

Computer Networks Lab- Week3

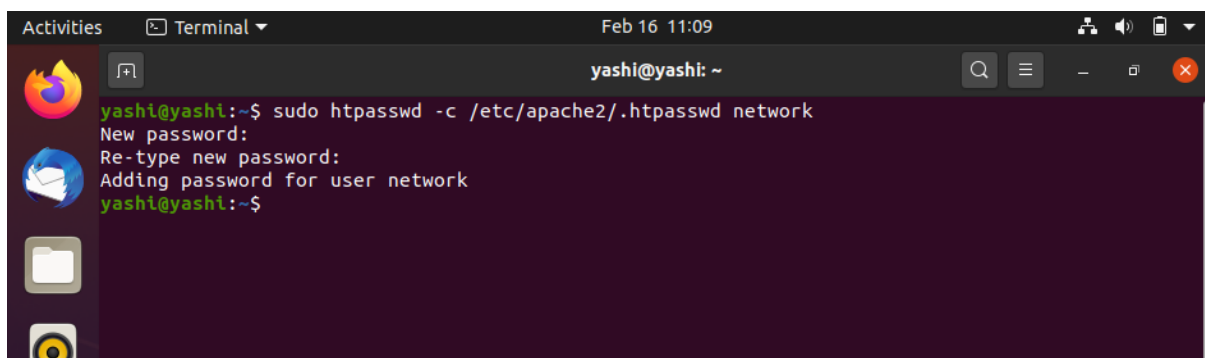
PES1UG19CS592

Yashi Chawla

1 Password Authentication

1.1 Password Generation

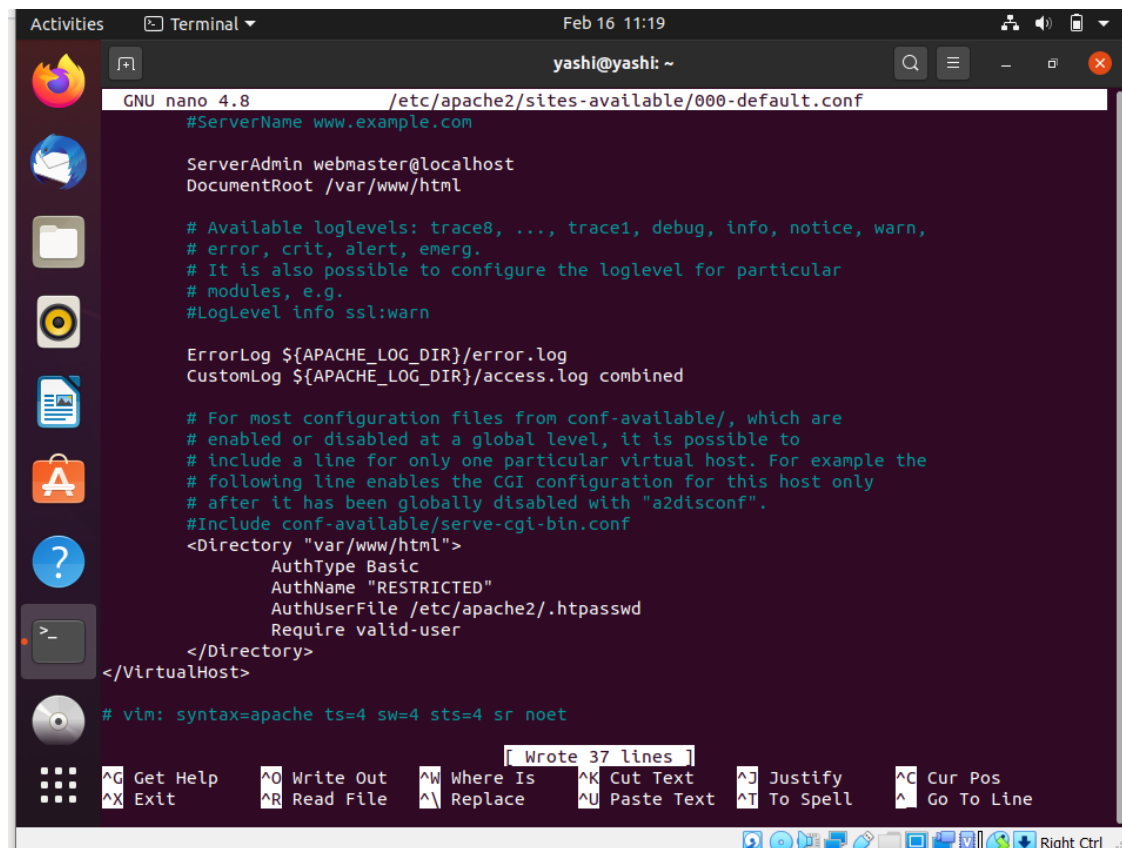
- To enable basic authentication for HTTP, we need to generate a password file. This file can be generated using the htpasswd command.
- Using the `sudo htpasswd -c /etc/apache2/.htpasswd username` we can set a password for the given user username and write it into the .htpasswd configuration file.
- The cat command can be used to view the encrypted password file, which is encrypted using the Data Encryption Standard algorithm.



```
Activities Terminal Feb 16 11:09
yashi@yashi: ~
yashi@yashi:~$ sudo htpasswd -c /etc/apache2/.htpasswd network
New password:
Re-type new password:
Adding password for user network
yashi@yashi:~$
```

1.2 Apache Server Authentication

- To enable password authentication in the server, we need to modify the Apache configuration file.
- This can be done using `sudo nano /etc/apache2/sites-available/000-default.conf`
- Password authentication is added to the /var/www/html directory which is the localhost home directory so that all files hosted here will require authentication to access.
- To activate the authentication and policy, we need to restart the server using `sudo service apache2 restart`.



```
GNU nano 4.8 /etc/apache2/sites-available/000-default.conf
#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

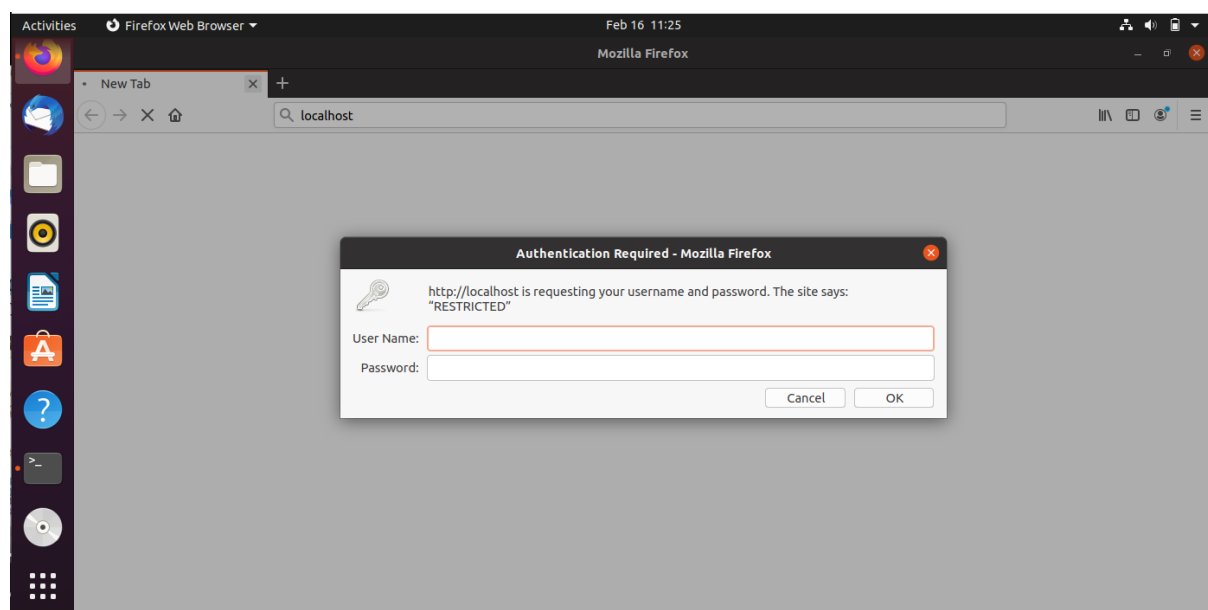
# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example the
# following line enables the CGI configuration for this host only
# after it has been globally disabled with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

[ Wrote 37 lines ]
^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
```

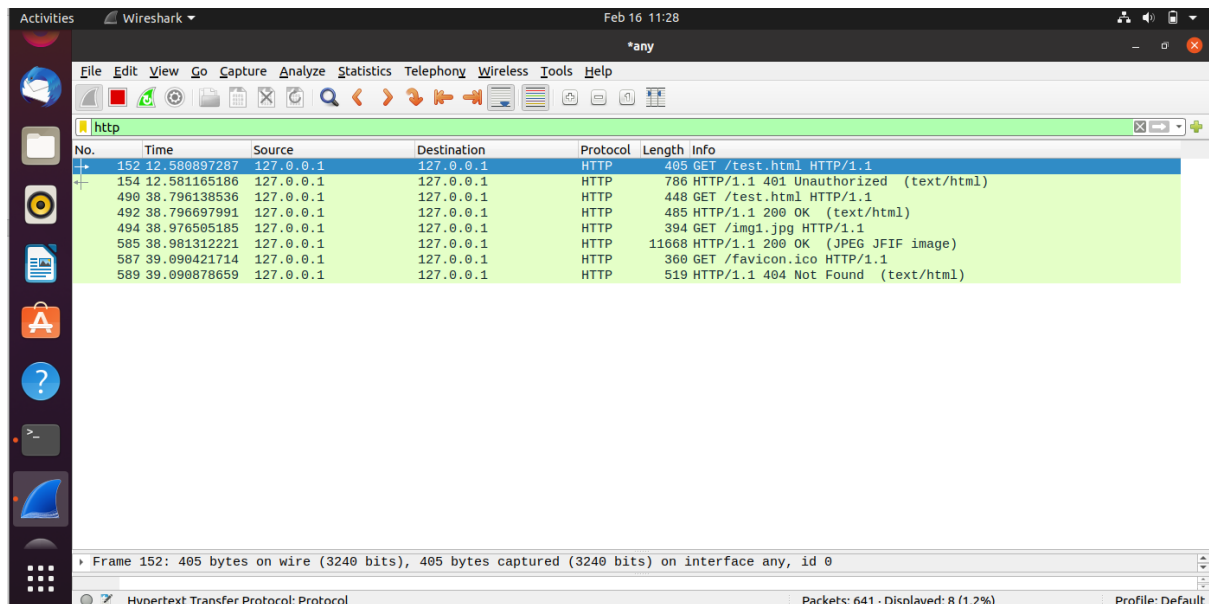
1.3 Accessing Localhost

- We can now access localhost only after entering the username and password set earlier
- These credentials are entered on the browser window.



1.4 Wireshark Packet Capture

Wireshark can be used to capture the packets sent on the network. The first GET request corresponding to the HTML file is analysed and its TCP stream is expanded, and parameters examined.



1.5 Decrypting Base64 Encryption

- We can observe that the Authorization field stores the password we had entered to access localhost.
- This password is encrypted using the Base64 algorithm before it is transmitted along the network.
 - Each character is converted into 8-bit binary ASCII representation

- Group these bits into chunks of 6-bits.
- Convert these chunks into their decimal equivalent and assign the corresponding Base64 character
- The Base64 algorithm supports the use of lowercase as well as uppercase alphabets, all digits from 0 to 9 and the special characters + and / only.
- Similarly, Base64 is decoded by obtaining the 6-bit binary chunks for each character, grouping them into chunks of 8-bits and then converting into their corresponding character

Thus, bmV0d29yazp5YXNoaQ==

can be converted to a 6-bit binary equivalent and then those binary equivalents can be grouped together and then decode to ASCII, giving us,

network:yashi

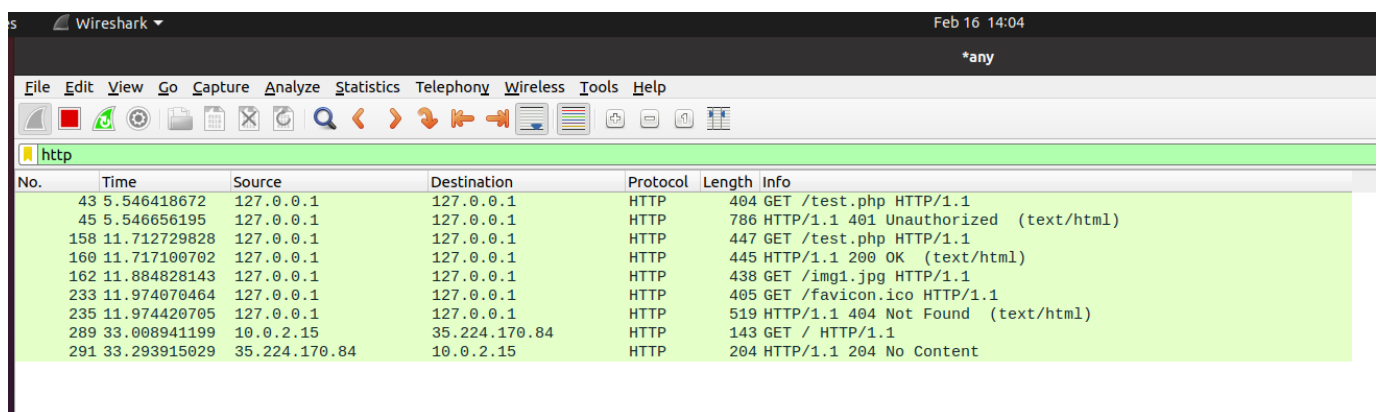
2 Setting Cookies

2.1 Setting Cookies with PHP

- We can set cookies using a PHP script and setcookie(name,value, expire_time) function
- When this file is required by the browser a cookie will be set.

2.2 Wireshark Capture

- Wireshark can be used to capture the packets sent on the network. The first GET request corresponding to the PHP file is analysed and its TCP Stream is expanded and examined.
- The Cookie name, value and the associated parameters can be viewed under the HTTP header Set-Cookie.
- We can observe the name, value, and the expiry time of the set cookie, if the cookie has not already expired.



No.	Time	Source	Destination	Protocol	Length	Info
43	5.546418672	127.0.0.1	127.0.0.1	HTTP	404	GET /test.php HTTP/1.1
45	5.546656195	127.0.0.1	127.0.0.1	HTTP	786	HTTP/1.1 401 Unauthorized (text/html)
158	11.712729828	127.0.0.1	127.0.0.1	HTTP	447	GET /test.php HTTP/1.1
160	11.717100702	127.0.0.1	127.0.0.1	HTTP	445	HTTP/1.1 200 OK (text/html)
162	11.884828143	127.0.0.1	127.0.0.1	HTTP	438	GET /img1.jpg HTTP/1.1
233	11.974070464	127.0.0.1	127.0.0.1	HTTP	405	GET /favicon.ico HTTP/1.1
235	11.974420705	127.0.0.1	127.0.0.1	HTTP	519	HTTP/1.1 404 Not Found (text/html)
289	33.008941199	10.0.2.15	35.224.170.84	HTTP	143	GET / HTTP/1.1
291	33.293915029	35.224.170.84	10.0.2.15	HTTP	204	HTTP/1.1 204 No Content

```

GET /test.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0
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 bmV0d29yazp5YXNoaQ==

HTTP/1.1 200 OK
Date: Tue, 16 Feb 2021 08:32:48 GMT
Server: Apache/2.4.41 (Ubuntu)
Set-Cookie: CookieName=Netqwert; expires=Tue, 16-Feb-2021 08:34:51 GMT; Max-Age=123
Set-Cookie: Nickname=work
Content-Length: 62
Keep-Alive: timeout=5, max=2
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<html>

</html>
GET /img1.jpg HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Basic bmV0d29yazp5YXNoaQ==
3 client pkts, 45 server pkts, 5 turns.

```

Entire conversation (1,619 kB) Show and save data as ASCII Stream 13

3. Conditional GET

- A conditional HTTP response is one that carries the resource only it had been modified since the last GET request by the client.
- The HTTP header If-Modified-Since is one way to implement Conditional GET
- The server checks the If-Modified-Since header value and resends the resource only if it has been modified since the timestamp in the header
- If it has not been modified, a 304 Not Modified status code is sent back.

3.1 Repeat Requests for HTML Page

- An HTML page is requested by the client and the HTML file is obtained along with a 200 OK response status
- Immediately, the request is made again either by refreshing or accessing it via a browser tab
- The second response from the server is obtained as 304 Not Modified since the resource has not been modified since the last GET.

No.	Time	Source	Destination	Protocol	Length	Info
38	1.536665356	10.0.2.15	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
68	2.057263150	128.119.245.12	10.0.2.15	HTTP	786	HTTP/1.1 200 OK (text/html)
79	2.096675074	10.0.2.15	128.119.245.12	HTTP	313	GET /favicon.ico HTTP/1.1
73	2.423477473	128.119.245.12	10.0.2.15	HTTP	541	HTTP/1.1 404 Not Found (text/html)
79	3.547173715	10.0.2.15	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
81	4.096943538	128.119.245.12	10.0.2.15	HTTP	295	HTTP/1.1 304 Not Modified

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

GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Host: gaia.cs.umass.edu
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0
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 13:11:20 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 1) · any

<html>

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

</html>

GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Host: gaia.cs.umass.edu
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0
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 13:11:22 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
```

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

GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Host: gaia.cs.umass.edu
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0
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 13:11:20 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 1) - any

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

</html>
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Host: gaia.cs.umass.edu
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0
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 13:11:22 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"
```

3.2 Conditional GET on Localhost

- A simple HTML file with 2 images is placed in the localhost home directory.
- From a browser, a request is made for the file, which receives a response of 200 OK with both images being sent by the server.
- When the request is sent again, the 304 Not Modified status code is sent and images are not sent back.

http						
No.	Time	Source	Destination	Protocol	Length	Info
32	1.237607768	10.0.2.15	172.217.163.67	OCSP	441	Request
34	1.322933347	172.217.163.67	10.0.2.15	OCSP	757	Response
71	8.049090218	127.0.0.1	127.0.0.1	HTTP	405	GET /test.html HTTP/1.1
73	8.049387139	127.0.0.1	127.0.0.1	HTTP	786	HTTP/1.1 401 Unauthorized (text/html)
126	16.191880393	127.0.0.1	127.0.0.1	HTTP	448	GET /test.html HTTP/1.1
128	16.195753748	127.0.0.1	127.0.0.1	HTTP	488	HTTP/1.1 200 OK (text/html)
130	16.289854864	127.0.0.1	127.0.0.1	HTTP	394	GET /img1.jpg HTTP/1.1
189	16.293291131	127.0.0.1	127.0.0.1	HTTP	394	GET /img2.jpg HTTP/1.1
293	16.602777593	127.0.0.1	127.0.0.1	HTTP	360	[TCP ACKed unseen segment] GET /favicon.ico HTTP/1.1
295	16.606442012	127.0.0.1	127.0.0.1	HTTP	519	HTTP/1.1 404 Not Found (text/html)
302	20.678419310	127.0.0.1	127.0.0.1	HTTP	564	GET /test.html HTTP/1.1
304	20.678843621	127.0.0.1	127.0.0.1	HTTP	488	HTTP/1.1 200 OK (text/html)
306	20.704770225	127.0.0.1	127.0.0.1	HTTP	509	GET /img1.jpg HTTP/1.1
308	20.705237984	127.0.0.1	127.0.0.1	HTTP	215	HTTP/1.1 304 Not Modified
316	20.706040053	127.0.0.1	127.0.0.1	HTTP	509	GET /img2.jpg HTTP/1.1
318	20.706511864	127.0.0.1	127.0.0.1	HTTP	250	HTTP/1.1 304 Not Modified