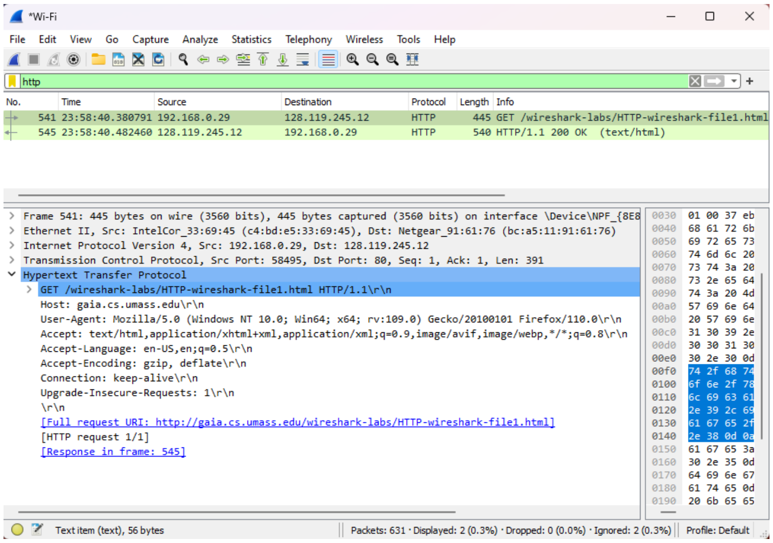
Vigomar Kim Algador
CPE 138 – 03
Professor Jun Dai
05 March 2023

Lab 2 – Wireshark – HTTP

Part 1: The Basic HTTP GET/response interaction


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

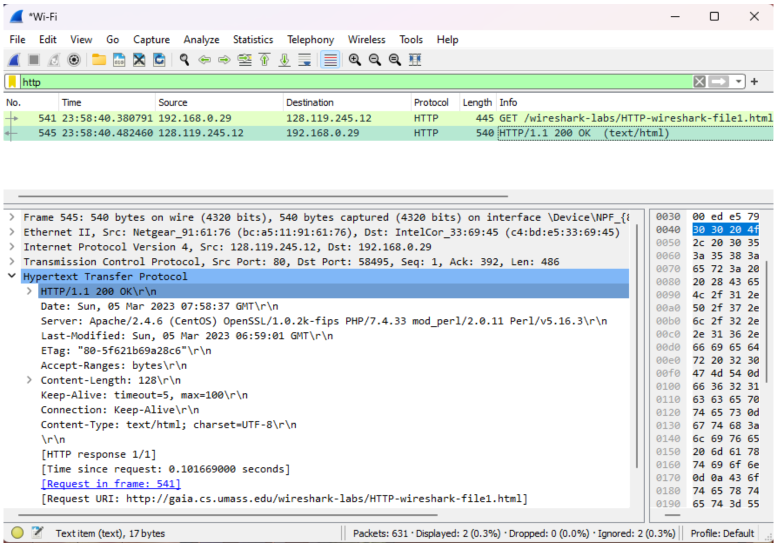
```
No.   Time            Source          Destination     Protocol Length Info
  541 23:58:40.380791 192.168.0.29    128.119.245.12  HTTP     445 GET /wireshark-labs/HTTP-wireshark-file1.html
  545 23:58:40.482460 128.119.245.12  192.168.0.29    HTTP     540 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 541: 445 bytes on wire (3560 bits), 445 bytes captured (3560 bits) on interface \Device\NPF_{8E8
> Ethernet II, Src: IntelCor_33:69:45 (c4:bd:e5:33:69:45), Dst: Netgear_91:61:76 (bc:a5:11:91:61:76)
> Internet Protocol Version 4, Src: 192.168.0.29, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 58495, Dst Port: 80, Seq: 1, Ack: 1, Len: 391
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0\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-file1.html]
    [HTTP request 1/1]
    [Response in frame: 545]
```

```
0030  01 00 37 eb
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  57 69 6e 64
00b0  20 57 69 6e
00c0  31 30 39 2e
00d0  30 30 31 30
00e0  30 2e 30 0d
00f0  74 2f 68 74
0100  6f 6e 2f 78
0110  6c 69 63 61
0120  2e 39 2c 69
0130  61 67 65 2f
0140  2e 38 0d 0a
0150  61 67 65 3a
0160  30 2e 35 0d
0170  64 69 6e 67
0180  61 74 65 0d
0190  20 6b 65 65
```

Text item (text), 56 bytes | Packets: 631 · Displayed: 2 (0.3%) · Dropped: 0 (0.0%) · Ignored: 2 (0.3%) | Profile: Default

Figure 1. Screenshot for GET


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

```
No.   Time            Source          Destination     Protocol Length Info
  541 23:58:40.380791 192.168.0.29    128.119.245.12  HTTP     445 GET /wireshark-labs/HTTP-wireshark-file1.html
  545 23:58:40.482460 128.119.245.12  192.168.0.29    HTTP     540 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 545: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{8
> Ethernet II, Src: Netgear_91:61:76 (bc:a5:11:91:61:76), Dst: IntelCor_33:69:45 (c4:bd:e5:33:69:45)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.29
> Transmission Control Protocol, Src Port: 80, Dst Port: 58495, Seq: 1, Ack: 392, Len: 486
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Sun, 05 Mar 2023 07:58:37 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: Sun, 05 Mar 2023 06:59:01 GMT\r\n
    ETag: "80-5f621b69a28c6"\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: 0.101669000 seconds]
    [Request in frame: 541]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
```

```
0030  00 ed e5 79
0040  30 30 20 4f
0050  2c 20 30 35
0060  3a 35 38 3a
0070  65 72 3a 20
0080  20 28 43 65
0090  4c 2f 31 2e
00a0  50 2f 37 2e
00b0  6c 2f 32 2e
00c0  2e 31 36 2e
00d0  66 69 65 64
00e0  72 20 32 30
00f0  47 4d 54 0d
0100  66 36 32 31
0110  63 63 65 70
0120  74 65 73 0d
0130  67 74 68 3a
0140  6c 69 76 65
0150  20 6d 61 78
0160  74 69 6f 6e
0170  0d 0a 43 6f
0180  74 65 78 74
0190  65 74 3d 55
```

Text item (text), 17 bytes | Packets: 631 · Displayed: 2 (0.3%) · Dropped: 0 (0.0%) · Ignored: 2 (0.3%) | Profile: Default

Figure 2. Screenshot for the response

Questions:

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
   The browser is running version 1.1
2. What languages (if any) does your browser indicate that it can accept to the server?
   Accept-Language: en-US (US English)
3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?
   The internet address of my computer is 192.168.0.29
   The internet address of the gaia.cs.umass.edu is 128.119.245.12
4. What is the status code returned from the server to your browser?
   200 OK
5. When was the HTML file that you are retrieving last modified at the server?
   If-Modified-Since: Sat, 04 Mar 2023 06:59:01 GMT

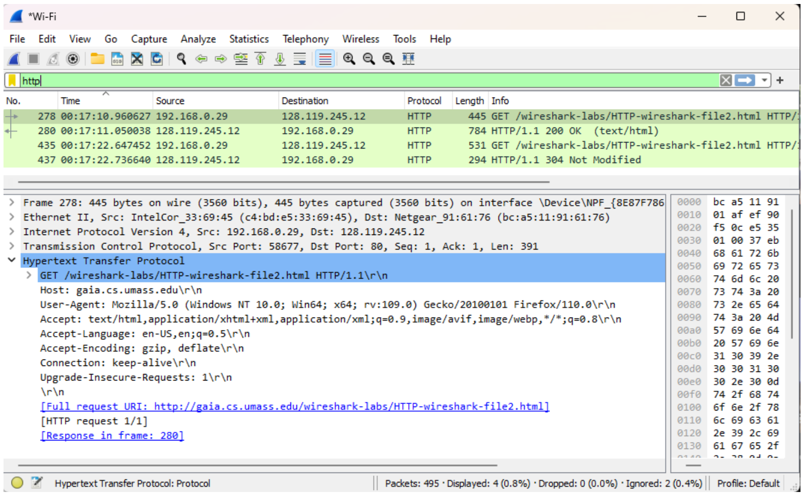
6. How many bytes of content are being returned to your browser?

    128

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.

    There are no any headers that are not displayed in the packet-listing window.

Part 2: The HTTP CONDITIONAL GET/response interaction



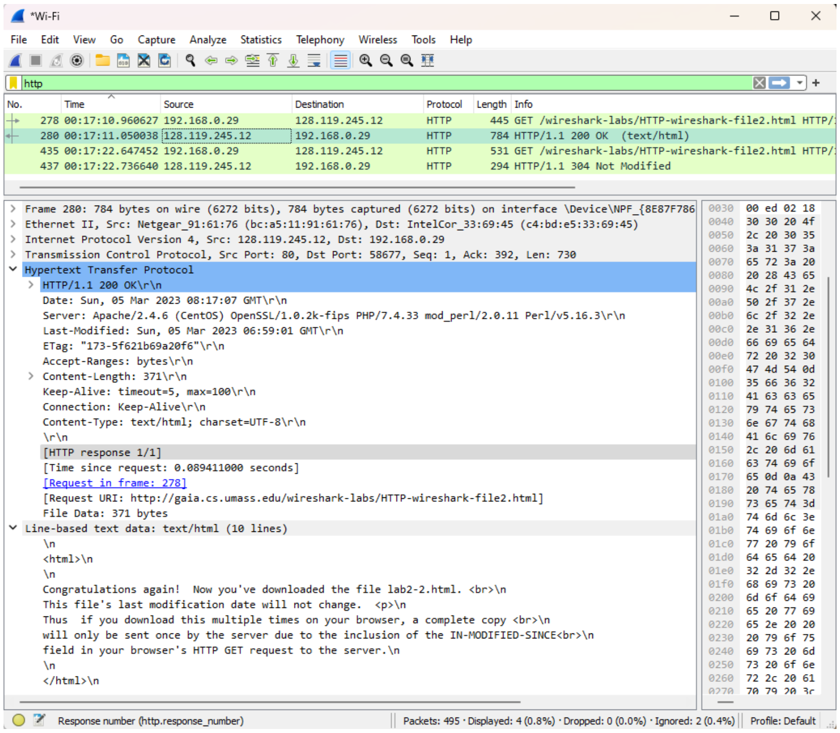
```
No.     Time            Source          Destination     Protocol Length Info
   278 00:17:10.960627 192.168.0.29    128.119.245.12  HTTP      445 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/
   280 00:17:11.050038 128.119.245.12  192.168.0.29    HTTP      784 HTTP/1.1 200 OK  (text/html)
   435 00:17:22.647452 192.168.0.29    128.119.245.12  HTTP      531 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/
   437 00:17:22.736640 128.119.245.12  192.168.0.29    HTTP      294 HTTP/1.1 304 Not Modified
```

```
> Frame 278: 445 bytes on wire (3560 bits), 445 bytes captured (3560 bits) on interface \Device\NPF_{8E87F786
> Ethernet II, Src: IntelCor_33:69:45 (c4:bd:e5:33:69:45), Dst: Netgear_91:61:76 (bc:a5:11:91:61:76)
> Internet Protocol Version 4, Src: 192.168.0.29, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 58677, Dst Port: 80, Seq: 1, Ack: 1, Len: 391
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0\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-file2.html]
    [HTTP request 1/1]
    [Response in frame: 280]
```

```
0000  bc a5 11 91
0010  01 af ef 90
0020  f5 0c e5 35
0030  01 00 37 eb
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  57 69 6e 64
00b0  20 57 69 6e
00c0  31 30 39 2e
00d0  30 30 31 30
00e0  30 2e 30 0d
00f0  74 2f 68 74
0100  6f 6e 2f 78
0110  6c 69 63 61
0120  2e 39 2c 69
0130  61 67 65 2f
```

```
Hypertext Transfer Protocol: Protocol    Packets: 495 · Displayed: 4 (0.8%) · Dropped: 0 (0.0%) · Ignored: 2 (0.4%)    Profile: Default
```

Figure 3. first HTTP GET



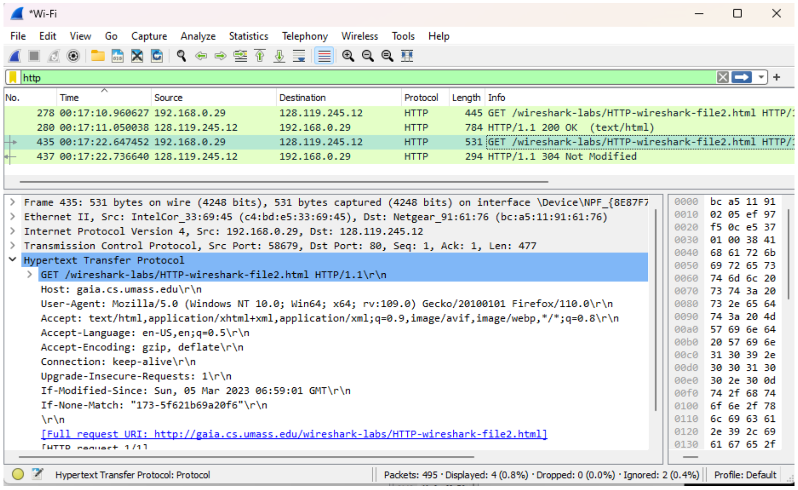
```
No.     Time            Source          Destination     Protocol Length Info
   278 00:17:10.960627 192.168.0.29    128.119.245.12  HTTP      445 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/
   280 00:17:11.050038 128.119.245.12  192.168.0.29    HTTP      784 HTTP/1.1 200 OK  (text/html)
   435 00:17:22.647452 192.168.0.29    128.119.245.12  HTTP      531 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/
   437 00:17:22.736640 128.119.245.12  192.168.0.29    HTTP      294 HTTP/1.1 304 Not Modified
```

```
> Frame 280: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{8E87F786
> Ethernet II, Src: Netgear_91:61:76 (bc:a5:11:91:61:76), Dst: IntelCor_33:69:45 (c4:bd:e5:33:69:45)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.29
> Transmission Control Protocol, Src Port: 80, Dst Port: 58677, Seq: 1, Ack: 392, Len: 730
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Sun, 05 Mar 2023 08:17:07 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: Sun, 05 Mar 2023 06:59:01 GMT\r\n
    ETag: "173-5f621b69a20f6"\r\n
    Accept-Ranges: bytes\r\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
    [HTTP response 1/1]
    [Time since request: 0.089411000 seconds]
    [Request in frame: 278]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    File Data: 371 bytes
v 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
```

```
0030  00 ed 02 18
0040  30 30 20 4f
0050  2c 20 30 35
0060  3a 31 37 3a
0070  65 72 3a 20
0080  20 28 43 65
0090  4c 2f 31 2e
00a0  50 2f 37 2e
00b0  6c 2f 32 2e
00c0  2e 31 36 2e
00d0  66 69 65 64
00e0  72 20 32 30
00f0  47 4d 54 0d
0100  35 66 36 32
0110  41 63 63 65
0120  79 74 65 73
0130  6e 67 74 68
0140  41 6c 69 76
0150  2c 20 6d 61
0160  63 74 69 6f
0170  65 0d 0a 43
0180  20 74 65 78
0190  73 65 74 3d
01a0  74 6d 6c 3e
01b0  74 69 6f 6e
01c0  77 20 79 6f
01d0  64 65 64 20
01e0  32 2d 32 2e
01f0  68 69 73 20
0200  6d 6f 64 69
0210  65 20 77 69
0220  65 2e 20 20
0230  20 79 6f 75
0240  69 73 20 6d
0250  73 20 6f 6e
0260  72 2c 20 61
0270  70 79 20 3c
```

```
Response number (http.response_number)    Packets: 495 · Displayed: 4 (0.8%) · Dropped: 0 (0.0%) · Ignored: 2 (0.4%)    Profile: Default
```

Figure 4. first HTTP response


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

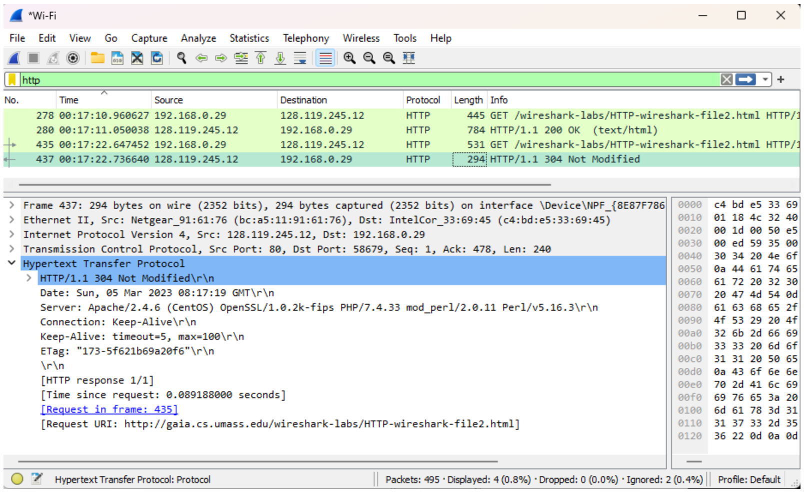
```
No.   Time            Source          Destination     Protocol Length Info
  278 00:17:10.960627 192.168.0.29    128.119.245.12  HTTP        445 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1
  280 00:17:11.050038 128.119.245.12  192.168.0.29    HTTP        784 HTTP/1.1 200 OK  (text/html)
  435 00:17:22.647452 192.168.0.29    128.119.245.12  HTTP        531 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1
  437 00:17:22.736640 128.119.245.12  192.168.0.29    HTTP        294 HTTP/1.1 304 Not Modified
```

```
> Frame 435: 531 bytes on wire (4248 bits), 531 bytes captured (4248 bits) on interface \Device\NPF_{8E87F7
> Ethernet II, Src: IntelCor_33:69:45 (c4:bd:e5:33:69:45), Dst: Netgear_91:61:76 (bc:a5:11:91:61:76)
> Internet Protocol Version 4, Src: 192.168.0.29, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 58679, Dst Port: 80, Seq: 1, Ack: 1, Len: 477
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0\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
    If-Modified-Since: Sun, 05 Mar 2023 06:59:01 GMT\r\n
    If-None-Match: "173-5f621b69a20f6"\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/1]
```

```
0000  bc a5 11 91
0010  02 05 ef 97
0020  f5 0c e5 37
0030  01 00 38 41
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  57 69 6e 64
00b0  20 57 69 6e
00c0  31 30 39 2e
00d0  30 30 31 30
00e0  30 2e 30 0d
00f0  74 2f 68 74
0100  6f 6e 2f 78
0110  6c 69 63 61
0120  2e 39 2c 69
0130  61 67 65 2f
```

Hypertext Transfer Protocol: Protocol | Packets: 495 · Displayed: 4 (0.8%) · Dropped: 0 (0.0%) · Ignored: 2 (0.4%) | Profile: Default

Figure 5. second HTTP GET


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time            Source          Destination     Protocol Length Info
  278 00:17:10.960627 192.168.0.29    128.119.245.12  HTTP        445 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1
  280 00:17:11.050038 128.119.245.12  192.168.0.29    HTTP        784 HTTP/1.1 200 OK  (text/html)
  435 00:17:22.647452 192.168.0.29    128.119.245.12  HTTP        531 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1
  437 00:17:22.736640 128.119.245.12  192.168.0.29    HTTP        294 HTTP/1.1 304 Not Modified
```

```
> Frame 437: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface \Device\NPF_{8E87F786
> Ethernet II, Src: Netgear_91:61:76 (bc:a5:11:91:61:76), Dst: IntelCor_33:69:45 (c4:bd:e5:33:69:45)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.29
> Transmission Control Protocol, Src Port: 80, Dst Port: 58679, Seq: 1, Ack: 478, Len: 240
v Hypertext Transfer Protocol
  > HTTP/1.1 304 Not Modified\r\n
    Date: Sun, 05 Mar 2023 08:17:19 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: "173-5f621b69a20f6"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.089188000 seconds]
    [Request in frame: 435]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

```
0000  c4 bd e5 33 69
0010  01 18 4c 32 40
0020  00 1d 00 50 e5
0030  00 ed 59 35 00
0040  30 34 20 4e 6f
0050  0a 44 61 74 65
0060  61 72 20 32 30
0070  20 47 4d 54 0d
0080  61 63 68 65 2f
0090  4f 53 29 20 4f
00a0  32 6b 2d 66 69
00b0  33 33 20 6d 6f
00c0  31 31 20 50 65
00d0  0a 43 6f 6e 6e
00e0  70 2d 41 6c 69
00f0  69 76 65 3a 20
0100  6d 61 78 3d 31
0110  31 37 33 2d 35
0120  36 22 0d 0a 0d
```

Hypertext Transfer Protocol: Protocol | Packets: 495 · Displayed: 4 (0.8%) · Dropped: 0 (0.0%) · Ignored: 2 (0.4%) | Profile: Default

Figure 6. second HTTP response

Questions:

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?

   There is no "IF-MODIFIED-SINCE" line in the first HTTP GET.

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 returns the contents of the file under the Line-based text data. It shows the exact message on the website.

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?

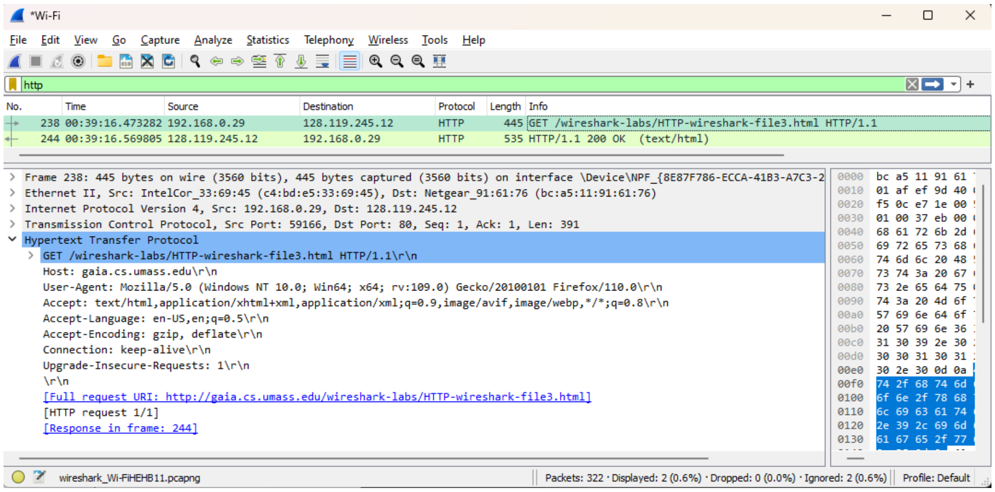
    There is "IF-MODIFIED-SINCE:" line in the second HTTP GET.

    If-Modified-Since: Sun, 05 Mar 2023 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? Explain.

    The status of the second HTTP GET is 304 Not Modified. The server didn't return the contents of the file because the browser retrieved it from the cache since the HTML file had been accessed before.

Part 3: Retrieving Long Documents


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

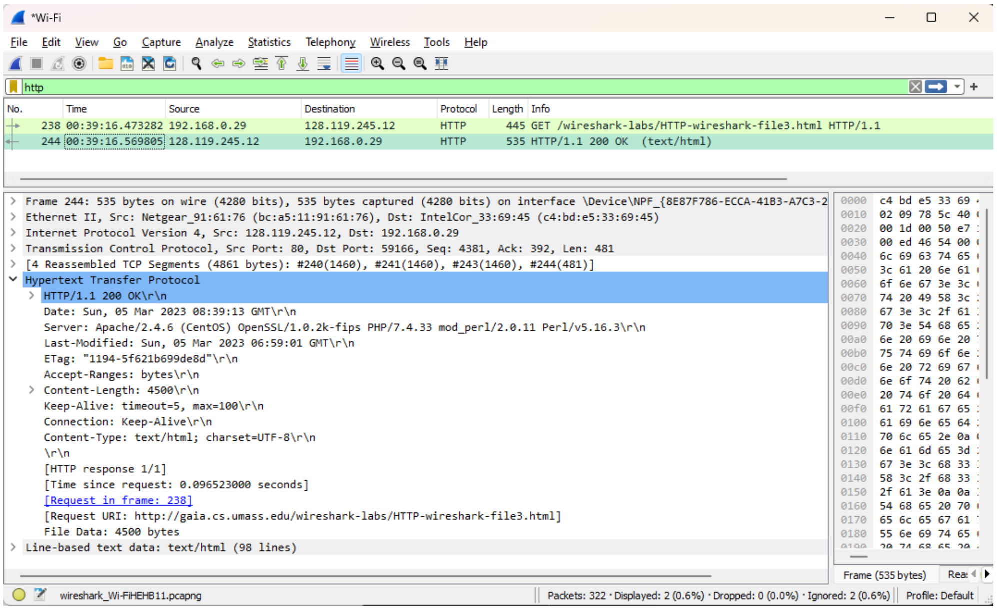
```
No.  Time            Source         Destination    Protocol Length Info
 238 00:39:16.473282 192.168.0.29   128.119.245.12 HTTP        445 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
 244 00:39:16.569805 128.119.245.12 192.168.0.29   HTTP        535 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 238: 445 bytes on wire (3560 bits), 445 bytes captured (3560 bits) on interface \Device\NPF_{8E87F786-ECCA-41B3-A7C3-2
> Ethernet II, Src: IntelCor_33:69:45 (c4:bd:e5:33:69:45), Dst: Netgear_91:61:76 (bc:a5:11:91:61:76)
> Internet Protocol Version 4, Src: 192.168.0.29, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 59166, Dst Port: 80, Seq: 1, Ack: 1, Len: 391
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0\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-file3.html]
    [HTTP request 1/1]
    [Response in frame: 244]
```

```
0000  bc a5 11 91 61
0010  01 af ef 9d 40
0020  f5 0c e7 1e 00
0030  01 00 37 eb 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  57 69 6e 64 6f
00b0  20 57 69 6e 36
00c0  31 30 39 2e 30
00d0  30 30 31 30 31
00e0  30 2e 30 0d 0a
00f0  74 2f 68 74 6d
0100  6f 6e 2f 78 68
0110  6c 69 63 61 74
0120  2e 39 2c 69 6d
0130  61 67 65 2f 77
```

```
wireshark_Wi-FiHEHB11.pcapng    Packets: 322 · Displayed: 2 (0.6%) · Dropped: 0 (0.0%) · Ignored: 2 (0.6%)    Profile: Default
```

Figure 7. screenshot of GET for US Bill of Rights file


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.  Time            Source         Destination    Protocol Length Info
 238 00:39:16.473282 192.168.0.29   128.119.245.12 HTTP        445 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
 244 00:39:16.569805 128.119.245.12 192.168.0.29   HTTP        535 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 244: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{8E87F786-ECCA-41B3-A7C3-2
> Ethernet II, Src: Netgear_91:61:76 (bc:a5:11:91:61:76), Dst: IntelCor_33:69:45 (c4:bd:e5:33:69:45)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.29
> Transmission Control Protocol, Src Port: 80, Dst Port: 59166, Seq: 4381, Ack: 392, Len: 481
> [4 Reassembled TCP Segments (4861 bytes): #240(1460), #241(1460), #243(1460), #244(481)]
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Sun, 05 Mar 2023 08:39:13 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: Sun, 05 Mar 2023 06:59:01 GMT\r\n
    ETag: "1194-5f621b699de8d"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 4500\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: 0.096523000 seconds]
    [Request in frame: 238]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
    File Data: 4500 bytes
> Line-based text data: text/html (98 lines)
```

```
0000  c4 bd e5 33 69
0010  02 09 78 5c 40
0020  00 1d 00 50 e7
0030  00 ed 46 54 00
0040  6c 69 63 74 65
0050  3c 61 20 6e 61
0060  6f 6e 67 3e 3c
0070  74 20 49 58 3c
0080  67 3e 3c 2f 61
0090  70 3e 54 68 65
00a0  6e 20 69 6e 20
00b0  75 74 69 6f 6e
00c0  6e 20 72 69 67
00d0  6e 6f 74 20 62
00e0  20 74 6f 20 64
00f0  61 72 61 67 65
0100  61 69 6e 65 64
0110  70 6c 65 2e 0a
0120  6e 61 6d 65 3d
0130  67 3e 3c 68 33
0140  58 3c 2f 68 33
0150  2f 61 3e 0a 0a
0160  54 68 65 20 70
0170  65 6c 65 67 61
0180  55 6e 69 74 65
```

```
Frame (535 bytes)    Rea:
wireshark_Wi-FiHEHB11.pcapng    Packets: 322 · Displayed: 2 (0.6%) · Dropped: 0 (0.0%) · Ignored: 2 (0.6%)    Profile: Default
```

Figure 8. screenshot of response for US Bill of Rights file

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?

    There is only 1 HTTP GET request message. The packet number is 238.

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 244.

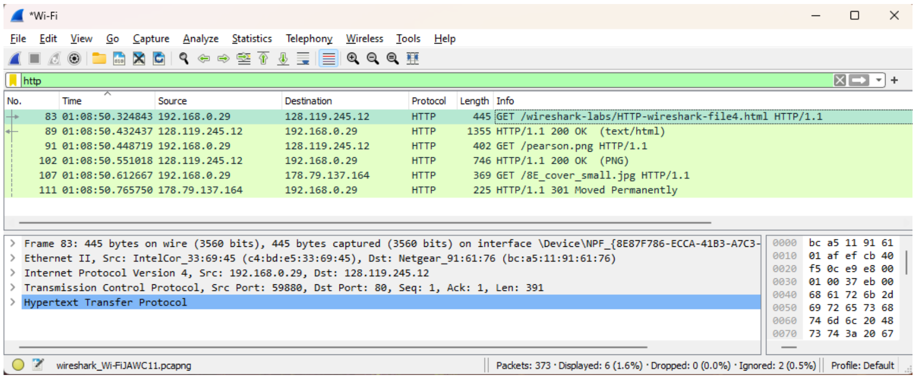
14. What is the status code and phrase in the response?

    Status code is 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?

    There are 4 TCP segments.

Part 4: HTML Documents with Embedded Objects


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.  Time            Source          Destination     Protocol Length Info
 83 01:08:50.324843 192.168.0.29    128.119.245.12  HTTP      445 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
 89 01:08:50.432437 128.119.245.12  192.168.0.29    HTTP     1355 HTTP/1.1 200 OK  (text/html)
 91 01:08:50.448719 192.168.0.29    128.119.245.12  HTTP      402 GET /pearson.png HTTP/1.1
102 01:08:50.551018 128.119.245.12  192.168.0.29    HTTP      746 HTTP/1.1 200 OK  (PNG)
107 01:08:50.612667 192.168.0.29    178.79.137.164  HTTP      369 GET /8E_cover_small.jpg HTTP/1.1
111 01:08:50.765750 178.79.137.164  192.168.0.29    HTTP      225 HTTP/1.1 301 Moved Permanently
```

```
> Frame 83: 445 bytes on wire (3560 bits), 445 bytes captured (3560 bits) on interface \Device\NPF_{8E87F786-ECCA-41B3-A7C3-
> Ethernet II, Src: IntelCor_33:69:45 (c4:bd:e5:33:69:45), Dst: Netgear_91:61:76 (bc:a5:11:91:61:76)
> Internet Protocol Version 4, Src: 192.168.0.29, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 59880, Dst Port: 80, Seq: 1, Ack: 1, Len: 391
> Hypertext Transfer Protocol
```

```
0000  bc a5 11 91 61
0010  01 af ef cb 40
0020  f5 0c e9 e8 00
0030  01 00 37 eb 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
```

```
wireshark_Wi-FiJAWC11.pcapng    Packets: 373 · Displayed: 6 (1.6%) · Dropped: 0 (0.0%) · Ignored: 2 (0.5%)    Profile: Default
```

Figure 9. Screenshot of all the packet GET/response from file 4

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

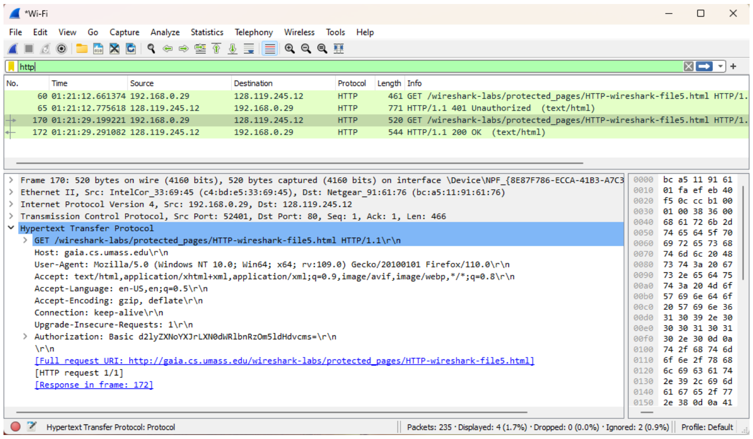
    There are 3 HTTP GET request messages. The internet addresses are:

    - Main: 128.119.245.12
    - pearson.png: 128.119.245.12
    - 8E_cover_small.jpg: 178.79.137.164

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 two images were downloaded serially because the first image, which is the logo, was requested before the second image, the book cover. If it's in parallel, both images should be requested and returned at the same time.

Part 5: HTTP Authentication


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.  Time            Source          Destination     Protocol Length Info
 60 01:21:12.661374 192.168.0.29    128.119.245.12  HTTP      461 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.
 65 01:21:12.775618 128.119.245.12  192.168.0.29    HTTP      771 HTTP/1.1 401 Unauthorized  (text/html)
170 01:21:29.199221 192.168.0.29    128.119.245.12  HTTP      520 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.
172 01:21:29.291082 128.119.245.12  192.168.0.29    HTTP      544 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 170: 520 bytes on wire (4160 bits), 520 bytes captured (4160 bits) on interface \Device\NPF_{8E87F786-ECCA-41B3-A7C3
> Ethernet II, Src: IntelCor_33:69:45 (c4:bd:e5:33:69:45), Dst: Netgear_91:61:76 (bc:a5:11:91:61:76)
> Internet Protocol Version 4, Src: 192.168.0.29, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 52401, Dst Port: 80, Seq: 1, Ack: 1, Len: 466
v Hypertext Transfer Protocol
  > GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0\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 d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
    [HTTP request 1/1]
    [Response in frame: 172]
```

```
0000  bc a5 11 91 61
0010  01 fa ef eb 40
0020  f5 0c cc b1 00
0030  01 00 38 36 00
0040  68 61 72 6b 2d
0050  74 65 64 5f 70
0060  69 72 65 73 68
0070  74 6d 6c 20 48
0080  73 74 3a 20 67
0090  73 2e 65 64 75
00a0  74 3a 20 4d 6f
00b0  57 69 6e 64 6f
00c0  20 57 69 6e 36
00d0  31 30 39 2e 30
00e0  30 30 31 30 31
00f0  30 2e 30 0d 0a
0100  74 2f 68 74 6d
0110  6f 6e 2f 78 68
0120  6c 69 63 61 74
0130  2e 39 2c 69 6d
0140  61 67 65 2f 77
0150  2e 38 0d 0a 41
```

```
Hypertext Transfer Protocol: Protocol    Packets: 235 · Displayed: 4 (1.7%) · Dropped: 0 (0.0%) · Ignored: 2 (0.9%)    Profile: Default
```

Figure 9. Screenshot for the authentication file

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

    401 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?

    There is a new field called Authorization which shows the credentials (username and password).