TOR (the onion router)

Tor is a free and open-source software for enabling anonymous communication. Tor directs Internet traffic through a free, worldwide, volunteer overlay network consisting of more than seven thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis.

Run `apt-get install tor` to install/update your Tor packages.

Run `service tor start` to start the Tor service.

Run `service tor status` to check Tor's availability.

Run `service tor stop` to stop the Tor service.

Proxychains :

Proxychains - a tool that forces any TCP connection made by any given application to follow through proxy like TOR or any other SOCKS4, SOCKS5 or HTTP(S) proxy.

Run `nano /etc/proxychains.conf` to edit the settings. (Note: You can use any text editing tool instead of nano.)

We can now see, that most of the methods are under comment mark. You can read their description and decide on using one of them in the future.
For this lesson let's uncomment `dynamic_chain` and comment others (simply put `#` to the left). Additionally, it is useful to uncomment `proxy_dns` in order to prevent DNS leak. Scroll through the document and see whenever you want to add some additional proxies at the bottom of the page (which is not required at this point).

Now let's check our settings.

Start the TOR service and run `proxychains firefox`. Usually, you are required to put `proxychains` command before anything in order to force it to transfer data through

Tor.

After the Firefox has loaded, check if your IP address has changed with any website that provides such information. Also, try running a test on `dnsleaktest.com` and see if your DNS address changed too.

use the commands in the non root user sessions in the terminal.