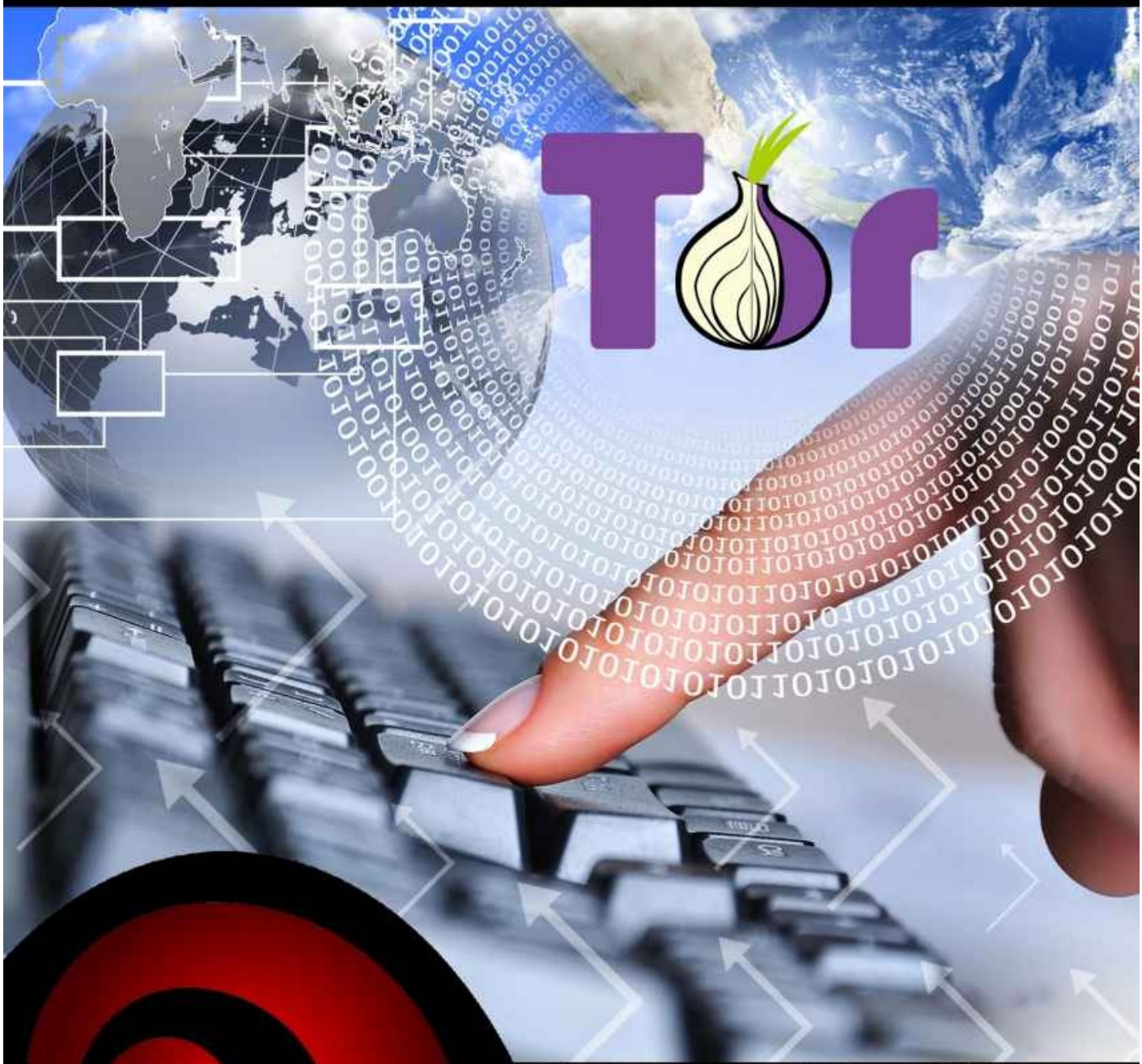
TOR BROWSER HANDBOOK

Quick Start Guide On How To Access The Deep Web, Hide Your IP Address and Ensure Internet Privacy

S.K. MASTERSON



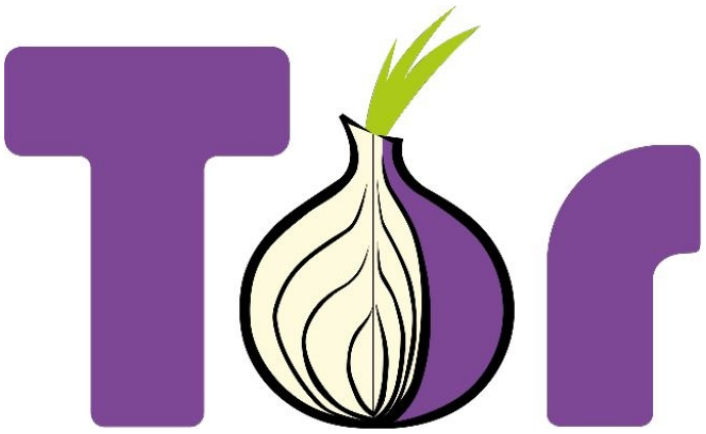
Includes a Tor Installation Guide for Linux & Windows + Over 50 Helpful Links

ADVANCED TECH GUIDES

Tor Browser Handbook:

Quick Start Guide On How To Access The Deep Web, Hide Your IP Address and Ensure Internet Privacy

(Includes a Tor Installation Guide for Linux & Windows + Over 50 Helpful Links)



Contents

Bonus

As a Thank You for downloading this book, you can find a Free Tor Tips & Links bonus report at torbrowserhandbook.com/bonus! It will provide condensed tips from this guide and clickable links in a handy pdf so you don’t have to disrupt your reading experience trying to write down or click links as you go through the book. I really appreciate your support and hope this book serves you well.

Introduction

The Internet can be a dangerous place. From hackers looking to make a quick buck at your expense to government agencies collecting information about you and your browsing habits to advertising networks that track your every move in an attempt to sell more products, there is no shortage of ways that your privacy is endangered every single time you go online.

The biggest problem with how the Internet operates as it relates to online privacy is the IP address. You will learn a lot more about IP addresses within this guide, but for now, understand that your IP address uniquely identifies you on the Internet and this address is available to any website you visit and can be traced back to you. In other words, your online activities can be tracked simply based on the IP address used to access the Internet.

Fortunately, protecting your IP address from prying eyes isn't that difficult once you understand the tools that are freely available and designed to keep your Web browsing activities completely anonymous. One of these tools is Tor – an encrypted network designed to keep your IP address and everything you do online safely tucked behind a layered system that is so robust even the NSA can't figure out what you're doing.

Whether you are concerned about Big Brother watching what you do, hackers stealing your personal information, or if you're just sick of advertisers displaying custom retargeting ads based on your browsing history, Tor is the answer. It is a free, open source tool designed specifically for people who value their online anonymity and using the information contained within this guide, you will be well equipped to carry the shield of privacy and anonymity wherever the Internet takes you.

In this guide, you will learn the answers to common questions about Tor such as:

- What is Tor, who created it, and why?
- Is Tor legal?
- What is the Deep Web and why should I access it?
- How do I set up Tor on my computer (Linux & Windows)?
- What can I do with Tor once it’s installed?
- How do I navigate the Deep Web?
- The important Do’s and Don’ts when Tor Browsing

This guide was written to teach everyone about the importance of Internet privacy and anonymity in an age where everything you do online is under a microscope. If you value your privacy, this book will teach you exactly how to protect yourself from the many threats that lurk within the massively valuable, yet dangerous, global network known as the Internet.

Each chapter is designed to address some of the specific questions you probably have in your quest to become an anonymous Internet user. Screenshots have been included as necessary to demonstrate the process of installing and using Tor. By the time you finish reading this guide, you will have joined the millions of others who value their online privacy and will never again need to worry about who could be watching your online activities or what they could be doing with the information they collect.

Online freedom comes in the form of anonymity and you now hold the key to unlocking that freedom for yourself.

Chapter 1: What is Tor?

The Tor Project was originally developed by the United States Naval Research Laboratory, along with a mathematician Paul Syverson and computer specialists Michael Reed and David Goldschlag in the 1990's as a way to protect sensitive intelligence communications. It was during this time that the core principle behind Tor–onion routing–was originally developed. This same technique, which protects users' anonymity by protecting online activity through a series of encrypted layers, is how Tor still works today.

It would be a few more years before the original version of Tor became available. Fast forward to 2002 when the alpha version of The Onion Router, or TOR, was released. Using the principles of onion routing developed in the 90's, a truly secure and anonymous way to browse the Internet had been born. It would still be another two years, however, before the Naval Research Laboratory would release the source code for the project under a free license. It was at this time that the Electronic Frontier Foundation (EFF) began funding the development of Tor although it would still be another couple of years (2006) before The Tor Project, a nonprofit organization responsible for maintaining Tor, would be born and Tor would become increasingly popular with anyone looking to keep their identity safe while browsing the Web.

In addition to EFF, other sponsors of The Tor Project have included Google, the University of Cambridge, Human Rights Watch, and the US International Broadcasting Bureau. Today, The Tor Project is based in Massachusetts as an education research organization and continues to maintain both the Tor Browser and the intricate global relay system that provides the layers of anonymity needed to safely browse the Internet in an age when surveillance by government agencies and private citizens is a growing concern for all Internet

users.

With the brief history lesson out of the way…what *exactly* is Tor? In its most basic form, The Tor Project is comprised of two parts: a browser client that allows users to connect to the Tor network and a global system of relays designed to anonymously bounce traffic from the Tor browser throughout the world before serving the requested content. When using a conventional Web browser, most Internet requests are easily intercepted. It is also easy to figure out where a particular user is located based on that individual's Internet Protocol (IP) address. Using Tor provides a secure way to browse the Internet without broadcasting the physical IP address of the device or any of the information being viewed during the session. The system works so well, in fact, that the National Security Agency (NSA) has been quoted as saying that Tor is "the king of high security, low latency Internet anonymity."

Interestingly enough, 80% of The Tor Projects current operating budget comes from sponsors within the United States Government including the US State Department, National Science Foundation, and Broadcasting Board of Governors. The remaining 20% comes from the Swedish government and thousands of individual sponsors.

Despite significant government sponsorship, a 2012 report leaked by ex-NSA contractor Edward Snowden reveals that the NSA has been unable to crack Tor as a network. In fact, when used in conjunction with other privacy tools, Tor makes it nearly impossible for the NSA or any other government agency to access the information viewed on the Tor network. It is one of the most powerful free anonymity tools available and with continued support, The Tor Project will continue to pave the way for Internet privacy and anonymity for years to come.

Chapter 2: How Do You Use Tor?

Tor is a service that helps you to protect your anonymity while using the Internet. Tor is comprised of two parts: software you can download that allows you to use the Internet anonymously, and the volunteer network of computers that makes it possible for that software to work.

Using Tor requires that a user download and install the Tor browser (freely available from The Tor Project website at https://torproject.org). Once properly installed and configured, the Tor browser connects to the Tor network using encryption techniques that protect the integrity of anything transmitted between the client machine and the Internet. The Tor browser is actually based on the popular Mozilla Firefox Web browser. In fact, users of Firefox should find interacting with the Tor browser client to be quite familiar.

Tor is not designed to erase the tracks left behind after Internet usage nor is it a 100% fail-safe way to protect one's identity while online. It is, however, a powerful tool designed to protect the integrity of data transportation so certain websites cannot trace back a Web session to a particular user–at least not without a lot of extra work.

Although the Deep Web is covered in detail in Chapter 11, it's important to realize that only about 5% of the Internet is available to users of traditional Web browsers like Internet Explorer, Google Chrome, and Mozilla Firefox. The rest of the Web, known as the Dark Web or Deep Web (though I'll provide a further distinction later on), can only be accessed using the Tor network and its hidden services feature. Without the Tor browser, it's as if these hidden websites do not exist at all. It's for this reason that The Tor Project has received bad press in the last several years as a hub for illicit drug sales, child pornography, and credit card fraud. That said, even the FBI has acknowledged the legitimate uses of Tor as a way to remain safe and

anonymous.

The Tor Project team claims that its users fall into four categories: regular people wanting to keep their Internet activities private from websites and advertisers, people concerned about cyberespionage, people avoiding censorship in various parts of the world, and military professionals. The U.S. Navy still relies heavily on the Tor network as do an assortment of activists and journalists in countries with strict media censorship policies.

Other legal users of Tor include law enforcement agencies seeking to mask their IP addresses while performing online undercover work, bloggers, IT professionals, and business executives. Some parents have even begun using Tor to protect their children’s location from potential criminals while browsing the Web. The legitimate uses of Tor are nearly endless but the same anonymity that makes all of these activities possible using Tor is the same reason why the Tor network has become home to so many black market online operations.

Despite the nefarious subculture that is readily accessible via Tor, the legitimate uses of the service should not be discounted by anyone concerned about online privacy in an age when government agencies and large corporations alike are determined to collect as much information about the general public as possible.

Chapter 3: How Does Tor Technically Work?

Tor allows Web traffic to be routed through several computers within the Tor network prior to reaching its destination. This means that the party on the other end cannot trace the traffic back to the physical IP address of the computer being used to access the information. The more Tor users there are, the more protection the onion routing protocol provides for users of the service.

The computers that handle the traffic between the Tor browser and the Internet are known as Tor Relays. There are actually three different types of relays that comprise the Tor network: end relays, middle relays, and bridges. Each of these relay types plays a pivotal role in the effectiveness of the Tor network as a privacy an anonymity tool.

End relays (sometimes also referred to as exit relays) are the final relay before the data transfer leaves the security of the Tor network and rejoins the public Internet. When a website attempts to track a user, the IP address the site sees is the IP address of the end relay being used for that particular request. After that, the trail runs cold which is why the Tor network works as well as it does. The problem with end relays is that it becomes possible for the operator of the end relay to be implicated in any illicit activity originating from that end relay. When illegal activity is detected, law enforcement and copyright holders usually target these end relays–it is a risk that not every Tor user is willing to take.

Middle relays are much safer because they only transfer data between other relays and clients within the Tor network. Anyone can setup a Tor middle relay from the comfort of home without having to worry about any of the data being sent through the relay or any illicit activity that may stem from the use of Tor.

A bridge is a Tor relay that isn’t publicly listed in an attempt to shield these relays from IP blockers. For instance, even though the data transmitted through the Tor network is anonymous and not easily tracked, it is very easy for others to establish that a particular person is using the Tor network when connecting to the public Tor network. To circumvent this, many Tor users operate a Tor bridge that shields the fact that Tor is being used at all.

Using Tor is free and no one is required to operate a Tor relay, but the more Tor relays that are available, the more secure the system becomes and the faster it operates. After using Tor for a while, you may decide to operate a Tor relay to assist the Tor community as its use continues to expand throughout the world.

To illustrate exactly how Tor works from end to end, consider the following example. A user opens the Tor browser client that connects to the Tor network using at least three relays. The connection between the Tor browser and the Tor network is encrypted as is every hop between relays. Finally, the transmitted data reaches the end relay where the request is decrypted and sent through the public Internet to its final destination.

There are few limitations to the Tor network, but it’s worth pointing out performance-related issues. New Tor users are especially confused by how slow the browser seems to run sometimes. The reason this occurs is two-fold. First, as part of the Tor protocol, all data must be routed through a minimum of three relays along the way and these relays could be located anywhere in the world. Second, the speed of the Tor network is dependent upon how many relays are active at the time and the overall traffic being handled by the network at a given moment. While there are times when Tor is as fast as any other browser, there are times when it is noticeably slower; especially when working with large data transfers such as audio and video files. Unfortunately, the slightly slower speeds associated with using Tor are

the price users must endure to remain anonymous while surfing the Web. This occasional sacrifice is most certainly worth the benefit received by using Tor.

Chapter 4: Tor Legal FAQ

Please note that this FAQ is for information purposes ONLY and should not be treated as legal advice. If you have any concerns about using Tor that are not covered below, please consult an attorney licensed in your jurisdiction.

General Information

Can I be prosecuted or sued for running Tor?

NO. At this time, there have been no reports of anyone living in the United States being prosecuted or sued for using Tor or running a Tor relay. Also, running a Tor relay (even an exit relay) is currently legal under U.S. law.

Should Tor be used for illegal purposes?

NO. Tor was developed as a way for people to communicate with privacy and anonymity. The Tor Project does not condone the use of Tor or Tor relays for illicit activities.

Can The Tor Project or EFF promise that I won’t get in trouble for operating a Tor relay?

NO. Laws change all the time as to the technologies those laws are based on and Tor is no exception to this rule. Neither Tor nor EFF can guarantee that you will never face legal liability by running a Tor relay.

Will EFF represent me if found legally liable for running a Tor relay?

MAYBE. EFF does not promise legal representation for relay operators but has stated that it will assist relay operators when assessing the situation and may even help to locate qualified legal counsel when deemed necessary.

Can I contact Tor developers with legal questions or if I suspect Tor is being used for illicit purposes?

NO. Tor developers are only available to answer technical questions about using the Tor network and browser. They are not qualified to provide legal advice. Also, keep in mind that communication with Tor developers is not protected by legal privilege. Law enforcement could subpoena and obtain any information shared with Tor developers. If faced with a specific legal issue, please contact info@eff.org. EFF cannot guarantee assistance but will make every attempt to help Tor users and relay operators with legal questions.

Are there any promises made by Tor developers about the reliability and trustworthiness of Tor relays within the directory?

NO. Tor developers attempt to verify that all listed relays are stable and provide adequate bandwidth but are unable to guarantee the trustworthiness or reliability of relay operators. The developers also reserve the right to refuse a relay to any operator and to remove relays from the directory for any reason.

Exit Relays

As mentioned in Chapter Three, running an exit relay means that any traffic coming from that relay can be traced back to the operator's IP address. Although running an exit relay is legal in the United States, when exit relays are used for illegal purposes (a statistical likelihood) it can draw the attention of law enforcement and/or private litigants.

You can learn more about the risks associated with running an exit relay as well as some recommended best practices by reading through

The Tor Project's blog.

Should an exit relay be run from my home?

NO. Law enforcement could seize your computer if the traffic coming from your exit relay is deemed illegal. Exit relays should not be run from a residence or using a home Internet connection. A better option is to operate an exit relay from a commercial facility. The relay should have a separate IP address and no other traffic should be routed through it. Avoid keeping personal data on the host computer and do not use the relay for illegal purposes.

Should my ISP be informed before running an exit relay?

YES. Let as many people as possible know that you are running an exit relay. The more people who are aware, the faster government officials will be able to determine that your IP address is part of the Tor network. This could prevent your computer from be seized by law enforcement.

The Tor Project also suggests:

- Create a reverse DNS name for the IP address that indicates the computer us being used as an exit relay.
- Set up a notice that explains you are running an exit relay
- Get ARIN registration for the exit relay with your contact information. This makes it so abuse complaints will come to you instead of the ISP.

Should I look at the plaintext traffic that exits my end relay?

NO. Even if you are capable of modifying the Tor source code to monitor and log plaintext coming from your relay, you could create civil

and/or criminal liability for yourself under both federal and state wiretap laws. Never examine any communications traveling through the exit node without first speaking with a qualified lawyer.

What should I do if I receive a subpoena or information request from law enforcement?

Start by educating the requestor about Tor. A properly configured Tor relay does not have any useful information for inquiring parties. If you do maintain logs, do not disclose this information to any third party (including law enforcement) without first talking with a lawyer so as not to violate the Electronic Communications Privacy Act.

What should I do if I receive a DMCA notice from my ISP?

The EFF provides a template that can be used when responding to a DMCA notice from the ISP. Keep in mind that this template only addresses copyright infringement complaints through a Tor node. Although it has not been addressed by a court yet, the EFF believes that relay operators are protected from copyright liability due to an immunity defense under DMCA and copyright's secondary liability doctrines. In other words, there is some uncertainty about if and how a court will rule on this matter. Following the suggestions listed on The Tor Project blog pertaining to setting up an exit relay helps to mitigate any liability you have as a Tor relay operator.

Chapter 5: Overview (What Tor Is and Is Not)

Although some of this information in this chapter may seem redundant, it is important to understand exactly what Tor is and is not before using this powerful anonymity tool. Basically, Tor is a service that helps protect a user's anonymity by hiding the user's IP address behind the volunteer network of computers that make up the Tor network.

When a user data transmission finally exits the Tor network via an exit relay (which can be anywhere in the world), the resulting IP address is that of the exit relay–not the Tor user.

Tor is useful for many legitimate purposes including preventing websites from tracking you and your browsing habits, accessing websites that are blocked in a particular country, and maintaining anonymity when communicating about sensitive information (i.e. whistleblowers who wish to remain anonymous).

For some, it may be helpful to think of Tor like a Hollywood car chase. In order to throw off the chase vehicle, it may be necessary to take a hard-to-follow route full of twists and turns rather than taking a direct route to the destination. Similarly, data sent across the Tor network take a random path through at least three Tor relays. This means that an observer at any single point along the network can determine where the data packets came from or where they are going.

The Tor network was designed to encrypt the data between each relay. Unlike standard TCP/IP packet headers–which indicate the origin and final destination of every packet sent–Tor headers only contain information about the next hop. This prevents traffic analysis by advertising networks and hackers.

With the shutdown of popular Tor destinations such as the Silk Road,

the anonymity network has received a lot of press (some good and a lot bad). It's important to consider the following seven facts about Tor that remain true regardless of what the media may portray about the Tor network.

1. *Tor Still Functions as Intended*

Despite rumors to the contrary, the NSA is still unable to circumvent the anonymity provided by using the Tor network. This was proven by leaked NSA documents in which the NSA claims that although it has had some luck compromising the identities of some Tor users in specific situations, it is still unable to track users "on demand."

2. *Tor Has Many Legitimate Uses*

Unfortunately, a common misconception about the Tor network is that it is only used by criminals and pedophiles. From activists to journalists to military professionals to whistleblowers, there are countless legitimate reasons to use Tor–none of which have anything to do with accessing illegal or illicit content.

3. *Tor Doesn't Have a Backdoor*

Another common misconception about Tor is that many people assume that since Tor was originally developed by the military it probably has a backdoor that the military can use to access the Tor network. Since Tor's introduction, it has been evaluated by several cryptographers who have confirmed that there isn't a backdoor. In fact, since Tor is an open source project, anyone can view the source code that makes up the Tor browser and the Tor network.

4. *It Is Not Illegal to Run a Tor Relay in the United States*

At the time of this writing, no one living in the US has been prosecuted or sued for operating a Tor relay. Although there has not yet been a legal precedent set as it relates to Tor, EFF stands by the fact that operating a Tor relay is not illegal.

5. *Tor is Easy to Use*

While it’s true that many privacy and security tools can be difficult to use for the uninitiated, Tor is extremely easy to use. The Tor browser bundle is the easiest way to get started using the Tor network as it comes pre-configured to use Tor in a secure manner. Another option is to use the Tails operating system. This live OS (runs from a DVD or flash drive) routes the entire Internet connection through Tor and removes all traces of the session upon being shut down.

6. *Tor is Faster than Most People Think*

Believe it or not, the Tor network is faster now than it has ever been in the past. Routing data transmissions through the Tor network does take slightly longer than traditional Web browsing but the Tor developers have been working diligently to maintain the speed of the network. The more Tor relays that become available, the faster the network operates.

7. *Tor is Not a Foolproof Solution*

Using Tor is an excellent way to protect your identity and browsing habits while using the Internet but it is not a perfect system and also depends on the activity of the user while online. Anonymity can be destroyed in an instant even while using Tor if it is used incorrectly or not properly configured. For this reason, use either the Tor browser bundle or Tails to ensure proper configuration.

Chapter 6: Tor vs. VPN – The Important Differences

Some similarities between using Tor and using a Virtual Private Network (VPN) do exist; however, the two technologies are completely different and should not be interchanged haphazardly when it comes to Internet privacy and anonymity. A VPN may be a better choice for some online activities while Tor is the better choice for other activities.

To understand the strengths and weaknesses of each, it's important to have at least a basic understanding of both technologies.

VPNs

A VPN connection is encrypted and passed through a server (or series of servers) before reaching its final destination. The encryption of the traffic to and from the computer cannot be viewed by anyone; including the ISP. For this reason, using a VPN when connecting to public Wi-Fi services prevents hackers from seeing what you are actually doing online.

VPNs also allow for circumventing of locational restrictions. For example, if you are visiting a foreign country and want to watch Netflix, you may find that the Netflix servers restrict access to your account while trying to watch shows or movies overseas. Using a VPN with server located in the US would trick Netflix into thinking you are actually viewing content from within the US. Using a VPN with a server located other than your physical location also prevents websites from knowing where you are located while accessing content.

The catch when using a VPN is that the VPN operator can see everything done while connected to the VPN service. While many VPN services claim not to maintain logs of user activity, it has been proven that many of them actually do keep logs that are promptly turned over

to the authorities in the face of a court order. VPNs are an excellent choice for low risk situations but they do not provide the same level of anonymity provided by Tor.

VPNs should be used in low risk situations and in situations where large amounts of bandwidth are required. Torrenting, for example, should be done using a VPN because it is much faster than using Tor. Furthermore, torrenting and other high bandwidth activities hurt the entire Tor network by consuming excessive bandwidth.

Tor

When using Tor, the connection is encrypted before being sent to through three or more Tor relays. When the connection reaches the exit relay, the data is decrypted and sent to the destination. It is true that the first relay in the Tor network can see your physical location but the second and third relays do not know where the data originated. This is how the Tor network provides anonymity.

Also, like a VPN, using Tor protects middle men (such as the ISP) from monitoring Internet traffic to and from the computer. Perhaps the only downside to using Tor is that if the exit relay has a malicious operator, that individual could decrypt and view all traffic leaving the exit relay. The way to get around this caveat is to ensure all connections are made using HTTPS. Browser add-ons such as HTTPS-Everywhere can be used to encrypt all data transmissions so that even a malicious exit relay cannot view the data being sent through the Tor network.

Tor should be used when anonymity is of the utmost importance and the activity does not require excessive amounts of bandwidth. Tor should also be used for casual browsing activities. Not only does using Tor during browsing prevent advertising networks from learning your location, it also provides diversity to the Tor network.

For even more anonymity while surfing the Web, some people have

begun using Tor and a VPN together. By combining both technologies, it is possible to further protect your online identity when properly configured. For most users, however, using both systems together is overkill, but it is a viable option for those concerned that neither technology provides enough layers of anonymity alone.

Chapter 7: What is My IP Address and How Do I Hide It?

As you've probably noticed, the primary service provided by Tor is the masking of a person's real IP address. But what is an IP address? And how exactly does Tor hide a computer's true IP address from the Internet?

An Internet Protocol address is the system by which all electronic devices connected to a network (whether a local network or the Internet) are identified as unique. Think of an IP address as the mailing address of a particular machine.

All IP addresses contain four sets of numbers each separated by a single dot. Each set of numbers contains one to three digits. The sets of four numbers range from 0 to 255. For example, an IP address might be 72.129.1.274 or 192.168.1.254. The point is that the IP address provided to a particular computer can be used to determine the location of that machine and in some cases can even provide personally identifiable information about the person using that IP address.

IP addresses can be static or dynamic. A static IP never changes and can be used to determine the location of the computer and the ISP being used. Dynamic IP addresses, on the other hand, are temporarily assigned to a computer when it tries to access the Internet. Usually, an ISP will assign a dynamic IP to subscribers every time these subscribers attempt to go online. While a dynamic IP address may not immediately be associated with a particular individual or machine, the ISP keeps records of what dynamic IP addresses are issued to what machines meaning that even when using a dynamic IP address, it is possible for people to figure out who was using a particular IP address at a specific time.

Hiding Your IP Address

Since the IP address is what provides websites with the very information that destroys your anonymity on the Web, hiding the real IP address of your computer should be your number one priority when sending data across the public Internet.

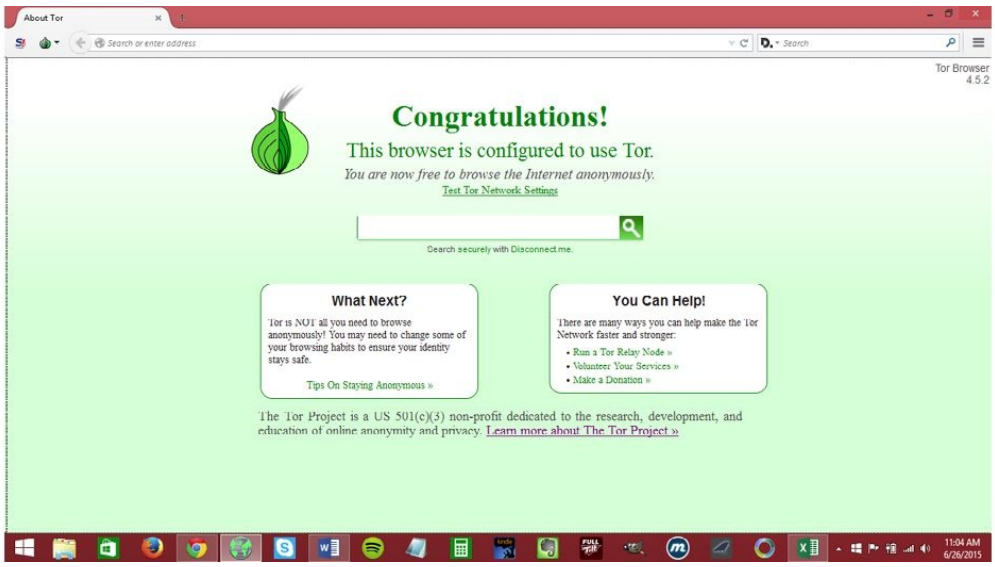
There are three common ways to hide your true IP address online. The first is the use of a trusted proxy server. A proxy is a service you connect to before making any other Web-based connections. This way all Internet traffic is routed from your computer to the proxy server before reaching its destination. Websites see the IP address of the proxy server instead of the IP address of your computer.

Second, a VPN can be used to mask your true IP address. As discussed in the previous chapter, a VPN creates an encrypted connection between the VPN server and your computer and exits via the VPN server. Like using a proxy server, websites you visit see the IP address of the VPN server instead of your real IP address with the added benefit of an added encryption layer.

Finally, use Tor to hide your IP address! Tor also encrypts data connections between your computer and its final destination while bouncing the transmission between various relays so it is impossible to see where the traffic originated. The whole idea behind The Tor Project is to protect your IP address from prying eyes while providing a level of online anonymity that is difficult to match using any other single technology.

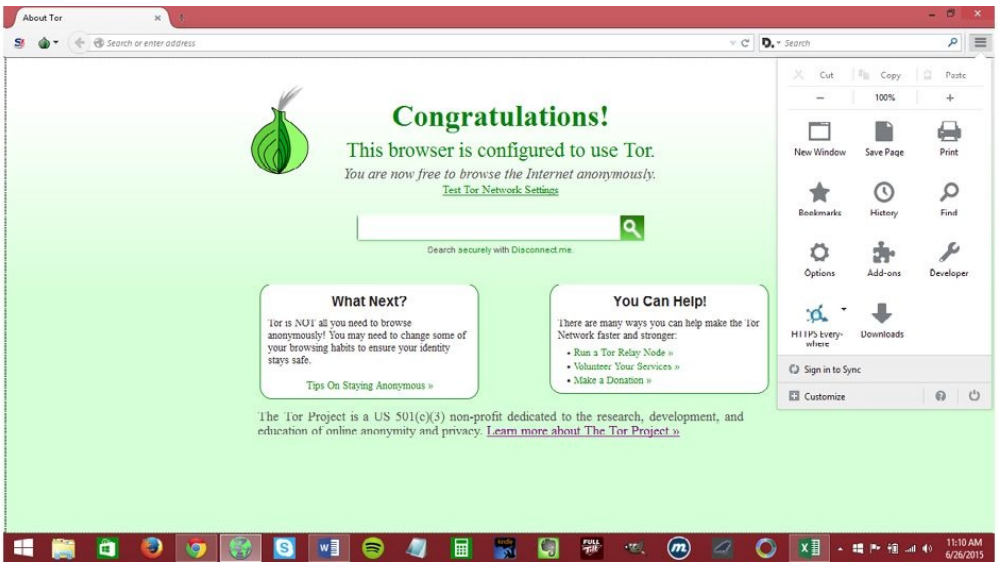
Chapter 8: Getting Started with the Tor Browser Bundle

The Tor Browser Bundle is a self-extracting package containing a special version of the Firefox browser designed specifically to work with the Tor network. Once the browser bundle has been extracted, double click on the ‘Start Tor Browser’ icon to launch the application. A connection window automates the process of connecting to relays in the Tor network. Once this connection loads, the special version of Firefox opens and you can start browsing anonymously through the Tor network.

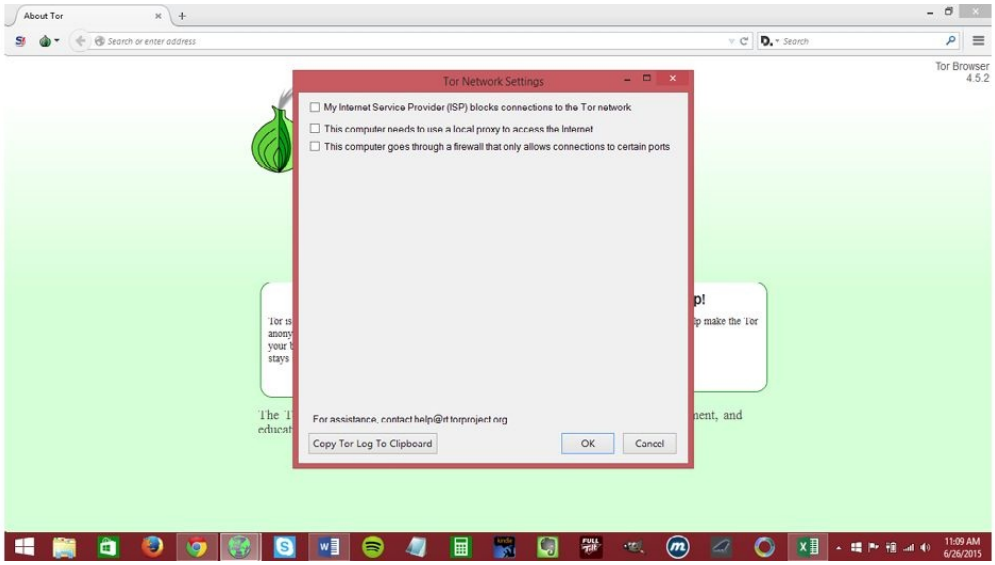


As you can see from the screenshot above, the Tor browser is setup just like Firefox with a different splash screen. Users already familiar with using Firefox will have no trouble adapting to the Tor Browser Bundle.

As you can see in the screenshot below, the options and settings available in Tor mimic those found in Firefox.

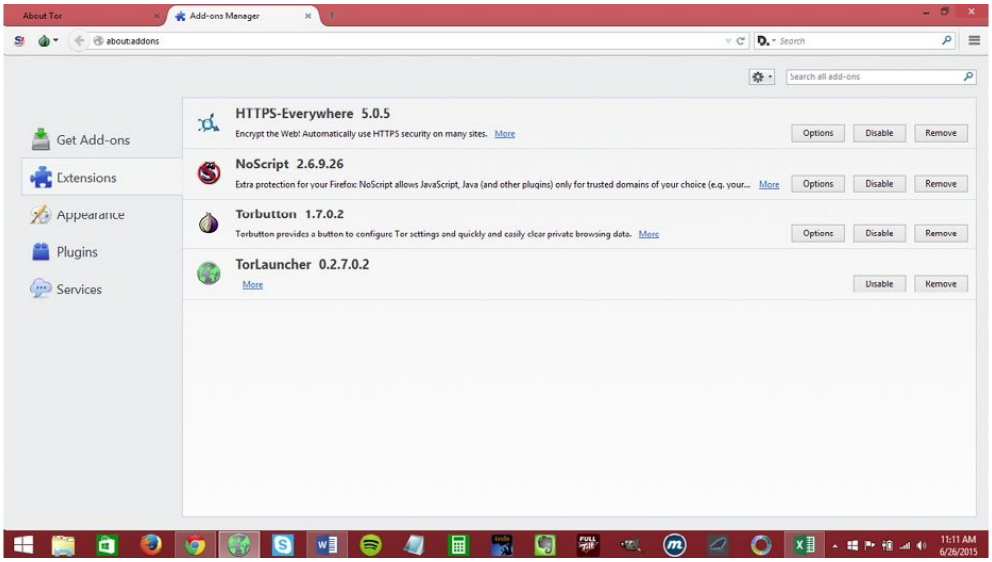


Unlike Firefox, however, the navigation bar contains options and settings that are specific to Tor. This makes it much easier to adjust Tor settings for optimal performance and anonymity in a variety of situations. This icon also makes it extremely easy to wipe all Web browsing data from the history after completing a Tor session. The image below shows what some of these options look like.



Just like Firefox, add-ons can be installed to work with the Tor browser for improved functionality. Some of the add-ons that come already installed in the latest release of the Tor Browser Bundle include NoScript and HTTPS-Everywhere. Both of these useful add-ons help to maintain your anonymity while browsing through the Tor network

and will be discussed in more detail in Chapter 12.



The latest stable Tor browser release is 4.5.2 and it offers numerous improvements over the previous version including a patch for the Logjam attack and updates to numerous Tor components.

The complete change log includes:

- All Platforms

o Update Tor to 0.2.6.9

o Update OpenSSL to 1.0.1n

o Update HTTPS-Everywhere to 5.0.5

o Update NoScript to 2.6.9.26

o Update Torbutton to 1.9.2.6

§ Bug 15984: Disabling Torbutton breaks the Add-ons Manager

§ Bug 14429: Make sure the automatic resizing is disabled

§ Translation updates

o Bug 16130: Defend against logjam attack

o Bug 15984: Disabling Torbutton breaks the Add-ons Manager

- Linux

o Bug 16026: Fix crash in GStreamer

o Bug 16083: Update comment in start-tor-browser

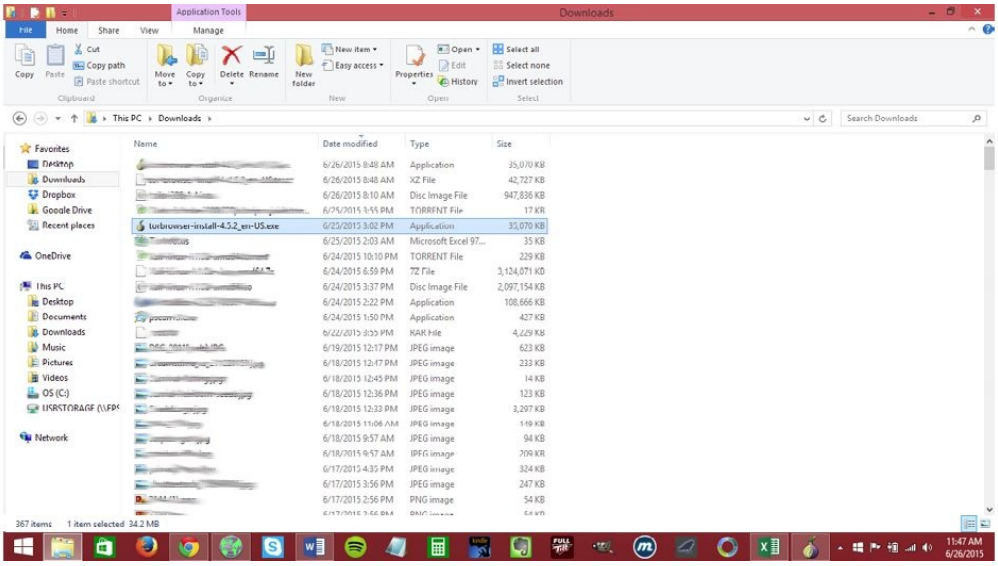
Once the Tor Browser Bundle has been installed, a message appears asking if you would like to connect or configure the browser. For most people, selecting ‘Connect’ is sufficient but the connection should be configured if the connection is filtered, censored, or proxied.

In cases where the network has firewalls that prohibit access to Tor, the Tor Browser Bundle can also be downloaded through Gmail. Send an email to gettor@gettor.torproject.org and write the word “help” in the body of the email. You will receive step-by-step instructions to download and install Tor in these circumstances.

Chapter 9: Installing Tor – Windows

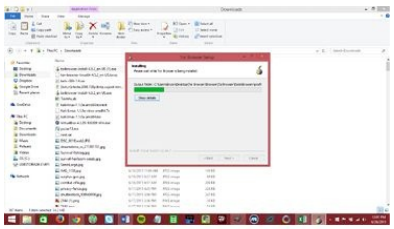
To install Tor on Windows machines, you will need a Windows computer (XP, Vista, 7, 8) and an active Internet connection. Start by opening a browser window and navigating to https://www.torproject.org/projects/torbrowser.html.en. Once the page has loaded, look for the large purple download button. Click this button to download the appropriate file for the version of Windows you are currently running. If you prefer to manually choose the installer file you can scroll down to the Tor Browser Downloads section and choose a different installer file.

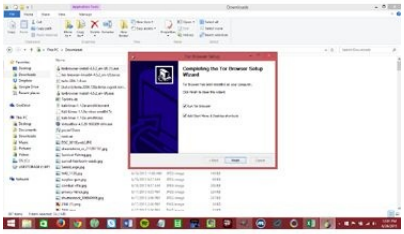
Once the download is complete, find the downloaded file (the default location should be the *Downloads* folder). Double click on the installation file. It should be named torbrowser-install-4.5.2_en-US.exe. After clicking on the file, a window will open with a warning about running the software. As long as you downloaded Tor from The Tor Project's secure site, click Run to start the installation process.



Next, a small window will open prompting you to select a language. Choose the appropriate language and click the OK button. A new window will appear asking where to install the Tor Browser Bundle.

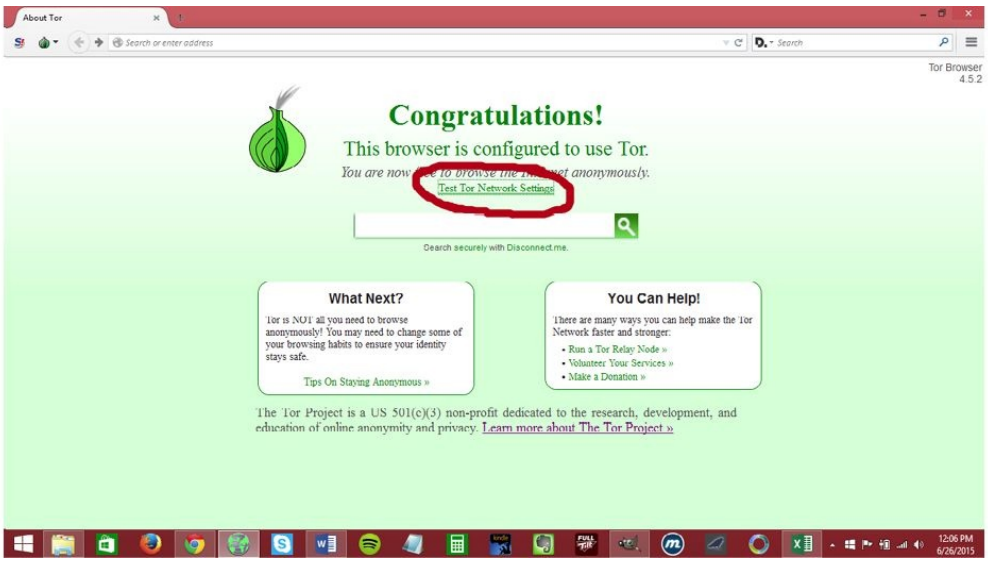
The default location is the PC desktop. This is fine in most cases but you can change the installation to a different location if you choose. Click Install and allow the installation to complete.





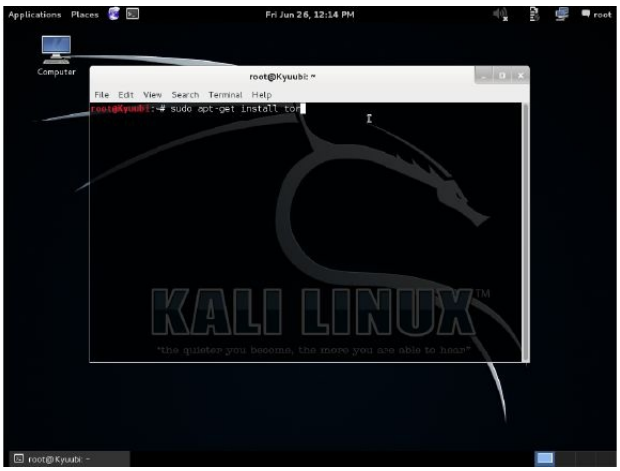
Once installation is complete, you have the option of running the Tor browser before clicking Finish. The browser will open after connecting to the Tor network and the process is complete. You can now safely browse the Internet using the Tor network.

To ensure the Tor network has been properly configured, test the network settings before beginning a browsing session. This can be accomplished by clicking on the link at the top of the Tor homepage as shown in the screenshot below.


About Tor
Search or enter address
Search
Tor Browser
4.5.2
Congratulations!
This browser is configured to use Tor.
You are now able to browse the Internet anonymously.
Test Tor Network Settings
Search securely with Disconnect.me.
What Next?
Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.
Tips On Staying Anonymous »
You Can Help!
There are many ways you can help make the Tor Network faster and stronger:
• Run a Tor Relay Node »
• Volunteer Your Services »
• Make a Donation »
The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »
12:06 PM
6/26/2015

Chapter 10: Installing Tor – Linux

Depending on the type of Linux distribution being used, the instructions for installing Tor and/or the Tor Browser Bundle may differ. Debian and Ubuntu systems are the easiest when it comes to installing Tor. In most cases, the command “sudo apt-get install tor” is all that is required to install Tor on a Debian-based distro as seen in the screenshot below.



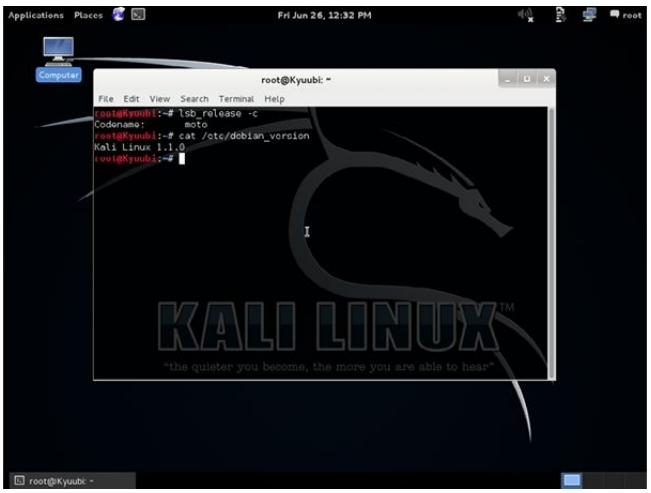
While this is certainly the easiest way to install Tor, the latest version of Tor may not be in the repository at the time of installation. This is especially true of the Ubuntu repos. To ensure you install the latest version of Tor, add the following repositories to the /etc/apt/sources.list file:

deb http://deb.torproject.org/torproject.org utopic main

deb-src http://deb.torproject.org/torproject.org utopic main

Notice that these repositories contain Tor for Ubuntu Utopic Unicorn. You will need to change the name to the version of Linux being used. If you unsure what version of Linux you are running, use the following command:

lsb_release –c or cat /etc/debian_version



Next, add the gpg key used to sign the packages by running these commands in the terminal:

gpg —keyserver keys.gnupg.net —recv 886DDD89

gpg —export A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89 | sudo apt-key add –

The latest version of Tor can now be installed by running the following:

$ apt-get update

$ apt-get install tor deb.torproject.org-keyring

If using another version of Linux, the installation method is slightly different. First, navigate to The Tor Project's Download page and download the appropriate package. Next, make sure libevent is installed and ensure the openssl and zlib are present.

Now, run the following commands to build Tor:

tar xzf tor-0.2.6.9.tar.gz; cd tor-0.2.6.9

./configure && make

Tor can now be run as *src/or/tor* or you can run *make install* as root to install Tor into /usr/local/. This way Tor can be started just by running tor in the terminal.

Like a Tor installation on Windows, the Tor Browser comes pre-configured to work with Tor and includes browser patches for improved anonymity while surfing the Internet. However, for users wanting to use

SOCKS directly (instant messaging, IRC, Jabber, etc.), the application can be pointed directly at Tor on localhost port 9050 (or port 9150 for Tor Browser). You can find more information about using other applications with Tor by checking out the Torify HOWTO.

Chapter 11: How to Access the Deep Web

The deep web gets its name because of its massive size. The public Internet, accessible via search engines like Google and Bing, only accounts for a small fraction of the total Internet puzzle. Everything else is part of the deep web. The deep web is completely anonymous– in fact, you cannot even access the deep web unless you are also anonymous. This is why the Tor browser is used to access these otherwise unseen parts of the Web.

It's worth pointing out that there seems to be some confusion about the difference between the deep web and the dark web. Mainstream media often portrays these two words as interchangeable when, in fact, they are not. The deep web refers to everything that is not accessible via the surface Internet (i.e. searching Google). The dark web, also known as dark net, is merely a small subset of the deep web and it refers to computers and networks that are not accessible at all without being invited into these groups. In other words, the dark web is still inaccessible via Tor unless you are invited to join a network that is a part of this elusive deep web component.

Once Tor is properly configured, accessing the deep web is simply a matter of running the browser and typing in domain names like you would with any other browser. The difference is that deep web addresses that are part of the hidden Tor services network end with an .onion address (instead of .com, .org, .net, etc.).

The deep web has gotten its share of bad press in recent years. Deep web sites like the Silk Road Marketplace (where people could buy drugs in exchange for Bitcoins) have given the deep web a bad reputation as a place full of societal deviants, hackers, and assorted criminal types. While these people and services do exist as a part of

the deep web, there are also many interesting things on the deep web that are not illegal, but would never be found on the public Internet.

Since you can't use Google or other popular search engines when accessing the deep web via Tor, you need to learn how to navigate throughout the deep web. The easiest way to start finding interesting sites that can only be accessed via the deep web is to check out thehiddenwiki.org. This site is an anonymously maintained directory of .onion sites that can be viewed when using the Tor browser. The Hidden Wiki and other .onion directories are covered in more detail in Chapter Fourteen but suffice it to say that this is one of the best resources available for people first starting out on an expedition into the world of the deep web.

Reddit is another excellent resource that is full of deep web destinations and users willing to help new deep web explorers find what they are looking for. Chances are that someone has already asked a question similar to anything you might think of so always search Reddit before posting a question. That said, many people will be happy to help you find the exact content and services you are looking for no matter how off the wall your request may seem.

While there is certainly no shortage of illicit activity happening on the deep web right now, do not be discouraged by claims that everyone accessing the deep web is a criminal. As mentioned time and again throughout this guide, there are many legitimate uses for accessing the deep web and only a portion of those uses have anything to do with illegal activity. The deep web is how the Internet should have been before it was regulated by governments and censorship agencies around the world. Enjoy your new found freedom as you explore the vast expanses of digital content and services known as the deep web.

Chapter 12: Do’s and Don’ts – Safe Browsing with Tor

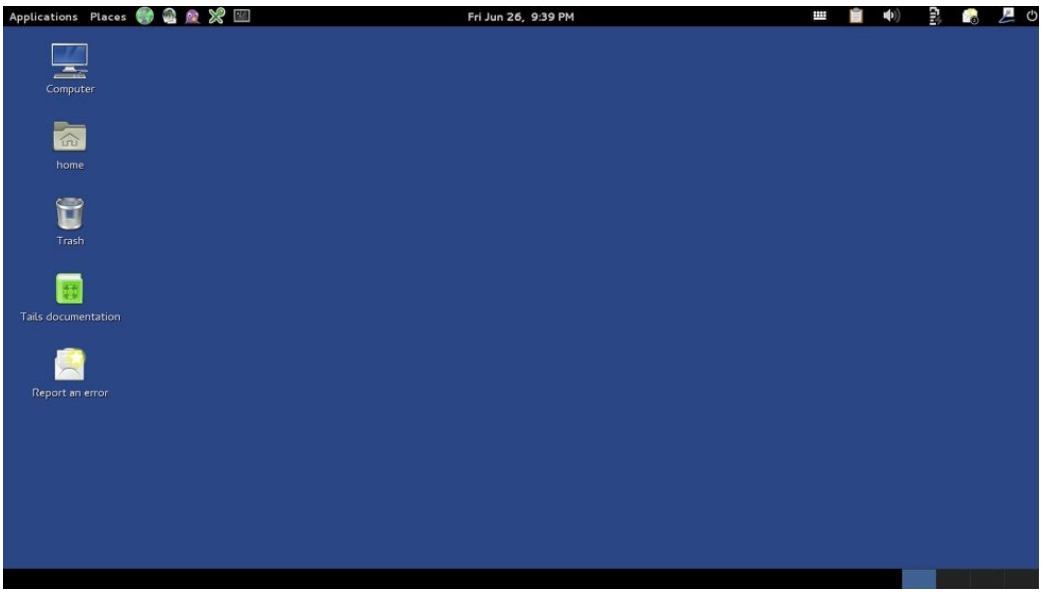
The best way to think about Tor as a privacy tool is to compare it to an umbrella. An umbrella only protects you from the rain if you have it with you and it is used as intended. Similarly, Tor only works as a privacy and security tool when it is used as intended. Furthermore, there are a few thing you must keep in mind when using Tor to ensure the maximum anonymity protection that this powerful service can offer when used as designed.

1. **Use Tor**

Whether you are looking for content or services that aren’t included in the normally accessible Web or you simply value the privacy and anonymity afforded by the Tor network, use Tor! Using Tor as often as possible keeps your identity safe while online and it also helps to diversify the traffic on the Tor network. If everyone only used Tor for illicit activities, it could be reasonably assumed that every Tor users should be investigated. By using Tor for mundane tasks and normal browsing activity, it helps to further protect the anonymity of everyone using the network–no matter what they are doing while online.

2. **Ditch Windows**

Windows is a popular operating system and the Tor Browser Bundle works very well on the Windows OS. However, the problem with Windows is that there are so many security vulnerabilities that your privacy could be compromised on a Windows machine even when actively connected to the Tor network. A better choice would be to use a Linux-based system or a Live OS made for privacy such as Tails.



Tails OS

3. **Perform Regular Updates**

The Tor browser still runs on top of whatever operating system you are using. This mean that Tor is only as secure and safe as the system running the browser client. The Tor client, any Tor-secured applications, and the operating system of the machine should all be updated regularly. Check for updates at least once a week (every day is even better) to ensure your system is always working as it should and is not vulnerable to security exploits that may have just recently been discovered.

4. **Don’t Use HTTP**

As previously mentioned, the Tor network only encrypts traffic as it moves through the intricate relay system that makes onion routing work in the first place. This means that a malicious exit relay operator could view any data sent or received by your machine that isn’t encrypted using SSL. Normal HTTP sites are not secured with encryption for your protection.

HTTPS-Everywhere is an add-on for the Tor browser that forces every communication between your machine and a server to be encrypted

using SSL standard encryption methods. This means that even if a Tor relay operator is snooping the traffic coming through the relay, that individual will not be able to view any of the data sent or received by your Tor-enabled browsing session.

5. **Encrypt Data Storage**

It's important to remember that Tor is only useful for anonymizing the original location of any Internet traffic you send out. Tor does nothing to protect the data already on your computer and the only real way to ensure the integrity of this data is to use strong encryption standards. LUKS and TrueCrypt are both examples of high-quality encryption programs that can ensure the safety of your sensitive personal data even if someone were to remotely access your machine.

6. **Tor Browser Bundle is Not Your Only Choice**

Although this guide recommends the Tor Browser Bundle for people just getting started in the world of anonymous surfing and the deep web, the Browser Bundle isn't the only, or even the best, way to leverage the power of Tor. The FBI's recent takedown of Freedom Hosting was only possible due to vulnerabilities within the Tor Browser Bundle. A better option is to install Tor and use it to protect the communications of other browsers compatible with the Tor network.

7. **Disable JavaScript, Java, and Flash**

If you are using the Tor Browser Bundle, these features should already be disabled by default. Also, add-ons such as NoScript prevent active code from running in the background of a particular webpage to provide another level of anonymity while browsing with the Tor network.

JavaScript, in particular, is a powerful scripting language that can be used to track you in ways that cannot be protected by the Tor network. Java and Flash both run in virtual machines within your physical computer meaning that they could ignore the proxy settings that tell

them to use Tor; essentially passing your information along to the website as if you weren't using Tor at all.

8. **No Filesharing or Torrent P2P**

Peer-to-peer file sharing or torrent downloads should not be used in Tor for two reasons. First, Tor is not designed to handle the additional load placed on the network by large bandwidth applications such as BitTorrent clients. It slows down the network significantly for other users and many exit relays actually block file sharing traffic anyway. Also, and more importantly, many torrent downloading clients send your real IP address directly to trackers and other peers. This compromises your anonymity even though you are using the Tor network to connect. It's worth restating — protect your privacy and anonymity and stay away from P2P!

9. **Delete Cookies and Local Data**

Even though Tor uses an elaborate system of encryption and relays to protect your identity while using the Internet, there are other tricks that can be used by websites to gather personal information about you and your browsing habits. Cookies and local data storage are two of the ways that websites can track you even when using Tor. Cookies and site local data must always be removed to ensure privacy while using the Tor network. We won't cover that in detail as it is assumed that if you're reading this book you know how to delete cookies and browsing history from your browsers. There are some more advanced options to help you though if needed, like add-ons available such as Self-Destructing Cookies that automatically delete cookies from the machine. Alternatively, you can use an OS like Tails that automatically deletes all session data when the OS is closed.

10. **Don't Use Your Real Email**

To be truly anonymous online, you need to create a separate identity that you can use when accessing the Tor network. It's impossible to

hide your real identity if you are giving out personally identifiable information such as your real email address. Basic private browsing is relatively simple, but as soon as you put any kind of footprint back out on the web—email, username registration, account setup, etc. think about how that may be linked back to you in any way. Consider creating an alternative email address that is not associated with your real identity at all to use when accessing sites through the Tor network.

11. **Ditch Google**

While Google is a popular search engine to use when combing through the surface web, it is a bad idea when using Tor. Google collects tons of information about users' browsing and search data that it uses to increase advertising revenue.

When searching for information via Tor, stick with search engines that do not log your IP address or store cookies on your computer. Good search engines to use in Tor include Startpage and DuckDuckGo.

While these are only a few of the many things you can do to increase your anonymity online, it is a good place to start and will allow you to avoid many of the mistakes made by novice Tor users.

Chapter 13: Top Tor Links and Resources

The first time you enter the deep web it may seem rather daunting. Where do you go? What do you do once you get there? The truth is that you can do pretty much anything on the deep web–many of these activities simply aren't available on the surface Internet. Some of these services are illegal; others are perfectly legal. In this chapter, you will learn about some of the top links that can be found on the deep web by using the Tor browser.

Using just one of the many hidden directory listings accessible via the Tor network, you quickly begin to see just how much of the Internet is out there that you've probably never seen before. Below you will find a breakdown that includes much of the information and services available on the deep web.

Search Engines

There are quite a few search engines that work well with Tor. Unfortunately, using Google, Bing, or other popular search engines is problematic when using the Tor network. First, these search engines are unable to index .onion pages so you probably won't find what you are looking for. Second, these search engines collect all kinds of data about you when using their services. Even if protected by the Tor network, it's possible that Google and others could collect personally identifiable information about you while using their search tools. Better choices when using Tor include:

- TORCH – http://xmh57jrzrnw6insl.onion/
- The Abyss – http://nstmo7lvh4l32epo.onion/
- DuckDuckGo – http://3g2upl4pq6kufc4m.onion/

General Things to Check Out

When you hit the deep web for the first time, be sure to check out these resources. You will learn valuable information about leveraging the power of the deep web and gain practice using this powerful anonymity network to your advantage.

- Tor WebDesign Guidelines – (provides information about starting your own hidden service) http://wf4df37hrebhwzts.onion/
- Welcome. We've Been Expecting You – (links to encryption guides) http://p3lr4cdm3pv4plyj.onion/
- OnionWiki – (general wiki about the technical side of Tor) http://ah5dm66duazqkz6h.onion/w/index.php/Main_Page

Marketplace

The marketplace is where people and businesses create hidden services that are only accessible via the Tor network. Everything listed in this section is accessible via Tor but in an effort to discourage using Tor for illegal purposes, links to questionable services have been intentionally omitted from this guide, but can of course be easily found.

Financial Services

Currencies (both legal and illegal), money markets, exchangers, and clearing houses are all available here.

- EasyCoin – Bitcoin wallet with free Bitcoin mixer http://easycoinsayj7p5l.onion/
- WeBuyBitcoins – Sell Bitcoins for cash http://jzn5w5pac26sqef4.onion/
- USD Counterfeits – Sells counterfeit US currency at 50% of face value
- OnionWallet – Anonymous Bitcoin wallet

http://ow24et3tetp6tvmk.onion/

Commercial Services

- Onion Identity Services – Passports and ID cards for sale http://abbujjh5vqtq77wg.onion/
- Rent-A-Hacker – For hire hacking services http://2ogmrlfzdthnwkez.onion/
- Hitman Network – Contract killers located in the US/Canada/EU
- Peoples Drug Store – Online drug supplier
- Brainmagic – Psychedelic drug marketplace
- Apples4Bitcoin – Discounted Apple products in exchange for Bitcoin http://tfwdi3izigxllure.onion/
- EuroGuns – European arms dealer

Hosting Services

There are an abundance of deep web hosting services that allow users to host files, images, or websites using Tor and other technology to keep transactions anonymous.

Filesharing

- The Bomb Shelter – Relatively new file and image hosting service with lots of features http://ntoibame4iky6xhv.onion/
- TorShare – 2GB upload limit. Illegal files not allowed http://oukryuqqc7ffenin.onion/
- Sky Fortress – Open source platform to upload and download encrypted files http://shxdhomhggy3bjrn.onion/skyfortress.php
- TOR Upload Service – Allows for files up to 10GB but uses JavaScript and Flash http://ocrlwkklxt3ud64u.onion/

Image Hosting

- Magic Mirror – Open source, encrypted image hosting
  http://4344457357774542.onion/
- IMGuru – Fast GIF/JPEG host where images never get removed
  http://p7d2k2xiioailnuu.onion/
- SquareBoard – Upload and share high quality images
  http://squareh565qgkioq.onion/

Web Hosting

- Torhost.onion – Free anonymous web hosting
  http://torhostg5s7pa2sn.onion/
- OnionHosting – Premium anonymous hosting service
  http://bj6sy3n7tbt3ot2f.onion/
- Liberty's Hackers – Service and hosting provider
  http://3vnjj7h6c6vw2yh5.onion/hello.php
- TorShops – Turnkey .onion stores with Bitcoin integration
  http://shopsat2dotfotbs.onion/

Blogs/Essays/Personal Pages

- Ismism – Provides visitors with a venue to publish opinion editorials on topics ranging from political language to modern uses and meanings to gibberish
  http://xqz3u5drneuzhaeo.onion/users/ismism/
- Tornado - Forum, blogs, polls, registered or anon posting
  http://b6kpigzhrdhibmos.onion/d6/
- Fake Checks; Real Pizza (clearnet) - Personal blog of the old TorChan administrator, cerulean
  http://torgame.crabdance.com/blog/
- My Hidden Blog - Security politics, security, tor, tools, personal

http://utup22qsb6ebeejs.onion/

- 404's Blog - Blog about a few things happening in Tor, mainly revolving around TorChan & other image boards http://5a7ryk7pdjflogpx.onion/flatpress/
- Dark Like My Soul - A blog by fancycakes. Has some of the most inspiring and beautiful poetry you will read within your lifetime http://ad52wtwp2goynr3a.onion/
- RespiraTOR - If something is infuriating you, it's better to get it off your chest http://6g2osf4l534bozmu.onion/
- Tor and blosxom - A Tor hidden service running on the blosxom blogging platform http://cxoz72fgevhfgitm.onion/
- The Croat's Blog - It's all about the intel and knowledge! Whistleblowing FTW! http://kv77v7n5kblz5tpw.onion/
- The Human Experiment - Human medical experiments. We go, where few dare. (Direct FH URL) http://xqz3u5drneuzhaeo.onion/users/experiments/

Forums

- TorShops Forum - Forums for discussion, reviews and feedback about TorShops vendors http://ui4zevqxi26kgenc.onion/
- Freedom For People - A revolutionary group against capitalism http://5xrder5zmkqkdary.onion/forum/
- SciBay Forum - Chemistry and other sciences forum http://sbforumaz7v3v6my.onion/
- Onionforum 2.0 - A restart of the popular Onionforum. No login required http://65bgvta7yos3sce5.onion/
- OnionMe - Forum for personal ads. All ages welcome http://stlw74hqbtzoshyg.onion/

Email/Messaging

- Tor Mail - Webmail/SMTP/IMAP/POP3. Can send/receive mail from outside Tor with a you@tormail.net address http://jhiwjjlqpyawmpjx.onion/
- SMS For Tor - Encrypted private messaging service http://sms4tor3vcr2geip.onion/
- SimplePM - A PM service by CWKU. No registration needed http://4v6veu7nsxklglnu.onion/SimplePM.php

Hacking

- DOXBIN - DOX go here. A pastebin for personally identifiable information http://npieqpvpjhrmdchg.onion/
- HackBB - Forums for hacking, carding, cracking, programming, anti-forensics, and other tech topics. Includes a marketplace with escrow http://clsvtzwzdgzkjda7.onion/
- Blackhats Anonymous - A download website. Currently under construction http://mqv7qz5rn3sf5dcx.onion/
- hashparty - Password hash cracking site http://3terbsb5mmmdyhse.onion/
- OnionWarez - Warez forum http://dts563ge5y7c2ika.onion/
- BRAMA - Linux/Wireless/Mobile tech consortium in Poland http://mtn2fcv7yerki2op.onion/
- TM Comm - For a Chaotic Tomorrow http://pdjcu4js2y4azvzt.onion/
- Shell In A Box - Shell In A Box http://rvomgbplxtz4e7jv.onion:8080/
- Requiem - Software for removing iTunes DRM http://tag3ulp55xczs3pn.onion/

- Crackwar - Pirates are the good guys! http://xqz3u5drneuzhaeo.onion/users/crackwar/
- Weird and Wonderful Old Stuff - A collection of old DOS and Windows software http://xqz3u5drneuzhaeo.onion/users/dosbox2/
- Onion Desktop - eyeOS web desktop http://ybi5yfcdw6mxqlvn.onion/
- bugmenot@tor - A user supplied database of account credentials for various websites http://fcl3t6t66uv3u4og.onion/

Politics

- profunc** - Information dissemination, info/files, political dissent, communism, socialism http://vc24blsbg5ow5slk.onion/
- The Anarchism Library Mirror - Mirrors books from The Anarchist Library http://4zeottxi5qmnnjhd.onion/

Weapons

- LiberaTor - Making weapons, military training, and related subjects http://p2uekn2yfvlvpzbu.onion/
- ParaZite - Collection of forbidden files and how-to's (pdf, txt, etc.) http://kpynyvym6xqi7wz2.onion/files.html

As you can see, there is a lot of information available on the deep web and most of it is relatively benign. Sure…there are a lot of other sites available through the Tor browser too (some good and some bad) but the list above should keep new Tor users busy for a while as they explore the hidden world of the Tor network.

Chapter 14: Hidden Wiki and Tor Directories

As you know by now, you can't open up Google when using Tor to find the sites and services you are seeking. There are some browsers that index .onion sites such as DuckDuckGo, but the single best way to find exactly what you are looking for on the deep web is to use a Tor directory such as the Hidden Wiki. In fact, many of the websites and services listed in the previous chapter came from the Hidden Wiki. But what exactly is the Hidden Wiki and how do you find it?

The Hidden Wiki is by far one of the best sites available to Tor users when looking for hidden services embedded within the Tor network. The Hidden Wiki is full of hundreds of thousands of links that lead to a myriad of places that are only accessible through the deep web. Everything is categorized and in most cases there is a short explanation next to each link so you know exactly where you're going before you click.

To access the Hidden Wiki, you first need to make sure Tor is installed and properly configured on your machine of choice. You cannot access any sites that end with .onion unless you are using the Tor browser. At the time of this writing, the original Hidden Wiki is down but the good news about the deep web is that someone almost always posts a mirror site when things like this happen. One of these mirrors is http://jh32yv5zgayyyts3.onion/ and when pasted into the Tor browser, this link will take you directly to a copy of the Hidden Wiki with links to just about anything you can imagine.

The Hidden Wiki isn't the only place where you can find cool .onion sites to visit while journeying through the deep web. Reddit is an excellent resource for finding out more information about hidden services offered via the Tor network. This post has some good

resources that are worth checking out (https://www.reddit.com/r/onions/comments/1zeve6/huge_list_of_hidde

Even on the surface Internet, some useful information can be found about hidden Tor services. Wikipedia has a list of known sites that are part of the Tor network (although there aren't nearly as many listed here as in the Hidden Wiki. You can view the Wikipedia page about Tor hidden services here.

Finally, don't forget to check out the uncensored Hidden Wiki which can be accessed by visiting http://uhwikih256ynt57t.onion/wiki/index.php/Main_Page from within the Tor browser. No matter where you go first, you are sure to find lots of information that you didn't even know existed before picking up this guide and entering the world of the deep web.

Conclusion

As you have seen, protecting your identity and browsing habits while perusing the Internet isn't difficult. In just a few minutes, you can enjoy the anonymity that comes with using the Tor browser without worrying about who might be watching what you do online.

Tor is simple, free, and effective. In addition to protecting your online identity, Tor also offers you a glimpse into the world of the Deep Web – a network so large that it makes the surface Internet look small. What other tool provides so many benefits for free? Very few…if any.

Even if you had never heard of Tor before picking up this guide, you now know what Tor is (and what it isn't), how to install it on your own PC and configure it for optimum performance, the legal issues surrounding the use of Tor, what the Deep Web is and how to navigate through it, and even how to support the Tor network by becoming a relay operator (if you so choose).

There is an entire world lying hidden underneath the Internet that most people don't even think about, or aren't even aware of, and you now have the tools to access that information without worrying about who might be watching or collecting data about you while browsing.

Yes, governments and organizations or shady characters are always trying to get/access/use your private information while online, but fear not my friends — the combination of safe browsing habits and a properly configured Tor client is all you need to make the Internet a safe place again. So what are you waiting for? There is A LOT of exploring to do and armed with the knowledge in this guide, you can do it without fear of reprisal from anyone. True online freedom comes from anonymity and that is something easily fixed with Tor.

Thank You

Thanks for downloading and reading this book. If you enjoyed reading the Tor Browser Handbook, I'd really appreciate it if you could take a moment to click here (torbrowserhandbook.com/review) to leave a review on Amazon. It will only take a few seconds, but it will really help me to reach more readers that will discover this book thanks to your review.

Don't forget to pick up your Free Tor Tips & Links bonus report at torbrowserhandbook.com/bonus!

Sincerely,

S.K.