

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

```

  ▾ 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]
        [GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
        Request Method: GET
        Request URI: /wireshark-labs/HTTP-wireshark-file1.html
        Request Version: HTTP/1.1

  ▾ 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]
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK

```

Both the server and my browser are running HTTP 1.1

2. What languages (if any) does your browser indicate that it can accept to the server?

Accept-Language: en-US,en;q=0.9\r\n

My browser indicates it can accept english (i.e en-US, en)

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

No.	Time	Source	Destination	Protocol	Length	Info
4854	09:11:41.180727	129.138.162.242	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

My IP address is 129.138.162.242

The Server's IP address is 128.119.245.12

4. What is the status code returned from the server to your browser?

```

  ▾ 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]
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK

```

The status returned by the server is 200

5. When was the HTML file that you are retrieving last modified at the server?

Last-Modified: Tue, 14 Sep 2021 05:59:01 GMT\r\n

The HTML file was last modified on Tuesday, september 14 at 5:59:01 GMT

6. How many bytes of content are being returned to your browser?

File Data: 128 bytes

128 bytes are returned to my browser

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.

```
▼ Line-based text data: text/html (4 lines)
<html>\n
Congratulations.  You've downloaded the file \n
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
</html>\n
```

The text/html header is not displayed in the packet-listing window.

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?

```
▼ 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
      Connection: keep-alive\r\n
      Upgrade-Insecure-Requests: 1\r\n
      User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36 Edg/93.0.961.47\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
      Accept-Encoding: gzip, deflate\r\n
      Accept-Language: en-US,en;q=0.9\r\n
      \r\n
      [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
      [HTTP request 1/3]
      [Response in frame: 200]
      [Next request in frame: 444]
```

I do not see an “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?

```
▼ Line-based text data: text/html (10 lines)
  \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
  field in your browser's HTTP GET request to the server.\n
  \n
  </html>\n
```

Yes, I can tell because of the contents of the text/html 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?

```
If-Modified-Since: Tue, 14 Sep 2021 05:59:01 GMT\r\n
\r\n
```

This time there is an “IF-MODIFIED-SINCE:” line, the information that follows is the time of my first request to the server.

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.

```
▼ [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n\r\n]
  [HTTP/1.1 304 Not Modified\r\n\r\n]
  [Severity level: Chat]
  [Group: Sequence]
  Response Version: HTTP/1.1
  Status Code: 304
  [Status Code Description: Not Modified]
  Response Phrase: Not Modified
```

The status code returned from the server is 304, and the server did NOT explicitly return the contents of the file. I can tell because the text/html header is missing from this packet.

```
▼ HTTP/1.1 304 Not Modified\r\n
  ▼ [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
    [HTTP/1.1 304 Not Modified\r\n]
    [Severity level: Chat]
    [Group: Sequence]
    Response Version: HTTP/1.1
    Status Code: 304
    [Status Code Description: Not Modified]
    Response Phrase: Not Modified
    Date: Tue, 14 Sep 2021 18:29:36 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.22 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=99\r\n
    ETag: "173-5cbee47435bf5"\r\n
    \r\n
    [HTTP response 2/3]
    [Time since request: 0.520614000 seconds]
    [Prev request in frame: 192]
    [Prev response in frame: 200]
    [Request in frame: 444]
    [Next response in frame: 645]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

There also isn't a "file data" section in this packet.

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?

Full request url: http://gaia.cs.
[HTTP request 1/1]

My browser only sent one request

01f0	70 3e 3c 62 72 3e 0a 3c 2f 70 3e 0a 3c 70 3e 3c	p> < /p><p><
0200	2f 70 3e 3c 63 65 6e 74 65 72 3e 3c 62 3e 54 48	/p><cent er>TH
0210	45 20 42 49 4c 4c 20 4f 46 20 52 49 47 48 54 53	E BILL O F RIGHTS
0220	3c 2f 62 3e 3c 62 72 3e 0a 20 20 3c 65 6d 3e 41	 . A
0230	6d 65 6e 64 6d 65 6e 74 73 20 31 2d 31 30 20 6f	mendment s 1-10 o
0240	66 20 74 68 65 20 43 6f 6e 73 74 69 74 75 74 69	f the Co nstituti
0250	6f 6e 3c 2f 65 6d 3e 0a 3c 2f 63 65 6e 74 65 72	on . </center
0260	3e 0a 0a 3c 70 3e 54 68 65 20 43 6f 6e 76 65 6e	> . <p>Th e Conven

Packet 0200 contains the Bill of Rights

13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

```
0000 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d HTTP/1.1 200 OK
```

Packet 0000 contains the status code and phrase associated with the response to HTTP GET

14. What is the status code and phrase in the response?

The status code is 200 and the phrase is 'OK'.

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

> [4 Reassembled TCP Segments (4861 bytes): #979(1452), #980(1452), #982(1452), #983(505)]

4 TCP segments were needed to carry the response and text of the Bill of Rights

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

No.	Time	Source	Destination	Protocol	Length	Info
175	13:00:10.420625	192.168.0.42	128.119.245.12	HTTP	534	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
193	13:00:10.594776	128.119.245.12	192.168.0.42	HTTP	1355	HTTP/1.1 200 OK (text/html)
194	13:00:10.631356	192.168.0.42	128.119.245.12	HTTP	480	GET /pearson.png HTTP/1.1
209	13:00:10.776962	128.119.245.12	192.168.0.42	HTTP	761	HTTP/1.1 200 OK (PNG)
224	13:00:10.993315	192.168.0.42	178.79.137.164	HTTP	447	GET /8E_cover_small.jpg HTTP/1.1
238	13:00:11.232166	178.79.137.164	192.168.0.42	HTTP	225	HTTP/1.1 301 Moved Permanently

There were three GET requests sent by my browser.

The addresses they were sent to, in order, are:

128.119.245.12

128.119.245.12

178.79.137.164

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.

No.	Time	Source	Destination	Protocol	Length	Info
175	13:00:10.420625	192.168.0.42	128.119.245.12	HTTP	534	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
193	13:00:10.594776	128.119.245.12	192.168.0.42	HTTP	1355	HTTP/1.1 200 OK (text/html)
194	13:00:10.631356	192.168.0.42	128.119.245.12	HTTP	480	GET /pearson.png HTTP/1.1
209	13:00:10.776962	128.119.245.12	192.168.0.42	HTTP	761	HTTP/1.1 200 OK (PNG)
224	13:00:10.993315	192.168.0.42	178.79.137.164	HTTP	447	GET /8E_cover_small.jpg HTTP/1.1
238	13:00:11.232166	178.79.137.164	192.168.0.42	HTTP	225	HTTP/1.1 301 Moved Permanently

They were sent serially, you can tell because the first GET for the image was sent at packet 194 and received an OK at 209, while the second GET was sent at 224 and received a 'Moved Permanently' at 238. So these clearly happened one after the other.

18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

```

▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 401 Unauthorized\r\n
    ▼ [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
      [HTTP/1.1 401 Unauthorized\r\n]
      [Severity level: Chat]
      [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 401
      [Status Code Description: Unauthorized]
      Response Phrase: Unauthorized
      Date: Tue, 14 Sep 2021 19:17:45 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.22 mod_perl/2.0.11 Perl/v5.16.3\r\n
      WWW-Authenticate: Basic realm="wireshark-students only"\r\n

```

The server's response to the initial GET was 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?

First GET

```

▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 401 Unauthorized\r\n
    ▼ [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
      [HTTP/1.1 401 Unauthorized\r\n]
      [Severity level: Chat]
      [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 401
      [Status Code Description: Unauthorized]
      Response Phrase: Unauthorized
      Date: Tue, 14 Sep 2021 19:17:45 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.22 mod_perl/2.0.11 Perl/v5.16.3\r\n
      WWW-Authenticate: Basic realm="wireshark-students only"\r\n
  ▼ Content-Length: 381\r\n
    [Content length: 381]
  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: 0.121268000 seconds]
  [Request in frame: 107]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
  File Data: 381 bytes

```

Second GET

```

▼ 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]
      [GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
      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
      Connection: keep-alive\r\n
      Cache-Control: max-age=0\r\n
      Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcm0=\r\n
      Upgrade-Insecure-Requests: 1\r\n
      User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36 Edg/93.0.961.47\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
      Accept-Encoding: gzip, deflate\r\n
      Accept-Language: en-US,en;q=0.9\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: 1155]

```

✓ Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcm5=\r\n
Credentials: wireshark-students:network

The new field in the second get is 'Authorization'

Full Data For Reference:

Problem Set 1

```
No.      Time      Source      Destination      Protocol Length Info
4854 09:11:41.180727 129.138.162.242 128.119.245.12 HTTP 529 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
Frame 4854: 529 bytes on wire (4232 bits), 529 bytes captured (4232 bits) on interface \Device\NPF_{9AD0EF15-6B08-4F7E-9671-CD0987287E3C}, id 0
Ethernet II, Src: Tp-LinkT_e0:ac:16 (98:48:27:e0:ac:16), Dst: JuniperN_ff:10:01 (00:10:db:ff:10:01)
Internet Protocol Version 4, Src: 129.138.162.242, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 65248, Dst Port: 80, Seq: 1, Ack: 1, Len: 475
Hypertext Transfer Protocol
No.      Time      Source      Destination      Protocol Length Info
4914 09:11:41.235622 129.119.245.12 129.138.162.242 HTTP 540 HTTP/1.1 200 OK (text/html)
Frame 4914: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{9AD0EF15-6B08-4F7E-9671-CD0987287E3C}, id 0
Ethernet II, Src: JuniperN_ff:10:01 (00:10:db:ff:10:01), Dst: Tp-LinkT_e0:ac:16 (98:48:27:e0:ac:16)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 129.138.162.242
Transmission Control Protocol, Src Port: 80, Dst Port: 65248, Seq: 1, Ack: 476, Len: 486
Hypertext Transfer Protocol
Line-based text data: text/html (4 lines)
No.      Time      Source      Destination      Protocol Length Info
5082 09:11:41.713651 129.138.162.242 128.119.245.12 HTTP 475 GET /Favicon.ico HTTP/1.1
Frame 5082: 475 bytes on wire (3800 bits), 475 bytes captured (3800 bits) on interface \Device\NPF_{9AD0EF15-6B08-4F7E-9671-CD0987287E3C}, id 0
Ethernet II, Src: Tp-LinkT_e0:ac:16 (98:48:27:e0:ac:16), Dst: JuniperN_ff:10:01 (00:10:db:ff:10:01)
Internet Protocol Version 4, Src: 129.138.162.242, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 65248, Dst Port: 80, Seq: 476, Ack: 487, Len: 421
Hypertext Transfer Protocol
No.      Time      Source      Destination      Protocol Length Info
5115 09:11:41.766462 128.119.245.12 129.138.162.242 HTTP 538 HTTP/1.1 404 Not Found (text/html)
Frame 5115: 538 bytes on wire (4304 bits), 538 bytes captured (4304 bits) on interface \Device\NPF_{9AD0EF15-6B08-4F7E-9671-CD0987287E3C}, id 0
Ethernet II, Src: JuniperN_ff:10:01 (00:10:db:ff:10:01), Dst: Tp-LinkT_e0:ac:16 (98:48:27:e0:ac:16)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 129.138.162.242
Transmission Control Protocol, Src Port: 80, Dst Port: 65248, Seq: 487, Ack: 897, Len: 484
Hypertext Transfer Protocol
Line-based text data: text/html (7 lines)
```

Problem Set 2

Julian Garcia

CSE 353: HW2

```
No.      Time      Source      Destination      Protocol Length Info
192 12:29:33.954956 192.168.0.42 128.119.245.12 HTTP 534 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Frame 192: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface \Device\NPF_{9AD0EF15-6B0B-4F7E-9671-CD0987287E3C}, id 0
Ethernet II, Src: Tp-LinkT_e0:ac:16 (98:48:27:e0:ac:16), Dst: ZyxelCom_e9:9d:30 (e4:18:6b:e9:9d:30)
Internet Protocol Version 4, Src: 192.168.0.42, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 49488, Dst Port: 80, Seq: 1, Ack: 1, Len: 480
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
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36 Edg/93.0.961.47\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
  [HTTP request 1/3]
  [Response in frame: 200]
  [Next request in frame: 444]
No.      Time      Source      Destination      Protocol Length Info
200 12:29:34.076174 128.119.245.12 192.168.0.42 HTTP 784 HTTP/1.1 200 OK (text/html)
Frame 200: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{9AD0EF15-6B0B-4F7E-9671-CD0987287E3C}, id 0
Ethernet II, Src: ZyxelCom_e9:9d:30 (e4:18:6b:e9:9d:30), Dst: Tp-LinkT_e0:ac:16 (98:48:27:e0:ac:16)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.42
Transmission Control Protocol, Src Port: 80, Dst Port: 49488, Seq: 1, Ack: 481, Len: 730
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]
  Response Version: HTTP/1.1
  Status Code: 200
  [Status Code Description: OK]
  Response Phrase: OK
  Date: Tue, 14 Sep 2021 18:29:34 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.22 mod_perl/2.0.11 Perl/v5.16.3\r\n
  Last-Modified: Tue, 14 Sep 2021 05:59:01 GMT\r\n
  ETag: "173-5cbee47435bf5"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 371\r\n
  [Content length: 371]
  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 1/3]
  [Time since request: 0.121218000 seconds]
  [Request in frame: 192]
  [Next request in frame: 444]
  [Next response in frame: 553]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
  File Data: 371 bytes
Line-based text data: text/html (10 lines)
  \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
  field in your browser's HTTP GET request to the server.\n
  \n
  </html>\n
No.      Time      Source      Destination      Protocol Length Info
444 12:29:35.948069 192.168.0.42 128.119.245.12 HTTP 646 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Frame 444: 646 bytes on wire (5168 bits), 646 bytes captured (5168 bits) on interface \Device\NPF_{9AD0EF15-6B0B-4F7E-9671-CD0987287E3C}, id 0
Ethernet II, Src: Tp-LinkT_e0:ac:16 (98:48:27:e0:ac:16), Dst: ZyxelCom_e9:9d:30 (e4:18:6b:e9:9d:30)
Internet Protocol Version 4, Src: 192.168.0.42, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 49488, Dst Port: 80, Seq: 481, Ack: 731, Len: 592
Hypertext Transfer Protocol
```


Julian Garcia
CSE 353: HW2

```
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
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36 Edg/93.0.961.47\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
If-None-Match: "173-5cbee47435bf5"\r\n
If-Modified-Since: Tue, 14 Sep 2021 05:59:01 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 2/3]
[Prev request in frame: 192]
[Response in frame: 553]
No.      Time      Source      Destination      Protocol Length Info
553 12:29:36.468683 128.119.245.12 192.168.0.42 HTTP 293 HTTP/1.1 304 Not Modified
Frame 553: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{9AD0EF15-6B0B-4F7E-9671-CD0987287E3C}, id 8
Ethernet II, Src: ZyxelCom_e9:9d:30 (e4:18:6b:e9:9d:30), Dst: Tp-LinkT_e0:ac:16 (98:48:27:e0:ac:16)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.42
Transmission Control Protocol, Src Port: 80, Dst Port: 49488, Seq: 731, Ack: 1073, Len: 239
Hypertext Transfer Protocol
HTTP/1.1 304 Not Modified\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
[HTTP/1.1 304 Not Modified\r\n]
[Severity level: Chat]
[Group: Sequence]
Response Version: HTTP/1.1
Status Code: 304
[Status Code Description: Not Modified]
Response Phrase: Not Modified
Date: Tue, 14 Sep 2021 18:29:36 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.22 mod_perl/2.0.11 Perl/v5.16.3\r\n
Connection: Keep-Alive\r\n
Keep-Alive: timeout=5, max=99\r\n
ETag: "173-5cbee47435bf5"\r\n
\r\n
[HTTP response 2/3]
[Time since request: 0.520614000 seconds]
[Prev request in frame: 192]
[Prev response in frame: 200]
[Request in frame: 444]
[Next response in frame: 645]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
No.      Time      Source      Destination      Protocol Length Info
645 12:29:36.836148 128.119.245.12 192.168.0.42 HTTP 293 [TCP Spurious Retransmission] HTTP/1.1 304 Not Modified
Frame 645: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{9AD0EF15-6B0B-4F7E-9671-CD0987287E3C}, id 8
Ethernet II, Src: ZyxelCom_e9:9d:30 (e4:18:6b:e9:9d:30), Dst: Tp-LinkT_e0:ac:16 (98:48:27:e0:ac:16)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.42
Transmission Control Protocol, Src Port: 80, Dst Port: 49488, Seq: 731, Ack: 1073, Len: 239
Hypertext Transfer Protocol
HTTP/1.1 304 Not Modified\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
[HTTP/1.1 304 Not Modified\r\n]
[Severity level: Chat]
[Group: Sequence]
Response Version: HTTP/1.1
Status Code: 304
[Status Code Description: Not Modified]
Response Phrase: Not Modified
Date: Tue, 14 Sep 2021 18:29:36 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.22 mod_perl/2.0.11 Perl/v5.16.3\r\n
Connection: Keep-Alive\r\n
Keep-Alive: timeout=5, max=99\r\n
ETag: "173-5cbee47435bf5"\r\n
\r\n
[HTTP response 3/3]
[Prev request in frame: 444]
[Prev response in frame: 553]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

Julian Garcia
CSE 353: HW2

Problem Set 3

```
No.      Time          Source            Destination      Protocol Length Info
 818 12:48:07.563676  192.168.0.42      128.119.245.12   HTTP      534    GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
Frame 818: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface \Device\NPF_{9AD0EF15-680B-4F7E-9671-CD0987287E3C}, id
0
Ethernet II, Src: Tp-LinkT_e0:ac:16 (98:48:27:e0:ac:16), Dst: ZyxelCom_e9:9d:30 (e4:18:6b:e9:9d:30)
Internet Protocol Version 4, Src: 192.168.0.42, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 61695, Dst Port: 80, Seq: 1, Ack: 1, Len: 480
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
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36 Edg/
93.0.961.47\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\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: 983]
No.      Time          Source            Destination      Protocol Length Info
 983 12:48:08.317978  128.119.245.12    192.168.0.42     HTTP      559    HTTP/1.1 200 OK (text/html)
Frame 983: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface \Device\NPF_{9AD0EF15-680B-4F7E-9671-CD0987287E3C}, id
0
Ethernet II, Src: ZyxelCom_e9:9d:30 (e4:18:6b:e9:9d:30), Dst: Tp-LinkT_e0:ac:16 (98:48:27:e0:ac:16)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.42
Transmission Control Protocol, Src Port: 80, Dst Port: 61695, Seq: 4357, Ack: 481, Len: 505
[4 Reassembled TCP Segments (4861 bytes): #979(1452), #980(1452), #982(1452), #983(505)]
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]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
    Date: Tue, 14 Sep 2021 18:48:08 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.22 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Tue, 14 Sep 2021 05:59:01 GMT\r\n
    ETag: "1194-5cbee474311bd"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 4500\r\n
    [Content length: 4500]
    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: 0.754302000 seconds]
    [Request in frame: 818]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
    File Data: 4500 bytes
Line-based text data: text/html (98 lines)
<html><head> \n
<title>Historical Documents:THE BILL OF RIGHTS</title></head>\n
\n
\n
<body bgcolor="#ffffff" link="#330000" vlink="#666633">\n
<p><br>\n
</p>\n
<p></p><center><b>THE BILL OF RIGHTS</b><br>\n
  <em>Amendments 1-10 of the Constitution</em>\n
</center>\n
\n
<p>The Conventions of a number of the States having, at the time of adopting\n
the Constitution, expressed a desire, in order to prevent misconstruction\n
or abuse of its powers, that further declaratory and restrictive clauses\n
should be added, and as extending the ground of public confidence in the\n
Government will best insure the beneficent ends of its institution; </p><p> Resolved, by the Senate and House of Representatives of the
United\n
States of America, in Congress assembled, two-thirds of both Houses concurring,\n
that the following articles be proposed to the Legislatures of the several\n
States, as amendments to the Constitution of the United States; all or any\n
```

of which articles, when ratified by three-fourths of the said Legislatures,\n to be valid to all intents and purposes as part of the said Constitution,\n namely: </p><p><h3>Amendment I</h3>\n \n <p></p><p>Congress shall make no law respecting an establishment of\n religion, or prohibiting the free exercise thereof; or\n abridging the freedom of speech, or of the press; or the\n right of the people peaceably to assemble, and to petition\n the government for a redress of grievances.\n \n </p><p><h3>Amendment II</h3>\n \n <p></p><p>A well regulated militia, being necessary to the security\n of a free state, the right of the people to keep and bear\n arms, shall not be infringed.\n \n </p><p><h3>Amendment III</h3>\n \n <p></p><p>No soldier shall, in time of peace be quartered in any house,\n without the consent of the owner, nor in time of war, but\n in a manner to be prescribed by law.\n \n </p><p><h3>Amendment IV</h3>\n \n <p></p><p>The right of the people to be secure in their persons, houses,\n papers, and effects, against unreasonable searches and seizures,\n shall not be violated, and no warrants shall issue, but upon\n probable cause, supported by oath or affirmation, and\n particularly describing the place to be searched, and the\n persons or things to be seized.\n \n </p><p><h3>Amendment V</h3>\n \n <p></p><p>No person shall be held to answer for a capital, or otherwise\n infamous crime, unless on a presentment or indictment of a grand\n jury, except in cases arising in the land or naval forces,\n or in the militia, when in actual service in time of war\n or public danger; nor shall any person be subject for the\n same offense to be twice put in jeopardy of life or limb;\n nor shall be compelled in any criminal case to be a witness\n against himself, nor be deprived of life, liberty, or property,\n without due process of law; nor shall private property be\n taken for public use, without just compensation.\n \n </p><p><h3>Amendment VI</h3>\n \n <p></p><p>In all criminal prosecutions, the accused shall enjoy the right\n to a speedy and public trial, by an impartial jury of the state\n and district wherein the crime shall have been committed, which\n district shall have been previously ascertained by law, and\n to be informed of the nature and cause of the accusation;\n to be confronted with the witnesses against him; to have\n compulsory process for obtaining witnesses in his favor,\n and to have the assistance of counsel for his defense.\n \n </p><p><h3>Amendment VII</h3>\n \n <p></p><p>In suits at common law, where the value in controversy shall\n exceed twenty dollars, the right of trial by jury shall be\n preserved, and no fact tried by a jury, shall be otherwise\n reexamined in any court of the United States, than according\n to the rules of the common law.\n \n </p><p><h3>Amendment VIII</h3>\n \n <p></p><p>Excessive bail shall not be required, nor excessive fines\n imposed, nor cruel and unusual punishments inflicted.\n \n </p><p><h3>Amendment IX</h3>\n \n <p></p><p>The enumeration in the Constitution, of certain rights, shall\n not be construed to deny or disparage others retained by the people.\n \n </p><p><h3>Amendment X</h3>\n \n <p></p><p>\n <p>The powers not delegated to the United States by the Constitution, nor prohibited\n by it to the states, are reserved to the states respectively, or to the people.</p>\n </body></html>

Julian Garcia
CSE 353: HW2

Problem Set 4:

```
No.      Time      Source      Destination      Protocol Length Info
175 13:00:10.420625 192.168.0.42 128.119.245.12 HTTP 534 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
Frame 175: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface \Device\NPF_{9AD0EF15-6B08-4F7E-9671-CD0987287E3C}, id
8
Ethernet II, Src: Tp-LinkT_e0:ac:16 (98:48:27:e0:ac:16), Dst: ZyxelCom_e9:9d:30 (e4:18:6b:e9:9d:30)
Internet Protocol Version 4, Src: 192.168.0.42, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 55570, Dst Port: 80, Seq: 1, Ack: 1, Len: 480
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]
  [GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n]
  [Severity level: Chat]
  [Group: Sequence]
  Request Method: GET
  Request URI: /wireshark-labs/HTTP-wireshark-file4.html
  Request Version: HTTP/1.1
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36 Edg/
93.0.961.47\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9\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: 193]
  [Next request in frame: 194]
No.      Time      Source      Destination      Protocol Length Info
193 13:00:10.594776 128.119.245.12 192.168.0.42 HTTP 1355 HTTP/1.1 200 OK (text/html)
Frame 193: 1355 bytes on wire (10840 bits), 1355 bytes captured (10840 bits) on interface \Device\NPF_{9AD0EF15-6B08-4F7E-9671-CD0987287E3C},
id 8
Ethernet II, Src: ZyxelCom_e9:9d:30 (e4:18:6b:e9:9d:30), Dst: Tp-LinkT_e0:ac:16 (98:48:27:e0:ac:16)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.42
Transmission Control Protocol, Src Port: 80, Dst Port: 55570, Seq: 1, Ack: 481, Len: 1301
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]
  Response Version: HTTP/1.1
  Status Code: 200
  [Status Code Description: OK]
  Response Phrase: OK
  Date: Tue, 14 Sep 2021 19:00:10 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.22 mod_perl/2.0.11 Perl/v5.16.3\r\n
  Last-Modified: Tue, 14 Sep 2021 05:59:01 GMT\r\n
  ETag: "3ae-5cbee4743503d"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 942\r\n
  [Content length: 942]
  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: 0.174151000 seconds]
  [Request in frame: 175]
  [Next request in frame: 194]
  [Next response in frame: 209]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]
  File Data: 942 bytes
Line-based text data: text/html (23 lines)
  <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
  \n
  <p>\n
   </p>\n
  <p>This little HTML file is being served by gaia.cs.umass.edu. \n
  It contains two embedded images. The image above, also served from the \n
  gaia.cs.umass.edu web site, is the logo of our publisher, Pearson. \n
  The image of our 8th edition book cover below is stored at, and served from,\n
  a WWW server kurose.cslash.net in France:</p>\n
  <p align="left"></p>\n
  And while we have your attention, you might want to take time to check out the\n
```

```

<tt>
  available open resources for this book at</tt>
  \t\t <a href="http://gaia.cs.umass.edu/kurose_ross"> http://gaia.cs.umass.edu/kurose_ross</a>.\n
  \n
</body>\n
</html>\n
No.      Time      Source      Destination      Protocol Length Info
  194 13:00:10.631356 192.168.0.42 128.119.245.12 HTTP 480 GET /pearson.png HTTP/1.1
Frame 194: 480 bytes on wire (3840 bits), 480 bytes captured (3840 bits) on interface \Device\NPF_{9AD0EF15-680B-4F7E-9671-CD0987287E3C}, id 0
Ethernet II, Src: Tp-LinkT_e0:ac:16 (98:48:27:e0:ac:16), Dst: ZyxelCom_e9:9d:30 (e4:18:6b:e9:9d:30)
Internet Protocol Version 4, Src: 192.168.0.42, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 55570, Dst Port: 80, Seq: 481, Ack: 1302, Len: 426
Hypertext Transfer Protocol
  GET /pearson.png HTTP/1.1\r\n
  [Expert Info (Chat/Sequence): GET /pearson.png HTTP/1.1\r\n]
  [GET /pearson.png HTTP/1.1\r\n]
  [Severity level: Chat]
  [Group: Sequence]
  Request Method: GET
  Request URI: /pearson.png
  Request Version: HTTP/1.1
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36 Edg/93.0.961.47\r\n
  Accept: image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
  Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/pearson.png]
  [HTTP request 2/2]
  [Prev request in frame: 175]
  [Response in frame: 209]
No.      Time      Source      Destination      Protocol Length Info
  209 13:00:10.776962 128.119.245.12 192.168.0.42 HTTP 761 HTTP/1.1 200 OK (PNG)
Frame 209: 761 bytes on wire (6088 bits), 761 bytes captured (6088 bits) on interface \Device\NPF_{9AD0EF15-680B-4F7E-9671-CD0987287E3C}, id 0
Ethernet II, Src: ZyxelCom_e9:9d:30 (e4:18:6b:e9:9d:30), Dst: Tp-LinkT_e0:ac:16 (98:48:27:e0:ac:16)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.42
Transmission Control Protocol, Src Port: 80, Dst Port: 55570, Seq: 4206, Ack: 907, Len: 707
[3 Reassembled TCP Segments (3611 bytes): #205(1452), #207(1452), #209(707)]
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]
  Response Version: HTTP/1.1
  Status Code: 200
  [Status Code Description: OK]
  Response Phrase: OK
  Date: Tue, 14 Sep 2021 19:00:10 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.22 mod_perl/2.0.11 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
  Content-Length: 3267\r\n
  [Content length: 3267]
  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: 0.145606000 seconds]
  [Prev request in frame: 175]
  [Prev response in frame: 193]
  [Request in frame: 194]
  [Request URI: http://gaia.cs.umass.edu/pearson.png]
  File Data: 3267 bytes
Portable Network Graphics
No.      Time      Source      Destination      Protocol Length Info
  224 13:00:10.993315 192.168.0.42 178.79.137.164 HTTP 447 GET /8E_cover_small.jpg HTTP/1.1
Frame 224: 447 bytes on wire (3576 bits), 447 bytes captured (3576 bits) on interface \Device\NPF_{9AD0EF15-680B-4F7E-9671-CD0987287E3C}, id 0
Ethernet II, Src: Tp-LinkT_e0:ac:16 (98:48:27:e0:ac:16), Dst: ZyxelCom_e9:9d:30 (e4:18:6b:e9:9d:30)
Internet Protocol Version 4, Src: 192.168.0.42, Dst: 178.79.137.164
Transmission Control Protocol, Src Port: 61240, Dst Port: 80, Seq: 1, Ack: 1, Len: 393
Hypertext Transfer Protocol
  GET /8E_cover_small.jpg HTTP/1.1\r\n
  [Expert Info (Chat/Sequence): GET /8E_cover_small.jpg HTTP/1.1\r\n]
  [GET /8E_cover_small.jpg HTTP/1.1\r\n]
  [Severity level: Chat]

```

Julian Garcia
CSE 353: HW2

```
[Group: Sequence]
Request Method: GET
Request URI: /8E_cover_small.jpg
Request Version: HTTP/1.1
Host: kurose.cslash.net\r\n
Connection: keep-alive\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36 Edg/93.0.961.47\r\n
Accept: image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
Referer: http://gaia.cs.umass.edu/\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
\r\n
[Full request URI: http://kurose.cslash.net/8E_cover_small.jpg]
[HTTP request 1/1]
[Response in frame: 238]
No.      Time          Source          Destination      Protocol Length Info
238 13:00:11.232166 178.79.137.164 192.168.0.42     HTTP      225    HTTP/1.1 301 Moved Permanently
Frame 238: 225 bytes on wire (1800 bits), 225 bytes captured (1800 bits) on interface \Device\NPF_{9AD0EF15-6B0B-4F7E-9671-CD0987287E3C}, id 0
Ethernet II, Src: ZyxelCom_e9:9d:30 (e4:18:6b:e9:9d:30), Dst: Tp-LinkT_e0:ac:16 (98:48:27:e0:ac:16)
Internet Protocol Version 4, Src: 178.79.137.164, Dst: 192.168.0.42
Transmission Control Protocol, Src Port: 80, Dst Port: 61240, Seq: 1, Ack: 394, Len: 171
Hypertext Transfer Protocol
  HTTP/1.1 301 Moved Permanently\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 301 Moved Permanently\r\n]
    [HTTP/1.1 301 Moved Permanently\r\n]
    [Severity level: Chat]
    [Group: Sequence]
    Response Version: HTTP/1.1
    Status Code: 301
    [Status Code Description: Moved Permanently]
    Response Phrase: Moved Permanently
    Location: https://kurose.cslash.net/8E_cover_small.jpg\r\n
    Content-Length: 0\r\n
    [Content length: 0]
    Date: Tue, 14 Sep 2021 19:00:11 GMT\r\n
    Server: lighttpd/1.4.47\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.238851000 seconds]
    [Request in frame: 224]
    [Request URI: http://kurose.cslash.net/8E_cover_small.jpg]
```

Problem set 5 Below:

Julian Garcia
CSE 353: HW2

```
No.      Time           Source           Destination      Protocol Length Info
 107 13:17:45.655546 192.168.0.42     128.119.245.12   HTTP             550     GET /wireshark-labs/protected_pages/HTTP-wireshark-
File5.html HTTP/1.1
Frame 107: 550 bytes on wire (4400 bits), 550 bytes captured (4400 bits) on interface \Device\NPF_{9AD0EF15-680B-4F7E-9671-CD0987287E3C}, id
0
Ethernet II, Src: Tp-LinkT_e0:ac:16 (98:48:27:e0:ac:16), Dst: ZyxelCom_e9:9d:30 (e4:18:6b:e9:9d:30)
Internet Protocol Version 4, Src: 192.168.0.42, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 56926, Dst Port: 80, Seq: 1, Ack: 1, Len: 496
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]
      [GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    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
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36 Edg/
93.0.961.47\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\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: 115]
No.      Time           Source           Destination      Protocol Length Info
 115 13:17:45.776814 128.119.245.12   192.168.0.42     HTTP             771     HTTP/1.1 401 Unauthorized (text/html)
Frame 115: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Device\NPF_{9AD0EF15-680B-4F7E-9671-CD0987287E3C}, id
0
Ethernet II, Src: ZyxelCom_e9:9d:30 (e4:18:6b:e9:9d:30), Dst: Tp-LinkT_e0:ac:16 (98:48:27:e0:ac:16)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.42
Transmission Control Protocol, Src Port: 80, Dst Port: 56926, Seq: 1, Ack: 497, Len: 717
Hypertext Transfer Protocol
  HTTP/1.1 401 Unauthorized\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
      [HTTP/1.1 401 Unauthorized\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Response Version: HTTP/1.1
    Status Code: 401
    [Status Code Description: Unauthorized]
    Response Phrase: Unauthorized
    Date: Tue, 14 Sep 2021 19:17:45 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.22 mod_perl/2.0.11 Perl/v5.16.3\r\n
    WWW-Authenticate: Basic realm="wireshark-students only"\r\n
    Content-Length: 381\r\n
    [Content length: 381]
    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: 0.121268000 seconds]
    [Request in frame: 107]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
    File Data: 381 bytes
Line-based text data: text/html (12 lines)
<!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
No.      Time           Source           Destination      Protocol Length Info
 1059 13:18:01.524239 192.168.0.42     128.119.245.12   HTTP             635     GET /wireshark-labs/protected_pages/HTTP-wireshark-
File5.html HTTP/1.1
Frame 1059: 635 bytes on wire (5080 bits), 635 bytes captured (5080 bits) on interface \Device\NPF_{9AD0EF15-680B-4F7E-9671-CD0987287E3C}, id
0
Ethernet II, Src: Tp-LinkT_e0:ac:16 (98:48:27:e0:ac:16), Dst: ZyxelCom_e9:9d:30 (e4:18:6b:e9:9d:30)
Internet Protocol Version 4, Src: 192.168.0.42, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 63714, Dst Port: 80, Seq: 1, Ack: 1, Len: 581
Hypertext Transfer Protocol
  GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
```

Julian Garcia
CSE 353: HW2

```
[Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
[GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
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
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcm5=\r\n
Credentials: wireshark-students:network
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36 Edg/93.0.961.47\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\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: 1155]
No.    Time                Source                Destination            Protocol Length Info
1155 13:18:02.447868      128.119.245.12         192.168.0.42           HTTP 544 HTTP/1.1 200 OK (text/html)
Frame 1155: 544 bytes on wire (4352 bits), 544 bytes captured (4352 bits) on interface \Device\NPF_{9AD0EF15-6B0B-4F7E-9671-CD0987287E3C}, id 0
Ethernet II, Src: ZyxelCom_e9:9d:30 (e4:18:6b:e9:9d:30), Dst: Tp-LinkT_e0:ac:16 (98:48:27:e0:ac:16)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.42
Transmission Control Protocol, Src Port: 80, Dst Port: 63714, Seq: 1, Ack: 582, Len: 490
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]
  Response Version: HTTP/1.1
  Status Code: 200
  [Status Code Description: OK]
  Response Phrase: OK
  Date: Tue, 14 Sep 2021 19:18:02 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.22 mod_perl/2.0.11 Perl/v5.16.3\r\n
  Last-Modified: Tue, 14 Sep 2021 05:59:01 GMT\r\n
  ETag: "84-5cbee4743774e"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 132\r\n
  [Content length: 132]
  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: 0.923629000 seconds]
  [Request in frame: 1059]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
  File Data: 132 bytes
Line-based text data: text/html (6 lines)
  \n
  <html>\n
  \n
  This page is password protected! If you're seeing this, you've downloaded the page correctly <br>\n
  Congratulations!\n
  </html>
```