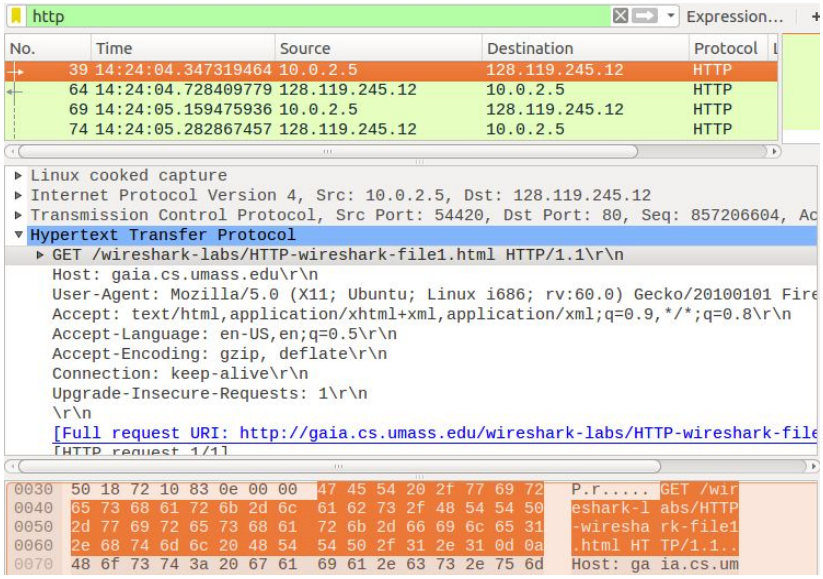
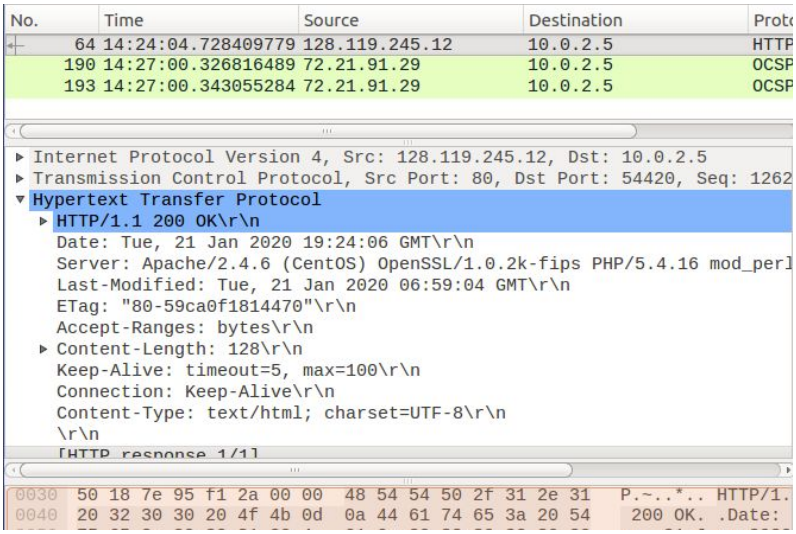
CPS 706 - Wireshark HTTP

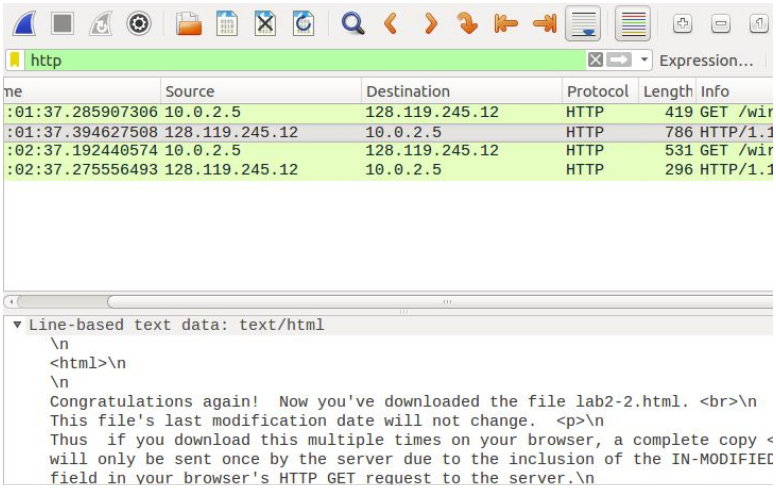


1. *Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?*
   - HTTP Version 1.1
2. *What languages (if any) does your browser indicate that it can accept to the server?*
   - En-us (US English)
3. *What is the IP address of your computer? Of the gaia.cs.umass.edu server?*
   - Computer IP address: 10.0.2.5
   - Gaia.cs.umass.edu server: 128.119.245.12

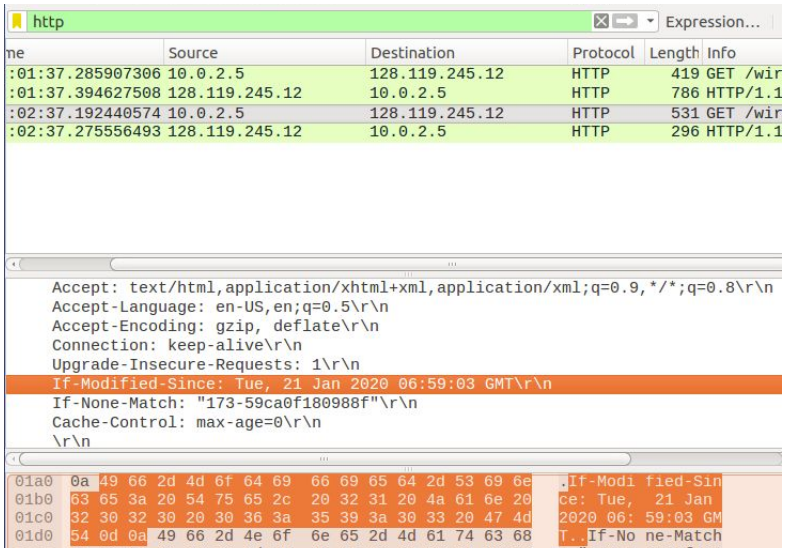


4. *What is the status code returned from the server to your browser?*
   - 200 OK

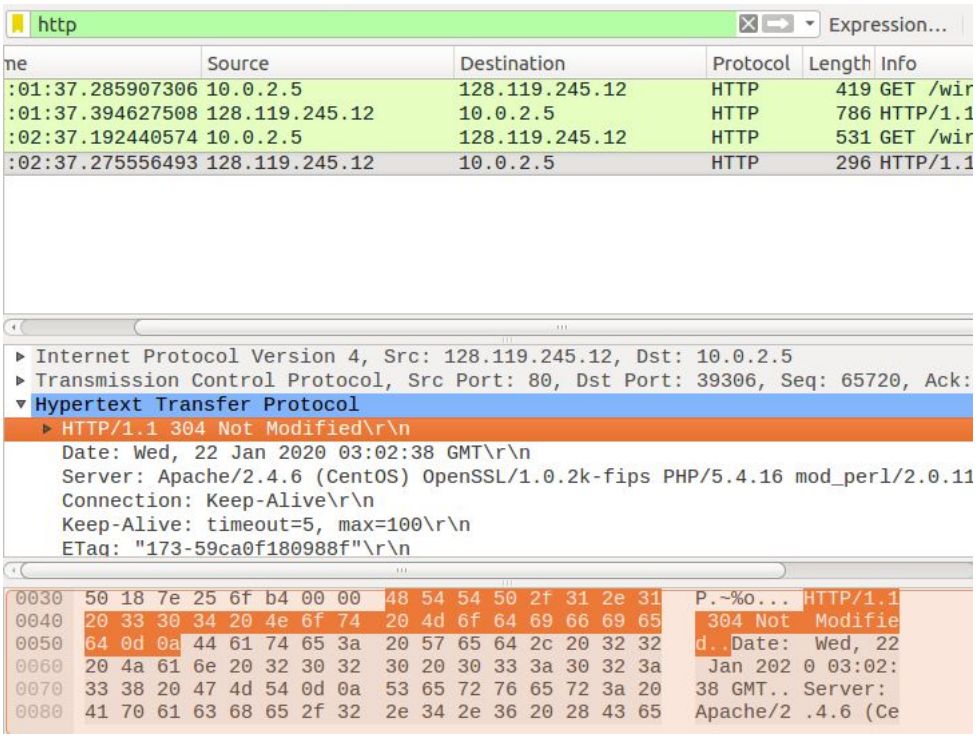
5. *When was the HTML file that you are retrieving last modified at the server?*
    - Last-modified: Tue, 21 Jan 2020 06:59:04
6. *How many bytes of content are being returned to our browser?*
    - Content-length: 128 bytes
7. *By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one*
    - No. All the raw data are also displayed in the packet-listing window



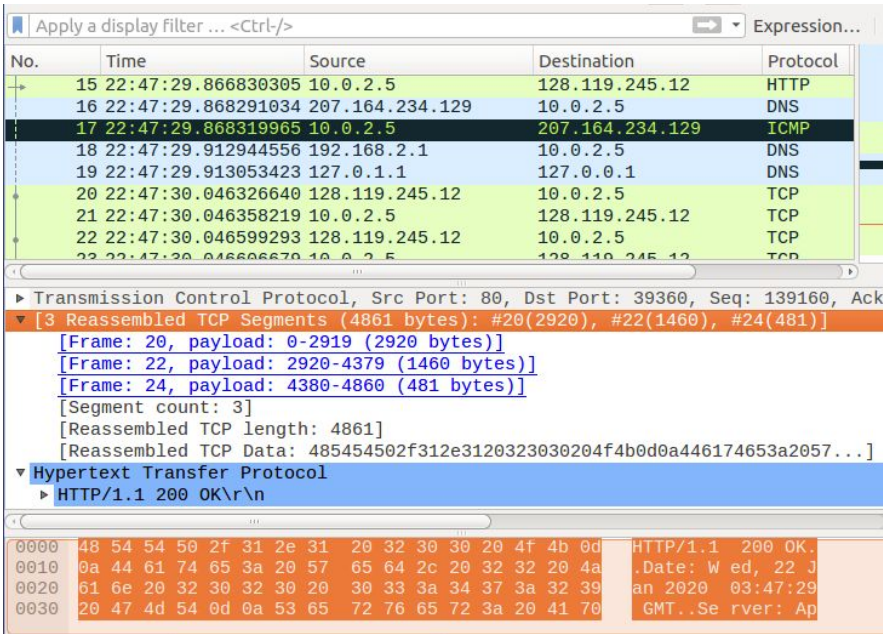
8. *Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?*
    - No
9. *Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?*
    - Yes, it provided the line-based text data (the HTML file)



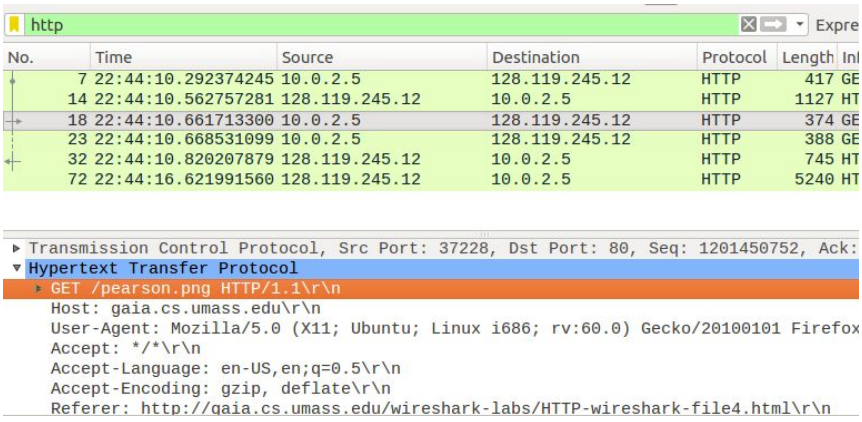
10. *Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET? If so, what information follows the "IF-MODIFIED-SINCE:" header?*
    - Yes. The information that follows the header includes the last modification date
    - If-Modified-Since: Tue, 21 Jan 2020 06:50:03 GMT



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.*
    - 304 Not Modified
    - No, the server did not return the contents of the file which can be seen based on the difference in content-length between the first and second HTTP reply
    - It is not being sent again because of the inclusion of the "If-Modified-Since" field in the second HTTP GET

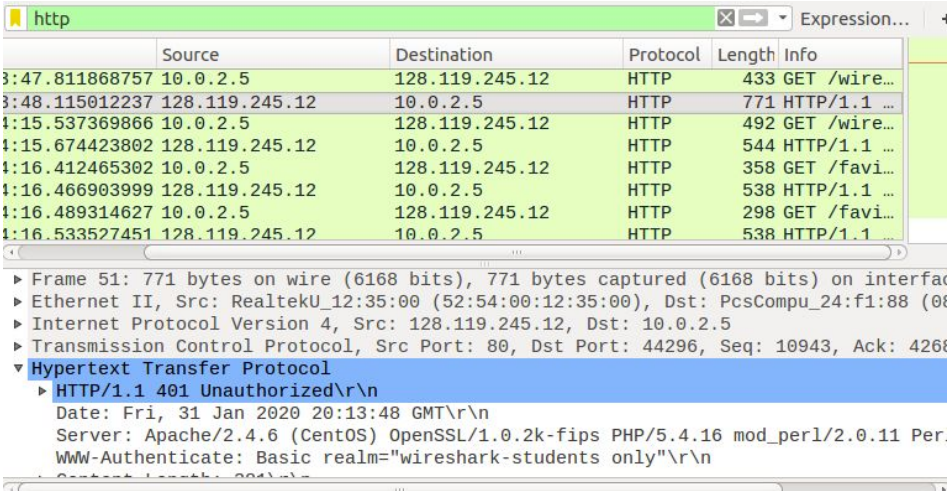


12. *How many HTTP GET request messages were sent by your browser?*
    - One HTTP GET request
13. *How many data-containing TCP segments were needed to carry the single HTTP response?*
    - 3 TCP segments were needed
14. *What is the status code and phrase associated with the response to the HTTP GET request?*
    - 200 OK
15. *Are there any HTTP status lines in the transmitted data associated with a TCP-induced "Continuation"?*
    - No



16. *How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent?*
    - 3 HTTP GET request messages were sent
    - Internet address: 128.119.245.12

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.*
    - The browser downloaded the 2 images serially because the HTTP responses were received at different times (one came after the other).
    - First response at 22:44:10
    - Second response at 22:44:16



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

19. *When your browser sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?*
    - Authorization Field

      Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n

      Credentials: wireshark-students:network