Acquisition and Analysis of Digital Artefacts from Cryptocurrency Wallets: Their Role in forensic Investigations

(Proposal for Masters project which is currently in progress)

Grade: A

ABSTRACT

Context
Criminals rely on the pseudo-anonymous functionality of cryptocurrency to carry out their illegal activities. Digital forensic investors are tasked with removing this anonymity and link them to the crime.

Aim
The work suggested in this report will investigate the cryptocurrency wallet artefacts available for a forensic investigation. Delivering a replicable methodology and visualisation technique that enables investigators to utilise the information obtained from the artefacts.

Method
Each cryptocurrency wallet will lie on one of three windows 10 virtual machines. Transactions will be carried out on these machines to populate the virtual machine environment with artefacts. An image will be taken of each virtual machine and transferred to a Kali Linux workstation for analysis. A methodology will be created in tandem with the analysis, which will include a new visualisation technique to be used by investigators.

Anticipated Results
This report is expected to yield a significant number of digital artifacts that provide additional insight to cryptocurrency transactions. These artefacts will encompass *wallet ID's, transaction ID's, names, geographical locations, passwords, and seed phrases.* The analysis aims to uncover the connections that these digital artefacts have to the criminal's utilising cryptocurrency for cybercrime.

Keywords
Cryptocurrency Wallets, Forensics, Investigation, ransomware, visualisation, methodology

1. INTRODUCTION
Understanding the functionality of cryptocurrency is essential in developing an applicable methodology for digital forensic investigations of crypto-related cybercrime.

1.1 Decentralisation
Decentralisation is a fundamental characteristic of cryptocurrency and is the process of distributing power amongst a network of participants (Suratkar, Shirole and Bhirud, 2020). This distribution is to negate one party having entire control, contrary to traditional, monitored financial structures with governing bodies. This lack of governance enables cryptocurrency to be used without regulation, thus creating different methods for monetary transactions.

1.2 Transactions
Decentralisation creates a layer of anonymity for each transaction. This anonymity can be utilised by cybercriminals who often assume cryptocurrency transactions are entirely untraceable. However, this is a misconception. When performing a transaction, two corresponding parties will each have a cryptocurrency address that will send and receive payment. Once a transaction takes place, it is registered in the blockchain. The blockchain acts as a public ledger and therefore will record each payment, for anyone to view. When investigators are attempting to connect a criminal to illegal payments, understanding technical processes to uncover additional information about these transactions could be vital to a successful investigation. Figure 1 highlights some of the public information about a transaction. Each ID will be made up of a long string formed of letters and numbers, providing pseudo-anonymity.

Example Transaction Record	
Sender ID	1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX
Recipient ID	*3J98t1WpEZ73CNmQviecmyiWmqRhWNLy*
Transaction ID	*d5d27987d2a3dfc724e359870c6644b40e497bdc0589a033220fe15429d88599*
Amount	0.03 BTC

[Figure 1 : Example Transaction Record]

1.3 Wallets
The payment for each transaction is stored within cryptocurrency wallets. These wallets are electronic storage for different types of cryptocurrencies. Some forms of these wallets are as follows: Hardware Wallets, that often resemble a USB or hard drive. Application wallets - software downloaded from vendors. And finally, web wallets that are often in the form of browser extensions. The chosen wallets are highlighted in Figure 2.

Wallets	
Application Wallets	***Exodus*** ***Electrum***
Web Walltes	***Metmask*** ***Brave Wallet***
Hardware Wallets	***Trezor Model one***

[Figure 2: Chosen wallets]

Each wallet normally has a corresponding address that is different from the collection of transaction ID's highlighted in figure 2 but are similar in structure. These wallet addresses are often private and do not appear on the public ledger (Suratkar, Shirole and Bhirud, 2020) . This creates the problem at hand; *how do investigators determine if a transaction belongs to the owner of a certain wallet?*

Whilst wallet ID's carry no revealing information at first, once a wallet ID is known to investigators, it can often act as a springboard for further investigation.

1.4 Cryptocurrency forensics

To accurately identify illicit activity involving cryptocurrency wallets and transactions, forensic investigators must rely on acquiring supporting digital artefacts. Digital artefacts are remnants of the actions carried out through applications or connected devices. As cryptocurrency wallets function similarly to other applications or devices, they leave behind their own set of digital artefacts that can be analysed to uncover further information on the illicit activities.

Different cryptocurrency wallet formats will require slight variation in the procedures taking place in forensic investigation. Figure 3 outlines the different type of digital artefacts that will be obtained through the work in this report.

Wallet Type	Forensic Procedure	Expected Artefacts
Application	Disk Forensics	***Registry Keys**; User preferences, Application Settings, Wallet Adresses, Transactions, Backup Data, Network* ***Log Files**; Wallet Application Logs, System Logs, Debug Logs, Transaction Logs, Error Logs* ***Configuration Files*** ***Wallet specific Informaiton***
Web	Browser Forensics	*Brosweer History, Cookies & Local Storagem Browser Cache, Downloaded Files, Bookmarks, Autofil Data, Autocomplete suggestions, Saved Passwords*
Hardware	Device, Disk & Memory Forensics	**On connected device;** *USB Connection logs, Temporary Files & Cache, Locally Stored Passwords* **On Hardware Wallet;** *Wallet Addresses, Private Keys, Transaction History, Device Configuration, DeviceLogs*

[Figure 3: digital artefacts]

This variation in procedure poses challenges for digital forensic investigators who must consider the wide range of digital artefacts in a cryptocurrency investigation. Therefore, a standardised approach is necessary to effectively handle these variations. This necessity is amplified by the numerous examples of related research papers authored by others previously, some of which discuss the broad implications of cryptocurrency within cybercrime.

2. BACKGROUND

2.1 Ransomware and cryptocurrency

Cryptocurrency has become the currency of choice for online criminals, being used on the dark web, where illegal drugs, weapons & documentation are all commonly bought and sold (Reedy, 2023). However, cryptocurrency is primarily associated online with ransomware. Ransomware malware will encrypt the victims' files on disk and present them with a pop up to pay to have their files unencrypted. This creates panic for the victim and will lead to them paying to get back access to their files. Because of this widespread usage of ransomware, it is estimated that from 2016-2018 there were 19,750 victims causing estimated damages of $1billion, showing the far reach of ransomware (O'Kane, Sezer and Carlin, 2018) .

The decentralisation, lack of governing body and utilising other operational security measures, enables malware authors to receive the ransom anonymously and be very difficult to track down. This anonymity is furthered when authors will create several different cryptocurrency addresses that will all receive smaller individual payments from the ransomware (Chesti *et al.,* 2020) . By separating the ransom payments, this will stop a noticeable, similar sized amount from being seen on the ledger to happen often. These security measures mean it is hard to punish ransomware authors. Therefore, the processes outlined in this report can help combat these issues for an alternative way.

2.2 Existing forensic approaches

When analysing the existing scope of digital forensic investigations into cryptocurrency, several omissions and compromises have been made for the research to be carried out. However, using this past work It is now possible to deliver a holistic approach to the proposed research, creating areas of research to negate these differences.

2.2.1 Wallet

The distinct separation of processes is commonplace throughout previous research, especially when considering the choice of cryptocurrency wallets. Often, authors of past work would make the decision to focus their research on one category of wallet. As exampled in the work of (Thomas *et al.,* 2020) where they discuss hardware wallets & memory forensics using volatility. Additionally, (Zollner, Choo and Le-Khac, 2019) focus their research on web wallets, resulting in primarily web browser forensics being used. Finally, the work of (Park *et al.,* 2023) will focus on cracking security to gain unauthorised access to application wallets, carrying out disk forensics. Therefore, it is clear to see from previous research that there is a negligence to a multi-wallet approach to the cryptocurrency wallet forensics. The work previously carried out has made it possible for this report to take a multi wallet approach.

2.2.2 Defining authorisation.

Firstly, researchers make the decision on whether they have knowledge of authorisation details for each of the wallets. Cryptocurrency wallets often have multiple layers of security. This will include seed phrases – commonly a bank of 12 random words, passwords, and passphrases. The work highlighted by (Park *et al.,* 2023) and (Holmes and Buchanan, 2023) focuses on breaking into the wallet without authorisation. This research highlights the importance of doing so during a forensic investigation, as often investigators might not have access to the appropriate seed phrase or password (preauthorisation). However as seen in (Thomas *et al.,* 2020) the research assumes the passphrase is previously known, enabling complete access to the cryptocurrency wallets (post-authorisation) Whilst both assumptions are valid for each investigation, favouring one method and negating the other will create an incomplete acquisition of the digital artefacts obtained. Through not acquiring artefacts for both pre and post authorisation, it will be near impossible to say with conclusive thought what the difference is knowing these authorisation details .Therefore, any report created will leave any accompanying methodology or visualisation of the collected artefacts incomplete. The work proposed in this report will account for digital artefact acquisition, for both pre and post authorisation variations.

2.2.3 Complexity

Members of law enforcement hold different technical backgrounds, therefore criminal cases involving complex technologies such as cryptocurrency and the blockchain can create confusion and unnecessary delay for forensic investigators' when they are investigating cybercrime (Reedy, 2023). Current literature does not assist in helping to negate this confusion as the research is commonly directed at other academics, for example the work of (Wu *et al.,* 2021)focuses on highly technical machine learning models for analyses of cryptocurrency wallets. Therefore, providing an easy to read, well documented methodology is essential to

allow the work being performed to be translated into actionable steps.

2.2.4 Visualisation

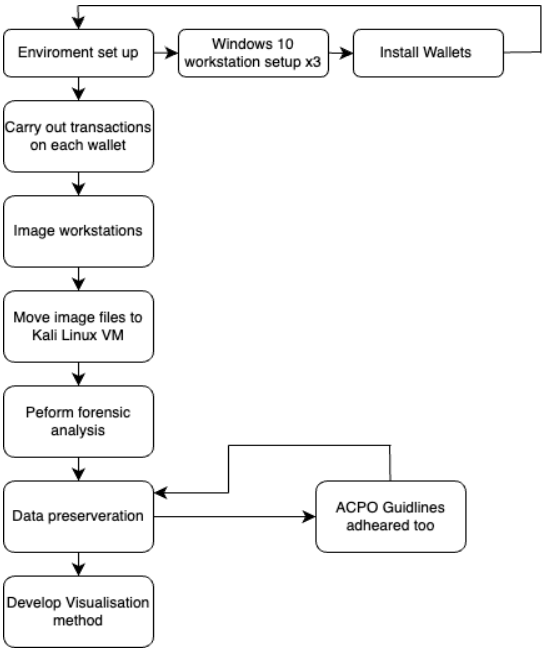
As previously highlighted, past research is primarily focused on the technical process of obtaining digital artefacts from cryptocurrency wallets. When attempting to create a replicable methodology to be used by investigators, too much technical focus can detract from its overall objective. This is particularly prominent in the research around machine learning and cryptocurrency analysis (Wu *et al.,* 2021).

Supplementing the methodology with a visualisation technique, can help keep the focus of the methodology on the bigger picture. This visualisation can come built into a methodology or framework such as the flow charts and diagrams in the work of (Park *et al.,* 2023) Alternatively, it can be developed around the specific data obtained from the digital artefacts, in which the researcher will create a utility tool such as the one suggested in (Ribeiro, Leale and Sendin, 2023)

Therefore, the work from this report will aim to develop a tool to handle all the artefacts obtained from the acquisition stage of the methodology. Time constraints are often a determination in the completeness of these tools; therefore, the limitations & mitigations outline in section 3.8 will be used to enable time to do so.

3. METHOD

An overview of the methodology and its structure is outlined in figure 4.



[Figure 4: Methodology Outline]

3.1. Environment setup

3.1.2 Virtual machines & imaging

Before tackling the issues of the wallets, it is important for the research to have its own testing environment to ensure there is no unforeseen variation in the information that is being obtained. Therefore, three Windows 10 virtual machines will be set up. Each of these machines will be the workstation where the wallets are installed, and transactions carried out.

3.1.3 Crypto wallet installation & registration

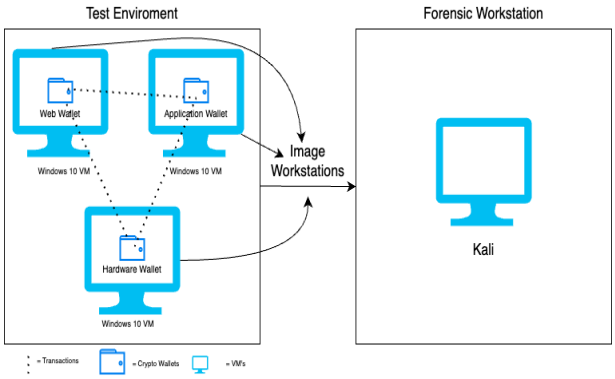
Each crypto wallet will require some initial set up to be usable. The desktop wallets Exodus & Electrum will be downloaded & installed from the appropriate vendor websites. Web browsers: Google Chrome and Brave will be used to enable use of the web browser wallet extensions. Finally, the Trezor hardware wallet will be installed, registering with the host machine & the Trezor Suite application.

3.1.4 Populating wallets with transactions

Each wallet, regardless of its function will require transactions to be made to and from its address. This is important to simulate the day-to-day application of the wallets and ensure there is the relevant artifacts to be left on the workstation image.

3.1.5 Imaging the workstations

After the transactions are carried out an Image will be taken from the VM workstation allowing for analysis of these image files on a separate Kali Linux machine.



[Figure 5 : Environment Setup]

3.3 Digital artefact collection

Hardware wallet artefact collection will include device, memory & network forensics. Network forensics entails monitoring packets using tools such as 'tcdump'. These monitoring tools will have to be utilised before the windows machines are imaged. Memory analysis using the tool Volatility will be attempted to try capture any volatile memory residing in RAM.

Application artefact collection will be performed using standard disk forensics, relying on tools such as Autopsy to search the disk in its entirety. For additional information on the artefacts that will be collected, refer to Figure 3 in section 1. Process will be carried out for web wallets, looking at popular web artefacts.

3.4 Preservation of digital artefacts

When preserving data, it is essential that certain procedures are used to maintain the integrity of the data, enabling the research remains uncompromised. As a result of the proposed

research closely following the process of a forensic investigation that could be carried out by law enforcement, ACPO guidelines will be followed. ACPO guidelines ensure proper handling of data & documentation, upholding the integrity and importance for crucial project data, whilst complying with forensic best practices (Holmes and Buchanan, 2023)

3.6 Analysis of digital artefacts

During the analysis of digital artefacts, prioritising relevant information for forensic investigators would be the first step. To deduce what information is most valuable to investigators would be done through relying on trusted, reliable sources. These sources, such as in (Reedy, 2023) will indicate what investigators, such as those in law enforcement would prioritise to analyse further. Once a decision has been made on the artefacts that will be most beneficial, the data can be parsed into more readable formats such as tables, graphs, or databases. This is where the focus on visualisation is important to help manage and reuse the obtained data.

3.7 Visualisation of data

Once valid data is obtained and analysed, detailed visualisation becomes crucial for understanding cryptocurrency wallets and transactions and the information from their digital artefacts. To assist basic visualisation techniques, Python can be used in conjunction with adaptable and flexible libraries to handle these large datasets and produce reusable tooling.

3.8 Limitations of research

The proposed research faces several limitations around the security of hardware wallets, ethical dilemmas, and lack of appropriate results. Mitigations are made to ensure project contingency and deliver on initial research questions.

A key limitation of this research is analysing the hardware wallets. Hardware wallets boast advanced technology and encryption that make it difficult to compromise. To address this, a post authorisation data acquisition phase will be conducted. Through post authorisation data acquisition, there will still be an ability to analyse the same information should the hardware wallet be too secure.

Ethical limitations are extremely important to consider. When analysing the acquired data, it is important that the researcher only covers data obtained through their personal environment and from no external sources. This will be checked with an ethics board before conducting the research to ensure that this has been approved. Throughout the research, ACPO guidelines will be followed to maintain correct preservation of data.

Challenges in obtaining relevant cryptocurrency wallet artefacts that would be useful to investigators exist. This is a result of the dynamic nature of cryptocurrency and the evolving cybercriminal tactics that may be introduced to help maintain anonymity. This will be mitigated though delivering an encompassing methodology with a wide scope to be used across different investigations.

4. CONCLUSION

The proposal outlines the need for further investigation to the digital artefacts left by crypto currency wallets after they perform transactions and how they can provide information to forensic investigators.

Acknowledging the fundamental principles of cryptocurrency and its underlining technology enables a broader understanding to be given to the investigator and provide reason as to why it is chosen for numerous cybercrimes. The discussion in the proposal outlines the misconception around the complete anonymity of cryptocurrency but recognises that there is still a large amount of work to be done to remove this anonymity - sometimes of which cannot be done due to limitations such as encryption.

When building upon previous working, it is clear this gap in knowledge is the result of decisions made by previous researchers and a focus towards academic readers with a neglect of real scenarios faced by digital forensic investigators. Highlighting the real-world problem of ransomware, and adopting a holistic approach on previous researchers work, a replicable and relevant methodology with visualisation techniques will be created by the work carried out suggested in this proposal.

The methodology carefully outlines the enviroment setup, detailing how transactions will create digital artefacts that are later acquired at different phases, preserved, and analysed by the researcher. Acknowledging limitations faced when conducting research, such as obtaining hardware wallet artefacts is essential to detail appropriate mitigations, enabling consistency across the proposed timeline in the accompanying Gantt chart.

Overall, there is consistent work in this area to build upon whilst interesting omissions will allow for original work to be carried out.

5. REFERENCES

Chesti, I.A., Humayun, M., Sama, N.U. and Jhanjhi, N. (2020) 'Evolution, Mitigation, and Prevention of Ransomware', *2020 2nd International Conference on Computer and Information Sciences (ICCIS),* , pp. 1-6. doi: 10.1109/ICCIS49240.2020.9257708 https://ieeexplore.ieee.org/document/9257708

Holmes, A. and Buchanan, W.J. (2023) 'A framework for live host-based Bitcoin wallet forensics and triage', *Forensic Science International: Digital Investigation,* 44(2666-2817), pp. 301486. doi: 10.1016/j.fsidi.2022.301486 https://dx.doi.org/10.1016/j.fsidi.2022.301486

O'Kane, P., Sezer, S. and Carlin, D. (2018) 'Evolution of ransomware', *IET networks,* 7(5), pp. 321-327. doi: 10.1049/iet-net.2017.0207 http://digital-library.theiet.org/content/journals/10.1049/iet-net.2017.0207

Park, A., Ryu, H., Park, W. and Jeong, D. (2023) 'Forensic investigation framework for cryptocurrency wallet in the end device', *Computers & security,* 133, pp. 103392. doi: 10.1016/j.cose.2023.103392 https://dx.doi.org/10.1016/j.cose.2023.103392

Reedy, P. (2023) 'Interpol review of digital evidence for 2019–2022', *Forensic science international. Synergy,* 6, pp. 100313. doi: 10.1016/j.fsisyn.2022.100313 https://dx.doi.org/10.1016/j.fsisyn.2022.100313

Ribeiro, P.H.R., Leale, P. and Sendin, I.d.S. (2023) 'A Proposal for an Open-Source Bitcoin Forensics Tool', *International Journal on Cybernetics & Informatics,* 12(6), pp. 173-178. doi: 10.5121/ijci.2023.120613 https://www.researchgate.net/publication/374734619_A_Proposal_for_an_Open-Source_Bitcoin_Forensics_Tool

Suratkar, S., Shirole, M. and Bhirud, S. (2020) 'Cryptocurrency Wallet: A Review', *2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP),* , pp. 1-7. doi: 10.1109/ICCCSP49186.2020.9315193 https://ieeexplore.ieee.org/document/9315193

Thomas, T., Piscitelli, M., Shavrov, I. and Baggili, I. (2020) 'Memory FORESHADOW: Memory FOREnSics of HArDware CryptOcurrency wallets – A Tool and Visualization Framework', *Forensic Science International: Digital Investigation,* 33, pp. 301002. doi: 10.1016/j.fsidi.2020.301002 https://dx.doi.org/10.1016/j.fsidi.2020.301002

Turner, A. and Irwin, A.S.M. (2018) 'Bitcoin transactions: a digital discovery of illicit activity on the blockchain', *Journal of financial crime,* 25(1), pp. 109-130. doi: 10.1108/JFC-12-2016-0078 https://www.emerald.com/insight/content/doi/10.1108/JFC-12-2016-0078/full/html

Zollner, S., Choo, K.R. and Le-Khac, N. (2019) 'An Automated Live Forensic and Postmortem Analysis Tool for Bitcoin on Windows Systems', *IEEE access,* 7, pp. 158250-158263. doi: 10.1109/ACCESS.2019.2948774 https://ieeexplore.ieee.org/document/8878085