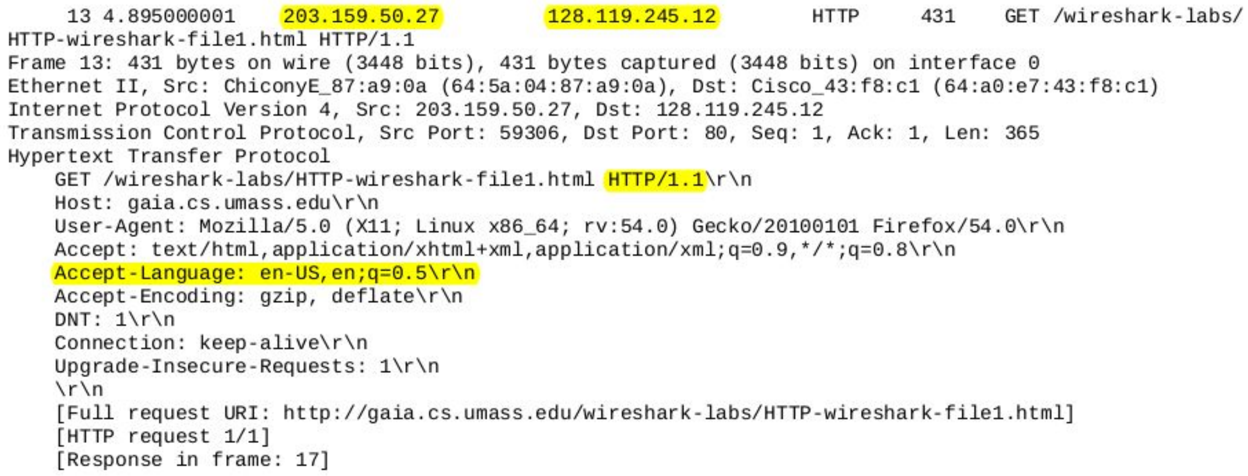
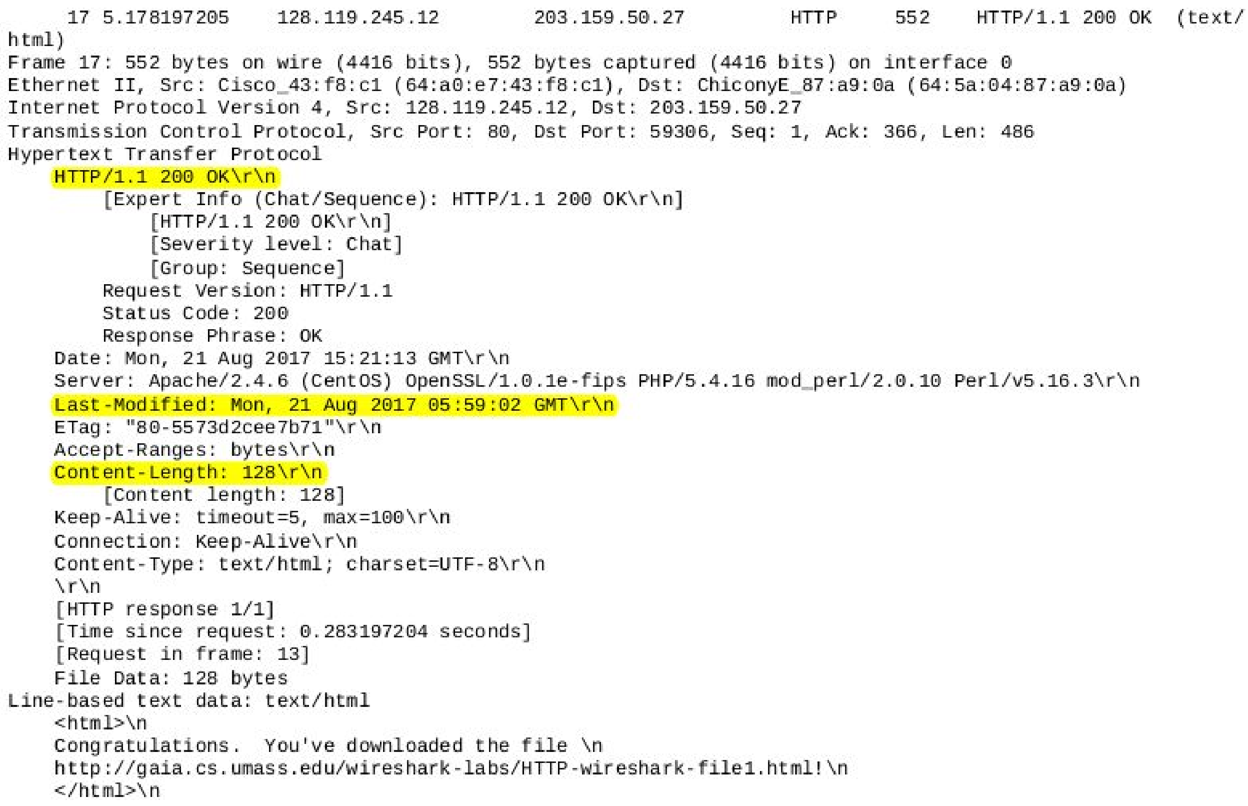
Wireshark Lab: HTTP

1. The Basic HTTP GET/response interaction



```
     13 4.895000001    203.159.50.27          128.119.245.12        HTTP     431    GET /wireshark-labs/
HTTP-wireshark-file1.html HTTP/1.1
Frame 13: 431 bytes on wire (3448 bits), 431 bytes captured (3448 bits) on interface 0
Ethernet II, Src: ChiconyE_87:a9:0a (64:5a:04:87:a9:0a), Dst: Cisco_43:f8:c1 (64:a0:e7:43:f8:c1)
Internet Protocol Version 4, Src: 203.159.50.27, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 59306, Dst Port: 80, Seq: 1, Ack: 1, Len: 365
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:54.0) Gecko/20100101 Firefox/54.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    DNT: 1\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\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: 17]
```



```
     17 5.178197205    128.119.245.12        203.159.50.27         HTTP     552    HTTP/1.1 200 OK  (text/
html)
Frame 17: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface 0
Ethernet II, Src: Cisco_43:f8:c1 (64:a0:e7:43:f8:c1), Dst: ChiconyE_87:a9:0a (64:5a:04:87:a9:0a)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 203.159.50.27
Transmission Control Protocol, Src Port: 80, Dst Port: 59306, Seq: 1, Ack: 366, Len: 486
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]
        Request Version: HTTP/1.1
        Status Code: 200
        Response Phrase: OK
    Date: Mon, 21 Aug 2017 15:21:13 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Mon, 21 Aug 2017 05:59:02 GMT\r\n
    ETag: "80-5573d2cee7b71"\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
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.283197204 seconds]
    [Request in frame: 13]
    File Data: 128 bytes
Line-based text data: text/html
    <html>\n
    Congratulations.  You've downloaded the file \n
    http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
    </html>\n
```

Answer the following questions:

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

Answer: Both runs HTTP 1.1

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

Answer: Accept-Language: en-us, en

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

Answer: My IP address is 203.159.50.27 and the server’s is 128.119.245.12

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

Answer: HTTP/1.1 200 OK (text/html)

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

Answer: Last-Modified: Mon, 21 Aug 2017 05:59:02 GMT

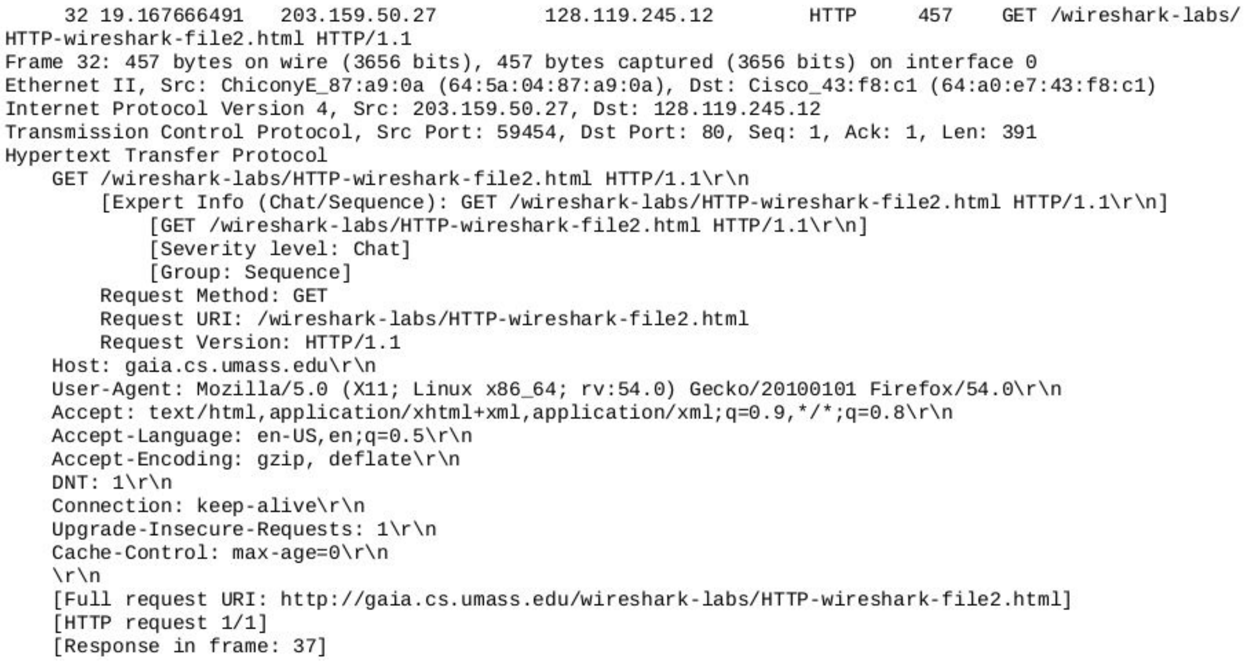
6. How many bytes of content are being returned to your browser?

Answer: Content-Length: 128

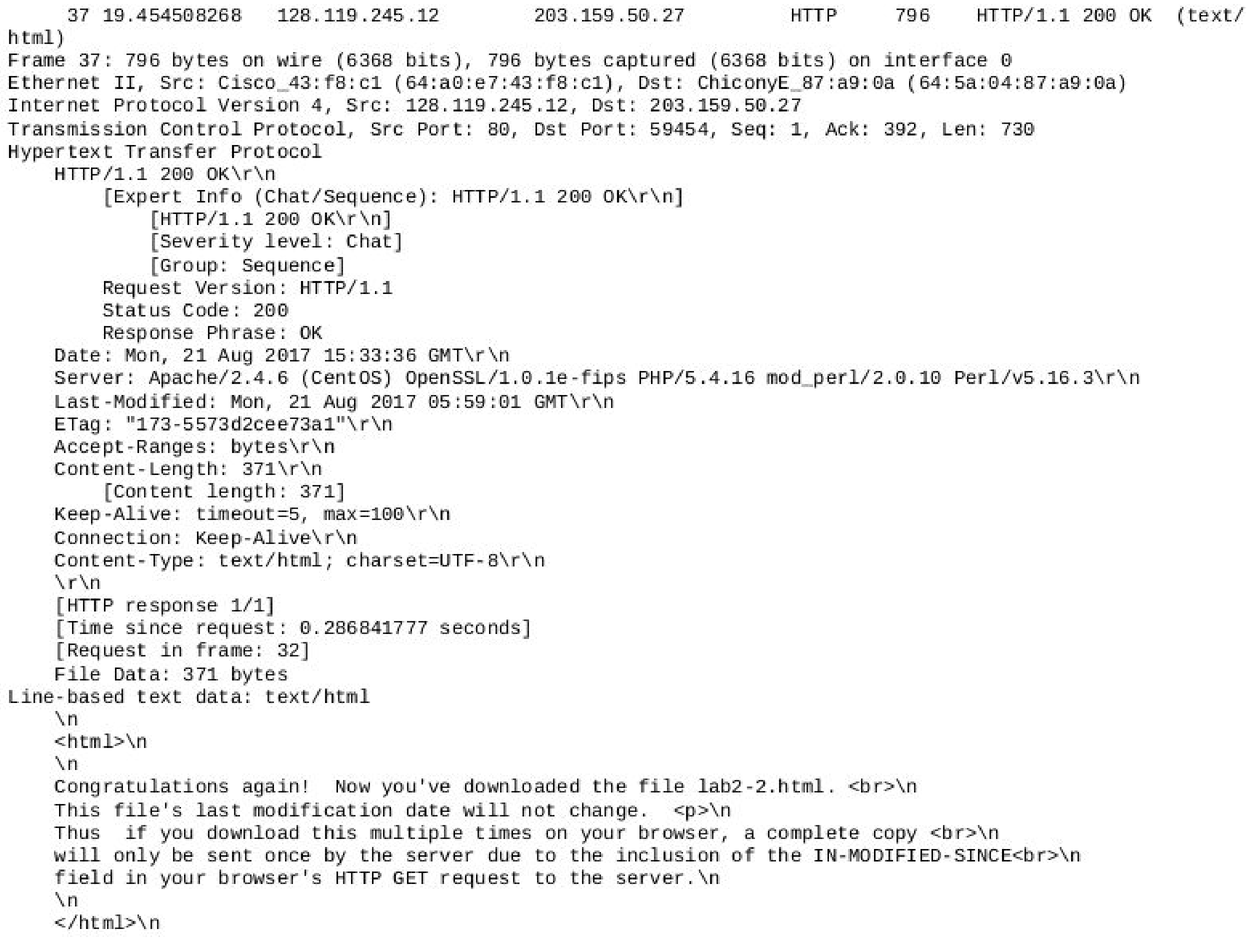
7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

Answer: No, all the headers can be found in the raw data.

2. The HTTP CONDITIONAL GET/response interaction



```
     32 19.167666491   203.159.50.27         128.119.245.12        HTTP     457    GET /wireshark-labs/
HTTP-wireshark-file2.html HTTP/1.1
Frame 32: 457 bytes on wire (3656 bits), 457 bytes captured (3656 bits) on interface 0
Ethernet II, Src: ChiconyE_87:a9:0a (64:5a:04:87:a9:0a), Dst: Cisco_43:f8:c1 (64:a0:e7:43:f8:c1)
Internet Protocol Version 4, Src: 203.159.50.27, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 59454, Dst Port: 80, Seq: 1, Ack: 1, Len: 391
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
        [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
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:54.0) Gecko/20100101 Firefox/54.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    DNT: 1\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Cache-Control: max-age=0\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: 37]
```



```
     37 19.454508268   128.119.245.12        203.159.50.27         HTTP     796    HTTP/1.1 200 OK  (text/
html)
Frame 37: 796 bytes on wire (6368 bits), 796 bytes captured (6368 bits) on interface 0
Ethernet II, Src: Cisco_43:f8:c1 (64:a0:e7:43:f8:c1), Dst: ChiconyE_87:a9:0a (64:5a:04:87:a9:0a)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 203.159.50.27
Transmission Control Protocol, Src Port: 80, Dst Port: 59454, Seq: 1, Ack: 392, Len: 730
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]
        Request Version: HTTP/1.1
        Status Code: 200
        Response Phrase: OK
    Date: Mon, 21 Aug 2017 15:33:36 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Mon, 21 Aug 2017 05:59:01 GMT\r\n
    ETag: "173-5573d2cee73a1"\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: 0.286841777 seconds]
    [Request in frame: 32]
    File Data: 371 bytes
Line-based text data: text/html
    \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
```

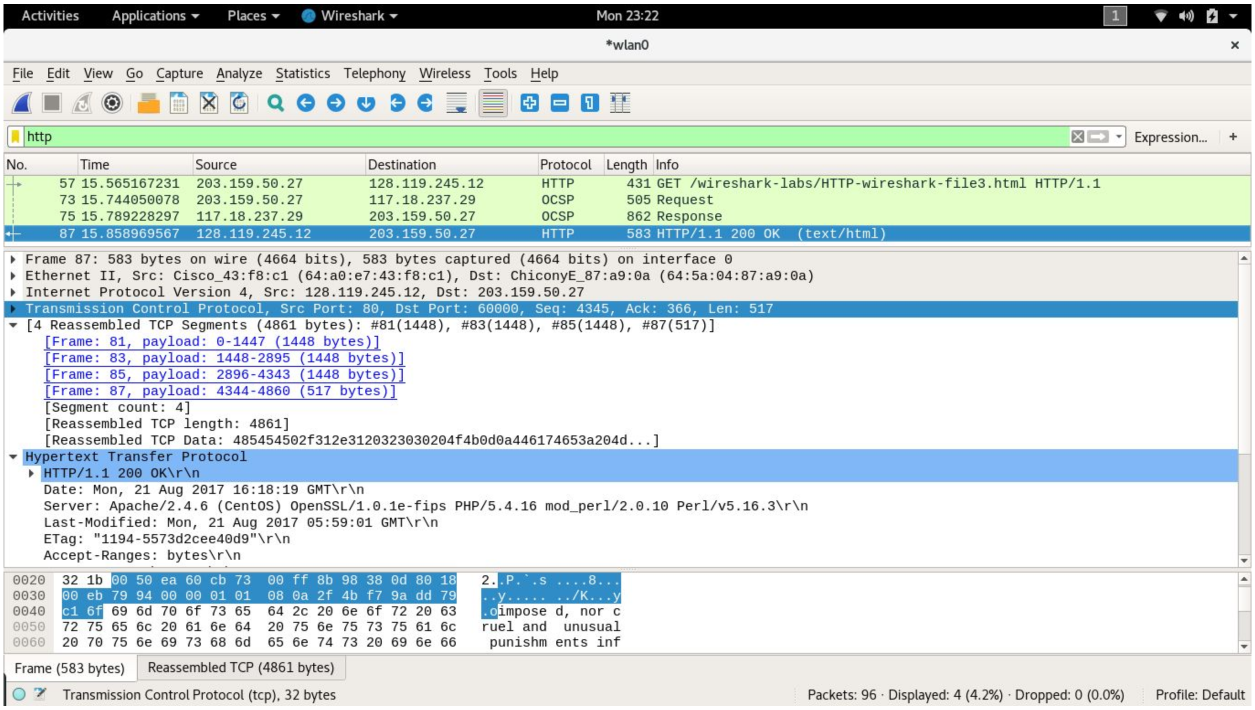
Answer the following questions:

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?

Answer: No

9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
Answer: Yes because the contents in the Line-based text data field are visible.
10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET? If so, what information follows the "IF-MODIFIED-SINCE:" header?
Answer: Yes. The information following is: Mon, 21 Aug 2017 05:59:01 GMT which is the date of the last modification of the file from the previous get request.
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.
Answer: The status code and phrase returned from the server is HTTP/1.1 200 ok.

3. Retrieving Long Documents


Activities
Applications ▾
Places ▾
Wireshark ▾
Mon 23:22
*wlan0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

```
http
```

```
No.   Time            Source          Destination     Protocol Length Info
   57 15.565167231    203.159.50.27   128.119.245.12  HTTP        431 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
   73 15.744050078    203.159.50.27   117.18.237.29   OCSP        505 Request
   75 15.789228297    117.18.237.29   203.159.50.27   OCSP        862 Response
   87 15.858969567    128.119.245.12  203.159.50.27   HTTP        583 HTTP/1.1 200 OK  (text/html)
```

```
▸ Frame 87: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface 0
▸ Ethernet II, Src: Cisco_43:f8:c1 (64:a0:e7:43:f8:c1), Dst: ChiconyE_87:a9:0a (64:5a:04:87:a9:0a)
▸ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 203.159.50.27
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 60000, Seq: 4345, Ack: 366, Len: 517
▾ [4 Reassembled TCP Segments (4861 bytes): #81(1448), #83(1448), #85(1448), #87(517)]
    [Frame: 81, payload: 0-1447 (1448 bytes)]
    [Frame: 83, payload: 1448-2895 (1448 bytes)]
    [Frame: 85, payload: 2896-4343 (1448 bytes)]
    [Frame: 87, payload: 4344-4860 (517 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a204d...]
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Date: Mon, 21 Aug 2017 16:18:19 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Mon, 21 Aug 2017 05:59:01 GMT\r\n
    ETag: "1194-5573d2cee40d9"\r\n
    Accept-Ranges: bytes\r\n
```

```
0020  32 1b 00 50 ea 60 cb 73  00 ff 8b 98 38 0d 80 18   2..P.`.s ....8...
0030  00 eb 79 94 00 00 01 01  08 0a 2f 4b f7 9a dd 79   ..y..... ../K...y
0040  c1 6f 69 6d 70 6f 73 65  64 2c 20 6e 6f 72 20 63   .oimpose d, nor c
0050  72 75 65 6c 20 61 6e 64  20 75 6e 75 73 75 61 6c   ruel and  unusual
0060  20 70 75 6e 69 73 68 6d  65 6e 74 73 20 69 6e 66    punishm ents inf
```

```
Transmission Control Protocol (tcp), 32 bytes          Packets: 96 · Displayed: 4 (4.2%) · Dropped: 0 (0.0%)     Profile: Default
```

Answer the following questions:

12. How many HTTP GET request messages were sent by your browser?

Answer: There was 1 HTTP GET request message sent by my browser as seen in the screenshot.

13. How many data-containing TCP segments were needed to carry the single HTTP
response?

Answer: There were 4 data containing TCP segments containing 1448,1448 ,1448, 571 respectively for a total of 4861 bytes.

14. What is the status code and phrase associated with the response to the HTTP GET

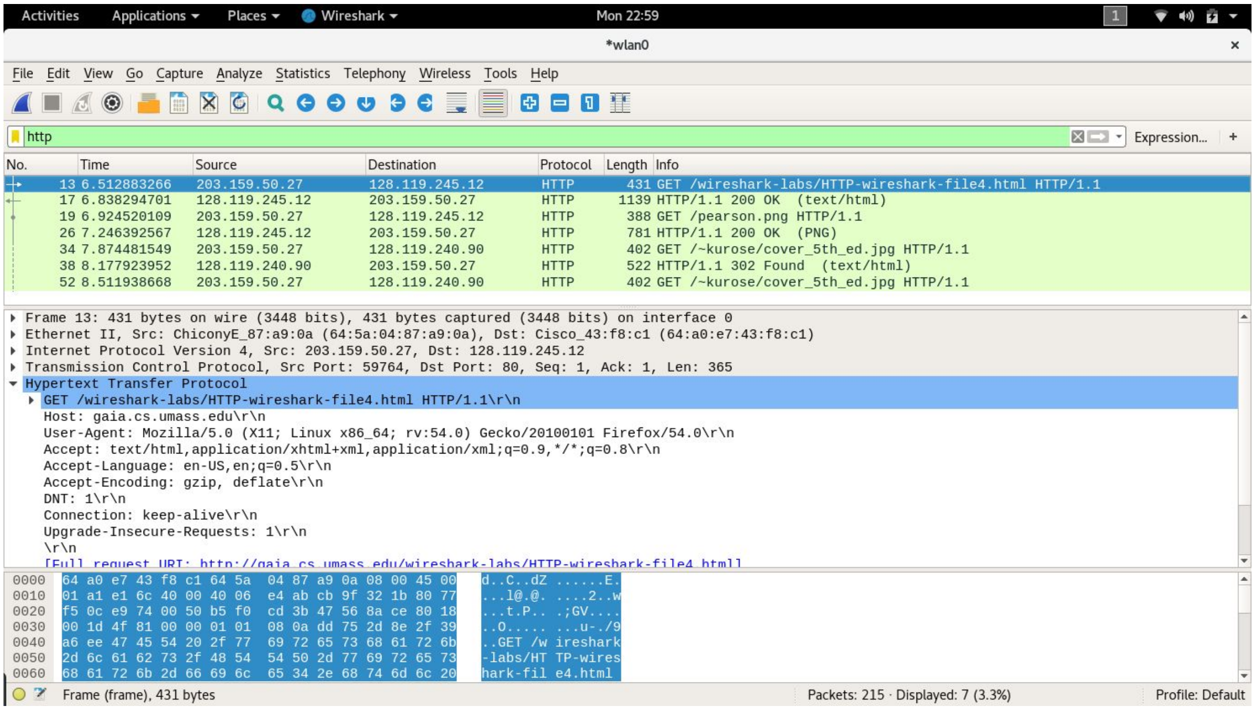
request?

Answer: 200 OK

15. Are there any HTTP status lines in the transmitted data associated with a TCP induced "Continuation"?

Answer: No

4. HTML Documents with Embedded Objects


Activities
Applications
Places
Wireshark
Mon 22:59
*wlan0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
+

No.	Time	Source	Destination	Protocol	Length	Info
13	6.512883266	203.159.50.27	128.119.245.12	HTTP	431	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
17	6.838294701	128.119.245.12	203.159.50.27	HTTP	1139	HTTP/1.1 200 OK (text/html)
19	6.924520109	203.159.50.27	128.119.245.12	HTTP	388	GET /pearson.png HTTP/1.1
26	7.246392567	128.119.245.12	203.159.50.27	HTTP	781	HTTP/1.1 200 OK (PNG)
34	7.874481549	203.159.50.27	128.119.240.90	HTTP	402	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
38	8.177923952	128.119.240.90	203.159.50.27	HTTP	522	HTTP/1.1 302 Found (text/html)
52	8.511938668	203.159.50.27	128.119.240.90	HTTP	402	GET /~kurose/cover_5th_ed.jpg HTTP/1.1

```
▸ Frame 13: 431 bytes on wire (3448 bits), 431 bytes captured (3448 bits) on interface 0
▸ Ethernet II, Src: ChiconyE_87:a9:0a (64:5a:04:87:a9:0a), Dst: Cisco_43:f8:c1 (64:a0:e7:43:f8:c1)
▸ Internet Protocol Version 4, Src: 203.159.50.27, Dst: 128.119.245.12
▸ Transmission Control Protocol, Src Port: 59764, Dst Port: 80, Seq: 1, Ack: 1, Len: 365
▾ Hypertext Transfer Protocol
  ▸ GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:54.0) Gecko/20100101 Firefox/54.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    DNT: 1\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]
```

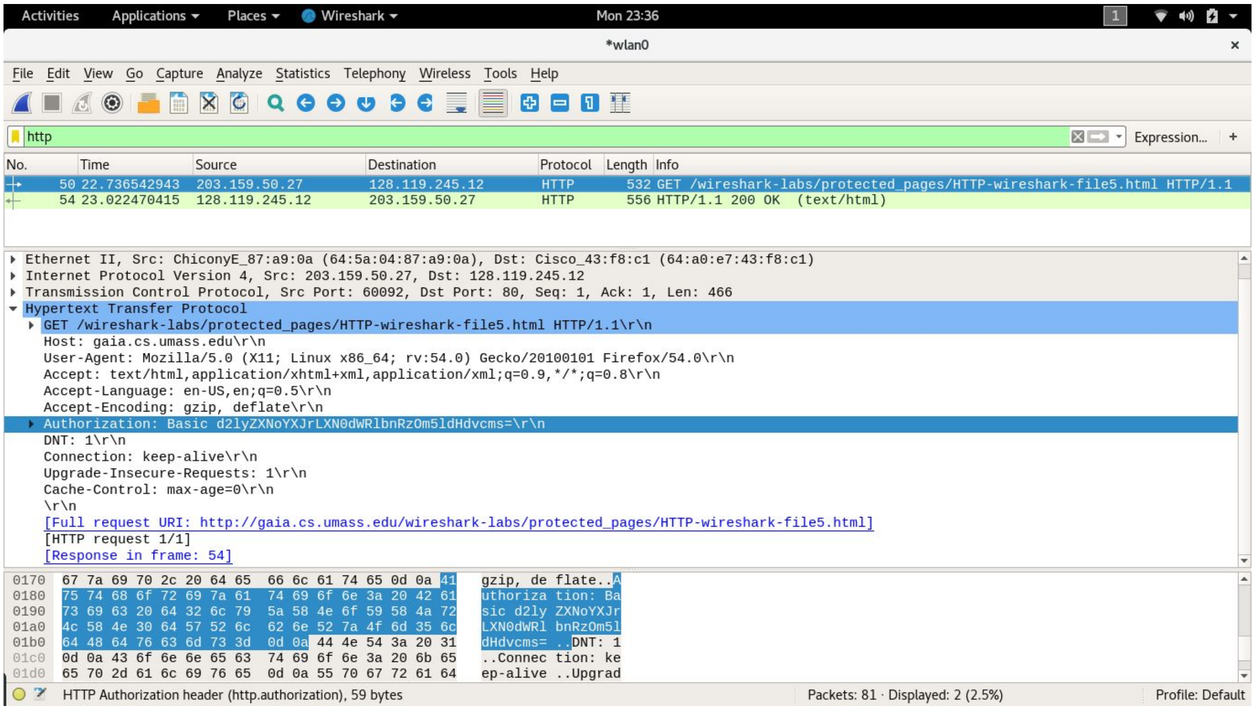
```
0000  64 a0 e7 43 f8 c1 64 5a  04 87 a9 0a 08 00 45 00   d..C..dZ ......E.
0010  01 a1 e1 6c 40 00 40 06  e4 ab cb 9f 32 1b 80 77   ...l@.@. ....2..w
0020  f5 0c e9 74 00 50 b5 f0  cd 3b 47 56 8a ce 80 18   ...t.P.. .;GV....
0030  00 1d 4f 81 00 00 01 01  08 0a dd 75 2d 8e 2f 39   ..O..... ...u-./9
0040  a6 ee 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
```

Frame (frame), 431 bytes | Packets: 215 · Displayed: 7 (3.3%) | Profile: Default

Answer the following questions:

16. How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent?
Answer: The 2 HTTP GET requests sent to the following Internet addresses:
a. 128.119.245.12
b. 128.119.240.90
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.
Answer: By checking the TCP ports the files were downloaded serially or in parallel. Here, 2 images were transmitted over 2 TCP connections therefore they were downloaded serially.

5. HTTP Authentication


Activities
Applications
Places
Wireshark
Mon 23:36
*wlan0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

```
http
```

```
No.   Time          Source          Destination     Protocol  Length Info
   50 22.736542943  203.159.50.27   128.119.245.12  HTTP       532 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
   54 23.022470415  128.119.245.12  203.159.50.27   HTTP       556 HTTP/1.1 200 OK  (text/html)
```

```
▸ Ethernet II, Src: ChiconyE_87:a9:0a (64:5a:04:87:a9:0a), Dst: Cisco_43:f8:c1 (64:a0:e7:43:f8:c1)
▸ Internet Protocol Version 4, Src: 203.159.50.27, Dst: 128.119.245.12
▸ Transmission Control Protocol, Src Port: 60092, Dst Port: 80, Seq: 1, Ack: 1, Len: 466
▾ Hypertext Transfer Protocol
  ▸ GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:54.0) Gecko/20100101 Firefox/54.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
  ▸ Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    DNT: 1\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Cache-Control: max-age=0\r\n
    \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: 54]
```

```
0170  67 7a 69 70 2c 20 64 65  66 6c 61 74 65 0d 0a 41   gzip, de flate..A
0180  75 74 68 6f 72 69 7a 61  74 69 6f 6e 3a 20 42 61   uthoriza tion: Ba
0190  73 69 63 20 64 32 6c 79  5a 58 4e 6f 59 58 4a 72   sic d2ly ZXNoYXJr
01a0  4c 58 4e 30 64 57 52 6c  62 6e 52 7a 4f 6d 35 6c   LXN0dWRl bnRzOm5l
01b0  64 48 64 76 63 6d 73 3d  0d 0a 44 4e 54 3a 20 31   dHdvcms= ..DNT: 1
01c0  0d 0a 43 6f 6e 6e 65 63  74 69 6f 6e 3a 20 6b 65   ..Connec tion: ke
01d0  65 70 2d 61 6c 69 76 65  0d 0a 55 70 67 72 61 64   ep-alive ..Upgrad
```

HTTP Authorization header (http.authorization), 59 bytes | Packets: 81 · Displayed: 2 (2.5%) | Profile: Default

Answer the following questions:

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

Answer: Status code: 401 & Phrase: Authorization Required

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

Answer: the new field is Authorization.

Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=