Chapter #1: What is Tor?

1. Protects users' anonymity by protecting online activity through a series of encrypted layers, is how Tor still works today.
2. 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
3. 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.
4. 2012 report leaked by ex-NSA contractor Edward Snowden reveals that the NSA has been unable to crack Tor as a network

Chapter #2: How Do You Use Tor?

1. 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 can only be accessed using the Tor network and its hidden services feature.
2. 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.

Chapter #3: How Does Tor Technically Work?

1. There are actually three different types of relays that comprise the Tor network: end relays, middle relays, and bridges.
2. 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.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.
3. 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.
4. A bridge is a Tor relay that isn't publicly listed in an attempt to shield these relays from IP blockers. To circumvent this, many Tor users operate a Tor bridge that shields the fact that Tor is being used at all.
5. 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.

Chapter #4: Tor Legal FAQ

1. Can I be prosecuted or sued for running Tor? NO
2. Should Tor be used for illegal purposes? NO
3. Can The Tor Project or EFF promise that I won't get in trouble for operating a Tor relay? NO
4. Will EFF represent me if found legally liable for running a Tor relay? MAYBE
5. Can I contact Tor developers with legal questions or if I suspect Tor is being used for illicit purposes? NO
   If faced with a specific legal issue, please contact info@eff.org.
6. Are there any promises made by Tor developers about the reliability and trustworthiness of Tor relays within the directory? NO
7. Should an exit relay be run from my home? NO
8. Should my ISP be informed before running an exit relay? YES.
9. Should I look at the plaintext traffic that exits my end relay? NO

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

1. Tor Still Functions as Intended
2. Tor Has Many Legitimate Uses
3. Tor Doesn't Have a Backdoor
4. It Is Not Illegal to Run a Tor Relay in the United States
5. Tor is Easy to Use
6. Tor is Faster than Most People Think
7. Tor is Not a Foolproof Solution

Chapter #6: Tor vs. VPN – The Important Differences

1. VPNs: encrypted and passed through a server (or series of servers) before reaching its final destination.
2. Tor: the connection is encrypted before being sent to through three or more Tor relays.

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

1. 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.
2. All IP addresses contain four sets of numbers each separated by a single dot.sets of four numbers range from 0 to 255. 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.

3. 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 are temporarily assigned to a computer when it tries to access the Internet.
4. Hiding Your IP Address

   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.

   b) VPN can be used to mask your true IP address.VPN creates an encrypted connection between the VPN server and your computer and exits via the VPN server.

   c) 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.

Chapter #8: Getting Started with the Tor Browser Bundle

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

Chapter #9: Installing Tor– Windows

To ensure the Tor network has been properly configured, test the network settings before beginning a browsing session.

Chapter #10: Installing Tor- Linux

Debian and Ubuntu systems are the easiest when it comes to installing Tor

Chapter #11: How to Access the Deep Web

1. 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.).
2. 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.
3. 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.

4. 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.

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

1. Use Tor: 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: A better choice would be to use a Linux-based system or a Live OS made for privacy such as Tails.
3. Perform Regular Updates: 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: 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.
5. Encrypt Data Storage: 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: The FBI's recent takedown of Freedom Hosting was only possible due to vulnerabilities within the Tor Browser Bundle.
7. Disable JavaScript, Java, and Flash: 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. It's worth restating protect your privacy and anonymity and stay away from P2P
9. Delete Cookies and Local Data: Cookies and local data storage are two of the ways that websites can track you even when using Tor. 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.
11. Ditch Google: 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.

Chapter #13: Top Tor Links and Resources

Search Engines, General Things to Check Out, Marketplace, Financial Services, Commercial Services, Hosting Services, Filesharing, Image Hosting, Web Hosting, Blogs/Essays/Personal Pages, Forums, Email/Messaging, Hacking, Politics, Weapons

Chapter #14: Hidden Wiki and Tor Directories

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.

Conclusion

1. 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.
2. 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
3. True online freedom comes from anonymity and that is something easily fixed with Tor.