applied sciences

MDPI

Article

Mobile Cyber Forensic Investigations of Web3 Wallets on Android and iOS

Mohammad Meraj Mirza [1,*], Akif Ozer [2] and Umit Karabiyik [2,*]

[1] Department of Computer Science, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia
[2] Department of Computer and Information Technology, Purdue University, West Lafayette, IN 47907, USA
* Correspondence: mmmirza@tu.edu.sa (M.M.M.); umit@purdue.edu (U.K.)

Featured Application: As many new mobile device applications are leveraging blockchain technologies, Web3 wallets were created as a tool to store, manage, stack, and perform cryptocurrency-related transactions. Therefore, it is necessary to investigate what these new nontraditional applications store in their mobile apps and what can be recovered through cyberforensic procedures, which can help the cyberforensics community, tool developers, and law enforcement.

Abstract: Constant advancements in technology have a significant impact on our everyday lives and the ecosystem in which we live. The growing popularity of cryptocurrencies (e.g., Bitcoin and Ethereum), along with Non-Fungible Tokens (NFTs), which are founded on blockchain technology, has opened the way for these blockchain projects to be integrated into a wide range of other kinds of applications (apps). Today, cryptocurrencies are used as a popular method of payment online; however, their popularity on the dark Web is also increasing. For example, they can be used to buy and perform various illegal activities among criminals due to their anonymity. Web3 cryptocurrency wallets, used to store cryptocurrencies, have not been studied as thoroughly as many other apps from a digital forensic perspective on mobile devices, given the increasing number of these services and apps today for many platforms, including the leading mobile operating systems (i.e., iOS and Android). Therefore, the purpose of this research is to guide investigators to unlock the full potential of popular cryptocurrency Web3 wallets, Trust Wallet and Metamask, to understand what can be recovered, and to look at areas where there are knowledge gaps. We digitally analyzed and forensically examined two mobile wallets that do not require any personal identifiers to register and are widely used for Web3 cryptocurrencies on Android and iOS devices. We review the digital evidence we have collected and discuss the implications of the forensic tools we have used. Finally, we propose a proof of concept extension to the iOS Logs, Events, And Plists Parser (iLEAPP) tool to automatically recover artifacts.

Keywords: blockchain; cyber forensic; crypto wallet; data privacy; data security; digital forensic; digital wallets; mobile forensic; Open Source Intelligence (OSINT); Non-Fungible Tokens (NFTs); Web3

check for updates

Citation: Mirza, M.M.; Ozer, A.; Karabiyik, U. Mobile Cyber Forensic Investigations of Web3 Wallets on Android and iOS. *Appl. Sci.* **2022**, *12*, 11180. https://doi.org/10.3390/app122111180

Academic Editor: David Megías

Received: 20 September 2022
Accepted: 31 October 2022
Published: 4 November 2022

1. Introduction

The advancement of technology has a significant influence not only on our daily lives, but also on the world around us. The increasing acceptance of blockchain-based cryptocurrencies such as Bitcoin and Ethereum and the Non-Fungible Tokens (NFTs) that accompany them has opened the way for the technology to be put into use in cases that were previously unimaginable. The third generation of the World Wide Web, known as Web3, includes features such as decentralized blockchain technology and token-based economics [1]. According to the National Institute of Standards and Technology (NIST) [2], most cryptocurrencies are built on the blockchain, which marks a paradigm shift in digital interactions and acts as the backbone of technology. Furthermore, in contrast to fiat currencies, the blockchain is a decentralized and tamper-resistant ledger that guarantees the accuracy of the information it stores [2,3], that is not controlled by the authority of monetary policymaking [3,4]. In [3], the United States Department of Justice created an illustration (see Figure 1) that highlights and gives a general anatomy for the transaction carried out with cryptocurrencies.

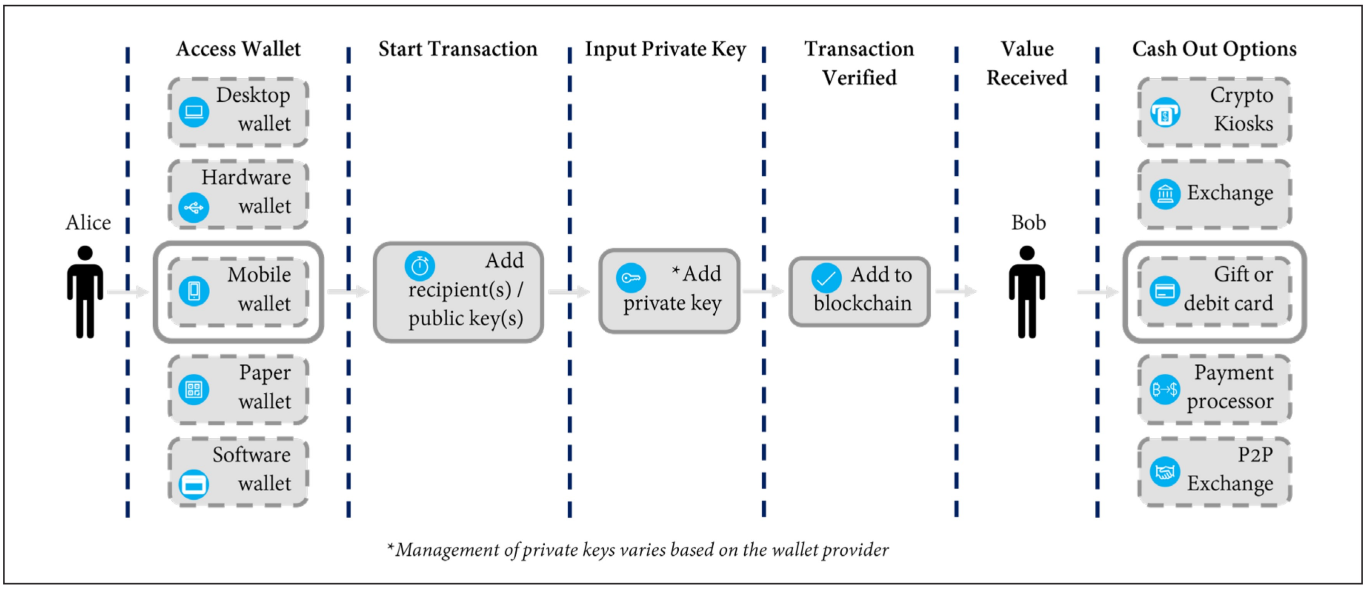


Figure 1. Figure of anatomy of cryptocurrency transactions taken from [3].

Furthermore, according to the 2021 Crypto Crime Report published by Chainalysis [5], the total volume of transactions on the cryptocurrency market has increased more than ever and reached approximately $15.5 trillion in 2021, with an increase of almost 560% in 2020. On the other hand, the Crypto Crime Report [5] also highlighted that the total amount of illicit cryptocurrency-related criminal activity reached a new high of approximately $14 billion in 2021 [6]. Tracking and invisibility in the digital world have become more difficult due to innovative methods combined with the use of cryptocurrency. According to [7], cryptocurrency has made it easy to carry out illicit and criminal activities (e.g., laundering large amounts of money) while remaining completely anonymous. Furthermore, cryptocurrencies are a well-established means of payment on the dark Web and can be used to trade illegal goods [8,9].

According to [10], as of April 2022, more than 82.8 million Blockchain.com wallet users are being used to hold and handle different cryptocurrencies around the world. Figure 2 shows the dramatic increase in the number of wallets between 2012 and 2022. Furthermore, the Blockchain.com (accessed on 21 May 2022) wallet has averaged around 266,000 transactions per day during the past year [10]. On the other hand, the Web3 latest-generation wallets have recently been introduced to the market. Two of the most well-known wallets based on Web3 technologies are Metamask, which recently reached 30 million users in 2022 [11,12], and Trust Wallet, which is also used by more than 25 million users around the world [13].

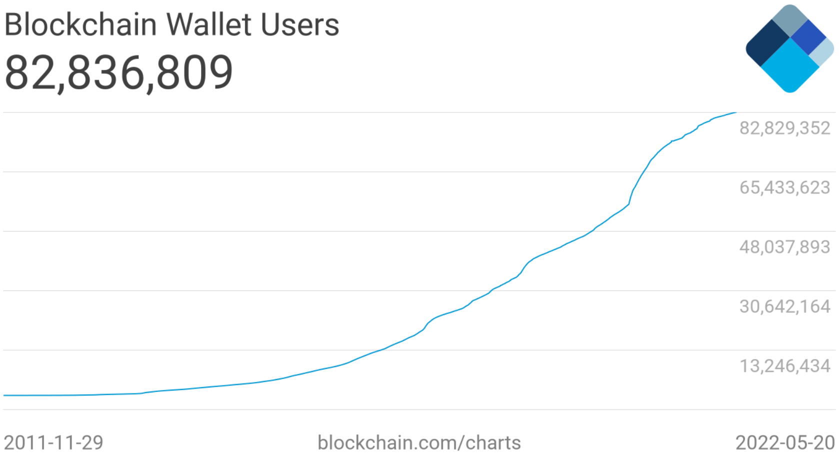


Figure 2. Blockchain.com chart of the number of unique wallets created over the years [14].

Digital personal identifiers (e.g., Personally Identifiable Information (PII)) of people are becoming increasingly important, as they are utilized by many technologies with which users interact digitally or physically [15]. Therefore, it is also more than ever important to ensure that these identities are secure and well encrypted. In cryptocurrency, there are two essential digital personal identifiers, public and private keys, which can be stored in many forms, such as digitally and on paper [3]. Cryptocurrency wallets can digitally store these and also allow users to move their funds across blockchains and track the value of their cryptocurrencies. Furthermore, the introduction of cryptocurrency wallet apps adds to the complexity of the existing challenges of new artifacts found in systems and applications (apps) that change rapidly with each new update [16,17].

Cryptocurrency wallets offer their users an environment that allows them to access and transact on blockchain networks. However, cryptocurrency wallet apps have not been studied as thoroughly as many other apps from a digital forensic perspective that also covers privacy and security concerns. This is particularly critical given the increasing number of these services and apps today for many platforms, including the leading mobile operating systems (i.e., iOS and Android). Furthermore, a lack of understanding of these technologies and their features could have contributed to the potential lack of research on them. Furthermore, any information that leads investigators to data that identify the person operating the wallet could be considered personally identifiable information, which is a significant issue that affects the outcome of many investigations.

The need to expand the existing body of knowledge in the area of mobile forensics when it comes to Web3 cryptocurrency wallets is emphasized extensively throughout our work. At the time of this research, no research was available that included the wallets investigated. Therefore, to help forensic investigators and contribute to the body of knowledge, the purpose of this research is to guide investigators to unlock the full potential of cryptocurrency wallets, understand what can be recovered, and look at areas where there are knowledge gaps. Therefore, in this paper, we use a wide variety of techniques that have all played roles in the development of mobile application forensics as it exists today. In addition, to ensure the reproducibility of the digital evidence that was collected, we conducted, validated, and verified the data utilizing two well-known tools. In this study, the use of Magnet Axiom [18] is an example of an industry standard commercial tool that many practitioners use, compared to Autopsy [19], which is a well-known open-source forensic tool.

The contributions of this research are as follows:

- Digitally analyzed and forensically examined two mobile wallets, Trust Wallet [13] and Metamask [11], which are widely used for Web3 cryptocurrencies on Android and iOS devices.

- Investigated the possibility that those two wallets kept unencrypted data that might have posed a security risk to the user's privacy.
- Highlighted Personal Identifiable Information (PII) that can be used as evidence.
- Recovered and reconstructed wallets and transactions, as well as NFTs that are owned by the wallet owner.
- Reviewed the digital evidence that has been collected and discussed the implications of the forensic tools that were used.
- Developed an artifact extension for the iOS Logs, Events, And Plists Parser (iLEAPP) [20] tool to automatically recover information about wallet addresses and transactions as a proof of concept.

The remainder of this paper is structured as follows. Section 2 discusses the literature review and other related work that has been conducted. Section 3 explains our research methodology and our experiment design. Detailed findings can be found in Section 4, while Section 5 provides an overview of the tool that we created as a proof of concept and as an outcome of this research. A more in-depth assessment of the analysis and the developed plugin and its significance can be found in Section 6. Finally, Section 7 concludes our research and gives future research directions. Note that Table 1 lists all the abbreviations used in the article.

Table 1. Abbreviations used in the manuscript.

Abbreviation	Name
ADB	Android Debug Bridge
ALEAPP	Android Logs, Events, And Plists Parser
API	Application Programming Interface
BNB	Binance Coin
CAKE	Pancake Swap Coin
ETH	Ethereum Coin
JSON	JavaScript Object Notation
HSTS	HTTP Strict Transport Security
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
iLEAPP	iOS Logs, Events, And Plists Parser
INTERPOL	International Criminal Police Organization
NFTs	Non-Fungible Tokens
NIST	National Institute of Standards and Technology
OS	Operating System
OSINT	Open-Source Intelligence
P2P	Peer-To-Peer
PII	Personal Identifiable Information
plist	Property List
QR	Quick Response
RAM	Random Access Memory
IoT	Internet of Things
URL	Uniform Resource Locator
UTC	Coordinated Universal Time

2. Literature Review

The following section provides an overview of previous studies that have laid the foundation for the current study and forensic investigation. It also addresses the limitations of prior research and explains how we overcome those problems in our own study.

2.1. Blockchain, Cryptocurrency, and NFTs

There has been great attention from academic and industrial specialists since blockchain technology was initially launched in 2008 after the global financial crisis [21]. Blockchain is the fundamental technology utilized in the production of a variety of cryptocurrencies due to the decentralized nature of the ledger it produces. In [22], Satoshi Nakamoto, the pseudonymous author(s) of the Bitcoin white paper, proposed that people can use blockchain technology to instantly send money to each other (that is, peer-to-peer) without the need for a mediator (i.e., trusted authorities) or the customary fees associated with online financial transactions [23,24]. As a result, according to statistics [25], Bitcoin is the leading cryptocurrency to date that disrupted the normal financial system and does not require trusted authorities to maintain [4,21,24,26].

Furthermore, according to [24], the introduction of blockchain 2.0 allowed Ethereum and other cryptocurrencies to play a role in the game with the launch of smart contract functionality. Therefore, law enforcement organizations around the world, including INTERPOL, began to focus on blockchain technology as it has been associated with a wide variety of illicit activities, such as drug trafficking, child exploitation, money laundering, and terrorist attacks [9]. For these reasons, and as a direct consequence of the activities outlined above, there has been an increase and expansion of studies, research, and investigations on how criminals utilize cryptocurrencies [9].

Therefore, according to the author of [9], in recent years, many organizations have been diligently working to develop forensic tools and methodologies for the investigation of various cryptocurrencies. For example, researchers in [27] proposed a methodology that was developed to help preserve and seize various types of crypto wallets found at a crime scene. In addition, researchers in [28] discuss the current state of knowledge centered on blockchain technologies and cryptocurrencies, specifically bitcoin, and how the use of anonymity in these technologies and transactions affects law enforcement in investigating crimes and criminal activities.

Despite the fact that cryptocurrency privacy has improved, criminals always try to make it harder for law enforcement investigators to track their transactions. Detecting malicious behavior on blockchain ledgers is difficult even if the data are, by design, open to the public [29]. According to [9], criminals often employ crypto-mixing/tumbler services and decentralized P2P exchange platforms to clean their dirty coins, adding an additional layer of protection to criminals and an additional layer of difficulty to investigators.

2.2. Privacy and Security of Wallets

Since blockchain technology was first introduced in 2008, CIA (i.e., Confidentiality, Integrity, and Availability) and security have been the focus of academic and industry professionals. Although many of the blockchain standards meet the CIA, there are many variables that need to be taken into consideration when building a Web3 platform. Researchers in [30] investigated the privacy and security of mobile wallets for Bitcoin, Dash, Monero, and Zcash. The authors conducted an examination to see whether the cryptocurrency transactions of the users of the investigated wallets are hidden from third parties. By examining the features of the wallets, researchers were able to determine how much personal data the creators of popular mobile wallets have access to [30]. As a result, they reported that if an adversary has sufficient resources, they can properly identify transactions that are produced by a single device. The authors in [31], have looked at the Electrum wallet v3.0.2 from a security point of view and found that there were major security vulnerabilities, allowing someone with malicious intent to potentially gain access to the wallet and steal the bitcoins stored there.

As mentioned in Section 1, blockchain transactions have increased rapidly over time. Since the blockchain is a public ledger, anyone can verify and view transactions that occurred in the past. The exponential visibility of these transactions allows people to create their own programs to create cryptocurrency intelligence, blockchain analytics, and automation with the help of public APIs. For example, the tool developed in [32] has helped identify cold wallets on the blockchain. In addition, there have been many attempts to create programs and interactive visualizations that can help find connections between wallets. Researchers in [33] proposed the use of graph theory to track cryptocurrency transactions, while researchers in [34,35], designed and developed new technical tools that allow interactive visualizations.

2.3. Forensically Relevant Artifacts

Forensic investigations of cryptocurrency wallets' objectives consist of discovering evidence of cryptocurrency activity, such as transaction logs and addresses used to send funds. Researchers in [36] studied data pertaining to RAM to check for traces of cryptocurrency wallets from Windows OS. The data retrieved in this study demonstrate that the memory processes of the wallets of popular bitcoin clients (i.e., Bitcoin Core and Electrum) may serve as a good source of information. Similarly, the researchers in [37,38] looked at what cryptocurrency relevant artifacts can be recovered from the RAM and hard disk image of the Windows OS.

Moreover, researchers in [39] investigated the cryptocurrency wallets of Monero and Verge coins that were installed on the Linux operating system. They were able to extract critical information from the RAM analysis, as well as the image of the drive that was acquired in the study. Furthermore, the researchers in [39] examined multiple sources of evidence that can be recovered from a virtual machine running Ubuntu OS. They analyzed the computer's volatile memory, network traffic, and hard-disk images of the computer, where they found many forensic artifacts. Furthermore, Litecoin and Dark currencies have been investigated in iOS and Android forensic research [40]. The authors were able to recover information such as metadata, installation data, timestamps, and usage traces. Furthermore, when it comes to mobile devices, the authors of [41] detail how to extract forensic information from the Bitcoin and Dogecoin wallets on the Android smartphone. They were able to retrieve information such as wallet identifiers, transaction identifiers, timestamps, emails, cookies, and OAuth tokens.

In the last few years, researchers have devoted a substantial amount of time and effort to advance the investigation of digital crimes. As a result, a significant number of researchers intend to assist law enforcement agencies when it comes to computer forensics [42–44], digital forensics [45,46], mobile forensics [47–49], cyber forensics [50–52], IoT forensics [53,54], and drone forensics [55,56]. However, to the best of our knowledge, no research has been conducted on selected cryptocurrency Web3 wallet apps on iOS and Android operating systems in the academic literature on mobile and cyber forensics. A few researchers have conducted forensic investigations on Bitcoin wallets, such as [37,38,40,57]; however, they are limited to outdated applications that are no longer used or are used in old versions of the OS. Furthermore, according to the findings of the researchers in [58], digital forensics is still relatively new for blockchain technologies. Table 2 provides a brief summary of the shortcomings identified in previous related studies. Therefore, with the dramatic increase in the use of Web3 wallets to store and manage cryptocurrencies and NFTs, there is a need to investigate what can be recovered and from where. Therefore, the purpose of this work is to contribute to filling the knowledge gap for Web3 wallets that can store cryptocurrencies and NFTs on iOS and Android devices.

Table 2. A summary of some shortcomings in related works.

Article	Objective(s)	Methods and Techniques	Shortcomings
Volety et al. [31]; Cracking Bitcoin wallets: I want what you have in the wallets	In this study, Multibit HD and Electrum, two Bitcoin Windows OS wallets, were studied for feasible vulnerabilities that can affect the users of these wallets.	In the paper, the authors focused on using vulnerabilities that enables a password exploit using offline brute force attempts, which can be used to steal cryptocurrency from the wallets investigated.	The focus of the investigation is more on the security side than on forensics.
Montanez [40]; Investigation of cryptocurrency wallets on iOS and Android mobile devices for potential forensic artifacts	This study's objective was to investigate the most widely used mobile wallet applications for Bitcoin, Litecoin, and Darkcoin cryptocurrencies to determine whether or not any forensic traces were left behind by these apps.	The author used iFunBOX for iOS, ADB for Android, and Cellebrite UFED physical Analyzer, which is a widely utilized commercial forensic software, the author was successful in recovering data such as metadata, installation data, timestamps.	Although the author was able to recover information, the author failed to extract information from the logical extractions of the Android Device (i.e., Samsung Galaxy S4), therefore, the study used an emulator to be able to recover information for Android.

Table 2. *Cont.*

Article	Objective(s)	Methods and Techniques	Shortcomings
Koerhuis et al. [39]; Forensic analysis of privacy-oriented cryptocurrencies	A forensic investigation of cryptocurrency wallets for Monero and Verge coins on an Ubuntu 16.04 LTS virtual machine.	This paper looked at a wide range of potential evidence that can be recovered from the computer's volatile memory, network activity and hard drives images.	The focus of the investigation concentrated on Ubuntu OS, more investigations are needed of similar kind on other popular platforms.
Van Der Horst et al. [36]; Process Memory Investigation of the Bitcoin Clients Electrum and Bitcoin Core	This article examined volatile memory of two popular Bitcoin clients (i.e., Bitcoin Core and Electrum) running in a virtual Windows machines, to better understand how important and where data may be kept (e.g., keys, transaction data, and passphrases).	The paper focused on extracting information and reporting it successfully by taking both RAM and device disk acquisitions.	Although the researchers were able to find that memory and disk images were valuable source of evidence, more research in needed for other platforms.
Doran [37]; A Forensic Look at Bitcoin Cryptocurrency	This research aimed at how to create a strong argument involving Bitcoin artifacts that are recovered and have Bitcoin wallets software installed. In addition, the author looked into how to recover evidence of Bitcoin mining.	The research concentrated on properly extracting and reporting information from RAM and hard disk.	The focus of the investigation concentrated on Windows OS Bitcoin wallets.
Jones [38]; Examining the forensic artifacts produced by use of bitcoin currency	The author in this paper studied a web version of the blockchain.con and the Bitcoin software wallet MultiBit v0.5.17 looking for recovered information in both RAM and hard disk images.	This research examined forensically two kinds of web based wallets and the MultiBit Bitcoin wallet running on windows OS and focused on extracting information and reporting it successfully by taking both RAM and device disk acquisitions.	Windows 7 OS was the only primary topic of investigation in this study.
Chang et al. [41]; Forensic Artefact Discovery and Attribution from Android Cryptocurrency Wallet Applications	This research focused on finding relative forensic artifacts about transactions involving bitcoin and dogecoin.	The research focused on the transaction hash IDs to find information about the cryptocurrency transfer using Ciphertrace. In addition to that, the authors back up the findings with the digital artifacts found in emails, cookies, and OAuth tokens.	This paper focuses on the individual currencies and transactions related to them on Android OS only.

3. Methodology

The following subsections details the methodology used in this paper. Figure 3 illustrates the steps followed in this study and provides an overview of the technique we used in our investigation, including all the procedures and components used.

Moreover, below is a brief explanation of what has been done in each step:

- **Experiment Design:** Discusses the guidelines followed for research and the population of devices.
- **Data Population:** This step is vital because it forms and tones the basis for the rest of the research. Therefore, the population of the two devices was carried out following well-known standards and was well documented. In addition, we tried to cover as many functions of the applications as possible.
- **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).

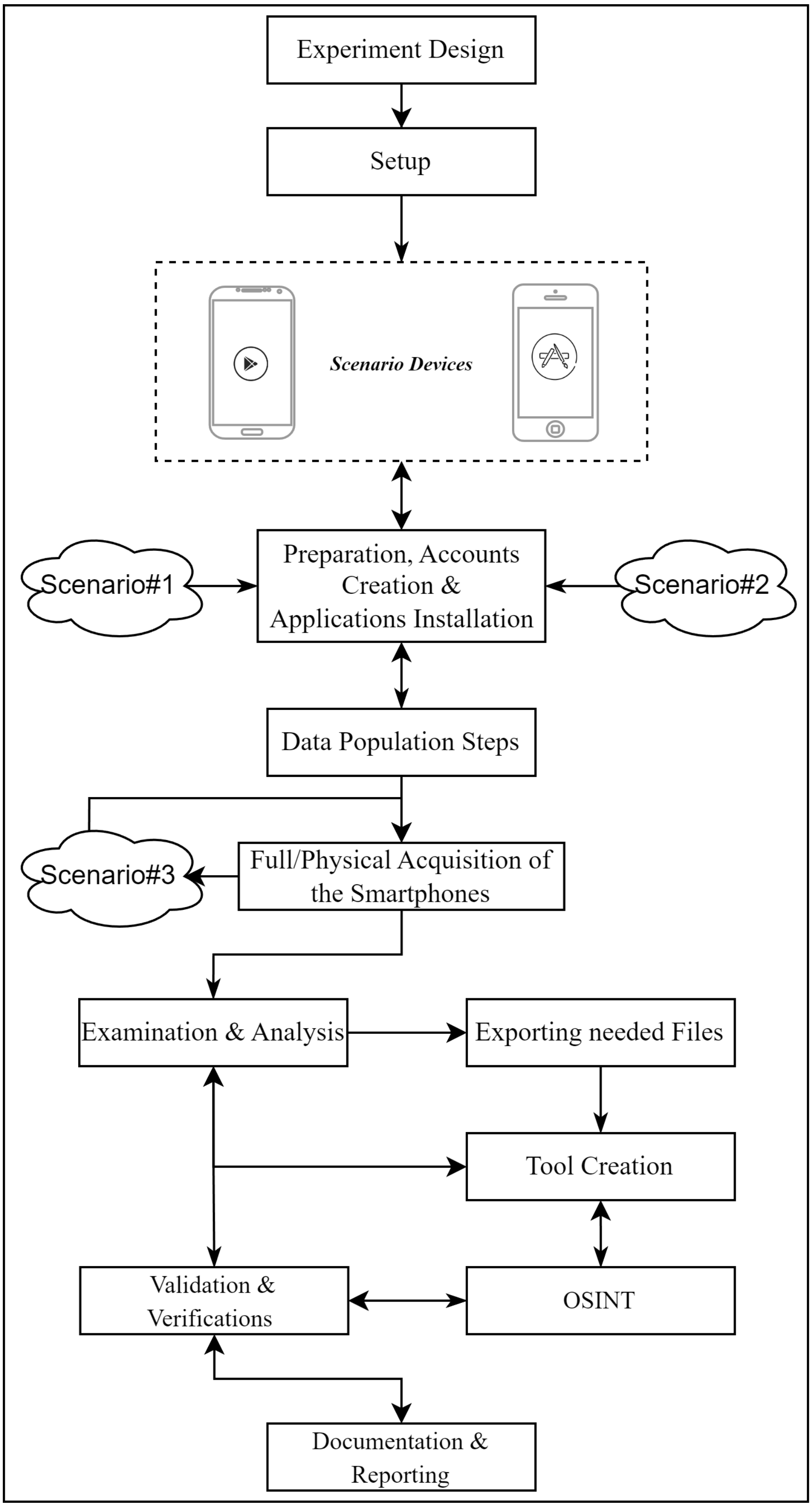

Experiment Design
Setup
Scenario Devices
Preparation, Accounts Creation & Applications Installation
Scenario#1
Scenario#2
Data Population Steps
Full/Physical Acquisition of the Smartphones
Scenario#3
Examination & Analysis
Exporting needed Files
Tool Creation
Validation & Verifications
OSINT
Documentation & Reporting

Figure 3. The research methodology.

3.1. Experiment Design

This research followed well-known guidelines in the digital forensics community that many researchers are following due to the clear instructions. For the case studies (scenarios) in this investigation, we populated the devices following the special publication 800-202 [59] published by the National Institute of Standards and Technology (NIST). Furthermore, best practices were used to obtain and analyze digital forensic images of related devices, which were then used in the subsequent analysis. Therefore, the study follows a well-defined digital forensic procedure for various devices provided by NIST, more specifically, the research follows the four primary steps of the NIST Special Publication 800-101 of the guidelines on mobile device forensics [60], as indicated in Figure 4.

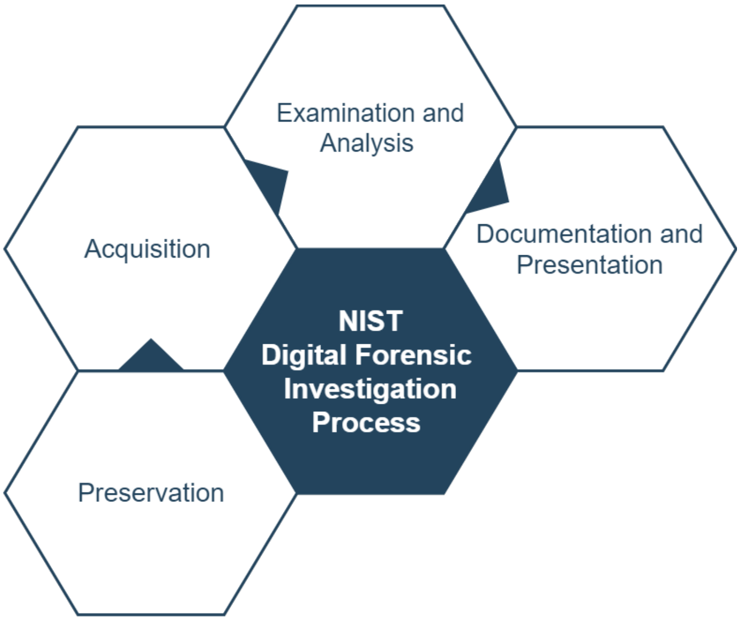

Examination and Analysis
Acquisition
Documentation and Presentation
NIST Digital Forensic Investigation Process
Preservation

Figure 4. NIST high-level guidelines on mobile device forensics in [60].

3.1.1. Devices Used

In this study, we selected two smartphones as test devices: (i) an iPhone 6s with iOS 14.1, and (ii) a Samsung SM-M205M running Android 10.0. Research required the creation of a new Google Gmail account [61], which we used to set up new iCloud [62] and Google Play [63] accounts for use on mobile devices. The devices used in the study and their specifications are highlighted in Table 3. Furthermore, the version of the apps used for this study was Metamask version 5.1.1 and Trust Wallet version 7.6 for the iPhone device, and on the Android device, they were Metamask version 5.0.1 and Trust Wallet version 5.37.

Table 3. Full specifications of the devices used in the study.

Device Name	Model/Version	Device ID
Samsung M20	Model: SM-M205M ∣ OS Android 10	SN: R28M42P586F
iPhone 6s	Model: A1688 ∣ iOS 14.1	MEID: 35542607266045

In this research, it was necessary to use the rooting method, which gives us full access to the user data partition and the device file system, where the most important forensic evidence is kept. Furthermore, it enables the extraction of more data that are useful at later stages of the investigation. To prepare the Android device for research, we had to do the following.

- Install TWRP [64];
- Flash Magisk [65] using TWRP;
- Phone will give Verification Failed error;
- Go back to TWRP and format the data.

However, preparing the iPhone device was a bit different since we had jailbroken the iPhone after finishing the data population steps. More details on jailbreak/rooting are discussed in Sections 3.3 and 3.4, and Figure 5 illustrates the order in which the rooting and jailbreak procedures were performed.

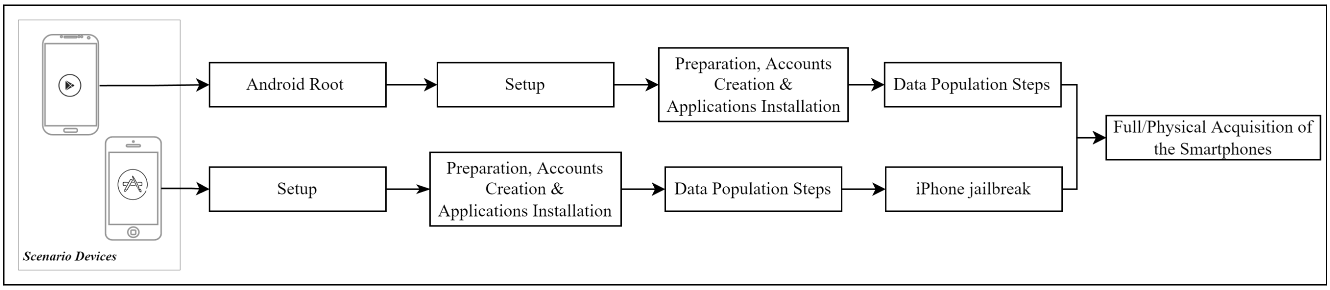

Android Root
Setup
Preparation, Accounts Creation & Applications Installation
Data Population Steps
Full/Physical Acquisition of the Smartphones
Setup
Preparation, Accounts Creation & Applications Installation
Data Population Steps
iPhone jailbreak
Scenario Devices

Figure 5. High level procedures order for rooting and jailbrarking the devices.

3.1.2. Machines Used for Investigations

In this investigation, two forensic workstations were used throughout the stages of the forensic investigation (see Table 4 for a complete description of the tools used in all phases). The first Forensics Workstation was running Windows 10 Pro Version 21H2 with an Intel Core (TM) i9-10900K CPU @3.70 GHz and the Workstation had 32.0 GB RAM installed. The second Forensics Workstation was running Windows 10 Education Version 21H2 with an AMD Ryzen 9 3900X 12-Core Processor 4.00 GHz and 32.0 GB RAM. Both machines were equipped with the same list of tools, except for the checkra1n program that was used to jailbreak the iPhone used in the study, where a MacBook Pro laptop was used to jailbreak, as the Windows operating system was not compatible with the tool.

Additionally, the programs and tools utilized in this study were carefully chosen to maintain integrity. Table 4 lists all the tools selected to carry out our digital forensic investigation. The list of tools includes forensic acquisition, forensic analysis, entropy measurement, jailbreak, and rooting tools. This study selected these tools because they are accessible to researchers and specifically designed for the investigation of mobile devices.

Table 4. Tools and applications used.

Software Name	Version	Usage	Availability
Autopsy	4.19.3	Examination and Analysis	Open-source
Magnet Acquire	v2.51.0.29844	Acquisition	Freeware
Magnet AXIOM Process	6.1.0.31400	Processing	Proprietary
Magnet AXIOM Examine	6.1.0.31400	Examination and Analysis	Proprietary
Odin3	v3.14.1	Rooting the Android phone	Freeware
TWRP	v3.6.1	Custom Recovery Image	open-source
Magisk	v25.2	Software for customizing Android	Open-source
checkra1n Program	0.12.3 Beta	Jailbreaking the iPhone in case 1	Freeware
iLEAPP	1.17 9	We developed our Plugin for this Tool	Open-source
ExifTool	v12.44	Reading meta-information	Open-source
Available online: https://codebeautify.org (accessed on 2 October 2022)	Online v6.4	Code Formatter	Online
Realm Studio	v12.0.0	Reading and Opening Realm Databases	Open-source

3.2. Data Population

The data population is explained in more detail in the following Figure 6. Scenario 1 involved the use of the Trust Wallet app on both phones, and Scenario 2 involved the Metamask app on both phones. We ensure that this step is well documented to allow the recovery of actions performed and information entered on the devices for later stages of analysis and examination. Although these are made-up scenarios and not real criminal investigations, we carried out actions that criminals would do. After populating Scenarios 1 and 2, we deleted both apps from the phones in Scenario 3 to see what could be recovered.

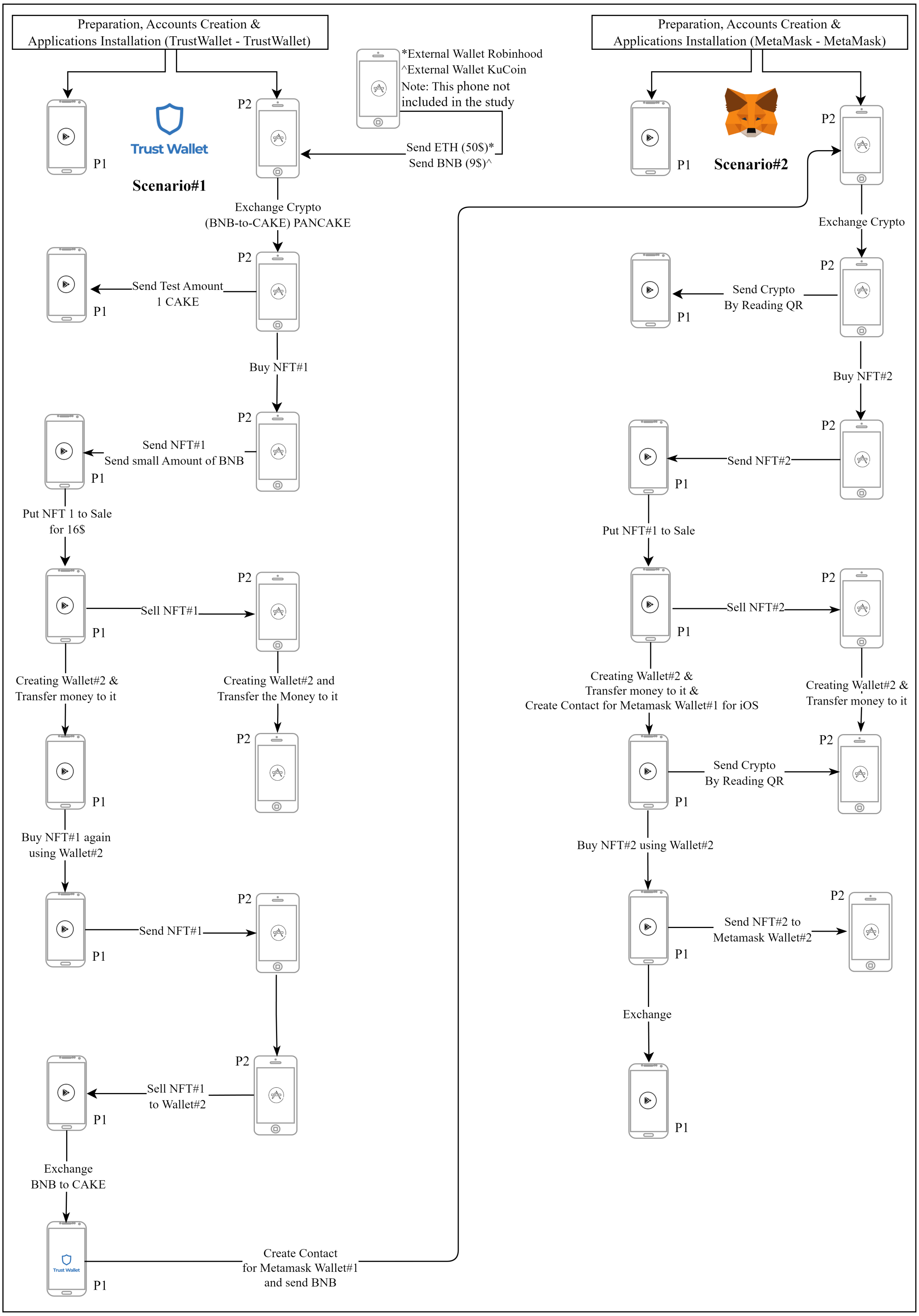

Preparation, Accounts Creation & Applications Installation (TrustWallet - TrustWallet)
P1
Trust Wallet
Scenario#1
P2
*External Wallet Robinhood
^External Wallet KuCoin
Note: This phone not included in the study
Send ETH (50$)*
Send BNB (9$)^
Exchange Crypto (BNB-to-CAKE) PANCAKE
P2
Send Test Amount 1 CAKE
P1
Buy NFT#1
P2
Send NFT#1
Send small Amount of BNB
P1
Put NFT 1 to Sale for 16$
P2
Sell NFT#1
P1
Creating Wallet#2 & Transfer money to it
Creating Wallet#2 and Transfer the Money to it
P2
P1
Buy NFT#1 again using Wallet#2
P2
Send NFT#1
P1
P2
Sell NFT#1 to Wallet#2
P1
Exchange BNB to CAKE
Trust Wallet
P1
Create Contact for Metamask Wallet#1 and send BNB
Preparation, Accounts Creation & Applications Installation (MetaMask - MetaMask)
P1
Scenario#2
P2
Exchange Crypto
P2
Send Crypto By Reading QR
P1
Buy NFT#2
P2
Send NFT#2
P1
Put NFT#1 to Sale
P2
Sell NFT#2
P1
Creating Wallet#2 & Transfer money to it & Create Contact for Metamask Wallet#1 for iOS
Creating Wallet#2 & Transfer money to it
P2
Send Crypto By Reading QR
P1
Buy NFT#2 using Wallet#2
P2
Send NFT#2 to Metamask Wallet#2
P1
Exchange
P1

Figure 6. Scenarios 1 and 2 for both apps on the two phones.

3.3. Preservation

The initial step in the NIST procedure is the preservation phase, which includes subprocesses that include search, identification, and evidence collection [60]. Therefore, the evidence must be retained in its original condition throughout the preservation phase, as failure to do so may result in the destruction or alteration of a component of the total evidence.

In order to obtain the most from the device and app data in the data collection process, for Android, Samsung's Odin3 (v3.04) firmware flashing software was used to flash a rooted patch on the operating system. On the iPhone, we had to perform jailbreaking using the Checkra1n (0.12.3 Beta) tool.

Throughout the paper, we use the epoch timestamp that shows the amount of time that elapsed (in seconds) since 1 January 1970 [66]. This is important because we can compare it with other sources, such as the public ledger. Although timestamps for HTTPS requests do not match the cache file creation time, there might be a ±3 s difference between the two. Therefore, we used the epoch time in the HTTPS request URL to compare it with the publicly available blockchain transaction history.

3.4. Acquisition

After the population and preservation stages were complete, we toggled the two smartphone's mode switch to "Airplane" and then used the Magnet Axiom Process (v 6.1.0.31400) tool to image the devices using full acquisition forensic techniques. The aim of obtaining full forensic image acquisition is to recover all the data that can be recovered from both devices. In specific situations, the Android and iOS operating systems generate their own unique artifacts, and the full physical acquisition method ensures that we retrieve both the system and the app data. Therefore, each and every piece of data that an application keeps locally on a device for the benefit of its end users should be included in the full forensic image acquisition along with the system data.

In this study, it was necessary to take more than one image for each device. To establish a baseline before the deletion of the apps and after the deletion, we took into account the two images for each phone to enable us to conduct the initial analysis and compare it with the images after the deletion of the apps. As a result, two images were taken from each device. The first was taken after the initial population, while the second acquisitions were taken after deleting the applications from both devices. Table 5 provides descriptions of all mobile forensic images taken in the study.

Table 5. Detailed acquisition process.

Device	Acquisition Tool	Description
iPhone	Magnet Acquire	iOSImage 1: After Scenarios 1 and 2
Samsung	Magnet Acquire	AndroidImage 1: After Scenarios 1 and 2
iPhone	Magnet Acquire	iOSImage 2: After Scenario 3
Samsung	Magnet Acquire	AndroidImage 2: After Scenario 3

4. Analysis and Findings

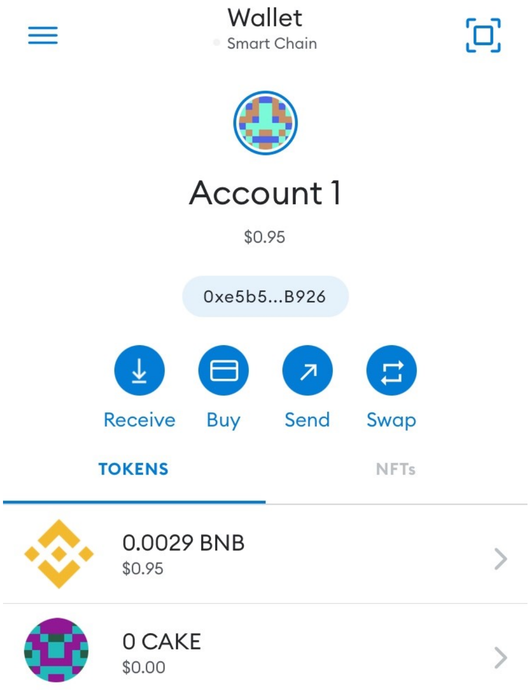
The analysis performed on the two apps on the two phones resulted in a wide range of forensically valuable artifacts after conducting a full digital forensic assessment of images from Android and iOS. The Web3 wallet apps for cryptocurrency on iOS and Android smartphones have the ability to retain a substantial amount of user information. Table 6 provides all the addresses of the wallets created in the study. We provide a complete summary of the findings of our study in the following Sections 4.1 and 4.2.

Table 6. Wallet addresses created in the study.

Device/OS	App Name	Wallet Address
Android	Metamask	Wallet1:0x012469cE84E7c64A94368C7D74F0e0D4a0671617 Wallet2:0xFE99dd4568D459e30E439D966C6deb9686F88A5A
	Trust Wallet	Wallet1:0x98b256497Ab16884cD8a6363A70cbC5Ef7AD917E Wallet2:0xC261645380F30224e820254736D0acE38311BF08
iOS	Metamask	Wallet1:0xe5b54Fe7E3289E9635Abd33361f6E3bfA21cB926 Wallet2:0xd3dd70db097cddc26fad833134548134e7f5a87d
	Trust Wallet	Wallet1:0x9E2C9A41C9c0661AeDEA9b494b20604a7dF62AD7 Wallet2:0xE689E84497c4560596a5f888a053093DcDAEBd1D

4.1. *iPhone Analysis*

iOS 14.1 by Apple saves a variety of artifacts associated with apps. These artifacts can provide insight into how a user interacts with an app. As discussed in [47], it may be possible to determine how frequently and for how long a user interacts with an app by looking at information such as the user's screen time and activity time within the application. Furthermore, the iPhone has the ability to take a screenshot of the application window so that it can display it when the user uses the app switcher functionality (i.e., app moved to the background). These screenshots are stored as individual photos in the folder `<AppUUID>\Library\SplashBoard\Snapshots\sceneID:<AppPackageName>` [47]. For example, we found that the Metamask app does not use any empty or blurred image; however, it uses a screenshot taken from the main screen of the app. Figure 7 shows the screenshot taken by the app that shows the main page of wallet 1, and we were able to recover this screenshot from `Library\SplashBoard\Snapshots\sceneID:io.metamask.MetaMask-default\0F8FD8B0-B5DB-4B36-8381-BB8666CCA1D2@2x.jpeg`. Using the timestamp of the screenshot, we determine the amount of the first wallet at that time.



Account 1

$0.95

0xe5b5...B926

0.0029 BNB
$0.95

0 CAKE
$0.00

Figure 7. Screenshot snip-it that was taken by the iOS.

Furthermore, another identifier, used as deviceUID, was recovered for both apps within `\private\var\mobile\Library\AggregateDictionary` inside a file named `session_bundles.log`. Figure 8 shows the name of the app, version number and DeviceUID `CC8DC2B3-C872-4594-8665-AEA27ACBE346` for Trust Wallet and `70AA222F-76E3-4E0D-A91C-E5A20E13F340` Metamask.

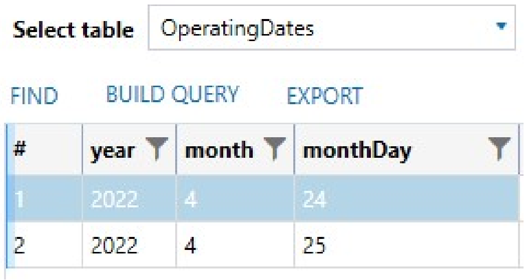
```
...
["com.apple.CryptoTokenKit.setoken",0,"00000000-0000-0000-0000-000000000000","","",""
  ,0,"",0,false,3]
["com.apple.Spotlight",0,"00000000-0000-0000-0000-000000000000","1","1.0","B949A2E1
  -0ECD-4631-80D7-419A0B8797BC",0,"",0,false,4]
["com.sixdays.trust",0,"00000000-0000-0000-0000-000000000000","640","7.6","CC8DC2B3
  -C872-4594-8665-AEA27ACBE346",1288339409,"10|date=1653422400000&sf=143441&pgtp
  =Search&pgid=300834cb-4d87-4923-9eb8-5457a8914463&prpg=Today_today&ctxt
  =Search&issrch=1",143441,false,5]
...
["io.metamask.MetaMask",0,"00000000-0000-0000-0000-000000000000","903","5.1.1"
  ,"70AA222F-76E3-4E0D-A91C-E5A20E13F340",1438144202,"10|date=1653422400000&sf
  =143441&pgtp=Software&pgid=1438144202&prpg=Search_fc7202cc-4c58-4899-9dd4
  -b8cfb5d8f4ad&ctxt=Search&issrch=1",143441,false,13]
```

Figure 8. The identifier called DeviceUID for both apps within session_bundles.log file.

4.1.1. Metamask

All Metamask-related files were located in the package `\private\var\mobile\Containers\Data\Application\81498DCE-4B2A-4322-B54B-F24EF002089F`, unless otherwise noted. We were able to recover the addresses of the two created wallet addresses from multiple locations and, most importantly, within the `\Library\ApplicationSupport\355io.metamask.MetaMask\RCTAsyncLocalStorage_V1\manifest.json` file. The deviceUID identifier was also recovered from the `\Library\Preferences\io.metamask.MetaMask.357plist` file. In general, the app's properties and preferences are stored in these properties list (plist) files.

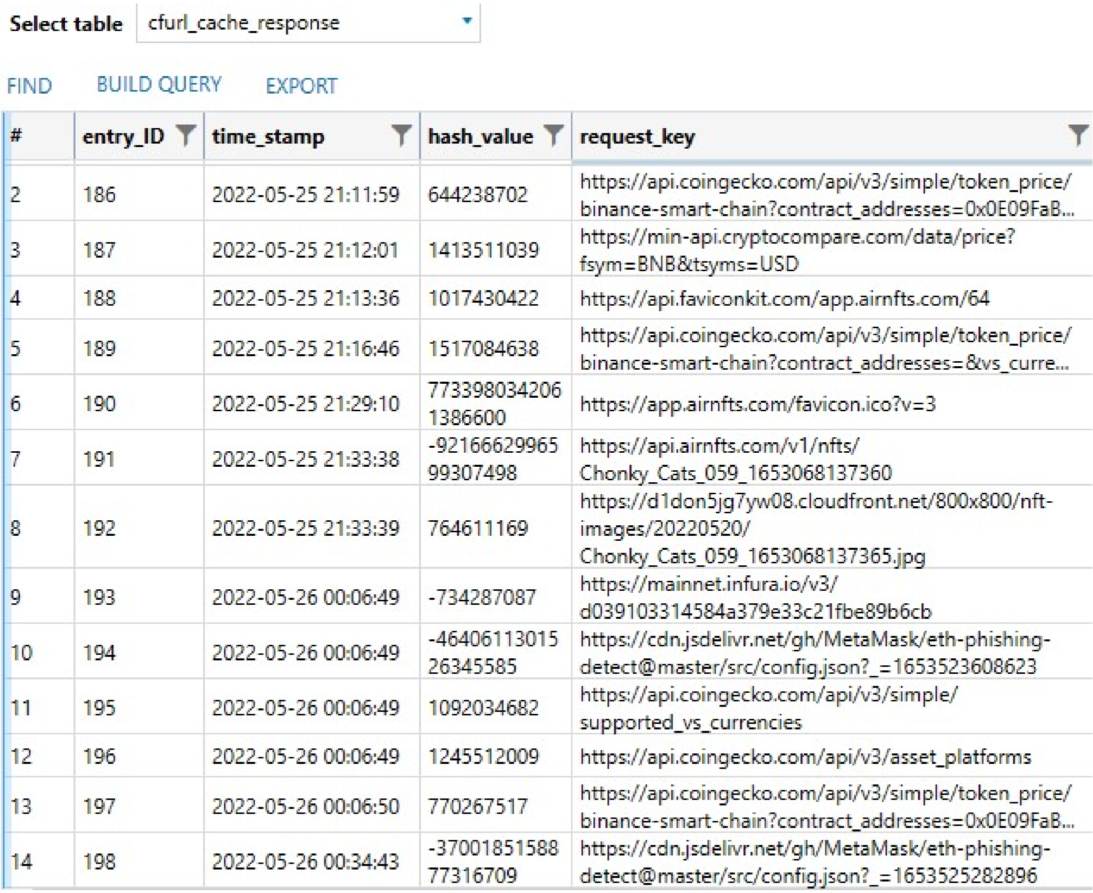
Additionally, we were able to recover a database with a table named `OperatingDates`, which shows the operating dates of the app. For the first forensic image we took, this table had only two entries, which are the dates of the first population (see Figure 9). The table `OperatingDates` is located within the `\Library\WebKit\WebsiteData\Resource\LoadStatistics\observations.db` database.



#	year	month	monthDay
1	2022	4	24
2	2022	4	25

Figure 9. Recovered operating dates of the app within the observations.db database.

Due to the fact that the app mainly uses https requests to receive data, most of the responses and received data cached were recovered in a database. The database called `Cache.db` is located in the `\Library\Cachesio.metamask.MetaMask` folder. It contains two very important tables named `cfurl_cache_response` and `cfurl_cache_receiver_data`. Figure 10 shows the contents of table `cfurl_cache_response` with its columns.



Select table cfurl_cache_response

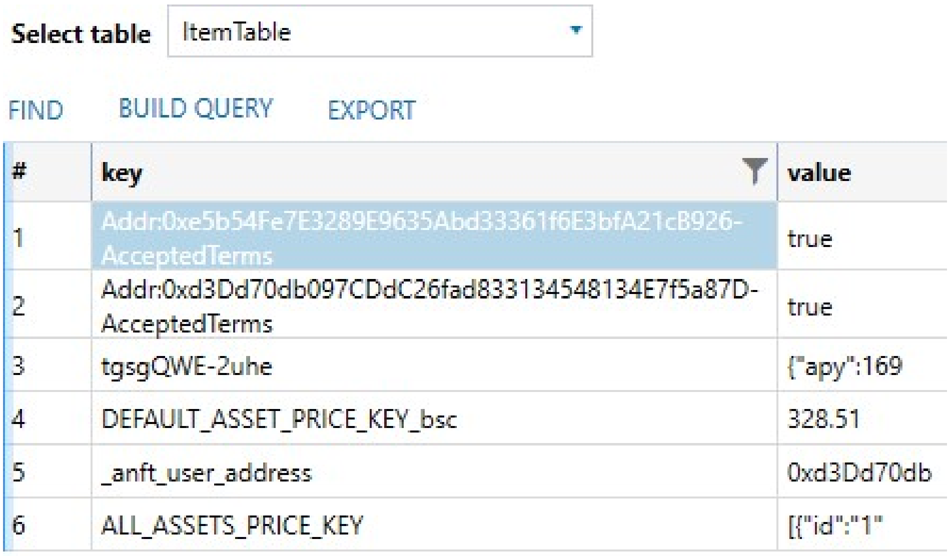
#	entry_ID	time_stamp	hash_value	request_key
2	186	2022-05-25 21:11:59	644238702	https://api.coingecko.com/api/v3/simple/token_price/binance-smart-chain?contract_addresses=0x0E09FaB...
3	187	2022-05-25 21:12:01	1413511039	https://min-api.cryptocompare.com/data/price?fsym=BNB&tsyms=USD
4	188	2022-05-25 21:13:36	1017430422	https://api.faviconkit.com/app.airnfts.com/64
5	189	2022-05-25 21:16:46	1517084638	https://api.coingecko.com/api/v3/simple/token_price/binance-smart-chain?contract_addresses=&vs_curre...
6	190	2022-05-25 21:29:10	7733980342061386600	https://app.airnfts.com/favicon.ico?v=3
7	191	2022-05-25 21:33:38	-9216662996599307498	https://api.airnfts.com/v1/nfts/Chonky_Cats_059_1653068137360
8	192	2022-05-25 21:33:39	764611169	https://d1don5jg7yw08.cloudfront.net/800x800/nft-images/20220520/Chonky_Cats_059_1653068137365.jpg
9	193	2022-05-26 00:06:49	-734287087	https://mainnet.infura.io/v3/d039103314584a379e33c21fbe89b6cb
10	194	2022-05-26 00:06:49	-4640611301526345585	https://cdn.jsdelivr.net/gh/MetaMask/eth-phishing-detect@master/src/config.json?_=1653523608623
11	195	2022-05-26 00:06:49	1092034682	https://api.coingecko.com/api/v3/simple/supported_vs_currencies
12	196	2022-05-26 00:06:49	1245512009	https://api.coingecko.com/api/v3/asset_platforms
13	197	2022-05-26 00:06:50	770267517	https://api.coingecko.com/api/v3/simple/token_price/binance-smart-chain?contract_addresses=0x0E09FaB...
14	198	2022-05-26 00:34:43	-3700185158877316709	https://cdn.jsdelivr.net/gh/MetaMask/eth-phishing-detect@master/src/config.json?_=1653525282896

Figure 10. Recovered content from the cfurl_cache_response table.

In addition, NFTs are purchased through NFT marketplaces such as Opensea, Rarible, and AirNFT. In our research, we used AirNFT (Available online: https://www.airnfts.com (accessed on 25 May 2022) in the scenarios. As a result, we were able to recover two account addresses that were used for the Airnft service and accepted the use terms stored in a table named `ItemTable` within the file `\Library\WebKit\WebsiteData\LocalStorage\https_app.airnfts.com_0.localstorage` (see Figure 11). This shows how important it is to investigate the local storage files that are kept for each service that the user uses in the app.

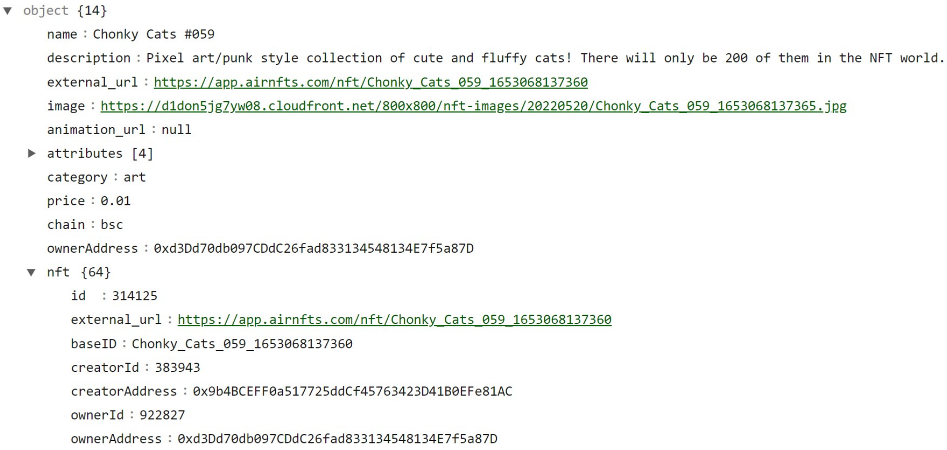
In the scenario, we purchased an NFT numbered *059* within the collection of *Chonky Cats*. We were able to find information (e.g., name, description, external_url, price, id, baseID, creatorAdress, and ownerAdress) about the NFT inside a file named 5A46EE9D-987E-42E8-A498-B401493E924E within the `\Library\Caches\io.metamask.MetaMask\fsCachedData\` path (see Figure 12 for all recovered information). Furthermore, this file contains other valuable information about the NFT attributes, a complete history of previous owners, the listing price, and its creator. For example, the country in which the account of the creator of NFT created the account was discovered within the file.

Furthermore, more information was recovered from the *com.apple.WebKit.Networking* layer within the app. The file named HSTS.plist within `\Library\Caches\com.apple.WebKit.Networking\` contains HTTP Strict Transport Security (HSTS), which is used mainly to aid in the prevention of attacks on websites, such as those using secure socket layer (SSL) stripping and man-in-the-middle tactic, by using a policy technique. (see Figure 13). This file can help determine the network services that were used by the user that created the storage sessions.



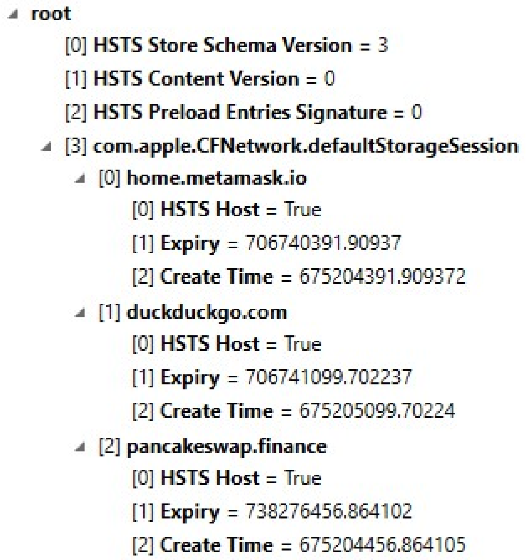
#	key	value
1	Addr:0xe5b54Fe7E3289E9635Abd33361f6E3bfA21cB926-AcceptedTerms	true
2	Addr:0xd3Dd70db097CDdC26fad833134548134E7f5a87D-AcceptedTerms	true
3	tgsgQWE-2uhe	{"apy":169
4	DEFAULT_ASSET_PRICE_KEY_bsc	328.51
5	_anft_user_address	0xd3Dd70db
6	ALL_ASSETS_PRICE_KEY	[{"id":"1"

Figure 11. AirNFT service recovered information, which shows two wallet addresses that have accepted the terms of use.



```
▼ object {14}
    name : Chonky Cats #059
    description : Pixel art/punk style collection of cute and fluffy cats! There will only be 200 of them in the NFT world.
    external_url : https://app.airnfts.com/nft/Chonky_Cats_059_1653068137360
    image : https://d1don5jg7yw08.cloudfront.net/800x800/nft-images/20220520/Chonky_Cats_059_1653068137365.jpg
    animation_url : null
  ▶ attributes [4]
    category : art
    price : 0.01
    chain : bsc
    ownerAddress : 0xd3Dd70db097CDdC26fad833134548134E7f5a87D
  ▼ nft {64}
      id  : 314125
      external_url : https://app.airnfts.com/nft/Chonky_Cats_059_1653068137360
      baseID : Chonky_Cats_059_1653068137360
      creatorId : 383943
      creatorAddress : 0x9b4BCEFF0a517725ddCf45763423D41B0EFe81AC
      ownerId : 922827
      ownerAddress : 0xd3Dd70db097CDdC26fad833134548134E7f5a87D
```

Figure 12. NFT information recovered.



```
◢ root
    [0] HSTS Store Schema Version = 3
    [1] HSTS Content Version = 0
    [2] HSTS Preload Entries Signature = 0
  ◢ [3] com.apple.CFNetwork.defaultStorageSession
    ◢ [0] home.metamask.io
        [0] HSTS Host = True
        [1] Expiry = 706740391.90937
        [2] Create Time = 675204391.909372
    ◢ [1] duckduckgo.com
        [0] HSTS Host = True
        [1] Expiry = 706741099.702237
        [2] Create Time = 675205099.70224
    ◢ [2] pancakeswap.finance
        [0] HSTS Host = True
        [1] Expiry = 738276456.864102
        [2] Create Time = 675204456.864105
```

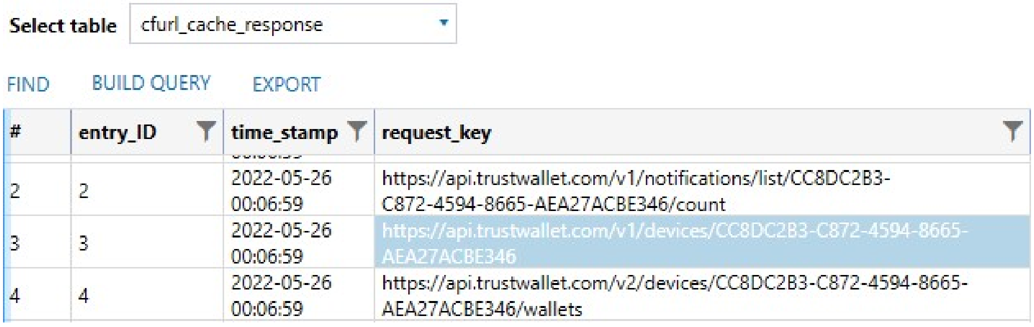
Figure 13. HSTS.plist file shows used services within the app.

Due to the use of the Pancakeswap service, which is used as a native decentralized exchange to the BNB chain, we were able to recover the account information for Pancakeswap within a file named `https_pancakeswap.finance_0.localstorage` within the `...\Library\WebKit\WebsiteData\LocalStorage` path.

4.1.2. Trust Wallet

All Trust Wallet-related files were located in package `\private\var\mobile\Containers\Data\Application\65BFA36C-A34F-4791-8BA9-E7AE9561A454`, unless otherwise noted.

The Trust Wallet app creates a database called *Cache.db* that stores a lot of information, and this database is sorted into the `\Library\Caches\com.sixdays.trust` folder. For example, tables named `cfurl_cache_response` and `cfurl_cache_response` store information-related responses to CFURL, where CFURL, according to the Apple Developer website [67], helps programs and apps that rely on URLs to access resources, such as local files. These tables were very useful for recovering the device ID that is needed to access the device wallets. Furthermore, within the table `cfurl_cache_response` we were able to recover the device ID used to create the wallets (see Figure 14). In addition, realm databases, a lightweight object-oriented cross-platform database developed by MongoDB [68] as an alternative to SQLite, were present in the app for wallets; however, they were all encrypted. They are stored in the `Documents\realm` folder. In Section 4.2.2, we explain more about these databases since the realm databases for wallets on Android were not encrypted.



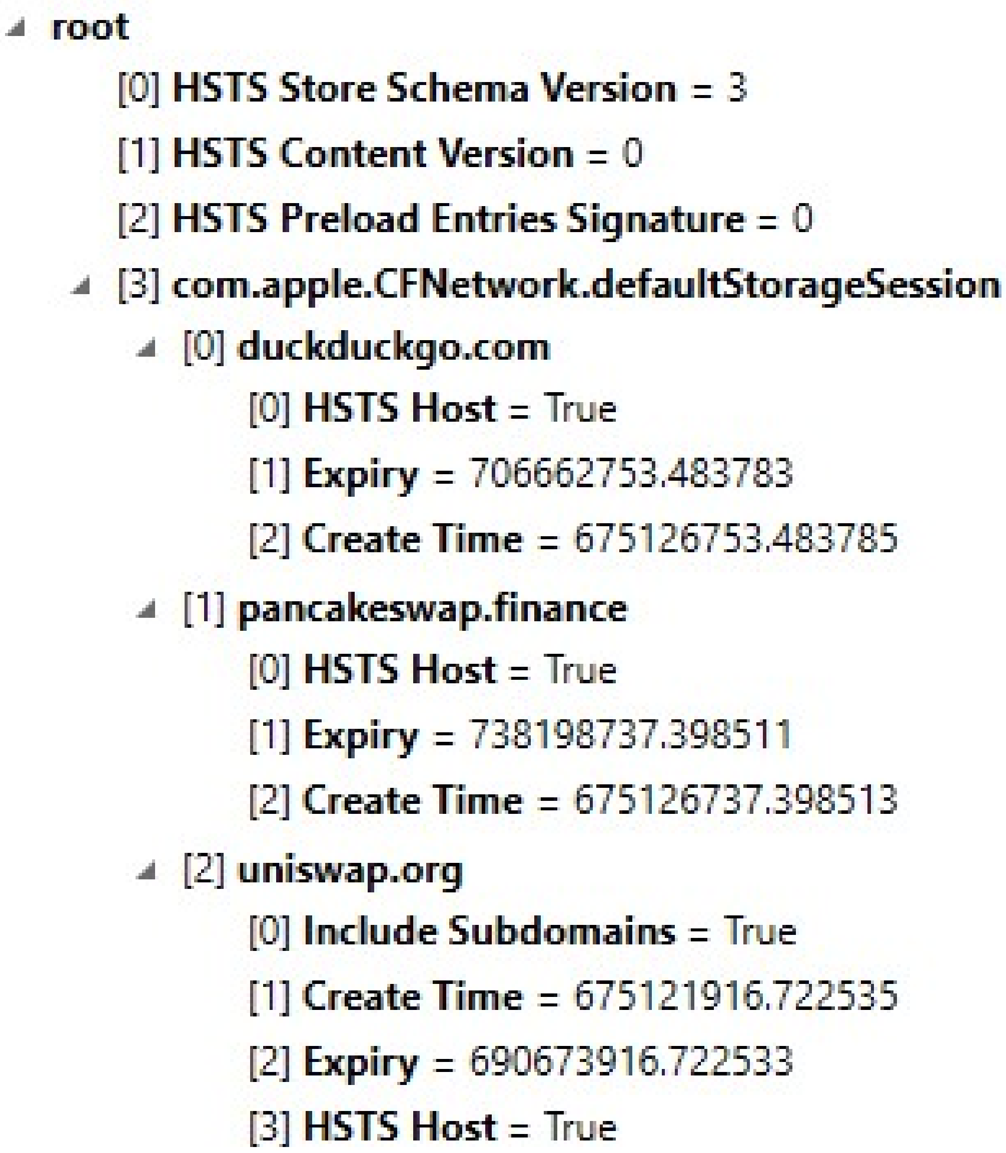
Select table: cfurl_cache_response

#	entry_ID	time_stamp	request_key
2	2	2022-05-26 00:06:59	https://api.trustwallet.com/v1/notifications/list/CC8DC2B3-C872-4594-8665-AEA27ACBE346/count
3	3	2022-05-26 00:06:59	https://api.trustwallet.com/v1/devices/CC8DC2B3-C872-4594-8665-AEA27ACBE346
4	4	2022-05-26 00:06:59	https://api.trustwallet.com/v2/devices/CC8DC2B3-C872-4594-8665-AEA27ACBE346/wallets

Figure 14. Trust Wallet device ID within one of the HTTPS requests.

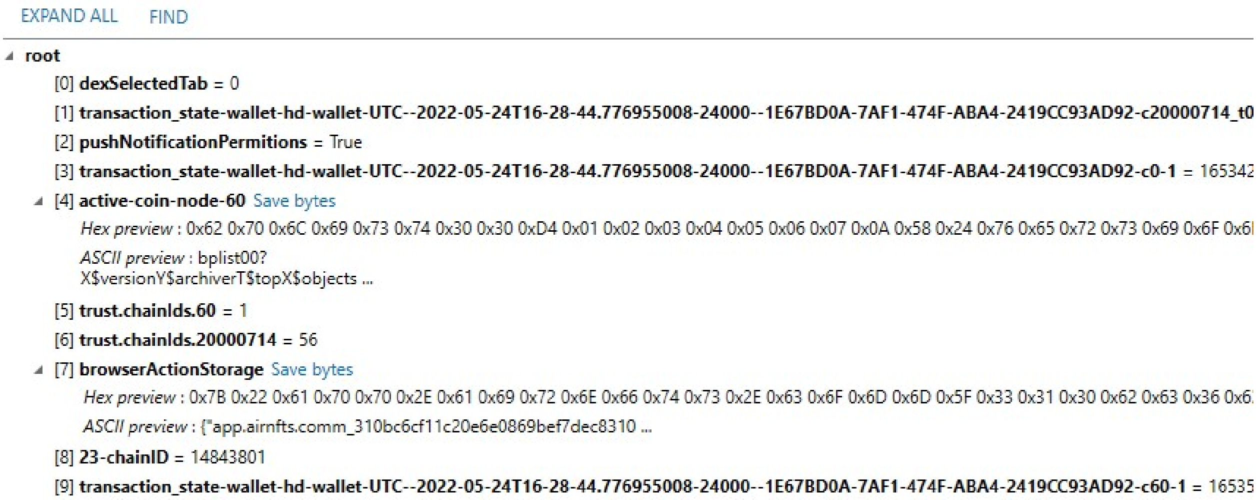
The folder `Library\Caches` contains many more crucial folders that contain important data for investigators. Furthermore, the folder named `com.onevcat.Kingfisher.ImageCache.default` contains all the cached images. The folder named `com.apple.WebKit.Networking` contains information about HSTS along with the creation time and the expiration time (see Figure 15 for an example of the HSTS.plist file). Moreover, the folder named `WebKit\Network\CacheVersion\16Blobs`, which is still in the folder `Caches`, contains blobs of all NFT images that were seen or cached by the phone.

After recovering the device ID used to create wallets and recover cached files, it is necessary to recover the transactions that occurred on the phone. The `\Library\Preferences\com.sixdays.trust.plist` file luckily contains preferences and information of the wallets that the user initiated using the device (see Figure 16). It is important to note that this plist file keeps a record of actions that were performed using the device; therefore, if the user was using another device, the information could be missing. Each recovered action is time-stamped using the UTC time.



```
◢ root
      [0] HSTS Store Schema Version = 3
      [1] HSTS Content Version = 0
      [2] HSTS Preload Entries Signature = 0
    ◢ [3] com.apple.CFNetwork.defaultStorageSession
        ◢ [0] duckduckgo.com
              [0] HSTS Host = True
              [1] Expiry = 706662753.483783
              [2] Create Time = 675126753.483785
        ◢ [1] pancakeswap.finance
              [0] HSTS Host = True
              [1] Expiry = 738198737.398511
              [2] Create Time = 675126737.398513
        ◢ [2] uniswap.org
              [0] Include Subdomains = True
              [1] Create Time = 675121916.722535
              [2] Expiry = 690673916.722533
              [3] HSTS Host = True
```

Figure 15. Example of the HSTS.plist file content.

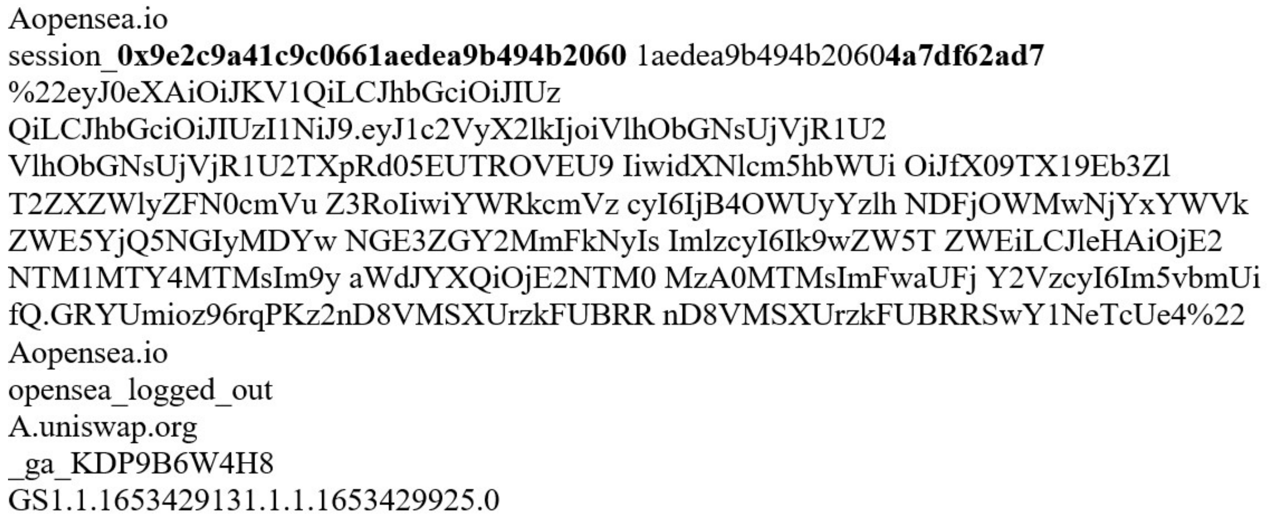


```
◢ root
    [0] dexSelectedTab = 0
    [1] transaction_state-wallet-hd-wallet-UTC--2022-05-24T16-28-44.776955008-24000--1E67BD0A-7AF1-474F-ABA4-2419CC93AD92-c20000714_t0
    [2] pushNotificationPermitions = True
    [3] transaction_state-wallet-hd-wallet-UTC--2022-05-24T16-28-44.776955008-24000--1E67BD0A-7AF1-474F-ABA4-2419CC93AD92-c0-1 = 165342
  ◢ [4] active-coin-node-60
        Hex preview : 0x62 0x70 0x6C 0x69 0x73 0x74 0x30 0x30 0xD4 0x01 0x02 0x03 0x04 0x05 0x06 0x07 0x0A 0x58 0x24 0x76 0x65 0x72 0x73 0x69 0x6F 0x6
        ASCII preview : bplist00?
        X$versionY$archiverT$topX$objects ...
    [5] trust.chainIds.60 = 1
    [6] trust.chainIds.20000714 = 56
  ◢ [7] browserActionStorage
        Hex preview : 0x7B 0x22 0x61 0x70 0x70 0x2E 0x61 0x69 0x72 0x6E 0x66 0x74 0x73 0x2E 0x63 0x6F 0x6D 0x6D 0x5F 0x33 0x31 0x30 0x62 0x63 0x36 0x6
        ASCII preview : {"app.airnfts.comm_310bc6cf11c20e6e0869bef7dec8310 ...
    [8] 23-chainID = 14843801
    [9] transaction_state-wallet-hd-wallet-UTC--2022-05-24T16-28-44.776955008-24000--1E67BD0A-7AF1-474F-ABA4-2419CC93AD92-c60-1 = 16535
```

Figure 16. The com.sixdays.trust.plist file that contains information of all transactions that happened on the device.

As highlighted in the scenarios covered in Figure 6, several services were used within the app. The file `Cookies.binarycookies` contains cookies and timestamps for the services visited, and this file is stored in the folder `Library\Cookies`. Figure 17 illustrates an example of a user-visit service (i.e., `OpenSea.io`) along with the session ID.

In the scenario, the AirNFT service was used to buy the NFT. Due to the fact that AirNFT is an online website service within the app, its data were recovered from the `Library\WebKit\WebsiteData` folder. This folder contains a subfolder named `LocalStorage`, which stores local information about user web sessions. The file `https_app.airnfts.com_0.localstorage` stores the AirNFT user ID (`0xE689E84497c4560596a5f888a053093DcDAEBd1D`), which confirms that it was used and that the user has logged into the service. This information can allow the investigator to link other online services, such as AirNFT accounts, with the device user. Furthermore, another service was used in the scenario, pancake swap, and information about this can be recovered from the file `https_pancakeswap.finance_0.localstorage-wal` within the folder `LocalStorage`. In the scenario, a 0.0148 BNB was swapped for 1 CAKE using the first wallet, and this information is recovered with the `https_pancakeswap.finance_0.localstorage-wal` file. In addition, other locally stored information can be found for other websites, such as opensea (within the file `https_opensea.io_0.localstorage`).

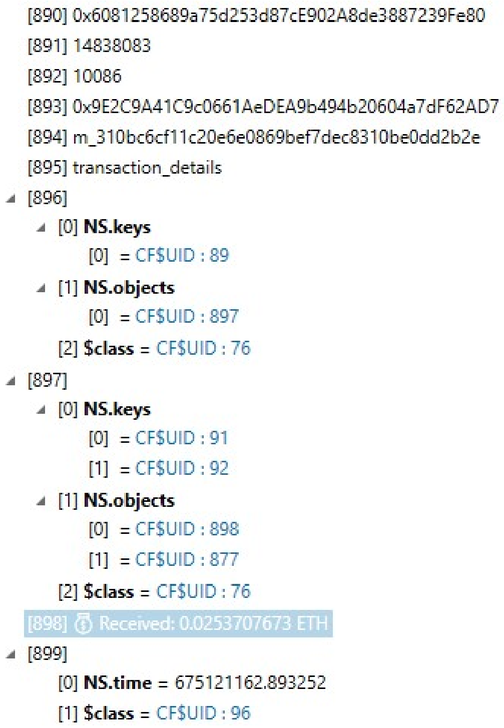


```
Aopensea.io
session_0x9e2c9a41c9c0661aedea9b494b2060 1aedea9b494b20604a7df62ad7
%22eyJ0eXAiOiJKV1QiLCJhbGciOiJIUz
QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoiVlhObGNsUjVjR1U2
VlhObGNsUjVjR1U2TXpRd05EUTROVEU9 IiwidXNlcm5hbWUi OiJfX09TX19Eb3Zl
T2ZXZWlyZFN0cmVu Z3RoIiwiYWRkcmVz cyI6IjB4OWUyYzlh NDFjOWMwNjYxYWVk
ZWE5YjQ5NGIyMDYw NGE3ZGY2MmFkNyIs ImlzcyI6Ik9wZW5T ZWEiLCJleHAiOjE2
NTM1MTY4MTMsIm9y aWdJYXQiOjE2NTM0 MzA0MTMsImFwaUFj Y2VzcyI6Im5vbmUi
fQ.GRYUmioz96rqPKz2nD8VMSXUrzkFUBRR nD8VMSXUrzkFUBRRSwY1NeTcUe4%22
Aopensea.io
opensea_logged_out
A.uniswap.org
_ga_KDP9B6W4H8
GS1.1.1653429131.1.1.1653429925.0
```

Figure 17. OpenSea.io Session ID using the **wallet address**, showing that the user has used this services sometime.

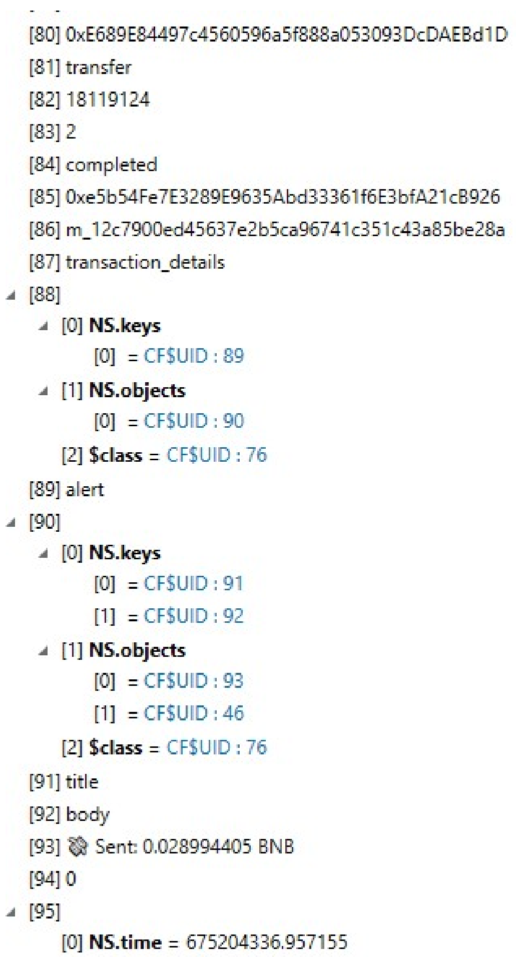
An interesting table named `OperatingDates` inside a database named `observations.db` is located in the `WebKit\WebsiteData\ResourceLoadStatistics` folder, containing information that shows the days the user accesses the web interface in the app. There is another table named `ObservedDomains` within the same database that holds information about user-resent interactions with web domains within the app, along with the timestamps of the most resent user interaction.

The notifications that were shown on the iPhone were recovered within a file named `DeliveredNotifications.plist` that is stored in `private\var\mobile\Library\UserNotifications\26CA2BEC-EDCC-4B75-B781-2D90DB3AF426`. Figure 18 shows the amount in ETH that was received from the Robinhood wallet, which was sent to the iOS trust wallet. Another notification can be seen in Figure 19, but this time it is a transaction of a BNB transfer initiated by the user.



```
     [890] 0x6081258689a75d253d87cE902A8de3887239Fe80
     [891] 14838083
     [892] 10086
     [893] 0x9E2C9A41C9c0661AeDEA9b494b20604a7dF62AD7
     [894] m_310bc6cf11c20e6e0869bef7dec8310be0dd2b2e
     [895] transaction_details
  ◢  [896]
       ◢  [0] NS.keys
                [0]  = CF$UID : 89
       ◢  [1] NS.objects
                [0]  = CF$UID : 897
          [2] $class = CF$UID : 76
  ◢  [897]
       ◢  [0] NS.keys
                [0]  = CF$UID : 91
                [1]  = CF$UID : 92
       ◢  [1] NS.objects
                [0]  = CF$UID : 898
                [1]  = CF$UID : 877
          [2] $class = CF$UID : 76
     [898] Received: 0.0253707673 ETH
  ◢  [899]
          [0] NS.time = 675121162.893252
          [1] $class = CF$UID : 96
```

Figure 18. The 0.0253707673 ETH that was received from the Robinhood wallet.



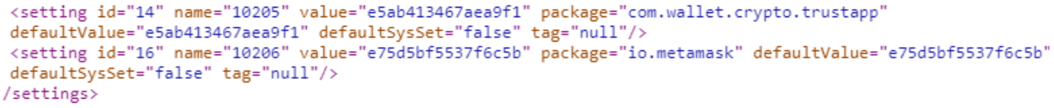
```
     [80] 0xE689E84497c4560596a5f888a053093DcDAEBd1D
     [81] transfer
     [82] 18119124
     [83] 2
     [84] completed
     [85] 0xe5b54Fe7E3289E9635Abd33361f6E3bfA21cB926
     [86] m_12c7900ed45637e2b5ca96741c351c43a85be28a
     [87] transaction_details
  ◢  [88]
       ◢  [0] NS.keys
                [0]  = CF$UID : 89
       ◢  [1] NS.objects
                [0]  = CF$UID : 90
          [2] $class = CF$UID : 76
     [89] alert
  ◢  [90]
       ◢  [0] NS.keys
                [0]  = CF$UID : 91
                [1]  = CF$UID : 92
       ◢  [1] NS.objects
                [0]  = CF$UID : 93
                [1]  = CF$UID : 46
          [2] $class = CF$UID : 76
     [91] title
     [92] body
     [93] Sent: 0.028994405 BNB
     [94] 0
  ◢  [95]
          [0] NS.time = 675204336.957155
```

Figure 19. Notification showing the transaction of a BNB transfer initiated by the user.

4.2. Android Analysis

In the course of our investigation, we followed the specified process and analyzed the data left behind by the two mobile apps running on an Android 10 smartphone.

The DeviceIDs of the Trust Wallet and Metamask apps can be found in the `system\users\0\settings_ssaid.xml` file. Figure 20 shows the recovery of the ssaid(s) that are used as DeviceIDs for both the Trust Wallet and Metamask apps found in the file `settings_ssaid.xml`. The importance of these DeviceIDs comes from the ability to use them to recover other wallets that have previously been associated with the device. However, if the device is set to factory reset, these ID numbers change. They can also be used to verify the wallet with the device because the investigator can obtain the device model from the API response.

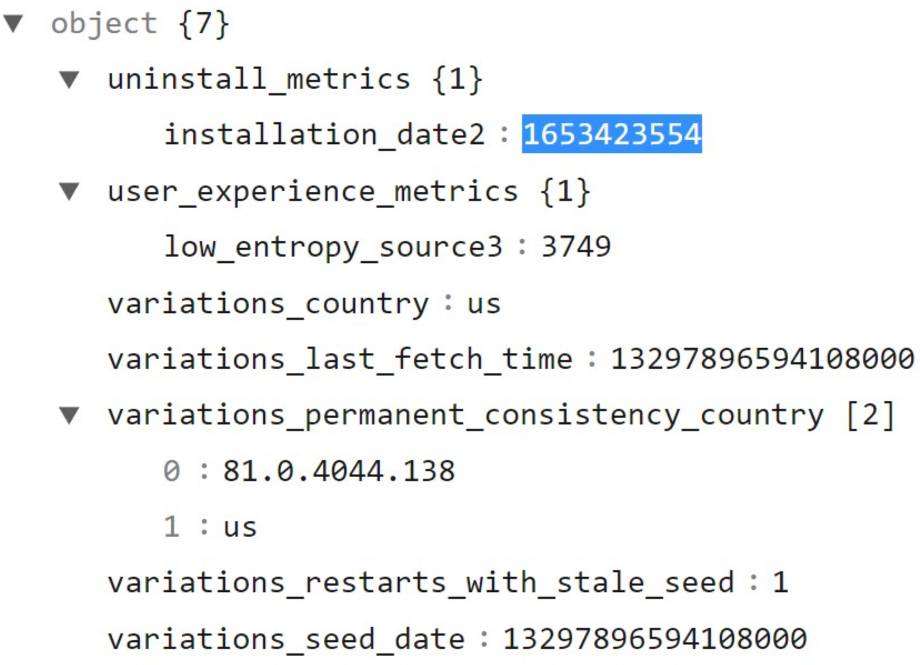


```
 <setting id="14" name="10205" value="e5ab413467aea9f1" package="com.wallet.crypto.trustapp"
 defaultValue="e5ab413467aea9f1" defaultSysSet="false" tag="null"/>
 <setting id="16" name="10206" value="e75d5bf5537f6c5b" package="io.metamask" defaultValue="e75d5bf5537f6c5b"
 defaultSysSet="false" tag="null"/>
/settings>
```

Figure 20. Recovered ssaid(s) for both apps.

4.2.1. Metamask

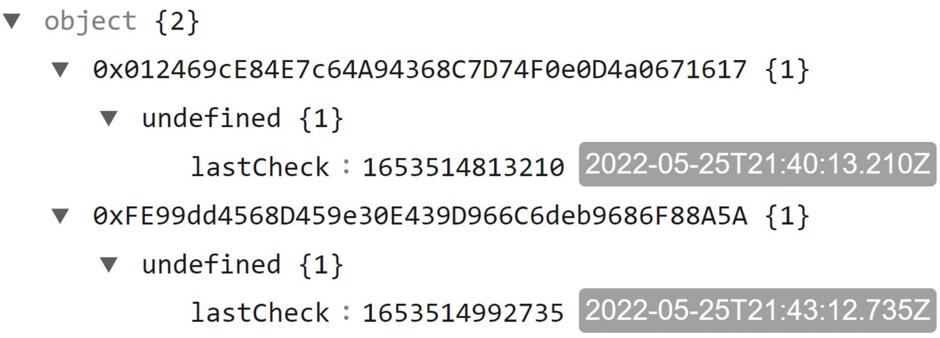
All files related to the Android Metamask app were found in package `\data\io.metamask`, unless otherwise noted. The file named `pref_store` that is stored in the folder `\app_webview` contains the timestamp of the installation of the app (see Figure 21).



```
▼ object {7}
    ▼ uninstall_metrics {1}
          installation_date2 : 1653423554
    ▼ user_experience_metrics {1}
          low_entropy_source3 : 3749
      variations_country : us
      variations_last_fetch_time : 13297896594108000
    ▼ variations_permanent_consistency_country [2]
          0 : 81.0.4044.138
          1 : us
      variations_restarts_with_stale_seed : 1
      variations_seed_date : 13297896594108000
```

Figure 21. App installation timestamp.

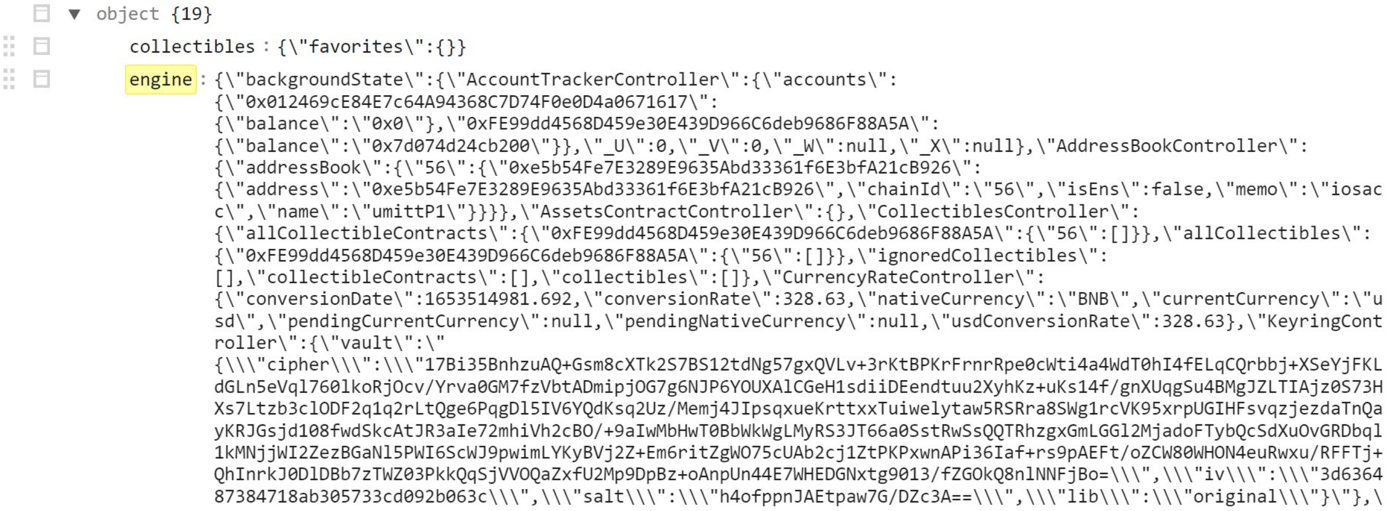
The row *@MetaMask:walletconnectSessions* within the table named *catalystLocalStorage* within the SQLite3 file named *RKStorage* in the path `\databases` contains the user-connected wallet addresses (see Figure 22). The same information can be found in the `\files\persistStore\persist-root` JSON file.



```
▼ object {2}
    ▼ 0x012469cE84E7c64A94368C7D74F0e0D4a0671617 {1}
        ▼ undefined {1}
            lastCheck : 1653514813210 2022-05-25T21:40:13.210Z
    ▼ 0xFE99dd4568D459e30E439D966C6deb9686F88A5A {1}
        ▼ undefined {1}
            lastCheck : 1653514992735 2022-05-25T21:43:12.735Z
```

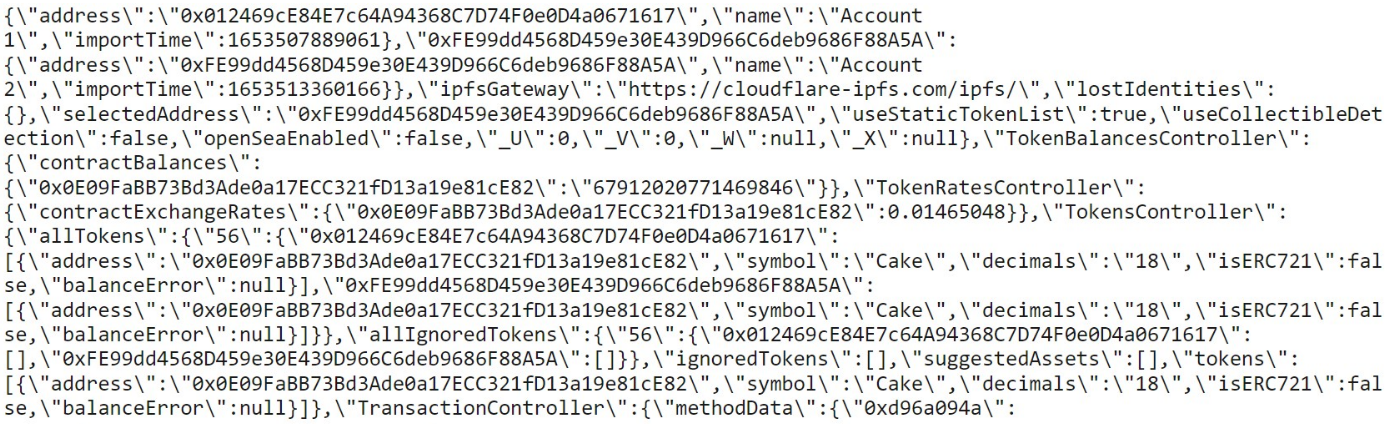
Figure 22. The value recovered from the row (i.e., @MetaMask:lastIncomingTxBlockInfo) that contains the user-connected wallets addresses and last time they were checked.

Furthermore, the `persist-root` JSON file contains 19 objects that hold many valuable information. The addresses of the wallets on the app, balances, contacts, collectibles, and cipher are examples of what can be recovered from the engine object within the JSON `persist-root` file (see Figure 23). Moreover, the Metamask app allows the user to store contacts which can be seen in *addressBook* in Figure 23). Other information on user accounts and when they were imported into the device can be recovered within the engine object inside the file `persist-root` (see Figure 24).



```
□ ▼ object {19}
□       collectibles : {\"favorites\":{}}
□       engine : {\"backgroundState\":{\"AccountTrackerController\":{\"accounts\":
                 {\"0x012469cE84E7c64A94368C7D74F0e0D4a0671617\":
                 {\"balance\":\"0x0\"},\"0xFE99dd4568D459e30E439D966C6deb9686F88A5A\":
                 {\"balance\":\"0x7d074d24cb200\"}},\"_U\":0,\"_V\":0,\"_W\":null,\"_X\":null},\"AddressBookController\":
                 {\"addressBook\":{\"56\":{\"0xe5b54Fe7E3289E9635Abd33361f6E3bfA21cB926\":
                 {\"address\":\"0xe5b54Fe7E3289E9635Abd33361f6E3bfA21cB926\",\"chainId\":\"56\",\"isEns\":false,\"memo\":\"iosac
                 c\",\"name\":\"umittP1\"}}}},\"AssetsContractController\":{},\"CollectiblesController\":
                 {\"allCollectibleContracts\":{\"0xFE99dd4568D459e30E439D966C6deb9686F88A5A\":{\"56\":[]}},\"allCollectibles\":
                 {\"0xFE99dd4568D459e30E439D966C6deb9686F88A5A\":{\"56\":[]}},\"ignoredCollectibles\":
                 [],\"collectibleContracts\":[],\"collectibles\":[]},\"CurrencyRateController\":
                 {\"conversionDate\":1653514981.692,\"conversionRate\":328.63,\"nativeCurrency\":\"BNB\",\"currentCurrency\":\"u
                 sd\",\"pendingCurrentCurrency\":null,\"pendingNativeCurrency\":null,\"usdConversionRate\":328.63},\"KeyringCont
                 roller\":{\"vault\":\"
                 {\\\"cipher\\\":\\\"17Bi35BnhzuAQ+Gsm8cXTk2S7BS12tdNg57gxQVLv+3rKtBPKrFrnrRpe0cWti4a4WdT0hI4fELqCQrbbj+XSeYjFKL
                 dGLn5eVql760lkoRjOcv/Yrva0GM7fzVbtADmipjOG7g6NJP6YOUXAlCGeH1sdiiDEendtuu2XyhKz+uKs14f/gnXUqgSu4BMgJZLTIAjz0S73H
                 Xs7Ltzb3clODF2q1q2rLtQge6PqgDl5IV6YQdKsq2Uz/Memj4JIpsqxueKrttxxTuiwelytaw5RSRra8SWg1rcVK95xrpUGIHFsvqzjezdaTnQa
                 yKRJGsjd108fwdSkcAtJR3aIe72mhiVh2cBO/+9aIwMbHwT0BbWkWgLMyRS3JT66a0SstRwSsQQTRhzgxGmLGGl2MjadoFTybQcSdXuOvGRDbql
                 1kMNjjWI2ZezBGaNl5PWI6ScWJ9pwimLYKyBVj2Z+Em6ritZgWO75cUAb2cj1ZtPKPxwnAPi36Iaf+rs9pAEFt/oZCW80WHON4euRwxu/RFFTj+
                 QhInrkJ0DlDBb7zTWZ03PkkQqSjVVOQaZxfU2Mp9DpBz+oAnpUn44E7WHEDGNxtg9013/fZGOkQ8nlNNFjBo=\\\",\\\"iv\\\":\\\"3d6364
                 87384718ab305733cd092b063c\\\",\\\"salt\\\":\\\"h4ofppnJAEtpaw7G/DZc3A==\\\",\\\"lib\\\":\\\"original\\\"}\"},\
```

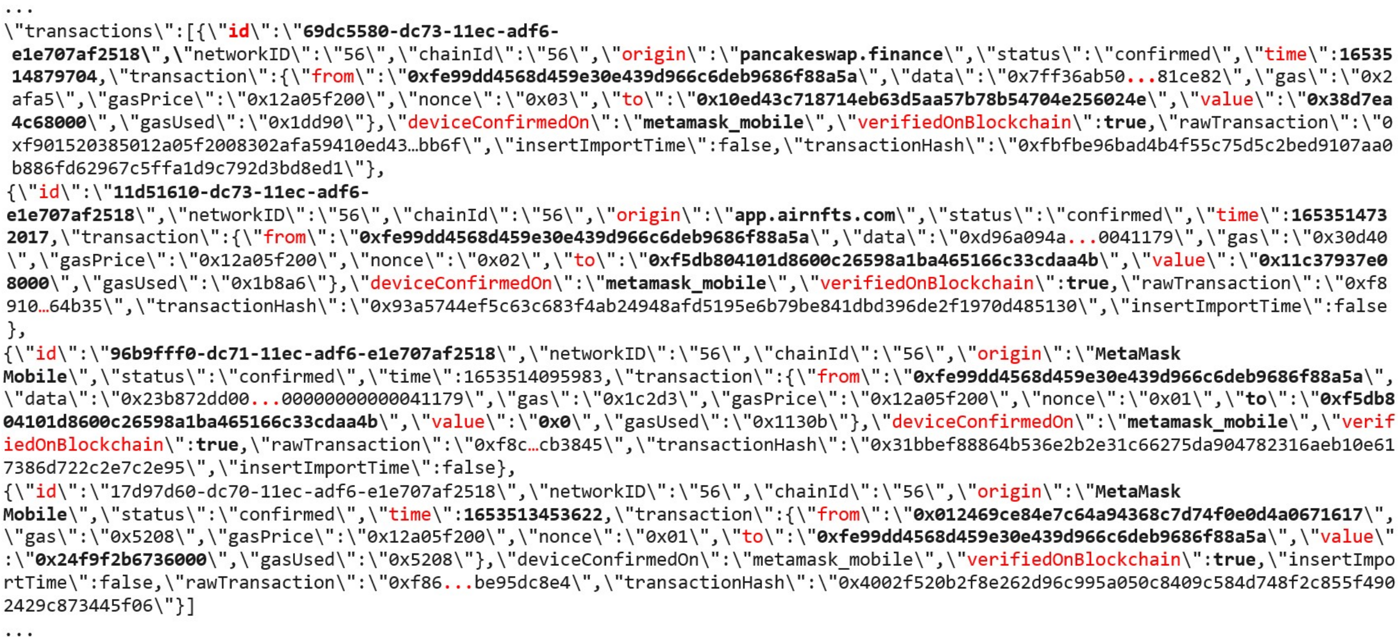
Figure 23. The persist-root file that contains valuable information, this Figure show the two wallets addresses, contact address, collectibles, and cipher.



```
{\"address\":\"0x012469cE84E7c64A94368C7D74F0e0D4a0671617\",\"name\":\"Account
1\",\"importTime\":1653507889061},\"0xFE99dd4568D459e30E439D966C6deb9686F88A5A\":
{\"address\":\"0xFE99dd4568D459e30E439D966C6deb9686F88A5A\",\"name\":\"Account
2\",\"importTime\":1653513360166}},\"ipfsGateway\":\"https://cloudflare-ipfs.com/ipfs/\",\"lostIdentities\":
{},\"selectedAddress\":\"0xFE99dd4568D459e30E439D966C6deb9686F88A5A\",\"useStaticTokenList\":true,\"useCollectibleDet
ection\":false,\"openSeaEnabled\":false,\"_U\":0,\"_V\":0,\"_W\":null,\"_X\":null},\"TokenBalancesController\":
{\"contractBalances\":
{\"0x0E09FaBB73Bd3Ade0a17ECC321fD13a19e81cE82\":\"67912020771469846\"}},\"TokenRatesController\":
{\"contractExchangeRates\":{\"0x0E09FaBB73Bd3Ade0a17ECC321fD13a19e81cE82\":0.01465048}},\"TokensController\":
{\"allTokens\":{\"56\":{\"0x012469cE84E7c64A94368C7D74F0e0D4a0671617\":
[{\"address\":\"0x0E09FaBB73Bd3Ade0a17ECC321fD13a19e81cE82\",\"symbol\":\"Cake\",\"decimals\":\"18\",\"isERC721\":fal
se,\"balanceError\":null}],\"0xFE99dd4568D459e30E439D966C6deb9686F88A5A\":
[{\"address\":\"0x0E09FaBB73Bd3Ade0a17ECC321fD13a19e81cE82\",\"symbol\":\"Cake\",\"decimals\":\"18\",\"isERC721\":fal
se,\"balanceError\":null}]}},\"allIgnoredTokens\":{\"56\":{\"0x012469cE84E7c64A94368C7D74F0e0D4a0671617\":
[],\"0xFE99dd4568D459e30E439D966C6deb9686F88A5A\":[]}},\"ignoredTokens\":[],\"suggestedAssets\":[],\"tokens\":
[{\"address\":\"0x0E09FaBB73Bd3Ade0a17ECC321fD13a19e81cE82\",\"symbol\":\"Cake\",\"decimals\":\"18\",\"isERC721\":fal
se,\"balanceError\":null}]},\"TransactionController\":{\"methodData\":{\"0xd96a094a\":
```

Figure 24. The persist-root file that contains valuable information; in this Figure we can see the wallets import times, contract exchange rates, and assets.

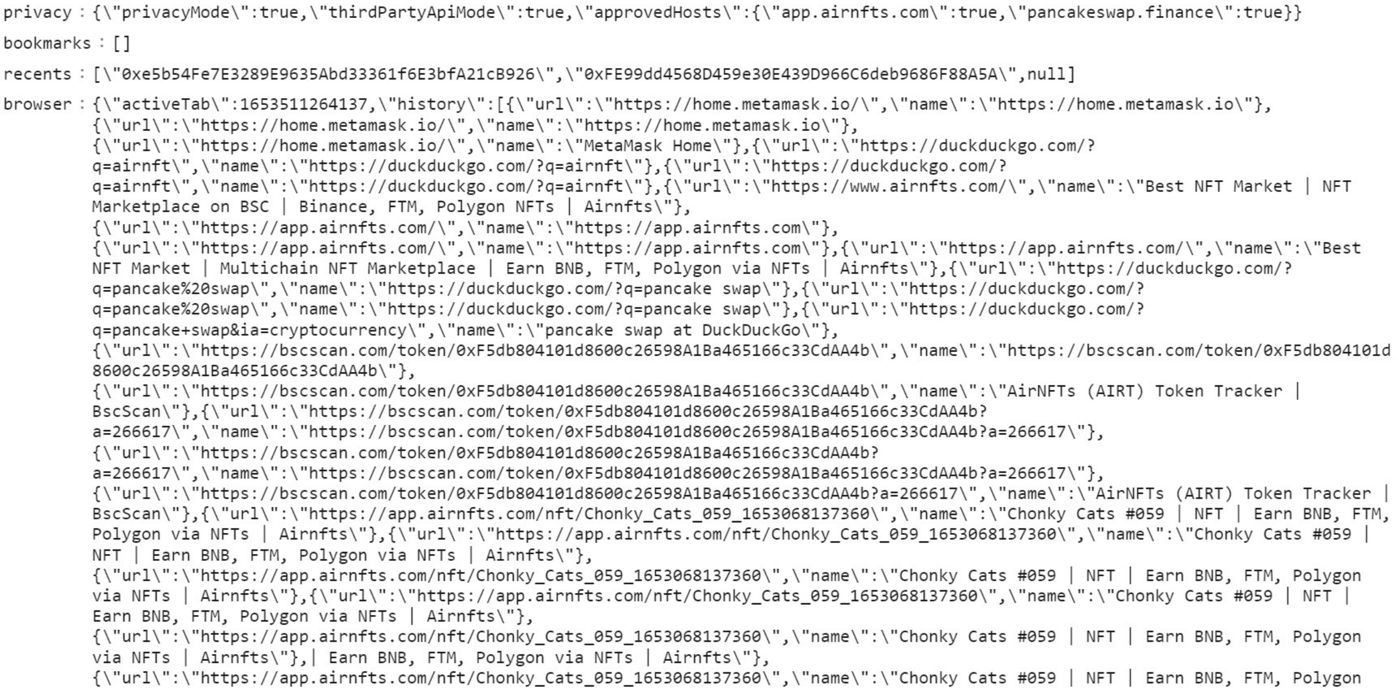
In addition, the file also stores the transactions that the user initiated using the devices in descending order, and they can be seen in Figure 25. The first shows the swapping of the BNB to Cake, the second shows the purchase of the NFT, the third shows the sending of the NFT, and the last shows the transfer of money from the first wallet to the second (see Figure 25).



```
...
\"transactions\":[{\"id\":\"69dc5580-dc73-11ec-adf6-
 e1e707af2518\",\"networkID\":\"56\",\"chainId\":\"56\",\"origin\":\"pancakeswap.finance\",\"status\":\"confirmed\",\"time\":16535
 14879704,\"transaction\":{\"from\":\"0xfe99dd4568d459e30e439d966c6deb9686f88a5a\",\"data\":\"0x7ff36ab50...81ce82\",\"gas\":\"0x2
 afa5\",\"gasPrice\":\"0x12a05f200\",\"nonce\":\"0x03\",\"to\":\"0x10ed43c718714eb63d5aa57b78b54704e256024e\",\"value\":\"0x38d7ea
 4c68000\",\"gasUsed\":\"0x1dd90\"},\"deviceConfirmedOn\":\"metamask_mobile\",\"verifiedOnBlockchain\":true,\"rawTransaction\":\"0
 xf901520385012a05f2008302afa59410ed43…bb6f\",\"insertImportTime\":false,\"transactionHash\":\"0xfbfbe96bad4b4f55c75d5c2bed9107aa0
 b886fd62967c5ffa1d9c792d3bd8ed1\"},
 {\"id\":\"11d51610-dc73-11ec-adf6-
e1e707af2518\",\"networkID\":\"56\",\"chainId\":\"56\",\"origin\":\"app.airnfts.com\",\"status\":\"confirmed\",\"time\":165351473
2017,\"transaction\":{\"from\":\"0xfe99dd4568d459e30e439d966c6deb9686f88a5a\",\"data\":\"0xd96a094a...0041179\",\"gas\":\"0x30d40
\",\"gasPrice\":\"0x12a05f200\",\"nonce\":\"0x02\",\"to\":\"0xf5db804101d8600c26598a1ba465166c33cdaa4b\",\"value\":\"0x11c37937e0
8000\",\"gasUsed\":\"0x1b8a6\"},\"deviceConfirmedOn\":\"metamask_mobile\",\"verifiedOnBlockchain\":true,\"rawTransaction\":\"0xf8
910…64b35\",\"transactionHash\":\"0x93a5744ef5c63c683f4ab24948afd5195e6b79be841dbd396de2f1970d485130\",\"insertImportTime\":false
},
{\"id\":\"96b9fff0-dc71-11ec-adf6-e1e707af2518\",\"networkID\":\"56\",\"chainId\":\"56\",\"origin\":\"MetaMask
Mobile\",\"status\":\"confirmed\",\"time\":1653514095983,\"transaction\":{\"from\":\"0xfe99dd4568d459e30e439d966c6deb9686f88a5a\",
\"data\":\"0x23b872dd00...00000000000041179\",\"gas\":\"0x1c2d3\",\"gasPrice\":\"0x12a05f200\",\"nonce\":\"0x01\",\"to\":\"0xf5db8
04101d8600c26598a1ba465166c33cdaa4b\",\"value\":\"0x0\",\"gasUsed\":\"0x1130b\"},\"deviceConfirmedOn\":\"metamask_mobile\",\"verif
iedOnBlockchain\":true,\"rawTransaction\":\"0xf8c…cb3845\",\"transactionHash\":\"0x31bbef88864b536e2b2e31c66275da904782316aeb10e61
7386d722c2e7c2e95\",\"insertImportTime\":false},
{\"id\":\"17d97d60-dc70-11ec-adf6-e1e707af2518\",\"networkID\":\"56\",\"chainId\":\"56\",\"origin\":\"MetaMask
Mobile\",\"status\":\"confirmed\",\"time\":1653513453622,\"transaction\":{\"from\":\"0x012469ce84e7c64a94368c7d74f0e0d4a0671617\",
\"gas\":\"0x5208\",\"gasPrice\":\"0x12a05f200\",\"nonce\":\"0x01\",\"to\":\"0xfe99dd4568d459e30e439d966c6deb9686f88a5a\",\"value\"
:\"0x24f9f2b6736000\",\"gasUsed\":\"0x5208\"},\"deviceConfirmedOn\":\"metamask_mobile\",\"verifiedOnBlockchain\":true,\"insertImpo
rtTime\":false,\"rawTransaction\":\"0xf86...be95dc8e4\",\"transactionHash\":\"0x4002f520b2f8e262d96c995a050c8409c584d748f2c855f490
2429c873445f06\"}]
...
```

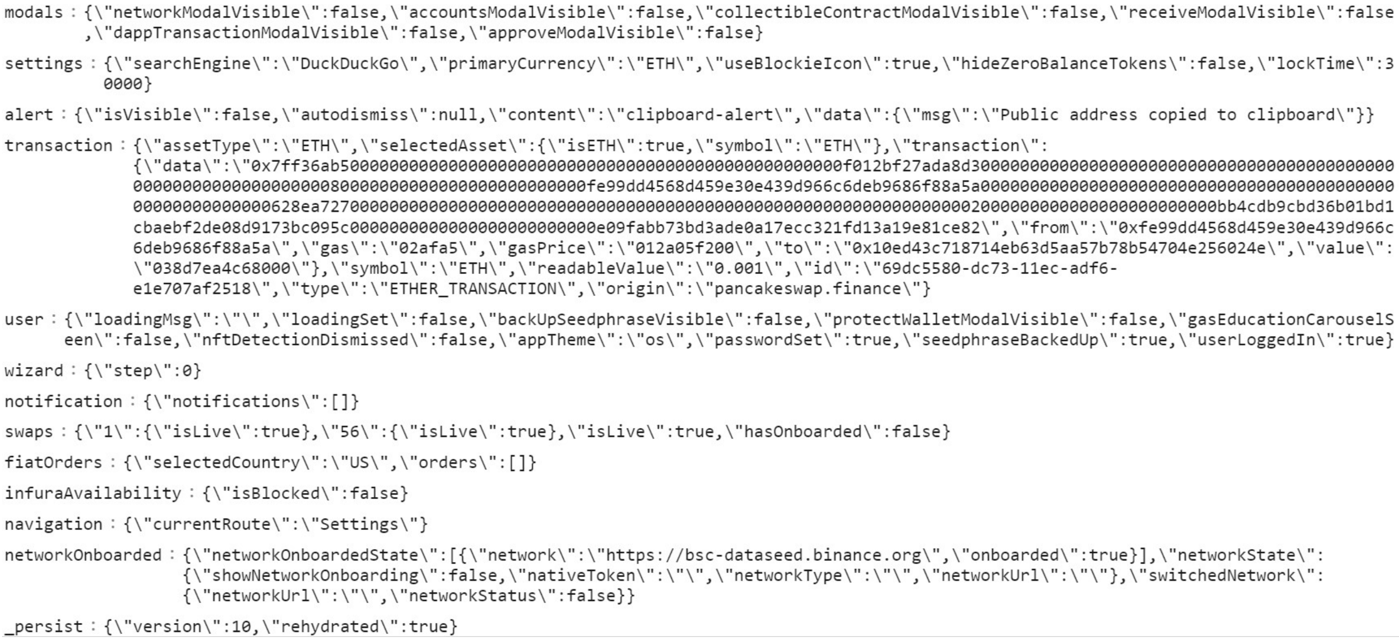
Figure 25. Recovered transactions that happened within the device (last is showing first).

Privacy settings (shows approved services), bookmarks, resents, and browser are other important objects in the `persist-root` JSON file (see Figure 26). The complete history of user activity (e.g., sites visited and search keywords) in the app can be recovered from the browser object. Other objects such as settings, alert, and the default fiat currency can be recovered (see Figure 27).



```
privacy : {\"privacyMode\":true,\"thirdPartyApiMode\":true,\"approvedHosts\":{\"app.airnfts.com\":true,\"pancakeswap.finance\":true}}

bookmarks : []

recents : [\"0xe5b54Fe7E3289E9635Abd33361f6E3bfA21cB926\",\"0xFE99dd4568D459e30E439D966C6deb9686F88A5A\",null]

browser : {\"activeTab\":1653511264137,\"history\":[{\"url\":\"https://home.metamask.io/\",\"name\":\"https://home.metamask.io\"},
          {\"url\":\"https://home.metamask.io/\",\"name\":\"https://home.metamask.io\"},
          {\"url\":\"https://home.metamask.io/\",\"name\":\"MetaMask Home\"},{\"url\":\"https://duckduckgo.com/?
          q=airnft\",\"name\":\"https://duckduckgo.com/?q=airnft\"},{\"url\":\"https://duckduckgo.com/?
          q=airnft\",\"name\":\"https://duckduckgo.com/?q=airnft\"},{\"url\":\"https://www.airnfts.com/\",\"name\":\"Best NFT Market | NFT
          Marketplace on BSC | Binance, FTM, Polygon NFTs | Airnfts\"},
          {\"url\":\"https://app.airnfts.com/\",\"name\":\"https://app.airnfts.com\"},
          {\"url\":\"https://app.airnfts.com/\",\"name\":\"https://app.airnfts.com\"},{\"url\":\"https://app.airnfts.com/\",\"name\":\"Best
          NFT Market | Multichain NFT Marketplace | Earn BNB, FTM, Polygon via NFTs | Airnfts\"},{\"url\":\"https://duckduckgo.com/?
          q=pancake%20swap\",\"name\":\"https://duckduckgo.com/?q=pancake swap\"},{\"url\":\"https://duckduckgo.com/?
          q=pancake%20swap\",\"name\":\"https://duckduckgo.com/?q=pancake swap\"},{\"url\":\"https://duckduckgo.com/?
          q=pancake+swap&ia=cryptocurrency\",\"name\":\"pancake swap at DuckDuckGo\"},
          {\"url\":\"https://bscscan.com/token/0xF5db804101d8600c26598A1Ba465166c33CdAA4b\",\"name\":\"https://bscscan.com/token/0xF5db804101d
          8600c26598A1Ba465166c33CdAA4b\"},
          {\"url\":\"https://bscscan.com/token/0xF5db804101d8600c26598A1Ba465166c33CdAA4b\",\"name\":\"AirNFTs (AIRT) Token Tracker |
          BscScan\"},{\"url\":\"https://bscscan.com/token/0xF5db804101d8600c26598A1Ba465166c33CdAA4b?
          a=266617\",\"name\":\"https://bscscan.com/token/0xF5db804101d8600c26598A1Ba465166c33CdAA4b?a=266617\"},
          {\"url\":\"https://bscscan.com/token/0xF5db804101d8600c26598A1Ba465166c33CdAA4b?
          a=266617\",\"name\":\"https://bscscan.com/token/0xF5db804101d8600c26598A1Ba465166c33CdAA4b?a=266617\"},
          {\"url\":\"https://bscscan.com/token/0xF5db804101d8600c26598A1Ba465166c33CdAA4b?a=266617\",\"name\":\"AirNFTs (AIRT) Token Tracker |
          BscScan\"},{\"url\":\"https://app.airnfts.com/nft/Chonky_Cats_059_1653068137360\",\"name\":\"Chonky Cats #059 | NFT | Earn BNB, FTM,
          Polygon via NFTs | Airnfts\"},{\"url\":\"https://app.airnfts.com/nft/Chonky_Cats_059_1653068137360\",\"name\":\"Chonky Cats #059 |
          NFT | Earn BNB, FTM, Polygon via NFTs | Airnfts\"},
          {\"url\":\"https://app.airnfts.com/nft/Chonky_Cats_059_1653068137360\",\"name\":\"Chonky Cats #059 | NFT | Earn BNB, FTM, Polygon
          via NFTs | Airnfts\"},{\"url\":\"https://app.airnfts.com/nft/Chonky_Cats_059_1653068137360\",\"name\":\"Chonky Cats #059 | NFT |
          Earn BNB, FTM, Polygon via NFTs | Airnfts\"},
          {\"url\":\"https://app.airnfts.com/nft/Chonky_Cats_059_1653068137360\",\"name\":\"Chonky Cats #059 | NFT | Earn BNB, FTM, Polygon
          via NFTs | Airnfts\"},| Earn BNB, FTM, Polygon via NFTs | Airnfts\"},
          {\"url\":\"https://app.airnfts.com/nft/Chonky_Cats_059_1653068137360\",\"name\":\"Chonky Cats #059 | NFT | Earn BNB, FTM, Polygon
```

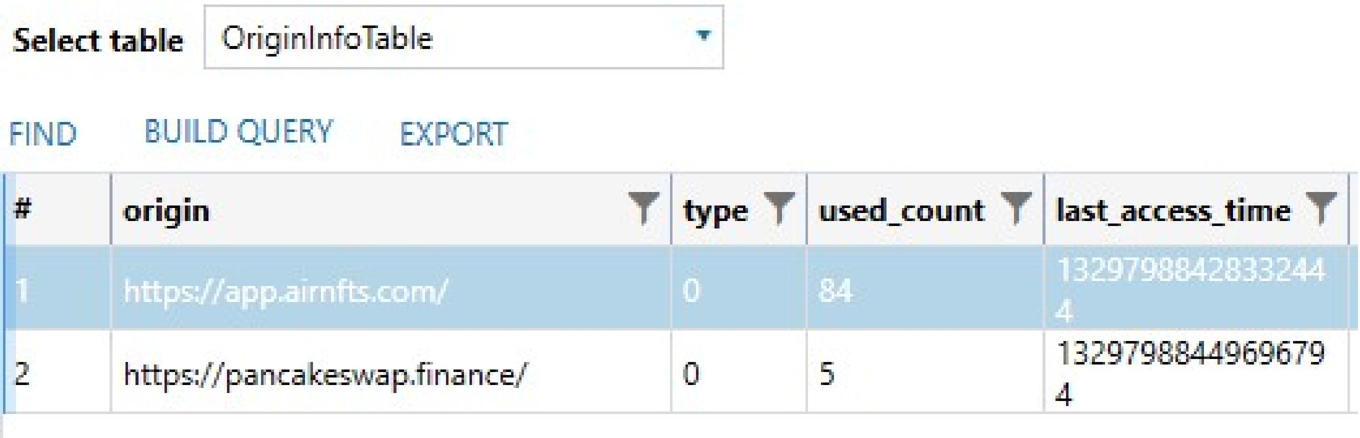
Figure 26. Privacy settings, resents, and browser activity objects within the persist-root file.



```
modals : {\"networkModalVisible\":false,\"accountsModalVisible\":false,\"collectibleContractModalVisible\":false,\"receiveModalVisible\":false
        ,\"dappTransactionModalVisible\":false,\"approveModalVisible\":false}
settings : {\"searchEngine\":\"DuckDuckGo\",\"primaryCurrency\":\"ETH\",\"useBlockieIcon\":true,\"hideZeroBalanceTokens\":false,\"lockTime\":3
           0000}
alert : {\"isVisible\":false,\"autodismiss\":null,\"content\":\"clipboard-alert\",\"data\":{\"msg\":\"Public address copied to clipboard\"}}
transaction : {\"assetType\":\"ETH\",\"selectedAsset\":{\"isETH\":true,\"symbol\":\"ETH\"},\"transaction\":
              {\"data\":\"0x7ff36ab500000000000000000000000000000000000000000000000000f012bf27ada8d3000000000000000000000000000000000000000000
              000000000000000000008000000000000000000000000fe99dd4568d459e30e439d966c6deb9686f88a5a000000000000000000000000000000000000000000
              00000000000000628ea727000000000000000000000000000000000000000000000000000000000000002000000000000000000000000bb4cdb9cbd36b01bd1
              cbaebf2de08d9173bc095c0000000000000000000000000e09fabb73bd3ade0a17ecc321fd13a19e81ce82\",\"from\":\"0xfe99dd4568d459e30e439d966c
              6deb9686f88a5a\",\"gas\":\"02afa5\",\"gasPrice\":\"012a05f200\",\"to\":\"0x10ed43c718714eb63d5aa57b78b54704e256024e\",\"value\":
              \"038d7ea4c68000\"},\"symbol\":\"ETH\",\"readableValue\":\"0.001\",\"id\":\"69dc5580-dc73-11ec-adf6-
              e1e707af2518\",\"type\":\"ETHER_TRANSACTION\",\"origin\":\"pancakeswap.finance\"}
user : {\"loadingMsg\":\"\",\"loadingSet\":false,\"backUpSeedphraseVisible\":false,\"protectWalletModalVisible\":false,\"gasEducationCarouselS
       een\":false,\"nftDetectionDismissed\":false,\"appTheme\":\"os\",\"passwordSet\":true,\"seedphraseBackedUp\":true,\"userLoggedIn\":true}
wizard : {\"step\":0}
notification : {\"notifications\":[]}
swaps : {\"1\":{\"isLive\":true},\"56\":{\"isLive\":true},\"isLive\":true,\"hasOnboarded\":false}
fiatOrders : {\"selectedCountry\":\"US\",\"orders\":[]}
infuraAvailability : {\"isBlocked\":false}
navigation : {\"currentRoute\":\"Settings\"}
networkOnboarded : {\"networkOnboardedState\":[{\"network\":\"https://bsc-dataseed.binance.org\",\"onboarded\":true}],\"networkState\":
                   {\"showNetworkOnboarding\":false,\"nativeToken\":\"\",\"networkType\":\"\",\"networkUrl\":\"\"},\"switchedNetwork\":
                   {\"networkUrl\":\"\",\"networkStatus\":false}}
_persist : {\"version\":10,\"rehydrated\":true}
```

Figure 27. Content of settings, set alerts, another transaction activity, and user settings within the persist-root file.

The table named `OriginalInfoTable`, which is contained in the file `app_webview\Default\QuotaManager`, contains the number of times the user opened the web services within the app (see Figure 28). This is an important table because it stores all the web services and the number of times the user has used them.



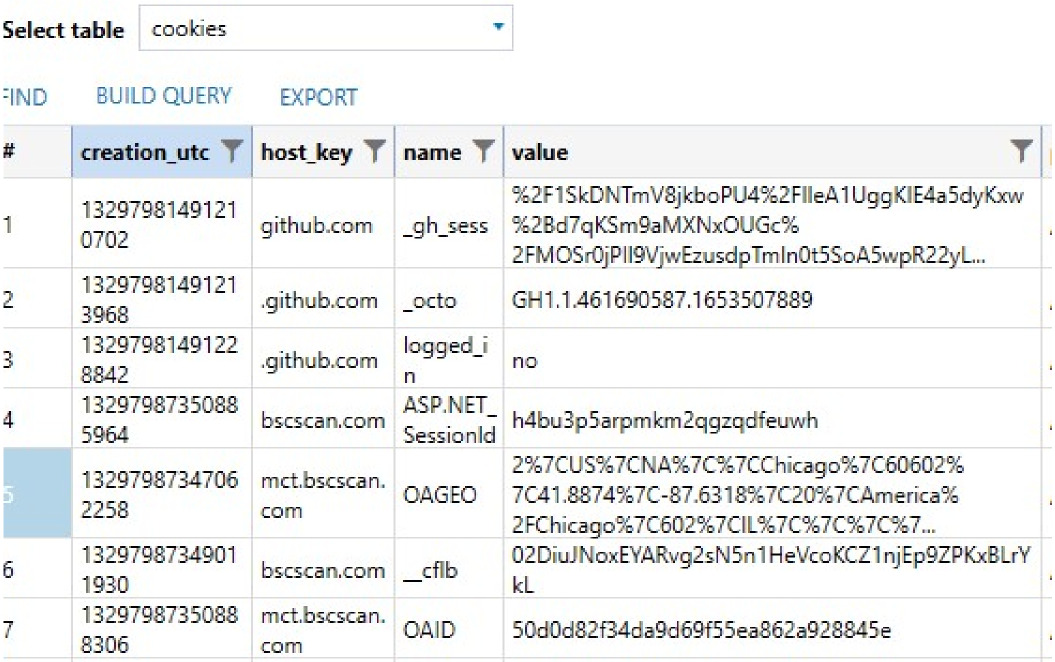
Select table OriginInfoTable

#	origin	type	used_count	last_access_time
1	https://app.airnfts.com/	0	84	13297988428332444
2	https://pancakeswap.finance/	0	5	13297988449696794

Figure 28. Number of times that the user opened the web services within the app.

In addition, `app_webview\Default` has a file named `Cookies`, this file is a database that stores cookies. One of these cookie values has a relatively close location to where we have populated the device (see Figure 29).

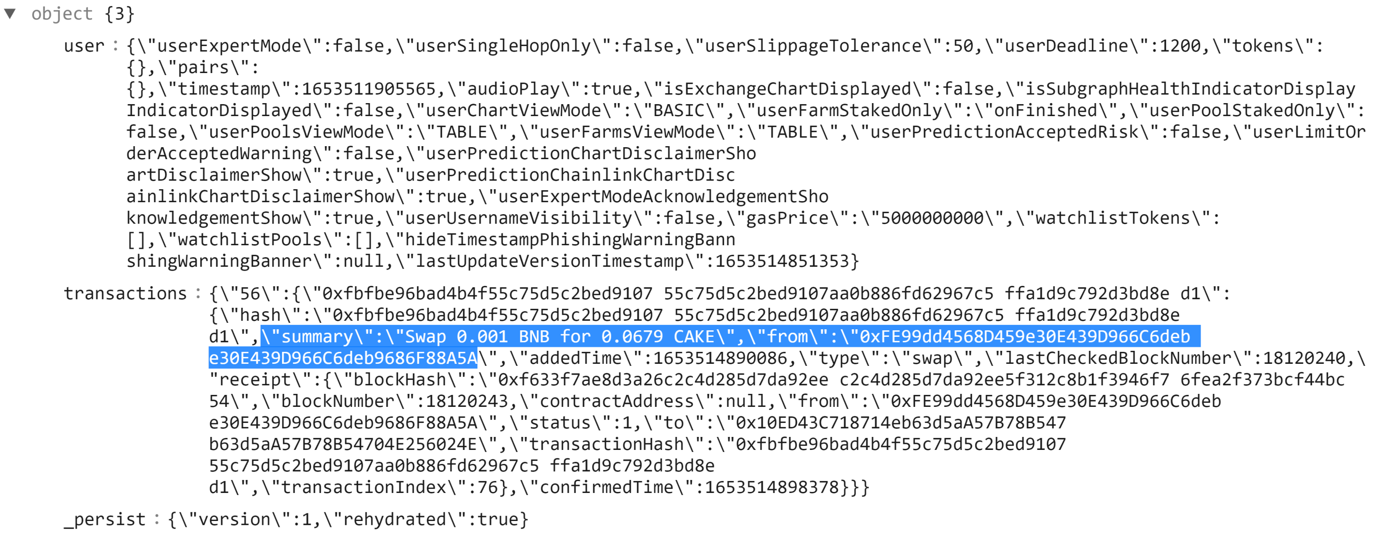
The swapping operation was performed in the Metamask app, and we were able to recover detailed swapping information from `app_webview\Default\LocalStorage\leveldb\000003.log`, which confirms and complements the information found within the `persist-root` JSON file. This is a log file in the local storage of the app web view that keeps activities. Figure 30 shows the BNB swapping for Cake, along with other information for the transaction from `000003.log` file.



Select table cookies

#	creation_utc	host_key	name	value
1	13297981491210702	github.com	_gh_sess	%2F1SkDNTmV8jkboPU4%2FIleA1UggKIE4a5dyKxw%2Bd7qKSm9aMXNxOUGc%2FMOSr0jPII9VjwEzusdpTmIn0t5SoA5wpR22yL...
2	13297981491213968	.github.com	_octo	GH1.1.461690587.1653507889
3	13297981491228842	.github.com	logged_in	no
4	13297987350885964	bscscan.com	ASP.NET_SessionId	h4bu3p5arpmkm2qgzqdfeuwh
5	13297987347062258	mct.bscscan.com	OAGEO	2%7CUS%7CNA%7C%7CChicago%7C60602%7C41.8874%7C-87.6318%7C20%7CAmerica%2FChicago%7C602%7CIL%7C%7C%7C%7...
6	13297987349011930	bscscan.com	__cflb	02DiuJNoxEYARvg2sN5n1HeVcoKCZ1njEp9ZPKxBLrYkL
7	13297987350888306	mct.bscscan.com	OAID	50d0d82f34da9d69f55ea862a928845e

Figure 29. Cookie values show geolocation.

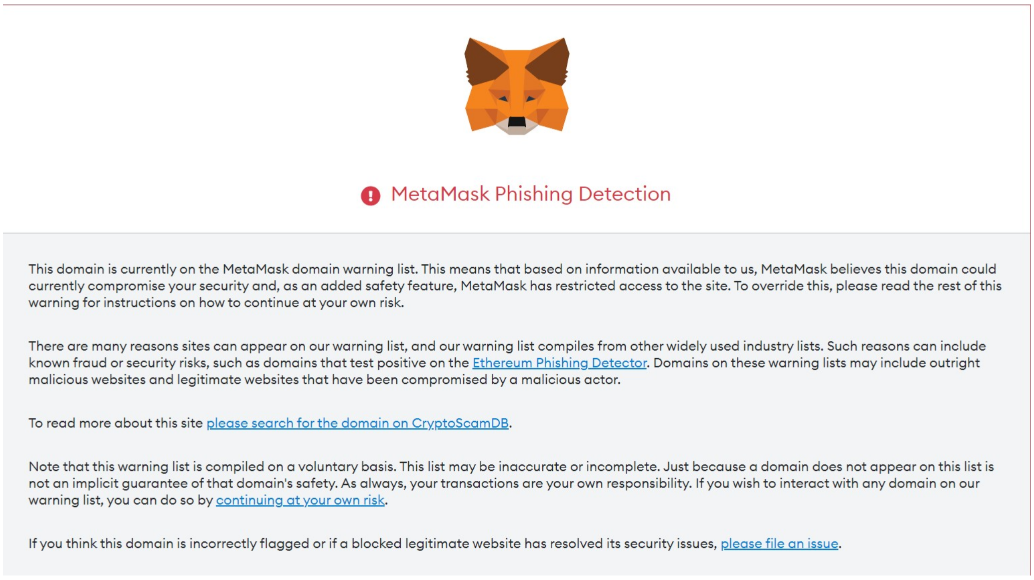


```
▼ object {3}
    user : {\"userExpertMode\":false,\"userSingleHopOnly\":false,\"userSlippageTolerance\":50,\"userDeadline\":1200,\"tokens\":
           {},\"pairs\":
           {},\"timestamp\":1653511905565,\"audioPlay\":true,\"isExchangeChartDisplayed\":false,\"isSubgraphHealthIndicatorDisplay
           IndicatorDisplayed\":false,\"userChartViewMode\":\"BASIC\",\"userFarmStakedOnly\":\"onFinished\",\"userPoolStakedOnly\":
           false,\"userPoolsViewMode\":\"TABLE\",\"userFarmsViewMode\":\"TABLE\",\"userPredictionAcceptedRisk\":false,\"userLimitOr
           derAcceptedWarning\":false,\"userPredictionChartDisclaimerSho
           artDisclaimerShow\":true,\"userPredictionChainlinkChartDisc
           ainlinkChartDisclaimerShow\":true,\"userExpertModeAcknowledgementSho
           knowledgementShow\":true,\"userUsernameVisibility\":false,\"gasPrice\":\"5000000000\",\"watchlistTokens\":
           [],\"watchlistPools\":[],\"hideTimestampPhishingWarningBann
           shingWarningBanner\":null,\"lastUpdateVersionTimestamp\":1653514851353}

    transactions : {\"56\":{\"0xfbfbe96bad4b4f55c75d5c2bed9107 55c75d5c2bed9107aa0b886fd62967c5 ffa1d9c792d3bd8e d1\":
                   {\"hash\":\"0xfbfbe96bad4b4f55c75d5c2bed9107 55c75d5c2bed9107aa0b886fd62967c5 ffa1d9c792d3bd8e
                   d1\",\"summary\":\"Swap 0.001 BNB for 0.0679 CAKE\",\"from\":\"0xFE99dd4568D459e30E439D966C6deb
                   e30E439D966C6deb9686F88A5A\",\"addedTime\":1653514890086,\"type\":\"swap\",\"lastCheckedBlockNumber\":18120240,\
                   "receipt\":{\"blockHash\":\"0xf633f7ae8d3a26c2c4d285d7da92ee c2c4d285d7da92ee5f312c8b1f3946f7 6fea2f373bcf44bc
                   54\",\"blockNumber\":18120243,\"contractAddress\":null,\"from\":\"0xFE99dd4568D459e30E439D966C6deb
                   e30E439D966C6deb9686F88A5A\",\"status\":1,\"to\":\"0x10ED43C718714eb63d5aA57B78B547
                   b63d5aA57B78B54704E256024E\",\"transactionHash\":\"0xfbfbe96bad4b4f55c75d5c2bed9107
                   55c75d5c2bed9107aa0b886fd62967c5 ffa1d9c792d3bd8e
                   d1\",\"transactionIndex\":76},\"confirmedTime\":1653514898378}}}

    _persist : {\"version\":1,\"rehydrated\":true}
```

Figure 30. The 000003.log within the Local Storage of the app web view that kept activities of swap transactions.

The folder `\cache\image_cache\v2.ols100.1` contains folders that have .png images stored as `.cnt` extension, these images are for the cached images in the app. In addition, folder `\cache` has other snapshots that the app took.

Additionally, the app provides white and black lists of phishing websites, where the app pulls this information once configured. This information is extracted from `https://cdn.jsdelivr.net/gh/MetaMask/eth-phishing-detect@master/src/config.json?`, and by navigating to one of the phishing websites, it provides the user with a warning (see Figure 31). At the time of writing the investigation, the file contained 15 fuzzy lists, 1594 whitelists, and 1454 blacklist links (see Figure 32).



MetaMask Phishing Detection

This domain is currently on the MetaMask domain warning list. This means that based on information available to us, MetaMask believes this domain could currently compromise your security and, as an added safety feature, MetaMask has restricted access to the site. To override this, please read the rest of this warning for instructions on how to continue at your own risk.

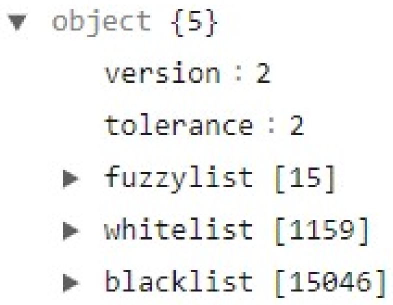
There are many reasons sites can appear on our warning list, and our warning list compiles from other widely used industry lists. Such reasons can include known fraud or security risks, such as domains that test positive on the Ethereum Phishing Detector. Domains on these warning lists may include outright malicious websites and legitimate websites that have been compromised by a malicious actor.

To read more about this site please search for the domain on CryptoScamDB.

Note that this warning list is compiled on a voluntary basis. This list may be inaccurate or incomplete. Just because a domain does not appear on this list is not an implicit guarantee of that domain's safety. As always, your transactions are your own responsibility. If you wish to interact with any domain on our warning list, you can do so by continuing at your own risk.

If you think this domain is incorrectly flagged or if a blocked legitimate website has resolved its security issues, please file an issue.

Figure 31. Metamask app warning to the user.



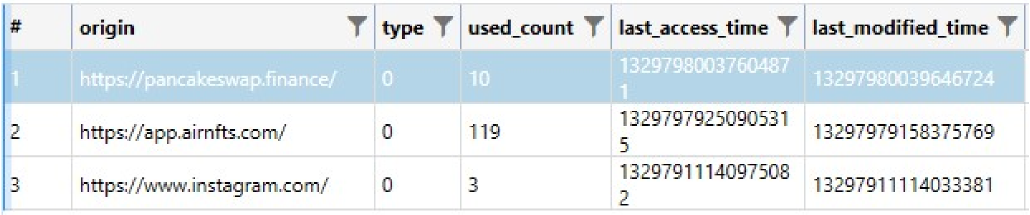
```
▼ object {5}
    version : 2
    tolerance : 2
  ▶ fuzzylist [15]
  ▶ whitelist [1159]
  ▶ blacklist [15046]
```

Figure 32. Metamask app recovered lists.

4.2.2. Trust Wallet

All Trust Wallet-related files were located in package `\data\com.wallet.crypto.trustapp`, unless otherwise noted. `\files` is an essential folder for the Trust Wallet app. This folder contains the two wallets created in the scenario Wallet `m-2-1653501108488` and `m-2-1653424125494`; all NFTs that are purchased or transferred into the app are stored here. These two databases are named using their creation epoch time. In addition, the folder `\files` contains all QR images generated using the app named as `<WalletAddress>.png`.

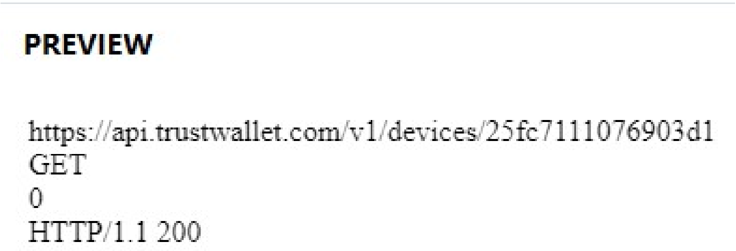
The file `com.wallet.crypto.trustapp_preferences.xml` located in the folder `shared_prefs` has the names of the wallets, the creation time, and the addresses and active coins within the wallets. Furthermore, the date of installation of the app was recoverable from `app_webview\pref_store`. Furthermore, similar to what was recovered in the iOS version of the app, we were able to recover the count of how many times the web services/website have been accessed by the user of the app in a table named `OriginInfoTable` within the following database `app_webview\Default` (see Figure 33).



#	origin	type	used_count	last_access_time	last_modified_time
1	https://pancakeswap.finance/	0	10	13297980037604871	13297980039646724
2	https://app.airnfts.com/	0	119	13297979250905315	13297979158375769
3	https://www.instagram.com/	0	3	13297911140975082	13297911114033381

Figure 33. Count of how many times the web services/websites have been accessed by the user.

Additionally, due to the fact that the app uses webview and HTTPS requests, these are cached and can be found in a folder called `\cache`. Furthermore, there is another folder named `image_manager_disk_cache` that contains cached images. Crucial information that points to the deviceID can also be recovered with the cache folder, which can be found in the HTTPS requests (see Figure 34).



PREVIEW

```
https://api.trustwallet.com/v1/devices/25fc7111076903d1
GET
0
HTTP/1.1 200
```

Figure 34. DeviceID recovered from a recovered HTTPS request.

Android and iOS file structures are different since the applications are developed differently. Trust Wallet uses realm databases to store information about currencies and wallets. However, the Trust Wallet app uses different database structures for Android and iOS. In Android, there are four realm databases that store information about bookmarks, app configurations, general wallet information, and an encrypted database named `wallets_info`. This allows investigators to obtain more information from Android devices. On the other hand, iOS uses only two realm databases, which are encrypted.

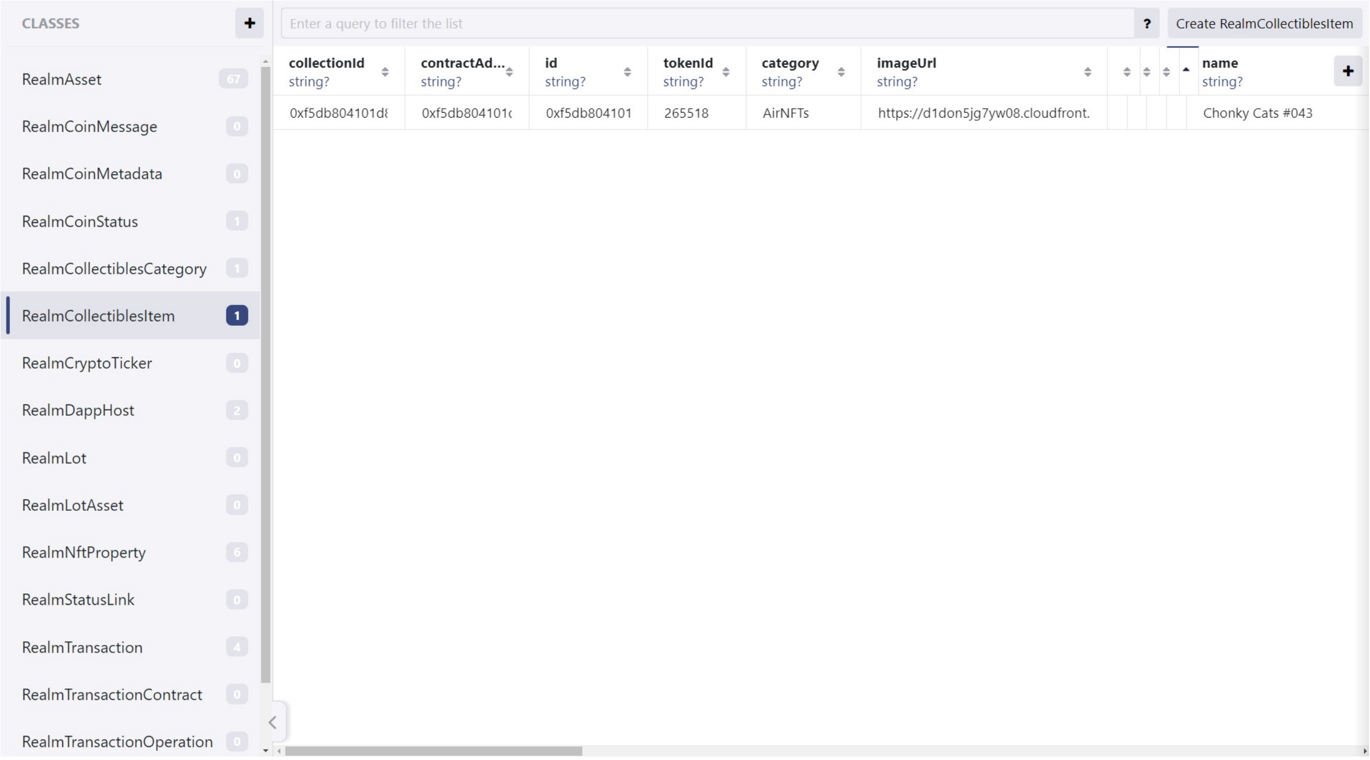
When realm databases on iOS were examined, they were all encrypted; however, this is not the case with the recovered realm databases named `m-2-1653424125494` and `m-2-1653501108488`, which contain information about enabled cryptocurrencies and their addresses, transaction history, decentralized apps used, and owned collectibles (e.g., NFTs). Figure 35 shows the different classes (tables) stored within the wallet `m-2-1653501108488` realm database. In Figure 35, the table named `RealmCollectiblesItem` is opened and we can see the NFT contract, ID, category, name, and image URL. Furthermore, Table `RealmAsset` contains all the cryptocurrency coins that the user has with their balances (e.g., available, locked, frozen, stacked, rewards, and pending) wallet addresses, and if these coins were manually added by the user. In addition, Table `RealmTransaction`, provides detailed information on transactions, such as timestamp, amount, gas fees, and transaction hash. With this information, you can use tools, such as Ciphertrace [69], to gain intelligent insight into transactions.

Throughout the analysis of Trust Wallet, we came across ciphertexts, salt, and IV, but were unable to decrypt these secrets. The assumption is that the salt and IVs found in the files can be used to decrypt encrypted realm databases.

4.3. Uninstalling/Deleting the Apps

There is an increase in the use of anti-forensic measures to obstruct forensic investigations and alter evidence [70]. This has the potential to substantially alter the precision of forensic investigations. Anti-forensic methods, such as those described in [71], should be taken into account when dealing with digital evidence. In our scenarios, we simulate the removal of artifacts by uninstalling the cryptocurrency wallets from the two phones after taking the first forensic image and before taking the second forensic image.

Our investigation shows that even when the user uninstalls the applications, the deletion of the Android deviceIDs is recorded in the `log\settingsprovider.txt` file. Table 7 highlights the recovered format as an example log entry after uninstalling the apps. From the investigation, we discovered that the device number is a very important piece of information and can be used to access the wallet functions using the APIs of the app, as seen in Figure 34.



CLASSES	
RealmAsset	67
RealmCoinMessage	0
RealmCoinMetadata	0
RealmCoinStatus	1
RealmCollectiblesCategory	1
RealmCollectiblesItem	1
RealmCryptoTicker	0
RealmDappHost	2
RealmLot	0
RealmLotAsset	0
RealmNftProperty	6
RealmStatusLink	0
RealmTransaction	4
RealmTransactionContract	0
RealmTransactionOperation	0

Enter a query to filter the list

collectionId string?	contractAd... string?	id string?	tokenId string?	category string?	imageUrl string?				name string?
0xf5db804101d8	0xf5db804101c	0xf5db804101	265518	AirNFTs	https://d1don5jg7yw08.cloudfront.				Chonky Cats #043

Figure 35. Wallet m-2-1653501108488 Realm database opened using Realm Studio software.

On the other hand, one can recover if the applications were installed on the iOS device using the `private\var\installd\Library\Logs\Mobile\Installation\mobile\installation.log.1` file and one can recover uninstalled apps in the `private\var\installd\Library\Logs\Mobile\Installation\mobile\installation.log.1` file and within the `\private\var\db\diagnostics\log\data.statistics.0.txt` file that shows processes, records of memory rollovers, and file rotations (see Figure 36), showing an example of a recovered memory rollover.

```
...
--- !logd statistics record
type  : Memory Rollover
time  : 2022-05-25 16:06:26-0400
total :
procs :
   - [3984608, 34.3, /usr/libexec/backboardd ]
   - [1594672, 13.7, /private/var/containers/Bundle/Application/CCEF3F88-456D-4C36-9FAE-
9720A9F79EE7/Trust.app/Trust ]
   - [1365546, 11.7, /private/var/containers/Bundle/Application/7DC0C05E-FE59-4375-B288-
F5B304DEE01A/MetaMask.app/MetaMask ]
   - [1268648, 10.9, /usr/libexec/locationd ]
   - [ 655160, 5.6, /System/Library/CoreServices/SpringBoard.app/SpringBoard ]
   - [ 579664, 5.0, /usr/libexec/runningboardd ]
   - [ 225280, 1.9, /usr/sbin/WirelessRadioManagerd ]
   - [ 219099, 1.9, /Applications/SafariViewService.app/SafariViewService ]
   - [ 176976, 1.5, /usr/libexec/symptomsd ]
   - [ 136296, 1.2, /usr/libexec/UserEventAgent ]
   - [ 109088, 0.9,
/System/Library/Frameworks/WebKit.framework/XPCServices/com.apple.WebKit.WebContent.xpc/com.apple.W
ebKit.WebContent ]
...
```

Figure 36. Example of a memory rollover recovered from logdata.statistics.0.txt.

Table 7. Full-device IDs recovered for cryptocurrency wallets in the Android OS.

App Name	Schema
Trustapp	<timestamp> SettingsState : deletesettingLocked() name : <Incremented number generated by the device>, value : <DeviceID>, package : com.wallet.crypto.trustapp, default : <DeviceID>
Metamask	<timestamp> SettingsState : deletesettingLocked() name : <Incremented number generated by the device>, value : <DeviceID>, package : io.metamask, default : <DeviceID>

4.4. Digital Forensic Tools Evaluation

Unfortunately, none of the tools used in this investigation were practical in automatically recovering the wallet ID, transactions, and NFTs associated with the two investigated apps. As a result, we needed to search file-by-file for information within the apps packages. This led to the need to find a way to perform automatic recovery. Therefore, we extend an open source tool that is well known by the digital forensics community, called iLEAPP [20], to automatically recover important artifacts. Details on how we added new modules to the tool are fully discussed in Section 5.

5. Proposed Tool

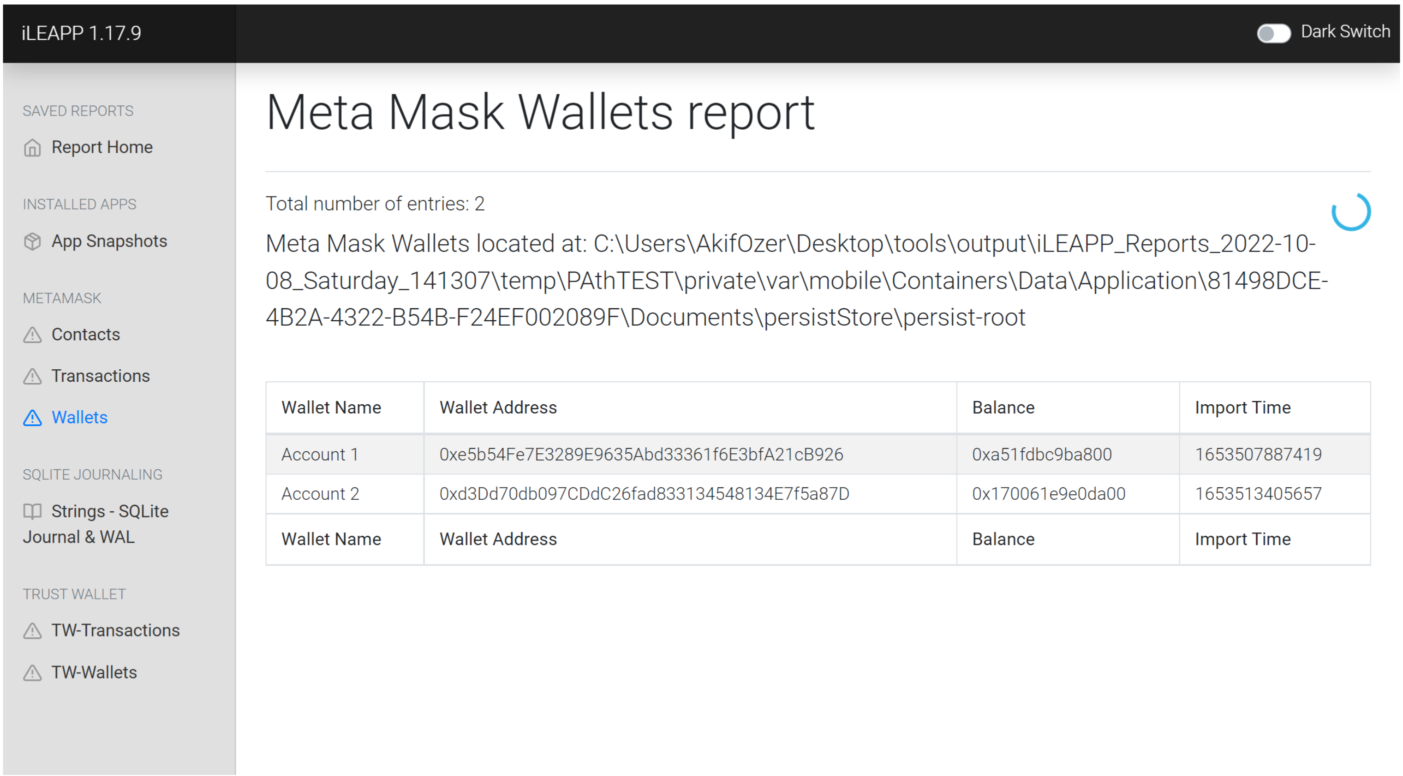
According to the authors in [72], it is difficult to obtain a complete picture of what happened over a long period of time in digital investigations without event reconstruction, which may be one of the most significant components to examine in forensic investigations. However, due to the lack of automatic recovery of these transactions when it comes to digital wallets utilizing the used digital forensics software (i.e. Magnet AXIOM, and Autopsy), investigators are left with a large amount of files that they have to cross-examine manually. Therefore, we developed a tool that can help investigators get a picture of the transaction events that occurred on the phone.

The solution focuses on recovering transaction events to provide a complete picture of the transaction using metadata and information extracted from the iOS and Android app files, as well as the use of blockchain technology and data analytics.

As we discussed earlier in the paper, digital forensics tools do not have an automated way to extract mobile crypto wallet-related information. To automate this step, we created an artifact plugin for iLEAPP [20] as a proof of concept. With this artifact plugin, one can automatically extract public wallet addresses and other artifacts that we discussed in the paper. Figure 37 shows the result of the tool to recover information from the Metamask app. Furthermore, Table 8 provides samples of API request parameters that can be used to recover information.

The extension is a proof of concept that employs Open Source Intelligence (OSINT), which is another method of unlocking the full potential of cryptocurrencies. The tool uses data that are publicly stored on the blockchain to compare and verify transactions that occurred on the phone. This allows investigators to differentiate between transactions that involve the investigated device and transactions of the same wallet that occurred using other apps or devices.

Since the blockchain has a public ledger, you can get more detailed information about the wallets, including the other wallets to which the target wallet sent coins. This artifact plugin can be extended to recover more information about the transactions made from the recovered device by using HTTPS caches.



Meta Mask Wallets report

Total number of entries: 2

Meta Mask Wallets located at: C:\Users\AkifOzer\Desktop\tools\output\iLEAPP_Reports_2022-10-08_Saturday_141307\temp\PAthTEST\private\var\mobile\Containers\Data\Application\81498DCE-4B2A-4322-B54B-F24EF002089F\Documents\persistStore\persist-root

Wallet Name	Wallet Address	Balance	Import Time
Account 1	0xe5b54Fe7E3289E9635Abd33361f6E3bfA21cB926	0xa51fdbc9ba800	1653507887419
Account 2	0xd3Dd70db097CDdC26fad833134548134E7f5a87D	0x170061e9e0da00	1653513405657
Wallet Name	Wallet Address	Balance	Import Time

Figure 37. Recovered Wallet addresses for the Metamask app in iOS.

Table 8. Examples of API requests from the Trust Wallet app and airnfts.com.

Usage	URL Schema
Display the device type, app version, wallets version, deice model, and default currency (e.g., USD).	Available online: `https://api.trustwallet.com/v1/devices/<DeviceID>`
Will display all wallets that were created using this device along with information such as phone wallet Id, accounts under that wallet, coins with their wallet addresses, coins blockchains.	`https://api.trustwallet.com/v2/devices/<DeviceID>/wallets`
Will return details about transactions such as receiver, transaction type, gas fee, and the amount involving the requested asset type.	Available online: `https://api.trustwallet.com/v1/chains/smartchain/transactions/<WalletAddress>?asset=c<AssetID>&since_created_at=<EpochTimestamp>&version=3`
Used to recover "token_id" and to get the URL to the NFT.	Available online: `https://api.trustwallet.com/v1/collectiblessmartchain/collections/<WalletAddress>/collection/<ContractID>`
Will display the wallet account in Airnft.	Available online: `https://app.airnfts.com/creators/<WalletAddress>`

6. Discussion

Digital forensic analysts, researchers, and investigators must employ an innovative approach to analyze, report, and display their findings while conducting cyberforensic investigations that include cryptocurrency wallets and transactions. To improve the reporting approach and provide assistance to expert witnesses and law enforcement, the forensic procedures followed in the investigation of the mobile applications studied here have been presented in detail. In addition, we have made a great effort to select the necessary software, hardware, and other tools for this study so that they are straightforward to replicate.

Furthermore, our research examines devices using validated methods for the preservation and examination of evidence and the tried-and-true techniques provided in Section 3. Therefore, other researchers in the law enforcement, private sector, and tool developers may benefit from the contribution to the validation technique used in this work.

6.1. Forensics Artifacts

According to our research, although we know that databases can store crucial data and information about user activity, our investigation directly led to the discovery that due to the fact that Metamask and Trust Wallet apps use HTTPS requests, these apps cache and store valuable information in the logs. Therefore, inspecting logs and web cached files by the apps is critical and may lead to great findings. We noted that Transfer/Swapping has two requests related to the transaction, where buy only has one HTTPS request related to that transaction.

Moreover, even after deleting apps, it is possible to recover the wallet addresses that were created or imported into the device using the DeviceID in the proper API request, as discussed in this paper. In addition, we were able to recover some transactions in the unallocated space of the phones using a combination of DeviceIDs and other unique words (e.g., io.metamask, Metamasp.app, Trustapp, and Trust.app) as keywords to search the entire image byte-by-byte (i.e., carving).

The increased popularity of cryptocurrency coins led some companies and stores to accept cryptocurrency coins as a payment method. Furthermore, the popularity in mobile wallets creates new challenges for mobile forensic investigators, and accepting cryptocurrencies as a payment method will also challenge forensic accountants. Especially in the United States, cryptocurrency regulations are strict. To buy cryptocurrency, cryptocurrency money services require identity verification. Therefore, these services will send the user a confirmation email about their purchases. Artifacts, such as emails, can also reveal information related to the time, type of payment, and origin of the cryptocurrency to the investigator. It is significant to tie different artifacts to each other; therefore, we argue that investigators should search for and connect the information found on the devices.

6.2. Security and Privacy Concerns

Blockchain technology has the potential to become a powerful tool that can improve information security and privacy as a result of its immutability, decentralization, and encryption at its core. These characteristics give blockchain technology its promise. In this research, we look at technology from a different perspective. Although the main objective of this study is to improve mobile forensics methods and investigations for new Web3 wallets, we also wanted to draw attention to privacy and security issues with the mobile apps we examined.

The investigation (i.e., analysis and examination) revealed potential privacy and security threats due to the many artifacts kept in plaintext that were not encrypted. We were able to retrieve significant information from http-get requests issued by the apps due to WebKit insufficient encryption implementation, which raises several questions about the security and privacy of these wallets' users. However, keywords (i.e., secret recovery phrase) and private keys for wallets were encrypted in both apps tested in the study for both phones. Although we were able to find information about the transactions and their decentralized application history, crucial information such as keywords was encrypted. An additional feature that the Trust Wallet provides in its applications is that the user cannot take a screenshot of the screen when it is on the screen with the secret recovery phrase, which is not provided in the Metamask app. It is always a good practice to search the phone for saved or stored secret phrases in other apps such as notes.

In addition, the realm databases were found to contain valuable information for the wallets and actions that were performed on the device. However, in our investigation, we opened the realm databases with an open-source app named Realm Studio because the digital forensic tools that we used, Autopsy and Axiom, were unable to open and process these database files.

As a result of using Realm Studio, we found that most of the realm databases on the Android device were not encrypted, while on the iOS device, all the realm databases are encrypted. In investigations, any evidence, such as that found in the Android realm database, can help investigators in their decision making.

The growing wave of NFT is making NFT platforms increasingly popular. These platforms allow their users to personalize their pages, including usernames and social media accounts, etc. Although crypto wallet addresses are difficult to remember and anonymous, NFT platforms can help law enforcement recover PIIs and link wallets to online personalities. In the Metamask app on iOS, we were able to recover all of the NFT history (i.e., transactions) of purchases, along with the previous owner information and wallet addresses.

As essential as recovering the transactions, it is important to recover the visited services that the user used in the app. According to [73], `WebKitWebsiteData` is a folder that stores information that a certain website has transmitted to the client's device. This technology has its weaknesses and strengths, and in this research, we were able to recover a lot of information from the WebKit.

Although HSTS is used to help prevent attacks on websites by implementing a policy technique; however, it still left some traces that helped recover the websites/services used in the app. In addition, cookies are similar to HSTS and have provided information along with timestamps for the services visited.

6.3. Automatic Reconstruction

Manual event reconstruction takes a significant amount of time that investigators could instead spend examining/analyzing 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. Event reconstruction is necessary to track related transactions and can facilitate relationships between transactions executed by the user.

6.4. Limitations

This research has some limitations. First, we did not include network traffic in the study design. This is needed to investigate security and privacy concerns introduced to app users as a result of their use. Second, analyzing HTTPS caches could cause discrepancies in the automated tool if the applications change their APIs or the way they store the caches, which means that any tool will require maintenance.

7. Conclusions and Future Work

This research can be a great resource for future work on cyber forensics on blockchain apps (e.g., Web3 crypto wallets). Blockchain technologies have found their way into many fields and will continue to grow in a diverse selection of sectors. This drastically increased the number of users who use blockchain technologies. Moreover, the increased popularity of blockchain technologies has attracted the attention of many investors as well as criminal organizations. Although everything seems transparent, techniques such as tumbling of cryptocurrencies can make it difficult to find the origin of the assets.

The findings of this research provide researchers, practitioners, and law enforcement with a roadmap for forensically analyzing and examining Web3 crypto wallets on mobile devices. Furthermore, the investigation enables a deeper understanding of the Web3 crypto wallet artifacts, which can be considered when recovered as significant sources of evidence in many cases. Therefore, they can be used in conjunction with other relevant artifacts to track cyber-financial activities of users.

As discussed earlier, the digital forensic tools used in this study do not automatically target and extract Web3 wallet apps. Therefore, it is crucial to improve known digital forensic tools and strengthen their ability to extract artifacts from Web3 applications. Furthermore, our goal in the future is to extend the plugin by adding more features and implement it in the Android version of the open source tool aLEAPP [74].

Author Contributions: Conceptualization, methodology, software, writing—original draft preparation, M.M.M. and A.O.; validation, formal analysis, investigation, funding acquisition, project administration, visualization, M.M.M.; resources, writing—review and editing, M.M.M., A.O. and U.K.; supervision, M.M.M. and U.K. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by Taif University Researchers Supporting Project number (TURSP-2020/329), Taif University, Taif, Saudi Arabia.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors are grateful for the support of Taif University Researchers Supporting Project number (TURSP-2020/329) Taif University, Taif, Saudi Arabia.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Fenwick, M.; Jurcys, P. The Contested Meaning of Web3 and Why it Matters for (IP) Lawyers. Available online http://copyrightblog.kluweriplaw.com/2022/01/27/the-contested-meaning-of-web3-why-it-matters-for-ip-lawyers/ (accessed on 2 November 2022).
2. NIST. Blockchain | NIST. Available online: https://www.nist.gov/blockchain (accessed on 21 May 2022).
3. U.S. Depertment of Justice. Report of the Attorney General's Cyber Digital Task Force: Cryptocurrency Enforcement Framework. 2020. Available online: https://www.justice.gov/archives/ag/page/file/1326061/download (accessed on 10 August 2022).
4. Peters, G.; Panayi, E.; Chapelle, A. Trends in cryptocurrencies and blockchain technologies: A monetary theory and regulation perspective. *J. Financ. Perspect.* **2015**, *3, 92–113.*
5. Chainalysis. Chainalysis-Crypto-Crime-2021.pdf. 2021. Available online: https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf (accessed on 20 May 2022).
6. SunFollow, M.; Smagalla, D. Cryptocurrency-Based Crime Hit a Record $14 Billion in 2021—WSJ. Available online: https://www.wsj.com/articles/cryptocurrency-based-crime-hit-a-record-14-billion-in-2021-11641500073. (accessed on 23 May 2022).
7. Brown, S.D. Cryptocurrency and criminality: The Bitcoin opportunity. *Police J.* **2016**, *89*, 327–339. [CrossRef]
8. Abdel Samad, Y. Case Study: Dark Web Markets. In *Dark Web Investigation*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 237–247.
9. Tziakouris, G. Cryptocurrencies—A forensic challenge or opportunity for law enforcement? An interpol perspective. *IEEE Secur. Priv.* **2018**, *16*, 92–94. [CrossRef]
10. De Best, R. Blockchain.com Wallets 2011–2022 | Statista. Available online: https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users/ (accessed on 21 May 2022).
11. Metamask. The Crypto Wallet for Defi, Web3 Dapps and NFTs | MetaMask. Available online: https://metamask.io/ (accessed on 21 May 2022).
12. Roberts, J.J. Ethereum Wallet MetaMask Passes 30M Users, Plans DAO and Token—Decrypt. Available online: https://decrypt.co/95039/metamask-consensys-30-million-users (accessed on 21 May 2022).
13. Wallet, T. Best Cryptocurrency Wallet | Ethereum Wallet | ERC20 Wallet | Trust Wallet. Available online: https://trustwallet.com/ (accessed on 21 May 2022).
14. Blockchain.com. Blockchain Explorer—Search the Blockchain | BTC | ETH | BCH. Available online: https://www.blockchain.com/charts/my-wallet-n-users (accessed on 21 May 2022).
15. Jørgensen, K.P.; Beck, R. Universal Wallets. *Bus. Inf. Syst. Eng.* **2022**, *64*, 115–125. [CrossRef]
16. Keim, Y.; Yoon, Y.H.; Karabiyik, U. Digital Forensics Analysis of Ubuntu Touch on PinePhone. *Electronics* **2021**, *10*, 343. [CrossRef]
17. Tzvetanov, K.; Karabiyik, U. A first look at forensic analysis of sailfishos. *Comput. Secur.* **2020**, *99*, 102054. [CrossRef]
18. Forensics, M. Magnet AXIOM—Digital Investigation Platform Magnet Forensics. Available online: https://www.magnetforensics.com/products/magnet-axiom/ (accessed on 20 May 2022).
19. Technology, B. Autopsy Digital Forensics. Available online: https://www.autopsy.com/ (accessed on 20 May 2022).
20. Abrignoni. abrignoni/iLEAPP: iOS Logs, Events, And Plist Parser. Available online: https://github.com/abrignoni/iLEAPP (accessed on 12 September 2022).
21. Yuan, Y.; Wang, F.Y. Blockchain and Cryptocurrencies: Model, Techniques, and Applications. *IEEE Trans. Syst. Man Cybern. Syst.* **2018**, *48*, 1421–1428. [CrossRef]
22. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Bus. Rev.* **2008**, 21260.
23. Manimuthu, A.; Rejikumar, G.; Marwaha, D. A literature review on Bitcoin: Transformation of crypto currency into a global phenomenon. *IEEE Eng. Manag. Rev.* **2019**, *47*, 28–35. [CrossRef]

24. Ghosh, A.; Gupta, S.; Dua, A.; Kumar, N. Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects. *J. Netw. Comput. Appl.* **2020**, *163*, 102635. [CrossRef]
25. Blockchain.com. Blockchain.com | Explorer. Available online: https://www.blockchain.com/explorer (accessed on 22 May 2022).
26. Malherbe, L.; Montalban, M.; Bédu, N.; Granier, C. Cryptocurrencies and blockchain: Opportunities and limits of a new monetary regime. *Int. J. Political Econ.* **2019**, *48*, 127–152. [CrossRef]
27. Taylor, S.K.; Ariffin, A.; Ariffin, K.A.Z.; Abdullah, S.N.H.S. Cryptocurrencies Investigation: A Methodology for the Preservation of Cryptowallets. In Proceedings of the 2021 3rd International Cyber Resilience Conference (CRC), Langkawi Island, Malaysia, 29–31 January 2021; pp. 1–5.
28. Dyson, S.; Buchanan, W.J.; Bell, L. The challenges of investigating cryptocurrencies and blockchain related crime. *arXiv* **2019**, arXiv:1907.12221.
29. Casino, F.; Dasaklis, T.K.; Spathoulas, G.; Anagnostopoulos, M.; Ghosal, A.; Borocz, I.; Solanas, A.; Conti, M.; Patsakis, C. Research trends, challenges, and emerging topics in digital forensics: A review of reviews. *IEEE Access* **2022**, *10*, 25464–25493. [CrossRef]
30. Biryukov, A.; Tikhomirov, S. Security and privacy of mobile wallet users in Bitcoin, Dash, Monero, and Zcash. *Pervasive Mob. Comput.* **2019**, *59*, 101030. [CrossRef]
31. Volety, T.; Saini, S.; McGhin, T.; Liu, C.Z.; Choo, K.K.R. Cracking Bitcoin wallets: I want what you have in the wallets. *Future Gener. Comput. Syst.* **2019**, *91*, 136–143. [CrossRef]
32. Khadzhi, A.S.; Zareshin, S.V.; Tarakanov, O.V. A Method for Analyzing the Activity of Cold Wallets and Identifying Abandoned Cryptocurrency Wallets. In Proceedings of the 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Moscow, Russia, 27–30 January 2020; pp. 1974–1977. [CrossRef]
33. Subbotin, D.A.; Antropova, M.A.; Sukharev, P.V. Tracking Transactions in Crypto Currencies Using the Graph Theory. In Proceedings of the 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus) Moscow, Russia, 27–30 January 2020; pp. 526–529. [CrossRef]
34. Yue, X.; Shu, X.; Zhu, X.; Du, X.; Yu, Z.; Papadopoulos, D.; Liu, S. Bitextract: Interactive visualization for extracting bitcoin exchange intelligence. *IEEE Trans. Vis. Comput. Graph.* **2018**, *25*, 162–171. [CrossRef]
35. Sun, Y.; Xiong, H.; Yiu, S.M.; Lam, K.Y. BitAnalysis: A Visualization System for Bitcoin Wallet Investigation. *IEEE Trans. Big Data* **2022**, 1–6. [CrossRef]
36. Van Der Horst, L.; Choo, K.K.R.; Le-Khac, N.A. Process memory investigation of the bitcoin clients electrum and bitcoin core. *IEEE Access* **2017**, *5*, 22385–22398. [CrossRef]
37. Doran, M.D. *A Forensic Look at Bitcoin Cryptocurrency*; ProQuest LLC.: Ann Arbor, MI, USA, 2014.
38. Jones, L.D. *Examining the Forensic Artifacts Produced by Use of Bitcoin Currency*; ProQuest LLC.: Ann Arbor, MI, USA, 2014.
39. Koerhuis, W.; Kechadi, T.; Le-Khac, N.A. Forensic analysis of privacy-oriented cryptocurrencies. *Forensic Sci. Int. Digit. Investig.* **2020**, *33*, 200891. [CrossRef]
40. Montanez, A. *Investigation of Cryptocurrency Wallets on iOS and Android Mobile Devices for Potential Forensic Artifacts*; Department Forensic Science, Marshall University: Huntington, WV, USA, 2014.
41. Chang, E.; Darcy, P.; Choo, K.K.R.; Le-Khac, N.A. Forensic Artefact Discovery and Attribution from Android Cryptocurrency Wallet Applications. *arXiv* **2022**, arXiv:2205.14611.
42. Saudi, M.M. *An Overview of Disk Imaging Tool in Computer Forensics*; SANS Institute: Bethesda, MD, USA, 2001.
43. Yusoff, Y.; Ismail, R.; Hassan, Z. Common phases of computer forensics investigation models. *Int. J. Comput. Sci. Inf. Technol.* **2011**, *3*, 17–31. [CrossRef]
44. Nelson, B.; Phillips, A.; Steuart, C. *Guide to Computer Forensics and Investigations*; Cengage Learning: Boston, MA, USA, 2014.
45. Garfinkel, S.L. Digital forensics research: The next 10 years. *Digit. Investig.* **2010**, *7*, S64–S73. [CrossRef]
46. Richard, G.G., III; Roussev, V. Next-generation digital forensics. *Commun. ACM* **2006**, *49*, 76–80. [CrossRef]
47. Salamh, F.E.; Mirza, M.M.; Hutchinson, S.; Yoon, Y.H.; Karabiyik, U. What's on the Horizon? An In-Depth Forensic Analysis of Android and iOS Applications. *IEEE Access* **2021**, *9*, 99421–99454. [CrossRef]
48. Ahmed, R.; Dharaskar, R.V. Mobile forensics: an overview, tools, future trends and challenges from law enforcement perspective. In Proceedings of the 6th International Conference on E-Governance, Iceg, Emerging Technologies in E-Government, M-Government, New Delhi, India 18–20 December 2008; pp. 312–323.
49. Humphries, G.; Nordvik, R.; Manifavas, H.; Cobley, P.; Sorell, M. Law Enforcement educational challenges for mobile forensics. *Forensic Sci. Int. Digit. Investig.* **2021**, *38*, 301129. [CrossRef]
50. Brinson, A.; Robinson, A.; Rogers, M. A cyber forensics ontology: Creating a new approach to studying cyber forensics. *Digit. Investig.* **2006**, *3*, 37–43. [CrossRef]
51. Park, H.; Cho, S.; Kwon, H.C. Cyber forensics ontology for cyber criminal investigation. In Proceedings of the International Conference on Forensics in Telecommunications, Information, and Multimedia, Adelaide, Australia, 19–21 January 2009, Springer: Berlin/Heidelberg, Germany, 2009; pp. 160–165.
52. Fernando, V. Cyber forensics tools: A review on mechanism and emerging challenges. In Proceedings of the 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 19–21 April 2021; pp. 1–7.
53. Liang, G.; Xin, J.; Wang, Q.; Ni, X.; Guo, X. Research on IoT Forensics System Based on Blockchain Technology. *Secur. Commun. Netw.* **2022**, *2022*. [CrossRef]

54. Kasukurti, D.H.; Patil, S. Wearable device forensic: Probable case studies and proposed methodology. In Proceedings of the International Symposium on Security in Computing and Communication; Springer: Berlin/Heidelberg, Germany, 2018; pp. 290–300.
55. Stanković, M.; Mirza, M.M.; Karabiyik, U. UAV forensics: DJI mini 2 case study. *Drones* **2021**, *5*, 49. [CrossRef]
56. Iqbal, F.; Alam, S.; Kazim, A.; MacDermott, Á. Drone forensics: A case study on DJI phantom 4. In Proceedings of the 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), Abu Dhabi, United Arab Emirates, 3–7 November 2019; pp. 1–6.
57. Dimotikalis, P. *Memory Forensics and Bitcoin Mining Malware*; International Hellenic University: Thermi, Greece, 2016.
58. Mas'ud, M.Z.; Hassan, A.; Shah, W.M.; Abdul-Latip, S.F.; Ahmad, R.; Ariffin, A.; Yunos, Z. A Review of Digital Forensics Framework for Blockchain in Cryptocurrency Technology. In Proceedings of the 2021 3rd International Cyber Resilience Conference (CRC), Langkawi Island, Malaysia, 29–31 January 2021; pp. 1–6.
59. Ayers, R.; Livelsberger, B.; Guttman, B. *Quick Start Guide for Populating Mobile Test Devices*; Technical report; National Institute of Standards and Technology: Gaithersburg, MA, USA, 2018.
60. Ayers, R.P.; Brothers, S.; Jansen, W. *Guidelines on Mobile Device Forensics*; Technical Report; National Institute of Standards and Technology: Gaithersburg, MA, USA, 2014.
61. Google. Gmail: Free, Private & Secure Email | Google Workspace. Available online: https://www.google.com/gmail/about/ (accessed on 22 May 2022).
62. Apple. iCloud. Available online: https://www.icloud.com/ (accessed on 22 May 2022).
63. Google. Google Play. Available online: https://play.google.com/store (accessed on 22 May 2022).
64. TeamWin. TeamWin-TWRP. Available online: https://twrp.me/ (accessed on 23 May 2022).
65. Wu, J. Topjohnwu/Magisk: The Magic Mask for Android. Available online: https://github.com/topjohnwu/Magisk (accessed on 22 May 2022).
66. Hauser, E. UNIX Time, UTC, and datetime: Jussivity, prolepsis, and incorrigibility in modern timekeeping. *Proc. Assoc. Inf. Sci. Technol.* **2018**, *55*, 161–170. [CrossRef]
67. Apple. CFURL | Apple Developer Documentation. Available online: https://developer.apple.com/documentation/corefoundation/cfurl-rd7 (accessed on 10 September 2022).
68. MongoDB. Realm Home | Realm.io. Available online: https://realm.io/ (accessed on 8 October 2022).
69. CipherTrace. Cryptocurrency Intelligence and Blockchain Analytics—CipherTrace. Available online: https://ciphertrace.com/ (accessed on 9 October 2022).
70. Harris, R. Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. *Digit. Investig.* **2006**, *3*, 44–49. [CrossRef]
71. Garfinkel, S. Anti-forensics: Techniques, detection and countermeasures. In Proceedings of the 2nd International Conference on i-Warfare and Security, Monterey, CA, USA, 8–9 March 2007; Volume 20087, pp. 77–84.
72. Chabot, Y.; Bertaux, A.; Nicolle, C.; Kechadi, M.T. A complete formalized knowledge representation model for advanced digital forensics timeline analysis. *Digit. Investig.* **2014**, *11*, S95–S105. [CrossRef]
73. WebKit.WebsiteData—Webkit2gtk-4.0. Available online: https://valadoc.org/webkit2gtk-4.0/WebKit.WebsiteData.html (accessed on 10 September 2022).
74. Abrignoni. Abrignoni/ALEAPP: Android Logs Events And Protobuf Parser. Available online: https://github.com/abrignoni/ALEAPP (accessed on 17 September 2022).