2023 - PDR - **678-1DF** - Cyber Forensics Investigation of Web3 Wallets - ozer@purdue.edu - Akif Ozer

CERIAS

The Center for Education and Research in Information Assurance and Security

Ubiquitous and Mobile Investigative Techniques and Technologies Lab — UMIT²

Cyber Forensics Investigation of Web3 Wallets

Akif Ozer, Mohammad Meraj Mirza, and Umit Karabiyik

OVERVIEW

This research aims at looking into mobile Web3 cryptocurrency wallets applications as a subjected to cyber forensic study, to investigate what can be recovered, and to highlight privacy and security concerns related to the investigated applications.

GOALS

The main goals of our project included:

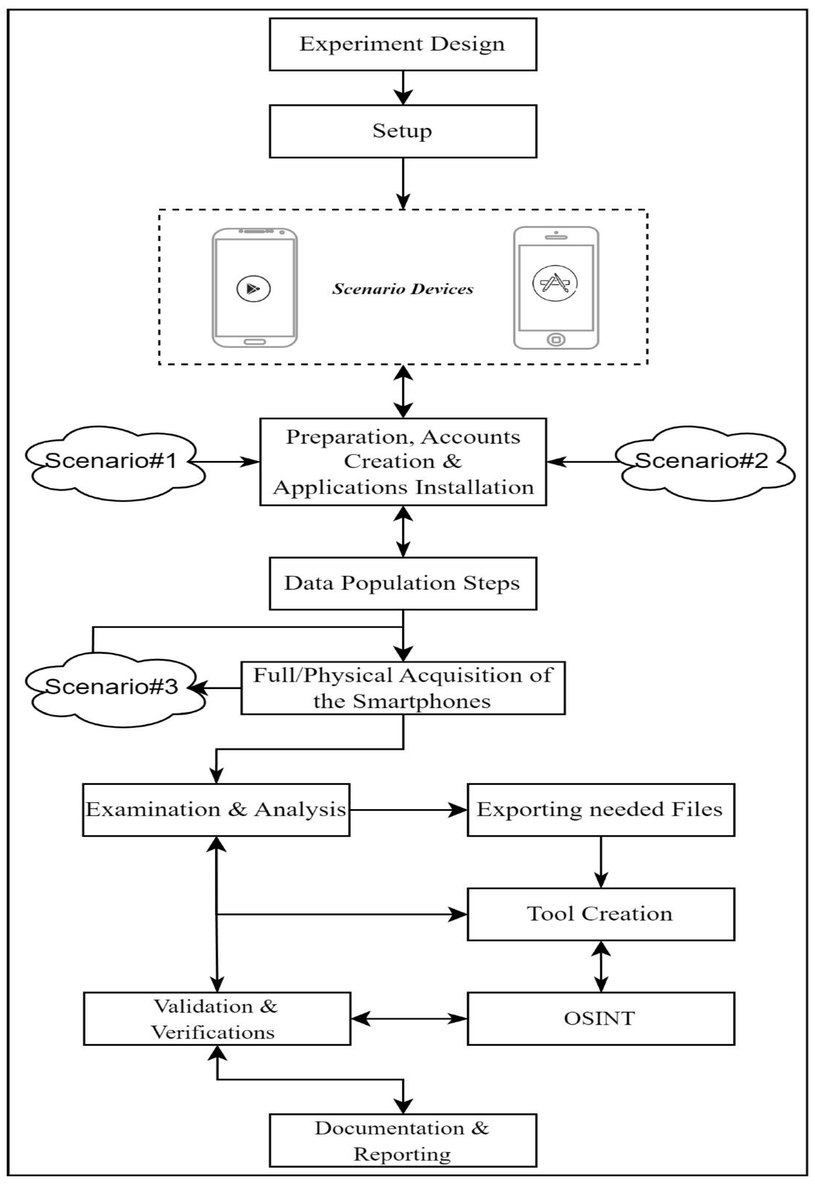
1. examined the possibility that the two wallets in consideration contained sensitive data that was not secured.

2. Developed a tool that can be used to help recover wallet addresses, transactions, and NFTs.

METHODOLOGY

In the research we used two devices: an iPhone 6s with iOS 14.1 and a Samsung SM-M205M running Android 10.0.
A brief explanation of what has been done in each step:

- **Experiment Design:** Discusses the guidelines followed for research and the device population.
- **Data Population:** the population of the two devices was carried out following well-known standards and was well documented. Data is populated using special publication 800-202 published by the National Institute of Standards and Technology (NIST).
- **Data Acquisition:** Along with the unique artifacts of the Android and iOS operating systems, we made sure that we could collect user data using proper tools.
- **Mobile Forensic Examination:** Evaluated what could be recovered.
- **Analysis:** Including our developed tool, different techniques, and Open Source Intelligence (OSINT).



FINDINGS

- Popular digital forensics tools such as Axiom and Autopsy does not detect crypto wallet application's artifacts.
- Our research showed that MetaMask and Trust Wallet stores transaction information differently.
- In Trust Wallet, we found valuable information like used decentralized finance applications and transaction history by analyzing https caches.
- Metamask stores general information about the wallet, such as Transaction History, Contacts, Balance, in a JSON file.
- Manual event reconstruction takes a significant amount of time that investigators could instead spend examining the evidence. Thus, the tool created as an outcome of this research has the ability to reconstruct transactions stored on the user's mobile phone and present them.

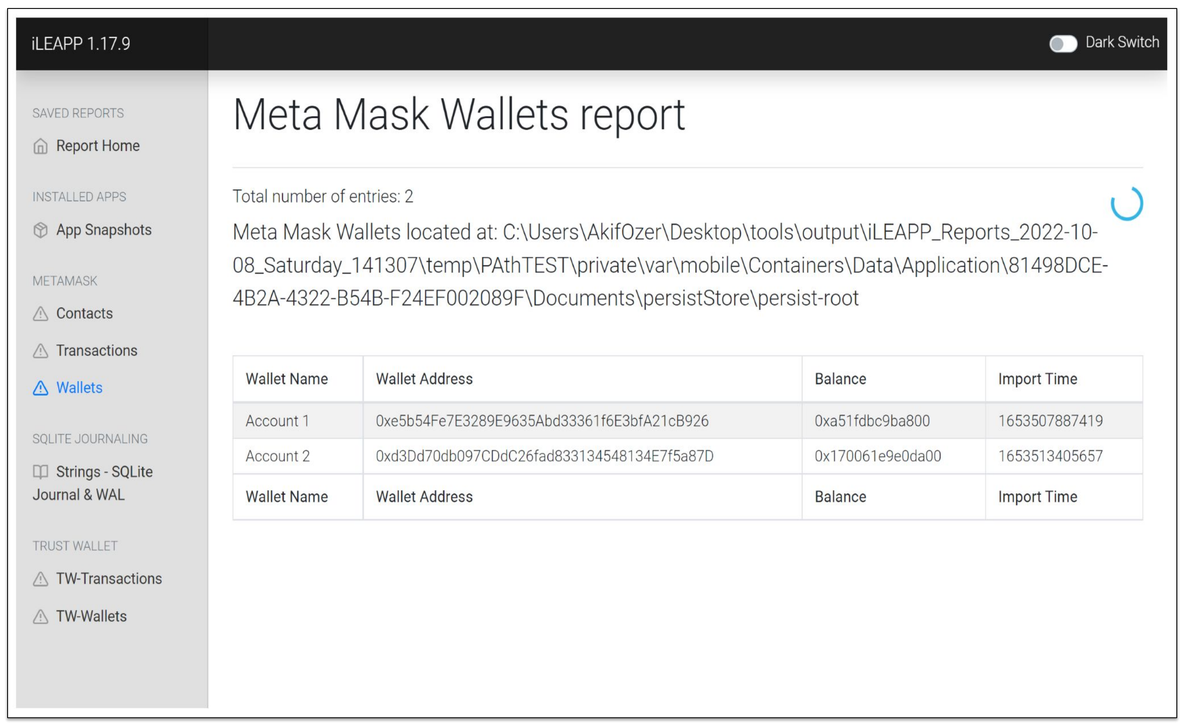


Fig. 2 Recovered Wallet addresses for the Metamask app on iOS using the developed tool

CONCLUSION

- This research can be a great resource for future research on cyber forensics in blockchain applications
- It is crucial to improve known digital forensic tools and strengthen their ability to extract artifacts from Web3 applications

PURDUE UNIVERSITY

{ozer, mmmirza, umit}@Purdue.edu

Mirza, M.M.; Ozer, A.; Karabiyik, U. Mobile Cyber Forensic Investigations of Web3 Wallets on Android and iOS. Appl. Sci. 2022, 12, 11180.

CERIAS