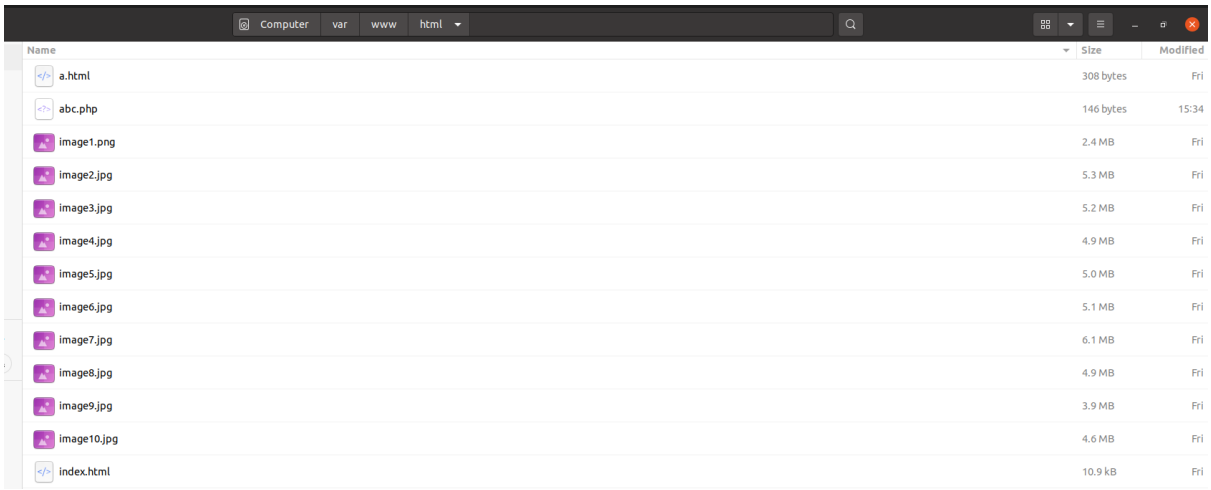
Week 3

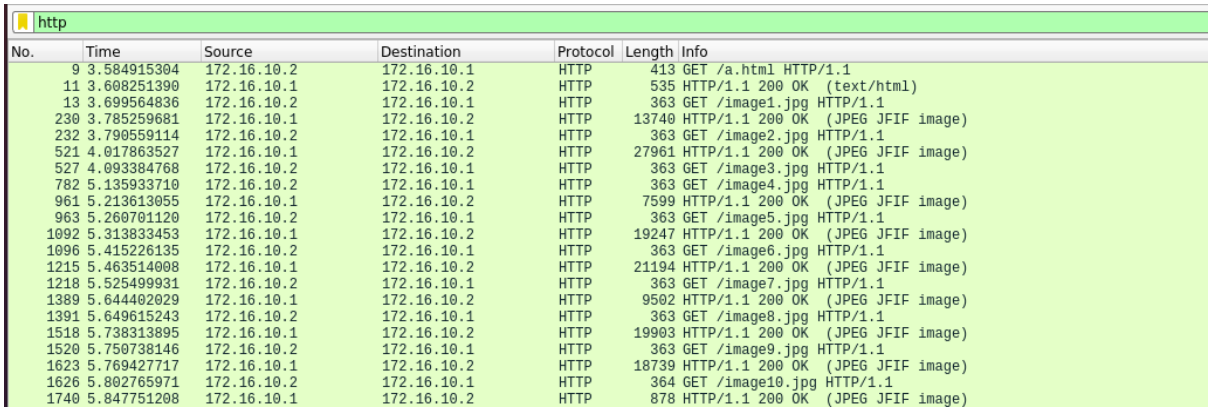
Name : SUNDEEP A	SRN: PES1UG20CS445
SEC: H	ROLL NO : 48

Part a) Understanding Persistent and Non-persistent HTTP Connections



So we can see that the size of each image is more than 2 mb.

For Non – Persistent connection.



http

No.	Time	Source	Destination	Protocol	Length	Info
9	3.584915304	172.16.10.2	172.16.10.1	HTTP	413	GET /a.html HTTP/1.1
11	3.608251390	172.16.10.1	172.16.10.2	HTTP	535	HTTP/1.1 200 OK (text/html)
13	3.699564836	172.16.10.2	172.16.10.1	HTTP	363	GET /image1.jpg HTTP/1.1
230	3.785259681	172.16.10.1	172.16.10.2	HTTP	13740	HTTP/1.1 200 OK (JPEG JFIF image)
232	3.790559114	172.16.10.2	172.16.10.1	HTTP	363	GET /image2.jpg HTTP/1.1
521	4.017863527	172.16.10.1	172.16.10.2	HTTP	27961	HTTP/1.1 200 OK (JPEG JFIF image)
527	4.093384768	172.16.10.2	172.16.10.1	HTTP	363	GET /image3.jpg HTTP/1.1
782	5.135933710	172.16.10.2	172.16.10.1	HTTP	363	GET /image4.jpg HTTP/1.1
961	5.213613055	172.16.10.1	172.16.10.2	HTTP	7599	HTTP/1.1 200 OK (JPEG JFIF image)
963	5.260701120	172.16.10.2	172.16.10.1	HTTP	363	GET /image5.jpg HTTP/1.1
1092	5.313833453	172.16.10.1	172.16.10.2	HTTP	19247	HTTP/1.1 200 OK (JPEG JFIF image)
1096	5.415226135	172.16.10.2	172.16.10.1	HTTP	363	GET /image6.jpg HTTP/1.1
1215	5.463514008	172.16.10.1	172.16.10.2	HTTP	21194	HTTP/1.1 200 OK (JPEG JFIF image)
1218	5.525499931	172.16.10.2	172.16.10.1	HTTP	363	GET /image7.jpg HTTP/1.1
1389	5.644402029	172.16.10.1	172.16.10.2	HTTP	9502	HTTP/1.1 200 OK (JPEG JFIF image)
1391	5.649615243	172.16.10.2	172.16.10.1	HTTP	363	GET /image8.jpg HTTP/1.1
1518	5.738313895	172.16.10.1	172.16.10.2	HTTP	19903	HTTP/1.1 200 OK (JPEG JFIF image)
1520	5.750738146	172.16.10.2	172.16.10.1	HTTP	363	GET /image9.jpg HTTP/1.1
1623	5.769427717	172.16.10.1	172.16.10.2	HTTP	18739	HTTP/1.1 200 OK (JPEG JFIF image)
1626	5.802765971	172.16.10.2	172.16.10.1	HTTP	364	GET /image10.jpg HTTP/1.1
1740	5.847751208	172.16.10.1	172.16.10.2	HTTP	878	HTTP/1.1 200 OK (JPEG JFIF image)

so time taken is = 5.8477 – 3.5849

= 2.2628 seconds

For 2 connections:

http

No.	Time	Source	Destination	Protocol	Length	Info
9	2.343218255	172.16.10.2	172.16.10.1	HTTP	413	GET /a.html HTTP/1.1
11	2.345239639	172.16.10.1	172.16.10.2	HTTP	535	HTTP/1.1 200 OK (text/html)
13	2.438911156	172.16.10.2	172.16.10.1	HTTP	363	GET /image1.jpg HTTP/1.1
148	2.460362619	172.16.10.2	172.16.10.1	HTTP	363	GET /image2.jpg HTTP/1.1
329	2.502584045	172.16.10.1	172.16.10.2	HTTP	28220	HTTP/1.1 200 OK (JPEG JFIF image)
457	2.631884383	172.16.10.2	172.16.10.1	HTTP	363	GET /image3.jpg HTTP/1.1
589	2.664179471	172.16.10.1	172.16.10.2	HTTP	13202	HTTP/1.1 200 OK (JPEG JFIF image)
741	2.740548193	172.16.10.1	172.16.10.2	HTTP	5375	HTTP/1.1 200 OK (JPEG JFIF image)
744	2.785437481	172.16.10.2	172.16.10.1	HTTP	363	GET /image4.jpg HTTP/1.1
911	2.861028283	172.16.10.1	172.16.10.2	HTTP	1807	HTTP/1.1 200 OK (JPEG JFIF image)
913	2.869719261	172.16.10.2	172.16.10.1	HTTP	363	GET /image5.jpg HTTP/1.1
1059	2.947975159	172.16.10.1	172.16.10.2	HTTP	35175	HTTP/1.1 200 OK (JPEG JFIF image)
1062	2.990987741	172.16.10.2	172.16.10.1	HTTP	363	GET /image6.jpg HTTP/1.1
1216	3.035759861	172.16.10.1	172.16.10.2	HTTP	34226	HTTP/1.1 200 OK (JPEG JFIF image)
1220	3.074772722	172.16.10.2	172.16.10.1	HTTP	363	GET /image7.jpg HTTP/1.1
1404	3.134569850	172.16.10.1	172.16.10.2	HTTP	8550	HTTP/1.1 200 OK (JPEG JFIF image)
1409	3.153508923	172.16.10.2	172.16.10.1	HTTP	363	GET /image8.jpg HTTP/1.1
1544	3.178406916	172.16.10.1	172.16.10.2	HTTP	31487	HTTP/1.1 200 OK (JPEG JFIF image)
1549	3.235761389	172.16.10.2	172.16.10.1	HTTP	363	GET /image9.jpg HTTP/1.1
1649	3.257859352	172.16.10.1	172.16.10.2	HTTP	21635	HTTP/1.1 200 OK (JPEG JFIF image)
1652	3.324441976	172.16.10.2	172.16.10.1	HTTP	364	GET /image10.jpg HTTP/1.1
1773	3.375052981	172.16.10.1	172.16.10.2	HTTP	6670	HTTP/1.1 200 OK (JPEG JFIF image)

so time taken is = 3.3750 – 2.3432

= 1.0318 seconds

For 4 connections:

http

No.	Time	Source	Destination	Protocol	Length	Info
6	1.863332709	172.16.10.2	172.16.10.1	HTTP	413	GET /a.html HTTP/1.1
8	1.869573086	172.16.10.1	172.16.10.2	HTTP	535	HTTP/1.1 200 OK (text/html)
10	1.970175098	172.16.10.2	172.16.10.1	HTTP	363	GET /image1.jpg HTTP/1.1
75	1.982608220	172.16.10.2	172.16.10.1	HTTP	363	GET /image2.jpg HTTP/1.1
167	1.991044484	172.16.10.2	172.16.10.1	HTTP	363	GET /image3.jpg HTTP/1.1
181	1.991668095	172.16.10.2	172.16.10.1	HTTP	363	GET /image4.jpg HTTP/1.1
654	2.058956245	172.16.10.1	172.16.10.2	HTTP	3604	HTTP/1.1 200 OK (JPEG JFIF image)
1193	2.260245848	172.16.10.2	172.16.10.1	HTTP	363	GET /image5.jpg HTTP/1.1
1496	2.309008312	172.16.10.1	172.16.10.2	HTTP	30768	HTTP/1.1 200 OK (JPEG JFIF image)
1577	2.325395231	172.16.10.1	172.16.10.2	HTTP	32306	HTTP/1.1 200 OK (JPEG JFIF image)
1714	2.378202751	172.16.10.1	172.16.10.2	HTTP	61239	HTTP/1.1 200 OK (JPEG JFIF image)
1725	2.396902345	172.16.10.1	172.16.10.2	HTTP	22368	HTTP/1.1 200 OK (JPEG JFIF image)
1731	2.429855412	172.16.10.2	172.16.10.1	HTTP	363	GET /image6.jpg HTTP/1.1
1785	2.449575098	172.16.10.2	172.16.10.1	HTTP	363	GET /image7.jpg HTTP/1.1
1830	2.459949084	172.16.10.2	172.16.10.1	HTTP	363	GET /image8.jpg HTTP/1.1
2335	2.681507711	172.16.10.2	172.16.10.1	HTTP	363	GET /image9.jpg HTTP/1.1
2461	2.695936973	172.16.10.1	172.16.10.2	HTTP	35674	HTTP/1.1 200 OK (JPEG JFIF image)
2529	2.721099885	172.16.10.1	172.16.10.2	HTTP	56103	HTTP/1.1 200 OK (JPEG JFIF image)
2626	2.781472675	172.16.10.1	172.16.10.2	HTTP	28875	HTTP/1.1 200 OK (JPEG JFIF image)
2646	2.825374027	172.16.10.1	172.16.10.2	HTTP	64526	HTTP/1.1 200 OK (JPEG JFIF image)
2650	2.883363310	172.16.10.2	172.16.10.1	HTTP	364	GET /image10.jpg HTTP/1.1
2844	2.976016232	172.16.10.1	172.16.10.2	HTTP	438	HTTP/1.1 200 OK (JPEG JFIF image)

so time taken is = 2.9760 – 1.8633

= 1.1127 seconds

For 6 connections:

http

No.	Time	Source	Destination	Protocol	Length	Info
5	0.382108307	172.16.10.2	172.16.10.1	HTTP	413	GET /a.html HTTP/1.1
7	0.384223792	172.16.10.1	172.16.10.2	HTTP	535	HTTP/1.1 200 OK (text/html)
9	0.512286282	172.16.10.2	172.16.10.1	HTTP	363	GET /image1.jpg HTTP/1.1
50	0.517912413	172.16.10.2	172.16.10.1	HTTP	363	GET /image2.jpg HTTP/1.1
150	0.525813452	172.16.10.2	172.16.10.1	HTTP	363	GET /image3.jpg HTTP/1.1
229	0.534042795	172.16.10.2	172.16.10.1	HTTP	363	GET /image4.jpg HTTP/1.1
311	0.543153208	172.16.10.2	172.16.10.1	HTTP	363	GET /image6.jpg HTTP/1.1
327	0.544509944	172.16.10.2	172.16.10.1	HTTP	363	GET /image5.jpg HTTP/1.1
1701	0.787724827	172.16.10.1	172.16.10.2	HTTP	708	HTTP/1.1 200 OK (JPEG JFIF image)
2191	0.884974284	172.16.10.1	172.16.10.2	HTTP	26987	HTTP/1.1 200 OK (JPEG JFIF image)
2294	0.915536241	172.16.10.2	172.16.10.1	HTTP	363	GET /image7.jpg HTTP/1.1
2384	0.922734987	172.16.10.1	172.16.10.2	HTTP	1808	HTTP/1.1 200 OK (JPEG JFIF image)
2484	0.950286215	172.16.10.1	172.16.10.2	HTTP	10586	HTTP/1.1 200 OK (JPEG JFIF image)
2696	1.056373903	172.16.10.1	172.16.10.2	HTTP	18120	HTTP/1.1 200 OK (JPEG JFIF image)
2732	1.085139490	172.16.10.1	172.16.10.2	HTTP	424	HTTP/1.1 200 OK (JPEG JFIF image)
2868	1.213117797	172.16.10.2	172.16.10.1	HTTP	363	GET /image8.jpg HTTP/1.1
2953	1.256831481	172.16.10.2	172.16.10.1	HTTP	363	GET /image9.jpg HTTP/1.1
3082	1.289669645	172.16.10.2	172.16.10.1	HTTP	364	GET /image10.jpg HTTP/1.1
3460	1.400948873	172.16.10.1	172.16.10.2	HTTP	5707	HTTP/1.1 200 OK (JPEG JFIF image)
3541	1.439894305	172.16.10.1	172.16.10.2	HTTP	878	HTTP/1.1 200 OK (JPEG JFIF image)
3559	1.475458981	172.16.10.1	172.16.10.2	HTTP	21351	HTTP/1.1 200 OK (JPEG JFIF image)
3563	1.480412785	172.16.10.1	172.16.10.2	HTTP	25430	HTTP/1.1 200 OK (JPEG JFIF image)

so time taken is = 1.4804 – 0.3821

= 1.0983 seconds

For 8 connections:

http

No.	Time	Source	Destination	Protocol	Length	Info
5	1.223237959	172.16.10.2	172.16.10.1	HTTP	413	GET /a.html HTTP/1.1
7	1.227930886	172.16.10.1	172.16.10.2	HTTP	535	HTTP/1.1 200 OK (text/html)
9	1.304743584	172.16.10.2	172.16.10.1	HTTP	363	GET /image1.jpg HTTP/1.1
24	1.307780857	172.16.10.2	172.16.10.1	HTTP	363	GET /image2.jpg HTTP/1.1
358	1.346745363	172.16.10.2	172.16.10.1	HTTP	363	GET /image3.jpg HTTP/1.1
421	1.354198173	172.16.10.2	172.16.10.1	HTTP	363	GET /image4.jpg HTTP/1.1
608	1.370166610	172.16.10.2	172.16.10.1	HTTP	363	GET /image8.jpg HTTP/1.1
609	1.370462341	172.16.10.2	172.16.10.1	HTTP	363	GET /image7.jpg HTTP/1.1
614	1.370857771	172.16.10.2	172.16.10.1	HTTP	363	GET /image6.jpg HTTP/1.1
633	1.371844213	172.16.10.2	172.16.10.1	HTTP	363	GET /image5.jpg HTTP/1.1
1535	1.456559604	172.16.10.1	172.16.10.2	HTTP	18084	HTTP/1.1 200 OK (JPEG JFIF image)
2789	1.721200758	172.16.10.2	172.16.10.1	HTTP	363	GET /image9.jpg HTTP/1.1
3386	1.830416252	172.16.10.1	172.16.10.2	HTTP	16851	HTTP/1.1 200 OK (JPEG JFIF image)
3626	1.867030406	172.16.10.1	172.16.10.2	HTTP	5376	HTTP/1.1 200 OK (JPEG JFIF image)
3696	1.889656223	172.16.10.1	172.16.10.2	HTTP	6152	HTTP/1.1 200 OK (JPEG JFIF image)
3768	1.906574144	172.16.10.1	172.16.10.2	HTTP	5432	HTTP/1.1 200 OK (JPEG JFIF image)
4000	1.988158248	172.16.10.1	172.16.10.2	HTTP	13482	HTTP/1.1 200 OK (JPEG JFIF image)
4316	2.112717818	172.16.10.1	172.16.10.2	HTTP	9768	HTTP/1.1 200 OK (JPEG JFIF image)
4344	2.139268446	172.16.10.1	172.16.10.2	HTTP	8603	HTTP/1.1 200 OK (JPEG JFIF image)
4397	2.256762276	172.16.10.1	172.16.10.2	HTTP	2263	HTTP/1.1 200 OK (JPEG JFIF image)
4405	2.380836746	172.16.10.2	172.16.10.1	HTTP	364	GET /image10.jpg HTTP/1.1
4630	2.464985252	172.16.10.1	172.16.10.2	HTTP	3774	HTTP/1.1 200 OK (JPEG JFIF image)

so time taken is = 2.4649 – 1.2232
= 1.2417 seconds

For 10 connections:

http

No.	Time	Source	Destination	Protocol	Length	Info
15	2.357150712	172.16.10.2	172.16.10.1	HTTP	413	GET /a.html HTTP/1.1
17	2.363076283	172.16.10.1	172.16.10.2	HTTP	535	HTTP/1.1 200 OK (text/html)
19	2.433833833	172.16.10.2	172.16.10.1	HTTP	363	GET /image1.jpg HTTP/1.1
36	2.441194312	172.16.10.2	172.16.10.1	HTTP	363	GET /image2.jpg HTTP/1.1
100	2.445916557	172.16.10.2	172.16.10.1	HTTP	363	GET /image3.jpg HTTP/1.1
354	2.471597996	172.16.10.2	172.16.10.1	HTTP	363	GET /image4.jpg HTTP/1.1
370	2.473229815	172.16.10.2	172.16.10.1	HTTP	363	GET /image5.jpg HTTP/1.1
528	2.488878379	172.16.10.2	172.16.10.1	HTTP	363	GET /image6.jpg HTTP/1.1
759	2.513506498	172.16.10.2	172.16.10.1	HTTP	363	GET /image7.jpg HTTP/1.1
777	2.516166134	172.16.10.2	172.16.10.1	HTTP	363	GET /image8.jpg HTTP/1.1
787	2.518513997	172.16.10.2	172.16.10.1	HTTP	363	GET /image9.jpg HTTP/1.1
1119	2.543412927	172.16.10.2	172.16.10.1	HTTP	364	GET /image10.jpg HTTP/1.1
3508	2.900938623	172.16.10.1	172.16.10.2	HTTP	7948	HTTP/1.1 200 OK (JPEG JFIF image)
4403	3.033706239	172.16.10.1	172.16.10.2	HTTP	40176	HTTP/1.1 200 OK (JPEG JFIF image)
4492	3.050155675	172.16.10.1	172.16.10.2	HTTP	5708	HTTP/1.1 200 OK (JPEG JFIF image)
4799	3.125451581	172.16.10.1	172.16.10.2	HTTP	9048	HTTP/1.1 200 OK (JPEG JFIF image)
4856	3.145600968	172.16.10.1	172.16.10.2	HTTP	2480	HTTP/1.1 200 OK (JPEG JFIF image)
4912	3.173202181	172.16.10.1	172.16.10.2	HTTP	6242	HTTP/1.1 200 OK (JPEG JFIF image)
4946	3.176749125	172.16.10.1	172.16.10.2	HTTP	424	HTTP/1.1 200 OK (JPEG JFIF image)
4987	3.198000934	172.16.10.1	172.16.10.2	HTTP	6715	HTTP/1.1 200 OK (JPEG JFIF image)
4991	3.203604503	172.16.10.1	172.16.10.2	HTTP	2519	HTTP/1.1 200 OK (JPEG JFIF image)
5067	3.269489874	172.16.10.1	172.16.10.2	HTTP	19703	HTTP/1.1 200 OK (JPEG JFIF image)

so time taken is = 3.2694 – 2.3571
= 0.9123 seconds

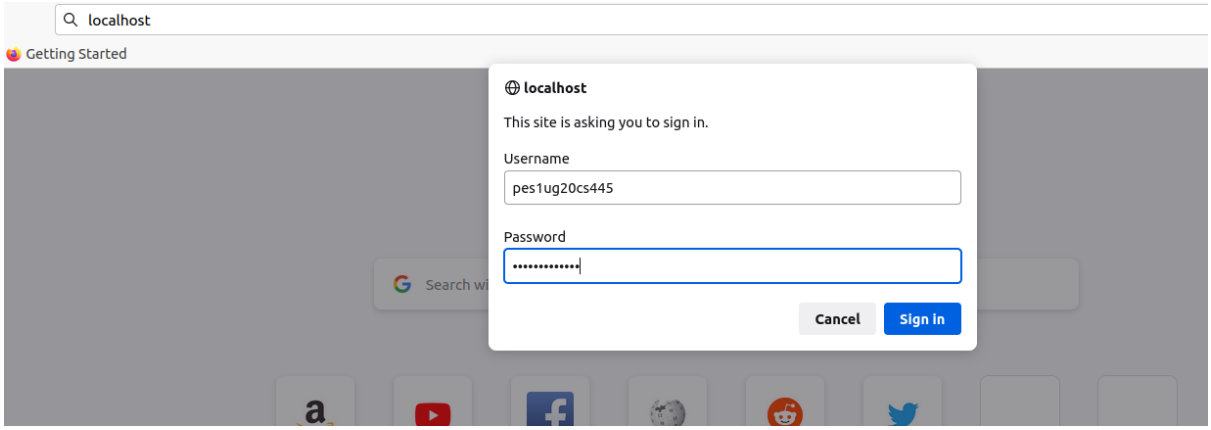
OBSERVATION:

Therefore, the best load time for this particular html page is obtained with **10 persistent connections**. For this particular html page 10 persistent connections takes least amount of time because it can request all the 10 images at once. As a result, the load time is reduced.

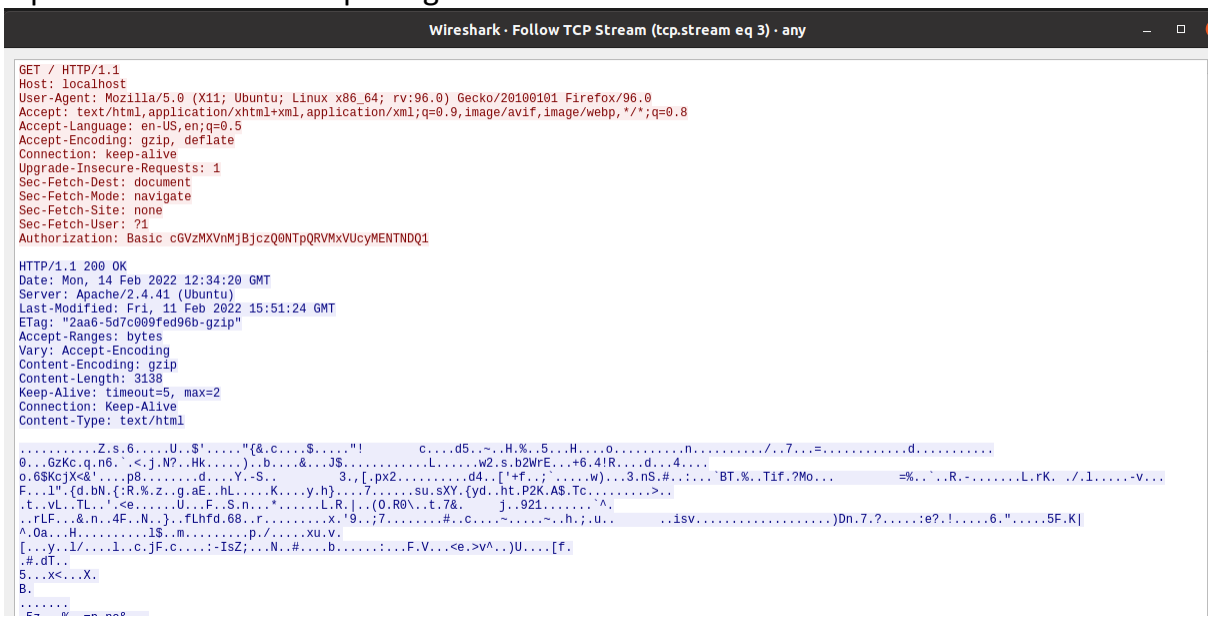
PART B) Understand working of HTTP Headers

Authentication:

Here we are accessing the localhost using the username and password set during the authentication process.

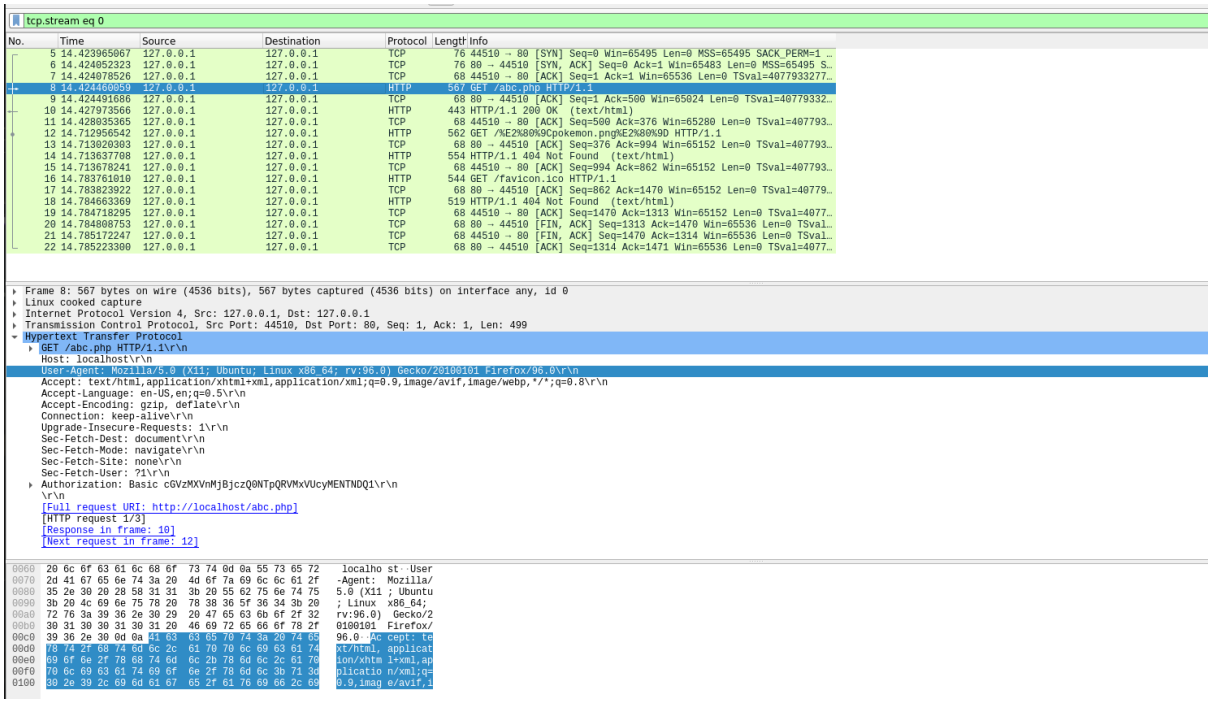


tcp stream content on opening localhost on the web browser:



Cookie setting:

We are opening the abc.php file on the local host. And trying to capture the packets on wireshark.



In the below image we can see that , by using the “follow TCP stream “ on the HTTP message. In the authentication section the password is retrieved and it is encrypted by base 64 algorithm.

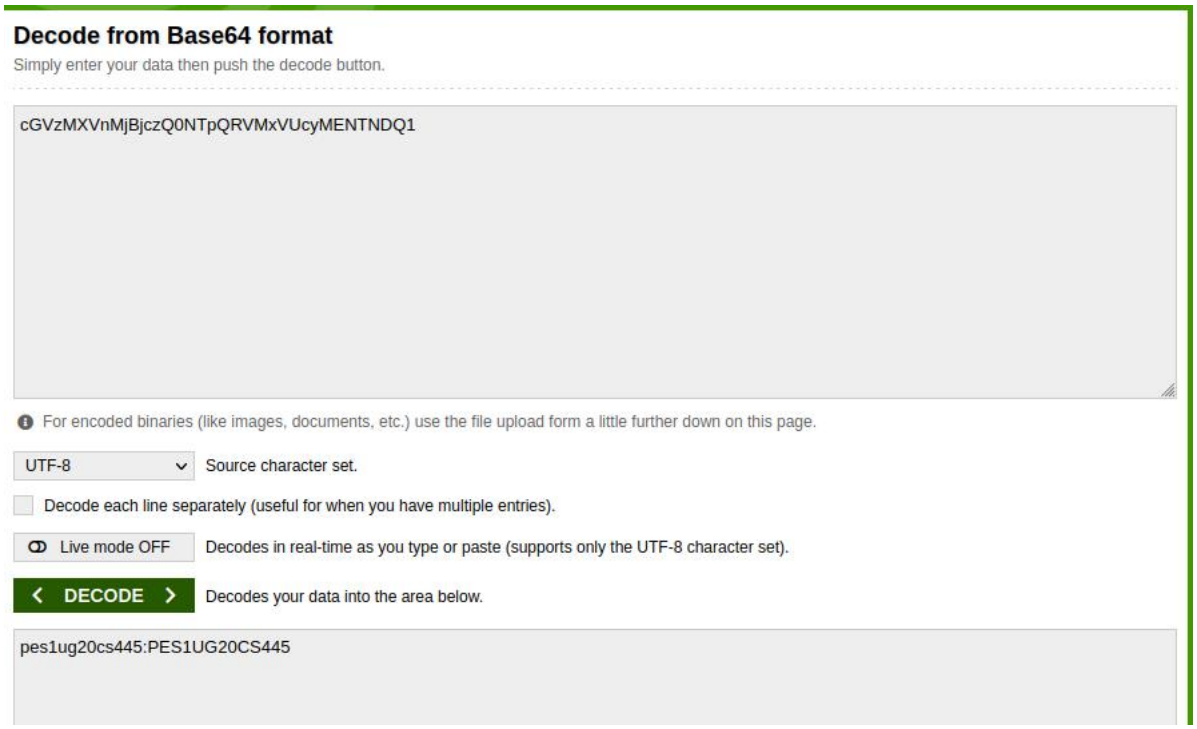
We can also see that , the cookies have been successfully set.
We can see information like namecookie : netqwerty, it expires on 14th Feb-2022; Max-Age=123 seconds

```
GET /abc.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Authorization: Basic cGVzMXVnMjBjczQ0NTpQRVMxVUcyMENTNDQ1

HTTP/1.1 200 OK
Date: Mon, 14 Feb 2022 09:20:08 GMT
Server: Apache/2.4.41 (Ubuntu)
Set-Cookie: namecookie=netqwerty; expires=Mon, 14-Feb-2022 09:22:11 GMT; Max-Age=123
Set-Cookie: nickname=work
Content-Length: 60
Keep-Alive: timeout=5, max=2
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8


<html>
</body>
<img src= ...pokemon.png...>
<body>
</html>
GET /%E2%80%9Cpokemon.png%E2%80%9D HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Basic cGVzMXVnMjBjczQ0NTpQRVMxVUcyMENTNDQ1
Connection: keep-alive
Referer: http://localhost/abc.php
Cookie: namecookie=netqwerty; nickname=work
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
```

In the below image we can see that the details which were encrypted by base64 algorithm are decrypted.
Encrypted form : cGVzMXVnMjBjczQ0NTpQRVMxVUcyMENTNDQ1
Decrypted form: pes1ug20cs445:PES1UG20CS445 [username:password]



Conditional Get: If-Modified-Since

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** there is no line called “IF-MODIFIED-SINCE”.

2.. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
=> **Yes the server explicitly retuned the contents of the file.** We can say that because in the below image we can see the html contents in the **request packet.**
we can see the text data fetched by the request packet.

```
http
No.  Time            Source          Destination     Protocol Length Info
21   6.524315395     192.168.100.137 128.119.245.12  HTTP     443    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
25   6.898340115     128.119.245.12  192.168.100.137 HTTP     786    HTTP/1.1 200 OK  (text/html)
49   7.129691899     192.168.100.137 128.119.245.12  HTTP     400    GET /favicon.ico HTTP/1.1
54   7.504346018     128.119.245.12  192.168.100.137 HTTP     541    HTTP/1.1 404 Not Found  (text/html)
65   10.135583237    192.168.100.137 128.119.245.12  HTTP     555    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
69   10.499250832    128.119.245.12  192.168.100.137 HTTP     295    HTTP/1.1 304 Not Modified

Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        [HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Mon, 14 Feb 2022 10:57:49 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.27 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Mon, 14 Feb 2022 06:59:01 GMT\r\n
    ETag: "173-5d7f4f38db802"\r\n
    Accept-Ranges: bytes\r\n
  Content-Length: 371\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.374024720 seconds]
    [Request in frame: 21]
    [Next request in frame: 65]
    [Next response in frame: 69]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    File Data: 371 bytes
Line-based text data: text/html (10 lines)
    \n
    <html>\n
    \n
    Congratulations again!  Now you've downloaded the file lab2-2.html. <br>\n
    This file's last modification date will not change.  <p>\n
    Thus  if you download this multiple times on your browser, a complete copy <br>\n
    will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
    field in your browser's HTTP GET request to the server.\n
    \n
    </html>\n
```

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?

=>**yes** we can see the line “IF-MODIFIED-SINCE:”.

The information that follows the header is Mon, 14 Feb 2022 06:59:01 GMT\r\n

```
65   10.135583237    192.168.100.137 128.119.245.12  HTTP     555    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
69   10.499250832    128.119.245.12  192.168.100.137 HTTP     295    HTTP/1.1 304 Not Modified

    [Next sequence number: 887    (relative sequence number)]
    Acknowledgment number: 731    (relative ack number)
    Acknowledgment number (raw): 1253532666
    0101 .... = Header Length: 20 bytes (5)
  Flags: 0x018 (PSH, ACK)
    Window size value: 63510
    [Calculated window size: 63510]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x9cc3 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  [SEQ/ACK analysis]
  [Timestamps]
    TCP payload (499 bytes)
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]
        [GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      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:96.0) Gecko/20100101 Firefox/96.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    If-Modified-Since: Mon, 14 Feb 2022 06:59:01 GMT\r\n
    If-None-Match: "173-5d7f4f38db802"\r\n
```

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.

=>HTTP status code: 304

Phrase returned: Not modified

```
69 10.499250832  128.119.245.12   192.168.100.137   HTTP   295 HTTP/1.1 304 Not Modified
    Sequence number: 731    (relative sequence number)
    Sequence number (raw): 1253532666
    [Next sequence number: 970    (relative sequence number)]
    Acknowledgment number: 887    (relative ack number)
    Acknowledgment number (raw): 3595321309
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x018 (PSH, ACK)
    Window size value: 64240
    [Calculated window size: 64240]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x9134 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ [SEQ/ACK analysis]
  ▸ [Timestamps]
    TCP payload (239 bytes)
▾ Hypertext Transfer Protocol
  ▾ HTTP/1.1 304 Not Modified\r\n
    ▾ [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
        [HTTP/1.1 304 Not Modified\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 304
      [Status Code Description: Not Modified]
      Response Phrase: Not Modified
    Date: Mon, 14 Feb 2022 10:57:53 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.27 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=99\r\n
    ETag: "173-5d7f4f38db802"\r\n
    \r\n
```

The server did not explicitly return the contents of the file. We can confirm this as there is no " Content-type" header present. This occurs because the html file is taken from the web cache as the same html file was requested in the previous get request.

Repeat the above task with some images on the server.

```
32 18.316480549  127.0.0.1   127.0.0.1   HTTP   571 GET /pokemon.png HTTP/1.1
49 18.364213313  127.0.0.1   127.0.0.1   HTTP   8059 HTTP/1.1 200 OK  (PNG)
54 19.175494845  127.0.0.1   127.0.0.1   HTTP   503 GET /favicon.ico HTTP/1.1
56 19.177531673  127.0.0.1   127.0.0.1   HTTP   554 HTTP/1.1 404 Not Found  (text/html)
62 23.242805087  127.0.0.1   127.0.0.1   HTTP   685 GET /pokemon.png HTTP/1.1
64 23.244834878  127.0.0.1   127.0.0.1   HTTP   214 HTTP/1.1 304 Not Modified
    Sequence number: 1    (relative sequence number)
    Sequence number (raw): 3697303109
    [Next sequence number: 504    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Acknowledgment number (raw): 1269576053
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x018 (PSH, ACK)
    Window size value: 512
    [Calculated window size: 65536]
    [Window size scaling factor: 128]
    Checksum: 0x0020 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▸ [SEQ/ACK analysis]
  ▸ [Timestamps]
    TCP payload (503 bytes)
▾ Hypertext Transfer Protocol
  ▾ GET /pokemon.png HTTP/1.1\r\n
    ▸ [Expert Info (Chat/Sequence): GET /pokemon.png HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /pokemon.png
      Request Version: HTTP/1.1
    Host: localhost\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Sec-Fetch-Dest: document\r\n
    Sec-Fetch-Mode: navigate\r\n
    Sec-Fetch-Site: none\r\n
    Sec-Fetch-User: ?1\r\n
  ▸ Authorization: Basic cGVzMXVnMjBjczQ0NTpQRVMxVUcyMENTNDQ1\r\n
    \r\n
    [Full request URI: http://localhost/pokemon.png]
    [HTTP request 1/3]
    [Response in frame: 49]
    [Next request in frame: 54]
```

So the first HTTP GET request has no line called "IF-MODIFIED-SINCE".

2.. from the below image we can see that the content length is 302615\r\n. and it contains information like Image header , Image data chunk,etc.
So we can say that the server explicitly returned the contents of the file

```
32 18.316480549  127.0.0.1   127.0.0.1   HTTP   571 GET /pokemon.png HTTP/1.1
49 18.364213313  127.0.0.1   127.0.0.1   HTTP  8059 HTTP/1.1 200 OK  (PNG)
54 19.175494845  127.0.0.1   127.0.0.1   HTTP   503 GET /favicon.ico HTTP/1.1
56 19.177531673  127.0.0.1   127.0.0.1   HTTP   554 HTTP/1.1 404 Not Found  (text/html)
[illegible]42805087  127.0.0.1   127.0.0.1   HTTP   685 GET /pokemon.png HTTP/1.1
Rhythmbox [illegible]44834878  127.0.0.1   127.0.0.1   HTTP   214 HTTP/1.1 304 Not Modified

    [Window size scaling factor: 128]
    Checksum: 0x1d60 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▸ [SEQ/ACK analysis]
  ▸ [Timestamps]
    TCP payload (7991 bytes)
    TCP segment data (7991 bytes)
▸ [10 Reassembled TCP Segments (302903 bytes): #34(32768), #36(32768), #38(32768), #40(32768), #41(32768), #44(32768), #45(32768), #47(32768), #48(32768), #49(7991)]
▾ Hypertext Transfer Protocol
  ▾ HTTP/1.1 200 OK\r\n
    ▸ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Mon, 14 Feb 2022 11:49:42 GMT\r\n
    Server: Apache/2.4.41 (Ubuntu)\r\n
    Last-Modified: Sat, 12 Feb 2022 09:00:13 GMT\r\n
    ETag: "49e17-5d7ce6954ac1d"\r\n
    Accept-Ranges: bytes\r\n
  ▸ Content-Length: 302615\r\n
    Keep-Alive: timeout=5, max=2\r\n
    Connection: Keep-Alive\r\n
    Content-Type: image/png\r\n
    \r\n
    [HTTP response 1/3]
    [Time since request: 0.047732764 seconds]
    [Request in frame: 32]
    [Next request in frame: 54]
    [Next response in frame: 56]
    [Request URI: http://localhost/pokemon.png]
    File Data: 302615 bytes
▾ Portable Network Graphics
    PNG Signature: 89504e470d0a1a0a
  ▸ Image Header (IHDR)
  ▸ Image data chunk (IDAT)
  ▸ Image Trailer (IEND)
```

3.. it contains an “IF-MODIFIED-SINCE” line.

```
32 18.316480549  127.0.0.1   127.0.0.1   HTTP   571 GET /pokemon.png HTTP/1.1
49 18.364213313  127.0.0.1   127.0.0.1   HTTP  8059 HTTP/1.1 200 OK  (PNG)
54 19.175494845  127.0.0.1   127.0.0.1   HTTP   503 GET /favicon.ico HTTP/1.1
56 19.177531673  127.0.0.1   127.0.0.1   HTTP   554 HTTP/1.1 404 Not Found  (text/html)
62 23.242805087  127.0.0.1   127.0.0.1   HTTP   685 GET /pokemon.png HTTP/1.1
64 23.244834878  127.0.0.1   127.0.0.1   HTTP   214 HTTP/1.1 304 Not Modified

    Acknowledgment number (raw): 1269879442
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x018 (PSH, ACK)
    Window size value: 6140
    [Calculated window size: 785920]
    [Window size scaling factor: 128]
    Checksum: 0x0092 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▸ [SEQ/ACK analysis]
  ▸ [Timestamps]
    TCP payload (617 bytes)
▾ Hypertext Transfer Protocol
  ▾ GET /pokemon.png HTTP/1.1\r\n
    ▸ [Expert Info (Chat/Sequence): GET /pokemon.png HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /pokemon.png
      Request Version: HTTP/1.1
    Host: localhost\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
  ▸ Authorization: Basic cGVzMXVnMjBjczQ0NTpQRVMxVUcyMENTNDQ1\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Sec-Fetch-Dest: document\r\n
    Sec-Fetch-Mode: navigate\r\n
    Sec-Fetch-Site: none\r\n
    Sec-Fetch-User: ?1\r\n
    If-Modified-Since: Sat, 12 Feb 2022 09:00:13 GMT\r\n
    If-None-Match: "49e17-5d7ce6954ac1d"\r\n
    Cache-Control: max-age=0\r\n
    \r\n
    [Full request URI: http://localhost/pokemon.png]
    [HTTP request 3/3]
    [Prev request in frame: 54]
    [Response in frame: 64]
```

4.. HTTP status code: 304

Phrase returned: Not modified

The server didn’t explicitly return the contents of the file . because the contents of the file have been fetched from the web cache as the same image was requested earlier.

32	18.316480549	127.0.0.1	127.0.0.1	HTTP	571	GET /pokemon.png HTTP/1.1
49	18.364213313	127.0.0.1	127.0.0.1	HTTP	8059	HTTP/1.1 200 OK (PNG)
54	19.175494845	127.0.0.1	127.0.0.1	HTTP	503	GET /favicon.ico HTTP/1.1
56	19.177531673	127.0.0.1	127.0.0.1	HTTP	554	HTTP/1.1 404 Not Found (text/html)
62	23.242805087	127.0.0.1	127.0.0.1	HTTP	685	GET /pokemon.png HTTP/1.1
64	23.244834878	127.0.0.1	127.0.0.1	HTTP	214	HTTP/1.1 304 Not Modified

```
    Source Port: 80
    Destination Port: 44552
    [Stream index: 2]
    [TCP Segment Len: 146]
    Sequence number: 303390    (relative sequence number)
    Sequence number (raw): 1269879442
    [Next sequence number: 303536    (relative sequence number)]
    Acknowledgment number: 1556    (relative ack number)
    Acknowledgment number (raw): 3697304664
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x018 (PSH, ACK)
    Window size value: 512
    [Calculated window size: 65536]
    [Window size scaling factor: 128]
    Checksum: 0xfeba [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▸ [SEQ/ACK analysis]
  ▸ [Timestamps]
    TCP payload (146 bytes)
▾ 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: Mon, 14 Feb 2022 11:49:47 GMT\r\n
    Server: Apache/2.4.41 (Ubuntu)\r\n
    Connection: close\r\n
    ETag: "49e17-5d7ce6954ac1d"\r\n
    \r\n
    [HTTP response 3/3]
    [Time since request: 0.002029791 seconds]
    [Prev request in frame: 54]
    [Prev response in frame: 56]
    [Request in frame: 62]
    [Request URI: http://localhost/pokemon.png]
```