OECD International Academy for Tax Crime Investigation

Anti-Money Laundering: Current Trends, Prosecutions, and the Challenges around Cryptocurrencies

OECD

BIP-39 Mnemonic Phrase Tool

Determining which wallet software to use

BIP-39 Mnemonic Phrase Tool

Law Enforcement tool.

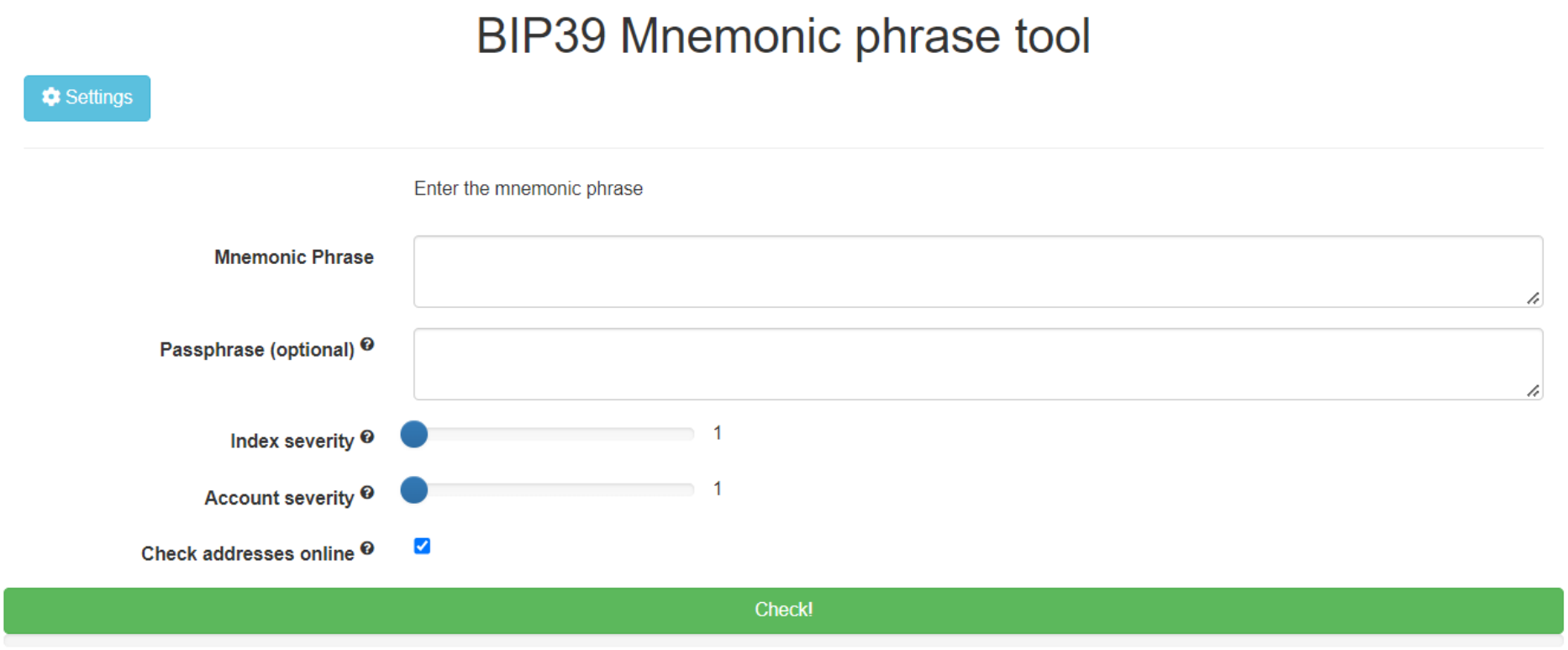
1. Creates a Seedbased on the mnemonic word list provided.
2. Derives keys and addresses along different derivation paths.
3. Verifies on the blockchain to see if derived addresses have been used.
4. Based on the results, the tool provides a list of possible wallets with the appropriate derivations paths.

BIP-39 Mnemonic Phrase Tool

- Online web page may be used (less secure)
- Tool may be downloaded (more secure)
- May be used with seed word lists which are written in different languages
- Advanced options are available in the downloadable tool.
- Only suggests wallets – they may not be the actual wallet which the suspect used.
- Some wallets may use the correct BTC derivation path, but not the correct ETH one.

https://cryptotools.nl/4ce35eb2e285eceaf0ef20f1b68aa4f8/tool/

Online Version

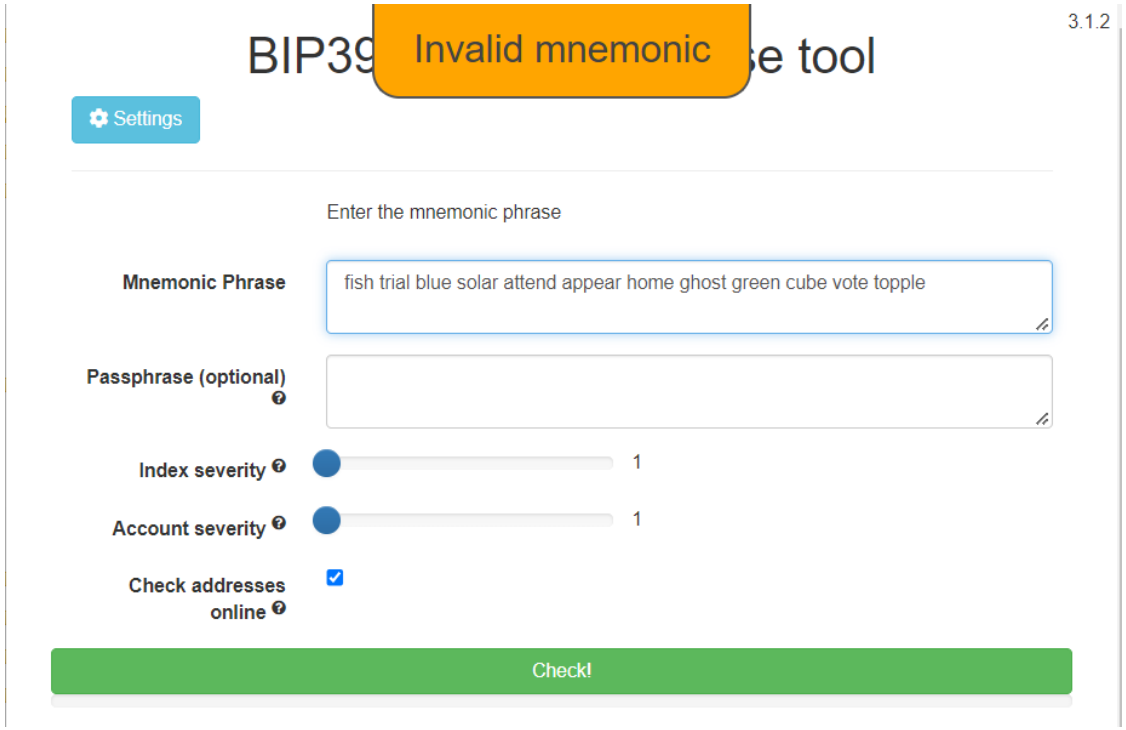


https://cryptotools.nl/4ce35eb2e285eceaf0ef20f1b68aa4f8/tool/

Use

- Enter the Mnemonic Phrase – i.e. the seed word list for the suspect's wallet.
- You don't need to worry about Passphrases, Index severity, or Account severity.
- Make sure **Check addresses online** is ticked if you want the tool to verify online whether the wallets it is suggesting contain cryptocurrency.
  - The tool will reach out to blockchain explorers and attempt to discover assets held by the addresses that it generates.
- Click the Green CHECK button.

You will receive an error message if you enter an invalid seed word list



Invalid mnemonic!

Possible reasons for this are:

- It is an Electrum mnemonic phrase, this is not a BIP39 mnemonic, works differently and is not supported right now
- The words are incorrect, for this look at Github for the wordlists
- The order of words are incorrect
- The words belong to another type of mnenomic phrase, for instance Monero (Monero requires the rescan of the blockchain and uses a different list of words)

Look for the green tick marks

Results

Coin	Type	Derivation path	Address	Used by	Is used?	Full Wallet
BTC	BIP32	m/44'/0'/0'/0	1CbZ1Kpu7NcjMsaVuT95snvr8YaPbetiDJ	Blockchain.info (legacy), Bitcoin.com (app), MultiBit HD, BRD, Coinomi (old legacy), Ledger (legacy)	✗	
BTC	BIP44	m/44'/0'/0'/0/0	1DV3jDfd6qfTtnvZ7HjbDFcmavTEsNjeDP	Exodus, Bitpay (app), Mycelium, Copay, Jaxx, Coinomi (current legacy), Enjin, KeepKey, Blockchain.info	✓	
BTCTEST	BIP44	m/44'/1'/0'/0/0	miY4xTAJ8u75MmB3qeQzCEDX7b5AYGRsgb	KeepKey	⛓	
BTC	BIP49	m/49'/0'/0'/0/0	392CPSHfqWhLM82q9DJGfdPW2Krx57khK7	Trezor, Ledger, edge, Coinomi (Compatibility)	✓	
BTCTEST	BIP49	m/49'/1'/0'/0/0	2N7F1irDpZ28iXVBmAFRh4L5tuTFF663MQr	Trezor, Ledger	⛓	
BTC	BIP84	m/84'/0'/0'/0/0	bc1qa6pya3pxqja795uh73xa8qlvuj0g5hfsy7czkz	Coinomi, Wasabi Wallet (password mandatory)	⛓	
ETH	BIP44	m/44'/60'/0'/0/0'	0x436B93CeC3872750dCd527379045d3D31baaaC3e	Ledger	✗	
ETH	BIP44	m/44'/60'/0'/0/0	0xCFeb408c1dD76587Dd241136582432EB52e521C1	Jaxx, Metamask, Exodus, imToken, Trezor, KeepKey	✓	
LTC	BIP44	m/44'/2'/0'/0/0	LfEzFu6yNjLDDKVEe2DRiJkr314xXcfnzB	Coinomi (legacy), KeepKey, Ledger	⛓	
LTC	BIP49	m/49'/2'/0'/0/0	MSsaRVmwzUvD8YdJsHWG3CCugxgfQ6TVX3	Coinomi (compatiblity), Trezor	⛓	
LTC	BIP84	m/84'/2'/0'/0/0	ltc1qvpexu95gs3f4prk5j0trl8gnq99yvp66rvva58	Coinomi (default)	⛓	
DASH	BIP44	m/44'/5'/0'/0/0	XbBE3SkMarCoCrtzndNNSUzgnULw4axwaf	Trezor, Ledger, KeepKey	✗	
DOGE	BIP44	m/44'/3'/0'/0/0	DLa3AZJw1TjeAJk9haPvA1QSVfDguwcsvc	Trezor, Ledger, KeepKey	⛓	

Results

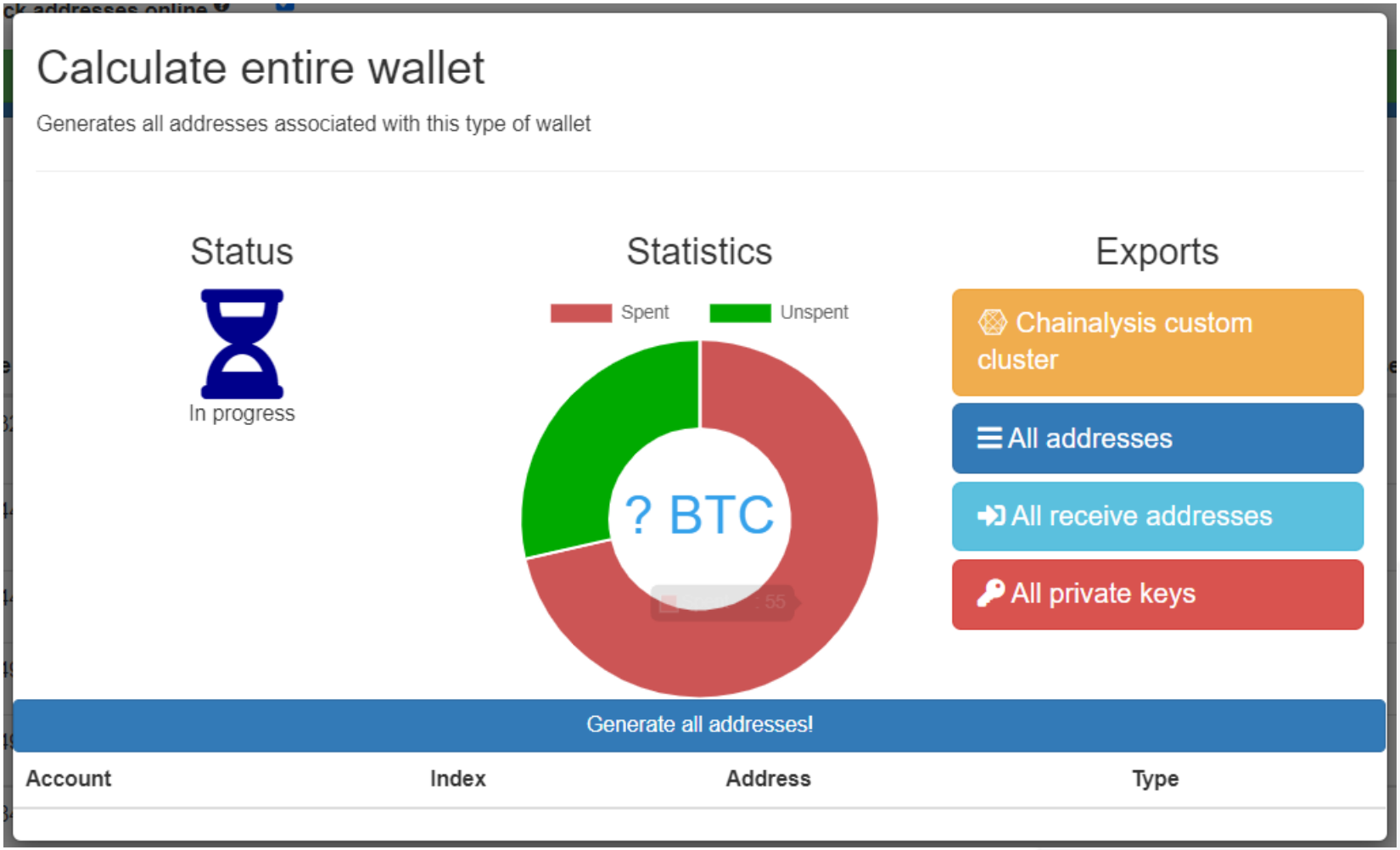
- **Coin** identifies which coins have been discovered.
- **Type** identifies the address type (P2PKH, SegWit, etc.).
- **Derivation path** identifies the path which was used to derive subkeys.
- **Address** identifies the first address which was generated when the wallet was created.
- **Used by** indicates possible wallets which can be used to recreate the suspect's wallet.

Results (cont.)

- **Is used** indicates whether the wallet type was used and contains coins.
  - A **green circle** with a tick mark indicates that it was used. 
- **Full wallet** indicates there are details available on how many coins are in the wallet.
- Identify a green tick and click on the wallet icon beside it to obtain and export details.
  - You will the need to click on the blue Generate all addresses button to see the available info.

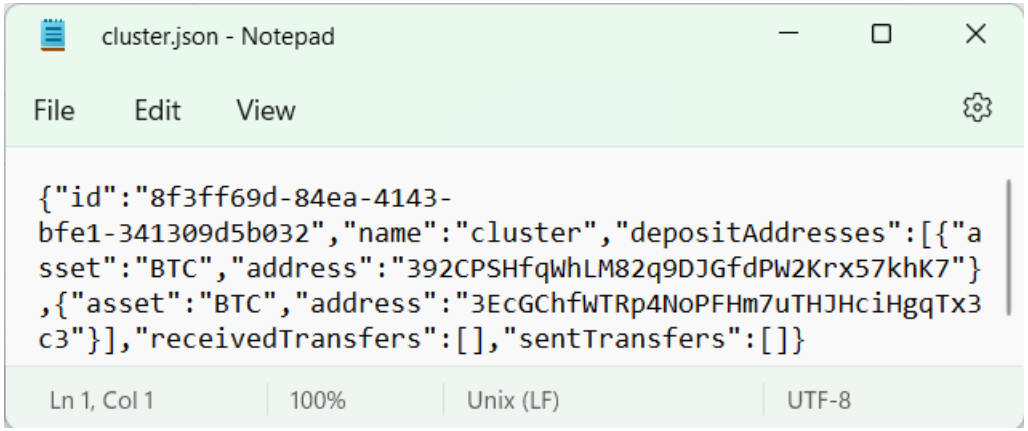
Attempt to recreate the suspect's wallet using the suggested software

- If more than one coin is discovered, you may want to select a wallet that appears for both coins.

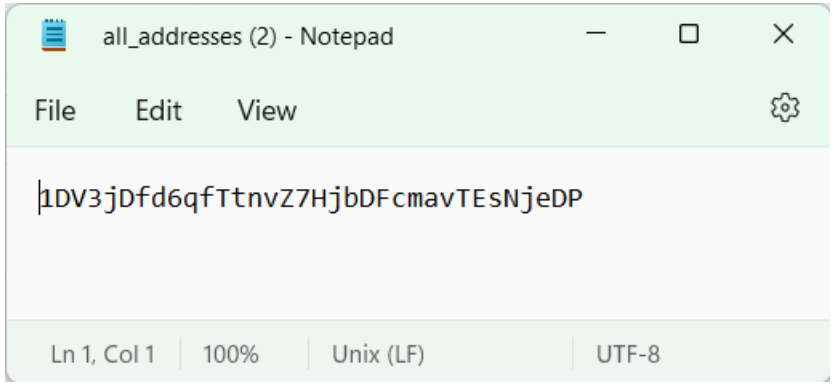

Calculate entire wallet
Generates all addresses associated with this type of wallet
Status
In progress
Statistics
Spent
Unspent
? BTC
Exports
Chainalysis custom cluster
All addresses
All receive addresses
All private keys
Generate all addresses!
Account
Index
Address
Type

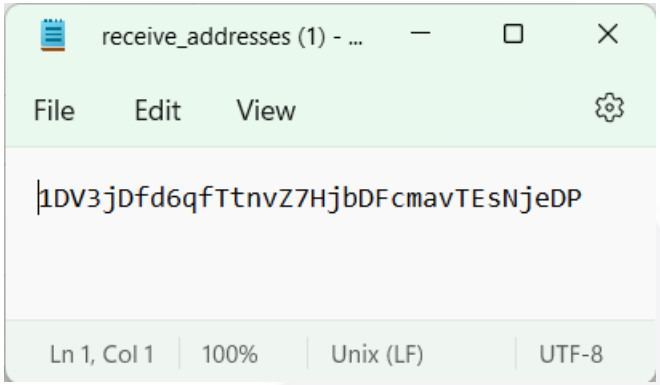
Exportable data

- **Chainalysis custom cluster**: a JSON file with the discovered cluster. This can be directly imported into Chainalysis Reactor for tracing and analysis.
- **All addresses**: a txt file containing all the addresses which were discovered by the tool.
- **All receive addresses**: a txt file containing all the receiving addresses discovered by the tool.
- **All private keys**: a txt file containing the private keys for the addresses discovered by the tool.

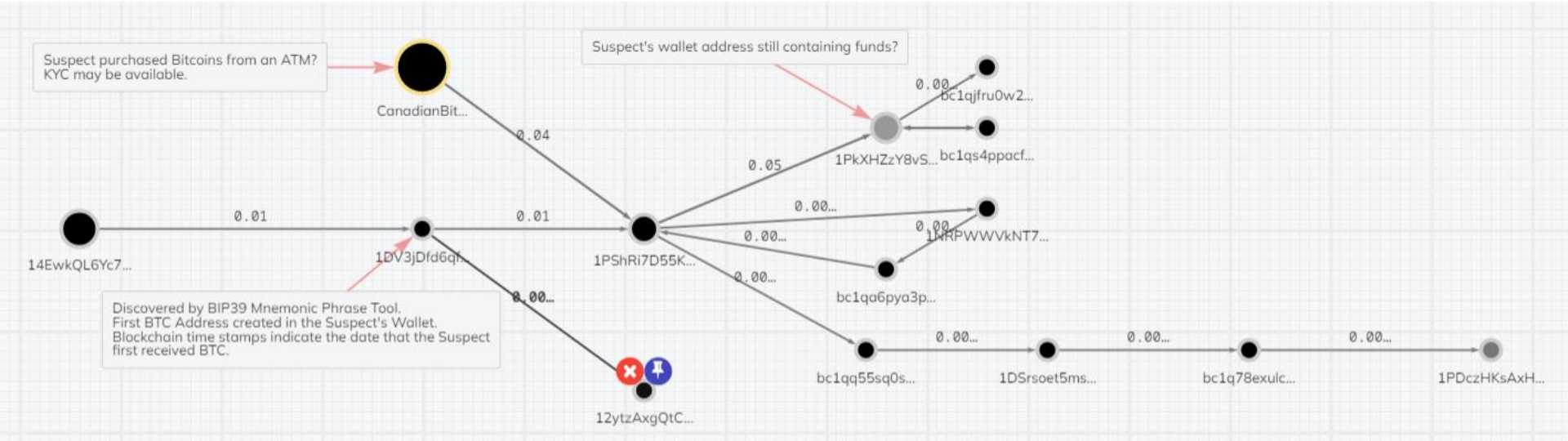

cluster.json - Notepad
File Edit View
{"id":"8f3ff69d-84ea-4143-bfe1-341309d5b032","name":"cluster","depositAddresses":[{"asset":"BTC","address":"392CPSHfqWhLM82q9DJGfdPW2Krx57khK7"},{"asset":"BTC","address":"3EcGChfWTRp4NoPFHm7uTHJHciHgqTx3c3"}],"receivedTransfers":[],"sentTransfers":[]}
Ln 1, Col 1 100% Unix (LF) UTF-8

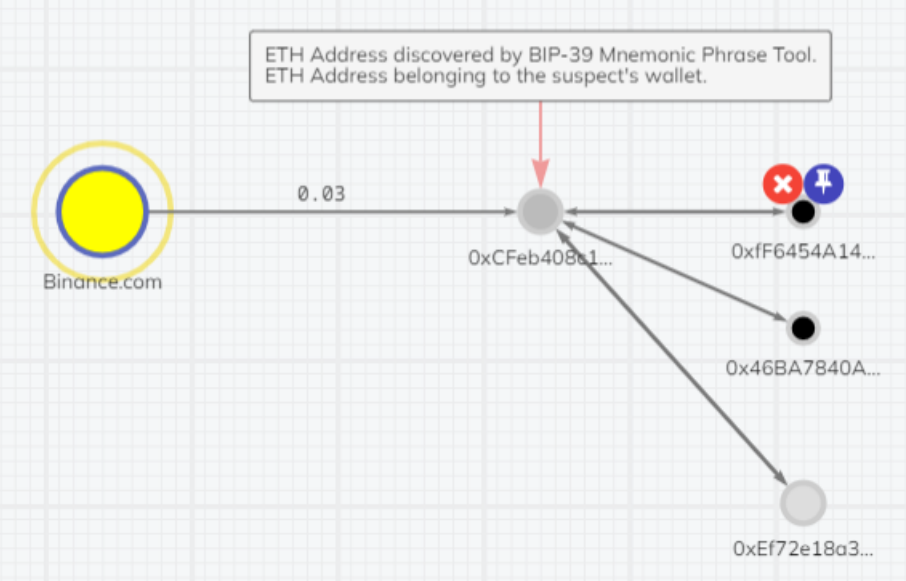

private_keys (2) - Notepad
File Edit View
undefined:L1STSa1UeQNu6BWvAqgU7bgo7yHssxQBpR9LeLfX4HC3LMSUEj72
undefined:L4wgySttuP5riMz8mn4o7qdnETotGqimTsJJ1CULLW58wcAyriCz
undefined:L1STSa1UeQNu6BWvAqgU7bgo7yHssxQBpR9LeLfX4HC3LMSUEj72
Ln 1, Col 1 100% Unix (LF) UTF-8


all_addresses (2) - Notepad
File Edit View
1DV3jDfd6qfTtnvZ7HjbDFcmavTEsNjeDP
Ln 1, Col 1 100% Unix (LF) UTF-8


receive_addresses (1) - ...
File Edit View
1DV3jDfd6qfTtnvZ7HjbDFcmavTEsNjeDP
Ln 1, Col 1 100% Unix (LF) UTF-8

Chainalysis custom cluster JSON file





Caution!

- **Don't trust the tool** when it comes to the exportable files containing addresses and keys (it doesn't always generate them).
- **Recreate the suspect's wallet by trying out different suggested wallets.** Once you have done this you can seize any coins available and/or export any log files generated by the wallet.
- **The suggested wallet may not be the one that the suspect used**.

BIP39 Mnemonic Phrase Tool Exercise

- You locate the following seed word list during a search.
- Identify wallets which you could use in order to gain access to the suspect's funds.

1. regret
2. earn
3. clerk
4. ginger
5. future
6. cook
7. million
8. sudden
9. bag
10. bird
11. prefer
12. spot

Results

Coin	Type	Derivation path	Address	Used by	Is used?	Full Wallet
BTC	BIP32	m/44'/0'/0'/0	1MeemYzXLzRjdFvYZxoKEtGDkGoimSnB2A	Blockchain.info (legacy), Bitcoin.com (app), MultiBit HD, BRD, Coinomi (old legacy), Ledger (legacy)	✗	
BTC	BIP44	m/44'/0'/0'/0/0	1PkXHZzY8vS8xUYZ8rEKwEGpqYX7vpFzZP	Exodus, Bitpay (app), Mycelium, Copay, Jaxx, Coinomi (current legacy), Enjin, KeepKey, Blockchain.info	✓	
BTCTEST	BIP44	m/44'/1'/0'/0/0	mv2e7tGapD4d1aDdQG4Jo2shVwNMzBR6Pj	KeepKey		
BTC	BIP49	m/49'/0'/0'/0/0	3PPiAFhNaU7XubbGDLNSA2uzfctwf2tnBi	Trezor, Ledger, edge, Coinomi (Compatibility)	✗	
BTCTEST	BIP49	m/49'/1'/0'/0/0	2NFvthrEimwrT8z3qzNaPNQyGGf3wWKWSMb	Trezor, Ledger		
BTC	BIP84	m/84'/0'/0'/0/0	bc1qmtp36dqeekz3gcjeu3sjldty5sdd3gy3ewlkdw	Coinomi, Wasabi Wallet (password mandatory)		
ETH	BIP44	m/44'/60'/0'/0/0'	0x4BD27acA1759c7c4f228b2bC948d91Eb7aE81AFE	Ledger	✗	
ETH	BIP44	m/44'/60'/0'/0/0	0x5DD2602A2DE363D6Edd258116468Ac08415b9B22	Jaxx, Metamask, Exodus, imToken, Trezor, KeepKey	✗	
LTC	BIP44	m/44'/2'/0'/0/0	LKrACYcCFoJZNvNEkArqM3nJWr8bUGo2rB	Coinomi (legacy), KeepKey, Ledger		
LTC	BIP49	m/49'/2'/0'/0/0	MC666mSAJa8K4eUvGPpt3sEDE9zqF9WgDF	Coinomi (compatiblity), Trezor		
LTC	BIP84	m/84'/2'/0'/0/0	ltc1qxejrhmt2l692g4d4eu9lenvczmw8tvm57q8p55	Coinomi (default)		
DASH	BIP44	m/44'/5'/0'/0/0	Xeofw4bfoxLsbhj4nP9EhXNnKH6YQVkgmt	Trezor, Ledger, KeepKey	✗	