THE UNIVERSITY OF DODOMA



COLLEGE OF INFORMATICS AND VIRTUAL EDUCATION
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (CSE)
WIRESHARK LABS PRESENTATION.
PROGRAM: BSc-CNISE
COURSE: IA 311

GROUP PARTICIPANTS

NAMES	REGISTRATION NUMBER
HENRY SELEMAN	T22-03-00295
JIMSON MAHENGE	T22-03-08372
PUDENCIANA KIYEGA	T22-03-11584
PETRO MOHERE	T22-03-02116
GEORGE KALAMU	T22-03-08400

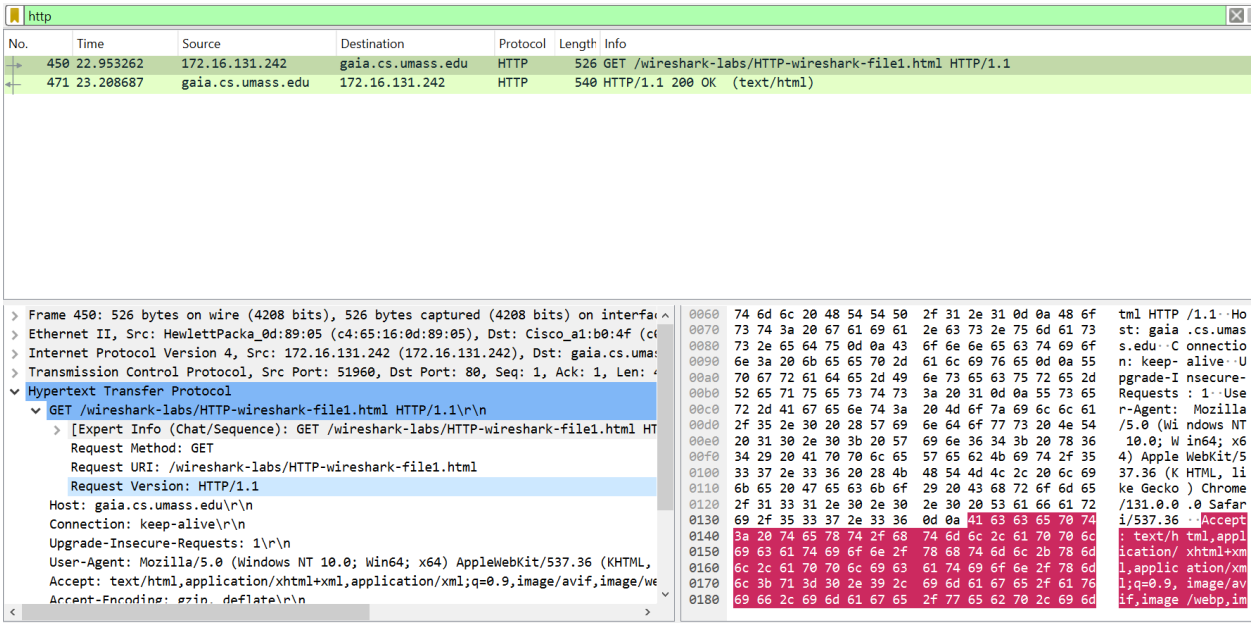
LAB 2.

➢ The Basic HTTP GET/response interaction

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

   Answer:

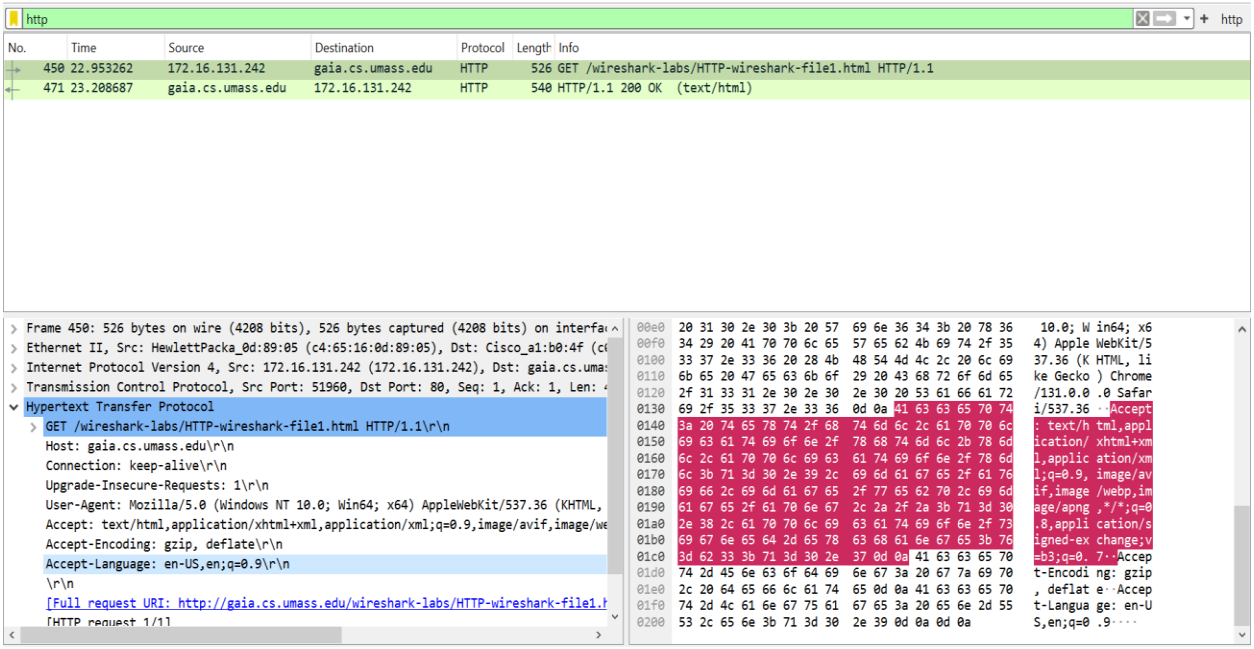
   My browser running HTTP version **1.1**, Version of HTTP server running is **1.1** .



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

   Answer:

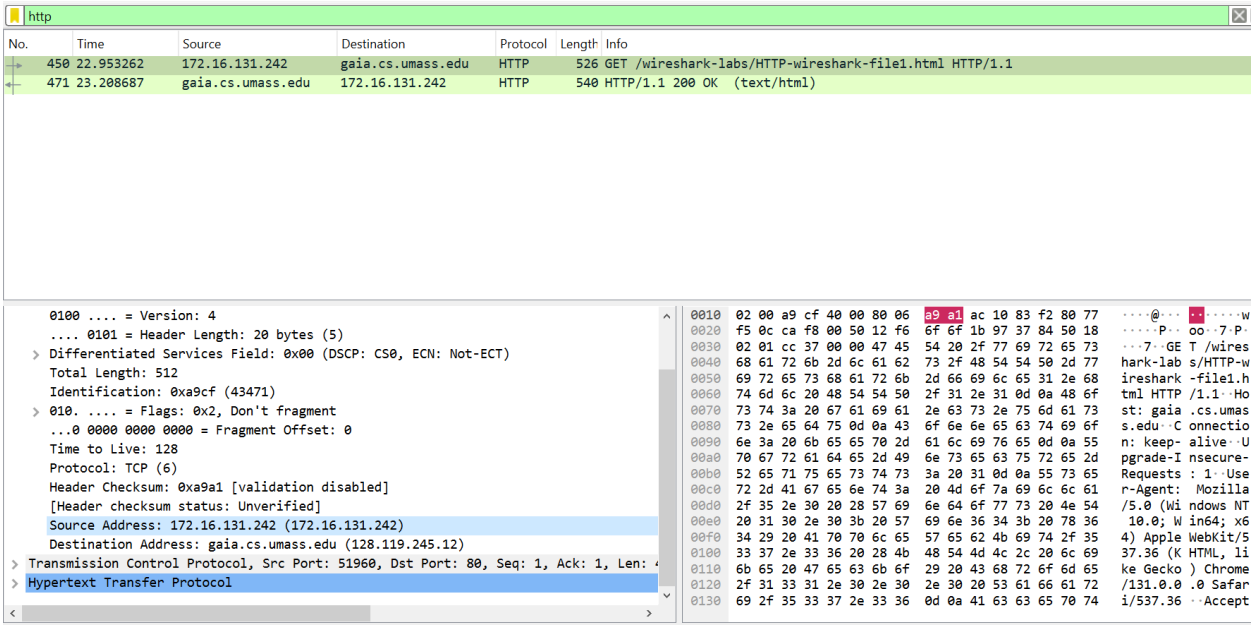
   Accept language that browser indicate is **en-US,en;q=0.9\r\n**



3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

Answer:

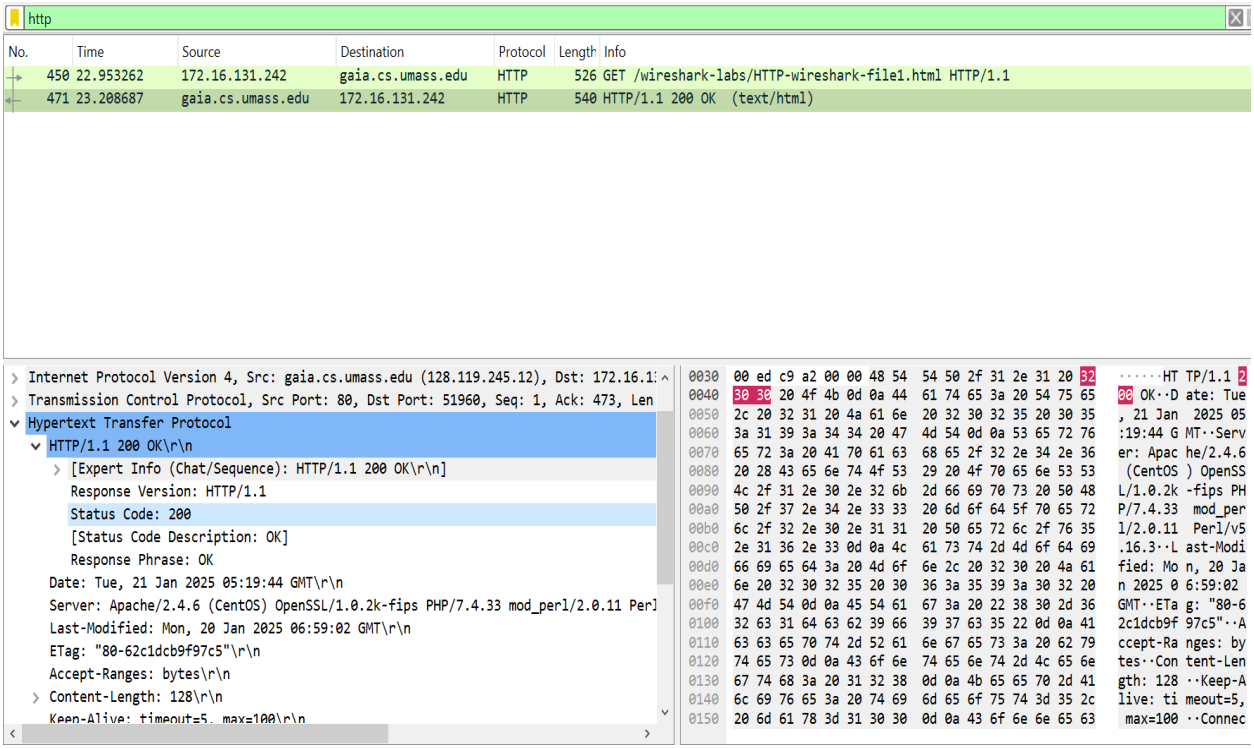
IP address of the computer is the source address that is **172.16.131.242** and the IP address of gaia.cs.umass.edu server is the destination address that is **128.119.245.12.**



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

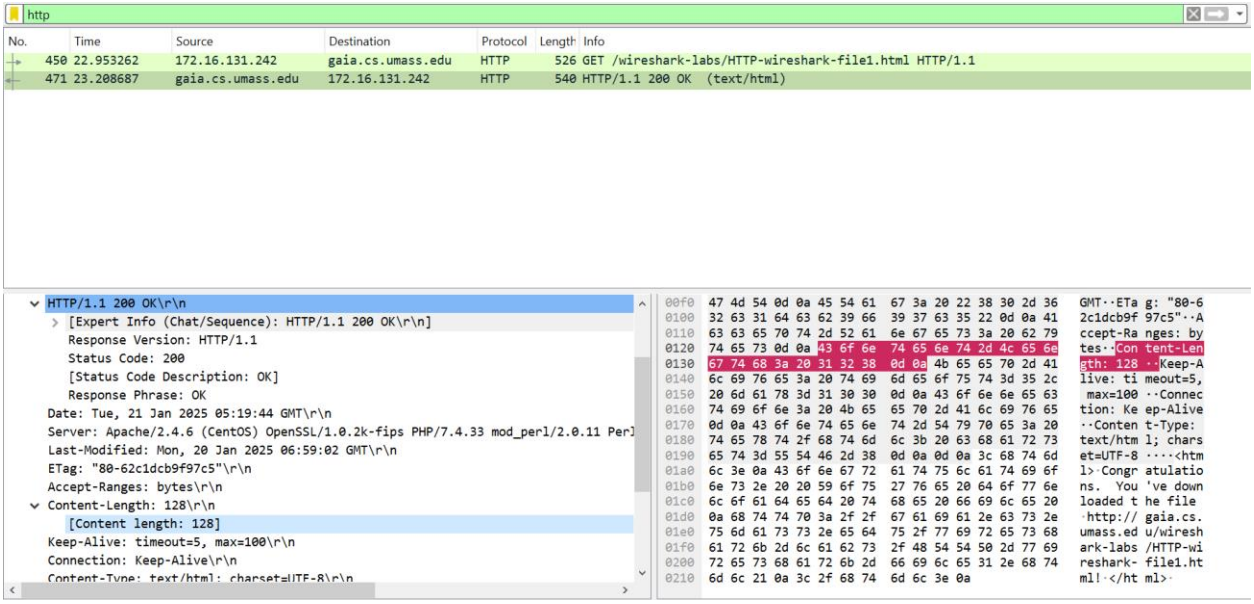
Answer:

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



5. When was the HTML file that you are retrieving last modified at the server?
   Answer:
   From the figure four above, **The Last-Modified : Monday, 20 Jan 2025 06:59:02 GMT\r\n.**

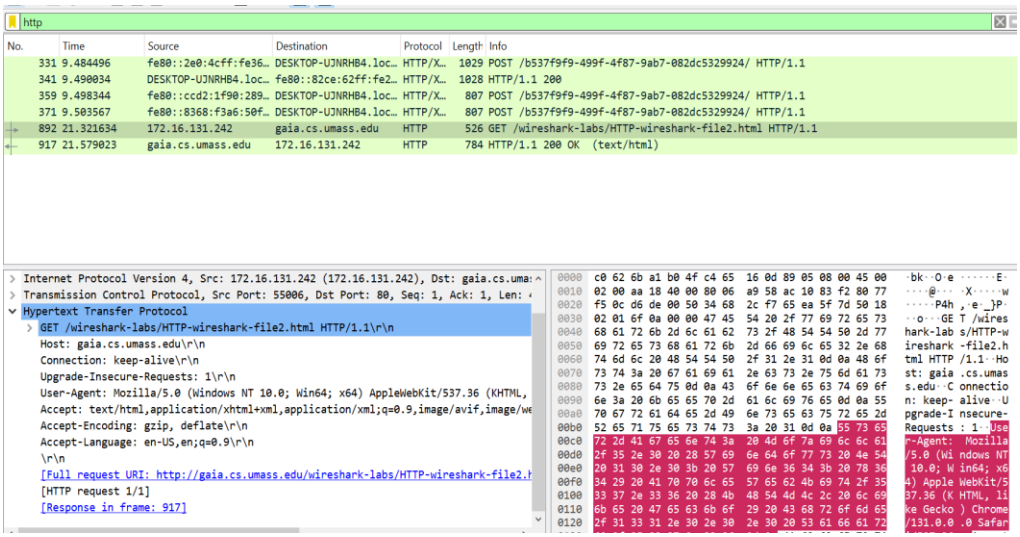
6. How many bytes of content are being returned to your browser?
   Answer:
   The content-length is **128 bytes**.



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, All headers are displayed**.**

➢ The HTTP CONDITIONAL GET/response interaction

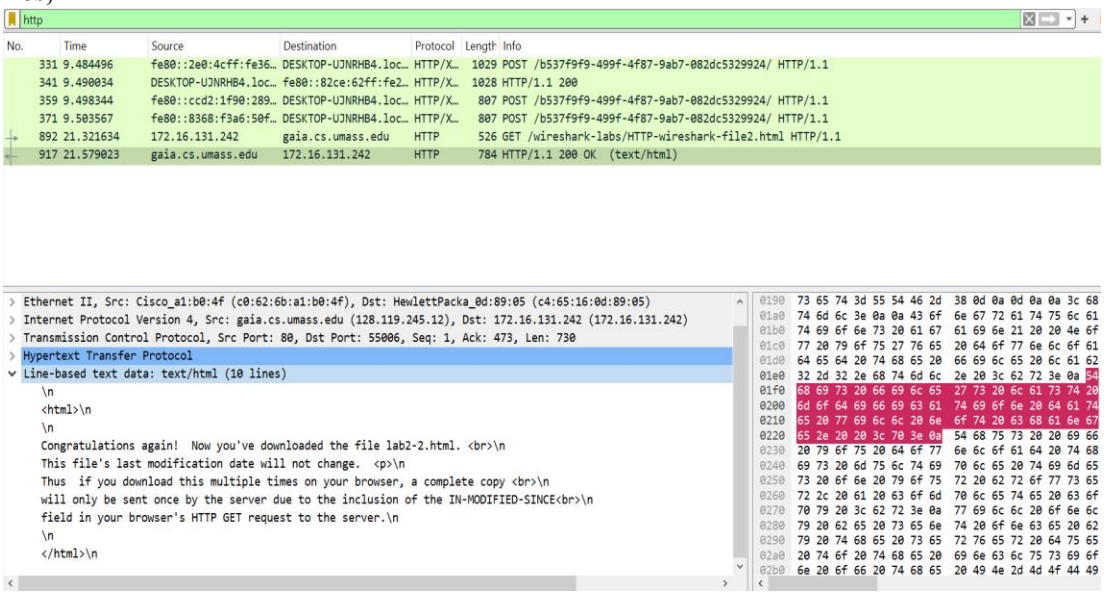
1. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?
   Answer:
   I do not see an IF-MODIFIED-SINCE.



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

   Answer:

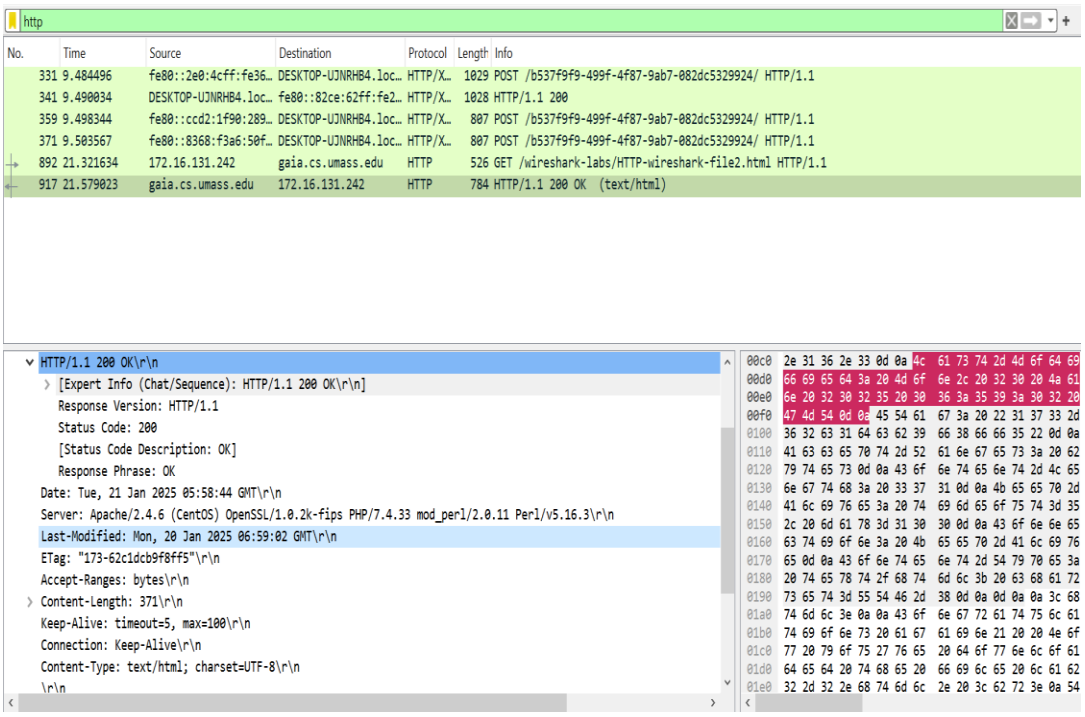
   Yes, the server return the content as seen in url as HTML file.



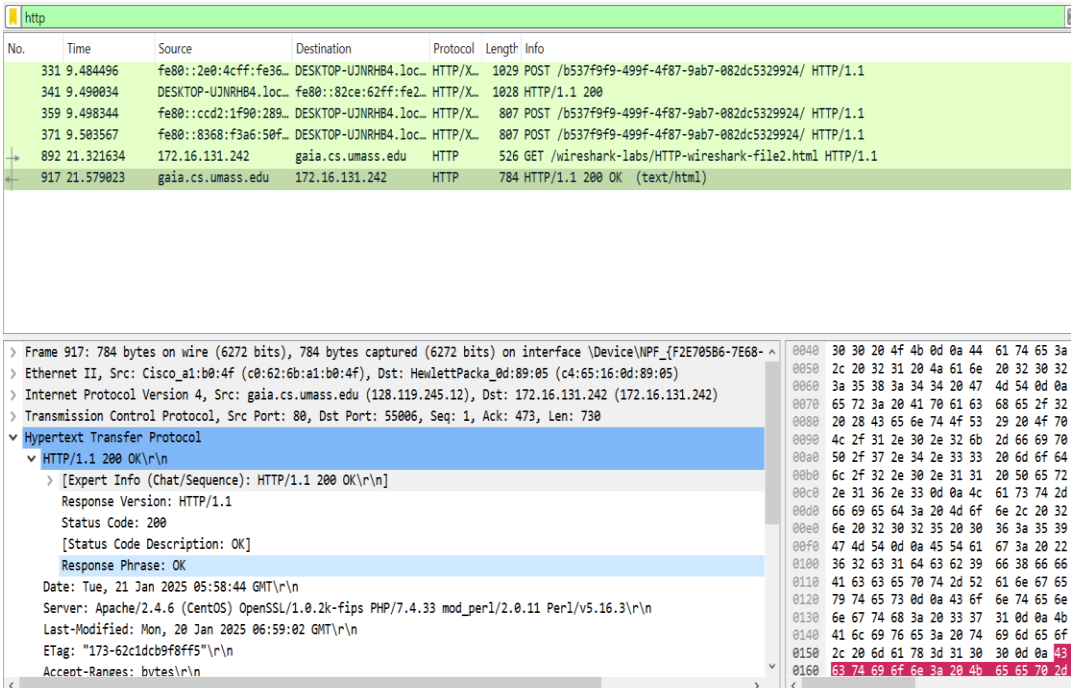
3. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

   Answer:

   I do not see the **“**IF-MODIFIED-SINCE” but I can see only Last-Modified.



4. 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:
HTTP status code is **200** and phrase returned from server in response is **OK.**

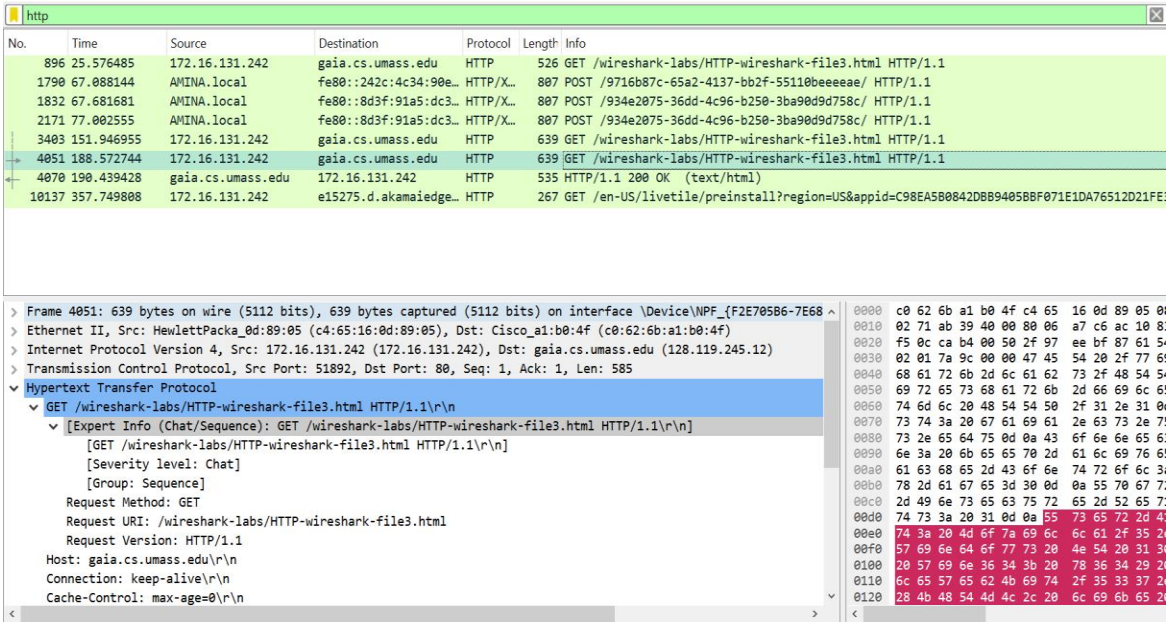


➢ Retrieving Long Documents

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?

   Answer:

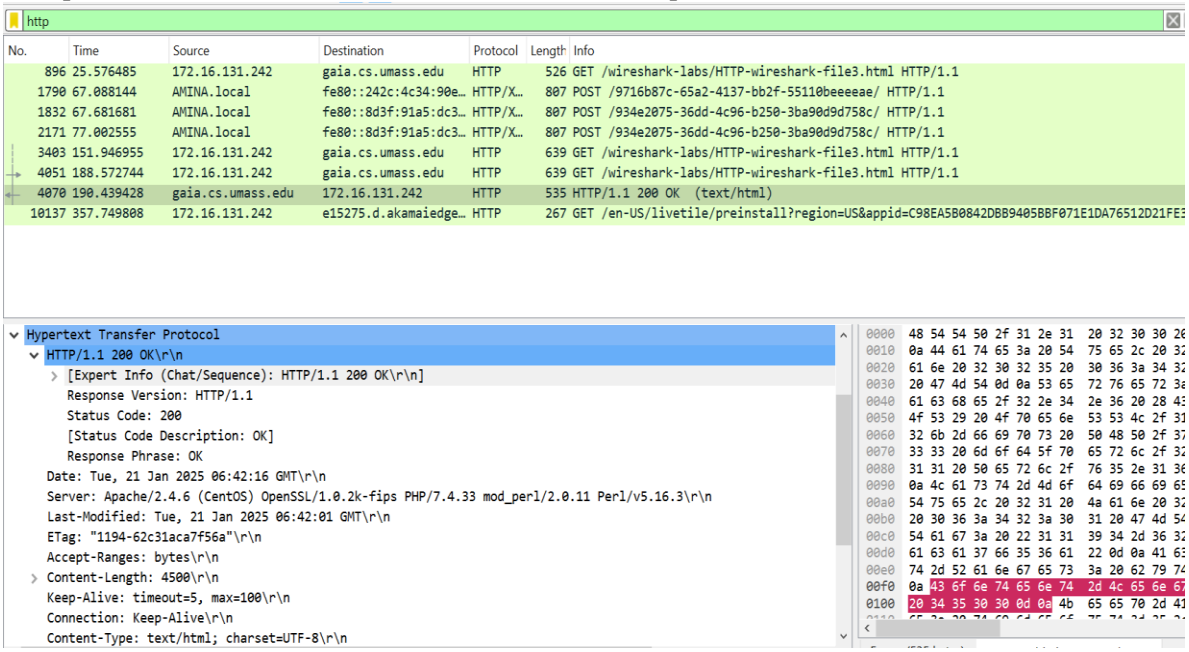
   Browser sent three HTTP GET request. The packet number in the trace contains **896, 3403 and 4051.**



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

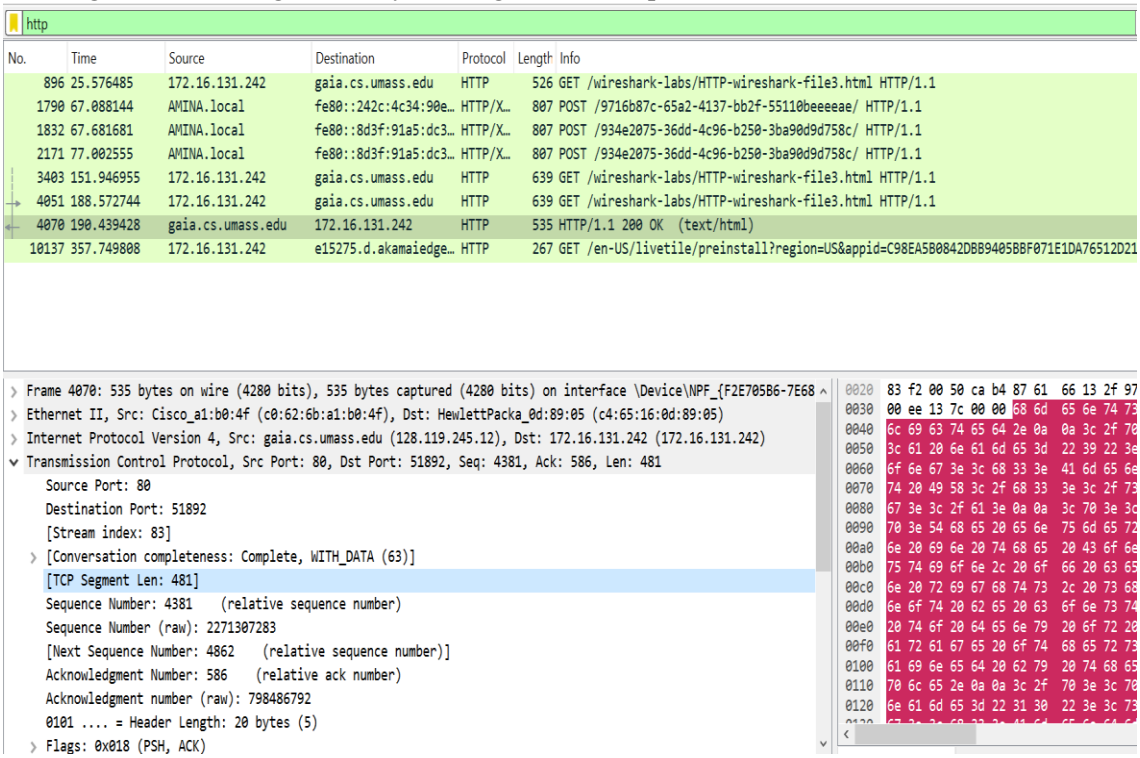
   Answer:

   The packet number in trace that contain status code and phrase is **4070.**

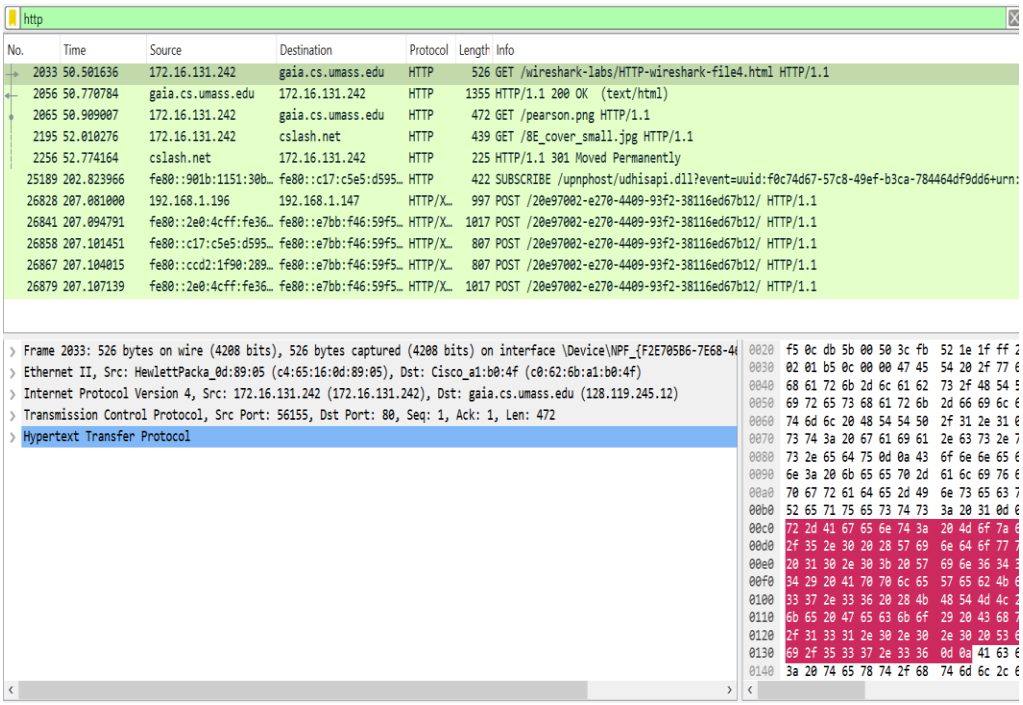


3. What is the status code and phrase in the response?
   Answer:
   From the figure above the status code **is 200** and response phrase is **OK.**

4. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?
   Answer:
   TCP segments data length to carry the single HTTP response is **481.**



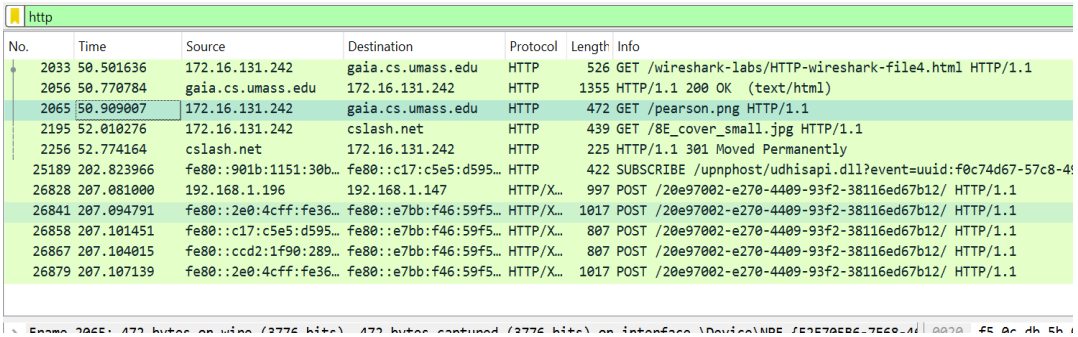
- **HTML Documents with Embedded Objects**
  1. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?
     Answer:
     The browser sent three HTTP GET requests where two HTTP GET request sent to the internet addresses which are **gaia.cs.umass.edu** and one sent to the **cslash.net.** The figure below show the HTTP GET requests and the internet address sent.



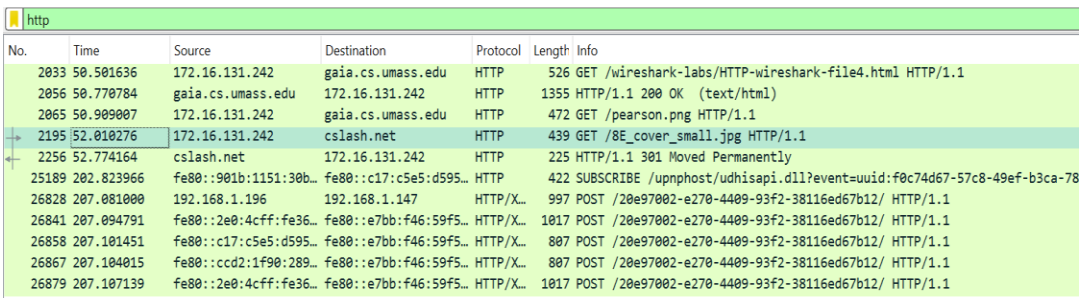
2. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

Answer:

The two images were downloaded **serially** since two HTTP GET request of the images have time difference.



First image Time:50.909007.



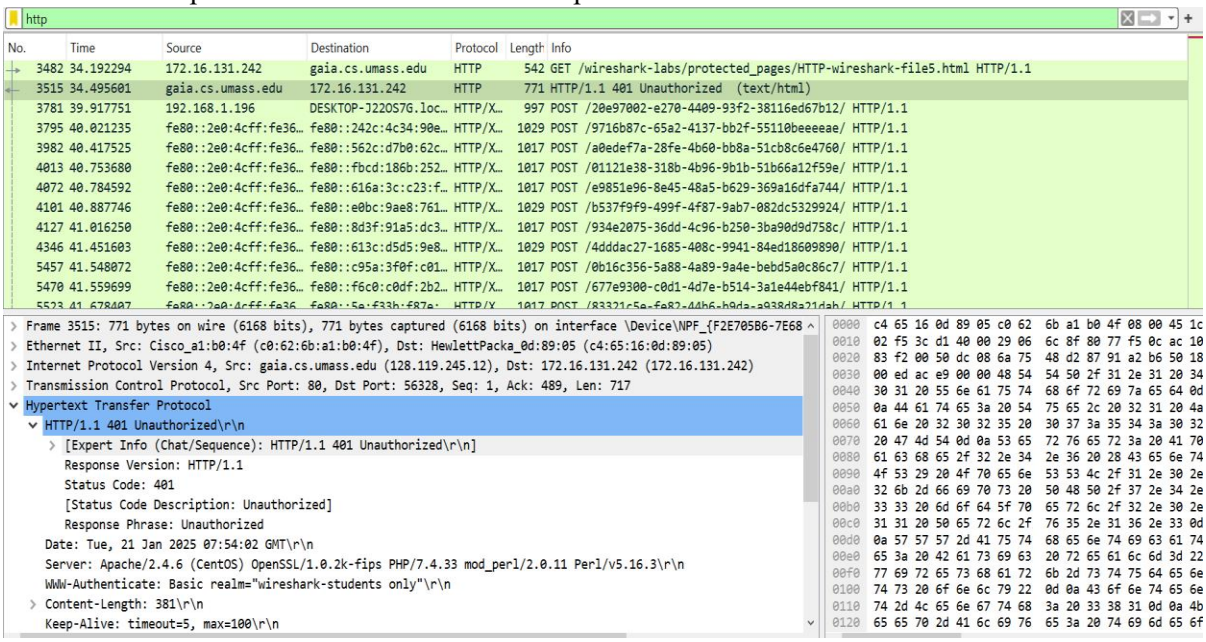
Second image Time: 52.010276

➢ HTTP Authentication

1. 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 status code is **401** and the phrase is **unauthorized.**



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

   Answer:

   The second HTTP GET request contain two new field which are **cache-control** and **Authorization** as seen in the figure below.

