

- 1. What is a Portable Application**
- 2. How to setup encryption and password protect your USB Key, run apps and save documents to it**
- 3. Run and tweak TorPark (Firefox + Tor routing app)**
- 4. Run and tweak a portable Firefox**
- 5. The best extensions for Firefox and Torpark that ensure anonymization and security**
- 6. Howto get and use Portable Thunderbird with GPG Encryption**
- 7. Howto get and use Portable GAIM**
- 8. How to setup encryption through GAIM**
- 9. How to use GAIM through Tor**
- 10. How to run uTorrent from the USB key**
- 11. How to run OpenOffice from your USB key and tweak it for speed**
- 12. How to use RealVNC to connect to your home computer**
- 13. Use PStart as a launcher for your USB programs**
- 14. Other USB applications you might find useful**
- 15. Run Skype from your USB key**
- 16. Automate the deletion of registry keys for all of these applications**
- 17. Nonportable Apps to help clear your tracks**
- 18. Installing Tor Onion Routing to a Hard-drive**
- 19. Generic proxy sites**
- 20. AnonymOS**
- 21. Test your privacy and anonymity**

What is a Portable Application?

First off, what is a portable application? They are software programs that are not required to be "installed" onto a computer's permanent storage device to be executed, and can be stored on a removable storage such as a [1GB USB Key](#) and used on multiple computers. Ideally it can be configured to read its configuration from the same location as the software. Portable applications come in a zip file. Contained in the zip file is their folder. There is NO installation process. The program runs from the folder itself without requirements of a Windows registry, without the requirements of putting DLL files in C:/Windows/Sytem32, without the need to create folders in your hidden folder C:/Documents and Settings/Username/Application Data (among other areas) MOST of the time. Occassionally some programs will leave a small footprint on a hard-drive, but we'll address that. Portable Apps simply run from the files on the USB key and it knows the location of supporting files that Windows already has (such as codecs, fonts, and such).

Encryption

First thing's first. What good is it to have your data stored, or portable applications running from, a removable disc if someone who connects remotely can access that disc? What if you lose that disc? Everything must be encrypted.

First you want to make sure that at minimum you have at least a 512MB USB Drive (aka thumb drive, jump drive, etc). You'll need at least 1 GB USB drive if you wish to do every single thing listed here.

We're going to be using TrueCrypt to do this. Which you can download here:
<http://www.truecrypt.org/downloads.php>

What we're about to do is create a file, and create a hidden "volume" (it'll show up as another drive) in that file and we're going to password protect it. Encryption is automatic, real-time (on-the-fly) and transparent. It provides two levels of plausible deniability, in case an adversary forces you to reveal the password. The first is b/c it's a hidden volume(steganography), the 2nd is that no TrueCrypt volume can be identified (volumes cannot be distinguished from random data). The encryption algorithms it uses are as follows: AES-256, Blowfish (448-bit key), CAST5, Serpent, Triple DES, and Twofish.

You want to download this application and run the installer. Do not install it to it's default location.

Install it to your USB drive. The program will run on every computer from the USB drive.

Once installed click the "Create Volume" button. This will guide you through the creation of two

volumes, one viewable and one hidden. The hidden one is impossible to prove existing, and thus, the software you will install next won't exist to someone who steals your key. During creation of the viewable volume, you want to make sure that you have a little breathing room so the drive can still be used without TrueCrypt..and enough so that TrueCrypt can still exist on the disc outside of the hidden volume. When you go to create the hidden volume the data path needs to be to your USB drive of course. 5-10 MB

free will be enough. So if you're running a 512MB USB stick, make you're viewable volume 500MB (the hidden volume will the the same size). Make sure the passwords you create for the viewable and hidden volumes are different. The hidden volume password should be alpha-numeric, not contain any common words or names, and at minimum 12 character long. (Also make sure you remember them b/c if you forget them you're screwed).

Back at the Truecrypt main menu. We are going to need to mount the hidden volume. So what you do is press the Select File Button, and select the file you used to create the volume. Click mount volume, put in your password for the hidden volume and be sure to check the protect hidden volume option if you plan on writing to the volume everyone can see. This prevents us from accidentally corrupting our hidden programs or files. TrueCrypt will mount your hidden volume as a drive letter.

Starting with Portable Applications

And here's where the fun begins.

Torpark

Torpark is Firefox and the Tor Onion Routing Software Combined. To explain Onion routing, Tor helps to reduce the risks of both simple and sophisticated traffic analysis by distributing your transactions over several places on the Internet, so no single point can link you to your destination. The idea is similar to using a twisty, hard-to-follow route in order to throw off somebody who is tailing you”and then periodically erasing your footprints. Instead of taking a direct route from source to destination, data packets on the Tor network take a random pathway through several servers that cover your tracks so no observer at any single point can tell where the data came from or where it's going.

Tor in itself requires a computer install, but not with Torpark. Note: the tor aspects of Torpark only work for this browser. For more info on how Tor works see:

<http://tor.eff.org/overview.html.en>

Download TorPark here:

<http://torpark.nfshost.com/>

Extract the zip file to your newly created Hidden Volume. The hidden volume will show up as a 2nd local disc on your My Computer. Chances are the drive letter is Z: (but not always by anymeans). And that's it. It's installed.

Browsing through TorPark is significantly slower than a regular connection. Here you will have to decide what's more important, speed, or staying anonymous. Unless you build and host a Tor server yourself, you can't complain.

Tweak TorPark

But alas there are hacks/tweaks to make TorPark run faster. (This can also be used on Portable Firefox as well).

First we'll Kill the amount of RAM Firefox uses for it's cache feature

Here's how to fix it:

1. type "about:config" (no quotes) in the browser address bar
2. Find browser.sessionhistory.max_total_viewer
2. set it's value to "0"

Increase the Speed in Which Firefox loads pages

1. stay in about:config
2. Alter the entries as follows:
Set "network.http.pipelining" to "true"
Set "network.http.proxy.pipelining" to "true"
Set "network.http.pipelining.maxrequests" to some number like 30 (this might piss off some website owners as it will request the page 30 times)
3. Lastly right-click anywhere and select New-> Integer. Name it "nglayout.initialpaint.delay" and set its value to "0".

This value is the amount of time the browser waits before it acts on information it receives.

Kill RAM usage to 10mb when FF is minimized

This little about:config hack will drop Firefox's/Torpark's RAM usage down to 10 Mb when minimized

1. Open Firefox and go to the Address Bar. Type in about:config and then press Enter.
2. Right Click in the page and select New -> Boolean.
3. In the box that pops up enter config.trim_on_minimize. Press Enter.
4. Now select True and then press Enter.
5. Restart Firefox or Torpark.

Torpark Switch Proxy Extension

You may decide you don't want 2 browsers on your USB key, but you don't always want to use the Tor network to do your browsing due to speed. If this is the case install the [Switch Proxy Extension](#) and configure it.

(Note, this will undue Torpark's default settings)

1. To Configure, install the extension, then restart TorPark.
2. A new toolbar has appeared.
3. Torpark already has a proxy configured.
4. Make sure the selected proxy says "None" and Hit Apply Now Torpark is no longer using Tor.

To set the option to turn Tor on:

1. So we'll press Add
- 2.. Select "Standard" and "Next"
- 3.. Name it Tor and select "Manual Proxy Configuration"
4. Add the values [127.0.0.1](#) to the SOCKS Host and Port 81 (note, port 81 is just for Torpark. With a hard-drive install of Tor Firefox and Thunderbird will run through 8118.)
5. Socksv5 should be Selected
6. Hit Apply. Now Torpark is using Tor and you have the ability to switch back and forth.

(If you use Tor off the hard-drive and not just TorPark, the Switch Proxy extension can be used in Thunderbird to send e-mail as well. To download, you right click the install file and "Save As", then in Thunderbird go to File --> Open. You'd configure it the same as the above.)

Portable Firefox

There's a multitude of reasons you may not wish to use TorPark. And below is some reasons why:

- 1) Too slow and you value speed more than anonymous traffic
- 2) If you're running applications through a hard-disk installed version of Tor (which you might decide to do with GAIM) you cannot run 2 Tor circuits simultaneously. You'd either have to run TorPark, or GAIM through Tor, but not both at the same time.

Download from here:

[Portable Firefox](#)

and do the same thing we did with TorPark. Unzip it to your hidden volume.

Firefox and TorPark Extensions

There's a ton of extensions for usability and other issues that i love and use, but i'm not going to cover these. I'm only going to cover issues of a security nature.

All firefox plugins work with both TorPark and Portable Firefox. You will have to install an instance of each, to use them on both. Or just install them on the browser you chose to use most often. I do recommend these extensions for ALL versions of Firefox (portable, tor, or not).

[NoScript](#) - (already included in TorPark) Disables all website Java script by default and allows you to whitelist the sites you chose.

[Customize Google](#)- This will allow you to block Google ads, anonymize your Google cookie ID, and it'll stop you from sending traffic to google analytics.

[AdBlock](#)-(already included in TorPark) Websites call ads that are actually just hot link scripts, flash files, images from other sites. These have the potential to install spyware. Best to block them. Ad block allows you to right click and ad and get rid of it for good.

[Adblock Filterset G.Update](#)- This loads a filterlist of most internet ad sites out there. This saves alot of time compared to manually blocking ads. It also updates itself automatically.

[CookieSafe](#)- This extension will allow you to easily control cookie permissions. It will appear on your statusbar. Just click on the icon to allow, block, or temporarily allow the site to set cookies.

[SafeHistory](#)- Restricts the marking of visited links on the basis of the originating document, defending against web privacy attacks that remote sites can use to determine your browser history at other sites. A link on [a.com](#) pointing at [b.com](#) will only be marked visited if you previously visited the [b.com](#) page with a referrer in the domain of [a.com](#). On-site links work normally. Checks cookie settings (allow, originating site only, deny) to determine your desired privacy level (segmented by origin, don't mark links visited in offsite frames, or never mark links visited).

[SafeCache](#)- Segments the cache on the basis of the originating document, defending against web privacy attacks that remote sites can use to determine your browser history at other sites. For example, a [b.com](#) image appearing on an [a.com](#) page would have a separate cache entry from the same image appearing on a [b.com](#) page, so [a.com](#) cannot use timing techniques to determine if you have visited [b.com](#) before. Checks cookie settings (allow, originating site only, deny) to determine your desired privacy level (segmented cache, cache originating site only, or never cache).

[ClamGlue](#) (will only work if WinClam is installed on the hard-drive.) This plugin uses WinClam anti-virus to scan every file Firefox downloads for viruses.

Portable Thunderbird with GPG Encryption

[Download it here](#)

Same process. Download, unzip, setup to connect to your mail server. When you want to send an email, use Portable Thunderbird w/ Enigmail & GPG. Secure and anonymous e-mail has been addressed much earlier than secure and anonymous web browsing. This means the technology for e-mail is more mature, and has been tested a whole lot longer. We know GPG encryption can be relied upon to make sure all of our email transmissions are at least as secure as sealed mail. It works by creating a public key and a private key. You give your public key to anyone you want to write to. They give you their public key, and you encrypt your email with the public key of the person you're talking to. Your email is then only readable by the person you send it to. With plenty of anonymous emailers around to send our email through, we can also be reassured our communication is anonymous. In other words, we can say it's technically impossible to prove an email was sent by us. This is a good thing.

Portable Gaim, Encryption and Tor

We have 2 routes we can go here. The portable way, or the non-portable.

First, place the PortableGaim directory on your hidden share. We must also install GAIM on the hard-drive first (the full version) in order to install GAIM encryption. Currently the GAIM encryption will not let you change the install location so we'll have to move the plugin manually. (FYI: Gaim-Encryption uses NSS to provide transparent RSA encryption as a Gaim plugin.)

[Download PortableGAIM here](#)

Lets get Encryption Working on Portable Gaim

1. Uncompress Portable Gaim into your hidden volume.(you may have already)
2. Download [GAIM \(the full version for Windows\)](#) and install it.
3. Download [GAIM Encryption](#)
4. Install Gaim Encryption on your hard-drive
5. Now it gets complex. We need to copy a series of files (about 20) from one location to another. Below is a list of the files that need to be copied from the install folder on your hard-drive, to the corresponding folder on your hidden volume. (If the folder isn't there on the hidden volume, it needs to be created)

What a pain in the ass you say!?! Well i wrote a batch file to automate this. You're welcome.

You MUST have your hidden volume mounted at Z:\ for this to work and your Gaimportable directory needs to be directly in that volume. So.. Z:\Gaimportable should exist. Then right click and save this zip file, then extract it and run it.

[gaimencryptportable.txt](#)

If that file doesn't work..[Download it here, Right Click and Save As](#) Once downloaded, right click and change the name. Change the extension from txt to bat. Double click to run it. and voila.

It copies these files and directories:

```
C:\Program Files\Gaim\plugins\encrypt.dll
C:\Program Files\Gaim\locale\cs\LC_MESSAGES\gaim-encryption.mo
C:\Program Files\Gaim\locale\da\LC_MESSAGES\gaim-encryption.mo
C:\Program Files\Gaim\locale\de\LC_MESSAGES\gaim-encryption.mo
C:\Program Files\Gaim\locale\es\LC_MESSAGES\gaim-encryption.mo
C:\Program Files\Gaim\locale\fr\LC_MESSAGES\gaim-encryption.mo
C:\Program Files\Gaim\locale\hu\LC_MESSAGES\gaim-encryption.mo
C:\Program Files\Gaim\locale\it\LC_MESSAGES\gaim-encryption.mo
C:\Program Files\Gaim\locale\ja\LC_MESSAGES\gaim-encryption.mo
C:\Program Files\Gaim\locale\nl\LC_MESSAGES\gaim-encryption.mo
C:\Program Files\Gaim\locale\pl\LC_MESSAGES\gaim-encryption.mo
C:\Program Files\Gaim\locale\pt_BR\LC_MESSAGES\gaim-encryption.mo
C:\Program Files\Gaim\locale\ru\LC_MESSAGES\gaim-encryption.mo
C:\Program Files\Gaim\locale\s\LC_MESSAGES\gaim-encryption.mo
C:\Program Files\Gaim\locale\uk\LC_MESSAGES\gaim-encryption.mo
C:\Program Files\Gaim\locale\zh_TW\LC_MESSAGES\gaim-encryption.mo
```

6. Load Gaim and go to Tools --> Plugins and you should have the option to set encryption (Don't click it yet)

7. Uninstall Gaim and Gaim Encryption from your computer in Add/Remove programs. Delete any residual folders in Program Files. and now test to see if the encryption plugin loads and creates a key.

This ONLY works if you're chatting with someone else using encryption. Good to note, that most simple packet sniffers that capture and translate AIM/Yahoo/MSN/Jabber traffic tend to read person to person conversations, not chat rooms. More sophisticated ones read both without a hitch. Encryption is meaningless in chatroom for AIM, MSN, and Yahoo. It simply does nothing.

If you want to have a secure connection that's encrypted for a chat room, (this is great of business conferences across the web), GAIM can connect you to another client. SILC. It will automatically assign you a name and password and prompt you to accept or deny encryption keys. Of course the people you chat with, will to use SILC as well.

Route GAIM through Tor

You can still chose to just use the above setup if you wish.. or you can use GAIM + encryption plugin loaded onto your hard drive and route it through Tor.

You'll need to install Tor Bundle for Windows (on the hard-drive.. it's not a portable application) and change the proxy for each account you're chatting on to a SOCKS5 proxy.

1. Go to Create a new or Modify an existing account.
2. Select "Show More Options". Here you can input proxy data.
3. Select Socksv4. You'll want to use the term "localhost" (no quotes) as the proxy (this will access the tor circuit). The port you'd chat on would be 9050.

uTorrent

Download the standalone application [here](#)

uTorrent is the most lightweight bit torrent application i can find. Weighing in at 154kb (smaller than this tutorial). Beware though, you can route this through Tor if you have a hard-drive install, but otherwise it's unencrypted. I also don't recommend doing bit torrent through the Tor network. Tor's network is slow enough as it is without people hogging it with bit torrent traffic. There's also no SafePeer-like plugin like there is for Azureus. I'm currently working to find an alternative that will allow you to load blocklists of IP addresses to ensure the RIAA or MPAA isn't tracking what files you're leeching/seeding. (among other issues). So use at your own risk. You know, if you're using it for illegal purposes. But you know, none of us would *dare* do that, would we?

If you could care less about if it's a portable app, i'd say go with Azureus and get the Safepeer plugin.

Portable Open Office and Abi Word

People tend to define their office software by the quality of the word processor more than anything. OpenOffice's Writer just doesn't add up, but the rest of the suite is more than suitable IMO. You can choose to go with or without Abi Word as Open Office does come with Writer, their word processor. I just prefer Abi Word over Writer myself.

I pick these apps, not only because they're portable, but unlike MS Office (which isn't portable) they don't leave behind data showing who made the file, edits and changes that were done to the file over time, etc. MS Office has the ability to turn those features off, but it's a pain in the ass.

Download and unzip just like all the rest.

[Here for Open Office](#) [Here for Abi Word](#)

OpenOffice tends to open up a bit slow. Once extracted to the hidden volume you can improve this by doing the following. Open any of OpenOffice's apps (Writer, Calc, Impress, Draw, Base, Math) and do the following:

1. Go to Tools
2. Go to Options
3. Go to Memory
4. Change number of steps to 10.
5. Change "Use for Open Office" to 30.
6. Change "Memory per Object" to 7.
7. Change "Remove After Memory" to 0:00:05
8. Change Number of Objects to 10
9. Close the app.

RealVNC

VNC can allow us to do some nifty tricks as well, or you may just need it to aid in technical problems of another, but we'll focus on hiding our network activity here.

1. Download it here <http://www.realvnc.com>
2. Install it (make sure you only install the viewer, unless you need people to connect to you..which i

wouldn't advise with you hidden drive mounted) to your hidden volume.

3. Unmount the volume
4. Go to Add/Remove Programs and uninstall RealVNC.
5. Delete residual files out of Program Files
6. Re-mount your hidden volume. And run vncviewer.exe

Now how to browse the web, chat, and e-mail from anywhere on your home computer:

1. You can install this on your home computer (this time install both the server and the viewer).
2. Password protect the server.
3. Make sure port 5900 is open on your firewall.
4. If you have a router, make sure your router forwards port 5900 to the private IP address of the machine you installed the VNC server on. (More than likely 192.168.x.x or 10.0.x.x)
5. Now mount your hidden volume on a computer at your place of business, education, a library, or a friend/family's house. Open VNCViewer, type the IP address and password to your home computer. Now you should be able to view the desktop of your home machine.. and use that to browse, chat, send e-mail. All traffic analyzing would see is that you're passing ARP packets and bmp files on port 5900. You're web activity on your home computer is untracable to the LAN you're connected to.

Pstart

Creates a tray icon that allows you to link in your portable applications. It simplifies access to the programs, rather than continually having to dig through folders to get the executable.

Other Portable Applications

These Portable Apps you may or may not need.

[ClamWin Anti-Virus](#)

[VLC Media Player](#)

[Scribus](#)

[GIMP Image Editor](#)

[NVU HTML Editor](#)

[Notepad2 \(open source Notepad with more functionality than MS's notepad](#)

[FoxitPDF Reader](#)

[Cyber Shredder \(has NSA 7 Pass deletion method\)](#)

[CurrPorts](#)

[Angry IP Scanner](#)

[Rootkit Revealer](#)

[Regmon](#)

[Filemon](#)

[Diskmon](#)

Skype

The encryption behind Skype's VoIP is amazing. So it's rather great the folks over at U3P to make a portable version of the software. You can obtain the U3P file [here](#)

Download it, use a program like 7-Zip to extract it your to hidden volume and in the Skype/host directory is the Skype.exe.

Autmoated Cleaning of Registry Keys

Ok, if so far you've installed "ALL" of the above applications, the following apps do leave behind registry keys showing these apps have been run on the machine.

1. Abiword
2. FoxitPDF Reader
3. Skype
4. RealVNC
5. Mozilla Thunderbird
6. gaim
7. 7-Zip

8. Notepad2
9. AngryIP
10. All of the Sysinternals programs (Regmon, Filemon, Diskmon, etc)
11. Scribus

This may not be a big deal to most. None of the registry info gives off anything identifiable but it does show that these applications have been used on the machine. If you're super paranoid, you'll want to get rid of these entries. They reside in HKEY_CLASSES_ROOT, HKEY_LOCAL_MACHINE, and HKEY_CURRENT_USERS.

Like with the batch file with GAIM, i have made an INF file that will automate the deletion of these registry keys.

WARNING: Deleting these keys has not been tested on a computer that has any of these applications natively installed on the hard-drive. If any of these applications are installed on the hard-drive, i'd suggest A) Do not use this INF, or B) edit this INF in Notepad to fit your settings.

Right click and save as this file: [stayhidden.zip](#)

1. Extract the INF file.
2. Right Click the extracted INF file, Install

When it runs it will delete the following registry entries.

```
HKCR,\"AbiSuite.AbiWord\"
HKCR,\"FoxitReader.Document\"
HKCR,\"skype\"
HKCR,\"Skype.Content\"
HKCR,\"Skype.Detection\"
HKLM,SOFTWARE\"RealVNC\"
HKLM,SOFTWARE\"Mozilla Thunderbird\"
HKLM,SOFTWARE\"gaim\"
HKLM,SOFTWARE\"7-Zip\"
HKLM,SOFTWARE\"Trolltech\"
HKCU,SOFTWARE\"7-Zip\"
HKCU,SOFTWARE\"Angryziber\"
HKCU,SOFTWARE\"Foxit Software\"
HKCU,SOFTWARE\"Notepad2\"
HKCU,SOFTWARE\"RealVNC\"
HKCU,SOFTWARE\"Skype\"
HKCU,SOFTWARE\"Sysinternals\"
HKCU,SOFTWARE\"gaim\"
```

and... we're done for the Portable stuff. Now you have a USB key you can take around with you and open your TrueCrypt volumes anywhere and run this software anywhere with a heightened sense of security. Whether at school, a library, work, a family's house.. your private business, stays private. Just don't be cocky. There's no such thing as being 100% secure, and 100% anonymous.

Common Sense Tips

1. Make sure you're firewall is on, and make sure it's configured well. Allowing through only the programs you need to allow through.
2. Get a registry or spyware monitor. Regmon is a good registry monitor. Winpooch is an excellent Registry and system file monitor and can prevent system changes (it can also hook WinClam anti-virus, and gives it real time active scanning ability.. which it doesn't have).
3. If it's a computer you use often, get some anti-spyware apps and some anti-virus apps if allowed and installed them on the hard-drive, run them at the very least weekly.
4. Try using the latest software and keeping up to date with security updates on a machine.

Nonportable App

I find it best to keep these install files on my USB key as well as most of my firewall, anti-spyware and

anti-virus tools.

The Crap Cleaner. The sucker gets rid of just about everything, for free. Unfortunately there's no program like it (or lesser but similar) that's portable at the moment. So if you must install on the hard-drive, lets go for the best. There is a way to place CCleaner batch file and some DLL files on your USB key, and run it from there without a GUI.. but i'm currently working on getting that up and running smoothly. Until then.. install the application.

1. Then go to Settings.
2. Then Change "Secure Deletion" from Normal to Secure.
3. Change the drop down to NSA (7 passes). (it re-writes over the deleted data with 7 layers of garbage to ensure against recovery). This can still be recovered, it just makes it a helluvalot less likely.

[Download Crap Cleaner here](#)

Cleans the following:

Internet Explorer: Temporary files, URL history, cookies, Autocomplete form history, index.dat.

Firefox: Temporary files, URL history, cookies, download history.

Windows: Recycle Bin, Recent Documents, Temporary files and Log files.

Registry cleaner

Advanced features: removes unused and old entries including File Extensions, ActiveX Controls, ClassIDs, ProgIDs, Uninstallers, Shared DLLs, Fonts, Help Files, Application Paths, Icons, Invalid Shortcuts and more... also comes with a comprehensive backup feature Third-party applications

Removes temp files and recent file lists (MRUs) from many apps including Opera, Media Player, eMule, Kazaa, Google Toolbar, Netscape, MS Office, Nero, Adobe Acrobat, WinRAR, WinAce, WinZip and many more...

Safe XP This makes Securing your system and shutting off some communication and some machine broadcasts easy.

<http://www.theorica.net/download.htm>

Installing Tor to a Hard-drive

I've mentioned several times throughout the article, that there are advantages to having Tor run locally on the machine. You can download and install the application here:

<http://tor.eff.org/download.html.en>

Proxy Sites

You can also go this route of going through a proxy site. There's hundreds of them. But be warned. A lot of websites also block these proxies. So don't be suprised if you can't post on your favorite message board with them. Also, it's generally a bad idea to input a password into a site while browsing through one of these. As your cookies for the site are stored on their servers and all information you input can be extracted from their servers. Also, these should be used to get around web filters more than anything. Don't expect them to keep you anonymous on your LAN, or on the servers of the pages you're accessing. There are packet sniffers that can see where you're going even through a web proxy

It should also be noted, that a proxy that will never go away is simply.. Google's translate function. Take your favorite website and get Google to translate it to English. Google will then automatically act as a proxy for your activity on the site.

[GO Anon](#)

[VTunnel](#)

[SickProxy](#)

[URhidden](#)

[Trickmy](#)

[aTunnel](#)

AnonymOS

For the truly dedicated, this is also a route to take. To do anonymous web activity (i wouldn't suggest this in a work place or a school..) Download this Live CD, burn the ISO as a bootable disc, boot your computer on it, and use this to access someone else's WiFi network. All your Windows Portable apps will not work with this as this is a version of Linux with applications installed for you. You merely boot your computer off the cd and the operating system loads. When you're done, eject the cd, boot your

computer back up, and you'll be back to normal with Windows and all. From their homepage:

kaos.theory's Anonym.OS LiveCD is a bootable live cd based on OpenBSD that provides a hardened operating environment whereby all ingress traffic is denied and all egress traffic is automatically and transparently encrypted and/or anonymized.

[Download it here](#)

Simple Tests

As the title says, SIMPLE. Meaning, just because you pass these tests doesn't mean you're 100% secure or anonymous (on the LAN side or the WAN side).

The easiest thing you can do to test your anonymity is to go to WhatismyIP.com and see if the IP showing up is yours or not.

After that you can check out services like:

[AuditmyPC Privacy & Spyware Check](#)

[BrowserSpy](#)

And then there are various proxy tests:

[Proxy Test](#) and [Proxy Checker](#).