Ethereal Lab: HTTP

1. The Basic HTTP GET/response interaction

```
No.     Time        Source                Destination
Protocol Info
   1190 131.859385  128.238.245.34        128.119.245.12        HTTP
GET /ethereal-labs/HTTP-ethereal-file1.html HTTP/1.1

Hypertext Transfer Protocol
    GET /ethereal-labs/HTTP-ethereal-file1.html HTTP/1.1\r\n
    Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/x-shockwave-flash, */*\r\n
    Accept-Language: en-us\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1;
.NET CLR 1.1.4322)\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: Keep-Alive\r\n
    \r\n
```

```
No.     Time        Source                Destination
Protocol Info
   1192 131.875550  128.119.245.12        128.238.245.34        HTTP
HTTP/1.1 200 OK (text/html)

Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Fri, 15 Oct 2004 18:13:19 GMT\r\n
    Server: Apache/2.0.40 (Red Hat Linux)\r\n
    Last-Modified: Fri, 15 Oct 2004 18:13:01 GMT\r\n
    ETag: "1bbf0-7e-60996540"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 126\r\n
    Keep-Alive: timeout=10, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=ISO-8859-1\r\n
    \r\n
Line-based text data: text/html
    <html>
    Congratulations.  You've downloaded the file
    http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-file1.html!
    </html>
```

Answer the following questions:

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

2. What languages (if any) does your browser indicate that it can accept to the server?
Answer: `Accept-Language: en-us`

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?
Answer: My IP address is `128.238.245.34` and the server's is `128.119.245.12`

4. What is the status code returned from the server to your browser?
Answer: `HTTP/1.1 200 OK (text/html)`

5. When was the HTML file that you are retrieving last modified at the server?
Answer: `Last-Modified: Fri, 15 Oct 2004 18:13:01 GMT`

6. How many bytes of content are being returned to your browser?
Answer: `Content-Length: 126`

7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.
Answer: No all of the headers can be found in the raw data.

2. The HTTP CONDITIONAL GET/response interaction

```
No.     Time        Source                Destination
Protocol Info
     72 6.592603    128.238.245.34        128.119.245.12        HTTP
GET /ethereal-labs/HTTP-ethereal-file2.html HTTP/1.1

Frame 72 (403 bytes on wire, 403 bytes captured)
    Arrival Time: Oct 15, 2004 15:21:06.783195000
    Time delta from previous packet: 6.592603000 seconds
    Time since reference or first frame: 6.592603000 seconds
    Frame Number: 72
    Packet Length: 403 bytes
    Capture Length: 403 bytes
Hypertext Transfer Protocol
    GET /ethereal-labs/HTTP-ethereal-file2.html HTTP/1.1\r\n
    Accept: */*\r\n
    Accept-Language: en-us\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1;
.NET CLR 1.1.4322)\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: Keep-Alive\r\n
    \r\n

No.     Time        Source                Destination
Protocol Info
     74 6.608674    128.119.245.12        128.238.245.34        HTTP
HTTP/1.1 200 OK (text/html)

Frame 74 (739 bytes on wire, 739 bytes captured)
    Arrival Time: Oct 15, 2004 15:21:06.799266000
    Time delta from previous packet: 0.016071000 seconds
    Time since reference or first frame: 6.608674000 seconds
    Frame Number: 74
    Packet Length: 739 bytes
    Capture Length: 739 bytes
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Fri, 15 Oct 2004 19:21:11 GMT\r\n
    Server: Apache/2.0.40 (Red Hat Linux)\r\n
    Last-Modified: Fri, 15 Oct 2004 19:21:01 GMT\r\n
    ETag: "1bfef-173-53c94140"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 371\r\n
    Keep-Alive: timeout=10, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=ISO-8859-1\r\n
    \r\n
Line-based text data: text/html

    <html>

    Congratulations again!  Now you've downloaded the file lab2-2.html.
<br>
    This file's last modification date will not change.  <p>
    Thus  if you download this multiple times on your browser, a
complete copy <br>
    will only be sent once by the server due to the inclusion of the
IN-MODIFIED-SINCE<br>
    field in your browser's HTTP GET request to the server.

    </html>

No.     Time        Source                Destination
Protocol Info
    118 10.458581   128.238.245.34        128.119.245.12        HTTP
GET /ethereal-labs/HTTP-ethereal-file2.html HTTP/1.1

Frame 118 (403 bytes on wire, 403 bytes captured)
    Arrival Time: Oct 15, 2004 15:21:10.649173000
    Time delta from previous packet: 3.849907000 seconds
    Time since reference or first frame: 10.458581000 seconds
    Frame Number: 118
    Packet Length: 403 bytes
    Capture Length: 403 bytes
Hypertext Transfer Protocol
    GET /ethereal-labs/HTTP-ethereal-file2.html HTTP/1.1\r\n
    Accept: */*\r\n
    Accept-Language: en-us\r\n
    Accept-Encoding: gzip, deflate\r\n
    If-Modified-Since: Fri, 15 Oct 2004 19:21:01 GMT\r\n
    If-None-Match: "1bfef-173-53c94140"\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1;
.NET CLR 1.1.4322)\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: Keep-Alive\r\n
    \r\n
```

```
No.     Time        Source                Destination
Protocol Info
    119 10.471105   128.119.245.12        128.238.245.34        HTTP
HTTP/1.1 304 Not Modified

Frame 119 (243 bytes on wire, 243 bytes captured)
    Arrival Time: Oct 15, 2004 15:21:10.661697000
    Time delta from previous packet: 0.012524000 seconds
    Time since reference or first frame: 10.471105000 seconds
    Frame Number: 119
    Packet Length: 243 bytes
    Capture Length: 243 bytes
Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
    Date: Fri, 15 Oct 2004 19:21:14 GMT\r\n
    Server: Apache/2.0.40 (Red Hat Linux)\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=10, max=99\r\n
    ETag: "1bfef-173-53c94140"\r\n
    \r\n
```

Answer the following questions:

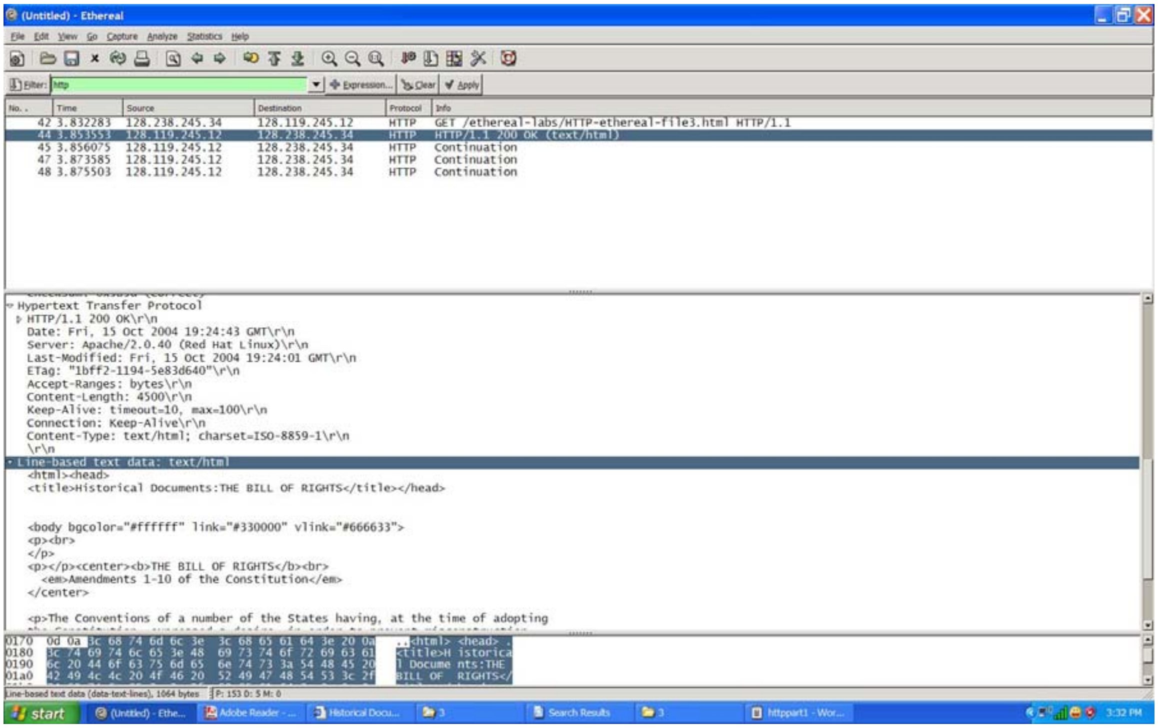
8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?
Answer: No

9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
Answer: Yes because we can see the contents in the `Line-based text data` field.

10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?
Answer: Yes. The information followed is: `Fri, 15 Oct 2004 19:21:01 GMT\r\n` which is the date of the last modification of the file from the previous get request.

11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.
Answer: The status code and phrase returned from the server is `HTTP/1.1 304 Not Modified.` The server didn’t return the contents of the file since the browser loaded it from its cache.

3. Retrieving Long Documents



(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: http
Expression... Clear Apply

```
No. .  Time      Source          Destination     Protocol Info
   42 3.832283  128.238.245.34  128.119.245.12  HTTP     GET /ethereal-labs/HTTP-ethereal-file3.html HTTP/1.1
   44 3.853553  128.119.245.12  128.238.245.34  HTTP     HTTP/1.1 200 OK (text/html)
   45 3.856075  128.119.245.12  128.238.245.34  HTTP     Continuation
   47 3.873585  128.119.245.12  128.238.245.34  HTTP     Continuation
   48 3.875503  128.119.245.12  128.238.245.34  HTTP     Continuation
```

```
Hypertext Transfer Protocol
 HTTP/1.1 200 OK\r\n
  Date: Fri, 15 Oct 2004 19:24:43 GMT\r\n
  Server: Apache/2.0.40 (Red Hat Linux)\r\n
  Last-Modified: Fri, 15 Oct 2004 19:24:01 GMT\r\n
  ETag: "1bff2-1194-5e83d640"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 4500\r\n
  Keep-Alive: timeout=10, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html; charset=ISO-8859-1\r\n
  \r\n
Line-based text data: text/html
  <html><head>
  <title>Historical Documents:THE BILL OF RIGHTS</title></head>


  <body bgcolor="#ffffff" link="#330000" vlink="#666633">
  <p><br>
  </p>
  <p></p><center><b>THE BILL OF RIGHTS</b><br>
    <em>Amendments 1-10 of the Constitution</em>
  </center>

  <p>The Conventions of a number of the States having, at the time of adopting
```

```
0170  0d 0a 3c 68 74 6d 6c 3e  3c 68 65 61 64 3e 20 0a   ..<html> <head> .
0180  3c 74 69 74 6c 65 3e 48  69 73 74 6f 72 69 63 61   <title>H istorica
0190  6c 20 44 6f 63 75 6d 65  6e 74 73 3a 54 48 45 20   l Docume nts:THE 
01a0  42 49 4c 4c 20 4f 46 20  52 49 47 48 54 53 3c 2f   BILL OF  RIGHTS</
```

Answer the following questions:

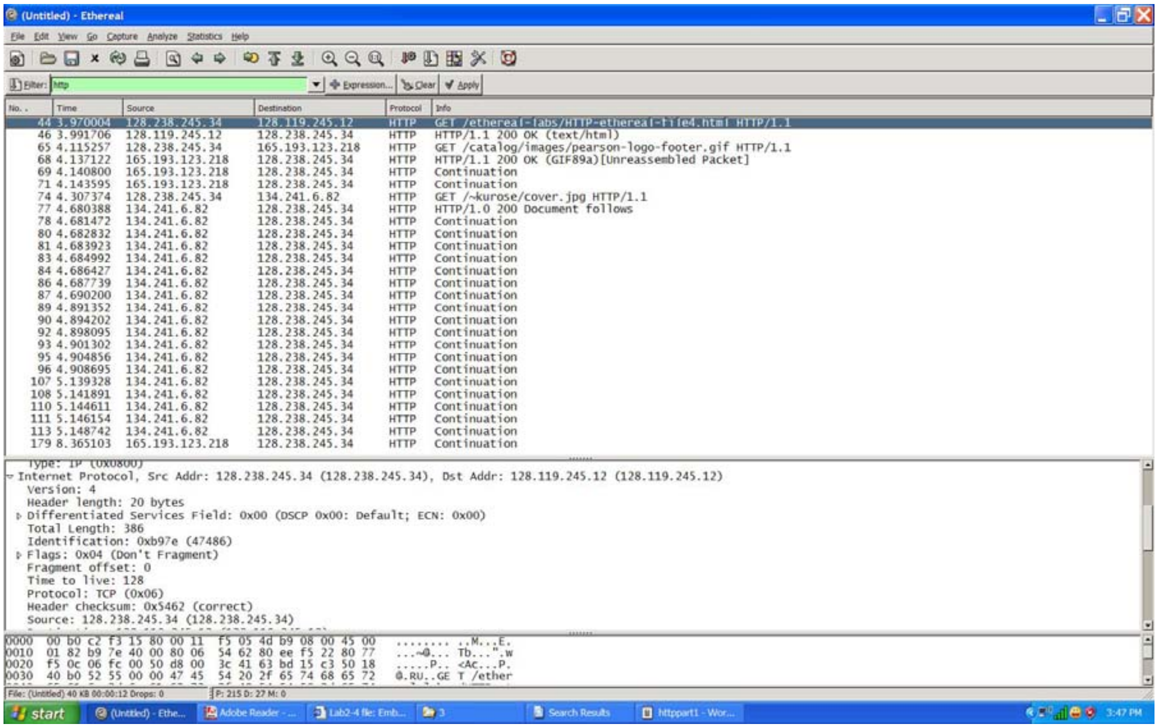
12. How many HTTP GET request messages were sent by your browser?
Answer: There was 1 HTTP GET request message sent by my browser as seen in the screenshot.

13. How many data-containing TCP segments were needed to carry the single HTTP response?
Answer: There were 4 data containing TCP segments containing 1064 ,1380 ,1380 and 679 bytes respectively for a total of 4500 bytes.

14. What is the status code and phrase associated with the response to the HTTP GET request?
Answer: 200 OK

15. Are there any HTTP status lines in the transmitted data associated with a TCP induced “Continuation”?
Answer: No

4. HTML Documents with Embedded Objects


(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Expression... Clear Apply
start (Untitled) - Ethe... Adobe Reader - ... Lab2-4 file: Emb... 3 Search Results httppart1 - Wor...
3:47 PM

Filter: http

```
No. .  Time      Source           Destination      Protocol Info
   44 3.970004  128.238.245.34   128.119.245.12   HTTP     GET /ethereal-labs/HTTP-ethereal-file4.html HTTP/1.1
   46 3.991706  128.119.245.12   128.238.245.34   HTTP     HTTP/1.1 200 OK (text/html)
   65 4.115257  128.238.245.34   165.193.123.218  HTTP     GET /catalog/images/pearson-logo-footer.gif HTTP/1.1
   68 4.137122  165.193.123.218  128.238.245.34   HTTP     HTTP/1.1 200 OK (GIF89a)[Unreassembled Packet]
   69 4.140800  165.193.123.218  128.238.245.34   HTTP     Continuation
   71 4.143595  165.193.123.218  128.238.245.34   HTTP     Continuation
   74 4.307374  128.238.245.34   134.241.6.82     HTTP     GET /~kurose/cover.jpg HTTP/1.1
   77 4.680388  134.241.6.82     128.238.245.34   HTTP     HTTP/1.0 200 Document follows
   78 4.681472  134.241.6.82     128.238.245.34   HTTP     Continuation
   80 4.682832  134.241.6.82     128.238.245.34   HTTP     Continuation
   81 4.683923  134.241.6.82     128.238.245.34   HTTP     Continuation
   83 4.684992  134.241.6.82     128.238.245.34   HTTP     Continuation
   84 4.686427  134.241.6.82     128.238.245.34   HTTP     Continuation
   86 4.687739  134.241.6.82     128.238.245.34   HTTP     Continuation
   87 4.690200  134.241.6.82     128.238.245.34   HTTP     Continuation
   89 4.891352  134.241.6.82     128.238.245.34   HTTP     Continuation
   90 4.894202  134.241.6.82     128.238.245.34   HTTP     Continuation
   92 4.898095  134.241.6.82     128.238.245.34   HTTP     Continuation
   93 4.901302  134.241.6.82     128.238.245.34   HTTP     Continuation
   95 4.904856  134.241.6.82     128.238.245.34   HTTP     Continuation
   96 4.908695  134.241.6.82     128.238.245.34   HTTP     Continuation
  107 5.139328  134.241.6.82     128.238.245.34   HTTP     Continuation
  108 5.141891  134.241.6.82     128.238.245.34   HTTP     Continuation
  110 5.144611  134.241.6.82     128.238.245.34   HTTP     Continuation
  111 5.146154  134.241.6.82     128.238.245.34   HTTP     Continuation
  113 5.148742  134.241.6.82     128.238.245.34   HTTP     Continuation
  179 8.365103  165.193.123.218  128.238.245.34   HTTP     Continuation
```

```
    Type: IP (0x0800)
▿ Internet Protocol, Src Addr: 128.238.245.34 (128.238.245.34), Dst Addr: 128.119.245.12 (128.119.245.12)
    Version: 4
    Header length: 20 bytes
  ▹ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 386
    Identification: 0xb97e (47486)
  ▹ Flags: 0x04 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (0x06)
    Header checksum: 0x5462 (correct)
    Source: 128.238.245.34 (128.238.245.34)
```

```
0000  00 b0 c2 f3 15 80 00 11  f5 05 4d b9 08 00 45 00   ........ ..M...E.
0010  01 82 b9 7e 40 00 80 06  54 62 80 ee f5 22 80 77   ...~@... Tb...".w
0020  f5 0c 06 fc 00 50 d8 00  3c 41 63 bd 15 c3 50 18   .....P.. <Ac...P.
0030  40 b0 52 55 00 00 47 45  54 20 2f 65 74 68 65 72   @.RU..GE T /ether
```

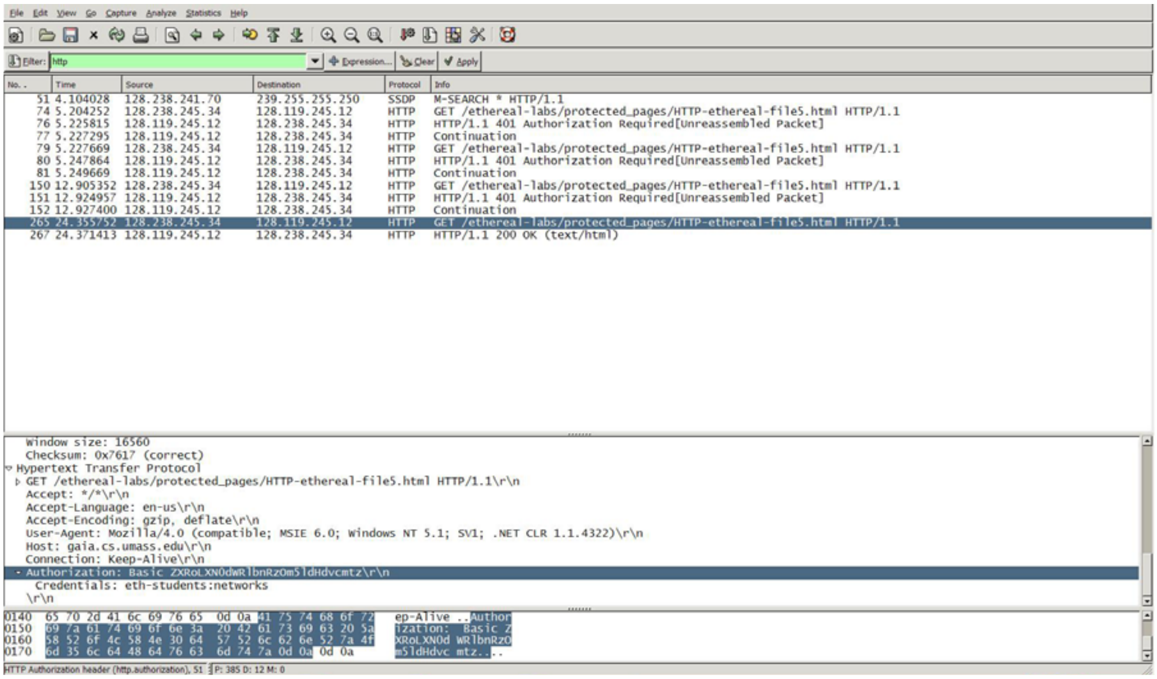
File: (Untitled) 40 KB 00:00:12 Drops: 0 P: 215 D: 27 M: 0

Answer the following questions:

16. How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent?
Answer: As you can see from the above screenshot there were 3 HTTP GET requests sent to the following Internet addresses:
a. 128.119.245.12
b. 165.193.123.218
c. 134.241.6.82

17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.
Answer: By checking the TCP ports we can see if our files were downloaded serially or in parallel. In this case the 2 images were transmitted over 2 TCP connections therefore they were downloaded serially.

5. HTTP Authentication



File Edit View Go Capture Analyze Statistics Help
Filter: http
Expression... Clear Apply

```
No. . Time      Source          Destination     Protocol Info
   51 4.104028  128.238.241.70  239.255.255.250 SSDP     M-SEARCH * HTTP/1.1
   74 5.204252  128.238.245.34  128.119.245.12  HTTP     GET /ethereal-labs/protected_pages/HTTP-ethereal-file5.html HTTP/1.1
   76 5.225815  128.119.245.12  128.238.245.34  HTTP     HTTP/1.1 401 Authorization Required[Unreassembled Packet]
   77 5.227295  128.119.245.12  128.238.245.34  HTTP     Continuation
   79 5.227669  128.238.245.34  128.119.245.12  HTTP     GET /ethereal-labs/protected_pages/HTTP-ethereal-file5.html HTTP/1.1
   80 5.247864  128.119.245.12  128.238.245.34  HTTP     HTTP/1.1 401 Authorization Required[Unreassembled Packet]
   81 5.249669  128.119.245.12  128.238.245.34  HTTP     Continuation
  150 12.905352 128.238.245.34  128.119.245.12  HTTP     GET /ethereal-labs/protected_pages/HTTP-ethereal-file5.html HTTP/1.1
  151 12.924957 128.119.245.12  128.238.245.34  HTTP     HTTP/1.1 401 Authorization Required[Unreassembled Packet]
  152 12.927400 128.119.245.12  128.238.245.34  HTTP     Continuation
  265 24.355752 128.238.245.34  128.119.245.12  HTTP     GET /ethereal-labs/protected_pages/HTTP-ethereal-file5.html HTTP/1.1
  267 24.371413 128.119.245.12  128.238.245.34  HTTP     HTTP/1.1 200 OK (text/html)
```

```
  Window size: 16560
  Checksum: 0x7617 (correct)
▿ Hypertext Transfer Protocol
 ▹ GET /ethereal-labs/protected_pages/HTTP-ethereal-file5.html HTTP/1.1\r\n
  Accept: */*\r\n
  Accept-Language: en-us\r\n
  Accept-Encoding: gzip, deflate\r\n
  User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)\r\n
  Host: gaia.cs.umass.edu\r\n
  Connection: Keep-Alive\r\n
 - Authorization: Basic ZXRoLXN0dWRlbnRzOm5ldHdvcmtz\r\n
    Credentials: eth-students:networks
  \r\n
```

```
0140  65 70 2d 41 6c 69 76 65  0d 0a 41 75 74 68 6f 72   ep-Alive ..Author
0150  69 7a 61 74 69 6f 6e 3a  20 42 61 73 69 63 20 5a   ization:  Basic Z
0160  58 52 6f 4c 58 4e 30 64  57 52 6c 62 6e 52 7a 4f   XRoLXN0d WRlbnRzO
0170  6d 35 6c 64 48 64 76 63  6d 74 7a 0d 0a 0d 0a      m5ldHdvc mtz....
```

HTTP Authorization header (http.authorization), 51 P: 385 D: 12 M: 0

Answer the following questions:

18. What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser?
Answer: Status code: 401 , Phrase: Authorization Required

19. When your browser’s sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?
Answer: As seen in the screenshot the new field (highlighted) is Authorization.
`Authorization: Basic ZXRoLXN0dWRlbnRzOm5ldHdvcmtz\r\n`