Mobile App Forensics

A forensic investigation of the Ride-hailing applications Taxi Stockholm and Sverigetaxi

Gebrecherkos Abrha Halefom

Department of Computer
and Systems Sciences

Degree project 30 HE credits
Computer and Systems Sciences
Degree project at the master level
Spring term 2024
Supervisor: Stefan Axelsson
Reviewer: Lars Asker

Stockholm
University

Abstract

Ride-hailing applications have revolutionized urban transportation, with their widespread adoption growing globally. Despite their convenience, these apps have raised concerns about the potential for misuse and the crimes they facilitate. Limited research exists on the forensic aspects of ride-hailing applications, particularly in the context of Android platforms. This study focuses on conducting a forensic investigation into two Android ride-sharing applications, Taxi Stockholm and Sverigetaxi. The research aims to identify forensically relevant artifacts recoverable from these apps. Therefore, the research work aims to answer the following question: What type of forensically relevant artifacts can be recovered from the ride-sharing mobile applications Taxi Stockholm and Sverigetaxi that could be relevant for forensic investigators? Using a case study approach as the research strategy, this study uses systematic observations and data extraction from forensic tools for the collection of digital artifacts. The qualitative data analysis method, content analysis, is applied to analyze the collected data. By obeying ethical principles, the research ensures data integrity, confidentiality, and privacy. The study recovered and analyzed various artifacts, that includes Rider info (First Name, Last Name, Gmail Address, Phone Number), Credit card details, Company details, booking details, Trip payment invoice details, Trip start and end address, Timestamps, GPS Coordinates, Continuous Routes, and Vehicle details that were extracted from the ride hailing applications. However, limitations of the study include its small-scale nature and the focus on only two specific ride-hailing applications on the Android platform.

Keywords: Mobile Applications, App forensics, ride-hailing applications

Synopsis

Background	The rise of ride-hailing applications has transformed urban transportation, offering convenience and efficiency to users worldwide. However, along with their widespread adoption, concerns have emerged regarding the potential misuse and criminal activities facilitated by these apps. Ride-hailing platforms collect extensive user data, raising questions about privacy, security, and forensic implications. Despite the growing usage of ride-hailing applications, limited research exists on the forensic aspects of these platforms. This gap in knowledge underscores the need for in-depth forensic investigations to uncover and analyze forensically relevant artifacts recoverable from ride-sharing mobile applications.
Problem	The thesis is driven by the concern over the misuse and potential criminal activities facilitated by ride-hailing applications, due to the vast amount of user data they collect. There is a notable gap in research concerning the forensic aspects of ride-hailing applications.
Research Question	The research question addressed by this thesis is, "What type of forensically relevant artifacts can be recovered from the ride-sharing mobile applications Taxi Stockholm and Sverigetaxi that could be relevant for forensic investigators?" The research question is interesting as it aims to identify the digital artifacts in the ride hailing apps that could be relevant for digital investigators.
Method	The thesis uses a case study approach as the research strategy, applying systematic observations and data extraction from forensic tools for the collection of digital artifacts. The qualitative data analysis method, content analysis, is applied to analyze the collected data. The research obeys ethical principles, ensuring data confidentiality and privacy.
Results	The forensic investigation of both ride-hailing applications resulted in valuable insights about the forensically relevant artifacts recoverable from these apps. The study recovered and

	analyzed various artifacts, that includes Rider info (First Name, Last Name, Gmail Address, Phone Number), Credit card details, Company details, booking details, Trip payment invoice details, Trip start and end address, Timestamps, GPS Coordinates and Vehicle detail.
Discussion	Limitations of the study include its small-scale nature, as it only involved data from individual users, and the focus on only two specific ride-hailing applications on the Android platform. The findings may not be generalizable to other contexts or ride-hailing applications, and the study may not be applicable to other mobile operating systems such as iOS. The thesis can be used by researchers, and digital forensics practitioners to advance the understanding of mobile app forensics in ride- hailing applications in particular.

Acknowledgment

I sincerely thank Professor Stefan Axelsson, my thesis supervisor, for his guidance and educational support throughout my thesis work. Under his supervision, I have benefited from his multifaceted expertise and profound insights. I also thank Lars Asker, my reviewer, for providing constructive feedback. Additionally, I want to thank my wife, whose constant encouragement was a significant source of motivation. Furthermore, I thank my teachers and colleagues at the Department of Computer and Systems Sciences (DSV), Stockholm University, with whom I shared the learning process. Lastly, I thank the Swedish Institute for generously granting me a full scholarship to pursue my master's studies.

Table of Contents

1 Introduction 1
1.1 Problem statement 2
1.2 Research question 3
1.3 Delimitations 3
1.4 Thesis Structure 3
2 Extended background 4
2.1 Android OS Platform Architecture 4
2.2 Android Storage Location 5
2.3 The Taxi Stockholm and Sverigetaxi applications 6
2.4 Related work 6
3 Methodology 7
3.1 Chosen Research strategy 7
3.2 Chosen Data Collection Method 7
3.3 Chosen Data Analysis Method 8
3.4 Research Ethics 9
4 Forensic investigation 10
4.1 Forensic Process 10
4.2 Preservation and investigation set up 10
4.3 Forensic Data Acquisition 15
4.4 Forensic Examination and Analysis 17
4.4.1 Taxi Stockholm and Sverigetaxi 18
5 Results 21
5.1 Taxi Stockholm 21
5.2 Sverigetaxi 24
5.3 Findings Themes and Patterns 31
6 Discussion 33
6.1 Analysis 33
6.2 Conclusion 34
6.3 Limitations 35
6.4 Future research 35
7 References 36
8 Appendix A - Scripts 39
9 Appendix B - Reflection 41

List of Figures

Figure 1: Android storage...5
Figure 2: Ride-Sharing App Ecosystem Interaction Flow ……..…………………………….….…11
Figure 3: Rooted oneplus 5T mobile ……………………………………………………….….….14
Figure 4: Digital experiment Setup ……………………………………………………………….16
Figure 5: Data Acquisition using XRY …………………………………………………………17
Figure 6: Extracted artifacts on XAMN view for Taxi Stockholm.…………………………………19
Figure 7: Extracted artifacts on XAMN view for Sverigetaxi (Cabonline) ………………………….19
Figure 8: Details of Stored Address Table ………………………………………………..……….21
Figure 9: tsab.db database table overview and StoredUser table data ……………………………….21
Figure 10: Stored payment card table …………………………………………………….….….22
Figure 11: Stored booking table - Part 1 ……………………………………………….…………22
Figure12: Stored booking table - Part 2 ……………………………………………………..….22
Figure 13: Stored booking table - Part 3 ……………………………………………………..……22
Figure 14: Payment transaction details in JSON format …………………………………………….24
Figure 15: data transport events table ……………………………………………………….….25
Figure 16: cache file EN4 data ……………………………………………………….………....26
Figure 17: cache file EN3 data ……………….……………………………………………………26
Figure 18: cache file EN5 data ……………………………………………………….…………30

List of Tables

Table 1: Overview of device ………………………………………………………….11
Table 2: Overview of Sverigetaxi ride-hailing app functionality ……………….…...…...12
Table 3: Overview of Taxi Stockholm ride-hailing app functionality…………………….13
Table 4: Tools used for backup and rooting. …………………………………………….15
Table 5: Data acquisition tool …………………………………………………………….16
Table 6: forensic analysis tools ……………………………………………..……..…20
Table 7: Extracted Artifacts……………………………………………………………….32

List of Abbreviations

- ADB: Android Debug Bridge
- API: Application Programming Interface
- ART: Android Runtime
- C/C++: C and C++ programming languages
- DEX: Dalvik Executable
- GPS - Global Positioning System
- HAL: Hardware Abstraction Layer
- ISO - International Organization for Standardization
- JSON: JavaScript Object Notation
- LBS: Location-based Services
- NIST: National Institute of Standards and Technology
- OS: Operating System
- PII: Personally, Identifiable Information
- SHA-256 - Secure Hash Algorithm 256-bit
- TWRP: Team Win Recovery Project
- UI: User Interface
- VM: Virtual Machine
- XML: Extensible Markup Language

1 Introduction

Ride-hailing services, also known as "E-hail" and "ride-sourcing," look like traditional taxi services but operate through mobile applications. Uber, founded in California in 2009 as UberCab, is a prime example of a Transportation Network Company (TNC) that offers such ride-hailing services through UberBLACK (Guyader et al., 2021). In 2020, the global ride-sharing market reached a value of USD 76.48 billion, and it is projected to grow to USD 242.73 billion by 2028, with ride-hailing services using mobile applications playing a significant role in this growth (Fortune Business Insights, 2021). The rise of urban transportation is being reshaped by app-based mobility services, with ride-hailing leading the way. This form of transportation has gained widespread popularity for its convenient on-demand urban travel solutions. However, most research in this field has predominantly focused on U.S. cities, with limited attention given to other regions like Europe. Europe's unique characteristics, including a robust public transportation system and a stronger emphasis on environmental concerns, necessitate distinct considerations (Gomez et al., 2021).

The use of ride-hailing mobile applications has seen steady growth, driven by the convergence of Information and Communication Technology (ICT) with the shared economy, which has led to the emergence of new transportation services spurred by enhanced online connectivity and evolving individual lifestyles (Alemi et al., 2018). Moreover, research by Thaithatkul et al. (2019) tells that information shared by friends on social networks, whether online or offline, significantly influences travellers' decisions in dynamic ride-sharing systems. A 2018 Pew Research Centre survey reported that 36% of U.S. adults have used a ride-hailing service like Uber or Lyft (Pew Research Centre, 2018). Additionally, Smiljanic Stasha (2022) notes that approximately 25% of the entire U.S. population uses ride-sharing at least once a month. In Europe, ride-sharing services were used by 146 million people in 2019, increasing to 150 million in 2020 (David Curry, 2022). In addition to their widespread use, ride-hailing applications have raised concerns about the potential for misuse and the crimes they facilitate, linked to the extensive user data collected by these apps.

Ride-hailing applications often collect user data to enhance service quality and generate additional revenue (Statista, 2022). Notably, GrabTaxi, Yandex Go, and Uber rank among the top applications known for collecting user data (Statista, 2022). These ride-hailing services store a wealth of personal information, including GPS locations, vehicle registration details, driver's licenses, and payment data (Zhao et al., 2019). However, these apps have also been exploited by criminals for various illicit activities (Luz Lazo, 2020). In one case in the U.S. District of Massachusetts, fourteen individuals were charged with creating fraudulent driver accounts using information obtained from the dark web, which they subsequently sold or rented via a ride-sharing mobile app (Andrew Wyrich, 2021). In another instance, Uber's lost-and-found feature, combined with Apple's Find My iPhone, enabled an intoxicated Uber customer to track and harass a female Uber driver at her residence (Johana Bhuiyan, 2015). More recently, a Lyft driver was accused of assaulting and robbing a guest at a Miami Beach hotel (Liane Morejon and Andrea Torres, 2022).

In most ride-sharing applications, users are requested to download and register themselves to use the service quickly and smoothly. At the same time to check a rider on their nearby, they are asked to allow the location application on their mobile application. Even though many crimes are being committed using ride-sharing mobile applications, little forensics research has been done on those applications. The study, entitled "Geolocation Tracking and Privacy Issues Associated with the Uber Mobile Application," revealed that Uber's mobile app utilizes extremely precise and potentially intrusive geolocation tracking techniques (Hayes, Christopher Snow, and Saleh Altuwayjiri, 2017). The experiments performed tells that Uber tracks the location of its users even after the conclusion of a ride for longer than its official privacy policy suggests (Hayes, Christopher Snow, and Saleh Altuwayjiri, 2017).

In the contract, much research is done on the privacy perspective of ride-sharing applications. A study on Solutions that preserve user privacy for location-based services, such as ride-hailing, which charges users based on distance travelled, recommends the best practices and solutions for privacy-oriented services (Balasch et al., 2010). According to a study on the leakage of privacy-sensitive data of drivers using the nearby feature of twenty ride-hailing applications, including Uber and Lyft, a data harvesting attack is feasible and possible (Zhao et al., 2019).

As a result of crimes committed using these applications, such as physical assaults, robberies, identity theft, and cyberbullying, the users, drivers, and even the owner of the ride-sharing application could all be impacted. So, it is essential to do a forensic investigation of those ride-sharing applications, i.e., Taxi Stockholm and Sverigetaxi, to try to get a forensically sound artifact that could be helpful in a court of law for crime reconstruction. This study intends to conduct a forensic investigation on two of the top ride-hailing Apps of 2021 (Android), Taxi Stockholm and Sverigetaxi in Stockholm, according to the survey, which was collected based on criteria including User Experience, Core Functionality, and Innovative solutions (Ken Pillar, 2021). This study wants to do a forensic investigation on those two apps because it is much more feasible to do a practical on-place experiment on those ride-sharing apps since they are being used in Stockholm. Both Taxi Stockholm and Sverigetaxi are installed by more than a hundred thousand users each. At the same time to the best of my knowledge, those two applications were not exposed to forensic investigation to date.

1.1 Problem statement

In research done by (Darren R. Hayes, Christopher Snow, and Saleh Altuwayjiri, 2018), the uber app forensics is mainly concerned with privacy and it recommends and highlights the huge possibilities for more research from the forensics perspective. According to the research done by (Zhao et al., 2019) though it tells that it was possible to harvest an extensive amount of sensitive information from the Uber app, the forensics investigation was mainly focused on the "nearby cars " feature of the app. In addition to this, Kiptoo explained the need for the further digital forensics research on android on-demand ride applications (odrs) “Emerging technologies associated to the odrs applications such as Uber Eats and Little coins among others is recommended for similar study” (Kiptoo, 2020).

On the other hand, there are multiple of research conducted on privacy concerns of the ride-hailing applications (Pham et al., 2017), (Balasch et al., 2010), (Martelli, Renda and Zhao, 2020), (Hayes, Christopher Snow, and Saleh Altuwayjiri, 2017). As (Martelli, Renda and Zhao, 2020) said, "Transportation and location data can reveal personal habits, preferences, and behaviours, and riders could be keen not to share the exact location of their origin and/or destination." And it explains how location privacy-preserving techniques can affect the performance of the ride-sharing applications in terms of quality service and system efficiency. According to the research done by (Pham et al., 2017), "Our analysis exposes high-risk privacy threats that do not occur in conventional taxi services. Therefore, we propose Private Ride, a privacy-enhancing and practical solution that offers anonymity and location privacy for riders and protects drivers' information from harvesting attacks." The varieties of the relevant artifacts obtained from the previous studies and their use for crime reconstruction imply the relevance of doing forensic research that can go beyond investigating a single feature of a ride-sharing mobile application. Therefore, the problem addressed in this thesis is conducting a forensic investigation to identify and explore the forensically relevant artifacts that can be extracted from both ride-hailing apps.

1.2 Research question

This research aims to conduct a forensic analysis of two Android ride-sharing mobile applications using logical acquisition techniques to extract data from the apps and analyse to get artifact that is forensically sound that can be used in crime investigation. Both ride-sharing mobile applications are among the top used taxi apps in Stockholm, and they are installed by more than a hundred thousand users each (Ken Pillar, 2021).

The research, therefore, aims to answer the following question:
What type of forensically relevant artifacts can be recovered from the ride-sharing mobile applications Taxi Stockholm and Sverigetaxi that could be relevant for forensic investigators?

1.3 Delimitations

Open-source and proprietary forensics tools will be used to conduct the application's forensic investigation to undertake this research. The data collection will be based on the installed ride-sharing application in a smartphone android powered mobile. That means we will use the data from the application, not from people. Limiting the number of applications to research to only two is because of the time constraint given to do the research study. In addition, the research will mainly focus on the android mobile application as it is the largest installed and used application (fortune business insights, 2021).

1.4 Thesis Structure

The thesis is structured into six main chapters. The initial chapter is the introduction, containing introduction, problem statement, research question, and delimitations. Following this, Chapter 2 covers an extended background, providing an in-depth exploration of the Android OS Platform Architecture, Android Storage Location, and details about both applications, along with a summary of related work.

Chapter 3 describes the methodology, justifying the chosen research strategy, and clarifying the selected data collection and analysis methods. This section also discusses alternative research strategies and techniques, alongside considerations of research ethics. Chapter 4 presents the forensic investigation process, which includes preparation, data acquisition, forensic examination, and analysis.

Chapter 5 presents the obtained results of the forensics investigation. Following this, the last chapter 6 discussions the analysis of the thesis, addressing the limitations of the research, offering a conclusion that summarizes key findings, and explaining future work.

2 Extended background

As Singh et al. (2019) argue, the technology revolution has given cybercrime a boost. They point out that the increasing use of technology has made it easier for criminals to launch cyberattacks. In the contemporary landscape, various entities, including financial institutions, hospitals, government agencies, businesses, media outlets, and even illicit organizations, heavily rely on the vast reservoirs of digital data and the array of digital devices that have become an integral part of our daily lives. Regrettably, this digital era has also witnessed the emergence of cybercrime, where wrongdoers employ digital tools and platforms to engage in unlawful activities such as hacking, identity theft, financial fraud, embezzlement, child exploitation, corporate espionage, and more. Consequently, digital devices like computers, cell phones, cameras, and the like are increasingly discovered as evidential artifacts at crime scenes during the course of criminal investigations (Lin, 2018). The increasing use of smartphones has led to a growing need for investigators to search digital devices for data evidence, such as emails, photos, videos, text messages, and transaction log files. This is because all of the applications installed on smartphones have the capacity to store information locally on the device. (Carrier, 2018, p. 10). The Android platform is particularly popular, and as a result, there is a high demand for smartphone digital forensics for Android devices. This is due to the increase of Android devices, the many features they provide, the many applications available for them, and the correspondingly rich set of data that can be found in local storage. (Shavers, 2021, p. 20). Android is a popular operating system for many ride-hailing applications, including Taxi Stockholm and Sverigetaxi, which are the focus of the forensic investigation in this study.

Digital forensics involves the collection, preservation, analysis, and presentation of digital evidence in legal proceedings (Casey, 2010). It requires a thorough understanding of digital devices, operating systems, applications, and their forensic artifacts, as well as obeying legal and ethical standards. Digital forensic investigations can uncover critical information that can be used in criminal investigations, litigation, and dispute resolution.

2.1 Android OS Platform Architecture

The Android operating system (OS) is an open-source, Linux-based OS developed by Google for mobile phones, tablets, and televisions. The architecture of the Android OS can be divided into seven components, each playing a crucial role in its overall functioning (Android developers, 2023). At the foundation of the Android OS is the Linux kernel, which provides essential functionalities such as threading and low-level memory management, Above the kernel is the hardware abstraction layer (HAL), which acts as an interface between the Android OS and the built-in hardware components on the device. The HAL allows the OS to communicate with hardware components effectively, making it possible to utilize various hardware features (Android developers, 2023).

Following the HAL, there are the native C/C++ libraries and the Android runtime (ART). Native C/C++ libraries are used to build core Android system components such as ART and HAL. ART, on the other hand, is responsible for running multiple virtual machines on low-memory devices through DEX file execution, which is a bytecode format specifically designed for Android. For devices running Android version 5.0 or higher, applications on the device run in their own process with their own instance of ART, ensuring efficient and isolated execution (Android developers, 2023). Moreover, the Java API framework is a crucial component of the Android OS architecture. It provides a set of APIs that allow developers to access the full feature-set of the Android OS. These APIs are valuable when creating Android applications as they provide a standardized way to interact with various OS functionalities, such as UI components, file system access, network communication, and more (Android developers, 2023).

2.2 Android Storage Location

The storage location on Android devices is a critical factor in forensic examinations of mobile applications. Before extracting and analyzing the data stored on smartphones, it is essential to know where the relevant data is located. Though the file structure of all android mobile is not identical "there are specific locations that are fairly standard (such as app data being stored in the "/data/data/" directory) "(Lin, 2018).

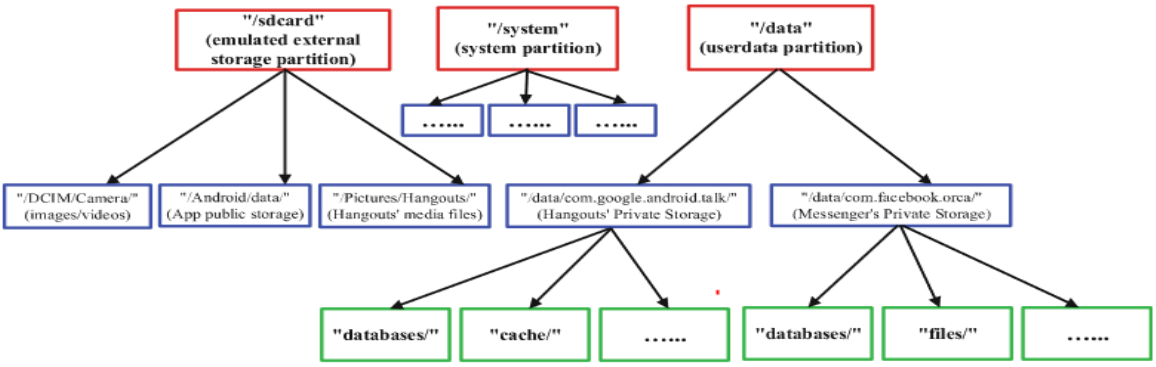


Figure: 1 Android storage

As shown from the figure above "The top level (red) represents partitions (a subset of all partitions); the second and third levels (blue and green respectively) represent content found in these partitions. The "userdata" partition, mounted at "/data", contains all private application storage. This is protected content, only accessible by each application"(Lin, 2018, p. 337). As a result, to perform a data acquisition a user is required to have root access (Lin, 2018).

In addition, methods for storing or discovering data in Android include Shared Preferences, Internal Storage, and External Storage (Heid et al., 2022). Shared Preferences allow storing data as key-value pairs in plain text files in internal storage and are often used for simple data that is app-specific. Internal Storage provides each app with its own exclusive storage directory on the device's internal storage and is often used for sensitive data or small data volumes. External Storage, which can be accessed by apps with the necessary permissions, is used for larger data volumes or for shared storage between apps. External storage can also include media files, downloads, and documents with dedicated folders, accessible through appropriate APIs (Heid et al., 2022).

2.3 The Taxi Stockholm and Sverigetaxi applications

Taxi Stockholm and Sverigetaxi are widely used ride-sharing services in Stockholm, Sweden. These applications are integral to forensic investigation due to their widespread use and the potential for data collection and privacy concerns. Both Taxi Stockholm and Sverigetaxi are among the largest ride-sharing service in Stockholm Sweden (Ken Pillar, 2021). The Sverigetaxi have features including Book a taxi quickly and easily, check Fixed price on all trips, pay by card or PayPal directly in the app and Get status updates for the trip (Sweden taxi, 2022). Taxi Stockholm has features including Pre-book or book directly, write a message to the driver, pay by card, by taxi account or in the car, Choose a standard, large car, or business, and Book pick-up via map or search by address (Taxi Stockholm, 2022). According to the privacy policy of Sverigetaxi it collects personal data such as name, phone number, e-mail address, age, payment details, frequently used addresses, transactional information, troubleshooting, information submitted when in contact with service staff, submitted ratings, the date and time accessed the platforms, the hardware and software used when visiting the platform, IP-addresses, information regarding your GPS-position etc. (Sweden taxi, 2022). On the other hand, the Taxi Stockholm. In taxi Stockholm they collect similar personal data but affirm to not collect more information than is necessary and to not use the collected data for the purposes other than those specified on their terms (Taxi Stockholm, 2022). Collecting of those data apart from their service facilitation role if they are exposed to an unauthorized user, it could be misused and can expose the privacy of those ride-sharing app users.

2.4 Related work

Though there was much more research on the privacy perspective of the ridesharing there is a huge need to work on the forensics aspects of the ride-sharing applications. In research done by (Darren R. Hayes, Christopher Snow, and Saleh Altuwayjiri, 2018), the uber app forensics is mainly concerned with privacy and it recommends and highlights the tremendous possibilities for more research from the forensics perspective. According to the research done by (Zhao et al., 2019) though it revealed that it was possible to harvest an extensive amount of sensitive information from the Uber app, the forensics investigation was mainly focused on the "nearby cars " feature of the app. In addition to this, Kiptoo explained the need for the further digital forensics research on android on-demand ride applications (odrs) “Emerging technologies associated to the odrs applications such as Uber Eats and Little coins among others is recommended for similar study” (Kiptoo, 2020). A forensic investigation was conducted to extract the artifacts from two popular third-party location sharing applications on iOS and Android devices which resulted in extracting evidence that can assist investigations reliant on knowing the past location of a suspect (Bays and Karabiyik, 2019). Additionally, the paper written by (Maus, Höfken and Schuba, 2010) proposes a comprehensive approach to analyzing geodata on smartphones using app-specific descriptions, allowing for automatic extraction and presentation of relevant geodata, and is currently being implemented for Android smartphones.

3 Methodology

3.1 Chosen Research strategy

In this study, forensic tools will be used to extract digital evidence from two popular ride-sharing apps in Sweden, namely Taxi Stockholm and Sverigetaxi. The chosen research strategy for this investigation is a case study approach, as described by Denscombe (2014), which involves focusing on a specific phenomenon to provide a detailed account of events, relationships, experiences, or processes occurring within that particular instance. “Case studies focus on one (or just a few) instances of a particular phenomenon with a view to providing an in-depth account of events, relationships, experiences, or processes occurring in that particular instance. The aim is to illuminate the general by looking at the particular” (Denscombe, 2014). The goal of this research is to explore the forensically extractable digital artifacts from the ride-sharing applications, which requires an understanding of the underlying dynamics and processes within these applications. Case studies provide a comprehensive perspective on naturally occurring phenomena, enabling descriptive and exploratory solutions for forensic investigators (Denscombe, 2014).

However, alternative research strategies that have been considered include action research and experimental research. Action research could involve actively engaging with the apps and taking actions to recover artifacts, while experimental research could involve conducting controlled experiments to systematically investigate artifact recovery (Denscombe, 2014). Nevertheless, the case study approach is considered suitable as it allows for a comprehensive understanding of the dynamics and processes within the applications and provides a holistic view of naturally occurring phenomena, which aligns with the research question and objectives of the investigation. While experiment and action research were considered, the case study approach was preferred due to its compatibility with the research's objective to comprehensively explore the real-world dynamics of the applications.

Compared to other research strategies, the case study approach has advantages such as its holistic approach that enables in-depth investigation of naturally occurring phenomena. However, it also has disadvantages, including challenges in generalizing findings and defining clear boundaries for the case, as noted by Denscombe (2014).

3.2 Chosen Data Collection Method

The data collection method for this research study will use a combined approach of systematic observations and data extraction from forensic tools, following the recommendations of Denscombe (2014) in his book "The Good Research Guide." Systematic observations will be conducted to minimize observer bias and ensure consistency in data collection (Denscombe, 2014). This will involve recording user interactions with the Taxi Stockholm and Sverigetaxi applications, such as creating accounts, making bookings, and paying for the ride-hailing service.

Additionally, forensic tools, such as XRY, XAMN, HxD, DB Browser for SQLite and notepad++ have been used to extract and analyze digital artifacts from the mobile devices on which the ride-hailing apps are installed. These tools will be used to acquire and analyze data stored in app caches, databases, files, logs, and other relevant artifacts. The collected data will be processed and analyzed using forensic techniques, such as timeline analysis and keyword searches, to identify forensically relevant artifacts.

To ensure the validity and reliability of the data collection process, several measures will be implemented. Firstly, methodological triangulation will be employed, using multiple data collection methods such as systematic observations and forensic data extraction. This approach is intended to corroborate the findings and enhance the overall validity of the research by ensuring that different data sources converge on similar results. Secondly, strict adherence to proper chain of custody procedures will be maintained throughout the data collection process. This careful documentation and handling of digital artifacts, from extraction to analysis, will preserve the integrity of the collected data, making it admissible as potential evidence in legal proceedings. Lastly, each data source, whether obtained through systematic observations or forensic extraction, will be thoroughly documented to provide transparency, and facilitate the traceability of findings. These comprehensive measures align with best practices in digital forensics (Casey, 2010) and collectively contribute to enhancing the validity and reliability of the data collection process.

An alternative data collection method that was considered for this research study was documentary research. This method involves treating documents, such as user manuals, terms of service, privacy policies, and other relevant documentation associated with the applications as primary data sources (Denscombe, 2014). Documentary research could have been useful in gaining insights into the functionalities and features of the applications, as well as any relevant legal or policy-related information.

However, the decision to use systematic observations and data extraction from forensic tools as the primary data collection method was made due to several reasons. Firstly, systematic observations allow for direct data collection by objectively observing user interactions with the applications, which is valuable in identifying forensically relevant artifacts in real-time. Secondly, the use of forensic tools enables the extraction of digital artifacts from the mobile devices themselves, providing a more comprehensive and accurate representation of the data generated by the applications. Thirdly, the systematic observations and data extraction approach aligns with the research objective of identifying artifacts that user using the ride-sharing applications would produce, and guarantees reliability and consistency in data collection, as recommended by Denscombe (2014).

Documentary research, while valuable in other contexts, would not provide the same depth of insight into the digital artifacts and their context, making it a less suitable choice for this study. The chosen data collection method, which combines systematic observations and forensic data extraction, was selected over documentary research due to its ability to provide a more comprehensive understanding of the naturally occurring phenomena within the ride-sharing applications and to ensure robust data collection for the study's objectives. However, the selected data collection methods are not without drawback including exposure to observer bias on the use of systematic observation and the incompatibility of forensics tools to some apps during artifact extraction.

3.3 Chosen Data Analysis Method

On this research the chosen data analysis method is qualitative data analysis, specifically content analysis. Content analysis involves examining and interpreting non-numerical data, such as artifacts, text, and images, to identify patterns, themes, and relationships within the data (Denscombe, 2014).

Qualitative data analysis was preferred over quantitative data analysis due to the exploratory nature of the study and the need to understand the meaning and context of the digital artifacts extracted from the ride-sharing applications. Qualitative data analysis allows for a more in-depth analysis of the content, which may include personal data, payment details, transactional information, logs, geolocation information, and provides a greater understanding of the observed objects.

Content analysis was specifically chosen as the method of qualitative data analysis due to its significance in investigating digital artifacts. Content analysis can involve categorizing the content based on emergent themes and may also include quantitative aspects such as frequency counts or coding schemes(Denscombe, 2014). This approach will enable the identification of patterns and themes within the extracted data, allowing for a systematic analysis of the digital artifacts and providing insights. While content analysis offers a systematic approach for interpreting artifacts, it does come with drawbacks such as being time-consuming and labor-intensive (Denscombe, 2014).

The practical application of content analysis in this study involves several key steps. Firstly, the digital artifacts extracted from the ride-sharing applications using XRY will be virtualized and reviewed using XAMN forensics tool. Subsequently, the researcher will systematically review and analyze the digital artifacts using various tools mentioned in the data collection section. During this process, emerging themes and patterns within the data will be identified. Finally, I will interpret the findings within the context of the research objectives, drawing meaningful insights and conclusions from the analyzed digital artifacts.

Quantitative data analysis was considered but not preferred for this study as it requires large data volumes and may become too complex with multiple variables to analyze (Denscombe, 2014). Additionally, the research question and scope of the study did not require precise measurements or numerical frequency counts, which are typically associated with quantitative data analysis. Content analysis was considered the most suitable method for this research due to its ability to provide a nuanced understanding of the digital artifacts and their context.

3.4 Research Ethics

As this study involves conducting digital forensics on mobile applications it is important to address the ethical considerations associated with the collection and analysis of personal and sensitive data. The mobile applications under investigation, namely Taxi Stockholm and Sverigetaxi, collect various types of personal information from their users, including phone number, e-mail address, payment details (Sweden taxi, 2022) (Taxi Stockholm, 2022), for the purpose of their operations and services.

Given the nature of the research, where the researcher will be using a mobile device with installed applications to conduct forensic analysis, it will be ensured that all data collected and analyzed are handled with utmost care and in compliance with relevant laws relating to digital forensics and data privacy. Proper measures will be taken to protect the confidentiality and privacy of the data, and all data collected will be stored securely to prevent unauthorized access or data breaches.

While the study does not involve obtaining explicit informed consent from individual participants, the researcher will follow to ethical principles of integrity, transparency, and respect for human subjects throughout the research process (Pritha Bhandari, 2021) .The findings of the study will be reported objectively and without disclosing any personally identifiable information, and the results will be used solely for academic purposes and the advancement of knowledge in the field of digital forensics.

4 Forensic investigation

4.1 Forensic Process

The forensic investigation follows established best practices and industry-standard directives outlined by the National Institute of Standards and Technology (NIST) (Ayers et al. in 2014). The systematic process comprises several interconnected phases, each executed with the consideration to maintain the investigation's integrity and preserve digital evidence.

The initial phase is Preservation, where the focus is on maintaining the chain of custody without changing the device data, in line with NIST guidelines for mobile device forensics as recommended by (Ayers et al. 2014).

Next is the Acquisition phase, involving creating a forensic image or retrieving information from the ride-hailing app. This step is essential to ensure data preservation without any risk of loss or tampering during the investigation.

Following Preservation and Acquisition is the Examination phase, where digital evidence is uncovered and analyzed in detail. The goal is to provide a comprehensive description of the data, including its source, significance, and relevance to the investigation (Ayers et al.2014).

After Examination, the Analysis phase evaluates the relevance and probative value of the discovered evidence to the case, considering various references and forensic methodologies to ensure a thorough analysis (Casey, E. 2010).

Finally, the Reporting stage involves the preparation of a detailed summary that outlines each step taken during the investigation and presents the conclusions reached. It includes documentation of all actions and provides explanations of the inferences drawn from the collected data. The investigation followed the chosen strategy of a case study approach, complemented by the data collection method i.e., systematic observations and data extraction from forensic tools and qualitative data analysis through content analysis.

4.2 Preservation and investigation set up

In preparation for the research study, an email account was set up under the address 'gebrethesis@gmail.com.' This particular email was used throughout the experiment for registration purposes within the Google Play store and serving as the primary account for accessing and using both ride-hailing apps throughout the investigative process. In compliance with best practices in digital forensics, emphasis is given to maintaining a secure chain of custody throughout the investigation process in this study. This ensures the integrity of the evidence from the moment of collection to analysis and reporting.

Device name	Model	Android version
Oneplus 5T	Oneplus A5010	10

Table 1: Overview of device

The interaction between the rider, the app's backend system, and the driver is a critical focus in these forensics. This interaction involves the rider initiating ride requests, the backend system facilitating communication and transaction processing, and the driver responding to ride requests. The forensic analysis aims to examine the digital trail left by each party in the apps, including user actions and data transactions to uncover relevant evidence. Figure 2 illustrates this interaction flow in a visual representation, providing a clear overview of the key components and data exchanges within the ride-sharing app ecosystem.

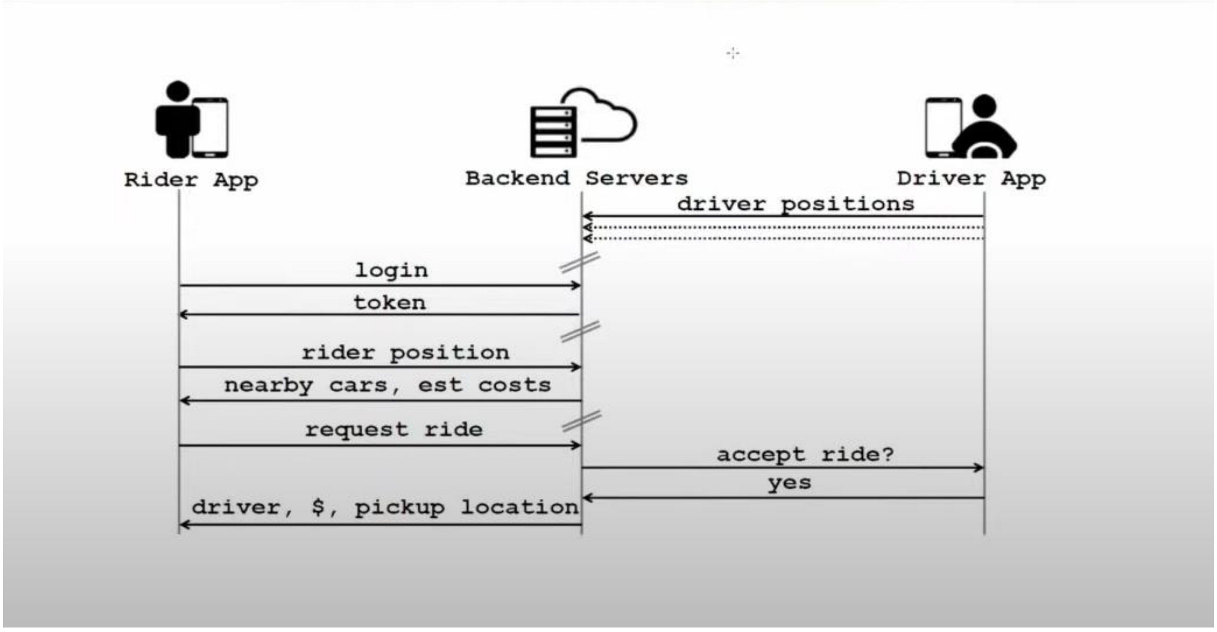


Figure 2: Ride-Sharing App Ecosystem Interaction Flow (Zhao et al., 2019)

As part of this investigation, multiple trips were taken using the ride-hailing services of both companies, with their respective ride-hailing apps. These trips include journeys from Solna Centrum to Armegatan 32, return trips between Armegatan 32 and Solna Centrum, as well as a separate trip from Solna Centrum to Råsundavägen. The selection of routes for the trips aimed to simulate typical user interactions with the ride-hailing apps and to incorporate a range of scenarios that users might encounter. All of these rides were conducted within the geographic area of Stockholm County. In my experience with the ride-hailing apps, I found it quite convenient to make reservations. During the investigation, both applications were observed to be user-friendly and easily accessible for trip bookings. Nice user ratings were given to both Taxi Stockholm (with a rating of 4.8 on Google Play) and Sverigetaxi (with a 4.6 rating). For authentication purposes, the input of a mobile number was required by both applications, and card details were requested for payment processing.

Furthermore, ethical considerations and privacy concerns were addressed, ensuring the protection of user data and the compliance to ethical research practices while dealing with digital evidence and user interaction, with a personal mobile device used on reserving the trips and on the investigation process. As part of my investigation, I examined the version of each ride-hailing application, assessed the available functionalities within each app, and documented the specific functionalities. The details are summarized in Table 2 and 3 below, providing an overview of the applications' capabilities during the investigation.

App	App version	Available functionalities
Sverigetaxi	3.16.4	- User Profiles - Pre-Book a Taxi - Travel Now (Immediate Booking) -Add Payment Methods (PayPal or Card) - Pay by card or PayPal directly in the app - Get status updates for the trip - Check Fixed price on all trips - Add Favorite Locations - Taxi Card Integration for Discounts - Travel from-to Selection to Book a Trip

Table 2: Overview of Sverigetaxi ride-hailing app functionality

App	App version	Available functionalities
Taxi Stockholm	7.0.2	-User Profiles -Payment Method - Pre-book or book directly - Write a message to the driver - Pay by card, by taxi account or in the car - Choose a standard, large car, or business - Book pick-up via map or search by address -Bookings: Active bookings and Finished bookings

Table 3: Overview of Taxi Stockholm ride-hailing app functionality

To facilitate a comprehensive investigation of the Android device, the initial step involved securely backing up mobile data, using a variety of methods. The phone is set up to save its data regularly and automatically to the Google Account linked with the email used for the investigation (gebrethesis@gmail.com). This arrangement ensures a safe and reliable backup for the data. With this system, all important information is consistently and continuously protected, making sure the data remains secure and accessible during the investigation. Data preservation was further strengthened using a PhoneTrans application. The utilization of diverse data preservation techniques not only safeguards data availability but also reinforces the credibility of the data source, offering redundancy, data verification, and the ability to perform comparative analysis for more robust and reliable forensic investigations.

The Oneplus 5T with the model Oneplus A5010 and running on Android version 10, served as the device for this study, as outlined in Table 1. To gain privileged access the device was rooted first before doing the data extraction.

The following section details the root process and the tools used to achieve root access on the Oneplus 5T.

Rooting a device involves gaining privileged access to the Android operating system, allowing users to remove limitations imposed by the manufacturer and customize their device (Bialon, R. 2020). To gain privileged access for data extraction and analysis, the study conducted by Elsersy and his team (2023) underlines the necessity of rooting in the Android security context.

On rooting process for the Oneplus 5T, I initiated the procedure by activating Developer Options on the device. Navigating through "Settings," accessing "About phone," and tapping the "Build number" seven times which unlocked the Developer Mode (Android Developers, 2023). Within the Developer Options, I enable both "OEM unlocking" and "USB debugging". After downloading platform-tools, essential for the rooting process, which includes `adb,` `fastboot`, and `twrp,` alongside `Magisk,` I continued with the rooting procedure (Google, 2023).

Executing the rooting process involved the following steps:

1. I powered off the Oneplus 5T and accessed Fastboot mode by holding down the Volume Down button + Power button.

2. Connecting the device to my computer via USB, I opened a command prompt or terminal, navigating to the directory housing the TWRP image file.

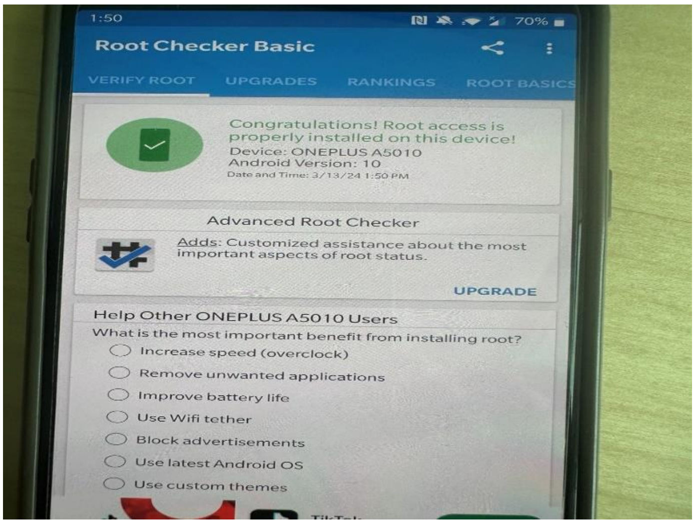
3. Executing the 'fastboot flash recovery twrp_filename.img' command, where 'twrp_filename.img' reflected the actual TWRP image file name, in this experiment ‘recovery.img’ facilitated the successful flashing of TWRP.

4. Using hardware buttons, I navigated to the "Recovery" option in the Fastboot menu and selected it, booting into TWRP.

5. Within TWRP, Magisk found its place on my device as I selected the Magisk zip file under the "Install" menu and confirmed the flash operation.

6. Post Magisk installation, I initiated a reboot of the device.

7. Upon the device’s restart, I verified the achievement of the rooting process by confirming the presence of Magisk Manager, evidence to the Oneplus 5T’s root access. The root access was also verified using a root checker app, as shown below in figure 3.



Congratulations! Root access is properly installed on this device!
Device: ONEPLUS A5010
Android Version: 10
Date and Time: 3/13/24 1:50 PM

Advanced Root Checker

Adds: Customized assistance about the most important aspects of root status.

Help Other ONEPLUS A5010 Users

What is the most important benefit from installing root?

○ Increase speed (overclock)
○ Remove unwanted applications
○ Improve battery life
○ Use Wifi tether
○ Block advertisements
○ Use latest Android OS
○ Use custom themes

Figure 3: Rooted oneplus 5T mobile

Forensic tools used for backup and rooting	Usage	Versions
Google drive	Backup	-
PhoneTrans	backup	5.0.1
Magisk	rooting	27.0
TWRP For Oneplus 5T	Used for Installing custom ROMs	3.5.1
Android Debug Bridge (Adb)	Enables Communication with Android devices from a computer over USB	1.0.41
Fastboot	Flashing partitions, installing custom software on Android devices via USB	34.0.4
Root checker	checks if an Android device has been rooted, confirming superuser access.	6.5.3

Table 4: Tools used for backup and rooting.

4.3 Forensic Data Acquisition

Data acquisition was conducted at CS2Lab, DSV, using the XRY tool developed MSAB. The XRY equipment used in this acquisition included four essential components:

1. A black physical XRY device facilitating the connection between the mobile device and the computer via a USB cable (refer to Figure 4).

2. A smaller gray USB stick containing the license key, inserted into the rear of the physical XRY device.

3. An acquisition program, also named "XRY," designed for Windows to communicate with the XRY device.

4. An analysis program titled "XAMN" for Windows, used for opening and analyzing files generated using the XRY program.

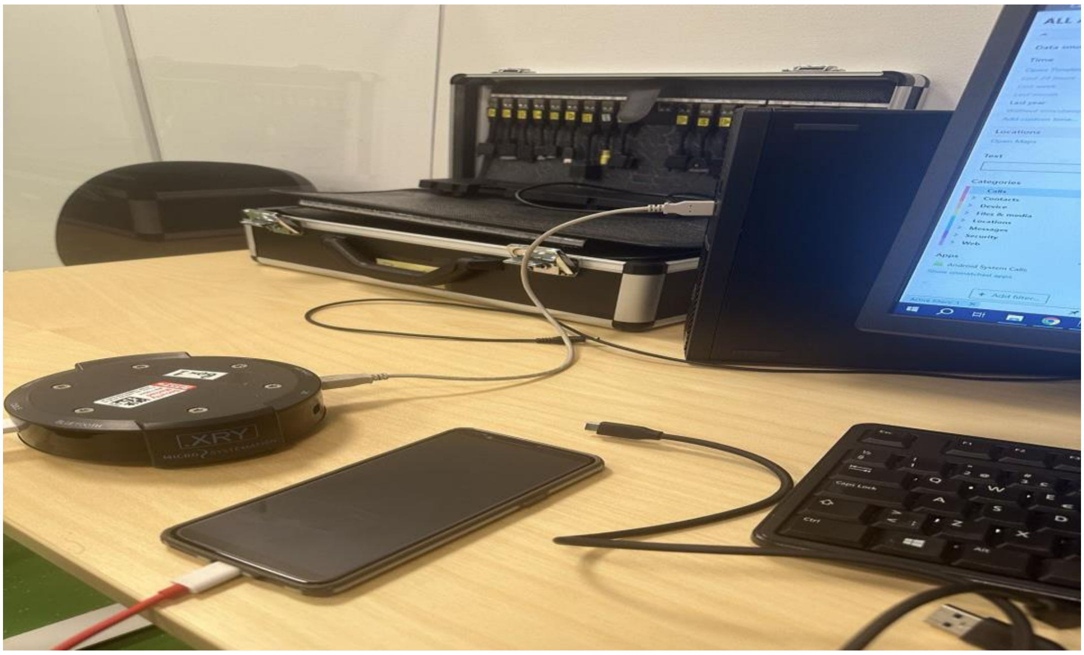


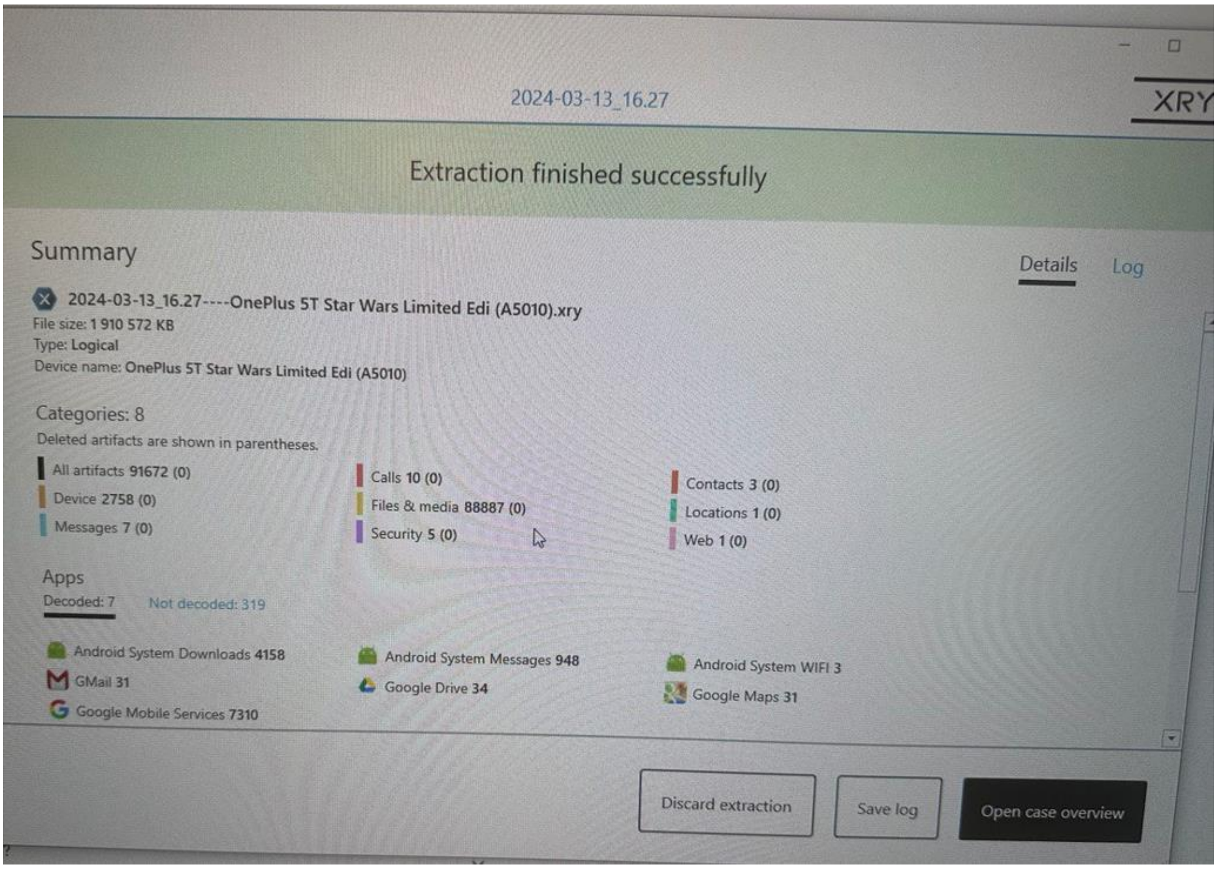
Figure 4: Digital experiment Setup

While physical acquisition was a possibility, a deliberate choice was made to select for logical acquisition. This selective approach prioritized the extraction of relevant artifacts over a comprehensive acquisition (Das, R. 2017). The main interest lies in the logical acquisition of data, ensuring the inclusion of all relevant artifacts. Version 10.6 of the `XRY` tool was used for this purpose. Extensive device compatibility is a notable factor in selecting `XRY` over alternative mobile forensic software for the data acquisition process. `XRY` supports data extraction for over 46,000 devices and over 4,500 app versions (MSAB, 2023). Moreover, the software can recover in-depth app profiles. Additionally, the presence of `XRY` in the DSV lab makes it easily accessible to me, further solidifying `XRY` as the ideal choice for my data acquisition needs.

To ensure data integrity, the hash sum `(SHA-256)` of the acquired file was generated to notice any alterations or tampering. Additionally, a copy of the extracted artifacts was stored on a Samsung portable `SSD T7` hard disk to mitigate the risk of data alteration during examination. This proactive measure not only preserves the integrity of the data but also aligns with `ISO 27037` standards (Ramadhan et al., 2022).

Tools for data Acquisition	Usage	Version
XRY	Employed for the logical acquisition of mobile devices	10.6.0

Table 5: Data acquisition tool



2024-03-13_16.27

Extraction finished successfully

Summary

2024-03-13_16.27----OnePlus 5T Star Wars Limited Edi (A5010).xry
File size: 1 910 572 KB
Type: Logical
Device name: OnePlus 5T Star Wars Limited Edi (A5010)

Categories: 8
Deleted artifacts are shown in parentheses.

All artifacts 91672 (0)	Calls 10 (0)	Contacts 3 (0)
Device 2758 (0)	Files & media 88887 (0)	Locations 1 (0)
Messages 7 (0)	Security 5 (0)	Web 1 (0)

Apps
Decoded: 7 Not decoded: 319

Android System Downloads 4158	Android System Messages 948	Android System WIFI 3
GMail 31	Google Drive 34	Google Maps 31
Google Mobile Services 7310		

Figure 5: Data Acquisition using XRY

4.4 Forensic Examination and Analysis

The forensic analysis of acquired data involved a comprehensive suite of tools, each serving a specific purpose in uncovering insights from the artifacts generated during the data acquisition process. One such instrumental tool was XAMN which played a central role in providing a user-friendly interface for the examination of digital evidence (MSAB,2024). Its capabilities extended to efficiently parsing and organizing data, facilitating a thorough understanding of the information extracted.

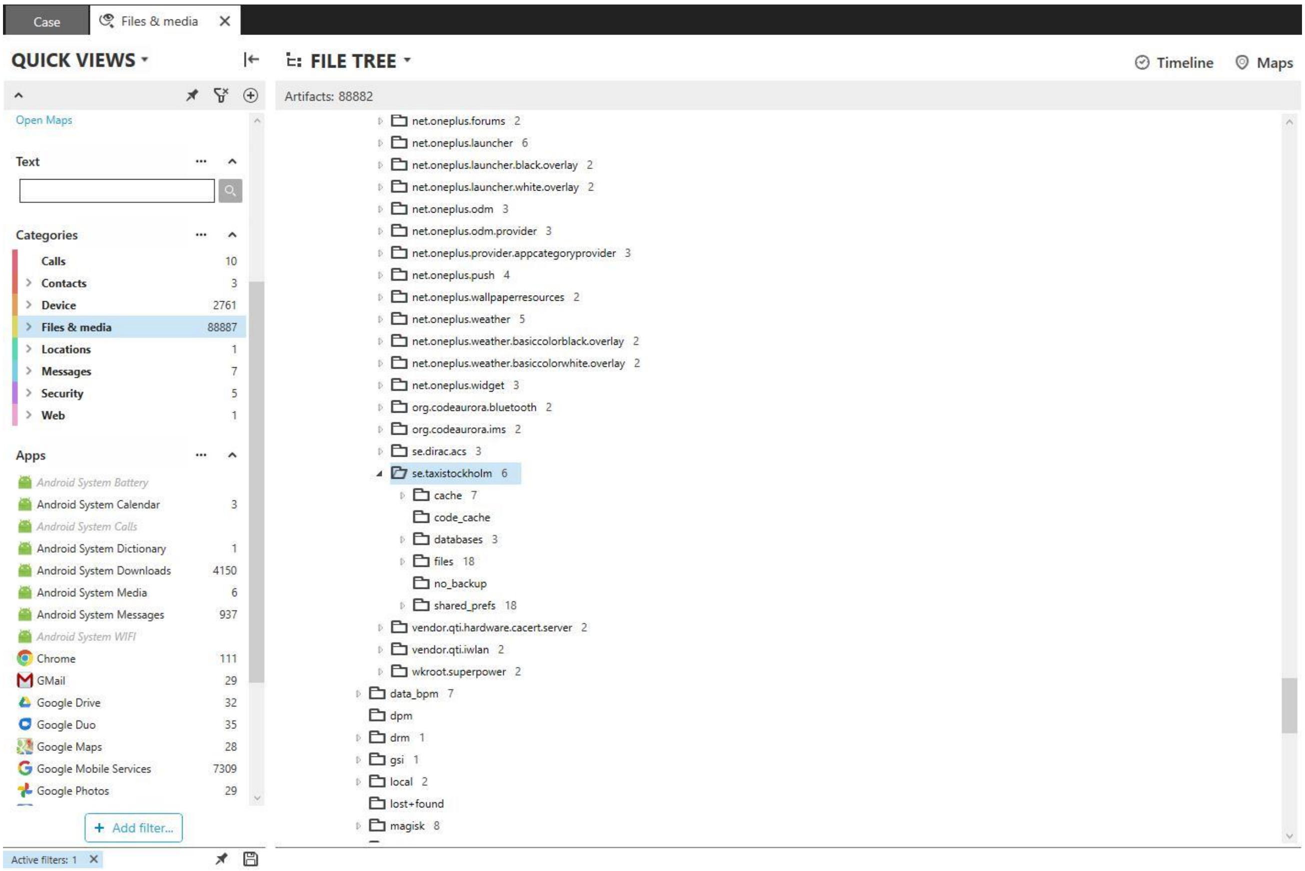
Additionally, the examination process used DB Browser for SQLite which was used for analyzing SQLite databases (Forensic Focus, 2018). This tool enabled investigators to navigate through structured data, query tables, and extract valuable information embedded within the databases (Schmitt et al., 2018). The forensic tool HxD Hex editor is used to parse artifacts with unknown or without file extensions (Warlock, 2018). This tool played a key role in inspecting file structures and identifying patterns in raw data. The detailed hexadecimal representation facilitated the identification of hidden information, enhancing forensic insights. Notepad++ served as a text editor during the forensic analysis (Forensafe, 2022). Its features, such as syntax highlighting and powerful search capabilities, made it a relevant tool in reviewing and interpreting textual artifacts. Notepad++ provided a user-friendly environment to examine logs, XML files, configuration files, and other text-based content, aiding in the identification of relevant artifacts.

After the artifacts were extracted using XRY they were open with XAMN for analysis and view. The XAMN viewer enabled the visualization of artifacts with various filtering options and a 'quick viewer'. The analysis included artifacts from different categories such as calls, messages, files and media, web, places, and contacts. Furthermore, artifacts relevant to the study undertook a detailed examination, investigating each section using XAMN and other tools for both ride-hailing applications. XAMN offered multiple ways to present extracted data, including "File Tree," "Column," "Gallery," and "List" views. These different ways of presenting the extracted artifact provided flexibility in exploring and interpreting the digital evidence. The filtering capabilities within XAMN, combined with the "quick show" feature and varied data presentation views, make it easy for in-depth analysis, allowing for a more rationalized and focused examination of the digital evidence. The artifacts generated were also examined by selecting different time intervals to provide a more focused look into the artifacts generated within specific time frames. For example, it was possible to analyze artifacts generated within the last 24 hours, last week, last month, last year, or artifacts with timestamps and without timestamps, providing insights into user activities during targeted periods.

Despite conducting a full logical acquisition, the primary data that aligned with addressing the research questions and objectives, was stored on the "Oneplus 5T/data/data/" directory for both ride-hailing applications, namely 'com.cabonline.taxi020' and 'se.taxistockholm'. Within the 'se.taxistockholm' subdirectory, a list of folders containing various files was extracted, namely cache, code_cache, databases, files, no_backup, and shared_prefs. Similarly, within the 'com.cabonline.taxi020' directory, similar folders as the earlier that contains various files were identified.

4.4.1 Taxi Stockholm and Sverigetaxi

The artifacts extracted from Taxi Stockholm were analyzed and examined with the tools mentioned below in table 6. First to simply visualize and see all possible artifacts and to know by which tools to see them the artifacts extracted from the taxi Stockholm was analyzed and viewed using XAMN as shown in a file tree shown in figure 6. The files found in the 'data/data/ se.taxistockholm' was examined with various tools. First the database files found in the 'databases' folder which includes the 'tsab.db' file were analyzed using DB Browser (SQLite). For a more in-depth analysis of timestamp data extracted from the database, a Python script was developed. This script helped the conversion of timestamps into a human-readable format, providing precise dates and months corresponding to when trips were completed. Such an approach aids in knowing the temporal aspects of the data, offering insights into the timing of various activities within the ride-hailing applications. To analysis the files found in the 'files', 'cache' and 'shared_prefs' folder of the taxi Stockholm app HxD Hex Editor and notepad++ application was used.



Artifacts: 88882

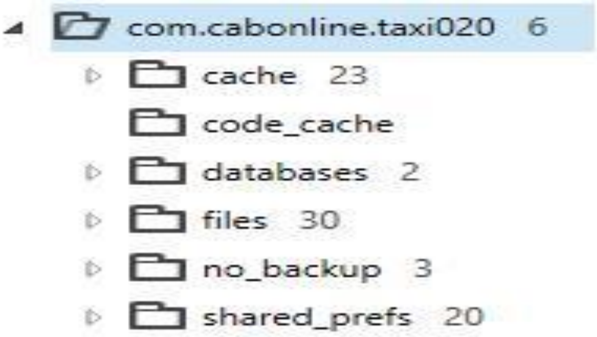
Calls 10
Contacts 3
Device 2761
Files & media 88887
Locations 1
Messages 7
Security 5
Web 1

Android System Battery
Android System Calendar 3
Android System Calls
Android System Dictionary 1
Android System Downloads 4150
Android System Media 6
Android System Messages 937
Android System WIFI
Chrome 111
GMail 29
Google Drive 32
Google Duo 35
Google Maps 28
Google Mobile Services 7309
Google Photos 29

```
net.oneplus.forums 2
net.oneplus.launcher 6
net.oneplus.launcher.black.overlay 2
net.oneplus.launcher.white.overlay 2
net.oneplus.odm 3
net.oneplus.odm.provider 3
net.oneplus.provider.appcategoryprovider 3
net.oneplus.push 4
net.oneplus.wallpaperresources 2
net.oneplus.weather 5
net.oneplus.weather.basiccolorblack.overlay 2
net.oneplus.weather.basiccolorwhite.overlay 2
net.oneplus.widget 3
org.codeaurora.bluetooth 2
org.codeaurora.ims 2
se.dirac.acs 3
se.taxistockholm 6
    cache 7
    code_cache
    databases 3
    files 18
    no_backup
    shared_prefs 18
vendor.qti.hardware.cacert.server 2
vendor.qti.iwlan 2
wkroot.superpower 2
data_bpm 7
dpm
drm 1
gsi 1
local 2
lost+found
magisk 8
```

Figure 6: Extracted artifacts on XAMN view for Taxi stockholm

The artifacts extracted from `SverigeTaxi` were analysis and examination using the tools outlined in Table 6, similar to the approach taken with `Taxi Stockholm`. Additionally, after analyzing and viewing the artifacts from the ‘`cache`’ folder of both Taxi Stockholm and SverigeTaxi, a simple Python script was developed for further analysis (Ranjan et al., 2023). The primary motivation behind developing the Python script was to avoid using online tools to uphold data integrity and privacy. To examine the cache, initially, the content was viewed using `HxD Hex Editor (HxD)`. To present it in a human-readable format, a Python script was used to facilitate the conversion of a file format to JSON format.



```
com.cabonline.taxi020 6
    cache 23
    code_cache
    databases 2
    files 30
    no_backup 3
    shared_prefs 20
```

Figure 7: Extracted artifacts on XAMN view for Sverigetaxi (Cabonline)

Tools used for forensic analysis	Usage	Version
XAMN	Analyzing device images to extract and interpret digital evidence.	7.8.0
DB Browser for SQLite	Parsing database files, enabling structured examination and extraction of relevant data.	3.12.2
HxD Hex editor	Analyzing files with unknown or no file extensions, exploring their hexadecimal structure.	2.5.0.0
Notepad ++	Reviewing and interpreting XML files to extract meaningful information.	8.5.2
Python	To write scripts to change some file to Json format	3.12.1

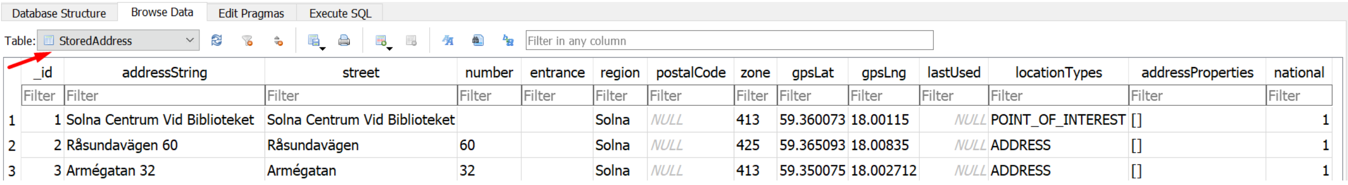
Table 6: forensic analysis tools

5 Results

The study aimed to investigate the forensic recovery of digital artifacts from the ride-hailing apps `Taxi Stockholm` and `SverigeTaxi`. The acquired data have been analyzed using various forensic tools, as discussed in the forensic examination and analysis section. The research outcomes are detailed in the following sections.

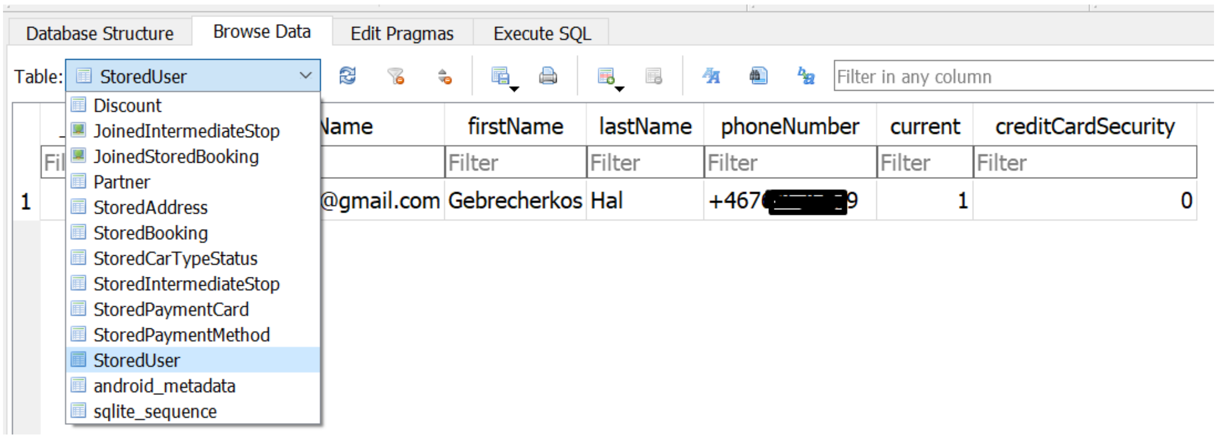
5.1 Taxi Stockholm

Relevant artifacts from Taxi Stockholm were found within the subdirectory `'Oneplus 5T/data/data/se.taxistockholm/'`. From the '**databases**' folder of the se.taxistockholm database, files specifically named ‘`tsab.db`’, ‘`google_app_measurement_local.db`’, and ‘`com.google.android.datatransport.events`’ were extracted. Although no relevant artifacts were extracted from the remaining database files, the ‘`tsab.db`’ database file resulted various artifacts including user first name, last name, phone number, user ID, credit card details, timestamp, GPS Coordinates, trip payment invoice, vehicle number, and vehicle plate number. These artifacts are demonstrated through the tables shown in the figures listed below using DB Browser (SQLite).



	_id	addressString	street	number	entrance	region	postalCode	zone	gpsLat	gpsLng	lastUsed	locationTypes	addressProperties	national
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	Solna Centrum Vid Biblioteket	Solna Centrum Vid Biblioteket			Solna	NULL	413	59.360073	18.00115	NULL	POINT_OF_INTEREST	[]	1
2	2	Råsundavägen 60	Råsundavägen	60		Solna	NULL	425	59.365093	18.00835	NULL	ADDRESS	[]	1
3	3	Armégatan 32	Armégatan	32		Solna	NULL	413	59.350075	18.002712	NULL	ADDRESS	[]	1

Figure 8: Details of Stored Address Table



	Name	firstName	lastName	phoneNumber	current	creditCardSecurity
		Filter	Filter	Filter	Filter	Filter
1	@gmail.com	Gebrecherkos	Hal	+467[redacted]9	1	0

Figure 9: tsab.db database table overview and StoredUser table data

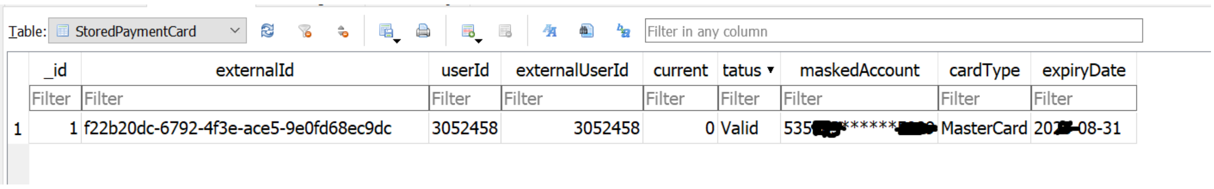


Table: StoredPaymentCard

	_id	externalId	userId	externalUserId	current	tatus	maskedAccount	cardType	expiryDate
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	f22b20dc-6792-4f3e-ace5-9e0fd68ec9dc	3052458	3052458	0	Valid	535[redacted]******[redacted]	MasterCard	202[redacted]-08-31

Figure 10: Stored payment card table

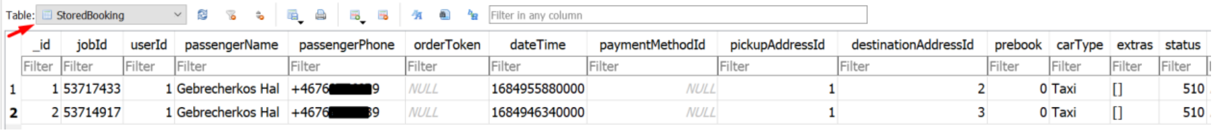
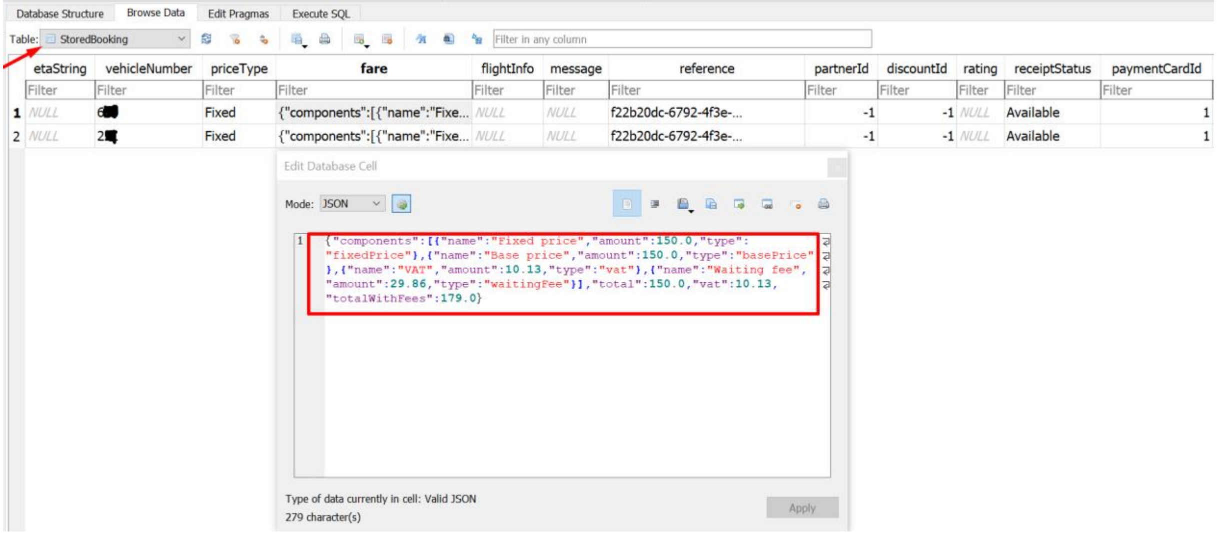


Table: StoredBooking

	_id	jobId	userId	passengerName	passengerPhone	orderToken	dateTime	paymentMethodId	pickupAddressId	destinationAddressId	prebook	carType	extras	status
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	53717433	1	Gebrecherkos Hal	+4676[redacted]9	NULL	1684955880000	NULL	1	2	0	Taxi	[]	510
2	2	53714917	1	Gebrecherkos Hal	+4676[redacted]9	NULL	1684946340000	NULL	1	3	0	Taxi	[]	510

Figure 11: Stored booking table - Part 1



Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: StoredBooking

	etaString	vehicleNumber	priceType	fare	flightInfo	message	reference	partnerId	discountId	rating	receiptStatus	paymentCardId
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	NULL	6[redacted]	Fixed	{"components":[{"name":"Fixe...	NULL	NULL	f22b20dc-6792-4f3e-...	-1	-1	NULL	Available	1
2	NULL	2[redacted]	Fixed	{"components":[{"name":"Fixe...	NULL	NULL	f22b20dc-6792-4f3e-...	-1	-1	NULL	Available	1

Edit Database Cell

Mode: JSON

```
{"components":[{"name":"Fixed price","amount":150.0,"type":
"fixedPrice"},{"name":"Base price","amount":150.0,"type":"basePrice"
},{"name":"VAT","amount":10.13,"type":"vat"},{"name":"Waiting fee",
"amount":29.86,"type":"waitingFee"}],"total":150.0,"vat":10.13,
"totalWithFees":179.0}
```

Type of data currently in cell: Valid JSON
279 character(s)

Figure12: Stored booking table - Part 2

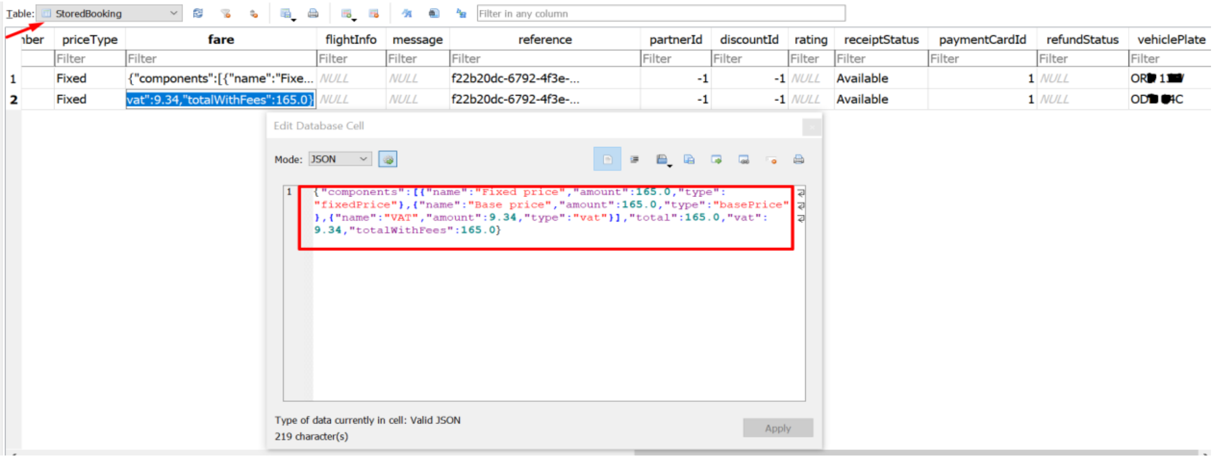


Table: StoredBooking

	ıber	priceType	fare	flightInfo	message	reference	partnerId	discountId	rating	receiptStatus	paymentCardId	refundStatus	vehiclePlate
		Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1		Fixed	{"components":[{"name":"Fixe...	NULL	NULL	f22b20dc-6792-4f3e-...	-1	-1	NULL	Available	1	NULL	OR[redacted] 1[redacted]
2		Fixed	vat":9.34,"totalWithFees":165.0}	NULL	NULL	f22b20dc-6792-4f3e-...	-1	-1	NULL	Available	1	NULL	OD[redacted] [redacted]C

Edit Database Cell

Mode: JSON

```
{"components":[{"name":"Fixed price","amount":165.0,"type":
"fixedPrice"},{"name":"Base price","amount":165.0,"type":"basePrice"
},{"name":"VAT","amount":9.34,"type":"vat"}],"total":165.0,"vat":
9.34,"totalWithFees":165.0}
```

Type of data currently in cell: Valid JSON
219 character(s)

Figure 13: Stored booking table - Part 3

Python script was used to convert timestamps into a human-readable format, allowing for precise determination of the date and time when each trip occurred (see figure 11). The converted timestamps, '1684955880000' and '1684946340000', correspond to the exact dates and times of the trips: May 24, 2023, at 19:18:00 UTC and 16:39:00 UTC, respectively.

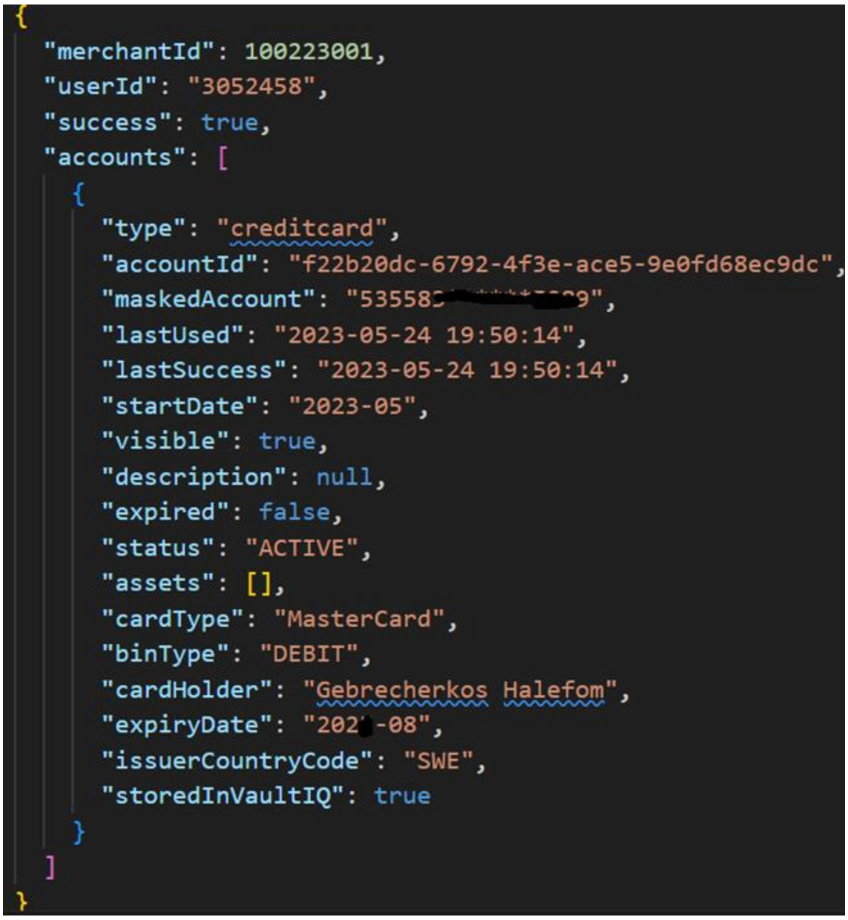
In investigation's continuation, among the files found in the 'files' section under [1] the 'userlog' file was examined. This file reveals activities such as 'StartupActivity', 'SignupActivity', and 'OnboardingActivity' which verifies what activities was the user doing.

In the se.taxistockholm**shared_prefs** folder, various XML files were discovered, containing settings, configurations, and user preferences. While examining these files could provide insights into user behavior, preferences, and interactions, the detailed investigation of these preferences falls outside the scope of this study.

In the [2] directory, the file 'embedded_GZip_1' contains data indicating the last usage and successful payment transactions. The data structure includes information such as the merchant ID, user ID, success status, and details of the payment method used. For instance, it reveals the credit card number, the last usage timestamp, and the date of the last successful transaction. The JSON representation of this file can be shown in Figure 14.

[1] *se.taxistockholm\**files**\\.com.google.firebase.crashlytics.files.v2se.taxistockholm\\open-sessions\\65F1A65A01E000013910658EEFC14241*

[2] *se.taxistockholm\**cache**\\79d70c17d5e1b374451b42d1298a114a.1.dir*

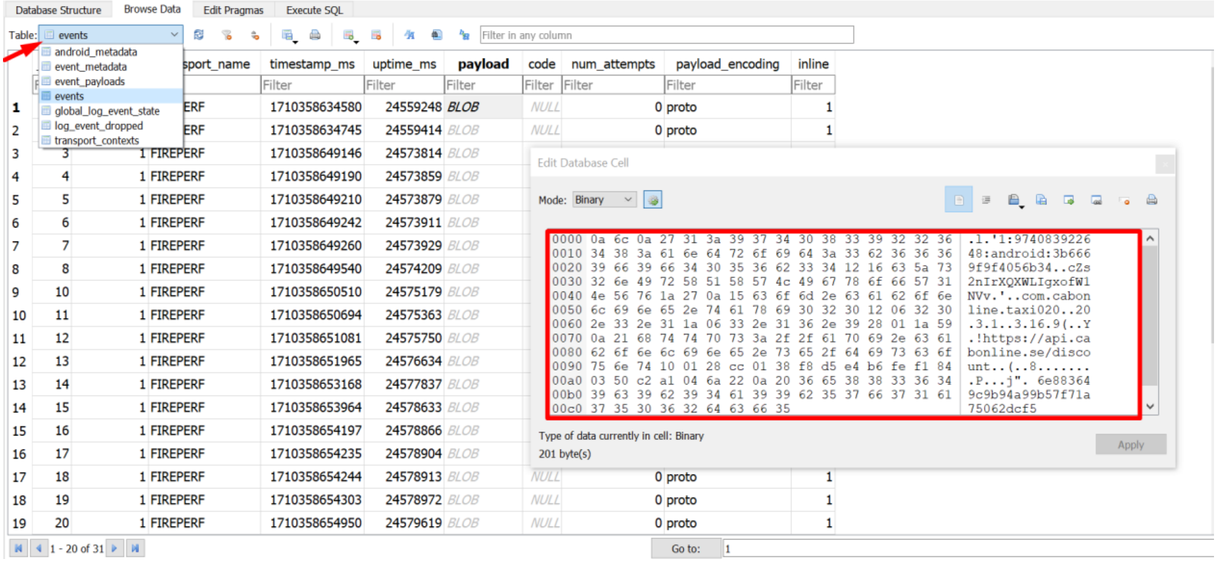


```
{
  "merchantId": 100223001,
  "userId": "3052458",
  "success": true,
  "accounts": [
    {
      "type": "creditcard",
      "accountId": "f22b20dc-6792-4f3e-ace5-9e0fd68ec9dc",
      "maskedAccount": "53558[redacted]9",
      "lastUsed": "2023-05-24 19:50:14",
      "lastSuccess": "2023-05-24 19:50:14",
      "startDate": "2023-05",
      "visible": true,
      "description": null,
      "expired": false,
      "status": "ACTIVE",
      "assets": [],
      "cardType": "MasterCard",
      "binType": "DEBIT",
      "cardHolder": "Gebrecherkos Halefom",
      "expiryDate": "202[redacted]-08",
      "issuerCountryCode": "SWE",
      "storedInVaultIQ": true
    }
  ]
}
```

Figure 14: Payment transaction details in JSON format

5.2 Sverigetaxi

In the directory 'Oneplus 5T/data/data/com.cabonline.taxi020**databases**', two files were extracted: '`com.google.android.datatransport.events`' and 'google_app_measurement_local.db'. Upon examination of '`google_app_measurement_local.db`', it was noted that it contained two tables. However, no actual data was present on the tables. This indicates that, although the database structure was present, the tables did not contain any tangible information. Further analysis may be required to ascertain the reasons behind this absence of data. However, the '`com.google.android.datatransport.events`' contained tables such as "`events`," which holds a log file including numerous entries. Each entry details events related to the app's data transport system, providing timestamps, payload information, event codes, and other relevant metadata.



			sport_name	timestamp_ms	uptime_ms	payload	code	num_attempts	payload_encoding	inline
				Filter	Filter	Filter	Filter	Filter	Filter	Filter
1			ERF	1710358634580	24559248	BLOB	NULL	0	proto	1
2			ERF	1710358634745	24559414	BLOB	NULL	0	proto	1
3	3	1	FIREPERF	1710358649146	24573814	BLOB				
4	4	1	FIREPERF	1710358649190	24573859	BLOB				
5	5	1	FIREPERF	1710358649210	24573879	BLOB				
6	6	1	FIREPERF	1710358649242	24573911	BLOB				
7	7	1	FIREPERF	1710358649260	24573929	BLOB				
8	8	1	FIREPERF	1710358649540	24574209	BLOB				
9	10	1	FIREPERF	1710358650510	24575179	BLOB				
10	11	1	FIREPERF	1710358650694	24575363	BLOB				
11	12	1	FIREPERF	1710358651081	24575750	BLOB				
12	13	1	FIREPERF	1710358651965	24576634	BLOB				
13	14	1	FIREPERF	1710358653168	24577837	BLOB				
14	15	1	FIREPERF	1710358653964	24578633	BLOB				
15	16	1	FIREPERF	1710358654197	24578866	BLOB				
16	17	1	FIREPERF	1710358654235	24578904	BLOB				
17	18	1	FIREPERF	1710358654244	24578913	BLOB	NULL	0	proto	1
18	19	1	FIREPERF	1710358654303	24578972	BLOB	NULL	0	proto	1
19	20	1	FIREPERF	1710358654950	24579619	BLOB	NULL	0	proto	1

1 - 20 of 31

Go to: 1

Edit Database Cell

Mode: Binary

```
0000 0a 6c 0a 27 31 3a 39 37 34 30 38 33 39 32 32 36  .l.'1:9740839226
0010 34 38 3a 61 6e 64 72 6f 69 64 3a 33 62 36 36 36  48:android:3b666
0020 39 66 39 66 34 30 35 36 62 33 34 12 16 63 5a 73  9f9f4056b34..cZs
0030 32 6e 49 72 58 51 58 57 4c 49 67 78 6f 66 57 31  2nIrXQXWLIgxofW1
0040 4e 56 76 1a 27 0a 15 63 6f 6d 2e 63 61 62 6f 6e  NVv.'..com.cabon
0050 6c 69 6e 65 2e 74 61 78 69 30 32 30 12 06 32 30  line.taxi020..20
0060 2e 33 2e 31 1a 06 33 2e 31 36 2e 39 28 01 1a 59  .3.1..3.16.9(..Y
0070 0a 21 68 74 74 70 73 3a 2f 2f 61 70 69 2e 63 61  .!https://api.ca
0080 62 6f 6e 6c 69 6e 65 2e 73 65 2f 64 69 73 63 6f  bonline.se/disco
0090 75 6e 74 10 01 28 cc 01 38 f8 d5 e4 b6 fe f1 84  unt..(..8.......
00a0 03 50 c2 a1 04 6a 22 0a 20 36 65 38 38 33 36 34  .P...j". 6e88364
00b0 39 63 39 62 39 34 61 39 39 62 35 37 66 37 31 61  9c9b94a99b57f71a
00c0 37 35 30 36 32 64 63 66 35                       75062dcf5
```

Type of data currently in cell: Binary
201 byte(s)

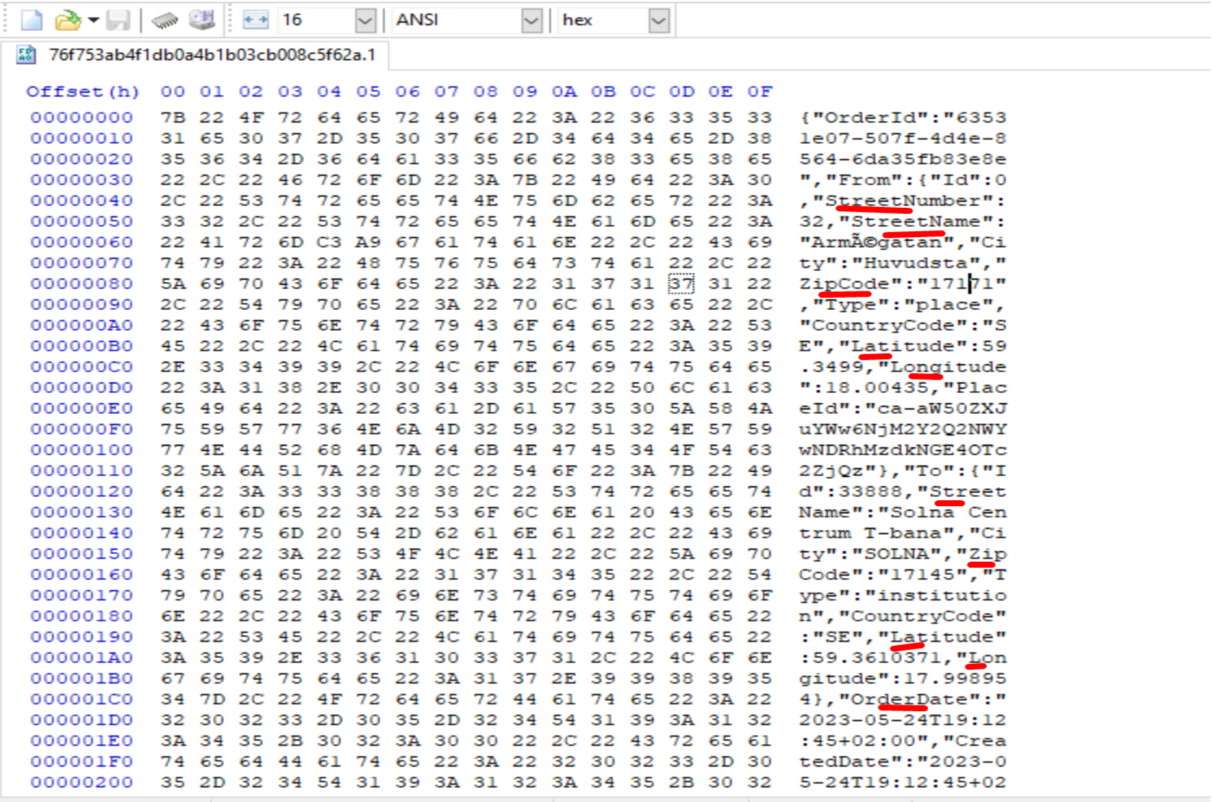
Figure 15: data transport events table

In addition to the discoveries in the databases directory, a significant number of artifacts were found in the 'com.cabonline.taxi020**cache**' directory. Various artifacts were discovered in different files within each cache file. After examining two of the cache files, namely EN4 and [3], multiple artifacts were extracted. Notably, the details of the artifacts found in the file named EN3 were a subset of the file named EN4. These extracted artifacts include VehicleModel, Vehicle RegistrationNumber, VehicleManufacturer, Driver ID, VehicleId, Phone number of the user and the driver, driver Gmail address, user Gmail name, Credit card details, trip fee, User First name and last name, timestamp, Start and end trip GPS Coordinates.

These artifacts serve as crucial evidence that could be used in a court of law. They provide detailed insights into the trip, including vehicle details, driver information, user data, payment details, and trip specifics. Forensically, these artifacts are considered sound and reliable, as they are extracted directly from the application's cache directory, ensuring data integrity and authenticity. Furthermore, they can be used to reconstruct and analyze the sequence of events leading up to and during the trip, assisting in investigations and legal proceedings.

Below is the full JSON format of the file EN4, preceded by the figure displaying the first few rows of data of both cache files using HxD. Some of the data in the JSON format was replaced by * to hide certain portions of the data for privacy or security reasons.

[3] *028447d0a52f50148751b9386d49c0f7.1*

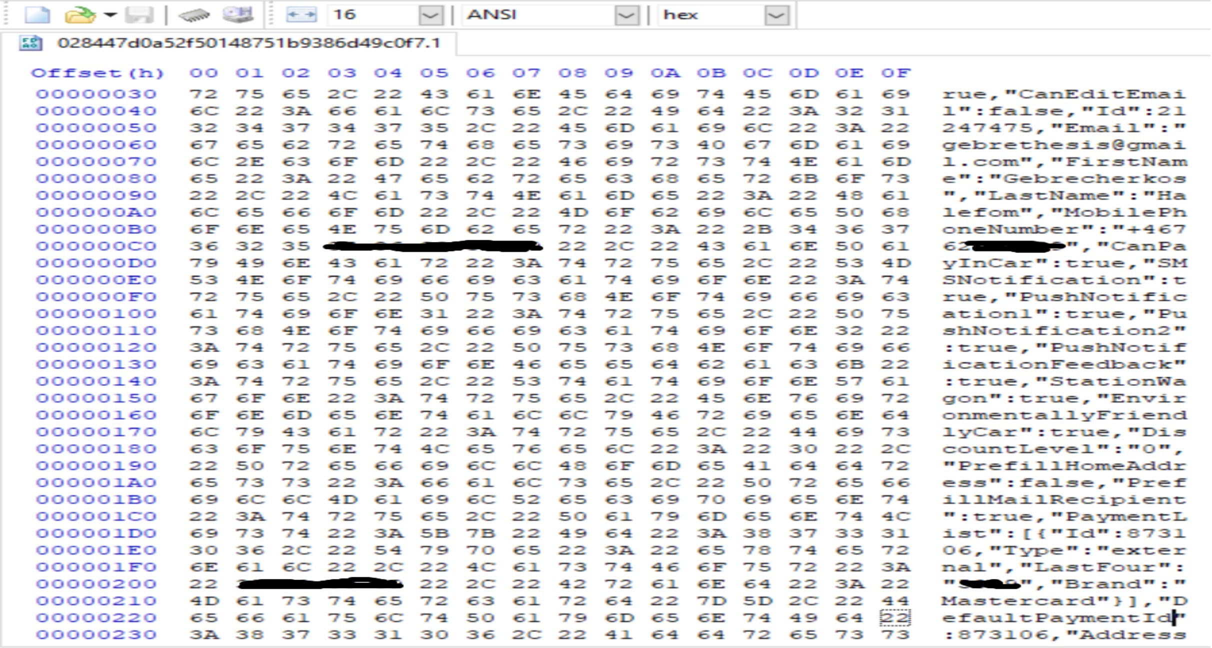


```
76f753ab4f1db0a4b1b03cb008c5f62a.1

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  7B 22 4F 72 64 65 72 49 64 22 3A 22 36 33 35 33  {"OrderId":"6353
00000010  31 65 30 37 2D 35 30 37 66 2D 34 64 34 65 2D 38  1e07-507f-4d4e-8
00000020  35 36 34 2D 36 64 61 33 35 66 62 38 33 65 38 65  564-6da35fb83e8e
00000030  22 2C 22 46 72 6F 6D 22 3A 7B 22 49 64 22 3A 30  ","From":{"Id":0
00000040  2C 22 53 74 72 65 65 74 4E 75 6D 62 65 72 22 3A  ,"StreetNumber":
00000050  33 32 2C 22 53 74 72 65 65 74 4E 61 6D 65 22 3A  32,"StreetName":
00000060  22 41 72 6D C3 A9 67 61 74 61 6E 22 2C 22 43 69  "ArmÃ©gatan","Ci
00000070  74 79 22 3A 22 48 75 76 75 64 73 74 61 22 2C 22  ty":"Huvudsta","
00000080  5A 69 70 43 6F 64 65 22 3A 22 31 37 31 37 31 22  ZipCode":"17171"
00000090  2C 22 54 79 70 65 22 3A 22 70 6C 61 63 65 22 2C  ,"Type":"place",
000000A0  22 43 6F 75 6E 74 72 79 43 6F 64 65 22 3A 22 53  "CountryCode":"S
000000B0  45 22 2C 22 4C 61 74 69 74 75 64 65 22 3A 35 39  E","Latitude":59
000000C0  2E 33 34 39 39 2C 22 4C 6F 6E 67 69 74 75 64 65  .3499,"Longitude
000000D0  22 3A 31 38 2E 30 30 34 33 35 2C 22 50 6C 61 63  ":18.00435,"Plac
000000E0  65 49 64 22 3A 22 63 61 2D 61 57 35 30 5A 58 4A  eId":"ca-aW50ZXJ
000000F0  75 59 57 77 36 4E 6A 4D 32 59 32 51 32 4E 57 59  uYWw6NjM2Y2Q2NWY
00000100  77 4E 44 52 68 4D 7A 64 6B 4E 47 45 34 4F 54 63  wNDRhMzdkNGE4OTc
00000110  32 5A 6A 51 7A 22 7D 2C 22 54 6F 22 3A 7B 22 49  2ZjQz"},"To":{"I
00000120  64 22 3A 33 33 38 38 38 2C 22 53 74 72 65 65 74  d":33888,"Street
00000130  4E 61 6D 65 22 3A 22 53 6F 6C 6E 61 20 43 65 6E  Name":"Solna Cen
00000140  74 72 75 6D 20 54 2D 62 61 6E 61 22 2C 22 43 69  trum T-bana","Ci
00000150  74 79 22 3A 22 53 4F 4C 4E 41 22 2C 22 5A 69 70  ty":"SOLNA","Zip
00000160  43 6F 64 65 22 3A 22 31 37 31 34 35 22 2C 22 54  Code":"17145","T
00000170  79 70 65 22 3A 22 69 6E 73 74 69 74 75 74 69 6F  ype":"institutio
00000180  6E 22 2C 22 43 6F 75 6E 74 72 79 43 6F 64 65 22  n","CountryCode"
00000190  3A 22 53 45 22 2C 22 4C 61 74 69 74 75 64 65 22  :"SE","Latitude"
000001A0  3A 35 39 2E 33 36 31 30 33 37 31 2C 22 4C 6F 6E  :59.3610371,"Lon
000001B0  67 69 74 75 64 65 22 3A 31 37 2E 39 39 38 39 35  gitude":17.99895
000001C0  34 7D 2C 22 4F 72 64 65 72 44 61 74 65 22 3A 22  4},"OrderDate":"
000001D0  32 30 32 33 2D 30 35 2D 32 34 54 31 39 3A 31 32  2023-05-24T19:12
000001E0  3A 34 35 2B 30 32 3A 30 30 22 2C 22 43 72 65 61  :45+02:00","Crea
000001F0  74 65 64 44 61 74 65 22 3A 22 32 30 32 33 2D 30  tedDate":"2023-0
00000200  35 2D 32 34 54 31 39 3A 31 32 3A 34 35 2B 30 32  5-24T19:12:45+02
```

Figure 16: cache file [4] data



```
028447d0a52f50148751b9386d49c0f7.1

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000030  72 75 65 2C 22 43 61 6E 45 64 69 74 45 6D 61 69  rue,"CanEditEmai
00000040  6C 22 3A 66 61 6C 73 65 2C 22 49 64 22 3A 32 31  l":false,"Id":21
00000050  32 34 37 34 37 35 2C 22 45 6D 61 69 6C 22 3A 22  247475,"Email":"
00000060  67 65 62 72 65 74 68 65 73 69 73 40 67 6D 61 69  gebrethesis@gmai
00000070  6C 2E 63 6F 6D 22 2C 22 46 69 72 73 74 4E 61 6D  l.com","FirstNam
00000080  65 22 3A 22 47 65 62 72 65 63 68 65 72 6B 6F 73  e":"Gebrecherkos
00000090  22 2C 22 4C 61 73 74 4E 61 6D 65 22 3A 22 48 61  ","LastName":"Ha
000000A0  6C 65 66 6F 6D 22 2C 22 4D 6F 62 69 6C 65 50 68  lefom","MobilePh
000000B0  6F 6E 65 4E 75 6D 62 65 72 22 3A 22 2B 34 36 37  oneNumber":"+467
000000C0  36 32 35 [redacted] 22 2C 22 43 61 6E 50 61  62[redacted]","CanPa
000000D0  79 49 6E 43 61 72 22 3A 74 72 75 65 2C 22 53 4D  yInCar":true,"SM
000000E0  53 4E 6F 74 69 66 69 63 61 74 69 6F 6E 22 3A 74  SNotification":t
000000F0  72 75 65 2C 22 50 75 73 68 4E 6F 74 69 66 69 63  rue,"PushNotific
00000100  61 74 69 6F 6E 31 22 3A 74 72 75 65 2C 22 50 75  ation1":true,"Pu
00000110  73 68 4E 6F 74 69 66 69 63 61 74 69 6F 6E 32 22  shNotification2"
00000120  3A 74 72 75 65 2C 22 50 75 73 68 4E 6F 74 69 66  :true,"PushNotif
00000130  69 63 61 74 69 6F 6E 46 65 65 64 62 61 63 6B 22  icationFeedback"
00000140  3A 74 72 75 65 2C 22 53 74 61 74 69 6F 6E 57 61  :true,"StationWa
00000150  67 6F 6E 22 3A 74 72 75 65 2C 22 45 6E 76 69 72  gon":true,"Envir
00000160  6F 6E 6D 65 6E 74 61 6C 6C 79 46 72 69 65 6E 64  onmentallyFriend
00000170  6C 79 43 61 72 22 3A 74 72 75 65 2C 22 44 69 73  lyCar":true,"Dis
00000180  63 6F 75 6E 74 4C 65 76 65 6C 22 3A 22 30 22 2C  countLevel":"0",
00000190  22 50 72 65 66 69 6C 6C 48 6F 6D 65 41 64 64 72  "PrefillHomeAddr
000001A0  65 73 73 22 3A 66 61 6C 73 65 2C 22 50 72 65 66  ess":false,"Pref
000001B0  69 6C 6C 4D 61 69 6C 52 65 63 69 70 69 65 6E 74  illMailRecipient
000001C0  22 3A 74 72 75 65 2C 22 50 61 79 6D 65 6E 74 4C  ":true,"PaymentL
000001D0  69 73 74 22 3A 5B 7B 22 49 64 22 3A 38 37 33 31  ist":[{"Id":8731
000001E0  30 36 2C 22 54 79 70 65 22 3A 22 65 78 74 65 72  06,"Type":"exter
000001F0  6E 61 6C 22 2C 22 4C 61 73 74 46 6F 75 72 22 3A  nal","LastFour":
00000200  22 [redacted] 22 2C 22 42 72 61 6E 64 22 3A 22  "[redacted]","Brand":"
00000210  4D 61 73 74 65 72 63 61 72 64 22 7D 5D 2C 22 44  Mastercard"}],"D
00000220  65 66 61 75 6C 74 50 61 79 6D 65 6E 74 49 64 22  efaultPaymentId"
00000230  3A 38 37 33 31 30 36 2C 22 41 64 64 72 65 73 73  :873106,"Address
```

Figure 17: cache file EN3 data

[4] 76f753ab4f1db0a4b1b03cb008c5f62a.1

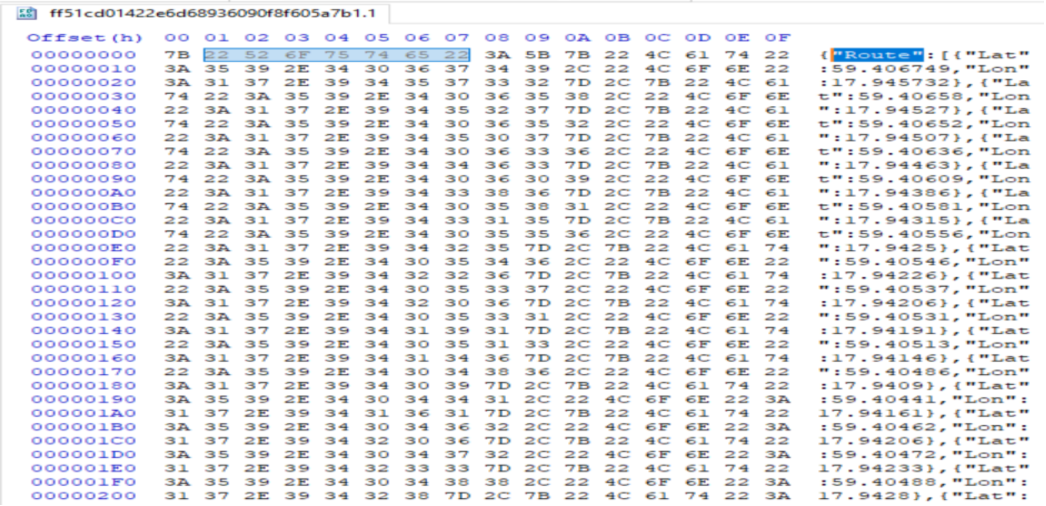
JSON Format of EN4:

```
{
"OrderId": "63531e07-507f-4d4e-8564-6da35fb83e8e",
"From": {
"Id": 0,
"StreetNumber": 32,
"StreetName": "ArmÃ©gatan",
"City": "Huvudsta",
"ZipCode": "17171",
"Type": "place",
"CountryCode": "SE",
"Latitude": 59.3499,
"Longitude": 18.00435,
"PlaceId": "ca-aW50ZXJuYWw6NjM2Y2Q2NWYwNDRhMzdkNGE4OTc2ZjQz"},
"To": {
"Id": 33888,
"StreetName": "Solna Centrum T-bana",
"City": "SOLNA",
"ZipCode": "17145",
"Type": "institution",
"CountryCode": "SE",
"Latitude": 59.3610371,
"Longitude": 17.998954},
"OrderDate": "2023-05-24T19:12:45+02:00",
"CreatedDate": "2023-05-24T19:12:45+02:00",
"PickupTime": "2023-05-24T19:16:00+02:00",
"DestinationTime": "2023-05-24T19:30:00+02:00",
"BookedPickupTime": "2023-05-24T19:12:00+02:00",
"ActualPickupTime": "2023-05-24T19:16:00+02:00",
"ActualDestinationTime": "2023-05-24T19:30:00+02:00",
"Status": "completed",
"CanModify": false,
"CanLeaveFeedback": false,
"CanCancel": false,
"StationWagon": false,
"EnvironmentallyFriendlyCar": false,
"OrderAttributes": [],
"AllowRouting": false,
"PriceType": "fixed",
"Price": 169.0,
"Currency": "SEK",
"FirstName": "Gebrecherkos",
"LastName": "Halefom",
"MobilePhoneNumber": "+467625****9",
"VehicleETA": -1,
"VehicleETAInSeconds": -1,
"VehicleLatitude": 0,
"VehicleLongitude": 0,
"PaymentType": {
"Id": 873106,
"Type": "external",
"LastFour": "5**9",
"Brand": "Mastercard"},
"DeliveryCompanyInformation": [{
"Identifier": "LINK-020",
"Name": "Cabonline Stockholm",
"PhoneNr": "+4620202020",
"Status": "",
"VehicleId": "6**9",
"DriverId": "853**1",
"ShortName": "CABONLINE",
"Color": "",
"Email": "kundservice@cabonline.com",
"Driver": {
"Id": "853**1"},
"RegistrationNumber": "TEK**G",
"VehicleManufacturer": "SKODA",
"VehicleModel": "OCTAVIA"}],
"SMSNotification": false,
"EmailRecipients": [
"gebrethesis@gmail.com"],
"OrderAttributesV2": [ ],
"Product": {
"Product": {
"Id": "PRODUCT_STANDARD",
"Price": 0.0},
"SubProduct": {
"Id": "TAXI_DEFAULT",
"Price": 0.0 },
"Options": [ ]},
"PaymentReserved": true,
"IsTravelNow": true,
"PublicOrderId": "RQ3XV7AE",
"DiscountAmount": 0.0,
"FeeAmount": 0,
"BaseExcludingProduct": 169.0,
"Fees": {
"Provider": 0,
"Prebook": 0}}
```

The cache file named `950171d4026b8b01ffcae80d3d274f2a.1` provides wide-ranging details on available fleet options and their associated settings, illustrating the customization and flexibility offered to users during booking. Additionally, it indicates whether children or animals are permitted in the fleet used for the trip, thereby offering valuable insights into the service's policies concerning passenger eligibility and safety measures. On the other hand, cache file named `a4afc7cf43837e6d4606071ea30192b1.1` provides detailed latitude and longitude coordinates of waiting cars. It includes vehicle IDs, last updated timestamps, and direction information, offering insights into the real-time locations of the vehicles and their statuses. Particularly noteworthy is the particular documentation of timestamps including OrderDate, PickupTime, DestinationTime, BookedPickupTime, ActualPickupTime, and ActualDestinationTime. These timestamps explain the entire journey's timeline, enabling forensic investigators to reconstruct the sequence of events with precision. The indication of the trip's status as "completed" is particularly significant, as it signifies the conclusion of the ride. Such status markers serve as essential forensic artifacts, providing crucial insights into the completion status of the trip and potentially verifying or disproving claims made by involved parties.

In cache file EN5, a series of latitude and longitude coordinates outlining a route were identified. When plotted on Google Maps, these coordinates revealed various locations visited during travel, potentially indicating the app's tracking of user movements. route included locations such as Stockholm University, DSV Lab and the user's residence, suggesting that the app may retain location information. It's possible that such data collection serves to enhance user experience, although it also raises questions about the app's data usage policies. Nevertheless, the recorded routes be relevant in scenarios involving accidents, violence, or criminal activities, as they provide precise details of the routes taken during trips. This information goes beyond just the starting and ending points of journeys, offering insights into the specific paths traveled, which could be crucial for investigations and legal proceedings.

This figure shows the few latitude and longitude coordinates of a trip found in the cache named [5]



```
ff51cd01422e6d68936090f8f605a7b1.1

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  7B 22 52 6F 75 74 65 22 3A 5B 7B 22 4C 61 74 22  {"Route":[{"Lat"
00000010  3A 35 39 2E 34 30 36 37 34 39 2C 22 4C 6F 6E 22  :59.406749,"Lon"
00000020  3A 31 37 2E 39 34 35 37 33 32 7D 2C 7B 22 4C 61  :17.945732},{"La
00000030  74 22 3A 35 39 2E 34 30 36 35 38 2C 22 4C 6F 6E  t":59.40658,"Lon
00000040  22 3A 31 37 2E 39 34 35 32 37 7D 2C 7B 22 4C 61  ":17.94527},{"La
00000050  74 22 3A 35 39 2E 34 30 36 35 32 2C 22 4C 6F 6E  t":59.40652,"Lon
00000060  22 3A 31 37 2E 39 34 35 30 37 7D 2C 7B 22 4C 61  ":17.94507},{"La
00000070  74 22 3A 35 39 2E 34 30 36 33 36 2C 22 4C 6F 6E  t":59.40636,"Lon
00000080  22 3A 31 37 2E 39 34 34 36 33 7D 2C 7B 22 4C 61  ":17.94463},{"La
00000090  74 22 3A 35 39 2E 34 30 36 30 39 2C 22 4C 6F 6E  t":59.40609,"Lon
000000A0  22 3A 31 37 2E 39 34 33 38 36 7D 2C 7B 22 4C 61  ":17.94386},{"La
000000B0  74 22 3A 35 39 2E 34 30 35 38 31 2C 22 4C 6F 6E  t":59.40581,"Lon
000000C0  22 3A 31 37 2E 39 34 33 31 35 7D 2C 7B 22 4C 61  ":17.94315},{"La
000000D0  74 22 3A 35 39 2E 34 30 35 35 36 2C 22 4C 6F 6E  t":59.40556,"Lon
000000E0  22 3A 31 37 2E 39 34 32 35 7D 2C 7B 22 4C 61 74  ":17.9425},{"Lat
000000F0  22 3A 35 39 2E 34 30 35 34 36 2C 22 4C 6F 6E 22  ":59.40546,"Lon"
00000100  3A 31 37 2E 39 34 32 32 36 7D 2C 7B 22 4C 61 74  :17.94226},{"Lat
00000110  22 3A 35 39 2E 34 30 35 33 37 2C 22 4C 6F 6E 22  ":59.40537,"Lon"
00000120  3A 31 37 2E 39 34 32 30 36 7D 2C 7B 22 4C 61 74  :17.94206},{"Lat
00000130  22 3A 35 39 2E 34 30 35 33 31 2C 22 4C 6F 6E 22  ":59.40531,"Lon"
00000140  3A 31 37 2E 39 34 31 39 31 7D 2C 7B 22 4C 61 74  :17.94191},{"Lat
00000150  22 3A 35 39 2E 34 30 35 31 33 2C 22 4C 6F 6E 22  ":59.40513,"Lon"
00000160  3A 31 37 2E 39 34 31 34 36 7D 2C 7B 22 4C 61 74  :17.94146},{"Lat
00000170  22 3A 35 39 2E 34 30 34 38 36 2C 22 4C 6F 6E 22  ":59.40486,"Lon"
00000180  3A 31 37 2E 39 34 30 39 7D 2C 7B 22 4C 61 74 22  :17.9409},{"Lat"
00000190  3A 35 39 2E 34 30 34 34 31 2C 22 4C 6F 6E 22 3A  :59.40441,"Lon":
000001A0  31 37 2E 39 34 31 36 31 7D 2C 7B 22 4C 61 74 22  17.94161},{"Lat"
000001B0  3A 35 39 2E 34 30 34 36 32 2C 22 4C 6F 6E 22 3A  :59.40462,"Lon":
000001C0  31 37 2E 39 34 32 30 36 7D 2C 7B 22 4C 61 74 22  17.94206},{"Lat"
000001D0  3A 35 39 2E 34 30 34 37 32 2C 22 4C 6F 6E 22 3A  :59.40472,"Lon":
000001E0  31 37 2E 39 34 32 33 33 7D 2C 7B 22 4C 61 74 22  17.94233},{"Lat"
000001F0  3A 35 39 2E 34 30 34 38 38 2C 22 4C 6F 6E 22 3A  :59.40488,"Lon":
00000200  31 37 2E 39 34 32 38 7D 2C 7B 22 4C 61 74 22 3A  17.9428},{"Lat":
```

Figure 18: cache file EN5 data

[5] *ff51cd01422e6d68936090f8f605a7b1.1*

The file named 'crashlytics-userlog-65F1A6D6031C-0001-390F-FCB942B912E5.temp' in the 'log-files' folder with directory 'com.cabonline.taxi020**files**\.com.google.firebase.crashlytics' contains a lots of information concerning user activities. These logs include various events such as the initiation of activities like "`start__signup_open`", interactions with the "BookingFlowActivity", actions like "start__signup_tap_google", "start__terms_open", "start__terms_accept", "start__login_success", and indications of successful processes like "`trip_calculation_success`". These logs trace the journey of user interactions from logging in to the app to accepting terms and completing actions, providing insights into user activities and app functionality. Such detailed activity logs can prove relevant in understanding the sequence of actions undertaken by users within the application.

In the `'com.cabonline.taxi020\shared_prefs'` folder, a collection of XML files was found, housing settings, configurations, and user preferences similar to those discovered in the taxistockholm. While analyzing these files could potentially offer valuable insights into user behavior, preferences, and interactions, a comprehensive investigation of these artifacts is beyond the scope of this study.

5.3 Findings Themes and Patterns

The analysis of digital artifacts extracted from the ride-sharing applications Taxi Stockholm and Sverigetaxi indicates significant insights into the forensically relevant artifacts available as already explained in the above section. These findings offer valuable insights into the potential forensic artifacts available within ride-sharing applications, contributing to the understanding of digital evidence in investigative procedures.

The examination revealed several themes and patterns, which are summarized as follows:

rider Information:

The artifacts extracted included rider information such as first name, last name, Gmail address, and phone number. Additionally, credit card details and user profiles were also identified. These artifacts provide valuable insights into the identities and payment methods used by riders.

Company Information:

The analysis shows company-related artifacts, including company Gmail addresses and support phone numbers. These details indicate the contact information associated with the ride-sharing companies.

Booking Details:

A comprehensive array of artifacts related to bookings was found, including booking details, trip payment invoice details, trip start and end addresses, timestamps, GPS coordinates, and continuous routes. These artifacts provide a detailed overview of each trip, including its fee and start and end trip location.

Vehicle Information:

The examination also revealed artifacts relating to vehicles used within the ride-sharing service, such as vehicle ID, vehicle plate numbers, driver IDs, and vehicle registration details including manufacturer and model information. These artifacts offer insights into the vehicles employed by the service and their associated drivers.

The following table presents artifacts extracted from Taxi Stockholm and Sverigetaxi applications:

Artifact	Taxi Stockholm	Sverige Taxi
Rider info (First Name, Last Name, Gmail Address, Phone Number)	✓	✓
Company gmail Addresse	x	✓
Company Support phone Number	x	✓
Credit card details	✓	✓
Trip payment invoice details	✓	✓
Trip start and end address	✓	✓
Vehicle number / VehicleId	✓	✓
Vehicle plate number	✓	x
Driver Id	x	✓
Vehicle (Registration Number, Manufacturer, Vehicle Model	x	✓
Booking detalis	✓	✓
Timestamps	✓	✓
GPS Coordinates	✓	✓
Continus Routes	x	✓

Table 7: Extracted Artifact

6 Discussion

6.1 Analysis

The study aimed to conduct a digital forensic investigation of two ride-hailing applications, `Taxi Stockholm` and `Sverigetaxi`. As detailed in the results chapter, various artifacts were successfully extracted from both ride-hailing apps.

When a rider becomes a victim of harm exploitation while using ride-hailing applications like Taxi Stockholm or Sverigetaxi, the artifacts extracted from these apps can be crucial in legal proceedings and investigations. These artifacts serve as a digital trail documenting the rider's interactions, movements, and transactions. Rider information such as names, contact details, and trip history can provide vital clues about the rider's activities, and interactions with drivers. Credit card details and trip payment invoices offer evidence of financial transactions associated with the rides, establishing a verifiable record of the rider's transactions within the app. Timestamps, GPS coordinates provide a detailed timeline and geographic footprint of the rider's journey, helping to reconstruct the sequence of events and identify the rider's location at different times. This digital evidence can verify the rider's account of events, support witness statements, and disprove any false claims or defenses presented by perpetrators. Ultimately, the artifacts extracted from ride-hailing apps can play an important role in bringing perpetrators to justice, ensuring accountability, and providing closure to victims and their families.

While it was feasible to extract artifacts using the `XRY` tool and analyze with `XAMN`, identifying the relevant artifacts required further analysis using additional relevant tools and the development of Python script. To assess the reliability and accuracy of GPS coordinates representing actual trip locations, longitude and latitude coordinates were cross-referenced using Google Earth. This process confirmed the reliability of the extracted data by investigating the exact start and end trip locations of various reserved trips conducted during the experiment. Additionally, route coordinates unique to SverigeTaxi were similarly verified using Google Earth, establishing the reliability. Furthermore, in the case of Taxi Stockholm, timestamps were extracted instead of human-readable time. To fix this, Python script was used to convert timestamps into a human-readable format, providing precise details of trip start and end times.

When extracting artifacts using the same tool i.e. `XRY`, it was observed that SverigeTaxi resulted in a greater number of artifacts compared to Taxi Stockholm. This difference could be attributed to application-specific restrictive features and potential limitations of the extraction tool in accessing certain features of the application.

In addition to verifying the reliability of GPS coordinates of the trip taken through cross-referencing with Google Earth, While the GPS coordinates provided by Taxi Stockholm ride-sharing application offer high accuracy, factors such as the device's GPS sensor quality and signal strength, as well as any potential inaccuracies introduced during data transmission or processing could contribute affecting the result. Furthermore, although the investigation successfully extracted trips from both Taxi Stockholm and SverigeTaxi without encountering any noticeable gaps in coverage, the possibility of occasional data omissions or inconsistencies could happen due to device-specific limitations, or other incidents.

To maintain the integrity of the extracted data, I calculated checksums using the SHA-256 hashing algorithm. This process helps to identify any changes or tampering with the data. The reliability of the artifacts depends on the integrity of the data, ensuring that it accurately reflects the information extracted from the mobile device and is securely stored. In digital forensics, artifacts obtained from digital devices are considered reliable when they are acquired using validated tools and methodologies. Reliability is further reinforced through rigorous analysis, verification procedures, and adherence to established standards. This involves confirming that artifacts are consistent, accurate, and maintain their integrity across multiple examinations. The forensic investigation done in both ride hailing apps followed these principles, ensuring the reliability of the extracted data. Any deviations from these standards may compromise the reliability of the artifacts extracted.

According to the research done by (Zhao et al., 2019), it was suggested that it was possible to harvest an extensive amount of sensitive information from the Uber app. However, their forensic investigation mainly focused on the "nearby cars" feature of the app. In contrast, this study extended its focus to all features of the Android application of both ride-hailing platforms, using a comprehensive data acquisition tool. This approach allows for a more holistic understanding of the potential forensically relevant artifacts within ride-hailing applications, going beyond specific features to encompass a broader spectrum of user data.

6.2 Conclusion

The research question, "What type of forensically relevant artifacts can be recovered from the ride-sharing mobile applications Taxi Stockholm and Sverigetaxi that could be relevant for forensic investigators?" was answered by identifying the extracted artifacts from both ride-sharing applications in the results chapter. The identified artifacts included Rider info (First Name, Last Name, Gmail Address, Phone Number), Credit card details, Company details, booking details, Trip payment invoice details, Trip start and end address, Timestamps, GPS Coordinates, Continuous Routes, and Vehicle details. As a result of crimes committed using these applications, such as physical assaults, robberies, identity theft, and cyberbullying, the users, drivers, and even the owner of the ride-sharing application could all be impacted. Unauthorized access to such data could compromise user privacy by revealing sensitive information such as the frequency and timing of rides, as well as common pickup and drop-off locations, thereby exposing user behavior and personal details. This echoes findings from previous research (Zhao et al., 2019), highlighting the vulnerability of ride-sharing apps to potential misuse of sensitive information. The possible extraction of such relevant artifacts could be useful in crime investigation and incident reconstruction.

Replicating the forensic analysis in a real-world scenario is not feasible due to the requirement of a rooted device. Even though it was tried to do the data extraction with unrooted device it was not possible to extract the data of the application. As a result, the device was rooted, and the required artifacts were extracted. Moreover, the conclusions drawn from the research is limited to specific application that were examined, namely the Oneplus 5T mobile device with Model Oneplus A5010, running on Android version 10. This research could contribute to the field of digital forensics, benefiting law enforcement agencies and digital forensic practitioners involved in crime investigations including ride-hailing applications.

6.3 Limitations

One of the limitations of this study is its small-scale nature, as it only involved data from individual user. This limited data may not be representative of the broader user population, and the findings may not be generalizable to other contexts or ride-hailing applications. Moreover, the study only focused on Android ride-hailing applications, and the findings may not be applicable to other mobile operating systems such as iOS. Additionally, the research was constrained to two specific applications, Taxi Stockholm and SverigeTaxi, due to time limitations, thereby limiting the generalizability of the findings to other ride-hailing platforms.

6.4 Future research

Potential areas for future research include expanding the scope of the investigation to include a broader range of ride-hailing applications across diverse geographical locations, thereby facilitating a comprehensive understanding of the forensic artifacts and privacy implications. Moreover, future studies could involve understanding user behavior and pattern based on the ride they took though those rides hailing application. By incorporating data from multiple users, researchers can analyze a wider range of user interactions and behaviors within ride-hailing applications, leading to a more understanding of the digital artifacts that can be extracted and their potential applications in forensic investigations. Furthermore, future research should extend its focus beyond Android users to include other popular mobile operating systems such as iOS. By conducting analyses across various mobile operating systems, researchers can gain insights into platform-specific differences in digital artifacts, security measures, and privacy implications within ride-hailing applications. This expanded approach will contribute to a more comprehensive understanding of the forensic landscape across different platforms and enable the development of platform-specific forensic methodologies to address potential vulnerabilities.

7 References

Alemi, F. et al. (2018) ‘What influences travellers to use Uber? Exploring the factors affecting the adoption of on-demand ride services in California,’ Travel Behaviour and Society, 13, pp. 88–104. Available at: https://doi.org/10.1016/j.tbs.2018.06.002.

Andrew Wyrich (2021) ‘14 charged in ride-hailing, delivery app identify theft scheme’, 20 September. Available at: https://www.dailydot.com/debug/14-charged-rideshare-delivery-app-identity-theft-scheme/.

Android Developers (2023), 'Enable Developer options', Android Developers, Available at: https://shorturl.at/fprwy (Accessed: 26 Aug 2023).

Google. (2023, October). Platform Tools Release Notes. Android Developers. Available at: https://developer.android.com/tools/releases/platform-tools (Accessed April 2024)

Balasch, J. et al. (2010) ‘PrETP: Privacy-Preserving Electronic Toll Pricing’, p. 16.

Bays, J. and Karabiyik, U. (2019) ‘Forensic Analysis of Third Party Location Applications in Android and iOS’.

Bialon, R. 2020, 'On Root Detection Strategies for Android Devices', Available at: https://arxiv.org/pdf/2012.01812 (Accessed: 18 Sep 2023).

Casey, E. (2010) Handbook of digital forensics and investigation. Amsterdam ; Boston: Academic.

Carrier, B. (2018). Smartphone forensics: A practical guide. Boston, MA: Syngress.

Darren R. Hayes, Christopher Snow, and Saleh Altuwayjiri (2018) ‘A Dynamic and Static Analysis of the Uber Mobile Application from a Privacy Perspective’, Journal of Information Systems Applied Research (JISAR), 11(1).

DAVID CURRY (2022) ‘Taxi App Revenue and Usage Statistics (2022)’, 21 April. Available at: https://www.businessofapps.com/data/taxi-app-market/ (Accessed: 25 April 2022).

Das, R. (2017). Evidence acquisition in mobile forensics. Infosec Institute. Available: [https://resources.infosecinstitute.com/topics/digital-forensics/evidence-acquisition-mobile-forensics-2/], Accessed: Dec 2023

Denscombe, M. (2014) The good research guide: for small-scale social research projects. 5. ed. Maidenhead: Open University Press.

Elsersy, W. F., Anuar, N. B., & Razak, M. F. A. (2023). ROOTECTOR: Robust Android Rooting Detection Framework Using Machine Learning Algorithms. Arabian Journal for Science and Engineering, 48, 1771–1791.

fortune business insights (2021) ‘Ride Sharing Market Size, Share & COVID-19 Impact Analysis, By Type (E-Hailing and Station Based), By Commute Type (Long Distance, Corporate, and Inter City), By Application Type (iOS, Android, and Others), and Regional Forecasts, 2021-2028’, December. Available at: https://www.fortunebusinessinsights.com/ride-sharing-market-103336 (Accessed: 23 April 2022).

Forensafe. (2022, December 30). Investigating Windows Notepad++ Desktop Application. Available at: https://forensafe.com/blogs/windows_notepad++.html (Accessed April 2024)

Forensic Focus. (2018, March 14). Forensic Analysis of Damaged SQLite Databases. Available at: https://www.forensicfocus.com/articles/forensic-analysis-of-damaged-sqlite-databases (Accessed: 22 April 2024).

Gomez, J. et al. (2021) 'Adoption and frequency of use of ride-hailing services in a European city: The case of Madrid', Transportation Research Part C: Emerging Technologies, 131, p. 103359. Available at: https://doi.org/10.1016/j.trc.2021.103359.

(Guyader et al., 2021) 'Shared Mobility: Evolving Practices for Sustainability', Sustainability, 13(21), p. 12148. Available at: https://doi.org/10.3390/su132112148.

Hayes, D.D.R., Christopher Snow, and Saleh Altuwayjiri (2017) 'Geolocation Tracking and Privacy Issues Associated with the Uber Mobile Application', Information Systems, p. 12.

Heid, K. et al. (2022) 'Android Data Storage Locations and What App Developers Do with It from a Security and Privacy Perspective':, in Proceedings of the 8th International Conference on Information Systems Security and Privacy. 8th International Conference on Information Systems Security and Privacy, Online Streaming, --- Select a Country ---: SCITEPRESS - Science and Technology Publications, pp. 378–387. Available at: https://doi.org/10.5220/0010838200003120.

Johana Bhuiyan (2015) 'Men Are Using Uber's Lost-And-Found Feature To Harass Female Drivers', 10 February. Available at: https://www.buzzfeednews.com/article/johanabhuiyan/faced-with-harassment-female-uber-drivers-often-left-to-fend#.eqRlzO4xR0.

Ken Pillar (2021) 'Best Stockholm Taxi Apps of 2021 (Android)'. Available at: https://leapdroid.com/best-stockholm-taxi-apps-of-2021-android/.

Kiptoo, K.K. (2020) 'A FORENSIC INVESTIGATION FRAMEWORK FOR ANDROID ON-DEMAND RIDE APPLICATIONS', p. one hundred.

Liane Morejon and Andrea Torres (2022) 'Lyft driver accused of raping and robbing Miami Beach hotel guest', 8 March. Available at: https://www.local10.com/news/local/2022/03/08/lyft-driver-accused-of-raping-and-robbing-miami-beach-customer/.

Lin, X. (2018) Introductory Computer Forensics: A Hands-on Practical Approach. Cham: Springer International Publishing. Available at: https://doi.org/10.1007/978-3-030-00581-8.

Luz Lazo (2020) 'Thieves are using peer-to-peer car rental apps to find their next ride', February. Available at: https://www.washingtonpost.com/local/trafficandcommuting/thieves-are-using-peer-to-peer-car-rental-apps-to-find-their-next-ride/2020/02/13/b84d8e16-49c0-11ea-9164-d3154ad8a5cd_story.html.

Martelli, F., Renda, M.E. and Zhao, J. (2020) 'The Price of Privacy Control in Mobility Sharing', Journal of Urban Technology, p. 25.

Maus, S., Höfken, H. and Schuba, M. (2010) 'Forensic Analysis of Geodata in Android Smartphones', p. 12.

(MSAB,2024). XAMN –Digital Forensic Analysis Solution. Available at: https://www.msab.com/product/analyze/ (Accessed: Jan 2024)

MSAB. (2023). XRY Extract. Available: [https://www.msab.com/product/xry-extract/] Accessed: Dec 2023

Pew Research Center (2018) 'The American Trends Panel survey methodology', More Americans are using ride-hailing apps. Available at: https://www.pewresearch.org/fact-tank/2019/01/04/more-americans-are-using-ride-hailing-apps/.

Pham, A. et al. (2017) 'PrivateRide: A Privacy-Enhanced Ride-Hailing Service', Proceedings on Privacy Enhancing Technologies, 2017(2), pp. 38–56. Available at: https://doi.org/10.1515/popets-2017-0015.

Pritha Bhandari (2021) 'Ethical Considerations in Research | Types & Examples', 18 October. Available at: https://www.scribbr.com/methodology/research-ethics/ (Accessed: 14 April 2023).

Ramadhan, R. A., et al. (2022). Digital Forensic Investigation for Non-Volatile Memory Architecture by Hybrid Evaluation Based on ISO/IEC 27037:2012 and NIST SP800-86 Framework. International Transaction Journal of Research and Development, 6(2), 162. DOI: 10.25299/itjrd.2022.8968.

Ranjan, M., Mritunjay, B., Barot, K., Krishna, V., Khairnar, V., Rawal, V., Pimpalgaonkar, A., Saxena, S., & Sattar, A. (2023). Python: Empowering Data Science Applications and Research. Journal of Operating Systems Development & Trends, 10, 27-33. Available at: https://doi.org/10.37591/joosdt.v10i1.576 (Accessed: 22 April 2024).

Schmitt, S., Nemetz, S., & Freiling, F. (2018). A standardized corpus for SQLite database forensics. Digital Investigation, 24, S121-S130.

Shavers, B. (2021). The essential guide to smartphone forensics. Indianapolis, IN: Wiley.

Singh, A., Singh, S. K., & Singh, S. K. (2019). Technology Revolution gives Cybercrime a Boost: Cyber-Attacks and Cyber Security. ARSSS International Conference, Cochin.

Smiljanic Stasha (2022) 'Ride-Sharing Industry Statistics to get you going in 2022', 5 March. Available at: https://policyadvice.net/insurance/insights/ride-sharing-industry-statistics/ (Accessed: 16 April 2022).

Statista (2022) 'Ride-hailing and taxi apps that collected the most data from users as of January 2022, based on a data sensitivity index*'. Available at: https://www.statista.com/statistics/1291806/data-sensitivity-index-ride-hailing-taxi-apps/.

Sweden taxi (2022) 'Sweden taxi app'. Available at: https://play.google.com/store/apps/details?id=com.cabonline.taxi020&hl=sv.

Taxi Sthlm (2022) 'Taxi Sthlm app'. Available at: https://play.google.com/store/apps/details?id=se.taxistockholm&hl=sv.

Thaithatkul, P. et al. (2019) 'Adoption of dynamic ridesharing system under influence of information on social network', Transportation Research Procedia, 37, pp. 401–408. Available at: https://doi.org/10.1016/j.trpro.2018.12.209.

Warlock. (2018, February 4). File carving. Infosec Institute. Available at: https://www.infosecinstitute.com/resources/digital-forensics/file-carving/ (Accessed April 2024)

Zhao, Q. et al. (2019) 'Geo-locating Drivers: A Study of Sensitive Data Leakage in Ride-Hailing Services', p. 15.

8 Appendix A - Scripts

The first Python script, saved as "convert_to_json.py," was utilized to automate the conversion process of various file formats into JSON. The second script, saved as "Timestamp_converter.py," was used to transform Unix timestamps into human-readable datetime objects.

1. convert_to_json.py

```
import json
import os

def convert_to_json(file_name):
try:
with open(file_name, 'r') as file:
data = file.read()
json_data = json.loads(data)
return json_data
except FileNotFoundError:
print("File not found.")
return None
except json.JSONDecodeError:
print("Invalid JSON format in the file.")
return None

def save_as_json(json_data, input_file_name):
try:
output_file_name = os.path.splitext(input_file_name)[0] + ".json"
with open(output_file_name, 'w') as file:
json.dump(json_data, file, indent=2)
print(f"JSON data saved to {output_file_name}")
except Exception as e:
print(f"Error occurred while saving JSON data: {e}")

def main():
file_name = input("Enter the file name: ")
json_data = convert_to_json(file_name)
if json_data:
save_as_json(json_data, file_name)

if __name__ == "__main__":
main()
```

2. Timestamp_converter.py

```
import datetime
import pytz

# Unix timestamp
timestamp_ms = 1710358657520

# milliseconds to seconds
timestamp_s = timestamp_ms / 1000

# timezone-aware datetime object in UTC
dt_object_utc = datetime.datetime.fromtimestamp(timestamp_s, pytz.utc)

# datetime object as a string
formatted_datetime = dt_object_utc.strftime('%Y-%m-%d %H:%M:%S UTC')

print(f"Converted Datetime of '{timestamp_ms}' is: {formatted_datetime}")
```

9 Appendix B - Reflection

Completing my master’s thesis on Mobile App Forensics has been challenging yet rewarding. Under the guidance of my supervisor, Stefan Axelsson, I conducted a forensic investigation specifically focusing on the ride-hailing applications Taxi Stockholm and Sverigetaxi. Reflecting on this academic journey, I am happy to share my thoughts and insights gained throughout the process.

My study aligned with the goals of the thesis course, particularly in contributing to the body of knowledge in mobile app forensics. One of the key goals achieved was the successful identification of forensically relevant artifacts from ride-hailing apps, which is important for forensic investigators. This accomplishment aligns with the course’s objective of conducting rigorous research with practical implications. However, the goal of conducting a broad-scale analysis was not fully met due to the focus on only two specific applications on the Android platform. Expanding the scope to include more apps and platforms could have enhanced the study's comprehensiveness.

The planning of my study was methodical, involving a detailed research design and systematic data collection using forensic tools. Despite this, there were areas for improvement. For instance, a more robust contingency plan could have mitigated the impact of unforeseen personal challenges, which delayed the completion of my thesis.

The courses I took in my master's program, particularly Digital Forensics, Cyber Forensics (CYFO), Information Security (INTROSEC), Scientific Communication and Research Methodology (FMVEK), Research Methodology for Computer and Systems Sciences (MMII), and Cyber Security (CYBER), were highly relevant to my thesis work. The theoretical foundations in these courses directly applied to my research, enabling me to approach forensic investigation with a solid academic background. The course on Digital Forensics, in particular, provided essential methodologies and tools crucial for data extraction and analysis.

The thesis has important value for my future work. It has equipped me with practical skills in forensic investigation and a profound understanding of app forensics. These competencies are highly relevant for a career in cybersecurity and digital forensics. The experience has also sparked a keen interest in data/artifacts-based decision-making, which I will use in my future work.

I am satisfied with my thesis work and its results. The ability to recover and analyze various artifacts from the ride-hailing applications demonstrates the practical impact of my research. These findings have the potential to contribute significantly to the field of digital forensics and can be used by forensic investigation practitioners. However, I acknowledge the limitations of the study, including its small-scale nature and focus on specific applications, and see these as areas for future improvement.

Throughout the thesis process, I utilized tools to enhance my research work. For instance, I used Grammarly to automate parts of the grammar-checking process, allowing for more efficient writing. AI tools such as ChatGPT were used to understand lengthy papers and determine their relevance to my work before doing a deep dive and citing them in my research.