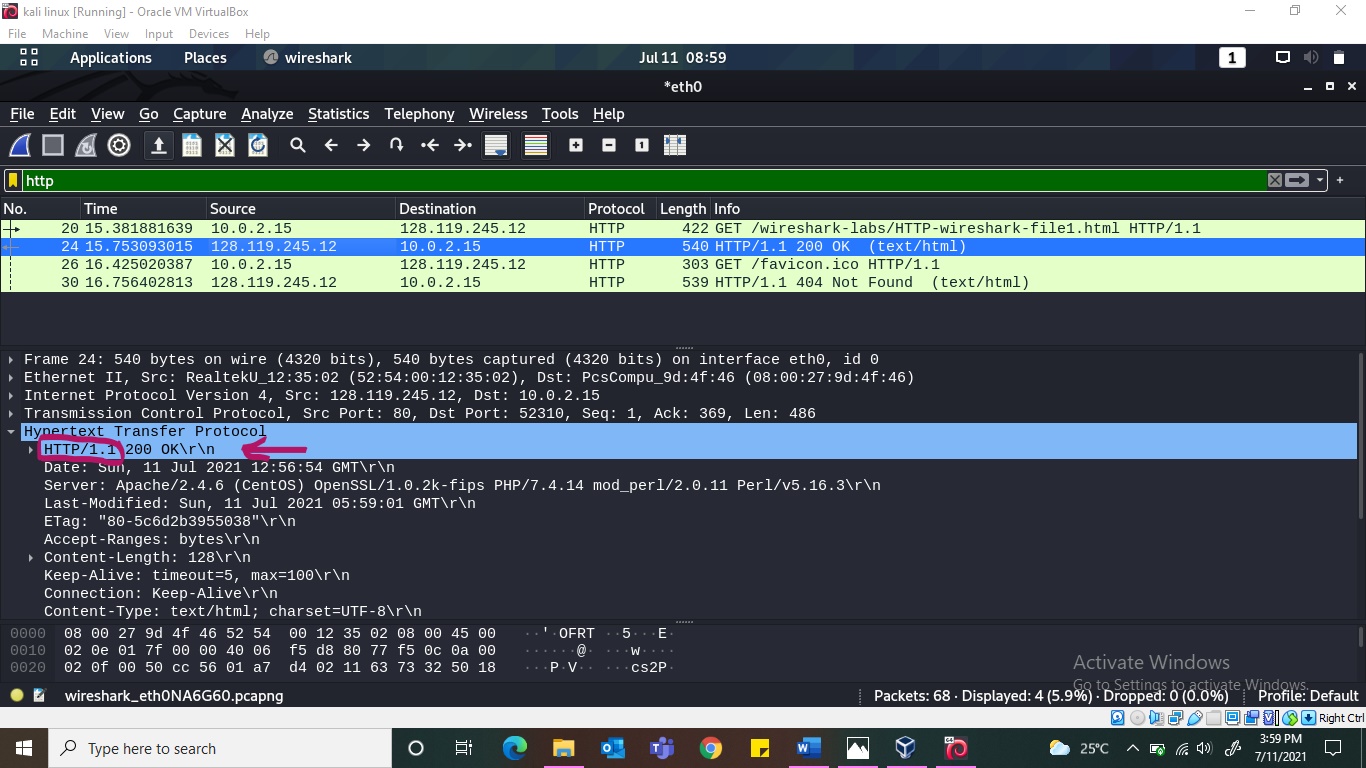
Sally Oketch.

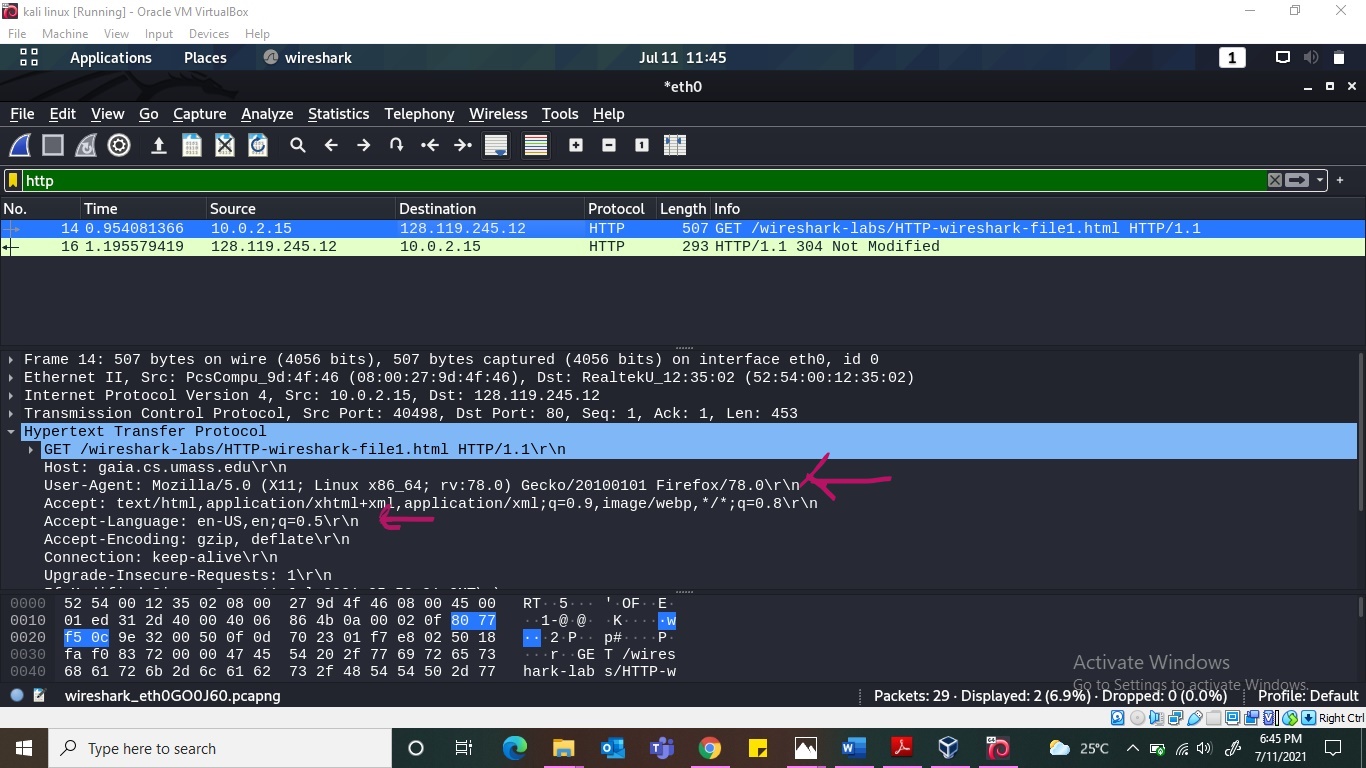
Sally.oketch@womentechsters.org

***Practical activity 6 wireshark***

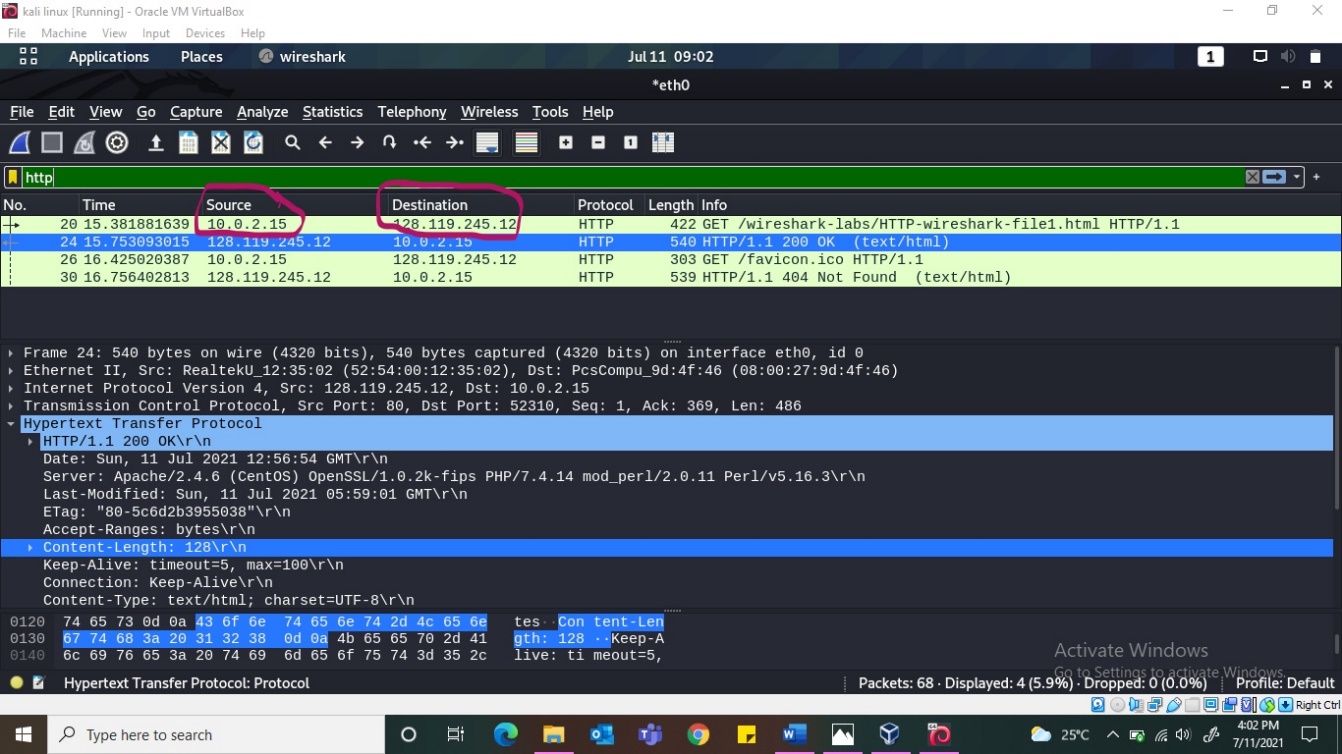
1. **Is your browser running on HTTP version 1.0 or 1.1?** HTTP/1.1



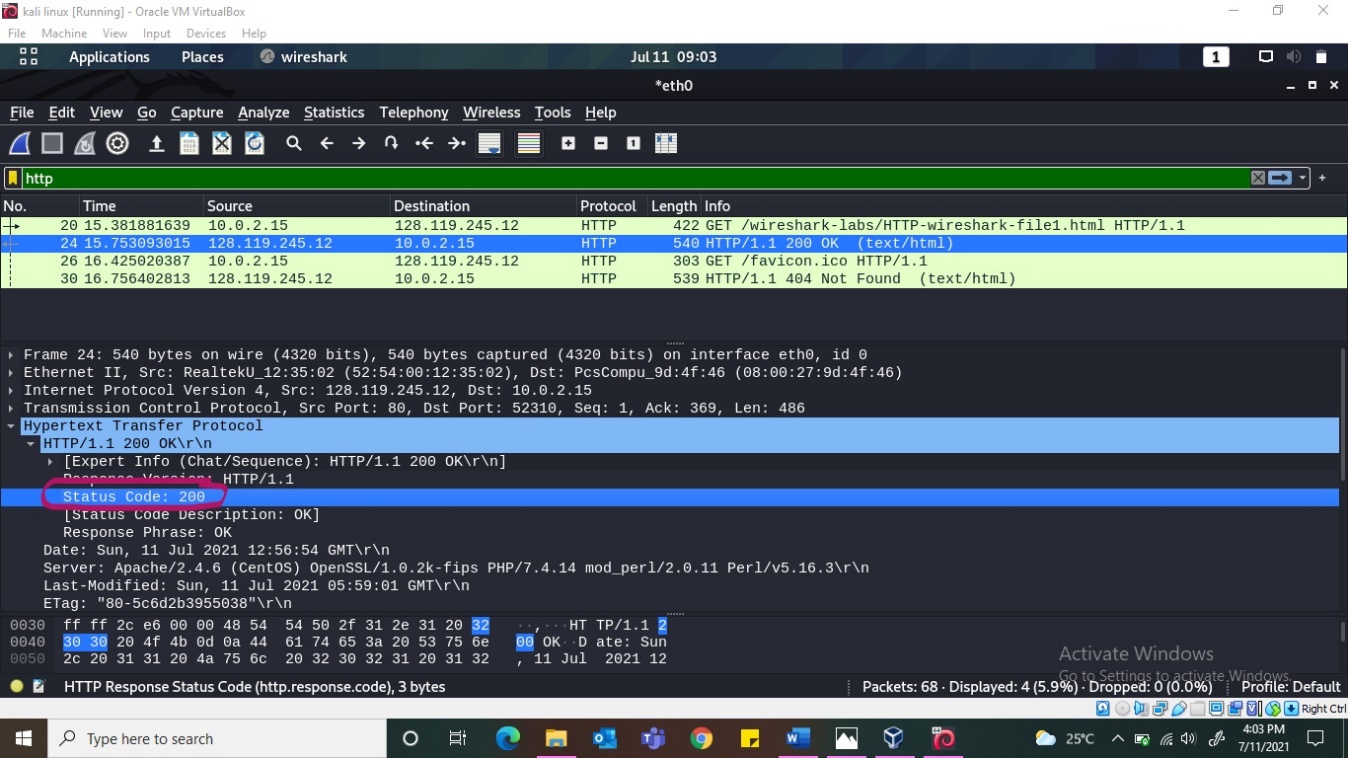
1. **What languages does your browser indicate that it can accept to the server?** en-US. **Information about the browser?** The browser is Mozilla/5.0 (x11; Linux x86\_64; rv;78.0) Gecko/20100101 Firefox/78.0

****

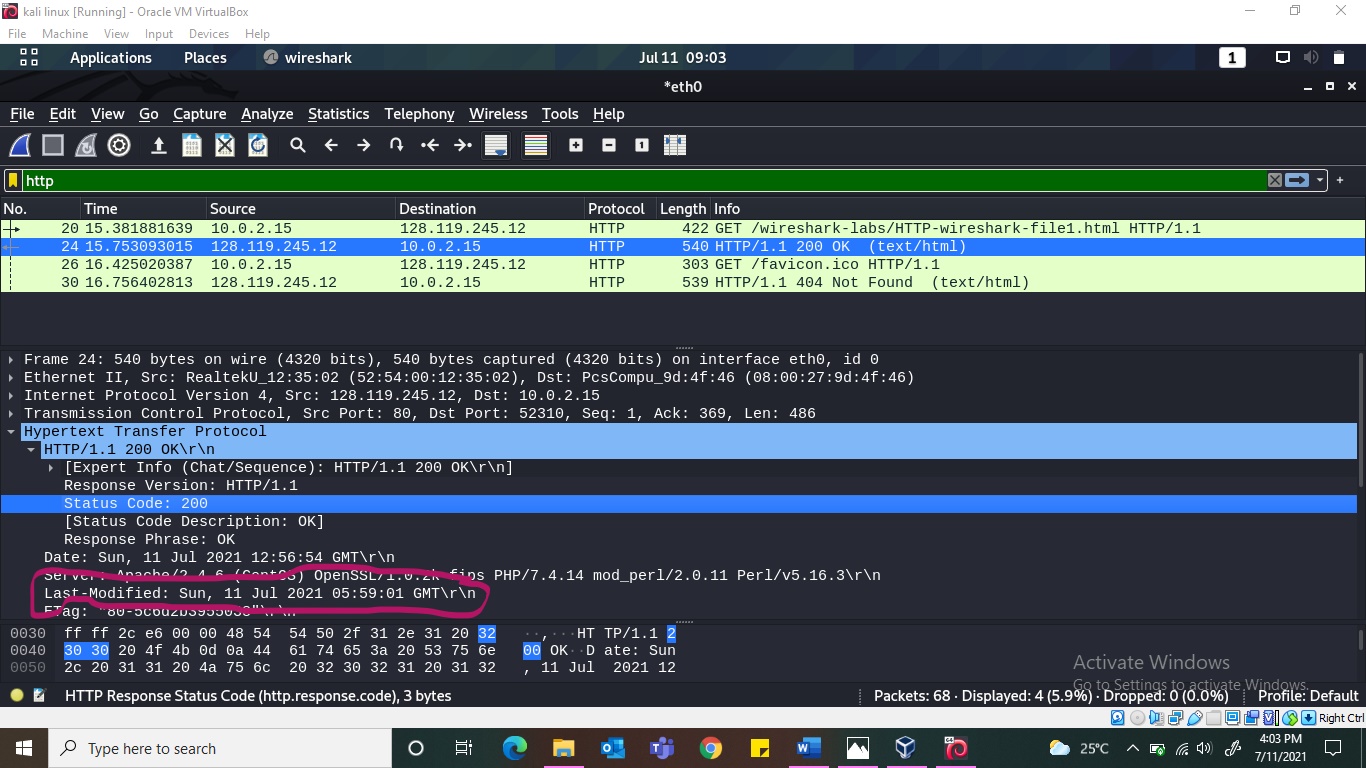
1. **What is the IP address of your computer?** 10.0.2.15 **Of gaia.cs.umass.edu server?** 128.119.245.12

****

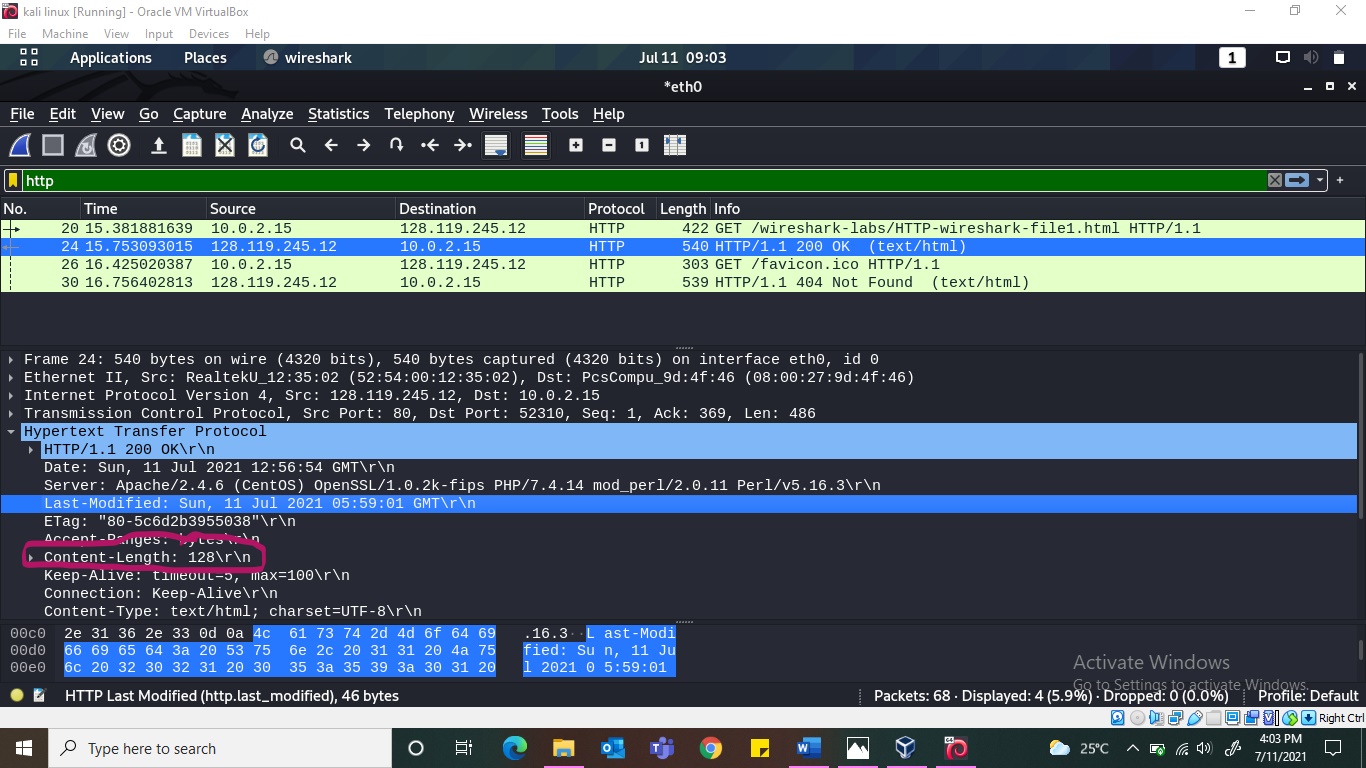
1. **What is the status code returned from the server to your browser?** 200

****

1. **When was the HTML file that you are retrieving last modified?** SUN 11 JUL 2021

****

1. **How many bytes of content are being returned to your browser?** 128

****

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?** No. All the headers are same.

**Description of what I have gathered here:**

We see things like the computer IP address being exposed (10.0.2.15) plus the server details, Apache/2.4.6(CentOs) OpenSSL/1.0.2k-fips PHP/7.4.14 mod\_perl/2.0.10 Perl/v5.16.3, which is risky. The contents of the file are also there for everyone to see or maliciously alter. The IP address of the destination is also exposed (128.119.245.12). We can see even the language the browser can accept which is en-US and the browser being used as Mozilla/5.0 (x11; Linux x86\_64; rv;78.0) Gecko/20100101 Firefox/78.0. The status code sent by the server which is 200 and content-length which is 128. HTTP is not secure all the details can be obtained by an unauthorized person because none if it is encrypted. That is why the use of HTTPS is advised.