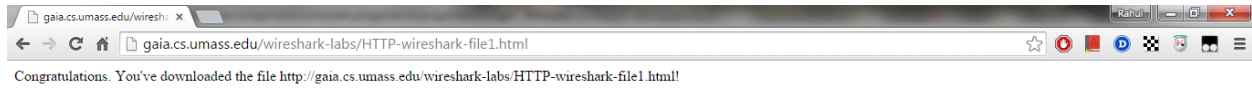
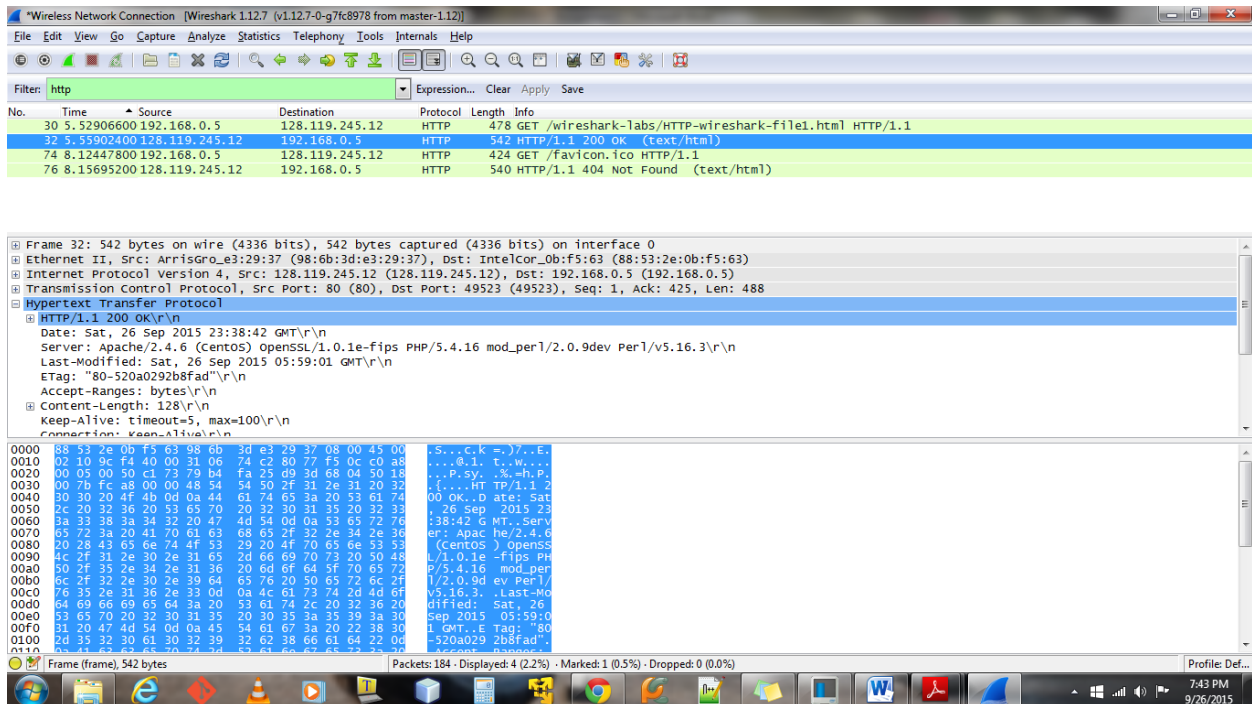


Assignment 3 - Wireshark Lab: HTTP v6.1

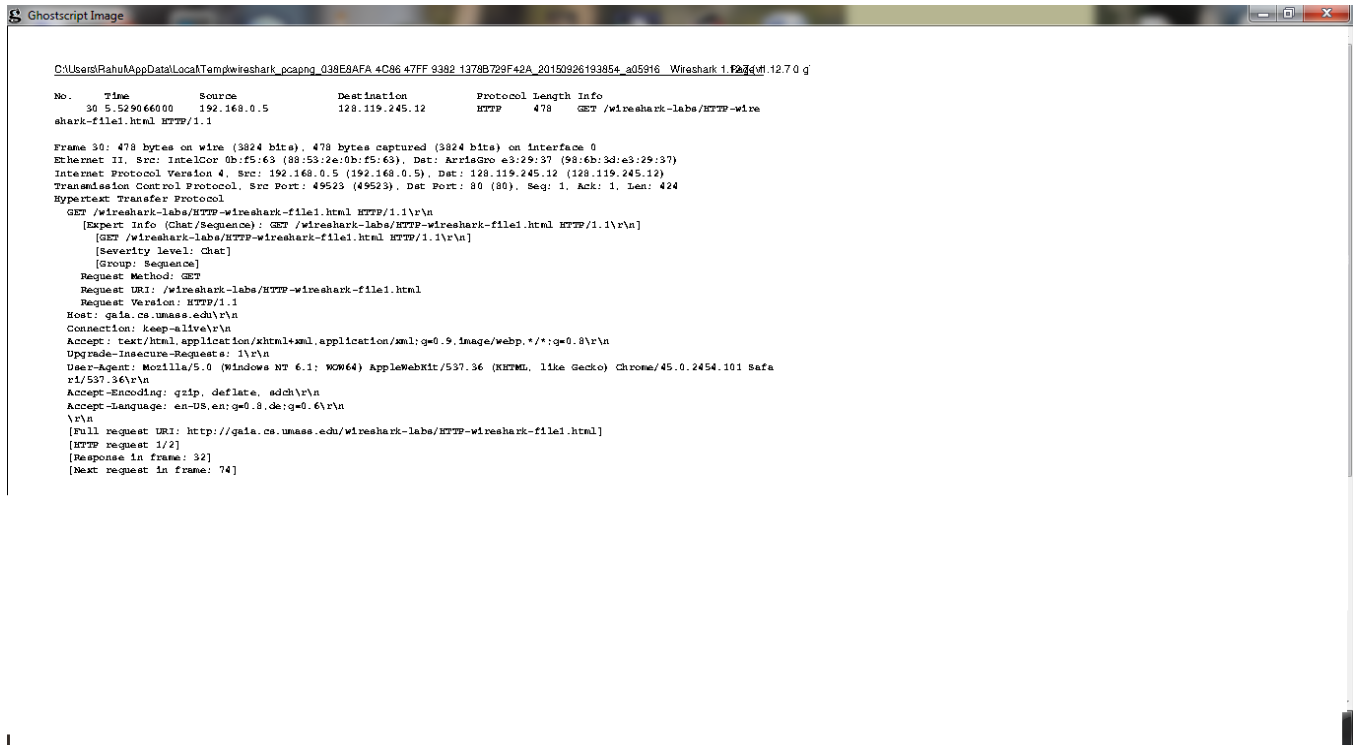
Answer 1: The Basic HTTP GET/response interaction



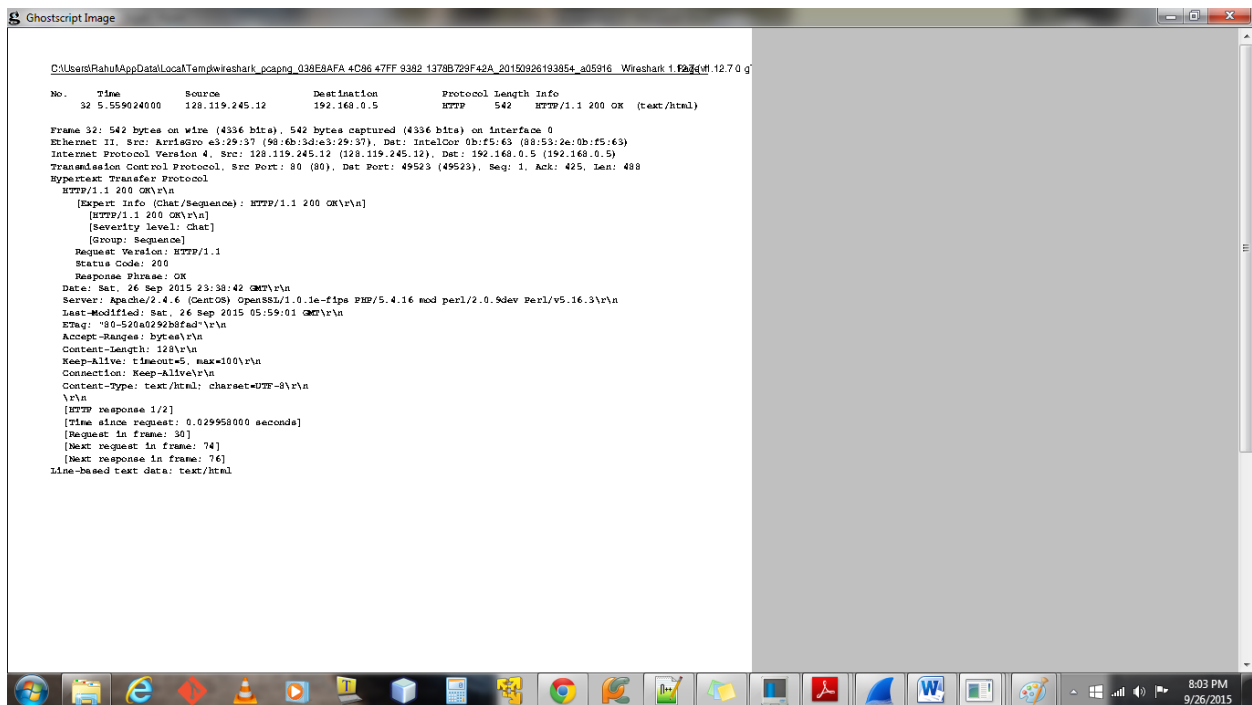
1a. Browser Output



1b. Wireshark Output



1c. Request Packet Print



1d. Response Packet Print

1. Browser is running **HTTP/1.1** version (from image 1c)

```
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
```

Server is running = **HTTP/1.1** (from image 1d)

```
HTTP/1.1 200 OK\r\n
```

2. The languages that the browser can detect are - **en-US ,en, de** (from image 1c) English – US Version, German

```
Accept-Encoding: gzip, deflate, sdch\r\n
Accept-Language: en-US,en;q=0.8,de;q=0.6\r\n
\r\n
```

3. IP address of the computer is : **192.168.0.5** (from image 1c)

```
Internet Protocol Version 4, Src: 192.168.0.5 (192.168.0.5), Dst: 128.119.245.12 (128.119.245.12)
```

IP address of gaia.cs.umass.edu server : **128.119.245.12** (from image 1c)

```
Internet Protocol Version 4, Src: 192.168.0.5 (192.168.0.5), Dst: 128.119.245.12 (128.119.245.12)
```

4. Status code returned from server: **200** (from image 1d)

```
HTTP/1.1 200 OK\r\n
```

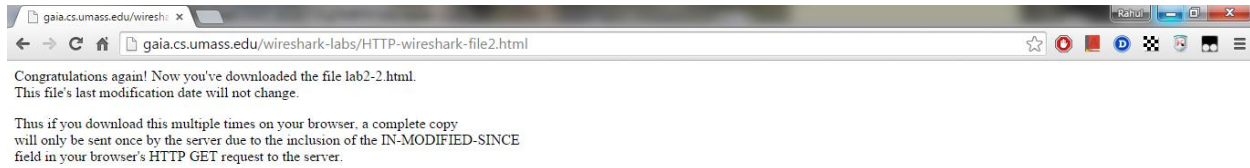
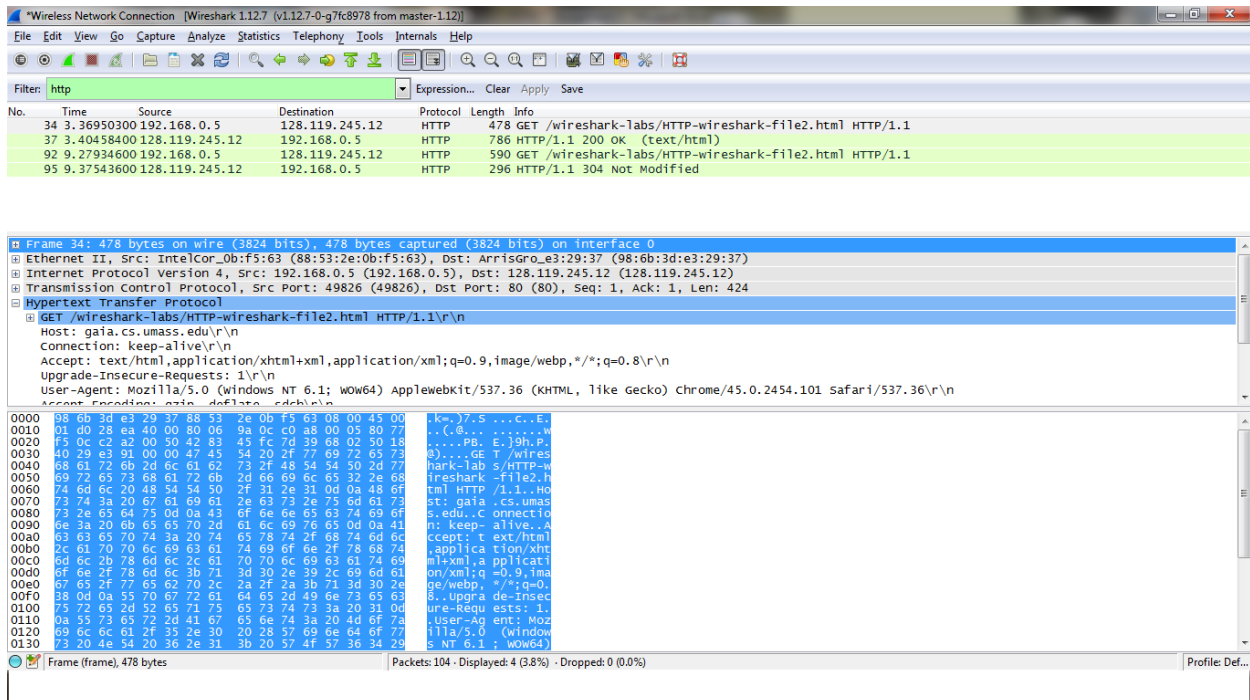
5. The HTML File retrieved from the server was last modified at **Sat, 26 Sep 2015 05:59:01 GMT** (from image 1d)

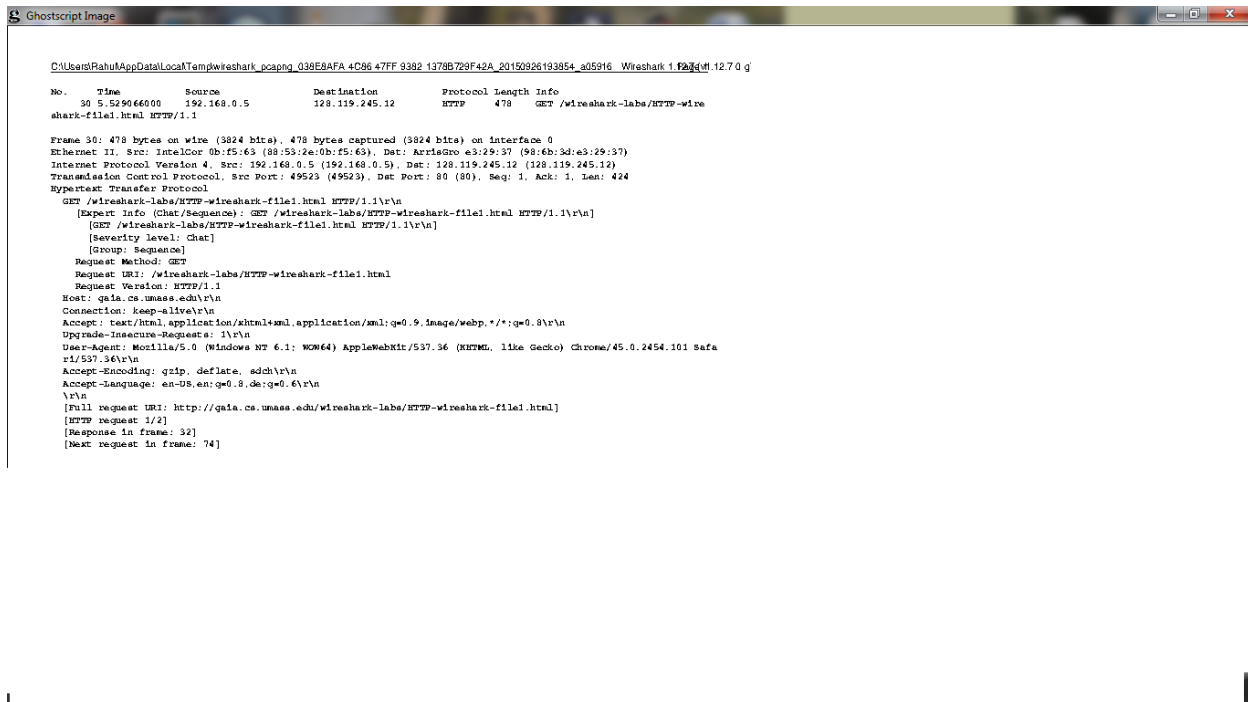
```
Last-Modified: Sat, 26 Sep 2015 05:59:01 GMT\r\n
```

6. The number of bytes of content returned are : **128**

```
Content-Length: 128\r\n
```

7. No extra headers are found that is not present in the packet content window.

Answer 2: The HTTP CONDITIONAL GET/response interaction**2a. Browser Output****2b. Wireshark Output**



2c. First Get Request to server

C:\Users\Rahul\AppData\Local\Temp\wireshark_pcapng_038E8AFA-4C86-47FF-9382-1378B729F42A_20150926203524_a07720 Wireshark 1.12.7.0 g

No.	Time	Source	Destination	Protocol	Length	Info
37	3.404584000	128.119.245.12	192.168.0.5	HTTP	786	HTTP/1.1 200 OK (text/html)

Frame 37: 786 bytes on wire (6288 bits), 786 bytes captured (6288 bits) on interface 0

Ethernet II, Src: ArriaGro e3:29:37 (98:6b:3d:e3:29:37), Dst: IntelCor 08:f5:63:88:53:2e (08:f5:63:88:53:2e)

Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.0.5 (192.168.0.5)

Transmission Control Protocol, Src Port: 80 (80), Dst Port: 49826 (49826), Seq: 1, Ack: 425, Len: 732

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Sun, 27 Sep 2015 00:35:10 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: Sat, 26 Sep 2015 05:59:01 GMT\r\n

ETag: "173-520a0292b800d"\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: 0.035081000 seconds]

[Request in frame: 34]

Line-based text data: text/html

2d. First Response from server

C:\Users\Rahul\AppData\Local\Temp\wireshark_pcapng_038E8AFA-4C86-47FF-9382-1378B729F42A_20150926203524_a07720_Wireshark 1.12.7.0 g

No.	Time	Source	Destination	Protocol	Length	Info
92	9.279346000	192.168.0.5	128.119.245.12	HTTP	590	GET /wireshark-labs/HTTP-wire

shark-file2.html HTTP/1.1

Frame 92: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface 0
 Ethernet II, Src: IntelCor 0b:f5:63 (88:53:2e:0b:f5:63), Dst: ArrisGro e3:29:37 (98:6b:3d:e3:29:37)
 Internet Protocol Version 4, Src: 192.168.0.5 (192.168.0.5), Dst: 128.119.245.12 (128.119.245.12)
 Transmission Control Protocol, Src Port: 49828 (49828), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 536
 Hypertext Transfer Protocol
 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
 Host: gaia.cs.umass.edu\r\n
 Connection: keep-alive\r\n
 Cache-Control: max-age=0\r\n
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
 Upgrade-Insecure-Requests: 1\r\n
 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safa
 ri/537.36\r\n
 Accept-Encoding: gzip, deflate, sdch\r\n
 Accept-Language: en-US,en;q=0.8,de;q=0.6\r\n
 If-None-Match: "173-520a0292b800d"\r\n
 If-Modified-Since: Sat, 26 Sep 2015 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: 95]

2e. Second Get request to server

C:\Users\Rahul\AppData\Local\Temp\wireshark_pcapng_038E8AFA-4C86-47FF-9382-1378B729F42A_20150926203524_a07720_Wireshark 1.12.7.0 g

No.	Time	Source	Destination	Protocol	Length	Info
95	9.375436000	128.119.245.12	192.168.0.5	HTTP	296	HTTP/1.1 304 Not Modified

Frame 95: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits) on interface 0
 Ethernet II, Src: ArrisGro e3:29:37 (98:6b:3d:e3:29:37), Dst: IntelCor 0b:f5:63 (88:53:2e:0b:f5:63)
 Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.0.5 (192.168.0.5)
 Transmission Control Protocol, Src Port: 80 (80), Dst Port: 49828 (49828), Seq: 1, Ack: 537, Len: 242
 Hypertext Transfer Protocol
 HTTP/1.1 304 Not Modified\r\n
 Date: Sun, 27 Sep 2015 00:35:16 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: "173-520a0292b800d"\r\n
 \r\n
 [HTTP response 1/1]
 [Time since request: 0.096090000 seconds]
 [Request in frame: 92]

2f. Second Response from server

8. From the above image (2c) it's clear that there is **no** IF-MODIFIED-SINCE field is present in the first GET Request.
9. Yes server returns the contents of the file. It can be known from the **status code 200** and the **content-length 371** from image (2d)

```

Hypertext Transfer Protocol
HTTP/1.1 200 OK
Date: Sun, 27 Sep 2015 00:35:10 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1
Last-Modified: Sat, 26 Sep 2015 05:59:01 GMT
Etag: "173-520a0292b800d"
Accept-Ranges: bytes
Content-Length: 371
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

[HTTP response 1/1]
[Time since request: 0.035081000 seconds]
[Request in frame: 34]
Line-based text data: text/html

```

10. From the image (2e) it's clear that the **field IF-MODIFIED-SINCE is present** and the value is:
Sat, 26 Sep 2015 05:59:01 GMT

```

If-Modified-Since: Sat, 26 Sep 2015 05:59:01 GMT

```

11. From the image (2f) the HTTP Status code is 304 and phrase is **NOT MODIFIED**

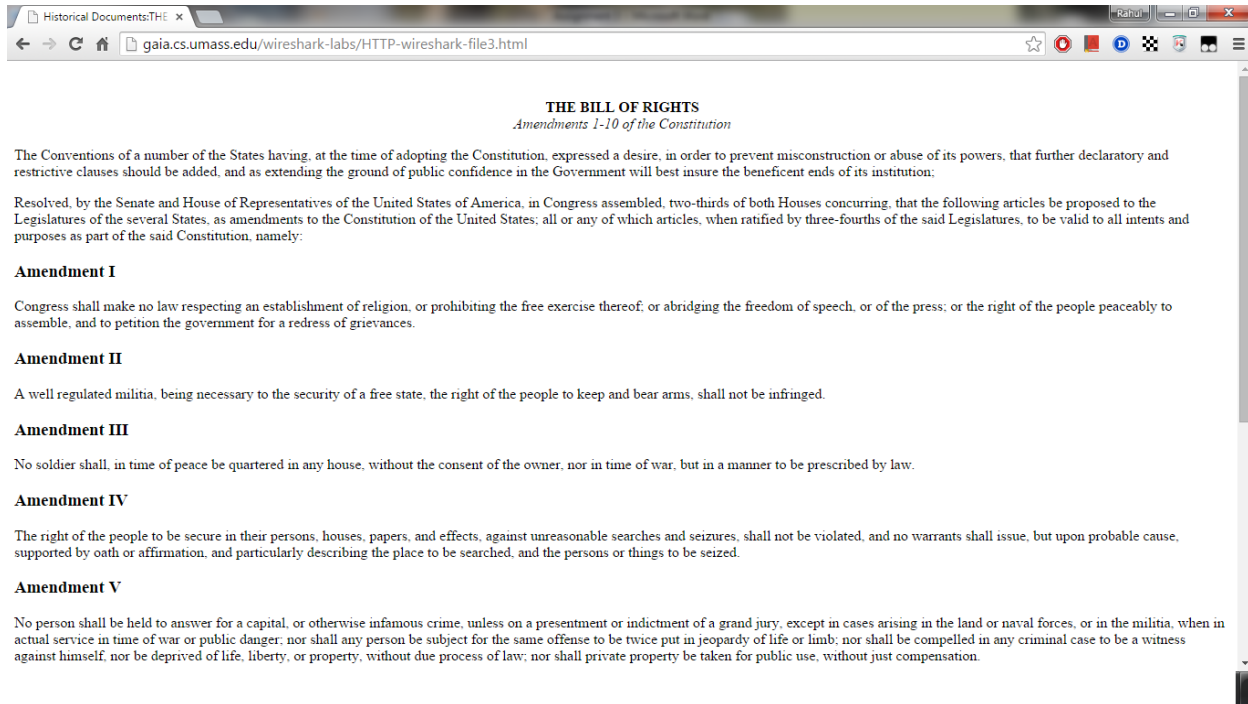
```

HTTP/1.1 304 Not Modified

```

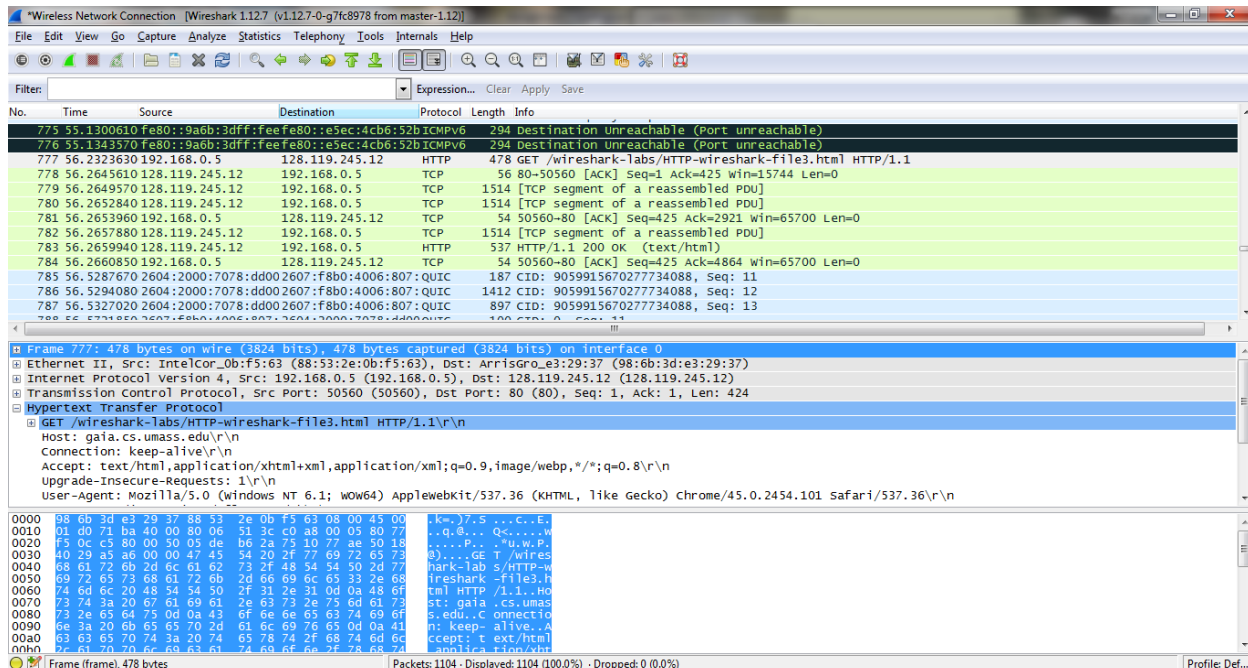
The server did not explicitly return the contents of the file. The server noticed that the file has not changed since **26 Sep 2015 05:59:01 GMT**, hence sent a **304** response code with phrase **NOT MODIFIED**

Answer 3: Retrieving Long Documents



The screenshot shows a web browser window with the address bar displaying `gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html`. The page content is titled "THE BILL OF RIGHTS" and "Amendments 1-10 of the Constitution". The text of the Bill of Rights is displayed, including the preamble and the first five amendments. The browser's address bar and the document's title are visible at the top.

3a. Browser Output



The screenshot shows a Wireshark network traffic capture. The top pane displays a list of captured packets. The selected packet is a GET request from 192.168.0.5 to 128.119.245.12. The packet details pane shows the following information:

- Frame 777: 478 bytes on wire (3824 bits), 478 bytes captured (3824 bits) on interface 0
- Ethernet II, Src: IntelCor_Ob:f5:63 (88:53:2e:0b:f5:63), Dst: ArrisGro_e3:29:37 (98:6b:3d:e3:29:37)
- Internet Protocol Version 4, Src: 192.168.0.5 (192.168.0.5), Dst: 128.119.245.12 (128.119.245.12)
- Transmission Control Protocol, Src Port: 50560 (50560), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 424
- 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
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
 - Upgrade-Insecure-Requests: 1\r\n
 - User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36\r\n

The packet bytes pane shows the raw data of the packet, including the HTTP request line and headers.

3b. Wireshark Output

12. One GET Request message is sent by the browser. The packet number that contains the GET message for the bill of rights is **777**

777	56.2323630	192.168.0.5	128.119.245.12	HTTP	478	GET /wireshark-labs/HTTP-wireshark-file3.html	HTTP/1.1
-----	------------	-------------	----------------	------	-----	---	----------

13. The packet number of the packet that contains the status code and the phrase associated with the response to the HTTP GET request is **779**

779	56.2649570	128.119.245.12	192.168.0.5	TCP	1514	[TCP segment of a reassembled PDU]	
Frame 779: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0							
Ethernet II, Src: ArrisGro_e3:29:37 (98:6b:3d:e3:29:37), Dst: IntelCor_0b:f5:63 (88:53:2e:0b:f5:63)							
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.0.5 (192.168.0.5)							
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 50560 (50560), Seq: 1, Ack: 425, Len: 1460							
Source Port: 80 (80)							
Destination Port: 50560 (50560)							
[Stream index: 19]							
[TCP Segment Len: 1460]							
0030	00 7b 7a 2f 00 00	48 54 54 50 2f 31 2e 31 20 32	{z/..HT TP/1.1 2				
0040	30 30 20 4f 4b 0d 0a 44	61 74 65 3a 20 53 75 6e	00 OK..D ate: Sun				
0050	2c 20 32 37 20 53 65 70	20 32 30 31 35 20 30 33	: 200 OK (text/html)				
0060	3a 35 30 3a 32 33 20 47	4d 54 0d 0a 53 65 72 76	: 50:23 G MT.. Serv				
0070	65 72 3a 20 41 70 61 63	68 65 2f 32 2e 34 2e 36	er: Apache/2.4.6				
0080	20 28 43 65 6e 74 4f 53	29 20 4f 70 65 6e 53 53	(CentOS) OpenSSL				
0090	4c 2f 31 2e 30 2e 31 65	2d 66 69 70 73 20 50 48	L/1.0.1e -fips PH				
00a0	50 2f 35 2e 34 2e 31 36	20 6d 6f 64 5f 70 65 72	P/5.4.16 mod_per				
00b0	6c 2f 32 2e 30 2e 39 64	65 76 20 50 65 72 6c 2f	l/2.0.9d ev Perl/				
00c0	76 35 2e 31 36 2e 33 0d	0a 4c 61 73 74 2d 4d 6f	v5.16.3. .Last-Mo				
00d0	64 69 66 69 65 64 3a 20	53 61 74 2c 20 32 36 20	dified: Sat, 26				
00e0	53 65 70 20 32 30 31 35	20 30 35 3a 35 39 3a 30	Sep 2015 05:59:0				
00f0	31 20 47 4d 54 0d 0a 45	54 61 67 3a 20 22 31 31	1 GMT..E Tag: "11				
0100	39 34 2d 35 32 30 61 30	32 39 32 62 34 64 34 34	94-520a0 292b4d44				
0110	22 0d 0a 41 63 63 65 70	74 2d 52 61 6e 67 65 73	".Accep t-Ranges				
0120	3a 20 63 70 74 65 73 0d	0a 43 65 6e 74 65 6e 74	. bytes Content				

14. The status code is **200** and the phrase is **OK** in the response

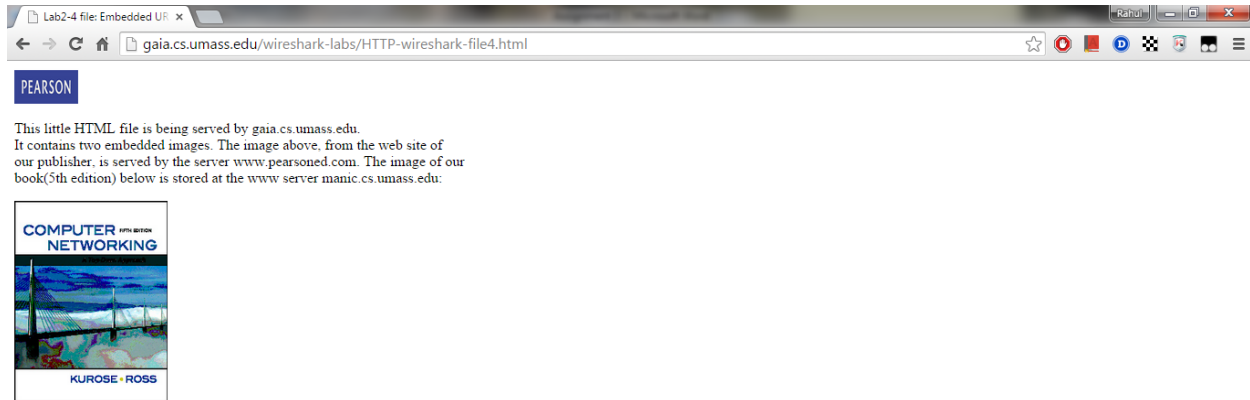
782	56.2657880	128.119.245.12	192.168.0.5	TCP	1514	[TCP segment of a reassembled PDU]	
783	56.2659940	128.119.245.12	192.168.0.5	HTTP	537	HTTP/1.1 200 OK (text/html)	
784	56.2660850	192.168.0.5	128.119.245.12	TCP	54	50560->80 [ACK] Seq=425 Ack=4864 Win=65700 Len=0	

No.	Time	Source	Destination	Protocol	Length	Info
783	56.2659940000	128.119.245.12	192.168.0.5	HTTP	537	HTTP/1.1 200 OK (text/html)

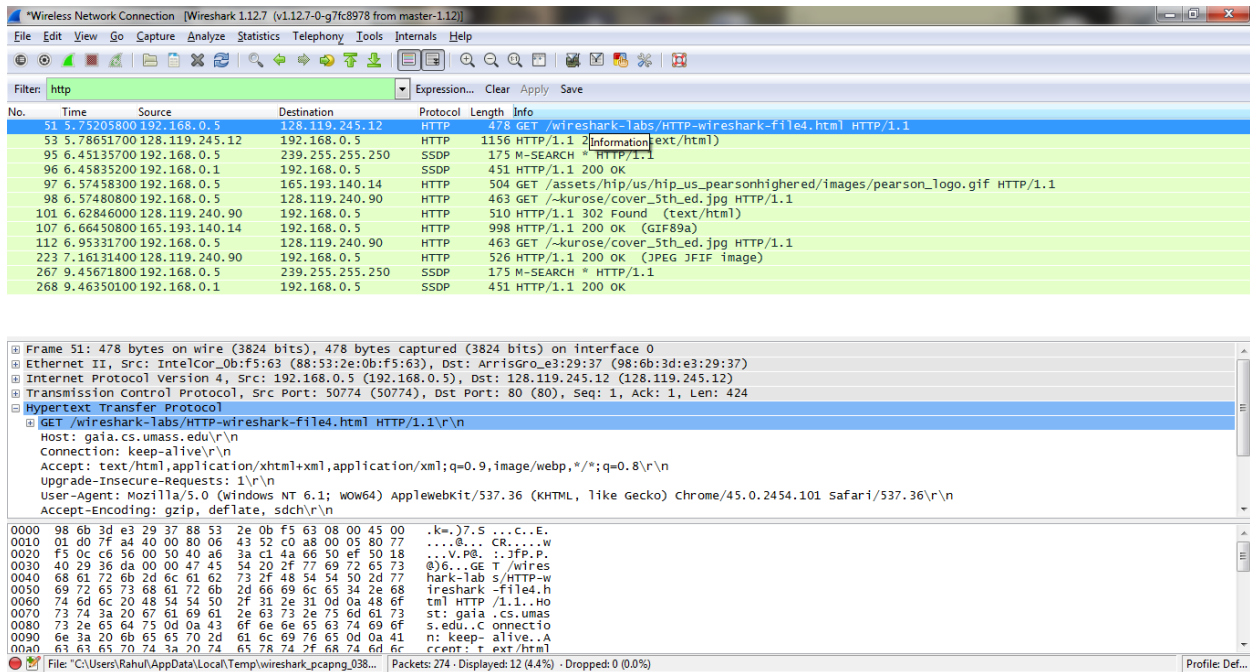
15. The number of data containing TCP Segments to carry the single HTTP response and the text of bill of rights is **5**

778	56.2645610	128.119.245.12	192.168.0.5	TCP	56	80->50560 [ACK] Seq=1 Ack=425 Win=15744 Len=0	3 → 5
779	56.2649570	128.119.245.12	192.168.0.5	TCP	1514	[TCP segment of a reassembled PDU]	
780	56.2652840	128.119.245.12	192.168.0.5	TCP	1514	[TCP segment of a reassembled PDU]	
781	56.2653960	192.168.0.5	128.119.245.12	TCP	54	50560->80 [ACK] Seq=425 Ack=2921 Win=65700 Len=0	
782	56.2657880	128.119.245.12	192.168.0.5	TCP	1514	[TCP segment of a reassembled PDU]	
783	56.2659940	128.119.245.12	192.168.0.5	HTTP	537	HTTP/1.1 200 OK (text/html)	2
784	56.2660850	192.168.0.5	128.119.245.12	TCP	54	50560->80 [ACK] Seq=425 Ack=4864 Win=65700 Len=0	

Answer 4: HTML Documents with Embedded Objects



4a. Browser Output



4b. Wireshark Output

16. The HTTP GET Request messages sent are **4**. They are -

1. GET Request for the **HTTP-wireshark-file4.html** to **gaia.cs.umass.edu** (Address : **128.119.245.12**)

```
51 5.75205800 192.168.0.5 128.119.245.12 HTTP 478 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
```

2. GET Request for the **pearson_logo.gif** to **www.pearsonhighered.com** (Address: **165.193.140.14**)

```
97 6.57458300 192.168.0.5 165.193.140.14 HTTP 504 GET /assets/hip/us/hip_us_pearsonhighered/images/pearson_logo.gif HTTP/1.1
```

3. GET Request for the **cover_5th-ed.jpg** to **manic.cs.umass.edu** (Address: **128.119.240.90**)

```
98 6.57480800 192.168.0.5 128.119.240.90 HTTP 463 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
```

4. Since the GET Request for **pearson_logo.gif** to **www.pearsonhighered.com** returns **302** page moved status, there is another redirect GET Request for **pearson_logo.gif** to **caite.cs.umass.edu** (Address: **128.119.240.90**)

```
112 6.95331700 192.168.0.5 128.119.240.90 HTTP 463 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
```

17. The two images were downloaded in parallel.

The first GET request was sent at **6.57458300**

```
97 6.57458300 192.168.0.5 165.193.140.14 HTTP 504 GET /assets/hip/us/hip_us_pearsonhighered/images/pearson_logo.gif HTTP/1.1
```

The second GET request was sent at **6.57480800** without waiting for 200 status code for the first GET request.

```
98 6.57480800 192.168.0.5 128.119.240.90 HTTP 463 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
```

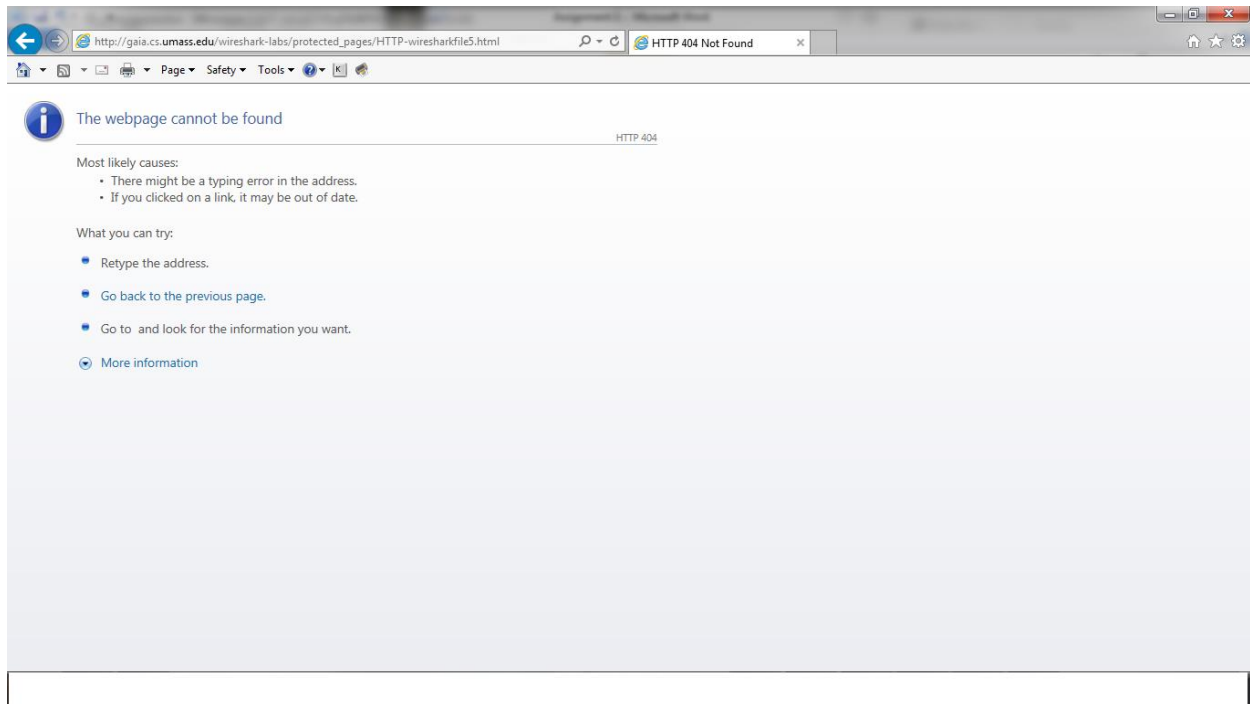
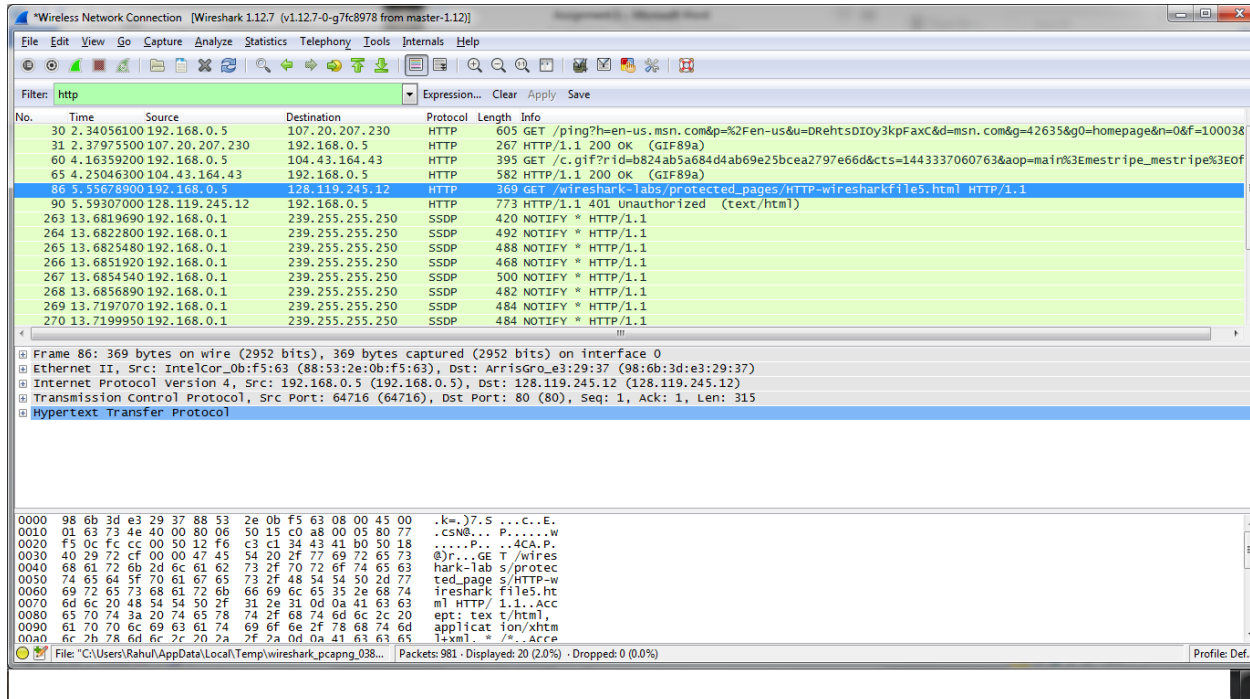
This means both the requests were sent in parallel and each response was handled by the browser asynchronously as the browser did not wait for first GET Request's response before sending the next GET Request.

The first response was received at **6.62846000** which is the response for the first GET Request

```
101 6.62846000 128.119.240.90 192.168.0.5 HTTP 510 HTTP/1.1 302 Found (text/html)
```

The second response was received at **6.66450800** which is the response for the second GET request.

```
107 6.66450800 165.193.140.14 192.168.0.5 HTTP 998 HTTP/1.1 200 OK (GIF89a)
```

Answer 5: HTTP Authentication**4a. Browser Output****4b. Wireshark Output**

18. The server's response to the initial HTTP GET message is –

Status Code – **401**

Status Phrase - **Unauthorized**

90	5.59307000	128.119.245.12	192.168.0.5	HTTP	773	HTTP/1.1 401 Unauthorized (text/html)
Frame 90: 773 bytes on wire (6184 bits), 773 bytes captured (6184 bits) on interface 0 Ethernet II, Src: ArrisGro e3:29:37 (98:6b:3d:e3:29:37), Dst: IntelCor 0b:f5:63 (88:53:2e:0b:f5:63) Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.0.5 (192.168.0.5) Transmission Control Protocol, Src Port: 80 (80), Dst Port: 64716 (64716), Seq: 1, Ack: 316, Len: 719 Hypertext Transfer Protocol HTTP/1.1 401 Unauthorized\r\n						

19. The new field included in the HTTP GET message is the **Authorization** Field

454	24.8096370	192.168.0.5	128.119.245.12	HTTP	428	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
No.	Time	Source	Destination	Protocol	Length	Info
454	24.809637000	192.168.0.5	128.119.245.12	HTTP	428	GET /wireshark-labs/protected pages/HTTP-wiresharkfile5.html HTTP/1.1
Host: gala.cs.umass.edu\r\n Authorization: Basic d2lyZXNoYXJrLXN0dWVlbnRzOm5ldHdvcm8=\r\n Connection: Keep-Alive\r\n						