

March 2020

THE DEEP WEB, THE DARK WEB AND DARKNETS:

**A guide to the unfamiliar dark reaches of the
Internet**



Todd G. Shipley

About the Author	2
Executive Summary	3
The Deep Web	4
Darknets	5
Tor-The Onion Router	5
I2P-The Invisible Internet Project.....	5
Accessing The Tor Project	6
Finding a Tor Hidden Service Website	6
References.....	8

Disclaimer:

The general use of the Internet is not without risk of seeing or hearing something that might be offensive. The use of other darker parts of the Internet as described herein add to the probability that a user will encounter some material that they find offensive and could be illegal to merely possess on your computer. We can't go without saying here that any persons going on any Darkweb tools or individual Darknets will most likely encounter offensive and illegal material. Downloading software and using it to access any of the material found in the back streets of the Internet are done so at your own risk. Our providing this document was done so for educational purposes and not to encourage any actions that might offend you. Users be ware! The author and Dark Intel assume no responsibility for any consequences resulting from use of any information obtained from this article or the sites mentioned. We are not responsible for, and expressly disclaim all liability for, damages of any kind arising out of use, reference to, or reliance on such information.

About the Author



Todd G. Shipley, CFE, CFCE
Author, Speaker, Cyber Explorer

Todd is an American Cyber Security expert and President of the High Technology Crime Investigation Association (HTCIA). He is a former Cyber Crimes Senior Detective Sergeant and a U.S.A.F combat veteran. He currently speaks and trains globally regarding technology investigations and the Darknet.

Todd has taught law enforcement investigators worldwide on Internet and Darknet investigation techniques. He started Dark Intel to continue providing Darknet Intelligence and investigative techniques to law enforcement and corporate investigators.

Executive Summary

The internet to most The Deep Web users is believed to be anything that Google's search engine has recorded and provides in its returns during a search. We once referred to this space as the World Wide Web. Often today's Internet user no longer looks for data beyond the use of a modern browser. There is much more to the Internet than the average browser can find. One of those is a space we refer to as the Deep Web. There are also areas referred to as the Dark Web and Darknets. These are places that Google has little vision of and can't access or record the contents.

This report presents a brief outline of what the Deep Web, Dark Web and Darknets are and how they are accessed.



The graphic above is the typical example of the visual depiction that describes the differences of the Regular or Surface web (think what Google see's) and hidden data in the deeper "Deep Web" and the further deeps of the Internet the "Darkweb" containing various tools called "Darknets". Darknet simply refers to a software based network that runs on top of the traditional Internets structure.

The Deep Web

The Deep web is a term used to describe a part of the Internet. This part is uniquely the area that Google, and the other Search Engines, can't access. A search engine is a software tool that is able to crawl (go from website to website) or follow hyperlinks (that blue link on every webpage to another webpage). The search engine crawler records what it finds and saves this information to a database. A crawler can only access a site if it has permission and has a compatible. Users then access that data through word queries at websites like www.google.com or www.bing.com.

But what happens to data that Google and the others can't access. Well by all accounts there is a lot of this data. Google can't access this data for a lot of good reasons. First, it is personal data about each of us. Google can't access and record data that is behind a username and password to login into a site. This could be your company network, a doctor's office, your bank or government servers.



Even sites like the New York Times have data that is not accessible to search engines. This is because they require payment to access the site. Lots of sites on the Internet are similar. Additionally, any database attached to the Internet, like searchable property records, are not generally a location that search engines can record data. So the Deep Web is really just data on the Internet that search engines can't access. It isn't really hidden or unknown, its just a specific site you have to go to and access yourself, no Google help there.

Darknets

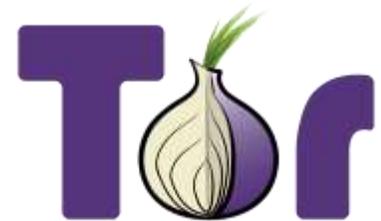
The Darkweb is not just data. The Darkweb describes a series of software tools. These tools allow a user to hide their online activities. These tools prevent Internet service providers (ISP's) or governments from eavesdropping on your browsing. Within the Darkweb are multiple tools individually called Darknets (Dark Networks). Some of the more common darknets include Tor and I2P.



Tor-The Onion Router

Tor or “The Onion Router” was developed by the United States Navy as a tool to hide military traffic over the Internet. It was later released as an open source tool and eventual development has continued under a non-profit corporation.

- According to the Tor Projects website the tool is designed to add privacy to a users Internet usage. Tor users can browse the Internet without being tracked.
- The Tor projects ability to surreptitious hide a users traffic is based on a complicated series of encrypted servers around the World.



I2P-The Invisible Internet Project

The invisible Internet Project was designed as a tool to provide privacy to a user's Internet communications. I2P is an anonymous network built on top of the internet but uses a Peer to Peer system of data transfer between users.



Accessing The Tor Project

Accessing the Tor network is as simple as going to www.torproject.org website and downloading the Tor software for your operating system and installing the software.



Once the software is installed the user can click on the Tor Icon on the desktop to start the newly installed Tor Browser. The Tor browser is uniquely designed to provide access the Tor Network. The Tor Browser uses the encrypted Tor network to hide the users activity. A user can go to websites on the regular Internet, such as www.google.com, and access the functions of the normal Internet. The Tor Browser also allows access to Tor specific websites hidden within the Tor network. These websites are commonly referred to as Hidden Services. These are not accessible from a regular browser or through the regular Internet. These Hidden Services are accessible only through the Tor network. A Tor Hidden Service prevents a user of the network from identifying the owner of a Hidden Service website. Additionally, the Tor network prevents that Hidden Service website from identifying specific users accessing that Tor Hidden Service website.



Finding a Tor Hidden Service Website

You can use Google on the regular Internet to research Tor sites. Keep in mind you have to put the unique Tor address in the Tor browser. These Tor Hidden Service website addresses are uniquely designed when a Tor Hidden Service is made. The address is either 16 or 56 random characters ending in “.onion”. An example address

is: o2seslcjo75fzu4d.onion. The TLD, or Top Level Domain, uniquely **.onion** for all Tor Hidden Service address. A TLD is a common function of the regular Internet but normally seen as .com, .org or .gov.

Finding Tor Hidden Service sites is as simple as going to a list of sites on the regular Internet such as:

- The Hidden Wiki <http://thehiddenwiki.org/>
- The Tor Hidden Wiki <http://torhiddenwiki.com/>

On the Tor network you can use similar sites such as:

- The Hidden Wiki http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page
- Hidden Wiki <http://hwikis25cffertqe.onion>

Tor has Google style search engines that can be also used such as:

- Torch <http://xmh57jrznw6insl.onion/>
- Not Evil <http://hss3uro2hsxfogfq.onion/>



References

1. Dark Intel www.darkintel.info
2. The Tor Project www.torproject.org
3. I2P-The Invisible Internet Project <https://geti2p.net/en/>
4. The Hidden Wiki <http://thehiddenwiki.org/>
5. The Tor Hidden Wiki <http://torhiddenwiki.com/>
6. The Hidden Wiki http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page
7. Hidden Wiki <http://hwikis25cffertqe.onion>
8. Torch <http://xmh57jrznw6insl.onion/>
9. Not Evil <http://hss3uro2hsxfogfq.onion/>