NAME	SRN	SECTION
ANKITH J RAI	PES1UG19CS069	B

PART 1:

Password Authentication

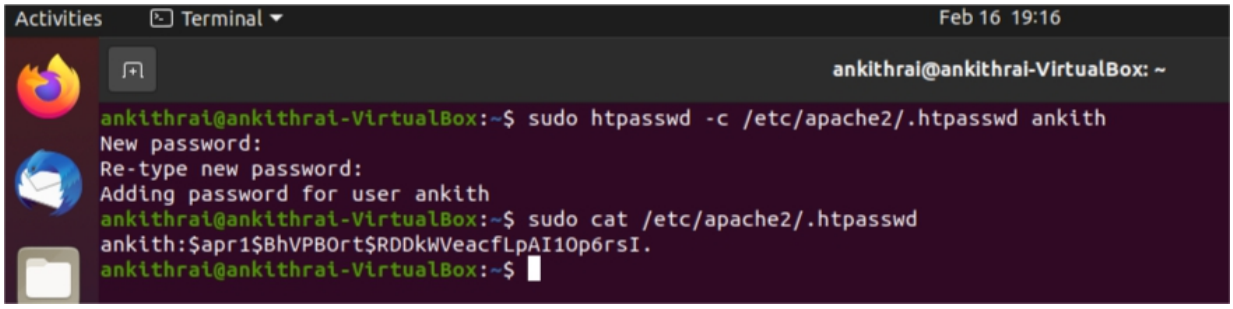
To install the apache2 utility

sudo apt-get install apache2 apache2-utils and

Provide username and password to set authentication

sudo htpasswd -c /etc/apache2/.htpasswd ANY_USERNAME

View the authentication : **sudo cat /etc/apache2/.htpasswd**



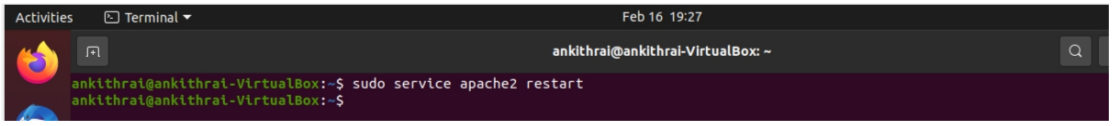
Opening the file for setting authentication

Opening the file for setting authentication

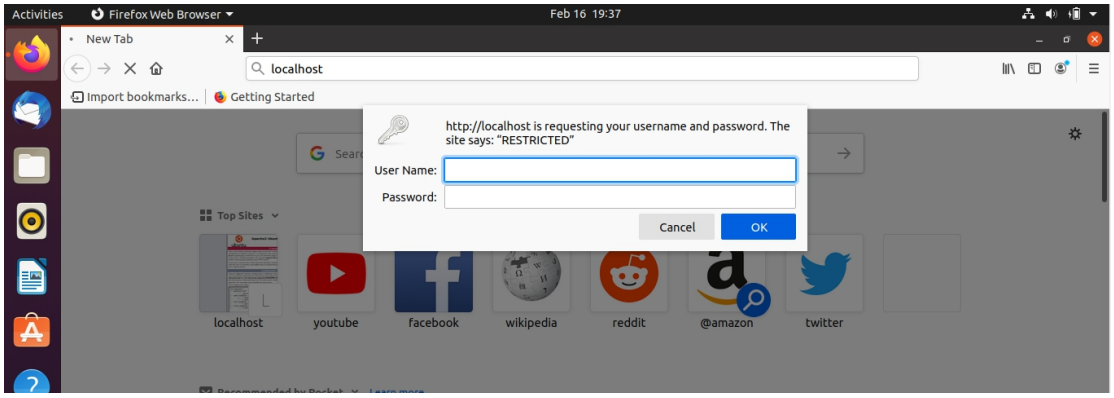
sudo nano /etc/apache2/sites-available/000-default.conf

```
<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
```

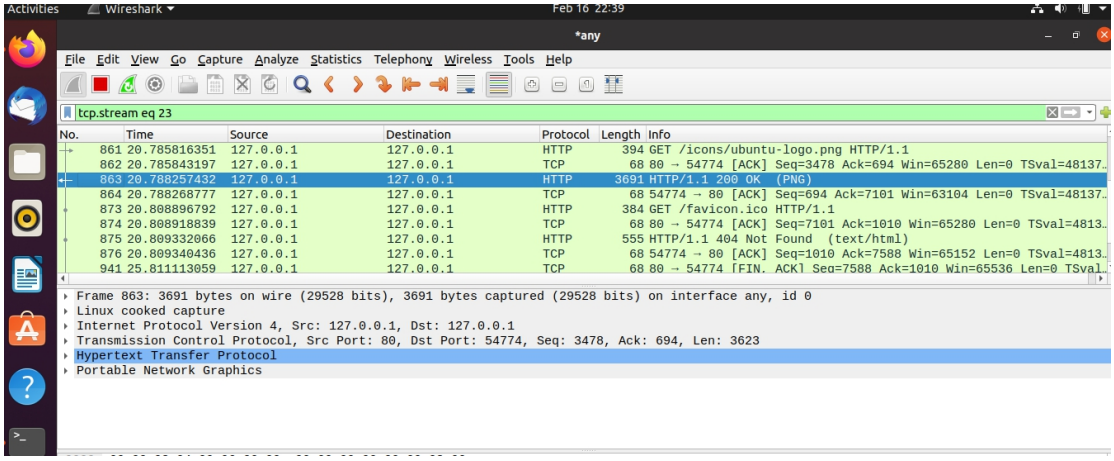
Password policy implementation is done by restarting the server as:
sudo service apache2 restart



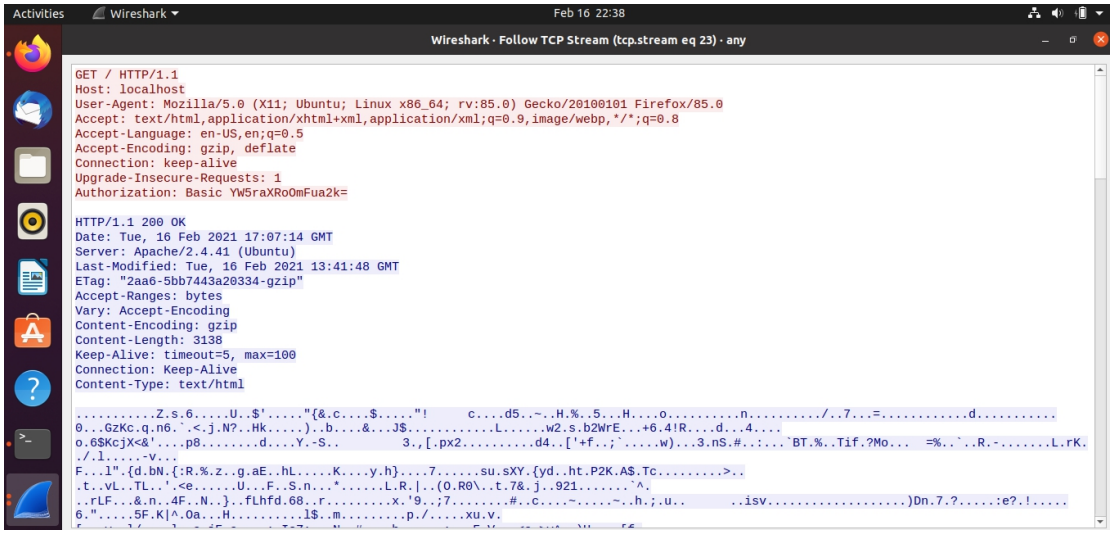
The localhost is then accessed using the Firefox browser requiring a username and a password set during the authentication phase.



Wireshark is used to capture the packets sent upon the network



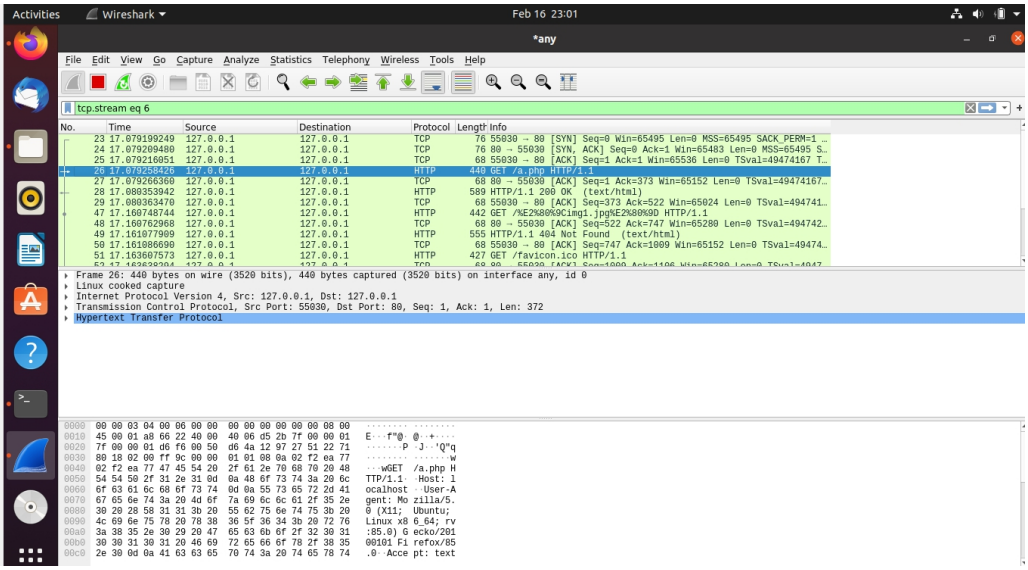
Using the “follow TCP stream” on the HTTP message segment the password was retrieved which was encrypted by the base64 algorithm and decryption could be done with same algorithm



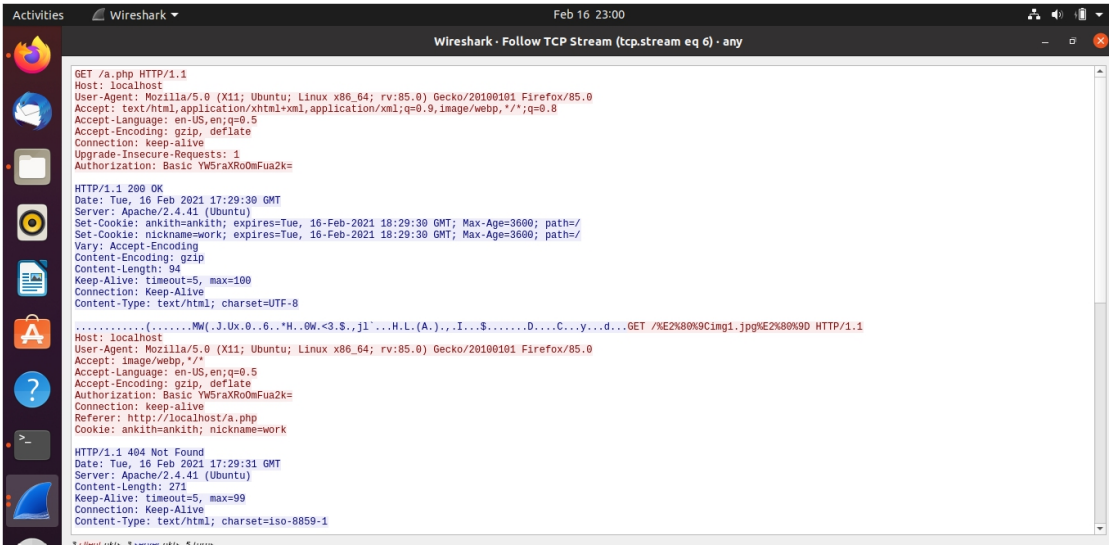
PART 2: **Cookie Setting**

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 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.



TCP STREAM :



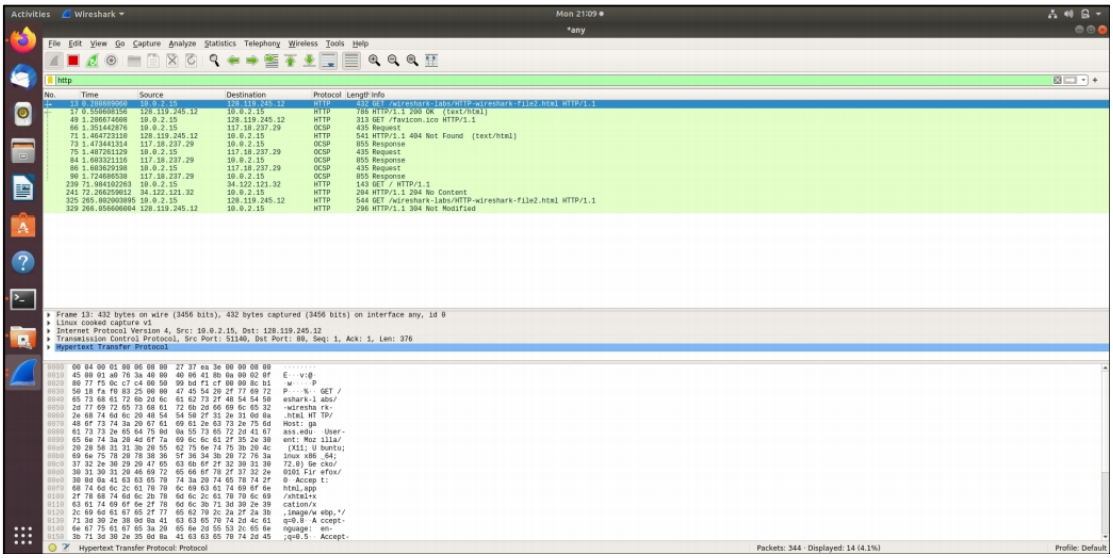
OBSERVATION :

Base64 algorithm is designed to **encode any binary data, an stream of bytes, into a stream of 64-printable characters .**

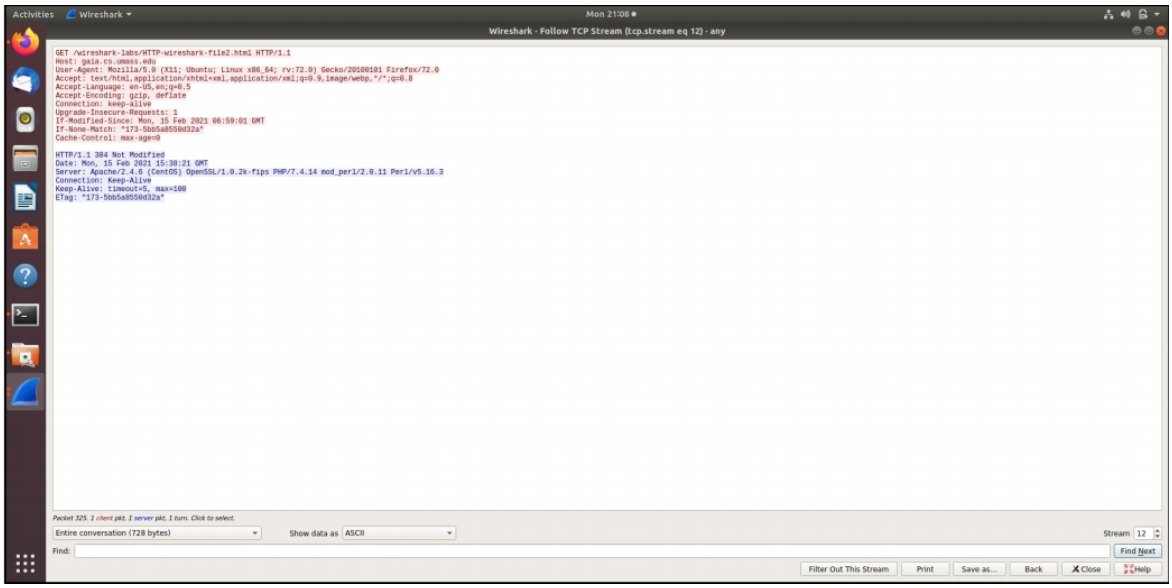
PART - 3 :

Conditional Get: If-Modified-Since

Entering the following URL in browser: http://gaia.cs.umass.edu/wireshark labs/HTTP-wireshark-file2.html and capturing using wireshark

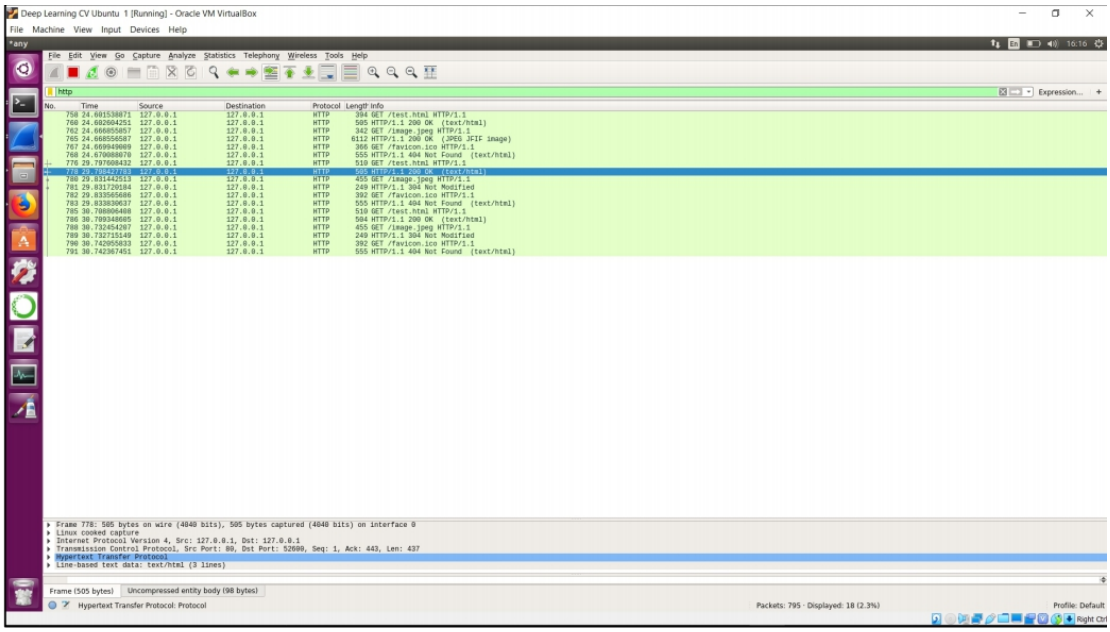


And opening TCP stream

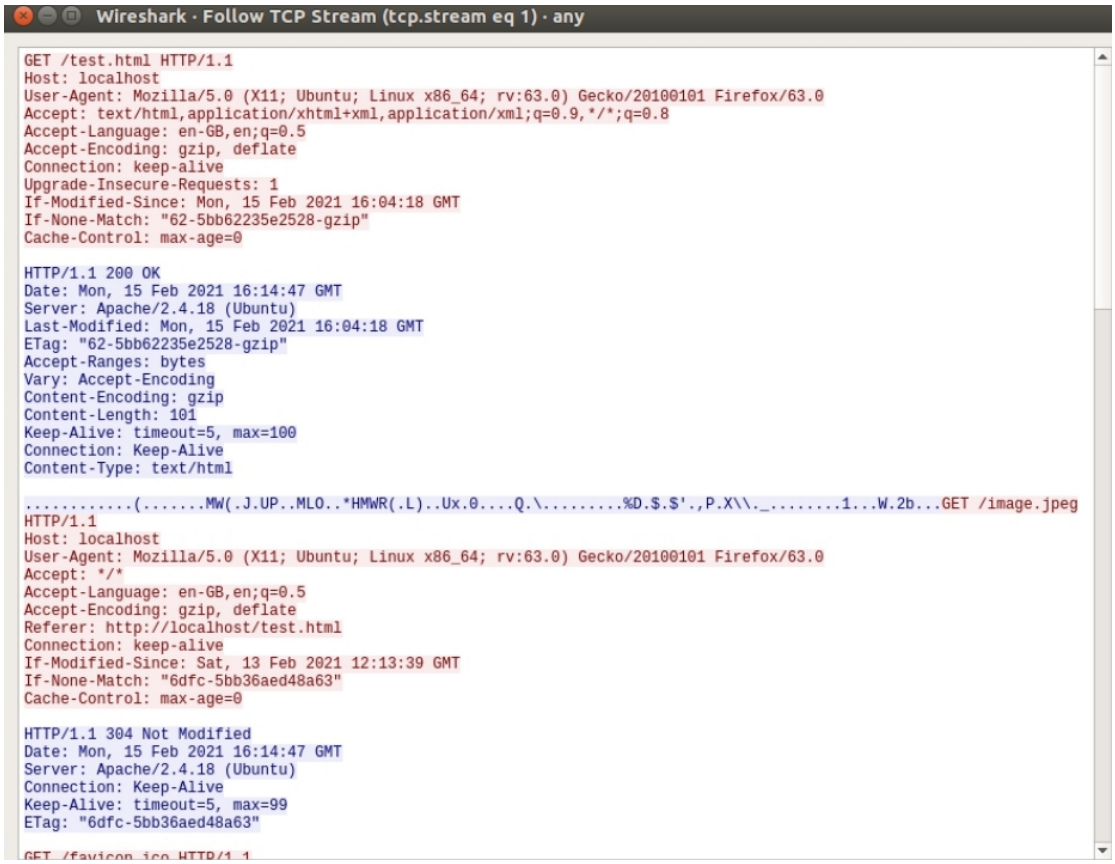


Making a test.html in /var/www/html and hosting that file in local network by apache2

Wireshark screen shot :



TCP stream :



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?

Ans : NO

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

Ans : NO

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?

Ans : The server checks for if-modified-since header value and resends the resource only if it has been modified since the timestamp in the header

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.

Ans : The status code is 304 and message is not modified. The server did not explicitly send the contents of the file as the response have no response body and a 304 not-modified response