1. The Basic HTTP GET/response interaction

HTTP request-response message contents:

No. Time Source Destination Protocol Length Info
6 18:44:14.707979 10.101.6.200 128.119.245.12 HTTP 465 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

Frame 6: 465 bytes on wire (3720 bits), 465 bytes captured (3720 bits) on interface en0, id 0
Ethernet II, Src: Apple_ca:bf:0b (f4:5c:89:ca:bf:0b), Dst: HewlettP_b8:1e:9d (44:31:92:b8:1e:9d)
Internet Protocol Version 4, Src: 10.101.6.200, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 58292, Dst Port: 80, Seq: 1, Ack: 1, Len: 399
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Upgrade-Insecure-Requests: 1\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_1) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.0.3 Safari/605.1.15\r\n
Accept-Language: en-us\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\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: 8]

No. Time Source Destination Protocol Length Info
8 18:44:14.889939 128.119.245.12 10.101.6.200 HTTP 552 HTTP/1.1 200 OK (text/html)

Frame 8: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface en0, id 0
Ethernet II, Src: HewlettP_b8:1e:9d (44:31:92:b8:1e:9d), Dst: Apple_ca:bf:0b (f4:5c:89:ca:bf:0b)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.101.6.200
Transmission Control Protocol, Src Port: 80, Dst Port: 58292, Seq: 1, Ack: 400, Len: 486
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Sat, 08 Feb 2020 12:44:14 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Sat, 08 Feb 2020 06:59:02 GMT\r\n
ETag: "80-59e0b0a946492"\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: 0.181960000 seconds]
[Request in frame: 6]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
File Data: 128 bytes
Line-based text data: text/html (4 lines)
<html>\n
Congratulations. You've downloaded the file \n
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
</html>\n

Answers:

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
    a. Browser: Browser is running HTTP/1.1. This can be found in the reference-line of the browser's HTTP request: " HTTP-wireshark-file1.html HTTP/1.1".
    b. Server: Server is running HTTP/1.1. This can be found in HTTP response message: "HTTP/1.1 200 OK\r\n"
2. What languages (if any) does your browser indicate that it can accept to the server?
    a. Browser indicates that user would prefer english, specifically US region type, but can accept english with a quality factor of 0.5. This is shown in HTTP header "accept-language" - "Accept-Language: en-US,en;q=0.5\r\n"
3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?
    a. IP datagram for a request from client to server: "Internet Protocol Version 4, Src: 10.101.6.200, Dst: 128.119.245.12". Hence my ip 10.101.6.200, server's 128.119.245.12
4. What is the status code returned from the server to your browser?
    a. 200, OK
5. When was the HTML file that you are retrieving last modified at the server?
    a. "Last-Modified: 08 Feb 2020 06:59:02 GMT"
6. How many bytes of content are being returned to your browser?
    a. "Content-Length: 128 bytes"

7. I see none that are not listed

2. The HTTP CONDITIONAL GET/response interaction

HTTP request-responses too large to paste here, attached to the archive as “second.txt”.

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?
    a. No, there is no such header.
2. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
    a. Yes, the server did return the contents of the file. This can be seen by looking at the headers “Content-Length: 371” and “Content-Type: text/html; charset=UTF-8”, as well as the response message body that is followed with the actual contents of the file.
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?
    a. Yes, there is “If-Modified-Since” header: “If-Modified-Since: Sat, 08 Feb 2020 06:59:02 GMT”.
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.
    a. Status code: 304, phrase: “Not Modified”. No, the server did not explicitly return the contents of the file. Headers “Content-Length”, “Content-Type” are absent and the HTTP response message body that follows headers is empty.

3. Retrieving Long Documents

HTTP request-responses too large to paste here, attached to the archive as “third.txt”.

Answers:

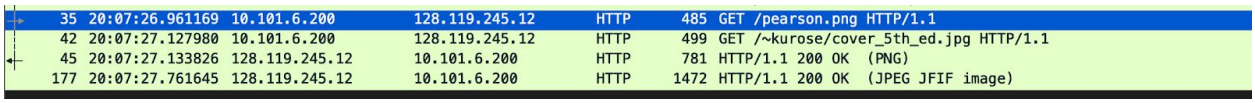
1. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?
    a. 1 HTTP request in total. Packet number 4 is the GET message.
2. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?
    a. Packet number 11.
3. What is the status code and phrase in the response?
    a. 200, OK.
4. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

a. 4.

```
[4 Reassembled TCP Segments (4861 bytes): #7(1448), #8(1448), #10(1448), #11(517)]
   [Frame: 7, payload: 0-1447 (1448 bytes)]
   [Frame: 8, payload: 1448-2895 (1448 bytes)]
   [Frame: 10, payload: 2896-4343 (1448 bytes)]
   [Frame: 11, payload: 4344-4860 (517 bytes)]
```

4. HTML Documents with Embedded Objects

1. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?
    a. 3 get requests. Initial GET request was sent to 128.119.245.12 (http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html), second was sent to the same ip (http://gaia.cs.umass.edu/pearson.png), third was sent to the same ip as well (http://manic.cs.umass.edu/~kurose/cover_5th_ed.jpg). Both URLs have same IP addresses.
2. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.
    a. In parallel. As can be seen in the screenshot below, first image was requested, but not received before the second image request was sent.



5. HTTP Authentication

HTTP request-responses too large to paste here, attached to the archive as “fifth.txt”.

1. What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser?
    a. 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?
    a. Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=