Criminal Investigations and Network Analysis
A DHS CENTER OF EXCELLENCE AT GEORGE MASON UNIVERSITY

Digital Forensic Investigations involving Cryptocurrency Wallets Installed on Mobile Devices

Lead PIs: Cesar Quezada | Diana Summers

Forensics

SUMMARY

A significant gap in the digital forensic capabilities, protocols and understanding currently exist in law enforcement agencies regarding digital currencies. Investigators need an efficient way to seize cryptocurrencies from software wallet applications and extract, preserve, and analyze related data recovered from suspects' mobile devices. This project will create an operational database of digital forensic artifacts to provide reference materials and best practices information to law enforcement, providing benefit across criminal investigations as more crimes contain cyber or digital components.

PROBLEM STATEMENT

There is a lack of structured research related to the seizing cryptocurrencies from software wallet applications and extracting, preserving, and analyzing related data recovered from suspects' mobile devices. This is a significant gap in the capabilities and level of understanding that currently exists in law enforcement agencies (LEAs) at all levels in the United States. The days of executing search warrants and recovering drugs (for instance) and significant amounts of fiat currency (e.g., USD) are numbered, and many police departments across the country have already witnessed the shift to forms of seemingly anonymous "cryptocurrencies" in criminal cases.

These currencies are gaining in popularity as their use is particularly ubiquitous on anonymizing platforms and darknets. As such, LEA need to have digital forensic capabilities and protocols in place to adapt to this changing landscape.

APPROACH

This project analyzes and seizes cryptocurrency wallets from mobile devices, focusing on practical techniques for law enforcement investigations. Using forensic images of 12 iOS and 12 Android wallet apps, the research investigates how wallet data is stored and encoded, identifying critical artifacts such as private keys, transaction hashes, and user identifiers. In addition to providing a comprehensive guide to wallet seizure, the project emphasizes the importance of understanding how wallet apps store and encode data locally, offering technical insights into artifact extraction. By equipping investigators with practical knowledge, this work addresses the growing challenges of cryptocurrency-related crime and lays the groundwork for future innovations, including automated tools and expanded wallet analyses.

RESULTS

A database of digital forensic artifacts from cryptocurrency software wallets, including file paths of transaction data, any private keys recovered, and user information is under construction, and the standard procedural guidelines for LEAs to use in an operational capacity has been drafted.

ANTICIPATED IMPACT FOR DHS

Digital forensic investigators will be able to reference the artifact database and step-by-step instruction materials to more quickly and accurately extract cryptocurrency wallet information from recovered mobile devices in support of criminal and other investigations.