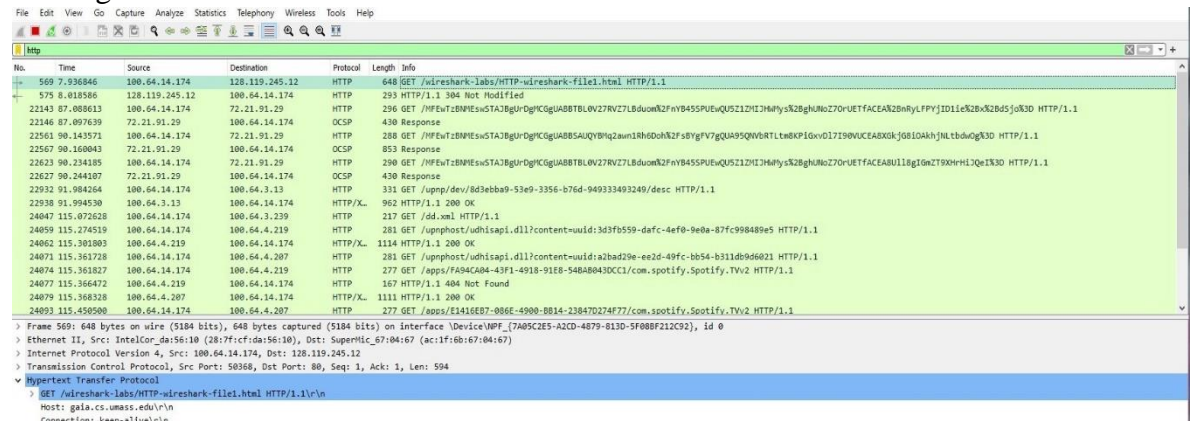


Lab 2 - Wireshark – HTTP

1. The Basic HTTP GET/response interaction

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 version 1.1. The version of HTTP the server is running is 1.1.



The screenshot shows a Wireshark packet capture of an HTTP GET request and response. The packet list on the left shows a GET request from 100.64.14.174 to 128.119.245.12 on port 80. The packet details pane on the right shows the request line: GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1. The response line shows: 200 OK. The packet bytes pane at the bottom shows the raw data of the request and response.

No.	Time	Source	Destination	Protocol	Length	Info
569	7.936846	100.64.14.174	128.119.245.12	HTTP	648	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
575	8.018586	128.119.245.12	100.64.14.174	HTTP	293	HTTP/1.1 200 Not Modified

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

The language that my browser indicate that it can accept to the server en-US.

```

Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
DNT: 1\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/94.0.4606.61 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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: "80-5cd809c1a605a"\r\n
If-Modified-Since: Mon, 04 Oct 2021 05:59:02 GMT\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: 575]
```

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

The IP address of my computer is 100.64.14.174 and the gaia.cs.umass.edu server is 128.119.245.12

No.	Time	Source	Destination	Protocol	Length	Info
569	7.936846	100.64.14.174	128.119.245.12	HTTP	648	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
575	8.018586	128.119.245.12	100.64.14.174	HTTP	293	HTTP/1.1 200 Not Modified

Youser Alalusi
CSC 138 – 01
10/07/2021

```
24077 115.366472 100.64.4.219 100.64.14.174 HTTP 167 HTTP/1.1 404 Not Found
24079 115.368328 100.64.4.207 100.64.14.174 HTTP/X- 1111 HTTP/1.1 200 OK
```

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

The status code returned from the server to my browser is 200.

```
24074 115.361827 100.64.14.174 100.64.4.219 HTTP 277 GET /apps/FA94CA04-43F1-4918-91E8-548AB043DCC1/com.spotify.Spotify.TVv2 HTTP/1.1
24077 115.366472 100.64.4.219 100.64.14.174 HTTP 167 HTTP/1.1 404 Not Found
24079 115.368328 100.64.4.207 100.64.14.174 HTTP/X- 1111 HTTP/1.1 200 OK
24093 115.450500 100.64.14.174 100.64.4.207 HTTP 277 GET /apps/E1416EB7-086E-4900-8B14-23847D274F77/com.spotify.Spotify.TVv2 HTTP/1.1

> Frame 24079: 1111 bytes on wire (8888 bits), 1111 bytes captured (8888 bits) on interface \Device\NPF_{7A05C2E5-A2CD-4879-813D-5F088F212C92}, id 0
> Ethernet II, Src: Microsof_90:1a:e7 (04:27:28:90:1a:e7), Dst: IntelCor_da:56:10 (28:7f:cf:da:56:10)
> Internet Protocol Version 4, Src: 100.64.4.207, Dst: 100.64.14.174
> Transmission Control Protocol, Src Port: 2869, Dst Port: 58181, Seq: 291, Ack: 228, Len: 1057
> [2 Reassembled TCP Segments (1347 bytes): #24078(290), #24079(1057)]
< Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
  > Content-Length: 1057\r\n
  > Content-Type: text/xml; charset=utf-8\r\n
  Server: Microsoft-Windows/10.0 UPnP/1.0 UPnP-Device-Host/1.0 Microsoft-HTTPAPI/2.0\r\n
  Application-URL: http://100.64.4.207:10247/apps/E1416EB7-086E-4900-8B14-23847D274F77\r\n
  Date: Mon, 04 Oct 2021 21:41:21 GMT\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.006600000 seconds]
  [Request in frame: 24071]
```

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

The HTML file that I was retrieving was last modified at the server on Mon, 04 OCT 2021 21:41:21 GMT.

```
> Transmission Control Protocol, Src Port: 2869, Dst Port: 58181, Seq: 291, Ack: 228, Len: 1057
> [2 Reassembled TCP Segments (1347 bytes): #24078(290), #24079(1057)]
< Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
  > Content-Length: 1057\r\n
  > Content-Type: text/xml; charset=utf-8\r\n
  Server: Microsoft-Windows/10.0 UPnP/1.0 UPnP-Device-Host/1.0 Microsoft-HTTPAPI/2.0\r\n
  Application-URL: http://100.64.4.207:10247/apps/E1416EB7-086E-4900-8B14-23847D274F77\r\n
  Date: Mon, 04 Oct 2021 21:41:21 GMT\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.006600000 seconds]
  [Request in frame: 24071]
```

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

1057 bytes of content are being returned to my browser.

```
24074 115.361827 100.64.14.174 100.64.4.219 HTTP 277 GET /apps/FA94CA04-43F1-4918-91E8-548AB043DCC1/com.spotify.Spotify.TVv2 HTTP/1.1
24077 115.366472 100.64.4.219 100.64.14.174 HTTP 167 HTTP/1.1 404 Not Found
24079 115.368328 100.64.4.207 100.64.14.174 HTTP/X- 1111 HTTP/1.1 200 OK
24093 115.450500 100.64.14.174 100.64.4.207 HTTP 277 GET /apps/E1416EB7-086E-4900-8B14-23847D274F77/com.spotify.Spotify.TVv2 HTTP/1.1

Frame 24079: 1111 bytes on wire (8888 bits), 1111 bytes captured (8888 bits) on interface \Device\NPF_{7A05C2E5-A2CD-4879-813D-5F088F212C92}, id 0
Ethernet II, Src: Microsof_90:1a:e7 (04:27:28:90:1a:e7), Dst: IntelCor_da:56:10 (28:7f:cf:da:56:10)
Internet Protocol Version 4, Src: 100.64.4.207, Dst: 100.64.14.174
Transmission Control Protocol, Src Port: 2869, Dst Port: 58181, Seq: 291, Ack: 228, Len: 1057
[2 Reassembled TCP Segments (1347 bytes): #24078(290), #24079(1057)]
< Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
  > Content-Length: 1057\r\n
  > Content-Type: text/xml; charset=utf-8\r\n
  Server: Microsoft-Windows/10.0 UPnP/1.0 UPnP-Device-Host/1.0 Microsoft-HTTPAPI/2.0\r\n
  Application-URL: http://100.64.4.207:10247/apps/E1416EB7-086E-4900-8B14-23847D274F77\r\n
  Date: Mon, 04 Oct 2021 21:41:21 GMT\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.006600000 seconds]
  [Request in frame: 24071]
  File Data: 1057 bytes
  eXtensible Markup Language
```

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.

No there is none.

2. The HTTP **CONDITIONAL GET/response** interaction

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?

There is an “IF-MODIFIED-SINCE” line in the HTTP GET and the date is Mon, 24 OCT 2021 at 05:25:02 GMT.

No.	Time	Source	Destination	Protocol	Length	Info
569	7.936846	100.64.14.174	128.119.245.12	HTTP	648	GET /wireshark-labs/HTTP-wireshark-file.html HTTP/1.1
575	8.018586	128.119.245.12	100.64.14.174	HTTP	203	HTTP/1.1 304 Not Modified
22148	87.088613	100.64.14.174	72.21.91.29	HTTP	296	GET /HFEvTzBNfEswSTAj8gUgICgUABBTBL0VZ7RVZ7L8duomK2FnYB455PUeWQ5ZlZlHJmHysxK28gHNoZ70VUETFACEA8ZbnRfLPYj1Dl1eK28xK28d5j0K3D HTTP/1.1
22146	87.097639	72.21.91.29	100.64.14.174	OCSP	430	Response
22561	90.143571	100.64.14.174	72.21.91.29	HTTP	288	GET /HFEvTzBNfEswSTAj8gUgICgUABSAQYbQzawn1Rh6dohK2FnYB455PUeWQ5ZlZlHJmHysxK28gHNoZ70VUETFACEA8XKj08iAkhJnlbtuohgK3D HTTP/1.1
22567	90.160043	72.21.91.29	100.64.14.174	OCSP	853	Response
26262	90.234195	100.64.14.174	72.21.91.29	HTTP	296	GET /HFEvTzBNfEswSTAj8gUgICgUABTBL0VZ7RVZ7L8duomK2FnYB455PUeWQ5ZlZlHJmHysxK28gHNoZ70VUETFACEA8U1l8gImZT9XhHh1j0eK3D HTTP/1.1
26267	90.244107	72.21.91.29	100.64.14.174	OCSP	430	Response
29332	91.584264	100.64.14.174	100.64.1.13	HTTP	331	GET /uuprp/dev/8d3ebba9-53e9-3356-b76d-949333493249/desc HTTP/1.1
29338	91.594530	100.64.1.13	100.64.14.174	HTTP/XL	962	HTTP/1.1 200 OK
24047	115.072628	100.64.14.174	100.64.4.239	HTTP	217	GET /dd.xml HTTP/1.1
24059	115.274519	100.64.14.174	100.64.4.219	HTTP	281	GET /uuprhst/udhisap1.d11?content=uid:3d3fb559-dafc-4ef0-9e0a-87fc998489e5 HTTP/1.1
24062	115.301803	100.64.4.219	100.64.14.174	HTTP/XL	1114	HTTP/1.1 200 OK
24071	115.361728	100.64.14.174	100.64.4.207	HTTP	281	GET /uuprhst/udhisap1.d11?content=uid:a2bad29e-ee2d-49fc-bb54-b311db9d0021 HTTP/1.1
24074	115.361728	100.64.14.174	100.64.4.219	HTTP	277	GET /apps/FA04CA40-63F1-4918-91E8-54B48043DCC1/com.spotify.Spotify.TVv2 HTTP/1.1
24077	115.366472	100.64.4.219	100.64.14.174	HTTP	167	HTTP/1.1 404 Not Found
24079	115.368328	100.64.4.207	100.64.14.174	HTTP/XL	1111	HTTP/1.1 200 OK
24083	115.450500	100.64.14.174	100.64.4.207	HTTP	277	GET /apps/E1416EB7-086E-4800-8B14-23847D274F77/com.spotify.Spotify.TVv2 HTTP/1.1

Frame 569: 648 bytes on wire (5184 bits), 648 bytes captured (5184 bits) on interface Device\NPF_{7A093C25-A2C0-4879-813D-F508BF212C92}, id 0

Ethernet II, Src: IntelCor_da:56:10 (28:7f:cf:da:56:10), Dst: SuperMic_67:04:67 (ac:1f:6b:67:04:67)

Internet Protocol Version 4, Src: 100.64.14.174, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 50368, Dst Port: 80, Seq: 1, Ack: 1, Len: 594

Hypertext Transfer Protocol

GET /wireshark-labs/HTTP-wireshark-file.html HTTP/1.1\r\n

Host: gaia.cs.umass.edu\r\n

Connection: keep-alive\r\n

Cache-Control: max-age=0\r\n

DNT: 1\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/94.0.4606.61 Safari/537.36\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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: "80-5cd089c1a605a"\r\n

If-Modified-Since: Mon, 04 Oct 2021 05:59:02 GMT\r\n

\r\n

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file.html]

[HTTP request 1/1]

[Response line: 575]

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 return the contents of the file and you can tell because the content is shown in the section “Line-based test data: text/html.”

```
HyperText Transfer Protocol
> HTTP/1.1 200 OK\r\n
Date: Thu, 07 Oct 2021 18:26:55 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Thu, 07 Oct 2021 05:59:01 GMT\r\n
ETag: "173-Scdbcf5957dd6"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 371\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.078690000 seconds]
[Request in frame: 783]
[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)
\r\n
<html>\r\n
\r\n
Congratulations again! Now you've downloaded the file lab2-2.html. <br>\r\n
This file's last modification date will not change. <p>\r\n
Thus if you download this multiple times on your browser, a complete copy <br>\r\n
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\r\n
field in your browser's HTTP GET request to the server.\r\n
\r\n
</html>\r\n
```

- 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?

I do see an “IF-MODIFIED-SINCE:” line in the HTTP GET. The information that follows in the header is Mon, 04 Oct 2021 05:59:02 GMT.

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 HTTP status code and phrase returned from the server in response to this second HTTP GET is 304 and Not Modified. The server did not explicitly return the contents of the file because the second HTTP GET request sent by the browser included the “IF-MOTIFIED-SINCE” header and since the file on the server has not been modified sinve the time

Youser Alalusi

CSC 138 – 01

10/07/2021

specidiewd by the IF MODIFIED SINCE header, the server simply responds that it has not been modified instead of retuening the contents of the file again.

```
> Transmission Control Protocol, Src Port: 80, Dst Port: 62850, Seq: 1, Ack: 594, Len: 241
  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]
```

3. Retrieving Long Documents

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?

The HTTP GET request messages that my browser send was 1288. The packet number in the trace that GET message for the Bill or Rights is 122336.

No.	Time	Source	Destination	Protocol	Length	Info
42960	907.016100	100.64.14.174	100.64.15.59	HTTP	332	GET /upnp/dev/10e8208c-ddd7-30f3-ad2e-51961a3a0e46/desc HTTP/1.1
42967	907.042370	100.64.15.59	100.64.14.174	HTTP/XL	955	HTTP/1.1 200 OK
122336	1288.524575	100.64.14.174	128.119.245.12	HTTP	647	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
122340	1289.004745	128.119.245.12	100.64.14.174	HTTP	295	HTTP/1.1 304 Not Modified
128493	1413.532858	100.64.14.174	104.114.77.27	HTTP	336	GET /msdownload/update/v3/static/trusted/en/pinrulesstl.cab?Seu54063d6809e6f HTTP/1.1
138405	1413.641438	104.114.77.27	100.64.14.174	HTTP	376	HTTP/1.1 304 Not Modified

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

The packet number in the trace that contains the status code and phrase associated with the response to the HTTP GET request is 4264.

No.	Time	Source	Destination	Protocol	Length	Info
4242	57.814944	100.64.14.174	128.119.245.12	HTTP	537	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
4264	57.896326	128.119.245.12	100.64.14.174	HTTP	535	HTTP/1.1 200 OK (text/html)

```
> Frame 4264: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{7A05C2E5-A2CD-4879-B13D-5F088F212C92}, id 0
> Ethernet II, Src: SuperMicro 67:04:67 (ac:1f:6b:67:04:67), Dst: IntelCor_da:56:10 (28:7f:cfcf:da:56:10)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 100.64.14.174
> Transmission Control Protocol, Src Port: 80, Dst Port: 50432, Seq: 4381, Ack: 484, Len: 481
> [4 Reassembled TCP Segments (4861 bytes): #4260(1460), #4261(1460), #4262(1460), #4264(481)]
  Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
      Date: Thu, 07 Oct 2021 19:01:37 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3\r\n
      Last-Modified: Thu, 07 Oct 2021 09:59:01 GMT\r\n
      ETag: "1104-Scd8cf595433e"\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: 0.081382000 seconds]
      [Request in frame: 4242]
      [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></p>\n
      <em>Amendments 1-10 of the Constitution</em>\n
      </center>\n
      \n
      <p><p><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><a name="1"><strong><h3>Amendment I</h3></strong></a>\n
      \n
      <p></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
      \n
      </p><p><a name="2"><strong><h3>Amendment II</h3></strong></a>\n
      \n
      <p></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
      \n
      </p><p><a name="3"><strong><h3>Amendment III</h3></strong></a>\n
      \n
      <p></p><p><p>No soldier shall, in time of peace be quartered in any house,\n
```

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

The status code and phrase in the response is 200 and OK.


```
Frame 4264: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{7A05C2E5-A2CD-4879-813D-5F08BF212C92}, id 0
Ethernet II, Src: SuperMic_67:04:67 (ac:1f:6b:67:04:67), Dst: IntelCor_da:56:10 (28:7f:cf:da:56:10)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 100.64.14.174
Transmission Control Protocol, Src Port: 80, Dst Port: 50432, Seq: 4381, Ack: 484, Len: 481
[4 Reassembled TCP Segments (4861 bytes): #4260(1460), #4261(1460), #4262(1460), #4264(481)]
Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
  Date: Thu, 07 Oct 2021 19:01:37 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3\r\n
  Last-Modified: Thu, 07 Oct 2021 05:59:01 GMT\r\n
  ETag: "1194-5cdbcf595433e"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 4500\r\n
  Keep-Alive: timeout=5, max=100\r\n
```

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

Four data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights.

```
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 100.64.14.174
> Transmission Control Protocol, Src Port: 80, Dst Port: 50432, Seq: 4381, Ack: 484, Len: 481
  [4 Reassembled TCP Segments (4861 bytes): #4260(1460), #4261(1460), #4262(1460), #4264(481)]
    [Frame: 4260, payload: 0-1459 (1460 bytes)]
    [Frame: 4261, payload: 1460-2919 (1460 bytes)]
    [Frame: 4262, payload: 2920-4379 (1460 bytes)]
    [Frame: 4264, payload: 4380-4860 (481 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a205468752c203037204f63742032...]
  > Hypertext Transfer Protocol
  > Line-based text data: text/html (98 lines)
```

4. HTML Documents with Embedded Objects

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

There are three HTTP GET request messages that my browser sent.

Time	Source IP	Destination IP	Protocol	Request
4242	57.814944	100.64.14.174	HTTP	537 GET /wiresark-labs/HTTP-wiresark-file3.html HTTP/1.1
4264	57.896326	128.119.245.12	HTTP	535 HTTP/1.1 200 OK (text/html)
23207	423.724516	100.64.14.174	HTTP	508 GET /kurose_ross HTTP/1.1
23211	423.807955	128.119.245.12	HTTP	632 HTTP/1.1 301 Moved Permanently (text/html)
23212	423.811137	100.64.14.174	HTTP	509 GET /kurose_ross/ HTTP/1.1
23213	423.893907	128.119.245.12	HTTP	649 HTTP/1.1 301 Moved Permanently (text/html)
23214	423.897477	100.64.14.174	HTTP	518 GET /kurose_ross/index.php HTTP/1.1
23223	423.982275	128.119.245.12	HTTP	379 HTTP/1.1 200 OK (text/html)
23225	424.036184	100.64.14.174	HTTP	429 GET /kurose_ross/custom.css HTTP/1.1
23228	424.037726	128.119.245.12	HTTP	413 GET /kurose_ross/script.js HTTP/1.1
23314	424.119533	128.119.245.12	HTTP	101 HTTP/1.1 200 OK (text/css)
23316	424.121249	100.64.14.174	HTTP	493 GET /kurose_ross/header_graphic_book_8E_3.jpg HTTP/1.1
23318	424.124453	128.119.245.12	HTTP	1349 HTTP/1.1 200 OK (application/javascript)
23625	424.466068	128.119.245.12	HTTP	596 HTTP/1.1 200 OK (JPEG JFIF image)
23995	429.472152	100.64.12.164	HTTP	369 GET /upphost/udhisapi.dll?content=uid:fae91469-05a7-4762-abe4-e309f77c6538 HTTP/1.1
24134	431.424813	100.64.12.164	HTTP	353 GET /upphost/udhisapi.dll?content=uid:fae91469-05a7-4762-abe4-e309f77c6538 HTTP/1.1
24140	431.454044	100.64.12.164	HTTP/XL	1114 HTTP/1.1 200 OK

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.

The browser downloaded that the browser sent the HTTP GET request message for the second image after the HTTP response for the first image was received.

5 HTTP Authentication

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 in response to the initial HTTP GET message from browser is 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?

Youser Alalusi

CSC 138 – 01

10/07/2021

The new field that is included in the HTTP GET message is Authorization: Basic.