Lab – Remaining Anonymous Online using TOR and Proxychains

In this lab, students will learn how to setup Proxychains in Kali Linux to stay anonymous while performing Nmap Scans or SQL Injection. Kali Linux 2.0, an Advanced Penetration Testing Linux distribution used for Penetration Testing, Ethical Hacking, and network security assessments.

TOR

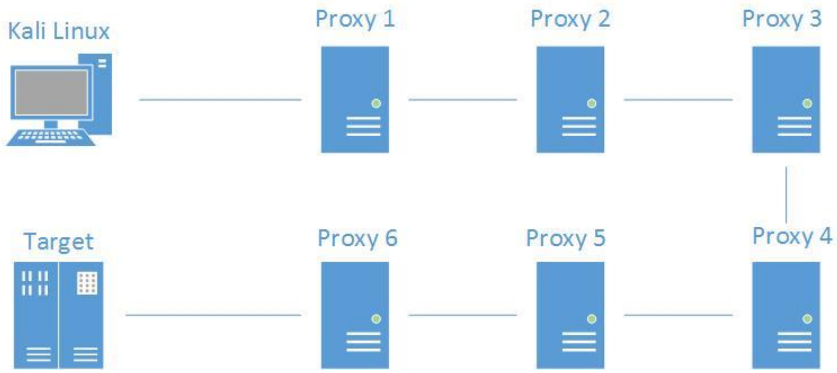
Tor is software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy.

PROXYCHAINS

A tool that forces any TCP connection made by any given application. to follow through a proxy such as TOR or any other SOCKS4, SOCKS5 or HTTP(S) proxy. Supported auth-types: "user/pass" for SOCKS4/5, "basic" for HTTP. proxyresolv - DNS resolving. Used to resolve hostnames via proxy or TOR.

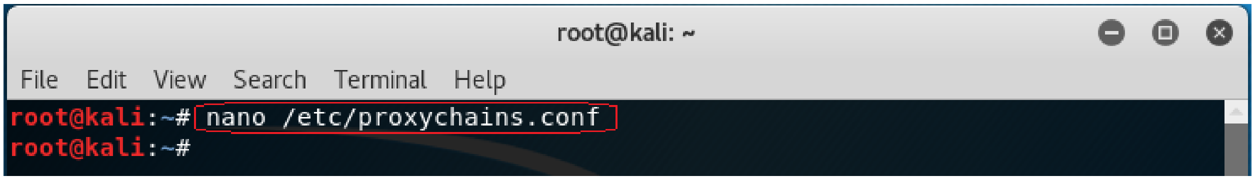
How Proxychains Work.

Using dynamic proxychains, our location is moved from one proxy server to another bouncing our location all over the world. With each proxy server, our location and IP address changes. When we add in the TOR network, we are given another layer of anonymity The TOR network disguises your identity by moving your traffic across different TOR servers and encrypting that traffic, so it isn't traced back to you.



What we first need to do is edit the proxychains.config file. Open a terminal and use the nano editor to edit the proxychains.conf file by typing:

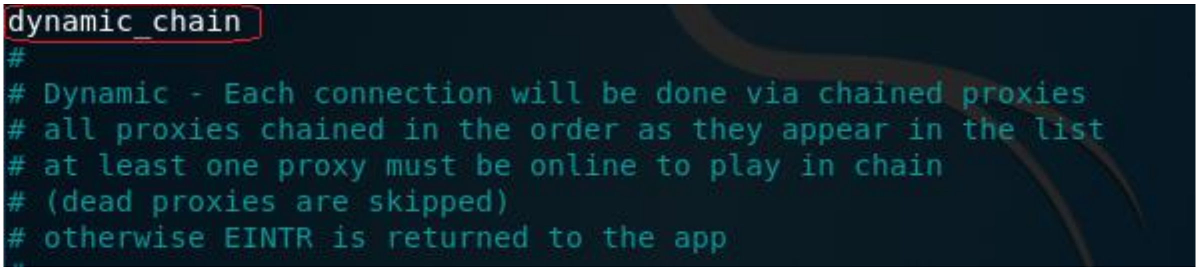
```
nano /etc/proxychains.conf
```



```
root@kali:~# nano /etc/proxychains.conf
root@kali:~#
```

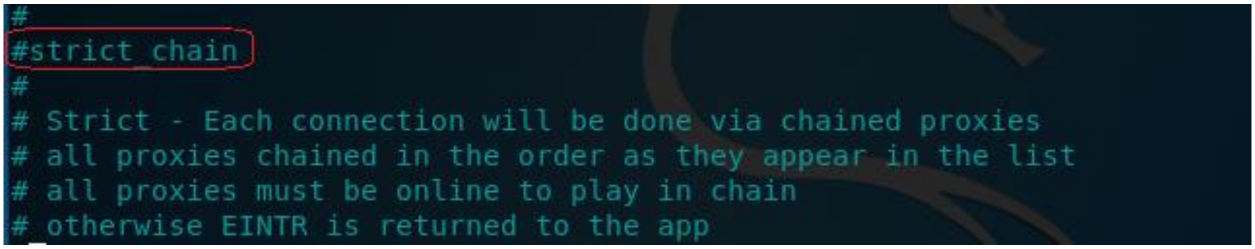
As we go through the file, you can read the comments for each of the sections to learn more about the different types of proxychains.

We need to uncomment out the line for dynamic_chain. Use your arrows keys to move up, down and across the file. Arrow down to the line, dynamic_chains and remove the # sign from it front of it.



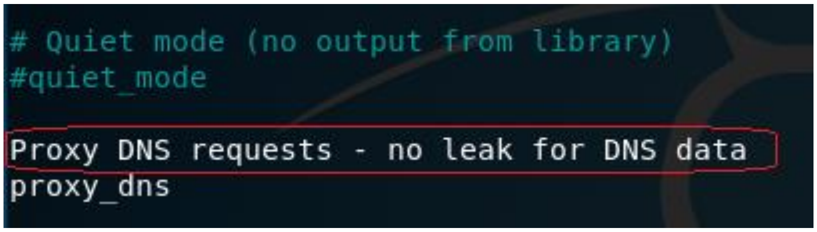
```
dynamic_chain
#
# Dynamic - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# at least one proxy must be online to play in chain
# (dead proxies are skipped)
# otherwise EINTR is returned to the app
```

We next want to comment out the line for strict_chain



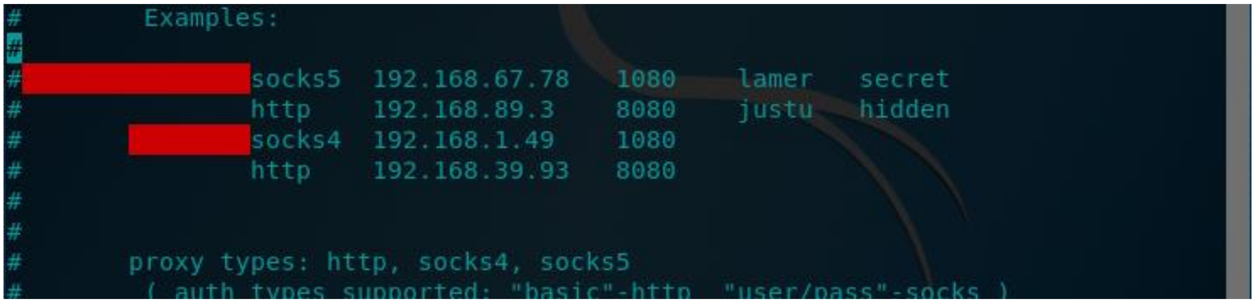
```
#
#strict_chain
#
# Strict - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# all proxies must be online to play in chain
# otherwise EINTR is returned to the app
```

To ensure we hide our DNS server information we need to enable or uncomment out the line for Proxy DNS requests - no leak for DNS data



```
# Quiet mode (no output from library)
#quiet_mode

Proxy DNS requests - no leak for DNS data
proxy_dns
```

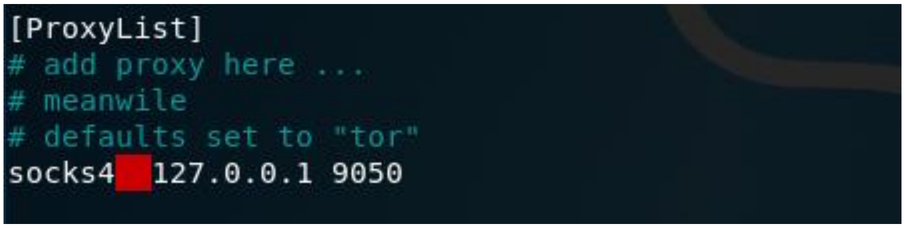
Scroll down to the examples section. Here we can see the formatting used for configuring a proxy file. We are concerned with the formation of the sock5 proxy type as these are the safest, and the fastest. If we were to subscribe to a proxychains service, they would provide you with a username and password, but we will be using the free sock5 proxychains.



```
#        Examples:
#
#               socks5  192.168.67.78   1080    lamer   secret
#               http    192.168.89.3    8080    justu   hidden
#               socks4  192.168.1.49    1080
#               http    192.168.39.93   8080
#
#
#       proxy types: http, socks4, socks5
#        ( auth types supported: "basic"-http  "user/pass"-socks )
```

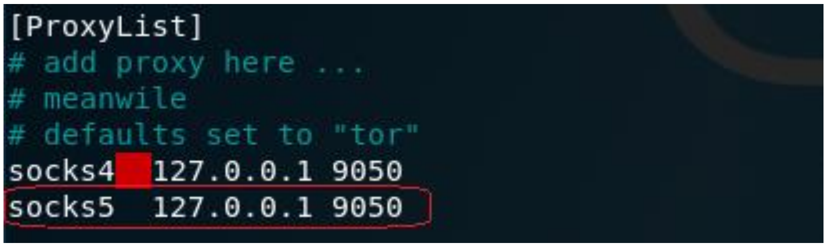
For this lab, we will be using a combination of TOR and proxychains.

Scroll down the [Proxylist] section of the file. Note the default as already been set to tor and the default is to use socks4. We need to add a line to the Proxylist to use sock5.



```
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks4  127.0.0.1 9050
```

Go to the line just below socks4 and add a line for sock5 using the same IP address and port number.



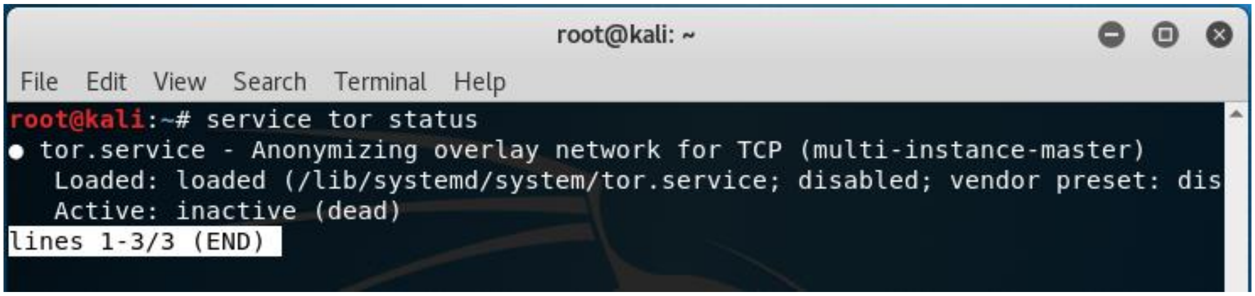
```
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks4  127.0.0.1 9050
socks5  127.0.0.1 9050
```

The red square represents a single tab key.

That’s it for configuring your proxychains.config file. We next need to test and confirm if our IP and DNS information is being randomly changed using proxychains.

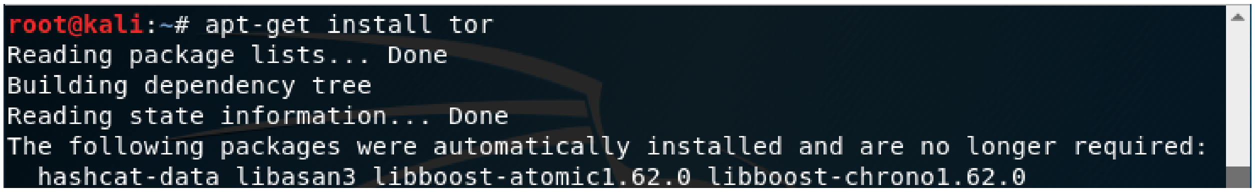
Save the file and the changes we made to it by pressing ctrl+x. Press y for yes and finally, press enter to exit the nano editor.

Check to see if the TOR service is installed and running.
Check the status of the tor service by typing, `service tor status`



```
root@kali:~# service tor status
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
   Loaded: loaded (/lib/systemd/system/tor.service; disabled; vendor preset: dis
   Active: inactive (dead)
lines 1-3/3 (END)
```

If TOR needs to be installed type, `apt-get install tor`



```
root@kali:~# apt-get install tor
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  hashcat-data libasan3 libboost-atomic1.62.0 libboost-chrono1.62.0
```

Troubleshooting:

If you get the following error when trying to update kali or install the tor service:

```
W: Failed to fetch http://http.kali.org/kali/dists/kali-rolling/InRelease The following signatures were invalid: EXPKEYSIG ED444FF07D8D0BF6 Kali Linux Repository <devel@kali.org>"
```

Type the following one line at a time:

```
wget https://http.kali.org/kali/pool/main/k/kali-archive-keyring/kali-archive-keyring_2018.1_all.deb

apt install ./kali-archive-keyring_2018.1_all.deb

apt update && apt upgrade
```

If you receive the following error:

```
"E: Unable to locate package" in Kali Linux.
```

If the package for TOR cannot be found, copy, and paste the following into the terminal, one line at a time:

```
apt-get update
apt-get update --fix-missing
```

Last ditch effort to get Tor and Proxychanins to work!

Open you proxychain.config file. Highlight the contents, hit delete. You should now have a clean proxychains.config file with no text.

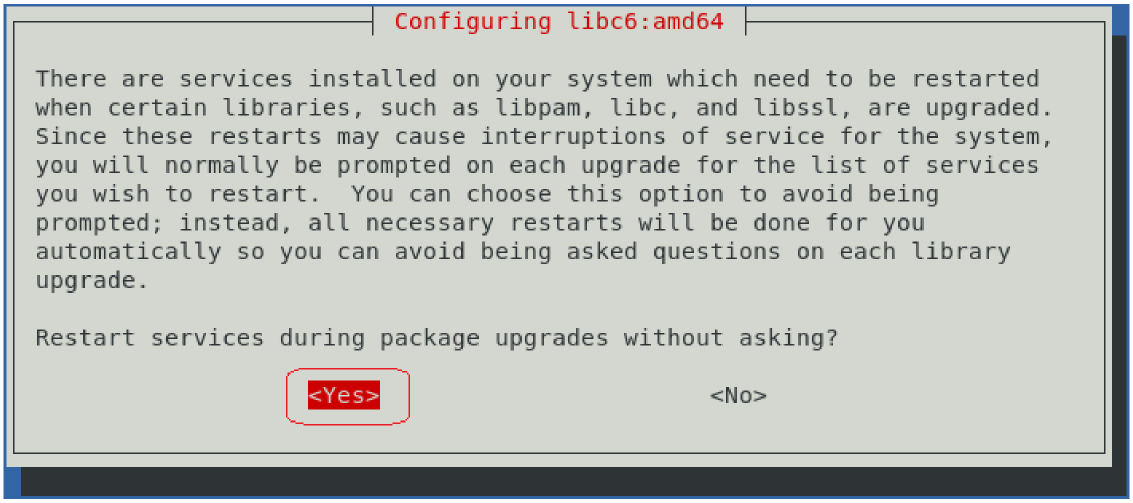
Open this text file and copy and paste the entire content in your blank, empty proxychains.config file.

[Working proxtchain.config file]

And finally:

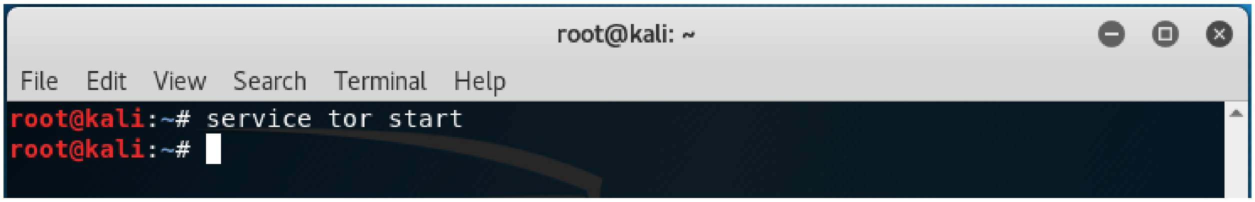
```
apt-get install tor
```

During the installation of TOR, all the services need to be restarted



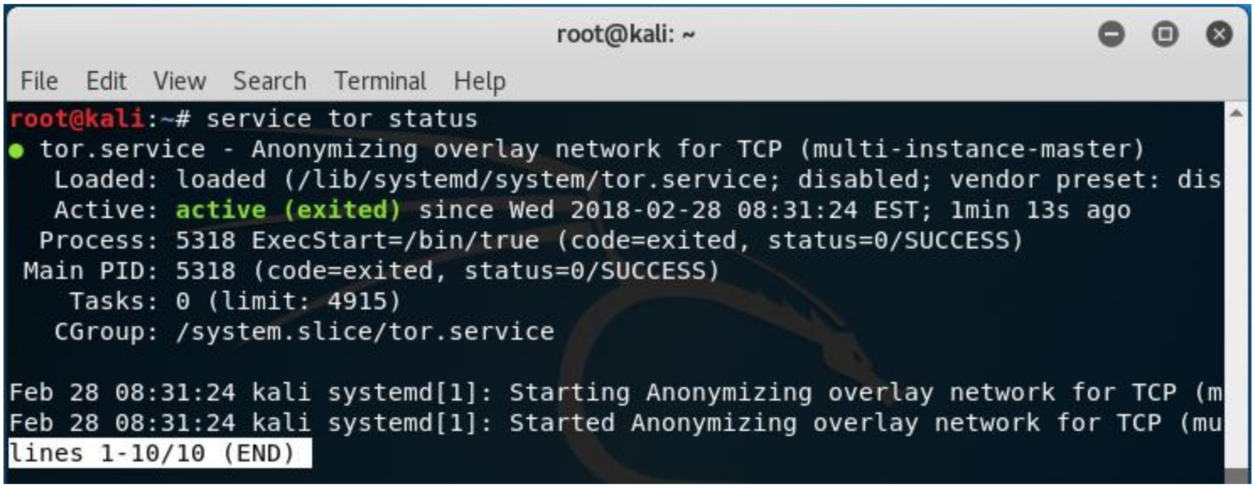
```
Configuring libc6:amd64

There are services installed on your system which need to be restarted
when certain libraries, such as libpam, libc, and libssl, are upgraded.
Since these restarts may cause interruptions of service for the system,
you will normally be prompted on each upgrade for the list of services
you wish to restart.  You can choose this option to avoid being
prompted; instead, all necessary restarts will be done for you
automatically so you can avoid being asked questions on each library
upgrade.

Restart services during package upgrades without asking?
```

TOR service needs to be started.



```
root@kali:~# service tor start
root@kali:~# 
```

Do a status check one more time. TOR is running!

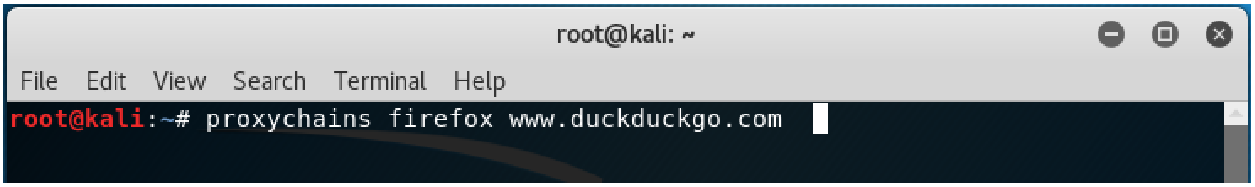


```
root@kali:~# service tor status
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
   Loaded: loaded (/lib/systemd/system/tor.service; disabled; vendor preset: dis
   Active: active (exited) since Wed 2018-02-28 08:31:24 EST; 1min 13s ago
  Process: 5318 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
 Main PID: 5318 (code=exited, status=0/SUCCESS)
    Tasks: 0 (limit: 4915)
   CGroup: /system.slice/tor.service

Feb 28 08:31:24 kali systemd[1]: Starting Anonymizing overlay network for TCP (m
Feb 28 08:31:24 kali systemd[1]: Started Anonymizing overlay network for TCP (mu
lines 1-10/10 (END)
```

Testing your TOR proxychain configuration

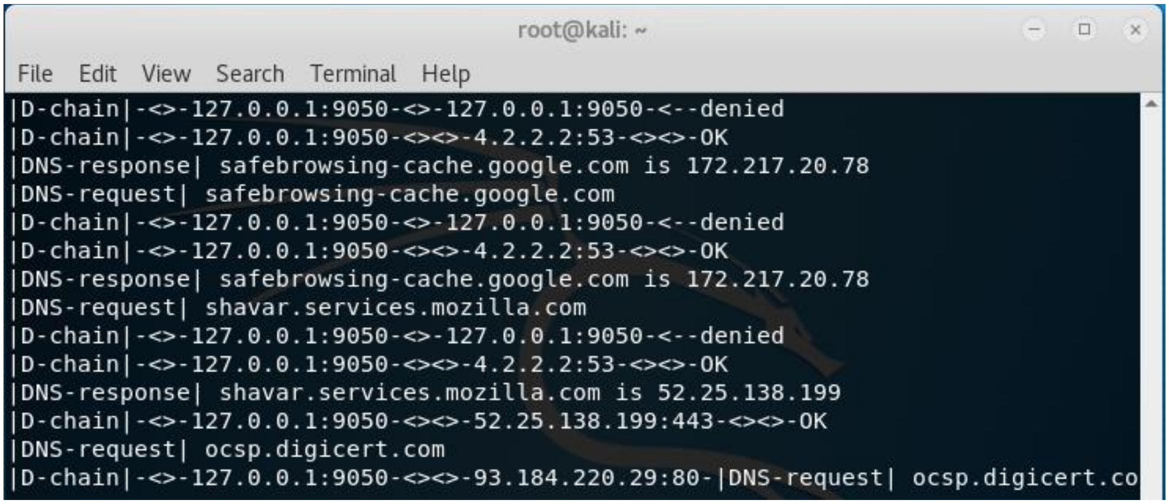
Open a new terminal and type the following:

`proxychains firefox` www.duckduckgo.com



```
root@kali:~# proxychains firefox www.duckduckgo.com
```

Be patient! The proxychains are routing the request through random proxies. If you minimize, your Firefox browser, you will see the different proxies rolling across the terminal prompt.

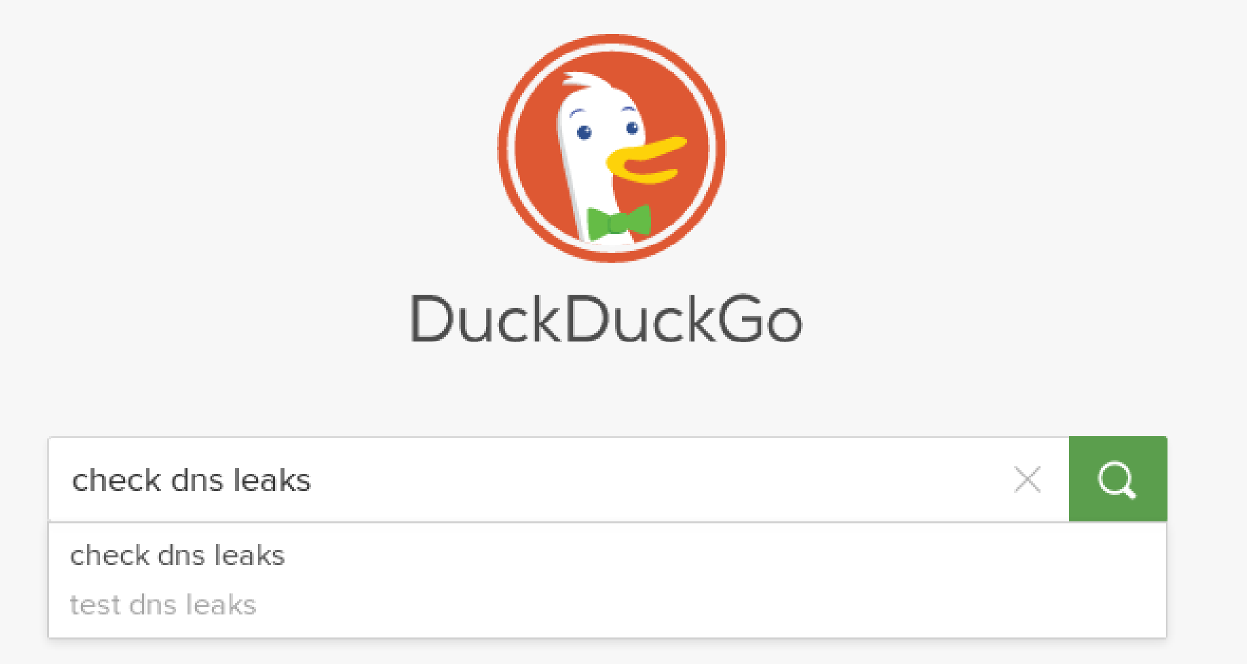


```
|D-chain|-<>-127.0.0.1:9050-<>-127.0.0.1:9050-<--denied
|D-chain|-<>-127.0.0.1:9050-<><>-4.2.2.2:53-<><>-OK
|DNS-response| safebrowsing-cache.google.com is 172.217.20.78
|DNS-request| safebrowsing-cache.google.com
|D-chain|-<>-127.0.0.1:9050-<>-127.0.0.1:9050-<--denied
|D-chain|-<>-127.0.0.1:9050-<><>-4.2.2.2:53-<><>-OK
|DNS-response| safebrowsing-cache.google.com is 172.217.20.78
|DNS-request| shavar.services.mozilla.com
|D-chain|-<>-127.0.0.1:9050-<>-127.0.0.1:9050-<--denied
|D-chain|-<>-127.0.0.1:9050-<><>-4.2.2.2:53-<><>-OK
|DNS-response| shavar.services.mozilla.com is 52.25.138.199
|D-chain|-<>-127.0.0.1:9050-<><>-52.25.138.199:443-<><>-OK
|DNS-request| ocsp.digicert.com
|D-chain|-<>-127.0.0.1:9050-<><>-93.184.220.29:80-|DNS-request| ocsp.digicert.co
```

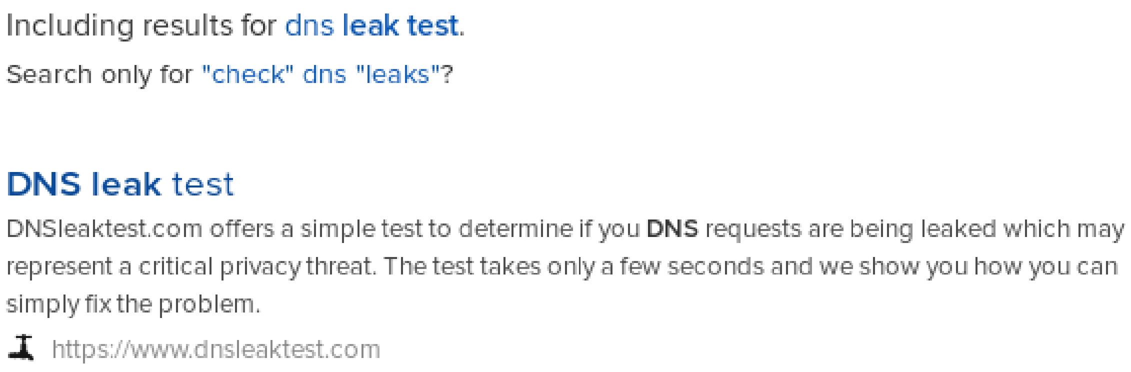
Unlike Google, duckduckgo.com does not log your IP address. Another layer of anonymity!

We can now confirm that our IP address has been hidden and our DNS information is not being exposed.

In the search bar for duckduckgo.com. type, `check dns leaks`



On the next page, click on the first link for DNS leak test.



Including results for dns **leak test**.

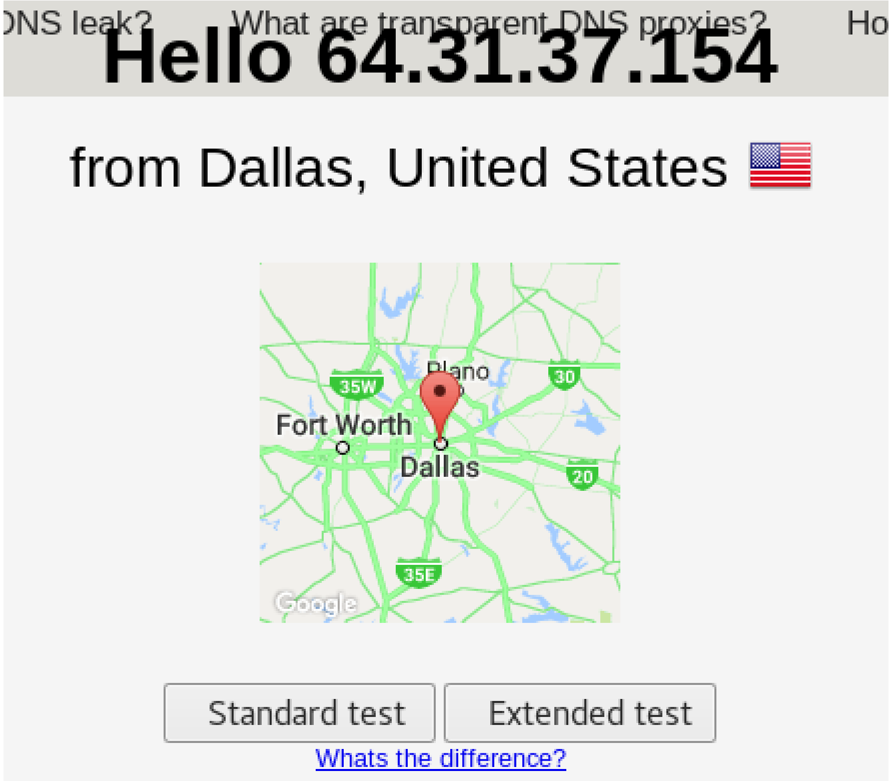
Search only for "check" dns "leaks"?

DNS leak test

DNSleaktest.com offers a simple test to determine if you **DNS** requests are being leaked which may represent a critical privacy threat. The test takes only a few seconds and we show you how you can simply fix the problem.

https://www.dnsleaktest.com

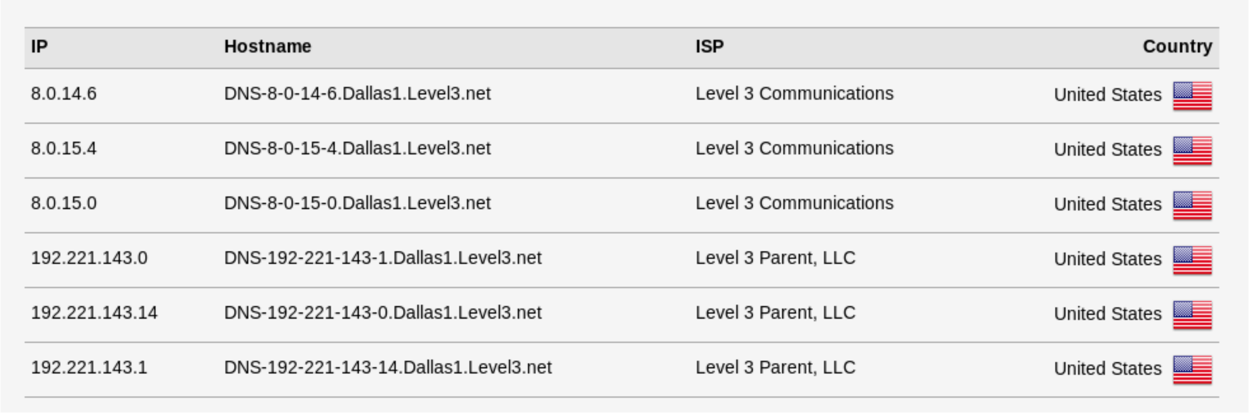
The next window shows you your spoofed IP address. In this example, I'm seen as being in Dallas, Texas with an IP address of 64.32.37.154, but my real location is in Philippines with a starting IP address of 130.x.x.x



Hello 64.31.37.154

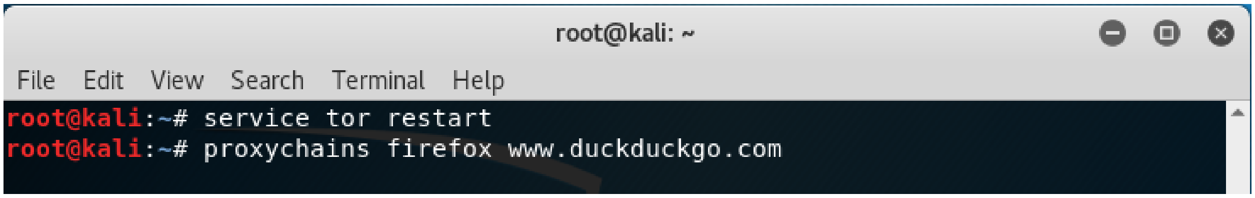
from Dallas, United States

Click on the Standard test button. This will show you where your DNS servers are originating from.



IP	Hostname	ISP	Country
8.0.14.6	DNS-8-0-14-6.Dallas1.Level3.net	Level 3 Communications	United States
8.0.15.4	DNS-8-0-15-4.Dallas1.Level3.net	Level 3 Communications	United States
8.0.15.0	DNS-8-0-15-0.Dallas1.Level3.net	Level 3 Communications	United States
192.221.143.0	DNS-192-221-143-1.Dallas1.Level3.net	Level 3 Parent, LLC	United States
192.221.143.14	DNS-192-221-143-0.Dallas1.Level3.net	Level 3 Parent, LLC	United States
192.221.143.1	DNS-192-221-143-14.Dallas1.Level3.net	Level 3 Parent, LLC	United States

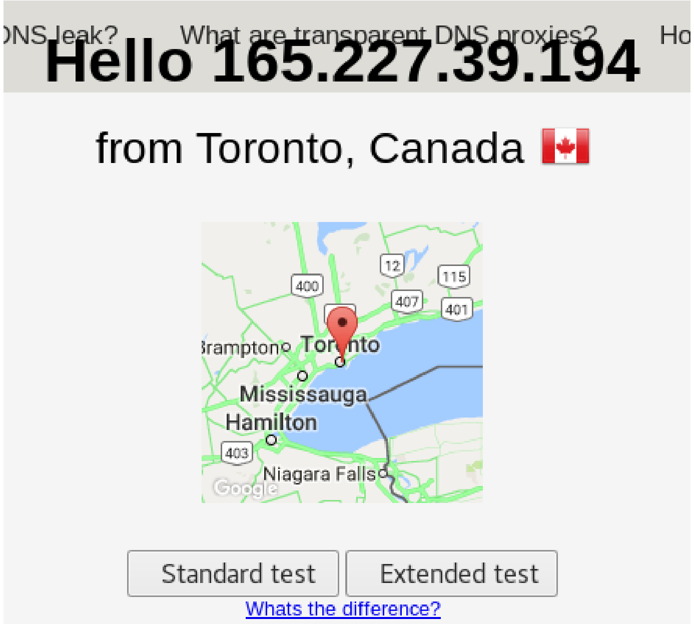
We can run another test by closing the browser, stopping, and restarting the TOR service and then restarting proxychains with the Firefox browser using the web page www.duckduckgo.com.



```
root@kali:~# service tor restart
root@kali:~# proxychains firefox www.duckduckgo.com
```

Run the DNS leak test again.

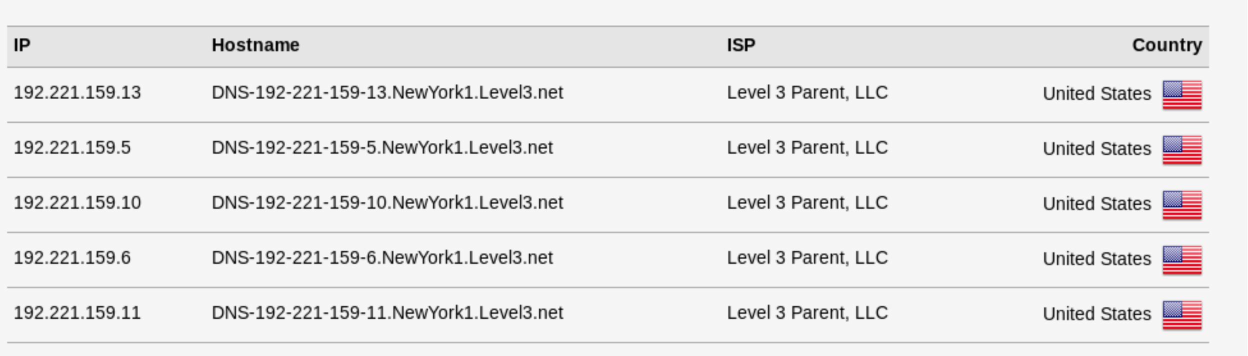
This time I'm seen as being in Toronto Canada.



Hello 165.227.39.194

from Toronto, Canada 🇨🇦

My DNS servers are located in the United States.



IP	Hostname	ISP	Country
192.221.159.13	DNS-192-221-159-13.NewYork1.Level3.net	Level 3 Parent, LLC	United States 🇺🇸
192.221.159.5	DNS-192-221-159-5.NewYork1.Level3.net	Level 3 Parent, LLC	United States 🇺🇸
192.221.159.10	DNS-192-221-159-10.NewYork1.Level3.net	Level 3 Parent, LLC	United States 🇺🇸
192.221.159.6	DNS-192-221-159-6.NewYork1.Level3.net	Level 3 Parent, LLC	United States 🇺🇸
192.221.159.11	DNS-192-221-159-11.NewYork1.Level3.net	Level 3 Parent, LLC	United States 🇺🇸

Summary

This is one of the best methods of remaining anonymous I have discovered, but there is no sure way to remain 100% anonymous online. Just using a VPN is not enough and there are a lot of hackers behind bars can attest to this being the case. If the VPN service states they do not log IPs, you have no idea if they do or not. Your best bet to make it as difficult as possible for law enforcement by using a VPN located in Russia where investigators are not likely to be given the information they seek even with a warrant.

You also must consider the breadcrumbs we leave behind when we search for information reckoning a potential target. Google makes a log search of every search query we perform. According to what information I can discern, www.duckduckgo.com does not.

The sacrifice we make for being anonymous is slower response time.

You can keep restarting the TOR service until you get a location that agrees with you.

End of the lab!