Scientific Working Group on Digital Evidence

Tech Notes on Cryptocurrency

23-F-006-1.1

The version of this document is in draft form and is being provided for comment by all interested parties for a minimum period of 60 days.

Disclaimer Regarding Use of SWGDE Documents

SWGDE documents are developed by a consensus process that involves the best efforts of relevant subject matter experts, organizations, and input from other stakeholders to publish suggested best practices, practical guidance, technical positions, and educational information in the discipline of digital and multimedia forensics and related fields. No warranty or other representation as to SWGDE work product is made or intended.

SWGDE requests notification by email before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in such proceeding. The notification should include: 1) The formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; and 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in the proceeding please notify SWGDE as to the outcome of the matter. Notifications should be submitted via the SWGDE Notice of Use/Redistribution Form or sent to secretary@swgde.org.

From time to time, SWGDE documents may be revised, updated, or sunsetted. Readers are advised to verify on the SWGDE website (https://www.swgde.org) they are utilizing the current version of this document. Prior versions of SWGDE documents are archived and available on the SWGDE website.

Redistribution Policy

SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain this SWGDE cover page containing the Disclaimer Regarding Use.
2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.
3. Any reference or quote from a SWGDE document must include the version number (or creation date) of the document and also indicate if the document is in a draft status.

Requests for Modification

SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be submitted via the SWGDE Request for Modification

Form or forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of any suggested modification:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) SWGDE Document title and version number
f) Change from (note document section number)
g) Change to (provide suggested text where appropriate; comments not including suggested text will not be considered)
h) Basis for suggested modification

Intellectual Property

Unauthorized use of the SWGDE logo or documents without written permission from SWGDE is a violation of our intellectual property rights.

Individuals may not misstate and/or over represent duties and responsibilities of SWGDE work. This includes claiming oneself as a contributing member without actively participating in SWGDE meetings; claiming oneself as an officer of SWGDE without serving as such; claiming sole authorship of a document; use the SWGDE logo on any material and/or curriculum vitae.

Any mention of specific products within SWGDE documents is for informational purposes only; it does not imply a recommendation or endorsement by SWGDE.

Scientific Working Group on Digital Evidence

Tech Notes on Cryptocurrency

Table of Contents

1. Purpose

The purpose of this document is to provide a reference for examiners conducting on-scene collection of cryptocurrency-related artifacts from digital evidence. The document is meant to assist in the recognition, triage, and collection of digital evidence associated with cryptocurrency assets.

2. Scope

The scope of this document is to provide guidance with recognition and collection of cryptocurrency-related artifacts from digital devices. This document is not designed to be a step-by-step guide on the acquisition of cryptocurrency.

Seizures or transfers of cryptocurrency assets have distinct legal, technical, and policy considerations. These considerations are outside the scope of this document, but examiners shall address them before conducting seizures or transfers of cryptocurrency assets.

The intended audience is personnel qualified to acquire digital evidence. For guidance on recommended training and qualifications, see *SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence*.

3. General Background

Cryptocurrencies are digital currencies produced by digital networks that use cryptography to ensure payments are sent and received securely. Examiners may be asked to identify evidence related to cryptocurrency use or transactions, or to conduct exigent extraction of information from digital devices needed to conduct seizures of cryptocurrency assets.

Cryptocurrency can be used for both illicit purposes and legitimate transactions. Cryptocurrency users may consider cryptocurrencies to provide enhanced anonymity compared to transactions using fiat currency and traditional payment systems.

Cryptocurrency is often used in ransomware schemes, with victims asked to make ransom payments using cryptocurrency.

Cryptocurrency mining is the process of verifying transactions on a digital ledger for a blockchain. Mining hardware can consist of single hardware up to multiple computer systems and can require extensive processing and electrical power.

4. Identification

Recognition of cryptocurrency activity involves looking for different types of cryptocurrency wallets, cryptocurrency addresses and key material, computer software or mobile applications, and artifacts associated with those applications.

4.1 Wallets

Wallets are used to store cryptocurrency and allow transfer of funds. Wallets can be software-based, hosted by a third-party service provider accessible through an app or web browser, paper wallets, or hardware wallets.

- Software wallets are maintained locally on computers and mobile devices. Some common software wallets are Electrum, Armory, and Copay. This type of wallet is recognizable on devices as installed software and applications, or by the presence of wallet data files associated with that application.
- Hosted wallets are maintained by a third-party service provider which is often also an exchange service. Common hosted wallets include Coinbase, Kraken, and Exodus.
- Paper wallets are physically printed, may include handwritten wallet recovery information, and may function as backup mechanisms for other wallet types. A paper wallet can fully recover a user's account. Paper wallets may include QR codes, cryptocurrency addresses, or printed private keys.
- Hardware wallets are devices, often resembling a USB thumb drive, specifically designed to maintain cryptocurrency wallets. Common hardware wallets include Ledger, Trezor, and KeepKey. This type of wallet plugs into a computer or mobile device via USB and is required to access the account.

Figure 1. Common hardware wallets.

4.2 Addresses

Each cryptocurrency has a unique address format associated with it. Most addresses are composed of letters and numbers and may be case sensitive. Below are examples of cryptocurrency addresses:

Coin Type	Alphanumeric sequence	Address structure
Bitcoin | BTC	25-36 characters beginning with a 1 or a 3	1BoatSLRHtKNngkdXEeobR76b53LETtpyT
Ethereum | ETH	42 characters beginning with Hex 0x	0x123f681646d4a755815f9cb19e1acc8565a0c2ac

Table 1. Examples of cryptocurrency addresses.

4.3 Seed Phrases

Seed phrases, sometimes called mnemonic phrases, are used to recover key pairs and other information needed to access and transfer cryptocurrency assets. Cryptocurrency seed phrases are a sequence of 12-25 seemingly random words or other characters. The seed phrase can be used to recover a cryptocurrency wallet to facilitate seizure of funds or further investigative or forensic analysis. Because seed phrases can be used to derive the information needed to execute transfers of funds, examiners should follow their organization's policies for handling valuable evidence when working with this artifact.

5. Triage of Artifacts

To facilitate successful on-scene seizures of cryptocurrency, examiners need to quickly identify, collect or extract, and sometimes reconstruct cryptocurrency-related digital and physical evidence.

If a device potentially containing cryptocurrency-related digital evidence is found powered on, examiners should keep the device powered on and prevent it from locking.

Examiners should review potentially involved devices and document the following:

- Presence of applications associated with cryptocurrency and encryption
- Any wallet addresses and passwords observed
- Encryption keys
- Wallet configuration or data files

Examiners should document or store information that can be used to cause the transfer of funds, including seed phrases and private keys, in a manner that prevents them from being accessed by unauthorized individuals.

Examiners should immediately acquire all pertinent artifacts associated with cryptocurrency applications, including:

- Username, passwords, passphrases, and seed phrases
- Encryption keys associated with wallets
- Encryption keys associated with user accounts (used for communication, etc.)
- Hardware wallets

Pertinent artifacts, such as usernames, passwords, and wallet addresses may be contained in multiple file types, including text files, image files, and documents. They may also be stored in non-digital locations, for example, on paper. Forensic triage should be thorough enough to identify these artifacts and review locations where they may reside.

Examiners should ensure that acquisitions are conducted in accordance with forensic best practices and document all actions. See *SWGDE Best Practices for Computer Forensic Acquisitions* for additional information.

6. Considerations

6.1 Cryptocurrency Seizure

Procedures and considerations for executing cryptocurrency asset seizures are outside the scope of this document. Examiners should follow their agency's policies and procedures for doing so.

6.2 Mobile Devices

If a mobile device is on and unlocked, keep it unlocked or secure the passphrase or swipe PIN to allow access for a triage exam. Recognition of artifacts is key in determining if a phone has been used to transact in cryptocurrency. Mobile devices may contain wallet applications and associated data used for cryptocurrency transactions. Wallet addresses with QR codes or text-based keys can reside entirely on a phone.

6.3 Hardware wallets/USB Devices

Accessing the funds associated with this type of wallet may require using the actual device the software is hosted on, in addition to the wallet dongle. If this is not identified on-scene, this wallet may remain unknown.

Hardware wallets may have anti-forensic features. For example, if the USB hardware devices are not connected properly, they can reset. Some are set to reset when connected to read-only

devices (such as to a write-blocker). Examiners should not attempt to forensically image USB hardware wallets as if they were USB storage media as this may engage anti-forensic features.

6.4 Volatility and Evidence Handling

Because of the ubiquity of encryption that may render data less accessible when devices are powered off or applications closed, examiners should triage devices to identify the use of encryption technologies and collect data that is most readily accessible via live acquisitions. This may include the contents of memory, encryption keys, activity in anonymous browsers such as the Tor Browser, data in encrypted messaging applications, and cryptocurrency artifacts.

Where the seizure of identified cryptocurrency is an investigative objective, identifying and recovering the artifacts needed to execute the seizure is time-sensitive, as the funds can be moved by a third party prior to seizure. Examiners should consider the order of their actions to facilitate this investigative objective.

Examiners should be aware of their organization's policies for handling and storing cryptocurrency artifacts, particularly those with the ability to affect the transfer of a cryptocurrency asset.

7. History

Revision	Issue Date	History
1.0 DRAFT	9/20/2022	Initial draft created.
1.0 DRAFT	10/13/2024	Released for Public Comment.
1.0 DRAFT	5/16/2024	Reworded to clarify concepts and release for Public Comment.
1.1 DRAFT	7/3/2024	SWGDE voted to approve as Draft for Public Comment. Formatted for release as a Draft for Public Comment.