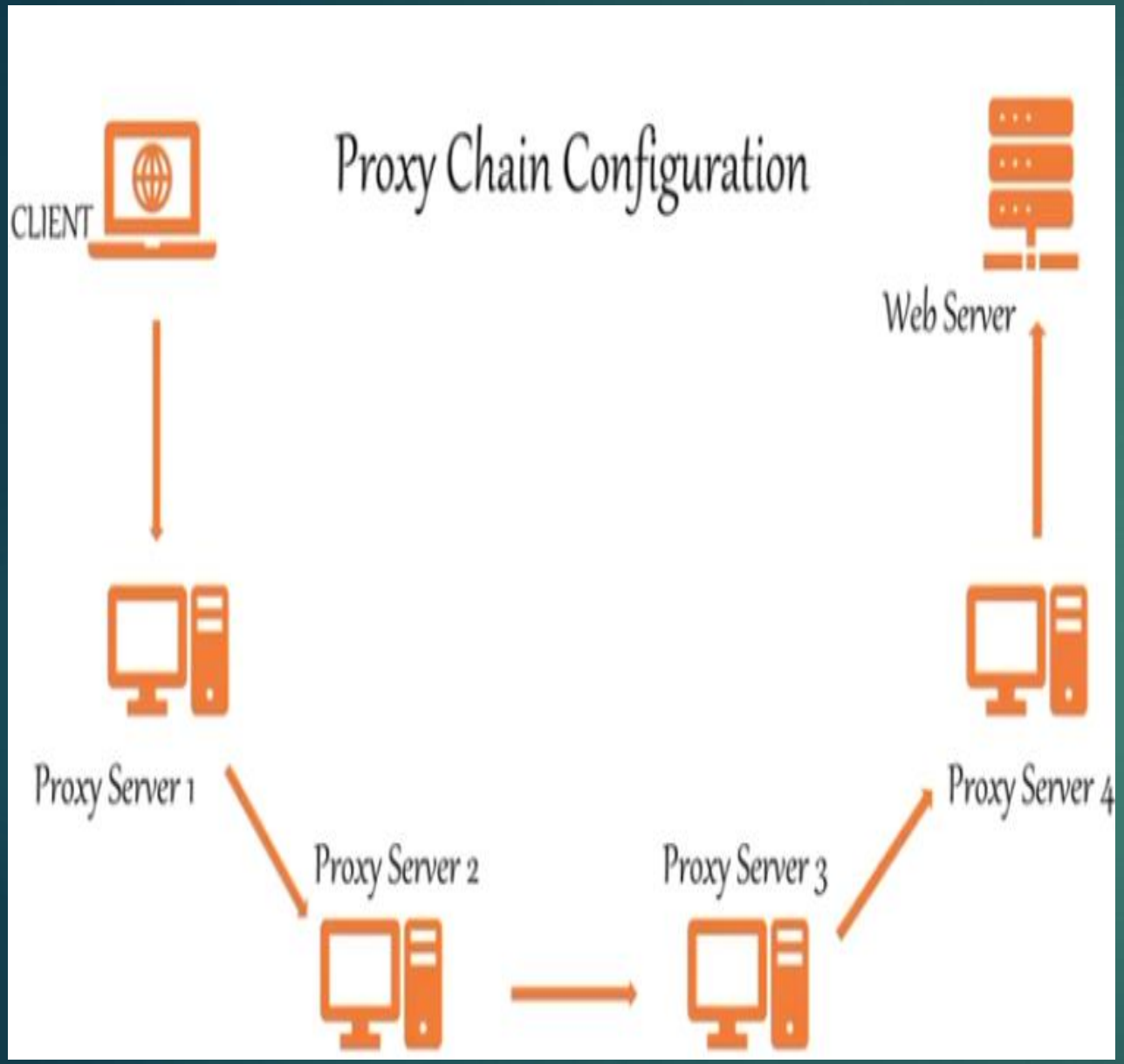
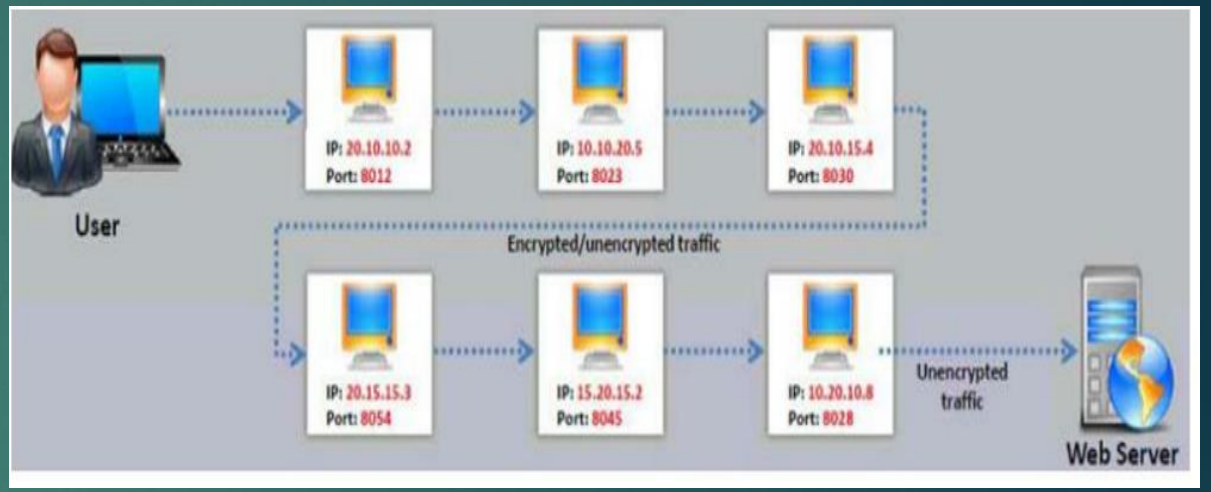


Proxy Chaining



Proxy & Proxies Chain

Proxy server is network computer that can serve as an intermediary for connecting with other computers .

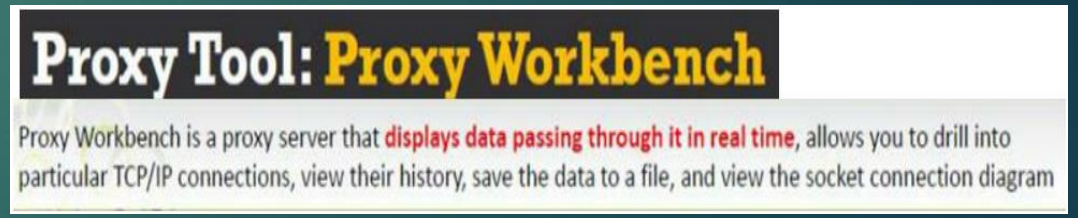
You can use proxy in many ways:

- As firewall to protect local from global
- As IP address multiplexer such as NAT
- To anonymize web surfing such as TOR
- To filter unwanted contents or URLs such as Bluecoat or WSA
- To save Bandwidth (cache contents) such as Bluecoat or WSA

Anonymous proxies hide your real IP from website you visit

Proxies Tools:

Proxy Switcher
Proxy Workbench
TOR
CyberGhostvpn
Tails
Psiphon



Proxy Tools: TOR and CyberGhost

Tor allows you to protect your privacy and defend yourself against network surveillance and traffic analysis

- CyberGhost allows you to protect your online privacy, surf anonymously, and access blocked or censored content
- It hides your IP and replaces it with one of your choice, allowing you to surf anonymously

https://www.torproject.org

http://www.cyberghostvpn.com

Proxy Tools for Mobile

3

Proxy Browser for Android | ProxyDroid | NetShade

Introduction to Anonymizers

An anonymizer removes all the identifying information from the user's computer while the user surfs the Internet

TOR Browser https://www.torproject.org/projects/torbrowser.html.en
JAP http://anon.inf.tu-dresden.de/download_en.html
Anonymous Browser Free https://branon.co.uk/win.php

Tails

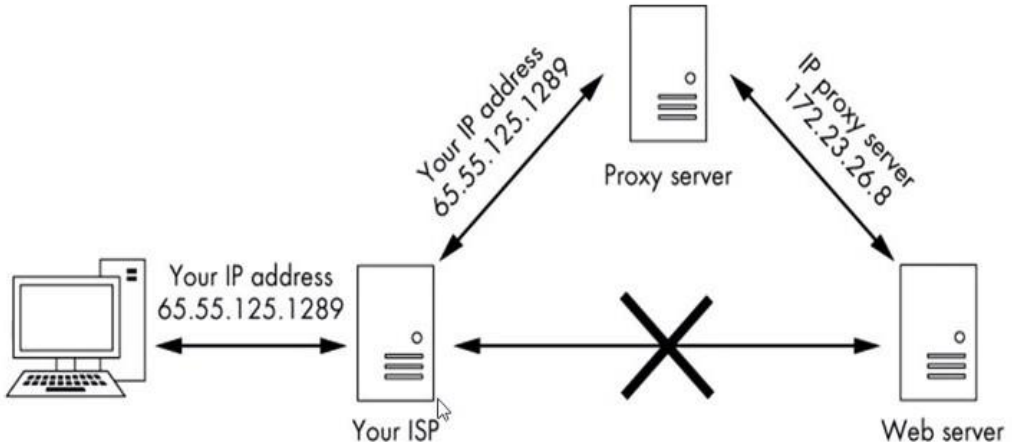
Tails is a live operating system, that user can start on any computer from a DVD, USB stick, or SD card

Anonymizers for Mobile

Orbot | Psiphon | OpenDoor

PROXY SERVERS

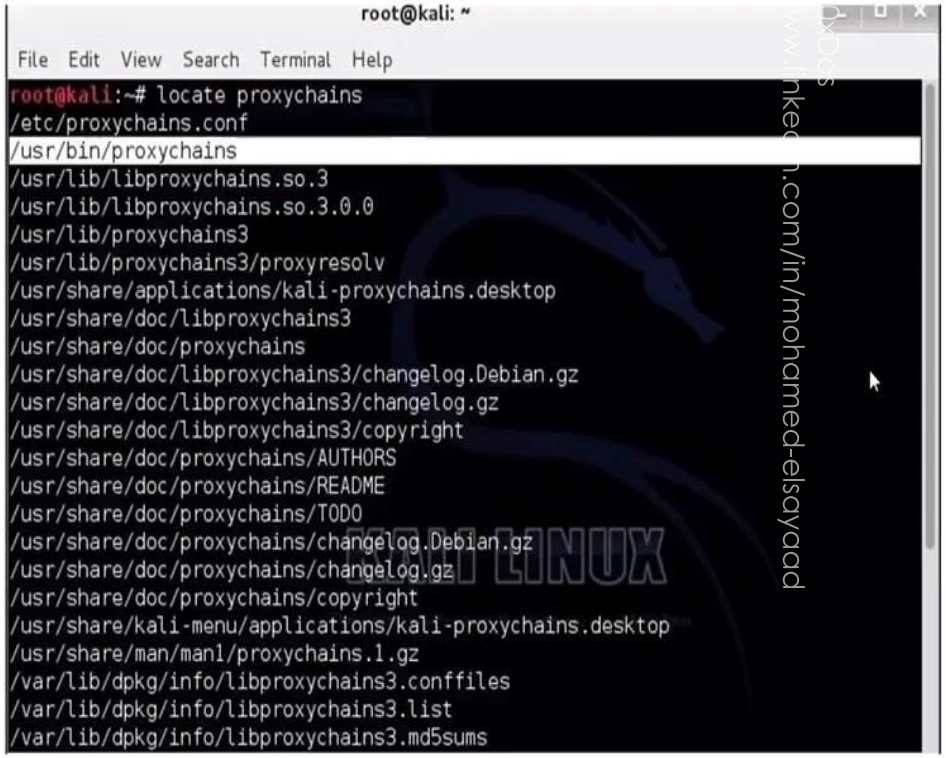
Another strategy for achieving anonymity on the internet is to use *proxies*, which are intermediate systems that act as middlemen for traffic: the user connects to a proxy, and the traffic is given the IP address of the proxy before it's passed on (



To make your traffic even harder to trace, you can use more than one proxy, in a strategy known as a *proxy chain*

locate proxychains

proxychains is in the */usr/bin* directory.



بفضل استخدام شبكة Tor ، يمكننا تكوين شبكة Tor في Proxychains للانتقال إلى الإنترنت من خلال هذه الشبكة المجهولة ، دون الحاجة إلى استخدام برامج معينة مثل Tor المتصفح يعمل على التنقل في شبكة Tor دون الحاجة إلى تكوين أي شيء آخر في فريقنا.

تثبيت Tor و Proxychains على Linux

أول شيء يجب أن نفعله هو تحديث النظام بالرقع وأحدث التطبيقات ، لذلك سنفتح Terminal ونكتب:

```
sudo apt update && sudo apt upgrade
```

سننتظر تحديث المستودعات وتثبيت كافة التحديثات قبل متابعة هذه العملية. بمجرد تحديث نظامنا ، سنقوم بتثبيت Tor فيه من نفس المستودعات عن طريق كتابة:

```
sudo apt install tor proxychains
```

بمجرد تثبيت الحزمتين اللازمتين لإجراء اتصالات مجهولة الهوية ، يجب علينا تمكين وحدة Tor ، مع الإشارة إلى الأمر التالي:

```
sudo service tor start
```

ونتحقق من أنها بدأت بشكل صحيح مع:

```
sudo service tor status
```

بشكل تلقائي يكون البروكسي ProxyChains مثبت في نظام التشغيل لينكس كالي و اذا لم يكن مثبت استخدام الامر التالي للتحميل

```
sudo apt-get install tor proxychains
```

هنا مجموعة من الاوامر لمعرفة حالة البروكسي Status و لبدء عمل البروكسي Start و لعملية ايقاف استخدام البروكسي Stop

sudo service tor status	معرفة حالة البروكسي
sudo service tor start	تشغيل البروكسي
sudo service tor stop	ايقاف عمل البروكسي

استخدم محرر النصوص nano لتحرير الملف proxychains.conf و المتوفر في مجلد etc

```
Nano /etc/proxychains.conf
```

الاختيارات Options		
	Strict Chain	الاختيار التلقائي المفعل في ملف الاعدادات و في هذا الاختيار يتم المرور على جميع العناوين في قائمة البروكسي بالترتيب مع التوقف في حالة وجود مشكلة في أحد عناوين البروكسي في القائمة
	Random Chain	يتم اختيار البروكسي من القائمة بشكل عشوائي مع اجراء عملية التبديل للتخفي
	Dynamic Chain	هذا الاختيار مشابه للـ Strict مع اختلاف انه يقوم بتجاهل البروكسي الذي يتوقف عن العمل من ضمن القائمة التي يتم اضافتها الى ملف الاعدادات.

في نهاية الملف سوف يجد العبارة SOCKS4 و التي تستخدم في توجيه البرنامج الى عنوان بروكسي مع تحديد المنفذ ، قم باضافة مجموعة من عناوين و ارقام المنافذ للبروكسي مع تغيير رقم SOCKS

socks5 IP Port Number

تشغيل البروكسي مع استخدام nmap

```
proxychains nmap -p 53 8.8.8.8
```

```
proxychains nmap scanme.nmap.org
```

تشغيل البروكسي مع استخدام متصفح فايرفكس

```
proxychains firefox www.duckduckgo.com
```

من الآن فصاعدًا ، ستكون كل حركة المرور التي ننتجها في نافذه المتصفح المفتوحة من الأمر السابق مجهولة تمامًا ، حيث ستكون قادرًا على إنشاء اتصال مباشر غير مجهول الهوية من أي نافذه أخرى نفتحها يدويًا من نفس المتصفح.

في حالة رغبتك في تشغيل أي برنامج آخر مع الوصول إلى الإنترنت من خلال هذا الوكيل الذي قمنا بتكوينه ، فسيتعين عليك ببساطة تشغيل "proxychains" متبوعًا بالبرنامج الذي نريده. على سبيل المثال ، يتم استخدام سلاسل البروكسي على نطاق واسع من قِبل pentesters لإجراء فحص المنافذ عن بُعد بشكل مجهول ، وبهذه الطريقة ، إذا قمنا بتنفيذ:

```
proxychains nmap -p 53 8.8.8.8
```

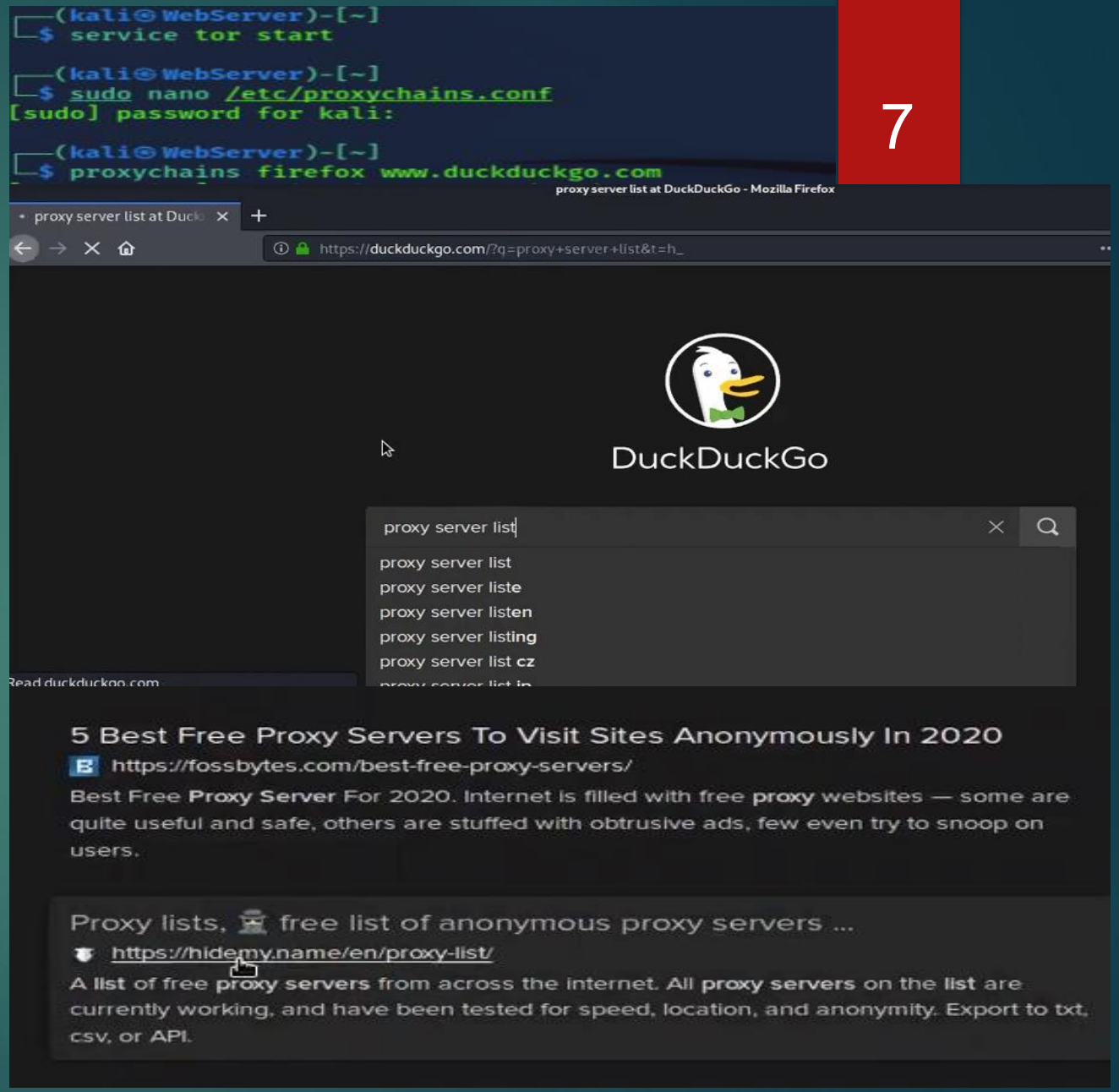
يمكننا إجراء فحص للمنافذ بناءً على الوكيل الذي قمنا بتكوينه ، وبهذه الطريقة ، لن يظهر عنوان IP العام الحقيقي الخاص بنا ، ولكن عنوان الوكيل الذي تم تكوينه.

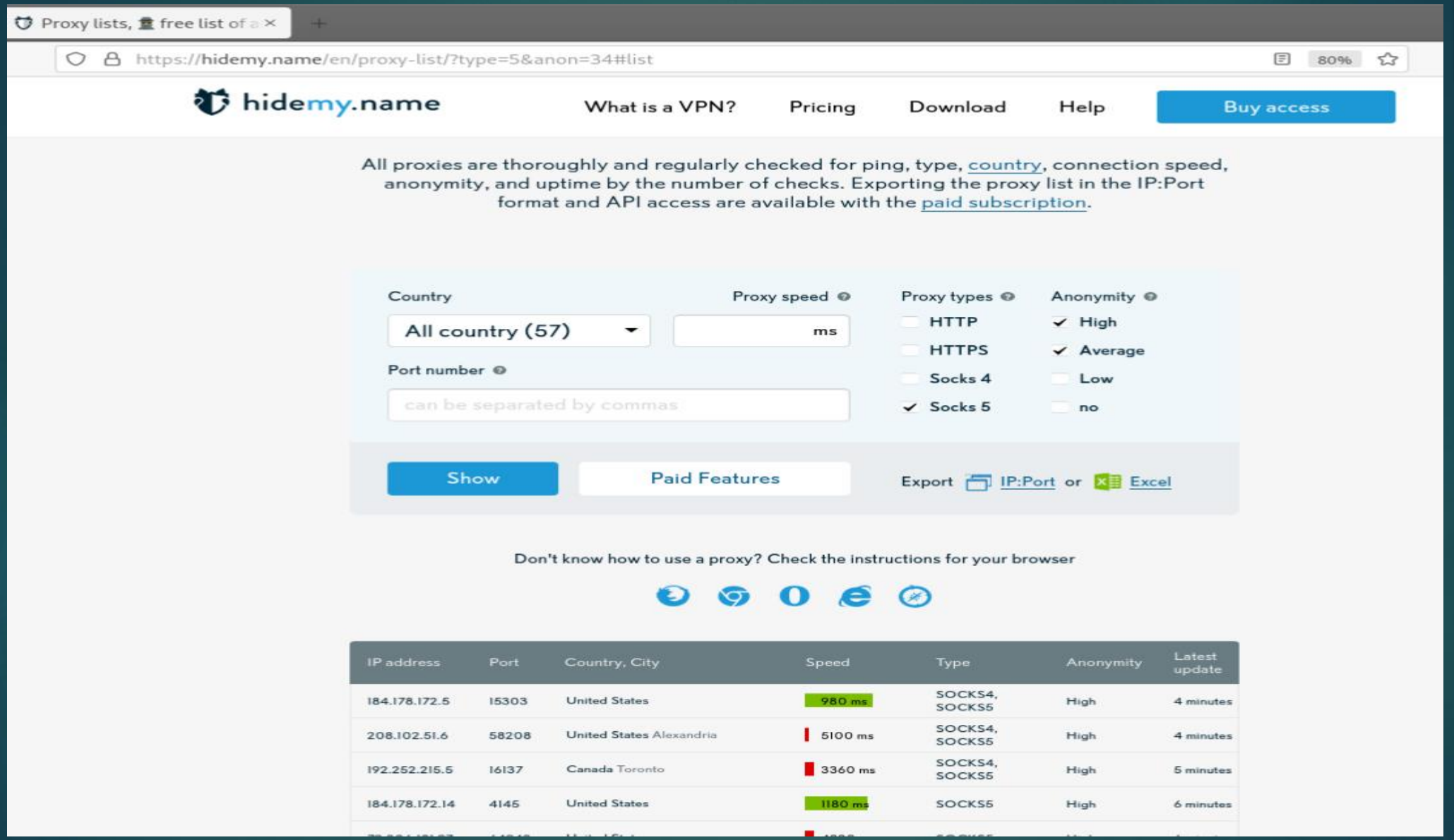
COMMON WAYS TO USE PROXIES

Setting a web browser to use a proxy works in general like this:

1. Log on to a website such whatismyip.com and pen down your current IP or use `ipconfig` to gain this information.
2. Log on to google.com and search for **'proxies**. You will get many sites providing you list of IPs and respective port numbers.
3. Now copy the IP and port number of a random proxy that you have selected.
4. In your browser locate the proxy settings
5. Check the option Manual Proxy Configuration, and fill in the IP address and port number. You can configure the proxies in any browser.
6. Check out whatismyip.com again, and hopefully the IP addressed has changed to reflect the proxy being used. Similarly, you can configure proxies in other web browsers.

Another way to use a proxy is to download a plug-in such as Foxy Proxy for Firefox or Chrome, which can automate the process of setting up a proxy.




Proxy lists, free list of
https://hidemy.name/en/proxy-list/?type=5&anon=34#list
80%
hidemy.name
What is a VPN?
Pricing
Download
Help
Buy access
All proxies are thoroughly and regularly checked for ping, type, country, connection speed, anonymity, and uptime by the number of checks. Exporting the proxy list in the IP:Port format and API access are available with the paid subscription.
Country
All country (57)
Proxy speed
ms
Port number
can be separated by commas
Proxy types
HTTP
HTTPS
Socks 4
Socks 5
Anonymity
High
Average
Low
no
Show
Paid Features
Export IP:Port or Excel
Don't know how to use a proxy? Check the instructions for your browser
IP address
Port
Country, City
Speed
Type
Anonymity
Latest update
184.178.172.5
15303
United States
980 ms
SOCKS4, SOCKS5
High
4 minutes
208.102.51.6
58208
United States Alexandria
5100 ms
SOCKS4, SOCKS5
High
4 minutes
192.252.215.5
16137
Canada Toronto
3360 ms
SOCKS4, SOCKS5
High
5 minutes
184.178.172.14
4145
United States
1180 ms
SOCKS5
High
6 minutes

Applications Places Leafpad Sun 07:27

proxychains.conf

File Edit Search Options Help

```
#
#random_chain
#
# Random - Each connection will be done via random proxy
# (or proxy chain, see  chain_len) from the list.
# this option is good to test your IDS :)

# Make sense only if random_chain
#chain_len = 2

# Quiet mode (no output from library)
#quiet_mode

# Proxy DNS requests - no leak for DNS data
proxy_dns

# Some timeouts in milliseconds
tcp_read_time_out 15000
tcp_connect_time_out 8000

# ProxyList format
#       type  host  port [user pass]
#       (values separated by 'tab' or 'blank')
#
#
#        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 )
#
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks4  127.0.0.1 9050
```

proxychains firefox www.hackers-arise.com
proxychains nmap 192.168.3.1

Like nearly every application in Linux/Unix, configuration is managed by a simple text file called the config file.
In the case of proxychains, this file is */etc/proxychains.conf*.

leafpad /etc/proxychains.conf

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

*proxychains.conf

File Edit Search Options Help

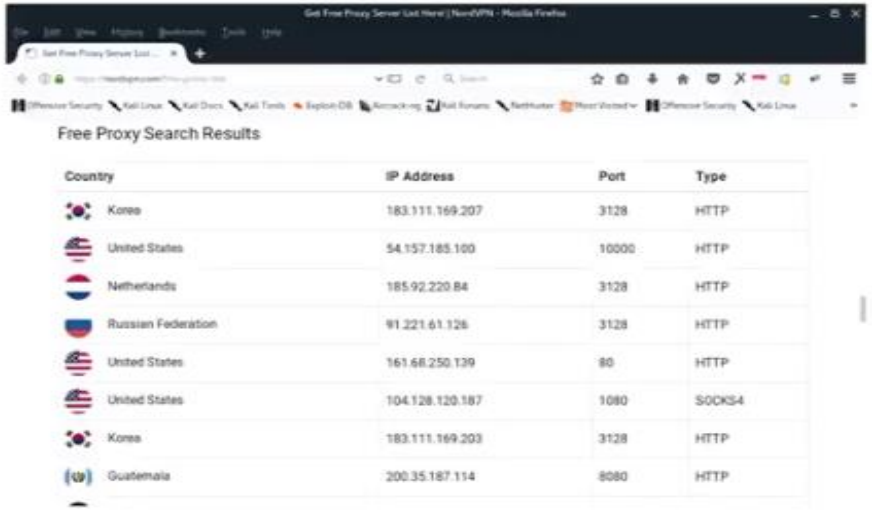
```
# ProxyList format
#       type  host  port [user pass]
#       (values separated by 'tab' or 'blank')
#
#
#        Examples:
#
#               socks5  192.168.67.78   1080    lamer   secret
#               http    192.168.89.3    8080    justu   hidden
#               socks4  192.168.1.49    1080
#               http    192.168.39.93   8080
#
#
#       proxy types: http, socks4, socks5
#        ( auth types supported: "basic"-http  "user/pass"-socks )
#
[ProxyList]
# add proxy here ...


# meanwile
# defaults set to "tor"
socks4  127.0.0.1 9050
```

A SOCKS server is a general purpose proxy server that establishes a TCP connection to another server on behalf of a client, then routes all the traffic back and forth between the client and the server. It works for any kind of network protocol on any port.
SOCKS Version 5 adds additional support for security and UDP.
he SOCKS server does not interpret the network traffic between client and server in any way.

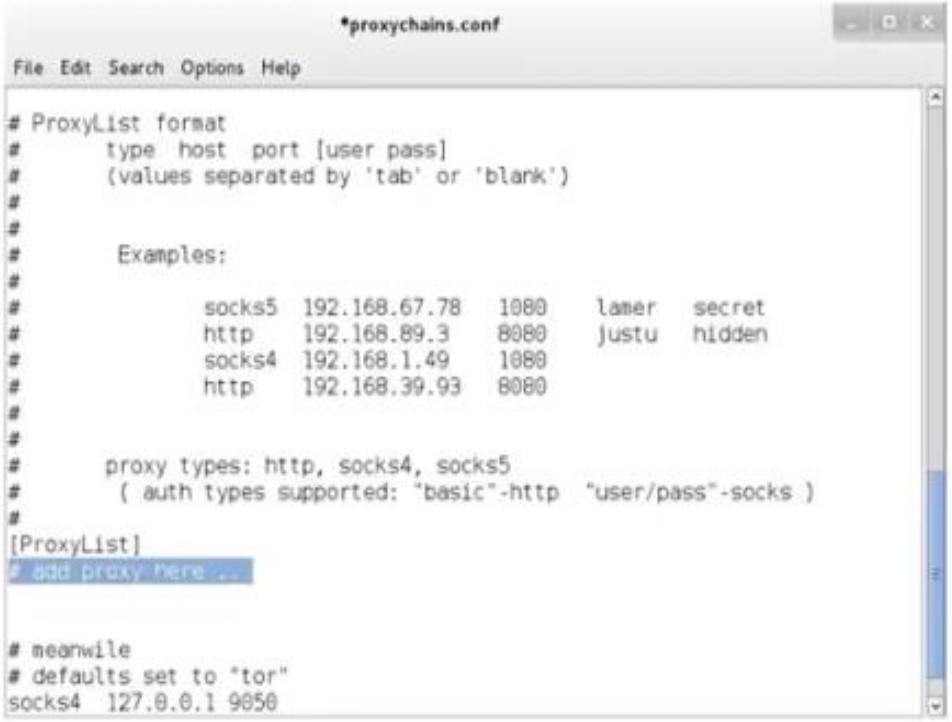
An HTTP proxy is similar, and may be used for the same purpose when clients are behind a firewall and are prevented from making outgoing TCP connections to servers outside the firewall.
However, unlike the SOCKS server, an HTTP proxy *does* understand and interpret the network traffic that passes between the client and downstream server, namely the HTTP protocol. Because of this the HTTP proxy can ONLY be used to handle HTTP traffic

To Add More Proxies

Free proxies from http://www.hidemy.name
Or https://nordvpn.com/free-proxy-list/



Notice the last line in the screenshot above. It directs proxychains to send the traffic first through our host at 127.0.0.1 on port 9050 (the default Tor configuration).
If you are using Tor, leaves this as it is. If you are not using Tor, you will need to comment out this line.



To Add More Proxies

proxychains.conf

File Edit Search Options Help

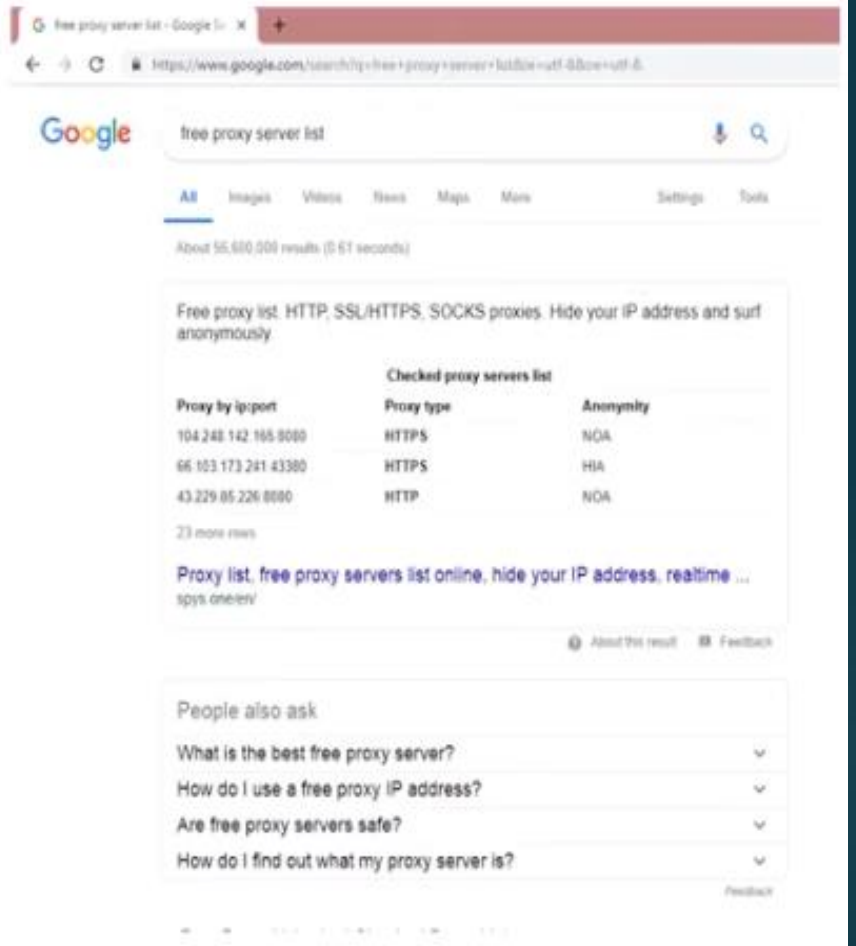
```
# ProxyList format
#       type  host  port [user pass]
#       (values separated by 'tab' or 'blank')
#
#
#       Examples:
#
#               socks5  192.168.67.78   1080    lamer   secret
#               http    192.168.89.3    8080    justu   hidden
#               socks4  192.168.1.49    1080
#               http    192.168.39.93   8080
#
#
#       proxy types: http, socks4, socks5
#        ( auth types supported: "basic"-http  "user/pass"-socks )
#
[ProxyList]
# add proxy here ...
socks4 5.9.212.53  9559
socks4 89.169.1.81 80
http 221.181.34.74  82
socks4 61.147.67.2
```

To use above proxies IP address as proxy chain:

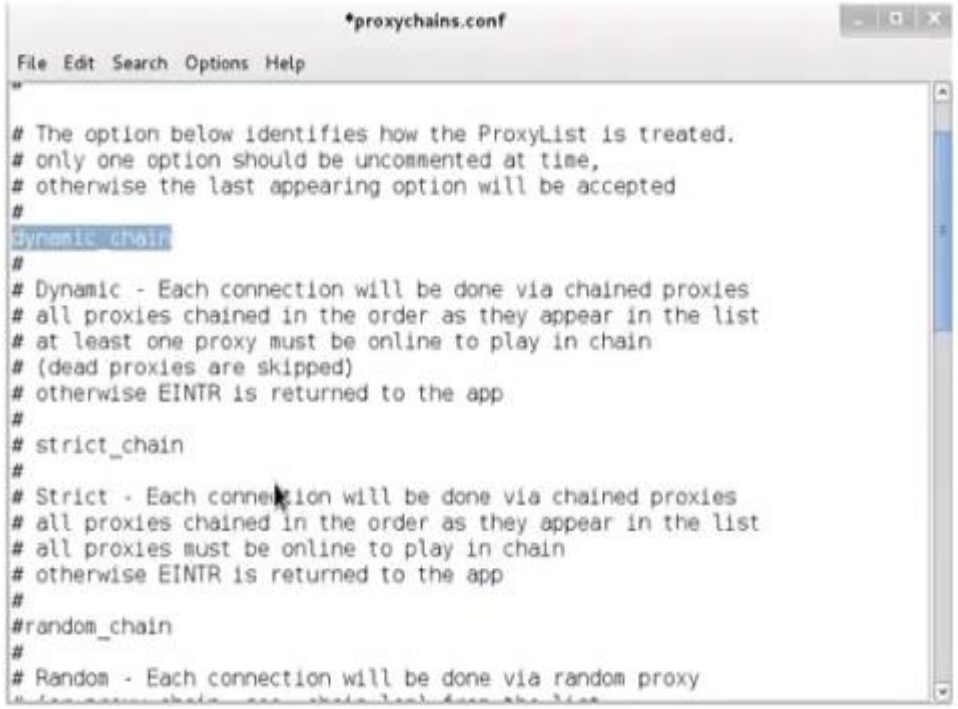
Dynamic chaining will enable us to run our traffic through every proxy on our list, and if one of the proxies is down or not responding, it will automatically go to the next proxy in the list without throwing an error.

To Add More Proxies

Or Google for it

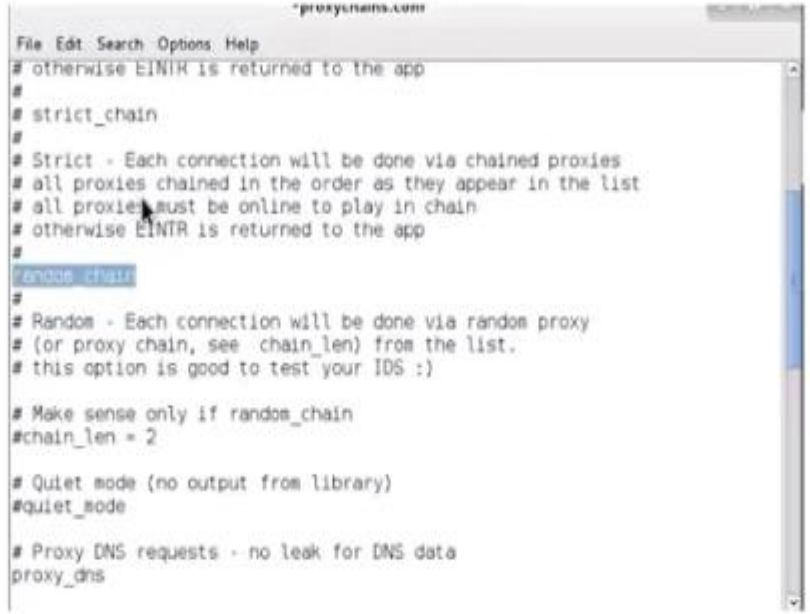


uncomment out the "dynamic_chains" line.



"random chaining". With this option, proxychains will randomly choose IP addresses from our list and use them for creating our proxychain. This means that each time we use proxychains, the chain of proxy will look different to the target, making it harder to track our traffic from its source.

Since we can only use one of these options at a time, make certain that you comment out the other options in this section before using proxychains.
In addition; you may want to uncomment the line with "chain_len". This will determine how many of the IP addresses in your chain will be used in creating your random proxy chain.



```
# 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
#
# 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
#
random_chain
# Random - Each connection will be done via random proxy
# (or proxy chain, see chain_len) from the list.
# this option is good to test your IDS :)

# Makes sense only if random_chain
chain_len = 3
```

Here, I have uncommented chain_len and given it a value of 3, meaning proxychains will now use three proxies from my list in the */etc/proxychains.conf* file, choosing them randomly and moving onto the next one if a proxy is down. Note that although this method certainly enhances your anonymity, it also increases the latency of your online activities.

Other ways than Tor and Proxychains to hide your self:

- Using a *virtual private network (VPN) such as* ExpressVPN *or NordVPN*
- *Encrypted Email such as using ProtonMail*

PROXYCHAINS FEATURES

1. Support SOCKS5, SOCKS4, and HTTP CONNECT proxy servers.
2. Proxychains can be mixed up with a different proxy types in a list
3. Proxychains also supports any kinds of chaining option methods, like: random, which takes a random proxy in the list stored in a configuration file, or chaining proxies in the exact order list, different proxies are separated by a new line in a file. There is also a dynamic option, that lets Proxychains go through the live only proxies, it will exclude the dead or unreachable proxies, the dynamic option often called smart option.
4. Proxychains can be used with servers, like squid, sendmail, etc.
5. Proxychains is capable to do DNS resolving through proxy.
6. Proxychains can handle any TCP client application, ie., nmap, telnet.

THE ONION ROUTER SYSTEM

In the 1990s, the US Office of Naval Research (ONR) set out to develop a method for anonymously navigating the internet for espionage purposes.

The Office of Naval Research is an organization within the United States Department of the Navy that coordinates, executes, and promotes the science and technology programs of the U.S

The plan was to set up a network of routers that was separate from the internet's routers, that could encrypt the traffic, and that only stored the unencrypted IP address of the *previous* router—meaning all other router addresses along the way were encrypted.

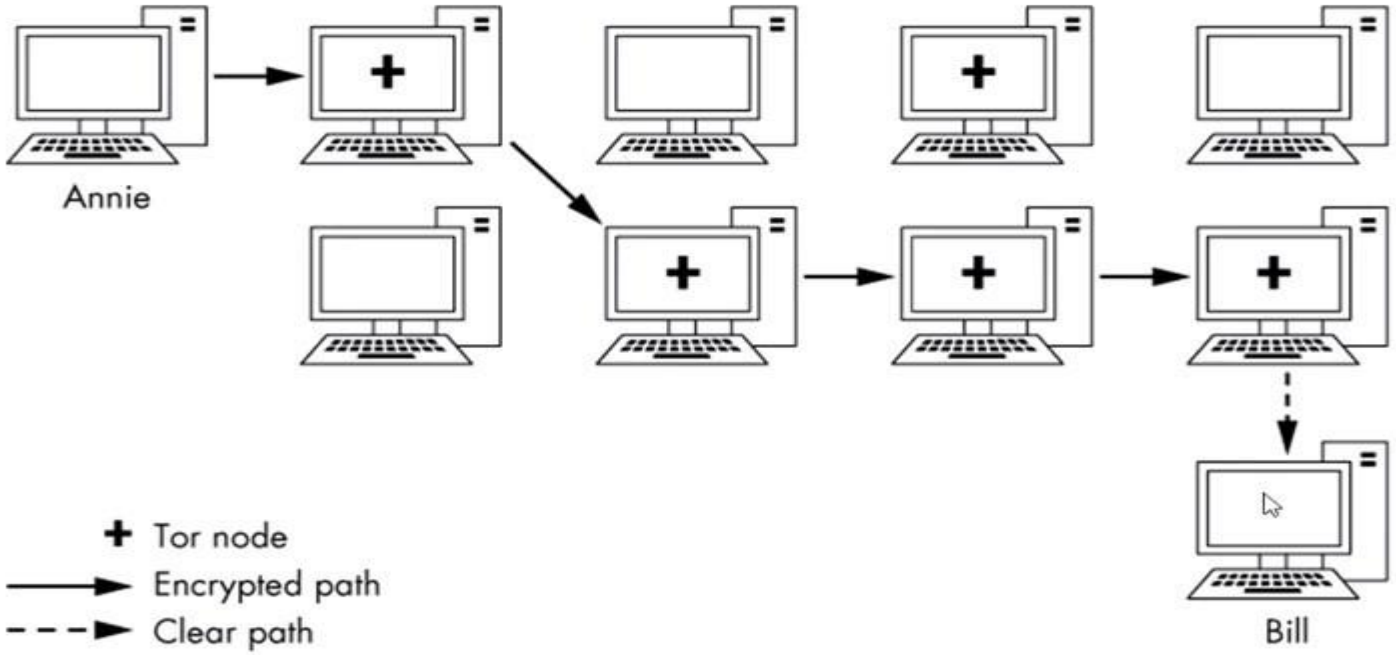
The idea was that anyone watching the traffic could not determine the origin or destination of the data.

This research became known as "**The Onion Router (Tor) Project**" in 2002, and it's now available to anyone to use for relatively safe and anonymous navigation on the web.

How ToR network work?

If someone intercepts the traffic, they can see only the IP address of the previous hop, and the website owner can see only the IP address of the last router that sent the traffic

Packets sent over Tor are not sent over the regular routers so closely monitored by so many but rather are sent over a network of over 7,000 routers around the world, thanks to volunteers who allow their computers to be used by Tor



The websites that make up the dark web require anonymity, so they allow access only through the Tor browser, and they have addresses ending in *.onion* for their top-level domain (TLD).

The problem of Tor

Tor's anonymity has been broken before by these authorities and will likely be broken again. The NSA, as one instance, runs its own Tor routers, meaning that your traffic may be traversing the NSA's routers when you use Tor. If your traffic is exiting the NSA's routers, that's even worse, because the exit router always knows your destination. The NSA also has a method known as *traffic correlation*, which involves looking for patterns in incoming and outgoing traffic, that has been able to break Tor's anonymity.

https://null-byte.wonderhowto.com/how-to/is-tor-broken-nsa-is-working-de-anonymize-you-when-browsing-deep-web-0148933/

Anonymizer Tool: Your Freedom

Your Freedom

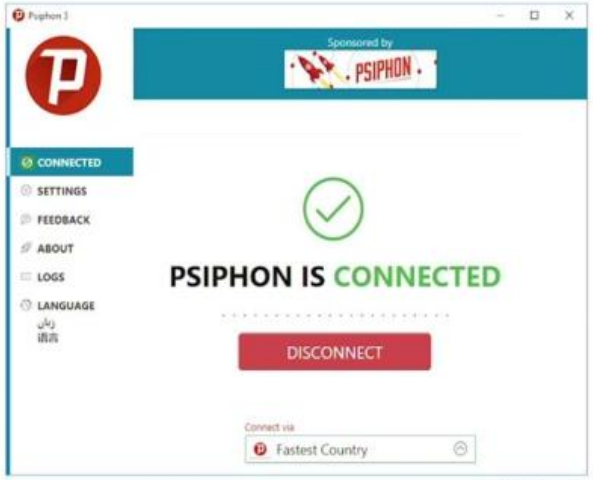
- Acts as a secure web and SOCKS proxy
- Bypass:
  - Firewalls, IDS
  - Content Filters
- Available for:
  - Windows
  - Android
  - Java 6

https://your-freedom.net/

Anonymizer Tool: Psiphon

Psiphon

- Acts as a secure proxy
- Bypass:
  - Firewalls
  - IDS
  - Content Filters
- Available for:
  - Windows
  - Android



https://psiphon.ca