PES UNIVERSITY

EC CAMPUS BANGALORE

NAME: R SHARMILA

SRN: PES2UG19CS309

DATE: 11-02-2021

SUBJECT: Computer Network Laboratory

WEEK: 3

Question: Understand working of HTTP headers Conditional Get: If-Modified-Since HTTP Cookies: Cookie and Set-Cookie Authentication: Auth-Basic Design a web page that has one embedded page (e.g. image) and sets a cookie and enables authentication. You are required to configure the web server (e.g. apache) with authentication mechanism. Show the behavior of conditional get when embedded objects are modified and when it is not (you can just change the create date of the embedded object). Decode the BasicAuth header using Base64 mechanism as per the password setup.

Observation: Show the behavior of browser when is cookie is set and when cookie is removed.

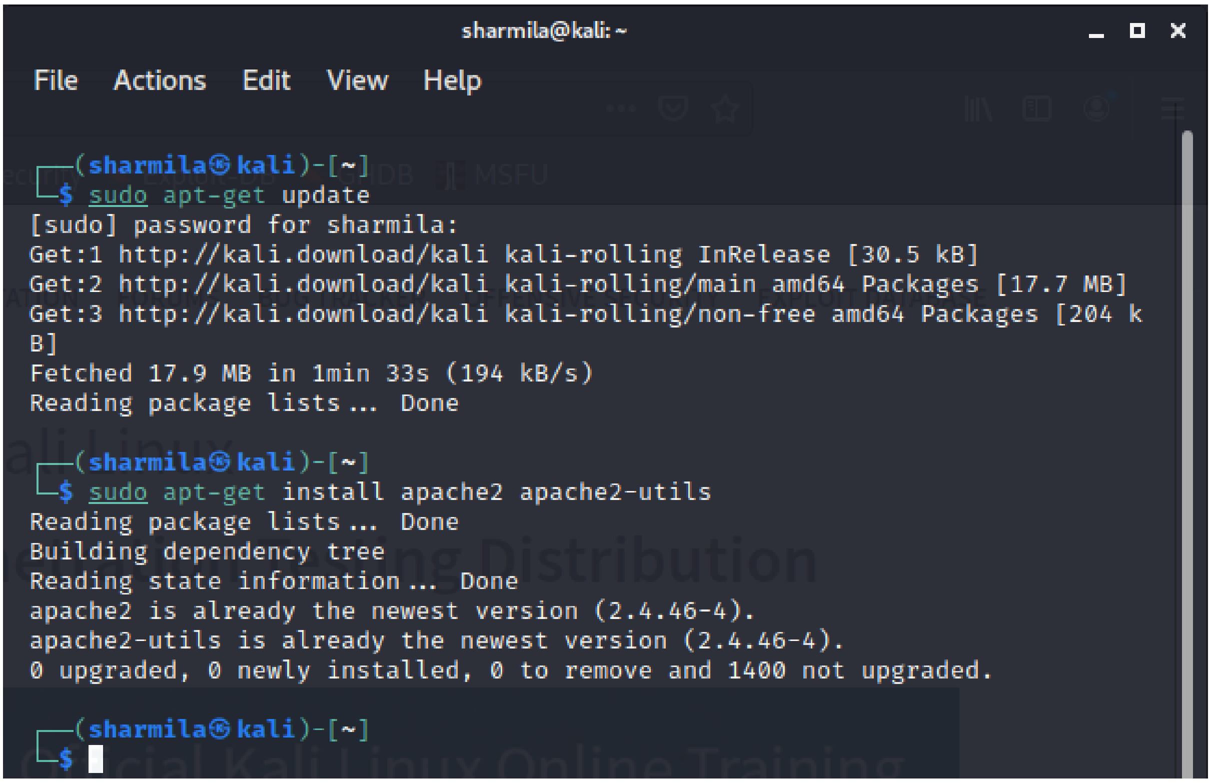
Solution:

1. Password Authentication

1.1 Password Generation

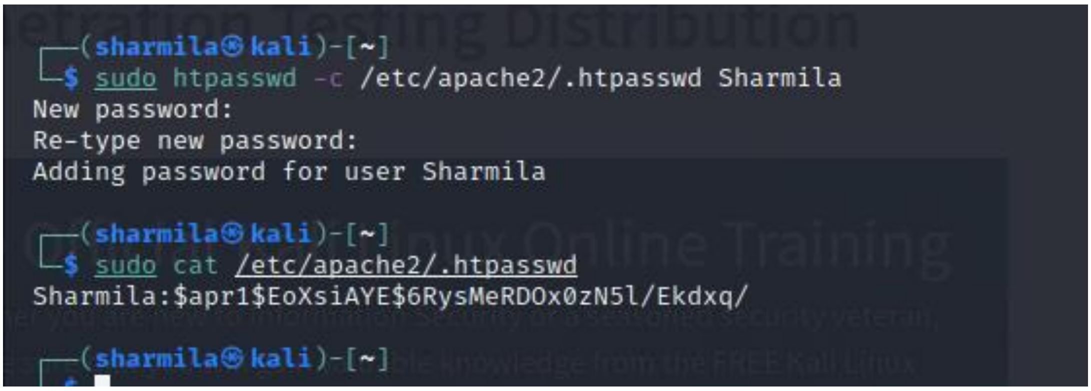
1. Executing the below commands on the terminal.

- *To update and integrate the existing softwares **sudo apt-get update***
- *To install the apache utility **sudo apt-get install apache2 apache2-utils***



```
┌──(sharmila㉿kali)-[~]
└─$ sudo apt-get update
[sudo] password for sharmila:
Get:1 http://kali.download/kali kali-rolling InRelease [30.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [17.7 MB]
Get:3 http://kali.download/kali kali-rolling/non-free amd64 Packages [204 k
B]
Fetched 17.9 MB in 1min 33s (194 kB/s)
Reading package lists... Done

┌──(sharmila㉿kali)-[~]
└─$ sudo apt-get install apache2 apache2-utils
Reading package lists... Done
Building dependency tree
Reading state information... Done
apache2 is already the newest version (2.4.46-4).
apache2-utils is already the newest version (2.4.46-4).
0 upgraded, 0 newly installed, 0 to remove and 1400 not upgraded.

┌──(sharmila㉿kali)-[~]
└─$ █
```

- *Provide username and password to set authentication **sudo htpasswd -c /etc/apache2/.htpasswd ANY_USERNAME***
- *View the authentication **sudo cat /etc/apache2/.htpasswd***

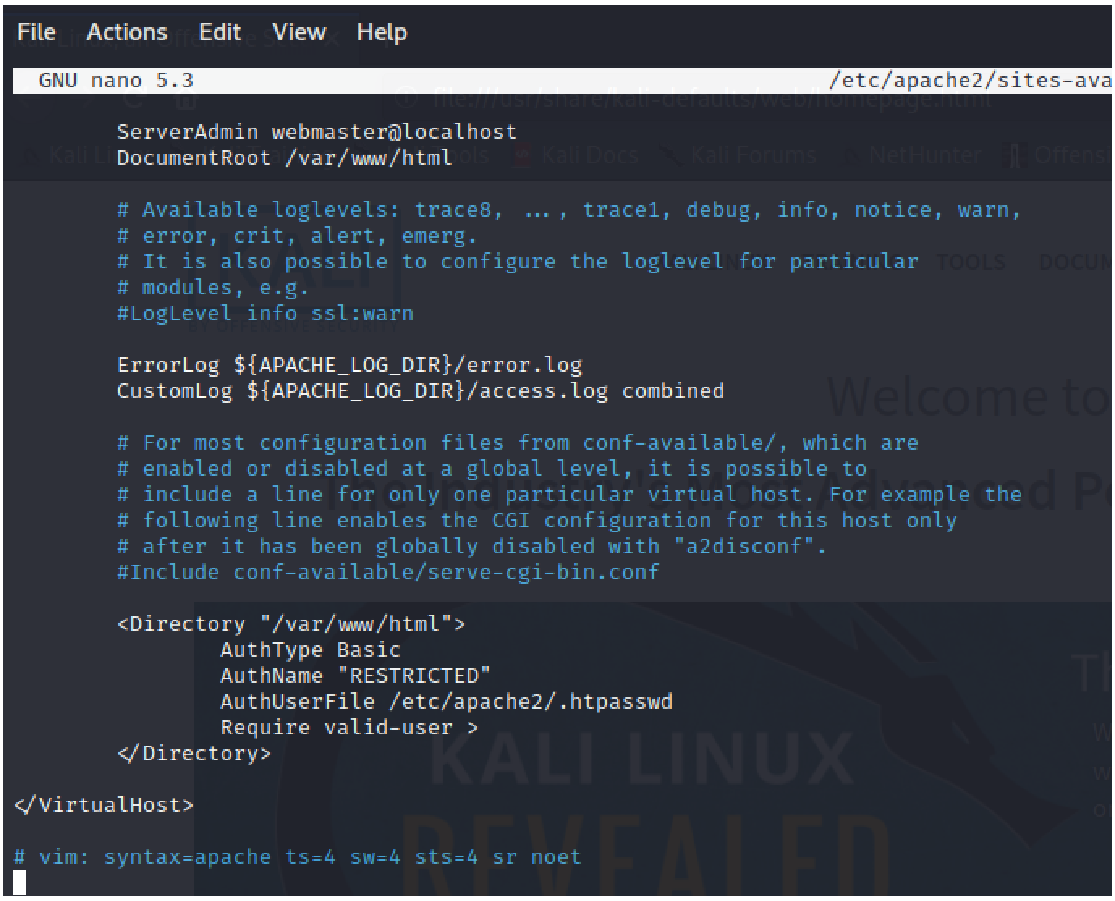


```
┌──(sharmila㉿kali)-[~]
└─$ sudo htpasswd -c /etc/apache2/.htpasswd Sharmila
New password:
Re-type new password:
Adding password for user Sharmila

┌──(sharmila㉿kali)-[~]
└─$ sudo cat /etc/apache2/.htpasswd
Sharmila:$apr1$EoXsiAYE$6RysMeRDOx0zN5l/Ekdxq/

┌──(sharmila㉿kali)-[~]
└─$ █
```

1.2 Apache Server Authentication

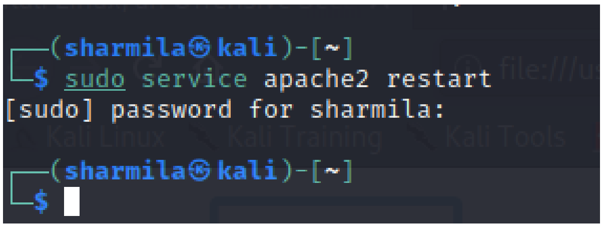
To setup the authentication phase, execute the following commands. Configuring Access control within the Virtual Host Definition.

- *Opening the file for setting authentication **sudo nano /etc/apache2/sites-available/000-default.conf***



```
 GNU nano 5.3                                                /etc/apache2/sites-ava
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf

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

</VirtualHost>

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

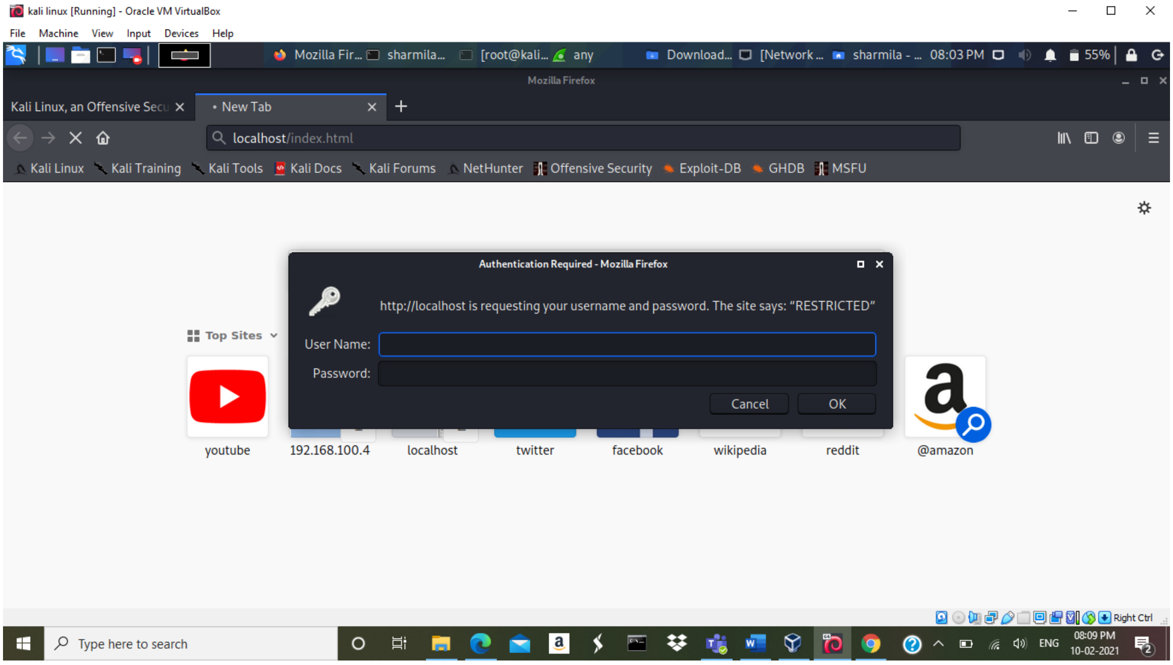
- *Password policy implementation is done by restarting the server as:* ***sudo service apache2 restart***



```
┌──(sharmila㉿kali)-[~]
└─$ sudo service apache2 restart
[sudo] password for sharmila:
┌──(sharmila㉿kali)-[~]
└─$ 
```

1.3 Accessing Localhost

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



localhost/index.html

Authentication Required - Mozilla Firefox

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

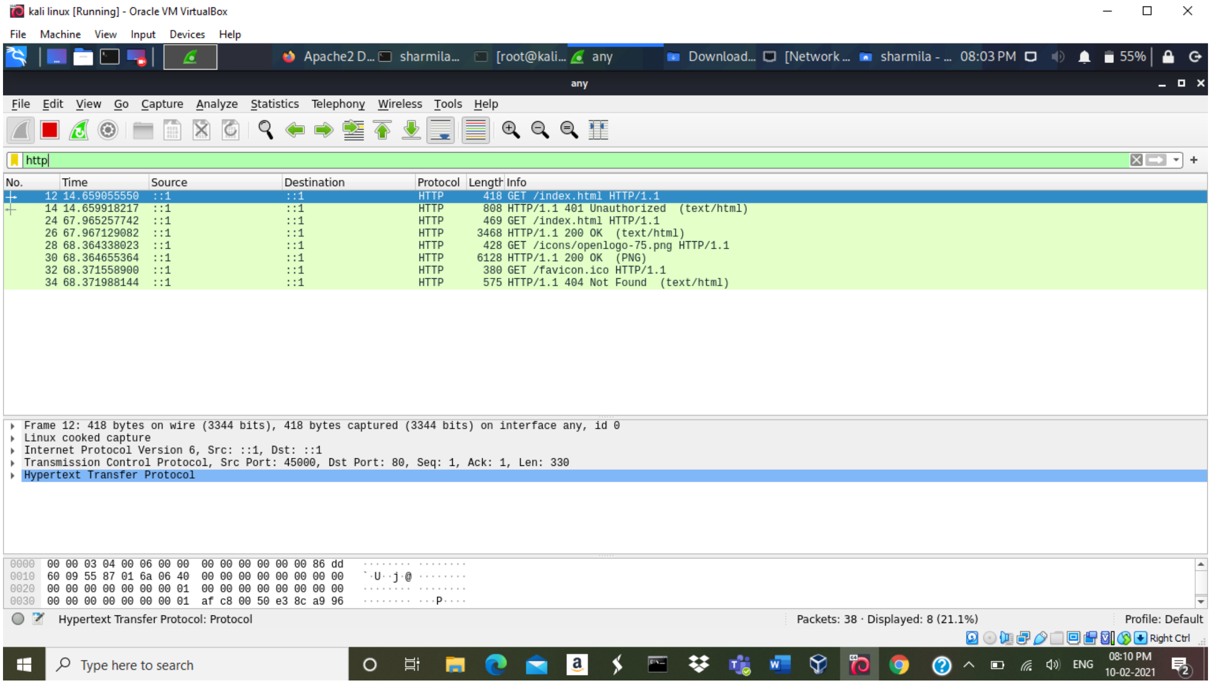
User Name:

Password:

Cancel OK

1.4 Wireshark Packet Capture

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



kali linux [Running] - Oracle VM VirtualBox

Filter: http

```
No.   Time          Source   Destination   Protocol  Length Info
  12 14.659055550   ::1      ::1           HTTP       418 GET /index.html HTTP/1.1
  14 14.659918217   ::1      ::1           HTTP       808 HTTP/1.1 401 Unauthorized  (text/html)
  24 67.965257742   ::1      ::1           HTTP       469 GET /index.html HTTP/1.1
  26 67.967129082   ::1      ::1           HTTP      3468 HTTP/1.1 200 OK  (text/html)
  28 68.364338023   ::1      ::1           HTTP       428 GET /icons/openlogo-75.png HTTP/1.1
  30 68.364655364   ::1      ::1           HTTP      6128 HTTP/1.1 200 OK  (PNG)
  32 68.371558900   ::1      ::1           HTTP       380 GET /favicon.ico HTTP/1.1
  34 68.371988144   ::1      ::1           HTTP       575 HTTP/1.1 404 Not Found  (text/html)
```

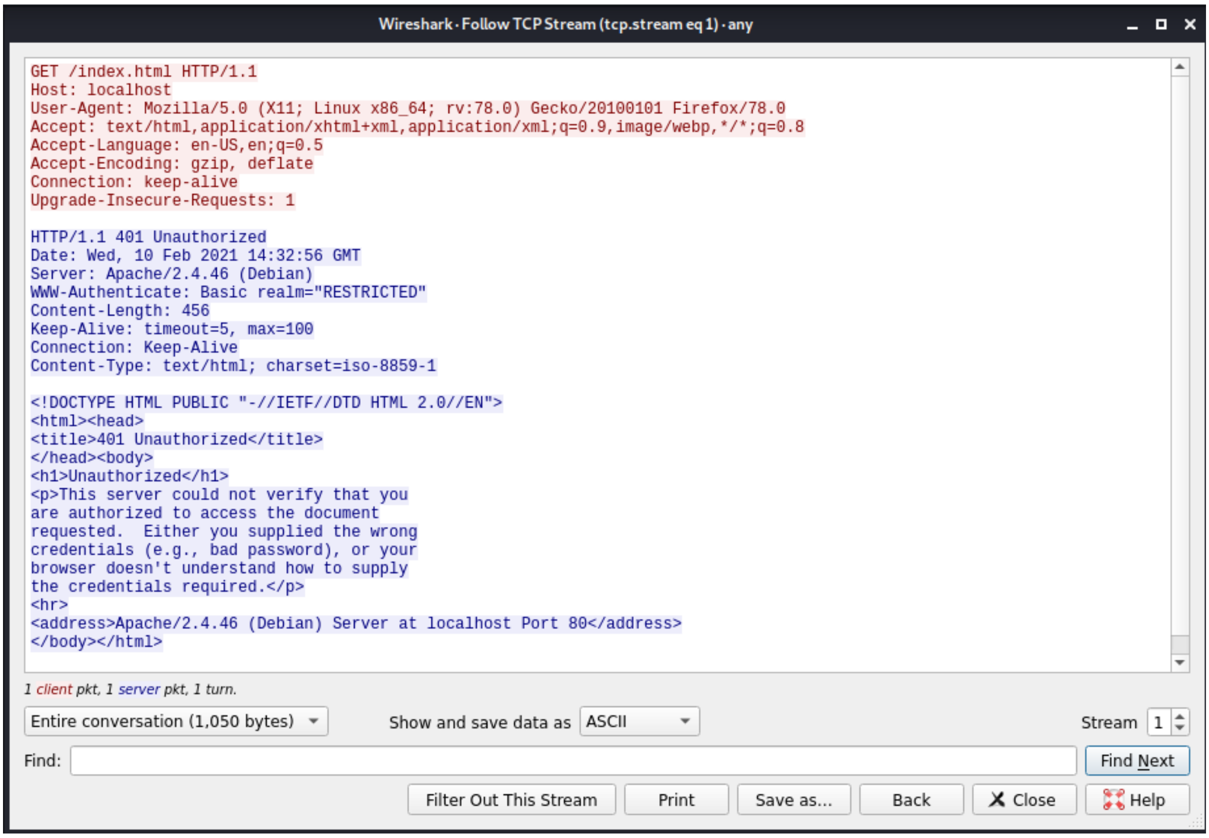
```
Frame 12: 418 bytes on wire (3344 bits), 418 bytes captured (3344 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 6, Src: ::1, Dst: ::1
Transmission Control Protocol, Src Port: 45000, Dst Port: 80, Seq: 1, Ack: 1, Len: 330
Hypertext Transfer Protocol
```

```
0000  00 00 03 04 00 06 00 00  00 00 00 00 00 00 86 dd   ········ ········
0010  60 09 55 87 01 6a 06 40  00 00 00 00 00 00 00 00   `·U··j·@ ········
0020  00 00 00 00 00 00 00 01  00 00 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 00 00 01  af c8 00 50 e3 8c a9 96   ········ ···P····
```

Hypertext Transfer Protocol: Protocol — Packets: 38 · Displayed: 8 (21.1%) — Profile: Default

File Machine View Input Devices Help
Apache2 D... sharmila... [root@kali... any Download... [Network... sharmila - ... 08:03 PM 55%
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Right Ctrl
Type here to search
ENG 08:10 PM 10-02-2021

- *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.*



Wireshark · Follow TCP Stream (tcp.stream eq 1) · any

```
GET /index.html HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
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/1.1 401 Unauthorized
Date: Wed, 10 Feb 2021 14:32:56 GMT
Server: Apache/2.4.46 (Debian)
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/2.4.46 (Debian) Server at localhost Port 80</address>
</body></html>
```

1 client pkt, 1 server pkt, 1 turn.

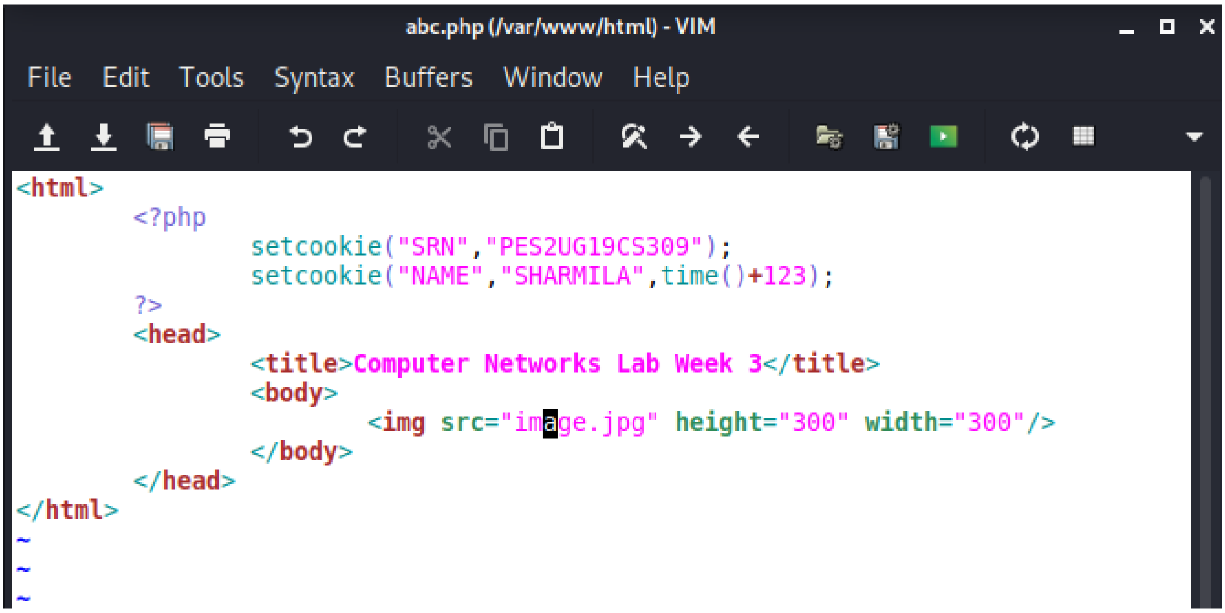
Entire conversation (1,050 bytes) — Show and save data as: ASCII — Stream: 1

Find:

2. Setting Cookies

2.1 Steps of Execution (Cookie Setting)

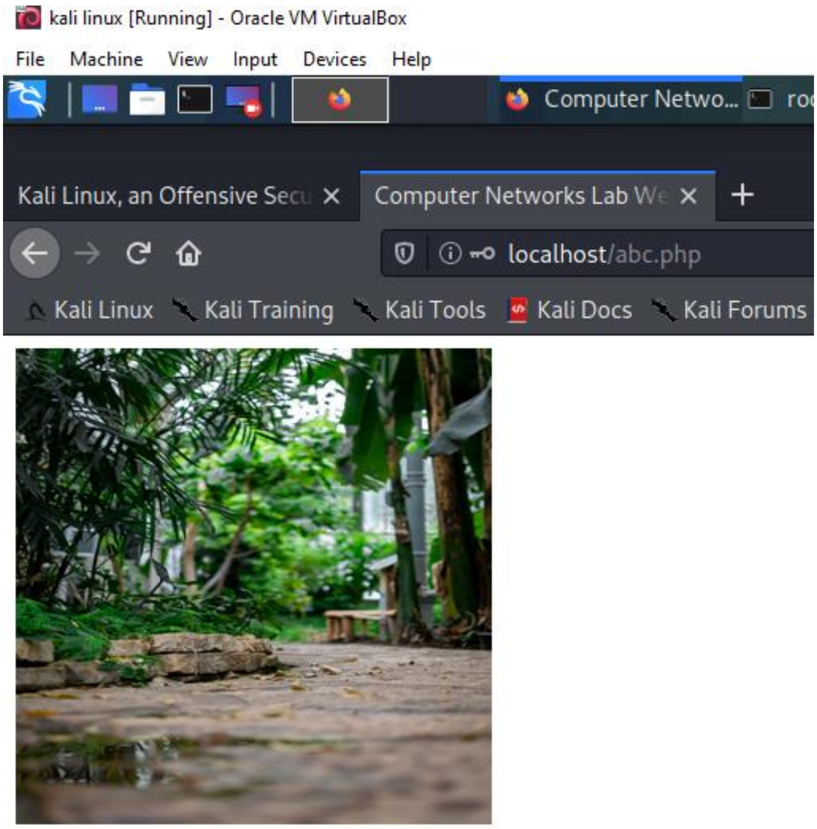
A PHP file to set the cookie is created which also contains an image in it (placed under the HTML directory) to be accessed once the cookie is set.



abc.php (/var/www/html) - VIM
File Edit Tools Syntax Buffers Window Help

```
<html>
        <?php
                setcookie("SRN","PES2UG19CS309");
                setcookie("NAME","SHARMILA",time()+123);
        ?>
        <head>
                <title>Computer Networks Lab Week 3</title>
                <body>
                        <img src="image.jpg" height="300" width="300"/>
                </body>
        </head>
</html>
~
~
~
```

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

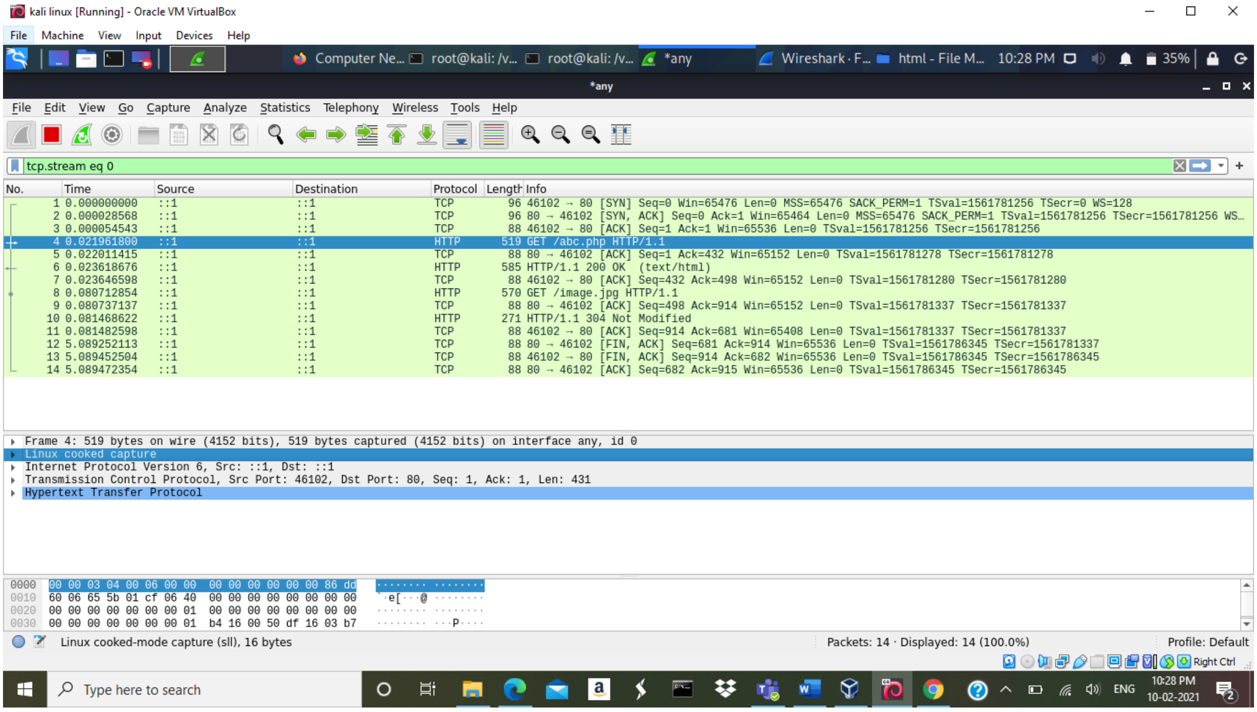


2.2 Wireshark Capture

- *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*


kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Computer Ne... root@kali: /v... root@kali: /v... *any Wireshark · F... html - File M... 10:28 PM 35%
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Type here to search
ENG 10:28 PM 10-02-2021
Right Ctrl

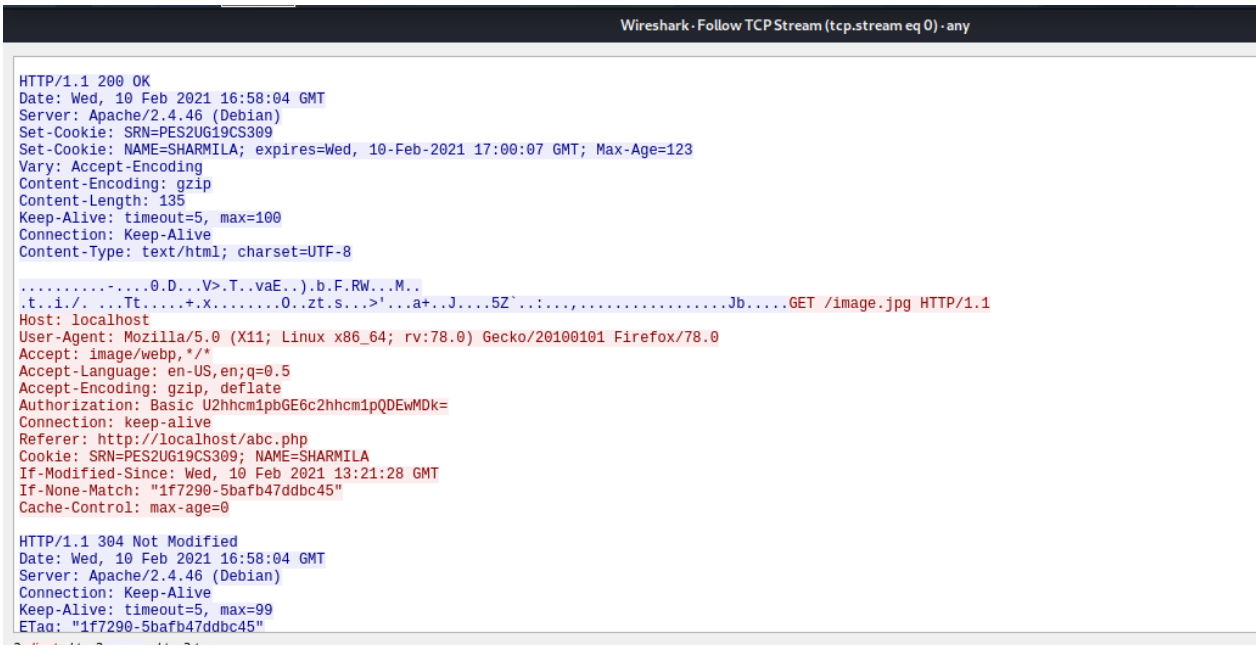
tcp.stream eq 0

```
No.  Time         Source  Destination  Protocol Length Info
   1 0.000000000  ::1     ::1          TCP       96 46102 → 80 [SYN] Seq=0 Win=65476 Len=0 MSS=65476 SACK_PERM=1 TSval=1561781256 TSecr=0 WS=128
   2 0.000028568  ::1     ::1          TCP       96 80 → 46102 [SYN, ACK] Seq=0 Ack=1 Win=65464 Len=0 MSS=65476 SACK_PERM=1 TSval=1561781256 TSecr=1561781256 WS…
   3 0.000054543  ::1     ::1          TCP       88 46102 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1561781256 TSecr=1561781256
   4 0.021961800  ::1     ::1          HTTP     519 GET /abc.php HTTP/1.1
   5 0.022011415  ::1     ::1          TCP       88 80 → 46102 [ACK] Seq=1 Ack=432 Win=65152 Len=0 TSval=1561781278 TSecr=1561781278
   6 0.023618676  ::1     ::1          HTTP     585 HTTP/1.1 200 OK  (text/html)
   7 0.023646598  ::1     ::1          TCP       88 46102 → 80 [ACK] Seq=432 Ack=498 Win=65152 Len=0 TSval=1561781280 TSecr=1561781280
   8 0.080712854  ::1     ::1          HTTP     570 GET /image.jpg HTTP/1.1
   9 0.080737137  ::1     ::1          TCP       88 80 → 46102 [ACK] Seq=498 Ack=914 Win=65152 Len=0 TSval=1561781337 TSecr=1561781337
  10 0.081468622  ::1     ::1          HTTP     271 HTTP/1.1 304 Not Modified
  11 0.081482598  ::1     ::1          TCP       88 46102 → 80 [ACK] Seq=914 Ack=681 Win=65408 Len=0 TSval=1561781337 TSecr=1561781337
  12 5.089252113  ::1     ::1          TCP       88 80 → 46102 [FIN, ACK] Seq=681 Ack=914 Win=65536 Len=0 TSval=1561786345 TSecr=1561781337
  13 5.089452504  ::1     ::1          TCP       88 46102 → 80 [FIN, ACK] Seq=914 Ack=682 Win=65536 Len=0 TSval=1561786345 TSecr=1561786345
  14 5.089472354  ::1     ::1          TCP       88 80 → 46102 [ACK] Seq=682 Ack=915 Win=65536 Len=0 TSval=1561786345 TSecr=1561786345
```

```
▸ Frame 4: 519 bytes on wire (4152 bits), 519 bytes captured (4152 bits) on interface any, id 0
▸ Linux cooked capture
▸ Internet Protocol Version 6, Src: ::1, Dst: ::1
▸ Transmission Control Protocol, Src Port: 46102, Dst Port: 80, Seq: 1, Ack: 1, Len: 431
▸ Hypertext Transfer Protocol
```

```
0000  00 00 03 04 00 06 00 00  00 00 00 00 00 00 86 dd   ········ ········
0010  60 06 65 5b 01 cf 06 40  00 00 00 00 00 00 00 00   `·e[···@ ········
0020  00 00 00 00 00 00 00 01  00 00 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 00 00 01  b4 16 00 50 df 16 03 b7   ········ ···P····
```

Linux cooked-mode capture (sll), 16 bytes   Packets: 14 · Displayed: 14 (100.0%)   Profile: Default



```
HTTP/1.1 200 OK
Date: Wed, 10 Feb 2021 16:58:04 GMT
Server: Apache/2.4.46 (Debian)
Set-Cookie: SRN=PES2UG19CS309
Set-Cookie: NAME=SHARMILA; expires=Wed, 10-Feb-2021 17:00:07 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

..........-....0.D...V>.T..vaE..).b.F.RW...M..
.t..i./. ...Tt.....+.x........O..zt.s...>'...a+..J....5Z`..:...,................Jb.....GET /image.jpg HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Basic U2hhcm1pbGE6c2hhcm1pQDEwMDk=
Connection: keep-alive
Referer: http://localhost/abc.php
Cookie: SRN=PES2UG19CS309; NAME=SHARMILA
If-Modified-Since: Wed, 10 Feb 2021 13:21:28 GMT
If-None-Match: "1f7290-5bafb47ddbc45"
Cache-Control: max-age=0

HTTP/1.1 304 Not Modified
Date: Wed, 10 Feb 2021 16:58:04 GMT
Server: Apache/2.4.46 (Debian)
Connection: Keep-Alive
Keep-Alive: timeout=5, max=99
ETag: "1f7290-5bafb47ddbc45"
```

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

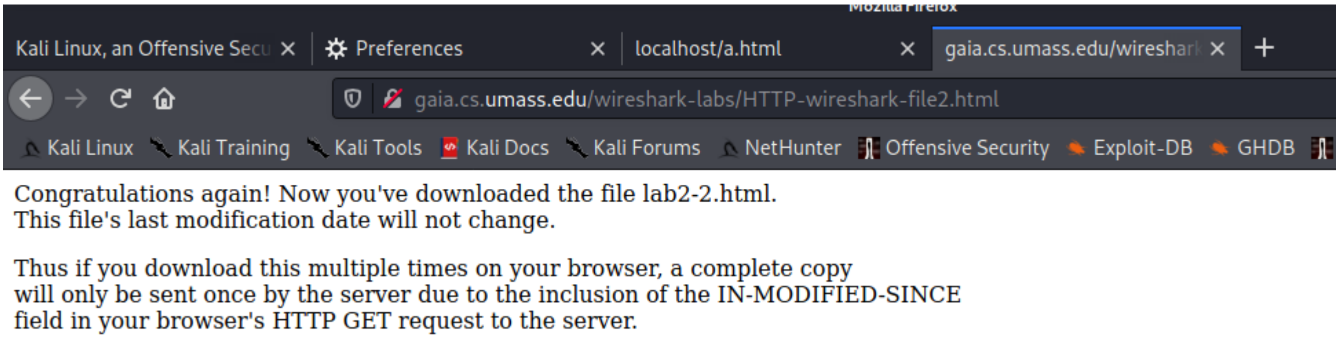
• If it has not been modified, a 304 Not Modified status code is sent back.

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

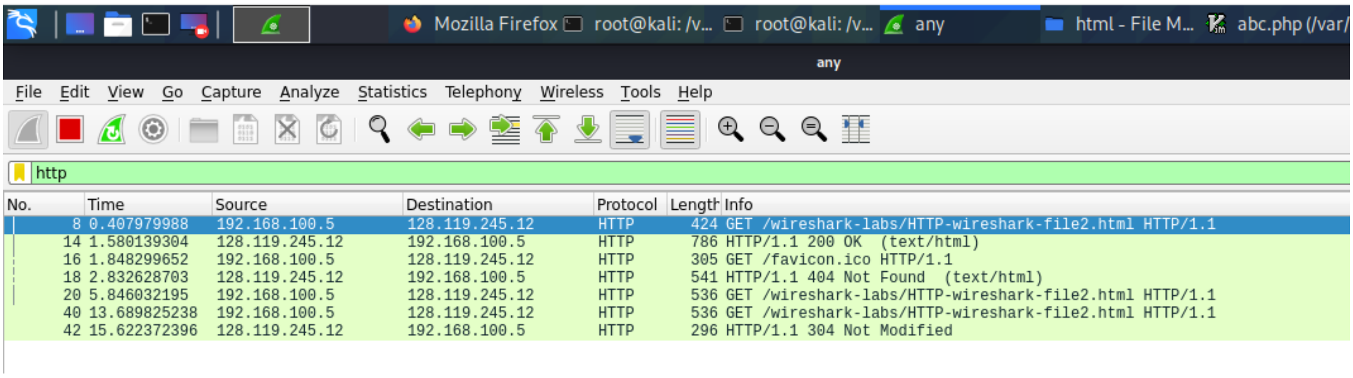
• Immediately, the request is made again either by refreshing or accessing it via a browser tab

• The second response from the server is obtained as 304 Not Modified since the resource has not been modified since the last GET.



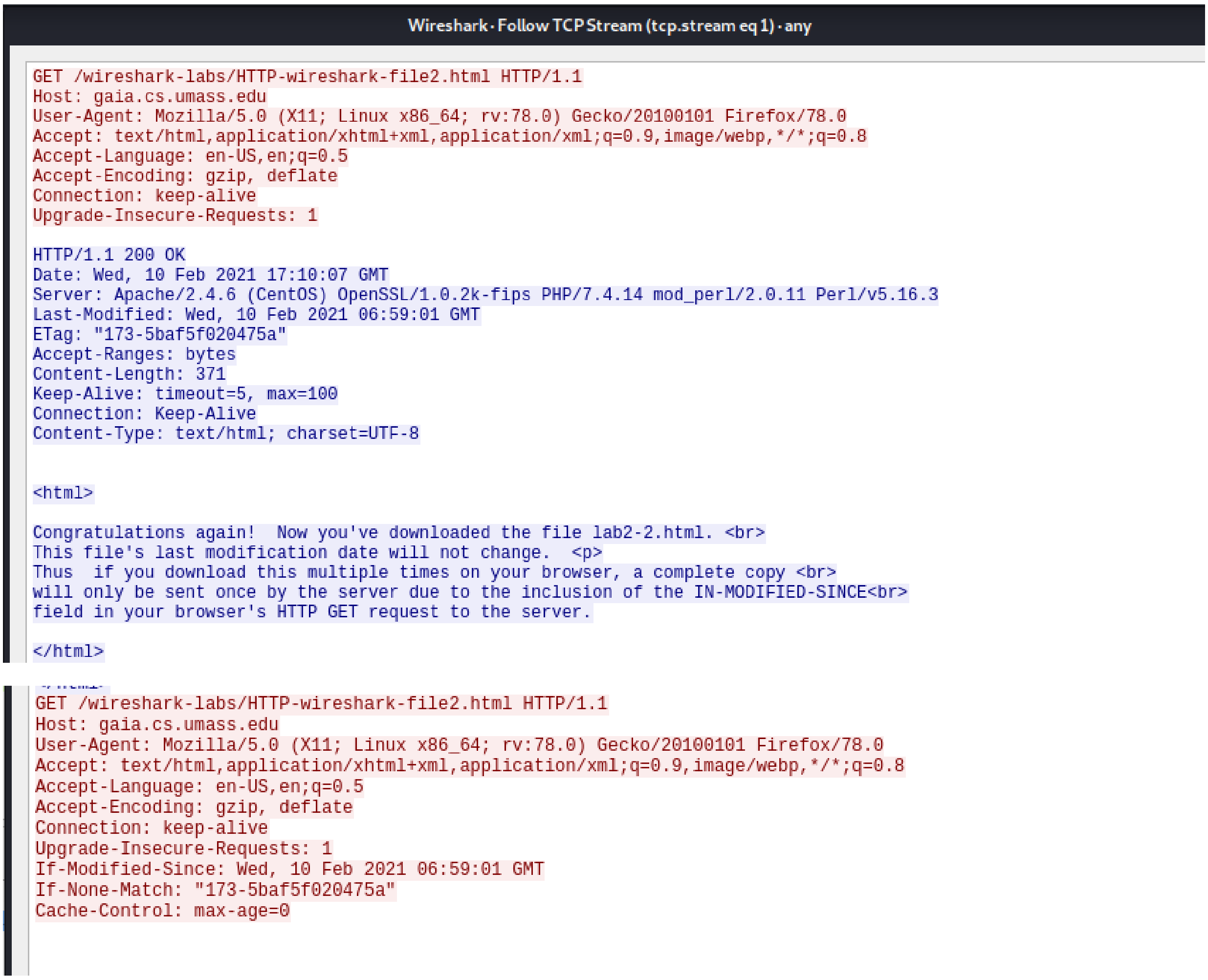
Congratulations again! Now you've downloaded the file lab2-2.html.
This file's last modification date will not change.

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 Length Info
     8 0.407979988   192.168.100.5    128.119.245.12   HTTP      424 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
    14 1.580139304   128.119.245.12   192.168.100.5    HTTP      786 HTTP/1.1 200 OK  (text/html)
    16 1.848299652   192.168.100.5    128.119.245.12   HTTP      305 GET /favicon.ico HTTP/1.1
    18 2.832628703   128.119.245.12   192.168.100.5    HTTP      541 HTTP/1.1 404 Not Found  (text/html)
    20 5.846032195   192.168.100.5    128.119.245.12   HTTP      536 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
    40 13.689825238  192.168.100.5    128.119.245.12   HTTP      536 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
    42 15.622372396  128.119.245.12   192.168.100.5    HTTP      296 HTTP/1.1 304 Not Modified
```

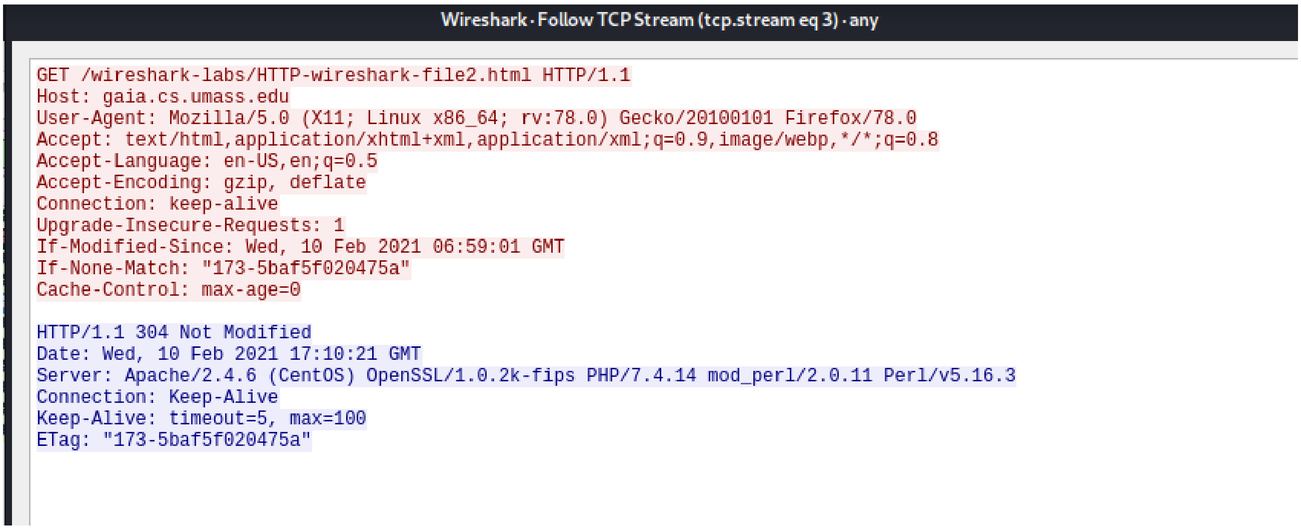


Wireshark · Follow TCP Stream (tcp.stream eq 1) · any

```
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Host: gaia.cs.umass.edu
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
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 17:10:07 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.

</html>
```

```
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Host: gaia.cs.umass.edu
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
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
```

First Request from Server – 200 OK



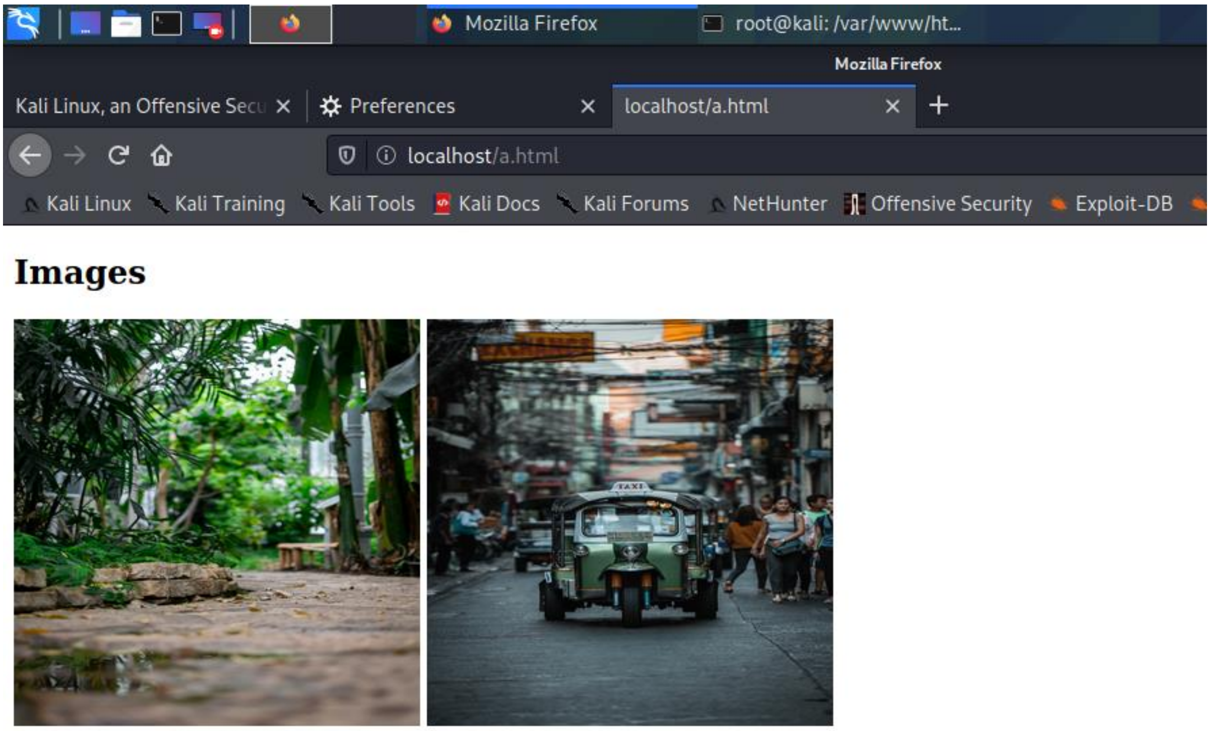
Wireshark · Follow TCP Stream (tcp.stream eq 3) · any

```
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Host: gaia.cs.umass.edu
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
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 17:10:21 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"
```

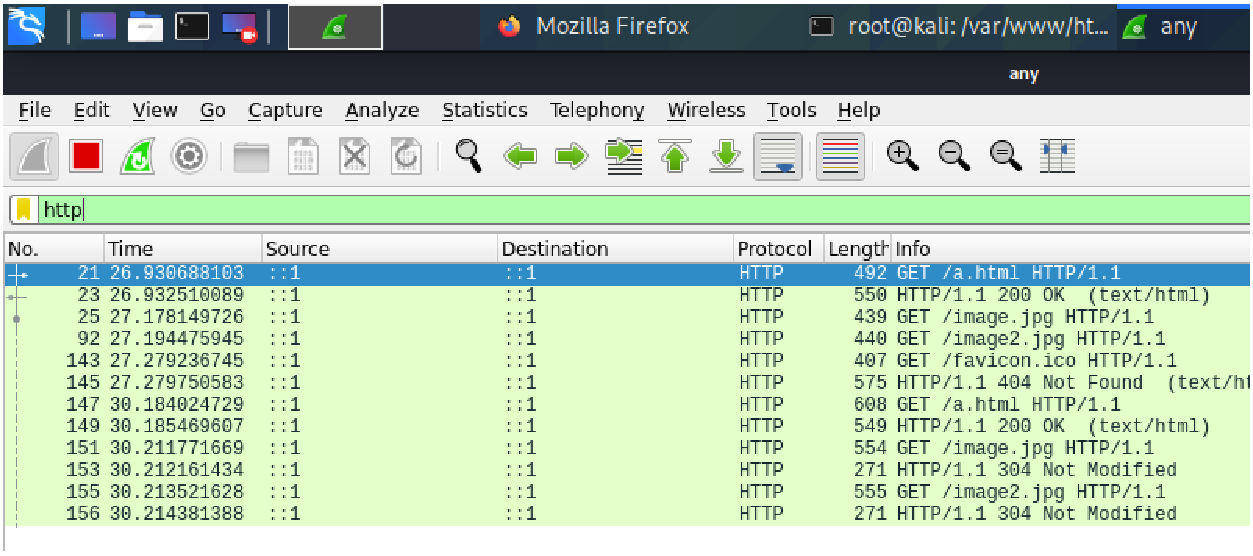
Second Request from Server – 304 Not Modified

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.*

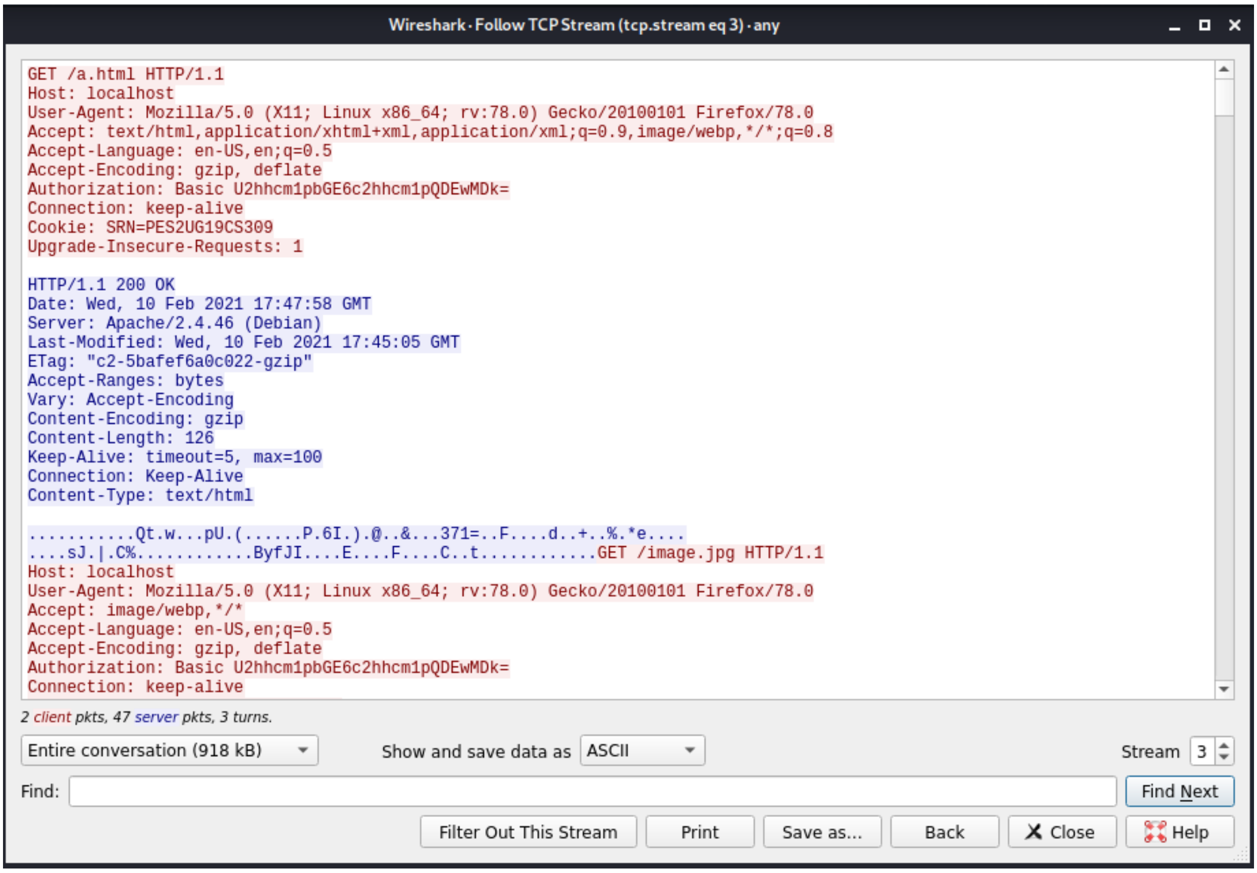


Images



http

```
No.    Time          Source    Destination   Protocol  Length Info
    21 26.930688103  ::1       ::1           HTTP       492 GET /a.html HTTP/1.1
    23 26.932510089  ::1       ::1           HTTP       550 HTTP/1.1 200 OK  (text/html)
    25 27.178149726  ::1       ::1           HTTP       439 GET /image.jpg HTTP/1.1
    92 27.194475945  ::1       ::1           HTTP       440 GET /image2.jpg HTTP/1.1
   143 27.279236745  ::1       ::1           HTTP       407 GET /favicon.ico HTTP/1.1
   145 27.279750583  ::1       ::1           HTTP       575 HTTP/1.1 404 Not Found  (text/ht
   147 30.184024729  ::1       ::1           HTTP       608 GET /a.html HTTP/1.1
   149 30.185469607  ::1       ::1           HTTP       549 HTTP/1.1 200 OK  (text/html)
   151 30.211771669  ::1       ::1           HTTP       554 GET /image.jpg HTTP/1.1
   153 30.212161434  ::1       ::1           HTTP       271 HTTP/1.1 304 Not Modified
   155 30.213521628  ::1       ::1           HTTP       555 GET /image2.jpg HTTP/1.1
   156 30.214381388  ::1       ::1           HTTP       271 HTTP/1.1 304 Not Modified
```



Wireshark · Follow TCP Stream (tcp.stream eq 3) · any

```
GET /a.html HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Basic U2hhcm1pbGE6c2hhcm1pQDEwMDk=
Connection: keep-alive
Cookie: SRN=PES2UG19CS309
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Wed, 10 Feb 2021 17:47:58 GMT
Server: Apache/2.4.46 (Debian)
Last-Modified: Wed, 10 Feb 2021 17:45:05 GMT
ETag: "c2-5bafef6a0c022-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 126
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

...........Qt.w...pU.(......P.6I.).@..&...371=..F....d..+..%.*e....
....sJ.|.C%............ByfJI....E....F....C..t............GET /image.jpg HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Basic U2hhcm1pbGE6c2hhcm1pQDEwMDk=
Connection: keep-alive
```

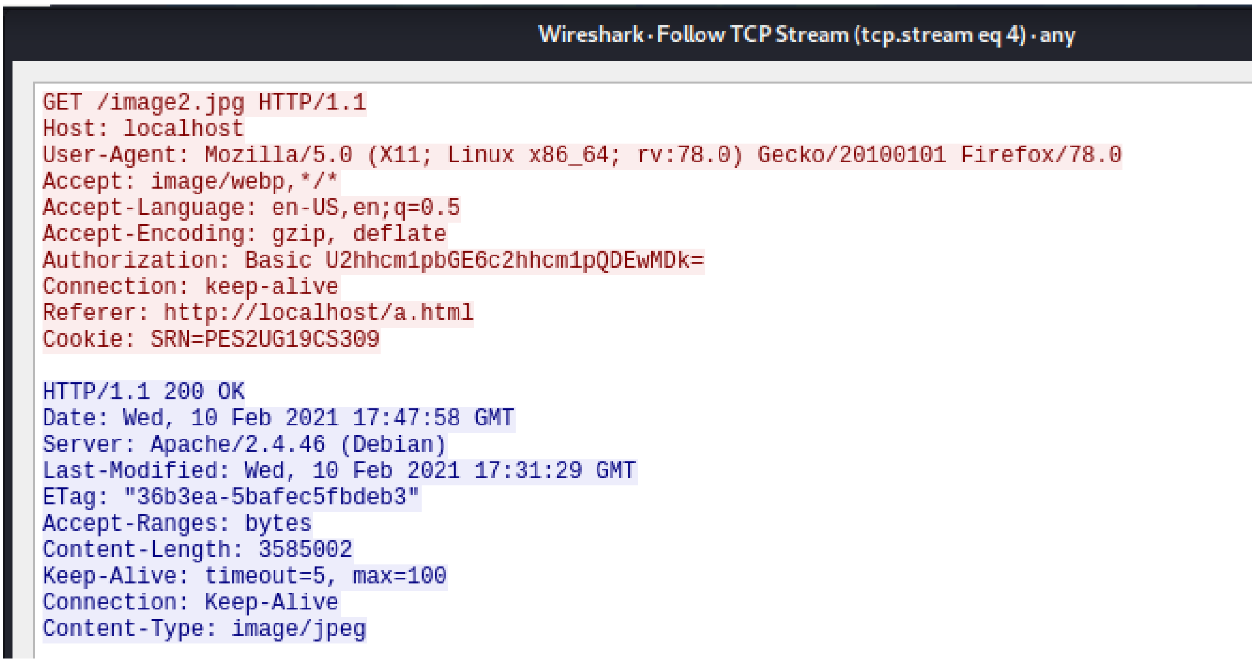
2 client pkts, 47 server pkts, 3 turns.

Entire conversation (918 kB)

Show and save data as ASCII

Stream 3

Find:



Wireshark · Follow TCP Stream (tcp.stream eq 4) · any

```
GET /image2.jpg HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Basic U2hhcm1pbGE6c2hhcm1pQDEwMDk=
Connection: keep-alive
Referer: http://localhost/a.html
Cookie: SRN=PES2UG19CS309

HTTP/1.1 200 OK
Date: Wed, 10 Feb 2021 17:47:58 GMT
Server: Apache/2.4.46 (Debian)
Last-Modified: Wed, 10 Feb 2021 17:31:29 GMT
ETag: "36b3ea-5bafec5fbdeb3"
Accept-Ranges: bytes
Content-Length: 3585002
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: image/jpeg
```

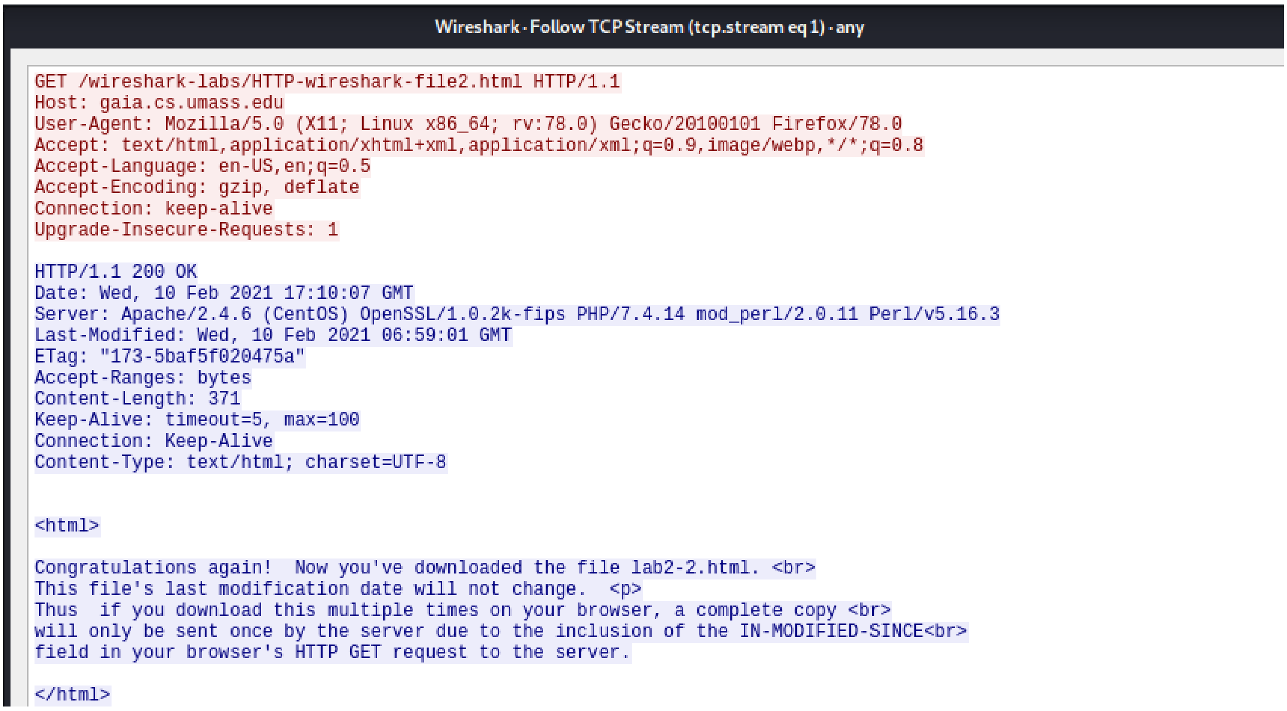
3.3 OBSERVATIONS

1 : Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?

No, in the first request after clearing the cache we don't see in "IF-MODIFIED-SINCE" line in the HTTP GET.

2 :Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Yes, we can see from the screenshot below

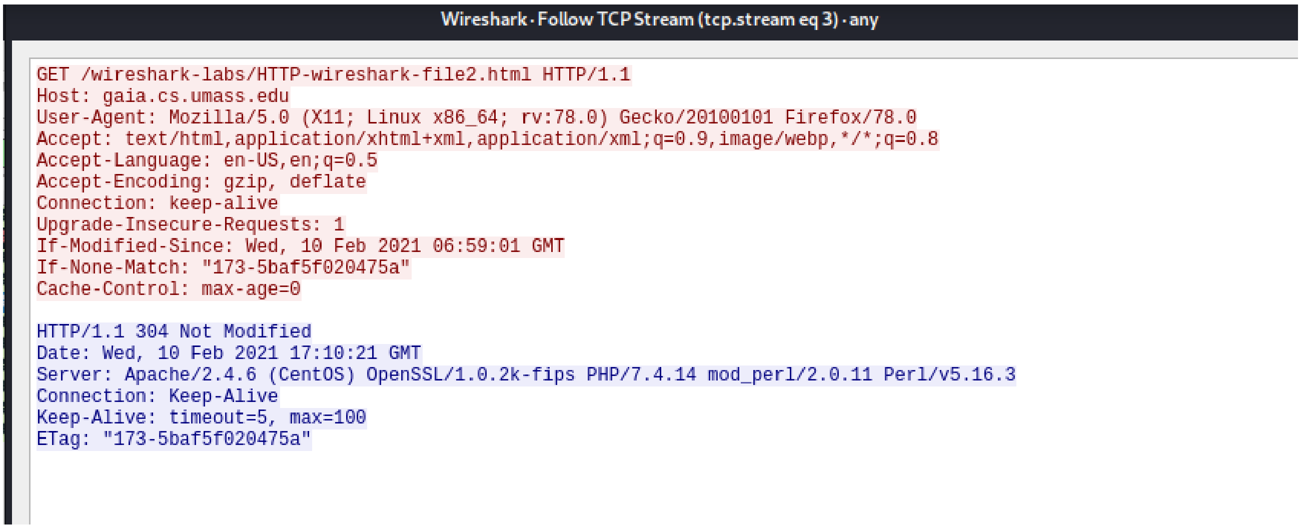


Wireshark · Follow TCP Stream (tcp.stream eq 1) · any

```
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Host: gaia.cs.umass.edu
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
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 17:10:07 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.

</html>
```

3: Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET? If so, what information follows the "IFMODIFIED-SINCE:" header?

IF-MODIFIED-SINCE: date is mentioned

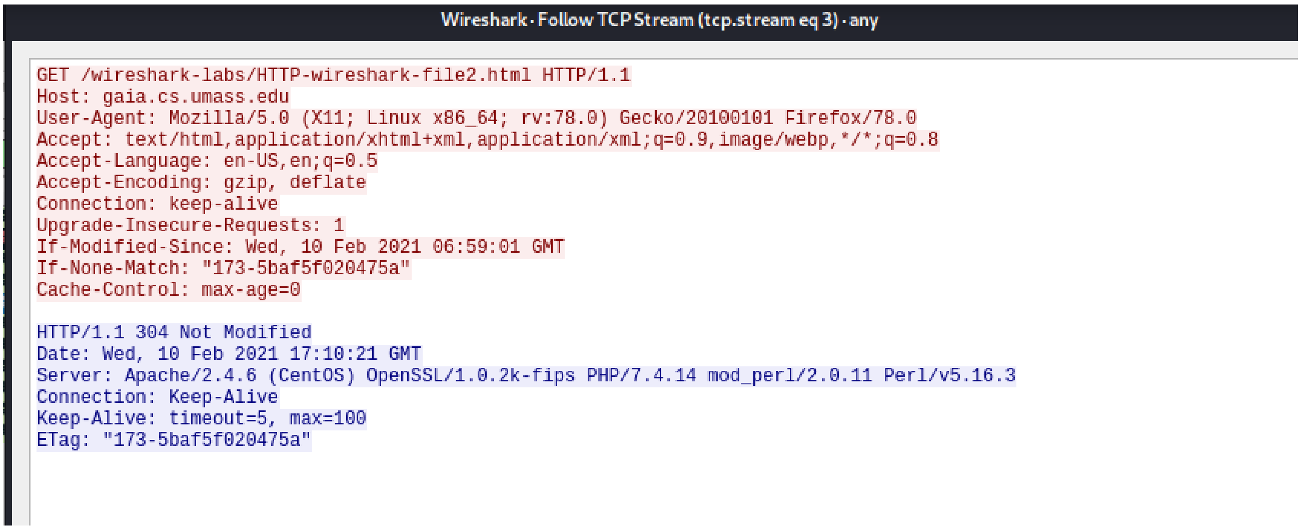


Wireshark · Follow TCP Stream (tcp.stream eq 3) · any

```
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Host: gaia.cs.umass.edu
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
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 17:10:21 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"
```

4 : What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

The HTTP CODE that was returned from the server in response to the second HTTP GET was 304 Not Modified. No, the server didn't return the contents of the file as it is seen in the screenshot below.



Wireshark · Follow TCP Stream (tcp.stream eq 3) · any

```
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Host: gaia.cs.umass.edu
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
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 17:10:21 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"
```