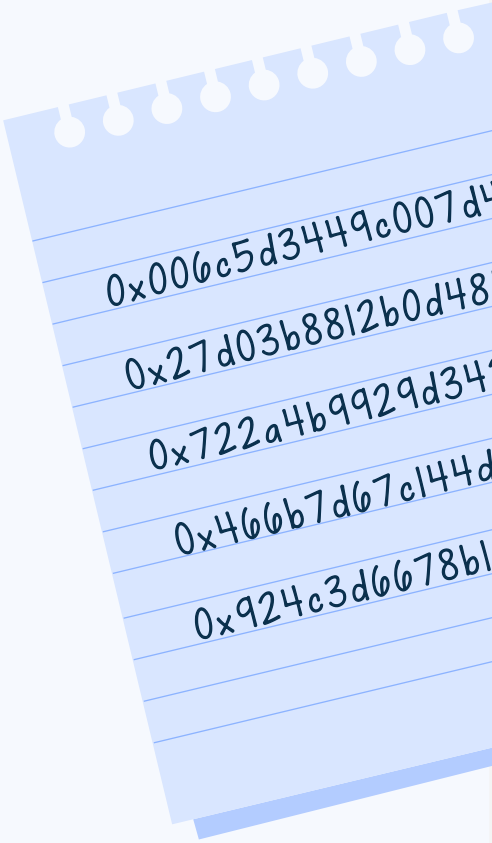
TRM

Collecting and investigating cryptocurrency data in real-time

A guide for law enforcement



trmlabs.com

Key considerations for law enforcement handling blockchain & cryptocurrency data

A checklist for investigators who are collecting, investigating and triaging blockchain and cryptocurrency data in real-time.

When investigating fraud, money laundering, or financial crime of any kind, speed is of the essence. Despite this, financial crime investigators often lose critical time waiting for access to tools or for third-parties to analyze and verify blockchain evidence that may be uncovered in the field during searches, seizures, and interviews.

The process of collecting evidence for subsequent forensic analysis can often result in weeks of delay, resulting in missed opportunities to seize or freeze funds which can be moved instantly by bad actors.

Moreover, at present, front line officers come across crypto wallets both in arrests and on-scene searches, but have no way to rapidly determine the value of the wallet or the investigative value/leads it could contain.

Additionally, sometimes investigators may not be expecting to find cryptocurrency at all and have to make decisions about whether to seize, examine, or follow up on cryptocurrency leads without a full picture of what they have found.

With the use of cryptocurrency by illicit actors rising across all violations, it is more important than ever for law enforcement officials to be able to identify, report, and disrupt illicit virtual currency transactions and the criminals conducting the transactions.

This checklist provides basic explanations, techniques, strategies, and resources for investigating blockchain data. Keep this checklist near duty phones, in digital forensics labs, or any other place where triaging evidence related to cryptocurrency might take place.

Key definitions

What is a transaction hash?

Also known as a "Transaction ID", this is a unique, alphanumeric sequence associated with a transaction on a blockchain. An investigator can identify specific transactions based on the transaction hash. A typical transaction hash may look like:

F21df8bb6aec0d8a13a7173999d98ac480f81f6734c86e5f2b229bf45ee4e8ba

or

0xd6310669180ad821d684c8a4a19ce3cf07a2dbdfa639f46f02a3c23391552430

What is a wallet address?

A wallet address is a string of letters and numbers from which cryptocurrencies or other tokens such as NFTs can be sent to and from.

A wallet address is also known as a Public Key and can be shared with different contacts like an email address. It can contain just one or multiple addresses. A typical wallet address may look like:

bc1qck9xla7ar3hy05rxm6wdt826aqlhhr95q7s4gm [Bitcoin]

or

0x9711f16d0a73ed72b16376cec15606e5b919c6fd [ETH or ERC-20 Token]

What is a software wallet?

A device or service that stores users' public and private keys, allowing them to interact with various blockchains and to send and receive crypto assets. These can be desktop, mobile, or online wallets. When wallets are held by individuals rather than at an exchange, investigators regularly refer to them as "un-hosted" wallets. Where an "un-hosted" software wallet is in a subject's possession, the only way to seize the value from that wallet is with the wallet's private keys. Software wallets can contain many addresses and many currencies, so one suspect's wallet may have multiple bitcoin addresses, multiple Ether addresses, and multiple ERC-20 token addresses.

A typical software wallet looks like many applications on a phone, computer, or other connected device:

What is a hardware crypto wallet?

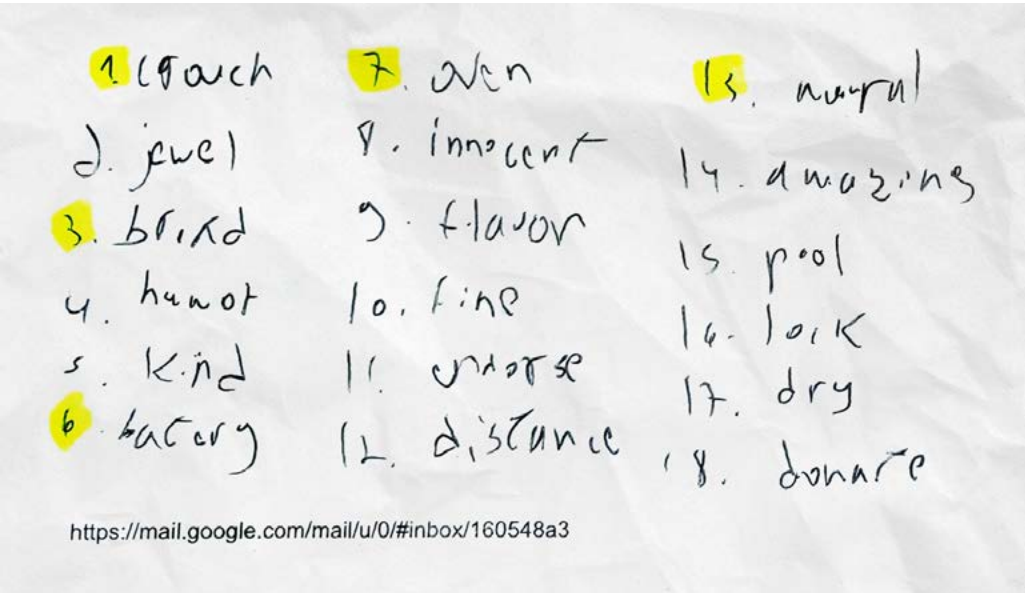
Hardware crypto wallets are small devices that store cryptocurrency offline. They are used to provide full isolation between the private keys, which are codes that only the user has access to in order to access the crypto assets in question, and the user's computer. Hardware wallets have an associated web, mobile and/or desktop application that enables you to monitor your cryptocurrency address and spend your cryptocurrency. Hardware wallets have several different physical forms, many of which look like thumb drive but commonly have crypto-centric labels on them:

What is a recovery seed or phrase?

A seed phrase is a sequence of random words that stores the data required to access or recover cryptocurrency on blockchains or crypto wallets.

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. Anyone who maintains a copy of the recovery phrase can re-create the wallet and could easily withdraw the funds– as such, recovering wallets and seizing cryptocurrency in an expeditious manner is highly recommended and should be treated with a sense of urgency.

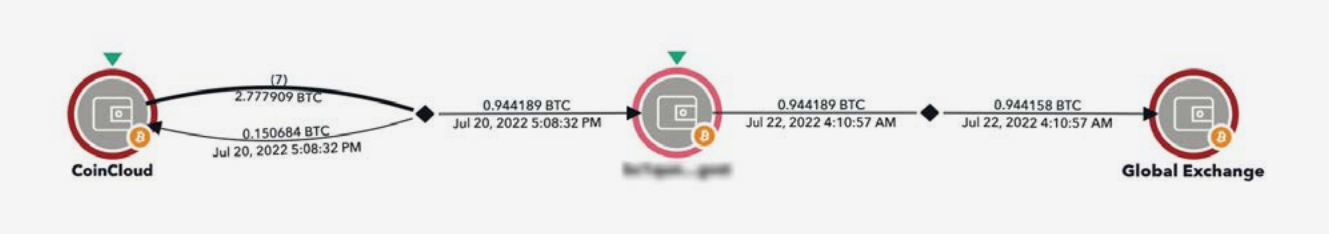
Recovery seeds also render mere physical seizure of software or hardware wallet as inadequate, because with recovery seeds, a suspect can reconstitute an address and move the funds out without physical possession. Conversely, when an investigator finds recovery seeds and has legal authority to seize contents of associated cryptocurrency addresses, the investigator can do so even when they do not have access to the private address. Recovery seeds may be held in text files, engraved in metal, or written down by hand on scratch paper:



Why is blockchain tracing important?

Blockchain tracing refers to tracking the source and destination of cryptocurrency transactions recorded on the currency's blockchain (generally, a publicly available ledger of completed transactions between two or more cryptocurrency addresses.)

The investigative goal of "blockchain tracing," generally, is to identify the actual controller of an otherwise pseudo-anonymous address. To do so, an investigator may be able to trace blockchain transactions and find counterparty exposure with an entity or individual that can provide the identity of the beneficial controller of an address.



More simply, an investigator should follow the money to or from an entity that can provide real-world identity.

Investigators run the risk of leaving leads and "money on the table" if they fail to expeditiously trace transactions on-chain when dealing with cryptocurrency investigations. On-chain transactions can show an investigator where the subject has interacted, related networks of transactions, and where assets are held with potential for seizure.

Identified wallets could contain critical leads based on the source and destination of funds, including:

- Actor attribution
- A more complete picture of the actor's assets
- Sources of funds
- Financial transactions on-chain and off-chain
- Other potential links to illicit activity

Tools at your disposal

TRM Tactical

TRM Tactical is a mobile-first blockchain forensics tool that empowers frontline investigators to uncover cryptocurrency evidence rapidly and easily – even without in-depth blockchain or crypto expertise.

It was specifically designed to rapidly empower investigators who may not have extensive blockchain/crypto experience to quickly analyze and determine if a wallet address found in the field has links to or has been used for illicit activity.

What should an investigator look for in their cases?

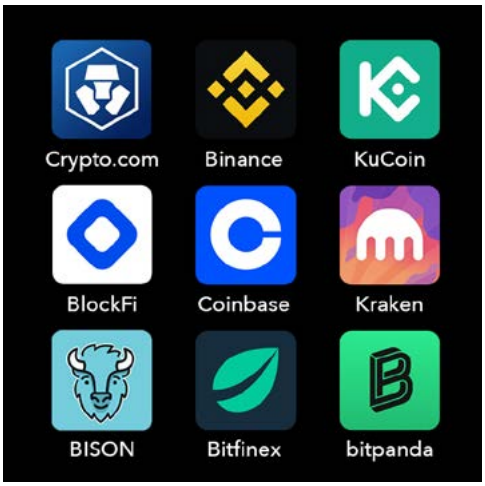
When investigating financial crime or any crime that includes the potential use of cryptocurrency, speed is of the essence, and critical to this is knowing what to look out for in order to surface critical cryptocurrency evidence to follow the money in a case.

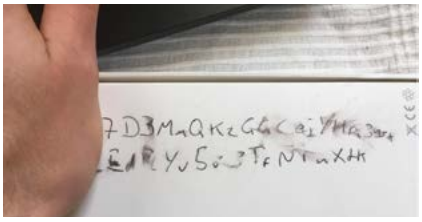
Let's hone in on what to keep an eye out for when collecting and triaging evidence:

Anything with a crypto related logo on it

Cryptocurrency applications can be found on mobile devices and computers. These apps are for accessing crypto exchanges and wallets. Some authenticator (2FA) and password vault apps can also store crypto addresses.

- Cryptocurrency apps: Bitcoin, Ethereum, Litecoin, Monero, etc
- Software Wallet apps: Examples of software include: Electrum, Exodus, Coinomi, Mycelium, etc.
- Exchange Wallet apps: Binance, Coinbase, Kraken, etc.





Scraps of paper or notes in a suspect's mobile phone or computer containing:

- Seed phrases
- Long strings of letters and numbers
- Wallet addresses
- QR codes
- Receipts mentioning crypto

Hardware wallets

These come in various shapes and sizes, with some looking like USB drives or smartphones. Hardware wallet names include Trezor One, Trezor Model T, Ledger Nano S, Ledger Nano X, and Keepkey.

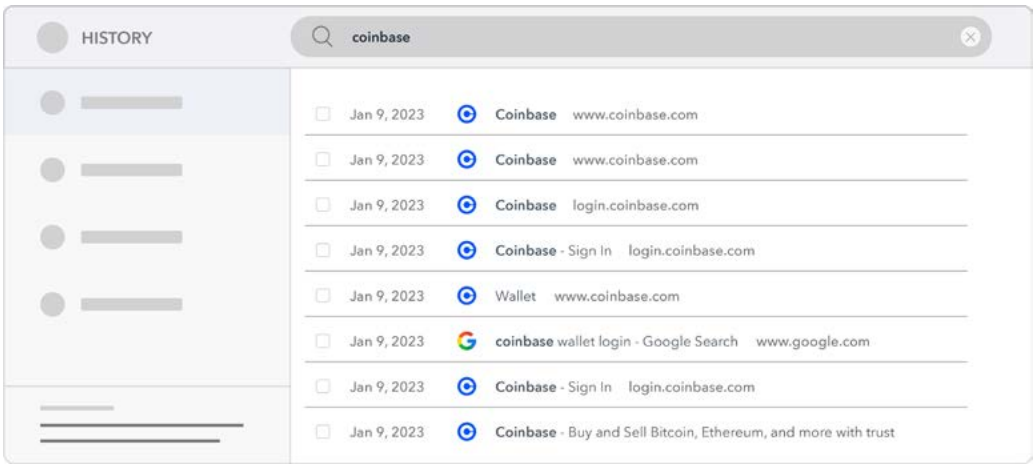
Mobile devices or computers

These can be searched to identify certain indicators of:

- Browsers such as Tor, Red Onion Tor, etc.
- Dark Net Market Links such as http://…… onion

Web browser history on mobiles and desktop computers

A browser's internet history can be searched to check if a suspect has accessed web-based crypto wallets, exchange websites, mining pools, mixers, etc.



Frontline use case example

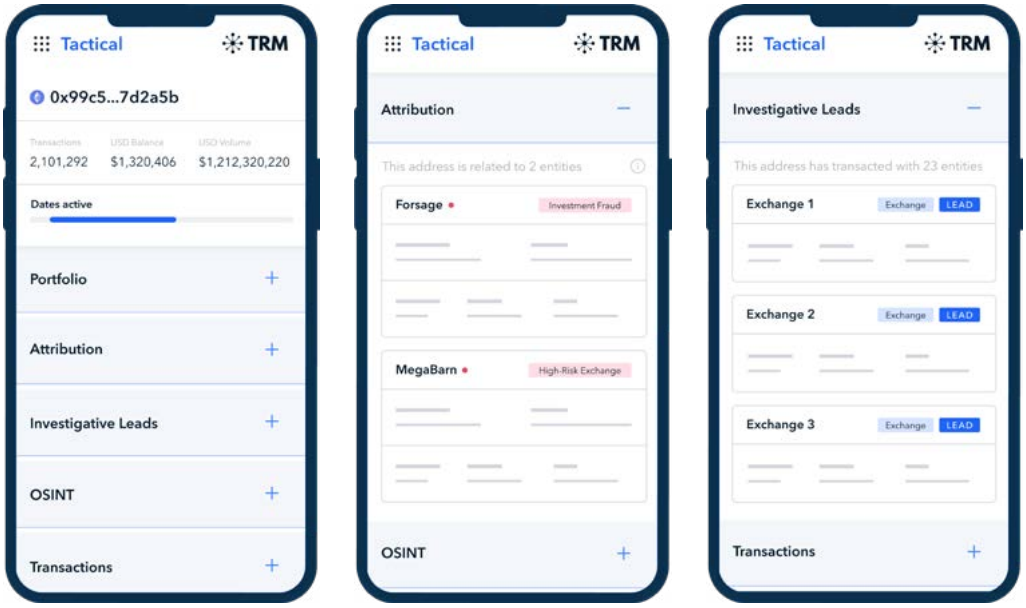
In this event, crypto data was found during a search of a suspect's vehicle.

A law enforcement officer detains a suspect based on probable cause, and during a vehicle search finds documents in plain view that have strings of numbers and characters written on them.

The officer can enter the address into TRM Tactical, which searches for the address in TRM's multi-blockchain dataset.

```
0x99c53f446ea5244b8rt3c6fef43b7b2f7d2a5b
```

Within seconds, TRM Tactical finds the address and displays the total volume of funds, entities it has transacted with as well as investigative leads.



Office-level triage use case example

A member of the police was reviewing a Suspicious Activity Report (SAR) from an exchange. The SAR stated that a customer had deposited funds into a known child abuse marketplace.

In this scenario, the staff member needs to corroborate this information in order to obtain a search warrant.

This staff member can use the detail from the SAR and ingest it into TRM Tactical, which in this situation showed the result of RISK (child abuse) and showed the transaction in question.

With the sensitive intel now having been corroborated, the officer can then go to a judge or magistrate and obtain a search warrant without needing to conduct a full forensic investigation at this stage.