Name: Khushei Meghana Meda

SRN: PES1201800416

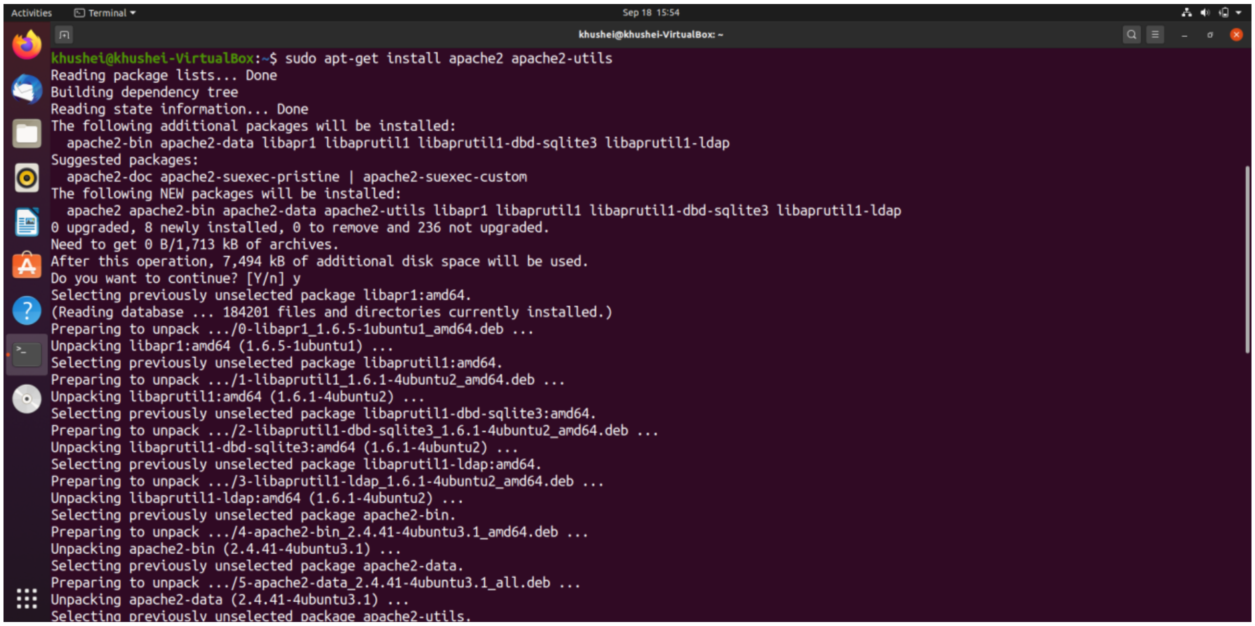
Week number: 3

Name of experiment: Understand working of HTTP Headers

Date: 19-09-2020

Objectives of the experiment: To understand working of HTTP headers, Conditional Get: If-Modified-Since, HTTP Cookies: Cookie and Set-Cookie, Authentication: Auth-Basic

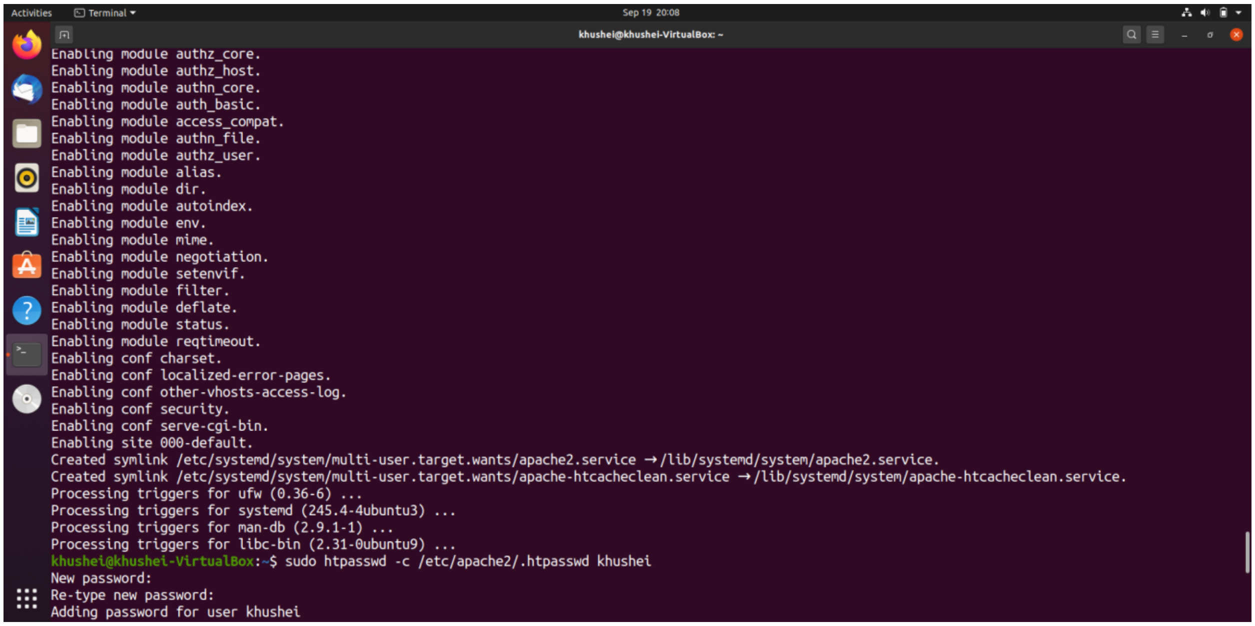
Steps of Execution (for Password Authentication)
1. Executing the below commands on the terminal.
--> To update and integrate the existing softwares
sudo apt-get update
--> To install the apache utility
sudo apt-get install apache2 apache2-utils



```
khushei@khushei-VirtualBox:~$ sudo apt-get install apache2 apache2-utils
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
0 upgraded, 8 newly installed, 0 to remove and 236 not upgraded.
Need to get 0 B/1,713 kB of archives.
After this operation, 7,494 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Selecting previously unselected package libapr1:amd64.
(Reading database ... 184201 files and directories currently installed.)
Preparing to unpack .../0-libapr1_1.6.5-1ubuntu1_amd64.deb ...
Unpacking libapr1:amd64 (1.6.5-1ubuntu1) ...
Selecting previously unselected package libaprutil1:amd64.
Preparing to unpack .../1-libaprutil1_1.6.1-4ubuntu2_amd64.deb ...
Unpacking libaprutil1:amd64 (1.6.1-4ubuntu2) ...
Selecting previously unselected package libaprutil1-dbd-sqlite3:amd64.
Preparing to unpack .../2-libaprutil1-dbd-sqlite3_1.6.1-4ubuntu2_amd64.deb ...
Unpacking libaprutil1-dbd-sqlite3:amd64 (1.6.1-4ubuntu2) ...
Selecting previously unselected package libaprutil1-ldap:amd64.
Preparing to unpack .../3-libaprutil1-ldap_1.6.1-4ubuntu2_amd64.deb ...
Unpacking libaprutil1-ldap:amd64 (1.6.1-4ubuntu2) ...
Selecting previously unselected package apache2-bin.
Preparing to unpack .../4-apache2-bin_2.4.41-4ubuntu3.1_amd64.deb ...
Unpacking apache2-bin (2.4.41-4ubuntu3.1) ...
Selecting previously unselected package apache2-data.
Preparing to unpack .../5-apache2-data_2.4.41-4ubuntu3.1_all.deb ...
Unpacking apache2-data (2.4.41-4ubuntu3.1) ...
Selecting previously unselected package apache2-utils.
```

--> Provide username and password to set authentication
sudo htpasswd -c /etc/apache2/.htpasswd ANY_USERNAME

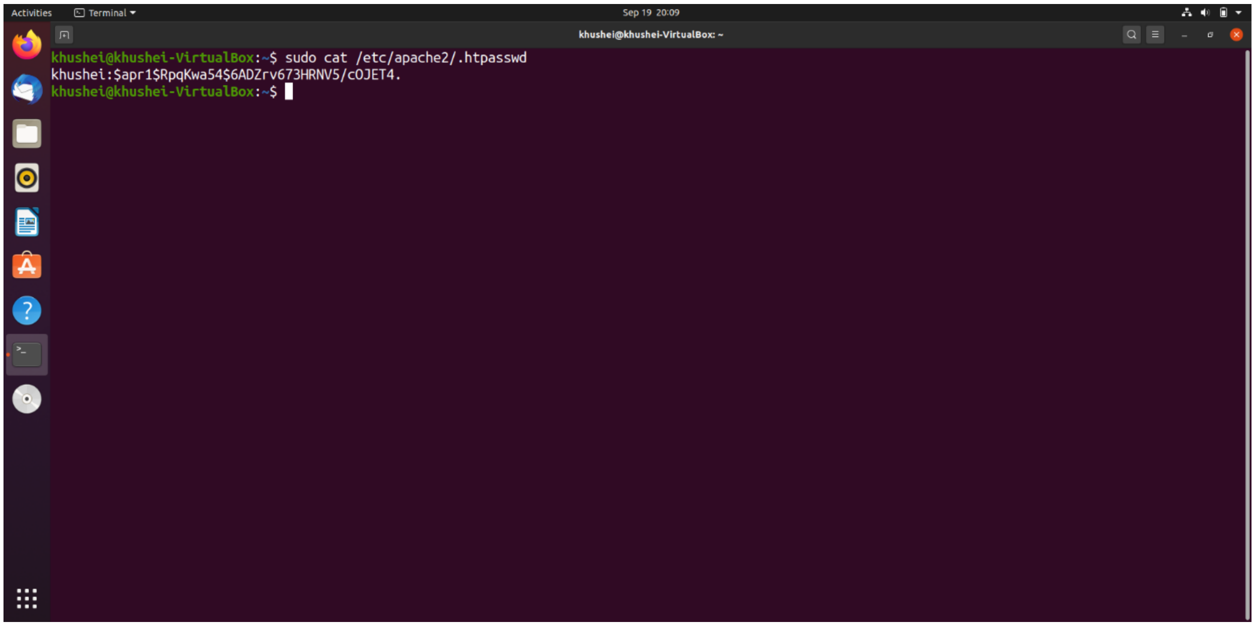
I have given the username as khushei



```
Enabling module authz_core.
Enabling module authz_host.
Enabling module authn_core.
Enabling module auth_basic.
Enabling module access_compat.
Enabling module authn_file.
Enabling module authz_user.
Enabling module alias.
Enabling module dir.
Enabling module autoindex.
Enabling module env.
Enabling module mime.
Enabling module negotiation.
Enabling module setenvif.
Enabling module filter.
Enabling module deflate.
Enabling module status.
Enabling module reqtimeout.
Enabling conf charset.
Enabling conf localized-error-pages.
Enabling conf other-vhosts-access-log.
Enabling conf security.
Enabling conf serve-cgi-bin.
Enabling site 000-default.
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service →/lib/systemd/system/apache2.service.
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcacheclean.service →/lib/systemd/system/apache-htcacheclean.service.
Processing triggers for ufw (0.36-6) ...
Processing triggers for systemd (245.4-4ubuntu3) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9) ...
khushei@khushei-VirtualBox:~$ sudo htpasswd -c /etc/apache2/.htpasswd khushei
New password:
Re-type new password:
Adding password for user khushei
```

--> View the authentication

sudo cat /etc/apache2/.htpasswd

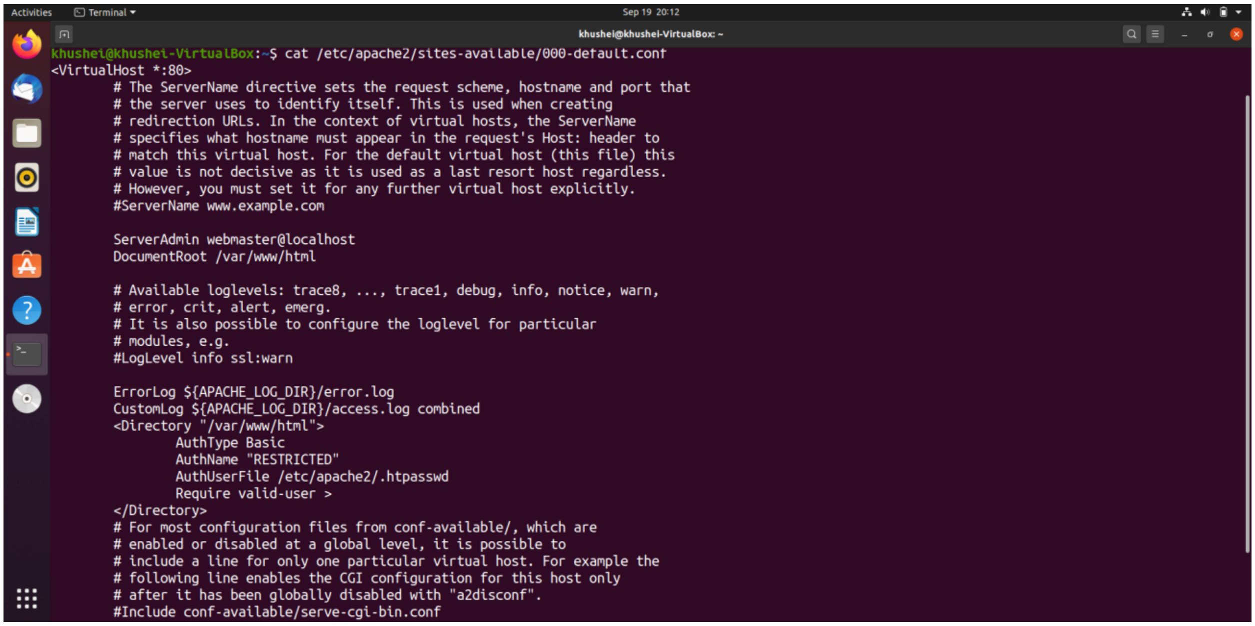


```
khushei@khushei-VirtualBox:~$ sudo cat /etc/apache2/.htpasswd
khushei:$apr1$RpqKwa54$6ADZrv673HRNV5/cOJET4.
khushei@khushei-VirtualBox:~$ 
```

2. To setup the authentication phase, execute the following commands. Configuring Access control within the Virtual Host Definition.

--> Opening the file for setting authentication

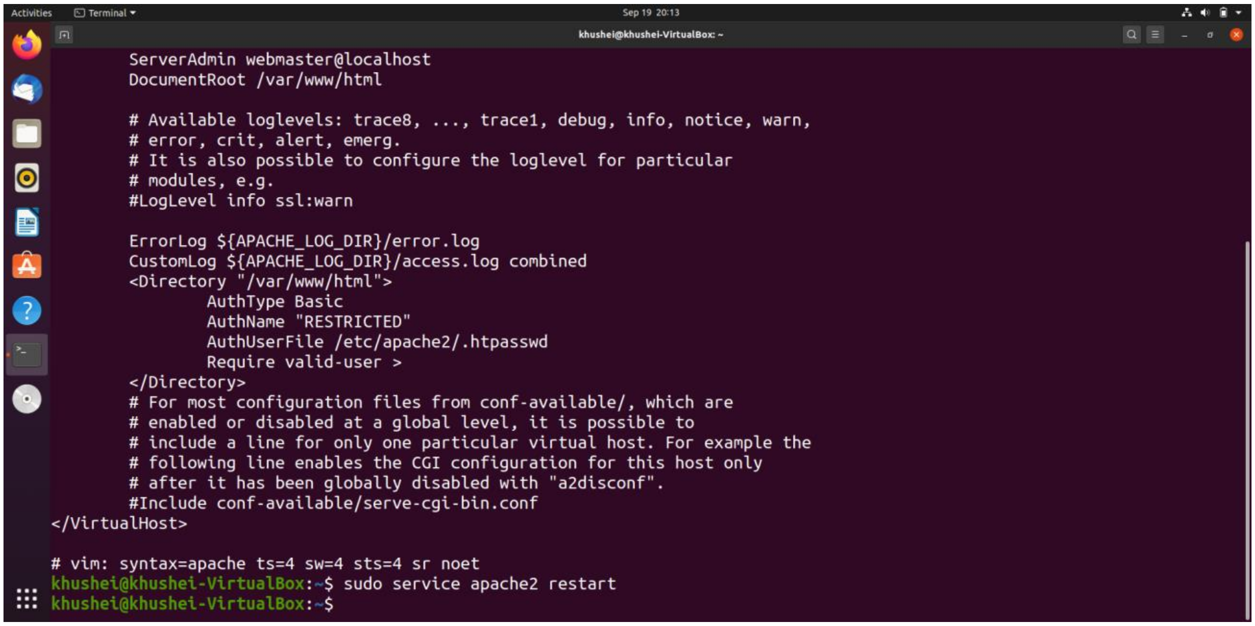
sudo nano /etc/apache2/sites-available/000-default.conf



```
khushei@khushei-VirtualBox:~$ cat /etc/apache2/sites-available/000-default.conf
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
        <Directory "/var/www/html">
                AuthType Basic
                AuthName "RESTRICTED"
                AuthUserFile /etc/apache2/.htpasswd
                Require valid-user >
        </Directory>
        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
```

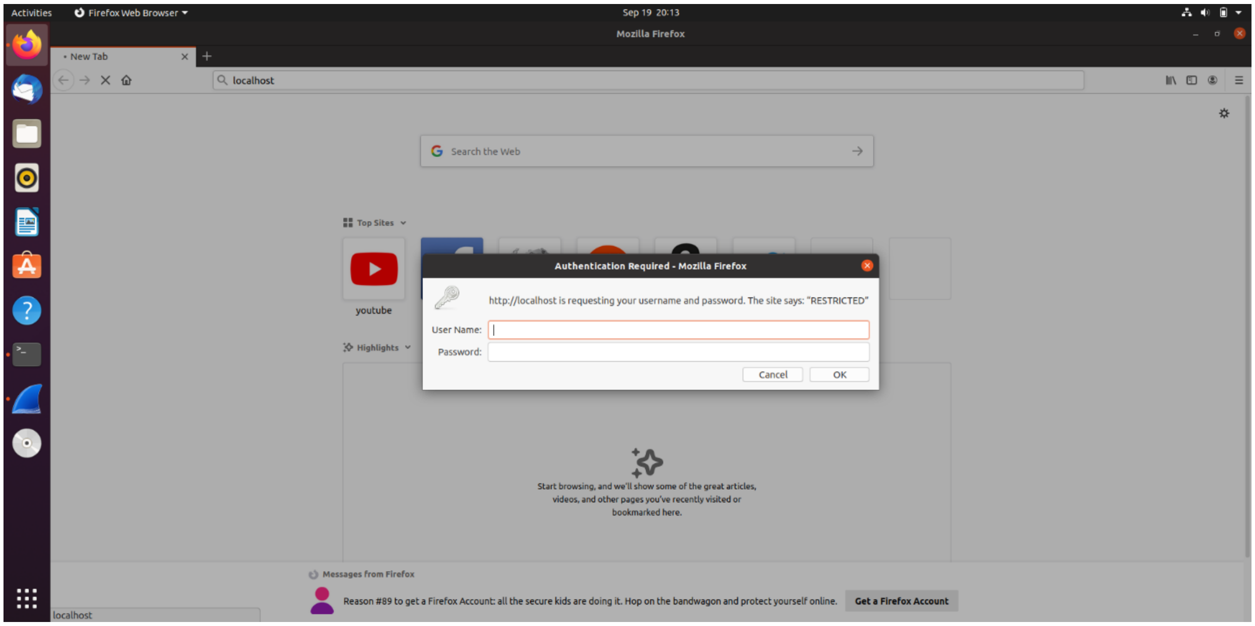
3. Password policy implementation is done by restarting the server as:

sudo service apache2 restart



```
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
        <Directory "/var/www/html">
                AuthType Basic
                AuthName "RESTRICTED"
                AuthUserFile /etc/apache2/.htpasswd
                Require valid-user >
        </Directory>
        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
khushei@khushei-VirtualBox:~$ sudo service apache2 restart
khushei@khushei-VirtualBox:~$
```

4. The localhost is then accessed using the Firefox browser requiring a username and a password set during the authentication phase.


Activities
Firefox Web Browser
Sep 19 20:13
Mozilla Firefox
New Tab
localhost
Search the Web
Top Sites
youtube
Highlights

Authentication Required - Mozilla Firefox

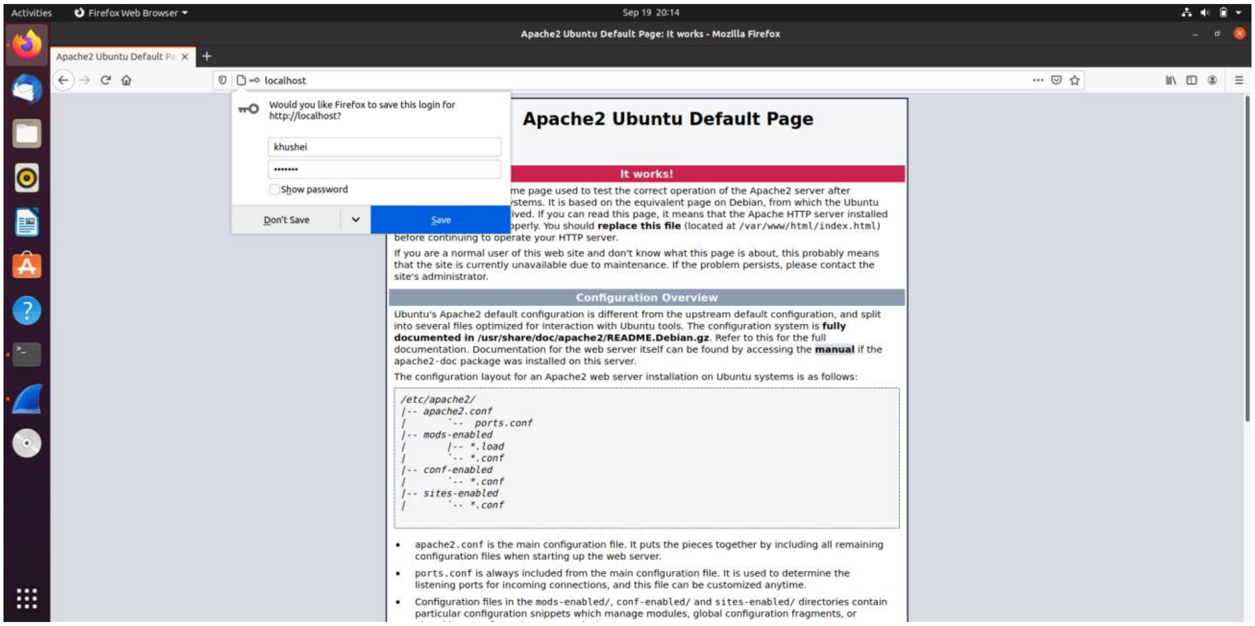
http://localhost is requesting your username and password. The site says: "RESTRICTED"

User Name:

Password:

Cancel OK

Start browsing, and we'll show some of the great articles, videos, and other pages you've recently visited or bookmarked here.
Messages from Firefox
Reason #89 to get a Firefox Account: all the secure kids are doing it. Hop on the bandwagon and protect yourself online.
Get a Firefox Account
localhost



Would you like Firefox to save this login for http://localhost?

khushei

•••••••

□ Show password

Don't Save | Save

Apache2 Ubuntu Default Page

It works!

me page used to test the correct operation of the Apache2 server after ystems. It is based on the equivalent page on Debian, from which the Ubuntu ived. If you can read this page, it means that the Apache HTTP server installed operly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

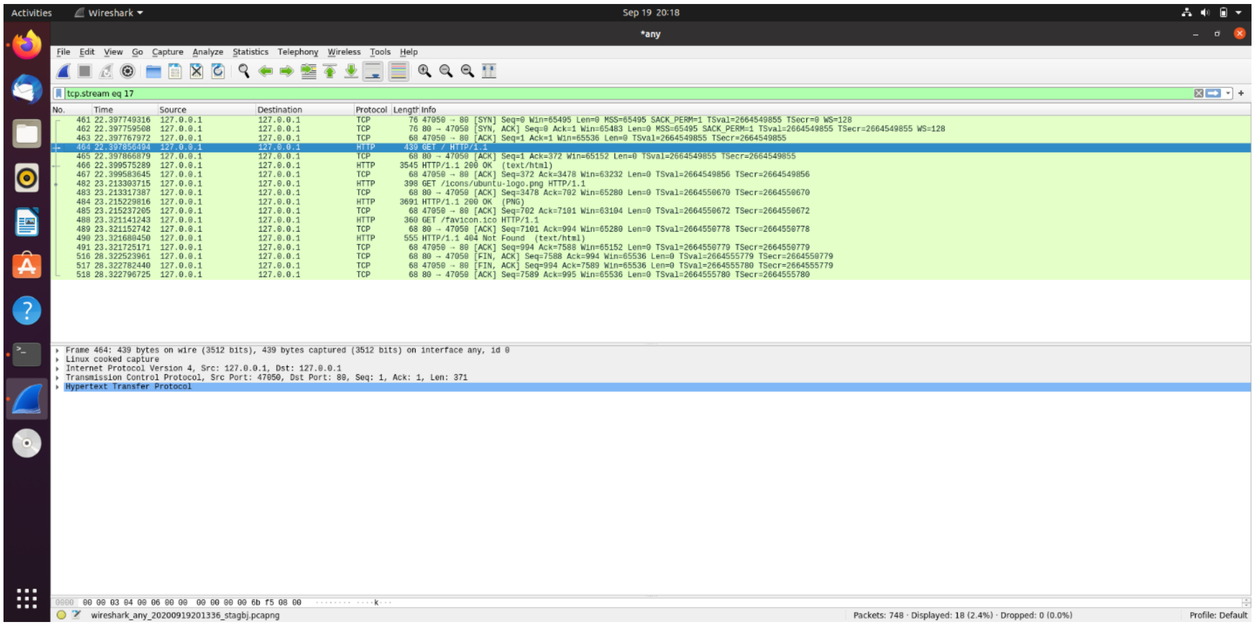
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or

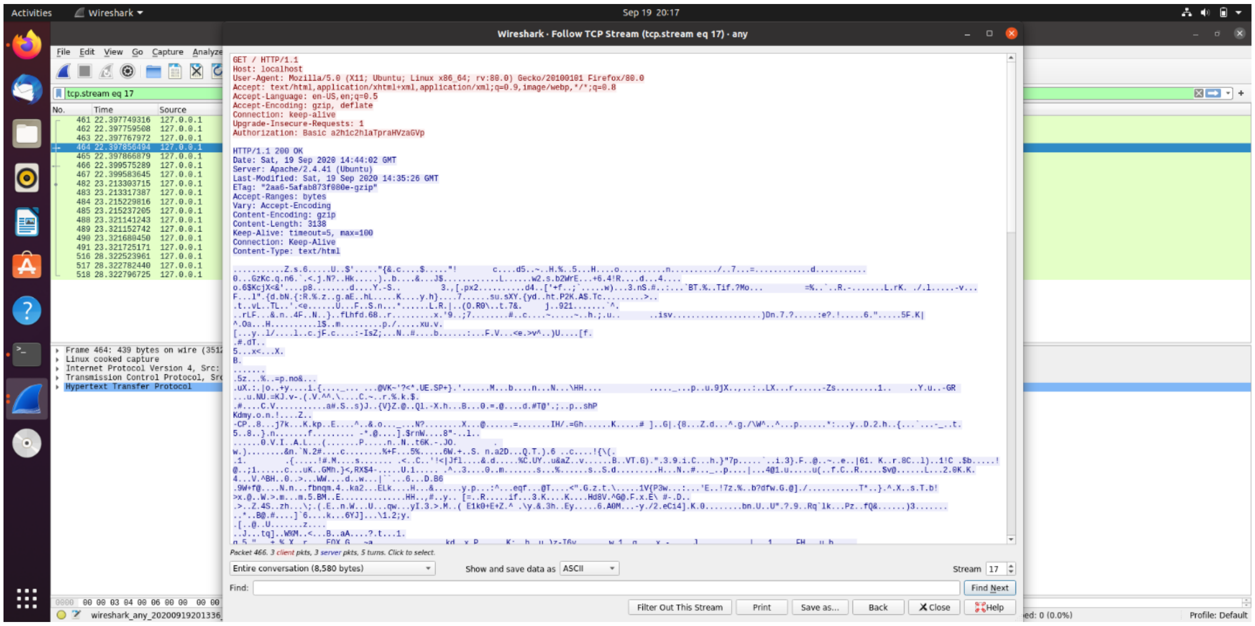
5. Wireshark is used to capture the packets sent upon the network.



```
tcp.stream eq 17

No.  Time          Source     Destination  Protocol Length Info
 461 22.397749316 127.0.0.1  127.0.0.1    TCP        76 47050 → 80 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=2664549855 TSecr=0 WS=128
 462 22.397759508 127.0.0.1  127.0.0.1    TCP        76 80 → 47050 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=2664549855 TSecr=2664549855 WS=128
 463 22.397767972 127.0.0.1  127.0.0.1    TCP        68 47050 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=2664549855 TSecr=2664549855
 464 22.397856494 127.0.0.1  127.0.0.1    HTTP      439 GET / HTTP/1.1
 465 22.397866879 127.0.0.1  127.0.0.1    TCP        68 80 → 47050 [ACK] Seq=1 Ack=372 Win=65152 Len=0 TSval=2664549855 TSecr=2664549855
 466 22.399575289 127.0.0.1  127.0.0.1    HTTP     3545 HTTP/1.1 200 OK  (text/html)
 467 22.399583645 127.0.0.1  127.0.0.1    TCP        68 47050 → 80 [ACK] Seq=372 Ack=3478 Win=63232 Len=0 TSval=2664549856 TSecr=2664549856
 482 23.213303715 127.0.0.1  127.0.0.1    HTTP      398 GET /icons/ubuntu-logo.png HTTP/1.1
 483 23.213317387 127.0.0.1  127.0.0.1    TCP        68 80 → 47050 [ACK] Seq=3478 Ack=702 Win=65280 Len=0 TSval=2664550670 TSecr=2664550670
 484 23.215229816 127.0.0.1  127.0.0.1    HTTP     3691 HTTP/1.1 200 OK  (PNG)
 485 23.215237205 127.0.0.1  127.0.0.1    TCP        68 47050 → 80 [ACK] Seq=702 Ack=7101 Win=63104 Len=0 TSval=2664550672 TSecr=2664550672
 488 23.321141243 127.0.0.1  127.0.0.1    HTTP      360 GET /favicon.ico HTTP/1.1
 489 23.321152742 127.0.0.1  127.0.0.1    TCP        68 80 → 47050 [ACK] Seq=7101 Ack=994 Win=65280 Len=0 TSval=2664550778 TSecr=2664550778
 490 23.321680450 127.0.0.1  127.0.0.1    HTTP      555 HTTP/1.1 404 Not Found  (text/html)
 491 23.321725171 127.0.0.1  127.0.0.1    TCP        68 47050 → 80 [ACK] Seq=994 Ack=7588 Win=65152 Len=0 TSval=2664550779 TSecr=2664550779
 516 28.322523961 127.0.0.1  127.0.0.1    TCP        68 80 → 47050 [FIN, ACK] Seq=7588 Ack=994 Win=65536 Len=0 TSval=2664555779 TSecr=2664550779
 517 28.322782440 127.0.0.1  127.0.0.1    TCP        68 47050 → 80 [FIN, ACK] Seq=994 Ack=7589 Win=65536 Len=0 TSval=2664555780 TSecr=2664555779
 518 28.322796725 127.0.0.1  127.0.0.1    TCP        68 80 → 47050 [ACK] Seq=7589 Ack=995 Win=65536 Len=0 TSval=2664555780 TSecr=2664555780

▸ Frame 464: 439 bytes on wire (3512 bits), 439 bytes captured (3512 bits) on interface any, id 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▸ Transmission Control Protocol, Src Port: 47050, Dst Port: 80, Seq: 1, Ack: 1, Len: 371
▸ Hypertext Transfer Protocol

0000  00 00 03 04 00 06 00 00  00 00 00 00 6b f5 08 00   ........ ....k...

wireshark_any_20200919201336_stagbj.pcapng    Packets: 748 · Displayed: 18 (2.4%) · Dropped: 0 (0.0%)    Profile: Default
```

Activities
Wireshark
Sep 19 20:18
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

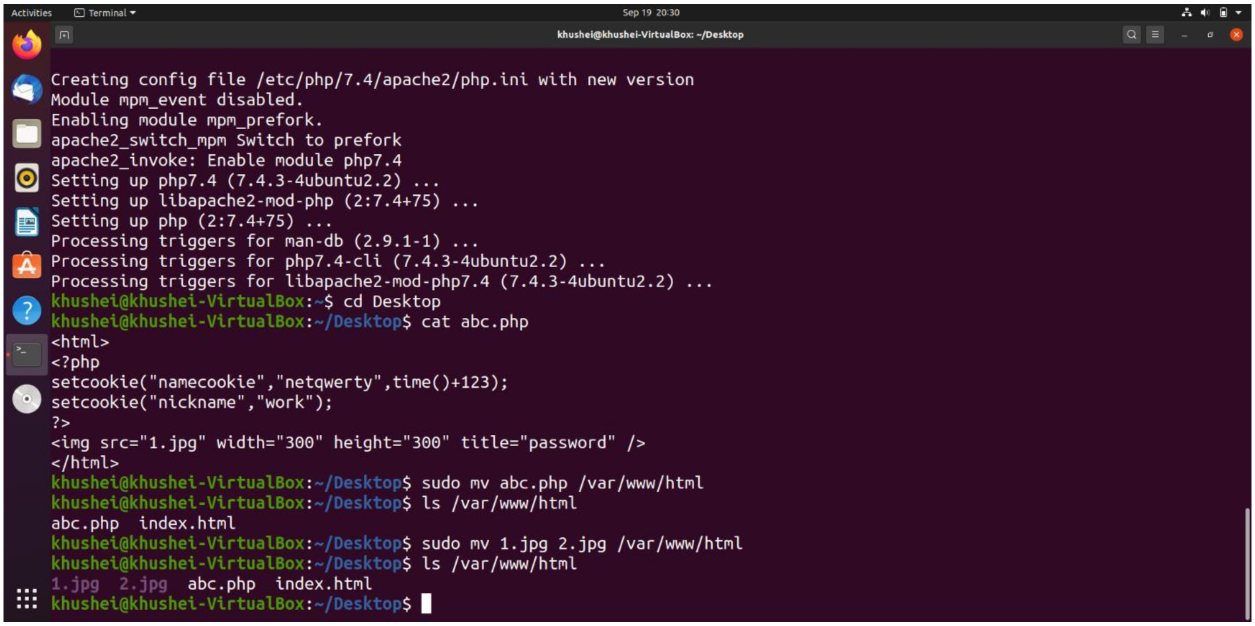
6. Using the “follow TCP stream” on the HTTP message segment the password was retrieved which was encrypted by the base64 algorithm and decryption could be done with same algorithm.



```
GET / HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
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
Authorization: Basic a2h1c2hlaTpraHVzaGVp

HTTP/1.1 200 OK
Date: Sat, 19 Sep 2020 14:44:02 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Sat, 19 Sep 2020 14:35:26 GMT
ETag: "2aa6-5afab873f080e-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 3138
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

Packet 466. 3 client pkts, 3 server pkts, 5 turns. Click to select.
Entire conversation (8,580 bytes)    Show and save data as ASCII    Stream 17
Find:
```

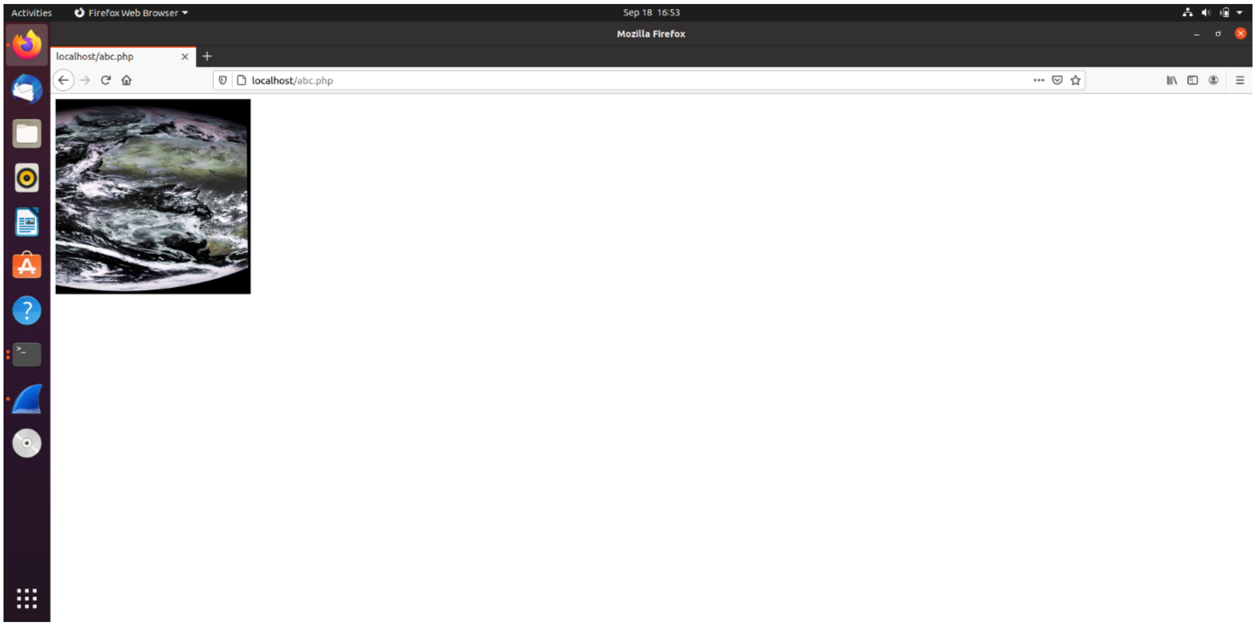
Steps of Execution (Cookie Setting)

1. A PHP file to set the cookie is created which also contains an image in it (placed under the HTML directory) to be accessed once the cookie is set. The following code helped to set the cookie:

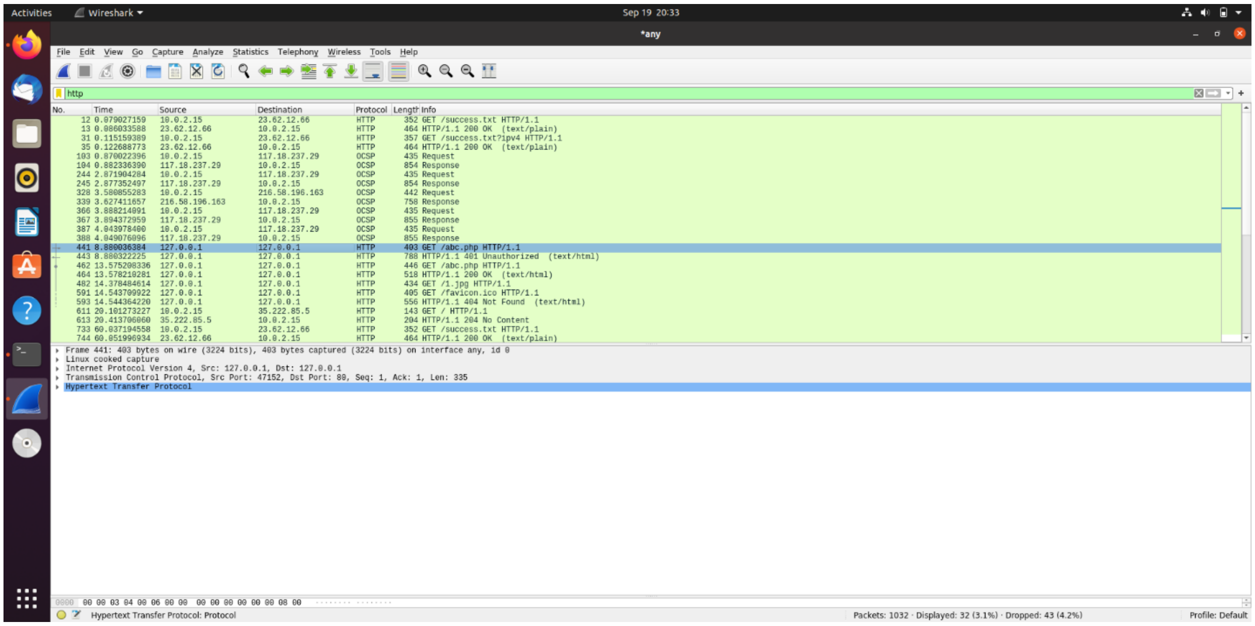


```
Creating config file /etc/php/7.4/apache2/php.ini with new version
Module mpm_event disabled.
Enabling module mpm_prefork.
apache2_switch_mpm Switch to prefork
apache2_invoke: Enable module php7.4
Setting up php7.4 (7.4.3-4ubuntu2.2) ...
Setting up libapache2-mod-php (2:7.4+75) ...
Setting up php (2:7.4+75) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for php7.4-cli (7.4.3-4ubuntu2.2) ...
Processing triggers for libapache2-mod-php7.4 (7.4.3-4ubuntu2.2) ...
khushei@khushei-VirtualBox:~$ cd Desktop
khushei@khushei-VirtualBox:~/Desktop$ cat abc.php
<html>
<?php
setcookie("namecookie","netqwerty",time()+123);
setcookie("nickname","work");
?>
<img src="1.jpg" width="300" height="300" title="password" />
</html>
khushei@khushei-VirtualBox:~/Desktop$ sudo mv abc.php /var/www/html
khushei@khushei-VirtualBox:~/Desktop$ ls /var/www/html
abc.php  index.html
khushei@khushei-VirtualBox:~/Desktop$ sudo mv 1.jpg 2.jpg /var/www/html
khushei@khushei-VirtualBox:~/Desktop$ ls /var/www/html
1.jpg  2.jpg  abc.php  index.html
khushei@khushei-VirtualBox:~/Desktop$
```

2. The combined file saved with a .php extension is placed under **/var/www/html** for accessing.



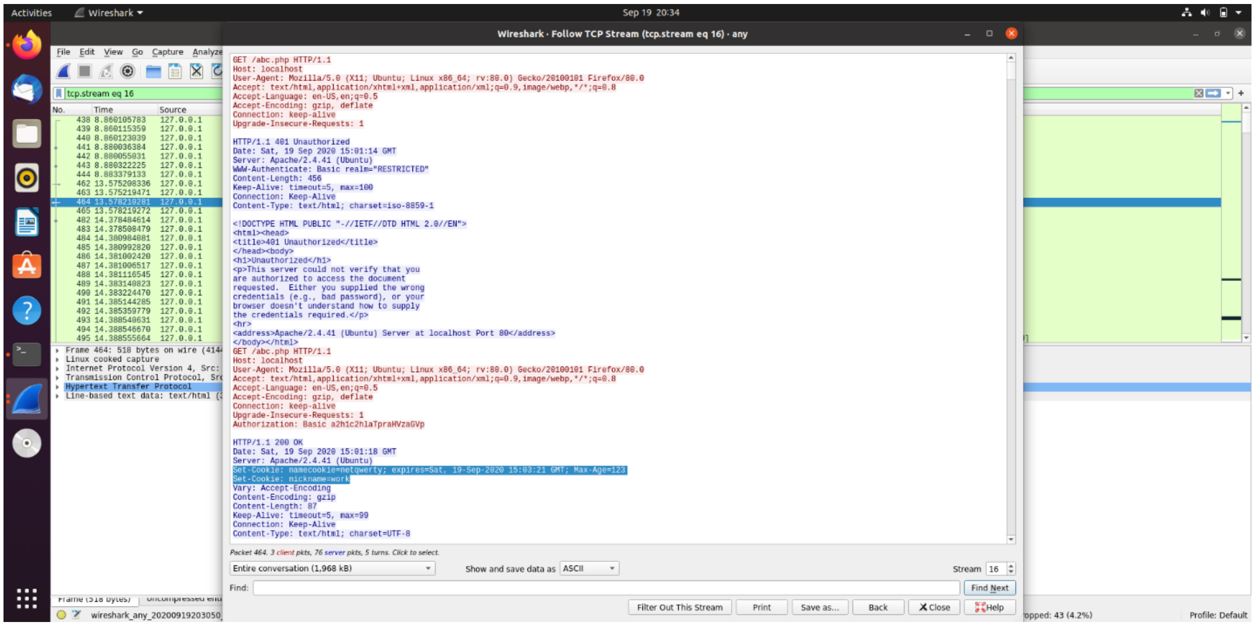
3. The packets are captured using Wireshark and using the “follow TCP stream” which checks for the set-cookie field whether the cookie is set or not set.



Activities
Wireshark
Sep 19 20:33
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
No.   Time          Source          Destination     Protocol Length Info
   12 0.079027159   10.0.2.15       23.62.12.66     HTTP     352 GET /success.txt HTTP/1.1
   13 0.086033588   23.62.12.66     10.0.2.15       HTTP     464 HTTP/1.1 200 OK  (text/plain)
   31 0.115159389   10.0.2.15       23.62.12.66     HTTP     357 GET /success.txt?ipv4 HTTP/1.1
   35 0.122688773   23.62.12.66     10.0.2.15       HTTP     464 HTTP/1.1 200 OK  (text/plain)
  103 0.870022396   10.0.2.15       117.18.237.29   OCSP     435 Request
  104 0.882336390   117.18.237.29   10.0.2.15       OCSP     854 Response
  244 2.871904284   10.0.2.15       117.18.237.29   OCSP     435 Request
  245 2.877352497   117.18.237.29   10.0.2.15       OCSP     854 Response
  328 3.580855283   10.0.2.15       216.58.196.163  OCSP     442 Request
  339 3.627411657   216.58.196.163  10.0.2.15       OCSP     758 Response
  366 3.888214091   10.0.2.15       117.18.237.29   OCSP     435 Request
  367 3.894372959   117.18.237.29   10.0.2.15       OCSP     855 Response
  387 4.043978400   10.0.2.15       117.18.237.29   OCSP     435 Request
  388 4.049076096   117.18.237.29   10.0.2.15       OCSP     855 Response
  441 8.880036384   127.0.0.1       127.0.0.1       HTTP     403 GET /abc.php HTTP/1.1
  443 8.880322225   127.0.0.1       127.0.0.1       HTTP     788 HTTP/1.1 401 Unauthorized  (text/html)
  462 13.575208336  127.0.0.1       127.0.0.1       HTTP     446 GET /abc.php HTTP/1.1
  464 13.578210281  127.0.0.1       127.0.0.1       HTTP     518 HTTP/1.1 200 OK  (text/html)
  482 14.378484614  127.0.0.1       127.0.0.1       HTTP     434 GET /1.jpg HTTP/1.1
  591 14.543709922  127.0.0.1       127.0.0.1       HTTP     405 GET /favicon.ico HTTP/1.1
  593 14.544364220  127.0.0.1       127.0.0.1       HTTP     556 HTTP/1.1 404 Not Found  (text/html)
  611 20.101273227  10.0.2.15       35.222.85.5     HTTP     143 GET / HTTP/1.1
  613 20.413706060  35.222.85.5     10.0.2.15       HTTP     204 HTTP/1.1 204 No Content
  733 60.037194558  10.0.2.15       23.62.12.66     HTTP     352 GET /success.txt HTTP/1.1
  744 60.051996934  23.62.12.66     10.0.2.15       HTTP     464 HTTP/1.1 200 OK  (text/plain)

▸ Frame 441: 403 bytes on wire (3224 bits), 403 bytes captured (3224 bits) on interface any, id 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▸ Transmission Control Protocol, Src Port: 47152, Dst Port: 80, Seq: 1, Ack: 1, Len: 335
▸ Hypertext Transfer Protocol

0000  00 00 03 04 00 06 00 00  00 00 00 00 00 00 08 00
Hypertext Transfer Protocol: Protocol      Packets: 1032 · Displayed: 32 (3.1%) · Dropped: 43 (4.2%)      Profile: Default
```

The cookie is set as shown in the below screenshot.



Activities
Wireshark
Sep 19 20:34
Wireshark · Follow TCP Stream (tcp.stream eq 16) · any
File Edit View Go Capture Analyze
Filter Out This Stream
Print
Save as…
Back
Close
Help

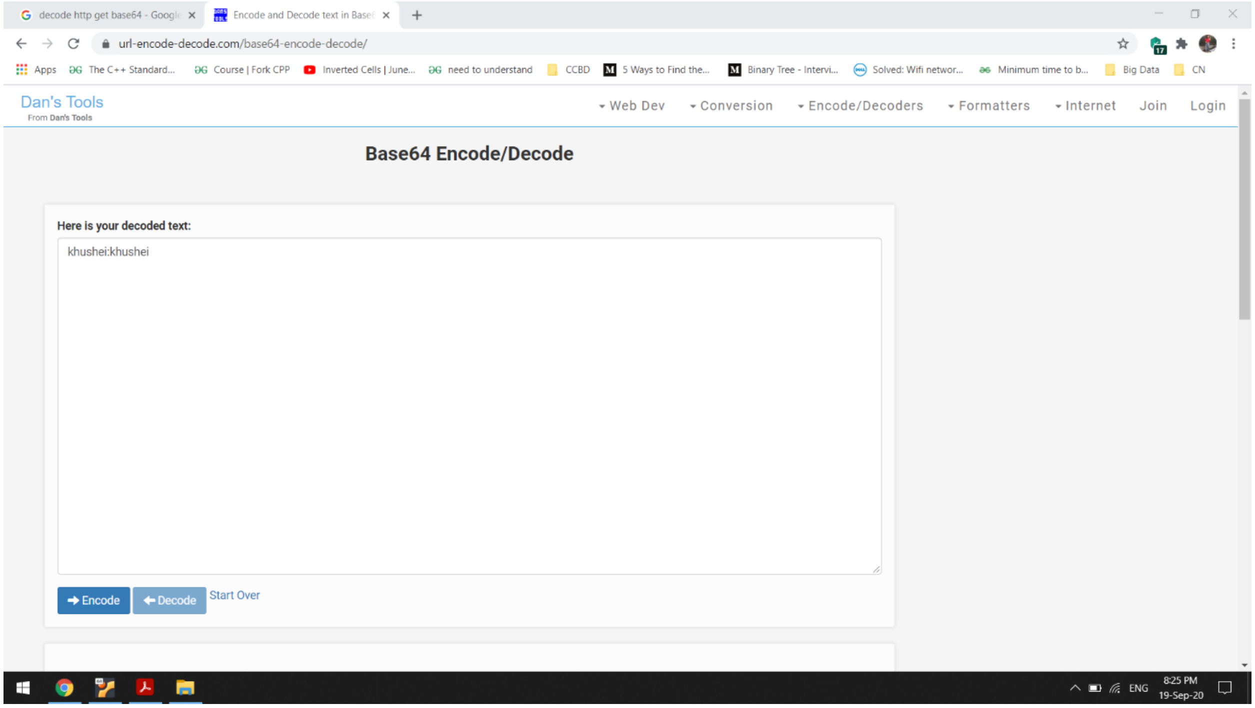
```
tcp.stream eq 16
No.   Time          Source
  438 8.860105783   127.0.0.1
  439 8.860115359   127.0.0.1
  440 8.860123039   127.0.0.1
  441 8.880036384   127.0.0.1
  442 8.880055031   127.0.0.1
  443 8.880322225   127.0.0.1
  444 8.883379133   127.0.0.1
  462 13.575208336  127.0.0.1
  463 13.575219471  127.0.0.1
  464 13.578210281  127.0.0.1
  465 13.578219272  127.0.0.1
  482 14.378484614  127.0.0.1
  483 14.378508479  127.0.0.1
  484 14.380984081  127.0.0.1
  485 14.380992820  127.0.0.1
  486 14.381002420  127.0.0.1
  487 14.381006517  127.0.0.1
  488 14.381116545  127.0.0.1
  489 14.383140823  127.0.0.1
  490 14.383224470  127.0.0.1
  491 14.385144285  127.0.0.1
  492 14.385359779  127.0.0.1
  493 14.388540631  127.0.0.1
  494 14.388546670  127.0.0.1
  495 14.388555664  127.0.0.1

▸ Frame 464: 518 bytes on wire (4144
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src:
▸ Transmission Control Protocol, Src
▸ Hypertext Transfer Protocol
▸ Line-based text data: text/html (3
```

```
GET /abc.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
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

HTTP/1.1 401 Unauthorized
Date: Sat, 19 Sep 2020 15:01:14 GMT
Server: Apache/2.4.41 (Ubuntu)
WWW-Authenticate: Basic realm="RESTRICTED"
Content-Length: 456
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>401 Unauthorized</title>
</head><body>
<h1>Unauthorized</h1>
<p>This server could not verify that you
are authorized to access the document
requested.  Either you supplied the wrong
credentials (e.g., bad password), or your
browser doesn't understand how to supply
the credentials required.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at localhost Port 80</address>
</body></html>
GET /abc.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
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
Authorization: Basic a2h1c2hlaTpraHVzaGVp

HTTP/1.1 200 OK
Date: Sat, 19 Sep 2020 15:01:18 GMT
Server: Apache/2.4.41 (Ubuntu)
Set-Cookie: namecookie=netqwerty; expires=Sat, 19-Sep-2020 15:03:21 GMT; Max-Age=123
Set-Cookie: nickname=work
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 87
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

Packet 464. 3 client pkts, 76 server pkts, 5 turns. Click to select.
Entire conversation (1,968 kB)      Show and save data as ASCII      Stream 16
Find:                                                                 Find Next
wireshark_any_20200919203050_      opped: 43 (4.2%)      Profile: Default
```

Observation: Understand and work out base 64 algorithm and write in your observation. Observe various parameters associated with Cookie in the wireshark capture.

In the above screenshot notice Authorization: Basic a2h1c2hlaTpraHVzaGVp

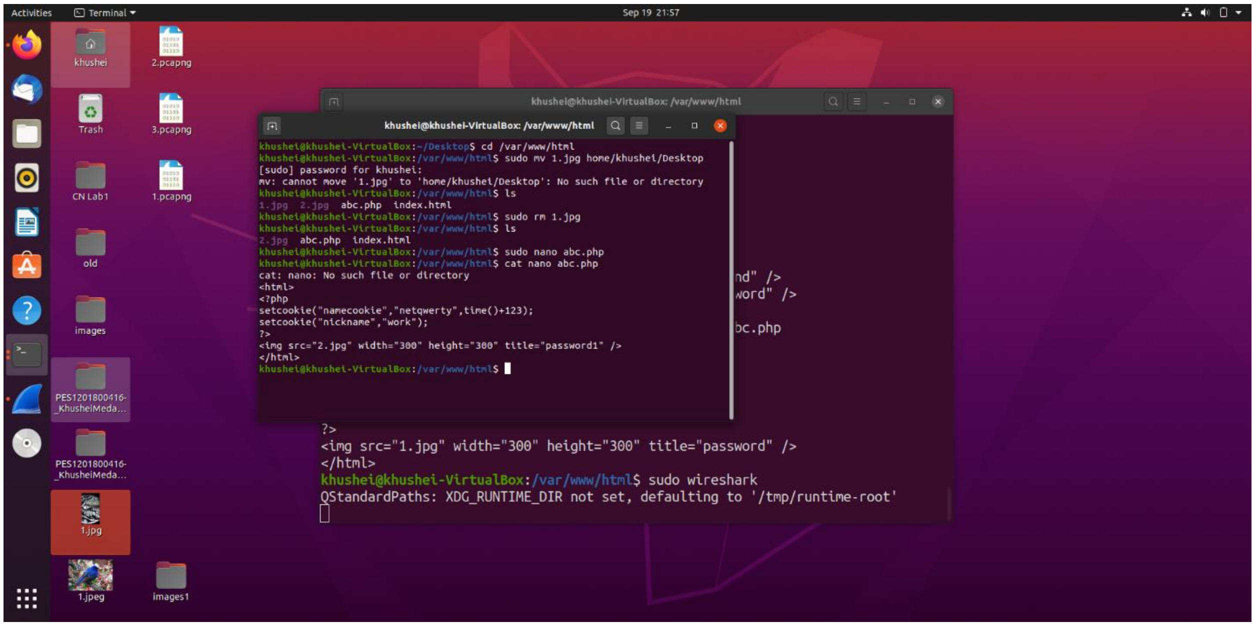
We decode this encoded text using an online decoder. We get the correct authentication id and password that we had set earlier, i.e, khushei:khushei



Here is your decoded text:

```
khushei:khushei
```

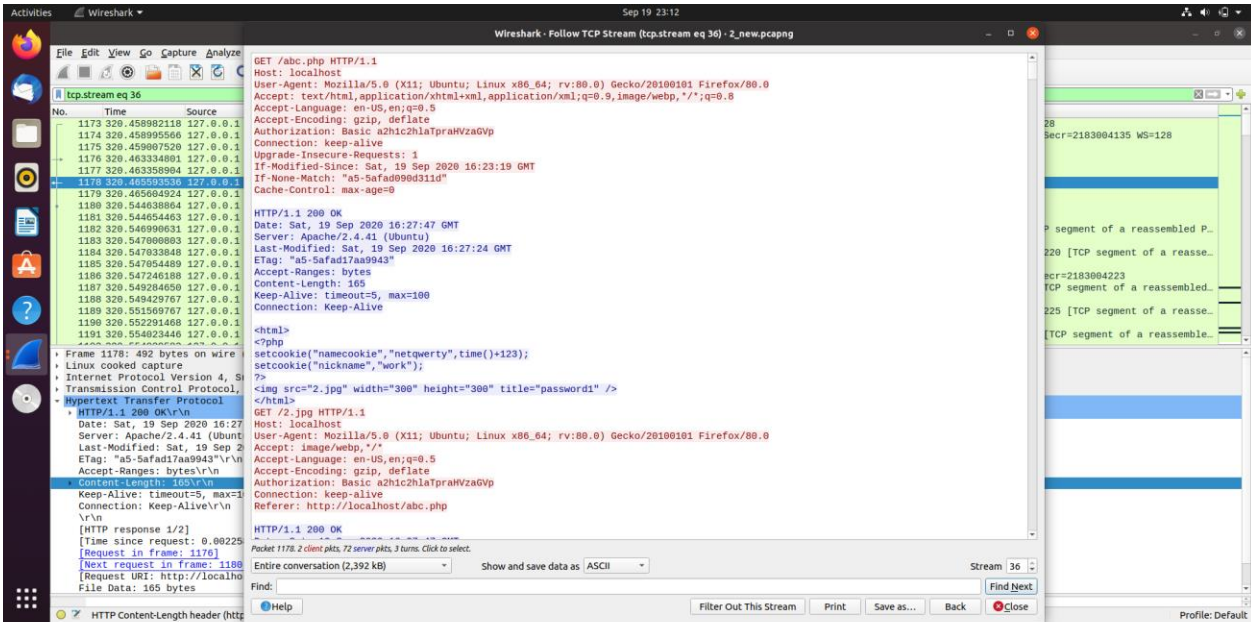
We now try to modify abc.php by adding another image to see if the Modified since parameter in the HTTP GET request changes. While Wireshark is capturing the packets, we open a new terminal and rename the image to 2.jpg. Note that we haven't stopped Wireshark when we do this, so it continues to capture the packets.



```
khushei@khushei-VirtualBox:~/Desktop$ cd /var/www/html
khushei@khushei-VirtualBox:/var/www/html$ sudo mv 1.jpg home/khushei/Desktop
[sudo] password for khushei:
mv: cannot move '1.jpg' to 'home/khushei/Desktop': No such file or directory
khushei@khushei-VirtualBox:/var/www/html$ ls
1.jpg  2.jpg  abc.php  index.html
khushei@khushei-VirtualBox:/var/www/html$ sudo rm 1.jpg
khushei@khushei-VirtualBox:/var/www/html$ ls
2.jpg  abc.php  index.html
khushei@khushei-VirtualBox:/var/www/html$ sudo nano abc.php
khushei@khushei-VirtualBox:/var/www/html$ cat nano abc.php
cat: nano: No such file or directory
<html>
<?php
setcookie("namecookie","netqwerty",time()+123);
setcookie("nickname","work");
?>
<img src="2.jpg" width="300" height="300" title="password1" />
</html>
khushei@khushei-VirtualBox:/var/www/html$
```

```
nd" />
word" />
bc.php
?>
<img src="1.jpg" width="300" height="300" title="password" />
</html>
khushei@khushei-VirtualBox:/var/www/html$ sudo wireshark
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```

Notice that on refreshing the page and then following TCP stream of the HTTP 200 OK message after this change, we see an if-modified-since parameter and notice that since there has been a change, the image is sent by the server.


Activities
Wireshark
Sep 19 23:12
Wireshark · Follow TCP Stream (tcp.stream eq 36) · 2_new.pcapng
File Edit View Go Capture Analyze

```
tcp.stream eq 36
No.    Time          Source
  1173 320.458982118 127.0.0.1
  1174 320.458995566 127.0.0.1
  1175 320.459007520 127.0.0.1
  1176 320.463334801 127.0.0.1
  1177 320.463358904 127.0.0.1
  1178 320.465593536 127.0.0.1
  1179 320.465604924 127.0.0.1
  1180 320.544638864 127.0.0.1
  1181 320.544654463 127.0.0.1
  1182 320.546990631 127.0.0.1
  1183 320.547000803 127.0.0.1
  1184 320.547033848 127.0.0.1
  1185 320.547054489 127.0.0.1
  1186 320.547246188 127.0.0.1
  1187 320.549284650 127.0.0.1
  1188 320.549429767 127.0.0.1
  1189 320.551569767 127.0.0.1
  1190 320.552291468 127.0.0.1
  1191 320.554023446 127.0.0.1

▸ Frame 1178: 492 bytes on wire
▸ Linux cooked capture
▸ Internet Protocol Version 4, Sı
▸ Transmission Control Protocol,
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Date: Sat, 19 Sep 2020 16:27
    Server: Apache/2.4.41 (Ubunt
    Last-Modified: Sat, 19 Sep 2
    ETag: "a5-5afad17aa9943"\r\n
    Accept-Ranges: bytes\r\n
  ▸ Content-Length: 165\r\n
    Keep-Alive: timeout=5, max=1
    Connection: Keep-Alive\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.00225
    [Request in frame: 1176]
    [Next request in frame: 1180
    [Request URI: http://localho
    File Data: 165 bytes
HTTP Content-Length header (http
```

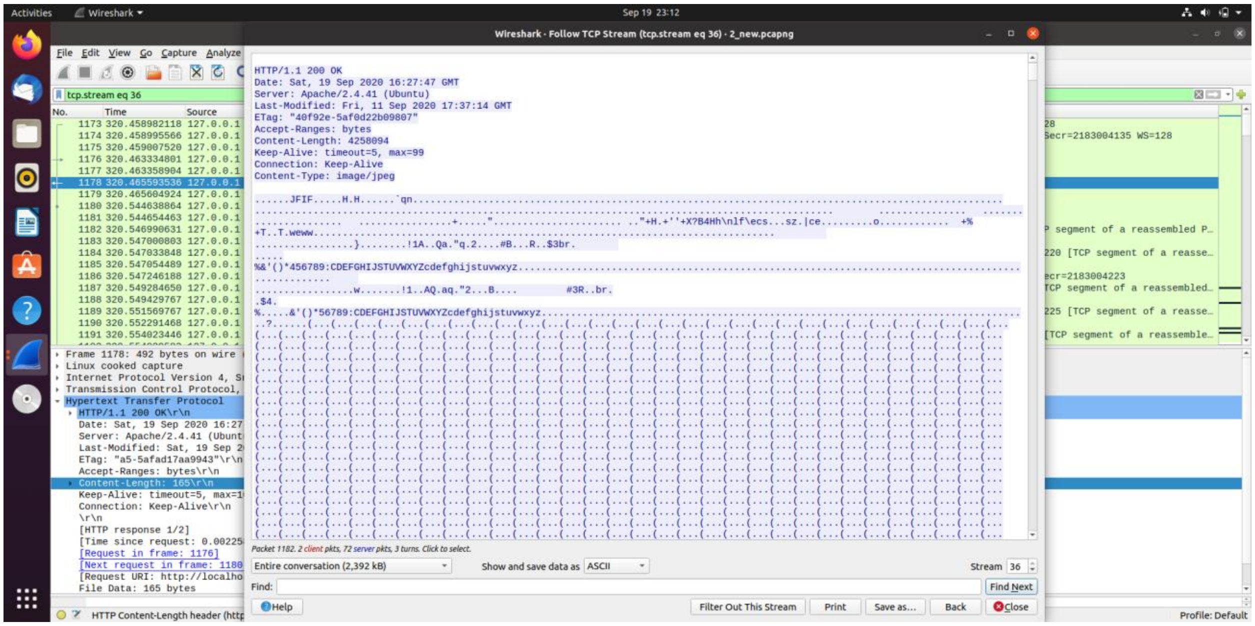
```
GET /abc.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Basic a2h1c2hlaTpraHVzaGVp
Connection: keep-alive
Upgrade-Insecure-Requests: 1
If-Modified-Since: Sat, 19 Sep 2020 16:23:19 GMT
If-None-Match: "a5-5afad090d311d"
Cache-Control: max-age=0

HTTP/1.1 200 OK
Date: Sat, 19 Sep 2020 16:27:47 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Sat, 19 Sep 2020 16:27:24 GMT
ETag: "a5-5afad17aa9943"
Accept-Ranges: bytes
Content-Length: 165
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

<html>
<?php
setcookie("namecookie","netqwerty",time()+123);
setcookie("nickname","work");
?>
<img src="2.jpg" width="300" height="300" title="password1" />
</html>
GET /2.jpg HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Basic a2h1c2hlaTpraHVzaGVp
Connection: keep-alive
Referer: http://localhost/abc.php

HTTP/1.1 200 OK
```

```
28
Secr=2183004135 WS=128
P segment of a reassembled P…
220 [TCP segment of a reasse…
ecr=2183004223
TCP segment of a reassembled…
225 [TCP segment of a reasse…
[TCP segment of a reassemble…
```

Packet 1178. 2 client pkts, 72 server pkts, 3 turns. Click to select.

Entire conversation (2,392 kB) Show and save data as ASCII Stream 36

Find:


Activities
Wireshark
Sep 19 23:12
Wireshark · Follow TCP Stream (tcp.stream eq 36) · 2_new.pcapng
File Edit View Go Capture Analyze

```
tcp.stream eq 36
No.    Time          Source
  1173 320.458982118 127.0.0.1
  1174 320.458995566 127.0.0.1
  1175 320.459007520 127.0.0.1
  1176 320.463334801 127.0.0.1
  1177 320.463358904 127.0.0.1
  1178 320.465593536 127.0.0.1
  1179 320.465604924 127.0.0.1
  1180 320.544638864 127.0.0.1
  1181 320.544654463 127.0.0.1
  1182 320.546990631 127.0.0.1
  1183 320.547000803 127.0.0.1
  1184 320.547033848 127.0.0.1
  1185 320.547054489 127.0.0.1
  1186 320.547246188 127.0.0.1
  1187 320.549284650 127.0.0.1
  1188 320.549429767 127.0.0.1
  1189 320.551569767 127.0.0.1
  1190 320.552291468 127.0.0.1
  1191 320.554023446 127.0.0.1

▸ Frame 1178: 492 bytes on wire
▸ Linux cooked capture
▸ Internet Protocol Version 4, Sı
▸ Transmission Control Protocol,
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Date: Sat, 19 Sep 2020 16:27
    Server: Apache/2.4.41 (Ubunt
    Last-Modified: Sat, 19 Sep 2
    ETag: "a5-5afad17aa9943"\r\n
    Accept-Ranges: bytes\r\n
  ▸ Content-Length: 165\r\n
    Keep-Alive: timeout=5, max=1
    Connection: Keep-Alive\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.00225
    [Request in frame: 1176]
    [Next request in frame: 1180
    [Request URI: http://localho
    File Data: 165 bytes
HTTP Content-Length header (http
```

```
HTTP/1.1 200 OK
Date: Sat, 19 Sep 2020 16:27:47 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Fri, 11 Sep 2020 17:37:14 GMT
ETag: "40f92e-5af0d22b09807"
Accept-Ranges: bytes
Content-Length: 4258094
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: image/jpeg

......JFIF.....H.H......`qn....................................................................................
..........................................................................................     ...............   .......
...............   ................+....."...................... .."+H.+''+X?B4Hh\nlf\ecs...sz.|ce.........o............  +%
+T..T.weww..........................................................................
.................}........!1A..Qa."q.2....#B...R..$3br.
.....
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..................................................................................
.............
.................w.......!1..AQ.aq."2...B....        #3R..br.
.$4.
%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..................................................................................
..?......(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...
```

```
28
Secr=2183004135 WS=128
P segment of a reassembled P…
220 [TCP segment of a reasse…
ecr=2183004223
TCP segment of a reassembled…
225 [TCP segment of a reasse…
[TCP segment of a reassemble…
```

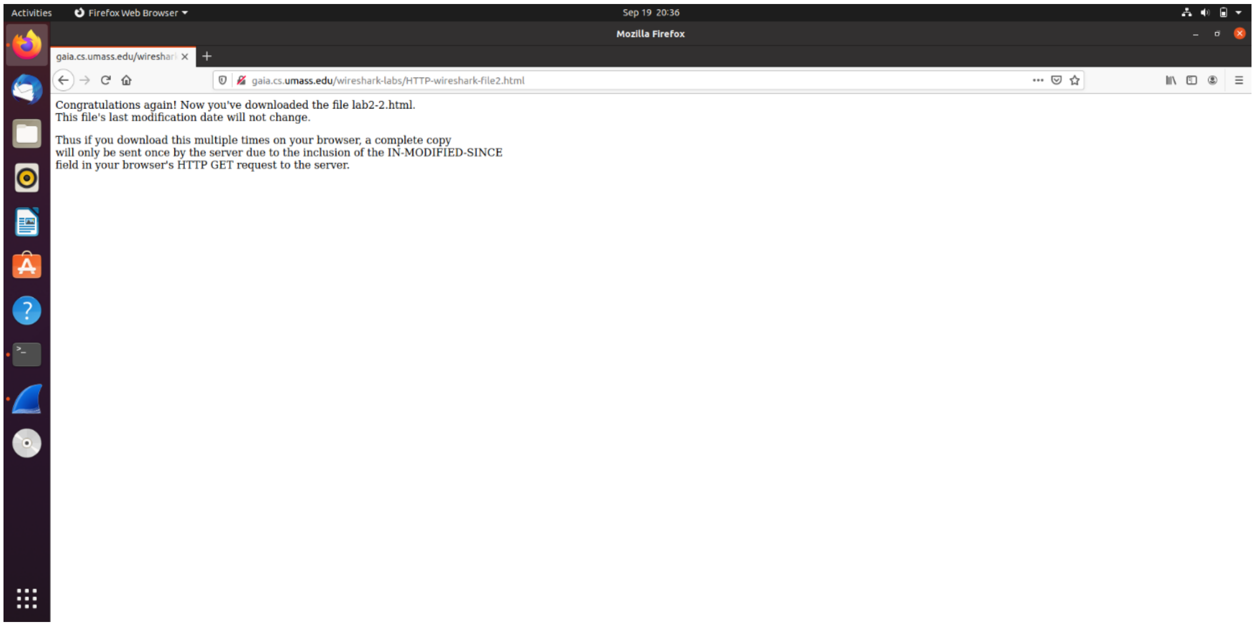
Packet 1182. 2 client pkts, 72 server pkts, 3 turns. Click to select.

Entire conversation (2,392 kB) Show and save data as ASCII Stream 36

Find:

Conditional Get: If-Modified-Since

Enter the following URL into your browser http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html


Activities
Firefox Web Browser
Sep 19 20:36
Mozilla Firefox
gaia.cs.umass.edu/wireshar
gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html

Congratulations again! Now you've downloaded the file lab2-2.html.
This file's last modification date will not change.

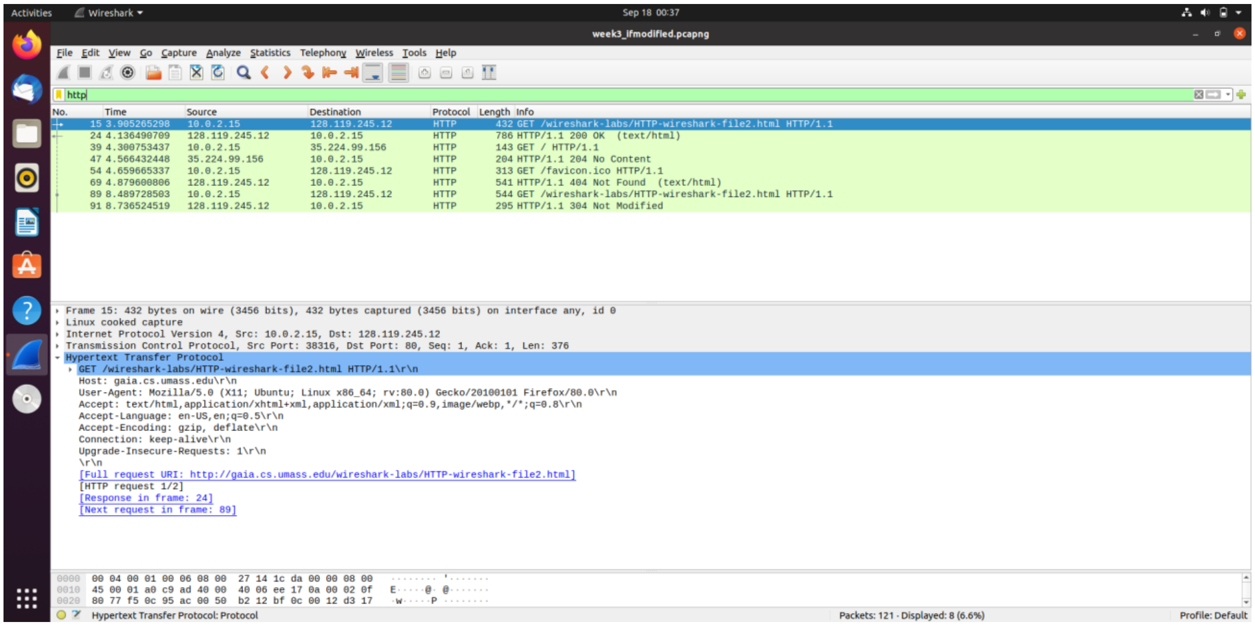
Thus if you download this multiple times on your browser, a complete copy
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE
field in your browser's HTTP GET request to the server.

Observations:

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?

No, there is no "IF-MODIFIED-SINCE" line in the HTTP GET in the first GET request. Obviously, this is understandable because this is the first time that we are accessing this page of the website.

Notice that under the HTTP GET details, there is no line about last modification.


Activities
Wireshark
Sep 18 00:37
week3_ifmodified.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time          Source          Destination     Protocol Length Info
   15 3.905265298   10.0.2.15       128.119.245.12  HTTP       432 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   24 4.136490709   128.119.245.12  10.0.2.15       HTTP       786 HTTP/1.1 200 OK  (text/html)
   39 4.300753437   10.0.2.15       35.224.99.156   HTTP       143 GET / HTTP/1.1
   47 4.566432448   35.224.99.156   10.0.2.15       HTTP       204 HTTP/1.1 204 No Content
   54 4.659665337   10.0.2.15       128.119.245.12  HTTP       313 GET /favicon.ico HTTP/1.1
   69 4.879600806   128.119.245.12  10.0.2.15       HTTP       541 HTTP/1.1 404 Not Found  (text/html)
   89 8.489728503   10.0.2.15       128.119.245.12  HTTP       544 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   91 8.736524519   128.119.245.12  10.0.2.15       HTTP       295 HTTP/1.1 304 Not Modified
```

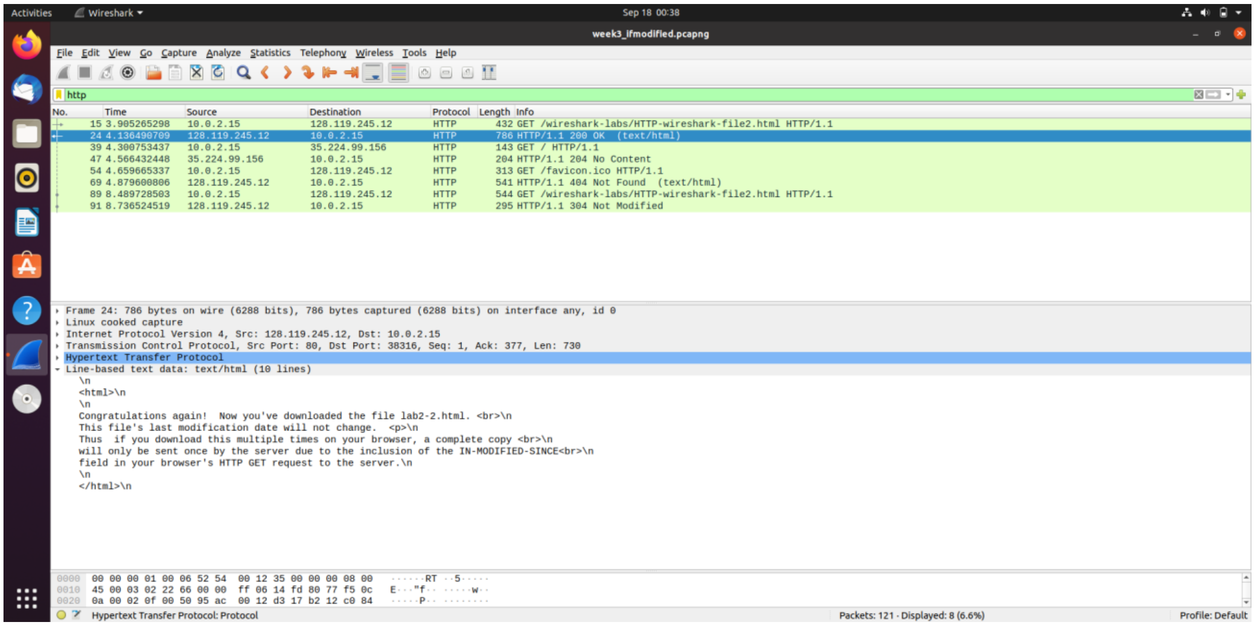
```
Frame 15: 432 bytes on wire (3456 bits), 432 bytes captured (3456 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 38316, Dst Port: 80, Seq: 1, Ack: 1, Len: 376
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
  [HTTP request 1/2]
  [Response in frame: 24]
  [Next request in frame: 89]
```

```
0000  00 04 00 01 00 06 08 00  27 14 1c da 00 00 08 00   ········ '·······
0010  45 00 01 a0 c9 ad 40 00  40 06 ee 17 0a 00 02 0f   E·····@· @·······
0020  80 77 f5 0c 95 ac 00 50  b2 12 bf 0c 00 12 d3 17   ·w·····P ········
```

Hypertext Transfer Protocol: Protocol
Packets: 121 · Displayed: 8 (6.6%)
Profile: Default

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

Yes, the server did explicitly return the contents of the file. We can see under Line-Based Text Data the text that the server sent back to the client browser.



Activities
Wireshark
Sep 18 00:38
week3_ifmodified.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

```
No.   Time          Source           Destination      Protocol Length Info
   15 3.905265298   10.0.2.15        128.119.245.12   HTTP      432 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   24 4.136490709   128.119.245.12   10.0.2.15        HTTP      786 HTTP/1.1 200 OK  (text/html)
   39 4.300753437   10.0.2.15        35.224.99.156    HTTP      143 GET / HTTP/1.1
   47 4.566432448   35.224.99.156    10.0.2.15        HTTP      204 HTTP/1.1 204 No Content
   54 4.659665337   10.0.2.15        128.119.245.12   HTTP      313 GET /favicon.ico HTTP/1.1
   69 4.879600806   128.119.245.12   10.0.2.15        HTTP      541 HTTP/1.1 404 Not Found  (text/html)
   89 8.489728503   10.0.2.15        128.119.245.12   HTTP      544 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   91 8.736524519   128.119.245.12   10.0.2.15        HTTP      295 HTTP/1.1 304 Not Modified
```

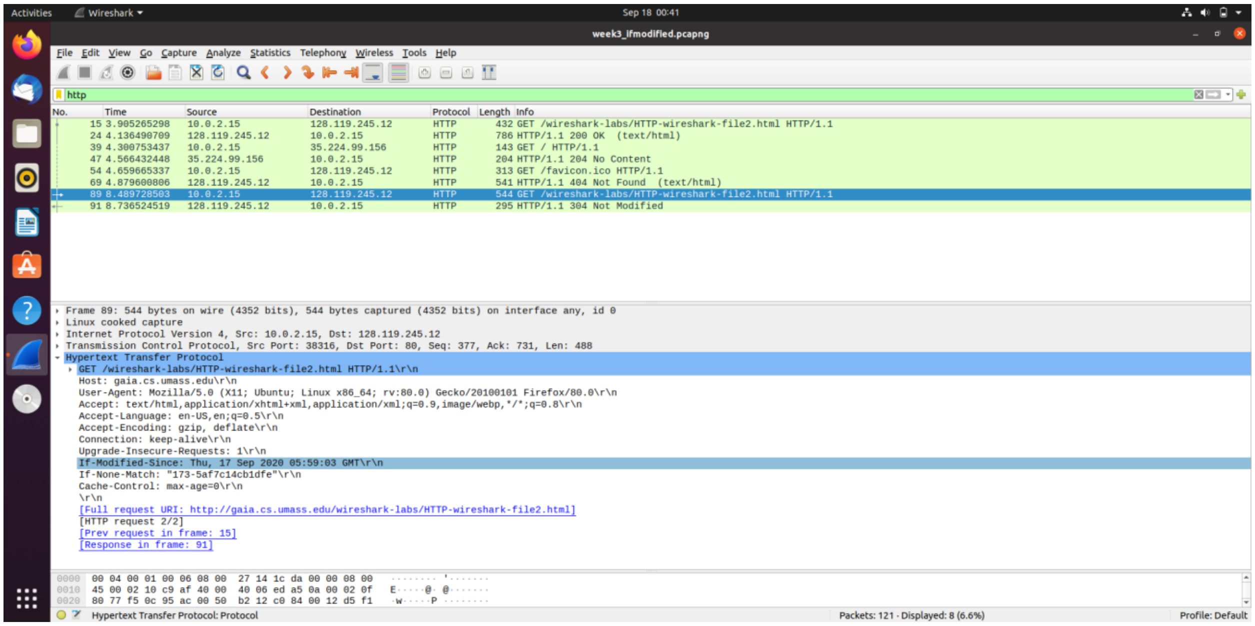
```
› Frame 24: 786 bytes on wire (6288 bits), 786 bytes captured (6288 bits) on interface any, id 0
› Linux cooked capture
› Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.2.15
› Transmission Control Protocol, Src Port: 80, Dst Port: 38316, Seq: 1, Ack: 377, Len: 730
› Hypertext Transfer Protocol
⌄ Line-based text data: text/html (10 lines)
    \n
    <html>\n
    \n
    Congratulations again!  Now you've downloaded the file lab2-2.html. <br>\n
    This file's last modification date will not change.  <p>\n
    Thus  if you download this multiple times on your browser, a complete copy <br>\n
    will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
    field in your browser's HTTP GET request to the server.\n
    \n
    </html>\n
```

```
0000  00 00 00 01 00 06 52 54  00 12 35 00 00 00 08 00   ······RT ··5·····
0010  45 00 03 02 22 66 00 00  ff 06 14 fd 80 77 f5 0c   E···"f·· ·····w··
0020  0a 00 02 0f 00 50 95 ac  00 12 d3 17 b2 12 c0 84   ·····P·· ········
```

Hypertext Transfer Protocol: Protocol   Packets: 121 · Displayed: 8 (6.6%)   Profile: Default

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?

In the second HTTP request, we do see the “IF-MODIFIED-SINCE:” line. The information that follows it is the date and timestamp of when my browser last accessed the webpage.



Activities
Wireshark
Sep 18 00:41
week3_ifmodified.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time          Source            Destination       Protocol Length Info
   15 3.905265298   10.0.2.15         128.119.245.12    HTTP     432 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   24 4.136490709   128.119.245.12    10.0.2.15         HTTP     786 HTTP/1.1 200 OK  (text/html)
   39 4.300753437   10.0.2.15         35.224.99.156     HTTP     143 GET / HTTP/1.1
   47 4.566432448   35.224.99.156     10.0.2.15         HTTP     204 HTTP/1.1 204 No Content
   54 4.659665337   10.0.2.15         128.119.245.12    HTTP     313 GET /favicon.ico HTTP/1.1
   69 4.879600806   128.119.245.12    10.0.2.15         HTTP     541 HTTP/1.1 404 Not Found  (text/html)
   89 8.489728503   10.0.2.15         128.119.245.12    HTTP     544 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   91 8.736524519   128.119.245.12    10.0.2.15         HTTP     295 HTTP/1.1 304 Not Modified
```

```
▸ Frame 89: 544 bytes on wire (4352 bits), 544 bytes captured (4352 bits) on interface any, id 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 128.119.245.12
▸ Transmission Control Protocol, Src Port: 38316, Dst Port: 80, Seq: 377, Ack: 731, Len: 488
▾ Hypertext Transfer Protocol
  ▸ GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    If-Modified-Since: Thu, 17 Sep 2020 05:59:03 GMT\r\n
    If-None-Match: "173-5af7c14cb1dfe"\r\n
    Cache-Control: max-age=0\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 2/2]
    [Prev request in frame: 15]
    [Response in frame: 91]
```

```
0000  00 04 00 01 00 06 08 00  27 14 1c da 00 00 08 00   ········ '·······
0010  45 00 02 10 c9 af 40 00  40 06 ed a5 0a 00 02 0f   E·····@· @·······
0020  80 77 f5 0c 95 ac 00 50  b2 12 c0 84 00 12 d5 f1   ·w·····P ········
```

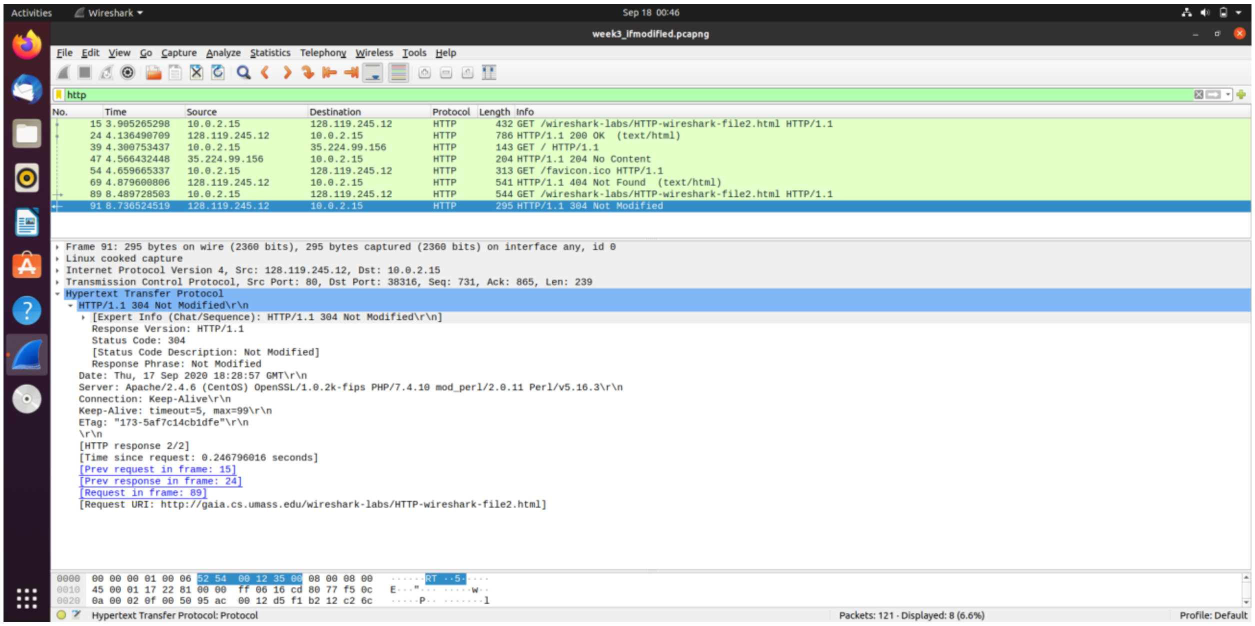
Hypertext Transfer Protocol: Protocol
Packets: 121 · Displayed: 8 (6.6%)
Profile: Default

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.

Status code: 304.

Response Phrase: Not Modified

The server didn’t return the contents of the file since the browser loaded it from its cache.



Activities
Wireshark
Sep 18 00:46
week3_ifmodified.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time          Source            Destination       Protocol Length Info
   15 3.905265298   10.0.2.15         128.119.245.12    HTTP     432 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   24 4.136490709   128.119.245.12    10.0.2.15         HTTP     786 HTTP/1.1 200 OK  (text/html)
   39 4.300753437   10.0.2.15         35.224.99.156     HTTP     143 GET / HTTP/1.1
   47 4.566432448   35.224.99.156     10.0.2.15         HTTP     204 HTTP/1.1 204 No Content
   54 4.659665337   10.0.2.15         128.119.245.12    HTTP     313 GET /favicon.ico HTTP/1.1
   69 4.879600806   128.119.245.12    10.0.2.15         HTTP     541 HTTP/1.1 404 Not Found  (text/html)
   89 8.489728503   10.0.2.15         128.119.245.12    HTTP     544 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   91 8.736524519   128.119.245.12    10.0.2.15         HTTP     295 HTTP/1.1 304 Not Modified
```

```
▸ Frame 91: 295 bytes on wire (2360 bits), 295 bytes captured (2360 bits) on interface any, id 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.2.15
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 38316, Seq: 731, Ack: 865, Len: 239
▾ Hypertext Transfer Protocol
  ▾ HTTP/1.1 304 Not Modified\r\n
    ▸ [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
      Response Version: HTTP/1.1
      Status Code: 304
      [Status Code Description: Not Modified]
      Response Phrase: Not Modified
    Date: Thu, 17 Sep 2020 18:28:57 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.10 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=99\r\n
    ETag: "173-5af7c14cb1dfe"\r\n
    \r\n
    [HTTP response 2/2]
    [Time since request: 0.246796016 seconds]
    [Prev request in frame: 15]
    [Prev response in frame: 24]
    [Request in frame: 89]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

```
0000  00 00 00 01 00 06 52 54  00 12 35 00 08 00 08 00   ······RT ··5·····
0010  45 00 01 17 22 81 00 00  ff 06 16 cd 80 77 f5 0c   E···"··· ·····w··
0020  0a 00 02 0f 00 50 95 ac  00 12 d5 f1 b2 12 c2 6c   ·····P·· ·······l
```

Hypertext Transfer Protocol: Protocol
Packets: 121 · Displayed: 8 (6.6%)
Profile: Default