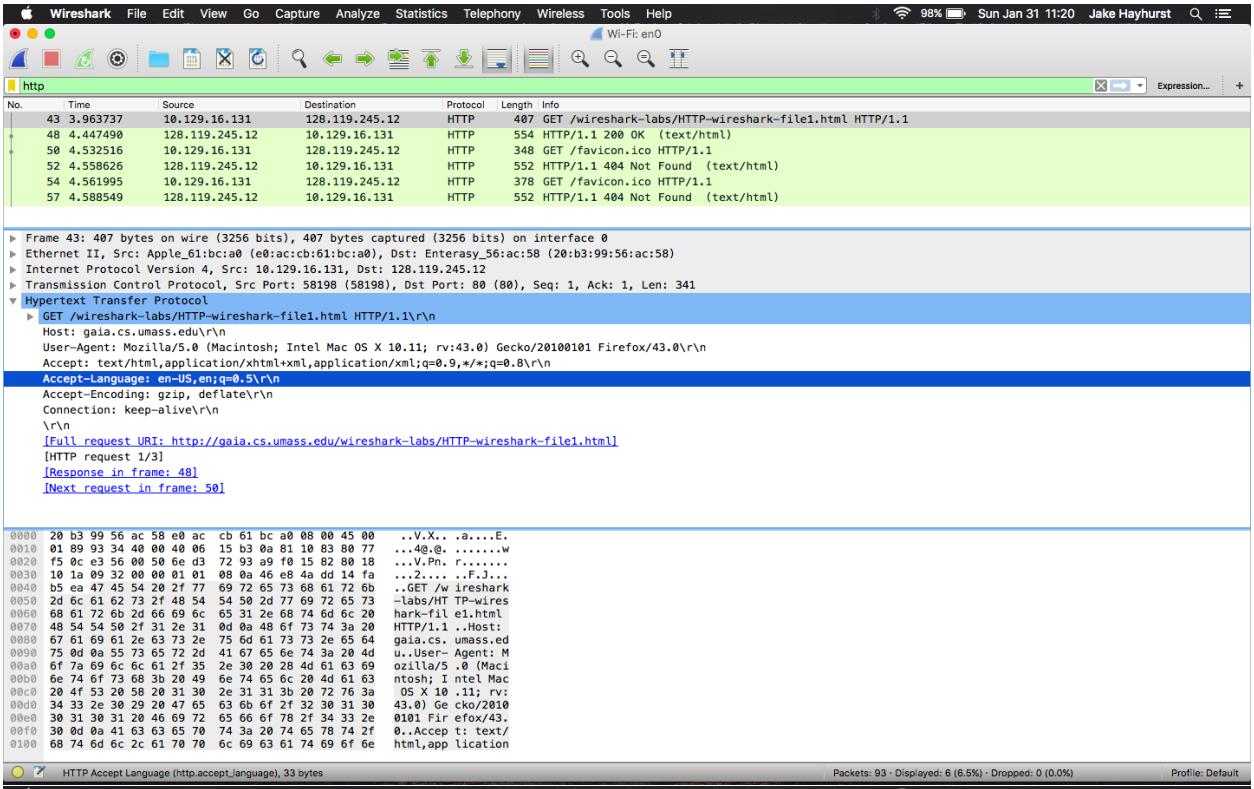
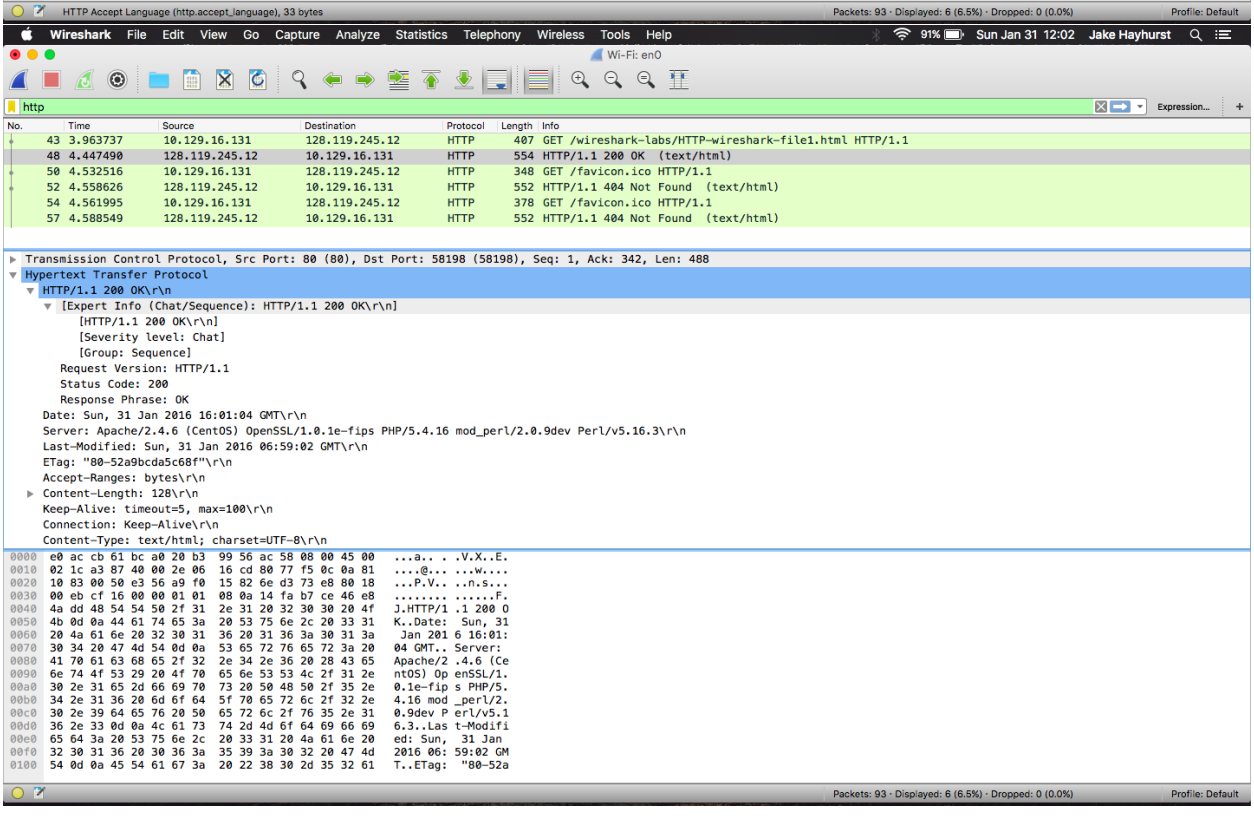
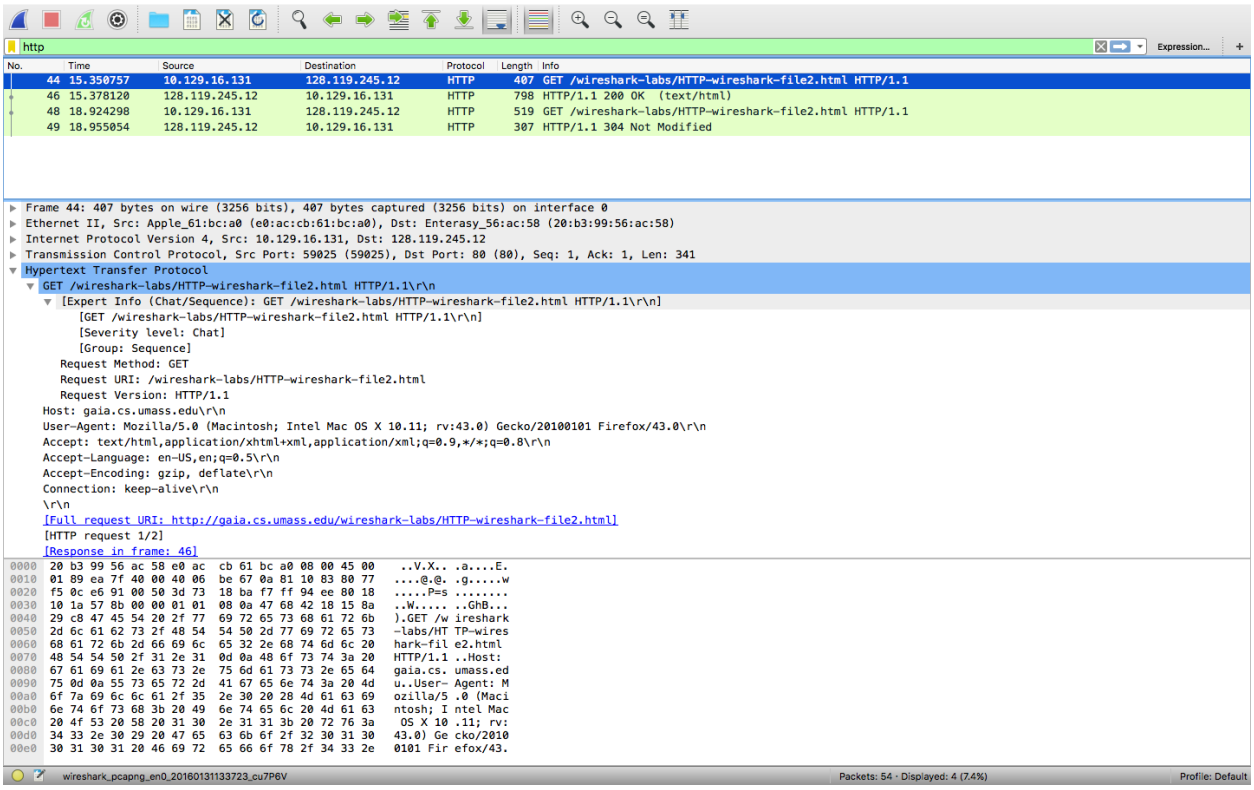
1 The Baisc HTTP GET / Responce Questions

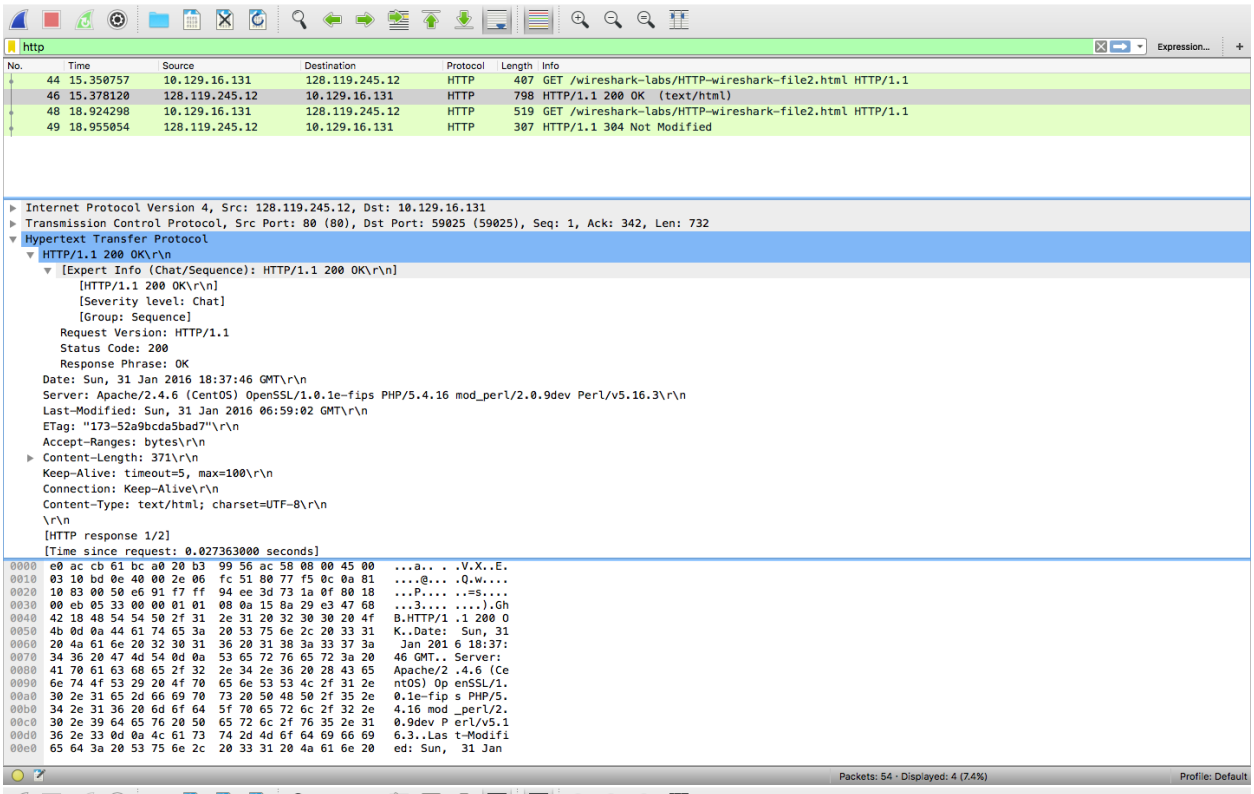


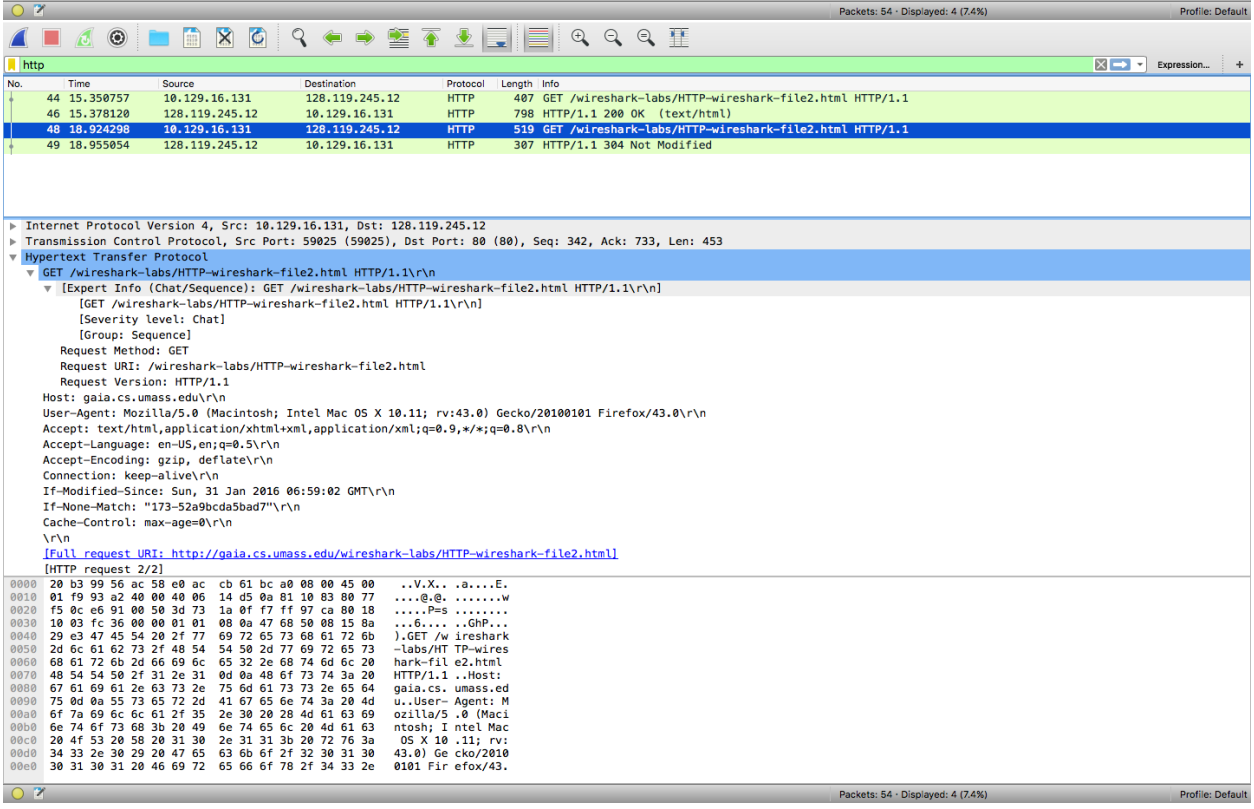


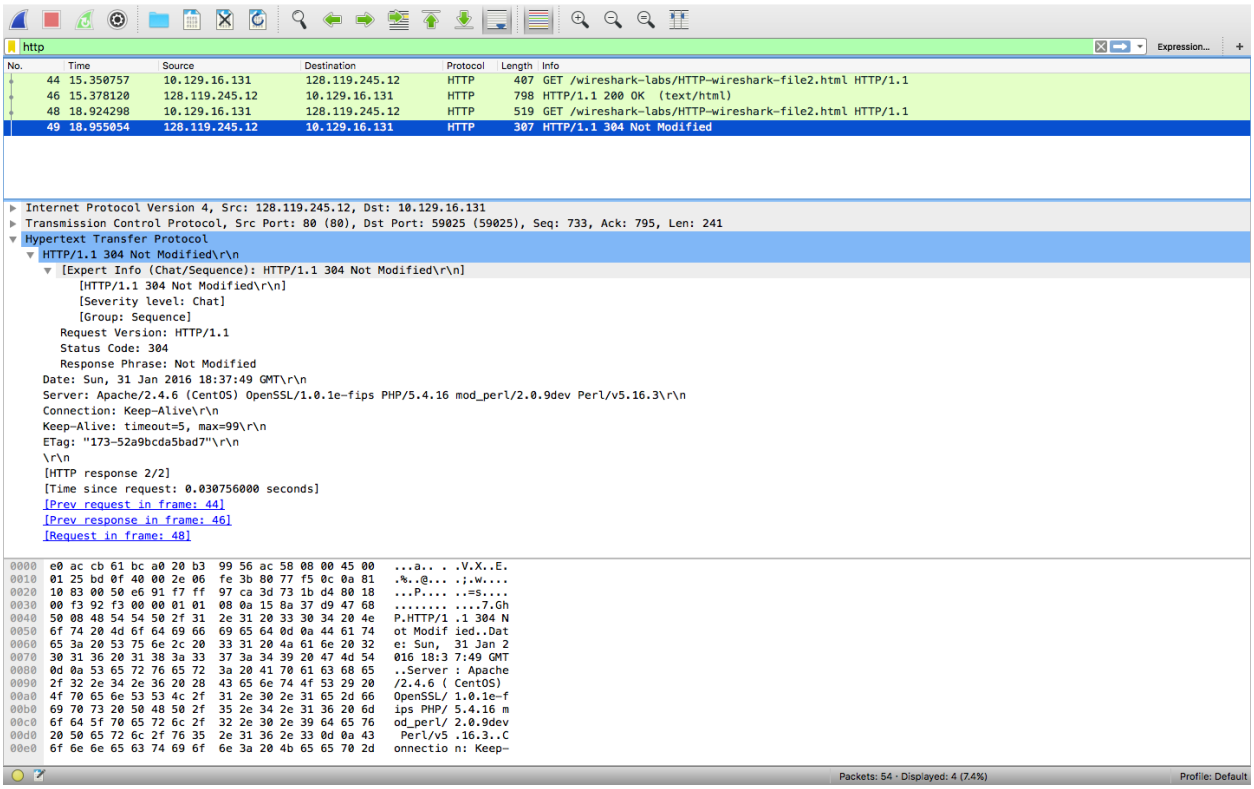
- The browser is running HTTP version 1.1, this can be seen in the GET request in HTTP 1.1; The server is running HTTP 1.1 as the OK response is HTTP 1.1
- The languages that the browser indicate that it can accept en-US or just english text
- The IP address of my computer is 10.129.16.131, this is indicated by the source of the HTTP get request; The IP address of the web server is 128.119.245.12, this is indicated by the destination of the HTTP get request
- The status code returned from the server to the browser is 200, this is seen in the OK response from the server
- The HTML file was last modified on Sunday 31st January 2016 at 6:59:02 GMT this is seen in the HTTP OK response
- The total number of bytes being sent to the computer are 128, this can be seen in the HTTP OK response
- By inspecting the raw data displayed in the packet-listing window I did not see any additional headers

2 The HTTP Conditional Get / Responce Questions



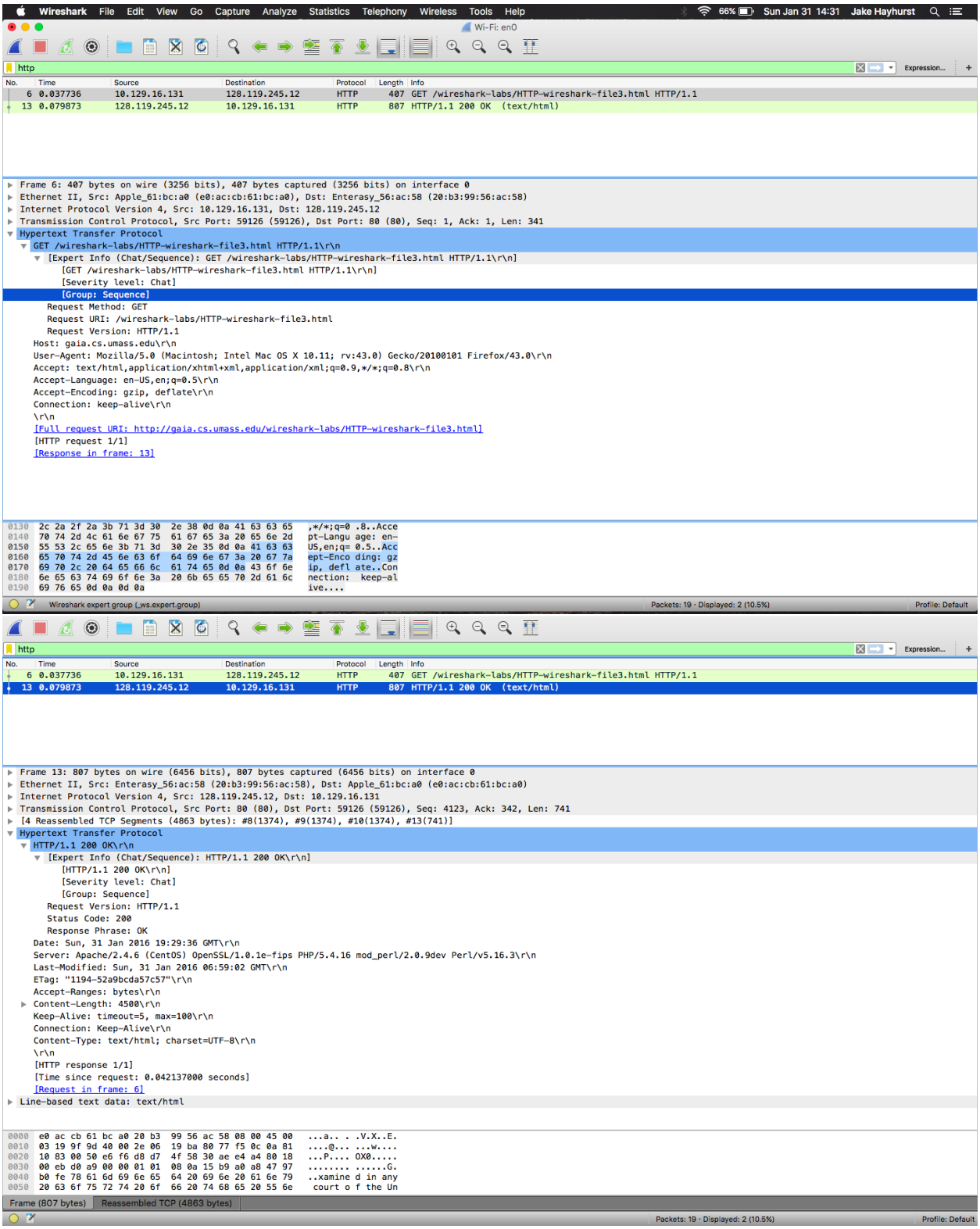

http
Expression...
No. Time Source Destination Protocol Length Info
44 15.350757 10.129.16.131 128.119.245.12 HTTP 407 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
46 15.378120 128.119.245.12 10.129.16.131 HTTP 798 HTTP/1.1 200 OK (text/html)
48 18.924298 10.129.16.131 128.119.245.12 HTTP 519 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
49 18.955054 128.119.245.12 10.129.16.131 HTTP 307 HTTP/1.1 304 Not Modified
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.129.16.131
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 59025 (59025), Seq: 1, Ack: 342, Len: 732
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
[HTTP/1.1 200 OK\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Version: HTTP/1.1
Status Code: 200
Response Phrase: OK
Date: Sun, 31 Jan 2016 18:37:46 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: Sun, 31 Jan 2016 06:59:02 GMT\r\n
ETag: "173-52a9bcda5bad7"\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 1/2]
[Time since request: 0.027363000 seconds]
0000 e0 ac cb 61 bc a0 20 b3 99 56 ac 58 08 00 45 00 ...a.. . .V.X..E.
0010 03 10 bd 0e 40 00 2e 06 fc 51 80 77 f5 0c 0a 81 ....@... .Q.w....
0020 10 83 00 50 e6 91 f7 ff 94 ee 3d 73 1a 0f 80 18 ...P.... ..=s....
0030 00 eb 05 33 00 00 01 01 08 0a 15 8a 29 e3 47 68 ...3.... ....).Gh
0040 42 18 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f B.HTTP/1 .1 200 O
0050 4b 0d 0a 44 61 74 65 3a 20 53 75 6e 2c 20 33 31 K..Date: Sun, 31
0060 20 4a 61 6e 20 32 30 31 36 20 31 38 3a 33 37 3a Jan 201 6 18:37:
0070 34 36 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 46 GMT.. Server:
0080 41 70 61 63 68 65 2f 32 2e 34 2e 36 20 28 43 65 Apache/2 .4.6 (Ce
0090 6e 74 4f 53 29 20 4f 70 65 6e 53 53 4c 2f 31 2e ntOS) Op enSSL/1.
00a0 30 2e 31 65 2d 66 69 70 73 20 50 48 50 2f 35 2e 0.1e-fip s PHP/5.
00b0 34 2e 31 36 20 6d 6f 64 5f 70 65 72 6c 2f 32 2e 4.16 mod _perl/2.
00c0 30 2e 39 64 65 76 20 50 65 72 6c 2f 76 35 2e 31 0.9dev P erl/v5.1
00d0 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 6.3..Las t-Modifi
00e0 65 64 3a 20 53 75 6e 2c 20 33 31 20 4a 61 6e 20 ed: Sun, 31 Jan
Packets: 54 · Displayed: 4 (7.4%)
Profile: Default

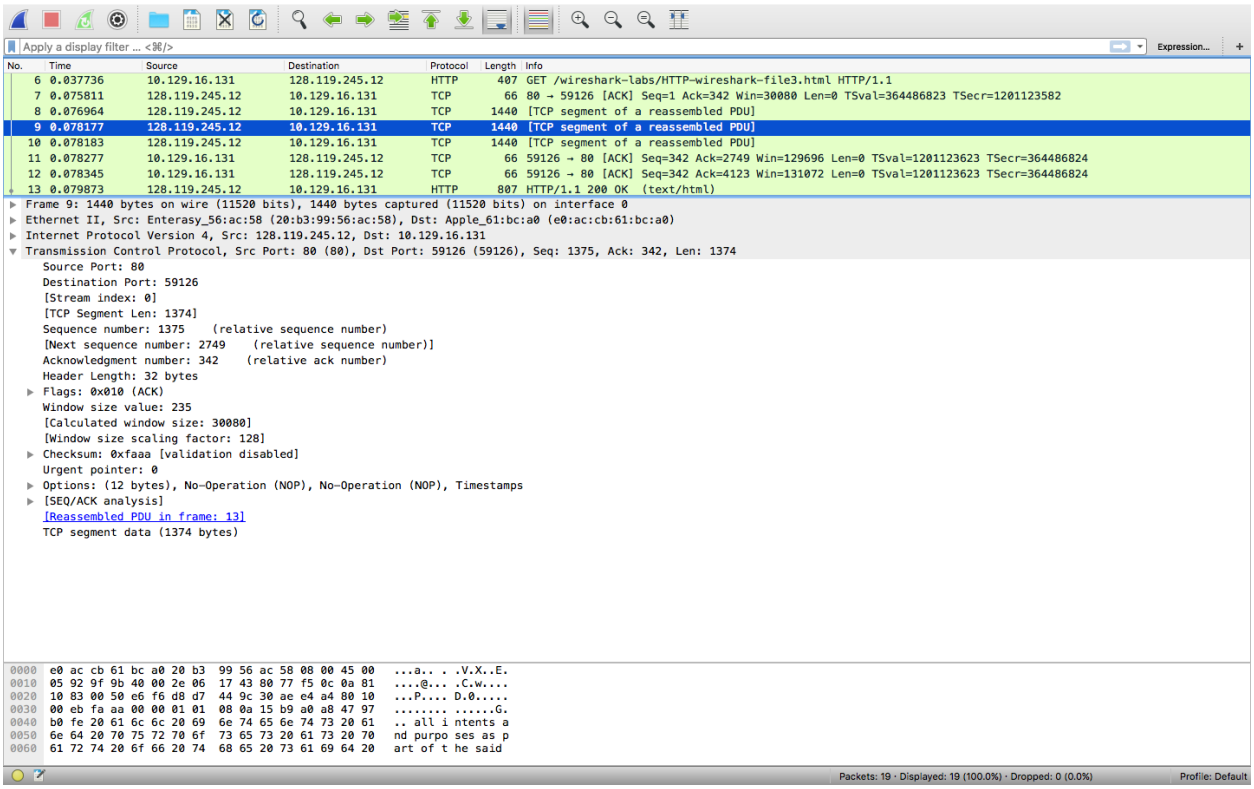

http
Expression...
No. Time Source Destination Protocol Length Info
44 15.350757 10.129.16.131 128.119.245.12 HTTP 407 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
46 15.378120 128.119.245.12 10.129.16.131 HTTP 798 HTTP/1.1 200 OK (text/html)
48 18.924298 10.129.16.131 128.119.245.12 HTTP 519 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
49 18.955054 128.119.245.12 10.129.16.131 HTTP 307 HTTP/1.1 304 Not Modified
Internet Protocol Version 4, Src: 10.129.16.131, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 59025 (59025), Dst Port: 80 (80), Seq: 342, Ack: 733, 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]
[GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
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 (Macintosh; Intel Mac OS X 10.11; rv:43.0) Gecko/20100101 Firefox/43.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
If-Modified-Since: Sun, 31 Jan 2016 06:59:02 GMT\r\n
If-None-Match: "173-52a9bcda5bad7"\r\n
Cache-Control: max-age=0\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 2/2]
0000 20 b3 99 56 ac 58 e0 ac cb 61 bc a0 08 00 45 00 ..V.X.. .a....E.
0010 01 f9 93 a2 40 00 40 06 14 d5 0a 81 10 83 80 77 ....@.@. ....w
0020 f5 0c e6 91 00 50 3d 73 1a 0f f7 ff 97 ca 80 18 .....P=s ....
0030 10 03 fc 36 00 00 01 01 08 0a 47 68 50 08 15 8a ...6.... ..GhP...
0040 29 e3 47 45 54 20 2f 77 69 72 65 73 68 61 72 6b).GET /w ireshark
0050 2d 6c 61 62 73 2f 48 54 54 50 2d 77 69 72 65 73 -labs/HT TP-wires
0060 68 61 72 6b 2d 66 69 6c 65 32 2e 68 74 6d 6c 20 hark-fil e2.html
0070 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 HTTP/1.1 ..Host:
0080 67 61 69 61 2e 63 73 2e 75 6d 61 73 73 2e 65 64 gaia.cs. umass.ed
0090 75 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d u..User- Agent: M
00a0 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 4d 61 63 69 ozilla/5 .0 (Maci
00b0 6e 74 6f 73 68 3b 20 49 6e 74 65 6c 20 4d 61 63 ntosh; I ntel Mac
00c0 20 4f 53 20 58 20 31 30 2e 31 31 3b 20 72 76 3a OS X 10 .11; rv:
00d0 34 33 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 30 43.0) Ge cko/2010
00e0 30 31 30 31 20 46 69 72 65 66 6f 78 2f 34 33 2e 0101 Fir efox/43.
Packets: 54 · Displayed: 4 (7.4%)
Profile: Default



- In the first contents of the HTTP GET request from the browser there is not an IF-MODIFIED-SINCE line in the packet
- The server explicitly returned a file, this can be seen in the HTTP OK responce since the server sent a packet of length 371 bytes
- The second contents of the HTTP GET request from the browser there is an IF-MODIFIED-SINCE line in the packet. The information that follows the IF-MODIFIED-SINCE header is : Sun, 31 Jan 2016 06:59:02 GMT
- The status code and phrase of the responce to the second HTTP Get is 304 Not Modified. The server did not explicitly return the contents of the file as it did not send anything other than headder information in the packet

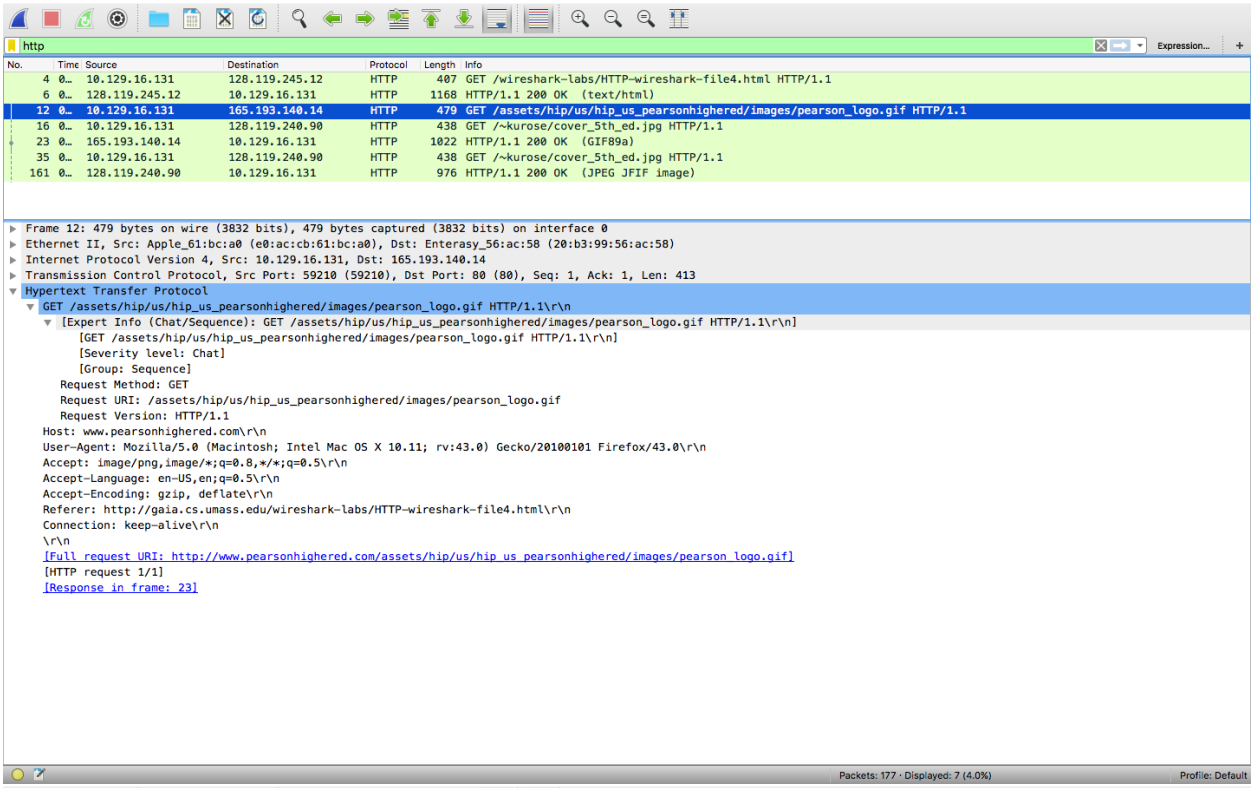
3 Retrieving Long Documents Questions

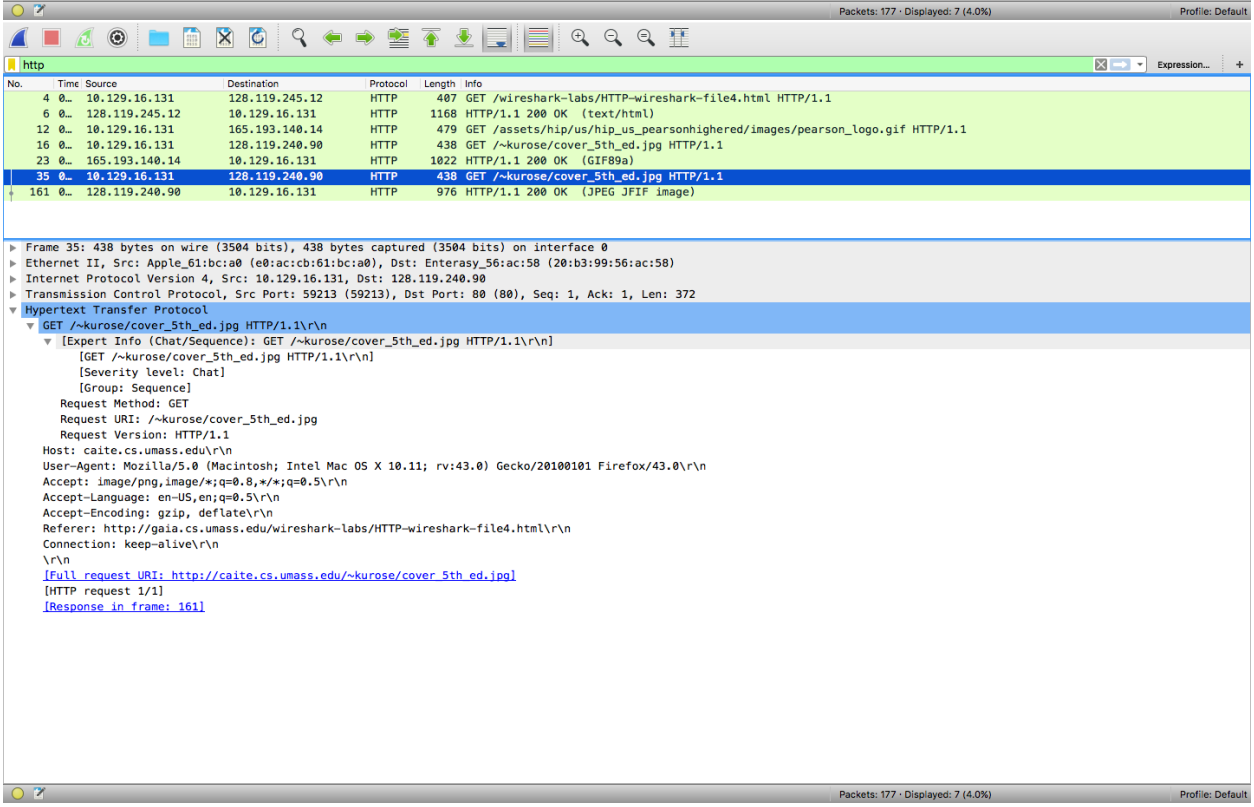




- The browser only sent one HTTP GET request. The packet number that contains the GET message is 6.
- The packet number that contains the status code and trace for the HTTP GET request was 13
- The status code and phrase in the HTTP GET responce was 200 OK
- The amount of TCP segments needed to carry the single HTTP responce and the text of the bill of rights were 3 segments at 1374 bytes per TCP segment

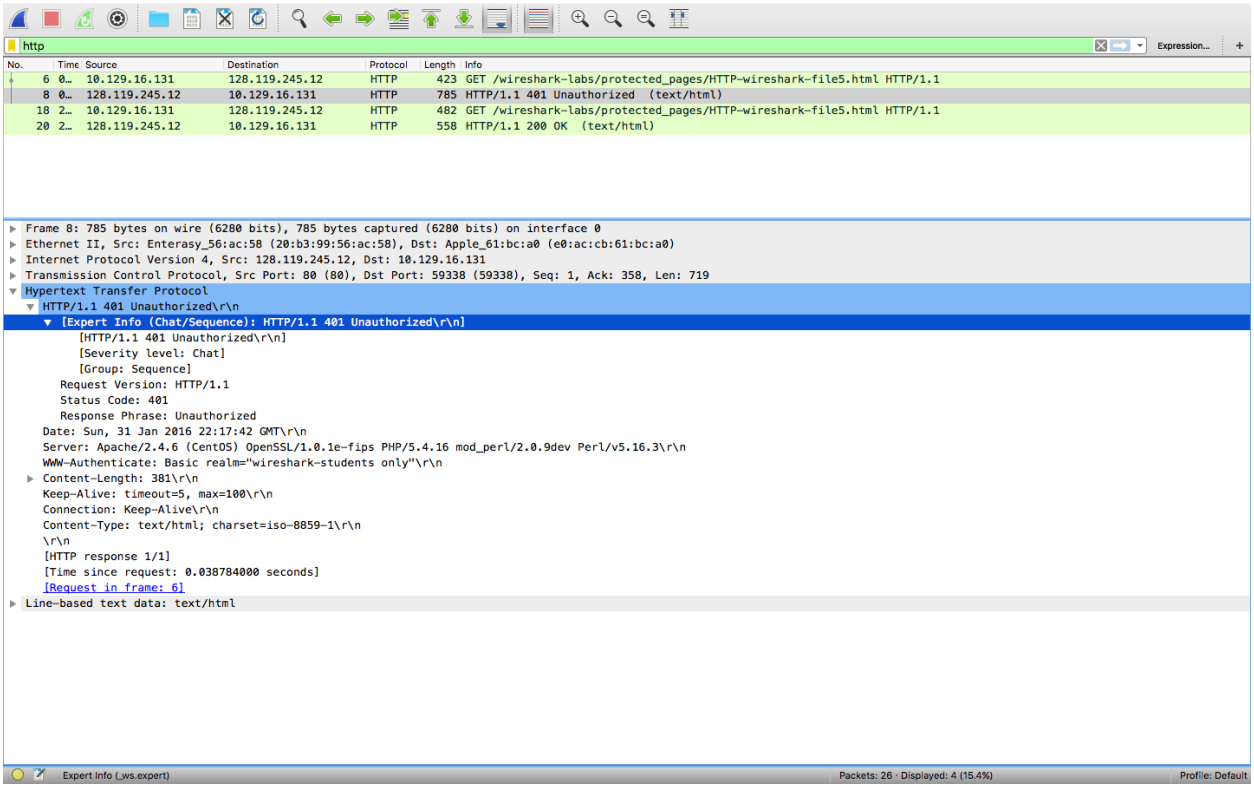
4 HTML Documents with Embedded Objects Questions

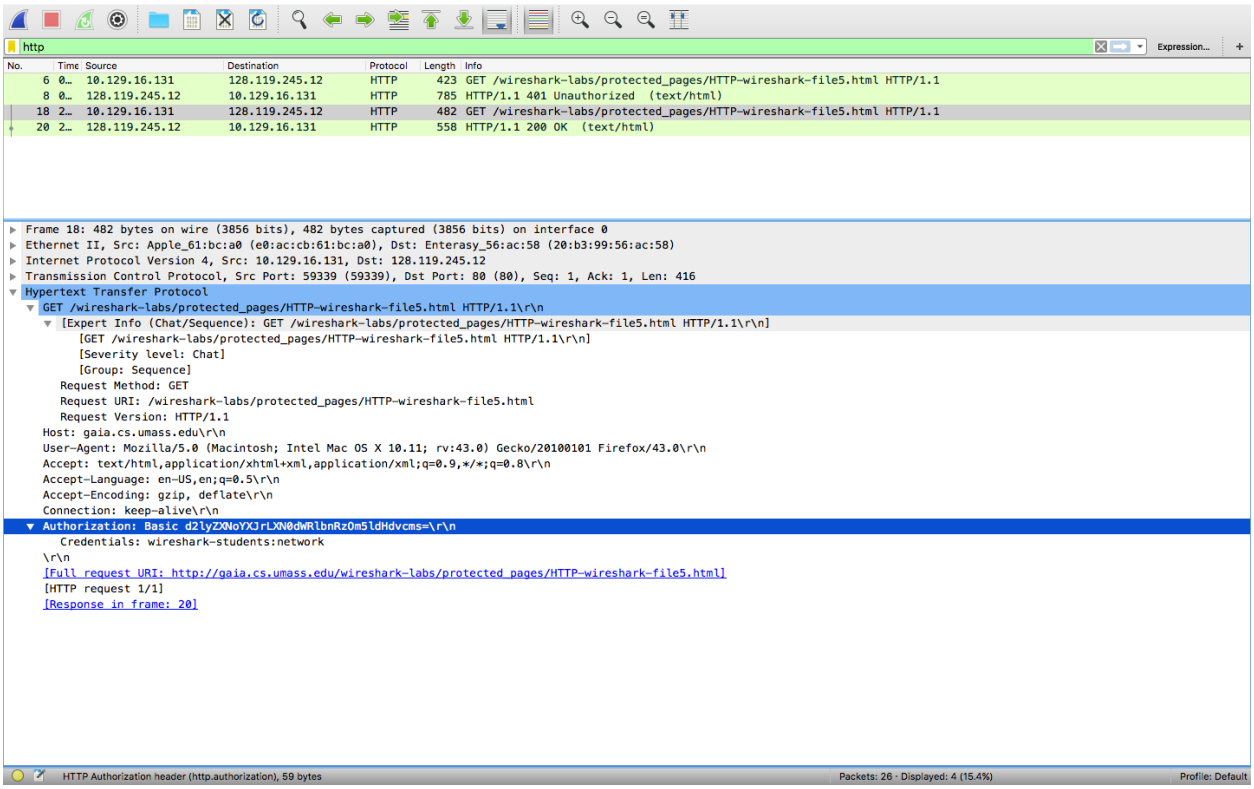




- There were a total of 4 HTTP GET requests from the browser. These Get requests were to gaia.cs.umass.edu, www.pearsonhighered.com, manic.cs.umass.edu/, caite.cs.umass.edu/
- The browser appeared to download the images in parallel as there were two GET requests and then a responce from the server

5 HTTP Authentication Questions





- The servers responce to the first HTTP GET is 401 Unauthorized
- With the second HTTP GET request from the browser the new field in the message is Authorization with the username and password displayed