Criminal Investigations and Network Analysis
A DHS CENTER OF EXCELLENCE

GEORGE MASON UNIVERSITY

THE UNIVERSITY OF ALABAMA

Digital Forensic Investigations Involving Cryptocurrency Wallets Installed on Mobile Devices

LEAD PI: DIANA DOLLIVER

Forensics

SUMMARY

A significant gap in the digital forensic capabilities, protocols, and understanding currently exists 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 of 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, LEAs need to have the digital forensic capabilities and protocols in place to adapt to this changing landscape.

APPROACH

This project is developing (1) a database of digital forensic artifacts from cryptocurrency software wallets and (2) standard procedural guidelines for LEAs to use in an operational capacity complete with recommendations and best practices. The approach is to first install Bitcoin, Monero, and Ethereum software wallet applications onto iOS and Android smartphones, create three accounts for each form of cryptocurrency, and generate nine transactions per cryptocurrency. The researchers then image both phones using two commercial forensic software applications and document the digital forensic artifacts recovered from the apps when the user was (a) logged into the apps and (b) logged out of the apps.

These forensic images will generate a database of artifacts, including file paths of transaction data, any private keys recovered, and user information. The researchers then attempt to "seize" or otherwise clone the accounts on a third investigational phone based on the recovered data, and finally they develop guidelines and best practices for LEAs based on project findings.

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 have 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.