Lab 1 Report: Examining HTTP Protocol with Wireshark

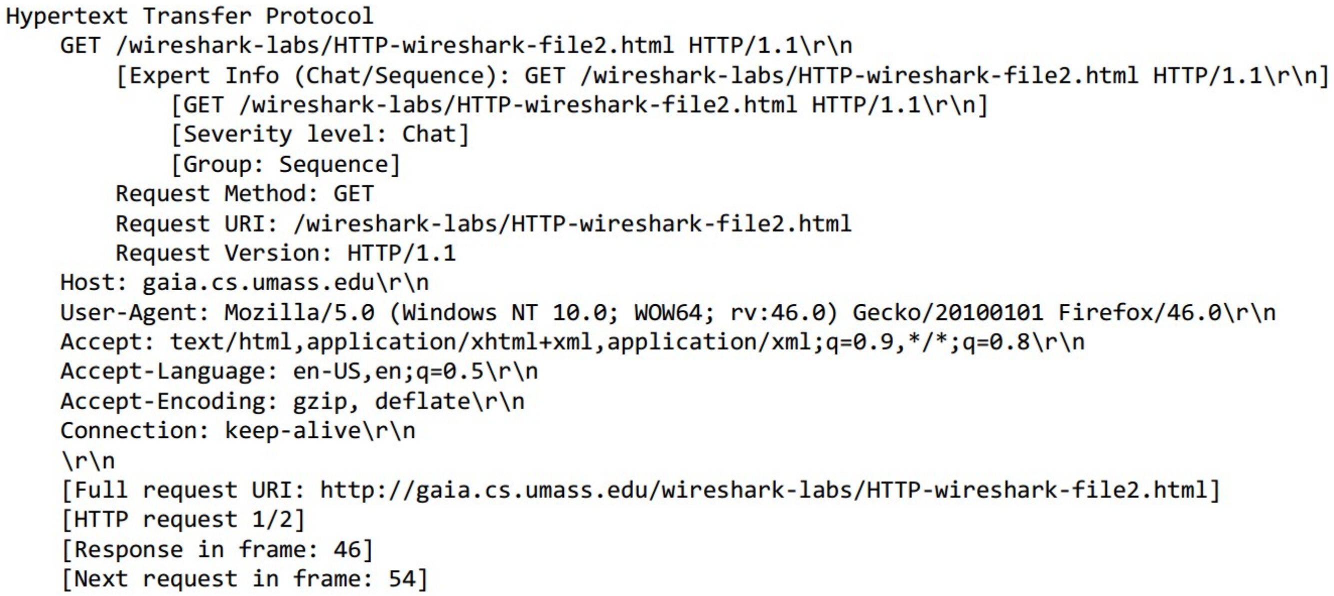
Name: Christopher Murray   Student Number: 3108107
Date: January 20th, 2017

Lab overview:
The motivation for this lab was to get a better understanding of HTTP (Hyper Text Transfer Protocol). This was achieved by examining HTTP request information using Wireshark.

Lab question answers:
Answers to question 6 were already included in the report template

Q 8.1 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 8.1 Referring to Figure 1, there was no “IF-MODIFIED-SINCE” line in the initial HTTP GET request.

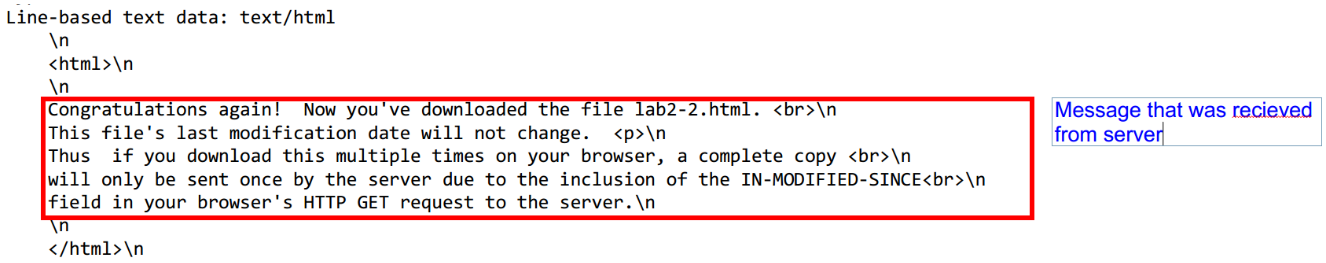


```
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
            [GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        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 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0\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
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/2]
    [Response in frame: 46]
    [Next request in frame: 54]
```

Figure 1: Initial HTTP GET request

Q 8.2 Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

A 8.2 Examining the response packet, there is a section containing Line-Based text data which contains the HTML stored at that address. This is shown in Figure 2.



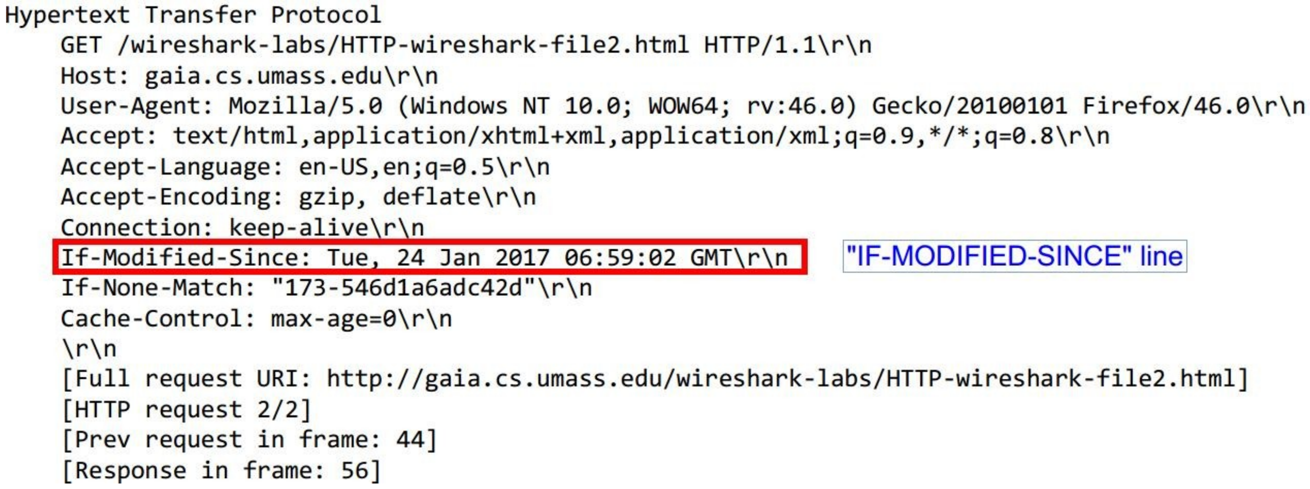
```
Line-based text data: text/html
    \n
    <html>\n
    \n
    Congratulations again!  Now you've downloaded the file lab2-2.html. <br>\n
    This file's last modification date will not change.  <p>\n
    Thus  if you download this multiple times on your browser, a complete copy <br>\n
    will only 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
```

Message that was recieved from server

Figure 2: HTML embedded in first HTTP response received

Q 8.3 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 8.3 Referring to Figure 3, the contents of the second HTTP GET request contain an “IF-MODIFIED-SINCE” line which is followed by the value of Tue, 24 Jan 2017 06:69:02 GMT



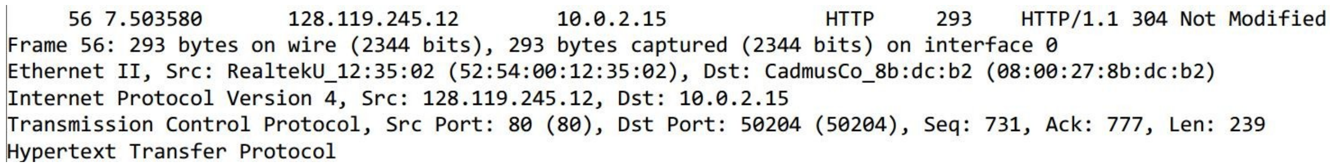
```
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    If-Modified-Since: Tue, 24 Jan 2017 06:59:02 GMT\r\n
    If-None-Match: "173-546d1a6adc42d"\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 2/2]
    [Prev request in frame: 44]
    [Response in frame: 56]
```

"IF-MODIFIED-SINCE" line

Figure 3: Contents of the second HTTP GET request showing the "IF-MODIFIED-SINCE" line.

Q 8.4 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 8.4 The HTTP status code returned from the second HTTP GET request was “304 Not Modified”. This means that the file at that point has not changed since the previous request so the server doesn't return any file. This can be seen in Figure 4 where there is no information embedded beneath the HTTP.



```
     56 7.503580       128.119.245.12       10.0.2.15            HTTP      293     HTTP/1.1 304 Not Modified
Frame 56: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface 0
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: CadmusCo_8b:dc:b2 (08:00:27:8b:dc:b2)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 50204 (50204), Seq: 731, Ack: 777, Len: 239
Hypertext Transfer Protocol
```

Figure 4: Second HTTP response with status code 304 Not Modified