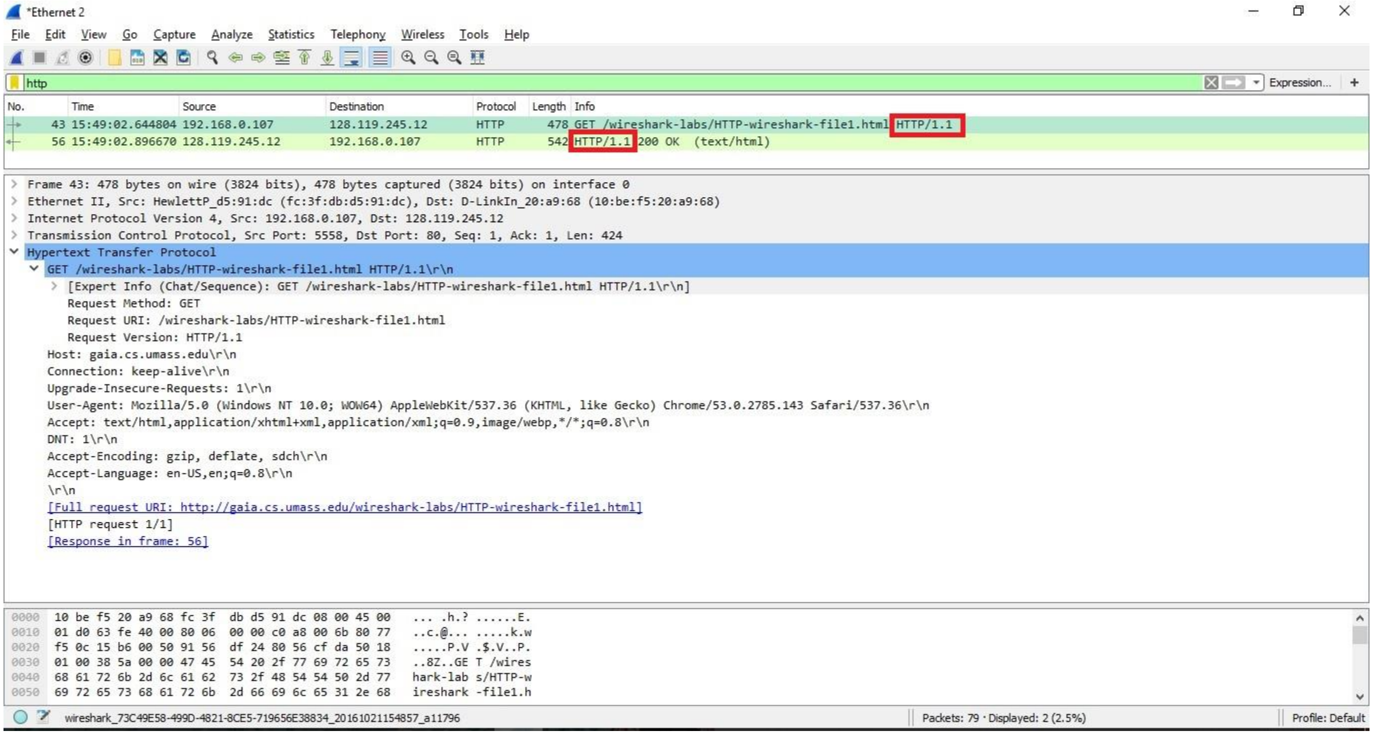
Jessica Spokoyny
Oct 21, 2016
CS 372 – Lab 2

Lab 2

1. The Basic HTTP GET/response interaction

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

Both my browser and the server are running HTTP 1.1


*Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
+

```
No.     Time             Source          Destination     Protocol  Length Info
    43 15:49:02.644804 192.168.0.107   128.119.245.12  HTTP      478 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
    56 15:49:02.896670 128.119.245.12  192.168.0.107   HTTP      542 HTTP/1.1 200 OK  (text/html)
```

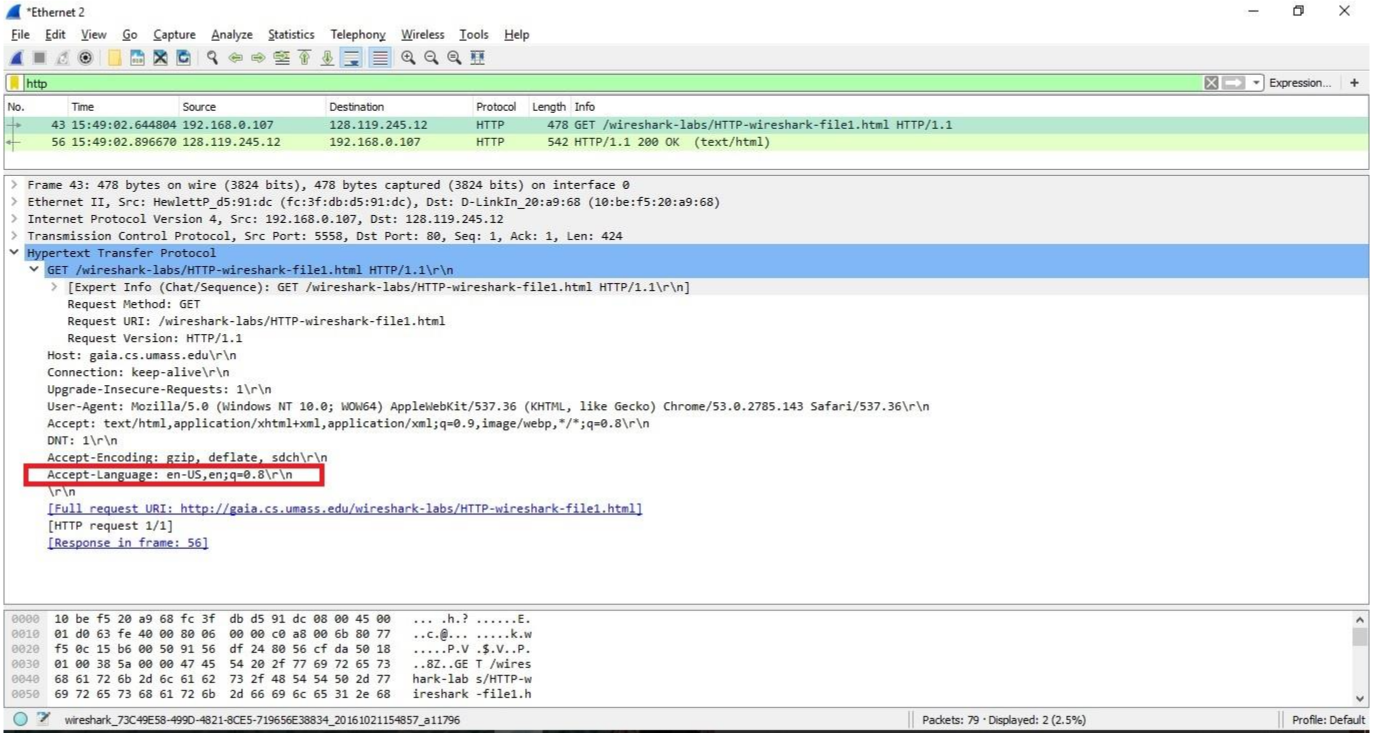
```
> Frame 43: 478 bytes on wire (3824 bits), 478 bytes captured (3824 bits) on interface 0
> Ethernet II, Src: HewlettP_d5:91:dc (fc:3f:db:d5:91:dc), Dst: D-LinkIn_20:a9:68 (10:be:f5:20:a9:68)
> Internet Protocol Version 4, Src: 192.168.0.107, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 5558, Dst Port: 80, Seq: 1, Ack: 1, Len: 424
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    DNT: 1\r\n
    Accept-Encoding: gzip, deflate, sdch\r\n
    Accept-Language: en-US,en;q=0.8\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: 56]
```

```
0000  10 be f5 20 a9 68 fc 3f  db d5 91 dc 08 00 45 00   ... .h.? ......E.
0010  01 d0 63 fe 40 00 80 06  00 00 c0 a8 00 6b 80 77   ..c.@... .....k.w
0020  f5 0c 15 b6 00 50 91 56  df 24 80 56 cf da 50 18   .....P.V .$.V..P.
0030  01 00 38 5a 00 00 47 45  54 20 2f 77 69 72 65 73   ..8Z..GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 31 2e 68   ireshark -file1.h
```

```
wireshark_73C49E58-499D-4821-8CE5-719656E38834_20161021154857_a11796    Packets: 79 · Displayed: 2 (2.5%)    Profile: Default
```

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

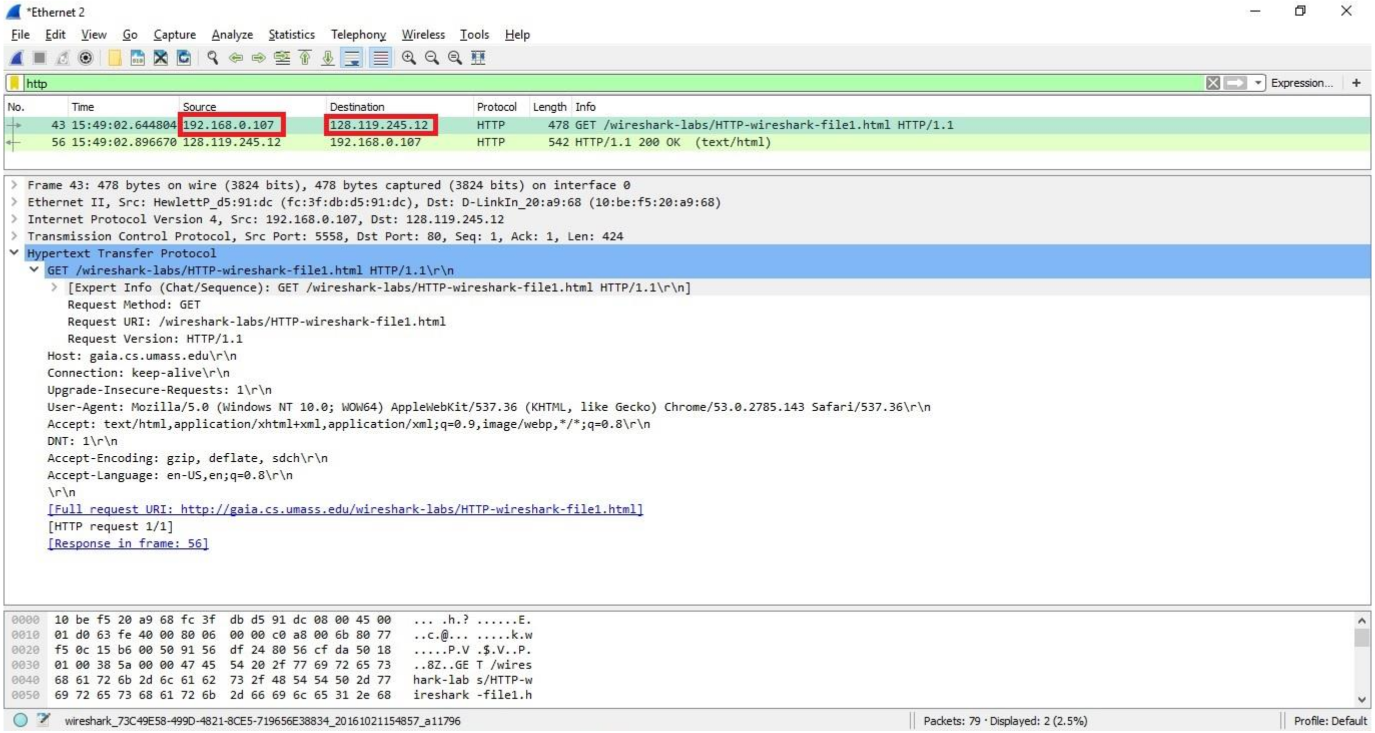
My browser indicates that it can accept English-US and English languages


*Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

```
http

No.    Time             Source           Destination      Protocol  Length Info
    43 15:49:02.644804 192.168.0.107    128.119.245.12   HTTP         478 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
    56 15:49:02.896670 128.119.245.12   192.168.0.107    HTTP         542 HTTP/1.1 200 OK  (text/html)

> Frame 43: 478 bytes on wire (3824 bits), 478 bytes captured (3824 bits) on interface 0
> Ethernet II, Src: HewlettP_d5:91:dc (fc:3f:db:d5:91:dc), Dst: D-LinkIn_20:a9:68 (10:be:f5:20:a9:68)
> Internet Protocol Version 4, Src: 192.168.0.107, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 5558, Dst Port: 80, Seq: 1, Ack: 1, Len: 424
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    DNT: 1\r\n
    Accept-Encoding: gzip, deflate, sdch\r\n
    Accept-Language: en-US,en;q=0.8\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: 56]

0000  10 be f5 20 a9 68 fc 3f  db d5 91 dc 08 00 45 00   ... .h.? ......E.
0010  01 d0 63 fe 40 00 80 06  00 00 c0 a8 00 6b 80 77   ..c.@... .....k.w
0020  f5 0c 15 b6 00 50 91 56  df 24 80 56 cf da 50 18   .....P.V .$.V..P.
0030  01 00 38 5a 00 00 47 45  54 20 2f 77 69 72 65 73   ..8Z..GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 31 2e 68   ireshark -file1.h

wireshark_73C49E58-499D-4821-8CE5-719656E38834_20161021154857_a11796    Packets: 79 · Displayed: 2 (2.5%)    Profile: Default
```

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

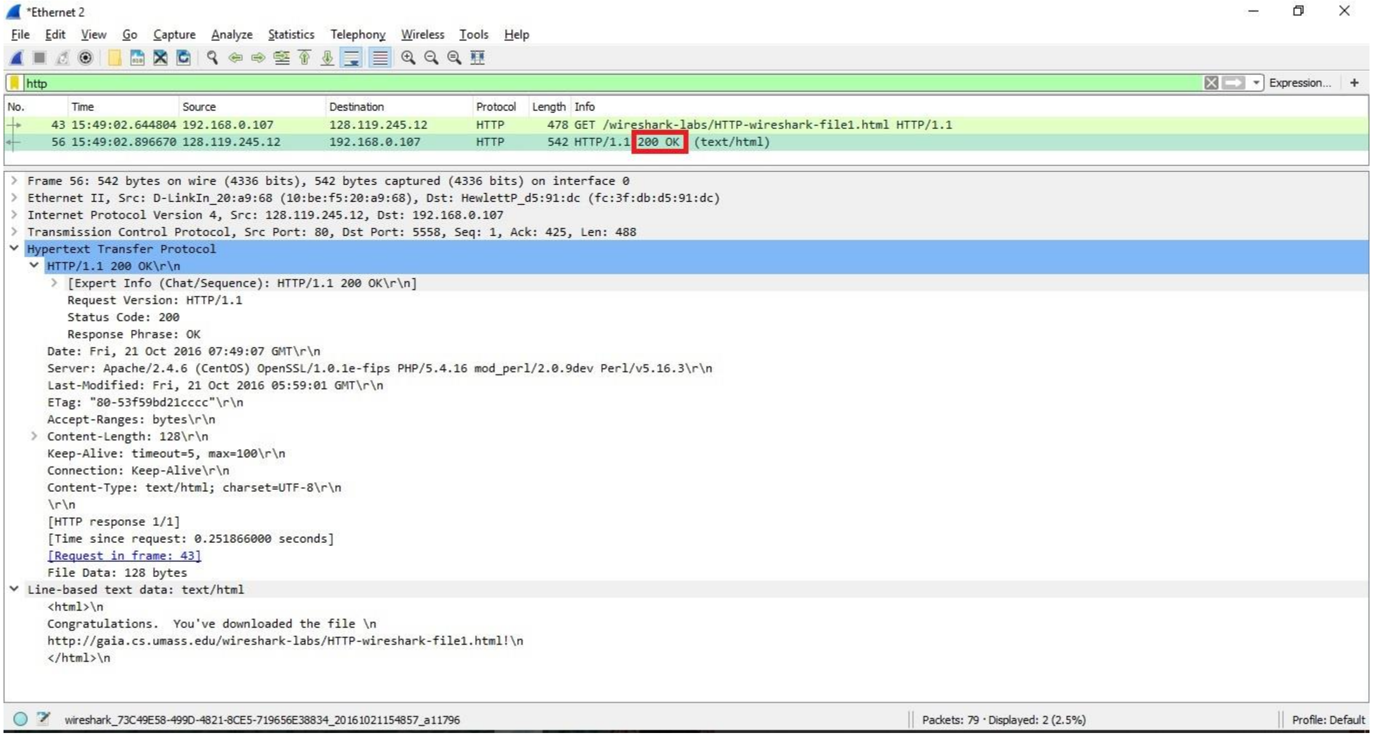
My browser's IP address is: 192.168.0.107
The gaia.cs.umass.edu server's IP address is: 128.119.245.12


*Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

```
http

No.    Time             Source           Destination      Protocol  Length Info
    43 15:49:02.644804 192.168.0.107    128.119.245.12   HTTP         478 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
    56 15:49:02.896670 128.119.245.12   192.168.0.107    HTTP         542 HTTP/1.1 200 OK  (text/html)

> Frame 43: 478 bytes on wire (3824 bits), 478 bytes captured (3824 bits) on interface 0
> Ethernet II, Src: HewlettP_d5:91:dc (fc:3f:db:d5:91:dc), Dst: D-LinkIn_20:a9:68 (10:be:f5:20:a9:68)
> Internet Protocol Version 4, Src: 192.168.0.107, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 5558, Dst Port: 80, Seq: 1, Ack: 1, Len: 424
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    DNT: 1\r\n
    Accept-Encoding: gzip, deflate, sdch\r\n
    Accept-Language: en-US,en;q=0.8\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: 56]

0000  10 be f5 20 a9 68 fc 3f  db d5 91 dc 08 00 45 00   ... .h.? ......E.
0010  01 d0 63 fe 40 00 80 06  00 00 c0 a8 00 6b 80 77   ..c.@... .....k.w
0020  f5 0c 15 b6 00 50 91 56  df 24 80 56 cf da 50 18   .....P.V .$.V..P.
0030  01 00 38 5a 00 00 47 45  54 20 2f 77 69 72 65 73   ..8Z..GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 31 2e 68   ireshark -file1.h

wireshark_73C49E58-499D-4821-8CE5-719656E38834_20161021154857_a11796    Packets: 79 · Displayed: 2 (2.5%)    Profile: Default
```

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

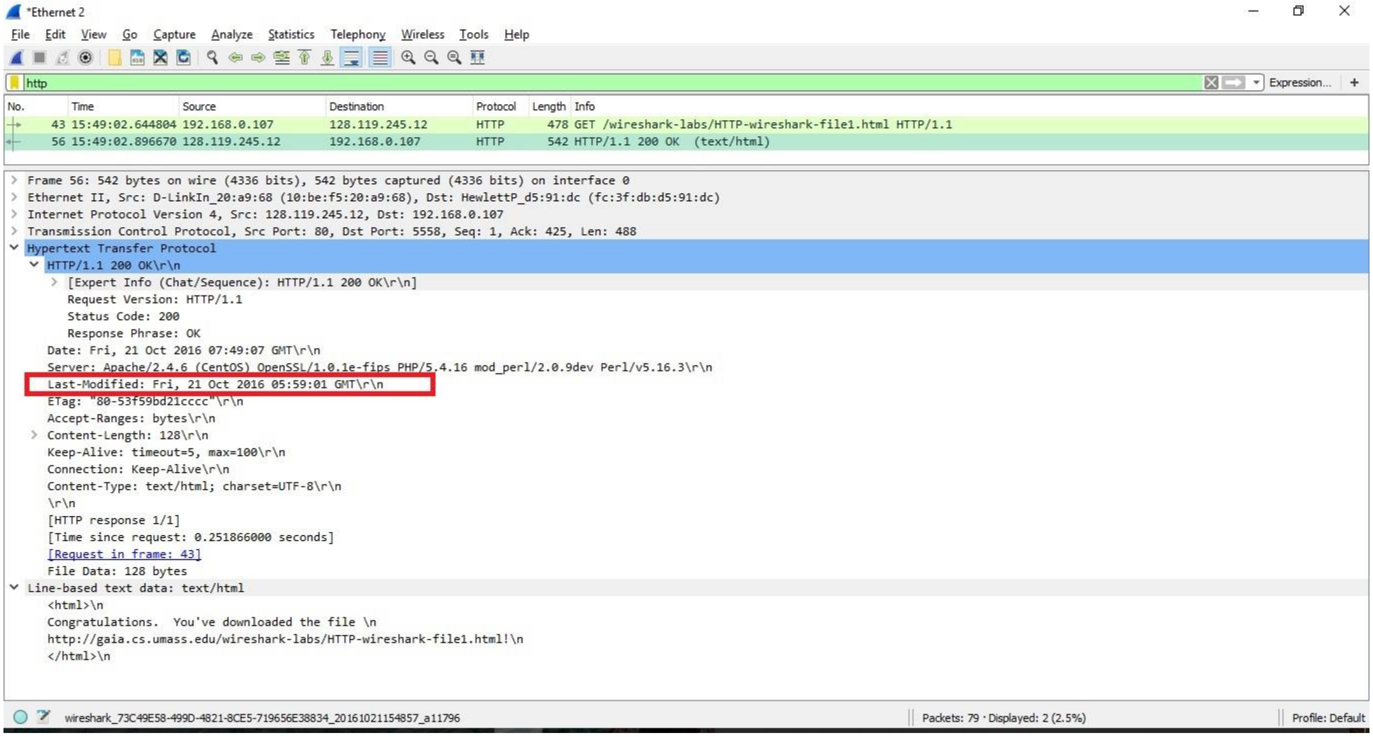
The status code returned from the server to my browser is: 200 OK


*Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+
Packets: 79 · Displayed: 2 (2.5%)
Profile: Default

```
http

No.  Time             Source           Destination      Protocol  Length  Info
  43 15:49:02.644804  192.168.0.107    128.119.245.12   HTTP         478  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  56 15:49:02.896670  128.119.245.12   192.168.0.107    HTTP         542  HTTP/1.1 200 OK  (text/html)

> Frame 56: 542 bytes on wire (4336 bits), 542 bytes captured (4336 bits) on interface 0
> Ethernet II, Src: D-LinkIn_20:a9:68 (10:be:f5:20:a9:68), Dst: HewlettP_d5:91:dc (fc:3f:db:d5:91:dc)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.107
> Transmission Control Protocol, Src Port: 80, Dst Port: 5558, Seq: 1, Ack: 425, Len: 488
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Request Version: HTTP/1.1
      Status Code: 200
      Response Phrase: OK
    Date: Fri, 21 Oct 2016 07:49:07 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n
    Last-Modified: Fri, 21 Oct 2016 05:59:01 GMT\r\n
    ETag: "80-53f59bd21cccc"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.251866000 seconds]
    [Request in frame: 43]
    File Data: 128 bytes
v 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

wireshark_73C49E58-499D-4821-8CE5-719656E38834_20161021154857_a11796
```

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

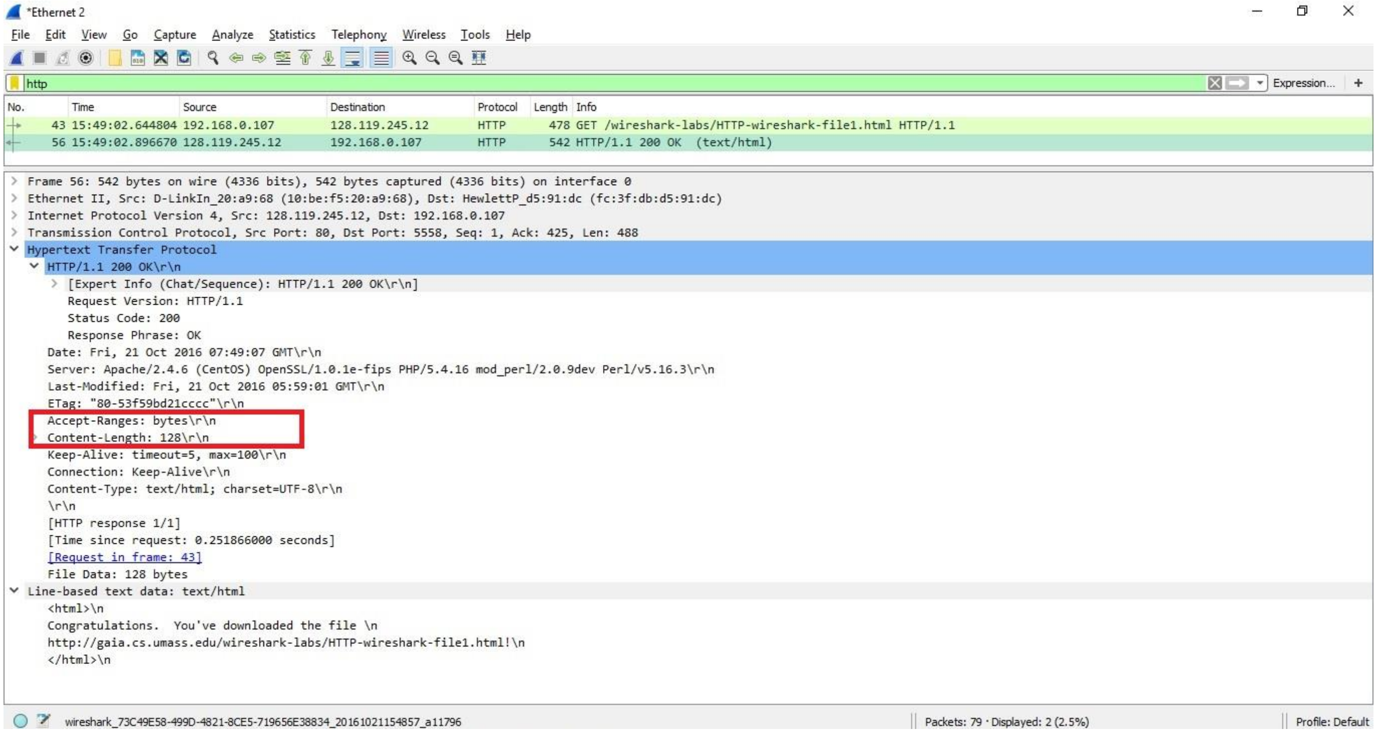
The HTML file was last modified at the server at: Fri, 21 Oct 2016 05:59:01 GMT


*Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+
Packets: 79 · Displayed: 2 (2.5%)
Profile: Default

```
http

No.  Time             Source           Destination      Protocol  Length  Info
  43 15:49:02.644804  192.168.0.107    128.119.245.12   HTTP         478  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  56 15:49:02.896670  128.119.245.12   192.168.0.107    HTTP         542  HTTP/1.1 200 OK  (text/html)

> Frame 56: 542 bytes on wire (4336 bits), 542 bytes captured (4336 bits) on interface 0
> Ethernet II, Src: D-LinkIn_20:a9:68 (10:be:f5:20:a9:68), Dst: HewlettP_d5:91:dc (fc:3f:db:d5:91:dc)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.107
> Transmission Control Protocol, Src Port: 80, Dst Port: 5558, Seq: 1, Ack: 425, Len: 488
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Request Version: HTTP/1.1
      Status Code: 200
      Response Phrase: OK
    Date: Fri, 21 Oct 2016 07:49:07 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n
    Last-Modified: Fri, 21 Oct 2016 05:59:01 GMT\r\n
    ETag: "80-53f59bd21cccc"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.251866000 seconds]
    [Request in frame: 43]
    File Data: 128 bytes
v 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

wireshark_73C49E58-499D-4821-8CE5-719656E38834_20161021154857_a11796
```

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

The length of the content returned to my browser is: 128 bytes


*Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
+

```
No.   Time             Source          Destination     Protocol Length Info
   43 15:49:02.644804 192.168.0.107   128.119.245.12  HTTP      478 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
   56 15:49:02.896670 128.119.245.12  192.168.0.107   HTTP      542 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 56: 542 bytes on wire (4336 bits), 542 bytes captured (4336 bits) on interface 0
> Ethernet II, Src: D-LinkIn_20:a9:68 (10:be:f5:20:a9:68), Dst: HewlettP_d5:91:dc (fc:3f:db:d5:91:dc)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.107
> Transmission Control Protocol, Src Port: 80, Dst Port: 5558, Seq: 1, Ack: 425, Len: 488
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Request Version: HTTP/1.1
      Status Code: 200
      Response Phrase: OK
    Date: Fri, 21 Oct 2016 07:49:07 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n
    Last-Modified: Fri, 21 Oct 2016 05:59:01 GMT\r\n
    ETag: "80-53f59bd21cccc"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.251866000 seconds]
    [Request in frame: 43]
    File Data: 128 bytes
v 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
```

wireshark_73C49E58-499D-4821-8CE5-719656E38834_20161021154857_a11796 | Packets: 79 · Displayed: 2 (2.5%) | Profile: Default

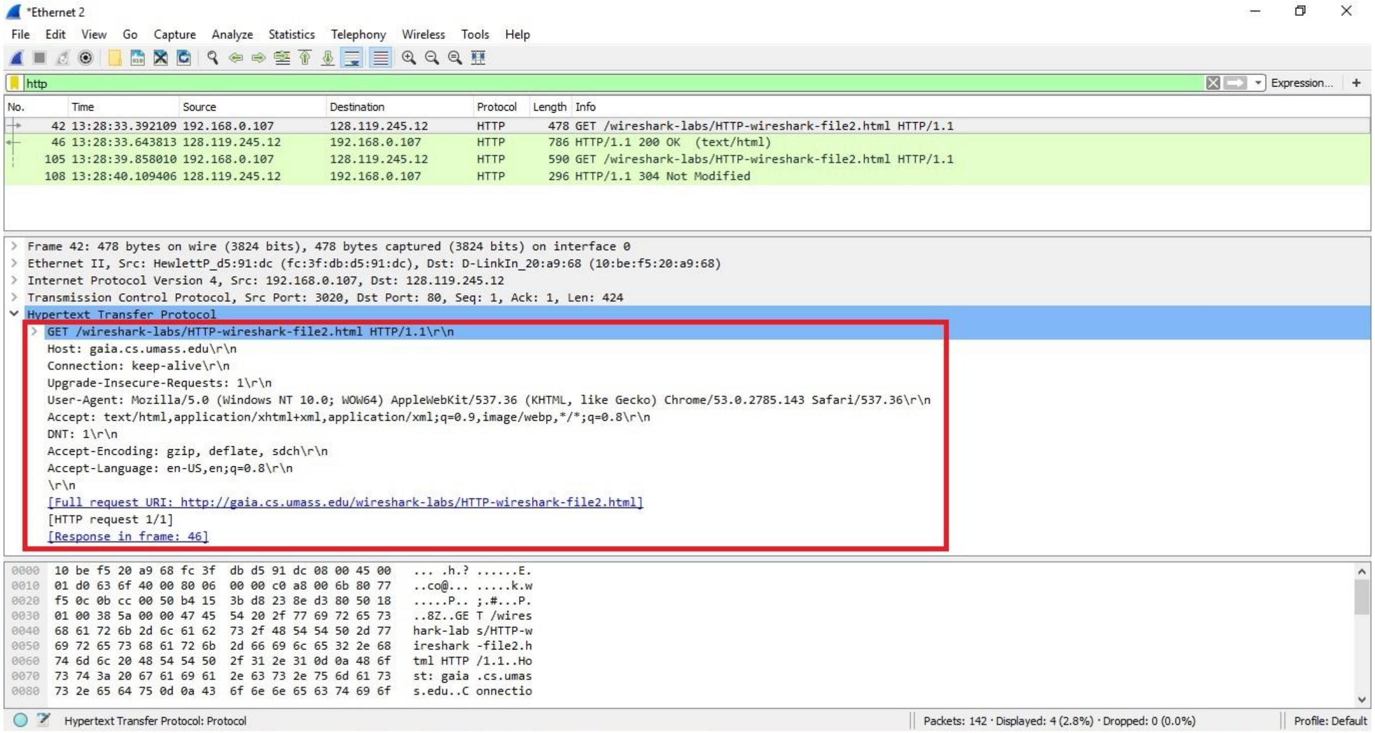
7. **By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.**

No, all of the headers displayed within the data are displayed in the packet-listing window

2. The HTTP CONDITIONAL GET/response interaction

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

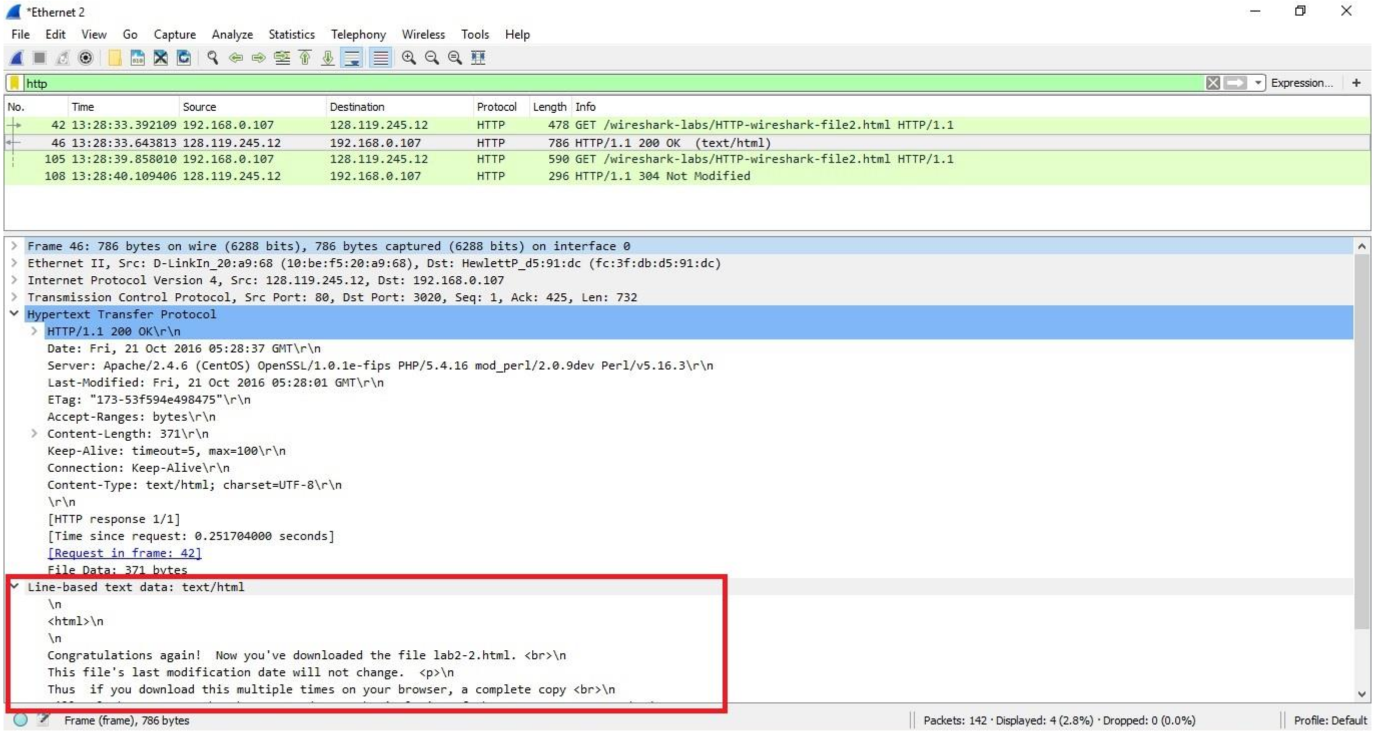
No, there isn’t an “IF-MODIFIED-SINCE” line in the HTTP GET


*Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

```
http

No.  Time            Source          Destination     Protocol Length Info
  42 13:28:33.392109 192.168.0.107   128.119.245.12  HTTP     478 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  46 13:28:33.643813 128.119.245.12  192.168.0.107   HTTP     786 HTTP/1.1 200 OK  (text/html)
 105 13:28:39.858010 192.168.0.107   128.119.245.12  HTTP     590 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 108 13:28:40.109406 128.119.245.12  192.168.0.107   HTTP     296 HTTP/1.1 304 Not Modified

> Frame 42: 478 bytes on wire (3824 bits), 478 bytes captured (3824 bits) on interface 0
> Ethernet II, Src: HewlettP_d5:91:dc (fc:3f:db:d5:91:dc), Dst: D-LinkIn_20:a9:68 (10:be:f5:20:a9:68)
> Internet Protocol Version 4, Src: 192.168.0.107, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 3020, Dst Port: 80, Seq: 1, Ack: 1, Len: 424
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    DNT: 1\r\n
    Accept-Encoding: gzip, deflate, sdch\r\n
    Accept-Language: en-US,en;q=0.8\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: 46]

0000  10 be f5 20 a9 68 fc 3f  db d5 91 dc 08 00 45 00   ... .h.? ......E.
0010  01 d0 63 6f 40 00 80 06  00 00 c0 a8 00 6b 80 77   ..co@... .....k.w
0020  f5 0c 0b cc 00 50 b4 15  3b d8 23 8e d3 80 50 18   .....P.. ;.#...P.
0030  01 00 38 5a 00 00 47 45  54 20 2f 77 69 72 65 73   ..8Z..GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 32 2e 68   ireshark -file2.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1..Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu..C onnectio

Hypertext Transfer Protocol: Protocol    Packets: 142 · Displayed: 4 (2.8%) · Dropped: 0 (0.0%)    Profile: Default
```

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

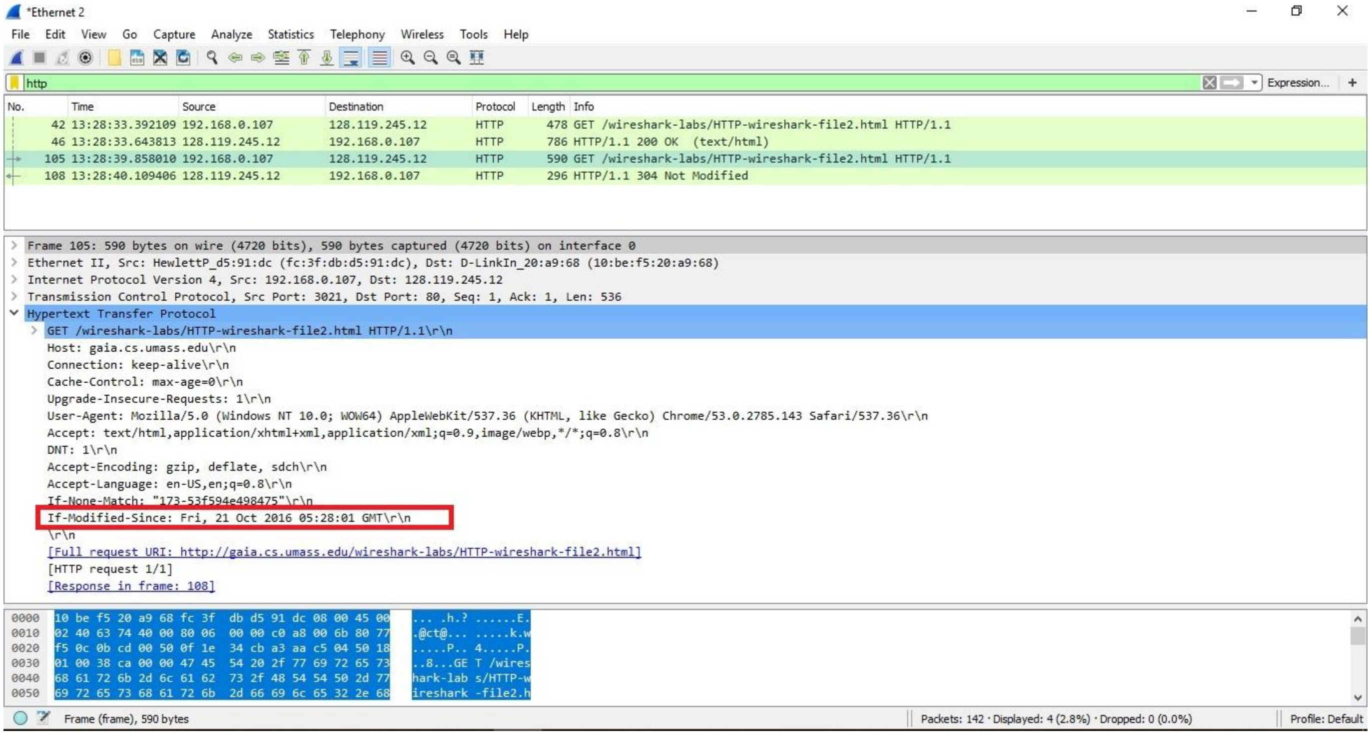
Yes, the server explicitly returned the contents of the file and I can tell because the contents are shown in the "Line-based text data" field


*Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

```
http

No.  Time            Source          Destination     Protocol Length Info
  42 13:28:33.392109 192.168.0.107   128.119.245.12  HTTP     478 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  46 13:28:33.643813 128.119.245.12  192.168.0.107   HTTP     786 HTTP/1.1 200 OK  (text/html)
 105 13:28:39.858010 192.168.0.107   128.119.245.12  HTTP     590 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 108 13:28:40.109406 128.119.245.12  192.168.0.107   HTTP     296 HTTP/1.1 304 Not Modified

> Frame 46: 786 bytes on wire (6288 bits), 786 bytes captured (6288 bits) on interface 0
> Ethernet II, Src: D-LinkIn_20:a9:68 (10:be:f5:20:a9:68), Dst: HewlettP_d5:91:dc (fc:3f:db:d5:91:dc)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.107
> Transmission Control Protocol, Src Port: 80, Dst Port: 3020, Seq: 1, Ack: 425, Len: 732
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Fri, 21 Oct 2016 05:28:37 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n
    Last-Modified: Fri, 21 Oct 2016 05:28:01 GMT\r\n
    ETag: "173-53f594e498475"\r\n
    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 1/1]
    [Time since request: 0.251704000 seconds]
    [Request in frame: 42]
    File Data: 371 bytes
v 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

Frame (frame), 786 bytes    Packets: 142 · Displayed: 4 (2.8%) · Dropped: 0 (0.0%)    Profile: Default
```

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?**

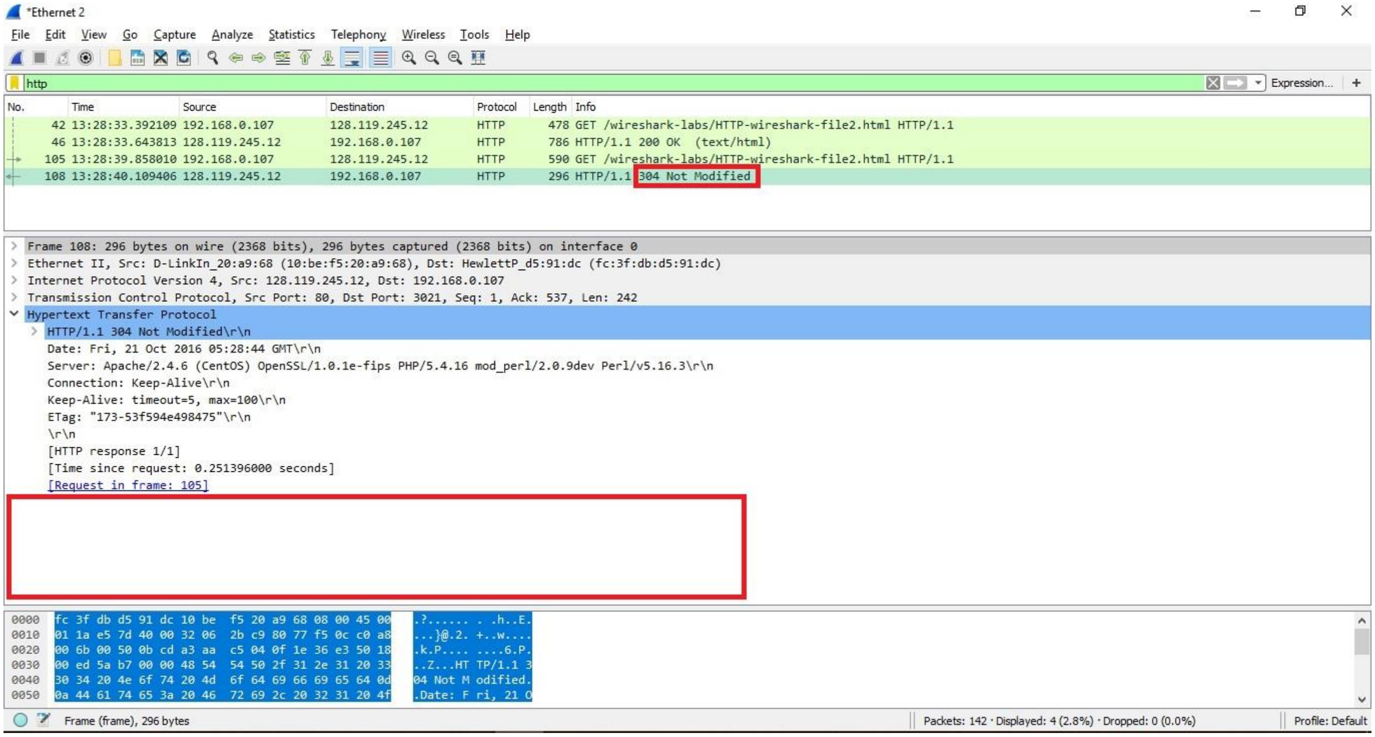
Yes, there is an "IF-MODIFIED-SINCE:" line in the second HTTP GET and the information following the header is: Fri, 21 Oct 2016 05:28:01 GMT


*Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...

```
No.   Time            Source          Destination     Protocol Length Info
   42 13:28:33.392109 192.168.0.107   128.119.245.12  HTTP      478 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   46 13:28:33.643813 128.119.245.12  192.168.0.107   HTTP      786 HTTP/1.1 200 OK  (text/html)
  105 13:28:39.858010 192.168.0.107   128.119.245.12  HTTP      590 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  108 13:28:40.109406 128.119.245.12  192.168.0.107   HTTP      296 HTTP/1.1 304 Not Modified

> Frame 105: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface 0
> Ethernet II, Src: HewlettP_d5:91:dc (fc:3f:db:d5:91:dc), Dst: D-LinkIn_20:a9:68 (10:be:f5:20:a9:68)
> Internet Protocol Version 4, Src: 192.168.0.107, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 3021, Dst Port: 80, Seq: 1, Ack: 1, Len: 536
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    DNT: 1\r\n
    Accept-Encoding: gzip, deflate, sdch\r\n
    Accept-Language: en-US,en;q=0.8\r\n
    If-None-Match: "173-53f594e498475"\r\n
    If-Modified-Since: Fri, 21 Oct 2016 05:28:01 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/1]
    [Response in frame: 108]

0000  10 be f5 20 a9 68 fc 3f  db d5 91 dc 08 00 45 00   ... .h.? ......E.
0010  02 40 63 74 40 00 80 06  00 00 c0 a8 00 6b 80 77   .@ct@... .....k.w
0020  f5 0c 0b cd 00 50 0f 1e  34 cb a3 aa c5 04 50 18   .....P.. 4.....P.
0030  01 00 38 ca 00 00 47 45  54 20 2f 77 69 72 65 73   ..8...GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 32 2e 68   ireshark -file2.h

Frame (frame), 590 bytes    Packets: 142 · Displayed: 4 (2.8%) · Dropped: 0 (0.0%)    Profile: Default
```

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.

The status code and phrase returned from the server in response to the second HTTP GET is: 304 Not Modified. No, the server did not explicitly return the contents of the file as they were loaded by the browser from cache.

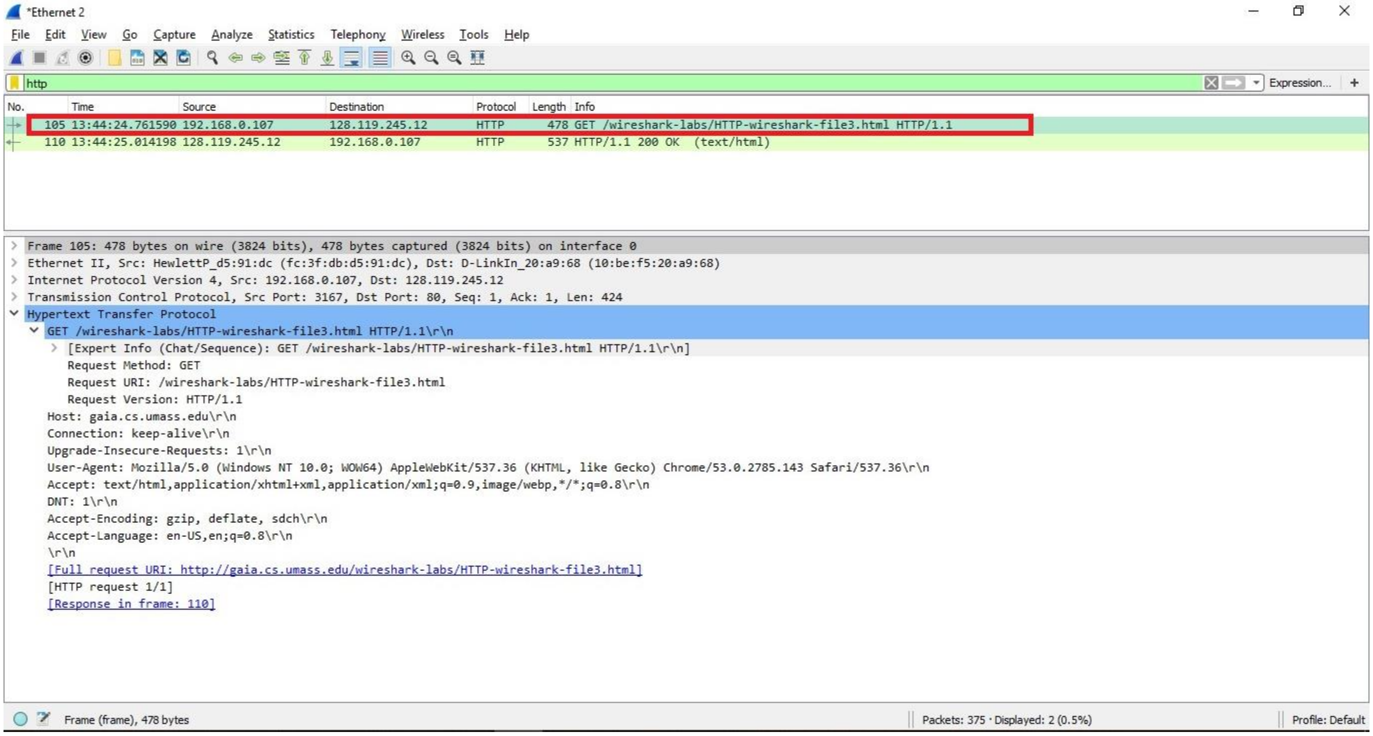

*Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...

```
No.   Time            Source          Destination     Protocol Length Info
   42 13:28:33.392109 192.168.0.107   128.119.245.12  HTTP      478 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   46 13:28:33.643813 128.119.245.12  192.168.0.107   HTTP      786 HTTP/1.1 200 OK  (text/html)
  105 13:28:39.858010 192.168.0.107   128.119.245.12  HTTP      590 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  108 13:28:40.109406 128.119.245.12  192.168.0.107   HTTP      296 HTTP/1.1 304 Not Modified

> Frame 108: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits) on interface 0
> Ethernet II, Src: D-LinkIn_20:a9:68 (10:be:f5:20:a9:68), Dst: HewlettP_d5:91:dc (fc:3f:db:d5:91:dc)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.107
> Transmission Control Protocol, Src Port: 80, Dst Port: 3021, Seq: 1, Ack: 537, Len: 242
v Hypertext Transfer Protocol
  > HTTP/1.1 304 Not Modified\r\n
    Date: Fri, 21 Oct 2016 05:28:44 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "173-53f594e498475"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.251396000 seconds]
    [Request in frame: 105]

0000  fc 3f db d5 91 dc 10 be  f5 20 a9 68 08 00 45 00   .?...... . .h..E.
0010  01 1a e5 7d 40 00 32 06  2b c9 80 77 f5 0c c0 a8   ...}@.2. +..w....
0020  00 6b 00 50 0b cd a3 aa  c5 04 0f 1e 36 e3 50 18   .k.P.... ....6.P.
0030  00 ed 5a b7 00 00 48 54  54 50 2f 31 2e 31 20 33   ..Z...HT TP/1.1 3
0040  30 34 20 4e 6f 74 20 4d  6f 64 69 66 69 65 64 0d   04 Not M odified.
0050  0a 44 61 74 65 3a 20 46  72 69 2c 20 32 31 20 4f   .Date: F ri, 21 O

Frame (frame), 296 bytes    Packets: 142 · Displayed: 4 (2.8%) · Dropped: 0 (0.0%)    Profile: Default
```

3. Retrieving Long Documents

12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

My browser sent 1 HTTP GET request message. The packet that contained the GET message is 105.



```
http
```

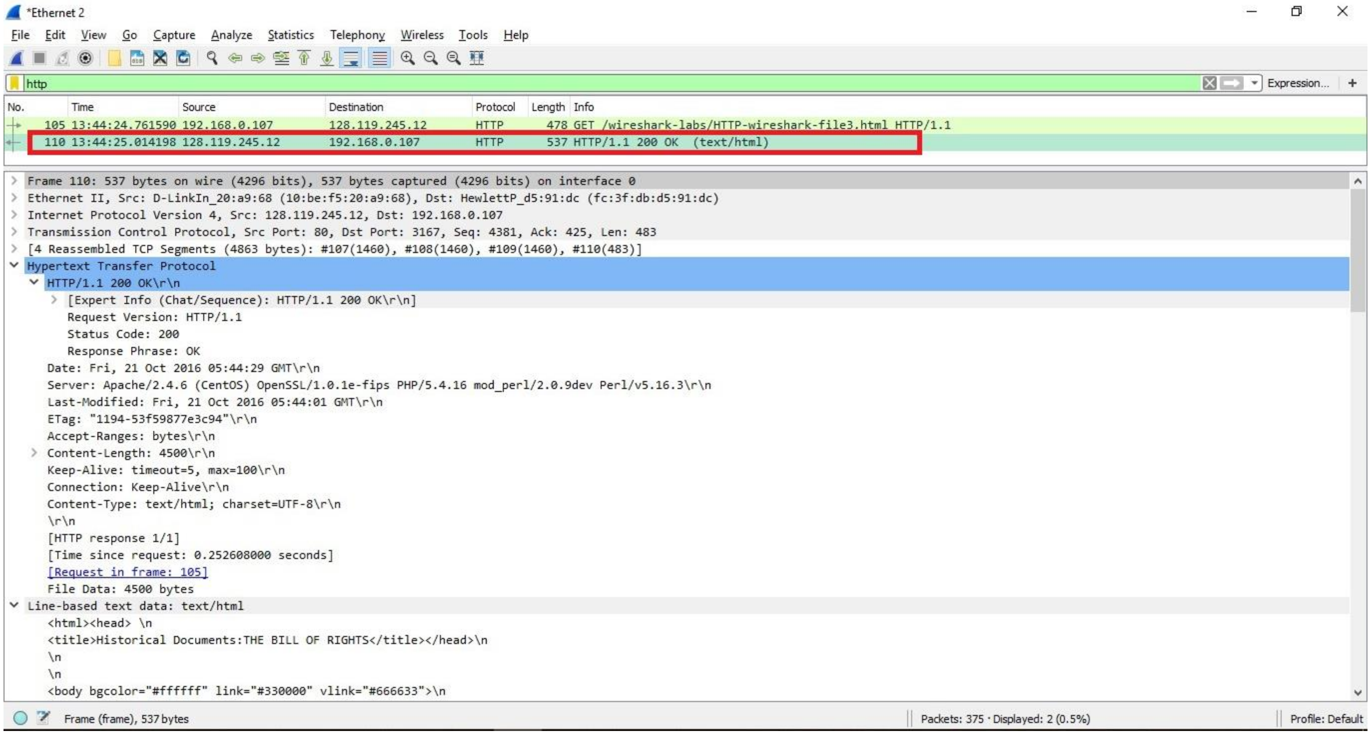
```
No.   Time            Source          Destination     Protocol Length Info
  105 13:44:24.761590 192.168.0.107   128.119.245.12  HTTP     478 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  110 13:44:25.014198 128.119.245.12  192.168.0.107   HTTP     537 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 105: 478 bytes on wire (3824 bits), 478 bytes captured (3824 bits) on interface 0
> Ethernet II, Src: HewlettP_d5:91:dc (fc:3f:db:d5:91:dc), Dst: D-LinkIn_20:a9:68 (10:be:f5:20:a9:68)
> Internet Protocol Version 4, Src: 192.168.0.107, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 3167, Dst Port: 80, Seq: 1, Ack: 1, Len: 424
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
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    DNT: 1\r\n
    Accept-Encoding: gzip, deflate, sdch\r\n
    Accept-Language: en-US,en;q=0.8\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
    [HTTP request 1/1]
    [Response in frame: 110]
```

```
Frame (frame), 478 bytes        Packets: 375 · Displayed: 2 (0.5%)        Profile: Default
```

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

The packet that contained the status code and phrase associated with the response is 110.



```
http
```

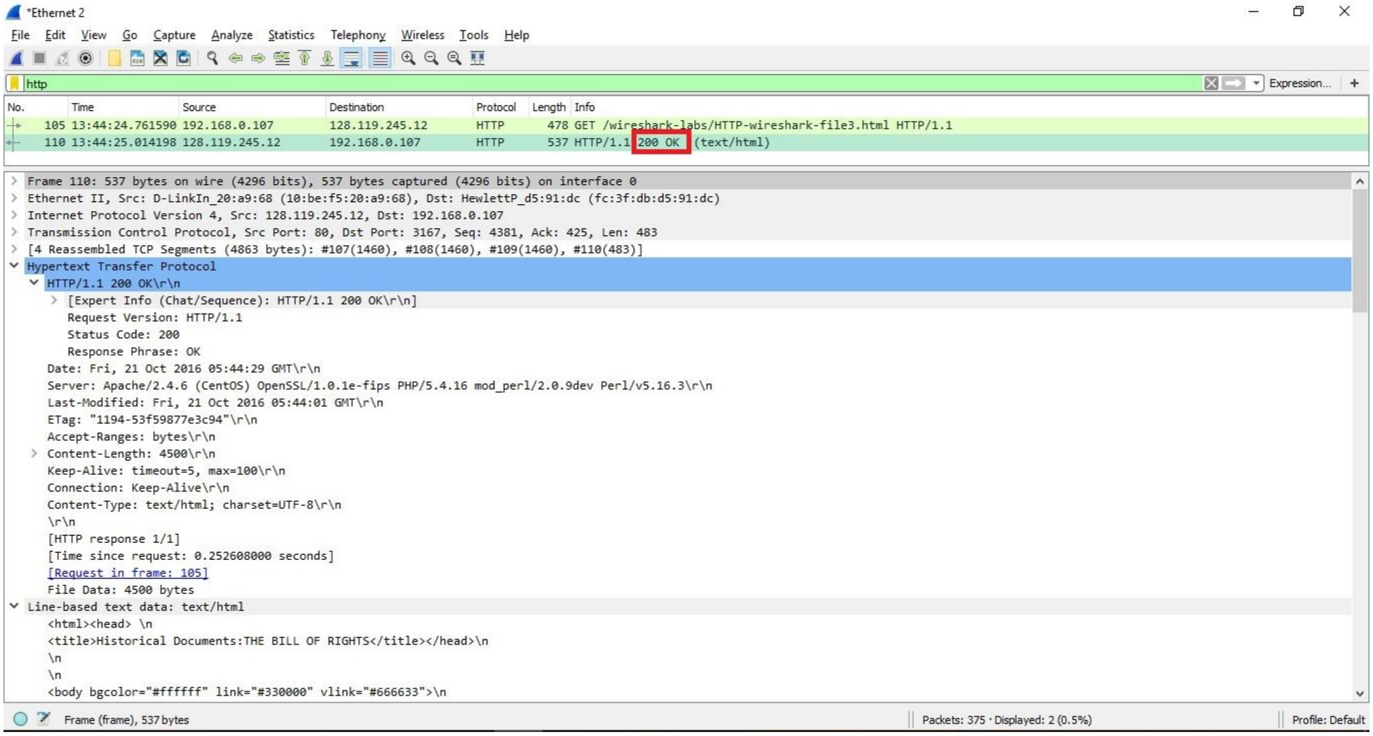
```
No.   Time            Source          Destination     Protocol Length Info
  105 13:44:24.761590 192.168.0.107   128.119.245.12  HTTP     478 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  110 13:44:25.014198 128.119.245.12  192.168.0.107   HTTP     537 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 110: 537 bytes on wire (4296 bits), 537 bytes captured (4296 bits) on interface 0
> Ethernet II, Src: D-LinkIn_20:a9:68 (10:be:f5:20:a9:68), Dst: HewlettP_d5:91:dc (fc:3f:db:d5:91:dc)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.107
> Transmission Control Protocol, Src Port: 80, Dst Port: 3167, Seq: 4381, Ack: 425, Len: 483
> [4 Reassembled TCP Segments (4863 bytes): #107(1460), #108(1460), #109(1460), #110(483)]
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Request Version: HTTP/1.1
      Status Code: 200
      Response Phrase: OK
    Date: Fri, 21 Oct 2016 05:44:29 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n
    Last-Modified: Fri, 21 Oct 2016 05:44:01 GMT\r\n
    ETag: "1194-53f59877e3c94"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 4500\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.252608000 seconds]
    [Request in frame: 105]
    File Data: 4500 bytes
v Line-based text data: text/html
    <html><head> \n
    <title>Historical Documents:THE BILL OF RIGHTS</title></head>\n
    \n
    \n
    <body bgcolor="#ffffff" link="#330000" vlink="#666633">\n
```

```
Frame (frame), 537 bytes        Packets: 375 · Displayed: 2 (0.5%)        Profile: Default
```

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

The status code and phrase in the response are: 200 OK


*Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
+

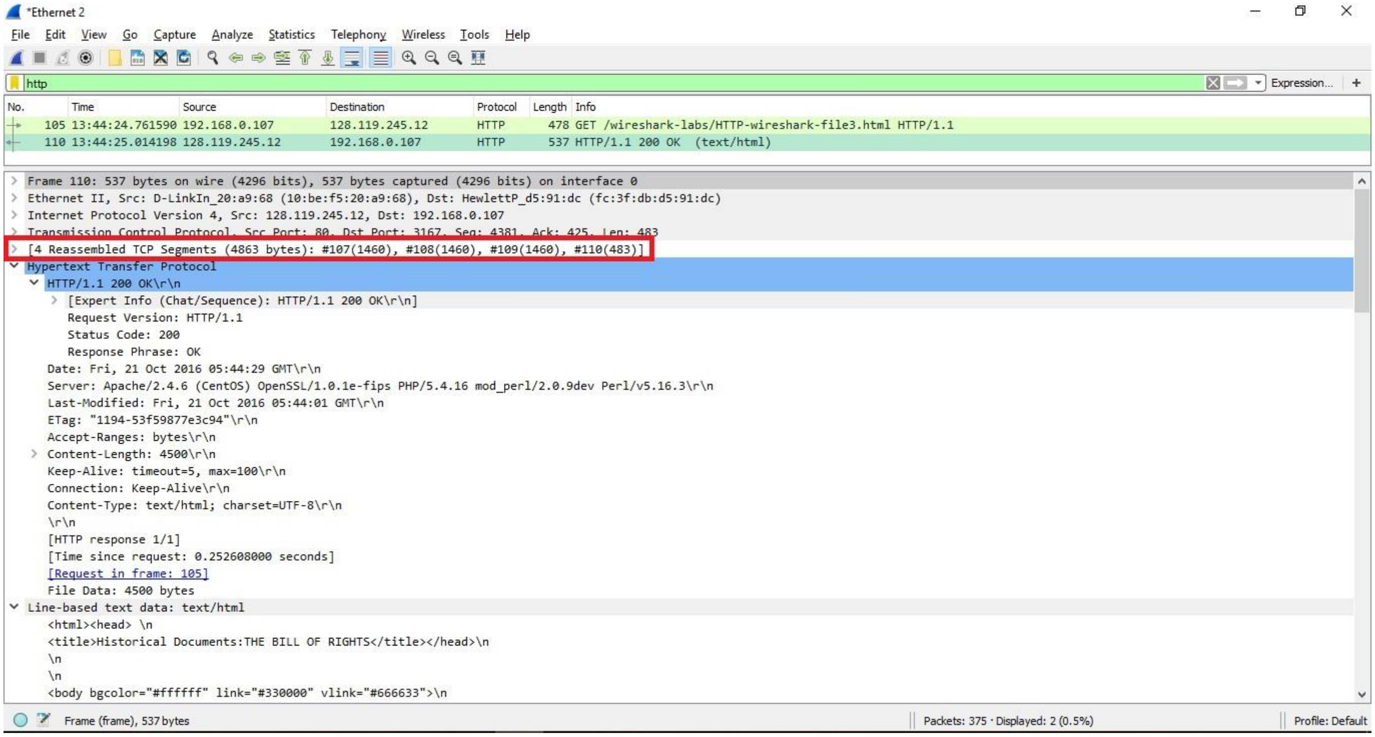
```
No.   Time            Source          Destination     Protocol Length Info
  105 13:44:24.761590 192.168.0.107   128.119.245.12  HTTP      478 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  110 13:44:25.014198 128.119.245.12  192.168.0.107   HTTP      537 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 110: 537 bytes on wire (4296 bits), 537 bytes captured (4296 bits) on interface 0
> Ethernet II, Src: D-LinkIn_20:a9:68 (10:be:f5:20:a9:68), Dst: HewlettP_d5:91:dc (fc:3f:db:d5:91:dc)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.107
> Transmission Control Protocol, Src Port: 80, Dst Port: 3167, Seq: 4381, Ack: 425, Len: 483
> [4 Reassembled TCP Segments (4863 bytes): #107(1460), #108(1460), #109(1460), #110(483)]
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Request Version: HTTP/1.1
      Status Code: 200
      Response Phrase: OK
    Date: Fri, 21 Oct 2016 05:44:29 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n
    Last-Modified: Fri, 21 Oct 2016 05:44:01 GMT\r\n
    ETag: "1194-53f59877e3c94"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 4500\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.252608000 seconds]
    [Request in frame: 105]
    File Data: 4500 bytes
v Line-based text data: text/html
    <html><head> \n
    <title>Historical Documents:THE BILL OF RIGHTS</title></head>\n
    \n
    \n
    <body bgcolor="#ffffff" link="#330000" vlink="#666633">\n
```

Frame (frame), 537 bytes | Packets: 375 · Displayed: 2 (0.5%) | Profile: Default

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

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


*Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
+

```
No.   Time            Source          Destination     Protocol Length Info
  105 13:44:24.761590 192.168.0.107   128.119.245.12  HTTP      478 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  110 13:44:25.014198 128.119.245.12  192.168.0.107   HTTP      537 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 110: 537 bytes on wire (4296 bits), 537 bytes captured (4296 bits) on interface 0
> Ethernet II, Src: D-LinkIn_20:a9:68 (10:be:f5:20:a9:68), Dst: HewlettP_d5:91:dc (fc:3f:db:d5:91:dc)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.107
> Transmission Control Protocol, Src Port: 80, Dst Port: 3167, Seq: 4381, Ack: 425, Len: 483
> [4 Reassembled TCP Segments (4863 bytes): #107(1460), #108(1460), #109(1460), #110(483)]
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Request Version: HTTP/1.1
      Status Code: 200
      Response Phrase: OK
    Date: Fri, 21 Oct 2016 05:44:29 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n
    Last-Modified: Fri, 21 Oct 2016 05:44:01 GMT\r\n
    ETag: "1194-53f59877e3c94"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 4500\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.252608000 seconds]
    [Request in frame: 105]
    File Data: 4500 bytes
v Line-based text data: text/html
    <html><head> \n
    <title>Historical Documents:THE BILL OF RIGHTS</title></head>\n
    \n
    \n
    <body bgcolor="#ffffff" link="#330000" vlink="#666633">\n
```

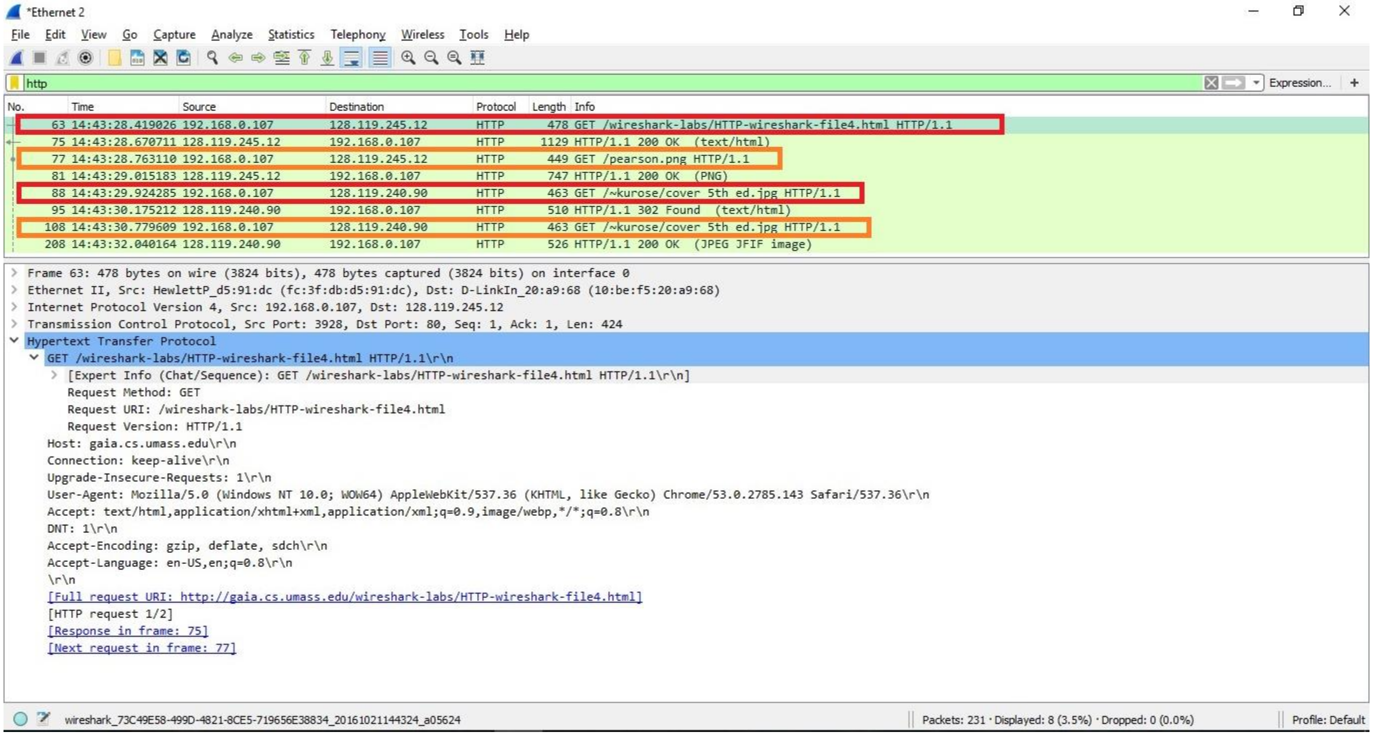
Frame (frame), 537 bytes | Packets: 375 · Displayed: 2 (0.5%) | Profile: Default

4. HTML Documents with Embedded Objects

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

My browser sent 4 GET requests – 2 to each of the following addresses:

- 128.119.245.12
- 128.119.240.90



*Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
+

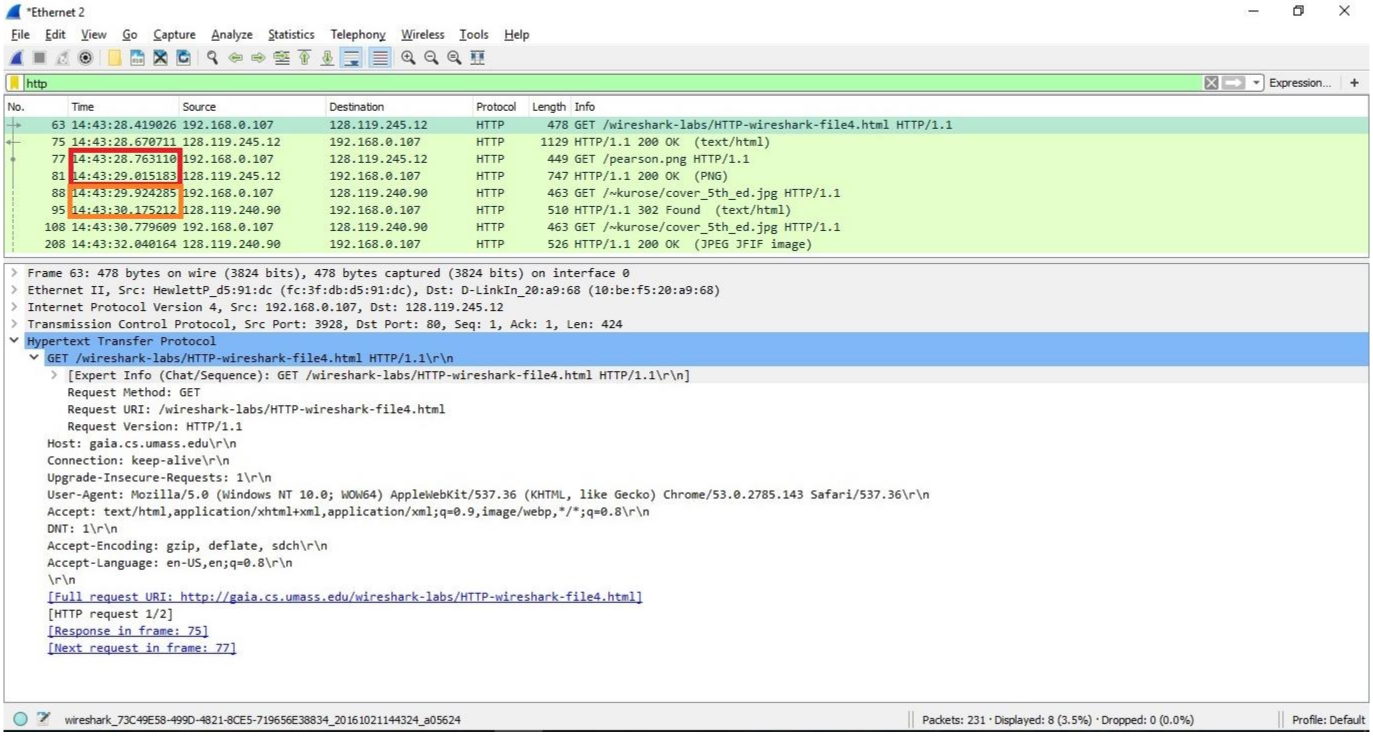
```
No.  Time            Source          Destination     Protocol Length Info
  63 14:43:28.419026 192.168.0.107   128.119.245.12  HTTP      478 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
  75 14:43:28.670711 128.119.245.12  192.168.0.107   HTTP     1129 HTTP/1.1 200 OK  (text/html)
  77 14:43:28.763110 192.168.0.107   128.119.245.12  HTTP      449 GET /pearson.png HTTP/1.1
  81 14:43:29.015183 128.119.245.12  192.168.0.107   HTTP      747 HTTP/1.1 200 OK  (PNG)
  88 14:43:29.924285 192.168.0.107   128.119.240.90  HTTP      463 GET /~kurose/cover 5th ed.jpg HTTP/1.1
  95 14:43:30.175212 128.119.240.90  192.168.0.107   HTTP      510 HTTP/1.1 302 Found  (text/html)
 108 14:43:30.779609 192.168.0.107   128.119.240.90  HTTP      463 GET /~kurose/cover 5th ed.jpg HTTP/1.1
 208 14:43:32.040164 128.119.240.90  192.168.0.107   HTTP      526 HTTP/1.1 200 OK  (JPEG JFIF image)
```

```
> Frame 63: 478 bytes on wire (3824 bits), 478 bytes captured (3824 bits) on interface 0
> Ethernet II, Src: HewlettP_d5:91:dc (fc:3f:db:d5:91:dc), Dst: D-LinkIn_20:a9:68 (10:be:f5:20:a9:68)
> Internet Protocol Version 4, Src: 192.168.0.107, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 3928, Dst Port: 80, Seq: 1, Ack: 1, Len: 424
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file4.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; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    DNT: 1\r\n
    Accept-Encoding: gzip, deflate, sdch\r\n
    Accept-Language: en-US,en;q=0.8\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]
    [HTTP request 1/2]
    [Response in frame: 75]
    [Next request in frame: 77]
```

wireshark_73C49E58-499D-4821-8CE5-719656E38834_20161021144324_a05624 | Packets: 231 · Displayed: 8 (3.5%) · Dropped: 0 (0.0%) | Profile: Default

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

My browser downloaded the two images serially. If they were being downloaded in parallel, the timing of the requests/returns would have overlapped. Here we can clearly see that the second image was only requested after the first had already returned.



*Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...

```
No.  Time            Source          Destination     Protocol Length Info
 63 14:43:28.419026 192.168.0.107   128.119.245.12  HTTP      478 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
 75 14:43:28.670711 128.119.245.12  192.168.0.107   HTTP     1129 HTTP/1.1 200 OK  (text/html)
 77 14:43:28.763110 192.168.0.107   128.119.245.12  HTTP      449 GET /pearson.png HTTP/1.1
 81 14:43:29.015183 128.119.245.12  192.168.0.107   HTTP      747 HTTP/1.1 200 OK  (PNG)
 88 14:43:29.924285 192.168.0.107   128.119.240.90  HTTP      463 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
 95 14:43:30.175212 128.119.240.90  192.168.0.107   HTTP      510 HTTP/1.1 302 Found  (text/html)
108 14:43:30.779609 192.168.0.107   128.119.240.90  HTTP      463 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
208 14:43:32.040164 128.119.240.90  192.168.0.107   HTTP      526 HTTP/1.1 200 OK  (JPEG JFIF image)
```

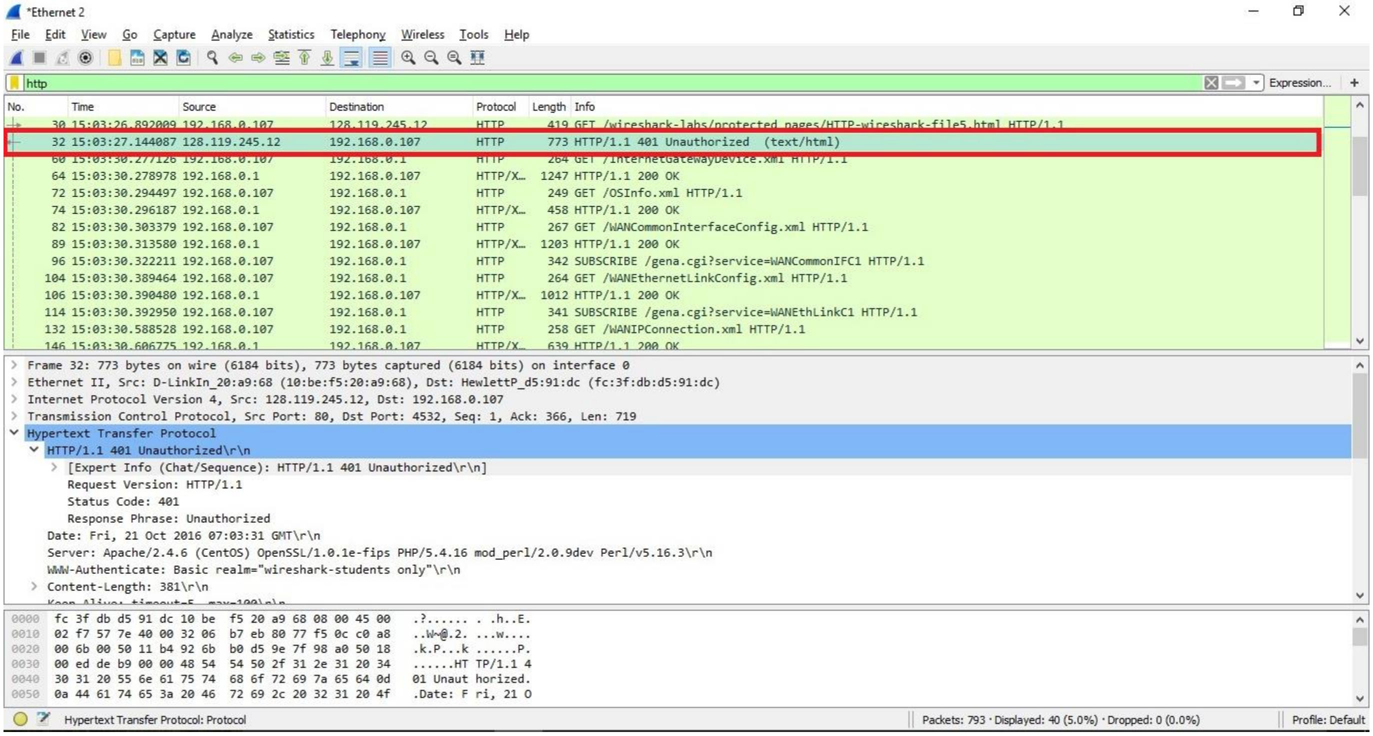
```
> Frame 63: 478 bytes on wire (3824 bits), 478 bytes captured (3824 bits) on interface 0
> Ethernet II, Src: HewlettP_d5:91:dc (fc:3f:db:d5:91:dc), Dst: D-LinkIn_20:a9:68 (10:be:f5:20:a9:68)
> Internet Protocol Version 4, Src: 192.168.0.107, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 3928, Dst Port: 80, Seq: 1, Ack: 1, Len: 424
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file4.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; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    DNT: 1\r\n
    Accept-Encoding: gzip, deflate, sdch\r\n
    Accept-Language: en-US,en;q=0.8\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]
    [HTTP request 1/2]
    [Response in frame: 75]
    [Next request in frame: 77]
```

```
wireshark_73C49E58-499D-4821-8CE5-719656E38834_20161021144324_a05624    Packets: 231 · Displayed: 8 (3.5%) · Dropped: 0 (0.0%)    Profile: Default
```

5 HTTP Authentication

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

The server's response to the initial HTTP GET message from my browser is: 401 Unauthorized



*Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...

```
No.  Time            Source          Destination     Protocol Length Info
 30 15:03:26.892009 192.168.0.107   128.119.245.12  HTTP      419 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
 32 15:03:27.144087 128.119.245.12  192.168.0.107   HTTP      773 HTTP/1.1 401 Unauthorized  (text/html)
 60 15:03:30.277126 192.168.0.107   192.168.0.1     HTTP      264 GET /InternetGatewayDevice.xml HTTP/1.1
 64 15:03:30.278978 192.168.0.1     192.168.0.107   HTTP/X…  1247 HTTP/1.1 200 OK
 72 15:03:30.294497 192.168.0.107   192.168.0.1     HTTP      249 GET /OSInfo.xml HTTP/1.1
 74 15:03:30.296187 192.168.0.1     192.168.0.107   HTTP/X…   458 HTTP/1.1 200 OK
 82 15:03:30.303379 192.168.0.107   192.168.0.1     HTTP      267 GET /WANCommonInterfaceConfig.xml HTTP/1.1
 89 15:03:30.313580 192.168.0.1     192.168.0.107   HTTP/X…  1203 HTTP/1.1 200 OK
 96 15:03:30.322211 192.168.0.107   192.168.0.1     HTTP      342 SUBSCRIBE /gena.cgi?service=WANCommonIFC1 HTTP/1.1
104 15:03:30.389464 192.168.0.107   192.168.0.1     HTTP      264 GET /WANEthernetLinkConfig.xml HTTP/1.1
106 15:03:30.390480 192.168.0.1     192.168.0.107   HTTP/X…  1012 HTTP/1.1 200 OK
114 15:03:30.392950 192.168.0.107   192.168.0.1     HTTP      341 SUBSCRIBE /gena.cgi?service=WANEthLinkC1 HTTP/1.1
132 15:03:30.588528 192.168.0.107   192.168.0.1     HTTP      258 GET /WANIPConnection.xml HTTP/1.1
146 15:03:30.606775 192.168.0.1     192.168.0.107   HTTP/X…   639 HTTP/1.1 200 OK
```

```
> Frame 32: 773 bytes on wire (6184 bits), 773 bytes captured (6184 bits) on interface 0
> Ethernet II, Src: D-LinkIn_20:a9:68 (10:be:f5:20:a9:68), Dst: HewlettP_d5:91:dc (fc:3f:db:d5:91:dc)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.107
> Transmission Control Protocol, Src Port: 80, Dst Port: 4532, Seq: 1, Ack: 366, Len: 719
v Hypertext Transfer Protocol
  v HTTP/1.1 401 Unauthorized\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
      Request Version: HTTP/1.1
      Status Code: 401
      Response Phrase: Unauthorized
    Date: Fri, 21 Oct 2016 07:03:31 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n
    WWW-Authenticate: Basic realm="wireshark-students only"\r\n
  > Content-Length: 381\r\n
    Keep-Alive: timeout=5, max=100\r\n
```

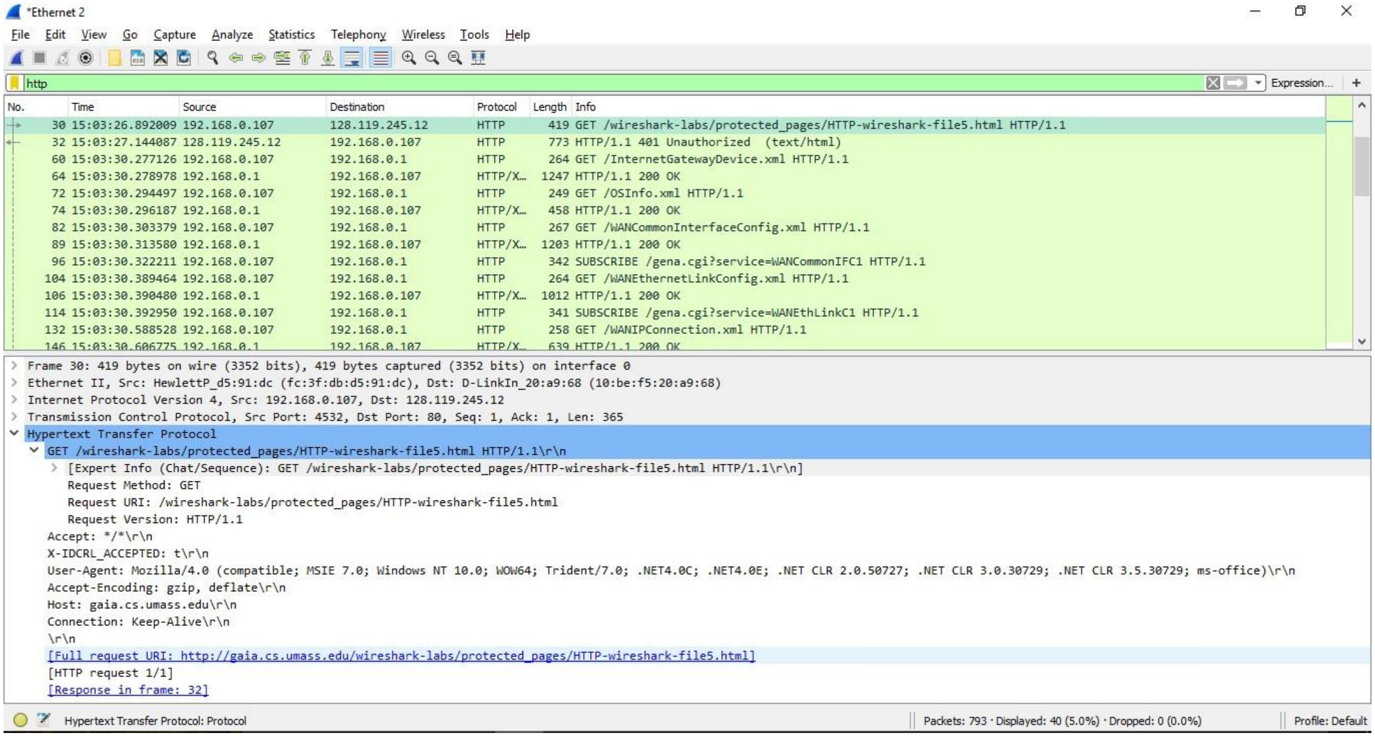
```
0000  fc 3f db d5 91 dc 10 be  f5 20 a9 68 08 00 45 00   .?...... . .h..E.
0010  02 f7 57 7e 40 00 32 06  b7 eb 80 77 f5 0c c0 a8   ..W~@.2. ...w....
0020  00 6b 00 50 11 b4 92 6b  b0 d5 9e 7f 98 a0 50 18   .k.P...k ......P.
0030  00 ed de b9 00 00 48 54  54 50 2f 31 2e 31 20 34   ......HT TP/1.1 4
0040  30 31 20 55 6e 61 75 74  68 6f 72 69 7a 65 64 0d   01 Unaut horized.
0050  0a 44 61 74 65 3a 20 46  72 69 2c 20 32 31 20 4f   .Date: F ri, 21 O
```

```
Hypertext Transfer Protocol: Protocol    Packets: 793 · Displayed: 40 (5.0%) · Dropped: 0 (0.0%)    Profile: Default
```

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

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

First GET:

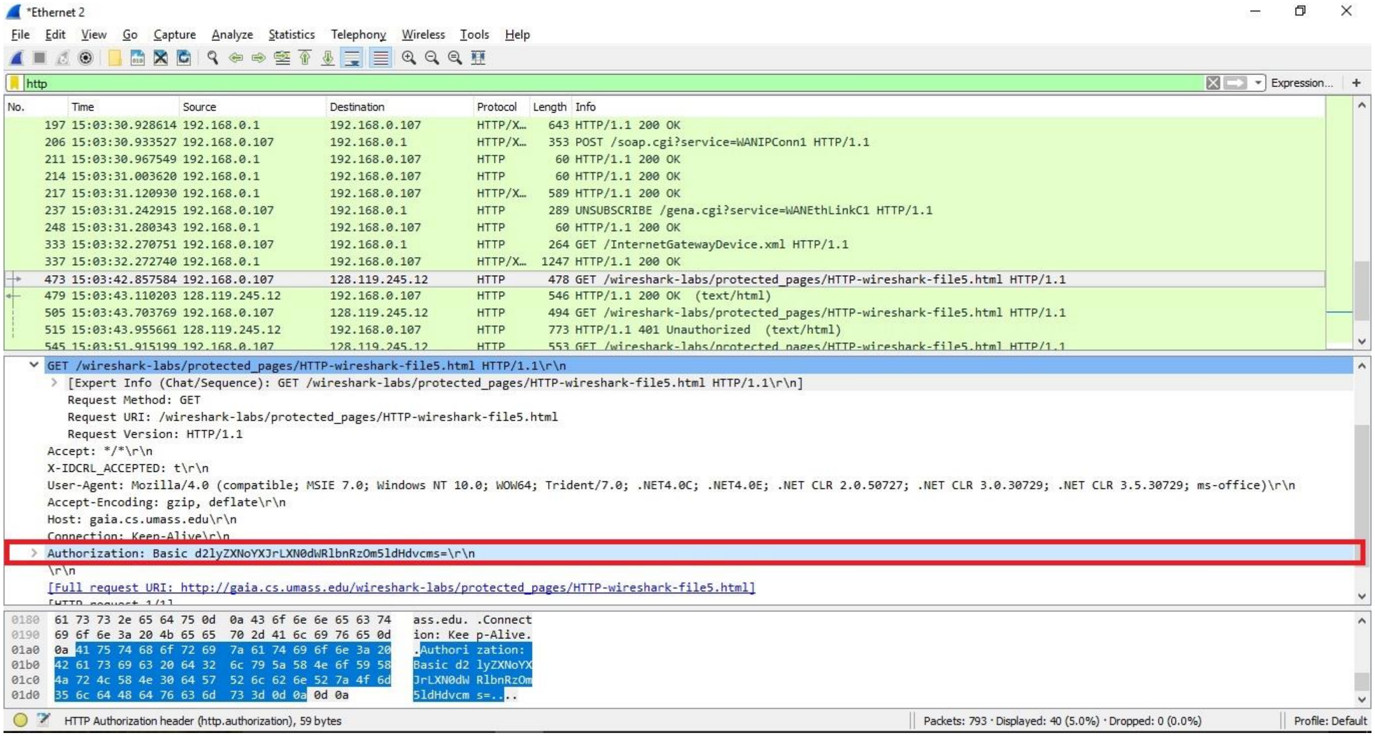

*Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression…

```
No.  Time              Source          Destination     Protocol Length Info
  30 15:03:26.892009 192.168.0.107   128.119.245.12  HTTP      419 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
  32 15:03:27.144087 128.119.245.12  192.168.0.107   HTTP      773 HTTP/1.1 401 Unauthorized  (text/html)
  60 15:03:30.277126 192.168.0.107   192.168.0.1     HTTP      264 GET /InternetGatewayDevice.xml HTTP/1.1
  64 15:03:30.278978 192.168.0.1     192.168.0.107   HTTP/X…  1247 HTTP/1.1 200 OK
  72 15:03:30.294497 192.168.0.107   192.168.0.1     HTTP      249 GET /OSInfo.xml HTTP/1.1
  74 15:03:30.296187 192.168.0.1     192.168.0.107   HTTP/X…   458 HTTP/1.1 200 OK
  82 15:03:30.303379 192.168.0.107   192.168.0.1     HTTP      267 GET /WANCommonInterfaceConfig.xml HTTP/1.1
  89 15:03:30.313580 192.168.0.1     192.168.0.107   HTTP/X…  1203 HTTP/1.1 200 OK
  96 15:03:30.322211 192.168.0.107   192.168.0.1     HTTP      342 SUBSCRIBE /gena.cgi?service=WANCommonIFC1 HTTP/1.1
 104 15:03:30.389464 192.168.0.107   192.168.0.1     HTTP      264 GET /WANEthernetLinkConfig.xml HTTP/1.1
 106 15:03:30.390480 192.168.0.1     192.168.0.107   HTTP/X…  1012 HTTP/1.1 200 OK
 114 15:03:30.392950 192.168.0.107   192.168.0.1     HTTP      341 SUBSCRIBE /gena.cgi?service=WANEthLinkC1 HTTP/1.1
 132 15:03:30.588528 192.168.0.107   192.168.0.1     HTTP      258 GET /WANIPConnection.xml HTTP/1.1
 146 15:03:30.606775 192.168.0.1     192.168.0.107   HTTP/X…   639 HTTP/1.1 200 OK
```

```
> Frame 30: 419 bytes on wire (3352 bits), 419 bytes captured (3352 bits) on interface 0
> Ethernet II, Src: HewlettP_d5:91:dc (fc:3f:db:d5:91:dc), Dst: D-LinkIn_20:a9:68 (10:be:f5:20:a9:68)
> Internet Protocol Version 4, Src: 192.168.0.107, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 4532, Dst Port: 80, Seq: 1, Ack: 1, Len: 365
v Hypertext Transfer Protocol
  v GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
      Request Version: HTTP/1.1
    Accept: */*\r\n
    X-IDCRL_ACCEPTED: t\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; ms-office)\r\n
    Accept-Encoding: gzip, deflate\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: Keep-Alive\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: 32]
```

```
Hypertext Transfer Protocol: Protocol    Packets: 793 · Displayed: 40 (5.0%) · Dropped: 0 (0.0%)    Profile: Default
```

Second GET:


*Ethernet 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression…

```
No.  Time              Source          Destination     Protocol Length Info
 197 15:03:30.928614 192.168.0.1     192.168.0.107   HTTP/X…   643 HTTP/1.1 200 OK
 206 15:03:30.933527 192.168.0.107   192.168.0.1     HTTP/X…   353 POST /soap.cgi?service=WANIPConn1 HTTP/1.1
 211 15:03:30.967549 192.168.0.1     192.168.0.107   HTTP       60 HTTP/1.1 200 OK
 214 15:03:31.003620 192.168.0.1     192.168.0.107   HTTP       60 HTTP/1.1 200 OK
 217 15:03:31.120930 192.168.0.1     192.168.0.107   HTTP/X…   589 HTTP/1.1 200 OK
 237 15:03:31.242915 192.168.0.107   192.168.0.1     HTTP      289 UNSUBSCRIBE /gena.cgi?service=WANEthLinkC1 HTTP/1.1
 248 15:03:31.280343 192.168.0.1     192.168.0.107   HTTP       60 HTTP/1.1 200 OK
 333 15:03:32.270751 192.168.0.107   192.168.0.1     HTTP      264 GET /InternetGatewayDevice.xml HTTP/1.1
 337 15:03:32.272740 192.168.0.1     192.168.0.107   HTTP/X…  1247 HTTP/1.1 200 OK
 473 15:03:42.857584 192.168.0.107   128.119.245.12  HTTP      478 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
 479 15:03:43.110203 128.119.245.12  192.168.0.107   HTTP      546 HTTP/1.1 200 OK  (text/html)
 505 15:03:43.703769 192.168.0.107   128.119.245.12  HTTP      494 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
 515 15:03:43.955661 128.119.245.12  192.168.0.107   HTTP      773 HTTP/1.1 401 Unauthorized  (text/html)
 545 15:03:51.915199 192.168.0.107   128.119.245.12  HTTP      553 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
```

```
  v GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
      Request Version: HTTP/1.1
    Accept: */*\r\n
    X-IDCRL_ACCEPTED: t\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; ms-office)\r\n
    Accept-Encoding: gzip, deflate\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: Keep-Alive\r\n
  > Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
    [HTTP request 1/1]
```

```
0180  61 73 73 2e 65 64 75 0d  0a 43 6f 6e 6e 65 63 74   ass.edu. .Connect
0190  69 6f 6e 3a 20 4b 65 65  70 2d 41 6c 69 76 65 0d   ion: Kee p-Alive.
01a0  0a 41 75 74 68 6f 72 69  7a 61 74 69 6f 6e 3a 20   .Authori zation: 
01b0  42 61 73 69 63 20 64 32  6c 79 5a 58 4e 6f 59 58   Basic d2 lyZXNoYX
01c0  4a 72 4c 58 4e 30 64 57  52 6c 62 6e 52 7a 4f 6d   JrLXN0dW RlbnRzOm
01d0  35 6c 64 48 64 76 63 6d  73 3d 0d 0a 0d 0a         5ldHdvcm s=....
```

```
HTTP Authorization header (http.authorization), 59 bytes    Packets: 793 · Displayed: 40 (5.0%) · Dropped: 0 (0.0%)    Profile: Default
```