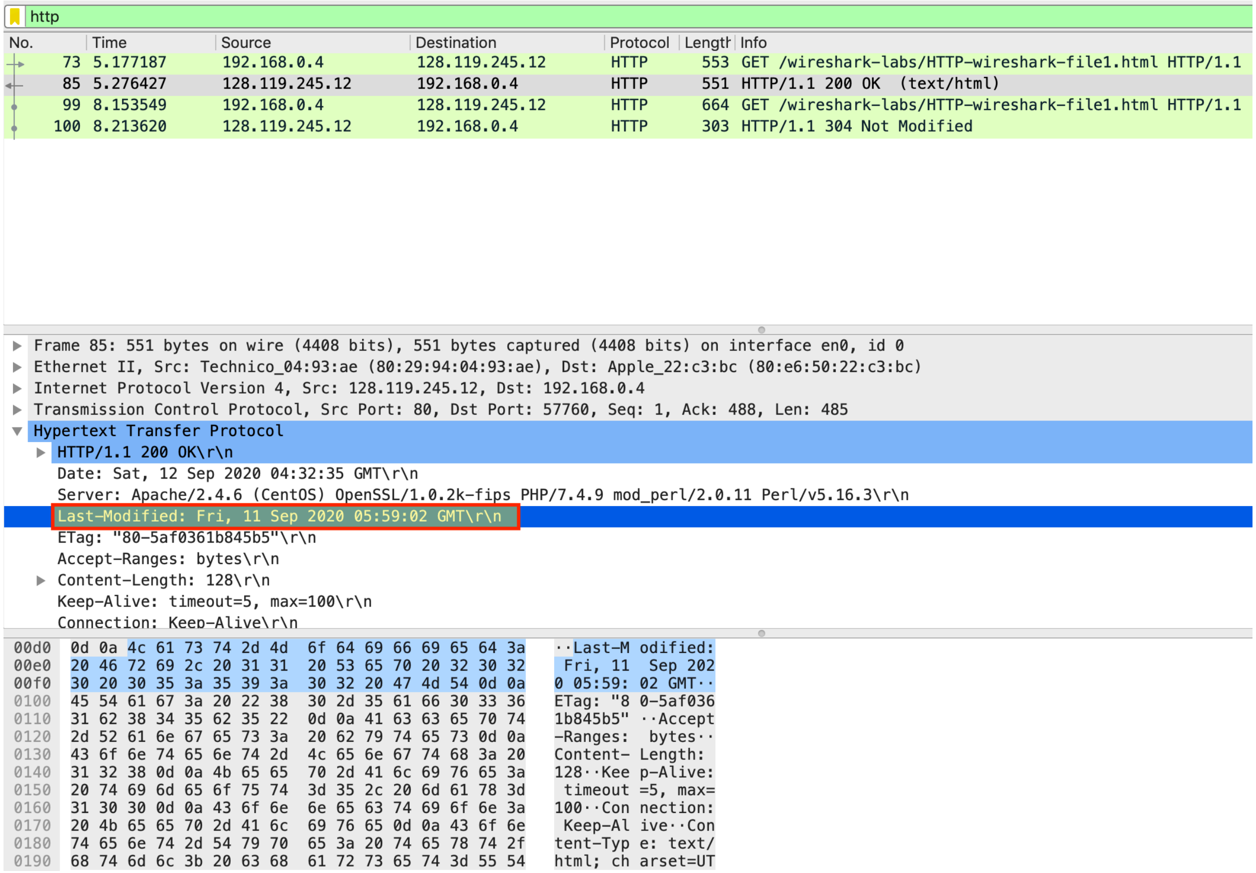
4. The status code returned is 304. This means that the document is not modified.



```
http
No.    Time         Source            Destination       Protocol  Length Info
    59 5.315292     192.168.0.4       128.119.245.12    HTTP       664  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
    61 5.379773     128.119.245.12    192.168.0.4       HTTP       304  HTTP/1.1 304 Not Modified

▶ Frame 61: 304 bytes on wire (2432 bits), 304 bytes captured (2432 bits) on interface en0, id 0
▶ Ethernet II, Src: Technico_04:93:ae (80:29:94:04:93:ae), Dst: Apple_22:c3:bc (80:e6:50:22:c3:bc)
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.4
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 56126, Seq: 1, Ack: 599, Len: 238
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 304 Not Modified\r\n
    ▶ [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
      Response Version: HTTP/1.1
      Status Code: 304
      [Status Code Description: Not Modified]
      Response Phrase: Not Modified
    Date: Sat, 12 Sep 2020 02:56:22 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.9 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
```

5. The file was last modified on Friday, September 11, 2020 at 05:59:02 GMT



```
http
No.    Time         Source            Destination       Protocol  Length Info
    73 5.177187     192.168.0.4       128.119.245.12    HTTP       553  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
    85 5.276427     128.119.245.12    192.168.0.4       HTTP       551  HTTP/1.1 200 OK  (text/html)
    99 8.153549     192.168.0.4       128.119.245.12    HTTP       664  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
   100 8.213620     128.119.245.12    192.168.0.4       HTTP       303  HTTP/1.1 304 Not Modified

▶ Frame 85: 551 bytes on wire (4408 bits), 551 bytes captured (4408 bits) on interface en0, id 0
▶ Ethernet II, Src: Technico_04:93:ae (80:29:94:04:93:ae), Dst: Apple_22:c3:bc (80:e6:50:22:c3:bc)
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.4
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 57760, Seq: 1, Ack: 488, Len: 485
▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 200 OK\r\n
    Date: Sat, 12 Sep 2020 04:32:35 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.9 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Fri, 11 Sep 2020 05:59:02 GMT\r\n
    ETag: "80-5af0361b845b5"\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

00d0  0d 0a 4c 61 73 74 2d 4d  6f 64 69 66 69 65 64 3a   ··Last-M odified:
00e0  20 46 72 69 2c 20 31 31  20 53 65 70 20 32 30 32    Fri, 11  Sep 202
00f0  30 20 30 35 3a 35 39 3a  30 32 20 47 4d 54 0d 0a   0 05:59: 02 GMT··
0100  45 54 61 67 3a 20 22 38  30 2d 35 61 66 30 33 36   ETag: "8 0-5af036
0110  31 62 38 34 35 62 35 22  0d 0a 41 63 63 65 70 74   1b845b5" ··Accept
0120  2d 52 61 6e 67 65 73 3a  20 62 79 74 65 73 0d 0a   -Ranges:  bytes··
0130  43 6f 6e 74 65 6e 74 2d  4c 65 6e 67 74 68 3a 20   Content- Length: 
0140  31 32 38 0d 0a 4b 65 65  70 2d 41 6c 69 76 65 3a   128··Kee p-Alive:
0150  20 74 69 6d 65 6f 75 74  3d 35 2c 20 6d 61 78 3d    timeout =5, max=
0160  31 30 30 0d 0a 43 6f 6e  6e 65 63 74 69 6f 6e 3a   100··Con nection:
0170  20 4b 65 65 70 2d 41 6c  69 76 65 0d 0a 43 6f 6e    Keep-Al ive··Con
0180  74 65 6e 74 2d 54 79 70  65 3a 20 74 65 78 74 2f   tent-Typ e: text/
0190  68 74 6d 6c 3b 20 63 68  61 72 73 65 74 3d 55 54   html; ch arset=UT
```

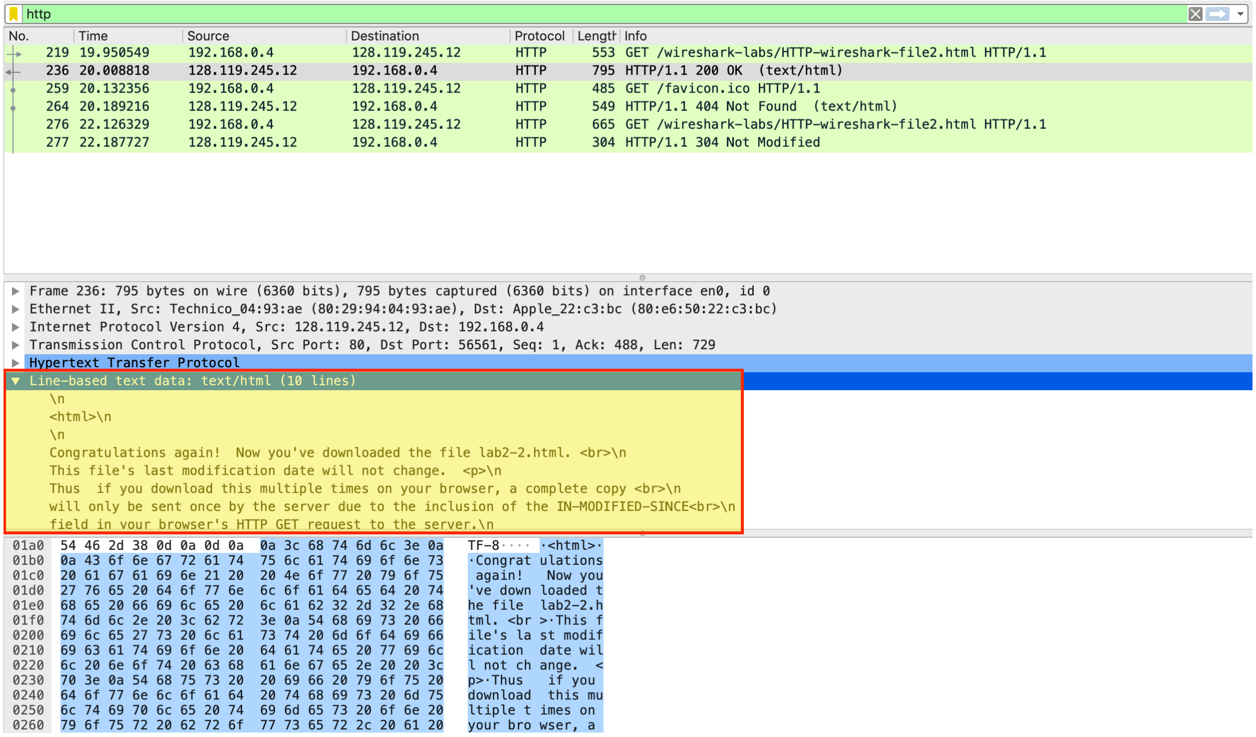
6. As seen in the screenshot above (Anwer #5), 128 bytes of content are being returned.

7. No, all of the headers can be found in the raw data.

PART 2: The HTTP CONDITIONAL GET/response interaction

8. No, I do not see an "IF-MODIFIED-SINCE" line in the HTTP GET.

9. Yes, the server did explicitly return the contents of the file. As we can see, Wireshark now includes a section titled "Line-Based Text Data" which shows what the server sent back to my browser.

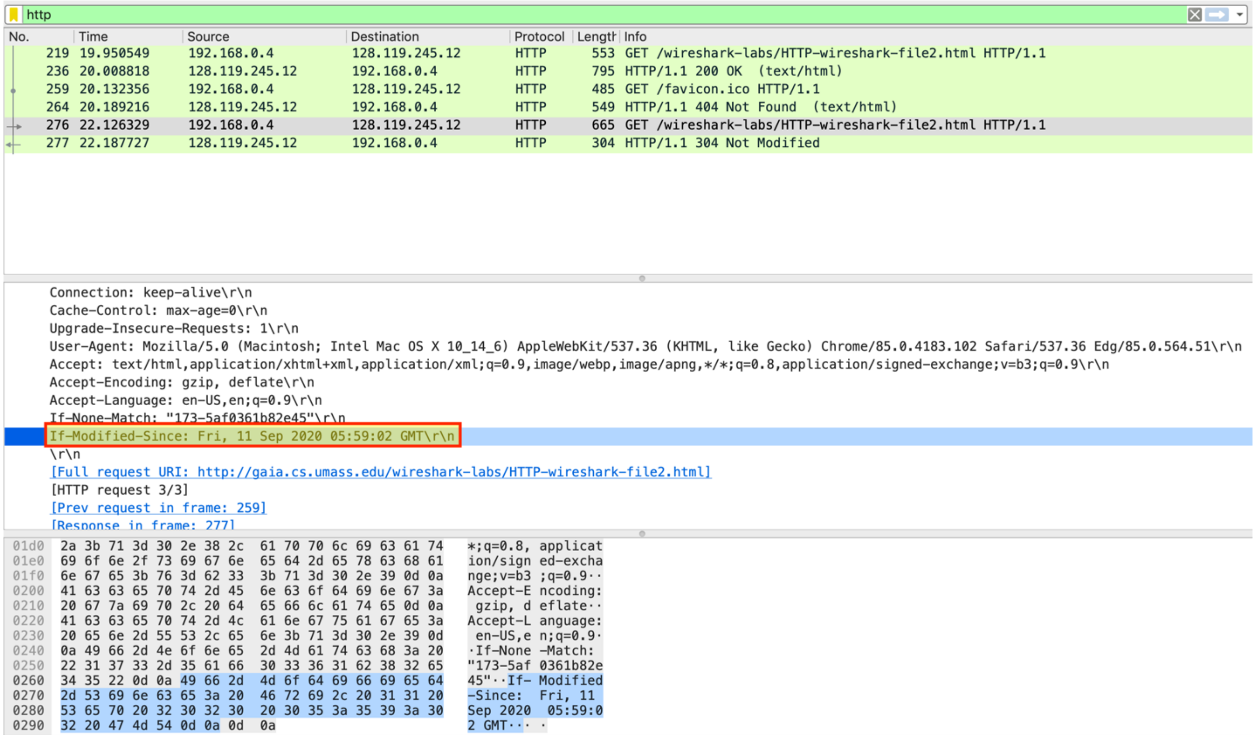


```
No.    Time       Source          Destination     Protocol Length Info
  219 19.950549  192.168.0.4     128.119.245.12  HTTP      553 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  236 20.008818  128.119.245.12  192.168.0.4     HTTP      795 HTTP/1.1 200 OK  (text/html)
  259 20.132356  192.168.0.4     128.119.245.12  HTTP      485 GET /favicon.ico HTTP/1.1
  264 20.189216  128.119.245.12  192.168.0.4     HTTP      549 HTTP/1.1 404 Not Found  (text/html)
  276 22.126329  192.168.0.4     128.119.245.12  HTTP      665 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  277 22.187727  128.119.245.12  192.168.0.4     HTTP      304 HTTP/1.1 304 Not Modified
```

```
▶ Frame 236: 795 bytes on wire (6360 bits), 795 bytes captured (6360 bits) on interface en0, id 0
▶ Ethernet II, Src: Technico_04:93:ae (80:29:94:04:93:ae), Dst: Apple_22:c3:bc (80:e6:50:22:c3:bc)
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.4
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 56561, Seq: 1, Ack: 488, Len: 729
▶ Hypertext Transfer Protocol
▼ 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
```

```
01a0  54 46 2d 38 0d 0a 0d 0a  0a 3c 68 74 6d 6c 3e 0a   TF-8···· ·<html>·
01b0  0a 43 6f 6e 67 72 61 74  75 6c 61 74 69 6f 6e 73   ·Congrat ulations
01c0  20 61 67 61 69 6e 21 20  20 4e 6f 77 20 79 6f 75    again!   Now you
01d0  27 76 65 20 64 6f 77 6e  6c 6f 61 64 65 64 20 74   've down loaded t
01e0  68 65 20 66 69 6c 65 20  6c 61 62 32 2d 32 2e 68   he file  lab2-2.h
01f0  74 6d 6c 2e 20 3c 62 72  3e 0a 54 68 69 73 20 66   tml. <br >·This f
0200  69 6c 65 27 73 20 6c 61  73 74 20 6d 6f 64 69 66   ile's la st modif
0210  69 63 61 74 69 6f 6e 20  64 61 74 65 20 77 69 6c   ication  date wil
0220  6c 20 6e 6f 74 20 63 68  61 6e 67 65 2e 20 20 3c   l not ch ange.  <
0230  70 3e 0a 54 68 75 73 20  20 69 66 20 79 6f 75 20   p>·Thus   if you 
0240  64 6f 77 6e 6c 6f 61 64  20 74 68 69 73 20 6d 75   download  this mu
0250  6c 74 69 70 6c 65 20 74  69 6d 65 73 20 6f 6e 20   ltiple t imes on 
0260  79 6f 75 72 20 62 72 6f  77 73 65 72 2c 20 61 20   your bro wser, a 
```

10. Yes in the second HTTP message an IF-MODIFIED-SINCE line is included. The information that follows is the date and time that I last accessed the webpage



```
http
No.   Time        Source           Destination      Protocol Length Info
  219 19.950549   192.168.0.4      128.119.245.12   HTTP      553 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  236 20.008818   128.119.245.12   192.168.0.4      HTTP      795 HTTP/1.1 200 OK  (text/html)
  259 20.132356   192.168.0.4      128.119.245.12   HTTP      485 GET /favicon.ico HTTP/1.1
  264 20.189216   128.119.245.12   192.168.0.4      HTTP      549 HTTP/1.1 404 Not Found  (text/html)
  276 22.126329   192.168.0.4      128.119.245.12   HTTP      665 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  277 22.187727   128.119.245.12   192.168.0.4      HTTP      304 HTTP/1.1 304 Not Modified
```

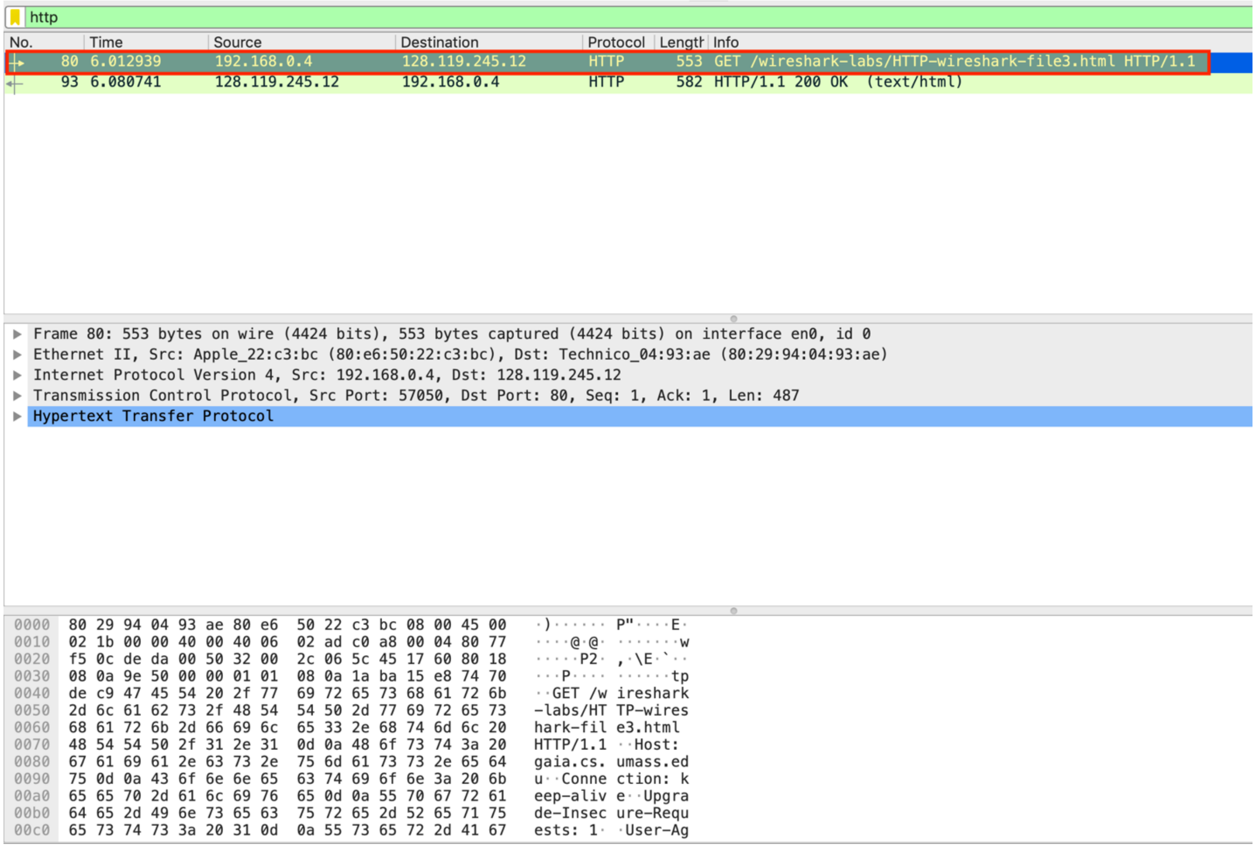
```
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.102 Safari/537.36 Edg/85.0.564.51\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
If-None-Match: "173-5af0361b82e45"\r\n
If-Modified-Since: Fri, 11 Sep 2020 05:59:02 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 3/3]
[Prev request in frame: 259]
[Response in frame: 277]
```

```
01d0  2a 3b 71 3d 30 2e 38 2c  61 70 70 6c 69 63 61 74   *;q=0.8, applicat
01e0  69 6f 6e 2f 73 69 67 6e  65 64 2d 65 78 63 68 61   ion/sign ed-excha
01f0  6e 67 65 3b 76 3d 62 33  3b 71 3d 30 2e 39 0d 0a   nge;v=b3 ;q=0.9··
0200  41 63 63 65 70 74 2d 45  6e 63 6f 64 69 6e 67 3a   Accept-E ncoding:
0210  20 67 7a 69 70 2c 20 64  65 66 6c 61 74 65 0d 0a    gzip, d eflate··
0220  41 63 63 65 70 74 2d 4c  61 6e 67 75 61 67 65 3a   Accept-L anguage:
0230  20 65 6e 2d 55 53 2c 65  6e 3b 71 3d 30 2e 39 0d    en-US,e n;q=0.9·
0240  0a 49 66 2d 4e 6f 6e 65  2d 4d 61 74 63 68 3a 20   ·If-None -Match:
0250  22 31 37 33 2d 35 61 66  30 33 36 31 62 38 32 65   "173-5af 0361b82e
0260  34 35 22 0d 0a 49 66 2d  4d 6f 64 69 66 69 65 64   45"··If- Modified
0270  2d 53 69 6e 63 65 3a 20  46 72 69 2c 20 31 31 20   -Since:  Fri, 11
0280  53 65 70 20 32 30 32 30  20 30 35 3a 35 39 3a 30   Sep 2020  05:59:0
0290  32 20 47 4d 54 0d 0a 0d  0a                        2 GMT··· ·
```

11. The HTTP status code is “304: Not Modified”. The server did not return the contents of the file because the browser instead obtained the contents from the cache. If the file had been modified since it was last accessed, it would have returned the contents of the file, but it only used the last file from cached memory.

PART 3: Retrieving Long Documents

12. My browser only sent 1 HTTP GET request to the server. The packet containing the GET message was packet number 80.



```
No.   Time       Source          Destination     Protocol Length Info
  80  6.012939   192.168.0.4     128.119.245.12  HTTP     553  GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  93  6.080741   128.119.245.12  192.168.0.4     HTTP     582  HTTP/1.1 200 OK  (text/html)
```

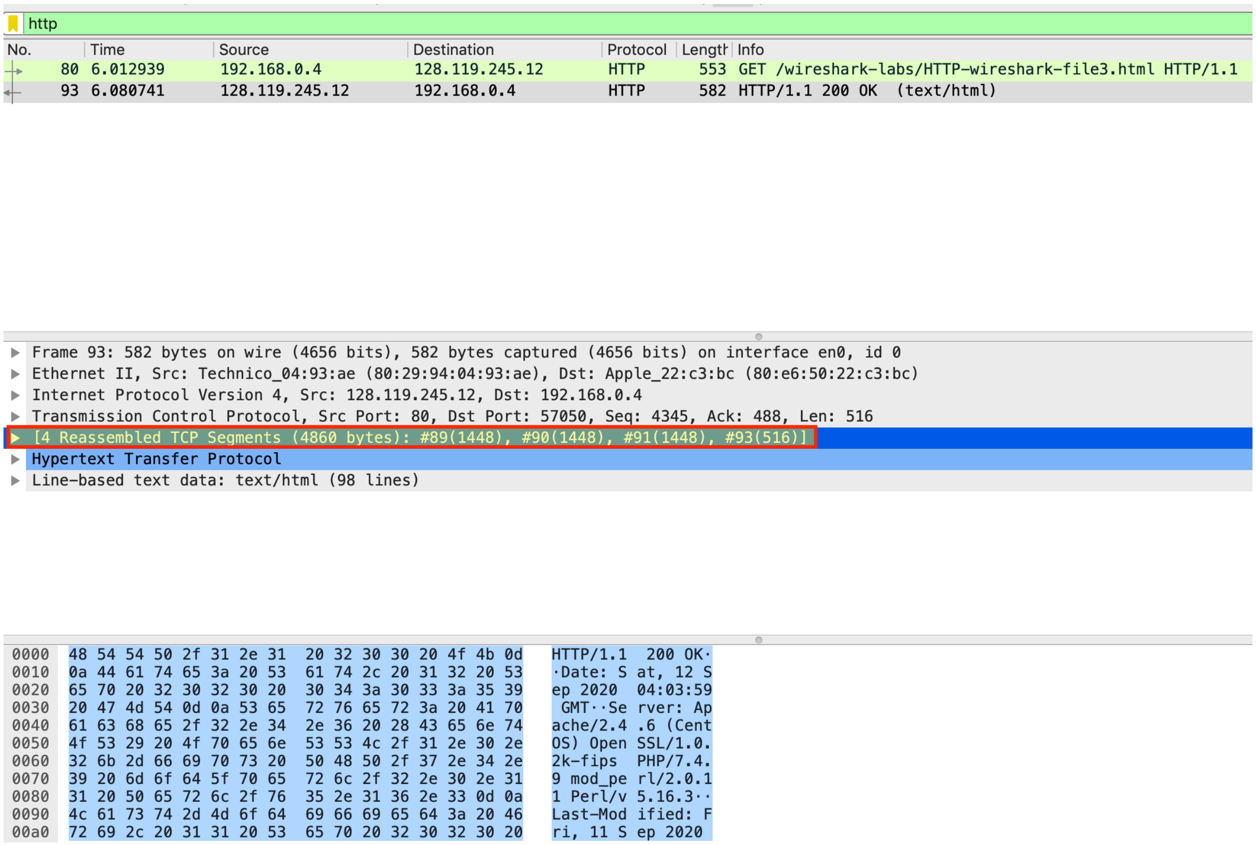
```
▶ Frame 80: 553 bytes on wire (4424 bits), 553 bytes captured (4424 bits) on interface en0, id 0
▶ Ethernet II, Src: Apple_22:c3:bc (80:e6:50:22:c3:bc), Dst: Technico_04:93:ae (80:29:94:04:93:ae)
▶ Internet Protocol Version 4, Src: 192.168.0.4, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 57050, Dst Port: 80, Seq: 1, Ack: 1, Len: 487
▶ Hypertext Transfer Protocol
```

```
0000  80 29 94 04 93 ae 80 e6  50 22 c3 bc 08 00 45 00   ·)······ P"····E·
0010  02 1b 00 00 40 00 40 06  02 ad c0 a8 00 04 80 77   ····@·@· ·······w
0020  f5 0c de da 00 50 32 00  2c 06 5c 45 17 60 80 18   ·····P2· ,·\E·`··
0030  08 0a 9e 50 00 00 01 01  08 0a 1a ba 15 e8 74 70   ···P···· ······tp
0040  de c9 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   ··GET /w ireshark
0050  2d 6c 61 62 73 2f 48 54  54 50 2d 77 69 72 65 73   -labs/HT TP-wires
0060  68 61 72 6b 2d 66 69 6c  65 33 2e 68 74 6d 6c 20   hark-fil e3.html 
0070  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.1 ··Host: 
0080  67 61 69 61 2e 63 73 2e  75 6d 61 73 73 2e 65 64   gaia.cs. umass.ed
0090  75 0d 0a 43 6f 6e 6e 65  63 74 69 6f 6e 3a 20 6b   u··Conne ction: k
00a0  65 65 70 2d 61 6c 69 76  65 0d 0a 55 70 67 72 61   eep-aliv e··Upgra
00b0  64 65 2d 49 6e 73 65 63  75 72 65 2d 52 65 71 75   de-Insec ure-Requ
00c0  65 73 74 73 3a 20 31 0d  0a 55 73 65 72 2d 41 67   ests: 1· ·User-Ag
```

13. Packet number 93 contains the status code and phrase associated with the response to the HTTP GET request, as can be seen in the screenshot above.

14. The code and phrase in the response was 200 OK, as can be seen in the image from #12.

15. The data was sent in 4 TCP segments to the browser, then reassembled.



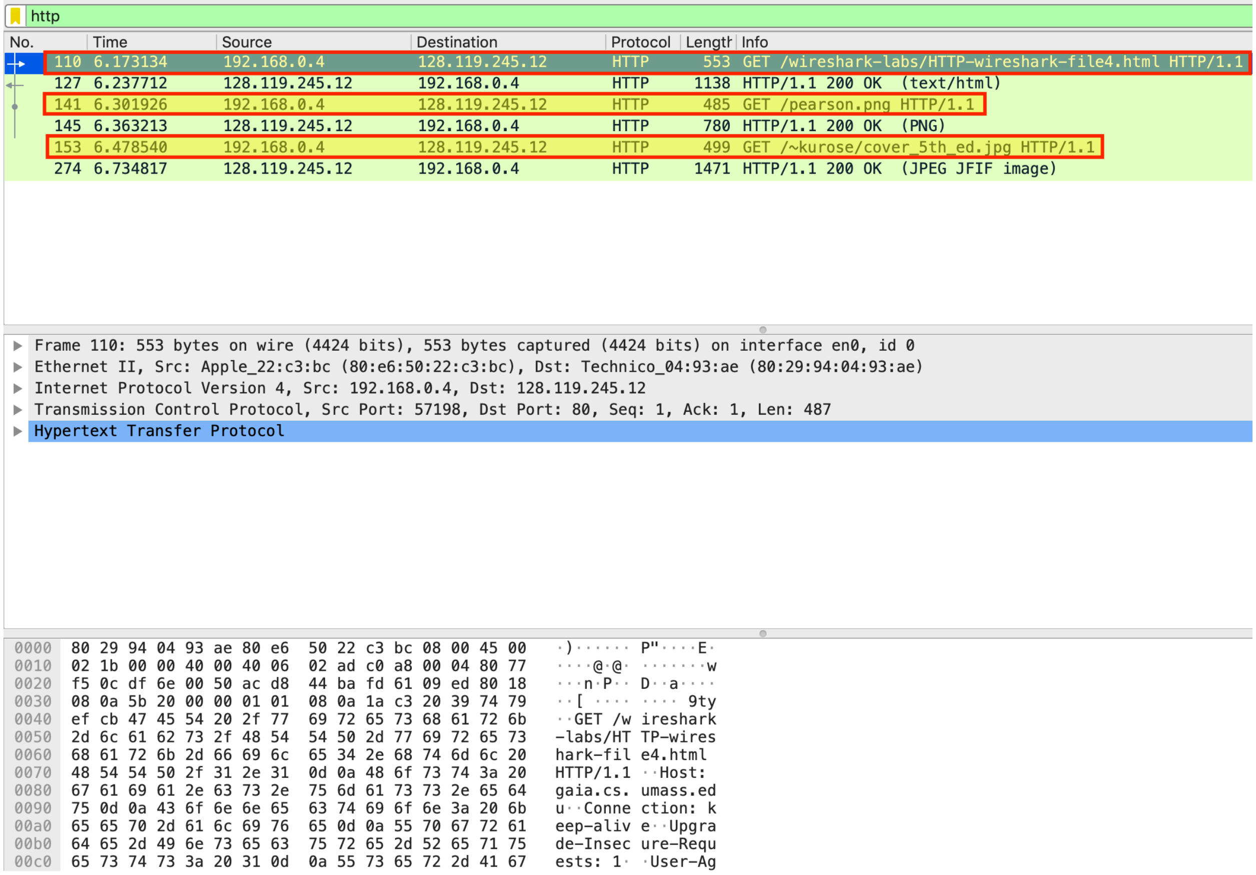
```
No.   Time       Source          Destination     Protocol Length Info
   80 6.012939   192.168.0.4     128.119.245.12  HTTP     553    GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
   93 6.080741   128.119.245.12  192.168.0.4     HTTP     582    HTTP/1.1 200 OK  (text/html)
```

```
▶ Frame 93: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits) on interface en0, id 0
▶ Ethernet II, Src: Technico_04:93:ae (80:29:94:04:93:ae), Dst: Apple_22:c3:bc (80:e6:50:22:c3:bc)
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.4
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 57050, Seq: 4345, Ack: 488, Len: 516
▶ [4 Reassembled TCP Segments (4860 bytes): #89(1448), #90(1448), #91(1448), #93(516)]
▶ Hypertext Transfer Protocol
▶ Line-based text data: text/html (98 lines)
```

```
0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK·
0010  0a 44 61 74 65 3a 20 53  61 74 2c 20 31 32 20 53   ·Date: S at, 12 S
0020  65 70 20 32 30 32 30 20  30 34 3a 30 33 3a 35 39   ep 2020  04:03:59
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 37 2e 34 2e   2k-fips  PHP/7.4.
0070  39 20 6d 6f 64 5f 70 65  72 6c 2f 32 2e 30 2e 31   9 mod_pe rl/2.0.1
0080  31 20 50 65 72 6c 2f 76  35 2e 31 36 2e 33 0d 0a   1 Perl/v 5.16.3··
0090  4c 61 73 74 2d 4d 6f 64  69 66 69 65 64 3a 20 46   Last-Mod ified: F
00a0  72 69 2c 20 31 31 20 53  65 70 20 32 30 32 30 20   ri, 11 S ep 2020
```

PART 4: HTML Documents with Embedded Objects

16. My browser sent 3 http GET message requests. One each to each for each of the following: The initial page, the Pearson logo, and the cover of the Pearson book, 5th Edition.
These were retrieved from the page address: 128.119.245.12



```
http
No.   Time       Source           Destination      Protocol  Length  Info
110   6.173134   192.168.0.4      128.119.245.12   HTTP      553  GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
127   6.237712   128.119.245.12   192.168.0.4      HTTP      1138  HTTP/1.1 200 OK  (text/html)
141   6.301926   192.168.0.4      128.119.245.12   HTTP      485  GET /pearson.png HTTP/1.1
145   6.363213   128.119.245.12   192.168.0.4      HTTP      780  HTTP/1.1 200 OK  (PNG)
153   6.478540   192.168.0.4      128.119.245.12   HTTP      499  GET /~kurose/cover_5th_ed.jpg HTTP/1.1
274   6.734817   128.119.245.12   192.168.0.4      HTTP      1471  HTTP/1.1 200 OK  (JPEG JFIF image)
```

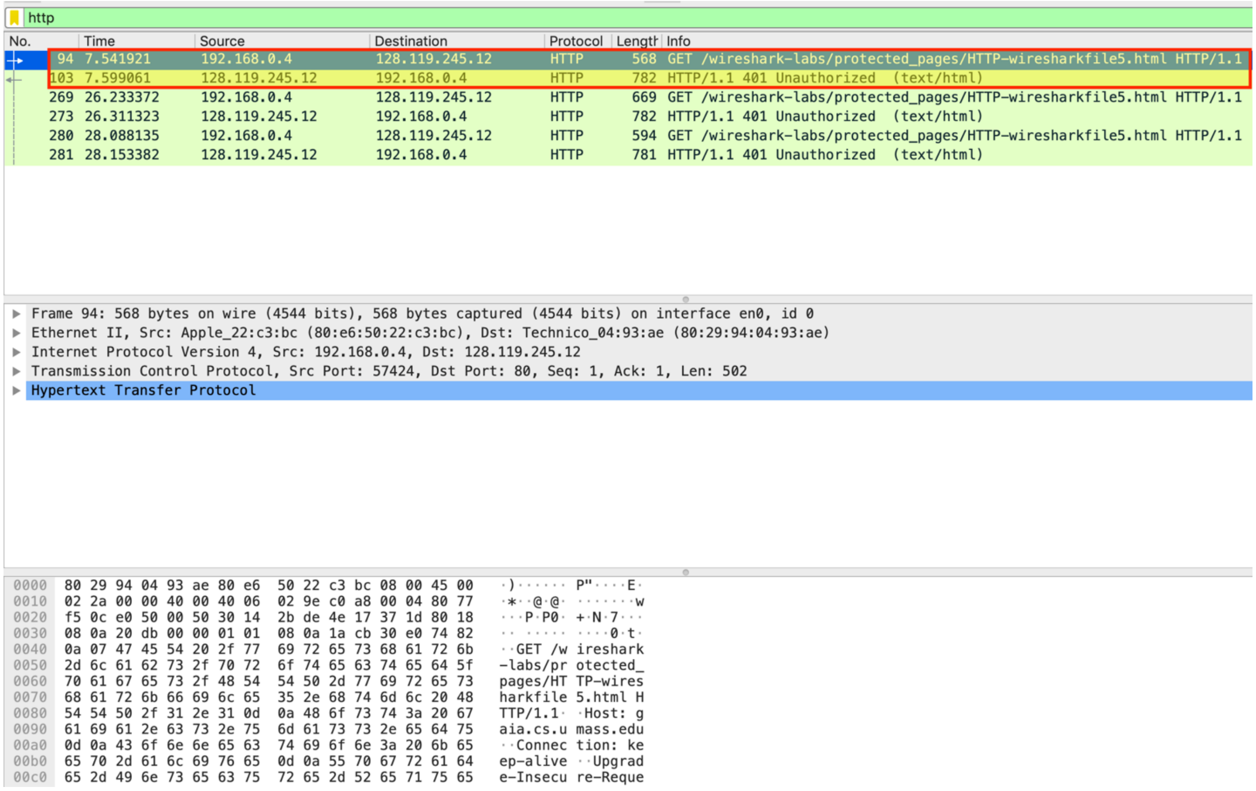
```
▶ Frame 110: 553 bytes on wire (4424 bits), 553 bytes captured (4424 bits) on interface en0, id 0
▶ Ethernet II, Src: Apple_22:c3:bc (80:e6:50:22:c3:bc), Dst: Technico_04:93:ae (80:29:94:04:93:ae)
▶ Internet Protocol Version 4, Src: 192.168.0.4, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 57198, Dst Port: 80, Seq: 1, Ack: 1, Len: 487
▶ Hypertext Transfer Protocol
```

```
0000  80 29 94 04 93 ae 80 e6  50 22 c3 bc 08 00 45 00   ·)······ P"····E·
0010  02 1b 00 00 40 00 40 06  02 ad c0 a8 00 04 80 77   ····@·@· ·······w
0020  f5 0c df 6e 00 50 ac d8  44 ba fd 61 09 ed 80 18   ···n·P·· D··a····
0030  08 0a 5b 20 00 00 01 01  08 0a 1a c3 20 39 74 79   ··[ ···· ···· 9ty
0040  ef cb 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   ··GET /w ireshark
0050  2d 6c 61 62 73 2f 48 54  54 50 2d 77 69 72 65 73   -labs/HT TP-wires
0060  68 61 72 6b 2d 66 69 6c  65 34 2e 68 74 6d 6c 20   hark-fil e4.html 
0070  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.1 ··Host: 
0080  67 61 69 61 2e 63 73 2e  75 6d 61 73 73 2e 65 64   gaia.cs. umass.ed
0090  75 0d 0a 43 6f 6e 6e 65  63 74 69 6f 6e 3a 20 6b   u··Conne ction: k
00a0  65 65 70 2d 61 6c 69 76  65 0d 0a 55 70 67 72 61   eep-aliv e··Upgra
00b0  64 65 2d 49 6e 73 65 63  75 72 65 2d 52 65 71 75   de-Insec ure-Requ
00c0  65 73 74 73 3a 20 31 0d  0a 55 73 65 72 2d 41 67   ests: 1· ·User-Ag
```

17. The browser downloaded the two images serially. This is the case because the first image was requested and sent before the second image was requested by the browser. If they were running in parallel, both files would have been requested then would have returned in the same time period.

PART 5: HTTP Authentication

18. The servers initial response was “401 Authentication Required”

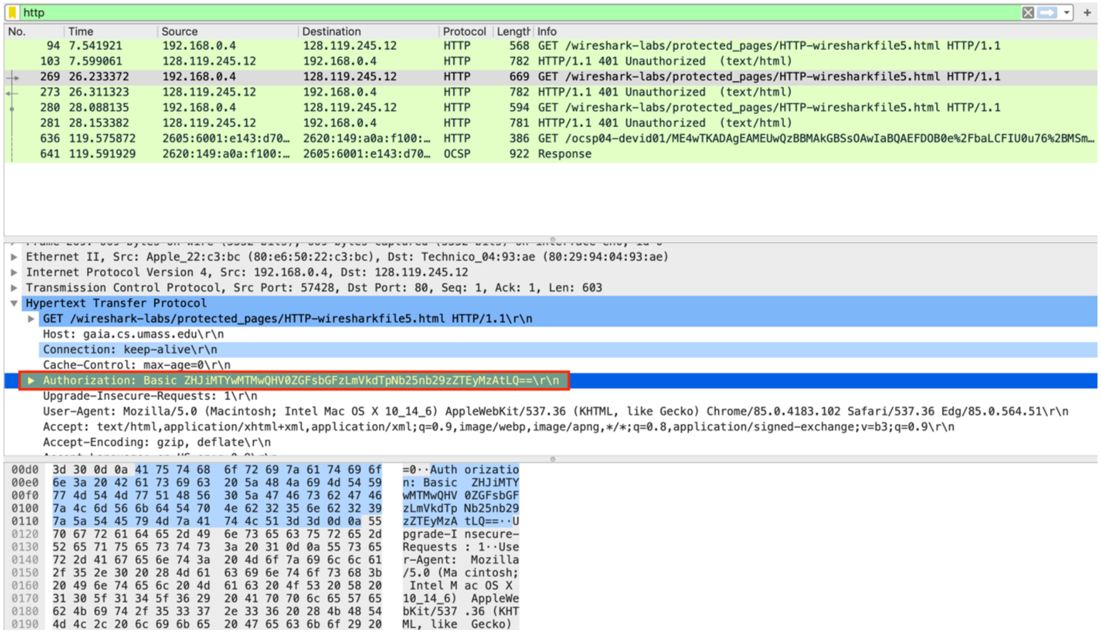


```
http
No.   Time       Source          Destination     Protocol Length Info
 94   7.541921   192.168.0.4     128.119.245.12  HTTP     568 GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
103   7.599061   128.119.245.12  192.168.0.4     HTTP     782 HTTP/1.1 401 Unauthorized  (text/html)
269   26.233372  192.168.0.4     128.119.245.12  HTTP     669 GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
273   26.311323  128.119.245.12  192.168.0.4     HTTP     782 HTTP/1.1 401 Unauthorized  (text/html)
280   28.088135  192.168.0.4     128.119.245.12  HTTP     594 GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
281   28.153382  128.119.245.12  192.168.0.4     HTTP     781 HTTP/1.1 401 Unauthorized  (text/html)
```

```
▶ Frame 94: 568 bytes on wire (4544 bits), 568 bytes captured (4544 bits) on interface en0, id 0
▶ Ethernet II, Src: Apple_22:c3:bc (80:e6:50:22:c3:bc), Dst: Technico_04:93:ae (80:29:94:04:93:ae)
▶ Internet Protocol Version 4, Src: 192.168.0.4, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 57424, Dst Port: 80, Seq: 1, Ack: 1, Len: 502
▶ Hypertext Transfer Protocol
```

```
0000  80 29 94 04 93 ae 80 e6  50 22 c3 bc 08 00 45 00   ·)······ P"····E·
0010  02 2a 00 00 40 00 40 06  02 9e c0 a8 00 04 80 77   ·*··@·@· ·······w
0020  f5 0c e0 50 00 50 30 14  2b de 4e 17 37 1d 80 18   ···P·P0· +·N·7···
0030  08 0a 20 db 00 00 01 01  08 0a 1a cb 30 e0 74 82   ·· ····· ····0·t·
0040  0a 07 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   ··GET /w ireshark
0050  2d 6c 61 62 73 2f 70 72  6f 74 65 63 74 65 64 5f   -labs/pr otected_
0060  70 61 67 65 73 2f 48 54  54 50 2d 77 69 72 65 73   pages/HT TP-wires
0070  68 61 72 6b 66 69 6c 65  35 2e 68 74 6d 6c 20 48   harkfile 5.html H
0080  54 54 50 2f 31 2e 31 0d  0a 48 6f 73 74 3a 20 67   TTP/1.1· ·Host: g
0090  61 69 61 2e 63 73 2e 75  6d 61 73 73 2e 65 64 75   aia.cs.u mass.edu
00a0  0d 0a 43 6f 6e 6e 65 63  74 69 6f 6e 3a 20 6b 65   ··Connec tion: ke
00b0  65 70 2d 61 6c 69 76 65  0d 0a 55 70 67 72 61 64   ep-alive ··Upgrad
00c0  65 2d 49 6e 73 65 63 75  72 65 2d 52 65 71 75 65   e-Insecu re-Reque
```

19. The new field that is now included is the authorization field. This is included because we sent the server a username and password along with our request stating that we were authorized to receive the page.



```
http

No.   Time        Source               Destination          Protocol  Length  Info
   94 7.541921    192.168.0.4          128.119.245.12       HTTP       568  GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
  103 7.599061    128.119.245.12       192.168.0.4          HTTP       782  HTTP/1.1 401 Unauthorized  (text/html)
  269 26.233372   192.168.0.4          128.119.245.12       HTTP       669  GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
  273 26.311323   128.119.245.12       192.168.0.4          HTTP       782  HTTP/1.1 401 Unauthorized  (text/html)
  280 28.088135   192.168.0.4          128.119.245.12       HTTP       594  GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
  281 28.153382   128.119.245.12       192.168.0.4          HTTP       781  HTTP/1.1 401 Unauthorized  (text/html)
  636 119.575872  2605:6001:e143:d70…  2620:149:a0a:f100:…  HTTP       386  GET /ocsp04-devid01/ME4wTKADAgEAMEUwQzBBMAkGBSsOAwIaBQAEFDOB0e%2FbaLCFIU0u76%2BMSm…
  641 119.591929  2620:149:a0a:f100:…  2605:6001:e143:d70…  OCSP       922  Response
```

```
▶ Ethernet II, Src: Apple_22:c3:bc (80:e6:50:22:c3:bc), Dst: Technico_04:93:ae (80:29:94:04:93:ae)
▶ Internet Protocol Version 4, Src: 192.168.0.4, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 57428, Dst Port: 80, Seq: 1, Ack: 1, Len: 603
▼ Hypertext Transfer Protocol
  ▶ GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.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
  ▶ Authorization: Basic ZHJiMTYwMTMwQHV0ZGFsbGFzLmVkdTpNb25nb29zZTEyMzAtLQ==\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.102 Safari/537.36 Edg/85.0.564.51\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;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
```

```
00d0  3d 30 0d 0a 41 75 74 68  6f 72 69 7a 61 74 69 6f   =0··Auth orizatio
00e0  6e 3a 20 42 61 73 69 63  20 5a 48 4a 69 4d 54 59   n: Basic  ZHJiMTY
00f0  77 4d 54 4d 77 51 48 56  30 5a 47 46 73 62 47 46   wMTMwQHV 0ZGFsbGF
0100  7a 4c 6d 56 6b 64 54 70  4e 62 32 35 6e 62 32 39   zLmVkdTp Nb25nb29
0110  7a 5a 54 45 79 4d 7a 41  74 4c 51 3d 3d 0d 0a 55   zZTEyMzA tLQ==··U
0120  70 67 72 61 64 65 2d 49  6e 73 65 63 75 72 65 2d   pgrade-I nsecure-
0130  52 65 71 75 65 73 74 73  3a 20 31 0d 0a 55 73 65   Requests : 1··Use
0140  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a 69 6c 6c 61   r-Agent:  Mozilla
0150  2f 35 2e 30 20 28 4d 61  63 69 6e 74 6f 73 68 3b   /5.0 (Ma cintosh;
0160  20 49 6e 74 65 6c 20 4d  61 63 20 4f 53 20 58 20    Intel M ac OS X
0170  31 30 5f 31 34 5f 36 29  20 41 70 70 6c 65 57 65   10_14_6)  AppleWe
0180  62 4b 69 74 2f 35 33 37  2e 33 36 20 28 4b 48 54   bKit/537 .36 (KHT
0190  4d 4c 2c 20 6c 69 6b 65  20 47 65 63 6b 6f 29 20   ML, like  Gecko)
```