The Basic HTTP GET/response interaction

HTTP GET Message:

```
   145  17:20:45.823862    172.17.104.228       128.119.245.12       HTTP    581    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
Frame 145: 581 bytes on wire (4648 bits), 581 bytes captured (4648 bits) on interface 0
Ethernet II, Src: IntelCor_1c:96:a2 (5c:51:4f:1c:96:a2), Dst: 02:81:83:11:02:05 (02:81:83:11:02:05)
Internet Protocol Version 4, Src: 172.17.104.228, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 61957 (61957), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 527
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
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Encoding: gzip, deflate, sdch\r\n
    Accept-Language: en-US,en;q=0.8\r\n
    If-None-Match: "80-536b4ea95956a"\r\n
    If-Modified-Since: Sun, 03 Jul 2016 05:59:01 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: 147]
```

HTTP Response Message:

```
    33  14:48:12.593680    128.119.245.12       192.168.0.102       HTTP    542    HTTP/1.1 200 OK  (text/html)
Frame 33: 542 bytes on wire (4336 bits), 542 bytes captured (4336 bits) on interface 0
Ethernet II, Src: Tp-LinkT_93:d0:8c (14:cc:20:93:d0:8c), Dst: IntelCor_1c:96:a2 (5c:51:4f:1c:96:a2)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.102
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 62856 (62856), Seq: 1, Ack: 417, Len: 488
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Mon, 04 Jul 2016 21:48:10 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n
    Last-Modified: Mon, 04 Jul 2016 05:59:01 GMT\r\n
    ETag: "80-536c908741110"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.090432000 seconds]
    [Request in frame: 31]
Line-based text data: text/html
```

1. My browser is running on HTTP version 1.1 ✓

```
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
```

The server is also running on HTTP version 1.1

```
HTTP/1.1 200 OK  (text/html)
```

2. Accepted Language(s): English (U.S.) ✓

```
Accept-Language: en-US,en;q=0.8\r\n
```

3. IP Address of My Computer: 172.17.104.228 ✓

```
Src: 172.17.104.228
```

IP Address of the gaia.cs.umass.eud Server: 128.119.245.12 ✓

```
Dst: 128.119.245.12
```

4. The status code returned from the server to my browser was <u>200</u>

```
200 OK ✓
```

5. The HTTML file I was retrieving was last modified at the server on
   <u>Monday, July 4th, 2016 at 12:20AM</u>

```
Mon, 04 Jul 2016 00:20:43      ✓
```

6. <u>295 bytes</u> of <u>content</u> was being returned to my browser

~~29S~~ bytes   *128 bytes (see above) (-3)*

7. <u>No data</u> that I notice. ✓

The HTTP CONDITIONAL GET/response interaction

First HTTP GET Request

```
    38 14:11:03.488654     192.168.0.102          128.119.245.12       HTTP     470     GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Frame 38: 470 bytes on wire (3760 bits), 470 bytes captured (3760 bits) on interface 0
Ethernet II, Src: IntelCor_1c:96:a2 (5c:51:4f:1c:96:a2), Dst: Tp-LinkT_93:d0:8c (14:cc:20:93:d0:8c)
Internet Protocol Version 4, Src: 192.168.0.102, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 62656 (62656), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 416
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    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; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Encoding: gzip, deflate, sdch\r\n
    Accept-Language: en-US,en;q=0.8\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: 40]
    [Next request in frame: 52]
```

First Server Response

```
    40 14:11:03.577194     128.119.245.12          192.168.0.102           HTTP     786     HTTP/1.1 200 OK  (text/html)
Frame 40: 786 bytes on wire (6288 bits), 786 bytes captured (6288 bits) on interface 0
Ethernet II, Src: Tp-LinkT_93:d0:8c (14:cc:20:93:d0:8c), Dst: IntelCor_1c:96:a2 (5c:51:4f:1c:96:a2)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.102
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 62656 (62656), Seq: 1, Ack: 417, Len: 732
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Mon, 04 Jul 2016 21:11:00 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n
    Last-Modified: Mon, 04 Jul 2016 05:59:01 GMT\r\n
    ETag: "173-536c908740940"\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: 0.088540000 seconds]
    [Request in frame: 38]
    [Next request in frame: 52]
    [Next response in frame: 53]
Line-based text data: text/html
```

Second HTTP GET Request

```
    52 14:11:05.236498    192.168.0.102        128.119.245.12       HTTP    582    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Frame 52: 582 bytes on wire (4656 bits), 582 bytes captured (4656 bits) on interface 0
Ethernet II, Src: IntelCor_1c:96:a2 (5c:51:4f:1c:96:a2), Dst: Tp-LinkT_93:d0:8c (14:cc:20:93:d0:8c)
Internet Protocol Version 4, Src: 192.168.0.102, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 62656 (62656), Dst Port: 80 (80), Seq: 417, Ack: 733, Len: 528
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file2.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
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Encoding: gzip, deflate, sdch\r\n
    Accept-Language: en-US,en;q=0.8\r\n
    If-None-Match: "173-536c908740940"\r\n
    If-Modified-Since: Mon, 04 Jul 2016 05:59:01 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 2/2]
    [Prev request in frame: 38]
    [Response in frame: 53]
```

Second Server Response

```
    53 14:11:05.325531    128.119.245.12        192.168.0.102        HTTP    295    HTTP/1.1 304 Not Modified
Frame 53: 295 bytes on wire (2360 bits), 295 bytes captured (2360 bits) on interface 0
Ethernet II, Src: Tp-LinkT_93:d0:8c (14:cc:20:93:d0:8c), Dst: IntelCor_1c:96:a2 (5c:51:4f:1c:96:a2)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.102
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 62656 (62656), Seq: 733, Ack: 945, Len: 241
Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
    Date: Mon, 04 Jul 2016 21:11:02 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=99\r\n
    ETag: "173-536c908740940"\r\n
    \r\n
    [HTTP response 2/2]
    [Time since request: 0.089033000 seconds]
    [Prev request in frame: 38]
    [Prev response in frame: 40]
    [Request in frame: 52]
```

8. I <u>do not</u> see an "IF-MODIFIED-SINCE:" line in the first HTTP GET request. ✓

```
    38 14:11:03.488654    192.168.0.102        128.119.245.12       HTTP    470    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Frame 38: 470 bytes on wire (3760 bits), 470 bytes captured (3760 bits) on interface 0
Ethernet II, Src: IntelCor_1c:96:a2 (5c:51:4f:1c:96:a2), Dst: Tp-LinkT_93:d0:8c (14:cc:20:93:d0:8c)
Internet Protocol Version 4, Src: 192.168.0.102, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 62656 (62656), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 416
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    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; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Encoding: gzip, deflate, sdch\r\n
    Accept-Language: en-US,en;q=0.8\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: 40]
    [Next request in frame: 52]
```

9. <u>Yes</u>, the server explicitly retuned the contents of the file. I can tell because there is a line-based text data section displayed within the response stating a fresh download completion of the contents of the file as shown below. ✓

```
Line-based text data: text/html
    \n
    <html>\n
    \n
    Congratulations again!  Now you've downloaded the file lab2-2.html. <br>\n
    This file's last modification date will not change.  <p>\n
    Thus  if you download this multiple times on your browser, a complete copy <br>\n
    will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
    field in your browser's HTTP GET request to the server.\n
    \n
    </html>\n
```

10. <u>Yes</u>, I do see an "IF-MODIDIED-SINCE:" line in the second HTTP GET request.
    Information Followed: <u>Mon, 04 Jul 2016 05:59:01 GMT\r\n</u>

```
    If-Modified-Since: Mon, 04 Jul 2016 05:59:01 GMT\r\n
``` ✓

11. The HTTP status code and phrase returned from the server in response to this second HTTP GET is <u>304 Not Modified</u> ✓
    Since the file was not modified, the server explicitly <u>did not</u> return the contents of the file.

```
    53 14:11:05.325531    128.119.245.12       192.168.0.102       HTTP    295    HTTP/1.1 304 Not Modified
Frame 53: 295 bytes on wire (2360 bits), 295 bytes captured (2360 bits) on interface 0
Ethernet II, Src: Tp-LinkT_93:d0:8c (14:cc:20:93:d0:8c), Dst: IntelCor_1c:96:a2 (5c:51:4f:1c:96:a2)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.102
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 62656 (62656), Seq: 733, Ack: 945, Len: 241
Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
    Date: Mon, 04 Jul 2016 21:11:02 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=99\r\n
    ETag: "173-536c908740940"\r\n
    \r\n
    [HTTP response 2/2]
    [Time since request: 0.089033000 seconds]
    [Prev request in frame: 38]
    [Prev response in frame: 40]
    [Request in frame: 52]
```

Retrieving Long Documents

12. <u>1</u> HTTP GET request messages was sent by my browser. ✓

```
    32 15:20:09.320451 192.168.0.102     128.119.245.12     HTTP    470 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
    34 15:20:09.407259 128.119.245.12     192.168.0.102     HTTP    1494 [TCP Previous segment not captured] Continuation
    38 15:20:09.412062 128.119.245.12     192.168.0.102     HTTP    1494 Continuation
    39 15:20:09.412068 128.119.245.12     192.168.0.102     HTTP    597 Continuation
```

Packet Number <u>32</u> in the trace contains the GET message for the Bill of Rights.

```
    32 15:20:09.320451 192.168.0.102     128.119.245.12     HTTP    470 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
```

13. I was <u>unable</u> to find a pack that contained the status code and phrase associated with the response to the HTTP GET response. But I would assume it would have be the response packet immediately following the HTTP GET message, which would have been packet number <u>34</u>. *ok.*

```
32 15:20:09.320451 192.168.0.102      128.119.245.12      HTTP    470 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
34 15:20:09.407259 128.119.245.12     192.168.0.102       HTTP    1494 [TCP Previous segment not captured] Continuation
38 15:20:09.412062 128.119.245.12     192.168.0.102       HTTP    1494 Continuation
39 15:20:09.412068 128.119.245.12     192.168.0.102       HTTP    597 Continuation
```

```
34 15:20:09.407259 128.119.245.12     192.168.0.102       HTTP    1494 [TCP Previous segment not captured] Continuation
```
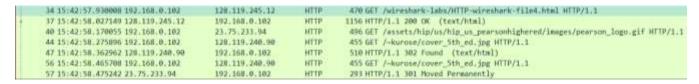
14. The potential status code and phrase in the response could have been <u>200 and OK</u>. ✓

15. <u>3</u> data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights. Packet Numbers 34, 38, and 39 ✓

```
34 15:20:09.407259 128.119.245.12     192.168.0.102       HTTP    1494 [TCP Previous segment not captured] Continuation
38 15:20:09.412062 128.119.245.12     192.168.0.102       HTTP    1494 Continuation
39 15:20:09.412068 128.119.245.12     192.168.0.102       HTTP    597 Continuation
```

HTML Documents with Embedded Objects

16. <u>4</u> HTTP GET request messages were sent by my browser.

One to <u>128.119.245.12</u>, one to <u>23.75.233.94</u>, and two to <u>128.119.240.90</u> ✓

```
34 15:42:57.930000 192.168.0.102      128.119.245.12      HTTP    470 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
37 15:42:58.027149 128.119.245.12     192.168.0.102       HTTP    1156 HTTP/1.1 200 OK  (text/html)
40 15:42:58.170055 192.168.0.102      23.75.233.94        HTTP    496 GET /assets/hip/us/hip_us_pearsonhighered/images/pearson_logo.gif HTTP/1.1
44 15:42:58.275896 192.168.0.102      128.119.240.90      HTTP    455 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
47 15:42:58.362962 128.119.240.90     192.168.0.102       HTTP    510 HTTP/1.1 302 Found  (text/html)
56 15:42:58.465700 192.168.0.102      128.119.240.90      HTTP    455 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
57 15:42:58.475242 23.75.233.94       192.168.0.102       HTTP    293 HTTP/1.1 301 Moved Permanently
```

17. I am <u>unable</u> to tell whether my browser downloaded the two images serially or in parallel.
But I would assume that my browser downloaded the images from the two web sites in <u>parallel</u>, because the second image had went through two HTTP GET request messages in the trace, which leads me to assume that the two images with initially called in parallel, yet something occurred while analyzing the second image causing for second GET afterwards. ✓

HTTP Authentication

18. The server's response in response to the initial HTP GET message from my browser is
<u>401 Unauthorized</u> ✓

```
59 16:07:30.991603 192.168.0.102      128.119.245.12      HTTP    486 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
61 16:07:31.082245 128.119.245.12     192.168.0.102       HTTP    773 HTTP/1.1 401 Unauthorized  (text/html)
143 16:07:47.379714 192.168.0.102     128.119.245.12      HTTP    545 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
145 16:07:47.470340 128.119.245.12    192.168.0.102       HTTP    546 HTTP/1.1 200 OK  (text/html)
```

```
61 16:07:31.082245 128.119.245.12     192.168.0.102       HTTP    773 HTTP/1.1 401 Unauthorized  (text/html)
```

19. <u>Authorization: Basic</u> is the new field that is included in the second HTTP GET message. ✓

```
    143 16:07:47.379714     192.168.0.102           128.119.245.12          HTTP    545     GET /wireshark-labs/protected_pages/HTTP-wireshark-
file5.html HTTP/1.1
Frame 143: 545 bytes on wire (4360 bits), 545 bytes captured (4360 bits) on interface 0
Ethernet II, Src: IntelCor_1c:96:a2 (5c:51:4f:1c:96:a2), Dst: Tp-LinkT_93:d0:8c (14:cc:20:93:d0:8c)
Internet Protocol Version 4, Src: 192.168.0.102, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 63018 (63018), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 491
Hypertext Transfer Protocol
    GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Encoding: gzip, deflate, sdch\r\n
    Accept-Language: en-US,en;q=0.8\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: 145]
```