

## LAB 2

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

Answer: My browser is running HTTP version 1.1 and the server is running HTTP 1.1.

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

Answer: en-us

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

Answer: My IP = 192.168.1.11; Server IP = 128.119.245.12

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

Answer: 200 OK

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

Answer: Wed, 19 Oct 2016 05:59:01 GMT

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

Answer: 128 bytes

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 I do not

Screenshots for section 1:

No.	Time	Source	Destination	Protocol	Length	Info
26	19:14:16.693859	192.168.1.11	128.119.245.12	HTTP	546	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
35	19:14:16.762892	128.119.245.12	192.168.1.11	HTTP	554	HTTP/1.1 200 OK (text/html)

3

1

```
▶ Frame 26: 546 bytes on wire (4368 bits), 546 bytes captured (4368 bits) on interface 0
▶ Ethernet II, Src: Apple_b9:c1:e7 (a4:5e:60:b9:c1:e7), Dst: Netgear_29:90:66 (c4:04:15:29:90:66)
▶ Internet Protocol Version 4, Src: 192.168.1.11, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 49500, Dst Port: 80, Seq: 1, Ack: 1, Len: 480
▼ Hypertext Transfer Protocol
  ▶ GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n 1
    Host: gaia.cs.umass.edu\r\n
    If-None-Match: "80-53f1d63a6f671"\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    If-Modified-Since: Tue, 18 Oct 2016 05:59:02 GMT\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12) AppleWebKit/602.1.50 (KHTML, like Gecko) Version/10.0 Safari/602.1.50\r\n
    Accept-Language: en-us\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 35]
```

2

35	19:14:16.762892	128.119.245.12	192.168.1.11	HTTP	554	HTTP/1.1 200 OK (text/html)
----	-----------------	----------------	--------------	------	-----	-----------------------------

  

```

> Frame 35: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface 0
> Ethernet II, Src: Netgear_29:90:66 (c4:04:15:29:90:66), Dst: Apple_b9:c1:e7 (a4:5e:60:b9:c1:e7)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.11
> Transmission Control Protocol, Src Port: 80, Dst Port: 49508, Seq: 1, Ack: 481, Len: 488
< Hypertext Transfer Protocol
  < HTTP/1.1 200 OK\r\n
    1 Date: Thu, 20 Oct 2016 01:4:17 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: Wed, 19 Oct 2016 05:59:01 GMT\r\n
      ETag: "00-53f318174cfee"\r\n
      Accept-Ranges: bytes\r\n
      Content-Length: 128\r\n
        [Content length: 128]
      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: 0.069033000 seconds]
      [Request in frame: 26]
      File Data: 128 bytes
  < Line-based text data: text/html
  
```

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 I do not.

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

Answer: Yes, you can see the contents of the file below the packet. It is titled as Line-based text data.

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, I do see that line. It contains: Wed, 19 Oct 2016 05:59:01 GMT\r\n

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 code returned is 304 Not Modified. Since the file had not changed since last accessed, no data was sent from the server with this request.

Section 2 Screenshots:

1<sup>st</sup> Get Request

No.	Time	Source	Destination	Protocol	Length	Info
22	19:59:12.188188	192.168.1.11	128.119.245.12	HTTP	519	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
26	19:59:12.255968	128.119.245.12	192.168.1.11	HTTP	798	HTTP/1.1 200 OK (text/html)
38	19:59:21.469743	192.168.1.11	128.119.245.12	HTTP	685	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
43	19:59:21.532941	128.119.245.12	192.168.1.11	HTTP	388	HTTP/1.1 304 Not Modified

```

▶ Frame 22: 519 bytes on wire (4152 bits), 519 bytes captured (4152 bits) on interface 0
▶ Ethernet II, Src: Apple_b9:c1:e7 (a4:3e:68:b9:c1:e7), Dst: Netgear_29:90:66 (c4:04:15:29:90:66)
▶ Internet Protocol Version 4, Src: 192.168.1.11, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 52550, Dst Port: 80, Seq: 1, Ack: 1, Len: 453
▼ 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
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_0) 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
    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 26]

```

1<sup>st</sup> Response

No.	Time	Source	Destination	Protocol	Length	Info
22	19:59:12.188188	192.168.1.11	128.119.245.12	HTTP	519	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
26	19:59:12.255968	128.119.245.12	192.168.1.11	HTTP	798	HTTP/1.1 200 OK (text/html)
38	19:59:21.469743	192.168.1.11	128.119.245.12	HTTP	685	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
43	19:59:21.532941	128.119.245.12	192.168.1.11	HTTP	388	HTTP/1.1 304 Not Modified

```

▶ Frame 26: 798 bytes on wire (6384 bits), 798 bytes captured (6384 bits) on interface 0
▶ Ethernet II, Src: Netgear_29:90:66 (c4:04:15:29:90:66), Dst: Apple_b9:c1:e7 (a4:3e:68:b9:c1:e7)
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.11
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 52550, Seq: 1, Ack: 454, Len: 732
▼ Hypertext Transfer Protocol
  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: Thu, 20 Oct 2016 01:59:13 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: Wed, 19 Oct 2016 05:59:01 GMT\r\n
    ETag: "173-53f318174c81e"\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: 0.067780000 seconds]
    [Request in frame 22]
    File Data: 371 bytes
▶ Line-based text data: text/html

```

2<sup>nd</sup> Get request

No.	Time	Source	Destination	Protocol	Length	Info
22	19:59:12.188188	192.168.1.11	128.119.245.12	HTTP	519	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
26	19:59:12.255968	128.119.245.12	192.168.1.11	HTTP	798	HTTP/1.1 200 OK (text/html)
38	19:59:21.469743	192.168.1.11	128.119.245.12	HTTP	685	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
43	19:59:21.532941	128.119.245.12	192.168.1.11	HTTP	388	HTTP/1.1 304 Not Modified

```

Frame 38: 685 bytes on wire (4840 bits), 685 bytes captured (4840 bits) on interface 0
Ethernet II, Src: Apple_b9:c1:e7 (a4:5e:60:b9:c1:e7), Dst: Netgear_29:98:66 (c4:04:15:29:98:66)
Internet Protocol Version 4, Src: 192.168.1.11, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 52551, Dst Port: 80, Seq: 1, Ack: 1, Len: 539
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
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_0) 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
    Accept-Encoding: gzip, deflate, sdch\r\n
    Accept-Language: en-US,en;q=0.8\r\n
    If-None-Match: "173-53f318174c81e"\r\n
    If-Modified-Since: Wed, 19 Oct 2016 05:59:01 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: 43]

```

2<sup>nd</sup> Response

No.	Time	Source	Destination	Protocol	Length	Info
22	19:59:12.188188	192.168.1.11	128.119.245.12	HTTP	519	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
26	19:59:12.255968	128.119.245.12	192.168.1.11	HTTP	798	HTTP/1.1 200 OK (text/html)
38	19:59:21.469743	192.168.1.11	128.119.245.12	HTTP	685	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
43	19:59:21.532941	128.119.245.12	192.168.1.11	HTTP	388	HTTP/1.1 304 Not Modified

11

```

Frame 43: 388 bytes on wire (2464 bits), 388 bytes captured (2464 bits) on interface 0
Ethernet II, Src: Netgear_29:98:66 (c4:04:15:29:98:66), Dst: Apple_b9:c1:e7 (a4:5e:60:b9:c1:e7)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.11
Transmission Control Protocol, Src Port: 80, Dst Port: 52551, Seq: 1, Ack: 540, Len: 242
Hypertext Transfer Protocol
  HTTP/1.1 304 Not Modified\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
    Request Version: HTTP/1.1
    Status Code: 304
    Response Phrase: Not Modified
    Date: Thu, 20 Oct 2016 01:59:22 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: "173-53f318174c81e"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.063198000 seconds]
    [Request in frame: 38]

```

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

Answer: There was one GET request sent. It was contained in packet 215.

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

Answer: Packet 219

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

Answer: 200 OK

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

Answer: 4 packets

## GET Request

No.	Time	Source	Destination	Protocol	Length	Info
215	20:19:12.280077	192.168.1.11	128.119.245.12	HTTP	493	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
222	20:19:12.358136	128.119.245.12	192.168.1.11	HTTP	585	HTTP/1.1 200 OK (text/html)

12

```

▶ Frame 215: 493 bytes on wire (3944 bits), 493 bytes captured (3944 bits) on interface 0
▶ Ethernet II, Src: Apple_b9:c1:e7 (a4:5e:60:b9:c1:e7), Dst: Netgear_29:90:66 (c4:04:15:29:90:66)
▶ Internet Protocol Version 4, Src: 192.168.1.11, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 52705, Dst Port: 80, Seq: 1, Ack: 1, Len: 427
▼ Hypertext Transfer Protocol
  ▶ GET /wireshark-labs/HTTP-wireshark-file3.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 (Macintosh; Intel Mac OS X 10_12_0) 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
    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: 222]

```

## Response

No.	Time	Source	Destination	Protocol	Length	Info
215	20:19:12.280077	192.168.1.11	128.119.245.12	HTTP	493	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
222	20:19:12.358136	128.119.245.12	192.168.1.11	HTTP	585	HTTP/1.1 200 OK (text/html)

```

▶ Frame 222: 585 bytes on wire (4680 bits), 585 bytes captured (4680 bits) on interface 0
▶ Ethernet II, Src: Netgear_29:90:66 (c4:04:15:29:90:66), Dst: Apple_b9:c1:e7 (a4:5e:60:b9:c1:e7)
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.11
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 52705, Seq: 4345, Ack: 428, Len: 519
▶ [4 Reassembled TCP Segments (4863 bytes): #219(1448), #220(1448), #221(1448), #222(519)]
  [Frame: 219, payload: 0-1447 (1448 bytes)]
  [Frame: 220, payload: 1448-2895 (1448 bytes)]
  [Frame: 221, payload: 2896-4343 (1448 bytes)]
  [Frame: 222, payload: 4344-4862 (519 bytes)]
  [Segment count: 4]
  [Reassembled TCP length: 4863]
  [Reassembled TCP Data: 405454582f312e3128323036204f4e0d8a46174653a2054...]
▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 200 OK\r\n
    Date: Thu, 20 Oct 2016 02:19:13 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: Wed, 19 Oct 2016 05:59:01 GMT\r\n
    ETag: "1194-52f318174609d"\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: 0.078059000 seconds]
    [Request in frame: 215]
    File Data: 4500 bytes
  ▶ Line-based text data: text/html

```

13, 15

14

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

Answer: My browser sent a total of 4 GET requests. They are as follows:

GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1

Destination: 128.119.245.12

GET /pearson.png HTTP/1.1

Destination: 128.119.245.12

GET /~kurose/cover\_5th\_ed.jpg HTTP/1.1

Destination: 128.119.240.90

GET /~kurose/cover\_5th\_ed.jpg HTTP/1.1

Destination: 128.119.240.90

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

Answer: They were sent serially; you can tell this since the GET requests occur one after another. This is also confirmed since the images were sent over TCP and came from the same port.

#### Section 4 Screenshots

No.	Time	Source	Destination	Protocol	Length	Info
94	20:32:51.752972	192.168.1.11	128.119.245.12	HTTP	519	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
98	20:32:51.827649	128.119.245.12	192.168.1.11	HTTP	1141	HTTP/1.1 200 OK (text/html)
100	20:32:51.832921	192.168.1.11	128.119.245.12	HTTP	464	GET /pearson.png HTTP/1.1
104	20:32:51.896928	128.119.245.12	192.168.1.11	HTTP	783	HTTP/1.1 200 OK [PNG]
112	20:32:51.985327	192.168.1.11	128.119.240.90	HTTP	478	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
114	20:32:52.033626	128.119.240.90	192.168.1.11	HTTP	522	HTTP/1.1 302 Found (text/html)
126	20:32:52.163772	192.168.1.11	128.119.240.90	HTTP	478	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
247	20:32:52.429879	128.119.240.90	192.168.1.11	HTTP	1366	HTTP/1.1 200 OK (JPEG image)

16

<div><div>▶ Frame 104: 783 bytes on wire (6264 bits), 783 bytes captured (6264 bits) on interface 0</div><div>▶ Ethernet II, Src: Netgear_28:98:06 (c4:b4:15:28:98:06), Dst: Apple_B9:c1:e7 (a4:5e:08:b9:c1:e7)</div><div>▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.11</div><div>▶ Transmission Control Protocol, Src Port: 80, Dst Port: 52814, Seq: 3972, Ack: 852, Len: 717</div><div>▼ [3 Reassembled TCP Segments (3613 bytes): #102(1448), #103(1448), #104(717)]</div><div><div>[Frame 102, payload: 0-1447 (1448 bytes)]</div><div>[Frame 103, payload: 1448-2895 (1448 bytes)]</div><div>[Frame 104, payload: 2896-3612 (717 bytes)]</div><div>[Segment count: 3]</div><div>[Reassembled TCP length: 3613]</div><div>[Reassembled TCP Data: 485454582f312e3128323838204f4b80a446174653a2854...]</div></div></div> <div>▼ Hypertext Transfer Protocol</div> <div><div>▶ HTTP/1.1 200 OK\r\n</div><div>  Date: Thu, 20 Oct 2016 02:32:51 GMT\r\n</div><div>  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</div><div>  Last-Modified: Sat, 06 Aug 2016 10:00:14 GMT\r\n</div><div>  ETag: "cc3-599645c7f1ee7"\r\n</div><div>  Accept-Ranges: bytes\r\n</div><div>  Content-Length: 3267\r\n</div><div>  Keep-Alive: timeout=5, max=99\r\n</div><div>  Connection: Keep-Alive\r\n</div><div>  Content-Type: image/png\r\n</div><div>  \r\n</div><div>  [HTTP response 2/2]</div><div>  [Time since request: 0.063999800 seconds]</div><div>  [Prev request in frame: 94]</div><div>  [Prev response in frame: 98]</div><div>  [Request in frame: 100]</div><div>  File Data: 3267 bytes</div><div>▶ Portable Network Graphics</div></div>	17
--	----



No.	Time	Source	Destination	Protocol	Length	Info
94	20:32:51.752072	192.168.1.11	128.119.245.12	HTTP	519	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
98	20:32:51.827649	128.119.245.12	192.168.1.11	HTTP	1141	HTTP/1.1 200 OK (text/html)
100	20:32:51.832921	192.168.1.11	128.119.245.12	HTTP	464	GET /pearson.png HTTP/1.1
104	20:32:51.896928	128.119.245.12	192.168.1.11	HTTP	783	HTTP/1.1 200 OK (PNG)
112	20:32:51.965327	192.168.1.11	128.119.248.90	HTTP	478	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
114	20:32:52.033266	128.119.248.90	192.168.1.11	HTTP	522	HTTP/1.1 302 Found (text/html)
126	20:32:52.163772	192.168.1.11	128.119.248.90	HTTP	478	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
247	20:32:52.429079	128.119.248.90	192.168.1.11	HTTP	1366	HTTP/1.1 200 OK (JPEG JFIF image)

```

Frame 247: 1366 bytes on wire (10928 bits), 1366 bytes captured (10928 bits) on interface 0
Ethernet II, Src: Netgear_29:90:66 (c4:04:15:29:90:66), Dst: Apple_b9:c1:e7 (a4:5e:60:b9:c1:e7)
Internet Protocol Version 4, Src: 128.119.240.90, Dst: 192.168.1.11
Transmission Control Protocol, Src Port: 80, Dst Port: 52017, Seq: 99913, Ack: 411, Len: 1300
78 Reassembled TCP Segments (101212 bytes): #128(1448), #129(1448), #130(1448), #131(1448), #134(1448), #135(1448), #136(1448), #137(1448), #141(1448), #142(1448), #143(1448), #144(1448), #145(1448), #146(1448), #147(1448), #148(1448), #149(1448), #150(1448), #151(1448), #152(1448), #153(1448), #154(1448), #155(1448), #156(1448), #157(1448), #158(1448), #159(1448), #160(1448), #161(1448), #162(1448), #163(1448), #164(1448), #165(1448), #166(1448), #167(1448), #168(1448), #169(1448), #170(1448), #171(1448), #172(1448), #173(1448), #174(1448), #175(1448), #176(1448), #177(1448), #178(1448), #179(1448), #180(1448), #181(1448), #182(1448), #183(1448), #184(1448), #185(1448), #186(1448), #187(1448), #188(1448), #189(1448), #190(1448), #191(1448), #192(1448), #193(1448), #194(1448), #195(1448), #196(1448), #197(1448), #198(1448), #199(1448), #200(1448), #201(1448), #202(1448), #203(1448), #204(1448), #205(1448), #206(1448), #207(1448), #208(1448), #209(1448), #210(1448), #211(1448), #212(1448), #213(1448), #214(1448), #215(1448), #216(1448), #217(1448), #218(1448), #219(1448), #220(1448), #221(1448), #222(1448), #223(1448), #224(1448), #225(1448), #226(1448), #227(1448), #228(1448), #229(1448), #230(1448), #231(1448), #232(1448), #233(1448), #234(1448), #235(1448), #236(1448), #237(1448), #238(1448), #239(1448), #240(1448), #241(1448), #242(1448), #243(1448), #244(1448), #245(1448), #246(1448), #247(1448), #248(1448), #249(1448), #250(1448), #251(1448), #252(1448), #253(1448), #254(1448), #255(1448), #256(1448), #257(1448), #258(1448), #259(1448), #260(1448), #261(1448), #262(1448), #263(1448), #264(1448), #265(1448), #266(1448), #267(1448), #268(1448), #269(1448), #270(1448), #271(1448), #272(1448), #273(1448), #274(1448), #275(1448), #276(1448), #277(1448), #278(1448), #279(1448), #280(1448), #281(1448), #282(1448), #283(1448), #284(1448), #285(1448), #286(1448), #287(1448), #288(1448), #289(1448), #290(1448), #291(1448), #292(1448), #293(1448), #294(1448), #295(1448), #296(1448), #297(1448), #298(1448), #299(1448), #300(1448), #301(1448), #302(1448), #303(1448), #304(1448), #305(1448), #306(1448), #307(1448), #308(1448), #309(1448), #310(1448), #311(1448), #312(1448), #313(1448), #314(1448), #315(1448), #316(1448), #317(1448), #318(1448), #319(1448), #320(1448), #321(1448), #322(1448), #323(1448), #324(1448), #325(1448), #326(1448), #327(1448), #328(1448), #329(1448), #330(1448), #331(1448), #332(1448), #333(1448), #334(1448), #335(1448), #336(1448), #337(1448), #338(1448), #339(1448), #340(1448), #341(1448), #342(1448), #343(1448), #344(1448), #345(1448), #346(1448), #347(1448), #348(1448), #349(1448), #350(1448), #351(1448), #352(1448), #353(1448), #354(1448), #355(1448), #356(1448), #357(1448), #358(1448), #359(1448), #360(1448), #361(1448), #362(1448), #363(1448), #364(1448), #365(1448), #366(1448), #367(1448), #368(1448), #369(1448), #370(1448), #371(1448), #372(1448), #373(1448), #374(1448), #375(1448), #376(1448), #377(1448), #378(1448), #379(1448), #380(1448), #381(1448), #382(1448), #383(1448), #384(1448), #385(1448), #386(1448), #387(1448), #388(1448), #389(1448), #390(1448), #391(1448), #392(1448), #393(1448), #394(1448), #395(1448), #396(1448), #397(1448), #398(1448), #399(1448), #400(1448), #401(1448), #402(1448), #403(1448), #404(1448), #405(1448), #406(1448), #407(1448), #408(1448), #409(1448), #410(1448), #411(1448), #412(1448), #413(1448), #414(1448), #415(1448), #416(1448), #417(1448), #418(1448), #419(1448), #420(1448), #421(1448), #422(1448), #423(1448), #424(1448), #425(1448), #426(1448), #427(1448), #428(1448), #429(1448), #430(1448), #431(1448), #432(1448), #433(1448), #434(1448), #435(1448), #436(1448), #437(1448), #438(1448), #439(1448), #440(1448), #441(1448), #442(1448), #443(1448), #444(1448), #445(1448), #446(1448), #447(1448), #448(1448), #449(1448), #450(1448), #451(1448), #452(1448), #453(1448), #454(1448), #455(1448), #456(1448), #457(1448), #458(1448), #459(1448), #460(1448), #461(1448), #462(1448), #463(1448), #464(1448), #465(1448), #466(1448), #467(1448), #468(1448), #469(1448), #470(1448), #471(1448), #472(1448), #473(1448), #474(1448), #475(1448), #476(1448), #477(1448), #478(1448), #479(1448), #480(1448), #481(1448), #482(1448), #483(1448), #484(1448), #485(1448), #486(1448), #487(1448), #488(1448), #489(1448), #490(1448), #491(1448), #492(1448), #493(1448), #494(1448), #495(1448), #496(1448), #497(1448), #498(1448), #499(1448), #500(1448), #501(1448), #502(1448), #503(1448), #504(1448), #505(1448), #506(1448), #507(1448), #508(1448), #509(1448), #510(1448), #511(1448), #512(1448), #513(1448), #514(1448), #515(1448), #516(1448), #517(1448), #518(1448), #519(1448), #520(1448), #521(
```

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

Answer: 401 Unauthorized

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

Answer: The authorization field was added and has the value Basic d2lyZXNoYXJrLXN0dWRIbnRzOm5ldHdvcm0=

## Section 5 Screenshots:

No.	Time	Source	Destination	Protocol	Length	Info
75	20:55:05.003378	192.168.1.11	128.119.245.12	HTTP	477	GET /wireshark-labs/protected_pages/HTTP-wireshark-files.html HTTP/1.1
77	20:55:05.678183	128.119.245.12	192.168.1.11	HTTP	785	HTTP/1.1 403 Unauthorized (text/html)
97	20:55:17.201816	192.168.1.11	128.119.245.12	HTTP	536	GET /wireshark-labs/protected_pages/HTTP-wireshark-files.html HTTP/1.1
99	20:55:17.346732	128.119.245.12	192.168.1.11	HTTP	558	HTTP/1.1 200 OK (text/html)

```

▶ Frame 77: 783 bytes on wire (6288 bits), 783 bytes captured (6288 bits) on interface 0
▶ Ethernet II, Src: Netgear_28:90:d6 (c4:04:15:29:90:d6), Dst: Apple_b9:cl:e7 (04:1e:00:b9:cl:e7)
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.11
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 52957, Seq: 1, Ack: 412, Len: 719
▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 401 Unauthorized\r\n 18
    Date: Thu, 20 Oct 2016 02:55:03 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
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.006895000 seconds]
    [Request in frame: 75]
    File Data: 381 bytes
  ▶ Line-based text data: text/html

```

No.	Time	Source	Destination	Protocol	Length	Info
75	20:55:03.003376	192.168.1.11	128.119.245.12	HTTP	477	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
77	20:55:03.070183	128.119.245.12	192.168.1.11	HTTP	785	HTTP/1.1 401 Unauthorized (text/html)
97	20:55:17.281616	192.168.1.11	128.119.245.12	HTTP	536	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
99	20:55:17.340732	128.119.245.12	192.168.1.11	HTTP	558	HTTP/1.1 200 OK (text/html)

```

Frame 97: 536 bytes on wire (4288 bits), 536 bytes captured (4288 bits) on interface 0
Ethernet II, Src: Apple_B9:c1:e7 (04:3e:60:b9:c1:e7), Dst: Netgear_29:90:66 (c4:84:15:29:90:66)
Internet Protocol Version 4, Src: 192.168.1.11, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 52958, Dst Port: 80, Seq: 1, Ack: 1, Len: 470
Hypertext Transfer Protocol
  GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1/r/n
    Host: gaia.cs.umass.edu/r/n
    Connection: keep-alive/r/n
    Upgrade-Insecure-Requests: 1/r/n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8/r/n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12) AppleWebKit/602.1.50 (KHTML, like Gecko) Version/10.0 Safari/602.1.50/r/n
    Accept-Language: en-us/r/n
    Accept-Encoding: gzip, deflate/r/n
    Authorization: Basic d2lyZXR0eXZlLXN0bWVibG9zZm5ldm9vcz0r/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 99]

```

19