

Lab_2a_Wireshark_HTTP_v8.0

• The Basic HTTP GET/response interaction

1367	7.266649835	192.168.30.111	128.119.245.12	HTTP	542 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1447	7.512303399	128.119.245.12	192.168.30.111	HTTP	554 HTTP/1.1 200 OK (text/html)

HTTP GET:

```
▼ Frame 1367: 542 bytes on wire (4336 bits), 542 bytes captured (4336 bits) on interface any, id 0
  ▶ Interface id: 0 (any)
    Encapsulation type: Linux cooked-mode capture (25)
    Arrival Time: Sep 23, 2021 10:09:23.528152516 +07
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1632366563.528152516 seconds
    [Time delta from previous captured frame: 0.000237544 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 7.266649835 seconds]
    Frame Number: 1367
    Frame Length: 542 bytes (4336 bits)
    Capture Length: 542 bytes (4336 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: sll:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]

  ▼ 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
      Upgrade-Insecure-Requests: 1\r\n
      User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 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,vi;q=0.8\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: 1447]
```

HTTP Response:

```
▼ Frame 1447: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface any, id 0
  ▶ Interface id: 0 (any)
    Encapsulation type: Linux cooked-mode capture (25)
    Arrival Time: Sep 23, 2021 10:09:23.773806080 +07
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1632366563.773806080 seconds
    [Time delta from previous captured frame: 0.001256880 seconds]
    [Time delta from previous displayed frame: 0.245653564 seconds]
    [Time since reference or first frame: 7.512303399 seconds]
    Frame Number: 1447
    Frame Length: 554 bytes (4432 bits)
    Capture Length: 554 bytes (4432 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: sll:ethertype:ip:tcp:http:data-text-lines]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]

  ▼ Hypertext Transfer Protocol
    ▶ HTTP/1.1 200 OK\r\n
      Date: Thu, 23 Sep 2021 03:09:23 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: Wed, 22 Sep 2021 05:59:01 GMT\r\n
      ETag: "80-5cc8f35fb78e7"\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: 0.245653564 seconds]
      [Request in frame: 1367]
      [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
      File Data: 128 bytes
```

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

Answer: version 1.1

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

Answer: Accept-Language: en-US, vi

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

Internet address of the gaia.cs.umass.edu: 128.119.245.12

Internet address of my computer: 192.168.30.111

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

Answer: Status code: 200

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

Answer: Last-Modified: Wed, 22 Sep 2021 05:59:01 GMT

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

Answer: 128 bytes

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.

- **The HTTP CONDITIONAL GET/response interaction:**

First time:

HTTP GET

+	189	3.165248515	192.168.30.111	128.119.245.12	HTTP	542 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
-	209	3.413530335	128.119.245.12	192.168.30.111	HTTP	798 HTTP/1.1 200 OK (text/html)

▼ Frame 189: 542 bytes on wire (4336 bits), 542 bytes captured (4336 bits) on interface any, id 0

▶ Interface id: 0 (any)
Encapsulation type: Linux cooked-mode capture (25)
Arrival Time: Sep 23, 2021 11:04:16.431763626 +07
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1632369856.431763626 seconds
[Time delta from previous captured frame: 0.000177491 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 3.165248515 seconds]
Frame Number: 189
Frame Length: 542 bytes (4336 bits)
Capture Length: 542 bytes (4336 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: sll:ethertype:ip:tcp:http]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]

▼ 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 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 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,vi;q=0.8\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: 209]

HTTP Response

▼	Frame 209: 798 bytes on wire (6384 bits), 798 bytes captured (6384 bits) on interface any, id 0
▶	Interface id: 0 (any) Encapsulation type: Linux cooked-mode capture (25) Arrival Time: Sep 23, 2021 11:04:16.680045446 +07 [Time shift for this packet: 0.000000000 seconds] Epoch Time: 1632369856.680045446 seconds [Time delta from previous captured frame: 0.000764579 seconds] [Time delta from previous displayed frame: 0.248281820 seconds] [Time since reference or first frame: 3.413530335 seconds] Frame Number: 209 Frame Length: 798 bytes (6384 bits) Capture Length: 798 bytes (6384 bits) [Frame is marked: False] [Frame is ignored: False] [Protocols in frame: sll:ethertype:ip:tcp:http:data-text-lines] [Coloring Rule Name: HTTP] [Coloring Rule String: http tcp.port == 80 http2]

```

Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    Date: Thu, 23 Sep 2021 04:04:16 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: Wed, 22 Sep 2021 05:59:01 GMT\r\n
    ETag: "173-5cc8f35fb7117"\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: 0.248281820 seconds]
  [Request in frame: 189]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
  File Data: 371 bytes

```

Second time:

HTTP GET

83825	631.613145339	192.168.30.111	128.119.245.12	HTTP	654 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
83867	631.862543711	128.119.245.12	192.168.30.111	HTTP	308 HTTP/1.1 304 Not Modified

```

Frame 83825: 654 bytes on wire (5232 bits), 654 bytes captured (5232 bits) on interface any, id 0
  Interface id: 0 (any)
  Encapsulation type: Linux cooked-mode capture (25)
  Arrival Time: Sep 23, 2021 11:14:44.879660450 +07
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1632370484.879660450 seconds
  [Time delta from previous captured frame: 0.000418687 seconds]
  [Time delta from previous displayed frame: 192.124118557 seconds]
  [Time since reference or first frame: 631.613145339 seconds]
  Frame Number: 83825
  Frame Length: 654 bytes (5232 bits)
  Capture Length: 654 bytes (5232 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ethertype:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80 || http2]

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 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 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,vi;q=0.8\r\n
    If-None-Match: "173-5cc8f35fb7117"\r\n
    If-Modified-Since: Wed, 22 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 1/1]
  [Response in frame: 83867]

```

HTTP Response

```

Frame 83825: 654 bytes on wire (5232 bits), 654 bytes captured (5232 bits) on interface any, id 0
  Interface id: 0 (any)
  Encapsulation type: Linux cooked-mode capture (25)
  Arrival Time: Sep 23, 2021 11:14:44.879660450 +07
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1632370484.879660450 seconds
  [Time delta from previous captured frame: 0.000418687 seconds]
  [Time delta from previous displayed frame: 192.124118557 seconds]
  [Time since reference or first frame: 631.613145339 seconds]
  Frame Number: 83825
  Frame Length: 654 bytes (5232 bits)
  Capture Length: 654 bytes (5232 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: sll:ethertype:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80 || http2]

```

```

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 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 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,vi;q=0.8\r\n
If-None-Match: "173-5cc8f35fb7117"\r\n
If-Modified-Since: Wed, 22 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 1/1]
[Response in frame: 83867]

```

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?

Answer: No, there is no IF-MODIFIED-SINCE line in the GET message.

9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Answer: The server did explicitly return the contents of the file. Wireshark includes a section titled “Line-Based Text Data” which shows what the server sent back to my browser which is specifically what the website showed when I brought it up on my browser.

```

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

```

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?

```

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 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 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,vi;q=0.8\r\n
If-None-Match: "173-5cc8f35fb7117"\r\n
If-Modified-Since: Wed, 22 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 1/1]
[Response in frame: 83867]

```

```

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

```

Answer:

Yes, in the second HTTP message an IF-MODIFIED-SINCE line is included. The information that follows is the date and time that I last accessed the webpage

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.

Answer:

- The HTTP status code is “304: Not Modified”
- The server did not return the contents of the file because the browser simply retrieved the contents from its cache. Had the file been modified since it was last accessed, it would have returned the contents of the file, instead it simply told my browser to retrieve the old file from its cached memory.

● **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?

42	4.608598826	192.168.30.111	128.119.245.12	TCP	66 36832 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3200092508...
43	4.609044309	192.168.30.111	128.119.245.12	HTTP	627 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
44	4.635860439	128.119.245.12	192.168.30.111	TCP	74 80 → 36834 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SA...
45	4.635994337	192.168.30.111	128.119.245.12	TCP	66 36834 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3200092535...
48	4.861698093	192.168.30.111	35.224.170.84	TCP	74 49750 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
49	4.863986892	128.119.245.12	192.168.30.111	TCP	66 80 → 36830 [ACK] Seq=1 Ack=562 Win=30208 Len=0 TSval=86003336...
50	4.867183901	128.119.245.12	192.168.30.111	TCP	1494 80 → 36830 [ACK] Seq=1 Ack=562 Win=30208 Len=1428 TSval=86003...
51	4.867258607	192.168.30.111	128.119.245.12	TCP	66 36830 → 80 [ACK] Seq=562 Ack=1429 Win=63104 Len=0 TSval=32000...
52	4.867664443	128.119.245.12	192.168.30.111	HTTP	3499 HTTP/1.1 200 OK (text/html)
53	4.867714306	192.168.30.111	128.119.245.12	TCP	66 36830 → 80 [ACK] Seq=562 Ack=4862 Win=59776 Len=0 TSval=32000...
54	5.116980033	35.224.170.84	192.168.30.111	TCP	74 80 → 49750 [SYN, ACK] Seq=0 Ack=1 Win=64768 Len=0 MSS=1420 SA...
55	5.117010573	192.168.30.111	35.224.170.84	TCP	66 49750 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=6713998 TS...
56	5.117082120	192.168.30.111	35.224.170.84	HTTP	153 GET / HTTP/1.1
57	5.272989003	192.168.30.111	128.119.245.12	HTTP	486 GET /favicon.ico HTTP/1.1

Answer:

- 1 HTTP GET request messages send
- The Packet that contained the GET message was packet number 43.

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

Answer:

43	4.609044309	192.168.30.111	128.119.245.12	HTTP	627 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
52	4.867664443	128.119.245.12	192.168.30.111	HTTP	3499 HTTP/1.1 200 OK (text/html)
56	5.117082120	192.168.30.111	35.224.170.84	HTTP	153 GET / HTTP/1.1
57	5.272989003	192.168.30.111	128.119.245.12	HTTP	486 GET /favicon.ico HTTP/1.1
60	5.318726298	35.224.170.84	192.168.30.111	HTTP	214 HTTP/1.1 204 No Content
75	5.530825004	128.119.245.12	192.168.30.111	HTTP	550 HTTP/1.1 404 Not Found (text/html)

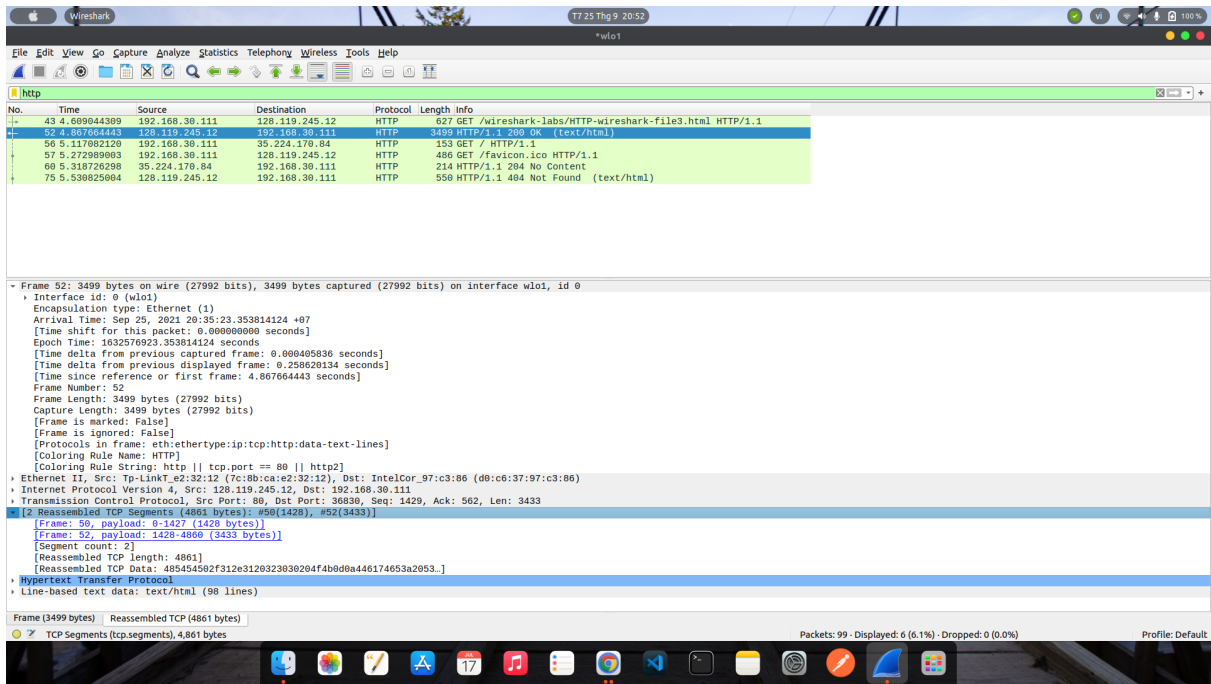
The packet that contains the status code and phrase which the server sent in response to the GET message was packet number 52.

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

Answer: 200 (OK)

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

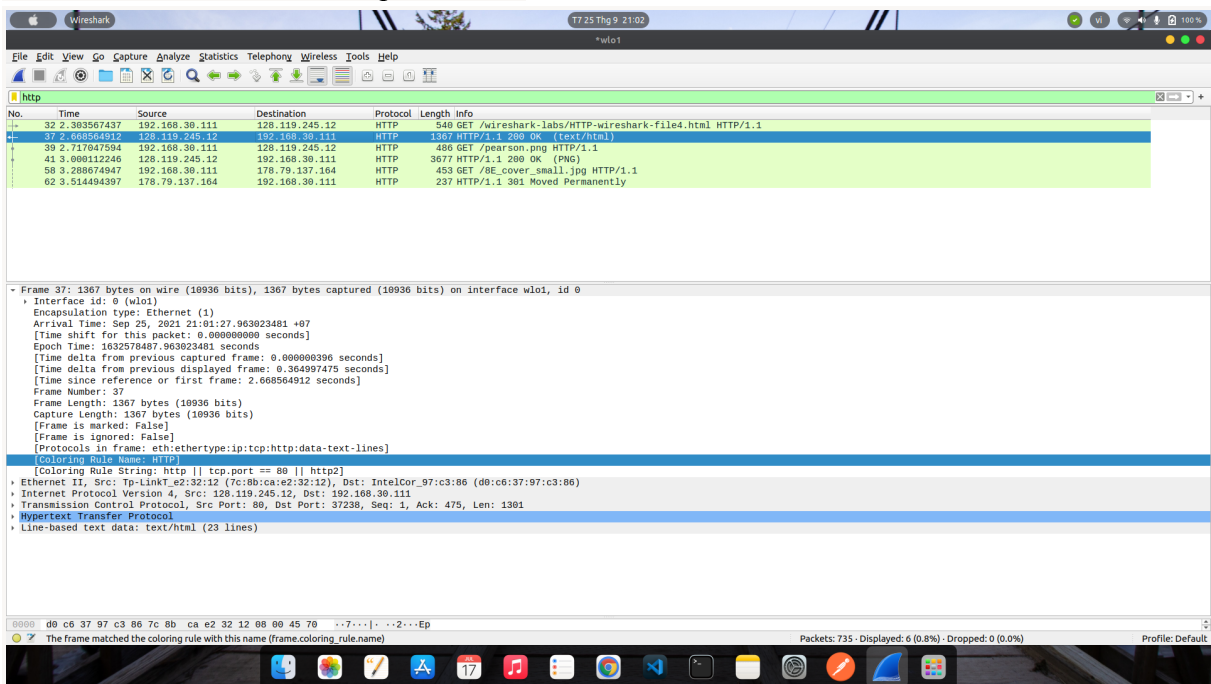
Answer:



The data was sent in 2 TCP segments to the browser, then reassembled.

- **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?



Answer:

- My browser sent 3 http GET message requests. One each to each for each of the following: The initial page, the Pearson logo, and the cover of the Pearson book, 5th Edition.
- Initial Page address: 128.119.245.12
- Pearson Logo: 128.119.245.12

- Pearson book, 5th Edition: 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.

Answer:

The browser downloaded the two images in serially. I believe this to be the case because the first image was requested and sent before the second image was requested by the browser. Had they been running in parallel, both files would have been requested then would have returned in the same time period. In this case however, the second image was only requested after the first image came back.

- **HTTP Authentication:**

44	3.244851054	192.168.30.111	128.119.245.12	HTTP	556 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
49	3.491357830	128.119.245.12	192.168.30.111	HTTP	783 HTTP/1.1 401 Unauthorized (text/html)
151	19.790174432	192.168.30.111	128.119.245.12	HTTP	641 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
162	20.052938853	128.119.245.12	192.168.30.111	HTTP	556 HTTP/1.1 200 OK (text/html)

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

Answer:

Packet 44 in the trace contains the first GET and packet 49 contains the REPLY. The server's in packet 49 is: 401 Authorization Required

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

Answer:

The new field that is now included is the authorization field. This is included because we sent the server a username and password along with our request stating that we were authorized to receive the page

Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcm5=\r\n