Emerging Trends in Narcotics Investigations:

The Rising Threat from Dark Web Drug Marketplaces

Prepared by the Houston Investigative Support Center
An Initiative of the Houston HIDTA
Office of National Drug Control Policy

December 2018
# Table of Contents

The Rising Threat of the Dark Web ........................................3

Dark Web Drug Investigations: Outlook for the Future .................4

Best Practices for Investigations involving Dark Web Drug Market Transactions ........................................5

Basic Concepts to Assist Law Enforcement in Dark Web-Related Drug Investigations ........................................7

Understanding the World Wide Web ....................................8

The Layers of the Internet: Surface Web, Deep Web, Dark Web and Darknets ........................................9

Accessing the Tor Darknet ..................................................9

The Tor Browser and Tor Applications for Mobile Phones
Tor’s Onionland: Onion Websites and Onion Routing

Finding Darknet Onion Addresses ......................................12

Clearnet Websites with Information about the Dark Web
Clearnet Websites with Links to Dark Web Onion Addresses
Darknet Search Engines for Tor’s Hidden Internet

Navigating Dark Web Drug Marketplaces ................................14

Dark Web Drug Marketplaces: An Overview
Dark Web Drug Marketplace Seizures
Ban of Fentanyl Sales on Dark Web Drug Markets

Using Cryptocurrency on Dark Web Markets ........................17

Overview of Cryptocurrency
Types of Cryptocurrency
Cryptocurrency Wallets
Methods of Purchasing Cryptocurrency
Sending and Receiving Cryptocurrency
Cryptocurrency Transactions on Dark Web Drug Markets

Appendices ........................................................................34

Endnotes ............................................................................44
The Rising Threat of the Dark Web

The expanding use of the internet continues to transform the world as we know it. From the use of stationary personal computers to mobile devices such as laptops, tablets, smartphones and smartwatches, people have the ability to access the world wide web almost everywhere they go. With the advent of the Internet of Things (IoT), a wide variety of objects are now being produced as “smart” devices with an internet connection. From a law enforcement standpoint, the data from phones, computers, smartwatches, and these other smart objects can provide officers with important investigative clues. In fact, because the internet is such an integral part of our daily existence, it is becoming imperative to combine technology-based approaches to investigations with traditional case work in order to successfully solve crimes.1

This changing nature of crime is creating significant investigative challenges for narcotics officers. Criminals are largely using smartphone applications with security features such as encryption and/or time-based message deletion options to safeguard their drug-related communications and social media platforms are now regularly used to negotiate drug deals. Another growing technology-based trend that is complicating narcotics investigations is the movement of modern-day drug deals from dimly-lit street corners to the darkest recesses of the internet referred to as the “dark web.” The allure of the dark web to sell and/or obtain illicit drugs is gaining momentum, due to the appeal of being able to maintain one’s anonymity while conducting transactions online. Although use of this part of the world wide web is not well-known to the general public, a quick Google search will provide anyone who wants to know how to access it with detailed, step-by-step instructions. Dark web drug marketplaces, also called “cryptomarkets” may sound somewhat mysterious, but they are actually quite similar to eBay or Amazon, except that payment accepted for the illicit goods and services includes various forms of cryptocurrency rather than traditional means such as credit cards or PayPal. As this trend rises in popularity, illicit drugs are increasingly being delivered right to one’s doorstep, using unwitting postal carriers as drug couriers.

It is of utmost concern that these dark web drug marketplaces are playing a significant role in fueling the opioid addiction crisis in the United States. Although a wide variety of drug types can be purchased on the dark web, shipments of fentanyl, fentanyl analogs and other synthetic opioids originating from dark web marketplace vendors are contributing to an alarming number of drug overdoses and deaths across the nation. As such, there has been a growing interest in this drug underworld, both by drug dealers and/or opioid users who want to explore their online shopping options on the dark web and law enforcement who are committed to stopping this illicit activity and shutting down these drug marketplaces. Unfortunately, because of the severity of the opioid problem in this country, it is probable that many officers may have their first exposure to the dark web due to an investigation initiated as the result of a tragic drug overdose death in their own community.

Law enforcement needs to understand this emerging threat in order to be able to effectively combat it. While actual training on dark web drug-related investigations is well beyond the scope of this report, this document will provide basic recommendations for best practices that were shared by those with investigative experience of this nature. It was also prepared to serve as resource by presenting an introductory overview of the dark web, dark web drug markets, and information related to the various types of cryptocurrencies that are being used for drug purchases.

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE
Dark Web Drug Investigations: Outlook for the Future

An Increasing Number of Drug Cases with a Nexus to the Dark Web is Likely

The tragic epidemic of drug-related overdoses and fatalities in this country is connected, at least in part, to drug deals that originate on the dark web. Purchasing drugs on dark web marketplaces offers those involved in this illicit activity more privacy than other traditional methods. Similarly, drug delivery using mail services provides them with a higher sense of security, eliminating the need for interacting with a stranger to finalize the sale. For these reasons, use of the dark web is likely to remain an attractive option that will continue to increase in the future.

Since dangerous synthetic drugs such as fentanyl and fentanyl analogs are increasingly being purchased in these hidden corners of the internet, law enforcement cannot afford to overlook this very real although somewhat obscure realm in which drug transactions are taking place. To keep up with the evolution of crime in this digital age, counternarcotics efforts must include an investigative component that focuses on this method of buying and selling drugs. To effectively reduce this rising threat, it is now more imperative than ever for officers to take a stronger role in investigating illicit drug activities with internet-based sources of supply.

Law enforcement’s recent focus on darknet marketplaces have already led criminals to find new ways to adapt, delving even deeper into the darkness of cyberspace. As an example, some dark web market users are reportedly beginning to move away from using “traditional” darknet marketplaces toward decentralized, peer-to-peer darknet marketplaces like OpenBazaar where vendors deal directly with the customer, eliminating the “host” or middleman. According to experienced dark web drug investigators, this is concerning because law enforcement will not be able to infiltrate or take down these marketplaces in the same way as they could with marketplaces like Silk Road and AlphaBay. Substantial investigative challenges lie ahead, but federal agencies such as Homeland Security Investigations and the United States Postal Inspection Service, whose work has been significantly impacted by the increase in dark web drug purchases being shipped through the mail, are leading the way to halt the further progression of these dark web-related drug trends. Their role in assisting other law enforcement entities to increase their participation in dark web investigations through training and partnership is to be commended.

Drug cases with a nexus to the dark web will not be a temporary trend. As our society becomes even more deeply entrenched in its reliance on the internet, individuals are increasingly becoming more comfortable in using technology to their advantage. Because of the ease of accessing the dark web and drug marketplaces there, those wishing to “safely” purchase illicit products will gravitate toward experimentation with dark web options. Although law enforcement officers cannot be expected to become computer science specialists in order to solve drug crimes, they can maximize their ability for successful dark web investigations by working together with other individuals and agencies, and collaborating with those who do have this expertise. By staying open to learning about new technology in this rapidly changing world, law enforcement will not only be acquiring valuable new investigative skills, they will ultimately be playing a much larger role in their communities. They’ll be saving lives.
Best Practices for Investigations Involving Dark Web Drug Market Transactions

Law enforcement officers have learned a great deal from previous dark web-related investigations. One prime example of a successful dark web-related investigation is the “Peter the Great” case. Initiated by investigators in Portland with the Oregon-Idaho HIDTA in response to a fatal synthetic opioid overdose, this case highlights the value of local, state, and federal law enforcement working together in partnership across the country in their counternarcotics efforts. A summary of the “Peter the Great” case can be found in Appendix A on pages 34 and 35. Some lessons learned from this case, as well as advice shared by investigators who are currently involved in dark web investigations and/or are teaching classes related to this type of case work are provided below.

Dark Web Investigative Tips

- Training will be Imperative

A very comprehensive report entitled The Changing Nature of Crime and Criminal Investigations published by the Police Executive Research Forum in January of 2018 summarizes the concerns of law enforcement leadership from across the county who convened to discuss the increased complexity of criminal investigative work due to rapidly evolving technology. Some of the insights and guidance shared as a result of their meeting are relevant to dark web-related investigations. They reported that:

- “The reality is that the science of criminal investigations is changing rapidly and many law enforcement agencies are not prepared for the changes that are taking place. This report is a wake-up call for the policing profession. If we are to be successful in combating crime in the 21st century, agencies must have the training, tools, and skilled personnel to understand the changing nature of crime and to be resourceful in investigating new types of crime.”
- They noted that “Nearly every type of crime today has a digital component.”
- “Experts also note that while the dark web still accounts for a relatively small share of total drug sales, especially regarding cocaine and marijuana, it has emerged as a major source for sales of highly lethal synthetic opioids, such as fentanyl and U-47700.” “Many drug dealers feel safer on the dark web, so they are using this approach more frequently.”

Drug investigators who teach classes on dark web investigations agree that this method of buying and selling drugs is on the rise. They state that dark web-related cases are not going away and therefore, one of the most important things that officers can do to prepare themselves to successfully investigate cases with a dark web nexus is obtain training and educate themselves on this important topic. They emphasize that education for prosecutors will be important as well.

Homeland Security Investigations (HSI) is now conducting training classes throughout the United States to bring law enforcement up-to-speed on investigations related to the dark web and use of cryptocurrency. There are an increasing number of other agencies and groups who are beginning to offer this type of training as well. For instance, HIDTA’s National Emerging Threats Initiative (NETI) is now focusing its efforts on increasing awareness of this emerging trend and will be offering training courses to HIDTAs and other law enforcement groups in the near future. Information about NETI can be found at www.nhac.org. For those who are not able to attend classes in person, training courses on the dark web and cryptocurrency can be found online, including those designed specifically for law enforcement professionals such as at Instruq.co.
In addition to formal classroom and web-based training, dark web investigators say that websites about the dark web such as deepdotweb.com, darkwebnews.com, and darknetmarkets.com can and should be used as reference guides. Articles on these sites teach “newbies” about the do’s and the don’ts of darknet use, provide lists and current statuses of darknet markets and even show how to access these marketplaces to purchase drugs and other items. Investigators warn that deepdotweb.com posts reports of law enforcement actions that have been taken on darknet vendors and buyers, including links to affidavits in their articles. This is why it is important to educate prosecutors to limit the amount of details that are incorporated into unsealed court documents or if details are provided, to make sure indictments are sealed. Dark web investigators also recommend that law enforcement officers go out to the dark web to see the dark web marketplaces for themselves, operating, of course, within the policies and guidelines of their department when doing so.

- **Networking and Partnerships will be Crucial**

Investigators with experience in dark web investigations also stress the importance of networking with other local, state, and federal law enforcement and intelligence partners. When beginning an investigation of this nature, officers do not have to work through the process alone. The value of reaching out and forming these partnerships to share resources and knowledge cannot be overemphasized. Federal agencies such as HSI have personnel who are routinely working on dark web cases and can assist by sharing their expertise. They can also help with backstopping, as well as deconflicting targets. It is becoming increasingly apparent that all levels of law enforcement will need to take responsibility for identifying and investigating dark web drug-related criminal activity in order to reduce this growing threat. To achieve this goal, HSI has a wealth of resources available to offer to investigators to help them develop their skills and/or to augment their cases. For example, their financial analysts can provide highly specialized services such as blockchain analysis to trace cryptocurrency transactions. Additional information on how HSI is assisting other law enforcement agencies to successfully investigate drug-related cybercrimes can be found in Appendix B on page 36.

It is also vital for law enforcement officers to form close working relationships with their local postal inspectors. Dark web investigators say that although drug dealers’ attempts to conceal their identity by making purchases using the dark web does make this type of case more challenging, one must remember that ultimately, “illicit dark web dealers cannot avoid using traditional shipping methods such as the U.S. Postal Service to deliver goods to customers.” This is “a key vulnerability that must be better exploited.” Some postal inspectors have become subject matter experts on dark web investigations, positioning them to more successfully identify and investigate the increasing problem of drugs being shipped through the mail. These inspectors can help officers by making shipping-specific searching tools available to them to develop their cases. Important tips related to the postal aspect of dark web drug investigations can be found on pages 32 and 33.

- **Other Important Advice: Remember, It’s Still Traditional Investigative Work at its Core**

Although the technological component to these cases can be intimidating, successful dark web drug investigations, at their core, still rely heavily on well-developed, traditional narcotics investigative skills. According to one experienced dark web investigator, “Dark web drug dealers are smart about covering their tracks online and staying anonymous, but they don’t have the old school drug dealer street awareness. Traditional investigative techniques still work when there is a target you believe is involved in dark web narcotics.” Standard methods of obtaining evidence such as surveillance, trash runs, etc. will continue to be important to substantiate these cases.
Basic Concepts to Assist Law Enforcement in Dark Web-Related Drug Investigations

The following pages provide information about the dark web, including basic concepts related to cryptocurrency since it is the standard form of payment in this internet-based environment. The content in the rest of this report is intended to be an introduction to this important topic and to serve as a resource for law enforcement as they begin to work cases that have a nexus to dark web drug marketplaces. The wide variety of associated images in this document are specifically intended to assist officers to recognize potential indicators of dark web-related activity when they encounter them in the course of their counternarcotics investigations.
Understanding the World Wide Web

The Layers of the Internet

The Surface Web

The part of the world wide web that is easily accessible to the general public is called the surface web or visible web. It contains web pages that are indexed and can be easily located using search engines such as Yahoo, Google Chrome, Internet Explorer, etc. The surface web includes but is not limited to news media websites, online stores, and other private-sector and government websites. It may be surprising to some that surface web pages are actually only a small percentage of what exists on the entire internet. Some experts believe it constitutes less than one percent. The full scope of the world wide web is often described using an iceberg analogy. As can be seen in the accompanying figure, the surface web is truly just the tip of this iceberg.

The Deep Web

The deep web (also referred to as the invisible web) is a much larger percentage of the world wide web. The term “deep web” was coined by Michael K. Bergman, a computer scientist who founded an internet intelligence company called the BrightPlanet Corporation. Bergman stated that “searching on the internet today can be compared to dragging a net across the surface of the ocean. While a great deal of information may be caught in the net, there is still a wealth of information that is deep, and therefore, missed.” Bergman also concluded that the deep web could be estimated to be at least 400 to 500 times larger than the surface web. Of course, the entire internet has grown exponentially since that time. On their website, BrightPlanet reported that they have not completed any additional studies to predict the size of the deep web, stating that, “The internet has grown so vast and so large that we now classify the deep web as infinite.”

Unlike surface web pages, deep web content can’t be found by traditional search engines. For various reasons, deep web pages are constructed so that they are essentially invisible to web crawlers that track and index linked webpages. This does not mean that one cannot access the deep web. In fact, people access the deep web every day without realizing that this is what they are doing. One of the most common examples is the use of an email account. If you have an email address, you are using the deep web. You can access it with proper credentials (your username and password), but you can’t “google” someone else’s email account and expect to get search results that will take you to their email inbox. This deep web content is purposely made inaccessible to search engines.
Much of the information on the deep web is private data. In addition to email accounts, some other examples of the type of information located on the deep web include online bank account information, electronic health records, private social media content, as well as web-based subscriptions such as to newspapers and academic libraries. Additionally, there are numerous online databases that can be found on the surface web using a traditional search engine, but the actual content of these databases is housed on the deep web. Extraction of the raw unlinked data requires a manual directed query (i.e. one must type keywords into a website’s search box to access this type of deep web content).

The Dark Web and Darknets

The dark web is a small subset of the deep web that has been intentionally hidden. It is not a single, centralized place, but instead, the dark web is scattered among servers around the world. The terms dark web and darknet are often used interchangeably. Technically they are interrelated, but they have different definitions. Just as surface web pages exists on the publicly accessible part of the internet, the dark web refers to a collection of websites that exist within an encrypted network called a darknet. A darknet is an overlay network meaning that it exists as a layer built on top of the existing internet. Darknets attempt to block the tracking of a user’s IP address while on the internet and are thus referred to an anonymity networks. Dark web users often refer to the regular internet that most people are familiar with as the “clearnet” to distinguish it from these encrypted darknets. There are a number of different darknets. These darknets include small, peer-to-peer networks as well as larger networks such as Tor (The Onion Router), I2P (The Invisible Internet Project), and Freenet. By far, the most well-known and widely used of these dark web networks is Tor and therefore, this darknet will be the focus of further discussion related to dark web activity.

Accessing the Tor Darknet

**The Tor Browser**

Internet users cannot accidentally end up on the dark web because accessing this part of the world wide web requires the use of specialized technology (software, configurations or authorization). The Tor Browser is the most commonly used mechanism for accessing the dark web. It is available, free-of-charge on the torproject.org website. This browser makes the process of getting on to the dark web fairly simplistic, even for those who are not particularly tech-savvy. Anyone who has access to a computer and has an internet connection can download and use the Tor software. A virtual private network (VPN) is often used in conjunction with Tor as an added measure to maintain privacy. Some dark web users feel that they provide maximum security when used together. An external computer operating system called Tails is also often used in combination with Tor. Tails is designed to be used from a USB stick or DVD, allowing the user to bypass the computer’s original operating system so that no trace of internet activity will be left on their computer after accessing the dark web. Other similar systems include Whonix and Qubes.
The Tor Browser looks quite similar to traditional web browsers, as can be seen in the screenshot on the right. Many equate Tor solely with the dark web and criminal activity, but it should be noted that the Tor Browser is not only being used for nefarious purposes. In fact, use of the Tor Browser is not illegal in the United States and the Tor Project is actually funded, at least in part, through several government agencies and research groups. Tor can be used to browse the surface web as well as the dark web and is used by those who simply wish to browse the surface web with a higher level of privacy. In some circumstances, using the Tor browser may be the only way to access the world wide web. For example, Tor is used by people who live or work in countries that ban or restrict internet access in an attempt to circumvent this censorship. Interestingly, the social media platform Facebook actually has two website addresses: one on the surface web and another on the dark web to accommodate access for a wider range of potential users of this service.

Tor Applications for Mobile Phones

The Tor Network can be accessed via smartphone applications in addition to personal computers and laptops. For Android phones, Orbot is often used in combination with a Tor-enabled browser called Orfox that is similar to Firefox. Additionally, the Tor Browser for Android has recently been released by the Tor Project. Two iPhone applications that provide access to the Tor network include Onion Browser and Red Onion. Icons for these applications may be found on the phones of those who are using the dark web.
Tor’s Onionland: Onion Websites and Onion Routing

.Onion Websites

The Tor Network is sometimes referred to as Onionland because internet addresses for Tor’s darknet websites (called “onion services”) end with “.onion” rather than .com, .gov, .org or other extensions commonly associated with the surface web. Onion websites can only be reached through Tor-enabled browsers. These onion web addresses have a combination of 16 letters and/or numbers followed by the .onion suffix. The letters are all lowercase and numbers include only 2 through 7. For example, Facebook’s onion website address is https://facebookcorewwwi.onion, as shown above. The onion address for the original Silk Road (the first anonymous drug marketplace to be shut down by federal authorities) was http://silkroadvb5piz3r.onion.

Onion Routing: The Basics of How Tor Works

Why do these addresses end in .onion? It is due to the technique used by Tor to safeguard users’ identities and online activity called “onion routing.” It involves the use of a collection of volunteer-operated servers from all around the world. Tor attempts to mask one’s identity when they are using the internet by using many layers of encryption, metaphorically similar to the layers of an onion. Onion routing is a technical process that is beyond the scope of this report, but an analogy provided by Jessica Roy in a Time.com article entitled Everything You Need to Know about Silk Road, the Online Black Market Raided by the FBI, describes it well in layman’s terms. She states:

“Think of every message sent through the Internet – whether it be an email, a tweet or traffic to a website – as being a mailbag full of letters. Your I.P. address or “Internet Protocol” address, can be likened to the letters’ return address. When a user uses the Tor Browser bundle (which provides the Tor software plus a browser) instead of a regular browser like Chrome or Firefox, the letters become encrypted so that the contents of the letters can’t be read. The encryption also obscures the return address, making it impossible to tell where the letters came from. Tor then takes these encrypted letters (technically called “packets”) and passes them through a large network of routers, which are intermediaries that direct Internet traffic, much like a post office directs letters. The routers pass the letters back and forth between one another, further obscuring the letters’ source. Each time a letter passes through a router, it’s decrypted slightly, so that the router knows where next to send it, and re-encrypted. Eventually, each letter will reach a router designated as an “exit node,” where the final layer of encryption is decrypted, revealing the original. The latter is then stamped with the exit node’s IP address (like a new return address) and is sent to its destination.”

Since these “letters” go through a series of servers rather than taking a direct path along their route, Tor users have reported that requests are often slower than when searching the surface web with traditional search engines. Not only do requests take longer to process on the dark web, there is some instability in relying on a network of decentralized, private servers and thus, darknet websites are notorious for being unreliable, going on and offline fairly frequently. Because this is a common issue (and also because these websites are purportedly often hacked), darknet drug marketplaces generally have additional alternative .onion addresses called “mirror” websites so that they can remain up and running with minimal interruptions in service.
Finding Darknet Onion Addresses

Clearnet Websites with Information about the Dark Web

Since the dark web is not indexed, traditional search engines won’t find darknet websites. However, site administrators for darknet marketplaces are highly motivated to find ways to advertise their existence and location in order to stay in business. Therefore, although darknet marketplaces can’t be accessed via the surface web, websites on the surface web have been created to provide information about them. Investigators who work dark web drug investigations say that clearnet websites can actually be a very good starting point for those wanting to learn more about the dark web. Some websites with a wealth of dark web-related resources include, but are not limited to these surface websites:

- https://deepdotweb.com
- https://darkwebnews.com
- https://www.darknetmarkets.net

On these websites, information includes lists and comparisons of the top darknet markets, including their primary and mirror onion web addresses, tutorials for navigating popular marketplaces with step-by-step instructions on how to make purchases, and general advice related to privacy protection when accessing the dark web. For example, darkwebnews.com/darkwebmarkets/dream-market provides an article on how to access a marketplace called Dream Market, including screenshots to assist users through the process. News about markets that have been shut down, or believed to be being monitored or taken over by law enforcement are also popular topics on these websites to warn potential customers and vendors of the possible risks involved. Because cryptocurrency is the type of payment typically accepted on these marketplaces, articles on Bitcoin and other types of cryptocurrency are also fairly standard content on these sites. Most of these sites on the surface web also have their own onion websites on the dark web that they advertise here.
Clearnet Websites with Links to Dark Web Onion Addresses

Some clearnet websites actually contain links to darknet websites, but the links are only active when using the Tor Browser. Two examples are The Hidden Wiki and Ahmia. Additionally, DuckDuckGo is a privacy-based search engine that can be accessed on the clearnet or through Tor.47

The Hidden Wiki (https://www.hiddenwiki.com)

The Hidden Wiki looks similar in format to Wikipedia. It is described on its website as the “largest active dark web websites URL directory.”48 Onion websites in this directory are organized into categories to assist users to find websites of interest that it would otherwise be difficult to impossible to find. For instance, The Hidden Wiki has a page with links specifically for the most current darknet markets, as shown below. In addition to its surface website, The Hidden Wiki also has an onion website (http://kpvz7ki2lzvnwve7.onion) that is advertised on its clearnet website.

Ahmia (https://ahmia.fi)

The website Ahmia.fi is a clearnet search engine for Tor’s onion services.49 As with The Hidden Wiki, Ahmia.fi must be accessed using the Tor Browser in order to be able to go to the dark web links provided through this search tool. Without the Tor Browser, the search engine does not work. Ahmia is also a darknet search engine with its own onion website on the Tor Network (https://msydqstl2zkzerdg.onion) that is advertised on its surface webpage.

Darknet Search Engines for Tor’s Hidden Internet

Torch (https://xmh57jrzrnw6insl.onion)
Not Evil (https://hss3uro2hsxfogfq.onion)

Once on the dark web, individuals can use darknet search engines to explore the Tor Network’s onion services. In addition to Ahmia, two of these include Torch and Not Evil.47 Using the Tor Browser, individuals can query these search engines as they would traditional search engines on the surface web. For example, after typing in a particular drug type, dark web users can review and click on a list of active onion website links for marketplace vendors that offer the desired product.
Navigating Dark Web Drug Marketplaces

Dark Web Drug Marketplaces: An Overview

**Darknet Marketplaces: the eBay of the Dark Web**

It is fairly safe to say that most people have not visited marketplaces on the dark web, but many have a general idea of what they look like because of the media attention that occurs when these sites are seized and shut down. These darknet marketplaces are similar to eBay or Amazon except that vendors specialize in the sale of illicit goods and services, and merchandise is typically purchased using cryptocurrency such as Bitcoin. Vendor-customer communications are commonly protected through the use of encryption software programs such as Pretty Good Privacy (PGP) and drug products are often sent to customers using “stealth shipping” to discreetly conceal and/or disguise the true contents of packages.\(^{50,51}\) Another difference is that some of these markets require an invitation or referral code in order to register for an account. Invitation codes can be obtained from other market users and they can also easily be acquired from the surface web sites that advertise for dark web marketplaces, as they often receive a commission for referrals.\(^{52}\)

Dark web markets are best known as a haven for buying and selling illicit drugs, but they also offer a wide variety of other items such as, but not limited to stolen and fraudulent identification documents, counterfeit goods, weapons, malware and computer hacking tools.\(^{1,53}\)

Since 2013, it is believed that over 100 dark web marketplaces have been created and most of them stay in existence for an average of about eight months.\(^{54}\) A study funded by the National Institute on Drug Abuse (NIDA) that was conducted from March through August of 2018 found that about thirty of these markets were thought to be currently active during this time period. A wide variety of illicit drug types are being sold on dark web marketplaces as can be seen in the accompanying screenshot from Dream Market.\(^{54}\) On this marketplace, the highest number of vendor listings were for the sale of cannabis.\(^{54}\) While all of the drugs being offered on the dark web pose some level of threat, dangerous synthetic chemicals such as fentanyl and fentanyl analogs sold on these online black markets are of the utmost concern. Tragically, a growing number of narcotics investigations now have a dark web component due to overdose deaths from synthetic opioids that originated from dark web marketplaces.

**Dark Web Drug Marketplace Seizures**

**Silk Road and Silk Road 2.0**

Images of the original Silk Road can be found all over the surface web. When it was seized by federal authorities in 2013, it was the “cyber-underworld’s largest black market, with $1.2 billion in sales and nearly a million customers.”\(^{55}\) Similar marketplaces quickly emerged to provide alternative venues for clientele of the dark web, including Silk Road 2.0. When law enforcement shut down Silk Road 2.0 in 2014, it had over 13,000 listings for illegal and controlled substances, including 379 listings for opioids.\(^{56}\)
AlphaBay and Hansa

Synthetic drugs being sold on darknet markets are playing a role in fueling the nation’s opioid epidemic. Because of this serious public health threat, law enforcement investigations targeting these websites have intensified. In July of 2017, two of the top darknet drug marketplaces, AlphaBay and Hansa were seized as the result of the cooperation of numerous international partners. AlphaBay was touted by the U.S. Attorney General as “the largest darknet marketplace in history.” It was at least ten times larger than Silk Road and purchases from this site were linked to multiple overdoses and deaths in the United States. At the time of the takedown, there were over 250,000 listings for illegal drugs and toxic chemicals on this darknet marketplace. It was reportedly being used by hundreds of thousands of people throughout the world, and was a major source for heroin and fentanyl, with 122 vendors selling fentanyl and 238 advertising heroin. Once again, almost as soon as these seizures occurred, vendors and customers flocked to other markets such as “Dream” and “Wall Street” for their illicit drug sales. Dream Market has emerged as the top darknet drug marketplace.

This darknet screenshot of Dream Market was provided courtesy of Instrux, a company that provides online training for law enforcement on a variety of topics including courses on the dark web.

Dark web drug investigators emphasize that historical information from seized sites such as Silk Road, AlphaBay, and Hansa is available and may aid in investigations since many of these vendors use the same or similar monikers, and their public PGP keys can link a current account to a former seized account. (Further information about PGP encryption keys can be found on page 31.)
Ban of Fentanyl Sales on Dark Web Drug Markets?

Dream Market formally banned the sale of fentanyl in May of 2018, most likely to lessen the level of law enforcement attention toward this marketplace. However, vendors are still selling fentanyl and/or fentanyl analogs; some are just being more discreet than before.54 Before the ban, vendors were openly advertising that their products contained fentanyl, fentanyl analogs or other synthetic opioids. Some still do, but after the ban, many vendors began advertising that their products did not contain fentanyl.54 Other vendors chose not to indicate whether or not fentanyl was present, but instead used a ranking system to describe the potency of their products.54 Other drug markets such as Wall Street Market were still selling fentanyl and/or fentanyl analogs as of late November of 2018.62

The dark web screenshots above were obtained from a National Drug Early Warning System (NDEWS) Webinar entitled Collecting and Analyzing Cryptomarket Data on Novel Synthetic Opioids, October 24, 2018 and from Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), Houston, Texas on November 29, 2018.54,62
Using Cryptocurrency on Dark Web Markets

Overview of Cryptocurrency

A basic understanding of cryptocurrency will be important for law enforcement officers working darknet investigations. This is because darknet market vendors generally require that customers use this type of payment for their purchases in an attempt to safeguard the anonymity of both parties. Because cryptocurrency is the standard method of payment, these markets are often referred to as “cryptomarkets.” Traditional payment methods such as checks, credit cards, or PayPal that may potentially identify purchasers are typically not accepted.

Cryptocurrency is digital currency, meaning that it exists only on computers. It has no physical form, such as bills or coins, like the type of money most people are familiar with, although it is often depicted with images of gold or silver coins. Cryptocurrency is decentralized, meaning that it is not controlled by a centralized government, but instead by its users. There is no middleman as with the traditional banking system. It is transferred directly from one individual to another (peer-to-peer) using digital wallets. Since cryptocurrency can be difficult to trace back to those who are using it, dark web drug investigations are posing unique challenges for investigators.

Types of Cryptocurrency used on Dark Web Drug Marketplaces

There are actually more than a thousand different types of cryptocurrencies in existence, though only a select few are generally accepted by vendors on dark web markets. The market for cryptocurrency has been quite volatile and prices fluctuate, sometimes fairly dramatically. There are a number of clearnet websites that provide updated price information for cryptocurrencies. For example, a listing of the top 300 cryptocurrencies can be found at bitinfocharts.com/top-cryptocurrency-list.html. The top five ranked by this site as of December 14, 2018 are shown on the right. Other websites such as coinmarketcap.com also provide this type of information.

Two of the most common cryptocurrencies that are accepted as payment by vendors on darknet drug markets include Bitcoin and Monero. However, there are a variety of others that are accepted, depending on the vendor’s preferences. Some of these cryptocurrencies include, but are not limited to Litecoin, Bitcoin Cash, and Ethereum. The chart on the right shows the results of a study that surveyed 12 darknet marketplaces between February and March of 2018. Marketplaces included in this study were the current top drug market, Dream Market, along with Valhalla, Tochka (also referred to as “Point/Th3ch3a”), Berlusconi Market, Wall Street Market, Olympus Market, Zion Market, Drug Market, Libertas Market, Empire Market, Silk Road 3 and Apollon Market.
**Bitcoin (BTC)**

Bitcoin (BTC) was created in 2009 by an unknown person (or possibly a group of people) who used the alias Satoshi Nakamoto. It was the first popular cryptocurrency and it remains the most widely accepted form of cryptocurrency being used for purchases on dark web drug marketplaces. It is often depicted online as a gold coin, as in the photo on the right, however neither Bitcoin nor any other cryptocurrencies actually exist in a physical form, as mentioned earlier. The price of Bitcoin has fluctuated widely in recent years. The volatility in the price of Bitcoin was seen most prominently in 2017 when, over the course of the year, the price for one Bitcoin ranged from as low as $900 to nearly $20,000. As of December 14, 2018, the price for one Bitcoin was $3,223.

**Bitcoin Blockchain Technology and Bitcoin Mining**

All Bitcoin transactions ever processed are recorded on a digital distributed public ledger called a blockchain that anyone can see at any time. However, Bitcoin transactions are considered to be pseudo-anonymous rather than completely anonymous because although the blockchain does not contain actual names of the buyers and sellers involved in Bitcoin transactions, it does record the balance and history of transactions of each Bitcoin wallet address (a unique digital signature). This public ledger is available to view and/or search online at www.blockchain.info. Some level of knowledge about the blockchain is important because forensic analysis of transactions has assisted investigators in solving cases and arresting and prosecuting those using Bitcoin for illegal purposes.

The concepts of Bitcoin’s blockchain technology and blockchain mining are quite complicated and beyond the scope of this report. However, some general concepts to note about this technology are that new Bitcoins are created through a process called cryptocurrency mining. One website providing a beginner’s course on this topic stated that, “While this may sound like something that would require a shovel and hard hat, it’s not – it’s actually more of a process like accounting.” Bitcoin miners use large numbers of powerful computers “to run incredibly complicated mathematical formulas to provide the verification for Bitcoin transactions, and at the same time create new Bitcoins.” Those who are able to solve these computational puzzles first add a block to the blockchain and are rewarded with a payment in Bitcoin for their mining efforts. Bitcoins will be mined until the number created reaches 21 million, the amount designated by Bitcoin’s founder as the maximum number that will ever exist. This is forecasted to occur around the year 2040.

**Irreversible Bitcoin Transactions: Use of Escrow Services**

In the example on the right, illustrating the use of Bitcoin on Dream Market, the vendor HappyDrugs is advertising three grams of China White “synthetic heroin” for a portion of a Bitcoin equal to 0.00684. This vendor will ship products from Europe (EU) to locations worldwide (WW). The word ESCROW in the green box next to the synthetic heroin photo means that Dream Market’s escrow service will hold the Bitcoin, acting as an intermediary until conditions agreed to by the buyer and seller are met. Although it is not fail-safe, using an escrow service can help to protect buyers against fraudulent vendors by holding payment until the buyer authorizes the release of funds after they have received their order. Unlike traditional financial transactions where buyers can get their money refunded back to their credit card if they are not satisfied with a product, Bitcoin transactions are irreversible, making the use of an escrow service a desirable feature when making purchases.
Altcoins

There are many other types of cryptocurrency besides Bitcoin, but only a few that have gained popularity for use on darknet markets. All cryptocurrencies other than Bitcoin are referred to as “altcoins,” an abbreviation for alternative coins. As with Bitcoin, most altcoins are transferred directly from one individual to another (peer-to-peer), they operate using a blockchain with a shared ledger, and creation of coins involves a mining process. Most altcoins are described by their founders as being modified or improved versions of Bitcoin. Bitcoin remains the most commonly used cryptocurrency by far, but because it has become fairly well-known that it is not anonymous and is, in fact, traceable, this has led some individuals who use dark web markets for the purchase of illicit products to move away from Bitcoin toward other digital currencies that offer more privacy and are more difficult for law enforcement to track. Other reasons for movement away from Bitcoin are that Bitcoin transactions tend to be slower and transaction fees are higher compared to some of the newer altcoins.

Monero (XMR) is an altcoin that offers more security that Bitcoin, designed with enhanced features for users who wish to ensure their anonymity. Compared to Bitcoin where multiple payments to the same address can be linked unless a new wallet address is created for each transaction, Monero uses technology called stealth addresses to deal with this security issue. Some believe that “stealth addresses are completely anonymous and untraceable and they add privacy to the receiver of a transaction.” When a transaction is recorded on the blockchain, only the sender and receiver can determine where the payment was actually sent. In addition to stealth addresses, Monero uses ring signatures and RingCT (ring confidential transactions) to protect users’ privacy. Ring signatures make it “impossible to tell who the actual sender was” and RingCT “allows users to hide transaction amounts.” IP addresses are also hidden. Other coins that are privacy-focused coins include, but are not limited to Dash (DASH) and Z-Cash (ZEC).

Because their names are so similar, it is important to explain, at least in simplified terms, the difference between Bitcoin (BTC) and Bitcoin Cash (BCH). They are two separate cryptocurrencies. As Bitcoin became more and more popular and the volume of daily transactions increased, the amount of time it was taking to process these transactions was becoming much slower and transaction fees were increasing. In order to increase the number of transactions that can be processed by the network, developers initiated what is known as a “hard fork,” a permanent split from Bitcoin, making changes to the Bitcoin protocol that increased the block size in the blockchain, and creating a new currency called Bitcoin Cash. By splitting from Bitcoin, they were able to “essentially create a new blockchain with altered rules” to achieve this goal.

Litecoin (LTC) is also a spinoff (hard fork) of Bitcoin. It is often depicted as a silver coin and referred to as “silver to Bitcoin’s gold.” As with Bitcoin Cash, some consider Litecoin to be an improved version of Bitcoin. Whereas Bitcoin Cash was created to increase the number of transactions that could be processed, Litecoin’s goal was to achieve a higher transaction speed (block time) than Bitcoin. “It is four times quicker to mine a Litecoin block, taking only two and a half minutes as opposed to Bitcoin’s ten.” Litecoin also increased the maximum number of coins to 84 million, much higher than Bitcoin’s 21 million limit.

Ethereum (ETH) or “ether” is another altcoin used on the dark web. It has gained popularity due to its unique concept of smart contracts, a protocol that allows anonymous parties to “enter into a binding, transparent agreement with each other. Value can be transferred between parties or held in escrow inside the smart contract itself.”
Cryptocurrency Wallets

Before making dark web purchases, one must first obtain a cryptocurrency wallet. Below is a brief overview of how cryptocurrency wallets work, types of cryptocurrency wallets, and key terms that will be important for law enforcement to understand before beginning to conduct investigations related to dark web activity. Bitcoin wallets will be the focus of discussion since Bitcoin is the most widely used type of cryptocurrency.

How Cryptocurrency Wallets Work: Public and Private Keys

- It is important to become familiar with the terms public key and private key as they are the basic components of cryptocurrency wallets.

Cryptocurrency wallets do not actually store currency. They are software programs that store public and private keys. These keys are what allow the digital wallet to “interface with various blockchains so users can monitor their balance, send money and conduct other operations.”

Basically, the public key is, as its name implies, publicly known and used for identification purposes – it is a public address. The private key, also as described by its name, is meant to be kept secret. It is used for authentication and for encryption. These keys are used together as a pair for cryptocurrency transactions. An analogy comparing the use of public and private keys to sending email explains the process in a more simplified way. If you’d like someone to send you an email, you must first give them your email address. Similarly, if you want someone to send you some cryptocurrency, you must first give them your public key. If you want to read the email and/or send one, you will have to enter your email password to gain access to your account. Similarly, to make cryptocurrency transactions, a private key is like a password to your cryptocurrency wallet.

The private key is very important. Possession of the private key allows access to the wallet’s contents. Just as you cannot access your email without your password, you cannot access your cryptocurrency wallet without your private key. For this reason, people may write down their private key or keep it a copy of it somewhere on their computer or phone. Below is a screenshot showing what the public and private keys look like for a paper Bitcoin wallet. The public key is the unique alphanumeric identifier for one’s account on the blockchain. It can be viewed by anyone at blockchain.com/explorer. The private key is also an alphanumeric string, but it is typically known only to the user of the account. “While the public key is used to deposit Bitcoins into a wallet, the private key is used to withdraw them.” Without the private key, one is not able to access their cryptocurrency. The QR codes shown below are also the public and private keys in a scannable form.
How Cryptocurrency Wallets Work: “Backup,” “Recovery,” or “Seed” Phrase

If someone loses their private key or if they can’t access it where it is stored due to a problem with their phone or computer, etc, there is still a chance that the wallet can be recovered, but only if the owner has access to their back-up phrase called a “seed.” As shown in the screenshot on the right, a wallet seed is generated when one opens their cryptocurrency wallet account. It is a mnemonic phrase consisting of a string of either 12, 18, or 24 random words. Seeing this random string of words can become important if discovered during a dark web-related investigation because it is information related to one’s private key.

Websites with information about cryptocurrency wallets warn owners to keep their wallet “seeds” hidden in a secure location. By obtaining the “seed,” one would technically be able to clone the wallet and access its funds. If investigators see a handwritten list of words on notepaper, such as in the photo on the left, or saved as screenshots on phones or on computers, it could be much more valuable information than one would typically assume at first glance. Investigators advise not to just take a picture of the seed, but to physically seize it because otherwise the suspect can still use it to recover their private key. The same holds true if one were to find the private key.

Types of Cryptocurrency Wallets

There are three main categories of cryptocurrency wallets: hardware, software, and paper. Software wallets can be desktop, mobile or online. Each of these types of wallets will be described briefly on the following pages, along with icons for the various brands and/or applications so that investigators will be more likely to be able to identify the use of cryptocurrency wallets if they come across them in their case work.
Hardware Wallets

Hardware wallets store a user’s private key on a device that looks like a USB drive. Two of the better-known hardware wallets include Ledger and Trezor, as shown in the accompanying photos. Digital Bitbox and Keep Key are also hardware wallets. To make a cryptocurrency transaction, users “simply plug in their device to any internet-enabled computer or device, enter a pin, send currency and confirm.” Hardware wallets are described as extremely secure compared to the other types of wallets and thus recommended for those who have a large amount of cryptocurrency. It is important for law enforcement officers to become familiar with what these hardware wallets look like as they can become a very valuable part of a dark web investigation if found during a search.

Software Wallets

Desktop: Desktop cryptocurrency wallets are downloaded onto one’s personal computer or laptop. They are considered to have a high level of security, but these wallets can only be accessed from the specific computer on which they were installed so they are not as easily accessible “on-the-go.” With this type of wallet, it is recommended to have a digital back up of one’s wallet in case something happens to the computer on which the wallet is downloaded. Some of the more popular desktop Bitcoin wallets include Atomic, Exodus, Jaxx, Electrum, Copay and Bitcoin Core.

Mobile: Mobile cryptocurrency wallets run on applications on one’s smartphone. They are convenient because of their ease of accessibility, low cost, and ease of use. They are, however, less likely to be as secure. Therefore, it is recommended that individuals only keep a small amount of cryptocurrency in this type of wallet at a time. Many of the desktop wallets discussed have a mobile version. Some examples of mobile wallets are Bitcoin Wallet, AirBitz, Mycelium, Coinomi, Coinbase, Infinito Wallet, Bither, FreeWallet, and Green Address, as well as Electrum and Jaxx.

Online/Web-Based: Online wallets are accessible from any computing device in any location, making them very convenient. However, because they are “in the cloud,” the owner’s private keys are stored online. Since they are controlled by a third party, they are more vulnerable to security issues than other types of cryptocurrency wallets. Some example of web-based cryptocurrency wallets include BitGo, BTC.com, and Coin.Space.
Paper Wallets

A paper cryptocurrency wallet is simply a paper print out with information on one’s public and private key on it, along with scannable QR codes that also contain this information. It is considered the safest type of wallet because it is not vulnerable to computer viruses or device malfunctions, hacking or other technological issues that can occur with the other types of cryptocurrency wallets. Paper cryptocurrency wallets can be generated at sites such as walletgenerator.net. This website gives step-by-step instructions on how to obtain and print a paper wallet. Dark web drug investigators emphasize that if officers see a paper wallet in the course of their investigation, they should photograph it, but cover up the private key so it can’t be accessed by anyone else. One must be able to clone the wallet in order to seize the cryptocurrency. Wallets are cloned by using the private key. If you see a private key, this is very important information.

Icons for Cryptocurrency Wallets

Law enforcement should be aware that if they see any of these icons on one’s phone or computer it could be an indicator of dark-web related activity. Handwritten notes or information on one’s phone may have valuable information related to their cryptocurrency wallets such as the private key or seed phrase. Dark web drug investigators say that Bitcoin and other virtual currencies can be transferred by anyone with the proper passwords and/or recovery seed phrase and that when an officer encounters virtually currency that they plan to take from the target, they should transfer it to government control immediately. Even with the target in custody, someone else could transfer all of the virtual currency and leave basically no trail.

Step 0. Follow the security checklist recommendation

First step is to download this website from GitHub and open the index.html file directly from your computer. It’s just too easy to sneak some evil code in the 600+ lines of javascript to leak your private key, and you don’t want to see your fund stolen. Copy version control make it much easier to cross check what actually run. For extra security, unplug your Internet access while generating your wallet.

Step 1. Generate new address

Choose your currency and click on the “Generate new address” button.

Step 2. Print the Paper Wallet

Click the Paper Wallet tab and print the page on high quality settings. Never save the page as a PDF file to print it later since a file is more likely to be hacked than a piece of paper.

Step 3. Fold the Paper Wallet

Fold your new Paper wallet following the lines.

You can insert one slide inside the other to lock the wallet.

Step 4. Share your public address

Use your public address to receive money from other crypto-currency users. You can share your public address as much as you want.

Step 5. Keep your private key secret

The private key is literally the keys to your coins, if someone was to obtain it they could withdraw the funds currently in the wallet, and any funds that might be deposited in that wallet.

Please test spending a small amount before receiving any large payments.
Other Important Information about Cryptocurrency Wallets

Multi Signature Wallets ("Multi-Sig")

Another term that investigators may hear when beginning to work dark web-related cases is the term “multi-sig.” Some cryptocurrency wallets, as well as some darknet marketplaces, offer a multi-signature feature to make transactions more secure. Some examples of multi-signature desktop/mobile cryptocurrency wallets for Bitcoin include, but are not limited to Electrum, Armory, CoPay, and BitGo. Whereas most cryptocurrency wallets use a single private key, multi-signature wallets require more than one private key for a transaction to be authorized. These are called M-of-N transactions. For example, one’s wallet can be configured for 2-of-3 authorized signatures, meaning that a transaction will only become valid after at least two of three “authorizers” have provided signatures to approve it. Another term that investigators may hear when beginning to work dark web-related cases is the word “multi-sig.” Some cryptocurrency wallets, as well as some darknet marketplaces, offer a multi-signature feature to make transactions more secure. Some examples of multi-signature desktop/mobile cryptocurrency wallets for Bitcoin include, but are not limited to Electrum, Armory, CoPay, and BitGo. Whereas most cryptocurrency wallets use a single private key, multi-signature wallets require more than one private key for a transaction to be authorized. These are called M-of-N transactions. For example, one’s wallet can be configured for 2-of-3 authorized signatures, meaning that a transaction will only become valid after at least two of three “authorizers” have provided signatures to approve it. A user can provide his private key on his phone for a transaction. The service provider for the multi-signature wallet will then receive a message regarding this signature and then provide the second, or two out of three signatures needed for the transaction. A short and informative video explaining how this works in more detail can be found at https://coinsutra.com/best-multi-signature-bitcoin-wallets/.

Some darknet marketplaces use a similar “multi-sig” process for transactions on their websites, requiring more than one party to approve a transaction before the payment will be released from escrow. For this service, the marketplace will generally charge a small fee. With “2-of-2 multi-sig,” the buyer and seller must both provide signatures before payment will be released. In “2-of-3 multi-sig,” the buyer, seller, and escrow agent (the site administrator) must all sign before payment will be released. “2-of-3 multi-sig” is reportedly becoming an increasingly popular option.

This chart from the document The State of Opioid Sales on the Dark Web by LegitScript shows the escrow or “multi-sig” process used on darknet drug markets.
Ways to Increase Anonymity of Cryptocurrency Wallet Transactions

One-Time Use of Bitcoin Wallet Addresses to Protect Anonymity: Cryptocurrency wallets are considered to be “pseudonymous,” meaning they are not completely anonymous. Although identifying information such as one’s name and address won’t be found on the blockchain, data such as one’s wallet address is stored there publicly and permanently. Law enforcement investigations have shown that information on the blockchain can be analyzed using forensic blockchain analysis software, and in some instances, these forensic tools, along with other information have led to the identification of cryptocurrency wallet owners. To eliminate the tracing of transactions through one’s public key, some Bitcoin wallet users attempt to protect their anonymity by creating a new Bitcoin address for each of their transactions. Although cumbersome, this work-around may protect them from law enforcement scrutiny. Although they are not always successful, blockchain analytical tools can be very helpful for dark web investigators. Some forensic blockchain analysis services include Chainalysis, BlockSeer, Coinalytics, Elliptic, and Blockchain Intelligence Group. Although not as quick or sophisticated as the software programs provided by these companies, individuals can also analyze the blockchain themselves by going to walletexplorer.com.

Coin Mixing Services as Anonymizers to Defeat Blockchain Analysis Tools: Before using cryptocurrency, some individuals will have their cryptocurrency mixed with others to make their transactions more anonymous and harder to track. Coin mixing businesses will provide this tumbling service for a fee that is typically 1-3% of the total. Essentially, when one sends Bitcoins to a mixing service, the service will send them an equal amount of other people’s Bitcoins, minus their fee. Some of the most popular Bitcoin mixing services one can access through the Tor Network include BestMixer.io, PrivCoin.io, Bitco in Blender, CryptoMixer, Bitcoin Fog, Blender.io and MixTum.io. Dream Market also provides mixing services.

Methods of Purchasing Cryptocurrency

Various Methods of Buying Bitcoin and other Cryptocurrencies

Once one has obtained a cryptocurrency wallet, purchasing cryptocurrency such as Bitcoin can be accomplished in a number of different ways. Some methods are quite transparent, but there are other more privacy-focused options for those who prefer to protect their anonymity. The main methods involve the use of fiat and “C2C” cryptocurrency exchanges, peer-to-peer exchanges, and cryptocurrency ATMs. Each of these methods will be described briefly.
Fiat and “C2C” Exchanges

Licensed cryptocurrency exchanges are the most transparent method of obtaining cryptocurrency. Coinbase is the most popular online cryptocurrency exchange in the United States, but there are many other exchanges. Some of these include Kraken, Coinmama, Luno, Bitpanda (called the Coinbase of Europe), Cex, Bitstamp, and Gemini. These “fiat” exchanges allow government-backed currency to be traded for cryptocurrency. To use exchanges like Coinbase, one must provide official identification and then for a fee, users can purchase various types of cryptocurrency using their bank account or credit card. Coinbase is particularly convenient because one can obtain a cryptocurrency wallet directly from this exchange.117,118,119

“C2C” exchanges allow cryptocurrencies to be traded for other cryptocurrencies. Some of these “crypto-to-crypto” exchanges include Shapeshift, Binance, Changelly, Kucoin, Bittrex, Cryptopia, Bitfinex, and Poloniex. 117,120

Peer-to-Peer Exchanges

For those who want a more anonymous way of purchasing cryptocurrency, localbitcoins.com offers a peer-to-peer (P2P) exchange.121 This type of exchange allows users to trade between themselves. It also operates as an escrow service. Users of this method meet in person for the trade and can even pay with cash allowing Bitcoin to be purchased “without linking an identity to an exchange.”117 To use this exchange, one can type in their location and obtain a list of buyers and/or sellers of Bitcoin. Sellers list information such as the price they are asking for the Bitcoin, what type of payment will be accepted, and a method of contacting them for the transaction. This method offers a higher degree of privacy for users and is reportedly favored by darknet market users. Other P2P exchanges include BitSquare, Coinffeine, and OpenBitcoin Privacy Project.
Cryptocurrency ATMs

Another method of obtaining small amounts of cryptocurrency anonymously is through the use of cryptocurrency ATMs. For larger amounts, some information may need to be provided. There are actually over 4,000 of these machines, according to coinatmradar.com. They estimate that approximately nine cryptocurrency ATMs are being installed throughout the world each day.\textsuperscript{122,123} The coinatmradar.com website keeps a listing of the location of these ATM machines and one can use the search option on their online map to find those that are nearby.

Although all of these methods of obtaining cryptocurrency can be used for legitimate purposes, according to investigators, darknet market purchasers are known to use these anonymous services to obtain cryptocurrency to buy illicit drugs such as fentanyl and fentanyl analogs. Those working dark web-related drug cases report that Bitcoin ATMs are ideal locations for developing targets for investigations. Money laundering suspects using Bitcoin ATMs use the same techniques as in traditional ATM narcotics investigations. These institutions fall under banking acts requiring them to file SARs and therefore, officers can serve court orders to obtain account information.
Sending and Receiving Cryptocurrency

How to Send and Receive Cryptocurrency: Example with a Bitcoin Wallet

After an individual has obtained a cryptocurrency wallet and has purchased cryptocurrency, they will be able to both send and receive cryptocurrency. The following screenshot shows what it looks like inside a Bitcoin Wallet. In order to send Bitcoins to someone, one must first know the public wallet address of the recipient in order to send the cryptocurrency payment. This is put into the “Pay To” line, as shown below. It is very important to be sure the address is correct because cryptocurrency transactions are irreversible. In order to receive cryptocurrency, one will need to share their public wallet address with the sender. If the sender and user are together in the same place, both sending and receiving can be accomplished by allowing the QR code for public address to be scanned.124

How to Send and Receive Cryptocurrency: Example with an Ethereum or “Ether” Wallet

While most Bitcoin public addresses start with the numbers 1 or 3, the Ethereum public addresses start with 0x, as shown in the example below.125,126 For Litecoin, they start with an L.124 Monero public addresses begin with a number 4. This is one way to tell some of the various cryptocurrencies apart if an investigator finds what appears to be a cryptocurrency public address written down somewhere during the course of an investigation. Other examples of indicators of cryptocurrency use are provided in Appendix C on pages 37 through 43.
Cryptocurrency Transactions on Dark Web Drug Markets

As mentioned earlier in this report, there are numerous websites on the clearnet that provide detailed instructions for those who wish to make purchases with cryptocurrency on darknet marketplaces. Investigators say that these sites are a great place for law enforcement to learn about the dark web without actually going there themselves. Darkwebrnews.com provides screenshots of the process for making purchases on Dream Market.127 Another similar tutorial can be found on deepdotweb.com.128 Some screenshots from these websites are provided below to illustrate the process that individuals use to order illicit drugs and other items on the dark web.

After opening an account on Dream Market, it must be set up to accept the various types of cryptocurrency the potential buyer has in their wallet. In the screenshot below, when Bitcoin (BTC) is clicked on to the left of the cart, a Bitcoin address appears on the screen. This address is where a buyer will need to send Bitcoins to add them to their Dream Market account. This same process can be repeated for other types of digital currencies.

Adding Types of Cryptocurrency Options to a Dream Market Account

![Image of Dream Market interface showing cryptocurrency options and withdrawal process.]

To generate a Bitcoin wallet or to see your BTC wallet, click on the "Bitcoin" Option and the page below appears.

![Image showing Bitcoin wallet setup on a web interface.]

To withdraw Bitcoins, scroll down on the same page until you see the withdraw option as shown below.

![Image with instructions on how to withdraw Bitcoins from a Dream Market account.]

Send bitcoins to the address from above to deposit bitcoins into your account. After you have sent bitcoins to this address the deposit will show up instantly as pending balance. After an average of 20 minutes (2 confirmations) the deposit is confirmed. Addresses are valid for one week. The bitcoin address will change after each deposit, please always deposit to the latest address. Get proof of ownership here.
Now that a buyer has deposited cryptocurrency in their Dream Market account, they are ready to make a purchase. After browsing through the categories of items for sale and choosing a product to buy, they can click on the item to view additional information about it and also about the vendor such as vendor ratings. To order the item, the buyer will click on it and then click on “View Offer” to review the vendor’s terms of sale and, if acceptable, they will then click on the “Add to Cart” option. At this time, a screen will appear showing the types of cryptocurrency the vendor will accept. The buyer must choose from the types on the vendor list. Only one type of cryptocurrency can be selected for the transaction.

**Choosing an Item for Purchase and Payment Type**

![Dream Market screenshot](image)

**How to Buy**

Even though there are three cryptocurrencies in the marketplace, it is important to note that you cannot use all of them.

The first step is to identify what cryptocurrency the vendor accepts before you can go ahead and make a deposit.

![Crypto selection screenshot](image)

If the vendor accepts all the three options as shown above, then you may select one cryptocurrency then proceed and click “Add to cart.”
The buyer will need to communicate with the vendor at some point before finalizing the sale because the vendor needs to know where to send the purchased item. In order to maintain privacy of vendor-buyer communications, PGP encryption is generally used when sending sensitive information about the name and address for the package label. PGP conversations may also include what type of “stealth” packaging, if any, will be provided to conceal purchased items such as illicit drugs. With PGP encryption, each person has a key pair: a public key and a private key. On these marketplaces, vendors provide their public PGP key. The buyer uses the vendor’s public PGP key to send an encrypted message and the vendor will use the buyer’s public PGP key to send a response. Both parties have their own private PGP key that they will use to decrypt and read their messages. To send private, protected messages on Dream Market, the buyer must click on the box that says Encrypt. A PGP encryption option will appear on the screen.

Using PGP Encryption for Vendor-Buyer Communications

"Each public key is bound to a username or an e-mail address” and therefore, they can become important clues in investigations. In some instances, the email address may have been used for other purposes, for instance, for P.O. box applications or mailing/shipping-related accounts. Dark web investigators say that a public PGP key is almost like a digital fingerprint on the dark web markets because it is common for vendors to use the same public PGP key on various markets. Vendors try to provide evidence of their trustworthiness by showing that they’ve been selling successfully since Silk Road or AlphaBay were operational, and they use numbers and symbols to show this, as in the screenshot above. Their posted public PGP keys can be compared to seized data from these earlier markets, potentially providing identification information such as an address and a time frame that may prove to be important in a current investigation."
Tips related to the Postal Aspect of Dark Web Drug Investigations: Identifying Shipments of Products Purchased on Dark Web Drug Markets

Drugs purchased on anonymous darknet markets still have to be mailed in order for the buyer to receive them. According to dark web investigators, most of these purchases are coming through the U.S. Postal Service. Law enforcement can exploit this vulnerability by working with their local postal inspectors to identify these purchasers. These tips related to shipment methods used by darknet vendors may assist investigators to understand this important aspect of dark web-related drug cases.

- Dark web narcotics transactions are largely conducted via the U.S. mail system. Online forums exhaustively cover the benefits of using the U.S. mail system versus a private courier service such as FedEx or UPS (courier services grant no expectation of privacy, can be opened with consent of the company, or by state search warrant, while U.S. mail requires a federal search warrant to open). The former “Reddit” posts on darknet have been moved to the “Dread” forum on Tor which posts numerous boards on tradecraft for shipping and receiving narcotics via U.S. mail and international mail.

- Dark web marketplaces and forums are aware of narcotics parcel profile characteristics. They go to great lengths to avoid packages giving any indications, and often use multiple methods to conceal and mask detection by K9. Unlike traditional narcotics parcels, which are large, heavily-taped, handwritten with fictitious names, and mailed over the Postal counter paid by cash:
  - Dark web parcels are small, often using flat rate envelopes and “bubble” mailers.
  - The labels are usually typed or computer-generated accounts that appear to be legitimate mailings. Vendors will often use company returns in order to further attempt to legitimize the parcel.
  - Most times the parcels are addressed to a person’s true name.
  - Vendors are aware to use gloves while packaging the mail, often using multiple layers of vacuum sealed and Mylar seal bags to reduce the presence of odor contamination and latent fingerprints.
  - Vendors will generally never enter a post office to mail and will drop the parcels in multiple blue boxes in several different areas in order to conceal their location.
  - Tradecraft to conceal detection for dark web vendors is so important, vendors on markets are selling rolls of stamps, tracking number labels, and mailing containers to further obfuscate the purchaser’s origin.
  - Dark web traffickers often use VPN services, hosted overseas to protect their browsing history, and employ IP masking functions to hide IPs when tracking parcels.

- Dark web traffickers have shown a significant desire to continually learn and improve their tradecraft on shipping narcotics. Dark web users are using PACER to obtain court records on indictments and affidavits, which show steps LEOs took to ID and arrest a vendor or receiver. It is common to find copies of the orders from PACER uploaded to the dark web. Some newer trends learned from Silk Road and AlphaBay are:
  - All communications, private messages, and order logs are deleted upon receipt. On a recent proffer, a dark web mailer for a vendor who operated a separate buyer account stated he was instructed to delete everything on this account after reading it, so if he was ever arrested and his account compromised, there would be nothing left to incriminate anyone else.
• Dark web traffickers are now rarely providing tracking numbers on transactions and will only provide them to site moderators on marketplaces like “Dream” and Wall Street” to dispute if an order never arrived.
• Dark web users are using a “dead man switch”, which means upon arrest, their accounts are held by a trusted associate who will be called with their first phone call. The trusted associate will then delete as much account history as possible and liquidate all Bitcoin so it cannot be seized.
• Dark web users are increasingly familiar with law enforcement techniques and terminologies. Dark web forums explain what controlled deliveries and knock and talks are, and give advice about how to handle them to avoid arrest. Open source forums will freely discuss the implications of receiving a “love letter,” and how to sanitize one’s house, computer, phones, and addresses from further law enforcement investigations. A domestic love letter is the code for a USPIS seizure letter, and an international love letter is code for a CBP border seizure letter.

- Indications of a dark web mailer on a traffic stop:
  - Will have numerous flat rate and bubble mailing envelopes packaged and ready to ship, despite just leaving a post office, or make spontaneous utterances that he is going somewhere else besides the post office.
  - The person in the vehicle will have no affiliation to the sender name on the parcels.
  - Their phone may contain the Tor app.
  - The vehicle may contain journals with handwritten seed phrases, cryptocurrency wallet addresses, paper wallets, and order numbers.
  - Their residence will contain more drugs and packaging materials.

**Some Packaging Materials from Dark Web Investigations**

- Mail Box Keys or PO Box Keys
- Flat Rate Envelopes
- Mailing Labels
- Mylar Bags
- Activated Carbon – looks like coffee grounds and is used for packaging the meth for international shipments. The theory is that the scent thrown off may confuse narcotics dogs that may be in the vicinity.
- Heat Sealed Bags – The Meth was double bagged in Ziploc bags then mixed with the activated carbon, then heat sealed in the food bags for shipment.
- Heat Sealing Device
Appendix A: Peter the Great Case Study


---

**Peter the Great: A Case Study in New Investigative Techniques**

*How an Overdose Death in Portland, Oregon Led Police to an International Online Drug Trafficker*

When there is a fatal drug overdose in Portland, Oregon, the Portland Police Bureau (PPB) immediately initiates a full-scale investigation into the circumstances surrounding the death. If detectives can determine who supplied the drugs and the evidence is strong enough, prosecutors may seek so-called “Len Bias charges” against the supplier.

Named after the University of Maryland basketball star who died of a cocaine overdose in 1986, the Len Bias Act is a federal law that provides for a 20-year minimum prison term for dealers convicted of supplying drugs that result in a person’s death. Under the law, when a local police department investigates an overdose death, the U.S. Attorney’s Office in that jurisdiction may take the case for federal prosecution if sufficient evidence is present and certain requirements are met. In Portland, the PPB works closely with the U.S. Attorney’s Office and federal law enforcement agencies to determine whether a case warrants prosecution under the Len Bias Act.

A recent opioid overdose case in Portland illustrates the important role that technology—in particular, dark web investigations—can play in drug trafficking investigations. At the Critical Issues meeting, officials with the Portland Police Bureau, Immigration and Customs Enforcement/Homeland Security Investigations (ICE/HSI), the U.S. Postal Inspection Service, and the Greenville, SC Police Department detailed a compelling case that they recently investigated, involving an online trafficker who went by the name of “Peter the Great.”

**Combining Digital and Physical Evidence to Trace the Last Actions of an Overdose Victim**

On February 16, 2017, 18-year-old Aisha Zughieb-Collins was found dead in her Southeast Portland apartment from an overdose of a synthetic opioid called U-47700 (or simply U4). The drug was so new to the Portland area that neither police investigators nor the city’s public health officials had ever encountered it before.

Aisha’s mother, suspecting that her daughter had purchased the drugs online, provided detectives with Aisha’s email address. That was a start, but not enough to launch an online investigation.

At the scene, however, detectives uncovered important physical evidence indicating that the drugs had likely been shipped through the mail. This evidence included a distinctive brand of pregnancy kit (sold only at Dollar Tree stores) that was likely used to hide the drugs during shipment. They also found a mailing envelope inside the apartment. U.S. postal inspectors determined that envelope had a fictitious return address, but that it was purchased at a post office in Greenville, SC. Importantly, they discovered a notepad with an alphanumeric code written on it.

Unsure of what the code meant, Portland police turned to a Portland-based ICE/HSI agent who is regarded as a national expert in “dark web” marketplaces, where synthetic opioids and other drugs are often sold. Special Agent Cuy Gino is assigned full-time to Portland’s High Intensity Drug Trafficking Area (HIDTA) interdiction team. He is housed in a PPB facility, and therefore can work directly with police investigators at the onset of cases such as this one that involve the dark web.

Investigators learned that the alphanumeric code was Aisha’s PGP key. PGP, or Pretty Good Privacy, is an encryption program designed to increase the security of email communications and other online transactions. PGP keys are often used by individuals to access hidden marketplaces on the dark web.

**One Case Leads to Nearly 10,000 Drug Transactions**

Using Aisha’s email address and PGP key, investigators determined that just five days before her death, she had purchased the U-4 opioid on a dark web marketplace called AlphaBay, which had emerged as
a leading marketplace for illegal merchandise following the takedown of Silk Road in 2013. The date of that purchase matched up with the timing of the mailing envelope recovered inside Aisha’s apartment. The alleged online seller’s username was “Peter the Great.” Data from AlphaBay indicated he had made nearly 10,000 transactions on the site.

In April, detectives went on the dark web and purchased U4 from Peter the Great. The drugs arrived wrapped in the same pregnancy kits and containing the same type of shipping labels found in Aisha’s apartment. Postal inspectors further determined that the shipping labels used on the packaging originated from an online company that accepts only Bitcoin digital currency.

From Portland, to Greenville, to China
Further investigation revealed that the online shipping label purchases were tied to two secure email addresses. Investigators filed a subpoena for any records connected to those email addresses. That led them to Theodore Khleborod, a person of interest living in Greenville. Detectives determined that Khleborod had received numerous international packages from China, where a great deal of U4 is made. Through social media postings, they also found out that Khleborod was in a relationship with a woman named Ana Barrero.

Next, investigators collected sales information showing a spike in pregnancy kit purchases at a particular Dollar Tree store in Greenville. They also retrieved store video showing Barrero purchasing numerous pregnancy kits at that store. Portland officials traveled to Greenville and, with the assistance of Greenville Police and ICE/HIS agents in South Carolina, began surveillance of both Khleborod and Barrero. They witnessed Barrero mailing large numbers of parcels that matched other packages in the investigation, including the one from Aisha’s apartment.

In late April, officers arrested Khleborod and Barrero. They faced federal drug distribution charges in both South Carolina and Oregon, with Oregon officials considering additional “Len Bias charges” as well. Investigators believed “Peter the Great” may be connected to more than a dozen other overdose deaths across the country. In November 2017, Khleborod was found dead in a jail cell in Spartanburg County, SC, an apparent suicide.

3 Lessons Learned
From the Peter the Great case, the Portland Police Bureau developed critical lessons for future high-tech overdose investigations. Captain Mark Kruger and Sergeant Chris Kenagy outlined three of those lessons at the Critical Issues meeting:

1. Police and prosecutors need to develop a working knowledge of the dark web and the use of cryptocurrency (such as Bitcoin). These investigative elements can be present not only in drug cases, but also gun sales, human trafficking, and financial fraud crimes committed by gang members and other criminals to fund their operations.

2. To effectively collect and analyze digital evidence from the dark web, local, state, and federal agencies should have a close working relationship with one another and be willing to share information, resources, and expertise.

3. New, technology-based approaches to criminal investigations are important, but they must be combined with traditional investigative work that is thorough and detailed.

Captain Kruger noted that if every state had at least one multi-jurisdictional team like the Portland HIDTA that investigated overdose deaths, and if each team conducted at least one major takedown per year, then police could potentially save hundreds of lives.
Appendix B: How HSI Assists Local and State Law Enforcement in Online Opioid Trafficking Investigations

This information was extracted from an article entitled Opioid Distribution on the Dark Web published in the Police Chief Magazine in March of 2018. It can be accessed at www.policechiefmagazine.org/wp-content/uploads/PoliceChief_March-2018_F2_WEB.pdf.
Appendix C:
Indicators of Dark Web Marketplace and Cryptocurrency Use from Actual Dark Web Drug Investigations

Paper Bitcoin Wallets with Private Key Covered Up
Paper Wallet for the Cryptocurrency “Ether” (Ethereum) and Notes Related to Buying Cryptocurrency

Password - GYRACLAC05secrrityn0248

Binance.com - Site to buy TRON.
email - lanivlife
pass - gyebradaj astractag 6y5i0322
10878288

Backup Key - W7AZWK6A7BDCLVVY

liqui.io
email - lanivlife
pass - gyebradaj 8

TRON - TRX account

ShapeShift.io

Big money
Bircon with Credit Card.
Example showing the “Seed” Recovery Phrase for an Electrum Cryptocurrency Wallet

Localbitcoin.com
Login – davenport216
Pass – darknets

Dream Market - 0322987
Silk Road
Wallstreet Market
Name – gregorian45
Pass – kryptonite

Point T.chka
Login – steve1
Pass – kryptonite

Wallet one - Bitstamp
Wallet two - Electrum
Wallet three - Coin Core

Electrum - oval once skin before scan
fossil language time rubber goat useless have

Pass - 9741032

coin@net

Million dollars - Pass
Secret Pass - 9741032

(070)

London

UPN Connection
Example Showing Information about Ripple Cryptocurrency including a Ripple Wallet Address

CXRPS

Gatehub.net

Ripple Cryptocurrency

email: lanier@quasi.com

password: quasilanier088

@lanier

Gatehub for deposit

Authentication Key

Gatehub.net

AC04F1785D6672AF45D5462
973E2496

057455

Ripple Wallet Address

rz2wythcu2rBv0Vt7N7zmKVC6Z6J 94n
Information related to a Peer-to-Peer Bitcoin Exchange, Dark Web Drug Market Accounts, Cryptocurrency Wallets and a Bitcoin “Tumbler” (Coincure)

Localbitcoin.com
Login – davenport216
Password – darknets
Email – davenport1522@mail.com

Dream Market – 0322987
Silk Road
Wallstreet Market
All three sites - User Name (gregorian45), Password (kryptonite)

Point T.chka
Login – steve1
Password – kryptonite

Bitcoin Wallets – (user 2015@protonmail.com (password – milliondollars)
1. Bitstamp – my account info
2. Electrum (oval once skin before scan fossil language time rubber goat useless have)
   (password – gyasi0322)
3. Coincure.net – bitcoin laundering account – (user 0702) (password –
   milliondollars) VPN connection – London.
PGP Encryption Note and Handwritten Notes with the “Seed” (Recovery Phrase) for a Cryptocurrency Wallet Found During Investigation
Trezor Hardware Cryptocurrency Wallet Found During Investigation
Endnotes


33. Tor Project. *Tor at the Heart: Onion Browser (and more iOS Tor)*. (December 5, 2016). Retrieved from https://blog.torproject.org/tor-heart-onion-browser-and-more-ios-tor.


61. Photo provided by Instruq, a company that provides online training for law enforcement, including courses on topics such as the dark web and cryptocurrency, https://instruq.co/go

62. Information and dark web screenshots provided by Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), Houston, Texas in November of 2018.


