CHAPTER

Online Anonymity

8

INFORMATION IN THIS CHAPTER

- Anonymity
- Online anonymity
- Proxy
- Virtual private network
- Anonymous network

ANONYMITY

Anonymity, the basic definition of this term is “being without a name.” Simply understood someone is anonymous if his/her identity is not known. Psychologically speaking, being anonymous may be perceived as a reduction in the accountability for the actions performed by the person. Anonymity is also associated with privacy as sometimes it is desirable not to have a direct link with a specific entity, though sometimes it is required by law to present an identity before and/or during an action is performed. In the physical world we have different forms of identification, such as Social Security Number (SSN), driving license, passport etc., which are widely acceptable.

ONLINE ANONYMITY

In the virtual space we do not have any concrete form of ID verification system. We usually use pseudonyms to make a statement. These pseudonyms are usually are not related to our actual identity and hence provide a sense of anonymity. But the anonymity present on the internet is not complete. Online we may not be identified by our name, SSN, or passport number, but we do reveal our external IP address. This IP address can be used to track back to the computer used. Also on some platforms like social network websites we create a virtual identification as they relate to our relationships in physical world. Some websites have also started to ask users to present some form of identification or information which can be related directly to a person, in the name of security. So basically we are not completely anonymous in the

Hacking Web Intelligence. http://dx.doi.org/10.1016/B978-0-12-801867-5.00008-2

cyber space. Usually we do reveal some information which might be used to trace the machine and/or the person.

WHY DO WE NEED TO BE ANONYMOUS

There are many reasons to be anonymous. Different people have different reasons for that some may want to be anonymous due to their work demands such as those who are into cyber investigation, journalism, and some might want to be anonymous because of their concern of their privacy etc. There are times when we want to protest on something good but doing that openly might create some problems so we want to be anonymous. As we say in physical life, people who do bad things like a criminal after doing a crime want to go underground the same way in virtual life or in the internet. Cyber-criminals and hackers wanted to be anonymous.

Being anonymous is just a choice. It does not always need a reason. It's just a state to be in virtual life. It's a virtual lifestyle and while some want to enjoy the same and others might be forced to be. Similar to the physical world we do have a need or desire to stay anonymous on the internet. It may just be that we are concerned about our privacy, we want to make a statement but won't do it with our true identity, we need to report something to someone without getting directly involved, communicate sensitive information, or simply want to be a stranger to strangers (anonymous forums, chat rooms etc.). Apart from the mentioned reason, we may simply want to bypass a restriction put up by the authority (e.g., college Wi-Fi) to visit certain portions of the web. The motivation behind it can be anything, but a requirement is surely there.

People might get confused of being anonymous that means just hiding the identity. It can also about hiding what you are doing and what you want to be. A simple example can help us to understand this. Let's say we wanted to buy something and we visited an e-commerce site to buy it. We liked the product but due to some reasons we did not buy that. But as we were surfing normally, we may found advertisement of the same product all over the internet. It's just a marketing policy for the e-commerce giants by tracking a user's cookies to understand his/her likes and dislikes and post the advertisement according to that.

Some might like this and some might not. It's not just about somebody is monitoring on what are you doing in the internet but also about flooding adds about similar things to lure us to buy. To avoid such scenarios also people might prefer to browse anonymous. For a quick revision, there are private browsing options available in most of the browsers and there are specific anonymous browsers available that do this work for us.

In this chapter we will deal with different ways to stay anonymous online. 100% anonymity cannot be guaranteed on the internet, still with the tools and techniques that will be mentioned in this chapter, we can hide our identity up to a reasonable level.

WAYS TO BE ANONYMOUS

There are many ways to be anonymous and there are many aspects of being anonymous. Some might focus on the personal details to be hidden such as in social networking sites by using aliases, generic information or fake information, generic e-mail id, and other details. Some might want to be anonymous while browsing so that nobody can track what resource they are looking into. Some might want to hide their virtual identity address such as IP address etc.

There are different ways to achieve the above conditions. But the major and popular solutions available are either proxy or virtual private network (VPN). Though there are other methods to be anonymous but still these two are widely used and we will focus on these majorly in this chapter.

PROXY

Proxy is a word generally used for doing stuffs on behalf of someone or something. Similarly in technology, proxy can be treated as an intermediate solution that forwards the request sent by the source to the destination and collects response from the destination and sends it to the source again.

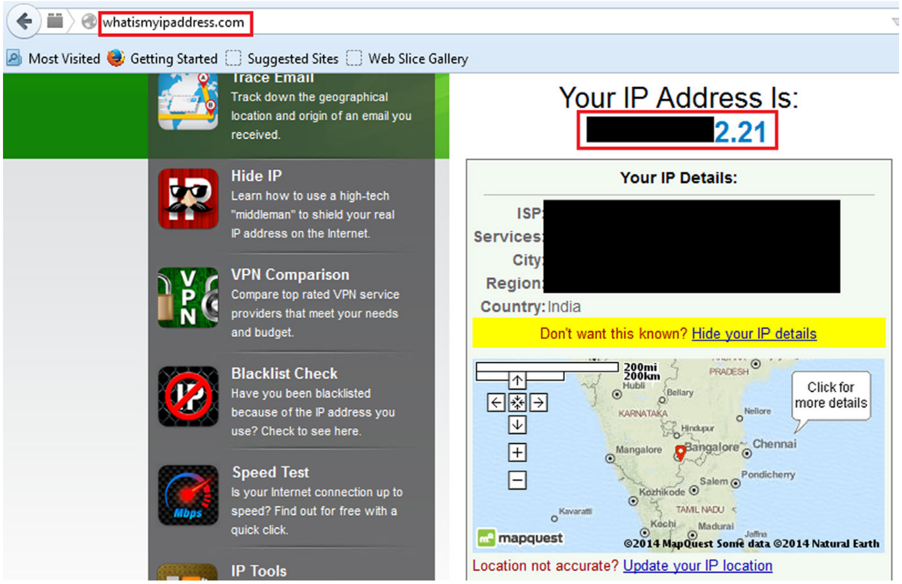
It is one of the widely used solutions used for anonymity. The only reason to use proxy is to hide the IP address. There are different proxy solutions available such as web proxy, proxy software etc. Basically all the solutions work on a basic principle to redirect traffic to the destination from some other IP address. The process might differ from solution to solution but the bottom line remains the same.

Though proxy can be used for many other purposes just apart from being anonymous, we will focus only the anonymity as the chapter demands the same.

Before focusing into the very deep technical aspects of proxy let's look into some work around to be anonymous. As in earlier chapters we learned how to use search engines efficiently and power searching. Now it's time to look into how a search engine can be used as a proxy to provide anonymity.

As Google is a popular search engine it can also be used as proxy with its feature called as Google Translate. Google provides its services in many countries apart from the English speaking ones and it also supports multiple languages. The Google Translate option allows a user to read web content in any other language a user wants. For a generic example, a non-English content can be translated to English and vice versa. So this feature allows a user to use Google server to forward the request and collect the response on his/her behalf, which is the basic fundamental of a proxy.

Now for testing the same, first we will look into our own IP address using a site called http://whatismyipaddress.com/ and later use Google translator to check the same site. The work of this site is to tell the IP address used to send the request to the site. If for the normal browsing and browsing through Google Translate the IP address differs, it means we achieved anonymity using Google Translate.



whatismyipaddress.com

Most Visited · Getting Started · Suggested Sites · Web Slice Gallery

Trace Email
Track down the geographical location and origin of an email you received.

Hide IP
Learn how to use a high-tech "middleman" to shield your real IP address on the Internet.

VPN Comparison
Compare top rated VPN service providers that meet your needs and budget.

Blacklist Check
Have you been blacklisted because of the IP address you use? Check to see here.

Speed Test
Is your Internet connection up to speed? Find out for free with a quick click.

IP Tools

Your IP Address Is:
[redacted]2.21

Your IP Details:

ISP: [redacted]
Services:
City:
Region:
Country: India

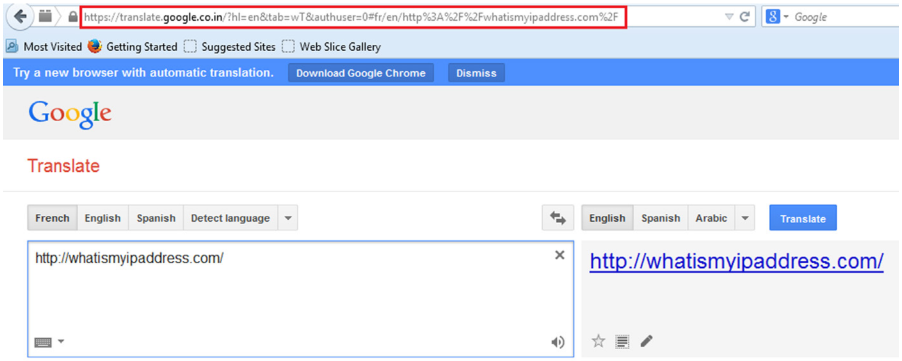
Don't want this known? Hide your IP details

Location not accurate? Update your IP location

FIGURE 8.1

whatismyipaddress.com.

Now visit translate.google.com. Select any language in source and any other language in destination to translate this web page as shown in below image.



https://translate.google.co.in/?hl=en&tab=wT&authuser=0#fr/en/http%3A%2F%2Fwhatismyipaddress.com%2F

Most Visited · Getting Started · Suggested Sites · Web Slice Gallery

Try a new browser with automatic translation. Download Google Chrome Dismiss

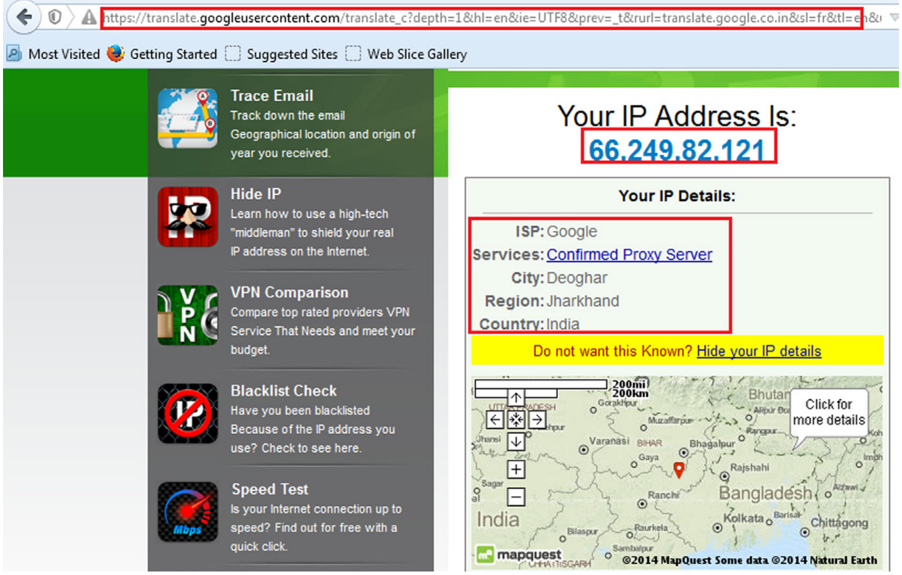
http://whatismyipaddress.com/

http://whatismyipaddress.com/

FIGURE 8.2

Google Translate.

Now click on Translate to check the whether the IP address matches with the IP address disclosed in above image for direct browsing or not.



https://translate.googleusercontent.com/translate_c?depth=1&hl=en&ie=UTF8&prev=_t&rurl=translate.google.co.in&sl=fr&tl=en&

Trace Email
Track down the email Geographical location and origin of year you received.

Hide IP
Learn how to use a high-tech "middleman" to shield your real IP address on the Internet.

VPN Comparison
Compare top rated providers VPN Service That Needs and meet your budget.

Blacklist Check
Have you been blacklisted Because of the IP address you use? Check to see here.

Speed Test
Is your Internet connection up to speed? Find out for free with a quick click.

Your IP Address Is:
66.249.82.121

Your IP Details:

ISP: Google
Services: Confirmed Proxy Server
City: Deoghar
Region: Jharkhand
Country: India

Do not want this Known? Hide your IP details

FIGURE 8.3

Page opened inside Google Translate.

We can see from the above image that the IP addresses of direct browsing and of browsing using Google Translate are different. Thus it is proved that we can use Google Translate as proxy server to serve our purpose. In many cases it will work fine. Though it's just a work around it's very simple and effective. In terms of full anonymity it might not be helpful but still we may use this method where we need a quick anonymity solution.

PROXY IN TERMS OF ANONYMITY

As we came across one example where we can use search engine feature as proxy. But the point to be considered is anonymity. There are different levels of anonymity based on different proxy solutions. Some proxies just hide our details but keeping the same in their logs, and sometime some proxies can be detected as proxy by the server and some might not. That's not the best solution if you want full anonymity. There are some solutions available which cannot be detected as proxy by the destination server and also delete all the user details the time user ends the session. Those are the best solutions for full anonymity. It all depends on our requirement to choose what service or what kind of proxy we want to use because fully anonymous proxy might charge the user some amount to use the solution.

TYPES OF PROXY SOLUTIONS

Now there are different types of proxy solutions available some are based on anonymity and also based on its type such as whether application-based or web-based. So let's start exploring some of the available options in application-based proxy.

APPLICATION-BASED PROXY

Application-based proxy is just a software or tool which can be installed in our operating system to use it as proxy solution.

Ultrasurf

It is an application-based proxy solution which can be found at http://ultrasurf.us/.

This is now available as Chrome plugin also. Though this is in beta stage if we are lazy to download and install it in our system and then use, we might use the Chrome plugin that will serve our purpose. The plugin can be found at https://chrome.google.com/webstore/detail/ultrasurf/mjnbclmflcpookeapghfhapeffmpodij?hl=en.

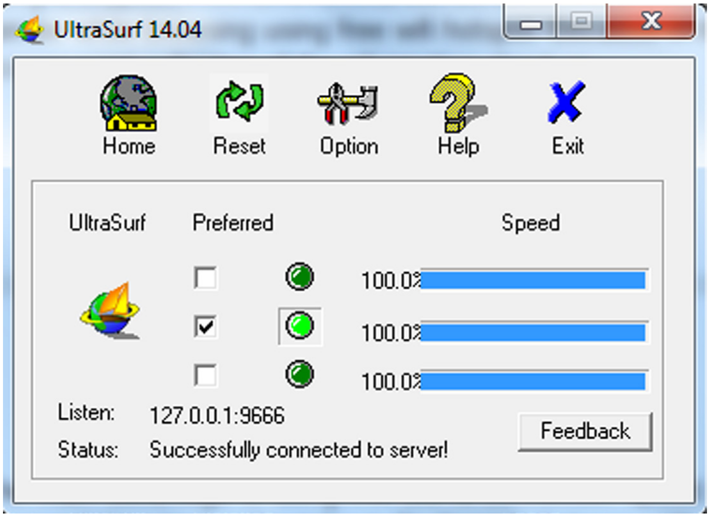
Let's first explore its plugin version then we will go deep in to the application version. The best part of this plugin is that it's simple to use and it supports many languages such as English, French, Portuguese, and Roman etc. Once the chrome plugin gets added in the browser, we will see its icon on the right top addon bar just in the right side of the address bar. When we have to use that just click on the icon, a small window will open then click on the switch available in that window to ON. Then the addon will connect to its server. Once it is connected to the server only then we can browse anonymous. In case of we forgot to switch on the addon or the addon is trying to connect to the server or the addon is unable to connect the server then all the thing we browse will be as normal browsing. So put it in mind to switch on and let it connect to the server before browsing or else all the anonymity process will go to vain.

The application version can be downloaded quite easily from the link http://ultrasurf.us/download/u.zip.

It's just a compressed file, extracting the file we can get the application. The best part of this process is that we need not to install the application. We can simply double click on that and that will configure the required settings in our system and let us browse anonymously. The default settings allow to open the Internet Explorer by double clicking the application. We can change the application settings using its options tab.

Though the tool was earlier developed for anticensorship protest in china, now it's used widely as a proxy solution. It not only just helps user to hide the details but also allows a user to communicate using encryption mechanism. This can be used in many different areas but the most general use can be while browsing using free Wi-Fi hotspot. Because in that case, there is a chance of rogue access point collecting all the information about us.

The main advantage of using this tool is connection speed. Generally when we use any kind of proxy solution as it redirects the traffic through that server the connection speed reduces drastically and user can feel that; but in this case it's very fast as compared to other proxy solutions. Apart from that we can see the connection speed in the tool itself and it provides three connection options, user can switch to any one of them any moment to avoid speed drop. To distinguish between normal browsing and browsing using Ultrasurf, this tool provides a cool lock symbol in the right corner of the browser to make sure that user is browsing anonymously.



□ ● 100.0%
☑ ● 100.0%
□ ● 100.0%

Listen: 127.0.0.1:9666

Status: Successfully connected to server!

FIGURE 8.4

UltraSurf interface.

A small drawback about this tool is that this tool supports only Windows. And another drawback is that the IP-checking solutions detect it as proxy server. But as we discussed earlier, this can be used in different other conditions based on our requirements and it’s easy to use. Just download, run, and browse anonymously.

JonDo

JonDo previously known as JAP is a proxy tool available at https://anonymous-proxy-servers.net/en/jondo.html.

It is available for wide range of operating systems such as Windows, Mac, for different flavors of Linux, and also for Android mobile. The full-fledged documentation of how to install and use makes it very essential as a proxy solution. Different proxy solutions come up with different types. It also provides one of its type for Firefox anonymous browsing known as JonDoFox.

Before exploring JonDo let’s first look into the Firefox anonymous browsing solution i.e., JonDoFox. It can be found at https://anonymous-proxy-servers.net/en/jondofox.html.

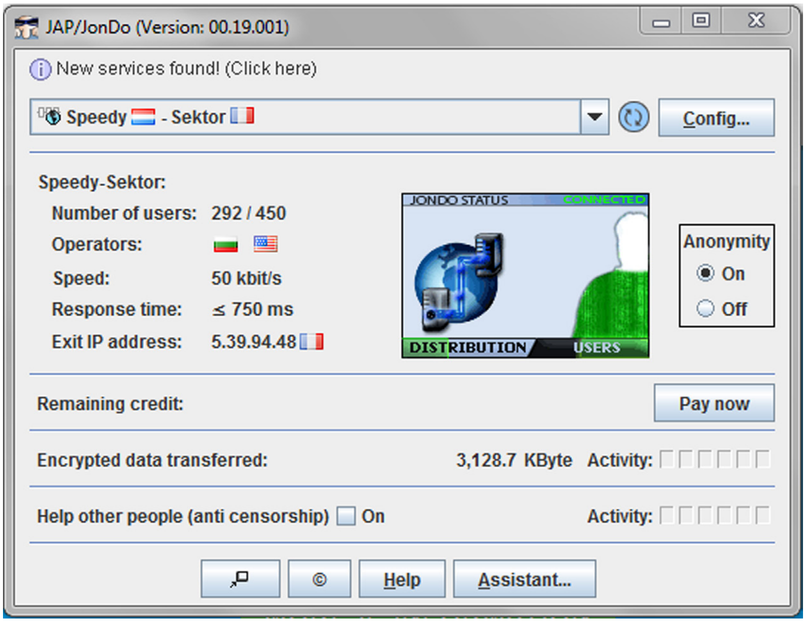
As JonDo, JonDoFox is also available for different operating systems such as Windows, Mac, and Linux. User can download as per his/her operating system from the above URL. The documentation of how to install is also available just next to the download link. But let’s download and install while we discuss more about the same.

Windows users will get JonDoFox.paf after downloading. After installing the same it will create a Firefox profile in name of JonDoFox. If user selects the same, the profile consists of many Firefox addons such as cookie manager, adblocker, etc., which will come to act. But to use it for full anonymity user needs to install certain dependent softwares such as Tor etc.

It’s good to use JonDoFox but user has to install all the dependent softwares once after installing the same. Some might not love to do so but still this is a great solution to browse anonymously.

Like JonDoFox, JonDo can also be downloaded from the above URL. It will give you the installer. Windows user will get an exe file “JonDoSetuup.paf” after downloading. The installation can be done for the operating system we are using and also for the portable version that can be taken away using the USB drive. User needs to choose according to his/her requirements. The only dependency of this software is JAVA. But as earlier we discussed how to install the same we are not going to touch that here again and by the way while installing this software it also installs JAVA, if it won’t find the compatible version available in the operating system. Once JonDo is installed, we can double click on its desktop icon to open the same. By default after installation it creates a desktop icon and enables it to start in Windows startup.

JonDo only provides full anonymity and fast connection to premium users. But we still can use the same. But first time we need to activate it with its free code. Test coupon can be found at https://shop.anonymous-proxy-servers.net/bin/testcoupon?lang=en but we need to provide our e-mail address to get it.



JAP/JonDo (Version: 00.19.001)

New services found! (Click here)

Speedy - Sektor

Speedy-Sektor:

Number of users:	292 / 450
Operators:	
Speed:	50 kbit/s
Response time:	≤ 750 ms
Exit IP address:	5.39.94.48

Anonymity ● On ○ Off

Remaining credit:

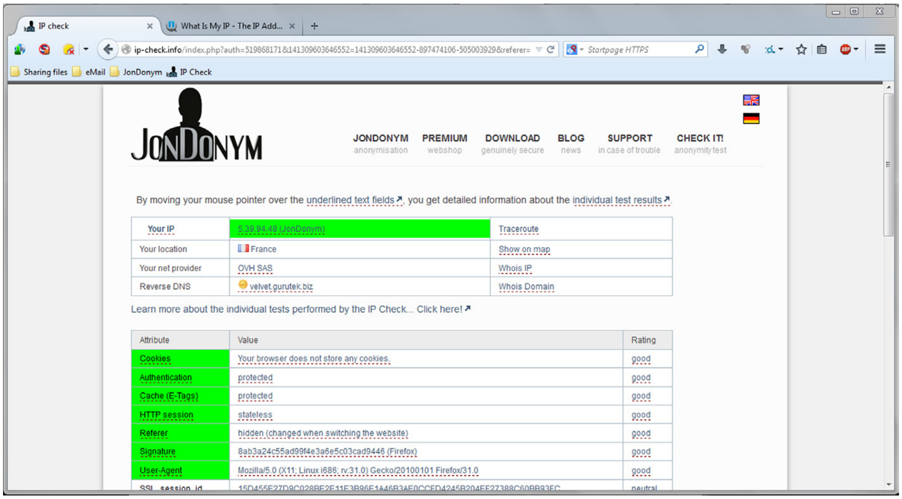
Encrypted data transferred: 3,128.7 KByte Activity: □□□□□□

Help other people (anti censorship) □ On Activity: □□□□□□

FIGURE 8.5

JonDo interface.

After providing the e-mail address we will get a link in our e-mail id. Visit the link to get the free code. Once we get the free code, put it in the software to complete the installation process.


IP check
What Is My IP - The IP Add...
ip-check.info/index.php?auth=519868171&141309603646552=141309603646552-897474106-505003929&referer=
Startpage HTTPS
Sharing files
eMail
JonDonym
IP Check
JONDONYM
JONDONYM anonymisation
PREMIUM webshop
DOWNLOAD genuinely secure
BLOG news
SUPPORT in case of trouble
CHECK IT! anonymity test

By moving your mouse pointer over the underlined text fields ↗, you get detailed information about the individual test results ↗.

Your IP	5.39.94.48 (JonDonym)	Traceroute
Your location	France	Show on map
Your net provider	OVH SAS	Whois IP
Reverse DNS	velvet.gurutek.biz	Whois Domain

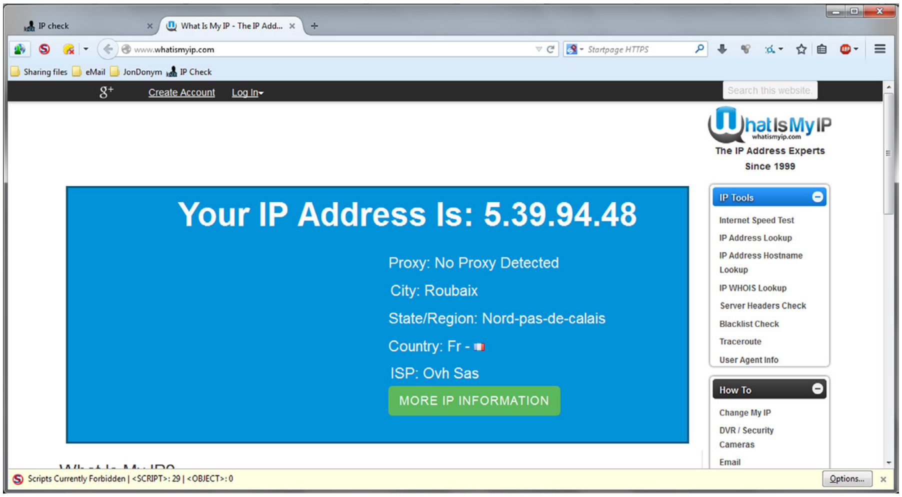
Learn more about the individual tests performed by the IP Check... Click here! ↗

Attribute	Value	Rating
Cookies	Your browser does not store any cookies.	good
Authentication	protected	good
Cache (E-Tags)	protected	good
HTTP session	stateless	good
Referer	hidden (changed when switching the website)	good
Signature	8ab3a24c55ad99f4e3a6e5c03cad9446 (Firefox)	good
User-Agent	Mozilla/5.0 (X11; Linux i686; rv:31.0) Gecko/20100101 Firefox/31.0	good
SSL_session_id	15D455F27D9C028BE2E11F3B96F1A46B3AE0CCED4245B204EE27388C60BB93EC	neutral

FIGURE 8.6

JonDO test.

If you want to use JonDo you need to install JonDoFox also; as we already covered JonDoFox, we can assume that it is already present in the system. When both the softwares are installed in a system, if we want to use just JonDoFox then we can simply use that by opening Firefox with JonDoFox profile. To test whether we are browsing anonymously, we just need to check the IP address using whatismyipaddress.com.



Your IP Address Is: 5.39.94.48

Proxy: No Proxy Detected

City: Roubaix

State/Region: Nord-pas-de-calais

Country: Fr -

ISP: Ovh Sas

What Is My IP?

Scripts Currently Forbidden | <SCRIPT>: 29 | <OBJECT>: 0

FIGURE 8.7

JonDo running.

If we want to use JonDo then we need to configure the same in the browser. In case of Mozilla go to Tools → Options → Advanced → Network → Connection Settings → select Manual proxy configuration and use 127.0.0.1:4001 as the default port used by JonDo is 4001.

Once it's done, open Firefox with JonDoFox profile, we will see a JonDo icon in the top left corner. Click there and it will open a tab. Select "Test Anonymity" to check the IP address.

JonDo provides us with a set of proxy servers that can be changed quite easily from the dropdown box. So it is also known as JonDo the IP changer proxy solution.

As we already discussed about how to use JonDo and its paid solution for full anonymity. This tool has variety of features but the major one is its compatibility with different operating systems. This makes JonDo unique in proxy solutions.

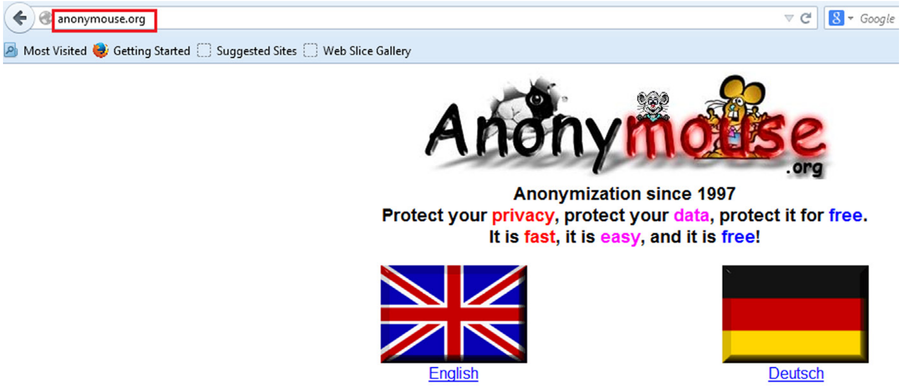
WEB-BASED PROXY

Web-based proxy solutions are the simple and efficient way of getting anonymity. The best thing is that we can use them anywhere. No setup needed. No dependencies. Best to use when using a shared computer or in public computers for browsing and sometime when using open Wi-Fi connections. The simple user interface makes it very popular to use. Just open the browser and open the proxy, and you are good to go.

There are many web-based proxy solutions. Some are just used for browsing and other may have more features like sending e-mails anonymously or reading news feeds. It's just depending upon our requirement and the anonymity level provided to choose a particular web-based proxy solution.

anonymouse.org

If user just wanted to browse anonymously there are different live anonymous browsing options available. One of such is anonymouse.org.

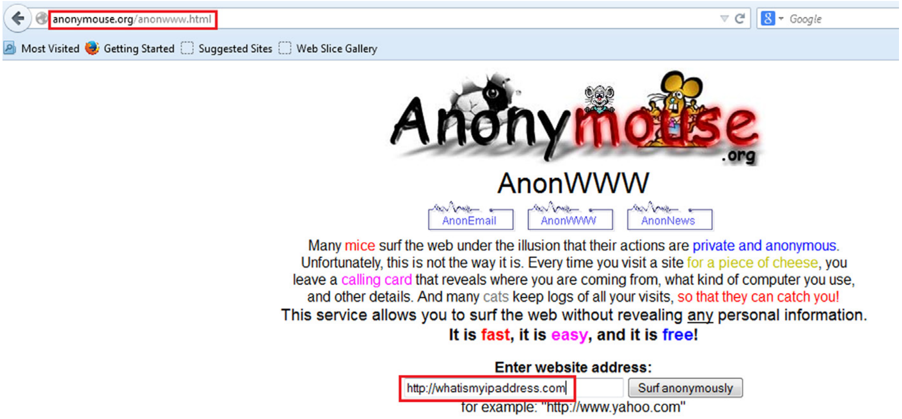


Anonymization since 1997
Protect your privacy, protect your data, protect it for free.
It is fast, it is easy, and it is free!

FIGURE 8.8

Anonymouse homepage.

It is a free site which provides its users to browse anonymously with two different languages, English and Dutch. Visit the site, choose the language in which you want to browse then type the site name in the Surf anonymously field and click on Surf anonymously to browse the site.



Many mice surf the web under the illusion that their actions are private and anonymous. Unfortunately, this is not the way it is. Every time you visit a site for a piece of cheese, you leave a calling card that reveals where you are coming from, what kind of computer you use, and other details. And many cats keep logs of all your visits, so that they can catch you!

This service allows you to surf the web without revealing any personal information.

It is fast, it is easy, and it is free!

Enter website address:

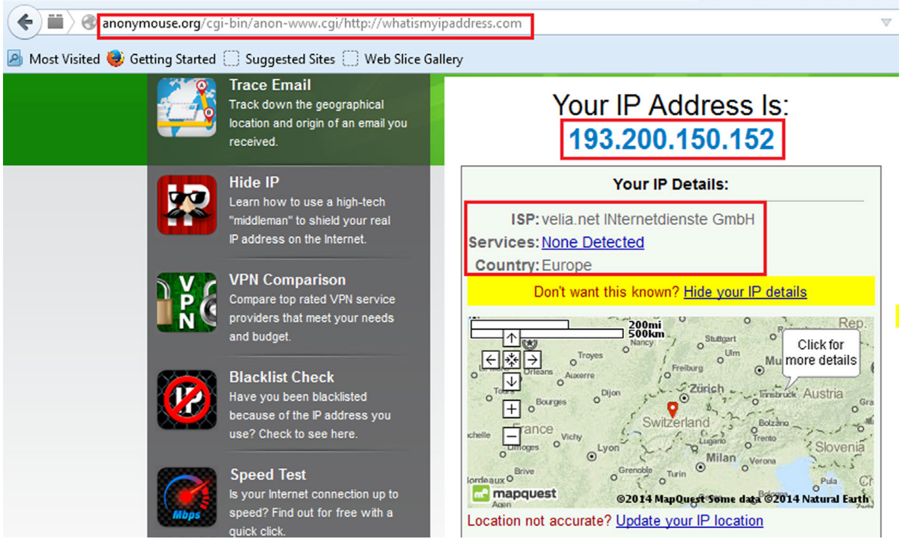
http://whatismyipaddress.com

for example: "http://www.yahoo.com"

FIGURE 8.9

Enter website address: Anonymouse.

The only disadvantage of this site is it only supports http protocol not https. But apart from that it provides better anonymity as we can see from the below image, it's not detected as proxy server. And the IP address is also from a different location.


anonymouse.org/cgi-bin/anon-www.cgi/http://whatismyipaddress.com
Most Visited
Getting Started
Suggested Sites
Web Slice Gallery

Trace Email
Track down the geographical location and origin of an email you received.

Hide IP
Learn how to use a high-tech "middleman" to shield your real IP address on the Internet.

VPN Comparison
Compare top rated VPN service providers that meet your needs and budget.

Blacklist Check
Have you been blacklisted because of the IP address you use? Check to see here.

Speed Test
Is your Internet connection up to speed? Find out for free with a quick click.

Your IP Address Is:
193.200.150.152

Your IP Details:

ISP: velia.net INternetdienste GmbH
Services: None Detected
Country: Europe

Don't want this known? Hide your IP details

Location not accurate? Update your IP location

FIGURE 8.10

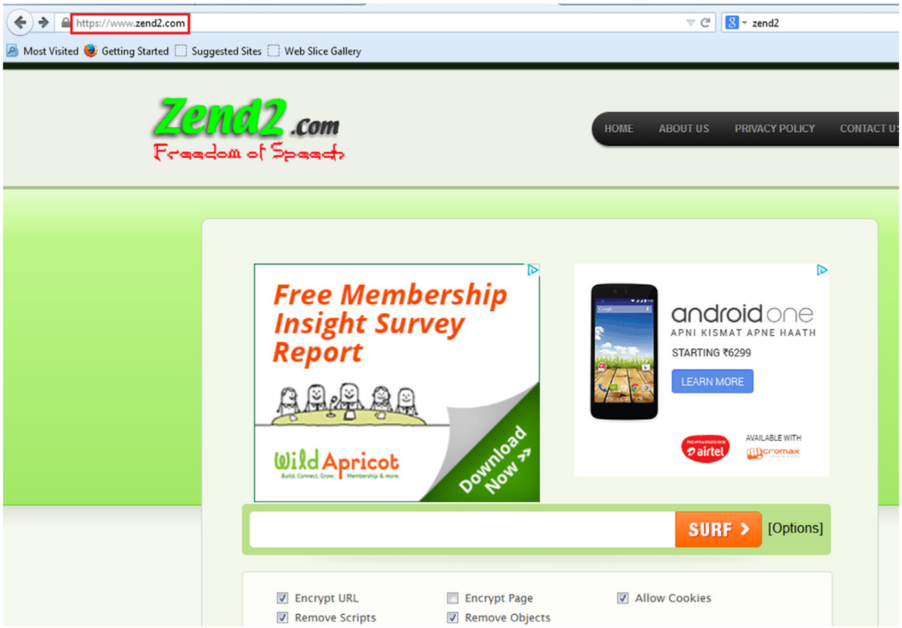
Anonymouse test.

As we discussed the pros and cons of this service still it's very good proxy solution for anonymous browsing and there are some other features like send e-mail and check e-news available. But as we are more focused on hiding our details on browsing, right now we will conclude this here itself.

Zend2

It is also a web-based proxy solution unlike anonymouse.org, which only supports http protocol. So user cannot use anonymouse.org to browse popular sites such as Facebook and YouTube as these sites force to use https connection.

https://www.zend2.com/ has no restrictions on https-enabled sites or technically SSL-enabled sites. It allows user to surf both http and https sites. So user can use the same to check his/her e-mails also.



☑ Encrypt URL ☐ Encrypt Page ☑ Allow Cookies
☑ Remove Scripts ☑ Remove Objects

FIGURE 8.11

Zend2 homepage.

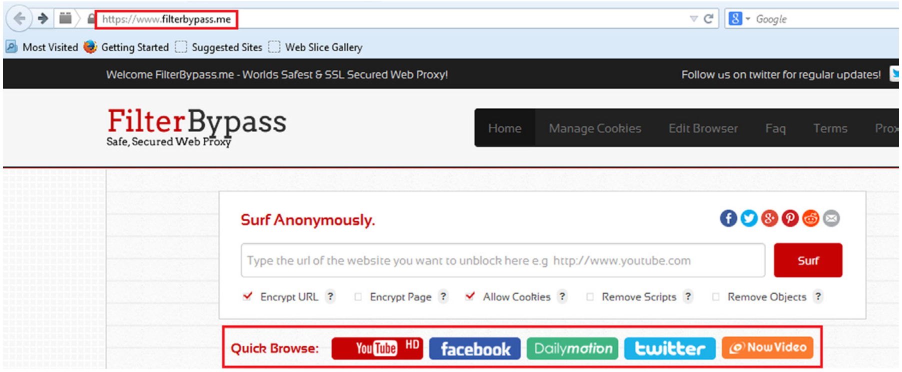
Apart from that for two popular web resources such as Facebook and YouTube, it also provides special GUI to use. For Facebook: https://zend2.com/facebook-proxy/. For YouTube: https://zend2.com/youtube-proxy/. The YouTube proxy page contains instructions how to unblock YouTube if it's blocked in your school, college, office, or by the ISP while the Facebook proxy page contains general information how this web proxy works.

Though we can use all these three user interfaces to visit any site, as the bottom line of all, we want it to work as intermediary between user and the server. Apart from just surfing it also provides user some options to choose such as:

- Encrypt URL
- Encrypt Page
- Allow Cookies
- Remove Scripts
- Remove Objects
- User can check whatever he/she wants as per the requirement.

FilterBypass.me

Similar to zend2 it also allows users to surf anonymously with some more options such as Encrypt URL, Allow cookie etc. The only drawback of the proxy solution is that it fails to resolve some of the e-mail-providing sites but apart from that its user interface contains some popular site links that can be visited directly using this such as Facebook, YouTube, DailyMotion, Twitter etc.



https://www.filterbypass.me

Welcome FilterBypass.me - Worlds Safest & SSL Secured Web Proxy!

Follow us on twitter for regular updates!

Surf Anonymously.

Type the url of the website you want to unblock here e.g http://www.youtube.com

✓ Encrypt URL ? □ Encrypt Page ? ✓ Allow Cookies ? □ Remove Scripts ? □ Remove Objects ?

FIGURE 8.12

FilterBypass homepage.

Boomproxy.com

It is quite similar to anonymouse.org as it only supports http sites to browse but the only extra feature available here is that it contains options such as Encrypt URL, Remove Objects etc.

Some more proxy solutions:

- http://www.internetcloak.com/
- http://www.crownproxy.com/
- http://www.hidesurf.us/
- http://www.webevade.com/
- http://www.proxyemails.com/
- http://www.proxytopsite.us/

Continued

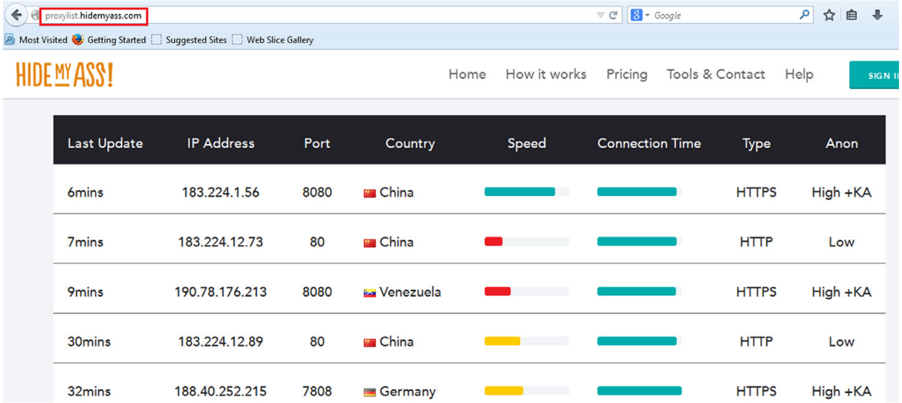
—cont'd

- http://www.proxysites.net/
- http://www.everyproxy.com/
- http://www.ip-hide.com/
- http://www.greatproxies.com/
- http://proxy.org/
- http://www.proxyservers.info/
- http://thehiddenguide.com

HOW TO SET UP PROXY MANUALLY IN A BROWSER

There are many sites that provide proxy addresses in terms of IP and port but it's not that easy to get the genuine site. It's because the list might not be updated for sometime and in the meanwhile the proxy server might not be working anymore. Though we can get still a good amount of sites, a good one is http://proxylist.hidemyass.com/.

The major benefit that user will get using this is it provides user a updated list with latest proxy IP addresses and port number along with that the expected speed, anonymity level, and country name where that IP belongs.



Last Update	IP Address	Port	Country	Speed	Connection Time	Type	Anon
6mins	183.224.1.56	8080	China	🟩	🟩	HTTPS	High +KA
7mins	183.224.12.73	80	China	🟥	🟩	HTTP	Low
9mins	190.78.176.213	8080	Venezuela	🟥	🟩	HTTPS	High +KA
30mins	183.224.12.89	80	China	🟨	🟩	HTTP	Low
32mins	188.40.252.215	7808	Germany	🟨	🟩	HTTPS	High +KA

FIGURE 8.13

HideMyAss proxy list.

Apart from that it also allows user to filter the requirements based on country, protocol supported, connection speed, anonymity level, and many more. So this is one of the finest sources in terms of using the proxy IP and port.

Though most of the case the IP and port will work but before using it, it's better to test whether the IP is alive or not.

So simply choose an IP address and associated port based upon the requirement such as based on speed, protocol, anonymity level, and country. Try to choose the latest one which is updated in the list recently. Then open command prompt in case of Windows and terminal in case of Mac and Linux. In case of

Windows, type "ipconfig" and the chosen IP address to check whether the IP is alive or not and in case of Mac and Linux the command is "ifconfig" with the chosen IP address.

Once we see the IP is alive, configure the same in browser. In case of Mozilla Firefox we did it earlier but let's revise the process.

Go to Tools → Options → Advanced → Network → Connection Settings → select Manual proxy configuration and use the chosen IP address and port number in respective fields.

In case of Chrome go to Settings → Show advanced settings → under Network tab click on Change proxy settings → click on LAN settings → check Use a proxy server for LAN then use the chosen IP address and port number in respective fields.

This is how proxy can be configured manually.

VIRTUAL PRIVATE NETWORK

Simply stated it allows us to create a private network across a public network. Most of the organizations use an internal private network for their day to day operations, but sometimes people need to access this network from outside, where there is no direct connection to this network. This is when VPN comes into play; it allows users to access the private network from the internet securely.

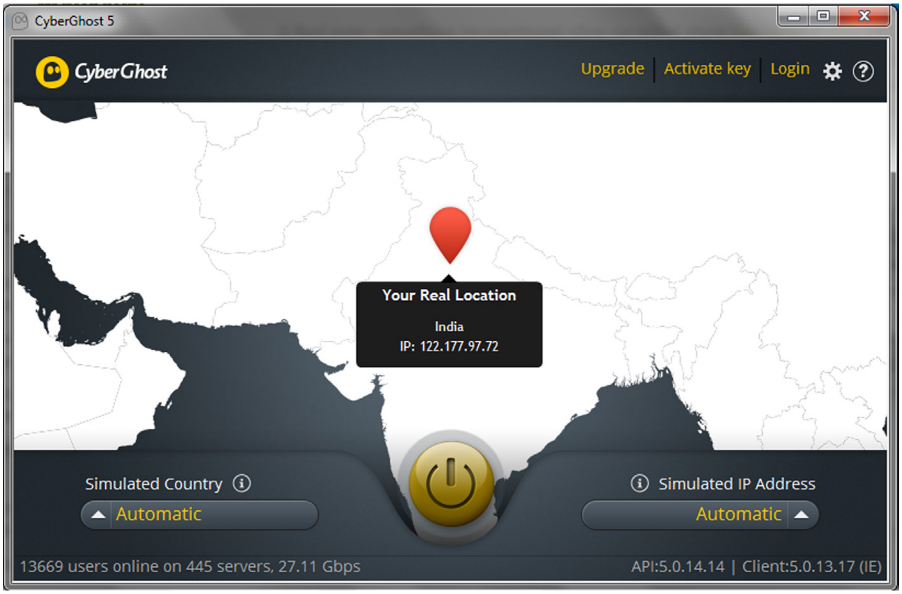
VPN basically creates a virtual point to point connection between two machines. The VPN server is installed at one point and the user accesses it using a VPN client. VPN uses different mechanisms and technologies, such as authentication, authorization, encryption etc., to achieve this and keep the connection secure. There are various use cases and implementations of VPN and how it operates, but in this chapter our main focus is on its use to stay anonymous.

VPN-based anonymity works similar to the proxy-based anonymity, the only major difference is the connection to the server is made using a VPN which adds an extra layer of security, though we should not forget that here we are trusting the VPN service provider to be secure.

There are various such services available online and most of them are paid. Here we are listing two services which provide a free version, but they do come with their own restrictions such as limited time, speed etc.

cyberghostvpn.com

CyberGhost is one of the best VPN-based anonymity providers. It provides both free and paid service. To use the service we need to download the client from the website http://www.cyberghostvpn.com. Once the client is downloaded we can simply install it and start the application.



Your Real Location

India

IP: 122.177.97.72

Simulated Country: Automatic

Simulated IP Address: Automatic

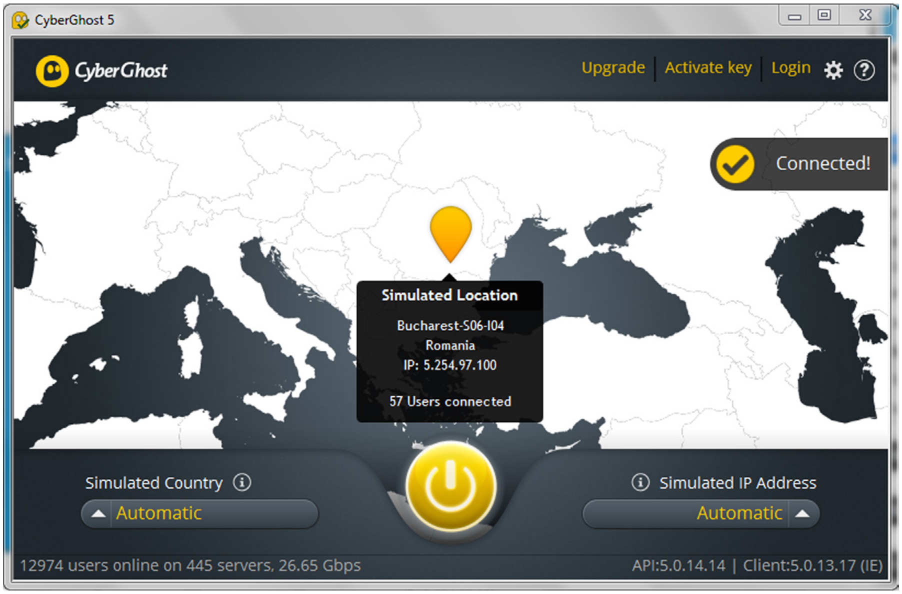
13669 users online on 445 servers, 27.11 Gbps

API:5.0.14.14 | Client:5.0.13.17 (IE)

FIGURE 8.14

CyberGhost interface.

The interface of the application is pretty simple. We can make the configuration changes and also upgrade to a paid account from it. On the home screen the application will display our current IP address with the location in map. To start using the service we simply need to click on the power button icon. Once we click on it CyberGhost will initiate a connection to one of the servers and will display a new location once the connection is made.



Connected!

Simulated Location

Bucharest-S06-I04

Romania

IP: 5.254.97.100

57 Users connected

Simulated Country: Automatic

Simulated IP Address: Automatic

12974 users online on 445 servers, 26.65 Gbps

API:5.0.14.14 | Client:5.0.13.17 (IE)

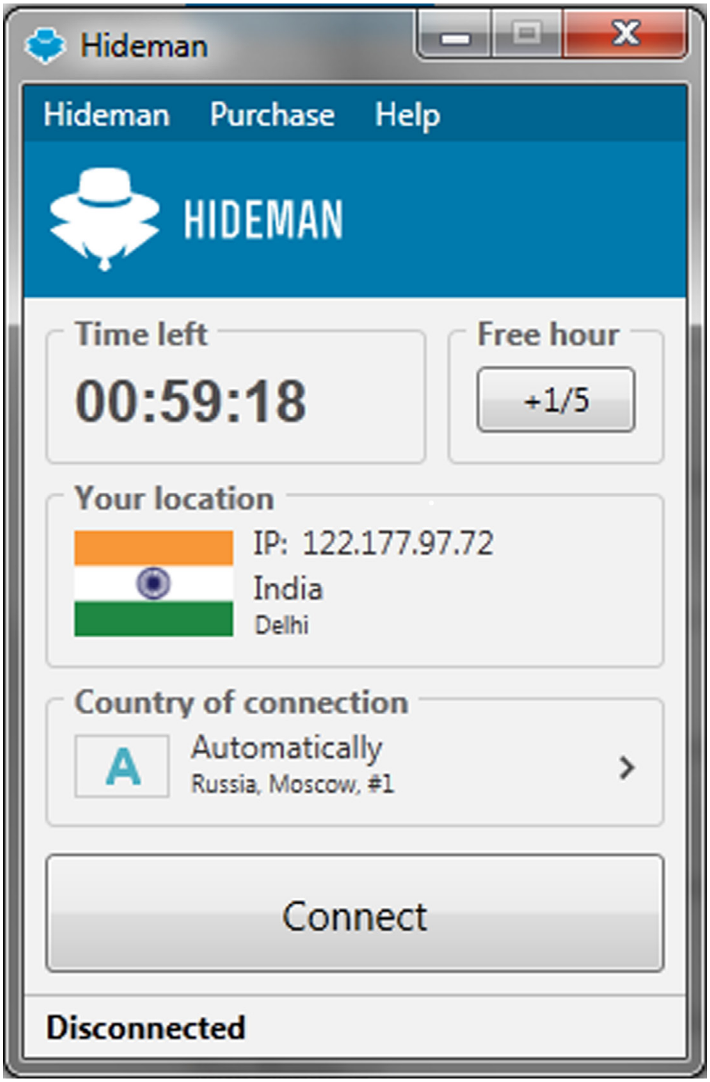
FIGURE 8.15

CyberGhost in action.

In the settings menu of CyberGhost we can also make changes such as Privacy Control and Proxy which further allows us to hide our identity while connected online.

Hideman

Similar to CyberGhost, Hideman is another application which allows us to conceal our identity. The client for the application can be downloaded from https://www.hideman.net/. Like CyberGhost, in Hideman also we don't need to make much configuration changes before using it, simply install the application and we are good to go. Once the application is installed, it provides a small graphical interface, which displays our IP and location. Below that there is an option where we can choose the country of connection, which is set to "Automatically" by default. Once this is done we simply need to click on the Connect button and the connection will be initiated. Currently Hideman provides free usage for 5 hours a week.



Time left

00:59:18

Free hour

+1/5

Your location

IP: 122.177.97.72
India
Delhi

Country of connection

A Automatically
Russia, Moscow, #1

Disconnected

FIGURE 8.16

Hideman interface.

Apart from the mentioned services there are also many other ways to utilize VPN for anonymity. Some service providers provide VPN credentials which can be configured into any VPN client and can be used, others provide their own client as well as the credentials.

ANONYMOUS NETWORKS

An anonymous network is a bit different in the way it operates. In this the traffic is routed through a number of different users who have created a network of their own inside the internet. Usually the users of the network are the participants and they help each other to relay the traffic. The network is built in a way that the source and the destination never communicate directly to each other, but the communication is done in multiple hops through the participating nodes and hence anonymity is achieved.

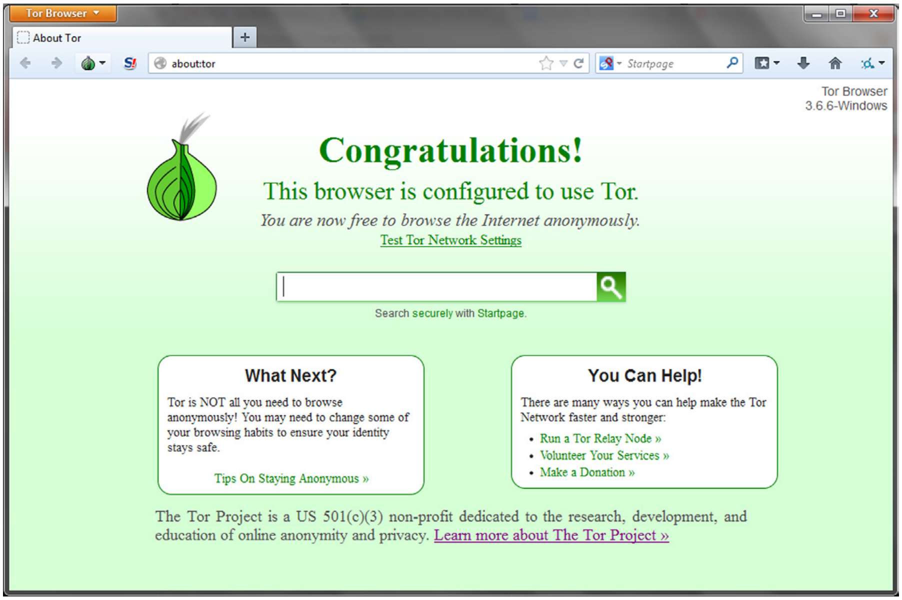
The Onion Router

Tor stands for "The Onion Router." It is one of most popular and widely used methods to stay anonymous online. It is basically a software and an open network which allows its users to access the web anonymously. It started as a US navy research project and now is run by a nonprofit organization. The user simply needs to download and install the Tor application and start it. The application starts a local SOCKS proxy which then connects to the Tor network.

Tor uses layered encryption over bidirectional tunnels. What this means is that once the user is connected to the Tor network, he/she sends out the data packet with three layers of encryption (default configuration) to the entry node of the Tor network. Now this node removes the uppermost layer of the encryption as it has the key for that only but the data packet is still encrypted, so this node knows the sender but not the data. Now the data packet moves to second node which similarly removes the current uppermost encryption layer as it has the key for that only, but this node does not know the data as well as the original sender. The packet further moves to the next node of the Tor network, which removes the last encryption layer using the key which works for that layer only. Now this last node, also called the exit node has the data packet in its raw form (no encryption) so it knows what the data is, but it is not aware who the actual sender of the data is. This raw data packet is then further sent to public internet to the desired receiver, without revealing the original sender. As already stated this is bidirectional so the sender can also receive the response in similar fashion. One thing that needs to be mentioned here is that the nodes of the Tor network between which the data packet hops are choosen randomly, once the user wants to access another site, the Tor client will choose another random path between the nodes in the Tor network. This complete process is termed as onion routing.

So Tor is pretty good at what it does and we just learned how it works. But as we need to use different nodes (relay points) and there is also cryptographic functions involved, which makes it pretty slow. Apart from this we are also trusting the exit nodes with the data (they can see the raw packet).

Tor is available in many different forms, as a browser bundle, as a complete OS package etc. The browser bundle is the recommended one as it is completely preconfigured, very easy to use, and comes with additional settings which helps to keep the user safe and anonymous. The browser bundle is basically a portable Firefox browser with Tor configured. It also contains some additional addons such as HTTPS Everywhere, NoScript. Tor browser can be downloaded from https://www.torproject.org/download/download-easy.html.en. Once it is downloaded we simply need to execute the exe file and it will extract it in the mentioned directory. After this has been completed we simply need to execute the "Start Tor Browser" application, which is a portable Firefox browser with Tor configured. It will present us with the choice to connect directly to the Tor network or configure it before going forward. General users simply need to click on the Connect button, in case the network we are connected to requires proxy or other advanced settings, we can click on the Configure button to make these settings first. Once we are good to go, we can connect to the network and the Tor browser will open up as soon as the connection is made. Apart from this other packages which allow us to run bridge, relay, and exit nodes can be downloaded from https://www.torproject.org/download/download.html.en.



Congratulations!

This browser is configured to use Tor.

You are now free to browse the Internet anonymously.

Test Tor Network Settings

Search securely with Startpage.

What Next?

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

Tips On Staying Anonymous »

You Can Help!

There are many ways you can help make the Tor Network faster and stronger:

- Run a Tor Relay Node »
- Volunteer Your Services »
- Make a Donation »

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »

FIGURE 8.17

Tor Browser.

Apart from allowing users to surf the web anonymously, Tor also provides another interesting service, about which we will learn in next chapter.

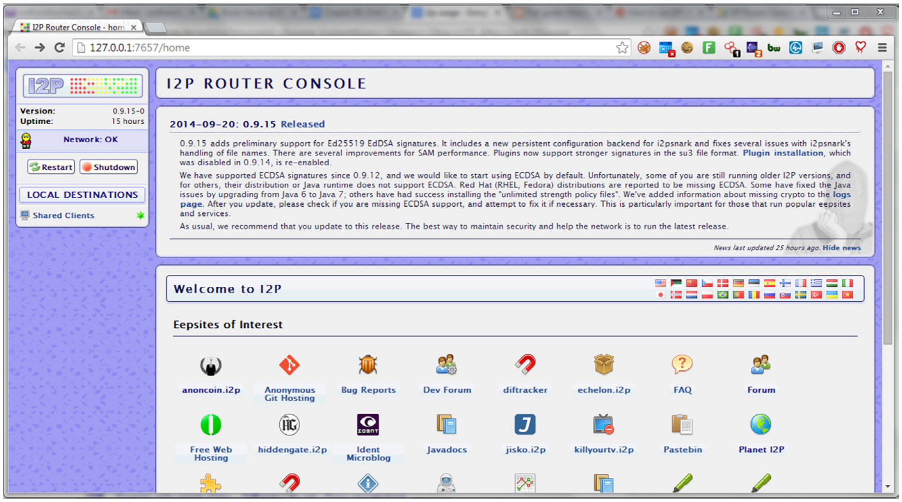
Invisible Internet Project

I2P stands for Invisible Internet Project. Similar to Tor, I2P is also an anonymous network. Like any network there are multiple nodes in this network, which are used to pass the data packets. As opposed to Tor, I2P is more focused on internal services.

What this means is that Tor's main focus is to allow people to access the clear web (explained in next chapter, for now let's just say the part of web accessible without any restrictions) anonymously, whereas I2P focuses more on allowing people to use the web anonymously but in the context of the applications/features available in it, such as e-mail services, IRCs, Torrents, etc.

Unlike Tor, I2P uses layered encryption over unidirectional connections. Each I2P client application has I2P routers, which builds inbound and outbound tunnels. So each client has different incoming and outgoing points. When a client needs to send a message to another client, it sends it to its outbound tunnel with specifying the target. Depending upon the configuration this message will hop through a number of clients and eventually will reach the inbound node of the target and then the target. To receive the message in reverse order the same process will be followed but the nodes involved will be different as the inbound and outbound tunnels are separated from each other for each node. Any content that is passed over I2P is passed using layered encryption. The layers are garlic encryption, which is between the starting node of the sender outbound tunnel to the end node of the receiver inbound tunnel; tunnel encryption, which is between the starting node of the outbound tunnel to the end node of it and the starting node of the inbound tunnel to the end node of it; transport encryption, which is between the each node and its next hop.

I2P can be downloaded from https://geti2p.net/en/download. The installation of the application is pretty simple and straightforward. Once the installation is completed we simply need to open "Start I2P," it will open up the router console. In case the web page does not open up we can simply browse to the URL http://127.0.0.1:7657/home and we will get a page showing the status. Once the application has made connection to other nodes we will get a "Network: OK" status. Now we need to configure a browser to connect through I2P, for this we need to add a Manual proxy setting to the IP address 127.0.0.1 and port 4444. It is also suggested to add "localhost, 127.0.0.1" to the "No Proxy for" box. Once the proxy settings are done we can surf the web using this browser anonymously.



I2P ROUTER CONSOLE

Version: 0.9.15-0
Uptime: 15 hours
Network: OK

2014-09-20: 0.9.15 Released

0.9.15 adds preliminary support for Ed25519 EdDSA signatures. It includes a new persistent configuration backend for i2psnark and fixes several issues with i2psnark's handling of file names. There are several improvements for SAM performance. Plugins now support stronger signatures in the su3 file format. Plugin installation, which was disabled in 0.9.14, is re-enabled.

We have supported ECDSA signatures since 0.9.12, and we would like to start using ECDSA by default. Unfortunately, some of you are still running older I2P versions, and for others, their distribution or Java runtime does not support ECDSA. Red Hat (RHEL, Fedora) distributions are reported to be missing ECDSA. Some have fixed the Java issues by upgrading from Java 6 to Java 7; others have had success installing the "unlimited strength policy files". We've added information about missing crypto to the logs page. After you update, please check if you are missing ECDSA support, and attempt to fix it if necessary. This is particularly important for those that run popular eepsites and services.

As usual, we recommend that you update to this release. The best way to maintain security and help the network is to run the latest release.

News last updated 25 hours ago. Hide news

Welcome to I2P

Eepsites of Interest

FIGURE 8.18

Invisible Internet Project. Network: OK.

Similar to Tor, I2P also provides other services which we will discuss in next chapter.

Browser addons like FoxyProxy (http://getfoxyproxy.org/) can be used to make the proxy changes easily in the browser.

The individual techniques we have discussed in this chapter can also be chained together to make it more difficult to get traced. For example, we can connect to a VPN-based proxy server, further configure it to connect to another proxy server in another country, and then use a web-based proxy to access a website. In this case the web server will get the IP address of the web-based proxy server used to connect to it, and it will get the IP address of the proxy server we connected through the VPN; we can also increase the length of this chain by connecting one proxy to another. There is also a technique called proxy bouncing or hopping in which the user keeps on jumping from one proxy to another using an automated tool or custom script with a list of proxies, in this way the user keeps on changing his/her identity after a short period of time and hence makes it very difficult to be traced. This can also be implemented at server side.

Some scenarios in which people still get caught after using these tools/techniques:

- The user of a specific network (e.g., University) is known, and it is also known that which one of them was connected to a specific proxy server/Tor around a specific time.
- Rogue entry and exit points. In an anonymous network like Tor if the entry point and the exit point can correlate the data packet based on its size or some other signature, they can identify who the real sender might be.
- DNS leak. Sometimes even when we are connected to an anonymous network our machines might send out the DNS requests to the default DNS server instead of the DNS server of the anonymous network. It means that the default DNS server now may have a log that this specific address resolution was requested by this IP at this point of time.
- Leaked personal information. Sometimes people who are anonymous to the internet leak some information which can be used to directly link it to them such as phone numbers, same forum handles which is used by them when they are not anonymous, unique ids etc.
- Metadata. As discussed in the last chapter there is so much hidden data in the files that we use and it might also be used to track down a person.
- Hacking. There can be security holes in any IT product which can be abused to identify the real identity of the people using it.
- Basic correlation. As shown in the first scenario, correlation can be used to pinpoint someone based on various factors such as timing, location, restricted usage, and other factors.

Some of the suggestions/warnings for using Tor are listed at https://www.torproject.org/download/download-easy.html.en#warning. These should be followed with every tool/technique discussed above, where applicable. Also use a separate browser for anonymous usage only and do not install addons/plugins which are not necessary.

So we learned about various ways to stay anonymous online, but as stated earlier 100% anonymity cannot be guaranteed online. What we can do is to try to leak as little information about ourselves as possible. The methods discussed in this chapter are some of the most popular and effective ways to do this. Online anonymity can have various use cases such as privacy, protest, accessing what is restricted by the authority, business related, law enforcement, journalism but it can also be used by people to perform illegal activities like malicious hacking, illegal online trade, money laundering, selling drugs etc. We need to be very careful what we do with the knowledge we acquire.

Moving on, in the next chapter we will extend the topic and deal with the darknet and other associated terms. We will learn more about the tools like Tor and I2P and see what parts of the internet we haven't touched yet, how to access/create it, and what we can expect to find there.