

Anthony Chavez

Professor Sun

Lab 2 – Wireshark – HTTP Lab

The Basic HTTP Get/response interaction

No.	Time	Source	Destination	Protocol	Length	Info
9	00:57:25.575371	10.0.0.236	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
11	00:57:25.678089	128.119.245.12	10.0.0.236	HTTP	540	HTTP/1.1 200 OK (text/html)
27	00:57:25.797485	10.0.0.236	128.119.245.12	HTTP	389	GET /favicon.ico HTTP/1.1
60	00:57:25.896299	128.119.245.12	10.0.0.236	HTTP	538	HTTP/1.1 404 Not Found (text/html)

> Ethernet II, Src: LiteonTe_95:eb:c7 (64:6e:69:95:eb:c7), Dst: Technico_f4:da:f5 (f4:c1:14:f4:da:f5)

> Internet Protocol Version 4, Src: 10.0.0.236, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 56750, Dst Port: 80, Seq: 1, Ack: 1, Len: 378

> Hypertext Transfer Protocol

> GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\nAccept-Language: en-US,en;q=0.5\r\nAccept-Encoding: gzip, deflate\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\n\r\n[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]\n[HTTP request 1/2]\n[Response in frame: 11]\n[Next request in frame: 27]

Here are the http packets I captured following the provided instructions. Please ignore packets 27 and 60 as they do not pertain to the scope of this experiment.

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

No.	Time	Source	Destination	Protocol	Length	Info
9	00:57:25.575371	10.0.0.236	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
11	00:57:25.678089	128.119.245.12	10.0.0.236	HTTP	540	HTTP/1.1 200 OK (text/html)
27	00:57:25.797485	10.0.0.236	128.119.245.12	HTTP	389	GET /favicon.ico HTTP/1.1
60	00:57:25.896299	128.119.245.12	10.0.0.236	HTTP	538	HTTP/1.1 404 Not Found (text/html)

> Ethernet II, Src: LiteonTe_95:eb:c7 (64:6e:69:95:eb:c7), Dst: Technico_f4:da:f5 (f4:c1:14:f4:da:f5)

> Internet Protocol Version 4, Src: 10.0.0.236, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 56750, Dst Port: 80, Seq: 1, Ack: 1, Len: 378

> Hypertext Transfer Protocol

> GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\nAccept-Language: en-US,en;q=0.5\r\nAccept-Encoding: gzip, deflate\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\n\r\n[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]\n[HTTP request 1/2]\n[Response in frame: 11]\n[Next request in frame: 27]

- a. As marked by the red rectangles in the image above, my browser is running HTTP version 1.1

No.	Time	Source	Destination	Protocol	Length	Info
9	00:57:25.575371	10.0.0.236	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
11	00:57:25.678089	128.119.245.12	10.0.0.236	HTTP	540	HTTP/1.1 200 OK (text/html)
27	00:57:25.797485	10.0.0.236	128.119.245.12	HTTP	389	GET /favicon.ico HTTP/1.1
60	00:57:25.896299	128.119.245.12	10.0.0.236	HTTP	538	HTTP/1.1 404 Not Found (text/html)


```

> Ethernet II, Src: Technico_f4:da:f5 (f4:c1:14:f4:da:f5), Dst: LiteonTe_95:eb:c7 (64:6e:69:95:eb:c7)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.236
> Transmission Control Protocol, Src Port: 80, Dst Port: 56750, Seq: 1, Ack: 379, Len: 486
> Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Wed, 28 Oct 2020 07:57:26 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.11 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Wed, 28 Oct 2020 05:59:02 GMT\r\n
    ETag: "80-5b2b4dc3cfc7d"\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 1/2]
  [Time since request: 0.102718000 seconds]
  [Request in frame: 9]

```

- b. As marked by the red rectangles in the image above, the server is running HTTP 1.1

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

```

> Ethernet II, Src: LiteonTe_95:eb:c7 (64:6e:69:95:eb:c7), Dst: Technico_f4:da:f5 (f4:c1:14:f4:da:f5)
> Internet Protocol Version 4, Src: 10.0.0.236, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 56750, Dst Port: 80, Seq: 1, Ack: 1, Len: 378
> Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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-file1.html]
  [HTTP request 1/2]
  [Response in frame: 11]
  [Next request in frame: 27]

```

- a. en-US, indicated by the red rectangle in the image above.

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

No.	Time	Source	Destination	Protocol	Length	Info
9	00:57:25.575371	10.0.0.236	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
11	00:57:25.678089	128.119.245.12	10.0.0.236	HTTP	540	HTTP/1.1 200 OK (text/html)

- a. My computer IP address is 10.0.0.236 (red rectangles) and the server IP address is 128.119.245.12 (black rectangles).

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

No.	Time	Source	Destination	Protocol	Length	Info
9	00:57:25.575371	10.0.0.236	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
11	00:57:25.678089	128.119.245.12	10.0.0.236	HTTP	540	HTTP/1.1 200 OK (text/html)

- a. 200 OK is the status code returned from the server to my browser.

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

```

Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
Date: Wed, 28 Oct 2020 07:57:26 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.11 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Wed, 28 Oct 2020 05:59:02 GMT\r\n
ETag: "80-5b2b4dc3cfc7d"\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

```

- a. The HTML file was last modified on Wednesday, 28 Oct 2020 05:59:02 GMT.
See red rectangle in the image above.

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

```

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.11 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Wed, 28 Oct 2020 05:59:02 GMT\r\n
ETag: "80-5b2b4dc3cfc7d"\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 1/2]
[Time since request: 0.102718000 seconds]
[Request in frame: 9]
[Next request in frame: 27]
[Next response in frame: 60]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
File Data: 128 bytes

```

- a. 128 bytes of content are being returned to my browser as shown in the above image.

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.

0000	f4 c1 14 f4 da f5 64 6e 69 95 eb c7 08 00 45 00dn i.....E	0000	64 6e 69 95 eb c7 f4 c1 14 f4 da f5 08 00 45 00	dn.....E
0010	01 a2 d0 3f 40 00 80 06 a8 a6 0a 00 00 ec 80 77?@.....w	0010	02 0e 34 e0 40 00 1d 06 a6 9a 80 77 f5 0c 0a 00	...4 @...w...
0020	f5 0c dd ae 00 50 b6 00 83 5b ae c1 14 62 50 18P...[...bP	0020	00 ec 00 50 dd ae ae c1 14 62 b6 00 84 d5 50 18	...P...b...P
0030	02 01 0f 9b 00 00 47 45 54 20 2f 77 69 72 65 73GE T/wires	0030	00 ed 5f 5e 00 00 48 54 54 50 2f 31 2e 31 20 32	...^...HT TP/1.1 2
0040	68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77	hark-lab s/HTTP-w	0040	30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 57 65 64	00 OK...D ate: Wed
0050	69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68	ireshark -file1.h	0050	2c 20 32 38 20 4f 63 74 20 32 30 32 30 20 30 37	, 28 Oct 2020 07
0060	74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f	tml HTTP /1.1..Ho	0060	3a 35 37 3a 32 36 20 47 4d 54 0d 0a 53 65 72 76	:57:26 G MT...Serv
0070	73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73	st: gaia .cs.umas	0070	65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36	er: Apac he/2.4.6
0080	73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67 65 6e	s.edu...U ser-Agen	0080	20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53	(CentOS) OpenSS
0090	74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28	t: Mozil la/5.0 (0090	4c 2f 31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48	L/1.0.2k -fips PH
00a0	20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b	Windows NT 10.0;	00a0	50 2f 32 2e 3a 2e 31 31 20 6d 6f 64 5f 70 65 72	P/7.4.11 mod_per
00b0	6e 67 75 61 67 65 3a 20 65 6e 2d 55 53 2c 65 6e	Win64; x64; rv:	00b0	6c 2f 32 2e 30 2e 31 31 20 50 65 72 6c 2f 76 35	l/2.0.11 Perl/v5
00c0	38 31 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 30	81.0) Gecko/2010	00c0	2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69	.16.3... last-Modi
00d0	30 31 30 31 20 46 69 72 65 66 6f 78 2f 38 31 2e	0101 Firefox/81.	00d0	66 69 65 64 3a 20 57 65 64 2c 20 32 38 20 4f 63	fied: We d, 28 Oc
00e0	30 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f	0...Accept t: text/	00e0	74 20 32 30 32 30 20 30 35 3a 35 39 3a 30 32 20	t 2020 0 5:59:02
00f0	68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e	html,application	00f0	47 4d 54 0d 0a 45 54 61 67 3a 20 22 38 20 4f 63	GMT...ETA g: "80-5
0100	2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69	/xhtml+xml,appli	0100	62 32 62 34 64 63 33 63 66 63 37 64 22 0d 0a 41	b2b4dc3c fc7d"...A
0110	63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39	cation/x ml;q=0.9	0110	63 63 65 70 74 2d 52 61 6e 67 65 73 3a 20 62 79	ccept-Ra nges: by
0120	2c 69 6d 61 67 65 2f 77 65 62 70 2c 2a 2f 2a 3b	,image/w ebp,*/*;	0120	74 65 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e	tes...Con tent-Len
0130	71 3d 30 2e 38 0d 0a 41 63 63 65 70 74 2d 4c 61	q=0.8...A ccept-La	0130	67 74 68 3a 20 31 32 38 0d 0a 4b 65 65 70 2d 41	gth: 128 ...Keep-A
0140	6e 67 75 61 67 65 3a 20 65 6e 2d 55 53 2c 65 6e	nguage: en-US,en	0140	6c 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c	live: t1 meout=5,
0150	3b 71 3d 30 2e 35 0d 0a 41 63 63 65 70 74 2d 45	;q=0.5... Accept-E	0150	20 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63	max=100 ...Connec
0160	6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64	ncoding: gzip, d	0160	74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65	tion: Ke ep-Alive
0170	65 66 6c 61 74 65 0d 0a 43 6f 6e 6e 65 63 74 69	eflate... Connecti	0170	0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20	...Conten t-Type:
0180	6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a	on: keep -alive...	0180	74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73	text/htm l; chars
0190	55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65	Upgrade- Insecure	0190	65 74 3d 55 54 46 2d 38 0d 0a 0d 0a 3c 68 74 6d	et=UTF-8 ...<htm
01a0	2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 0d 0a	-Request s: 1... ..	01a0	6c 3e 0a 43 6f 6e 67 72 61 74 75 6c 61 74 69 6f	l>. Congr atulatio
			01b0	6e 73 2e 20 20 59 6f 75 27 76 65 20 64 6f 77 6e	ns. You 've down
			01c0	6c 6f 61 64 65 64 20 74 68 65 20 66 69 6c 65 20	loaded t he file
			01d0	0a 68 74 74 70 3a 2f 2f 67 61 69 61 2e 63 73 2e	...http:// gaia.cs.
			01e0	75 6d 61 73 73 2e 65 64 75 2f 77 69 72 65 73 68	umass.ed u/wiresh
			01f0	71 62 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 69	ark-lab s /HTTP-wi
			0200	62 75 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68 74	reshark- file1.ht
			0210	6d 6c 21 0a 3c 2f 68 74 6d 6c 3e 0a	ml</>ht ml>.

- a. No additional headers within the data that are not displayed in the packet-listing window. Raw data of GET packet on the left and raw data of 200 OK packet on the right.

The HTTP Conditional GET/response interaction

No.	Time	Source	Destination	Protocol	Length	Info
9	01:44:58.750684	10.0.0.236	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
12	01:44:58.868848	128.119.245.12	10.0.0.236	HTTP	784	HTTP/1.1 200 OK (text/html)
28	01:44:58.984109	10.0.0.236	128.119.245.12	HTTP	389	GET /favicon.ico HTTP/1.1
45	01:44:59.086639	128.119.245.12	10.0.0.236	HTTP	538	HTTP/1.1 404 Not Found (text/html)
107	01:45:12.103942	10.0.0.236	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
109	01:45:12.210299	128.119.245.12	10.0.0.236	HTTP	294	HTTP/1.1 304 Not Modified

Here are the http packets I captured following the provided instructions. Please ignore packets 28 and 45 as they do not pertain to the scope of this experiment.

1. 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]
    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 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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: 12]
    [Next request in frame: 28]
```

- a. As can be seen in the above image, the first HTTP GET request from the browser to the server does not contain an “IF-MODIFIED-Since:” line in the HTTP GET.
2. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    Date: Wed, 28 Oct 2020 08:44:59 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.11 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Wed, 28 Oct 2020 05:59:02 GMT\r\n
    ETag: "173-5b2b4dc3cecd"\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: 0.118164000 seconds]
    [Request in frame: 9]
    [Next request in frame: 28]
    [Next response in frame: 45]
    [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 IF-MODIFIED-SINCE<br>\n
    field in your browser's HTTP GET request to the server.\n
    \n
    </html>\n
```

- a. The server explicitly returned the contents of the file. Refer to the Line-based text data segment indicated by the red rectangle in the above image.

3. 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?

```
▼ Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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: Wed, 28 Oct 2020 05:59:02 GMT\r\n
    If-None-Match: "173-5b2b4dc3cecdd"\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: 109]
```

- a. As we can see in the above image, the second HTTP GET request from the browser to the server does contain an “IF-MODIFIED-SINCE:” line in the HTTP GET. The information that follows the “IF-MODIFIED-SINCE:” header is the time condition of when to update the cached object.
4. 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.

```
▼ Hypertext Transfer Protocol
  > HTTP/1.1 304 Not Modified\r\n
    Date: Wed, 28 Oct 2020 08:45:12 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.11 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "173-5b2b4dc3cecdd"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.106357000 seconds]
    [Request in frame: 107]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

- a. The HTTP status code and phrase returned from the server in response to this second HTTP GET is “304 Not Modified”. Since the “If-Modified-Since:” time condition was not met, the cached object is considered up to date. We avoided meeting this condition by quickly refreshing the page. Therefore, the server did not explicitly return the contents of the file for the second HTTP GET.

Retrieving Long Documents

No.	Time	Source	Destination	Protocol	Length	Info
15	02:17:13.795144	10.0.0.236	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
22	02:17:13.897311	128.119.245.12	10.0.0.236	HTTP	535	HTTP/1.1 200 OK (text/html)
37	02:17:14.014748	10.0.0.236	128.119.245.12	HTTP	389	GET /favicon.ico HTTP/1.1
51	02:17:14.113073	128.119.245.12	10.0.0.236	HTTP	538	HTTP/1.1 404 Not Found (text/html)

```
TCP segment data (481 bytes)
> [4 Reassembled TCP Segments (4861 bytes): #18(1460), #19(1460), #21(1460), #22(481)]
> Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Wed, 28 Oct 2020 09:17:14 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.11 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Wed, 28 Oct 2020 05:59:02 GMT\r\n
    ETag: "1194-5b2b4dc3c6424"\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 1/2]
  [Time since request: 0.102167000 seconds]
  [Request in frame: 15]
  [Next request in frame: 37]
  [Next response in frame: 51]
  [Request URI: http://gaia.cs.umass.edu/favicon.ico]
  File Data: 4500 bytes
> Line-based text data: text/html (98 lines)
```

Here are the http packets I captured following the provided instructions. Please ignore packets 37 and 51 as they do not pertain to the scope of this experiment.

1. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill of Rights?

No.	Time	Source	Destination	Protocol	Length	Info
15	02:17:13.795144	10.0.0.236	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
22	02:17:13.897311	128.119.245.12	10.0.0.236	HTTP	535	HTTP/1.1 200 OK (text/html)
37	02:17:14.014748	10.0.0.236	128.119.245.12	HTTP	389	GET /favicon.ico HTTP/1.1
51	02:17:14.113073	128.119.245.12	10.0.0.236	HTTP	538	HTTP/1.1 404 Not Found (text/html)

- a. My browser sent only 1 HTTP GET request message. The packet number in the trace that contains the GET message for the Bill of Rights is 15.
2. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

No.	Time	Source	Destination	Protocol	Length	Info
15	02:17:13.795144	10.0.0.236	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
22	02:17:13.897311	128.119.245.12	10.0.0.236	HTTP	535	HTTP/1.1 200 OK (text/html)
37	02:17:14.014748	10.0.0.236	128.119.245.12	HTTP	389	GET /favicon.ico HTTP/1.1
51	02:17:14.113073	128.119.245.12	10.0.0.236	HTTP	538	HTTP/1.1 404 Not Found (text/html)

- a. Packet number 22 contains the status code and phrase associated with the response to the HTTP GET request.
3. What is the status code and phrase in the response?

No.	Time	Source	Destination	Protocol	Length	Info
15	02:17:13.795144	10.0.0.236	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
22	02:17:13.897311	128.119.245.12	10.0.0.236	HTTP	535	HTTP/1.1 200 OK (text/html)
37	02:17:14.014748	10.0.0.236	128.119.245.12	HTTP	389	GET /favicon.ico HTTP/1.1
51	02:17:14.113073	128.119.245.12	10.0.0.236	HTTP	538	HTTP/1.1 404 Not Found (text/html)

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

4. 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): #18(1460), #19(1460), #21(1460), #22(481)]  
  [Frame: 18, payload: 0-1459 (1460 bytes)]  
  [Frame: 19, payload: 1460-2919 (1460 bytes)]  
  [Frame: 21, payload: 2920-4379 (1460 bytes)]  
  [Frame: 22, payload: 4380-4860 (481 bytes)]  
  [Segment count: 4]  
  [Reassembled TCP length: 4861]  
  [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a4461746553a2057...]
```

- a. 4 data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights.

HTML Documents with Embedded Objects

No.	Time	Source	Destination	Protocol	Length	Info
65	03:08:54.394255	10.0.0.236	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
67	03:08:54.513506	128.119.245.12	10.0.0.236	HTTP	1127	HTTP/1.1 200 OK (text/html)
128	03:08:54.805129	10.0.0.236	128.119.245.12	HTTP	389	GET /favicon.ico HTTP/1.1
134	03:08:54.907240	128.119.245.12	10.0.0.236	HTTP	538	HTTP/1.1 404 Not Found (text/html)
144	03:08:54.938725	10.0.0.236	128.119.245.12	HTTP	389	GET /pearson.png HTTP/1.1
196	03:08:55.044858	128.119.245.12	10.0.0.236	HTTP	745	HTTP/1.1 200 OK (PNG)
205	03:08:55.150541	10.0.0.236	128.119.245.12	HTTP	403	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
301	03:08:55.477882	128.119.245.12	10.0.0.236	HTTP	632	HTTP/1.1 200 OK (JPEG JFIF image)


```

> Frame 65: 432 bytes on wire (3456 bits), 432 bytes captured (3456 bits) on interface \Device\NPF_{269853DA-DD3B-4C3A-8517-9DE937CFB40}
> Ethernet II, Src: LiteonTe_95:eb:c7 (64:6e:69:95:eb:c7), Dst: Technico_f4:da:f5 (f4:c1:14:f4:da:f5)
> Internet Protocol Version 4, Src: 10.0.0.236, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 57542, Dst Port: 80, Seq: 1, Ack: 1, Len: 378
< Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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 1/3]
    [Response in frame: 67]
    [Next request in frame: 128]
  
```

Here are the http packets I captured following the provided instructions. Please ignore packets 128 and 134 as they do not pertain to the scope of this experiment.

- 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
65	03:08:54.394255	10.0.0.236	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
67	03:08:54.513506	128.119.245.12	10.0.0.236	HTTP	1127	HTTP/1.1 200 OK (text/html)
128	03:08:54.805129	10.0.0.236	128.119.245.12	HTTP	389	GET /favicon.ico HTTP/1.1
134	03:08:54.907240	128.119.245.12	10.0.0.236	HTTP	538	HTTP/1.1 404 Not Found (text/html)
144	03:08:54.938725	10.0.0.236	128.119.245.12	HTTP	389	GET /pearson.png HTTP/1.1
196	03:08:55.044858	128.119.245.12	10.0.0.236	HTTP	745	HTTP/1.1 200 OK (PNG)
205	03:08:55.150541	10.0.0.236	128.119.245.12	HTTP	403	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
301	03:08:55.477882	128.119.245.12	10.0.0.236	HTTP	632	HTTP/1.1 200 OK (JPEG JFIF image)

- A total of 3 HTTP GET request messages were sent by my browser.
 - Wireshark-labs/HTTP-wireshark-file4.html
 - Pearson.png
 - ~kurose/cover_5th_ed.jpg
- 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 the two images serially. The images could not have been downloaded from the two web sites in parallel as shown in the packet listing window. The browser sent an HTTP GET request packet for the pearson.png first and after receiving the image, only then sent another HTTP GET request packet for the second image.

HTTP Authentication

No.	Time	Source	Destination	Protocol	Length	Info
116	03:25:17.822001	2601:204:c401:33a0::...	2600:1901:0:38d7::...	HTTP	75	Continuation
118	03:25:17.898124	2601:204:c401:33a0::...	2600:1901:0:38d7::...	HTTP	75	Continuation
119	03:25:17.913338	10.0.0.236	34.107.221.82	HTTP	55	Continuation
136	03:25:18.657831	10.0.0.236	151.139.128.14	HTTP	55	Continuation
159	03:25:18.869915	10.0.0.236	128.119.245.12	HTTP	448	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
161	03:25:18.974171	128.119.245.12	10.0.0.236	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
261	03:25:37.631977	2601:204:c401:33a0::...	2600:1901:0:38d7::...	HTTP	372	GET /success.txt HTTP/1.1
263	03:25:37.649437	2600:1901:0:38d7::...	2601:204:c401:33a0::...	HTTP	294	HTTP/1.1 200 OK (text/plain)
266	03:25:37.651484	10.0.0.236	34.107.221.82	HTTP	357	GET /success.txt?ipv4 HTTP/1.1
268	03:25:37.652196	2601:204:c401:33a0::...	2600:1901:0:38d7::...	HTTP	377	GET /success.txt?ipv6 HTTP/1.1
270	03:25:37.668274	34.107.221.82	10.0.0.236	HTTP	274	HTTP/1.1 200 OK (text/plain)
272	03:25:37.673429	2600:1901:0:38d7::...	2601:204:c401:33a0::...	HTTP	294	HTTP/1.1 200 OK (text/plain)
319	03:25:38.413471	10.0.0.236	128.119.245.12	HTTP	507	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
323	03:25:38.517291	128.119.245.12	10.0.0.236	HTTP	544	HTTP/1.1 200 OK (text/html)
663	03:25:38.796255	10.0.0.236	128.119.245.12	HTTP	405	GET /favicon.ico HTTP/1.1
669	03:25:38.898688	128.119.245.12	10.0.0.236	HTTP	538	HTTP/1.1 404 Not Found (text/html)
711	03:25:40.242922	10.0.0.236	151.139.128.14	OCSP	434	Request
714	03:25:40.271837	151.139.128.14	10.0.0.236	OCSP	525	Response

```
> Frame 161: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Device\NPF_{269B53DA-DD3B-4C3A-8517-9DE937CFB405}, id 0
> Ethernet II, Src: Technico_f4:da:f5 (f4:c1:14:f4:da:f5), Dst: LiteonTe_95:eb:c7 (64:6e:69:95:eb:c7)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.236
> Transmission Control Protocol, Src Port: 80, Dst Port: 59671, Seq: 1, Ack: 395, Len: 717
< Hypertext Transfer Protocol
  < HTTP/1.1 401 Unauthorized\r\n
    Date: Wed, 28 Oct 2020 10:25:19 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.11 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
  < 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: 0.104256000 seconds]
  [Request in frame: 159]
  [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)
```

Here are the http packets I captured following the provided instructions. Please ignore packets 663 and 669 as they do not pertain to the scope of this experiment.

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

No.	Time	Source	Destination	Protocol	Length	Info
116	03:25:17.822001	2601:204:c401:33a0::...	2600:1901:0:38d7::...	HTTP	75	Continuation
118	03:25:17.898124	2601:204:c401:33a0::...	2600:1901:0:38d7::...	HTTP	75	Continuation
119	03:25:17.913338	10.0.0.236	34.107.221.82	HTTP	55	Continuation
136	03:25:18.657831	10.0.0.236	151.139.128.14	HTTP	55	Continuation
159	03:25:18.869915	10.0.0.236	128.119.245.12	HTTP	448	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
161	03:25:18.974171	128.119.245.12	10.0.0.236	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
261	03:25:37.631977	2601:204:c401:33a0::...	2600:1901:0:38d7::...	HTTP	372	GET /success.txt HTTP/1.1
263	03:25:37.649437	2600:1901:0:38d7::...	2601:204:c401:33a0::...	HTTP	294	HTTP/1.1 200 OK (text/plain)
266	03:25:37.651484	10.0.0.236	34.107.221.82	HTTP	357	GET /success.txt?ipv4 HTTP/1.1
268	03:25:37.652196	2601:204:c401:33a0::...	2600:1901:0:38d7::...	HTTP	377	GET /success.txt?ipv6 HTTP/1.1
270	03:25:37.668274	34.107.221.82	10.0.0.236	HTTP	274	HTTP/1.1 200 OK (text/plain)
272	03:25:37.673429	2600:1901:0:38d7::...	2601:204:c401:33a0::...	HTTP	294	HTTP/1.1 200 OK (text/plain)
319	03:25:38.413471	10.0.0.236	128.119.245.12	HTTP	507	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
323	03:25:38.517291	128.119.245.12	10.0.0.236	HTTP	544	HTTP/1.1 200 OK (text/html)
663	03:25:38.796255	10.0.0.236	128.119.245.12	HTTP	405	GET /favicon.ico HTTP/1.1
669	03:25:38.898688	128.119.245.12	10.0.0.236	HTTP	538	HTTP/1.1 404 Not Found (text/html)
711	03:25:40.242922	10.0.0.236	151.139.128.14	OCSP	434	Request
714	03:25:40.271837	151.139.128.14	10.0.0.236	OCSP	525	Response

```
> Frame 161: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Device\NPF_{269B53DA-DD3B-4C3A-8517-9DE937CFB405}, id 0
> Ethernet II, Src: Technico_f4:da:f5 (f4:c1:14:f4:da:f5), Dst: LiteonTe_95:eb:c7 (64:6e:69:95:eb:c7)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.236
> Transmission Control Protocol, Src Port: 80, Dst Port: 59671, Seq: 1, Ack: 395, Len: 717
< Hypertext Transfer Protocol
  < HTTP/1.1 401 Unauthorized\r\n
    Date: Wed, 28 Oct 2020 10:25:19 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.11 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
  < 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: 0.104256000 seconds]
  [Request in frame: 159]
  [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)
```

- a. The server's response in response to the initial HTTP GET message from my browser is "401 Unauthorized".

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

No.	Time	Source	Destination	Protocol	Length	Info
116	03:25:17.822001	2601:204:c401:33a0::...	2600:1901:0:38d7::...	HTTP	75	Continuation
118	03:25:17.898124	2601:204:c401:33a0::...	2600:1901:0:38d7::...	HTTP	75	Continuation
119	03:25:17.913338	10.0.0.236	34.107.221.82	HTTP	55	Continuation
136	03:25:18.657831	10.0.0.236	151.139.128.14	HTTP	55	Continuation
159	03:25:18.869915	10.0.0.236	128.119.245.12	HTTP	448	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
161	03:25:18.974171	128.119.245.12	10.0.0.236	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
261	03:25:37.631977	2601:204:c401:33a0::...	2600:1901:0:38d7::...	HTTP	372	GET /success.txt HTTP/1.1
263	03:25:37.649437	2600:1901:0:38d7::...	2601:204:c401:33a0::...	HTTP	294	HTTP/1.1 200 OK (text/plain)
266	03:25:37.651484	10.0.0.236	34.107.221.82	HTTP	357	GET /success.txt?ip=4 HTTP/1.1
268	03:25:37.652196	2601:204:c401:33a0::...	2600:1901:0:38d7::...	HTTP	377	GET /success.txt?ip=6 HTTP/1.1
270	03:25:37.668274	34.107.221.82	10.0.0.236	HTTP	274	HTTP/1.1 200 OK (text/plain)
272	03:25:37.673429	2600:1901:0:38d7::...	2601:204:c401:33a0::...	HTTP	294	HTTP/1.1 200 OK (text/plain)
319	03:25:38.413471	10.0.0.236	128.119.245.12	HTTP	507	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
323	03:25:38.517291	128.119.245.12	10.0.0.236	HTTP	544	HTTP/1.1 200 OK (text/html)
663	03:25:38.796255	10.0.0.236	128.119.245.12	HTTP	405	GET /favicon.ico HTTP/1.1
669	03:25:38.898688	128.119.245.12	10.0.0.236	HTTP	538	HTTP/1.1 404 Not Found (text/html)
711	03:25:40.242922	10.0.0.236	151.139.128.14	OCSP	434	Request
714	03:25:40.271837	151.139.128.14	10.0.0.236	OCSP	525	Response


```

> Frame 319: 507 bytes on wire (4056 bits), 507 bytes captured (4056 bits) on interface \Device\NPF_{269B53DA-DD38-4C3A-8517-9DE937CFB405}, id 0
> Ethernet II, Src: LiteonTe_95:eb:c7 (64:6e:69:95:eb:c7), Dst: Technico_f4:da:f5 (f4:c1:14:f4:da:f5)
> Internet Protocol Version 4, Src: 10.0.0.236, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 59673, Dst Port: 80, Seq: 1, Ack: 1, Len: 453
▼ Hypertext Transfer Protocol
  > GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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 d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcm0=\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: 323]
    [Next request in frame: 663]
  
```

- a. When the browser sends the HTTP GET message for the second time, the new field included in the HTTP GET message is “Authorization: Basic”