Part 01:

Here we have 7 questions. The answer of this question are given below…

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

Answer: both of the browser and server are running HTTP version 1.1.

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

Answer: en-US

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

Answer: my IP: 10.0.2.15
gaia.cs.umass.edu IP: 128.119.245.12

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

Answer: 200

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

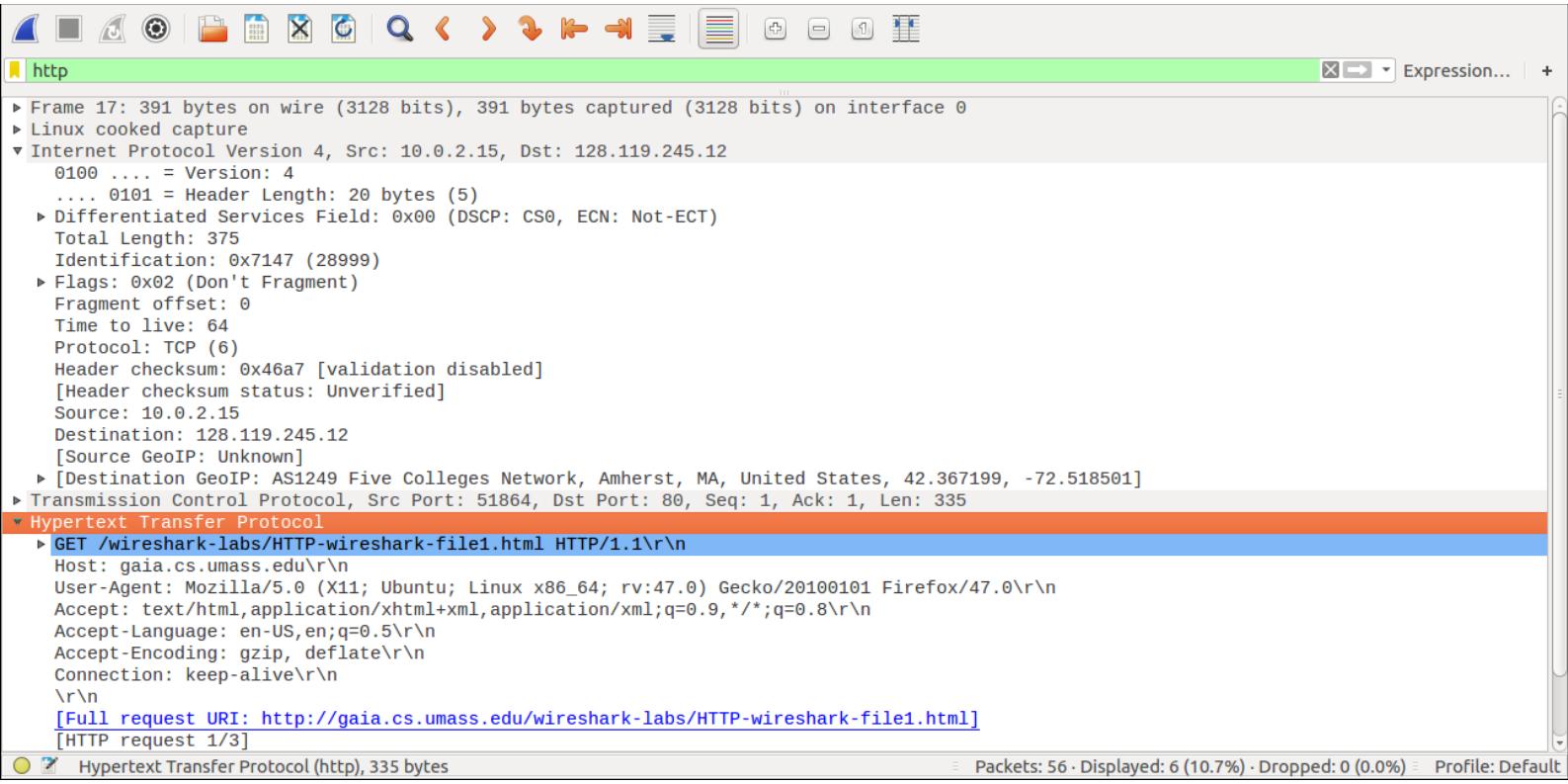
Answer: Mon, 14 Aug 2017 05:59:01 GMT

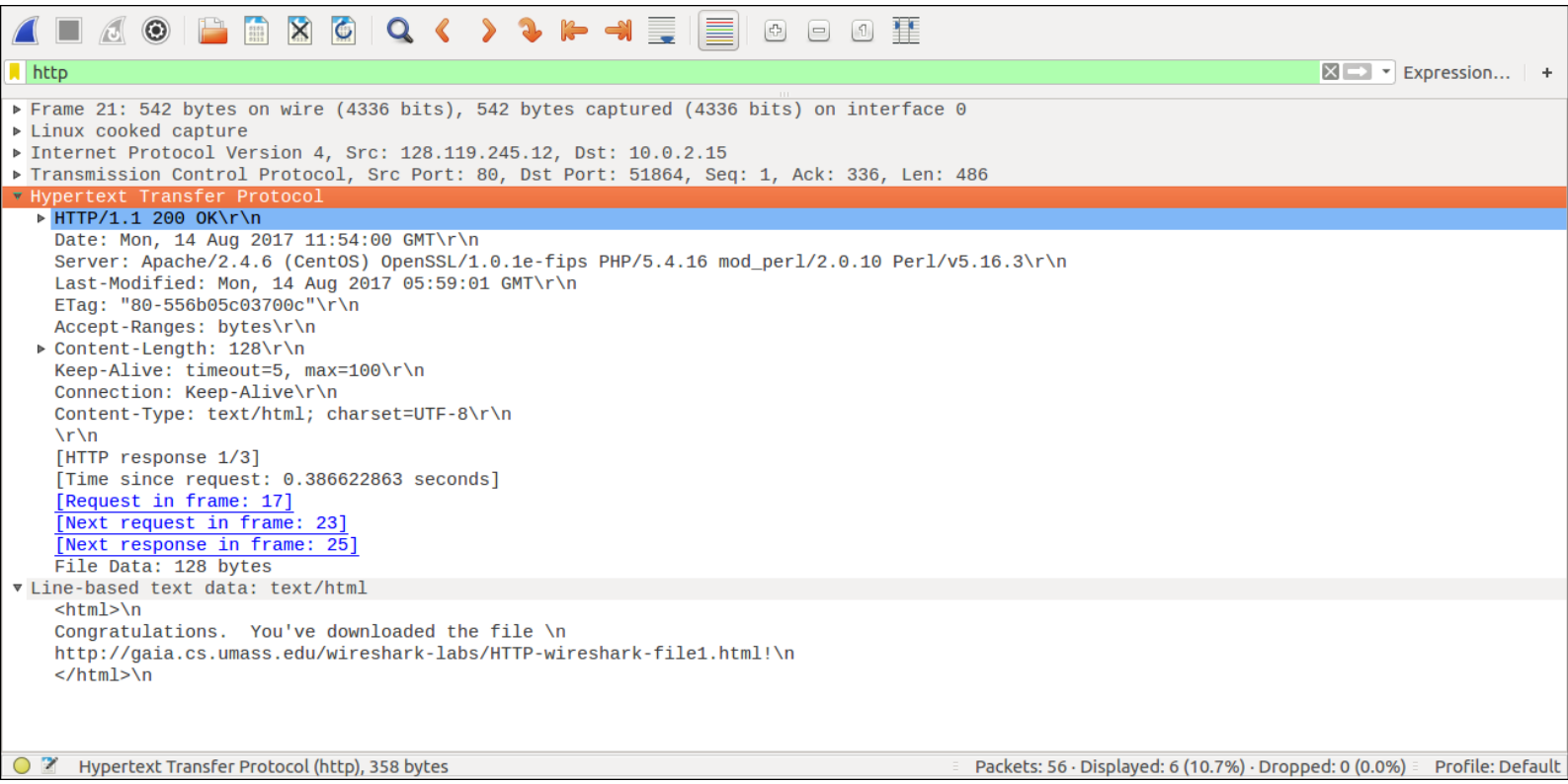
6. How many bytes of content are being returned to your browser?

Answer: 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


http
Expression...
Frame 17: 391 bytes on wire (3128 bits), 391 bytes captured (3128 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.0.2.15, 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: 375
Identification: 0x7147 (28999)
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 64
Protocol: TCP (6)
Header checksum: 0x46a7 [validation disabled]
[Header checksum status: Unverified]
Source: 10.0.2.15
Destination: 128.119.245.12
[Source GeoIP: Unknown]
[Destination GeoIP: AS1249 Five Colleges Network, Amherst, MA, United States, 42.367199, -72.518501]
Transmission Control Protocol, Src Port: 51864, Dst Port: 80, Seq: 1, Ack: 1, Len: 335
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; Ubuntu; Linux x86_64; rv:47.0) Gecko/20100101 Firefox/47.0\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
Connection: keep-alive\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
[HTTP request 1/3]
Hypertext Transfer Protocol (http), 335 bytes
Packets: 56 · Displayed: 6 (10.7%) · Dropped: 0 (0.0%)
Profile: Default


http
Expression...
Frame 21: 542 bytes on wire (4336 bits), 542 bytes captured (4336 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 80, Dst Port: 51864, Seq: 1, Ack: 336, Len: 486
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Mon, 14 Aug 2017 11:54:00 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, 14 Aug 2017 05:59:01 GMT\r\n
ETag: "80-556b05c03700c"\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 1/3]
[Time since request: 0.386622863 seconds]
[Request in frame: 17]
[Next request in frame: 23]
[Next response in frame: 25]
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
Hypertext Transfer Protocol (http), 358 bytes
Packets: 56 · Displayed: 6 (10.7%) · Dropped: 0 (0.0%)
Profile: Default

part 02:

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 “IF-MODIFIED-SINCE” line.

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

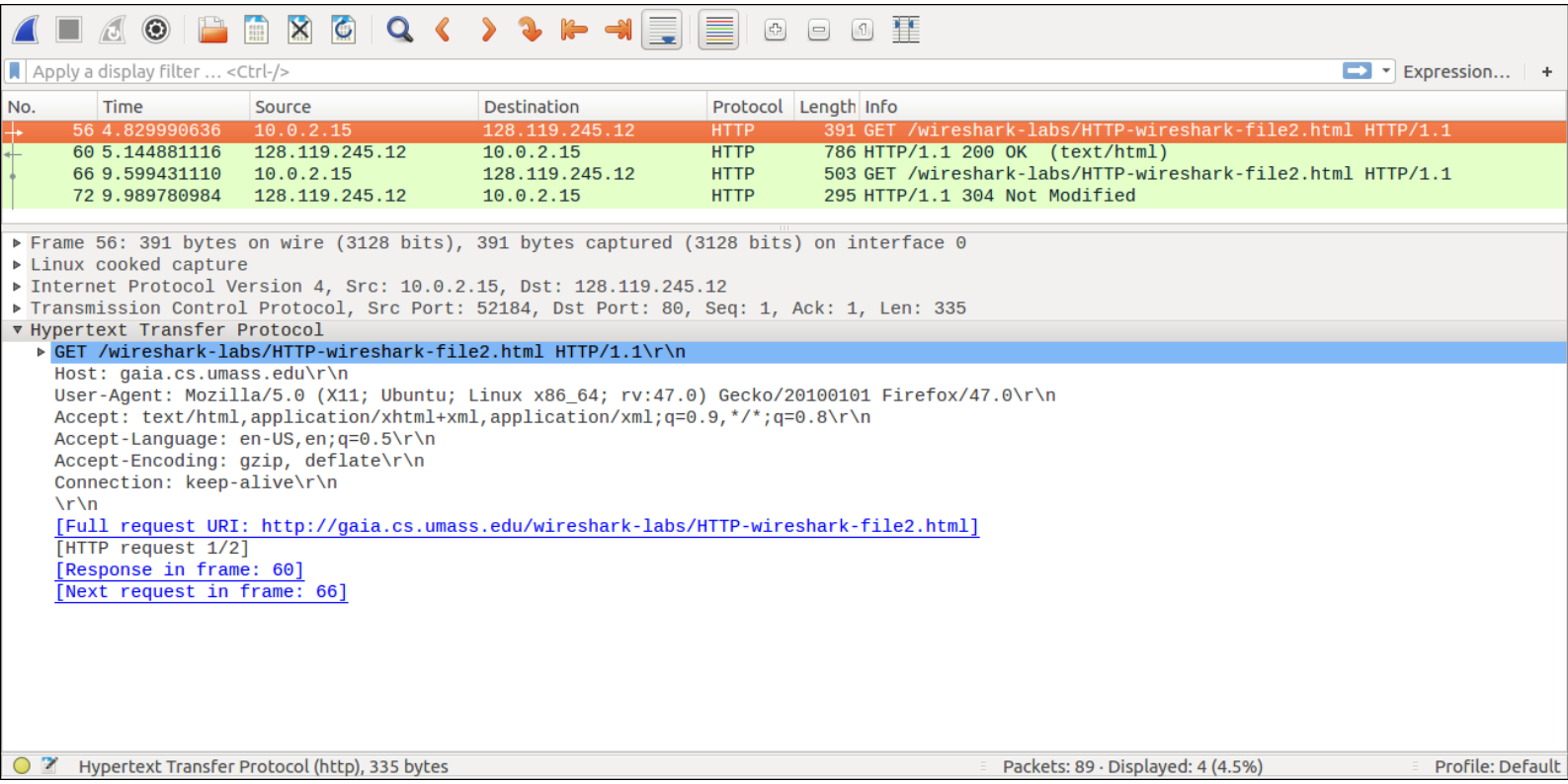
Answer: yes, server return the contents of the file.

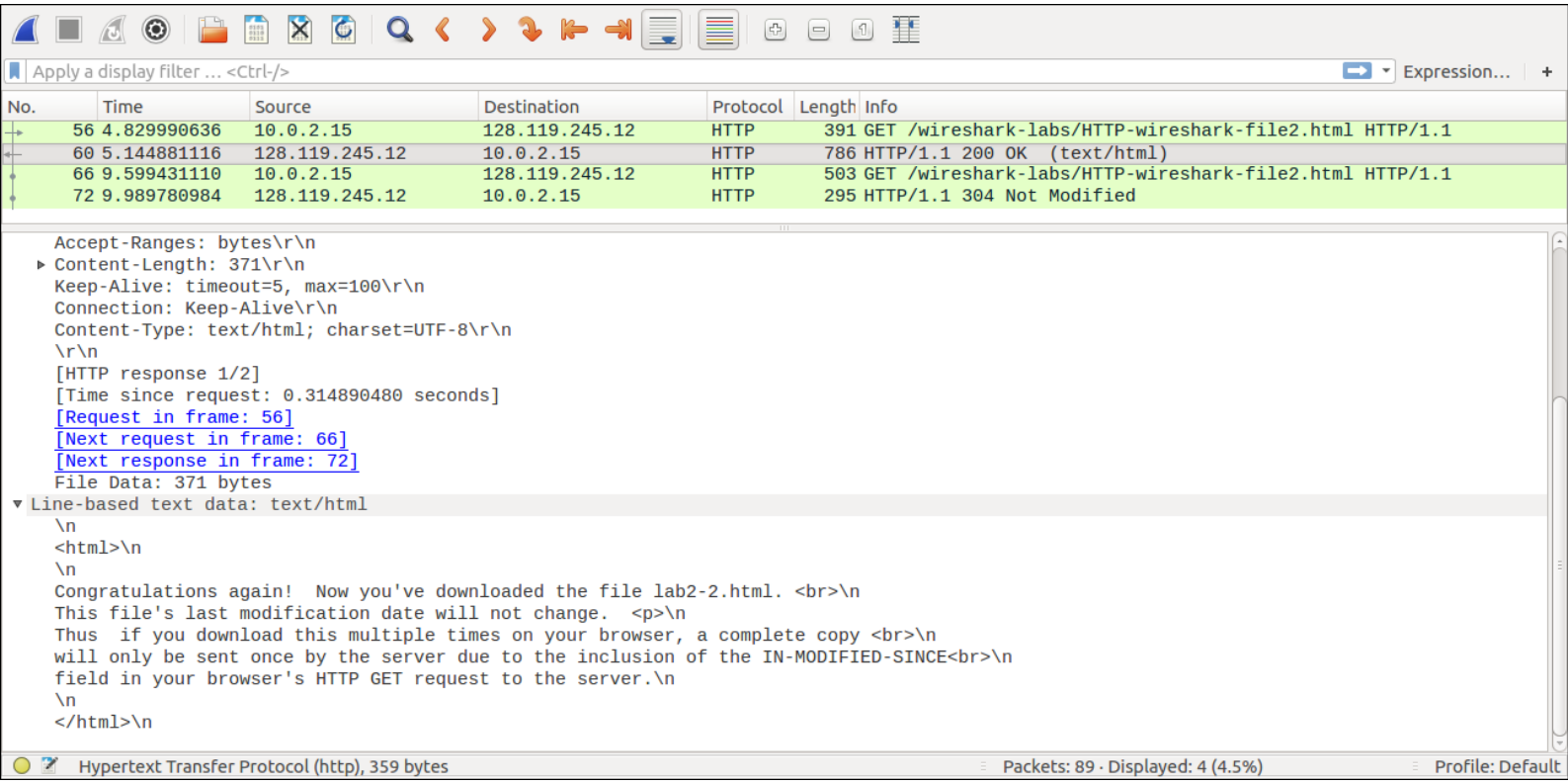
10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” header?

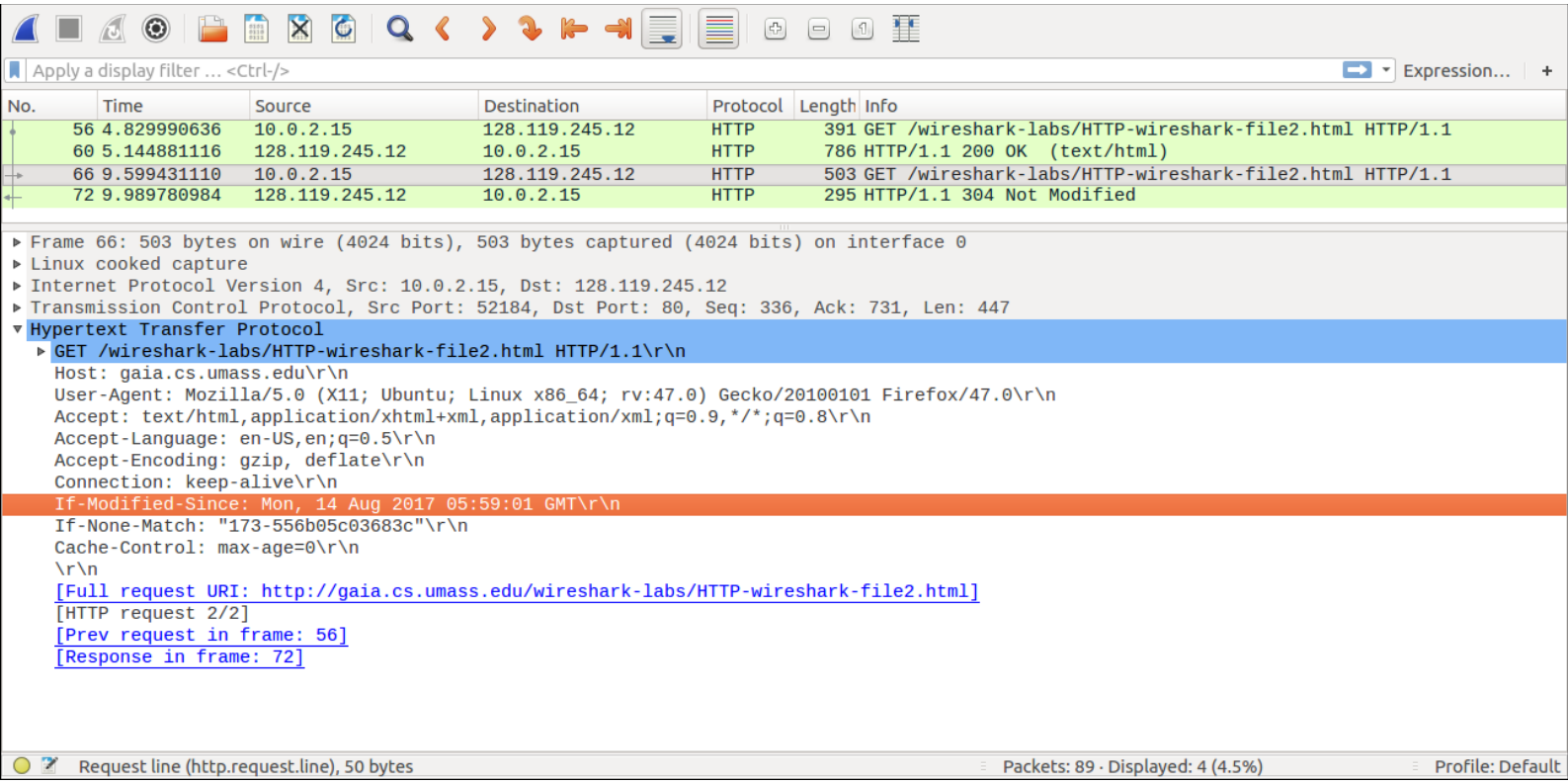
Answer: yes.

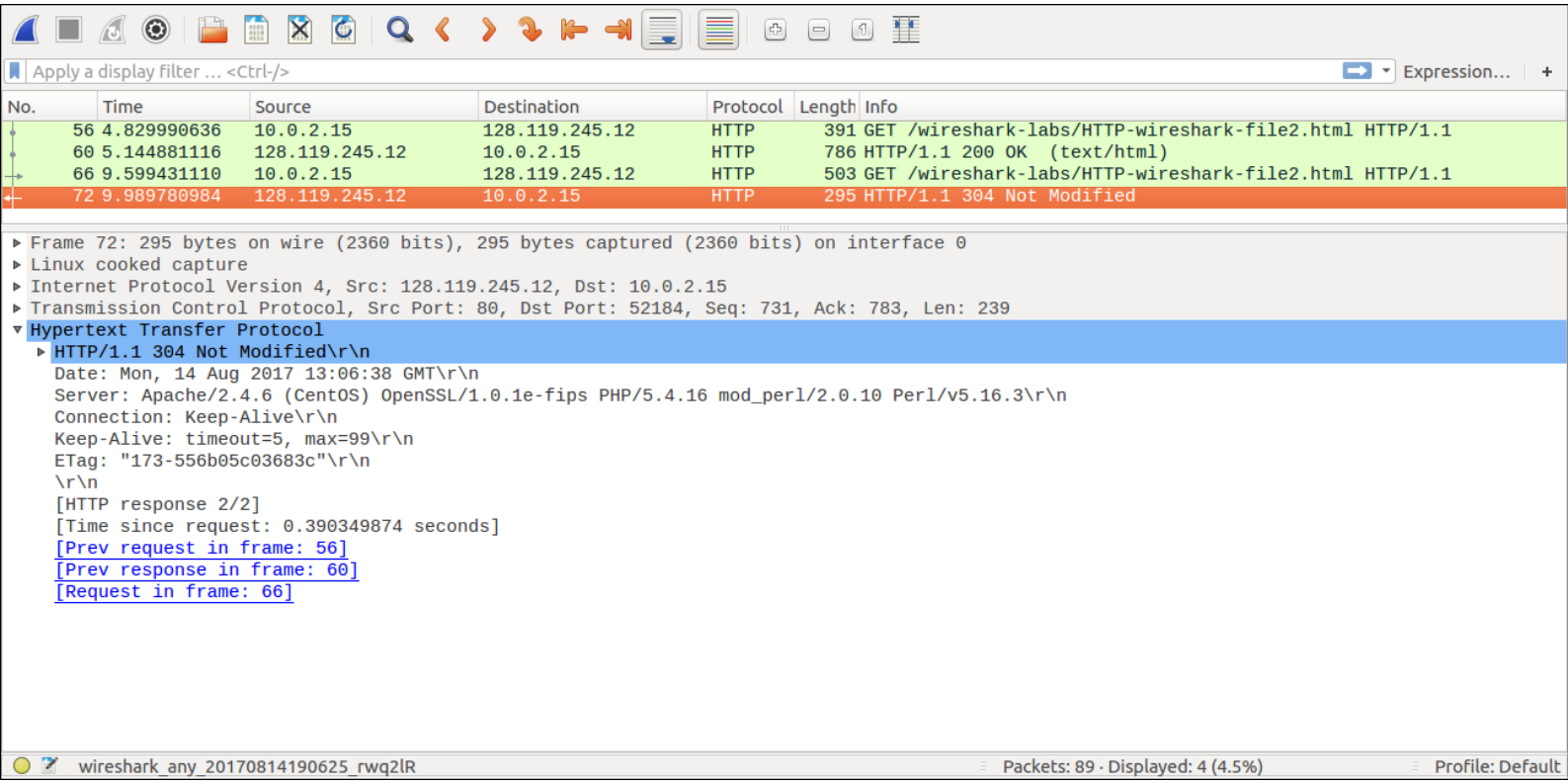
11. What is the HTTP status code and phrase returned from the server in respect to this second HTTP GET? Did the server explicitly return the contents of the file?

Answer: No, the file has not been modified, so the text of the file Is not returned in the HTTP message.




Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
56 4.829990636 10.0.2.15 128.119.245.12 HTTP 391 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
60 5.144881116 128.119.245.12 10.0.2.15 HTTP 786 HTTP/1.1 200 OK (text/html)
66 9.599431110 10.0.2.15 128.119.245.12 HTTP 503 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
72 9.989780984 128.119.245.12 10.0.2.15 HTTP 295 HTTP/1.1 304 Not Modified
Accept-Ranges: bytes\r\n
Content-Length: 371\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 1/2]
[Time since request: 0.314890480 seconds]
[Request in frame: 56]
[Next request in frame: 66]
[Next response in frame: 72]
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.
\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
\n
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE
\n
field in your browser's HTTP GET request to the server.\n
\n
</html>\n
Hypertext Transfer Protocol (http), 359 bytes
Packets: 89 · Displayed: 4 (4.5%)
Profile: Default


Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
56 4.829990636 10.0.2.15 128.119.245.12 HTTP 391 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
60 5.144881116 128.119.245.12 10.0.2.15 HTTP 786 HTTP/1.1 200 OK (text/html)
66 9.599431110 10.0.2.15 128.119.245.12 HTTP 503 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
72 9.989780984 128.119.245.12 10.0.2.15 HTTP 295 HTTP/1.1 304 Not Modified
Frame 66: 503 bytes on wire (4024 bits), 503 bytes captured (4024 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 52184, Dst Port: 80, Seq: 336, Ack: 731, Len: 447
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:47.0) Gecko/20100101 Firefox/47.0\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
Connection: keep-alive\r\n
If-Modified-Since: Mon, 14 Aug 2017 05:59:01 GMT\r\n
If-None-Match: "173-556b05c03683c"\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 2/2]
[Prev request in frame: 56]
[Response in frame: 72]
Request line (http.request.line), 50 bytes
Packets: 89 · Displayed: 4 (4.5%)
Profile: Default


Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
56 4.829990636 10.0.2.15 128.119.245.12 HTTP 391 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
60 5.144881116 128.119.245.12 10.0.2.15 HTTP 786 HTTP/1.1 200 OK (text/html)
66 9.599431110 10.0.2.15 128.119.245.12 HTTP 503 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
72 9.989780984 128.119.245.12 10.0.2.15 HTTP 295 HTTP/1.1 304 Not Modified
Frame 72: 295 bytes on wire (2360 bits), 295 bytes captured (2360 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 80, Dst Port: 52184, Seq: 731, Ack: 783, Len: 239
Hypertext Transfer Protocol
HTTP/1.1 304 Not Modified\r\n
Date: Mon, 14 Aug 2017 13:06:38 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
Connection: Keep-Alive\r\n
Keep-Alive: timeout=5, max=99\r\n
ETag: "173-556b05c03683c"\r\n
\r\n
[HTTP response 2/2]
[Time since request: 0.390349874 seconds]
[Prev request in frame: 56]
[Prev response in frame: 60]
[Request in frame: 66]
wireshark_any_20170814190625_rwq2lR
Packets: 89 · Displayed: 4 (4.5%)
Profile: Default

Part 03:

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?

Answer: 1 HTTP GET request. In my case, packet number 13 contains the GET message.

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

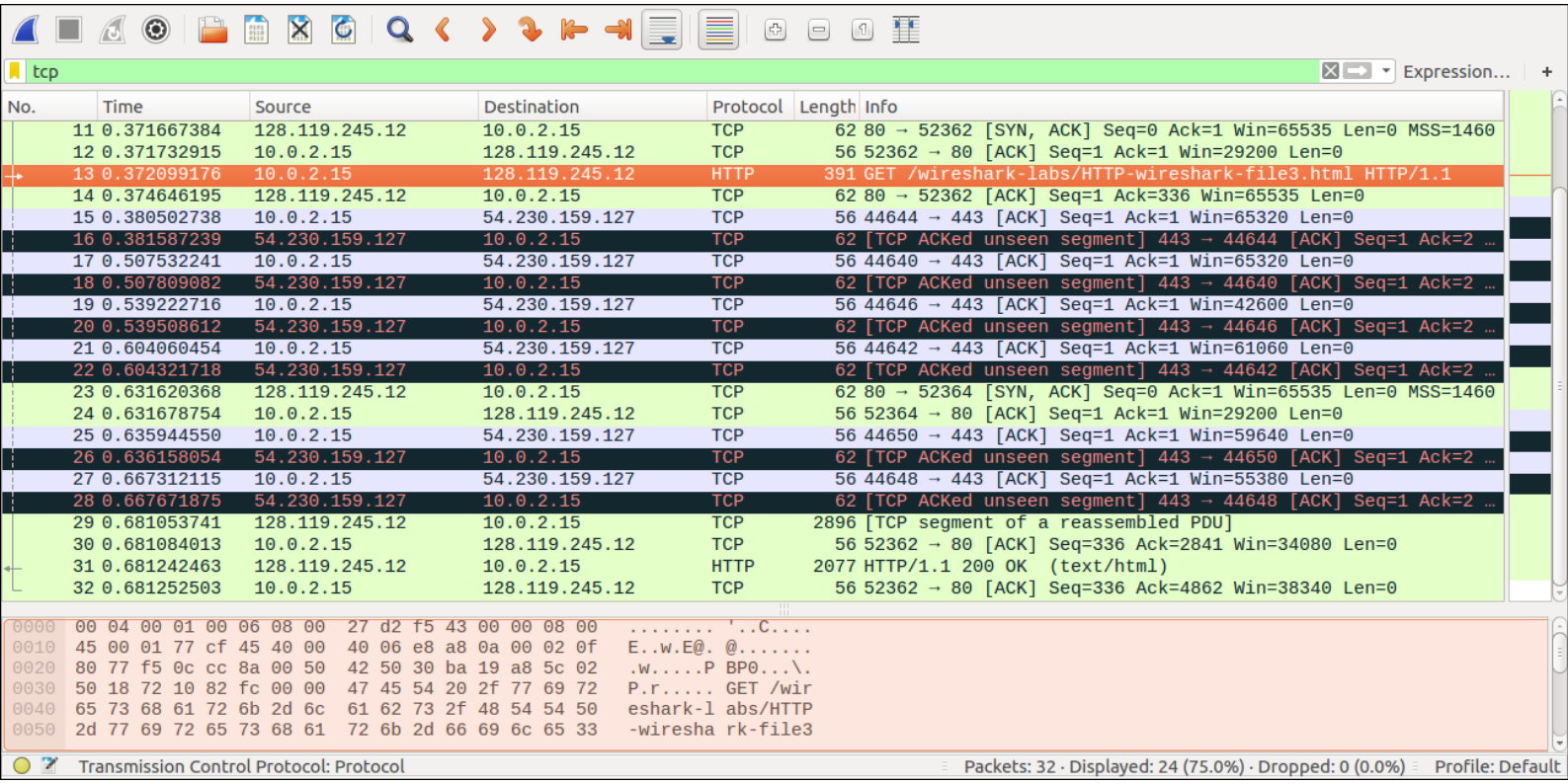
Answer: packet number 31.

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

Answer: 200 OK.

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

Answer: 3 TCP segments needed. They are in packet 14,23,29.



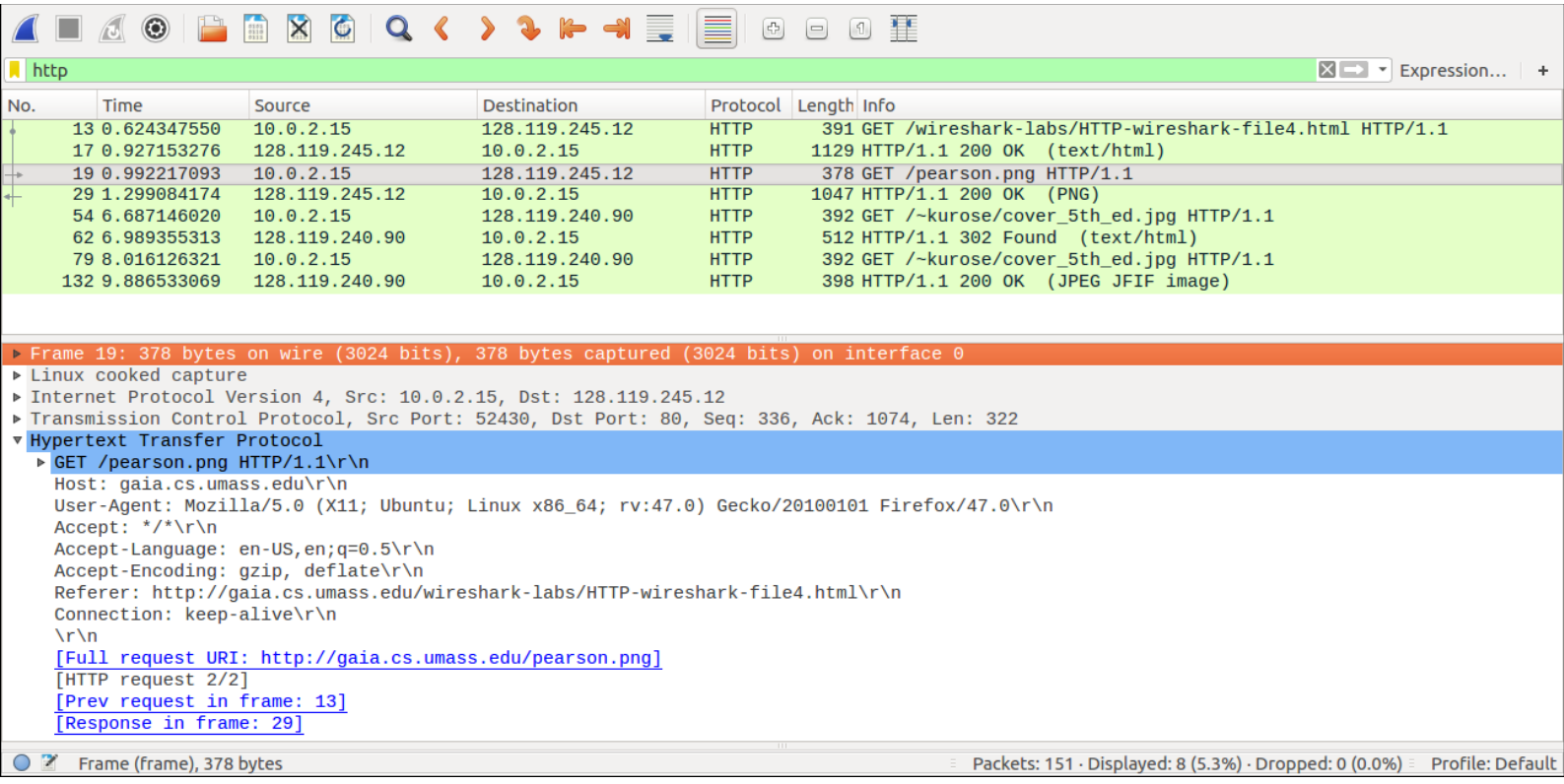
part 04

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

Answer: There are 4 HTTP GET request messages that my browser send.
First one sent to: 128.119.245.12
second one sent to: 128.119.245.12
third one sent to : 128.119.240.90
fourth one sent to: 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: The downloads occurred in serially. Here we see, first request for image in packet 19 and its response in packet 29. After that second request for image in packet 54 and its response in packet 62. So, after downloading first image, second image is downloaded. So, here downloads occurred in serially.



Part 05

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

Answer: First HTTP GET request in the packet 23. In the packet 27 server response with status code 401 and phrase Unauthorized.

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

Answer: The HTTP GET includes the *Authorization: Basic: field*