Computer Networks Lab

UE19CS256

Week 3

Name: Sreenath Saikumar

Semester: 4 Section: G

SRN: PES2UG19CS406

Date: 10/02/2021

Objectives:

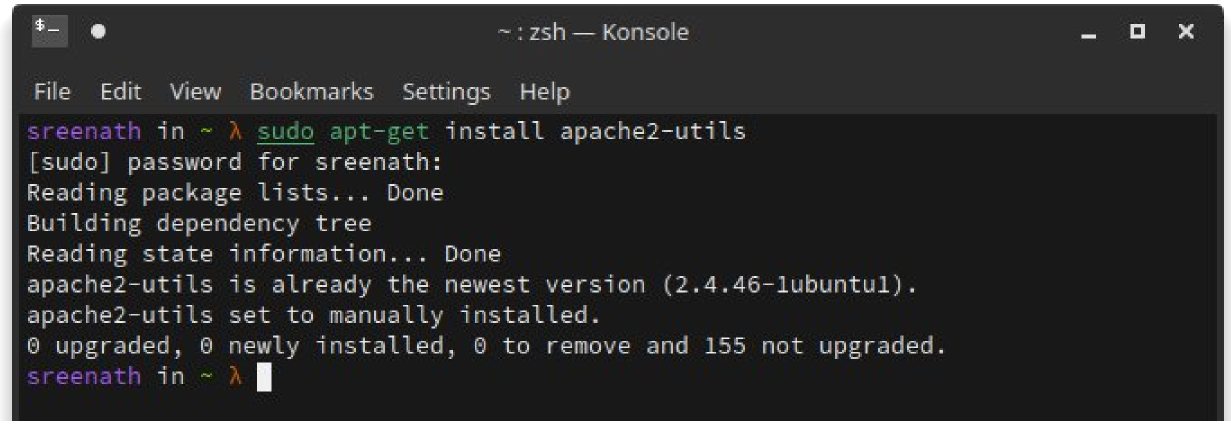
1. To understand working of HTTP headers, Conditional GET: If-modified-since.
2. To understand HTTP Cookies and Set-Cookie.
3. To understand Authentication: Auth-Basic.

Procedure for Password Authentication:

Step 1: Installing the Apache2 Utilities package

Ensure that the `apache2-utils` package is installed by using the command:

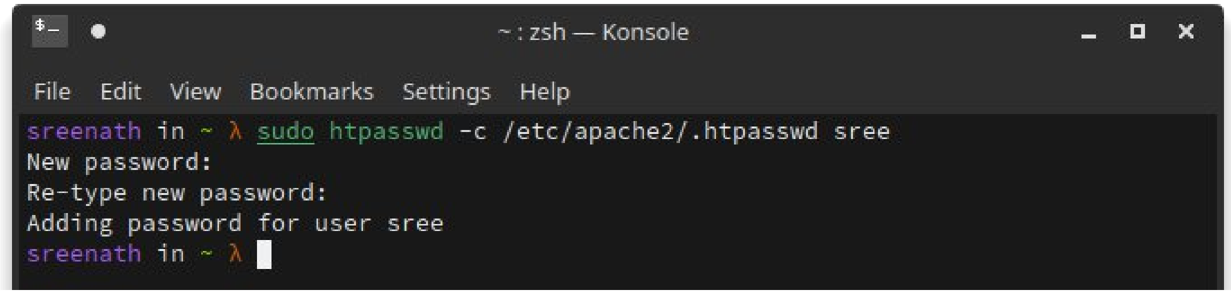
```
sudo <package manager> install apache2-utils
```



```
sreenath in ~ λ sudo apt-get install apache2-utils
[sudo] password for sreenath:
Reading package lists... Done
Building dependency tree
Reading state information... Done
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 155 not upgraded.
sreenath in ~ λ
```

Now provide the username and password to set authentication:

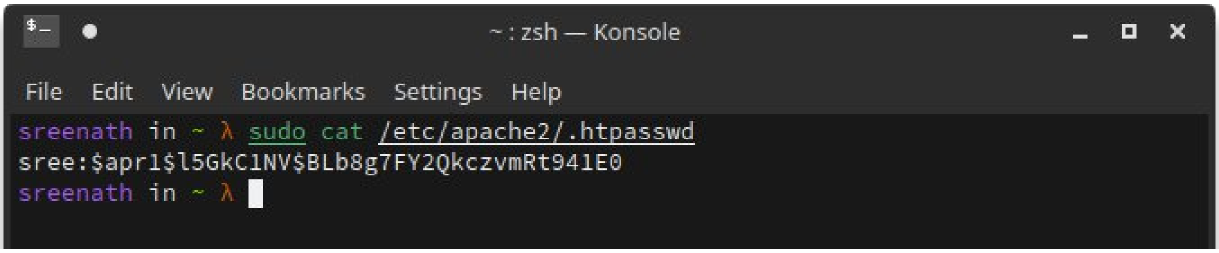
```
sudo htpasswd -c /etc/apache2/.htpasswd sree
```



```
sreenath in ~ λ sudo htpasswd -c /etc/apache2/.htpasswd sree
New password:
Re-type new password:
Adding password for user sree
sreenath in ~ λ
```

We can view the authentication we setup using:

```
sudo cat /etc/apache2/.htpasswd
```



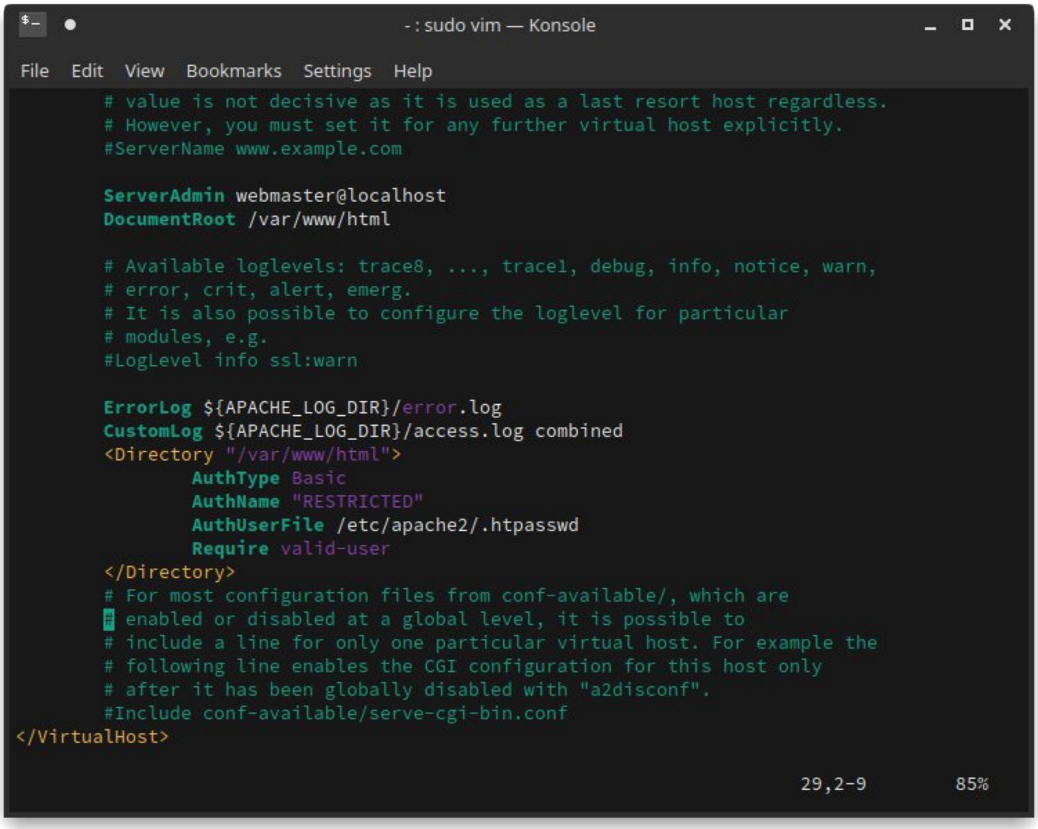
```
sreenath in ~ λ sudo cat /etc/apache2/.htpasswd
sree:$apr1$l5GkC1NV$BLb8g7FY2QkczvmRt941E0
sreenath in ~ λ 
```

Step 2: Setting up the authentication phase

To setup the authentication phase, execute the following commands to configure access control within the Virtual Host Definition.

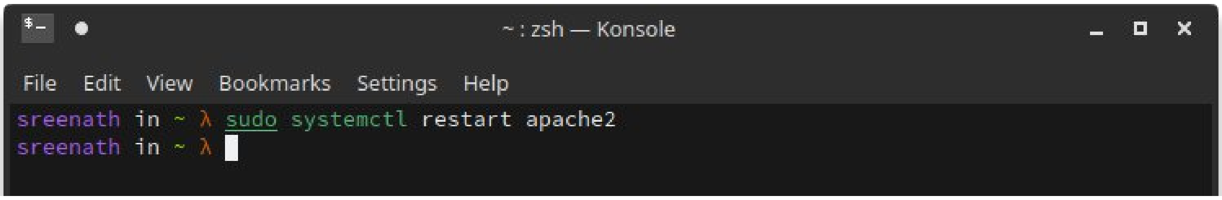
Open the file to set the authentication using

```
sudo vim /etc/apache2/sites/sites-available/000-default.conf
```



```
        # 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
</VirtualHost>

                                                            29,2-9        85%
```

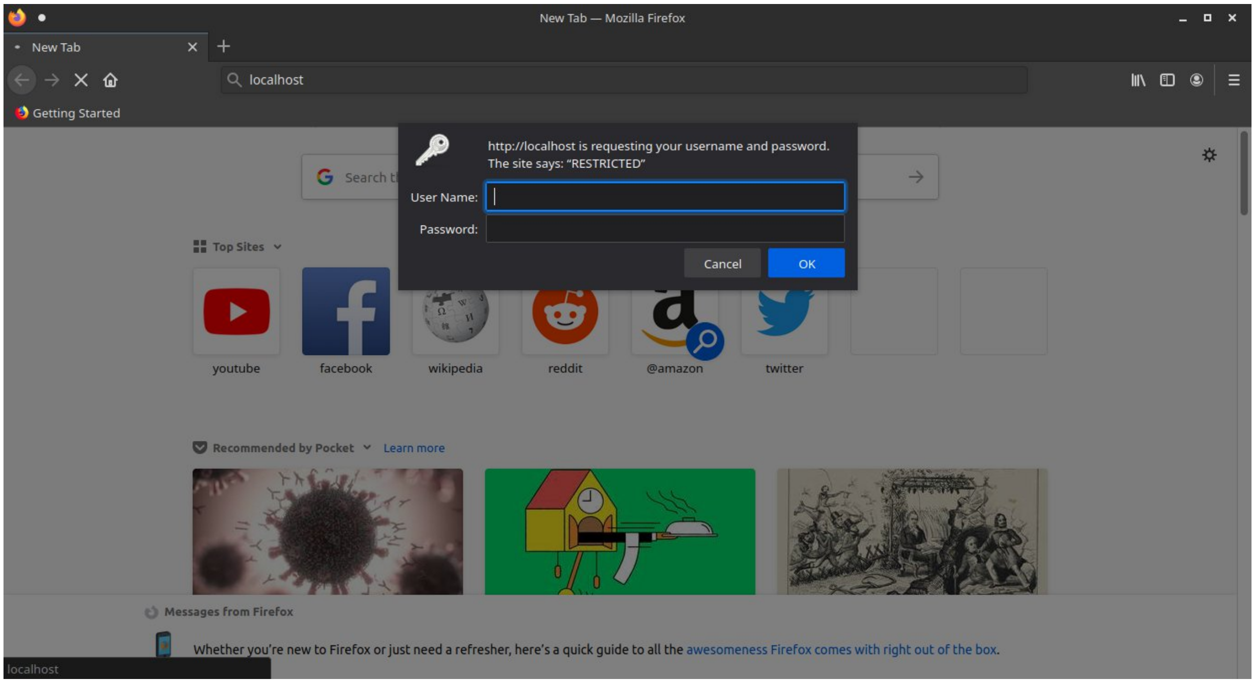
Now restart the `apache2` server using `sudo systemctl restart apache2` on a system that uses `systemd.`



```
sreenath in ~ λ sudo systemctl restart apache2
sreenath in ~ λ
```

Step 3: Accessing localhost using Firefox

The localhost is accessed using the Firefox web browser and we notice that there is now a prompt asking for a username and password for authentication.



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

User Name:

Password:

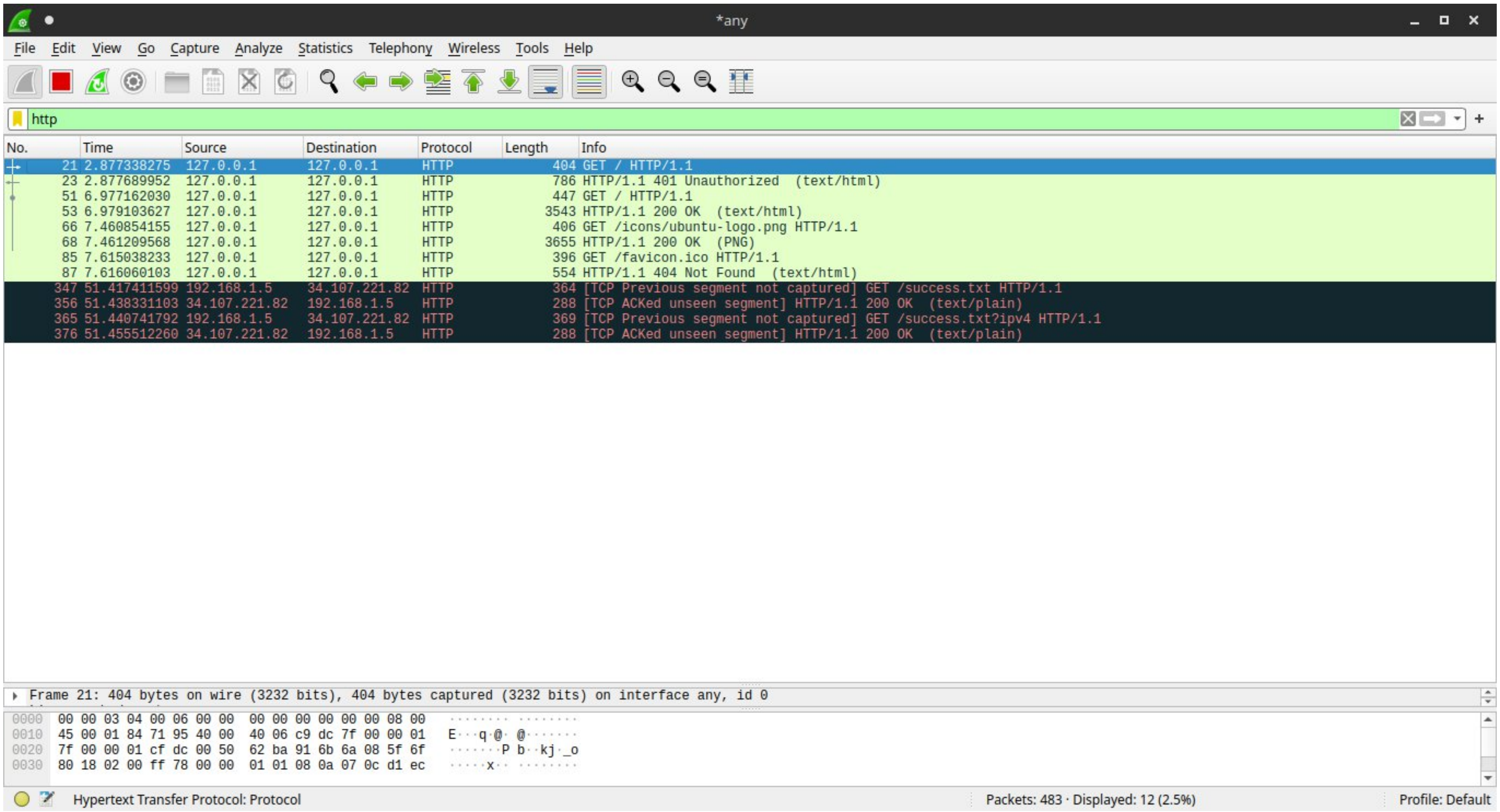
Cancel OK

Whether you're new to Firefox or just need a refresher, here's a quick guide to all the awesomeness Firefox comes with right out of the box.

We then capture any packets using Wireshark.

Step 4: Wireshark Captures

We inspect the GET request received using the Follow TCP Stream option.



*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

```
No.   Time         Source        Destination   Protocol Length Info
   21 2.877338275  127.0.0.1     127.0.0.1     HTTP        404 GET / HTTP/1.1
   23 2.877689952  127.0.0.1     127.0.0.1     HTTP        786 HTTP/1.1 401 Unauthorized  (text/html)
   51 6.977162030  127.0.0.1     127.0.0.1     HTTP        447 GET / HTTP/1.1
   53 6.979103627  127.0.0.1     127.0.0.1     HTTP       3543 HTTP/1.1 200 OK  (text/html)
   66 7.460854155  127.0.0.1     127.0.0.1     HTTP        406 GET /icons/ubuntu-logo.png HTTP/1.1
   68 7.461209568  127.0.0.1     127.0.0.1     HTTP       3655 HTTP/1.1 200 OK  (PNG)
   85 7.615038233  127.0.0.1     127.0.0.1     HTTP        396 GET /favicon.ico HTTP/1.1
   87 7.616060103  127.0.0.1     127.0.0.1     HTTP        554 HTTP/1.1 404 Not Found  (text/html)
  347 51.417411599 192.168.1.5   34.107.221.82 HTTP        364 [TCP Previous segment not captured] GET /success.txt HTTP/1.1
  356 51.438331103 34.107.221.82 192.168.1.5   HTTP        288 [TCP ACKed unseen segment] HTTP/1.1 200 OK  (text/plain)
  365 51.440741792 192.168.1.5   34.107.221.82 HTTP        369 [TCP Previous segment not captured] GET /success.txt?ipv4 HTTP/1.1
  376 51.455512260 34.107.221.82 192.168.1.5   HTTP        288 [TCP ACKed unseen segment] HTTP/1.1 200 OK  (text/plain)
```

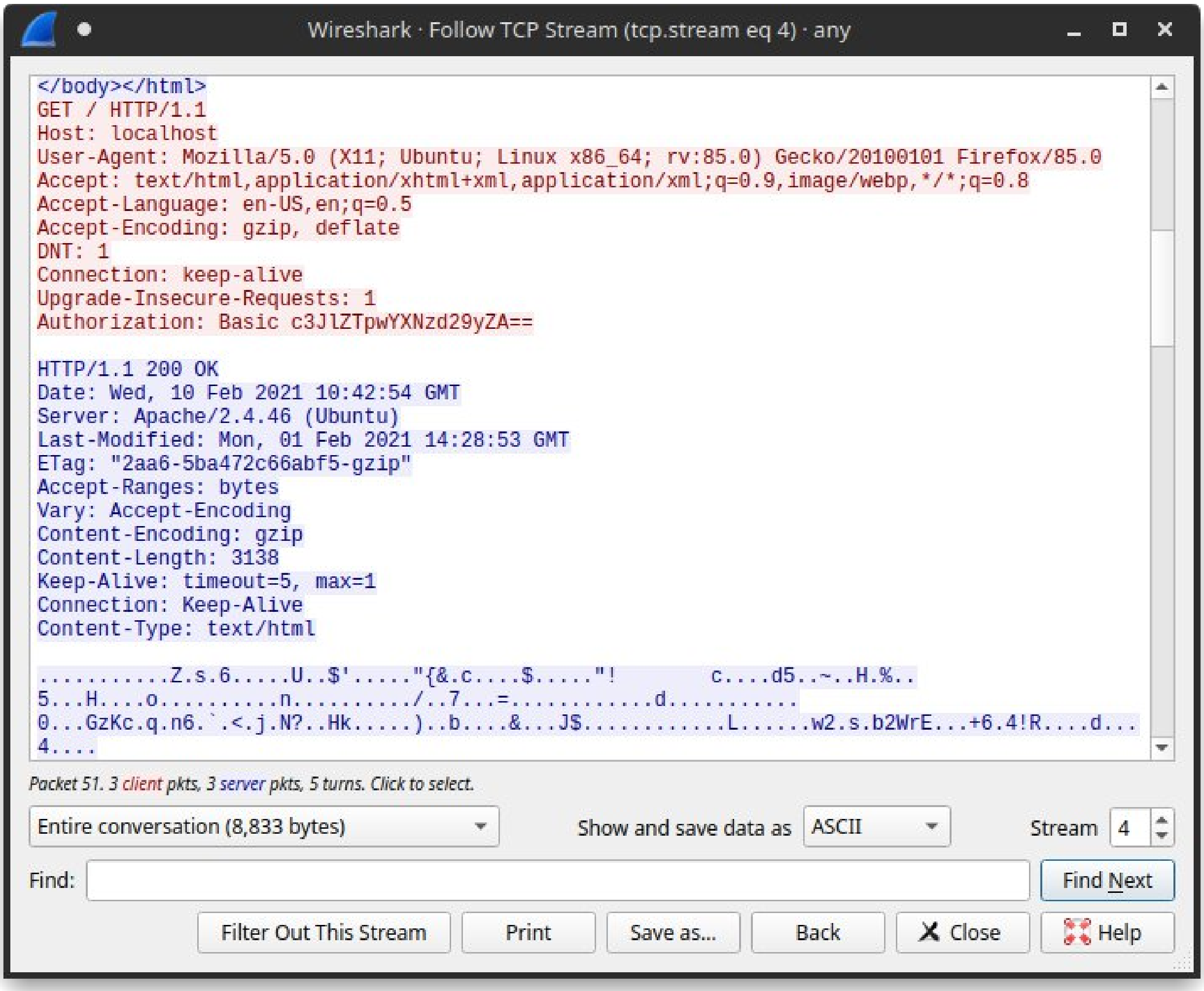
```
Frame 21: 404 bytes on wire (3232 bits), 404 bytes captured (3232 bits) on interface any, id 0
```

```
0000  00 00 03 04 00 06 00 00  00 00 00 00 00 00 08 00   ········ ········
0010  45 00 01 84 71 95 40 00  40 06 c9 dc 7f 00 00 01   E···q·@· @·······
0020  7f 00 00 01 cf dc 00 50  62 ba 91 6b 6a 08 5f 6f   ·······P b··kj·_o
0030  80 18 02 00 ff 78 00 00  01 01 08 0a 07 0c d1 ec   ·····x·· ········
```

Hypertext Transfer Protocol: Protocol

Packets: 483 · Displayed: 12 (2.5%)

Profile: Default



```
</body></html>
GET / HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:85.0) Gecko/20100101 Firefox/85.0
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
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Authorization: Basic c3JlZTpwYXNzd29yZA==

HTTP/1.1 200 OK
Date: Wed, 10 Feb 2021 10:42:54 GMT
Server: Apache/2.4.46 (Ubuntu)
Last-Modified: Mon, 01 Feb 2021 14:28:53 GMT
ETag: "2aa6-5ba472c66abf5-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 3138
Keep-Alive: timeout=5, max=1
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....
```

Packet 51. 3 client pkts, 3 server pkts, 5 turns. Click to select.

Entire conversation (8,833 bytes) | Show and save data as: ASCII | Stream: 4

Find:

Using the Follow TCP Stream option on the HTTP message segment, we can retrieve the password which is encrypted in the base64 algorithm and we can decrypt it using the same algorithm.

Step 5: Decoding the base64 encrypted password

The `Authorization` field int the request body contains the password that we have entered to access the localhost.

We notice that the password is stored as `c3JlZTpwYXNzd29yZA==,` we decode using the Base64 character table to get index values which we convert into 6 digit binary values.

```
c - 28 - 011100

3 - 55 - 110111
```

```
J - 9 - 001001

l - 37 - 100101

Z - 25 - 011001

T - 19 - 010011

p - 41 - 101001

w - 48 - 110000

Y - 24 - 011000

X - 23 - 010111

N - 13 - 001101

z - 51 - 110011

d - 29 - 011101

2 - 54 - 110110

9 - 61 - 111101

y - 50 - 110010

Z - 25 - 011001

A - 0 - 000000
```

Now joining all of these binary values and splitting it into 8 digit binary numbers and converting them to characters using the ASCII table ,we get

```
01110011 - s

01110010 - r

01100101 - e

01100101 - e

00111010 - :

01110000 - p

01100001 - a

01110011 - s
```

```
01110011 - s

01110111 - w

01101111 - o

01110010 - r

01100100 - d
```

Applying the steps to decode the password, we get the password in it’s unencrypted form:

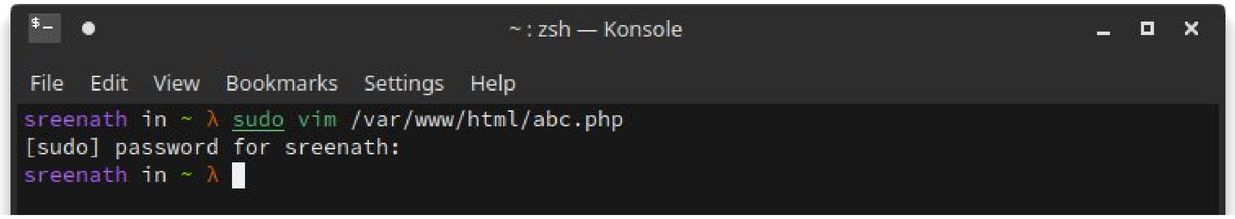
```
sree:password
```

Procedure for Cookie Setting:

Step 1: Creating a PHP File

We first create a PHP file with some image and set a cookie and store it in the `/var/www/html/` folder.

```
sudo vim /var/www/html/abc.php
```

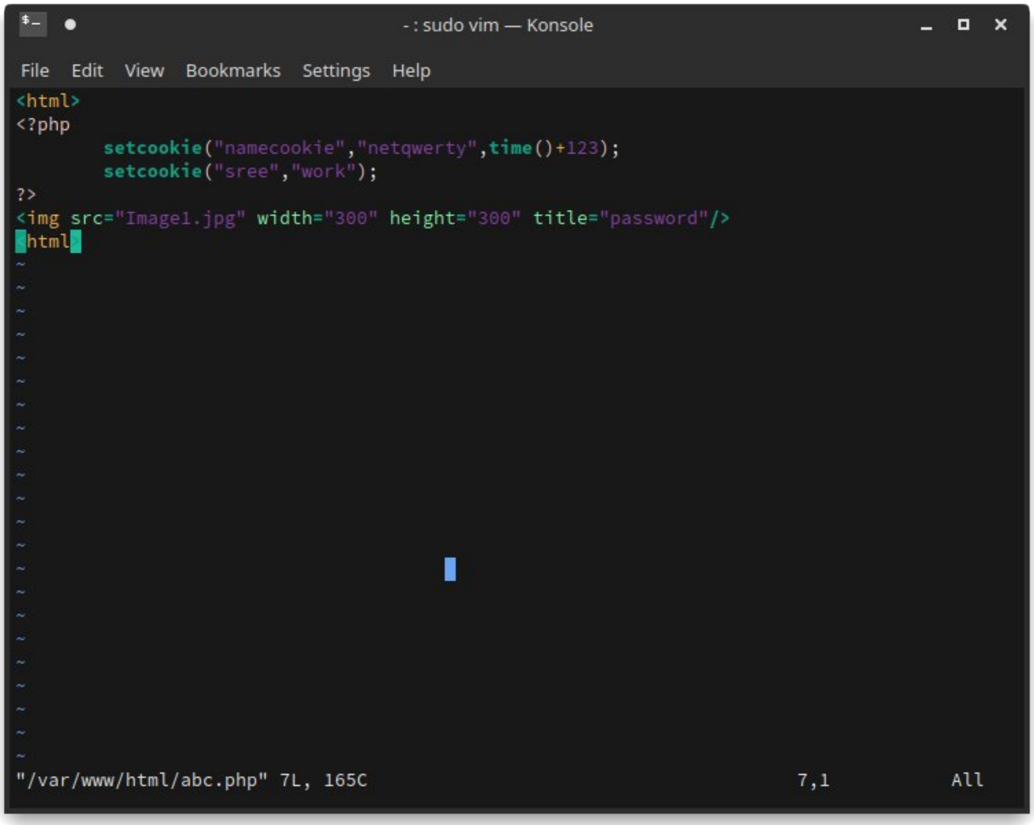


```
sreenath in ~ λ sudo vim /var/www/html/abc.php
[sudo] password for sreenath:
sreenath in ~ λ
```

Also, make sure PHP is installed on the system:

```
sudo apt-get install php
```

on Debian/Ubuntu based Linux distributions.



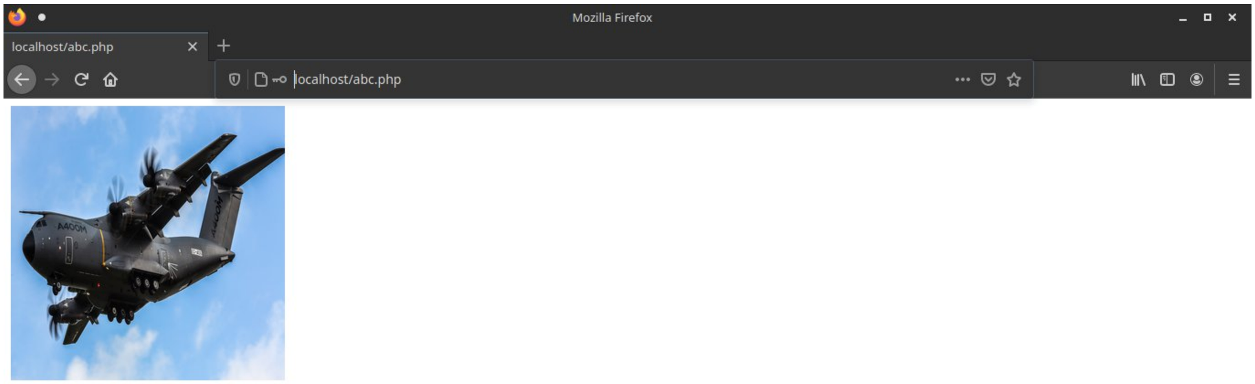
```
<html>
<?php
        setcookie("namecookie","netqwerty",time()+123);
        setcookie("sree","work");
?>
<img src="Image1.jpg" width="300" height="300" title="password"/>
<html>
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"/var/www/html/abc.php" 7L, 165C                          7,1           All
```

Step 2: Accessing the file using Firefox

Open the Firefox browser and type in the following:

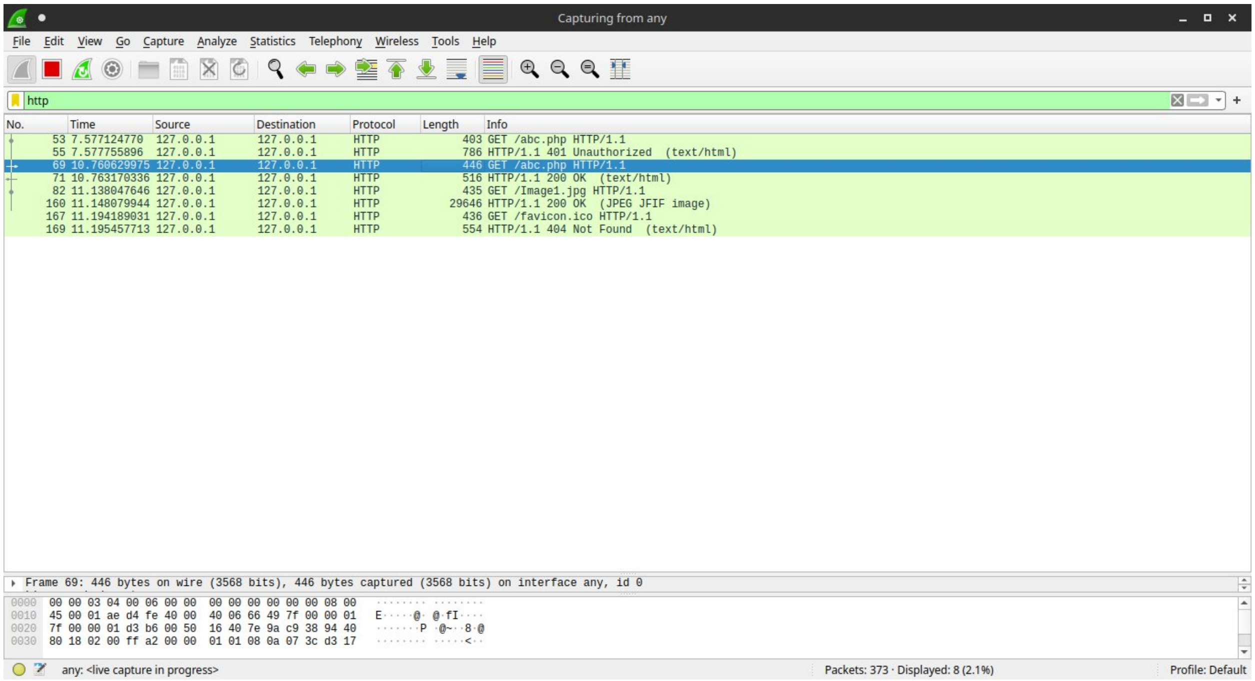
```
localhost/abc.php
```

Enter the username and password in the prompt from the authentication experiment and we notice that a webpage appears with the image that we have included.



Step 3: Wireshark Capture

We capture the HTTP GET request using Wireshark and use the ‘Follow TCP Stream’ option to check if the cookie is set or not by inspecting the `Set-Cookie` field.


Capturing from any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

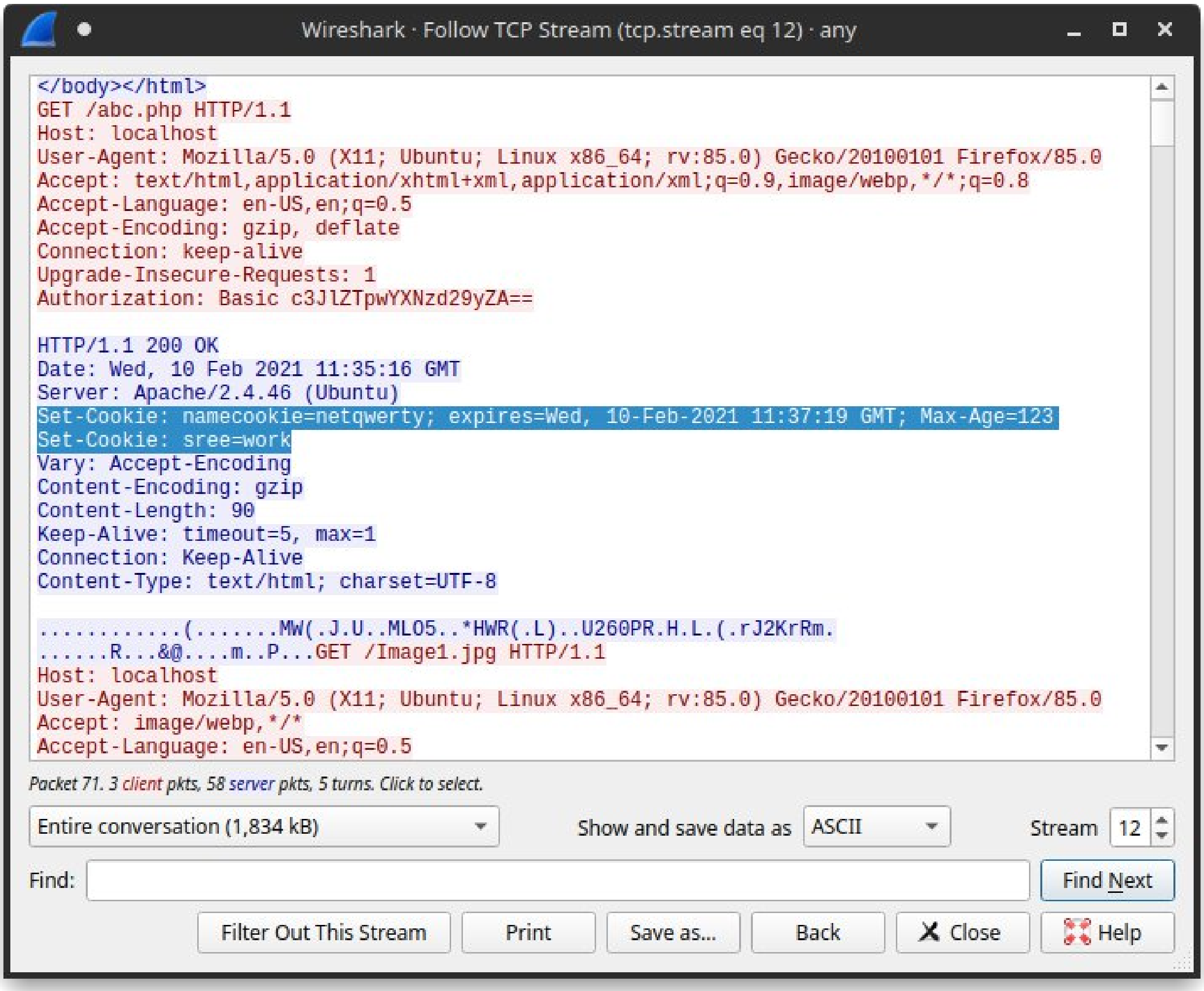
http

```
No.    Time         Source     Destination Protocol Length Info
    53 7.577124770  127.0.0.1  127.0.0.1   HTTP        403 GET /abc.php HTTP/1.1
    55 7.577755896  127.0.0.1  127.0.0.1   HTTP        786 HTTP/1.1 401 Unauthorized  (text/html)
    69 10.760629975 127.0.0.1  127.0.0.1   HTTP        446 GET /abc.php HTTP/1.1
    71 10.763170336 127.0.0.1  127.0.0.1   HTTP        516 HTTP/1.1 200 OK  (text/html)
    82 11.138047646 127.0.0.1  127.0.0.1   HTTP        435 GET /Image1.jpg HTTP/1.1
   160 11.148079944 127.0.0.1  127.0.0.1   HTTP      29646 HTTP/1.1 200 OK  (JPEG JFIF image)
   167 11.194189031 127.0.0.1  127.0.0.1   HTTP        436 GET /favicon.ico HTTP/1.1
   169 11.195457713 127.0.0.1  127.0.0.1   HTTP        554 HTTP/1.1 404 Not Found  (text/html)
```

```
▸ Frame 69: 446 bytes on wire (3568 bits), 446 bytes captured (3568 bits) on interface any, id 0
```

```
0000  00 00 03 04 00 06 00 00  00 00 00 00 00 00 08 00   ········ ········
0010  45 00 01 ae d4 fe 40 00  40 06 66 49 7f 00 00 01   E·····@· @·fI····
0020  7f 00 00 01 d3 b6 00 50  16 40 7e 9a c9 38 94 40   ·······P ·@~··8·@
0030  80 18 02 00 ff a2 00 00  01 01 08 0a 07 3c d3 17   ········ ·····<··
```

any: <live capture in progress>   Packets: 373 · Displayed: 8 (2.1%)   Profile: Default



```
</body></html>
GET /abc.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:85.0) Gecko/20100101 Firefox/85.0
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 c3JlZTpwYXNzd29yZA==

HTTP/1.1 200 OK
Date: Wed, 10 Feb 2021 11:35:16 GMT
Server: Apache/2.4.46 (Ubuntu)
Set-Cookie: namecookie=netqwerty; expires=Wed, 10-Feb-2021 11:37:19 GMT; Max-Age=123
Set-Cookie: sree=work
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 90
Keep-Alive: timeout=5, max=1
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

............(.......MW(.J.U..MLO5..*HWR(.L)..U260PR.H.L.(.rJ2KrRm.
......R...&@....m..P...GET /Image1.jpg HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:85.0) Gecko/20100101 Firefox/85.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
```

Packet 71. 3 client pkts, 58 server pkts, 5 turns. Click to select.

Entire conversation (1,834 kB) Show and save data as: ASCII Stream: 12

We notice that there are 2 `Set-Cookie` fields in our response body and one cookie includes the time limit that we had set.

```
Set-Cookie: namecookie=netqwerty; expires=Wed, 10-Feb-2021
11:37:19 GMT: Max-Age=123

Set-Cookie: sree=work
```

Procedure for Conditional Get: If-Modified-Since

Step 1: Accessing a site

Make sure the browser’s cache is empty. Now do the following:

1) Start the web browser (Firefox) and make sure Wireshark is sniffing packets too.

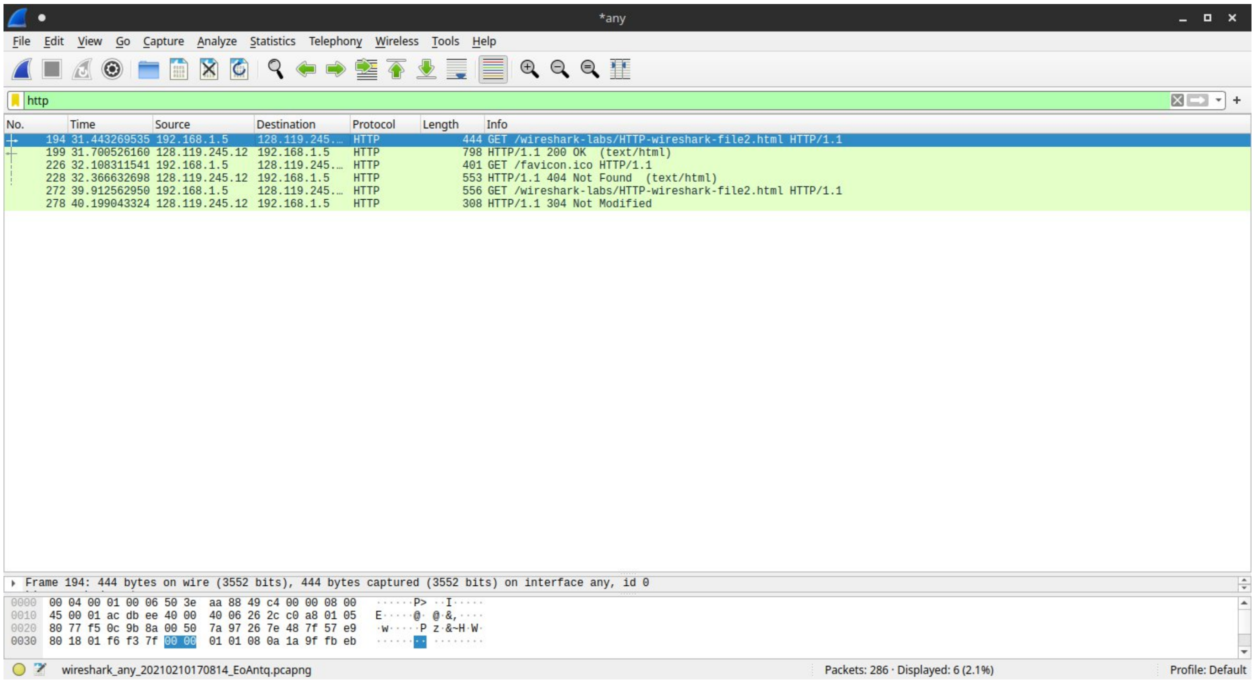
2) Enter the following URL into the web browser:

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

3) The browser should display a 5 line HTML file.

4) Refresh the page using F5.

5) Now stop the Wireshark capture and filter the packets for http requests.



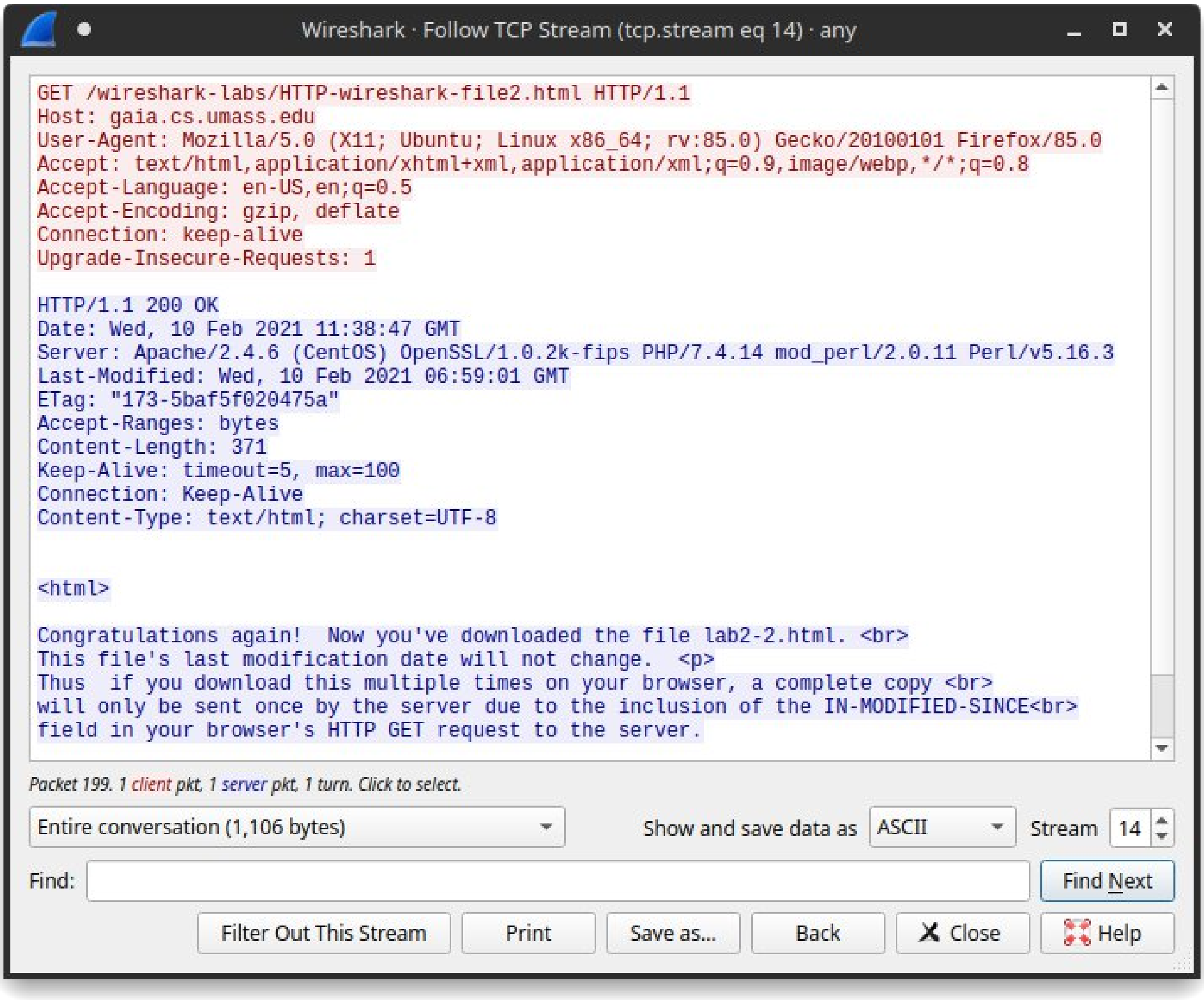
http

```
No.   Time         Source          Destination     Protocol  Length Info
  194 31.443269535 192.168.1.5     128.119.245.…   HTTP         444 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  199 31.700526160 128.119.245.12  192.168.1.5     HTTP         798 HTTP/1.1 200 OK  (text/html)
  226 32.108311541 192.168.1.5     128.119.245.…   HTTP         401 GET /favicon.ico HTTP/1.1
  228 32.366632698 128.119.245.12  192.168.1.5     HTTP         553 HTTP/1.1 404 Not Found  (text/html)
  272 39.912562950 192.168.1.5     128.119.245.…   HTTP         556 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  278 40.199043324 128.119.245.12  192.168.1.5     HTTP         308 HTTP/1.1 304 Not Modified
```

```
Frame 194: 444 bytes on wire (3552 bits), 444 bytes captured (3552 bits) on interface any, id 0
```

```
0000  00 04 00 01 00 06 50 3e  aa 88 49 c4 00 00 08 00   ······P> ··I·····
0010  45 00 01 ac db ee 40 00  40 06 26 2c c0 a8 01 05   E·····@· @·&,····
0020  80 77 f5 0c 9b 8a 00 50  7a 97 26 7e 48 7f 57 e9   ·w·····P z·&~H·W·
0030  80 18 01 f6 f3 7f 00 00  01 01 08 0a 1a 9f fb eb   ········ ········
```

wireshark_any_20210210170814_EoAntq.pcapng   Packets: 286 · Displayed: 6 (2.1%)   Profile: Default

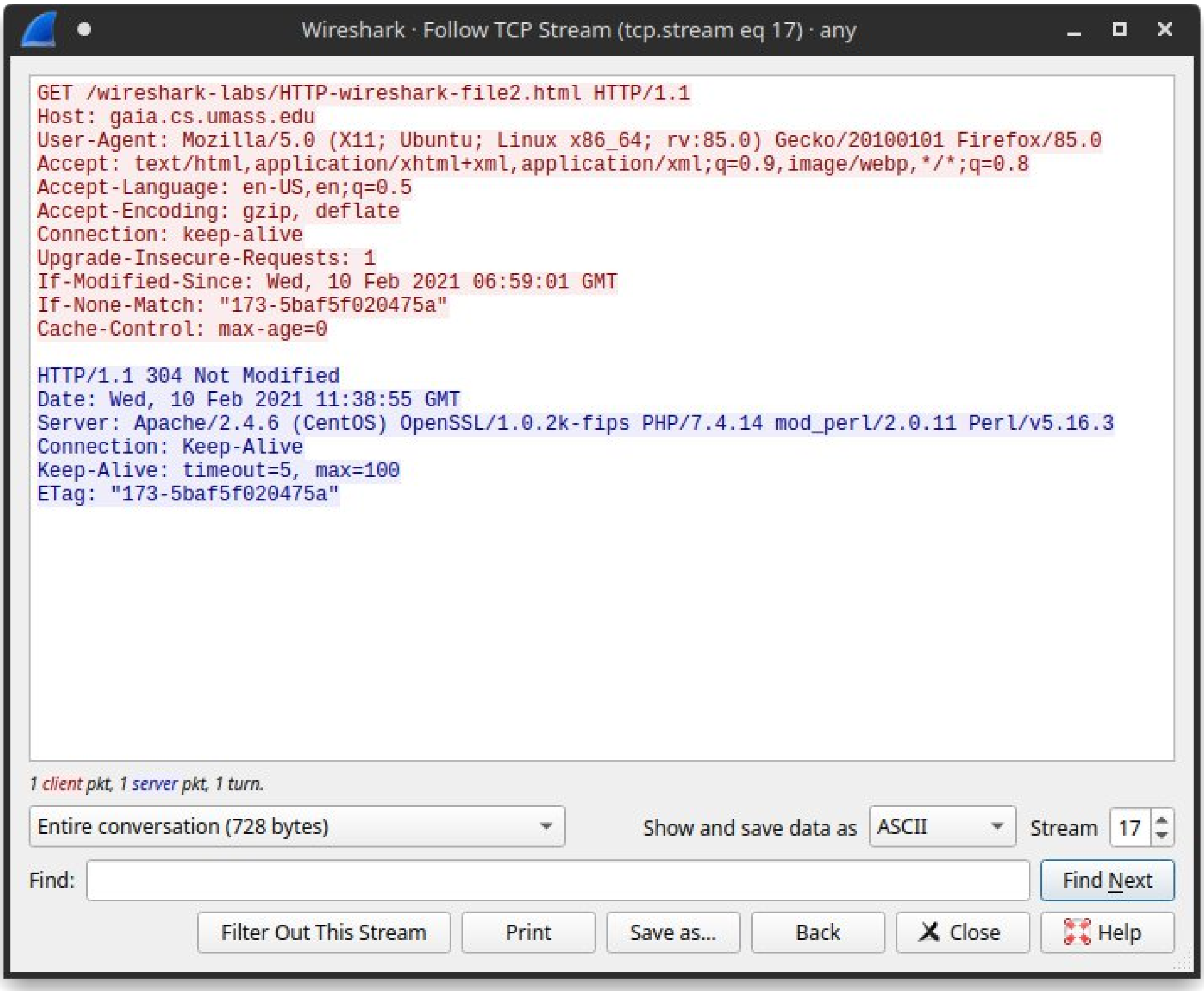


```
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Host: gaia.cs.umass.edu
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:85.0) Gecko/20100101 Firefox/85.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Wed, 10 Feb 2021 11:38:47 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: Wed, 10 Feb 2021 06:59:01 GMT
ETag: "173-5baf5f020475a"
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.
```

Packet 199. 1 client pkt, 1 server pkt, 1 turn. Click to select.

Entire conversation (1,106 bytes) · Show and save data as: ASCII · Stream: 14

On inspecting the 1st GET request, we do not see an ‘IF-MODIFIED-SINCE’ line in the HTTP GET request. The server also explicitly returns the contents of the file accessed. We can see that since the OK response also includes the full html file.


Wireshark · Follow TCP Stream (tcp.stream eq 17) · any
1 client pkt, 1 server pkt, 1 turn.
Entire conversation (728 bytes)
Show and save data as
ASCII
Stream
17
Find:
Find Next
Filter Out This Stream
Print
Save as…
Back
Close
Help

```
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:85.0) Gecko/20100101 Firefox/85.0
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: Wed, 10 Feb 2021 06:59:01 GMT
If-None-Match: "173-5baf5f020475a"
Cache-Control: max-age=0

HTTP/1.1 304 Not Modified
Date: Wed, 10 Feb 2021 11:38:55 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: "173-5baf5f020475a"
```

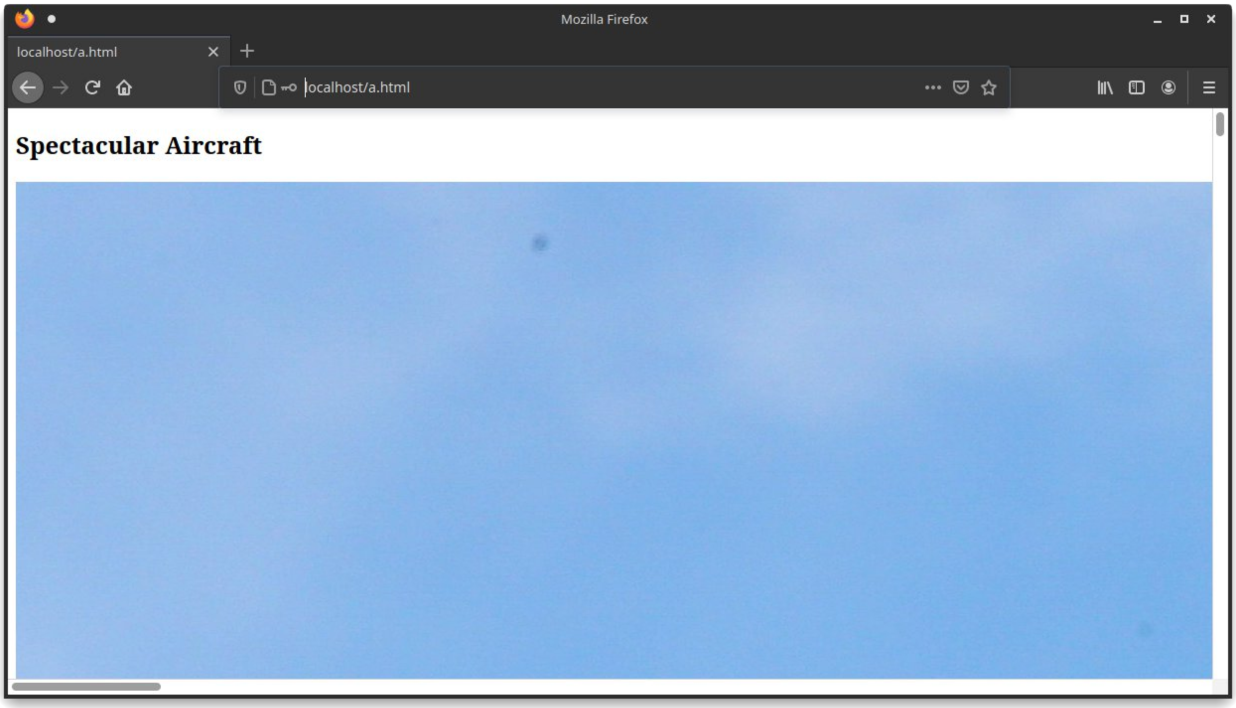
On inspecting the contents of the 2nd GET request, we see that there now is an IF-MODIFIED-SINCE line:

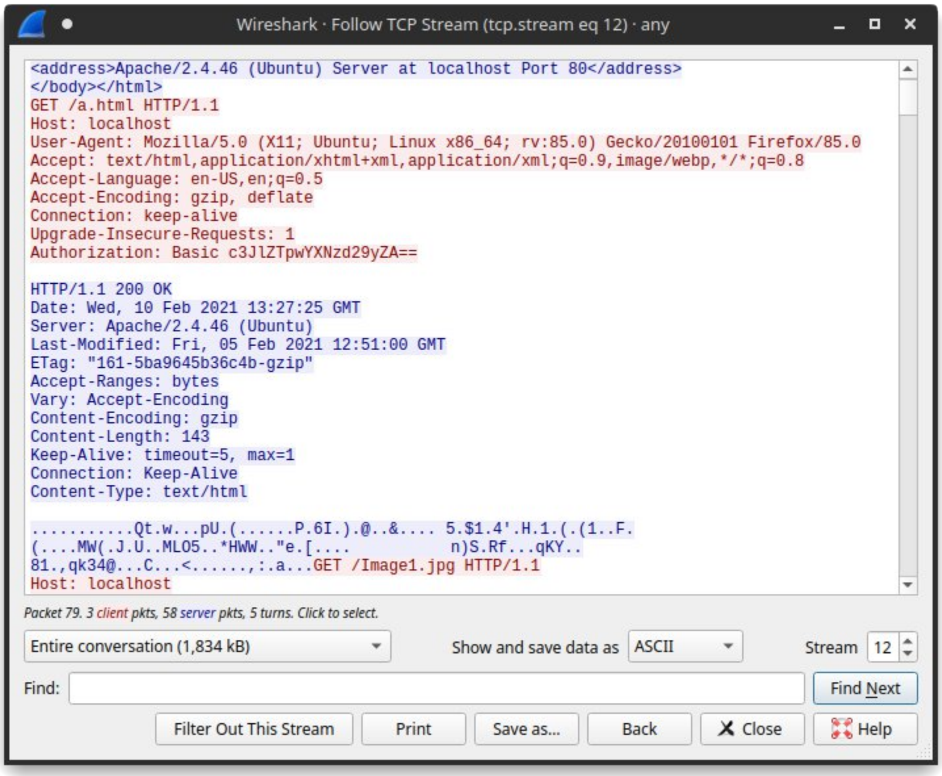
```
If-Modified-Since: Wed, 10 Feb 2021 06:59:01 GMT
```

In the 2nd response, the HTTP status response has a code of **304** since it implies that nothing has changed since the previous GET request. This also means that the entire file isn’t loaded again and hence the response body doesn’t contain the contents of the file.

Step 2: Using a local site to test

We access a sample HTML file created with some images using a web browser and use Wireshark to inspect the packets.





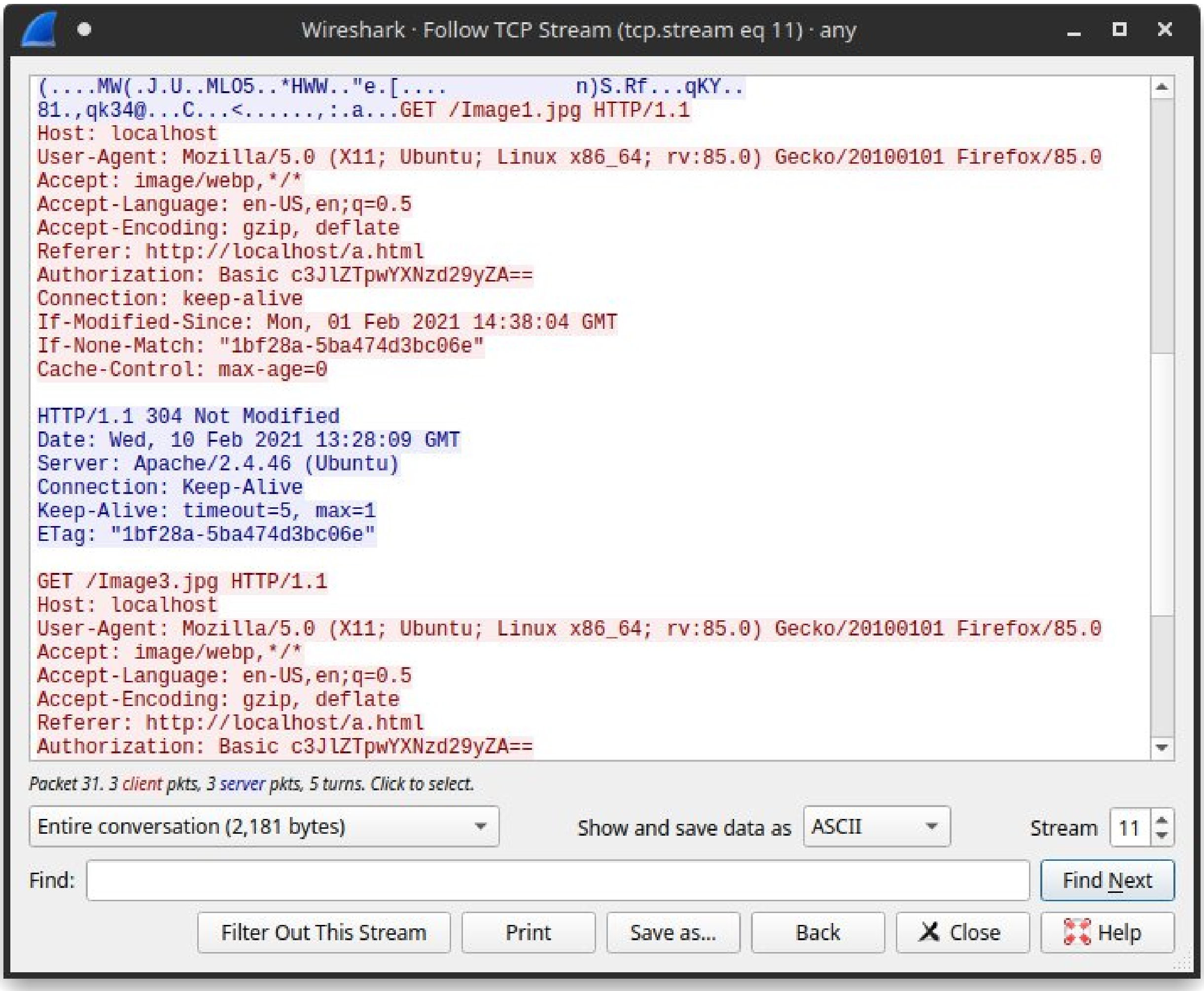
```
<address>Apache/2.4.46 (Ubuntu) Server at localhost Port 80</address>
</body></html>
GET /a.html HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:85.0) Gecko/20100101 Firefox/85.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Authorization: Basic c3JlZTpwYXNzd29yZA==

HTTP/1.1 200 OK
Date: Wed, 10 Feb 2021 13:27:25 GMT
Server: Apache/2.4.46 (Ubuntu)
Last-Modified: Fri, 05 Feb 2021 12:51:00 GMT
ETag: "161-5ba9645b36c4b-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 143
Keep-Alive: timeout=5, max=1
Connection: Keep-Alive
Content-Type: text/html

...........Qt.w...pU.(......P.6I.).@..&.... 5.$1.4'.H.1.(.(1..F.
(....MW(.J.U..MLO5..*HWW.."e.[....            n)S.Rf...qKY..
81.,qk34@...C...<......,:.a...GET /Image1.jpg HTTP/1.1
Host: localhost
```

Packet 79. 3 client pkts, 58 server pkts, 5 turns. Click to select.

Entire conversation (1,834 kB)   Show and save data as ASCII   Stream 12

Find:

1st GET Request



```
(....MW(.J.U..MLO5..*HWW.."e.[....          n)S.Rf...qKY..
81.,qk34@...C...<......,:.a...GET /Image1.jpg HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:85.0) Gecko/20100101 Firefox/85.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://localhost/a.html
Authorization: Basic c3JlZTpwYXNzd29yZA==
Connection: keep-alive
If-Modified-Since: Mon, 01 Feb 2021 14:38:04 GMT
If-None-Match: "1bf28a-5ba474d3bc06e"
Cache-Control: max-age=0

HTTP/1.1 304 Not Modified
Date: Wed, 10 Feb 2021 13:28:09 GMT
Server: Apache/2.4.46 (Ubuntu)
Connection: Keep-Alive
Keep-Alive: timeout=5, max=1
ETag: "1bf28a-5ba474d3bc06e"

GET /Image3.jpg HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:85.0) Gecko/20100101 Firefox/85.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://localhost/a.html
Authorization: Basic c3JlZTpwYXNzd29yZA==
```

Packet 31. 3 client pkts, 3 server pkts, 5 turns. Click to select.

Entire conversation (2,181 bytes)

Show and save data as: ASCII

Stream: 11

Find:

2nd GET Request that shows the 304 code.