

ECS 152A Programming 2

Daniel Phan
ID 914831996
Section A04

Noah Tarr
ID 917286014
Section A02

Due: 03/07/2021

1 HTTP Wireshark Lab

1.1 The Basic HTTP GET/Response Interaction

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

- Both my browser and the server are running HTTP version 1.1.

```

# Frame 55: 532 bytes on wire (4256 bits), 532 bytes captured (4256 bits) on interface wlp2s0, id 0
# Ethernet II, Src: RivetNet_e8:d3:fb (9c:b6:d0:e8:d3:fb), Dst: BelkinIn_78:10:f4 (14:91:82:78:10:f4)
# Internet Protocol Version 4, Src: 192.168.1.127, Dst: 128.119.245.12
# Transmission Control Protocol, Src Port: 55052, Dst Port: 80, Seq: 1, Ack: 1, Len: 466
# 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
  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/88.0.4324.150 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\r\n
  \r\n

# Frame 57: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface wlp2s0, id 0
# Ethernet II, Src: BelkinIn_78:10:f4 (14:91:82:78:10:f4), Dst: RivetNet_e8:d3:fb (9c:b6:d0:e8:d3:fb)
# Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.127
# Transmission Control Protocol, Src Port: 80, Dst Port: 55052, Seq: 1, Ack: 467, Len: 486
# 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, 04 Mar 2021 04:12:19 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: Wed, 03 Mar 2021 06:59:01 GMT\r\n
    ETag: "80-5bc9c62c44dfe"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
    \r\n

```

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

- My browser indicates that it accepts US English.

- ```

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
 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/88.0.4324.150 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\r\n

```

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

- My IP address is 192.168.1.127, while the server's IP address is 128.119.245.12.

- ```

- Internet Protocol Version 4, Src: 192.168.1.127, 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: 518
  Identification: 0x41f6 (16886)
  + Flags: 0x40, Don't fragment
  Fragment Offset: 0
  Time to Live: 64
  Protocol: TCP (6)
  Header Checksum: 0xbf50 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.127
  Destination Address: 128.119.245.12

```
- ```

- Internet Protocol Version 4, Src: 192.168.1.127, 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: 518
 Identification: 0x41f6 (16886)
 + Flags: 0x40, Don't fragment
 Fragment Offset: 0
 Time to Live: 64
 Protocol: TCP (6)
 Header Checksum: 0xbf50 [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 192.168.1.127
 Destination Address: 128.119.245.12

```

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

- The server returned 200 for the HTML file and 404 for favico.ico.

- ```

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, 04 Mar 2021 04:12:19 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: Wed, 03 Mar 2021 06:59:01 GMT\r\n
    ETag: "80-5bc9c62c44dfe"\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

```
- ```

Hypertext Transfer Protocol
 HTTP/1.1 404 Not Found\r\n
 [Expert Info (Chat/Sequence): HTTP/1.1 404 Not Found\r\n]
 Response Version: HTTP/1.1
 Status Code: 404
 [Status Code Description: Not Found]
 Response Phrase: Not Found
 Date: Thu, 04 Mar 2021 04:12:19 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
 Content-Length: 209\r\n
 Keep-Alive: timeout=5, max=99\r\n
 Connection: Keep-Alive\r\n
 Content-Type: text/html; charset=iso-8859-1\r\n
 \r\n
 [HTTP response 2/2]
 [Time since request: 0.095551449 seconds]

```

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

- It was last modified on March 3, 2021, at 06:59:01 GMT.

- ```

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, 04 Mar 2021 04:12:19 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: Wed, 03 Mar 2021 06:59:01 GMT\r\n
    ETag: "80-5bc9c62c44dfe"\r\n
    Accept-Ranges: bytes\r\n

```

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

- There were 128 bytes for the HTML file, and 209 bytes for favico.ico.

- ```

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, 04 Mar 2021 04:12:19 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: Wed, 03 Mar 2021 06:59:01 GMT\r\n
 ETag: "80-5bc9c62c44dfe"\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 1/2]

```
- ```

Hypertext Transfer Protocol
  HTTP/1.1 404 Not Found\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 404 Not Found\r\n]
      Response Version: HTTP/1.1
      Status Code: 404
      [Status Code Description: Not Found]
      Response Phrase: Not Found
      Date: Thu, 04 Mar 2021 04:12:19 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
    Content-Length: 209\r\n
      Keep-Alive: timeout=5, max=99\r\n
      Connection: Keep-Alive\r\n
      Content-Type: text/html; charset=iso-8859-1\r\n
      \r\n
    [HTTP response 2/2]
    [Time since request: 0.095551449 seconds]
  
```

- 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.
 - I do not see any headers that are not displayed.

Wireshark interface showing packet 55 (HTTP GET) and packet 56 (HTTP 200 OK). The packet list shows the source and destination IP addresses, the protocol, and the length of the packet. The packet details pane shows the structure of the HTTP packet, including the request line, headers, and body. The packet bytes pane shows the raw data of the packet.

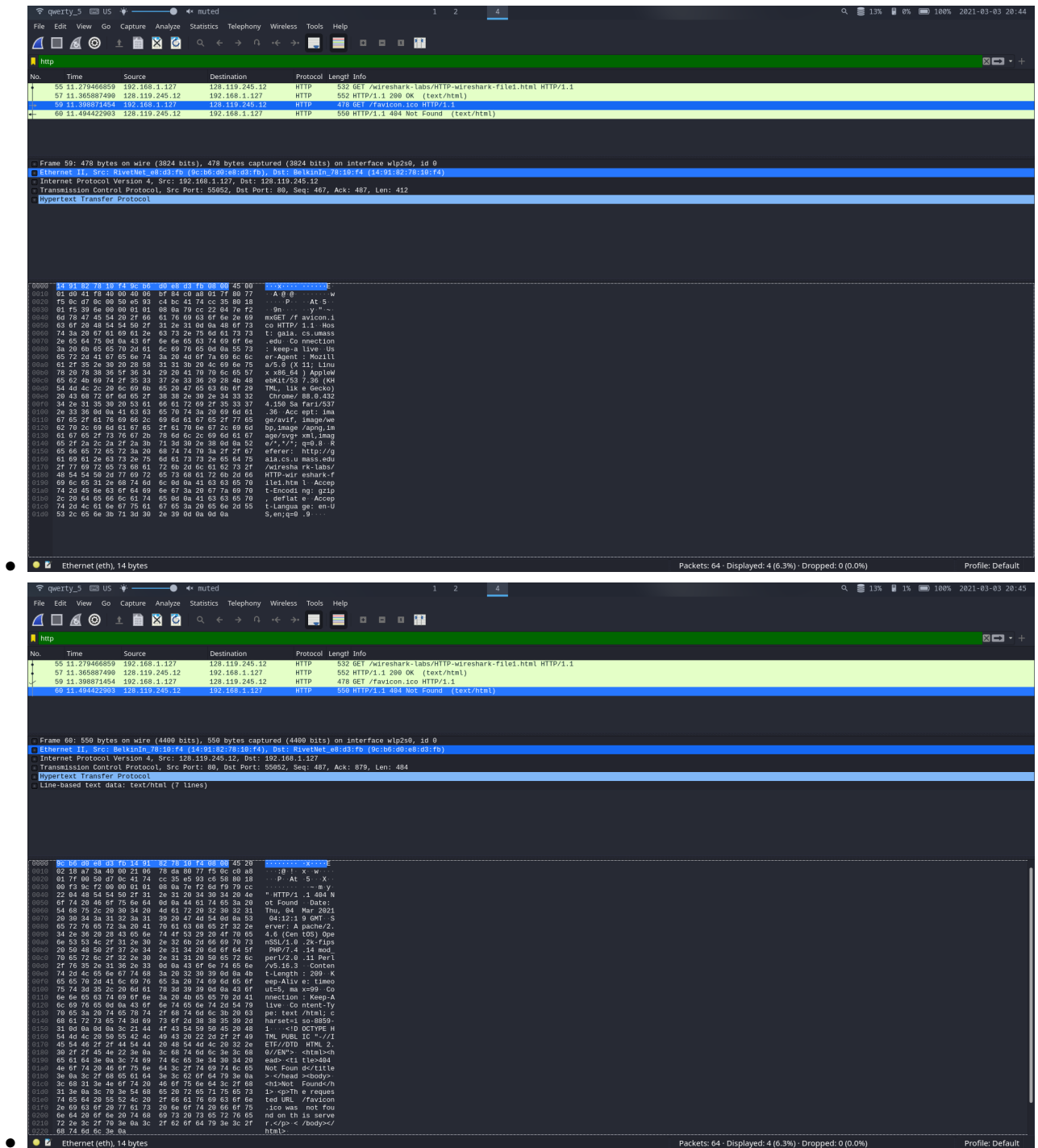
Frame 55: 592 bytes on wire (4256 bits), 592 bytes captured (4256 bits) on interface wlp2s0, id 0
Ethernet II, Src: Rivetnet.e8:d3:fb (9c:b6:d0:e8:d3:fb), Dst: Belkinin.78:16:f4 (14:91:82:78:16:f4)
Internet Protocol Version 4, Src: 192.168.1.127, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 55052, Dst Port: 80, Seq: 1, Ack: 1, Len: 466
Hypertext Transfer Protocol

Frame 56: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface wlp2s0, id 0
Ethernet II, Src: Belkinin.78:16:f4 (14:91:82:78:16:f4), Dst: Rivetnet.e8:d3:fb (9c:b6:d0:e8:d3:fb)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.127
Transmission Control Protocol, Src Port: 80, Dst Port: 55052, Seq: 1, Ack: 467, Len: 466
Hypertext Transfer Protocol
Line-based text data: text/html (4 lines)

Wireshark interface showing packet 57 (HTTP GET) and packet 58 (HTTP 200 OK). The packet list shows the source and destination IP addresses, the protocol, and the length of the packet. The packet details pane shows the structure of the HTTP packet, including the request line, headers, and body. The packet bytes pane shows the raw data of the packet.

Frame 57: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface wlp2s0, id 0
Ethernet II, Src: Belkinin.78:16:f4 (14:91:82:78:16:f4), Dst: Rivetnet.e8:d3:fb (9c:b6:d0:e8:d3:fb)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.127
Transmission Control Protocol, Src Port: 80, Dst Port: 55052, Seq: 1, Ack: 467, Len: 466
Hypertext Transfer Protocol
Line-based text data: text/html (4 lines)

Frame 58: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface wlp2s0, id 0
Ethernet II, Src: Rivetnet.e8:d3:fb (9c:b6:d0:e8:d3:fb), Dst: Belkinin.78:16:f4 (14:91:82:78:16:f4)
Internet Protocol Version 4, Src: 192.168.1.127, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 55052, Dst Port: 80, Seq: 1, Ack: 467, Len: 466
Hypertext Transfer Protocol



1.2 The HTTP GET/response interaction

- 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?

- I do not see an “IF-MODIFIED-SINCE” line in the HTTP GET.

```

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/88.0.4324.150 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\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
  [HTTP request 1/2]
  [Response in frame: 85]
  [Next request in frame: 88]

```

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

- The server explicitly returned the contents. I can tell because the response contains the HTML file content, and content fields like “Content-Type” and “Content Length” are set.

```

Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/2]
[Time since request: 0.088990448 seconds]
[Request in frame: 83]
[Next request in frame: 88]
[Next response in frame: 89]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
File Data: 371 bytes
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

```

```

Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Thu, 04 Mar 2021 04:59:38 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: Wed, 03 Mar 2021 06:59:01 GMT\r\n
  ETag: "173-5bc9c62c4462e"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 371\r\n
    [Content length: 371]
  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 1/2]
  [Time since request: 0.088990448 seconds]
  [Request in frame: 83]
  [Next request in frame: 88]
  [Next response in frame: 89]
  [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 GET? If so, what information

follows the “IF-MODIFIED-SINCE:” header?

- There is an “If-Modified-Since” line, and it contains “Wed, 03 Mar 2021 06:59:01 GMT”.

```
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/88.0.4324.150 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\r\n
If-None-Match: "173-5bc9c62c4462e"\r\n
If-Modified-Since: Wed, 03 Mar 2021 06:59:01 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?

- The HTTP status code is 304 and the response phrase is “Not Modified”. The server did not explicitly return the contents of the file, as none of the signs described in the response to question 9 appeared here.

```
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
```

1.3 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?

- My browser sent one HTTP GET request. The packet number was 63.

```
No.    Time           Source            Destination      Protocol  Length  Info
--
63    12.208433409    192.168.1.127     128.119.245.12   HTTP      532     GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
67    12.295984448    128.119.245.12    192.168.1.127   HTTP      3479    HTTP/1.1 200 OK (text/html)

Frame 63: 532 bytes on wire (4256 bits), 532 bytes captured (4256 bits) on interface wlp2s0, id 0
Ethernet II, Src: RivetNet_e8:d3:fb (9c:b6:d0:e8:d3:fb), Dst: BelkinIn_78:10:f4 (14:91:82:78:10:f4)
Internet Protocol Version 4, Src: 192.168.1.127, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 55892, Dst Port: 80, Seq: 1, Ack: 1, Len: 466
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
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/88.0.4324.150 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\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
[HTTP request 1/1]
[Response in frame 67]
```


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

- The packet number is 65. We see that the response was broken into 2 TCP segments. The raw data of the first segment, packet 65, is highlighted in blue, and we see the HTTP status code and phrase at the top of the raw data.

```

[2 Reassembled TCP Segments (4861 bytes): #65(1448), #67(3413)]
[Frame: 65, payload: 0-1447 (1448 bytes)]
[Frame: 67, payload: 1448-4860 (3413 bytes)]
[Segment count: 2]
[Reassembled TCP length: 4861]
[Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a4461746553a205468752c2030342
0000 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d HTTP/1.1 200 OK·
0010 0a 44 61 74 65 3a 20 54 68 75 2c 20 30 34 20 4d ·Date: T hu, 04 M
0020 61 72 20 32 30 32 31 20 30 35 3a 33 34 3a 34 33 ar 2021 05:34:43
0030 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70 GMT·Se rver: Ap
0040 61 63 68 65 2f 32 2e 34 2e 36 20 28 43 65 6e 74 ache/2.4 .6 (Cent
0050 4f 53 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 30 2e OS) Open SSL/1.0.
0060 32 6b 2d 66 69 70 73 20 50 48 50 2f 37 2e 34 2e 2k-fips PHP/7.4.
0070 31 34 20 6d 6f 64 5f 70 65 72 6c 2f 32 2e 30 2e 14 mod_p erl/2.0.
0080 31 31 20 50 65 72 6c 2f 76 35 2e 31 36 2e 33 0d 11 Perl/ v5.16.3·
0090 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64 3a 20 ·Last-Mo dified:
00a0 57 65 64 2c 20 30 33 20 4d 61 72 20 32 30 32 31 Wed, 03 Mar 2021
00b0 20 30 36 3a 35 39 3a 30 31 20 47 4d 54 0d 0a 45 06:59:0 1 GMT·E
00c0 54 61 67 3a 20 22 31 31 39 34 2d 35 62 63 39 63 Tag: "11 94-5bc9c
00d0 36 32 63 33 66 62 66 36 22 0d 0a 41 63 63 65 70 62c3fbf6 "··Accep
00e0 74 2d 52 61 6e 67 65 73 3a 20 62 79 74 65 73 0d t-Ranges : bytes·
00f0 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a ·Content -Length:
0100 20 34 35 30 30 0d 0a 4b 65 65 70 2d 41 6c 69 76 4500·K eep-Aliv
0110 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c 20 6d 61 e: timeo ut=5, ma
0120 78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63 74 69 6f x=100··C onnectio
0130 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 43 n: Keep- Alive··C
0140 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 ontent-T ype: tex
0150 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d t/html; charset=
0160 55 54 46 2d 38 0d 0a 0d 0a 3c 68 74 6d 6c 3e 3c UTF-8·· ·<html><

```

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

- The status code is 200, and the phrase is “OK”.

- [-] 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

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

- 2 data-containing TCP segments were needed.

- [2 Reassembled TCP Segments (4861 bytes): #65(1448), #67(3413)]
 - [Frame: 65, payload: 0-1447 (1448 bytes)]
 - [Frame: 67, payload: 1448-4860 (3413 bytes)]
 - [Segment count: 2]
 - [Reassembled TCP length: 4861]
 - [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a4461746553a205468752c203034204d61722032...]

1.4 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?

- 3 HTTP GET requests were sent. The first two went to 128.119.245.12 (gaia.cs.umass.edu), while the third went to 178.79.137.164 (kurose.cslash.net).

- | | | | | | | |
|-----|--------------|----------------|----------------|------|------|--|
| 89 | 16.301100606 | 192.168.1.127 | 128.119.245.12 | HTTP | 532 | GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1 |
| 91 | 16.387613418 | 128.119.245.12 | 192.168.1.127 | HTTP | 1367 | HTTP/1.1 200 OK (text/html) |
| 93 | 16.426631679 | 192.168.1.127 | 128.119.245.12 | HTTP | 478 | GET /pearson.png HTTP/1.1 |
| 99 | 16.513495514 | 128.119.245.12 | 192.168.1.127 | HTTP | 2229 | HTTP/1.1 200 OK (PNG) |
| 104 | 16.684490700 | 192.168.1.127 | 178.79.137.164 | HTTP | 445 | GET /8E_cover_small.jpg HTTP/1.1 |
| 108 | 16.898240272 | 178.79.137.164 | 192.168.1.127 | HTTP | 237 | HTTP/1.1 301 Moved Permanently |

- Internet Protocol Version 4, Src: 192.168.1.127, 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: 518
 - Identification: 0x067a (1658)
 - Flags: 0x40, Don't fragment
 - Fragment Offset: 0
 - Time to Live: 64
 - Protocol: TCP (6)
 - Header Checksum: 0xfacc [validation disabled]
 - [Header checksum status: Unverified]
 - Source Address: 192.168.1.127
 - Destination Address: 128.119.245.12

- 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
 - 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/88.0.4324.150 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\r\n

- Internet Protocol Version 4, Src: 192.168.1.127, 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: 464
 - Identification: 0x067c (1660)
 - Flags: 0x40, Don't fragment
 - Fragment Offset: 0
 - Time to Live: 64
 - Protocol: TCP (6)
 - Header Checksum: 0xfb00 [validation disabled]
 - [Header checksum status: Unverified]
 - Source Address: 192.168.1.127
 - Destination Address: 128.119.245.12
 - Hypertext Transfer Protocol
 - GET /pearson.png HTTP/1.1\r\n
 - Host: gaia.cs.umass.edu\r\n
 - Connection: keep-alive\r\n
 - User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36\r\n
 - Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
 - Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html\r\n
 - Accept-Encoding: gzip, deflate\r\n
 - Accept-Language: en-US,en;q=0.9\r\n
- Internet Protocol Version 4, Src: 192.168.1.127, Dst: 178.79.137.164
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 431
 - Identification: 0x542e (21550)
 - Flags: 0x40, Don't fragment
 - Fragment Offset: 0
 - Time to Live: 64
 - Protocol: TCP (6)
 - Header Checksum: 0xe6ff [validation disabled]
 - [Header checksum status: Unverified]
 - Source Address: 192.168.1.127
 - Destination Address: 178.79.137.164
 - Hypertext Transfer Protocol
 - GET /8E_cover_small.jpg HTTP/1.1\r\n
 - Host: kurose.cslash.net\r\n
 - Connection: keep-alive\r\n
 - User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36\r\n
 - Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
 - Referer: http://gaia.cs.umass.edu\r\n
 - Accept-Encoding: gzip, deflate\r\n
 - Accept-Language: en-US,en;q=0.9\r\n

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.

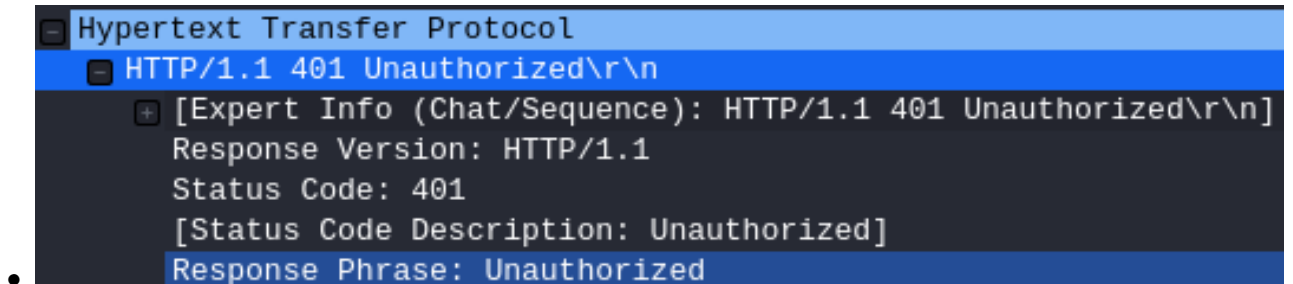
- The images were downloaded serially. The last packet for `pearson.png` (packet 99) arrived before the GET request for `8E_cover_small.jpg` (packet 104) was sent.

- | | | | | | |
|-----|--------------|----------------|----------------|------|--------------------------------------|
| 93 | 16.426631679 | 192.168.1.127 | 128.119.245.12 | HTTP | 478 GET /pearson.png HTTP/1.1 |
| 99 | 16.513495514 | 128.119.245.12 | 192.168.1.127 | HTTP | 2229 HTTP/1.1 200 OK (PNG) |
| 104 | 16.684490700 | 192.168.1.127 | 178.79.137.164 | HTTP | 445 GET /8E_cover_small.jpg HTTP/1.1 |
| 108 | 16.898240272 | 178.79.137.164 | 192.168.1.127 | HTTP | 237 HTTP/1.1 301 Moved Permanently |

1.5 HTTP Authentication

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

- The server responded with 401 and "Unauthorized".



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

- The "Authorization" and "Cache-Control" fields are new.

