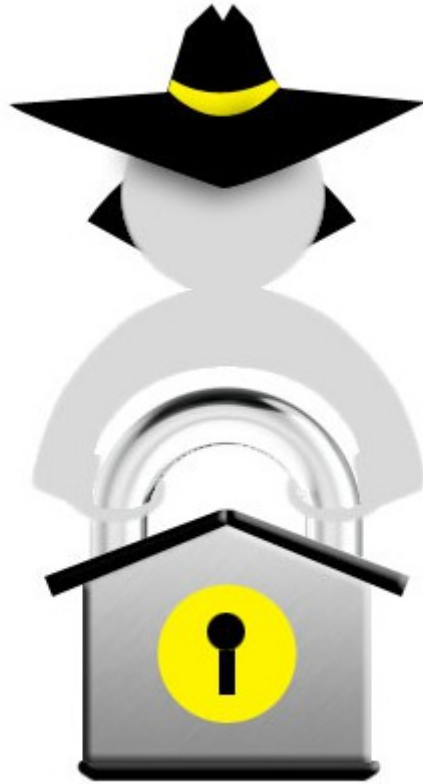# The Ultimate Anon Guide

V2 By School of Privacy

[Website](#) | [Twitter](#)

Guide on How To be Safe, Secure and Protect Your Online Anonymity.

Contents

Intro

We live in a different world now, whether we like to accept it or not, this new world is a Police state. For All people far and wide, you are under surveillance, everything you do, everyone you talk to will or can be recorded. Governments and corporations buy your rights for dirt cheap and they hurt the many to punish the few, Dragnet spying affects us all.

In 2009, 2,376 wiretaps were authorized in the United States (U.S.) for the purpose of rooting out criminal activity. The average cost per wiretap order was $52,200 U.S. Dollars (USD) and every request for a wiretap was approved that year. The federal government requested 663 and 24 of the U.S. states requested the remaining 1,713.

96% of the taps were on mobile phones, listening to drug chatter. The two nosiest states were California, with 425 wiretaps, and New York, with 402. The $52,200 resulted in 678 convictions out of 4,537 arrests. 19% of the overheard calls were incriminating.

In 2011, Law enforcement agencies in the U.S. made more than 1.3 million requests for consumers' cellphone records in. At AT&T, a team of more than 100 workers handle the requests pouring in from local, state and federal law enforcement agencies. More than 250,000 such requests came in last year, a more than two-fold increase over five years ago. Sprint said it received about 500,000 subpoenas in 2011. Verizon and T-Mobile, two other major U.S. carriers, both reported annual increases in requests exceeding 12 percent.

Cricket has seen a steady increase every year since 2007, and although the company once had a 10-person team handling inquiries, it has now outsourced that task to a company called Neustar. Many of the requests cover a number of cellphone subscribers. The costs have become so large that carriers have started charging law enforcement for the records they turn over.

AT&T collected almost $8.3 million in 2011 in fees from police agencies, although the company said it believes that number falls far short of what it costs AT&T to accommodate the requests. Police requesting data from U.S. Cellular services are asked to pay $25 to locate a cellphone using GPS (the first three requests are free), $25 to retrieve a user's text messages and $50 for a "cell tower dump".

A breakdown of all the cellphones that interacted with a given cellphone tower at a specific time. These are just covering phones; ISP's receive just as many requests if not more. These are terrifying numbers for ILLEGAL spying, and your ISP's, phone providers and most services retain this data for extremely long times and in great detail.

"On 15 March 2006 the European Union adopted the Data Retention Directive, on "the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and

amending Directive 2002/58/EC". The Directive requires Member States to ensure that communications providers retain, for a period of between 6 months and 2 years, necessary data as specified in the Directive"

And your emails;

"Emails are currently intercepted via the ISP (Internet Service Provider). Technical details about this are not released. In the press the method of interception are referred to as "black boxes" at the ISP. In all probability these black boxes are an advanced a network tap/packet sniffer, which pulls out all of the required information for a given protocol."

The ISPs are required under RIPA to provide the ability to maintain interception capability. This means that the government, when required, can monitor any person's internet activity. In the US "Individual ISPs are essentially free to keep or delete your data as they see fit, with little regulations in place. Because ISPs are private companies, they're not obligated to reveal how long they keep customer data. So it's hard to find out what each ISP's individual policy on data retention actually is. Some may delete the data after 30 days, some may hold onto it for longer."

There are no regulations on what they keep how long and how they use it, and they are not obligated to disclose information to you about their policies. This is a huge conflict of interest we keep data "don't worry about what data" we keep it for as long as we SEE FIT "none of your business how long" and we use it accordingly "don't worry how or for what". It is not your right to ask us about it either, that is an absurd stance on data retention.

Any law enforcement officer can request an administrative subpoena for your data and demand the third party keep the information of the request from you so that you may not use your legal right to defend yourself in Court to this violation of privacy. You have no say in the matter and your legal right to detest this injustice is null and void you won't even know it's happening to you, it may have already happened. How would you know? This is your privacy don't leave yourself with questions like this, in this day and age encrypting every packet prevents this.

Jacob Applebaum is a victim of this "the founder of the Tor Project". "For the last two years, Appelbaum has been repeatedly detained and harassed at American airports upon his return to the country, including having his laptops and cellphone seized, all without a search warrant of course, and never returned. The U.S. Government has issued secret orders to Internet providers demanding they provide information about his email communications and social networking activities. He has never been charged with, let alone convicted of, any crime."

In the surveillance state we live in, it is not just your privacy that is violated, but your

dignity as well. You are no longer a person but rather a set of numbers, a few packets and a Geo location. You are a product. In many examples private companies have been proven to buy the personal information of people who are hurting their business such as political activists opposing chemical spills caused by big corporations, occupy Wall Street participants, and people who just tweet about the news. Having an opinion makes you a target to someone somewhere and if they have the money and power your privacy is theirs.

Possessed by third parties, you are for sale and you are guilty until proven otherwise. This Police State wishes to maintain so much control on you, me and everything we do and say, censorship and fighting dissent in all nations, they are terrified of a world with privacy and freedom, so they categorize this concept as chaotic and unmanageable.

So what do we do now? We fight back in our technocratic environments with the best tools man has to offer.

Personal Identifiable Information or D0x

In this day and age, your Personal Identifiable Information (PII) or your "D0x" is everywhere. From Social Networks to Profiles made on a game console, this will leave traces of your identity back to you quickly and easily for anyone to access publicly and legally. It is known and proven that employers use this information to research a desired employee, government agencies use this for spying or investigative purposes and identity thieves use this for social engineering purposes. Here is some information you can use to find this information yourself and rid the internet of it, eliminating all traces of who you are and making it more difficult to be spied on and found.

Self Doxing, the way we mean here is NOT getting your personal information and releasing it to the public. This Self Dox tutorial will explain and help you with information about gathering all of the information you have online and either getting rid of it OR changing it to a misinformative profile.

Many reasons you would want to do this is quite simple, how can you be anonymous in any way if you can easily be traced to your private and or personal information? You have to use the same techniques you use on your intended targets to Dox yourself, and then cleanse the internet of your information. Now you might think to yourself "I think i am okay on this field, I will leave this for another time.", In fact that can be one careless mistake you might not want to make. Information is quite easily accessible to the world, all it takes is some crafty person to come along, grab you IP, email, first name and location and BAM! they got you.

To fully secure your anonymity, go to these sites listed here, enter your information, and check to make sure you have close to nothing out there (of course nothing being better, but sometimes can be hard to get rid of some information.) that can be traced back to you.

This site has great information on how data is stored, obtained and found.

http://www.spiesonline.net

This is a Dox Tool that was created by @Joepie91

- http://pastehtml.com/view/b1026x5qu.html

Misc. Search Sites:

- http://www.spokeo.com
- http://www.pipl.com
- http://www.peekyou.com/
- http://www.ipeople.com
- http://www.yasni.com
- http://www.skipease.com
- http://www.peekyou.com

- http://www.soople.com
- http://Abika.com
- http://freeality.com
- http://radaris.com
- http://wink.com/
- http://www.isearch.com/
- http://www.keotag.com/
- http://yahoo.intelius.com/
- http://www.findermind.com/free-people-search-engines/
- http://www.192.com/ (UK)

WhitePages Search:

- http://www.whitepages.com
- http://www.zabasearch.com/

Archives Search:

- http://aad.archives.gov/aad/series-list.jsp?cat=GS29
- http://www.archive.org/web/web.php

Social Network Searches:

- http://www.facebook.com/directory/people/
- http://topsy.com/
- http://monitter.com/ (Monitor twitter convos)
- http://socialmention.com/
- http://knowem.com/
- http://twoogel.com/
- http://www.yacktrack.com
- http://www.samepoint.com/
- http://www.whostalkin.com/
- http://namechk.com/

Phone Information & Lookups:

- http://www.freecellphonedirectorylookup.com
- http://www.numberway.com/
- http://www.fonefinder.net

Public & Criminal Records Search:

- http://publicrecords.onlinesearches.com
- http://www.jailbase.com/en/sources/fl-lcso/

To remove your webpages/results off of Google:

http://support.google.com/webmasters/bin/answer.py?hl=en&answer=164734

How to hide your tweets from Google:

http://lifehacker.com/5911079/how-to-hide-your-tweets-from-google

[Delete Your GMail](#) - GMail accounts can obtain A LOT of information, deleting them can be a ticket to your anonymous longevity.

[How to Permanently Delete a Facebook Account](#) - Deactivating your Facebook account will temporarily hide your information, but deletion is permanent. Here's how to completely remove your Facebook account.

Now a lot of these websites have a feature where you can remove your own data off of their sites. Be vigilant when looking at every corner of these websites as you can possibly miss one or two things. Double check after removing your data and always remember, MISINFORMATION MISINFORMATION MISINFORMATION. Never put any of your real information online at any costs, if you have absolutely no choice but to, then be sure if in a highly secure area and it is not visible to the public. Always trace your steps and be sure you did not leave any cookie crumbs laying around.

I STRONGLY RECOMMEND THIS SITE

http://www.accountkiller.com - It has information on how to remove just about every type of account online and is extremely helpful.

Layers of Protection

If you want to be anonymous online, we will have to start with choosing our first layer of protection, this will be a VPN. The VPN is a Multi-Protocol protected layer which if a protocol issue breaks the other layers, we will not be exposed. For example, when flash player, Microsoft Silverlight or QuickTime's packets are handled by Tor or other socks 4 and 5 proxies their security will be broken if not firewalled, a VPN is always the foundation of security.

So we must make good choices on Vpns and good Vpn practices, when a VPN says they don't log and offer multiple servers u have to research all the servers individual policies. This is a good start, you may be wondering why this is. Well many VPNs you may find may not log and they admit this, but that does not specify which servers they don't log on. This was found with PrivateTunnel.se and they have updated their terms of service to explain this for their US server.

Another major thing we must worry about is IP leakage which there are program and firewall ways to prevent this. Via TorrentFreak VPNetMon

"VPNetMon continuously watches the IP addresses of your PC. If the IP address of your VPN is not detected anymore, VPNetMon closes specified programs instantly. The program reacts so quickly that a new connection through your real IP will not be established by these applications," - creator Felix told TorrentFreak.

VPNetMon (Windows) can be downloaded [here](#).

"VPNCheck helps you to feel safe if your VPN connection breaks, this is done by shutting down your main network connection or programs of your choice and showing a notification box," Jonathan from Guavi.com told TorrentFreak. "Basically it constantly looks for a change in your VPN network adapter. You can connect to either PPTP or L2TP with VPNCheck."

VPNCheck (Windows/Linux) can be downloaded [here](#).

Now both of these options are good for our windows users and less technical users, I use vpncheck the free version on my windows boxes and you can firewall up to 3 applications in case of ip leakage .

Now for our Linux users we can use IPTables which is much more efficient. IPTables is a user space application program that allows a system administrator to configure the tables provided by the Linux kernel firewall (implemented as different NetFilter modules) and the chains and rules it stores. Different kernel modules and programs are currently used for different protocols; IPTables applies to IPv4, IP6Tables to IPv6, ARPTables to ARP, and

EBTables to Ethernet frames.

IPTables requires elevated privileges to operate and must be executed by user root, otherwise it fails to function. On most Linux systems, IPTables is installed as /usr/sbin/iptables and documented in its man page, which can be opened using man iptables when installed. It may also be found in /sbin/iptables, but since iptables is more like a service rather than an "essential binary", the preferred location remains /usr/sbin. IPTables is also commonly used to inclusively refer to the kernel-level components. x_tables is the name of the kernel module carrying the shared code portion used by all four modules that also provides the API used for extensions; subsequently, Xtables is more or less used to refer to the entire firewall (v4,v6,arp,eb) architecture. with this you can force default inbound and outbound ip regulations on Linux.

([Instructions](#))

So now that we are picking VPNs who do not log, checking TOS (Terms of Service) and which severs are un-logged and firewalling IP leakage its time to talk about DNS. Now a DNS leak can compromise your security because your ISP dns server is regional specific so even though your IP is protected the DNS narrows your location and gives what ISP you really use which can significantly single you out.
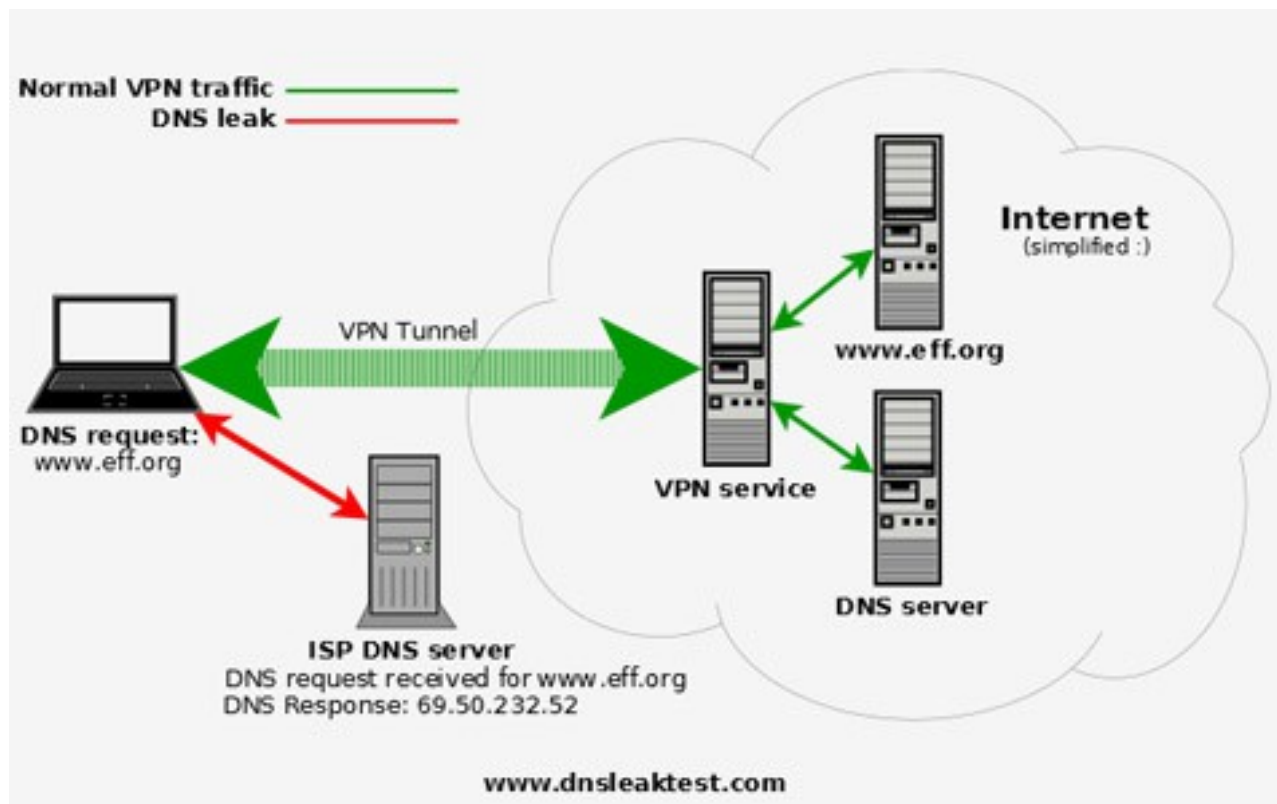
([Check your DNS](#))

And solutions to fix DNS leaks are [here](#).

And for PPTP VPNs there is a IPv6 vulnerability which can compromise you but is easily fixed

For Windows Vista and above:

Open cmd prompt and type: netsh interface teredo set state disabled.

For Ubuntu 10+: Copy and paste all four lines into a terminal:

echo "#disable ipv6″ | sudo tee -a /etc/sysctl.conf

echo "net.ipv6.conf.all.disable_ipv6 = 1″ | sudo tee -a /etc/sysctl.conf

echo "net.ipv6.conf.default.disable_ipv6 = 1″ | sudo tee -a /etc/sysctl.conf

echo "net.ipv6.conf.lo.disable_ipv6 = 1″ | sudo tee -a /etc/sysctl.conf

Now A list of privacy protecting vpn providers

- proxy.sh
- [TorGuard](#)
- [Btguard](#)
- [Privateinternetaccess](#)
- [vpntunnel.se](#)
- [TorrentPrivacy](#)
- [Cryptocloud](#)
- [BlackVPN](#)
- [Ipredator](#)
- [nVPN](#)
- [Anonine](#)

Now a VPN is a good start for your fail safe security against invasive protocols and applications if you do not block things properly, but we must not put our apples in one basket. So we must look elsewhere for a second layer we can go with tor, ssh tunneling or i2p.
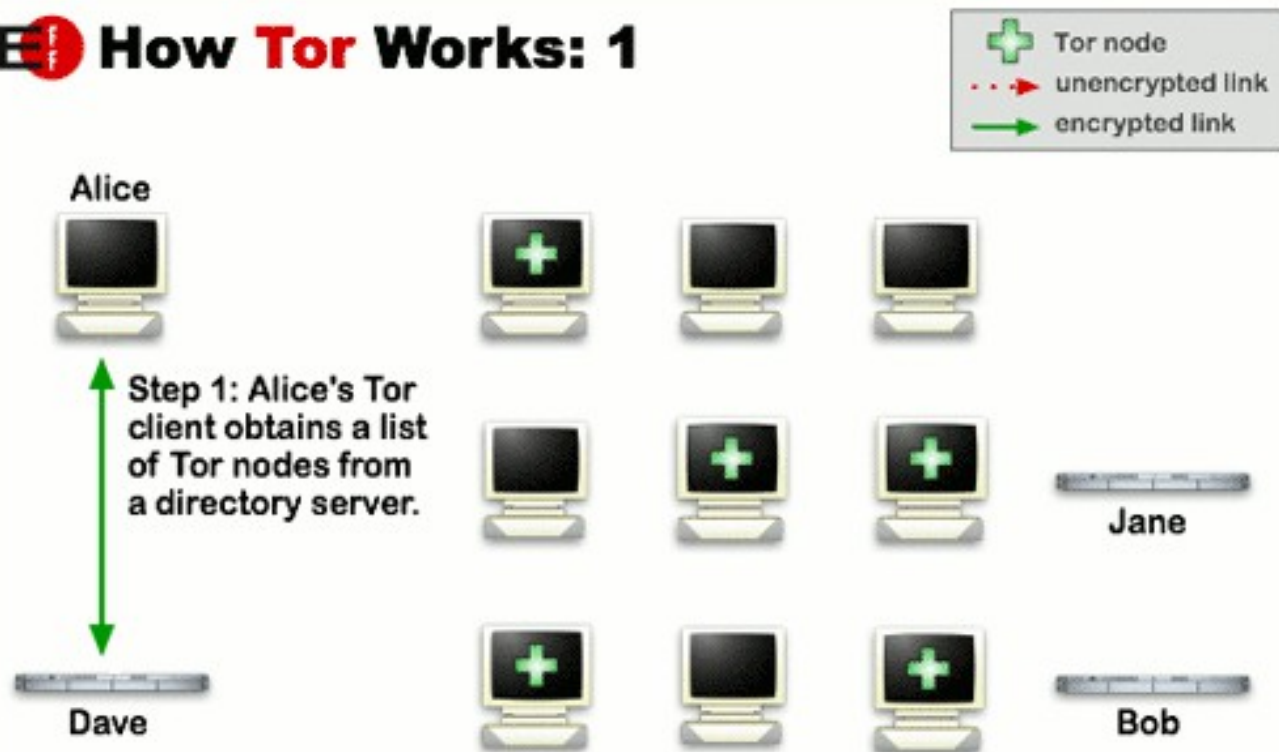
TOR

What is Tor?

Tor was originally designed, implemented, and deployed as a third-generation onion routing project of the U.S. Naval Research Laboratory. It was originally developed with the U.S. Navy in mind, for the primary purpose of protecting government communications. Today, it is used every day for a wide variety of purposes by normal people, the military, journalists, law enforcement officers, activists, and many others.
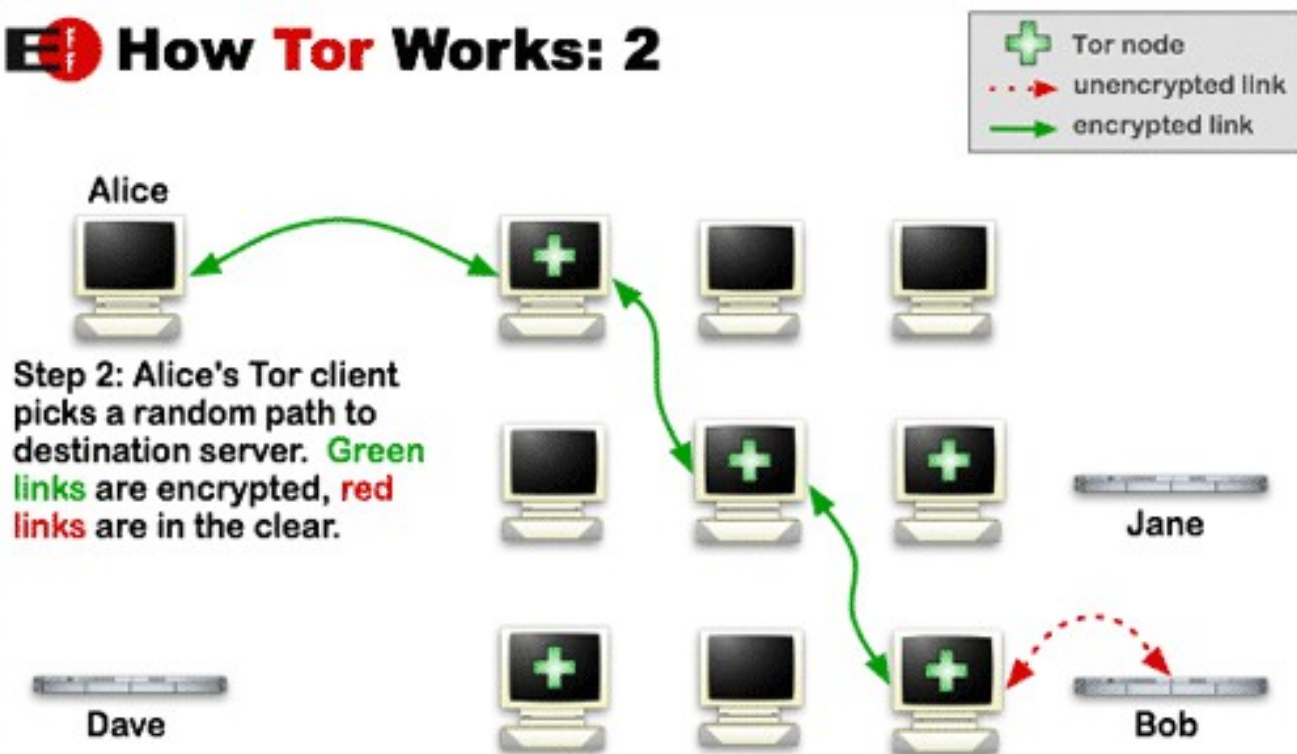
Why do we need Tor?

Using Tor protects you against a common form of Internet surveillance known as "traffic analysis." Traffic analysis can be used to infer who is talking to whom over a public network. Knowing the source and destination of your Internet traffic allows others to track your behavior and interests. This can impact your checkbook if, for example, an e-commerce site uses price discrimination based on your country or institution of origin. It can even threaten your job and physical safety by revealing who and where you are.
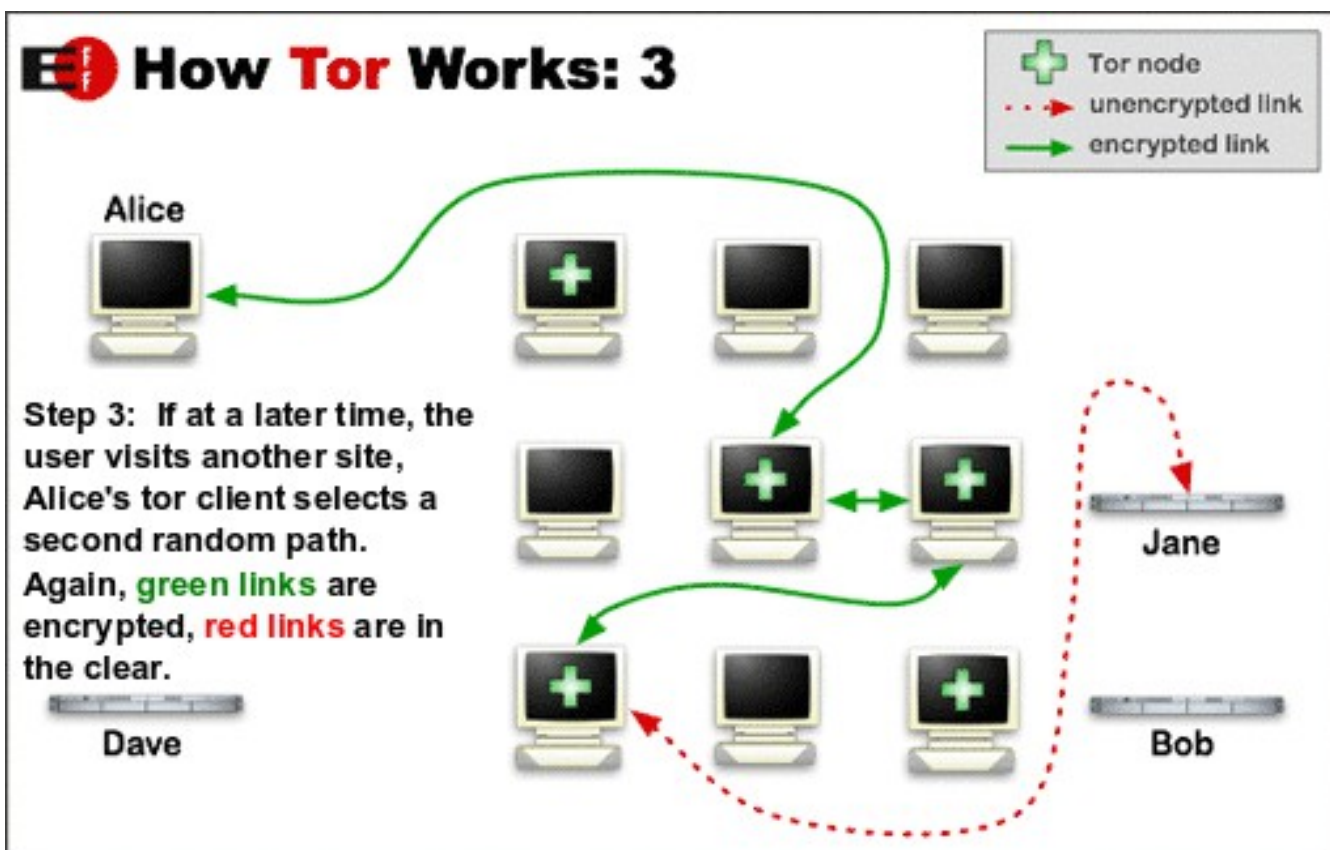
For example, if you're traveling abroad and you connect to your employer's computers to check or send mail, you can inadvertently reveal your national origin and professional affiliation to anyone observing the network, even if the connection is encrypted. Tor is a very great tool, but it is not entirely user friendly. It is most effective when configured properly and offers an extra proxy on top of its node set up. Tor also has an add on for *Firefox* called **TorButton** ([MacOS](#) | [Linux](#) | [Windows](#)) which works great if you use *Firefox*. For some people Tor can be a bit difficult to use at first but again, take your time to learn security and safety.

How Tor Works: 1

EFF

✚	Tor node
·· ▸	unencrypted link
→	encrypted link

Alice

Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.

Dave

Jane

Bob

How Tor Works: 2

EFF

✚	Tor node
·· ▸	unencrypted link
→	encrypted link

Alice

Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

Dave

Jane

Bob

How Tor Works: 3

	Tor node
· · · ►	unencrypted link
──►	encrypted link

Alice

Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.

Dave

Jane

Bob

And tor for phones

Orbot is an application that allows mobile phone users to access the web, instant messaging and email without being monitored or blocked by their mobile internet service provider. Orbot brings the features and functionality of Tor to the Android mobile operating system. Orbot contains Tor, libevent and privoxy. Orbot provides a local HTTP proxy and the standard SOCKS4A/SOCKS5 proxy interfaces into the Tor network. Orbot has the ability to transparently torify all of the TCP traffic on your Android device when it has the correct permissions and system libraries.

Proxy settings and Configuration

Orbot offers three interfaces into the Tor network:
- SOCKS 4A/5 proxy 127.0.0.1:9050
- HTTP proxy 127.0.0.1:8118
- Transparent proxying (on select devices)

For Instant Messaging, try Gibberbot, which includes support for connecting via Tor and Off-the-Record encryption.
(Install)

SSH Tunneling

A Secure Shell (SSH) Tunnel consists of an encrypted tunnel created through a SSH protocol connection. Users may set up SSH tunnels to transfer unencrypted traffic over a network through an encrypted channel. For example, Microsoft Windows machines can share files using the Server Message Block (SMB) protocol, a non-encrypted protocol. If one were to mount a Microsoft Windows file-system remotely through the Internet, someone snooping on the connection could see transferred files.

To mount the Windows file-system securely, one can establish a SSH tunnel that routes all SMB traffic to the remote fileserver through an encrypted channel. Even though the SMB protocol itself contains no encryption, the encrypted SSH channel through which it travels offers security.

To set up an SSH tunnel, one configures an SSH client to forward a specified local port to a port on the remote machine. Once the SSH tunnel has been established, the user can connect to the specified local port to access the network service. The local port need not have the same port number as the remote port. SSH tunnels provide a means to bypass firewalls that prohibit certain Internet services —so long as a site allows outgoing connections.

For example, an organization may prohibit a user from accessing Internet web pages (port 80) directly without passing through the organization's proxy filter ssh tunneling is a great resource to utilize if you or friends have a server. by creating a ssh user for yourself you can tunnel with your server as a proxy with 256 bit AES encryption and of course if you have root you can not log.

First we get a ssh client

Tunnelier Portable - this is our favorite, it has nice features, portable, smooth and efficient. you can download it here

or

PUTTY - which is a alternative ssh client and telnet client.

1. We start by putting our host, which is the server **IP address** and port **22** is the SSH port
2. Then we choose our login method which will be likely username, password unless you choose a different method.
3. Set your credentials in and login.
4. Now your ssh connection will be listening on 127.0.0.1 port 1080 unless you go into options and change the port which you can.

5. For any application just Plugin proxy settings host:127.0.0.1 port 1080* or your chosen port.

You are now tunneling through your 256 bit AES SSH tunnel, alternatively you can use Proxifier and set all traffic to run though your SSH tunnel or set rules to which programs you want to go through it or not.

Here is a list of free shell services.

We recommend ShellMix, they allow a lot of good software, web hosting, around 350mb of space and SSH tunneling on their Polish server. TorVPN also with their 1GB VPN trial offers and 1 month of SSH access.

We can get a free shell from ShellMix, they offer FreeBSD shells. This only takes a few minutes to do. So we can run scripts inside our new shell, use it for tunneling as a proxy we can host some files on it and also use IRC directly inside of our shell in the console with IRSSI.

Since the ShellMix shell is FreeBSD, here is a script to install IRSSI from command line and all its dependencies. You can copy and paste that into command line and then just type **irssi** to use IRSSI, then the regular IRC commands like;
- /connect irc.likeaboss.net
- /list
- /join #shell
- etc.

This is a great way to be safe using IRC while SSH tunneling, practice using this method and enjoy the feeling of being much more safe and secure.

I2P

What is I2P?

I2P is an anonymizing network, offering a simple layer that identity-sensitive applications can use to securely communicate. All data is wrapped with several layers of encryption, and the network is both distributed and dynamic, with no trusted parties. Many applications are available that interface with I2P, including mail, peer-peer, IRC chat, and others.

The I2P project was formed in 2003 to support the efforts of those trying to build a more free society by offering them an uncensorable, anonymous, and secure communication system. I2P is a development effort producing a low latency, fully distributed, autonomous, scalable, anonymous, resilient, and secure network. The goal is to operate successfully in hostile environments - even when an organization with substantial financial or political resources attacks it. All aspects of the network are open source and available without cost, as this should both assure the people using it that the software does what it claims, as well as enable others to contribute and improve upon it to defeat aggressive attempts to stifle free speech.

Anonymity is not a boolean - we are not trying to make something "perfectly anonymous", but instead are working at making attacks more and more expensive to mount. I2P is a low latency mix network, and there are limits to the anonymity offered by such a system, but the applications on top of I2P, such asSyndie, I2P mail, and I2PSnark extend it to offer both additional functionality and protection.

I2P is still a work in progress. It should not be relied upon for "guaranteed" anonymity at this time, due to the relatively small size of the network and the lack of extensive academic review. It is not immune to attacks from those with unlimited resources, and may never be, due to the inherent limitations of low-latency mix networks.

I2P works by routing traffic through other peers, as shown in the following picture. All traffic is encrypted end-to-end. For more information about how I2P works, see the Introduction. ([Read More](#))

How To Browse securely using I2P with Firefox and FoxyProxy

You can configure your browser manually to use the I2P proxy settings (**127.0.0.1:4444** by default), or if you are using FireFox, you can use an add-on by Eric Jung called FoxyProxy to configure those URLs for you.

Here's how;
1. Download and install FoxyProxy. Firefox needs to be restarted after you add this.
2. When Firefox comes back up, you'll see a new item in your status bar

Left-click the word "`FoxyProxy`" in your status bar to bring up the FoxyProxy configuration dialog, which should look something like this:

1. The important items are to make sure that your "`Host or IP Address`" does not have '`http://`' in it, and that you do not enable the "`SOCKS proxy?`" boxes. Save that configuration and exit back to your browser.
2. *Right*-click on "`FoxyProxy`
3. If you wanted to use i2p for *ALL* urls, you could select it from the `i2p Proxy -> Use proxy "i2p Proxy" for all URLs"` option, but we're not going to do that right now.
4. Choose the "`Use proxies based on their pre-defined patterns and priorities`" option at the top of this menu (the orange part in the image above).

Now when you're browsing "normally", you'll fall through to the "Default" proxy (none). When you reach an i2p UR such as sponge.i2p, it will pass into the i2p proxy we've set up. By default, I2P comes with two outproxies configured: `false.i2p` (an HTTP-only proxy) and `outproxyng.h2ik.i2p` (an HTTPS proxy routed through Tor.

Both of these outproxies are configured with connection limits. This means that only set amount of accesses are allowed per client. Once the limit is reached, the client is blocked out for a timeframe of 1min/1h/1 day. Be respectful and do not overload these services with too many requests!

TrueCrypt

Now what do we do if someone has our computer with our private data on it already?? Lets say you loose your computer or it gets into the wrong hands? What then, well this is not an issue when you encrypt your drives with true crypt.

TrueCrypt is a software system for establishing and maintaining an on-the-fly-encrypted volume (data storage device). On-the-fly encryption means that data is automatically encrypted right before it is saved and decrypted right after it is loaded, without any user intervention. No data stored on an encrypted volume can be read (decrypted) without using the correct password/keyfile(s) or correct encryption keys. Entire file system is encrypted (e.g., file names, folder names, contents of every file, free space, meta data, etc).

TrueCrypt can currently encrypt the following operating systems:
- Windows 7 (32-bit and 64-bit)
- Windows Vista
- Windows Vista x64 (64-bit) Edition
- Windows XP
- Windows XP x64 (64-bit) Edition
- Windows Server 2008 R2 (64-bit)
- Windows Server 2008
- Windows Server 2008 x64 (64-bit)
- Windows Server 2003
- Windows Server 2003 x64 (64-bit)
- Windows 2000 SP4
- Mac OS X 10.7 Lion (64-bit and 32-bit)
- Mac OS X 10.6 Snow Leopard (32-bit)
- Mac OS X 10.5 Leopard
- Mac OS X 10.4 Tiger
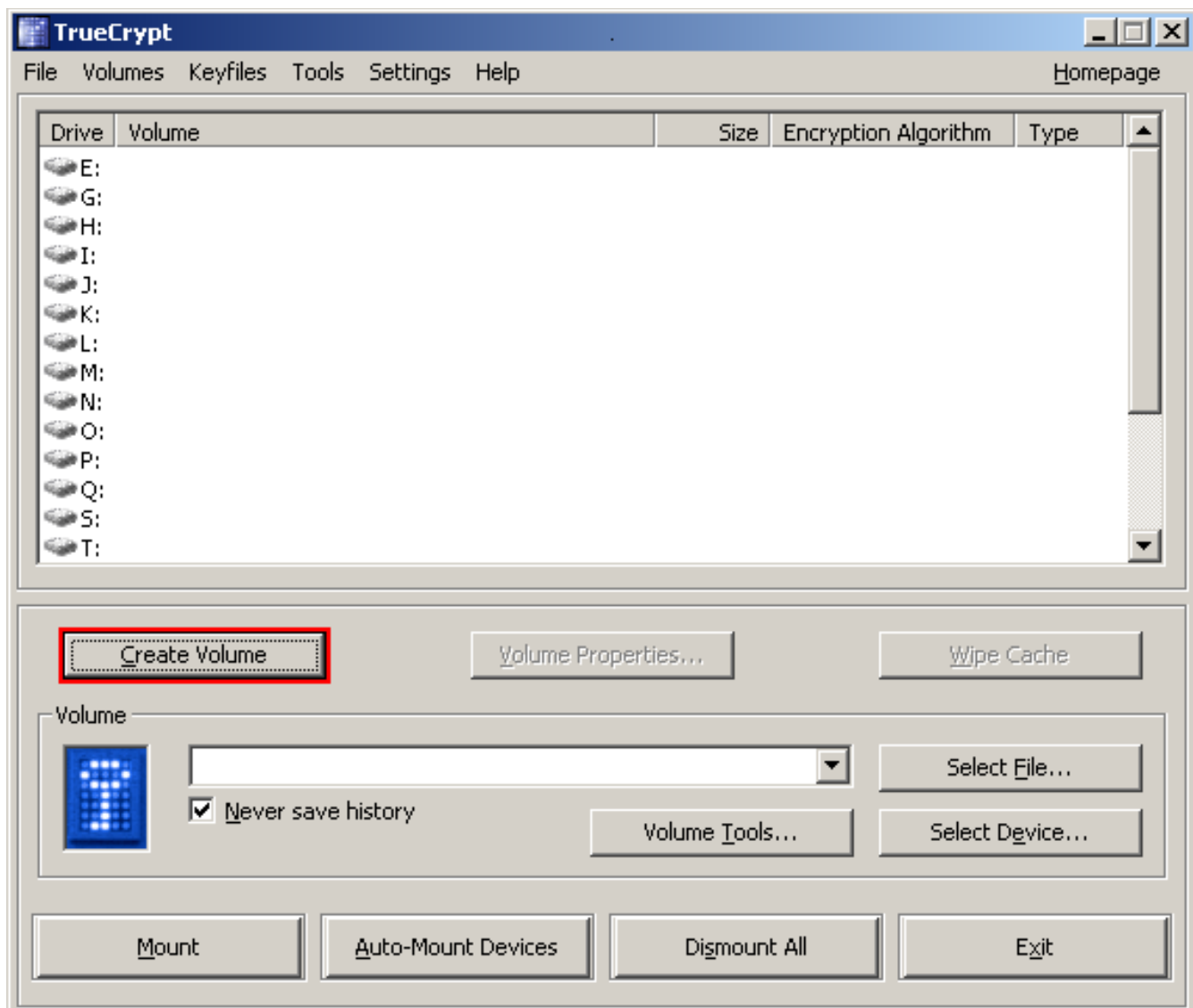- Linux (32-bit and 64-bit versions, kernel 2.6 or compatible)

Downloads (.exe and PGP signature)

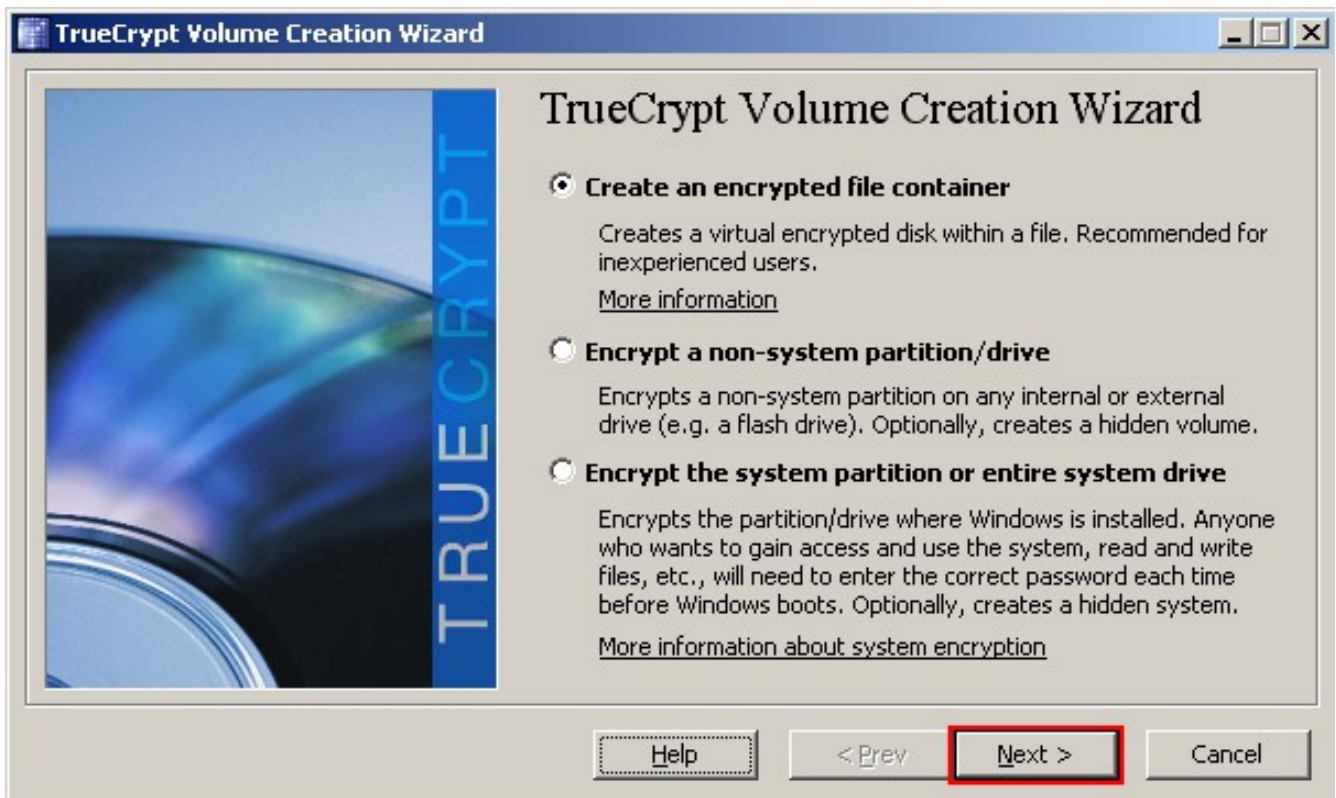**How to Create and Use a TrueCrypt Container (Tutorial)**

Step 1:
If you have not done so, download and install TrueCrypt. Then launch TrueCrypt by double-clicking the file TrueCrypt.exe or by clicking the TrueCrypt shortcut in your Windows Start menu.

Step 2:

The main TrueCrypt window should appear. Click Create Volume(marked with a red rectangle for clarity)
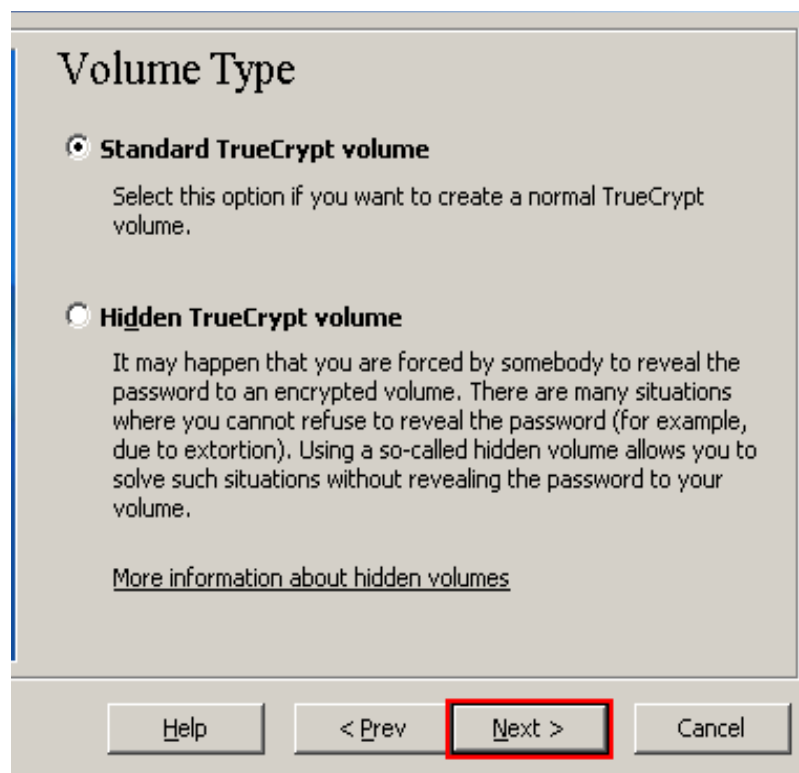
Step 3:

The TrueCrypt Volume Creation Wizard window should appear.

In this step you need to choose where you wish the TrueCrypt volume to be created. A TrueCrypt volume can reside in a file, which is also called container, in a partition or drive.

In this tutorial, we will choose the first option and create a TrueCrypt volume within a file. As the option is selected by default, you can just click **Next**

Note: In the following steps, the screenshots will show only the right-hand part of the Wizard window.
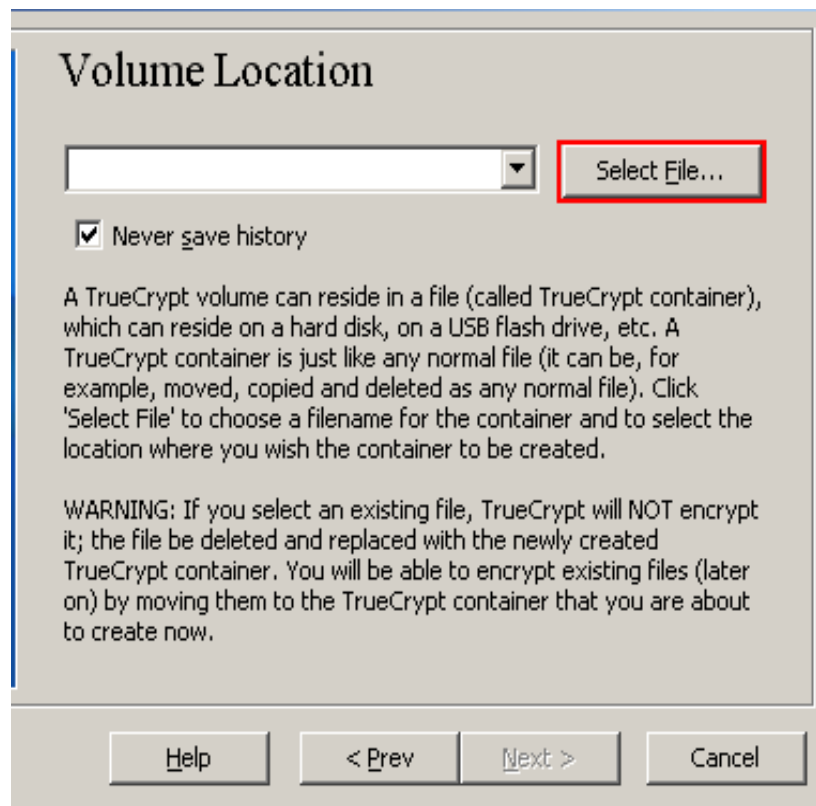
Step 4:

In this step you need to choose whether to create a standard or hidden TrueCrypt volume. In this tutorial, we will choose the former option and create a standard TrueCrypt volume.

As the option is selected by default, you can just click **Next**.

Step 5:

In this step you have to specify where you wish the TrueCrypt volume (file container) to be created. Note that a TrueCrypt container is just like any normal file. It can be, for example, moved or deleted as any normal file. It also needs a filename, which you will choose in the next step.

Click **Select File**.

The standard Windows file selector should appear (while the window of the TrueCrypt Volume Creation Wizard remains open in the background).

Step 6:
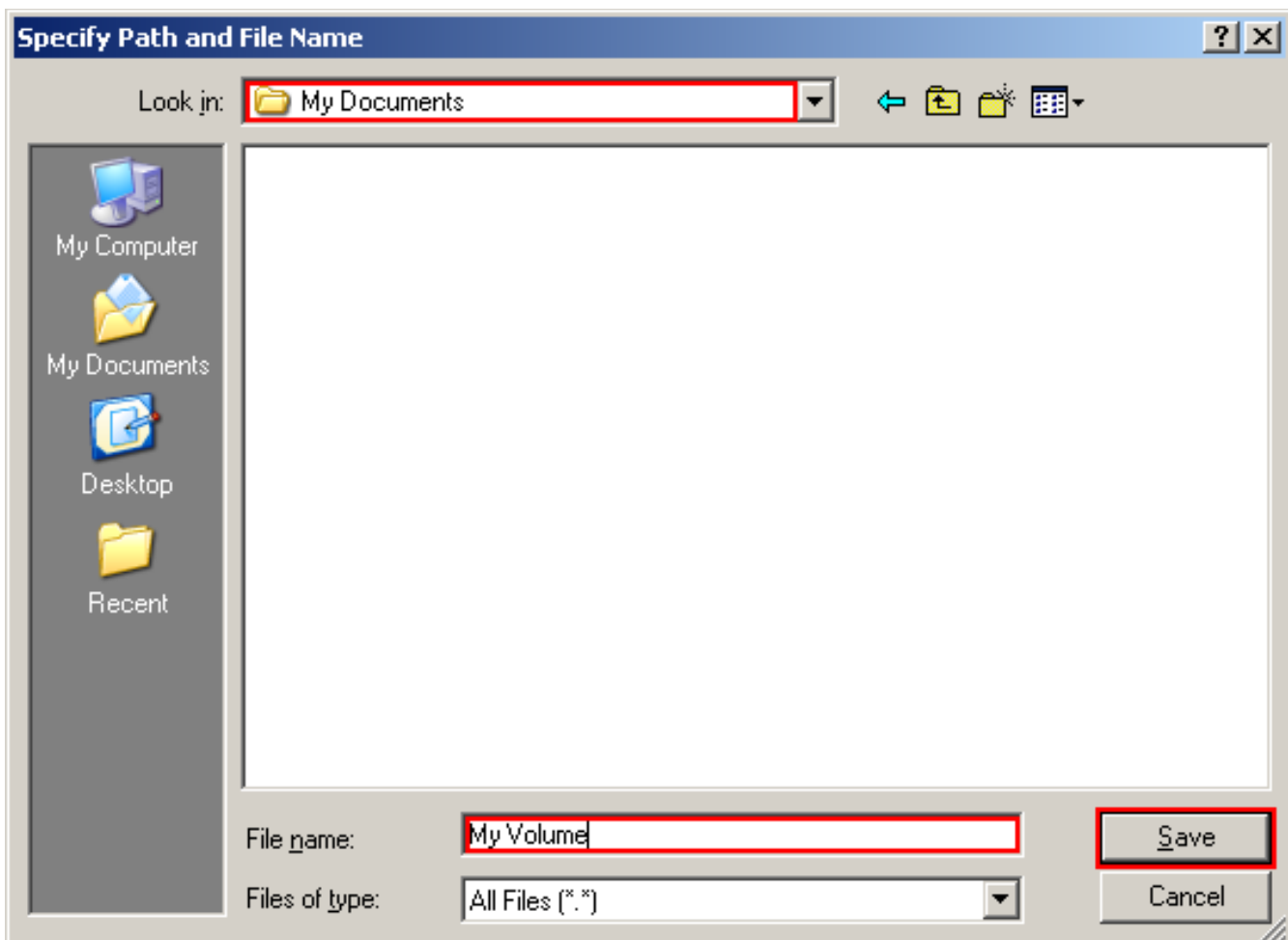
**In this tutorial, we will create our TrueCrypt volume in the folder*D:\My Documents*
and the filename of the volume (container) will be *My Volume* (as can be seen in the
screenshot above). You may, of course, choose any other filename and location you like
(for example, on a USB memory stick). Note that the file *My Volume*does not exist yet –
TrueCrypt will create it.**

IMPORTANT: Note that TrueCrypt will not encrypt any existing files (when creating a
TrueCrypt file container). If you select an existing file in this step, it will be overwritten and
replaced by the newly created volume (so the overwritten file will be lost, notencrypted).
You will be able to encrypt existing files (later on) by moving them to the TrueCrypt
volume that we are creating now.*

Select the desired path (where you wish the container to be created) in the file selector.
Type the desired container filename in the **File name** box.

Click **Save**.

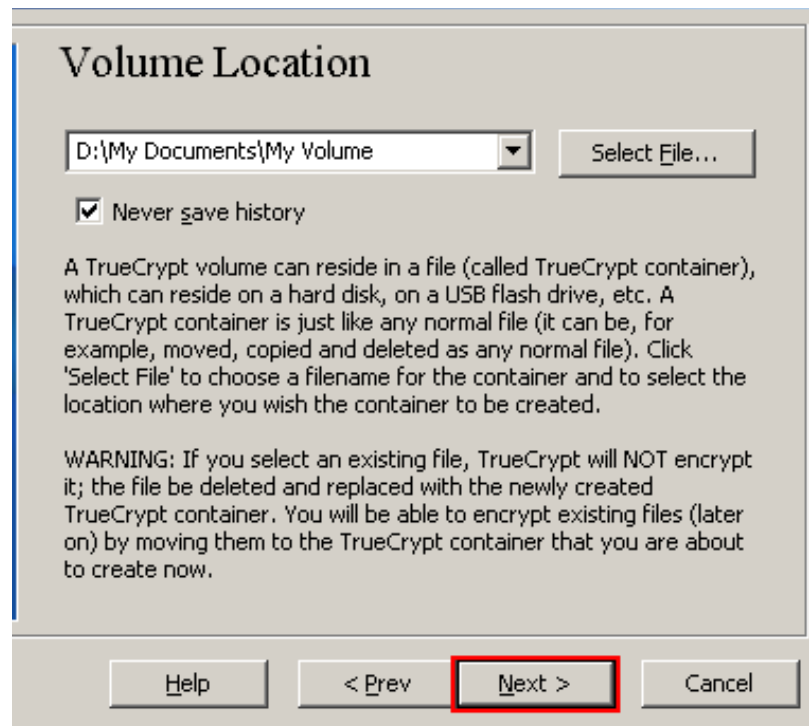The file selector window should disappear.

In the following steps, we will return to the TrueCrypt Volume Creation Wizard.

- *Note that after you copy existing unencrypted files to a TrueCrypt volume, you should securely erase (wipe) the original unencrypted files. There are software tools that can be used for the purpose of secure erasure (many of them are free).*
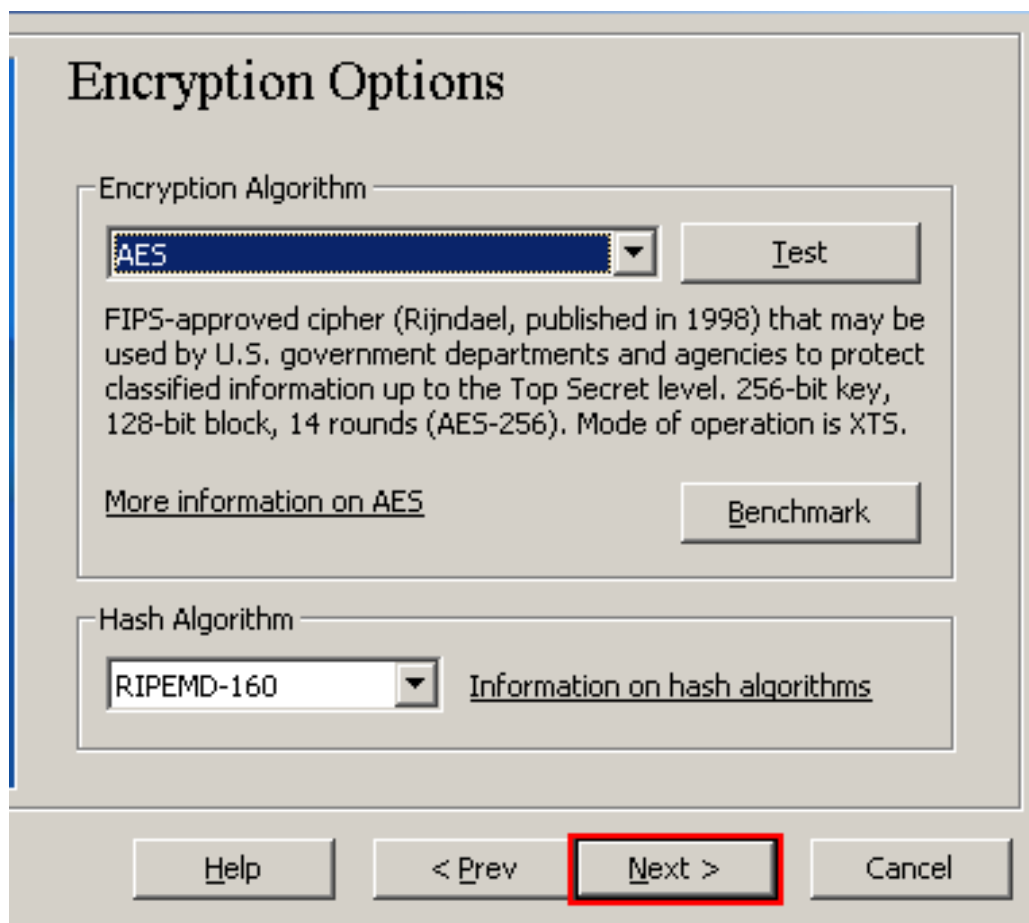-

Step 7:

In the Volume Creation Wizard window, click Next.

Step 8:

Here you can choose an encryption algorithm and a hash algorithm for the volume. If you are not sure what to select here, you can use the default settings and click Next Here is some technical details, but not part of actual installation, you may skip this and go straight to step 9.

TrueCrypt volumes can be encrypted using the following algorithms:

Algorithm -Key size (bits)-Block size (bits)
AES -256-128
Serpent -256-128
Twofish -256 -128
AES-Twofish -256;256 -128
AES-Twofish-Serpent-256;256;256 -128
Serpent-AES -256;256-128
Serpent-Twofish-AES -256;256;256-128
Twofish-Serpent -256;256 -128

Mac Address Spoofing

First off what is MAC

When you think about networking, IP addresses are probably the first things that come to mind. But there's another type of network address called a MAC address that actually forms the foundation upon which IP address communication is built, at least where local area networks are concerned.

A **MAC (Media Access Control)** address, sometimes referred to as a hardware address or physical address, is an ID code that's assigned to a network adapter or any device with built-in networking capability, such as a printer. While an IP address can potentially be assigned to any device, a MAC address is "burned into" a given device from the factory. A MAC address takes the form of six pairs of hexadecimal digits.

Given that IP addresses can't be permanently assigned to a device —after all, a particular address can belong to one computer today and another one tomorrow — MAC addresses allow communication between devices on a local network by making it possible to reliably distinguish one computer from another.

A MAC (Media Access Control) address is a number that identifies the network adaptor(s) installed on your computer. To find your MAC address on a Windows, Mac, or Linux system, use one of the following methods.

How to find the MAC address on your computer

Windows method 1:
1) **Click on the *Start* button**.
2) **Click on *Run***.
3) **Type *cmd* and press *Enter***.
4) **At the command prompt, type *ipconfig /all* and press*Enter*.** *Don't forget the space.*
5) **Look for *Physical Address*. This your MAC address. Make sure you get the physical address of the correct network adapter - usually there are several listed.**

Windows Method 2:
1) **Connect to a network**. *This method is only applicable if you are currently connected.*
2) **2) Open *Network Connections***. If you don't have a desktop icon for this, find the connection icon in the taskbar (the lower right-hand corner of the Windows toolbar) and click on it to either bring up your current connection or a list of available networks. .
3) **3) Right-click your connection and select *Status***.

4) **4) Click "Details"**. Note that, in some versions of Windows, this may be under the *Support* tab.
5) **5) Look for *Physical Address*. This your MAC address. Make sure you get the physical address of the correct network adapter - usually there are several listed.**

MAC OS X Method:
1) **Go to *System Preferences*.**
2) **Select *AirPort* or *Built-in Ethernet*, depending on how you access your network**.
• For Ethernet, click *Advanced* and navigate to the *Ethernet*tab. At the top you will see the Ethernet ID, which is your MAC address.

• For AirPort, click *Advanced* and navigate to the bottom of the page. There you will see the AirPort ID your MAC address.

Linux Method:
1) **Obtain a *command shell*.** Depending on your system, this might be called *Xterm*, *Shell*, *Terminal*, *Command Prompt*, or something similar. It can usually be found under *Applications >Accessories* (or the equivalent).
2) **Type */sbin/ipconfig* and press *Enter*.** If you are denied access, enter *su –c "/sbin/ipconfig"* and enter the root password if prompted.
3) **Look for your *HWaddr*.** This is your MAC address.

Tips:
• A MAC address is a series of 6 groups character pairs separated by dashes.
• Your MAC address can also be found with third party networking utilities, or by checking the network adapter properties under Device Manager.
• For Mac OS X, you can also try the Linux method in Terminal.app. This will work on because MacOS X uses the Darwin kernel (based upon BSD).

Reasons for why you may want to spoof your MAC address:
1. To get past MAC address filtering on a router. Valid MAC addresses can be found by sniffing them and then the deviant user could assume the MAC of a valid host. Having two hosts on the same network can cause some network stability problems, but much of the time it's workable. This is one of the reasons why MIC Address filtering on a wireless router is pointless. An attacker can just sniff the MAC address out of the air while in monitor mode and set his WiFi NIC to use it. Interestingly, a lot of hotels use MAC filtering in their "pay to surf" schemes, so this method can be an instant in for cheap skate road warriors.
2. Sniffing other connections on the network. By assuming another host's MAC as their own they may receive packets not meant for them. However, ARP poisoning is generally a better method than MAC spoofing to accomplish this task.
3. So as to keep their burned in MAC address out of IDS and security logs, thus

keeping deviant behavior from being connected to their hardware. For example, two of the main things a DHCP server logs when it leases an IP to a client is the MAC address and host name. If you have a wireless router look around on it's web interface for where it logs this info. Luckily there are tools to randomize this information **(MadMACs) ([Download here](#))**

EXIF Stripping

EXIF (Exchangeable Image File) Data is something not a lot of people know about but should. This form of data is embedded in pictures and in some cases other files. This has in previous cases have revealed identities of people who did not want their identities revealed. If you are taking pictures with your mobile phones and uploading them to social sites, then there is a chance you are releasing your location and computer information along with that particular picture.

Here are some links and Apps that can help you combat this;

- [Online EXIF Data Strip](#) - Upload an image file and the sites strips the data for you.
- [Geosetter](#) - a freeware tool for Windows (XP or higher) for showing and changing geo data and other metadata (IPTC/XMP/Exif) of image files (e.g. images taken by digital cameras).

Always be safe and check the images you plan on putting online before actually putting them up. Simple mistakes like this can be very damaging to your Anonymity.

How to be a Mobile Ninja! (Cellular Security)

With the current rise in people purchasing Smart phones and relying on that alone, the issue of how to remain safe and anonymous comes to mind. We have written this post for those who rely on phones greatly and hope to help a couple of people with little to no knowledge of phones.

Believe it or not, Smart Phones are NOT the safest tool that one can have, with multiple ways these devices can send out data and information on you, this can be troublesome to those wanting to remain anonymous and untraceable. Fortunately there are many ways you CAN remain anonymous and untraceable. Here are some tips for those Mobile-Geeks;

With Smart Phones there are many features which can be altered with a tap of the screen, we prefer Android devices since they are not only safer and more flexible BUT they are also a lot cooler. When purchasing your new smart phone or looking to alter your current one, one mistake people often make is they never turn off their "Location Services", this is key to not being easily tracked by certain apps or mistakenly tweeting out your location. Turn is off!!!

How you ask? The majority of Droids are similar in settings, so we will give the most basic steps to shut this feature off;

- Go to Settings
- Click on the "Location" sub category
- You should see three options, "Use Wireless Networks", "Use GPS satellites" and "Phone Finder", now of course you want to shut off TWO of these, Phone Finder and Use GPS Satellites. (Phone Finder is needed? NO, just do not lose your phone or you are pretty much at a loss)

That simple, you now have disabled Location services. GPS is something you should avoid at all cost, since obviously you can be tracked that way.

Another thing you might want to avoid at ALL cost is taking photos with your phone and posting them online without take precautions, for this you might want to NEVER do that, simply take photos, wait until you get home, upload them to your computer and clean them out with an EXIF data remover/injector. This will ensure maximum anonymity as your location, date and time the photo was taken and User agent data is stored on that picture alone. There are EXIF data removers for mobile devices but most people do not know or understand how to properly use them, so we recommend using a desktop one and taking that extra step, remember maintaining anonymity and security may be tedious BUT rewarding.

Another tip would be to NEVER make phone calls from your smart phone or primary phone, for the obvious. Contract cell phone plans or Phones with your information attached to them can very easily be lead right back to you. For this we highly recommend acquiring what we like to call a "Burn Phone". A "Burn Phone" is a phone you pay little to no money for, has a pre-paid cellular plan and is activated with no real information of yours. This can ensure safety when calling friends, family and or colleagues.

For this to be fully effective you have to make sure when purchasing and or activating this phone you DO NOT give any of your real information, to make this simpler purchase a pre-paid cell phone from a big chain pharmacy or department store, they may not be attractive at all BUT it will be one step to keeping you more secure. After purchasing a pre-paid cell phone, head over to Google and create a brand new Google account with information that does NOT tie to you in any way. After creating an account with Google, sign up for a [Google Voice](#) account and connect it to your number on the Burn Phone you just purchased. Voila, from now on you will dial in your Google voice number to make phone calls from your "Burn Phone".

To do this;

- On your "Burn Phone" dial *67
- Call your Google Voice number
- Press number 2
- Dial the number you wish to call
- Press the # key

Doing this will help fail your ANI (Automatic Number Identifier) and this would make your call a bit harder to trace. It is recommended you use your burn phone for at LEAST 3 months, then destroying that phone, purchasing a new one and completing all of these steps again. As we said, being secure and anonymous was never said to be quick and easy, it may be tedious BUT it is rewarding.

**Note: Remember to pick a number when signing up for Google Voice that has a location completely opposite of where you currently are, to fully throw people off.

If you prefer to use an Android or an iPhone as a burner phone, you can download an

app call Burner. Burner is an app for Android and iOS that can route all of your phone traffic through their "burner" numbers. Once you install their app you get one free number BUT if you wish to burn it and get another number you will then have to spend some cash. Here is how their pricing works;

Burner options:

- SAMPLE BURNER (Available once) - 1 day or 5 voice or 15 text (FREE)
- Mini Burner - 7 days or 20 voice or 60 texts (3 credits)
- Standard Burner - 30 days or 50 voice or 150 texts (5 credits)
- Large Burner - 30 days or 90 voice or 270 texts (8 credits)
- Long Burner - 60 days or 75 voice or 225 texts (8 credits)

Burner extension optons:

- Add 30 days or 50 voice or 150 texts (5 credits)
- Add 90 days or 90 minutes or 270 texts (10 credits)
- Add 60 voice or 180 texts (5 credits)

Cost of credits:

- 3 Credits = $1.99
- 8 Credits = $4.99
- 15 Credits = $7.99
- 25 Credits = $11.99

Now I know what you are saying, "I don't want to pay for anything…", BUT rest assure that great privacy comes with a price, and free services are almost always unsafe. Think of it as investing in your safety and privacy, plus you can earn free credits by inviting your friends with a referral code, anyhow, this service is great and we have been waiting for something like this to come along, not to mention it is available on iOS and Android, both widely used devices.

Here are some of their features;

TEMPORARY PHONE NUMBERS

- Find a number in any area code
- Create multiple phone numbers
- Easily name each one so you can keep track of its purpose (e.g. "Craigslist")
- Quickly share your number via social networks or email

STAY IN TOUCH

- Access your address book from Burner
- Manage SMS and ringer notifications for each burner
- View and manage history for all your burners

STAY PRIVATE

- Callers will only ever see your disposable phone number
- "Burn" your disposable phone number at the click of a button
- Burned numbers instantly go out of service and are deleted from your phone
- Reverse lookups on your disposable phone numbers will not lead back to your info

EARN FREE CREDITS AND BURNERS

- Share your referral code with your friends
- For every friend that signs up using your code, you'll earn credits and they will too!

Now that you have mastered the Ninja Art of Shadow Calling, you have to still secure that Smart Phone, here are some quick tips for that;

It is recommended that you Root your droid before using mobile Tor but it can still work without that step. So head over to Google Play and download Orbot: Tor on Android, this is basically Tor just for Android devices. For instant messaging, download Gibberbot, the multi-chat client for Android devices supported by Tor. Also, TextSecure is a great android app for encrypting outgoing text messages to the other party that are sent through this application (this is meant as a replacement for the typical text messaging software).

Another great way to secure your web traffic and hide your IP is by using an Android VPN, you can find some on our VPN section. AVOID services such as Foursquare, and location posting services that Facebook and Twitter currently have at all costs, those type of services can jeopardize your location and one less person knowing where you are located the better.

Another great tip is to USE Pattern Locks for your device, this can place one more obstacle in the way if your phone is taken by a thief or someone looking for some evidence. Use this tool to come up with a pretty extensive Pattern Password for your device. Always remember to LEAVE NO fingerprints, believe it or not, this can sometimes lead to cracked passwords.

Being secure and safe is a tedious job BUT highly rewarding.

Conclusion

Now we have covered everything you need in order to maintain your anonymity, keep your freedom and be secure online while these good for nothing governments do their best to infringe on our civil liberties. There is nothing wrong with fighting to keep what you do in the privacy of your own home and on the privacy of your own computer private. We can not allow these governments to continue spying on us, make sure you sign petitions and get the word out that we will not stand to have our rights taken away, united we can defeat bills like CISPA.

Spread this book around to all of those you know, and make sure they understand how important our privacy is and show them the way to remain faceless, every person who can help another person is another person saved. Check out our website as we are constantly doing our best to bring you the best tools, tutorials and services the internet has to offer in security and anonymity, and if you have any questions do not hesitate to ask us.

This will be an ever updating book, we hope most of you find this useful, and as always, we love you all...

--Team WeAreHidden | School Of Privacy