

Questions:

The Basic HTTP GET/response interaction

1. Is your browser running HTTP version 1.0, 1.1, or 2? What version of HTTP is the server running?

Ans: 1.1

```
TCP payload (488 bytes)
  Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Sat, 30 Jan 2021 21:43:30 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Sat, 30 Jan 2021 06:59:02 GMT\r\n
```

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

Ans:

```
User-Agent: Mozilla/5.0 (Macintosh;
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
\r\n
```

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

Source	Destination
128.119.245.12	10.0.0.44
10.0.0.44	128.119.245.12

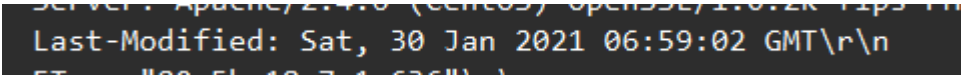
Ans :

10.0.0.44 128.119.245.12

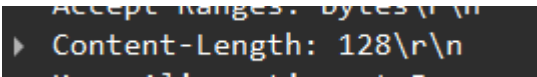
4. What is the status code returned from the server to your browser?

Ans: 200

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

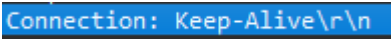
Ans: 

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

Ans:  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.

Ans: Yes, there are extra headers in the raw data that are not displayed in the packet-listing window. For example:



The HTTP CONDITIONAL GET/response interaction

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?

Ans: There is **no** "If-Modified-Since" line....

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

Ans:

```
\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
```

```
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
[Request in frame: 56]
[Time since request: 0.024609000 seconds]
[Request URI: /wireshark-labs/HTTP-wireshark-file2.html]
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
File Data: 371 bytes
```

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 GET6? If so, what information follows the “IF-MODIFIED-SINCE:” header?

Ans :

```
If-None-Match: "173-5ba18a7e1ba7e"\r\n
If-Modified-Since: Sat, 30 Jan 2021 06:59:02 GMT\r\n
```

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.

```
▼ Hypertext Transfer Protocol
  HTTP/1.1 304 Not Modified\r\n
  Date: Sat, 30 Jan 2021 18:19:56 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
  Connection: Keep-Alive\r\n
  Keep-Alive: timeout=5, max=99\r\n
  ETag: "173-5ba18a7e1ba7e"\r\n
  \r\n
  [Request in frame: 555]
  [Time since request: 0.022630000 seconds]
  [Request URI: /wireshark-labs/HTTP-wireshark-file2.html]
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

Ans:

304 Not Modified. The server did **not** return the file contents

Retrieving Long Documents

No.	Time	Source	Destination	Protocol	Length	Info
26	3.813230	10.0.0.44	128.119.245.12	HTTP	547	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
32	3.842202	128.119.245.12	10.0.0.44	HTTP	583	HTTP/1.1 200 OK (text/html)

<p>Frame 26: 547 bytes on wire (4376 bits), 547 bytes captured (4376 bits) on interface en0, id 0</p> <p>Ethernet II, Src: Apple 98:d9:27 (78:4f:43:98:d9:27), Dst: Maxlinear_80:00:00 (00:50:f1:80:00:00)</p> <p>Internet Protocol Version 4, Src: 10.0.0.44, Dst: 128.119.245.12</p> <p>Transmission Control Protocol, Src Port: 54985, Dst Port: 80, Seq: 1, Ack: 1, Len: 481</p> <p>Hypertext Transfer Protocol</p> <p>GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n</p> <p>Request Method: GET</p> <p>Request URI: /wireshark-labs/HTTP-wireshark-file3.html</p> <p>Request Version: HTTP/1.1</p> <p>Host: gaia.cs.umass.edu\r\n</p> <p>Connection: keep-alive\r\n</p> <p>Upgrade-Insecure-Requests: 1\r\n</p> <p>User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3989.101 Safari/537.36\r\n</p> <p>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</p> <p>Accept-Encoding: gzip, deflate\r\n</p> <p>\r\n</p> <p>[Response in frame: 32]</p> <p>[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]</p>	<p>0040 f6 f9 47 45 54 20 2f 77 69 72 65 73 68 61 72 6b GET /w ireshark</p> <p>0050 2d 66 61 62 73 2f 48 54 54 5b 2d 77 69 72 65 73 -labs//HT P-wiresh</p> <p>0060 68 61 72 6b 2d 66 69 6c 65 33 2e 68 74 6d 6c 20 ark-fil e3.html</p> <p>0070 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 HTTP/1.1 Host:</p> <p>0080 67 61 69 61 2e 63 73 2e 75 6d 61 73 73 2e 65 64 gaia.cs. umass.ed</p> <p>0090 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b u. Conne ction: k</p> <p>00a0 65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 67 72 61 eep-ali v e Upgra</p> <p>00b0 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 de-Insec ure-Requ</p> <p>00c0 65 73 74 73 3a 20 31 0d 0a 55 73 65 72 2d 41 67 est: 1. User-Ag</p> <p>00d0 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 ent: Moz illa/5.0</p> <p>00e0 20 28 4d 61 63 69 6e 74 6f 73 68 3b 20 49 6e 74 (Macint osh; Int</p> <p>00f0 65 6c 20 4d 61 63 20 4f 53 20 58 20 31 30 5f 31 el Mac O S X 10.1</p> <p>0100 35 5f 34 29 20 41 70 70 6c 65 57 65 62 4b 69 74 5.4) App leWebKit</p> <p>0110 2f 35 33 37 2e 33 36 20 28 4b 49 54 4d 4c 2c 20 /537.36 (KHTML,</p> <p>0120 6c 69 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f like Gec ko) Chro</p> <p>0130 6d 65 2f 38 38 2e 30 2e 34 33 32 34 2e 39 36 20 me/88.0. 4324.96</p> <p>0140 53 61 66 61 72 69 2f 35 33 37 2e 33 36 0d 0a 41 Safari/5 37.36. A</p> <p>0150 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c ccept: t ext/html</p> <p>0160 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 ,applica tion/xht</p> <p>0170 6d 6c 2b 78 6d 6c 2c 61 70 78 6c 69 63 61 74 69 ,xml,a pplicati</p> <p>0180 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 on/xml;q =0.9,ima</p> <p>0190 67 65 2f 61 76 69 6e 2c 69 6d 61 67 65 2f 77 65 ge/avif, image/we</p> <p>01a0 62 70 2c 69 6d 61 67 65 2f 61 70 6e 67 2c 2a 2f bp,image /apng,*</p> <p>01b0 2a 3b 71 3d 30 2e 38 2c 61 70 70 6c 69 63 61 74 /*;q=0.8, applicat</p> <p>01c0 69 6f 6e 2f 73 69 67 6e 65 4a 2d 65 78 63 68 61 ion/sign ed-excha</p> <p>01d0 6e 67 65 3b 7d 3d 62 33 3b 71 3d 30 2e 39 0d 0a ngey;b3;q=0.9</p> <p>01e0 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a Accept-E ncoding:</p> <p>01f0 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a gzip, d eflate</p>
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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?

Ans: 1.....26

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

Ans : 32

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

Ans: 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?

Ans: 3(28, 29, 31)

28	3.841957	128.119.245.12	10.0.0.44	TCP	1514	80 → 54985 [ACK] Seq=1 Ack=482 Win=30080 Len=1448 TSval=3636786980 TSecr=492255584 [TCP PDU reassembled in 32]
29	3.841961	128.119.245.12	10.0.0.44	TCP	1514	80 → 54985 [ACK] Seq=1449 Ack=482 Win=30080 Len=1448 TSval=3636786980 TSecr=492255584 [TCP PDU reassembled in 32]
30	3.842054	10.0.0.44	128.119.245.12	TCP	66	54985 → 80 [ACK] Seq=482 Ack=2897 Win=128832 Len=0 TSval=492255612 TSecr=3636786980
31	3.842198	128.119.245.12	10.0.0.44	TCP	1514	80 → 54985 [ACK] Seq=2897 Ack=482 Win=30080 Len=1448 TSval=3636786980 TSecr=492255584 [TCP PDU reassembled in 32]

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?

Ans: There are 4 HTTP GET request messages. These requests are sent to the IP address :

1. 178.79.137.164
2. 104.98.115.146
3. 128.119.245.12

No.	Time	Source	Destination	Protocol	Length	Info
118	3.309908	10.0.0.44	178.79.137.164	HTTP	500	GET /8E_cover_small.jpg HTTP/1.1
144	3.757683	10.0.0.44	104.98.115.146	HTTP	361	GET /MFgwVqADAgEAME8wTTBLMAkGBSs0AwIaBQAEFEja
99	3.072335	10.0.0.44	128.119.245.12	HTTP	493	GET /pearson.png HTTP/1.1
95	3.018199	10.0.0.44	128.119.245.12	HTTP	547	GET /wireshark-labs/HTTP-wireshark-file4.html

17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two websites in parallel? Explain.

Ans:

99	3.072335	10.0.0.44	128.119.245.12	HTTP	493	GET /pearson.png HTTP/1.1
104	3.092770	128.119.245.12	10.0.0.44	HTTP	781	HTTP/1.1 200 OK (PNG)
118	3.309908	10.0.0.44	178.79.137.164	HTTP	500	GET /8E_cover_small.jpg HTTP/1.1
120	3.451822	178.79.137.164	10.0.0.44	HTTP	237	HTTP/1.1 301 Moved Permanently

Serially. As the GET request for the second image (packet 118 at 3.309s) was sent after the 200 OK response for the first image (packet 104 at 3.092s) was received.

HTTP Authentication:

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

Ans: There are two response packets: 482 and 94

The response in packet 482 is:

```
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 200 OK\r\n
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
```

Packet 482

The server responded with status code 200 and phrase OK

The response in packet 94 is:

```
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 401 Unauthorized\r\n
    Response Version: HTTP/1.1
    Status Code: 401
    [Status Code Description: Unauthorized]
    Response Phrase: Unauthorized
```

Packet 94

The server responded with status code 401 and phrase "Unauthorized"

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

Ans:

```
▼ Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcm5=\r\n  
  Credentials: wireshark-students:network
```