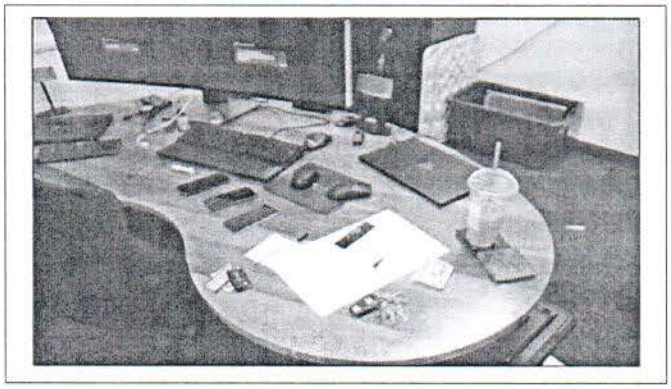
Dark Web and Cryptocurrency What to Look for During a Search Warrant

Nevada High Intensity Drug Trafficking Area BULLETIN • September 2021

(U) Overview

(U//FOUO) In June of 2021, the Nevada High Intensity Drug Trafficking Area (HIDTA) Drug Enforcement Agency (DEA) Enforcement Group 3 arrested four members of a Drug Trafficking Money Laundering Organization (DTMLO) responsible for selling millions of dollars' worth of cocaine on the dark web and transporting it through the United States Postal Services (USPS). Federal search warrants were executed at the DTMLO's primary residences in Las Vegas as well as two stash locations which resulted in the seizure of approximately 12.6 kilograms of cocaine, 13 firearms, approximately $86,000 in bulk currency, 1 vehicle, and numerous luxury motorcycles valued at $450,000. At all locations, electronic devices such as phones, computers, and cryptocurrency devices were located as well as drug records, financial documents, and paper recovery seeds. Subsequent to the search warrants, over 30 wallets were reconstituted which allowed for the seizure of approximately $115,000 worth of cryptocurrency.[1] The purpose of this product is to inform law enforcement partners on how to better recognize key indicators of dark web activity while executing search warrants. This includes information to assist law enforcement in positively identifying cryptocurrency devices, electronic applications, and recovery seeds, which is critical for seizing digital assets.

(U//LES) Photo of cocaine and pharmaceuticals found at stash location. Source: DEA Enforcement Group 3 June 2021.



(U//LES) Electronics and crypto devices located at stash location. Source: DEA Enforcement Group 3 June 2021.

(U) Relevance

(U//FOUO) In 2020, the Nevada HIDTA reported a surge in dark web drug

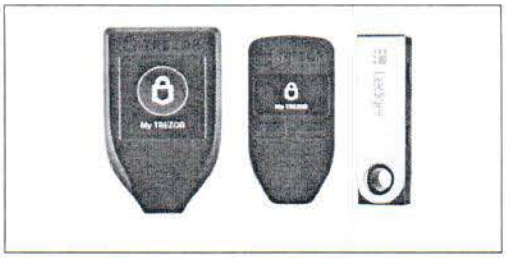
Please complete our survey by clicking on the link below.
https://www.surveymonkey.com/r/2021NVHIDTA-Information-Intelligence-Bulletin-Survey

related activity and cryptocurrency usage.[2] Due to the unique nature of the case and having limited local resources that specialized in cryptocurrency and cyber related crimes, along with several locations involved, investigators required additional support from an out-of-state digital forensics group to be on site at all locations during the execution of the search warrants. Prior to the warrants, an overview of key things to look for regarding cryptocurrency devices, recovery seeds and any electronics that could be examined for evidentiary value was necessary for all law enforcement personnel involved; however, many of the law enforcement personnel were not familiar with the information and terminology that was provided during the brief. Details and examples of what to look for during a search warrant involving dark web and cryptocurrency related crime is provided below for law enforcement partners.

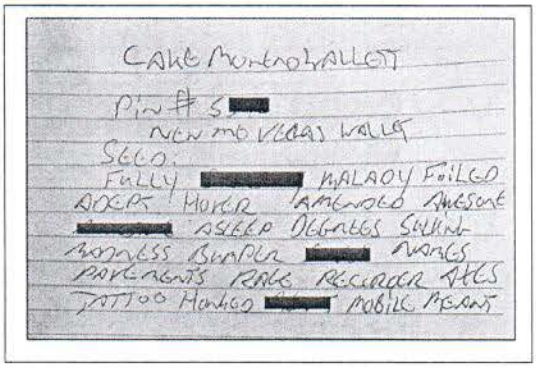
(U) Hardware Wallets and Devices

(U//FOUO) Hardware wallets are commonly used by cryptocurrency investors as well as dark web criminals and are considered the best method to store cryptocurrencies. A hardware wallet is a cryptocurrency wallet which stores the user's private keys in a secure hardware device. The main principle behind a hardware wallet is to provide full isolation between the private keys and the user's computer. Private keys are codes that only the user has access to and are used to access the user's crypto assets. Private keys are what gives the user ownership of their cryptocurrency. Hardware wallets have an associated web, mobile, and/or desktop application that enables you to monitor your cryptocurrency addresses and spend your cryptocurrency. Examples of hardware wallets are shown below.[3]

- **Trezor** – Single chip base
- **Ledger** – Double chip base (provides more security)



(U//FOUO) Example photos of Trezors and Ledger
Source: The Crypto Merchant Website August 2021.



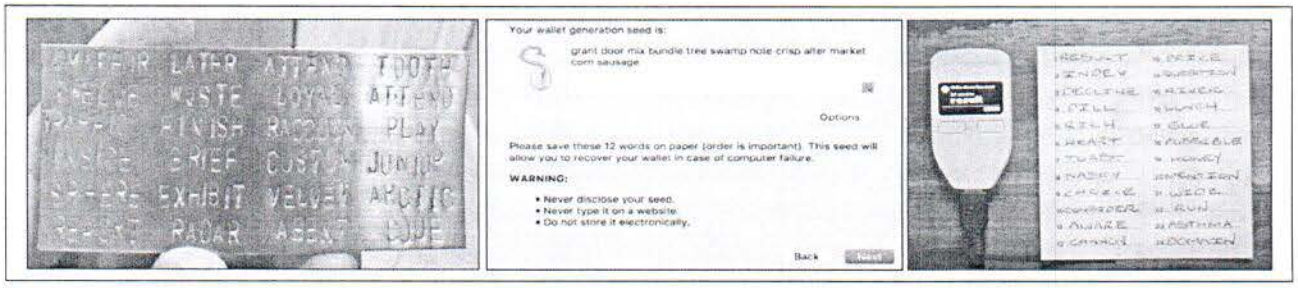
(U//LES) Photo of recovery seed belonging to a dark web pill distributor. Source: DEA Tactical Diversion Squad December 2019.

(U//FOUO) Trezor models are built on a single chip base, whereas Ledger devices use a double chip base. Ledger's second chip is a bank-grade secure element (SE), providing additional security against hardware-based attacks.

(U) Recovery Seeds and Phrases

(U//FOUO) A crypto wallet will randomly generate a seed phrase or recovery phrase in an ordered set of 12 or 24 words, sometimes more depending on the type of wallet being used. The crypto wallet also uses the seed

phrase to create private keys. The seed phrase is not linked to a particular cryptocurrency and can be used to access an entire portfolio of cryptocurrencies such as Bitcoin, Litecoin, Ethereum and other crypto assets. A seed phrase is the only way to access and recover a wallet as well as all of its contents if a device that was linked to the wallet is wiped, lost, or stolen.[4] If possible, recovering wallets and seizing cryptocurrency in an expeditious manner is highly recommended and should be treated with a sense of urgency. Anyone who maintains a copy of the recovery seed or has access to the recovery seed can re-create the wallet without geographical limitations and could easily withdrawal the funds. Examples of seed phrases are shown below.



(U//FOUO) Example photos of recovery seed phrase.
Source: The Crypto Merchant and Decryptionary website accessed August 2021.

(U) Software Wallets

(U//FOUO) Software wallets come in many forms, each with its own set of unique characteristics and are somehow connected to the internet. Wallets are distinguished by a set of supported cryptocurrencies and software platforms such as Windows, Mac and other operating systems. Software wallets are available in three forms — desktop, mobile and online.[5]

- Desktop wallets are computer programs that store cryptocurrencies on a PC so that its information is not accessible to anyone but the user. Private keys are typically kept on a desktop.

- Mobile wallets come in the form of a smartphone app and are easily accessible to their users at any time. However, mobile devices are vulnerable to various malware and can be easily lost.

- Online wallets are web-based wallets that can be accessed from anywhere and any device. This makes them more convenient for accessing funds, and their private keys are stored by website owners rather than locally on user devices.

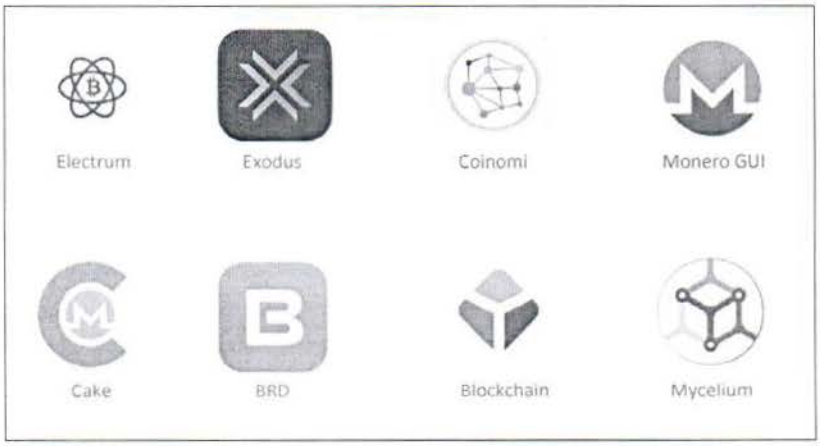
(U) Common Types of Cryptocurrencies, Wallets and Exchanges

(U//FOUO) The most common cryptocurrencies, wallets and exchanges encountered in the Nevada HIDTA AOR are shown on the following page:[6]

- **Cryptocurrency Icons:**

(U//FOUO) Photos of commonly used cryptocurrencies.
Source: Cryptologos.cc website accessed August 2021.

- **Software Wallets** are used solely for storage, sending and receiving cryptocurrency and providing more anonymity. Examples of common software wallets encountered during Nevada HIDTA investigations are shown below.



(U//FOUO) Photos of commonly used software wallets.
Source: Google images accessed August 2021.

- **Exchange Wallets** have the same functions as software wallets but can be cashed out and require specific user information. Examples are shown below.

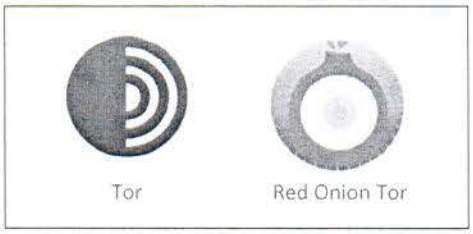
(U//FOUO) Photos of commonly used exchange wallets.
Source: Google images accessed August 2021.

Please complete our survey by clicking on the link below.
https://www.surveymonkey.com/r/2021NVHIDTA-Information-Intelligence-Bulletin-Survey

(U) Indicators of Dark Web Usage

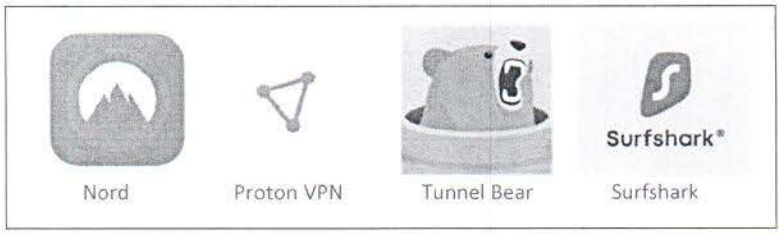
(U//FOUO) Common indicators of dark web usage used on computers and phones encountered during Nevada HIDTA investigations are shown below.[7]

- **Browsers:**



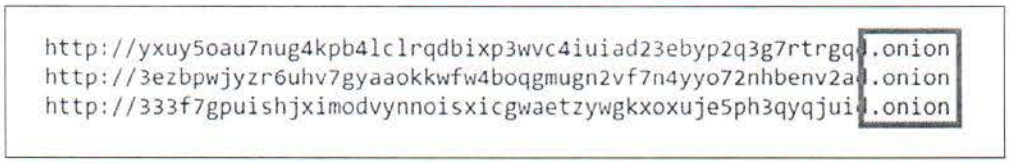
(U//FOUO) Photos of commonly used browsers.
Source: Google images accessed August 2021.

- **Virtual Private Networks (VPN):**



(U//FOUO) Photos of commonly used VPNS.
Source: Google images accessed August 2021.

- **Examples of Dark Net Market Links:**

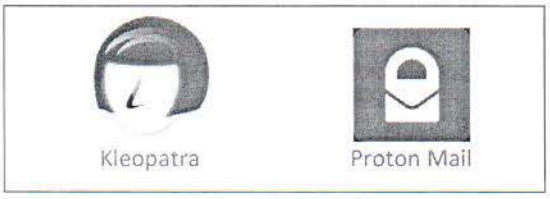


(U//FOUO) Example photo of dark net market links.
Source: Dark Net Live website accessed August 2021.

(U) Pretty Good Privacy (PGP) Encryption

(U//FOUO) Pretty Good Privacy (PGP) is an encryption system used for both sending and receiving encrypted emails and encrypting sensitive files. PGP encryption is required on most popular dark net markets such as White House Market. If messages are not encrypted using PGP encryption, dark net markets will not allow users to send and receive messages or purchase illicit commodities. Examples of PGP encryption are shown below.

- **PGP Encryption:**



(U//FOUO) Photos of commonly used PGP encryption systems.
Source: Google images accessed August 2021.

Please complete our survey by clicking on the link below.
https://www.surveymonkey.com/r/2021NVHIDTA-Information-Intelligence-Bulletin-Survey

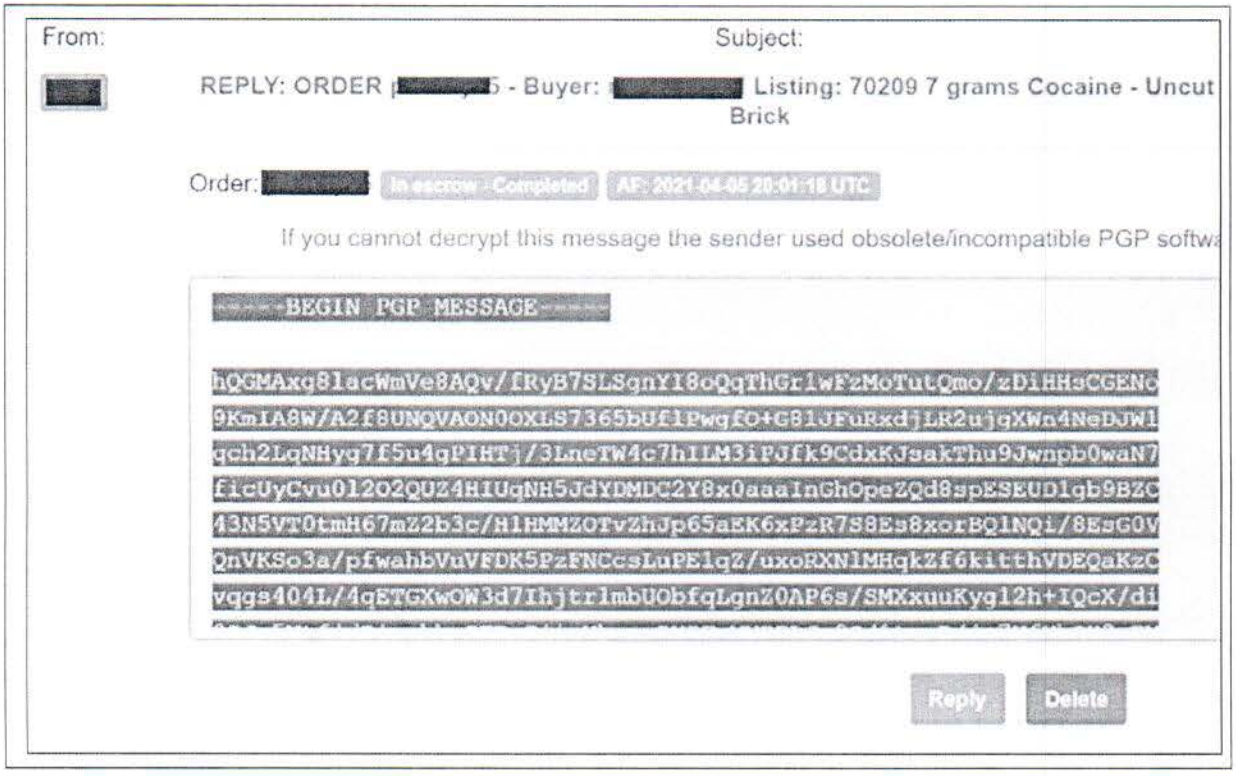
*Untitled - Notepad

File Edit Format View Help

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBF/CxbMBEADNa2cw+bcdZJ0Z6Q83Rg9W4syBhW3eWLH/CnI+D5OYXSdKU+2e
dSe03KHdfwj7Mko3MRfXpuA1Pe4ZJeBnPDRtYn7nqu5gVG6j51WgMUPkhXy8Hi8D
rqNL7qD7PaIX4eihlWZB91pD9+rKRuARIbwRE6q/Oz5739euenGyoPebrYU9Ej4Q
NZ31Fb3bRXX2rYcKEjLOcmwsWuojt6V02pX6dOGKFrxCBXMyL8fpqrqLgki+svXE
Mo3Uu0G41bhGAI2w/sxz+m2y/dv8603nLTcdIf+1tE26T2aycmEIsBIBc1ttquc7
nYq7a4i2dLH7nUJ/o1VRlDSgngvxivwJV0hr0t6HbnN1OUbgyR2UC4rzdeZOya2y
AbZ/UIvNRky2btlusJJBhbGo3ZjiSGw06En4w5Fsj6MrQlurxzupqxoP836cVhj1
XETknSYfULy47jTTmUXnyzUWZ9GAmhq3nO2tIDiQHM0GHDM1XtqvBmhgXVQAvql4
e87GtGJKCq/b+F16wGRWbd9KS0rmPY6e7ACaZqg8A0KgfXEsORo/9rkAYzEBqd4Q
F5Xjy1xhASHx4hFh7tRt91g6pzmtbtrj10CYg7eqqlI4lt2jnJrZhbHPWcy0lYjs
COv1xnSkVtqVr3lcZ0DeTM/WGnPsHDQGzDHmixw4h8MdQF8caDVuqNQO0wARAQAB
t8NJbnN0YSA8aW5zdGFaaW5zdGE+iQJOBBMBCgA4FiEEEZ1UlFg5BdmTjvLWKVC5
qwZwMnYFAl/CxbMCGwMFCwkIBwMFFQoJCAsFFgIDAQACHgECF4AACgkQKVC5qwZw
MnZaSQ/+LYHEXtb0qp9R5f9KAQaBphbFuUD8hsOHdxZmWRBOwrhijbYFqeMo0Nob
wUO3iMI8R8nckVfYz4JYxeiFAXRj0SMy+b9S/N2q8xBMFfawkKUbWqIVVZFAar4K
kb1gYqaNqY6Z65H9h6OoF+TwFkytudxHjcnEv+oiU5vpOQY53Z4e/zxyZvp1tv+1
/XFEfE19dlpKbcu1zj9PXqc0tMjDjS7MhbfumKv7WyeFWDbUv4JPdGrT5vhPHl7A
DLMLdOnlZEu2lKw4JE/cuuYcJPmoG8r+l5KohyFURgf+eMSP/pg0lyZR2ckSDaIK
EaedLDKeURDnBtye8RV066Sc0/xwrlGaFuXiHqihgeIx6ztlaNHBLiQiYT20JIv8
+dC4bwIXUlvHc5xRYkh4YRwnDBZzQNiBwp3LF2cnLRpGm2JttYPTgoVxL42L8M7I
-----END PGP PUBLIC KEY BLOCK-----
```

(U//FOUO) Photo example of PGP public key.
Source: Nevada HIDTA supported investigation August 2021



From: [redacted] Subject: REPLY: ORDER [redacted] - Buyer: [redacted] Listing: 70209 7 grams Cocaine - Uncut Brick

Order: [redacted] In escrow - Completed AF: 2021-04-05 20:01:18 UTC

If you cannot decrypt this message the sender used obsolete/incompatible PGP softwa

```
-----BEGIN PGP MESSAGE-----

hQGMAxg8lacWmVe8AQv/fRyB7SLSgnYI8oQqThGr1wFzMoTutQmo/zDiHHsCGENc
9KmIA8W/A2f8UNQVAON0OXLS7365bUflPwqfO+G81JFuRxdjLR2ujqXWn4NeDJWl
qch2LqNHyq7f5u4qPiHTj/3LneTW4c7h1LM3iPJfk9CdxKJsakThu9Jwnpb0waN7
ficUyCvu0l2O2QU24HIUqNH5JdYDMDC2Y8x0aaaInGhOpeZQd8spESEUD1gb9BZC
43N5VT0tmH67mZ2b3c/H1HMMZOTvZhJp65aEK6xPzR7S8Es8xorBQlNQi/8EsG0V
QnVKSo3a/pfwahbVuVFDK5PzFNCcsLuPE1qZ/uxoRXNlMHqkZf6kitthVDEQaKzC
vqgs404L/4qETGXwOW3d7IhjtrlmbUObfqLgnZ0AP6s/SMXxuuKyg12h+IQcX/di
```

Reply Delete

(U//LES) Photo of encrypted message on White House Market.
Source: Nevada HIDTA supported investigation accessed August 2021.

Please complete our survey by clicking on the link below.
https://www.surveymonkey.com/r/2021NVHIDTA-Information-Intelligence-Bulletin-Survey

(U//LES) Photo of decrypted message on White House Market.
Source: Nevada HIDTA supported investigation accessed August 2021.

(U) Conclusion

(U//FOUO) In 2020, the Nevada HIDTA reported an increase in dark web related drug activity and crypto currency usage and assessed with high confidence that the use of the dark web for drug trafficking and money laundering activities will continue.[8] With the progression and advancement of technologies, coupled with the rise of cryptocurrencies, it is important for all law enforcement personnel to familiarize themselves with the ever-changing methodologies that criminals utilize to participate in illegal activities such as drug trafficking, distribution and money laundering on the dark web.

(U) Contact

(U//FOUO) This bulletin was produced by Nevada HIDTA. For more information about this bulletin, please email, or direct questions to NV-HIDTA@lvmpd.com.

---

[1] (U//FOUO) Nevada HIDTA Supported Initiatives; 2021; UNCLASSIFIED//FOR OFFICIAL USE ONLY.
[2] (U//FOUO) 2020 Nevada HIDTA Threat Assessment; 2021; UNCLASSIFIED//FOR OFFICIAL USE ONLY.

[3] (U) The Crypto Merchant https://www.thecryptomerchant.com/blogs/resources/why-you-need-a-hardware-wallet-1; "Why You Need a Hardware Wallet"; 01 July 2019; UNCLASSIFIED.
[4] (U) The Crypto Merchant https://www.thecryptomerchant.com/blogs/resources/hardware-wallet-recovery-seeds-explained; "Hardware Wallet Recovery Seeds Explained"; accessed on 12 August 2021; UNCLASSIFIED.
[5] (U) Coin Telegraph https://cointelegraph.com/news/overview-of-software-wallets-the-easy-way-to-store-crypto; "Overview of Software Wallets, the Easy Way to Store Crypto"; 29 March 2020; UNCLASSIFIED.
[6] (U//FOUO) Nevada HIDTA Supported Initiatives; 2021; UNCLASSIFIED//FOR OFFICIAL USE ONLY.
[7] (U//FOUO) Nevada HIDTA Supported Initiatives; 2021; UNCLASSIFIED//FOR OFFICIAL USE ONLY.
[8] U//FOUO) 2020 Nevada HIDTA Threat Assessment; 2021; UNCLASSIFIED//FOR OFFICIAL USE ONLY.

Please complete our survey by clicking on the link below.
https://www.surveymonkey.com/r/2021NVHIDTA-Information-Intelligence-Bulletin-Survey