Week: #3

Understand working of HTTP Headers

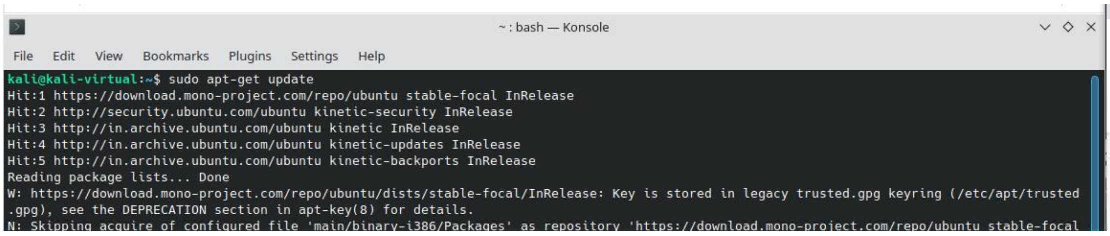
Name = Rachappa

Srn = PES1UG19CS359

ROLL NO = 1

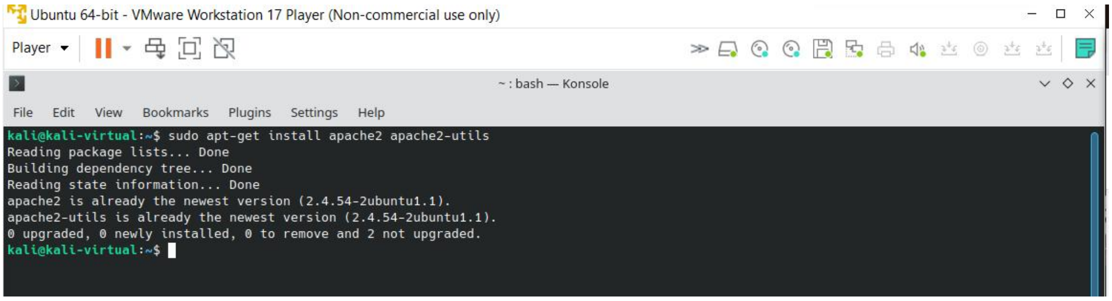
CLASS = A

sudo apt-get update



```
kali@kali-virtual:~$ sudo apt-get update
Hit:1 https://download.mono-project.com/repo/ubuntu stable-focal InRelease
Hit:2 http://security.ubuntu.com/ubuntu kinetic-security InRelease
Hit:3 http://in.archive.ubuntu.com/ubuntu kinetic InRelease
Hit:4 http://in.archive.ubuntu.com/ubuntu kinetic-updates InRelease
Hit:5 http://in.archive.ubuntu.com/ubuntu kinetic-backports InRelease
Reading package lists... Done
W: https://download.mono-project.com/repo/ubuntu/dists/stable-focal/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted
.gpg), see the DEPRECATION section in apt-key(8) for details.
N: Skipping acquire of configured file 'main/binary-i386/Packages' as repository 'https://download.mono-project.com/repo/ubuntu stable-focal
```

sudo apt-get install apache2 apache2-utils

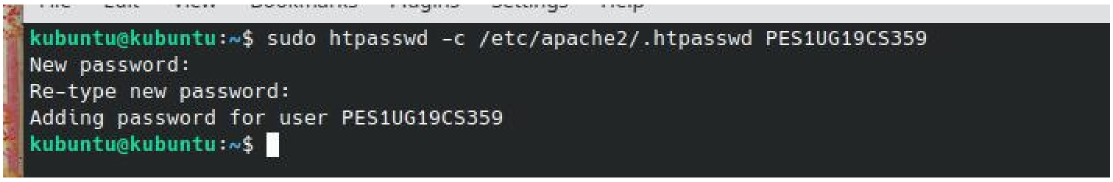


Ubuntu 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
~ : bash — Konsole
File
Edit
View
Bookmarks
Plugins
Settings
Help

```
kali@kali-virtual:~$ sudo apt-get install apache2 apache2-utils
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
apache2 is already the newest version (2.4.54-2ubuntu1.1).
apache2-utils is already the newest version (2.4.54-2ubuntu1.1).
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
kali@kali-virtual:~$ 
```

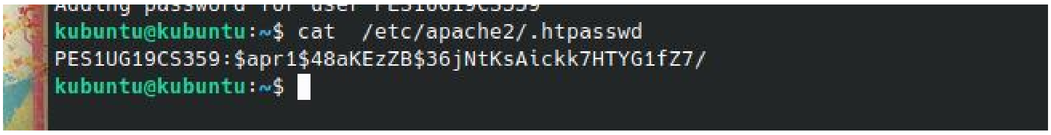
--> Provide username and password to set authentication

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

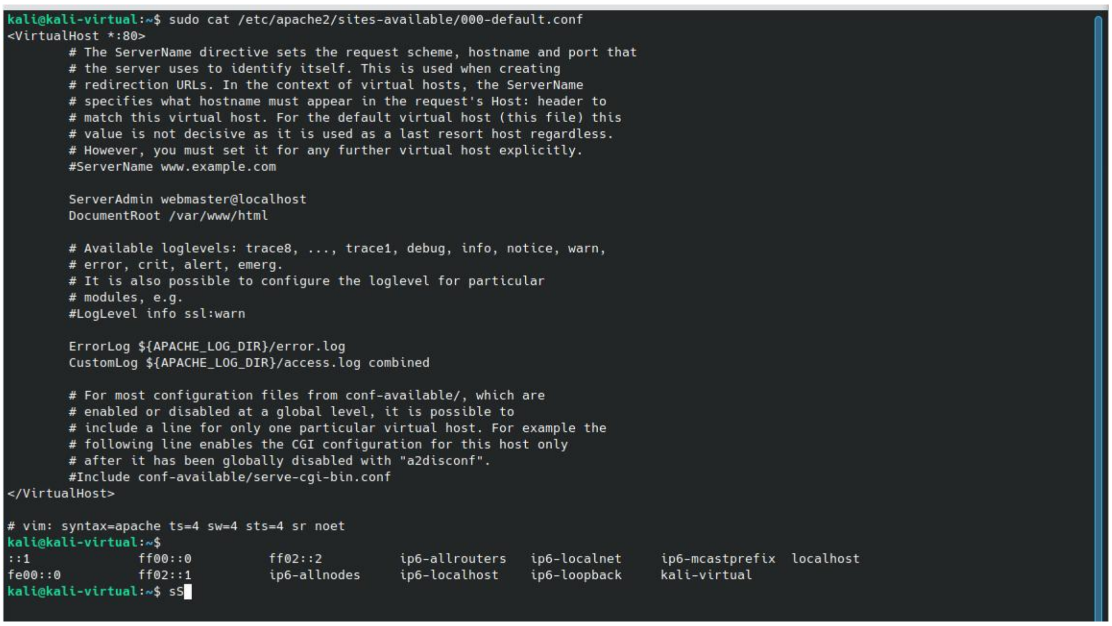


```
kubuntu@kubuntu:~$ sudo htpasswd -c /etc/apache2/.htpasswd PES1UG19CS359
New password:
Re-type new password:
Adding password for user PES1UG19CS359
kubuntu@kubuntu:~$
```

sudo cat /etc/apache2/.htpasswd



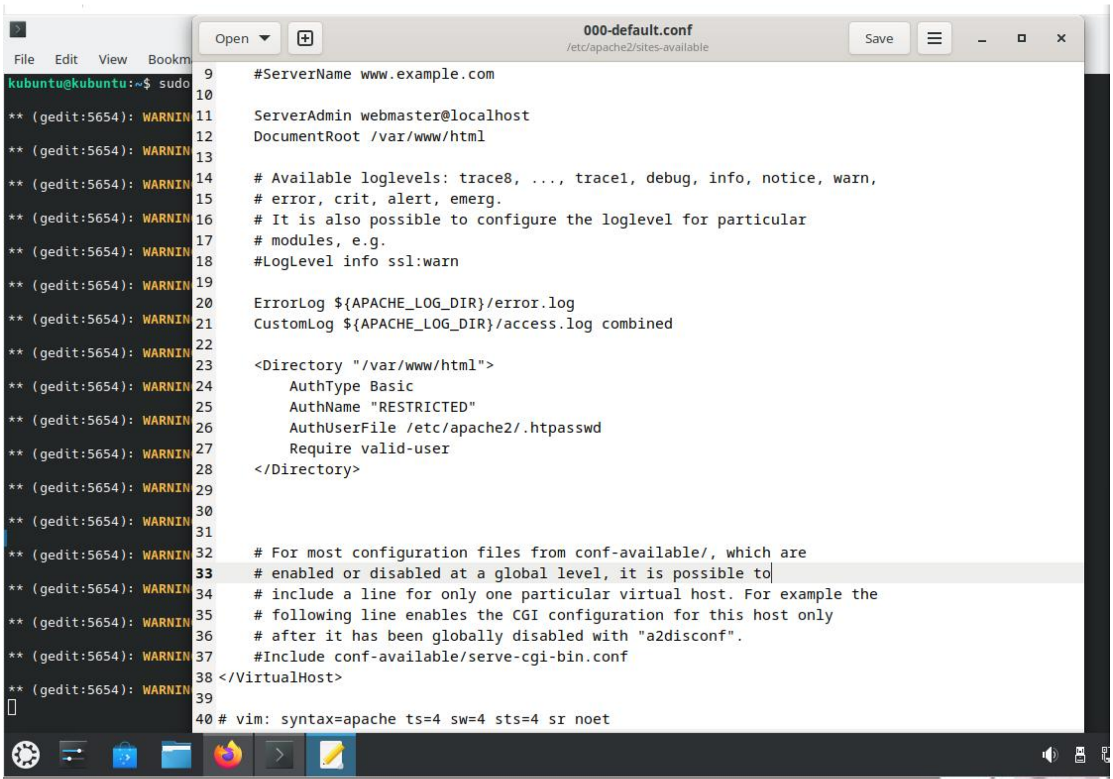
```
Adding password for user PES1UG19CS359
kubuntu@kubuntu:~$ cat  /etc/apache2/.htpasswd
PES1UG19CS359:$apr1$48aKEzZB$36jNtKsAickk7HTYG1fZ7/
kubuntu@kubuntu:~$
```



```
kali@kali-virtual:~$ sudo cat /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
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
kali@kali-virtual:~$
::1             ff00::0         ff02::2         ip6-allrouters   ip6-localnet     ip6-mcastprefix  localhost
fe00::0         ff02::1         ip6-allnodes    ip6-localhost    ip6-loopback     kali-virtual
kali@kali-virtual:~$ sS
```

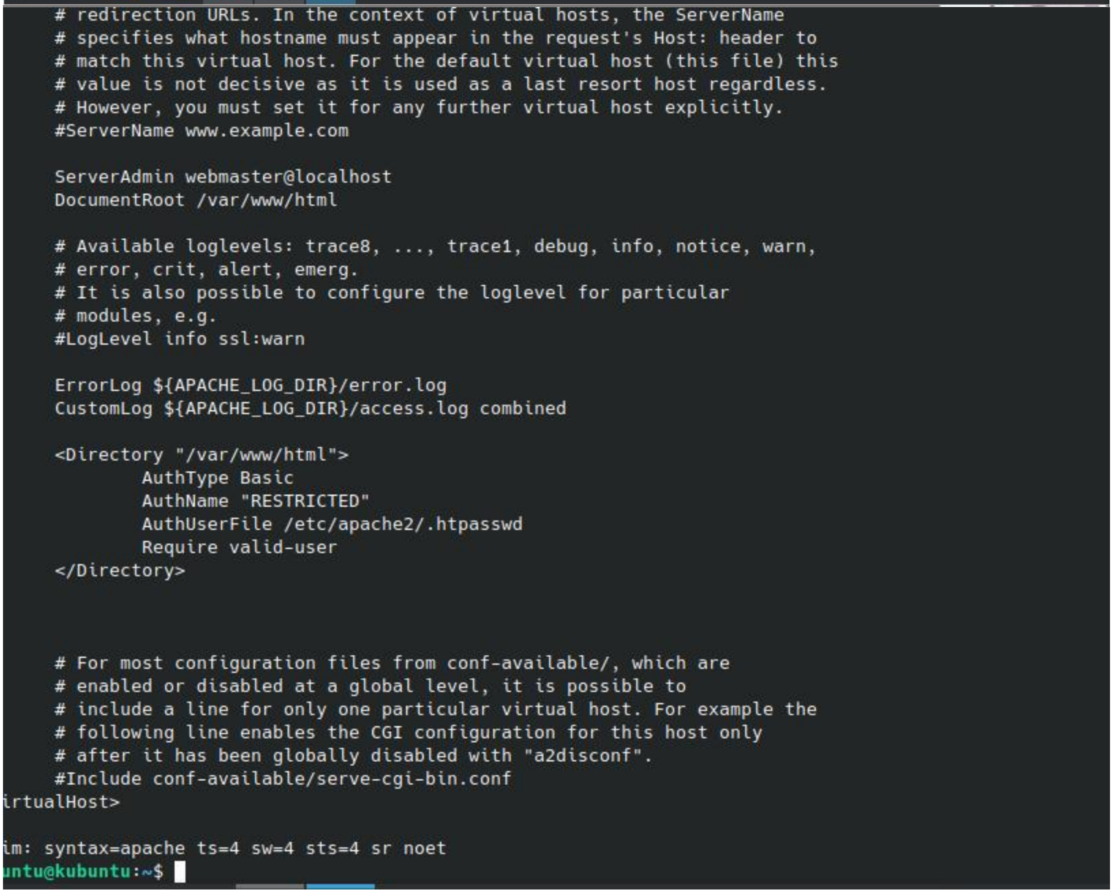
--> Opening the file for setting authentication

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



```
kubuntu@kubuntu:~$ sudo

** (gedit:5654): WARNIN

** (gedit:5654): WARNIN

** (gedit:5654): WARNIN

** (gedit:5654): WARNIN

** (gedit:5654): WARNIN

** (gedit:5654): WARNIN

** (gedit:5654): WARNIN

** (gedit:5654): WARNIN

** (gedit:5654): WARNIN

** (gedit:5654): WARNIN

** (gedit:5654): WARNIN

** (gedit:5654): WARNIN

** (gedit:5654): WARNIN

** (gedit:5654): WARNIN

** (gedit:5654): WARNIN

** (gedit:5654): WARNIN

** (gedit:5654): WARNIN

** (gedit:5654): WARNIN
```

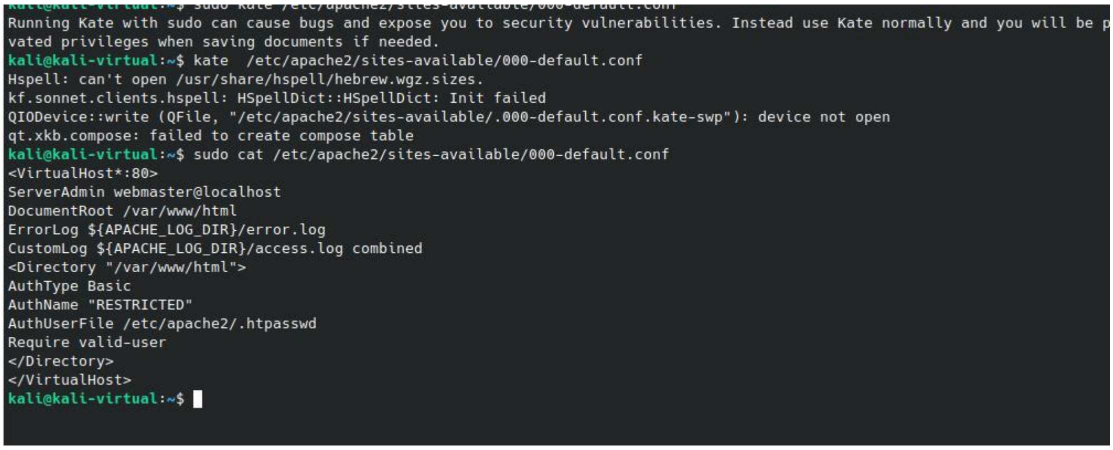
```
    #ServerName www.example.com

    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>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```



```
     # 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
irtualHost>

im: syntax=apache ts=4 sw=4 sts=4 sr noet
untu@kubuntu:~$
```

--> Opening the file for setting authentication

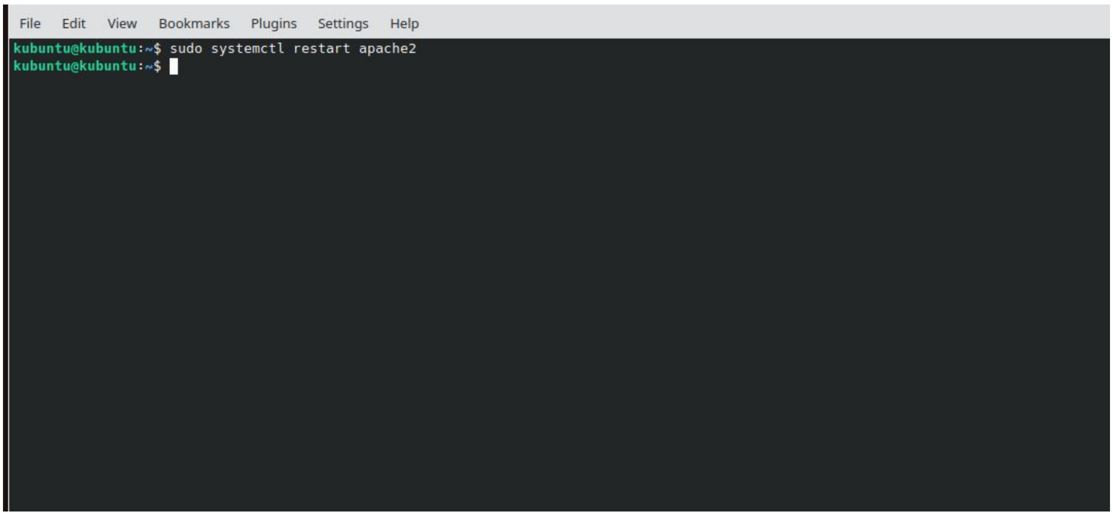
sudo nano /etc/apache2/sites-available/000-default.conf



```
kali@kali-virtual:~$ sudo kate /etc/apache2/sites-available/000-default.conf
Running Kate with sudo can cause bugs and expose you to security vulnerabilities. Instead use Kate normally and you will be p
vated privileges when saving documents if needed.
kali@kali-virtual:~$ kate  /etc/apache2/sites-available/000-default.conf
Hspell: can't open /usr/share/hspell/hebrew.wgz.sizes.
kf.sonnet.clients.hspell: HSpellDict::HSpellDict: Init failed
QIODevice::write (QFile, "/etc/apache2/sites-available/.000-default.conf.kate-swp"): device not open
qt.xkb.compose: failed to create compose table
kali@kali-virtual:~$ sudo cat /etc/apache2/sites-available/000-default.conf
<VirtualHost*:80>
ServerAdmin webmaster@localhost
DocumentRoot /var/www/html
ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined
<Directory "/var/www/html">
AuthType Basic
AuthName "RESTRICTED"
AuthUserFile /etc/apache2/.htpasswd
Require valid-user
</Directory>
</VirtualHost>
kali@kali-virtual:~$
```

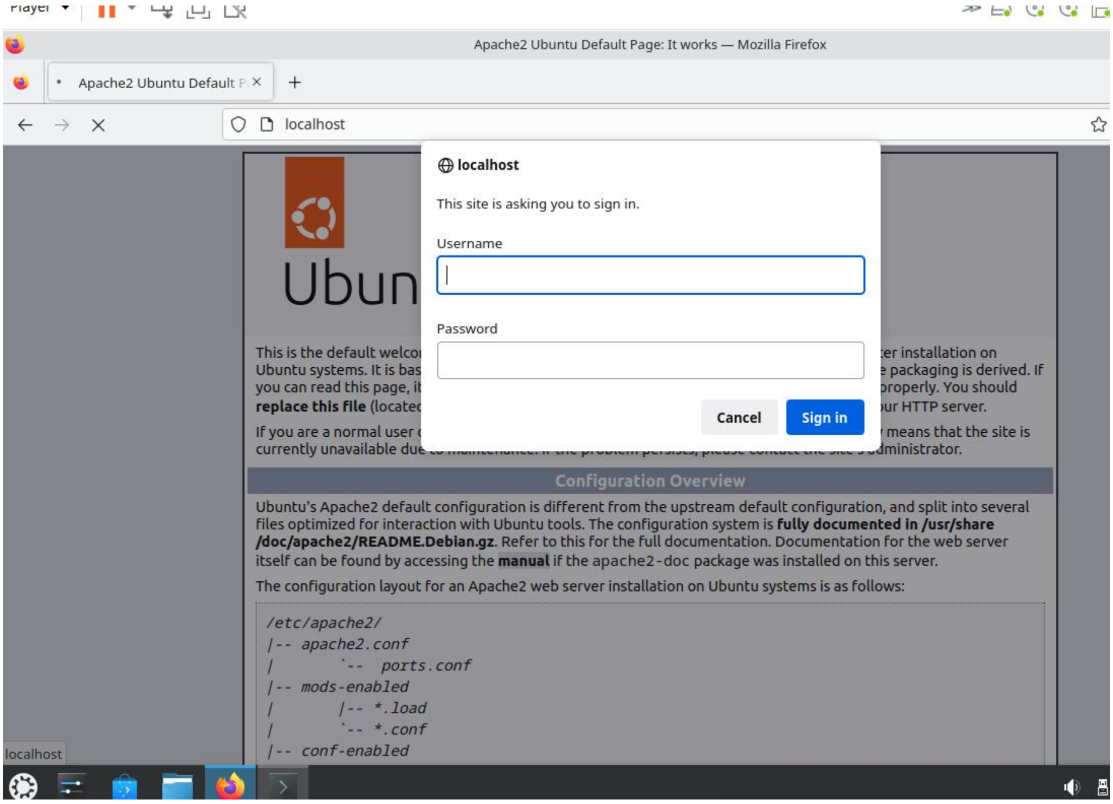
. Password policy implementation is done by restarting the server as:

sudo service apache2 restart



```
kubuntu@kubuntu:~$ sudo systemctl restart apache2
kubuntu@kubuntu:~$
```

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



localhost

This site is asking you to sign in.

Username

Password

Cancel Sign in

This is the default welco… …er installation on Ubuntu systems. It is bas… …e packaging is derived. If you can read this page, it… …properly. You should **replace this file** (locate… …ur HTTP server.

If you are a normal user… …means that the site is currently unavailable due… …administrator.

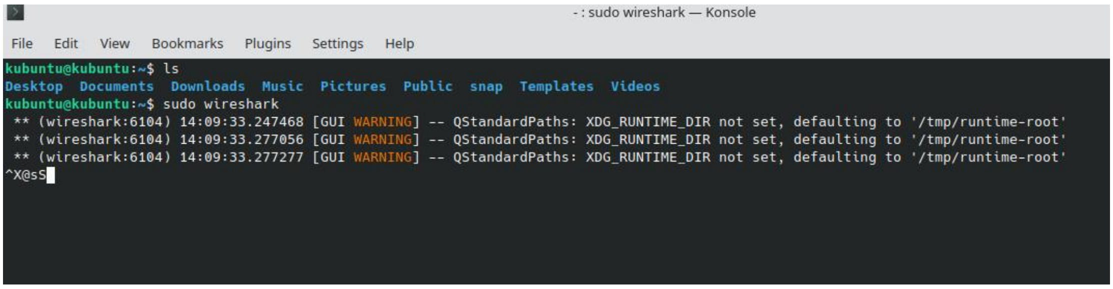
Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share /doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

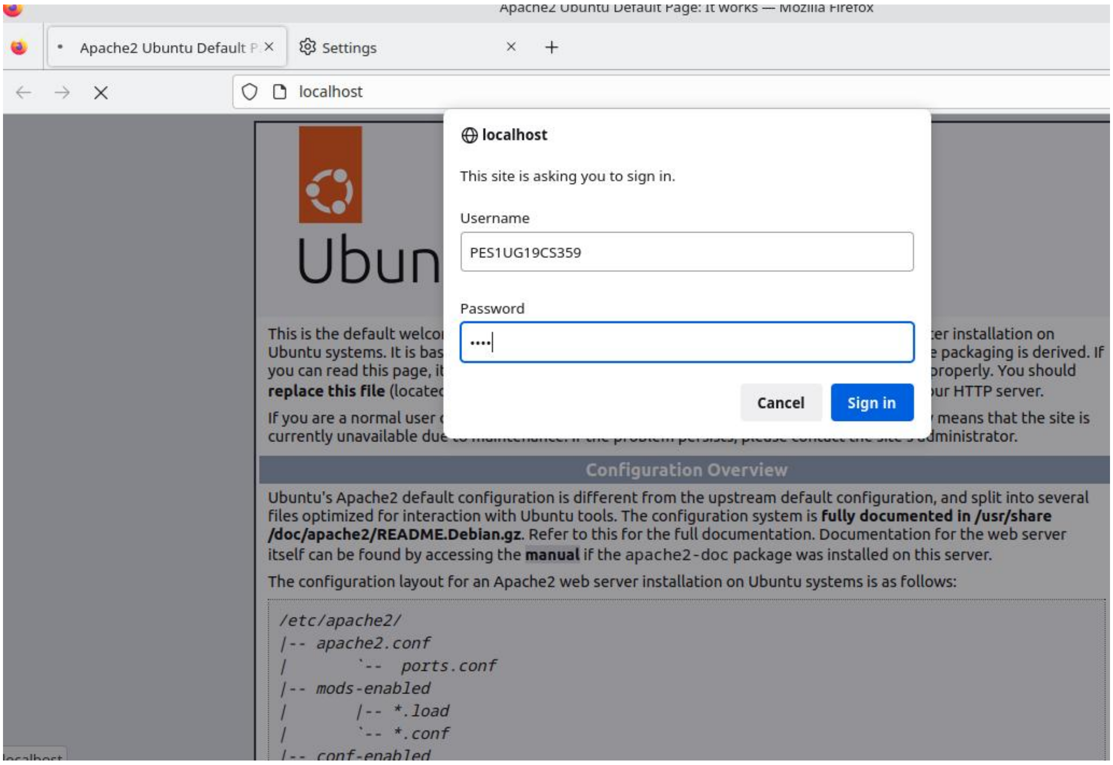
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
```

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


- : sudo wireshark — Konsole
File Edit View Bookmarks Plugins Settings Help

```
kubuntu@kubuntu:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  snap  Templates  Videos
kubuntu@kubuntu:~$ sudo wireshark
 ** (wireshark:6104) 14:09:33.247468 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
 ** (wireshark:6104) 14:09:33.277056 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
 ** (wireshark:6104) 14:09:33.277277 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
^X@sS
```



localhost

This site is asking you to sign in.

Username: PES1UG19CS359

Password: ••••

This is the default welco… …er installation on Ubuntu systems. It is bas… …e packaging is derived. If you can read this page, it… …properly. You should **replace this file** (located… …ur HTTP server.

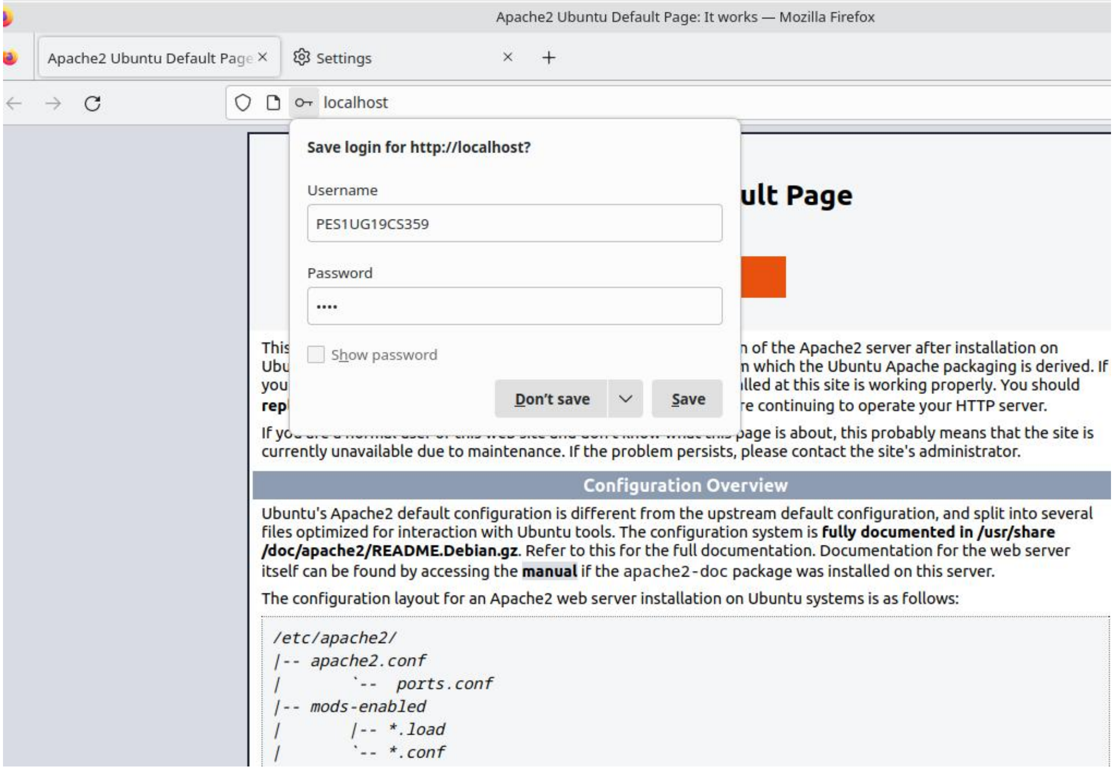
If you are a normal user o… …means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share /doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
```


Apache2 Ubuntu Default Page: It works — Mozilla Firefox
Apache2 Ubuntu Default Page
Settings
localhost
ult Page
Don't save
Save

Save login for http://localhost?

Username: PES1UG19CS359

Password: ••••

□ Show password

This… …n of the Apache2 server after installation on Ubu… …n which the Ubuntu Apache packaging is derived. If you… …lled at this site is working properly. You should rep… …re continuing to operate your HTTP server.

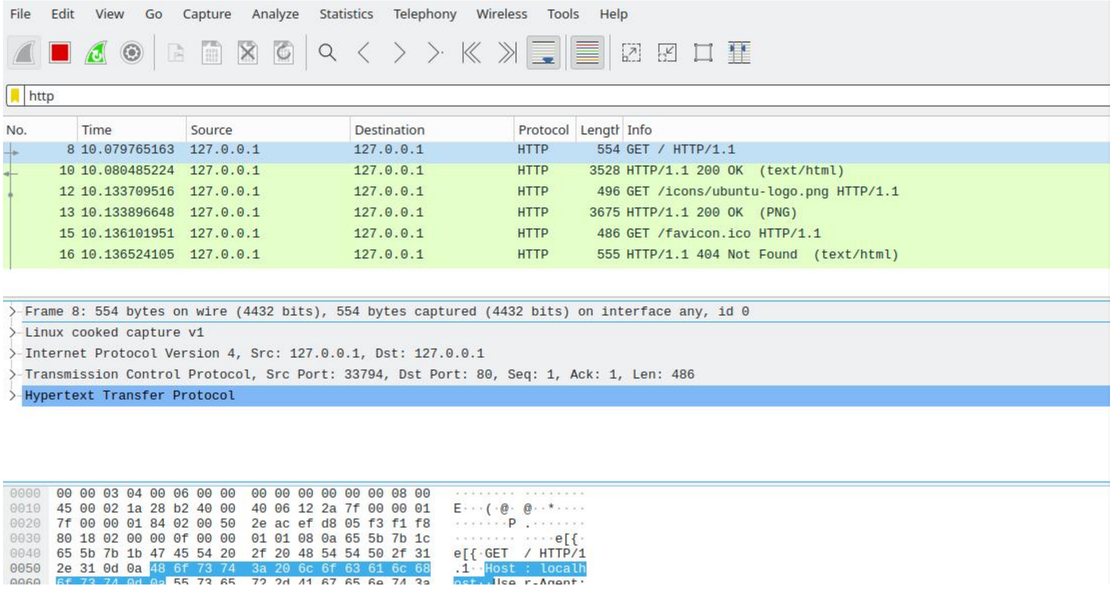
If yo… …page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share /doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
```



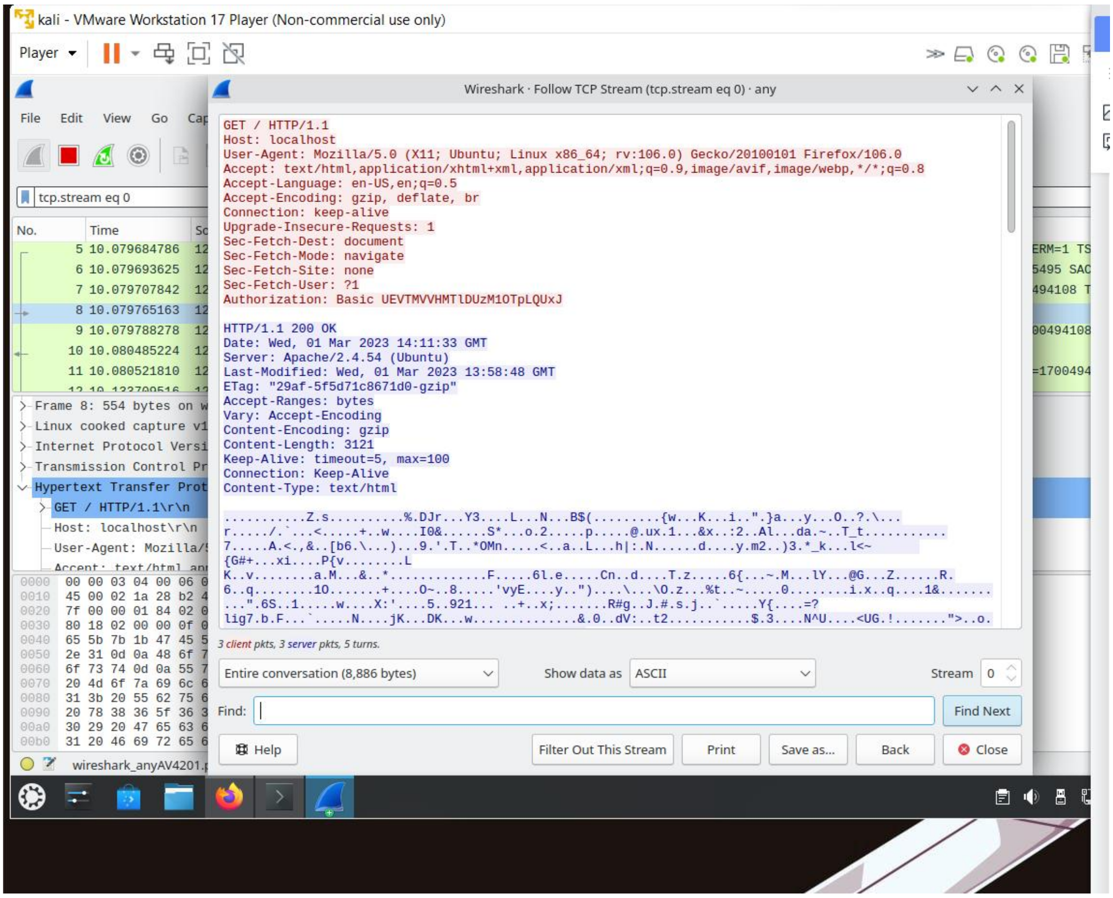
http

```
No.    Time          Source      Destination  Protocol  Length Info
     8 10.079765163  127.0.0.1   127.0.0.1    HTTP       554 GET / HTTP/1.1
    10 10.080485224  127.0.0.1   127.0.0.1    HTTP      3528 HTTP/1.1 200 OK  (text/html)
    12 10.133709516  127.0.0.1   127.0.0.1    HTTP       496 GET /icons/ubuntu-logo.png HTTP/1.1
    13 10.133896648  127.0.0.1   127.0.0.1    HTTP      3675 HTTP/1.1 200 OK  (PNG)
    15 10.136101951  127.0.0.1   127.0.0.1    HTTP       486 GET /favicon.ico HTTP/1.1
    16 10.136524105  127.0.0.1   127.0.0.1    HTTP       555 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 8: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface any, id 0
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 33794, Dst Port: 80, Seq: 1, Ack: 1, Len: 486
> Hypertext Transfer Protocol
```

```
0000  00 00 03 04 00 06 00 00  00 00 00 00 00 00 08 00   ········ ········
0010  45 00 02 1a 28 b2 40 00  40 06 12 2a 7f 00 00 01   E···(·@· @··*····
0020  7f 00 00 01 84 02 00 50  2e ac ef d8 05 f3 f1 f8   ·······P .·······
0030  80 18 02 00 00 0f 00 00  01 01 08 0a 65 5b 7b 1c   ········ ····e[{·
0040  65 5b 7b 1b 47 45 54 20  2f 20 48 54 54 50 2f 31   e[{·GET  / HTTP/1
0050  2e 31 0d 0a 48 6f 73 74  3a 20 6c 6f 63 61 6c 68   .1··Host : localh
```

6. 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



kali - VMware Workstation 17 Player (Non-commercial use only)

Wireshark · Follow TCP Stream (tcp.stream eq 0) · any

```
GET / HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:106.0) Gecko/20100101 Firefox/106.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Authorization: Basic UEVTMVVHMTlDUzM1OTpLQUxJ

HTTP/1.1 200 OK
Date: Wed, 01 Mar 2023 14:11:33 GMT
Server: Apache/2.4.54 (Ubuntu)
Last-Modified: Wed, 01 Mar 2023 13:58:48 GMT
ETag: "29af-5f5d71c8671d0-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 3121
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

..........Z.s..........%.DJr...Y3....L...N...B$(.........{w...K...i..".}a...y...O..?.\...
r...../.`...<.....+..w....I0&......S*...o.2.....p.....@.ux.1...&x..:2..Al...da.~..T_t..........
7.....A.<.,&..[b6.\...)...9.'.T..*OMn.....<..a..L...h|:.N......d....y.m2..)3.*_k...l<~
{G#+...xi....P{v........L
K..v........a.M...&..*.............F.....6l.e.....Cn..d....T.z.....6{...~.M...lY...@G...Z......R.
6..q........1O.......+....O~..8.....'vyE....y..")....\...\O.z...%t..~.....0........i.x..q....1&.......
..."..6S..1.....w....X:'....5..921...  ..+..x;.......R#g..J.#.s.j..`.....Y{....=?
lig7.b.F...`.....N....jK...DK...w..............&.0..dV:..t2..........$.3....N^U....<UG.!.......">..o.
```

3 client pkts, 3 server pkts, 5 turns.

Entire conversation (8,886 bytes)   Show data as ASCII   Stream 0

Find:

1.1 Understanding Base64 Algorithm

Base64 encode and decode algorithm converts any data into plain text and vice versa.

1.1.1 Base64 Encoding

Encoding is done in few simple steps.

Convert each character in the input string to its equivalent binary value. The binary value is obtained by converting the ASCII value of the character to binary.

PES1UG19CS359:1234 would be encoded as follows :

P - 01010000
E - 01000101
S - 01010011
1 - 00110001
U - 01010101
G - 01000111
1 - 00110001
9 - 00111001
C - 01000011
S - 01010011
3 - 00110011
5 - 00110101
9 - 00111001
: - 00111010
1 - 00110001
2 - 00110010
3 - 00110011
4 - 00110100

Now we will concatenate all the binary values together to get one big number.

0101000001000101010100110011000101010101010001110011000100111001...

Divide this giant number into chunks of 6 binary digits as follows.

010100 000100 010101 010011 001100 ....

Add 00 in beginning of every chunk and convert each chunk into its decimal equivalent as follows :

00010100 - 20
00000100 - 04

00010101 - 21
00010011 - 19
00001100 - 12
.
... and so on.

Now replace these decimal values with their corresponding alphabets. The alphabet set consists of all characters indexed from 0 i.e A = 0, B = 1, C = 2, D = 3 ... and so on.

Hence PES1UG19CS359:1234 in Base64 encode will result in

UEVTMVVHMTlDUzU3M10TpLQUxJ

1.1.2 Base64 Decoding

Decoding a Base64 encoded string is very simple and can be done as follows.

Split the Base64 encoded string character by character.

U
E
V
T
M
... and so on

Convert the alphabets into its decimal equivalents. If A = 0, B = 1, C = 2 ,...... then

U - 20
E - 4
V - 21
T - 19
M - 12
... and so on.

Convert these decimal numbers into its equivalent binary value.

20 - 00010100
04 - 00000100
21 - 00010101
... and so on.

Remove the first two 0's from each binary value and concatenate all the values into one big value.

010100000100010101010011 ...

Divide the above string into chunks of 8 as follows

01010000
01000101

01010011
... and so on.

Converting this binary number into decimal format will give us the ASCII value.
Based on the ASCII value we can convert it into alphabets.

$$01010000 \rightarrowtail 80(ASCII) \rightarrowtail P$$

$$01000101 \rightarrowtail 69(ASCII) \rightarrowtail E$$

$$01010011 \rightarrowtail 83(ASCII) \rightarrowtail S$$

... so on.

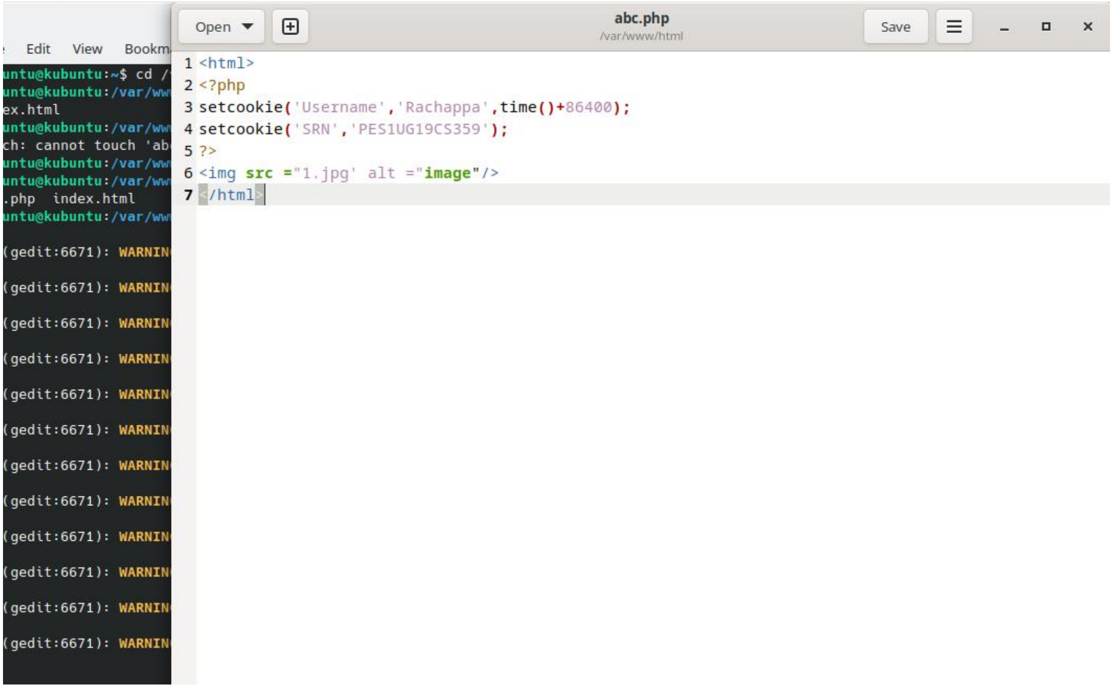
Concatenating all letters, we get back PES1UG19CS571:1234.
Thus we have successfully decoded the credentials.

UEVTMVVHMTlDUzU3M10TpLQUxJ ↣ PES1UG19CS5359:1234

Steps of Execution (Cookie Setting)

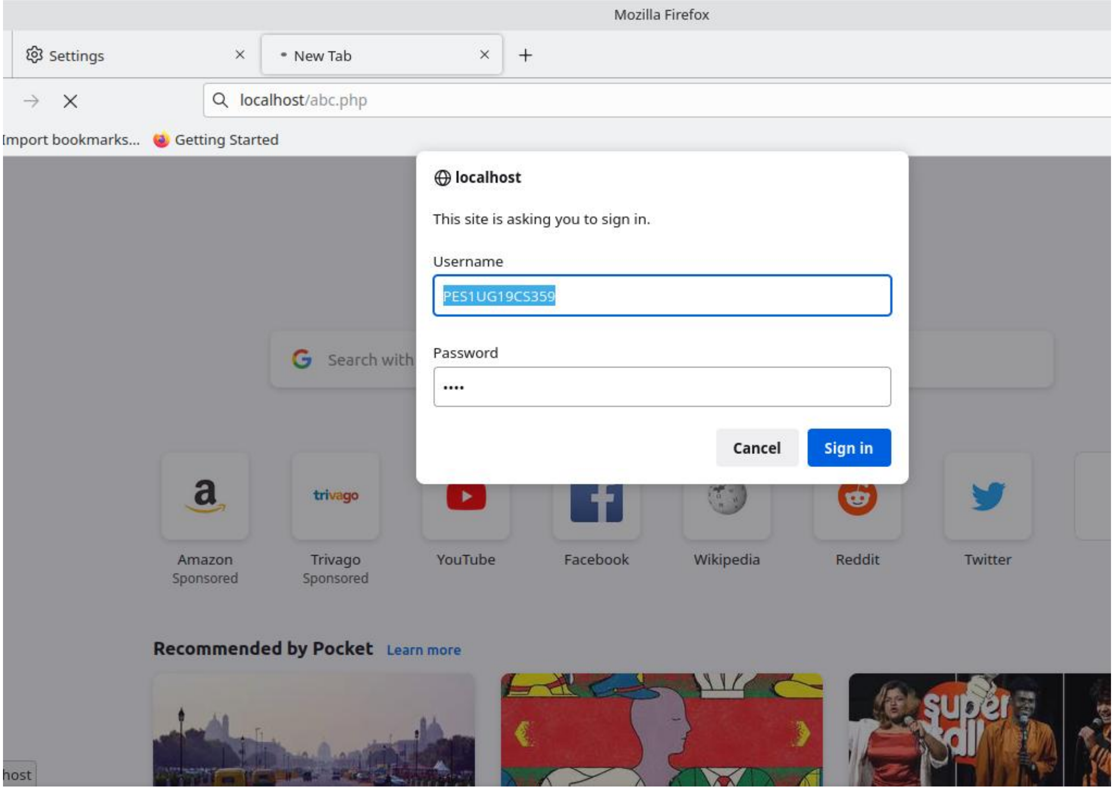
1. A PHP file to set the cookie is created which also contains an image in it (placed under the HTML directory) to be accessed once the cookie is set. The following code helped to set the cookie:

1.2 Setting Cookies using PHP



```
untu@kubuntu:~$ cd /
untu@kubuntu:/var/ww
ex.html
untu@kubuntu:/var/ww
ch: cannot touch 'ab
untu@kubuntu:/var/ww
untu@kubuntu:/var/ww
.php  index.html
untu@kubuntu:/var/ww

(gedit:6671): WARNIN

(gedit:6671): WARNIN

(gedit:6671): WARNIN

(gedit:6671): WARNIN

(gedit:6671): WARNIN

(gedit:6671): WARNIN

(gedit:6671): WARNIN

(gedit:6671): WARNIN

(gedit:6671): WARNIN

(gedit:6671): WARNIN

(gedit:6671): WARNIN

(gedit:6671): WARNIN
```

```
<html>
<?php
setcookie('Username','Rachappa',time()+86400);
setcookie('SRN','PES1UG19CS359');
?>
<img src ="1.jpg' alt ="image"/>
</html>
```



localhost

This site is asking you to sign in.

Username

PES1UG19CS359

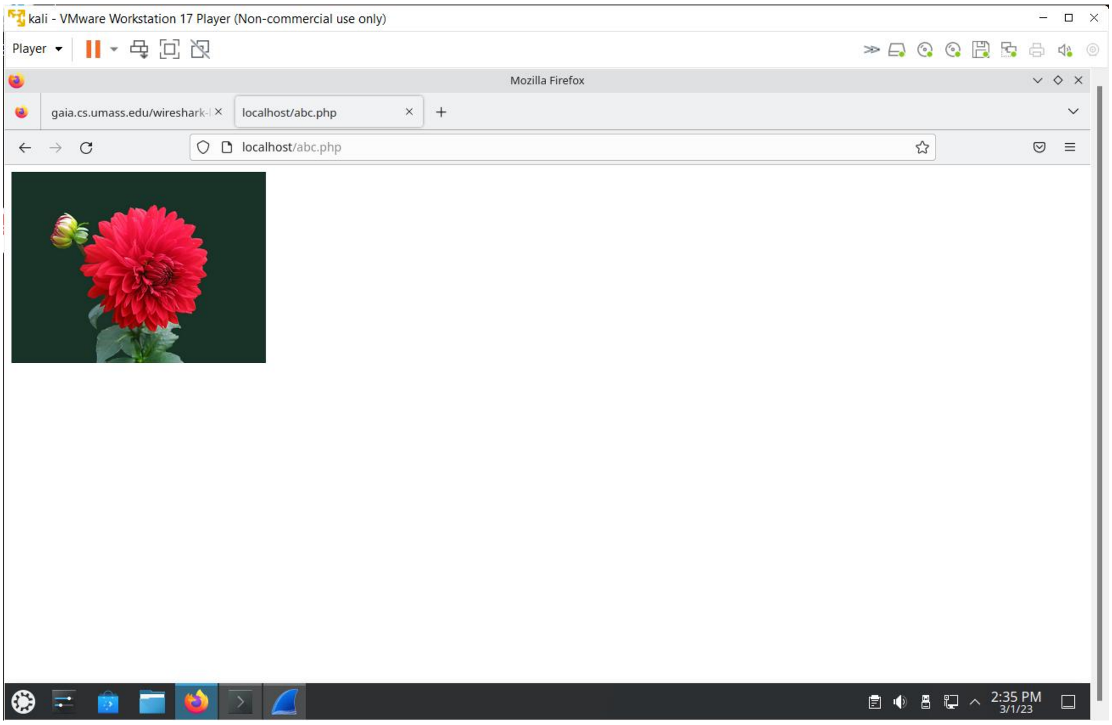
Password

••••

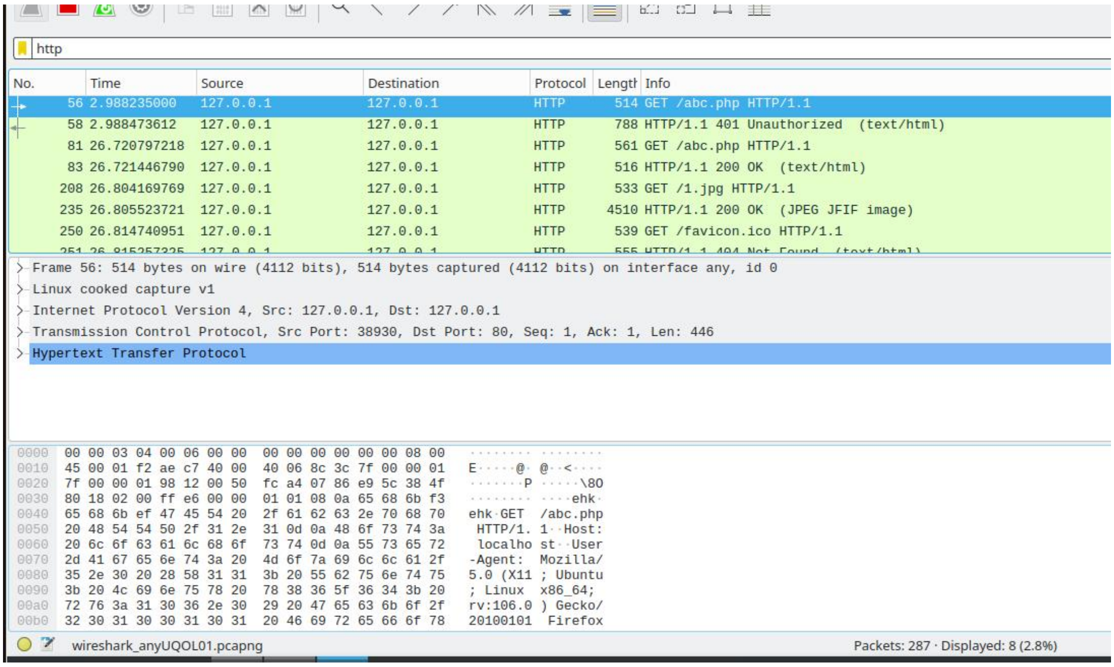
Cancel

Sign in

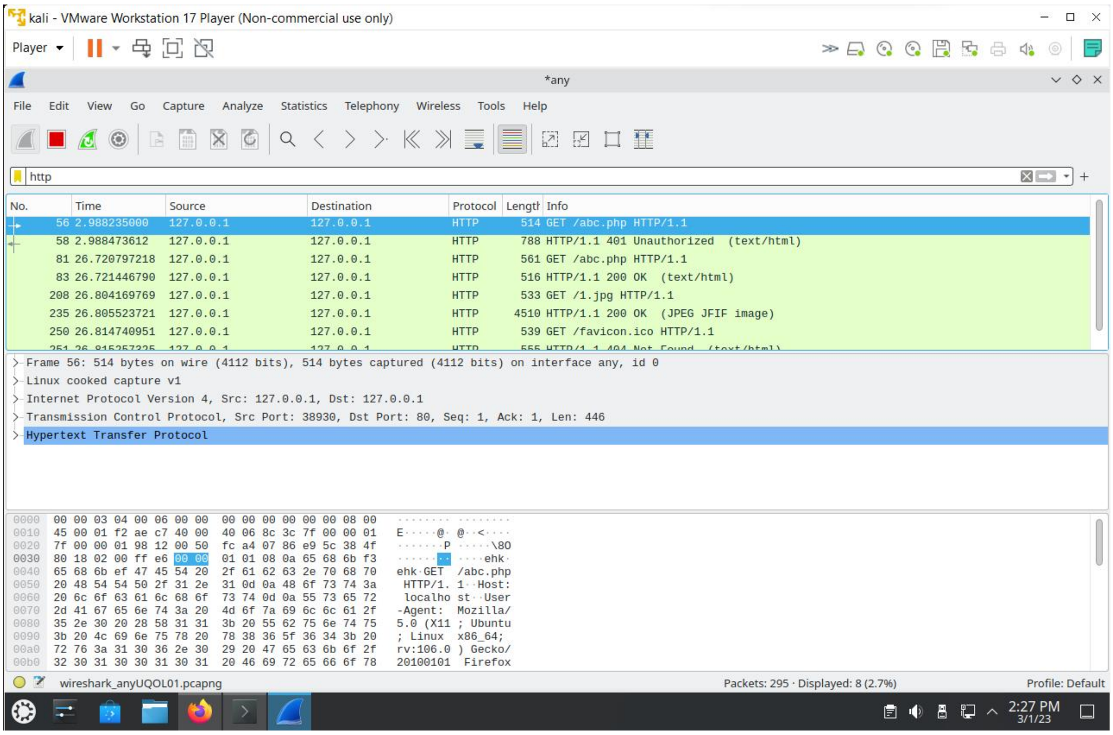
2. The combined file saved with a .php extension is placed under ***/var/www/html*** for accessing.


kali - VMware Workstation 17 Player (Non-commercial use only)
Player
Mozilla Firefox
gaia.cs.umass.edu/wireshark-
localhost/abc.php
localhost/abc.php
2:35 PM
3/1/23

1.3 Capturing Packets in Wireshark



```
http

No.   Time          Source      Destination  Protocol  Length  Info
   56 2.988235000   127.0.0.1   127.0.0.1    HTTP       514 GET /abc.php HTTP/1.1
   58 2.988473612   127.0.0.1   127.0.0.1    HTTP       788 HTTP/1.1 401 Unauthorized  (text/html)
   81 26.720797218  127.0.0.1   127.0.0.1    HTTP       561 GET /abc.php HTTP/1.1
   83 26.721446790  127.0.0.1   127.0.0.1    HTTP       516 HTTP/1.1 200 OK  (text/html)
  208 26.804169769  127.0.0.1   127.0.0.1    HTTP       533 GET /1.jpg HTTP/1.1
  235 26.805523721  127.0.0.1   127.0.0.1    HTTP      4510 HTTP/1.1 200 OK  (JPEG JFIF image)
  250 26.814740951  127.0.0.1   127.0.0.1    HTTP       539 GET /favicon.ico HTTP/1.1
  251 26.815257325  127.0.0.1   127.0.0.1    HTTP       555 HTTP/1.1 404 Not Found  (text/html)

> Frame 56: 514 bytes on wire (4112 bits), 514 bytes captured (4112 bits) on interface any, id 0
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 38930, Dst Port: 80, Seq: 1, Ack: 1, Len: 446
> Hypertext Transfer Protocol

0000  00 00 03 04 00 06 00 00  00 00 00 00 00 00 08 00   ········ ········
0010  45 00 01 f2 ae c7 40 00  40 06 8c 3c 7f 00 00 01   E·····@· @··<····
0020  7f 00 00 01 98 12 00 50  fc a4 07 86 e9 5c 38 4f   ·······P ·····\8O
0030  80 18 02 00 ff e6 00 00  01 01 08 0a 65 68 6b f3   ········ ····ehk·
0040  65 68 6b ef 47 45 54 20  2f 61 62 63 2e 70 68 70   ehk·GET  /abc.php
0050  20 48 54 54 50 2f 31 2e  31 0d 0a 48 6f 73 74 3a    HTTP/1. 1··Host:
0060  20 6c 6f 63 61 6c 68 6f  73 74 0d 0a 55 73 65 72    localho st··User
0070  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
0080  35 2e 30 20 28 58 31 31  3b 20 55 62 75 6e 74 75   5.0 (X11 ; Ubuntu
0090  3b 20 4c 69 6e 75 78 20  78 38 36 5f 36 34 3b 20   ; Linux  x86_64;
00a0  72 76 3a 31 30 36 2e 30  29 20 47 65 63 6b 6f 2f   rv:106.0 ) Gecko/
00b0  32 30 31 30 30 31 30 31  20 46 69 72 65 66 6f 78   20100101  Firefox

wireshark_anyUQOL01.pcapng                               Packets: 287 · Displayed: 8 (2.8%)
```



kali - VMware Workstation 17 Player (Non-commercial use only)
Player
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

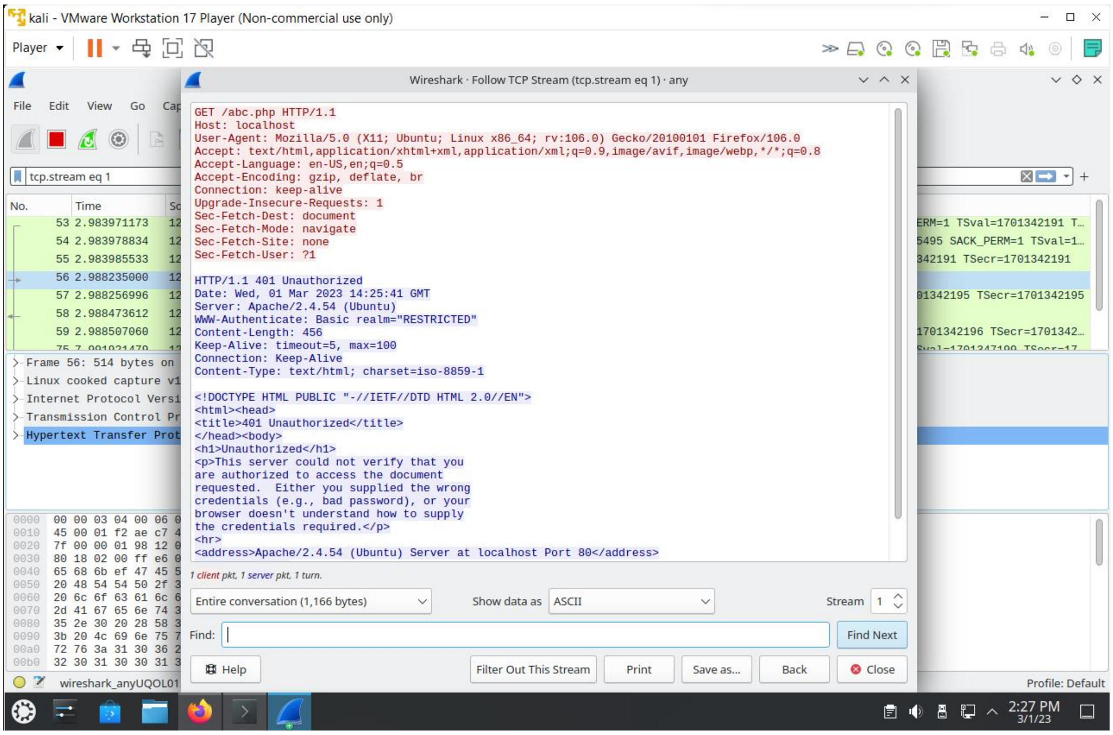
http

```
No.   Time          Source      Destination  Protocol  Length  Info
   56 2.988235000   127.0.0.1   127.0.0.1    HTTP       514 GET /abc.php HTTP/1.1
   58 2.988473612   127.0.0.1   127.0.0.1    HTTP       788 HTTP/1.1 401 Unauthorized  (text/html)
   81 26.720797218  127.0.0.1   127.0.0.1    HTTP       561 GET /abc.php HTTP/1.1
   83 26.721446790  127.0.0.1   127.0.0.1    HTTP       516 HTTP/1.1 200 OK  (text/html)
  208 26.804169769  127.0.0.1   127.0.0.1    HTTP       533 GET /1.jpg HTTP/1.1
  235 26.805523721  127.0.0.1   127.0.0.1    HTTP      4510 HTTP/1.1 200 OK  (JPEG JFIF image)
  250 26.814740951  127.0.0.1   127.0.0.1    HTTP       539 GET /favicon.ico HTTP/1.1
  251 26.815257325  127.0.0.1   127.0.0.1    HTTP       555 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 56: 514 bytes on wire (4112 bits), 514 bytes captured (4112 bits) on interface any, id 0
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 38930, Dst Port: 80, Seq: 1, Ack: 1, Len: 446
> Hypertext Transfer Protocol
```

```
0000  00 00 03 04 00 06 00 00  00 00 00 00 00 00 08 00   ········ ········
0010  45 00 01 f2 ae c7 40 00  40 06 8c 3c 7f 00 00 01   E·····@· @··<····
0020  7f 00 00 01 98 12 00 50  fc a4 07 86 e9 5c 38 4f   ·······P ·····\8O
0030  80 18 02 00 ff e6 00 00  01 01 08 0a 65 68 6b f3   ········ ····ehk·
0040  65 68 6b ef 47 45 54 20  2f 61 62 63 2e 70 68 70   ehk·GET  /abc.php
0050  20 48 54 54 50 2f 31 2e  31 0d 0a 48 6f 73 74 3a    HTTP/1. 1··Host:
0060  20 6c 6f 63 61 6c 68 6f  73 74 0d 0a 55 73 65 72    localho st··User
0070  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
0080  35 2e 30 20 28 58 31 31  3b 20 55 62 75 6e 74 75   5.0 (X11 ; Ubuntu
0090  3b 20 4c 69 6e 75 78 20  78 38 36 5f 36 34 3b 20   ; Linux  x86_64;
00a0  72 76 3a 31 30 36 2e 30  29 20 47 65 63 6b 6f 2f   rv:106.0 ) Gecko/
00b0  32 30 31 30 30 31 30 31  20 46 69 72 65 66 6f 78   20100101  Firefox
```

wireshark_anyUQOL01.pcapng   Packets: 295 · Displayed: 8 (2.7%)   Profile: Default



kali - VMware Workstation 17 Player (Non-commercial use only)
Player
Wireshark · Follow TCP Stream (tcp.stream eq 1) · any

tcp.stream eq 1

```
GET /abc.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:106.0) Gecko/20100101 Firefox/106.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1

HTTP/1.1 401 Unauthorized
Date: Wed, 01 Mar 2023 14:25:41 GMT
Server: Apache/2.4.54 (Ubuntu)
WWW-Authenticate: Basic realm="RESTRICTED"
Content-Length: 456
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>401 Unauthorized</title>
</head><body>
<h1>Unauthorized</h1>
<p>This server could not verify that you
are authorized to access the document
requested.  Either you supplied the wrong
credentials (e.g., bad password), or your
browser doesn't understand how to supply
the credentials required.</p>
<hr>
<address>Apache/2.4.54 (Ubuntu) Server at localhost Port 80</address>
```

1 client pkt, 1 server pkt, 1 turn.

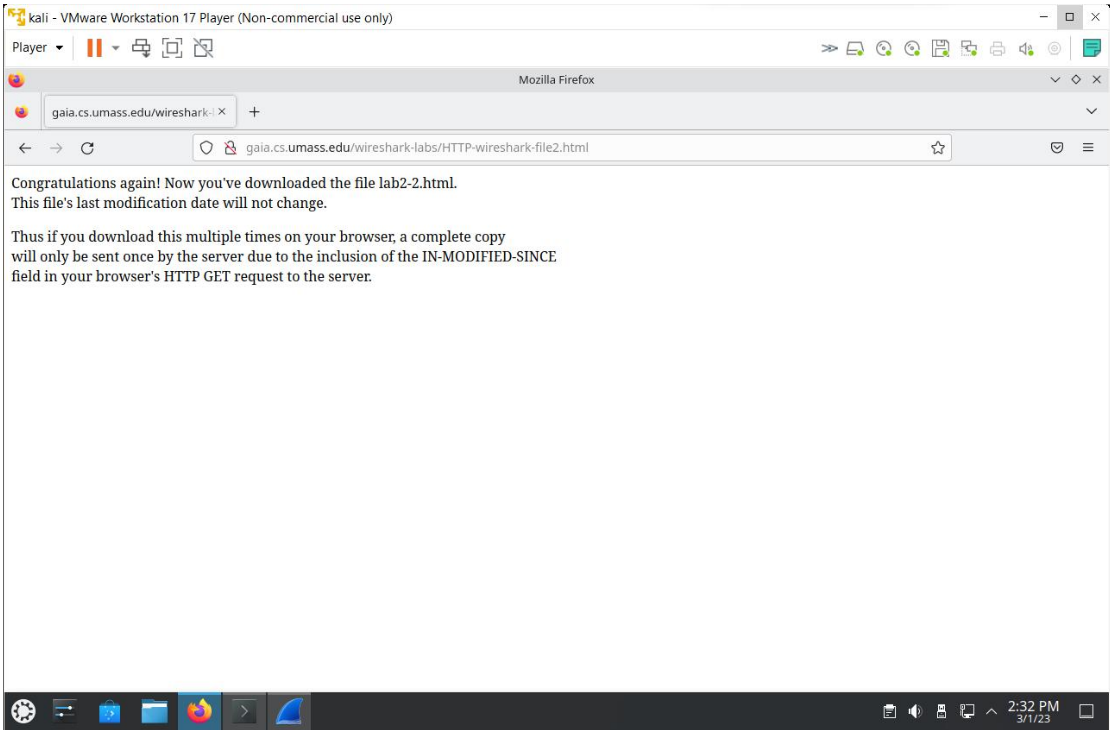
Entire conversation (1,166 bytes)   Show data as ASCII   Stream 1

Find:

Conditional Get: If-Modified-Since

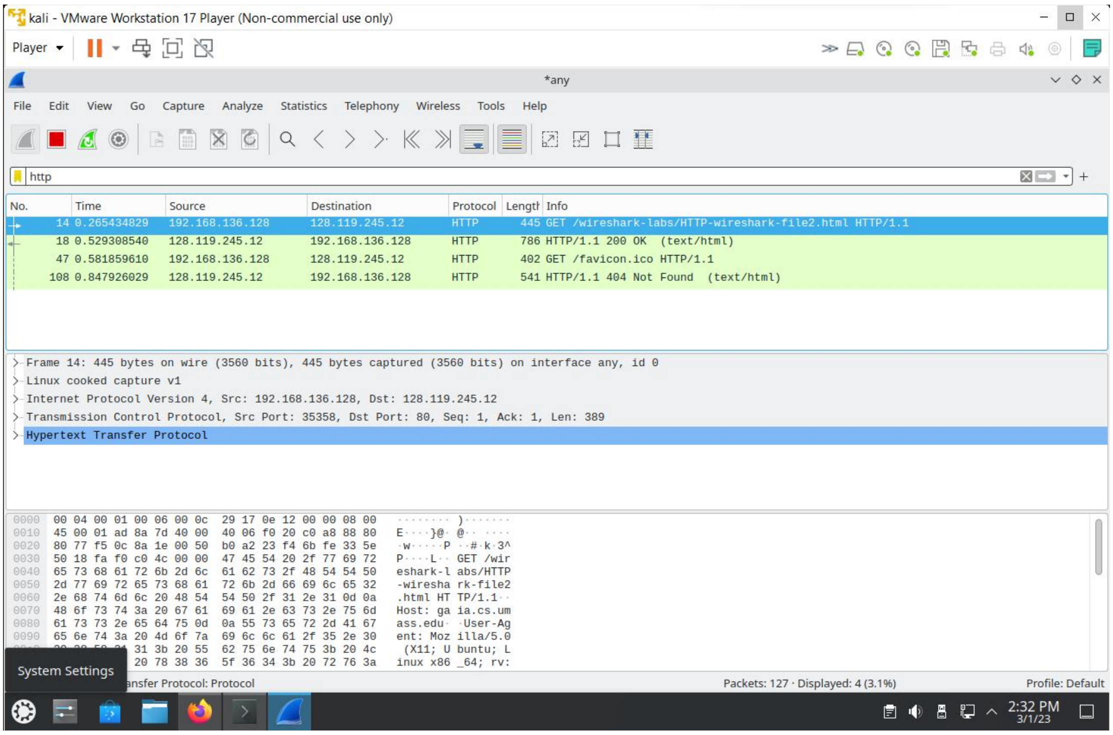
Before performing the steps below, make sure your browser’s cache is empty. (To do this under
Firefox, select Tools -> Clear Recent History and check the Cache box). Now do the following:➢ Start up your web browser, and make sure your browser’s cache is cleared, as discussed

above.
➢ Start up the Wireshark packet sniffer.
➢ Enter the following URL into your browser http://gaia.cs.umass.edu/wireshark labs/HTTP-wireshark-file2.html
➢ Your browser should display a very simple five-line HTML file.
➢ Quickly enter the same URL into your browser again (or simply select the refresh button
on your browser)
➢ Stop Wireshark packet capture, and enter “http” in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet listing window.


kali - VMware Workstation 17 Player (Non-commercial use only)
Player
Mozilla Firefox
gaia.cs.umass.edu/wireshark-l
gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html
2:32 PM
3/1/23

Congratulations again! Now you've downloaded the file lab2-2.html.
This file's last modification date will not change.

Thus if you download this multiple times on your browser, a complete copy
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE
field in your browser's HTTP GET request to the server.



```
http
```

```
No.     Time          Source            Destination       Protocol  Lengtł Info
     14 0.265434829   192.168.136.128   128.119.245.12    HTTP       445 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
     18 0.529308540   128.119.245.12    192.168.136.128   HTTP       786 HTTP/1.1 200 OK  (text/html)
     47 0.581859610   192.168.136.128   128.119.245.12    HTTP       402 GET /favicon.ico HTTP/1.1
    108 0.847926029   128.119.245.12    192.168.136.128   HTTP       541 HTTP/1.1 404 Not Found  (text/html)
```

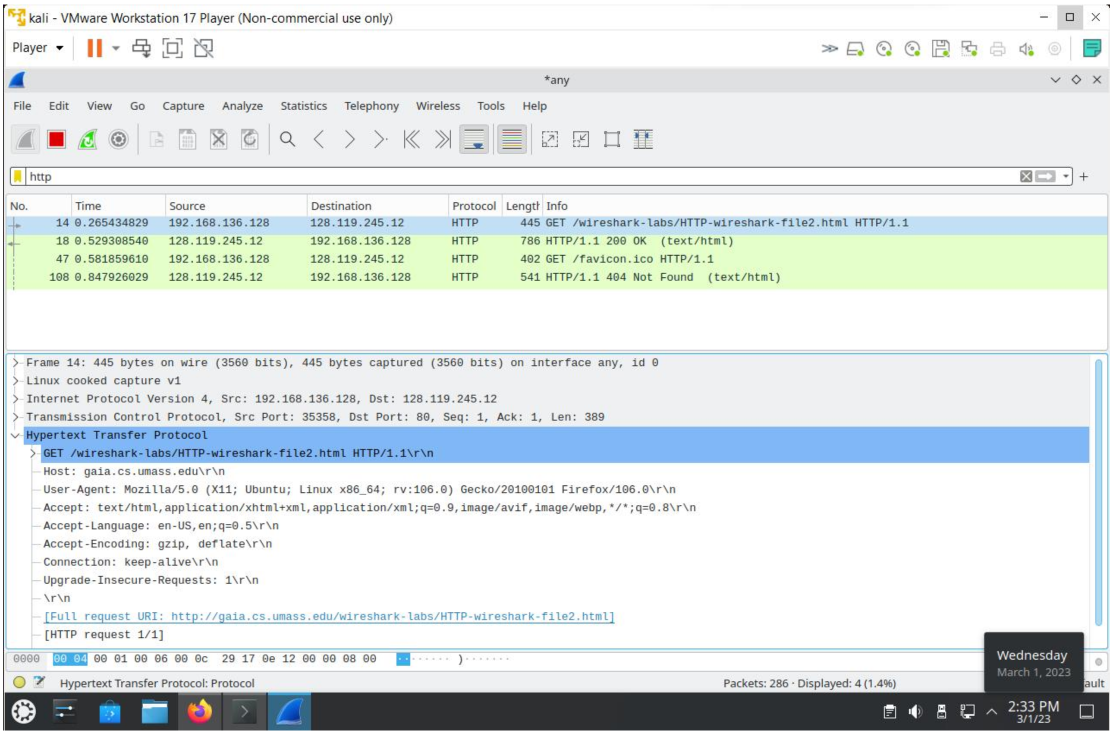
```
> Frame 14: 445 bytes on wire (3560 bits), 445 bytes captured (3560 bits) on interface any, id 0
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 192.168.136.128, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 35358, Dst Port: 80, Seq: 1, Ack: 1, Len: 389
> Hypertext Transfer Protocol
```

```
0000  00 04 00 01 00 06 00 0c  29 17 0e 12 00 00 08 00   ········ )·······
0010  45 00 01 ad 8a 7d 40 00  40 06 f0 20 c0 a8 88 80   E····}@· @·· ····
0020  80 77 f5 0c 8a 1e 00 50  b0 a2 23 f4 6b fe 33 5e   ·w·····P ··#·k·3^
0030  50 18 fa f0 c0 4c 00 00  47 45 54 20 2f 77 69 72   P····L·· GET /wir
0040  65 73 68 61 72 6b 2d 6c  61 62 73 2f 48 54 54 50   eshark-l abs/HTTP
0050  2d 77 69 72 65 73 68 61  72 6b 2d 66 69 6c 65 32   -wiresha rk-file2
0060  2e 68 74 6d 6c 20 48 54  54 50 2f 31 2e 31 0d 0a   .html HT TP/1.1··
0070  48 6f 73 74 3a 20 67 61  69 61 2e 63 73 2e 75 6d   Host: ga ia.cs.um
0080  61 73 73 2e 65 64 75 0d  0a 55 73 65 72 2d 41 67   ass.edu· ·User-Ag
0090  65 6e 74 3a 20 4d 6f 7a  69 6c 6c 61 2f 35 2e 30   ent: Moz illa/5.0
                  31 3b 20 55  62 75 6e 74 75 3b 20 4c    (X11; U buntu; L
                  20 78 38 36  5f 36 34 3b 20 72 76 3a   inux x86 _64; rv:
```

ansfer Protocol: Protocol

Packets: 127 · Displayed: 4 (3.1%)

Profile: Default



```
http
```

```
No.     Time          Source            Destination       Protocol  Lengtł Info
     14 0.265434829   192.168.136.128   128.119.245.12    HTTP       445 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
     18 0.529308540   128.119.245.12    192.168.136.128   HTTP       786 HTTP/1.1 200 OK  (text/html)
     47 0.581859610   192.168.136.128   128.119.245.12    HTTP       402 GET /favicon.ico HTTP/1.1
    108 0.847926029   128.119.245.12    192.168.136.128   HTTP       541 HTTP/1.1 404 Not Found  (text/html)
```

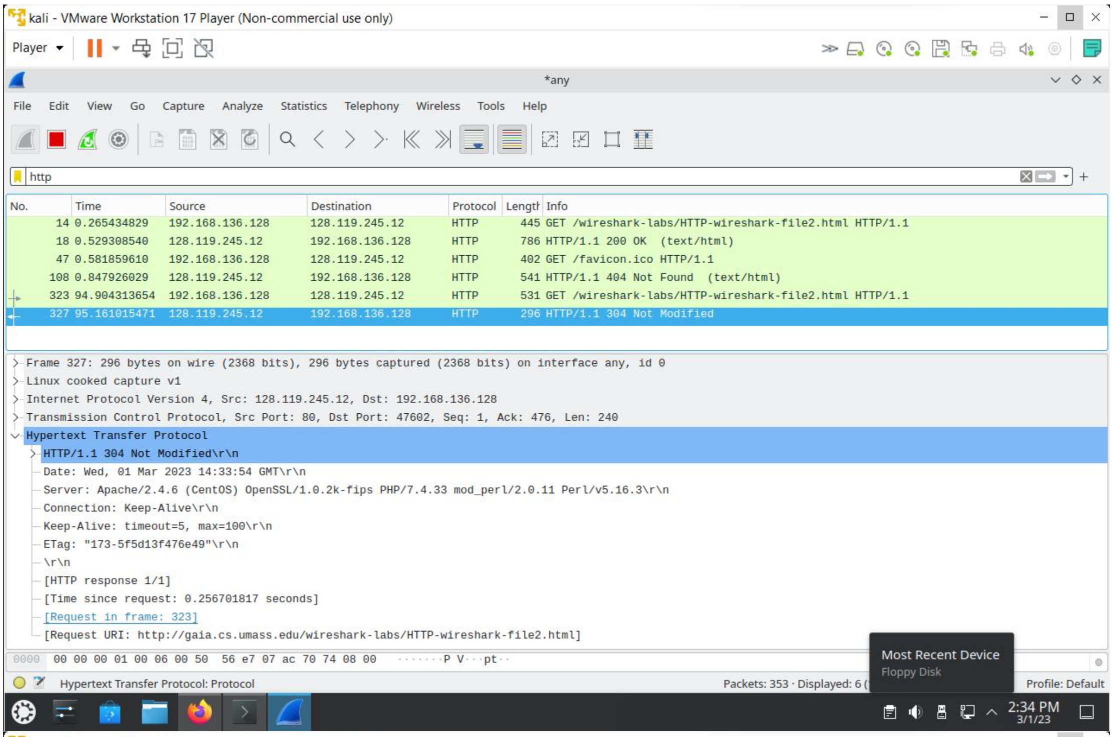
```
> Frame 14: 445 bytes on wire (3560 bits), 445 bytes captured (3560 bits) on interface any, id 0
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 192.168.136.128, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 35358, Dst Port: 80, Seq: 1, Ack: 1, Len: 389
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:106.0) Gecko/20100101 Firefox/106.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/1]
```

```
0000  00 04 00 01 00 06 00 0c  29 17 0e 12 00 00 08 00   ········ )·······
```

Hypertext Transfer Protocol: Protocol

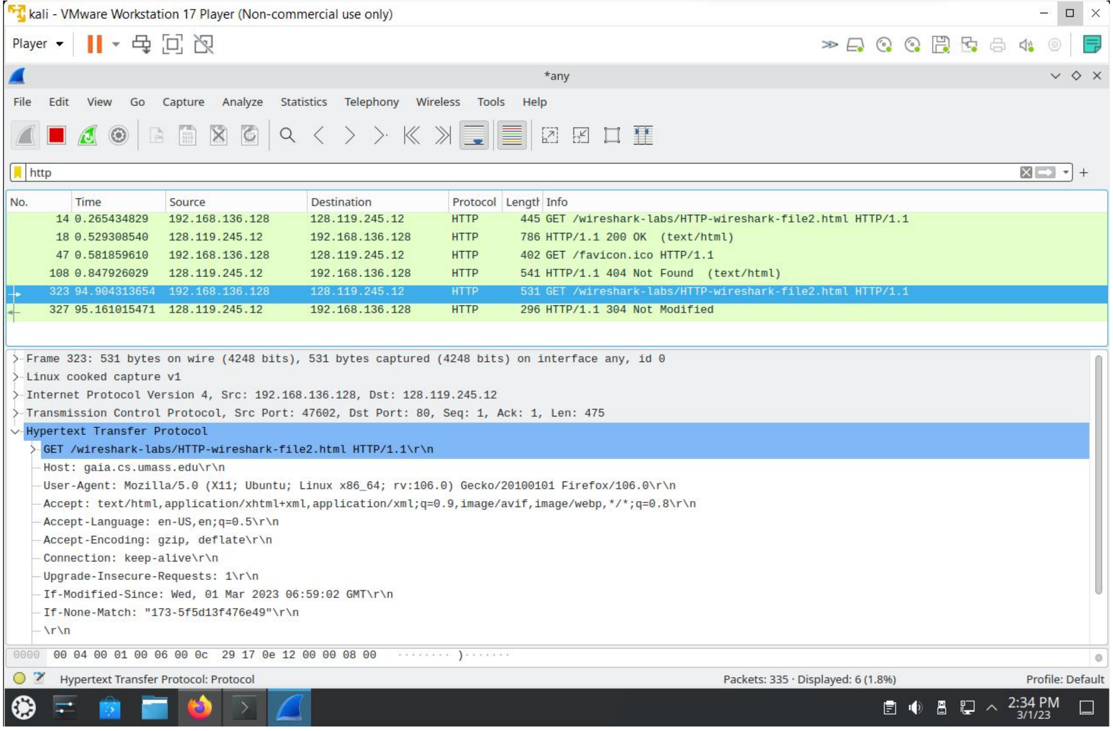
Packets: 286 · Displayed: 4 (1.4%)

ault


kali - VMware Workstation 17 Player (Non-commercial use only)
Player
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Most Recent Device
Floppy Disk
2:34 PM
3/1/23

```
No.   Time          Source           Destination      Protocol Length Info
   14 0.265434829   192.168.136.128  128.119.245.12   HTTP      445 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   18 0.529308540   128.119.245.12   192.168.136.128  HTTP      786 HTTP/1.1 200 OK  (text/html)
   47 0.581859610   192.168.136.128  128.119.245.12   HTTP      402 GET /favicon.ico HTTP/1.1
  108 0.847926029   128.119.245.12   192.168.136.128  HTTP      541 HTTP/1.1 404 Not Found  (text/html)
  323 94.904313654  192.168.136.128  128.119.245.12   HTTP      531 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  327 95.161015471  128.119.245.12   192.168.136.128  HTTP      296 HTTP/1.1 304 Not Modified
```

```
> Frame 327: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits) on interface any, id 0
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.136.128
> Transmission Control Protocol, Src Port: 80, Dst Port: 47602, Seq: 1, Ack: 476, Len: 240
v Hypertext Transfer Protocol
  > HTTP/1.1 304 Not Modified\r\n
    Date: Wed, 01 Mar 2023 14:33:54 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "173-5f5d13f476e49"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.256701817 seconds]
    [Request in frame: 323]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
0000  00 00 00 01 00 06 00 50  56 e7 07 ac 70 74 08 00   ·······P V···pt··
Hypertext Transfer Protocol: Protocol          Packets: 353 · Displayed: 6 (          Profile: Default
```


kali - VMware Workstation 17 Player (Non-commercial use only)
Player
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
2:34 PM
3/1/23

```
No.   Time          Source           Destination      Protocol Length Info
   14 0.265434829   192.168.136.128  128.119.245.12   HTTP      445 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   18 0.529308540   128.119.245.12   192.168.136.128  HTTP      786 HTTP/1.1 200 OK  (text/html)
   47 0.581859610   192.168.136.128  128.119.245.12   HTTP      402 GET /favicon.ico HTTP/1.1
  108 0.847926029   128.119.245.12   192.168.136.128  HTTP      541 HTTP/1.1 404 Not Found  (text/html)
  323 94.904313654  192.168.136.128  128.119.245.12   HTTP      531 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  327 95.161015471  128.119.245.12   192.168.136.128  HTTP      296 HTTP/1.1 304 Not Modified
```

```
> Frame 323: 531 bytes on wire (4248 bits), 531 bytes captured (4248 bits) on interface any, id 0
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 192.168.136.128, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 47602, Dst Port: 80, Seq: 1, Ack: 1, Len: 475
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:106.0) Gecko/20100101 Firefox/106.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    If-Modified-Since: Wed, 01 Mar 2023 06:59:02 GMT\r\n
    If-None-Match: "173-5f5d13f476e49"\r\n
    \r\n
0000  00 04 00 01 00 06 00 0c  29 17 0e 12 00 00 08 00   ········ )·······
Hypertext Transfer Protocol: Protocol          Packets: 335 · Displayed: 6 (1.8%)          Profile: Default
```

As you can see from the figure, the first time page is requested by client, the resourcesare cached by browser. When we made the second GET request, we got a response as **304 Not Modified** indicating that the resource has not been modified since the last GET request made by the client. If the resource had been modified, the server would send the contents to client.