THE COMPLEXITIES OF INVESTIGATING ILLEGAL ACTIVITY ON THE DARK WEB

ACCESSDATA®
an exterro® company

INTRODUCTION

The Complexities of Investigating Illegal Activity on the Dark Web

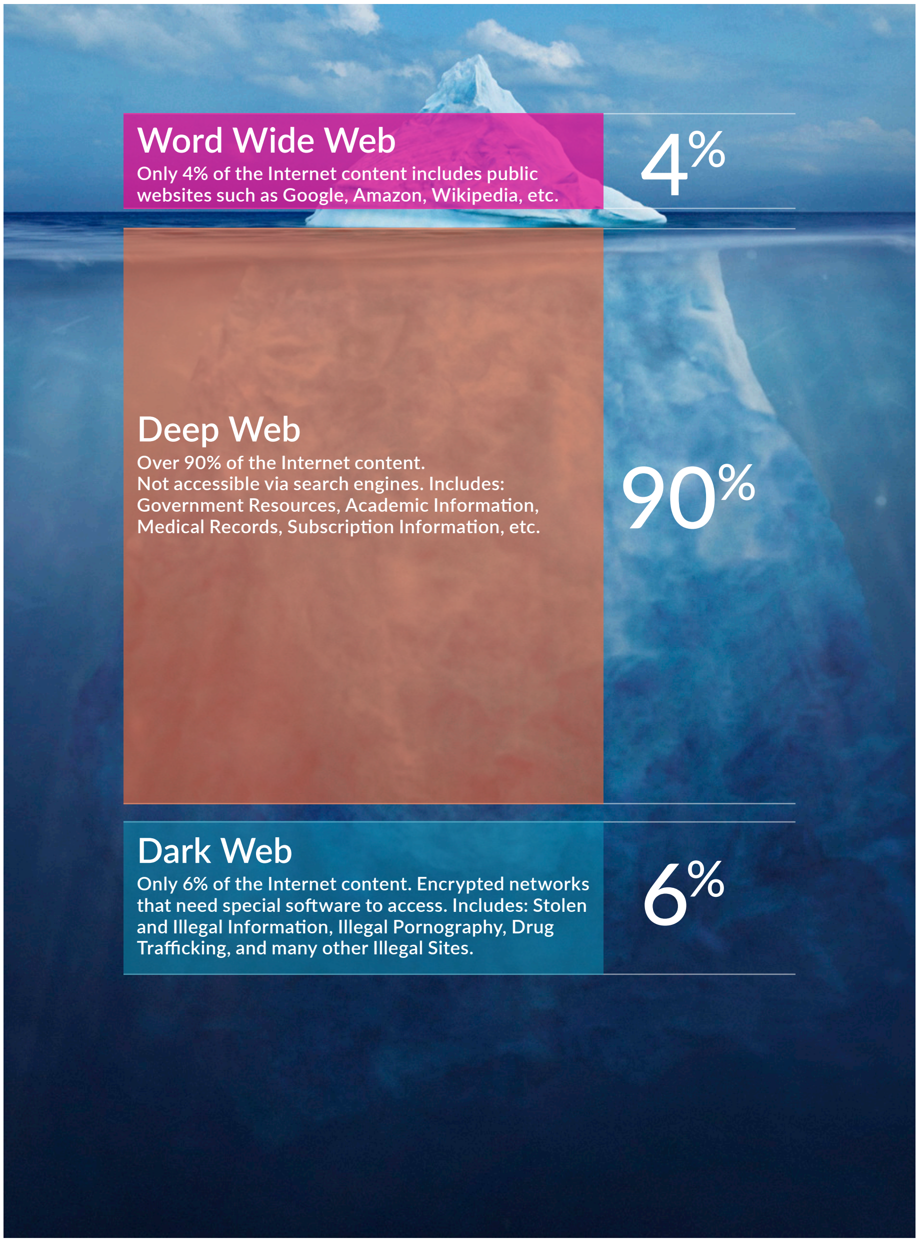
In today's world, given the situations that we are in with both the COVID-19 pandemic and the remote workforce—realities that will be with us for a long time to come—the need for Internet access has never been greater than it is now. Workers, along with everyday people, need access to many different websites, online portals, the company intranet—and yes, even Google—to conduct and execute daily job functions.

While the Internet is a gargantuan repository of information (in fact, there are some 1.7 billion websites currently available), this is actually an exceedingly small percentage of what's out there. Yet another vast expanse of the Internet exists that many people have never heard of. This part of the Internet is known as the "Dark Web."

What Is the Dark Web?

As noted, the Internet that is made available and can be accessed by the public at large is technically known as the "World Wide Web," also known as "www" in the URL or domain of the website in question. As one can see from the graphic below, believe it or not, this only makes up about 4% of the entire Internet.

The remainder comes from what is known as the "Deep Web" (at 90%), and only a small portion of that consists of the "Dark Web" (6%). This is illustrated here:


Word Wide Web
Only 4% of the Internet content includes public websites such as Google, Amazon, Wikipedia, etc.
4%
Deep Web
Over 90% of the Internet content.
Not accessible via search engines. Includes: Government Resources, Academic Information, Medical Records, Subscription Information, etc.
90%
Dark Web
Only 6% of the Internet content. Encrypted networks that need special software to access. Includes: Stolen and Illegal Information, Illegal Pornography, Drug Trafficking, and many other Illegal Sites.
6%

SOURCE: 1

What Is the Dark Web? CONTINUED

One of the key distinctions between the World Wide Web and the Deep Web is that with the former, all 1.7 billion websites and their corresponding sites are “indexable,” which means that on a 24 x 7 x 365 basis, the search engines of Google, Yahoo, Bing, AOL, etc., are continually ranking both current and new websites based upon both Search Engine Optimization (SEO) and the keywords that have been implemented into their respective content.

Only the most relevant results will be displayed instantly within the first one or two pages of the search results when you conduct a specific web-based query. There will be others as well, but they will be filtered based upon their level of relevance in subsequent search page results.

The Deep Web on the other hand does not index any of the websites or their corresponding pages. That is one of the primary reasons why they are not made available to the public. They can still be accessed, but you need to have special tools to do it safely, which will be addressed later in this whitepaper. The terms **Dark Web** and the **Deep Web** are often used interchangeably, but the two are vastly different.

As can be seen from the above illustration, the Deep Web can be deemed “neutral.” In other words, it consists of websites and resources that have been established by other entities that do not want their material to be accessed by the public and are out of plain view. Examples of this include the Federal Government, organizations in the healthcare industry, and other research and development entities. There is nothing illegal about accessing this part of the Internet. Other key differences between the **Deep Web** the **Dark Web** Internet are as follows:

- → The Deep Web is also known as the “Invisible Academic” for reasons just stated.
- → Most of the domain extensions in the Deep Web are that of the “.onion” and “.12p,” very much unlike the traditional “.com” domain extensions used by the Public Internet.
- → The data size of the Deep Web is currently estimated to be at 7,500 terabytes. It only consists of about 200,000 websites but has more than 500 times the information and data of the Public Internet.
- → To conduct transactions on the Deep Web, only virtual currencies are used, such as Bitcoin.

SOURCE: 2

What Is the Dark Web? CONTINUED

The Dark Web is considered the "sinister side" of the Deep Web. This is where most of the web's illegal activities occur and where the criminal based chat and messaging forums reside. After a Cyber attacker has launched their threat vectors, all the valuable Personal Identifiable Information (PII) datasets that are hijacked eventually make their way to the Dark Web to sell for a rather nice price and can even be used to launch subsequent Cyberattacks. Typical information and activities found on the Dark Web include:

→ Credit card numbers and other relevant banking/financial data. The Dark Web is a dumping ground for confidential information that has been stolen.

→ Payment cards forged with stolen credit card numbers and the ability to obtain them.

→ How-to guides on how to extort and defraud just about any business in virtually all industries.

→ The source code that is leaked from a threat variant (such as that from a SQL injection attack) often make their way here as well. This allows the competitors of a business to take complete advantage of this for their own nefarious purposes.

→ Ready-made phishing templates and other illegal forms of documentation that guide the Cyber attacker in launching a security breach quickly and easily, can be found here.

→ The Dark Web creates a safe haven for those involved in human trafficking and other nefarious activities.

→ Prefilled tax returns with real and legitimate taxpayer information can be found which allows the Cyber attacker to file fraudulent tax returns to obtain refunds.

→ Fake identification, such as fictitious passports, driver's licenses and military IDs are available which allows a Cyber attacker to launch a Social Engineering attack in a very sophisticated way.

There is much more that goes on; the above is only part of it. Now, the next question you might ask is:

> *"Although the Dark Web is the place for all the nasty and illegal stuff to happen, is it still illegal to access it?"*

Technically no, it is not. But it all comes down to what kind of activities you are doing on the Dark Web. Obviously, if you are engaging in some sort of criminal activity, then yes it is illegal . But if you are going into the Dark Web for curiosity's sake, then no, it is not illegal.

Many law enforcement agencies and even IT Security teams across corporate America routinely access the Dark Web to collect pieces of evidence to build a case for subsequent prosecution and arrests. IT Security teams also penetrate the Dark Web to check for hijacked PII datasets. If any are found, there's a good chance that a Cyber attacker has covertly breached an organization.

How to Access the Dark Web

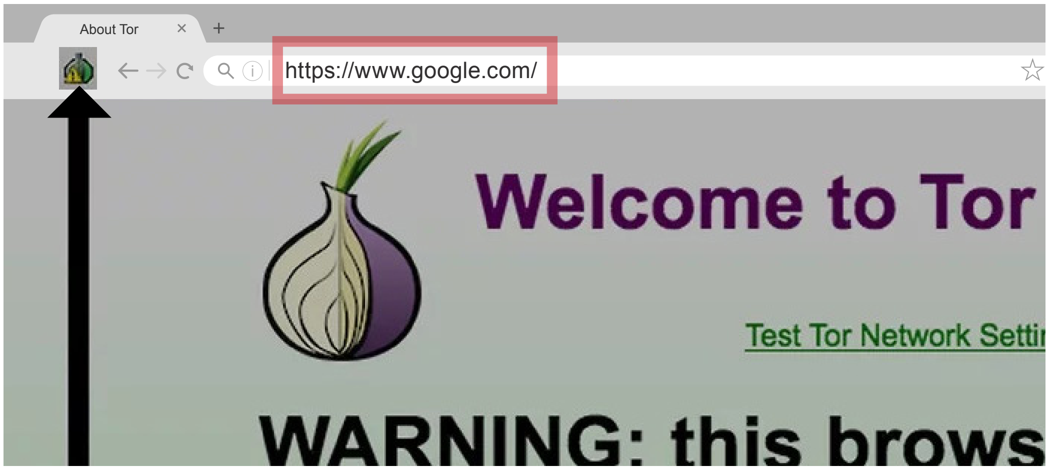
It's relatively easy to access the public portion of the Internet. It is a process that we take for granted until we do not have an Internet connection for some reason. But, accessing the Dark Web is quite the opposite. It cannot be accessed via any regular browser you've heard of (such as Google Chrome, Microsoft Edge, Firefox Mozilla, the iOS Safari, etc.). Instead, you need a specialized web browser, as well as other tools to access it.

Here is how to do it, on a high-level basis:

1

You need to download and install the TOR web browser:

As we discussed previously, one of the primary file extensions that is supported by both the Deep and Dark Web is that of the ".onion." You will need a web browser that can handle any web requests made from this extension; one being the "TOR" browser. It was designed and created by the U.S. intelligence community to access highly classified documents and engage in highly classified online communications. It is a specialized version of the Firefox web browser, so the overall UI/UX environment will be the same. It also has safety features incorporated into it so that you can "surf" the Dark Web anonymously. In other words, it is designed so that any attempts made by other malicious third parties to find your identity cannot happen. It even provides recommendations on how to stay safe as you are working your way around the Dark Web, on a real-time basis.



You can download the TOR browser here:
https://www.torproject.org/download/

SOURCE: 3

How to Access the Dark Web CONTINUED

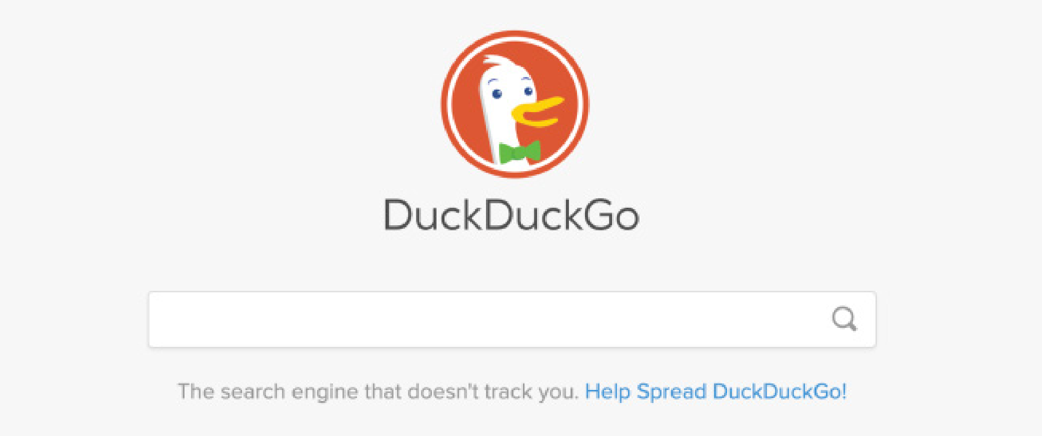
2 Download an exceptionally reliable Virtual Private Network (VPN) Service:

While many ISPs offer unbelievably cheap VPN services, it is important that you choose one that is not only highly reliable but also designed specifically for accessing the Dark Web. One such VPN service that has both characteristics is known "ExpressVPN," and it can be downloaded from this link: https://www.expressvpn.com/

At this point, keep in mind that while the TOR browser can ***mask your identity***, it cannot conceal ***your actual physical location***. This is where ExpressVPN will come into play.

3 Be careful of the search engine that you use:

While Google may be the search engine of choice on the Public Internet, it is not available for use on the Dark Web. Instead, there is a safe alternative to use when it comes to this part as you surf through the Dark Web, and it is known as "DuckDuckGo." When using this search engine, your queries and keyword searches will be hidden from view.



DuckDuckGo

The search engine that doesn't track you. Help Spread DuckDuckGo!

It can be downloaded here: https://duckduckgo.com/

SOURCE: 4

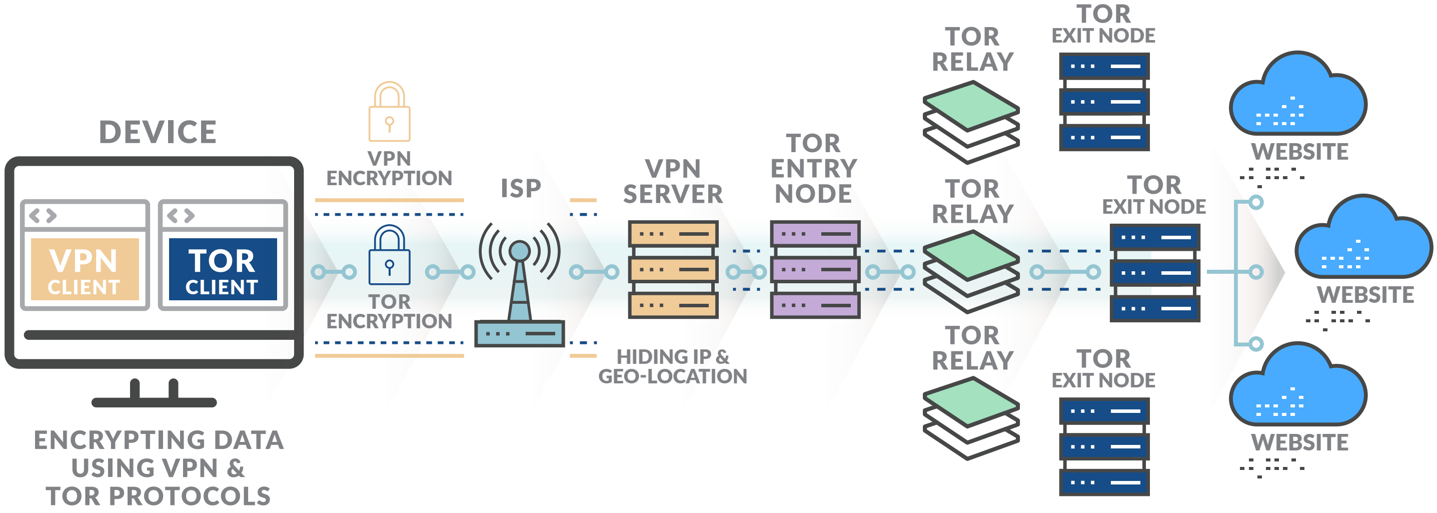
4 You need an email address:

Just like the public Internet, you also need to have an email address from which you can access information in the Dark Web. It's important to have an email address ***that is completely untraceable and using the ones from Yahoo and Google will simply not suffice***. TOR has a couple of email services that you can use in this regard, which are the "TORbox" and the "Mail2Tor." Keep in mind that you will need to have a TOR browser up and running before you can download any of the email services.

How the Whole Process Works

Now that you have a more solid background on what you need to access the Dark Web, the next question you may have is: "How does all of this come together?" The answer to this is simple: It is the connection known technically as the "TOR Over VPN."

In this kind of network activity, all the requests that you place over your TOR browser are sent to the VPN service that you are using, and from there, it goes through the TOR Network, making at least three separate network-based hops before you reach your destination on the Dark Web.

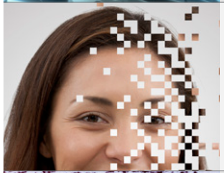


SOURCE: 5

But here is one caveat. The VPN service that you are using to access the Dark Web keeps track of metadata logs. This means that any queries, keyword searches, or even any websites you visit on the Dark Web are being recorded and kept track of.

The Challenges for Law Enforcement

While policing the Public Internet can be a relatively complicated task for law enforcement, this is compounded even more in the Dark Web, given the high level of complexity involved. While many obstacles are involved, the matrix below provides an overview of some of the challenges law enforcement officials and even digital forensics investigators face when trying to collect evidence on the Dark Web:

THE CHALLENGE		WHY IT IS SO
	Higher levels of encryption	There are more and higher levels of encryption on the Dark Web as compared to the Public Internet. Because of this, it can be almost impossible to keep track of a user's identity, geophysical location, or even what specific activities they are undertaking.
	**High levels of anonymity**	Criminals, and Cyber attackers on the Dark Web, and even legitimate users, try want to keep their identities a secret on the Dark Web, making it difficult to keep track of them.
	User identities keep changing	The criminals and the Cyber attackers on the Dark Web are continually changing their identities. It is exceedingly difficult for law enforcement officials and digital forensics experts to build reliable profiles on these individuals and/or groups.
	The difficulties of jurisdiction	Traditionally, law enforcement has jurisdiction in the location where the crime happens. But in the Dark Web, with everything hidden, especially the geophysical location, it nearly impossible to determine which law enforcement agency has control over what on the Dark Web. This could make the collectability and preservation of evidence even more questionable.
	It takes highly skilled professionals	Trying to track Criminals and Cyber attackers on the Dark Web requires that law enforcement officers get into the actual mindset of the criminals. The only way to truly do this is to hire people who have turned from the "bad side" to the "good side"—but in the end, do you know if you can trust them?
	Evidence collected comes in different formats	Once a digital forensics team gets involved in collecting evidence on the Dark Web, one of the key challenges is that there is no set of best standards or practices that allow it to be admissible in a court of law without any question.
	Tracebacking becomes more difficult	This is the process of where any type or kind of illicit activities or transactions can be traced back to its source. While this may be a relatively easier task to do on the Public Internet because of the availability of resources, this is far more difficult to do on the Dark Web.

CONCLUSION

Overall, this whitepaper has examined what the Dark Web is, noting its differences from the Deep Web. Also, it closely examined the tools needed to penetrate the Dark web and some of the obstacles faced by law enforcement officials when trying to collect evidence from it. The bottom line is that going into the Dark Web is not technically illegal, but what you do there will be closely watched, so you must proceed at your own risk.

Turn to the **FTK** product family when you need the gold standard in forensic investigation tools. The **FTK portfolio** will transform the investigative environment, empowering users with pioneering tools so that they can get access to evidence faster and help uncover more relevant findings when processing and analyzing data, while understanding connections that could sharpen focus and direction.

LEARN MORE

ACCESSDATA®
an exterro® company

Visit us online:
www.accessdata.com

Global Headquarters
+1 801 377 5410
603 E Timpanogos Circle, Bldg H
Orem, UT 84097

North American Sales
+1 800 574 5199
Fax: +1 801 765 4370
sales@accessdata.com

International Sales
+44 20 7856 9500
internationalsales@accessdata.com

Sources:

1. https://whhspatriotpress.com/15447/fashionentertainment/entertainment-watch/dark-web-crackdown/#modal-photo
2. https://www.masterdc.com/blog/dark-web-deep-web-differences/
3. https://heimdalsecurity.com/blog/how-to-get-on-the-dark-web/
4. https://www.webhostingsecretrevealed.net/blog/web-tools/tourist-guide-to-dark-web-accessing-the-dark-web-tor-browser-and-onion-websites/
5. https://www.comparitech.com/blog/vpn-privacy/access-dark-web-safely-vpn/