rofiat Ajagbe  Practical Activity

Rofiat.ayagbe@womentechsters.org

**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.

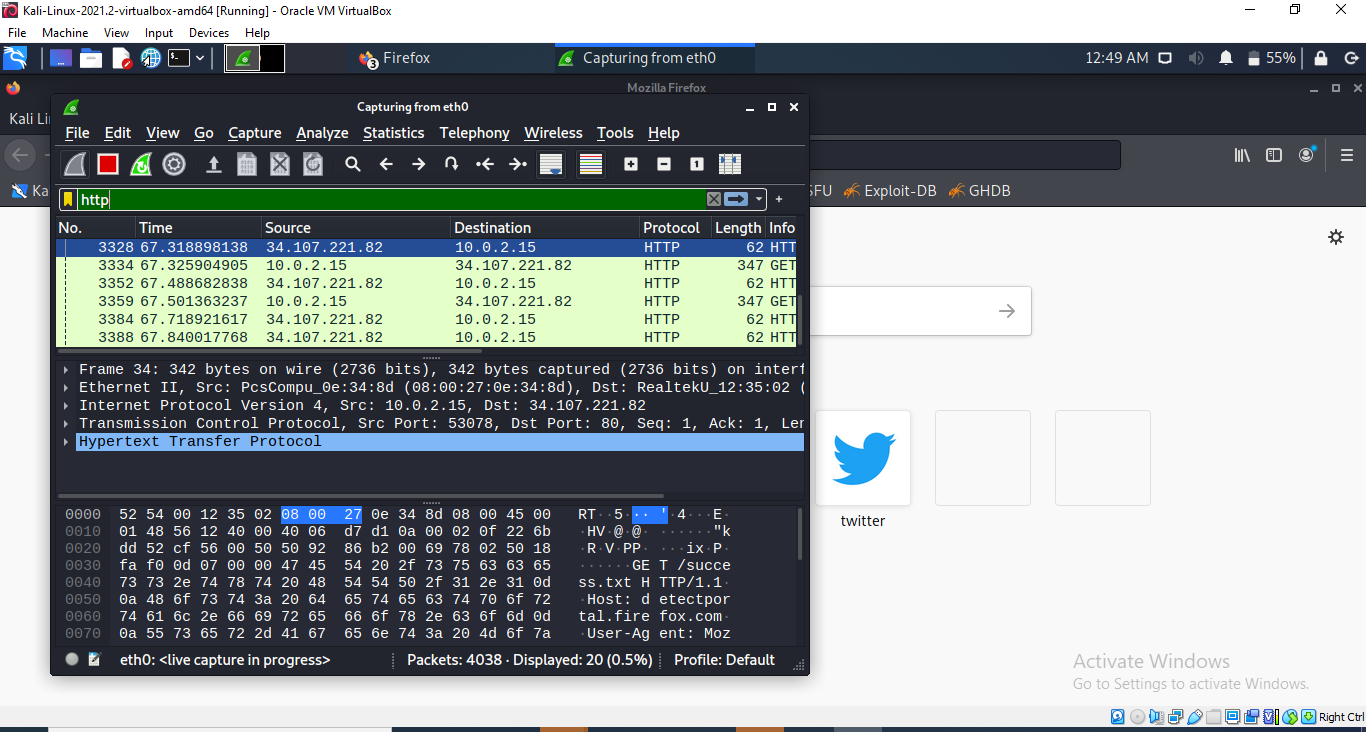
**Instructions:**

* 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?

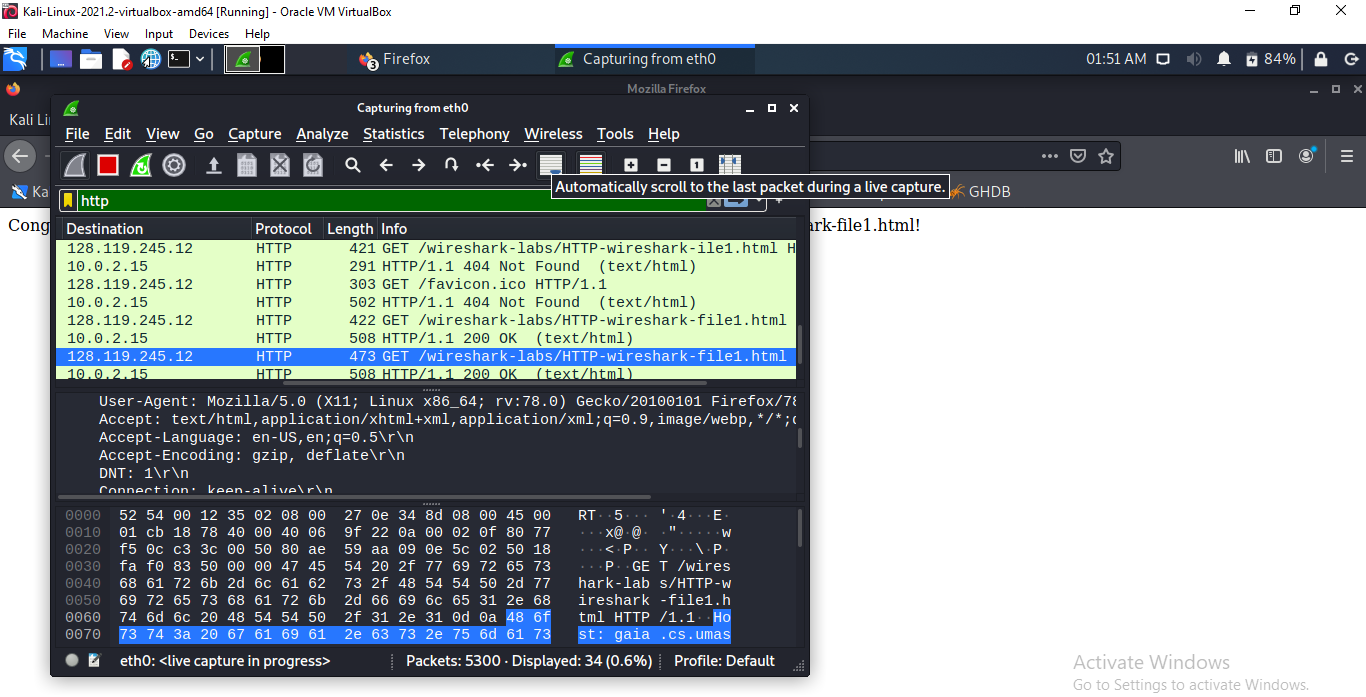
**Answer: Browser is running Version 1.1 from the http details displayed below**

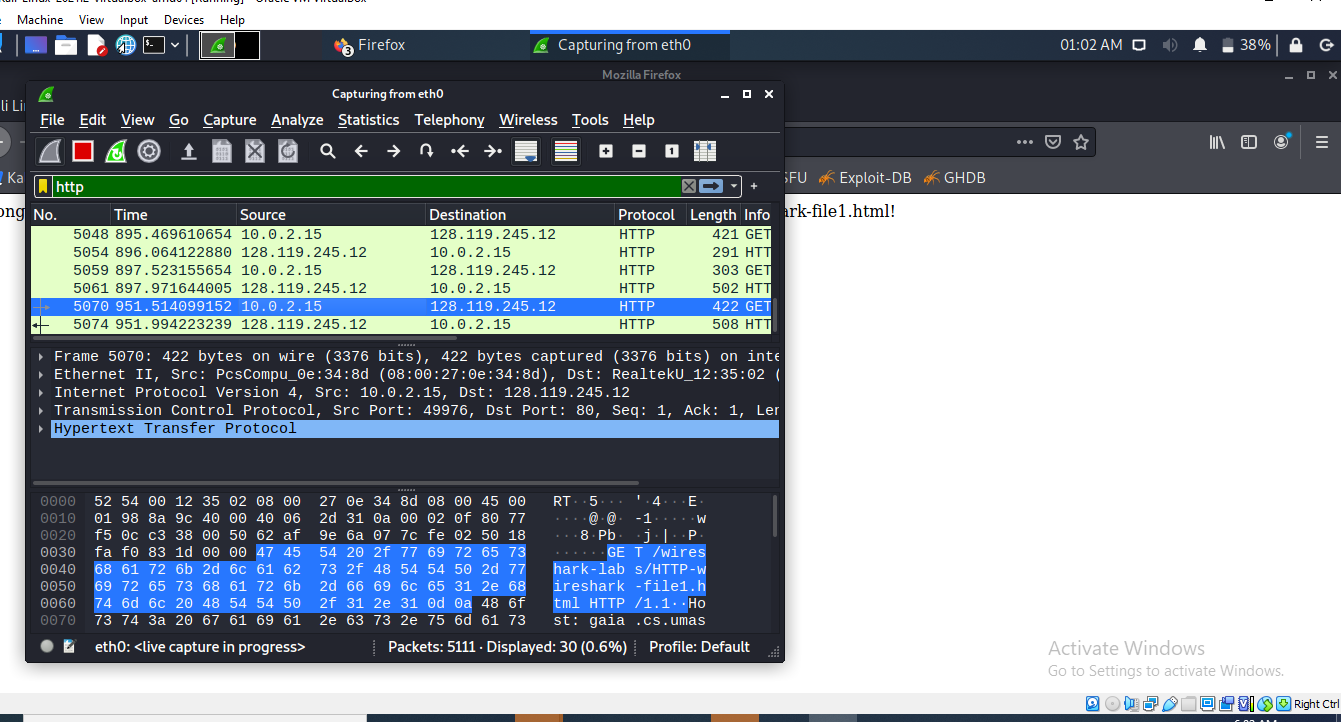


1. What languages (if any) does your browser indicate that it can accept to the server? In the captured session, what other information (if any) does the browser provide the server with regarding the user/browser?

**Answer: From the below it entails an accept language which is English en:US ,en;q=0. It provides that it can accept English. Other information includes**

* **Time**
* **Source**
* **Destination**
* **Protocol**
* **Length**
* **Info**





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

**Answer: IP for my computer is 10.0.2.15**

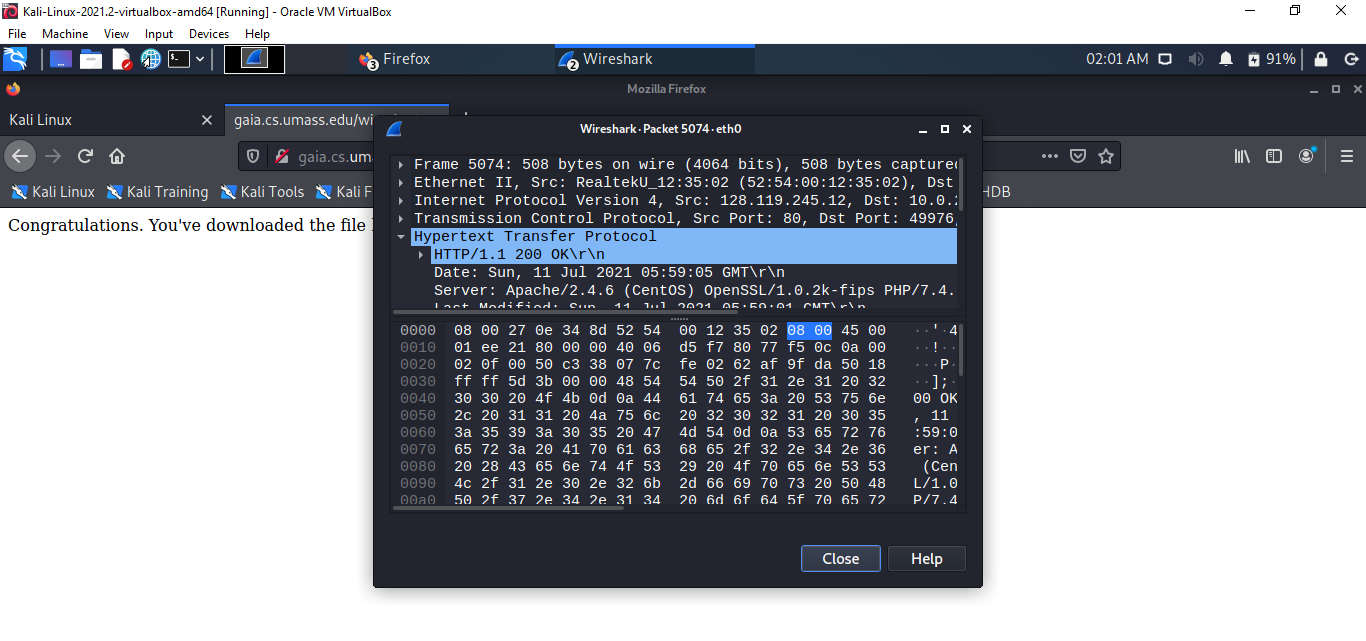
**IP for gaia.cs.umass.ed.server is 128.119.245.12**

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

**Answer: Status code returned is 200 Ok**

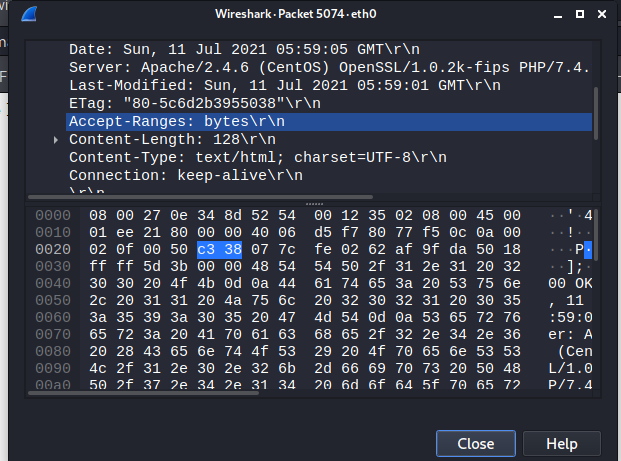
1. When was the HTML file that you are retrieving last modified at the server?

**Answer :Sun 11, Jul 2021 05:59.05 GMT\r\n**



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

**Answer :128 bytes is being returned.**



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.

**Answer : No there is none**

**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.

**Answer : The get message from my browser to the (gaia.cs.umass.edu.) and the response message from the server were captured. The content windows showed the details of the highlighted and selected http message. The wireshark displays in the frame IP TCP Ethernet and http information.**