Computer Networks Lab 1

Shane Cincotta

March 11, 2020

/tmp/wireshark_wlp6s0_20200310151227_EgKPqE.pcapng 36 total packets, 2 shown

```
No.    Time         Source           Destination        Protocol Length Info
    15 1.939780707  192.168.1.216    128.119.245.12     HTTP     442    GET /wireshark-labs/HTTP-wireshark-
file1.html HTTP/1.1
Frame 15: 442 bytes on wire (3536 bits), 442 bytes captured (3536 bits) on interface 0
Ethernet II, Src: AskeyCom_49:ad:62 (e8:d1:1b:49:ad:62), Dst: Verizon_58:d5:33 (20:c0:47:58:d5:33)
Internet Protocol Version 4, Src: 192.168.1.216, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 45502, Dst Port: 80, Seq: 1, Ack: 1, Len: 376
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 (X11; Ubuntu; Linux x86_64; rv:73.0) Gecko/20100101 Firefox/73.0\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
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 24]
No.    Time         Source           Destination        Protocol Length Info
    24 1.959686932  128.119.245.12   192.168.1.216      HTTP     552    HTTP/1.1 200 OK  (text/html)
Frame 24: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface 0
Ethernet II, Src: Verizon_58:d5:33 (20:c0:47:58:d5:33), Dst: AskeyCom_49:ad:62 (e8:d1:1b:49:ad:62)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.216
Transmission Control Protocol, Src Port: 80, Dst Port: 45502, Seq: 1, Ack: 377, Len: 486
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Tue, 10 Mar 2020 19:12:30 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Tue, 10 Mar 2020 05:59:02 GMT\r\n
    ETag: "80-5a079d11503fc"\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: 0.019906225 seconds]
    [Request in frame: 15]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    File Data: 128 bytes
Line-based text data: text/html (4 lines)
```

Figure 1:

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

a) According to figure 1, my browser is running HTTP version 1.1.

b) According to figure 1, the server is running HTTP version 1.1.

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

a) According to figure 1, my browser can accept en-US, en.

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

a) According to figure 1, the IP address of my computer is 192.168.1.216

b) According to figure 1, the IP address of the server is 128.119.245.12

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

a) According to figure 1, the status code returned is HTTP/1.1 200 OK (text/html)

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

a) According to figure 1, the HTML was Last-Modified: Tue, 10 Mar 2020 05:59:02 GMT

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

a) According to figure 1, there are 128 bytes of content being returned to my browser.

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.

a) No, I don't see any headers that are not displayed in the packet-listing window.

```
No.    Time          Source          Destination     Protocol Length Info
    65 5.839778844   192.168.1.216   128.119.245.12  HTTP     442    GET /wireshark-labs/HTTP-wireshark-
file2.html HTTP/1.1
Frame 65: 442 bytes on wire (3536 bits), 442 bytes captured (3536 bits) on interface 0
Ethernet II, Src: AskeyCom_49:ad:62 (e8:d1:1b:49:ad:62), Dst: Verizon_58:d5:33 (20:c0:47:58:d5:33)
Internet Protocol Version 4, Src: 192.168.1.216, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 35580, Dst Port: 80, Seq: 1, Ack: 1, Len: 376
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 (X11; Ubuntu; Linux x86_64; rv:73.0) Gecko/20100101 Firefox/73.0\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
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/1]
    [Response in frame: 75]
No.    Time          Source          Destination     Protocol Length Info
    75 5.862513494   128.119.245.12  192.168.1.216   HTTP     796    HTTP/1.1 200 OK  (text/html)
Frame 75: 796 bytes on wire (6368 bits), 796 bytes captured (6368 bits) on interface 0
Ethernet II, Src: Verizon_58:d5:33 (20:c0:47:58:d5:33), Dst: AskeyCom_49:ad:62 (e8:d1:1b:49:ad:62)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.216
Transmission Control Protocol, Src Port: 80, Dst Port: 35580, Seq: 1, Ack: 377, Len: 730
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Wed, 11 Mar 2020 03:14:37 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Tue, 10 Mar 2020 05:59:02 GMT\r\n
    ETag: "173-5a079d114ae0b"\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: 0.022734650 seconds]
    [Request in frame: 65]
    [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
No.    Time          Source          Destination     Protocol Length Info
   153 17.187609405  192.168.1.216   128.119.245.12  HTTP     554    GET /wireshark-labs/HTTP-wireshark-
file2.html HTTP/1.1
Frame 153: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface 0
Ethernet II, Src: AskeyCom_49:ad:62 (e8:d1:1b:49:ad:62), Dst: Verizon_58:d5:33 (20:c0:47:58:d5:33)
Internet Protocol Version 4, Src: 192.168.1.216, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 35584, Dst Port: 80, Seq: 1, Ack: 1, Len: 488
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 (X11; Ubuntu; Linux x86_64; rv:73.0) Gecko/20100101 Firefox/73.0\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: Tue, 10 Mar 2020 05:59:02 GMT\r\n
    If-None-Match: "173-5a079d114ae0b"\r\n
    Cache-Control: max-age=0\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: 155]
No.    Time          Source          Destination     Protocol Length Info
   155 17.228910957  128.119.245.12  192.168.1.216   HTTP     306    HTTP/1.1 304 Not Modified
Frame 155: 306 bytes on wire (2448 bits), 306 bytes captured (2448 bits) on interface 0
Ethernet II, Src: Verizon_58:d5:33 (20:c0:47:58:d5:33), Dst: AskeyCom_49:ad:62 (e8:d1:1b:49:ad:62)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.216
Transmission Control Protocol, Src Port: 80, Dst Port: 35584, Seq: 1, Ack: 489, Len: 240
Hypertext Transfer Protocol
```

Figure 2:

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?

a) According to figure 2, I do not see an "IF-MODIFIED-SINCE" line in the HTTP GET.

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

a) According to figure 2, yes the server did. I can tell because I can see the contents of the file in the "Line-based text data" field.

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?

a) According to figure 2, yes. The information that follows is: Tue, 10 Mar 2020 05:59:02 GMT which is the date of the last modification of the file from the previous get request.

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.

a) According to figure 2, the status code and phrase returned from the server is HTTP/1.1 304 Not Modified. The server didn't return the contents of the file since the browser loaded it from its cache.

```
/tmp/wireshark_wlp6s0_20200311002812_NjrvNv.pcapng 120 total packets, 2 shown

No.    Time          Source              Destination         Protocol Length Info
   79 3.328021221   192.168.1.216       128.119.245.12      HTTP     442    GET /wireshark-labs/HTTP-wireshark-
file3.html HTTP/1.1
Frame 79: 442 bytes on wire (3536 bits), 442 bytes captured (3536 bits) on interface 0
Ethernet II, Src: AskeyCom_49:ad:62 (e8:d1:1b:49:ad:62), Dst: Verizon_58:d5:33 (20:c0:47:58:d5:33)
Internet Protocol Version 4, Src: 192.168.1.216, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 37144, Dst Port: 80, Seq: 1, Ack: 1, Len: 376
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 (X11; Ubuntu; Linux x86_64; rv:73.0) Gecko/20100101 Firefox/73.0\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
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
    [HTTP request 1/1]
    [Response in frame: 87]
No.    Time          Source              Destination         Protocol Length Info
   87 3.343268697   128.119.245.12      192.168.1.216       HTTP     583    HTTP/1.1 200 OK  (text/html)
Frame 87: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface 0
Ethernet II, Src: Verizon_58:d5:33 (20:c0:47:58:d5:33), Dst: AskeyCom_49:ad:62 (e8:d1:1b:49:ad:62)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.216
Transmission Control Protocol, Src Port: 80, Dst Port: 37144, Seq: 4345, Ack: 377, Len: 517
[2 Reassembled TCP Segments (4861 bytes): #85(4344), #87(517)]
    [Frame: 85, payload: 0-4343 (4344 bytes)]
    [Frame: 87, payload: 4344-4860 (517 bytes)]
    [Segment count: 2]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2057...]
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Wed, 11 Mar 2020 04:28:15 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Tue, 10 Mar 2020 05:59:02 GMT\r\n
    ETag: "1194-5a079d113b022"\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: 0.015247476 seconds]
    [Request in frame: 79]
    [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)
```

Figure 3:

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?

a) According to figure 3, there was 1 HTTP GET requests message that my browser sent.

b) According to figure 3, the packet is number 79 in the trace.

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

a) According to figure 3, the packet number in the trace which contains the status code and phrase is 87.

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

a) According to figure 3, the status code is 200 and the phrase in the response is "OK".

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

a) According to figure 3, 2 TCP segments were needed to carry the single HTTP response.

```
/tmp/wireshark_wlp6s0_20200311131904_7vcRYE.pcapng 148 total packets, 6 shown

No.     Time           Source                Destination           Protocol Length Info
     58 3.560493484    192.168.1.216         128.119.245.12        HTTP     442    GET /wireshark-labs/HTTP-wireshark-
file4.html HTTP/1.1
Frame 58: 442 bytes on wire (3536 bits), 442 bytes captured (3536 bits) on interface 0
Ethernet II, Src: AskeyCom_49:ad:62 (e8:d1:1b:49:ad:62), Dst: Verizon_58:d5:33 (20:c0:47:58:d5:33)
Internet Protocol Version 4, Src: 192.168.1.216, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 44976, Dst Port: 80, Seq: 1, Ack: 1, Len: 376
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 (X11; Ubuntu; Linux x86_64; rv:74.0) Gecko/20100101 Firefox/74.0\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
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]
    [HTTP request 1/1]
    [Response in frame: 63]
No.     Time           Source                Destination           Protocol Length Info
     63 3.584841287    128.119.245.12        192.168.1.216         HTTP     1139   HTTP/1.1 200 OK  (text/html)
Frame 63: 1139 bytes on wire (9112 bits), 1139 bytes captured (9112 bits) on interface 0
Ethernet II, Src: Verizon_58:d5:33 (20:c0:47:58:d5:33), Dst: AskeyCom_49:ad:62 (e8:d1:1b:49:ad:62)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.216
Transmission Control Protocol, Src Port: 80, Dst Port: 44976, Seq: 1, Ack: 377, Len: 1073
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: Wed, 11 Mar 2020 17:19:07 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Wed, 11 Mar 2020 05:59:01 GMT\r\n
    ETag: "2ca-5a08deed646d6"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 714\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: 0.024347803 seconds]
    [Request in frame: 58]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]
    File Data: 714 bytes
Line-based text data: text/html (17 lines)
No.     Time           Source                Destination           Protocol Length Info
     69 3.669434767    192.168.1.216         128.119.245.12        HTTP     399    GET /pearson.png HTTP/1.1
Frame 69: 399 bytes on wire (3192 bits), 399 bytes captured (3192 bits) on interface 0
Ethernet II, Src: AskeyCom_49:ad:62 (e8:d1:1b:49:ad:62), Dst: Verizon_58:d5:33 (20:c0:47:58:d5:33)
Internet Protocol Version 4, Src: 192.168.1.216, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 44978, Dst Port: 80, Seq: 1, Ack: 1, Len: 333
Hypertext Transfer Protocol
    GET /pearson.png HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /pearson.png HTTP/1.1\r\n]
        Request Method: GET
        Request URI: /pearson.png
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:74.0) Gecko/20100101 Firefox/74.0\r\n
    Accept: image/webp,*/*\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/pearson.png]
    [HTTP request 1/1]
    [Response in frame: 75]
No.     Time           Source                Destination           Protocol Length Info
     74 3.686187799    192.168.1.216         128.119.245.12        HTTP     413    GET /~kurose/cover_5th_ed.jpg HTTP/1.1
Frame 74: 413 bytes on wire (3304 bits), 413 bytes captured (3304 bits) on interface 0
Ethernet II, Src: AskeyCom_49:ad:62 (e8:d1:1b:49:ad:62), Dst: Verizon_58:d5:33 (20:c0:47:58:d5:33)
Internet Protocol Version 4, Src: 192.168.1.216, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 44980, Dst Port: 80, Seq: 1, Ack: 1, Len: 347
Hypertext Transfer Protocol
    GET /~kurose/cover_5th_ed.jpg HTTP/1.1\r\n
```

Figure 4:

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

a) According to figure 4, there were 3 GET messages sent

b) According to figure 4, the get messages were sent to 128.119.245.12

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.

a) We can look at the GET messages and determine if the images were sent in serial or parallel. According to figure 4, the GET messssage for the second image was sent before the first image was received. Thus the images were sent in parallel.

Figure 5:

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

a) According to figure 5, the server's response is 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?

a) According to figure 5, an Authorization field is now added.