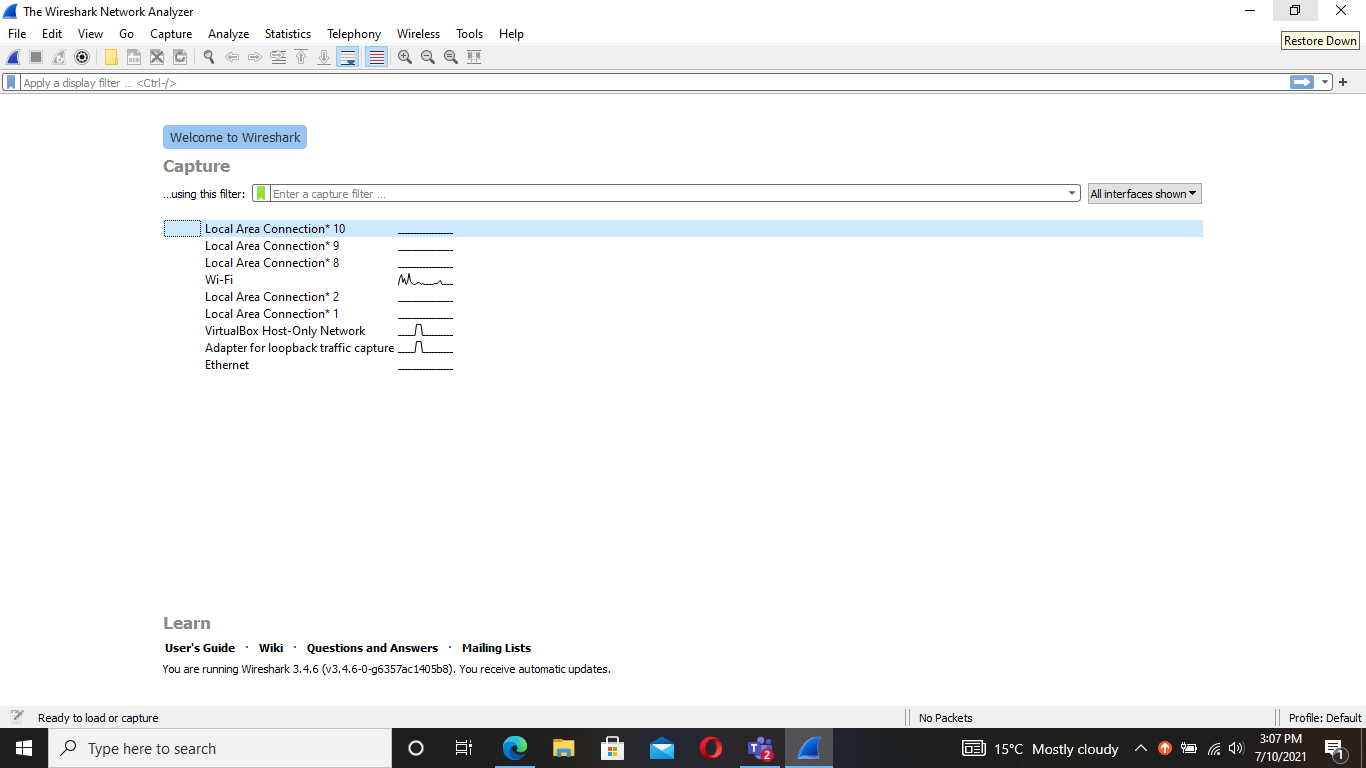
**SIMIYU JOY ABIGAEL**

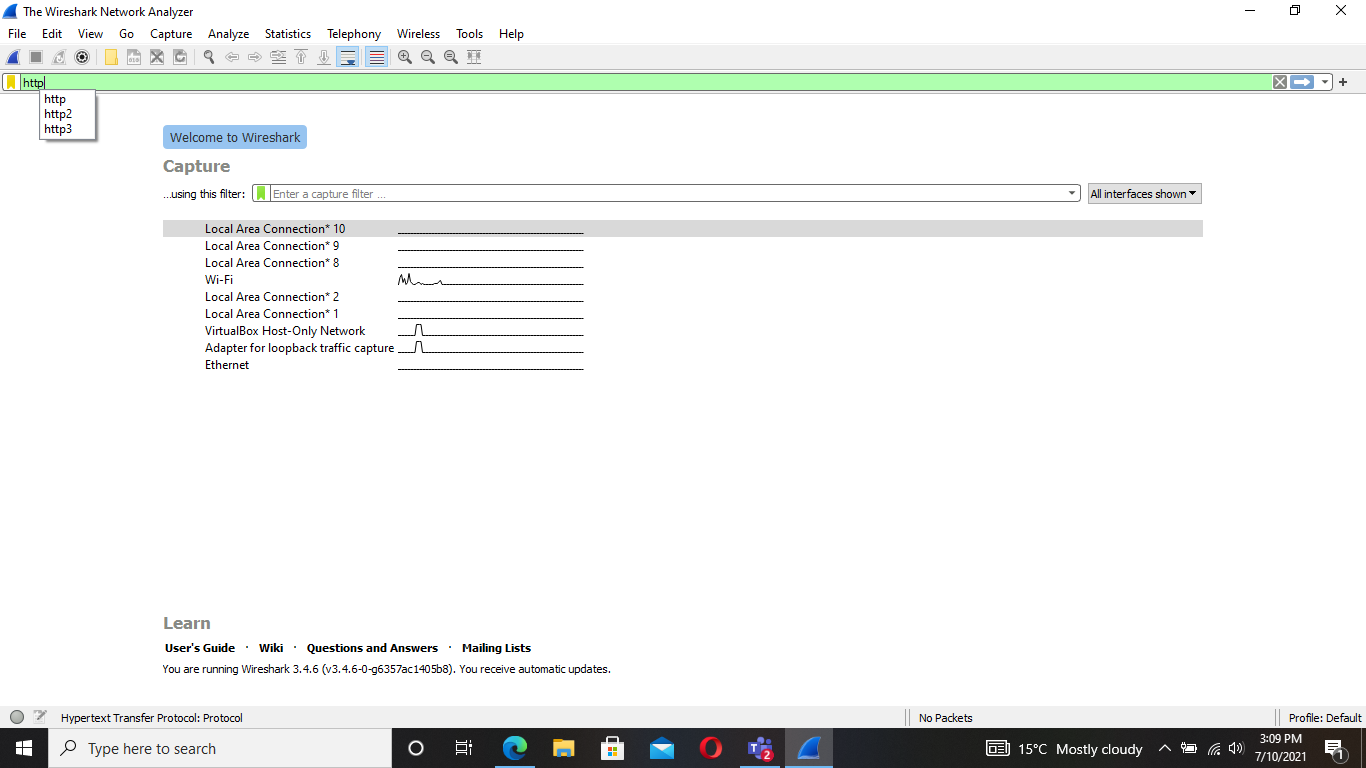
**EMAIL:** [**joy.simiyu@womentechsters.org**](mailto:joy.simiyu@womentechsters.org)

**PRACITAL ACTIVITY: WEEK 6 – WIRESHARK**

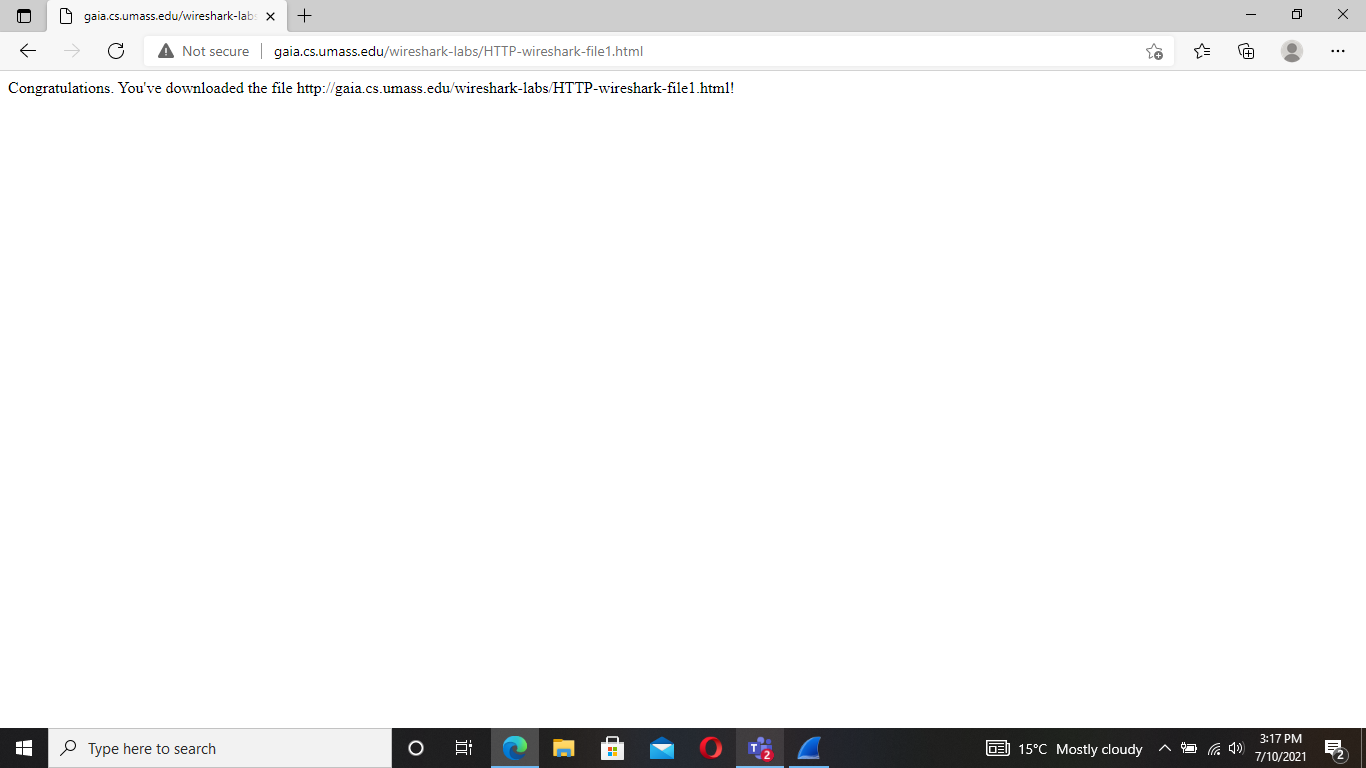
Part 1:

1. Start up your web browser.
2. Start up the Wireshark packet sniffer (but don’t yet begin packet capture). Enter “http” (just the letters, not the quotation marks) in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window. (We’re only interested in the HTTP protocol here, and don’t want to see the clutter of all captured packets).





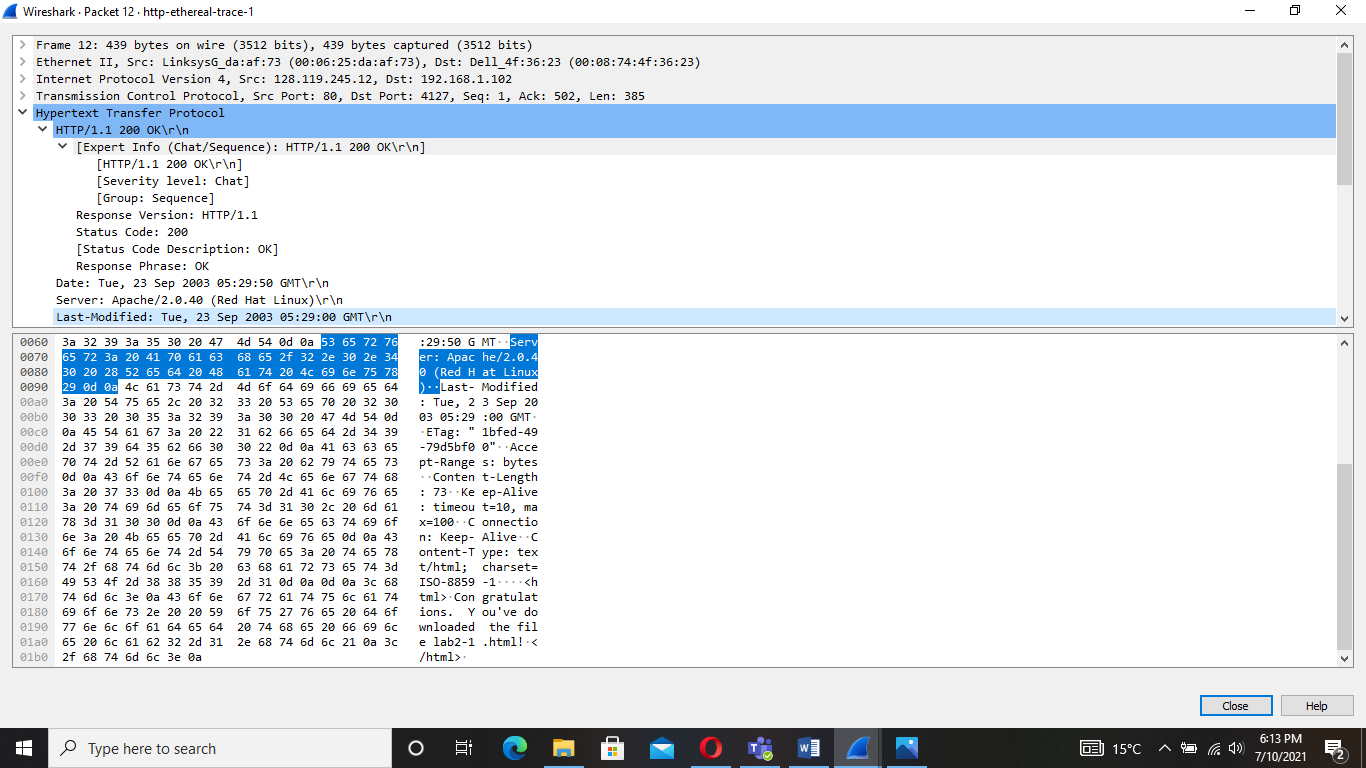
1. Wait a bit more than one minute (we’ll see why shortly), and then begin Wireshark packet capture.
2. Enter the following to your browser <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html> Your browser should display the very simple, one-line HTML file.
3. Stop Wireshark packet capture.



Part 2:

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

It is running under HTTP/1.1 version.

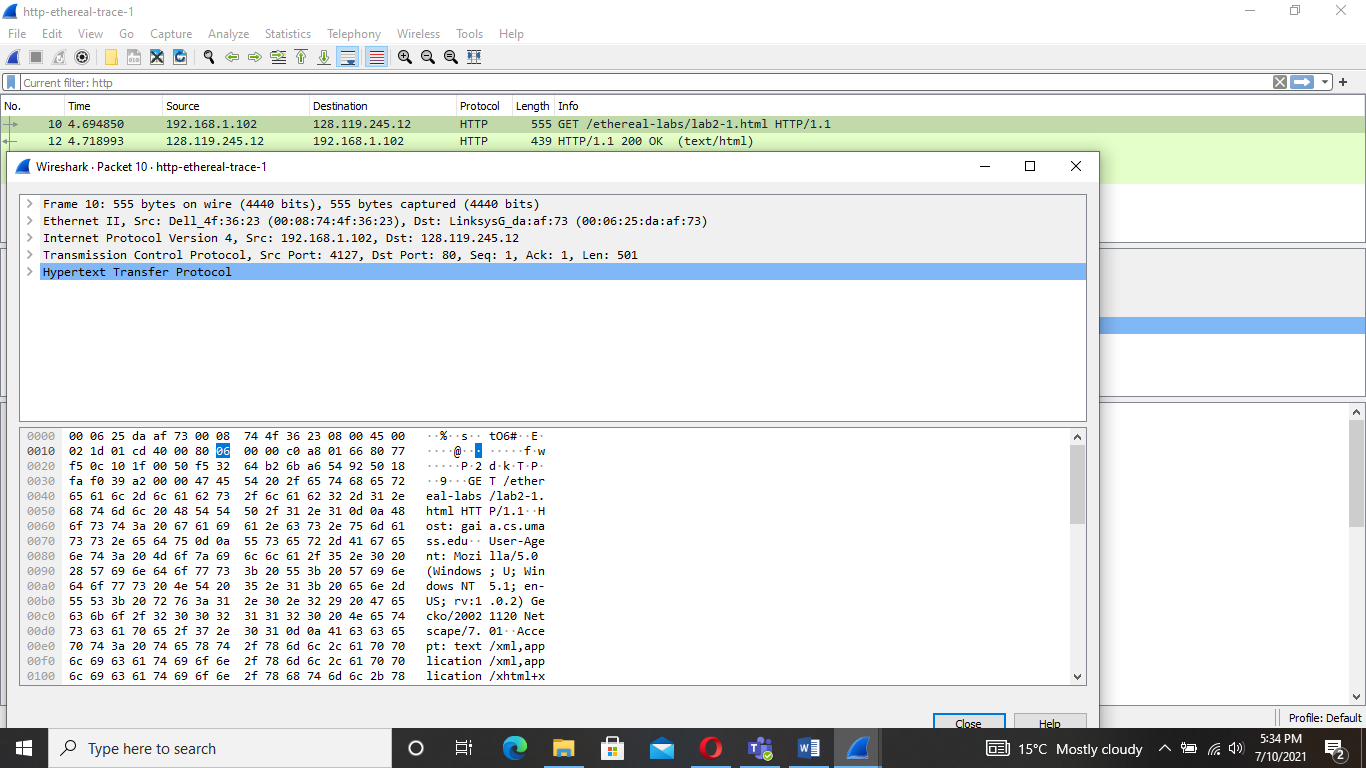


1. What languages (if any) does your browser indicate that it can accept to the server? In the captured session, what other information (if any) does the browser provide the server with regarding the user/browser?

The languages accepted are en- US, en;q=0.50\r\n

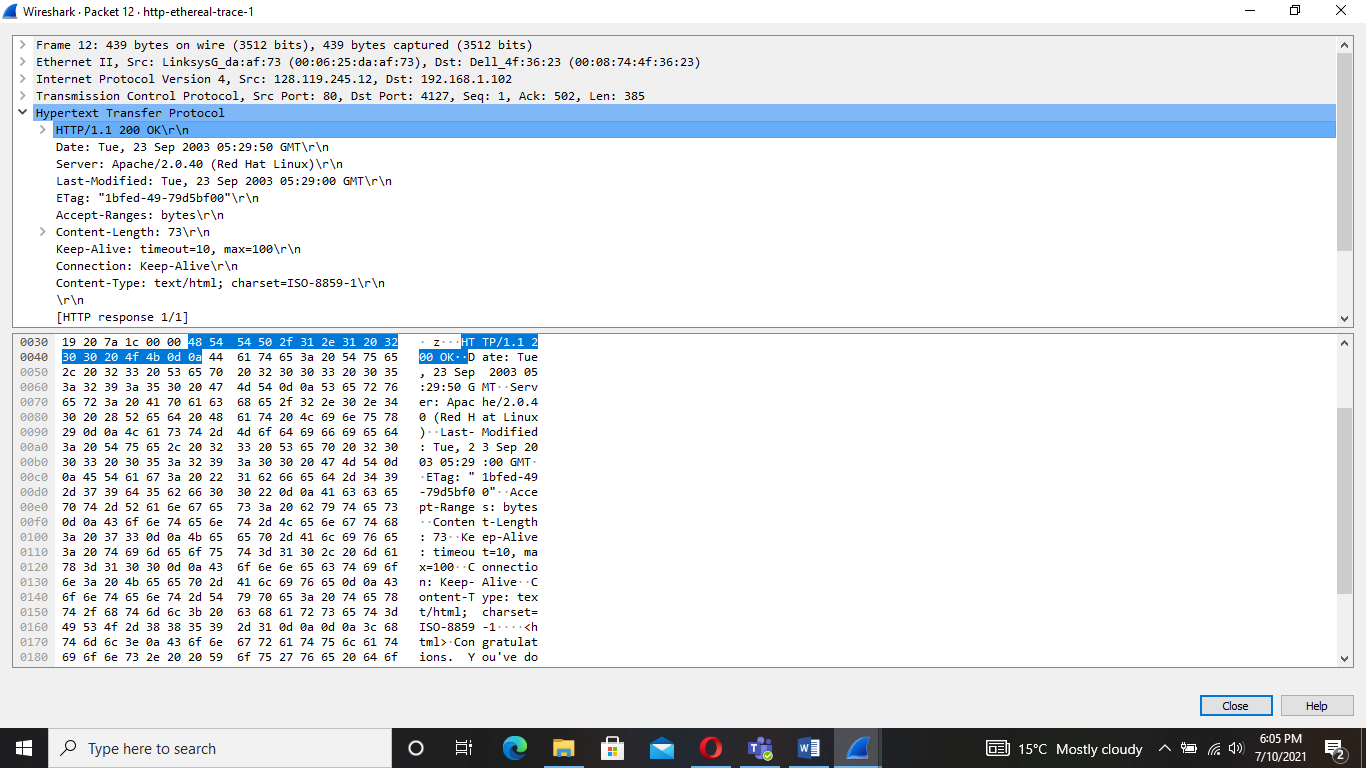
1. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

IP address of my computer is 192.168.1.102 and of the server is 128.119.245.12



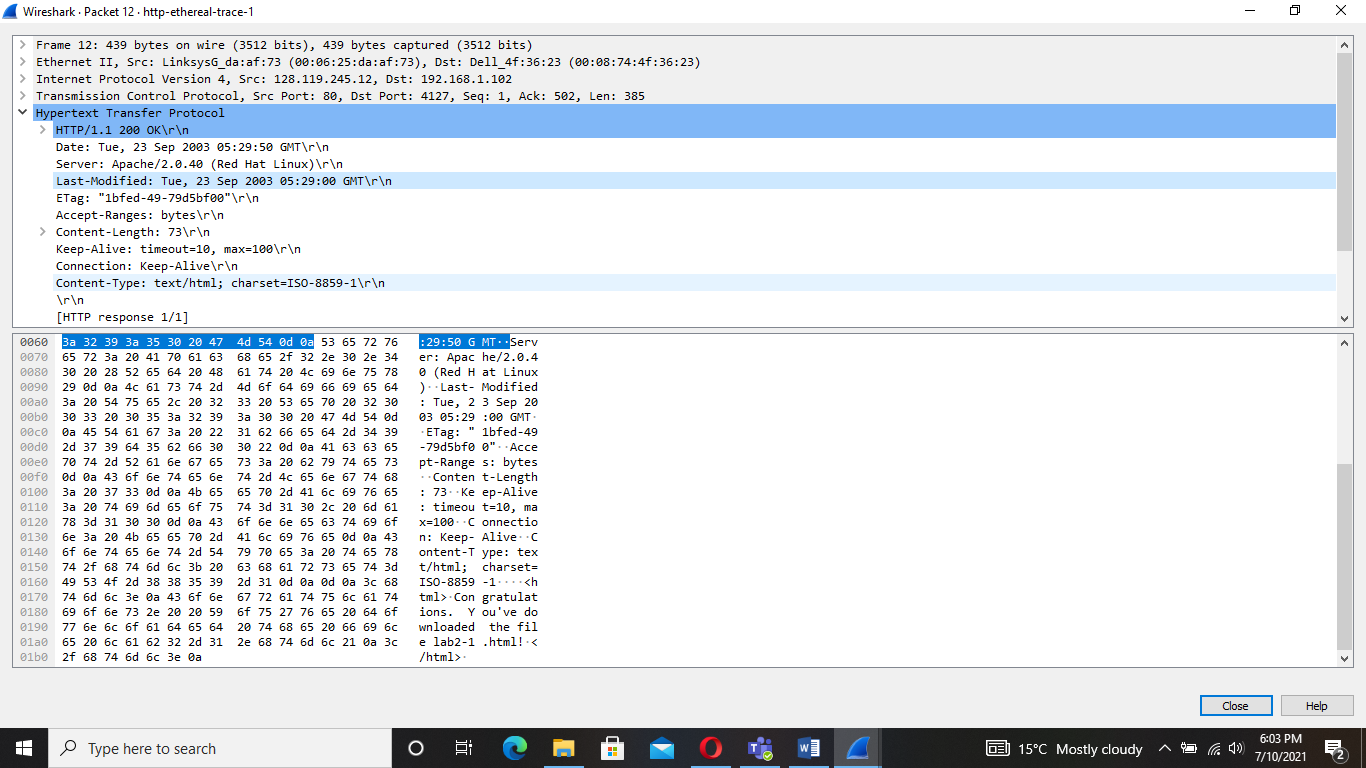
1. What is the status code returned from the server to your browser?

200 is the status code being returned to the browser.



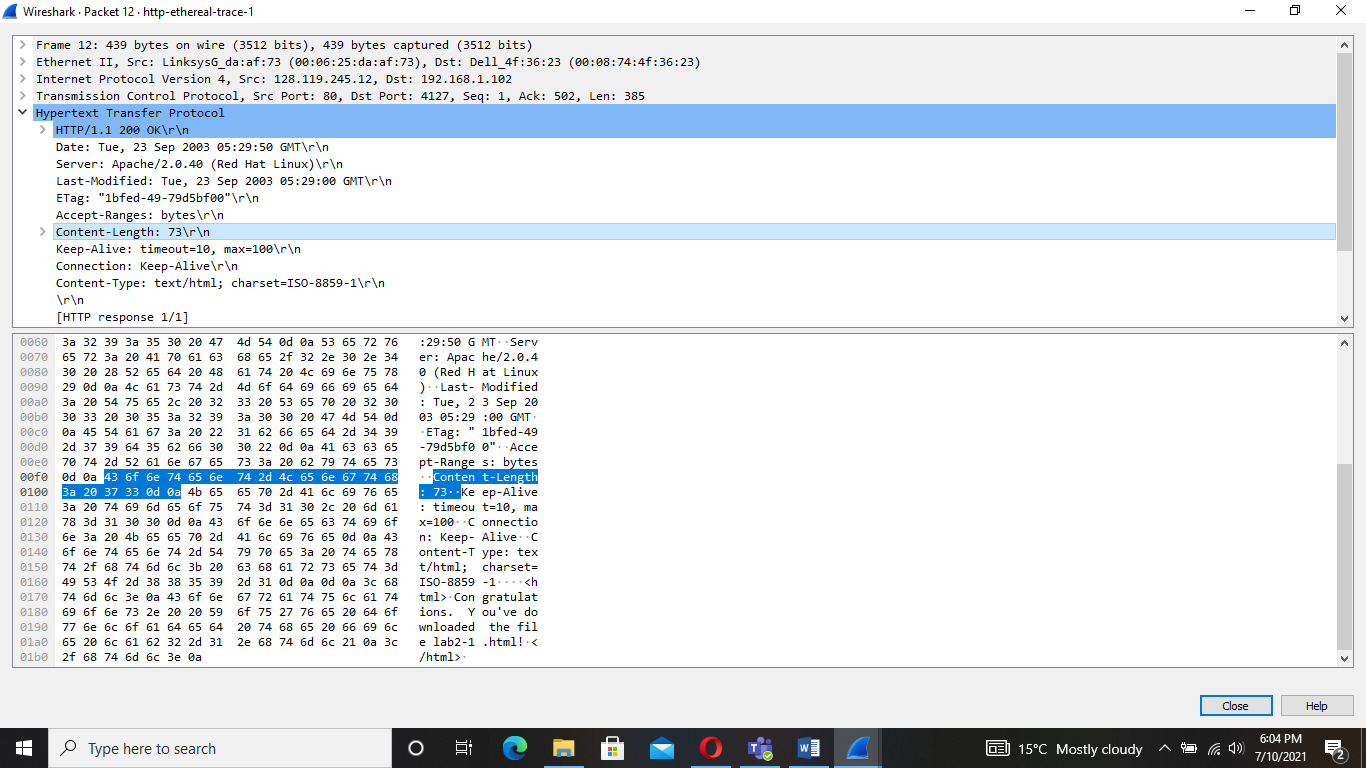
1. When the HTML file that you are retrieving was last modified at the server?

Tue, 23 Sept 2003 05:29:50 GTM



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

73 bytes is what is being returned to the browser.



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

Brief explanation of task and findings.

This analysis is used to display html files using the http protocol that is specified on the display filter search bar. This search displays all the HTTP traffic available to be displayed. It then specifies the aspect of the HTTP protocol which is the basic GET/response interaction.

The results of the operation displayed on the packet-listing window showed that two HTTP messages were captured: the GET message from your browser to the server and the RESPONSE message from the server to your browser.  The packet-contents window shows details of the specified message. The HTTP message is carried inside a TCP segment which is shown by wireshark which also displays its Frame, Ethernet, IP, and TCP packet information.