

Student Information

Full Name : Mehmet Rüçhan Yavuzdemir
Id Number: 2522159

1 The Basic HTTP GET/response interaction

Answer 1

Both my browser, Firefox, and the server running HTTP/1.1. This is from the packet listing window, as shown below.

```
Info
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
HTTP/1.1 200 OK (text/html)
```

Answer 2

We should look at the HTTP GET request to see languages that our browser accepts. They are en-US and en.

```
~ Hypertext Transfer Protocol
  ~ GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
      Host: gaia.cs.umass.edu\r\n
      User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/118.0\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
      Accept-Language: en-US,en;q=0.5\r\n
      Accept-Encoding: gzip, deflate\r\n
      Connection: keep-alive\r\n
      Upgrade-Insecure-Requests: 1\r\n
```

Answer 3

IP address information can be retrieved from the network layer. The IP address of my computer is 192.168.1.11 and the IP address of gaia.cs.umass.edu server is 128.119.245.12.

```
~ Internet Protocol Version 4, Src: 192.168.1.11, Dst: 128.119.245.12
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 435
    Identification: 0x0000 (0)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x020e [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.11
    Destination Address: 128.119.245.12
```

Answer 4

The status code returned from the server to my browser is 200 OK.

```
Info  
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1  
HTTP/1.1 200 OK (text/html)
```

Answer 5

The retrieved HTML file is modified at the server on Thu, 26 Oct 2023 05:59:02 GMT, close to the time I sent the request.

```
‐ Hypertext Transfer Protocol  
  ‐ HTTP/1.1 200 OK\r\n    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n      Response Version: HTTP/1.1  
      Status Code: 200  
      [Status Code Description: OK]  
      Response Phrase: OK  
      Date: Thu, 26 Oct 2023 18:57:22 GMT\r\n      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n      Last-Modified: Thu, 26 Oct 2023 05:59:02 GMT\r\n      ETag: "80-6089844c7567c"\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
```

Answer 6

The content returned to my browser is 128 bytes, which is the Content-Length.

```
‐ Hypertext Transfer Protocol  
  ‐ HTTP/1.1 200 OK\r\n    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n      Response Version: HTTP/1.1  
      Status Code: 200  
      [Status Code Description: OK]  
      Response Phrase: OK  
      Date: Thu, 26 Oct 2023 18:57:22 GMT\r\n      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n      Last-Modified: Thu, 26 Oct 2023 05:59:02 GMT\r\n      ETag: "80-6089844c7567c"\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
```

Answer 7

No, I do not see any single missing data. I examined the raw data, which is the actual bytes corresponding to the HTTP header and body information, and matched all the bytes with the corresponding headers. For example, I highlighted the raw data of the `Last-Modified` header information.

The screenshot shows a Wireshark capture of an HTTP response. The left pane displays the packet details, including the HTTP header fields:

- HTTP/1.1 200 OK\r\n
- Response Version: HTTP/1.1
- Status Code: 200
- [Status Code Description: OK]
- Response Phrase: OK
- Date: Thu, 26 Oct 2023 18:57:22 GMT\r\n
- Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.1
- Last-Modified: Thu, 26 Oct 2023 05:59:02 GMT\r\n
- ETag: "80-6089844c7567c"\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

The right pane shows the raw hex and ASCII data. The `Last-Modified` header is highlighted in blue in the ASCII view, showing the value `Thu, 26 Oct 2023 05:59:02 GMT`.

2 The HTTP CONDITIONAL GET/response interaction

Answer 8

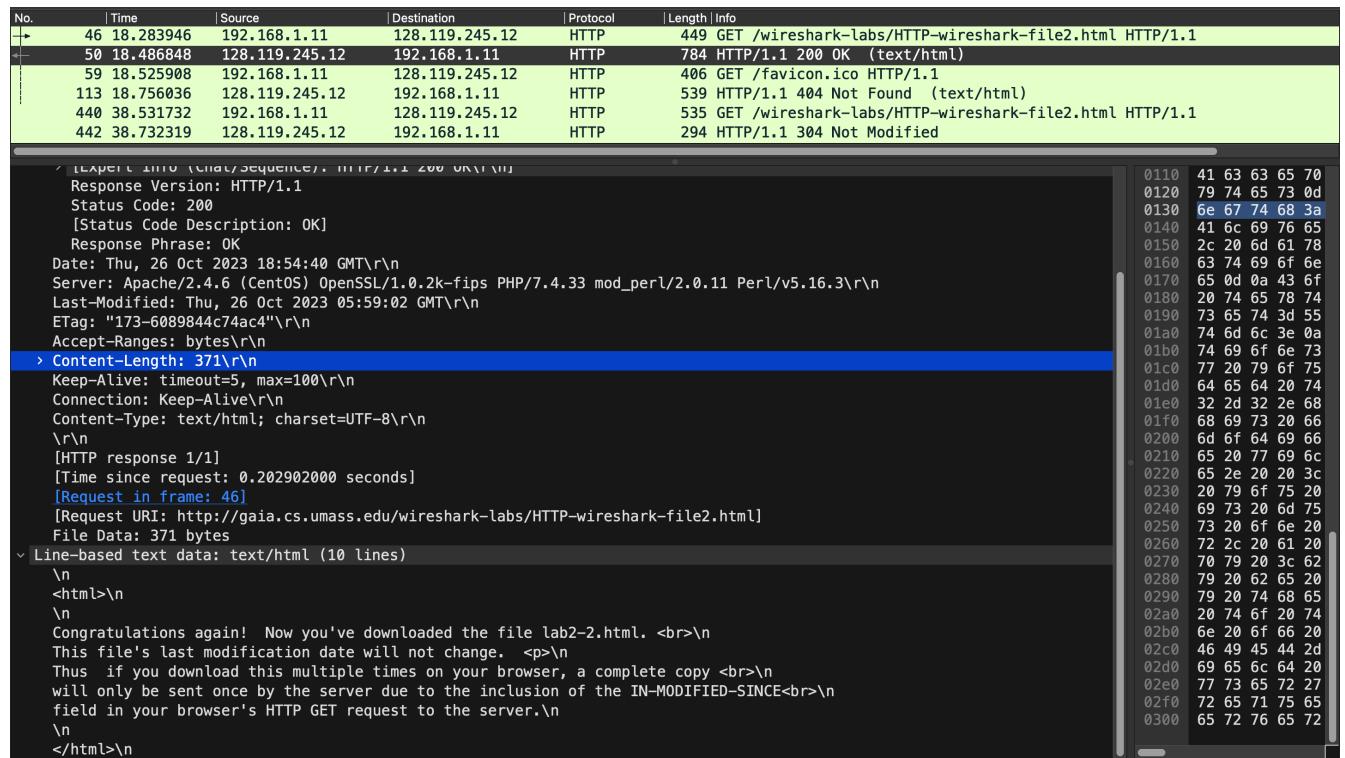
The HTTP GET request headers do not include IF-MODIFIED-SINCE header information since this is the first time sending the request. (The Google Chrome browser adds it the first time though, but my browser is Firefox)

No.	Time	Source	Destination	Protocol	Length	Info
46	18.283946	192.168.1.11	128.119.245.12	HTTP	449	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
50	18.486848	128.119.245.12	192.168.1.11	HTTP	784	HTTP/1.1 200 OK (text/html)
59	18.525908	192.168.1.11	128.119.245.12	HTTP	406	GET /favicon.ico HTTP/1.1
113	18.756036	128.119.245.12	192.168.1.11	HTTP	539	HTTP/1.1 404 Not Found (text/html)
440	38.531732	192.168.1.11	128.119.245.12	HTTP	535	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
442	38.732319	128.119.245.12	192.168.1.11	HTTP	294	HTTP/1.1 304 Not Modified


```
> Frame 46: 449 bytes on wire (3592 bits), 449 bytes captured (3592 bits)
> Ethernet II, Src: Apple_18:03:f1 (50:ed:3c:18:03:f1), Dst: zte_b1:ad:d8 (5c:a4:f4:b1:ad:d8)
> Internet Protocol Version 4, Src: 192.168.1.11, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 52625, Dst Port: 80, Seq: 1, Ack: 1, Len: 395
`- Hypertext Transfer Protocol
  + GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    + [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file2.html
      Request Version: HTTP/1.1
      Host: gaia.cs.umass.edu\r\n
      User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/118.0\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
      Accept-Language: en-US,en;q=0.5\r\n
      Accept-Encoding: gzip, deflate\r\n
      Connection: keep-alive\r\n
      Upgrade-Insecure-Requests: 1\r\n
      \r\n
      0000  5c a4 f4 b1
      0010  01 b3 00 00
      0020  f5 0c cd 91
      0030  10 00 26 2b
      0040  68 61 72 6b
      0050  69 72 65 73
      0060  74 6d 6c 20
      0070  73 74 3a 20
      0080  73 2e 65 64
      0090  74 3a 20 4d
      00a0  4d 61 63 69
      00b0  20 4d 61 63
      00c0  20 72 76 3a
      00d0  2f 32 30 31
      00e0  78 2f 31 31
      00f0  20 74 65 78
      0100  63 61 74 69
      0110  2c 61 70 70
      0120  3b 71 3d 30
      0130  66 2c 69 6d
      0140  3b 71 2d 20
```

Answer 9

In the response, there are two pieces of evidence that show the server explicitly returned the contents of the file. First, **Content-Length** is 371 bytes, which means 371 bytes were sent. Second, we see **Line-based text data**, containing the corresponding HTML file. Hence, the server explicitly returned the contents of the file.



Answer 10

Yes, in the HTTP GET request, there is `If-Modified-Since` header information. It is a human-readable ASCII text containing the date and time, Thu, 26 Oct 2023 05:59:02 GMT.

No.	Time	Source	Destination	Protocol	Length	Info
46	18.283946	192.168.1.11	128.119.245.12	HTTP	449	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
50	18.486848	128.119.245.12	192.168.1.11	HTTP	784	HTTP/1.1 200 OK (text/html)
59	18.525908	192.168.1.11	128.119.245.12	HTTP	406	GET /favicon.ico HTTP/1.1
113	18.756036	128.119.245.12	192.168.1.11	HTTP	539	HTTP/1.1 404 Not Found (text/html)
+ 440	38.531732	192.168.1.11	128.119.245.12	HTTP	535	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
+ 442	38.732319	128.119.245.12	192.168.1.11	HTTP	294	HTTP/1.1 304 Not Modified


```

> Frame 440: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits)
> Ethernet II, Src: Apple_18:03:f1 (50:ed:3c:18:03:f1), Dst: zte_b1:ad:d8 (5c:a4:f4:b1:ad:d8)
> Internet Protocol Version 4, Src: 192.168.1.11, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 52628, Dst Port: 80, Seq: 1, Ack: 1, Len: 481
  Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
      [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
        Request Method: GET
        Request URI: /wireshark-labs/HTTP-wireshark-file2.html
        Request Version: HTTP/1.1
        Host: gaia.cs.umass.edu\r\n
        User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/118.0\r\n
        Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
        Accept-Language: en-US,en;q=0.5\r\n
        Accept-Encoding: gzip, deflate\r\n
        Connection: keep-alive\r\n
        Upgrade-Insecure-Requests: 1\r\n
        If-Modified-Since: Thu, 26 Oct 2023 05:59:02 GMT\r\n
        If-None-Match: "173-6089844c74ac4"\r\n
      \r\n
  0000  5c a4 f4 b1 ad
  0010  02 09 00 00 40
  0020  f5 0c cd 94 00
  0030  10 00 06 60 00
  0040  68 61 72 6b 2d
  0050  69 72 65 73 68
  0060  74 6d 6c 73 68
  0070  73 74 5a 20 67
  0080  73 2e 65 64 75
  0090  74 3a 20 4d 6f
  00a0  4d 61 63 69 6e
  00b0  20 4d 61 63 20
  00c0  20 72 76 3a 31
  00d0  2f 32 30 31 30
  00e0  78 2f 31 31 38
  00f0  20 74 65 78 74
  0100  63 61 74 69 6f
  0110  2c 61 70 70 6c
  0120  3b 71 3d 30 2e
  0130  66 2c 69 6d 61
  0140  3b 71 3d 30 2e
  0150  61 6e 67 75 61

```

Answer 11

After sending the HTTP GET request a second time, the server returns 304 Not Modified. Furthermore, it did not explicitly return the HTML file, because there is no Content-Length header information and Line-based text data appearing at the bottom of the screen.

No.	Time	Source	Destination	Protocol	Length	Info
46	18.283946	192.168.1.11	128.119.245.12	HTTP	449	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
50	18.486848	128.119.245.12	192.168.1.11	HTTP	784	HTTP/1.1 200 OK (text/html)
59	18.525908	192.168.1.11	128.119.245.12	HTTP	406	GET /favicon.ico HTTP/1.1
113	18.756036	128.119.245.12	192.168.1.11	HTTP	539	HTTP/1.1 404 Not Found (text/html)
+ 440	38.531732	192.168.1.11	128.119.245.12	HTTP	535	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
+ 442	38.732319	128.119.245.12	192.168.1.11	HTTP	294	HTTP/1.1 304 Not Modified


```

> Frame 442: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits)
> Ethernet II, Src: zte_b1:ad:d8 (5c:a4:f4:b1:ad:d8), Dst: Apple_18:03:f1 (50:ed:3c:18:03:f1)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.11
> Transmission Control Protocol, Src Port: 80, Dst Port: 52628, Seq: 1, Ack: 482, Len: 240
  Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
      [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
        Date: Thu, 26 Oct 2023 18:55:01 GMT\r\n
        Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
        Connection: Keep-Alive\r\n
        Keep-Alive: timeout=5, max=100\r\n
        ETag: "173-6089844c74ac4"\r\n
      \r\n
  0000  50 ed 3c 18 03
  0010  01 18 0e 56 40 0
  0020  01 0b 00 50 cd 9
  0030  00 ed 89 5b 00 0
  0040  30 34 20 4e 6f 7
  0050  0a 44 61 74 65 3
  0060  63 74 20 32 30 3
  0070  20 47 4d 54 0d 0
  0080  61 63 68 65 2f 3
  0090  4f 53 29 20 4f 7
  00a0  32 6b 2d 66 69 7
  00b0  33 33 20 6d 6f 6
  00c0  31 31 20 50 65 7
  00d0  0a 43 6f 6e 6e 6
  00e0  70 2d 41 6c 69 7
  00f0  69 76 65 3a 20 7
  0100  6d 61 78 3d 31 3
  0110  31 37 33 2d 36 3
  0120  34 22 0d 0a 0d 0

```

3 Retrieving Long Documents

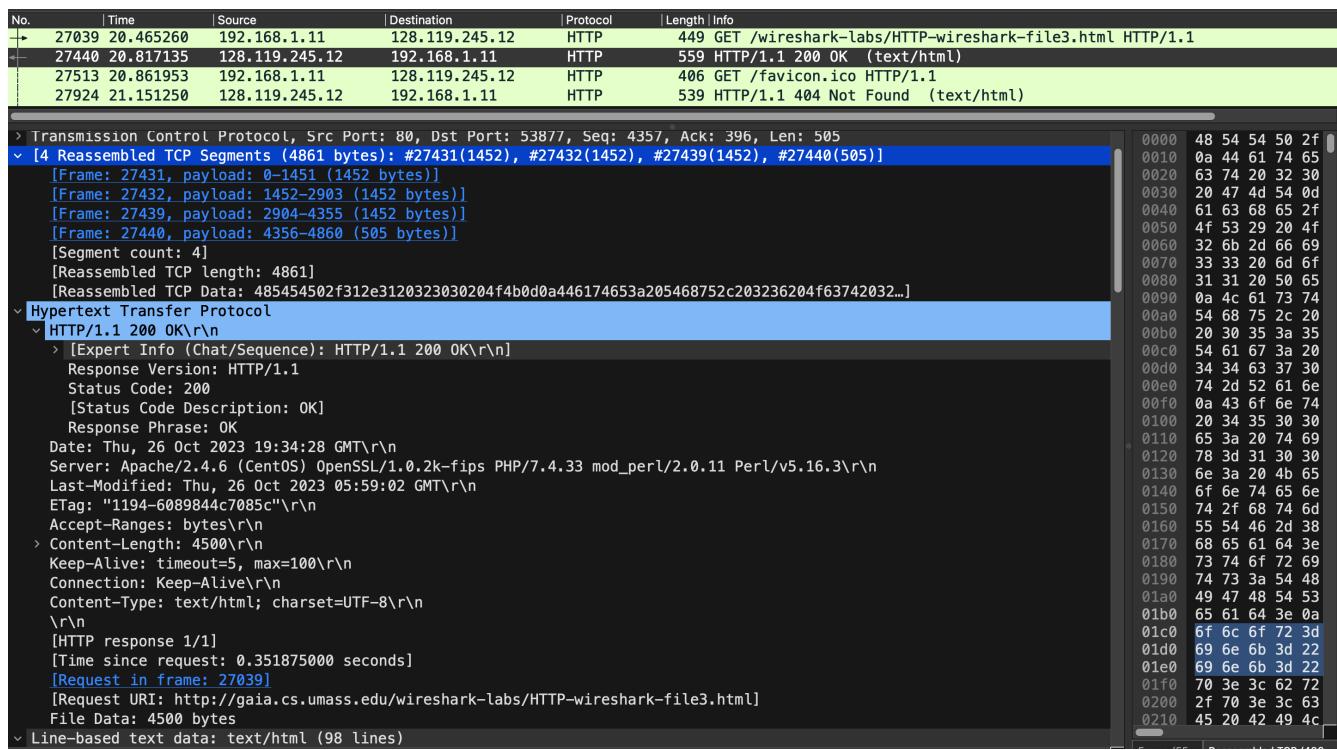
Answer 12

My browser only sent one HTTP GET request with the packet number 27039. (actually, there is one more to favicon.ico, but in the lab manual, it is said that we can ignore it)

No.	Time	Source	Destination	Protocol	Length	Info
27039	20.465260	192.168.1.11	128.119.245.12	HTTP	449	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
27440	20.817135	128.119.245.12	192.168.1.11	HTTP	559	HTTP/1.1 200 OK (text/html)
27513	20.861953	192.168.1.11	128.119.245.12	HTTP	406	GET /favicon.ico HTTP/1.1
27924	21.151250	128.119.245.12	192.168.1.11	HTTP	539	HTTP/1.1 404 Not Found (text/html)


```
> Frame 27039: 449 bytes on wire (3592 bits), 449 bytes captured (3592 bits)
> Ethernet II, Src: Apple_18:03:f1 (50:ed:3c:18:03:f1), Dst: zte_b1:ad:d8 (5c:a4:f4:b1:ad:d8)
> Internet Protocol Version 4, Src: 192.168.1.11, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 53877, Dst Port: 80, Seq: 1, Ack: 1, Len: 395
└ Hypertext Transfer Protocol
  └ GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file3.html
      Request Version: HTTP/1.1
      Host: gaia.cs.umass.edu\r\n
      User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/118.0\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n\r\n
      Accept-Language: en-US,en;q=0.5\r\n
      Accept-Encoding: gzip, deflate\r\n
      Connection: keep-alive\r\n
      Upgrade-Insecure-Requests: 1\r\n
      \r\n
```

0000	5c a4 f4 b1 ad d
0010	01 b3 00 00 40 0
0020	f5 0c d2 75 00 5
0030	10 00 cd 16 00 0
0040	68 61 72 6b 2d 6
0050	69 72 65 73 68 6
0060	74 6d 6c 20 48 5
0070	73 74 3a 20 67 6
0080	73 2e 65 64 75 0
0090	74 3a 20 4d 6f 7
00a0	4d 61 63 69 6e 7
00b0	20 4d 61 63 20 4
00c0	20 72 76 3a 31 3
00d0	2f 32 30 31 30 3
00e0	78 2f 31 31 38 2
00f0	20 74 65 78 74 2
0100	63 61 74 69 6f 6
0110	2c 61 70 70 6c 6
0120	3b 71 3d 30 2e 3
0130	66 2c 69 6d 61 6



Answer 13

The packet with packet number 27440 contains the status code and the corresponding phrase associated with the response to the HTTP GET request.

Answer 14

The status code and the phrase in the response were 200 OK.

Answer 15

The text of the Bill of Rights did not fit into one TCP segment, hence **4** data-containing TCP segments were needed to carry this big HTTP response.

4 HTML Documents with Embedded Objects

Answer 16

If we again exclude the HTTP GET request to favicon.ico, there were **3** HTTP GET requests that my browser sent. These requests below were sent to these addresses respectively:

```
128.119.245.12 → http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html
128.119.245.12 → http://gaia.cs.umass.edu/pearson.png
178.79.137.164 → http://kurose.csslash.net/8E_cover_small.jpg
```

No.	Time	Source	Destination	Protocol	Length	Info
23	6.309763	192.168.1.11	128.119.245.12	HTTP	449	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
25	6.489772	128.119.245.12	192.168.1.11	HTTP	1355	HTTP/1.1 200 OK (text/html)
31	6.543324	192.168.1.11	128.119.245.12	HTTP	406	GET /pearson.png HTTP/1.1
42	6.734339	128.119.245.12	192.168.1.11	HTTP	762	HTTP/1.1 200 OK (PNG)
57	6.840648	192.168.1.11	128.119.245.12	HTTP	406	GET /favicon.ico HTTP/1.1
60	6.860339	192.168.1.11	178.79.137.164	HTTP	385	GET /8E_cover_small.jpg HTTP/1.1
62	6.946782	178.79.137.164	192.168.1.11	HTTP	237	HTTP/1.1 301 Moved Permanently
65	7.020135	128.119.245.12	192.168.1.11	HTTP	538	HTTP/1.1 404 Not Found (text/html)
87	7.300187	192.168.1.11	23.213.161.18	OCSP	495	Request
89	7.370775	23.213.161.18	192.168.1.11	OCSP	955	Response


```
> Frame 23: 449 bytes on wire (3592 bits), 449 bytes captured (3592 bits)
> Ethernet II, Src: Apple_18:03:f1 (50:ed:3c:18:03:f1), Dst: zte_b1:ad:d8 (5c:a4:f4:b1:ad:d8)
> Internet Protocol Version 4, Src: 192.168.1.11, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 54202, Dst Port: 80, Seq: 1, Ack: 1, Len: 395
`- Hypertext Transfer Protocol
  `- GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file4.html
      Request Version: HTTP/1.1
      Host: gaia.cs.umass.edu\r\n
      User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/118.0\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
      Accept-Language: en-US,en;q=0.5\r\n
      Accept-Encoding: gzip, deflate\r\n
      Connection: keep-alive\r\n
      Upgrade-Insecure-Requests: 1\r\n
      \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]
```

0000	5c a4 f4 b1 ad
0010	01 b3 00 00 40
0020	f5 0c d3 ba 00
0030	10 00 60 33 00
0040	68 61 72 6b 2d
0050	69 72 65 73 68
0060	74 6d 6c 20 48
0070	73 74 3a 20 67
0080	73 2e 65 64 75
0090	74 3a 20 4d 6f
00a0	4d 61 63 69 6e
00b0	20 4d 61 63 20
00c0	20 72 76 3a 31
00d0	2f 32 30 31 30
00e0	78 2f 31 31 38
00f0	20 74 65 78 74
0100	63 61 74 69 6f
0110	2c 61 70 70 6c
0120	3b 71 3d 30 2e
0130	66 2c 69 6d 61
0140	3b 71 3d 30 2e

Answer 17

If we consider Time column in the packet-listing window, although I am not 100% sure if my browser downloaded these two images serially, it seems it downloaded serially because the second HTTP GET request for 8E_cover_small.jpg was sent after the HTTP response for pearson.png arrived. On the other hand, even though we excluded favicon.ico HTTP requests and responses, it is also possible that the browser used parallel downloading in some cases because packet 62 including the HTTP response is not the response to packet 57 including the HTTP request. However, I am convinced that the browser downloaded the two images serially, as explained above.

5 HTTP Authentication

Answer 18

The server returns the status code and phrase 401 Unauthorized to the initial HTTP GET request sent by the browser.

No.	Time	Source	Destination	Protocol	Length	Info
113	26.106006	192.168.1.11	128.119.245.12	HTTP	465	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
117	26.271651	128.119.245.12	192.168.1.11	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
195	48.492292	192.168.1.11	128.119.245.12	HTTP	524	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
197	48.654650	128.119.245.12	192.168.1.11	HTTP	544	HTTP/1.1 200 OK (text/html)
207	48.717677	192.168.1.11	128.119.245.12	HTTP	422	GET /favicon.ico HTTP/1.1
213	48.871342	128.119.245.12	192.168.1.11	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Answer 19

I merged two images so that you can see the difference very clearly. In the second HTTP GET request, Authorization: Basic header information was added as a new field.

```
^ Hypertext Transfer Protocol
  ^ GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
      Request Version: HTTP/1.1
      Host: gaia.cs.umass.edu\r\n
      User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/118.0\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
      Accept-Language: en-US,en;q=0.5\r\n
      Accept-Encoding: gzip, deflate\r\n
      Connection: keep-alive\r\n
      Upgrade-Insecure-Requests: 1\r\n
    \r\n
  ^ Hypertext Transfer Protocol
  ^ GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
      Request Version: HTTP/1.1
      Host: gaia.cs.umass.edu\r\n
      User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/118.0\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
      Accept-Language: en-US,en;q=0.5\r\n
      Accept-Encoding: gzip, deflate\r\n
      Connection: keep-alive\r\n
      Upgrade-Insecure-Requests: 1\r\n
    > Authorization: Basic d2lyZXNoYXJrLXN0dWRlbz0m5ldHdvcmzs=\r\n
    \r\n
```