ADDIS ABABA UNIVERSITY

ADDIS ABABA INSTITUTE OF TECHNOLOGY - AAiT

SCHOOL OF INFORMATION TECHNOLOGY AND ENGINEERING – SiTE

Framework for Identifying Forensic Artifacts from Ride-hailing Android Applications

Supervised by

Dr. Fitsum Assamnew

by

Munir Kemal

March 2025

A Thesis submitted in partial fulfillment of the requirements of Master of Science in Cyber Security

(SCHOOL OF INFORMATION TECHNOLOGY AND ENGINEERING)

Framework for Identifying Forensic Artifacts from Ride-hailing Android Applications

by

Munir Kemal

Examiners' Committee

Name	**Signature**	**Date**
(**Proposal Advisor**)		
(**Chairman of Department**)		
(**Internal Examiner**)		
(**External Examiner**)		

A Thesis Submitted in Partial Fulfillment of the Requirements
For Masters of Science in Cyber Security
Addis Ababa Institute of Technology
School of Information Technology and Engineering
March 2025

Abstract

Different services are offered through our mobile devices as a result of the increasing usage of smartphones in this world. One of these services is the ride-hailing service in which the taxi transportation service is managed from a common operation center with the help of driver and passenger applications that the end users have installed on their smartphones. In our country, Ethiopia, there are many companies that offer this service, such as Ride, Feres, ZayRide, Seregela, Safe, Taxiye, and others. Today, many crimes such as theft, murder, etc. are committed against drivers or riders while working or using this transportation service in Ethiopia. Current research focuses mainly on the forensic investigation of social networks and banking applications. A research by K. Kiptoo proposed a forensic investigation framework to identify forensic artifacts from Android on-demand ride applications such as Uber, Little and Bolt that operate in Kenya. In this research, we propose a forensic framework by customizing the existing framework proposed by K. Kiptoo to enhance the identification of forensic artifacts from Android based ride-hailing applications after experimentation with ride-hailing applications such as Ride, Zayride and Feres. The proposed forensic framework for ride-hailing applications involves six phases: Collection, Setting up and Configuration, Extraction and Preservation, Application Database Location, Examination and Analysis, and finally Reporting. While experimenting, we were able to recover valuable artifacts such as passenger profile information, passenger device details, location data, time information, and driver-related data from ride-hailing applications, which are crucial digital evidence in the investigation of digital crimes. This research also investigated the level of role and the challenges of using digital forensic evidence to close a criminal case by Ethiopian law enforcement agencies using a specially designed questionnaire distributed to them. The research findings show that even though its role as evidence usage is increasing, we were able to identify major issues such as legal and procedural inconsistencies, lack of expertise, resource limitation, and lack of clear forensic standards that may hinder the use of digital evidence obtained from digital systems such as ride-hailing applications in a digital world full of complex digital crimes.

Acknowledgment

Generally, I would like to express my gratitude to everyone who helped me throughout the journey to finish my thesis and research.

My advisor Dr. Fitsum Assamnew, deserves my first gratitude. His encouragement, guidance, patience, and feedback were invaluable for me to come up with this thesis. I would like to express my appreciation to the School Graduating Committee (SGC) for their suggestions and feedbacks during proposal defense and progress report sessions.

I am also very grateful to my colleagues, Tariku Eshetu and Tekeste Fekadu for their invaluable moral and technical support throughout the journey of this thesis.

I would like to thank Mubarek Shamil, Yilkal Argaw, Girma Alemu, Fikresilassie Getachew, Dagnachew Ibrahim, Desalegn Wada and all the participants of this research for giving me a lot of support and necessary information at the required time.

My beloved families deserve special acknowledgement for giving me time and the moral to fulfil my thesis.

Finally, I would like to thank the management of INSA for giving me the opportunity to attend my MSc program in Cyber Security.

Thank you all!

Dedication

This thesis is dedicated to my dear mama and baba, my beloved wife, and sweet children. Their presence, love, encouragement, and support have improved me throughout my life. I acknowledge you being my inspiration, my pillars of support, and the reasons why I keep going to achieve my goals.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

ACPO	**A**ssociation of **C**hief **P**olice **O**fficers
ADB	**A**droid **D**ebugging
APK	**A**ndroid **A**pplication **P**ackage
DD	**D**ata **D**ump
DNA	**D**eoxyribo **N**ucleic **A**cid
EC-Council	International **C**ouncil of **E-C**ommerce Consultants
E2EE	**E**nd-to-**E**nd **E**ncryption
HxD	**H**ex and **D**isk editor
GPS	**G**lobal **P**ositioning **S**ystem
ID	**I**dentity or **I**dentification
IEC	**I**nternational **E**lectrotechnical **C**ommission
INSA	**I**nformation **N**etwork **S**ecurity **A**dministration
INTERPOL	**Inter**national Criminal **Pol**ice Organization
iOS	**i**Phone **O**perating **S**ystem
IOT	**I**nternet of **T**hings
ISO	**I**nternational **O**rganization for **S**tandardization
IT	**I**nformation **T**echnology
JTAG	**J**oint **A**ction **T**est **G**roup
LEA	**L**aw **E**nforcement **A**gencies
MS	**M**icro**S**oft

NIJ	**N**ational **I**nstitute of **J**ustice
NIST	**N**ational **I**nstitute of **S**tandards and **T**echnology
PNG	**P**ortable **N**etwork **G**raphics
PII	**P**ersonally **I**dentifiable **I**nformation
PIN	**P**ersonal **I**dentification **N**umber
ODRS	**O**n-**D**emand **R**ide **S**ervices
OS	**O**perating **S**ystem
RQ	**R**esearch **Q**uestion
SIM CARD	**S**ubscriber **I**dentity **M**odule **CARD**
SMS	**S**hort **M**essage **S**ervice
SQL	**S**tructured **Q**uery **L**anguage
SWGDE	**S**cientific **W**orking **G**roup on **D**igital **E**vidence
UK	**U**nited **K**ingdom
US	**U**nited **S**tates
USB	**U**niversal **S**Serial **B**us

Chapter 1

1. Introduction

1.1 Background Information

Due to the increasing usage of smartphones in the world in general and particularly in Ethiopia, different services are nowadays offered through mobile applications. One of these services provided through mobile applications is in transportation area such as ride-hailing platforms. These ride-hailing platforms have become one of the popular ways for transport facilitation

According to Cepheus Growth Capital, the ride-hailing platforms provided approximately 90,000 rides in Addis Ababa, the capital of Ethiopia per day as of early 2021. If we estimate the average cost of each trip as 150 Birr, there will be an approximate transaction of 13 million Birr per day using these platforms. Due to this, ride-hailing platforms are becoming one of the leading digital economy sectors of the country[1][2].

Nowadays, there are more than 40 different types of transportation groups offering ride-hailing services in this country. Some of the popular ride-hailing transportation services in Ethiopia include Feres, Ride, ZayRide, Seregela, Taxiye, Weye, and others[1][3].

Even though ride-hailing platforms are highly booming in the country, it is not fully safe for drivers or passengers providing or using services in this sector. Using ride-hailing applications, attackers can precisely detect the driver's confidential information such as his/her driving license number, actual GPS location, plate number, and even his home

address[4] which helps the attackers to identify the driver they targeted to commit crimes they wanted easily. In our country as well, there are rising number of reports of crimes committed against drivers offering service in this sector such as theft and murder[5][6].

Forensic artifacts that can be identified from those ride-hailing applications can be a powerful tool in the investigation of crimes committed in relation to customers or stakeholders of ride-hailing applications. By carefully collecting and analyzing forensic artifacts, investigators can build a strong case against suspects and help to bring criminals to justice.

1.2 Motivation

Motivations for this research are:

- Rising number of crimes committed against using ride-hailing services.
- Potential integration and impact of digital evidence in the Ethiopian court.
- To make identification and extraction of digital evidence from ride-hailing applications easier for law enforcement agencies.

1.3 Statement of the Problem

Our day-to-day lifestyles are extremely influenced by the growing popularity of smartphones due to advancements in mobile technology and various applications running on the gadgets. With the help of our smartphones, we carry out various tasks such as calling a taxi, paying for our monthly electricity consumption fee and booking a flight. In our country, Ethiopia, considering ride-hailing / taxi calling applications as an example, they are facilitating the transportation services. But these services are under scrutiny due to rising number of crimes committed against drivers and passengers / customers such as theft and murder.

There are different researches that focus on forensic investigation of social media applications to identify artifacts left inside the smartphones as a result of those applications

which are helpful for the investigation of digital crimes[7][8][9]. There are also other researches that focus on forensic investigation of banking applications that give an online banking service in different countries of the world[10][11][12].

Moreover, one research done by K. Kiptoo proposed a specific forensic investigation framework for android on-demand ride applications that are operating in Kenya such as Uber, Little and Bolt[13]. To the best of our knowledge, this is the only research which is specifically focusing on forensic investigation of ride-hailing applications. This research was focusing on Uber, Little and Bolt applications that were offering transportation services only in Kenya[13]. Looking into the framework proposed by author of the research, it is very detailed even though it was a great work. But, we can easily identify a gap in it. Some of the identified gaps of the framework in the research include:

1. Identifying ODRS Applications Functionalities, as explained in the framework, is concerned with knowing the functionalities of each application. It is true that having any level of knowledge about applications, tools and devices will help for better forensic investigation and findings[14]. But restricting this only to the beginning phase of the framework neglects importance of knowledge of application functionalities throughout the framework.

2. Since there are some forensic imaging tools that even don't need root privilege for imaging and also due to the risks of rooting phones, the rooting step in the framework should not be compulsory. It is known that rooting phones has drawbacks that include bricking, losing warranty of the phone and impact on integrity of user data[15].

Therefore, customizing the framework is necessary to enhance the forensic investigation process focusing on ride-hailing applications.

In addition, the level of role and challenges in usage of forensically recovered digital evidences in Ethiopian courts is not researched.

In this research, we are going to identify the different types of forensic artifacts that can be found in ride-hailing applications which are operating in Ethiopia and how those artifacts can be used by courts to help the investigation of crimes committed that are

associated with ride-hailing transportation services in particular and digital crimes in general.

1.4 Research Questions

The identified research questions for this research are the following:

RQ 1. What forensic artifacts can be effectively recovered from Ethiopian ride-hailing applications?

RQ 2. How can those recovered forensic artifacts be effectively used for court purpose?

1.5 Objective of the Study

The general objective of this research is to identify digital evidence that can be recovered from ride-hailing applications to effectively use them in the Ethiopian court in the investigation of digital crimes.

In addition to the general objective mentioned above, the specific objectives considered for this research include:

1. Identify the different types of forensic artifacts from selected Ethiopian ride-hailing applications.
2. Propose a forensic investigation framework specific for ride-hailing applications
3. Investigate the role and challenges of law enforcement agencies in using digital evidence for crime investigation in this country.
4. Recommendation to enhance the use of digital forensic evidences in this country after identifying the challenges.

1.6 Contribution of the Study

The contributions of this research include the following:

- Enhance the use and acceptance of digital forensic evidence in Ethiopian courts to close a criminal case involving digital crimes.
- Enhance the forensic investigation task involving ride-hailing applications by developing a framework specific to ride-hailing applications.
- The research will provide new insights by identifying the usage and challenges faced during digital forensic investigation by Ethiopian LEA.
- Recommendation on how to effectively use digital forensic investigation in Ethiopia based on the identified issues.

1.7 Scope / delimitation

In this research, we will work on identifying forensic artifacts from selected top three internet-based ride-hailing applications offering transportation services in Ethiopia. Since these ride-hailing services provide two separate applications for the rider and the driver, the main focus of research will be on the passenger's application due to the risk and lack of voluntary taxi drivers for imaging their phones while working on the research. In addition, I will focus only on the Android versions of the applications. Simply the scopes of this research are the following:

- The research will focus on extracting and identifying forensic artifacts from three popular ride-hailing applications that offer transportation services in Ethiopia.
- The research will focus only on the rider's application from those selected ride-hailing applications.
- We will focus only on Android version of the applications.
- The research focuses only on extraction and identification of artifacts left on local on-devices only not on the cloud.

1.8 Structure of the Document

This thesis document has seven main sections. Section 1 is an introduction section which discusses the background, motivation, statement of the problem, research questions, objective, expected contribution, and scope of the study. Section 2 is about the literature review having two subsections each discussing about current knowledge related to digital forensic. In section 3, we will discuss the methodology employed in this research. Section 4 is about the proposed framework in this research. In section 5, we will discuss the experimentation and analysis to the research. Section 6 will discuss about results found as a result of the experimentation and Finally, in sections 7, we will summarize the research and point out possible future works.

Chapter 2

2. Literature and Related Works

2.1 Literature Review

2.1.1 Digital Forensic

NIST defines forensic science as the application of scientific knowledge or techniques to criminal investigations or the analysis of evidence that may be used in court. Forensic science encompasses a wide range of fields from anthropology and wildlife forensics to fingerprint and DNA analysis[16]. Different forensic techniques are used in a wide range of crime investigations[17][18]. NIST states that forensics may be required in a variety of circumstances, including gathering evidence for court cases and internal disciplinary procedures, handling malicious events, and peculiar operating issues. They also emphasized that the four-phase method shown in Figure 2.1 should be followed when performing forensics, regardless of the circumstances[19].

A digital forensic science is one category of forensic science dedicated to collecting and analyzing evidences linked to digital crime that is discovered on digital devices[20]. As technology becomes more and more integrated into our daily life, the possibility that digital devices will be relevant to a criminal investigation or civil lawsuit rises accordingly. Law enforcement agencies worldwide are facing massive backlogs of digital evidence as a direct result of the increase in investigations needing digital forensic expertise. Future trends indicate that there will likely be a significant rise in the number of instances

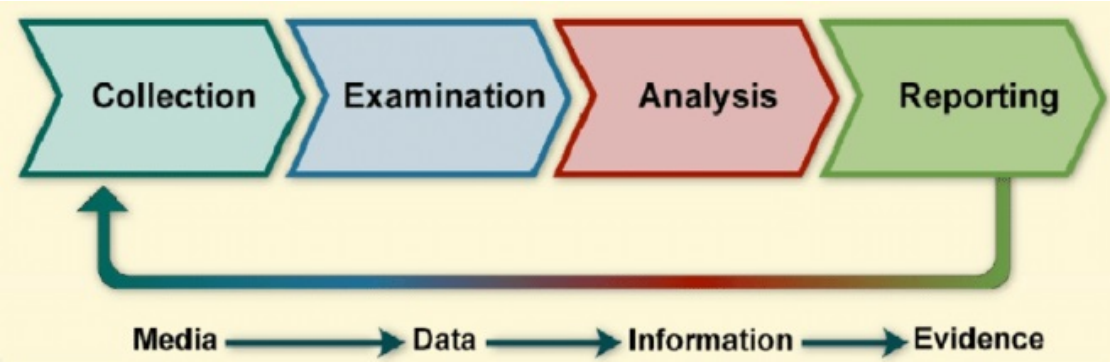


FIGURE 2.1: The four Phases of Forensic Investigation[19]

requiring digital forensic examination. Additionally, it's possible that each case will call for the examination of an ever-increasing array of gadgets, such as wearables, computers, cellphones, tablets, cloud-based services, IOT devices, and so forth[21].

2.1.1.1 Mobile Forensic

Mobile Forensic is a branch of digital forensics that deals with the forensically sound recovery of data from devices, like tablets and smartphones. Mobile device forensics helps to retrieve deleted data, call logs, SMS messages, application data, GPS data, pictures, and videos, among other types of data[22]. The primary goal of mobile forensic investigation is to identify criminals using suspicious pattern recognition techniques from the data extracted from mobile devices. Matching behavior prediction is a possible problem when illegal acts are associated with fully automated operations, such malware dissemination[23][24]. Prediction and detection, however, are stronger when human behavior is involved, as is the case with classic criminal cases[23][24]. EC-Council states that, during a forensic investigation, there are four basic procedures to take: locating the evidence, gathering the evidence, evaluating the evidence, and creating a forensic report. The following stages are related to those four mobile phone forensics procedure[22]:

1. **Device seizure:** Initially, the phone is taken from the owner of the device. At this point, the chain of custody should also be documented by the investigators. For instance, the documentation of who was using the phone and its time of seizure. If the phone is being used in an inquiry into a crime, a warrant for seizure is typically necessary.

2. **Device acquisition:** Second, investigators make a sector-level duplicate of the phone by "imaging" or "acquiring," it. To make sure it is an exact copy, the outputs of the hashing functions similarity are checked between this duplicate image and the original device. Analysts then choose the best course of action and objectives for the investigation.

3. **Device Analysts:** In order to verify a theory or look for concealed information, investigators start working on the device image. Information is located and recovered with the aid of specialized instruments. Data can be found in storage drive, erased (unallocated) drive space, or available hard drive space.

4. **Reporting:** Investigators save and examine the facts together into a credible account of what happened. Depending on the intended spectators, a technical or non-technical report might be created[22].

2.1.1.2 Tools and Techniques

There are different tools and techniques used by mobile phone forensic examiners. The popular mechanisms to extract data from these devices include[22][25]:

- **Logical Extraction**: - The phone is attached to a forensics investigation computer with the help of Bluetooth or a wire. This extraction is best for working with unrooted mobile devices. This method is fast and easiest to use, but has limitations. Tools such as Oxygen Forensic Device Extractor and XRY Logical are examples in this category.

- **Physical Extraction**: - Using this technique, the bit by bit memory of the device is dumped for forensic investigation. The method helps to have root access on the phone thus give full control of the device. This technique is the most comprehensive one, although it is technically challenging and depends on the producer of the device. Tools such as Cellebrite UFED Physical Pro and XRY Physical are well known examples in this category[22][25].

2.1.2 Android Operating System

The Android OS is a mobile operating system built on a customized version of the Linux kernel and other open-source software. It was drafted mainly for touchscreen mobile phones such as smartphones and tablets. Android is developed by an alliance of developers called Open Handset Alliance. But its most widely used version is mainly developed by Google[26][27]. The Android operating system is free and open-source. Due to these, anyone can modify and customize it based on his/her need free of charge. As a result, so many variants of Android devices are available on the market, ranging from low-cost budget phones to high-end flagship devices providing qualified services due to this powerful operating system[26][27]. Google made regular and continuous modifications to the OS with different and sequential releases to provide security patches and performance improvements. At the time of writing, the latest version of Android released is Android 15. It was released on 03 September 2024. It added various customizable features such as theme, language, music, and others. The added security updates established a control over the information that applications can obtain, the necessary permission for notification needed by all the applications, and the clipboard to erase personal information[26][27]. Even though Android is an open source software, most Android devices are shipped with a suite of proprietary software, like Gmail, Google Play, Google Maps, YouTube, Google Chrome, and others[28].

Moreover, software and application developers can utilize Android technology for building and developing mobile applications of their need or sell using application stores, like Google Play. Since the applications are developed as Google products, customers of Android have the option to link their Android devices to other products of Google like email services, cloud storage services, video services, and others[29].

2.1.3 Digital forensic in the Legal System

The process of event construction from a set of evidence to be presented in a court is called Forensic Investigation. It involves different investigations including financial fraudulent schemes to manslaughter[30]. According to INTERPOL definition, Digital

forensics is a kind of forensic science dealing with the identification, acquisition, processing, analysis, and reporting of data accumulated on a digital device such as a computer, or smartphone. Extracting artifacts from digital evidence, processing it into valid information, and handing over the results of the investigation for prosecution are the primary objectives of a digital forensics investigation[31]. Harbawi et al. explained that the idea of digital forensics had emerged in an effort to devise potential procedures to investigate and analyze digital crimes[32]. Digital forensics has developed quickly over the past ten years as a new battleground in the battle against crimes associated with the cyber ecosystem. Numerous nations have improved their academic system and research in this developing subject, established innovative technologies, and implemented new legislation and legal processes[33].

The United States has enforced legislation aimed at reducing a wide variety of cybercrimes at the state and federal levels[34]. NIJ publication prepared by researchers Goodison et al. discussed that extraordinary changes in the technology aspect over the last twenty years have increasingly emphasized the role of gathering and analyzing digital evidence in law enforcement proceedings[35]. Boost in technology has led to the gathering, storage, and accessibility of enormous amounts of data[35]. Modern devices, which are pocket-sized and can be used with a single touch, contain a significant amount of personal data. While accessing a wealth of information is advantageous for achieving convictions, it is very crucial for law enforcement agencies and their partners in the court system to find a balance between utilizing digital evidence and respecting individual's privacy[35].

NIST serves as a significant laboratory focusing on physical sciences and a primary provider of measurement standards in the United States of America. Cooperating with NIJ, NIST plays a crucial role in creating equipment standards for agencies within the crime investigation system. NIST made a significant step in September 2014 by launching a sub-committee on digital evidence who are dedicated with the task of "identifying and developing national standards and guidelines for practitioners of forensic science." The initiative - as explained by the researchers - was part of continuing efforts by NIST. The initiative included the publication of various reports and organizing seminars and conferences that focus on optimizing the practices of data mobile phones extraction[35].

Based on a research by Lallie H., the 2008 Mumbai terror attacks signaled the crucially for India to enhance its readiness in digital surveillance and improve its capabilities to orchestrate investigations after incidents. The researcher investigated state of digital forensic investigation infrastructure within India, by examining the legal frameworks, law enforcement agencies, and academic contributions of the country. He concludes that despite progress in establishing digital forensic investigation guidelines, these do not hold the same level of recognition as those in the UK (ACPO guidelines) and the US (NIST guidelines). He also noted that the potential for greater international cooperation in addressing cybercrimes that go beyond borders, the possibility for private entities to offer investigative and training support to law enforcement parties, and the opportunity for academic institutions in the US/UK to form partnerships with higher education establishments in India to foster and enhance the field of digital forensic investigation[36].

Apau et al. suggested that incidents of cybercrime persistently hinder economic growth across Africa. They also have explained that as a result of cybercrimes, the region loses millions of dollars each year. However, the potential for Digital Forensics Investigation, as seen in developed nations, offers a promising avenue for overcoming these cybercriminals. They evaluated the effectiveness of the legal framework, technical systems, capacity building initiatives, organizational structures, and the presence of collaborative efforts among key stakeholders in Ghana. They asserted for the presence of particular laws and designated agencies. Their findings suggest that, despite some progress over the years, advancement in the field of digital forensic investigation has been significantly slow, with the practice still in its early stages. Current laws are fragmented and complex and also the responsible agencies lack necessary capabilities. The researchers stressed need of consolidation in existing legislation into a unified and coherent legal system. Additionally, significant investments are needed to upgrade the capabilities of the respective agencies[37].

Looking at Ethiopia's context in crime investigation with the help of digital forensic analysis, there is a big gap in its status. Part one, article six and sub article fifteen of the Ethiopian Federal Police Commission establishment proclamation No.720/2011 states that Ethiopian Federal Police Commission can carry out forensic analysis, presenting the conclusions, and offer professional testimony to the court or the requesting body[38].

Whereas article number six and sub-article number eight of the Ethiopian federal proclamation number no 808/2013 for the re-establishment of INSA states that INSA has the power to perform digital forensic investigations with or without physical presence if authorized by a court warrant. This can be done in conjunction with the police on computers or infrastructure that are believed to be compromised or sources of cyber-attacks, in order to prevent further incidents and offer early warnings to the public[39].

Moreover, chapter thirty-three, article two of the Ethiopian computer crime proclamation No.958/2016 states that evidence obtained based on the criminal procedure code, related regulations or any computer evidence generated based on the proclamation or gained from relevant overseas law enforcement agencies with respect to the country's regulation may be accepted in the courtroom associated with digital offences[39].

Despite the forensic science practice has long age in this country, its evolution does not match its longevity. Forensic science does not have pivotal support for the crime investigation system. The main challenges lie in the scarcity of highly skilled professionals and a lack of essential resources. Low-level awareness among members of the law enforcement agencies regarding the significance of forensic science evidence is another challenge[40].

In a similar way researchers Kataria et al. suggested the need for prominent electronic forensic technologies for hampering digital crime in this country. In this country, there is no established digital forensic laboratory from which techniques or software tools can be employed[41].

2.2 Related works

N. Khoa et al. explained the analysis of forensic artifacts left due to Tik-Tok application on Android-based smartphones. They described in detail the full artifacts they obtained from this application from which an investigator can reconstruct exchanged message chats and followers of the user under investigation. In addition, they investigated the details of keywords and favorites of the user that can be used as evidence during a crime investigation[7].

While they were analyzing the forensic investigation of TikTok's application, P. Domingues et al. categorized the forensic artifacts obtained from Android smartphones into two groups. The first group is those that can be accessed without requiring the root privilege of the Android phone and the other group is for artifacts that are found in an Android phone that is rooted. In the rooted device, they were able to obtain a large amount of data such as the user account of the device under investigation, messages exchanged, and videos that can be important for a digital forensic investigator[8].

O. Osho et al. performed a digital forensic investigation on famous Nigerian Android-based mobile banking applications. They found that none of the applications they investigated kept critical data in their backups, and only one of the twelve applications they investigated kept critical data in the memory of the phone under investigation without imposing any of its security policies. In addition, they found that any of the applications deleted critical information while the applications were running in the background[10].

R. Chanajitt et al. performed a forensic and security investigation on Thailand's seven well-known mobile banking applications that run on Android operating systems. By applying the DD and JTAG methods, they learned that fascinating forensic data such as confidential data of the user involved with those applications installed on the device can be revealed. As an example from the banking applications, they recovered the bank details of the user from one bank. From three banks, they recovered the personal details of the user, whereas from two banks they were able to recover the PIN code of the user[11].

H. Kim et al. analyzed data remnants on phones after the data were deleted to know the capability of recovering data for better privacy of users using smartphones installed with recent Android versions 9 and 10. They performed three schemes of data deletion - data deletion due to application functionality, data deletion due to system application functionality, and due to removal of applications that were installed on the devices - and tried to show possible user privacy leakages on the two Android versions. They stressed the necessity of upgrading the security of user privacy in case of data deletion remnants[42].

While conducting forensic analysis on encrypted common Instant Messaging (IM) applications, K. Rathi et al. are able to show the locations of encrypted databases and

the possibility of decrypting the database files of WeChat, Viber, and WhatsApp applications installed on either rooted or unrooted devices. But they were able to locate the database files of the Telegram application only if the device was rooted[9].

Using qualitative and quantitative approaches, M. Al Thebaity et al. deduce that chat messages, login credentials, information about friends, and details of user accounts can be recovered after removing a Facebook application installed on a smartphone[12]. J. Bays et al. deduced that GPS artifacts such as GPS coordinates and reserved area positions can be recovered from Android and iOS phones with the help of either Life360 or the iSharing app. Additional data such as text chats and user account detailed information can be retrieved when the phones have root privileges[43]. R. Sinha et al. demonstrated that they are able to retrieve accurate forensic artifacts from six groups of Android fitness applications[44].

F. Salamh et al. conducted a deep and extensive forensic analysis of different famous applications installed on the recent versions of Android 10 and iOS 13 smartphones. They investigated 27 applications installed on Android and 33 applications installed on iOS. From the remnants due to those applications on the devices, they were able to identify suitable and useful data structures, stressed the privacy plus the security issues found on the two operating systems, and validated the replicability and ratification of the investigation on the chosen applications[45].

H. Zhang et al. investigated the various chat styles and the respective encryption conditions of artifacts from four famous Instant Messaging applications such as Facebook messenger, Hangouts, Line, and WhatsApp which are installed on Android devices. They found that Facebook applies private mode encryption to hide the message, in the case of Line and WhatsApp apps, they apply E2EE encryption to protect the messages which are vulnerable if they do not implement end-to-end protection. They also revealed that the database was not encrypted for a local user in a rooted phone so analyzing artifacts became easy[46].

I. Riadi et al. performed the analysis capability of the two commonly used forensic tools on mobile devices - Oxygen and MOBILedit - by investigating digital artifacts from the Line app. They concluded that for performing better timeline analysis and gaining chat text messages, the Oxygen forensics tool is better but it came short of obtaining

pictures or video data from the app. With MOBILedit, however, they recovered chat text messages, contact files, and pictures despite it failing to sort timeline chats[47].

F. Daryabar et al. examined four famous cloud client applications - OneDrive, Box, GoogleDrive, and Dropbox, on phones using both Android and iOS platforms. They found out that filenames as well as data that remain correlated to the employment of OneDrive and Box Android-based applications can possibly be retrieved from the device beneath the user IDs. They also found out that general details such as the name of the product, the name of the device, the iOS version, and the recent backup time of the client app remains are found in the files named with 'info.plist' and 'manifest.plist'[48].

A. Uduimoh et al. performed a digital forensic investigation on five Android mobile apps in Nigeria that facilitate banking tasks. In doing so, they were able to obtain digital artifacts such as login accounts of a user and details of bank transactions of the user[49].

N. Matulis et al. conducted a forensic analysis of Uber applications installed on iPhone mobile to identify where most of the data from Uber apps are saved or stored. Their findings showed that a large amount of forensic artifacts such as the PII of the user and geolocational information can be retrieved from the data of the application stored both in the cloud and the device[50].

T. Kitsaki et al. performed a forensic investigation on a different group of applications such as mobile banking, transport hailing, and network carrier applications to discover sensitive artifacts left on the mobile device. They employed disk and code investigation. From their findings, they concluded that those applications failed to apply efficient security procedures and techniques to keep safe the user data and important forensic artifacts that can be obtained from the devices. The leakage of private information like credit card detail, and bank transaction details are violating the critical privacy of the user which can lead to serious damage[51].

After surveying and analyzing the principal privacy and security-related risks due to the usage of ride-hailing services, Pham et al. proposed PrivateRide - a practical privacy-protecting and secure ride-hailing service - a solution that protects the satisfaction and practicality provided by ride-hailing services at the time. Implementation of this prototype on the passenger application and ride-hailing server introduces a minor delay by

ensuring privacy security but with little consequence on the functionality of the service provided[52].

In their research, Chen et al. disclosed that users may have varying knowledge of vulnerabilities and impact rating criteria, most modern tools are not efficient in identifying the vulnerabilities that need great attention in the banking sector and securing mobile banking applications need great effort[53].

Asher et al. performed an investigation of reverse engineering tools that are available to check the security of mobile banking applications that give service in Pakistan. In doing so, they got that any of the currently available reverse engineering tools perform a full reversing task independently. Additionally, they noticed that there is a remarkable variation in run time in addition to the amount of files produced by the tools on a single file[54].

Researchers A. Al-Dhaqm et al. stated that the field of mobile forensics employs an established scientific method with the goal of utilizing forensic techniques to retrieve valuable evidences from mobile devices. As a result, mobile forensic field has developed and recently gained prominence due to technology expansion, mobile-based products and services, and the demand for novel criteria. In order to discover open and upcoming difficulties and to expose the mobile forensic transitions, the authors undertake a survey of mobile forensics investigation process models. After reviewing about 100 papers regarding Mobile Forensics Investigation Process Models, they proposed a mobile forensic model titled with "Harmonized Mobile Forensic Investigation Process Model" in order to integrate and organize all of the superfluous investigation procedures activities, and functions associated with the mobile forensic profession[55].

Because of the complex nature of mobile phones and the requirement for specific methods and equipment, mobile forensics presents particular difficulties as explained in a recent research work by M. Moreb et al.[56]. They proposed a unique framework for mobile forensics investigation in order to overcome these issues. The researchers emphasized that the framework includes all of the steps and data sources required to build a case for criminal activity. Additionally, the framework eases the complexity and ambiguity in the field of mobile forensics, facilitates the collection and utilization of particular forensic understandings and eases the examination procedure[56].

As discussed in a research by B. M. V. Bernardo et al., many issues arise with mobile devices such as highly dynamic ecosystem, growing variation and cloud/IOT assimilation. As a result, having a safe and dependable toolkit is crucial for preventing, identifying, and resolving any issue associated with mobile forensics while investigating any type of criminal investigations. They propose a novel and creative framework in a forensic toolbox for mobile phones, associated to a series of diverse programs, procedures, and best application insights aimed at refining and enhancing the investigation process of a digital investigation[57].

K. Kiptoo on his thesis research, proposed a specific forensic investigation framework for android on-demand ride applications that are operating in Kenya such as Uber, Little and Bolt. His proposed framework was based on a flowchart involving the following repeated activities: Identify ODRS Application Functionalities, Artifact Location and Format Experiments, Android Rooting, Data Extraction, Preservation, Artifacts Examination and Analysis, and finally Forensics Report[13].

All the researches discussed in this section are so magnificent in the field of mobile forensic investigation including the findings, procedures and frameworks proposed. For the frameworks proposed by the researchers, even though they can be adopted as a general guide, they lack specialization for forensic investigation of ride-hailing applications to ease the task of a forensic investigator. Whereas, looking into the ride-hailing framework proposed by K.Kiptoo, it is very detailed even though it was a great work done by the author. But, we can easily identify a gap in it. Some of the identified drawbacks in the framework include:

1. Identifying ODRS Applications Functionalities as explained in the framework, it is concerned with knowing the functionalities of each application. It is true that having any information about applications, tools and devices will help for better forensic investigation and findings[14]. But putting this to the beginning of the process in the framework restricts the importance of knowledge of functionalities of applications throughout the framework.

2. Since there are some forensic imaging tools that even don't need root privilege for imaging and also due to the risks of rooting phones, the rooting step in the

framework should not be compulsory. It is known that rooting phones has drawbacks that include bricking, losing warranty of the phone and impact on integrity of user data[15].

Summarizing the review, we can see that there are many different research papers focusing on the forensic investigation and analysis of Android-based applications in different countries offering different services in particular and different social media applications in general. But any of the research papers propose a framework for identifying forensic artifacts from Android-based applications that are providing ride-hailing services, particularly in Ethiopia except a research done by K.Kiptoo which focuses only on ride-hailing service operating in Kenya. And also the framework proposed by the researcher has gaps identified in this research. So, the findings of this research will also serve as an insight to other researchers for further study on the issue in this country.

Chapter 3

3. Methodology

3.1 Research Methods

In this chapter, the details of the methods, approaches and techniques that will be used to conduct the research will be explained. In doing so, it discusses the procedures followed and instruments used to achieve the specific and general objectives of the research.

3.1.1 Study Design

In this research, we adopted a hybrid approach to address our objectives. The research involved a qualitative and quantitative study using open-ended and close-ended questionnaires to investigate digital forensics role as evidence in criminal case investigations in Ethiopia with an experimental approach to determine the types of forensic artifacts that can be recovered from ride-hailing applications that are installed on Android devices. A specific forensic investigation framework will be proposed after repeatedly analyzing the process of finding the artifacts from ride-hailing applications.

3.1.2 Tools Used

A questionnaire was designed to investigate the role and challenges of digital forensics in the investigation of criminal cases in Ethiopia from randomly selected participants. The

No	Smart Phone Used	Android Version
1.	Samsung Galaxy S8 (SM-G950U)	9
2.	Tecno (Spark 4 KC8)	10(HiOS v 6.2.0)

TABLE 3.1: Android phones selected for examination

No	Ride Application name	Application Version
1.	Ride	0.44.04
2.	Feres	1.0.55
3.	ZayRide	6.13.35

TABLE 3.2: Ride-hailing applications selected for examination

No	Organization Name	Population Size	Participants	Coverage
1.	Ministry of Justice	10	2	20%
2.	Ethiopian Federal Police	10	3	30%
3.	Information Network Security Administration	15	4	26.7%
Total		**35**	**9**	**25.7%**

TABLE 3.3: Participants' organizations (strata) and total population

designed questionnaire that was distributed to the participants is listed on Appendix B of this research. Google Forms[58] was used to distribute the questionnaire to the participants and for visualizing the quantitative part of responses from the participants. Moreover, the tools used and specifications of the Android phones and ride-hailing applications investigated in the experimentation are described in Table 3.4, Table 3.1 and Table 3.2.

No	Tool Used	Version	Description
1.	Windows 10 Pro 64-bit (with Intel Core i3, 4GB RAM)	22H2 (OS Build 19045.4780)	Workstation
2.	App APK Extractor & Analyzer	1.6.1(39)	An APK file used for extracting, generating and backing up APK files
3.	Cellebrite UFED	7.64.0.271	For acquisition forensic image from devices
4.	DB Browser for SQLite	3.12.2.0	To view database files recovered from the devices
5.	HxD	1.7.7.0	A Hex editor to view any hex data
6.	Notepad++	8.6.8	Different text file parser
7.	7-Zip File manager	16.04	Compressed file extractor
8.	MS Edge browser	128.0.2739.67	To browse xml files in this research

TABLE 3.4: Tools used in Experimentation

3.1.3 Sample

The population considered to participate in the questionnaire part of this research consists of professionals familiar with digital forensic investigations working at different organizations which are the responsible bodies for this task in the country [38][39]. Because of this, a stratified random sampling method was used with each strata representing different organizations involved in digital forensics related responsibilities. From each stratum, more than 5% of the available population was randomly selected as shown in Table 3.3. Inclusion criteria required participants to have experience in digital forensic investigations, while exclusion criteria omitted those without direct involvement in digital forensic investigations.

To forensically investigate and identify artifacts from ride-hailing application on mobile devices, two Android based phones were selected for experimentation in this research. The top two most popular mobile operating systems globally in the second quarter of 2024 are Android and iOS with a market allocation of roughly 71.65% for Android and 27.62% for iOS[59] as indicated by Statista. In a similar way, using Statista, we can

see that the Android market share in Ethiopia is very high with respect to iOS: 95.63% for Android to 3.52% for iOS as of August 2024[60]. Regarding the type of smartphone devices, Samsung and Tecno have the top two highest market share in Ethiopia as of August 2024[61]. Considering this statistics, we selected two Android devices namely Samsung and Tecno for this research. In our country, ride-hailing transportation services are becoming more and more popular as a result of rising urbanization and smartphone usage[2][3][62]. To the best of our knowledge, we could not find a research explicitly indicating the market share of each ride-hailing service in this country. In this research, the investigation will be done on Ride, Feres and ZayRide which are the most popular ride-hailing services offering transportation services in the country as explained on different sources[1][2][3][63].

Finding a volunteer was challenging because of the requirement of imaging of the phones to extract the forensic data and it was also risky because the phones may be damaged in case of rooting the devices when rooting the device is mandatory to extract the forensic data. Due to this and budgetary limitations for this research experimentation, only two smartphone devices having the top two highest market share in this country were selected.

3.1.4 Procedure

The questionnaire was distributed to participants using Google Forms as stated in section 3.1.2. Then participants' responses were collected, data was verified for completeness and the quantitative part of the responses were visualized using Google Forms. The qualitative part of the responses was manually analyzed to determine themes and codes that will help us answer our second research question. The three selected ride-hailing applications were installed on the two selected Android devices by downloading them from google play store[64]. Here are all the procedures to setup data collection environment.

1. Internet/ data and GPS location services on the devices were turned on.
2. Ride, Feres and Zayride applications are installed on the two devices directly from google play store[64].

3. The applications are activated using user phone numbers and user profile data are created including user name, mobile number and e-mail information.
4. Ride services are requested using each application from each device at a time.
5. After confirming the trip and boarding on the taxi, the driver is requested to start the trip using application.
6. Complete the trip by following the trip information on the applications.
7. Throughout the trip, random screenshots were taken by the passenger from each phone for comparison purpose.
8. Remove SIM Card from the devices and flight mode is turned on for each device.

After completing the trip using each ride-hailing application installed on the two devices at a time, data extraction process was started. The procedure for data extraction on each device is as follows:

1. Turn Developer options on for each device.
2. Turn USB debugging on for each device.
3. Start Cellebrite UFED from the workstation.
4. Connect one device at a time to the workstation using original USB cable.
5. After Cellebrite had detected the connected device, select the directory to save extracted data from the phone.
6. Choose Smart Flow Action.
7. After Cellebrite analyzed the phone internal memory, select “full file system” extraction option.
8. Wait the extraction process to finish which is a time taking process. Finishing this phase, we will have the extracted image file.

3.1.5 Data Analysis

In this research, the research questions identified are

1. What forensic artifacts can be effectively recovered from Ethiopian ride-hailing applications
2. How can those recovered forensic artifacts be effectively used for court purpose?

To answer the first research question, the strategy we followed is first identify Android package name of the three selected ride-hailing applications. This can be done by looking in Android manifest file after downloading the corresponding APK file into the forensic workstation from the smartphones using different tools such as FastBoot ADB and then reversing it using different APK reversing tools. Alternatively, an APK file named "App APK Extractor & Analyzer"[65] can show us the package name by simply installing and running it on our mobile as shown in Figure 3.1

To gather artifacts and their locations inside internal memory of the phones, we used Android package names we found using an Android application called "App APK Extractor & Analyzer". We investigated every file we found under those package names using tools such as Notepad++, HxD and DB Browser for SQLite. All the artifacts we found were located in the directory data/data/app_package_name inside the phones internal memory which is not visible using normal privilege to access the device directory and can only be accessed with root privilege[66]. For confirmation, we checked generated artifacts with the data we had while using each application.

The quantitative parts of participants' responses for the questionnaire were visualized using Google Forms whereas the qualitative parts of the responses were manually analyzed using thematic analysis method to determine codes and themes that will help us answer our second research question.

3.1.6 Evaluation criteria of the framework

The framework will be evaluated using evaluation criteria reliability, efficacy and cost-effectiveness to validate its effectiveness.

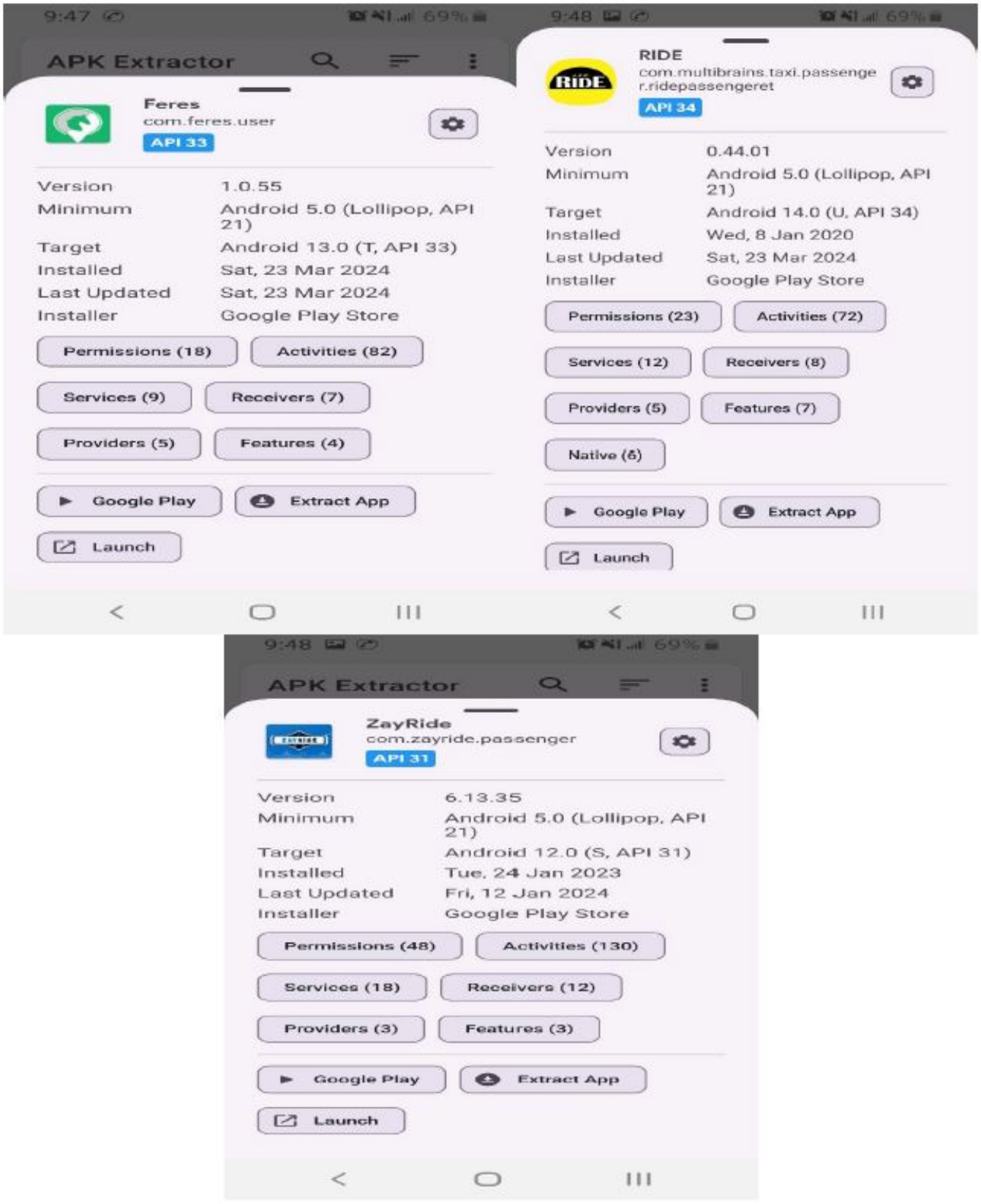


FIGURE 3.1: Package names for each ride-hailing application directly on the phone

3.1.7 Ethical Consideration

To ensure ethical compliance, participants' identity was anonymized while they make responses to the questionnaire after a consent was obtained from all participants before data collection was started. While working on the experimentation part, we may encounter sensitive information from passengers, drivers and application developers.

Generally, to protect the privacy and security of passengers, drivers, application vendors, participants of the questionnaire and any party involved in the research, we took the following measures:

- Any sensitive data found will be will be blurred for use in the research findings discussion.
- In case vulnerabilities are discovered, it will be ethically disclosed the vulnerability details to the specific vendor.
- Cooperate with the vendors to eliminate the vulnerability and minimize user risk in case of vulnerabilities.
- Consent should be obtained from all participants of the questionnaire respondents.
- Anonymizing participants' identity.

Chapter 4

4. Proposed Framework

A framework is a comprehensive structure for organizing and guiding complex activities, without dictating strict sequences. It is different from a step as step is a distinct, actionable element within a sequential linear process[67].

As explained in literature review section of this research, the universal framework for digital forensics investigation adopted by NIST has a four-stages. These are collection, examination, analysis, and reporting and they are explained as follows:

1. In data collection phase, data of a particular event is detected, designated recorded, gathered, and also its integrity is maintained.
2. During the examination phase, applicable forensic tools and techniques are applied to detect and extract valuable artifacts from the acquired data while maintaining its integrity.
3. In the analysis phase, results from the examination phase are examined to extract valuable artifacts that motivated the data collection and examination tasks.
4. Reporting the analysis's findings is the last stage of the framework proposed by NIST. This can include summarizing the steps taken, figuring out what more needs to be done, and suggesting changes to the forensic process's policies, standards, procedures, tools, and other elements[19].

It is true that this framework process can be used for any digital forensics investigation purpose. But this is very generic that for a mobile forensic practitioner, it doesn't specify particular and detailed steps like configurations needed or locating databases that would help the expert executing the examination job to speed up and make the investigation job easy.

Whereas mobile forensics framework for ride-hailing applications that was proposed by K.Kiptoo[13] is much more detailed than the one adopted by NIST and it helps to easy the task of forensic practitioner as it is very particular for ride-hailing applications.

This research paid attention to the processes and findings of experiments done in those researches mainly the one done by K.Kiptoo[13] and other researches to propose an enhanced framework that is specific to ride-hailing Android mobiles forensic investigations. In doing so, the framework proposed in this research addresses the issues discovered in the above forensics frameworks. The proposed framework after customizing K.Kiptoo's[13] framework has six phases as depicted in Figure 4.1. As it can be seen in the proposed framework, it gives more emphasis to the collection and examination phase of the forensic framework adopted by NIST discussed in the literature review section. This makes sense when looking at the challenges of forensic data acquisition in mobile devices. It involves cautious activities while collecting and examining mobile forensic investigation. The phases of this forensic investigation framework is explained as follows:

1. **Collection** This involves device identification, designation, collection of any data associated with the smartphone such as vendor, model, the device's user name, state of the device and others by following the forensic protocol and keeping the phone in a secured manner. Device isolation should be done immediately to keep the data inside the phone from being lost as the device data may be wiped using remote communication mechanisms. To avoid the data from lose, disabling the communication system should be enforced, for example, turning on the flight or airplane mode of the phone is needed.

2. **Set Up and Configuration** After collection, the Set Up and Configuration phase is very critical for data extraction phase based on this proposed framework. In this phase, based on the information gained in the collection phase, setting up and some device configuration tasks are accomplished. This may include rooting the device,

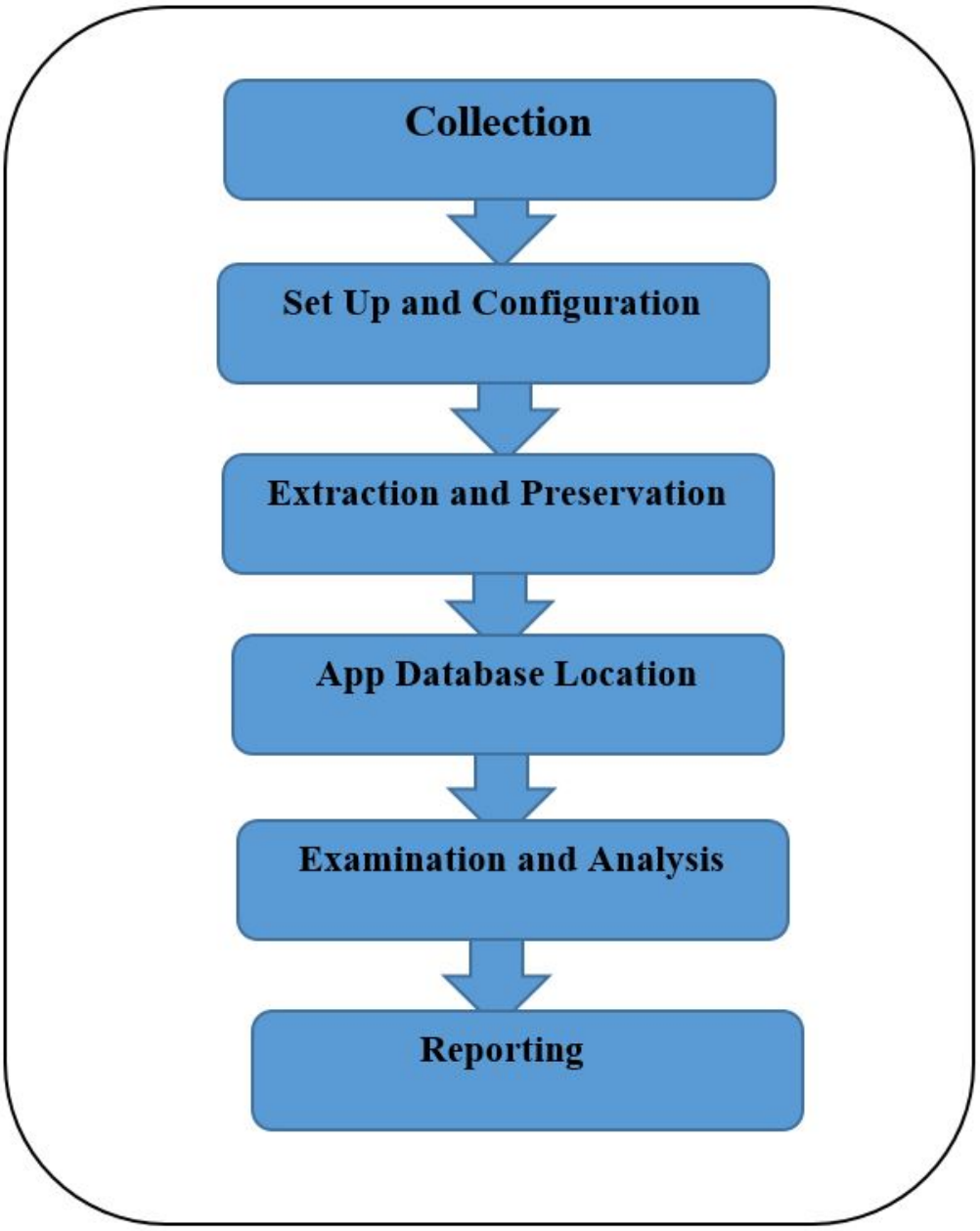


FIGURE 4.1: The Proposed Forensic Framework

enabling developer mode, enabling USB debugging and others. Due to android security enhancement, rooting the device might not be successful[15][68]. In that case, other configuration mechanism may be needed. This phase also focuses on choosing appropriate forensic imaging and analysis tools and configuring them. Some tools are so robust that data extraction becomes easy.

3. **Extraction and Preservation** In this phase of the framework, extraction of the mobile data is done using appropriate tools and materials. There are tools that can easily extract the memory of the phone. In this phase, full data of the phone is extracted and should be stored in a secured way using some labeling on the file name. The extraction processes may take some time. Thus, patience is needed until it finishes. The extracted image should be preserved securely to keep the data from modification and its original copy should be kept safely.

4. **Application Database Location** This phase is concerned with looking for the database directory of the applications being investigated inside the extracted image file. Since most of private data are stored in the application database as indicated in this research experimentation and the research of K.Kiptoo[13], the forensic investigation practitioner should look for this database at first. Otherwise since the acquired image may be bulky, looking inside each file may complicate the artifact identification process. The task of looking for application database becomes simple with the help of the APK's Android package name and use this package name to find its database where many important artifacts can be located.

5. **Examination and Analysis** After locating those important files from the acquired image, the next phase is examining and analyzing the files that can help as evidence in the court. Every file under the APK's package name should be examined properly. Some files identified may be encrypted or seem meaningless. But with the help of different tools, those files should be tried to parse them. We can use some online tools which can help to have a meaningful artifact. Offline tools such as SQL Lite, text editor and hex parser like HxD are powerful in artifact identification from a selected file.

6. **Reporting** The last phase of the proposed framework is reporting. In a similar way to the basic digital forensic investigation framework, this phase should have a summary of the whole steps followed and judgment made through the examination

phase. All the necessary information such as name of the forensic expert, case number and reporting agency[15] should be included.

Chapter 5

5. Experiment and Analysis

After data was collected for the questionnaire, it was organized into quantitative and qualitative data. We used the Google Form built-in graphical representations feature for visualizing the quantitative data of the responses. Thematic analysis method was used to identify, analyze patterns (themes) within the qualitative data.

Due to budgetary limitations and lack of volunteers (due to the risks of device damaging while imaging the device), only two Android based phones were used by the researchers for experimentation. Those selected device models are Samsung S8 (Android version 9) and Tecno Spark RC8 (Android version 10) as explained in Table 3.1 of the research methodology section. Ride-hailing applications considered for the experimentation are: Ride, Feres and Zayride with their application version as explained in Table 3.2. The procedures for installation of the applications on each device, profile creation and taking ride services were explained in the research methodology section.

Data extraction was attained using the well know forensic imaging tool Cellebrite UFED installed on the forensic workstation. Before extracting data from the devices, developer options and USB debugging mode should be enabled on each phone. It is explained as follow:

- Open phone “Setting”.
- Go to “About”/ “Software Information”
- Find “Build Number” information.

- Press "Build Number" seven times.

Finishing those activities will turn on the developer options and USB debugging mode settings on the two phones. After that, the default USB configuration protocol should be set to file transfer. This can be done as follow:

- Go to the developer options.
- Search for USB configuration and press/ tab it.
- Select file transfer from the available options.

Now on the workstation, Cellebrite UFED was opened to start the device's image acquisition process. All the pictures of the procedures are shown in Appendix A.

1. On the first page, the option "Mobile device" is selected from the given options as shown in Figure A.1 of Appendix A.
2. When the UFED asks to choose action on the next page, "Smart Flow" option is selected as shown in Figure A.2 of Appendix A.
3. UFED on the workstation waits the phones to connect as shown in Figure A.3 of Appendix A.
4. Using original USB cable, the phone becomes connected to the workstation and wait until the phone is detected in the UFED.
5. Next select directory where to save the extracted data.
6. After that UFED tries to access the devices Operating system. When it recognizes the Operating system, it will display detailed information of the phone after gaining Operating system access as shown in Figure A.4 of Appendix A.
7. From that page, preferred extraction type is selected. In this research the option "FULL FILE SYSTEM" is selected as shown in Figure A.4 of Appendix A.
8. Wait to finish extraction which is a long time process. When it finishes, press the finish button as shown in Figure A.5 of Appendix A.

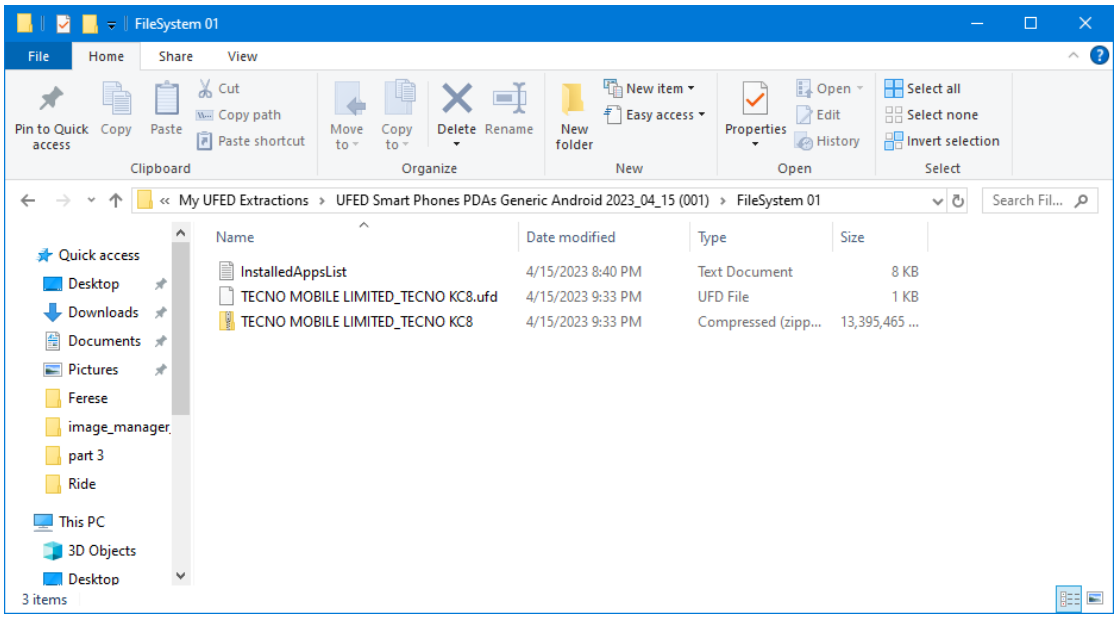


FIGURE 5.1: Inside the extracted data

After data extraction from each phone is finished, a copy of the image file should be saved in a secured path or device before analyzing it. Looking into the extracted data, there are three files inside the directory as shown in Figure 5.1.

For the forensic purpose, important file from data directory is a compressed/zipped file having a filename of the phone vendor name and its model. To search forensic artifacts, the compressed file is extracted using 7-Zip file manager. Inside the extracted file, there is a file named "Dump". When this file is opened, there are other sub files under this file.

The extracted data is huge so that searching artifacts in every file inside the image is very complex and time consuming. To simplify this task, we have to locate or find the database files related to each ride-hailing application. The database files can be found with the help of each ride-hailing application package name[13]. To determine the package names, an APK file called "App APK Extractor & Analyzer" was used. The procedure is as follows:

1. Open "App APK Extractor & Analyzer" APK file on a phone.

2. Select the three ride-hailing applications installed on the devices one at a time inside "App APK Extractor & Analyzer".

No	Application Name	Package name
1.	Ride	com.multibrains.taxi.passenger.ridepassengeret
2.	Feres	com.feres.user
3.	ZayRide	com.zayride.passenger

TABLE 5.1: APK file and corresponding package name

3. It will show the package name of each selected application as shown in Figure 3.1 in research methodology section.

Using "App APK Extractor & Analyzer", the identified package names of each APK file is as shown in Table 5.1.

The APK package name of each ride-hailing application can also be verified by looking inside the manifest file of each application after by decompiling the application using an APK file decompiler[69][70].

Using the package name of each ride-hailing application, the extracted forensic image file is examined to identify directory of each corresponding application in the image file. After identifying the path / directory of each of the three applications, the data inside that directory is parsed and examined using different tools such as SQL Lite, HxD, Notepad++ and other tools to gather meaningful artifacts.

The questionnaire disseminated to the participants involved open-ended and close-ended questions that were expected to be responded by the participants. After collecting participants' responses, the close-ended responses were analyzed using quantitative data analysis approach whereas the open-ended responses were analyzed using thematic analysis for qualitative data. The detailed analysis of the key insights from responses of participants of the questionnaire are discussed as follows.

All of the respondents are from law enforcement and legal institutions as shown in Table 3.3. Their professions are Police Officers, Public Prosecutors, Forensic Analyst and IT & Cybersecurity Instructor in those organizations. Most of the respondents have 6–10 years of experience, with some having 0–5 years and the rest having 11–15 years of experience as shown in Figure 5.2. All of the participants used digital forensic evidence

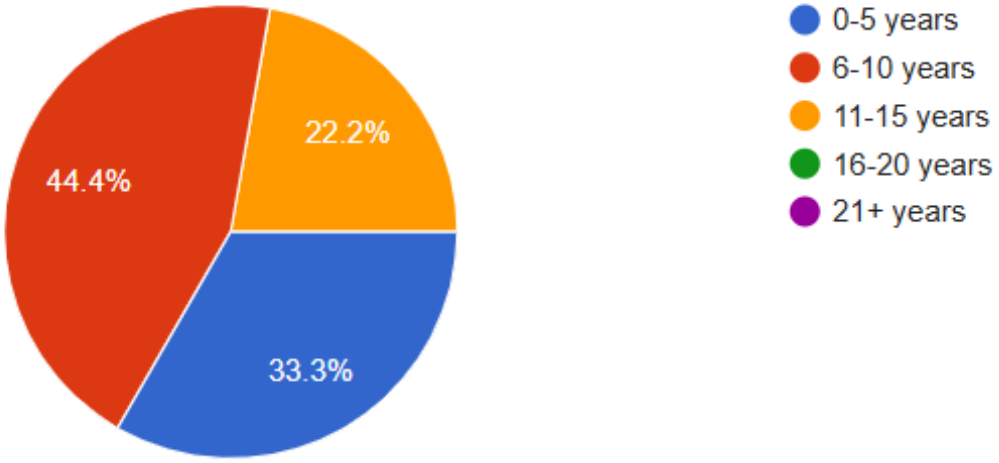


FIGURE 5.2: Participants year of experience in digital forensic investigation

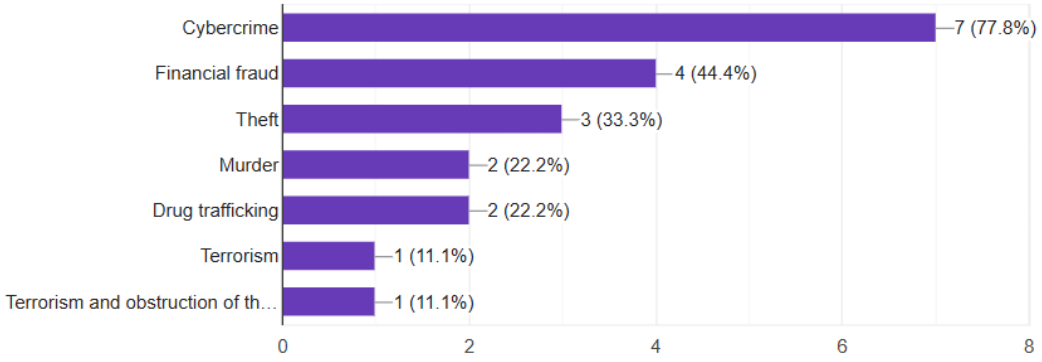


FIGURE 5.3: Type of cases respondents have used with digital forensic investigation

in their work with 55.6% (5 out of 9) participants said they are very familiar with digital forensics investigation while the rest 44.4% said they are moderately familiar with it.

The type of crimes on which they used digital forensic investigation for evidence are Cybercrime, Financial fraud, Theft, Murder, Drug trafficking, Terrorism and Obstruction of the constitutional order. The details are shown in Figure 5.3.

Majority (66.7%) of the respondents said they follow standards or best practices to maintain the admissibility of their digital forensic investigation with many (55.6%) saying ISO/IEC is the standard or best practice they adopt to maintain the admissibility of the digital forensic evidence as shown in Figure 5.4 and Figure 5.5 respectively.

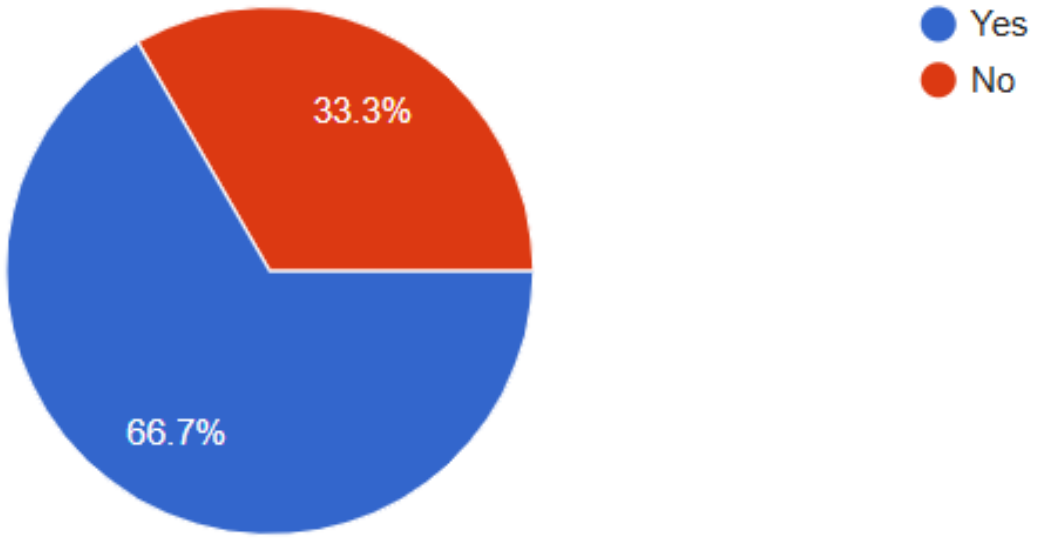


FIGURE 5.4: Standards or best practices adoption by percent

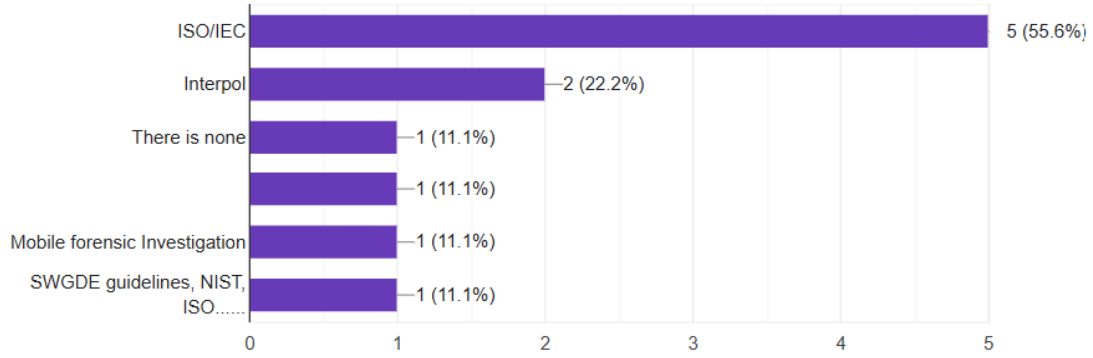


FIGURE 5.5: Type of Standards or best practices adopted

Even though they adopt a standards or best practice, 77.8All of the respondents said "Lack of clear guidelines" is the main challenge they face when they try to keep the admissibility of digital forensic evidence in court. "Discrepancies in the legal standards" was selected by four of them and "Difficulty in meeting admissibility criteria" also was selected by four of the respondents as the main challenge they face when keeping admissibility of digital forensic evidence in court as shown in Figure 5.6.

55.6% of the respondents said they recently had experienced legal cases that had been challenged the admissibility of digital forensic evidence. The general challenges they have encountered when working in digital forensic investigation are shown in Figure 5.7.

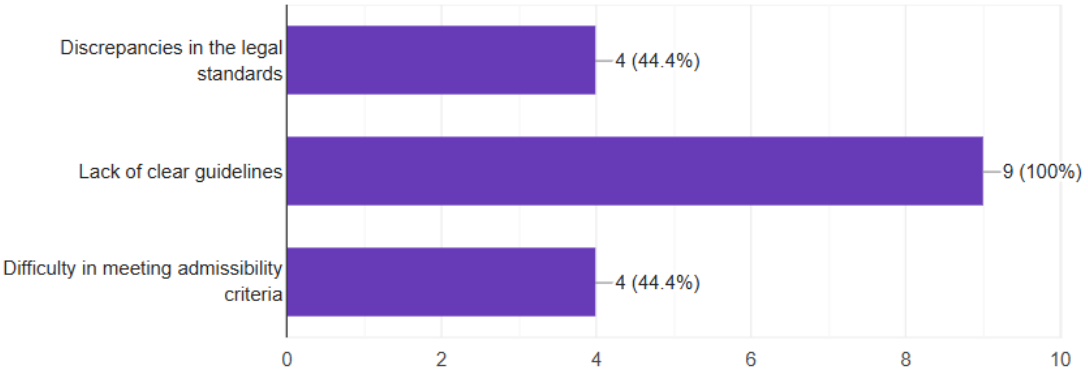


FIGURE 5.6: Challenges of admissibility of digital forensic evidence

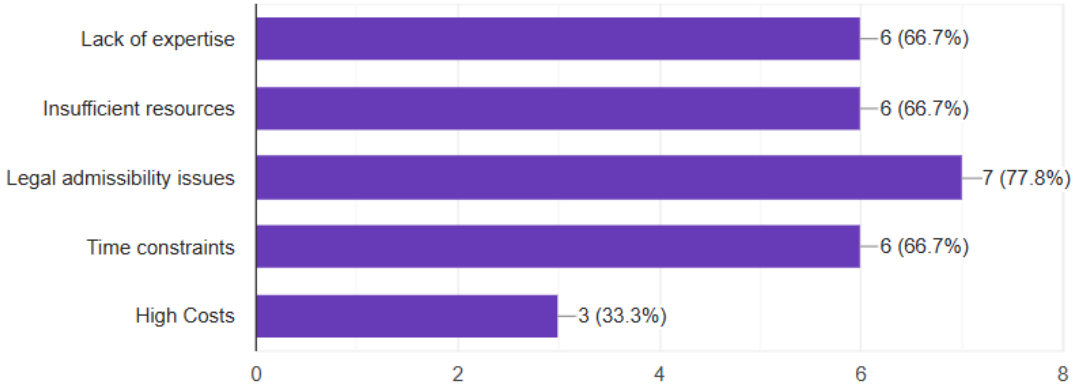


FIGURE 5.7: General challenges while working in digital forensic investigation

Majority (55.6%) the respondents said the general challenges shown in Figure 5.7 are very significant in affecting the use of digital forensic evidence in the court as shown in Figure 5.8.

According to the respondents, digital forensic evidence has been crucial in closing criminal cases. Most respondents replied 1–5 cases while a few replied 6–10 or more cases that have helped secure a conviction as shown in Figure 5.9.

However, there are also cases where digital forensic evidence was unable to help to conclude a criminal case, with 77.8% of the respondents reporting 1–5 cases or more failing to help to conclude a criminal case as shown in Figure 5.10.

The improvements suggested by the respondents (based on the challenges they faced) to enhance the use of digital forensic evidence in Ethiopian courts is shown in Figure 5.11

For the qualitative data, we used thematic analysis method as we explained in the beginning of this section. V. Clarke et al. defined thematic analysis as the process of

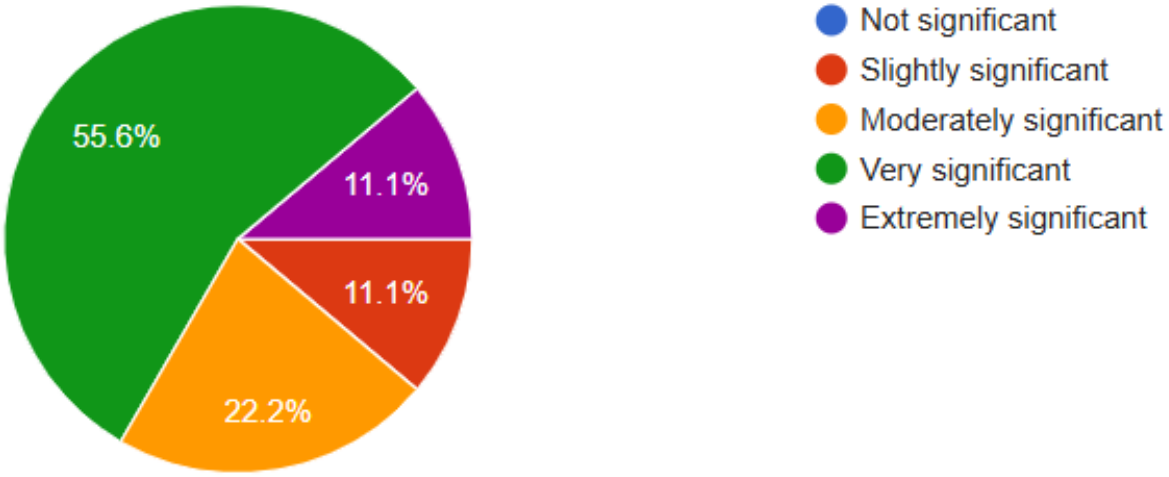


FIGURE 5.8: Significance of the challenges on digital forensic investigation task

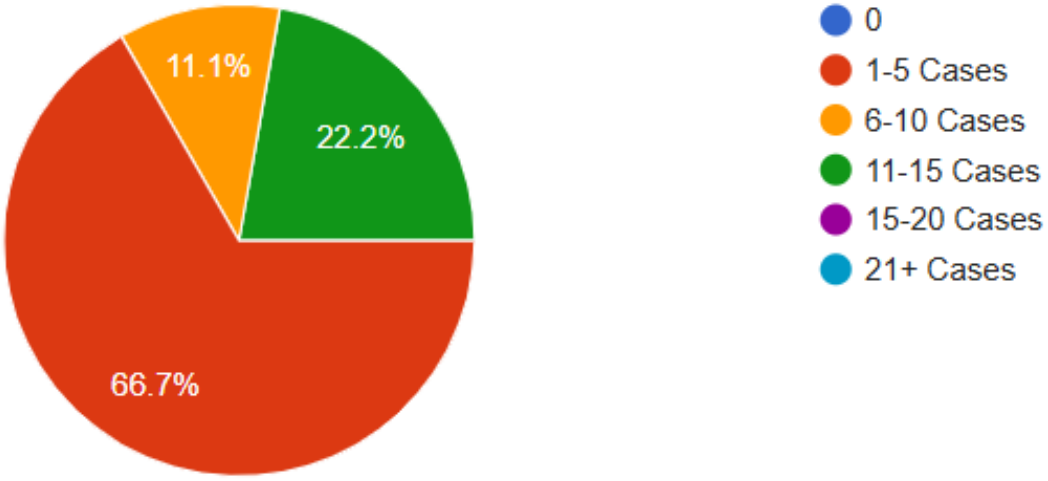


FIGURE 5.9: Digital forensic evidences cases that helped to secure a conviction

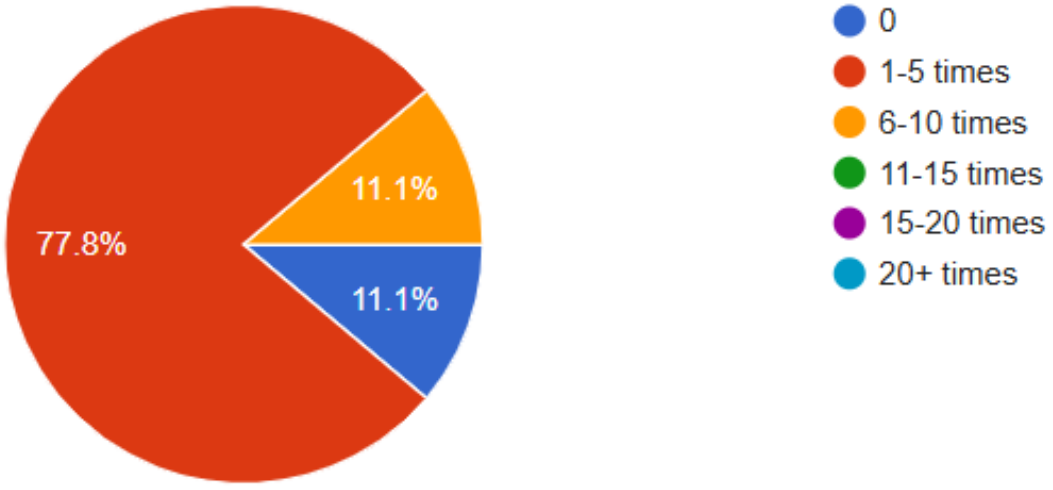


FIGURE 5.10: Digital forensic evidences cases that failed to help to secure a conviction

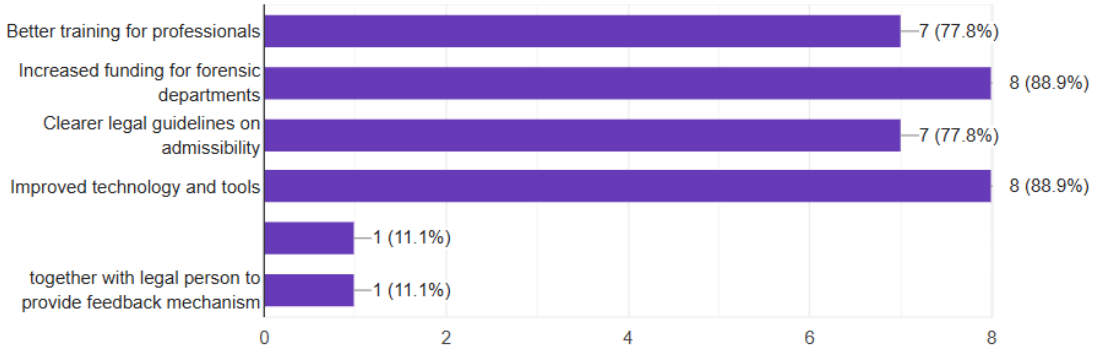


FIGURE 5.11: Improvements suggested to enhance use of digital forensic evidence

finding, examining, and interpreting meaningful patterns - also known as themes – inside the qualitative data. Using a research question as a guide, thematic analysis helps to discover and understand important, though not necessarily all, aspects of the data rather than merely summarizing its content. They outlined the six phases of thematic analysis as familiarizing oneself with own data, generating initial codes, searching for themes, reviewing themes, defining and naming themes and finally producing a report[71].

Since the data at our hand were small, we used the thematic analysis method manually. After familiarizing ourselves with our data, we identified the following codes from our collected data: Legal admissibility issues, Chain of custody problems, Judicial reluctance, Revise current criminal law, Data integrity concerns, Standardized forensic

No	Theme	Code
1.	Legal Admissibility	Legal admissibility issues, Chain of custody problems, Judicial reluctance, Revise criminal law
2.	Expertise and Training	Lack of forensic expertise, Training for professionals, Launch educational campaigns
3.	Challenges in Investigations	Challenges in admissibility, Investigation complexity, Data integrity concerns, Standardized forensic practices , Courts prefer eyewitness, Privacy issue
4.	Forensic Tools and Resources	Resource limitations, High costs
5.	Judicial Impact	Digital forensic as evidence, Criminal case resolutions

TABLE 5.2: Identified codes and themes using thematic analysis

practices, Lack of forensic expertise, Training for professionals, Launch educational campaigns, Challenges in admissibility, Courts prefer eyewitness, Investigation complexity, Insufficient resources, High costs, Digital forensic evidence use and finally Role in case resolutions. We organized these codes in to themes by arranging closely related codes into one theme as shown in Table 5.2

Next, we discuss the definitions of each theme generated by categorizing similar codes with respect to our second research question:

Theme 1: Legal Admissibility

This theme refers to the ability of digital forensic artifacts to be legally accepted as evidence in the court. It includes challenges such as ensuring compliance with legal standards, maintaining a proper chain of custody, and overcoming the hesitation of the judicial in using digital evidence.

- **Legal admissibility issues:-** Barriers that prevent digital evidence from being accepted in the court.
- **Chain of custody problems:-** Issues in maintaining the integrity of evidence from collection to court presentation.
- **Judicial reluctance:-** The reluctance of courts to accept digital forensic evidence due to a lack of legal precedents or technical understanding.

- **Revise criminal law:-** The need to update or introduce criminal law to explicitly address the admissibility and acceptance of digital forensic evidence in court.

Theme 2: Expertise and Training

This theme focuses on training and recruiting the required number and adequate level of expertise for law enforcement, forensic analysts, and legal professionals to properly handle digital forensic investigation.

- **Lack of forensic expertise:-** The shortage of skilled professionals capable of analyzing and utilizing digital artifacts.
- **Training for professionals:-** The need for practical training to improve digital forensic investigations task.
- **Launch educational campaigns:-** Raising awareness to the concerned bodies about digital forensics, its role in criminal investigations, and the importance of forensic artifacts as legal evidence.

Theme 3: Challenges in Investigations

This theme addresses the difficulties faced in conducting mobile forensic investigations, particularly in extracting and analyzing data.

- **Challenges in admissibility:-** Problems that arise when presenting digital forensic evidence in court, such as unclear regulations or technical limitations.
- **Investigation complexity:-** The process of retrieving, analyzing, and interpreting digital artifacts from digital devices.
- **Data integrity concerns:-** Challenges in proving that digital artifacts have not been altered.
- **Standardized forensic practices:-** The need for uniform procedures to ensure consistency in collecting and analyzing digital evidence.
- **Courts prefer eyewitness:-** Challenges due to courts prefer to use eyewitness rather than digital evidence.

- **Privacy issue:-** This refers to manipulation or accessing unnecessary data of the suspect by the forensic analyst during investigation.

Theme 4: Forensic Tools and Resources

This theme is about the financial and technological constraints impacting digital forensic investigations. It stresses the need for advanced tools and proper infrastructure to effectively analyze digital crime.

- **Insufficient resources:-** It is about limited funding and outdated infrastructure that hinder proper digital forensic investigations.
- **High costs:-** The expensive nature of advanced forensic tools and technologies required for recovering and analyzing digital artifacts.

Theme 5: Judicial Impact

This theme explores the impact of digital forensic evidence in securing a conviction or dismissal of criminal cases.

- **Digital forensic as evidence:-** The extent to which courts use digital forensic artifacts in legal proceedings.
- **Criminal case resolutions:-** The role of digital forensic evidence in securing a conviction or dismissal of criminal cases.

Chapter 6

6. Result and Discussion

6.1 Results

After locating the respective directory to look for possible artifacts from each ride application installed on the two phones, we were able to identify different artifacts. All of the artifacts identified are located in the **data/data/package name** directory. We were able to recover possible forensic artifacts such as passenger identity, driver identity, location information, device information and time of the ride service. The detailed analysis is explained below.

1. **Phone 1: Samsung Galaxy S8**

    - **Ride Application Analysis on Samsung S8**

      As can be seen from Figure 6.1, we were able to identify the passenger's phone number and user name from the Ride App installed on Samsung Galaxy S8. The identified information about the device can be seen in Figure 6.2. Location information such as trip starting, trip route and drop off location are identified as shown in Figure 6.3. The identified location information is expressed using waypoint and it is using some type of encoding. According to national geographic education definition, a waypoint serves as a point of reference for us to determine our current location and future destination.

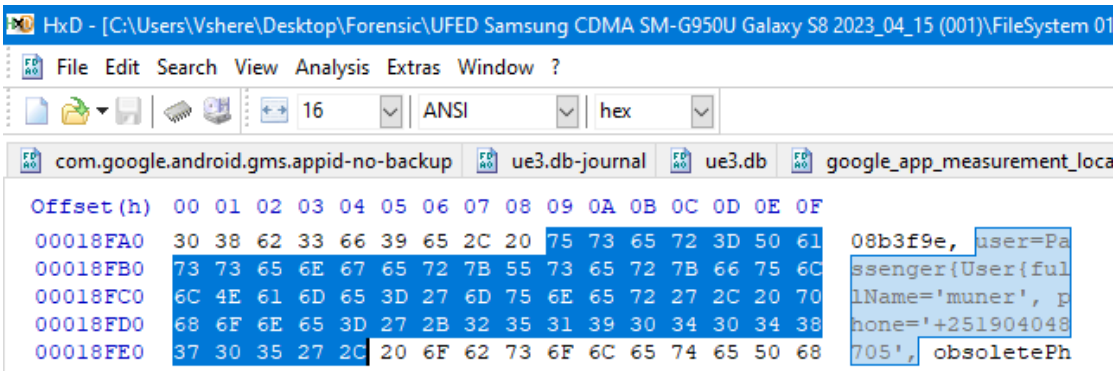


FIGURE 6.1: User profile from Ride/Samsung S8

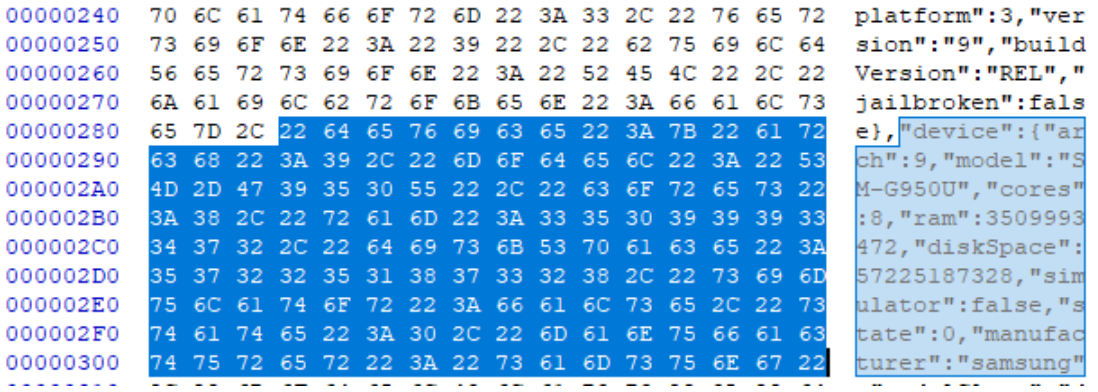


FIGURE 6.2: Device information from Ride/Samsung S8

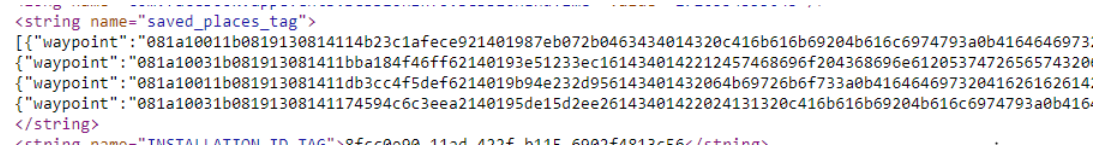


FIGURE 6.3: Trip information Ride/Samsung S8

Waypoints are helpful when we are flying, sailing, or driving[72].

As shown in Figure 6.3, there are four saved waypoints and decoding the first and last waypoints using an online tool called coder's tool[73] shows that they are the starting and destination point of the trip as shown in Figures 6.4 and 6.5 respectively.

The waypoint shown in Figure 6.3 also includes time information of the trip as 1718722633372 for the trip starting time and 1718725510714 for the time at trip destination which are in Unix epoch format. Converting this information into standard human readable time format using an online tool called epoch converter[74] reveals that the time and date of trip start was 5:57

FIGURE 6.4: Trip starting waypoint Ride on Samsung

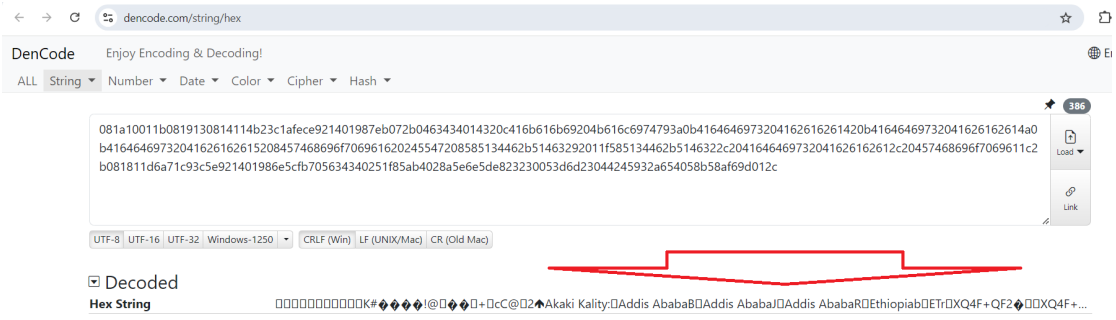


FIGURE 6.5: Trip destination waypoint Ride on Samsung

FIGURE 6.6: Time information at trip starting point Ride on Samsung

PM on Tuesday, June 18, 2024 while the time and date at trip destination was 6:45 PM on Tuesday, June 18, 2024 as shows in Figures 6.6 and 6.7.

Additionally, we were able to recover photograph of the passenger from different junk files inside one subdirectory all having no extension as shown in Figure 6.8. Examining all the files using a hex editor tool called HxD, we were able to understand that all the files were images files with different file format structures and saved them based on their format. The passenger junk file was a PNG file as shown in Figure 6.8. So we saved it using a .PNG

FIGURE 6.7: Time information at trip starting point Ride on Samsung

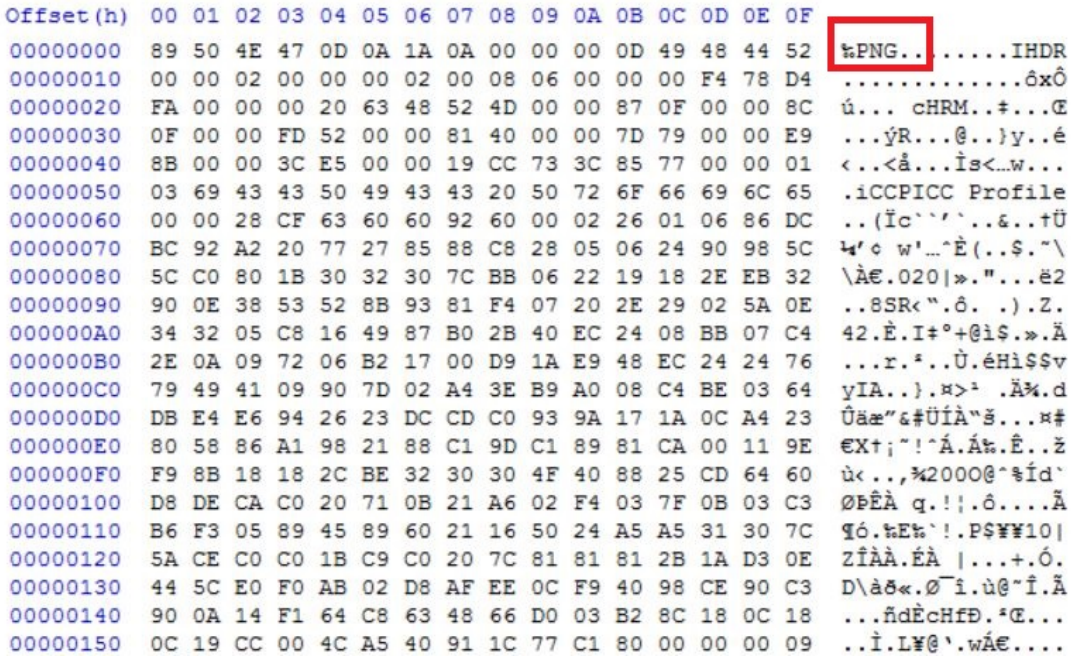


FIGURE 6.8: Retrieved photograph of the driver in hex format Ride/Samsung S8

extension and when parsing it with an image parser, we can see that it is the photograph of the driver as shown in Figure 6.8 and 6.9

- **Feres Application Analysis on Samsung S8**

Recovered forensic artifacts from Feres application include the following. As seen from Figure 6.10, user profile artifact was identified from the forensic image file.

FIGURE 6.9: Retrieved photograph of the driver on Ride/Samsung

```
<string name="first_name">M</string>
<string name="email">[redacted]m@gmail.com</string>
<int name="is_referral_apply" value="1"/>
<boolean name="is_promo_voucher_active" value="false"/>
<boolean name="user_emergency_help" value="true"/>
<boolean name="is_show_invoice" value="true"/>
<string name="frompage">OTHER</string>
<boolean name="autocomplete_switch_to_google" value="false"/>
<string name="fromwhere">SPLASH</string>
<string name="profile_pic">android.resource://com.feres.user/2131231048</string>
<string name="last_name"/>
<int name="provider_timeout" value="15"/>
<string name="mart_user_id">65febe24f3a766e59414c745</string>
<int name="autocomplete_map_from" value="1"/>
<boolean name="is_show_available" value="false"/>
<string name="city_currency">ETB</string>
<string name="device_token">cr7-lkafSAqGXvsDQ8VHAH:APA91bHIeZEqyVlZKaw9TbWMtngYtMOUh6r2FElwWxBGE-
6PPbAny6lkeOSycc3bbMDlox76fPWmfuctpHHGwn3N_tbzfcjTQ9GktFiITPf51PrO_Jw1_HoWaiCzkgVsVtwPBQDv65e6</string>
<string name="referral_code">904[redacted]05</string>
<int name="skip_destination" value="0"/>
```

FIGURE 6.10: User profile recovered from Feres/Samsung

```
00000230  76 69 63 65 22 3A 7B 22 61 72 63 68 22 3A 39 2C  vice":{"arch":9,
00000240  22 6D 6F 64 65 6C 22 3A 22 53 4D 2D 47 39 35 30  "model":"SM-G950
00000250  55 22 2C 22 63 6F 72 65 73 22 3A 38 2C 22 72 61  U","cores":8,"ra
00000260  6D 22 3A 33 35 30 39 39 39 33 34 37 32 2C 22 64  m":3509993472,"d
00000270  69 73 6B 53 70 61 63 65 22 3A 35 37 32 32 35 31  iskSpace":572251
00000280  38 37 33 32 38 2C 22 73 69 6D 75 6C 61 74 6F 72  87328,"simulator
00000290  22 3A 66 61 6C 73 65 2C 22 73 74 61 74 65 22 3A  ":false,"state":
000002A0  30 2C 22 6D 61 6E 75 66 61 63 74 75 72 65 72 22  0,"manufacturer"
000002B0  3A 22 73 61 6D 73 75 6E 67 22 2C 22 6D 6F 64 65  :"samsung","mode
000002C0  6C 43 6C 61 73 73 22 3A 22 64 72 65 61 6D 71 6C  lClass":"dreamql
000002D0  74 65 73 71 22 7D 2C 22 67 65 6E 65 72 61 74 6F  tesq"},"generato
000002E0  72 54 79 70 65 22 3A 33 7D 7D                    rType":3}}
```

FIGURE 6.11: Device information on Feres/Samsung

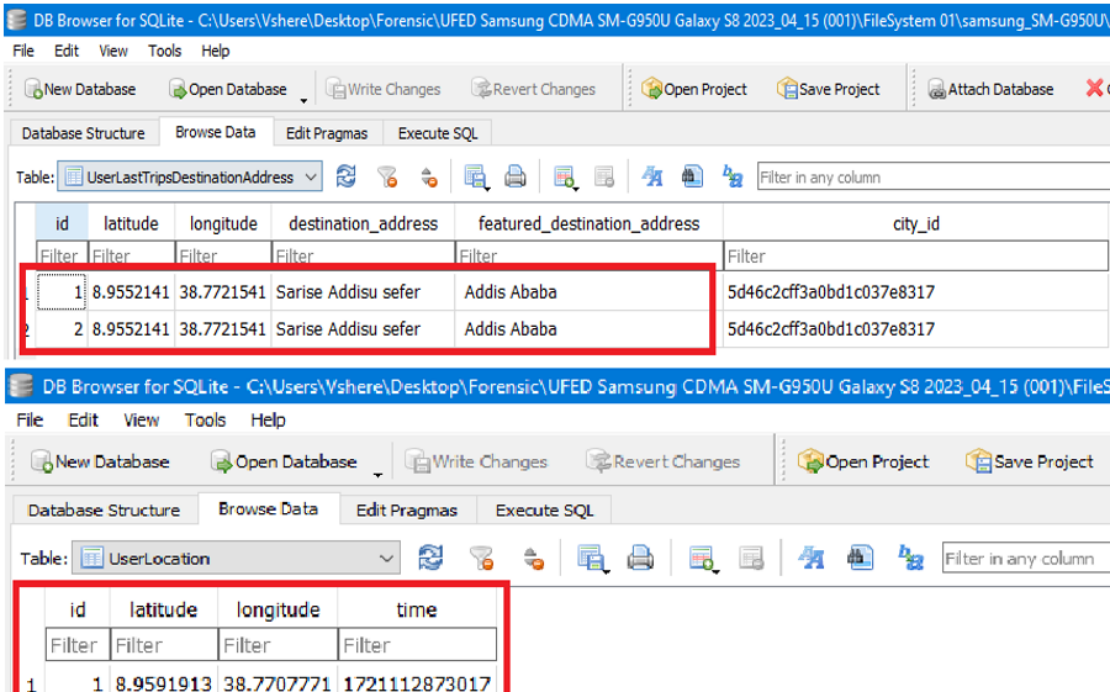


FIGURE 6.12: Destination location and time from Feres app on Samsung.

We were also able to identify device information from the extracted forensic image. As shown in Figure 6.11, device model and manufacturer of the device are SM-G950U and Samsung respectively.

The trip information can be seen on Figure 6.12. It contains the trip destination as "Saris Addisu Sefer" and its time during drop of as 1721112873017 which is in Unix epoch format. Converting it to standard human readable time format using epoch converter[74], it is 9:54 AM as shown in Figure 6.13. Another artifact identified from the Feres application is the driver's photograph. After identifying the photograph using a hex editor called HxD and

FIGURE 6.13: Time at trip destination from Feres app on Samsung

saved it with a .PNG extension, an image parser will be able to parse it simply as shown in Figure 6.14.

- **Zayride Application Analysis on Samsung S8**

  Similarly, we were able to retrieve valuable forensic artifacts from Zayride application. Passenger profile containing phone number and user name, and time of the trip were recovered as shown in Figure 6.15.

  Trip information such as starting point, destination point and fare amount can be seen from Figure 6.16.

  Figure 6.17 shows the device manufacturer name and the model of the device. Finally, we were also able to distinguish driver's photo from a set of junk files found inside the image of Samsung mobile as shown in Figure 6.18.

2. **Phone 2: Tecno**

   As we identified important forensic artifacts on the Samsung phone, we also found some interesting artifacts from the Tecno mobile phone. We will discuss them here.

   - **Ride Application Analysis on Tecno Mobile**

FIGURE 6.14: Driver photograph from Feres app on Samsung

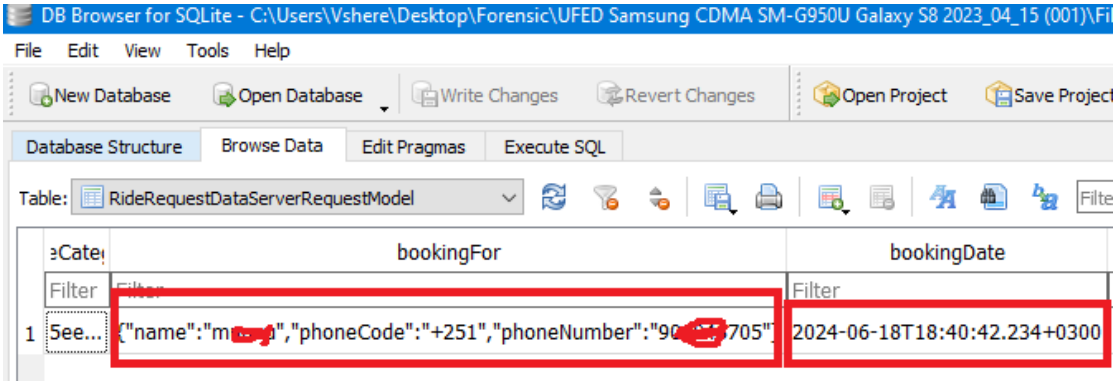


FIGURE 6.15: Passenger profile information from Zayride app on Samsung

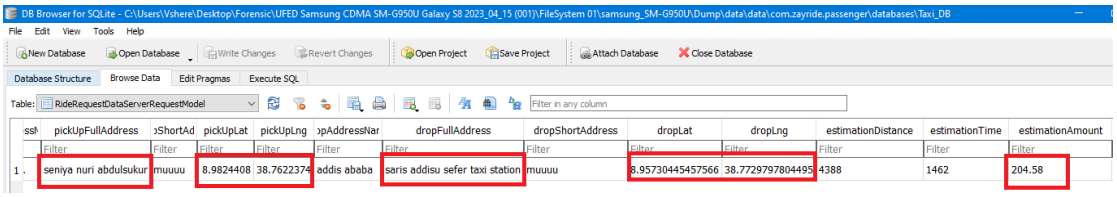


FIGURE 6.16: Trip information from Zayride app on Samsung.

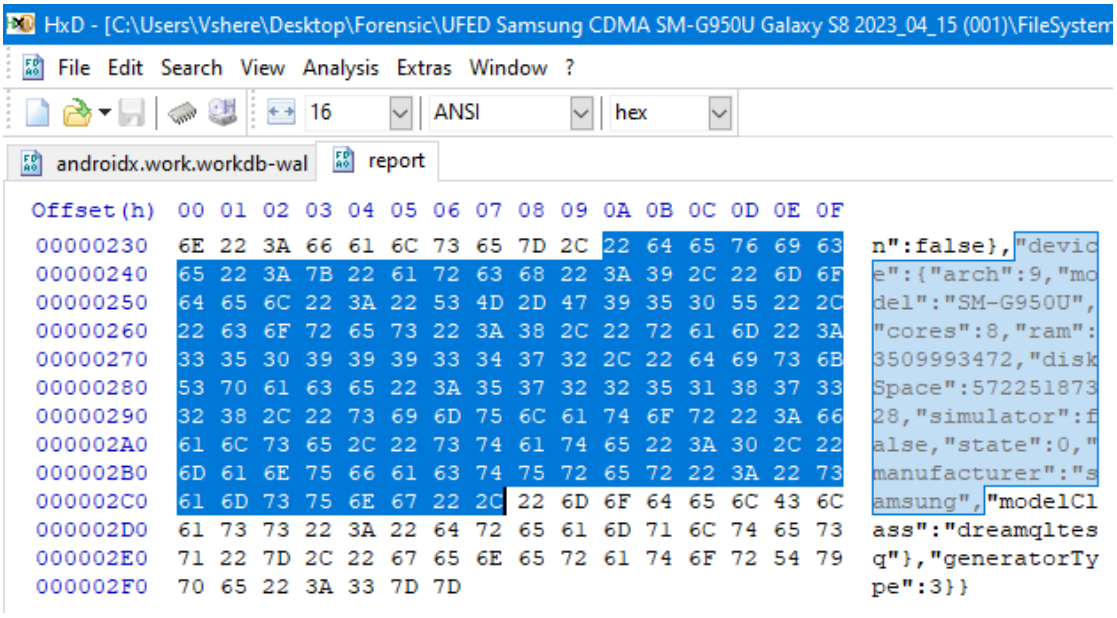


FIGURE 6.17: Device manufacturer and model Zayride app on Samsung

In this case we got a file named user log inside the forensic image file under the ride application package directory **"com.multibrains.taxi.passenger.ridepassengeret"**. Using this file, we got many artifacts. From the file, we were able to identify the driver name, phone number, license number, car model, plate number and registered address of the driver as shown in Figure 6.19.

We were also able to retrieve the driver's photograph from junk files after examining them using a hex editor. The identified driver's photograph is as shown in Figure 6.20.

Even though we retrieved many artifacts from the image file, we were unable to get passenger profile information. This doesn't mean there is no trace about passenger profile information. But, this may be due to different issues such as encryption, or in our case the trip was abruptly stopped in the middle of our trip by the driver for unknown reason. Thus, we were not simply

FIGURE 6.18: Photograph of driver from Zayride app on Samsung

able to retrieve those information.

Device information was retrieved showing the device model, operating system version and installed ride application version. In addition, trip start, trip destination and time information of the ride are identified. This information is shown in Figure 6.21.

- **Feres Application Analysis on Tecno Mobile**

  To identify artifacts as a result of Feres application on a forensic image extracted from Tecno Spark RC8, we used package name of the application

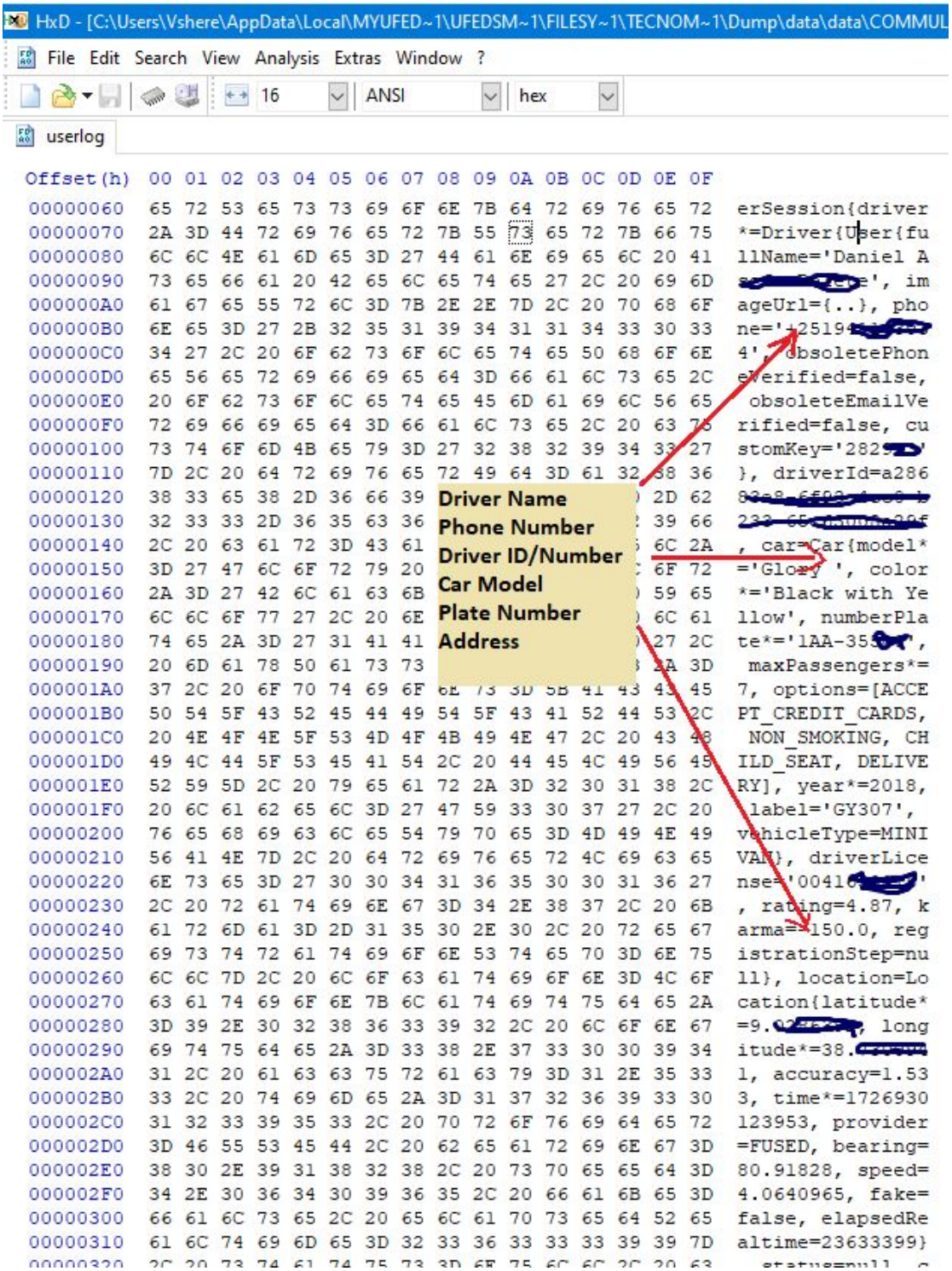


FIGURE 6.19: Driver information from Ride app on Tecno phone

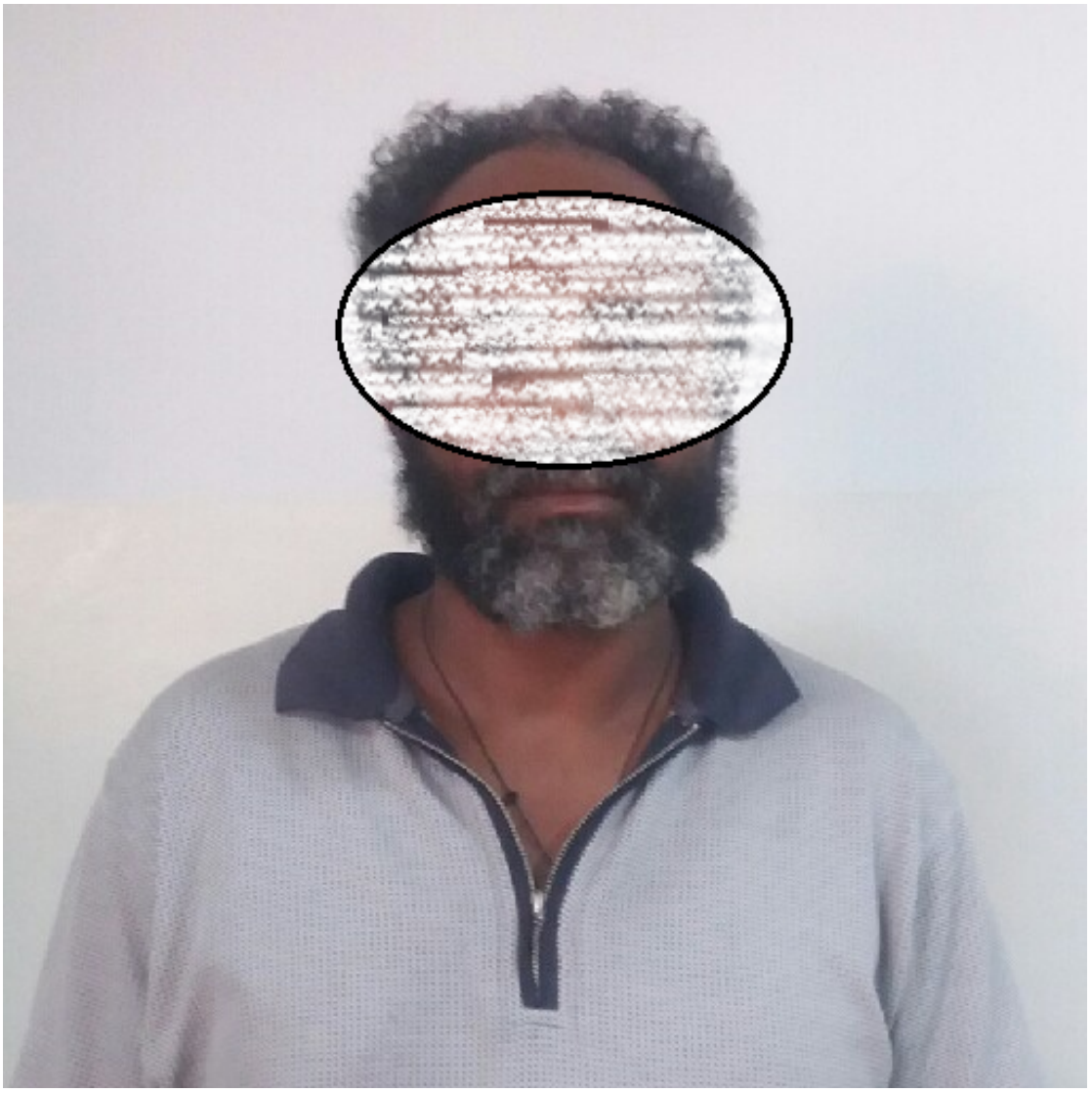


FIGURE 6.20: Driver photograph from Ride app on Tecno phone

which was identified earlier with the help **"App APK Extractor & Analyzer"**. For Feres application, the identified package name is **"com.feres.user"**. And thus, we analyzed every file under the directory **"com.feres.user"** in the image file. The identified artifacts are explained as follows:
Passenger profile information such as name. email address and phone number were identified as shown in Figure 6.22.

Another artifact identified from this forensic image is passenger device information indicating the manufacturer of the device and its model.This is shown in Figure 6.23.

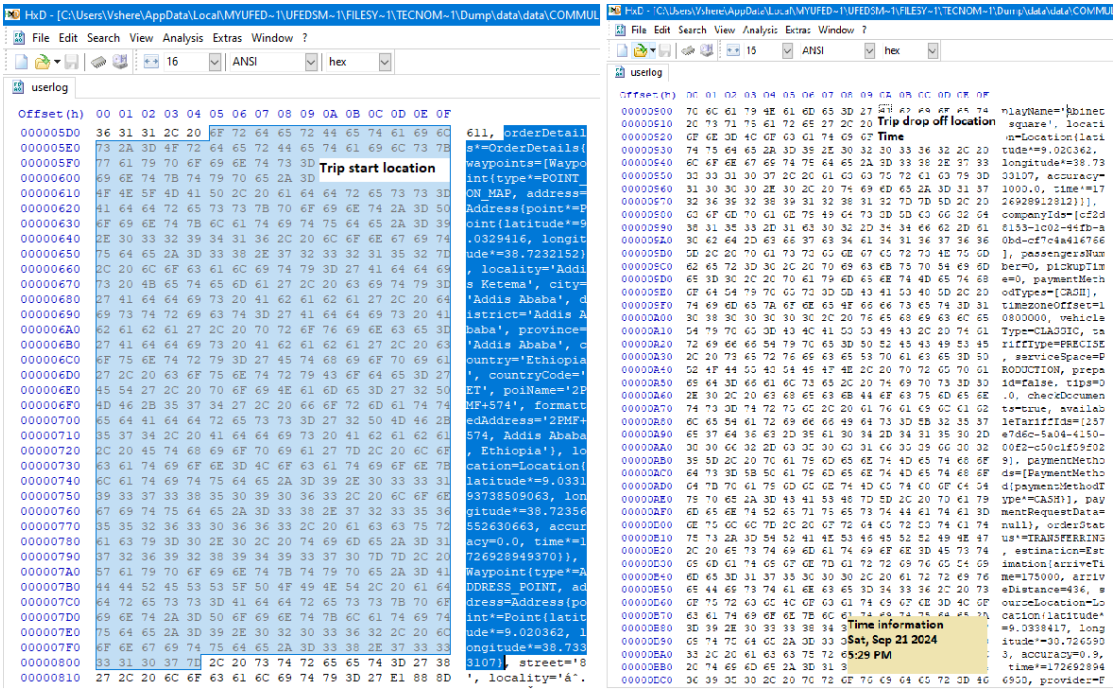


FIGURE 6.21: Trip information from Ride app on Tecno

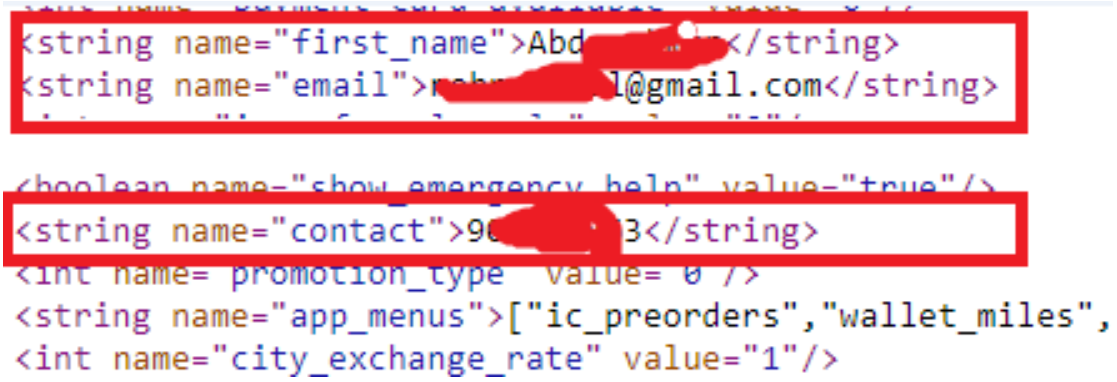


FIGURE 6.22: Passenger profile from Feres app on Tecno

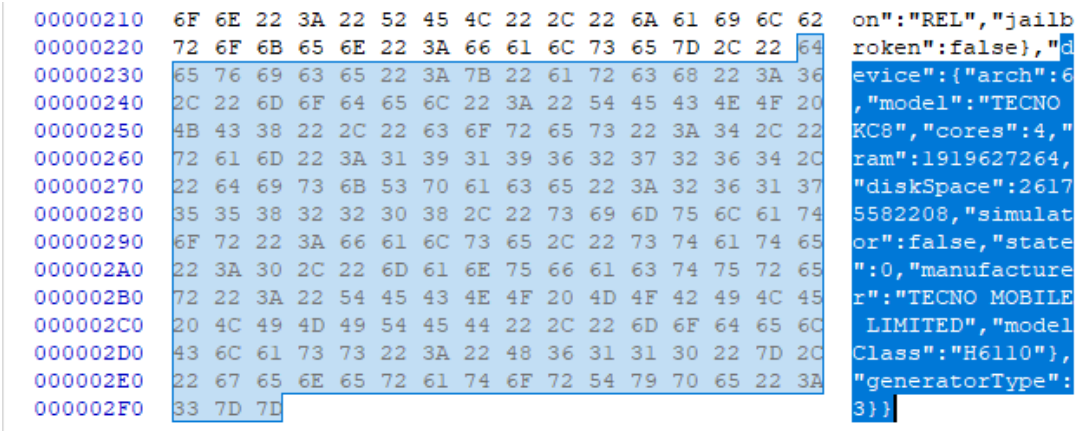


FIGURE 6.23: Passenger device information from Feres app on Tecno

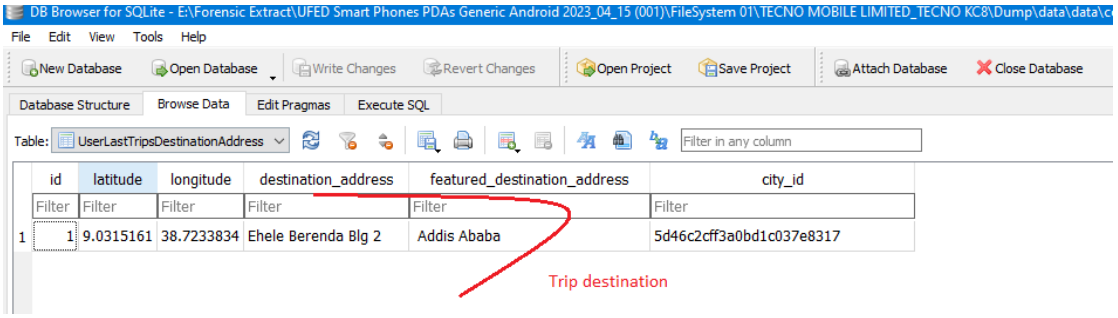


FIGURE 6.24: Passenger trip destination from Feres app on Tecno

Figure 6.24 shows passenger trip destination/ location retrieved from Feres application installed on Tecno Spark KC8.

Finally, as shown in Figure 6.25, we were able to recover photograph of the driver from junk files found in the forensic image extracted from Tecno device due to Feres application.

- **Zayride Application Analysis on Tecno Mobile**

  Using the package name of Zayride application which is **"com.zayride.passenger"**, we located its database directory. From this directory, were also able to identify some important artifacts. As shown in Figure 6.26, we identified passenger profile information and the time of ride taken place.

  As shown in Figure 6.27, device information such as model and manufacturer name are Tecno KC8 and Tecno respectively as identified from the forensic image.

  In Figure 6.28, the recovered information related to the trip taken place are shown.

  Finally, the photograph of the driver was recovered from junk files found in the image file by examining the files using a hex editor tool called HxD. The photograph recovered is shown in Figure 6.29.

FIGURE 6.25: Photograph of the driver from Feres app on Tecno

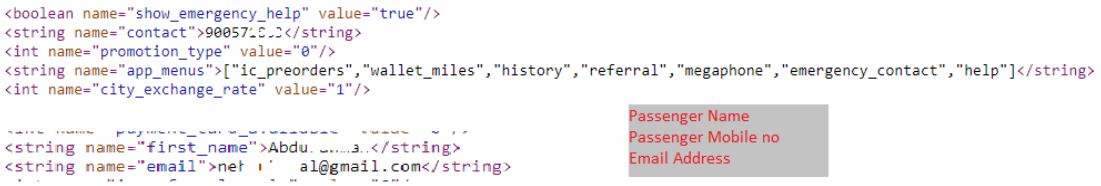


FIGURE 6.26: Passenger profile and time from Zayride app on Tecno

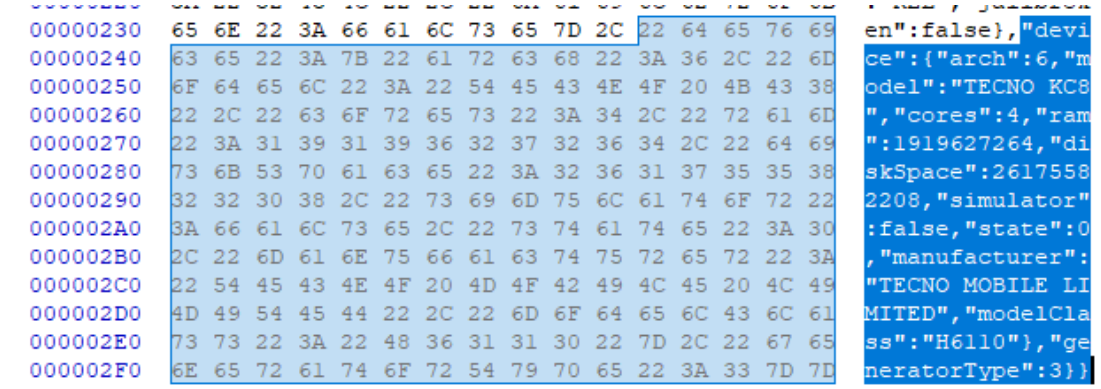


FIGURE 6.27: Device information identified from Zayride app on Tecno

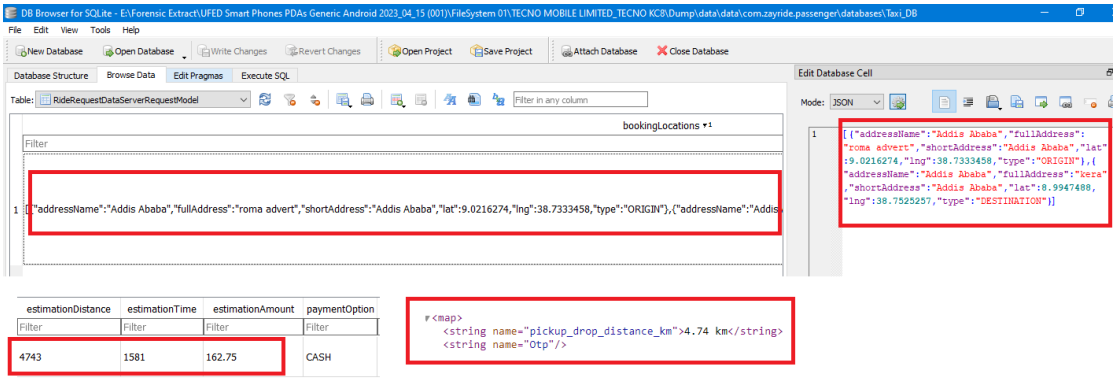


FIGURE 6.28: Trip information from Zayride app on Tecno

We have categorized all the codes generated from responses of the participants into five themes as shown in Table 5.2. Therefore, we were able to identify key factors that influence the use of digital forensic evidence such as artifacts recovered from mobile devices in the court. We have categorized the findings of this research under five major themes:

1. **Legal Admissibility**

   This refers to the ability of digital forensic artifacts to be legally accepted as evidence in the court. It includes challenges such as ensuring compliance with legal standards, maintaining a proper chain of custody, and overcoming the hesitation of the judicial in using digital evidence. The main points in this issue are:

   - The legal admissibility of digital forensic evidence remains uncertain due to unclear legal frameworks and the lack of established precedents in Ethiopia.
   - Judicial reluctance to accept digital forensic evidence is a major obstacle as courts often prefer traditional evidence such as eyewitness testimony.

FIGURE 6.29: Photograph of the passenger from Zayride app on Tecno

- Chain of custody problems arise due to weak procedures in handling and preserving digital evidence leading to concerns over evidence integrity.
- The need to revise the current criminal law was emphasized to ensure digital forensic artifacts are explicitly recognized and admissible in court.

2. **Expertise and Training**

   It focuses on training and recruiting the required number and adequate level of expertise for law enforcement, forensic analysts, and legal professionals to properly handle digital forensic investigation. The details for the generated codes are :

   - Shortage of trained professionals in digital forensic investigation and evidence handling hinders effective investigations.

- Inadequate training for professionals results in inconsistent forensic practices and difficulties in analyzing and using digital evidence.
- Educational campaigns are necessary to raise awareness among law enforcement officers, prosecutors, and judges about digital forensics and its role in criminal investigations.

3. **Challenges in Investigations**

   This outlines the difficulties faced while conducting digital forensic investigation particularly in extracting and analyzing artifacts.

   - Admissibility challenges arise due to unclear regulations making it difficult to present digital forensic evidence in court.
   - Highly complex investigation process due to difficulties in extracting and interpreting data from some digital devices such as Apple phones.
   - Data integrity concerns remain a significant issue as the investigation process involves separate parties without a common guideline to maintain the evidence has not been altered or tampered with.
   - Lack of standardized forensic practices leads to inconsistencies in digital forensic investigations.
   - Judicial preference of eyewitnesses over digital evidence weakens the role of digital forensic artifacts in court to close criminal cases.
   - Privacy concerns may arise when forensic professionals may access or manipulate the evidence during investigations.

4. **Forensic Tools and Resources**

   This explains the financial and technological constraints impacting digital forensic investigations. It stresses the need for advanced tools and proper infrastructure to effectively analyze digital crime.

   - Insufficient resources are a major challenge as the concerned departments in forensic investigation lack up-to-date technology and infrastructure.
   - The high cost of forensic tools hinders forensic analysts from acquiring advanced technologies needed for forensic investigations.

5. **Judicial Impact**

   This final result explores the level and role of digital forensic evidence in securing a conviction or dismissal of criminal cases in Ethiopia.

   - Digital forensic evidence usage in Ethiopia in helping to close court cases is increasing but its acceptance is inconsistent.
   - Criminal case resolutions rely on forensic evidence in some cases but its impact varies due to legal and technical challenges.

6.2 Discussion

6.2.1 Research Findings

Investigating forensic artifacts associated with Android ride-hailing applications, provides critical insights into the nature of digital evidence and its potential implications for legal contexts. Looking at the Figures from Figure 6.1 to 6.29, we were able to gather many artifacts from both devices relating to the three ride-hailing applications that were installed on each device.

The two research questions identified in this thesis document are:
RQ 1. What forensic artifacts can be effectively recovered from Ethiopian ride-hailing applications?
RQ 2. How can those recovered forensic artifacts be effectively used for court purpose?

Here, we will discuss the experiment findings related to passenger profile information, trip location information, driver information, trip time information, and passenger device information with respect to the two research questions.

1. **Passenger Profile Information**

   Ride-hailing applications investigated shows that detailed passenger profile information, which include username, phone number, email address, and ride history

information can be recovered as demonstrated in the results of the forensic investigation. These profiles are critical as they establish not only the passenger's identity but also their usage patterns within the application.

2. **Trip Location Information**

   Trip location information is one of the significant categories of forensic artifacts. The starting and ending locations, in addition to timestamps, provide a geographic footprint of passenger movements. Such information can be invaluable in the court to establish a denial or supporting evidence. The precision of GPS data may also allow the reconstruction of the trip, which can serve as crucial evidence in investigations related to criminal activity or disputes arising from ride services.

3. **Driver Information**

   Driver information, including driver identification and vehicle details, was also recovered during the experiment. This information is vital for accountability, particularly in passenger safety incidents during ride services. From a legal context, establishing the driver's identity can significantly influence the outcomes of criminal cases related to crimes or misconduct.

4. **Trip Time Information**

   The recorded trip time, including the trip duration, exact day, and time of the ride service contribute to the overall understanding of the dynamics of each ride. This information can play a pivotal role in assessing the fairness of the driver's actions during the ride, particularly in cases involving accusations of misconduct or the need to clarify the sequence of events.

5. **Passenger's Device Information**

   The identification of passenger's device information using the device manufacturer, model, operating system version, and installed application version can help to facilitate a court case against a passenger or a driver for crimes committed.

Research findings after analyzing responses of participants based on the questionnaire can be summarized as follows:

- Nowadays digital forensic evidence is increasingly used in Ethiopian legal cases, particularly in cybercrime. But it is still underutilized in general.

- Legal and procedural inconsistencies limit the effectiveness of digital forensic evidence in court with many cases challenging the its admissibility and preferring mainly eyewitness rather than considering the digital evidence.
- Lack of expertise among legal professionals and forensic analysts is another identified major barrier in the usage of digital forensic in the court.
- Resource constraints, time-intensive forensic processes, and legal admissibility issues are another key challenges identified.
- Using clear forensic standards, revising legal systems, and arranging better training are identified areas that need improvements.

6.2.2 Addressing Research Questions

RQ 1. What forensic artifacts can be effectively recovered from Ethiopian ride-hailing applications:
The experimental findings of this research indicates that the types of forensic artifacts available due to ride-hailing applications encompass a wide range of information categories. Passenger profiles, trip location data, driver information, trip timing, and device information can be foundational to constructing comprehensive evidence for the court. Each category of information serves individual investigative purposes and links to provide a holistic view of the events associated with ride services. This comprehensive understanding may be essential for forensic analysts in the assessment of evidence and for law enforcement agencies pursuing investigations. The identified artifacts are summarized as shown in Table 6.1.

RQ2 : How can those recovered forensic artifacts be effectively used for court purpose?

The potential use of those recovered artifacts in courts may have a significant effect in closing a criminal case. The digital footprint left by users of ride-hailing applications can reinforce or challenge testimonies, provide supporting evidence, and establish timelines that are critical in legal scenarios. For instance, GPS location data can validate or contradict passengers' claim regarding their whereabouts during a specific timeframe. Furthermore, the ability to trace rides' journey through application logs can assist in

No	Smartphone	Recovered Artifacts
1.	Samsung S8	• Passenger profile information (Name, Phone No, Email) • Passenger device information (Vendor, Model) • Location information (Trip Start, Destination) • Time Information (Trip Start, Destination Time) • Driver information (Photo)
2.	Tecno Spark 4	• Passenger profile information (Name, Phone No, Email) • Passenger device information (Vendor, Model, Version) • Location information (Trip Start, Destination, Distance) • Time Information (Trip Start, Destination Time • Driver information (Name, Phone No, Vehicle Model, Plate No, Address, Photo)

TABLE 6.1: Artifacts recovered from the two devices

clarifying the sequence of events leading up to an incident.

However, the admissibility of such evidence in court will depend on demonstrating the integrity and authenticity of the digital artifacts and other factors. Ensuring that the forensic process complies with established legal standards is another essential thing to maintain the probative value of the data collected.

Looking into our country's legislation system, we see that an important attention was given by the government by declaring a proclamation for it and giving INSA the mandate of the investigation task as we discussed in the literature review section[39]. This is not enough. We could not find any prepared standard (which helps to maintain admissibility of digital forensic evidence in the court) that is adopted by our country's law

enforcement agencies while working on this job and make it admissible in the court.

Additionally, based on our research findings from the questionnaire, 33.3% of the respondents replied they do not use any digital forensic standard or guideline to maintain the admissibility of their forensic evidence in the court as shown in Figure 5.4. Also looking into the type of standard or guideline used by the participants who say the use a specific digital forensic standard or guideline to maintain the admissibility of their forensic evidence in the court, it varies with the majorities replying they use ISO/IEC while some replying they use Interpol guideline and others. This shows that there is a lack of uniformity among the LEA of this country while working on digital forensic investigation.

The valuable digital evidence we were able to get from ride-hailing applications such as passenger profiles, trip location data, driver information, trip timing, and device information that are crucial to close criminal cases involving ride related cases such as murder and theft would become void or weak or further widen the gap of judicial reluctance to accept digital evidence in this highly digital world involving complicated digital crimes[75].

Whereas looking into chapter thirty-three, article two of the Ethiopian computer crime proclamation No.958/2016, it states that evidence obtained based on the criminal procedure code, related regulations or any computer evidence generated based on the proclamation or gained from relevant overseas law enforcement agencies with respect to the country's regulation may be accepted in the courtroom associated with digital offenses[39].

A digital evidence has to be precise, genuine and complete to be admissible in the court[76]. M. Grobler stated that to regulate the usage and implementation of digital forensic procedures, a recognized standard must be established and upheld[77]. Common standards such as ISO/IEC provide investigative guidelines in a variety of investigations such as digital evidence[78]. Looking at the above four paragraphs, to effectively use digital evidences from ride-hailing applications in Ethiopian courts, a standard or guideline is needed for all concerned LEA parties that they should adopt it to maintain the

admissibility of digital evidences in the court.

But this is also not enough. All the findings of this research should be addressed for the effective use of digital evidence in Ethiopian courts. Overall, considering the increasing and complex nature of digital crimes, Ethiopia should address the following findings of this research for effective use of forensic evidence from ride-hailing applications in particular and any digital forensic evidence in general:

- Ensure digital forensic evidence to be used in Ethiopian courts by revising the current criminal law to address the issues of legal admissibility and judicial reluctance of digital evidence.
- Adopt one of the well-known world standards such as INTERPOL or ISO/IEC or develop own standard to maintain integrity related issues throughout the investigation process.
- Enhance the digital forensic infrastructure by building up-to-date digital forensic laboratory, allocate adequate and capable expertise for the LEA in this area and train them.

6.2.3 Implication of Artifacts

If the process involved throughout the forensic investigation and analysis in identifying important artifacts to the process of criminal case closing was based on the recommendations of this research based on its findings, identification of those artifacts listed in Table 6.1 are invaluable to establish denials or supporting evidences.

Suppose one case involving a crime involving ride-hailing service. If a passenger had murdered the driver of the car while using a ride service in Addis Ababa and he immediately changed his location to Hawassa. After the passenger became suspected and detained after some time interval, and the prosecutor got many supporting evidences against him but the criminal passenger defended by repeatedly saying he was out of

Addis Ababa during the day of murdering, he may be acquitted due to lack of sufficient evidence against him.

Think of what would be the verdict if the prosecutor was supported by evidences using forensic investigation of the passenger's phone and got every information we discussed earlier such as passenger profile information (name, phone no, email), passenger device information (vendor, model), location information(trip start, destination), time information(date and time of ride taken, trip start and destination time) and driver information (photo, phone no, vehicle model, plate no, address) from a forensic expert.

To have better understanding in the issue, a real criminal case using location data recovered from the device of the criminal was published by the America's National Institute of Justice by researchers Goodison et al.[35] is discussed below.

Goodison et al. explored that in September 2012, the disappearance of Christian Aguilar - a freshman at the University of Florida - accelerated a significant investigation following his last sighting with Pedro Bravo - his close friend - at a Best Buy store in their locality. Nearly three weeks subsequent to his disappearance, Aguilar's remains were discovered over 60 miles west of the initial location, buried in a shallow grave. The investigation swiftly turned its focus towards Bravo, especially after the discovery of Aguilar's blood in Bravo's vehicle and Aguilar's backpack in Bravo's possession. Both of them studied at the same high school and it was speculated that Bravo's motives may have been fueled by jealousy and betrayal, because of Aguilar's relationship with ex-girlfriend of Bravo. The case, initially reliant on circumstantial evidence, was significantly strengthened through the analysis of digital artifacts. Forensic examiners investigated Bravo's mobile device uncovering compelling evidence within the data cache of the phone's Facebook application. Notably, a screenshot captured a query to Siri, made around the time of Aguilar's disappearance, stating, "I need to hide my roommate." Although Bravo's device was not equipped with the Siri functionality, the inquiry was recorded due to his use of Facebook to access the feature. Further analysis of the cell phone's location data, through the examination of signal pings to cell towers, evidenced Bravo's westward movement post-disappearance. In addition to that, the flashlight application on

Bravo's phone was activated for an extended period of time exceeding one hour shortly after Aguilar was last seen. This convergence of digital evidence played a pivotal role in the legal proceedings that ensued, leading to Bravo's trial in August 2014. As a result, Bravo was convicted of first-degree murder. This underscored a profound impact to the digital forensic analysis by resolving issues leading to Aguilar's death[35].

6.2.4 Evaluating the Framework

We evaluated the framework using the criteria reliability, efficacy and cost-effectiveness to evaluate its effectiveness.

1. Efficacy

The efficacy of the framework was evaluated by the degree to which the framework was able to achieve the intended goal of recovering artifacts from ride-hailing applications. Looking at the recovered artifacts by this framework and the research by K.Kiptoo[13], we were able to recover the following artifacts which were among the aims of this research:

- Passenger profile information (Name, Phone No, Email)
- Passenger device information (Vendor, Model, Version)
- Location information (Trip Start, Destination, Distance)
- Time Information (Trip Start, Destination Time
- Driver information (Name, Phone No, Vehicle Model, Plate No, Address, Photo)

This shows the framework satisfies the criteria of efficacy.

2. Reliability

To evaluate its reliability, we compared artifacts obtained from using this forensic investigation framework with the information found on the device that are easily accessible like profile setup, device setting and screenshots taken during riding.

- **Passenger Profile Information**

  Figure 6.30 shows that screenshot of the user profile from Feres application installed on Tecno phone and the forensically recovered user profile due to the same application that was installed on the same device are similar.

- **Device Information**

  Figure 6.31 shows that screenshot of the device information on Samsung phone on which Feres application was installed and the forensically recovered device information from the same application that was installed on the same device are identical.

- **Location Information**

  From Figure 6.32, we can see that location information from screenshot while taking Zayride application is matching with location information recovered using forensic recovery.

  Looking at all those three samples, we can see that the reliability criteria is satisfied.

3. Cost-effectiveness

This framework is more cost-effective than the forensic framework proposed by K.Kiptoo[13] as it avoids the unnecessary phase of rooting that was made compulsory by the researcher. This is because of:

- Rooting may result in bricking the devices which results in loss of the device and data.
- Since there are tools or devices that are able to image devices without rooting them, adopting that framework may result in investing more time while doing unnecessary device rooting.

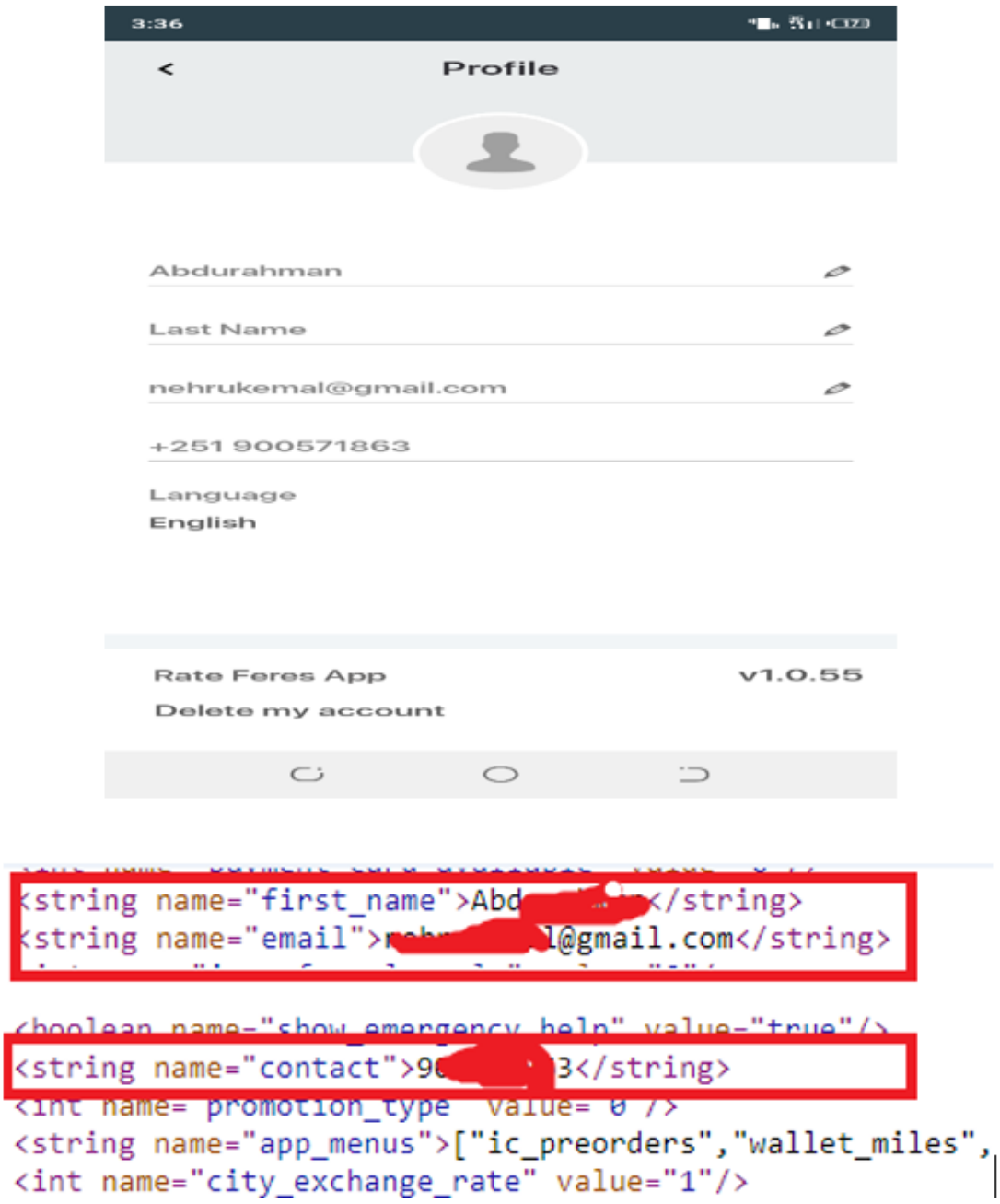
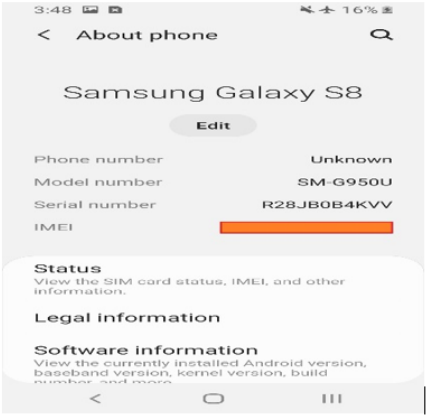


FIGURE 6.30: Screenshot from Tecno for Feres versus the recovered user profile




```
00000230  76 69 63 65 22 3A 7B 22 61 72 63 68 22 3A 39 2C   vice":{"arch":9,
00000240  22 6D 6F 64 65 6C 22 3A 22 53 4D 2D 47 39 35 30   "model":"SM-G950
00000250  55 22 2C 22 63 6F 72 65 73 22 3A 38 2C 22 72 61   U","cores":8,"ra
00000260  6D 22 3A 33 35 30 39 39 39 33 34 37 32 2C 22 64   m":3509993472,"d
00000270  69 73 6B 53 70 61 63 65 22 3A 35 37 32 32 35 31   iskSpace":572251
00000280  38 37 33 32 38 2C 22 73 69 6D 75 6C 61 74 6F 72   87328,"simulator
00000290  22 3A 66 61 6C 73 65 2C 22 73 74 61 74 65 22 3A   ":false,"state":
000002A0  30 2C 22 6D 61 6E 75 66 61 63 74 75 72 65 72 22   0,"manufacturer"
000002B0  3A 22 73 61 6D 73 75 6E 67 22 2C 22 6D 6F 64 65   :"samsung","mode
000002C0  6C 43 6C 61 73 73 22 3A 22 64 72 65 61 6D 71 6C   lClass":"dreamql
000002D0  74 65 73 71 22 7D 2C 22 67 65 6E 65 72 61 74 6F   tesq"},"generato
000002E0  72 54 79 70 65 22 3A 33 7D 7D                     rType":3}}
```

FIGURE 6.31: Device information from the device and recovered from Feres application

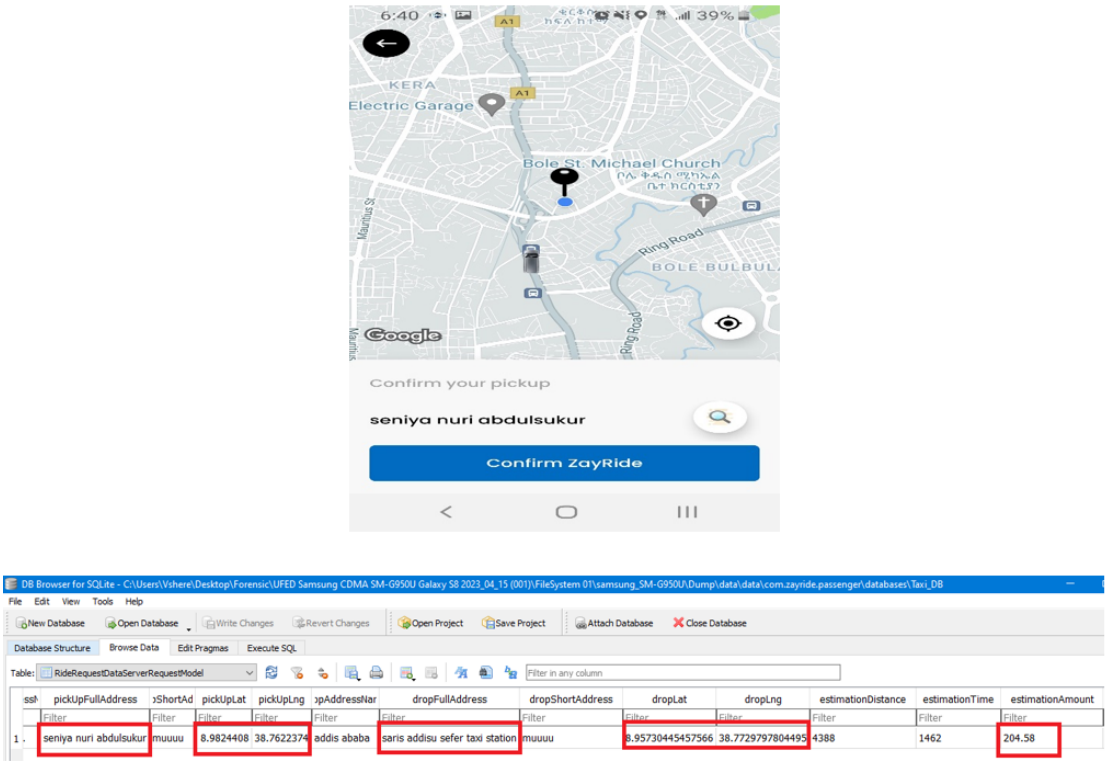


FIGURE 6.32: Location from screenshot versus recovered one from Zayride application

Chapter 7

7. Summary and Future Work

In this research, we presented our proposed framework for identifying forensic artifacts from ride-hailing Android applications to enhance the existing forensic framework proposed by K.Kiptoo[13] due to the increasing reliance on mobile applications giving transportation services in this country. We went through a comprehensive experimentation using three ride-hailing applications each installed on two mobile devices, after investigating their popularity by looking at their market share in this country.

We used ride services using both mobile phones, on which all three ride applications were installed to acquire enough artifacts and thus, forensically investigate each device based on the proposed framework.

We used various tools including **"App APK Extractor & Analyzer"** to identify package name of the APKs' and the well-known UFED Cellebrite to extract the forensic image from the devices. Whereas the tools SQL DB browser, HxD, Notepad++, MS Edge browser and MS paint are used to facilitate the analysis of forensically acquired image.

Our findings demonstrated the effectiveness of the proposed framework in recovering a variety of relevant artifacts, including passenger profile information (such as names, phone numbers, and email addresses), device information (vendor and model), location

data (trip start and destination), time details (date and time of the ride), and driver information (photo, phone number, vehicle model, plate number, and address).

Despite the positive outcomes of this research, we acknowledge a significant challenge for this country in digital forensics: while a legislative proclamation gives a responsible body to do a forensic investigation, there remains a lack of standardized protocols to ensure that recovered artifacts are admissible in court. This gap poses a potential barrier to the practical application of digital forensic findings in legal contexts, emphasizing the need for the development of clear guidelines and standards within the field.

We also investigated the role, level and challenges of usage of digital evidence in this country by the LEAs after distributing a questionnaire specifically designed to professionals in those organizations and identified the following issues legal and procedural inconsistencies limit the effectiveness of digital forensic evidence in court, there is a lack of expertise among legal professionals and forensic analysts, resource constraints and lack of capable expertise, and legal admissibility issues, inconsistency in usage of forensic standards among LEAs, challenges on digital evidence admissibility and preference of eyewitness over digital evidence.

Based on the findings of this research, we recommend that, this country should address the issues identified in this research for effective use of forensic evidence from ride-hailing applications in particular and any digital forensic evidence in general. These include revise the current criminal law to address the issues of legal admissibility and judicial reluctance of digital evidence, adopt or develop a standards to maintain integrity of the evidence, build up-to-date digital forensic laboratory, allocate adequate and capable expertise.

In summary, this research contributes valuable insights by identifying, and recovering forensic artifacts from ride-hailing applications and discovering the challenges of using digital forensic evidence in the Ethiopian court and then highlighting recommendations for those challenges. Future work should focus on identifying artifacts that can be recovered from the cloud using forensic investigation. Nowadays, since applications

are managing their data on the cloud, having a forensic investigation due to those applications on the cloud will help law enforcement agencies, as we explained for the on premise application.

References

[1] Ethiopia's digital economy - cepheus growth capital, 2019. URL https://cepheuscapital.com/wp-content/uploads/2019/01/Ethiopias-Digital-Economy.pdf. Accessed on : 2023-02-08.

[2] Ethiopia's ride-hailing startups face their toughest opponents: each other - rest of world, 2023. URL https://restofworld.org/2022/ethiopias-ride-hailing-wars-spill-into-court-with-copyrightclaims-and-trademark-disputes. Accessed on : 2023-02-08.

[3] Ride-hailing companies proliferate, gov't remains incognizant, 2023. URL https://addisfortune.news/ride-hailing-companies-proliferate-govt-remains-incognizant/. Accessed on : 2023-02-08.

[4] Qingchuan Zhao, Chaoshun Zuo, Giancarlo Pellegrino, and Zhiqiang Lin. Geo-locating Drivers: A Study of Sensitive Data Leakage in Ride-Hailing Services. "", (February), 2019. doi: 10.14722/ndss.2019.23052.

[5] Analysis: Risking it all to make ends meet: Stories of killings, theft in addis terrify private transport providers - addis standard, 2023. URL https://addisstandard.com/analysis-risking-it-all-to-make-ends-meet-stories-of-killings-theft-in-addis-terrify-private-transport-providers/. Accessed on : 2023-02-08.

[6] Addis ababa police ride-hailing crime (report on facebook), 2023. URL https://www.facebook.com/Addisababapolice/posts/pfbid02vheQm89kYuviuZF6wdVh2rm1gvbL3A2KLcTGnuEN5gHxrsNM11Xd2v2cnnVpLwrl. Accessed on : 2023-02-08.

[7] Nghi Hoang Khoa, Phan The Duy, Hien Do Hoang, Do Thi Thu Hien, and Van Hau Pham. Forensic analysis of TikTok application to seek digital artifacts on Android

smartphone. *Proceedings - 2020 RIVF International Conference on Computing and Communication Technologies, RIVF 2020*, 2020. doi: 10.1109/RIVF48685.2020.9140739.

[8] Patrício Domingues, Rúben Nogueira, José Francisco, and Miguel Frade. Post-mortem digital forensic artifacts of tiktok android app. pages 1–8, 08 2020. doi: 10.1145/3407023.3409203.

[9] Khushboo Rathi, Umit Karabiyik, Temilola Aderibigbe, and Hongmei Chi. Forensic analysis of encrypted instant messaging applications on Android. *6th International Symposium on Digital Forensic and Security, ISDFS 2018 - Proceeding*, 2018-Janua: 1–6, 2018. doi: 10.1109/ISDFS.2018.8355344.

[10] Oluwafemi Osho, Uthman L. Mohammed, Nanfa N. Nimzing, Andrew A. Uduimoh, and Sanjay Misra. *Forensic Analysis of Mobile Banking Apps*, volume 11623 LNCS. Springer International Publishing, 2019. ISBN 9783030243074. doi: 10.1007/978-3-030-24308-1_49. URL http://dx.doi.org/10.1007/978-3-030-24308-1_49.

[11] Rajchada Chanajitt, Wantanee Viriyasitavat, and Kim-Kwang Raymond Choo. Forensic analysis and security assessment of android m-banking apps. *Australian Journal of Forensic Sciences*, 50:1–17, 05 2016. doi: 10.1080/00450618.2016.1182589.

[12] Majid ALThebaity, Shailendra Mishra, and Manoj Kumar Shukla. Forensic Analysis of Third-party Mobile Application. *Helix*, 10(4):32–38, 2020. ISSN 22773495. doi: 10.29042/2020-10-4-32-38.

[13] KEVIN KIBIWOTT KIPTOO. A forensic investigation framework for android on-demand ride applications, 2020. URL https://erepo.usiu.ac.ke/bitstream/handle/11732/6746/Kiptoo%20Kevin%20Kibiwott%20MIST%202020.pdf?sequence=1&isAllowed=y. Accessed on : 2023-06-22.

[14] Digital Forensics in Cyber Security - GeeksforGeeks — geeksforgeeks.org. https://www.geeksforgeeks.org/digital-forensics-in-cyber-security/. [Accessed 26-10-2024].

[15] Mohammed Moreb. *Practical Forensic Analysis of Artifacts on iOS and Android Devices: Investigating Complex Mobile Devices*. Apress, 01 2022. ISBN 978-1-4842-8025-6. doi: 10.1007/978-1-4842-8026-3.

[16] Forensic Science — nist.gov. https://www.nist.gov/forensic-science. [Accessed 24-10-2024].

[17] Forensic Science. https://pubs.acs.org/doi/10.1021/ac050682e. [Accessed 24-10-2024].

[18] The use of forensic science in volume crime investigations. https://assets.publishing.service.gov.uk/media/5a7ad567e5274a34770e76f6/hoor4305.pdf. [Accessed 24-10-2024].

[19] K. Kent. S. Chevalier. T. Grance. and H. Dang. Special publication 800-86 guide to integrating forensic techniques into incident response recommendations of the national institute of standards and technology, 2006. URL https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf. Accessed on : 2024-10-10.

[20] What is digital forensics — phases of digital forensics. https://www.eccouncil.org/cybersecurityexchange/computer-forensics/what-is-digital-forensics/. [Accessed 24-10-2024].

[21] David Lillis, Brett Becker, Tadhg O'Sullivan, and Mark Scanlon. Current challenges and future research areas for digital forensic investigation. 05 2016. doi: 10.48550/arXiv.1604.03850.

[22] What is mobile device forensics: Benefits, process & challenges. https://www.eccouncil.org/cybersecurityexchange/computer-forensics/mobile-device-forensics/. [Accessed 24-10-2024].

[23] Konstantia Barmpatsalou, Tiago Cruz, Paulo Simoes, and Edmundo Monteiro. Mobile forensic data analysis: Suspicious pattern detection in mobile evidence. *IEEE Access*, 10 2018. doi: 10.1109/ACCESS.2018.2875068.

[24] Mobile device forensics archives. https://cellebrite.com/en/digitalforensics/mobile-device-forensics/. [Accessed 24-10-2024].

[25] Data acquisition in mobile forensics: The critical process to collect mobile evidence. https://www.salvationdata.com/knowledge/data-acquisition-in-mobile-forensics/. [Accessed 24-10-2024].

[26] Android 15 is released to AOSP — android-developers.googleblog.com. https://android-developers.googleblog.com/2024/09/android-15-is-released-to-aosp.html. [Accessed 24-10-2024].

[27] Secure an Android device — Android Open Source Project — source.android.com. https://source.android.com/docs/security/overview. [Accessed 24-10-2024].

[28] What is Android OS? — Definition from TechTarget — techtarget.com. https://www.techtarget.com/searchmobilecomputing/definition/Android-OS. [Accessed 24-10-2024].

[29] Android Operating System (OS): Definition and How It Works — investopedia.com. https://www.investopedia.com/terms/a/android-operating-system.asp. [Accessed 24-10-2024].

[30] A Comprehensive Guide To Crime Scene Investigation — financialcrimeacademy.org. https://financialcrimeacademy.org/what-is-forensic-investigation/. [Accessed 24-10-2024].

[31] Digital forensics — interpol.int. https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics. [Accessed 24-10-2024].

[32] Malek Harbawi and Asaf Varol. The role of digital forensics in combating cybercrimes. pages 138–142, 04 2016. doi: 10.1109/ISDFS.2016.7473532.

[33] Jigang Liu, Tetsutaro Uehara, and Ryoichi Sasaki. Development of digital forensics practice and research in japan. *Wireless Communications and Mobile Computing*, 11:240–253, 02 2011. doi: 10.1002/wcm.981.

[34] Malek Harbawi and Asaf Varol. Cybercrime legislation in the united states. pages 257–280, 2020. doi: https://doi.org/10.1007/978-3-319-78440-3_3.

[35] Digital evidence and the u.s. criminal justice system identifying technology and other needs to more effectively acquire and utilize digital evidence. https://www.ojp.gov/pdffiles1/nij/grants/248770.pdf, 2015. [Accessed 15-10-2024].

[36] Harjinder Lallie. An overview of the digital forensic investigation infrastructure of india. *Digital Investigation*, 9:3–7, 06 2012. doi: 10.1016/j.diin.2012.02.002.

[37] Richard Apau and Felix Koranteng. An overview of the digital forensic investigation infrastructure of ghana. *Forensic Science International: Synergy*, 2:299–309, 10 2020. doi: 10.1016/j.fsisyn.2020.10.002.

[38] Efp - proclamation. https://www.federalpolice.gov.et/en/federal/police/document/proclamation. [Accessed 24-10-2024].

[39] - insa. https://insa.gov.et/web/guest/%E1%88%B0%E1%8A%90%E1%8B%B6%E1%89%BD(. [Accessed 24-10-2024].

[40] Behaylu Desta. Forensic science evidence under ethiopian criminal justice system: -the case of homicide in addis ababa. https://www.academia.edu/42005735/FORENSIC_SCIENCE_EVIDENCE_UNDER_ETHIOPIAN_CRIMINAL_JUSTICE_SYSTEM_The_Case_of_Homicide_in_Addis_Ababa, . [Accessed 24-10-2024].

[41] Behaylu Desta. Mapping of the emerging digital forensic technologies for crime investigations in ethiopia: A call for nation security,safety and sustainability. https://www.questjournals.org/jrhss/papers/vol3-issue6/H364246.pdf, . [Accessed 24-10-2024].

[42] Hyungchan Kim, Yeonghun Shin, Sungbum Kim, Wooyeon Jo, Minju Kim, and Taeshik Shon. Digital forensic analysis to improve user privacy on android. *Sensors*, 22:3971, 05 2022. doi: 10.3390/s22113971.

[43] Jason Bays and Umit Karabiyik. Forensic Analysis of Third Party Location Applications in Android and iOS. *INFOCOM 2019 - IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS 2019*, 2019-Janua(June), 2019.

[44] Rahul Sinha, Vikas Sihag, Gaurav Choudhary, Manu Vardhan, and Pradeep Singh. Forensic Analysis of Fitness Applications on Android. *Communications in Computer and Information Science*, 1544 CCIS(October):222–235, 2022. ISSN 18650937. doi: 10.1007/978-981-16-9576-6_16.

[45] Fahad Salamh, Mohammad Mirza, Shinelle Hutchinson, Yung Yoon, and Umit Karabiyik. What's on the horizon? an in-depth forensic analysis of android and ios applications. *IEEE Access*, PP:1–1, 07 2021. doi: 10.1109/ACCESS.2021.3095562.

[46] Hao. Zhang, Lei Chen, and Qingzhong Liu. Digital Forensic Analysis of Instant Messaging Applications on Android Smartphones. *IEEE Access*, pages 647–651, 2018. doi: 10.1109/ICCNC.2018.8390330.

[47] Imam Riadi. Examination of Digital Evidence on Android-based LINE Messenger. *International Journal of Cyber-Security and Digital Forensics*, 7(3):336–343, 2018. ISSN 2305-0012. doi: 10.17781/p002472.

[48] Farid Daryabar, Ali Dehghantanha, Brett Eterovic-Soric, and Kim-Kwang Raymond Choo. Forensic investigation of onedrive, box, googledrive and dropbox applications on android and ios devices. *Australian Journal of Forensic Sciences*, 48: 1–28, 03 2016. doi: 10.1080/00450618.2015.1110620.

[49] Andrew Uduimoh, Ismaila Idris, Oluwafemi Osho, and Shafi'i Abdulhamid. Forensic analysis of mobile banking applications in nigeria. *i-manager's Journal on Mobile Applications and Technologies*, 6:9–20, 06 2019. doi: 10.26634/jmt.6.1.15704.

[50] Umit Karabiyik. Digital Forensics for Mobility as A Service Platform: Analysis of Uber Application on iPhone and Cloud — commons.erau.edu. https://commons.erau.edu/adfsl/2022/presentations/5/. [Accessed 24-10-2024].

[51] Theodoula Ioanna Kitsaki, Anna Angelogianni, Christoforos Ntantogian, and Christos Xenakis. A forensic investigation of android mobile applications. *ACM International Conference Proceeding Series*, pages 58–63, 2018. doi: 10.1145/3291533.3291573.

[52] Thi Pham, Italo Petrocelli, Bastien Jacot-Guillarmod, Kévin Huguenin, Taha Hajar, Florian Tramer, and Jean-Pierre Hubaux. Privateride: A privacy-preserving and secure ride-hailing service. 01 2016.

[53] Sen Chen, Ting Su, Lingling Fan, Guozhu Meng, Minhui Xue, Yang Liu, and Lihua Xu. Are mobile banking apps secure? what can be improved? pages 797–802, 10 2018. doi: 10.1145/3236024.3275523.

[54] Syeda Asher, Sadeeq Jan, George Tsaramirsis, Fazal Khan, Abdullah Khalil, and Muhammad Obaidullah. Reverse engineering of mobile banking applications. *Computer Systems Science and Engineering*, 38:265–278, 05 2021. doi: 10.32604/csse.2021.016787.

[55] Arafat Al-dhaqm, Shukor Razak, Ikuesan Adeyemi, and Victor Kebande. A review of mobile forensic investigation process models. *IEEE Access*, PP:1–1, 08 2020. doi: 10.1109/ACCESS.2020.3014615.

[56] Mohammed Moreb, Saeed Salah, and Belal Amro. A novel framework for mobile forensics investigation process. *International Journal of Computing and Digital Systems*, 16:125–135, 04 2024. doi: 10.12785/ijcds/160110.

[57] Bruno Bernardo, Henrique Mamede, João Barroso, and Vítor Santos. Mobile device forensics framework: A toolbox to support and enhance this process. *Emerging Science Journal*, 8:972–998, 06 2024. doi: 10.28991/ESJ-2024-08-03-011.

[58] Google Form: Login — docs.google.com. https://docs.google.com/forms/u/0/?hl=id. [Accessed 04-04-2025].

[59] Mobile OS market share worldwide 2009-2024 — Statista — statista.com. https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/. [Accessed 26-10-2024].

[60] Mobile, Tablet & Operating System Market Share Ethiopia — Statcounter Global Stats — gs.statcounter.com. https://gs.statcounter.com/os-market-share/mobile-tablet-/ethiopia. [Accessed 26-10-2024].

[61] Mobile, Tablet & Vendor Market Share Ethiopia — Statcounter Global Stats — gs.statcounter.com. https://gs.statcounter.com/vendor-market-share/mobile-tablet-/ethiopia. [Accessed 26-10-2024].

[62] Ride-hailing - Ethiopia — Statista Market Forecast — statista.com. https://www.statista.com/outlook/mmo/shared-mobility/ride-hailing/ethiopia. [Accessed 26-10-2024].

[63] Ride Hailing Apps in Ethiopia: Top 5 Picks - Aemero Media — aemeromedia.com. https://aemeromedia.com/ride-hailing-app-in-ethiopia/. [Accessed 26-10-2024].

[64] Android Apps on Google Play — play.google.com. https://play.google.com/store/games?hl=en. [Accessed 15-10-2024].

[65] App APK Extractor & Analyzer - Apps on Google Play — play.google.com. https://play.google.com/store/apps/details?id=com.ytheekshana.apkextractor&hl=en. [Accessed 04-04-2025].

[66] View on-device files with Device Explorer Android Studio Android Developers — developer.android.com. https://developer.android.com/studio/debug/device-file-explorer. [Accessed 26-10-2024].

[67] A guide to the project management body of knowledge (pmbok® guide)–seventh edition and the standard for project management. Project Management Institute, 2021.

[68] Implement dm-verity Android Open Source Project — source.android.com. https://source.android.com/docs/security/features/verifiedboot/dm-verity. [Accessed 26-10-2024].

[69] UATeam. APK Decompiler: A Comprehensive Guide to Decompiling Android APKs — aleksej.gudkov. https://medium.com/@aleksej.gudkov/apk-decompiler-a-comprehensive-guide-to-decompiling-android-apks-d2a5e1a51307. [Accessed 04-04-2025].

[70] Lana Begunova. Android App Package Name—5 Ways of Retrieval — begunova. https://medium.com/@begunova/android-app-package-name-5-ways-of-retrieval-57089a3cf33a. [Accessed 04-04-2025].

[71] Victoria Clarke and Virginia Braun and. Thematic analysis. *The Journal of Positive Psychology*, 12(3):297–298, 2017. doi: 10.1080/17439760.2016.1262613. URL https://doi.org/10.1080/17439760.2016.1262613.

[72] Waypoint — education.nationalgeographic.org. https://education.nationalgeographic.org/resource/waypoint/. [Accessed 26-10-2024].

[73] Unicode Converter - encoding / decoding — coderstool.com. https://www.coderstool.com/unicode-text-converter. [Accessed 26-10-2024].

[74] Epoch Converter — epochconverter.com. https://www.epochconverter.com/. [Accessed 26-10-2024].

[75] Tetiana Batrachenko, Iryna Lehan, Vitalii Kuchmenko, Volodymyr Kovalchuk, and Olha Mazurenko. Cybercrime in the context of the digital age: analysis of threats, legal challenges and strategies. *Multidisciplinary Science Journal*, 6, 2024.

[76] Abel Yeboah-Ofori and Akoto Derick Brown. Digital forensics investigation jurisprudence: issues of admissibility of digital evidence. *Journal of Forensic, Legal & Investigative Sciences*, 6(1):1–8, 2020.

[77] Marthie Grobler. The need for digital evidence standardisation. *Emerging Digital Forensics Applications for Crime Detection, Prevention, and Security*, page 234, 2013.

[78] Nickson M Karie, Victor R Kebande, HS Venter, and Kim-Kwang Raymond Choo. On the importance of standardising the process of generating digital forensic reports. *Forensic Science International: Reports*, 1:100008, 2019.

Appendix A

Cellebrite UFED Procedures

Pictures of device imaging or acquisition procedures using Cellebrite UFED are listed here:

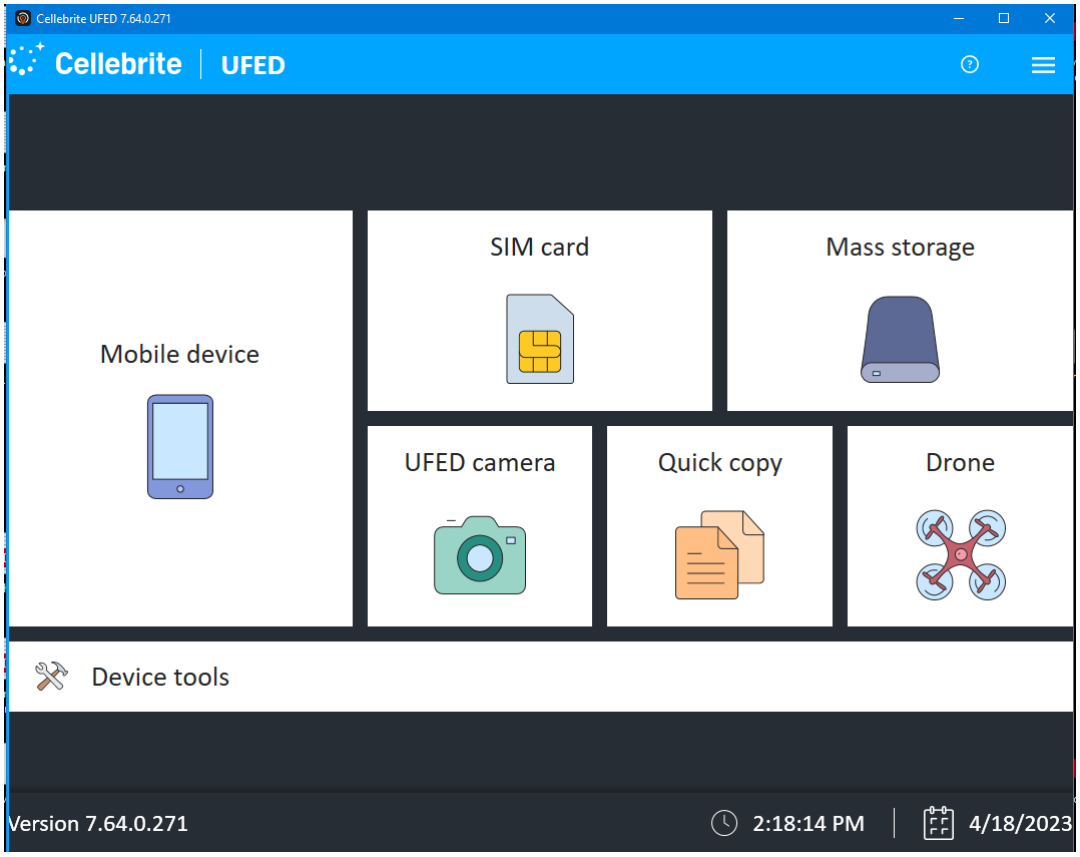


FIGURE A.1: Options on Cellebrite UFED home page

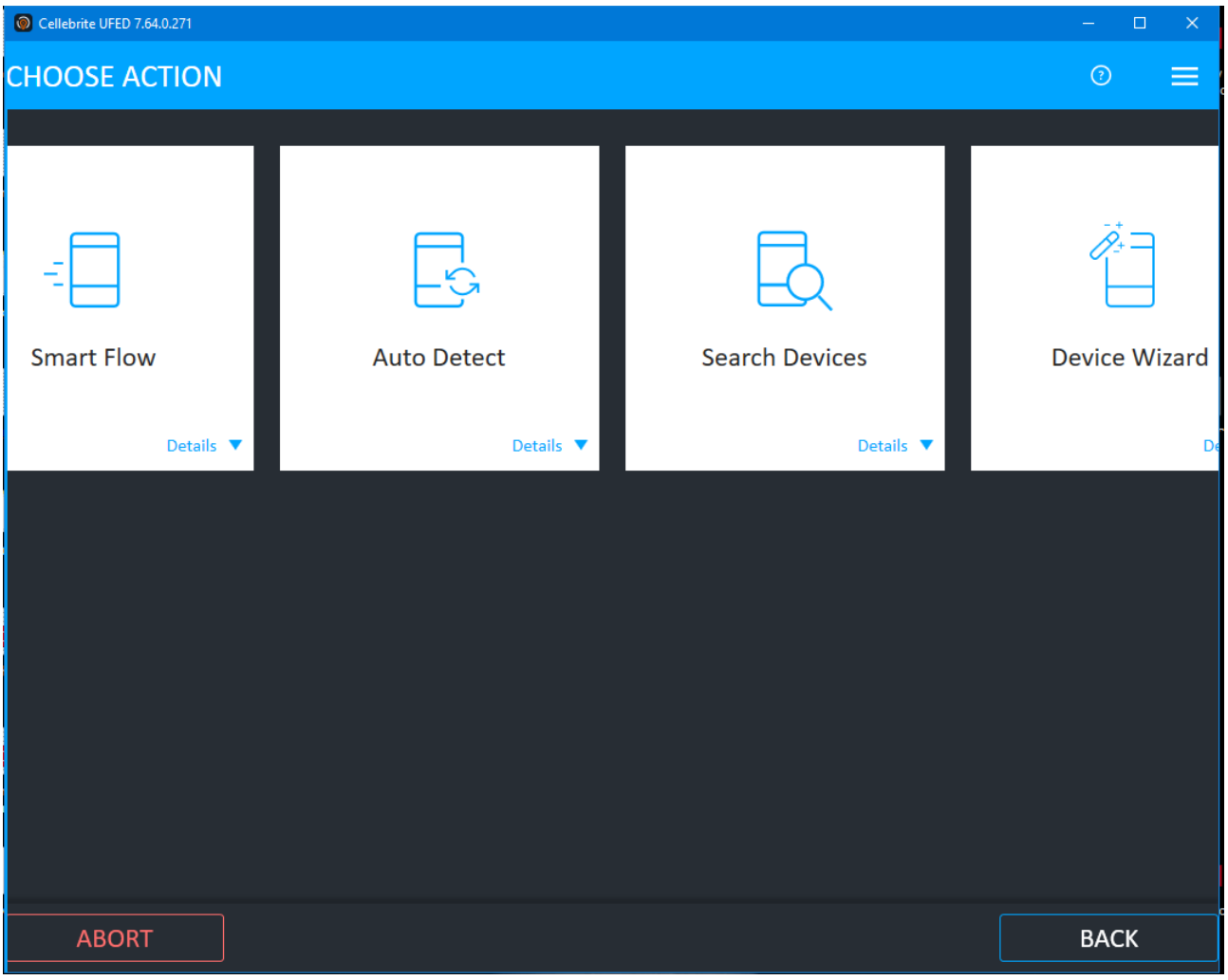


FIGURE A.2: Options on Cellebrite UFED on Choose Action page

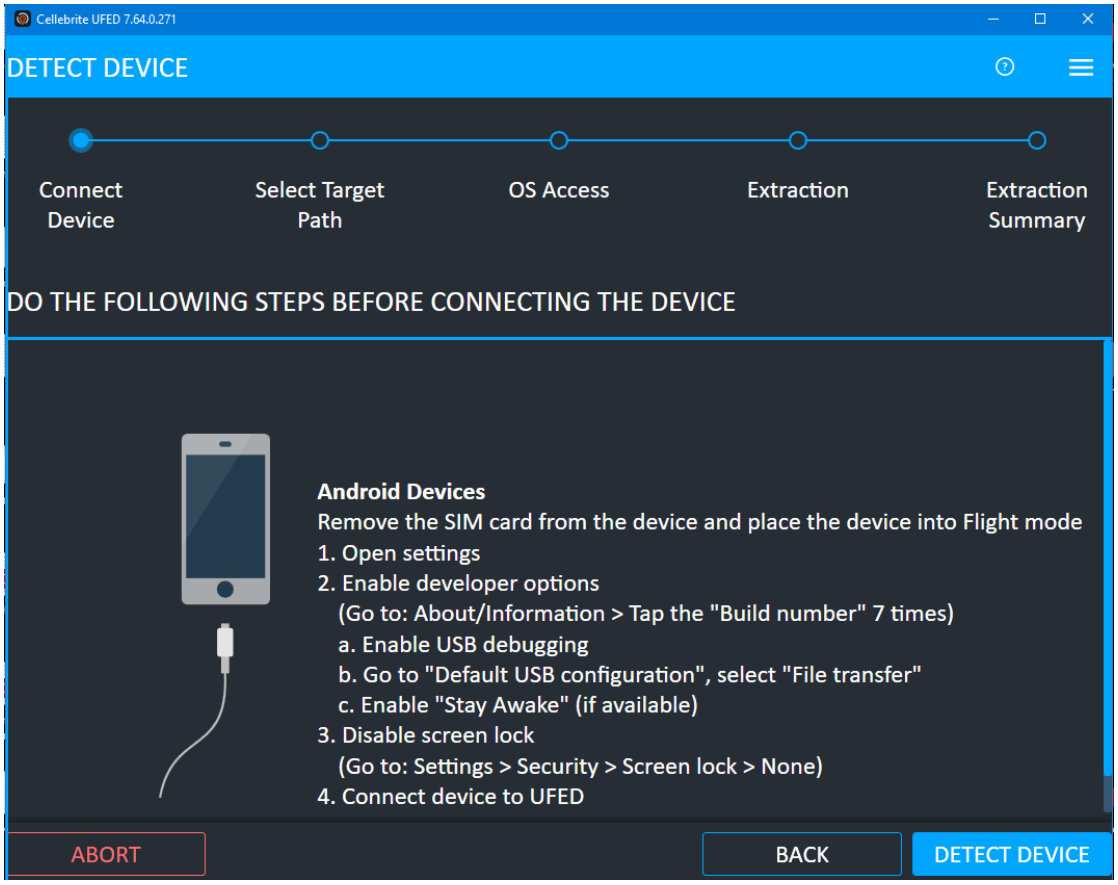


FIGURE A.3: UFED waiting for a device to be detected for imaging

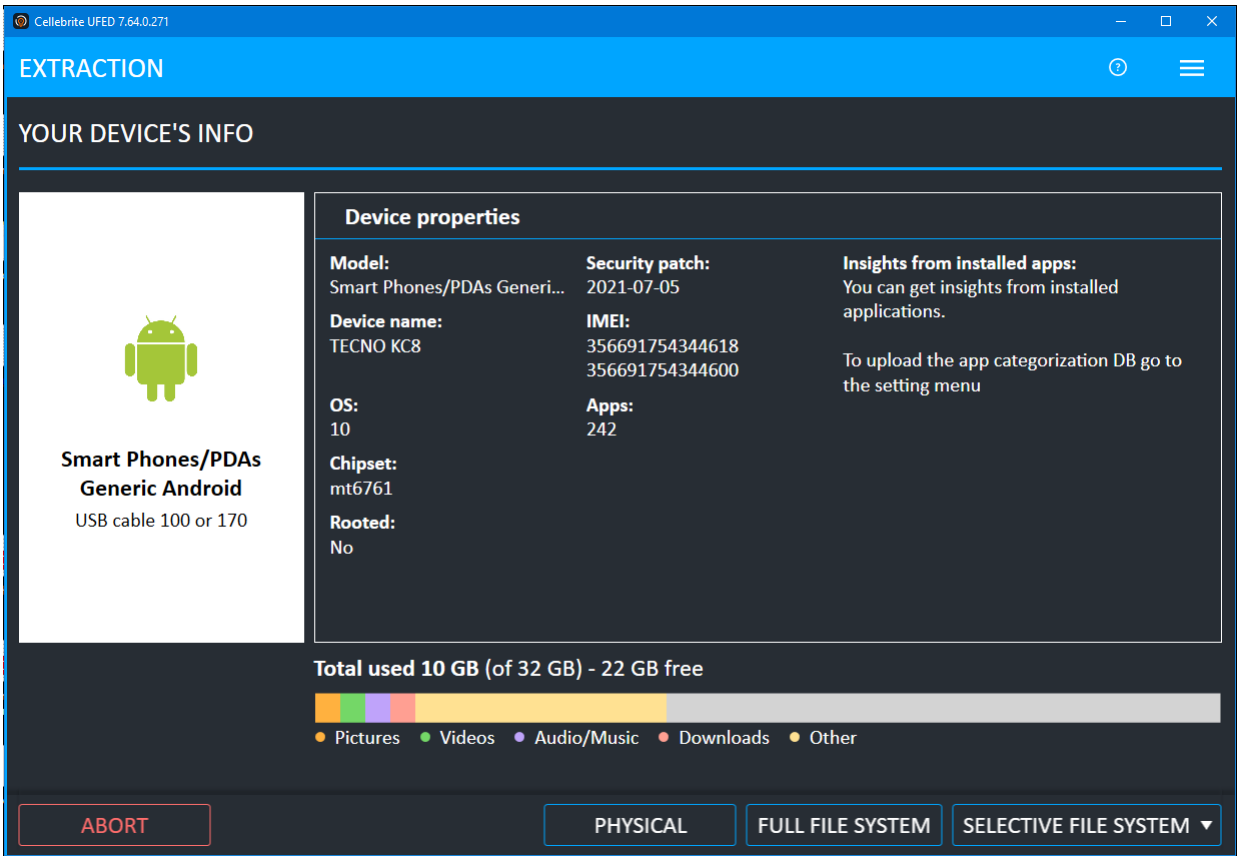


FIGURE A.4: Detailed phone information of the device after it was detected by UFED

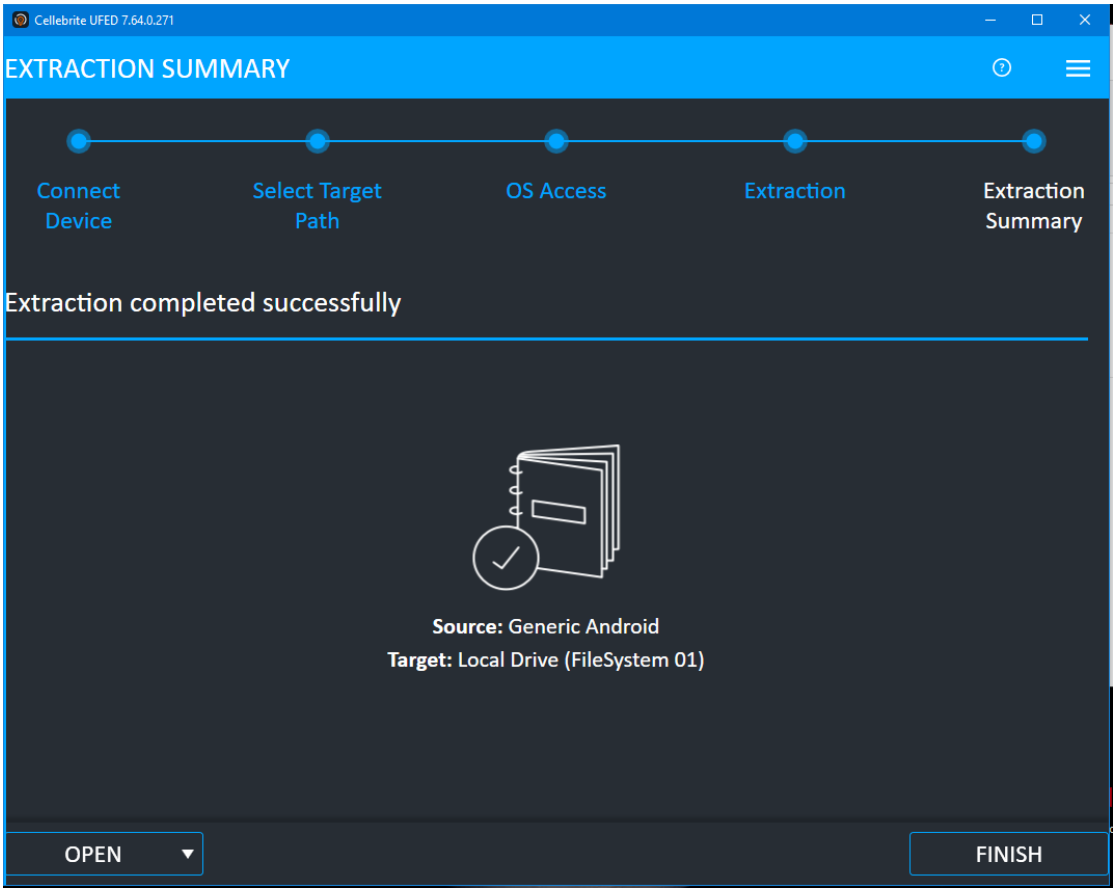


FIGURE A.5: UFED finishes extraction of the phone

Appendix B

Questionnaire

At first, I would like to thank you for taking time to participate in this questionnaire. This questionnaire aims to investigate digital forensics and its role as evidence in criminal case investigations and legal proceedings in our country, Ethiopia. The main objective of the questionnaire is to understand the level of usage of digital forensics evidence and identify the challenges faced throughout the process of digital forensic evidence collection to its usage in the court in facilitating the closure of criminal case. Please be assured that all information you provided here will be kept strictly confidential. Your identity will not be disclosed in any of the results or reports generated using this questionnaire.

SECTION 1: BACKGROUND INFORMATION

1. Name of your organization.....

2. What is your profession?

☐ Judge

☐ Forensic Analyst

☐ Police Officer

☐ Other (please specify).....

3. How many years of experience do you have in your current profession?

☐ 0-5 years

☐ 6-10 years

☐ 11-15 years

☐ 16-20 years

☐ 21+ years

SECTION 2: AWARENESS AND USAGE

4. How familiar are you with digital forensics?

☐ Not familiar

☐ Slightly familiar

☐ Moderately familiar

☐ Very familiar

☐ Extremely familiar

5. Have you ever used digital forensic evidence in your work?

☐ Yes

☐ No

6. If yes, in what type of cases have you used digital forensic evidence? (Select all that apply)

☐ Cybercrime

☐ Financial fraud

☐ Theft

☐ Murder

☐ Drug trafficking

☐ Other (please specify).....

SECTION 3: LEGAL FRAMEWORK

7. Is there any standards or best practices you follow to check / maintain the admissibility of the digital forensic evidences?

☐ Yes

☐ No

8. If yes, which standards or best practices are you adopting to check / maintain the admissibility of the digital forensic evidences?

☐ ISO/IEC ☐ Interpol ☐ Other (please specify) .....

9. For the standard or best practices you are adopting as mentioned above, do you face challenges when you use digital forensic evidence to close a criminal case?

☐ Yes

☐ No

10. If yes, what are the main challenges you face when you use digital forensic evidence

to close a criminal case?

.....

.....

11. How do the current laws ensure the integrity and authenticity of digital evidence? (Select all that apply)

☐ Clear definitions and criteria for admissibility

☐ Requirements for maintaining a chain of custody

☐ Guidelines for proper documentation and storage

☐ Standards for evidence handling procedures ☐ Other (please specify) .....

12. What legal procedures must be followed to obtain a search warrant for digital evidence? (Please specify the steps involved)

.....

.....

.....

13. Are there any specific challenges you face with the legal admissibility of digital forensic evidence in court? (Select all that apply)

☐ Discrepancies in the legal standards

☐ Lack of clear guidelines

☐ Difficulty in meeting admissibility criteria

☐ Other (please specify) .....

14. Have there been any recent legal cases that have challenged the admissibility of digital forensic evidence?

☐ Yes

☐ No

15. If yes, can you provide details about these cases and their outcomes? (Please include case names, dates, and key findings)

.....

.....

SECTION 4: CHALLENGES IN USING DIGITAL FORENSICS

16. What challenges have you encountered when using digital forensic evidence in court? (Select all that apply)

☐ Lack of expertise

☐ Insufficient resources

☐ Legal admissibility issues

☐ Time constraints

☐ High costs

☐ Other (please specify) .....

17. How significant are these challenges in affecting the use of digital forensic evidence?

☐ Not significant

☐ Slightly significant

☐ Moderately significant

☐ Very significant

☐ Extremely significant

SECTION 5: EFFECTIVENESS AND IMPACT

18. How often has digital forensic evidence been crucial in closing a criminal case in your experience?

☐ Never

☐ Rarely (1-2 cases)

☐ Sometimes (3-5 cases)

☐ Often (6-10 cases)

☐ Always (10+ cases)

19. Can you provide specific examples of cases where digital forensic evidence played a pivotal role in the outcome? (Please include case names, dates, and key findings)

.....

.....

20. In how many cases do you believe digital forensic evidence helped to secure a conviction? (Please provide an approximate number)

.....

.....

21. How many times has digital forensic evidence been unable to help in concluding a case? (Please provide an approximate number)

.....

.....

SECTION 6: RECOMMENDATIONS AND IMPROVEMENTS

22. What improvements do you think (based on the challenges you face) are needed to enhance the use of digital forensic evidence in courts? (Select all that apply)

☐ Better training for professionals

☐ Increased funding for forensic departments

☐ Clearer legal guidelines on admissibility

☐ Improved technology and tools

☐ Other (please specify) .....

23. Are there any specific suggestions you would like to make regarding the integration of digital forensics into the legal system? (Please provide detailed recommendations)

.....

.....

Assurance

This thesis is submitted as a partial fulfillment of Master of Science in Cyber Security (SCHOOL OF INFORMATION TECHNOLOGY AND ENGINEERING), Addis Ababa institute of Technology, Addis Ababa University. The author carried out the work included in this thesis, and no part of it has been submitted for a degree or a qualification at any other scientific entity.

Munir Kemal Seman

Signature

.....

Date: March, 2025