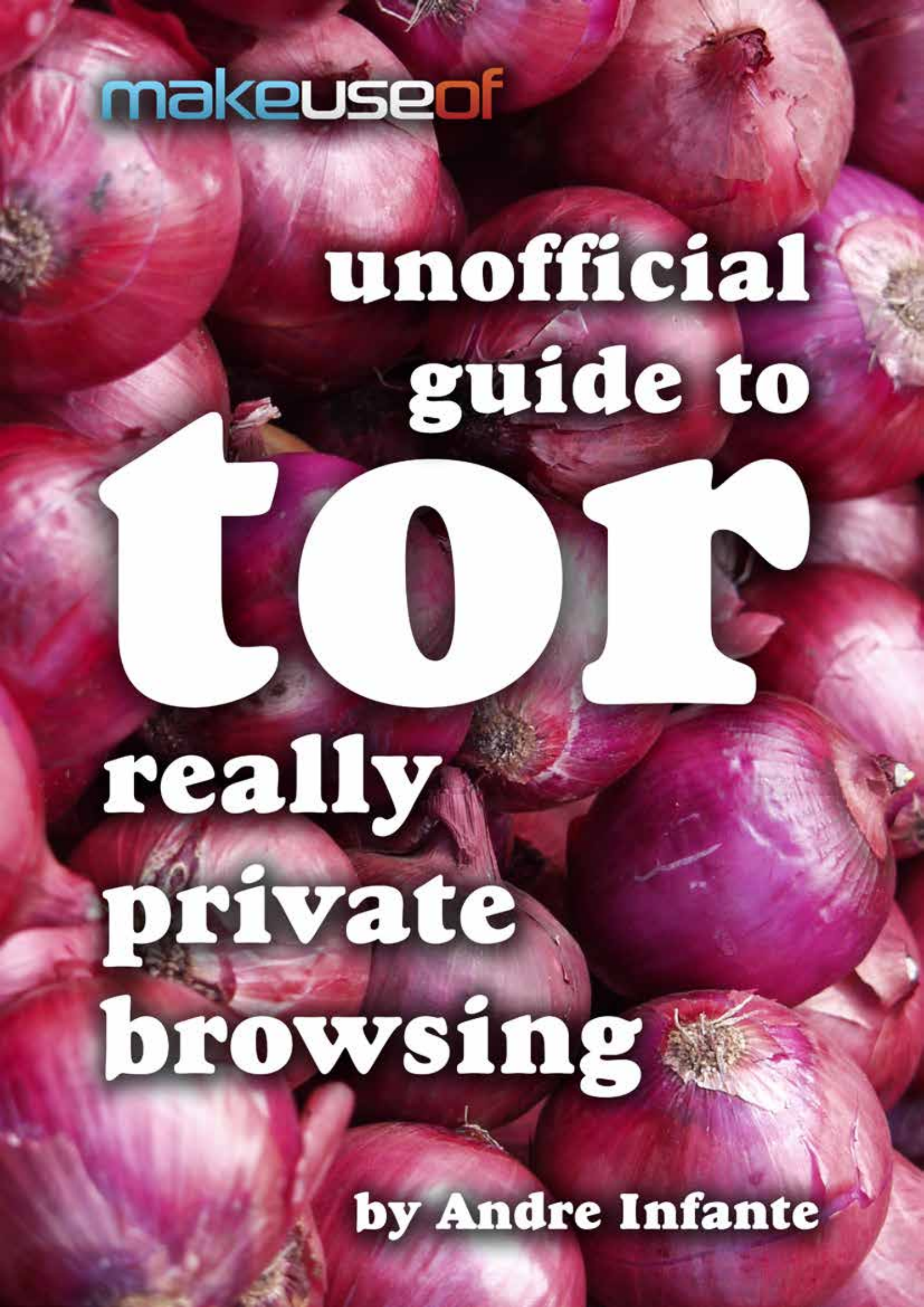

makeuseof
unofficial
guide to
TOR
really
private
browsing
by Andre Infante

by Andre Infante
http://www.petafl0p.com/

Published October 2013

share: 

Think you've got what it takes to write a manual for MakeUseOf.com? We're always willing to hear a pitch!
Send your ideas to justinpot@makeuseof.com.

Table Of Contents

1. Introduction

The issue of privacy on the Internet has long been a difficult one: there are a lot of good reasons that you might be leery of strangers reading your emails or spying on the websites you visit – and there are equally compelling reasons that various unscrupulous people, corporations, and governments might want to do just that. The whole issue has come to a head recently with the revelation that the NSA has been illicitly spying on American citizens and others through Facebook, Google, and Skype – including, probably, you.

This sort of invasion of privacy makes a number of people very nervous. If you're one of these nervous people, there's some good news: a number of powerful tools exist which allow you to protect your privacy online. One of the most useful of these tools is called Tor. Tor provides truly anonymous and untraceable browsing and messaging, as well as access to the so called "Deep Web" – a network of anonymous, untraceable, unblockable websites, available only through Tor, which provide everything from resources for political activists to pirated movies. The military-grade encryption behind Tor is so powerful that it can't plausibly be broken by any organization on the planet.

While there are a number of ways to try to protect your privacy online, only a few of them are resilient against a really dedicated adversary (like, for example, the NSA). One of the exceptions is Tor. Tor is designed to be, more or less, impenetrable to any attacker without a completely implausible amount of computing power.

Even better, the software itself is designed to be easy to use without a technical background: if you can use Firefox, you can use Tor.

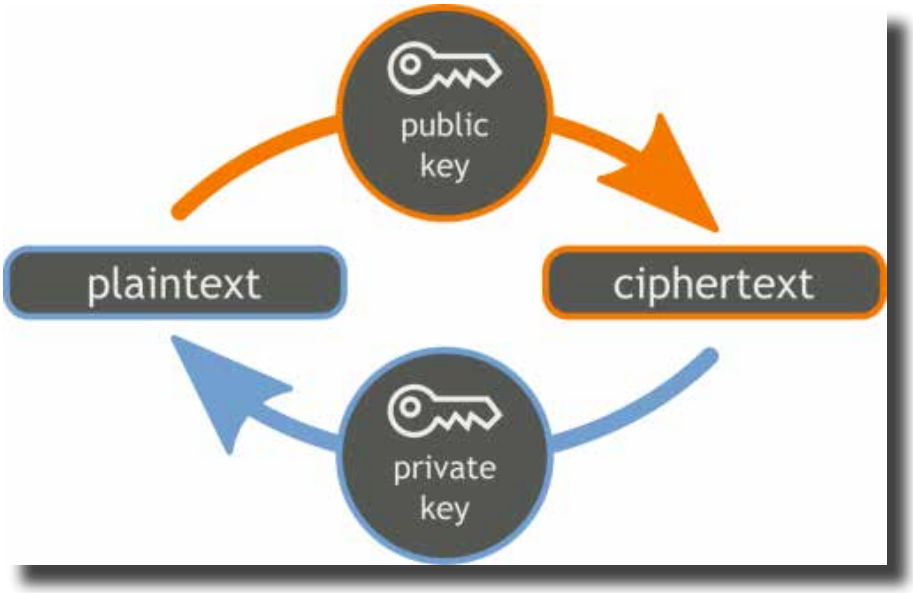
In a nutshell, Tor is a powerful, easy-to-use piece of software that lets you keep your online life private. This guide will provide a step-by-step guide to installing, configuring, and using Tor, and getting you started taking an active role in defending your privacy on the Internet.

2. How Tor Works

One of Tor's strengths is that you don't need to know how it works to use it. If you're not interested in the technical details, you can skip to the installation section below. However, because the mechanics behind it are clever and interesting, I will briefly run down the technology behind Tor for the curious.

2.1 Modern Cryptography in Brief

Most modern cryptographic tools are based on a technology called **asymmetric encryption**. Don't let the name scare you: it's actually pretty simple. Asymmetric encryption allows you to use two different "keys" (passwords) to encode and decode information: the encoding and decoding key are linked so that each can only be used with the other, but there exists no efficient way to find one key given the other. As a result, you can safely distribute an **encoding key** while keeping the matching **decoding key** a secret. This means that anyone who wants to communicate with you secretly can take your public encoding key, and encode a message with it that only you (the owner of the secret, matching decoding key) can read. The names of these keys are typically shortened to '**public key**' and '**private key**,' respectively.

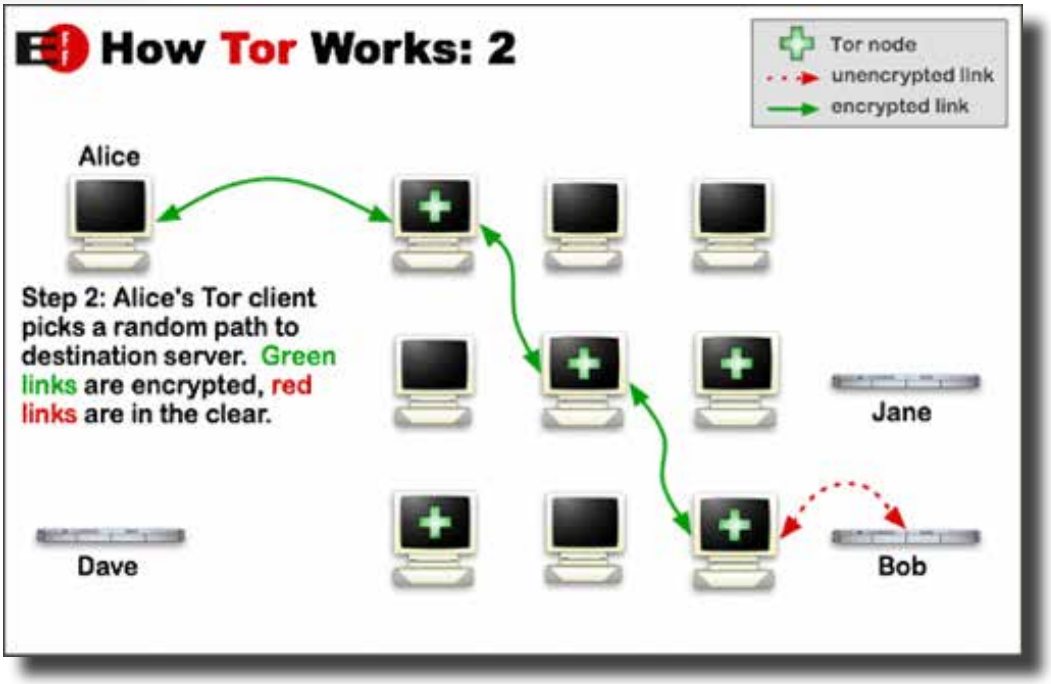


For any Tor communication through a secure HTTPS connection (for example, between your computer and a server hosting a website), you and the person you're communicating with both begin by exchanging your public keys: this allows both of you to talk to the other securely, even over a tapped line: a third party listening to the line would only see two public keys being exchanged, and then a sequence of gibberish that they can't decode.

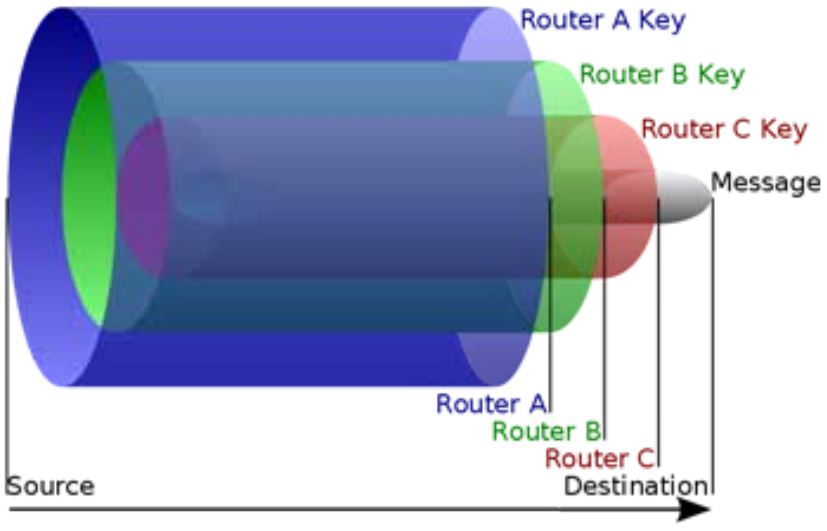
This is a good start, but Tor goes even farther to protect your privacy online. A number of services provide strong encryption for messages - for example, it is relatively easy to implement end to end encryption for Gmail messages, but there are limitations to the security that this provides.

2.2 Onion Routing: Not Just For Vegetables

Even if two people are speaking a language that you can't understand, you can still deduce a lot by watching who talks to who. That's why Tor implements a technology called **onion routing**, which obscures not just the contents of a message but who they're passing between.



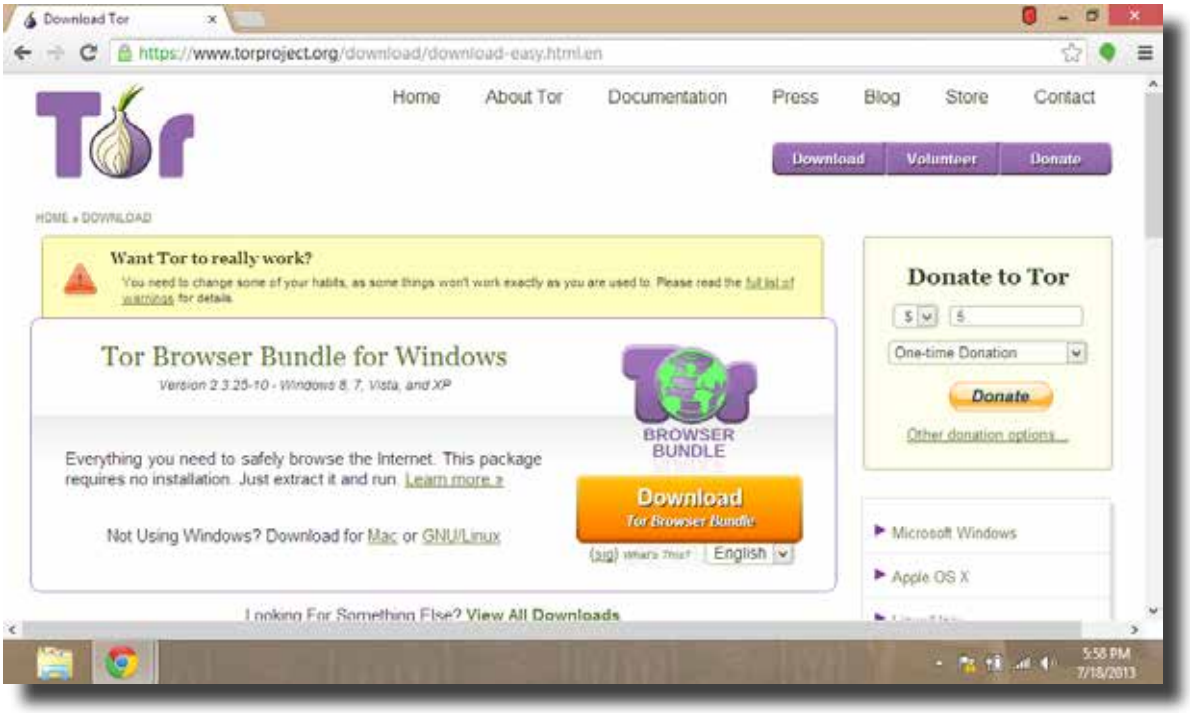
The way onion routing works is as follows: everyone who uses Tor distributes, peer to peer, a copy of their public key and their IP address. When you want to send a message untraceably to another user (call her 'Alice'), your copy of the Tor software goes to your list of known Tor nodes and randomly picks three intermediaries (Bob, Charlie, and Dave). It encrypts the message, in turn, for each link in the chain, along with instructions to pass it on to the next link in the chain. Because nobody can read the message intended for the next link in the chain, nobody knows what the message says, or where it's going next. Furthermore, when they get a message, they don't know whether the message originated with the person sending it to them, or if they're just someone passing it on. As a consequence, unless Bob, Charlie, and Dave all happen to be in cahoots, it's impossible for any of them to find out where the message originated, or where it's going.

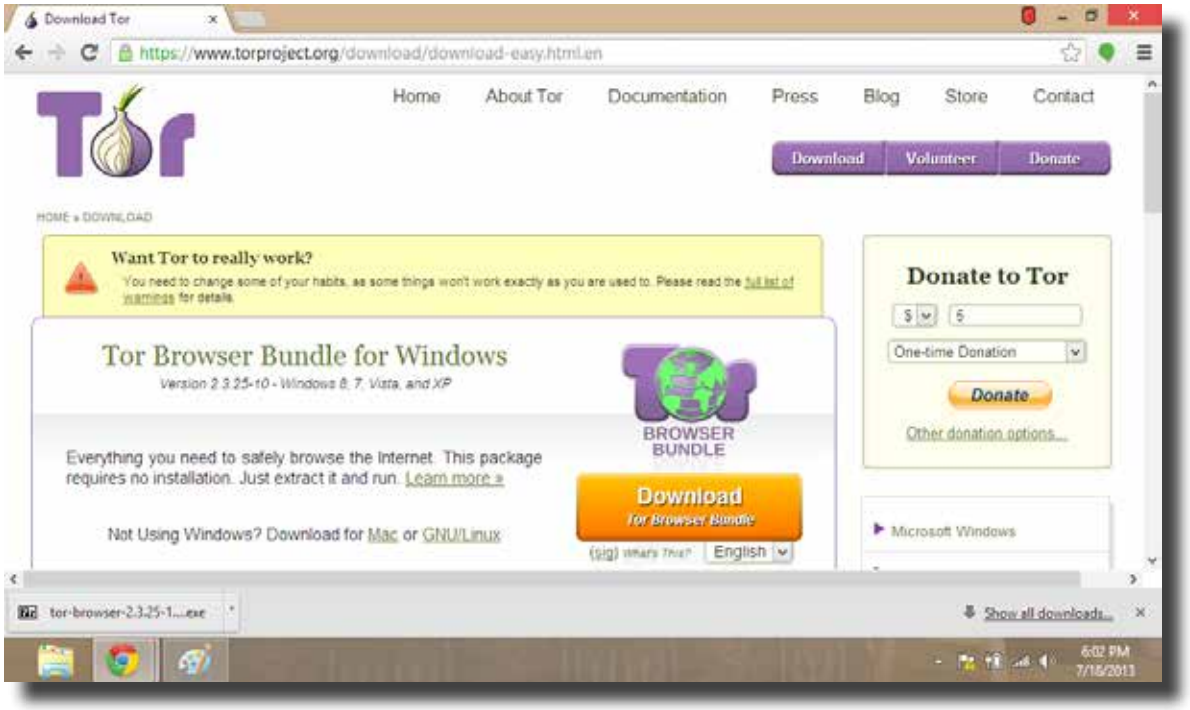


It it this technology that provides the backbone of Tor, and gives it most of its strength. For a more in-depth explanation, check out this article on what onion routing is.

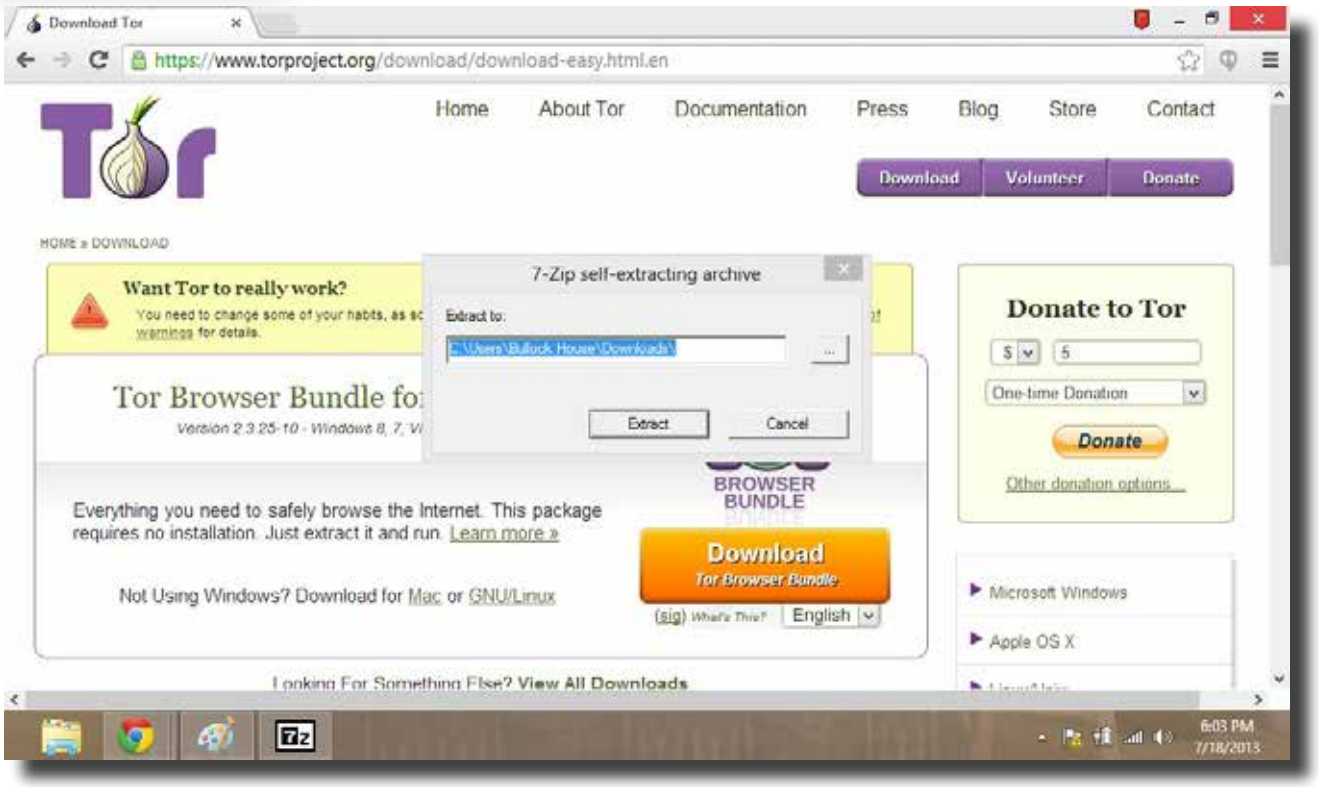
3. Installing the TOR Browser Bundle

Installing the Tor Browser Bundle is easy. It's available for Windows, Mac and Linux, but we'll go through the process for Windows. First, go to https://www.torproject.org/ - the 's' after 'http' is important, as it means (among other things) that your computer is verifying that the website you're talking to is what it claims to be. Click the large 'download Tor' button, and, when the website loads a new page, click the orange button labelled 'Download Tor Browser Bundle.'

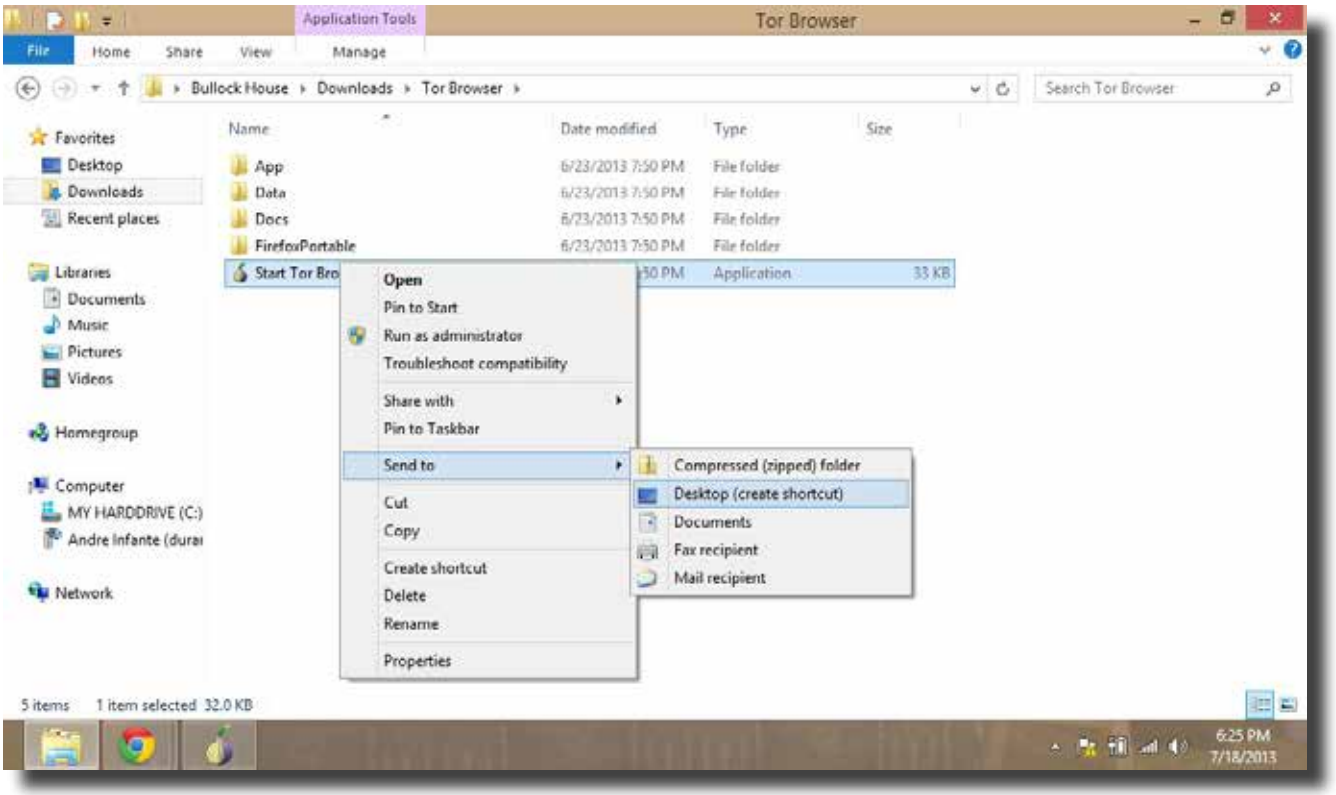


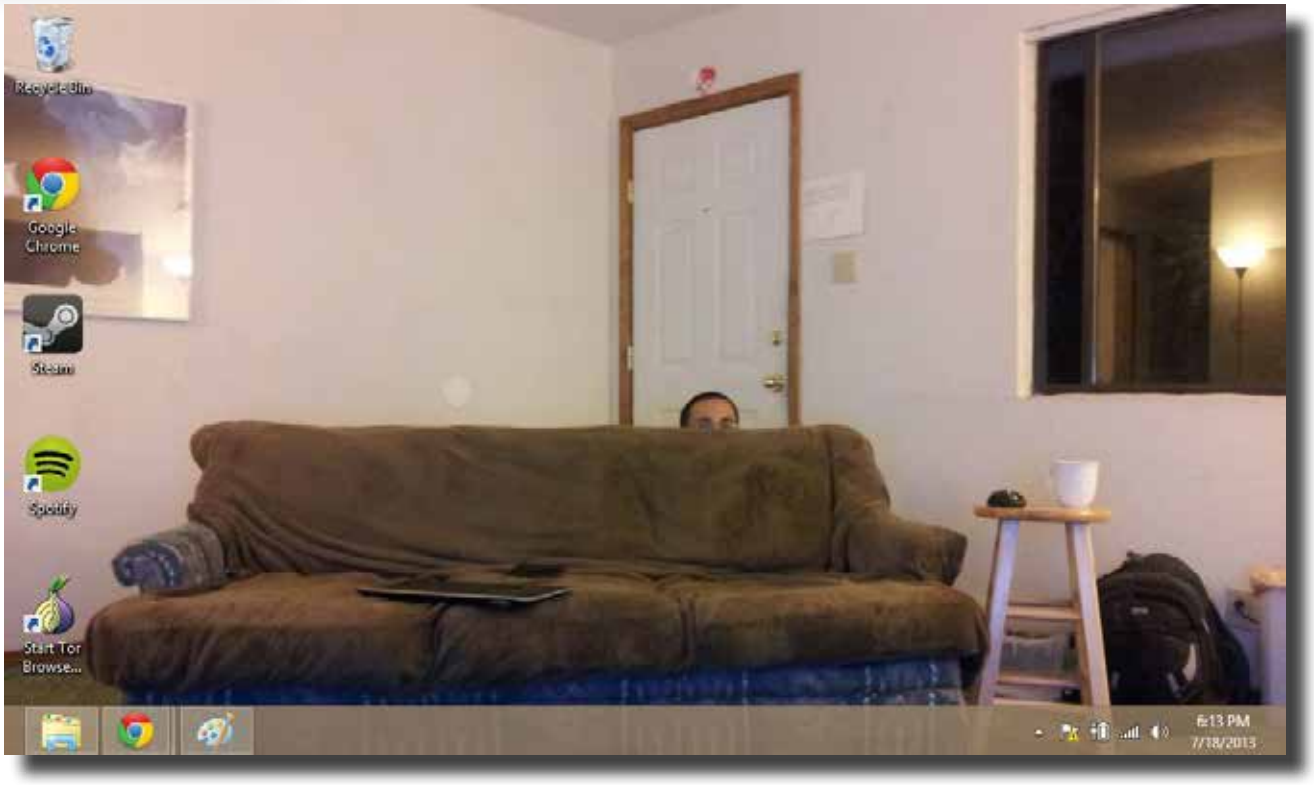


A download will begin. When it's finished, you can view it in your download bar or download menu. When the download has finished, run it, and you should see a window appear. Select a directory where you want to install the Tor program and associated files (if in doubt, put it on your Desktop). Make a note of the directory you selected and click 'extract' at the prompt that you see. A loading bar will appear.



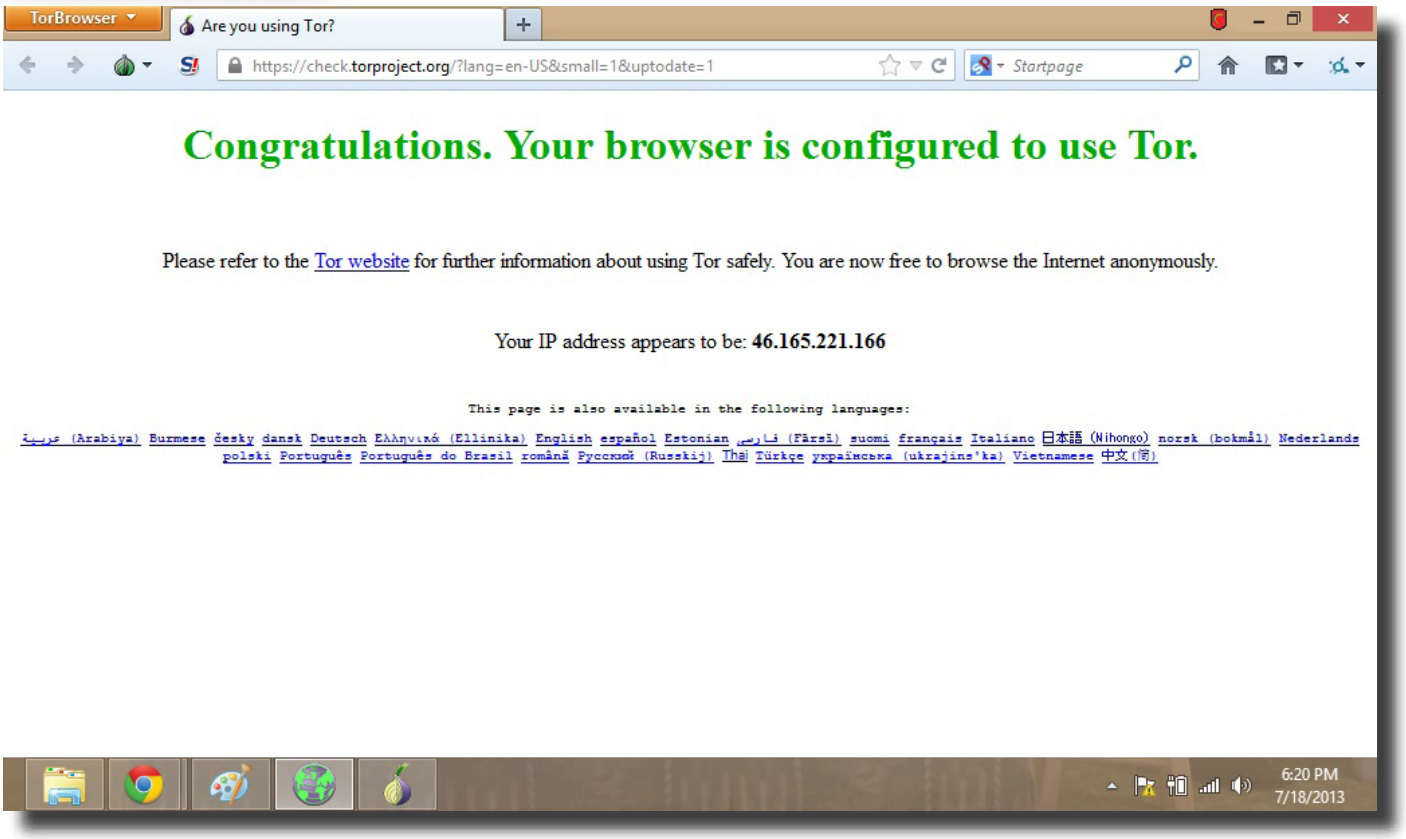
When the extraction is finished, go to the directory you selected. You'll see a folder named 'Tor Browser' - open it, and you'll see a document entitled 'Start Tor Browser.exe' In Windows, right-click on the file, and select 'send to.' In the sub menu you see next, click 'Desktop (create shortcut).' This allows you to access the Tor browser easily from the desktop. Go to your desktop and double click on the Tor shortcut (it will have a cartoon image of an onion).





This will open a small menu with a loading bar labelled 'Vidalia control panel.' When the loading bar completes, check to make sure that it shows an active connection to the Tor network (see below). If it doesn't, you may have an issue with your Tor connection. Go to the 'support' section below for suggestions.

A few seconds after the connection is established, the Tor browser itself will open and display a test page. It should look something like this:



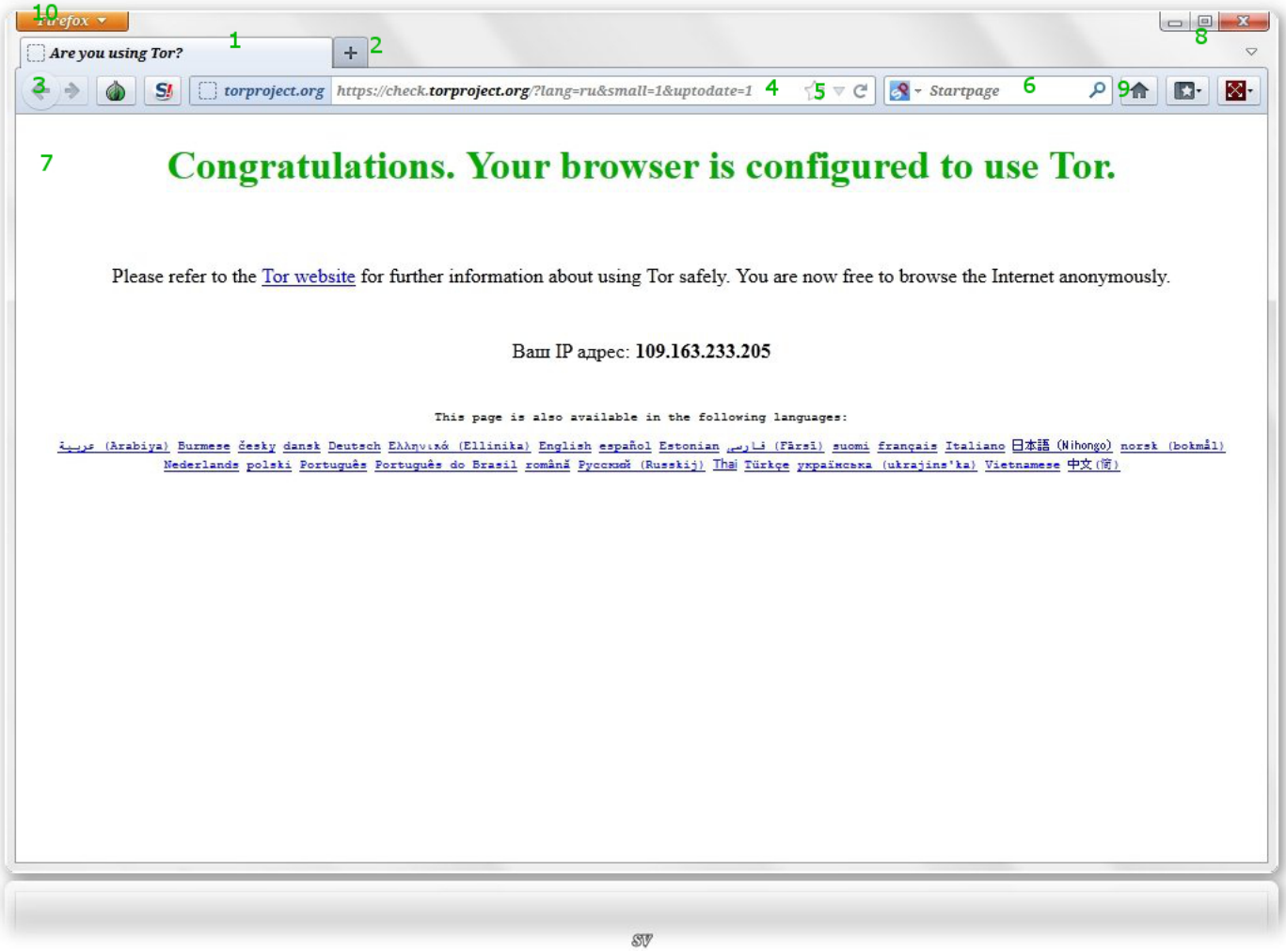
Congratulations! You're now connected to the Tor network. If it tells you to update your client, do so before moving on (this is very important). If not, please proceed to the next section of the tutorial.

4. Browsing Basics

One of the things you'll notice quickly is that the browser looks almost exactly like Firefox. There's a reason for that: the Tor browser is based on Firefox. For the most part you can browse with it exactly like you would on classic Firefox, or other modern web browsers. For those who are unfamiliar with modern browsers, we'll do a brief tutorial on how to use the basic features before we move on to the cool stuff.

4.1 Browser Layout

The lower portion of the browser simply displays the contents of the web page you're currently viewing. Above it is a two-layer control bar. See the diagram below for a list of the basic controls and what they're for.



1. **The tab bar**. *This bar can comfortably hold between one and about a dozen tabs - each one represents a website that's currently 'active' in your browser, and you can see an icon and a name associated with each page. Navigate quickly between different tabs by clicking on them.*

2. **New tab**. *The 'plus' button pictured creates new blank tabs, which allow you to browse to a new website*

3. **Back / Forward**. *These arrow buttons allow you to browse back and forth through your recent history. Note that this history will be purged when you close the browser.*

4. **URL box**. *This field allows you to enter and edit URLs, for finding websites directly.*

5. **Bookmark button**. *This 'star' allows you to save a page to your bookmarks for future reference.*

6. **Search box**. *This box allows you to search the Internet anonymously.*
7. **Current page**. *This large field shows the contents of the web page or hidden service represented by the tab you're currently viewing.*
8. **Applications controls**. *These buttons allow you to minimize, maximize, or close the Tor browser.*
9. **Menus**. *These menus give you access to your home page, your bookmarks, and certain settings, respectively.*
10. **Tor-Specific Settings**. *These settings allow you to alter some of Tor's behavior. Be careful, as these can compromise your security online.*

4.2 Tabbed Browsing

Tabbed browsing, a core feature of modern browsers, allows you a fast way to switch between many open web pages, without having to navigate between multiple windows. It's one of those features that is way more useful than it sounds By default, the browser launches with one tab open. You can open more by clicking the small plus beside the tabs, or by right clicking a link and selecting 'open in a new tab.' You'll see the names of the websites arranged in the top bar, and you can swap between the open web pages by clicking on them. Try it. Open a new tab, enter, 'https://www.google.com', and hit enter. Now swap back and forth between the Google homepage and the Tor splash page. Cool, right? When you want to close a tab, click on the little 'x' at the far right-hand side of a particular tab. You can click and drag on a particular tab to change its position in the sequence.

4.3 Bookmarks

Remember that Tor only protects you against snooping on your network activity: if you bookmark a page, it will leave a record on your computer that you visited it. If you're okay with that, then bookmarks can be created by holding the key combination Ctrl-D, or by clicking on the 'bookmark' icon in the upper right and selecting 'Bookmark this page' from the dropdown menu. You can see a list of pages you've bookmarked in the past on the same menu.

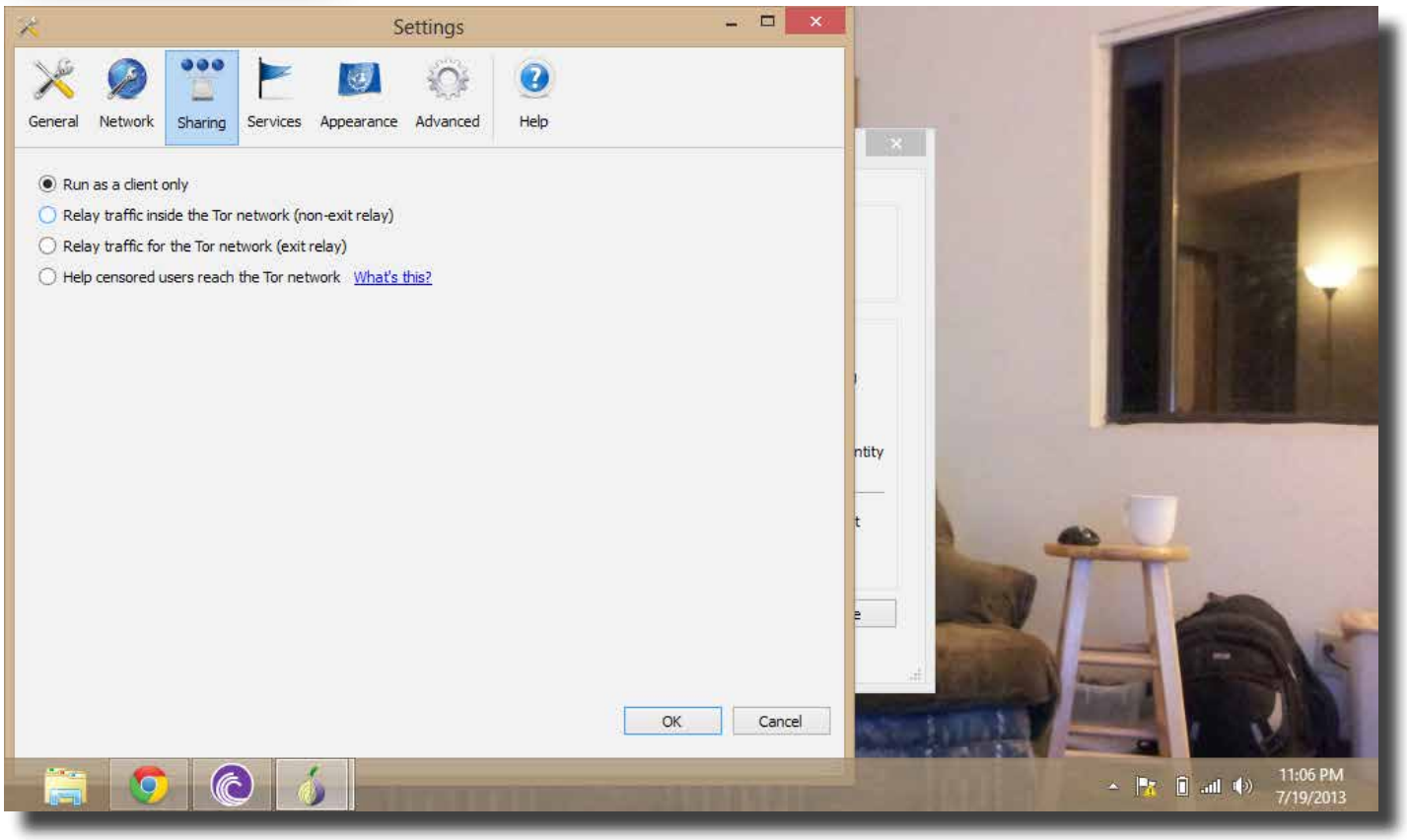
4.4 History

One useful feature of modern web browsers is that they keep a log of websites you've visited. In Tor, this log is cleared when you close the browser for security purposes, but it's still useful within a particular browsing session. You can page backward and forward through the list of recent websites by using the arrow buttons in the upper left hand portion of the browser.

5. Configuring Tor

By default, Tor is designed to run in client mode, which uses the Tor network but does not contribute to its operation. If you have a comfortable Internet connection, you may wish to contribute a small amount of bandwidth to help keep the network operational.

To do this, go to the 'Vidalia control panel' window that opened with Tor. Be very careful about changing any settings here, as they could potentially compromise the security of your connection. Click 'Setup Relaying' and select the 'Sharing' tab.



You have a few options here. The simplest way to help is to turn your Tor client into a relay, which simply allocates a small portion of your bandwidth to routing messages within Tor. This makes it more difficult for malicious parties to insert so many compromised nodes that they can reliably trace messages from end to end. This option is safe and mostly anonymous. To do this, click the option labelled 'Non-Exit Relay,' and select how much bandwidth you want to provide to the network.

Those who are more ambitious may choose to run a Tor exit node. Exit nodes provide an interface between the Tor network and the Internet at large, and you use them every time you connect to a normal website through Tor. Exit nodes are very important to the operation of the network, but there are risks to running them. Some jurisdictions will hold (or try to hold) Exit Node operators responsible for the traffic going through their node, which can include illicit activities like piracy and illegal pornography. We do not suggest running an exit node unless you are prepared to face the potentially serious consequences for doing so. If you do choose to run an exit node, this can be enabled under the appropriately-labelled option, at your own risk. For more information about running an exit note, check the Tor Project FAQ.

Finally, if you know people who live in an area where access to Tor is censored, and you'd like to give them access to the network, you can configure your Tor software into what is called a 'bridge.' A bridge is a proxy, not obviously associated with the Tor network, which can provide a secure access point. Such functionality can also be accessed from here, although it's somewhat more complicated. Again, we suggest that you visit the Tor Project FAQ for more detailed instructions if this interests you.

6. Tips for Safe Browsing

Tor does a great deal to keep you anonymous on the Internet, but, if you want Tor to be completely effective, you'll need to make a few changes to the way you use the Internet.

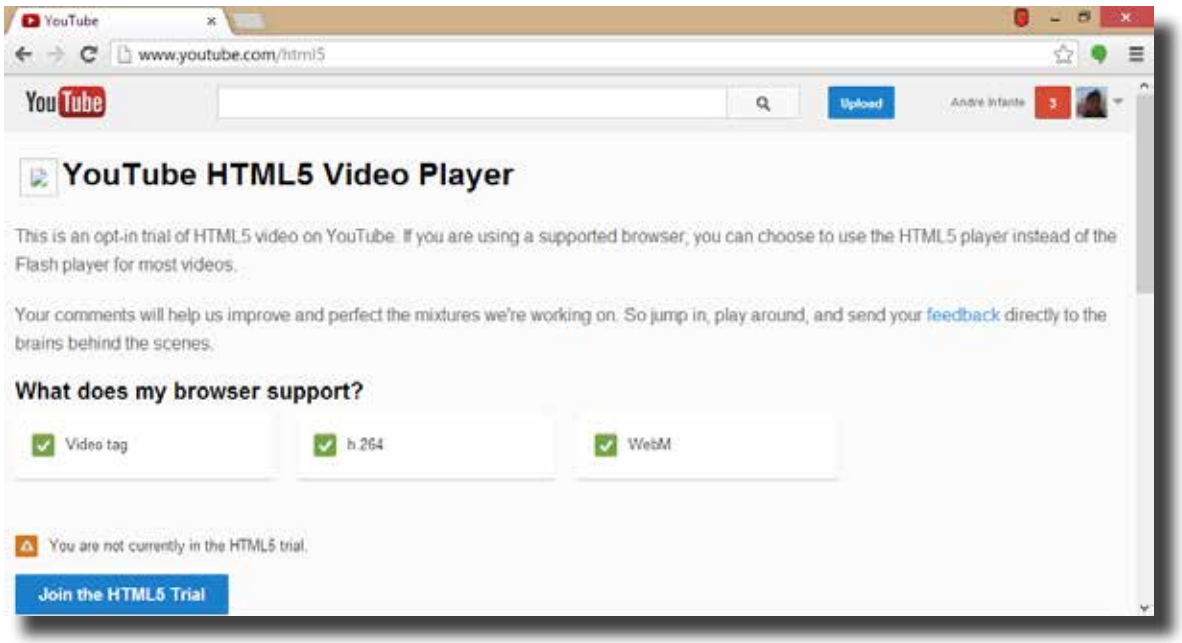
A good start is to be aware of Tor's limitations. Importantly, Tor only protects traffic that you route through the built-in Tor browser, or other Tor-compatible applications – it will not protect your normal web browser, or the activity of other programs on your computer. Tor also can't protect you if the person or server you're communicating with is keeping logs. It will prevent your IP address from being revealed, but the contents of your conversation with the other party can, unilaterally, be stored by them, or made public. For example: if you log into Facebook or other social networks through Tor, anything you do on that social network will likely be logged by it, and may be stolen or seized by malicious parties later. The same goes for webmail accounts like Gmail, or chat websites.

You may notice that Tor does not connect to Google, by default. This is because Google keeps extensive logs on all searches made by it, which could, potentially, be traced back to you from their content. Instead, Tor connects to a service called 'StartPage,' which anonymizes your interactions with Google's service to prevent a list of searches from being attributable to a particular browsing session.

Tor also can't control the behavior of its browser extensions, or scripts on websites, which can sidestep Tor entirely and report information about your activity directly to third parties. As a result, Tor (by default) automatically blocks the execution of scripts on websites, and prevents the use of extensions. While this behavior can be changed, it's not a good idea. Most websites will work fine without scripts or extensions, and it contributes tremendously to your security online.

Tor can also not always guarantee that the website you're visiting is the one you think you're visiting. It attempts to force HTTPS support (which forces websites to authenticate themselves in a secure way and maintain their end of the encrypted channel) - but not all websites support HTTPS - make sure you're visiting a secure website, and be careful on those that aren't.

One of the side-effects of this added security that might affect you is that it disables YouTube, as flash has serious security vulnerabilities. Fortunately, YouTube currently supports an HTML5 beta, which will run in Tor. You can opt in here, though it may not work on all videos.



Lastly, know that a number of document types – including executable files, PDFs, and .doc files – can contain resources that circumvent Tor and can, maliciously or innocently, disclose information about your browsing activity. Tor will warn you when you download a file that could potentially be a security risk, and it's wise to pay attention.

7. Tor Tips and Tricks

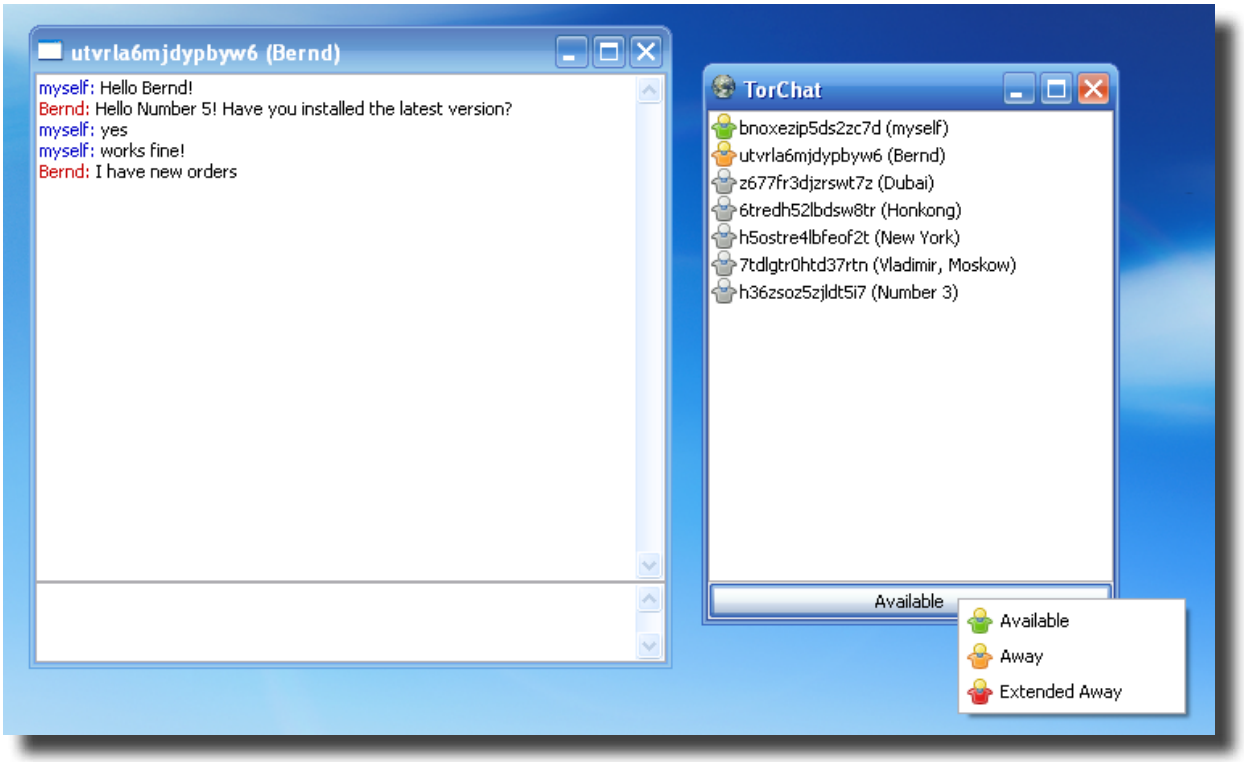
Out of the box, Tor allows you to browse the Internet anonymously. This is extremely powerful, and has been useful to people all over the world. Beyond this, though, there's a lot of cool functionality that you can get out of Tor. Here are a few simple tricks to let you use Tor for much more than its normal browsing behavior.

7.1 Anonymous Messaging

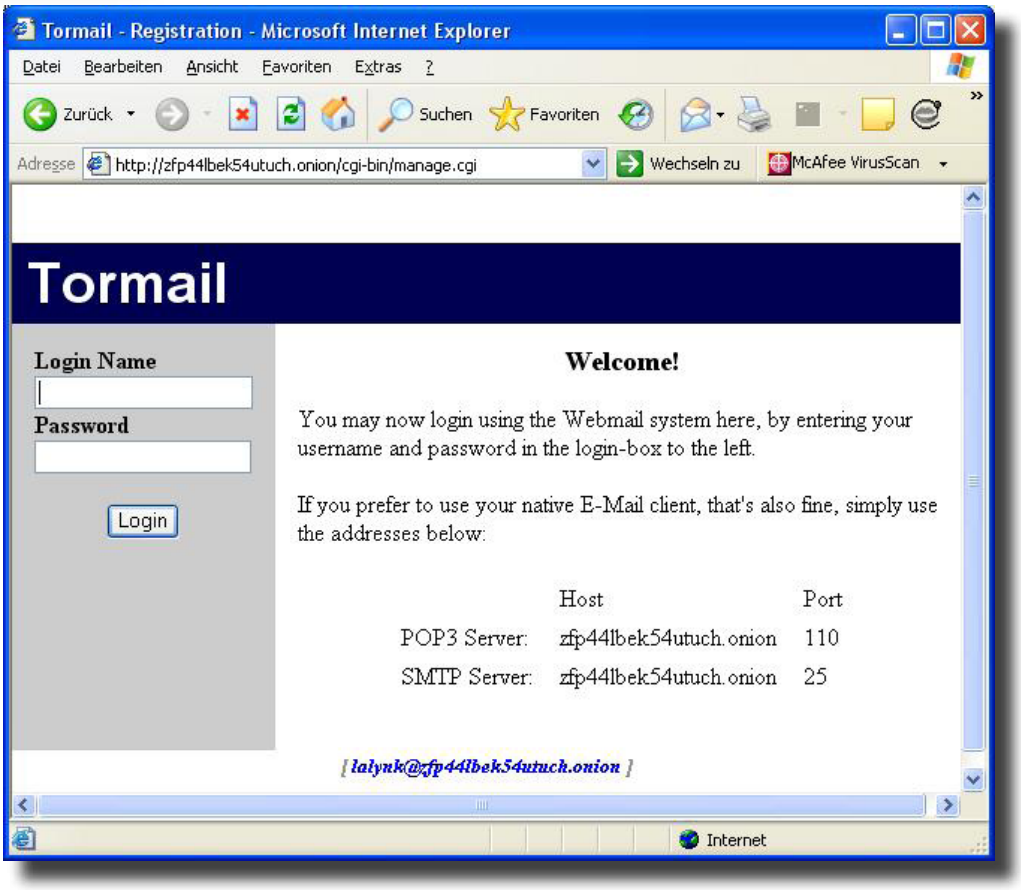
One particularly worrying feature of the recent spying leak was the revelation that a number of supposedly private avenues of messaging – notably Google Chat, Facebook messaging, and Skype – are being monitored and recorded. In today's world, a number of intensely personal matters are discussed every day over instant messaging, and it would be nice to have a private channel to have those conversations. Fortunately, several methods exist to establish just that.

The strongest guarantee of privacy available in instant messaging is TorChat, an anonymous chat application that runs over the Tor backbone. You can get the TorChat extension here. Unzip it into a folder of your choosing,open the 'bin' folder, and select the 'torchat' executable. The application will open.

TorChat operates like a traditional chat client, except that instead of your name, you are represented by a string of random numbers and letters. This string is your public key, and you can freely distribute it to people you want to talk to, and they can use it to add you as a contact. From here, a traditional (if very secure) IM conversation can ensue. You can add contacts using their public keys by right clicking in the chat window and selecting 'add contact.' TorChat also runs over the Tor background, making it impossible to determine who is communicating with who within the network proper.



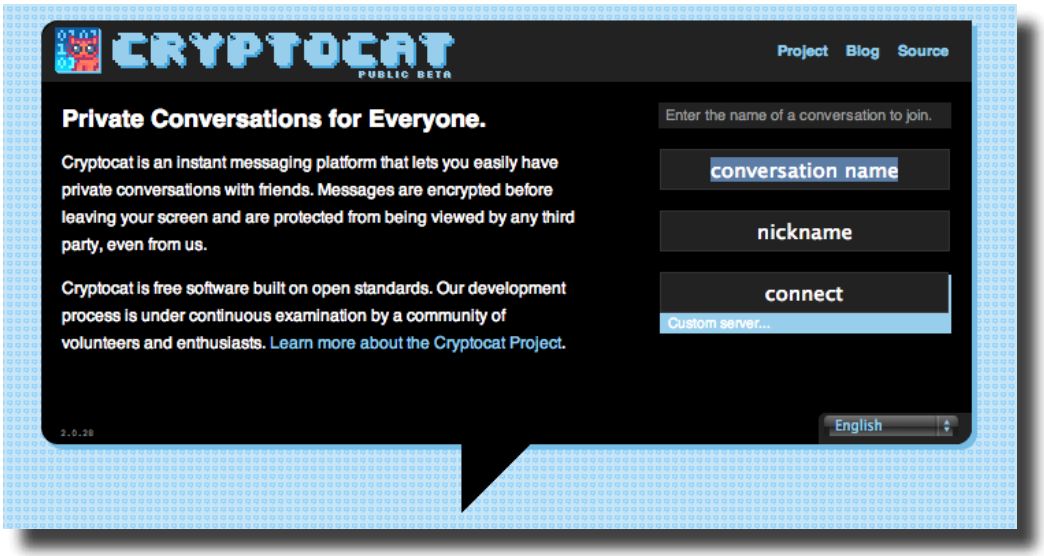
If you're looking for something more like a cryptographically secure IRC, accessing the cryptocat service (which employs an absurdly paranoid level of encryption) via Tor provides a strong degree of protection, though communication within the cryptocat network are not onion routed themselves. You can find the web app and more detailed instructions on the crypto.cat website.



7.2 Anonymous Email

One of the coolest features of Tor is the ability to run so-called “hidden services,” which we’ll go into in more detail in section 8, “The Deep Web.” For now, understand that a hidden service is a service, operated through Tor, which does not exist outside of Tor, and does not reveal anything about itself to the world except its contents, making it (for practical intents and purposes) impossible to identify in any real-world context.

One of the most useful hidden services is called Tor Mail. Tor Mail provides a service very similar to Gmail or Yahoo mail, except that it can only be accessed through Tor, it can’t be subpoenaed, seized, or searched, and the server keeps no unencrypted records about the contents of your mailbox. To access the Tor Mail hidden service, go to http://jhiwjjlqpyawmpjx.onion/ in the Tor browser, and follow the instructions you see there.



7.3 Run a Secure Operating System with TorBox

While IM, web browsing, and email are useful, there are many pieces of software that require Internet access, and vanilla Tor can't provide security for all of them. Furthermore, Tor does not protect documents that you collect, nor does it stop local records from accumulating. A good long-term solution is called TorBox, which is a virtual machine that provides an added layer of security. TorBox, which is based on Linux, creates a simulated computer which encrypts its hard drive when you shut it down, and routes all of its traffic through Tor.

Any application run through Torbox is secure, and, when the operating system is shut down, no unencrypted data about its use is stored. If you feel that you need that level of security, TorBox can be helpful. Installing and setting up TorBox is a little bit more in-depth than simply using the Tor browser, and beyond the scope of this guide. You can find a more in-depth explanation and guide to configuring TorBox here.

In this section, we're going to discuss the Hidden Services mentioned in the last section in substantially more detail. To understand why hidden services are important, we should first talk about one of the major weaknesses of Tor, namely the exit nodes. All traffic that goes to the outside Internet, while it's encrypted if you use HTTPS, has to pass over non-Tor nodes and risk (potentially) being spied upon. If you have enough information about the flow of traffic through the network, it might be possible to deduce who is talking to who by doing timing analysis of the behavior of individuals and the behavior of Tor exit nodes. The problem is exacerbated by the small number of exit nodes.

Worse, on the traditional Internet it is more or less impossible to conceal the physical location and ownership of a particular website server – using Tor, the viewer of the website may be safely anonymous, but the same is not true for the website owner or provider. As an example, the Pirate Bay has become accustomed to changing domain name every few months or weeks, as legal action is taken against it.

What a hidden service allows you to do is to is to insert a server as just another node in the Tor network -- when you access a hidden service, both you and the server are anonymous nodes on the Tor network, and the traffic between you never leaves the network - and, therefore, never is exposed to prying eyes. Furthermore, because the server is anonymous, it can't be taken down, subpoenaed, or blocked.

Taken together, the hidden services available on Tor comprise a major portion of what is ominously referred to as the 'deep web' or the 'darknet' – the portion of the Internet that is not accessible through traditional search engines. In this section, we're going to talk about how to explore this portion of Tor.

First, though, beware: the deep web is populated by a number of strange and scary people: drug dealers, pedophiles, terrorists, and Libertarians all have their little corner of the deep web. Obviously, neither the author nor makeuseof.com endorse any illegal activity of any kind. Furthermore, you should be very careful when exploring the deep web. Be very careful and not too trusting – beyond what you already are on the rest of the web.

Now, with all caveats well and truly emptored, let's get started.

Tor hidden services have addresses that follow the following format: **http://[big block of nonsense here].onion**. The .onion signifies that it's a hidden service, and the big block of nonsense is a randomly generated public key for the hidden service. We suggest bookmarking them to avoid having to type the block of nonsense in every time, which can become tedious. Because the deep web isn't networked by regular search engines, navigating it can be a bit troublesome. However, a new search engine called TorSearch is attempting to become a Google for the Tor network.

A good starting place is the hidden wiki, which you can access through the Tor browser at http://3suaolltfj2xjksb.onion/hiddenwiki. The hidden wiki archives most of the Tor hidden services that are open to the public, but is moderated to remove some of the worst content and provide something that, if not actually family friendly, is probably not illegal to view. The wiki is divided up into sections, and you can browse lists of hidden services that interest you from there. Once again: be careful, and don't give anyone money.

9. Uses of Tor

To people first encountering it, it can be difficult to imagine a use for Tor. In truth, most people in first world countries without strong feelings on privacy have no practical application for it, though they may find it interesting to browse anyway.

For the rest of the world, a number of applications have arisen, from the criminal to the noble. It is, of course, used for distribution of illegal substances: you may have heard of The Silk Road, which is an ebay-like venue for drugs and other illicit materials, hosted as a Tor hidden service. On a more positive note, Tor is used to coordinate political activism against a number of oppressive regimes around the world, most recently in the Middle East. It's also used as a channel to distribute banned books in countries with weaker free speech laws than the US. Its ability to anonymize access to the Internet is also used every day by Chinese nationals to circumvent the so-called Great Firewall of China and access western websites. In the United States and Western Europe, use of Tor is often seen as a safe and legal way to protest intrusive government surveillance.

As with any technology, the ability to communicate anonymously through Tor can be used for many purposes, good and bad, legal and illegal. How you choose to use it is, as always, your own prerogative.

10. Support and Problems

Sometimes, software doesn't work. If Tor is giving you problems, there are resources to help you. First, make sure your version of the Tor client is up to date (the default start page will warn you if it isn't). If it's still not working, reinstall the Tor software, and check your firewall software and make sure that Tor is allowed. Additionally, try running the application in administrator mode (right click on the executable and select the 'administrator mode' option).

If these basic solutions don't help, or if you have more detailed questions about using Tor, you can view the project documentation here, and the FAQ here. If all else fails to solve your problem, you can also email the developers of Tor at *help@rt.torproject.org*

Tor is not commercial software, so it may take some time for someone to help you resolve your issue. However, there is a vibrant and active Tor community, and most problems can be solved by asking politely for help and being patient.

11. The Future of Tor

Recent political revelations have inspired a new surge of interest in Tor, and the community of users is expanding rapidly. Additionally, the recent political instability in the Middle East has dramatically bolstered Tor's reputation with the public, by vividly showing that the software has uses above and beyond the drug trade and Bitcoins. It seems likely that the Tor network will continue to grow for the foreseeable future.

Legally, the water is somewhat murkier. Tor is illegal in a number of jurisdictions, and –while it remains legal in the United States – Tor has come under fire from the FBI, DEA, and many other agencies there. So that legal status may change. Tor is difficult or impossible to effectively restrict access to, but a change in legal status in the West could certainly slow its adoption.

What will remain true, however, is that freedom of discourse is most needed when it is not allowed, and Tor will remain a powerful tool against oppressive regimes around the globe for many years to come.

Guide Published: November 2013

Did you like this PDF Guide? Then why not visit MakeUseOf.com for daily posts on cool websites, free software and internet tips?

If you want more great guides like this, why not subscribe to MakeUseOf and receive instant access to 50+ PDF Guides like this one covering wide range of topics. Moreover, you will be able to download free Cheat Sheets, Free Giveaways and other cool things.

Home:	**http://www.makeuseof.com**
MakeUseOf Answers:	**http://www.makeuseof.com/answers**
PDF Guides:	**http://www.makeuseof.com/pages/**
Tech Deals:	**http://www.makeuseof.com/pages/hot-tech-deals**

Follow MakeUseOf:

RSS Feed:	**http://feedproxy.google.com/Makeuseof**
Newsletter:	**http://www.makeuseof.com/pages/subscribe-to-makeuseof-newsletter**
Facebook:	**http://www.facebook.com/makeuseof**
Twitter:	**http://www.twitter.com/Makeuseof**

Think you've got what it takes to write a manual for MakeUseOf.com? We're always willing to hear a pitch! Send your ideas to justinpot@makeuseof.com.

Download Other MakeUseOf PDF Guides!

http://makeuseof.com/pages