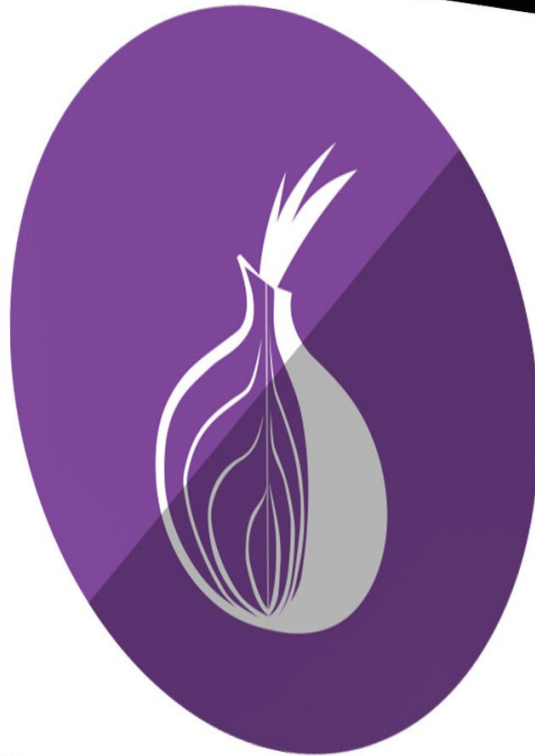


# TOR AND THE DEEP WEB

HOW TO BE ANONYMOUS ONLINE IN THE DARK  
NET THE COMPLETE GUIDE



PHILL VEGA

# **Tor And The Deep Web**

**How to Be Anonymous Online In The Dark Net The Complete Guide**

By

**Phill Vega**

**Beginners to Expert Guide to Accessing the Dark Net, TOR Browsing, and  
Remaining Anonymous Online**

## Disclaimer

This document is geared towards providing exact and reliable information in regards to the topic and issue covered. The publication is sold with the idea that the publisher is not required to render accounting, officially permitted, or otherwise, qualified services. If advice is necessary, legal or professional, a practiced individual in the profession should be ordered.

- From a Declaration of Principles which was accepted and approved equally by a Committee of the American Bar Association and a Committee of Publishers and Associations.

In no way is it legal to reproduce, duplicate, or transmit any part of this document in either electronic means or in printed format. Recording of this publication is strictly prohibited and any storage of this document is not allowed unless with written permission from the publisher. All rights reserved.

The information provided herein is stated to be truthful and consistent, in that any liability, in terms of inattention or otherwise, by any usage or abuse of any policies, processes, or directions contained within is the solitary and utter responsibility of the recipient reader. Under no circumstances will any legal responsibility or blame be held against the publisher for any reparation, damages, or monetary loss due to the information herein, either directly or indirectly.

## Copyright

Respective authors own all copyrights not held by the publisher.

The information herein is offered for informational purposes solely, and is universal as so. The presentation of the information is without contract or any type of guarantee assurance.

The trademarks that are used are without any consent, and the publication of the trademark is without permission or backing by the trademark owner. All trademarks and brands within this book are for clarifying purposes only and are the owned by the owners themselves, not affiliated with this document.

# Table of Contents

## INTRODUCTION

## CHAPTER 1: WHAT IS TOR?

### INTRODUCTION TO TOR

### WHAT IS THE DARK WEB?

#### SURFACE WEB:

#### DEEP WEB

#### DARK WEB

### WHY DOES THE DEEP WEB EXIST?

### HISTORY OF TOR AND WHY IT WAS CREATED

#### LEGALITY OF DARK WEB

## CHAPTER 2: WHY IS TOR USED?

### WHY COMMON PEOPLE USE TOR

#### PROTECTION

#### CENSORSHIP

#### SURVEILLANCE

### HOW TOR CAN HELP MEDIA AND JOURNALISM

### USE OF TOR BY LAW ENFORCEMENT

#### STING OPERATIONS

#### ANONYMOUS TIP LINES

### HOW WHISTLE-BLOWERS CAN USE TOR

### HOW CAN CELEBRITIES AND UNDERPRIVILEGED PEOPLE USE TOR?

#### ILLEGAL USES

## **CHAPTER 3: HOW TO ACCESS THE DARK WEB USING TOR: A GUIDE**

### **HOW TO ACCESS DARK WEB USING A COMPUTER**

INSTALLING TOR

USING THE TOR BROWSER

### **HOW TO USE DEEP WEB ON A PHONE**

HOW TO ACCESS DEEP WEB ON AN ANDROID PHONE

HOW TO ACCESS TOR ON AN IPHONE

I2P

## **CHAPTER 4: DARKNET MARKETS**

### **CRYPTOCURRENCY & PAYMENTS**

ESCROW AND MULTI-SIG

### **POPULAR DARK MARKETS**

DREAM MARKET

VALHALLA

ALPHA BAY

THE REAL DEAL

CRYPTO MARKET

MIDDLE EARTH MARKETPLACE

OXYGEN

## **CHAPTER 5: HOW TO USE BITCOIN?**

### **USING BITCOIN PRIVATELY: A GUIDE**

USING DISPOSABLE ADDRESSES

BITCOIN MIXING

HOW TO TRADE BITCOINS ANONYMOUSLY

USING PEER-TO-PEER EXCHANGE

SECURITY

ID VERIFICATION

STEALTH ADDRESSES

TAINT ANALYSIS

## **CHAPTER 6: DO'S AND DON'T S**

**DO TRY TOR**

**DON'T USE WINDOWS OR USE IT WISELY**

ALWAYS UPDATE YOUR SYSTEM

AVOID HTTP WEBSITES

DON'T GET CONFUSED BETWEEN DARK WEB AND DEEP WEB

ENCRYPT EVERYTHING

NEVER USE JAVA, JAVASCRIPT, FLASH

AVOID P2P

ALWAYS DELETE YOUR BROWSING DATA AND COOKIES

NEVER USE YOUR PERSONAL DETAILS

AVOID GOOGLE AS MUCH AS POSSIBLE

ALWAYS USE TRUSTED DIRECTORIES TO FIND LINKS

## **CHAPTER 7: DARK WEB RESOURCES**

**THE SILK ROAD**

**TOR MAIL**

**THE HIDDEN WIKI**

**HIDDEN WIKI IS USUALLY UP**

TORDIR

CORE.ONION

HASH PARTY

FBGB CRACKING FOR BITCOIN

TORLINKS

HACKBB

## **CHAPTER 8: FAQs**

### **DIFFERENCE BETWEEN SURFACE WEB, DARK WEB, AND DEEP WEB**

SURFACE WEB

DEEP WEB

DARK WEB

**WHEN WAS THE DARK NET INVENTED?**

**WHY WAS TOR FORMED?**

**WHY IS TOR SO SLOW?**

**WHAT IS TOR?**

I AM SCARED, IS THE DARK NET SAFE?

DOES TOR WORK WITH WINDOWS 10/7/XP?

WHAT IS THE HIDDEN WIKI AND WHERE CAN I FIND IT?

IF DARK WEB IS SO SCARY/ILLEGAL, WHY IS IT STILL WORKING?

I DON'T LIKE THE SITES MENTIONED IN THE HIDDEN WIKI, ARE THERE ANY OTHER SITES THAT I CAN ACCESS, WHERE CAN I FIND THEM?

IS THERE CHILD PORN ON THE DARK NET? WHAT IF I ACCIDENTALLY SEE IT? WILL I BE ARRESTED?

ARE THERE ANY SEARCH ENGINES FOR TOR?

CAN I GET ADDICTED TO TOR/DARK WEB?

WHAT IS TO BE AVOIDED ON DARK NET?

I BROWSED DARK WEB, NOW WHAT TO DO?

IS TOR BASICALLY A PROXY? WHY SHOULDN'T I USE PROXY INSTEAD OF TOR?

DOESN'T THE GOVERNMENT BACK TOR? SO, DO THEY HAVE A BACKDOOR IN TOR?

IS IT POSSIBLE TO SHARE FILES USING TOR? WILL THE PROCESS BE ANONYMOUS AS WELL?

CAN TOR BE USED ON MY CELLULAR DEVICE?

HOW CAN I CHECK IF TOR IS WORKING?

I DO NOT LIKE TOR, HOW DO I UNINSTALL IT?

IS TOR SAFE? OR IS IT MALWARE?

DOES TOR PROVIDE FULL ANONYMITY?



IS TOR A FORM OF VPN? SHOULD I USE VPN INSTEAD OF TOR?

DOES TOR PROMOTE CRIMINAL ACTIVITY? CAN CRIMINALS USE TOR TO COMMIT CRIMES?

WHY SOME VIDEOS DON'T WORK ON TOR?

CAN I USE CHROME/OPERA/IE ETC. WITH TOR?

WHY DOES MY GOOGLE PAGE COME OUT IN WEIRD LANGUAGES?

CAN/SHOULD I INSTALL MY FAVORITE FIREFOX EXTENSIONS?

**CONCLUSION**

## Introduction

I want to thank you and congratulate you for purchasing the book, "TOR: Beginners to Expert Guide to Accessing the Dark Net, TOR Browsing, and Remaining Anonymous Online"

This is the age of the Internet and everyone who wants to be informed needs to be online. The Internet is a giant web of information and content is used for a variety of purposes nowadays. However, there are many things that the Internet cannot provide. One of these things is privacy. Internet privacy is a thing of the bygone era. Any device that is on the network is unsafe, and nothing is private. A devastating but universal fact!

The FBI, the NSA and third-party sophisticated hackers can track and monitor what you do. Though not many of us are concerned with the fact that our data, our files, our location, etc. are not private, a significant chunk of society is wary of it. If you were not protected, it's not too late, keep on reading to find out how you can prevent this from happening.

If you aren't worried about your privacy, you might be curious about what exactly the dark web is and how you can benefit from it. Or maybe you want to access certain products that are not accessible over regular Internet or offline. Well, you will find a complete guide in this book to help you.

If you follow the instructions given in this book

correctly, no one will be able to track you, and you will be safe and secure. Thus, this book is a complete and foolproof guide to Dark Web and TOR, and will help you access the world of the Dark Web without any problems.

I want to thank you once again for choosing this book, and I hope you find this book useful and informational and will help you access everything you want anonymously. I hope you enjoy it!

# Chapter 1: What is TOR?

To understand the intricacies of the Dark Web and its many uses and problems, it is first necessary to understand TOR. This chapter will mainly touch upon the topic and will be an introductory guide to Tor.

## Introduction to Tor

In simple words, TOR is the short form of The Onion Router. It is a free of cost software that enables the user to communicate anonymously. It can channel Internet traffic through a worldwide network of seven thousand plus free relays, which can keep the location, as well as usage of the user, anonymous. It can keep you safe and can make it difficult to trace you or your Internet activity.

So, TOR is a service that allows its users to browse the Internet, send IMs, chat and socialize but anonymously. What makes it different than other forms of the Internet is that it delivers what it promises. The primary purpose of TOR is to keep the personal privacy of the users secure and allow them a free space to conduct their affairs without any form of monitoring or surveillance. It is thus a mode of confidential communication.

You must have noticed the icon of the logo of TOR - it is an onion. This is no coincidence. The onion portrays the system correctly; as the form of routing that is done by TOR is called onion routing. It is the encryption of communication protocol stack in the application layer, one under another, thus, forming an onion-like structure. Tor can encrypt

almost all major types of data such as IP address, and forward it through a circuit of various randomly selected relays where each relay decrypts only one layer and forwards the remaining ahead. The final layer is decoded at the destination, and thus the information received is concealed and so is the sender's IP address.

In general terms, Tor is also called a browser that is used to browse Dark Web. In the next section of this chapter let us have a look at what is Dark Web or Dark Net and how is it different from Surface Web as well as Deep Web.

## **What is the Dark Web?**

As explained in the last section of this chapter, Tor is used to access locations on the Dark Web. However, to understand the nature of the Dark Web, it is necessary to figure out what is Surface Web and what is Deep Web. So, let us have a look at these two terms first.

### **Surface Web:**

Surface Web is basically whatever your notions of the Web are. It includes social networking sites, shopping sites, search engines, news media, etc. Almost every site that you can access without any additional settings except a regular web browser and active Internet connection is on Surface Web.

A basic definition of Surface Web is as follows - It is a web made of various fixed and static pages. These pages are not dependent on a database for content. However, some sites like amazon.com do have

connections with the deep web in the form of database. The pages on static web stay on a server waiting for users to retrieve them. Thus, these pages are nothing but HTML files that are static and whose content never change. To update the pages, it is necessary to replace the HTML file of the page.

All websites with domains such as .com, .in, .uk, .org, co.in, .net, etc are Surface Website sites.

You must have seen various pictures on the Internet representing Surface web and Deep web. One of the most commonly used pictures to represent the above equation is the picture of an iceberg- where the iceberg above the surface of water represents the surface web while the iceberg below the surface represents deep/dark web. Let us now have a look at what Deep Web is.

## **Deep Web**

A simple definition of the Deep Web is all the pages that a search engine cannot find. i.e. these pages are not indexed by the databases of the search engines. There exist a variety of reasons why a search engine cannot access the Deep Web pages. But before we go there, let us first have a close look at Deep Web.

Deep Web is the online database and dynamic web pages that a standard search engine like Google or Yahoo cannot access. It is the content and data behind HTML forms. Like Surface web, the Deep web too has many applications such as email, online banking, chat rooms, etc. There are also services such as video chat rooms, various paid services,

video on demand, etc.

It is estimated that the Deep Web is almost 400 to 500 times larger than the Surface Web. This means it has more than eight petabytes. Compare this with the nineteen terabytes of data present on the Surface Web, and you will realize how huge the Deep Web is.

Certain search engines can access Deep Webs. Some of them include Intent, DeepPeep, Deep Web Technologies, Ahmia.fi, and Scirus, etc. Invisible Web or Deep Web is often confused with Dark Web; however, both these terms are different and refer to different things. While it is legal to access information off Deep Web almost all the time, it is not the case with Dark Web. In the next section let us have a look at the Dark Web.

## **Dark Web**

As said earlier, the Dark Web is often confused with Deep Web thanks to the hidden nature of both the Webs. However, Deep Web and Dark Web are two different things.

It is possible to say that the Dark Web is a part of Deep Web, as standard search engines cannot access it as well. However, it is different than Deep Web as the content on Dark Web is often hidden deliberately. It is a network of sites that can be accessed but are hosted anonymously. These sites are inaccessible to standard browsers and browser techniques and often require special software.

The Dark Web is an almost untraceable worldwide network that has many uses, which may or may not be

legal. The sites on Dark Web are accessible to only those who know what they are looking for.

The main motive of the Dark Web is anonymity and privacy. This anonymity is Dark Web's boon as well as a curse. The anonymous veil of the Dark Web is often used to conduct a variety of illicit and illegal activities, which is why the Dark Web is so notorious. This notoriety is often carried forward to Deep Web, making it a stigmatized concept as well. However, as made clear above, both the Webs are two different entities. The Deep Web is a simple collection of databases that is not indexed by standard search engines, while the Dark Web is an encrypted network among TOR servers and users. It is just a tiny, albeit very famous part of the Deep Web. In a single line- all Dark Web is Deep Web, however not all Deep Web is Dark Web.

The Dark Web is a minuscule part of the Deep Web; it is estimated that it does not even form 0.5% of the Deep Web. However, it is highly popular thanks to its various anonymous and private markets that often trade in illegal products.

Now that you know what Deep Web and Dark Web are, you must be wondering why they exist and whether they are needed. Let us have a look at this question.

### **Why does the Deep Web exist?**

A simple answer to the above question is because we need to hide certain things. For instance, if you have an Internet Banking account, your account details are on the Internet. However, they cannot be



accessed by a simple Google search. Thus, your account pages are secure and safe in the Deep Web. Without the Deep Web, it is safe to assume that the Internet would have been much less useful. We would not be able to have social networks, Internet Banking, E-shopping, etc. as these sites store your sensitive data on Deep Web to make them secure.

It also exists to store a large amount of data of the corporate world. For instance, many large corporations store their business-related data on Deep Web. This provides them with safety and security.

You might be surprised to know that you access Deep Web almost every day. Yes, as said earlier, your social networking accounts, your email, etc. store your personal data on Deep Web, hence whenever you access your email, your bank statement, Twitter DMs, your office intranet, etc. are all a part of Deep Web. However, all of the above things are not always secure, and you are not anonymous on the Surface Web, even if it is connected to Deep Web. This constant need for anonymity and privacy from the governmental surveillance led to the formation of Dark Web.

## **History of TOR and why it was created**

TOR is one of the most commonly used software to access the Dark Web. It is almost a fail-proof way of being anonymous. The history of Tor is quite interesting, and it can help people to understand why the need of Tor arose and why it is still relevant.

It will come as a surprise that the roots of Tor can be traced back to the United States Naval Research Lab. Employees of the above organization viz. Syverson, Reed and Goldschlag researched ways to protect the intelligence communication in the mid-90s. This was the beginning of Onion routing. Onion routing then moved on to DARPA, and it was enhanced there in the late 90s.

Syverson along with Mathewson and Dingledine launched the alpha version of Tor on 20th September 2002. It was then known as The Onion Routing project. A public version was released the next year.

A turning point in the history of Tor was when Mathewson, Dingledine, and others created Tor Project in 2006. A non-profit organization runs and maintains Tor. It is a surprising fact that some of the early financiers of the project were Internews, Google, and University of Cambridge, US. International Broadcasting Bureau etc. It also received monetary support from Human Rights Watch. Nowadays, the US government supports the Tor Project financially.

So, the Navy created Tor, to hide/protect governmental communications. The purpose has not changed a lot since then, however, the user circle has expanded and now common people like us can use it to safeguard our privacy as well.

### **Legality of Dark Web**

One of the most frequently asked questions regarding the Dark Web is its legality, and to be honest, the

issue is rather muddled. In this section, I have tried to shed ample light on this topic to clear any confusion associated with it.

Before moving on to the topic, please remember that the Deep web does not equal to Dark web. The deep web is anything that is not indexed by any popular search engine and is thus hidden. However, it can be accessed with regular browsers, unlike the Dark web that needs a particular browser or software. The sites on Dark web are built on the public Internet as well; however, they cannot be accessed easily.

Browsing the deep web and dark web is not illegal, technically. Unless you are trying to find content that is inherently illegal like child pornography, you are not doing anything illegal.

For instance, there exist many websites on the Dark web that proclaim to sell drugs, fake IDs, guns, and weapons. Some also sell stolen goods etc. Browsing such sites is not illegal, you can browse all you want, however, if you buy something from these sites then it is illegal. As the products available on these sites are stolen, you are practically committing theft by buying these goods. Some of the most popular stolen goods available on Dark Web are guns, weapons, drugs, meth, hacked PayPal Cards, fake ID, stolen iPhones, grenades, etc.

Dark Web is not inherently illegal. For instance, there are many harmless sites available on the Dark Web like social networking sites, email services, message boards, etc. These sites are not illegal per se, however, if you discuss illicit content over them then your activities can be counted as illegal

or problematic.

The legality of the Dark Web also depends upon your area and nation. For instance, Dark Web is allowed in the US, however, accessing it in North Korea is illegal. If your nation has an intrusive and regressive government, then the Dark Web can be illegal in your country.

In recent times the FBI and other such organizations have blocked many websites on the Dark Web. Most of these sites dealt with illegal and illicit activities such as illegal guns, weapons, drugs, human trafficking, etc. It is not clear whether just visiting these sites is illegal or not; however, it is safe to assume if you do not own one of such sites or do not buy goods from them regularly, you won't be prosecuted.

So, I hope I have answered your question about the legality of Dark Web. Yes, it is not illegal to access the Dark Web, however, it is necessary to understand that the nature and content of the sites that you visit can jeopardize your anonymity and security. I do not recommend purchasing/ selling anything on the Dark Web; neither do I recommend downloading anything from the network.

As a safety measure, it is recommended that you avoid all the links that are unlabeled. These unlabeled links are often without any description and can lead you to some honestly horrifying and disturbing content.

In the next chapter let us have a look at the variety of uses of TOR and how it can benefit you.

## Chapter 2: Why is TOR Used?

TOR is a remarkable project to protect everyone from surveillance. It is becoming more and more essential in today's world thanks to the constant presence of government and other institutes in our day-to-day life. The world has become an Orwellian nightmare and thus, Tor and other such ways of staying anonymous are a boon for the society.

TOR has many uses and users, all with different purposes. In this chapter, let us have a look at the variety of uses of Tor, which will promote you to try and use it. The uses have been divided into multiple sections for convenience.

### Why common people use Tor

#### Protection

As mentioned earlier, the world is rapidly becoming an Orwellian nightmare thanks to the constant surveillance of the government and various other institutes. Our ISPs or Internet Service Providers can track and access almost all of your browsing and surfing data. Though ISPs do proclaim that they protect your data and information most of them can sell it to buyers for the right price. Your data includes everything right from a database of every site that you have visited, your search details, and in some cases even your User Id and passwords. As it is clear, this information is very sensitive and thus theft of this data can prove to be a nuisance.

Other than your ISPs, even regular websites can

access the above-mentioned sensitive information. Smart websites can also intercept and track your communication data as well. You cannot trust anyone with your data. No wonder all technology gurus recommend people to use Tor to keep their data safe from breaches and betrayers.

Although most of us do not share personal data over the Internet yet even simple things like IP address can prove to be harmful. For instance, it is now possible to trace your location using your IP address. This technology is becoming so sophisticated that now it is possible even to trace your street address.

### **Censorship**

Many nations do not allow their residents to use the Internet freely. Often various social networking sites such as Facebook, Twitter, YouTube, etc. are blocked on these nations. These sites are often blocked behind a national firewall.

The firewall often blocks sensitive information as well. For instance, if the topic of your research is AIDS, sexual diseases, birth control, abortion, religion, terrorism, etc. You cannot access these without raising red flags. Hence, if you want to conduct your research without any fear, Tor is essential.

### **Surveillance**

You will be surprised how even your simple, surface web browsing can make authorities suspicious. Your browsing history can cause a lot of problems if it does not remain private. And don't think that

Incognito mode of the various browsers can protect you. Only Tor can keep your online and offline life separate

## **How Tor can help media and journalism**

In today's world even the pillar of democracy that is media is not safe. Nowadays media is often biased, and paid media is a harsh reality. However, all of the media is not biased and many honest journalists exist unfortunately for them most of the media is now controlled and censored by the government of the world. This government does not let these honest journalists and media persons present their point of view in an unbiased and uncensored way. Tor can help such trapped media persons to present their honest views with full security, privacy, and anonymity.

Using Tor, media persons can present the truth of their homeland with total security. With this the people who want unbiased news can get it from Tor as well. It should not come as a surprise that various American institutes support Tor to promote free speech and independence. Tor can also help you research controversial topics without any problems. These topics include sensitive subjects such as religion, terrorism, abortion, etc.

## **Use of Tor by Law Enforcement**

The title of this section might surprise you thanks to various myths and legends prevalent about Tor and Dark web on the Surface web. One of the most common myths about Tor is that it is illegal and that it is only an interface to conduct illicit activities.

However as said earlier this just a myth which is why law enforcements all over the world use Tor for a variety of purposes. The most common use is online surveillance

Although it is quite possible to keep an eye on various illegal activities on the Surface web, it is a time and money-consuming affair. For instance, even if the cop is well versed in street slang and language their cover might blow away due to the simple fact their IP can be traced by these illegal sites. Hence cops often use Tor to conduct online surveillance. Tor can keep your IP, and all other details secure and hidden from everyone hence, making it one of the best options of surveillance to law forces.

But do not worry, police forces only track people who are already under suspicion of illegal and illicit activities. So you can be sure that the forces won't track you unless of course you visit and use these illegal sites

### **Sting operations**

Law enforcements can also use Tor to conduct various sting operations on suspicious people. These sting operations are far more sophisticated and safe than the real-life sting operations.

### **Anonymous Tip Lines**

Law forces all over the world agree that anonymous informants are the best informants available. However, these informants need to be protected, and their security is a sensitive issue. Although many Tip software and lines exit on the surface web but



they are not truly anonymous, and a person with sophisticated technical knowledge can trace the location or the details of the tipper. To prevent this, there exist many anonymous Tip lines on Tor. These lines are often untraceable and quite secure. Tipplers can send information without any second thoughts.

## **How Whistle-blowers can use Tor**

The world is becoming more and more violent day by day, which has led to the rise of human rights activists all over. However, due to censorship and archaic laws many human rights advocates cannot promote their cause freely. They cannot present their reports of abuses and dangers without threatening their lives. Tor can help these activists to present their point of view without any worry. Tor thus allows them to continue their work without the fear of persecution and in some cases execution.

One of the major humanitarian organizations, the Human Rights Watch recommends Tor in its report Internet Censorship. This report has a section on how it is possible to break the Chinese firewall. Other prominent organizations such as Amnesty and Global Voices also recommend Tor.

In many nations, whistle-blowers do not enjoy any legal protection provided by the government. However, whistle-blowers can continue with their work if they use Tor. They can continue their journey of seeking the truth without any problems.

## **How can celebrities and underprivileged people use Tor?**

Everyone is obsessed with celebrities, and the fan girl culture has gained momentum over the last few years. We love our stars and want to follow them. However, all this limelight often disturbs their lives, which often causes them a lot of problems. The constant interference can be avoided if Tor is used. Celebs can keep blogs and present their political or other views online without ruining their image. Along with celebs, this can also help other high profile people who cannot enjoy a private online life.

Underprivileged and people who live in poverty too cannot enjoy an entirely private life. They cannot participate in the society in totality. They constantly need to worry about their jobs, social workers, and others. A single bad comment can ruin their life. However, Tor can help such people to present their views without any fear. It gives voice to the voiceless. The poor, the dejected and the harassed can voice their opinion online without fearing any backlash.

## **Illegal Uses**

As said earlier, there exists an illegal side of the Dark Web. However, as this is a complete guidebook for Tor, I also include some information about this side here.

An unknown side of the Dark Web is that it is one of the biggest libraries. You can access and find almost every book in the annals of Tor. This is especially useful for the residents of nations where books are banned and censored heavily. This is also useful for people who want conduct a variety of

research.

You can find almost all kinds of books on Tor and can read them online or download them. However, downloading is not recommended unless you know what you are doing as Dark Web is not as simple as the Surface web.

One of the most frequently talked about aspect of the Dark Web is the presence of various markets. These markets often trade in a variety of illegal goods and services such as weapons, recreational drugs, fake IDs, etc. There are other markets on the Dark Web that are not as dangerous as the ones dealing with the above goods. You will find a list of various markets in a dedicated chapter below.

So, these were some of the many uses of Tor. In the next chapter let us have a look at how you can access the Dark Web using Tor.

## **Chapter 3: How to Access the Dark Web Using Tor: A Guide**

Till now we have seen the basics of the Dark Web and Tor. This must have made you curious about Tor, and now you must be wondering how to access the Dark Web. In this chapter, I have included the best way to access Tor using a computer. As cellular devices are almost as competent as computers nowadays, I have also included a guide on how to access the Dark Web using a mobile phone.

### **How to access Dark Web using a computer**

The easiest and the best way to access the Dark web on a computer is to download the Tor Browser bundle. Tor browser is a modified version of Mozilla Firefox along with other applications that allow you to connect to the Dark Web.

#### **Installing Tor**

The next step after downloading Tor is, of course, installing it. Installing Tor on a USB stick on a Windows system is easy as the Tor Browser is nothing but a bundle of EXE on the OS. You can install it like any other Windows program. However, the main difference between other programs and Tor is its default location is your desktop.

The Tor bundle installs itself on the desktop because it is a portable application and does not integrate and communicate with your OS like other software. What this means is that you can use the browser from anywhere you want. Just copy the folder

to a USB drive, and you can use it on any computer you want.

While installing the browser, when the 'Choose Where to Install' window pops up, just select your desired location and the browser will be installed there. As said earlier you could also choose USB drive. Once you select the location, just click on Install and the program will be installed in no time.

### **Using the Tor Browser**

Once the installation is done, you will see a folder in your desired location called Tor Browser. This is it. Open the folder, and here you will see an EXE file called 'Start Tor Browser.' Open this file to open a window. A window will pop up with options of configuring proxies or Direct Access. Unless you want to set up proxies, click on the direct option and then click connect. After a few seconds, a new Firefox window will appear. Congratulations, you are now connected to the Tor net. Now you can browse the Internet with almost total anonymity.

To check whether you are on Tor or not just go to [whatismyip.com](http://whatismyip.com). This site detects your IP and location and displays it on a webpage. If you are on Tor network, the site will display a place that is not your location. Remember, you are using a browser; hence, only the activities on the browser are anonymous, everything else outside the browser is still unsafe.

It is recommended that you always connect to HTTPS sites instead of HTTP sites. The sites you visit should have TSL or SSL encryption to protect your

identity. If the sites are not encrypted, your privacy can be threatened.

Do remember that anonymity does not equal to protection from malware and viruses. If you visit illicit and shady parts of the Internet, it is possible that you may download viruses. This malware can also threaten your security and privacy.

## **How to use Deep Web on a phone**

Although Deep web and Dark web are often only associated with computers, it is now possible to access these annals of Internet using your smartphones. However, it is necessary to take ample care and precautions while trying to access the Dark Net on any smartphone.

There exist many methods of accessing the Dark web using phones. These methods depend upon the phone model, its OS, the version of the OS, your carrier, your nation, etc. Mostly Android and sometimes iOS are used to access the Dark Web on the phone.

## **How to Access Deep Web on an Android Phone**

The best way to access the Dark web on an Android phone or device is using an app called Orbot. It is an app that allows you to connect to the Tor network. To access content on the Dark web, follow the following steps.

- Download the Orbot app and let it install.
- Once installed, open the app and long press the round switch that is displayed on the

screen of your phone.

- Once done, head over to the Play Store and download one of the following apps- Orfox or Orweb. These two are browsers that are to be used to access the Dark web.

You can use these browsers to access the sites on the Tor network.

### **How to access Tor on an iPhone**

Like Orweb the Apple App store too has a browser called the 'Onion Browser.' It has the same basic features as that of the Orweb browser; however, it is configured according to the iOS.

### **I2P**

I2P is not as popular as Tor however it is available for Android as well as iOS too. You can find I2P on the Play Store.

I2P is not recommended for beginners, as it is hard to configure, as you need to do it manually unlike Tor. You need to configure and manage your proxy as well as VPN settings, to enable your device to connect to the network properly and without any problem. If you are interested in I2P, you can find many good tutorials on how to set it up on YouTube.

Other than the tools mentioned above, there exist various other tools and apps that can be used on cellular devices. You can also use apps like Psiphon, CyberGhost VPN, and TunnelBear for the added benefit of encryption while surfing the dark web.

Remember; always be careful, your identity is sacred.



## Chapter 4: Darknet Markets

Till now we have seen the basics of the Dark Web and how to access it. However, now you must be wondering how to access web pages on the Dark Web. In this chapter let us have a look at the most popular web pages on the Dark web, the Dark Markets.

Dark Markets have become such an integral part of the Dark Web that the two terms have become almost synonymous for Surface web users. Everything evil that you associate with the Dark Web is often related to the Dark Markets. The Dark Markets are also known as E-Black Markets where you can find goods and products that are normally not available on the surface web. These often-shady markets are places where customers use Bitcoin, and similar cryptocurrencies to buy anything from weapons to drugs, escorts and stolen credit card details as well. Some bold shoppers can use Bitcoins and other cryptocurrencies to purchase things like illegal drugs, guns and stolen credit card details. If you have ever been curious about how these markets work how to access them, you can find complete information regarding them in this chapter.

One of the most common myths associated with Dark markets and Dark web is that they are free of any rules and conditions. However, this is not the case, as the sellers cannot simply sell anything they want and they have to follow the rules. You can buy illegal goods off the Dark markets however it is also necessary to understand the sellers need to follow strict rules. Sellers cannot sell videos showing violence, poison, weapons of mass

destruction and explosives. Some marketplaces also do not allow sellers to sell weapons and guns even in nations where guns are legal like the USA. Some markets don't allow stolen IDs, stolen credit card information, and other such stuff as well.

The most commonly found and bought stuff on the Dark market is drugs. Drugs include recreational drugs like marijuana as well as prescription medicines. You can also find counterfeit accessories, clothes, jewelry, etc. You can also find legal products like pepper spray, software, e-books, etc.

One of the important things that you should remember while using dark markets is that they have 'down' time. This means that most of the markets go offline once in a while, so if you are trying to visit your favorite market and you cannot; do not worry, it will be back in no time. If it does not come back soon, then it has probably been taken down by the administration. This is quite common on the Dark Web.

Remember to always protect your privacy when you want to access the dark markets. You can use Tor or I2P to access these markets. Both these networks offer you an opportunity to be anonymous.

Tor is the most popular of all the services that promise anonymity, which is why it is also highly recommended. You can find all the sites mentioned in this chapter on the Tor network with ease. Use the instructions mentioned in the last chapter to install Tor.

You don't need to use a VPN with Tor, as it is not

required. However, you can use one if you want to secure your normal, surface web browsing as well.

## CryptoCurrency & Payments

Once that you have installed Tor on your computer, you are ready to use the Onion network. However, you cannot start buying immediately after you set up the Tor browser, as the transactions on the Dark web do not use 'real world' currency. All the safe transactions on the Dark web are done by using digital money. If you buy items over the Dark web using your PayPal account or credit card, you will compromise your anonymity along with your privacy. The most common form of currency used on the Dark Web is Bitcoin and alt coins.

You can create an anonymous wallet using Bitcoin. However, the process is not entirely anonymous. The payments that are made using Bitcoin are stored on the blockchain, and it is public. Anyone can view the blockchain. It is recommended that you use some mixing service while transferring coins to your market wallet. By doing this, you can confuse anyone who is trying to track.

One of the best methods of buying coins is using peer-to-peer exchange services such as LocalBitcoins. Wallet services like Coinbase come with a built-in wallet, which makes the whole process a bit easy. Remember the exchange rate is not always constant, and it is possible that the rate might fluctuate after you convert your money; hence it is always recommended to buy more coins than you need just to be on the safe side. Don't worry; you can sell the remaining coins. You need to

provide ID to buy coins hence if you are afraid about your anonymity; it is recommended that you transfer them to your market wallet using a 'coin mixer.'

You can also use fake ID to buy the coins. Coin mixers are simple to use services. Instead of depositing your money in the market's value directly, these services provide you with a new address where you can make the payment. They then send the clean coins to the market making it almost impossible to track any transaction back to you. These services only charge 1-2% of the whole transaction and honestly, it is a small price for your anonymity. Coinmixer.se is one of the most popular coin mixers.

Many markets also have their coin mixing services and disposable addresses for an added layer of security. Some markets will also accept other forms of payment like Dashcoin. These coins have their special anonymity features built-in.

## **Escrow and Multi-Sig**

Buying from a stranger online- on the surface web or dark web is a risky business. You need to be careful whenever you decide to buy anything. One of the most frequent complaints regarding the dark markets is a seller disappearing with your money. It has been observed that sellers accept your money and just disappear without sending you the ordered goods. Almost all the popular markets have a rating system where you can check the ratings of a seller. This works like the Surface web markets if a seller has a high rating it is unlikely that they will disappear

with your coins. However, ratings are not the only thing that you should check as ratings can be faked. With this, it is also possible that the thing you need is only available with a seller who is new and has no rating. So what can be done in such a case?

Using escrow service can solve the above problem. Escrow is a third party in the transaction that is sort of a judge between you and the seller. Often administrators of the market act as escrows. Often markets use central escrow services that hold your coins and do not forward it to the seller until you get your product. However, if the product never comes, then you can ask for a refund from the escrow. This method has reduced vendor side scams, however, the escrow themselves can scam you in this system. Rest assured; not many cases have been reported of such scams, and hence you need not worry. Just for the added security, it is recommended that you use only reputed and popular sites.

An alternative to escrow is multi-sig, which is safer as compared to escrow. However, it is also more difficult to set up and thus, not offered by many markets. It can protect you from vendor side scams as well as escrow scams.

## **Popular Dark Markets**

Here is a list of some of the most popular Dark Markets that are available today. These markets are full of illegal and legal products hence user discretion is advised.

The websites on Dark Web often go down temporarily

so if any of the links given below do not seem to work, wait and try again after some time. If the link does not work after a few days, it might have become defunct.

### **Dream Market**

Dream Market is a well-made and quite established Dark Market. You can find almost all kinds of products in this market. It is fast, faster than other websites on the Dark Net. It is also very easy to use. It is quite reliable and thus is highly popular. It has a few added features to make it even safer. It only uses admin provided escrow service. The site generates a PIN when you sign up for the site. This PIN is an added benefit that works along with your password.

Link: <http://lchudifyeqm4ldjj.onion/?ai=88551>

### **Valhalla**

It is a popular European site that offers to ship all over the world, which has made it quite popular. It invites only and hence you can only access it using the link given below. Valhalla is popular for its large collection of drugs. It also has prescription drugs like Ritalin, Adderall, Viagra, anti-depressants, painkillers, etc.

Link: <Http://valhallaxmn3fydu.onion/register/Nyr2>

### **Alpha Bay**

Alpha Bay is a popular Dark Web market. It is often used for 'carding.' It has both central escrow and multi-sig escrow admin options. It has an 'auto-

shop' feature through which you can buy a bulk of hacked accounts from sites such as Netflix, PayPal, Facebook, etc. You can also 'auto-shop' stolen credit card details from this market. It also stocks weapons, drugs, and other products.

Main Link: <http://alphabaymarket.com/>

Other Links:

- [alphabaywyjrktqn.onion](http://alphabaywyjrktqn.onion)
- [zdfvqospmrbvzdn3.onion](http://zdfvqospmrbvzdn3.onion)
- [stbux7lrtpegcra2.onion](http://stbux7lrtpegcra2.onion)
- [jsbpbdf6mpw6s2oz.onion](http://jsbpbdf6mpw6s2oz.onion)

### **The Real Deal**

The Real Deal is one of the safest markets on the Dark Web. It has a multi-sig escrow with the option of using external Bitcoin wallet. You can also create a wallet on the site itself using client-side key generation. What this means is that the site's administrator can never escape with your money or steal it either.

The Real Deal is often used for trading hacking software and information, but it also stocks drugs, guns, weapons, etc. It has an option of two-factor authentication to make it even safer.

Link: [trdealimgn4uvm42g.onion](http://trdealimgn4uvm42g.onion)

### **Crypto Market**

Crypto Market is most famous for drugs; however, you

can find other products on it as well. It is possible to choose your desired currency on the site so that you can check the price with ease. It has a large selection of special offers and deals that you can grab. Many sellers also offer free samples of their products if you are willing to pay the shipping. It is admin escrow only, though.

Link: <http://cryptomktgxdn2zd.onion>

### **Middle Earth Marketplace**

Middle Earth Marketplace has a large inventory of products as well. You can find a variety of products on this market. It is quite well known for drugs. It has a beautiful interface and is quite pleasant to use. However, it uses JavaScript by default, which is considered to be a security risk. However, it is possible to disable it using Tor.

One problem with MEM is that it does not offer altcoin and multi-sig payments. If you want to use these methods of payment, it is recommended to use other markets.

Link: [mango7u3rivtwxy7.onion](http://mango7u3rivtwxy7.onion)

### **Oxygen**

This market has a large range of products and it also has a multi-sig option. It also has an admin escrow service.

Link: [o2oxycuvnwxhv73e.onion](http://o2oxycuvnwxhv73e.onion)



## Chapter 5: How to Use Bitcoin?

Bitcoin is the most famous digital currency and is often associated with the Dark web. People believe that it is a form of anonymous currency and is basically a digital version of the real-world, physical cash. However, this is not true as Bitcoin is not a truly anonymous currency.

Using Bitcoin is as easy as downloading software on your computer. As Bitcoin is not a centralized currency, you do not even need to register an account with your personal details to use it. When you get an ID, you can create addresses. These then become your online identity on the particular network. It is comparatively more private and secure as compared to regular digital payment methods as it works on the anonymous network.

However, as mentioned earlier, Bitcoin is not entirely anonymous, and it is possible to track its users. All the transactions done using Bitcoin are stored on a public record called blockchain. As this record is public anyone with little technical knowledge can access it, it compromises your anonymity.

Hence, even if your personal identity is not connected to your wallet, all the transactions done using the wallet are public, and it is possible to track you using them. There exist many ways to track the transactions back to your personal ID.

Most of the markets and traders need some ID while

buying or selling goods. Unless you provide them with ID, you cannot continue with the transaction.

However, don't worry, there exist many methods how you can solve the problem.

## **Using Bitcoin Privately: A Guide**

### **Using Disposable Addresses**

Users get the option of creating as many as addresses possible when you download a wallet. However, most of the users create a couple of addresses and stick to them. This practice is extremely unsafe and is not recommended for anyone who wants to protect his or her privacy online. If someone is observing your activities, it becomes incredibly easy for them to make your profile if you keep on using the same addresses every time. These people can then use your profile for advertising purposes as well as other more sinister reasons too. It is also possible to use this profile and track down your personal identity.

Always remember, Bitcoin addresses are not supposed to be permanent addresses. Always change them as much as possible. Each time you receive a payment create a new address just to be safe. Do not use this address again.

If you use a desktop wallet, you can create as many addresses as possible. As an added benefit, all the addresses that you create are always connected to your account, hence if someone pays you on one of your old accounts, the money will still come through.

## **Bitcoin Mixing**

Along with disposable addresses, you can also use Bitcoin mixing to enhance your anonymity. Whenever you want to send a payment to someone, use this service for an added layer of privacy. What Bitcoin mixing does is that it mixes your money with a large source of coins before sending them to the destination. This makes it impossible to track and link anyone. Thus, an observer cannot link the transactions to your account.

One of the most frequently used coin-mixing services is CoinMixer.se. It is reasonably priced and is easy to use. However, you can also find various other services online that offer the same features. It is recommended that you only choose sites that are popular and highly recommended, as there exist many scam sites that can disappear with your coins.

## **How to trade Bitcoins anonymously**

If you do not want to connect your Bitcoin transactions to your personal identity, it is possible using a few methods.

The riskiest part of Bitcoin transaction is buying the coins. Most of the sites where Bitcoin are sold need your personal ID documents. Unless you provide them with satisfactory proofs, you cannot buy the coins. This is done to avoid money laundering lawsuits, You will find some methods of making this process anonymous below, however, most of these are expert level methods and hence if you are not comfortable using them, it is recommended you stick to coin mixing for now.

## Using peer-to-peer exchange

It is possible to buy Bitcoin from other individuals on the web. Buying them from individuals is more private than buying them from a company. Here are the websites where you do not need to provide personal details or verify them for buying Bitcoin.

Bitsquare service is completely decentralized where you can trade Bitcoin with an individual without the need of any service provider. You just have to use P2P software instead of visiting a website. When you download this software it automatically creates you own hidden service or site on the Tor network and provides you with a .onion address. No registration required, however, you do need to provide a minuscule security deposit of 0.01 Bitcoin, so if you do not have one already, you cannot use this service. It is one of the best methods of staying anonymous while buying Bitcoin.

LocalBitcoins is a popular peer-to-peer service for purchasing and selling coins, which is available in a wide range of nations around the globe. You have the option of keeping your identity hidden while using this service. Other clients will likewise have the choice of trading with anonymous clients. They can also require ID.

- MultiSigna - As the name suggests, this site uses multi-sig technology for all trades, which means that you don't have to trust your coins to the exchange for safe keeping, or depend on the exchange to keep their personal internal books correct - all the things are on the blockchain. As the clients of dead

exchanges like Mt Gox will testify, this is a major asset as far as security is concerned. Furthermore, it also makes it more decentralized and peer-to-peer as compared with other options. The fees are quite low, just around 0.5% of the total transaction. If you become a regular dealer, you can also avail discount to reduce the fee.

- Coinffeine - It is a peer-to-peer as well as decentralized exchange. Right now it only uses OKPay, a service that has its identification needs, however, you do not need to share your private information with the Coinffeine. It is estimated that the service will soon add other payment shortly.

## Security

Whenever you make a transaction on LocalBitcoins, clients who are especially worried about their security ought to payment in real or physical money. This is especially important if you are planning to buy costly things, as the cost of the goods can itself trigger your bank and lead to an investigation. If you only make small transactions it is not necessary, however, it is recommended. There are two methods of doing this: an in-person exchange where you get together with someone (often a person who requires a large trade so that it is worthwhile for you and them as well), or 'cash deposit' where you go to a branch of the vendor's bank and deposit cash directly in their bank account. When you sign in just click on 'purchase Bitcoins,' then click on the link 'show more', which is often underneath the top offers. The show more

option will display a list of various payment methods from which you can select 'cash deposit.' Now you will only see sellers who want are ready to use 'cash deposit ' method.

### **ID Verification**

There exists an ID verification system on the LocalBitcoins page however it is not mandatory. Some sellers do require this, however, most of them do not. Some sellers probably will also ask for your ID in private message. Sharing your ID with a person is far better than sharing it with a site. However, some people might still be uncomfortable about this. Sellers often put in their requirements in their ads to avoid any confusion. You can also message the seller and inquire about the details before doing any transaction.

### **Stealth Addresses**

Stealth addresses are relatively new feature that has been added to the whole transaction. It allows clients to generate a new address to represent their Bitcoin address. This means that you can access the coins that are sent to this address safely, without anyone ever knowing their true destination. However, to avail this function a wallet is required, and it is not a widely popular feature. If you still want to try this feature, you can use the Dark Wallet service. It is an extension for Google Chrome and has many privacy features along with stealth addresses.

### **Taint Analysis**


If you have used a coin mixer, then it is possible

to check how concrete its security services are working with a taint analysis. This analysis displays what addresses have sent coins to your address and is a decent way to see if the mixing service is working according to your desire or not. The Internet is full of Taint Analysis services hence if one does not work for you well you can just pick another one.

You can also perform an analysis using the Blockchain website. As an example here is a link. Simply replace the BTC address with your address in the URL to conduct your Taint analysis.

<https://blockchain.info/taint/1dice6GV5Rz2iaifPvX7RM>

For instance, it is possible to enter the address presented to you for a market and check whether any outsider would be able to profile you and trace you. It is recommended that your personal ID should not show up in the list when you do this sort of test. If not, it should at least come with a low taint ratio, which means the observer cannot be sure of your identity.



## Chapter 6: Do's and Don't s

Tor is one of the best ways of staying anonymous online. It can keep your network protected and secure, and your identity was hidden. It is becoming a necessity in today's world where everyone is on your back. However, Tor itself can do nothing, as it is not a magic wand. Unless you take ample care and precautions, Tor cannot protect you. Tor is like an umbrella, if you don't know how to use one, you are going to get wet. Similarly, it is necessary to know how to use Tor and what to avoid when using it. In this chapter, let us have a look at some of the most common Do's and Don'ts of Tor.

### Do try Tor

Do not be afraid of trying Tor. It is possible that you might have heard various rumors about Tor; however, most of them are exaggerated. Unless you try Tor, you won't be able to understand how useful it is.

Everyone who is worried about his or her security online should try using Tor. Do not trust anyone including your ISPs, government agencies, service providers, etc. You can use Tor for a variety of sensitive purposes such as browsing, surfing, reporting, etc. Do read the chapter on the uses of Tor to know how Tor can be used for your and others' benefit.



## **Don't use Windows or Use it Wisely**

Windows maybe one of the most popular platforms but it is not that suitable for Tor. As you know, Tor is a way of helping you to stay anonymous on the Internet and keeping your data private. Unfortunately, Windows goes against these basic principles, as it is often full of security bugs and holes. It is highly vulnerable to attacks even if you Tor. Thus, it is possible that your privacy might be breached if you use Tor on Windows.

The best OS to use with Tor is using Tor-configured Linux system. Whonix, Tails are some of the popular Linux systems currently available.

### **Always update your system**

News ways of attacking a system are found almost daily making your system vulnerable. It is thus extremely necessary to update your system regularly and preferably daily. It is recommended that you update your Tor Client, your browsers, your antivirus and your OS as well.

Remember, Tor is only useful if your computer is secure. If a hacker gets into your system, not even Tor can protect your identity and anonymity. Therefore, it is extremely necessary to keep your system up-to-date.

### **Avoid HTTP Websites**

The Onion Router i.e. Tor only routes your traffic. It is not a complete solution for data encryption. Thus, Tor only encrypts and routes your traffic inside its network; however, everything out of it is

still vulnerable. It denotes that Tor anonymizes the source of your network and encodes data inside the Tor; however, it doesn't encode your Internet usage outside the network.

What this means is that the exit nodes of the network can read your Internet traffic if it is not encrypted and is in plain format. This is why it is necessary to use end-to-end encryption methods while doing anything on the network. Popular end-to-end services include SSL and TLS. These services can only be used on HTTPS websites, thus using HTTP should be avoided.

If you don't know which websites use HTTPS, you can download an extension called HTTPS Everywhere that automatically switches to HTTPS mode whenever it is available.

### **Don't get confused between Dark Web and Deep Web**

Although covered more than once already, this is still a confusion that might plague most of the beginners.

Remember Tor is not made for accessing the Deep Web. Yes, it can access the Deep Web; however, any other browser can do so as well. You often stumble into Deep web while browsing Surface web without your knowledge.

Remember the definition of Deep Web; it is anything that is not indexed by popular search engines. So for instance, if you search for something on a site

and the results come out in a pop-up window, it is safe to assume that the pop-up is not indexed, and thus by definition- congratulations, you have just visited Deep web.

The Dark Web is a part of Deep Web as it cannot be accessed/ indexed by search engines. However, it is quite different than Deep Web, as simple, regular browsers cannot access it. It needs special software out of which Tor is one.

Tor connects to a massive network called Tor network that helps you establish a private connection. By using Tor, you can access all your regular websites that are available on surface web and all the URL ending with .onion. These .onion URL are nothing but Dark Web URLs.

### **Encrypt Everything**

As said in the last point, Tor is nothing but a router that is used to keep you anonymous. However, it cannot secure the data that is present on your computer. The data can only be made secure if you use a strong cryptographic program or algorithm.

Two of the most commonly used services for data encryption are TrueCrypt and LUKS. These can keep your data well protected on Linux systems.

### **Never use Java, JavaScript, Flash**

Active content is bane for your data and anonymity. This content like JavaScript, Adobe Flash, VBScript, QuickTime, Java, ActiveX controls, etc. are binary applications that have the same privileges that your

user account has and thus they can access and share your data as well! Tor cannot protect you if you insist on using these active components.

Flash and JavaScript run in virtual machine that can easily bypass your proxy settings and thus can access and share your data as well. Tor currently does not have the capability of protecting you against these scripts.

Other than the reasons mentioned above, active components are also cookies hoarder. They store your browsing data and cookies separately. These data are often difficult to access and delete and hence is vulnerable to attacks. If you want to increase your security, it is highly recommended disabling these services.

### **Avoid P2P**

Do not use P2P while using Tor as it slows down the network for everyone. Tor is not made and configured to handle P2P yet and although it is possible to use it for file sharing it is not recommended as it makes the whole network slow and problematic. Exit nodes of the Tor network are configured to block file sharing.

However, if you still manage to find a way of downloading data from Tor do remember that you are jeopardizing your anonymity. BitTorrent is not safe on Tor, and it can compromise your anonymity and security. BitTorrent clients are not secure as they send your IP address to the peers and Trackers directly, bypassing Tor; hence it is never anonymous, even if you use Tor.

### **Always delete your browsing data and cookies**

Cookies are essential for websites to work, however, they can prove to be a nuisance if not cleaned regularly. Not only can cookies slow down your system by hogging memory, but they can also compromise your anonymity.

Websites can use cookies and temporary files to track your online doings, and by analyzing them and your overall Internet usage, they can many times guess your identity.

It is necessary to delete your local site data and cookies every time you use Tor and other browsers as well. You can use a variety of software to clean your cookies in one click. One of the most popular applications is Ccleaner. You can also install extensions like Self-Destructing Cookies that automatically deletes your cookies.

### **Never use your personal details**

This tip might seem stupid, but you will be surprised to know a large number of people use their personal details while using Tor. Once again, it is necessary to remember that Tor is a mere router and it won't protect your identity if you decide to.

If you still decided to use the websites mentioned above while using Tor, it is recommended that you use different accounts instead of using your personal ones. It is recommended that you use accounts that cannot be traced back to you in any possible way.

If you want to be truly anonymous, it is recommended that you invest in a virtual identity. A virtual identity with no connection to your real identity whatsoever can keep your real identity safe and secure.

### **Avoid Google as much as possible**

Google is a data hoarder. It does not care about your privacy at all and can access everything that you put on it. This is true about all of Google's products, including YouTube, Gmail, the search engine, etc. Google uses your private data to show you custom ads.

If you want to use a search engine, then it is recommended that you use DuckDuckGo or Startpage. Both of these services are quite adept and do not track you. They do not log your IP and do not store cookies on your PC either. Thus these search engines are security compliant. These also work on surface web.

### **Always use trusted directories to find links**

Let us assume that you have installed Tor and wanted to access the Dark Web, however; you must be confused where to go now. This is a common problem, as Tor does not come with links and information regarding how to access the Dark Web. However, the Internet is full of various resources that are nothing but directories of various Dark Web sites, often accompanied with short descriptions. You can find some of the most popular directories in the 'Resources' chapter of this book.

One of the most frequently used directories of the

Dark Web is The Hidden Wiki.  
<http://zqktlwi4fecvo6ri.onion>

What is essential to remember about the Hidden Wiki is that it is an extensive collection of links and hence it is possible that you might find harmful and illegal links on it. Do not access these links unless you want to get arrested. If you ignore the illegal content, you can find various useful sites on the wiki including links to secure email services, secure social networks, chat rooms, message boards, etc. Never click on suspicious-looking links and avoid anything that seems even remotely illegal.

While browsing the Dark web, you will always come across links and web pages that are illegal and dangerous. It is full of web pages that represent some of the darkest aspects of humanity. For instance, it has websites featuring child pornography, human trafficking, drug trafficking, theft, weapon trading, gore, etc. It is an unavoidable and unfortunately indivisible part of the Dark Web. Hence, it is extremely necessary always to check the source of the link that you are about to click. If you think that a link seems suspicious, avoid it.

Even after taking all the precautions mentioned in this book, it is possible that you may accidentally stumble upon illegal content. Don't panic, just close the window and clear your cookies and temporary folder. Do try to avoid such links in future, though.

Remember, you are on your own on the Dark Web, do

not trust anyone and always act appropriately.



## Chapter 7: Dark Web Resources

The Dark Web is full of many secrets, and most of these secrets can be utilized. Dark Web has many websites that are quite useful and that are not available on Surface Web. You can find a variety of products on the Dark Web that are not available elsewhere. Let us have a look at some of the most popular Dark Web resources here. This chapter can be used as a beginning point for your Dark Web journey. However, do remember all the tips mentioned in the chapter above.

### The Silk Road

<http://silkroadvb5piz3r.onion>

The most famous website on Dark Web, The Silk Road is almost synonymous with the Dark web. A marketplace where you can find almost everything, it is well known for selling drugs and weapons. However, you can also find books and other random things here. All the trading is done using Bitcoin.

Being the most popular sites, it is also one of the most monitored ones. It had become defunct recently thanks to the bust conducted by the US, however, apparently it is still working using different names and URL. It is advised to beware and cautious while trying to visit this site.

### Tor Mail

<http://jhiwjjlqpyawmpjx.onion>

Unless it is already clear, Gmail is not secure. Your emails and all other personal details are not secure on Gmail and most of the popular email services. However, you can find a good email service on the Tor network that is secure and safe.

The Tor mail system is guaranteed privacy and anonymity and is frequently used to help people out of the network as well. It is a brilliant service that once set can help you keep track of your private and public communications.

## **The Hidden Wiki**

<http://7jguhsfwruviatqe.onion>

The Hidden Wiki is as the title suggests a wiki that is hidden, nothing special there. However, unlike its name, it is not hidden, as it is accessible using surface web as well. It is the beginning point for every person who wants to start using Tor. It is basically an index/ list of various sites that can be found on the Dark Web. It also has short descriptions of the sites so that you know beforehand what you are getting into.

## **Hidden Wiki is usually up**

**TorDIR**

<http://dppmfxaacucguzpc.onion>

Like Hidden Wiki, TorDIR is a list of hidden sites, and services that are available on the Dark Web. It is a highly stable site and is well known amongst beginners. It features a concrete collection of sites. An added feature of TorDIR is that it has an

option of adding comments.

### **Core.Onion**

<http://eqt5g4fuenphqinx.onion>

The Onion Core is another comprehensive collection of sites that are available on the Dark Web. It is a collection of links from which you can branch out. What makes this directory special is that it does not have Child Porn and thus is very safe. It does not have other 'dark' parts of the web as well.

### **Hash Party**

<http://3terbsb5mmmdyhse.onion>

Hash party is a site where you can reverse other people's hashes. You can also request hashes. It is one of the most famous Black Hat resources available on the Dark Web.

### **FBGB Cracking for Bitcoin**

<http://rgvawpnaahbla3seq.onion>

If you require a hash to be cracked however are not extremely tech savvy? This site might help you. For a few Bitcoin, you can have any WPA/WPA2 password broken. However, like every other site on the Dark Net, please be careful before you use it.

### **TorLinks**

<http://torlinkbgs6aabns.onion>

Another great directory of .onion links, TorLinks is far more extensive than TorDIR. It has many more links as compared to TorDIR, so if you exhaust

TorDIR move on to TorLinks.

### **HackBB**

<http://clsvtzwzdgzkjda7.onion>

HackBB is a large community board for everyone to talk about hacking and related things. Everyone - amateurs and professionals alike, use it. You can get into discussions and learn new things using this board. It is a safe resource to learn about things that are not normally discussed on the surface web.

### **Freedom Hosting**

<http://xqz3u5drneuzhaeo.onion>

Freedom Hosting, as the name suggests gives you space to host your sites. It is free, and you stay anonymous. You are allowed to host anything you want on the service, however, the content should be legal according to the US laws. Most of the sites on the Onion network are hosted using this service.

Other than the sites mentioned above, there exist many other resources that can be used to access the Dark Web. However, like it is impossible to teach anyone how to use the Internet, it is also impossible to teach Dark Web as well. You need to browse and surf to understand it and use it properly. The directories mentioned above are great starting points that can often lead to whatever contents you are trying to find. Just remember, be safe and careful.

## Chapter 8: FAQs

Till now we have seen an in-depth account of Tor and the Dark Web. I am sure that you must be curious about accessing the labyrinth that is the Dark Web. However, there still might be some issues in your mind regarding Dark Web, Tor, and Deep Web. In this chapter, let us have a look at some of the most frequently asked questions and queries regarding the above topics.

### **Difference between Surface Web, Dark Web, and Deep Web**

Though covered throughout the book, let's us once again revise what we have learned so far. The terms Surface the Web, Dark Web and Deep Web can confuse any beginner and sometimes professionals as well. However, here are the simplest descriptions of the webs.

#### **Surface Web**

Surface web is nothing but the regular web that you and I access every day. It is the web that we use to talk with our friends, read news, play games, shop, etc. Basically, it is the 'regular' Internet.

#### **Deep Web**

Deep Web is the part of the Internet. This part is almost hidden and is not indexed by most of the major search engines. Thus, it does not turn up on your Google/ Yahoo results. To visit the pages on deep web, you need to visit them directly using their URLs. In simple words, deep web is everything

that cannot be seen by search engines thanks to the sheer size of the Internet.

## **Dark Web**

The Dark web or the Dark net is a part or subsection of Deep web; however, it is a bit different than the deep web. You can normally access deep web using your regular tools and software; however, it is not the case with Dark web. You need special software to access it. Dark web is notorious for the various illegal and illicit activities that go on it. Some of these activities include trading of drugs, gambling, illegal pornography, etc. It also allegedly it also harbors other forms of criminal activities.

Though the Dark web is used for a variety of illegal activities, it has many legitimate and legal uses as well. You can find the uses in the chapter above.

### **When was the Dark Net invented?**

The Darknet was not invented per se; however, the first hidden websites started appearing around the year 2004. Thus, 2004 is supposed to be the year when Darknet was 'invented.

### **Why was TOR formed?**

The US government formed Tor for anonymous communication and to keep its messages encrypted. Thus, the US government funded it.

### **Why is Tor so slow?**

Before answering the question, it is necessary to acknowledge that, yes, Tor is slow. It is also necessary to recognize that Tor will always be slow and there exist many reasons why this is the case.

Tor cannot ever become as fast as the Surface Web because it does not work like your regular browser. Your traffic is channeled and bounced through various systems all over the world, and it is obvious that some network latency will creep in. It is childish to expect a blazing fast bandwidth while using Tor. However, it is possible to improve the overall speed of the Tor network. The ratio of the number of users to the network is extremely low right now, and many of these users do not comprehend that Tor cannot handle the load file sharing. This often slows down the network. However, you can help Tor:

Configure your browser to become a relay: By making your browser a relay you can help the network to expand that can help the overall speed and quality of the network. You can also find sponsors for Tor to help it. With this, you can also donate to the project. Remember, without funding Tor cannot survive.

So basically, Tor is slow because whatever you search on the network goes through multiple channels throughout the world. This makes the whole process anonymous. However, as the query is supposed to travel to multiple places, it is often slow. In my opinion, this is a minuscule price for your privacy.

## **What is Tor?**

"Tor" can be used to refer to a variety of different but related components. The first one and the most popular one is the browser bundle. Tor, therefore, is "The Onion Router."

In simplest terms, Tor is software that you can use on your system that can help you anonymize your browsing habits, along with granting you access to the Dark Web. It helps you stay anonymous by bouncing and channeling your search queries over a large network of relays, spread throughout the world. Volunteers run these relays, and the combined network is known as the Tor Network. What this bouncing does is that it secures you and prevents anyone from tracking you. This includes even the sites that you visit. It prevents the sites you visit from learning your physical location.

Tor Browser is a modified version of Mozilla Firefox. All the privacy issues present in Firefox are fixed in the Tor version. It is one of the most popular ways of accessing the Dark web.

Other than the above references, Tor is also used to refer The Tor Project. The Tor Project is a non-profit organization that runs, develops and maintains the Tor software.

### **I am scared, is the Dark Net safe?**

If you look at the world closely, you can observe that nothing is harmless unless correct precautions are taken. For instance, the surface web itself is full of virus, malware, and various other hazards but no one has stopped using it due to these. Similarly, Darknet too is full of a variety of



hazards, however, if you are not planning to do anything illegal and dodgy, you will be safe. To take the necessary precautions whenever you access the Dark Web, having good antivirus software is a must.

### **Does Tor work with Windows 10/7/xp?**

Yes, Tor works with the Windows operating system; however, I do not recommend it. Windows operating system is full of holes and a variety of problems, hence, even if you use Tor, some expert might be able to exploit one of these holes and use it to access your data. You can find more information regarding this on the Tor website.

### **What is the Hidden Wiki and where can I find it?**

The hidden wiki is a compilation of some of the most popular pages on the Tor network. You can link to the popular and not so popular pages on the hidden wiki. Here is the link: [kpvz7ki2v5agwt35.onion](http://kpvz7ki2v5agwt35.onion)

### **If Dark Web is so scary/illegal, why is it still working?**

That is because the Internet does not work like this. Deep Web and the Internet are synonymous. As said earlier, the Deep Web, as said above, is nothing but a part of the Internet; therefore 'deleting' the Deep Web is like 'deleting' the Internet. With this, it is impossible to keep an eye on the Internet, as it is a vast entity. People will always find new ways of exploiting it and therefore it is not plausible to keep it safe.

### **I don't like the sites mentioned in the Hidden Wiki, are there any other sites that I can access, where can I find them?**

Yes, the sites mentioned in the Hidden Wiki form just a tiny chunk of a variety of sites and pages that are on the Dark Web. You can find out a variety of forums and other groups that have lists of links arranged according to subjects. Reddit is a good source of links as well. You can also find links from various anonymous message boards. However, do check the source before visiting any link.

### **Is there Child Porn on the Dark Net? What if I accidentally see it? Will I be arrested?**

Yes, unfortunately, Dark web does have a considerable amount of Child Pornography, and it is also possible that you may come across some while browsing the web. However, do not worry, unless you were deliberately looking for CP (Child Porn) you won't be arrested. If you come across it, just close the tab and do not visit it again.

### **Are there any search engines for Tor?**

One of the most popular search engines on the Tor Network is TorCH. It can be found easily, and it can help you with search queries. If you want other search engines, you can find links to them on the Hidden Wiki.

### **Can I get addicted to Tor/Dark Web?**

Unfortunately, yes, you can get addicted to the Dark Web. The Dark Web, like the Surface web, can prove to be highly addictive if you know where to look. However, unlike Surface Web, the Dark Web is not totally safe and hence it is better to stay away from Tor if you don't want to get addicted.

## **What is to be avoided on Dark Net?**

To be honest, it is necessary to keep your morals aside while browsing the Dark Web. Although even if you plan on visiting only legal and 'good' site, it is possible that you might stumble upon unsavory sights that might sicken or offend you. You should expect to tumble on these sites accidentally if you decide to use Dark Web for a long period.

## **I browsed Dark Web, now what to do?**

It is recommended to clean your cache and browsing history after you browse the dark web. Cleaning your temporary folder is also recommended. You can use Ccleaner or any other similar software to clean your history, cookies and other details at the click of one button.

## **Is Tor basically a proxy? Why shouldn't I use proxy instead of Tor?**

No, Tor is not as simple as proxy. Tor is far more sophisticated way of staying anonymous online. To understand the difference between Tor and proxies, let us have a look at what proxies do. Proxies are provided by various providers, what they normally do is that they set a server somewhere other than your place/nation. Your queries, in another word, your traffic, is then related to their server. This gives you a certain amount of anonymity. It is also a very easy to construct and maintain architecture. All the users using this proxy go in and come out using the same server that reduces the cost of the service provider. The provider often charges the user for using their proxy, however, certain providers get their monetary benefits from ads.

Proxies are quite easy to use for the user as well. You do not have to download anything extra to use proxies. You do not have to carry anything with you to use proxies as well. Simply direct your browser to the proxy, and you are good to go. Proxies are good option if you do not need total anonymity and privacy and are okay with the provider accessing your data. Yes, the provider can access and use your data if you use proxies. The provider is aware of your identity as well as your browser history. The provider can see all the traffic that is channeled through their server. In many cases, these providers can trace your encrypted traffic as well. Thus, your banking details, your e-commerce details come under a risk if you use proxies. All of this becomes a trust game, and you have to trust the provider with your information.

For added benefit, some providers also use SSL. This adds a level of protection as it can keep you secure from eavesdroppers if you are using a public network.

Unfortunately, the simplicity of proxies is their bane as well. As simple proxies only use a single server, they are extremely vulnerable. The failure of the server can bring down the complete network effectively.

What makes Tor better than proxies is that it is not dependent on a single server. Your traffic or queries pass through at least three different servers before they are forwarded to the destination. Each of the above relay points is encrypted and thus giving you a strong, multilayered protection. Thus, even if someone is observing your

connection, they cannot access your data, cannot read it or cannot modify it either. The complete journey between your system and the receiving system is encrypted.

### **Doesn't the government back TOR? So, do they have a backdoor in Tor?**

This is one of the most prevalent myths regarding Tor. There is no backdoor whatsoever in Tor, and no one can access your data. A backdoor would ruin the whole experience, as it will remove a large chunk of the offered protection.

However, as Tor is software that is constantly updated it is possible that a few bugs might jeopardize your anonymity. But thanks to a large number of users, these bugs are found pretty soon, and a new update is released immediately. So, if you plan to use Tor for long term, it is recommended you download the latest, stable version whenever it is released.

### **Is it possible to share files using Tor? Will the process be anonymous as well?**

Yes, it is possible to use Tor to share files using Tor. However, it is not recommended to do so as the Tor network is not designed for file sharing. File sharing often slows down the network for everyone and causes a lot of problems. Exit nodes are often programmed to block file sharing on the network. A tip, do not use BitTorrent on Tor as it is not anonymous.

### **Can Tor be used on my cellular device?**

Yes, Tor is available on Android; however, the

Guardian project maintains it. Currently, no way of using Tor on iOS exists.

### **How can I check if Tor is working?**

The easiest way to check whether Tor is working correctly is to use a variety of sites available online. One of the most commonly used sites is Tor Check.

### **I do not like Tor, how do I uninstall it?**

In Windows, installing and uninstalling Tor Browser does not work with other software. Tor Browser installs in a different way as compared to other programs. You do not need to uninstall Tor, just delete the folder called Tor Browser, and it will be deleted from your system completely.

### **Is Tor safe? Or is it malware?**

It has been seen that Tor often triggers many antivirus software. However, most of these triggers are false warnings. It is recommended to contact your software support and report the files as false positives. However, do this only if you downloaded Tor from a reputed source.

### **Does Tor provide full anonymity?**

No, currently no technology exists to provide anyone with full and unbreakable anonymity. Let us see why Tor is not (yet) fully anonymous.

It is important to understand that Tor only protects your network; it cannot provide you full anonymity if you do not know what you are doing. It only

allows you to hide your location and identity by using layered encryption. However, it cannot interfere with data that you intend to post. Hence, if you decide to access Google or Facebook while using Tor, your anonymity will be jeopardized. Your ISP will not know that you are visiting Facebook and Facebook will not know your location, however, Facebook will obviously know who you are if you log in. Thus, a large part of anonymity is in your control, if you don't share your personal information, you will be safe.

Another thing that can compromise with your anonymity is the use of active content. JavaScript, Java, Adobe Flash, QuickTime, Adobe Shockwave, RealAudio, VBScript, Active X controls, etc. are all active contents and binary application. What makes binary applications different than others is that they work as your user account and have permissions to use your OS. What this means that they can access everything that you as a user can. Adobe Flash and Java work on the virtual machine. The virtual machine can often ignore your configurations and thus bypass Tor as well. These applications thus can share your data and compromise your privacy. This is why it is always advised to disable these active components while using Tor.

The Tor Browser, which is a modified version of Mozilla Firefox, is already configured to block all the risks that can hamper your privacy and anonymity. All the technologies mentioned above are disabled in the Tor Browser. It also comes with various extensions like Torbutton and NoScript thus making it an extremely safe browser.

## **Is Tor a form of VPN? Should I use VPN instead of Tor?**

Do not use VPN if you want to be completely anonymous. If you want to hide the fact that you are using Tor, it is recommended to use a private server as a bridge.

What VPN does is that it encrypts the transfer between the sender and the provider. Thus they are a sort of proxy between the destination and the user. But like proxies, VPNs too have a single point of failure. A sophisticated hacker can attack the VPN to get identity information related to the VPN. VPN provider can also be threatened to reveal the identities of the user. Thus VPNs are subjective to outside forces that can interfere with your privacy and anonymity.

Tor is better than VPN because your IP address changes almost every 10 minutes when you use it. It becomes almost impossible for websites to form any concrete profile using this data. As Tor uses three-hop circuit with deep encryption, no relay has enough information to reveal your identity or details thus making it infinitely safer than using a VPN.

## **Does Tor promote criminal activity? Can criminals use Tor to commit crimes?**

Yes, criminals can use Tor to commit crimes and no, Tor does not support criminals. Tor was not made by or made for criminals. Coming back to crime, as said above yes, criminals can use Tor to commit crimes. However, just look around you, criminals can use anything to commit crimes. It will be childish to assume that criminals do not use Surface Web to



organize their crimes.

Criminals have no moral obligation whatsoever; hence, instead of using Tor they have a variety of options to conduct their crimes. For instance, they can use stolen phone and dispose of them later. Criminals can also use malware, spyware, etc. to control computer systems anywhere in the world. So, yes criminals already have a lot of privacy. The aim of Tor is to provide this anonymity to common people as well.

It is necessary to understand that everything comes with a good side and a bad side. Tor has a bad side but so do other forms of Web. Hence, instead of shutting down Tor or bad-mouthing it, it is necessary to take action against these illegal activities so that Tor stays safe. Remember, the main motto of Tor is to provide common people with anonymity.

### **Why some videos don't work on Tor?**

Nowadays many sites need extra plugins like Flash. These plugins operate without the support of the browser and hence are free to conduct activities on your computer. This can compromise your privacy. This compromise includes disregard of proxy settings, accessing your IP address, storing cookies, etc. To avoid this, the Tor bundle blocks Flash plugins that in turn can mess up with video playing ability of certain sites.

### **Can I use Chrome/Opera/ IE etc. with Tor?**

The short answer to this question is no; you should not use any third party browser with Tor. Right now,

it is not possible to use third party browsers with Tor and get the same amount of protection as when Tor Browser is used without any addition.

### **Why does my Google page come out in weird languages?**

Google uses various services to give you a highly personal browsing experience. To display results in your local language, it often uses Geolocation. Using your location, it determines which language you probably use in your day-to-day life and includes it in your search queries; however, as Tor uses different relays, your IP address changes rapidly. As Google uses your IP to determine your location, Google often shows results in languages that are different than yours. This is not a bug of the Tor network; rather, it is a feature. It shows that the system is working properly.

If you want to avoid this, you can use nation specific sites such as Google.au, google.co.in etc.

### **Can/should I install my favorite Firefox extensions?**

Tor Browser is free software, and it is open source so you can modify it and manipulate it however you want. As it is just a modified version of Firefox, you can add any extension or add-on that is available for Firefox. However, I do not recommend adding any extension to the browser as often these can compromise your privacy. Many browsers often do fingerprinting and can also bypass proxies.

It is not necessary to download ad-blocker extension as well. Tor provides you with sufficient security and privacy, and it does not need any additional

support. These extensions can cause problems with some sites that can break the network as well. Hence, it is recommended to avoid any extension or add-on. However, you can use your extensions of your regular Firefox.

## Conclusion

Thank you again for purchasing this book!

I hope that the book has solved most of your queries regarding the dark web and has perhaps dispelled most of the myths associated with it. However, it is still necessary to understand that the Dark Web and Tor network are dangerous places and should be used with proper care.

Although I have mentioned many sites in the book that deal with illegal trades, it is not my intention to promote any illicit activity. The links have only been provided for your information, and I do not recommend using the marketplaces to buy illegal goods.

Do follow all the instruction given in the book carefully to avoid any mishaps. Remember, your identity is sacred; protect and cherish it.

Finally, if you enjoyed this book, then I'd like to ask you for a favor, would you be kind enough to leave a review for this book on Amazon? It'd be greatly appreciated!

Click [here](#) to leave a review for this book on Amazon!