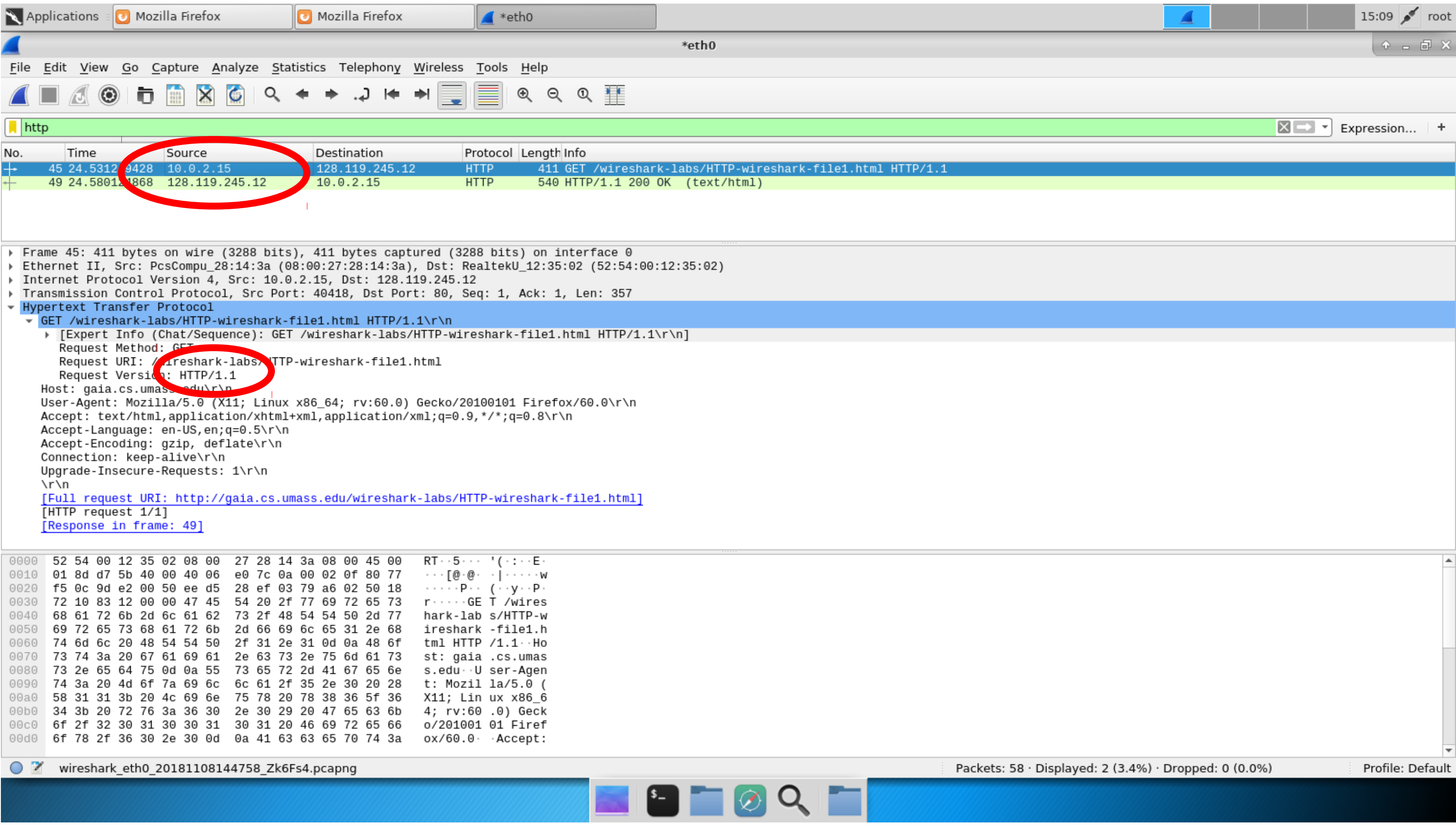
Luke Malloy

Wireshark Lab: HTTP

Questions:

1. My browser is running HTTP 1.1, the server is running HTTP 1.1(shown in next picture)
2. en-US, en languages (english)
3. My IP = 10.0.2.15
   Server IP = 128.119.245.12



http

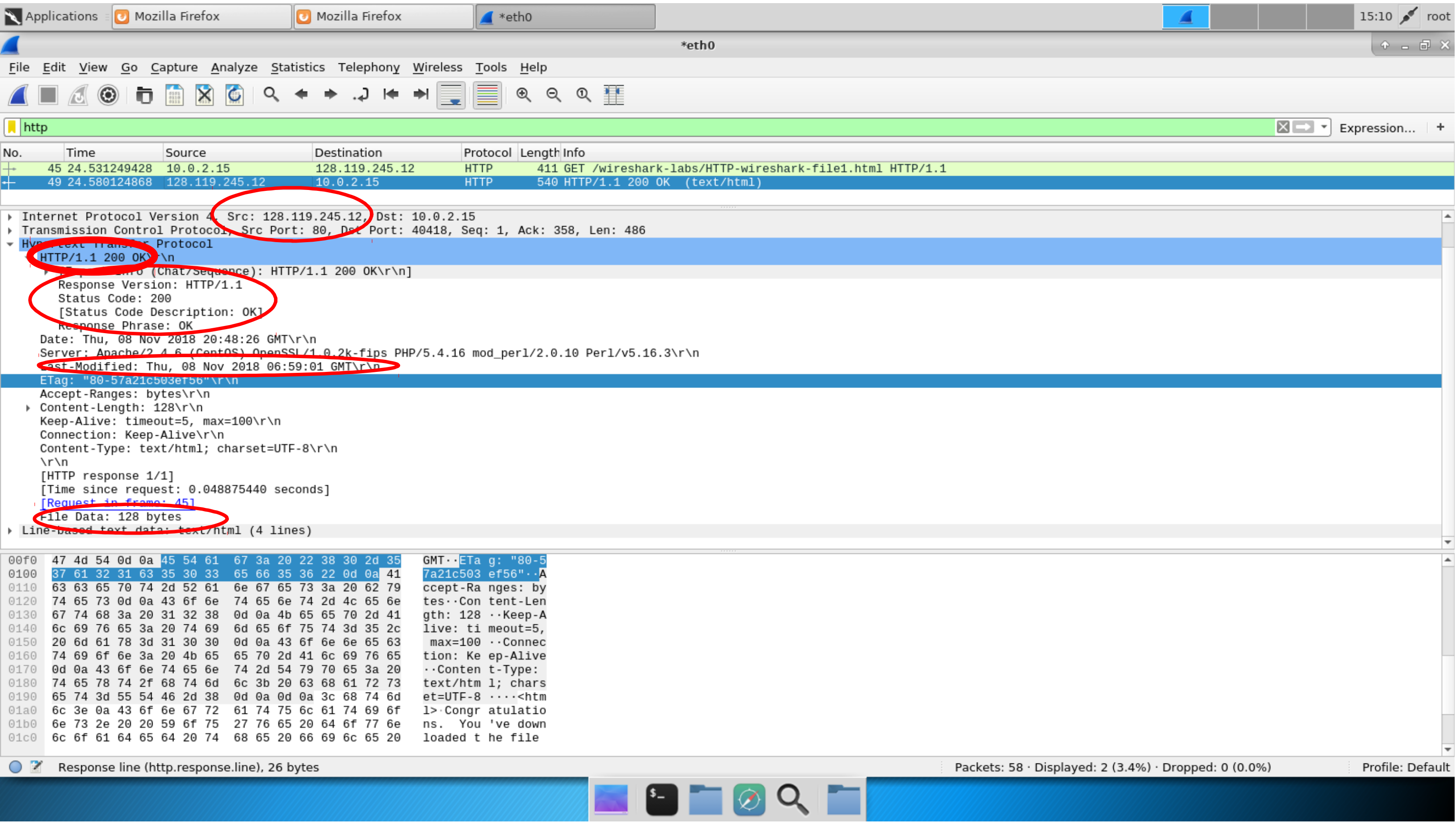
```
No.   Time              Source           Destination      Protocol  Length Info
   45 24.5312[illegible]9428    10.0.2.15        128.119.245.12   HTTP       411 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
   49 24.5801[illegible]868    128.119.245.12   10.0.2.15        HTTP       540 HTTP/1.1 200 OK  (text/html)
```

```
▸ Frame 45: 411 bytes on wire (3288 bits), 411 bytes captured (3288 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_28:14:3a (08:00:27:28:14:3a), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 128.119.245.12
▸ Transmission Control Protocol, Src Port: 40418, Dst Port: 80, Seq: 1, Ack: 1, Len: 357
▾ Hypertext Transfer Protocol
  ▾ 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
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0\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
    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: 49]
```

```
0000  52 54 00 12 35 02 08 00  27 28 14 3a 08 00 45 00   RT··5···  '(·:··E·
0010  01 8d d7 5b 40 00 40 06  e0 7c 0a 00 02 0f 80 77   ···[@·@·  ·|·····w
0020  f5 0c 9d e2 00 50 ee d5  28 ef 03 79 a6 02 50 18   ·····P··  (··y··P·
0030  72 10 83 12 00 00 47 45  54 20 2f 77 69 72 65 73   r·····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
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 55  73 65 72 2d 41 67 65 6e   s.edu··U  ser-Agen
0090  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil  la/5.0 (
00a0  58 31 31 3b 20 4c 69 6e  75 78 20 78 38 36 5f 36   X11; Lin  ux x86_6
00b0  34 3b 20 72 76 3a 36 30  2e 30 29 20 47 65 63 6b   4; rv:60  .0) Geck
00c0  6f 2f 32 30 31 30 30 31  30 31 20 46 69 72 65 66   o/201001  01 Firef
00d0  6f 78 2f 36 30 2e 30 0d  0a 41 63 63 65 70 74 3a   ox/60.0·  ·Accept:
```

wireshark_eth0_20181108144758_Zk6Fs4.pcapng   Packets: 58 · Displayed: 2 (3.4%) · Dropped: 0 (0.0%)   Profile: Default

4. Status Code is 200 Phrase is ‘OK’
5. Modified Last Nov 8th at 06:59PM GMT
6. 128 bytes
7. The expert info header



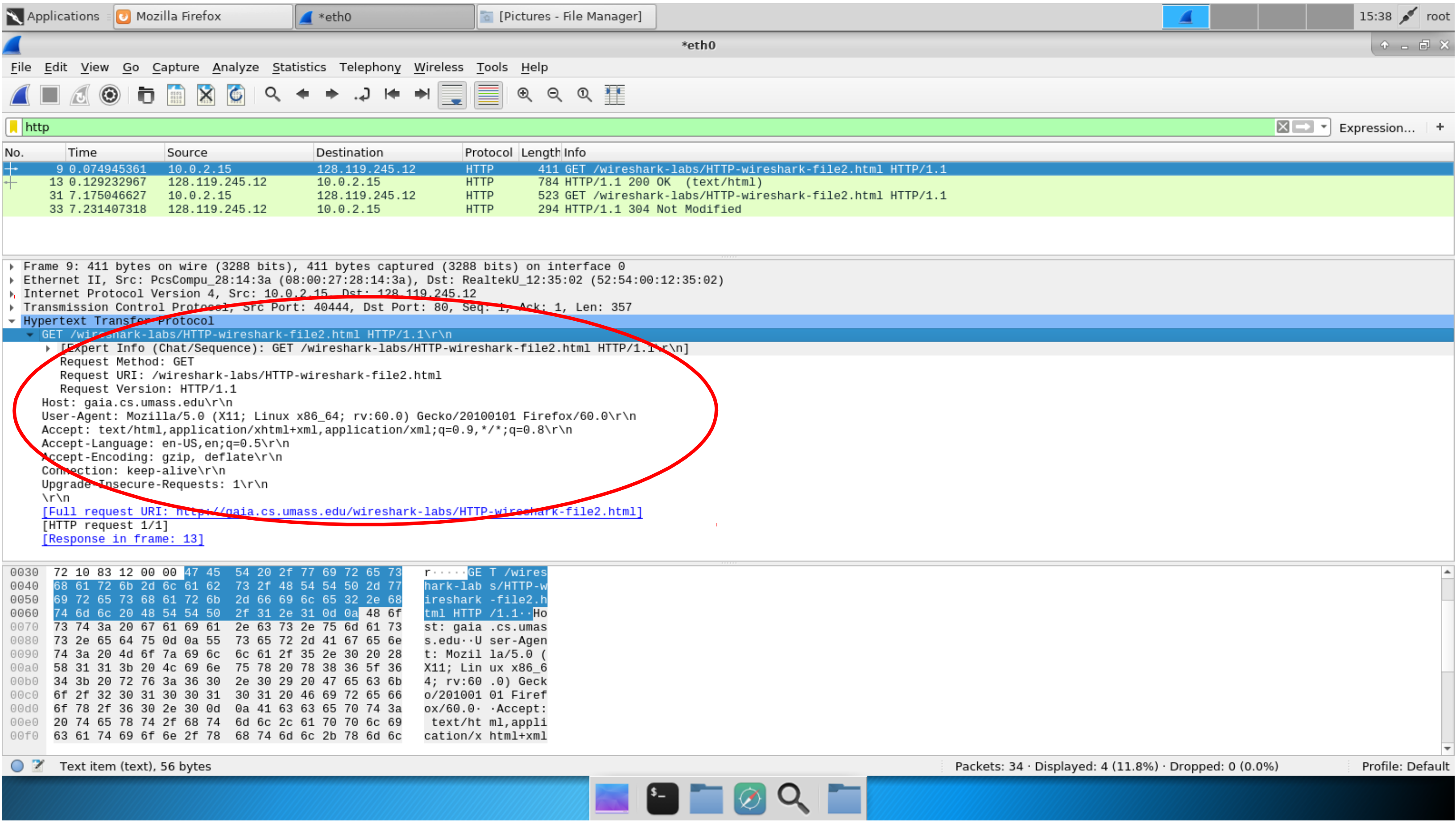
```
No.   Time           Source          Destination     Protocol Length Info
   45 24.531249428   10.0.2.15       128.119.245.12  HTTP        411 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
   49 24.580124868   128.119.245.12  10.0.2.15       HTTP        540 HTTP/1.1 200 OK  (text/html)

▸ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.2.15
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 40418, Seq: 1, Ack: 358, Len: 486
▾ Hypertext Transfer Protocol
  ▾ HTTP/1.1 200 OK\r\n
    ▸ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Thu, 08 Nov 2018 20:48:26 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Thu, 08 Nov 2018 06:59:01 GMT\r\n
    ETag: "80-57a21c503ef56"\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: 0.048875440 seconds]
    [Request in frame: 45]
    File Data: 128 bytes
▸ Line-based text data: text/html (4 lines)

00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 38 30 2d 35   GMT··ETa g: "80-5
0100  37 61 32 31 63 35 30 33  65 66 35 36 22 0d 0a 41   7a21c503 ef56"··A
0110  63 63 65 70 74 2d 52 61  6e 67 65 73 3a 20 62 79   ccept-Ra nges: by
0120  74 65 73 0d 0a 43 6f 6e  74 65 6e 74 2d 4c 65 6e   tes··Con tent-Len
0130  67 74 68 3a 20 31 32 38  0d 0a 4b 65 65 70 2d 41   gth: 128 ··Keep-A
0140  6c 69 76 65 3a 20 74 69  6d 65 6f 75 74 3d 35 2c   live: ti meout=5,
0150  20 6d 61 78 3d 31 30 30  0d 0a 43 6f 6e 6e 65 63    max=100 ··Connec
0160  74 69 6f 6e 3a 20 4b 65  65 70 2d 41 6c 69 76 65   tion: Ke ep-Alive
0170  0d 0a 43 6f 6e 74 65 6e  74 2d 54 79 70 65 3a 20   ··Conten t-Type: 
0180  74 65 78 74 2f 68 74 6d  6c 3b 20 63 68 61 72 73   text/htm l; chars
0190  65 74 3d 55 54 46 2d 38  0d 0a 0d 0a 3c 68 74 6d   et=UTF-8 ····<htm
01a0  6c 3e 0a 43 6f 6e 67 72  61 74 75 6c 61 74 69 6f   l>·Congr atulatio
01b0  6e 73 2e 20 20 59 6f 75  27 76 65 20 64 6f 77 6e   ns.  You 've down
01c0  6c 6f 61 64 65 64 20 74  68 65 20 66 69 6c 65 20   loaded t he file

Response line (http.response.line), 26 bytes    Packets: 58 · Displayed: 2 (3.4%) · Dropped: 0 (0.0%)    Profile: Default
```

8. No, it is not there in the first message



http

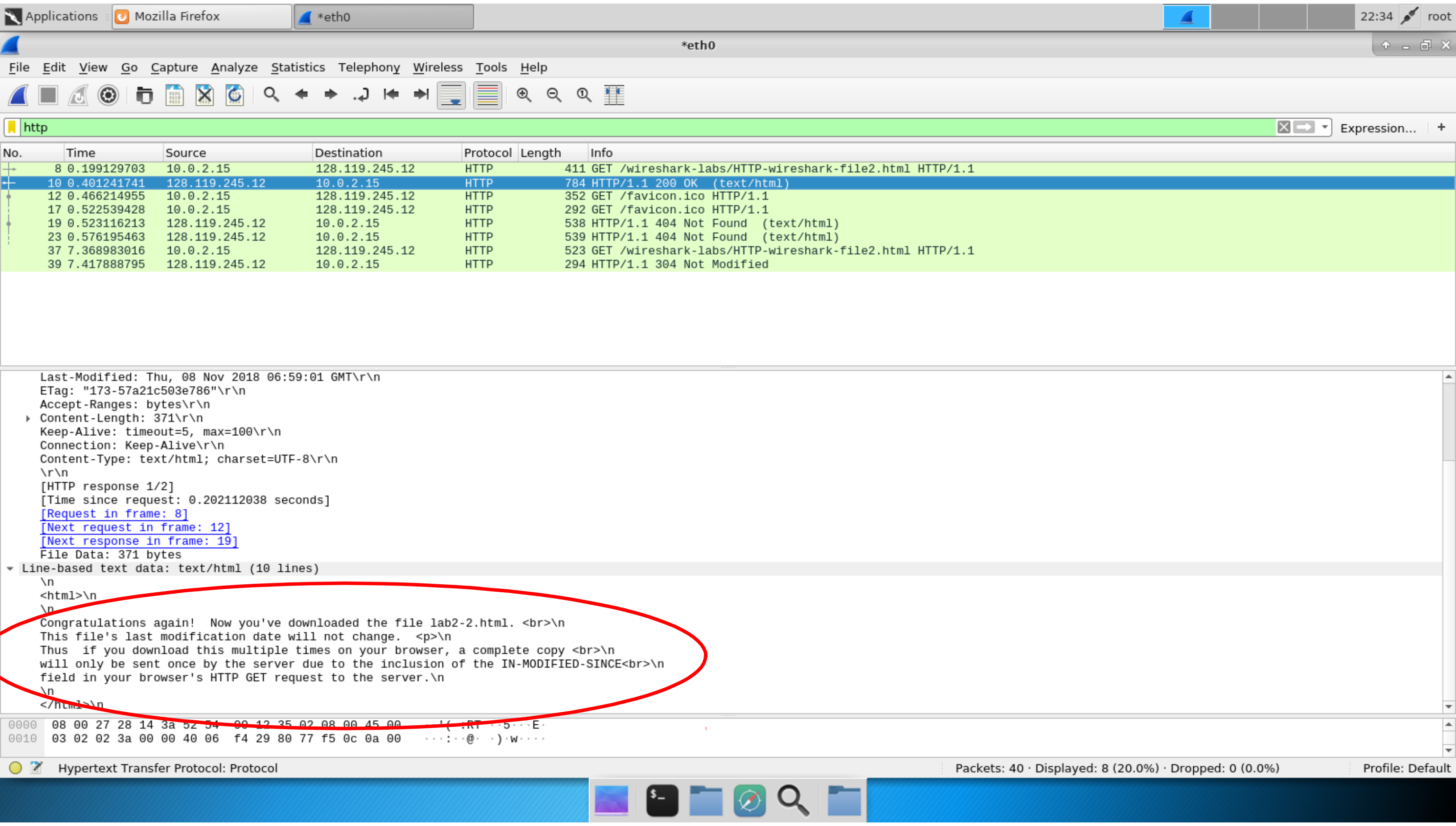
```
No.   Time         Source           Destination      Protocol Length Info
    9 0.074945361  10.0.2.15        128.119.245.12   HTTP      411 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   13 0.129232967  128.119.245.12   10.0.2.15        HTTP      784 HTTP/1.1 200 OK  (text/html)
   31 7.175046627  10.0.2.15        128.119.245.12   HTTP      523 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   33 7.231407318  128.119.245.12   10.0.2.15        HTTP      294 HTTP/1.1 304 Not Modified
```

```
Frame 9: 411 bytes on wire (3288 bits), 411 bytes captured (3288 bits) on interface 0
Ethernet II, Src: PcsCompu_28:14:3a (08:00:27:28:14:3a), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 40444, Dst Port: 80, Seq: 1, Ack: 1, Len: 357
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]
    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:60.0) Gecko/20100101 Firefox/60.0\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
  Upgrade-Insecure-Requests: 1\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: 13]
```

```
0030  72 10 83 12 00 00 47 45  54 20 2f 77 69 72 65 73   r·····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 55  73 65 72 2d 41 67 65 6e   s.edu··U ser-Agen
0090  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil la/5.0 (
00a0  58 31 31 3b 20 4c 69 6e  75 78 20 78 38 36 5f 36   X11; Lin ux x86_6
00b0  34 3b 20 72 76 3a 36 30  2e 30 29 20 47 65 63 6b   4; rv:60 .0) Geck
00c0  6f 2f 32 30 31 30 30 31  30 31 20 46 69 72 65 66   o/201001 01 Firef
00d0  6f 78 2f 36 30 2e 30 0d  0a 41 63 63 65 70 74 3a   ox/60.0· ·Accept:
00e0  20 74 65 78 74 2f 68 74  6d 6c 2c 61 70 70 6c 69    text/ht ml,appli
00f0  63 61 74 69 6f 6e 2f 78  68 74 6d 6c 2b 78 6d 6c   cation/x html+xml
```

Text item (text), 56 bytes   Packets: 34 · Displayed: 4 (11.8%) · Dropped: 0 (0.0%)   Profile: Default

9. Yes, the contents are located in the Line-based text data, it is returned here


Applications
Mozilla Firefox
*eth0
22:34
root
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

```
http
```

```
No.  Time         Source          Destination     Protocol Length Info
   8 0.199129703  10.0.2.15       128.119.245.12  HTTP        411 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  10 0.401241741  128.119.245.12  10.0.2.15       HTTP        784 HTTP/1.1 200 OK  (text/html)
  12 0.466214955  10.0.2.15       128.119.245.12  HTTP        352 GET /favicon.ico HTTP/1.1
  17 0.522539428  10.0.2.15       128.119.245.12  HTTP        292 GET /favicon.ico HTTP/1.1
  19 0.523116213  128.119.245.12  10.0.2.15       HTTP        538 HTTP/1.1 404 Not Found  (text/html)
  23 0.576195463  128.119.245.12  10.0.2.15       HTTP        539 HTTP/1.1 404 Not Found  (text/html)
  37 7.368983016  10.0.2.15       128.119.245.12  HTTP        523 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  39 7.417888795  128.119.245.12  10.0.2.15       HTTP        294 HTTP/1.1 304 Not Modified
```

```
    Last-Modified: Thu, 08 Nov 2018 06:59:01 GMT\r\n
    ETag: "173-57a21c503e786"\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 1/2]
    [Time since request: 0.202112038 seconds]
    [Request in frame: 8]
    [Next request in frame: 12]
    [Next response in frame: 19]
    File Data: 371 bytes
▾ Line-based text data: text/html (10 lines)
    \n
    <html>\n
    \n
    Congratulations again!  Now you've downloaded the file lab2-2.html. <br>\n
    This file's last modification date will not change.  <p>\n
    Thus  if you download this multiple times on your browser, a complete copy <br>\n
    will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
    field in your browser's HTTP GET request to the server.\n
    \n
    </html>\n
```

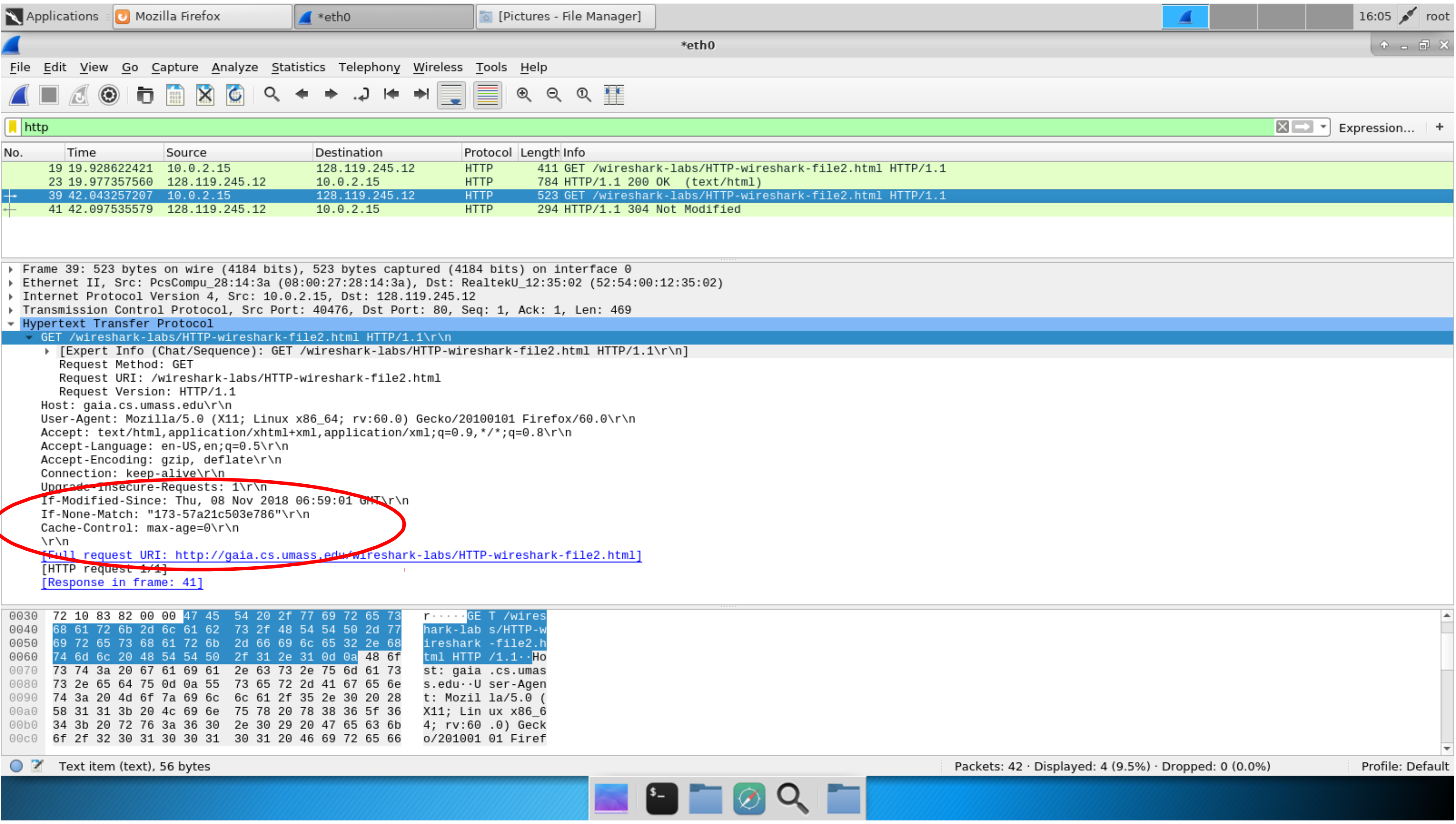
```
0000  08 00 27 28 14 3a 52 54  00 12 35 02 08 00 45 00   ··'(·:RT ··5···E·
0010  03 02 02 3a 00 00 40 06  f4 29 80 77 f5 0c 0a 00   ···:··@· ·)·w····
```

Hypertext Transfer Protocol: Protocol

Packets: 40 · Displayed: 8 (20.0%) · Dropped: 0 (0.0%)

Profile: Default

10. Yes, the line exists in the second HTTP GET request. If-non-match and cache-control follow.


Applications
Mozilla Firefox
*eth0
[Pictures - File Manager]
16:05
root
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression…

```
No.   Time          Source           Destination      Protocol Length Info
   19 19.928622421  10.0.2.15        128.119.245.12   HTTP      411 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   23 19.977357560  128.119.245.12   10.0.2.15        HTTP      784 HTTP/1.1 200 OK  (text/html)
   39 42.043257207  10.0.2.15        128.119.245.12   HTTP      523 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   41 42.097535579  128.119.245.12   10.0.2.15        HTTP      294 HTTP/1.1 304 Not Modified
```

```
Frame 39: 523 bytes on wire (4184 bits), 523 bytes captured (4184 bits) on interface 0
Ethernet II, Src: PcsCompu_28:14:3a (08:00:27:28:14:3a), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 40476, Dst Port: 80, Seq: 1, Ack: 1, Len: 469
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]
    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:60.0) Gecko/20100101 Firefox/60.0\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
  Upgrade-Insecure-Requests: 1\r\n
  If-Modified-Since: Thu, 08 Nov 2018 06:59:01 GMT\r\n
  If-None-Match: "173-57a21c503e786"\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: 41]
```

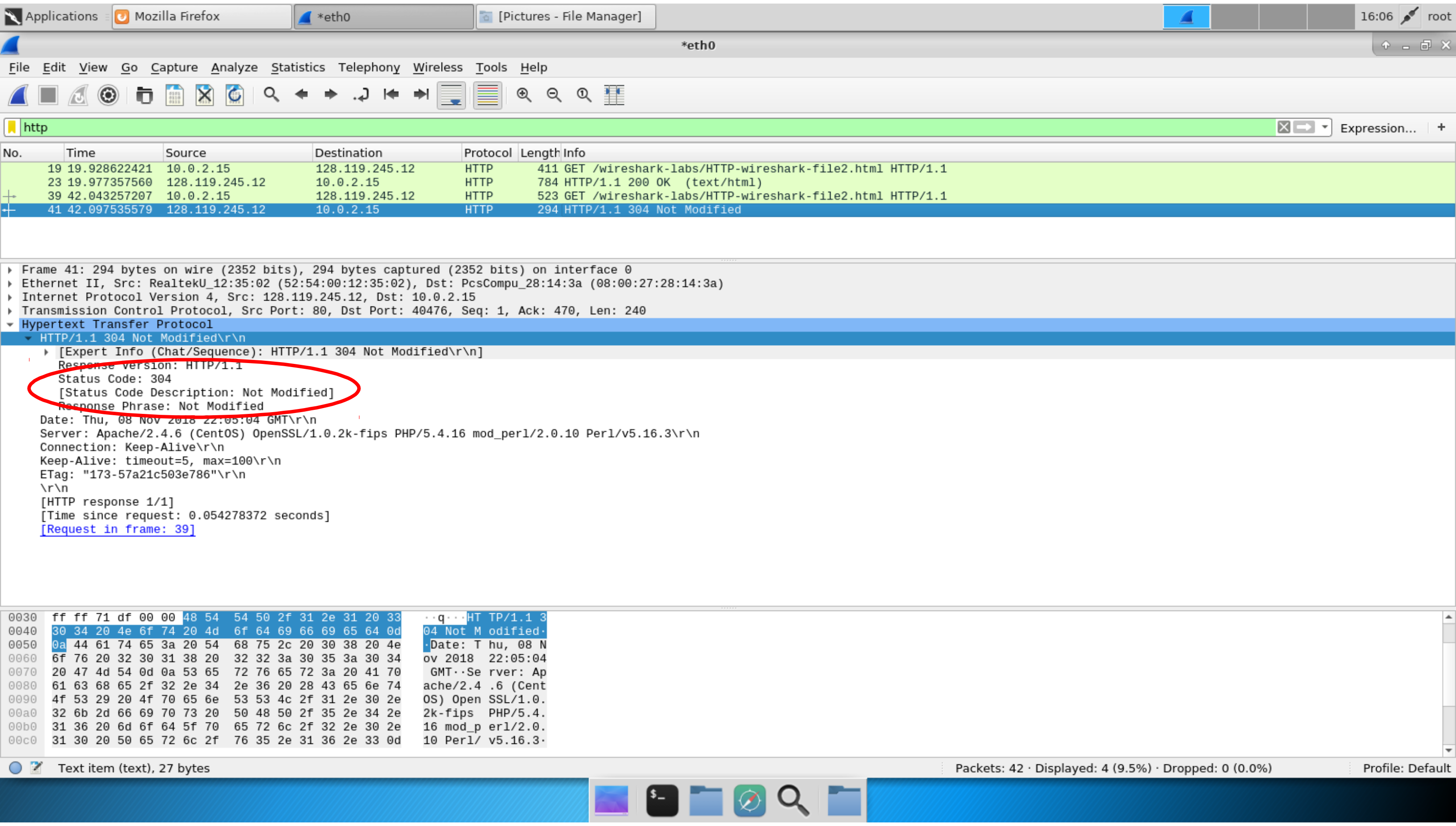
```
0030  72 10 83 82 00 00 47 45  54 20 2f 77 69 72 65 73   r·····GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 32 2e 68   ireshark -file2.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
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 55  73 65 72 2d 41 67 65 6e   s.edu··U ser-Agen
0090  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil la/5.0 (
00a0  58 31 31 3b 20 4c 69 6e  75 78 20 78 38 36 5f 36   X11; Lin ux x86_6
00b0  34 3b 20 72 76 3a 36 30  2e 30 29 20 47 65 63 6b   4; rv:60 .0) Geck
00c0  6f 2f 32 30 31 30 30 31  30 31 20 46 69 72 65 66   o/201001 01 Firef
```

Text item (text), 56 bytes

Packets: 42 · Displayed: 4 (9.5%) · Dropped: 0 (0.0%)

Profile: Default

11. The status code is 304 and response phrase is ‘Not Modified’


Applications
Mozilla Firefox
*eth0
[Pictures - File Manager]
16:06
root
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

http

```
No.  Time          Source          Destination     Protocol Length Info
  19 19.928622421  10.0.2.15       128.119.245.12  HTTP      411 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  23 19.977357560  128.119.245.12  10.0.2.15       HTTP      784 HTTP/1.1 200 OK  (text/html)
  39 42.043257207  10.0.2.15       128.119.245.12  HTTP      523 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  41 42.097535579  128.119.245.12  10.0.2.15       HTTP      294 HTTP/1.1 304 Not Modified
```

```
Frame 41: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface 0
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_28:14:3a (08:00:27:28:14:3a)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 80, Dst Port: 40476, Seq: 1, Ack: 470, Len: 240
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: Thu, 08 Nov 2018 22:05:04 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
  Connection: Keep-Alive\r\n
  Keep-Alive: timeout=5, max=100\r\n
  ETag: "173-57a21c503e786"\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.054278372 seconds]
  [Request in frame: 39]
```

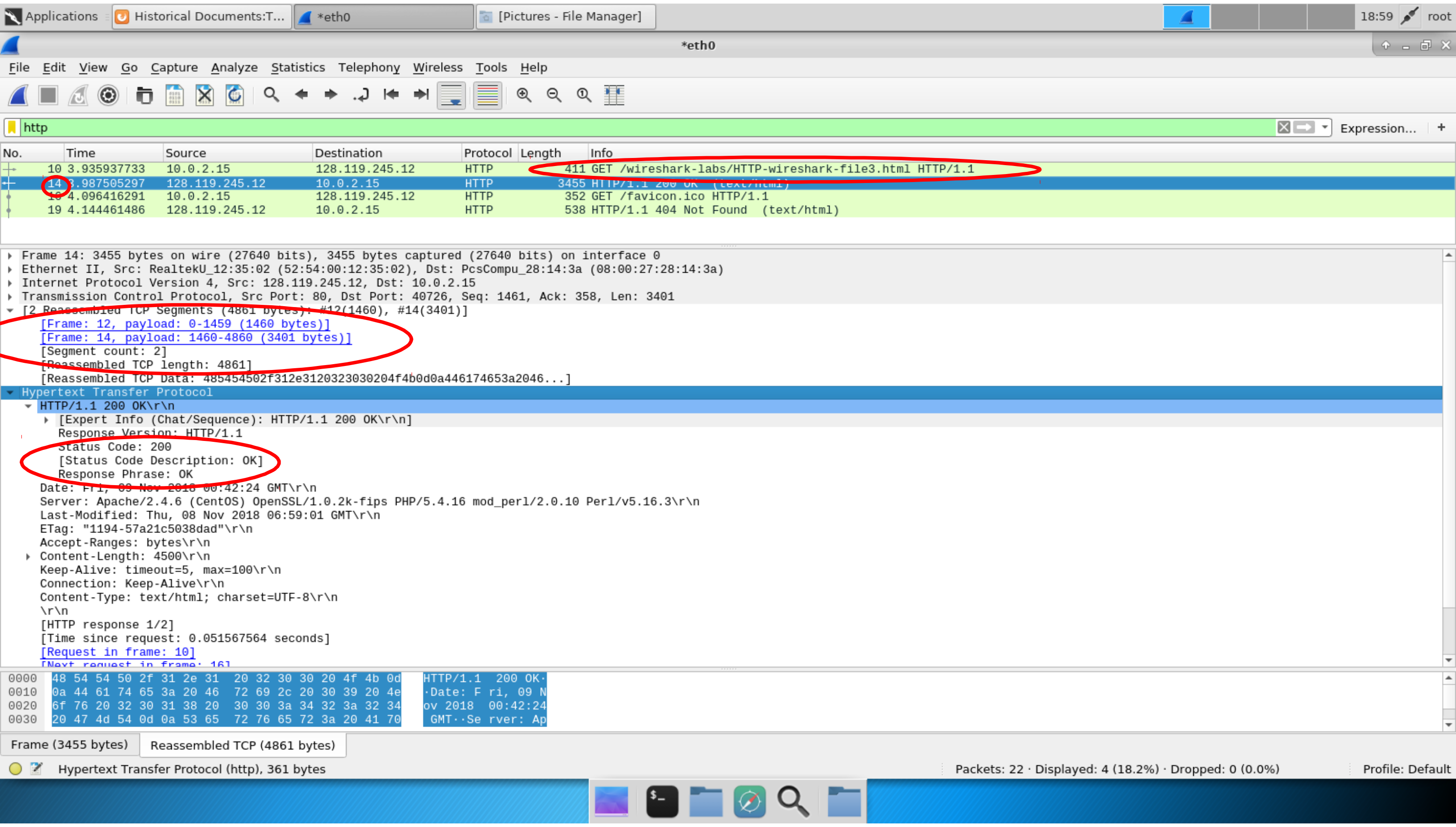
```
0030  ff ff 71 df 00 00 48 54  54 50 2f 31 2e 31 20 33   ··q···HT TP/1.1 3
0040  30 34 20 4e 6f 74 20 4d  6f 64 69 66 69 65 64 0d   04 Not M odified·
0050  0a 44 61 74 65 3a 20 54  68 75 2c 20 30 38 20 4e   ·Date: T hu, 08 N
0060  6f 76 20 32 30 31 38 20  32 32 3a 30 35 3a 30 34   ov 2018  22:05:04
0070  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT··Se rver: Ap
0080  61 63 68 65 2f 32 2e 34  2e 36 20 28 43 65 6e 74   ache/2.4 .6 (Cent
0090  4f 53 29 20 4f 70 65 6e  53 53 4c 2f 31 2e 30 2e   OS) Open SSL/1.0.
00a0  32 6b 2d 66 69 70 73 20  50 48 50 2f 35 2e 34 2e   2k-fips  PHP/5.4.
00b0  31 36 20 6d 6f 64 5f 70  65 72 6c 2f 32 2e 30 2e   16 mod_p erl/2.0.
00c0  31 30 20 50 65 72 6c 2f  76 35 2e 31 36 2e 33 0d   10 Perl/ v5.16.3·
```

Text item (text), 27 bytes

Packets: 42 · Displayed: 4 (9.5%) · Dropped: 0 (0.0%)

Profile: Default

12. My browser sent 1 GET request for the .html and one for favicon.ico, which returns 404 not found from the server. Packet number 10 contains the GET for the Bill of Rights.
13. Packet 14
14. Status Code is 200 Phrase is ‘OK’
15. 2 Re-assembled TCP Segments 1460+3401 bytes for a total of 4861 bytes.


Applications
Historical Documents:T...
*eth0
[Pictures - File Manager]
18:59
root
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

```
http
```

```
No.  Time         Source          Destination     Protocol Length Info
  10 3.935937733  10.0.2.15       128.119.245.12  HTTP      411 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  14 3.987505297  128.119.245.12  10.0.2.15       HTTP     3455 HTTP/1.1 200 OK  (text/html)
  16 4.096416291  10.0.2.15       128.119.245.12  HTTP      352 GET /favicon.ico HTTP/1.1
  19 4.144461486  128.119.245.12  10.0.2.15       HTTP      538 HTTP/1.1 404 Not Found  (text/html)
```

```
▸ Frame 14: 3455 bytes on wire (27640 bits), 3455 bytes captured (27640 bits) on interface 0
▸ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_28:14:3a (08:00:27:28:14:3a)
▸ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.2.15
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 40726, Seq: 1461, Ack: 358, Len: 3401
▾ [2 Reassembled TCP Segments (4861 bytes): #12(1460), #14(3401)]
    [Frame: 12, payload: 0-1459 (1460 bytes)]
    [Frame: 14, payload: 1460-4860 (3401 bytes)]
    [Segment count: 2]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2046...]
▾ Hypertext Transfer Protocol
  ▾ HTTP/1.1 200 OK\r\n
    ▸ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Fri, 09 Nov 2018 00:42:24 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Thu, 08 Nov 2018 06:59:01 GMT\r\n
    ETag: "1194-57a21c5038dad"\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 1/2]
    [Time since request: 0.051567564 seconds]
    [Request in frame: 10]
    [Next request in frame: 16]
```

```
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 46  72 69 2c 20 30 39 20 4e   ·Date: F ri, 09 N
0020  6f 76 20 32 30 31 38 20  30 30 3a 34 32 3a 32 34   ov 2018  00:42:24
0030  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT··Se rver: Ap
```

Frame (3455 bytes) | Reassembled TCP (4861 bytes)

Hypertext Transfer Protocol (http), 361 bytes

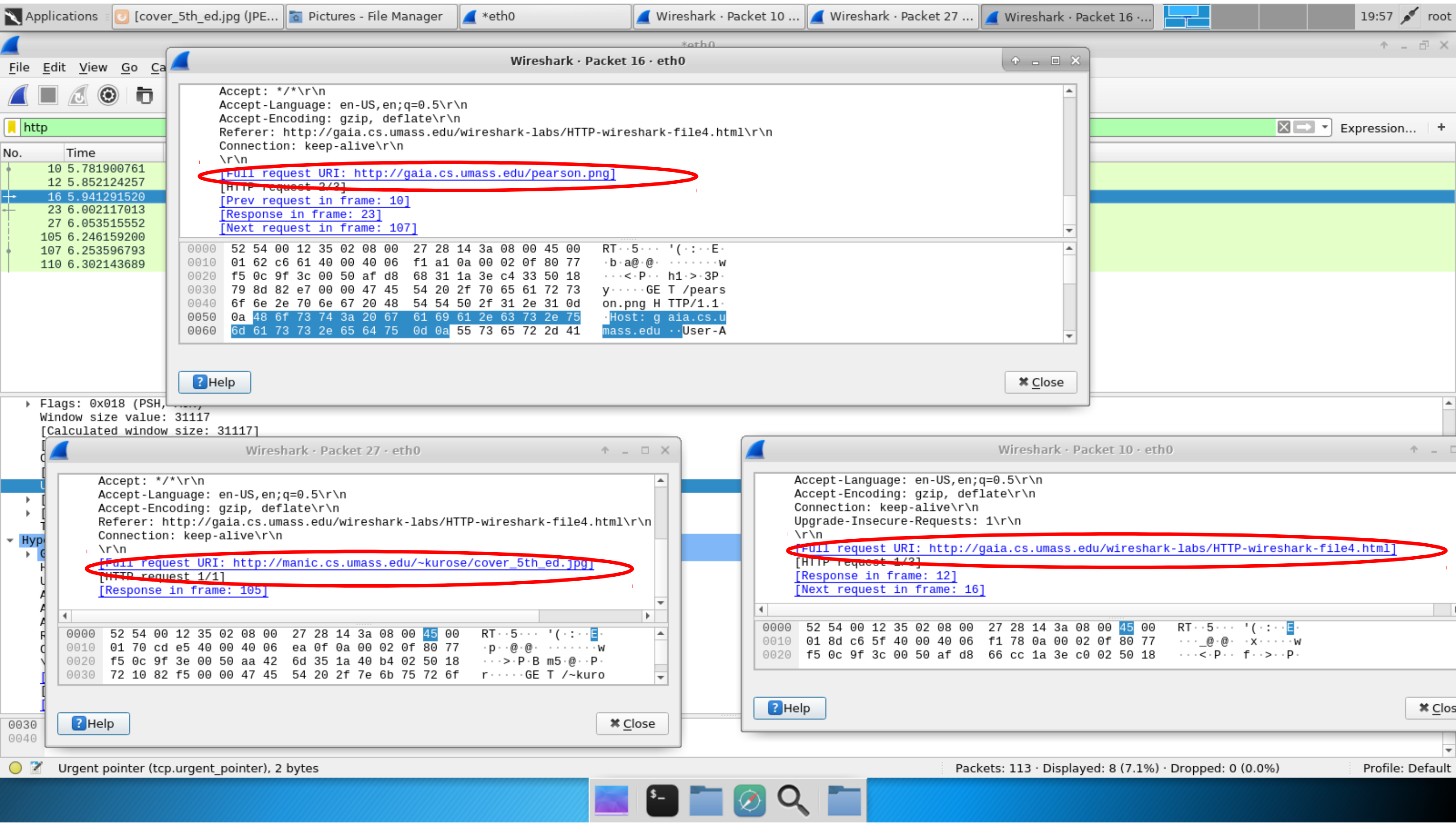
Packets: 22 · Displayed: 4 (18.2%) · Dropped: 0 (0.0%)

Profile: Default

16. Ignoring the 404 not found returned from a GET for an icon image, there are 3 GET requests. These were sent to:

http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html
http://gaia.cs.umass.edu/pearson.png
http://manic.cs.umass.edu/~kurose/cover_5th_ed.jpg

all show as IP 128.119.245.12 as highlighted as the destination for these requests



Applications
[cover_5th_ed.jpg (JPE...
Pictures - File Manager
*eth0
Wireshark · Packet 10 ...
Wireshark · Packet 27 ...
Wireshark · Packet 16 ·...
19:57
root
File Edit View Go Ca
http
Expression...

```
No.  Time
  10 5.781900761
  12 5.852124257
  16 5.941291520
  23 6.002117013
  27 6.053515552
 105 6.246159200
 107 6.253596793
 110 6.302143689
```

Wireshark · Packet 16 · eth0

```
    Accept: */*\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/pearson.png]
    [HTTP request 2/3]
    [Prev request in frame: 10]
    [Response in frame: 23]
    [Next request in frame: 107]
```

```
0000  52 54 00 12 35 02 08 00  27 28 14 3a 08 00 45 00   RT··5···  '(·:··E·
0010  01 62 c6 61 40 00 40 06  f1 a1 0a 00 02 0f 80 77   ·b·a@·@·  ·······w
0020  f5 0c 9f 3c 00 50 af d8  68 31 1a 3e c4 33 50 18   ···<·P··  h1·>·3P·
0030  79 8d 82 e7 00 00 47 45  54 20 2f 70 65 61 72 73   y·····GE  T /pears
0040  6f 6e 2e 70 6e 67 20 48  54 54 50 2f 31 2e 31 0d   on.png H  TTP/1.1·
0050  0a 48 6f 73 74 3a 20 67  61 69 61 2e 63 73 2e 75   ·Host: g  aia.cs.u
0060  6d 61 73 73 2e 65 64 75  0d 0a 55 73 65 72 2d 41   mass.edu  ··User-A
```

```
  Flags: 0x018 (PSH, ACK)
  Window size value: 31117
  [Calculated window size: 31117]
```

Wireshark · Packet 27 · eth0

```
    Accept: */*\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://manic.cs.umass.edu/~kurose/cover_5th_ed.jpg]
    [HTTP request 1/1]
    [Response in frame: 105]
```

```
0000  52 54 00 12 35 02 08 00  27 28 14 3a 08 00 45 00   RT··5···  '(·:··E·
0010  01 70 cd e5 40 00 40 06  ea 0f 0a 00 02 0f 80 77   ·p··@·@·  ·······w
0020  f5 0c 9f 3e 00 50 aa 42  6d 35 1a 40 b4 02 50 18   ···>·P·B  m5·@··P·
0030  72 10 82 f5 00 00 47 45  54 20 2f 7e 6b 75 72 6f   r·····GE  T /~kuro
```

Wireshark · Packet 10 · eth0

```
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\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]
    [HTTP request 1/3]
    [Response in frame: 12]
    [Next request in frame: 16]
```

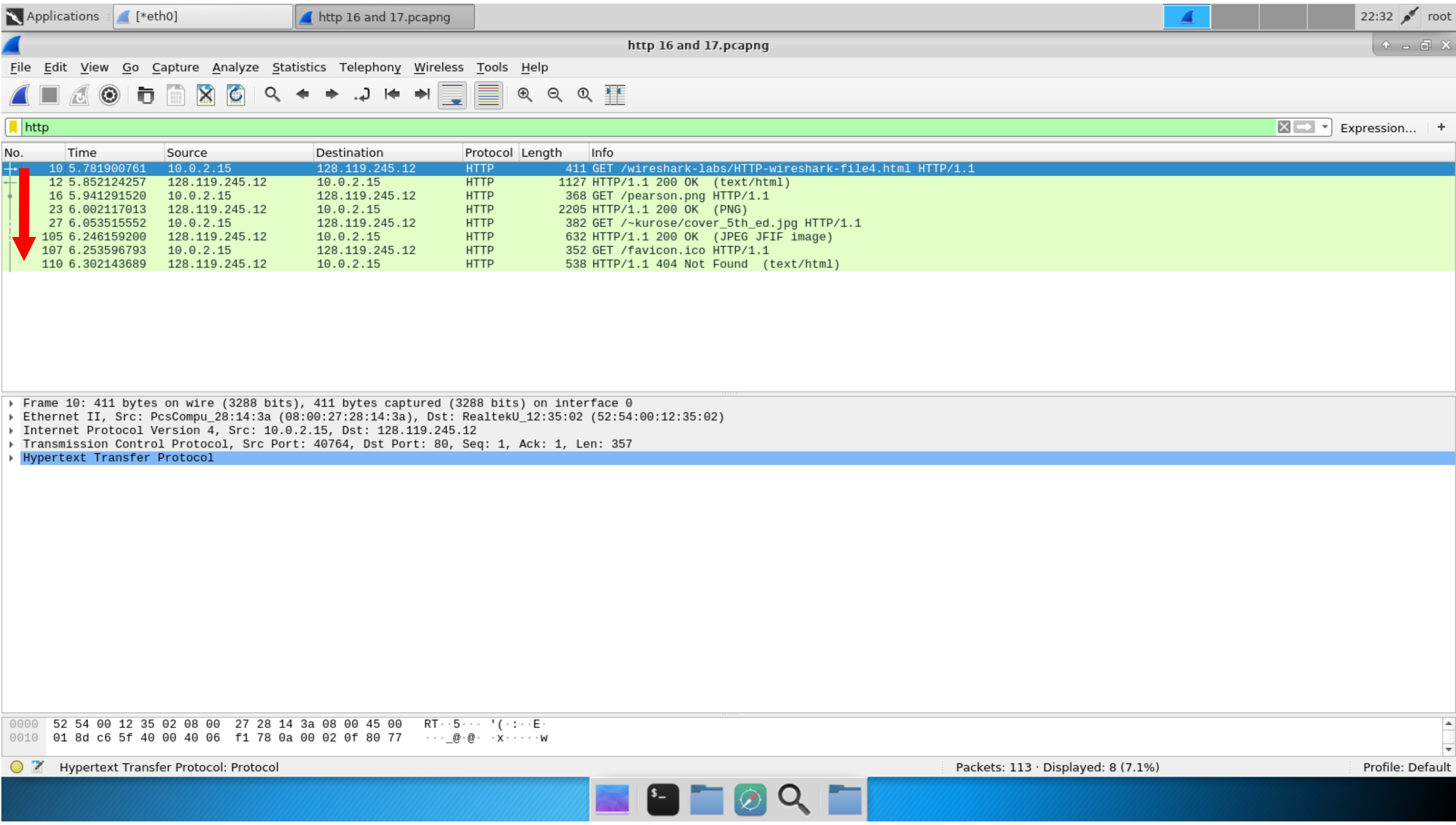
```
0000  52 54 00 12 35 02 08 00  27 28 14 3a 08 00 45 00   RT··5···  '(·:··E·
0010  01 8d c6 5f 40 00 40 06  f1 78 0a 00 02 0f 80 77   ···_@·@·  ·x·····w
0020  f5 0c 9f 3c 00 50 af d8  66 cc 1a 3e c0 02 50 18   ···<·P··  f··>··P·
```

Urgent pointer (tcp.urgent_pointer), 2 bytes

Packets: 113 · Displayed: 8 (7.1%) · Dropped: 0 (0.0%)

Profile: Default

17. Packet 23 contains the image for GET request at packet 16. Packet 105 contains the jpeg image for GET request 27. These requests are being made serially as they come one after another. This can be seen in the Frame data on the timestamp as well.



http

```
No.   Time           Source           Destination      Protocol Length Info
   10 5.781900761    10.0.2.15        128.119.245.12   HTTP      411 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
   12 5.852124257    128.119.245.12   10.0.2.15        HTTP     1127 HTTP/1.1 200 OK  (text/html)
   16 5.941291520    10.0.2.15        128.119.245.12   HTTP      368 GET /pearson.png HTTP/1.1
   23 6.002117013    128.119.245.12   10.0.2.15        HTTP     2205 HTTP/1.1 200 OK  (PNG)
   27 6.053515552    10.0.2.15        128.119.245.12   HTTP      382 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
  105 6.246159200    128.119.245.12   10.0.2.15        HTTP      632 HTTP/1.1 200 OK  (JPEG JFIF image)
  107 6.253596793    10.0.2.15        128.119.245.12   HTTP      352 GET /favicon.ico HTTP/1.1
  110 6.302143689    128.119.245.12   10.0.2.15        HTTP      538 HTTP/1.1 404 Not Found  (text/html)
```

```
▸ Frame 10: 411 bytes on wire (3288 bits), 411 bytes captured (3288 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_28:14:3a (08:00:27:28:14:3a), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 128.119.245.12
▸ Transmission Control Protocol, Src Port: 40764, Dst Port: 80, Seq: 1, Ack: 1, Len: 357
▸ Hypertext Transfer Protocol
```

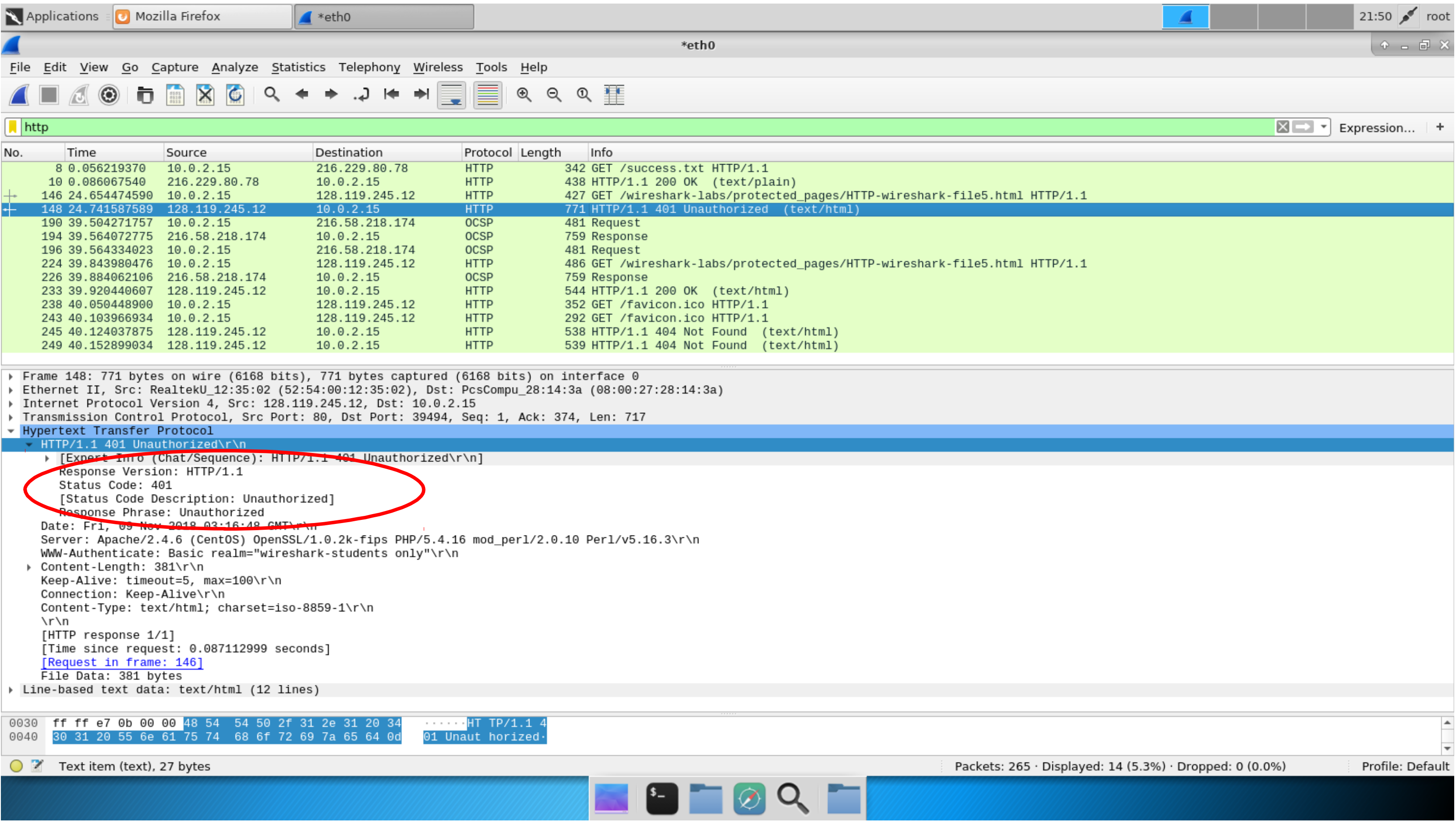
```
0000  52 54 00 12 35 02 08 00  27 28 14 3a 08 00 45 00   RT··5···  '(·:··E·
0010  01 8d c6 5f 40 00 40 06  f1 78 0a 00 02 0f 80 77   ···_@·@·  ·x·····w
```

Hypertext Transfer Protocol: Protocol

Packets: 113 · Displayed: 8 (7.1%)

Profile: Default

18. The initial GET is for success.txt, this response code and phrase is 200, OK.
The second GET, packet 146, is for the protected page and the response status code and phrase is 401 Authorization Required in packet 148.



Applications
Mozilla Firefox
*eth0
21:50
root
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

```
http
```

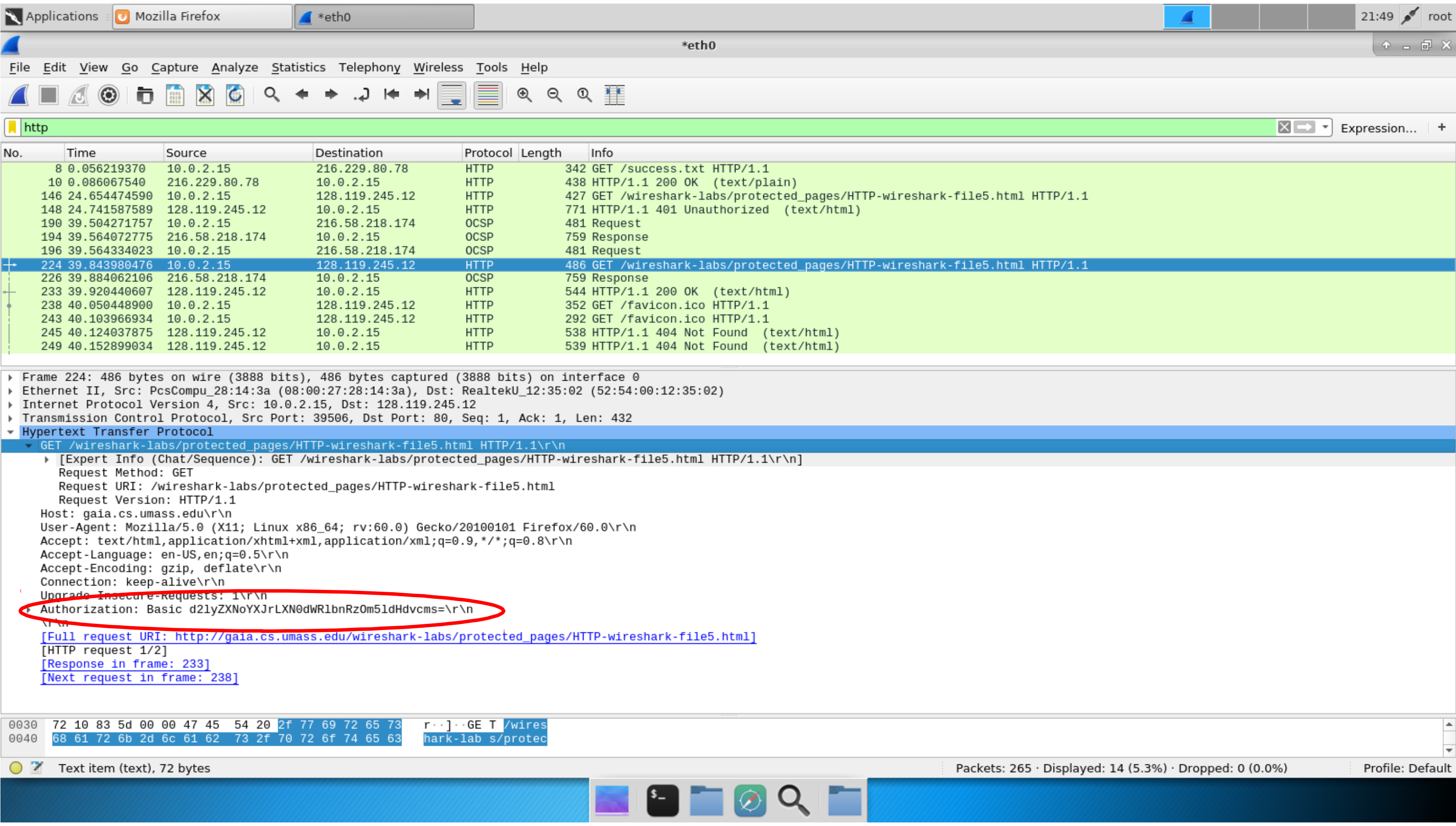
```
No.  Time          Source           Destination      Protocol Length Info
   8 0.056219370   10.0.2.15        216.229.80.78    HTTP       342 GET /success.txt HTTP/1.1
  10 0.086067540   216.229.80.78    10.0.2.15        HTTP       438 HTTP/1.1 200 OK  (text/plain)
 146 24.654474590  10.0.2.15        128.119.245.12   HTTP       427 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
 148 24.741587589  128.119.245.12   10.0.2.15        HTTP       771 HTTP/1.1 401 Unauthorized  (text/html)
 190 39.504271757  10.0.2.15        216.58.218.174   OCSP       481 Request
 194 39.564072775  216.58.218.174   10.0.2.15        OCSP       759 Response
 196 39.564334023  10.0.2.15        216.58.218.174   OCSP       481 Request
 224 39.843980476  10.0.2.15        128.119.245.12   HTTP       486 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
 226 39.884062106  216.58.218.174   10.0.2.15        OCSP       759 Response
 233 39.920440607  128.119.245.12   10.0.2.15        HTTP       544 HTTP/1.1 200 OK  (text/html)
 238 40.050448900  10.0.2.15        128.119.245.12   HTTP       352 GET /favicon.ico HTTP/1.1
 243 40.103966934  10.0.2.15        128.119.245.12   HTTP       292 GET /favicon.ico HTTP/1.1
 245 40.124037875  128.119.245.12   10.0.2.15        HTTP       538 HTTP/1.1 404 Not Found  (text/html)
 249 40.152899034  128.119.245.12   10.0.2.15        HTTP       539 HTTP/1.1 404 Not Found  (text/html)
```

```
▸ Frame 148: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface 0
▸ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_28:14:3a (08:00:27:28:14:3a)
▸ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.2.15
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 39494, Seq: 1, Ack: 374, Len: 717
▾ Hypertext Transfer Protocol
  ▾ HTTP/1.1 401 Unauthorized\r\n
    ▸ [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
      Response Version: HTTP/1.1
      Status Code: 401
      [Status Code Description: Unauthorized]
      Response Phrase: Unauthorized
    Date: Fri, 09 Nov 2018 03:16:48 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    WWW-Authenticate: Basic realm="wireshark-students only"\r\n
  ▸ Content-Length: 381\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.087112999 seconds]
    [Request in frame: 146]
    File Data: 381 bytes
▸ Line-based text data: text/html (12 lines)
```

```
0030  ff ff e7 0b 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·
```

Text item (text), 27 bytes   Packets: 265 · Displayed: 14 (5.3%) · Dropped: 0 (0.0%)   Profile: Default

19. Authorization: Basic is the new field.



Applications
Mozilla Firefox
*eth0
21:49
root
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression…
+

```
No.   Time          Source           Destination      Protocol Length Info
    8 0.056219370   10.0.2.15        216.229.80.78    HTTP        342 GET /success.txt HTTP/1.1
   10 0.086067540   216.229.80.78    10.0.2.15        HTTP        438 HTTP/1.1 200 OK  (text/plain)
  146 24.654474590  10.0.2.15        128.119.245.12   HTTP        427 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
  148 24.741587589  128.119.245.12   10.0.2.15        HTTP        771 HTTP/1.1 401 Unauthorized  (text/html)
  190 39.504271757  10.0.2.15        216.58.218.174   OCSP        481 Request
  194 39.564072775  216.58.218.174   10.0.2.15        OCSP        759 Response
  196 39.564334023  10.0.2.15        216.58.218.174   OCSP        481 Request
  224 39.843980476  10.0.2.15        128.119.245.12   HTTP        486 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
  226 39.884062106  216.58.218.174   10.0.2.15        OCSP        759 Response
  233 39.920440607  128.119.245.12   10.0.2.15        HTTP        544 HTTP/1.1 200 OK  (text/html)
  238 40.050448900  10.0.2.15        128.119.245.12   HTTP        352 GET /favicon.ico HTTP/1.1
  243 40.103966934  10.0.2.15        128.119.245.12   HTTP        292 GET /favicon.ico HTTP/1.1
  245 40.124037875  128.119.245.12   10.0.2.15        HTTP        538 HTTP/1.1 404 Not Found  (text/html)
  249 40.152899034  128.119.245.12   10.0.2.15        HTTP        539 HTTP/1.1 404 Not Found  (text/html)
```

```
Frame 224: 486 bytes on wire (3888 bits), 486 bytes captured (3888 bits) on interface 0
Ethernet II, Src: PcsCompu_28:14:3a (08:00:27:28:14:3a), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 39506, Dst Port: 80, Seq: 1, Ack: 1, Len: 432
Hypertext Transfer Protocol
  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
  Host: gaia.cs.umass.edu\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0\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
  Upgrade-Insecure-Requests: 1\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 1/2]
  [Response in frame: 233]
  [Next request in frame: 238]
```

```
0030  72 10 83 5d 00 00 47 45  54 20 2f 77 69 72 65 73   r··]··GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 70 72 6f 74 65 63   hark-lab s/protec
```

Text item (text), 72 bytes

Packets: 265 · Displayed: 14 (5.3%) · Dropped: 0 (0.0%)

Profile: Default