**PRACTICAL ACTIVITY WEEK 6-WIRESHARK**

* In this week’s practical activity, we’ll explore several aspects of the HTTP protocol: the basic GET/response interaction, HTTP message formats, retrieving large HTML files, retrieving HTML files with embedded objects using Wireshark for Traffic Analysis.

|  |
| --- |
|  |
|  |

The activity entails exploration of HTTP by downloading a very simple HTML file - one that is very short, and contains no embedded objects. Do the following:

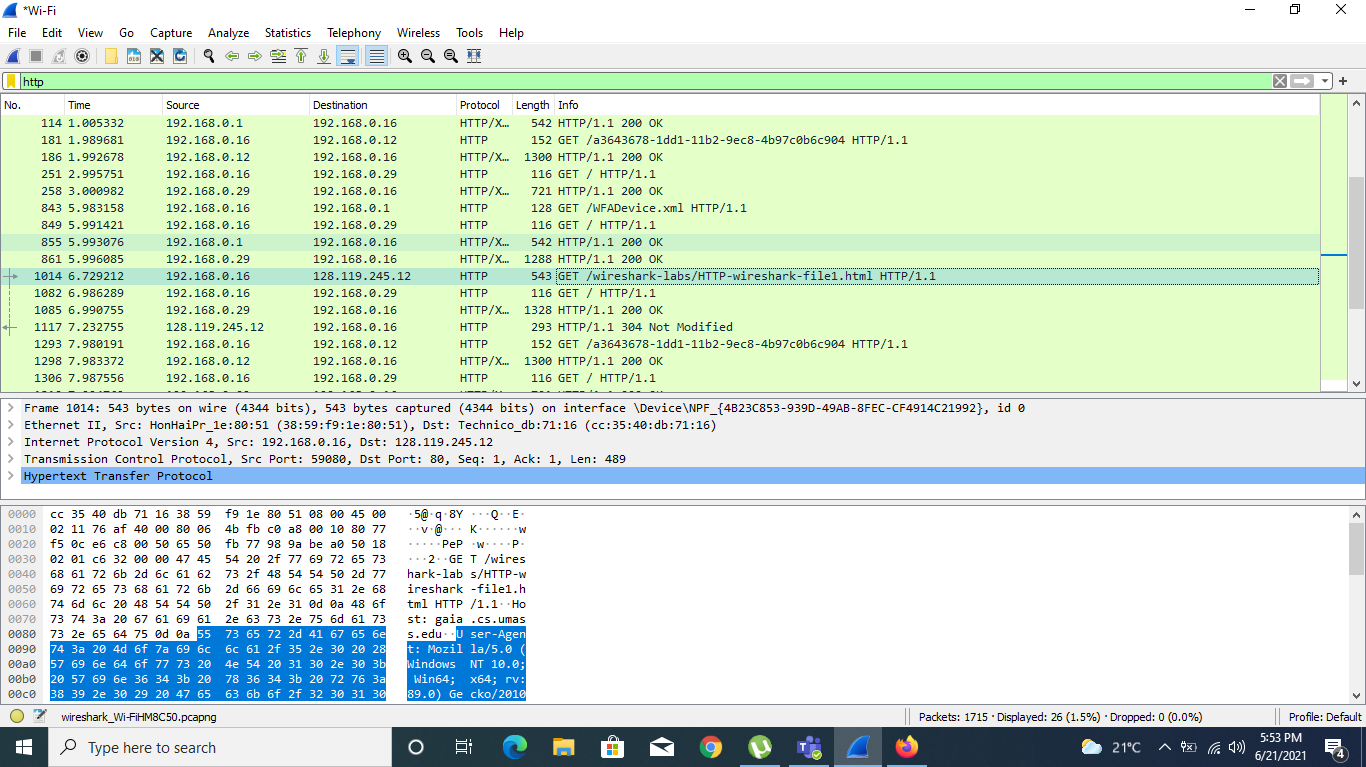
1. Start up your web browser.
2. Start up the Wireshark packet sniffer (but don’t yet begin packet capture). Enter “http” (just the letters, not the quotation marks) in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window. (We’re only interested in the HTTP protocol here, and don’t want to see the clutter of all captured packets).
3. Wait a bit more than one minute (we’ll see why shortly), and then begin Wireshark packet capture.
4. 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.
5. Stop Wireshark packet capture.

**Instructions:**

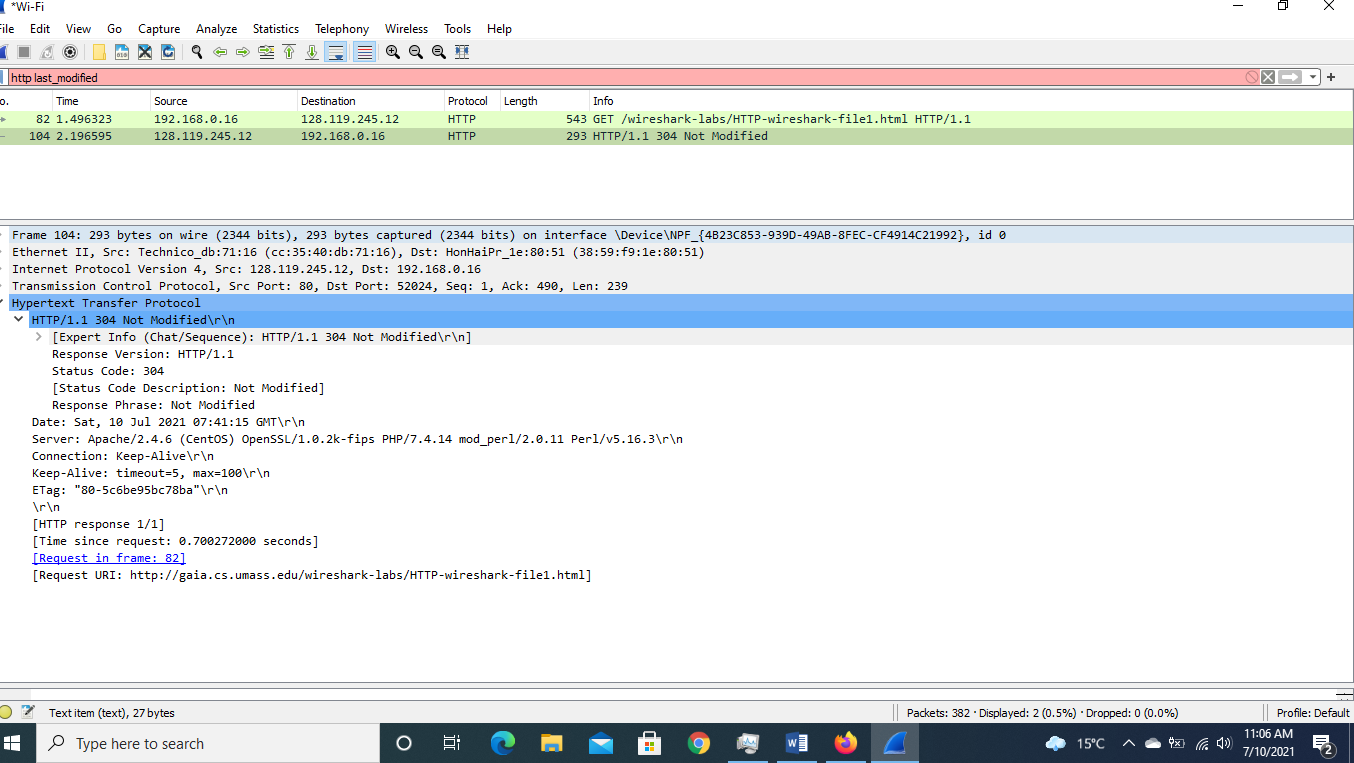
* By looking at the information in the HTTP GET and response messages, answer the following questions. When answering the following questions, you should print out the GET and response messages and indicate where in the message you’ve found the information that answers the following questions. (add screenshots on this)

**As for all questions in this course it is important that you clearly indicate what your answer is, how you obtained the answer, and (if applicable) discuss implications/insights regarding your answers. For example, in the questions below, can you elaborate on why you may have observed what you observed?**

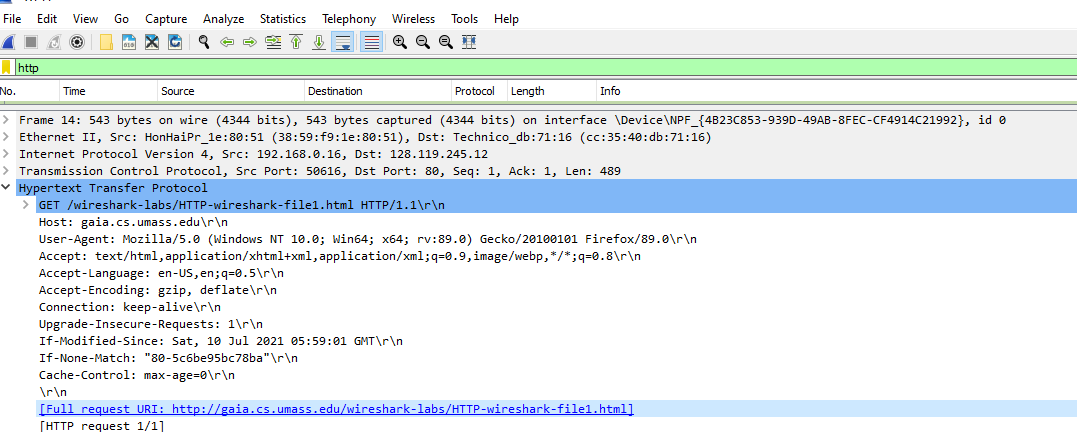
1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running? Browser and the server are both running on http 1.1
2. What languages (if any) does your browser indicate that it can accept to the server? In the captured session, what other information (if any) does the browser provide the server with regarding the user/browser? En-US,en;q=0.5\r\n Mozilla/5.0
3. What is the IP address of your computer? Of the gaia.cs.umass.edu server? 128.119.245.12 is the IP address of the gaia.cs.umass.edu server and 192.168.0.16 is the IP of my laptop



1. What is the status code returned from the server to your browser? 304
2. When was the HTML file that you are retrieving last modified at the server? Not Modified



1. How many bytes of content are being returned to your browser? Couldn’t find the content-length on my captured data



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. No.

**My observations**

To work with Wireshark, one has to understand some basics. Wireshark is dived into 5 sections

***Command menu***: this the top most window. It contains buttons and the menu for actions such as file, edit and others

***Packet-listing windows***: show the summary of each captured packet

***Packet-content window***: it displays the content of the captured frames in both ASCII and hexadecimals format

***Packet-display filter field***: This the field that is used to filter packages to be shown

***Packet-header details window***: provides details about the packed selected in the packet-listing window