

COMPUTER NETWORKS LABORATORY

WEEK #3

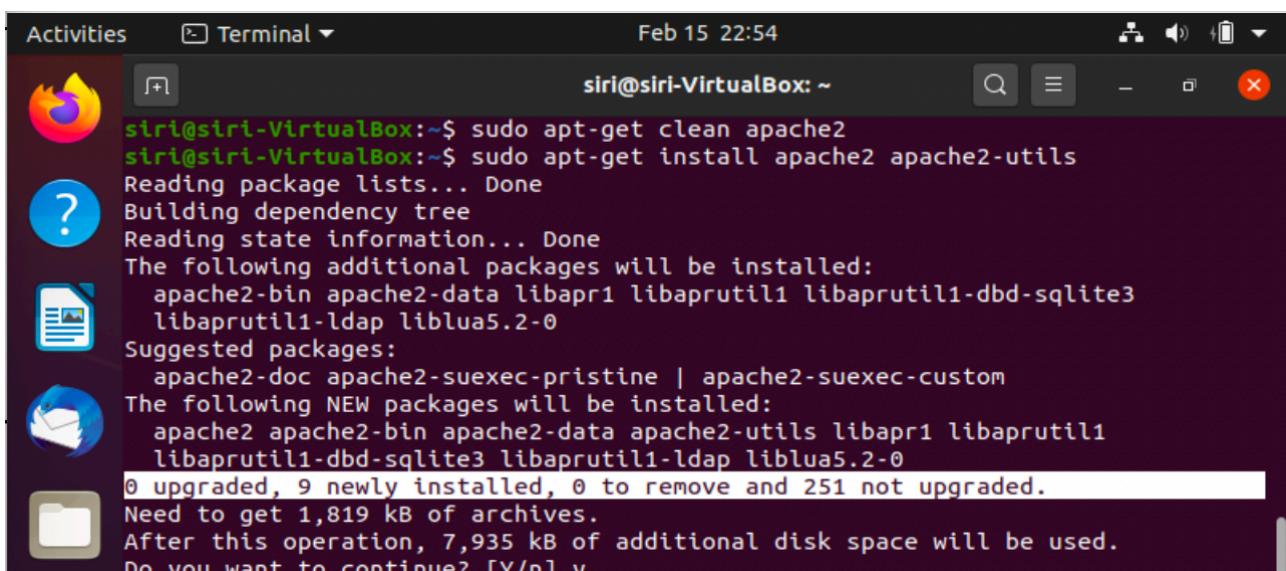
NAME : SIRI S

SEMESTER : 4

SECTION : H

SRN : PESIUGI9CS485

INSTALLATIONS:



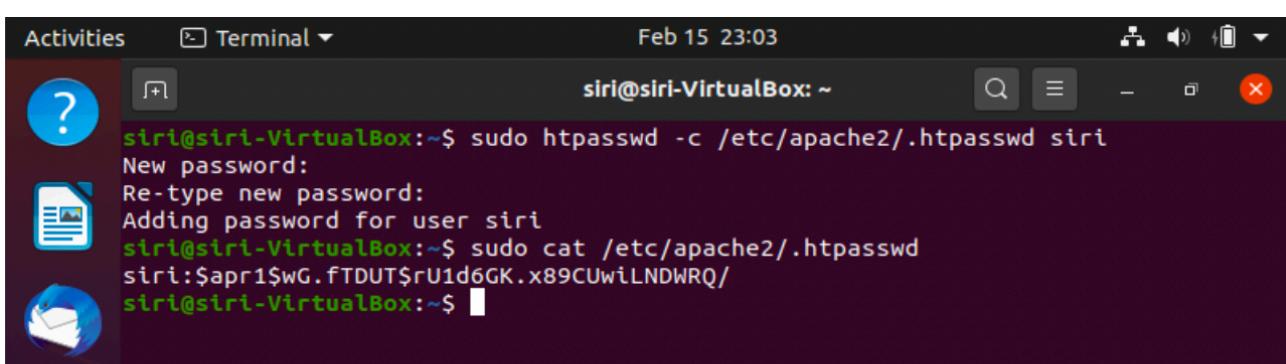
A screenshot of a Linux desktop environment, likely Ubuntu, showing a terminal window. The terminal window title is "Terminal". The date and time at the top right are "Feb 15 22:54". The terminal content shows the user "siri" running commands to install Apache2 and its utilities. The output includes package lists, dependency trees, state information, additional packages to be installed (like apache2-bin, apache2-data, libapr1, libaprutil1, libaprutil1-dbd-sqlite3, libaprutil1-ldap, liblua5.2-0), suggested packages, and newly installed packages. It also shows the user confirming the operation with "y".

```
siri@siri-VirtualBox:~$ sudo apt-get clean apache2
siri@siri-VirtualBox:~$ sudo apt-get install apache2 apache2-utils
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data libapr1 libaprutil1 libaprutil1-dbd-sqlite3
    libaprutil1-ldap liblua5.2-0
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1
    libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.2-0
0 upgraded, 9 newly installed, 0 to remove and 251 not upgraded.
Need to get 1,819 kB of archives.
After this operation, 7,935 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

1. PASSWORD AUTHENTICATION:

PASSWORD GENERATION:

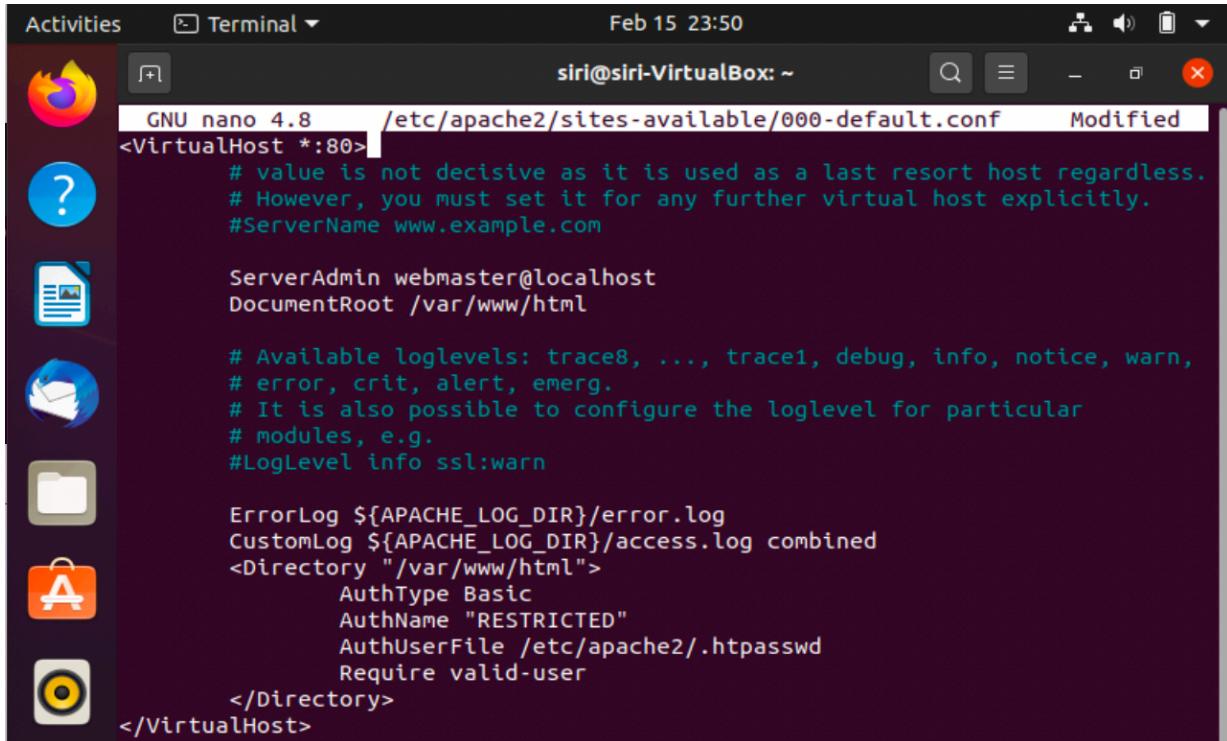
- We are setting a password for the said username.
- The cat command can be used to view the authentication.



A screenshot of a Linux desktop environment, likely Ubuntu, showing a terminal window. The terminal window title is "Terminal". The date and time at the top right are "Feb 15 23:03". The terminal content shows the user "siri" using the "htpasswd" command to add a password for the user "siri". It prompts for a new password and re-type it. Then it uses the "cat" command to view the contents of the ".htpasswd" file, which shows the hashed password for "siri".

```
siri@siri-VirtualBox:~$ sudo htpasswd -c /etc/apache2/.htpasswd siri
New password:
Re-type new password:
Adding password for user siri
siri@siri-VirtualBox:~$ sudo cat /etc/apache2/.htpasswd
siri:$apr1$WG.fTDUT$rU1d6GK.x89CUwiLNDWRQ/
siri@siri-VirtualBox:~$
```

- SERVER AUTHENTICATION SETUP:
- Modifying the Apache configuration file to enable password authentication.
- Password authentication is added to **/var/www/html** directory.
- The server is restarted to activate the authentication.



```

GNU nano 4.8 /etc/apache2/sites-available/000-default.conf Modified
<VirtualHost *:80>
    # 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

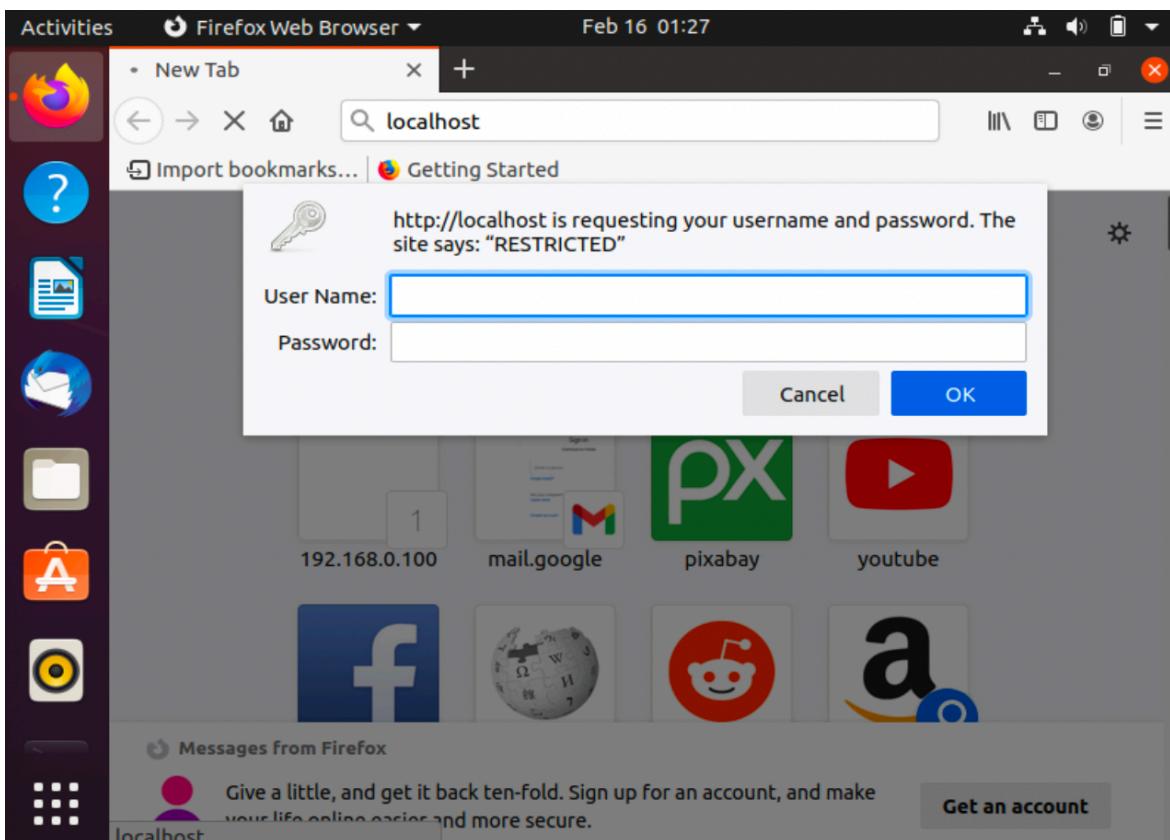
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html

    # 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>
</VirtualHost>

```

- ACCESSING LOCALHOST:
- Local host can be accessed only by entering username and password set in previous steps.



- WIRESHARK PACKET CAPTURE:

Wireshark is used to capture packets sent on the network. The first GET request which corresponds to the HTML file is analysed and its TCP Stream is expanded and parameters explained.

No.	Time	Source	Destination	Protocol	Length
277	57.735035183	192.168.0.107	34.107.221.82	HTTP	364 G
279	57.743874268	34.107.221.82	192.168.0.107	HTTP	288 H
310	57.787706676	192.168.0.107	34.107.221.82	HTTP	369 G
312	57.798605194	34.107.221.82	192.168.0.107	HTTP	288 H
381	58.592689141	192.168.0.107	117.18.237.29	OCSP	447 R
390	58.596603718	117.18.237.29	192.168.0.107	OCSP	867 R
468	58.818786874	192.168.0.107	117.18.237.29	OCSP	447 R
470	58.822348210	117.18.237.29	192.168.0.107	OCSP	867 R
474	58.822576242	192.168.0.107	117.18.237.29	OCSP	447 R
475	58.826981375	117.18.237.29	192.168.0.107	OCSP	867 R
791	59.425826051	192.168.0.107	117.18.237.29	OCSP	447 R
792	59.430094862	117.18.237.29	192.168.0.107	OCSP	867 R
842	59.889268398	192.168.0.107	117.18.237.29	OCSP	447 R
843	59.892795763	117.18.237.29	192.168.0.107	OCSP	867 R
986	65.200360849	192.168.0.107	172.217.163.99	OCSP	453 R
988	65.241958827	172.217.163.99	192.168.0.107	OCSP	769 R
1476	117.677176923	192.168.0.107	34.107.221.82	HTTP	364 G
1482	117.692340745	34.107.221.82	192.168.0.107	HTTP	288 H
1488	117.694076008	192.168.0.107	34.107.221.82	HTTP	369 G
1505	117.704487729	34.107.221.82	192.168.0.107	HTTP	288 H

```

GET /success.txt HTTP/1.1
Host: detectportal.firefox.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101
Firefox/84.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
Pragma: no-cache
Connection: keep-alive

HTTP/1.1 200 OK
Server: nginx
Date: Mon, 15 Feb 2021 00:02:20 GMT
Content-Type: text/plain
Content-Length: 8
Via: 1.1 google
Age: 72996
Cache-Control: public, must-revalidate, max-age=0, s-maxage=86400

success

```

2 client pkts, 2 server pkts, 3 turns.

Entire conversation (1,032 bytes) Show and save data as ASCII Stream 0 Find: Find Next Filter Out This Stream Print Save as... Back Close

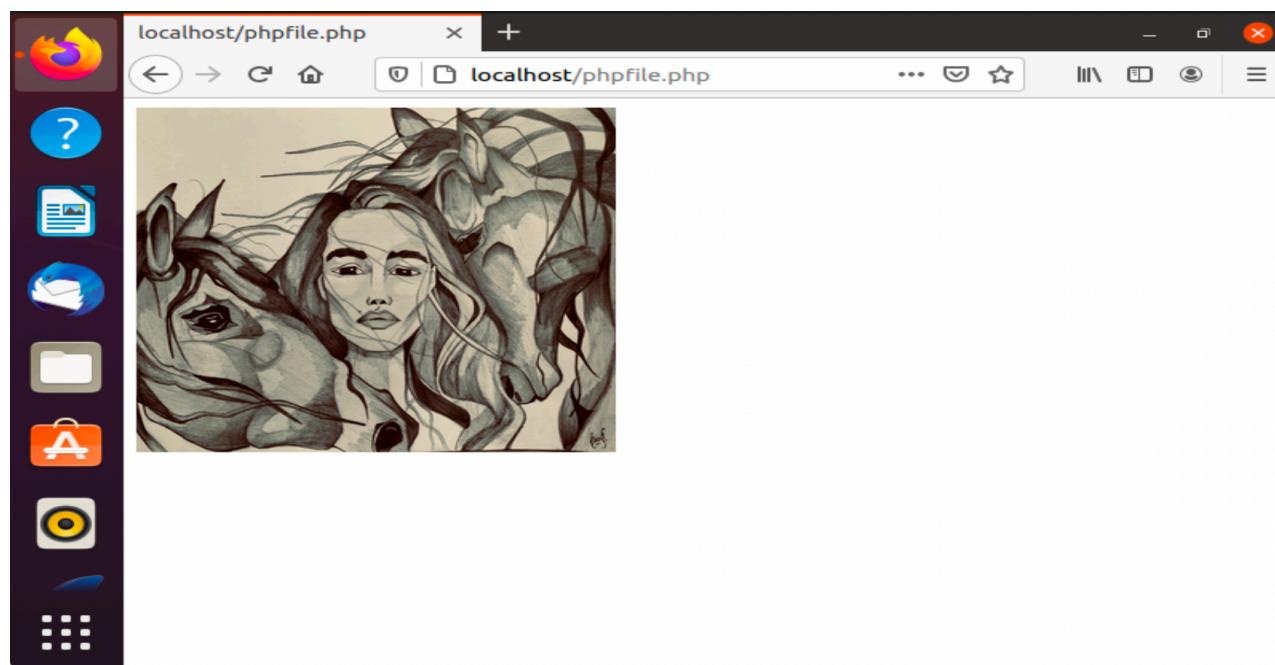
2. SETTING COOKIES:

- PHP:
 - We are setting cookies with PHP script.
 - When this file is requested by the browser, a cookie will be set.



```
1 <html>
2 <?php
3 setcookie("namecookie", "netqwerty", time() + 123);
4 setcookie("nickname", "work");
5 ?>
6 
7 </html>
8 |
```

Localhost:



- WIRESHARK CAPTURE:

- The first GET request corresponding to the PHP file is analysed and its TCP Stream is expanded and examined.
- We can find out the value, name and expiry time of the set cookie, if it hasn't already expired.

*any

Time	Source	Destination	Protocol	Length	Info
6.234605511	192.168.0.107	34.107.221.82	HTTP	364	GET
6.246975753	34.107.221.82	192.168.0.107	HTTP	288	HTTP
6.275786699	192.168.0.107	34.107.221.82	HTTP	369	GET
6.286825236	34.107.221.82	192.168.0.107	HTTP	288	HTTP
6.895932879	192.168.0.107	117.18.237.29	OCSP	447	Requ
6.903254894	117.18.237.29	192.168.0.107	OCSP	867	Resp
7.676212984	192.168.0.107	117.18.237.29	OCSP	447	Requ
7.774296791	117.18.237.29	192.168.0.107	OCSP	866	Resp
8.367686136	192.168.0.107	117.18.237.29	OCSP	447	Requ
8.371569643	117.18.237.29	192.168.0.107	OCSP	867	Resp
9.505774208	192.168.0.107	117.18.237.29	OCSP	447	Requ
9.509304836	117.18.237.29	192.168.0.107	OCSP	866	Resp
14.006623666	192.168.0.107	216.58.200.131	OCSP	453	Requ
14.049274678	216.58.200.131	192.168.0.107	OCSP	769	Resp
25.133328522	127.0.0.1	127.0.0.1	HTTP	407	GET
25.133520877	127.0.0.1	127.0.0.1	HTTP	788	HTTP
28.464855112	127.0.0.1	127.0.0.1	HTTP	446	GET
28.465396944	127.0.0.1	127.0.0.1	HTTP	488	HTTP
66.204924679	192.168.0.107	34.107.221.82	HTTP	364	GET

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

```

GET /success.txt HTTP/1.1
Host: detectportal.firefox.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101
Firefox/84.0
Accept: /*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
Pragma: no-cache
Connection: keep-alive

HTTP/1.1 200 OK
Server: nginx
Date: Mon, 15 Feb 2021 23:25:55 GMT
Content-Type: text/plain
Content-Length: 8
Via: 1.1 google
Age: 61086
Cache-Control: public, must-revalidate, max-age=0, s-maxage=86400

success
GET /success.txt HTTP/1.1

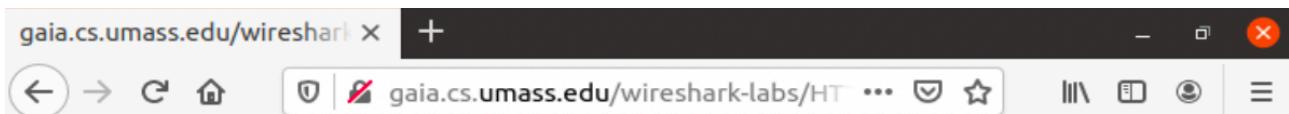
```

3. CONDITIONAL GET:

OBSERVATION:

The HTTP header If-Modified-Since is One way to implement Conditional Get.

On running the given URL in Firefox:



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.

WIRESHARK PACKETS CAPTURED:

Source	Destination	Protocol	Length	Info
192.168.0.107	216.58.200.131	OCSP	453	Request
216.58.200.131	192.168.0.107	OCSP	769	Response
192.168.0.107	128.119.245.12	HTTP	444	GET /wireshark-labs/HTT
128.119.245.12	192.168.0.107	HTTP	798	HTTP/1.1 200 OK (text/
192.168.0.107	128.119.245.12	HTTP	401	GET /favicon.ico HTTP/1
128.119.245.12	192.168.0.107	HTTP	553	HTTP/1.1 404 Not Found
192.168.0.107	128.119.245.12	HTTP	556	GET /wireshark-labs/HTT
128.119.245.12	192.168.0.107	HTTP	307	HTTP/1.1 304 Not Modifi

First HTTP GET Request:

```
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; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101
Firefox/84.0
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: Tue, 16 Feb 2021 16:47:24 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: Tue, 16 Feb 2021 06:59:02 GMT
ETag: "173-5bb6ea32df602"
Accept-Ranges: bytes
Content-Length: 371
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

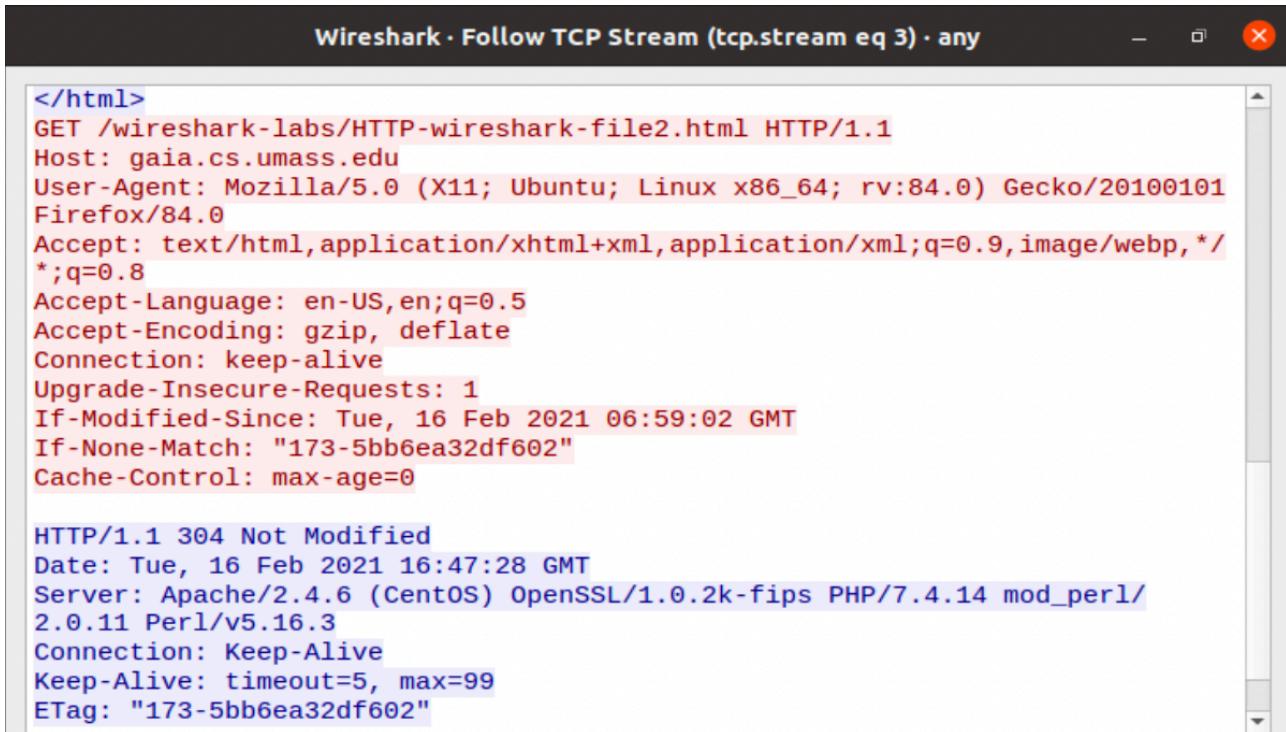
```
Wireshark · Follow TCP Stream (tcp.stream eq 3) · any

</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:84.0) Gecko/20100101
Firefox/84.0
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: Tue, 16 Feb 2021 06:59:02 GMT
If-None-Match: "173-5bb6ea32df602"
Cache-Control: max-age=0

HTTP/1.1 304 Not Modified
Date: Tue, 16 Feb 2021 16:47:28 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=99
ETag: "173-5bb6ea32df602"
```

The server has returned the contents of the file. We know this because the HTML File is obtained along with a 200 OK response status.

Second HTTP GET Request:



The screenshot shows a Wireshark window titled "Follow TCP Stream (tcp.stream eq 3) · any". The content pane displays an HTTP GET request from a Firefox browser to a local file. The request includes headers such as Host, User-Agent, Accept, Accept-Language, Accept-Encoding, Connection, Upgrade-Insecure-Requests, If-Modified-Since, If-None-Match, and Cache-Control. The response is an HTTP/1.1 304 Not Modified message from an Apache server, which includes Date, Server, Connection, Keep-Alive, and ETag headers.

```
</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:84.0) Gecko/20100101
Firefox/84.0
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: Tue, 16 Feb 2021 06:59:02 GMT
If-None-Match: "173-5bb6ea32df602"
Cache-Control: max-age=0

HTTP/1.1 304 Not Modified
Date: Tue, 16 Feb 2021 16:47:28 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=99
ETag: "173-5bb6ea32df602"
```

There is an “IF-MODIFIED-SINCE:” line in the HTTP GET. The information that follows this header is the date and time at which the response was captured.

The second Response from the server is obtained as 304 Not Modified.

4. REPEATING CONDITIONAL GET WITH IMAGES:

- A HTML file containing 10 images is accessed through localhost from Firefox.
- This receives a 200 OK response and the images are sent to the server.
- When the images are sent again, 304 Not Modified status code is sent and images are not sent back.

*any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

Destination	Protocol	Length	Info
127.0.0.1	HTTP	38993	HTTP/1.1 200 OK (JPEG JFIF image)
127.0.0.1	HTTP	396	GET /favicon.ico HTTP/1.1
127.0.0.1	HTTP	555	HTTP/1.1 404 Not Found (text/html)
127.0.0.1	HTTP	564	GET /webpage.html HTTP/1.1
127.0.0.1	HTTP	519	HTTP/1.1 200 OK (text/html)
127.0.0.1	HTTP	505	GET /1.jpg HTTP/1.1
127.0.0.1	HTTP	251	HTTP/1.1 304 Not Modified
127.0.0.1	HTTP	505	GET /2.jpg HTTP/1.1
127.0.0.1	HTTP	251	HTTP/1.1 304 Not Modified
127.0.0.1	HTTP	505	GET /3.jpg HTTP/1.1
127.0.0.1	HTTP	251	HTTP/1.1 304 Not Modified
127.0.0.1	HTTP	505	GET /4.jpg HTTP/1.1
127.0.0.1	HTTP	251	HTTP/1.1 304 Not Modified
127.0.0.1	HTTP	505	GET /5.jpg HTTP/1.1
127.0.0.1	HTTP	251	HTTP/1.1 304 Not Modified
127.0.0.1	HTTP	505	GET /6.jpg HTTP/1.1
127.0.0.1	HTTP	251	HTTP/1.1 304 Not Modified
127.0.0.1	HTTP	504	GET /7.jpg HTTP/1.1
127.0.0.1	HTTP	250	HTTP/1.1 304 Not Modified

*any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

Destination	Protocol	Length	Info
127.0.0.1	HTTP	251	HTTP/1.1 304 Not Modified
127.0.0.1	HTTP	505	GET /2.jpg HTTP/1.1
127.0.0.1	HTTP	251	HTTP/1.1 304 Not Modified
127.0.0.1	HTTP	505	GET /3.jpg HTTP/1.1
127.0.0.1	HTTP	251	HTTP/1.1 304 Not Modified
127.0.0.1	HTTP	505	GET /4.jpg HTTP/1.1
127.0.0.1	HTTP	251	HTTP/1.1 304 Not Modified
127.0.0.1	HTTP	505	GET /5.jpg HTTP/1.1
127.0.0.1	HTTP	251	HTTP/1.1 304 Not Modified
127.0.0.1	HTTP	505	GET /6.jpg HTTP/1.1
127.0.0.1	HTTP	251	HTTP/1.1 304 Not Modified
127.0.0.1	HTTP	504	GET /7.jpg HTTP/1.1
127.0.0.1	HTTP	250	HTTP/1.1 304 Not Modified
127.0.0.1	HTTP	505	GET /8.jpg HTTP/1.1
127.0.0.1	HTTP	251	HTTP/1.1 304 Not Modified
127.0.0.1	HTTP	505	GET /9.jpg HTTP/1.1
127.0.0.1	HTTP	251	HTTP/1.1 304 Not Modified
127.0.0.1	HTTP	506	GET /10.jpg HTTP/1.1
127.0.0.1	HTTP	251	HTTP/1.1 304 Not Modified

Wireshark · Follow TCP Stream (tcp.stream eq 24) · any

```
GET /2.jpg HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101
Firefox/84.0
Accept: image/webp, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Basic c2lyyaToxMjM0NQ==
Connection: keep-alive
Referer: http://localhost/webpage.html

HTTP/1.1 200 OK
Date: Tue, 16 Feb 2021 17:56:36 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Fri, 05 Feb 2021 20:07:26 GMT
ETag: "3d9141-5ba9c5e780429"
Accept-Ranges: bytes
Content-Length: 4034881
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: image/jpeg
```

13 client nktc 78 server nktc 25 turns