Tony Gao
CS453
HW3, Lab 2

Problem 1:

```
/var/folders/09/r5pnxj9j7nv5wg5744rrw2840000gn/T//
wireshark_en0_20180211235311_pLgII7.pcapng 271 total packets, 2 shown
```

Request:

```
    78 3.034957       192.168.1.20          128.119.245.12        HTTP     602    GET /
wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
Frame 78: 602 bytes on wire (4816 bits), 602 bytes captured (4816 bits) on interface 0
Ethernet II, Src: Apple_10:41:06 (80:e6:50:10:41:06), Dst: AsustekC_3f:90:60 (74:d0:2b:3f:
90:60)
Internet Protocol Version 4, Src: 192.168.1.20, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 53814, Dst Port: 80, Seq: 1, Ack: 1, Len: 536
Hypertext Transfer Protocol
   GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
      [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/
1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.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_13_2) AppleWebKit/537.36
(KHTML, like
Gecko) Chrome/63.0.3239.84 Safari/537.36\r\n
   Upgrade-Insecure-Requests: 1\r\n
   Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
*;q=0.8\r\n
   DNT: 1\r\n
   Accept-Encoding: gzip, deflate\r\n
   Accept-Language: en-US,en;q=0.9\r\n
   Cookie: __unam=9514ce4-1613a14b9fc-6188e86c-8;
SESSIONIDMOODLE=2bb7b2175c5885e21c0a6cdefe65c41b\r\n
   \r\n
   [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
   [HTTP request 1/1]
   [Response in frame: 81]
```

Response:

```
    81 3.058911       128.119.245.12        192.168.1.20          HTTP     552    HTTP/1.1 200
OK  (text/html)
Frame 81: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface 0
Ethernet II, Src: AsustekC_3f:90:60 (74:d0:2b:3f:90:60), Dst: Apple_10:41:06
(80:e6:50:10:41:06)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.20
Transmission Control Protocol, Src Port: 80, Dst Port: 53814, Seq: 1, Ack: 537, Len: 486
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
      [Status Code Description: OK]
      Response Phrase: OK
   Date: Mon, 12 Feb 2018 04:53:15 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\r\n
   Last-Modified: Sun, 11 Feb 2018 06:59:01 GMT\r\n
   ETag: "80-564ea4bd7c777"\r\n
   Accept-Ranges: bytes\r\n
   Content-Length: 128\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: 0.023954000 seconds]
   [Request in frame: 78]
   File Data: 128 bytes
Line-based text data: text/html
   <html>\n
   Congratulations.  You've downloaded the file \n
   http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
   </html>\n
```

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
   My browser is running HTTP 1.1 indicated by the HTTP/1.1 after the GET. The server is

running HTTP 1.1 indicated by the tag in the response.

2. What languages (if any) does your browser indicate that it can accept to the server? Text/Html, Application/XHTML+XML, APPLICATION/XML with q preference weight .9, image/webp, image/apng, and everything else with preference weight .8.
3. What is the IP address of your computer? Of the gaia.cs.umass.edu server? My computer is 192.168.1.20 indicated by the source ip field in the request. The Umass server is 128.119.245.12 indicated by the destination ip field in the request.
4. What is the status code returned from the server to your browser? 200 OK. This is seen in the response.
5. When was the HTML file that you are retrieving last modified at the server? 2/11/2018 at 06:59:01 GMT. This is seen in the last-modified header of the response.
6. How many bytes of content are being returned to your browser? 128 bytes, seen in the content-length header of the response.
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. All of the raw data headers resolve to list items in the packet content window. By going through the raw data and clicking on the beginning of each header, I see that all of the headers are parsed into the packet display window.

Problem 2:

/var/folders/09/r5pnxj9j7nv5wg5744rrw2840000gn/T//
wireshark_en0_20180212001233_qstIpS.pcapng 1398 total packets, 6 shown

Request 1:

```
    56 3.231640       192.168.1.20          128.119.245.12        HTTP     437    GET /
wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Frame 56: 437 bytes on wire (3496 bits), 437 bytes captured (3496 bits) on interface 0
Ethernet II, Src: Apple_10:41:06 (80:e6:50:10:41:06), Dst: AsustekC_3f:90:60 (74:d0:2b:3f:
90:60)
Internet Protocol Version 4, Src: 192.168.1.20, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 53917, Dst Port: 80, Seq: 1, Ack: 1, Len: 371
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
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:56.0) Gecko/20100101
Firefox/
56.0\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
    Upgrade-Insecure-Requests: 1\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: 58]
    [Next request in frame: 67]
```

Response 1:

```
     58 3.256686       128.119.245.12        192.168.1.20          HTTP     796    HTTP/1.1 200
OK  (text/html)
Frame 58: 796 bytes on wire (6368 bits), 796 bytes captured (6368 bits) on interface 0
Ethernet II, Src: AsustekC_3f:90:60 (74:d0:2b:3f:90:60), Dst: Apple_10:41:06
(80:e6:50:10:41:06)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.20
Transmission Control Protocol, Src Port: 80, Dst Port: 53917, Seq: 1, Ack: 372, Len: 730
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
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Mon, 12 Feb 2018 05:12:36 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\r\n
    Last-Modified: Sun, 11 Feb 2018 06:59:01 GMT\r\n
    ETag: "173-564ea4bd7c38f"\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: 0.025046000 seconds]
    [Request in frame: 56]
    [Next request in frame: 67]
    [Next response in frame: 69]
    File Data: 371 bytes
Line-based text data: text/html
    \n
    <html>\n
    \n
    Congratulations again!  Now you've downloaded the file lab2-2.html. <br>\n
    This file's last modification date will not change.  <p>\n
    Thus  if you download this multiple times on your browser, a complete copy <br>\n
    will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
/var/folders/09/r5pnxj9j7nv5wg5744rrw2840000gn/T//
wireshark_en0_20180212001233_qstIpS.pcapng 1400 total packets, 6 shown

    field in your browser's HTTP GET request to the server.\n
    \n
    </html>\n
```

Request 2:

```
    462 14.714944      192.168.1.20          128.119.245.12        HTTP     549    GET /
wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Frame 462: 549 bytes on wire (4392 bits), 549 bytes captured (4392 bits) on interface 0
Ethernet II, Src: Apple_10:41:06 (80:e6:50:10:41:06), Dst: AsustekC_3f:90:60 (74:d0:2b:3f:
90:60)
Internet Protocol Version 4, Src: 192.168.1.20, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 53918, Dst Port: 80, Seq: 1, Ack: 1, Len: 483
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
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:56.0) Gecko/20100101
Firefox/
56.0\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
    Upgrade-Insecure-Requests: 1\r\n
    If-Modified-Since: Sun, 11 Feb 2018 06:59:01 GMT\r\n
    If-None-Match: "173-564ea4bd7c38f"\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 1/1]
    [Response in frame: 464]
```

Response 2:

```
    464 14.744805      128.119.245.12        192.168.1.20         HTTP     306    HTTP/1.1 304
Not Modified
Frame 464: 306 bytes on wire (2448 bits), 306 bytes captured (2448 bits) on interface 0
Ethernet II, Src: AsustekC_3f:90:60 (74:d0:2b:3f:90:60), Dst: Apple_10:41:06
(80:e6:50:10:41:06)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.20
Transmission Control Protocol, Src Port: 80, Dst Port: 53918, Seq: 1, Ack: 484, Len: 240
Hypertext Transfer Protocol
    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
        [Status Code Description: Not Modified]
        Response Phrase: Not Modified
    Date: Mon, 12 Feb 2018 05:12:47 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\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "173-564ea4bd7c38f"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.029861000 seconds]
    [Request in frame: 462]
```

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?
   No, there is no IF-MODIFIED-SINCE line.
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
   Yes, the server explicitly returned the contents of the file. This is seen in the packet capture window under “File data: 371 bytes” or by inspecting the raw data output for data after the end tag of the html headers.
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?
    Yes, If-Modified-Since: Sun, 11 Feb 2018 06:59:01 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.
    The server returns HTTP/1.1 304 Not Modified\r\n. The Server does not explicitly return the contents of the file, since it can be loaded from the cached copy. This is because the data was not modified since the last cached copy of the response data, so my browser is loading that information from the web cache. I can tell this is the case because there is no data following the headers, or a content-length/content-type header.

Problem 3:

/var/folders/09/r5pnxj9j7nv5wg5744rrw2840000gn/T//
wireshark_en0_20180212002038_FuLbgc.pcapng 242 total packets, 2 shown

Request:

```
   109 11.865038      192.168.1.20          128.119.245.12        HTTP     602    GET /
wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
Frame 109: 602 bytes on wire (4816 bits), 602 bytes captured (4816 bits) on interface 0
Ethernet II, Src: Apple_10:41:06 (80:e6:50:10:41:06), Dst: AsustekC_3f:90:60 (74:d0:2b:3f:
90:60)
Internet Protocol Version 4, Src: 192.168.1.20, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 53939, Dst Port: 80, Seq: 1, Ack: 1, Len: 536
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]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file3.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_13_2) AppleWebKit/537.36
(KHTML, like
Gecko) Chrome/63.0.3239.84 Safari/537.36\r\n
   Upgrade-Insecure-Requests: 1\r\n
   Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
*;q=0.8\r\n
   DNT: 1\r\n
   Accept-Encoding: gzip, deflate\r\n
   Accept-Language: en-US,en;q=0.9\r\n
   Cookie: __unam=9514ce4-1613a14b9fc-6188e86c-8;
SESSIONIDMOODLE=2bb7b2175c5885e21c0a6cdefe65c41b\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: 115]
```

Response:

```
   115 11.887571      128.119.245.12       192.168.1.20         HTTP     583    HTTP/1.1 200
OK  (text/html)
Frame 115: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface 0
Ethernet II, Src: AsustekC_3f:90:60 (74:d0:2b:3f:90:60), Dst: Apple_10:41:06
(80:e6:50:10:41:06)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.20
Transmission Control Protocol, Src Port: 80, Dst Port: 53939, Seq: 4345, Ack: 537, Len: 517
[4 Reassembled TCP Segments (4861 bytes): #112(1448), #113(1448), #114(1448), #115(517)]
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
      [Status Code Description: OK]
      Response Phrase: OK
   Date: Mon, 12 Feb 2018 05:20:50 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\r\n
   Last-Modified: Sun, 11 Feb 2018 06:59:01 GMT\r\n
   ETag: "1194-564ea4bd794af"\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: 0.022533000 seconds]
   [Request in frame: 109]
   File Data: 4500 bytes
Line-based text data: text/html
```

data truncated by student

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?
    My browser sent 1 HTTP Get request. Packet 78 is the GET for the Bill of Rights, seen in "**78** 3.034957   192.168.1.20   128.119.245.12   HTTP   602   GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1"

13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?
    Packet 115 contains the response. This is seen in "[Response in frame: 115]" of the GET request.

14. What is the status code and phrase in the response?
    The code and phrase are "HTTP/1.1 200 OK" seen in "HTTP/1.1 200 OK\r\n" of the response message.

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

    4 TCP segments were needed to carry the HTTP response and text of the Bill of Rights. This is seen in the "[4 Reassembled TCP Segments (4861 bytes): #112(1448), #113(1448), #114(1448), #115(517)]" section of the response.

Part 4

```
/var/folders/09/r5pnxj9j7nv5wg5744rrw2840000gn/T//
wireshark_en0_20180212003733_M6KSq9.pcapng 711 total packets, 8 shown

    21 3.720233       192.168.1.20          128.119.245.12        HTTP     437    GET /
wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
Frame 21: 437 bytes on wire (3496 bits), 437 bytes captured (3496 bits) on interface 0
Ethernet II, Src: Apple_10:41:06 (80:e6:50:10:41:06), Dst: AsustekC_3f:90:60 (74:d0:2b:3f:
90:60)
Internet Protocol Version 4, Src: 192.168.1.20, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 54029, Dst Port: 80, Seq: 1, Ack: 1, Len: 371
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/
1.1\r\n]
        Request Method: GET
        Request URI: /wireshark-labs/HTTP-wireshark-file4.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:56.0) Gecko/20100101
Firefox/
56.0\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
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]
    [HTTP request 1/2]
    [Response in frame: 23]
    [Next request in frame: 28]
     23 3.741174       128.119.245.12        192.168.1.20          HTTP     1139   HTTP/1.1 200
OK  (text/html)
Frame 23: 1139 bytes on wire (9112 bits), 1139 bytes captured (9112 bits) on interface 0
Ethernet II, Src: AsustekC_3f:90:60 (74:d0:2b:3f:90:60), Dst: Apple_10:41:06
(80:e6:50:10:41:06)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.20
Transmission Control Protocol, Src Port: 80, Dst Port: 54029, Seq: 1, Ack: 372, Len: 1073
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
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Mon, 12 Feb 2018 05:37:37 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\r\n
    Last-Modified: Sun, 11 Feb 2018 06:59:01 GMT\r\n
    ETag: "2ca-564ea4bd7bbbf"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 714\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: 0.020941000 seconds]
    [Request in frame: 21]
    [Next request in frame: 28]
    [Next response in frame: 32]
    File Data: 714 bytes
Line-based text data: text/html
    <html>\n
    <head>\n
    <title>Lab2-4 file: Embedded URLs</title>\n
    <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">\n
    </head>\n
    \n
```

```
   <body bgcolor="#FFFFFF" text="#000000">\n
/var/folders/09/r5pnxj9j7nv5wg5744rrw2840000gn/T//
wireshark_en0_20180212003733_M6KSq9.pcapng 711 total packets, 8 shown

   \n
   <p>\n
   <img src="http://gaia.cs.umass.edu/pearson.png" WIDTH="70" HEIGHT="41" > </p>\n
   <p>This little HTML file is being served by gaia.cs.umass.edu. \n
   It contains two embedded images. <br> The image above, also served from the \n
   gaia.cs.umass.edu web site, is the logo of our publisher, Pearson. <br>\n
   The image of our 5th edition book cover below is stored at, and served from, the www server
caite.cs.umass.edu:</p>\n
   <p align="left"><img src="http://manic.cs.umass.edu/~kurose/cover_5th_ed.jpg"
width="168"
height="220"></p>\n
   </body>\n
   </html>\n
    28 3.761693       192.168.1.20          128.119.245.12        HTTP     394    GET /
pearson.png HTTP/1.1
Frame 28: 394 bytes on wire (3152 bits), 394 bytes captured (3152 bits) on interface 0
Ethernet II, Src: Apple_10:41:06 (80:e6:50:10:41:06), Dst: AsustekC_3f:90:60 (74:d0:2b:3f:
90:60)
Internet Protocol Version 4, Src: 192.168.1.20, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 54029, Dst Port: 80, Seq: 372, Ack: 1074, Len: 328
Hypertext Transfer Protocol
   GET /pearson.png HTTP/1.1\r\n
      [Expert Info (Chat/Sequence): GET /pearson.png HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /pearson.png
      Request Version: HTTP/1.1
   Host: gaia.cs.umass.edu\r\n
   User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:56.0) Gecko/20100101
Firefox/
56.0\r\n
   Accept: */*\r\n
   Accept-Language: en-US,en;q=0.5\r\n
   Accept-Encoding: gzip, deflate\r\n
   Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html\r\n
   Connection: keep-alive\r\n
   \r\n
   [Full request URI: http://gaia.cs.umass.edu/pearson.png]
   [HTTP request 2/2]
   [Prev request in frame: 21]
   [Response in frame: 32]
    32 3.784361       128.119.245.12        192.168.1.20          HTTP     781
OK  (PNG)
HTTP/1.1 200

Frame 32: 781 bytes on wire (6248 bits), 781 bytes captured (6248 bits) on interface 0
Ethernet II, Src: AsustekC_3f:90:60 (74:d0:2b:3f:90:60), Dst: Apple_10:41:06
(80:e6:50:10:41:06)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.20
Transmission Control Protocol, Src Port: 80, Dst Port: 54029, Seq: 3970, Ack: 700, Len: 715
[3 Reassembled TCP Segments (3611 bytes): #30(1448), #31(1448), #32(715)]
   [Frame: 30, payload: 0-1447 (1448 bytes)]
   [Frame: 31, payload: 1448-2895 (1448 bytes)]
   [Frame: 32, payload: 2896-3610 (715 bytes)]
   [Segment count: 3]
   [Reassembled TCP length: 3611]
   [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a204d...]
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
      [Status Code Description: OK]
      Response Phrase: OK
   Date: Mon, 12 Feb 2018 05:37:37 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\r\n
   Last-Modified: Sat, 06 Aug 2016 10:08:14 GMT\r\n
   ETag: "cc3-539645c7f1ee7"\r\n
   Accept-Ranges: bytes\r\n
/var/folders/09/r5pnxj9j7nv5wg5744rrw2840000gn/T//
wireshark_en0_20180212003733_M6KSq9.pcapng 711 total packets, 8 shown

   Content-Length: 3267\r\n
   Keep-Alive: timeout=5, max=99\r\n
   Connection: Keep-Alive\r\n
   Content-Type: image/png\r\n
   \r\n
   [HTTP response 2/2]
   [Time since request: 0.022668000 seconds]
   [Prev request in frame: 21]
   [Prev response in frame: 23]
   [Request in frame: 28]
   File Data: 3267 bytes
Portable Network Graphics
    39 3.820528       192.168.1.20          128.119.240.90        HTTP     408
GET /~kurose/
cover_5th_ed.jpg HTTP/1.1
Frame 39: 408 bytes on wire (3264 bits), 408 bytes captured (3264 bits) on interface 0
Ethernet II, Src: Apple_10:41:06 (80:e6:50:10:41:06), Dst: AsustekC_3f:90:60 (74:d0:2b:3f:
90:60)
Internet Protocol Version 4, Src: 192.168.1.20, Dst: 128.119.240.90
Transmission Control Protocol, Src Port: 54030, Dst Port: 80, Seq: 1, Ack: 1, Len: 342
Hypertext Transfer Protocol
   GET /~kurose/cover_5th_ed.jpg HTTP/1.1\r\n
      [Expert Info (Chat/Sequence): GET /~kurose/cover_5th_ed.jpg HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /~kurose/cover_5th_ed.jpg
      Request Version: HTTP/1.1
   Host: manic.cs.umass.edu\r\n
   User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:56.0) Gecko/20100101
Firefox/
56.0\r\n
   Accept: */*\r\n
   Accept-Language: en-US,en;q=0.5\r\n
   Accept-Encoding: gzip, deflate\r\n
   Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html\r\n
   Connection: keep-alive\r\n
   \r\n
   [Full request URI: http://manic.cs.umass.edu/~kurose/cover_5th_ed.jpg]
   [HTTP request 1/1]
   [Response in frame: 42]
    42 3.845907       128.119.240.90        192.168.1.20          HTTP     522
Found  (text/html)
HTTP/1.1 302

Frame 42: 522 bytes on wire (4176 bits), 522 bytes captured (4176 bits) on interface 0
Ethernet II, Src: AsustekC_3f:90:60 (74:d0:2b:3f:90:60), Dst: Apple_10:41:06
(80:e6:50:10:41:06)
Internet Protocol Version 4, Src: 128.119.240.90, Dst: 192.168.1.20
Transmission Control Protocol, Src Port: 80, Dst Port: 54030, Seq: 1, Ack: 343, Len: 456
Hypertext Transfer Protocol
   HTTP/1.1 302 Found\r\n
      [Expert Info (Chat/Sequence): HTTP/1.1 302 Found\r\n]
      Request Version: HTTP/1.1
      Status Code: 302
```

```
        [Status Code Description: Found]
        Response Phrase: Found
    Date: Mon, 12 Feb 2018 05:37:37 GMT\r\n
    Server: Apache\r\n
    Location: http://caite.cs.umass.edu/~kurose/cover_5th_ed.jpg\r\n
    Content-Length: 234\r\n
    Connection: close\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.025379000 seconds]
    [Request in frame: 39]
    File Data: 234 bytes
Line-based text data: text/html
    <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
/var/folders/09/r5pnxj9j7nv5wg5744rrw2840000gn/T//
wireshark_en0_20180212003733_M6KSq9.pcapng 711 total packets, 8 shown

    <html><head>\n
    <title>302 Found</title>\n
    </head><body>\n
    <h1>Found</h1>\n
    <p>The document has moved <a href="http://caite.cs.umass.edu/~kurose/
cover_5th_ed.jpg">here</
a>.</p>\n
    </body></html>\n
     51 3.872692       192.168.1.20          128.119.240.90        HTTP     408    GET /~kurose/
cover_5th_ed.jpg HTTP/1.1
Frame 51: 408 bytes on wire (3264 bits), 408 bytes captured (3264 bits) on interface 0
Ethernet II, Src: Apple_10:41:06 (80:e6:50:10:41:06), Dst: AsustekC_3f:90:60 (74:d0:2b:3f:
90:60)
Internet Protocol Version 4, Src: 192.168.1.20, Dst: 128.119.240.90
Transmission Control Protocol, Src Port: 54031, Dst Port: 80, Seq: 1, Ack: 1, Len: 342
Hypertext Transfer Protocol
    GET /~kurose/cover_5th_ed.jpg HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /~kurose/cover_5th_ed.jpg HTTP/1.1\r\n]
        Request Method: GET
        Request URI: /~kurose/cover_5th_ed.jpg
        Request Version: HTTP/1.1
    Host: caite.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:56.0) Gecko/20100101
Firefox/
56.0\r\n
```

```
Accept: */*\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html\r\n
Connection: keep-alive\r\n
\r\n
[Full request URI: http://caite.cs.umass.edu/~kurose/cover_5th_ed.jpg]
[HTTP request 1/1]
[Response in frame: 168]
168 3.982841       128.119.240.90       192.168.1.20         HTTP     1366
HTTP/1.1 200

OK  (JPEG JFIF image)
Frame 168: 1366 bytes on wire (10928 bits), 1366 bytes captured (10928 bits) on interface 0
Ethernet II, Src: AsustekC_3f:90:60 (74:d0:2b:3f:90:60), Dst: Apple_10:41:06
(80:e6:50:10:41:06)
Internet Protocol Version 4, Src: 128.119.240.90, Dst: 192.168.1.20
Transmission Control Protocol, Src Port: 80, Dst Port: 54031, Seq: 99913, Ack: 343, Len: 1300
[70 Reassembled TCP Segments (101212 bytes): #53(1448), #54(1448), #56(1448), #57(1448),
#58(1448), #59(1448), #60(1448), #61(1448), #62(1448), #63(1448), #69(1448), #70(1448),
#71(1448), #74(1448), #75(1448), #76(1448), #77(1448), #78(1448]
   [Frame: 53, payload: 0-1447 (1448 bytes)]
   [Frame: 54, payload: 1448-2895 (1448 bytes)]
   [Frame: 56, payload: 2896-4343 (1448 bytes)]
   [Frame: 57, payload: 4344-5791 (1448 bytes)]
   [Frame: 58, payload: 5792-7239 (1448 bytes)]
   [Frame: 59, payload: 7240-8687 (1448 bytes)]
   [Frame: 60, payload: 8688-10135 (1448 bytes)]
   [Frame: 61, payload: 10136-11583 (1448 bytes)]
   [Frame: 62, payload: 11584-13031 (1448 bytes)]
   [Frame: 63, payload: 13032-14479 (1448 bytes)]
   [Frame: 69, payload: 14480-15927 (1448 bytes)]
   [Frame: 70, payload: 15928-17375 (1448 bytes)]
   [Frame: 71, payload: 17376-18823 (1448 bytes)]
   [Frame: 74, payload: 18824-20271 (1448 bytes)]
   [Frame: 75, payload: 20272-21719 (1448 bytes)]
   [Frame: 76, payload: 21720-23167 (1448 bytes)]
   [Frame: 77, payload: 23168-24615 (1448 bytes)]
   [Frame: 78, payload: 24616-26063 (1448 bytes)]
   [Frame: 82, payload: 26064-27511 (1448 bytes)]
   [Frame: 83, payload: 27512-28959 (1448 bytes)]
   [Frame: 86, payload: 28960-30407 (1448 bytes)]
   [Frame: 87, payload: 30408-31855 (1448 bytes)]
```

```
    [Frame: 88, payload: 31856-33303 (1448 bytes)]
    [Frame: 91, payload: 33304-34751 (1448 bytes)]
    [Frame: 92, payload: 34752-36199 (1448 bytes)]
    [Frame: 95, payload: 36200-37647 (1448 bytes)]
    [Frame: 96, payload: 37648-39095 (1448 bytes)]
    [Frame: 97, payload: 39096-40543 (1448 bytes)]
    [Frame: 98, payload: 40544-41991 (1448 bytes)]
    [Frame: 102, payload: 41992-43439 (1448 bytes)]
    [Frame: 103, payload: 43440-44887 (1448 bytes)]
    [Frame: 106, payload: 44888-46335 (1448 bytes)]
    [Frame: 107, payload: 46336-47783 (1448 bytes)]
    [Frame: 110, payload: 47784-49231 (1448 bytes)]
    [Frame: 111, payload: 49232-50679 (1448 bytes)]
    [Frame: 112, payload: 50680-52127 (1448 bytes)]
    [Frame: 113, payload: 52128-53575 (1448 bytes)]
    [Frame: 114, payload: 53576-55023 (1448 bytes)]
    [Frame: 115, payload: 55024-56471 (1448 bytes)]
    [Frame: 120, payload: 56472-57919 (1448 bytes)]
    [Frame: 121, payload: 57920-59367 (1448 bytes)]
    [Frame: 122, payload: 59368-60815 (1448 bytes)]
    [Frame: 123, payload: 60816-62263 (1448 bytes)]
    [Frame: 124, payload: 62264-63711 (1448 bytes)]
    [Frame: 125, payload: 63712-65159 (1448 bytes)]
    [Frame: 126, payload: 65160-66607 (1448 bytes)]
    [Frame: 127, payload: 66608-68055 (1448 bytes)]
    [Frame: 134, payload: 68056-69503 (1448 bytes)]
    [Frame: 135, payload: 69504-70951 (1448 bytes)]
    [Frame: 138, payload: 70952-72399 (1448 bytes)]
    [Frame: 139, payload: 72400-73847 (1448 bytes)]
    [Frame: 142, payload: 73848-75295 (1448 bytes)]
    [Frame: 143, payload: 75296-76743 (1448 bytes)]
    [Frame: 146, payload: 76744-78191 (1448 bytes)]
    [Frame: 147, payload: 78192-79639 (1448 bytes)]
    [Frame: 149, payload: 79640-81087 (1448 bytes)]
    [Frame: 150, payload: 81088-82535 (1448 bytes)]
    [Frame: 151, payload: 82536-83983 (1448 bytes)]
    [Frame: 152, payload: 83984-85431 (1448 bytes)]
    [Frame: 156, payload: 85432-86879 (1448 bytes)]
    [Frame: 157, payload: 86880-88327 (1448 bytes)]
    [Frame: 160, payload: 88328-89775 (1448 bytes)]
    [Frame: 161, payload: 89776-91223 (1448 bytes)]
    [Frame: 162, payload: 91224-92671 (1448 bytes)]
    [Frame: 163, payload: 92672-94119 (1448 bytes)]
    [Frame: 164, payload: 94120-95567 (1448 bytes)]
    [Frame: 165, payload: 95568-97015 (1448 bytes)]
    [Frame: 166, payload: 97016-98463 (1448 bytes)]
    [Frame: 167, payload: 98464-99911 (1448 bytes)]
    [Frame: 168, payload: 99912-101211 (1300 bytes)]
    [Segment count: 70]
    [Reassembled TCP length: 101212]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a204d...]
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
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Mon, 12 Feb 2018 05:37:37 GMT\r\n
    Server: Apache\r\n
    Last-Modified: Tue, 15 Sep 2009 18:23:27 GMT\r\n
    ETag: "78004-18a68-473a1e0e6e5c0"\r\n
/var/folders/09/r5pnxj9j7nv5wg5744rrw2840000gn/T//
wireshark_en0_20180212003733_M6KSq9.pcapng 711 total packets, 8 shown

    Accept-Ranges: bytes\r\n
    Content-Length: 100968\r\n
    Connection: close\r\n
    Content-Type: image/jpeg\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.110149000 seconds]
    [Request in frame: 51]
    File Data: 100968 bytes
JPEG File Interchange Format
```

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?
    My browser sent 4 requests. The first 2 requests (for the html and pearson.png) were sent to 128.119.245.12 indicated by the destination field in their respective request packets. The last requests for the cover_5th_ed.jpg were sent to 128.119.240.90, indicated by the destination field in those request packets.

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.
    Just by looking at the packet capture window, I deduce that since the GET request for the book cover was sent after the response for the GET request for the pearson logo was received, the images were downloaded serially.

    However, it is also possible that the internet connection speed is sufficiently fast that the response for the pearson logo returned before the browser could send the GET for the book cover in parallel, but this is unlikely. Since HTTP/1.1 according to RFC 2616 supports pipelining and there is no specification for a GET request header to specify a pipelined request, it is impossible to completely tell whether this request was pipelined or not.

Part 5

```
/var/folders/09/r5pnxj9j7nv5wg5744rrw2840000gn/T//
wireshark_en0_20180212005725_oKirDU.pcapng 411 total packets, 6 shown

   210 9.183073       192.168.1.20          128.119.245.12        HTTP     453    GET /
wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
Frame 210: 453 bytes on wire (3624 bits), 453 bytes captured (3624 bits) on interface 0
Ethernet II, Src: Apple_10:41:06 (80:e6:50:10:41:06), Dst: AsustekC_3f:90:60 (74:d0:2b:3f:
90:60)
Internet Protocol Version 4, Src: 192.168.1.20, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 54365, Dst Port: 80, Seq: 1, Ack: 1, Len: 387
Hypertext Transfer Protocol
    GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-
file5.html HTTP/1.1\r\n]
        Request Method: GET
        Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:58.0) Gecko/20100101
Firefox/
58.0\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
    Upgrade-Insecure-Requests: 1\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: 217]
    217 9.202827       128.119.245.12       192.168.1.20         HTTP     783    HTTP/1.1 401
Unauthorized  (text/html)
Frame 217: 783 bytes on wire (6264 bits), 783 bytes captured (6264 bits) on interface 0
Ethernet II, Src: AsustekC_3f:90:60 (74:d0:2b:3f:90:60), Dst: Apple_10:41:06
(80:e6:50:10:41:06)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.20
Transmission Control Protocol, Src Port: 80, Dst Port: 54365, Seq: 1, Ack: 388, Len: 717
Hypertext Transfer Protocol
    HTTP/1.1 401 Unauthorized\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
        Request Version: HTTP/1.1
        Status Code: 401
        [Status Code Description: Unauthorized]
        Response Phrase: Unauthorized
    Date: Mon, 12 Feb 2018 05:57:34 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\r\n
    WWW-Authenticate: Basic realm="wireshark-students only"\r\n
    Content-Length: 381\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.019754000 seconds]
    [Request in frame: 210]
    File Data: 381 bytes
Line-based text data: text/html
    <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
    <html><head>\n
    <title>401 Unauthorized</title>\n
    </head><body>\n
    <h1>Unauthorized</h1>\n
    <p>This server could not verify that you\n
    are authorized to access the document\n
    requested.  Either you supplied the wrong\n
    credentials (e.g., bad password), or your\n
    browser doesn't understand how to supply\n
```

```
    the credentials required.</p>\n
```

```
   </body></html>\n
   385 22.113908      192.168.1.20          128.119.245.12        HTTP     512    GET /
wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
Frame 385: 512 bytes on wire (4096 bits), 512 bytes captured (4096 bits) on interface 0
Ethernet II, Src: Apple_10:41:06 (80:e6:50:10:41:06), Dst: AsustekC_3f:90:60 (74:d0:2b:3f:
90:60)
Internet Protocol Version 4, Src: 192.168.1.20, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 54370, Dst Port: 80, Seq: 1, Ack: 1, Len: 446
Hypertext Transfer Protocol
   GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
      [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-
file5.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
      Request Version: HTTP/1.1
   Host: gaia.cs.umass.edu\r\n
   User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:58.0) Gecko/20100101
Firefox/
58.0\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
   Upgrade-Insecure-Requests: 1\r\n
   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 1/2]
   [Response in frame: 390]
   [Next request in frame: 395]
   390 22.139282      128.119.245.12       192.168.1.20         HTTP     556
HTTP/1.1 200

OK  (text/html)
Frame 390: 556 bytes on wire (4448 bits), 556 bytes captured (4448 bits) on interface 0
Ethernet II, Src: AsustekC_3f:90:60 (74:d0:2b:3f:90:60), Dst: Apple_10:41:06
(80:e6:50:10:41:06)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.20
Transmission Control Protocol, Src Port: 80, Dst Port: 54370, Seq: 1, Ack: 447, Len: 490
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
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Mon, 12 Feb 2018 05:57:47 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\r\n
    Last-Modified: Sun, 11 Feb 2018 06:59:01 GMT\r\n
    ETag: "84-564ea4bd7d32f"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 132\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: 0.025374000 seconds]
    [Request in frame: 385]
    [Next request in frame: 395]
    [Next response in frame: 396]
    File Data: 132 bytes
Line-based text data: text/html
    \n
<html>\n

/var/folders/09/r5pnxj9j7nv5wg5744rrw2840000gn/T//
wireshark_en0_20180212005725_oKirDU.pcapng 411 total packets, 6 shown

\n

    This page is password protected!  If you're seeing this, you've downloaded the page correctly
<br>\n
    Congratulations!\n
    </html>
```

18. What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser?
    The server’s response is HTTP/1.1 401 Unauthorized, seen in the description field of response to the first GET request.

19. When your browser’s sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n. This is seen in the “Authorization” header of the second GET request, which was not in the first request.