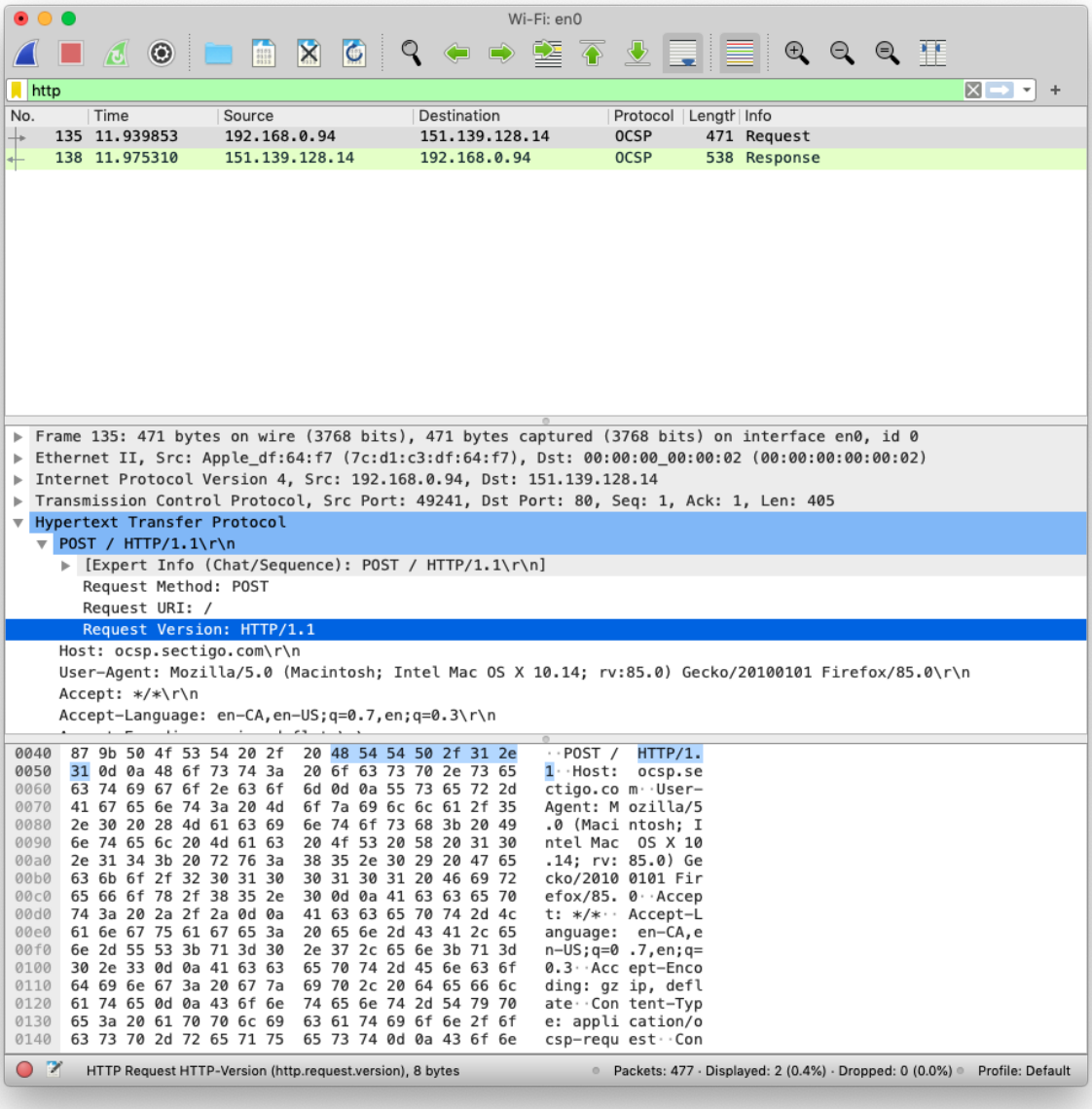
Class: CompSci 4C03
Student Name: Jatin Chowdhary
Student ID: 400033011
Date: February 1st, 2020

Assignment #1
Introduction To WireShark

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

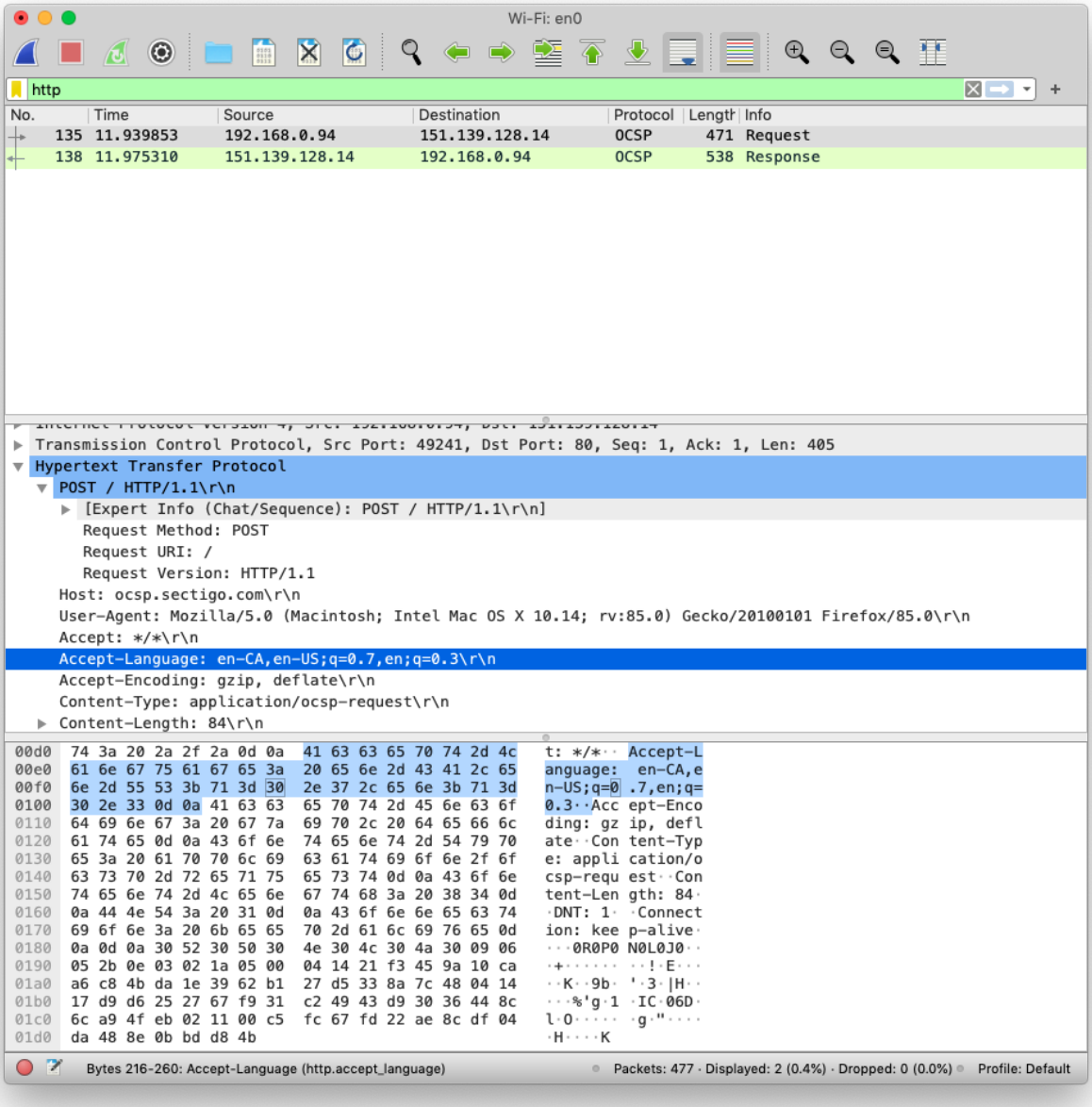
Answer:
My browser is running HTTP version 1.1. The server is running HTTP version 1.1. Both are running HTTP version 1.1.
This can be seen in the screenshot below.



Answer 1: The text highlighted in light-blue pertains to my laptop, and it shows that my laptop is running HTTP version 1.1. The text in dark-blue pertains to the server and shows that the server is running HTTP version 1.1. All of this information is available in the "Hypertext Transfer Protocol" section for the "Request" packet, in the "Packet-Header Details" window.

Question #2:
What languages (if any) does your browser indicate that it can accept to the server?

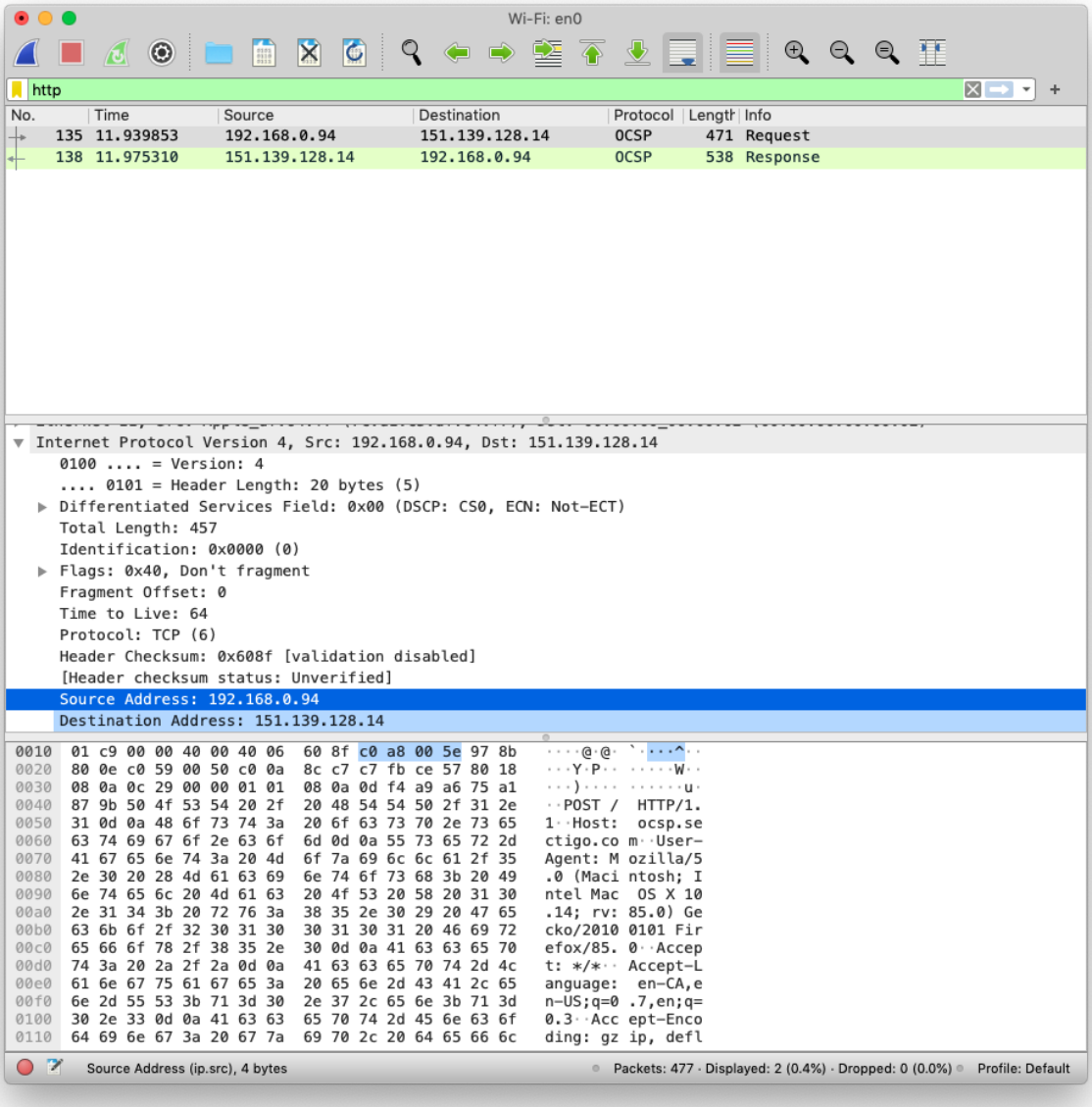
Answer:
My browser indicates that it can accept English (Canadian and United States) as a language to the server.
This can be seen in the screenshot below.



Answer 2: The text highlighted in dark-blue shows that my laptop accepts two languages, and they are "English-Canada", and "English-United States". All of this information is available in the "Hypertext Transfer Protocol" section for the "Request" packet, in the "Packet-Header Details" window.

Question #3:
What is the IP address of your computer? Of the www.cas.mcmaster.ca server?

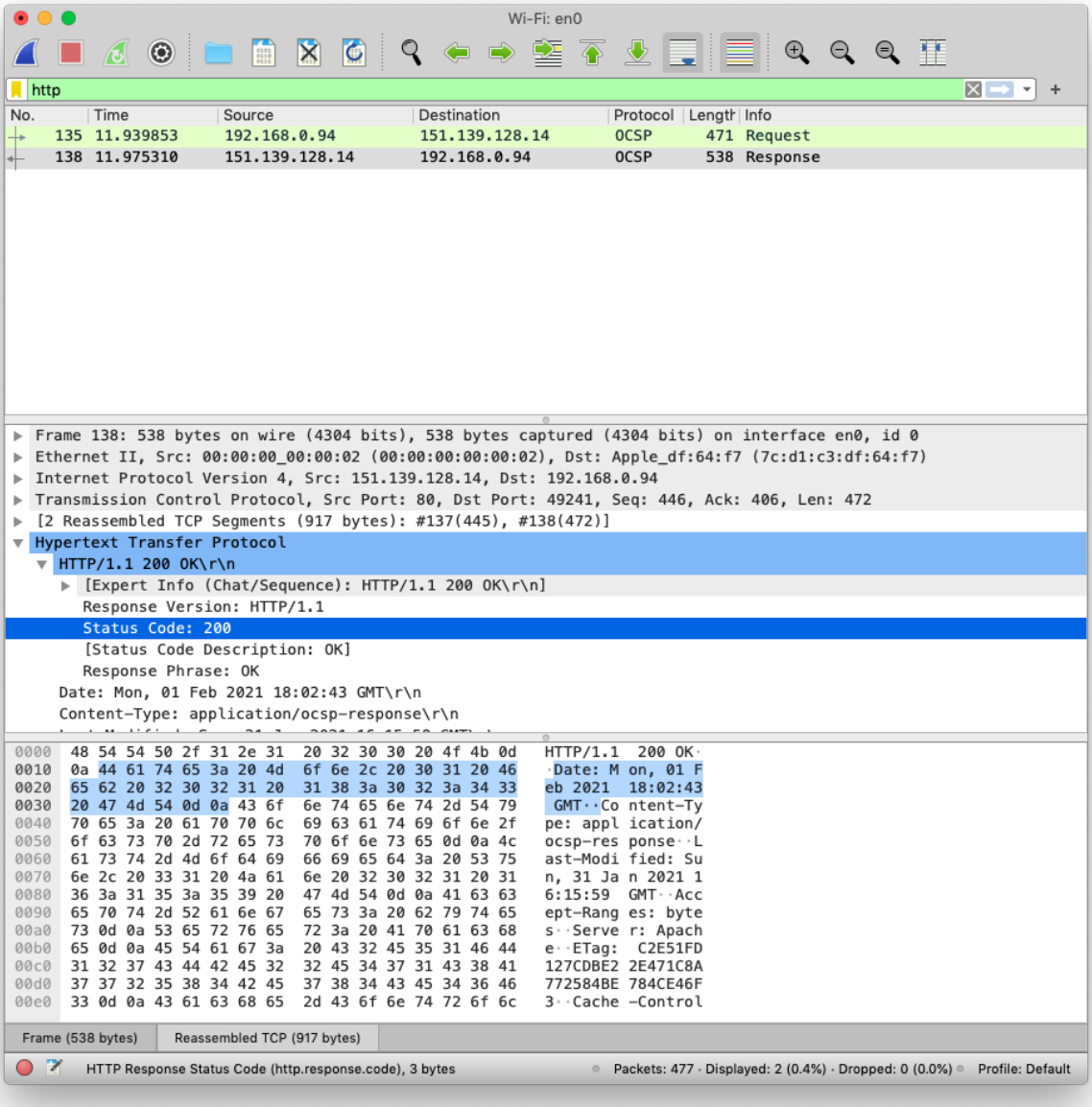
Answer:
The (local) IP address of my computer is: 192.168.0.94.
The IP address of the server is: 151.139.128.14.
This can be seen in the screenshot below.



Answer 3: The text highlighted in dark-blue is my (local) IP address; the source address. My (local) IP address is making the request to the server. The text highlighted in light-blue is the destination address, which is the server that contains the information I want. All of this information is available in the "Internet Protocol Version 4..." section for the "Request" packet, in the "Packet-Header Details" window.

Question #4:
What is the status code returned from the server to your browser?

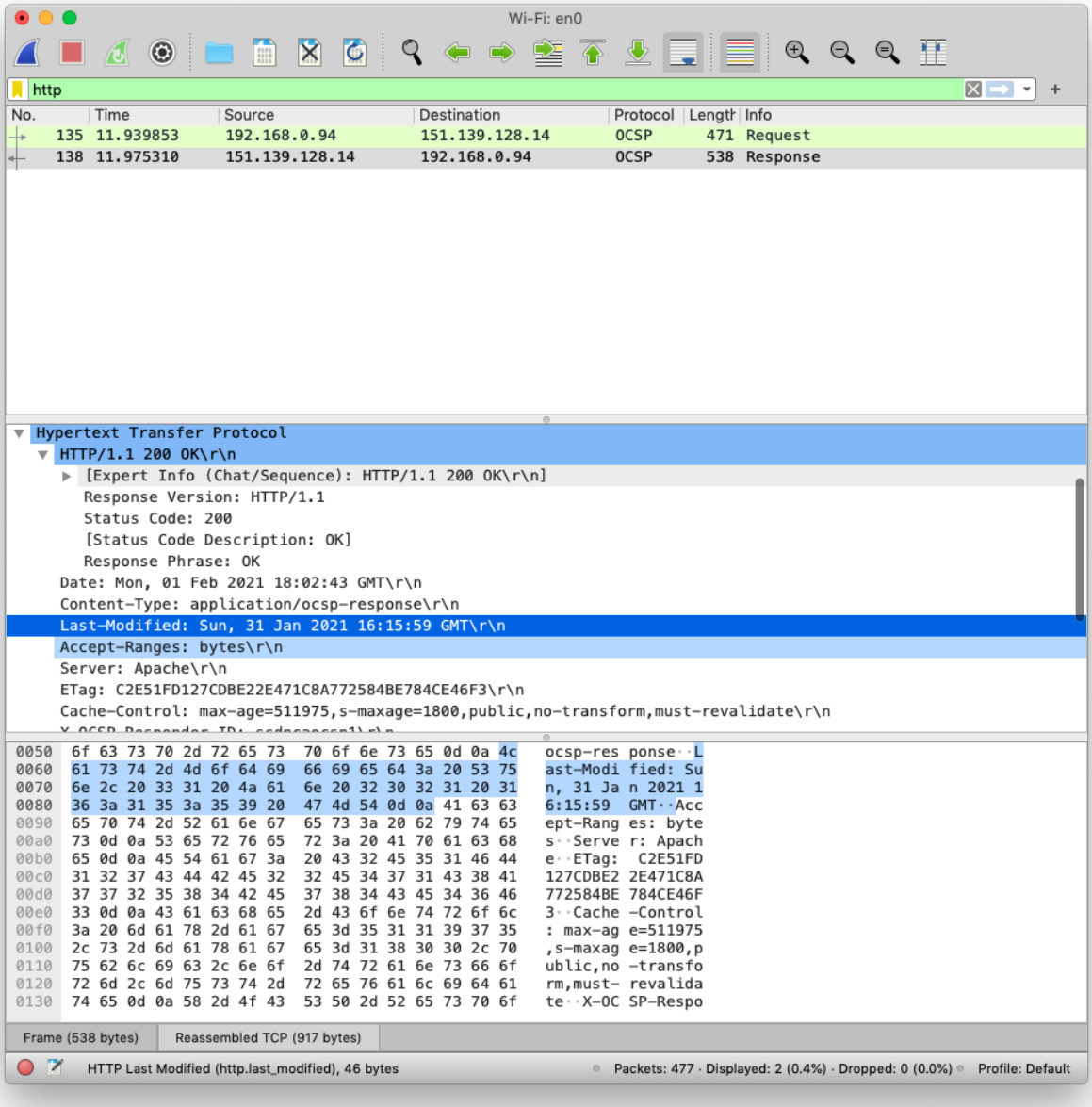
Answer:
The status code returned from the server to my browser is 200. This means that the transfer of information completed without errors. This can be seen in the screenshot below.



Answer 4: The text highlighted in dark-blue is the "Status Code" that is returned from the server to my browser. As you can see, the server returns a "Status Code" of 200. All of this information is available in the "Hypertext Transfer Protocol" section for the "Response" packet, in the "Packet-Header Details" window.

Question #5:
When was the HTML file that you are retrieving last modified at the server?

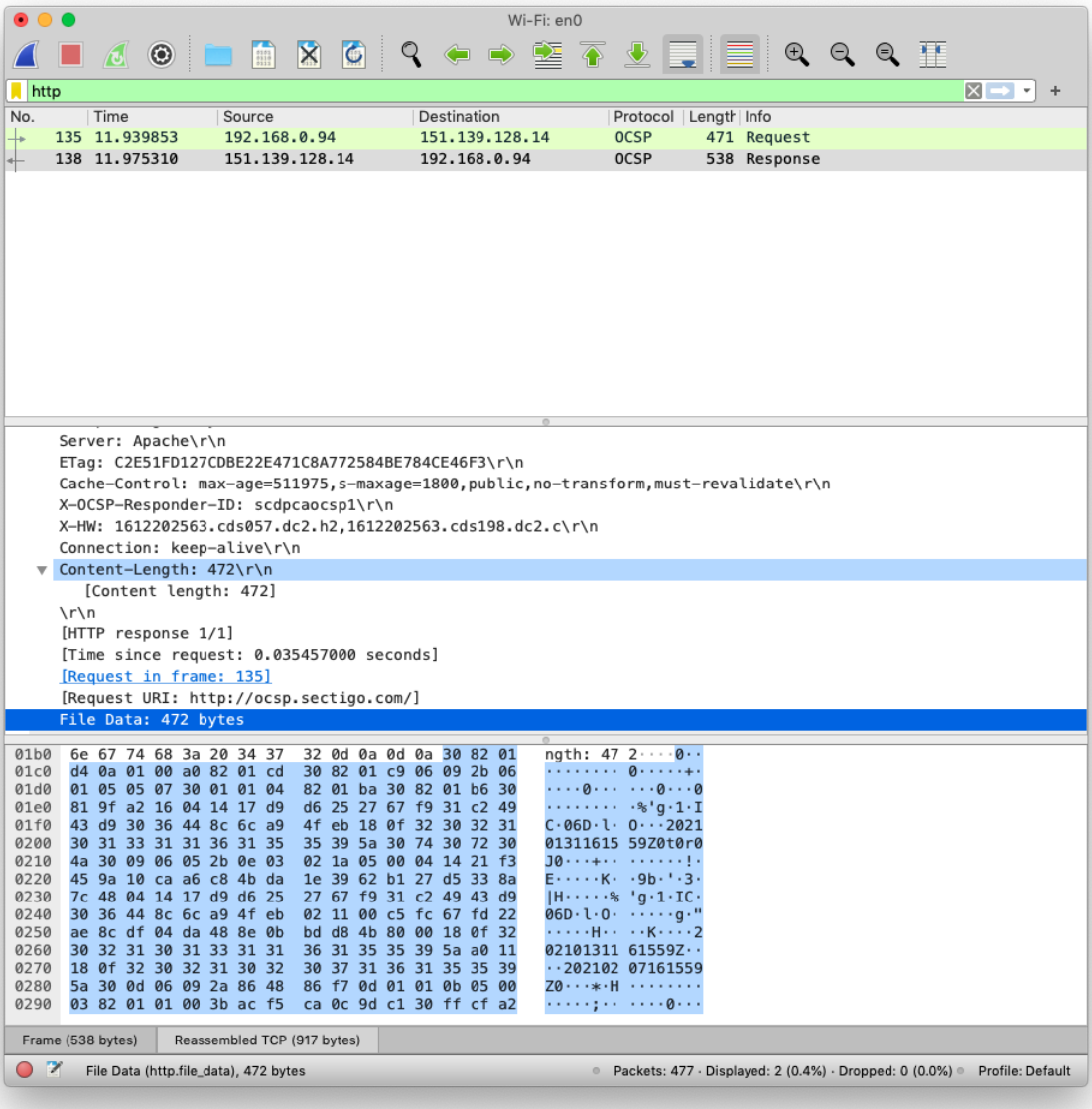
Answer:
The HTML file that I am retrieving from the server was last modified on: Sunday, January 31st, 2021.
This can be seen in the screenshot below.



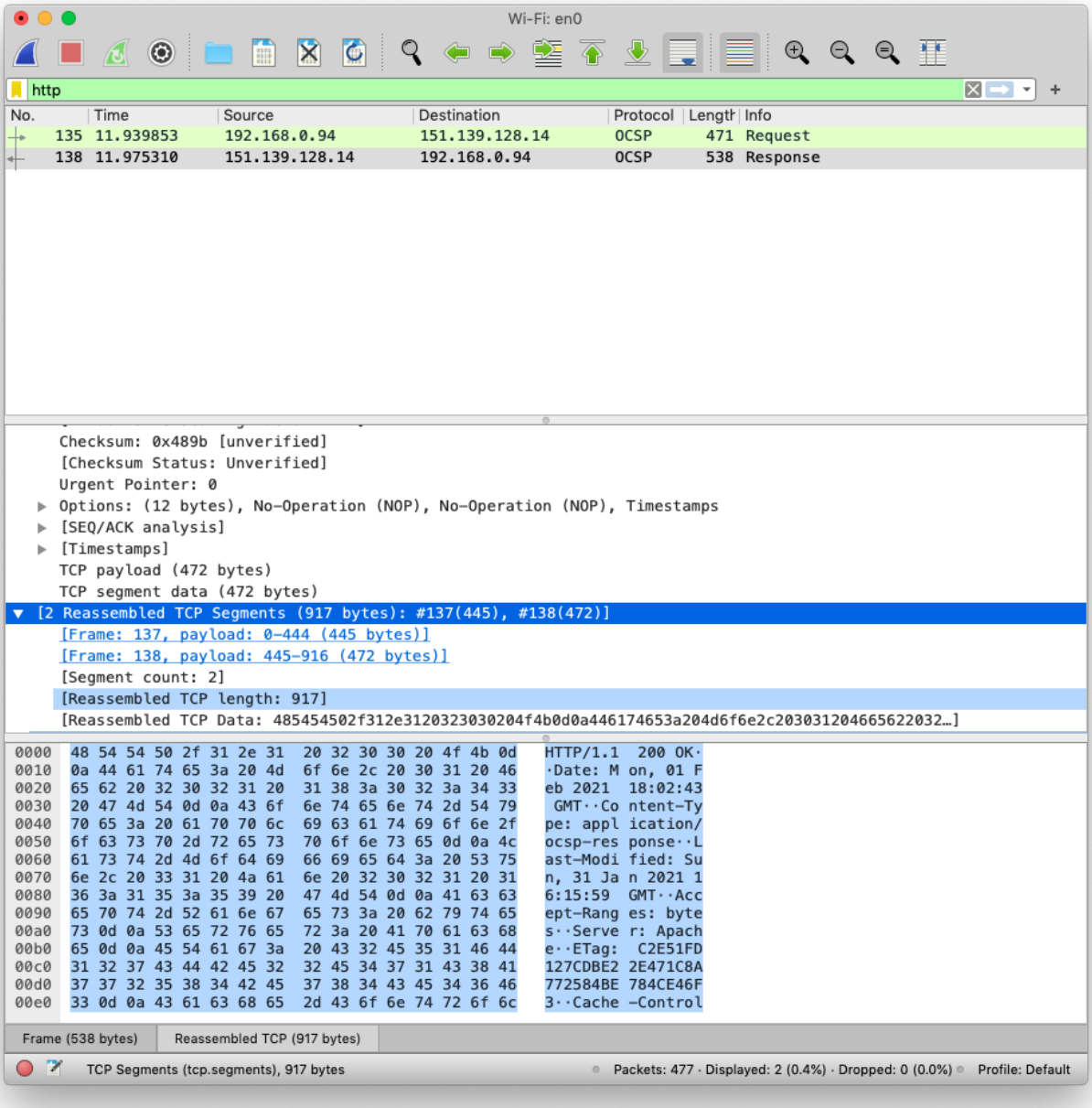
Answer 5: The text highlighted in dark-blue is the date, and exact time that the HTML file was last modified. All of this information is available in the "Hypertext Transfer Protocol" section for the "Response" packet, in the "Packet-Header Details" window.

Question #6:
How many bytes of content are being returned to your browser?

Answer:
The server is returning 472 bytes of data to my browser. This is the size of the HTML file. However, if you include the size of the entire datagram/packet, and not just the message, but the header as well, then 917 bytes of data are being returned to my browser.
This can be seen in the screenshots below.
The first screenshot shows the size of the HTML file; the message.
The second screenshot shows the size of the entire packet divided into 2 TCP segments.



Answer 6: The text highlighted in dark-blue shows the size of the HTML file. The text highlighted in light-blue is the same information but is called "Content-Length". All of this information is available in the "Hypertext Transfer Protocol" section for the "Response" packet, in the "Packet-Header Details" window.



Answer 6: The text highlighted in dark-blue is the section where the entire size of the packet is located. The text highlighted in light-blue is the total size of the TCP packet; this includes both header and message. Above this, is text in light-blue color, and it is underlined. This information breaks down the size of the TCP packet into its segments/parts. As you can see, one TCP segment is 445 bytes, and the other TCP segment is 472 bytes. Since we already know that the size of the message/data is 472, the first TCP segment, which is 445 bytes, must be the size of the header. All of this information is available in the "...Reassembled TCP Segments..." section for the "Response" packet, in the "Packet-Header Details" window.

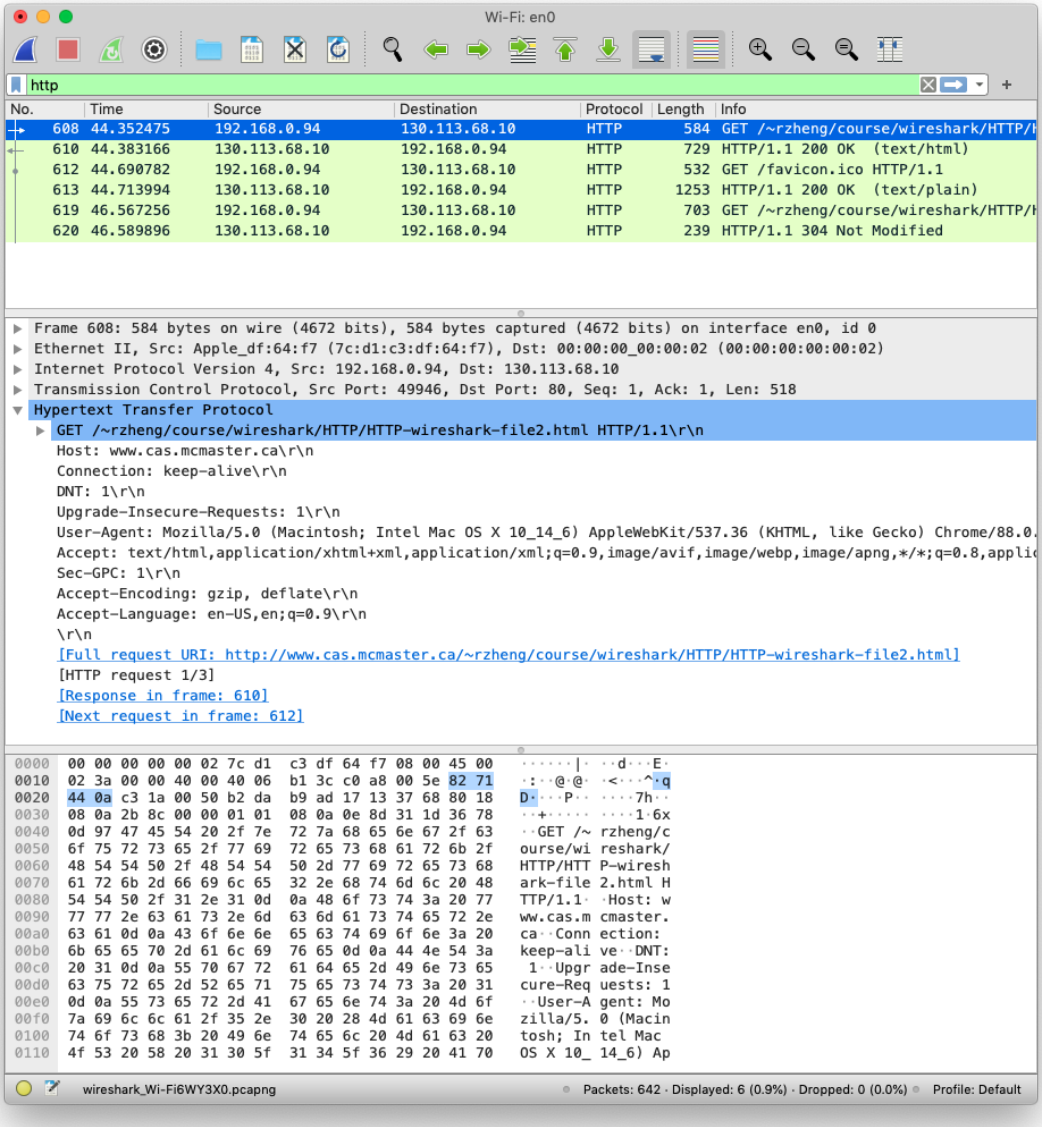
Question #7:
By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

Answer:
No, I do not see any headers in the raw data that are not displayed in the packet-listing window. All headers are present and accounted for in the packet-listing window. Every byte in the packet’s raw data is accounted for in the packet-listing window.

No screenshot(s) provided for this question, because it is not required.

Question #8:
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?

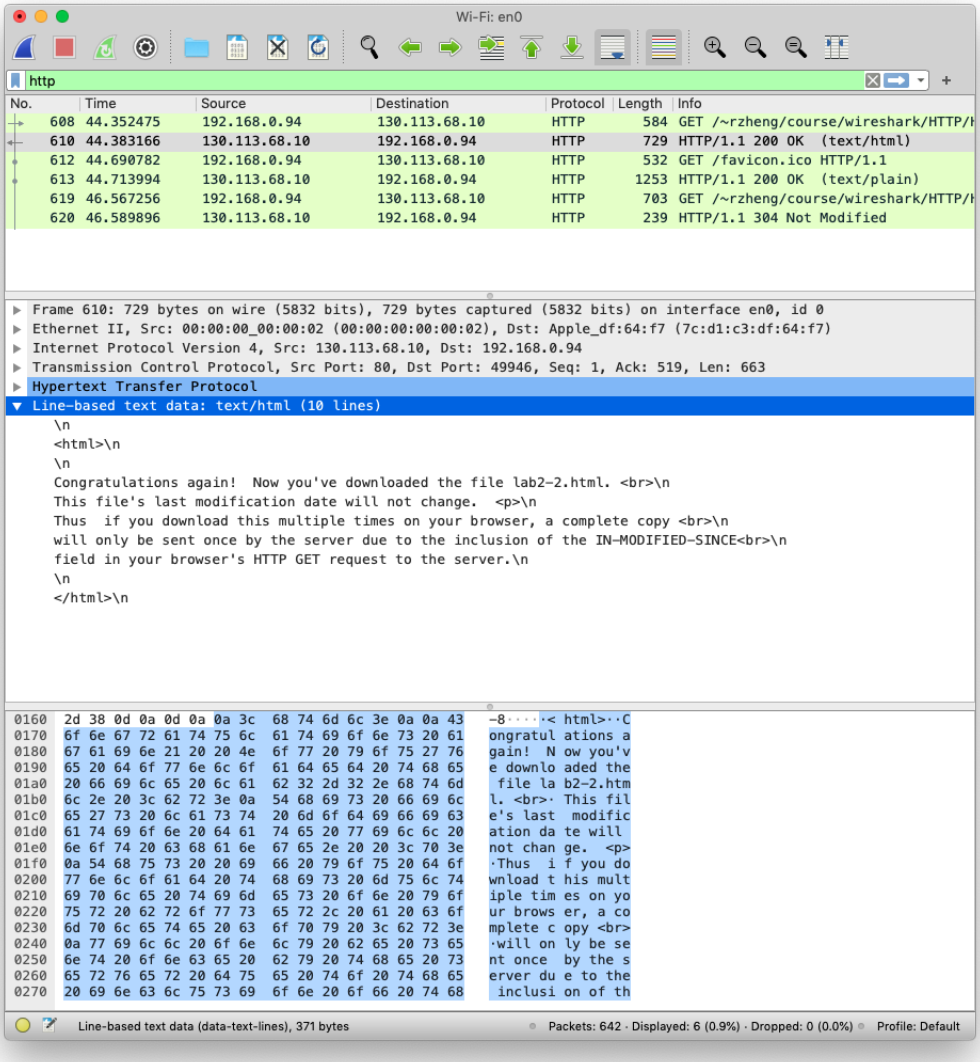
Answer:
No, I do not see an “IF-MODIFIED-SINCE:” line in the first ‘HTTP GET’ packet. There is no “IF-MODIFIED-SINCE:” line in the “Hypertext Transfer Protocol” section. This can be seen in the screenshot below.



Answer 8: The text highlighted in light-blue is the “Hypertext Transfer Protocol” section, and everything underneath it pertains to it. There is no “IF-MODIFIED-SINCE:” in the information below the heading. If there was an “IF-MODIFIED-SINCE:” field and value, then this information would be available in the “Hypertext Transfer Protocol” section for the “HTTP GET” packet, in the “Packet-Header Details” window.

Question #9:
Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

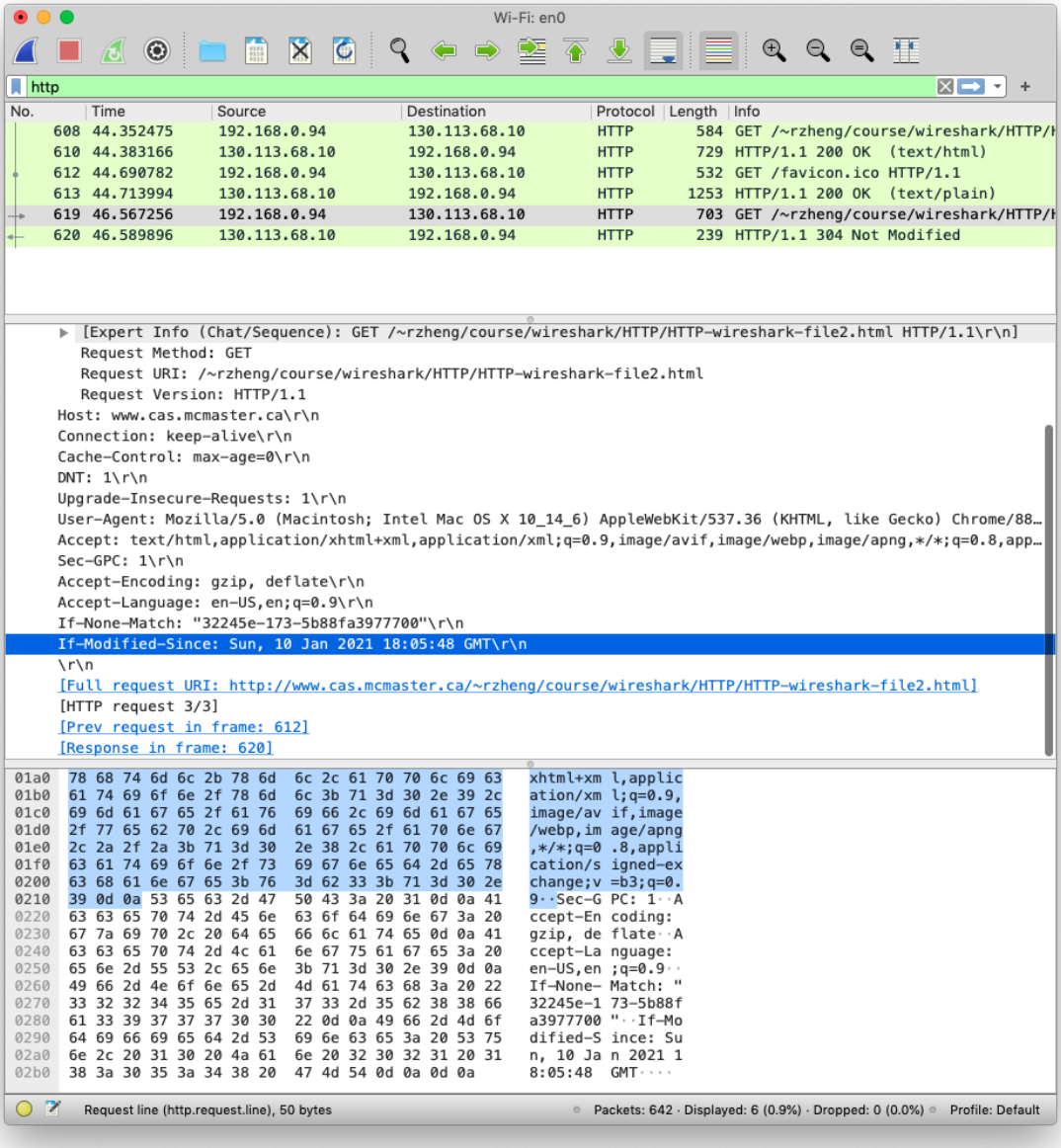
Answer:
Yes, the server did explicitly return the contents of the file. I can tell because there is text/data in the packet's raw data that is not part of the header file. This data is part of the webpage. Also, under the "Line-based text data..." section, I can see that data was returned from the server to my browser.
This can be seen in the screenshot below.



Answer 9: The text highlighted in dark-blue is the "Line-based text data..." section, and it contains the data that was sent to my browser from the server. This proves that the server's response to my "HTTP GET" request returned valid data. Furthermore, in the "Packet-list" window we can see that the response from the server is '200', which indicates that the data was transferred without any errors. All of this information is available in the "Line-based text data..." section for the "HTTP/Response" packet, in the "Packet-Header Details" window.

Question #10:
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?

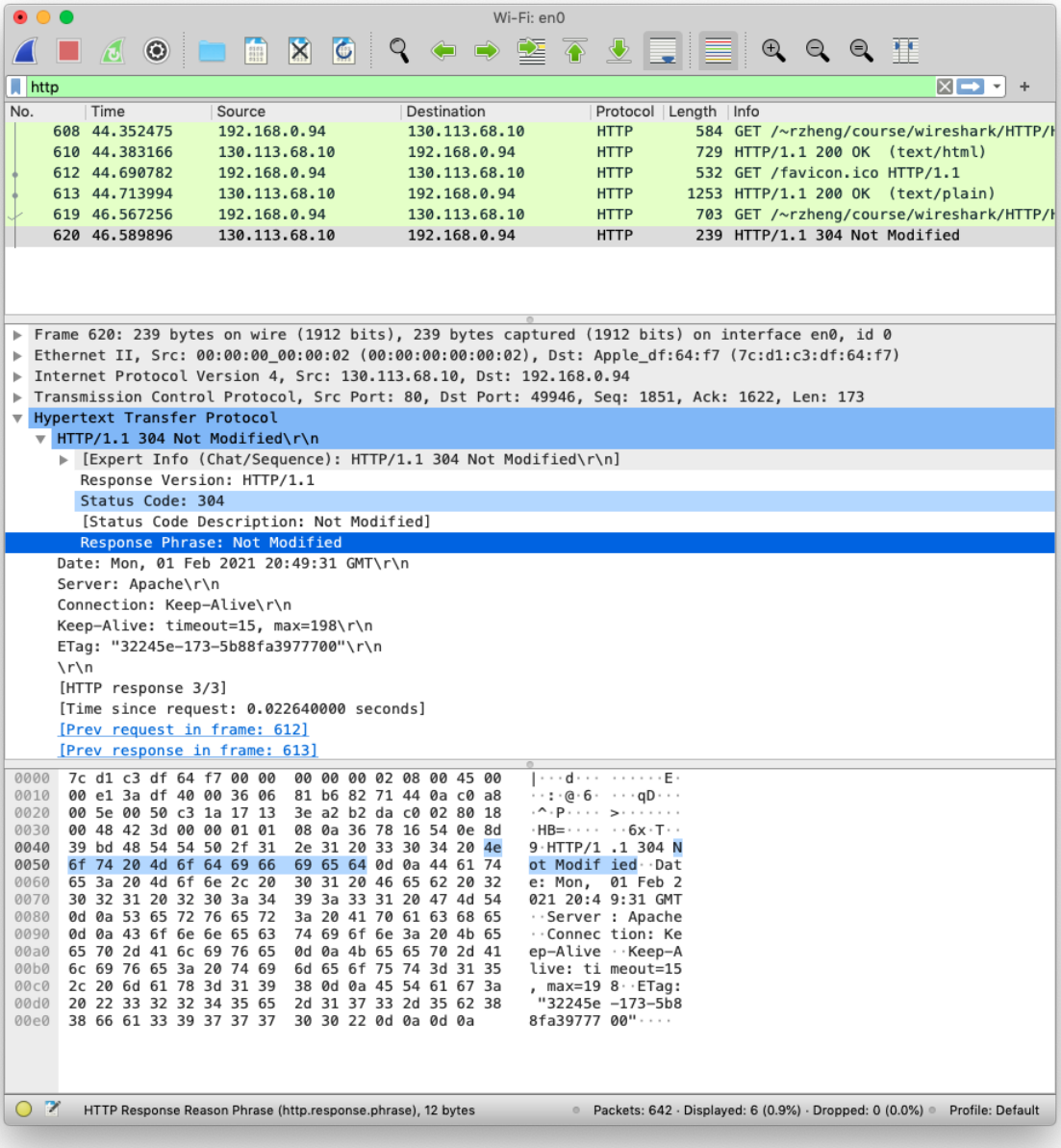
Answer:
Yes, I do see an “IF-MODIFIED-SINCE:” line. The value of this field is: *If-Modified-Since: Sun, 10 Jan 2021 18:05:48 GMT*.
This can be seen in the screenshot below.



Answer 10: The text highlighted in dark-blue is the "If-Modified-Since:" line. It is present in the second "HTTP GET" packet and contains a value, a date and time. All of this information is available in the “Hypertext Transfer Protocol” section for the “HTTP GET” packet, in the “Packet-Header Details” window.

Question #11:
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.

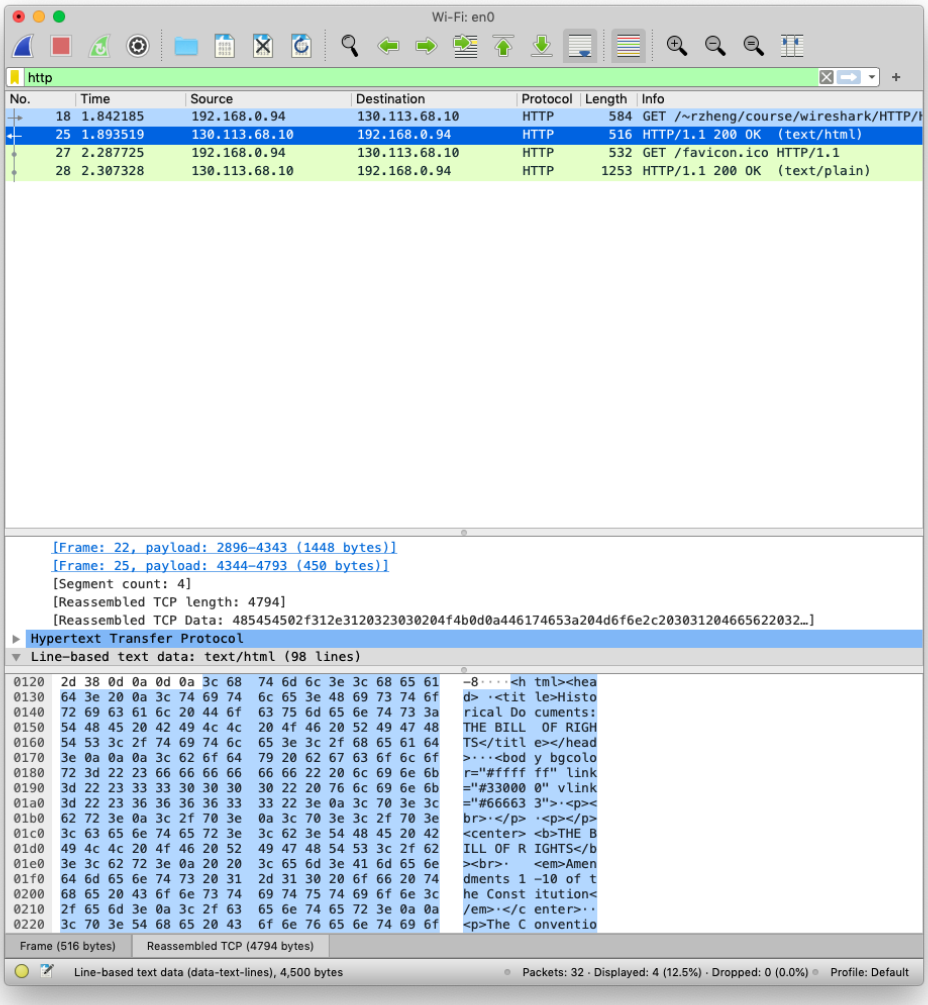
Answer:
In response to the second HTTP GET, the response phrase from the server is “Not Modified”, and the response status code is “304”. The server did not explicitly return the contents of the file. I can tell that the server did not return the contents of the file because of the status code and phrase returned. Furthermore, there is no “Line-based text data...” section that contains information. Therefore, the server did not explicitly return the contents of the file. This is because the file on the server remained the same. So the HTTP protocol decided it would be more efficient to just check if the data was modified, instead of returning a whole block of data that is already loaded on my browser.
This can be seen in the screenshot below.



Answer 11: The text highlighted in dark-blue is the "Response Phrase" from the server, and, directly above, the text highlighted in light-blue is the "Status Code" response from the server. All of this information is available in the "Hypertext Transfer Protocol" section for the "HTTP/Request" packet, in the "Packet-Header Details" window.

Question #12:
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?

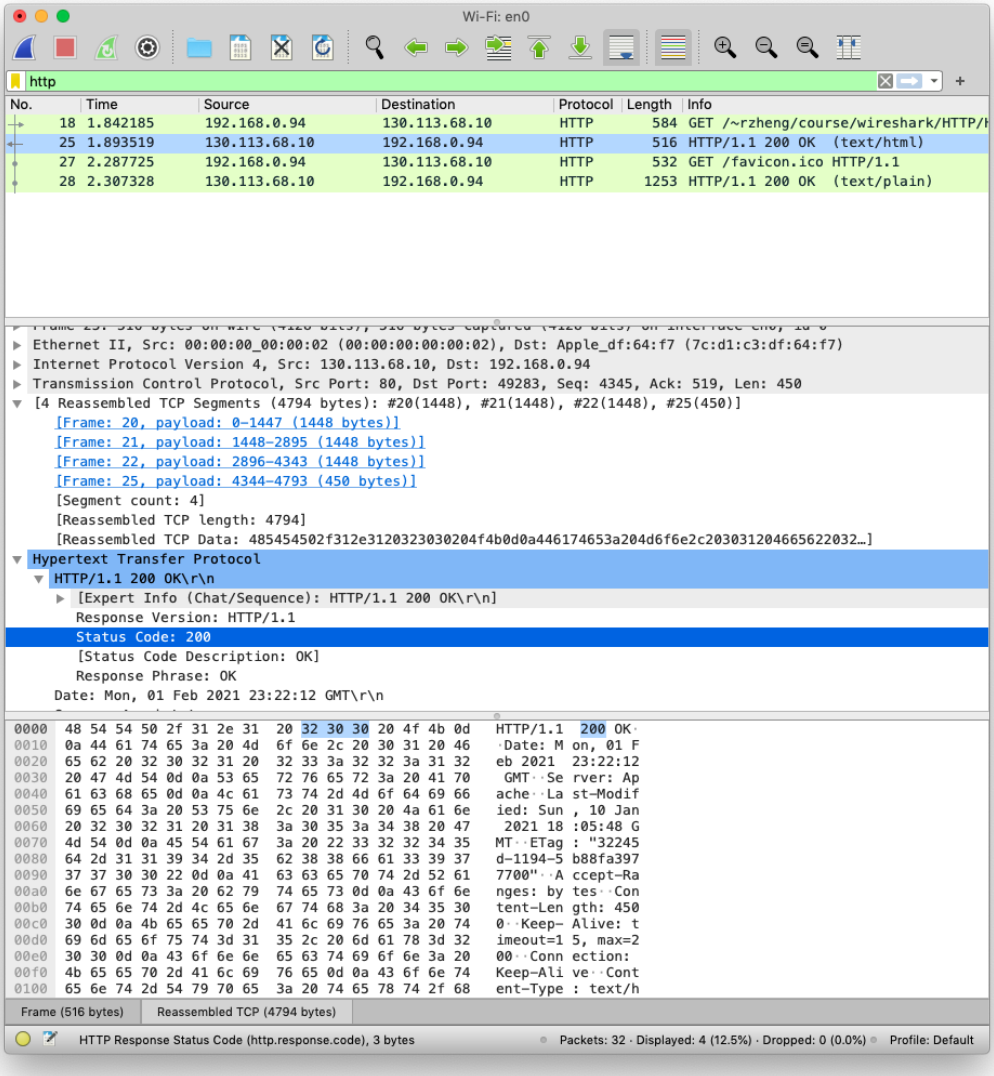
Answer:
My browser sent (1 + 1) HTTP GET request messages. However, one of them is a `*favicon.ico*` request and is not being counted for this assignment. Therefore, my browser sent 1 HTTP GET request message. Packet #25 in the trace contains the HTTP GET message for the “Bill Of Rights”. In Packet #25, all the Frames (20, 21, 22, 25) contain the “Bill Of Rights”.
This can be seen in the screenshot below.



Answer 12: At the top of the Wireshark application, in the “Packet-listing” window, the packet highlighted in light-blue is the HTTP GET packet that is sent by my browser. Just below it, the packet highlighted in dark-blue is the HTTP/Response for the HTTP GET packet that is right above it. All of this information is available in the "Packet-listing" window.

Question #13:
Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

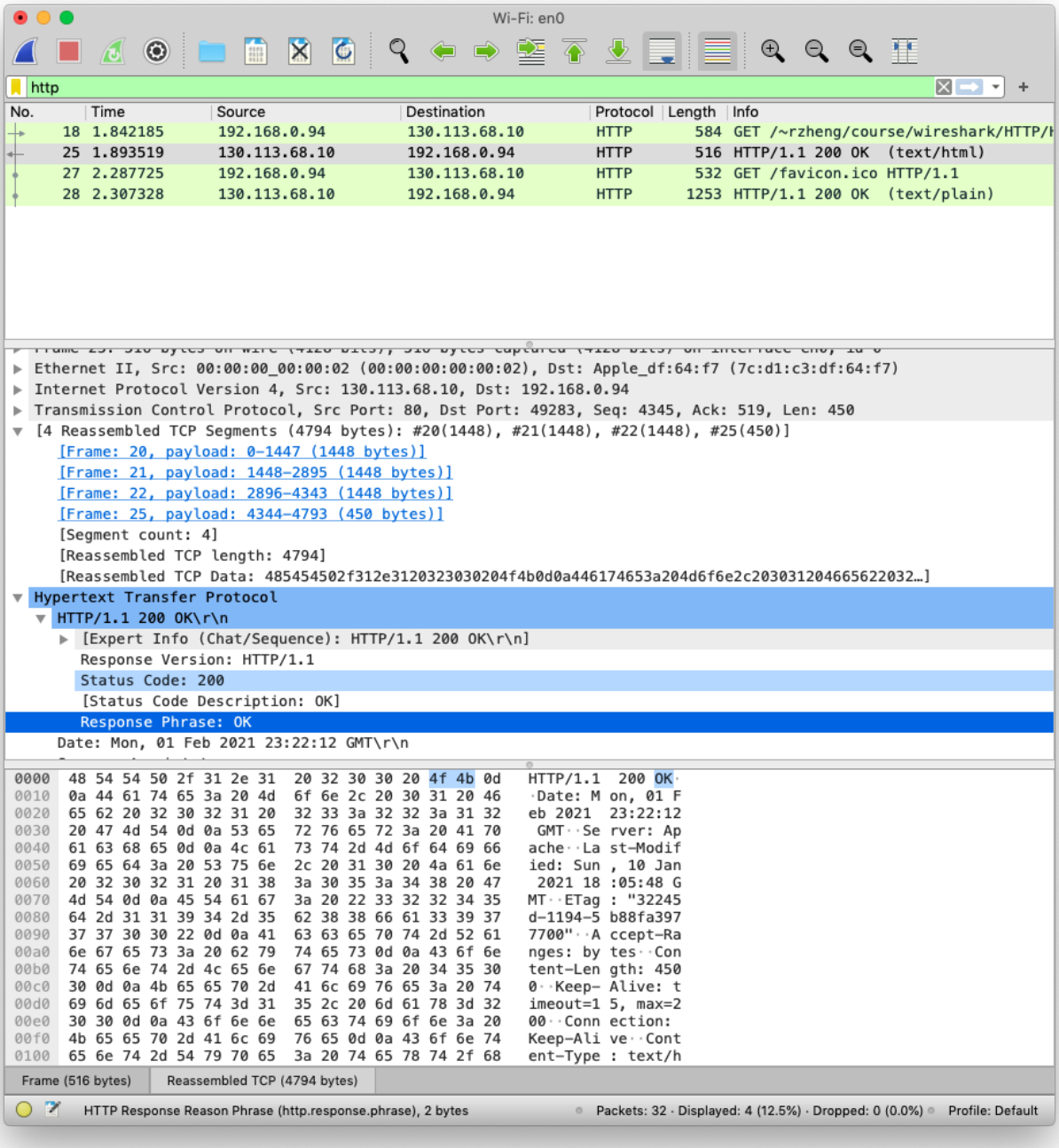
Answer:
In the trace, Packet #25 contains the *status code* and *status response phrase* that is associated to the HTTP GET request that is sent by my browser. In Packet #25, the first Frame, Frame 20, contains the *status code* and *status response phrase*.
This can be seen in the screenshot below.



Answer 13: The text highlighted in light-blue at the top of the Wireshark application, in the "Packet-listing" window contains brief information about the Packet, including it's trace number; on the left side. In addition, the "Status Code" and "Response Phrase" are on the right side. The text highlighted in dark-blue in the "Packet-header details" window is the "Status Code" of the HTTP/Response, and just below it, on the next line, is the "Response Phrase". All of this information is also available in the "Hypertext Transfer Protocol" section for the "HTTP/Request" packet, in the "Packet-Header Details" window.

Question #14:
What is the status code and phrase in the response?

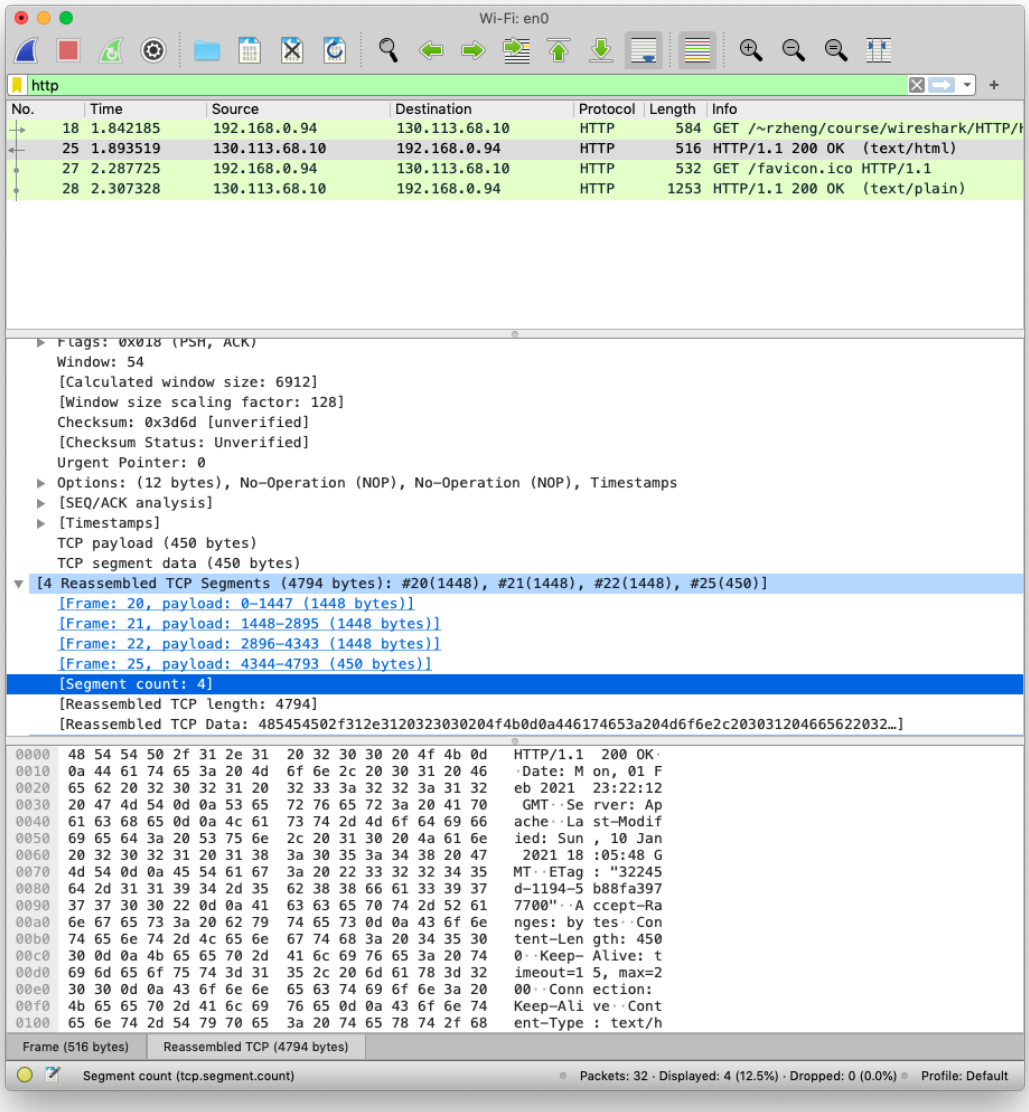
Answer:
In the HTTP/Response packet, the *status code* is “200”.
And, the *status response phrase* is “OK”.
This can be seen in the screenshot below.



Answer 14: The text highlighted in dark-blue is the “Response Phrase”. Above it, the text highlighted in light-blue, is the “Status Code”. All of this information is available in the “Hypertext Transfer Protocol” section for the “HTTP/Request” packet, in the “Packet-Header Details” window.

Question #15:
How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

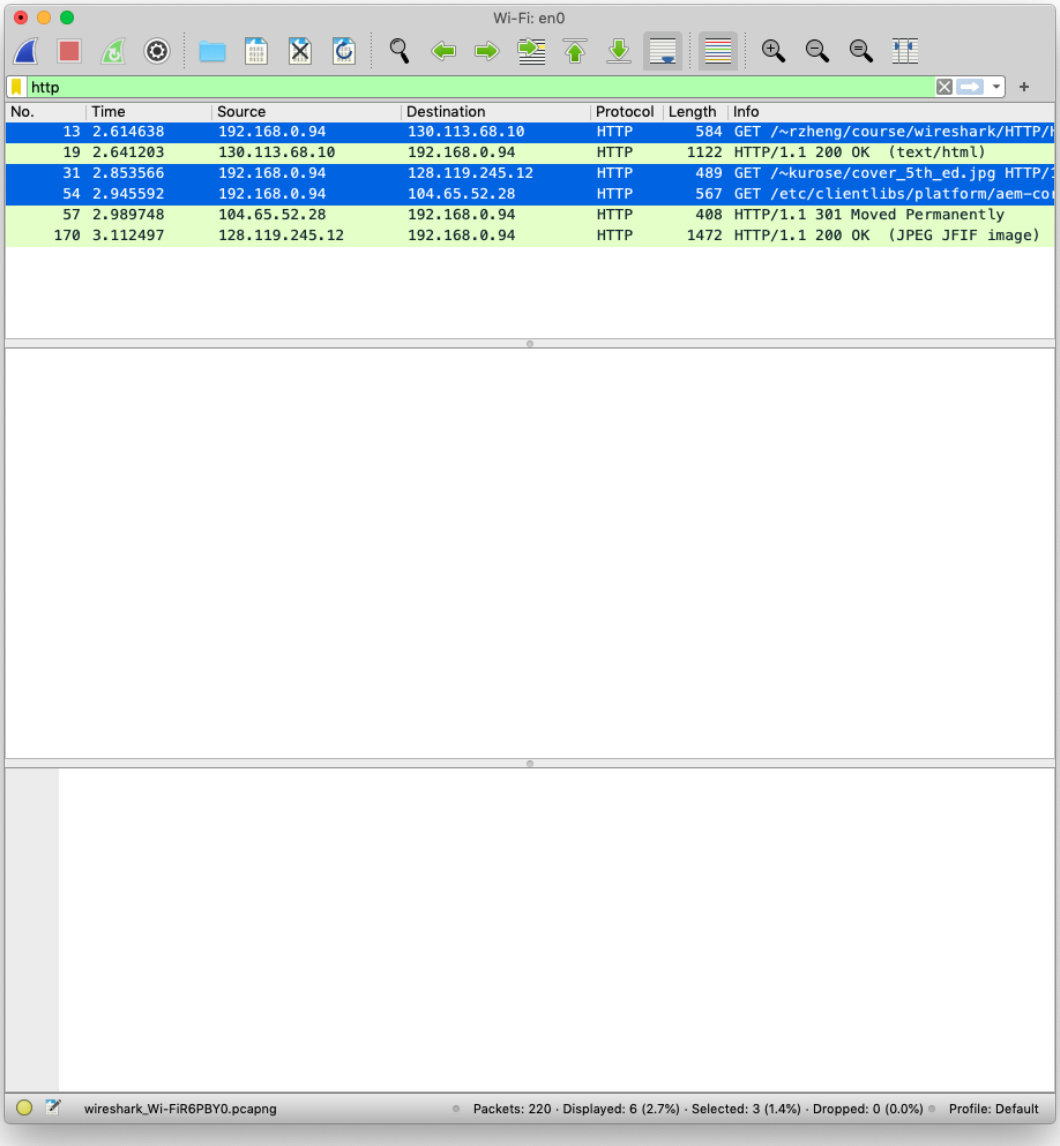
Answer:
In total, there are 4 data-containing TCP segments. These 4 TCP segments were needed to carry the single HTTP response and the text of the *Bill of Rights*. Note: We are ignoring the 'favicon.ico' packet.
This can be seen in the screenshot below.



Answer 15: The text highlighted in dark-blue is the "Segment Count", which states how many TCP segments were sent from the server to my browser. The text highlighted in light-blue is the section where all of this information is found. In addition, it contains the number of TCP segments in its title. All of this information is available in the "...Reassembled TCP Segments..." section for the "HTTP/Request" packet, in the "Packet-Header Details" window.

Question #16:
How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

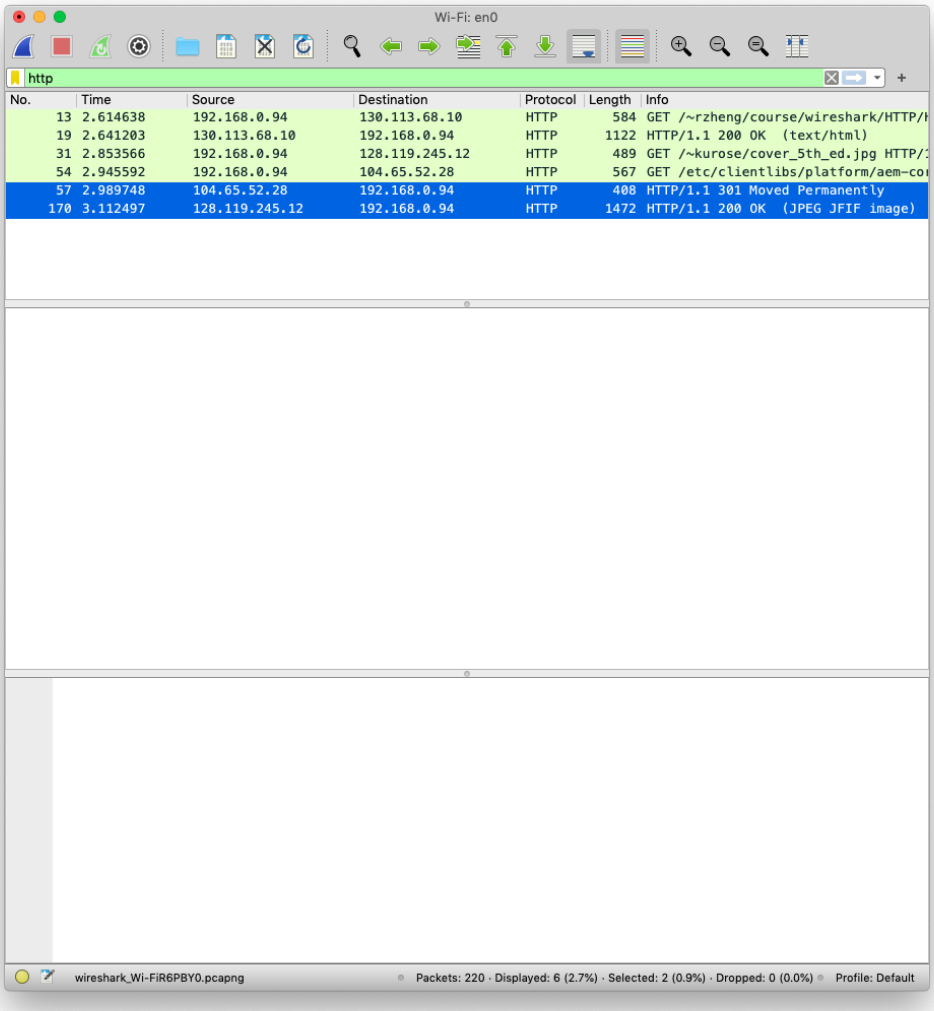
Answer:
My browser sent 3 HTTP GET request messages to 3 different sites/internet addresses. They are:
1) 130.113.68.10 (McMaster's Website)
2) 128.119.245.12 (Kurose's Website)
3) 104.65.52.28   (Pearson's Website)
This can be seen in the screenshot below.



Answer 16: The text fields highlighted in dark-blue, at the top, are the HTTP GET packet requests. This is what my browser sends to the servers. All of this information can be found in the "Packet-listing" window that is at the top of the Wireshark application.

Question #17:
Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel Explain.

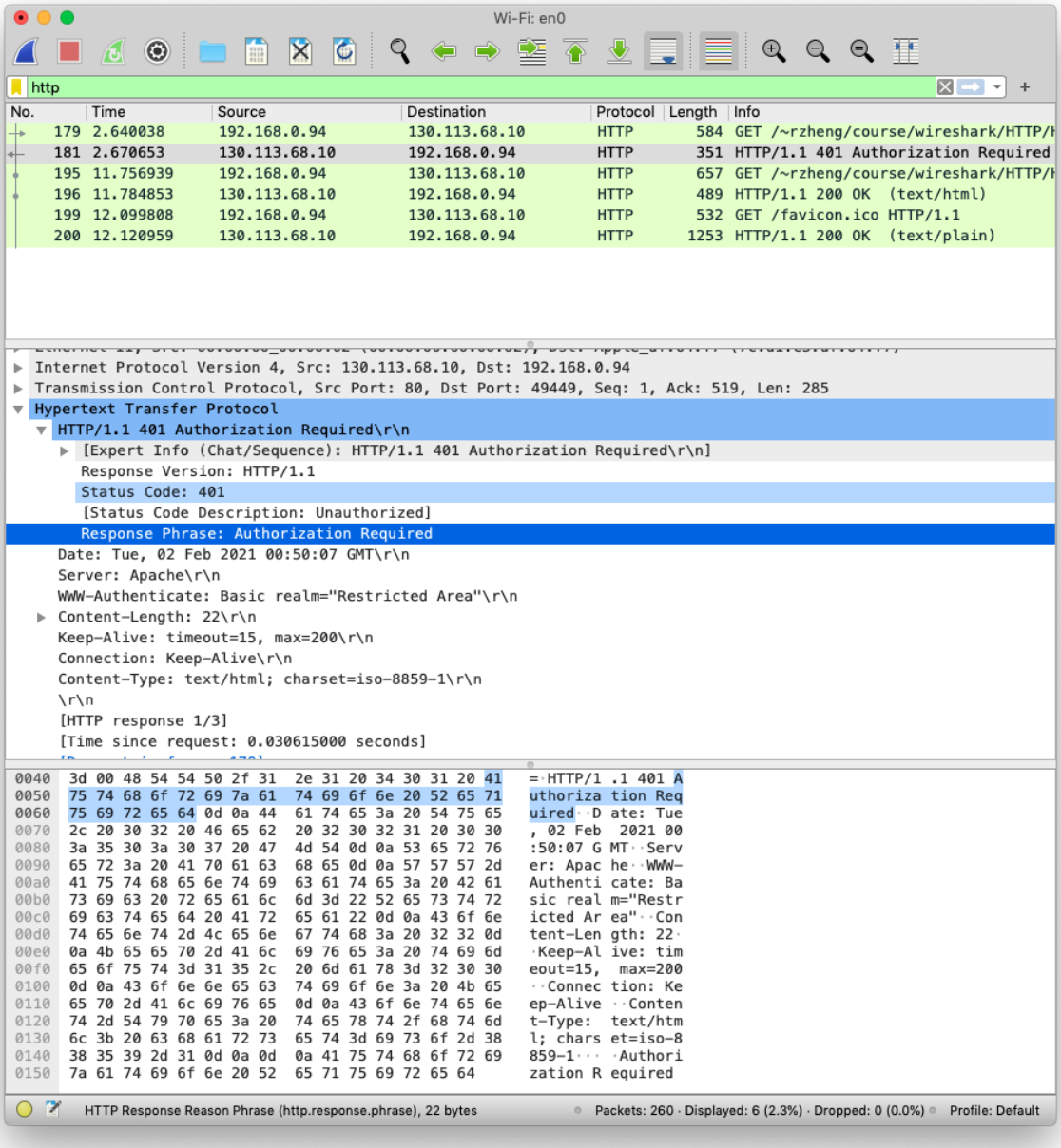
Answer:
My browser downloaded the two images serially, and NOT in parallel. I can tell because the HTTP/Response packets that correspond to the images have a different packet number and received time in the "Packet-listing" window. The differences in their respective values is significant, which indicates that the images were downloaded serially.
This can be seen in the screenshot below.



Answer 17: The text fields highlighted in dark-blue at the top of the program are the HTTP/Response packets for the images. As you can see, the packet number and time are listed on the left side for both packets, and their values are different. Thus, they were downloaded serially. All of this information is in the "Packet-listing" window at the top of the Wireshark application.

Question #18:
What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

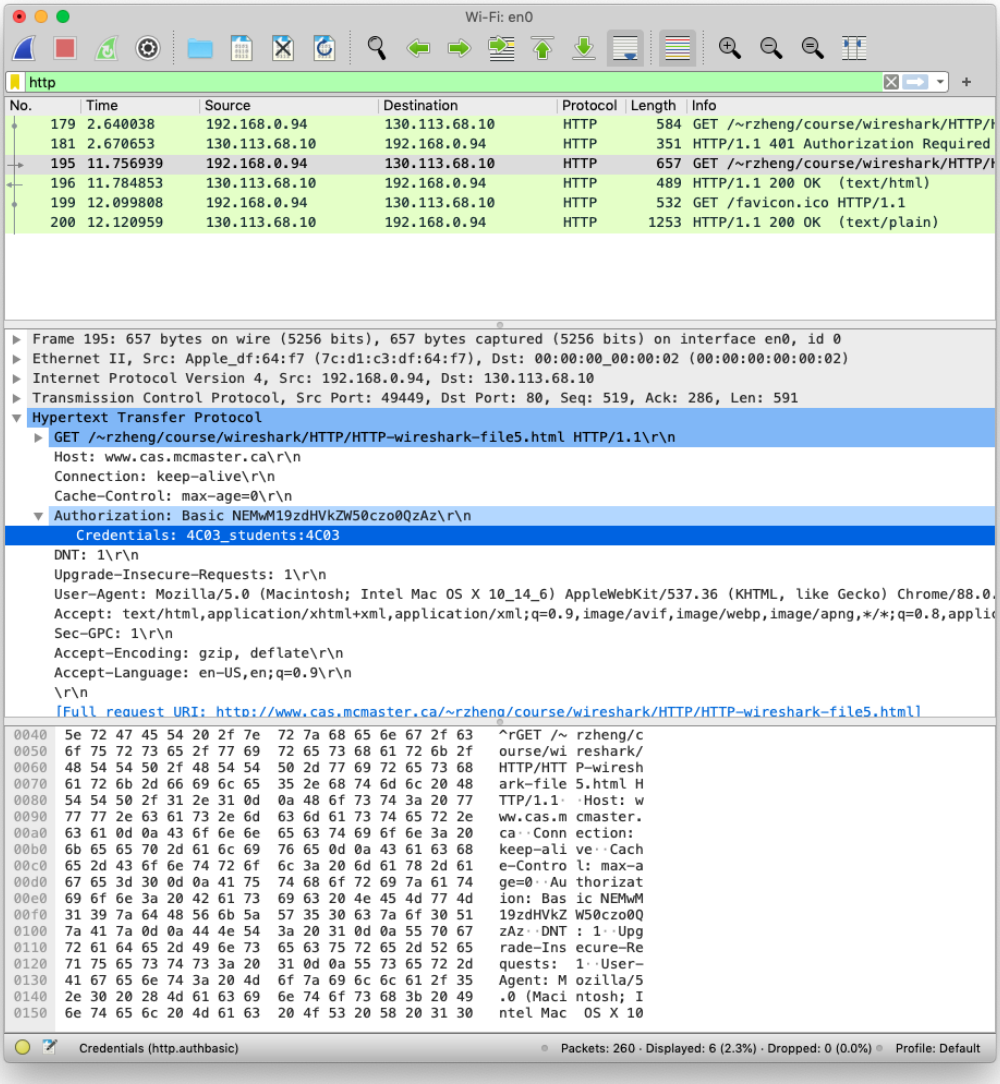
Answer:
The server's *response phrase* to my initial HTTP GET message from my browser is, "Authorization Required", with a *status code* of 401 This can be seen in the screenshot below.



Answer 18: The text field highlighted in dark-blue is the server's "Response Phrase" to my browser's initial HTTP GET, and the text field above it, highlighted in light-blue, is the "Status Code". All of this information is available in the "Hypertext Transfer Protocol" section for the "HTTP/Request" packet, in the "Packet-Header Details" window.

Question #19:
When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

Answer:
When my browser sends the HTTP GET message for the second time to the server, the new field in the HTTP GET message is "Authorization". This field contains "Credentials", which holds the username and password to login.
This can be seen in the screenshot below.



Answer 19: The text field highlighted in dark-blue is the "Credentials" field and holds the username and password that is used to authenticate accss to the server. Above this, the field "Authorization", highlighted in light-blue, is a new field that is added when your browser sends login information to the destination server. All of this information is available in the "Hypertext Transfer Protocol" section for the "HTTP GET" packet, in the "Packet-Header Details" window.