Christopher Desir
Cd2902@nyu.edu
Week 4: Wireshark Lab: HTTP

1) The browser is running HTTP version 1.1 and Sever is running the same version as well.
2) The languages can accept English to the server.
3) The IP address of gaia.csumass.edu is 128.119.245.12
4) The status code for my browser is 200 OK
5) The HTML file that I retrieved modified at Tue, 01 Oct 2019 05:59:01 GMT
6) 128 bytes of content are being returned to my browser.

Christopher Desir
Cd2902@nyu.edu
Week 4: Wireshark Lab: HTTP

```
<html>\n
Congratulations.  You've downloaded the file \n
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
</html>\n
```

7) I see the data which is not listed in the packet listing window.

```
No.     Time                           Source                Destination           Protocol Length Info
     49 2019-10-01 20:12:48.465526     128.119.245.12        192.168.1.249         HTTP     784    HTTP/1.1 200 OK  (text/html)
Frame 49: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface 0
Ethernet II, Src: AsustekC_d3:3e:b4 (1c:87:2c:d3:3e:b4), Dst: Micro-St_92:30:cb (4c:cc:6a:92:30:cb)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.249
Transmission Control Protocol, Src Port: 80, Dst Port: 53030, Seq: 1, Ack: 368, Len: 730
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
            [HTTP/1.1 200 OK\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Wed, 02 Oct 2019 00:12:47 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Tue, 01 Oct 2019 05:59:01 GMT\r\n
    ETag: "173-593d30c88d995"\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: 0.025642000 seconds]
    [Request in frame: 47]
    [Next request in frame: 51]
    [Next response in frame: 53]
    [Request URI: http://gaia.cs.umass.edu/favicon.ico]
    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
```

Christopher Desir
Cd2902@nyu.edu
Week 4: Wireshark Lab: HTTP

```
No.     Time                           Source                Destination           Protocol Length Info
     53 2019-10-01 20:12:48.806118     128.119.245.12        192.168.1.249         HTTP     538    HTTP/1.1 404 Not Found  (text/
Frame 53: 538 bytes on wire (4304 bits), 538 bytes captured (4304 bits) on interface 0
Ethernet II, Src: AsustekC_d3:3e:b4 (1c:87:2c:d3:3e:b4), Dst: Micro-St_92:30:cb (4c:cc:6a:92:30:cb)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.249
Transmission Control Protocol, Src Port: 80, Dst Port: 53030, Seq: 731, Ack: 627, Len: 484
Hypertext Transfer Protocol
    HTTP/1.1 404 Not Found\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 404 Not Found\r\n]
            [HTTP/1.1 404 Not Found\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Response Version: HTTP/1.1
        Status Code: 404
        [Status Code Description: Not Found]
        Response Phrase: Not Found
    Date: Wed, 02 Oct 2019 00:12:47 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Content-Length: 209\r\n
        [Content length: 209]
    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: 0.021794000 seconds]
    [Prev request in frame: 47]
    [Prev response in frame: 49]
    [Request in frame: 51]
    [Request URI: http://gaia.cs.umass.edu/favicon.ico]
    File Data: 209 bytes
Line-based text data: text/html (7 lines)
    <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
    <html><head>\n
    <title>404 Not Found</title>\n
    </head><body>\n
    <h1>Not Found</h1>\n
    <p>The requested URL /favicon.ico was not found on this server.</p>\n
    </body></html>\n
```

8) Yes, I do see a “IF-MODIFIED-SINCE” in the HTTP GET line.
9) Yes, it displayed the file because it send a Header OK with the content of the data.
10) No, I do not see a “IF-MODIFIED-SINCE” in the HTTP GET line.
11) No, the packet displayed the 404-error code and the content of the data mention it could not find the request file in the server.

```
    55 2019-10-01 20:33:03.739921 192.168.1.249 128.119.245.12      HTTP     421 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
    56 2019-10-01 20:33:03.768154 128.119.245.12 192.168.1.249      TCP       64 80 → 53583 [ACK] Seq=1 Ack=368 Win=30336 Len=0
    57 2019-10-01 20:33:03.769059 128.119.245.12 192.168.1.249      TCP     1514 80 → 53583 [ACK] Seq=1 Ack=368 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
    58 2019-10-01 20:33:03.769059 128.119.245.12 192.168.1.249      TCP     1514 80 → 53583 [ACK] Seq=1461 Ack=368 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
    59 2019-10-01 20:33:03.769060 128.119.245.12 192.168.1.249      TCP     1514 80 → 53583 [ACK] Seq=2921 Ack=368 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
    60 2019-10-01 20:33:03.769060 128.119.245.12 192.168.1.249      HTTP     535 HTTP/1.1 200 OK  (text/html)
    61 2019-10-01 20:33:03.769079 192.168.1.249 128.119.245.12      TCP       54 53583 → 80 [ACK] Seq=368 Ack=4862 Win=262656 Len=0
```

Christopher Desir
Cd2902@nyu.edu
Week 4: Wireshark Lab: HTTP

```
No.     Time                           Source                Destination           Protocol Length Info
     60 2019-10-01 20:33:03.769060     128.119.245.12        192.168.1.249         HTTP     535    HTTP/1.1 200 OK  (text/html)
Frame 60: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface 0
Ethernet II, Src: AsustekC_d3:3e:b4 (1c:87:2c:d3:3e:b4), Dst: Micro-St_92:30:cb (4c:cc:6a:92:30:cb)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.249
Transmission Control Protocol, Src Port: 80, Dst Port: 53583, Seq: 4381, Ack: 368, Len: 481
    Source Port: 80
    Destination Port: 53583
    [Stream index: 5]
    [TCP Segment Len: 481]
    Sequence number: 4381    (relative sequence number)
    [Next sequence number: 4862    (relative sequence number)]
    Acknowledgment number: 368    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window size value: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
    Checksum: 0xfcbc [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
    [Timestamps]
    TCP payload (481 bytes)
    TCP segment data (481 bytes)
[4 Reassembled TCP Segments (4861 bytes): #57(1460), #58(1460), #59(1460), #60(481)]
Hypertext Transfer Protocol
Line-based text data: text/html (98 lines)
    <html><head> \n
    <title>Historical Documents:THE BILL OF RIGHTS</title></head>\n
    \n
    \n
    <body bgcolor="#ffffff" link="#330000" vlink="#666633">\n
    <p><br>\n
    </p>\n
    <p></p><center><b>THE BILL OF RIGHTS</b><br>\n
```

12) My Browser only send one HTTP Get Request.
13) Packet number 60 contains the status code and phrase associated with the response to the HTTP GET request,
14) The status code and phrase in the response is 200 OK.
15) There are 4 data containing TCP segments which contains a total of 4,606 bytes

No.	Time	Source	Destination	Protocol	Length	Info
15	2019-10-01 22:58:29.628195	192.168.1.249	128.119.245.12	HTTP	421	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
17	2019-10-01 22:58:29.656081	128.119.245.12	192.168.1.249	HTTP	1127	HTTP/1.1 200 OK (text/html)
18	2019-10-01 22:58:29.672175	192.168.1.249	128.119.245.12	HTTP	389	GET /pearson.png HTTP/1.1
22	2019-10-01 22:58:29.695022	128.119.245.12	192.168.1.249	HTTP	745	HTTP/1.1 200 OK (PNG)
30	2019-10-01 22:58:29.755908	192.168.1.249	128.119.245.12	HTTP	403	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
114	2019-10-01 22:58:29.856401	128.119.245.12	192.168.1.249	HTTP	632	HTTP/1.1 200 OK (JPEG JFIF image)

16) 3 GET request and the IP address is 128.119.245.12
17) The browser downloaded the images serial because image file is being sent one request at of time.

Christopher Desir
Cd2902@nyu.edu
Week 4: Wireshark Lab: HTTP

```
No.     Time                           Source                Destination           Protocol Length Info
     42 2019-10-01 22:47:56.317478     128.119.245.12        192.168.1.249         HTTP     771    HTTP/1.1 401 Unauthorized  (text
Frame 42: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface 0
Ethernet II, Src: AsustekC_d3:3e:b4 (1c:87:2c:d3:3e:b4), Dst: Micro-St_92:30:cb (4c:cc:6a:92:30:cb)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.249
Transmission Control Protocol, Src Port: 80, Dst Port: 58882, Seq: 1, Ack: 384, Len: 717
    Source Port: 80
    Destination Port: 58882
    [Stream index: 15]
    [TCP Segment Len: 717]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 718    (relative sequence number)]
    Acknowledgment number: 384    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window size value: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
    Checksum: 0xb58f [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
    [Timestamps]
        [Time since first frame in this TCP stream: 0.046166000 seconds]
        [Time since previous frame in this TCP stream: 0.001179000 seconds]
    TCP payload (717 bytes)
Hypertext Transfer Protocol
    HTTP/1.1 401 Unauthorized\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
            [HTTP/1.1 401 Unauthorized\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Response Version: HTTP/1.1
        Status Code: 401
        [Status Code Description: Unauthorized]
        Response Phrase: Unauthorized
    Date: Wed, 02 Oct 2019 02:47:54 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    WWW-Authenticate: Basic realm="wireshark-students only"\r\n
    Content-Length: 381\r\n
        [Content length: 381]
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.023934000 seconds]
    [Request in frame: 40]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
    File Data: 381 bytes
Line-based text data: text/html (12 lines)
    <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
    <html><head>\n
    <title>401 Unauthorized</title>\n
    </head><body>\n
    <h1>Unauthorized</h1>\n
    <p>This server could not verify that you\n
    are authorized to access the document\n
    requested.  Either you supplied the wrong\n
    credentials (e.g., bad password), or your\n
    browser doesn't understand how to supply\n
    the credentials required.</p>\n
    </body></html>\n
```

Christopher Desir
Cd2902@nyu.edu
Week 4: Wireshark Lab: HTTP

```
No.     Time                           Source                Destination           Protocol Length Info
    458 2019-10-01 22:48:34.340577     192.168.1.249         128.119.245.12        HTTP     496    GET /wireshark-labs/protected_p
HTTP-wireshark-file5.html HTTP/1.1
Frame 458: 496 bytes on wire (3968 bits), 496 bytes captured (3968 bits) on interface 0
Ethernet II, Src: Micro-St_92:30:cb (4c:cc:6a:92:30:cb), Dst: AsustekC_d3:3e:b4 (1c:87:2c:d3:3e:b4)
Internet Protocol Version 4, Src: 192.168.1.249, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 58898, Dst Port: 80, Seq: 1, Ack: 1, Len: 442
    Source Port: 58898
    Destination Port: 80
    [Stream index: 53]
    [TCP Segment Len: 442]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 443    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window size value: 1026
    [Calculated window size: 262656]
    [Window size scaling factor: 256]
    Checksum: 0x12a2 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
    [Timestamps]
        [Time since first frame in this TCP stream: 0.022730000 seconds]
        [Time since previous frame in this TCP stream: 0.000107000 seconds]
    TCP payload (442 bytes)
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]
            [GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        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 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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
        Credentials: wireshark-students:network
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
    [HTTP request 1/2]
    [Response in frame: 460]
    [Next request in frame: 472]
```

18) The server response is 401 unauthorized in response to the HTTP GET message from my browser.

19) The field That is shown is the Authorization and credentials within the HTTP GET Message.