Wireshark Lab: HTTP

1. The Basic HTTP GET/response interaction

```
No.     Time           Source            Destination       Protocol Info
4      0.048291       192.168.1.46      128.119.245.12    HTTP     GET /wireshark-
labs/HTTP-wireshark-file1.html HTTP/1.1

Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.4)
Gecko/20070515 Firefox/2.0.0.4\r\n
    Accept:
text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8
,image/png,*/*;q=0.5\r\n
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    Cookie: MintUnique=1;
__utmz=198765611.1176212581.8.2.utmccn=(referral)|utmcsr=cs.umass.edu|utmcct=/c
sinfo/news.html|utmcmd=referral;
__utma=198765611.821901841.1145892528.1176212581.1179945703.9;
__utma=267820956.1666738513.1163587262.118
    If-Modified-Since: Thu, 07 Jun 2007 22:07:01 GMT\r\n
    If-None-Match: "d6c95-7e-224fab40"\r\n
    \r\n
```

```
No.    Time         Source          Destination    Protocol Info
6      0.155044     128.119.245.12 192.168.1.46   HTTP     HTTP/1.1 200 OK
(text/html)

Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Thu, 07 Jun 2007 22:09:08 GMT\r\n
    Server: Apache/2.0.52 (CentOS)\r\n
    Last-Modified: Thu, 07 Jun 2007 22:09:01 GMT\r\n
    ETag: "d6c95-7e-2976b940"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 126
    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>\n
    Congratulations.  You've downloaded the file \n
    http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-file1.html!\n
    </html>\n
```

Answer the following questions:

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

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?
Answer: My IP address is `192.168.1.46` 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: Thu, 07 Jun 2007 22:09:01 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
      4 0.046887    192.168.1.46          128.119.245.12        HTTP     GET
/wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1

Hypertext Transfer Protocol
    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 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.4)
Gecko/20070515 Firefox/2.0.0.4\r\n
    Accept:
text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8
,image/png,*/*;q=0.5\r\n
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    Cookie:
__utmz=198765611.1176212581.8.2.utmccn=(referral)|utmcsr=cs.umass.edu|utmcct=/c
sinfo/news.html|utmcmd=referral;
__utma=198765611.821901841.1145892528.1176212581.1179945703.9;
__utmz=267820956.1180131637.4.1.utmccn=(organic)|utmcsr=
    \r\n
```

```
No.     Time        Source                Destination           Protocol Info
      7 0.151515    128.119.245.12        192.168.1.46          HTTP
HTTP/1.1 200 OK (text/html)

Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        Request Version: HTTP/1.1
        Response Code: 200
    Date: Thu, 07 Jun 2007 16:29:06 GMT\r\n
    Server: Apache/2.0.52 (CentOS)\r\n
    Last-Modified: Thu, 07 Jun 2007 16:29:01 GMT\r\n
    ETag: "d6c96-173-69876d40"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 371
    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
    \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
```

```
No.     Time        Source                Destination           Protocol Info
     12 2.932093    192.168.1.46          128.119.245.12        HTTP     GET
/wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1

Hypertext Transfer Protocol
    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 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.4)
Gecko/20070515 Firefox/2.0.0.4\r\n
    Accept:
text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8
,image/png,*/*;q=0.5\r\n
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    Cookie:
__utmz=198765611.1176212581.8.2.utmccn=(referral)|utmcsr=cs.umass.edu|utmcct=/c
sinfo/news.html|utmcmd=referral;
__utma=198765611.821901841.1145892528.1176212581.1179945703.9;
__utmz=267820956.1180131637.4.1.utmccn=(organic)|utmcsr=
    If-Modified-Since: Thu, 07 Jun 2007 16:29:01 GMT\r\n
    If-None-Match: "d6c96-173-69876d40"\r\n
    Cache-Control: max-age=0\r\n
    \r\n
```

```
No.     Time        Source                Destination           Protocol Info
     13 3.030398    128.119.245.12        192.168.1.46          HTTP
HTTP/1.1 304 Not Modified

Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
        Request Version: HTTP/1.1
        Response Code: 304
    Date: Thu, 07 Jun 2007 16:29:09 GMT\r\n
    Server: Apache/2.0.52 (CentOS)\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=10, max=98\r\n
    ETag: "d6c96-173-69876d40"\r\n
    \r\n
```

Answer the following questions:

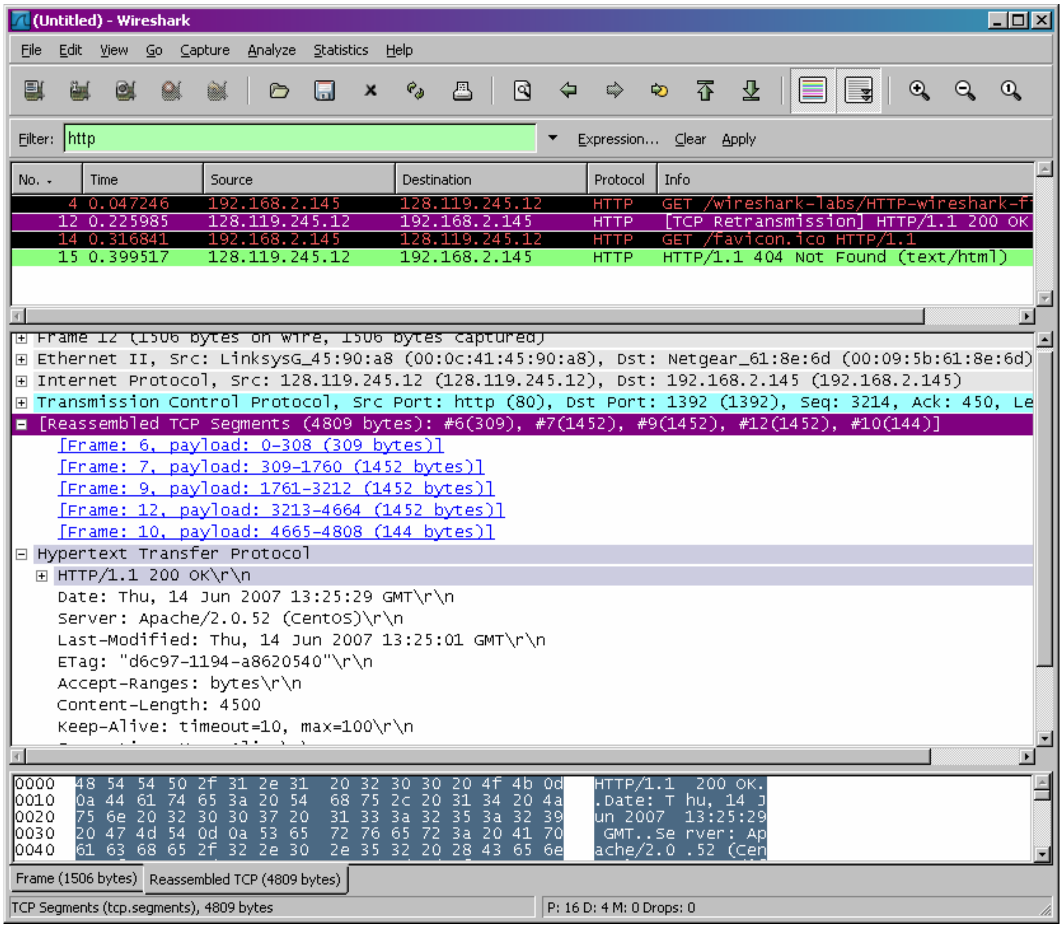
8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?
Answer: No

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 following is: `Thu, 07 Jun 2007 16:29:01 GMT` which is the date of the last modification of the file from the previous get request.

11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.
Answer: The status code and phrase returned from the server is `HTTP/1.1 304 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) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: http
Expression... Clear Apply

```
No. -  Time      Source          Destination     Protocol Info
     4 0.047246  192.168.2.145   128.119.245.12  HTTP     GET /wireshark-labs/HTTP-wireshark-f
    12 0.225985  128.119.245.12  192.168.2.145   HTTP     [TCP Retransmission] HTTP/1.1 200 OK
    14 0.316841  192.168.2.145   128.119.245.12  HTTP     GET /favicon.ico HTTP/1.1
    15 0.399517  128.119.245.12  192.168.2.145   HTTP     HTTP/1.1 404 Not Found (text/html)
```

```
⊞ Frame 12 (1506 bytes on wire, 1506 bytes captured)
⊞ Ethernet II, Src: LinksysG_45:90:a8 (00:0c:41:45:90:a8), Dst: Netgear_61:8e:6d (00:09:5b:61:8e:6d)
⊞ Internet Protocol, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.2.145 (192.168.2.145)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 1392 (1392), Seq: 3214, Ack: 450, Le
⊟ [Reassembled TCP Segments (4809 bytes): #6(309), #7(1452), #9(1452), #12(1452), #10(144)]
    [Frame: 6, payload: 0-308 (309 bytes)]
    [Frame: 7, payload: 309-1760 (1452 bytes)]
    [Frame: 9, payload: 1761-3212 (1452 bytes)]
    [Frame: 12, payload: 3213-4664 (1452 bytes)]
    [Frame: 10, payload: 4665-4808 (144 bytes)]
⊟ Hypertext Transfer Protocol
  ⊞ HTTP/1.1 200 OK\r\n
    Date: Thu, 14 Jun 2007 13:25:29 GMT\r\n
    Server: Apache/2.0.52 (CentOS)\r\n
    Last-Modified: Thu, 14 Jun 2007 13:25:01 GMT\r\n
    ETag: "d6c97-1194-a8620540"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 4500
    Keep-Alive: timeout=10, max=100\r\n
```

```
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 54  68 75 2c 20 31 34 20 4a   .Date: T hu, 14 J
0020  75 6e 20 32 30 30 37 20  31 33 3a 32 35 3a 32 39   un 2007  13:25:29
0030  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT..Se rver: Ap
0040  61 63 68 65 2f 32 2e 30  2e 35 32 20 28 43 65 6e   ache/2.0 .52 (Cen
```

```
TCP Segments (tcp.segments), 4809 bytes    P: 16 D: 4 M: 0 Drops: 0
```

Answer the following questions:

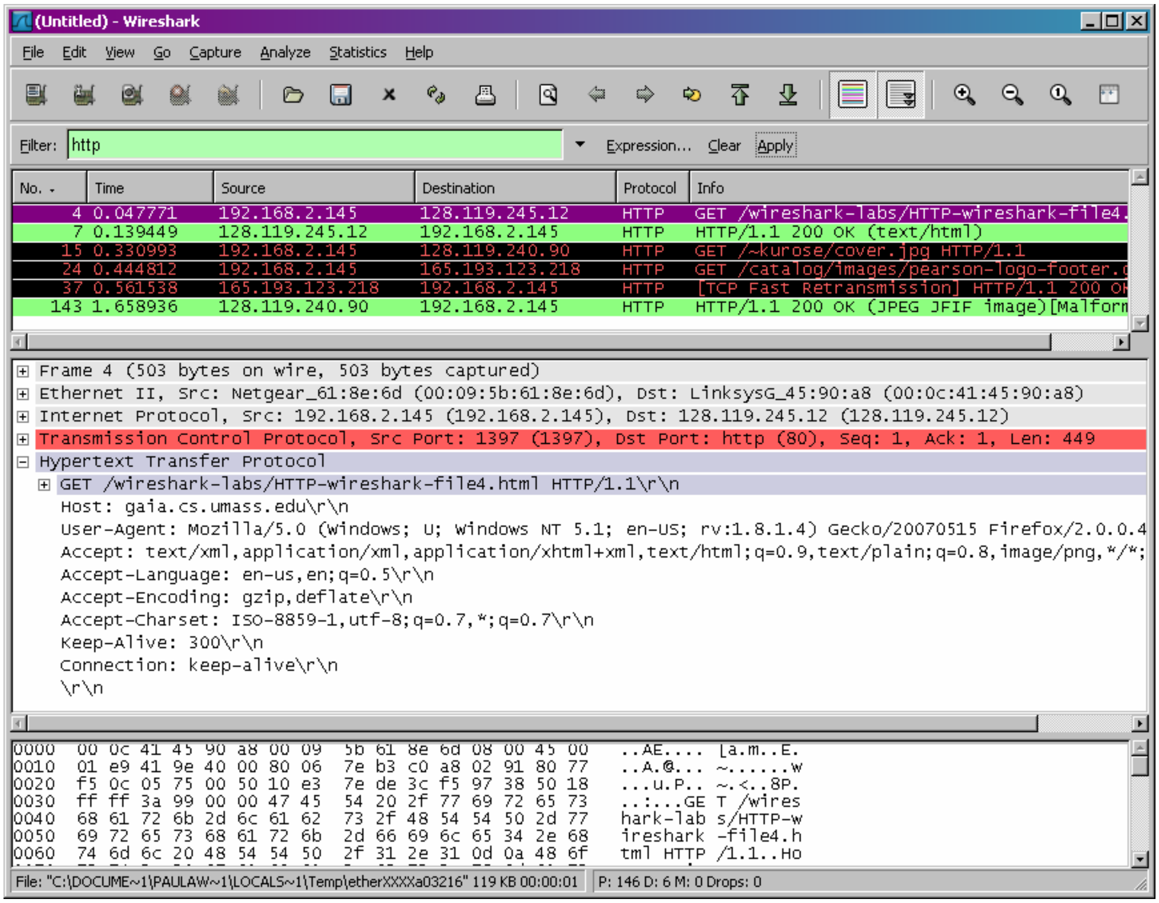
12. How many HTTP GET request messages were sent by your browser?
Answer: There was 1 HTTP GET request message sent by my browser as seen in the screenshot.

13. How many data-containing TCP segments were needed to carry the single HTTP response?
Answer: There were 5 data containing TCP segments containing 309 ,1452 ,1452, 1452 and 144 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) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Expression... Clear Apply

Filter: http

```
No. -  Time      Source           Destination      Protocol  Info
    4 0.047771   192.168.2.145    128.119.245.12   HTTP      GET /wireshark-labs/HTTP-wireshark-file4.
    7 0.139449   128.119.245.12   192.168.2.145    HTTP      HTTP/1.1 200 OK (text/html)
   15 0.330993   192.168.2.145    128.119.240.90   HTTP      GET /~kurose/cover.jpg HTTP/1.1
   24 0.444812   192.168.2.145    165.193.123.218  HTTP      GET /catalog/images/pearson-logo-footer.
   37 0.561538   165.193.123.218  192.168.2.145    HTTP      [TCP Fast Retransmission] HTTP/1.1 200 OK
  143 1.658936   128.119.240.90   192.168.2.145    HTTP      HTTP/1.1 200 OK (JPEG JFIF image)[Malforn
```

```
⊞ Frame 4 (503 bytes on wire, 503 bytes captured)
⊞ Ethernet II, Src: Netgear_61:8e:6d (00:09:5b:61:8e:6d), Dst: LinksysG_45:90:a8 (00:0c:41:45:90:a8)
⊞ Internet Protocol, Src: 192.168.2.145 (192.168.2.145), Dst: 128.119.245.12 (128.119.245.12)
⊞ Transmission Control Protocol, Src Port: 1397 (1397), Dst Port: http (80), Seq: 1, Ack: 1, Len: 449
⊟ Hypertext Transfer Protocol
  ⊞ GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.4) Gecko/20070515 Firefox/2.0.0.4
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    \r\n
```

```
0000  00 0c 41 45 90 a8 00 09  5b 61 8e 6d 08 00 45 00   ..AE.... [a.m..E.
0010  01 e9 41 9e 40 00 80 06  7e b3 c0 a8 02 91 80 77   ..A.@... ~......w
0020  f5 0c 05 75 00 50 10 e3  7e de 3c f5 97 38 50 18   ...u.P.. ~.<..8P.
0030  ff ff 3a 99 00 00 47 45  54 20 2f 77 69 72 65 73   ..:...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 34 2e 68   ireshark -file4.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1..Ho
```

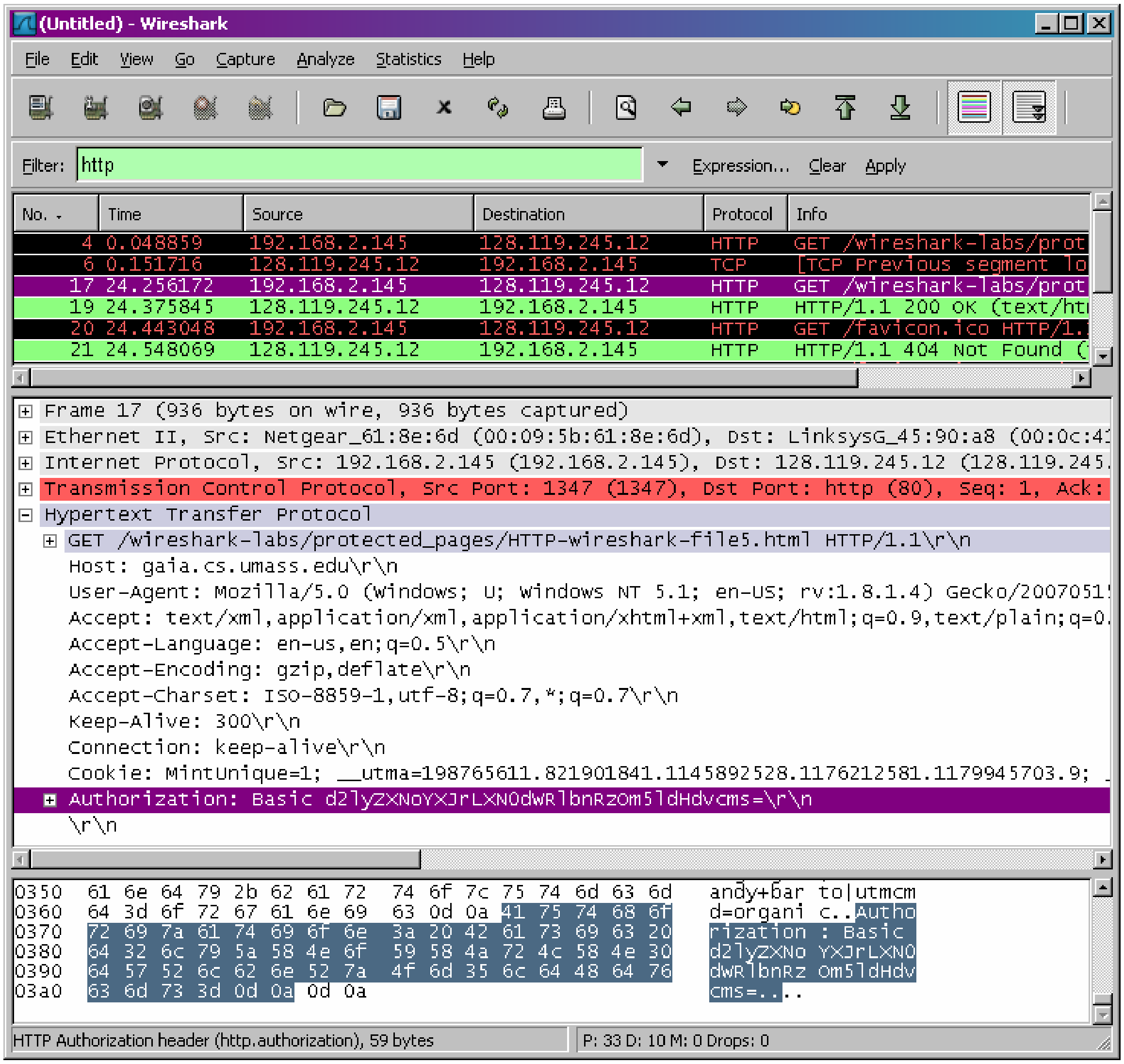
File: "C:\DOCUME~1\PAULAW~1\LOCALS~1\Temp\etherXXXXa03216" 119 KB 00:00:01 | P: 146 D: 6 M: 0 Drops: 0

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. 128.119.240.90
c. 165.193.123.218

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


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

```
No. .  Time         Source           Destination      Protocol  Info
    4  0.048859     192.168.2.145    128.119.245.12   HTTP      GET /wireshark-labs/prot
    6  0.151716     128.119.245.12   192.168.2.145    TCP       [TCP Previous segment lo
   17  24.256172    192.168.2.145    128.119.245.12   HTTP      GET /wireshark-labs/prot
   19  24.375845    128.119.245.12   192.168.2.145    HTTP      HTTP/1.1 200 OK (text/ht
   20  24.443048    192.168.2.145    128.119.245.12   HTTP      GET /favicon.ico HTTP/1.
   21  24.548069    128.119.245.12   192.168.2.145    HTTP      HTTP/1.1 404 Not Found (
```

```
⊞ Frame 17 (936 bytes on wire, 936 bytes captured)
⊞ Ethernet II, Src: Netgear_61:8e:6d (00:09:5b:61:8e:6d), Dst: LinksysG_45:90:a8 (00:0c:41
⊞ Internet Protocol, Src: 192.168.2.145 (192.168.2.145), Dst: 128.119.245.12 (128.119.245.
⊞ Transmission Control Protocol, Src Port: 1347 (1347), Dst Port: http (80), Seq: 1, Ack:
⊟ Hypertext Transfer Protocol
  ⊞ GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.4) Gecko/2007051
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    Cookie: MintUnique=1; __utma=198765611.821901841.1145892528.1176212581.1179945703.9; _
  ⊞ Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    \r\n
```

```
0350  61 6e 64 79 2b 62 61 72  74 6f 7c 75 74 6d 63 6d   andy+bar to|utmcm
0360  64 3d 6f 72 67 61 6e 69  63 0d 0a 41 75 74 68 6f   d=organi c..Autho
0370  72 69 7a 61 74 69 6f 6e  3a 20 42 61 73 69 63 20   rization : Basic
0380  64 32 6c 79 5a 58 4e 6f  59 58 4a 72 4c 58 4e 30   d2lyZXNo YXJrLXN0
0390  64 57 52 6c 62 6e 52 7a  4f 6d 35 6c 64 48 64 76   dWRlbnRz Om5ldHdv
03a0  63 6d 73 3d 0d 0a 0d 0a                            cms=....
```

HTTP Authorization header (http.authorization), 59 bytes | P: 33 D: 10 M: 0 Drops: 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 d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n`