COMPUTER NETWORKS LAB

COURSE CODE:UE19CS255

NAME:PRIYA MOHATA SRN:PES2UG19CS301

SECTION:E DATE:11/02/2021

EXPERIMENT : **Understand working of HTTP Headers**

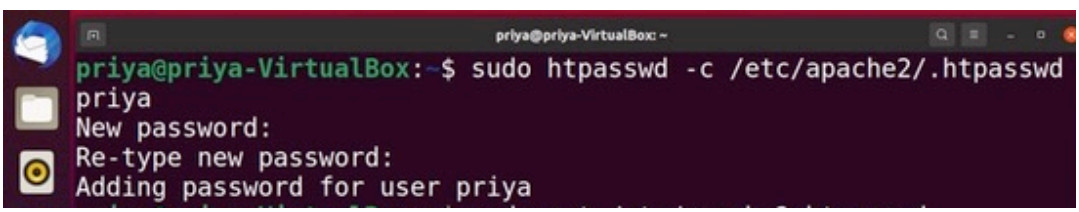
Design a web page that has one embedded page (e.g. image) and sets a cookie and enables authentication. You are required to configure the web server (e.g. apache) with authentication mechanism. Show the behaviour of conditional get when embedded objects is modified and when it is not (you can just change the create date of the embedded object).

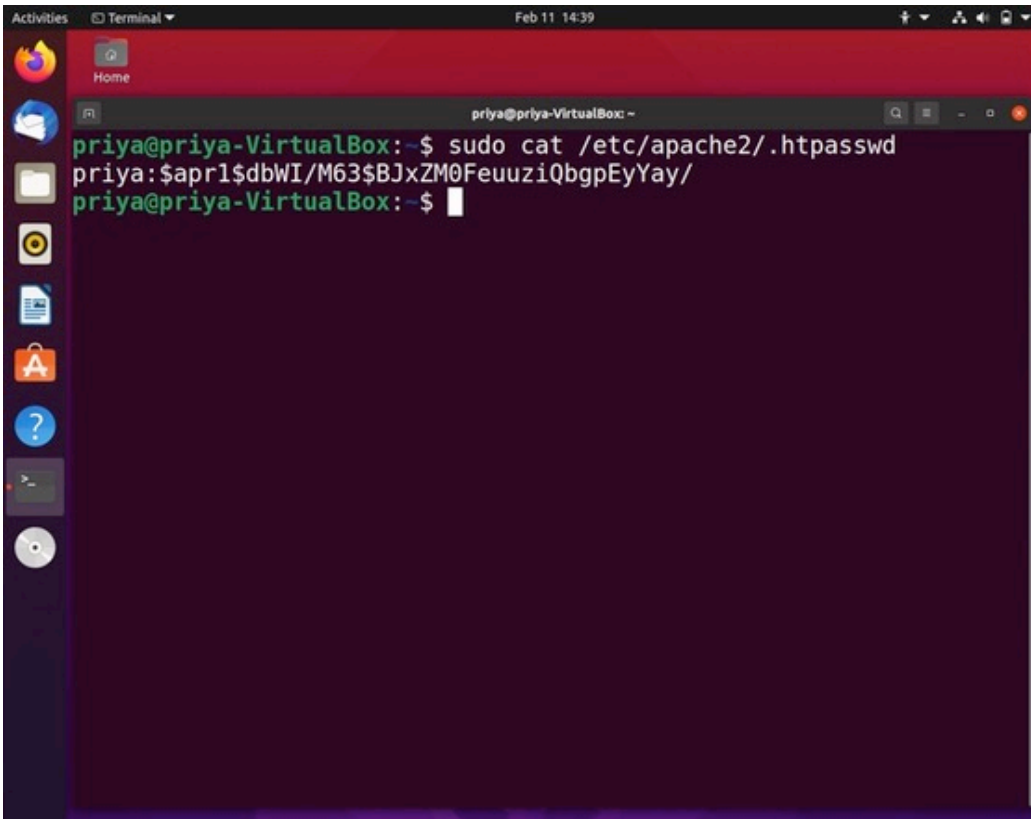
3.1 PASSWORD AUTHENTICATION

COMMAND USED : To install the apache utility **sudo apt-get install apache2 apache2-utils**

```
priya@priya-VirtualBox:~$ sudo apt-get install apache2 apache2-utils
Reading package lists... Done
Building dependency tree
Reading state information... Done
apache2 is already the newest version (2.4.46-1ubuntu1).
apache2-utils is already the newest version (2.4.46-1ubuntu1).
apache2-utils set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 79 not upgraded.
priya@priya-VirtualBox:~$
```

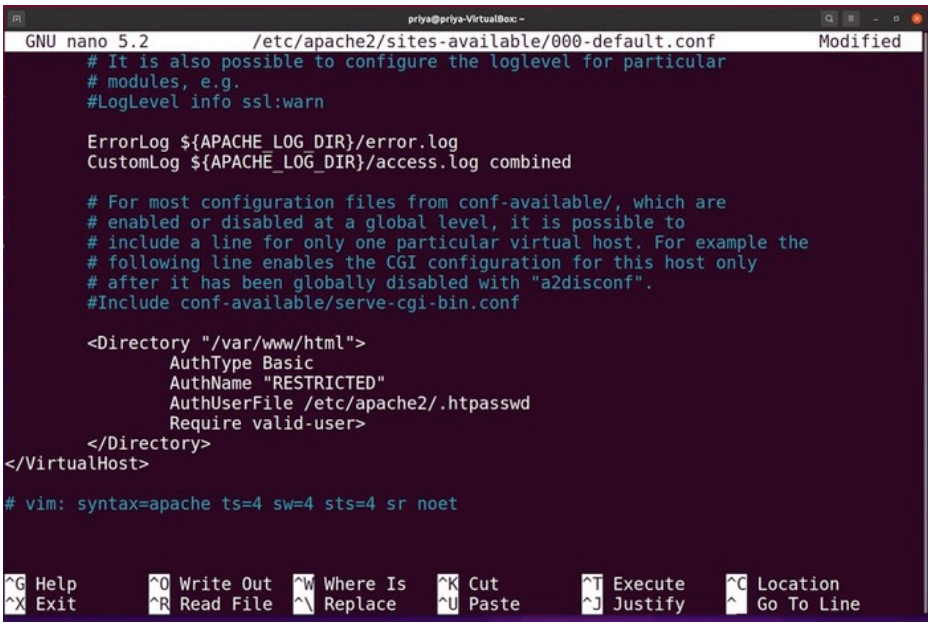
- To enable basic authentication for HTTP, we need to generate a password file. This file can be generated using the htpasswd command.
- Using **sudo htpasswd -c /etc/apache2/.htpasswd username** we can set a password for the given user username and write it into the **.htpasswd** configuration file.
- The cat command can be used to view the encrypted password file, which is encrypted using the Data Encryption Standard algorithm.




Activities
Terminal
Feb 11 14:39
Home
priya@priya-VirtualBox: ~
priya@priya-VirtualBox:~$ sudo cat /etc/apache2/.htpasswd
priya:$apr1$dbWI/M63$BJxZM0FeuuziQbgpEyYay/
priya@priya-VirtualBox:~$

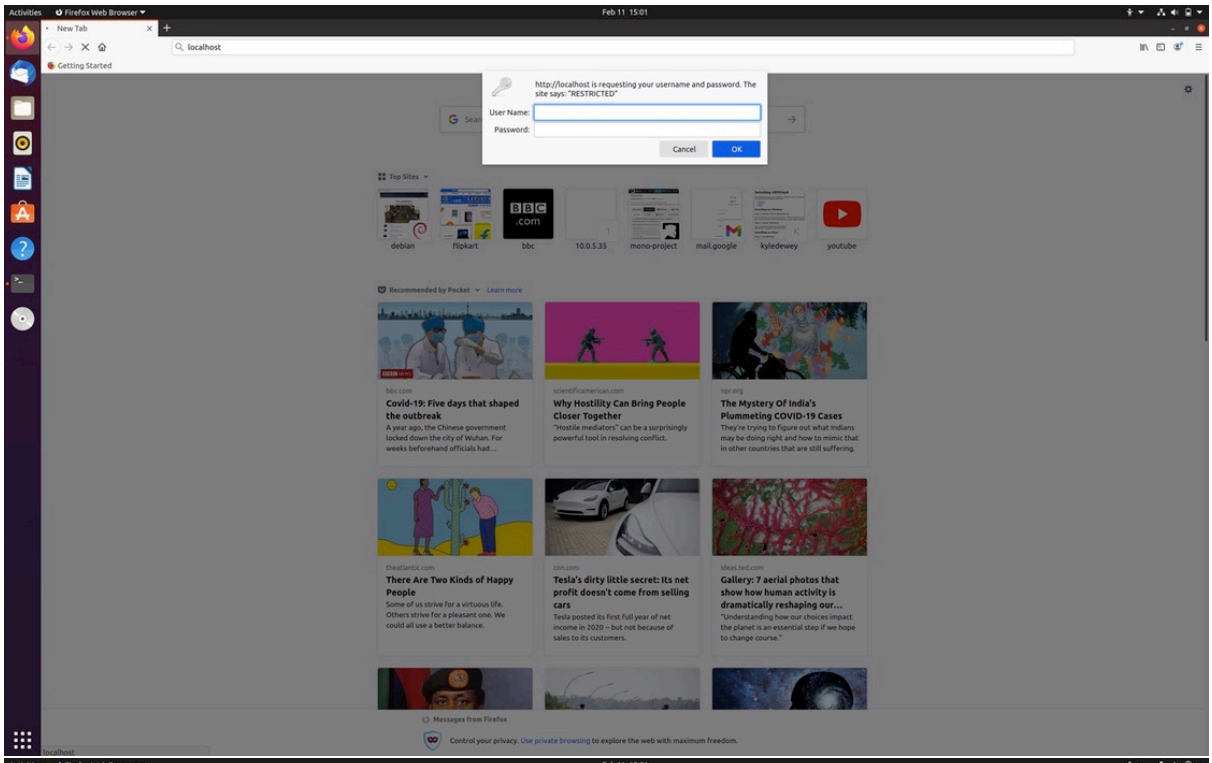
3.2 APACHE SERVER AUTHENTICATION

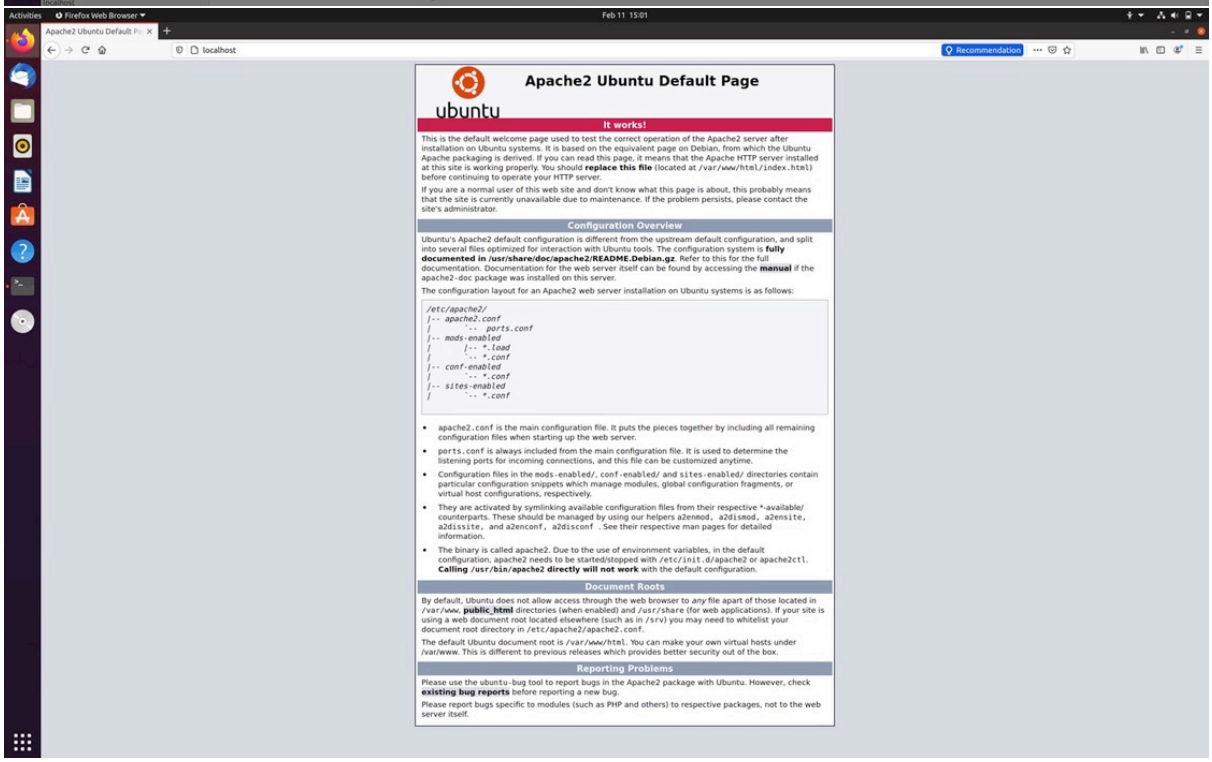
- To enable password authentication in the server, we need to modify the Apache configuration file.
- This can be done using **sudo nano /etc/apache2/sites-available/000-default.conf**
- Password authentication is added to the **/var/www/html** directory which is the localhost home directory so that all files hosted here will require authentication to access.
- To activate the authentication and policy, we need to restart the server using **sudo service apache2 restart.**



3.3 ACCESSING LOCALHOST

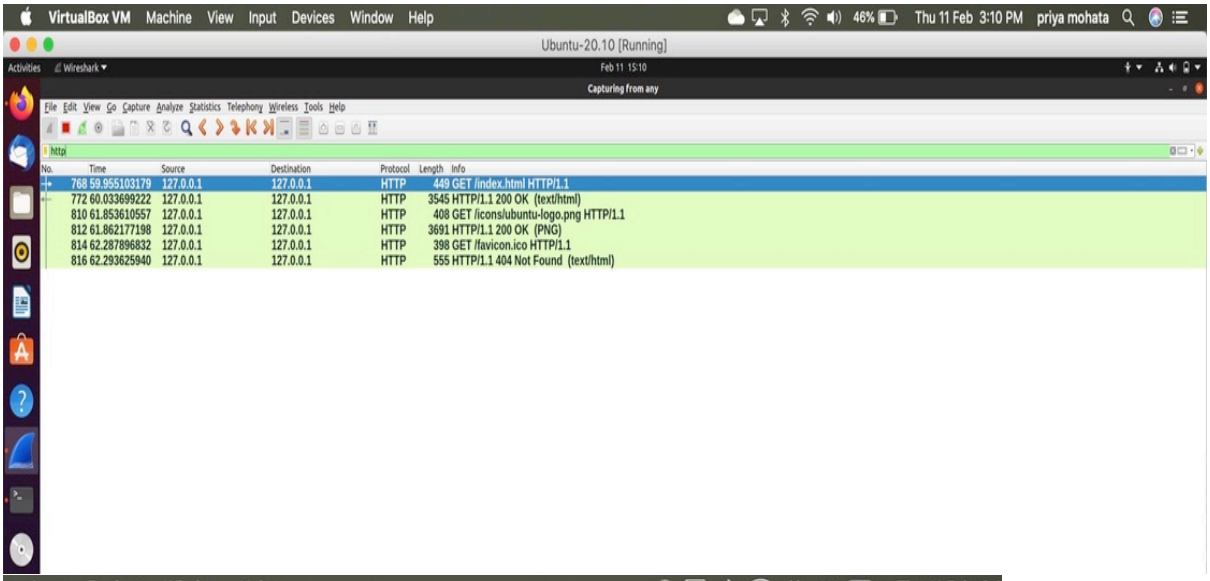
- We can now access localhost only after entering the username and password set earlier
- These credentials are entered on the browser window.

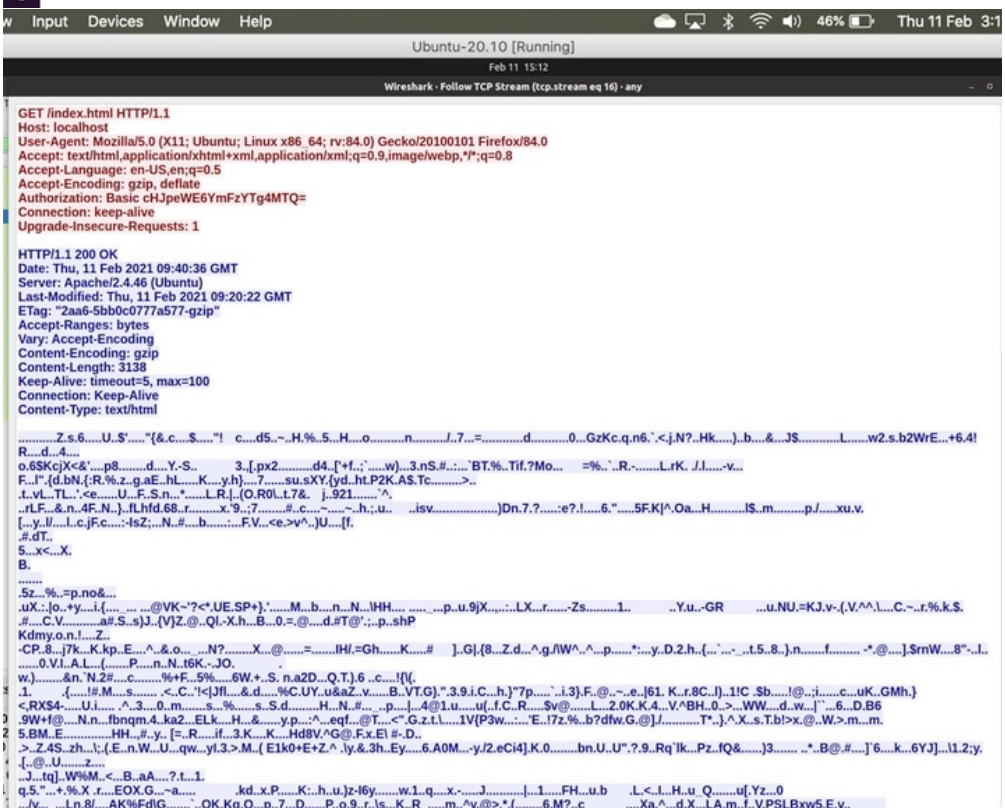




3.4 WIRESHARK PACKET CAPTURE

- Wireshark can be used to capture the packets sent on the network. The first GET request corresponding to the HTML file is analysed and its TCP Stream is expanded, and parameters examined.

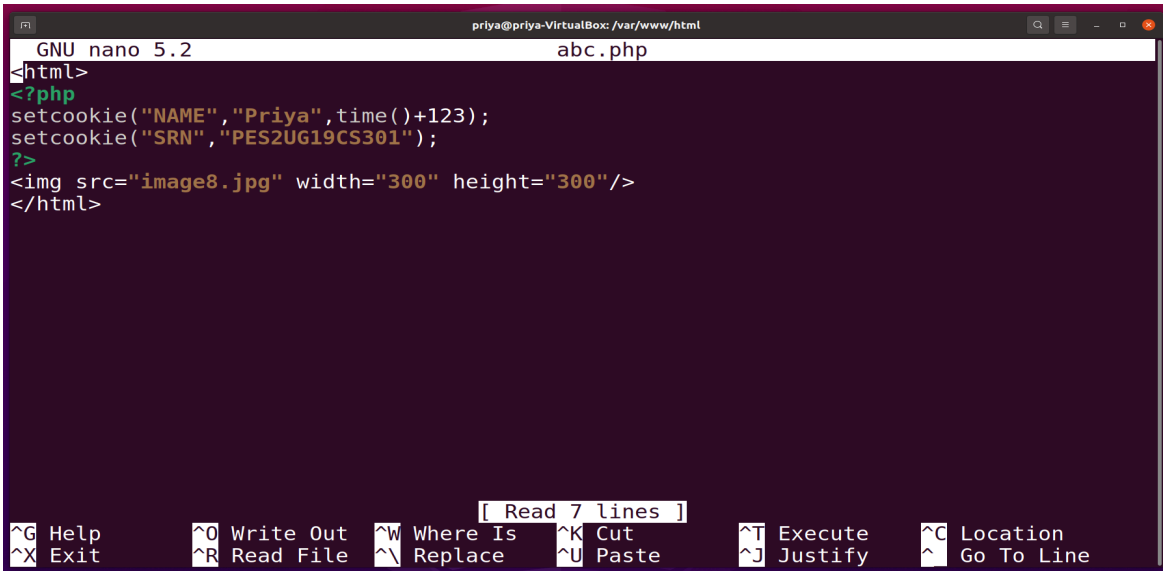




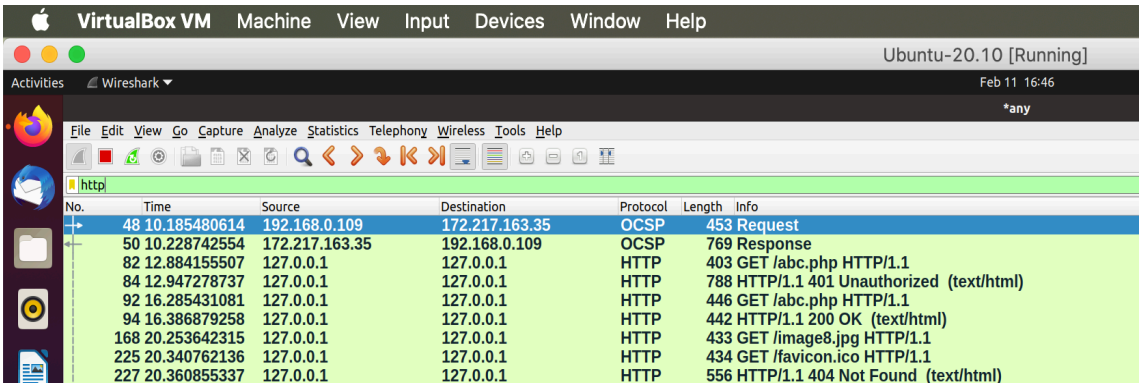
3.5 SETTING COOKIES

- We can set cookies using a PHP script and the **setcookie(name, value, expire_time)** function
- When this file is requested by the browser a cookie will be set

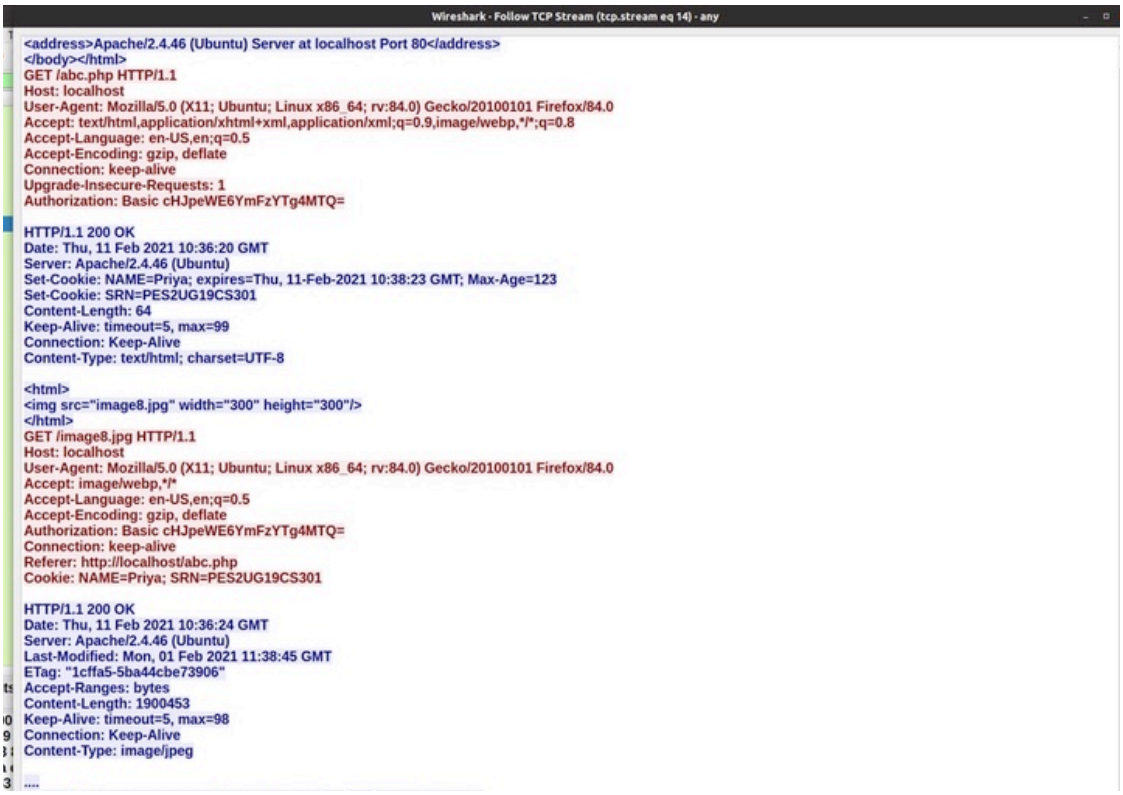
CODE:



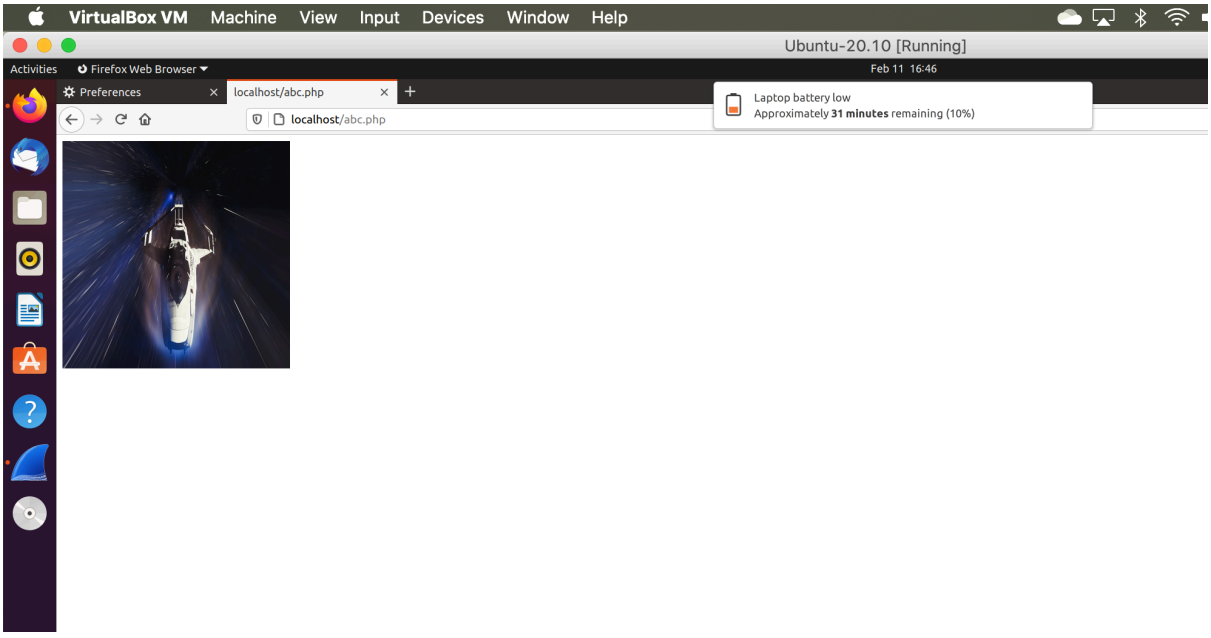
abc.php



Request to localhost/abc.php



The cookie is set as shown in the above screenshot.

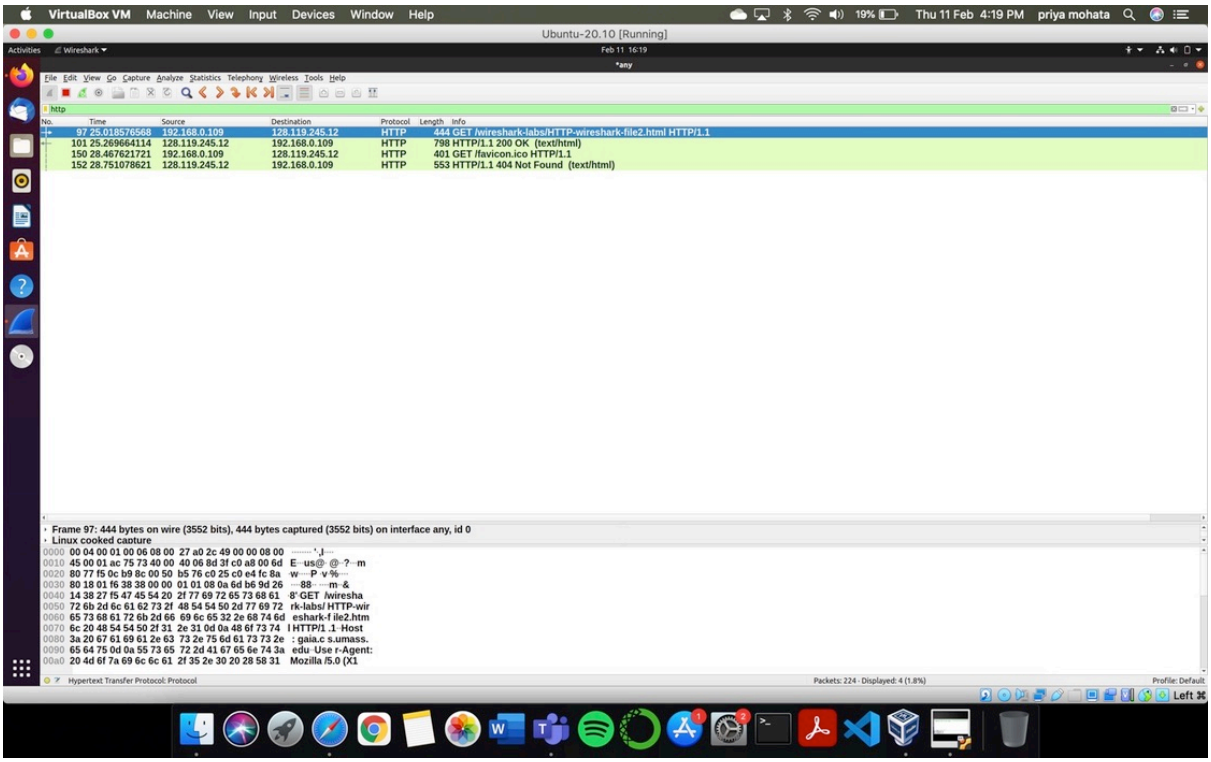


localhost/abc.php

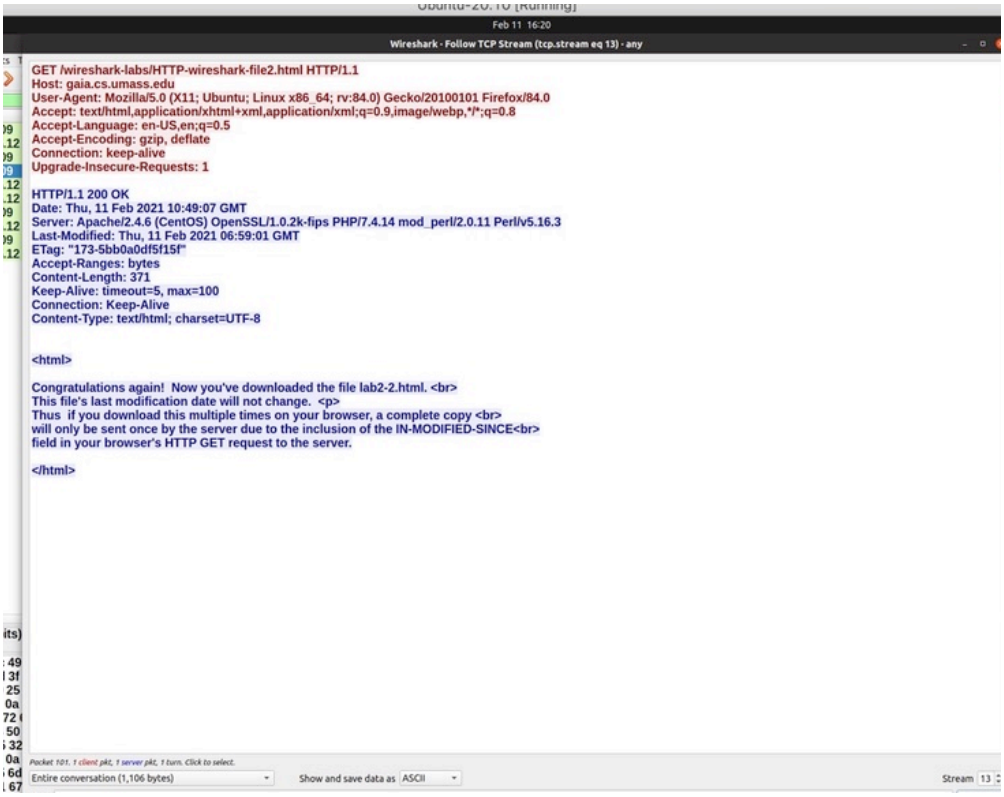
3.6 CONDITIONAL GET : IF-MODIFIED SINCE

- Start up your web browser, and make sure your browser's cache is cleared, as discussed above.
- Start up the Wireshark packet sniffer.
- Enter the following URL into your browser http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html
- Your browser should display a very simple five-line HTML file.
- Quickly enter the same URL into your browser again (or simply select the refresh button on your browser)
- Stop Wireshark packet capture, and enter "http" in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet- listing window.
- An HTML page is requested by the client and the HTML file is obtained along with a 200 OK response status

ON ENTERING http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html

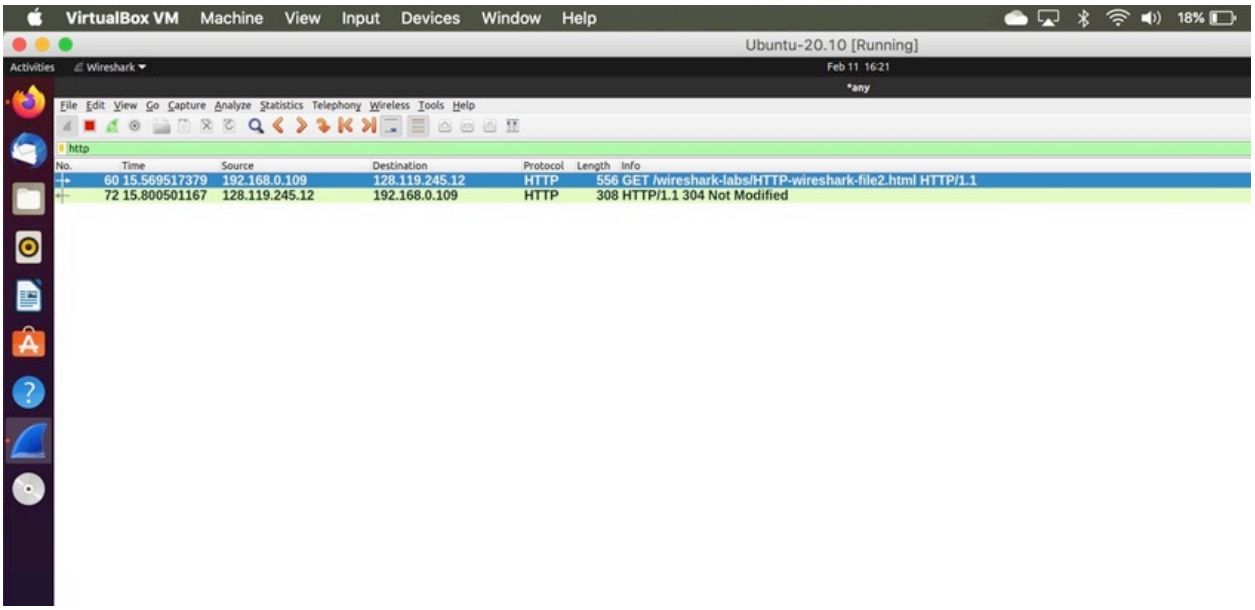


WIRESHARK PACKET CAPTURE

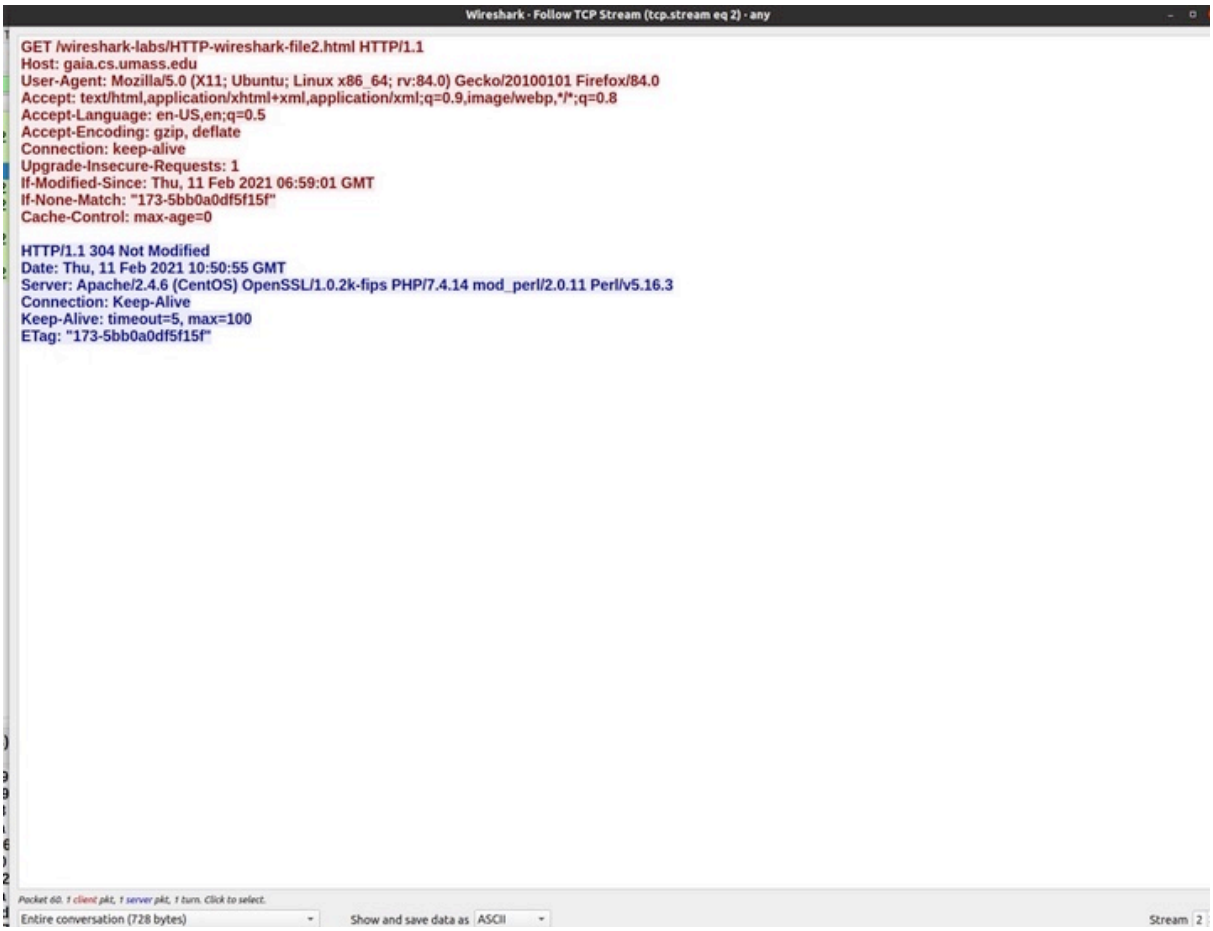


TCP STREAM

- A conditional HTTP response is one that carries the resource only it had been modified since the last GET request by the client.
- The HTTP header **If-Modified-Since** is one way to implement Conditional GET
- The server checks the **If-Modified-Since** header value and resends the resource only if it has been modified since the timestamp in the header
- If it has not been modified, a **304 Not Modified** status code is sent back.



ON REFRESHING THE WEBSITE


Wireshark · Follow TCP Stream (tcp.stream eq 2) · any
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Host: gaia.cs.umass.edu
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/84.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
If-Modified-Since: Thu, 11 Feb 2021 06:59:01 GMT
If-None-Match: "173-5bb0a0df5f15f"
Cache-Control: max-age=0
HTTP/1.1 304 Not Modified
Date: Thu, 11 Feb 2021 10:50:55 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
ETag: "173-5bb0a0df5f15f"
Packet 60. 1 client pkt, 1 server pkt, 1 turn. Click to select.
Entire conversation (728 bytes)
Show and save data as ASCII
Stream 2

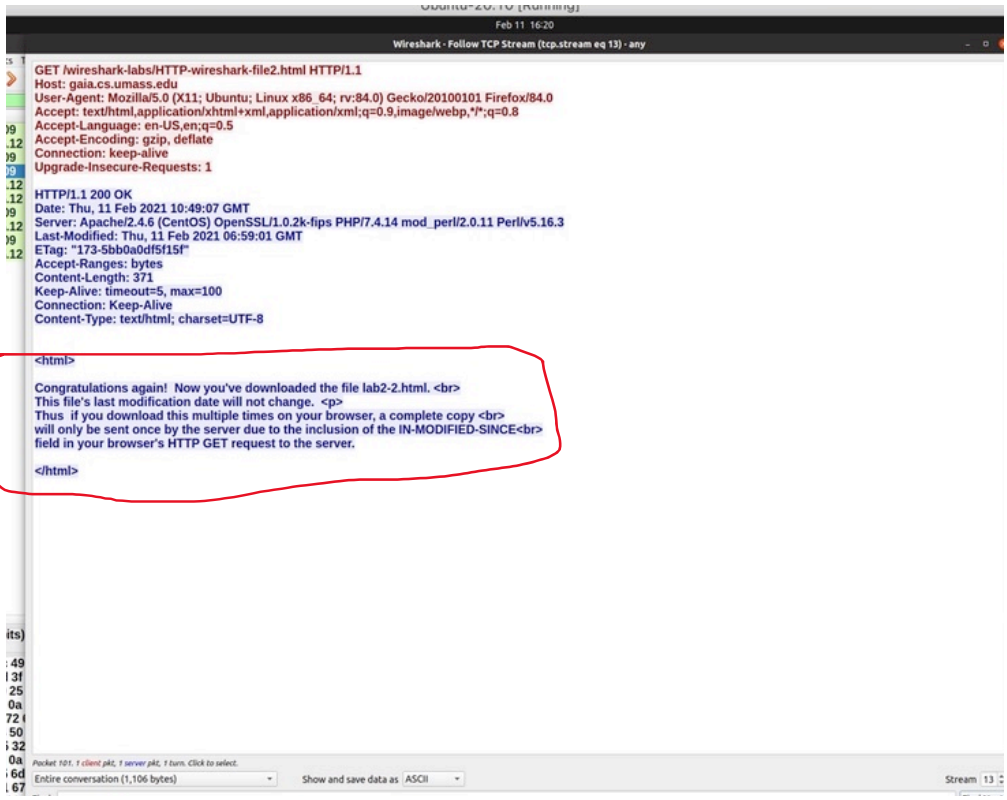
3.7 OBSERVATIONS

QUESTION 1 : Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

ANSWER : No, in the first request after clearing the cache we don’t see in “IF-MODIFIED-SINCE” line in the HTTP GET.

QUESTION 2 :Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

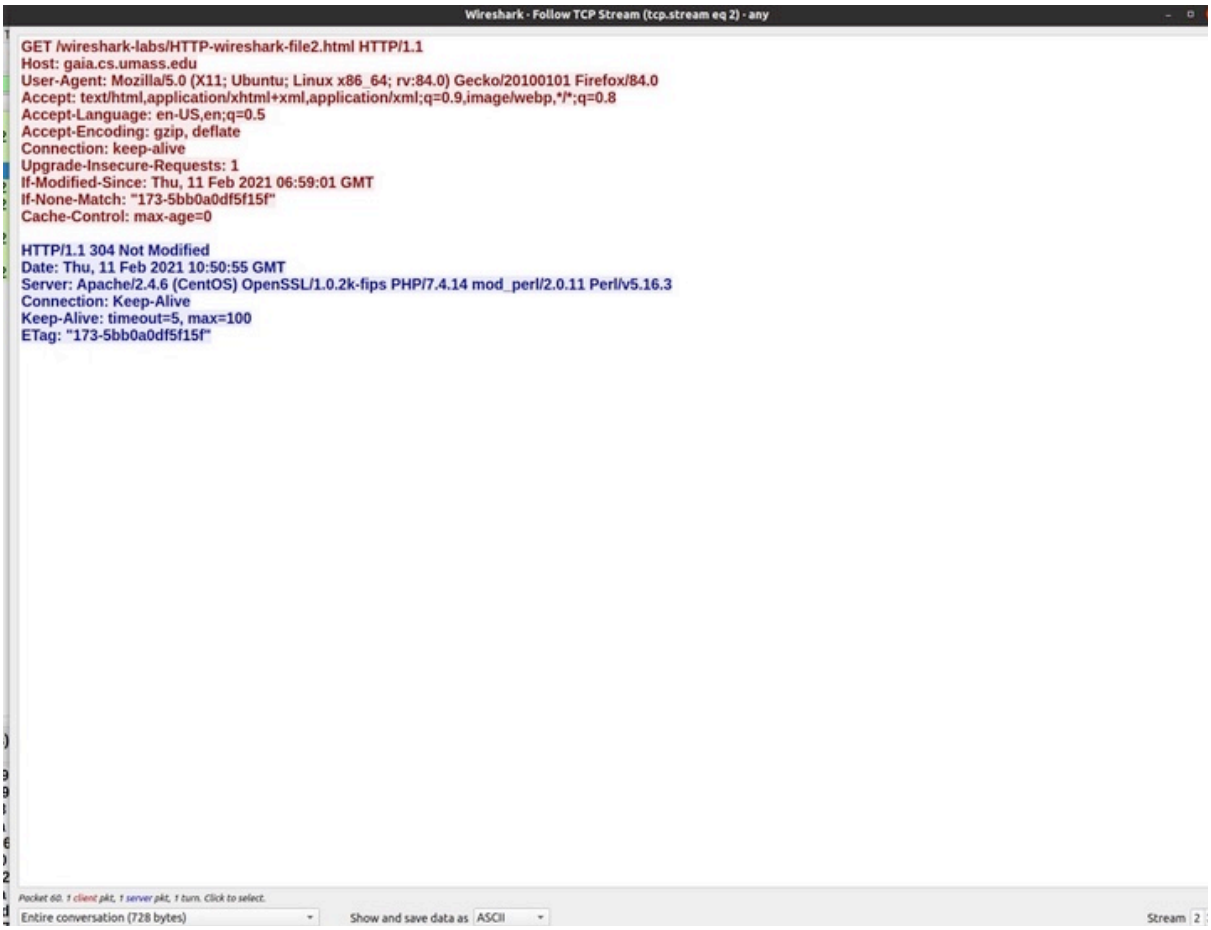
Yes, we can see from the screenshot below



QUESTION 3: Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

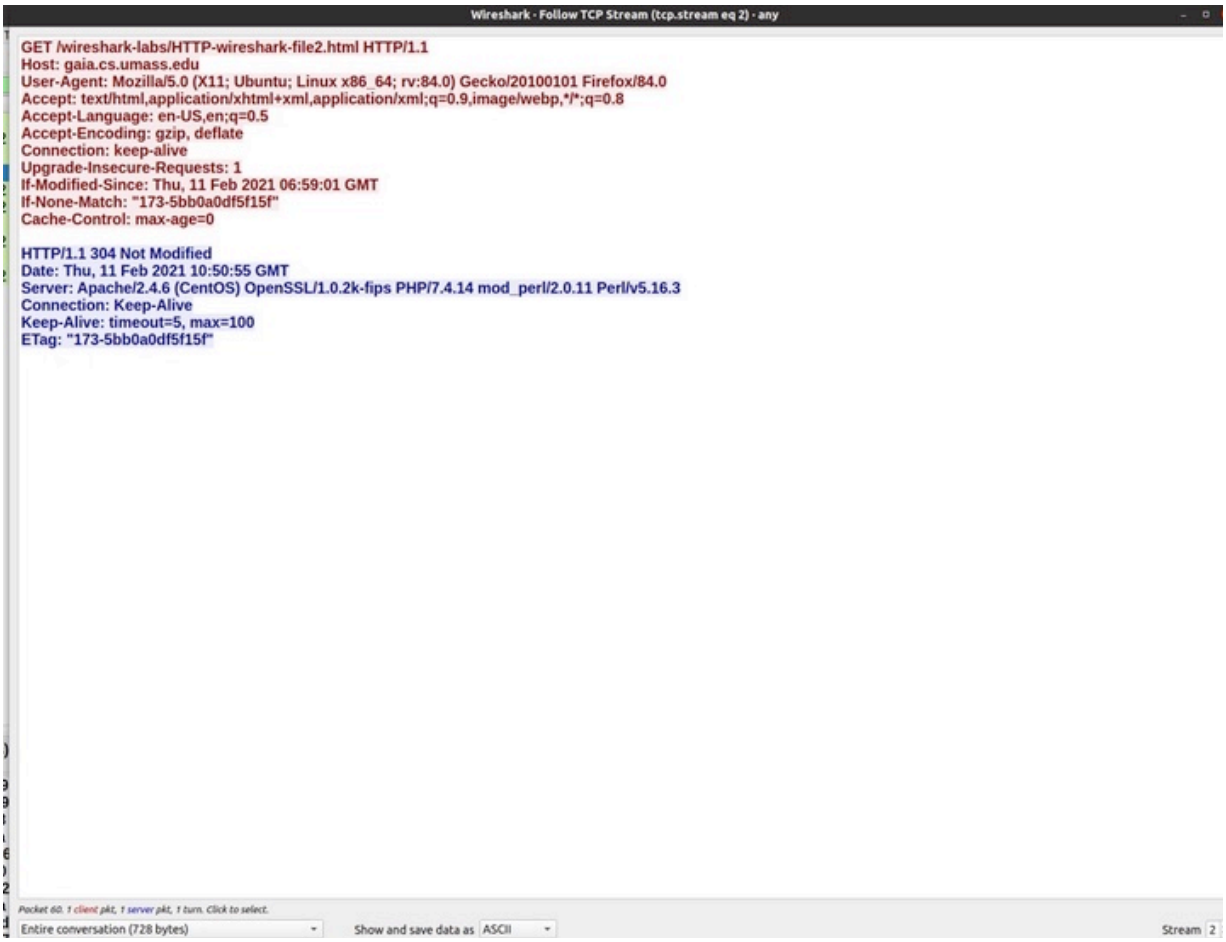
ANSWER : IF-MODIFIED-SINCE: *date is mentioned*

Example IF-MODIFIED-SINCE:Thu,11 Feb 2021 06:59:01 GMT



QUESTION 4 : What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

ANSWER : The HTTP CODE that was returned from the server in response to the second HTTP GET was 304 Not Modified. No, the server didn’t return the contents of the file as it is seen in the screenshot below.


Wireshark · Follow TCP Stream (tcp.stream eq 2) · any
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Host: gaia.cs.umass.edu
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/84.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
If-Modified-Since: Thu, 11 Feb 2021 06:59:01 GMT
If-None-Match: "173-5bb0a0df5f15f"
Cache-Control: max-age=0
HTTP/1.1 304 Not Modified
Date: Thu, 11 Feb 2021 10:50:55 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
ETag: "173-5bb0a0df5f15f"
Packet 60. 1 client pkt, 1 server pkt, 1 turn. Click to select.
Entire conversation (728 bytes)
Show and save data as ASCII
Stream 2