**Practical Activity 6**

**WIRESHARK**



**Name**: Lamis Mohamed GabAllah

**Email**: [lamis.mohammed@womentechsters.org](mailto:lamis.mohammed@womentechsters.org)

**Date**: 11th July 2021

**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:**

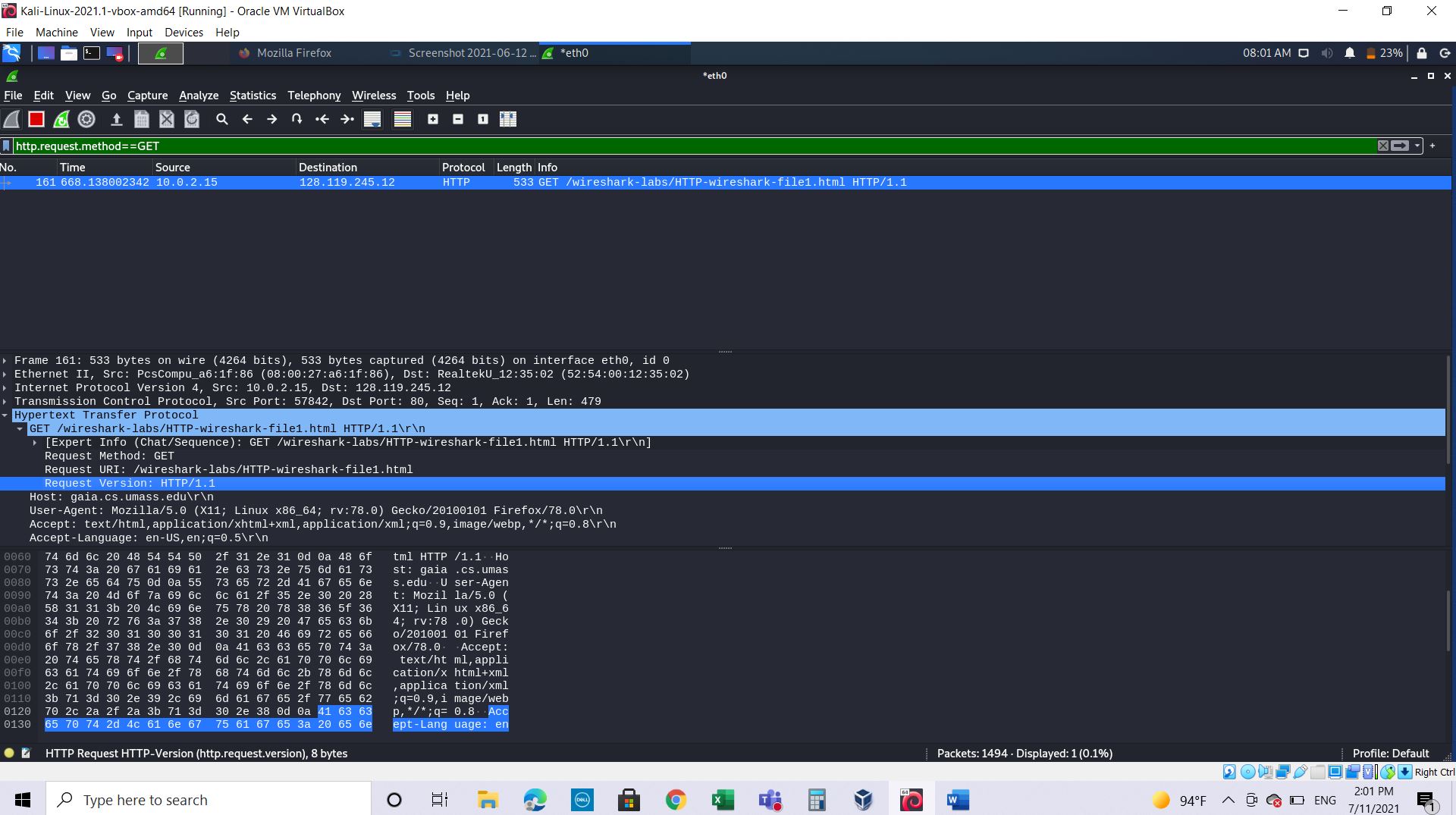
* By looking at the information in the HTTP GET and response messages, answer the following questions. When answering the following questions, you should print out the GET and response messages and indicate where in the message you’ve found the information that answers the following questions. (add screenshots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

ANS: Both of them are version 1.1

(HTTP version information is listed in the item ‘Request 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?

ANS: en-US

(languages information is listed in the item ‘Accept-Language’ in the HTTP

GET message)

Other information:

**1.Request Method:** **GET ==>** The packet is a HTTP GET .

**2.Request URI: /wireshark-labs/alice.txt** ==> The client is asking for file alice.txt present under /Wireshark-labs

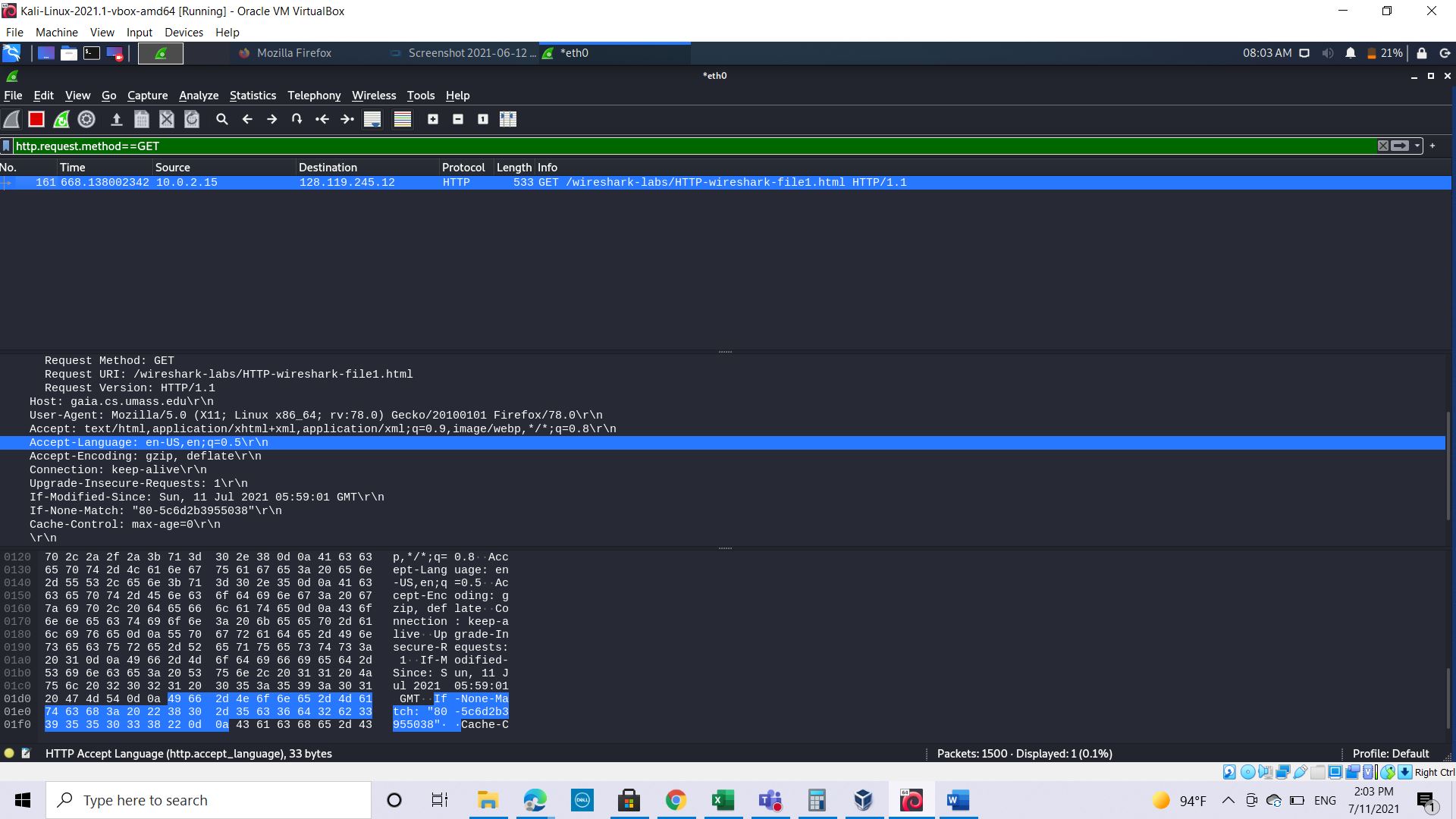
**3.Accept: text/html, application/xhtml+xml, image/jxr, \*/\* ==>** Tells server about the type of file it [client side browser] can accept. Here the client is expecting alice.txt which is text type.

**4.User-Agent:** **Mozilla/5.0 (X11, Linux:x86\_64 ,rv:78.0) like Gecko ==>** Client side browser type.

**5.Accept-Encoding:** **gzip, deflate** ==> Accepted encoding in client side.

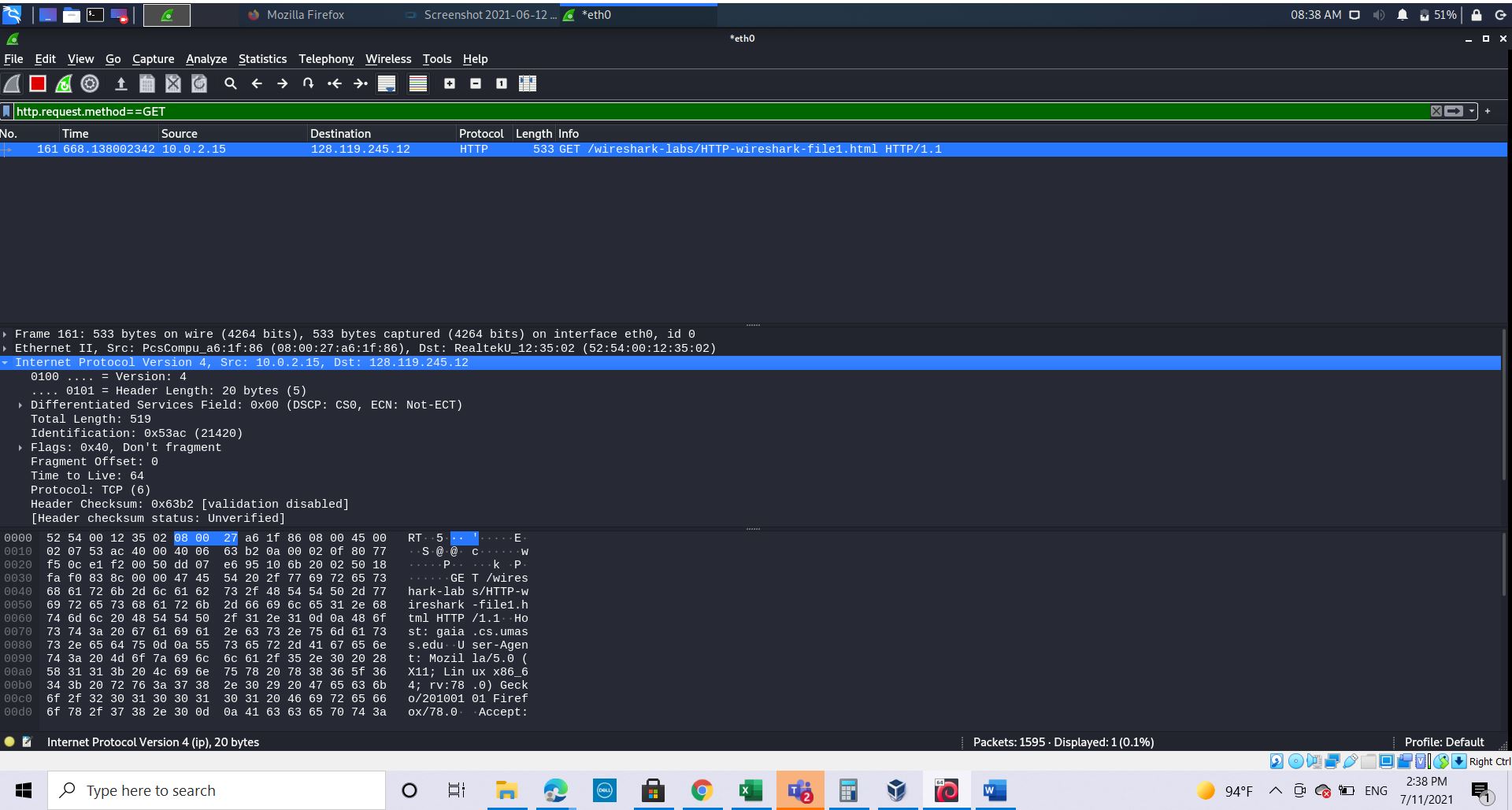
**6.Host:** **gaia.cs.umass.edu** ==> This is the web server name where client is sending HTTP GET request.

**7.Connection:** **Keep-Alive ==>** Connection controls whether the network connection stays open after the current transaction finishes. Connection type is keep alive.



1. What is the IP address of your computer? Of the gaia.cs.umass.edu server?  
   My computer IP :10.0.2.15

gaia.cs.umass.edu server : 128.119.245.12

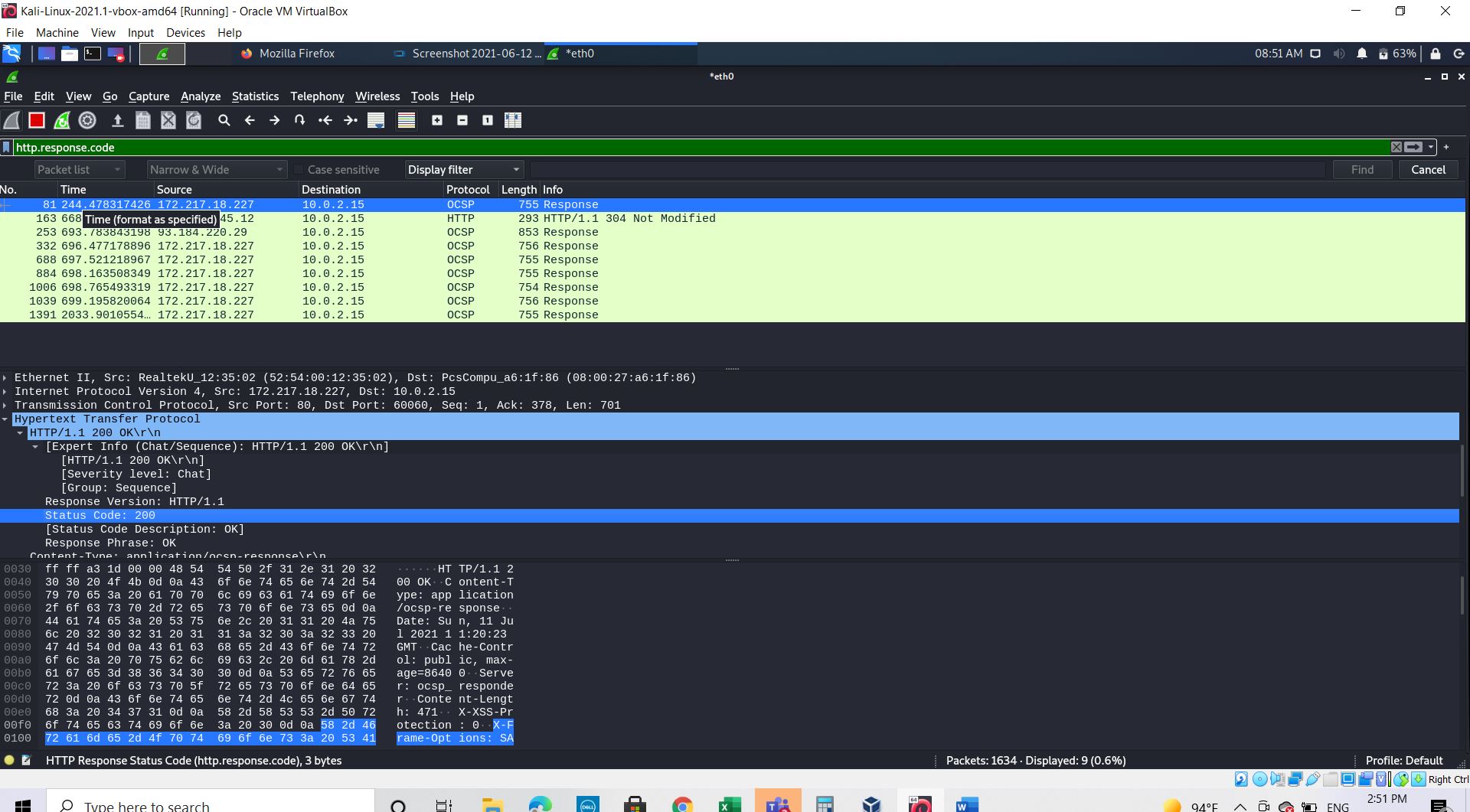


1. What is the status code returned from the server to your browser?

Using the filtering : http.response.code

ANS: status code:200

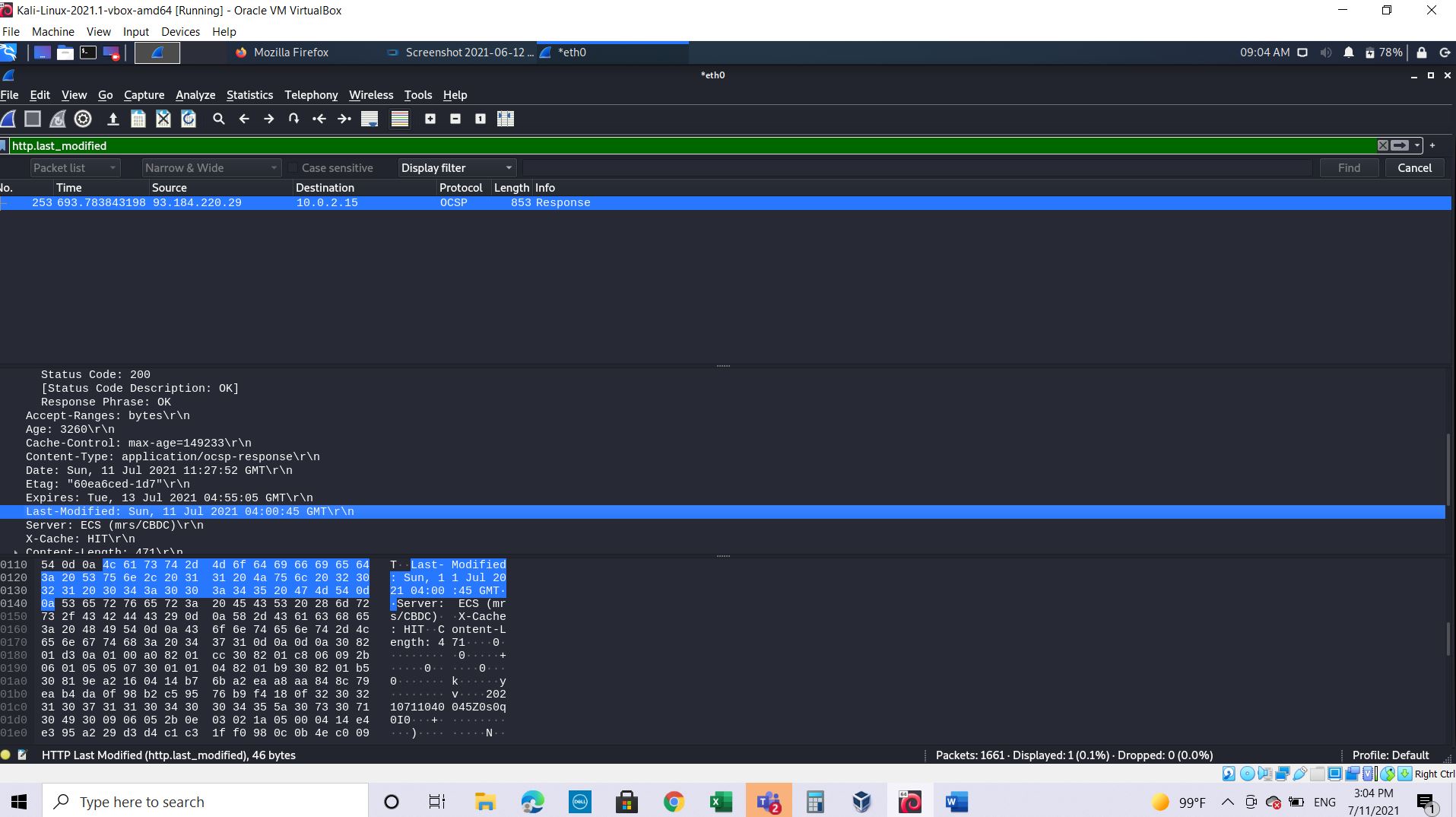
(status code information is listed in the HTTP OK message)



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

Using the filter :http.last\_modified

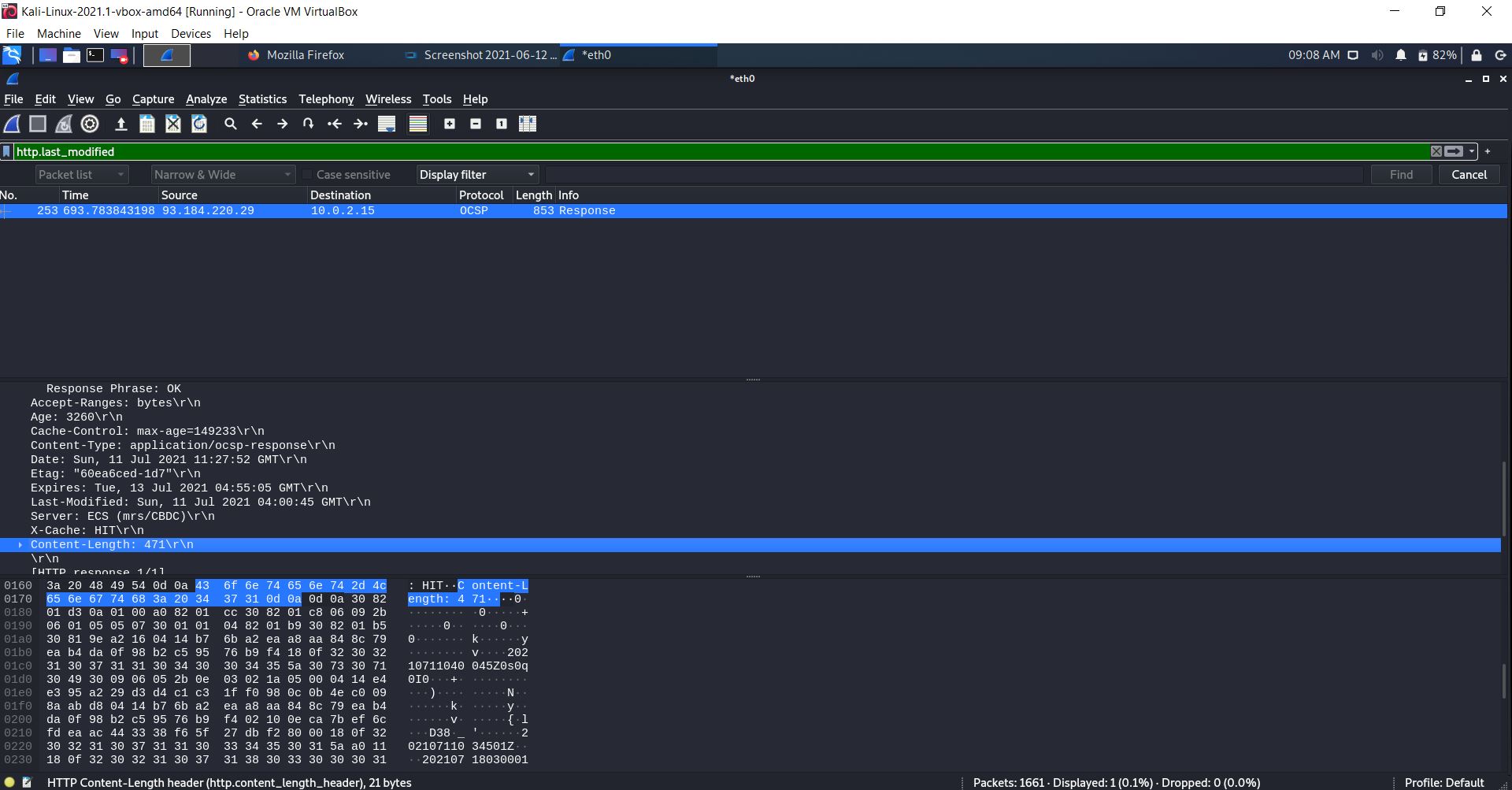
Sun, 11 Jul 2021  
 (last modified information is listed in the item ‘Last-Modified’ in the HTTP OK message)



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

Content length: 471

(Content length information is listed in the item ‘Content-Length’ in the HTTP OK message)



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.

Ans: yes , Connection