



CATlabs
Crypto Asset Technology

Recovery CAT Guide to Finding and Seizing Crypto

Recovery CAT is a digital asset discovery and seizure platform that looks for traces of cryptocurrency use within digital data collected during investigations. Recovery CAT finds and identifies immediately seizable assets and provides actionable intelligence on leads for further investigation.

With the current prevalence of cryptocurrency use by malicious actors, digital data collected during investigations often contains seed phrases and private keys that can lead to an immediate asset seizure. Additionally, digital data can also contain leads for further investigation that could result in a seizure down the line with additional legal process or blockchain analytics.

Below are common data types collected by criminal investigators which often contain crypto traces or immediately seizable assets.





CATlabs

Crypto Asset Technology

On-Prem First Recovery CAT

In **Q3 2025**, an enhanced version of on-premise Recovery CAT was released. This updated version of the product is built on a performant and scalable foundation.

Instant Results

View real-time results in the interface while the scan is in progress.

Instant Scans

No need to upload datasets, begin scanning immediately.

Intuitive

See more details about current scan progress, cancel scans, streamlined way to organize datasets within cases.



Mobile Devices (iPhone, Android)

1

Mobile devices seized from criminal targets can often contain traces of cryptocurrency use or immediately seizable assets. Common sources of crypto within a mobile device include:



Messaging Apps



Notetaking Apps (Apple Notes , Evernote, etc .)



Documents (presentations, word, text, spreadsheets, pdf)



Crypto Wallet Applications



Email



Image Gallery



Web Search History / Bookmarks / Cookies

Personal Computers / Laptops

2

Personal computers seized from criminal targets can often contain traces of cryptocurrency use or immediately seizable assets. Common sources of crypto within a personal computer include:



Messaging Apps



Notetaking Apps



Documents (presentations, word, text, spreadsheets, pdf)



Crypto Wallet Applications



Web Search History / Bookmarks / Cookies



Image Gallery



Email



Hardware Wallet Attachments

Cloud Accounts

(iCloud, Google Drive, Dropbox, Box)

3

Below are common data types collected by criminal investigators which often contain crypto traces or immediately sizable assets



Messages



Notes



Documents (presentations, word, text, spreadsheets, pdf)



Email



Image Gallery

Bank / Financial Statements / Financial Compliance Reports

4

PDF files and spreadsheets containing financial transaction data (fiat and/or crypto) can be located within financial statements and compliance reports.

Messaging Services

5

Search warrant returns from messaging service providers that don't utilize end to end encryption often contain traces of cryptocurrency use or immediately seizable assets.

Email

6

Search warrant returns of target email accounts often contain traces of cryptocurrency use or immediately seizable assets.

Hardware Storage Devices

7

Hardware storage devices like hard drives or usb drives often contain traces of cryptocurrency use or immediately seizable assets.

Recovery CAT Support Reference Guide

Seized Data	Data Format	Crypto Sources	Crypto Artifacts
iPhone / Android Phone	Cellebrite UFDR Report	Images, Wallet Apps, Browsing History, Documents **Notes **Messages *Email	Seed Phrases, Partial Seed Phrases, Crypto Addresses, Crypto Wallets Apps, Crypto Exchanges, DeFi Services
Windows Laptop	EWF (Recommended) DD RAW	Images, Wallet Apps, Browsing History, Documents **Notes **Messages *Email	Seed Phrases, Partial Seed Phrases, Crypto Addresses, Crypto Wallet Apps, Crypto Exchanges, DeFi Services, Browser Wallets, Hardware Wallets
Mac Laptop	AFF4 (Partial Support - APFS)	Images, Wallet Apps, Browsing History, Documents **Notes **Messages *Email	Seed Phrases, Partial Seed Phrases, Crypto Addresses, Crypto Wallet Apps, Crypto Exchanges, DeFi Services, Browser Wallets, Hardware Wallet Software

**Supported only if service provider's warrant return or forensic extraction tool displays text from notes and messages in supported file types

*Supported only if service provider's search warrant return or forensic extraction tool produces the supported file type

Seized Data	Data Format	Crypto Sources (Where crypto traces can be found)	Crypto Artifacts Seizable Assets & Leads.
Apple iCloud	Zip	Images, Software Apps, Documents **Notes **Messages *Email	Seed Phrases, Partial Seed Phrases, Crypto Addresses, Crypto Wallet Apps, Crypto Exchanges
Google Cloud	Zip	Images, Documents **Notes **Messages *Email	Seed Phrases, Partial Seed Phrases, Crypto Addresses, Crypto Wallet, Crypto Exchanges
Dropbox, Box	Zip	Documents, Images	Seed Phrases, Partial Seed Phrases, Crypto Addresses
Messaging Service	Zip	Images, Documents	Seed Phrases, Partial Seed Phrases, Crypto Addresses
Hardware Storage Device	Zip	Images Documents, Notes	Seed Phrases, Partial Seed Phrases, Crypto Addresses

**Supported only if service provider's warrant return or forensic extraction tool displays text from notes and messages in supported file types

*Supported only if service provider's search warrant return or forensic extraction tool produces the supported file type



Data Types



Data Format



Format

Email	Locally saved (.eml, .emlx) Mozilla (MBOXRD) Outlook (.msg)	Seed Phrases, Partial Seed Phrases, Crypto Addresses, Crypto Exchanges, DeFi Services
Documents	Docs (.doc/x, .rtf, .pdf, .txt, .pages, .odt) Spreadsheets (.xls/x, .csv, .numbers, .ods) Presentations (.ppt/x, .key, .odp) Web pages (.html) Markup (.xml, .fodp)	Seed Phrases Partial Seed Phrases Crypto Addresses
Archives	7-ZIP (.7z)* BZIP2 (.bz2) GZIP (.gz) RAR (.rar, .rev, .r00, .r01, .rar) TAR (.tar) ZIP (.zip, .zipx, .z01, .zx01)	Varies
Images	JPG, PNG, BMP, GIF, TIFF, HEIC, WebP	Seed Phrases, Partial Seed Phrases, Crypto Addresses
Browsers	Brave, Chrome, Edge, Firefox, Opera, Safari	Crypto Exchanges, Browser Wallets, DeFi Services



Crypto Support



Type



Coming Soon

Seed Phrases - Full Support

Seed Detection
Validation

BIP39
Electrum

Address Derivation
Missing Word Brute Force

Seed Phrases - Partial Support

Seed Detection
Validation

Monero

Blockchains - Full Support

Address Detection
Validation

Bitcoin (BTC), Ethereum (ETH), BNB Smart Chain (BSC), Bitcoin Cash (BCH), Litecoin (LTC), Polygon (MATIC), Ripple (XRP), TRON (TRX), Monero (XMR), Zcash (ZEC)

Recovery Seed Derivation
Chain Identification
History and Balance Check