# CN Lab Report – Week 3

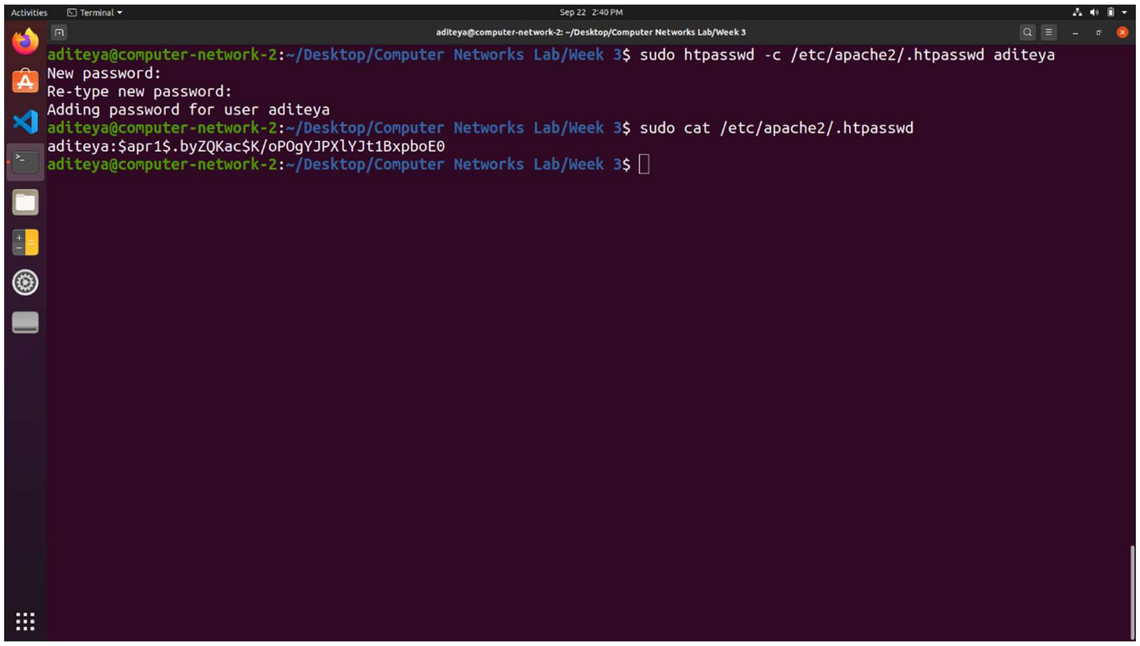
PES1UG21CS361

Nandan N

## 1. Password Authentication

### 1.1 Password Generation

- To enable basic authentication for HTTP, we need to generate a password file. This file can be generated using the **`htpasswd`** command.
- Using **`sudo htpasswd -c /etc/apache2/.htpasswd`** `username` we can set a password for the given user username and write it into the **`.htpasswd`** configuration file.
- The cat command can be used to view the encrypted password file, which is encrypted using the Data Encryption Standard algorithm.

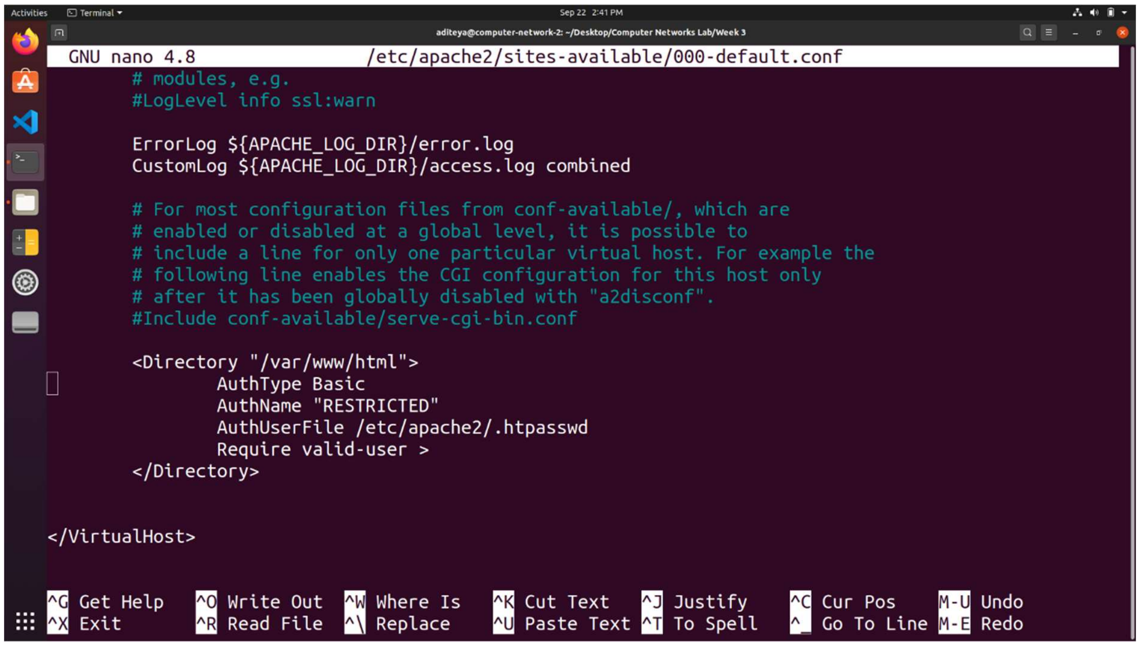


```
aditeya@computer-network-2:~/Desktop/Computer Networks Lab/Week 3$ sudo htpasswd -c /etc/apache2/.htpasswd aditeya
New password:
Re-type new password:
Adding password for user aditeya
aditeya@computer-network-2:~/Desktop/Computer Networks Lab/Week 3$ sudo cat /etc/apache2/.htpasswd
aditeya:$apr1$.byZQKac$K/oPOgYJPXlYJt1BxpboE0
aditeya@computer-network-2:~/Desktop/Computer Networks Lab/Week 3$ 
```

### 1.2 Apache Server Authentication

- To enable password authentication in the server, we need to modify the Apache configuration file.
- This can be done using **`sudo nano /etc/apache2/sites-available/000-default.conf`**

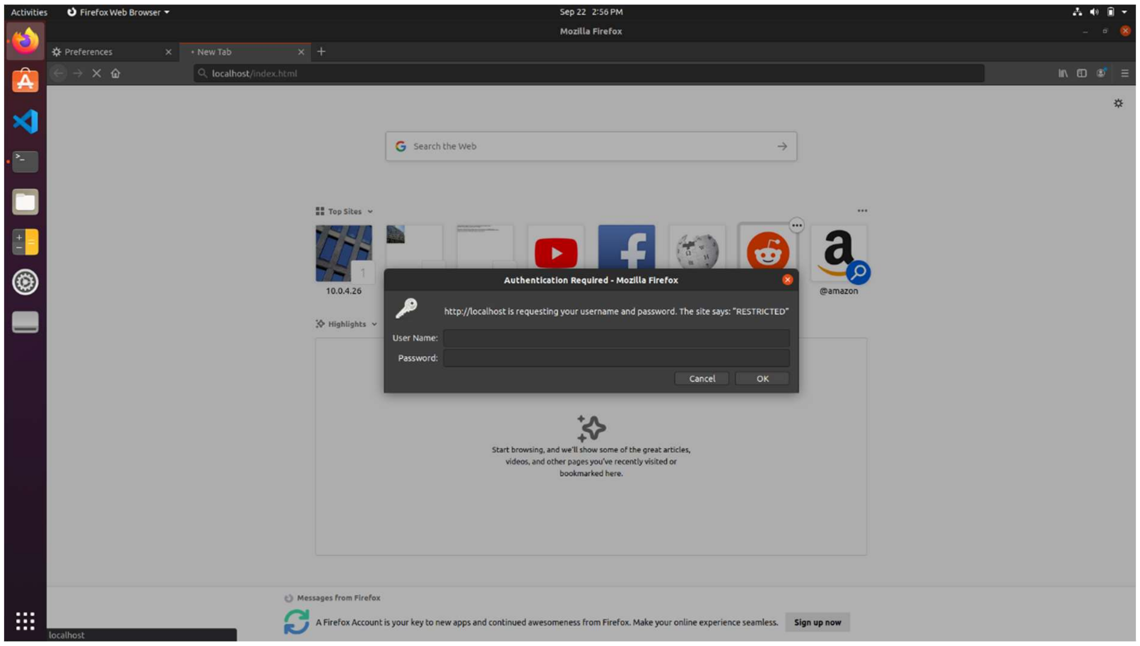
- Password authentication is added to the **`/var/www/html`** directory which is the localhost home directory so that all files hosted here will require authentication to access.
- To activate the authentication and policy, we need to restart the server using **`sudo service apache2 restart`**.


Activities
Terminal
Sep 22 2:41 PM
aditeya@computer-network-2: ~/Desktop/Computer Networks Lab/Week 3

```
  GNU nano 4.8                 /etc/apache2/sites-available/000-default.conf
        # 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>

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo
^X Exit       ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line M-E Redo
```

## 1.3 Accessing Localhost

- We can now access localhost only after entering the username and password set earlier
- These credentials are entered on the browser window.



Authentication Required - Mozilla Firefox

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

User Name:
Password:

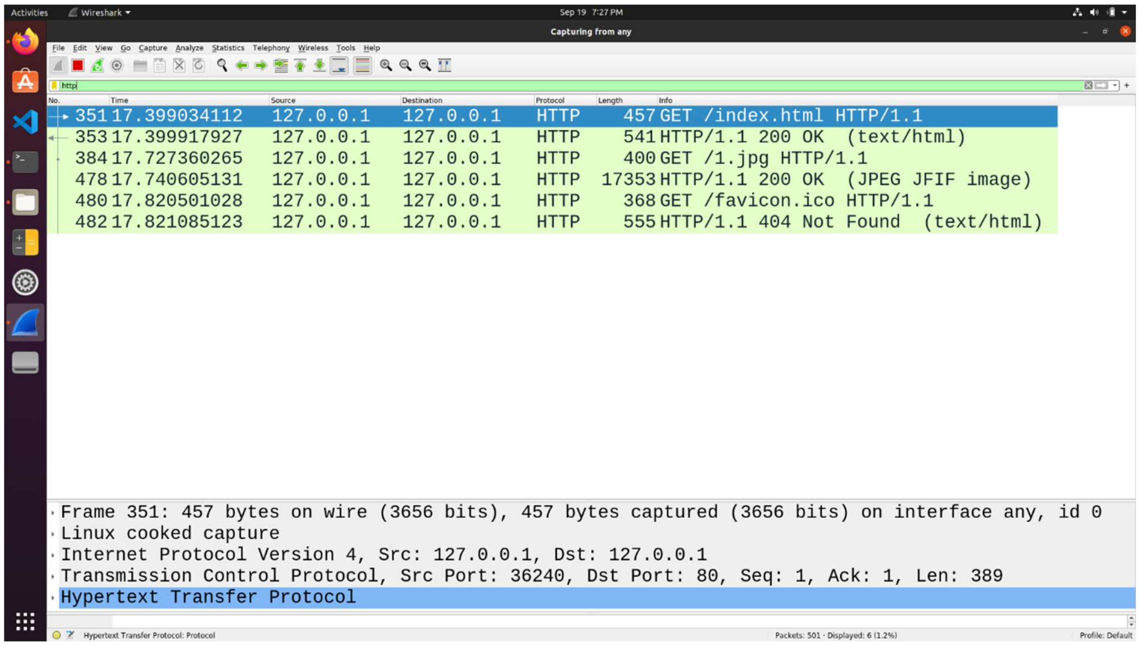
Cancel OK

Start browsing, and we'll show some of the great articles, videos, and other pages you've recently visited or bookmarked here.

A Firefox Account is your key to new apps and continued awesomeness from Firefox. Make your online experience seamless.

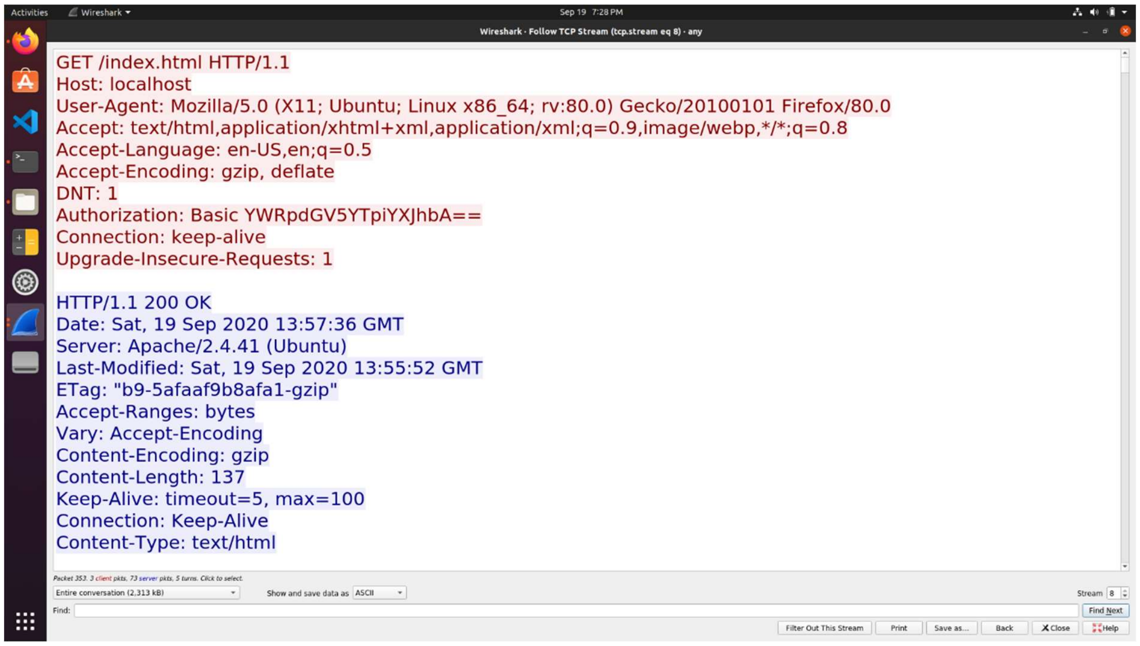
## 1.4 Wireshark Packet Capture

Wireshark can be used to capture the packets sent on the network. The first GET request corresponding to the HTML file is analysed and its TCP Stream is expanded, and parameters examined.



```
No.  Time          Source     Destination Protocol Length Info
351 17.399034112  127.0.0.1  127.0.0.1   HTTP     457 GET /index.html HTTP/1.1
353 17.399917927  127.0.0.1  127.0.0.1   HTTP     541 HTTP/1.1 200 OK  (text/html)
384 17.727360265  127.0.0.1  127.0.0.1   HTTP     400 GET /1.jpg HTTP/1.1
478 17.740605131  127.0.0.1  127.0.0.1   HTTP   17353 HTTP/1.1 200 OK  (JPEG JFIF image)
480 17.820501028  127.0.0.1  127.0.0.1   HTTP     368 GET /favicon.ico HTTP/1.1
482 17.821085123  127.0.0.1  127.0.0.1   HTTP     555 HTTP/1.1 404 Not Found  (text/html)

Frame 351: 457 bytes on wire (3656 bits), 457 bytes captured (3656 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: 36240, Dst Port: 80, Seq: 1, Ack: 1, Len: 389
Hypertext Transfer Protocol
```

Activities
Wireshark
Sep 19 7:27 PM
Capturing from any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Hypertext Transfer Protocol: Protocol
Packets: 501 · Displayed: 6 (1.2%)
Profile: Default

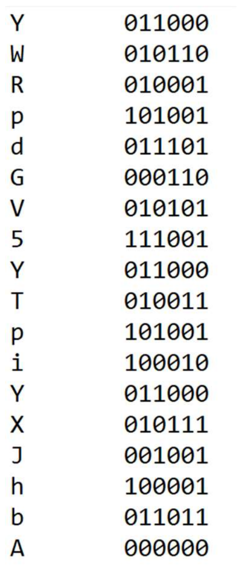


```
GET /index.html HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Authorization: Basic YWRpdGV5YTpiYXJhbA==
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Sat, 19 Sep 2020 13:57:36 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Sat, 19 Sep 2020 13:55:52 GMT
ETag: "b9-5afaaf9b8afa1-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 137
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
```

Activities
Wireshark
Sep 19 7:28 PM
Wireshark · Follow TCP Stream (tcp.stream eq 8) · any
Packet 353. 3 client pkts, 73 server pkts, 5 turns. Click to select.
Entire conversation (2,313 kB)
Show and save data as ASCII
Stream 8
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

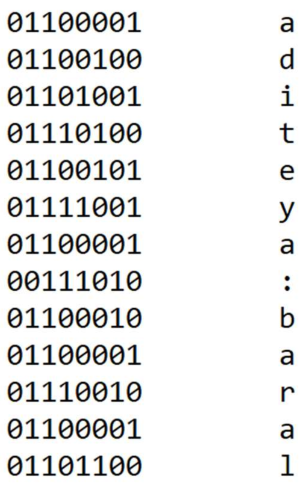
## 1.5 Decrypting Base64 Encryption

- We can observe that the **`Authorization`** field stores the password we had entered to access localhost.
- This password is encrypted using the Base64 algorithm before it is transmitted along the network.
  - Each character is converted into 8-bit binary ASCII representation
  - Group these bits into chunks of 6-bits.
  - Convert these chunks into their decimal equivalent and assign the corresponding Base64 character
  - The Base64 algorithm supports the use of lowercase as well as uppercase alphabets, all digits from 0 to 9 and the special characters + and / only.
- Similarly, Base64 is decoded by obtaining the 6-bit binary chunks for each character, grouping them into chunks of 8-bits and then converting into their corresponding character
  - **`YWRpdGV5YTpiYXJhbA==`** can be first converted to a 6-bit binary equivalent



| | |
|---|---|
| Y | 011000 |
| W | 010110 |
| R | 010001 |
| p | 101001 |
| d | 011101 |
| G | 000110 |
| V | 010101 |
| 5 | 111001 |
| Y | 011000 |
| T | 010011 |
| p | 101001 |
| i | 100010 |
| Y | 011000 |
| X | 010111 |
| J | 001001 |
| h | 100001 |
| b | 011011 |
| A | 000000 |

  - These binary equivalents can then be grouped together and then decoded to ASCII



```
01100001        a
01100100        d
01101001        i
01110100        t
01100101        e
01111001        y
01100001        a
00111010        :
01100010        b
01100001        a
01110010        r
01100001        a
01101100        l
```

## 2. Setting Cookies

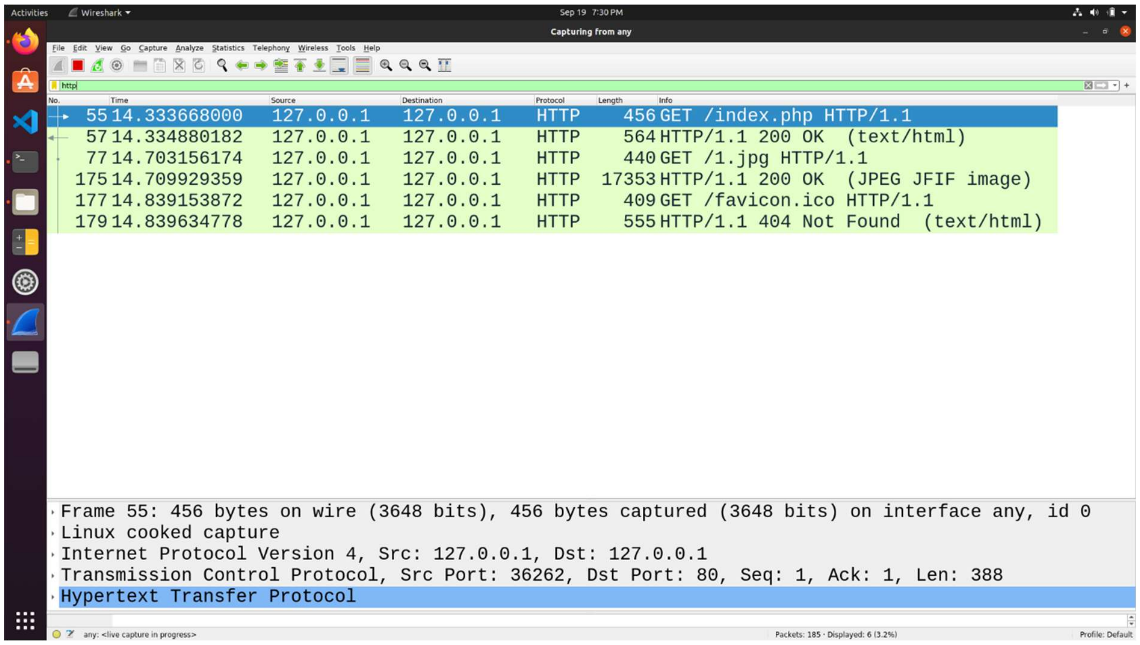
### 2.1 Setting Cookies with PHP

- We can set cookies using a PHP script and the **`setcookie(name, value, expire_time)`** function
- When this file is requested by the browser a cookie will be set

```
<html>
    <?php
       setcookie("SRN", "PES1201800366");
       setcookie("NAME", "Aditeya", time()+123);
    ?>
    <head>
        <title>Computer Networks Lab Week 3</title>
        <body>
            <img src="1.jpg" height="300" width="300"/>
        </body>
    </head>
</html>
```

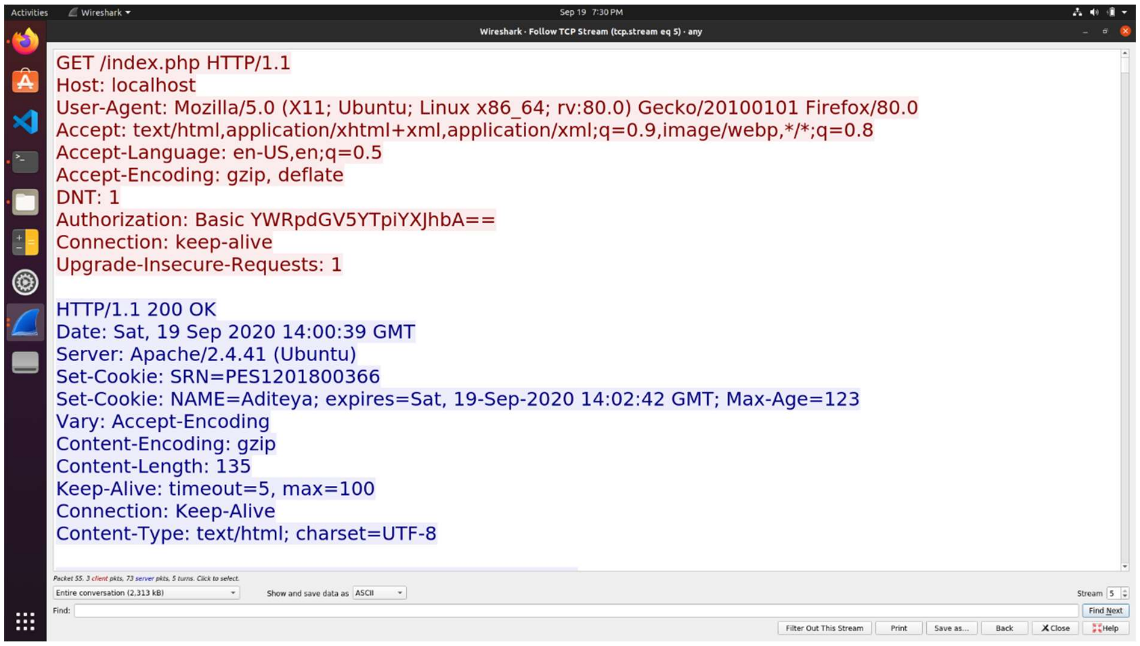
### 2.2 Wireshark Capture

- Wireshark can be used to capture the packets sent on the network. The first GET request corresponding to the PHP file is analysed and its TCP Stream is expanded and examined.
- 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.



```
No.  Time            Source     Destination  Protocol  Length  Info
 55  14.333668000    127.0.0.1  127.0.0.1    HTTP        456   GET /index.php HTTP/1.1
 57  14.334880182    127.0.0.1  127.0.0.1    HTTP        564   HTTP/1.1 200 OK  (text/html)
 77  14.703156174    127.0.0.1  127.0.0.1    HTTP        440   GET /1.jpg HTTP/1.1
175  14.709929359    127.0.0.1  127.0.0.1    HTTP      17353   HTTP/1.1 200 OK  (JPEG JFIF image)
177  14.839153872    127.0.0.1  127.0.0.1    HTTP        409   GET /favicon.ico HTTP/1.1
179  14.839634778    127.0.0.1  127.0.0.1    HTTP        555   HTTP/1.1 404 Not Found  (text/html)

Frame 55: 456 bytes on wire (3648 bits), 456 bytes captured (3648 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: 36262, Dst Port: 80, Seq: 1, Ack: 1, Len: 388
Hypertext Transfer Protocol
```

Activities
Wireshark
Sep 19 7:30 PM
Capturing from any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
any: <live capture in progress>
Packets: 185 · Displayed: 6 (3.2%)
Profile: Default



```
GET /index.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
DNT: 1
Authorization: Basic YWRpdGV5YTpiYXJhbA==
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Sat, 19 Sep 2020 14:00:39 GMT
Server: Apache/2.4.41 (Ubuntu)
Set-Cookie: SRN=PES1201800366
Set-Cookie: NAME=Aditeya; expires=Sat, 19-Sep-2020 14:02:42 GMT; Max-Age=123
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 135
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

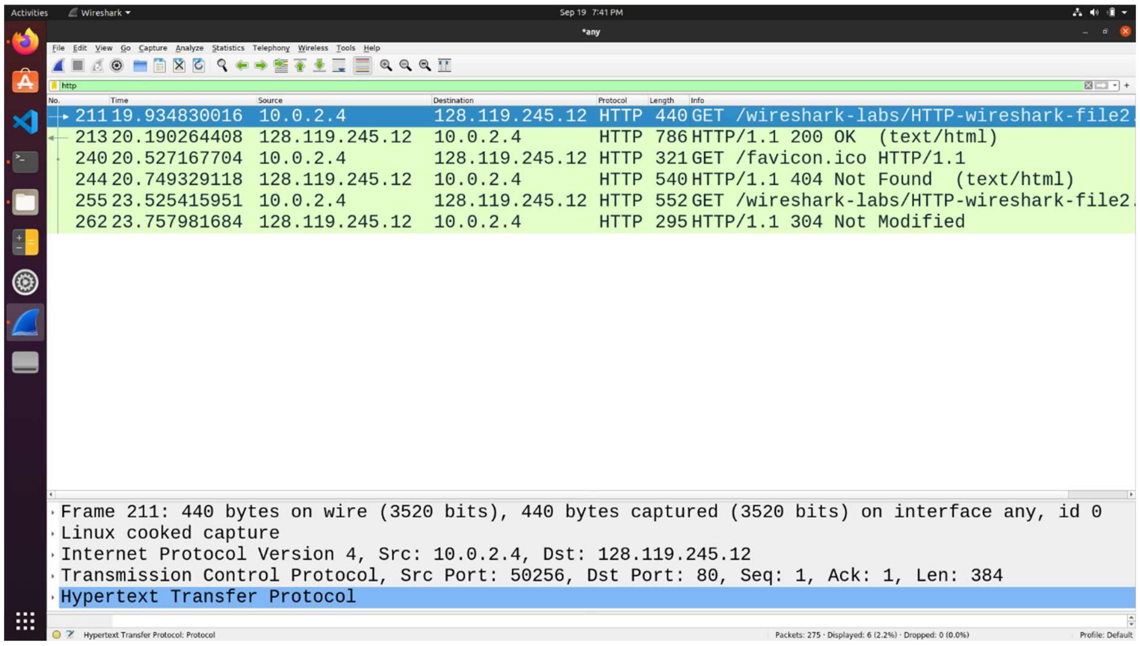
Activities
Wireshark
Sep 19 7:30 PM
Wireshark · Follow TCP Stream (tcp.stream eq 5) · any
Packet 55. 3 client pkts, 73 server pkts, 5 turns. Click to select.
Entire conversation (2,313 kB)
Show and save data as ASCII
Stream 5
Find:
Find Next
Filter Out This Stream
Print
Save as…
Back
Close
Help

## 3. Conditional GET

- A conditional HTTP response is one that carries the resource only it had been modified since the last GET request by the client.
- The HTTP header **`If-Modified-Since`** is one way to implement Conditional GET
- The server checks the **`If-Modified-Since`** header value and resends the resource only if it has been modified since the timestamp in the header
- If it has not been modified, a **`304 Not Modified`** status code is sent back.

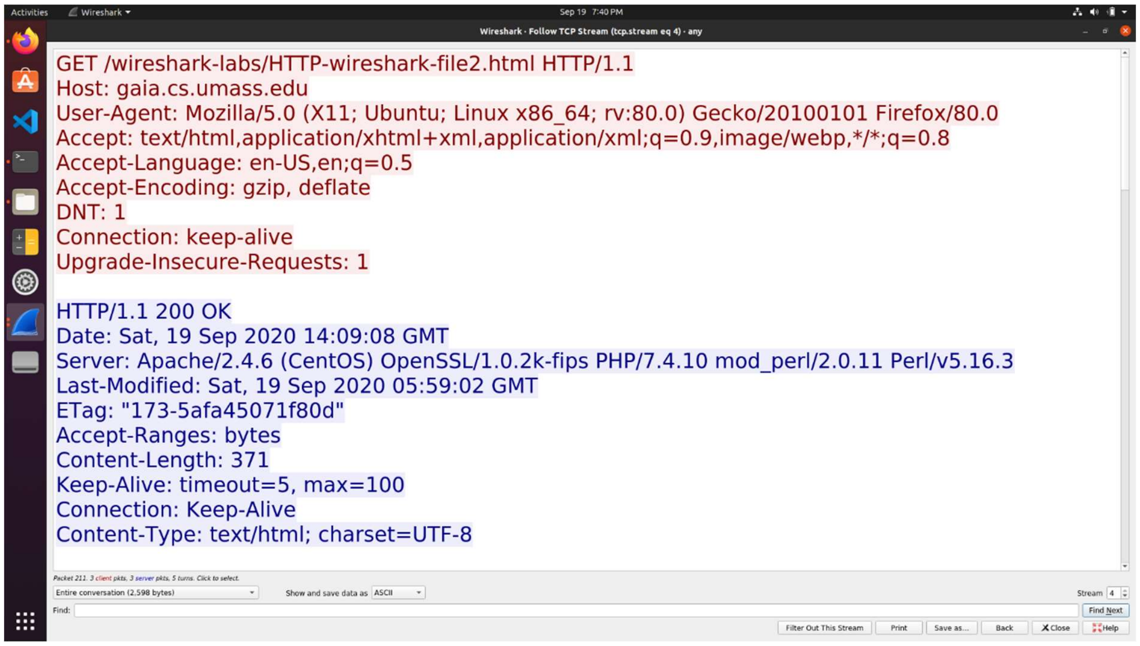
## 3.1 Repeat Requests for HTML Page

- An HTML page is requested by the client and the HTML file is obtained along with a **`200 OK`** response status
- Immediately, the request is made again either by refreshing or accessing it via a browser tab
- The second response from the server is obtained as **`304 Not Modified`** since the resource has not been modified since the last GET.



```
No.  Time           Source          Destination     Protocol Length Info
211  19.934830016   10.0.2.4        128.119.245.12  HTTP     440    GET /wireshark-labs/HTTP-wireshark-file2
213  20.190264408   128.119.245.12  10.0.2.4        HTTP     786    HTTP/1.1 200 OK  (text/html)
240  20.527167704   10.0.2.4        128.119.245.12  HTTP     321    GET /favicon.ico HTTP/1.1
244  20.749329118   128.119.245.12  10.0.2.4        HTTP     540    HTTP/1.1 404 Not Found  (text/html)
255  23.525415951   10.0.2.4        128.119.245.12  HTTP     552    GET /wireshark-labs/HTTP-wireshark-file2
262  23.757981684   128.119.245.12  10.0.2.4        HTTP     295    HTTP/1.1 304 Not Modified

Frame 211: 440 bytes on wire (3520 bits), 440 bytes captured (3520 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50256, Dst Port: 80, Seq: 1, Ack: 1, Len: 384
Hypertext Transfer Protocol
```

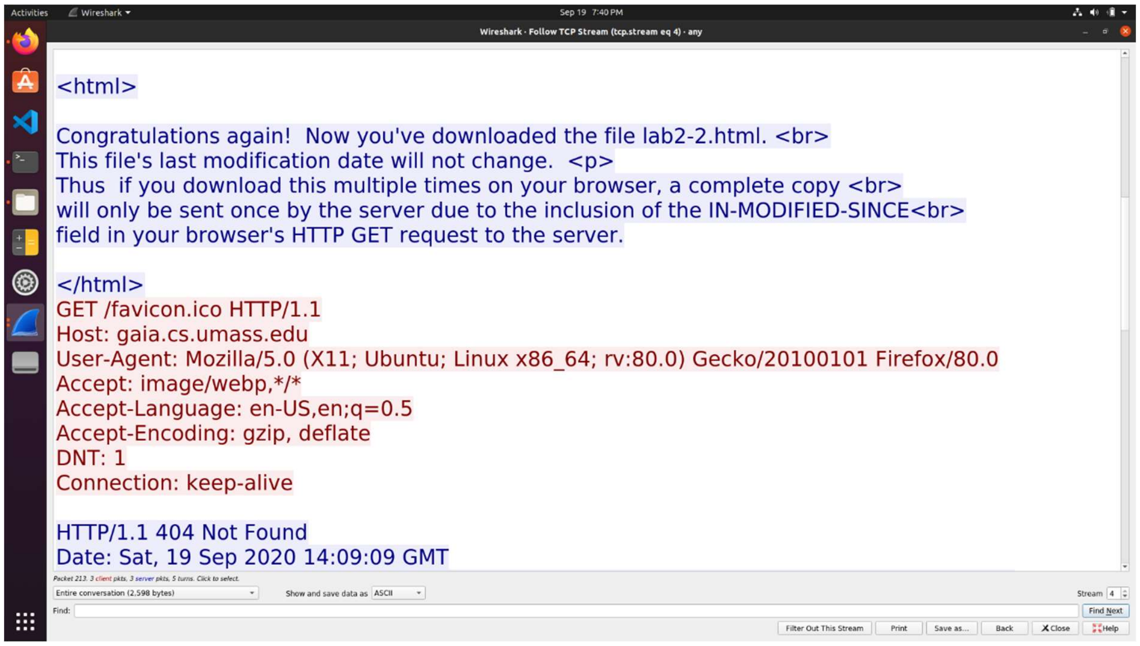
Activities
Wireshark
Sep 19 7:41 PM
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Hypertext Transfer Protocol: Protocol
Packets: 275 · Displayed: 6 (2.2%) · Dropped: 0 (0.0%)
Profile: Default



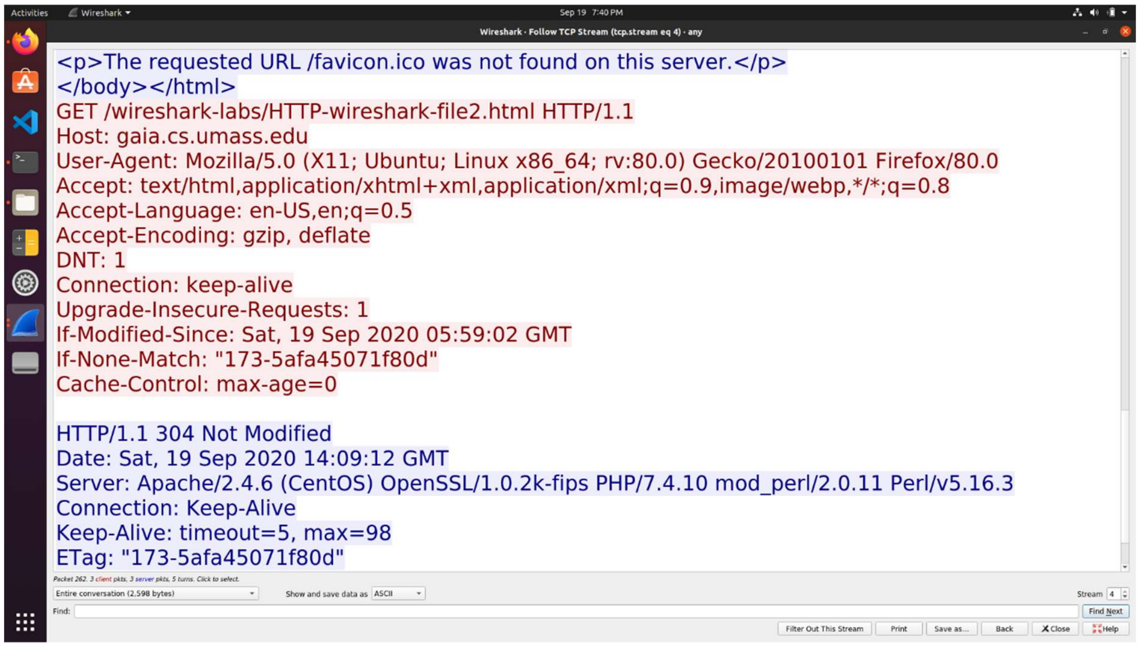
```
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Host: gaia.cs.umass.edu
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Sat, 19 Sep 2020 14:09:08 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.10 mod_perl/2.0.11 Perl/v5.16.3
Last-Modified: Sat, 19 Sep 2020 05:59:02 GMT
ETag: "173-5afa45071f80d"
Accept-Ranges: bytes
Content-Length: 371
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

Activities
Wireshark
Sep 19 7:40 PM
Wireshark · Follow TCP Stream (tcp.stream eq 4) · any
Packet 211. 3 client pkts, 3 server pkts, 5 turns. Click to select.
Entire conversation (2,598 bytes)
Show and save data as ASCII
Stream 4
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

First Request from Server – **`200 OK`**


Wireshark · Follow TCP Stream (tcp.stream eq 4) · any
Entire conversation (2,598 bytes)
Show and save data as ASCII
Stream 4
Find:
Find Next
Filter Out This Stream
Print
Save as…
Back
Close
Help

```
<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>
GET /favicon.ico HTTP/1.1
Host: gaia.cs.umass.edu
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
DNT: 1
Connection: keep-alive

HTTP/1.1 404 Not Found
Date: Sat, 19 Sep 2020 14:09:09 GMT
```


Wireshark · Follow TCP Stream (tcp.stream eq 4) · any
Entire conversation (2,598 bytes)
Show and save data as ASCII
Stream 4
Find:
Find Next
Filter Out This Stream
Print
Save as…
Back
Close
Help

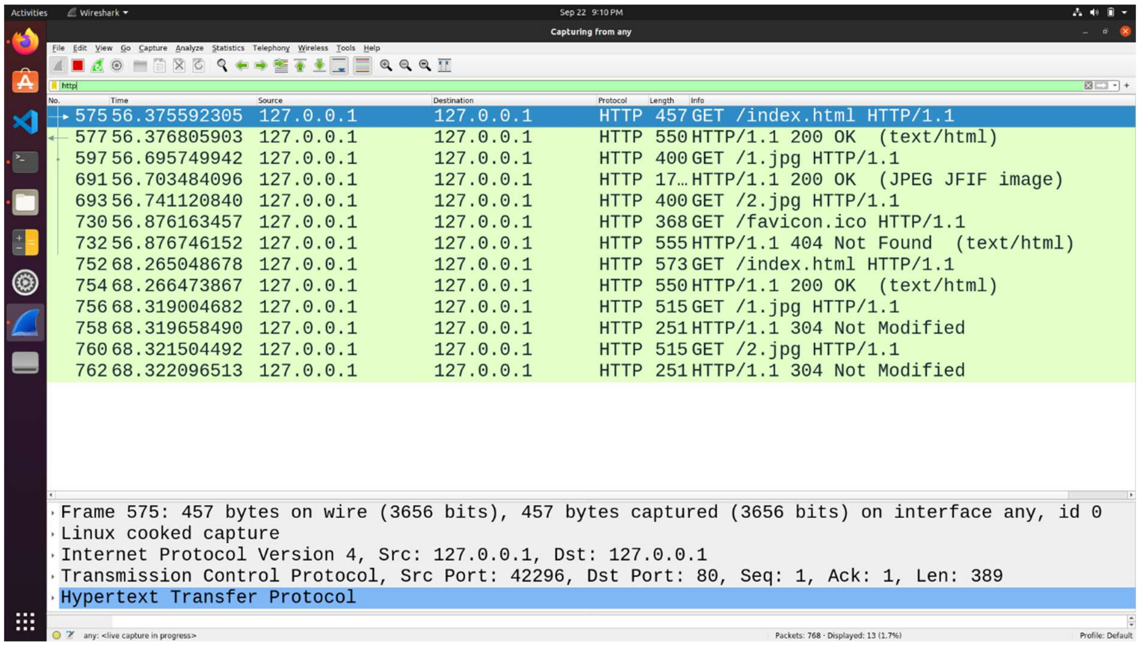
```
<p>The requested URL /favicon.ico was not found on this server.</p>
</body></html>
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Host: gaia.cs.umass.edu
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
If-Modified-Since: Sat, 19 Sep 2020 05:59:02 GMT
If-None-Match: "173-5afa45071f80d"
Cache-Control: max-age=0

HTTP/1.1 304 Not Modified
Date: Sat, 19 Sep 2020 14:09:12 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.10 mod_perl/2.0.11 Perl/v5.16.3
Connection: Keep-Alive
Keep-Alive: timeout=5, max=98
ETag: "173-5afa45071f80d"
```

Second Request from Server – **`304 Not Modified`**

## 3.2 Conditional GET on Localhost

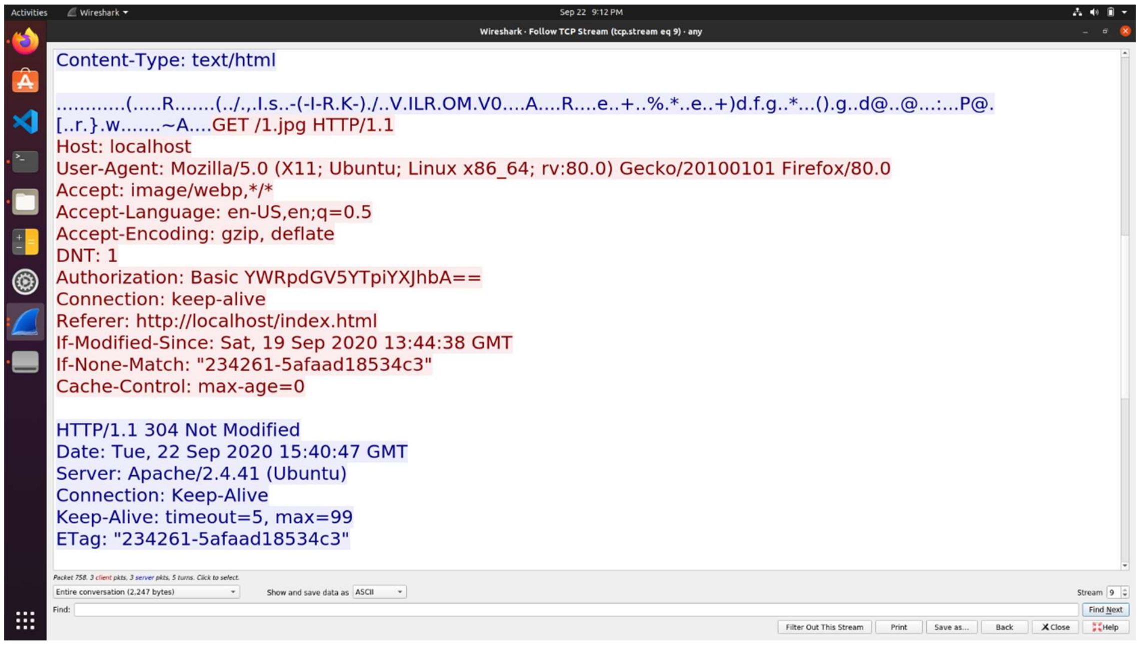
- A simple HTML file with 2 images is placed in the localhost home directory.
- From a browser, a request is made for the file, which receives a response of 200 OK with both images being sent by the server.

- When the request is sent again, the **`304 Not Modified`** status code is sent and images are not sent back.

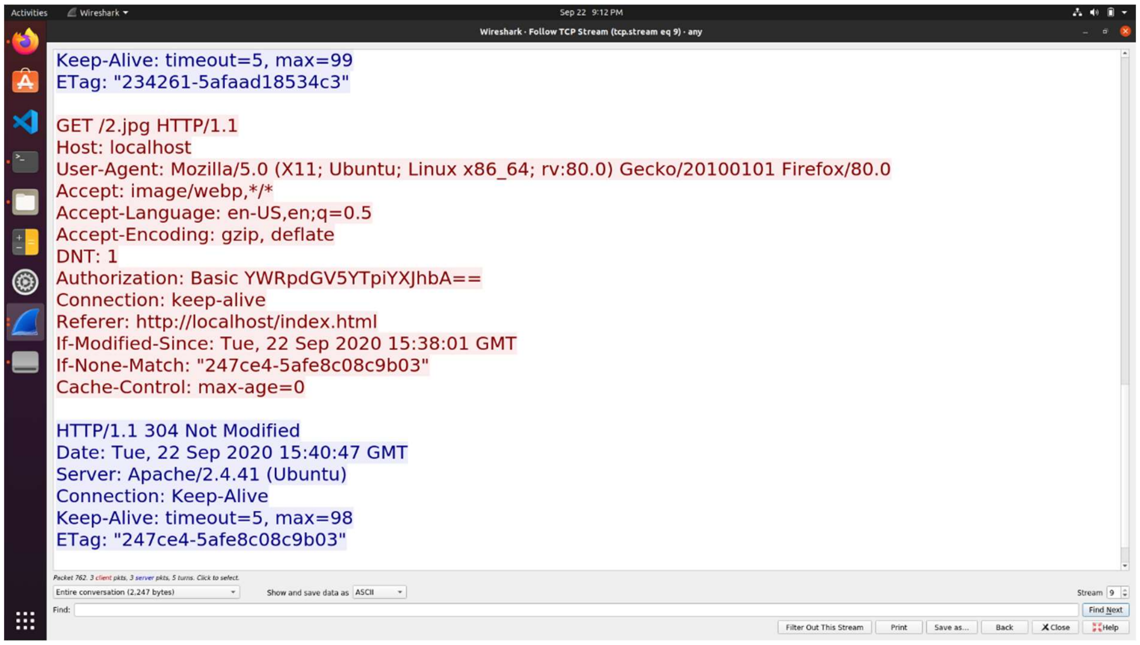


```
No.  Time          Source     Destination  Protocol Length Info
575  56.375592305  127.0.0.1  127.0.0.1    HTTP     457    GET /index.html HTTP/1.1
577  56.376805903  127.0.0.1  127.0.0.1    HTTP     550    HTTP/1.1 200 OK  (text/html)
597  56.695749942  127.0.0.1  127.0.0.1    HTTP     400    GET /1.jpg HTTP/1.1
691  56.703484096  127.0.0.1  127.0.0.1    HTTP     17…    HTTP/1.1 200 OK  (JPEG JFIF image)
693  56.741120840  127.0.0.1  127.0.0.1    HTTP     400    GET /2.jpg HTTP/1.1
730  56.876163457  127.0.0.1  127.0.0.1    HTTP     368    GET /favicon.ico HTTP/1.1
732  56.876746152  127.0.0.1  127.0.0.1    HTTP     555    HTTP/1.1 404 Not Found  (text/html)
752  68.265048678  127.0.0.1  127.0.0.1    HTTP     573    GET /index.html HTTP/1.1
754  68.266473867  127.0.0.1  127.0.0.1    HTTP     550    HTTP/1.1 200 OK  (text/html)
756  68.319004682  127.0.0.1  127.0.0.1    HTTP     515    GET /1.jpg HTTP/1.1
758  68.319658490  127.0.0.1  127.0.0.1    HTTP     251    HTTP/1.1 304 Not Modified
760  68.321504492  127.0.0.1  127.0.0.1    HTTP     515    GET /2.jpg HTTP/1.1
762  68.322096513  127.0.0.1  127.0.0.1    HTTP     251    HTTP/1.1 304 Not Modified

Frame 575: 457 bytes on wire (3656 bits), 457 bytes captured (3656 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: 42296, Dst Port: 80, Seq: 1, Ack: 1, Len: 389
Hypertext Transfer Protocol

any: <live capture in progress>    Packets: 768 · Displayed: 13 (1.7%)    Profile: Default
```

Activities
Wireshark
Sep 22 9:10 PM
Capturing from any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http



```
Content-Type: text/html

...........(.....R.......(../.,.l.s..-(-I-R.K-)./..V.ILR.OM.V0....A....R....e..+..%.*..e..+)d.f.g..*...().g..d@..@...:...P@.
[..r.}.w.......~A....GET /1.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
DNT: 1
Authorization: Basic YWRpdGV5YTpiYXJhbA==
Connection: keep-alive
Referer: http://localhost/index.html
If-Modified-Since: Sat, 19 Sep 2020 13:44:38 GMT
If-None-Match: "234261-5afaad18534c3"
Cache-Control: max-age=0

HTTP/1.1 304 Not Modified
Date: Tue, 22 Sep 2020 15:40:47 GMT
Server: Apache/2.4.41 (Ubuntu)
Connection: Keep-Alive
Keep-Alive: timeout=5, max=99
ETag: "234261-5afaad18534c3"

Packet 758. 3 client pkts, 3 server pkts, 5 turns. Click to select.
Entire conversation (2,247 bytes)    Show and save data as ASCII    Stream 9
```



```
Keep-Alive: timeout=5, max=99
ETag: "234261-5afaad18534c3"

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
DNT: 1
Authorization: Basic YWRpdGV5YTpiYXJhbA==
Connection: keep-alive
Referer: http://localhost/index.html
If-Modified-Since: Tue, 22 Sep 2020 15:38:01 GMT
If-None-Match: "247ce4-5afe8c08c9b03"
Cache-Control: max-age=0

HTTP/1.1 304 Not Modified
Date: Tue, 22 Sep 2020 15:40:47 GMT
Server: Apache/2.4.41 (Ubuntu)
Connection: Keep-Alive
Keep-Alive: timeout=5, max=98
ETag: "247ce4-5afe8c08c9b03"
```

Packet 762. 3 client pkts, 3 server pkts, 5 turns. Click to select.

Entire conversation (2,247 bytes)

Show and save data as ASCII

Stream 9

Find: