**ANSWERS TO 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, 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)

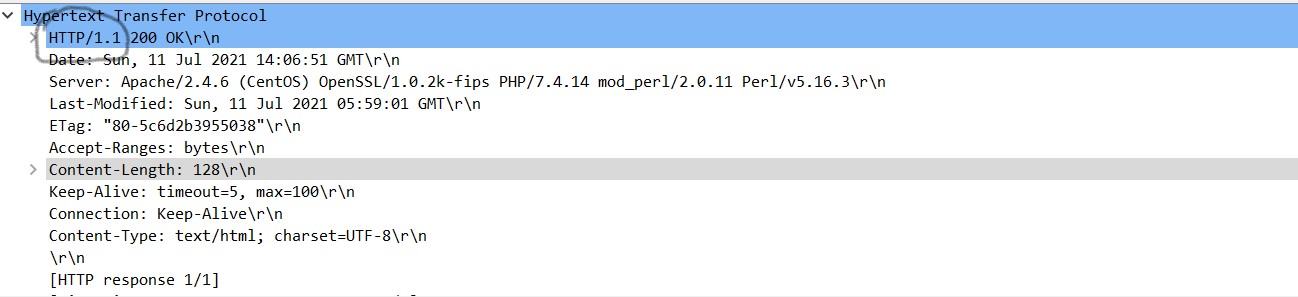
**As for all questions in this course it is important that you clearly indicate what your answer is, how you obtained the answer, and (if applicable) discuss implications/insights regarding your answers. For example, in the questions below, can you elaborate on why you may have observed what you observed?**

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

My browser is running HTTP version 1.1



The browser is running http version 1.1 as well



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 browser indicates that it can accept English language (US)

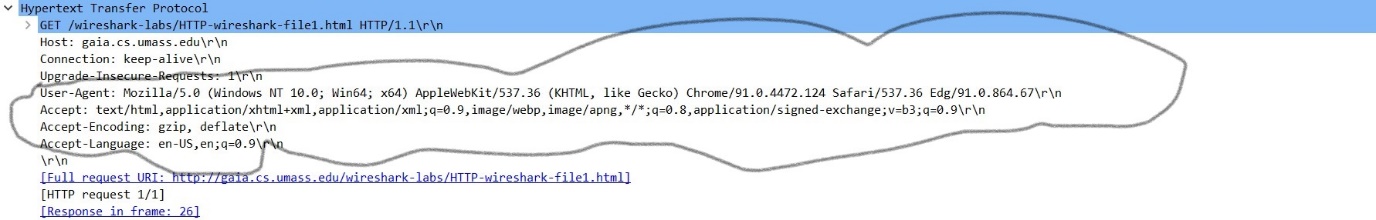


The other information the browser provides the server with regarding the user/browser are:

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36 Edg/91.0.864.67

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9

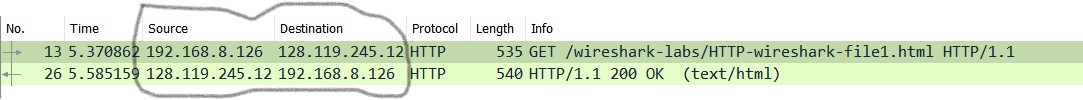
Accept-Encoding: gzip, deflate



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

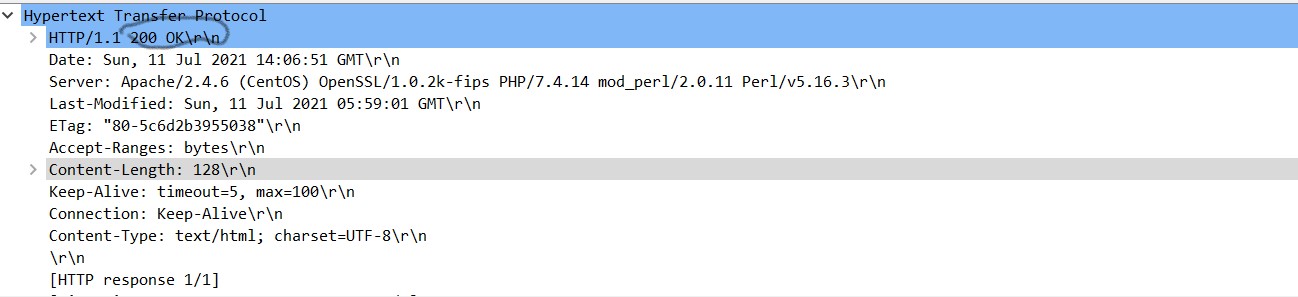
IP address of my computer- 192.168.8.126

IPaddress of gaia.cs.umass.edu.server- 128.119.245.12



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

The response code is 200 ok

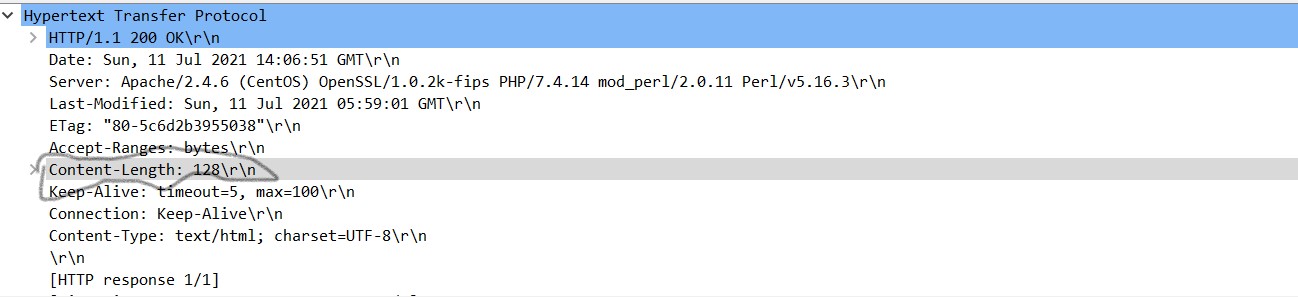


1. When was the HTML file that you are retrieving last modified at the server?



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

128 bytes of content 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.

No all http headers in the packet content pane is displayed in the packet-listing window

**Task A:** For questions 1-7, first write a brief but precise answer for each of the above questions, then write a (combined) paragraph explaining and discussing your observations from the above practice questions. Note that your answer may benefit from explaining and/or referring to some of your observations explicitly.

The two servers involved in the communication are both using the newest version of http, 1.1. The Accept-Language request HTTP header indicates that the client is able to understand the US format of English Language. The request header also gives three more information about the user/browser these are:

The user-agent: The User-Agent request header is a characteristic string that lets servers and network peers identify the application, operating system, vendor, and/or version of the requesting user agent.

Accept: The Accept request HTTP header advertises which content types, expressed as MIME types, the client is able to understand

Accept-encoding: The Accept-Encoding request HTTP header advertises which content encoding, usually a compression algorithm, the client is able to understand

The source and destination IP address indicates the public ip address the request and response is coming from. The HTTP Status Code 200: The “OK” Response. An HTTP status code 200 means success. The client has requested documents from the server. The server has replied to the client and given the client the documents. The Last-Modified response HTTP header contains the date and time at which the origin server believes the resource was last modified. It is used as a validator to determine if a resource received or stored is the same from our data capture, the file was last modified, Sunday, 11 July 2021 5:59:01 GMT. The HTTP Content-Length entity-header is used to indicate the size of entity-body in decimal number of octets i.e., bytes and sent it to the recipient. It is 128 bytes from our packet capture.