

PES1UG20CS821

NIKHIL T M

Week:3 Understanding Working of HTTP Headers

1. Password Authentication

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

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

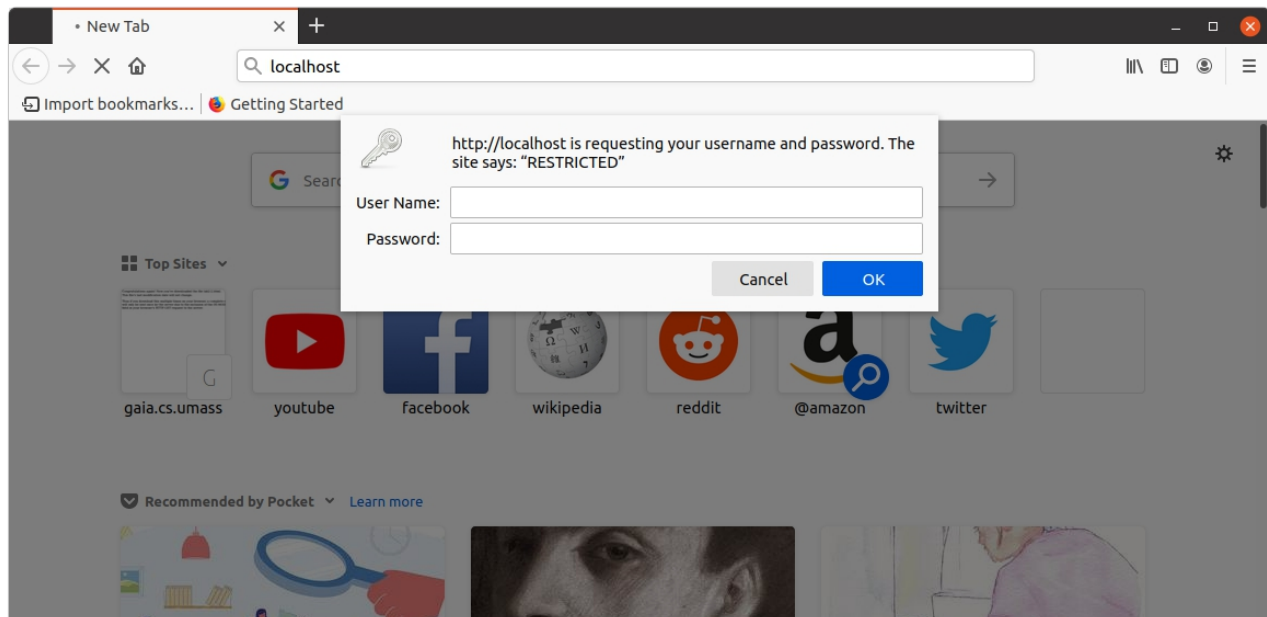
`sudo cat /etc/apache2/.htpasswd`

```
nikhil@nikhil-VirtualBox:~$ sudo htpasswd -c /etc/apache2/.htpasswd nikhil
New password:
Re-type new password:
Adding password for user nikhil
nikhil@nikhil-VirtualBox:~$ sudo cat /etc/apache2/.htpasswd
nikhil:$apr1$EAd87lFt$zaDKc.DjI3Ir40yJeEYlE1
```

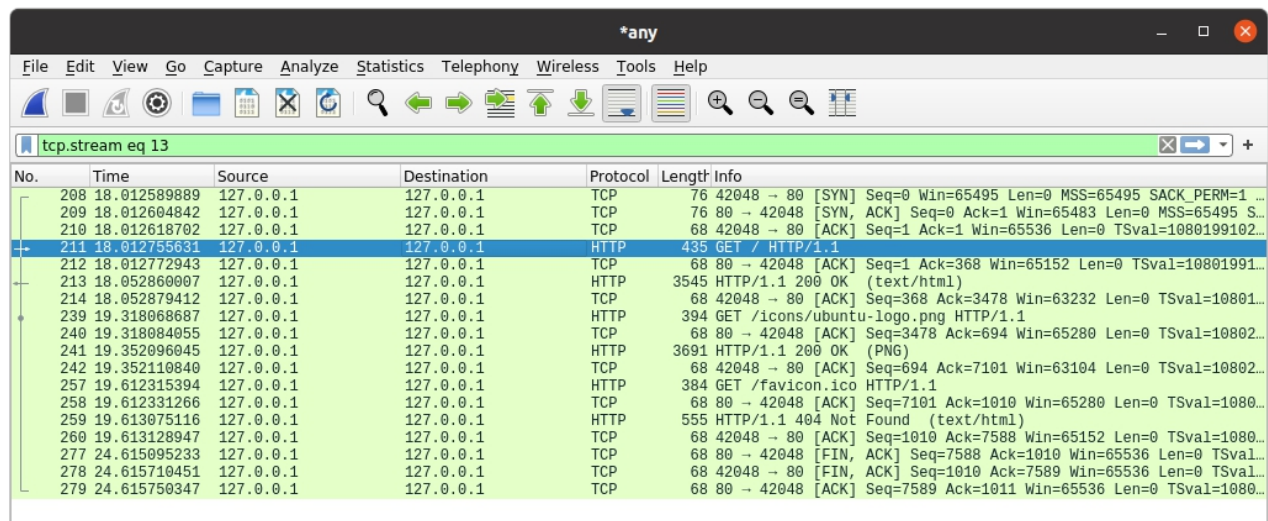
`sudo service apache2 restart`

```
nikhil@nikhil-VirtualBox: ~
nikhil@nikhil-VirtualBox:~$ sudo service apache2 restart
[sudo] password for nikhil:
nikhil@nikhil-VirtualBox:~$
```

Access the localhost



Capture the packets using wireshark



No.	Time	Source	Destination	Protocol	Length	Info
208	18.012589889	127.0.0.1	127.0.0.1	TCP	76	42048 → 80 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 ...
209	18.012604842	127.0.0.1	127.0.0.1	TCP	76	80 → 42048 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 S...
210	18.012618702	127.0.0.1	127.0.0.1	TCP	68	42048 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1080199102...
211	18.012755631	127.0.0.1	127.0.0.1	HTTP	435	GET / HTTP/1.1
212	18.012772943	127.0.0.1	127.0.0.1	TCP	68	80 → 42048 [ACK] Seq=1 Ack=368 Win=65152 Len=0 TSval=10801991...
213	18.052860007	127.0.0.1	127.0.0.1	HTTP	3545	HTTP/1.1 200 OK (text/html)
214	18.052879412	127.0.0.1	127.0.0.1	TCP	68	42048 → 80 [ACK] Seq=368 Ack=3478 Win=63232 Len=0 TSval=10801...
239	19.318068687	127.0.0.1	127.0.0.1	HTTP	394	GET /icons/ubuntu-logo.png HTTP/1.1
240	19.318084055	127.0.0.1	127.0.0.1	TCP	68	80 → 42048 [ACK] Seq=3478 Ack=694 Win=65280 Len=0 TSval=10802...
241	19.352096045	127.0.0.1	127.0.0.1	HTTP	3691	HTTP/1.1 200 OK (PNG)
242	19.352110840	127.0.0.1	127.0.0.1	TCP	68	42048 → 80 [ACK] Seq=694 Ack=7101 Win=63104 Len=0 TSval=10802...
257	19.612315394	127.0.0.1	127.0.0.1	HTTP	384	GET /favicon.ico HTTP/1.1
258	19.612331266	127.0.0.1	127.0.0.1	TCP	68	80 → 42048 [ACK] Seq=7101 Ack=1010 Win=65280 Len=0 TSval=1080...
259	19.613075116	127.0.0.1	127.0.0.1	HTTP	555	HTTP/1.1 404 Not Found (text/html)
260	19.613128947	127.0.0.1	127.0.0.1	TCP	68	42048 → 80 [ACK] Seq=1010 Ack=7588 Win=65152 Len=0 TSval=1080...
277	24.615095233	127.0.0.1	127.0.0.1	TCP	68	80 → 42048 [FIN, ACK] Seq=7588 Ack=1010 Win=65536 Len=0 TSval=...
278	24.615710451	127.0.0.1	127.0.0.1	TCP	68	42048 → 80 [FIN, ACK] Seq=1010 Ack=7589 Win=65536 Len=0 TSval=...
279	24.615750347	127.0.0.1	127.0.0.1	TCP	68	80 → 42048 [ACK] Seq=7589 Ack=1011 Win=65536 Len=0 TSval=1080...

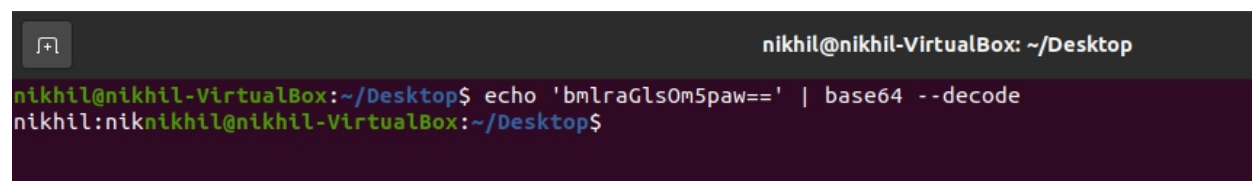
Follow TCP stream



```
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
Authorization: Basic bmlraGlsOm5paw==

HTTP/1.1 200 OK
Date: Mon, 15 Feb 2021 15:48:58 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Mon, 15 Feb 2021 13:01:35 GMT
ETag: "2aa6-5bb5f95f136f8-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 3138
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
```

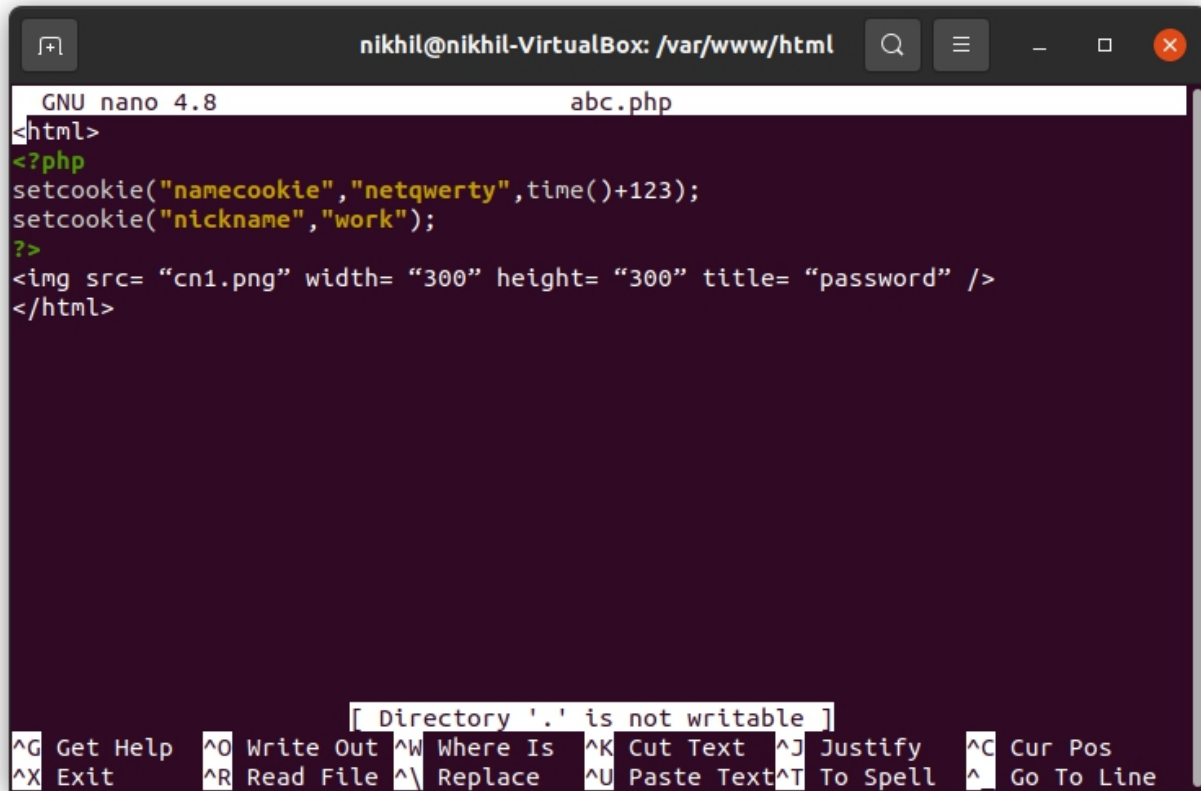
Decoding



```
nikhil@nikhil-VirtualBox: ~/Desktop
nikhil@nikhil-VirtualBox:~/Desktop$ echo 'bmlraGlsOm5paw==' | base64 --decode
nikhil:bniknikhil@nikhil-VirtualBox:~/Desktop$
```

2.Cookie Setting

Create a php file and set cookie and open it in browser.

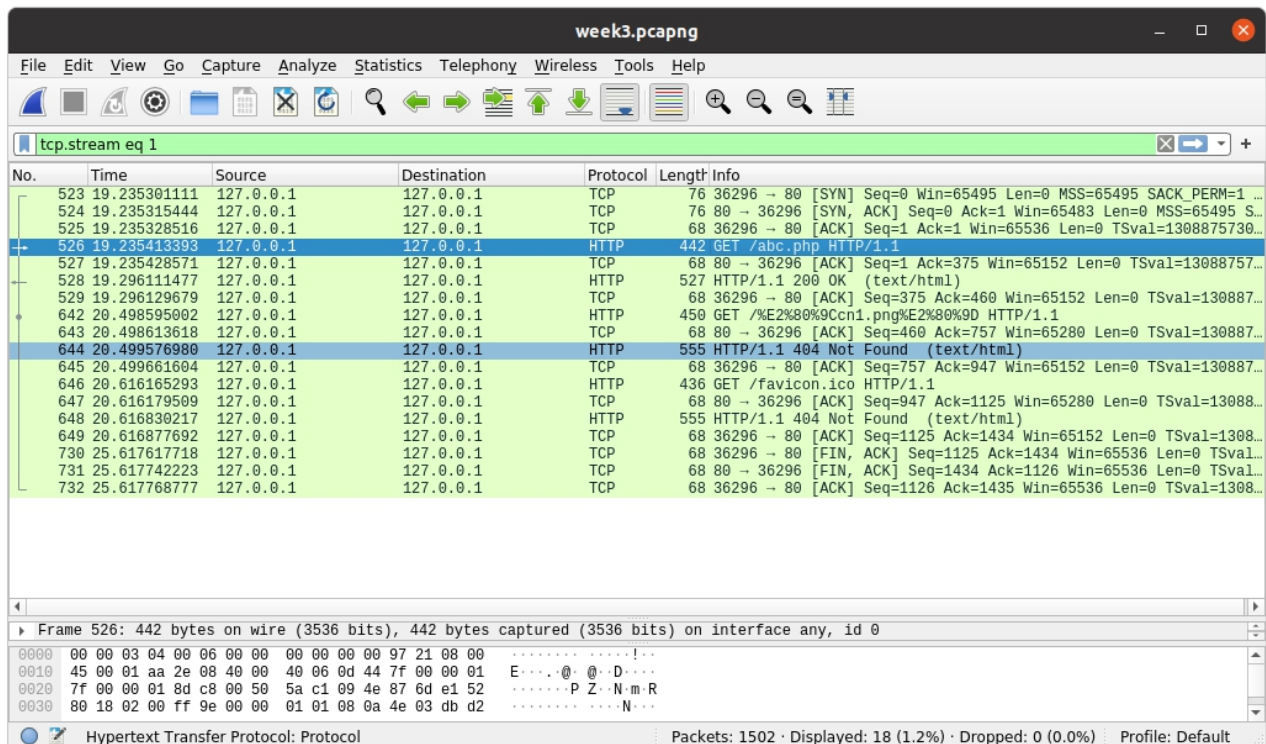


```
GNU nano 4.8 abc.php
<html>
<?php
setcookie("namecookie","netqwerty",time()+123);
setcookie("nickname","work");
?>
<img src= "cn1.png" width= "300" height= "300" title= "password" />
</html>
```

[Directory '.' is not writable]

^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

Capture using wireshark



No.	Time	Source	Destination	Protocol	Length	Info
523	19.235301111	127.0.0.1	127.0.0.1	TCP	76	36296 → 80 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 ...
524	19.235315444	127.0.0.1	127.0.0.1	TCP	76	80 → 36296 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 S...
525	19.235328516	127.0.0.1	127.0.0.1	TCP	68	36296 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1308875730...
526	19.235413393	127.0.0.1	127.0.0.1	HTTP	442	GET /abc.php HTTP/1.1
527	19.235428571	127.0.0.1	127.0.0.1	TCP	68	80 → 36296 [ACK] Seq=1 Ack=375 Win=65152 Len=0 TSval=13088757...
528	19.296111477	127.0.0.1	127.0.0.1	HTTP	527	HTTP/1.1 200 OK (text/html)
529	19.296129679	127.0.0.1	127.0.0.1	TCP	68	36296 → 80 [ACK] Seq=375 Ack=460 Win=65152 Len=0 TSval=130887...
642	20.498595002	127.0.0.1	127.0.0.1	HTTP	450	GET /%E2%80%9Ccn1.png%E2%80%9D HTTP/1.1
643	20.498613618	127.0.0.1	127.0.0.1	TCP	68	80 → 36296 [ACK] Seq=460 Ack=757 Win=65280 Len=0 TSval=130887...
644	20.499576980	127.0.0.1	127.0.0.1	HTTP	555	HTTP/1.1 404 Not Found (text/html)
645	20.499661604	127.0.0.1	127.0.0.1	TCP	68	36296 → 80 [ACK] Seq=757 Ack=947 Win=65152 Len=0 TSval=130887...
646	20.616165293	127.0.0.1	127.0.0.1	HTTP	436	GET /favicon.ico HTTP/1.1
647	20.616179509	127.0.0.1	127.0.0.1	TCP	68	80 → 36296 [ACK] Seq=947 Ack=1125 Win=65280 Len=0 TSval=13088...
648	20.616830217	127.0.0.1	127.0.0.1	HTTP	555	HTTP/1.1 404 Not Found (text/html)
649	20.616877692	127.0.0.1	127.0.0.1	TCP	68	36296 → 80 [ACK] Seq=1125 Ack=1434 Win=65152 Len=0 TSval=1308...
730	25.617617718	127.0.0.1	127.0.0.1	TCP	68	36296 → 80 [FIN, ACK] Seq=1125 Ack=1434 Win=65536 Len=0 TSva...
731	25.617742223	127.0.0.1	127.0.0.1	TCP	68	80 → 36296 [FIN, ACK] Seq=1434 Ack=1126 Win=65536 Len=0 TSva...
732	25.617768777	127.0.0.1	127.0.0.1	TCP	68	36296 → 80 [ACK] Seq=1126 Ack=1435 Win=65536 Len=0 TSval=1308...

Frame 526: 442 bytes on wire (3536 bits), 442 bytes captured (3536 bits) on interface any, id 0

0000 00 00 03 04 00 06 00 00 00 00 00 97 21 08 00!..
0010 45 00 01 aa 2e 08 40 00 40 06 0d 44 7f 00 00 01 E...@. @. D...
0020 7f 00 00 01 8d c8 00 50 5a c1 09 4e 87 6d e1 52P Z. N.m.R
0030 80 18 02 00 ff 9e 00 00 01 01 08 0a 4e 03 db d2N...

Hypertext Transfer Protocol: Protocol Packets: 1502 · Displayed: 18 (1.2%) · Dropped: 0 (0.0%) Profile: Default

Follow TCP Stream

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

```
GET /abc.php 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
Authorization: Basic bmlraGlsOm5paw==

HTTP/1.1 200 OK
Date: Mon, 15 Feb 2021 16:30:52 GMT
Server: Apache/2.4.41 (Ubuntu)
Set-Cookie: namecookie=netqwerty; expires=Mon, 15-Feb-2021 16:32:55 GMT; Max-Age=123
Set-Cookie: nickname=work
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 95
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

.....(.....MW(.J.Ux.0'9.P. /.Q.\.....H #53=..Y.$.$'.P.X\.\_.....
1....4...d...GET /%E2%80%9Ccn1.png%E2%80%9D 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 bmlraGlsOm5paw==
Connection: keep-alive
```

Packet 642. 3 client pkts, 3 server pkts, 5 turns. Click to select.

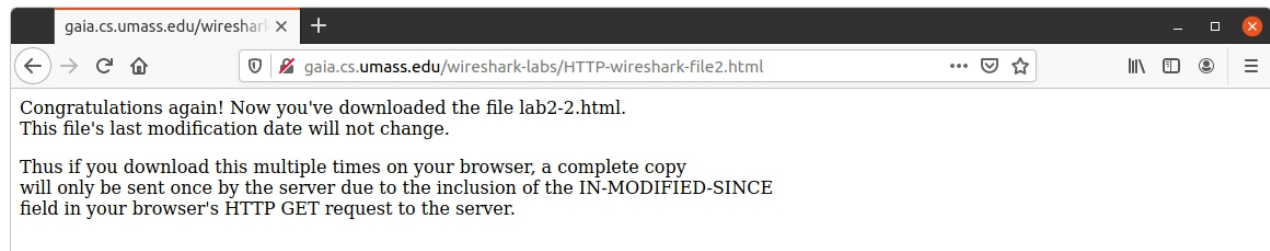
Entire conversation (2,557 bytes) Show and save data as ASCII Stream 1

Find: Find Next

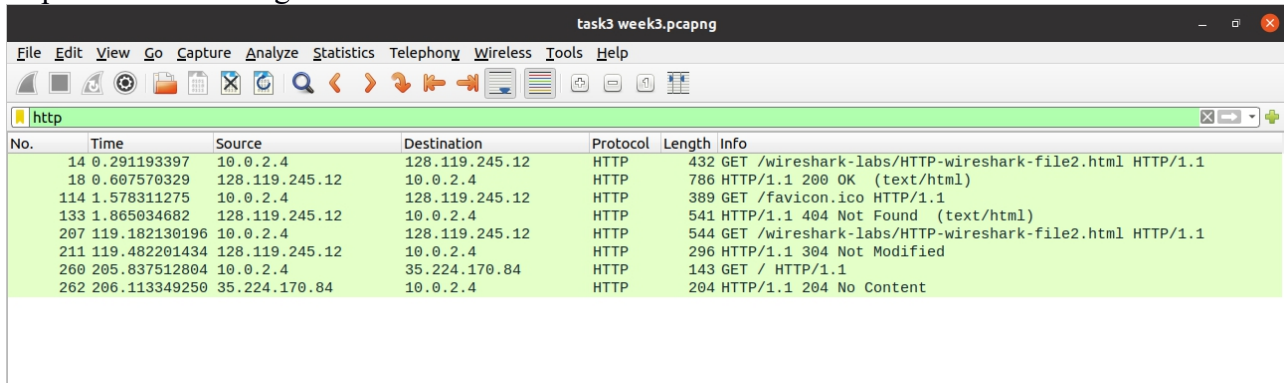
Filter Out This Stream Print Save as... Back Close Help

Conditional Get: If-Modified-Since

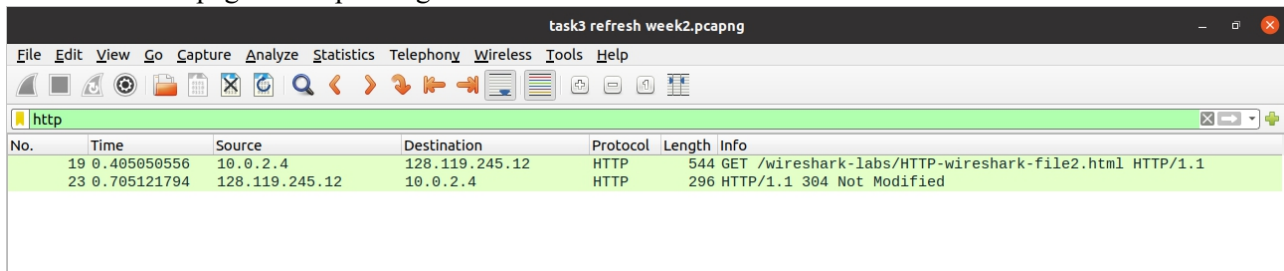
Access the website



Capture Packets using wireshark



Refresh the webpage and capture again



Follow TCP Stream



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?

Ans: No there is no IF-MODIFIED-SINCE line in the GET message, Since it is the first HTTP GET request.

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

Ans: we can see the contents in the Line-based text data field which implies that the server explicitly return the contents of the file.

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 “IF-MODIFIED-SINCE:” header?

Ans: Yes. The information followed is: Mon, 15 Feb 2021 06:59:01 GMT\r\n which is the date of the last modification of the file from the previous get request.

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.

Ans: The status code and phrase returned from the server is “HTTP/1.1 304 Not Modified “ that means the server didn’t return the contents of the file because the browser loaded it from its cache.