

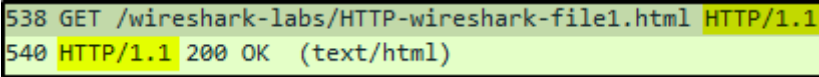
- Josh Poe - Wireshark Lab 2

Part 1 - The Basic HTTP GET/response interaction -

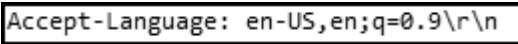
<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>

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

1. Browser HTTP 1.1
2. Server HTTP 1.1

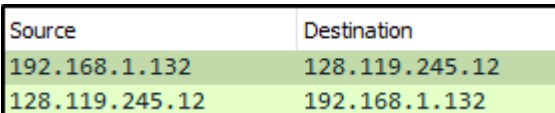
3. A screenshot of a Wireshark packet capture. The first packet (538) is a GET request for /wireshark-labs/HTTP-wireshark-file1.html using HTTP/1.1. The second packet (540) is the response, showing a 200 OK status and content type of text/html.

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

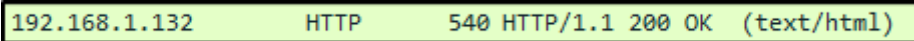
1. A screenshot of the 'Accept-Language' header from a browser request, showing 'en-US,en;q=0.9\r\n'.

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

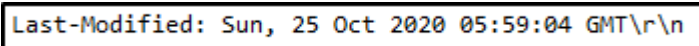
1. PC - 192.168.1.132
2. Server 128.119.245.12

3. A screenshot of a Wireshark packet capture showing the source and destination IP addresses. The source IP is 192.168.1.132 and the destination IP is 128.119.245.12.

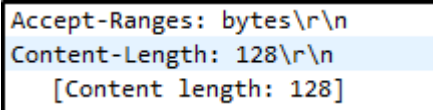
4. What is the status code returned from the server to your browser?

1. A screenshot of a Wireshark packet capture showing the status code 200 OK.

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

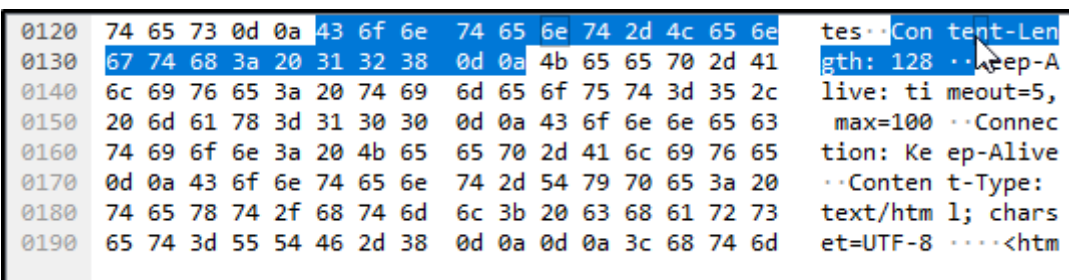
1. A screenshot of the 'Last-Modified' header from a server response, showing 'Sun, 25 Oct 2020 05:59:04 GMT\r\n'.

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

1. A screenshot of the 'Content-Length' header from a server response, showing '128\r\n'.

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.

1. Raw content matches what is shown in the packet window

2. A screenshot of a Wireshark packet capture showing the raw data of a packet. The raw data is displayed in hexadecimal and ASCII. The ASCII part shows the start of an HTML document with a content length of 128.

Part 2 - The HTTP CONDITIONAL GET/response interactio -

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html>

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?

1. Negative

2. Request Method: GET

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

```
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
```

1.

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?

1. If-Modified-Since: Sun, 25 Oct 2020 05:59:04 GMT\r\n

01a0	2d 52 65 71 75 65 73 74	73 3a 20 31 0d 0a 49 66	-Request s: 1..If
01b0	2d 4d 6f 64 69 66 69 65	64 2d 53 69 6e 63 65 3a	-Modifie d-Since:
01c0	20 53 75 6e 2c 20 32 35	20 4f 63 74 20 32 30 32	Sun, 25 Oct 202
01d0	30 20 30 35 3a 35 39 3a	30 34 20 47 4d 54 0d 0a	0 05:59: 04 GMT..
01e0	49 66 2d 4e 6f 6e 65 2d	4d 61 74 63 68 3a 20 22	If-None- Match: "
01f0	31 37 33 2d 35 62 32 37	38 38 32 64 33 66 64 66	173-5b27 882d3fdf
0200	39 22 0d 0a 43 61 63 68	65 2d 43 6f 6e 74 72 6f	9"··Cach e-Contro
0210	6c 3a 20 6d 61 78 2d 61	67 65 3d 30 0d 0a 0d 0a	l: max-age=0····

Request line (http.request.line), 50 bytes

2.

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.

1. 293 HTTP/1.1 304 Not Modified

2. Server did not explicitly return contents

Part 3 - Retrieving Long Documents - <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html>

12. 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?

1. 11234 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1

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

1. 11324 HTTP/1.1 200 OK (text/html)

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

1. HTTP/1.1 200 OK (text/html)

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

1. [4 Reassembled TCP Segments (4861 bytes): #6897(1460), #6898(1460), #6900(1460), #6901(481)]
[Frame: 6897, payload: 0-1459 (1460 bytes)]
[Frame: 6898, payload: 1460-2919 (1460 bytes)]
[Frame: 6900, payload: 2920-4379 (1460 bytes)]
[Frame: 6901, payload: 4380-4860 (481 bytes)]

Part 4 - HTML Documents with Embedded Objects -

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>

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

1.

Destination	Length	Protocol	Info
128.119.245.12	389	HTTP	GET /pearson.png HTTP/1.1
128.119.245.12	432	HTTP	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
128.119.245.12	403	HTTP	GET /~kurose/cover_5th_ed.jpg HTTP/1.1

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.

1. [70 Reassembled TCP Segments (101318 bytes): #5518(1460),
[Frame: 5518, payload: 0-1459 (1460 bytes)]
[Frame: 5519, payload: 1460-2919 (1460 bytes)]
[Frame: 5521, payload: 2920-4379 (1460 bytes)]
[Frame: 5522, payload: 4380-5839 (1460 bytes)]
[Frame: 5524, payload: 5840-7299 (1460 bytes)]
[Frame: 5525, payload: 7300-8759 (1460 bytes)]
[Frame: 5527, payload: 8760-10219 (1460 bytes)]
[Frame: 5529, payload: 10220-11679 (1460 bytes)]
[Frame: 5530, payload: 11680-13139 (1460 bytes)]

2. Images downloaded in serial. TCP payloads requested one after another.

Part 5 - HTTP Authentication - http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresharkfile5.html

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

1. HTTP/1.1 401 Unauthorized (text/html)

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

1. HTTP/1.1 200 OK (text/html)

2. Authentication

1. `Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcms=\r\n`

2. Decoded using Base64

3. `wireshark-students:network`