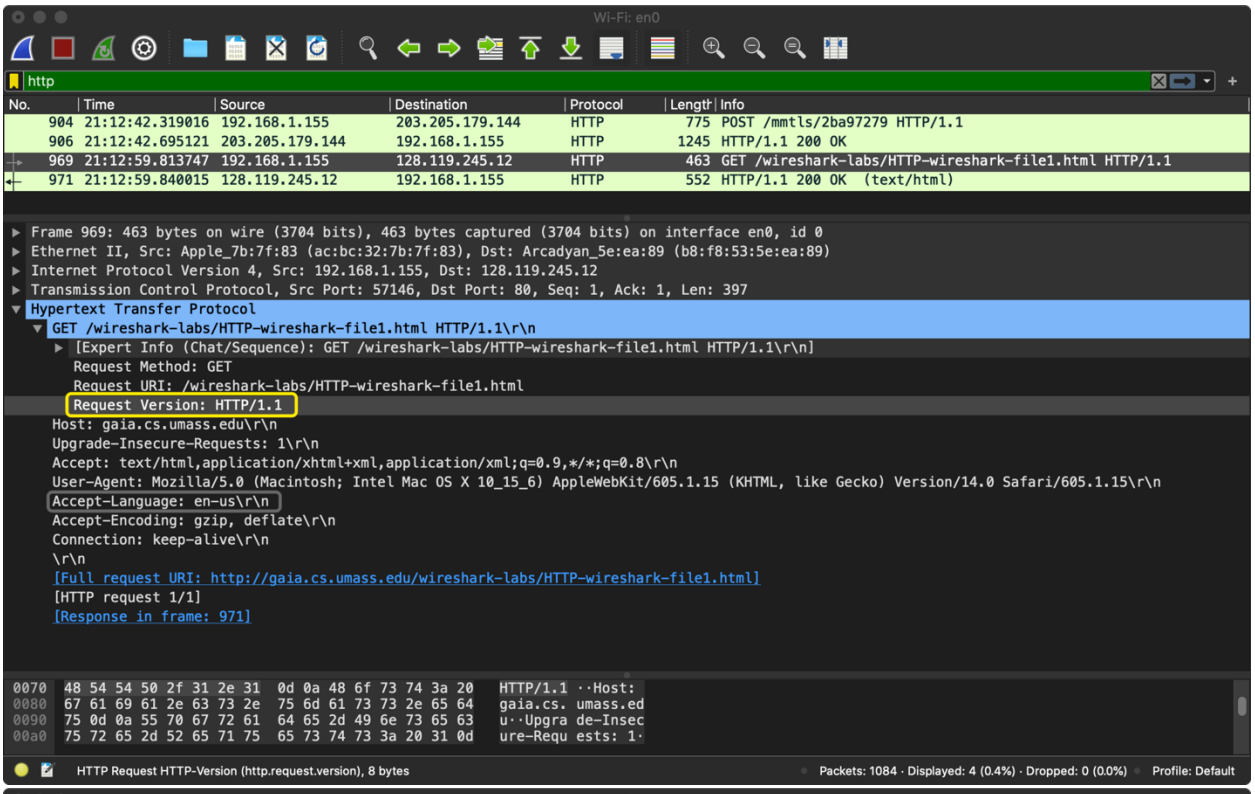
Wireshark Lab 1 -- Getting Started

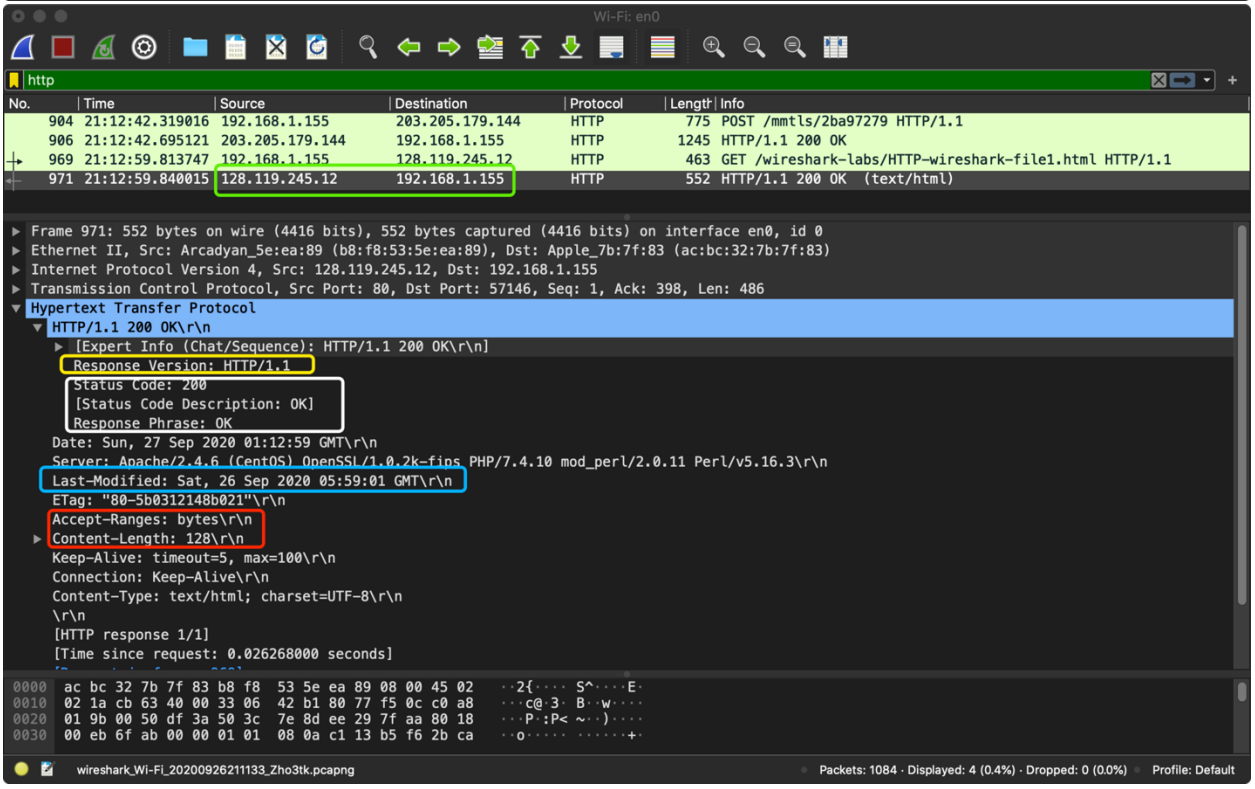
Jiaying Li
jl10919

Lab environment:

Answer: My PC uses macOS Catalina 10.15.6, shows the following setting with *ifconfig*:

The Basic HTTP GET/response interaction. Answer the following questions:





Q1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
Answer: As shown in the screenshots for GET and Response above, HTTP get and reply message below, highlighted with yellow, my browser is running HTTP 1.1, and server is running HTTP 1.1

Q2. What languages (if any) does your browser indicate that it can accept to the server?
Answer: As shown in the screenshot for GET above, HTTP get message below, highlighted with gray, my browser indicate that it can accept en-us (US English).

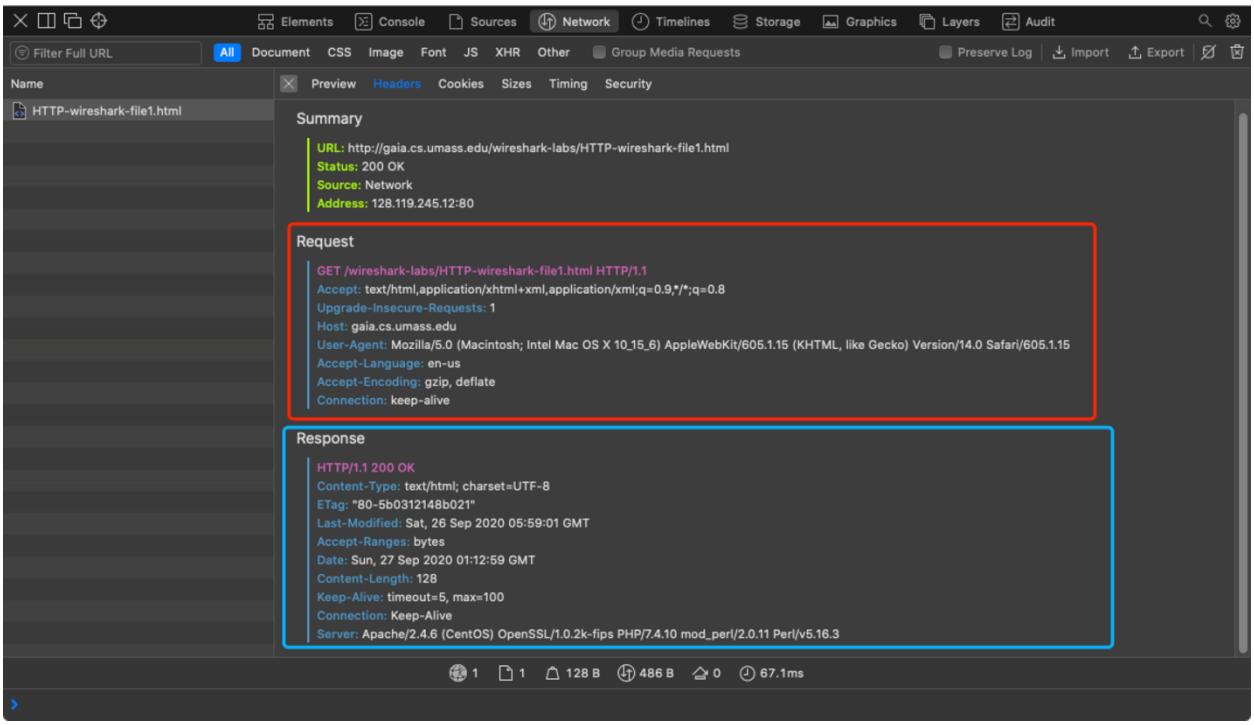
Q3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?
Answer: As shown in the screenshot for Response above, HTTP reply message below, highlighted with green, the IP address of my computer (shown as destination) is 192.168.1.155, the IP address of gaia.cs.umass.edu server (shown as Source) is 128.119.245.12.

Q4. What is the status code returned from the server to your browser?
Answer: As shown in the screenshot for Response above, HTTP reply message below, highlighted with purple(white in the screenshot), the status code returned from the server to my browser is 200, the phrase is OK.

Q5. When was the HTML file that you are retrieving last modified at the server?
Answer: As shown in the screenshot for Response above, HTTP reply message below, highlighted with blue, the HTML file that I am retrieving last modified at Sat, 26 Sep 2020 05:59:01 GMT at the server.

Q6. How many bytes of content are being returned to your browser?
Answer: As shown in the screenshot for Response above, HTTP reply message below, highlighted with red, the size of content is 128 bytes.

Q7. 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.
Answer: No. All the data that in the headers are in the packet content window. As shown in the screenshot below, the headers of request and response can be checked in the browser and the information of them are circled in red and blue. All the header information is contained in the packet content window.



HTTP GET message:

No. Time Source Destination Protocol Length Info
969 21:12:59.813747 192.168.1.155 128.119.245.12 HTTP 463 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

Frame 969: 463 bytes on wire (3704 bits), 463 bytes captured (3704 bits) on interface en0, id 0
Ethernet II, Src: Apple_7b:7f:83 (ac:bc:32:7b:7f:83), Dst: Arcadyan_5e:ea:89 (b8:f8:53:5e:ea:89)
Internet Protocol Version 4, Src: 192.168.1.155, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 57146, Dst Port: 80, Seq: 1, Ack: 1, Len: 397
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
Request Method: GET
Request URI: /wireshark-labs/HTTP-wireshark-file1.html
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
Upgrade-Insecure-Requests: 1\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Safari/605.1.15\r\n
Accept-Language: en-us\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-file1.html]
[HTTP request 1/1]
[Response in frame: 971]

HTTP REPLY message:

No. Time Source Destination Protocol Length Info
971 21:12:59.840015 128.119.245.12 192.168.1.155 HTTP 552 HTTP/1.1 200 OK (text/html)

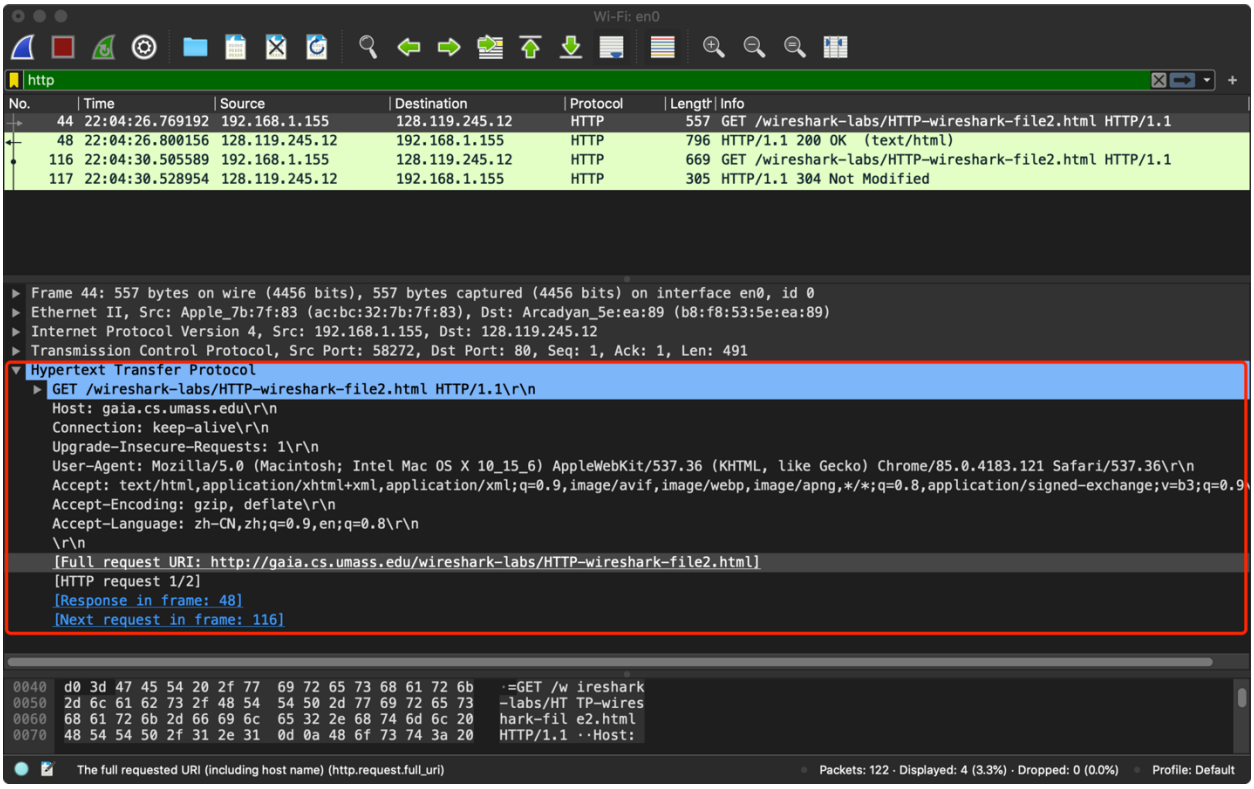
Frame 971: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface en0, id 0
Ethernet II, Src: Arcadyan_5e:ea:89 (b8:f8:53:5e:ea:89), Dst: Apple_7b:7f:83 (ac:bc:32:7b:7f:83)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.155
Transmission Control Protocol, Src Port: 80, Dst Port: 57146, Seq: 1, Ack: 398, Len: 486
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: Sun, 27 Sep 2020 01:12:59 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.10 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Sat, 26 Sep 2020 05:59:01 GMT\r\n
ETag: "80-5b0312148b021"\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: 0.026268000 seconds]
[Request in frame: 969]
[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)

The HTTP CONDITIONAL GET/response interaction. Answer the following questions:

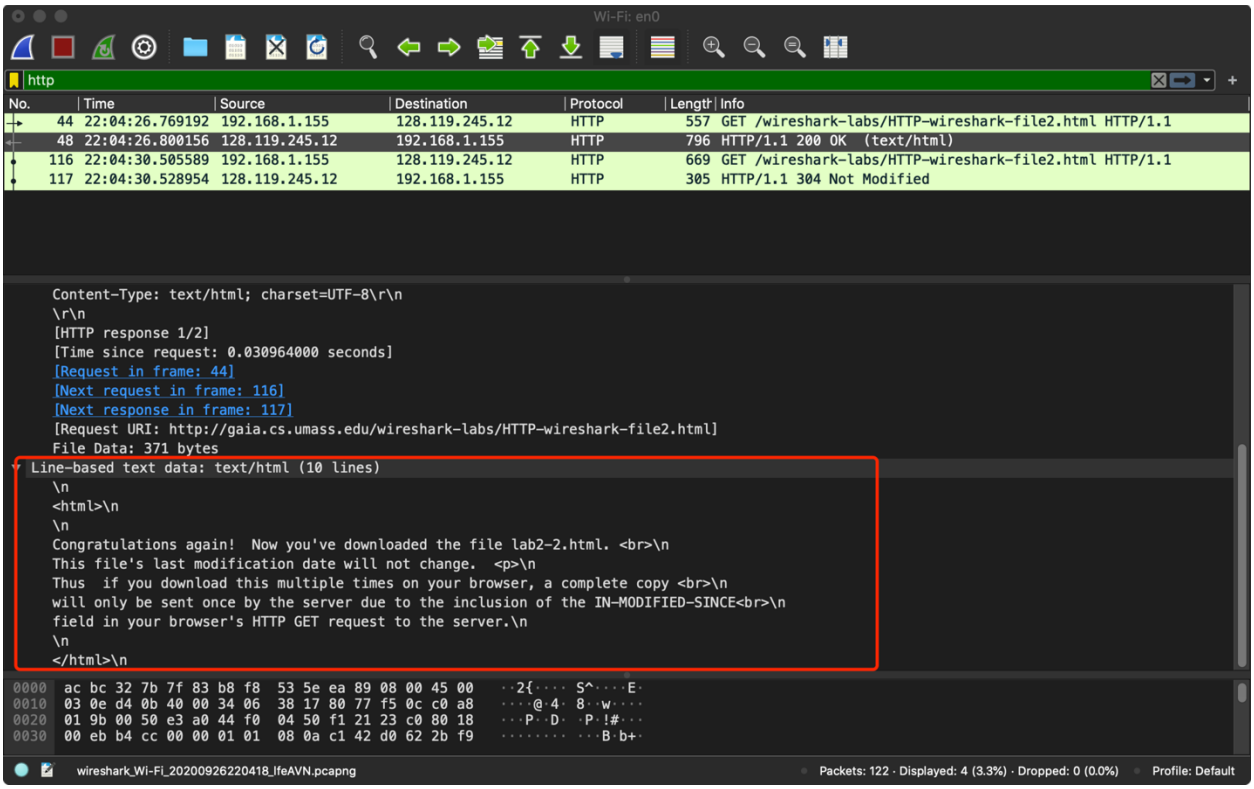
Q8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?

Answer: As shown in the screenshot below, there is no "IF-MODIFIED-SINCE" line in the first HTTP GET.



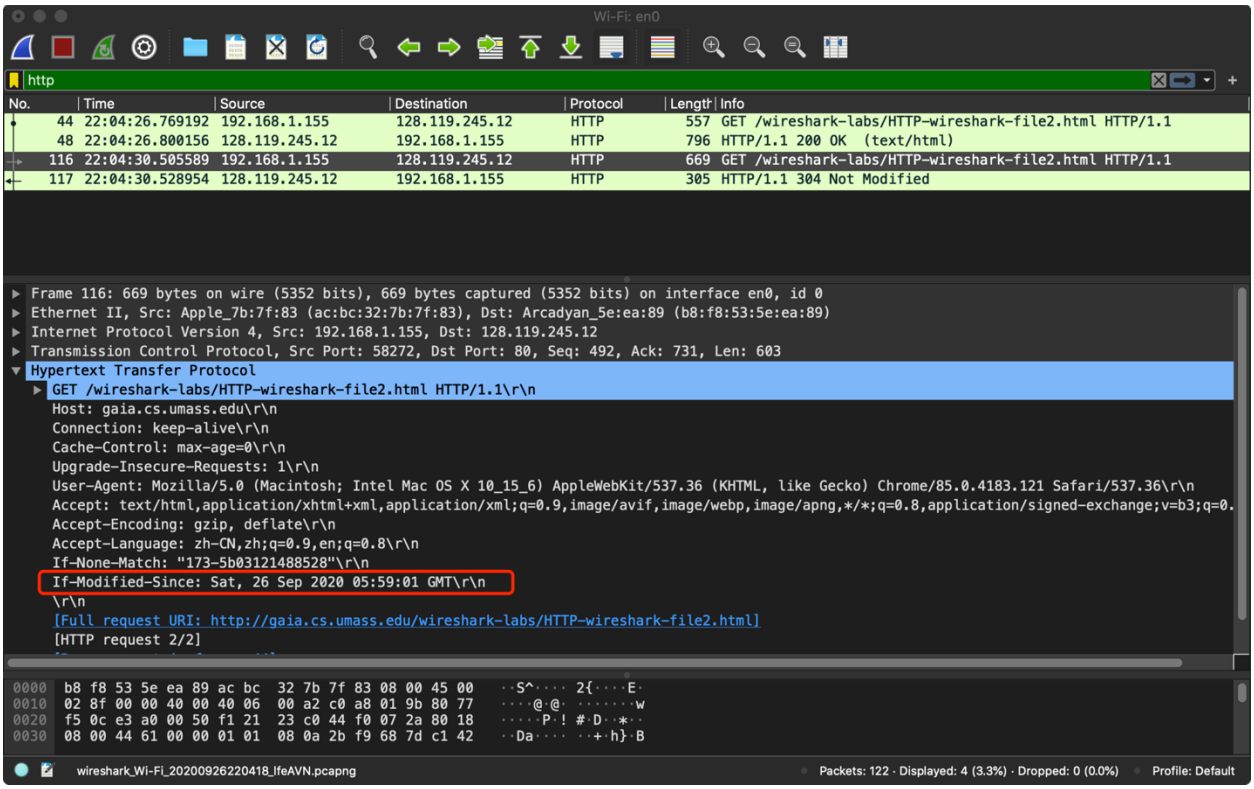
Q9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Answer: As shown in the screenshot below, we can see that the server explicitly return the contents of the file. We can see the content under the "Line-based text data". And the content here is exactly the content we can see on the webpage(http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html).



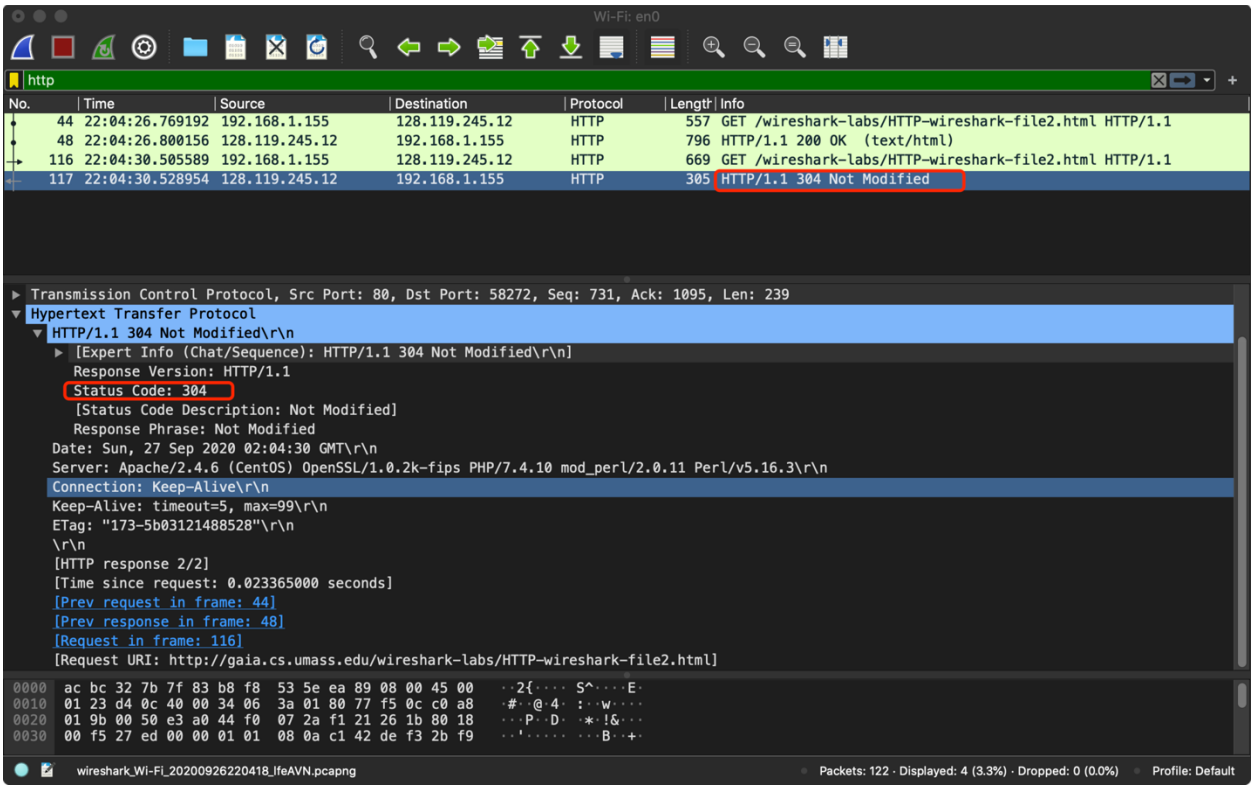
Q10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

Answer: As shown in the screenshot below, there is “IF-MODIFIED-SINCE” line in the second HTTP GET. IF-MODIFIED-SINCE: Sat, 26 Sep 2020 05:50:01 GMT\r\n



Q11. 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.

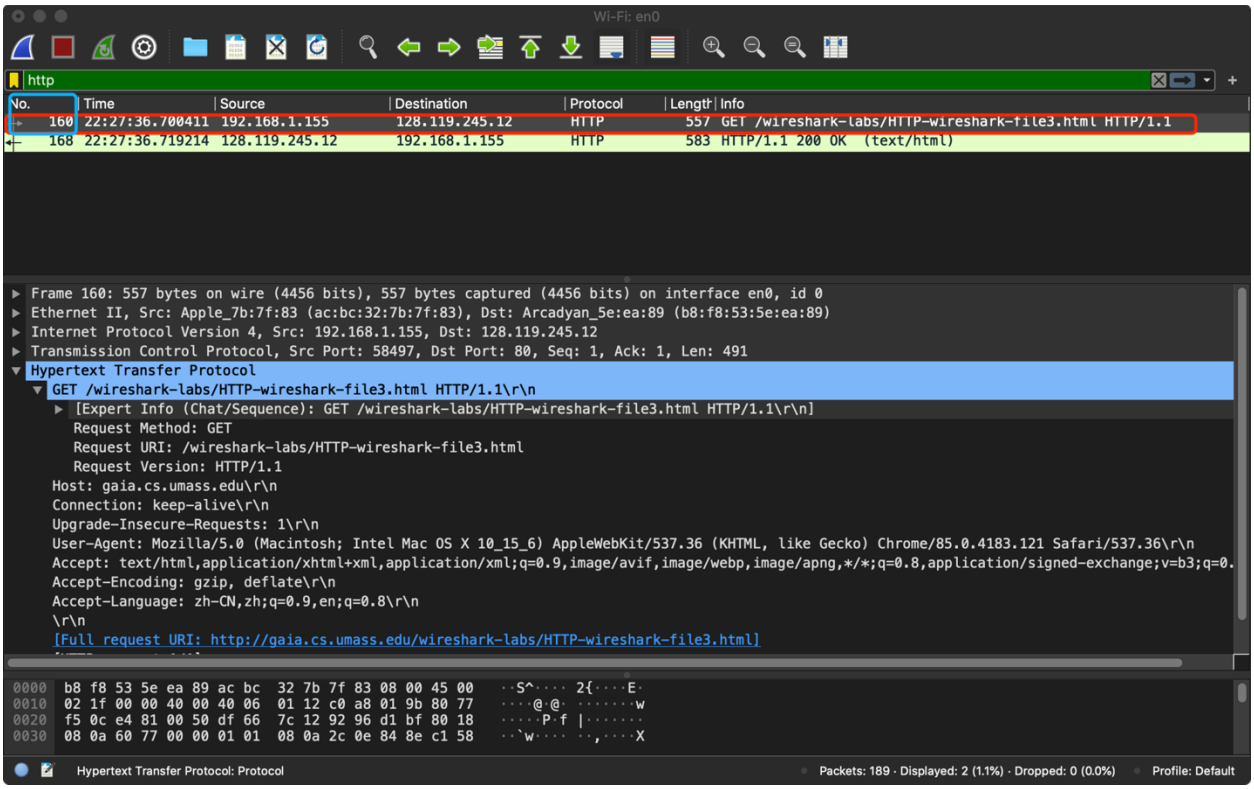
Answer: As shown in the screenshot below, the status code and phrase returned from the server in response to this second HTTP GET is “304” and “Not Modified”. And the server didn’t return the contents of the file. That’s because the we already have this file cached so when we request the same file for the second time, server doesn’t need to return the full response packet like it did for the first time.



Retrieving Long Documents. Answer the following questions:

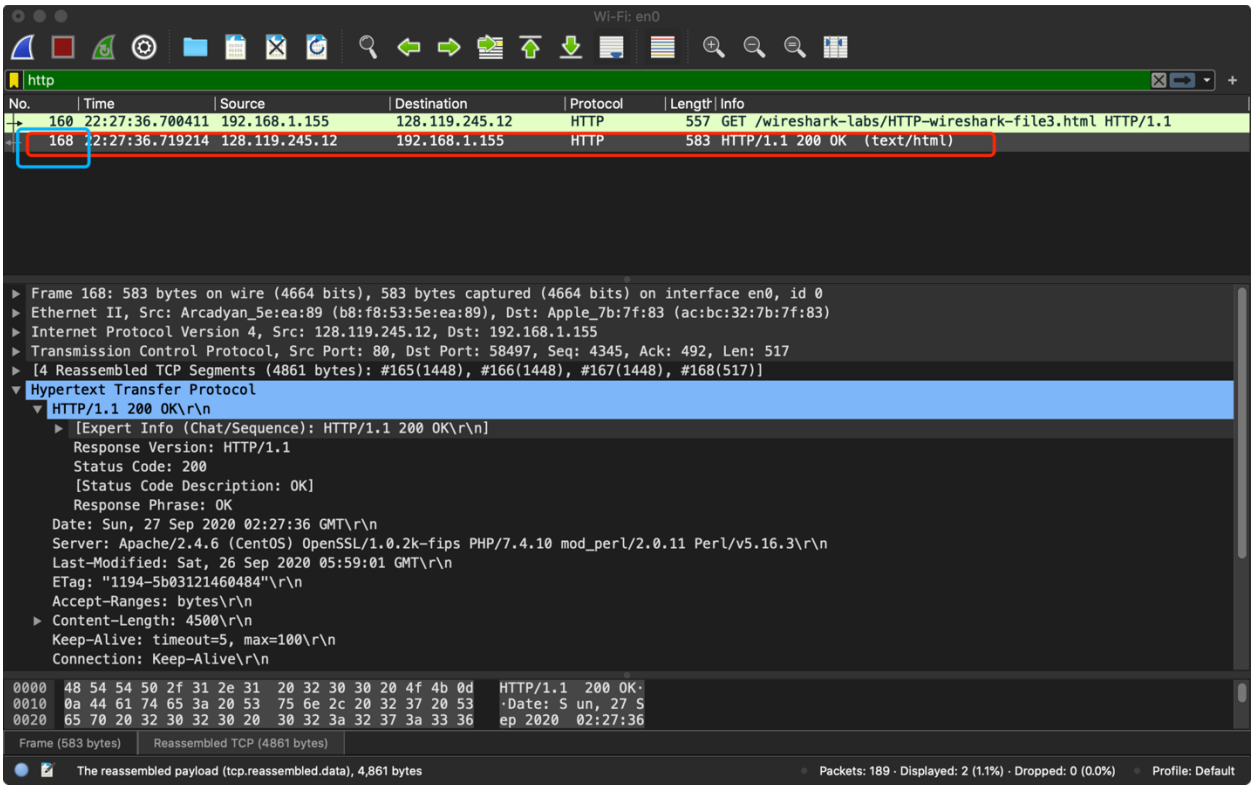
Q12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

Answer: As shown in the screenshot below my browser send one HTTP GET request messages. And the packet No.160 contains the GET message.



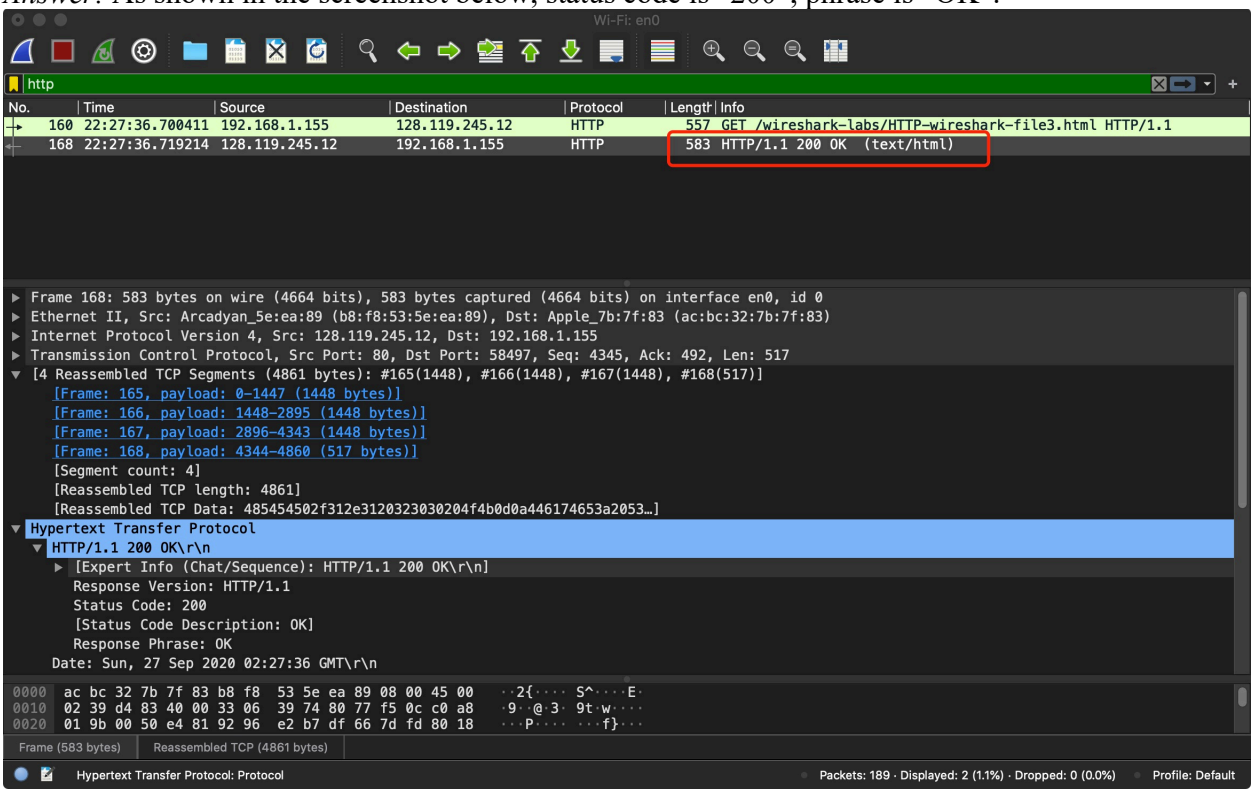
Q13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

Answer: As shown in the screenshot below, packet No.168 contains the status code and phrase associated with the response to the HTTP GET request.



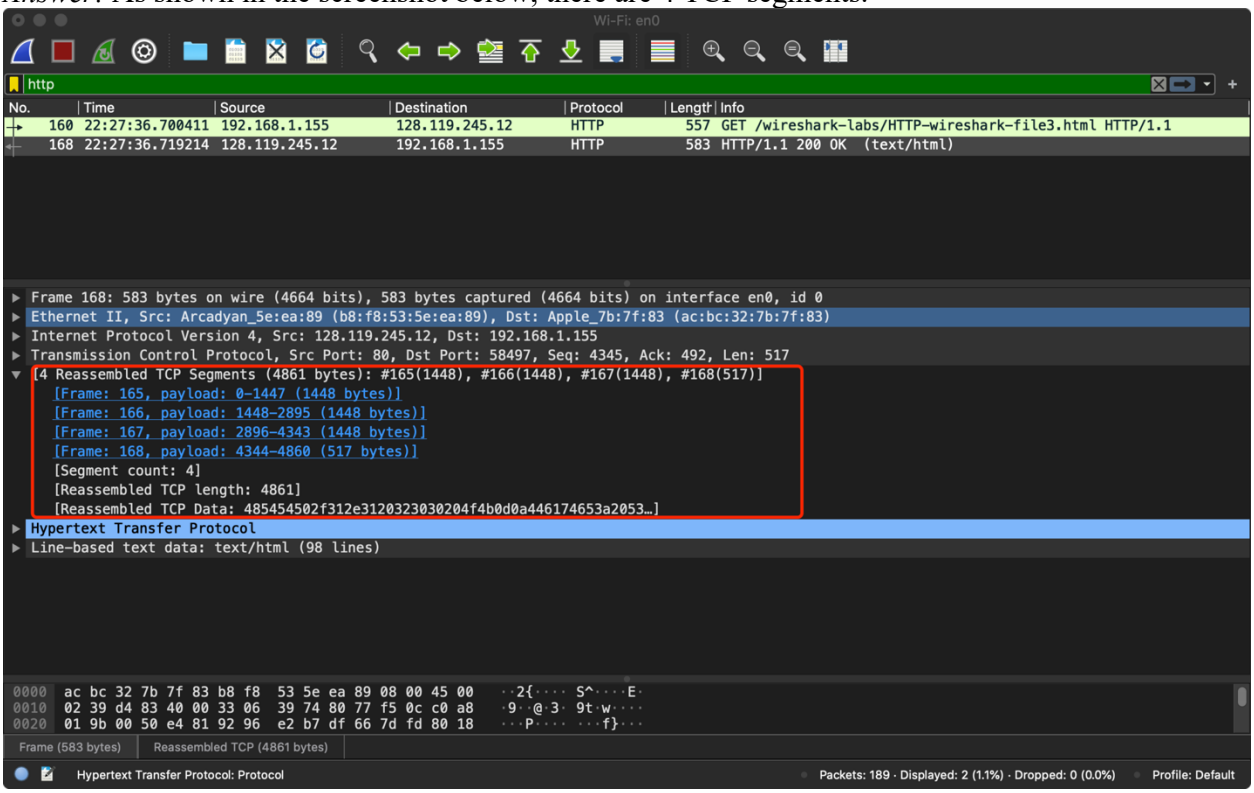
Q14. What is the status code and phrase in the response?

Answer: As shown in the screenshot below, status code is “200”, phrase is “OK”.



Q15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

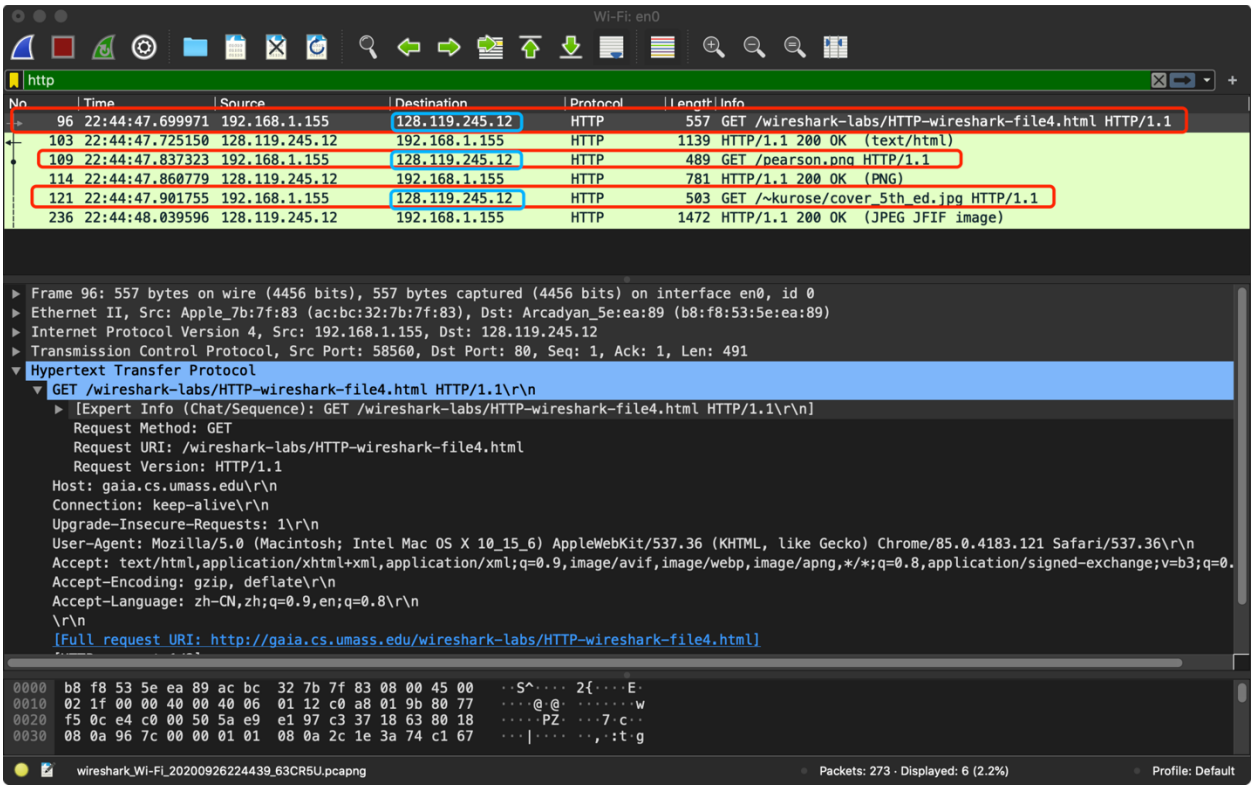
Answer: As shown in the screenshot below, there are 4 TCP segments.



HTML Documents with Embedded Objects. Answer the following questions:

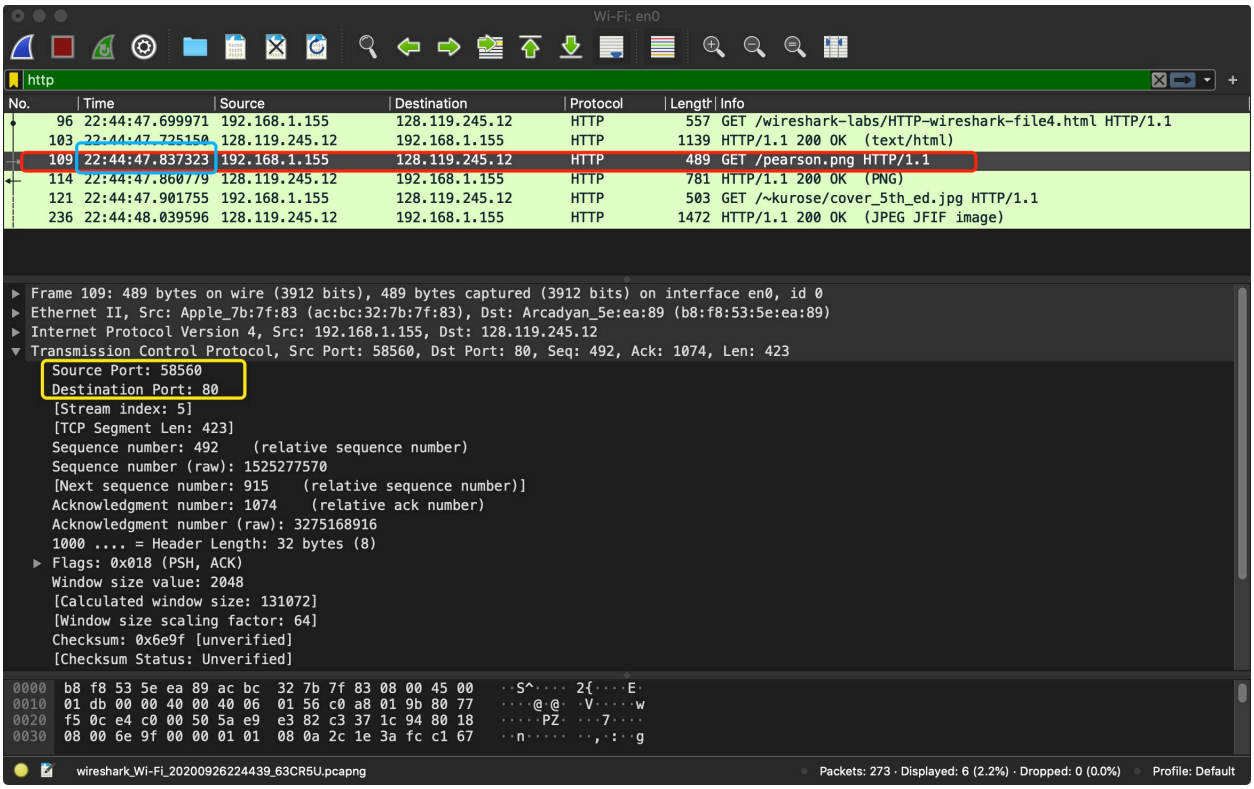
Q16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

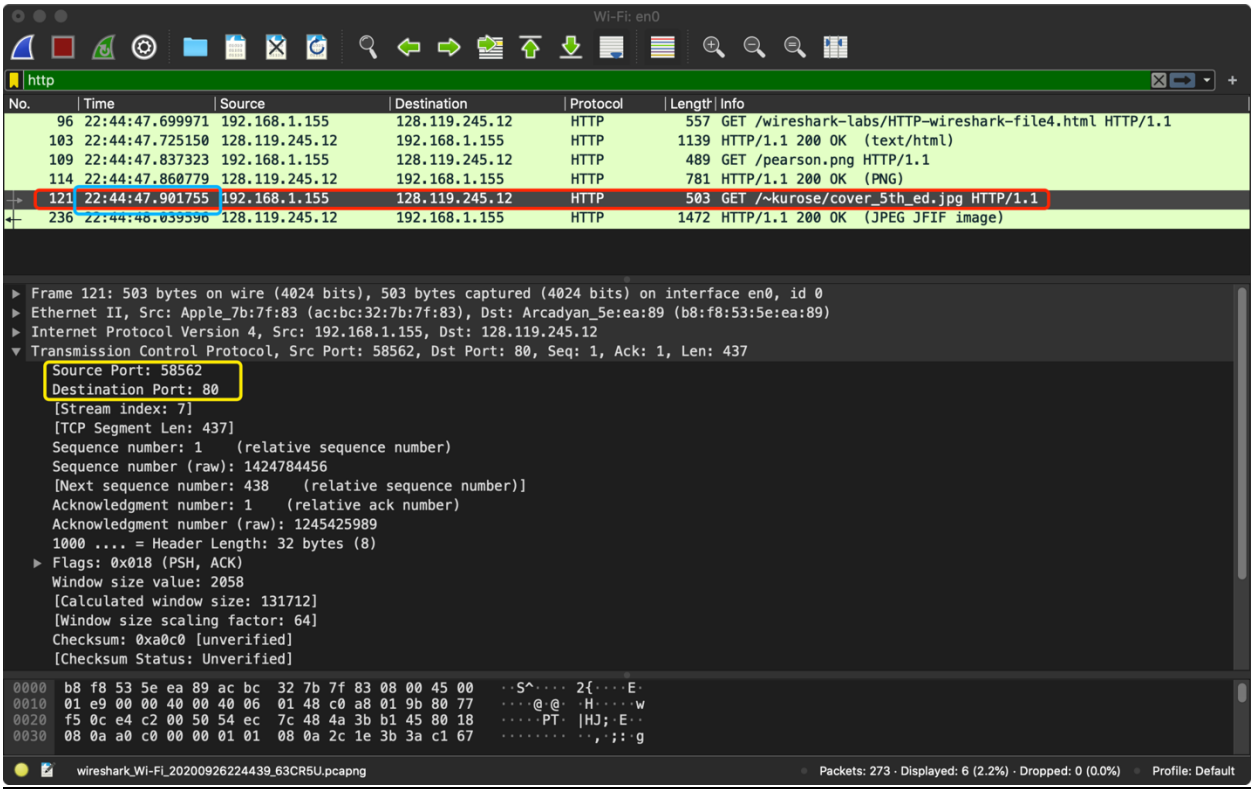
Answer: As shown in the screenshot below, there are 3 HTTP GET request messages did my browser send. The three Internet address are all 128.119.245.12.



Q17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

Answer: As shown in the screenshot below, from the timestamp we can see, two images were downloaded serially—the first image was requested at 22:44:47.837323 and finished download at 22:44:47.860779, the second image was requested at 22:44:47.901755 and finished download at 22:44:48.039596. What's more, the first image is transmitted via source port 58560, and the second image is transmitted via source port 58562. Thus we can know that two images were downloaded serially through two different TCP connections.

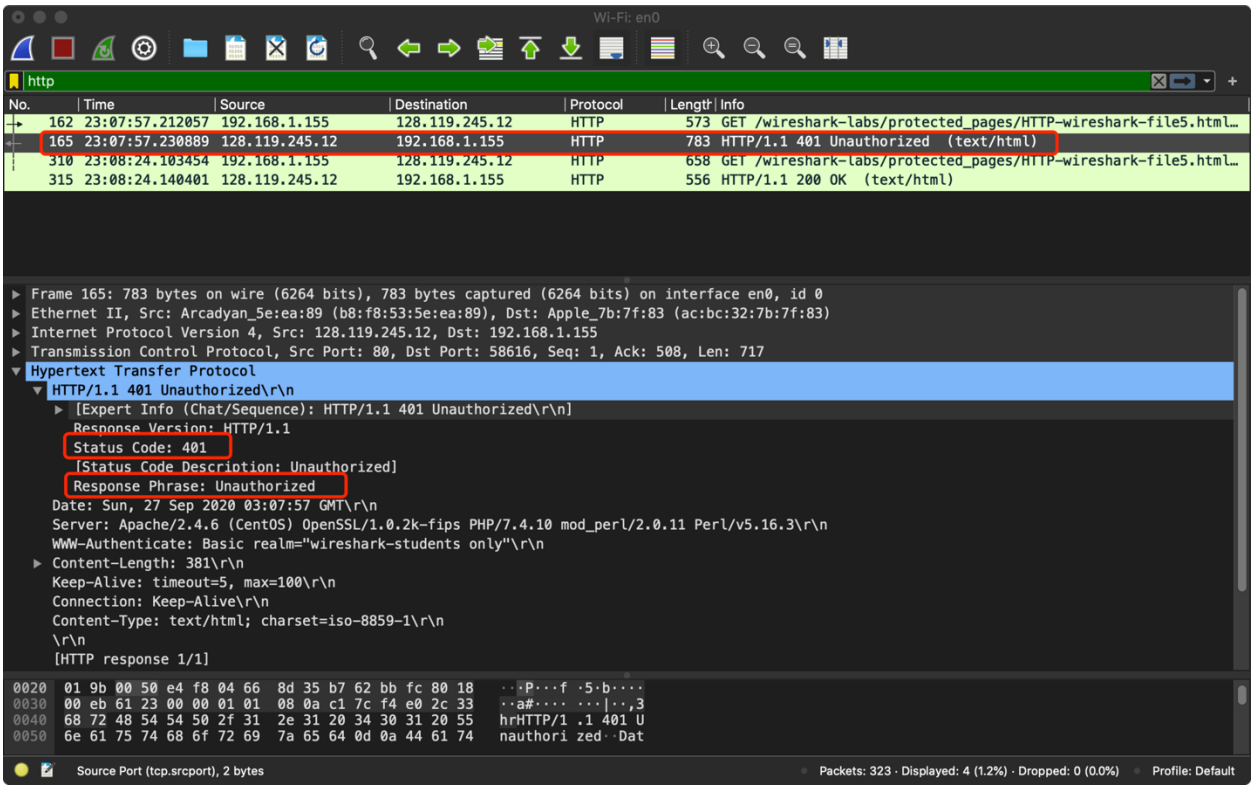




HTTP Authentication. Answer the following questions:

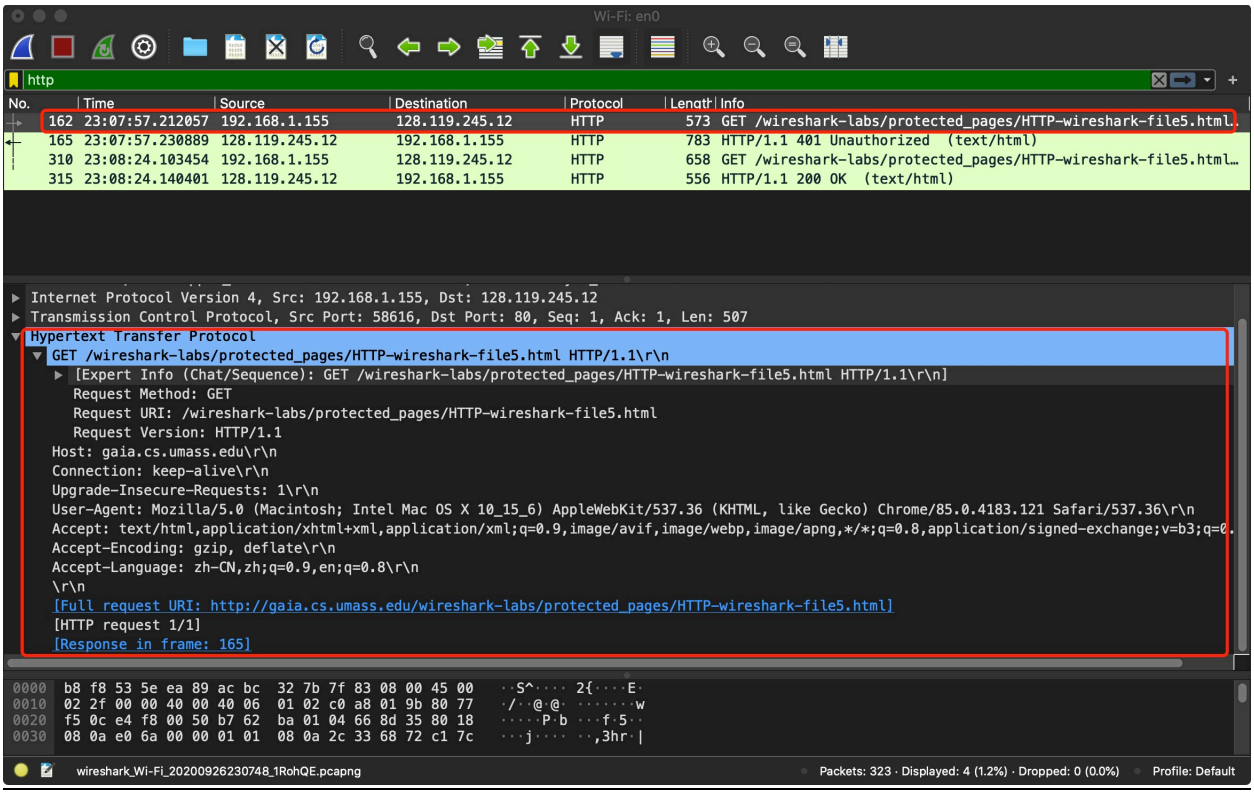
Q18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

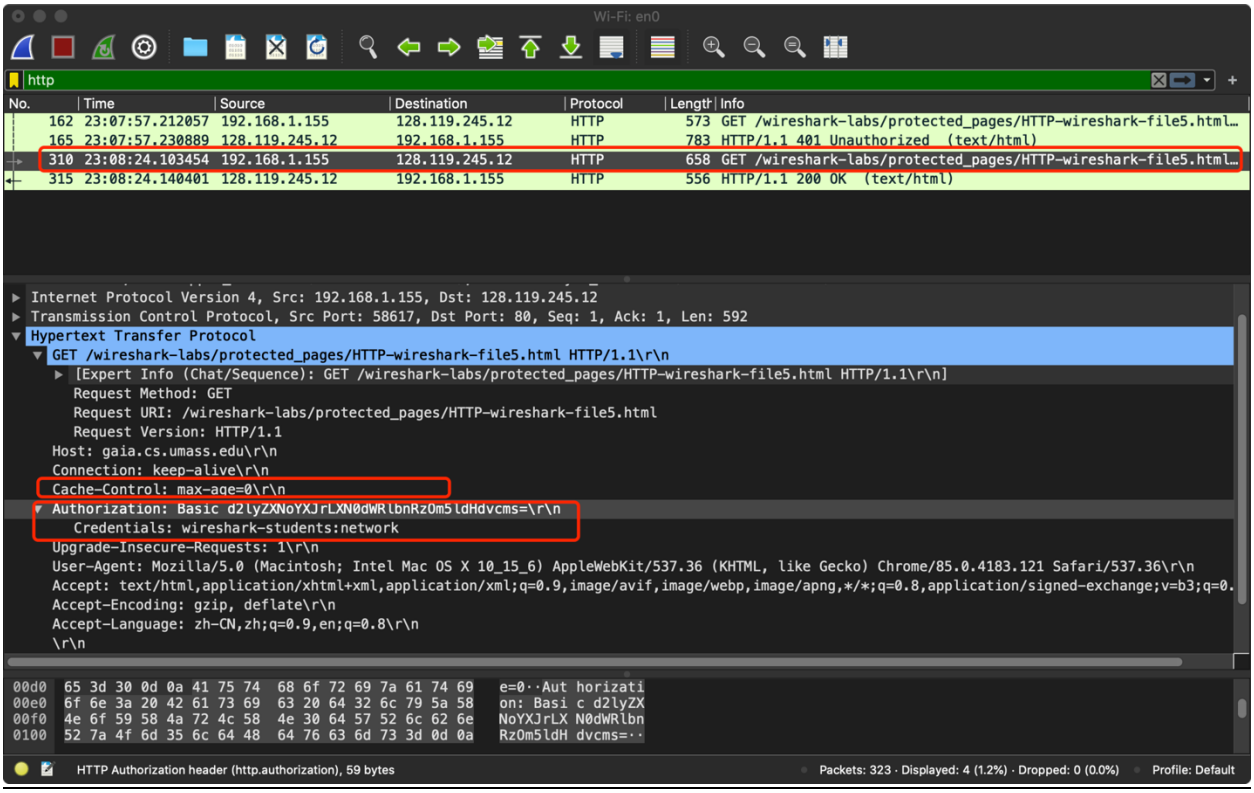
Answer: As shown in the screenshot below, the response to the initial HTTP GET message is "401 Unauthorized".



Q19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

Answer: As shown in the screenshots below, the first screenshot shows the data of the first HTTP GET and the second screenshot shows the data of the second HTTP GET. By comparing these two images we can see that the new fields are "Authorization" and "Cache-control".


Wi-Fi: en0
http
No. Time Source Destination Protocol Lengtf Info
162 23:07:57.212057 192.168.1.155 128.119.245.12 HTTP 573 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html…
165 23:07:57.230889 128.119.245.12 192.168.1.155 HTTP 783 HTTP/1.1 401 Unauthorized (text/html)
310 23:08:24.103454 192.168.1.155 128.119.245.12 HTTP 658 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html…
315 23:08:24.140401 128.119.245.12 192.168.1.155 HTTP 556 HTTP/1.1 200 OK (text/html)
Internet Protocol Version 4, Src: 192.168.1.155, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 58616, Dst Port: 80, Seq: 1, Ack: 1, Len: 507
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]
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
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 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-exchange;v=b3;q=0.
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
[HTTP request 1/1]
[Response in frame: 165]
0000 b8 f8 53 5e ea 89 ac bc 32 7b 7f 83 08 00 45 00
0010 02 2f 00 00 40 00 40 06 01 02 c0 a8 01 9b 80 77
0020 f5 0c e4 f8 00 50 b7 62 ba 01 04 66 8d 35 80 18
0030 08 0a e0 6a 00 00 01 01 08 0a 2c 33 68 72 c1 7c
wireshark_Wi-Fi_20200926230748_1RohQE.pcapng
Packets: 323 · Displayed: 4 (1.2%) · Dropped: 0 (0.0%)
Profile: Default


Wi-Fi: en0
http
No. Time Source Destination Protocol Lengtf Info
162 23:07:57.212057 192.168.1.155 128.119.245.12 HTTP 573 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html…
165 23:07:57.230889 128.119.245.12 192.168.1.155 HTTP 783 HTTP/1.1 401 Unauthorized (text/html)
310 23:08:24.103454 192.168.1.155 128.119.245.12 HTTP 658 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html…
315 23:08:24.140401 128.119.245.12 192.168.1.155 HTTP 556 HTTP/1.1 200 OK (text/html)
Internet Protocol Version 4, Src: 192.168.1.155, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 58617, Dst Port: 80, Seq: 1, Ack: 1, Len: 592
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]
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
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
Credentials: wireshark-students:network
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 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-exchange;v=b3;q=0.
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8\r\n
\r\n
00d0 65 3d 30 0d 0a 41 75 74 68 6f 72 69 7a 61 74 69
00e0 6f 6e 3a 20 42 61 73 69 63 20 64 32 6c 79 5a 58
00f0 4e 6f 59 58 4a 72 4c 58 4e 30 64 57 52 6c 62 6e
0100 52 7a 4f 6d 35 6c 64 48 64 76 63 6d 73 3d 0d 0a
HTTP Authorization header (http.authorization), 59 bytes
Packets: 323 · Displayed: 4 (1.2%) · Dropped: 0 (0.0%)
Profile: Default