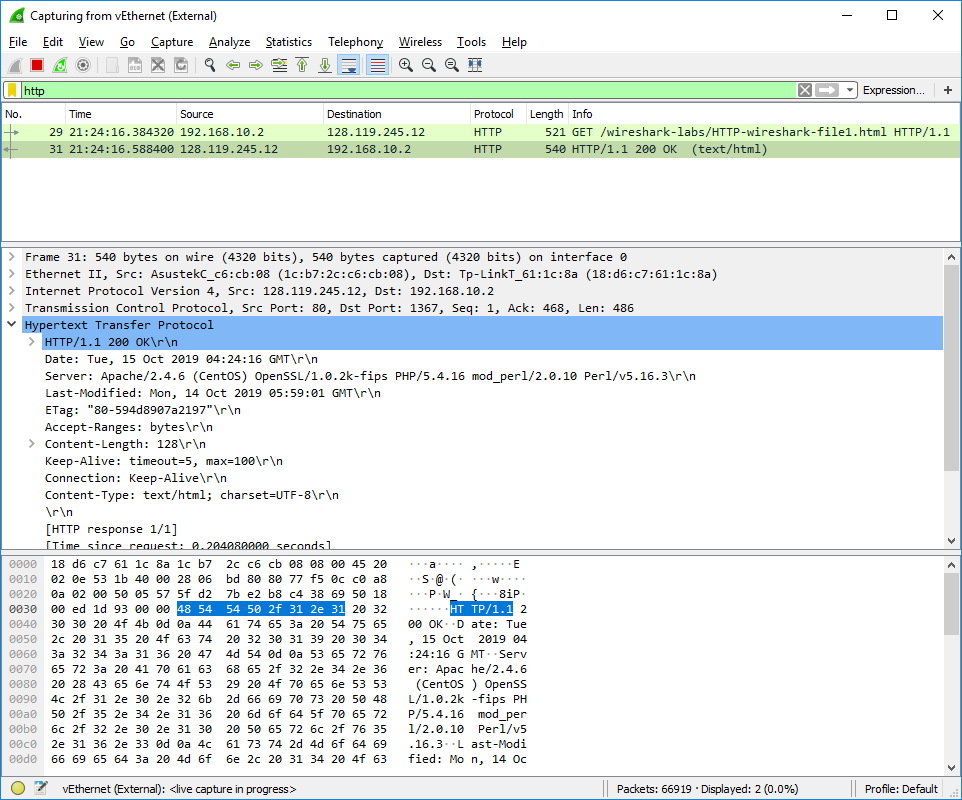
|  |  |
| --- | --- |
| CS372-400 | Edmund Dea |
| 10/13/2019 | ID# 933280343 |

**Lab 2: Wireshark**

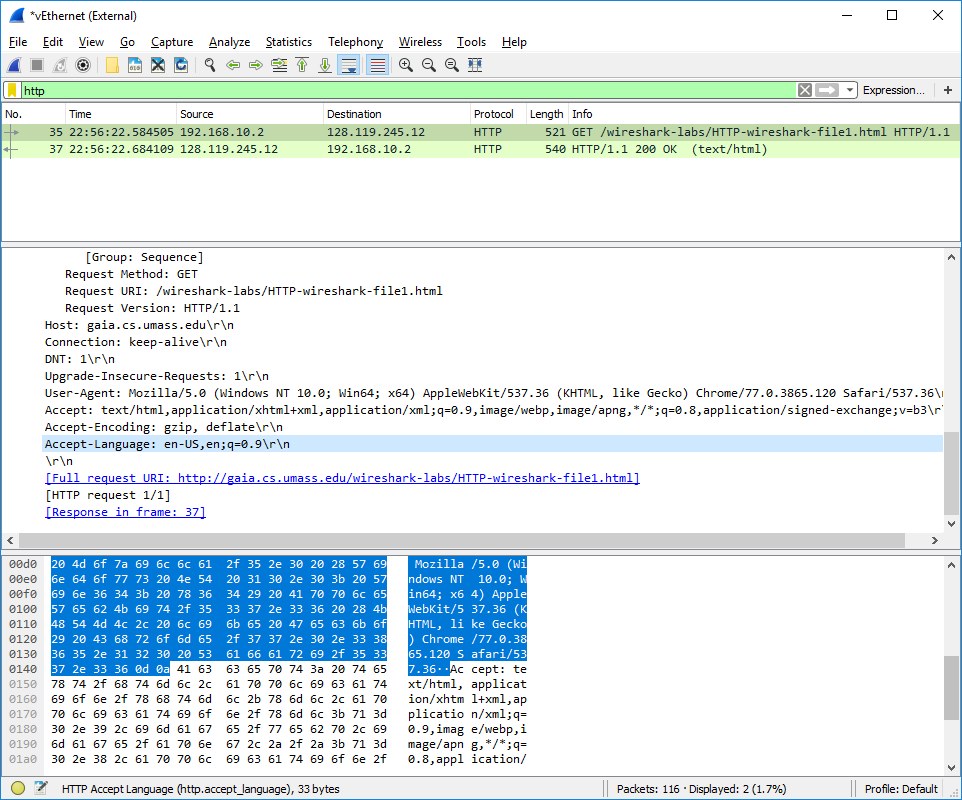
1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

My browser is running HTTP 1.1. The server is also running HTTP 1.1.



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

My browser indicates that it can accept “en-US, en; q=0.9\r\n”, which means that my browser can accept English US or English language with a q-factor weighting of 0.9.



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

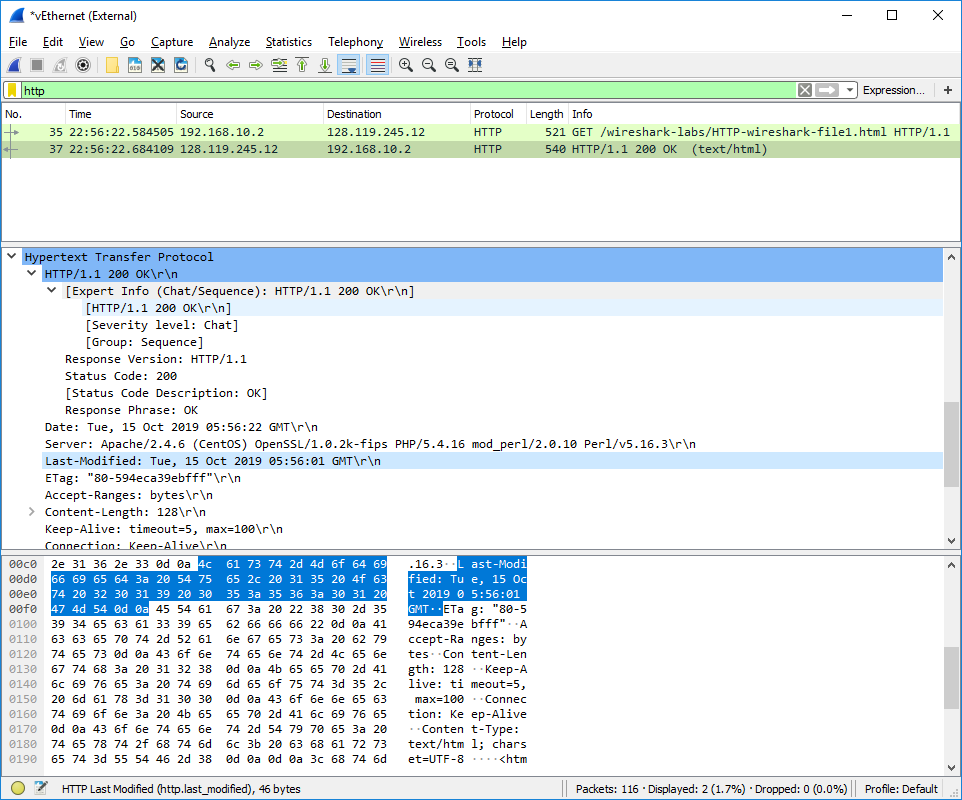
The IP address of my computer is 192.168.10.2, which is the source address. The IP address of gaia.cs.umass.edu is 128.119.245.12, which is the destination address.

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

Status code 200 OK was returned from the server to my browser.

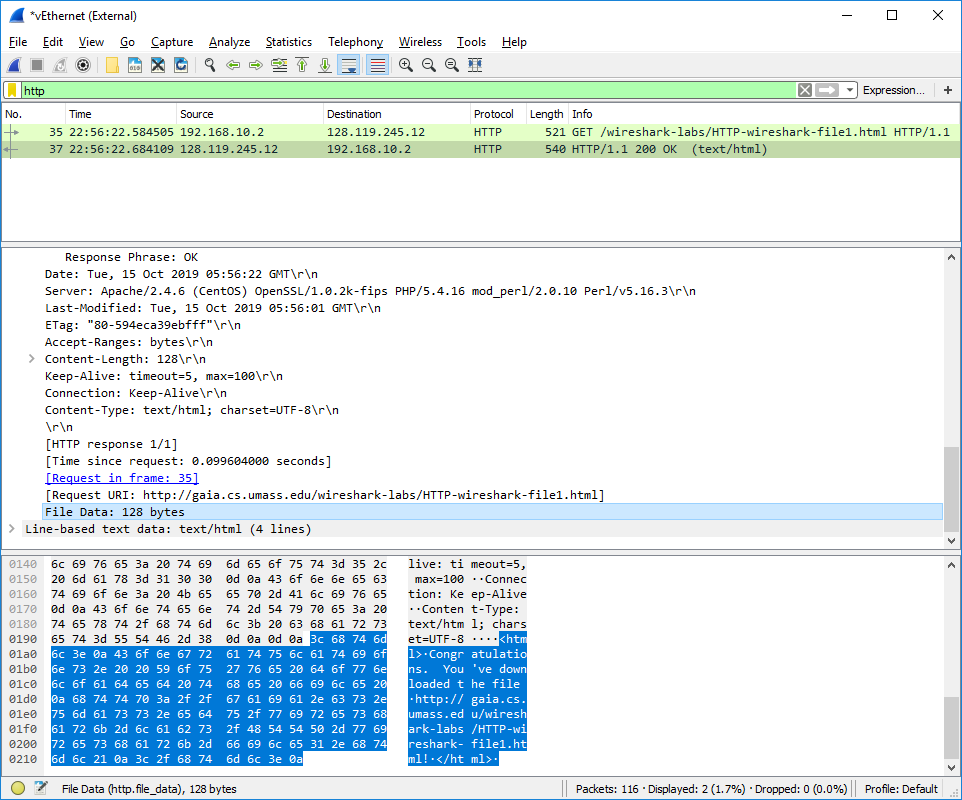
1. When was the HTML file that you are retrieving last modified at the server?

The HTML file that I am retrieving was last modified at the server on “Tue, 15 Oct 2019 05:56:01 GMT”.



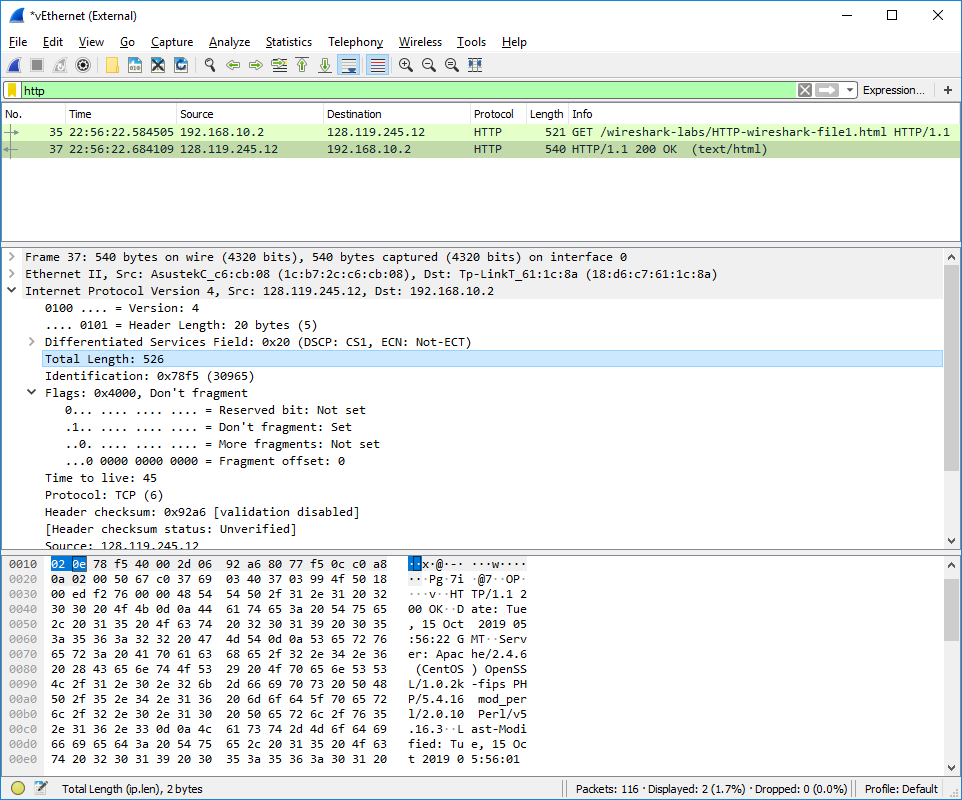
1. How many bytes of content are being returned to your browser?

128 bytes of content were returned to my browser.



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.

Yes, the Total Length header specifies the size of the IP packet, as shown below.



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?
2. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
3. Now inspect the contents of the second and third HTTP GET requests from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in one of the HTTP GETs? If so, what information follows the “IF-MODIFIED-SINCE:” header?
4. What is the HTTP status code and phrase returned from the server in response to the HTTP GET with IF MODIFIED SINCE (if there is one)? Did the server explicitly return the contents of the file? Explain.
5. 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?
6. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?
7. What is the status code and phrase in the response?
8. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?
9. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?
10. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.
11. What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser?
12. When your browser’s sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?