# CS 3873: Net-Centric Computing
# Lab 2: Examining HTTP with Wireshark

Student Name: ____Adrian Freeman_____ Student Number: __3661616__

**[Mandatory]** Declaration: “I warrant that this is my own work.”

Signed by _Adrian Freeman___

[Optional] “I hereby give my permission for this work to be used (with my name and identifying information removed) for UNB Faculty of Computer Science program accreditation purposes.”

Signed by _Adrian Freeman__

# Report for Lab Exercise 2:
# Examining HTTP with Wireshark

**LAB ACTIVITIES:**

In this lab, we used Wireshark to examine the details of the hypertext transfer protocol (HTTP).

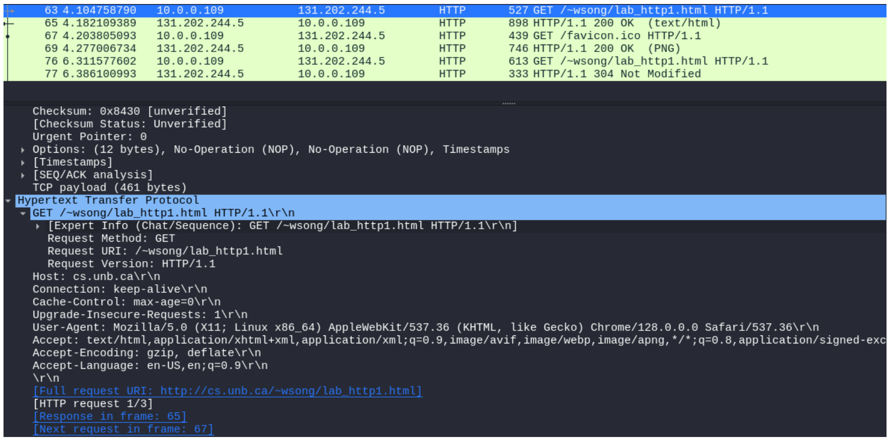
**ANSWERS TO LAB QUESTIONS:**

Remember to include annotated screenshot to justify your answer.

3. Examine your trace captured above and answer the following questions:

a. Inspect the contents of the first HTTP GET request **for the Webpage "lab_http1.html"** from your browser to the server. Do you see an "If-Modified-Since" line in the HTTP GET?

As shown in the screenshot below, The first HTTP GET message did not contain an "If-Modified-Since" line.

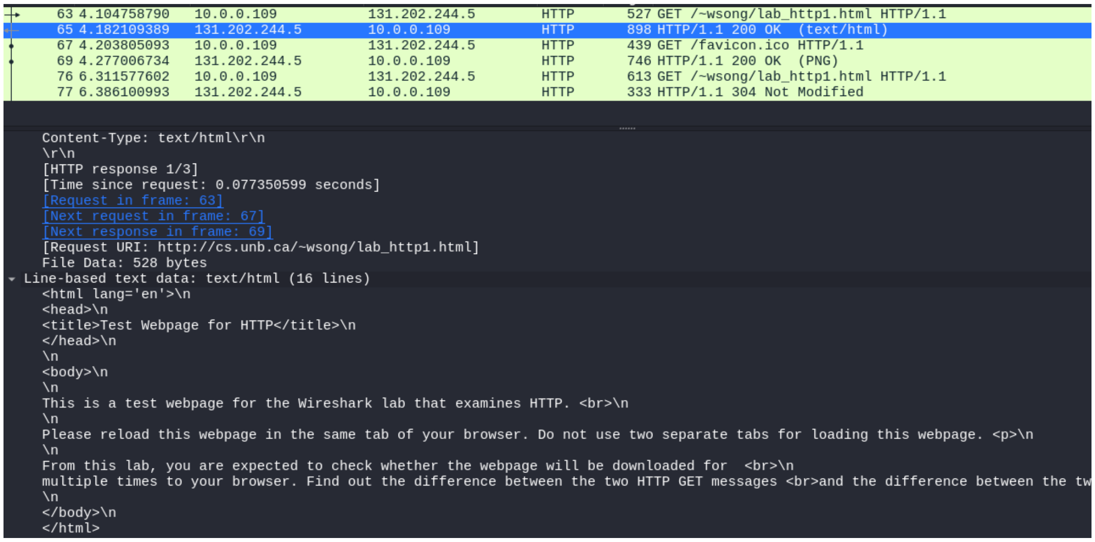


```
63 4.104758790   10.0.0.109      131.202.244.5   HTTP   527 GET /~wsong/lab_http1.html HTTP/1.1
65 4.182109389   131.202.244.5   10.0.0.109      HTTP   898 HTTP/1.1 200 OK  (text/html)
67 4.203805093   10.0.0.109      131.202.244.5   HTTP   439 GET /favicon.ico HTTP/1.1
69 4.277006734   131.202.244.5   10.0.0.109      HTTP   746 HTTP/1.1 200 OK  (PNG)
76 6.311577602   10.0.0.109      131.202.244.5   HTTP   613 GET /~wsong/lab_http1.html HTTP/1.1
77 6.386100993   131.202.244.5   10.0.0.109      HTTP   333 HTTP/1.1 304 Not Modified

    Checksum: 0x8430 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▸ [Timestamps]
  ▸ [SEQ/ACK analysis]
    TCP payload (461 bytes)
▾ Hypertext Transfer Protocol
  ▾ GET /~wsong/lab_http1.html HTTP/1.1\r\n
    ▸ [Expert Info (Chat/Sequence): GET /~wsong/lab_http1.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /~wsong/lab_http1.html
      Request Version: HTTP/1.1
    Host: cs.unb.ca\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/128.0.0.0 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-exc
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://cs.unb.ca/~wsong/lab_http1.html]
    [HTTP request 1/3]
    [Response in frame: 65]
    [Next request in frame: 67]
```

b. Inspect the contents of the server response to the first HTTP GET request. Did the server explicitly return the contents of the file? How can you tell?

The server did explicitly return the contents of the file, as shown in the screenshot below. The 200 OK message contains the raw text data from the webpage's html.



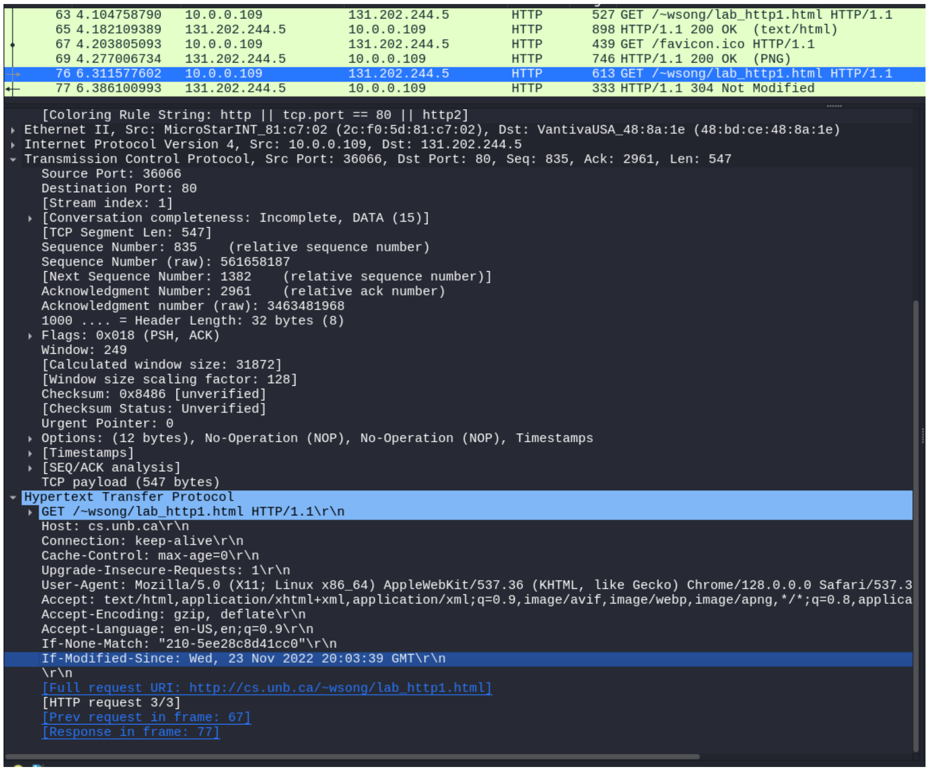
```
63 4.104758790   10.0.0.109      131.202.244.5   HTTP   527 GET /~wsong/lab_http1.html HTTP/1.1
65 4.182109389   131.202.244.5   10.0.0.109      HTTP   898 HTTP/1.1 200 OK  (text/html)
67 4.203805093   10.0.0.109      131.202.244.5   HTTP   439 GET /favicon.ico HTTP/1.1
69 4.277006734   131.202.244.5   10.0.0.109      HTTP   746 HTTP/1.1 200 OK  (PNG)
76 6.311577602   10.0.0.109      131.202.244.5   HTTP   613 GET /~wsong/lab_http1.html HTTP/1.1
77 6.386100993   131.202.244.5   10.0.0.109      HTTP   333 HTTP/1.1 304 Not Modified

    Content-Type: text/html\r\n
    \r\n
    [HTTP response 1/3]
    [Time since request: 0.077350599 seconds]
    [Request in frame: 63]
    [Next request in frame: 67]
    [Next response in frame: 69]
    [Request URI: http://cs.unb.ca/~wsong/lab_http1.html]
    File Data: 528 bytes
▾ Line-based text data: text/html (16 lines)
    <html lang='en'>\n
    <head>\n
    <title>Test Webpage for HTTP</title>\n
    </head>\n
    \n
    <body>\n
    \n
    This is a test webpage for the Wireshark lab that examines HTTP. <br>\n
    \n
    Please reload this webpage in the same tab of your browser. Do not use two separate tabs for loading this webpage. <p>\n
    \n
    From this lab, you are expected to check whether the webpage will be downloaded for  <br>\n
    multiple times to your browser. Find out the difference between the two HTTP GET messages <br>and the difference between the tw
    \n
    </body>\n
    </html>
```

c. Now inspect the contents of the next HTTP GET request for the Webpage “lab_http1.html” 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 within that line, there is a time, representing the last time the client accessed this data, the most recent cached time.

After the header, there are other lines, including the request URI, the # of HTTP requests in the current capture, a reference to the previous GET request, and a reference to the response request for this GET.

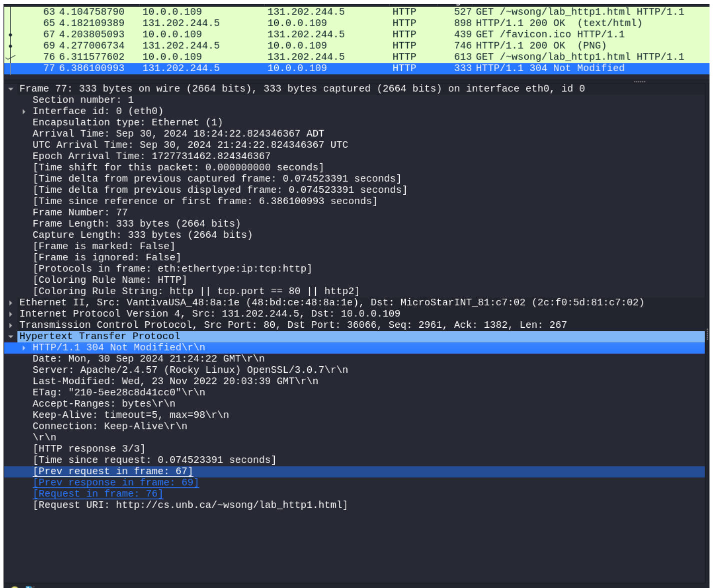


```
   63 4.104758790   10.0.0.109          131.202.244.5       HTTP      527 GET /~wsong/lab_http1.html HTTP/1.1
   65 4.182109389   131.202.244.5       10.0.0.109          HTTP      898 HTTP/1.1 200 OK  (text/html)
   67 4.203805093   10.0.0.109          131.202.244.5       HTTP      439 GET /favicon.ico HTTP/1.1
   69 4.277006734   131.202.244.5       10.0.0.109          HTTP      746 HTTP/1.1 200 OK  (PNG)
   76 6.311577602   10.0.0.109          131.202.244.5       HTTP      613 GET /~wsong/lab_http1.html HTTP/1.1
   77 6.386100993   131.202.244.5       10.0.0.109          HTTP      333 HTTP/1.1 304 Not Modified

    [Coloring Rule String: http || tcp.port == 80 || http2]
 Ethernet II, Src: MicroStarINT_81:c7:02 (2c:f0:5d:81:c7:02), Dst: VantivaUSA_48:8a:1e (48:bd:ce:48:8a:1e)
 Internet Protocol Version 4, Src: 10.0.0.109, Dst: 131.202.244.5
 Transmission Control Protocol, Src Port: 36066, Dst Port: 80, Seq: 835, Ack: 2961, Len: 547
    Source Port: 36066
    Destination Port: 80
    [Stream index: 1]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 547]
    Sequence Number: 835    (relative sequence number)
    Sequence Number (raw): 561658187
    [Next Sequence Number: 1382    (relative sequence number)]
    Acknowledgment Number: 2961    (relative ack number)
    Acknowledgment number (raw): 3463481968
    1000 .... = Header Length: 32 bytes (8)
    Flags: 0x018 (PSH, ACK)
    Window: 249
    [Calculated window size: 31872]
    [Window size scaling factor: 128]
    Checksum: 0x8486 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (547 bytes)
 Hypertext Transfer Protocol
    GET /~wsong/lab_http1.html HTTP/1.1\r\n
    Host: cs.unb.ca\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/128.0.0.0 Safari/537.3
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applica
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    If-None-Match: "210-5ee28c8d41cc0"\r\n
    If-Modified-Since: Wed, 23 Nov 2022 20:03:39 GMT\r\n
    \r\n
    [Full request URI: http://cs.unb.ca/~wsong/lab_http1.html]
    [HTTP request 3/3]
    [Prev request in frame: 67]
    [Response in frame: 77]
```

d. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET for “lab_http1.html”? Did the server explicitly return the contents of the file? Explain

The status code for the HTTP response is “304 Not Modified” which means that the “If-Modified-Since” returned that the page was not modified.  Because of this, the server did not need to return the contents of the file as the client already had an up-to-date version of it.



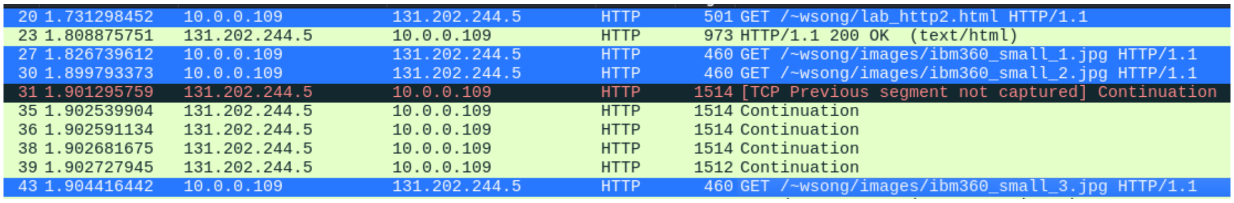
```
   63 4.104758790   10.0.0.109          131.202.244.5       HTTP      527 GET /~wsong/lab_http1.html HTTP/1.1
   65 4.182109389   131.202.244.5       10.0.0.109          HTTP      898 HTTP/1.1 200 OK  (text/html)
   67 4.203805093   10.0.0.109          131.202.244.5       HTTP      439 GET /favicon.ico HTTP/1.1
   69 4.277006734   131.202.244.5       10.0.0.109          HTTP      746 HTTP/1.1 200 OK  (PNG)
   76 6.311577602   10.0.0.109          131.202.244.5       HTTP      613 GET /~wsong/lab_http1.html HTTP/1.1
   77 6.386100993   131.202.244.5       10.0.0.109          HTTP      333 HTTP/1.1 304 Not Modified

 Frame 77: 333 bytes on wire (2664 bits), 333 bytes captured (2664 bits) on interface eth0, id 0
    Section number: 1
    Interface id: 0 (eth0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 30, 2024 18:24:22.824346367 ADT
    UTC Arrival Time: Sep 30, 2024 21:24:22.824346367 UTC
    Epoch Arrival Time: 1727731462.824346367
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.074523391 seconds]
    [Time delta from previous displayed frame: 0.074523391 seconds]
    [Time since reference or first frame: 6.386100993 seconds]
    Frame Number: 77
    Frame Length: 333 bytes (2664 bits)
    Capture Length: 333 bytes (2664 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
 Ethernet II, Src: VantivaUSA_48:8a:1e (48:bd:ce:48:8a:1e), Dst: MicroStarINT_81:c7:02 (2c:f0:5d:81:c7:02)
 Internet Protocol Version 4, Src: 131.202.244.5, Dst: 10.0.0.109
 Transmission Control Protocol, Src Port: 80, Dst Port: 36066, Seq: 2961, Ack: 1382, Len: 267
 Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
    Date: Mon, 30 Sep 2024 21:24:22 GMT\r\n
    Server: Apache/2.4.57 (Rocky Linux) OpenSSL/3.0.7\r\n
    Last-Modified: Wed, 23 Nov 2022 20:03:39 GMT\r\n
    ETag: "210-5ee28c8d41cc0"\r\n
    Accept-Ranges: bytes\r\n
    Keep-Alive: timeout=5, max=98\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [HTTP response 3/3]
    [Time since request: 0.074523391 seconds]
    [Prev request in frame: 67]
    [Prev response in frame: 69]
    [Request in frame: 76]
    [Request URI: http://cs.unb.ca/~wsong/lab_http1.html]
```

5. Examine your trace captured above and answer the following questions:

a. How many HTTP GET request messages did your browser send? Were these request messages sent toward the same or different Web servers? How can you tell?

The browser sent 4 HTTP GET requests, all towards the same web server, which I can tell because the destination IP address is the same for all 4.



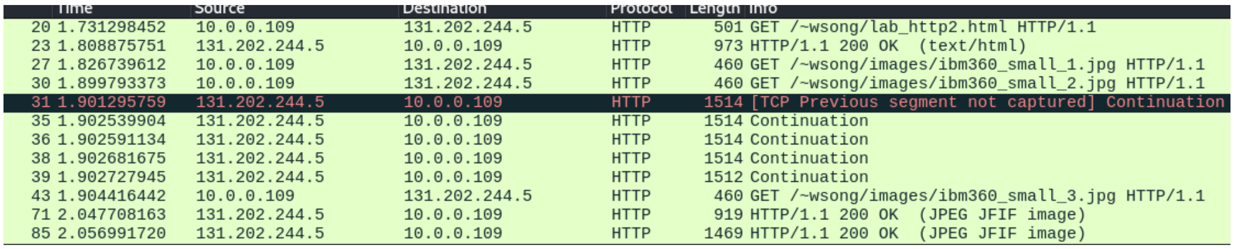
```
20 1.731298452    10.0.0.109       131.202.244.5    HTTP     501 GET /~wsong/lab_http2.html HTTP/1.1
23 1.808875751    131.202.244.5    10.0.0.109       HTTP     973 HTTP/1.1 200 OK  (text/html)
27 1.826739612    10.0.0.109       131.202.244.5    HTTP     460 GET /~wsong/images/ibm360_small_1.jpg HTTP/1.1
30 1.899793373    10.0.0.109       131.202.244.5    HTTP     460 GET /~wsong/images/ibm360_small_2.jpg HTTP/1.1
31 1.901295759    131.202.244.5    10.0.0.109       HTTP    1514 [TCP Previous segment not captured] Continuation
35 1.902539904    131.202.244.5    10.0.0.109       HTTP    1514 Continuation
36 1.902591134    131.202.244.5    10.0.0.109       HTTP    1514 Continuation
38 1.902681675    131.202.244.5    10.0.0.109       HTTP    1514 Continuation
39 1.902727945    131.202.244.5    10.0.0.109       HTTP    1512 Continuation
43 1.904416442    10.0.0.109       131.202.244.5    HTTP     460 GET /~wsong/images/ibm360_small_3.jpg HTTP/1.1
```

b. Was persistent or non-persistent HTTP used between your browser and the Web server? How can you tell?

Persistent HTTP was used, which I can tell by looking in the Http section of the GET message, where it says “Connection: keep-alive\r\n”

c. According to the order of the HTTP messages for the embedded images, do you find the browser waits for the response for an earlier request before it sends the HTTP GET request for another image?

The browser does not wait for the response for the GET message. Which can be seen as there are 2 HTTP get messages next to each other, before a response is received. (My response ended up being an error, unsure as of why.)



```
   Time           Source           Destination      Protocol Length Info
20 1.731298452    10.0.0.109       131.202.244.5    HTTP     501 GET /~wsong/lab_http2.html HTTP/1.1
23 1.808875751    131.202.244.5    10.0.0.109       HTTP     973 HTTP/1.1 200 OK  (text/html)
27 1.826739612    10.0.0.109       131.202.244.5    HTTP     460 GET /~wsong/images/ibm360_small_1.jpg HTTP/1.1
30 1.899793373    10.0.0.109       131.202.244.5    HTTP     460 GET /~wsong/images/ibm360_small_2.jpg HTTP/1.1
31 1.901295759    131.202.244.5    10.0.0.109       HTTP    1514 [TCP Previous segment not captured] Continuation
35 1.902539904    131.202.244.5    10.0.0.109       HTTP    1514 Continuation
36 1.902591134    131.202.244.5    10.0.0.109       HTTP    1514 Continuation
38 1.902681675    131.202.244.5    10.0.0.109       HTTP    1514 Continuation
39 1.902727945    131.202.244.5    10.0.0.109       HTTP    1512 Continuation
43 1.904416442    10.0.0.109       131.202.244.5    HTTP     460 GET /~wsong/images/ibm360_small_3.jpg HTTP/1.1
71 2.047708163    131.202.244.5    10.0.0.109       HTTP     919 HTTP/1.1 200 OK  (JPEG JFIF image)
85 2.056991720    131.202.244.5    10.0.0.109       HTTP    1469 HTTP/1.1 200 OK  (JPEG JFIF image)
```