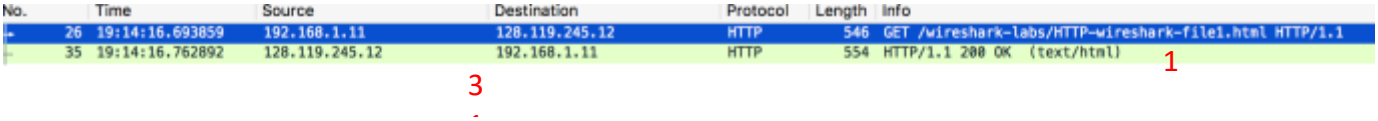
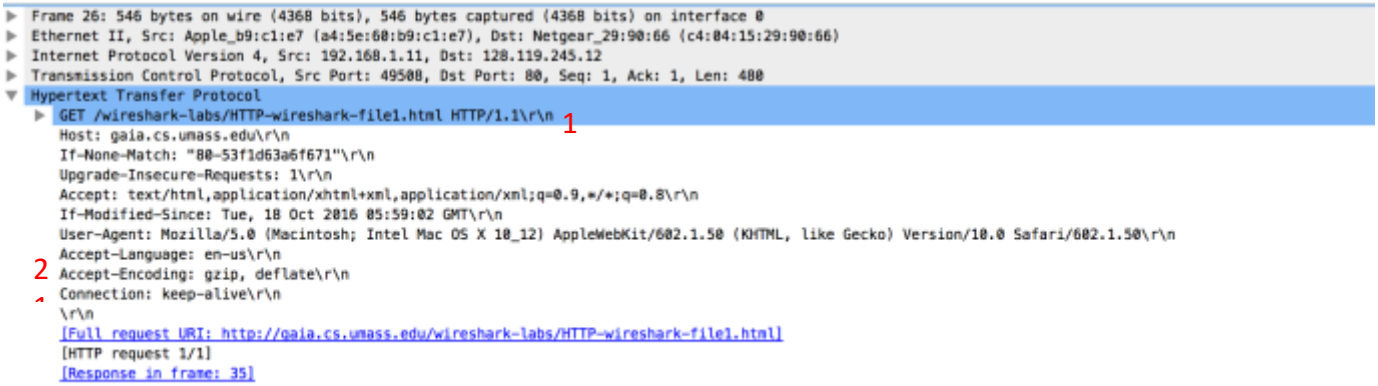
Rob Navarro
CS372

LAB 2

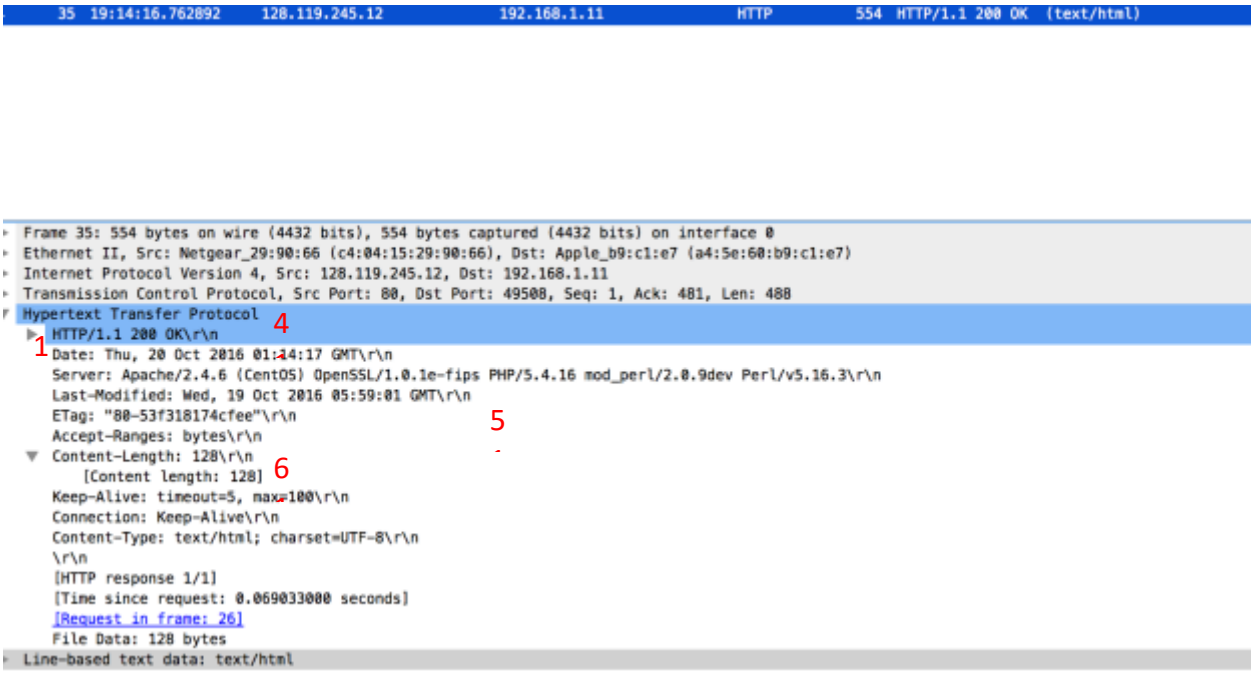
1. **Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?**
   Answer: My browser is running HTTP version 1.1 and the server is running HTTP 1.1.
2. **What languages (if any) does your browser indicate that it can accept to the server?**
   Answer: en-us
3. **What 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:





Rob Navarro
CS372



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:

Rob Navarro
CS372

1st 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	605	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
43	19:59:21.532941	128.119.245.12	192.168.1.11	HTTP	308	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 (a4:5e: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: 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]
```

1st 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	605	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
43	19:59:21.532941	128.119.245.12	192.168.1.11	HTTP	308	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 (a4:5e: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: 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
```

Rob Navarro
CS372

2nd 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	605	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
43	19:59:21.532941	128.119.245.12	192.168.1.11	HTTP	308	HTTP/1.1 304 Not Modified

```
▶ Frame 38: 605 bytes on wire (4840 bits), 605 bytes captured (4840 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: 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 10
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/1]
    [Response in frame: 43]
```

2nd Response

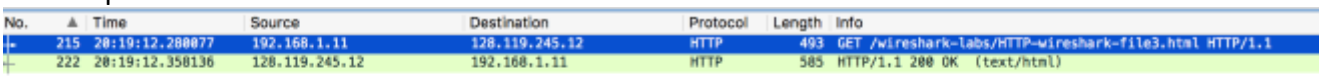
No.	Time	Source	Destination	Protocol	Length	Info
22	19:59:12.188188	192.168.1.11	128.119.245.12	HTTP	519	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
26	19:59:12.255968	128.119.245.12	192.168.1.11	HTTP	798	HTTP/1.1 200 OK (text/html)
38	19:59:21.469743	192.168.1.11	128.119.245.12	HTTP	605	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
43	19:59:21.532941	128.119.245.12	192.168.1.11	HTTP	308	HTTP/1.1 304 Not Modified

```
▶ Frame 43: 308 bytes on wire (2464 bits), 308 bytes captured (2464 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: 52551, Seq: 1, Ack: 540, Len: 242
▼ Hypertext Transfer Protocol
11  ▼ 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]
```

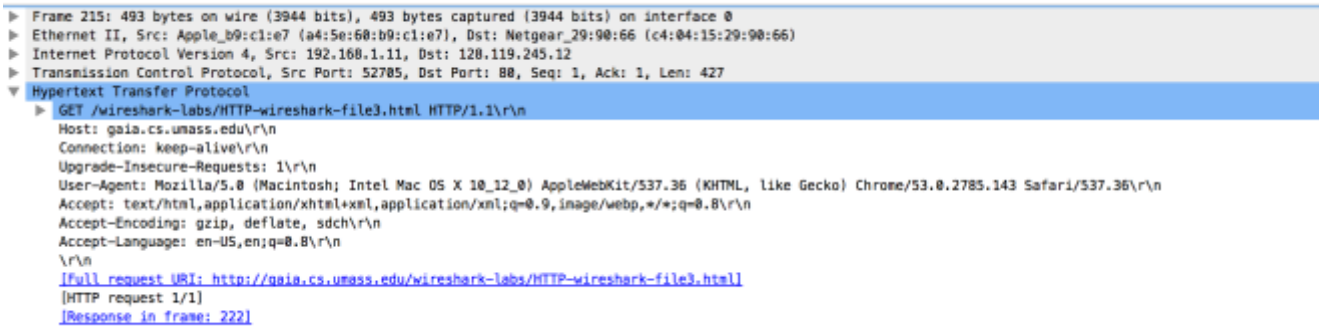
Rob Navarro
CS372

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

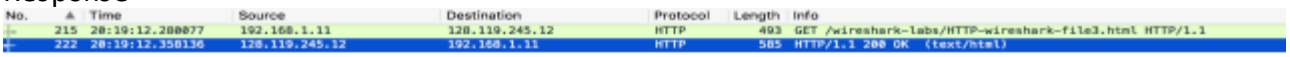
GET Request

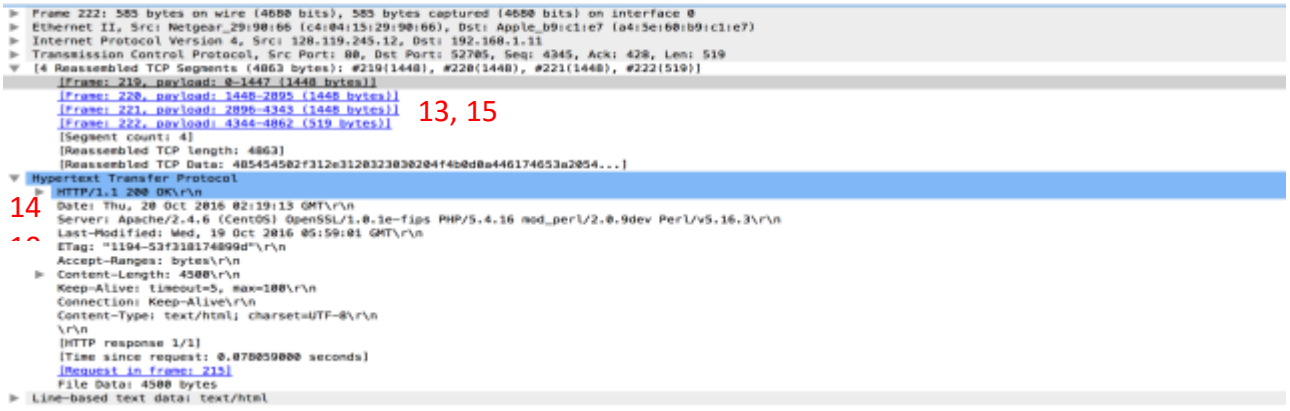


12



Response





13, 15

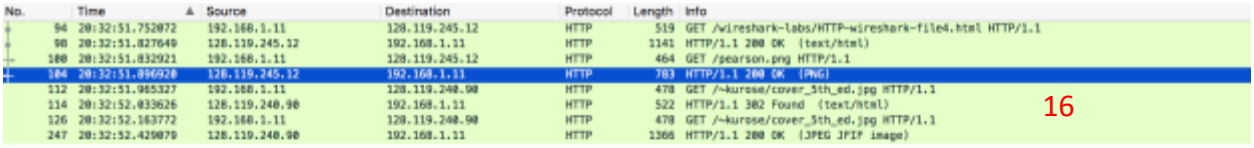
14

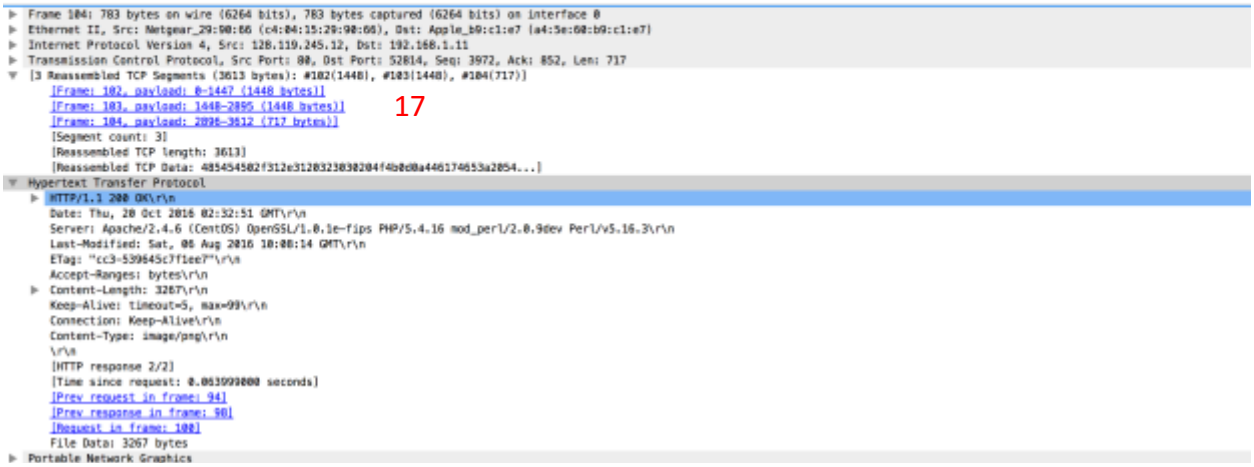
Rob Navarro
CS372

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

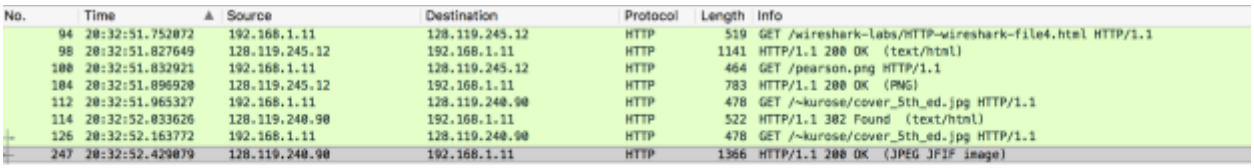
17. **Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.**
    Answer: They were sent serially; you can tell this since the GET requests occur one after another. This is also confirmed since the images were sent over TCP and came from the same port.

Section 4 Screenshots

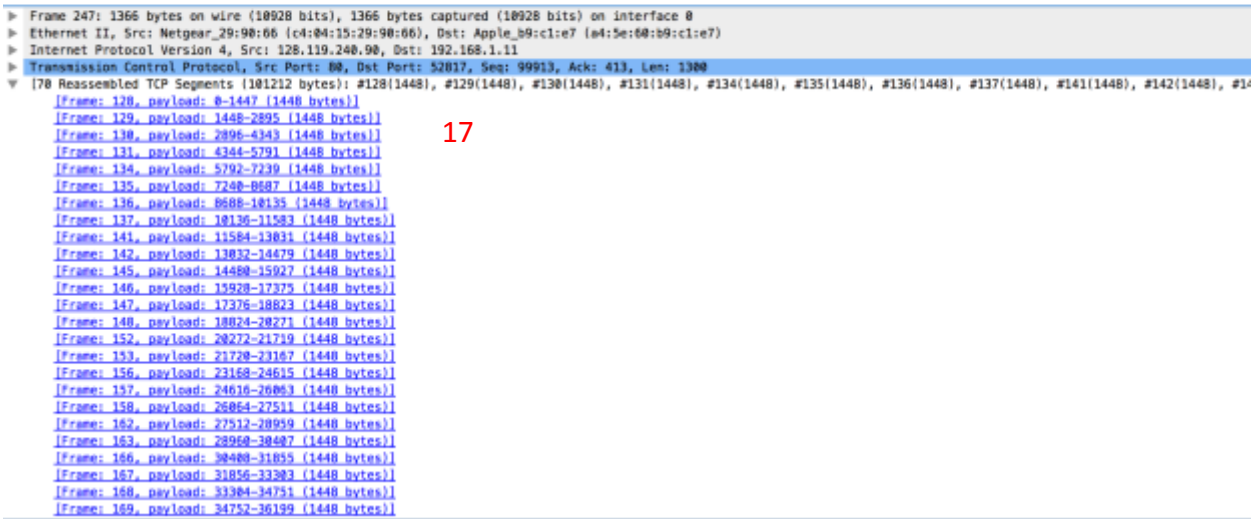




Rob Navarro
CS372

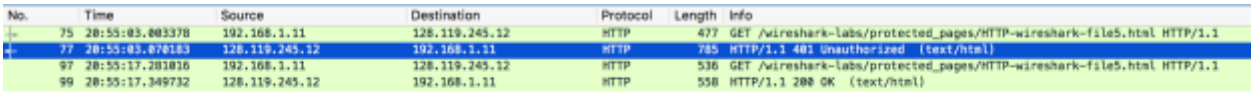


No.	Time	Source	Destination	Protocol	Length	Info
94	20:32:51.752072	192.168.1.11	128.119.245.12	HTTP	519	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
98	20:32:51.827649	128.119.245.12	192.168.1.11	HTTP	1141	HTTP/1.1 200 OK (text/html)
100	20:32:51.832921	192.168.1.11	128.119.245.12	HTTP	464	GET /pearson.png HTTP/1.1
104	20:32:51.896920	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	128.119.240.90	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	20:32:52.429079	128.119.240.90	192.168.1.11	HTTP	1366	HTTP/1.1 200 OK (JPEG JFIF image)

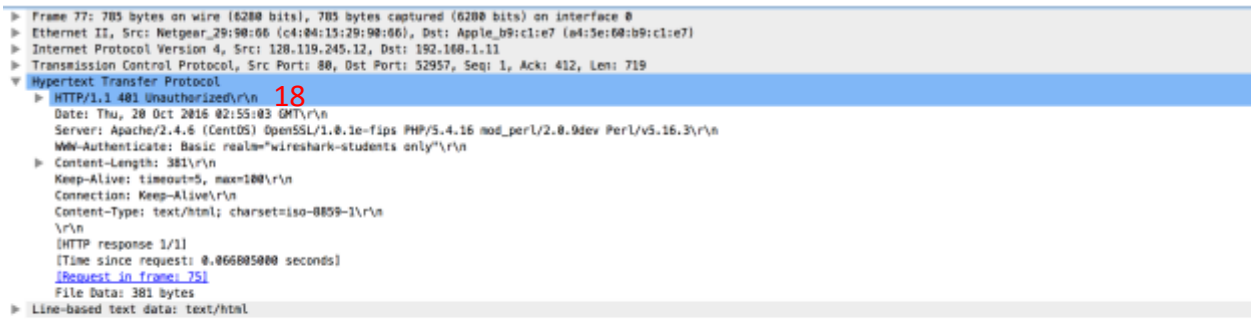


18. **What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?**
    Answer: 401 Unauthorized
19. **When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?**
    Answer: The authorization field was added and has the value Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n

Section 5 Screenshots:

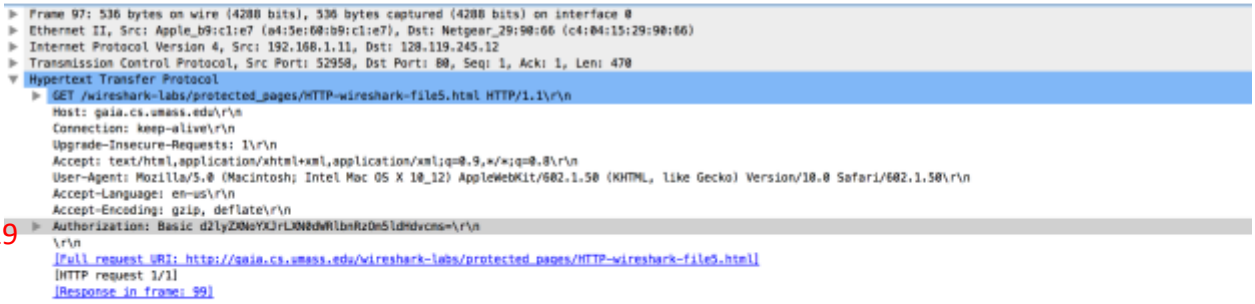


No.	Time	Source	Destination	Protocol	Length	Info
75	20:55:03.003378	192.168.1.11	128.119.245.12	HTTP	477	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
77	20:55:03.070183	128.119.245.12	192.168.1.11	HTTP	785	HTTP/1.1 401 Unauthorized (text/html)
97	20:55:17.281016	192.168.1.11	128.119.245.12	HTTP	536	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
99	20:55:17.349732	128.119.245.12	192.168.1.11	HTTP	550	HTTP/1.1 200 OK (text/html)



Rob Navarro
CS372

No.	Time	Source	Destination	Protocol	Length	Info
75	20:55:03.003378	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	20:55:17.281016	192.168.1.11	128.119.245.12	HTTP	536	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
99	20:55:17.349732	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 (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: 52950, 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
19  ▶ Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\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]
```