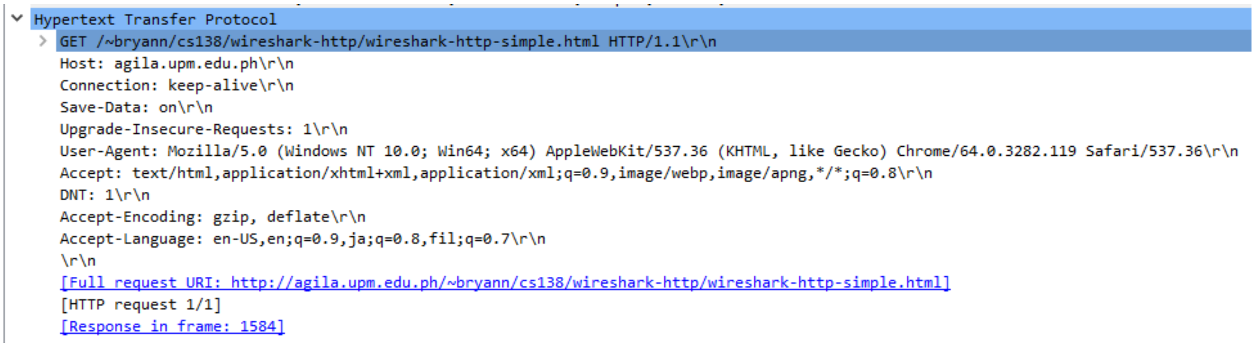
BAYANI, Femo Steven Felicisimo

2015-07104

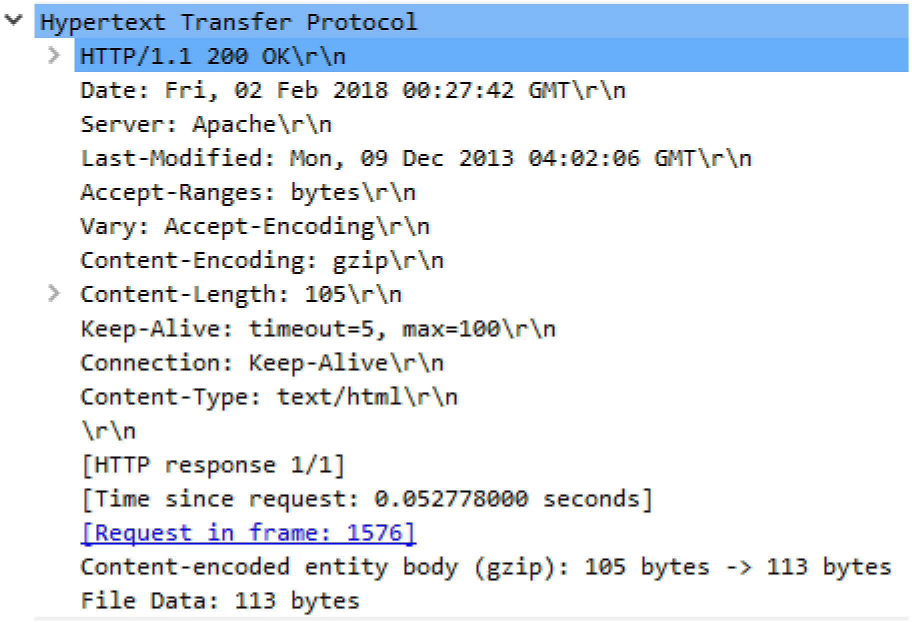
1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

My browser is running **HTTP version 1.1**.



```
Hypertext Transfer Protocol
  GET /~bryann/cs138/wireshark-http/wireshark-http-simple.html HTTP/1.1\r\n
  Host: agila.upm.edu.ph\r\n
  Connection: keep-alive\r\n
  Save-Data: on\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.119 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
  DNT: 1\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9,ja;q=0.8,fil;q=0.7\r\n
  \r\n
  [Full request URI: http://agila.upm.edu.ph/~bryann/cs138/wireshark-http/wireshark-http-simple.html]
  [HTTP request 1/1]
  [Response in frame: 1584]
```

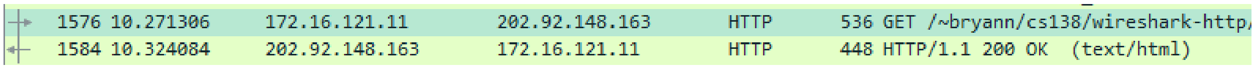
The server is running **HTTP version 1.1**.



```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Fri, 02 Feb 2018 00:27:42 GMT\r\n
  Server: Apache\r\n
  Last-Modified: Mon, 09 Dec 2013 04:02:06 GMT\r\n
  Accept-Ranges: bytes\r\n
  Vary: Accept-Encoding\r\n
  Content-Encoding: gzip\r\n
  Content-Length: 105\r\n
  Keep-Alive: timeout=5, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.052778000 seconds]
  [Request in frame: 1576]
  Content-encoded entity body (gzip): 105 bytes -> 113 bytes
  File Data: 113 bytes
```

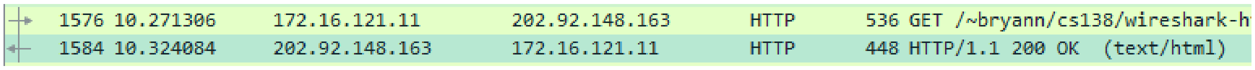
2. What is the IP address of your computer? Of the agila.upm.edu.ph?

The IP address of my computer is **172.16.121.11**.



```
1576 10.271306    172.16.121.11     202.92.148.163    HTTP    536 GET /~bryann/cs138/wireshark-http/
1584 10.324084    202.92.148.163    172.16.121.11     HTTP    448 HTTP/1.1 200 OK  (text/html)
```

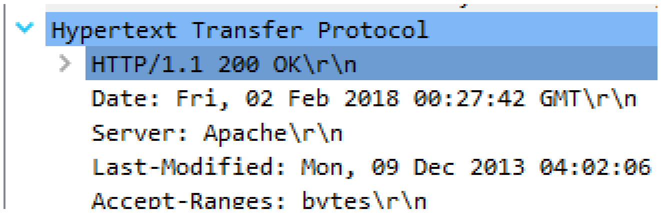
The IP address of agila.upm.edu.ph is **202.92.148.163**.



```
1576 10.271306    172.16.121.11     202.92.148.163    HTTP    536 GET /~bryann/cs138/wireshark-h
1584 10.324084    202.92.148.163    172.16.121.11     HTTP    448 HTTP/1.1 200 OK  (text/html)
```

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

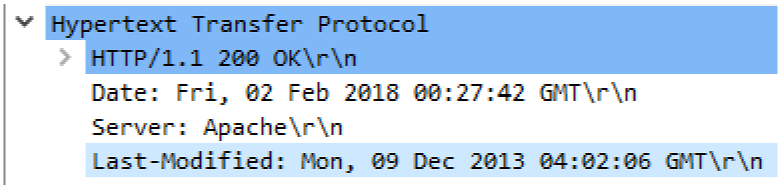
The status code returned from the server is **200**.



```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Fri, 02 Feb 2018 00:27:42 GMT\r\n
  Server: Apache\r\n
  Last-Modified: Mon, 09 Dec 2013 04:02:06
  Accept-Ranges: bytes\r\n
```

4. When was the HTML file that you are retrieving (in MNL time) last modified at the server?

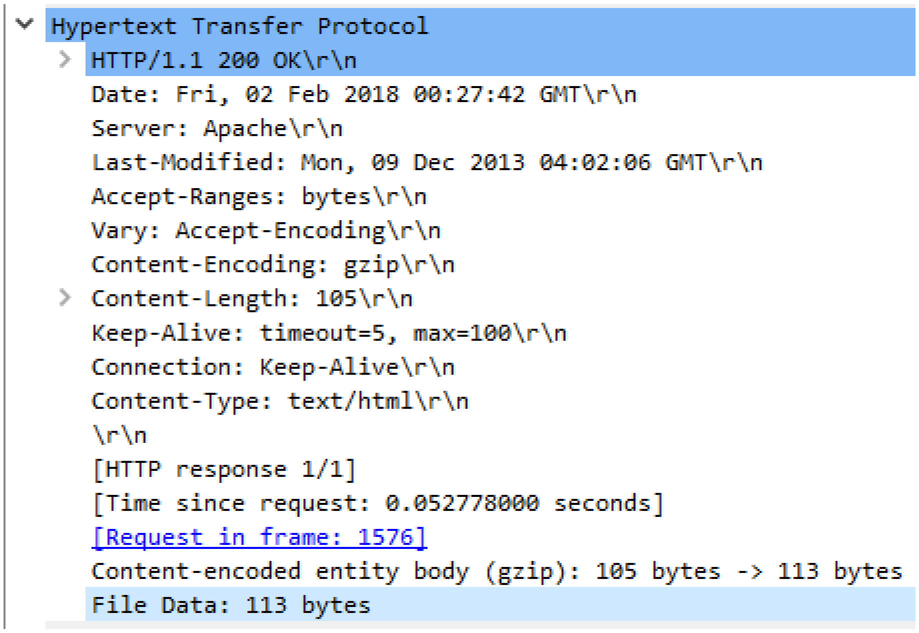
The HTML file was lasted modified (in MNL time) on **Mon, 09 Dec 2013, 12:02:06 GMT+8**.



```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Fri, 02 Feb 2018 00:27:42 GMT\r\n
  Server: Apache\r\n
  Last-Modified: Mon, 09 Dec 2013 04:02:06 GMT\r\n
```

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

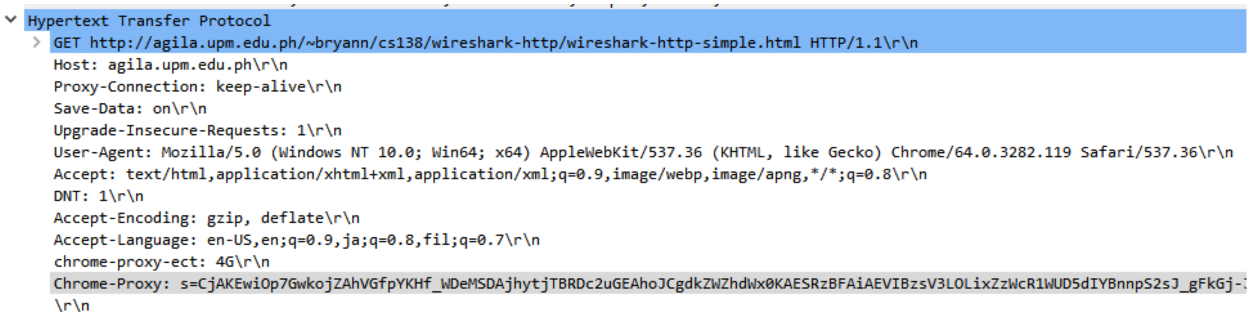
113 bytes



```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Fri, 02 Feb 2018 00:27:42 GMT\r\n
  Server: Apache\r\n
  Last-Modified: Mon, 09 Dec 2013 04:02:06 GMT\r\n
  Accept-Ranges: bytes\r\n
  Vary: Accept-Encoding\r\n
  Content-Encoding: gzip\r\n
  Content-Length: 105\r\n
  Keep-Alive: timeout=5, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.052778000 seconds]
  [Request in frame: 1576]
  Content-encoded entity body (gzip): 105 bytes -> 113 bytes
  File Data: 113 bytes
```

6. 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?

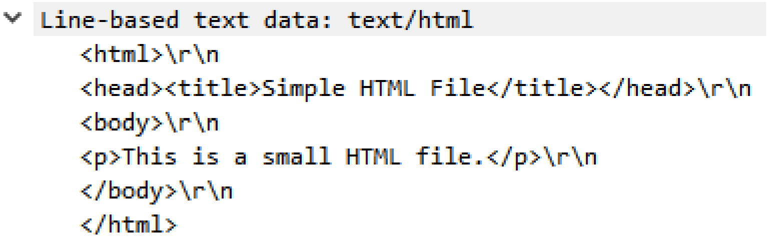
No.



```
Hypertext Transfer Protocol
  GET http://agila.upm.edu.ph/~bryann/cs138/wireshark-http/wireshark-http-simple.html HTTP/1.1\r\n
  Host: agila.upm.edu.ph\r\n
  Proxy-Connection: keep-alive\r\n
  Save-Data: on\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.119 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
  DNT: 1\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9,ja;q=0.8,fil;q=0.7\r\n
  chrome-proxy-ect: 4G\r\n
  Chrome-Proxy: s=CjAKEwiOp7GwkojZAhVGfpYKHf_WDeMSDAjhytjTBRDc2uGEAhoJCgdkZWZhdWx0KAESRzBFAiAEVIBzsV3LOLixZzWcR1WUD5dIYBnnpS2sJ_gFkGj-
  \r\n
```

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

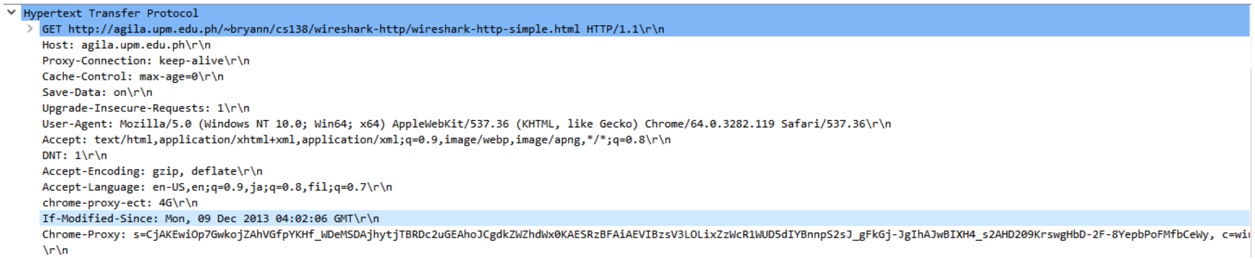
Yes, because the server response contains line-based text data.



```
Line-based text data: text/html
    <html>\r\n
    <head><title>Simple HTML File</title></head>\r\n
    <body>\r\n
    <p>This is a small HTML file.</p>\r\n
    </body>\r\n
    </html>
```

8. 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?

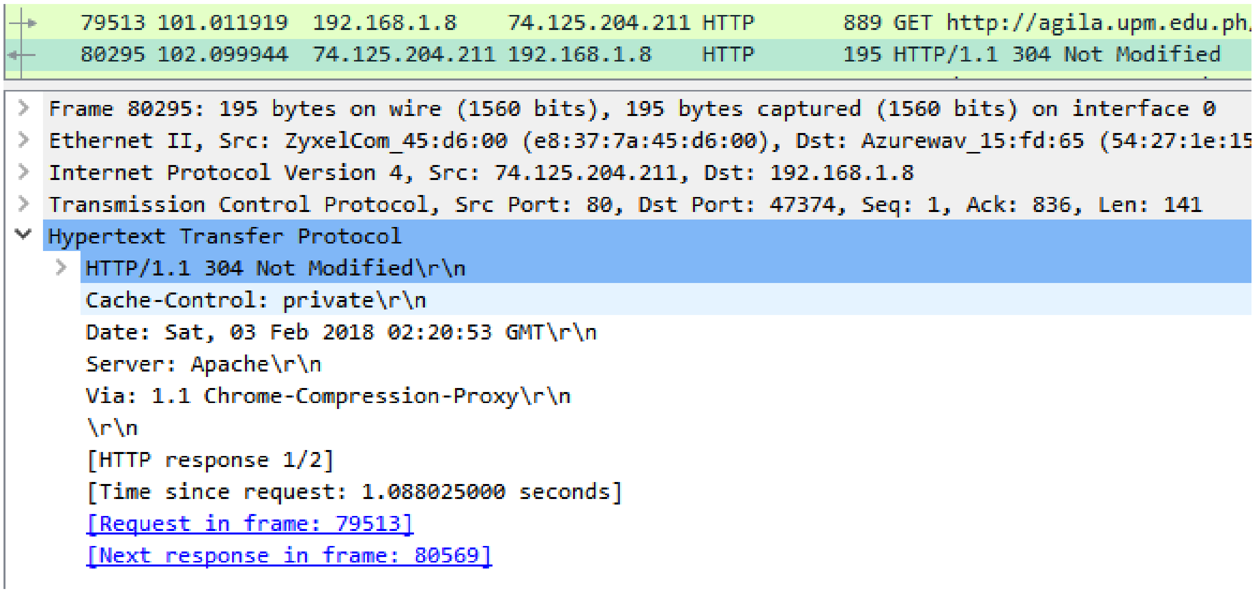
Yes. The information that follows the If-Modified-Since header is the **Chrome-Proxy** header.



```
Hypertext Transfer Protocol
  GET http://agila.upm.edu.ph/~bryann/cs138/wireshark-http/wireshark-http-simple.html HTTP/1.1\r\n
  Host: agila.upm.edu.ph\r\n
  Proxy-Connection: keep-alive\r\n
  Cache-Control: max-age=0\r\n
  Save-Data: on\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.119 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
  DNT: 1\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9,ja;q=0.8,fil;q=0.7\r\n
  chrome-proxy-ect: 4G\r\n
  If-Modified-Since: Mon, 09 Dec 2013 04:02:06 GMT\r\n
  Chrome-Proxy: s=CjAKEwiOp7GwkojZAhVGfpYKHf_WDeMSDAjhytjTBRDc2uGEAhoJCgdkZWZhdWx0KAESRzBFAiAEVIBzsV3LOLixZzWcR1WUD5dIYBnnpS2sJ_gFkGj-JgIhAJwBIXH4_s2AHD209KrswgHbD-2F-8YepbPoFMfbCeWy, c=wi
  \r\n
```

9. 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 server returned the HTTP status code **304 Not Modified**, and did not explicitly return the contents of the file, because a local file is already stored in the cache, and the original file on the server has not been modified by the data set by the HTTP GET request above, therefore, it did not explicitly send the file.

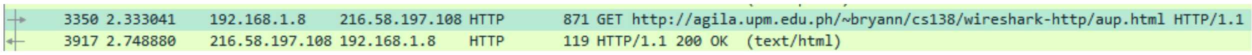


```
79513 101.011919  192.168.1.8     74.125.204.211 HTTP       889 GET http://agila.upm.edu.ph
80295 102.099944  74.125.204.211 192.168.1.8     HTTP       195 HTTP/1.1 304 Not Modified

> Frame 80295: 195 bytes on wire (1560 bits), 195 bytes captured (1560 bits) on interface 0
> Ethernet II, Src: ZyxelCom_45:d6:00 (e8:37:7a:45:d6:00), Dst: Azurewav_15:fd:65 (54:27:1e:15
> Internet Protocol Version 4, Src: 74.125.204.211, Dst: 192.168.1.8
> Transmission Control Protocol, Src Port: 80, Dst Port: 47374, Seq: 1, Ack: 836, Len: 141
v Hypertext Transfer Protocol
  > HTTP/1.1 304 Not Modified\r\n
    Cache-Control: private\r\n
    Date: Sat, 03 Feb 2018 02:20:53 GMT\r\n
    Server: Apache\r\n
    Via: 1.1 Chrome-Compression-Proxy\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 1.088025000 seconds]
    [Request in frame: 79513]
    [Next response in frame: 80569]
```

10. How many HTTP GET request messages were sent by your browser?

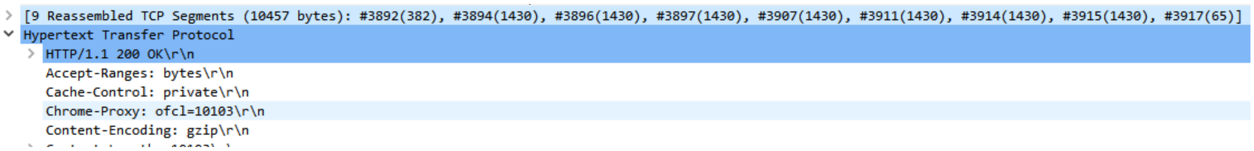
Only **1** HTTP GET request message was sent.



```
3350 2.333041    192.168.1.8     216.58.197.108 HTTP       871 GET http://agila.upm.edu.ph/~bryann/cs138/wireshark-http/aup.html HTTP/1.1
3917 2.748880    216.58.197.108 192.168.1.8     HTTP       119 HTTP/1.1 200 OK  (text/html)
```

11. How many data-containing TCP segments were needed to carry the single HTTP response?

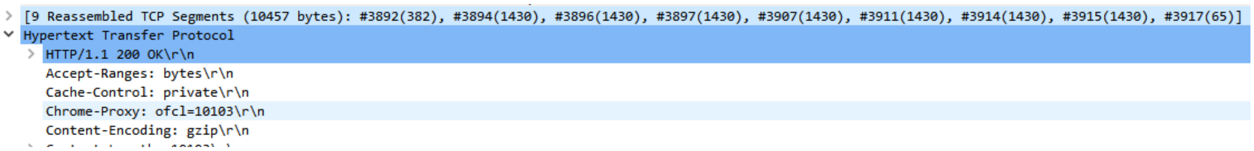
The number of data-containing TCP fragments needed was **9**.



```
> [9 Reassembled TCP Segments (10457 bytes): #3892(382), #3894(1430), #3896(1430), #3897(1430), #3907(1430), #3911(1430), #3914(1430), #3915(1430), #3917(65)]
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Accept-Ranges: bytes\r\n
    Cache-Control: private\r\n
    Chrome-Proxy: ofcl=10103\r\n
    Content-Encoding: gzip\r\n
```

12. How did you know that a particular response was fragmented into multiple parts?

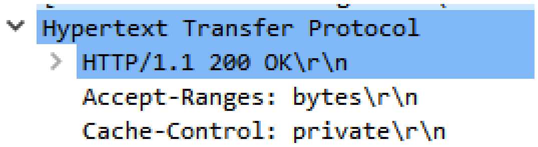
Wireshark's interface shows "Reassembled TCP Segments" that indicates that a response was fragmented into multiple parts. Like the screenshot above:



```
> [9 Reassembled TCP Segments (10457 bytes): #3892(382), #3894(1430), #3896(1430), #3897(1430), #3907(1430), #3911(1430), #3914(1430), #3915(1430), #3917(65)]
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Accept-Ranges: bytes\r\n
    Cache-Control: private\r\n
    Chrome-Proxy: ofcl=10103\r\n
    Content-Encoding: gzip\r\n
```

13. What is the status code and phrase associated with the response to the HTTP GET request?

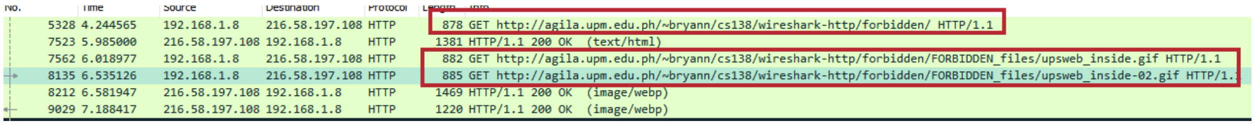
200 OK was returned.



```
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Accept-Ranges: bytes\r\n
    Cache-Control: private\r\n
```

14. How many HTTP GET request messages were sent by your browser to retrieve all the objects that were displayed by the browser?

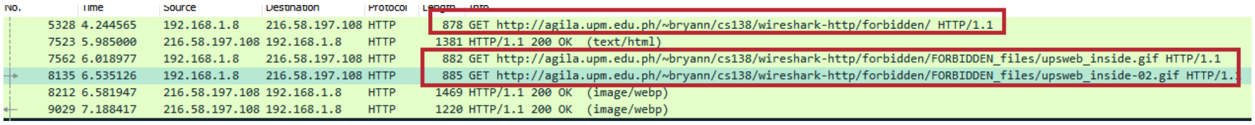
3 HTTP GET request messages were sent.



```
No.   Time      Source         Destination    Protocol Length Info
 5328 4.244565  192.168.1.8    216.58.197.108 HTTP      878 GET http://agila.upm.edu.ph/~bryann/cs138/wireshark-http/forbidden/ HTTP/1.1
 7523 5.985000  216.58.197.108 192.168.1.8    HTTP     1381 HTTP/1.1 200 OK  (text/html)
 7562 6.018977  192.168.1.8    216.58.197.108 HTTP      882 GET http://agila.upm.edu.ph/~bryann/cs138/wireshark-http/forbidden/FORBIDDEN_files/upsweb_inside.gif HTTP/1.1
 8135 6.535126  192.168.1.8    216.58.197.108 HTTP      885 GET http://agila.upm.edu.ph/~bryann/cs138/wireshark-http/forbidden/FORBIDDEN_files/upsweb_inside-02.gif HTTP/1.
 8212 6.581947  216.58.197.108 192.168.1.8    HTTP     1469 HTTP/1.1 200 OK  (image/webp)
 9029 7.188417  216.58.197.108 192.168.1.8    HTTP     1220 HTTP/1.1 200 OK  (image/webp)
```

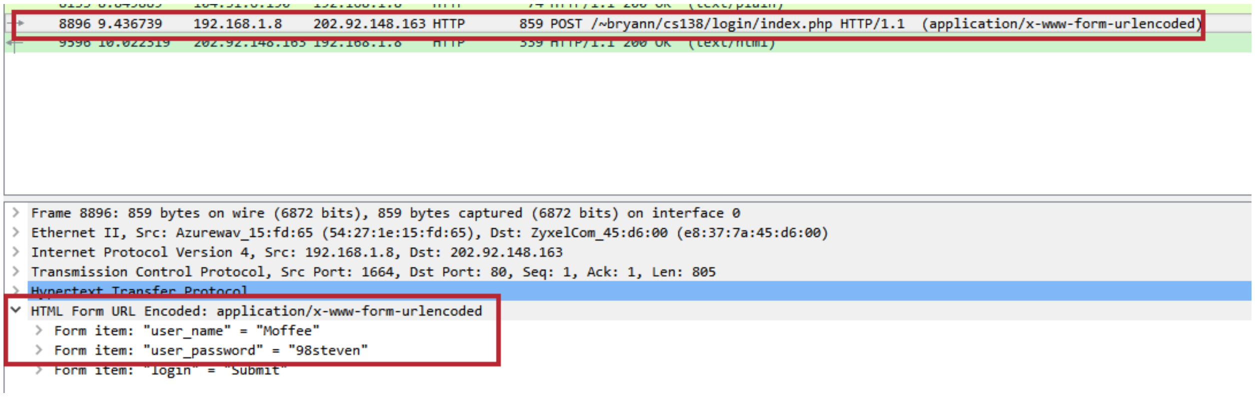
15. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

The two images were downloaded serially as the two requests were also sent serially, one after the other, and if they were running in parallel, they would have been returned in the same time.



```
No.   Time      Source         Destination    Protocol Length Info
 5328 4.244565  192.168.1.8    216.58.197.108 HTTP      878 GET http://agila.upm.edu.ph/~bryann/cs138/wireshark-http/forbidden/ HTTP/1.1
 7523 5.985000  216.58.197.108 192.168.1.8    HTTP     1381 HTTP/1.1 200 OK  (text/html)
 7562 6.018977  192.168.1.8    216.58.197.108 HTTP      882 GET http://agila.upm.edu.ph/~bryann/cs138/wireshark-http/forbidden/FORBIDDEN_files/upsweb_inside.gif HTTP/1.1
 8135 6.535126  192.168.1.8    216.58.197.108 HTTP      885 GET http://agila.upm.edu.ph/~bryann/cs138/wireshark-http/forbidden/FORBIDDEN_files/upsweb_inside-02.gif HTTP/1.
 8212 6.581947  216.58.197.108 192.168.1.8    HTTP     1469 HTTP/1.1 200 OK  (image/webp)
 9029 7.188417  216.58.197.108 192.168.1.8    HTTP     1220 HTTP/1.1 200 OK  (image/webp)
```

16. You should be able to capture the packet that contain the username and password that you have just entered in the login. Show the packet that contains the username and password.



```
8896 9.436739    192.168.1.8    202.92.148.163 HTTP    859 POST /~bryann/cs138/login/index.php HTTP/1.1  (application/x-www-form-urlencoded)
9396 10.022519   202.92.148.163 192.168.1.8    HTTP    339 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 8896: 859 bytes on wire (6872 bits), 859 bytes captured (6872 bits) on interface 0
> Ethernet II, Src: Azurewav_15:fd:65 (54:27:1e:15:fd:65), Dst: ZyxelCom_45:d6:00 (e8:37:7a:45:d6:00)
> Internet Protocol Version 4, Src: 192.168.1.8, Dst: 202.92.148.163
> Transmission Control Protocol, Src Port: 1664, Dst Port: 80, Seq: 1, Ack: 1, Len: 805
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
   > Form item: "user_name" = "Moffee"
   > Form item: "user_password" = "98steven"
   > Form item: "login" = "Submit"
```