

Challenges: Seizure, detention and realisation

Initial thoughts

- What challenges do you foresee in relation to seizing criminal property in the form of cryptocurrencies?

Discuss in your breakout groups and record your thoughts on the following form:

<https://forms.gle/uNKuGFgGy3HKJhJB8>

Planning: Central Coordination Team

- To assist with enforcement aspects of Operation S*****d featuring cryptocurrency, a central coordination team run by NCCU Op Support will be deployed.
- This team will focus on providing officers at scene with:
 - Tactical advice on aspects relating to cryptocurrency search and seizure.
 - Technical assistance in gathering evidence relating to cryptocurrency e.g. rebuilding wallets.
 - Obtaining necessary legal authorities.
 - Providing seizure infrastructure for cryptocurrency assets e.g. NCA controlled addresses.
- It is acknowledged that this subject can be complex and the medium used to provide assistance can be important. As such Telephone, Messaging and Video calling facilities will look to be utilised as required.

Planning: Cryptocurrency Officer

- It is advised for each enforcement team to designate a cryptocurrency officer prior to the date of the operation and inform NCCU Op Support of the contact details for this individual. This officer will act as the primary contact for the central coordination team.
- Further to a telephone number being provided, this officer should also have the Signal app installed on their works mobile to allow for messaging/video calling. Access to a standalone/open source laptop would also be beneficial to this officer.
- At the scene the cryptocurrency officer will be responsible (if necessary) for managing the following:
 - First response (see following slide)
 - Recovery seeds found
 - Hardware wallets identified
 - Mobile cryptocurrency applications accessible on devices
 - Desktop applications accessible on devices
 - Sending cryptocurrency assets to addresses provided by the central coordination team.
 - Capturing transaction histories
- The cryptocurrency officer will not be expected to complete relevant processes without extensive input from the central coordination team. Further to this they will not be responsible for seeking senior officer approval in regards to the legal process used for seizure.

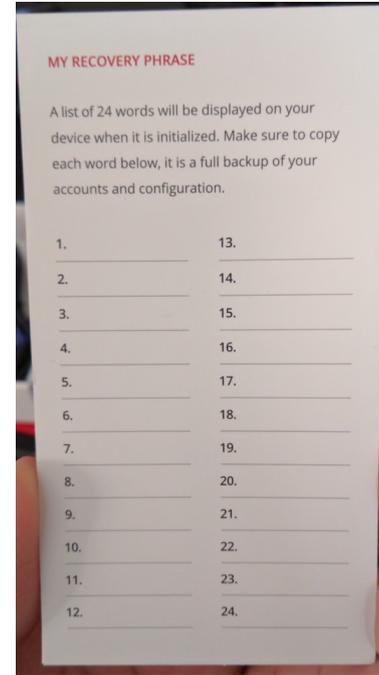
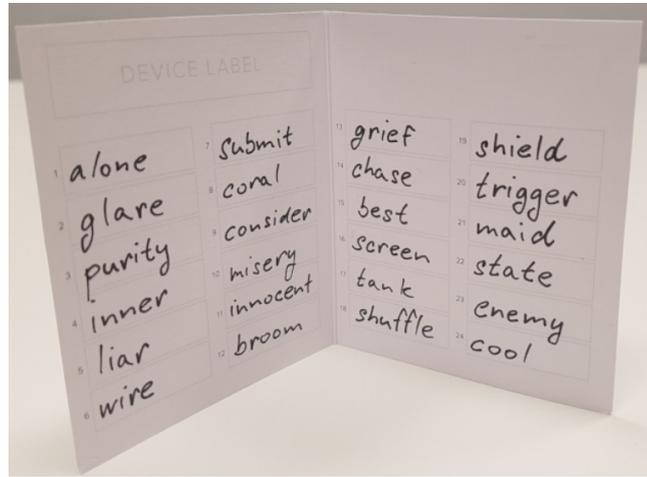
What to look for



TX ID: RKAT27
Time: 19.01.2019
12:25:36
Price: 520.00 GBP
Crypto: 0.163506 BTC
Rate: 1 BTC =
3180.311426 GBP
Destination:
19tvVbAEkpwzjAehCA7
sHPgmGJJWQZHbxi

Keep this receipt!

Location: Nincomsoup,
satoshipoint.com, 020
3026 6037



Seizure challenges

- Two factor authentication
- Address whitelisting
- Asset time locks (both technical and via financial applications)
- Passphrases
- Technical details (Hardware wallets, Shamir Secret sharing, multi signature, fees, privacy coins)
- Nuances of coins e.g. need base asset to send second layer or tokens
- Derivation paths and nuances of applications
- Second layer assets
- Seizure equipment available including that necessary for audit trail
- Trained staff (Financial investigators in particular, who lawfully can make the seizure?)
- Time pressures
- Hostile environment

Internal security

- What devices are being used to secure the asset?
- Where are they being stored?
- Is a third party provider being utilised instead/or for long term storage?
- What are the terms of the contract in respect of a third party?
- How can the asset be accessed?
- Who is responsible for handling the asset?
- How is the recovery seed being handled?
- Is there any insurance policy in place to cover loss of the asset?
- How is this process going to be audited?
- Who is handling the long-term legal process for maintaining possession of the asset? Is there a need to give evidence in respect of this?

Realisation

- At what point is the criminal benefit figure determined?
- What liability is in place in respect of the value of items seized by law enforcement?
- Can cryptocurrency be accepted as payment for proceeds of crime orders?
- What process would be in place for converting into fiat currency? (Auction, sale to an exchange, alternative?) Is there any need to do this covertly? (could move the market if significant figures involved) Does due diligence need to be done on the buyer?
- What legal process is in place to allow the conversion of cryptocurrency into fiat currency?
- What costs are involved in long term storage of cryptocurrency in its raw form?
- What costs are involved in converting into fiat currency?
- How will this process be audited?

BIP39 Tool

This tool is relevant to cryptocurrencies which comply with the BIP39 standard. The objective is to convert a mnemonic phrase/recovery seed into a master private key. This is then used by the tool to generate public addresses. The information on which wallet software/hardware may have been used to generate the address is also outlined. This is not a definitive list and is not confirming which application has been used.

It is also important to note that the tool is not reporting that any addresses generated have been used. Further analysis is required to identify if the addresses have been used to transact. This analysis can be completed by entering the generated addresses into relevant block explorers.

The tool has four main options which can be used to extend its functionality:

BIP Tool features

- The first is a “Passphrase (optional)” field. If the mnemonic phrase/recovery seed has a 25th word added to it, this can be entered into the “Passphrase (optional)” field. This is not related to the BIP38 encryption scheme (passphrase for encrypting private keys).
- “Index severity” refers to the number of public addresses the tool can generate. Every BIP32 compliant wallet (HD wallet) can use the master private key to deterministically generate an almost infinite number of public addresses. Wallets will often use this feature to generate a new address for every receipt of cryptocurrency. As such multiple public addresses within a wallet may have a cryptocurrency balance associated to them.
- The best starting point in relation to this option is to consider that only technical users will alternate the automatic process of generating addresses. The vast majority of users will have utilised the first address generated by the wallet (if they have in fact transacted with cryptocurrency). Analysis of the first address populated by the tool will therefore often be sufficient to highlight if a wallet has been active. If this proves to be the case, then the wallet would be rebuilt and the full balance of all addresses identified in this manner.

BIP Tool features

- “Account Severity” refers to different accounts which may be present in a wallet. BIP32 wallets can be envisaged as a tree structure. The master private key is the root and branch with all subsequent addresses branching off from this. Accounts can also be considered a branch of this tree. Users can define a that a particular branch is used for a particular purpose and derive addresses using this account location in the “tree” if they wish. This will likely require manual intervention within a wallets settings menu and as such will not always show up when a wallet is automatically recovered using software.
- The option here is for the tool to start exploring account branches of the “tree” and deriving addresses linked. Again, it is not providing addresses that have definitely been utilised. Given the same considerations as with “Index severity” (only technical users will do this), the starting point should be the same. If funds are identified on the first account, then once rebuilt further exploration may be carried out.
- “Check addresses online” option will provide input on whether any activity has been seen according to the blockchain API’s utilised by the tool. This is not advisable; any compromise of the device or network being utilised could lead to a malicious party obtaining the mnemonic/recovery seed.

BIP Tool procedure

BIP39 Mnemonic phrase tool

Settings

Enter the mnemonic phrase

Mnemonic Phrase

Passphrase (optional)

Index severity

1

Account severity

1

Check addresses online

Check

Results

Coin	Type	Derivation path	Address	Used by	Is used?	Full Wallet
------	------	-----------------	---------	---------	----------	-------------

Based on Ian Coleman's BIP39 libraries

Run a virus scan on the device to be used (can be done in advance). Disconnect the internet connection on the device being used. This is a security measure to help prevent any compromise issues. Do not save the mnemonic phrase/recovery seed on the device or transmit it via any medium in its entirety.

Ensure that your screen cannot be monitored and only the necessary individuals have access to the mnemonic phrase/recovery seed. Load up your default browser and clear all history/cookie data.

Double click on the index.html file, this will open the tool in a browser window.

BIP Tool procedure cont.

- Click on “Check!”. This will start the process of the seed being converted into a master private key. Once this is done the “Results” section will begin to automatically populate addresses that can be derived from the seed.

Check!

Results

Coin	Type	Derivation path	Address	Used by	Is used?	Full Wallet
BTC	BIP32	m/44'/0'/0'/0	1B3CGuY3XZFBcDVMPsjAPL8VLmtmCj114y	Blockchain.info (legacy), Bitcoin.com (app), MultiBit HD, BRD, Coinomi (old legacy), Ledger (legacy)		
BTC	BIP44	m/44'/0'/0'/0/0	1QBXa35un5PSCExdsoTLFuAEZ9E8hPtcZd	Exodus, Bitpay (app), Mycelium, Copay, Jaxx, Coinomi (current legacy), Enjin, KeepKey, Blockchain.info		
BTCTEST	BIP44	m/44'/1'/0'/0/0	my5K6JYBX6c3kuaSTTFBuSWZUKUX3h1kBw	KeepKey		
BTC	BIP49	m/49'/0'/0'/0/0	36R3KsRpfuRjn4UYbChX8TN15oZW4ub3Hd	Trezor, Ledger, edge, Coinomi (Compatibility)		
BTCTEST	BIP49	m/49'/1'/0'/0/0	2N1N7FWJzKHAK1XJCjrp7KmqgBvDmPGV3C	Trezor, Ledger		
BTC	BIP84	m/84'/0'/0'/0/0	bc1q77ace4xe3dvla08t333uz2e834hft7lvcwkyda	Coinomi, Wasabi Wallet (password mandatory)		
ETH	BIP44	m/44'/60'/0'/0/0	0x160d0aa58f04EaE2Ad40DB581E554b719A281C9E	Ledger		
ETH	BIP44	m/44'/60'/0'/0/0	0xead0BA3d8a933d3CB3C70035D9A595A05Bfb8B81	Jaxx, Metamask, Exodus, imToken, Trezor, KeepKey		
LTC	BIP44	m/44'/2'/0'/0/0	LbE86chRvNsWYwK79d6o5vneyuPLst9Yah	Coinomi (legacy), KeepKey, Ledger		
LTC	BIP49	m/49'/2'/0'/0/0	MTY9MSAJW2Rsp5RguUvubM1gYQnXyzWF1	Coinomi (compatibility), Trezor		
LTC	BIP84	m/84'/2'/0'/0/0	ltc1qxwtmmhrs2lu823j9ngx4hhe6cza6gkprftq4j	Coinomi (default)		
DASH	BIP44	m/44'/5'/0'/0/0	Xf1a3iKoCoYdWzui44bTHPayS2hDZThQmk	Trezor, Ledger, KeepKey		
DOGE	BIP44	m/44'/3'/0'/0/0	D7VNkmrCKZc8sWfHABJ2pRnnwEGkpMk2GE	Trezor, Ledger, KeepKey		

BIP Tool procedure cont.

- Highlight the results and copy them. Paste the results into a word/txt document. Return to index.html and delete the words in the “Mnemonic Phrase” field. Clear all history/cookies data and close the tab. The results in the word/txt document can then be used to check for a balance and identify if the mnemonic phrase/recovery seed needs to be re-built.
- Once the above is completed re-connect device to the internet and utilise a block explorer to identify if any funds are associated with the addresses recovered.

Blockpath	Bloxy.info
Bitquery	Bitcoin.com
Walletexplorer.com	Blockchair.com
Blockchain.com	Ethplorer.io
Blockstream.info	Bitinfocharts.com
Oxt.me	Blockcypher.com

Demonstration

- The following demo provides an outline of the BIP39 Tool and a seizure of cryptocurrency using a recovery seed/mnemonic.

Conclusion

- There is a lot to consider in relation to the seizure, detention and realisation of cryptocurrency. It needs to be a collaborative effort involving the relevant personal to complete the task lawfully and appropriately.
- Unfortunately, this training only covers the basics. The rate of growth within the cryptocurrency space is breath-taking. The nuances of seizure processes will inevitably grow, and the relevant policies will need reviewing regularly require a constant monitoring.
- Establishing work groups or online forums to share knowledge between investigators is a great way of keeping track of what is happening. The OECD is a unique forum for this but there are others such as Interpol and Europol.
- Practice sessions and engagement with colleagues is also a good foundation for dealing with such matters. You can utilise testnet coins which cost nothing or purchase small amounts of cheap cryptocurrencies (e.g. Dogecoin or Digibyte are low-cost networks.)