

# Computers Network Laboratory

Name – B.Pravna  
SRN – PES2UG19CS076

## Week: #3 Understand working of HTTP Headers

### **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 is modified and when it is not (you can just change the create date of the embedded object). Decode the Basic-Auth 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.

## Week: 3

### Understanding Working of HTTP Headers

**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:** Analyzing Basic Authentication and Cookies

The three parts of experiment are:

1. Password Authentication
2. Cookie Setting
3. Conditional get

## 1) Password Authentication

### Steps of Execution

1. Execute the commands on the terminal.

--> To update existing softwares

**sudo apt-get update**

--> To install the apache utility

**sudo apt-get install apache2**

```
prav@prav-VirtualBox:~$ sudo apt-get install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data libaprutil1-dbd-sqlite3 libaprutil1-ldap
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data libaprutil1-dbd-sqlite3 libaprutil1-ldap
0 upgraded, 5 newly installed, 0 to remove and 62 not upgraded.
Need to get 1,453 kB of archives.
After this operation, 6,526 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu focal/main amd64 libaprutil1-dbd-sqlite3 amd64 1.6.1-4ubuntu2
[10.5 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu focal/main amd64 libaprutil1-ldap amd64 1.6.1-4ubuntu2 [8,736
B]
Get:3 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 apache2-bin amd64 2.4.41-4ubuntu3.1 [
1,180 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 apache2-data all 2.4.41-4ubuntu3.1 [1
58 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 apache2 amd64 2.4.41-4ubuntu3.1 [95.5
kB]
Fetched 1,453 kB in 3s (544 kB/s)
Selecting previously unselected package libaprutil1-dbd-sqlite3:amd64.
```

--> Provide username and password to set authentication

-->View the authentication

**sudo cat /etc/apache2/.htpasswd**

```
prav@prav-VirtualBox:~$ sudo htpasswd -c /etc/apache2/.htpasswd prav
New password:
Re-type new password:
Adding password for user prav
prav@prav-VirtualBox:~$ sudo cat /etc/apache2/.htpasswd
prav:$apr1$eXPMj1Q0$t2rwDHJIotMXxnLweFdYY1
prav@prav-VirtualBox:~$ █
```

Here “prav” is the username. Also, password is entered twice.

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

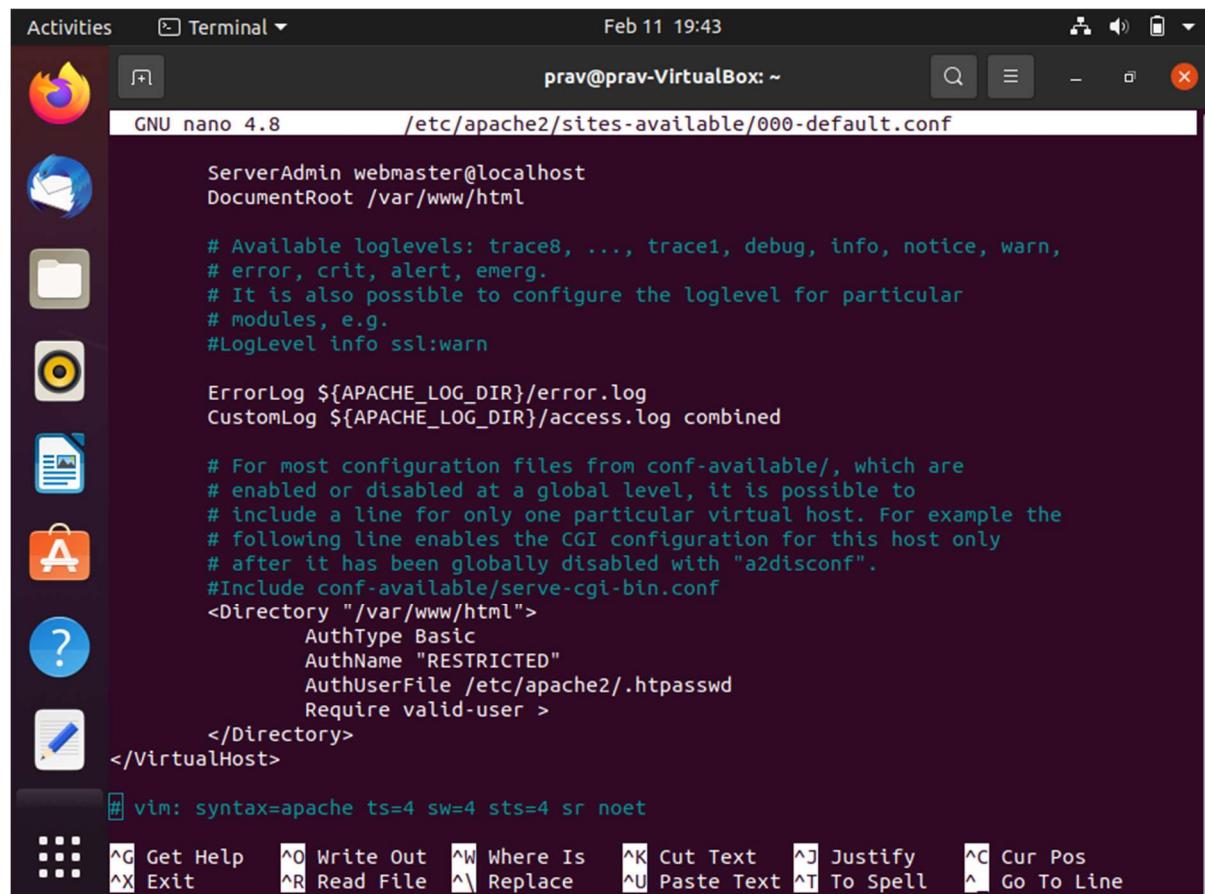
--> Opening the file for setting authentication **sudo**

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

```
<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>
```



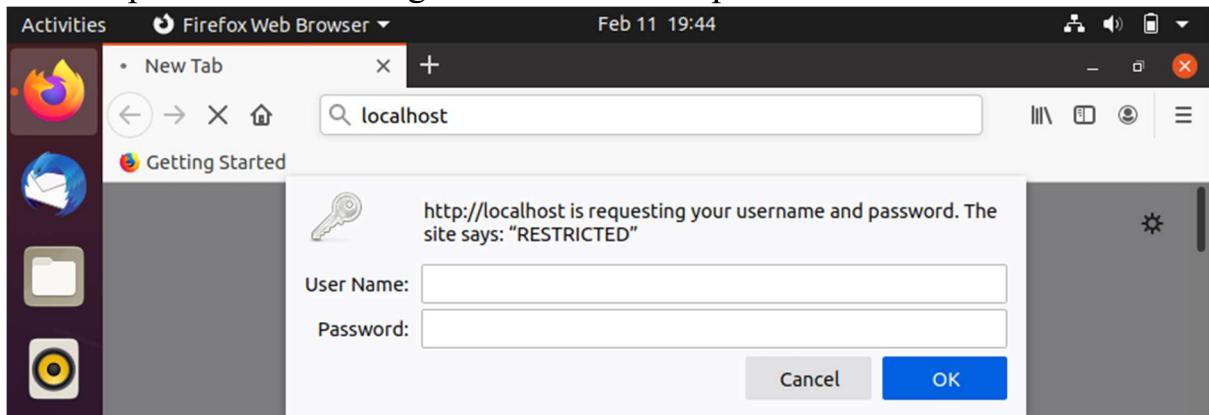
```
Activities Terminal Feb 11 19:43  
prav@prav-VirtualBox: ~  
GNU nano 4.8 /etc/apache2/sites-available/000-default.conf  
ServerAdmin webmaster@localhost  
DocumentRoot /var/www/html  
  
# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,  
# error, crit, alert, emerg.  
# It 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  
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos  
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell ^_ Go To Line
```

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

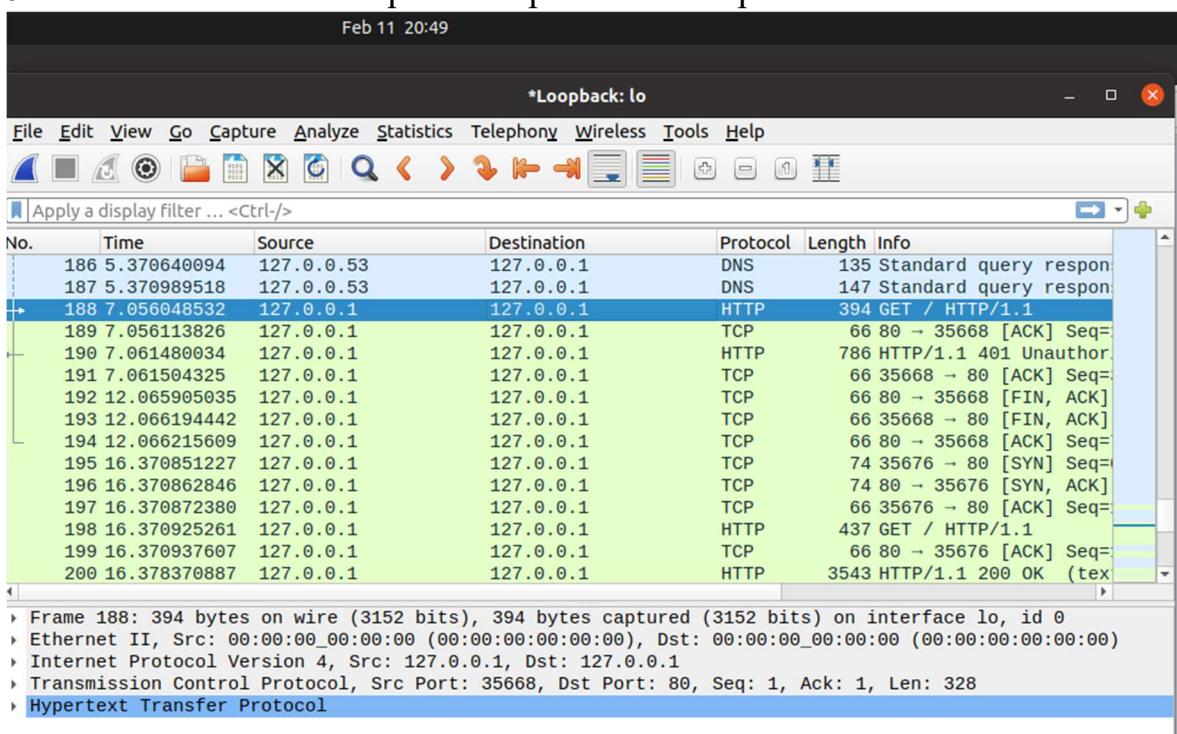
```
sudo service apache2 restart
```

```
prav@prav-VirtualBox:~$ sudo service apache2 restart
prav@prav-VirtualBox:~$ █
```

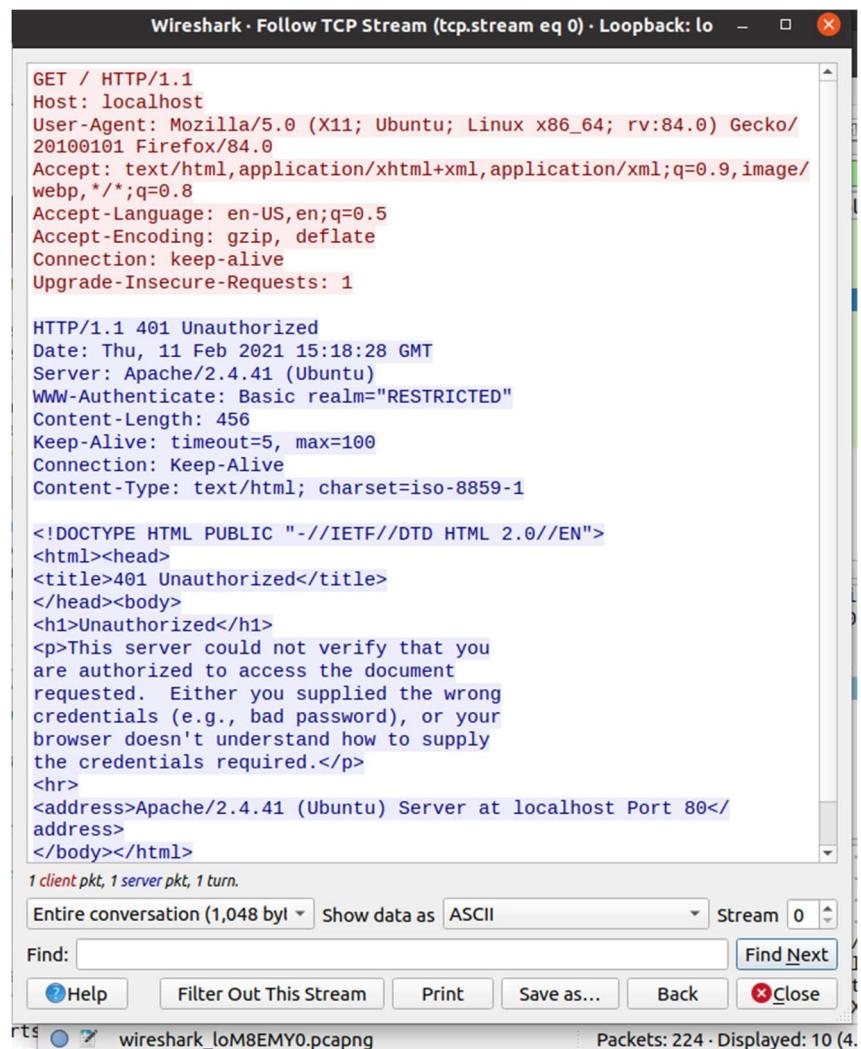
4. The localhost is then accessed using the Firefox browser requiring a username and a password set during the authentication phase.



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



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.



The screenshot shows the Wireshark application window titled "Wireshark - Follow TCP Stream (tcp.stream eq 0) · Loopback: lo". The main pane displays an ASCII dump of an HTTP response. The request line is "GET / HTTP/1.1". The response starts with "HTTP/1.1 401 Unauthorized" and includes headers such as "Date: Thu, 11 Feb 2021 15:18:28 GMT", "Server: Apache/2.4.41 (Ubuntu)", and "WWW-Authenticate: Basic realm="RESTRICTED"". The body of the response contains an HTML error page explaining the unauthorized access. The footer of the window shows "1 client pkt, 1 server pkt, 1 turn.", "Entire conversation (1,048 byt)", "Show data as ASCII", "Stream 0", and various buttons like "Find Next", "Help", "Filter Out This Stream", "Print", "Save as...", "Back", and "Close". At the bottom, it says "wireshark\_loM8EMY0.pcapng" and "Packets: 224 · Displayed: 10 (4)".

```
GET / HTTP/1.1
Host: localhost
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/1.1 401 Unauthorized
Date: Thu, 11 Feb 2021 15:18:28 GMT
Server: Apache/2.4.41 (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/2.4.41 (Ubuntu) Server at localhost Port 80</address>
</body></html>

1 client pkt, 1 server pkt, 1 turn.
Entire conversation (1,048 byt) Show data as ASCII Stream 0
Find: Find Next
Help Filter Out This Stream Print Save as... Back Close
wireshark_loM8EMY0.pcapng Packets: 224 · Displayed: 10 (4)
```

## 2) Cookie Setting

### Steps of Execution

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:

```
<html>
<?php

setcookie("namecookie","netqwerty",time()+12
3);      setcookie("nickname","work"); ?>
<img src= "highres.png" width= "300" height= "300" title= "password" />
</html>
```

```
GNU nano 2.5.3          File: abc.php

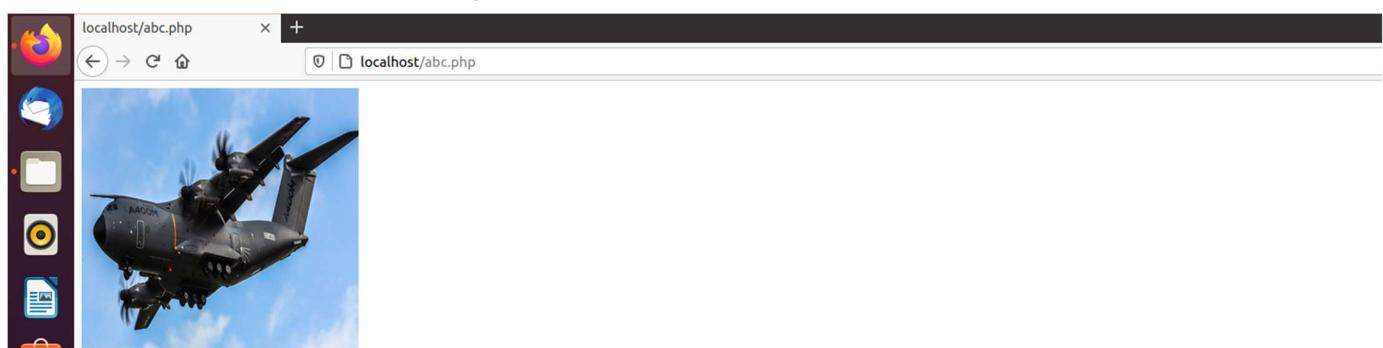
<html>
<?php
setcookie("namecookie","netqwerty",time()+123);
setcookie("nickname","work");
?>

</html>
```

Note: Here you can add any image if required

**Note: You can capture Cookies mostly during the first time of web access. Hence keep wireshark capture ready before executing the task for the first time.**

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



3. The packets are captured using Wireshark and using the “follow TCP stream” which checks for the set-cookie field whether the cookie is set or not set.

No.	Time	Source	Destination	Protocol	Length	Info
169	8.996985685	127.0.0.1	127.0.0.1	TCP	74	33136 → 80 [SYN] Seq=
170	8.996997050	127.0.0.1	127.0.0.1	TCP	74	80 → 33136 [SYN, ACK]
171	8.997005595	127.0.0.1	127.0.0.1	TCP	66	33136 → 80 [ACK] Seq=
172	9.019440473	127.0.0.1	127.0.0.1	HTTP	401	GET /abc.php HTTP/1.1
173	9.019467605	127.0.0.1	127.0.0.1	TCP	66	80 → 33136 [ACK] Seq=
174	9.082806641	127.0.0.1	127.0.0.1	HTTP	448	HTTP/1.1 200 OK (tex
175	9.082867696	127.0.0.1	127.0.0.1	TCP	66	33136 → 80 [ACK] Seq=
184	10.528378695	127.0.0.1	127.0.0.1	HTTP	394	GET /image1.jpg HTTP/
185	10.528396194	127.0.0.1	127.0.0.1	TCP	66	80 → 33136 [ACK] Seq=
186	10.545297949	127.0.0.1	127.0.0.1	TCP	32834	80 → 33136 [ACK] Seq=
187	10.545315225	127.0.0.1	127.0.0.1	TCP	66	33136 → 80 [ACK] Seq=
188	10.545329675	127.0.0.1	127.0.0.1	TCP	32834	80 → 33136 [PSH, ACK]
189	10.545335483	127.0.0.1	127.0.0.1	TCP	66	33136 → 80 [ACK] Seq=
190	10.545522816	127.0.0.1	127.0.0.1	TCP	66	[TCP Window Update] 3:
191	10.549864541	127.0.0.1	127.0.0.1	TCP	32834	80 → 33136 [ACK] Seq=
192	10.550093248	127.0.0.1	127.0.0.1	TCP	66	33136 → 80 [ACK] Seq=
193	10.551217927	127.0.0.1	127.0.0.1	TCP	32834	80 → 33136 [PSH, ACK]
194	10.552371639	127.0.0.1	127.0.0.1	TCP	66	33136 → 80 [ACK] Seq=
195	10.552781826	127.0.0.1	127.0.0.1	TCP	32834	80 → 33136 [ACK] Seq=
196	10.552789116	127.0.0.1	127.0.0.1	TCP	66	33136 → 80 [ACK] Seq=
197	10.552800099	127.0.0.1	127.0.0.1	TCP	32834	80 → 33136 [PSH, ACK]
198	10.552804932	127.0.0.1	127.0.0.1	TCP	66	33136 → 80 [ACK] Seq=

```

> Frame 172: 401 bytes on wire (3208 bits), 401 bytes captured (3208 bits) on interface lo, id 0
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 33136, Dst Port: 80, Seq: 1, Ack: 1, Len: 335
> Hypertext Transfer Protocol

```

```

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

HTTP/1.1 200 OK
Date: Thu, 11 Feb 2021 15:47:07 GMT
Server: Apache/2.4.41 (Ubuntu)
Set-Cookie: namecookie=netqwert; expires=Thu, 11-Feb-2021 15:49:10 GMT; Max-Age=123
Set-Cookie: nickname=work
Content-Length: 65
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<html>

</html>
GET /image1.jpg HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:85.0) Gecko/20100101
Firefox/85.0
Accept: image/webp,*/
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://localhost/abc.php
Cookie: namecookie=netqwert; nickname=work

```

Packet 174. 2 client pkts, 29 server pkts, 3 turns. Click to select.

Entire conversation (918 kB) Show and save data as ASCII Stream Find

The cookie is set as shown in the above screenshot.

## **Observations :-**

### **Working of base 64 algorithm**

Base64 encoding is used to convert binary data into a text-like format to be transported across channels that only reliably support text context.

Base64 encoding takes the original binary data and operates on it by dividing it into tokens of 3 bytes. A byte consists of 8 bits, so Base64 takes 24 bits in total. These 3 bytes are then converted into 4 printable characters from the ASCII standard.

### **Parameters associated with cookie in Wireshark capture :-**

-Cookie name and value

-Expiry time of the cookie

-Max indicated the number of milliseconds the cookie will expire in if its not deleted before.

### **3) 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/wiresharklabs/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 packetlisting window.

Wireshark

gaia.cs.umass.edu/wireshark

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.

## Observations :-

### 1)First HTTP Get Request :-

\*any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

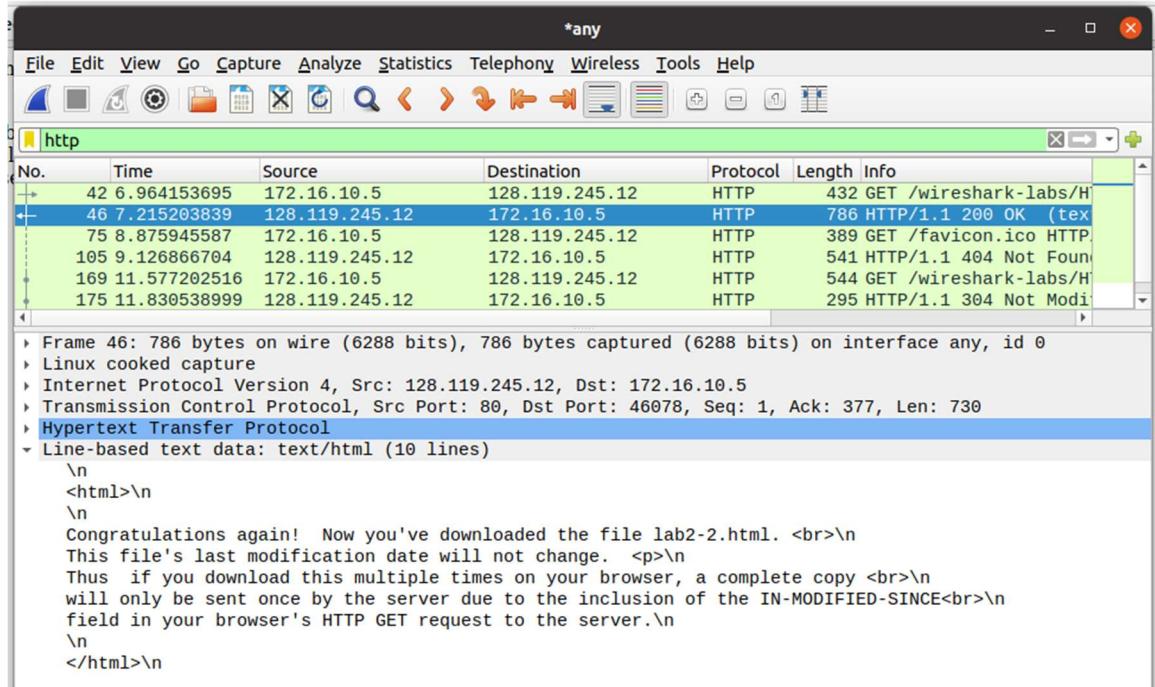
No.	Time	Source	Destination	Protocol	Length	Info
42	6.964153695	172.16.10.5	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file2.html
46	7.215203839	128.119.245.12	172.16.10.5	HTTP	786	HTTP/1.1 200 OK (text/html)
75	8.875945587	172.16.10.5	128.119.245.12	HTTP	389	GET /favicon.ico HTTP/1.1
105	9.126866704	128.119.245.12	172.16.10.5	HTTP	541	HTTP/1.1 404 Not Found (text/html)
169	11.577202516	172.16.10.5	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wireshark-file2.html
175	11.830538999	128.119.245.12	172.16.10.5	HTTP	295	HTTP/1.1 304 Not Modified

```

Frame 42: 432 bytes on wire (3456 bits), 432 bytes captured (3456 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 172.16.10.5, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 46078, Dst Port: 80, Seq: 1, Ack: 1, Len: 376
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /wireshark-labs/HTTP-wireshark-file2.html
    Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:85.0) Gecko/20100101 Firefox/85.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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 1/2]
[Response in frame: 46]
[Next request in frame: 169]
```

It does not contain an “IF MODIFIED-SINCE LINE”.

## 2) Contents of the server response :-



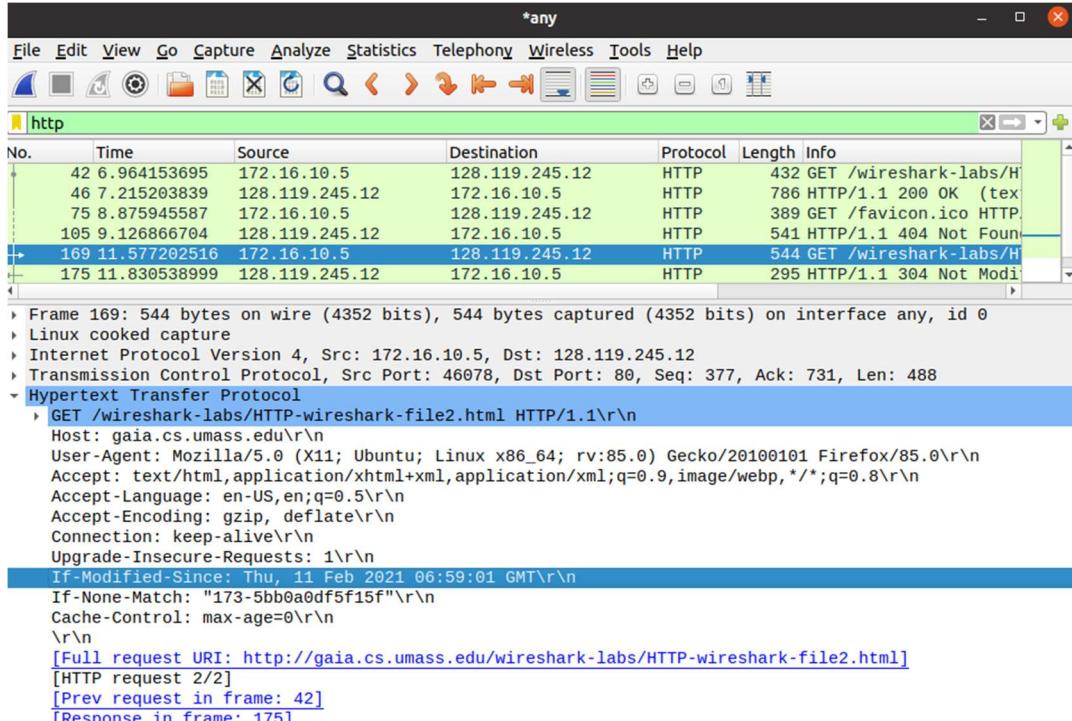
The screenshot shows a Wireshark capture window with the following details:

- Protocol:** http
- Frame 46:** 786 bytes on wire (6288 bits), 786 bytes captured (6288 bits) on interface any, id 0
- HTTP Headers:**
  - Linux cooked capture
  - Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.16.10.5
  - Transmission Control Protocol, Src Port: 80, Dst Port: 46078, Seq: 1, Ack: 377, Len: 730
  - Hypertext Transfer Protocol
- HTTP Body:**

```
\n<html>\n\nCongratulations again! Now you've downloaded the file lab2-2.html. <br>\nThis file's last modification date will not change. <p>\nThus if you download this multiple times on your browser, a complete copy <br>\nwill only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\nfield in your browser's HTTP GET request to the server.\n</p>\n</html>\n
```

The server explicitly returns the contents of the file since we can see the contents of an HTML document that has been returned.

## 4) Second HTTP GET Request :-



The screenshot shows a Wireshark capture window with the following details:

- Protocol:** http
- Frame 169:** 544 bytes on wire (4352 bits), 544 bytes captured (4352 bits) on interface any, id 0
- HTTP Headers:**
  - Linux cooked capture
  - Internet Protocol Version 4, Src: 172.16.10.5, Dst: 128.119.245.12
  - Transmission Control Protocol, Src Port: 46078, Dst Port: 80, Seq: 377, Ack: 731, Len: 488
  - 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:85.0) Gecko/20100101 Firefox/85.0\r\n
    - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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: Thu, 11 Feb 2021 06:59:01 GMT\r\n
    - If-None-Match: "173-5bb0a0df5f15f"\r\n
    - Cache-Control: max-age=0\r\n
- HTTP Body:**
  - [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
  - [HTTP request 2/2]
  - [Prev request in frame: 42]
  - [Response in frame: 175]

We see the IF-MODIFIED-SINCE header. It returns the date and time for which a server first downloaded a resource from the server.

#### 4)Second Server Response

The screenshot shows the Wireshark interface with a list of network frames at the top and a detailed packet analysis window below. The selected frame is a response from port 172.16.10.5 to port 128.119.245.12, labeled as HTTP/1.1 304 Not Modified. The detailed view shows the following response headers:

```
HTTP/1.1 304 Not Modified\r\nContent-Type: text/html\r\nContent-Length: 0\r\nDate: Thu, 11 Feb 2021 16:20:17 GMT\r\nServer: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\nConnection: Keep-Alive\r\nKeep-Alive: timeout=5, max=99\r\nETag: "173-5bb0a0df5f15f"\r\n\r\n[HTTP response 2/2]\r\n[Time since request: 0.253336483 seconds]
```

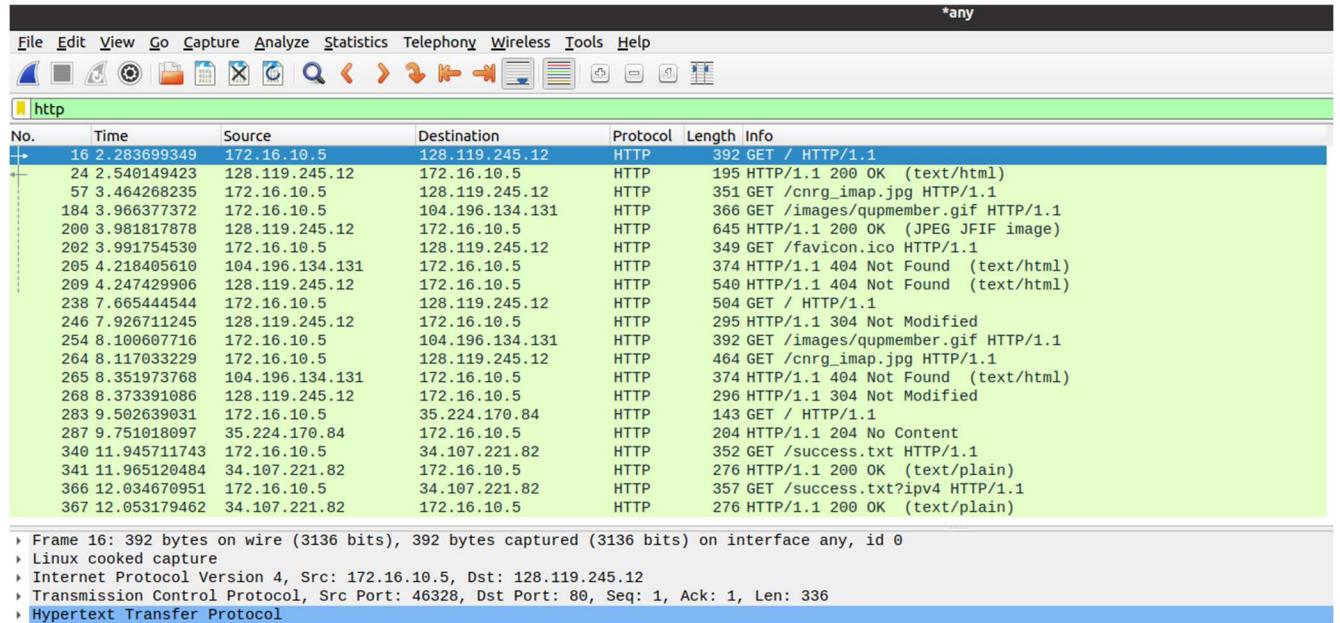
Below the headers, there are links to previous requests and responses in the frame sequence.

HTTP Status Code 304 and phrase Not Modified returned.

This means that the file has not changed since the last time it was accessed and there is no need to download the file again. Hence the file contents not returned too. This allows both the website owner and the visitor to conserve resources as the file does not have to be retrieved each time.

# SERVER WITH IMAGES

Accessing a website with images :-



The Wireshark interface shows a list of captured network frames. Frame 16 is selected, which is a GET request for the root URL. The packet details pane shows the HTTP headers and body. The bytes pane shows the raw binary data of the packet.

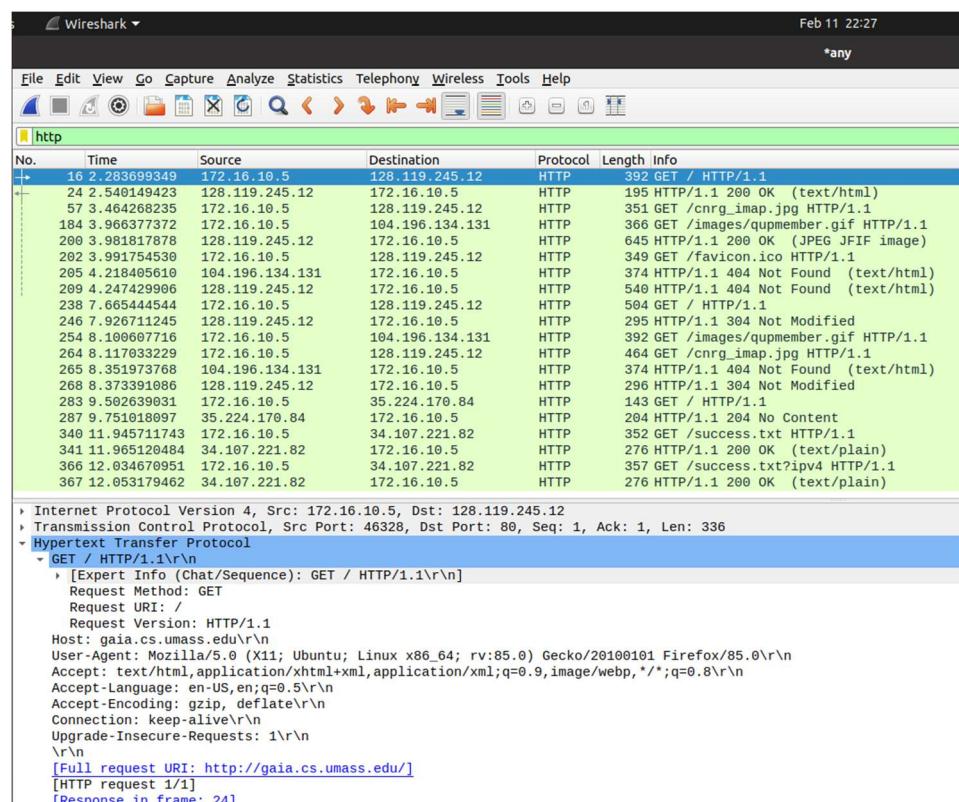
No.	Time	Source	Destination	Protocol	Length	Info
16	2.283699349	172.16.10.5	128.119.245.12	HTTP	392	GET / HTTP/1.1
24	2.540149423	128.119.245.12	172.16.10.5	HTTP	195	HTTP/1.1 200 OK (text/html)
57	3.464268235	172.16.10.5	128.119.245.12	HTTP	351	GET /cnrg_imap.jpg HTTP/1.1
184	3.966377372	172.16.10.5	104.196.134.131	HTTP	366	GET /images/qupmember.gif HTTP/1.1
200	3.981817878	128.119.245.12	172.16.10.5	HTTP	645	HTTP/1.1 200 OK (JPEG/JFIF image)
202	3.991754530	172.16.10.5	128.119.245.12	HTTP	349	GET /favicon.ico HTTP/1.1
205	4.218405610	104.196.134.131	172.16.10.5	HTTP	374	HTTP/1.1 404 Not Found (text/html)
209	4.247429906	128.119.245.12	172.16.10.5	HTTP	540	HTTP/1.1 404 Not Found (text/html)
238	7.665444544	172.16.10.5	128.119.245.12	HTTP	504	GET / HTTP/1.1
246	7.926711245	128.119.245.12	172.16.10.5	HTTP	295	HTTP/1.1 304 Not Modified
254	8.100607716	172.16.10.5	104.196.134.131	HTTP	392	GET /images/qupmember.gif HTTP/1.1
264	8.117033229	172.16.10.5	128.119.245.12	HTTP	464	GET /cnrg_imap.jpg HTTP/1.1
265	8.351973768	104.196.134.131	172.16.10.5	HTTP	374	HTTP/1.1 404 Not Found (text/html)
268	8.373391086	128.119.245.12	172.16.10.5	HTTP	296	HTTP/1.1 304 Not Modified
283	9.502639031	172.16.10.5	35.224.170.84	HTTP	143	GET / HTTP/1.1
287	9.751018097	35.224.170.84	172.16.10.5	HTTP	204	HTTP/1.1 204 No Content
340	11.945711743	172.16.10.5	34.107.221.82	HTTP	352	GET /success.txt HTTP/1.1
341	11.965120484	34.107.221.82	172.16.10.5	HTTP	276	HTTP/1.1 200 OK (text/plain)
366	12.034670951	172.16.10.5	34.107.221.82	HTTP	357	GET /success.txt?ipv4 HTTP/1.1
367	12.053179462	34.107.221.82	172.16.10.5	HTTP	276	HTTP/1.1 200 OK (text/plain)

Frame 16: 392 bytes on wire (3136 bits), 392 bytes captured (3136 bits) on interface any, id 0  
Linux cooked capture  
Internet Protocol Version 4, Src: 172.16.10.5, Dst: 128.119.245.12  
Transmission Control Protocol, Src Port: 46328, Dst Port: 80, Seq: 1, Ack: 1, Len: 336  
Hypertext Transfer Protocol

## OBSERVATIONS :-

Accessing the website for the first time :-

HTTP GET Request :-



The Wireshark interface shows a list of captured network frames. Frame 16 is selected, which is a GET request for the root URL. The packet details pane shows the HTTP headers and body. The bytes pane shows the raw binary data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
16	2.283699349	172.16.10.5	128.119.245.12	HTTP	392	GET / HTTP/1.1
24	2.540149423	128.119.245.12	172.16.10.5	HTTP	195	HTTP/1.1 200 OK (text/html)
57	3.464268235	172.16.10.5	128.119.245.12	HTTP	351	GET /cnrg_imap.jpg HTTP/1.1
184	3.966377372	172.16.10.5	104.196.134.131	HTTP	366	GET /images/qupmember.gif HTTP/1.1
200	3.981817878	128.119.245.12	172.16.10.5	HTTP	645	HTTP/1.1 200 OK (JPEG/JFIF image)
202	3.991754530	172.16.10.5	128.119.245.12	HTTP	349	GET /favicon.ico HTTP/1.1
205	4.218405610	104.196.134.131	172.16.10.5	HTTP	374	HTTP/1.1 404 Not Found (text/html)
209	4.247429906	128.119.245.12	172.16.10.5	HTTP	540	HTTP/1.1 404 Not Found (text/html)
238	7.665444544	172.16.10.5	128.119.245.12	HTTP	504	GET / HTTP/1.1
246	7.926711245	128.119.245.12	172.16.10.5	HTTP	295	HTTP/1.1 304 Not Modified
254	8.100607716	172.16.10.5	104.196.134.131	HTTP	392	GET /images/qupmember.gif HTTP/1.1
264	8.117033229	172.16.10.5	128.119.245.12	HTTP	464	GET /cnrg_imap.jpg HTTP/1.1
265	8.351973768	104.196.134.131	172.16.10.5	HTTP	374	HTTP/1.1 404 Not Found (text/html)
268	8.373391086	128.119.245.12	172.16.10.5	HTTP	296	HTTP/1.1 304 Not Modified
283	9.502639031	172.16.10.5	35.224.170.84	HTTP	143	GET / HTTP/1.1
287	9.751018097	35.224.170.84	172.16.10.5	HTTP	204	HTTP/1.1 204 No Content
340	11.945711743	172.16.10.5	34.107.221.82	HTTP	352	GET /success.txt HTTP/1.1
341	11.965120484	34.107.221.82	172.16.10.5	HTTP	276	HTTP/1.1 200 OK (text/plain)
366	12.034670951	172.16.10.5	34.107.221.82	HTTP	357	GET /success.txt?ipv4 HTTP/1.1
367	12.053179462	34.107.221.82	172.16.10.5	HTTP	276	HTTP/1.1 200 OK (text/plain)

Internet Protocol Version 4, Src: 172.16.10.5, Dst: 128.119.245.12  
Transmission Control Protocol, Src Port: 46328, Dst Port: 80, Seq: 1, Ack: 1, Len: 336  
Hypertext Transfer Protocol  
GET / HTTP/1.1\r\n[Expert Info (Chat/Sequence): GET / HTTP/1.1\r\nRequest Method: GET  
Request URI: /  
Request Version: HTTP/1.1  
Host: gaia.cs.umass.edu\r\nUser-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:85.0) Gecko/20100101 Firefox/85.0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8\r\nAccept-Language: en-US,en;q=0.5\r\nAccept-Encoding: gzip, deflate\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\n\r\n[Full request URI: http://gaia.cs.umass.edu/]  
[HTTP request 1/1]  
[Response in frame: 24]

## Response :-

NetworkMiner capture showing the response:

No.	Time	Source	Destination	Protocol	Length	Info
16	2.283699349	172.16.10.5	128.119.245.12	HTTP	392	GET / HTTP/1.1
24	2.540149423	128.119.245.12	172.16.10.5	HTTP	195	HTTP/1.1 200 OK (text/html)
57	3.464268235	172.16.10.5	128.119.245.12	HTTP	351	GET /cnrg_imap.jpg HTTP/1.1
184	3.966377372	172.16.10.5	104.196.134.131	HTTP	366	GET /images/uqpmember.gif HTTP/1.1
200	3.981817878	128.119.245.12	172.16.10.5	HTTP	645	HTTP/1.1 200 OK (JPEG/JFIF image)
202	3.991754530	172.16.10.5	128.119.245.12	HTTP	349	GET /favicon.ico HTTP/1.1
205	4.218405610	104.196.134.131	172.16.10.5	HTTP	374	HTTP/1.1 404 Not Found (text/html)
209	4.247429966	128.119.245.12	172.16.10.5	HTTP	540	HTTP/1.1 404 Not Found (text/html)
238	7.665444544	172.16.10.5	128.119.245.12	HTTP	504	GET / HTTP/1.1
246	7.926711245	128.119.245.12	172.16.10.5	HTTP	295	HTTP/1.1 304 Not Modified
254	8.100607716	172.16.10.5	104.196.134.131	HTTP	392	GET /images/uqpmember.gif HTTP/1.1
264	8.117033229	172.16.10.5	128.119.245.12	HTTP	464	GET /cnrg_imap.jpg HTTP/1.1
265	8.351973768	104.196.134.131	172.16.10.5	HTTP	374	HTTP/1.1 404 Not Found (text/html)
268	8.373391086	128.119.245.12	172.16.10.5	HTTP	296	HTTP/1.1 304 Not Modified
283	9.502639031	172.16.10.5	35.224.170.84	HTTP	143	GET / HTTP/1.1
287	9.751018097	35.224.170.84	172.16.10.5	HTTP	204	HTTP/1.1 204 No Content
340	11.945711743	172.16.10.5	34.107.221.82	HTTP	352	GET /success.txt HTTP/1.1
341	11.965120484	34.107.221.82	172.16.10.5	HTTP	276	HTTP/1.1 200 OK (text/plain)
366	12.034670951	172.16.10.5	34.107.221.82	HTTP	357	GET /success.txt?ipv4 HTTP/1.1
367	12.053179462	34.107.221.82	172.16.10.5	HTTP	276	HTTP/1.1 200 OK (text/plain)

Hypertext Transfer Protocol

```
> Line-based text data: text/html (68 lines)
<html>
<head>
<title>Computer Network Research Group - UMass Amherst</title>
</head>
<body bgcolor="#ffffff">
<center>
<p>
<map name="cnrg_imapMAP">
<area coords="290,177,407,205" shape="rect" href="/networks/resources/index.html">
<area coords="163,178,275,205" shape="rect" href="/networks/education/index.html">
<area coords="62,165,145,191" shape="rect" href="/search.html">
<area coords="6,63,157,98" shape="rect" href="/networks/collaborations.html">
<area coords="64,7,146,34" shape="rect" href="/networks/people.html">
<area coords="163,7,270,33" shape="rect" href="/networks/research.html">

```

Contents of the HTML document are returned.

## Request for an image :-

NetworkMiner capture showing the request for an image:

No.	Time	Source	Destination	Protocol	Length	Info
16	2.283699349	172.16.10.5	128.119.245.12	HTTP	392	GET / HTTP/1.1
24	2.540149423	128.119.245.12	172.16.10.5	HTTP	195	HTTP/1.1 200 OK (text/html)
57	3.464268235	172.16.10.5	128.119.245.12	HTTP	351	GET /cnrg_imap.jpg HTTP/1.1
184	3.966377372	172.16.10.5	104.196.134.131	HTTP	366	GET /images/uqpmember.gif HTTP/1.1
200	3.981817878	128.119.245.12	172.16.10.5	HTTP	645	HTTP/1.1 200 OK (JPEG/JFIF image)
202	3.991754530	172.16.10.5	128.119.245.12	HTTP	349	GET /favicon.ico HTTP/1.1
205	4.218405610	104.196.134.131	172.16.10.5	HTTP	374	HTTP/1.1 404 Not Found (text/html)
209	4.247429966	128.119.245.12	172.16.10.5	HTTP	540	HTTP/1.1 404 Not Found (text/html)
238	7.665444544	172.16.10.5	128.119.245.12	HTTP	504	GET / HTTP/1.1
246	7.926711245	128.119.245.12	172.16.10.5	HTTP	295	HTTP/1.1 304 Not Modified
254	8.100607716	172.16.10.5	104.196.134.131	HTTP	392	GET /images/uqpmember.gif HTTP/1.1
264	8.117033229	172.16.10.5	128.119.245.12	HTTP	464	GET /cnrg_imap.jpg HTTP/1.1
265	8.351973768	104.196.134.131	172.16.10.5	HTTP	374	HTTP/1.1 404 Not Found (text/html)
268	8.373391086	128.119.245.12	172.16.10.5	HTTP	296	HTTP/1.1 304 Not Modified
283	9.502639031	172.16.10.5	35.224.170.84	HTTP	143	GET / HTTP/1.1
287	9.751018097	35.224.170.84	172.16.10.5	HTTP	204	HTTP/1.1 204 No Content
340	11.945711743	172.16.10.5	34.107.221.82	HTTP	352	GET /success.txt HTTP/1.1
341	11.965120484	34.107.221.82	172.16.10.5	HTTP	276	HTTP/1.1 200 OK (text/plain)
366	12.034670951	172.16.10.5	34.107.221.82	HTTP	357	GET /success.txt?ipv4 HTTP/1.1
367	12.053179462	34.107.221.82	172.16.10.5	HTTP	276	HTTP/1.1 200 OK (text/plain)

Frame 57: 351 bytes on wire (2808 bits), 351 bytes captured (2808 bits) on interface any, id 0

Linux cooked capture

Internet Protocol Version 4, Src: 172.16.10.5, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 46326, Dst Port: 80, Seq: 1, Ack: 1, Len: 295

Hypertext Transfer Protocol

- GET /cnrg\_imap.jpg HTTP/1.1\r\n
 [Expert Info (Chat/Sequence): GET /cnrg\_imap.jpg HTTP/1.1\r\n]
 Request Method: GET
 Request URI: /cnrg\_imap.jpg
 Request Version: HTTP/1.1
 Host: gaia.cs.umass.edu\r\n
 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:85.0) Gecko/20100101 Firefox/85.0\r\n
 Accept: image/webp,\*/\*\r\n
 Accept-Language: en-US,en;q=0.5\r\n
 Accept-Encoding: gzip, deflate\r\n
 Connection: keep-alive\r\n
 Referer: http://gaia.cs.umass.edu/\r\n

[Full request URI: http://gaia.cs.umass.edu/cnrg\_imap.jpg]

HTTP request 1/41

## Accessing the website for the second time :-

HTTP Get Request :-

No.	Time	Source	Destination	Protocol	Length	Info
16	2.283699349	172.16.10.5	128.119.245.12	HTTP	392	GET / HTTP/1.1
24	2.540149423	128.119.245.12	172.16.10.5	HTTP	195	HTTP/1.1 200 OK (text/html)
57	3.464268235	172.16.10.5	128.119.245.12	HTTP	351	GET /cnrg_imap.jpg HTTP/1.1
184	3.966377372	172.16.10.5	104.196.134.131	HTTP	366	GET /images/qupmember.gif HTTP/1.1
200	3.981817878	128.119.245.12	172.16.10.5	HTTP	645	HTTP/1.1 200 OK (JPEG JFIF image)
202	3.991754530	172.16.10.5	128.119.245.12	HTTP	349	GET /favicon.ico HTTP/1.1
205	4.218405610	104.196.134.131	172.16.10.5	HTTP	374	HTTP/1.1 404 Not Found (text/html)
209	4.247429906	128.119.245.12	172.16.10.5	HTTP	540	HTTP/1.1 404 Not Found (text/html)
238	7.665444544	172.16.10.5	128.119.245.12	HTTP	504	GET / HTTP/1.1
246	7.926711245	128.119.245.12	172.16.10.5	HTTP	295	HTTP/1.1 304 Not Modified
254	8.100607716	172.16.10.5	104.196.134.131	HTTP	392	GET /images/qupmember.gif HTTP/1.1
264	8.117033229	172.16.10.5	128.119.245.12	HTTP	464	GET /cnrg_imap.jpg HTTP/1.1
265	8.351973768	104.196.134.131	172.16.10.5	HTTP	374	HTTP/1.1 404 Not Found (text/html)
268	8.373391086	128.119.245.12	172.16.10.5	HTTP	296	HTTP/1.1 304 Not Modified
283	9.502639031	172.16.10.5	35.224.170.84	HTTP	143	GET / HTTP/1.1
287	9.751018097	35.224.170.84	172.16.10.5	HTTP	204	HTTP/1.1 204 No Content
340	11.945711743	172.16.10.5	34.107.221.82	HTTP	352	GET /success.txt HTTP/1.1
341	11.965120484	34.107.221.82	172.16.10.5	HTTP	276	HTTP/1.1 200 OK (text/plain)
366	12.034670951	172.16.10.5	34.107.221.82	HTTP	357	GET /success.txt?ipv4 HTTP/1.1
367	12.053179462	34.107.221.82	172.16.10.5	HTTP	276	HTTP/1.1 200 OK (text/plain)
▼ GET / HTTP/1.1\r\n						
▶ [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]						
Request Method: GET						
Request URI: /						
Request Version: HTTP/1.1						
Host: gaia.cs.umass.edu\r\n						
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:85.0) Gecko/20100101 Firefox/85.0\r\n						
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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: Tue, 01 Mar 2016 18:57:50 GMT\r\n						
If-None-Match: "a5b-52d015789ee9e"\r\n						
Cache-Control: max-age=0\r\n						

We can see the IF-MODIFIED-SINCE header.

Server Response :-

No.	Time	Source	Destination	Protocol	Length	Info
16	2.283699349	172.16.10.5	128.119.245.12	HTTP	392	GET / HTTP/1.1
24	2.540149423	128.119.245.12	172.16.10.5	HTTP	195	HTTP/1.1 200 OK (text/html)
57	3.464268235	172.16.10.5	128.119.245.12	HTTP	351	GET /cnrg_imap.jpg HTTP/1.1
184	3.966377372	172.16.10.5	104.196.134.131	HTTP	366	GET /images/qupmember.gif HTTP/1.1
200	3.981817878	128.119.245.12	172.16.10.5	HTTP	645	HTTP/1.1 200 OK (JPEG JFIF image)
202	3.991754530	172.16.10.5	128.119.245.12	HTTP	349	GET /favicon.ico HTTP/1.1
205	4.218405610	104.196.134.131	172.16.10.5	HTTP	374	HTTP/1.1 404 Not Found (text/html)
209	4.247429906	128.119.245.12	172.16.10.5	HTTP	540	HTTP/1.1 404 Not Found (text/html)
238	7.665444544	172.16.10.5	128.119.245.12	HTTP	504	GET / HTTP/1.1
246	7.926711245	128.119.245.12	172.16.10.5	HTTP	295	HTTP/1.1 304 Not Modified
254	8.100607716	172.16.10.5	104.196.134.131	HTTP	392	GET /images/qupmember.gif HTTP/1.1
264	8.117033229	172.16.10.5	128.119.245.12	HTTP	464	GET /cnrg_imap.jpg HTTP/1.1
265	8.351973768	104.196.134.131	172.16.10.5	HTTP	374	HTTP/1.1 404 Not Found (text/html)
268	8.373391086	128.119.245.12	172.16.10.5	HTTP	296	HTTP/1.1 304 Not Modified
283	9.502639031	172.16.10.5	35.224.170.84	HTTP	143	GET / HTTP/1.1
287	9.751018097	35.224.170.84	172.16.10.5	HTTP	204	HTTP/1.1 204 No Content
340	11.945711743	172.16.10.5	34.107.221.82	HTTP	352	GET /success.txt HTTP/1.1
▶ Frame 268: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits) on interface any, id 0						
▶ Linux cooked capture						
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.16.10.5						
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 46326, Seq: 33981, Ack: 1445, Len: 240						
▶ Hypertext Transfer Protocol						
▶ HTTP/1.1 304 Not Modified\r\n						
▶ [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]						
Response Version: HTTP/1.1						
Status Code: 304						
[Status Code Description: Not Modified]						
Response Phrase: Not Modified						
Date: Thu, 11 Feb 2021 16:55:50 GMT\r\n						
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n						
Connection: Keep-Alive\r\n						
Keep-Alive: timeout=5, max=97\r\n						

The status code is 304 (description – Not Modified).

Request for the same image :-

The Wireshark screenshot displays a list of network captures. The timeline shows several requests for the same image, specifically 'cnrg\_imap.jpg'. The details pane shows the full HTTP request for frame 264, which includes the URL, headers (Host, User-Agent, Accept, Accept-Language, Accept-Encoding, Connection, Referer, If-Modified-Since, If-None-Match, Cache-Control), and a note indicating it's the fourth HTTP request.

No.	Time	Source	Destination	Protocol	Length	Info
16	2.283699349	172.16.10.5	128.119.245.12	HTTP	392	GET / HTTP/1.1
24	2.540149423	128.119.245.12	172.16.10.5	HTTP	195	HTTP/1.1 200 OK (text/html)
57	3.464268235	172.16.10.5	128.119.245.12	HTTP	351	GET /cnrg_imap.jpg HTTP/1.1
184	3.966377372	172.16.10.5	104.196.134.131	HTTP	366	GET /images/qupmember.gif HTTP/1.1
200	3.981817878	128.119.245.12	172.16.10.5	HTTP	645	HTTP/1.1 200 OK (JPEG JFIF image)
202	3.991754530	172.16.10.5	128.119.245.12	HTTP	349	GET /favicon.ico HTTP/1.1
205	4.218405610	104.196.134.131	172.16.10.5	HTTP	374	HTTP/1.1 404 Not Found (text/html)
209	4.247429906	128.119.245.12	172.16.10.5	HTTP	540	HTTP/1.1 404 Not Found (text/html)
238	7.665444544	172.16.10.5	128.119.245.12	HTTP	504	GET / HTTP/1.1
246	7.926711245	128.119.245.12	172.16.10.5	HTTP	295	HTTP/1.1 304 Not Modified
254	8.100607716	172.16.10.5	104.196.134.131	HTTP	392	GET /images/qupmember.gif HTTP/1.1
264	8.117033229	172.16.10.5	128.119.245.12	HTTP	464	GET /cnrg_imap.jpg HTTP/1.1
265	8.351973768	104.196.134.131	172.16.10.5	HTTP	374	HTTP/1.1 404 Not Found (text/html)
268	8.373391086	128.119.245.12	172.16.10.5	HTTP	296	HTTP/1.1 304 Not Modified
283	9.502639031	172.16.10.5	35.224.170.84	HTTP	143	GET / HTTP/1.1
287	9.751018097	35.224.170.84	172.16.10.5	HTTP	204	HTTP/1.1 204 No Content
340	11.945711743	172.16.10.5	34.107.221.82	HTTP	352	GET /success.txt HTTP/1.1

Frame 264: 464 bytes on wire (3712 bits), 464 bytes captured (3712 bits) on interface any, id 0  
Linux cooked capture  
Internet Protocol Version 4, Src: 172.16.10.5, Dst: 128.119.245.12  
Transmission Control Protocol, Src Port: 46326, Dst Port: 80, Seq: 1037, Ack: 33981, Len: 408  
Hypertext Transfer Protocol  
GET /cnrg\_imap.jpg HTTP/1.1\r\n [Expert Info (Chat/Sequence): GET /cnrg\_imap.jpg HTTP/1.1\r\n]  
 Request Method: GET  
 Request URI: /cnrg\_imap.jpg  
 Request Version: HTTP/1.1  
 Host: gaia.cs.umass.edu\r\n User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:85.0) Gecko/20100101 Firefox/85.0\r\n Accept: image/webp, \*/\*\r\n Accept-Language: en-US,en;q=0.5\r\n Accept-Encoding: gzip, deflate\r\n Connection: keep-alive\r\n Referer: http://gaia.cs.umass.edu/\r\n If-Modified-Since: Tue, 30 Oct 2007 16:59:43 GMT\r\n If-None-Match: "808d-43db8be4f7dc0"\r\n Cache-Control: max-age=0\r\n \r\n [Full request URI: http://gaia.cs.umass.edu/cnrg\_imap.jpg]  
 [HTTP request 4/4]

IF-MODIFIED-SINCE header is included here.