COMPUTER NETWORKS LAB – WEEK 3

Name: TUSHAR Y S

SRN: PES1UG19CS545

1. Password Authentication:

1.1. Setting the username and password:

- The apache utilities are installed using the following command:

    sudo apt-get install apache2 apache2-utils

- We can set a password for a given user and write it into .htpasswd file after running the following command:

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

Here username is 'tushar'

- To view the authentication , following command is used:

sudo cat /etc/apache2/.htpasswd

```
tushar@tushar:~$ sudo cat /etc/apache2/.htpasswd
tushar:$apr1$HFr9Ea21$e39WJyvBMa0CYcAD/8ihL0
tushar@tushar:~$
```

1.2. Setting up the Authentication phase:

- The file is opened for authentication by using the command:

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

The file is modified by writing the following:

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

```
    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
```
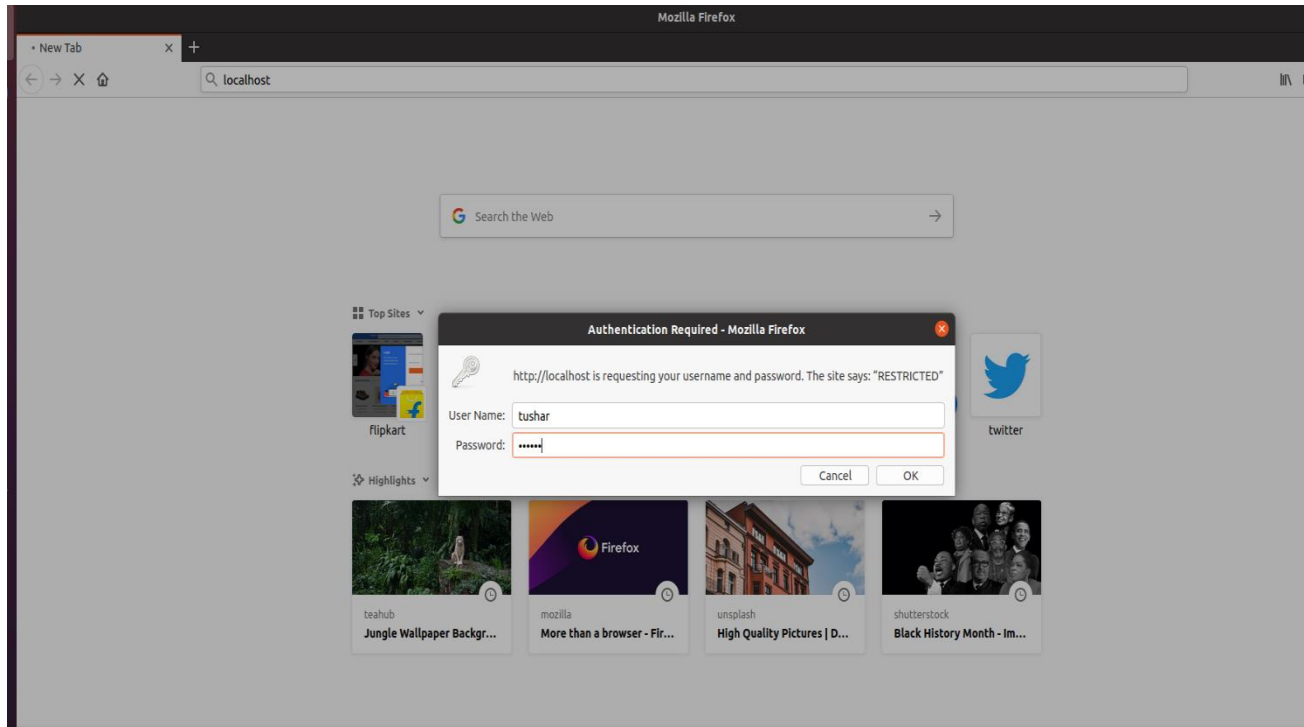
- Password policy implementation is done by restarting the apache server by using the command:

sudo service apache2 restart

```
tushar@tushar:~$ sudo service apache2 restart
tushar@tushar:~$ 
```
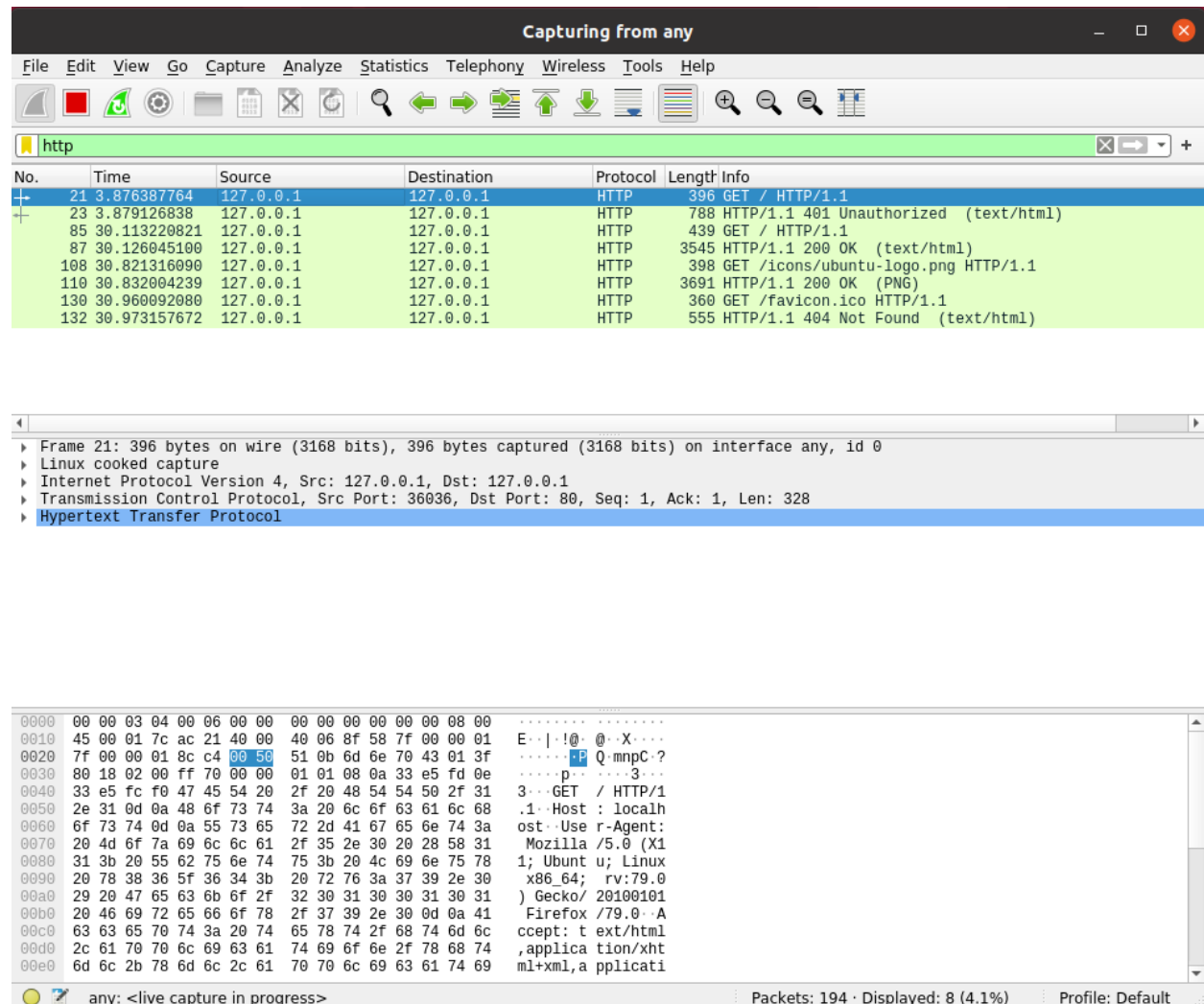
1.3. Accessing the localhost:

- The local host is accessed using the browser by entering the username and password.
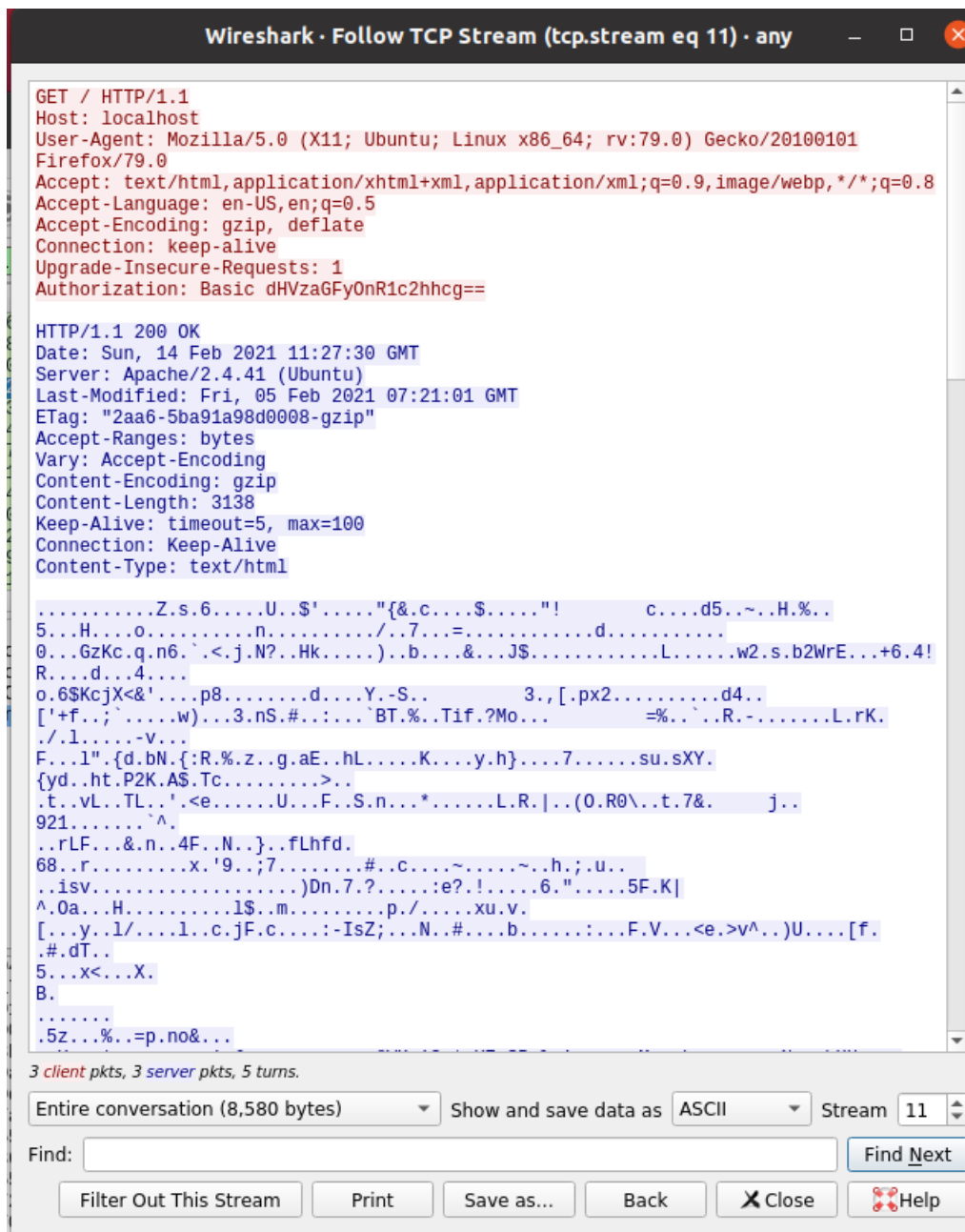
1.4. Packets capture using Wireshark

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

Wireshark packet capture:

- Using the 'follow TCP stream' on HTTP message segment the password is retrieved which is being encrypted by the base64 algorithm.

```
Wireshark · Follow TCP Stream (tcp.stream eq 11) · any      —   □   ✕

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
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Authorization: Basic dHVzaGFyOnR1c2hhcg==

HTTP/1.1 200 OK
Date: Sun, 14 Feb 2021 11:27:30 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Fri, 05 Feb 2021 07:21:01 GMT
ETag: "2aa6-5ba91a98d0008-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$.Tc.........>..
.t..vL..TL..'.<e......U...F..S.n...*......L.R.|..(O.R0\..t.7&.     j..
921.......`^.
..rLF...&.n..4F..N..}..fLhfd.
68..r.........x.'9..;7........#..c....~.....~..h.;.u..
..isv...................)Dn.7.?.....:e?.!.....6."....5F.K|
^.Oa...H..........l$..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&...
```

3 *client* pkts, 3 *server* pkts, 5 turns.

Entire conversation (8,580 bytes) ▾   Show and save data as ASCII ▾   Stream 11 ⬍

Find: [   ]   Find Next

Filter Out This Stream   Print   Save as...   Back   ✕ Close   Help

As we can observe above, the encrypted content is :

"dHVzaGFyOnR1c2hhcg"

1.5. Decrypting the encryption (base64 algorithm):

Encrypted Character	Index	Binary Equivalent
d	29	011101
H	7	000111
V	21	010101
z	51	110011
a	26	011010
G	6	000110
F	5	000101
y	50	110010
O	14	001110
n	39	100111
R	17	010001
1	53	110101
c	28	011100
2	54	110110
h	33	100001
h	33	100001
c	28	011100
g	32	100000

Combined 8 bit word	ASCII Value	Decrypted Character
01110100	116	t
01110101	117	u
01110011	115	s
01101000	104	h
01100001	97	a
01110010	114	r
00111010	58	:
01110100	116	t
01110101	117	u
01110011	115	s
01101000	104	h
01100001	97	a
01110010	114	r

Therefore, the decrypted content is:

tushar:tushar

The word before the semi colon is the username.
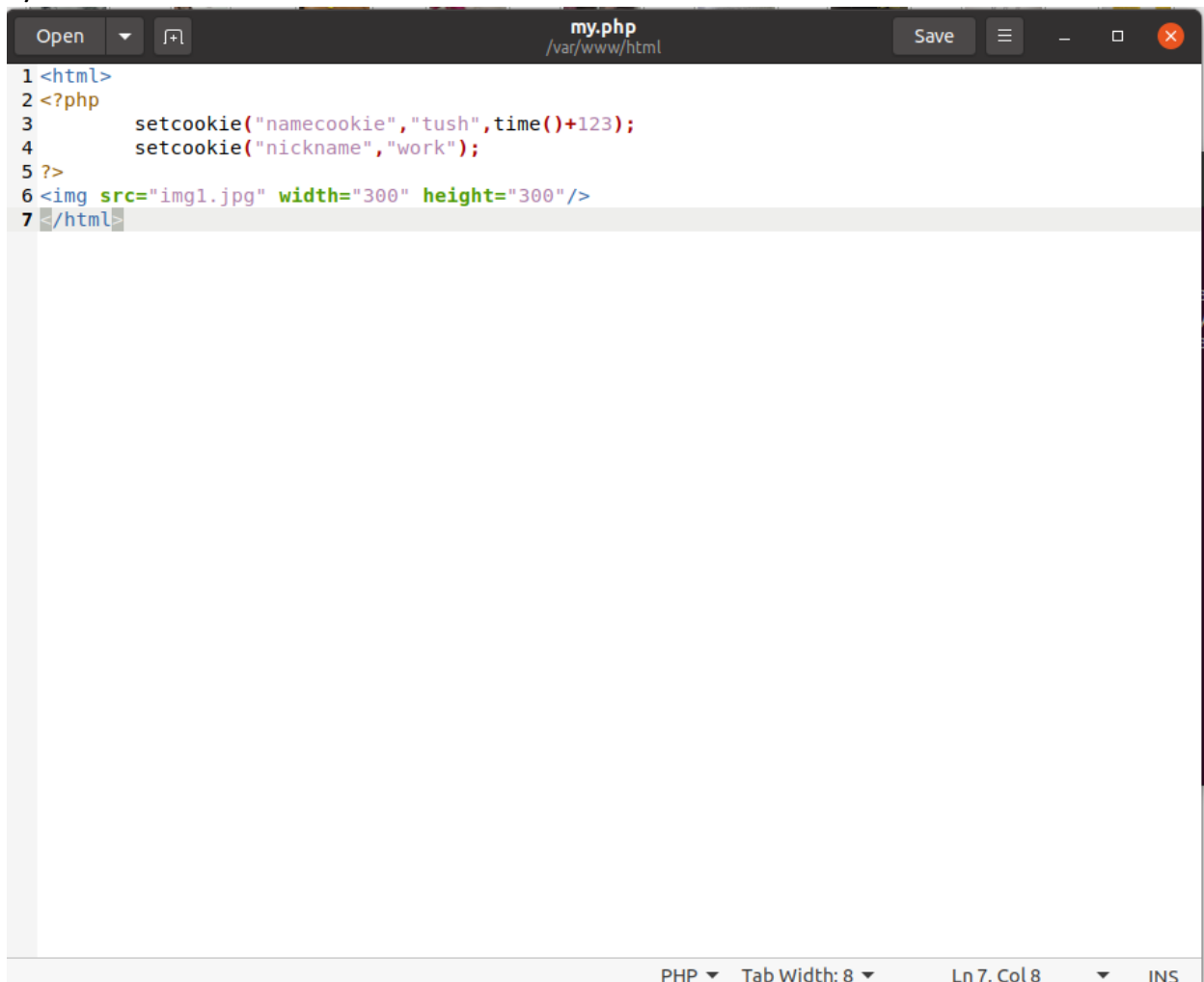
The word after the semi colon is the password corresponding to that username.

2. Cookie Setting:

2.1. Cookie setting using PHP:

- A PHP file is created to set the cookie using the following code:

```html
<html>
<?php
        setcookie("namecookie","tush",time()+123);
        setcookie("nickname","work");
?>
<img src= "img1.jpg" width= "300" height= "300" />
</html>
```

```
1 <html>
2 <?php
3         setcookie("namecookie","tush",time()+123);
4         setcookie("nickname","work");
5 ?>
6 <img src="img1.jpg" width="300" height="300"/>
7 </html>
```

This 'my.php' is palced under /var/www/html.

2.2. Wireshark Packet Capture:

- The php file is accessed using the browser.
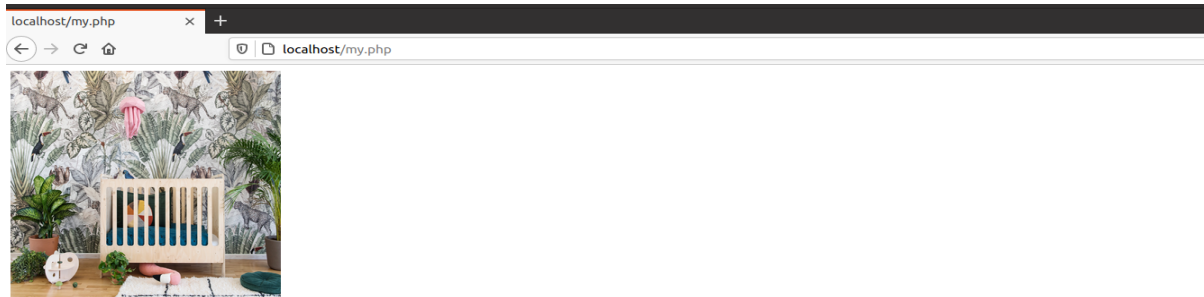
- At the same time, packets are captured using wireshark.
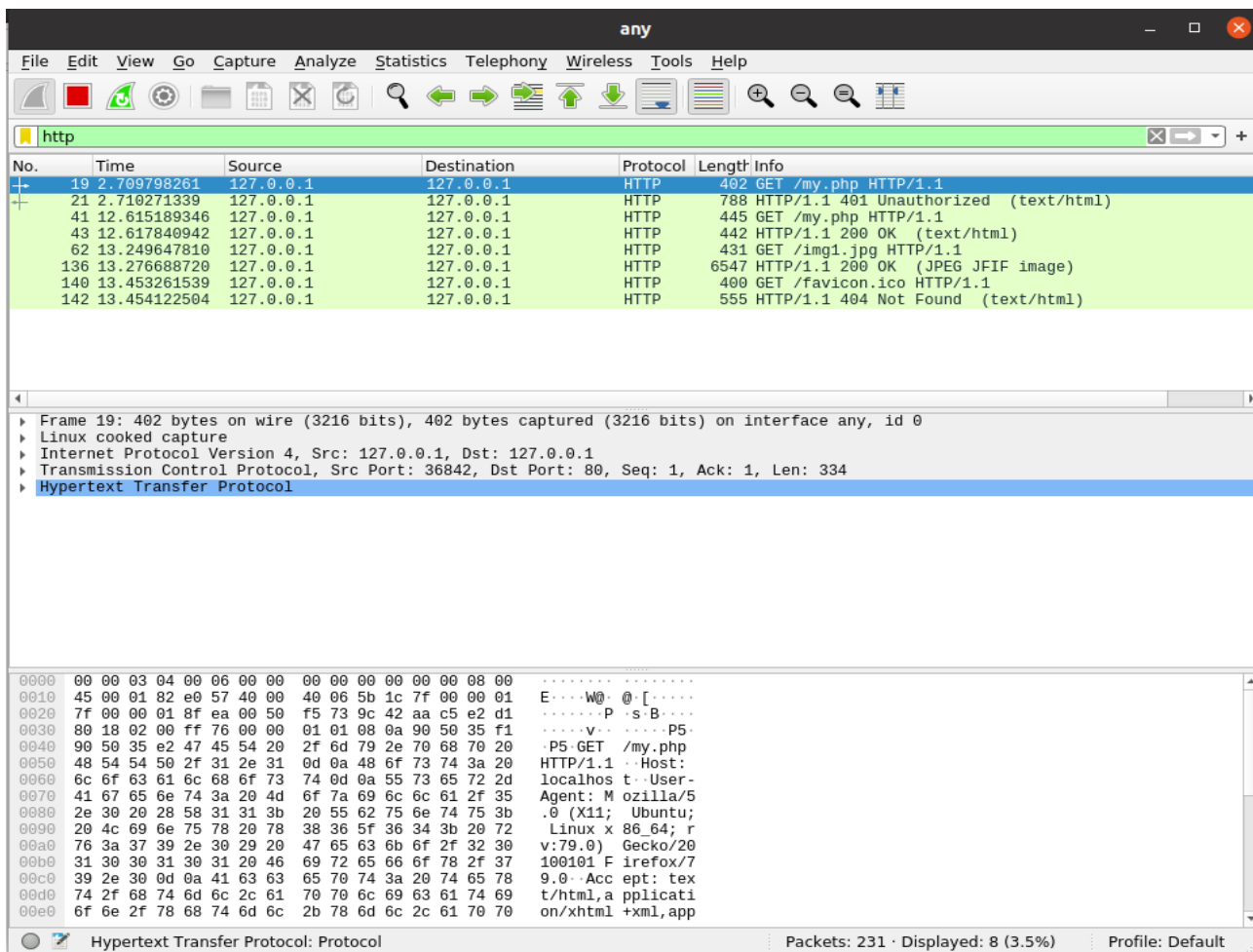
- The packet of GET request for the php file is analyzed and its follow TCP stream is shown below:

Wireshark · Follow TCP Stream (tcp.stream eq 8) · any

```
GET /my.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 dHVzaGFyOnR1c2hhcg==

HTTP/1.1 200 OK
Date: Sun, 14 Feb 2021 17:14:37 GMT
Server: Apache/2.4.41 (Ubuntu)
Set-Cookie: namecookie=tush; expires=Sun, 14-Feb-2021 17:16:40 GMT; Max-Age=123
Set-Cookie: nickname=work
Content-Length: 62
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<html>
<img src="img1.jpg" width="300" height="300"/>
</html>
GET /img1.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 dHVzaGFyOnR1c2hhcg==
Connection: keep-alive
Referer: http://localhost/my.php
Cookie: namecookie=tush; nickname=work

HTTP/1.1 200 OK
Date: Sun, 14 Feb 2021 17:14:38 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Fri, 05 Feb 2021 10:26:28 GMT
ETag: "1b982b-5ba9440c6c108"
Accept-Ranges: bytes
Content-Length: 1808427
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
```
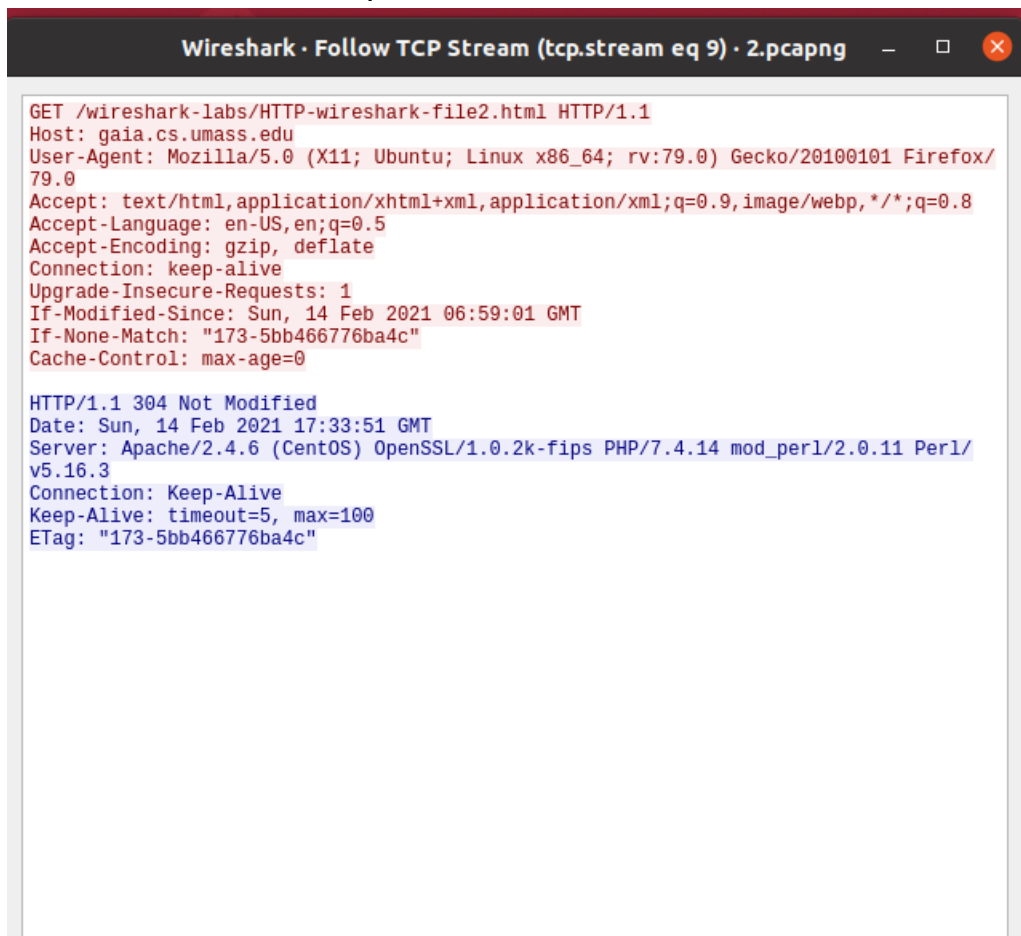
3 *client* pkts, 58 *server* pkts, 5 turns.

Entire conversation (1,810 kB) ▾   Show and save data as ASCII ▾   Stream 8 ⬍

Find: [   ]   Find Next

Filter Out This Stream   Print   Save as...   Back   ✕ Close   Help

From the above screenshot, it can be seen that the cookie has been set.

The cookie name, value and the expiry time of the cookie are some of the parameters associated with the cookie which can be observed above.

3. Conditional Get: If-Modified-Since

3.1. Conditional Get for plain HTML:

- The browser cache and browser history is cleared.

- Wireshark is launched.

- The following URL is entered in the browser:

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

Next, the website is refreshed.

- Wireshark packet capture:

As can be observed above, the response for the first GET request is having a 200 OK response status. The response from the server for the second request is obtained as '304 Not Modified'. This is because we just refreshed the page and while doing so there wasn't any change in the content of the resource(it wasn't modified).

- Follow TCP Stream:

    First GET request:

As can be observed from the above screenshot, there is no "If-Modified-Since" line for the first GET request.

Server Response for first GET request:

```
Wireshark · Follow TCP Stream (tcp.stream eq 3) · 2.pcapng     –  ▢  ✕

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: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

HTTP/1.1 200 OK
Date: Sun, 14 Feb 2021 17:33:25 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
Last-Modified: Sun, 14 Feb 2021 06:59:01 GMT
ETag: "173-5bb466776ba4c"
Accept-Ranges: bytes
Content-Length: 371
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8


<html>

Congratulations again!  Now you've downloaded the file lab2-2.html. <br>
This file's last modification date will not change.  <p>
Thus  if you download this multiple times on your browser, a complete copy <br>
will only be sent once by the server due to the inclusion of the IN-MODIFIED-
SINCE<br>
field in your browser's HTTP GET request to the server.

</html>
```
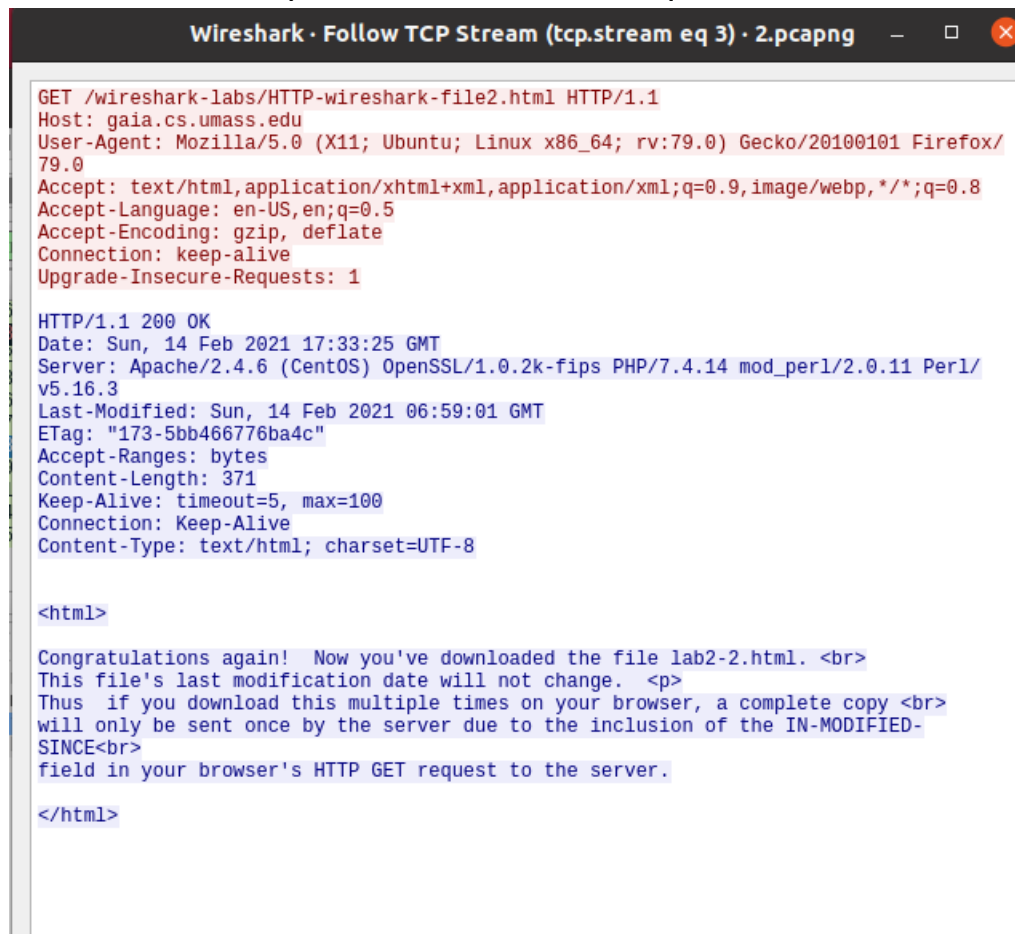
As can be observed above, the server has explicitly returned the content of the file. The HTML file contents can be seen above.

Second GET request:


```
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: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
If-Modified-Since: Sun, 14 Feb 2021 06:59:01 GMT
If-None-Match: "173-5bb466776ba4c"
Cache-Control: max-age=0

HTTP/1.1 304 Not Modified
Date: Sun, 14 Feb 2021 17:33:51 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: "173-5bb466776ba4c"
```

From the above screenshot , we can see the "If-Modified-Since" field for the second GET request(if the resource remains unmodified).

The "If-Modified-Since" header indicates the time for which a browser first downloaded a resource from the server.

Server response for second GET request:


```
Wireshark · Follow TCP Stream (tcp.stream eq 9) · 2.pcapng    –   □   ✕

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: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
If-Modified-Since: Sun, 14 Feb 2021 06:59:01 GMT
If-None-Match: "173-5bb466776ba4c"
Cache-Control: max-age=0

HTTP/1.1 304 Not Modified
Date: Sun, 14 Feb 2021 17:33:51 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: "173-5bb466776ba4c"
```

The server response for the second GET request is having a response status code and phrase of "304 Not Modified".

The server hasn't explicitly returned the contents of the file(as the request is made for the second time and the resource remains unchanged).

3.2. Conditional GET in Local machine(with some image):

- The browser cache and browser history is cleared.

- Wireshark is launched.

- A html file named 'this.html' is placed under the html directory.

- This html file accessed with the help of a web browser
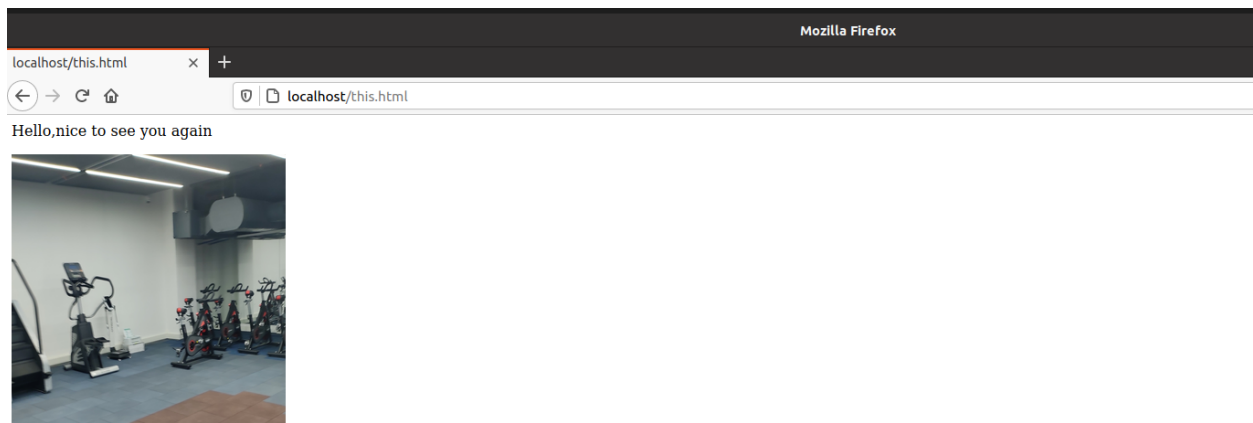
Now the website is refreshed.

- Wireshark Packet Capture:
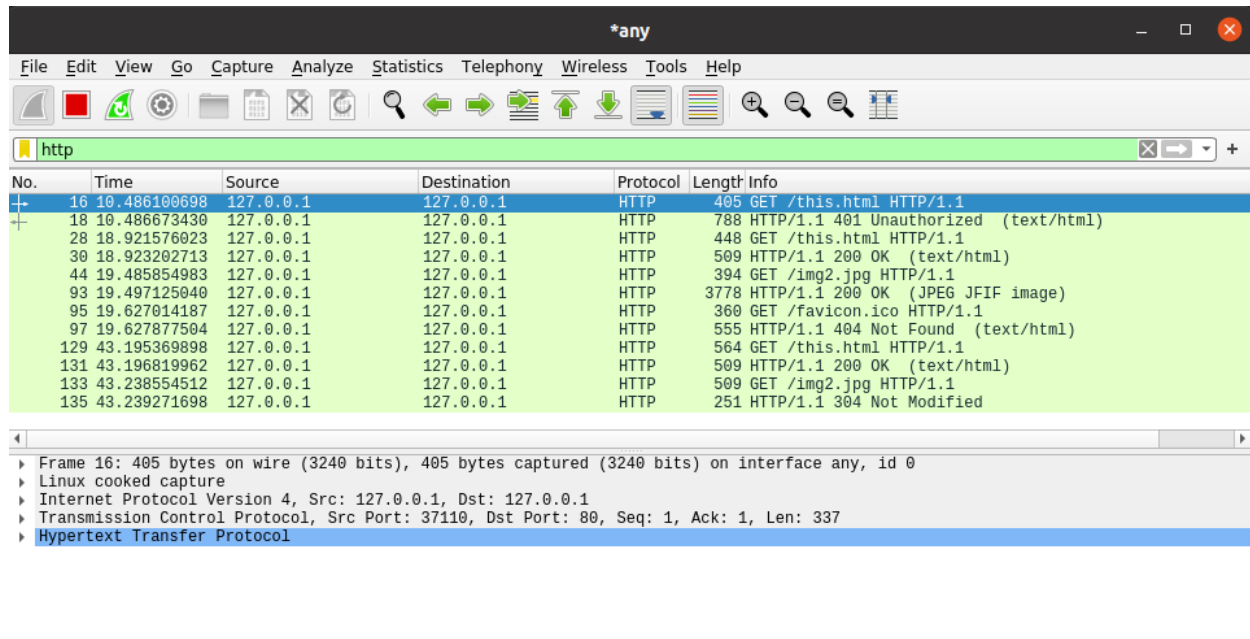
Again, the response for the first GET request of image is having a 200 OK response status. The response from the server for the second request of image is obtained as '304 Not Modified'. Since the image wasn't modified , we get '304 Not Modified' server response.

- Follow TCP Stream:

First GET request:

As can be observed from the above screenshot, there is no "If-Modified-Since" line for the first GET request.

Server response for first GET request:

As can be observed above, the server has explicitly returned the content of the file. GET request is made further for obtaining the image from the server.

Second GET request:

From the above screenshot , we can see the "If-Modified-Since" field (highlighted in blue color)for the second GET request(if the resource remains unchanged).

The "If-Modified-Since" header indicates the time for which a browser first downloaded a resource from the server.

Server response for second GET request:

```
Content-Type: text/html

...........(.....)..H......LNU(.W(NMU../UHLO..../.*..MW(.J.U.2...
...2R3.3J1..
....3SJ2 1}.r}....../a...GET /img2.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 dHVzaGFyOnR1c2hhcg==
Connection: keep-alive
Referer: http://localhost/this.html
If-Modified-Since: Fri, 05 Feb 2021 14:45:53 GMT
If-None-Match: "118d5a-5ba97e0835d54"
Cache-Control: max-age=0

HTTP/1.1 304 Not Modified
Date: Sun, 14 Feb 2021 17:45:25 GMT
Server: Apache/2.4.41 (Ubuntu)
Connection: Keep-Alive
Keep-Alive: timeout=5, max=99
ETag: "118d5a-5ba97e0835d54"
```

2 *client* pkts, 2 *server* pkts, 3 turns.

Entire conversation (1,561 bytes) ▼   Show and save data as ASCII   ▼ Stream 6 ⬍

Find: [   ]   Find Next

Filter Out This Stream   Print   Save as...   Back   ✕ Close   ✖ Help

The server response for the second GET request is having a response status code and phrase of "304 Not Modified". This is because the resource which is being requested has not been modified.