

Firstly, we fetch the ip address of Facebook using either of the following 2 methods:  
(Type on your terminal):

- ping [www.facebook.com](http://www.facebook.com)

**OR**

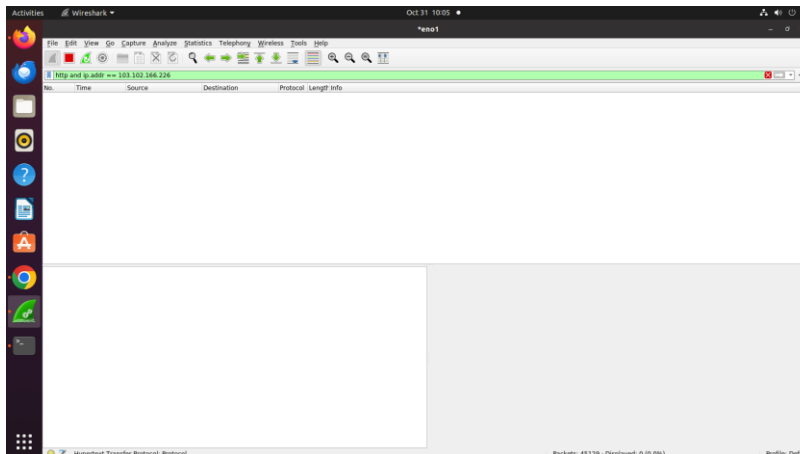
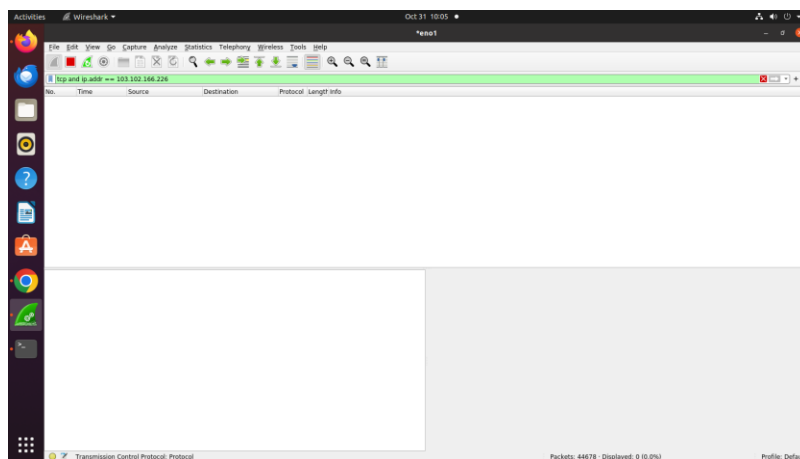
- host www.facebook.com

The above mentioned steps will give you the ip address of your site.

Now, open the wireshark application and choose eno1 as capturing option and write the following command :

tcp && ip.addr == <address of site you received from your terminal>

Now, there might a case, you may get the following blank outputs (as shown in the following two images):



In this case, you need to note that here your site is using ICMP protocol and not tcp and http as required in our case. This happens because as there are n number of address associated with a single site (in our case facebook), the address you fetched from the terminal is using ICMP protocol rather than tcp and http.

To resolve this problem:

Enter the following command:

```
tcp && ip.addr == <ip address of your system>
```

This will give you a list of all the ip addresses that are using TCP protocol on your machine.

Here's a tip, most of the time Facebook uses ip address that starts with 31.xx.xx.xx

Search this ip address in the list of ip addresses that are displayed after executing above command.

Now the procedure is simple, just use the above address 31.xx.xx.xx in further procedure ahead:

a. Capture all TCP traffic to/from Facebook, during the time when you log in to your Facebook account using:

```
tcp && ip.addr == <ip address of facebook in your case> (eg. 31.13.79.26)
```

b. Capture all HTTP traffic to/from Facebook (other website), when you log in to your Facebook account using:

```
http && ip.addr == 31.13.79.26
```

c. Write a DISPLAY filter expression to count all TCP packets (captured under item #1) that have the flags SYN, PSH, and RST set. Show the fraction of packets that had each flag set:

```
tcp.flags.syn == 1 && ip.addr == 31.13.79.26
```

```
tcp.flags.push == 1 && ip.addr == 31.13.79.26
```

```
tcp.flags.reset == 1 && ip.addr == 31.13.79.26
```

Refer the following images:

