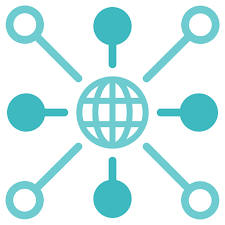
Addis Ababa Institute of Technology







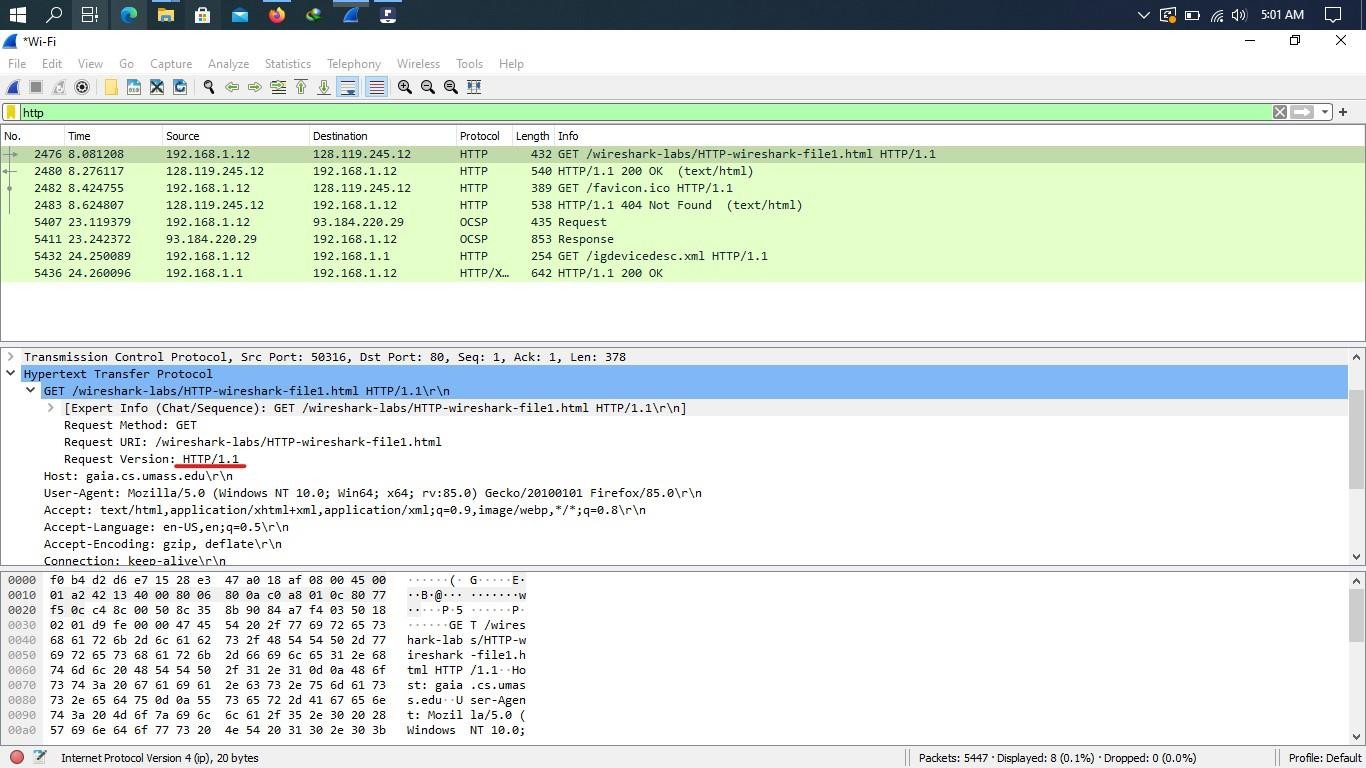
Chapter 2: Wire Shark HTTP Lab Report

What to hand in:

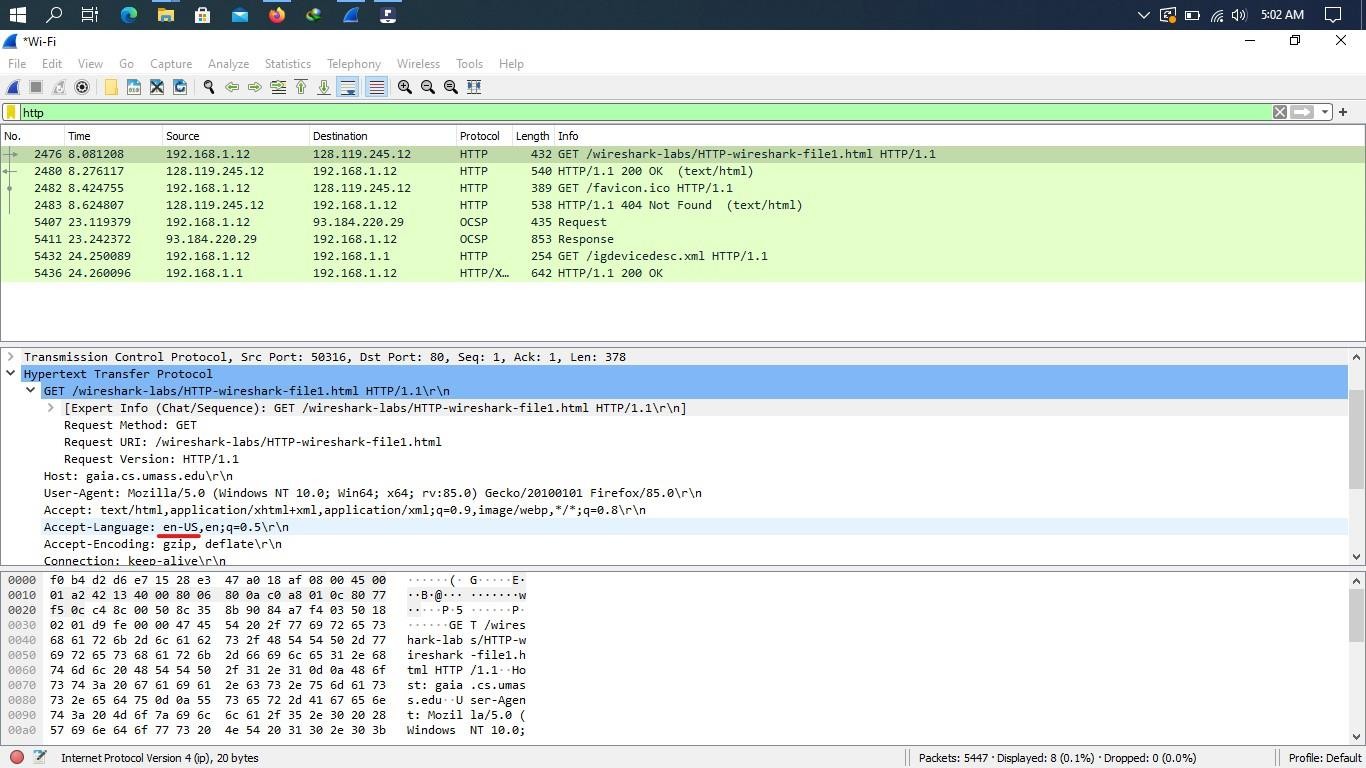
By looking at the information in the HTTP GET and response messages, answer the following questions. When answering the following questions, you should print out the GET and response messages (see the introductory Wireshark lab for an explanation of how to do this) and indicate where in the message you’ve found the information that answers the following questions.

When you hand in your assignment, annotate the output so that it’s clear where in the output you’re getting the information for your answer (e.g., for our classes, we ask that students markup paper copies with a pen, or annotate electronic copies with text in a colored font).

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



1. What languages (if any) does your browser indicate that it can accept to the server?
   * The language the browser is using is en-US.

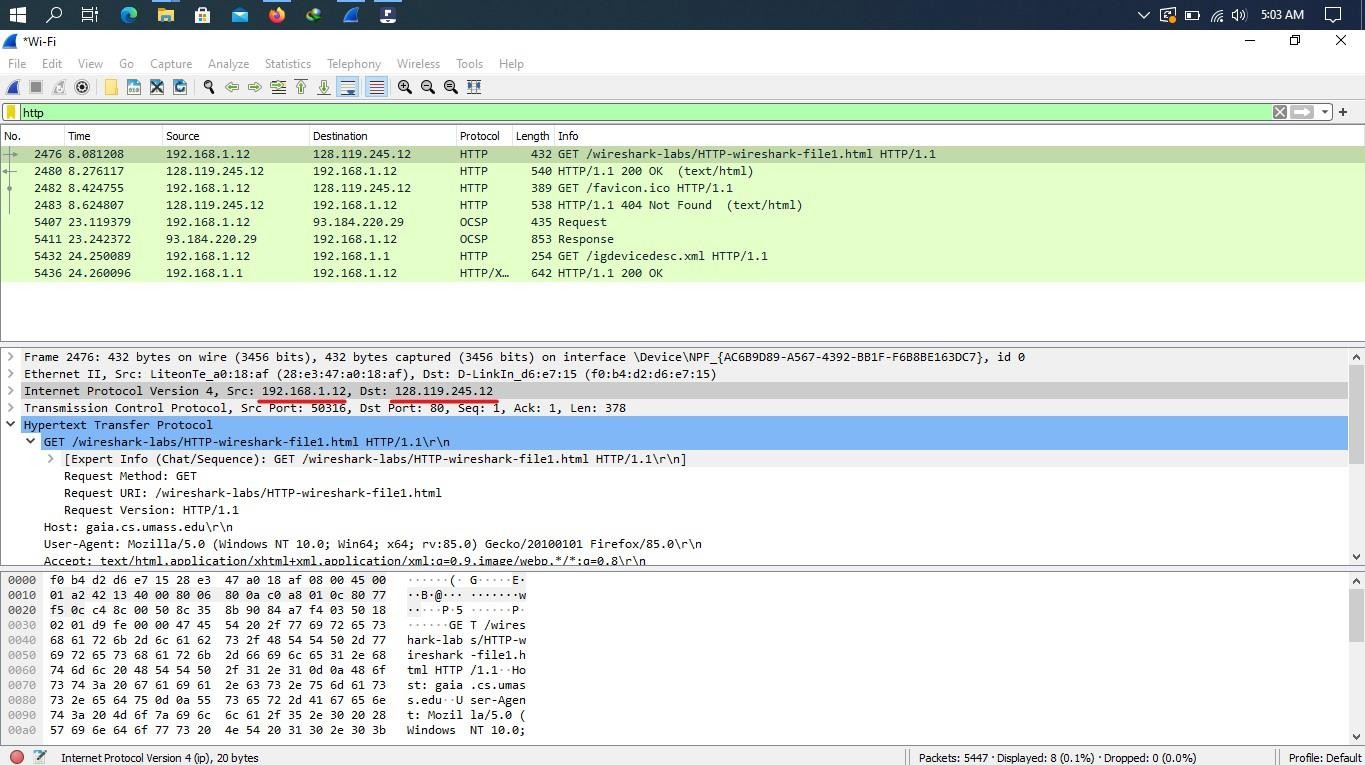


1. What is the IP address of your computer? Of the gaia.cs.umass.edu server?
   * The Internet address of the gaia.cs.umass.edu is:

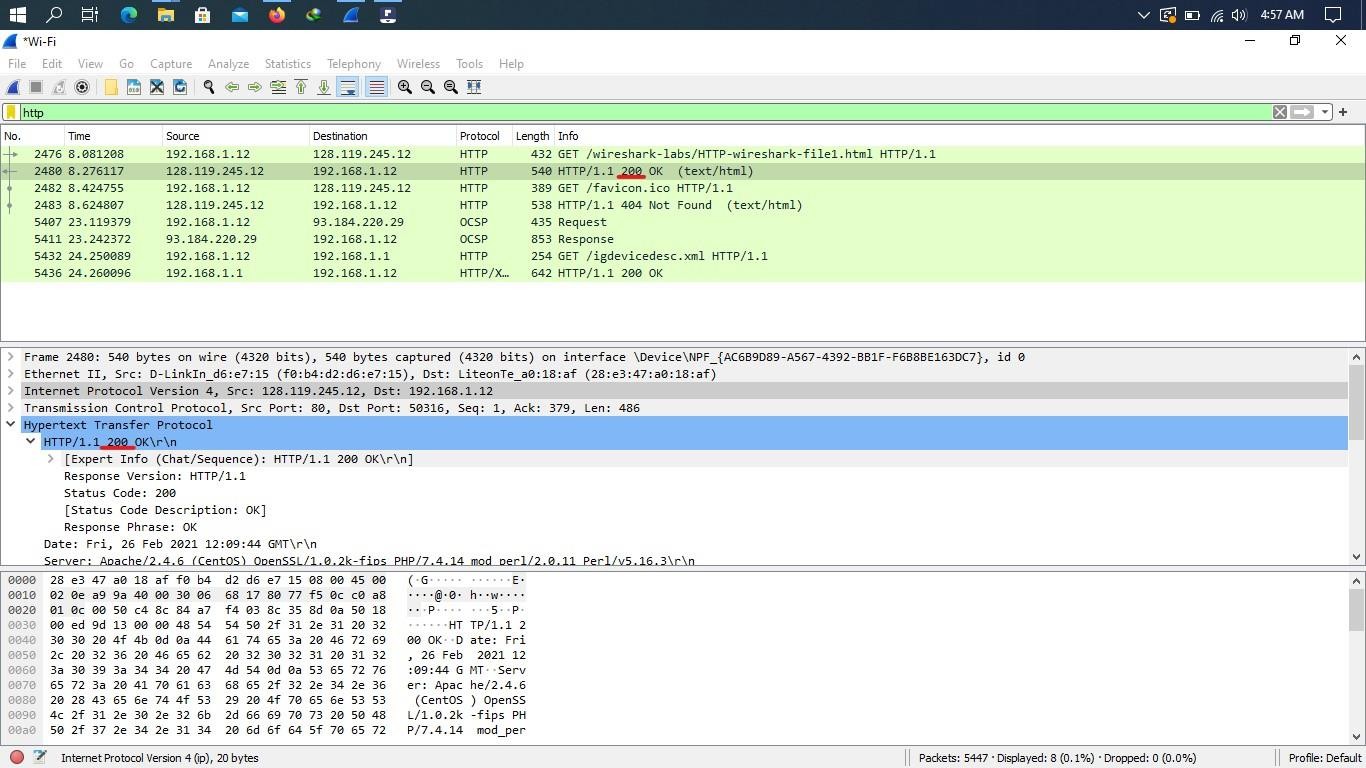
128.119.245.12

* + The Computer Address used for this Assignment is:

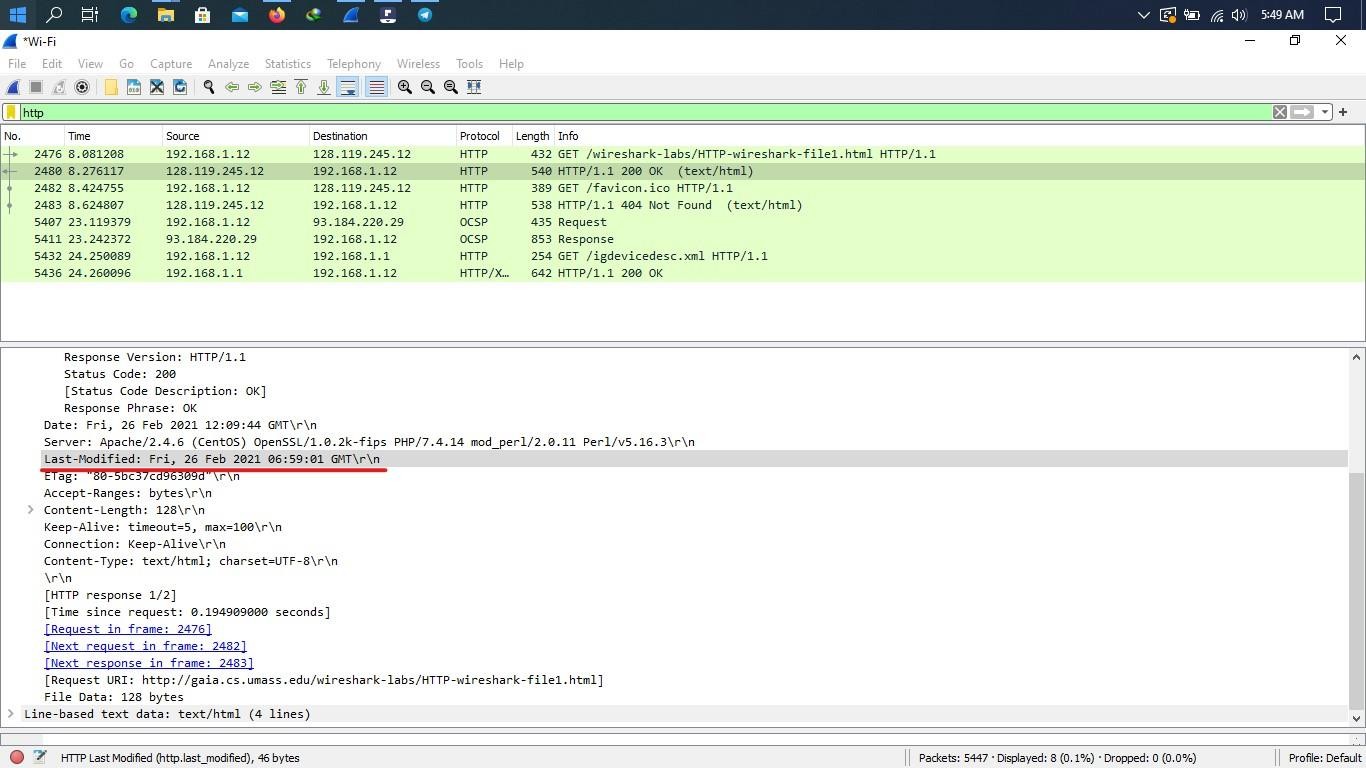
192.168.1.12



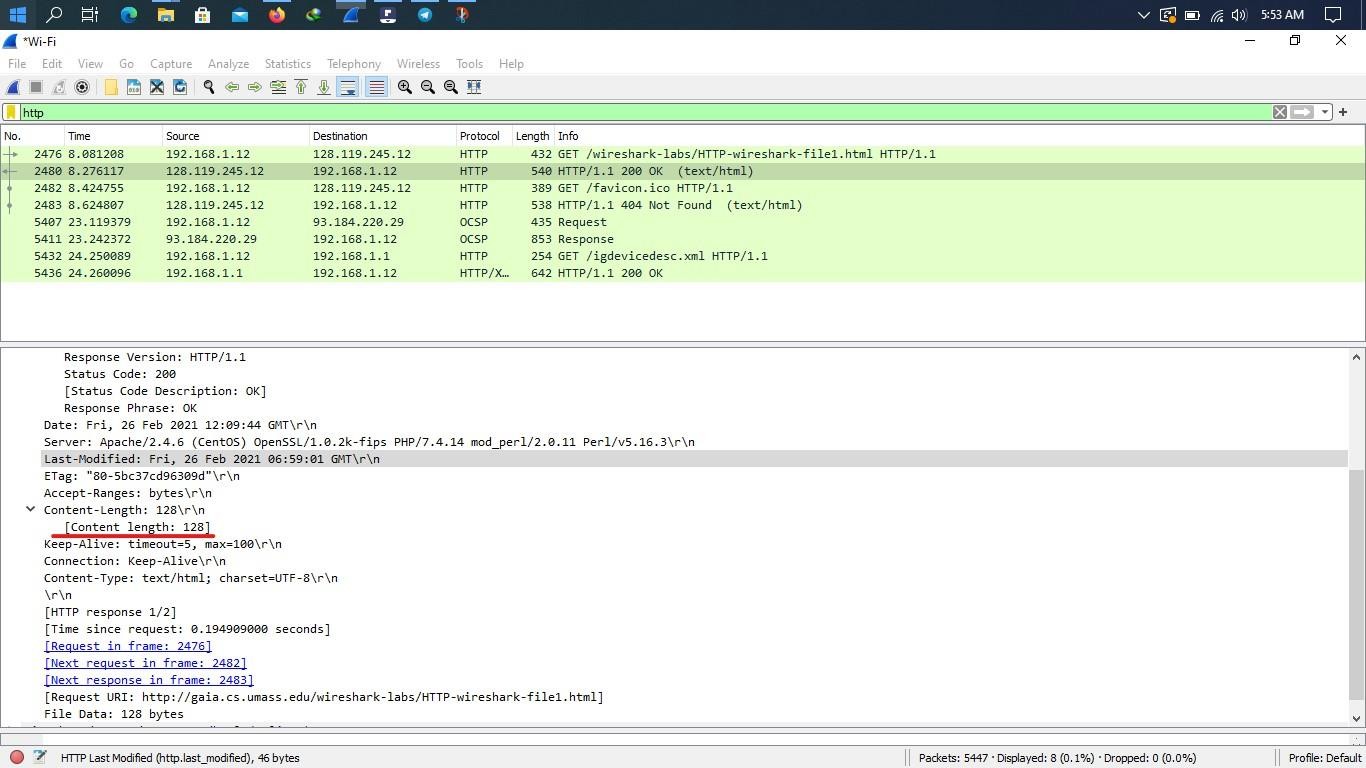
1. What is the status code returned from the server to your browser?
   * The status code returned is 200.

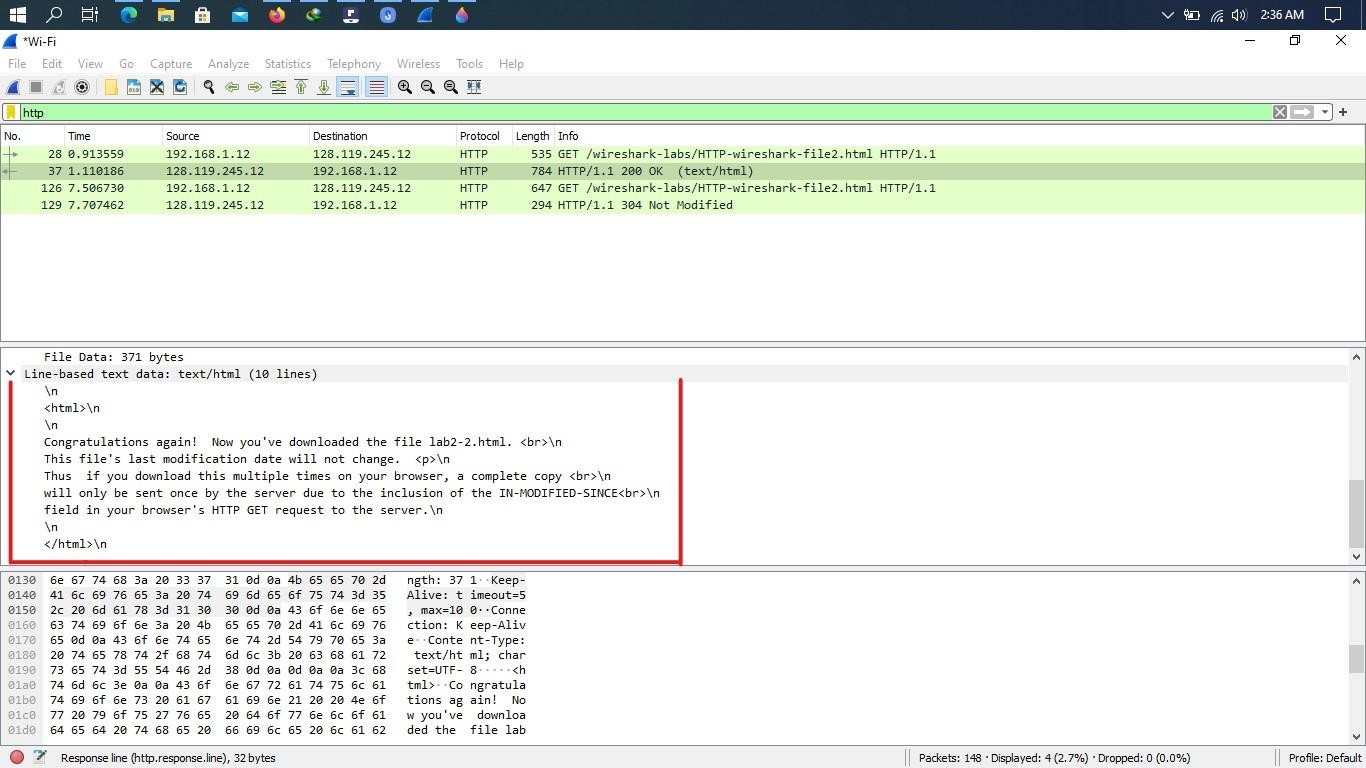


1. When was the HTML file that you are retrieving last modified at the server?
   * Last modified on Fri, 26 Feb 2021, 06:59:01 GMT



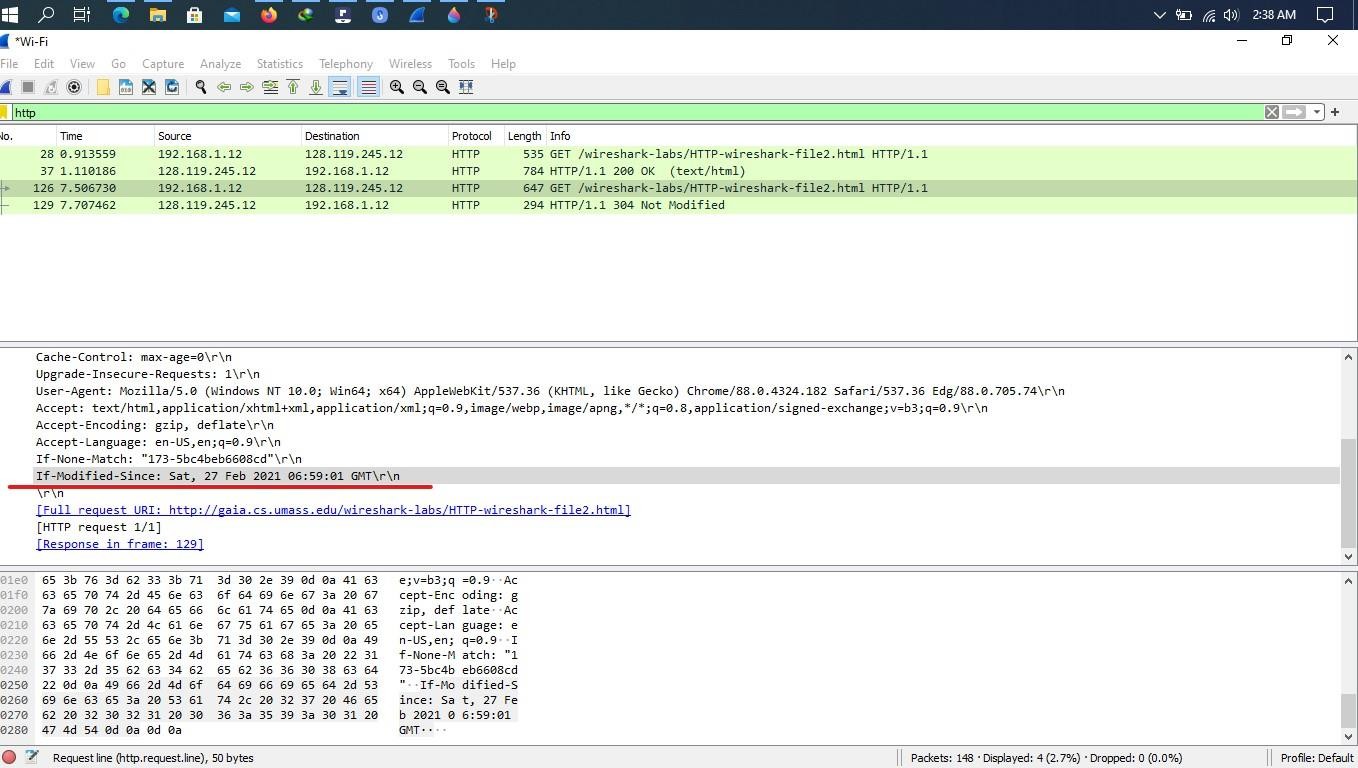
1. How many bytes of content are being returned to your browser?
   * 128 bytes of content length are being returned.



1. 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.
   * No. The raw data appears to match up exactly with what is shown in the packet-listing window.
2. 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.
3. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
   *  Yes it did, we can tell buy the line-based data: text/html which is 10 lines of contents.
4. 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?

* + If-Modified-Since: Sat, 27 2021, 06:59:01 GMT

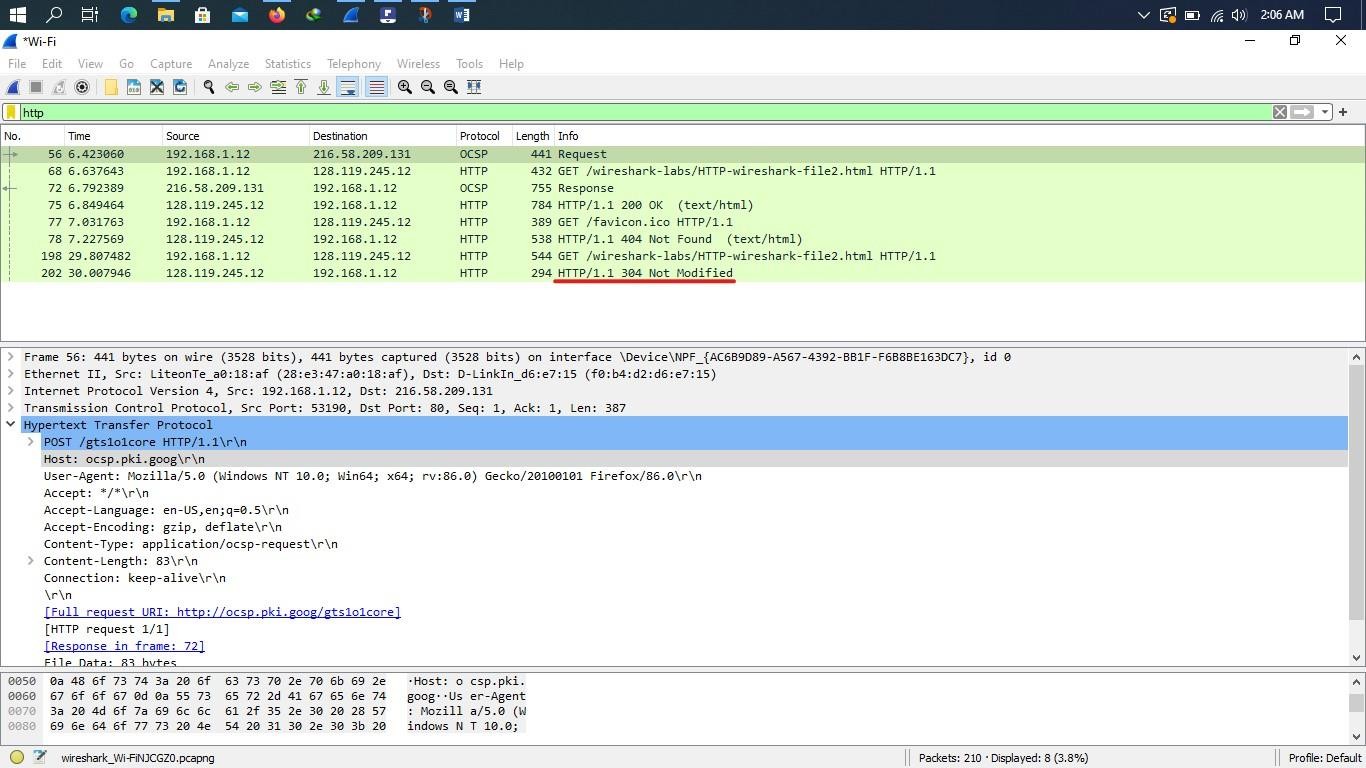


1. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file?

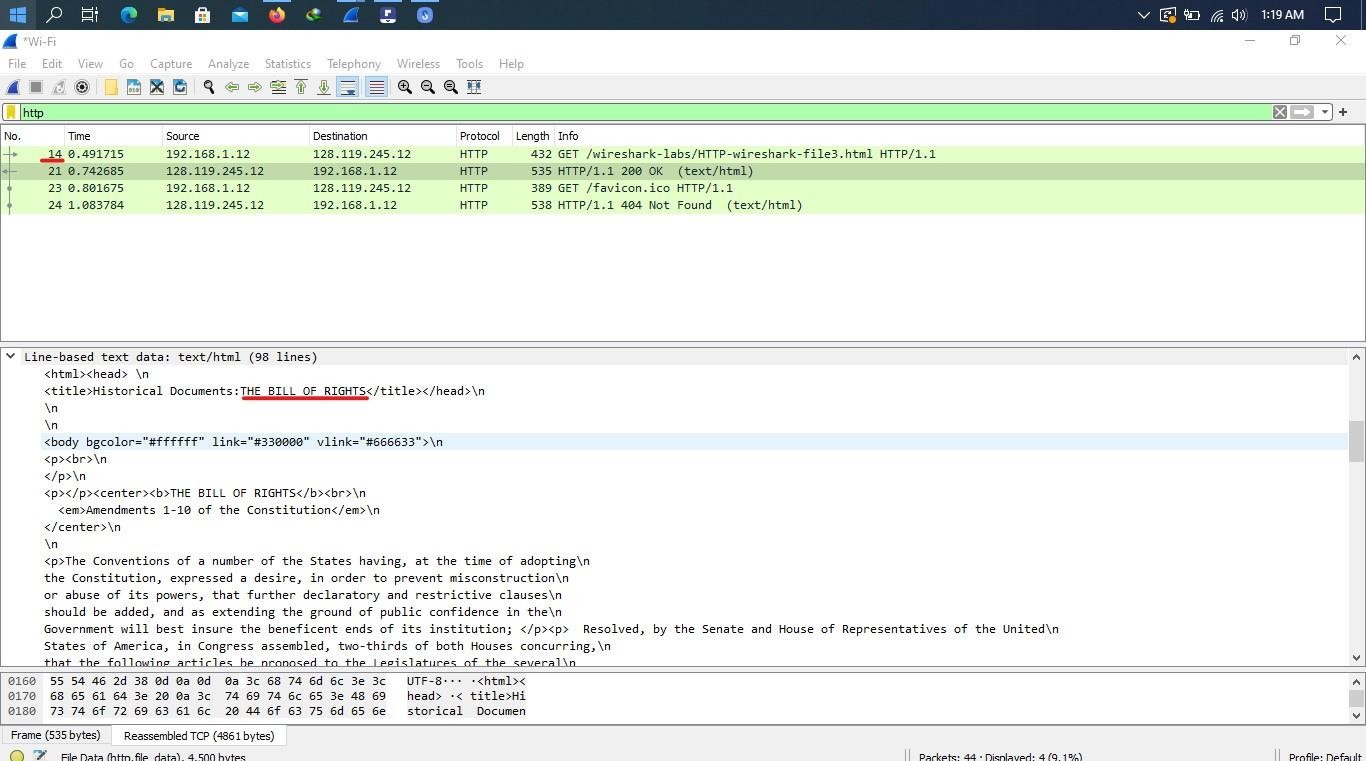
Explain.

* + - 304 not modified.

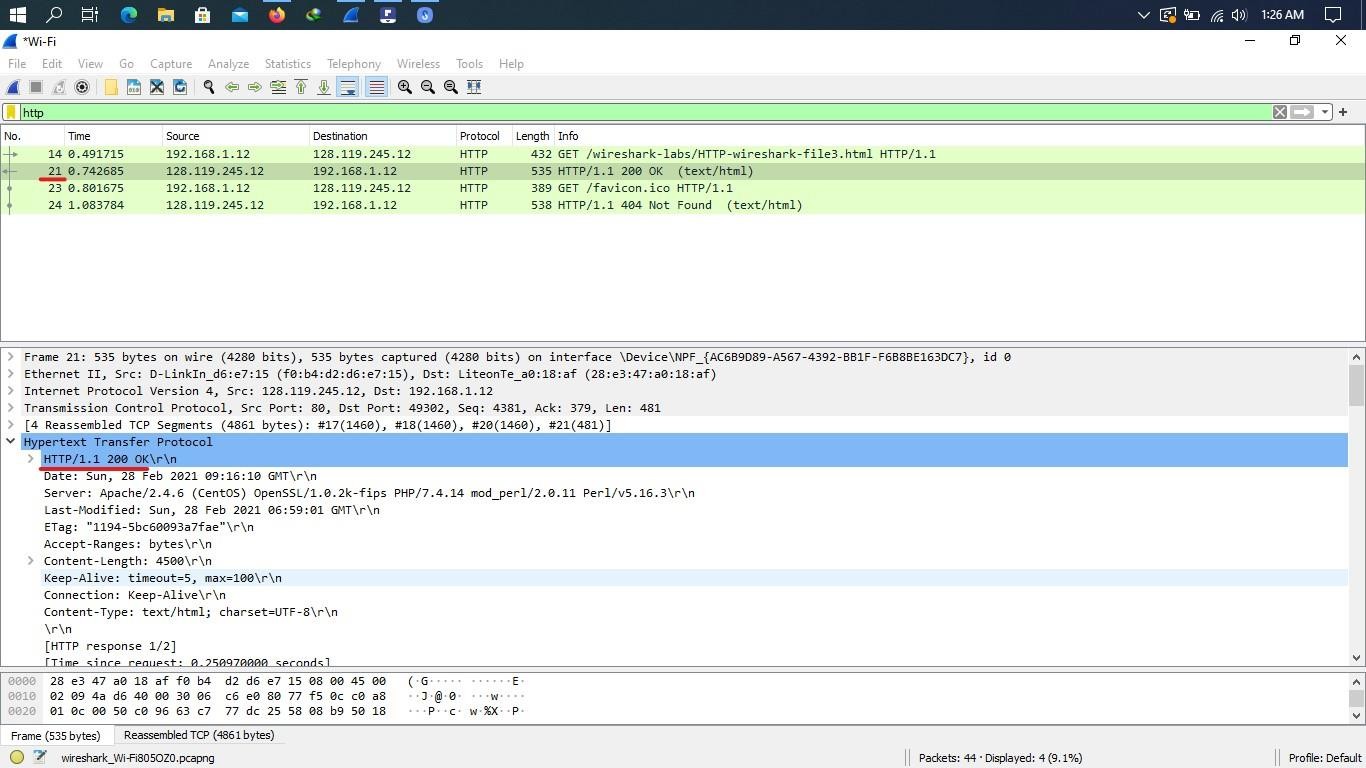
- The server did not response because the content hasn’t been updated recently.



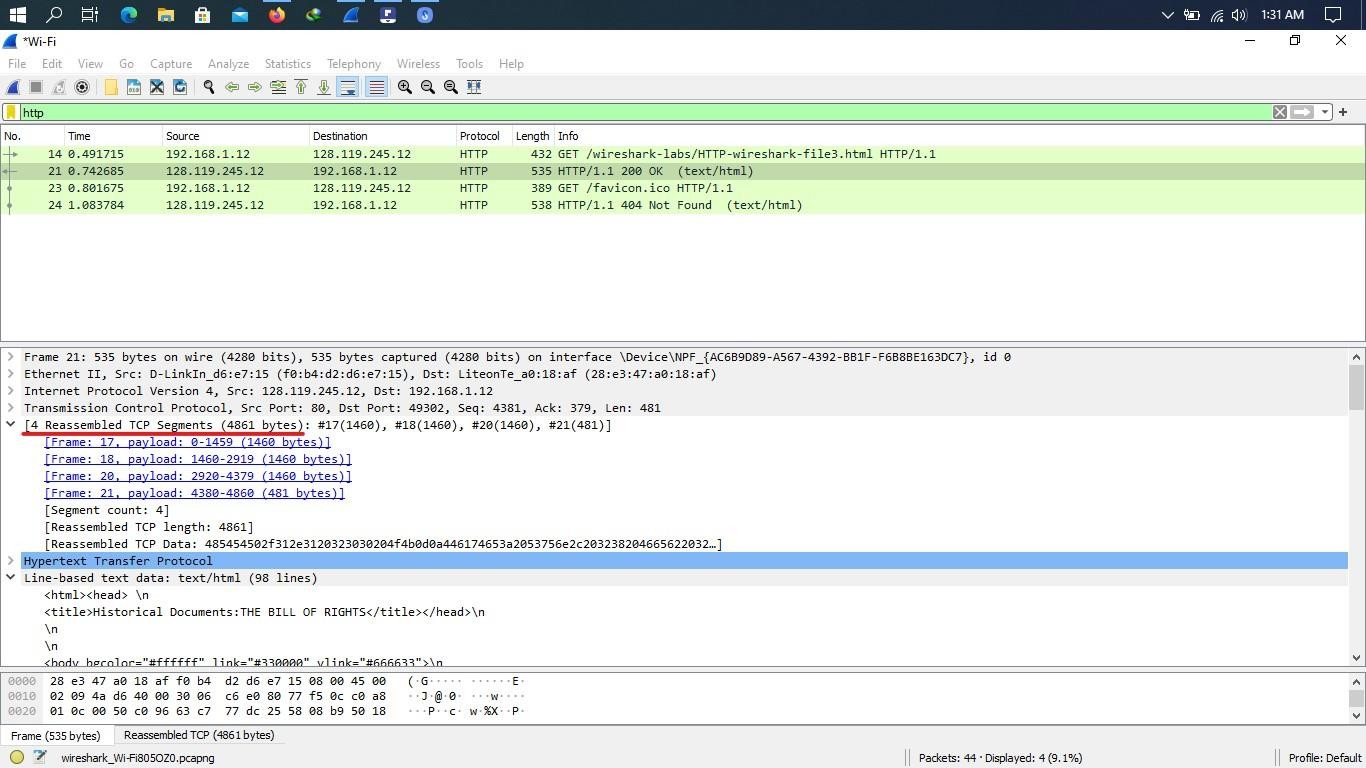
1. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?
   * Just one Get request messages except favicon.ico Packet number 14 contains the Bill of rights.



1. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?
   * As seen in the screen shot below packet number 21.



1. What is the status code and phrase in the response?
   * As seen in the above screen shot Http/1.1 200 OK.
2. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?
   * There are 4 TCP Segments.

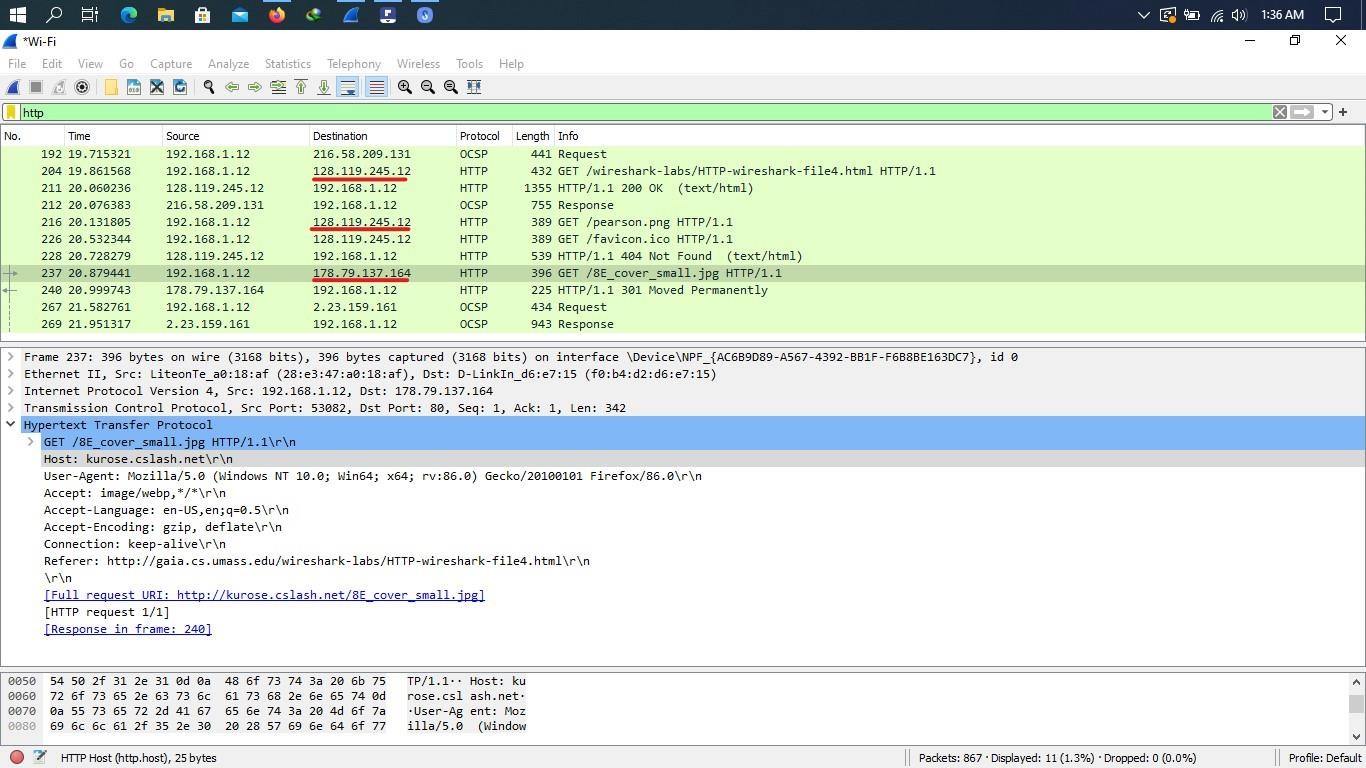


1. How many HTTP GET request messages did your browser send? To which internet addresses were these GET requests sent?
   * The browser sent 3 HTTP GET request messages. The GET request was sent to:

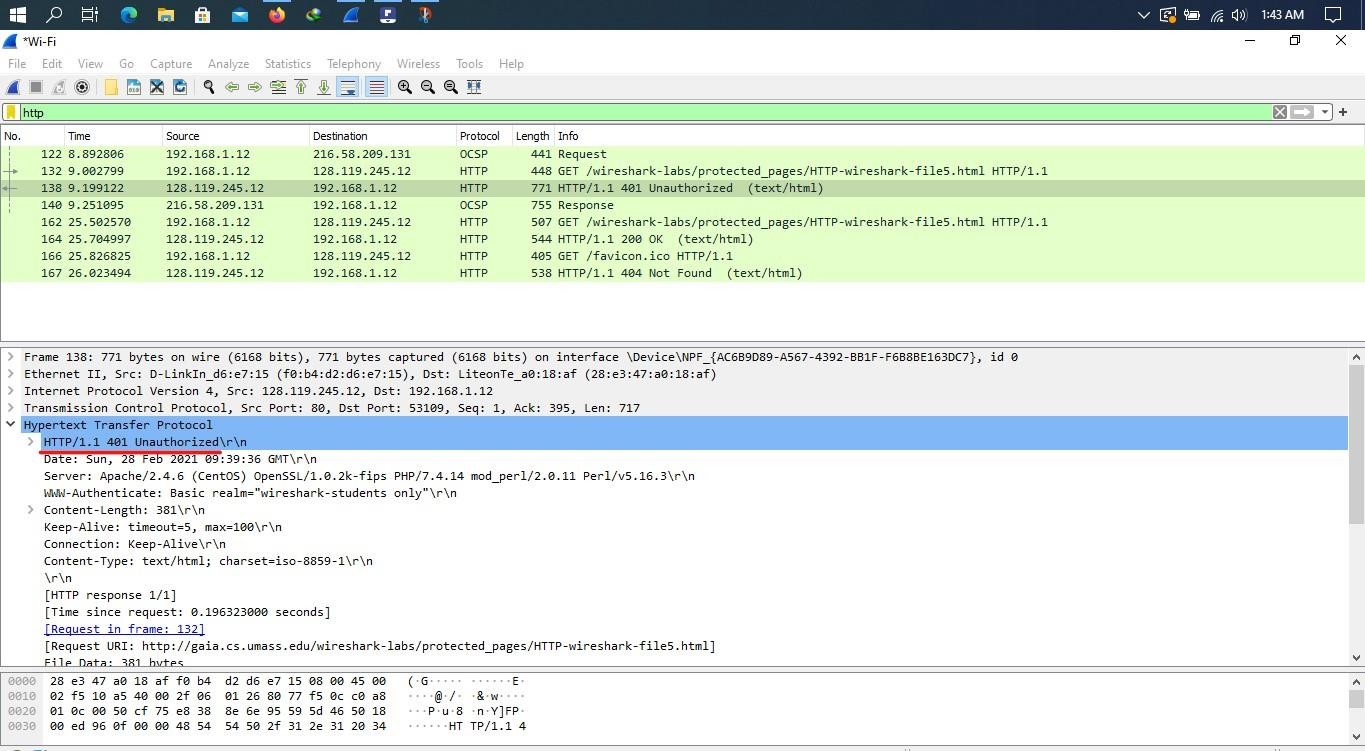
- 128.119.245.12 – wireshark-labs

- 128.119.245.12 – pearson.png

- 178.79.137.164 – 8E\_cover\_small.jpg

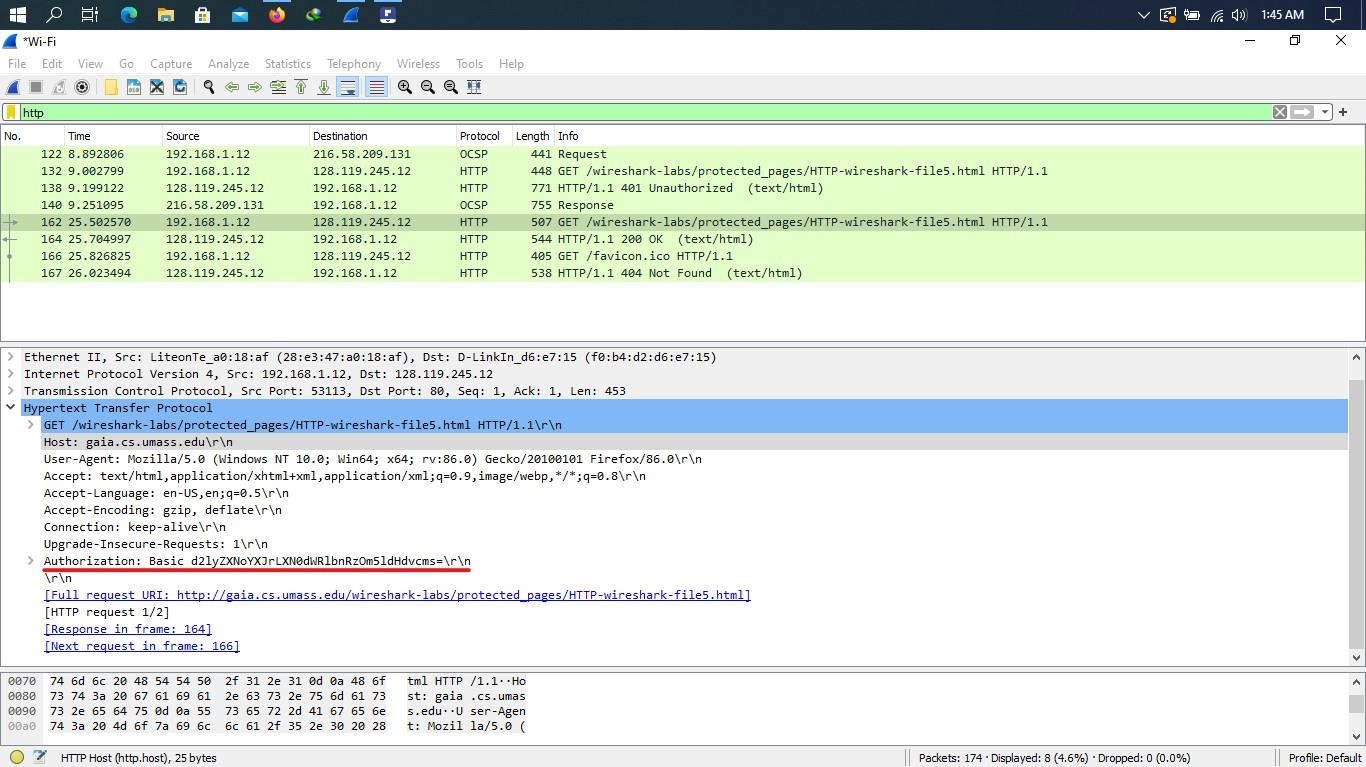


1. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.
   * Based on the timestamps, it appears the images were downloaded serially. The first image was requested and sent before the second image was requested by the browser.
2. What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser?



* + Status code - 401 Phrase – Unauthorized.

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



* + Authorization:

Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms