

1 The Basic HTTP GET / Response Questions

The image shows two screenshots of the Wireshark network protocol analyzer. The top screenshot displays a packet capture of an HTTP GET request from 10.129.16.131 to 10.129.245.12. The packet details pane shows the Hypertext Transfer Protocol section with fields like Host, User-Agent, and Accept. The packet bytes pane shows the raw data in hexadecimal and ASCII. The bottom screenshot shows the same capture with the packet details pane expanded to show the HTTP response status code 200 OK and various response headers like Date, Server, and Content-Type.

Wireshark Packet Capture Details:

Packet 43: GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

Packet 48: 200 OK (text/html)

Packet 50: GET /favicon.ico HTTP/1.1

Packet 52: 404 Not Found (text/html)

Packet 54: GET /favicon.ico HTTP/1.1

Packet 57: 404 Not Found (text/html)

HTTP Request Details:

- Host: gaia.cs.umass.edu
- User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:43.0) Gecko/20100101 Firefox/43.0
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
- Accept-Language: en-US,en;q=0.5
- Accept-Encoding: gzip, deflate
- Connection: keep-alive
- Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html

HTTP Response Details:

- Status: 200 OK
- Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3
- Content-Type: text/html; charset=UTF-8

- 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 / Response Questions

The image shows a Wireshark packet capture of an HTTP transaction. The packet list at the top shows four packets: a GET request (44), a 200 OK response (46), and two subsequent GET requests (48 and 49). The packet details pane for packet 44 shows the full request structure, including the request line, headers, and body. The packet bytes pane shows the raw data of the request and response.

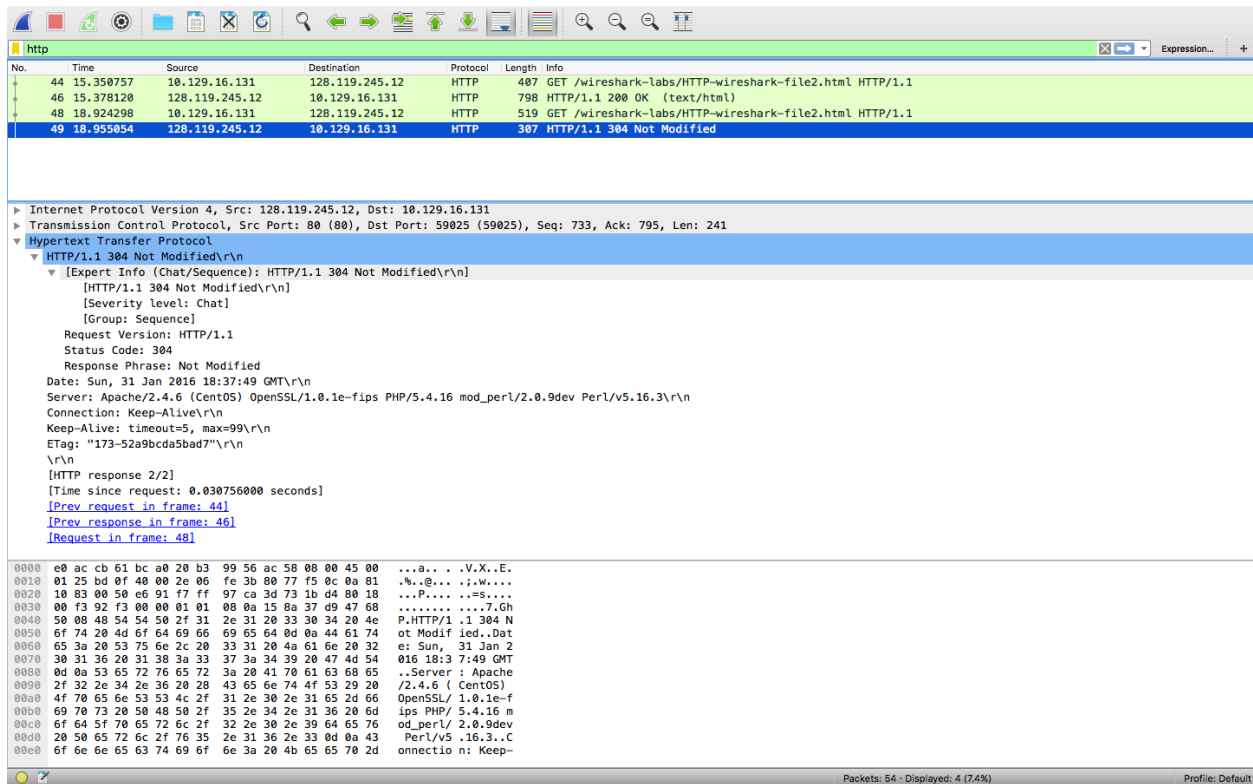
No.	Time	Source	Destination	Protocol	Length	Info
44	15.350757	10.129.16.131	128.119.245.12	HTTP	407	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
46	15.378120	128.119.245.12	10.129.16.131	HTTP	798	HTTP/1.1 200 OK (text/html)
48	18.924298	10.129.16.131	128.119.245.12	HTTP	519	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
49	18.955854	128.119.245.12	10.129.16.131	HTTP	307	HTTP/1.1 304 Not Modified

Frame 44: 407 bytes on wire (3256 bits), 407 bytes captured (3256 bits) on interface 0
 Ethernet II, Src: Apple_GigabitEthernet0 (e0:ac:cb:61:bc:a0), Dst: Enterasys_56:ac:58 (20:b3:99:56:ac:58)
 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: 1, Ack: 1, Len: 341

▼ 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
 \r\n
 [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
 [HTTP request 1/2]
 [Response in frame: 46]

0000 20 b3 99 56 ac 58 e0 ac cb 61 bc a0 00 00 45 00 ..V.X..a....E.
 0010 01 89 ea 7f 40 00 40 06 be 67 0a 81 10 83 80 77@. .g.....w
 0020 f5 0c e6 91 00 50 3d 73 18 ba f7 ff 94 ee 80 18P=s
 0030 10 1a 57 8b 00 00 01 01 00 0a 47 68 42 18 15 8a ..W.... .GhB...
 0040 29 c8 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 50 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.

3



- 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 response 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 response 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 header information in the packet

3 Retrieving Long Documents Questions

The image displays two screenshots of the Wireshark network protocol analyzer. The top screenshot shows the initial capture of an HTTP GET request (Frame 6) from 10.129.16.131 to 128.119.245.12. The bottom screenshot shows the corresponding HTTP 200 OK response (Frame 13) from 128.119.245.12 back to 10.129.16.131.

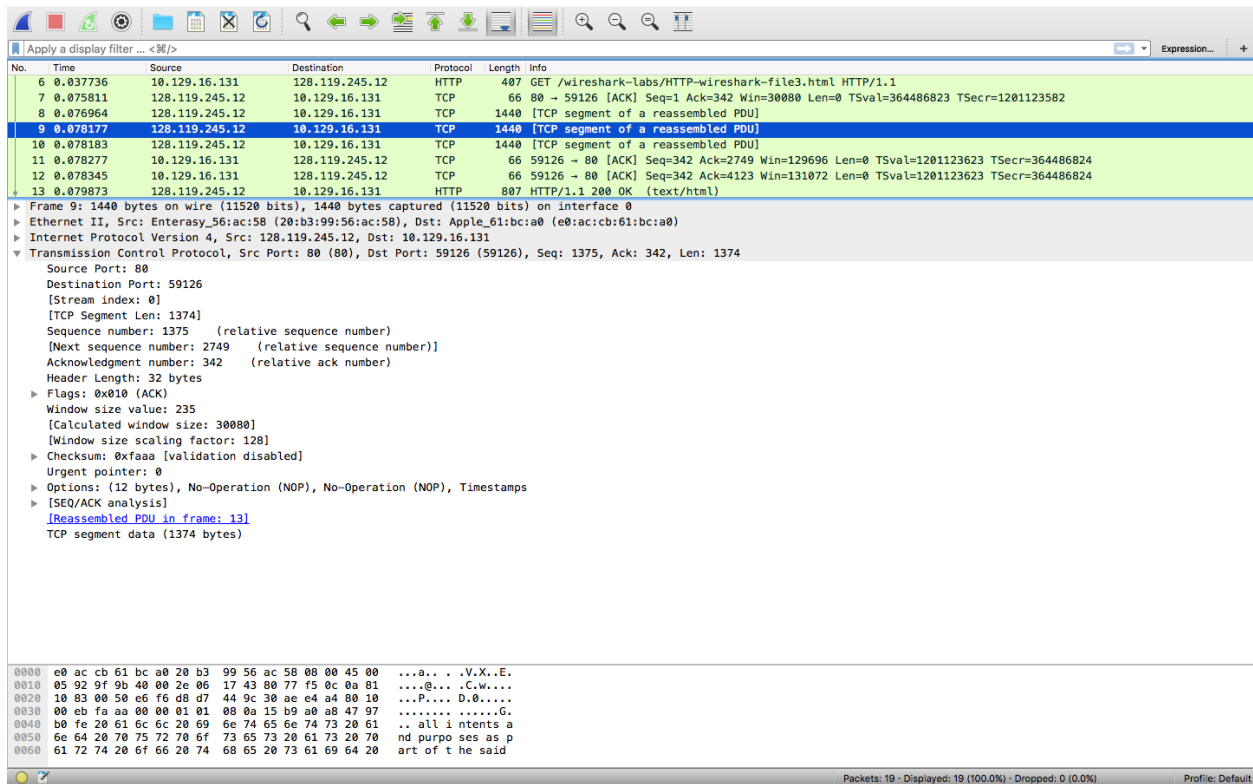
Frame 6: 407 bytes on wire (3256 bits), 407 bytes captured (3256 bits) on interface 0

- Ethernet II, Src: Apple_61:bc:a0 (e0:ac:cb:61:bc:a0), Dst: Enterasy_56:ac:58 (20:b3:99:56:ac:58)
- Internet Protocol Version 4, Src: 10.129.16.131, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 59126 (59126), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 341
- Hypertext Transfer Protocol
 - GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
 - [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]
 - [GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]
 - [Severity level: Chat]
 - [Group: Sequence]
 - Request Method: GET
 - Request URI: /wireshark-labs/HTTP-wireshark-file3.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
 - \r\n
 - [Full request URI: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html>]
 - [HTTP request 1/1]
 - [Response in frame: 13]

Frame 13: 807 bytes on wire (6456 bits), 807 bytes captured (6456 bits) on interface 0

- Ethernet II, Src: Enterasy_56:ac:58 (20:b3:99:56:ac:58), Dst: Apple_61:bc:a0 (e0:ac:cb:61:bc:a0)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.129.16.131
- Transmission Control Protocol, Src Port: 80 (80), Dst Port: 59126 (59126), Seq: 4123, Ack: 342, Len: 741
- [4 Reassembled TCP Segments (4863 bytes): #8(1374), #9(1374), #10(1374), #13(741)]
- 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 19:29:36 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: "1194-52a9bcd57c57"\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: 0.042137000 seconds]
 - [Request in frame: 6]
- Line-based text data: text/html

Frame (807 bytes) Reassembled TCP (4863 bytes)



- 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 response was 200 OK
- The amount of TCP segments needed to carry the single HTTP response and the text of the bill of rights were 3 segments at 1374 bytes per TCP segment

4 HTML Documents with Embedded Objects Questions

The image displays two screenshots of the Wireshark network protocol analyzer. The top screenshot shows a packet capture of an HTTP session. The packet list pane highlights packet 12, which is a GET request for `/assets/hip/us/hip_us_pearsonhighered/images/pearson_logo.gif`. The packet details pane shows the full request, including the URI, headers, and the request body. The bottom screenshot shows a similar packet capture, but with packet 35 highlighted, which is a GET request for `~/kurose/cover_5th_ed.jpg`. The packet details pane shows the full request, including the URI, headers, and the request body.

Wireshark Packet Capture 1 (Top):

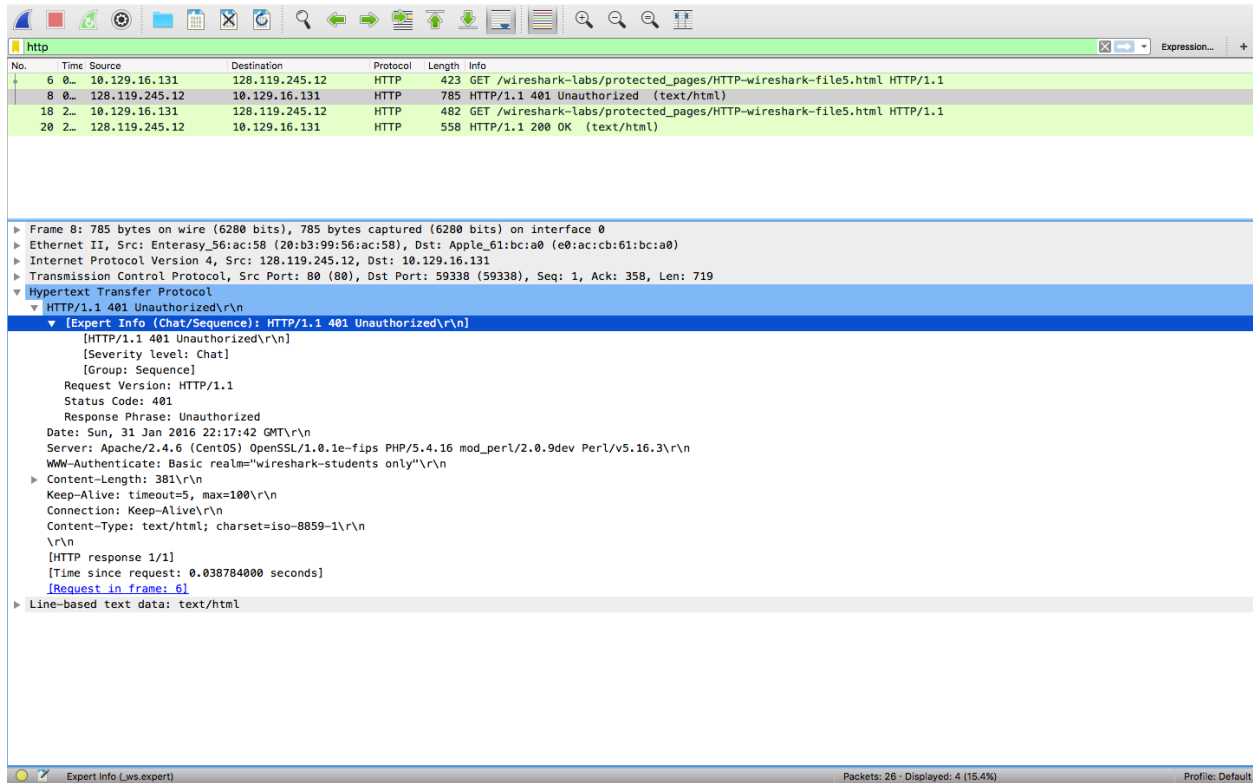
No.	Time	Source	Destination	Protocol	Length	Info
4	0.000000	10.129.16.131	128.119.245.12	HTTP	407	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
6	0.000000	128.119.245.12	10.129.16.131	HTTP	1168	HTTP/1.1 200 OK (text/html)
12	0.000000	10.129.16.131	165.193.140.14	HTTP	479	GET /assets/hip/us/hip_us_pearsonhighered/images/pearson_logo.gif HTTP/1.1
16	0.000000	10.129.16.131	128.119.240.90	HTTP	438	GET ~/kurose/cover_5th_ed.jpg HTTP/1.1
23	0.000000	165.193.140.14	10.129.16.131	HTTP	1022	HTTP/1.1 200 OK (GIF89a)
35	0.000000	10.129.16.131	128.119.240.90	HTTP	438	GET ~/kurose/cover_5th_ed.jpg HTTP/1.1
161	0.000000	128.119.240.90	10.129.16.131	HTTP	976	HTTP/1.1 200 OK (JPEG JFIF image)

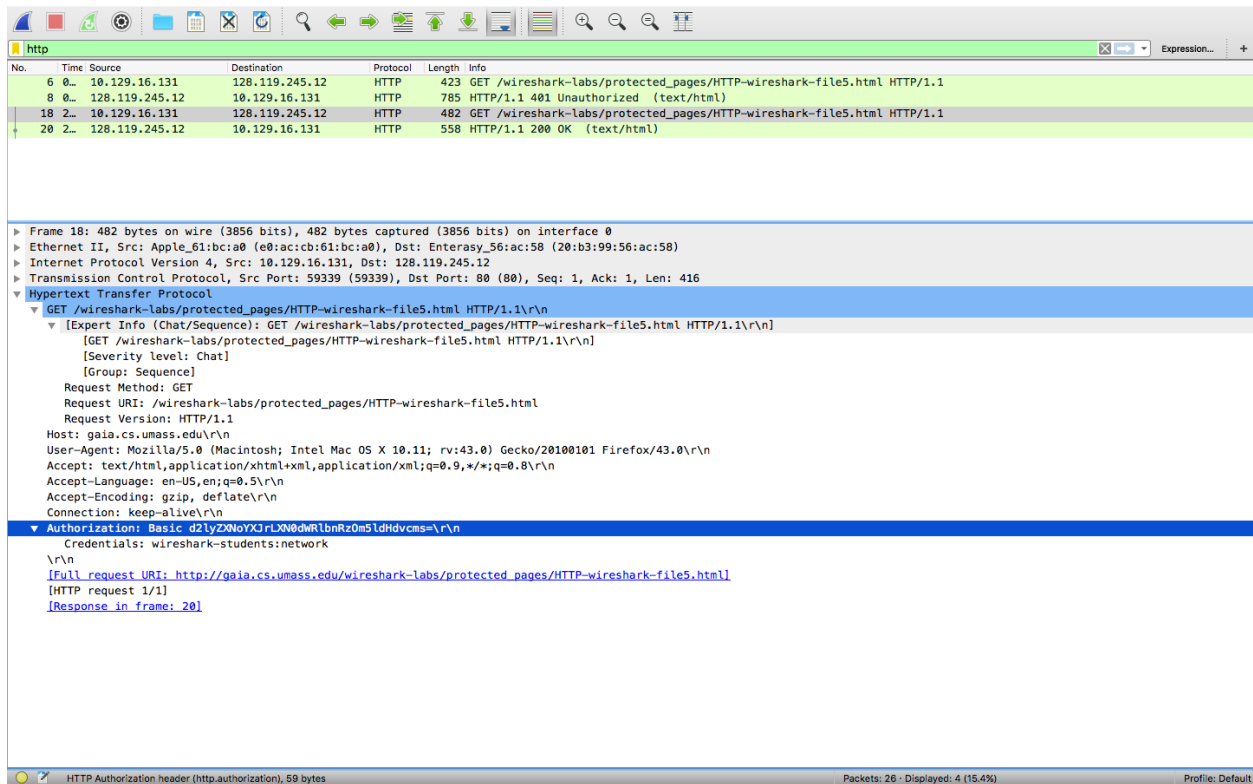
Wireshark Packet Capture 2 (Bottom):

No.	Time	Source	Destination	Protocol	Length	Info
4	0.000000	10.129.16.131	128.119.245.12	HTTP	407	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
6	0.000000	128.119.245.12	10.129.16.131	HTTP	1168	HTTP/1.1 200 OK (text/html)
12	0.000000	10.129.16.131	165.193.140.14	HTTP	479	GET /assets/hip/us/hip_us_pearsonhighered/images/pearson_logo.gif HTTP/1.1
16	0.000000	10.129.16.131	128.119.240.90	HTTP	438	GET ~/kurose/cover_5th_ed.jpg HTTP/1.1
23	0.000000	165.193.140.14	10.129.16.131	HTTP	1022	HTTP/1.1 200 OK (GIF89a)
35	0.000000	10.129.16.131	128.119.240.90	HTTP	438	GET ~/kurose/cover_5th_ed.jpg HTTP/1.1
161	0.000000	128.119.240.90	10.129.16.131	HTTP	976	HTTP/1.1 200 OK (JPEG JFIF image)

- 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 response from the server

5 HTTP Authentication Questions





- The server's response 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