

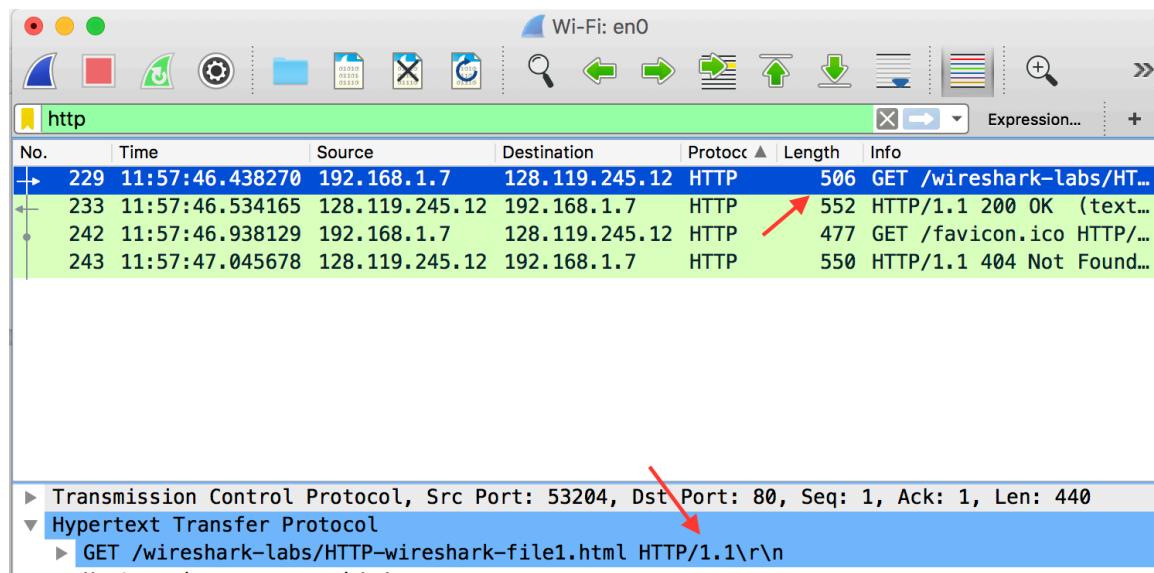
Class: CS-372  
Term: Fall 2017  
Author: Jon-Eric Cook  
Date: October 22, 2017  
Lab: #2

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

Answer:

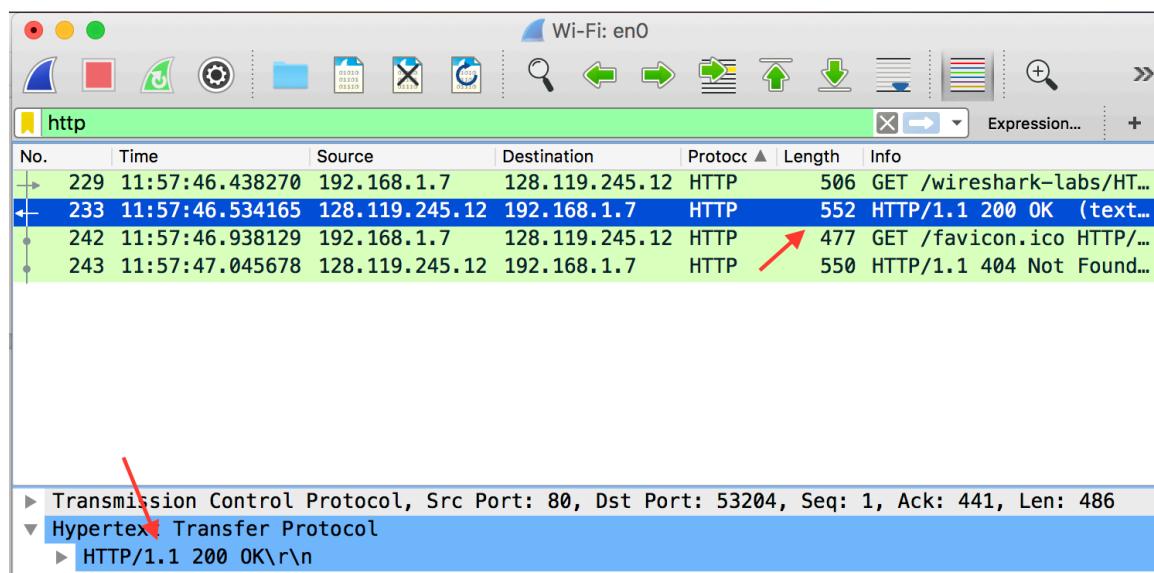
My browser is running HTTP version 1.1

In the screen shot below, see the 1.1 in the request line made by my browser.



The server is running HTTP version 1.1

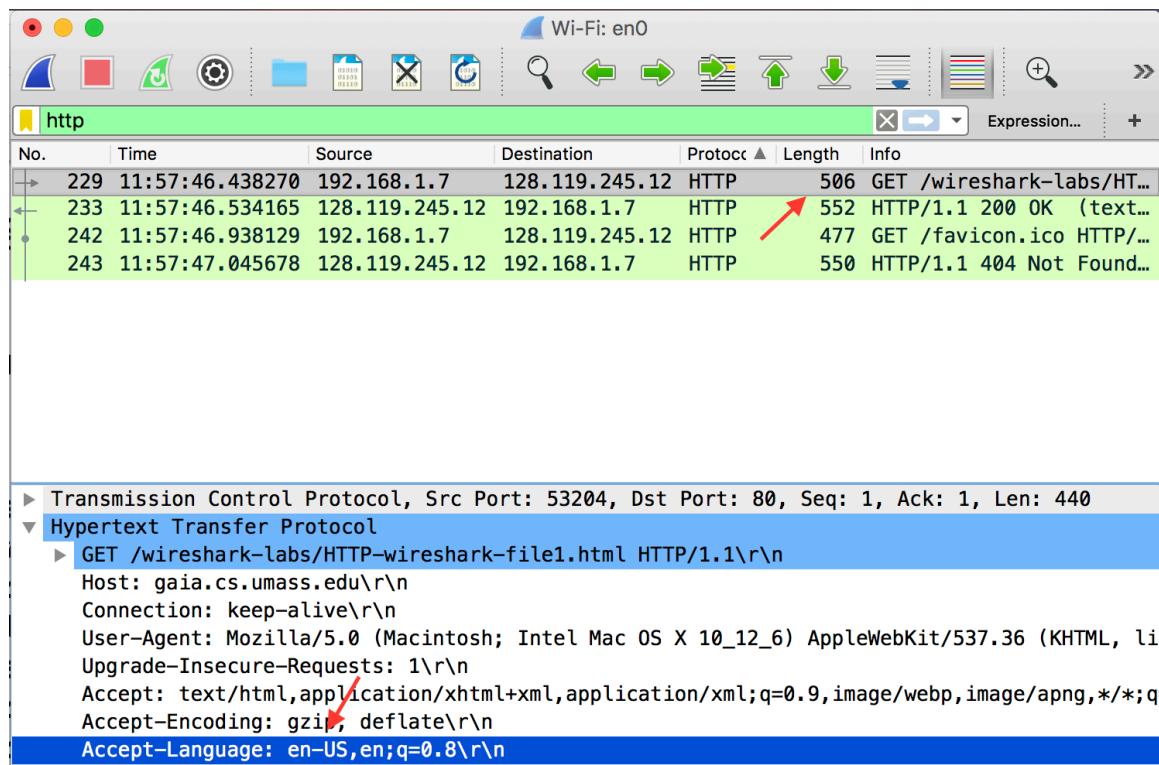
In the screen shot below, see the 1.1 in the status line returned by the server.



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

Answer:

My browser indicates that it can accept the English-US language from the server. See screen shot below.



The screenshot shows a Wireshark interface with the following details:

Network Interface: Wi-Fi: en0

Selected Protocol: http

Table Headers: No., Time, Source, Destination, Protocol, Length, Info

Table Data:

No.	Time	Source	Destination	Protocol	Length	Info
229	11:57:46.438270	192.168.1.7	128.119.245.12	HTTP	506	GET /wireshark-labs/HT...
233	11:57:46.534165	128.119.245.12	192.168.1.7	HTTP	552	HTTP/1.1 200 OK (text...)
242	11:57:46.938129	192.168.1.7	128.119.245.12	HTTP	477	GET /favicon.ico HTTP/...
243	11:57:47.045678	128.119.245.12	192.168.1.7	HTTP	550	HTTP/1.1 404 Not Found...

Details pane (expanded for the second row):

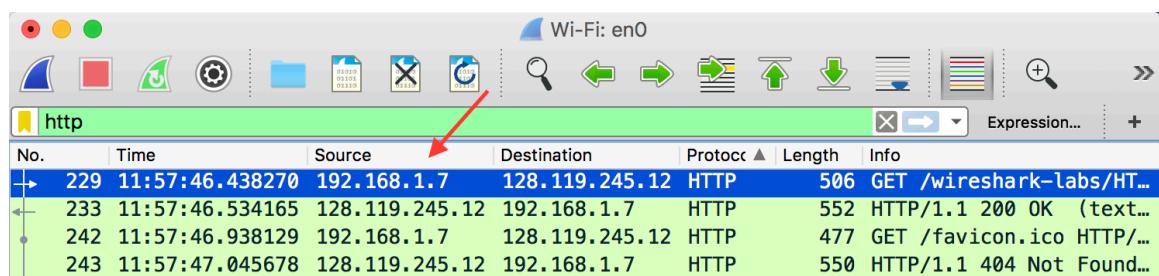
- Transmission Control Protocol, Src Port: 53204, Dst Port: 80, Seq: 1, Ack: 1, Len: 440
- Hypertext Transfer Protocol
  - GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
  - Host: gaia.cs.umass.edu\r\n
  - Connection: keep-alive\r\n
  - User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_12\_6) AppleWebKit/537.36 (KHTML, li
  - Upgrade-Insecure-Requests: 1\r\n
  - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q
  - Accept-Encoding: gzip, deflate\r\n
  - Accept-Language: en-US,en;q=0.8\r\n

- 3) What is the IP address of your computer? Of the [gaia.cs.umass.edu](http://gaia.cs.umass.edu) server?

Answer:

The IP address of my computer is 192.186.1.7

See screen shot below.



The screenshot shows a Wireshark interface with the following details:

Network Interface: Wi-Fi: en0

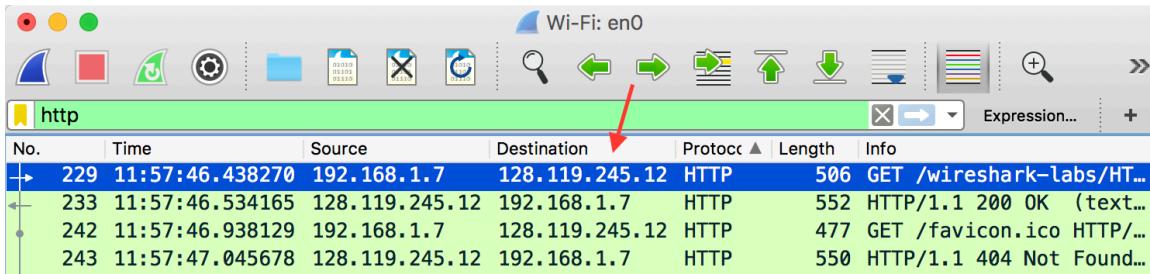
Selected Protocol: http

Table Headers: No., Time, Source, Destination, Protocol, Length, Info

Table Data:

No.	Time	Source	Destination	Protocol	Length	Info
229	11:57:46.438270	192.168.1.7	128.119.245.12	HTTP	506	GET /wireshark-labs/HT...
233	11:57:46.534165	128.119.245.12	192.168.1.7	HTTP	552	HTTP/1.1 200 OK (text...)
242	11:57:46.938129	192.168.1.7	128.119.245.12	HTTP	477	GET /favicon.ico HTTP/...
243	11:57:47.045678	128.119.245.12	192.168.1.7	HTTP	550	HTTP/1.1 404 Not Found...

The IP address of [gaia.cs.umass.edu](http://gaia.cs.umass.edu) server is 128.119.245.12  
See screen shot below.

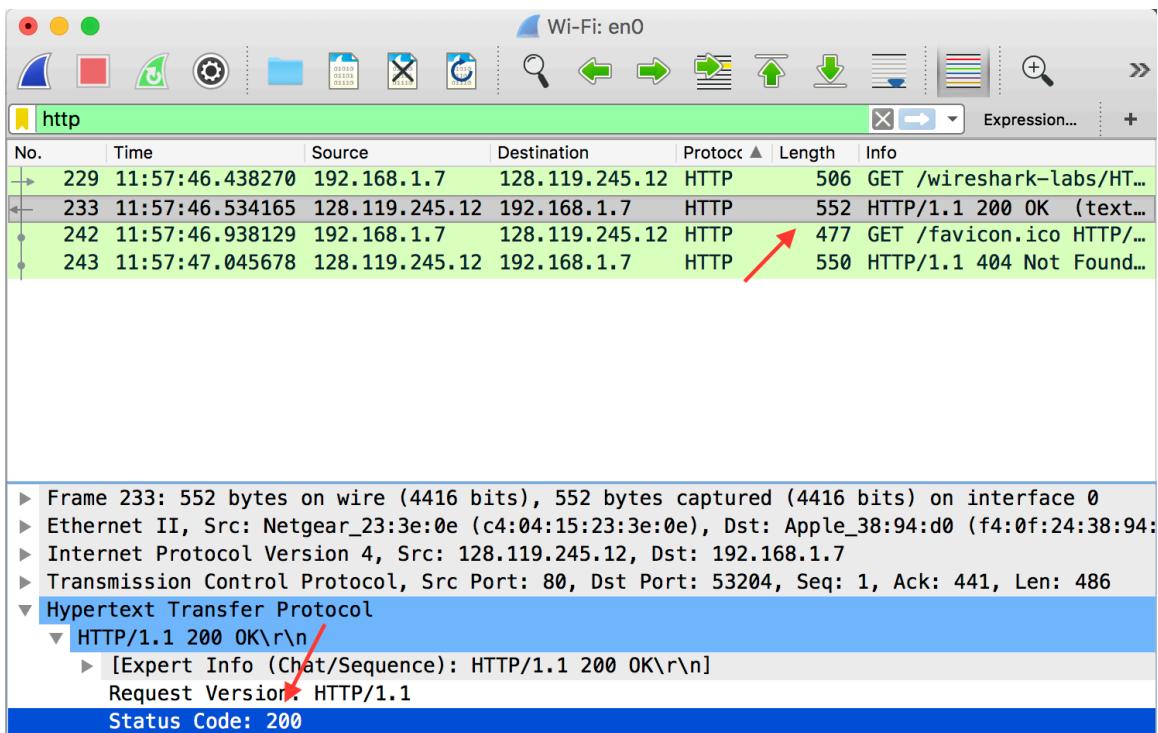


- 4) What is the status code returned from the server to your browser?

Answer:

200

See screen shot below.



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

Answer:

Friday, 13 October 2017 05:59:01 GMT

See screen shot below.

The screenshot shows a Wireshark interface with the following details:

**Network Interface:** Wi-Fi: en0

**Selected Filter:** http

**Table Headers:** No., Time, Source, Destination, Protocol, Length, Info

**Table Data:**

No.	Time	Source	Destination	Protocol	Length	Info
229	11:57:46.438270	192.168.1.7	128.119.245.12	HTTP	506	GET /wireshark-labs/HT...
233	11:57:46.534165	128.119.245.12	192.168.1.7	HTTP	552	HTTP/1.1 200 OK (text/...
242	11:57:46.938129	192.168.1.7	128.119.245.12	HTTP	477	GET /favicon.ico HTTP/...
243	11:57:47.045678	128.119.245.12	192.168.1.7	HTTP	550	HTTP/1.1 404 Not Found...

**Detailed View (Bottom Panel):**

```
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Date: Fri, 13 Oct 2017 18:57:48 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
Last-Modified: Fri, 13 Oct 2017 05:59:01 GMT\r\n
```

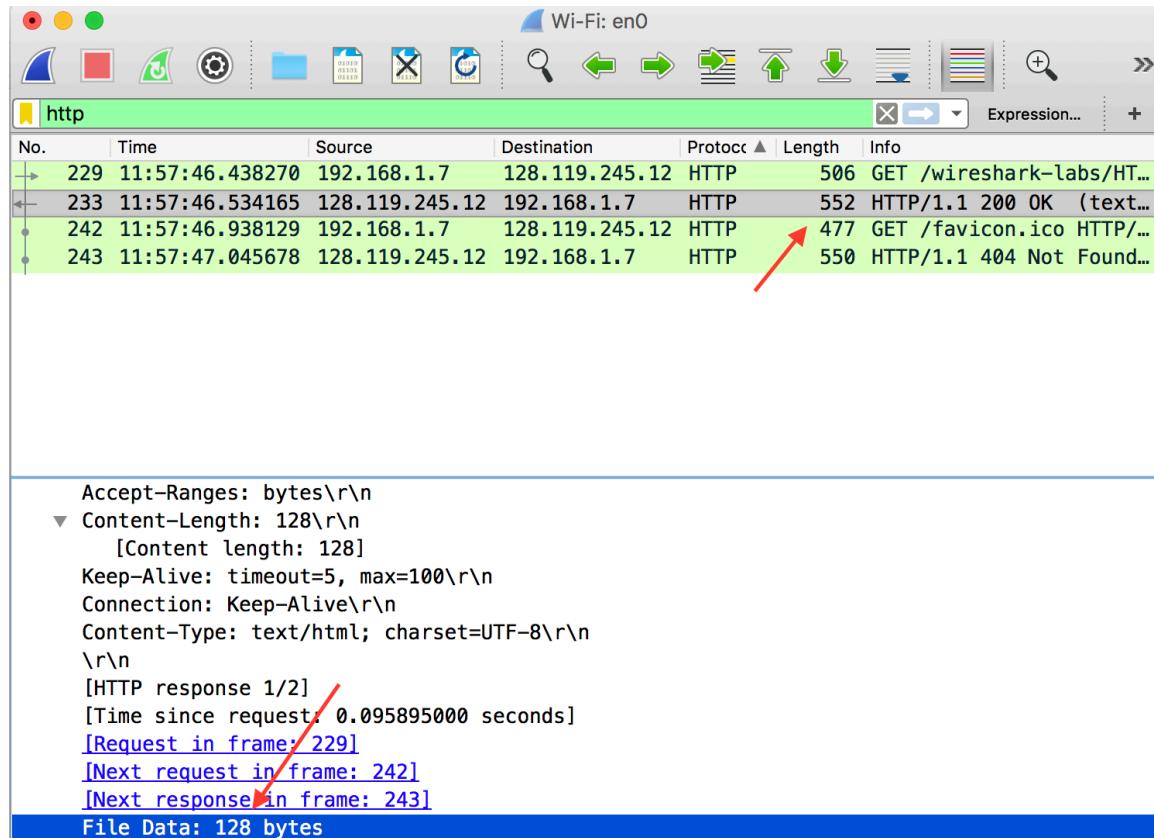
A red arrow points to the "Last-Modified" header in the detailed view, highlighting the date and time.

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

Answer:

128 bytes

See screen shot below.



- 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:

After an extensive inspection of the raw data in the packet content window, it was determined that all the headers within the data are in fact displayed in the packet-listing window.

See screen shot below.

No.	Time	Source	Destination	Protocol	Length	Info
229	11:57:46.438270	192.168.1.7	128.119.245.12	HTTP	506	GET /wireshark-labs/HT...
233	11:57:46.534165	128.119.245.12	192.168.1.7	HTTP	552	HTTP/1.1 200 OK (text...
242	11:57:46.938129	192.168.1.7	128.119.245.12	HTTP	477	GET /favicon.ico HTTP/...
243	11:57:47.045678	128.119.245.12	192.168.1.7	HTTP	550	HTTP/1.1 404 Not Found...

Frame 229: 506 bytes on wire (4048 bits), 506 bytes captured (4048 bits) on interface 0

- Interface id: 0 (en0)
- Encapsulation type: Ethernet (1)
- Arrival Time: Oct 13, 2017 11:57:46.438270000 PDT

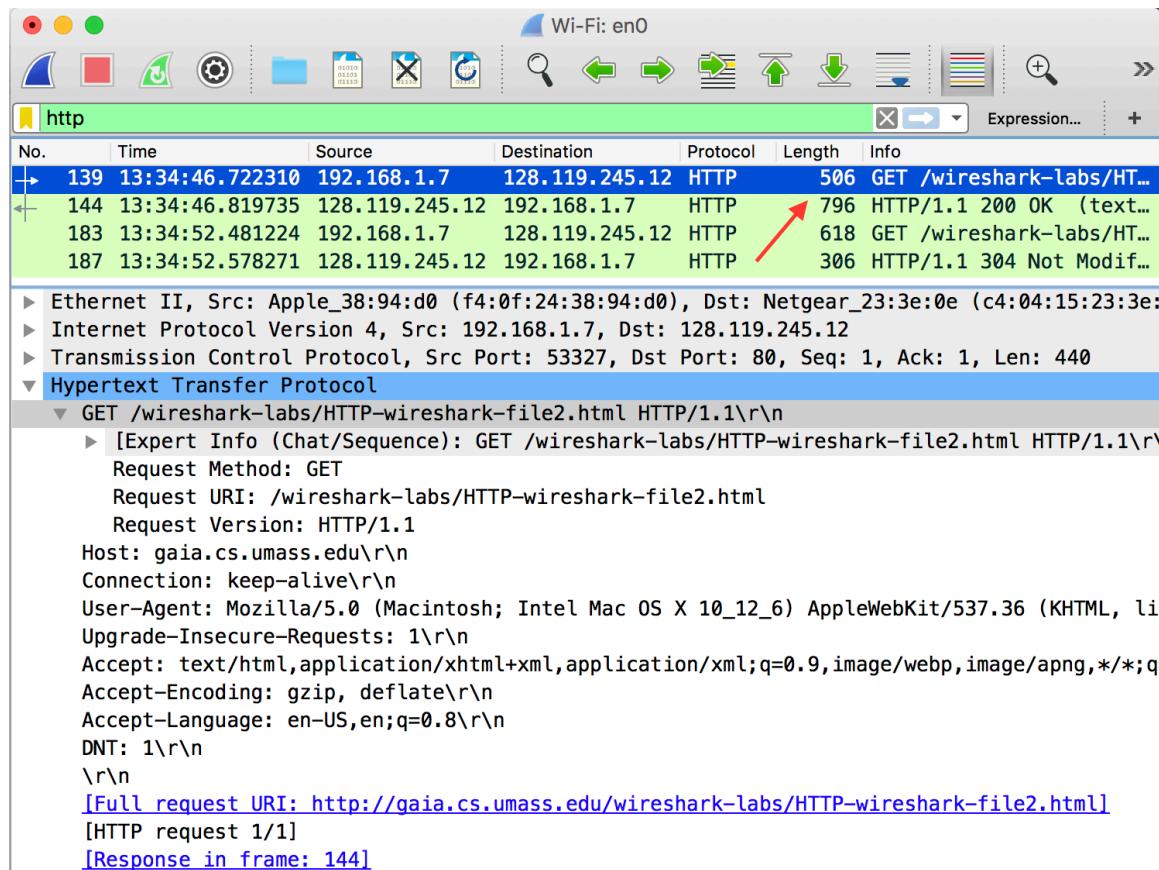
Hex	Dec	Text
0000	c4 04 15 23 3e 0e f4 0f	...#>.... \$8....E.
0010	01 ec c3 a7 40 00 40 06	....@. >.....w
0020	f5 0c cf d4 00 50 18 70	.....P.p .....
0030	10 15 a3 99 00 00 01 01	..... 2/\$.@.
0040	05 46 47 45 54 20 2f 77	.FGET /w ireshark
0050	2d 6c 61 62 73 2f 48 54	-labs/HT TP-wires
0060	68 61 72 6b 2d 66 69 6c	hark-fil e1.html
0070	48 54 54 50 2f 31 2e 31	HTTP/1.1 ..Host:
0080	67 61 69 61 2e 63 73 2e	gaia.cs. umass.ed
0090	75 0d 0a 43 6f 6e 65 63	u..Conne ction: k
00a0	65 65 70 2d 61 6c 69 76	eep-aliv e..User-
00b0	41 67 65 6e 74 3a 20 4d	Agent: M ozilla/5
00c0	2e 30 20 28 4d 61 63 69	.0 (Macintosh; I
00d0	6e 74 65 6c 20 4d 61 63	ntel Mac OS X 10
00e0	5f 31 32 5f 36 29 20 41	_12_6) A ppleWebK
00f0	69 74 2f 35 33 37 2e 33	it/537.3 6 (KHTML
0100	2c 20 6c 69 6b 65 20 47	, like Gecko) Ch
0110	72 6f 6d 65 2f 36 31 2e	rome/61. 0.3163.1
0120	30 30 20 53 61 66 61 72	00 Safar i/537.36
0130	0d 0a 55 70 67 72 61 64	..Upgrad e-Insecu
0140	72 65 2d 52 65 71 75 65	re-Reque sts: 1..
0150	41 63 63 65 70 74 3a 20	Accept: text/htm
0160	6c 2c 61 70 70 6c 69 63	l,application/xhtml
0170	74 6d 6c 2b 78 6d 6c 2c	+xml, applicat
0180	69 6f 6e 2f 78 6d 6c 3b	ion/xml; q=0.9,image/webp ,image/a
0190	61 67 65 2f 77 65 62 70	png,*/*; q=0.8..A
01a0	70 6e 67 2c 2a 2f 2a 3b	ccept-En coding:
01b0	63 63 65 70 74 2d 45 6e	gzip, de flate..A
01c0	67 7a 69 70 2c 20 64 65	ccept-La nguage:
01d0	63 63 65 70 74 2d 4c 61	en-US,en ;q=0.8..
01e0	65 6e 2d 55 53 2c 65 6e	DNT: 1... .
01f0	44 4e 54 3a 20 31 0d 0a	

- 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

See screen shot below.



The screenshot shows the Wireshark interface with the "http" protocol selected in the top bar. The packet list pane displays several HTTP requests. A red arrow points to the length field of the second packet (HTTP response), which is 796 bytes long. The expanded details pane shows the full HTTP request for "GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n". The request includes standard headers like Host, Connection, User-Agent, Accept, Accept-Encoding, Accept-Language, and DNT. It also includes a [Full request URI] link and [HTTP request 1/1] and [Response in frame: 144] links at the bottom.

No.	Time	Source	Destination	Protocol	Length	Info
139	13:34:46.722310	192.168.1.7	128.119.245.12	HTTP	506	GET /wireshark-labs/HT...
144	13:34:46.819735	128.119.245.12	192.168.1.7	HTTP	796	HTTP/1.1 200 OK (text...
183	13:34:52.481224	192.168.1.7	128.119.245.12	HTTP	618	GET /wireshark-labs/HT...
187	13:34:52.578271	128.119.245.12	192.168.1.7	HTTP	306	HTTP/1.1 304 Not Modif...

► Ethernet II, Src: Apple\_38:94:d0 (f4:0f:24:38:94:d0), Dst: Netgear\_23:3e:0e (c4:04:15:23:3e:  
► Internet Protocol Version 4, Src: 192.168.1.7, Dst: 128.119.245.12  
► Transmission Control Protocol, Src Port: 53327, Dst Port: 80, Seq: 1, Ack: 1, Len: 440  
▼ 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            User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_12\_6) AppleWebKit/537.36 (KHTML, li  
            Upgrade-Insecure-Requests: 1\r\n            Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q  
            Accept-Encoding: gzip, deflate\r\n            Accept-Language: en-US,en;q=0.8\r\n            DNT: 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: 144]

- 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 the contents can be seen in line-based text data.

See screen shot below.

Wi-Fi: en0

http

No.	Time	Source	Destination	Protocol	Length	Info
139	13:34:46.722310	192.168.1.7	128.119.245.12	HTTP	506	GET /wireshark-labs/HT...
144	13:34:46.819735	128.119.245.12	192.168.1.7	HTTP	796	HTTP/1.1 200 OK (text...
183	13:34:52.481224	192.168.1.7	128.119.245.12	HTTP	618	GET /wireshark-labs/HT...
187	13:34:52.578271	128.119.245.12	192.168.1.7	HTTP	306	HTTP/1.1 304 Not Modif...

Content-Length: 371\r\n[Content length: 371]  
Keep-Alive: timeout=5, max=100\r\nConnection: Keep-Alive\r\nContent-Type: text/html; charset=UTF-8\r\n\r\n[HTTP response 1/1]  
[Time since request: 0.097425000 seconds]  
[Request in frame: 139](#)  
File Data: 371 bytes

Line-based text data: text/html

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

- 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, there is an “IF-MODIFIED-SINCE:” line in the HTTP GET. The date “Fri, 13 Oct 2017 05:59:01 GMT” follows the “IF-MODIFIED-SINCE:” header.

See screen shot below.

The screenshot shows a Wireshark capture window for the 'http' protocol. The packet list pane shows several HTTP requests and responses. A red arrow points to the 'If-None-Match' header in the request for frame 183, which contains the value '173-55b675a7d6d78'. Another red arrow points to the 'If-Modified-Since' header in the response for frame 187, which contains the value 'Fri, 13 Oct 2017 05:59:01 GMT'.

No.	Time	Source	Destination	Protocol	Length	Info
139	13:34:46.722310	192.168.1.7	128.119.245.12	HTTP	506	GET /wireshark-labs/HT...
144	13:34:46.819735	128.119.245.12	192.168.1.7	HTTP	796	HTTP/1.1 200 OK (text...
183	13:34:52.481224	192.168.1.7	128.119.245.12	HTTP	618	GET /wireshark-labs/HT...
187	13:34:52.578271	128.119.245.12	192.168.1.7	HTTP	306	HTTP/1.1 304 Not Modif...

Frame 183: 618 bytes on wire (4944 bits), 618 bytes captured (4944 bits) on interface 0  
Ethernet II, Src: Apple\_38:94:d0 (f4:0f:24:38:94:d0), Dst: Netgear\_23:3e:0e (c4:04:15:23:3e:  
Internet Protocol Version 4, Src: 192.168.1.7, Dst: 128.119.245.12  
Transmission Control Protocol, Src Port: 53328, Dst Port: 80, Seq: 1, Ack: 1, Len: 552  
Hypertext Transfer Protocol  
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nConnection: keep-alive\r\nCache-Control: max-age=0\r\nUser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_12\_6) AppleWebKit/537.36 (KHTML, li  
Upgrade-Insecure-Requests: 1\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q  
Accept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.8\r\nDNT: 1\r\nIf-None-Match: '173-55b675a7d6d78"\r\nIf-Modified-Since: Fri, 13 Oct 2017 05:59:01 GMT\r

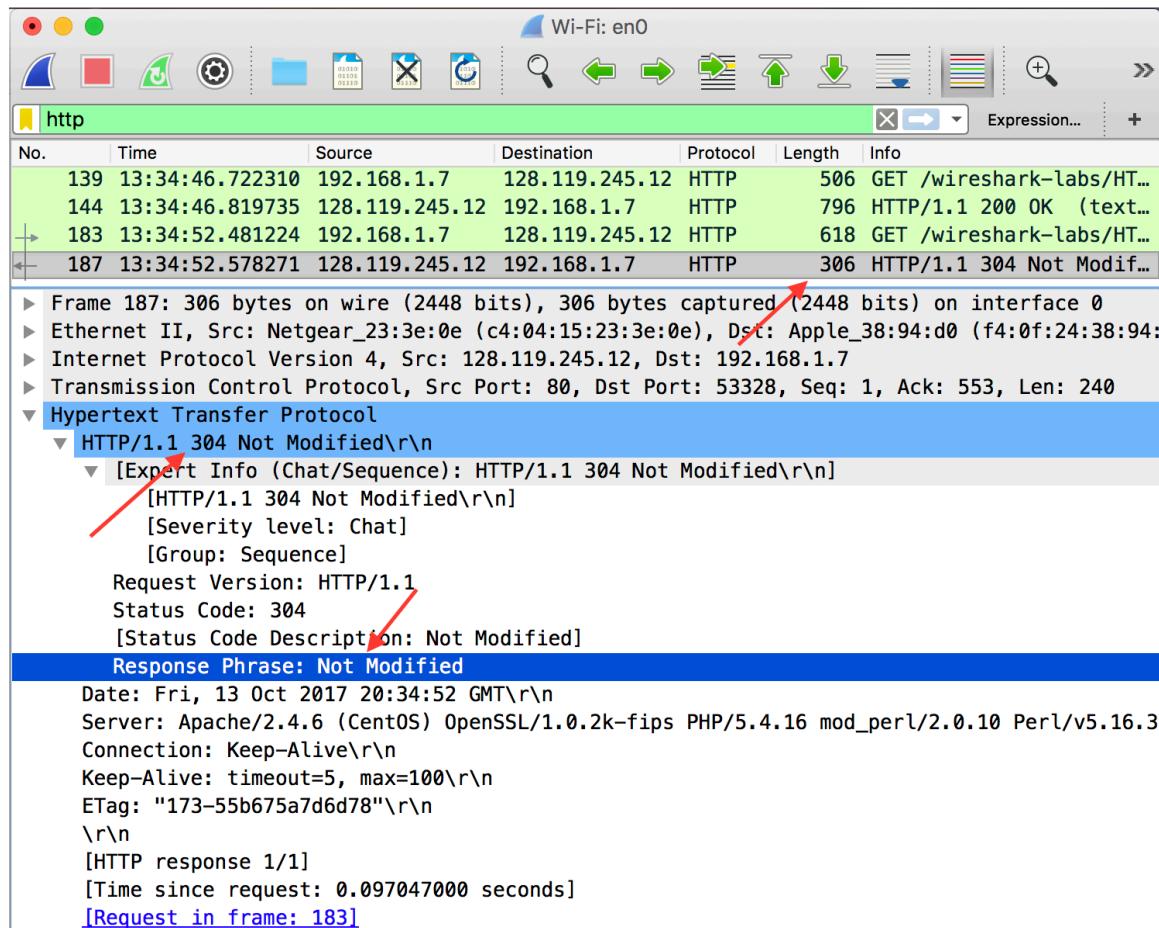
- 11) What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

Answer:

HTTP/1.1 304 Not Modified

The server did not explicitly return the contents of the file because the browser loaded it from its cache.

See screen shot below.



The screenshot shows a Wireshark interface with the following details:

- Wi-Fi: en0** is selected.
- http** is selected in the filter bar.
- Frame 187** is selected in the list.
- HTTP/1.1 304 Not Modified** is expanded in the tree view.
- [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]** is shown under the expanded item.
- [Severity level: Chat]** and **[Group: Sequence]** are listed under the expert info.
- Request Version: HTTP/1.1**, **Status Code: 304**, and **[Status Code Description: Not Modified]** are listed under the expanded item.
- Response Phrase: Not Modified** is highlighted in blue.
- Date: Fri, 13 Oct 2017 20:34:52 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**, **Connection: Keep-Alive\r\n**, **Keep-Alive: timeout=5, max=100\r\n**, **ETag: "173-55b675a7d6d78"\r\n**, **\r\n**, **[HTTP response 1/1]**, **[Time since request: 0.097047000 seconds]**, and **[Request in frame: 183]** are listed under the expanded item.

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

Answer:

My browser only sent 1 HTTP GET request message. Packet number 183 contained the GET request message for the Bill of Rights.

See screen shot below.

No.	Time	Source	Destination	Protocol	Length	Info
→ 183	14:06:28.879365	192.168.1.7	128.119.245.12	HTTP	506	GET /wireshark-labs/HT...
← 188	14:06:28.976983	128.119.245.12	192.168.1.7	HTTP	583	HTTP/1.1 200 OK (text...)

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

Answer:

Packet number 188

See screen shot below.

No.	Time	Source	Destination	Protocol	Length	Info
→ 183	14:06:28.879365	192.168.1.7	128.119.245.12	HTTP	506	GET /wireshark-labs/HT...
← 188	14:06:28.976983	128.119.245.12	192.168.1.7	HTTP	583	HTTP/1.1 200 OK (text...)

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

Answer:

HTTP/1.1 200 OK

See screen shot below.

No.	Time	Source	Destination	Protocol	Length	Info
→ 183	14:06:28.879365	192.168.1.7	128.119.245.12	HTTP	506	GET /wireshark-labs/HT...
← 188	14:06:28.976983	128.119.245.12	192.168.1.7	HTTP	583	HTTP/1.1 200 OK (text...)

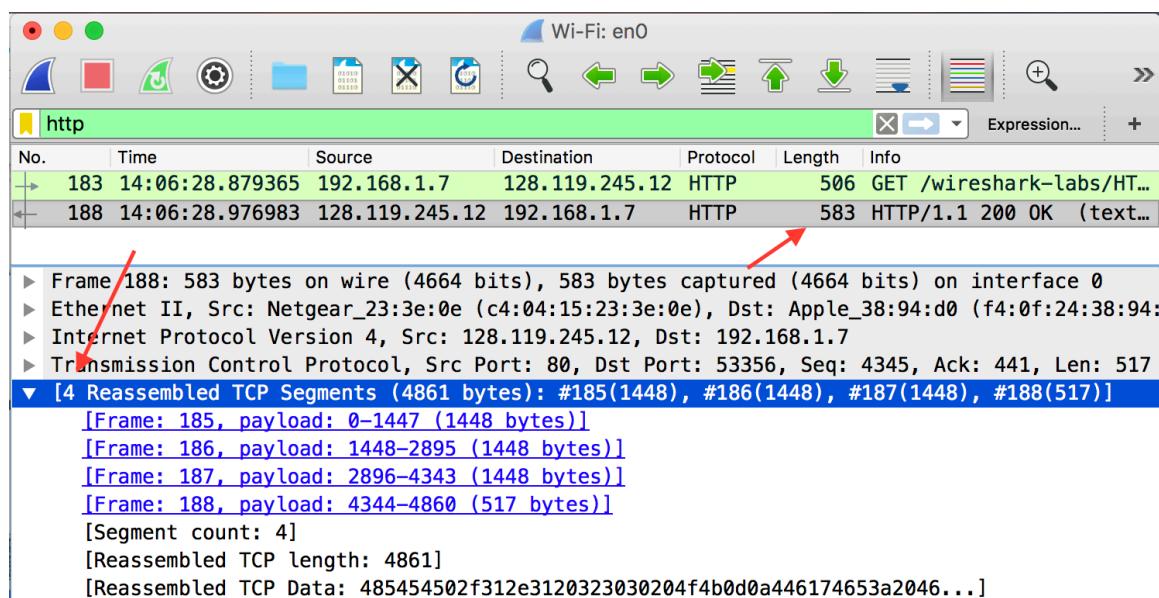
Frame 188: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface 0  
Ethernet II, Src: Netgear\_23:3e:0e (c4:04:15:23:3e:0e), Dst: Apple\_38:94:d0 (f4:0f:24:38:94:  
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.7  
Transmission Control Protocol, Src Port: 80, Dst Port: 53356, Seq: 4345, Ack: 441, Len: 517  
[4 Reassembled TCP Segments (4861 bytes): #185(1448), #186(1448), #187(1448), #188(517)]  
▼ Hypertext Transfer Protocol  
    ▼ HTTP/1.1 200 OK\r\n

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

Answer:

There was 4 data-containing TCP segments.

See the screen shot below.



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

Answer:

My browser sent 4 HTTP GET request messages. The following are the IP address that the 4 HTTP GET requests were sent to:

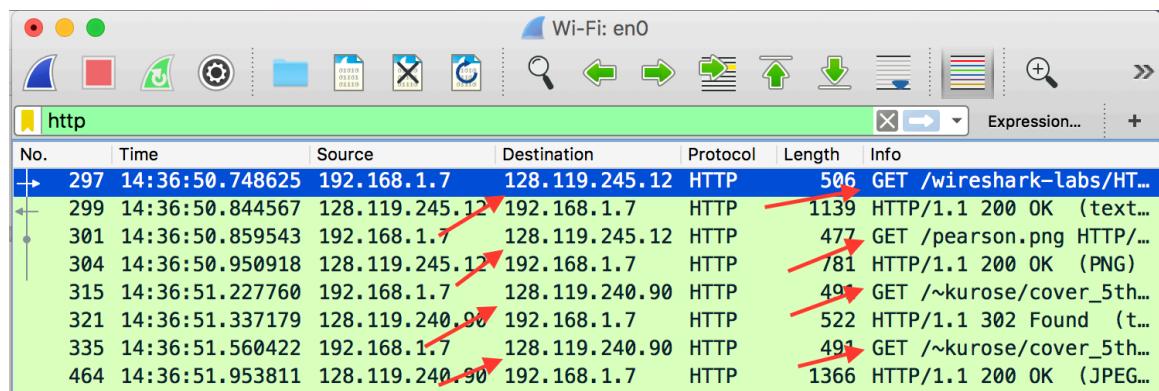
128.119.245.12

128.119.245.12

128.119.240.19

128.119.240.19

See screen shot below.



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

Answer:

My browser downloaded the two images serially because one image was requested and then returned and then another image was requested and then returned. Also, the time stamps indicate that time elapsed after each HTTP GET request. Also, if the images were downloaded in parallel, I think there would only be one HTTP GET request for both images.

See screen shot below.

No.	Time	Source	Destination	Protocol	Length	Info
297	14:36:50.748625	192.168.1.7	128.119.245.12	HTTP	506	GET /wireshark-labs/HT...
299	14:36:50.844567	128.119.245.12	192.168.1.7	HTTP	1139	HTTP/1.1 200 OK (text...
301	14:36:50.859543	192.168.1.7	128.119.245.12	HTTP	477	GET /pearson.png HTTP/...
304	14:36:50.950918	128.119.245.12	192.168.1.7	HTTP	781	HTTP/1.1 200 OK (PNG)
315	14:36:51.227760	192.168.1.7	128.119.240.90	HTTP	491	GET /~kurose/cover_5th...
321	14:36:51.337179	128.119.240.90	192.168.1.7	HTTP	522	HTTP/1.1 302 Found (t...
335	14:36:51.560422	192.168.1.7	128.119.240.90	HTTP	491	GET /~kurose/cover_5th...
464	14:36:51.953811	128.119.240.90	192.168.1.7	HTTP	1366	HTTP/1.1 200 OK (JPEG...

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

Answer:

HTTP/1.1 401 Unauthorized

See screen shot below.

No.	Time	Source	Destination	Protocol	Length	Info
46	14:52:55.272114	192.168.1.7	128.119.245.12	HTTP	525	GET /wireshark-labs/pr...
48	14:52:55.372660	128.119.245.12	192.168.1.7	HTTP	783	HTTP/1.1 401 Unauthorized
159	14:53:19.609332	192.168.1.7	128.119.245.12	HTTP	584	GET /wireshark-labs/pr...
161	14:53:19.707181	128.119.245.12	192.168.1.7	HTTP	597	HTTP/1.1 404 Not Found...

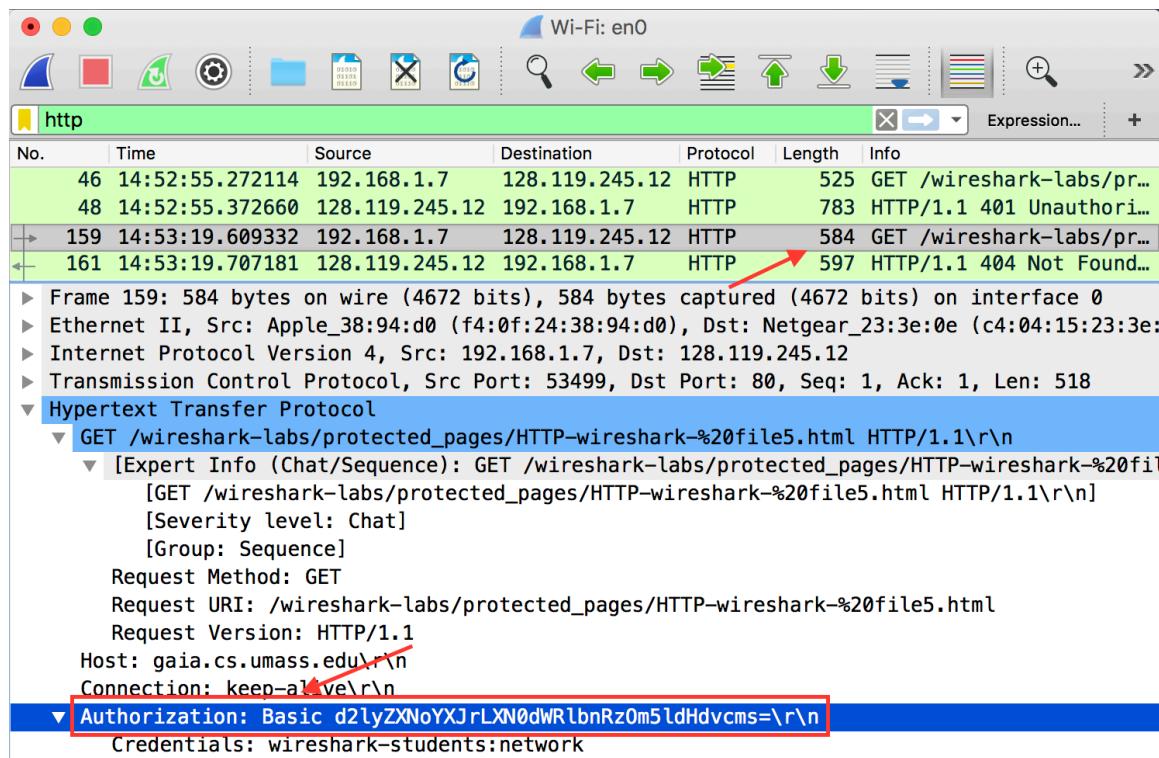
Frame 48: 783 bytes on wire (6264 bits), 783 bytes captured (6264 bits) on interface 0  
Ethernet II, Src: Netgear\_23:3e:0e (c4:04:15:23:3e:0e), Dst: Apple\_38:94:d0 (f4:0f:24:38:94:  
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.7  
Transmission Control Protocol, Src Port: 80, Dst Port: 53497, Seq: 1, Ack: 460, Len: 717  
Hypertext Transfer Protocol  
HTTP/1.1 401 Unauthorized\r\n

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:

Authorization: Basic .....

See screen shot below.



The screenshot shows a Wireshark interface with the following details:

- Network Interface:** Wi-Fi: en0
- Selected Filter:** http
- Captured Packets:** 161 (Frame 159 highlighted)
- Protocol Tree:** Frame 159 details:
  - Frame 159: 584 bytes on wire (4672 bits), 584 bytes captured (4672 bits) on interface 0
  - Ethernet II, Src: Apple\_38:94:d0 (f4:0f:24:38:94:d0), Dst: Netgear\_23:3e:0e (c4:04:15:23:3e:0e)
  - Internet Protocol Version 4, Src: 192.168.1.7, Dst: 128.119.245.12
  - Transmission Control Protocol, Src Port: 53499, Dst Port: 80, Seq: 1, Ack: 1, Len: 518
- HTTP Request Details:** GET /wireshark-labs/protected\_pages/HTTP-wireshark-%20file5.html HTTP/1.1\r\n
- Authorization Header:** Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRz0m5ldHdvcmss=\r\n (highlighted with a red box)
- Credentials:** Credentials: wireshark-students:network