Arab American University

Faculty of Graduate Studies

Mobile Forensics for E-wallet Artifact in Mobile Device: Case Study in Palestine

By

Maryam Tareq Mesbah Abu Safeia

Supervisor

Dr. Mohammed Moreb

This thesis was submitted in partial fulfillment of the requirements for the Master`s degree in Cybercrime and digital evidence analysis

July/ 2023

Thesis Approval

Mobile Forensics for E-wallet Artifact in Mobile Device: Case Study in Palestine

By

Maryam Tareq Mesbah Abu Safeia

This thesis was defended successfully on .....and approved by:

Committee members	signature
1. Dr. Mohammed Moreb/ Supervisor:	.....
2. Dr. Ahmed Hasasneh/ Internal Examiner:	.
3. Dr. Bilal Amro/ Internal Examiner:	.

Declaration

I declare that this thesis entitled " Mobile Forensics for E-wallet Artifact in Mobile Device: Case Study in Palestine " is my work and has been composed solely by myself, does not contain any work from other researchers, and has not been submitted for any other degree or scientific qualification except the references is made.

Signed: .....

Maryam Tareq Mesbah Abu Safeia

Date: 23/1/2024

Student ID: 201920282

DEDICATION

This thesis is dedicated to that beautiful land that carries the fragrance of heritage and history, to the city of GAZA that insisted on remaining strong and beautiful despite the challenges of time. To this city that has learned from all its challenges how to transform into a chapter in the book of resilience and defiance.

Acknowledgments

I am deeply grateful to my supervisor, Dr. Mohammed Moreb, for his unwavering support and guidance throughout my master's program. Their expertise and patience have been invaluable to me and have played a crucial role in the success of this thesis.

I am also grateful to Arab American University for providing me with the opportunity to conduct my research and for all the resources and support they provided. I want to extend a special thanks to My husband, Eng. Samir Sahmoud went above and beyond to help me with my work.

Zina, Nizar, and Sila, my great children and my support in the first place, the safe embrace after all the tiredness, I am grateful for your presence, endurance, and support in this work.

I also thank dear discussants for serving on my thesis committee and providing valuable feedback and suggestions. Their insights and guidance were instrumental in helping me to shape my research and write this thesis.

I am deeply thankful to my friends and family for their love and support during this process. Without their encouragement and motivation, I would not have been able to complete this journey.

My father, mother, and brothers are far away and closer to the soul than itself; I am grateful for all your support.

ABSTRACT

Given the rising use of electronic wallets for financial transactions and their potential misuse in illicit activities (e.g., money laundering, extortion, and tax evasion), the challenge lies in tracking and regulating these transactions due to their global and relatively anonymous nature. This prompts the inquiry into the feasibility of identifying electronic wallet presence and usage on mobile devices, particularly in digital forensics and security.

This study presents a framework for validating e-wallet artifacts in mobile forensics. The framework comprises three phases: data collection, feature selection, and validation. Using e-wallet artifacts from an Intrusion Detection System, we assess their validity through stochastic modeling.

Furthermore, after repeatedly acquiring data when deleting the application from the phone, it was revealed that it retains all user movements and information. This is unacceptable in cybersecurity as it facilitates embezzlement and the transfer of illicit funds.

The research employs both deductive (questionnaire) and inductive (forensic analysis) approaches. The statistical analysis results for a sample of 70 users of electronic wallets in Palestine have shown that local e-wallets demonstrate an acceptable level of security. We recommend Implementing a robust strategy to counter electronic wallet threats and enhance their competitiveness on the global stage and adopting the model proposed in this research when establishing electronic wallet systems.

Results indicate that the Reflect NeoBank application is not adequately secure. It retains user data even after deletion, posing cybersecurity risks, including embezzlement and illicit fund transfers. We also compare local and global electronic wallets, highlighting security disparities.

This research will contribute to the knowledge recommending future research topics and methods in which digital forensic examiners might apply the findings to instances involving local e-wallet use on mobile devices or any illicit e-wallet transactions.

Keywords: electronic wallet, digital wallet, payment, neo bank, wallet, bank, digital forensics, acquisition, data analysis, Ios mobile wallet, android mobile wallet

Table of contents

List of Tables

List of Figures

List of Abbreviations

ADB	Android Debug Bridge
ISA	Information Security Awareness
MAEE-dst	Mobile Applications Engineering for Ewallet design, security, and testing
AWS	Amazon Web Services
KYC	know-your-customer
AML	anti-money laundering
API	Application programming interfaces
POS	point of sale
ICT	Information and Communication Technology
AWS4	Amazon Web Services version 4
NFC	Near Field Communications
WHO	World Health Organization
DDoS	Distributed Denial of Service

Chapter 1
Introduction

1.1 Introduction

Recently, after the spread of the COVID-19 pandemic, people resorted to converting their lifestyles to digital electronics to continue and lead their normal lives. For example: In shopping for daily necessities, purchasing clothes online, ordering their favorite food, planning for travel and conducting all banking transactions via the Internet. This shift led all institutions to convert their services from tangible to electronic, prompting companies to transition their systems into electronic systems. Consequently, electronic wallets have become instrumental in facilitating the digital payment process[1]. The nationwide lockdown imposed in India due to the Coronavirus (COVID-19) pandemic resulted in a 44% surge in e-wallet usage[2]. However, this increase in digital transactions accompanied an 86% rise in cybercrime attacks. Because of the large number of electronic wallets for stores and institutions makes them vulnerable to hacking and theft. It has an increased attack surface since data can be accessed anywhere and anytime.

As the COVID-19 pandemic spreads, government officials in an increasing number of nations are taking steps to promote contactless payments. The World Health Organization's (WHO) physical distancing policy has urged consumers to engage in contactless activities, including financial transactions. People are concerned that tangible currency could be used to spread a novel coronavirus (SARS-Cov2). It prompts them to switch to an e-wallet, and the study proved that COVID-19 may influence customers' desire to use e-wallets [2].

Using electronic wallets for COVID-19 By combining government backing, the perception of risk, and societal impact as possible influencing elements, the Pandemic has been interested in bridging a knowledge gap. Moreover, to aid in developing efficient tactics that can accurately capture consumers' intents to utilize e-wallets by policymakers. Data was gathered via a Google Forms survey and covariance-based structural equation modeling (CB-SEM). It was found that attitudes regarding the use of e-wallets are positively correlated with perceived utility, government backing, perceived danger, and social impact.

A favorable relationship exists between attitude and the user's desire to use the wallets. Additionally, it suggests that the government boosts incentives to hasten the transition to a cashless society. The associated organizations ought to raise public awareness of the value of electronic wallets in reducing the spread of viruses [3]. E-Wallet effects on community behavior are evaluated with various facilities offered. It is generated that e-wallets are readily accepted in the community because social life cannot be separated from information system technology, where technology has entered into all aspects of social life [4].

In today's tech-driven era, electronic terminologies can sometimes overlap, so it's important to distinguish between a mobile wallet, an e-wallet, and a Digital Wallet.

A digital wallet is a technology created to hold the data required for online transactions. Although some digital wallets can also operate through mobile applications, most are primarily utilized for internet purchases. One of the best examples is Google's e-commerce platform, which works flawlessly on computers, mobile devices, and tablets. Others are more specialized and are frequently accessed through specialist applications that cater to particular businesses or services.

Mobile Wallet: Only mobile applications are used in a mobile wallet. These virtual wallets are found on portable electronics like smartphones and tablets, where they safely hold credit card data. Mobile wallets have a tight relationship with a device's capabilities. Mobile wallets include names like Apple Pay and Android Pay, for instance. They are becoming increasingly popular as practical payment options for a range of services, including in-store purchases, transportation, and more.

Although an Electronic Wallet has several features, its main function is the ability to save a balance. It may be used for many things, including offline and online purchases, sending money, and paying bills. Because of their adaptability and capacity for a range of financial activities, e-wallets are a popular choice among customers.

By distinguishing between these words, we may more clearly comprehend the unique functions and roles that digital wallets, mobile wallets, and e-wallets each play in the current digital environment. Keeping up with development and the continuation of the work of traditional banks, NEOBANK, an innovative concept, emerged as a smart and personal banking digital platform that was specially designed to provide a simple and integrated banking experience through smartphones. It is the first digital bank in Palestine called REFLECT[5].

In unbanked regions, prepaid wallets offer a practical solution. Likewise, for vendors seeking guaranteed payment, e-wallet transactions are a secure choice. To maintain a positive balance, users can fund their e-wallets through a bank account, in cash, or even with cryptocurrency. E-wallets can serve as digital wallets, enabling users to access payment information for transactions. Due to their versatile nature, the term 'e-wallet' has become a catch-all phrase, even though various types of e-wallets exist.

A neobank is a type of financial institution that operates exclusively online without any physical branches and generally offers services such as digital wallets, money transfers, and debit cards. Neobanks are often designed to be more user-friendly and cost-effective than traditional brick-and-mortar banks, with a strong focus on mobile banking and providing a seamless user experience through intuitive apps and interfaces[1]. Figure 1 shows the most significant differences between traditional banks, digital banks, and neobanks.

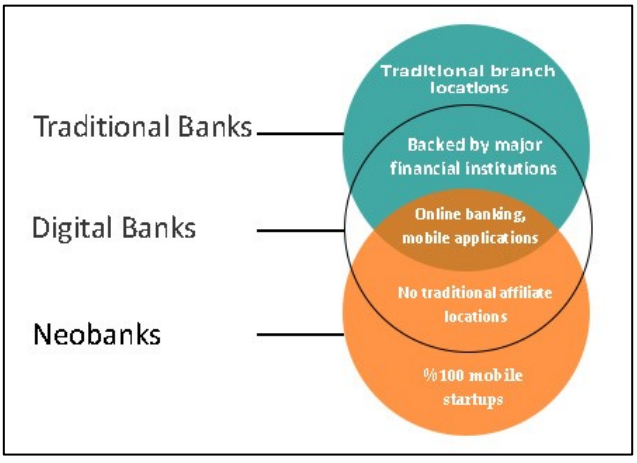


Figure 1 Traditional bank to neobank [6]

Despite the absence of physical branches, neobanks are licensed and regulated like traditional banks and frequently collaborate with established financial institutions to offer services such as deposit insurance and access to payment networks. Neobanks are gaining popularity, particularly among younger generations, prioritizing convenience and digital accessibility. However, it's important to note that certain services, such as cash deposits and in-person customer support, may be limited or unavailable due to the lack of physical branches. Although neobanks may provide competitive interest rates and fee structures, they might not offer the same level of security and stability as traditional banks, which boast a long history and a well-established reputation in the financial industry [6].

NEOBANK Reflect

Reflect is a startup that has been offering financial services to consumers since 2012. They specialize in simplifying consumer financial management. Reflect is a digital financial institution with a clear mission: to make banking easier, more engaging, and accessible to everyone. As a digital bank, they enable consumers to bank from the comfort of their homes, providing an entirely new banking experience that empowers you to take control of your finances. Reflect represents a fresh approach to banking, making it distinctive and competitive in the digital financial industry. They are committed to enhancing the accessibility and convenience of banking services for all customers. Their product is not only convenient but also tailored to meet individual needs. Reflect NeoBank empowers you to manage your finances on your terms.

In recent times, there has been substantial growth within the Neobank ecosystem, marked by a significant rise in both the quantity of Neobank entities and their customer populations. This expansion was particularly striking during the period spanning from 2018 to 2020, when the worldwide presence of digital-only challenger banks surged dramatically, surging from approximately 60 to well over 250 Neobanks. Europe played a pivotal role in driving this trend, with nearly half of these 256 Neobanks being based in the region. This growth was significantly fueled by substantial investments aimed at advancing their business operations.[6]

Neobanks, like any other financial institution, have their own set of limitations and vulnerabilities, such as restricted physical presence where Neobanks exclusively function in the digital realm or via mobile applications, resulting in the absence of physical brick-and-mortar branches. This may pose a constraint for customers who favor face-to-face engagements or require access to tangible services such as depositing cash, and its heavy reliance on technology makes it vulnerable to technical glitches, cyberattacks, and outages.

Additionally, numerous neobanks are limited to specific regions, implying that they may not be available to customers residing outside of particular countries or geographic areas. Furthermore, despite neobanks' emphasis on security, their digital infrastructure renders them appealing targets for cybercriminals. Security breaches have the potential to lead to financial losses and harm the neobank's reputation. One of the most important vulnerabilities is that Neobanks handles vast amounts of customer data, including personal and financial information. A data breach can occur if security measures are not robust enough. In such incidents, customer data may be exposed, leading to identity theft, financial fraud, and legal repercussions for the neobank.

Distributed Denial of Service (DDoS) Attacks: Cybercriminals may launch DDoS attacks against neobanks online systems, overwhelming their servers and causing service outages. These attacks disrupt customer access to accounts and services and can lead to financial losses. Neobanks handle vast amounts of customer data, including personal and financial information. A data breach can occur if security measures are not robust enough. In such incidents, customer data may be exposed, leading to identity theft, financial fraud, and legal repercussions for the neobank.

Distributed Denial of Service (DDoS) Attacks: Cybercriminals may launch DDoS attacks against neobanks' online systems, overwhelming their servers and causing service outages. These attacks disrupt customer access to accounts and services and can lead to financial losses.

This research aims to ascertain the ability of a digital forensic investigator to identify potential threats that may compromise the security of Neobank applications. We intend to extract artifacts from two distinct e-wallet and Neobank applications operating on the Android and iOS platforms. Given the increasing popularity of e-wallets, the likelihood of malicious actors exploiting vulnerabilities is anticipated to rise. Our research is driven by the theory that an e-wallet, being a digital system, leaves traces of its presence and activities in the memory of a mobile device, detectable through forensic investigation. This study includes a comparative analysis of a local and an international e-wallet application. The artifacts within an e-wallet application primarily comprise user-entered data, such as shipment addresses, billing details, and payment methods, including credit card numbers, expiration dates, and security codes. Our investigation will evaluate the security measures implemented in devices utilizing the application, and we will extract this data in various operating modes, including when the application is active and when the devices are rooted.

Our interest in this study stems from the growing prevalence of electronic wallets and the increasing adoption of digital wallet payment methods. Personal experiences with these technologies, including encountering unwarranted discounts from a local e-wallet application and assessing the sense of security associated with international digital wallets, have inspired our research. Furthermore, this study aims to contribute to the existing body of knowledge by offering recommendations for future research avenues. It also seeks to guide digital forensic examiners in applying the study's findings to scenarios involving the use of local e-wallets on mobile devices and potential illicit e-wallet transactions.

1.2 Statement of the Problem and Research Question

In line with Worldpay's Global Payments Report[7], e-wallets constituted 48.6% of the total value of global e-commerce transactions in 2021. Projections indicate that this share is set to rise to 52.5% by 2025. In contrast, traditional payment methods such as bank transfers, credit cards, and debit cards accounted for 7.4%, 13.2%, and 21%, respectively. It is anticipated that the usage of these conventional payment methods will decline by 2025 while e-wallets continue to gain prominence.

Given the rapid evolution of the digital landscape, many banks and institutions now offer e-wallets for easy bill payments. With the increasing availability of products and services online, fraudsters exploit the vulnerabilities of local online app users for financial gain. Therefore, my research focuses on evaluating the most common wallet programs on Android and iOS mobile systems for potential criminal evidence. Data was retrieved from both Android and iOS devices using various forensic extraction techniques, and all data that could potentially be linked to the digital wallet, whether active or removed from the mobile device, was analyzed.

Research questions:

1- Is your mobile wallet application truly secure? Despite the rapid shift from physical currency to digital wallets, significant security issues arise with the use of a mobile wallet.

2- Can we extract forensically relevant data related to mobile wallet usage, such as transaction history? If possible, what is the duration of data retention in memory? What specific data can be retrieved? In the event of data modification, is it possible to recover the previous unaltered log?

3- In cases of data deletion in mobile wallet , is it retrievable? If so, is it identified as deleted?"

1.3 Hypotheses

To formulate a solution for our thesis problem, we will proceed with the following hypotheses:

H1. E-wallet transactions can't be retrieved from deleted e-wallet applications, IOS Backup, or connected devices such as IOS and Android mobile systems.

H2. E-wallet data is secure on mobile.

And sub hypotheses from H2:

H2.1. The chance of users' data being stolen, destroyed, or tampered with grows as the number of mobile applications installed rises. (Not integrity).

H2.2. The increasing rate of mobile app installation raises the possibility of watching and eavesdropping on user data, as well as privacy breaches. (Not confidentiality).

H2.3. The high rate of mobile app installation may lead to the user being unable to access his personal information, such as encryption keys. (Not availability).

1.4 Research objectives

The research aims to achieve the following objectives:

1- Evaluate the Security of Mobile Wallet Applications

Assess the perceived security of mobile wallet applications among local users and gauge user confidence in the security features of their mobile wallet applications.

2- Investigate Forensic Data Extraction from Wallet Applications

Perform practical experiments using digital forensic techniques to assess the security of electronic wallet applications. Determine the feasibility of forensically extracting data related to wallet usage, particularly transaction history, and investigate the duration of data retention in the memory of mobile devices and identify specific types of data that can be forensically retrieved from mobile wallet applications and then Explore the possibility of recovering previous unaltered transaction logs in the event of data modification.

3- *Assess Data Retrieval and Deletion in Mobile Wallets*

Examine the retrievability of data in cases of intentional data deletion from mobile wallets and determine if deleted data is identifiable and distinguishable, evaluate the success rate of retrieving deleted data, and understand its implications on user security perceptions.

4- *Measure User Security Perceptions*

Conduct statistical analysis on user surveys to measure the extent of security felt by users of local electronic wallets and correlate statistical findings with practical experiments, specifically in the context of forensic data analysis. Identify patterns and trends in user perceptions of electronic wallet security.

1.5 Significance of research

As technology progresses, cybersecurity threats continue to evolve. This research endeavors to keep pace with these advancements by shedding light on emerging threats and proposing proactive security measures to prevent fraud. E-wallets are vulnerable to various forms of fraudulent activities, such as unauthorized transactions and identity theft. By assessing the security of e-wallet applications, the research aims to contribute to the prevention and mitigation of financial fraud, safeguarding both users and financial institutions. Additionally, the study seeks to bolster user confidence in e-wallet applications by identifying security gaps and recommending necessary enhancements. A more secure environment can potentially foster greater user adoption of these technologies. Ultimately, the research focuses on evaluating the security of these applications to safeguard users' financial assets from potential threats and cyberattacks.

In all technical and electronic systems, there must be protection for the security of the data contained in the system by the CIA[8], as shown in Figure 2, as it ensures data security from all of the following security elements that are required for electronic payment systems: clients will not trust an e-payment system that is not secure. And, in order for clients to accept you, you must have their trust. Because they rely on basic ICT frameworks, e-banking and e-payment applications have security difficulties. This creates weaknesses in economic organizations and firms and can potentially harm clients, so we'll determine how to verify the safety and protection of the e-wallet application by the CIA:

Figure 2 CIA of security

1- **Confidentiality**: any data transmission over the Internet makes it more vulnerable and introduces security risks to the process. Therefore, data privacy and confidentiality must be secured in the case of migration over the Internet or to the cloud. In electronic payment systems, recent statistical reports[9] showed that in the year 2021, the highest rate of violation of e-wallets and their exposure to the risk of theft from hackers and thieves on the Internet, and therefore, it became necessary for specialists to address this gap by following the approach of security, privacy and risk management in the use of e-wallets [10]

2- **Integrity**, which is just as important for the confidentiality of information as its integrity and integrity changing and maintaining it. The emergence of blockchain technology can be clearly verified because it's one of the integrity standards of electronic wallets[11], as it helps verify their authenticity and prevents them from being changed or playing with the data.

3- **Availability:** Electronic wallet data is sensitive and personal data and should be preserved only for the people authorized to access the data. If this is not the case, the consequences of the availability of data at all times and for users who are not authorized to obtain information will constitute an obstacle and a major security breach in the protection and security of the application of electronic wallets.

To secure digital transactions effectively, several security measures and precautions must be taken in addition to the CIA principle (Confidentiality, Integrity, Availability). Here are some measures needed to achieve this goal:

1. Data Encryption, Identity and Access Management (IAM), Use of Digital Certificates, Security Policies Implementation, Security Monitoring, Software and Hardware Updates, User Education, Containment Strategy, Data Recovery, Compliance with Laws and Regulations

These are some of the fundamental measures that can be taken to secure digital transactions, which we will discuss in detail later. Achieving digital security requires a comprehensive strategy that encompasses technology, processes, education, and continuous monitoring.

Chapter 2
Literature Review& Research Model

2.1 Introduction

This chapter is dedicated to evaluating the security, reliability, and availability of electronic wallet applications. The initial focus will be on a comprehensive review of the literature pertaining to electronic wallets.

A study focused on assessing the security, reliability, and availability of electronic wallet applications. The methodology involves two main approaches:

Surveys and Questionnaires: The study is designed to collect data on the perceived security among users of local electronic wallets in Palestine. This will be accomplished through the distribution of surveys and polls, with the primary objective of gauging user opinions and attitudes regarding the security of electronic wallet applications.

Technical Analysis on Mobile Phones: Experiments will be conducted on mobile phones under various conditions, both with and without the electronic wallet installed. Subsequently, digital forensic techniques and digital extraction tools will be employed to examine the electronic wallet applications. The safety of these applications and the analysis of data extracted from the phones will be assessed. After these two main approaches, the study aims to:

Use statistical analysis tools to evaluate the collected survey data, then compare the results of the technical analysis with the statistical analysis results, and finally match the findings from a technical perspective with the perspectives of users regarding security and protection.

Overall, the study is comprehensive, combining both user perception through surveys and technical analysis through experiments and digital forensics. This multi-faceted approach aims to provide a holistic understanding of the security landscape of local electronic wallet applications.

2.2 Literature Review

In previous research delves into the worldwide expansion of mobile wallets and their increasing prevalence in emerging economies.[12] It utilizes a comprehensive research framework that combines different elements like beliefs, social elements, quality, and trust to bridge gaps in earlier studies. The study highlights the importance of trust and perceived utility in influencing the adoption of mobile wallets, underscoring the requirement for financial service providers to concentrate on establishing trust and improving perceived utility.

Additionally, it stresses the necessity of educating potential users about mobile wallets to encourage broader adoption.

With a big data analysis its purpose is to find and group similar e-wallet use themes. They used text mining to examine the actions of e-wallet users. Big data analytics of actual e-wallet usage results in a more pertinent and precise understanding of the mobile payment system. It exhibits the intricacy of relationships between people and computers. Additionally, it is advised that governments modernize and change the monitoring framework to account for the rise of payment systems. [13]

In previous research conducted in Bangkok, Thailand[14], the influence of various factors on the intention to use E-Wallets was examined. The findings revealed that E-Wallet usage is gaining popularity not only in developed economies but also in developing economies. This trend can be attributed to the convenience, safety, and efficiency it offers for everyday financial transactions. Furthermore, the global digitization of monetary transactions is a significant driving force behind the adoption of E-Wallets, leading to an anticipated increase in the number of users in the future.

A previous study indicates [15] that E-payment is in a revolutionary stage of the global economic industry. "Information and Communication Technology (ICT) and Digital technologies have made great evolutionary development in finance, economics, operational costs," and improved organizational performance. Where People's everyday lives are increasingly moving online, their purchasing habits have changed as they move from physical shops to online retailers, and the payment process has become more seamless thanks to in-app (e-Payment) electronic payment experiences, including cash transfers to cards and QR codes at the point of sale (POS). The societal ramifications were enormous. Accordingly, the motives for the existence of the neobank technology emerged.

The rise of e-wallets has been substantial, driven by the increasing prevalence of payment-enabled devices and their acceptance by retailers.[16] However, this surge in usage has also made e-wallet users susceptible to cyberattacks. This research concentrates on providing security advice specifically designed for the Android platform, which is a primary target for mobile malware. These security recommendations are grounded in established guidelines and industry standards. The results indicate that the e-wallet applications examined, associated with Canadian banks, display vulnerabilities when subjected to diverse security assessments. This underscores the necessity for enhanced security measures within this realm.

According to a recent study[17], E-wallet is a software-based system that stores users' payment information and passwords for numerous payment methods and websites. By using a digital wallet, users can complete purchases easily and quickly with near-field communication technology and can be used in conjunction with a mobile payment system that allows customers to pay for purchases with their smartphones. A digital wallet can also be used to store loyalty card information and digital coupons.

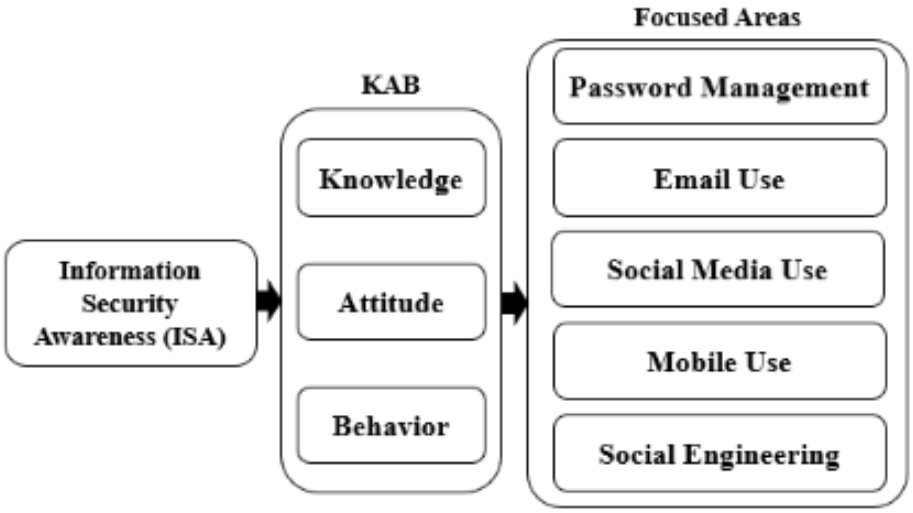


Figure 3 CIA of Security

This study compares factors influencing consumer acceptance of SMS, NFC, and QR mobile payment systems and explores the key factors affecting their adoption. It develops a behavioral model based on an extensive review of scientific literature to explain users' intentions to use mobile payments. The research reveals that user behavior varies depending on the payment tool chosen. It emphasizes the importance of perceived usefulness and security in driving the adoption of these systems. Companies should prioritize developing payment tools that offer greater perceived usefulness and security, surpassing traditional payment methods. This research underscores the significance of addressing perceived security as a critical factor in designing strategies for the adoption of new payment systems.

The results of another study [18] showed that the level of use of ISA, as shown in Figure 3 in terms of passwords, is relatively average, as participants use the same passwords for several different accounts, and sometimes, they may share their passwords with their other friends on the pretext that they may forget the passwords and be reminded of them by others, and about mobile devices, the participants have a good understanding of how to physically secure mobile devices.

The research emphasizes the significant role that users' behavior plays in cybersecurity threats. It highlights how users' lack of awareness and concern regarding security issues can lead to vulnerabilities that attackers exploit. This observation aligns with a common trend in cybersecurity research where human factors are increasingly recognized as crucial elements in overall security.

The study's findings highlight the overall carelessness of internet users concerning security measures, knowledge, and practices. Notably, a significant portion of respondents did not seek to enhance their security awareness through educational means, such as attending awareness courses. It is crucial to note that those with a higher level of security awareness demonstrated more professional behaviors in dealing with cyber threats.

The research concludes by emphasizing the critical importance of information security awareness, particularly within educational environments. It calls for a focus on the human aspect of cybersecurity, recognizing that users' knowledge, behavior, and attitudes significantly impact security. The study identifies areas where participants showed lower awareness, such as social engineering and password best practices, suggesting the need for targeted awareness campaigns and educational interventions.

They do, however, have an average degree of security awareness when it comes to sending sensitive information over public Wi-Fi and a relatively high level of conduct when it comes to making sure outsiders can't see their laptop screens if they're working on highly confidential material.

In today’s fast-moving lifestyle, people use the development of information technology with smartphones; most organizations make applications for smartphones to enable customers to deal and access all the services of the institution to manage accounts, buy and sell, and make all financial services by its private e-wallet, this makes cybercrime to try hack and access data increased, in this research, we’ll show the artifact of e-wallet on a mobile device, and how to decrease the risk of cybercrime and detection of the motives and mechanisms for hacking electronic wallets.

E-wallets use a specialized technology called Blockchain[19], which prevents double-spending. A chain is an encrypted and decentralized ledger of transactions available for each and every peer in the network. The findings of this study may help law enforcement agencies identify the individuals and devices involved in unauthorized transactions employing these Bitcoin wallets on mobile devices and forensically extract wallet application data from the devices.

As criminals began to penetrate and attack, targeting financial markets, electronic and personal digital wallets, and carrying out illegal actions on individual systems, digital forensics has become increasingly popular in combating electronic crimes around the world. This development necessitated the need to safeguard electronic and digital wallets.

The study showed the effectiveness of employing blockchain technology[20] in electronic wallets and how to protect them from potential attacks, such as Phishing attacks, social engineering for corporate employees, attacks on personal digital wallets, distributed denial-of-service attacks on marketplaces, and even coins can be used in these attacks as criminals attack financial markets to reduce the market value of a particular coin, which increases its monetary value and is a quick way to make money when digital criminals attack financial markets to reduce the market value of a particular coin, which increases its monetary value and is a quick way to make money when digital criminals attack financial markets to reduce.

2.3 Neobanks Architecture

A Neobank architecture's essential components are hosting infrastructure, core platform, and application front end. Neobanks use emerging technologies such as biometry, chatbots, and AI to enhance their remote customer interaction model. A neobank consists of three primary components: an API for connecting payment gateways to the neo-banking app, a Card Processing app for transactions, and a core banking system. Neobanks leverage microservices architecture at their heart on cloud platforms such as AWS4 to overcome the drawbacks of conventional banks' large, slow-moving monolithic ecosystems [21]. Hosting all services on the public cloud is not practical for the new banks since they operate in an environment that is highly regulated and data-sensitive. The majority of new banks, whether they are digital platforms or subsidiaries, choose a hybrid cloud infrastructure. A hybrid cloud architecture enables new banks to operate and store data in the private cloud for service development and third-party integration, as well as in the public cloud for third-party integration.

Building platforms that are future-proof is essential in the cloud computing environment because it gives developers the flexibility to quickly construct, test, deploy, and discontinue services.
It makes it possible for new banks to give an improved platform experience and regularly assess their customer experiences since all data and services are kept and hosted on internal or external cloud infrastructure[22] shown in Figure 4, the neobanks incur no capital charges for maintaining the local servers, allowing the banks to cut their capital expenditures and operating costs.

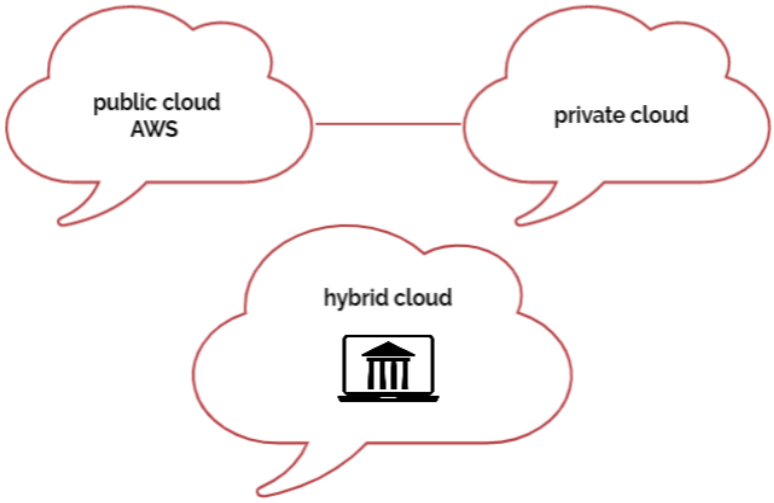


Figure 4 Neobank cloud platform

2.4 Main Components of Neobank Frameworks

Digital strategy: Neobanks places a high priority on digital channels, providing their services via online platforms or mobile apps. By utilizing cutting-edge technology and design ideas, they concentrate on offering a smooth and simple user experience.

Infrastructure: Neobanks frequently base their business operations on cloud-based technologies because they provide scalability, flexibility, and cost-effectiveness. As a result, they can easily adjust to shifting market conditions and rising user populations.

API-driven architecture: Application programming interfaces (APIs) are frequently utilized by Neobanks in order to link with external service providers and supply a variety of financial goods and services. Neobanks can provide services like account aggregation, payments, and collaborations with other fintech platforms thanks to APIs, which facilitate simple connections with other systems.

Innovative features: By providing innovative products and services, neobanks set themselves apart. These might include individualized financial insights, automatic savings, spending categorization, real-time transaction notifications, planning tools, and investment possibilities.

Enhanced user experience: Neobanks promote user-friendliness, efficiency, and accessibility while emphasizing customer-centric interactions. To customize suggestions and boost user engagement, they frequently use sophisticated data analytics and machine learning algorithms.

Regulation conformity: Neobanks must abide by the regulatory frameworks that control the financial sector, including know-your-customer (KYC) and anti-money laundering (AML) rules using blockchain technology. Compliance with these rules is essential to guarantee the integrity and security of consumer data.

Strategic alliances: To improve their product offerings, neobanks typically work with other fintech firms, conventional banks, or technology suppliers. These collaborations could entail adding new financial products to their platforms, including loans or insurance.

2.5 e-wallet architecture

An Android e-wallet is a digital platform that enables users to store, access, and manage their financial transactions. These platforms are often embedded in mobile devices, allowing users to make purchases and pay bills without having to carry cash or a payment card. The app runs on the user's mobile device and provides an interface for the user to interact with the wallet. The server component manages the user accounts and the transaction history. The BLE device acts as a token generator and communicates with the server. It also stores the encryption keys. When a user wants to carry out a transaction, he opens the app on his mobile device. Then, the BLE device generates a token and sends it to the mobile app. The mobile app uses this token to authenticate the transaction with the server, where it is processed and stored [23].

Bluetooth Low Energy (BLE) is a wireless personal area network technology that uses an asymmetric key exchange protocol, Elliptic Curve Digital Signature Algorithm (ECDSA), and a secure Hashing Function known as Secure Hash Algorithm-2 (SHA-2). This type of communication protocol is safer and more efficient than traditional Bluetooth protocols because it does not require pairing between the devices involved. In addition, it makes use of a physical security mechanism called Encryption of Basic Response (EBR) to ensure the integrity and confidentiality of the communication between devices[24].

In order to provide a simple, mobile, and essentially safe payment experience, digital wallets make use of a number of technologies, including mobile applications, mobile devices, near-field communication (NFC) [25], and security techniques like tokenization.

To utilize the electronic wallet, the user must enter their card information into the website or mobile application. The data is encrypted, and the wallet is available for usage after the device has been unlocked and the user has granted authorization for the wallet. To make a mobile payment, the user must keep their smartphone close to the contactless payment terminal; the steps to make a payment through an e-wallet application are shown in Figure 5.

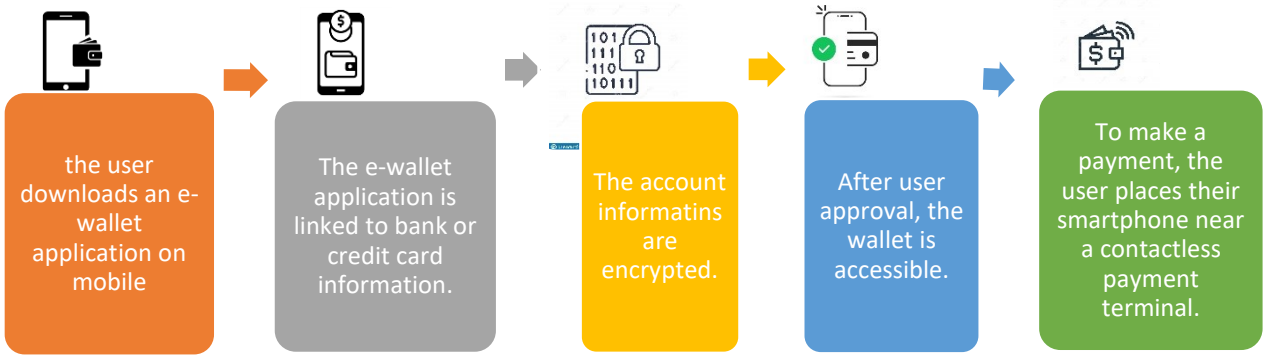


Figure 5- The steps to make a payment through an e-wallet application

The ease of payment through QR code scanning has led to a noticeable and widespread adoption of electronic wallets, as indicated by previous studies. Quick response (QR) codes are among the technologies that electronic wallets employ most frequently. To start the payment, the user can scan these barcodes with their smartphone camera or their electronic wallet system, which decodes the information into a black-and-white pattern. Information such as the transaction amount and the intended recipient can be encrypted by payment applications. For instance, a QR code that enables customers to use their account to pay for things in the store may be made in a PayPal app.

2.6 Mobile OS. architecture

2.6.1 Android architecture

Android, the world's most popular mobile operating system, is renowned for its robust and flexible architecture. This architecture serves as the foundation for the development and execution of Android applications. Understanding the intricacies of Android's architecture is crucial for both developers and enthusiasts, as it provides insights into how Android applications are created, managed, and run. In this exploration, we will delve into the key components and layers that comprise the Android architecture; as shown in Figure 6, android architecture is as follows: **Linux Kernel** covers key services such as memory, network, and process management, as well as security, **Libraries and android Runtime** It consists of a set of original code libraries that are written in C and C ++ and most of the libraries of this layer are open source for the possibility of modification[26].

Figure 6 Android architecture

Application Framework Provides an application programming interface and higher-level services to us. These high-level services are also used by Android developers to construct apps. **Applications** This layer is made up of native Android applications as well as third-party installed apps. They come as part of an Android package, and all of the apps that need to be installed, such as contacts, games, settings, and messages, are developed in this layer alone.

In a forensic investigation, it helps to comprehend the underlying functions, file structures, and capabilities of an Android device. In contrast to iOS, there are many different versions of the Android operating system, and each one may have a different file system and special features. [27] The openness and adaptability of Android also alter the playing field for digital forensics. When handling an Android device, a forensic examiner needs to be ready for the unexpected.

2.6.2 IOS architecture

iOS architecture, as shown in Figure 7, forms the foundation of Apple's mobile devices, defining how hardware and software interact to deliver a seamless user experience. This sophisticated operating system powers iPhones, iPads, and other Apple products. In this overview, we'll explore the key components and layers of iOS architecture, providing insights into its design and functionality[28].

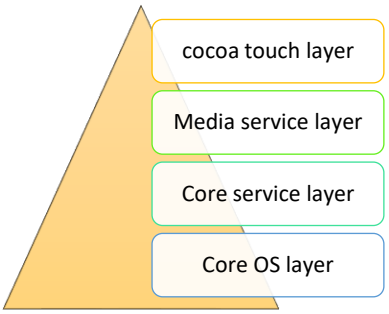


Figure 7 IOS architecture

The cocoa Touch layer includes the UI Kit Framework, the Map Kit Framework, Push Notification Service, Message UI Framework, Address Book UI Framework, the Game Kit Framework, the Event Kit UI Framework, the Accounts Framework, and the Social Framework.

The Media layer is considered one of the most important layers in the iPhone, as it consists of graphics, audio, and video. And **the core services**, which include the functions to manage the fundamental system services for native iOS applications. **The Core OS** is mainly responsible for all the tasks of other operating systems and management of the device's memory, file system, and networks, which is the layer of direct interaction, as shown in Figure.

2.7 e-wallet in Palestine

According to studies that show[10], [27], although the existence of electronic wallets in Palestine is considered a recent topic for the Palestinian user, it can be relied upon as a payment method approved by many users, as 70% of electronic wallet users are users of Jawwal Pay in Palestine, which is affiliated with Jawwal, which has effective and influential advertising tools to use the application. Cash payment is used on a daily basis, whereas the other payment methods (E-wallet and Debit/Credit Card) are used more frequently on a monthly and weekly basis. This is because debit cards and e-wallets have issues when people use them. Palestine recently began using 3G service, which is still new to users, does not cover all areas, and faces problems spreading due to obstacles posed by the occupation[29].

Arabi Wallet is a new electronic wallet from Arab Bank that allows you to receive and send money, deposit and withdraw cash, and complete all of your purchases at merchant POS terminals, delivering an easy and smooth digital experience for all Arab Bank customers. MaalChat, which is still a new application on the market, was the second and third company, respectively.

According to the report of the Palestinian Monetary Authority, table 1 shows the electronic wallet companies licensed by the Monetary Authority and active in the local market in the State of Palestine[30].

Note: the numbers in the Table 1, Until the moment of preparing this research

Table 1 E-wallets in Palestine and Downloads number

E-wallet company name	Acronym	Website	Download number	
			Android	IOS
National Electronic Payment Company	JAWWAL PAY	www.jawwalpay.ps	Above 100K	78.2K
Pal Bay Advance Payment Company	PalPay	www.palpay.ps	Above 10K	
Middle East Payment Services	MEPSPay	www.mepspay.com	Above 10K	
Malchat Electronic Payment Company	Maalchat	www.maalchat.ps	Above 50K	
Your online payment company	eFAWATEERcom	https://madfooat.com/ar/	Above 500K	

2.8 e-wallet in worldwide

In Table 2, the seven best electronic wallets in the world are with the country of origin, according to previous studies, and according to the highest number of downloads.

Table 2 Best e-wallet application in the world by its countries

E-wallet name	Country	website	Download number	
			Android	IOS
Boost	Malaysia	https://www.myboost.com.my	+ 5M	78.2K
DANA	Indonesia	https://www.dana.id/en	+ 50M	
MOMO	Vietnam	https://momo.vn	+ 10M	
APPLE PAY	United States and international	https://www.apple.com/apple-pay/	No	
VENMO	United States and international	https://venmo.com	+ 10M	
SAMSUNG PAY	South Korea and international	https://www.samsung.com/us/samsung-pay/	+ 100M	No
GOOGLE PAY	United States and India	https://pay.google.com/gp/w/u/0/home/signup?sctid=8199300639024387	+100M	

2.9 Summary comparison between e-wallet in Palestine and worldwide

BOOST, Malaysia's mobile payment app, officially launched in 2017 as a platform that digitized one of the telco's core services – the way prepaid users top up their mobile credit. Boost allows users to pay via their mobile device at participating locations without the hassle of using physical cash or cards; to date, they have 8.8 million Boosties and more[3]. **DANA** is an Indonesian e-wallet that provides clients with simple services for paying for services and goods. Customers may use DANA to pay their monthly power and water bills and a telephone data plan. Vendors who accept DANA as a form of payment are easily identified by their blue QRIS scanners. Vendors can simply match a customer's DANA QR code with their scanners for a fast e-wallet payment procedure. DANA does not charge a fee for transactions to or from any bank or between DANA accounts. **MOMO** is the best one in Vietnam, and it's an e-wallet and mobile payment software developed by a Vietnamese company. Users can pay bills online, conduct peer-to-peer transfers, acquire gaming credit, and top up their accounts[31] presently integrated with 24 domestic banks as well as foreign payment networks like Visa, MasterCard, and JCB, and supports payments to approximately 100 service providers and online enterprises. The program had around 10 million subscribers on both iOS and Android as of October 2020.

APPLE PAY is a mobile payment and digital wallet service. It's an international E-wallet and it's developed in the United States by Apple Inc. It is a simple, streamlined digital wallet app for iPhone and Apple Watch users only. It allows you to participate in both in-store and online transactions. In-store, simply use your smartphone's PIN number or FaceID to verify your identity, then hold your handset near a compatible Point of Sale (POS) system to complete the transaction. One of the most appealing features of Apple Pay is its simplicity, which allows you to make payments quickly and securely. That allows users to pay in person, via iOS applications, and on the web using Safari.

It runs on Macs, iPads, Apple Watches, and iPhones. It cannot be utilized on any client device that is not an Apple product, including any Android devices and browsers that are Windows-based. It digitizes and can take the place of a credit or debit card chip and PIN transaction at a point-of-sale terminal that supports contactless payments. Apple Pay is an NFC-based wireless payment system, NFC is a catch-all phrase for wireless data transfer across short distances of less than 10 cm. Smartphones can connect with anything, having an NFC interface via peer-to-peer communication, allowing them to receive information from the payment terminal and make transactions. **PAYPAL** was one of the first digital wallet companies to emerge in the United States and internationally. it is a tried-and-true, trustworthy organization; look no further than it is one of the oldest prominent digital payment companies. The software allows you to send money or make payments faster than usual by bypassing the login screen and the time-consuming process of inputting your password. You may enjoy this experience on your desktop, tablet, or laptop as well. The disadvantage is that PayPal (PYPL) - Get PayPal Holdings, Inc. Report still charges a fee when transferring funds from a credit card or converting a transaction to another currency, and it has steadily evolved into a platform based on customer feedback. Consequently, users may make and receive payments in over 25 currencies worldwide using a single browser platform, making it ideal for personal usage. **VENMO** is the best e-wallet in New York, and it's an international peer-to-peer (P2P) payment service. It's a smartphone app that makes it simple to send money to pals. There's no need for a credit card, a wallet, fees, or nagging about overdue beverages. Simply link the app to a debit card and start spending. **SAMSUNG PAY** is a South Korean and international e-wallet mobile payment and digital wallet service by Samsung Electronics that allows customers to pay with compatible phones and other Samsung-made devices. By combining magnetic secure transmission, the service allows contactless payments through near-field communications (NFC), as well as magnetic strip–only payment terminals. It also facilitates bill payments in India.[32] it's one of the most popular digital wallet apps on the market. They've been in business since 2011. It's highly adaptable, even though it's only for Samsung (SSNLF) users. You can pay in person, on the app, or online, and

you can earn unique perks and cash back at key stores along the way. This results in a potent combination that is impossible to ignore. Make sure your preferred banking institutions are covered before committing to Samsung Pay. Though they support the majority of large financial institutions as well as a slew of smaller ones, it's always a good idea to double-check. **GOOGLE PAY** is a Google-developed Users of Android smartphones, tablets, or watches can utilize the digital wallet platform and online payment system to do contactless in-app, online, and offline transactions. In India and the US, iOS smartphones are also usable, albeit with fewer capabilities. Furthermore, the program supports coupons, boarding passes, campus ID cards, auto keys, event tickets, movie tickets, public transportation tickets, shop cards, health records, and loyalty cards. **JAWWAL PAY** is a leading company in the field of electronic payment and electronic wallet services in Palestine. It was established as a private limited joint stock company in February 2018 and was licensed by the Palestinian Monetary Authority (PMA) as a PSP payment service provider to provide electronic payment services and electronic wallet services. The company was established to develop services for electronic payment and its provision to the Palestinian community, especially citizens who do not have bank accounts or who do not benefit from current banking services. Among the company's services: transferring funds locally, paying bills, recharging the balance, online shopping, and paying via QR code for merchants, the company came to fill the gap in the absence of electronic payment services that the Palestinian market desperately needs, through innovative electronic payment systems, to transform the national economy to an advanced digital economy and control the Coronavirus crisis and the many ways of infection of the disease.[33] Pal Pay was established in 2010 in partnership with the Bank of Palestine, the First National Bank, and PCNC IT Solutions to create a new electronic collection system in Palestine in particular and the region in general. By dealing with **Pal Pay** services and paying his bills, charging his mobile device, paying his dues, or paying a friend easily and safely without waiting in queues and wasting time and going to the nearest collection center to pay his dues with the companies he deals with. It also reduces the cost of collection on billing companies

and introduces new and innovative collection mechanisms that serve the interests of these companies and institutions substantially and provide them with cash very quickly, which gives them the ability to grow and develop.[34]

MEPS is a mobile payment service provided by the Middle East Payment Services Company - MEPS, and licensed by the Central Bank of Jordan under the umbrella of the national mobile payment gateway JoMoPay; it has been present in Palestine since 2009 and is now a licensed party to undertake the activities of issuing and providing payment cards in the Palestinian markets, where the demand for electronic payment services is increasing. The company provides a variety of services to several banks, including card issuance services, ATM management, and point-of-sale management services.[35]

Maalchat is an electronic wallet that guarantees you a safe and easy way to organize your financial priorities in one place through your smart device connected to any network of licensed Palestinian cellular telecommunications companies (Jawwal and Ooredoo). With an escrow account with a working bank under the supervision of the Palestinian Monetary Authority, a secure chat system provides instant communication with your friends and customers, exchanging photos and files and sharing sites. [36]

eFAWATEERcom is an integrated instantaneous system that replaces paper bills and traditional payments with an easy-to-use electronic payment service system on the Internet and mobile devices, accelerating the adoption of this payment system. It was established in partnership with the Central Bank of Jordan and licensed by the Palestinian Monetary Authority. It provides electronic cash collection services, facilitating payments, reducing costs, and collecting payments efficiently [37]

2.10 Comparative

Prior research revealed a significant increase in interest in e-wallets and online payment. This, combined with the prevalence of people using various types of wallets for electronic payment, calls for researchers to concentrate on the security features of e-wallets to close the significant gaps. Electronic payment offers several security features, including confidentiality, availability, authorization, integrity, and non-repudiation[38].

In Palestine, Jawwal Pay, Pal Pay, and eFAWATEERcom are leading the way in providing efficient and secure electronic payment services. Jawwal Pay, licensed by the Palestinian Monetary Authority, offers services like fund transfers, bill payments, and online shopping to bridge the gap in electronic payment services within the Palestinian market. Pal Pay, established in partnership with local banks, enables easy bill payments and reduces business collection costs. MEPS, licensed by the Central Bank of Jordan, facilitates card issuance and management services, catering to the increasing demand for electronic payment services in Palestine. Maalchat, with its secure chat system and diverse financial services, offers a comprehensive digital experience for users.

On the global front, e-wallets like BOOST in Malaysia, DANA in Indonesia, and MOMO in Vietnam have gained popularity for their user-friendly interfaces and versatile payment options. BOOST provides a convenient way to top up mobile credit, while DANA simplifies bill payments and offers QR-based transaction services. MOMO, integrated with multiple banks and foreign payment networks, allows users to pay bills, transfer funds, and make online purchases seamlessly. Apple Pay, known for its simplicity and secure transactions, is exclusive to Apple devices and facilitates in-store and online transactions. PayPal, a trusted digital payment platform, offers fast and efficient money transfers, although it may incur specific transaction fees. Venmo, an easy-to-use P2P payment service, allows users to send money effortlessly. With its adaptable payment options and perks for Samsung device users, Samsung Pay has become popular. Google Pay, a Google-developed digital wallet, provides a versatile payment system for Android users, with support for various coupons and loyalty cards.

Both the e-wallets in Palestine and those in the global market offer unique features and cater to specific user needs, contributing to the growth of the digital payment landscape.

In this context, security concerns the risk of fraud and the level of protection against fraudulent activities. Mobile payments ensure secure transactions through advanced technological techniques like encryption, reducing the likelihood of theft. However, user concerns about security and technical measures remain widespread. Some users may hesitate to adopt electronic payments due to their apprehensions about sharing personal data and their lack of trust in e-wallet application providers [39]. Table 3 below presents a comparative analysis of the automation features between a local e-wallet in Palestine, Jawwal Pay, and the global e-wallet, Apple Pay:

Table 3 compares e-wallets in the world and Palestine.

	e-wallet in worldwide	**e-wallet in Palestine**
Geographic Reach	A globally recognized e-wallet is accepted in numerous countries, making it suitable for international travelers. Device Compatibility:	Primarily serves customers in Palestine and may have limited international acceptance.
Device Compatibility	Apple devices like iPhones, Apple Watches, iPads, and Macs.	Android and iOS
Currency	multiple global currencies	Palestinian currency (NIS)
Security	security features, including tokenization, biometric authentication (Face ID/Touch ID), and device-specific security.	Standard security measures, but their level of security may vary.
Developer Ecosystem	provides a robust developer ecosystem for integrating payment functionalities into various apps and services	limited third-party app integrations
Example	Apple pay	Jwawal pay, Reflect Neobank

In the Apple Pay Wallet, Apple assigns a unique account number to each approved payment card to be authenticated and stored in the secure element of iPhone phones, where these account numbers are used by coding schemes in addition to the security code instead of using the credit card details, whether the card number or the C number In the card's VV, this guarantees the consumer higher protection and security, as he does not have to reveal his credit card details when making payments. One of the advantages of the Apple Pay Wallet is also the ability to add the payment card to the Apple passbook through the iTunes application [39]

The prosperous electronic wallet market's future depends on how satisfied consumers are. To combat hackers and fraud that are starting to appear in Palestine, e-wallet security should be established. To improve customer satisfaction with e-wallets and boost consumers' confidence in what competes with global wallets, wallet providers may utilize this to strengthen system security and concentrate on crucial security elements. [40]

The neobank framework and the cloud payment framework are two separate ideas that have to do with various facets of the financial sector. Let's see how they differ from one another:

Cloud payment framework: The infrastructure and technology needed to facilitate payment processing and related services using cloud-based systems are referred to as the cloud payment framework.

Cloud payment frameworks take advantage of cloud computing's capabilities to offer scalable, secure, and adaptable payment processing solutions. With this architecture, data, and transactions pertaining to payments are stored, processed, and sent via cloud servers. It eliminates the need for expensive on-premises equipment by enabling companies and financial institutions to delegate the management of payment systems to cloud service providers.

Cloud-based payment systems can be used by a variety of organizations, such as conventional banks, fintech firms, payment processors, and other financial service providers. Peer-to-peer transfers, internet transactions, mobile payments, and other types of digital payments are all handled more efficiently, thanks to these frameworks.

The cloud payment framework places a strong emphasis on the technological side of payment processing, enabling quick and safe transaction processing. This framework is on the PAYPAL wallet.

Neobank framework: as was previously mentioned, neobanks are exclusively online financial institutions that provide banking services primarily through digital channels. The neobank framework relates to the operational and technological framework used by neobanks. Neobanks strive to offer a technologically advanced, user-friendly banking experience, generally via mobile applications or web platforms, because it includes more services than just payment processing. In addition to checking and savings accounts, budgeting tools, investment possibilities, loans, and other specialized financial services, neobanks also provide a variety of additional financial goods and services that as REFLECT Neobank. To supply these services, they frequently make use of cloud-based infrastructure, API connections, data analytics, and cutting-edge features.

The neobank framework covers every aspect of a digital bank's operational structure, including customer acquisition, account management, financial products, user experience, compliance, and partnerships, in contrast to the cloud payment framework, which focuses specifically on the technology and infrastructure for payment processing.

In summary, the cloud payment framework primarily focuses on the technical aspects of payment processing via cloud-based systems. In contrast, the neobank framework is more comprehensive, encompassing the entirety of operations and technology within an online-only bank. This broader framework extends beyond payments, encompassing a wide range of financial services.

Chapter 3
Research Methodology and Experiment Setup

3.1 Introduction

The main objective of the research is to measure the security and reliability of local electronic wallets. In designing the research, the researcher distributed a questionnaire to electronic wallet users to assess the level of security they perceive, comparing it with the security level observed by the researcher in the practical aspect of digital forensics for electronic wallets as shown in Figure 8. The research also explains the details of the data acquisition process on Android and iOS operating systems, in addition to the research tools that were used.

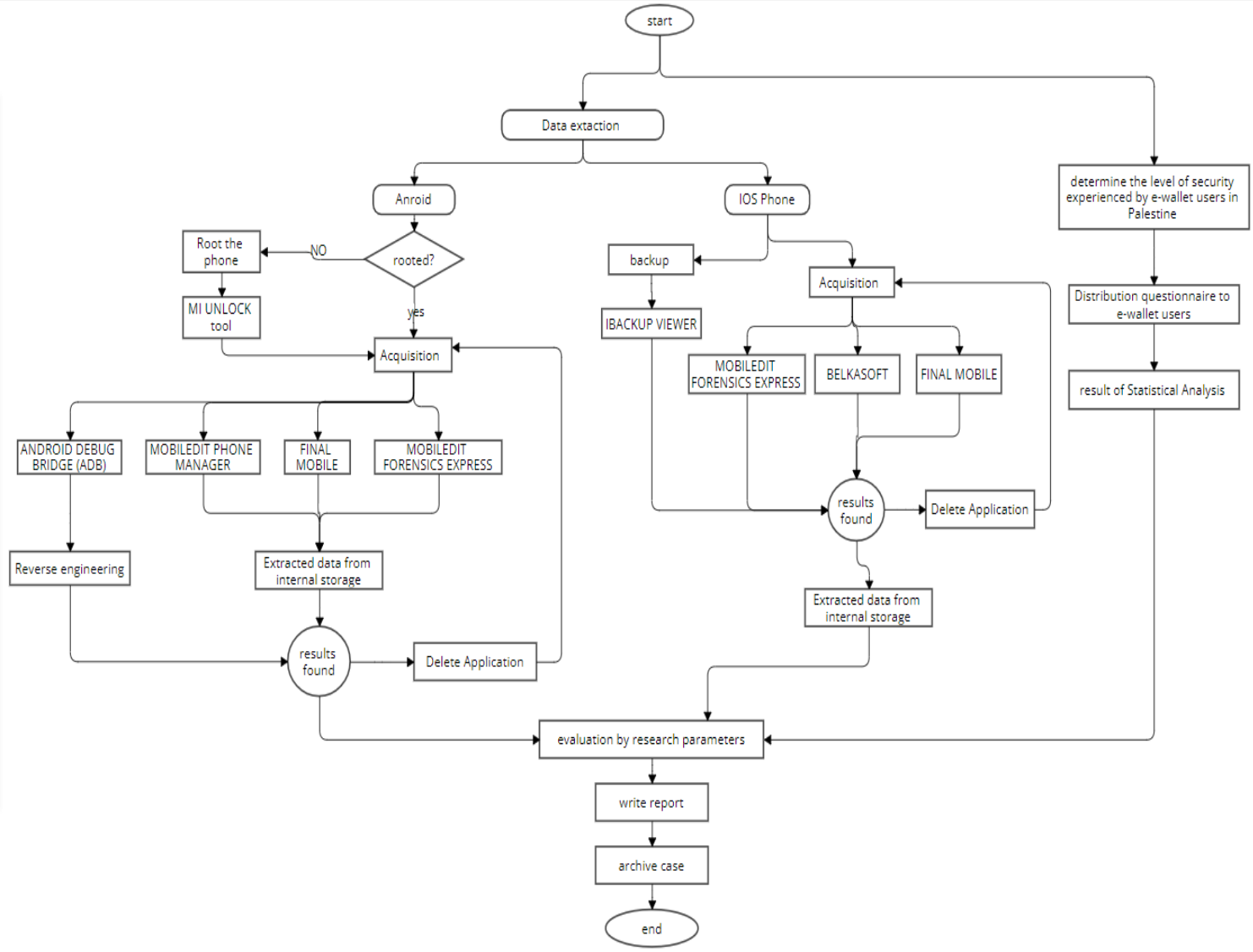


Figure 8 Research methodology: a detailed flow chart of actions performed during forensic analysis.

The ease of digital payment methods attracts people, but they fear the extent of their exposure to these sites. According to recent statistics [2] 69% of digital payment users are worried about security issues, but the majority still use the platforms monthly because security concerns increase with the use of e-wallets; for example (41%) of people fear hacking because it the most common security concern followed by fraud (16%) and theft (12%). The research indicates that despite security precautions such as two-factor authentication, encryption, and tokenization, users are still suspicious of these sites.

We conducted a survey and statistical analysis by selecting a sample of 90 participants to determine the level of security experienced by e-wallet users in Palestine. *Figure 9* illustrates the axes used to measure e-wallet security in the questionnaire for this research. After compiling the questionnaire from the sample participants and coding it, the data was entered into the computer and processed using the statistical analysis program (SPSS) version 27.

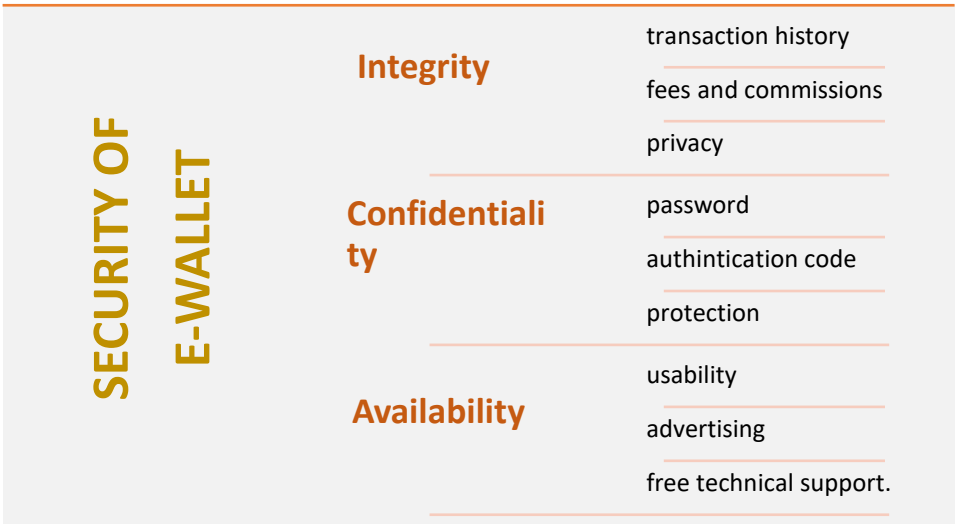


Figure 9 SECURITY axes in the electronic wallet according to the questionnaire for this research.

This section of the study utilized an empirical research methodology. Participants who met the requirements for using any electronic wallet platform, including mobile applications and web-based systems, were given access to a quantitative online survey. A total of 90 responses were received. The survey had two components. The first component collected demographic information, such as gender, age, employment, and the frequency of e-wallet transactions, while the second part involved respondents rating their agreement with each statement on a five-point Likert scale.

To ensure the research's credibility, we will implement measures to control for potential confounding variables and data errors. Utilizing SPSS analysis, I will evaluate the logical alpha value of the questionnaire data. A satisfactory alpha value surpassing 70 will validate the data, while any value falling below this threshold will prompt the collection of new data for further validation.

To ensure the integrity of the analysis, it is imperative to clean the mobile devices thoroughly and eliminate any potential interference from other applications. Furthermore, employing a diverse range of mobile forensics tools for data acquisition will be essential to validate the accuracy and consistency of the data obtained from multiple sources.

3.2 Statistical Analysis

Respondents used a five-point Likert scale to indicate their level of agreement with each statement in the second section. The degree of agreement is considered in the study's evaluation process. The 22 questions in the second section were grouped into four categories, each comprising four questions. Ten questions were designed to assess the use and safety of the e-wallet, while six questions were dedicated to evaluating the proposed framework's confidentiality and availability. Factor analysis and reliability analysis were performed using the collected questionnaires. IBM's Statistical Package for Social Science (SPSS) version 27.0 software was employed for statistical significance determination.

Given the limited sample size and the novelty of the topic in Palestine, it was necessary to assess the reliability of the respondents using a reverse question in the questionnaire. The statistical analysis results revealed that out of the initial 91 surveys, 70 were considered valid, while 21 were excluded due to providing random responses to two reverse questions, indicating an unreliable completion of the questionnaire. These findings are presented in Table 4.

Table 4 case processing

Case Processing Summary

		N	%
Cases	Valid	70	76.9
	Excluded[a]	21	23.1
	Total	91	100.0

a. Listwise deletion based on all variables in the procedure.

As shown in Table 5, the majority of respondents use a JawwalPay wallet and a Palpay wallet, which are popular with young people.

Table 5 CHARACTERISTICS OF RESPONDENTS

Indicator	Total cell	Accuracy (%)
Gender	male	56.7
	female	43.33
Age	15-24	14.44
	25-34	46.67
	UP 35	38.89
Job	student	11.11
	government employee	45.67
	special officer	25.44
	not working	17.78
It knowledge	very high	26.88
	high	33.22
	neutral	32.11
	weak	6.44
	Very weak	1.35
Payment method	Jawwalpay	44.22
	Palpay	23.43
	Reflect neobank	20.11
	Apple pay	10.11
	Efawateer	1
	Maalchat	1.13

The internal consistency of the dataset was evaluated through a reliability test conducted using the SPSS program. The reliability coefficient yielded a value of 0.76, which is considered acceptable. This result suggests that the questionnaire administered to the study participants is statistically reliable. The study findings can be confidently interpreted based on this coefficient, providing insights into the level of security perceived by the users. Table 6 presents the reliability coefficient.

Table 6 Reliability statistics

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.760	.916	22

In testing the second hypothesis concerning the safety and impenetrability of the electronic wallet application, it was observed that 66.67 percent of the respondents viewed electronic wallets as safe and impenetrable, while 33.33 percent expressed doubts about their security. This confirms the users' perception that electronic wallets are secure, as indicated by our study. Furthermore, to evaluate hypothesis H2.1, which suggests a lack of integrity in the local electronic wallet, the responses to the questionnaire on the third axis were considered. It was noted that Paragraph No. 3, which asserts that users can easily view and verify their account transaction log, received the highest percentage. In contrast, Paragraph No. 2 and Paragraph No. 4, highlighting the provision of accurate details of fees and commissions and technical support for financial transaction issues, respectively, obtained the lowest percentage, as illustrated in Table 7. This contradictory data confirms that the e-wallet maintains a sufficient level of integrity, according to user perspectives, with variations observed in the performance of technical support and user follow-up for e-wallets.

Table 7 Integrity levels

b1.5	4.0429	1.10906	70
b2.7	4.0714	1.14615	70
b3.8	4.1000	1.15658	70
b4.9	3.7571	1.20909	70
b5.10	3.9286	1.10757	70

In assessing hypothesis H2.2, which suggests the lack of confidentiality in the local electronic wallet, the responses to the questionnaire on the third axis were considered. It was noted that Paragraph No. 2, emphasizing the use of strong passwords for the electronic wallet, received the highest percentage. In contrast, Paragraph No. 6, which highlights the activation of the wallet by an authentication code via the mobile phone, and Paragraph No. 5, mentioning the practice of recording passwords in a notebook, obtained the lowest percentage, as indicated in Table 8. This data contradicts the hypothesis, demonstrating that the e-wallet is indeed reliable, according to user perspectives.

Table 8 Confidentiality level

c1.11	3.3429	1.50252	70
c2.12	4.3000	1.05432	70
c3.13	4.0429	1.16016	70
c4.14	3.0286	1.51295	70
c5.15	2.8286	1.55080	70
c6.16	4.1143	1.21038	70

Examining hypothesis H2.3, which suggests the unavailability of the local e-wallet, based on responses to the questionnaire's fourth axis, it was observed that Paragraph No. 1, highlighting the ease of dealing with the e-wallet application, received the highest percentage. In contrast, Paragraph No. 2 immediately follows it and emphasizes the presence of a dedicated guide provided by the e-wallet company for facilitating transactions, along with Paragraph No. 6, which mentions the lack of awareness about a dedicated assistance number within the e-wallet company, obtained the lowest percentage, as depicted in Table 9. This finding contradicts the

hypothesis, suggesting that the electronic wallet is indeed available, according to user perspectives.

Table 9 Availability level

d1.17	4.2714	1.03450	70
d2.18	3.8857	1.16149	70
d3.19	3.8571	1.17073	70
d4.20	3.5571	1.25843	70
d5.21	3.5000	1.31601	70
d6.22	2.9857	1.47926	70

The results of the statistical analysis demonstrate the users' sense of security, reliability, and accessibility in Palestine. The findings indicate that the limited use or non-use of e-wallets, particularly for transferring significant amounts, could be influencing their perceived level of security. Additionally, users might be content with their restricted interactions with local electronic wallets due to their lack of familiarity or experience with such platforms.

3.3 Tools & Methods

By using the SPSS program is a software platform that includes advanced statistical analysis, a large library of machine learning algorithms, text analysis, open-source extensibility, big data integration, and seamless application deployment. Ad hoc analysis, hypothesis testing, spatial analysis, and predictive analytics are used to solve commercial and research challenges, and this requires checking the alpha value of the SPSS result and ensuring that all data is valid before analysis. Make Data acquisition for android mobile in many modes, first one when application is installed, second application deleted, third when make reset factory of mobile, and fourth when application turn on, and finally with rooted, make these steps with Android and IOS mobile. Will extract all artifacts of e-wallet application on mobile by many mobile forensics tools:

- Belkasoft Evidence Center program, Software Belkasoft Evidence Center also has the ability to automatically perform all the analysis and analysis. Support for Windows, Linux, macOS, iOS, Android, Windows Phone, Blackberry OS, including a variety of smart devices. The performance of this program is less evidence, which will be ignored. This means that the software will not remove data corrupted and broken by looking for unusual locations and analyzing deleted data.
- MOBILedit forensics express is a tool to extract phone data analysis and create reports. A powerful application that uses both methods to collect physical data and logic, Forensic Express is great for process analysis, application, advanced recovery, and deleted data. Many types of phones are supported, including most of the feature phones, report, refine, handle the mobile device at the same time and easy to use user interface, and it collect all application info standard and deleted are installed via phone and displayed as a timeline.
- ibackup viewer pro this program Extract all things on IOS device, and the most important feature of an iPhone backup extractor is recovering applications.
- FINAL MOBILE FORENSICS4 provides our forensic community with the most cutting-edge data-carving tool. FINALMobile can transform unstructured data into understandable data with a few easy clicks thanks to our in-depth understanding of file systems and data patterns. Specific file formats are used to store data on mobile devices, and the data is frequently left behind. These "deleted entires," or buried treasures, can be recovered together with the entirety of the "live" material by looking for precise patterns. Additionally, as numerous gadgets follow the same pattern, we could already have a fix for phones in the future. We can still evaluate data by examining each sector for certain data even if the file system fails to fill. To make it simpler for the user, the data may be arranged in a number of different ways.

Our research methodology uses mixed methods: the quantitative approach to measure the safety of the application and the qualitative approach to know the improvements that must be developed to improve the security and safety of the application[41]. Information can be collected through questionnaires for e-wallet users to measure the security of e-wallet application and the most used, and through data-set by acquisition of e-wallet application on two mobiles with different operating systems on many modes. The research population is users of electronic wallets in Palestine and compared with international feedback users of electronic wallets.

3.3.1 Extract Data - Acquisition stage:

To extract data from devices, we need to conduct acquisitions from the mobile. Table 10 provides details about the tools and devices that have been used in the practical forensics for this research.

Table 10 Hardware forensics details

DEVICE	SPECIFICATION
FORENSIC WORKSTATION	MSI laptop Window 11 Pro OS Processor intel core i5- 2.40GHz Memory 8 GB
IPHONE DEVICE	iPhone 11 Storage 128 GB IOS 16.4.1
	Redmi Note 8 -rooted phone Storage 64 Android 11 RKQ1.201004.002

3.3.2 Extract Android data

The rooting technique must be employed in this study because it grants us complete access to the user data area and the device file system, which house the most crucial forensic evidence. Additionally, it makes it possible to retrieve additional beneficial data at a later stage of the research.

3.3.2.1 Android Rooting

To enable root process in mobile we need to open developer mode on MI mobile device via ***settings,*** find ***about phone*** section, and tap on ***MIUI version*** several times to enable a developer and use secret options Android. After that must unlock the MI device and open the bootloader as follows:

1- disconnect wifi and connect 3G

2- login to mi cloud account

3- install MI UNLOCK

4- Shutdown the mobile

5- Open fast boot mode by press volume down and power button to 30sec, or enter fast boot by using ADB tools as shown in Figure 10.

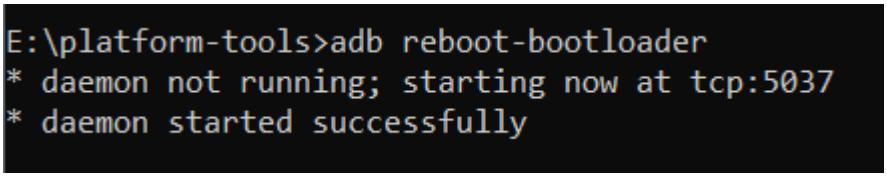


Figure 10 adb fastboot mode

6- After that, open MI unlock, connect the device by cable, and Click on UNLOCK button as shown in Figure 11 (A valid MI Account, associated with the phone used to certification in the bootloader unlocking procedure. (Via official MI UNLOCK)

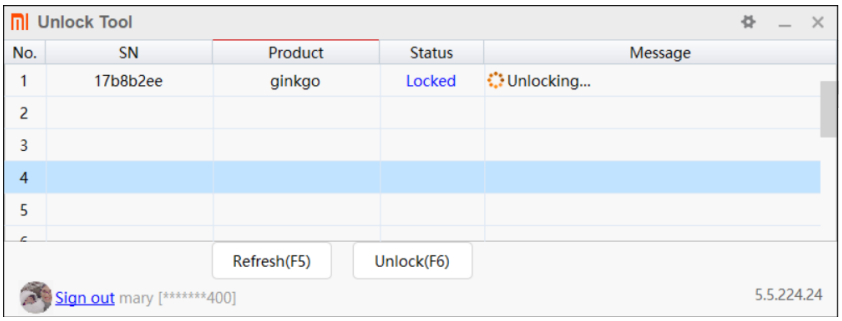


Figure 11 MI phone unlocking

7- And after at least a week's duration, the message appears on MI UNLOCK TOOL when the phone is rooted. Unlocked Bootloader *(new devices usually have a 7-day waiting period)*

3.3.2.2 MOBILedit forensics express

Reflect application on Android mobile:

I took a backup copy from my Android mobile device and made an acquisition for the reflect application, and this was made by activate the developer option and USB Debugging; after several attempts to perform a forensic analysis of the application it failed as shown in Figure 12.

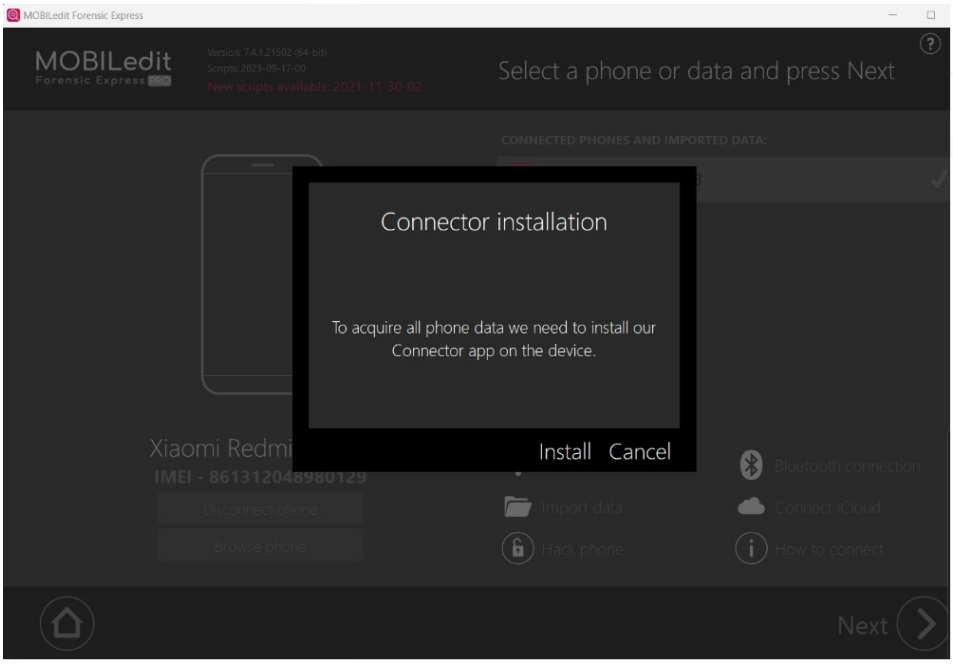


Figure 12 Unsuccessful attempts to acquire for android mobile

Another tool of mobileEdit is Mobile Edit Phone Manger V10.7 - Enterprise, which makes sure the forensic connector is available for the acquisition, as shown in Figures 12-a and 12-b, and it turns out that the problem is not in the analysis tool.

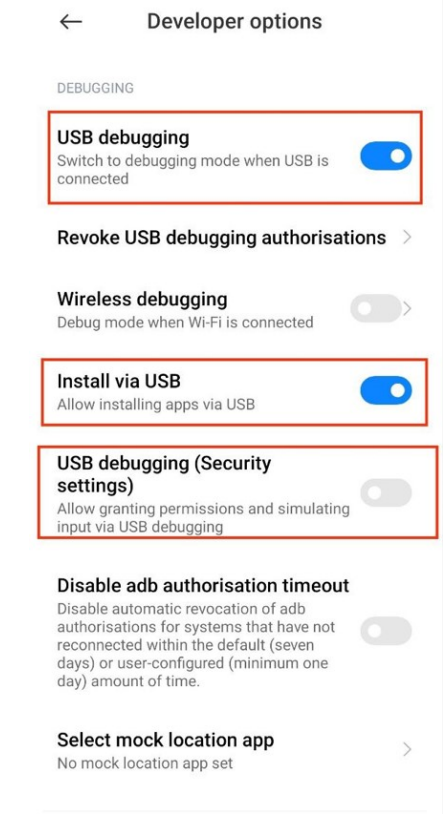


Figure 12-a Solved connection between xiaomi phone and forensics tool

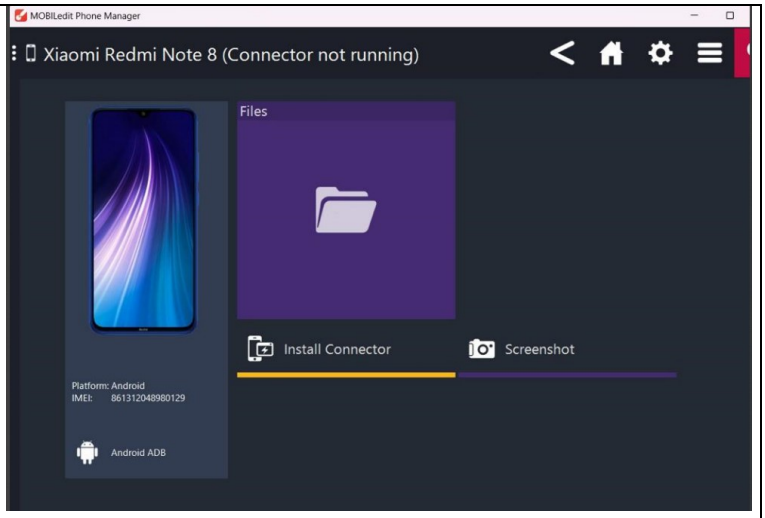


Figure 12-b Mobile-edit phone manager shows the phone but is not able to make a connector.

So, it turns out that there's a problem with connecting the phone to the forensic tool, and after many attempts to solve it, it turns out that so that the analytical tools can access Xiaomi devices, it requires activating **Install via USB** from developer option and deactivated USB debugging security setting as shown in Figure 13 and make acquisition.

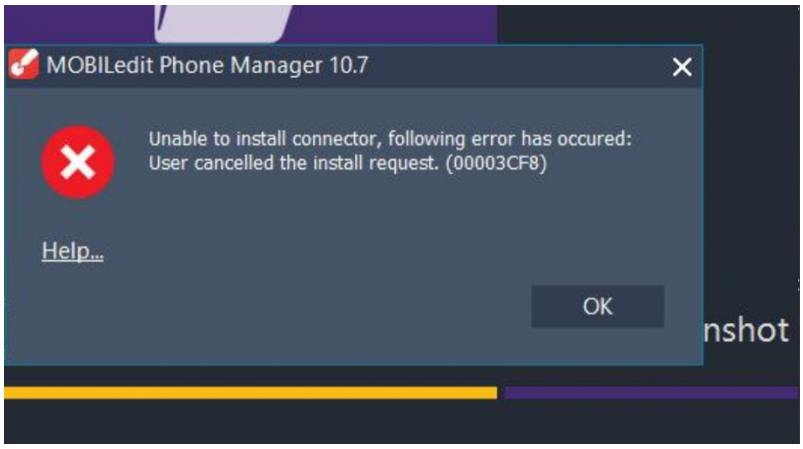


Figure 13 Same error of connection with Mobileedit phone manger tools

After solve the problem by available install via USB and Ensure that the crack is activated for the analysis tool, Data acquisition is possible through the analysis tool, and the communication issue between the phone and the analysis tool has been resolved, as shown in Figure 14

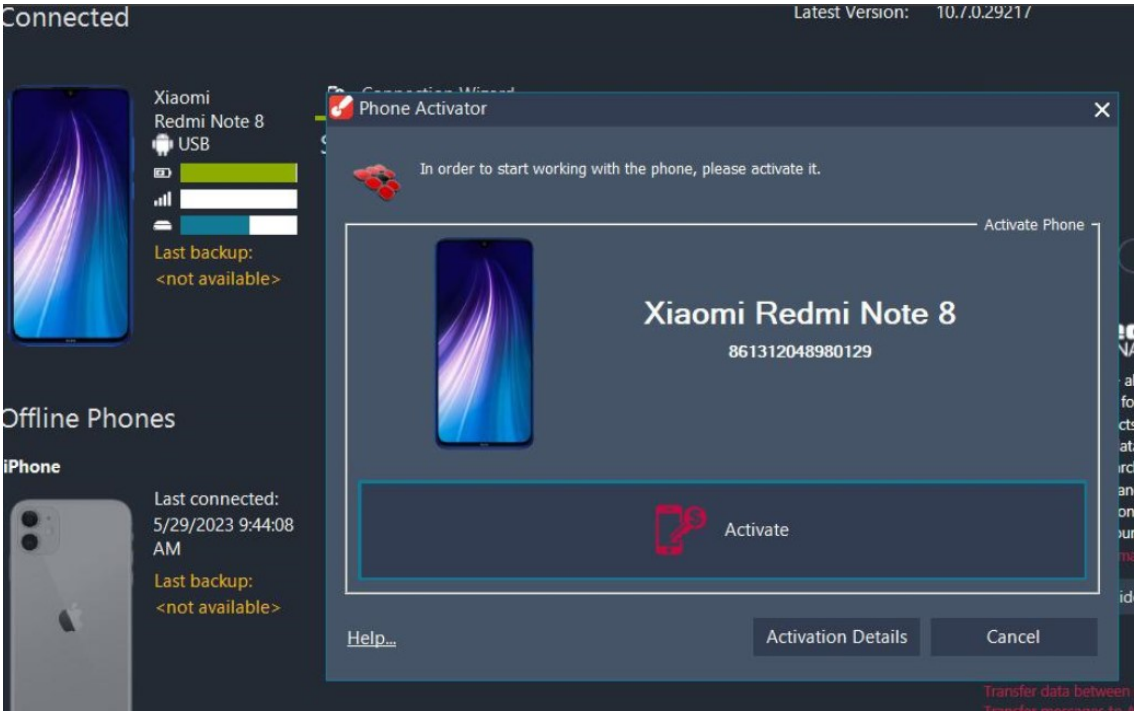


Figure 14 Connected mobile device by mobileedit phone manager forensic tool

And make acquisitions for reflect application by mobile phone manager, as shown in Figure 15

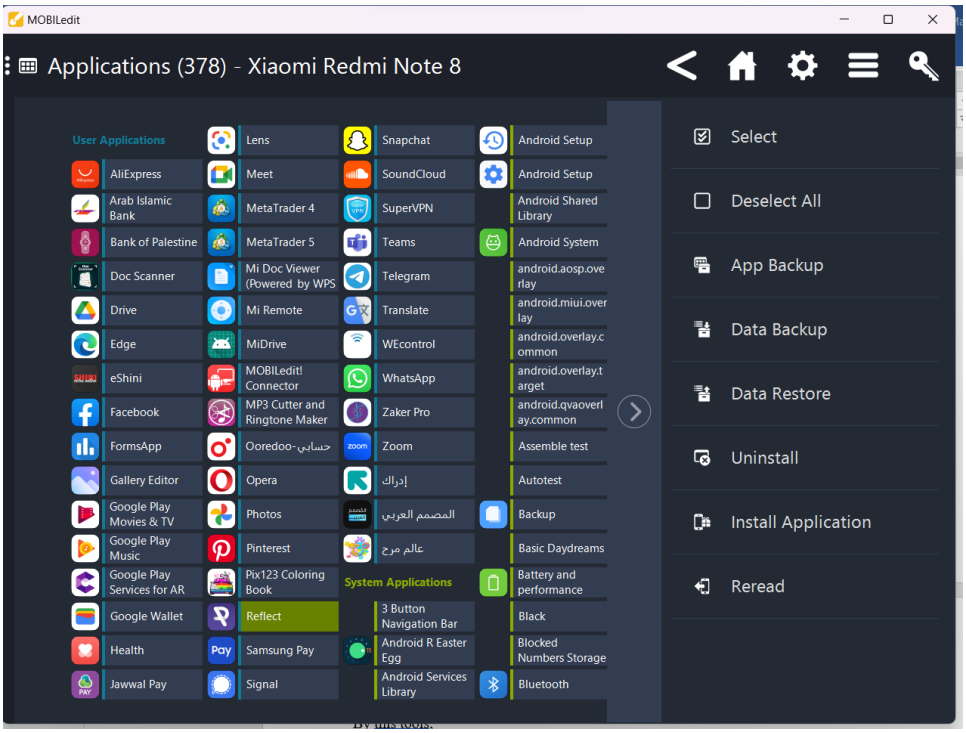


Figure 15 Mobile-edit Enterprise tool

And make a copy acquisition for reflect application by mobileedit forensics tool, as shown in Figures 16, 17, and 18, after resolve the connection problem, and Figure 19 shows the result of the reflect application using mobile edit tools.

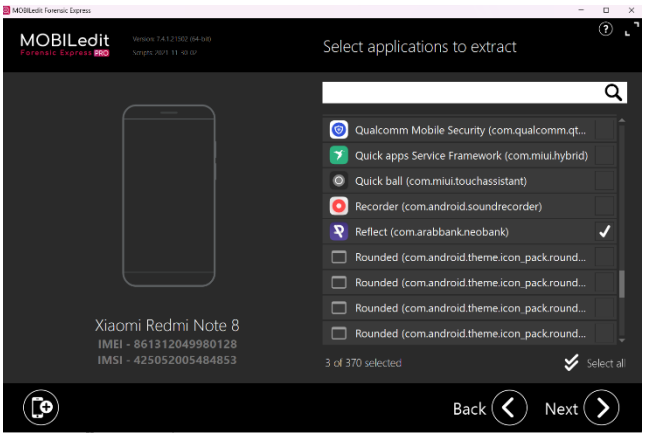


Figure 16 Forensic tool make connection between xiaomi phone

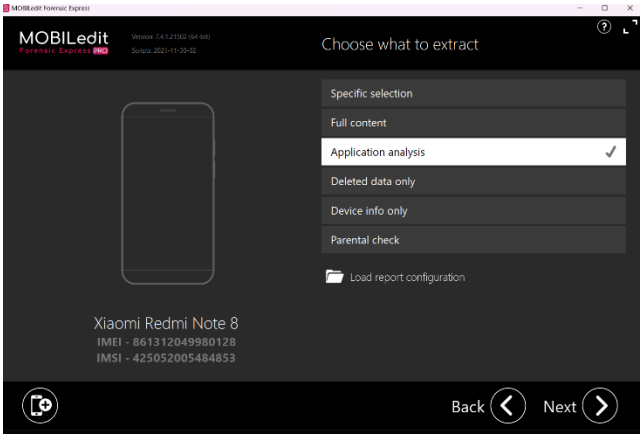


Figure 17 Make acquisition by mobile edit forensics tool

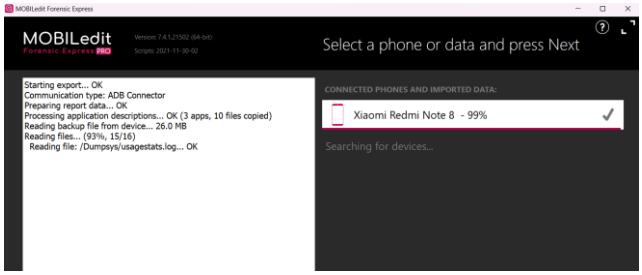


Figure 18 Mobile edit forensics acquisition

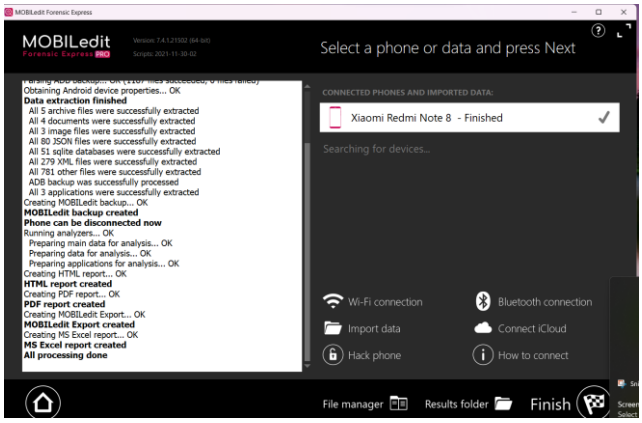


Figure 19 Done acquisition by mobile edit tool for reflect application

With this tool, I found many artifacts, such as verified documentation of reflect applications on Android mobile. This result shows the extent of insecurity in e-wallets even if they are on modern technology Neobanks.

3.3.2.3 Final mobile

By making an acquisition to reflect Neobanks application by final mobile forensics tool, as shown in Figure 20, found Wi-Fi mac address for which the electronic wallet has been logged in, as shown in Figure 21.

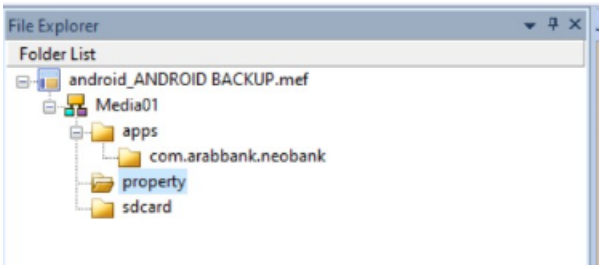


Figure 20 Backup copy for Android with final mobile

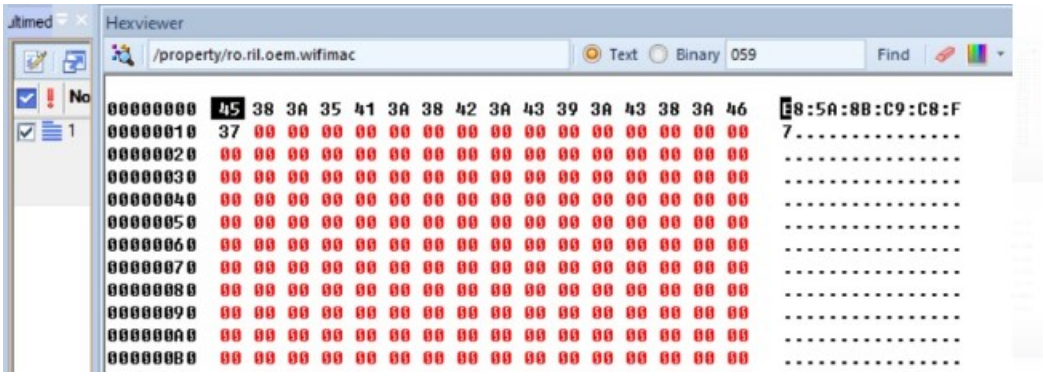


Figure 21 Wi-Fi mac address

Another artifact is many properties as stop snapshot serves as shown in Figure 22

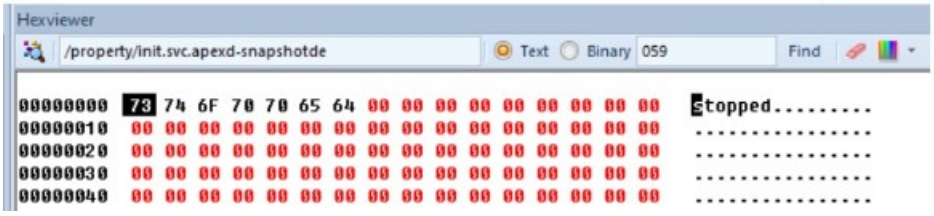


Figure 22 Snapshot serves

3.3.2.4 Android Data Extraction in Briefly

Finally, Table 11 will briefly describe the purpose of each tool that was used, the results that emerged, and the difficulties that I encountered in each experiment.

Table 11 Summary of the process of extracting data from an Android phone.

TOOL NAME	PURPOSE	RESULTS	DIFFICULTIES
MI UNLOCK	allows users to bypass the bootloader restriction and unlock the device for customization and other advanced operations	Mi Note8 phone rooted and Unlocked Bootloader	The waiting period before a phone is approved for jailbreaking is typically seven days.
ANDROID DEBUG BRIDGE (ADB)	Data Acquisition, Device Information Extraction, Application Analysis, File System Examination	extract various types of information from Android devices, including device specifications, system logs, and configuration details.	Compatibility issues with some older devices or the base system.
MOBILEDIT FORENSICS EXPRESS	Data Extraction, Deleted Data Recovery, Analysis and Reporting, Device Imaging, Application Analysis	a verified documentation of reflect application on Android mobile. - personal ID	failed connector installation
MOBILEDIT PHONE MANAGER	phone management and data extraction	application data	
FINAL MOBILE	allows forensic investigators to access and extract a wide range of information, such as call logs, text messages, multimedia files, application data, and other types of digital evidence stored on the device	WiFi mac address, properties as stop snapshot serves, time of logging in and out	compatibility with certain device models or operating systems, technical issues or software errors during the data extraction process.

3.3.3 Extract IOS data:

Reflect application on IOS mobile, make acquisition analysis by many tools as:

3.3.3.1 MOBILedit forensics express

After make an acquisition for reflect application on IOS mobile device by mobile edit forensics tool, all information about my iPhone, on the pdf report viewed in pdf report as shown in Figure 23 and sorted by filter as the database table

Figure 23 IOS mobile information- reflect case

Result for artifacts of reflect app: the base artifact is a picture of documents we verified the account of reflect with it as personal ID and housing proof document as shown in Figures 24 and 25. It helps the cyber analyzer know who the owner of the original application is since the application cannot be activated without the official documents of the person.

Images (3)

1 nationaId-back-page.png

Filename	nationaId-back-page.png
Path	phone/applications0/com.arabbank.neobank/backup/Documents/nationaId-back-page.png
Size	925 KB
Created	2023-03-05 11:25:31 (UTC+2)
Modified	2023-03-20 12:22:24 (UTC+2)
Accessed	2023-03-20 12:22:24 (UTC+2)
Width	966 px
Height	566 px
Format	png

2 nationaId-front-page.png

Filename	nationaId-front-page.png
Path	phone/applications0/com.arabbank.neobank/backup/Documents/nationaId-front-page.png
Size	1.24 MB
Created	2023-03-05 11:25:14 (UTC+2)
Modified	2023-03-20 12:22:11 (UTC+2)
Accessed	2023-03-20 12:22:11 (UTC+2)
Width	966 px
Height	566 px
Format	png

Figure 24 Personal ID uploaded to activate Reflect account

3 proof-of-work-document-page.png

Filename	proof-of-work-document-page.png
Path	phone/applications0/com.arabbank.neobank/backup/Documents/proof-of-work-document-page.png
Size	1.45 MB
Created	2023-03-20 12:27:36 (UTC+2)
Modified	2023-03-20 12:27:36 (UTC+2)
Accessed	2023-03-20 12:27:36 (UTC+2)
Width	966 px
Height	1110 px
Format	png

Figure 25 Housing proof document uploaded to document Reflect account

3.3.3.2 BelkaSoft

By this tool many problems were encountered during the installation of the app because the tool is not free, and we used another copy of the tool; with the use of another version of the tool, an error appeared after activating, and the tool did not respond as shown in Figure 26.

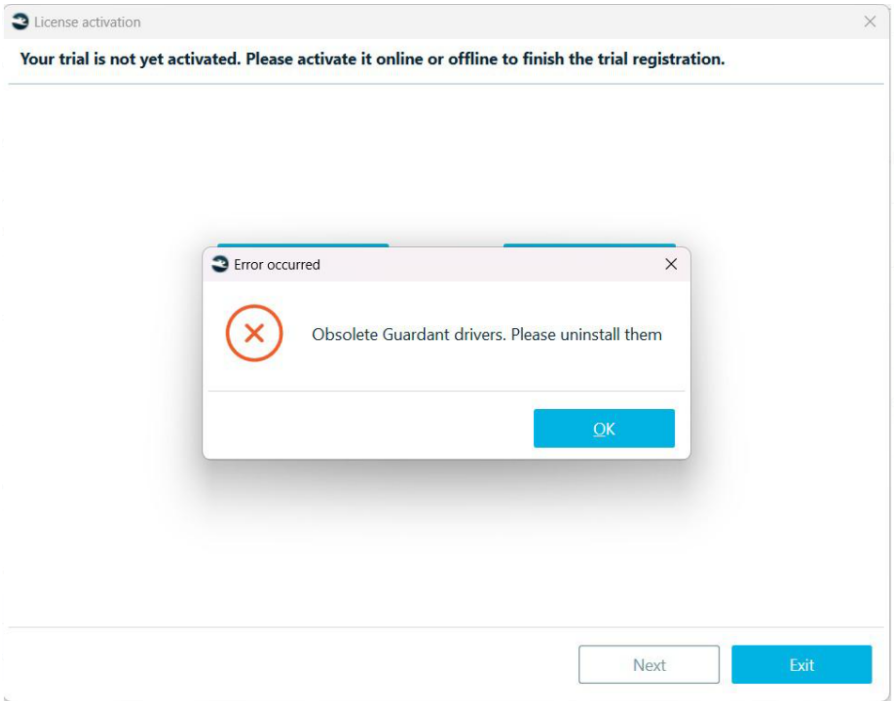


Figure 26 Error of belkasoft installlation

3.3.3.3 iBackup viewer

With make backup by iTunes application, view the backup by iBackup viewer tool as shown in Figure 27, and choose view as the row file to show data and artifacts.

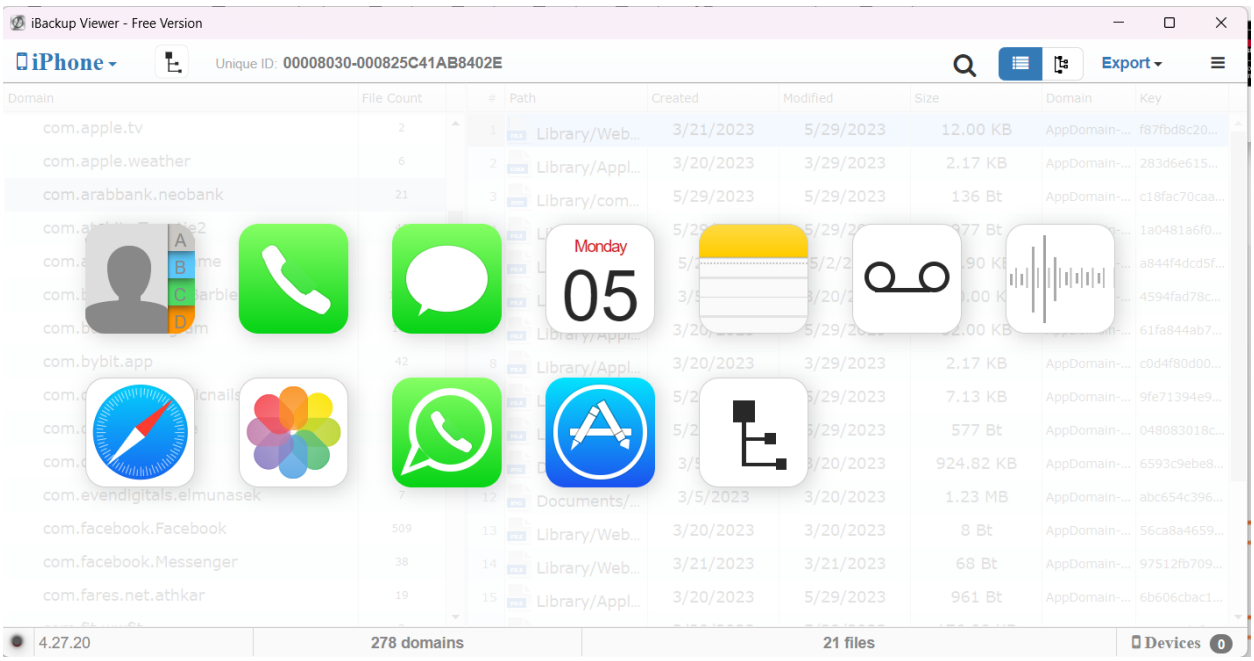


Figure 27 iBackup viewer front

For Reflect Noebank application, show on a folder (com.arabbank.neobank) as shown in Figure 28

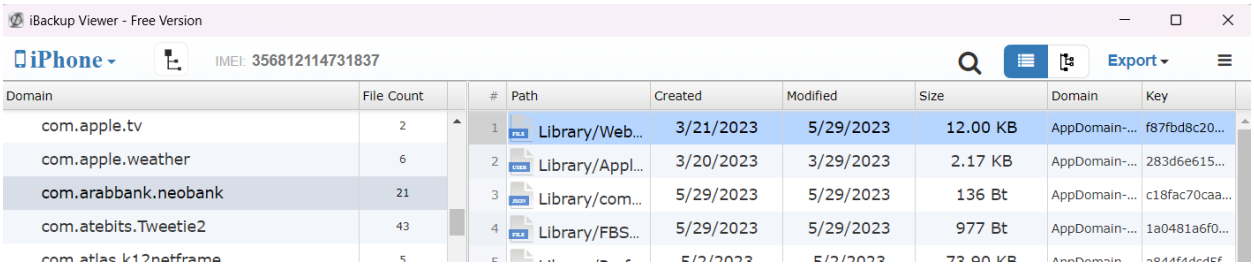


Figure 28 Reflect neobank folder in iphone backup

In folder – com.mobile-messaging.user as shown in Figure 29, we found many artifacts such as (the email of user, username, and mobile phone number, as shown in Figure 30

Email: marytareq1@gmail.com, username: marytareq, phone number: 970592252056

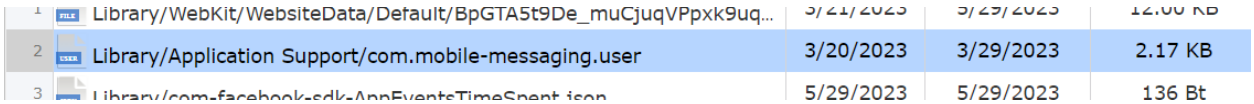


Figure 29 Artifacts file director

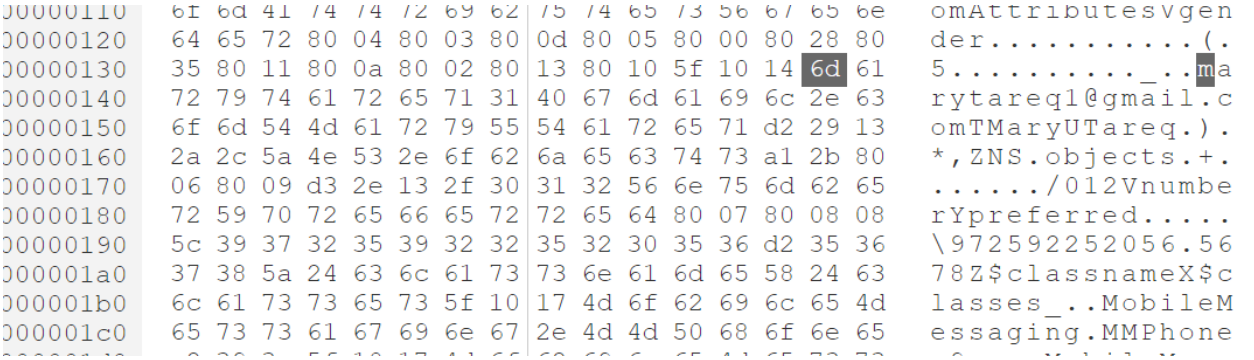


Figure 30 Email address, user name and phone number artifacts

And wallet activated date and time: 20-03-2023, 8:23, and the list of wallet open date and time is shown in Figure 31 This confirms that the electronic wallet has sufficient abundance to obtain its information and all payment movements that take place through it, which reflects the impression that the modern wallet is unsafe, and this is what is proven by the fourth hypothesis that the e-wallet is not integrity.

```
22 80 21 80 24 5f 10 11 69 73 57 61 6c 6c 65 74   ".!.$_..isWallet
41 63 74 69 76 61 74 65 64 5f 10 17 77 61 6c 6c   Activated_..wall
65 74 41 63 74 69 76 61 74 65 64 44 61 74 65 54   etActivatedDateT
69 6d 65 54 5f 5f 69 64 5f 10 13 77 61 6c 6c 65   imeT__id_..walle
74 4f 70 65 6e 64 44 61 74 65 54 69 6d 65 5e 69   tOpendDateTime^i
73 57 61 6c 6c 65 74 4f 70 65 6e 65 64 09 5f 10   sWalletOpened._.
14 32 30 32 33 2d 30 33 2d 32 30 54 31 31 3a 31   .2023-03-20T11:1
38 3a 32 33 5a 5f 10 24 38 34 33 62 31 34 66 34   8:23Z_.$843b14f4
2d 33 63 30 63 2d 34 30 36 39 2d 62 63 34 30 2d   -3c0c-4069-bc40-
```

Figure 31 Activated and open wallet date- artifacts

On folder /group.com.arabbank.NewBank.plist, as shown in Figure 32

5	Library/Preferences/group.com.arabbank.NewBank.plist	5/2/2023	5/2/2023	73.90 KB
6	Library/LogDatabase.sqlite	3/5/2023	3/20/2023	100.00 KB

Figure 32 File

found a list of Contacts have reflect application on his phone, as shown in Figure 33

```
000002e0 | 6e 61 6d 65 22 3a 22 20 48 61 73 73 61 6e 20 53      name":" Hassan S
000002f0 | 68 61 74 61 74 22 2c 22 6d 6f 62 69 6c 65 22 3a      hatat","mobile":
00000300 | 22 39 37 32 35 39 37 36 35 35 37 34 32 22 2c 22      "972597655742","
00000310 | 74 79 70 65 22 3a 22 4e 4f 4e 45 22 7d 2c 7b 22      type":"NONE"},{"
00000320 | 6e 61 6d 65 22 3a 22 20 33 61 73 65 66 22 2c 22      name":" 3asef","
00000330 | 6d 6f 62 69 6c 65 22 3a 22 30 35 39 39 34 37 36      mobile":"0599476
00000340 | 37 33 35 22 2c 22 74 79 70 65 22 3a 22 4e 4f 4e      735","type":"NON
00000350 | 45 22 7d 2c 7b 22 6e 61 6d 65 22 3a 22 20 33 6c      E"},{"name":" 3l
00000360 | 6f 6f 73 68 22 2c 22 6d 6f 62 69 6c 65 22 3a 22      oosh","mobile":"
00000370 | 39 37 30 35 39 38 36 39 31 35 35 36 22 2c 22 74      970598691556","t
00000380 | 79 70 65 22 3a 22 4e 4f 4e 45 22 7d 2c 7b 22 6e      ype":"NONE"},{"n
```

Figure 33 Contacts list from the application

Time of login and out from the application as shown in Figure 34

```
�
�Y  ·····U�5··ı���·@1ECD2987-8E9F-4AB1-889F-AB7DED8D18B62023-03-20 12:24:29:6000  Instan
.LogRequest.getLogData  Message: Method Start

�·�X    ·····U�S··ı���·61ECD2987-8E9F-4AB1-889F-AB7DED8D18B62023-03-20 12:24:29:5990  I
ZID.MetaDataUtilities.addSessionToMetaData  Message: Method End

�·�W    ·····U�W··ı���·"1ECD2987-8E9F-4AB1-889F-AB7DED8D18B62023-03-20 12:24:29:5970  I
ZID.MetaDataUtilities.addSessionToMetaData  Message: Method Start

�·�V    ·····U�S··ı����·1ECD2987-8E9F-4AB1-889F-AB7DED8D18B62023-03-20 12:24:29:5950  I
ZID.MetaDataUtilities.getAppMetaDataConfig  Message: Method End

�·�U    ·····U�W··ı����·1ECD2987-8E9F-4AB1-889F-AB7DED8D18B62023-03-20 12:24:29:5940  I
ZID.MetaDataUtilities.getAppMetaDataConfig  Message: Method Start
```

Figure 34 Login and logout history.

The found documents of the activated application are shown in Figure 35 – nationID back and front page photo.

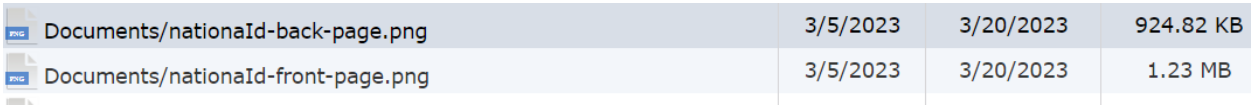


Figure 35 Artifacts document activated neobank application

By this tool, Despite the high level of security for modern iPhone devices and their good reputation in level of protection, however, after the acquisition of private data in the e-wallet application, it is easy to access all the wallet data and movements made in all the details. This is what we said earlier, which underscores the invalidity of the first hypothesis of this research. All data can be recovered on iPhone after downloading and activating the wallet app.

3.3.3.4 FINAL MOBILE

After making a payment via the reflect neobank app, as shown in Figure 36, delete the app from the mobile device and then make an acquisition for IOS mobile after delete reflect neobank application; shows the emergence of several valuable artifacts. After analyzing the acquisition results via the Final Mobile tool and searching by word for "Reflect", several results emerged, as shown in Figure 37,

Figure 37 reflect payment movement

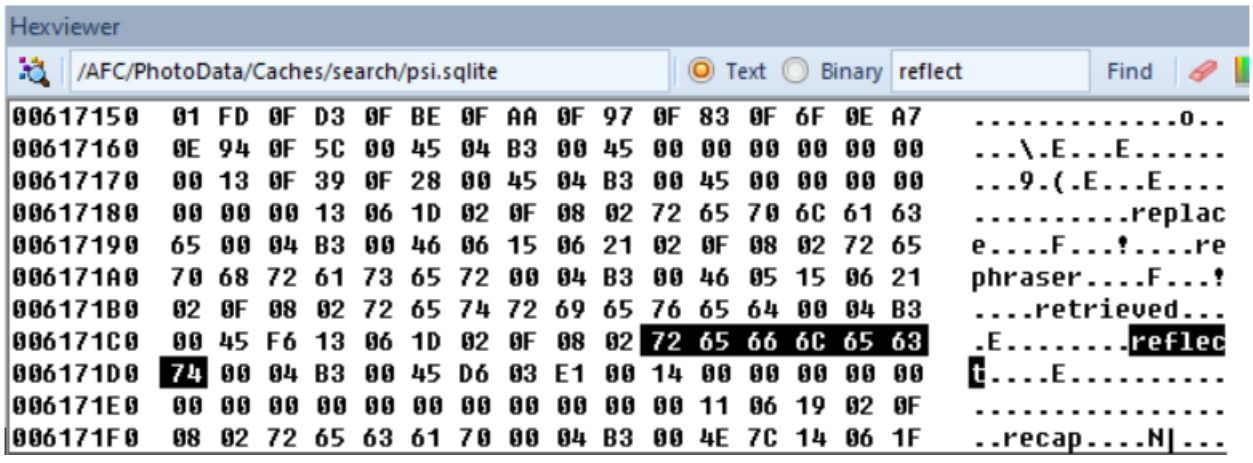


Figure 36 Search by word on hexviewer of IOS with deleted reflect neobank application.

After searching, see the payment movement I made in Figure 36, this is shown in Figure 38, Beneficiary Name, and amount sent: 5nis as shown in Figure 39.

```
006D7C50  0F 06 15 02 0F 08 02 61 73 68 00 04 B3 00 06 02   .......ash......
006D7C60  15 06 21 02 0F 08 02 61 73 63 65 6E 64 69 6E 67   ..!....ascending
006D7C70  00 04 B3 00 06 5B 10 06 17 02 0F 08 02 61 73 61   .....[.......asa
006D7C80  64 00 04 B3 00 08 AD 16 06 23 02 0F 08 02 61 73   d........#....as
006D7C90  34 2C 32 30 31 2C 31 30 00 04 B3 00 14 64 11 06   4,201,10.....d..
```

Figure 38 Beneficiary Name of Payment Movement

And total balance credit after payment movement, as shown in Figure 39

```
00735600  35 6E 69 73 00 04 B3 00 17 5D 0F 06 15 02 0F 08   5nis.....]......
00735610  02 31 35 6D 00 04 B3 00 22 31 0F 06 15 02 0F 08   .15m....."1......
00735620  02 31 35 68 00 04 B3 00 10 0F 13 06 1D 02 0F 08   .15h............
00735630  02 31 35 39 39 2E 32 30 00 04 B3 00 05 03 14 06   .1599.20........
00735640  1F 02 0F 08 02 31 35 39 36 34 2E 35 38 00 04 B3   .....15964.58...
00735650  00 3C 53 13 06 1D 02 0F 08 02 31 35 39 35 2E 32   .<S.......1595.2
00735660  30 00 04 B3 00 05 A0 13 06 1D 02 0F 08 02 31 35   0.............15
00735670  39 34 2E 30 30 00 04 B3 00 36 F7 10 06 17 02 0F   94.00....6......
00798A00  02 0F 08 02 32 31 2C 32 30 31 00 04 B3 00 35 AB   ....21,201....5.
00798A10  0D 06 13 02 0F 08 01 32 31 00 04 B3 00 52 11 06   .......21....R..
00798A20  19 02 0F 08 02 32 30 6E 69 73 00 04 B3 00 17 66   .....20nis.....f
00798A30  0F 06 15 02 0F 08 02 32 30 6D 00 04 B3 00 24 81   .......20m....$.
00798A40  13 06 1D 02 0F 08 02 32 30 39 39 2E 31 35 00 04   .......2099.15..
006D7C50  0F 06 15 02 0F 08 02 61 73 68 00 04 B3 00 06 02   .......ash......
```

Figure 39 Total balance credit after payment movement

These results answer the first research question: since all movements made through the Neobank app can be obtained even if the app is deleted from the mobile device, this is one of the most important solutions to cybersecurity challenges and money transfer problems, and embezzlement, as all transfers made through electronic payment can be obtained via the Reflect app.

3.3.3.5 IOS Data Extraction in Briefly

Table 12 Summary of the process of extracting data from an IOS device

TOOL NAME	PURPOSE	RESULTS	DIFFICULTIES
MOBILEDIT FORENSICS EXPRESS	extracting and analyzing data from mobile devices enables the examination of deleted or hidden data	documents we verified the account of reflect as personal ID and housing proof document	Use the trial version
BELKASOFT	collect and examine digital evidence and recover deleted or hidden data	Several attempts to download the tool failed	the tool is not free, and it is very difficult to use the trial version
IBACKUP VIEWER	analyze data from iPhone backups and extract app data from iOS devices	- The email of user verified the reflect account - username - and mobile phone number - list of wallet open date and time - all payment movements that take place through it. - list of Contacts has reflect application on his phone. - documents of activated application	
FINAL MOBILE	access and extract a wide range of information, examination of deleted or hidden data,	This results in deleted reflect application: - payment movement I made It - Beneficiary Name and amount sent - total balance credit after payment movement	

3.4 Reverse Engineering

The reverse-engineering procedure is unique to the object being reverse-engineered. Regardless of the situation, all reverse-engineering efforts follow the same three steps. Here are a few examples: Data extraction that the thing being reverse-engineered is evaluated, design information collected, and that information reviewed to see how the components fit together. This may entail acquiring source code and related design documentation for analysis in software reverse engineering. It might also entail the use of tools like a disassembler to break the software down into its component elements.

Building a model or modeling that the gathered data is abstracted into a conceptual model, with each component describing its role in the broader framework. The goal of this stage is to abstract particular information from the original into a general model that may be used to guide the creation of new items or systems. This might be a data flow diagram or a structure chart in software reverse engineering.

Review. This entails looking at the model and putting it through its paces in different settings to ensure that it is a true representation and realistic abstraction of the original object or system. This might take the shape of software testing in the software engineering world. The model may then be used to reengineer the original thing once it has been thoroughly tested.

Reverse engineering, to put it simply, is the process of extracting source code from an executable. Reverse engineering an Android app is done to figure out how the app works, where data is stored, what security methods are in place, and so on.

Figure 40 shows the basic understanding of the Android application source.

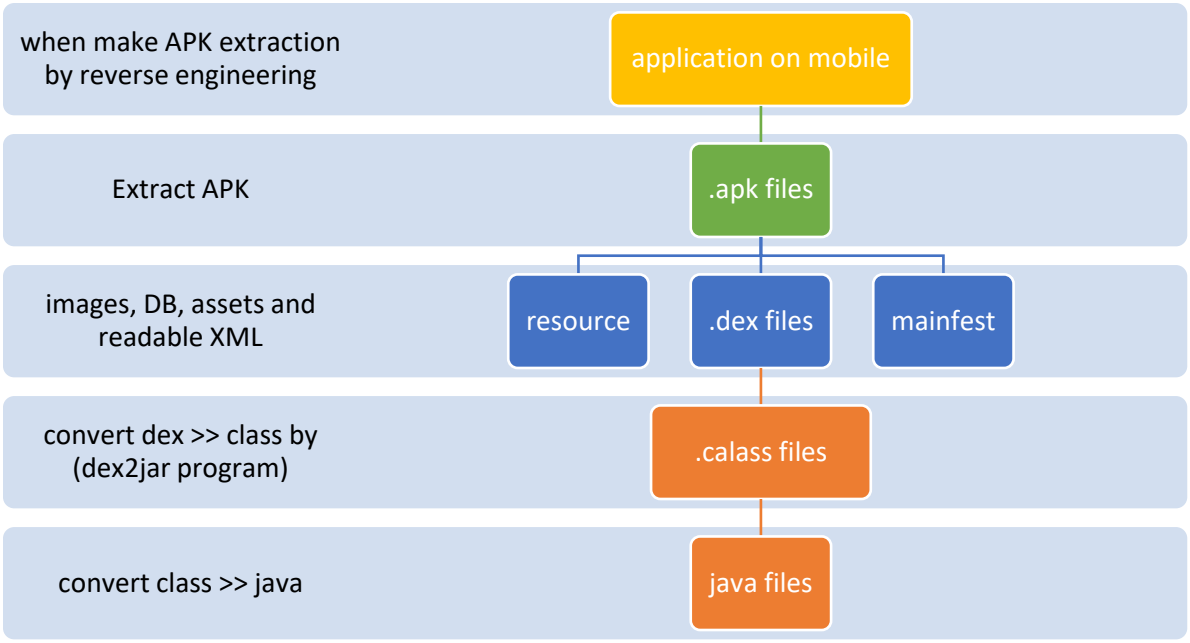


Figure 40 Basic understanding of the Android application source

In reverse engineering for Jawwalpay wallet, on mobile Redmi Note 8, this mobile uses Android operating system, so we make the following steps: ((this step gives the same result in rooted and nonrooted mobile))

NOTE: reverse engineering is not available for IOS operating system.

1- Extracting an APK file from the rooted mobile by platform tools, as shown in Figure 41 by code: *Adb.exe shell pm list packages* and, take name of the application packages, and focus of a required application as shown in Figure 42

```
H:\platform-tools>adb.exe shell pm list packages
```

Figure 41 Code of take package name

```
package:com.android.providers.media.module
package:ps.jawwalPay.customer
package:com.android.emergency
```

Figure 42 JawwalPay application package name

Finally by following command *adb.exe shell pm pathps.jawwalPay.customer*, find the entire pathname of the APK file for the requested package as shown in Figure 43:

```
H:\platform-tools>adb.exe shell pm path ps.jawwalPay.customer
package:/data/app/~~mxiXUHmoLn1WScO_mvAmBQ==/ps.jawwalPay.customer-NvwFjSgpDx0knmh1JGNA-g==/base.apk
```

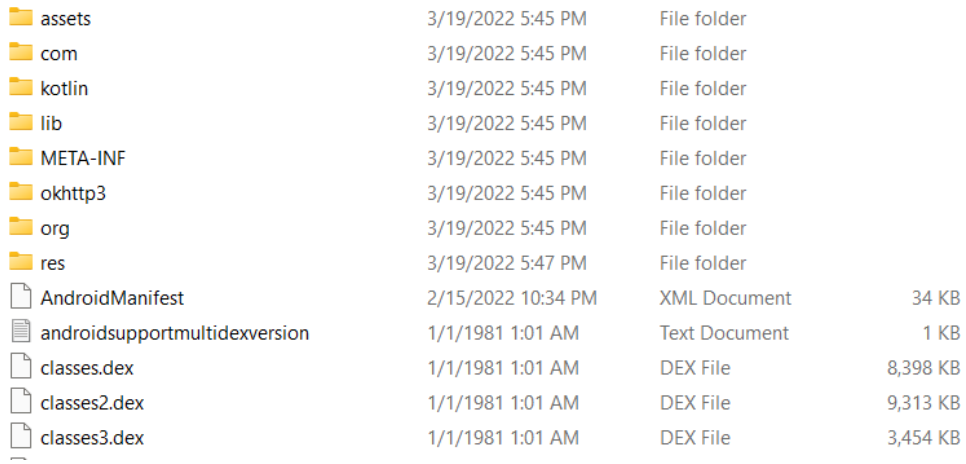
Figure 43 Code of extract the pathname of APK file and result of code

2- Using the *adb.exe pull* command, transfer the APK file from the Android smartphone to the forensic workstation, as shown in Figure 44.

```
H:\platform-tools>adb.exe pull /data/app/~~mxiXUHmoLn1WScO_mvAmBQ==/ps.jawwalPay.customer-NvwFjSg
pDx0knmh1JGNA-g==/base.apk
/data/app/~~mxiXUHmoLn1WScO_mvAmBQ==/ps.jawwalPay.customer...le pulled, 0 skipped. 32.6 MB/s (354
24861 bytes in 1.036s)
```

Figure 44 Transfer APK file from mobile to forensic workstation

3- Rename the APK extension to ZIP to see the contents of the file, base.apk to base.zip, and extract the file using archive application in Figure 45. The screenshot shows the files extracted from the original APK file YT6



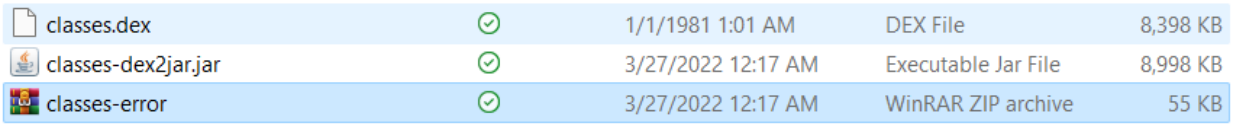
assets	3/19/2022 5:45 PM	File folder	
com	3/19/2022 5:45 PM	File folder	
kotlin	3/19/2022 5:45 PM	File folder	
lib	3/19/2022 5:45 PM	File folder	
META-INF	3/19/2022 5:45 PM	File folder	
okhttp3	3/19/2022 5:45 PM	File folder	
org	3/19/2022 5:45 PM	File folder	
res	3/19/2022 5:47 PM	File folder	
AndroidManifest	2/15/2022 10:34 PM	XML Document	34 KB
androidsupportmultidexversion	1/1/1981 1:01 AM	Text Document	1 KB
classes.dex	1/1/1981 1:01 AM	DEX File	8,398 KB
classes2.dex	1/1/1981 1:01 AM	DEX File	9,313 KB
classes3.dex	1/1/1981 1:01 AM	DEX File	3,454 KB

Figure 45 The file extracted from original file (ps.jawwalPay.customer)

4- after install dex2jar tool [42] drag the file classes. dex on folder of tools, and by CMD code, write *d2j-dex2jar classes. dex,* as shown in Figure 46; after that, we found a new file, classes.jar, in the tools folder, but with file classes-error.zip, as shown in Figure 47!

```
C:\Users\red-r\OneDrive\Documents\dex2jar-2.0>d2j-dex2jar classes.dex
dex2jar classes.dex -> .\classes-dex2jar.jar
Detail Error Information in File .\classes-error.zip
Please report this file to http://code.google.com/p/dex2jar/issues/entry if possible.
```

Figure 46 Code of convert dex to jar file and its results.,



classes.dex	✓	1/1/1981 1:01 AM	DEX File	8,398 KB
classes-dex2jar.jar	✓	3/27/2022 12:17 AM	Executable Jar File	8,998 KB
classes-error	✓	3/27/2022 12:17 AM	WinRAR ZIP archive	55 KB

Figure 47 The classes file

5- Make all of the steps to convert the three classes files we found in the base folder, classes2.dex, and classes3.dex

6- Finally, to view the content of classes jar file, can use JD-GUI tools [43] and import files to view content by the tool, as shown in Figure 48.

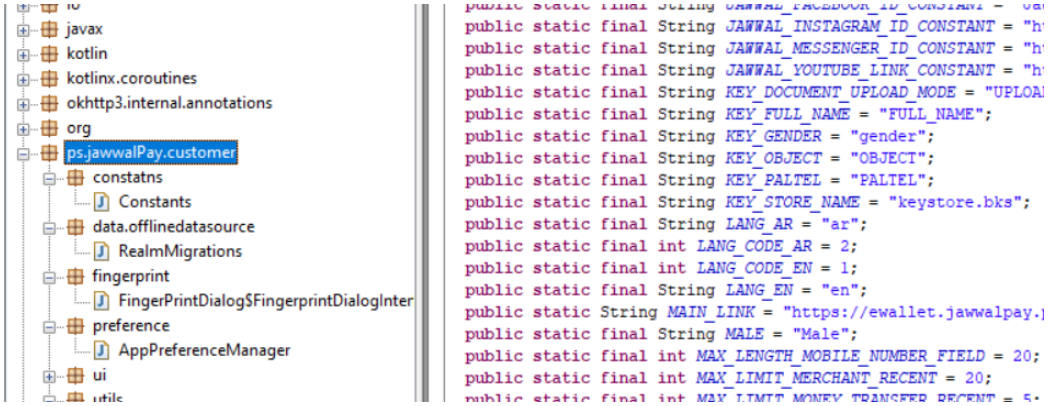


Figure 48 The content of classes.jar file by JD-GUI tools

After extensive investigation, we uncovered the open-source code of Jawwalpay wallet, as depicted in *Figure 49*. The code's susceptibility to modifications underscores one of the primary reasons highlighting the inherent weaknesses of the mobile wallet application. The need to discontinue its services within the community became imperative, especially after encountering evasion from the technical support team during our visit to the company's exhibition to activate the application. This incident served as compelling evidence, indicating the illicit nature of the wallet and its significant operational challenges [45]. The structure of the wallet application comprises multiple libraries integrated into a single code, lacking the specific security measures typically associated with electronic wallets, thereby rendering the application more susceptible to breaches and privacy violations. Although the application has been replaced by the newer banking application Reflect, as previously examined in this research, it remains active for users who had utilized it previously. This perpetuates the users' exposure to the risks associated with unauthorized money transfers, potentially leading to theft and illicit financial activities. Our reverse engineering efforts throughout this research have validated these concerns.

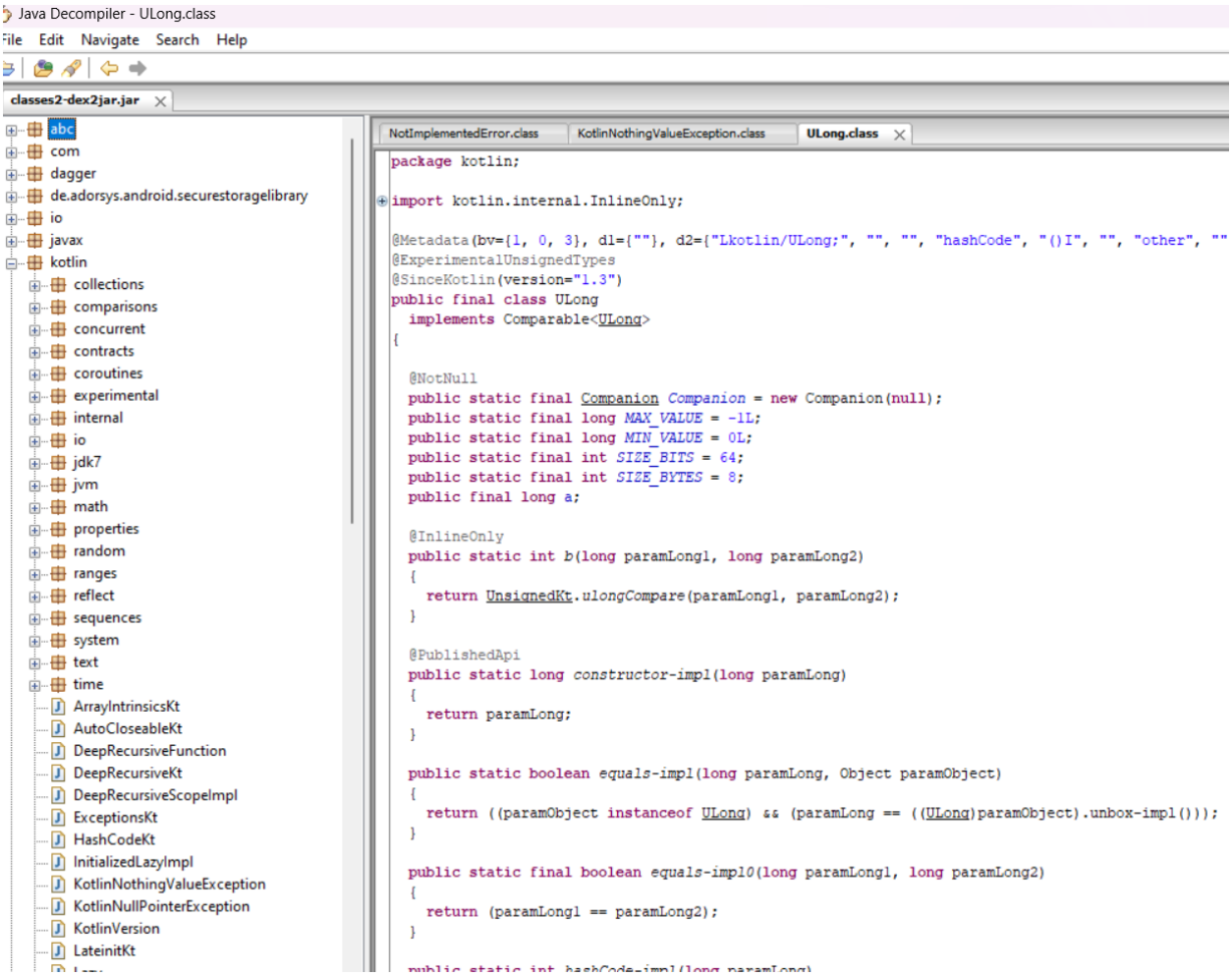


Figure 49 Jawwal pay wallet- open-source code

Chapter 4

Suggested model

MOBILE APPS ENGINEERING FOR E-WALLET DESIGN, SECURITY and TESTING (MAEE)

4.1 Suggested mobile application model MAEE ((MOBILE APPS ENGINEERING FOR E-WALLET DESIGN, SECURITY and TESTING)) MAEE-dst

The MAEE model is a useful tool for academics and developers of mobile applications who want to raise the overall standard and security of e-wallet applications, as shown in Figure 50.

In order to safeguard user information and stop illegal access, MAEE-dst includes cutting-edge authentication procedures, encryption techniques, and secure data storage technologies. In order to find and fix such vulnerabilities, the testing process also involves thorough functional, performance, and security testing that adheres to industry best practices.

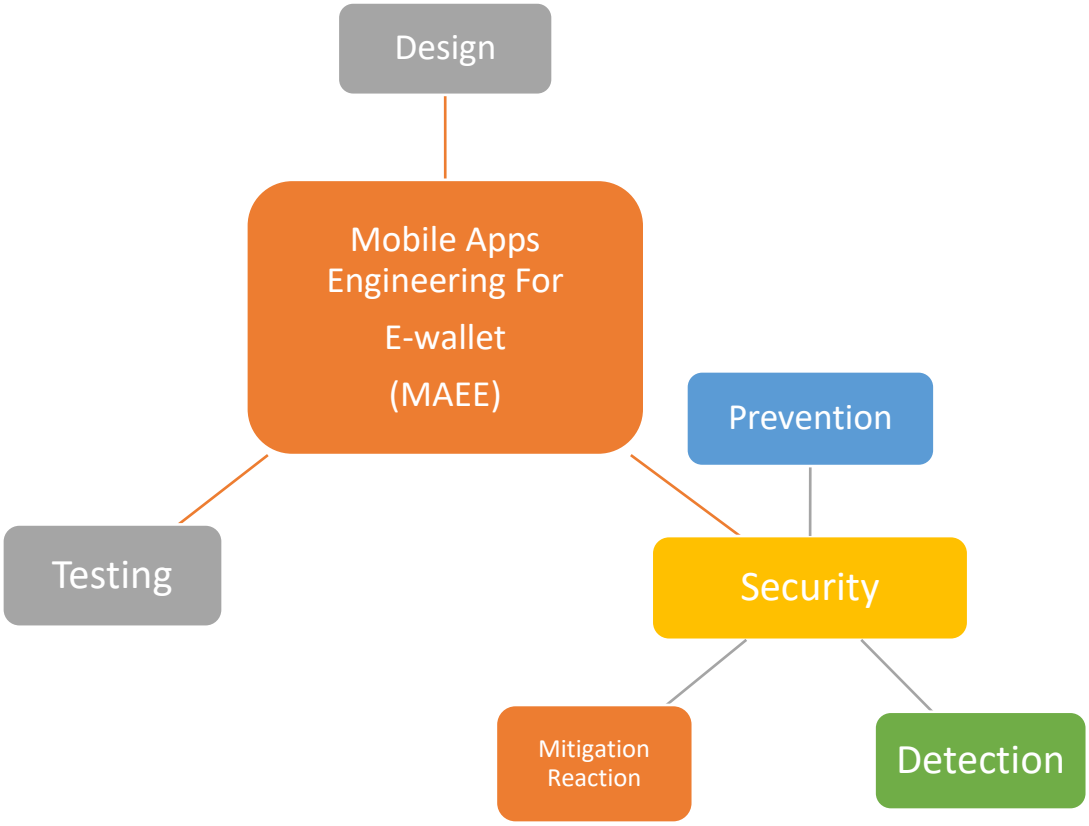


Figure 50 Suggested Mobile Application Model (MAEE-dst)

4.1.1 Design

The creation of a user-friendly user interface and the integration of crucial functionality, such as payment processing, transaction history, and account management, are the main goals of the design phase. The approach places a focus on agile development techniques, guaranteeing iterative improvements and quick distribution of updates, as shown in Figure 51, which displays the application permission workflow.

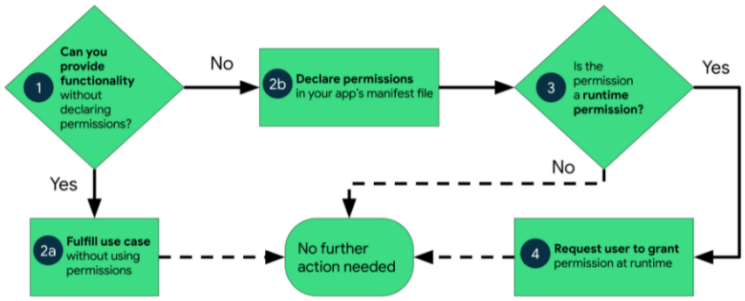


Figure 51 Application permission work flow [11]

Android has a permission structure in place to protect its vulnerable components, but many users are unaware of the permissions that are being requested or may not even know what they are for. Most users don't refrain from using unsecured public Wi-Fi networks, and more than half of those who took part in the security study had never thought about the security risk that accessing an unsecured Wi-Fi network represents. Droid was designed to enable apps to become more dynamic and autonomous in their operation. The permissions were established to assist apps in retrieving certain information from a user's device and then using that information to assist the user in carrying out transactions and services in the background to benefit the user and update their account.

Excessive usage of mobile application permissions has resulted in severe information and data security breaches for many users, and it continues to present difficulties for mobile phone users. Android permissions may be used for a variety of activities, including spying, stealing information and data, altering data, monitoring users, and even collecting personal information and passwords.[44] Android developers can exploit application permissions to follow users, wipe their data, steal personal and private information such as passwords and emails, steal money from users, and drain money from users through unnecessary service fees. They can also listen in on and view the user through the gadget, as well as monitor the user's whereabouts.

There are four categories of permissions:

1- Normal permissions are required when a program wants to access data or resources outside of its sandbox, but they pose no danger to user privacy or the functionality of other apps[45].
2- Dangerous permissions when an app needs data or resources that include the user's private information or might potentially damage the user's stored data or the operation of other applications.
3- Signed permission is a permit given by the system to an application that shares the same certificate category as the one that requested it. If the certificate categories match, the system grants authorization automatically.
4- Signature or system permission: the system only grants this permission to programs that are part of the Android system image or have the same certificate category as the declarer. Is permission is only used in exceptional circumstances, such as when many vendors have applications that must explicitly share resources while being constructed jointly.

By leaving location services on all the time and publishing their location on social media, Users expose themselves to attackers who may seek to damage them physically or benefit from their presence in a certain spot, allowing them to participate in burglary, robbery, or theft.

In order to cause damage, attackers frequently aim to exploit either technical flaws in operating systems or a person's inexperience or generosity in completing tasks for them. Malicious software may infiltrate mobile devices in a variety of ways presented in the following Figure 52:

Figure 52 Malicious Software ways

4.1.2 Security

Prevention is the earliest step of the security life cycle, and it is also the least invasive, minimizing resource waste such as mobile device battery use. Several protection mechanisms have been included in mobile devices as a precautionary step to reduce the quantity of potentially destructive malware programs that enter the device or that exploit established attack routes. The following are the most often utilized preventative methods:

1- installation of malware to prevent attacks
2- monitor application and mobile device behavior, such as applications sending frequent data to remote sites without user permission
3- reduce potential threats such as malware accessing personal data.

The evolution of mobile devices as their complexity increases allows users to perform more complex tasks and creates significant challenges for application developers to create secure and reliable applications. Modern mobile devices are capable of performing tasks that were never thought possible.

It does not impose any restrictions on the movement of the carrier or the host. By facilitating the movement of people, the characteristics of these devices are limited in dimensions and weight, as they can be easily lost, they can connect to other devices without any awareness of the user, and they can connect to unsecured networks without the consent of the user or trusted authority. In addition to all of the functions already stated, the connection often consists of 3G/4G, Wi-Fi, Bluetooth, NFC, airdrop, and GPS capabilities.

One of the most important risks that users fall into is the user's belief that all applications in the official application stores are safe, and this is a misconception, and their lack of awareness of the extent to which their devices and the security of their information are at risk due to the behaviors with which they interact and authorize such as credit card details or electronic wallets details that They use it, this confirms that users have a very poor awareness of privacy and security. Also, the user's lack of interest in protection permissions when downloading applications on mobile devices, and this, if anything, indicates the user's lack of awareness of the extent of the security risk that the user is exposed to when accessing an unsafe Wi-Fi network, also running the location service from the permissions that display the user at risk, and permission to allow access to private photos in the gallery.

Recent reports show that most of the cyber-attacks on mobile devices are malware, key logging, credential and phishing attacks, and software permissions.

The life cycle of Security for Mobile Devices is shown in Figure 53

1- Prevention, which is preventing danger before it occurs
2- Monitoring and detection, which is the continuous analysis to follow up on the behavior of the device
3- Reacting or mitigating the precautionary measure to protect against danger, even if that action causes damage to the device

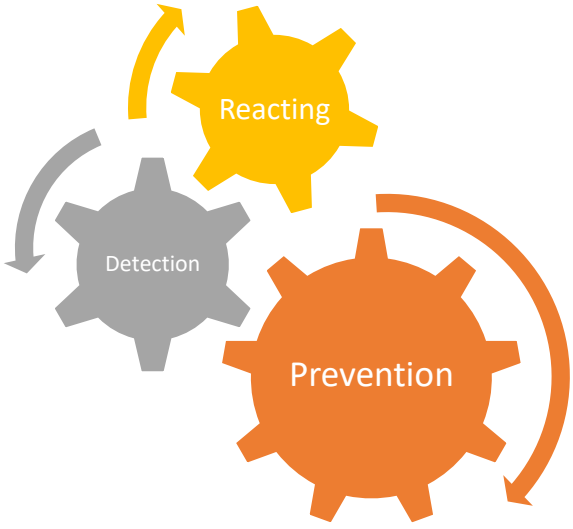


Figure 53 Life cycle of security for mobile devices

The following are the *preventative* strategies most frequently employed to system security from being compromised:

1- *Sandboxing* is a cybersecurity approach where code is executed on a network that resembles end-user operating systems, watched, observed, and analyzed. To examine untried or untrusted programs and prevent threats from accessing the network, sandboxing is frequently utilized.
2- *Policies Matching:* A detailed analysis to match all security policies before distributing the application. This procedure is available in the App Store application for IOS Mobile devices, and the same procedure is available in Windows Phones, although it is not available in Google Play on Android mobile devices. This is what makes Android mobile devices more vulnerable to threats.
3- *Code and database* Enforce the behavior of app stores by linking them to unique signatures database of malware so that potential threats to the system can be identified
4- *Fragmentation* Separation of the personal space of the device from the workspace, with limited permissions available in the personal space of the device user
5- *Permission system* Phone companies should explicitly clarify system features or the capabilities of devices that (the user may) need access to measure risk when granting access to sensitive features, such as camera access or SD storage.

Monitoring enables detection and corroboration of malicious activity within the system during runtime as the logs are periodically sent to a trusted supervising server to delegate the heavier, more resource-intensive analysis burden out of the mobile device, albeit some minor analysis can still be performed on-site, and help to detect unnecessary use of mobile device resources such as cameras or microphones.

What was presented in the previous sections are some of the preventive techniques from the occurrence of any attack and *mitigate* the possibility of a threat, and the reaction in the event that the device is exposed to danger or attack, what will be done to reduce the damage and repair it, as shown in Figure 54

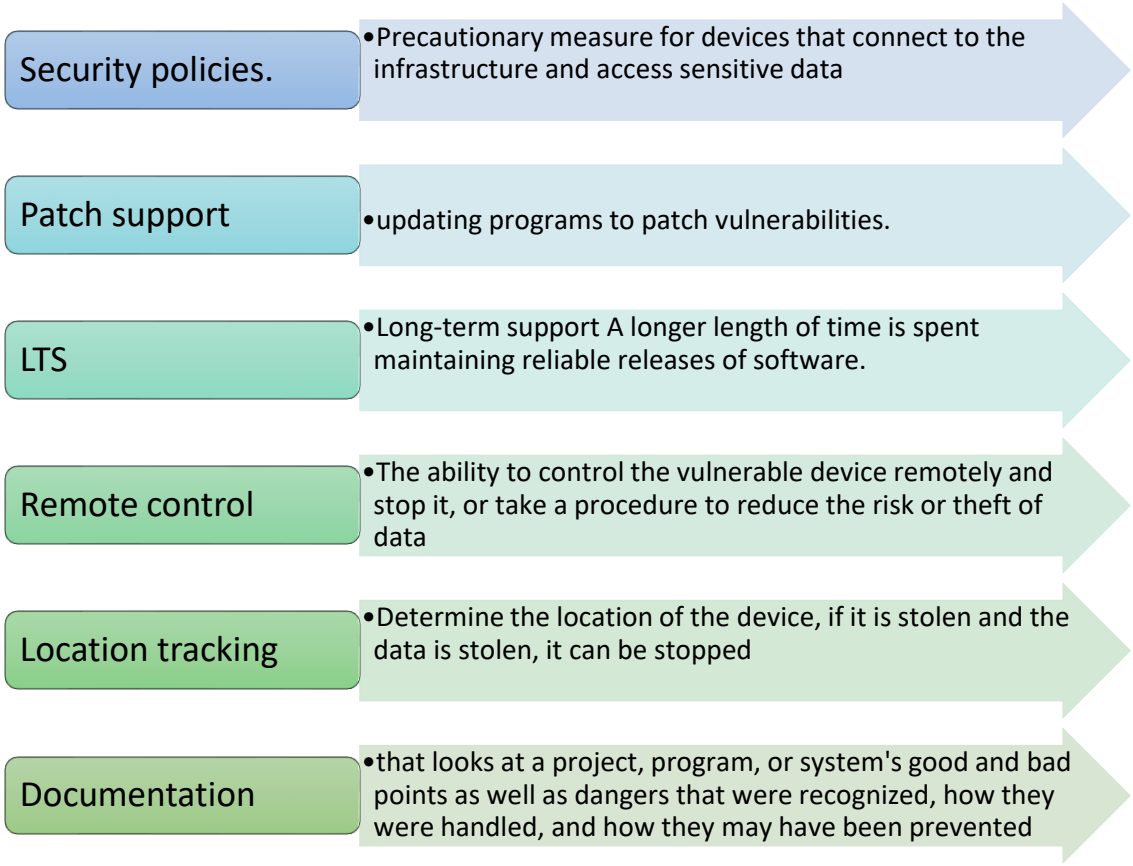


Figure 54 Mitigation Reaction techniques

Talking about security may take a long time and needs continuous follow-up in order to keep pace with threats, their updates, and their evolution with time, so it is necessary to tighten security and preventive techniques in more ways than the previously mentioned methods by encrypting applications with encryption algorithms, and protection environments as they isolate applications from each other and from The system, the use of modern cloud services to store data and not easily access physical data.

4.1.3 Testing

There are several degrees of testing in software development shown in Figure 55, particularly in the context of mobile applications. Unit testing, integration testing, system testing, and acceptance testing are the various testing tiers. A software module's smaller sections or components are the primary focus of unit testing. Integration testing examines the interrelationships between linked application components and detects coupling-related errors. System testing looks for flaws in the underlying hardware and the actual environment in which the mobile app will operate as a whole. To ascertain if the system satisfies user demands, requirements, and business procedures, acceptance testing is carried out.

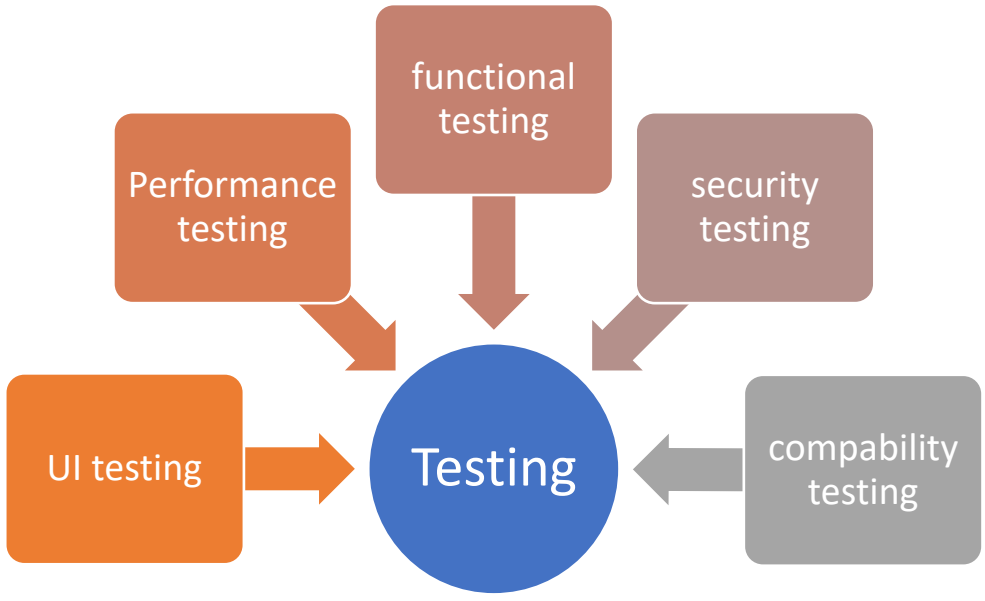


Figure 55 Testing levels

Testing presents a variety of difficulties in the mobile app space, like the continual updating, refactoring, and maintenance requirements brought on by the regular changes in business expectations. The goal of mobile app testing is to find flaws or identify problems in several areas of the app's quality, including its content, function, navigability, how well it performs, compatibility, accessibility, and security [46]. Designing testing activities with specific objectives is necessary for validating each aspect of the mobile app quality. In other words, it calls for various testing methods. Functional testing, testing for efficiency, security testing, connection testing, and testing for usability are the key forms of testing in the context of mobile apps.

UI Testing In order to provide users of mobile payment applications with a seamless and user-friendly experience, the user interface (UI) of the app is essential. To enable effective engagement with the payment app, the UI design should put an emphasis on readability, clarity, and straightforward navigation. The panels for starting transactions, entering payment information, and verifying transactions should be simple and straightforward in a well-designed user interface for a mobile payment application. It should provide simple tools, such as menus, buttons, and forms, to let consumers complete the payment procedure without difficulty. Users can better understand the status of the payment process by using visual cues like progress bars or loading animations. In order to increase user confidence in the payment app, the user interface should place a high priority on security measures. This entails adding security measures including encrypted sensitive data, secure login procedures, and obvious secure connection signs while processing payments.

Performance testing Software testing, known as performance testing, checks to see how well the program performs under demand. Performance testing's objective is to remove performance bottlenecks rather than uncover flaws. It evaluates the characteristics of the system's quality.

Performance testing attribute: the speed to establish the application's react responsiveness and scalability to establish the maximum load that the software program is capable of handling. And scalability to evaluate the stability of the application under changing loads.

We can do this testing using many tools, such as jMeter, webLoad, and LoadRunner.

Functional testing avoids a component or system's core mechanism in favor of focusing on the functionality requirements. It only focuses on the results produced in response to chosen inputs and circumstances of execution. Functional evaluation verifies UIs, external system behaviors, mobile web application programming interfaces (APIs), service functionalities, and system-based intelligence in mobile apps [47] Testing numerous features and capabilities such as account setup, fund transfers, payment processing, balance checks, transaction histories, and security measures like authentication and encryption would be included in functional testing for an electronic wallet mobile application.

Compatibility testing is a test that determines if a software program is compatible with a variety of hardware, operating systems (OS), mobile devices, networks, and databases. Compatibility testing is a type of non-functional software testing that is used to assure reliable applications and client satisfaction. It examines elements including usability, dependability, and performance.

Chapter 5
Results

5.1 Results.

5.1.1 Result of Statistical Analysis

The result of the statistical analysis shows that the local electronic wallets in Palestine enjoy integrity, confidentiality and availability from the point of view of users. However, there is a consensus among the users of the wallets that they are not satisfied with the technical support of electronic wallets. This reduces the percentage of the wallets enjoying integrity in exchange for availability and confidentiality. In addition, the results of statistical analysis were a sufficient answer to the main research question, Is e-wallet secure?

The results of the analysis underscored that the users of e-wallet feel safe in their use of the e-wallet, and with regard to the sub-search question regarding the integrity of the e-wallet, the users of the e-wallet also emphasize that there is a somewhat acceptable abundance of local e-wallets. with regard to the second sub-question concerning the confidentiality of the e-wallet, e-wallet users also confirm and demonstrate users' answers that local e-wallets enjoy a high level of confidentiality and protection. and finally, with regard to the recent sub-research question, which tests the abundance of local electronic portfolios, Users' answers show that portfolios have a fairly acceptable level,

5.1.2 Result of Reverse Engineering

Once we have access to the code, we may examine how the program keeps values, permissions, and other data that may be useful in bypassing specific constraints. When malware is discovered on a device, this approach of decompiling and analyzing the program may be beneficial in revealing what the virus is accessing and providing indications as to where the data is being transferred. The parts that follow go through Android malware in depth.

One of main results, found three files with name [classes], this may be the based difference between the local and international applications.

It is possible to modify the open-source code of a Jawwalpay wallet, as in the process of reverse engineering, its code was accessed in all details, and it turned out that it is several libraries interconnected with each other, which makes it easier for users to hack it and tamper with its contents and makes the application an unsafe application for its users According to the results of the current study and analysis of the application.

5.1.3 Result of Acquisition analysis

After conducting acquisitions of private data in the Reflect application on mobile devices that operate with the Android system and the IOS system, our results showed that it is easy to obtain data and information related to the e-wallet settings on the mobile, such as the documents through which the wallet was activated, such as a card Personal identity, proof of residence, also the payment movements that you had made on the e-wallet application were obtained and deleted later. This confirms that the wallet application is not secure and keeps all payment movements on the phone. For active e-wallet applications on Android devices, the Android Debug Bridge (ADB) pull command-line tool was able to effectively retrieve a lot of useful transaction data. The ADB pull might retrieve information showing both previous and present wallet existence on the mobile device in addition to transaction data.

The ADB pull was also capable of retrieving information indicating current and previous wallet existence on the mobile device[41], in addition to transaction data and the database file contains information, while the wallet data file contains keys, transaction metadata, and all file logs of the e-wallet. The results of this research indicate that it serves to aid law enforcement in connecting unlawful transactions involving these e-wallets on mobile devices to implicated individuals and devices.

5.2 Discussion

The current study found that users have faith in the well-known local mobile portfolio; given that people tend to remember and recover negative attitudes more readily than positive, [48] confirms that there is a noticeably positive perception of the local portfolio; and a greater percentage of study participants chose to describe a positive experience with the portfolio's electronic payment options.

Mobile payment features and conveniences can be used to explain the trend toward contentment. Mobile payments, which may be performed on the same mobile devices used for other daily duties in both the professional and personal spheres, simplify and accelerate time-consuming payments. Additionally, it does away with the need to type passwords and carry about extra codes like cash or credit cards. In general, mobile payments satisfy the needs and wants of contemporary customer. The incidence distribution and the high a susceptibility towards positive perception are probably influenced by sample characteristics. Participants in the study ranged in technological preparedness from average to below average. which is a constrained indicator of technological satisfaction [49].

Finally, the trustworthiness of the domestic portfolio is a favorable perception that may be influenced by the age of study participants. Younger people tend to be more comfortable learning and utilizing new technologies.

In this study, digital forensic examination of electronic payment apps was the primary cause of unacceptable accidents. According to the survey results, respondents believe that mobile payments are secure and reliable enough to prevent the theft of data from electronic wallets, which is at odds with the findings of digital forensic analysis. In addition, respondents' refusal to use electronic payment methods is a sign that the data they provide is unreliable. Due to the continued use of traditional payment methods, particularly card payments, any issues with mobile payment are likely to cause the client to switch to card payment. Another choice is to go with a different mobile payment company.

Due to the limited amount of data, only two groups of unsatisfactory sources emerged; however, individual occurrences demonstrate that some consumers have additional issues as a result of utilizing the payment solution and feel uneasy while using mobile device payments. Although the impacts of technological failure on customer discontent have been studied, complexity and security have not yet been the subject of any previous research.

5.3 Conclusion and Recommendations

This thesis presented a forensic analysis of the Android and IOS operating system and the remaining (digital) evidence in electronic wallets (Jawwal B and Reflect application) while the applications were on the phones and once the electronic wallet applications were uninstalled. The results showed that while the wallet application is on the phone, we can obtain valuable artifacts such as the email address through which the wallet was activated, and all the special documents that were uploaded to confirm the activation of the application and the possibility of using it. It is proven that when downloading/uninstalling e-wallet applications; Leave traces in the phone. This research proved that artifacts of forensic interest can be found in various locations within the Android and iOS systems, where all transactions made through the New Bank wallet are identified as plain text stored in the private log files in each wallet.

Based on the results obtained from the acquisitions of private data in the Reflect application on Android and iOS mobile devices, the research draws the following conclusions:

Lack of Security in E-Wallet Applications: The research demonstrates that the Reflect e-wallet application lacks sufficient security measures to protect sensitive user data. This includes personal identity documents, proof of residence, and payment transaction details.

Data Retention on Mobile Devices: The study reveals a concerning practice where the e-wallet application retains and stores payment transaction data on the user's mobile device. This data could potentially be accessed and exploited by unauthorized parties.

Effectiveness of ADB Pull Tool: The research highlights the effectiveness of the Android Debug Bridge (ADB) pull command-line tool in retrieving a significant amount of transaction data from active e-wallet applications on Android devices. This tool can access both historical and current wallet-related information.

Security Concerns for E-Wallet Users: These findings raise significant security concerns for e-wallet users, as their sensitive information and transaction history may be at risk of unauthorized access and potential misuse.

In conclusion, the research underscores the urgent need for e-wallet application developers to prioritize and enhance security measures to protect users' sensitive data. It is imperative that e-wallets implement robust encryption, data retention policies, and access controls to ensure the confidentiality and integrity of user information. Additionally, users should be educated about the potential security risks associated with e-wallet applications and be encouraged to adopt best practices for safeguarding their digital financial assets.

The recommendations of this research are to adopt a sound approach to overcome any threats to electronic wallets, and their ability to compete with international wallets, and to follow the proposed model in this research to establish electronic wallets in order to overcome all the challenges faced by cybersecurity in the world of electronic payment, theft of electronic wallets and embezzlement of funds

Based on the findings of your research regarding the security vulnerabilities in the Reflect e-wallet application, here are some recommendations:

Enhance Data Encryption: The e-wallet application should implement stronger data encryption protocols for both data in transit and data at rest. This will help protect sensitive user information from unauthorized access.

Secure Storage Practices: Implement secure storage practices within the application to ensure that user data, including personal identity documents and transaction details, is not stored locally on the mobile device. Data should be securely stored on remote servers with stringent access controls.

Data Retention Policies: Develop and enforce data retention policies to specify how long transaction data should be stored and when it should be automatically purged. This will reduce the risk of data exposure.

Access Controls: Implement robust access controls to limit who can access sensitive user data. Users should only be able to access their own information, and unauthorized access attempts should trigger security alerts.

Regular Security Audits: Conduct regular security audits and penetration testing to identify and address vulnerabilities in the application. This should include thorough testing of data extraction methods.

User Education: Educate e-wallet users about the importance of safeguarding their personal information and practicing good security hygiene. Encourage them to set strong, unique passwords and enable two-factor authentication where available.

Transparency and User Consent: Clearly inform users about what data is collected, how it is used, and for how long it will be retained. Obtain explicit consent from users for data collection and processing.

Continuous Monitoring: Implement continuous monitoring of the application for any suspicious or unauthorized activities. Set up alerts to detect and respond to potential security breaches in real-time.

Collaboration with Security Experts: Collaborate with cybersecurity experts and consultants to assess and improve the security of the e-wallet application.

Compliance with Regulations: Ensure that the application complies with relevant data protection and privacy regulations, such as GDPR or CCPA, to avoid legal and regulatory issues.

Regular Updates: Regularly update the e-wallet application with security patches and improvements to stay ahead of emerging threats.

Consider Third-Party Security Tools: Explore the use of third-party security tools and services to bolster the application's security posture.

By implementing these recommendations, the Reflect e-wallet application can significantly improve its security, protect user data, and enhance user trust in the platform.

5.4 limitation

One significant limitation of this study is the potential impact of new technology updates for e-wallets, which might restrict access to the required data by mobile forensic tools. The available mobile forensic tools, often limited in their trial versions, may not allow comprehensive data extraction, as compared to the more expensive premium versions, which could provide crucial data required for the study.

Furthermore, the methodology employed is expected to incur higher costs compared to previous research. This is primarily due to the necessity of conducting experiments on relatively new and expensive models of mobile phones. The inherent risks associated with these experiments, such as the potential need for jailbreaking or rooting the devices, add an additional layer of complexity.

Additionally, providing detailed explanations of electronic wallet procedures and functions will require trial requests, especially when investigating discrepancies related to discounts offered by local electronic wallets. These factors contribute to the overall challenges and complexities involved in the study.

Chapter 6
Appendices

6.1 Bibliography.

[1] A. Das, T. Satija, S. Zilpe, J. Kavya, and N. Kar, “A Study of Threat Model on Mobile Wallet Based Payment System,” 2018.

[2] S. Undale, A. Kulkarni, and H. Patil, “Perceived eWallet security: impact of COVID-19 pandemic,” *Vilakshan - XIMB Journal of Management*, vol. 18, no. 1, pp. 89–104, Mar. 2021, doi: 10.1108/xjm-07-2020-0022.

[3] K. Lee Yong Ming, M. Jais, and Y. Ming, “Factors Affecting the Intention to Use E-Wallets During the COVID-19 Pandemic,” *Gadjah Mada International Journal of Business*, vol. 24, no. 1, pp. 82–100, 2022, [Online]. Available: http://journal.ugm.ac.id/gamaijb

[4] L. Wulantika and S. R. Zein, “E-Wallet Effects on Community Behavior,” in *IOP Conference Series: Materials Science and Engineering*, IOP Publishing Ltd, Aug. 2020. doi: 10.1088/1757-899X/879/1/012121.

[5] yashraj Dokania, “neo bank revolution in indian banking sector - a critical analysis,” *3 Issue 6 Int’l J.L. Mgmt. & Human. 361 (2020)*, 2020.

[6] Z. Temelkov, “Factors affecting neobanks sustainability and development”, [Online]. Available: https://www.afi-global.org/wp-

[7] “Worldpay’s Global Payments .”

[8] Ezer Osei Yeboah-Boateng, “Cyber-Security Challenges with SMEs in Developing Economies: Issues of Confidentiality, Integrity & Availability (CIA),” *3 Issue 6 Int’l J.L. Mgmt. & Human. 361 (2020)*.

[9] M. Evangelou and N. M. Adams, “An anomaly detection framework for cyber-security data,” *Comput Secur*, vol. 97, Oct. 2020, doi: 10.1016/j.cose.2020.101941.

[10] L. A. Arram and M. Moreb, “Cyber Security In Mobile Apps And User CIA.” [Online]. Available: https://orcid.org/0000-0001-8146-6918

[11] P. Singh and R. S. Rajput, “Cybersecurity Analysis in the context of D.”

[12] P. M. Tun, “An Investigation of Factors Influencing Intention to Use Mobile Wallets of Mobile Financial Services Providers in Myanmar,” *The Asian Journal of Technology Management (AJTM)*, vol. 13, no. 2, pp. 129–144, 2020, doi: 10.12695/ajtm.2020.13.2.3.

[13] S. Teng and K. W. Khong, “Examining actual consumer usage of E-wallet: A case study of big data analytics,” *Comput Human Behav*, vol. 121, Aug. 2021, doi: 10.1016/j.chb.2021.106778.

[14] B. G. Amit Kumar Nag, “E-Wallet- Factors Affecting Its Intention to Use,” *International Journal of Recent Technology and Engineering*, vol. 8, no. 4, pp. 3411–3415, Nov. 2019, doi: 10.35940/ijrte.d6756.118419.

[15] Y. Yu, “Electronic Payment Performance: A Trend and Contextual Analysis of Its Social Impact on Secured E-Payment in 2016-19.” [Online]. Available: https://www.igi-global.com/chapter/electronic-payment-performance/293866

[16] R. Kaur, Y. Li, J. Iqbal, H. Gonzalez, and N. Stakhanova, “A Security Assessment of HCE-NFC Enabled E-Wallet Banking Android Apps,” in *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, IEEE, Jul. 2018, pp. 492–497. doi: 10.1109/COMPSAC.2018.10282.

[17] I. R. de Luna, F. Liébana-Cabanillas, J. Sánchez-Fernández, and F. Muñoz-Leiva, “Mobile payment is not all the same: The adoption of mobile payment systems depending on the technology applied,” *Technol Forecast Soc Change*, vol. 146, pp. 931–944, Sep. 2019, doi: 10.1016/j.techfore.2018.09.018.

[18] mohammed moreb, yaman salem and Khalid S. Rabayah, “Evaluation of Information Security Awareness among Palestinian Learners”.

[19] D. A. Orr and D. M. Lancaster, “Cryptocurrency and the Blockchain: A Discussion of Forensic Needs.”

[20] “master research-An investigation into blockchain’s forensic artifacts”.

[21] H. Chung, J. Park, and S. Lee, “Digital Forensic Approaches for Amazon Alexa Ecosystem.”

[22] A. Vaz, R. T. Fernandez, S. M. #3, and D. Rao, “Individual awareness of e-wallet and bank staff related fraud in Malaysia, in the face of widespread global digitalization.” [Online]. Available: https://ssrn.com/abstract=3811143

[23] S. Blenkin, “An Investigation into evidence (digital) artefacts resulting from the use of Cryptocurrency applications.”

[24] M. A. Hanul and S. G. In Recklinghausen, “Perceived Security and Usage of a Mobile Payment Application vorgelegt von,”

[25] S. Ghosh, A. Majumder, J. Goswami, A. Kumar, S. P. Mohanty, and B. K. Bhattacharyya, “Swing-Pay: One Card Meets All User Payment and Identity Needs: A Digital Card Module using NFC and Biometric Authentication for Peer-To-Peer Payment,” *IEEE Consumer Electronics Magazine*, vol. 6, no. 1, pp. 82–93, Jan. 2017, doi: 10.1109/MCE.2016.2614522.

[26] S. Brähler and B. Brähler, “Analysis of the Android Architecture Studienarbeit von,” 2010. [Online]. Available: www.kit.edu

[27] Satish. Bommisetty, Heather. Mahalik, Oleg. Skulkin, Rohit. Tamma, and Igor. Mikhaylov, *Practical Mobile Forensics : a hands-on guide to mastering mobile forensics for the iOS, Android, and the Windows Phone platforms.* Packt Publishing, 2018.

[28] Maryam Abu Safeia, “facebook messenger forensics- android and IOS operating system,” pp. 1–30, 2022.

[29] A. I. Ibrahim, O. Hamda, and M. Moreb, “The Efficiency of Mobile E-Wallet in Palestine - Case Study,” in *2021 International Congress of Advanced Technology and Engineering, ICOTEN 2021*, Institute of Electrical and Electronics Engineers Inc., Jul. 2021. doi: 10.1109/ICOTEN52080.2021.9493445.

[30] palestine monetary authority, “https://www.pma.ps/ar/الدفع-خدمات-شركات/المالي-القطاع-على-الرقابة-/الدفع-خدمات-شركات.”

[31] Vietnamese government, “VIETNAM FINTECH REPORT 2020 PRODUCED BY SUPPORTED BY,” 2021.

[32] samsung, “https://news.samsung.com/in/samsung-india-introduces-bill-payments-on-samsung-pay-now-pay-all-your-utility-bills-securely.”

[33] https://smartindex.ps/company/s/58695, “www.jawwalpay.ps,” 2020.

[34] PalPay, “https://www.palpay.ps,” https://www.palpay.ps.

[35] mepspay, “mepspay.”

[36] maalchat, “maalchat.”

[37] madfooat, “madfooat.”

[38] M. A. Hassan, Z. Shukur, M. K. Hasan, and A. S. Al-Khaleefa, “A review on electronic payments security,” *Symmetry*, vol. 12, no. 8. MDPI AG, pp. 1–24, Aug. 01, 2020. doi: 10.3390/sym12081344.

[39] ABDULLAH ALMUHAMMADI, “AN OVERVIEW OF MOBILE PAYMENTS FINTECH AND DIGITAL WALLET IN SAUDI ARABIA 2020 ,” 2020.

[40] D. A. Muhtasim, S. Yee Tan, A. Hassan, M. I. Pavel, and S. Susmit, “Customer Satisfaction with Digital Wallet Services: An Analysis of Security Factors.” [Online]. Available: www.ijacsa.thesai.org

[41] A. Montanez, “Investigation of Cryptocurrency Wallets on iOS and Android Mobile Devices for Potential Forensic Artifacts.”

[42] dex2jar, “https://github.com/pxb1988/dex2jar.”

[43] java project, “https://osdn.net/projects/sfnet_wwqjavaproject/downloads/jd-gui-0.3.1.windows.zip/.”

[44] M. Al Jutail, M. Al-Akhras, and A. Albesher, “Associated Risks in Mobile Applications Permissions,” *Journal of Information Security*, vol. 10, no. 02, pp. 69–90, 2019, doi: 10.4236/jis.2019.102004.

[45] S. Bhandari *et al.*, “Android inter-app communication threats and detection techniques,” *Computers and Security*, vol. 70. Elsevier Ltd, pp. 392–421, Sep. 01, 2019. doi: 10.1016/j.cose.2017.07.002.

[46] O. Hedlund, E. Liljekvist, and W. Mostowski, “Uncovering Signal Simplifying Forensic Investigations of the Signal Application,” 2021.

[47] “Mobile Apps Engineering Design, Development, Security, and Testing.”

[48] P. Otto, “The Effect of Gratitude and Compassion on Persuasion The Effect of Gratitude and Compassion on Persuasion Processing Processing.” [Online]. Available: https://digitalcommons.assumption.edu/honorstheses

[49] “Modeling Individual Beliefs to Transfigure Technology Readiness into Technology Acceptance in Financial Institutions”.

ملخص

نظرًا للارتفاع في استخدام المحافظ الإلكترونية للمعاملات المالية وإمكانية إساءتها في الأنشطة غير المشروعة (مثل غسيل الأموال وابتزاز الأموال والتهرب الضريبي)، يكمن التحدي في تتبع وتنظيم هذه المعاملات بسبب طبيعتها العالمية والنسبية المجهولة. وهذا يحفز الاستفسار حول إمكانية تحديد وجود واستخدام المحافظ الإلكترونية على الأجهزة المحمولة، خاصة في مجال الأدلة الرقمية والأمان.

تقدم هذه الدراسة إطارًا للتحقق من آثار المحافظ الإلكترونية في فحص الأدلة الرقمية للهواتف المحمولة. يتألف الإطار من ثلاث مراحل: جمع البيانات واختيار السمات والتحقق. باستخدام آثار المحافظ الإلكترونية من نظام اكتشاف التسلل، نقيم صحتها من خلال النمذجة الاحتمالية، وعلاوة على ذلك، بعد تكرار الحصول على البيانات عند حذف التطبيق من الهاتف، تبين أنه يحتفظ بجميع حركات المستخدم والمعلومات. وهذا أمر غير مقبول في مجال أمان المعلومات حيث يسهل سرقة الأموال وتحويلها بشكل غير قانوني.

تستخدم البحث كل من النهج الاستنتاجي (استبيان) والنهج الاستقرائي (تحليل رقمي). أظهرت نتائج التحليل الإحصائي لعينة من 70 مستخدمًا للمحافظ الإلكترونية في فلسطين أن المحافظ المحلية تظهر مستوى قبول للأمان. نوصي بتنفيذ استراتيجية قوية لمواجهة تهديدات المحافظ الإلكترونية وتعزيز تنافسيتها على المستوى العالمي، واعتماد النموذج المقترح في هذا البحث عند إنشاء أنظمة المحافظ الإلكترونية.

تشير النتائج إلى أن تطبيق Reflect NeoBank ليس آمنًا بشكل كافٍ. إنه يحتفظ ببيانات المستخدم حتى بعد الحذف، مما يشكل مخاطر أمان، بما في ذلك سرقة الأموال وتحويلها بشكل غير قانوني. نقارن أيضًا بين المحافظ الإلكترونية المحلية والعالمية، مسلطين الضوء على الاختلافات في الأمان.

سيسهم هذا البحث في توجيه البحوث المستقبلية وطرق التي يمكن لفحص الأدلة الرقمية تطبيق النتائج في حالات استخدام المحافظ الإلكترونية المحلية على الأجهزة المحمولة أو أي معاملات غير قانونية تتعلق بالمحافظ الإلكترونية.