COMPUTER NETWORKS LABORATORY

WEEK-3

NAME- T. LOHITH SRINIVAS

SECTION-D

SRN-PES2UG19CS203

DATE-13/02/2021

1.Password Authentication

INSTALL THE APACHE UTILITY:

sudo apt-get install apache2 apache2-utils

```
lohith@lohith-IdeaPad-3-15IIL05:~$ sudo apt-get install apache2-utils
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libapr1 libaprutil1
The following NEW packages will be installed:
  apache2-utils libapr1 libaprutil1
0 upgraded, 3 newly installed, 0 to remove and 325 not upgraded.
Need to get 260 kB of archives.
After this operation, 968 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu focal/main amd64 libapr1 amd64 1.6.5-1ubuntu1 [91.4 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu focal/main amd64 libaprutil1 amd64 1.6.1-4ubuntu2 [84.7 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 apache2-utils amd64 2.4.41-4ubuntu3.1 [83.8 kB]
Fetched 260 kB in 1s (500 kB/s)
Selecting previously unselected package libapr1:amd64.
(Reading database ... 189391 files and directories currently installed.)
Preparing to unpack .../libapr1_1.6.5-1ubuntu1_amd64.deb ...
Unpacking libapr1:amd64 (1.6.5-1ubuntu1) ...
Selecting previously unselected package libaprutil1:amd64.
Preparing to unpack .../libaprutil1_1.6.1-4ubuntu2_amd64.deb ...
Unpacking libaprutil1:amd64 (1.6.1-4ubuntu2) ...
Selecting previously unselected package apache2-utils.
Preparing to unpack .../apache2-utils_2.4.41-4ubuntu3.1_amd64.deb ...
Unpacking apache2-utils (2.4.41-4ubuntu3.1) ...
Setting up libapr1:amd64 (1.6.5-1ubuntu1) ...
Setting up libaprutil1:amd64 (1.6.1-4ubuntu2) ...
Setting up apache2-utils (2.4.41-4ubuntu3.1) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9) ...
```

PROVIDING USERNAME AND PASSWORD TO SET AUTHENTICATION AND VIEW THE AUTHENTICATION:

```
lohith@lohith-IdeaPad-3-15IIL05:~$ sudo htpasswd -c /etc/apache2/.htpasswd srinivas
New password:
Re-type new password:
Adding password for user srinivas
lohith@lohith-IdeaPad-3-15IIL05:~$ sudo cat /etc/apache2/.htpasswd
srinivas:$apr1$CAfIcjfs$d1pMlEkSAadFWKAV8apnJ0
```

CONFIGURING ACCESS CONTROL WITHIN THE VIRTUAL HOST DEFINITION:


```
  GNU nano 4.8                              /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

        # 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
        <Directory "/var/www/html">
                AuthType Basic
                AuthName "RESTRICTED"
                AuthUserFile /etc/apache2/.htpasswd
                Require valid-user >
        </Directory>
</VirtualHost>

        # vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```
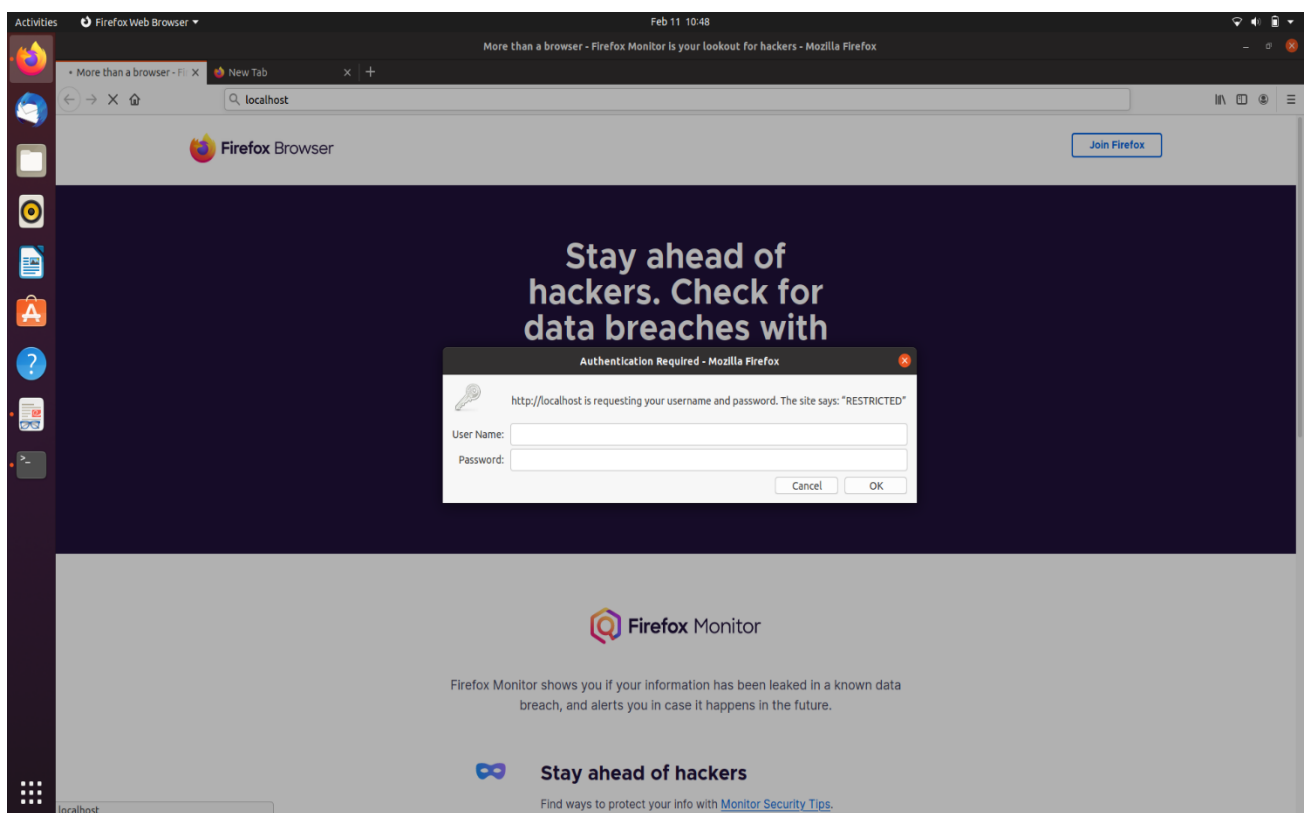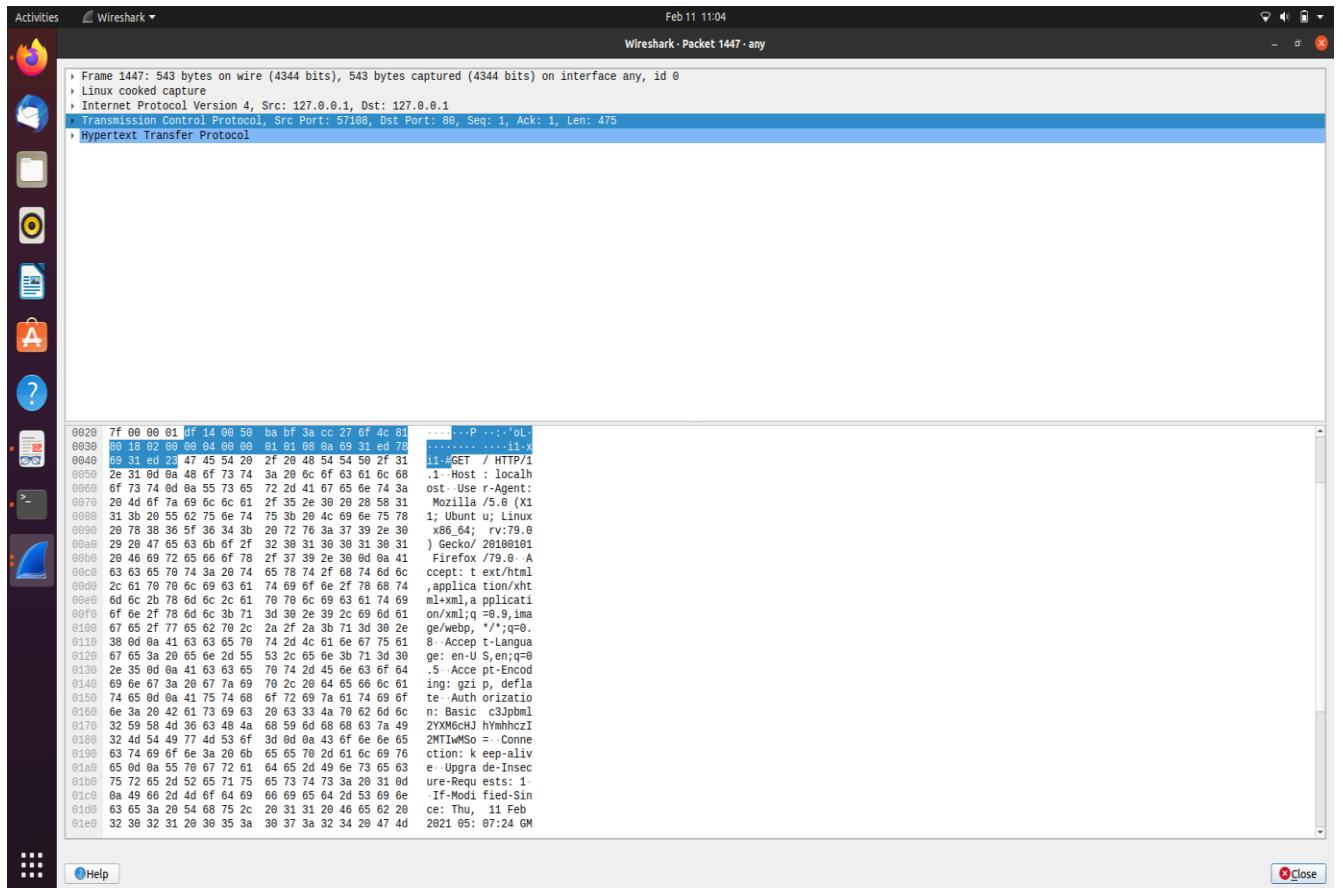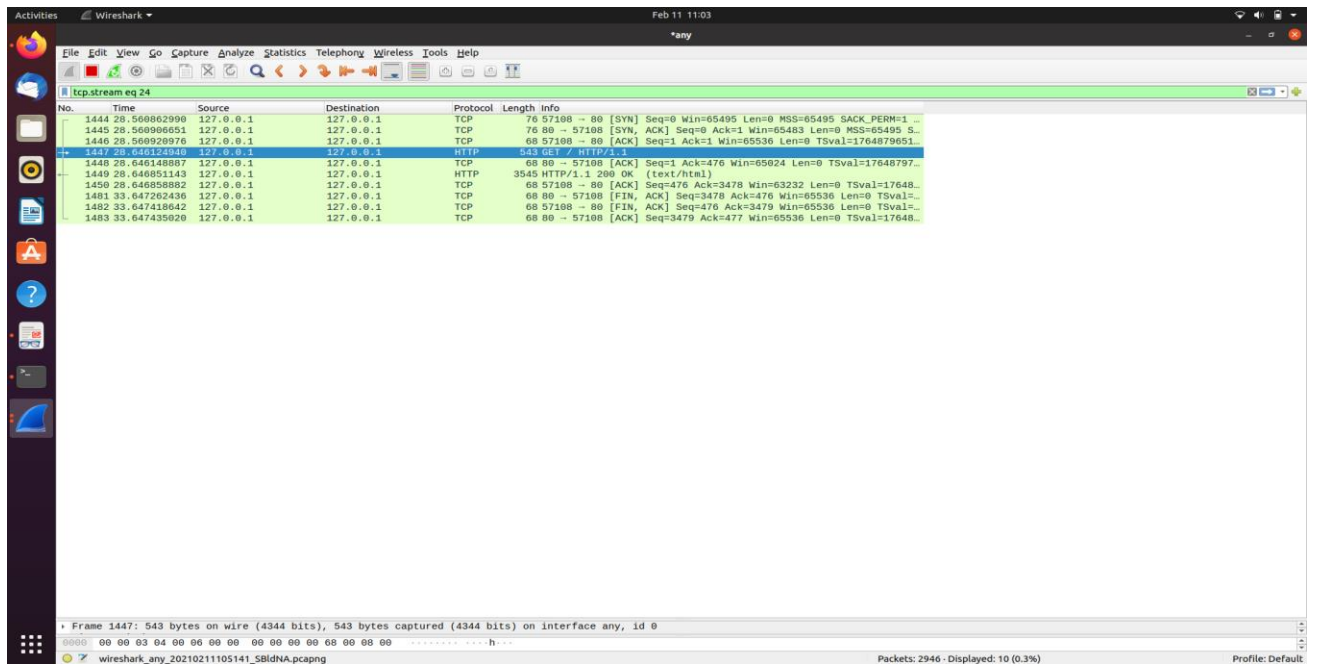
PASSWORD POLICY IMPLEMENTATION (RESTARTING THE SERVER):


```
lohith@lohith-IdeaPad-3-15IIL05:~$ sudo service apache2 restart
lohith@lohith-IdeaPad-3-15IIL05:~$ 
```

ACCESS OF LOCAL HOST USING FIREFOX BROWSER (REQUIRES USERNAME AND PASSWORD SET DURING THE AUTHENTICATION PHASE)
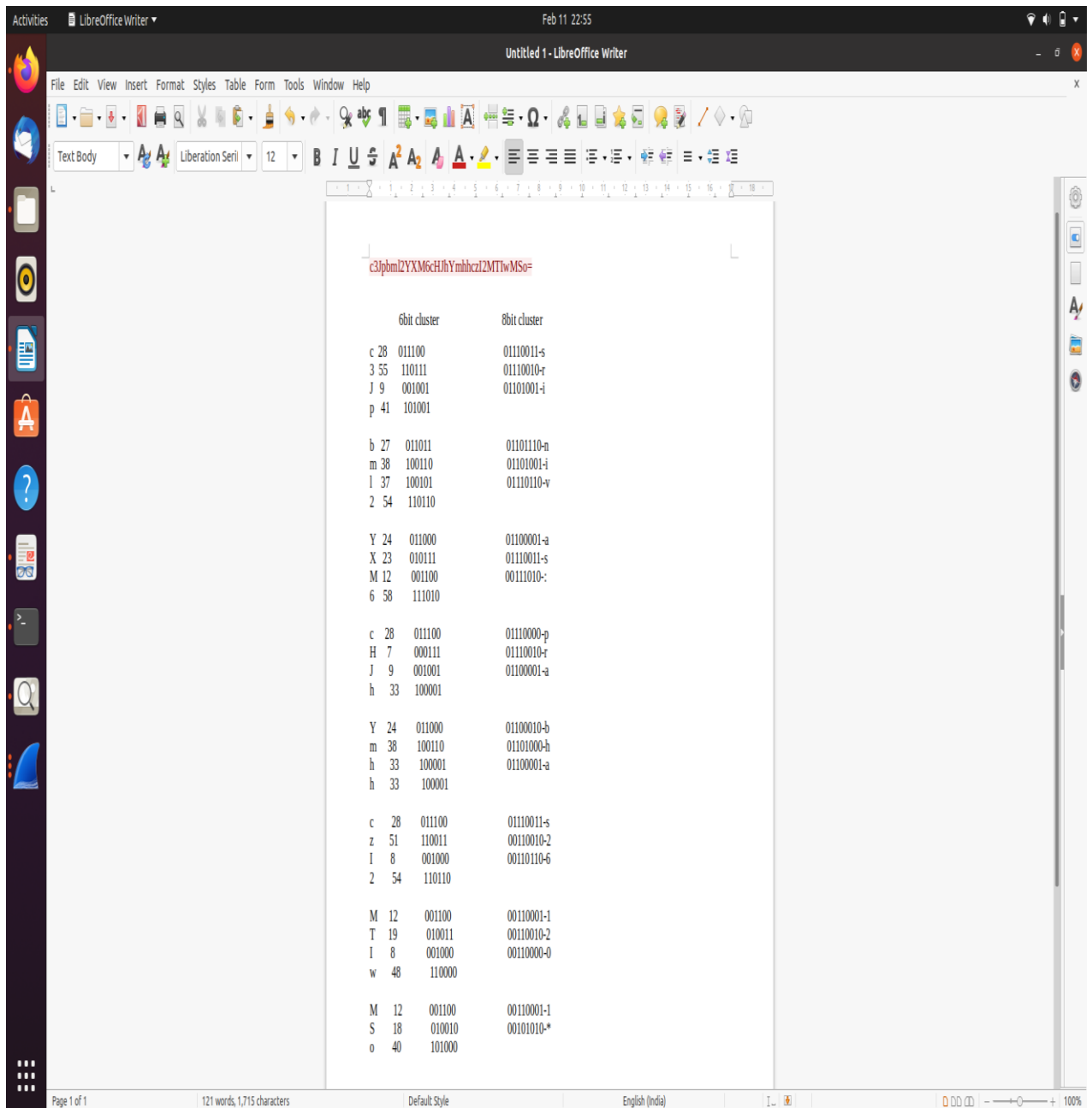

CAPTURE OF PACKETS SENT UPON THE NETWORK:
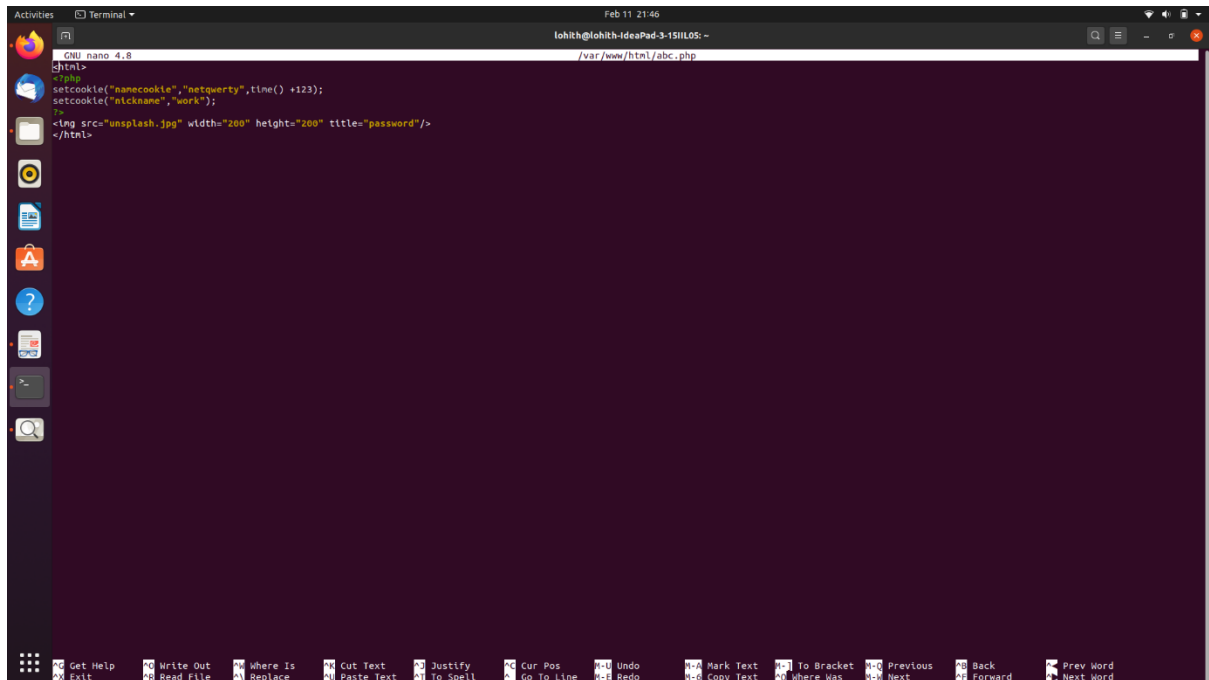
FOLLOWING TCP STREAM:

Week 3 - HTTP Headers_Auth_Cookies (1).pdf   100% ▾

Wireshark · Follow TCP Stream (tcp.stream eq 24) · any

tcp.stream eq 13   Expression... +

```
GET / HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:79.0) Gecko/20100101 Firefox/79.0
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 c3Jpbml2YXM6cHJhYmhhczI2MTIwMSo=
Connection: keep-alive
Upgrade-Insecure-Requests: 1
If-Modified-Since: Thu, 11 Feb 2021 05:07:24 GMT
If-None-Match: "2aa6-5bb087ec42bef-gzip"

HTTP/1.1 200 OK
Date: Thu, 11 Feb 2021 05:22:10 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Thu, 11 Feb 2021 05:07:24 GMT
ETag: "2aa6-5bb087ec42bef-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
```

...........Z.s.6.....U..$'....."{&.c....$....."!   c....d5..~..H.%..5..H....o.........n........./..
7...=...........d..........0...GzKc.q.n6.`.<.j.N?..Hk....).b...&...J$............L......w2.s.b2WrE...+6.4!R...d...4....
o.6$KcjX<&'....p8........d...Y.-S.   3,[.px2..........d4..['+f..;'....w)..3.nS.#..:...`BT.%..Tif.?Mo...
=%..`..R.-......L.rK. ./.l....-v...
F...l".{d.bN.{:R.%.z..g.aE..hL....K....y.h}....7.....su.sXY.{yd..ht.P2K.A$.Tc.........>..
.t..vL..TL..'.<e......U..F..S.n..*......L.R.|..(O.R0\..t.7&.j..921......`^.
..rLF...&.n..4F..N..}..fLhfd.68..r.........x.'9..;7.......#..c....~....~..h.;.u.   ..isv.................)Dn.
7.?.....:e?.!.....6."....5F.K|^.0a...H........l$..m........p./....xu.v.
[...y..l/....l..c.jF.c....:-IsZ;...N..#...b.....:..F.V...<e.>v^..)U....[f.
.#.dT..
5...x<...X.
B.
....
.5z...%..=p.no&...
.uX.:.|o..+y....i.{...._... .@VK~'?<*.UE.SP+}.'......M..b....n..N...\HH... .....__..p..u.9jX..,..:..LX...r......-Zs........
1..   ..Y.u..-GR   ...u.NU.=KJ.v-.(.V.^^.\....C.~..r.%.k.$.
.#....C.V............a#.S..s)J..{V}Z.@..Ql.-X.h...B...0.=.@....d.#T@'.;..p..shP
Kdmy.o.n.!....Z..
-CP..8...j7k...K.kp..E....^..&.o.._...N?........X...@......=.......IH/.=Gh......K.....#]..G|.{8...Z.d...^.g./
\W^..^...p......*:...y..D.2.h..{...`...-_..t.5..8..}.n.......f......... -*.@....].$rnW....8"..l..
......0.V.I..A.L...(.......P.....n..N..t6K.-.JO.   .
w.).......&n.`N.2#....c.......%+F...5%.....6W.+..S. n.a2D..Q.T.).6 ..c....!{\(.
.1.   .{.....!#.M....s....... .<..C..'!<|Jfl...&.d....%C.UY..u&aZ..v......B..VT.G)."..3.9.i.C...h.}"7p.....`.i.
3}.F..@..~..e..|61. K..r.8C..l)..1!C .$b.....!@..;i.......c...uK..GMh.}<,RX$4-.....U.i...... .^..3....0..m.......s...

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (3,952 bytes) ▾   Show and save data as   ASCII ▾   Stream 24

BASE64 ALGORITHM DECRYPTION:

c3Jpbml2YXM6cHJhYmhhczI2MTIwMSo=

		6bit cluster	8bit cluster
c	28	011100	01110011-s
3	55	110111	01110010-r
J	9	001001	01101001-i
p	41	101001	
b	27	011011	01101110-n
m	38	100110	01101001-i
l	37	100101	01110110-v
2	54	110110	
Y	24	011000	01100001-a
X	23	010111	01110011-s
M	12	001100	00111010-:
6	58	111010	
c	28	011100	01110000-p
H	7	000111	01110010-r
J	9	001001	01100001-a
h	33	100001	
Y	24	011000	01100010-b
m	38	100110	01101000-h
h	33	100001	01100001-a
h	33	100001	
c	28	011100	01110011-s
z	51	110011	00110010-2
I	8	001000	00110110-6
2	54	110110	
M	12	001100	00110001-1
T	19	010011	00110010-2
I	8	001000	00110000-0
w	48	110000	
M	12	001100	00110001-1
S	18	010010	00101010-*
o	40	101000	

srinivas:prabhas261201*

2.Cookie Setting

CREATION OF PHP FILE TO SET THE COOKIE:

PACKETS CAPTURE AND FOLLOWING TCP STREAM:


```
GET /abc.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:79.0) Gecko/20100101 Firefox/79.0
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 c3Jpbml2YXM6cHJhYmhhczI2MTIwMSo=

HTTP/1.1 200 OK
Date: Thu, 11 Feb 2021 15:45:14 GMT
Server: Apache/2.4.41 (Ubuntu)
Set-Cookie: namecookie=netqwerty; expires=Thu, 11-Feb-2021 15:47:17 GMT; Max-Age=123
Set-Cookie: nickname=work
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 93
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

*The Cookie name, value and the associated parameters can be viewed under the HTTP header Set-Cookie. We can observe the name, value, and the expiry time of the set cookie, if the cookie has not already expired.

3. Conditional Get

Simple 5 line html page.

FIRST HTTP GET REQUEST:
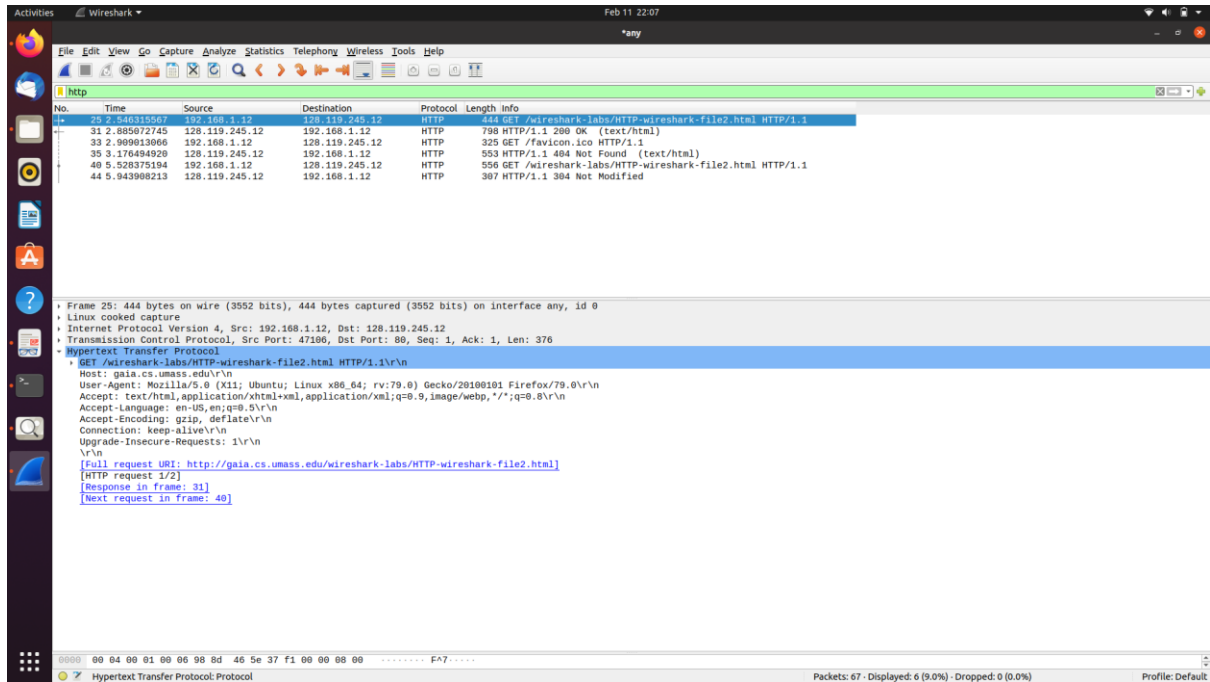
SERVER RESPONSE:
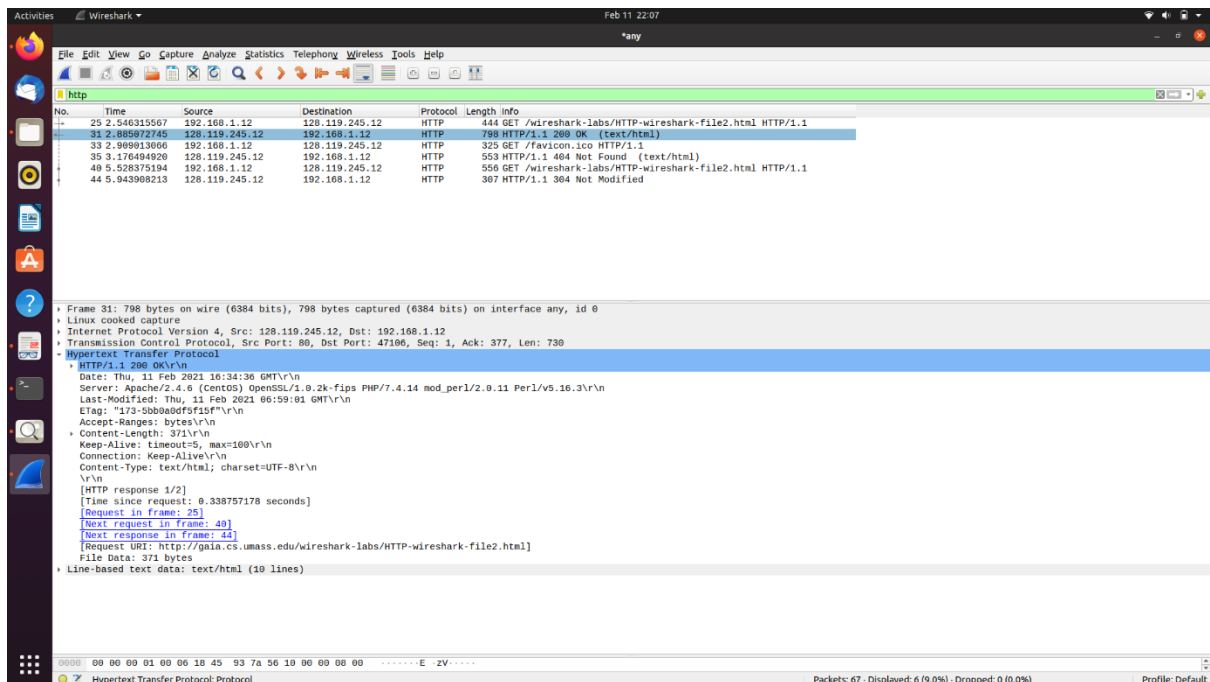
SECOND HTTP REQUEST:
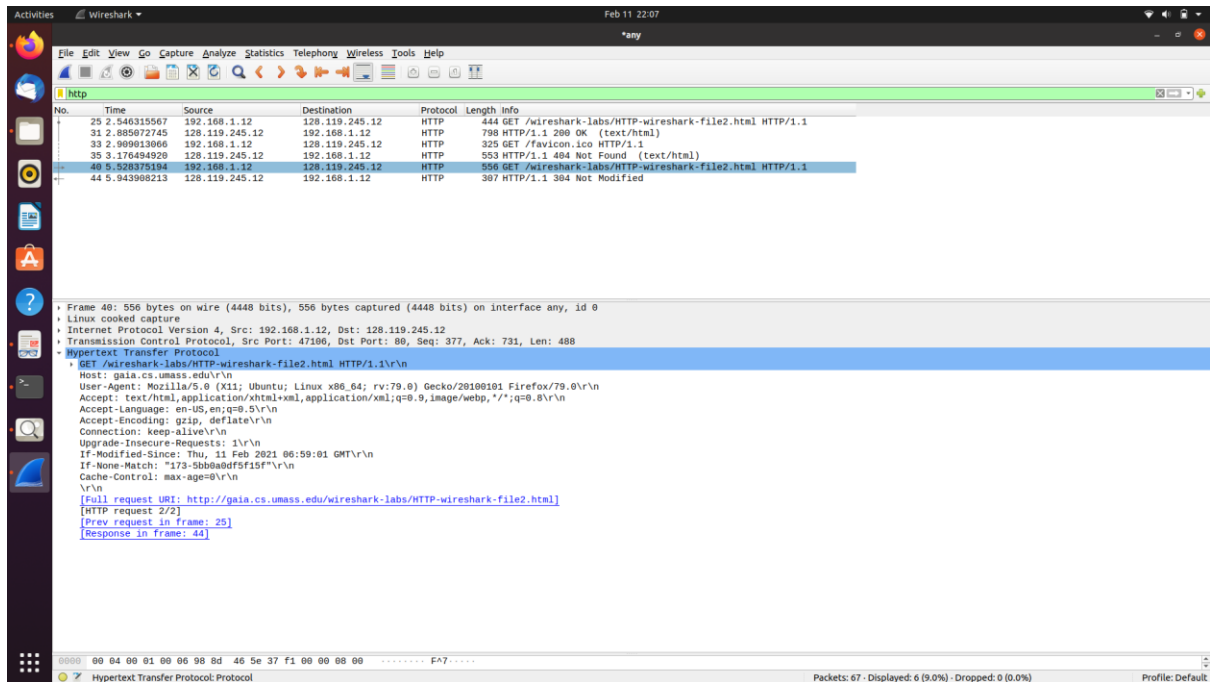
SERVER RESPONSE:
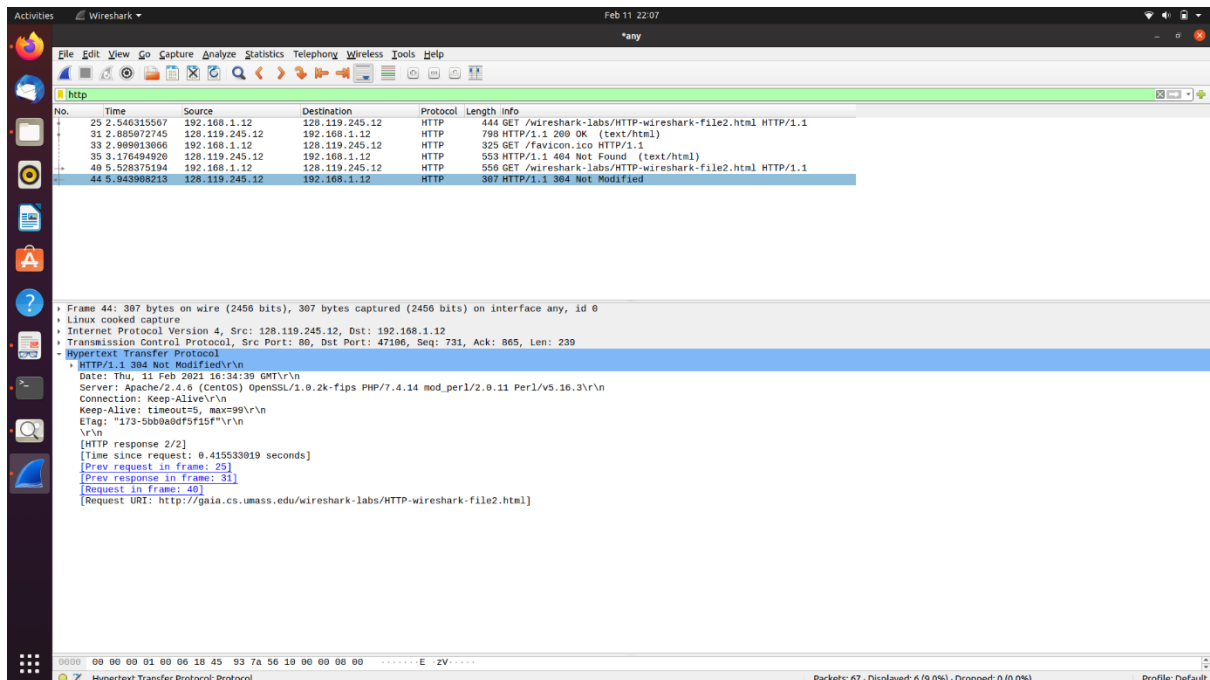
TCP STREAM:
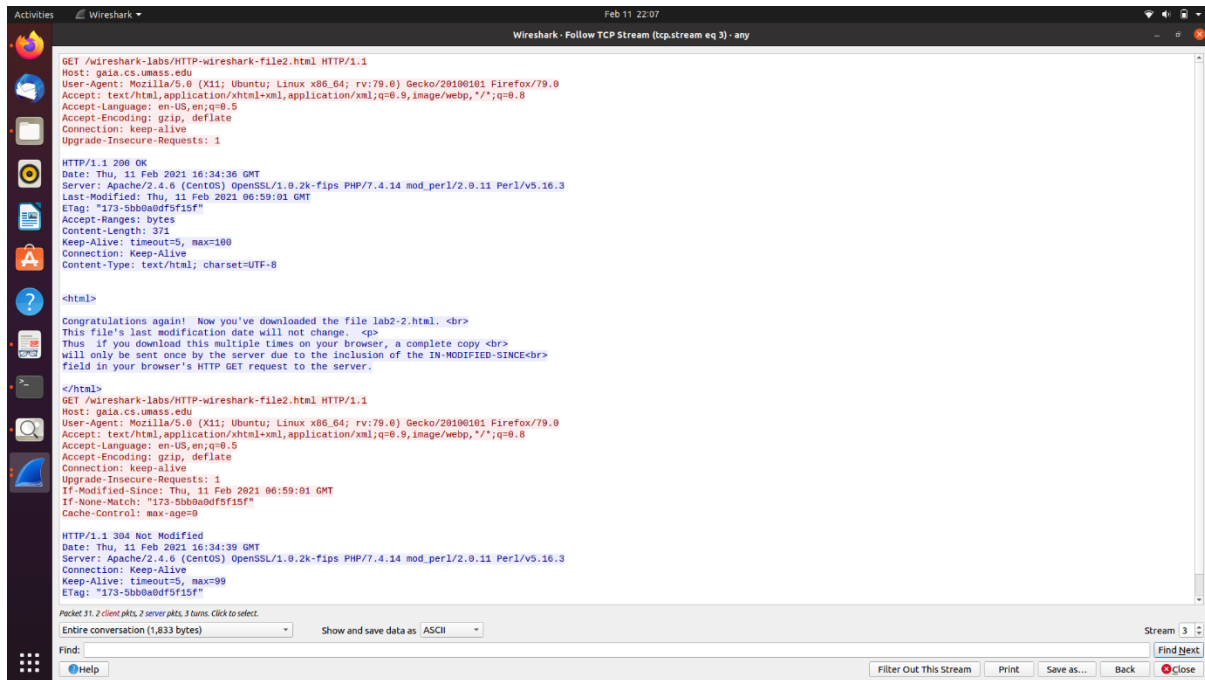
***The HTTP header If-Modified-Since is a way to implement Conditional GET .

***The server checks If-Modified-Since header value and resends the resource only if it has been modified since the timestamp in the header .

*** A 304 Not Modified status code is sent back, If it has not been modified,

1.An HTML page is requested by the client and the HTML file is obtained along with a 200 OK response status.

2. The second response from the server is obtained as 304 Not Modified since the resource has not been modified since the last GET.(REFRESHING OR AGAIN OPENING)

Html page with 2 images

PACKET CAPTURE UPON NETWORK:
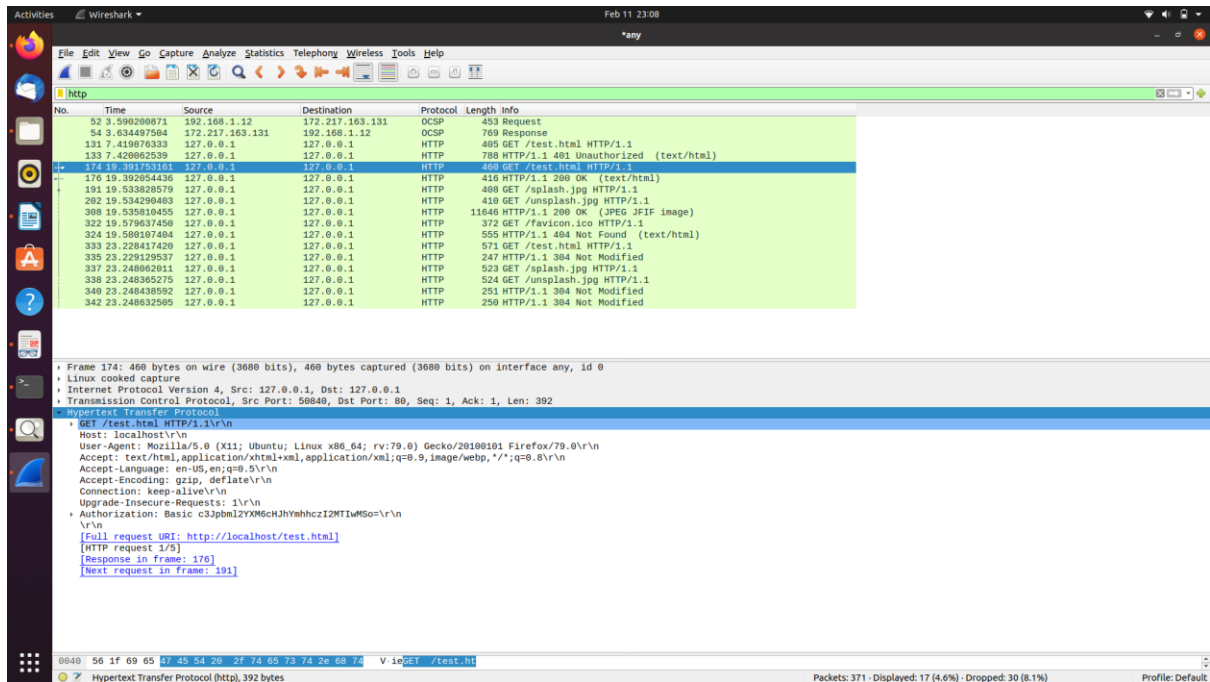
TCP FOLLOW FOR THE TWO IMAGES:

```
GET /splash.jpg HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:79.0) Gecko/20100101 Firefox/79.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Basic c3Jpbml2YXM6cHJhYmhhczI2MTIwMSo=
Connection: keep-alive
Referer: http://localhost/test.html
If-Modified-Since: Thu, 11 Feb 2021 17:27:04 GMT
If-None-Match: "26f6c7-5bb12d400ebb9"
Cache-Control: max-age=0

HTTP/1.1 304 Not Modified
Date: Thu, 11 Feb 2021 17:37:09 GMT
Server: Apache/2.4.41 (Ubuntu)
Connection: Keep-Alive
Keep-Alive: timeout=5, max=96
ETag: "26f6c7-5bb12d400ebb9"
```