Desktop Crypto Wallets: A Digital Forensic Investigation and Analysis of Remnants and Traces on end-User Machines

David Debono and Aleandro Sultana
Institute of Information and Communication Technology, Malta College of Arts, Science and Technology, Triq Kordin, Paola PLA9032, Malta

Keywords: Digital Forensic, Windows, Artefacts, Cryptocurrencies, Desktop Wallets.

Abstract: Cryptocurrencies have built-in anonymity and privacy features. These currencies can be used for illicit activities, and due to the nature of cryptocurrencies, it is difficult for forensic investigators to extract concrete proof and evidence from a seized system, that such wallets have been used for criminal activities. Evidence heavily depends on the status of the application, whether it is present on the system or has been recently uninstalled. In this study, we examine three mainstream desktop wallet cryptocurrencies Exodus, Electrum and Bitcoin Core and investigate which valuable forensic artefacts the software of these cryptocurrencies leaves behind on a Windows 10 computer system during the different phases of the application lifetime. Volatile and non-volatile memory as well as network traffic are examined. Artefacts included hidden files created from the wallet applications, roaming profiles, application directories, and cached browser history. Artefacts present in volatile memory included personal bank details, seed phrases, wallet names and plain text passwords. The network traffic generated was used to extract DNS records and IP addresses. Roaming profiles were still present after the uninstallation of the wallet applications Exodus and Bitcoin Core and passwords related to Bitcoin Core were found in volatile memory after the uninstallation process, before restarting the system.

1 INTRODUCTION

Cryptocurrencies, often referred to as "crypto", represent a form of digital or virtual currency that relies on cryptography for security. Unlike traditional fiat currencies issued and regulated by governments, cryptocurrencies operate on decentralized networks, which are independent of any central control by a financial or government institution (Bunjaku et al., 2017). The applications of cryptocurrencies are extensive and diverse. They have transformed the way we think about finance, by offering secure, efficient, and borderless transactions. Cryptocurrencies are used for various purposes, including online purchases, cross-border remittances, investment, and even as a store of value similar to gold. Moreover, blockchain, the technology on which cryptocurrencies are based, has far-reaching implications in industries beyond finance, such as supply chain management, healthcare, and voting systems (Mahabub et al., 2022). The technology can help in increasing transparency, reducing fraud, and improve efficiency (Issaoui et al.)

The proliferation of cryptocurrencies has raised concerns regarding their misuse for illicit activities. These activities include money laundering, tax evasion, the purchase of illegal goods and services on the dark web, ransomware attack payments and the injection of arbitrary encoded data chunks (for instance, pictures) in non-standard transactions (Tziakouris, 2018). These applications, which are designed to provide secure storage for cryptocurrencies, can also be exploited by individuals seeking anonymity in their financial transactions. This misuse poses challenges for law enforcement agencies and regulatory bodies in monitoring and preventing illegal activities. Striking a balance between user privacy and the prevention of illicit activities remains a significant challenge in the cryptocurrency realm (Dyson et al., 2018).

This work examines whether valuable artefacts residing on a Windows 10 local machine, created from desktop wallet cryptocurrency applications, can be retrieved after the said applications are uninstalled from a system. In the process it also examines the contents of volatile and non-volatile memory,

Debono, D. and Sultana, A.
Desktop Crypto Wallets: A Digital Forensic Investigation and Analysis of Remnants and Traces on end-User Machines.
DOI: 10.5220/0012313000003648

In *Proceedings of the 10th International Conference on Information Systems Security and Privacy (ICISSP 2024)*, pages 350-357
ISBN: 978-989-758-683-5; ISSN: 2184-4356

together with captured network traffic during the different phases of the applications' lifetime, including installation, creation of wallets and execution of peer-to-peer transactions. The aim is to determine whether any forensic evidence that could stand the test in court against illicit activity can be retrieved, depending on the state of the machine and the wallet application. Our contributions are the following:

- We present a digital forensic methodology for examining disk, memory and network traffic for three mainstream crypto desktop wallet applications Exodus, Electrum and Bitcoin Core installed on a Windows 10 machine.
- We provide an analysis of the information that can be retrieved from volatile, non-volatile and network traffic for the aforementioned applications during the different phases, including post-installation, after the creation of a new wallet, and after performing peer-to-peer transactions.
- We present a list of the location and content of artefacts and remnants that are present on a system after a desktop crypto wallet application is removed from a system and the system is restarted, simulating a typical criminal scenario.

This paper is organized as follows: Section 2 presents related work. Section 3 explains the methodology while Section 4 discusses the data analysis and results. Conclusions and future work are presented in Section 5 and 6 respectively.

2 RELATED WORK

The rise of cryptocurrencies over the past ten years has prompted researchers to pursue studies investigating the privacy of this technology. Throughout the years, cryptocurrencies have been affected by an increase in illegal activities due to their decentralized and pseudonymous nature, creating difficulties in tracing the source of funds related to money laundering, dark net transactions, ransomware attacks, tax evasions, fraud, and scams. This has also brought about an increase in research related to digital forensic investigation approaches that can be used against persons committing such crimes (Dudani et al., 2023).

In his work, Kovalcik (2022) constructs a scanning tool for forensic analysis of cryptocurrency wallets artefacts, based on the Linux operating system. The author made use of Python 3.8 on Ubuntu 20.04, to obtain various information from two distinct wallets, Exodus and Electrum. Throughout his findings, the author explains how the two applications differ from each other. Whilst the Exodus wallet did not reveal its configuration in its default settings where everything was stored in binary format, the Electrum wallet kept its configuration in JSON format and unencrypted. The paper also presents public and private keys along with addresses and personal information, which could be obtained from both wallets.

Adopting a similar memory forensic approach, Thomas et al. (2020) conducted memory forensics on hardware cryptocurrency wallets by first downloading the Ledger Live desktop client and installing it without changing the default USB drivers installed by Windows. This was accompanied by the installation of the Trezor wallet. 'Cheat Engine', a real-time memory analysis and debugging tool, was then used to observe Trezor wallet and Ledger Live processes during run time. Finally, the main tool named 'FORESHADOW', a volatility plugin for extracting forensically relevant data, was implemented. The Ledger Live process memory contained device information and preference settings such as the Model ID, region, application version, language, and OS version. The extended public keys were also obtained along with the full transaction balance, history address path and derivation path. Using Firefox and Chrome data including encrypted passphrase, unique device ID, version numbers, boot loader hash, boot loader, device firmware, model ID and all extended public keys from the Trezor wallet, were obtained.

Ngwu (2021) investigates and compares six different desktop wallets in his methodology. The wallets used were MultiBit HD, Electrum, mSIGNA, Bither, Armory and Bitpay. The study utilized the digital tools "OS Forensics Tool" and "Magnet RAM capture". RAM capture and memory analysis of the App data path folder, backup files, executable files, log files, registry files and program files were carried out against several snapshots taken at different stages of the investigation. All tests were performed on a Windows 10 virtual machine. The study concluded that confidential data including the remnant data of the different wallets, unique wallet addresses, encrypted passwords, wallet history and proof that the wallets had been uninstalled from the machine, could be obtained.

Koerhuis and Le Khac (2020) conducted a desktop-wallet forensic investigation dedicated specifically to the Monero and Verge software applications. Using an Ubuntu and a MacOS High Sierra operating system, the authors analysed a series of snapshots taken during the different stages of their methodology. Network traffic capture and analysis via Wireshark, volatile memory image analysis and disk analysis, were all performed.

Their findings concluded that wallet passphrases in ASCII and UTF-16, along with the public addresses of the wallets, full payment ID and transaction ID's of earlier transactions, transaction ID of incoming transactions with amount in XMR, public addresses of earlier receiving party, full payment ID of earlier transaction and both created labels could be obtained through the seven memory images taken. More importantly, when it came to the Monero network traffic, many indicators confirmed that a wallet is present and running, including the related DNS traffic, traffic that looks like blockchains due to its block hashes, and the public donation address of the Monero project. However, no forensic artefacts related to network traffic were found on the Verge wallet software.

Hirwani et al. (2012) created an automated tool named 'WinBAS', that automatically performs a forensic investigation and artefact search for Bitcoin Clients and Bitcoin Web Wallets. The authors tested their tool on 9 different Bitcoin clients during different phases of usage of the applications. They also used the tool to analyse evidence found in three different web browsers when using web wallets. They conclude that it is crucial to analyse evidence in RAM, pagefile.sys and hiberfil.sys. The authors present a list of the evidence found. Doran (2015) presents the location and files present when Bitcoin-Qt is installed on a machine and the details of possible data that can be extracted.

3 METHODOLOGY

For this research, the desktop wallets Exodus, Bitcoin Core and Electrum were used. The research pipeline depicted in Figure 1 was utilized for this study.

3.1 Phase 1

For this phase, the software listed in Table 1 were used.

Through VMware® Workstation 16 Pro, three virtual machines with a Windows 10 Home 64-Bit operating system were created, one for each wallet. A local user account was also created along with a valid email address for each Windows 10 machine together with a standard password and a pin.

Table 1: Software List.

Software	Version
VMware® Workstation 16 Pro	16.0.0 build-16894299
Windows 10 Home 64-Bit	2023-04 22H2
Exodus	23.8.28
Bitcoin Core	v22.0.0
Electrum	v4.4.6

For each virtual machine the latest cumulative update (2023-04 22H2) was installed to have the latest features, bug fixes and security patches.

Following this, Windows updates were paused to ensure that no system changes occur during the implementation of the methodology. The option 'only save local data' was selected and the OneDrive cloud storage feature was disabled and uninstalled, enabling only data to be saved locally. At this stage, a virtual machine snapshot named 'P1-Test' was taken and added to the snapshot manager.

Access Data FTK Imager 4.7.1.2, was used to acquire and analyse digital evidence. The tool was used to take an image of the full logical hard disk of each virtual machine and preserve the data in its original form, enabling the data to be investigated at a later stage without losing its integrity. FTK was directed to the VM's path where the snapshot named 'P1-Test' from Phase 1, was located. The tool converted the .vmdk files to raw/dd format. The application converts the snapshot along with any previous snapshots taken and the base vmdk files (Hirwani et al., 2012).

3.2 Phase 2

On all three virtual machines, 'Wireshark' was installed to capture network traffic. All captured data was saved to an external storage location. In addition, Browser History Examiner (BHE) was installed locally on the machines, along with Magnet Ram Capture (MRC).

The Desktop wallet applications for each virtual machine were then installed accordingly. Wireshark, BHE and MRC were used to acquire forensic data. The acquired data was named 'P2-Test'. At this stage, another snapshot with the name 'P2-Test', using VMware Workstation was taken along with a Raw Image via the FTK Imager.

3.3 Phase 3

This phase involved the creation of wallet accounts on each machine and simulating different types of transactions. All transactions were conducted using a very small amount of money. Wallet desktop applications differ in their functionality and a slightly different approach was taken for each different application.

3.3.1 Exodus

For Exodus, Wireshark was started on the local area network card along with the Exodus application. The latest update of Exodus 23.5.22 was installed. By default, a strong password for login purposes and a recovery phrase were enforced. The recovery phrase is used to recover the funds in case the machine crashes since all private keys in Exodus are generated from and tied to the 12-word recovery phrase.

A new portfolio under the name of 'Exodus' was generated. Through ramp, which is a secure payment system that makes it simple to buy crypto, 0.21691771 worth of SOL equivalent to €6.50, which is Solana's native cryptocurrency, were acquired through a secure Revolut payment. During the process, the email address associated with the machine 'exodusAs2023@outlook.com' also needed to be verified along with a confirmation code. Card details and a valid billing address were also inserted along with an Identity Card and a selfie image for verification purposes. After the verification process, the Solana wallet address was given as a code along with the card details used, whilst prompting to confirm the payment on the Revolut application and inserting the CSV on another pop up.

At this stage, a transaction was conducted to simulate illegal activity. The amount of 0.01 SOL, equivalent to €0.18, were sent to the external Exodus Solana address, 'HiEuKEYCyEhEKucNWyHsaGA-HUTbrUYW9dksg5KEPEtrU'. SOL crypto amount was deducted immediately with a transaction record populating in the Activity Section.

The Wireshark application was stopped, and the previous ongoing activity was saved externally along with BHE and MRC data files. A snapshot via the VMWare snapshot manager was also acquired. Using the Access Data FTK Imager an image of the current state of the machine was taken. All data files were named 'P3BR-Test'.

The machine was rebooted and all forensic applications, excluding Wireshark, were used to capture data under the name 'P3AR-Test'.

3.3.2 Electrum

By default, the Electrum crypto wallet application displaces Bitcoin value in mBTC, however, this was immediately changed to BTC. Unlike Exodus, the Electrum crypto wallet application does not support the process of buying and selling cryptocurrency with an easy accessable purchasing and sales option.

The Receive Bitcoin technique was used. Through the Receive tab, 0.0001 BTC were requested along with a description and an expiry time of one hour. After pressing the request button, a BTC address was generated. Through an external Exodus cryptocurrency wallet application, the 0.0001 BTC requested by the Electrum application were sent successfully by inserting the generated BTC address. Immediately after the transaction was conducted, the amount of BTC appeared in the Electrum application.

Shortly after the transaction was acknowledged and received, a transaction sent from the Electrum wallet application was conducted to the same external Exodus wallet. This time the same amount of 0.00001 BTC was sent together with an expiry time of one hour. The transaction was completed successfully in a short amount of time.

Like in the Exodus case, the same forensic tools were used to capture data before and after reboot.

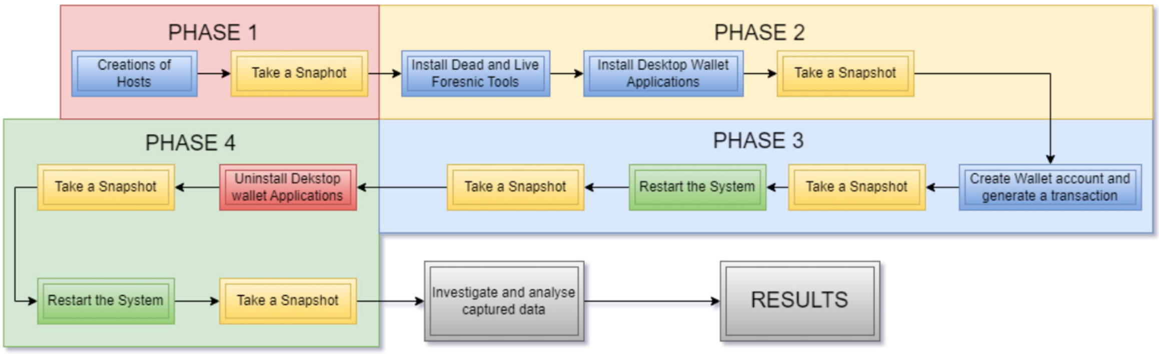

PHASE 1
Creations of Hosts
Take a Snaphot
PHASE 2
Install Dead and Live Foresnic Tools
Install Desktop Wallet Applications
Take a Snapshot
PHASE 3
Create Wallet account and generate a transaction
Take a Snapshot
Restart the System
Take a Snapshot
PHASE 4
Uninstall Dekstop wallet Applications
Take a Snapshot
Restart the System
Take a Snapshot
Investigate and analyse captured data
RESULTS

Figure 1: Research Pipeline.

3.3.3 Bitcoin Core

Electrum and Bitcoin Core operate in a similar manner and have similar GUI's. The Bitcoin Core application was initiated after synchronizing the whole blockchain network and creating an encrypted wallet. A name for the wallet along with a strong password were chosen. The password can recover the wallet accounts associated with the Bitcoin Core application.

Similar to Electrum, the Receive Bitcoin technique was used. Through the Receive tab of the Bitcoin core application, '0.00034954' of BTC were requested. The generate Native SegWit (Bech32) address along with a label to identify between different transactions and a message were entered. After clicking on the request button, a BTC address was generated. Through the Exodus application used in the Electrum phase, the request from Bitcoin core was sent successfully. In Bitcoin core, transactions are received and verified through a process called transaction validation. Once a transaction is validated, it gets added to the blockchain through an agreement among the network's nodes.

Immediately after the funds were approved and added to the wallet, a send transaction was conducted to the same Exodus wallet address. The amount of '0.00034954' was sent along with a fee of '0.00020080' of BTC. Unlike the Electrum application, there is no expiry time.

The same procedure used for Exodus & Electrum for data collection before and after rebooting of the machine was performed.

3.4 Phase 4

During this phase the same procedure was used for all three applications. After initiating the Wireshark application, each desktop wallet application was uninstalled through the Control Panel. After successfully uninstalling the crypto wallet, BHE and MRC images were taken. An image via FTK imager was also acquired. All the data files were saved to an external device and named 'P4BR-Test'.

All virtual machines were rebooted and final images using BHE, MRC and FTK imager were acquired using the name 'P4AR-Test'.

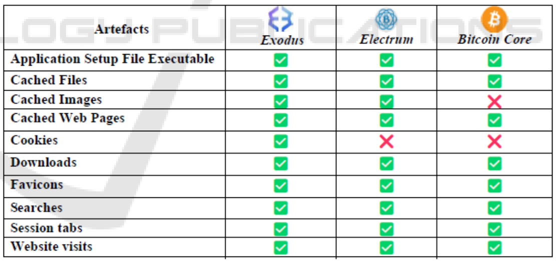
4 DATA ANALYSIS AND RESULTS

All images for volatile and non-volatile memory obtained during the different phases of the methodology were examined using Autopsy 4.20.0, Magnet Axiom Process 5.4.0.2 and Magnet Axiom Examine 5.4.0.2. For integrity purposes, the hashes of these images were verified with the original hashes of the virtualized snapshots. Artefacts were identified using automated string searches and manual searches using the keywords *Address, Amount, Bitcoin, Bitcoin Core, Btc, Electrum, Exodus, ID, Label, Message, Name, Password, Requested, Seed, Sent, Transaction, Username* and *Wallet*. Manual analysis was also performed on BHE and Wireshark data.

4.1 Phase 2

Figure 2 presents the data found through BHE for each wallet for Edge Browser. Session tabs and the downloads folder contained the application setup file executables, together with the bytes downloaded, start time of the application being downloaded and end time. The state 'confirmed' was found on all applications confirming that all applications were installed successfully.

For each desktop wallet, data in the non-volatile memory images included registry entries, installation path files and windows log files. Although all data present in the network traces was encrypted, through analysis of DNS records and IP addresses, it was possible to detect the installation of all three applications.



Artefacts	Exodus	Electrum	Bitcoin Core
Application Setup File Executable	✓	✓	✓
Cached Files	✓	✓	✓
Cached Images	✓	✓	✗
Cached Web Pages	✓	✓	✓
Cookies	✓	✗	✗
Downloads	✓	✓	✓
Favicons	✓	✓	✓
Searches	✓	✓	✓
Session tabs	✓	✓	✓
Website visits	✓	✓	✓

Figure 2: BHE Forensic Data.

4.2 Phase 3 (Before Reboot)

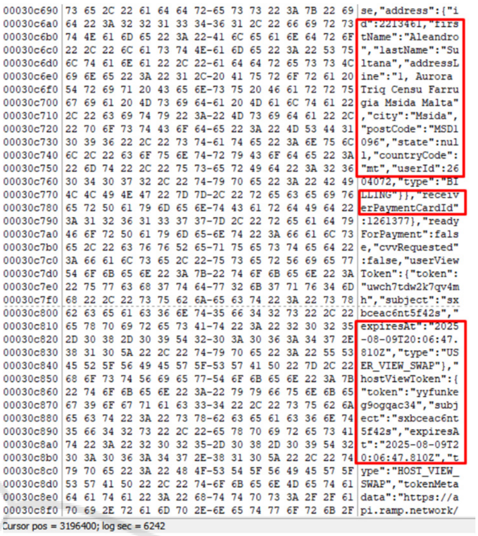
For both the Electrum and Bitcoin core desktop wallet applications, no additional browser history artefacts were found. For the Exodus wallet application, Browser History revealed new artefacts. The Ramp Network URL 'https://buy.ramp.network' was retrieved along with Fav Icons, cached files, session tabs and host API key. This confirmed that the ramp network was used. More importantly, through cached web images, the number of Euro paid (6.50), the type of Crypto bought (SOL) and the amount exchanged for the euro rate of SOL (0.176) were identified.

With regards to disk artefacts, for the Exodus Wallet, wallet data was found under '\Users\exodu\AppData\Roaming\Exodus\exodus.wallet' path. The folder contained the files 'info.seco', 'seed.seco', 'storage.seco', 'twofactor-secret.seco' and the 'twofactor.seco'. All data present inside the files was encrypted. A 'local state' file under the roaming Exodus folder was discovered, with just 389 bytes. The file contained an encrypted key which was used for the transactions.

For the Electrum wallet, wallet type (file), name (maltatesting_Electrum_wallet) and size in bytes (5148) were found under 'Users\elect\AppData\Roaming\Electrum\wallets'. The data inside the wallet, which includes private keys and wallet seed were all encrypted since the wallet was marked 'encrypted' during installation. Through the 'Windows Timeline Activity' section in Axiom Examine, the start and end times of the Electrum application were obtained. This confirmed that the application was used for approximately 38 minutes. Similar artefacts were obtained for the Bitcoin wallet application. Bitcoin wallet data was found under 'Users\bitco\AppData\Roaming\Bitcoin\wallets\MaltaTesting2023!'. Files present included the '.walletlock', which removes the wallet encryption key from memory, locking the wallet, the 'db.log' which holds all logs for the current wallet and the 'wallet.dat' which holds the personal wallet (BDB) with keys and transactions. Since the encryption option for the Bitcoin wallet was marked during the installation phase, all data was encrypted.

Wireshark traces were obtained during the creation of wallets and transactions. For Exodus, DNS records pointed directly to several crypto domains including the 'SOL' crypto which was used to conduct a send transaction, 'FIAT', 'MARLEY-P' and 'GETH'. Similar data was observed for the Electrum wallet. For the Bitcoin Core Application, the 'inv' message, which appears in the block inventories, containing hash blocks along with the 'getdata' message, which the IBD node uses during the received inventories to request 128 blocks from the sync node, were present. During transactions 'TX' messages were identified together with 'TCP' and 'Bitcoin' messages. Similar to Exodus and Electrum, All Data Was Encrypted.

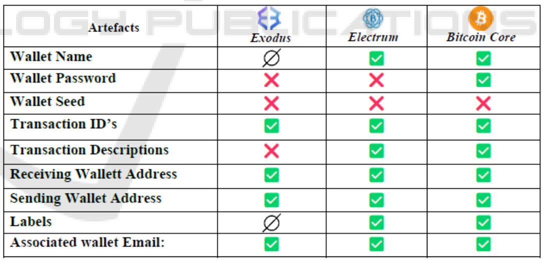
Since the Exodus Application Wallet Allowed to Buy and Sell Cryptocurrencies Using Ramp, Memory Forensics Revealed Card Details in Plain Text. However, Some Numerical Numbers of the Card Number Used Were Hashed Along with the Card Security Code. Type of Payment, Email, Full Address, Country, First Name, Last Name, Postcode, User Id, Token, Expiry Dates, Expiry Card Date, the Amount of Fiat Currency (Euro) Paid to Exchange the Sol Currency and Timestamps Were Extracted.



```
00030c690  73 65 2C 22 61 64 64 72-65 73 73 22 3A 7B 22 69  se,"address":{"i
00030c6a0  64 22 3A 32 32 31 33 34-36 31 2C 22 66 69 72 73  d":2213461,"firs
00030c6b0  74 4E 61 6D 65 22 3A 22-41 6C 65 61 6E 64 72 6F  tName":"Aleandro
00030c6c0  22 2C 22 6C 61 73 74 4E-61 6D 65 22 3A 22 53 75  ","lastName":"Su
00030c6d0  6C 74 61 6E 61 22 2C 22-61 64 64 72 65 73 73 4C  ltana","addressL
00030c6e0  69 6E 65 22 3A 22 31 2C-20 41 75 72 6F 72 61 20  ine":"1, Aurora 
00030c6f0  54 72 69 71 20 43 65 6E-73 75 20 46 61 72 72 75  Triq Censu Farru
00030c700  67 69 61 20 4D 73 69 64-61 20 4D 61 6C 74 61 22  gia Msida Malta"
00030c710  2C 22 63 69 74 79 22 3A-22 4D 73 69 64 61 22 2C  ,"city":"Msida",
00030c720  22 70 6F 73 74 43 6F 64-65 22 3A 22 4D 53 44 31  "postCode":"MSD1
00030c730  30 39 36 22 2C 22 73 74-61 74 65 22 3A 6E 75 6C  096","state":nul
00030c740  6C 2C 22 63 6F 75 6E 74-72 79 43 6F 64 65 22 3A  l,"countryCode":
00030c750  22 6D 74 22 2C 22 75 73-65 72 49 64 22 3A 32 36  "mt","userId":26
00030c760  30 34 30 37 32 2C 22 74-79 70 65 22 3A 22 42 49  04072,"type":"BI
00030c770  4C 4C 49 4E 47 22 7D 7D-2C 22 72 65 63 65 69 76  LLING"}},"receiv
00030c780  65 72 50 61 79 6D 65 6E-74 43 61 72 64 49 64 22  erPaymentCardId"
00030c790  3A 31 32 36 31 33 37 37-7D 2C 22 72 65 61 64 79  :1261377},"ready
00030c7a0  46 6F 72 50 61 79 6D 65-6E 74 22 3A 66 61 6C 73  ForPayment":fals
00030c7b0  65 2C 22 63 76 76 52 65-71 75 65 73 74 65 64 22  e,"cvvRequested"
00030c7c0  3A 66 61 6C 73 65 2C 22-75 73 65 72 56 69 65 77  :false,"userView
00030c7d0  54 6F 6B 65 6E 22 3A 7B-22 74 6F 6B 65 6E 22 3A  Token":{"token":
00030c7e0  22 75 77 63 68 37 74 64-77 32 6B 37 71 76 34 6D  "uwch7tdw2k7qv4m
00030c7f0  68 22 2C 22 73 75 62 6A-65 63 74 22 3A 22 73 78  h","subject":"sx
00030c800  62 63 65 61 63 36 6E 74-35 66 34 32 73 22 2C 22  bceac6nt5f42s","
00030c810  65 78 70 69 72 65 73 41-74 22 3A 22 32 30 32 35  expiresAt":"2025
00030c820  2D 30 38 2D 30 39 54 32-30 3A 30 36 3A 34 37 2E  -08-09T20:06:47.
00030c830  38 31 30 5A 22 2C 22 74-79 70 65 22 3A 22 55 53  810Z","type":"US
00030c840  45 52 5F 56 49 45 57 5F-53 57 41 50 22 7D 2C 22  ER_VIEW_SWAP"},"
00030c850  68 6F 73 74 56 69 65 77-54 6F 6B 65 6E 22 3A 7B  hostViewToken":{
00030c860  22 74 6F 6B 65 6E 22 3A-22 79 79 66 75 6E 6B 65  "token":"yyfunke
00030c870  67 39 6F 67 71 61 63 33-34 22 2C 22 73 75 62 6A  g9ogqac34","subj
00030c880  65 63 74 22 3A 22 73 78-62 63 65 61 63 36 6E 74  ect":"sxbceac6nt
00030c890  35 66 34 32 73 22 2C 22-65 78 70 69 72 65 73 41  5f42s","expiresA
00030c8a0  74 22 3A 22 32 30 32 35-2D 30 38 2D 30 39 54 32  t":"2025-08-09T2
00030c8b0  30 3A 30 36 3A 34 37 2E-38 31 30 5A 22 2C 22 74  0:06:47.810Z","t
00030c8c0  79 70 65 22 3A 22 48 4F-53 54 5F 56 49 45 57 5F  ype":"HOST_VIEW_
00030c8d0  53 57 41 50 22 2C 22 74-6F 6B 65 6E 4D 65 74 61  SWAP","tokenMeta
00030c8e0  64 61 74 61 22 3A 22 68-74 74 70 73 3A 2F 2F 61  data":"https://a
00030c8f0  70 69 2E 72 61 6D 70 2E-6E 65 74 77 6F 72 6B 2F  pi.ramp.network/
Cursor pos = 3196400; log sec = 6242
```

Figure 3: Exodus Card Details.

Figure 4 Presents a Summary of the Artefacts Obtained for the Three Wallet Applications During This Phase.



Artefacts	Exodus	Electrum	Bitcoin Core
Wallet Name	∅	✓	✓
Wallet Password	✗	✗	✓
Wallet Seed	✗	✗	✗
Transaction ID's	✓	✓	✓
Transaction Descriptions	✗	✓	✓
Receiving Wallett Address	✓	✓	✓
Sending Wallet Address	✓	✓	✓
Labels	∅	✓	✓
Associated wallet Email:	✓	✓	✓

Figure 4: Phase 3 non-Volatile Memory Artefacts.

4.3 Phase 3 (After Reboot)

After Reboot no Changes Were Observed in Browser History and Local Artefacts. also, no Additional Artefacts Were Present Through the Analysis of the Running Memory and Network Captures.

4.4 Phase 4 (Before Reboot)

After removing the wallet applications, browser-related history remained the same. All historical data in the previous images was still present.

After application removal, the Exodus wallet application was not visible in the installed programs, neither through the Axiom Examine or Autopsy. Autopsy could not locate any deleted folders or files related to Exodus. The application was also not available from the Windows search, the desktop, or any visible folder on the hard drive. However hidden folders located in the roaming profile '/Users/exodu/AppData/Roaming/Exodus' and containing data identical to that found in previous tests, was present. Remnants included wallet name, info seed, storage files, two-factor files and network files. In addition to the previous tests, database '.db' files were discovered under the local storage folders. Data residing in the LOCK, LOG and CURRENT database files was encrypted. The contents in the CURRENT database file holding records of the transactions done were also encrypted. However, full metadata and timestamps of transactions were available. Cached folders and files including 'Code Cache', 'Dawn Cache', and 'Cache' were also present. The OS-encrypted Exodus key was also found in the local state file. Although all the data was encrypted, these artefacts confirmed that the wallet application was present along with an active wallet.

For the Electrum wallet, the Autopsy 'Deleted Files' section marked the Electrum application as deleted along with other '.ink' and '.mo' file types. More importantly, metadata contained the created time, access time, change time and modified time stamps indicating the exact time at which the application was removed. All hex data inside the deleted files contained unreadable information. In the '/Users/elect/AppData/Roaming/Electrum' directory, data related to the Electrum wallet was obtained through file carving. Several folders and files were extracted including the wallet name residing in the 'wallets' folder, confirming that although the wallet application was not present on the local machine, traces of crypto wallets were still present. In the same directory, a readable file called 'recent servers', contained the public IP's '34.136.93.37' and '94.23.247.135' with the corresponding port numbers and DNS names. This file contained information about the servers that the Exodus application communicated with.

For the Bitcoin Core wallet application, unlike Electrum, the application was not present in the 'deleted' section of Autopsy. Bitcoin Core did not feature under the 'Installed Applications' section, meaning that the application was not present on the Windows 10 local machine and neither under the program files where the application used to reside. However, artefacts related to the Bitcoin Core wallet residing in the roaming profile '/Users/bitco/AppData/Roaming/Bitcoin/', were found. These consisted of the wallet folder and name, peers file, mempool file, block, and index folder. Although folders, files and wallet names were present, all data residing in the files was encrypted and not readable. The only data that Autopsy tagged as 'Deleted files' relating to the Bitcoin Core was the 'Block Data', which is used to record some, or all the recent transactions conducted.

Wireshark was unable to capture any packets related to Bitcoin Core application during uninstallation. For the Exodus and Electrum applications, identical public IP's as well as DNS records, similar to the once present in previous tests, were obtained.

In volatile memory, passphrases to login into the wallet application were found only for the Bitcoin Wallet application. For all applications, wallet names were located, however no additional remnants related to Transaction ID's and Seeds were available.

4.5 Phase 4 (After Reboot)

For all the desktop wallet applications, all data related to the browser history and local artefacts remained the same. Volatile memory revealed the name of the roaming paths for all three wallets.

5 CONCLUSIONS

The methodology presented in this study has shown to be effective in retrieving artefacts related to crypto wallets. Moreover, the work highlights the importance of the exact time forensic investigators perform collection of evidence. From the analysis it is evident that digital artefacts differ in presence and amount depending on the status of the application, whether the wallet has been created, transactions have been performed, or the applications have been used and removed. A difference in the recoverable data from volatile memory was also noticed when an application was uninstalled, before and after a reboot.

One of the most difficult scenarios that investigators are faced with is when the application has been completely uninstalled from the system and a shutdown was performed. At this stage, it was observed that unless manually cleared, browser history could serve as evidence of wallet usage, including relevant timestamps of application usage and transactions performed. From the tests performed, both Exodus and Bitcoin Core wallet left important artefacts in their respective roaming profiles. This could help in identifying the usage history of the wallets. For Exodus, important transaction metadata was present after removing the application whilst Bitcoin Core left behind traces suggesting the use of the wallet. After uninstalling and before rebooting, passphrases for Bitcoin Core were present in volatile memory. Artefacts for Electrum were only available through file carving. From the study, it is also evident that search terms play a vital role in discovering evidence and a longer list of terms together with a detailed manual search, led to more artefacts than reported in the studies of Ngwu (2021), Koerhuis (2020) and Doran (2015).

6 FUTURE WORK

Future work should include the testing of other prominent desktop wallet applications available on the market, such as Hive, Armory, Bitpay, Bitcoin-QT and MultiBit. Installation and analysis of these wallets should also be tested on different operating systems, including MAC OS and Linux operating systems. Remnants and traces from the different operating systems should be compared with each other along with the other wallet applications. Attempts to decrypt the artefacts found should be done using the techniques identified in the literature review, since the data from all desktop wallet applications was encrypted. The wallet applications that support unencrypted wallets should also be tested and remnants should be compared to the same encrypted wallets, differentiating between their content.

REFERENCES

F. Bunjaku, O. Gjorgieva-Trajkovska, E. Miteva-Kacarski (2017). *Cyptocurrencies - Advantages and Disadvantages* Journal of Economics, Vol. 2, No. 1, pp. 31-39. doi: 10.46763/JOE.

B. S. Mahabub, M. Kethan, V. Karumuri, S. K. Guha, A. Gehlot and D. Gangodkar (2022). *Revolutions of Blockchain Technology in the Field of Cryptocurrencies* 11th International Conference on System Modeling & Advancement in Research Trends (SMART), Moradabad, India, pp. 761-764, doi: 10.1109/SMART55829.2022.10047225.

G. Tziakouris (2018). *Cryptocurrencies - A Forensic Challenge or Opportunity for Law Enforcement? An INTERPOL Perspective* IEEE Security & Privacy, vol. 16, no. 4, pp. 92-94, doi: 10.1109/MSP.2018.3111243.

S. Dyson, W. J. Buchanan, L. Bell (2018). *The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime* The Journal of The British Blockchain Association, 1(2), 5779, doi: arXiv:1907.12221v1.

S. Dudani, I. Baggili, D. Raymond, R. Marchany (2023). *The current state of cryptocurrency forensics* Forensic Science International: Digital Investigation, Volume 46, https://doi.org/10.1016/j.fsidi.2023.301576.

T. Kovalcik (2022). *Digital forensics of cryptocurrency wallets* Dissertation. https://www.diva-portal.org/smash/get/diva2:1671204/FULLTEXT02

T. Thomas, M. Piscitelli, I. Shavrov, I. Baggili (2020). *Memory FORESHADOW: Memory FOREnSics of HArDware CryptOcurrency wallets – A Tool and Visualization Framework* Forensic Science International: Digital Investigation, Volume 33, Supplement, https://doi.org/10.1016/j.fsidi.2020.301002.

C. Ngwu (2021). *Digital Forensic Investigation and Analysis of Bitcoin Wallets: Data Remnants and Ttraces on User Machines* Umudike Journal of Enegineering and Technology, vol. 7.

W. Koerhuis. and N. Le-Khac (2020). *Forensic analysis of privacy-oriented cryptocurrencies* Digit. Investig. 33: 200891.

M. Hirwani, Y. Pan, B. Stackpole, D. Johnson (2012). *Forensic Acquisition and Analysis of VMware Virtual Hard Disks*, https://scholarworks.rit.edu/cgi/viewcontent.cgi?article=1300&context=other.

S. Zollner, K. -K. R. Choo and N. -A. Le-Khac (2019). *An Automated Live Forensic and Postmortem Analysis Tool for Bitcoin on Windows Systems* in IEEE Access, vol. 7, pp. 158250-158263, doi: 10.1109/ACCESS.2019.2948774.

M. Doran (2015). *A Forensic Look at Bitcoin Cryptocurrency* SANS Institute. Available: https://www.sans.org/white-papers/36437/

Y. Issaoui, A. Khiat, A. Bahnasse, H. Ouajji (2019). *Smart logistics: Study of the application of blockchain technology* in Procedia Computer Science, vol. 160, pp. 266-271, doi: 10.1016/j.procs.2019.09.467.