# Forensic Analysis of Travelling Applications on Android Devices

By

**Muhammad Anwar**

**171036-MS(IS)-9-2016**

Supervisor

**Dr. Mehdi Hussain**

**Department of Computing**

A thesis submitted in partial fulfillment of the requirements for the degree of Master of Science in Information Security (MS IS)

In
School of Electrical Engineering and Computer Science,
National University of Sciences and Technology (NUST), Islamabad, Pakistan.

(August 2020)

# Approval

It is certified that the contents and form of the thesis entitled "Forensic Analysis of Travelling Applications on Android Devices" submitted by Muhammad Anwar has been found satisfactory for the requirement of the degree.

Advisor: Dr. Mehdi Hussain

Signature: Hussain

Date: 12 August 2020

Committee Member I:

Dr. Shahzad Saleem

Signature: Shahzad

Date: 12 August 2020

Committee Member II:

Dr. Yousra Javed

Signature:

Date: 12 August 2020

Committee Member III:

Dr Sana Qadir

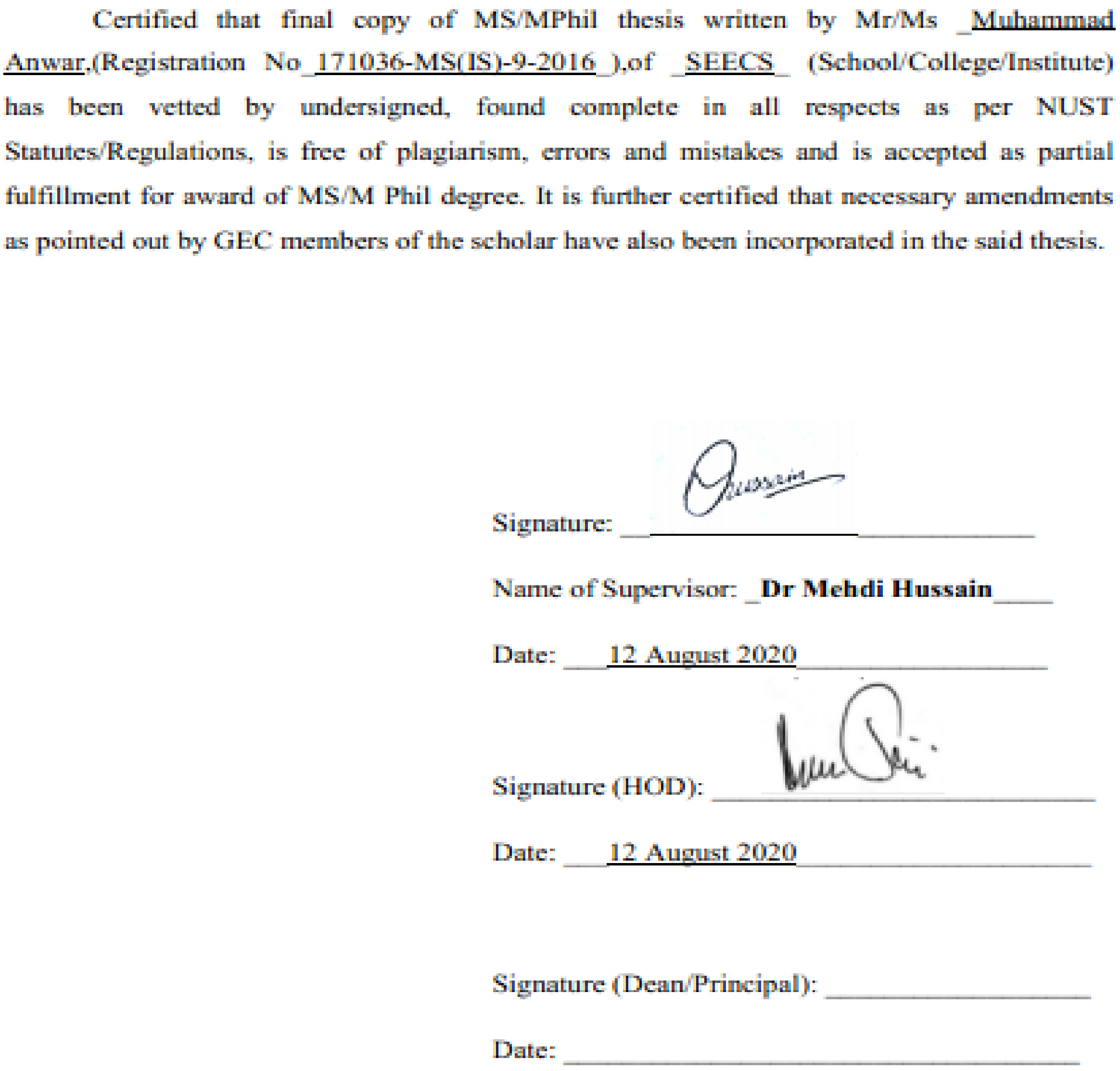
Signature: Sana Qadir

Date: 12/08/2020

# Dedication

To my family, my supervisor and my friends and who has always been supportive.

# THESIS ACCEPTANCE CERTIFICATE



Certified that final copy of MS/MPhil thesis written by Mr/Ms _Muhammad Anwar,(Registration No_171036-MS(IS)-9-2016_),of _SEECS_ (School/College/Institute) has been vetted by undersigned, found complete in all respects as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial fulfillment for award of MS/M Phil degree. It is further certified that necessary amendments as pointed out by GEC members of the scholar have also been incorporated in the said thesis.

Signature: ______________________________

Name of Supervisor: _**Dr Mehdi Hussain**____

Date: ___12 August 2020________________

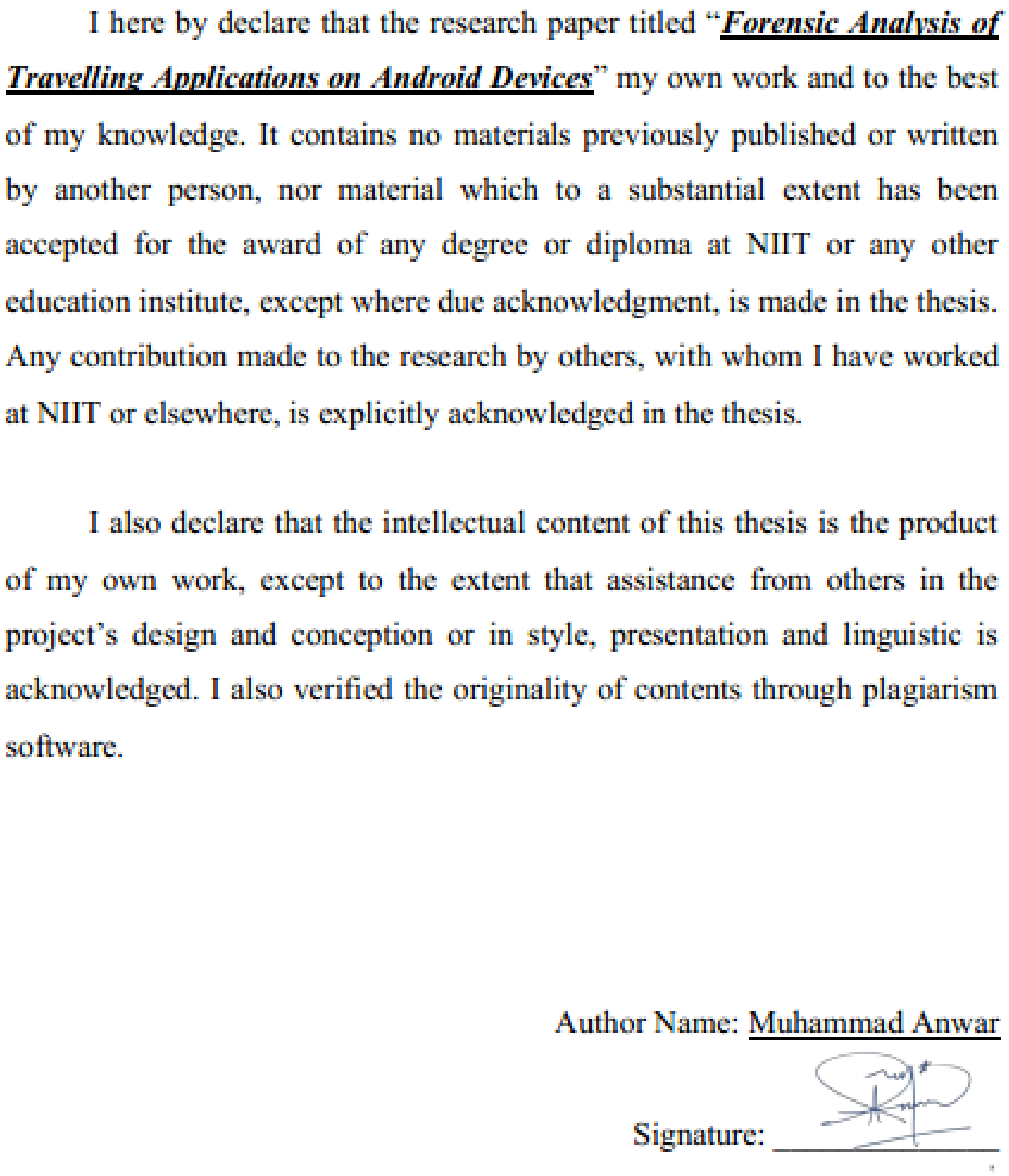
Signature (HOD): __________________________

Date: ___12 August 2020____________________

Signature (Dean/Principal): __________________

Date: ____________________________________

# Certificate of Originality



I here by declare that the research paper titled "***Forensic Analysis of Travelling Applications on Android Devices***" my own work and to the best of my knowledge. It contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at NIIT or any other education institute, except where due acknowledgment, is made in the thesis. Any contribution made to the research by others, with whom I have worked at NIIT or elsewhere, is explicitly acknowledged in the thesis.

I also declare that the intellectual content of this thesis is the product of my own work, except to the extent that assistance from others in the project's design and conception or in style, presentation and linguistic is acknowledged. I also verified the originality of contents through plagiarism software.

Author Name: Muhammad Anwar

Signature: _______________

# Acknowledgment

All praise to Allah, the most merciful, kind and beneficent, to all mankind. All respect and tributes goes to our Holy Prophet Muhammad (ﷺ).

I'm truly grateful to my supervisor Dr. Mehdi Hussain for his supervision, and direction throughout the research study. He inspired and motivated me throughout my research by his skills and knowledge; thank you so very much. I am obliged to all my respectable teachers for providing me their valuable time and considerations. I believe that this work would not have been possible without their guidance & expert suggestions.

I am also grateful to my committee members Dr. Shahzad Saleem for sharing with me his valuable experiences and knowledge of computer forensics and timely suggestions toward the successful completion of this research work.

In spite of all the assistance by the supervisor, committee members, and others, I take the responsibility for any errors and omissions which may exist unconsciously.

# Table of Contents

# Abstract

Travelling is the essential part of our daily life. With the advancement of mobile technology most of the traveling companies are providing online booking / reservation services to their customers. These services on devices may hold an enormous amount of information. With the increase of business in online traveling, there is an increase of threat. Therefore, Travelling is one of the major categories that need to be investigated by forensic investigators. In this study, for investigation, a *Careem* application is considered, where it is one of the most popular traveling apps with 10M+ install base. For a digital forensic examiner, this application is a vital source of information and evidence against the accused. We can draw more realistic results based on accused traveling. Moreover, the Careem app provides some additional features like balance transfer, mobile recharge, and item delivery which can provide sufficient clues and artifacts that can help forensic examiner. The objective of this study is to forensically search and analyze the remnants of performed activities on the application. It will facilitate the forensic community in the analysis of such applications found in the smartphone of the accused or a digital device at a crime scene. The findings may advance prosecution and provide valuable evidence in the court of law. This will help in providing justice with facts and confirmation.

**Keywords:** forensics analysis of Travelling apps, Careem app forensics, Mobile Forensics, Android application forensic, Autopsy, Travelling locations, geo locations, In app chat forensic

# Chapter 1

# 1. Introduction

The content of this chapter is organized in following manner.

- Research History (Section 1.1) describes the terms which are essential to understand proposed research work.
- Motivation (Section 1.2) describes the research motivation.
- Research Question (Section 1.3) narrates the need for this research.
- Problem Statement (Section 1.4) highlight the problem and challenges Goals and Objectives (Section 1.5) the intention and objective of this research under considered scope.
- Audience (Section 1.6) describes the Intended target audiences of this study.
- Scope of Study (Section 1.7) describes the scope of this study.
- Research Challenges (Section 1.8) highlight the Challenges involved in this research.
- Organization of Thesis (Section 1.9) Provide layout of this research.

## 1.1. Research History:

The commonplace phrases used in the following studies are “Forensics”, “Android App forensics”, “Travelling app”, “Android app”, “Forensic investigation”, “Mobile forensics”. We will talk approximately those terms in detail for those who have little knowledge of this research domain. Therefore, they might have advanced knowledge and top information of this research in appropriate way.

The significance of forensic study is highlighted in the following sub-sections. Moreover, we will focus on the challenges involved in mobile forensics. There are several Digital evidence collection techniques, moreover chain of custody is involved to preserve the evidence. We will elaborate chain of custody process in detail.

After this introductory part we will discuss our research motivation and challenging area of this research work. Adhering to research question we will future elaborate the challenges that are involved in this research and any mobile forensics investigator must face during forensics investigation process. After that we will discuss the target audience for this research. We will characterize the extent of this examination believing the applied constraints and objectives to be accomplished. After defining scope and highlighting research challenges a thesis layout is presented for better understanding of the research work.

### 1.1.1 Forensics Science:

Forensics a Latin word meaning public discussion or open debate. Forensics study has old roots but with non-standardized practices which eventually caused the poor results. Development of forensic science has its roots in Europe from 16th century and up till now there is continuous development in this domain [1]. Forensics in recent era refers to utilization of forensics science to the legal framework. With scientific method utilized, it is a test for forensics analysts to present the evidence with proven correctness and demonstrate the accuracy of proof while giving presenting to court of law. Hence, forensics in key terms is a procedure which assumes an indispensable job in recognizable proof and giving the real data through the examination procedure [2].

### 1.1.2 Digital Forensics

Digital forensics a branch of forensics science includes the recovery and investigation of artifacts present in digital gadget/device, mostly its related to crime which involves the usage of computer in criminal activity [3]. Digital forensics was previously considered as computer forensics but has further enhanced to compensate investigation of all devices having the ability to store digital data [3]. Digital forensics examinations have different categorization. In most cases it helps court of law to get useful evidence which ultimately leads to case solution. Criminal cases which includes violation of law using the digital devices are the mostly targeted of such investigations for example, murder, burglary and ambush against the individual with the involvement of digital devices which leads to track the culprit. Common cases which includes violation of property rights of people, contractual disputes where some sort of e-discovery may be involved [4].

Digital forensics is ordinarily used in both criminal law and private investigation. Generally, it has been related with criminal law, where proof is gathered to help or contradict a theory under the steady gaze of the courts. Thus, knowledge gathering is occasionally held to a less severe scientific norm. In common prosecution or corporate issues digital forensics frames some portion of the electronic discovery process. Legal methodology is like those utilized in criminal investigations, frequently with various lawful confinements. Outside of the courts digital forensics can frame a piece of interior corporate investigations [4].

### 1.1.3 Forensic Process

When leading the forensics investigation, it is critical to follow the digital forensics scientific procedure. This following procedure covers the whole evidence collection process from information identification to collection, preservation and examination to analysis and presentation. In the collection stage examiner acquired search authority, maintains the chain of custody and duplicate the evidence. In assessment and examination stage first tools validity is assured by investigator than analysis is done. The presentation stage refers to the results and when declaration is presented. PC portable devices, systems and cell phones would all be able to be used in or succumb to the digital assault. Every gadget type has diverse interruption techniques and prerequisites of evidence handling. This has prompted the development of three branches of digital forensics know as Computer forensics, Mobile forensics and Network forensics. Following model shows the process flow of the activities in figure 1 [5].

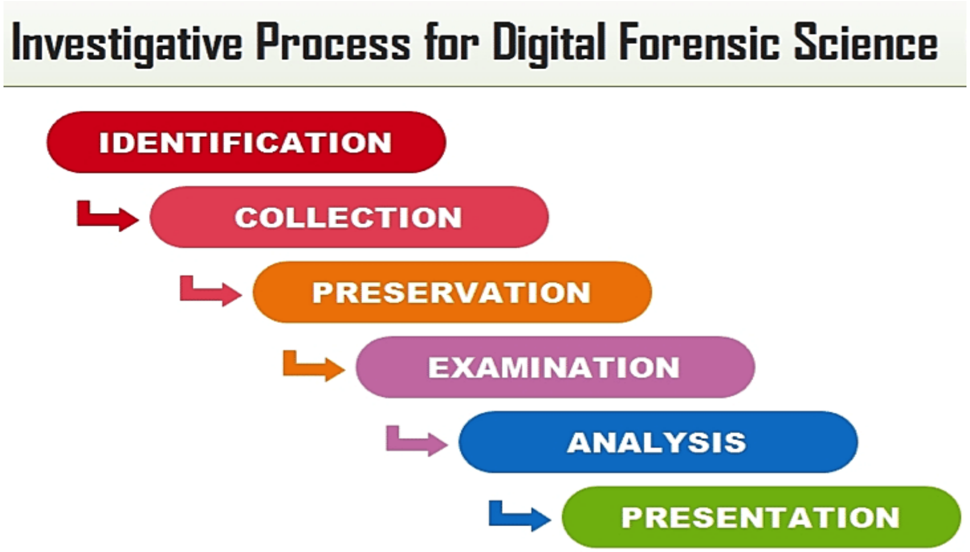


Figure 1-Investigation Process [5]

### 1.1.4 Evidence handling

Digital evidence can be found on varies storages mediums like SD card, Hard Disk, externally connected USBs and all other storage mediums that can hold digital data. There are serval tools which are designed to handle these storage mediums. NIST has employed some procedures and requirements to comply with standard provide by NIST.

### 1.1.5 Chain of Custody

Chain of custody (CoC), from a legal point of view, is the sequential document or paper trail that maintains the order of custody, transfer, control, analysis, and disposition of physical or electronic evidence [6]. Holding Chain of custody is very essential for the examiner that is collecting the evidence from the crime scene. Documenting the evidence is mandatory to maintain the chain of custody because every step involves in evidence handling must be recorded and whoever interacted with the evidence or involve in evidence collection is responsible for what happens to it. This prevents law officials and evidence collectors from altering the evidence [6]. Moreover, it is mandatory to maintain the chronological documentation of the digital evidence to be admissible in the court of law. Figure 2 shows the CoC model.

.

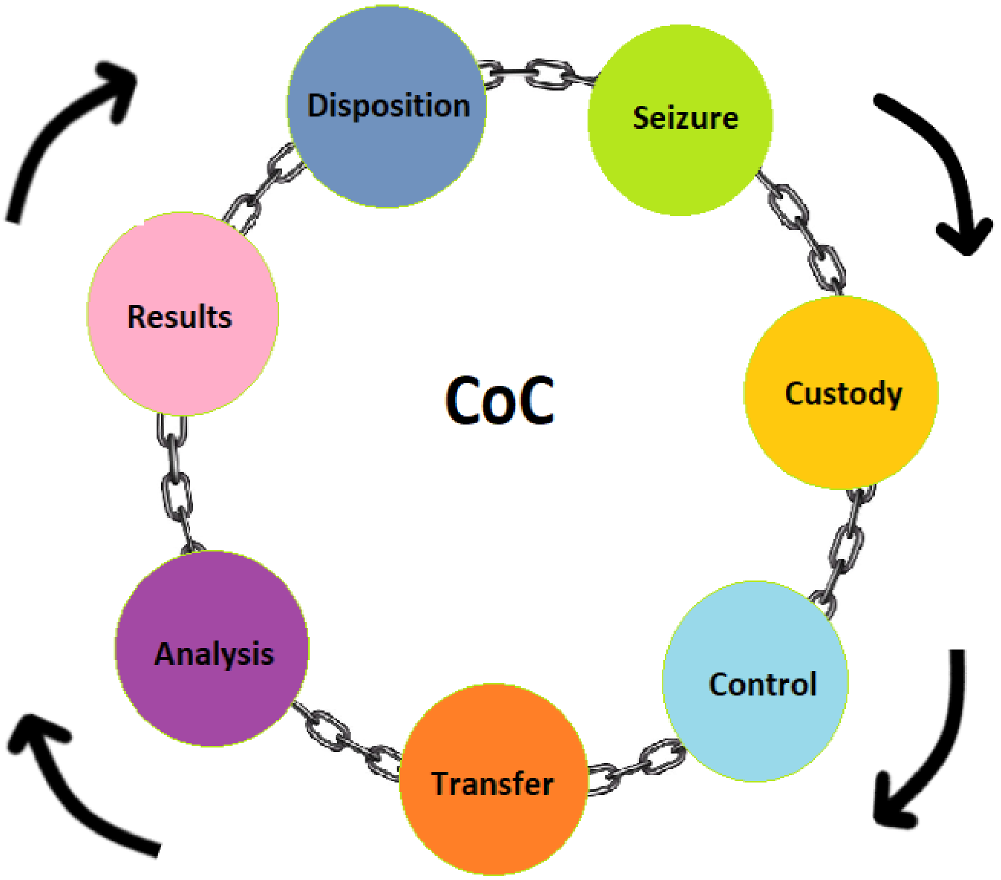


Figure 2-Chain of custody [6]

### 1.1.6 Challenges of Mobile device forensics

Mobile forensic is considerably more challenging than other digital devices due to its evolving technology. There are huge number of brands and model of mobile devices in the market. The operating systems on these mobile devices are constantly changing and new versions are released frequently by developer and mobile companies. Additionally, Information on these gadgets are constantly changing for example, live system association for correspondence, applications utilization information, programming updates and GPS area data and so on. In this way, alongside the general contemplations for investigation of digital gadgets, a forensic examiner may have following challenges

- Frequent change in hardware and software
- Frequent OS updates
- Constantly change GPS data
- Volatile data
- Different security controls like PIN, Password, and Pattern etc.
- Network connectivity
- Proprietary hardware

## 1.2 Motivation

According to web statistics the number of smartphone users worldwide exceeds three billion and it is expected that it will grow further by several hundred million in upcoming few years. A careful estimate showed that there is constant market growth with almost 1.4 billion smartphones sales annually [7]. Figure 3 shows number of smartphone users with year rang.

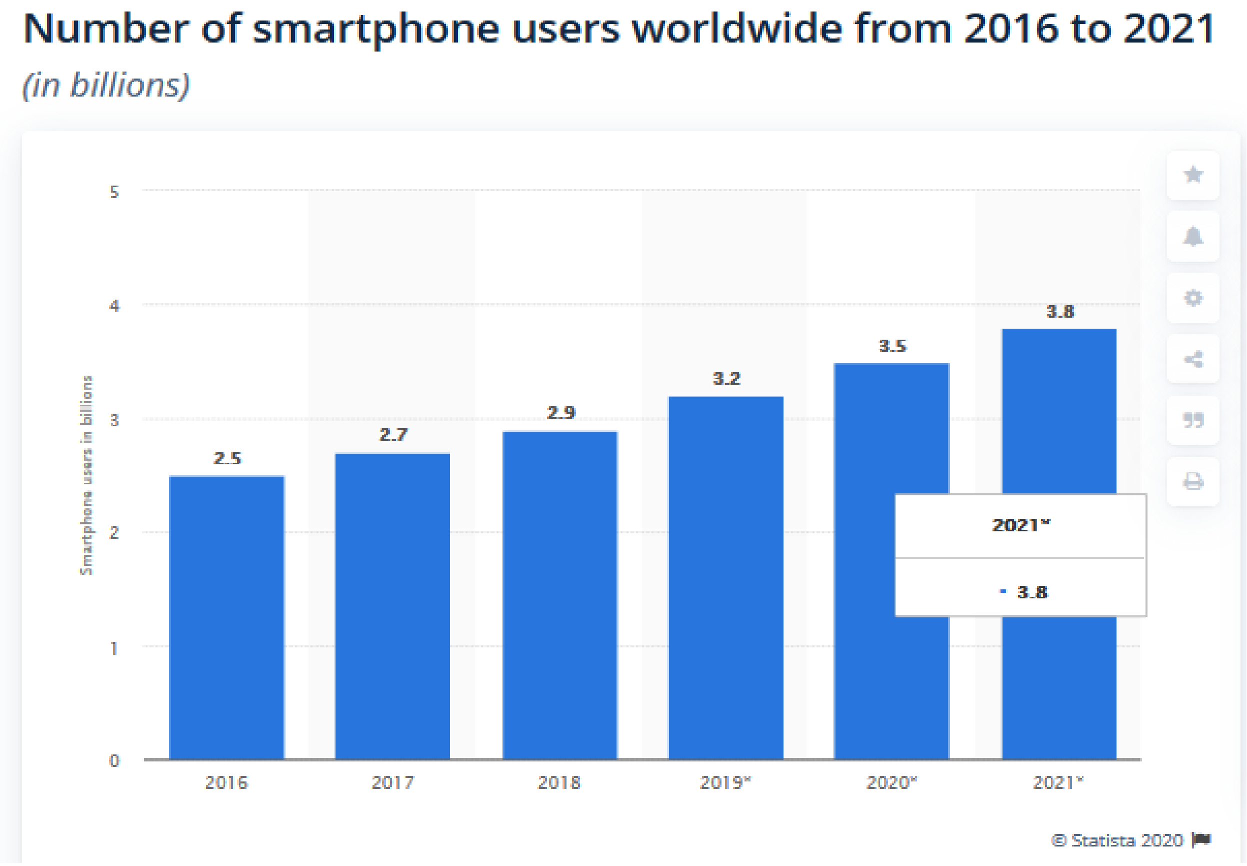


Figure 3- Smartphone Statistics by @Statista2020 [7]

Travelling is the essential part of our daily life. With the advancement of mobile technology most of the traveling companies are providing online booking / reservation services to their customers and these services on devices can hold enormous amount of information. With the increase of business in online traveling, there is an increase of threat. Therefore, Travelling is one of the major categories that need to be investigated by forensic investigators. For this, various types of applications exist in the market such as Careem, Uber, Bykea etc., where in Pakistan both Careem and Uber has most shared in term of usage. There is a need to design a standardized procedure which will be helpful identification of data remnants in applications. For this, we employed the Careem app, where it is considered one of the most popular traveling apps with 10M+ install base. For a digital forensic examiner, this application is a vital source of information and evidence against the accused.

As per our knowledge, there is lack of travelling app forensic. In this work we have provided details artifacts that are useful for forensic examiners.

## 1.3 Research Question

As previously there is no such work on android base travelling applications, this research will provide a platform to researchers, forensics examiner to have details analysis of android travelling applications. As Careem app is a popular with hug install base, we conducted this study on the latest version (10.0.2) of Careem app. Our research is to answer the following questions.

Question 1: What are the artifacts / remnants that we can found on the android device after using android travelling application Careem.

Question 2: How precisely we can reconstruct the artifacts to get insight of user activity on that application

Question 3: How to categories obtained artifacts with the level of criticality and usefulness.

## 1.4 Problem Statement

Travelling is a part of human life. With the advancement of technology smartphone rapidly becomes the essential part of routine life. It is estimated that almost 67 percent of world population have mobile phone [7]. With this increase number of mobile devices transporter are now facilitating their customer to book Taxi, Car online. With the increase of business in online traveling, there is an increase of threat. Therefore, Travelling is one of the major categories that need to be investigated by forensic investigators. Previously not enough research has been done to collect artefact from travelling applications. To facilitate and speedup evidence collection process moreover to analyze what Information can help investigation agencies to investigate the crime scene there is a need for forensic analysis of such applications. Moreover, to facilitate forensic community in the analysis of such applications found in smart phone of accused or in a digital device at crime scene forensic study is required.

## 1.5 Goals and objectives

The Goal of this study is to provide a roadmap for forensic analysis of other android travelling applications and help the forensic community in the analysis of such applications. The app chosen for study is based on the popularity and number of downloads from Android play store.

The objective of this study to collect and articulate the artifacts of android based travelling application. It will help forensic community to explore same application in same fashion and will produce better understanding on subsequent studies.

## 1.6 Audience

This research addresses to following audience.

- Application user
- Forensics examiner
- Vendor
- And research community

Application user will get insight of the security consideration associated with this application. Forensic examiner can easily find artifacts of this application and can reconstruct the events done through this application. Geo location provides the location artifacts which can facilitate forensic investigator to reconstruct the flow of activities with location artifacts. Vendor can evaluate their application security issues and research community will get facilitation in travelling application.

## 1.7 Scope of Study

In this study we have chosen Nexus 6P with 32GB internal storage with OS android Version 9, PixysOS. SD card storage and volatile memory are not included in our scope of study. Application selection is a tough challenge once you have several applications in this category. We have selected Careem app for our study with following reasons:

- Popularity
- Huge install Base
- Multiple service options
- Users reviews
- No previous forensics work

Our selected application has more popularity among same category application on google play store with its positive customer's reviews and downloads. It has huge install base almost 10M installation on google play store. Careem offers multiple service in a single app which is not limited to booking but item delivery and mobile recharge services. Careem has good user reviews about its services available on google play store. As per knowledge, there is no previous forensic study exits on this application

Our model of data acquisition relies on physical data extraction from the mobile device instead chip off or logical extraction of data. The tools we have used in this study will be able to recover files or directories that are deleted from storage media.

## 1.8 Research Challenges

Mobile phones are rapid growing technology with very frequent upgrades, updates and patches. Google play store keeps updating its installed application. Every application receives frequent update from its developers.  With every update in OS new security concerns and privacy issues arises.

To simulate real world usage scenario of this application we have created a dummy account. We have created all cases that depict the real usage scenarios. Later, performed all activities according to these cases. Activities involving, an account creation, ride booking, mobile recharge, food delivery and credit card payment using Careem application. All activities are time consuming and challenging in order to collect evidence afterwards by acquiring memory image of the mobile device.

## 1.9 Organization of thesis

For intended audience to understand this study in better manner we have divided the study into 6 chapters. Following is the details layout of chapter:

Chapter No. 1 "**Introduction**" provides history of research work. Two essential concepts Digital forensics and chain of custody are discussed for better understanding of study. This chapter also includes motivation behind this study and illustrates the problem domain with research question. It also highlights the goals and objective of this study. Scope and audience are mentioned at the end of this introductory chapter.

In Chapter No 2, "**Literature review**", we have discussed the previous work of different researcher in the "mobile forensics" domain. Their adopted process methodologies and evidence collection process are discussed in detail.

Chapter No 3 "**Research methodology**" elaborates the research methodology with its phases and our chosen methodology.

Chapter No 4 "**Evidence collection and Experimentation**" consist of list of steps involved in evidence collection. Complete details from rooting mobile devices to acquisition of memory image of the mobile device are discussed.

In Chapter No 5 "**Analysis of Android app**" we have analyzed the artifacts and discussed each artifact briefly.

In Chapter No 6 “**Results and Conclusion**” we discussed the results that we have derived from our research and made some conclusion on them and at the end we discussed future work.

# Chapter 2

# 2. Literature Review

In this chapter a focus will be on previous studies that have been done either on the same subject or related subject.

## 2.1 Introduction

The focus of this research is android mobile application. As mobile forensics is vast domain and lot of studies is done on mobile forensics, we have carefully chosen related research papers. The papers which are studied are categories based on following areas of the mobile forensics.

- Forensic Investigation of Android Mobile Applications (Section 2.2)
- Digital Forensic Analysis of Instant Messaging Applications on Android Smartphones (Section 2.3)
- Forensic Analysis of Mobile Banking Apps (Section 2.4)
- Forensic analysis and security assessment of Android m-banking apps (Section 2.5)

## 2.2 Identifying and managing the potential evidence for Android Devices

In android forensics it is crucial to identify and manage potential evidence. All related work is dependent on evidences. Dohyun Kim et al. carried out a research to effectively manage the potential evidence in android device forensics [20]. Recently, a report shows that the average storage capacity of smartphone has been increased up to 80 GB per device [21]. Therefore, due to huge data storage capabilities on devices, a rich source of potential evidences can also be identified Generally, an application logs are searched for application related artifacts like app permission, installation date and user information. Moreover, SQLite data and schema structure analysis are done for user information like time, location, user profile, and user behavior.

Research has proposed a new evidence management format for evidence management per app basis.

As each app has separate information that it contains on android data partition and android OS provides sandbox environment to each app to isolate it from accessing other apps data by providing unique path and pre-declared permissions to that application. Furthermore, android gives a unique ID at the time of app installation for easy management. Dohyun Kim et al. group the app artifacts base system log file and other related search criterial discussed earlier [20].

## 2.3 Forensic Investigation of Android Mobile banking application.

Mobile Banking apps Forensic analysis is done by Oluwa femi Osho [17]. Researcher selected twelve popular android mobile banking application of Nigeria. This study is conducted to collect sensitive data artifacts which are being stored in mobile device by these apps. This study showed that the application under study did not store any sensitive data in backup except one application which sensitive stored data in the test device memory and did not apply any security policy for securing data [17]. He employed two data methods for data acquisition, Manual data acquisition method and Physical data acquisition method [18]. Researcher used FRED tool to analysis the memory dump which was acquired through physical acquisition method to collect any sensitive data form mobile banking apps.

Forensic analysis and security assessment of Android m-banking app is another systematic study of forensic artifacts collected by Rajchada Chanajitt [19]. Researcher conducted this study by forensically analyzing seven different mobile banking apps of Thailand. Different artifacts revealed different security vulnerabilities like serval apps didn’t implemented root device detection [19]. Data Duplicator (DD) and JTAG methods were used to acquire data for mobile device. Application code analysis is also performed along with image analysis. Code decomplication and analysis is done through java decompiler. Code analysis helped the researcher to analyze the security structure of the application and the way database is populated and configuration entries are created. Static binaries analysis is also conducted to evaluate the features of the app. Different tools are used for directory analysis includes Dex2Jar, JD-GUI, APK-tool. Data partition model by Rajchada is shown in figure 4.

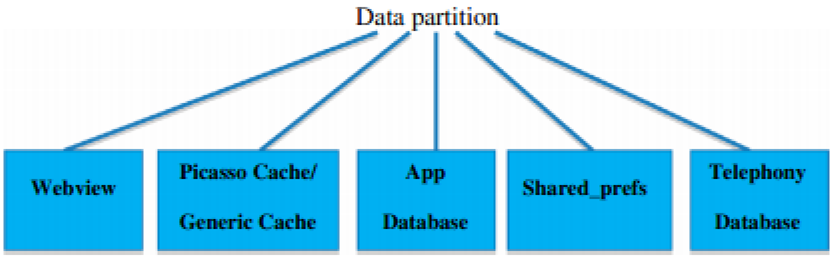


Figure 4- Data partition model by Rajchada Chanajitt [19]

## 2.4. Social & Chat application forensics

H Zhang et al. [16] conducted a digital forensic analysis of instant messaging application. They have selected four popular applications, Facebook, WhatsApp, Hangout and Line. They have investigated user chat messages and contacts list of each application. They have collected artifacts related to encryption status and chat messages for every application. SQLite databases examination was carried out to recover instant messages from different applications. Different apps encrypted messages locations with identifiers were analyzed. Location coordinates were collected to reconstruct the location of the sender's messages. For data collection hardware and software-based methods were used. Two different android phones were used for experimentation, 1-Google Nexus with OS 7.1.1 and Moto E with OS 6.0.1. For data collection, proposed approach rooted the devices.

## 2.4 Android application forensics tools

A big challenge to android forensic is the variety of android devices with different OS version that keeps on changing with the passage of time. No single tool is able to perform forensics for all android devices. Htar Htar Lwin et al. [22] conducted a comparative study of different tools used for android forensics. In this study they have analyzed different tools used for forensics to increase the accuracy and integrity. Both logical and physical method of data extraction were used. Tools include ADB, Linux DD utility, Magnet Acquire and Belkasoft Acquisition. Autopsy and Belkasoft evidence analyzing. Study showed that multiple tools can increase the integrity and reliability of the artifacts. Logical data acquisition relies on data available on file system. With logical data acquisition partial data can be extracted from device as it can’t extract deleted data from the file system. USB cable is used to connect the device with workstation and ADB and DD utility is used to extract the logical data form the device. In contrast to logical acquisition, a physical data extraction extracts all data on the device. Physical acquisition is not dependent on android file system. Magnet Acquire and autopsy are used in comparison to evaluate the results from both tools.

Another comparative study presented by Aiman Al-Sabaawi et al [23] on android forensic process for acquiring and analyzing android disk image. Four different tools are used to analyses data one using ViaExtract on a Linux VM, two tools used on AccessDataFTK Imager, and last in Autopsy on a Kali Linux VM.  Results showed that different artifacts can be collected which includes call logs, SMS, Photos, videos and contacts. The EaseUS Data Recovery tool is used for deleted files to recover from the extracted memory. Researcher tried to address the challenges involved in the acquisition and analysis. Challenges include complexity and verity of android application mainly dependent of underlying hardware and vendor specifications. The cost of the commercial tools and diversity of the techniques and procedures involve in obtaining data and further analysis. Study reveals that data recovery software is the best way to recover the deleted data on the device.

Imam Riadi et al [24] conducted the forensic tool comparison study on Instagram app with NIST method. This study utilized the NIST method which provides multiple stages of evidence collection, examination and analysis & Reporting, whereas, tools like oxygen and axiom magnets are utilized in this study. Researcher used quantitative comparison method based on expected data retrieval from the tool. Study showed that the Axiom Magnet result was 100% while Oxygen Forensic tool result was 84%.

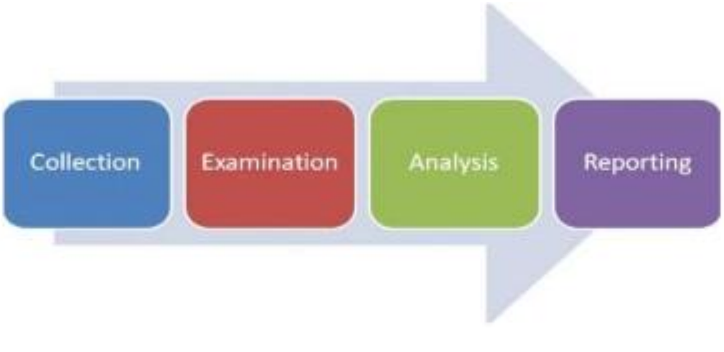


Figure 5- NIST Stages followed by Imam Riadi [24]

## 2.5 Android application productivity and navigation

Researchers suggested that productivity apps can increase worker productivity by more than 34% [26]. As being a rich source of information productivity apps are analyzed by several researchers. Theodoula-Ioanna Kitsaki et al. [15] carried out forensic investigation on few popular productivity apps available on play store. The aim was to collect sensitive data / information pertaining to the owner of mobile. The selection of apps was based on the popularity of the app, handling sensitive data, previously not evaluated by any researcher and freely available to all android users. Three chosen application belongs to three different categories like one belongs to banking, second belongs to mobile network carrier and third belongs to transport sector. They have separated forensics analysis into two categories: one code and second disk analysis [15]. Source code analysis was carried out to learn about sensitive date handling at developer end and disk analysis was carried out to collect sensitive data artifacts available on mobile device. In code analysis .apk file was decompiled and java code was extracted from that .apk file using some opensource tools like APKtool, dex2jar and jd-gui. jd-gui provides the graphical interface to analyze the jar files, it also extracts the .class files from the jar files for detail analysis. Whereas in disk analysis rooted android devices is used for application analysis along with Root Browser and DB Brower for SQLite.

Azfar et al. [25] conducted a study on productivity apps. They have examined 30 different productivity apps and analyze the remnants of the productivity apps. They have collected the data by logical extraction and used forensic tool XRY. They have collected information from these apps which include username, email id and list of task.  They have purposed two-dimensional taxonomy of the artifacts. The collected artifacts are summaries through taxonomy and comparison is done with existing taxonomies of different android apps categories.

## 2.6 Research consideration of travelling applications

Literature review enabled us to identify the current trends in the world. As discussed earlier, smartphone adoption is rapidly increasing in today’s world. Usage of utility application like mobile banking, e-commerce and travelling application are now prevalent. Previously there is reached carried out on utility applications like mobile banking and e-commerce.

As per our knowledge, there is no such work related to travelling app forensic exits which motivate us to conduct forensic analysis of travelling application.

# Chapter 3

# 3. Resarch Methodolgy

In this chapter, research phases with adopted methodology will be discussed in detail.

## 3.1 Introduction

In this section, we will discuss about proposed procedure model which we have followed for this examination. The periods of examination and selection of technique will be the focal point of fixation. The part conveyance is as followed

- Research Cycle (Section 3.2) explains the Research cycle we have followed in this study
- Phases of Research (Section 3.3) explains the different phases of research
- Research Approach (Section 3.4) elaborate the research approach followed in this study
- Workflow framework (Section 3.5) discussed the framework used in this study.

## 3.2 Research Cycle

A research cycle characterizes deliberate way, followed in a research. Its different stages comprise of various methods used to obtain results. Research cycle organizes the activities to achieve intended results in an organized manner. Research cycle followed in this investigation comprises of the following mentioned steps.

- First: Problem Area / Statement
- Second: Literature Study / Review
- Third: Research Reason / Purpose
- Fourth: Data Gathering / Collection
- Fifth: Data Analysis / Examination
- Sixth: Results Presentation / Findings

The above mentioned six phases are discussed in “J.Creswel’s book” on “Education Research” [8]. Figure 6 gives research cycle’s graphical representation.

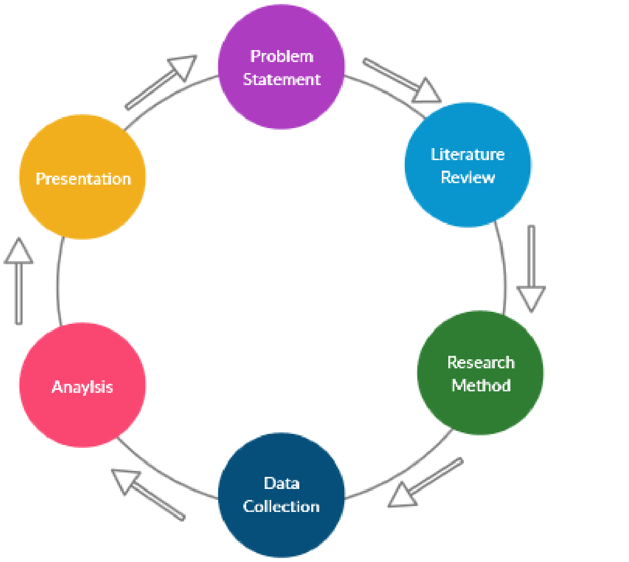


Figure 6-Research Cycle [8]

## 3.3 Phases of Research

Extracting the phases from research cycle we developed six research phases to organize this study in a systemic approach. Our extracted six phases have some modification as per requirements.

## 3.4 Research Approach

Six phases that we have extracted from our research cycle are explained for better understanding. We have explained the W’s of the research problem, literature review findings and research questions. Also, we have discussed mobile device forensic research design approach.

### 3.4.1 Getting Problem statement

Prior to beginning the research, problem statement recognition is a vital. Especially this stage is useful in distinguishing the space enthusiasm of the research. At first place research starts digging into the matter to know complete details about the domain. There are chances that some research might have done some work on the same domain that can be review from literature's study.

After getting sufficient details about the problem domain research start making problem statement with initial draft. Five w's what, why, where, who and when are very helpful in identifying the problem statement.

The five W's of research are discussed to have precise problem statement

**i)** **Who** is conducting this research, who is the beneficiaries of this study, who funded this study?

This research is conducted by Muhammad Anwar for forensics community and forensics practitioners. This research will benefit forensic community and forensics investigators. The study is conducted under the umbrella of National University of Sciences and Technology.

**ii)** **What** is this research? What is the significance of this study? And what steps involved in this study?

This study is about Forensics study of Android based Careem travelling application. This study will forensically examine the application which will help forensic investigators and research community to quickly analyze the application for evidence. We have devised different cases for forensic examination of the application based on real usage scenarios. The tools used in this study are mentioned in upcoming chapters.

**iii)** **Where** did this study conducted?

This study is conducted in National University of Sciences and Technology H-12 Campus. Most of the research part is conduct at home. Activities performed are under semi Controlled environment, as this application requires to visit different places, we have following NIST guidelines in this perspective.

**iv)** **When** this study is conducted?

Different time frames are assigned according to activities performed on the device with appropriate notations. For example, T1 denotes the time for collection of data, T2 denotes the analysis time and T3 is for presentation.

**v)** **Why** this research is required?

Forensic examination of the application will help forensic investigators, practitioners and research community in forensic investigation of the application with same functionality.

### 3.4.2 Literature Review findings

Literature review has significant importance in research process. To get sufficient information about problem domain, researcher needs to study previous research work if already done in same domain, and if there is already some research than researchers need to identify the gap between existing study and previous studies. Literature review gives clear understanding of problem domain. Some essential steps for efficient literature review are:

i) Look for relevant research papers
ii) Select papers within previous five years gap.
iii) Select 20-30 papers of Selected domain
iv) Give them sequence with respective to research time and domain knowledge
v) Go through Research Abstract and Conclusion
vi) Select the papers which are relevant to current study
vii) Extract useful point and enlist them make short summaries
viii) Comprehensive analysis of that summaries
ix) Shortlist most recent and relevant papers
x) Give a thorough review to selected papers.

### 3.4.3 Research Method

After finding gap between existing problem and previous studies we moved to formulate research method. By formulating research method, we try to answer the problem question in a systematic approach. It elaborates all the aspects from collection of data to timeframe implementation. This study is qualitative and qualitative search give us more freedom in data collection perspective. Forensic artifacts collection from travelling application is the intended purpose of this study. So, question is how can we say that these artifacts are useful for intended audience (Intended audience list already discussed)? And the answer is we will categories all data according to application usage scenarios and will analysis the significance of the data with respect to its criticality. We have adopted case study approach which incorporates our research cycle. In Case study methodology we have observed real world situation for application usage. The case study approach further divided into four steps:

- Case Selection and Situation identification
- Collection and recording
- Data interpretation
- Report writing

National Institute of Standard and Technology (NIST) provide some structure approach for mobile forensic. NIST framework consists of four stages which are incorporated in our model and that be seen in figure 7.

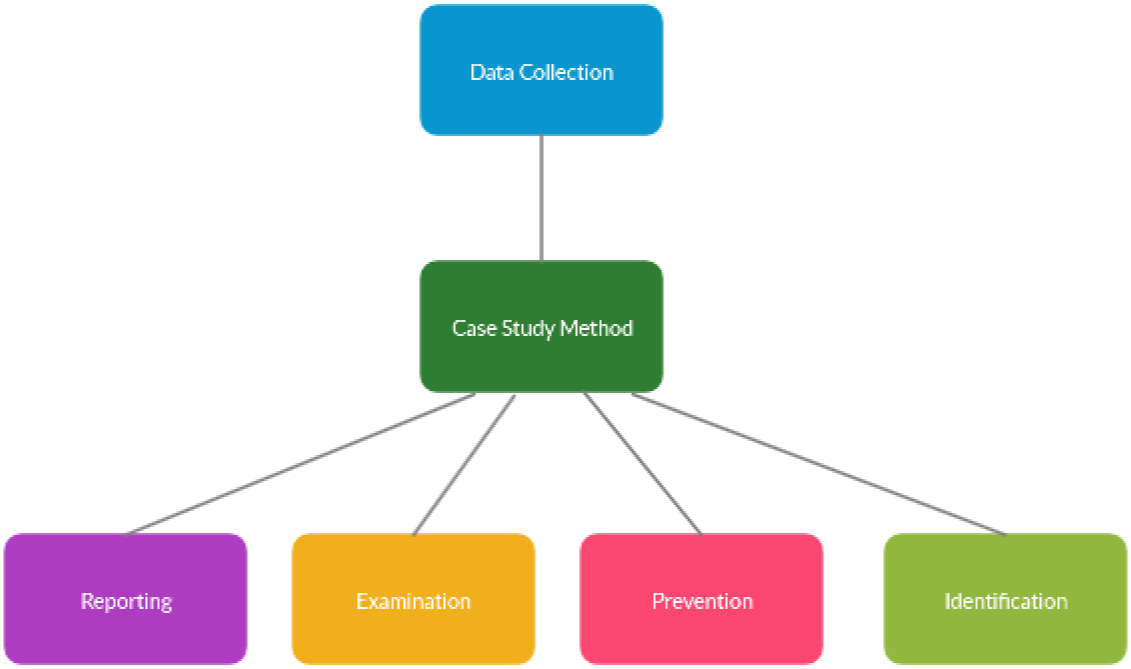


Figure 7-Research cycle with NIST Guidelines

### 3.4.4 Data Collection

Data collection is an important step in research process. Generally, research results are dependent on the data which is being collection for analysis. As we mentioned previously that it is a quantitative research and we have the flexibility of data collection. In this study we have developed cases based on real usage of application. In which, various activities were performed on application by the users in real life situation.

Based on our research cycle we have mapped our activities.

- **Identification**
  Sources → Acquisition →Maintaining log →Chain of custody
- **Prevention**

  Environmental isolation → Securing →Controlling device → Removing network access

- **Examination**
  Tools selection → Exploring evidence → Removing redundancies
- **Reports / presentation**
  Summarizing results → Conclusions → Report

**a) Case Selection and Scenario identification**

In this section, we discussed the five cases that are constructed to collect the artifacts from mobile device are listed below:

i. Case No. 1: App Info

Application is downloaded from google play store for installation. Application is updated and having latest version available to users. Case details are mentioned in table 1.

Table 1- App Info

| Case ID | Title | Information |
|---|---|---|
| 01 | Activity | App installation on Device. |
| 02 | Details | Collection of artifacts related to app installation time, Access time. |
| 03 | Goal | Collect data related to installation time, First Open, app update time, Last access for application. |

ii. Case No. 2: Login & account info

After the app installation next feature is login. There is an account creation procedure which is already done to obtain login credentials for the user. Table 2 show the activities done through this case.

Table 2- Login & account info

| Case ID | Title | Login to application and Profile info |
|---|---|---|
| 01 | Activity | Login through valid Username and Password |
| 02 | Details | Login artifacts collection by checking login date and time. Profile information of the User. Username, Email, Contact number etc. |
| 03 | Goal | It provides the user interaction with application. Common artifacts are login date and time and how frequently this app was used. Moreover, User account information such as Username, email and contact number. |

iii. Case No. 3: Booking Activity

After successful login into the application, user is expected to perform certain task through this application like booking, ride, and chat during ride etc. Below mentioned table 3 contains the booking activity.

Table 3- Booking Activity

| Case ID | Title | Seat booking / reservation through app |
|---|---|---|
| 01 | Activity | App user booking / reservation activity |
| 02 | Details | To Collect artifacts related to booking activity performed by app user. There are several other tasks during the booking activities are performed like chat with Driver. Checking deriver info, Taxi / Car info etc. |
| 03 | Goal | It provides the user activity artifacts related to booking / reservation includes chat, booking date, time, destination, fare etc. |

iv. Case No. 4: Financial / Transactional Activity

User will make some transactional activity by paying ride fare, making payment through Credit card, Mobile recharge, Food delivery charges etc. The case 4 activity can be shown in table 4.

Table 4- Financial / Transactional Activity

| Case ID | Title | Financial Activity through app |
|---|---|---|
| 01 | Activity | App user pay fare /bill online |
| 02 | Details | To Collect artifacts related to Financial activity done through app like online payment of the fare. |

|  |  |  |
|---|---|---|
| 03 | Goal | The remnants related to financial activity should be record. It may be credit card information, account details etc. |

v. Case No. 5: Interaction with Third Party (if any)

Last case is based on application internal usage. If this application is utilizing any 3rd party service User interaction and artifacts are collected. The table-5 shows the activity with detail.

Table 5- 3rd party Interaction

| **Case ID** | **Title** | **Third party Interaction** |
|---|---|---|
| 01 | Activity | App user interact with any third party |
| 02 | Details | To Collect artifacts related to any third-party API's, interaction through this app |
| 03 | Goal | It provides the user activity artifacts related to Third party communication through this app. All remnants are collected. |

## b) Collection & Recording

### i) Data Identification & collection

The next step is to collect data after user preform some activity on mobile according to cases. So, data is collected by taking complete image of the mobile phone bit by bit. We used Nexus 6P with 32GB Memory and OS version 9 (Pie).

The process of identification and collection in show in Figure 8.

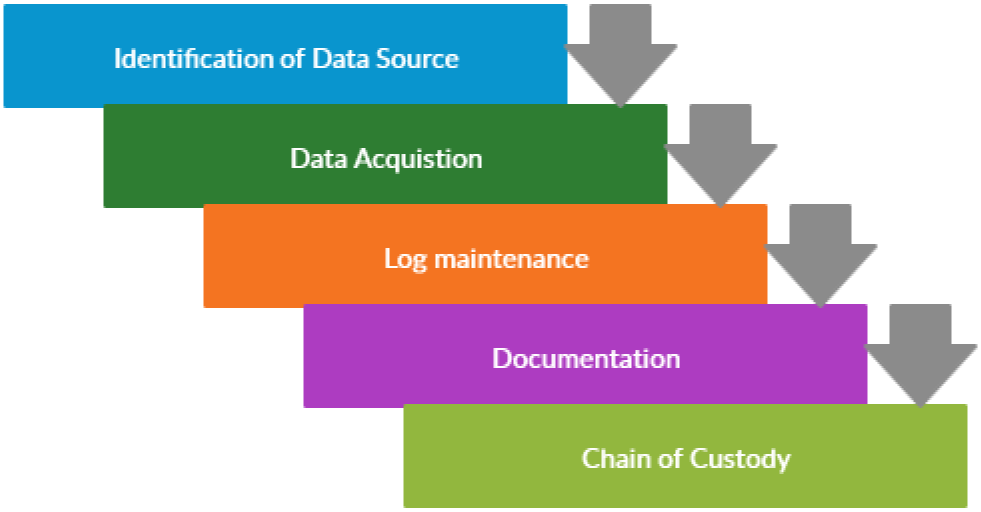


Figure 8-identification & Collection

a) Data Source Identification

After performing any activity, a bit by bit physical image of the complete memory of mobile phone is taken. Multiple activities are performed according to above cases. We make a comparison of every image with our base image.

b) Data Acquisition

Data is acquired while utilizing 3 steps approach, which can be seen in figure 9:

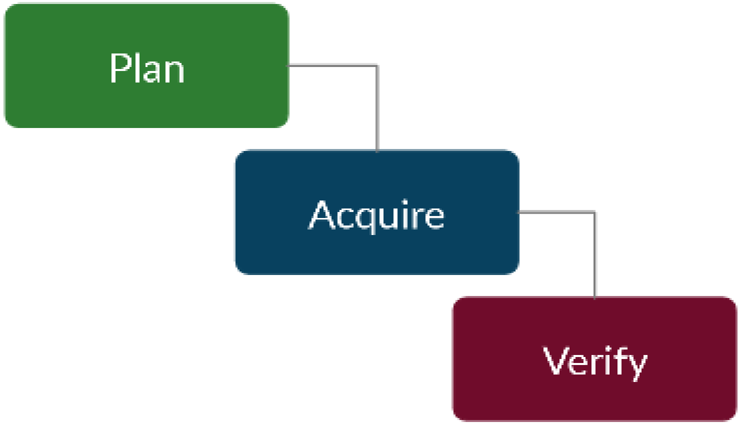


Figure 9-Acquistion of Data

In first step plan is consist of required data and process of acquiring the required data. Second step include actual process of acquiring and preparing it for analysis. In third step verification is done through hash calculation of both original and copied data to check the integrity of the acquired data.

c) Log Maintenance

Logs are maintained about tools and followed process / procedures. Maintaining log is an essential step to track the process.

d) Documentation

All the activities are documented. This will keep the record of each and every activity performed for data acquisition, respectively. Where this will help forensic examiner to reproduce same data by following the documentation.

e) Chain of Custody

Chain of custody is maintained to avoid any sort of tempering in acquired data. For chain of custody following protocols are considered

- Device accessed physically
- Strict timestamp maintained with every activity
- Duplication of evidence
- Evidence custody with secure procedures

**ii) Preservation**

Preservation is an important aspect of digital forensics investigation. NIST provide clear guidelines about the data preservation. Data preservation is critical, as results authenticity will become doubtful. From Preservation perspective we duplicated the extracted data. We calculated the following hashes of the image to keep the integrity of the data intact.

- MD5
- SHA1
- SHA256
- SHA512
- CRC32

### 3.4.5 Analysis

Analysis is the fifth phase of research cycle. It includes the 3rd step of case study which is the data interpretation.

**c) Data interpretation**

According to NIST guidelines 3rd step involves:

iii) Examination

A thorough analysis of complete physical image of the mobile device is performed. A brief summary is given below:

- Location identification for performed activities
- Checking for remnants of activities
- Examining the unallocated disk space for evidence.
- Examining the database contents
- Examining the cross-reference locations
- Examining the deleted content for evidence.

### 3.4.6 Reporting

Reporting is the last phase of research cycle and case study. Results are presented in this phase. This phase answers the problem statement and facilitates the researcher with the working of this study.

**d) Reporting**

Report writing ought to be finished in all perspectives in light of the fact that fragmented data may prompts misconception and bogus understanding of performed work. Under the guidelines of NIST case study last step emerges here.

iv) Presentation

Presentation of this investigative work incorporates the fundamental subtleties of work as per target audience. For instance, a court of law requires more details of all the finish up results as contrast with normal end user. In this way, presentation ought to incorporate rundown of all follow systems to the finish of the exploration work. From that point onward, conclude presentation ought to be arranged in the ideal organization of audience: ".doc, .ppt or .pdf." Final document will contain Tables and Figures for better comprehension of completed exploration work.

## 3.5 Workflow Framework

In qualitative research, research questions are very important. If the results of the study answer the problem statement, then it validates the study.  To answer research questions, we have designed the following frameworks.

a) Investigation Framework: A framework incorporates the activities for inquiring the research work

b) Analysis Framework: Analyzing the evidence and presenting the results to answer the question.

# Chapter 4

# 4. Evidence Collection and Experimentation

This chapter contains the information related to experimentation, procedure and the utilized tools.

## 4.1 Introduction

In this chapter we will be discussing following topics

- Hardware Specifications (Section 4.2) elaborate the hardware specification of the mobile device used for experimentations.
- Tools & Technologies (Section 4.3) highlights the tools and technologies used
- Environmental setting (Section 4.4) discuss about Environmental setup
- Connecting Device (Section 4.5) discuss the device connectivity with workstation
- Device Access (Section 4.6) explains the device access from workstation
- Getting Root Access (Section 4.7) explains the procedure of rooting device.
- Device partitions (Section 4.8) explains the device partition information
- Acquiring device image (Section 4.9) discusses the image acquisition procedure.
- Physical method for image acquisition (Section 4.10) explains the physical method of image acquisition.

## 4.2 Hardware specifications

In this study we have used following hardware for our experimentation.

### 4.2.1 Mobile Device Specifications

- Huawei Nexus 6P
- PIXYS OS Android Version 9
- 32 GB internal memory
- Octa-core (4x1.55 GHz Cortex-A53 & 4x2.0 GHz Cortex-A57

### 4.2.2 Workstation (Forensic)

- HP Probook 4440s
- RAM 16GB
- Core i3 @ 2.50 GHz

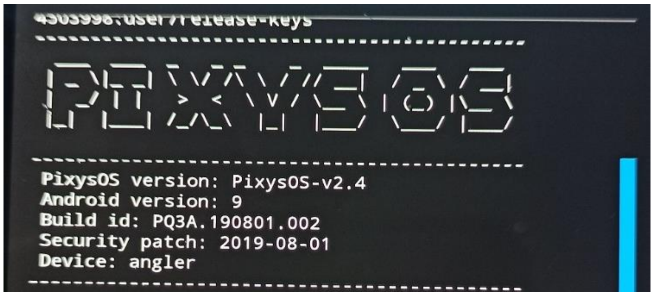
## 4.3 Tools and Technologies

For this study we have used several tools which are listed below:

### 4.3.1 Software tools installed on mobile / smartphone

- Custom ROM PixyOs
- Pie Android version 9
- MAGISK Root
- BusyBox
- Termux
- Careem Application

Figure 10 shows the installed version of OS on the mobile device.



```
4303998:user/release-keys
------------------------------------------------
------------------------------------------------
PixysOS version: PixysOS-v2.4
Android version: 9
Build id: PQ3A.190801.002
Security patch: 2019-08-01
Device: angler
------------------------------------------------
```

Figure 10-installed OS info

### 4.3.2 Software installed on Forensics workstation

- Microsoft Windows 10
- Bitdefender Antivirus Free edition
- Autopsy Sleuth Kit 4.13.0
- ADB tools
- DB Browser for SQLite Version 3.11.2

- DCode Version 4.02a Build 9306
- Notepad++

## 4.4 Environmental Settings

This section contains the information related to environmental setup for android device and workstation.

### 4.4.1 Smartphone / Mobile device

For mobile device we have made following environmental setup

a) Power

Ensuring proper battery charging level is essential to continue with un-interrupted experimentation. Device is charged with recommended power charger to ensure proper charging level.

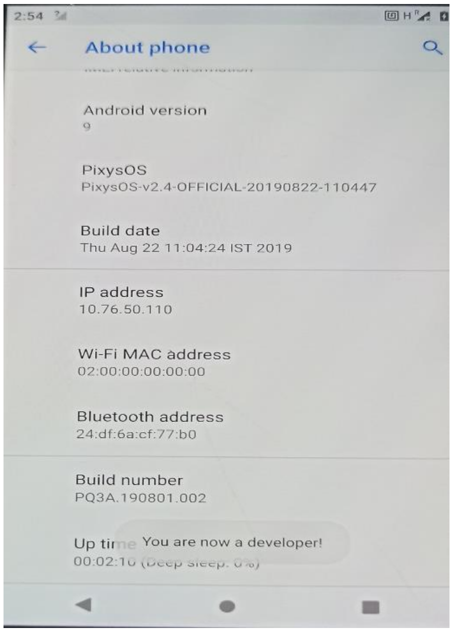
b) Allow installation from unknown source

It is necessary to make some changes in android phone setting to installed software from USB. Allowing installations from unknown sources are enabled as it is required by some of the software that is required for experimentation. This option can be unable by following way.

- Go to setting, find security option where you can see a check box for allowing installation form unknown sources.

c) Enabling Developer option

Next step is to enable Developer option. In setting menu, we have selected about phone option. A new menu appears with different option as show in figure 11. We have tapped the Build number 7 times and a popup appeared with message “you are now a developer”.



2:54

About phone

Android version
9

PixysOS
PixysOS-v2.4-OFFICIAL-20190822-110447

Build date
Thu Aug 22 11:04:24 IST 2019

IP address
10.76.50.110

Wi-Fi MAC address
02:00:00:00:00:00

Bluetooth address
24:df:6a:cf:77:b0

Build number
PQ3A.190801.002

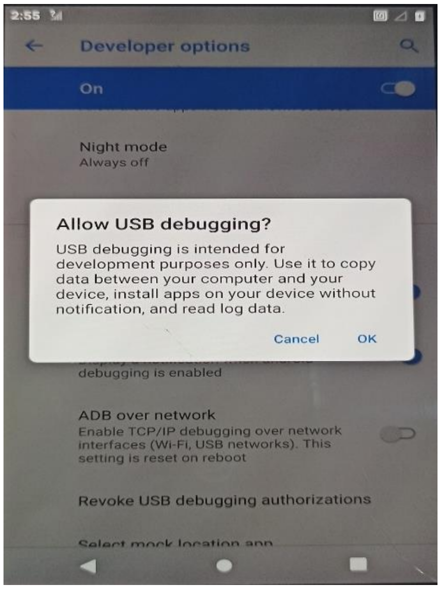
Up time
00:02:10 (Deep sleep: 0%)

You are now a developer!

Figure 11-About Phone menu

d) UBS Debug Mode enabling

Enabling USB Debug Mode is also important to access device from workstation. After enabling developer option, we have "Developer Options" menu in our settings tab. We have selected developer options for setting tab and a new menu appear with different options as show in the figure 12. We have checked the option "Allow USB Debugging" and a warning message appeared, tapped ok option.



2:55

Developer options

On

Night mode
Always off

Allow USB debugging?

USB debugging is intended for development purposes only. Use it to copy data between your computer and your device, install apps on your device without notification, and read log data.

Cancel OK

debugging is enabled

ADB over network
Enable TCP/IP debugging over network interfaces (Wi-Fi, USB networks). This setting is reset on reboot

Revoke USB debugging authorizations

Select mock location app

Figure 12 -USB Debugging

e) Installing Magisk

When we say system less root method then we are talking about Magisk as it is known as a “systemless” root method. It is a way to have root level access without modifying system. While using Google play services Magisk can provide root level access and custom modes. Magisk is not altering the boot partition or any system partition while provide root level access. Therefore, it's regarded as a “systemless” root method [9].

f) Checking Root level access

Open the Magisk from GUI options available in the main menu. Check the phone status.

g) Installation of BusyBox

BusyBox provides range of Unix utilities in a single executable file. A range of POSIX environments such as Linux, Android support the BusyBox application [10]. As in this study we need DD method to acquired device image, but this DD utility is not available in android devices by default. So, by installing BusyBox we can use DD method to acquire device bit by bit image.

### 4.4.2 Forensic Workstation

a) Antivirus

Presence of Antivirus software is important so that forensic system remains sterilized. We have installed Bit Defender Free antivirus to keep forensic workstation clean from malwares. Bit Defender provides real time protection from any malware attack.

b) Autopsy Sleuth kit 4.13.0

Autopsy is computer software program that performs forensic analysis of underlying volume providing easy way to flag the content through powerful GUI interface. Autopsy supports major file systems including NT file system, File Allocation Table (FAT), Extensible File Allocation Table (ExFAT), Hierarchical File System HFS+, Ext2/Ext3/Ext4 by hashing all files extracting any EXIF values and putting keywords in an index. Not all but some file types for example standard email formats can also be pared by autopsy [11]. We have used Autopsy Sleuth Kit Version 4.13.0 for this study.

c) Android debug bridge (ADB) tools

Android Debug Bridge (ADB) is a command line tool that allows you communicate with an android device. Through ADB different task can be performed like app installation and application debugging, and it provides access to a Unix / Linux shell that can be used to run a variety of commands on a device.

d) DB Browser for SQLite

DB Browser for SQLite is used to analyze the extracted database files from mobile device. Database files which are extracted from device image are further analyzed through DB browser to get artifacts that are stored within the SQLite database file.

e) DCode

DCode is used to covert timestamp of different activities that are stored in mobile device. In Unix / Linux devices timestamp is store in Epoch format that is not human friendly readable format. To convert that timestamp, we have utilized this utility software to get human readable format of timestamp.

f) Netcat

Netcat is command line utility use to transfer data over TCP/IP. We used netcat utility to transfer the data which is obtained through DD method from mobile device to Forensic workstation.

g) Notepad++

Notepad is advance text editor. We have used this text editor to view some of the extracted XML files.

h) Termux

Termux is an Android terminal emulator. It works without rooting the device and helps to check different utilities installed on the device.

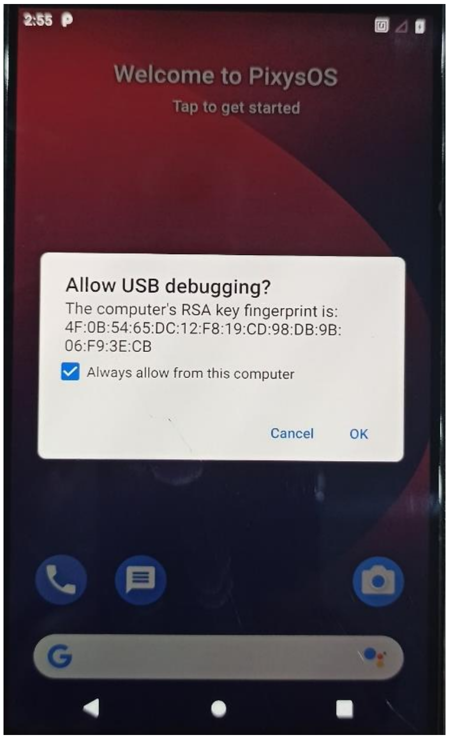
## 4.5 Connecting Device

After environmental setup on workstation and smartphone / mobile device we have established a connection between forensic workstation and mobile device. We have used USB data cable for connecting mobile device with forensic workstation.

## 4.6 Device Access

After connecting USB cable one end with mobile device and other end forensic workstation, a successful connection has established. Mobile device now can be accessed from forensic workstation. To perform certain action, we open ADB tools in window’s PowerShell. Following methods and commands are used to access mobile device.

- Typed “adb devices” to get the list of connected devices
- A popup appeared on mobile screen for displaying workstation fingerprint need to allow for connection as show in the figure 13.
- Select option “Always allow this device” and clicked Ok
- Connected devices are displayed.
- Typed “adb shell” to get the shell access of the mobile device.



Allow USB debugging?

The computer's RSA key fingerprint is:
4F:0B:54:65:DC:12:F8:19:CD:98:DB:9B:
06:F9:3E:CB

☑ Always allow from this computer

Figure 13 -Device Signatures

## 4.7 Getting Root Access

After getting shell access we need root privileges. To have root level access on mobile device we need to root the mobile device. Mobile rooting procedure is described below

### 4.7.1 Smartphone root process

Android operating system is based on Linux Operation System. Mobile user has normal user rights with limited privileges which can only perform normal task with specific permissions. It has limited access to system files with limited permissions. So, a root level or super user access mobile phone rooting is required.

### 4.7.2 Why rooting is required

As discussed earlier android phone user has limited rights to access operation system files and protected directories. For forensics investigation we need full control over device to access all system files and protected directories inside the android phone. As root user has all privileges on Android OS, he/she can access all system files and protected directories. After getting ADB shell we tried to access data directory, but it was not accessible with normal user rights.

### 4.7.3 How to root

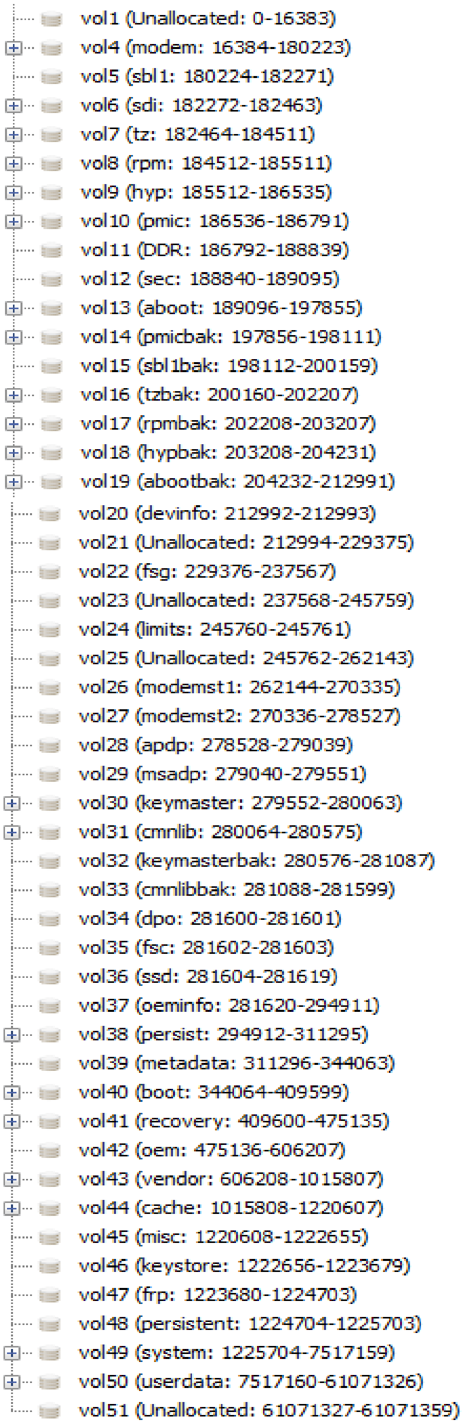
Following step were followed to get root level access.

- Power off the device
- Press Power button + Volume down button for 5 second
- Android starts in recovery mode
- Installed TWRP in the device
- With the help of TWRP installed Magisk

After reboot we have verified the root access by Termux or any root level checker from google play store.

## 4.8 Device partitions

Android device has several partitions. All partitions have different usage as per android OS system layout. Partitions are quite different by device make and model. Despite of the fact that partitions are not consistent among different vendors some partitions are persistent due to android operating structure. These consistent partitions are the vital source of information for forensic examinations. Layout of device we have used in this study is shown in the figure 14.



```
vol1 (Unallocated: 0-16383)
vol4 (modem: 16384-180223)
vol5 (sbl1: 180224-182271)
vol6 (sdi: 182272-182463)
vol7 (tz: 182464-184511)
vol8 (rpm: 184512-185511)
vol9 (hyp: 185512-186535)
vol10 (pmic: 186536-186791)
vol11 (DDR: 186792-188839)
vol12 (sec: 188840-189095)
vol13 (aboot: 189096-197855)
vol14 (pmicbak: 197856-198111)
vol15 (sbl1bak: 198112-200159)
vol16 (tzbak: 200160-202207)
vol17 (rpmbak: 202208-203207)
vol18 (hypbak: 203208-204231)
vol19 (abootbak: 204232-212991)
vol20 (devinfo: 212992-212993)
vol21 (Unallocated: 212994-229375)
vol22 (fsg: 229376-237567)
vol23 (Unallocated: 237568-245759)
vol24 (limits: 245760-245761)
vol25 (Unallocated: 245762-262143)
vol26 (modemst1: 262144-270335)
vol27 (modemst2: 270336-278527)
vol28 (apdp: 278528-279039)
vol29 (msadp: 279040-279551)
vol30 (keymaster: 279552-280063)
vol31 (cmnlib: 280064-280575)
vol32 (keymasterbak: 280576-281087)
vol33 (cmnlibbak: 281088-281599)
vol34 (dpo: 281600-281601)
vol35 (fsc: 281602-281603)
vol36 (ssd: 281604-281619)
vol37 (oeminfo: 281620-294911)
vol38 (persist: 294912-311295)
vol39 (metadata: 311296-344063)
vol40 (boot: 344064-409599)
vol41 (recovery: 409600-475135)
vol42 (oem: 475136-606207)
vol43 (vendor: 606208-1015807)
vol44 (cache: 1015808-1220607)
vol45 (misc: 1220608-1222655)
vol46 (keystore: 1222656-1223679)
vol47 (frp: 1223680-1224703)
vol48 (persistent: 1224704-1225703)
vol49 (system: 1225704-7517159)
vol50 (userdata: 7517160-61071326)
vol51 (Unallocated: 61071327-61071359)
```

Figure 14 -Android partitions

## 4.9 Acquiring device image

In mobile forensic there are two techniques that are widely used are logical image acquisition and physical image acquisition. Artifacts from mobile device are dependent on image which is acquired from mobile device also research results vary depending upon the image acquisition technique.

### 4.9.1 Logical method of Image Acquisition

In logical acquisition all the available data on the mobile phone is extracted. Image size always remain less the actual memory size because is only collect active data on the device. It ignores the deleted or unallocated space in the device storage. Therefore, removed or deleted artifacts are not available for forensic study. On the other hand, it is efficient, swift and supported by almost all devices. Several logical image acquisition methods are there for example SDcard imaging, Oxygen-Forensic, Android Backup Analysis. Android Backup analysis is considered best among them [12].

### 4.9.2 Physical method of Image Acquisition

In physical method of image acquisition whole memory is captured or dumped. In this method bit by bit image is copied along with all zeroes and ones. Physical image size is exactly same as device storage capacity [13]. Contrary to logical image acquisition physical image contain deleted data because it copies complete memory image regardless of allocated or unallocated memory space [14]. Different techniques like JTAG, Chip-Off, ISP and Boot loader flasher Box physical extraction are used for physical image acquisition. For some methods like Chip off and JTG hardware modification / alteration is required. While, other methods extract physical image without hardware modification like Boot-loader Flasher Box Physical Extraction. In our study we have adopted Boot-loader Flasher Box physical extraction using ADB and DD.

## 4.10 Physical Image acquisition procedure

To obtain physical image mobile device rooting is required. Rooting procedure has already been discussed in section 4.7.3. Netcat is installed on workstation to perform data read write operation through TCP/IP across network and busybox is installed on mobile device to get DD command utility on mobile device. Following step are considered while extracting physical image of the mobile device memory.

### 4.10.1 Connecting Device

After the installation of required software, we connected the mobile device with workstation through UBS cable. Opened the PowerShell window in the same directory where we have download adb.exe. Following sequence of commands are used to extract physical image from the mobile device.

- Used command “.\adb.exe devices” to list all attached supported devices, in our case we have only one device attached with forensic workstation.
- Used command “.\adb.exe shell” to get shell access on mobile device.
- Used command “ls -la” to list all directories
- Used command “su” to get root level access.

### 4.10.2 Extracting Image

After successfully establishing connection with mobile device we have opened another PowerShell terminal for port forwarding. We have forwarded the port “9999” of mobile device to forensic workstation.

- For port forwarding a command used “.\adb.exe forward tcp:9999 tcp:9999”
- Started netcat listener using command “.\nc.exe 127.0.0.1 9999 > full_image.dd”
- After that we have used Net cat and BusyBox application, with dd method to copy the entire memory block “mmcblk0” and forward that data on port 9999.
- Used command “dd if=/dev/block/mmcblk0 | busybox nc -lnvp 9999” to send the memory image data to port 9999.
- After completion of data transfer details appears on terminal which includes bytes transferred, time and rate of transfer statistics.

### 4.10.3 Saving Image

We have saved the acquired image in the same directory as of ADB. We moved the image to separate directory and renamed it so that we can distinguish between multiple images when we will extract new images from same device.

### 4.10.4 Extracting Artifacts Using Autopsy Sleuth Kit

After extracting image, we have used Autopsy sleuth kit Version 4.13.0 to perform analysis on this extracted image. Following step are taken to load image into Autopsy sleuth kit.

- Created “New Case” by clicking the option “New Case” as show in figure 15.

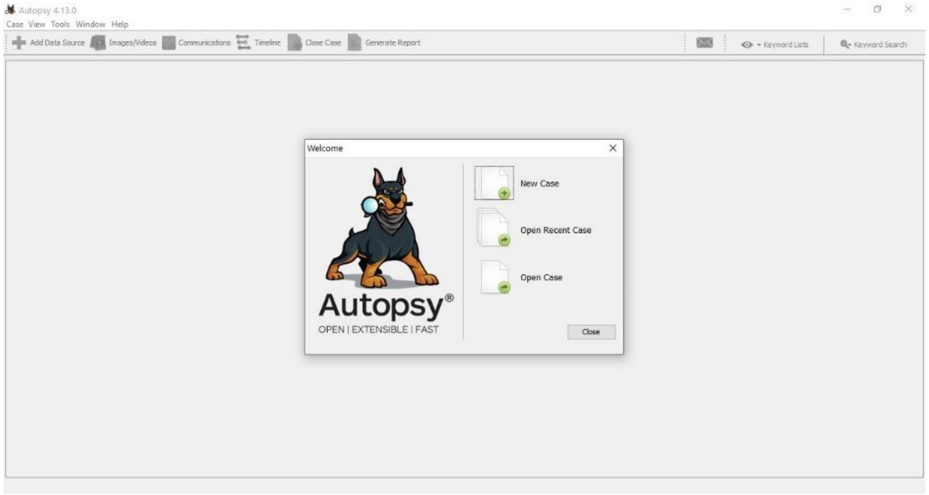
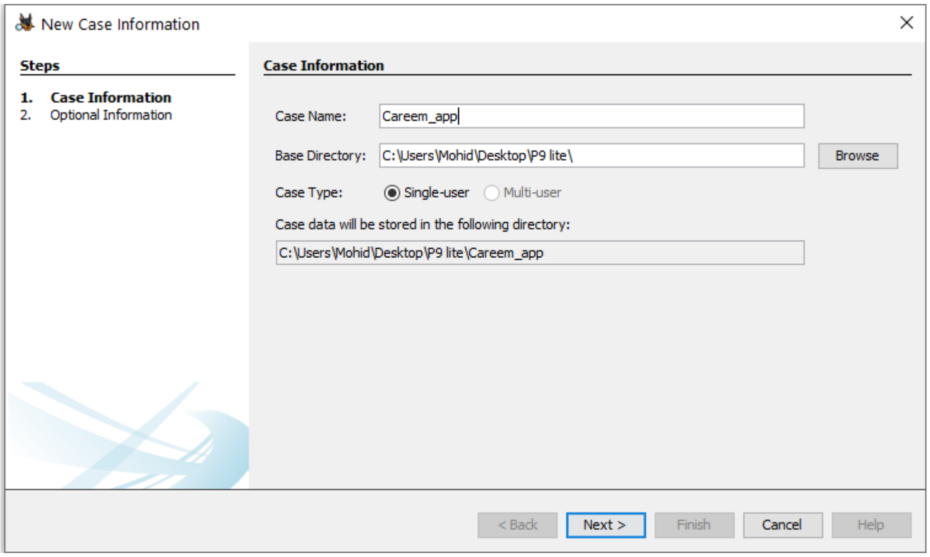


Figure 15 -Autopsy open new case

- Entered case name “Careem_app”
- Selected base directory “C:\Users\Mohid\Desktop\P9 lite\”
- Selected case type “Sigle user” as shown in the figure 16.



Case Name: Careem_app

Base Directory: C:\Users\Mohid\Desktop\P9 lite\

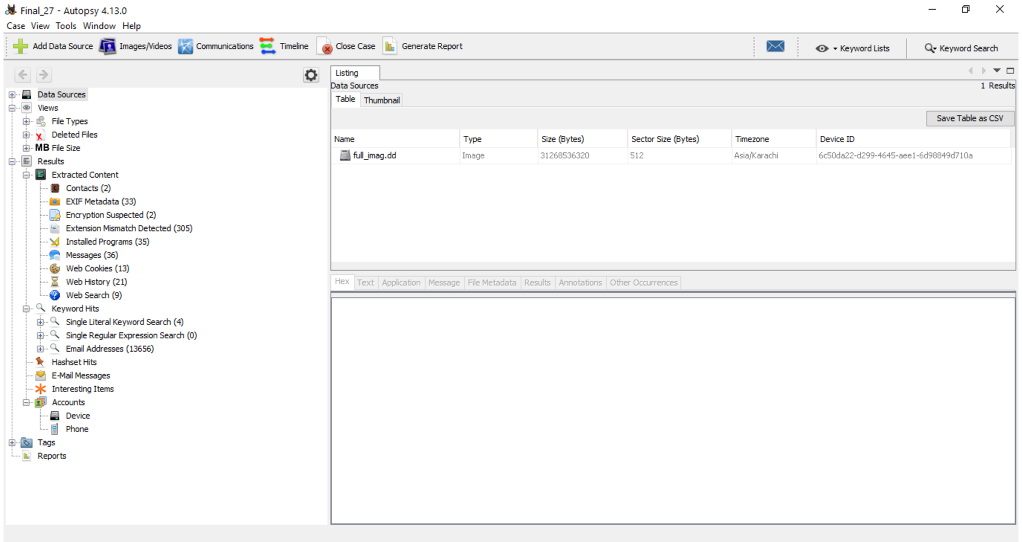
Case Type: ● Single-user ○ Multi-user

Case data will be stored in the following directory:

C:\Users\Mohid\Desktop\P9 lite\Careem_app

Figure 16 -Autopsy case name and directory selection

- Entered examiner information
- Clicked finished.
- Next selected data source of the Image. “Disk Image or VM file”
- Image successfully load as show in the figure 17.



Data Sources

1 Results

| Name | Type | Size (Bytes) | Sector Size (Bytes) | Timezone | Device ID |
|---|---|---|---|---|---|
| full_imag.dd | Image | 31268536320 | 512 | Asia/Karachi | 6c50da22-d299-4645-aee1-6d98849d710a |

Figure 17 -Image loaded in Autopsy

## 4.11 Summary of Evidence collection and experimentation

Artifacts extraction from the device in forensically sound manner is very critical for achieving forensics sound evidence. We have made all efforts to extract all possible artifacts from the device in forensically sound manner.

# Chapter 5

# 5. Analysis of the Application

## 5.1 Introduction

This chapter contains the analysis of the Careem application. We will discuss the remnants of the application and analyze the artifacts of the application.

## 5.2 Careem application

Careem is a taxi or ride booking service which was initially offered to Middle East region peoples. It is pioneer ride booking service in that region. Careem is expanding services across its platform to include mass transportation, delivery and payments to become the region's everyday SuperApp. Careem is providing simple way to book rides and other related services live delivery services conveniently. Careem was established in July 2012 and was acquired by Uber in 2020. Careem operates in over 100 cities across 14 countries [27].

We have used latest version of the application available on the play store at the time of experimentations. Keeping in mind the scope of our study we have performed following activities to identify the remnants location on the mobile device which can be seen in Table 6.

- C- AI (Careem - Application Information)
- C- ALA (Careem - Application Login & Account Information)
- C- BA (Careem - Booking Activity)
- C-TA (Careem - Transactional Activity)
- C-3PI (Careem - 3rd Party Interaction)

Table 6 – Activities with Case Code

| Case Code | Name | Activity Details |
|---|---|---|
| C-AI | Careem Application Information | • All information related to application including application download, directory, install date etc. |

| | | |
|---|---|---|
| C-ALA | Careem Application Login and Account Information | • All information related to application login details, account, User profile, Credit card information etc. |
| C-BA | Careem Booking Activity | • All information related to Booking activity performed on the device includes Pickup location, Drop location, In app chat, Driver picture, Vehicle number etc. |
| C-TA | Careem Transactional Activity | • All remnants related to payment, credit balance etc. |
| C-3PI | Careem 3rd Party Interaction | • All remnants related to 3rd party interaction like Google map API's, Google analytics |

## 5.3 Remnants of C-AI

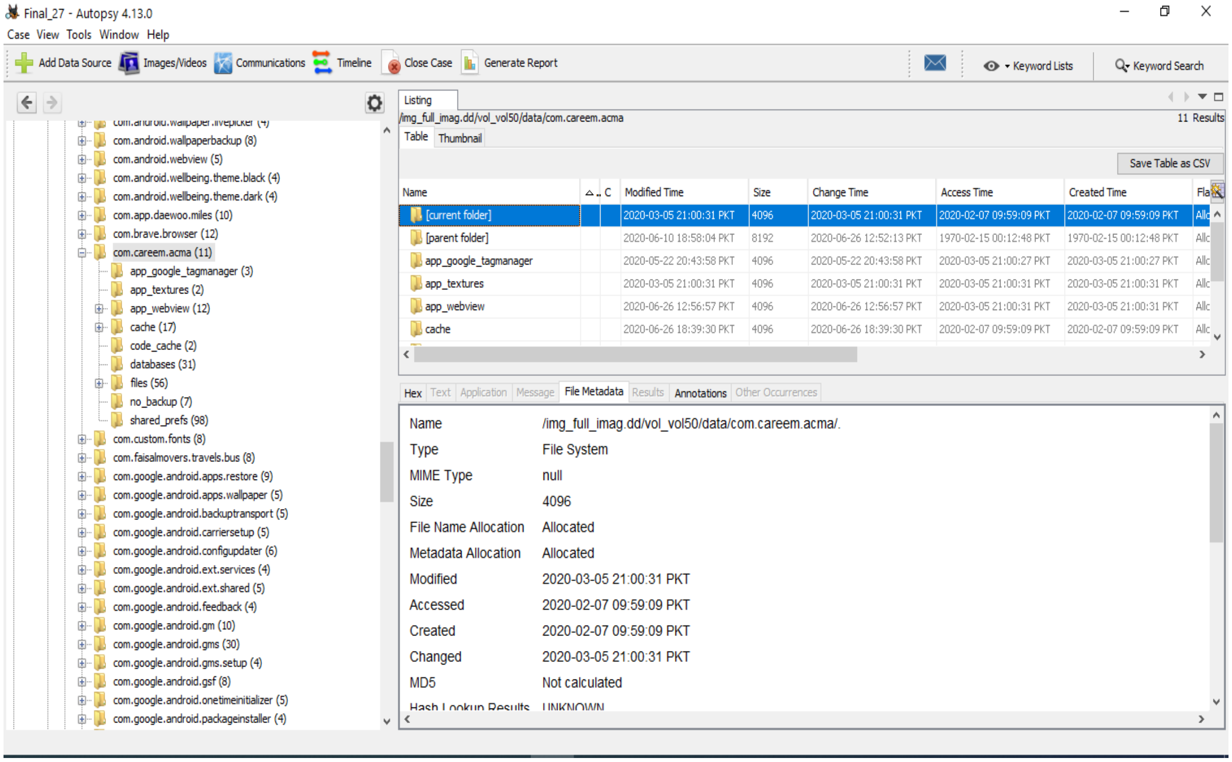
After preforming experimental activities following remnants were found.

### 5.3.1 Application Directory

In android operating system application parent directory keeps all application related data inside it. Parent directory resides inside the "data" directory. After the installation of Careem app it creates the directory "com.careem.acma".

Path: "imag.dd/vol_vol50/data/com.careem.acma/"

Which can be seen in figure 18.



- com.android.wallpaper.livepicker (4)
- com.android.wallpaperbackup (8)
- com.android.webview (5)
- com.android.wellbeing.theme.black (4)
- com.android.wellbeing.theme.dark (4)
- com.app.daewoo.miles (10)
- com.brave.browser (12)
- com.careem.acma (11)
  - app_google_tagmanager (3)
  - app_textures (2)
  - app_webview (12)
  - cache (17)
  - code_cache (2)
  - databases (31)
  - files (56)
  - no_backup (7)
  - shared_prefs (98)
- com.custom.fonts (8)
- com.faisalmovers.travels.bus (8)
- com.google.android.apps.restore (9)
- com.google.android.apps.wallpaper (5)
- com.google.android.backuptransport (5)
- com.google.android.carriersetup (5)
- com.google.android.configupdater (6)
- com.google.android.ext.services (4)
- com.google.android.ext.shared (5)
- com.google.android.feedback (4)
- com.google.android.gm (10)
- com.google.android.gms (30)
- com.google.android.gms.setup (4)
- com.google.android.gsf (8)
- com.google.android.onetimeinitializer (5)
- com.google.android.packageinstaller (4)

/img_full_imag.dd/vol_vol50/data/com.careem.acma 11 Results

| Name | △ .. | C | Modified Time | Size | Change Time | Access Time | Created Time | Fla |
|---|---|---|---|---|---|---|---|---|
| [current folder] | | | 2020-03-05 21:00:31 PKT | 4096 | 2020-03-05 21:00:31 PKT | 2020-02-07 09:59:09 PKT | 2020-02-07 09:59:09 PKT | Allc |
| [parent folder] | | | 2020-06-10 18:58:04 PKT | 8192 | 2020-06-26 12:52:13 PKT | 1970-02-15 00:12:48 PKT | 1970-02-15 00:12:48 PKT | Allc |
| app_google_tagmanager | | | 2020-05-22 20:43:58 PKT | 4096 | 2020-05-22 20:43:58 PKT | 2020-03-05 21:00:27 PKT | 2020-03-05 21:00:27 PKT | Allc |
| app_textures | | | 2020-03-05 21:00:31 PKT | 4096 | 2020-03-05 21:00:31 PKT | 2020-03-05 21:00:31 PKT | 2020-03-05 21:00:31 PKT | Allc |
| app_webview | | | 2020-06-26 12:56:57 PKT | 4096 | 2020-06-26 12:56:57 PKT | 2020-03-05 21:00:31 PKT | 2020-03-05 21:00:31 PKT | Allc |
| cache | | | 2020-06-26 18:39:30 PKT | 4096 | 2020-06-26 18:39:30 PKT | 2020-02-07 09:59:09 PKT | 2020-02-07 09:59:09 PKT | Allc |

| | |
|---|---|
| Name | /img_full_imag.dd/vol_vol50/data/com.careem.acma/. |
| Type | File System |
| MIME Type | null |
| Size | 4096 |
| File Name Allocation | Allocated |
| Metadata Allocation | Allocated |
| Modified | 2020-03-05 21:00:31 PKT |
| Accessed | 2020-02-07 09:59:09 PKT |
| Created | 2020-02-07 09:59:09 PKT |
| Changed | 2020-03-05 21:00:31 PKT |
| MD5 | Not calculated |
| Hash Lookup Results | UNKNOWN |

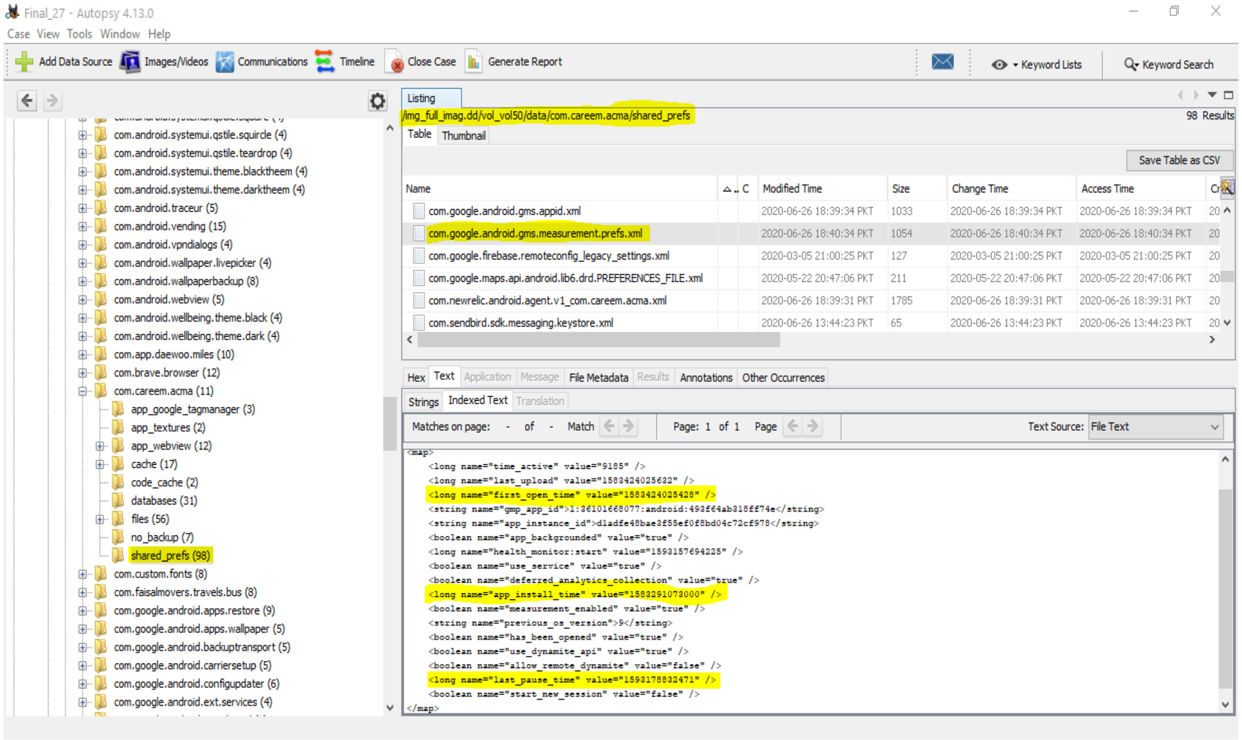
Figure 18 -Careem app Directory

### 5.3.2 Application Installation artifacts

We have found artifacts related to application on the following locations as you can see in figure 19.

path:

*“/img_full_imag.dd/vol_vol50/data/com.careem.acma/shared_prefs/com.google.android.gms.measurement.prefs.xml”*


Final_27 - Autopsy 4.13.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Timeline
Close Case
Generate Report
Keyword Lists
Keyword Search
com.android.systemui.qstile.squircle (4)
com.android.systemui.qstile.teardrop (4)
com.android.systemui.theme.blacktheem (4)
com.android.systemui.theme.darktheem (4)
com.android.traceur (5)
com.android.vending (15)
com.android.vpndialogs (4)
com.android.wallpaper.livepicker (4)
com.android.wallpaperbackup (8)
com.android.webview (5)
com.android.wellbeing.theme.black (4)
com.android.wellbeing.theme.dark (4)
com.app.daewoo.miles (10)
com.brave.browser (12)
com.careem.acma (11)
app_google_tagmanager (3)
app_textures (2)
app_webview (12)
cache (17)
code_cache (2)
databases (31)
files (56)
no_backup (7)
shared_prefs (98)
com.custom.fonts (8)
com.faisalmovers.travels.bus (8)
com.google.android.apps.restore (9)
com.google.android.apps.wallpaper (5)
com.google.android.backuptransport (5)
com.google.android.carriersetup (5)
com.google.android.configupdater (6)
com.google.android.ext.services (4)
Listing
Table
Thumbnail
Save Table as CSV
Hex
Text
Application
Message
File Metadata
Results
Annotations
Other Occurrences
Strings
Indexed Text
Translation
Matches on page: - of - Match
Page: 1 of 1 Page
Text Source: File Text

/img_full_imag.dd/vol_vol50/data/com.careem.acma/shared_prefs — 98 Results

| Name | C | Modified Time | Size | Change Time | Access Time | Cr |
|---|---|---|---|---|---|---|
| com.google.android.gms.appid.xml | | 2020-06-26 18:39:34 PKT | 1033 | 2020-06-26 18:39:34 PKT | 2020-06-26 18:39:34 PKT | 20 |
| com.google.android.gms.measurement.prefs.xml | | 2020-06-26 18:40:34 PKT | 1054 | 2020-06-26 18:40:34 PKT | 2020-06-26 18:40:34 PKT | 20 |
| com.google.firebase.remoteconfig_legacy_settings.xml | | 2020-03-05 21:00:25 PKT | 127 | 2020-03-05 21:00:25 PKT | 2020-03-05 21:00:25 PKT | 20 |
| com.google.maps.api.android.lib6.drd.PREFERENCES_FILE.xml | | 2020-05-22 20:47:06 PKT | 211 | 2020-05-22 20:47:06 PKT | 2020-05-22 20:47:06 PKT | 20 |
| com.newrelic.android.agent.v1_com.careem.acma.xml | | 2020-06-26 18:39:31 PKT | 1785 | 2020-06-26 18:39:31 PKT | 2020-06-26 18:39:31 PKT | 20 |
| com.sendbird.sdk.messaging.keystore.xml | | 2020-06-26 13:44:23 PKT | 65 | 2020-06-26 13:44:23 PKT | 2020-06-26 13:44:23 PKT | 20 |

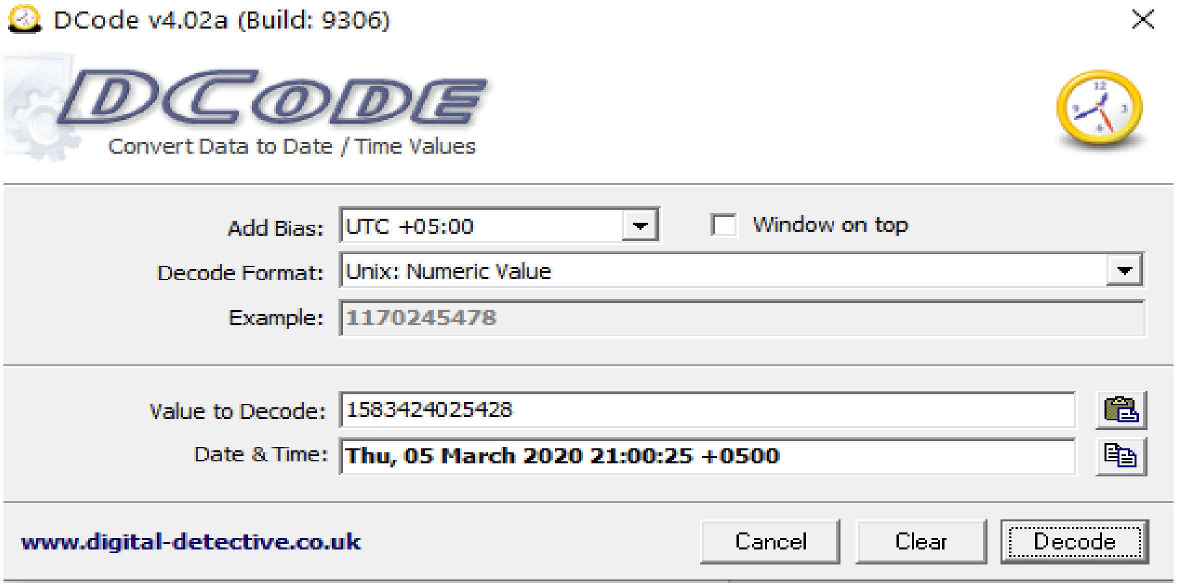
```
<map>
    <long name="time_active" value="9185" />
    <long name="last_upload" value="1583424025632" />
    <long name="first_open_time" value="1583424025428" />
    <string name="gmp_app_id">1:36101668077:android:493f64ab318ff74e</string>
    <string name="app_instance_id">d1adfe48bae3f55ef0f8bd04c72cf978</string>
    <boolean name="app_backgrounded" value="true" />
    <long name="health_monitor:start" value="1593157694225" />
    <boolean name="use_service" value="true" />
    <boolean name="deferred_analytics_collection" value="true" />
    <long name="app_install_time" value="1583291073000" />
    <boolean name="measurement_enabled" value="true" />
    <string name="previous_os_version">9</string>
    <boolean name="has_been_opened" value="true" />
    <boolean name="use_dynamite_api" value="true" />
    <boolean name="allow_remote_dynamite" value="false" />
    <long name="last_pause_time" value="1593178832471" />
    <boolean name="start_new_session" value="false" />
</map>
```

Figure 19 -Careem installation artifacts

This location contains the information about the application “first open time”, “app install time”, “last pause time”. Date time format used is Unix we have converted that Using utility “DCode v4.02a” to read that.

- **name="first_open_time" value="1583424025428"**

  We converted the value to human readable format and the resulting value was Thu, 05 March 2020 21:00:25 +0500. Figure 20 shows the extracted human readable date time format.



DCode v4.02a (Build: 9306)

Convert Data to Date / Time Values

Add Bias: UTC +05:00

□ Window on top

Decode Format: Unix: Numeric Value

Example: 1170245478

Value to Decode: 1583424025428

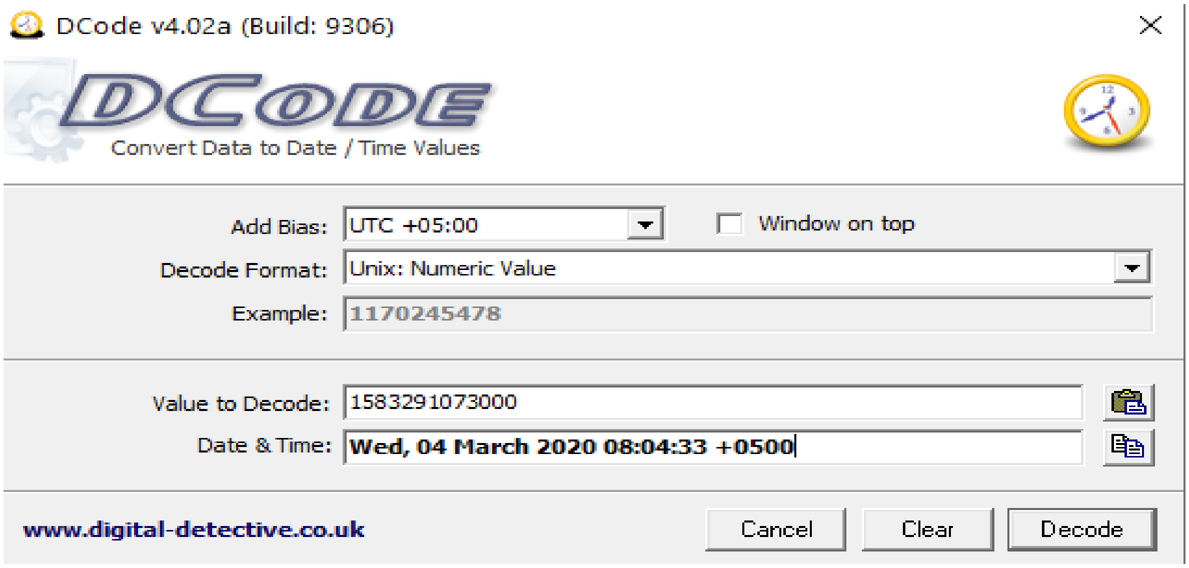
Date & Time: Thu, 05 March 2020 21:00:25 +0500

www.digital-detective.co.uk

Figure 20 -First open time

- **name="app_install_time" value="1583291073000"**

  We converted the value to human readable format and the resulting value was Wed, 04 March 2020 08:04:33 +0500. Figure 21 shows the extracted human readable date time format of the app install time.



DCode v4.02a (Build: 9306)

Convert Data to Date / Time Values

Add Bias: UTC +05:00

□ Window on top

Decode Format: Unix: Numeric Value

Example: 1170245478

Value to Decode: 1583291073000

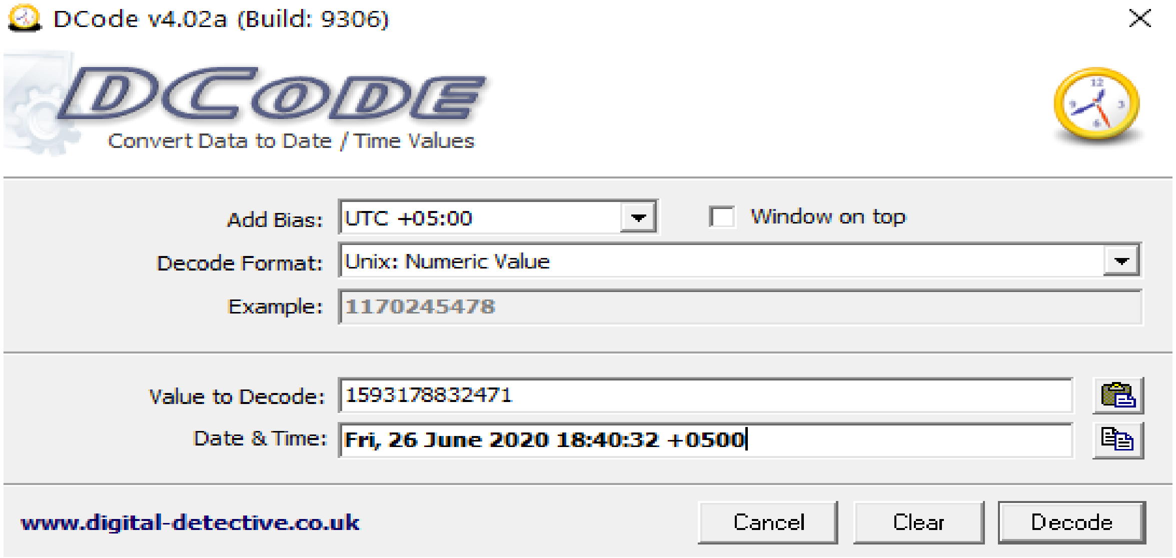
Date & Time: Wed, 04 March 2020 08:04:33 +0500

www.digital-detective.co.uk

Figure 21 -App install time

- **name="last_pause_time" value="1593178832471"**

We converted the value to human readable format and the resulting value was Fri, 26 June 2020 18:40:32 +0500. Figure 22 shows the extracted human readable date time format of the last pause time.



DCode v4.02a (Build: 9306)

Add Bias: UTC +05:00

□ Window on top

Decode Format: Unix: Numeric Value

Example: 1170245478

Value to Decode: 1593178832471

Date & Time: Fri, 26 June 2020 18:40:32 +0500

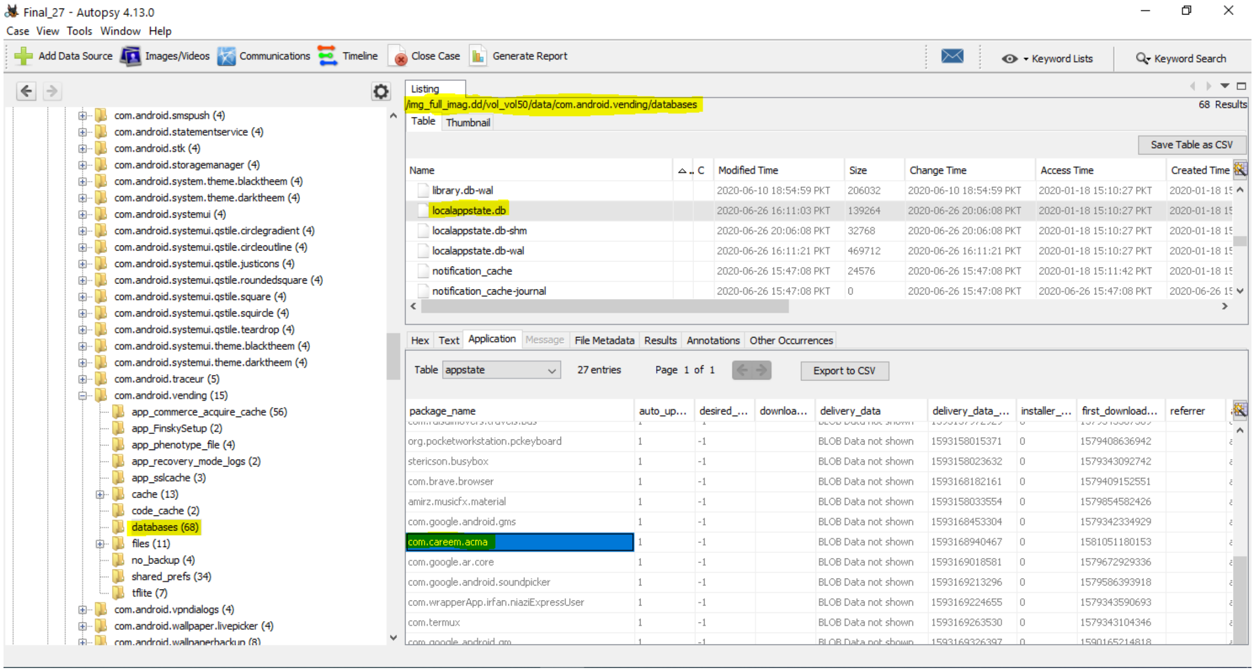
www.digital-detective.co.uk

Figure 22 -last pause time

### 5.3.3 Application installation database

Android devices maintain locally installed app record in separate db. We have found that database locations as you can see in figure 23. Full path to location is given bellow

path: *"/img_full_imag.dd/vol_vol50/data/com.android.vending/databases/localappstate.db"*



- com.android.smspush (4)
- com.android.statementservice (4)
- com.android.stk (4)
- com.android.storagemanager (4)
- com.android.system.theme.blacktheem (4)
- com.android.system.theme.darktheem (4)
- com.android.systemui (4)
- com.android.systemui.qstile.circlegradient (4)
- com.android.systemui.qstile.circleoutline (4)
- com.android.systemui.qstile.justicons (4)
- com.android.systemui.qstile.roundedsquare (4)
- com.android.systemui.qstile.square (4)
- com.android.systemui.qstile.squircle (4)
- com.android.systemui.qstile.teardrop (4)
- com.android.systemui.theme.blacktheem (4)
- com.android.systemui.theme.darktheem (4)
- com.android.traceur (5)
- com.android.vending (15)
  - app_commerce_acquire_cache (56)
  - app_FinskySetup (2)
  - app_phenotype_file (4)
  - app_recovery_mode_logs (2)
  - app_sslcache (3)
  - cache (13)
  - code_cache (2)
  - databases (68)
  - files (11)
  - no_backup (4)
  - shared_prefs (34)
  - tflite (7)
- com.android.vpndialogs (4)
- com.android.wallpaper.livepicker (4)
- com.android.wallpaperbackup (8)

/img_full_imag.dd/vol_vol50/data/com.android.vending/databases

68 Results

| Name | C | Modified Time | Size | Change Time | Access Time | Created Time |
|---|---|---|---|---|---|---|
| library.db-wal | | 2020-06-10 18:54:59 PKT | 206032 | 2020-06-10 18:54:59 PKT | 2020-01-18 15:10:27 PKT | 2020-01-18 15 |
| localappstate.db | | 2020-06-26 16:11:03 PKT | 139264 | 2020-06-26 20:06:08 PKT | 2020-01-18 15:10:27 PKT | 2020-01-18 15 |
| localappstate.db-shm | | 2020-06-26 20:06:08 PKT | 32768 | 2020-06-26 20:06:08 PKT | 2020-01-18 15:10:27 PKT | 2020-01-18 15 |
| localappstate.db-wal | | 2020-06-26 16:11:21 PKT | 469712 | 2020-06-26 16:11:21 PKT | 2020-01-18 15:10:27 PKT | 2020-01-18 15 |
| notification_cache | | 2020-06-26 15:47:08 PKT | 24576 | 2020-06-26 15:47:08 PKT | 2020-01-18 15:11:42 PKT | 2020-01-18 15 |
| notification_cache-journal | | 2020-06-26 15:47:08 PKT | 0 | 2020-06-26 15:47:08 PKT | 2020-06-26 15:47:08 PKT | 2020-06-26 15 |

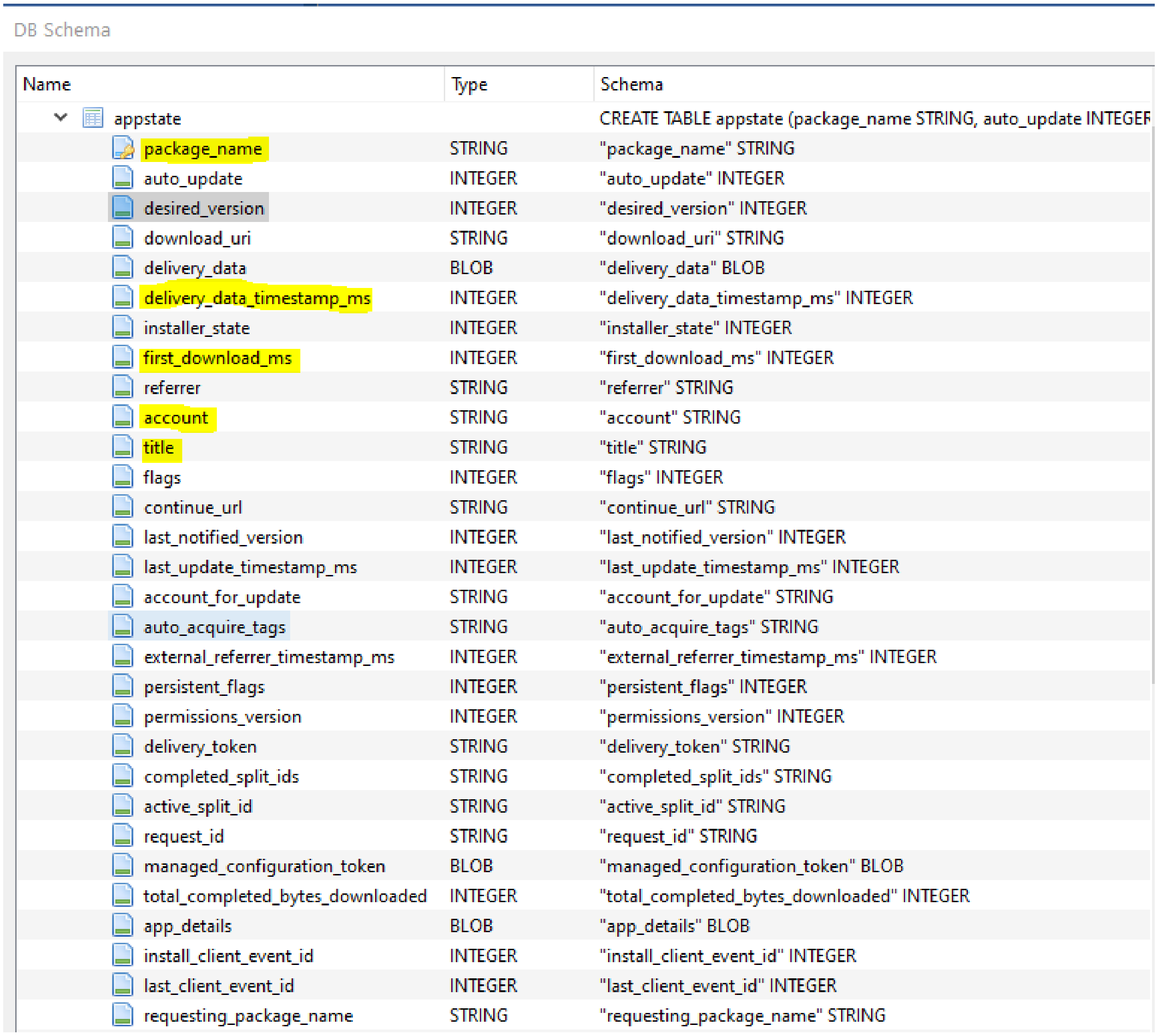
Table appstate 27 entries Page 1 of 1

| package_name | auto_up... | desired_... | downloa... | delivery_data | delivery_data_... | installer_... | first_download... | referrer |
|---|---|---|---|---|---|---|---|---|
| org.pocketworkstation.pckeyboard | 1 | -1 | | BLOB Data not shown | 1593158015371 | 0 | 1579408636942 | |
| stericson.busybox | 1 | -1 | | BLOB Data not shown | 1593158023632 | 0 | 1579343092742 | |
| com.brave.browser | 1 | -1 | | BLOB Data not shown | 1593168182161 | 0 | 1579409152551 | |
| amirz.musicfx.material | 1 | -1 | | BLOB Data not shown | 1593158033554 | 0 | 1579854582426 | |
| com.google.android.gms | 1 | -1 | | BLOB Data not shown | 1593168453304 | 0 | 1579342334929 | |
| com.careem.acma | 1 | -1 | | BLOB Data not shown | 1593168940467 | 0 | 1581051180153 | |
| com.google.ar.core | 1 | -1 | | BLOB Data not shown | 1593169018581 | 0 | 1579672929336 | |
| com.google.android.soundpicker | 1 | -1 | | BLOB Data not shown | 1593169213296 | 0 | 1579586393918 | |
| com.wrapperApp.irfan.niaziExpressUser | 1 | -1 | | BLOB Data not shown | 1593169224655 | 0 | 1579343590693 | |
| com.termux | 1 | -1 | | BLOB Data not shown | 1593169263530 | 0 | 1579343104346 | |
| com.google.android.gm | 1 | -1 | | BLOB Data not shown | 1593169326397 | 0 | 1590165214818 | |

Figure 23 – Local app database

- **localappstate.db**

We have analyzed the extracted database in “DB Explorer for SQLite” for details information gathering with the SQLite database. This database contains all the locally installed application record. Database has following structure which is shown in figure 24.



DB Schema

| Name | Type | Schema |
|---|---|---|
| appstate | | CREATE TABLE appstate (package_name STRING, auto_update INTEGER |
| package_name | STRING | "package_name" STRING |
| auto_update | INTEGER | "auto_update" INTEGER |
| desired_version | INTEGER | "desired_version" INTEGER |
| download_uri | STRING | "download_uri" STRING |
| delivery_data | BLOB | "delivery_data" BLOB |
| delivery_data_timestamp_ms | INTEGER | "delivery_data_timestamp_ms" INTEGER |
| installer_state | INTEGER | "installer_state" INTEGER |
| first_download_ms | INTEGER | "first_download_ms" INTEGER |
| referrer | STRING | "referrer" STRING |
| account | STRING | "account" STRING |
| title | STRING | "title" STRING |
| flags | INTEGER | "flags" INTEGER |
| continue_url | STRING | "continue_url" STRING |
| last_notified_version | INTEGER | "last_notified_version" INTEGER |
| last_update_timestamp_ms | INTEGER | "last_update_timestamp_ms" INTEGER |
| account_for_update | STRING | "account_for_update" STRING |
| auto_acquire_tags | STRING | "auto_acquire_tags" STRING |
| external_referrer_timestamp_ms | INTEGER | "external_referrer_timestamp_ms" INTEGER |
| persistent_flags | INTEGER | "persistent_flags" INTEGER |
| permissions_version | INTEGER | "permissions_version" INTEGER |
| delivery_token | STRING | "delivery_token" STRING |
| completed_split_ids | STRING | "completed_split_ids" STRING |
| active_split_id | STRING | "active_split_id" STRING |
| request_id | STRING | "request_id" STRING |
| managed_configuration_token | BLOB | "managed_configuration_token" BLOB |
| total_completed_bytes_downloaded | INTEGER | "total_completed_bytes_downloaded" INTEGER |
| app_details | BLOB | "app_details" BLOB |
| install_client_event_id | INTEGER | "install_client_event_id" INTEGER |
| last_client_event_id | INTEGER | "last_client_event_id" INTEGER |
| requesting_package_name | STRING | "requesting_package_name" STRING |

Figure 24 –"appstate" table Schema

We have extracted values related to our application which can be seen in following figure 25.

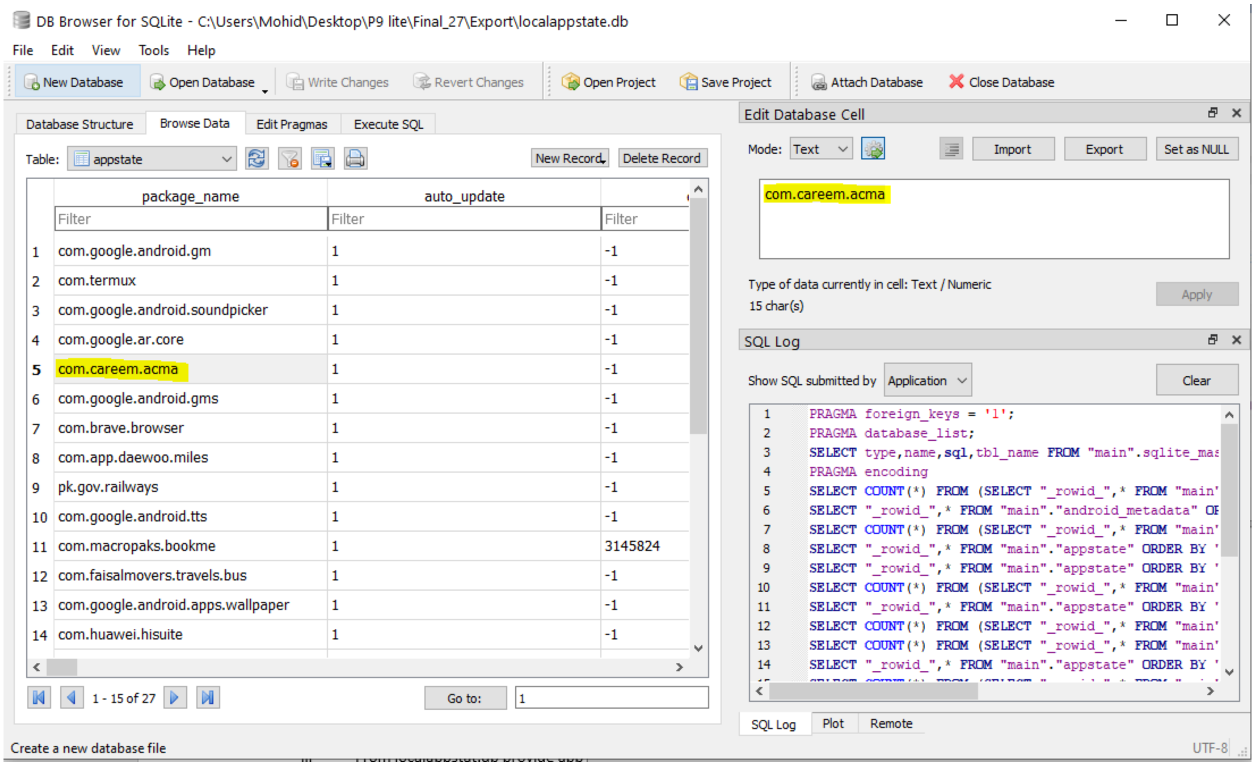


Table: appstate

|  | package_name | auto_update |  |
|---|---|---|---|
|  | Filter | Filter | Filter |
| 1 | com.google.android.gm | 1 | -1 |
| 2 | com.termux | 1 | -1 |
| 3 | com.google.android.soundpicker | 1 | -1 |
| 4 | com.google.ar.core | 1 | -1 |
| 5 | com.careem.acma | 1 | -1 |
| 6 | com.google.android.gms | 1 | -1 |
| 7 | com.brave.browser | 1 | -1 |
| 8 | com.app.daewoo.miles | 1 | -1 |
| 9 | pk.gov.railways | 1 | -1 |
| 10 | com.google.android.tts | 1 | -1 |
| 11 | com.macropaks.bookme | 1 | 3145824 |
| 12 | com.faisalmovers.travels.bus | 1 | -1 |
| 13 | com.google.android.apps.wallpaper | 1 | -1 |
| 14 | com.huawei.hisuite | 1 | -1 |

1 - 15 of 27

Go to: 1

Create a new database file

Mode: Text

com.careem.acma

Type of data currently in cell: Text / Numeric
15 char(s)

Show SQL submitted by: Application

```
PRAGMA foreign_keys = '1';
PRAGMA database_list;
SELECT type,name,sql,tbl_name FROM "main".sqlite_mas
PRAGMA encoding
SELECT COUNT(*) FROM (SELECT "_rowid_",* FROM "main'
SELECT "_rowid_",* FROM "main"."android_metadata" OF
SELECT COUNT(*) FROM (SELECT "_rowid_",* FROM "main'
SELECT "_rowid_",* FROM "main"."appstate" ORDER BY '
SELECT "_rowid_",* FROM "main"."appstate" ORDER BY '
SELECT COUNT(*) FROM (SELECT "_rowid_",* FROM "main'
SELECT "_rowid_",* FROM "main"."appstate" ORDER BY '
SELECT COUNT(*) FROM (SELECT "_rowid_",* FROM "main'
SELECT COUNT(*) FROM (SELECT "_rowid_",* FROM "main'
SELECT "_rowid_",* FROM "main"."appstate" ORDER BY '
```

Figure 25 –“appstate” table data

## 5.4 Remnants of C- ALA

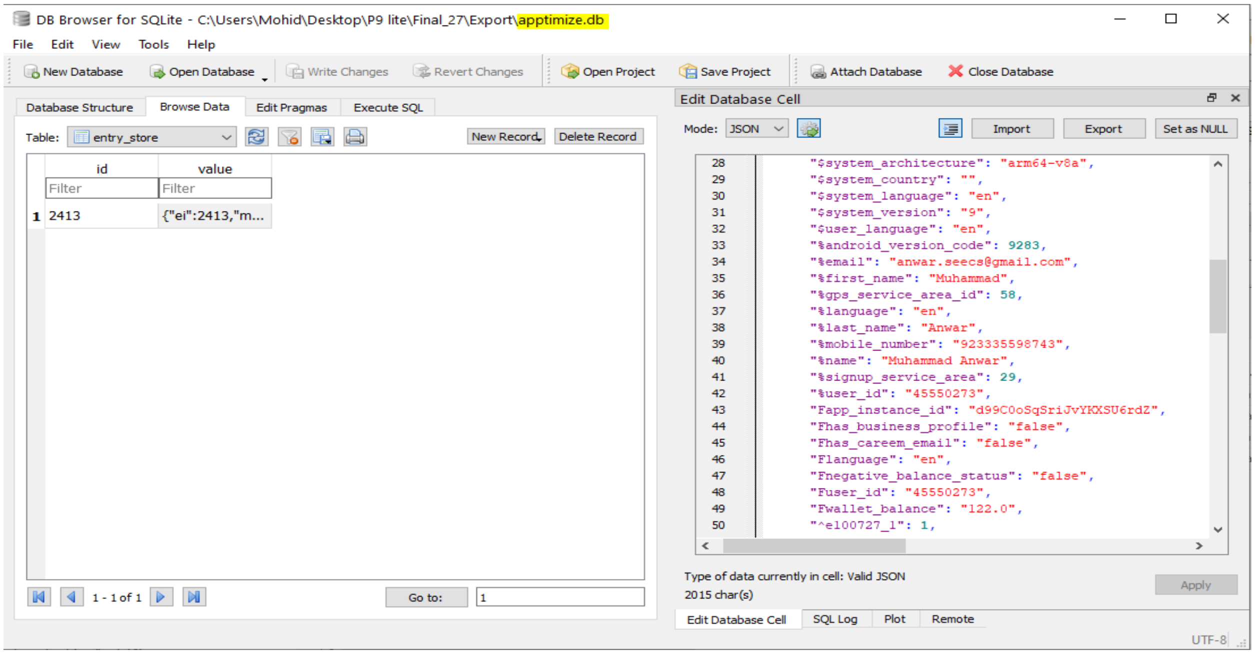
This section contains the remnants of login activity. Credentials Used for this study are: **anwar.seecs@gmail.com** and Password: **Seecs@1212** application.

### 5.4.1 Application Login & Account Information

We found user profile and other related information on multiple locations. Following are the different location where user related artifacts were found.

Path: “*/img_full_imag.dd/vol_vol50/data/com.careem.acma/databases/apptimize.db*”

This location contains all user information like first name, last name, email address, phone number and wallet balance. Figure 26 show the artifacts found in this database file.



|  | id | value |
|---|---|---|
|  | Filter | Filter |
| 1 | 2413 | {"ei":2413,"m... |

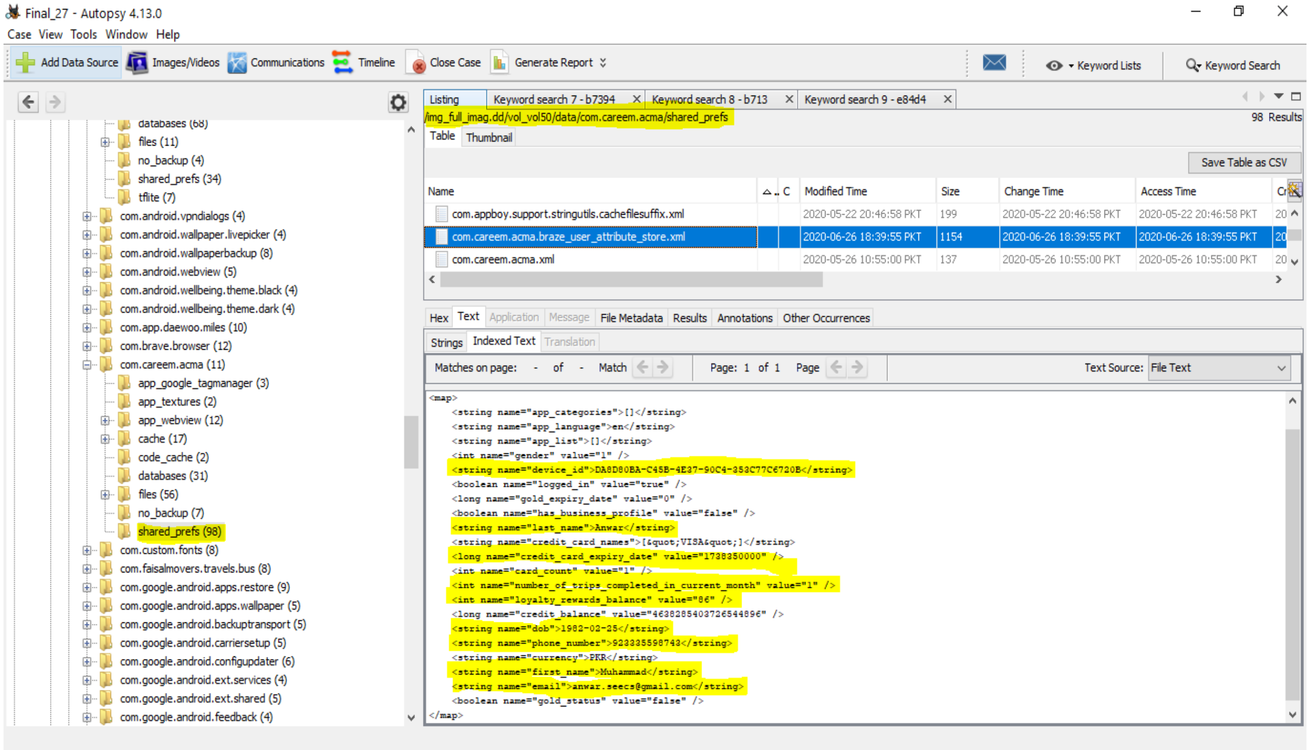
```
    "$system_architecture": "arm64-v8a",
    "$system_country": "",
    "$system_language": "en",
    "$system_version": "9",
    "$user_language": "en",
    "%android_version_code": 9283,
    "%email": "anwar.seecs@gmail.com",
    "%first_name": "Muhammad",
    "%gps_service_area_id": 58,
    "%language": "en",
    "%last_name": "Anwar",
    "%mobile_number": "923335598743",
    "%name": "Muhammad Anwar",
    "%signup_service_area": 29,
    "%user_id": "45550273",
    "Fapp_instance_id": "d99C0oSqSriJvYKXSU6rdZ",
    "Fhas_business_profile": "false",
    "Fhas_careem_email": "false",
    "Flanguage": "en",
    "Fnegative_balance_status": "false",
    "Fuser_id": "45550273",
    "Fwallet_balance": "122.0",
    "^e100727_1": 1,
```

Type of data currently in cell: Valid JSON
2015 char(s)

Figure 26 -User profile information at apptimize database

Path: *"/img_full_imag.dd/vol_vol50/data/com.careem.acma/shared_prefs/com.careem.acma.braze_user_attribute_store.xml"*

This location contains complete user profile information like First name, last name, gender, date of birth, credit card name, credit card expiry date, number of trips completed in current month and other app and device related information as shown in the figure 27.



/img_full_imag.dd/vol_vol50/data/com.careem.acma/shared_prefs

98 Results

| Name | C | Modified Time | Size | Change Time | Access Time | Cr |
|---|---|---|---|---|---|---|
| com.appboy.support.stringutils.cachefilesuffix.xml | | 2020-05-22 20:46:58 PKT | 199 | 2020-05-22 20:46:58 PKT | 2020-05-22 20:46:58 PKT | 20 |
| com.careem.acma.braze_user_attribute_store.xml | | 2020-06-26 18:39:55 PKT | 1154 | 2020-06-26 18:39:55 PKT | 2020-06-26 18:39:55 PKT | 20 |
| com.careem.acma.xml | | 2020-05-26 10:55:00 PKT | 137 | 2020-05-26 10:55:00 PKT | 2020-05-26 10:55:00 PKT | 20 |

```
<map>
    <string name="app_categories">[]</string>
    <string name="app_language">en</string>
    <string name="app_list">[]</string>
    <int name="gender" value="1" />
    <string name="device_id">DA8D80BA-C45B-4E37-90C4-353C77C6720B</string>
    <boolean name="logged_in" value="true" />
    <long name="gold_expiry_date" value="0" />
    <boolean name="has_business_profile" value="false" />
    <string name="last_name">Anwar</string>
    <string name="credit_card_names">[&quot;VISA&quot;]</string>
    <long name="credit_card_expiry_date" value="1738350000" />
    <int name="card_count" value="1" />
    <int name="number_of_trips_completed_in_current_month" value="1" />
    <int name="loyalty_rewards_balance" value="86" />
    <long name="credit_balance" value="4638285403726544896" />
    <string name="dob">1982-02-25</string>
    <string name="phone_number">923335598743</string>
    <string name="currency">PKR</string>
    <string name="first_name">Muhammad</string>
    <string name="email">anwar.seecs@gmail.com</string>
    <boolean name="gold_status" value="false" />
</map>
```

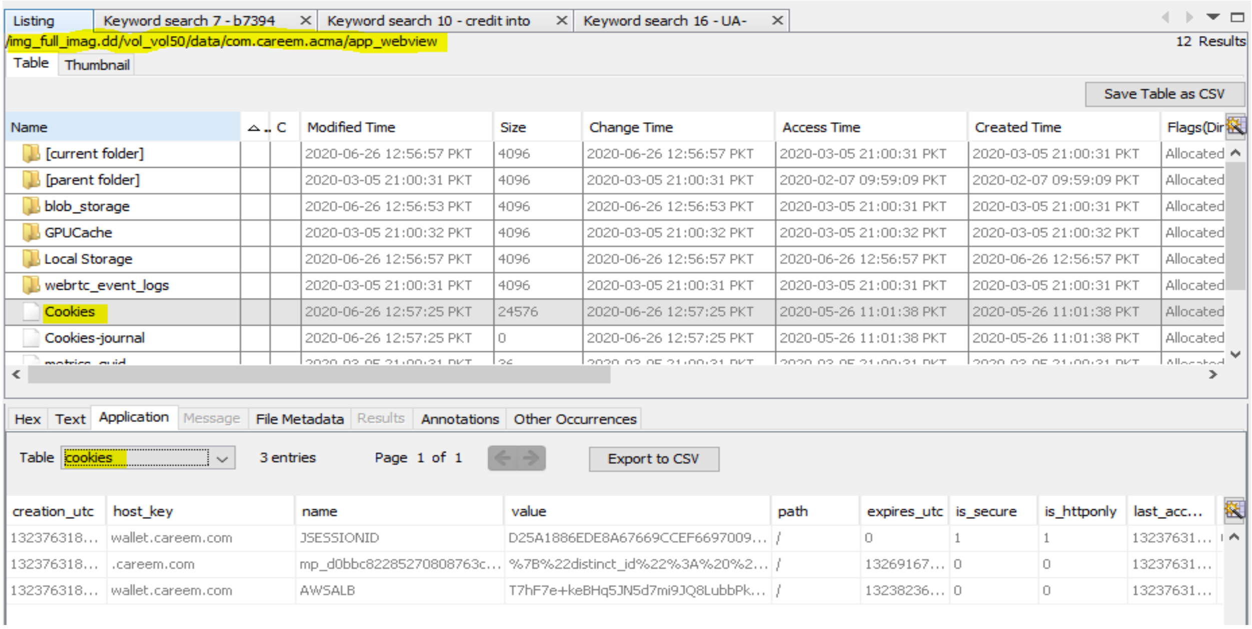
Figure 27 - com.careem.acma.braze_user_attribute_store.xml

### 5.4.2 Session information

Session information were found on the following location

Path: *"/img_full_imag.dd/vol_vol50/data/com.careem.acma/app_webview/Cookies"*

This location contains valuable information about the user's session. It contains three different Session cookies at the same time namely JSESSIONID, AWSALB, and 3rd cookie mp_d0bbc822852708087 63c59822c00f492_mixpanel. Figure 28 displays the cookie's location.



/img_full_imag.dd/vol_vol50/data/com.careem.acma/app_webview

12 Results

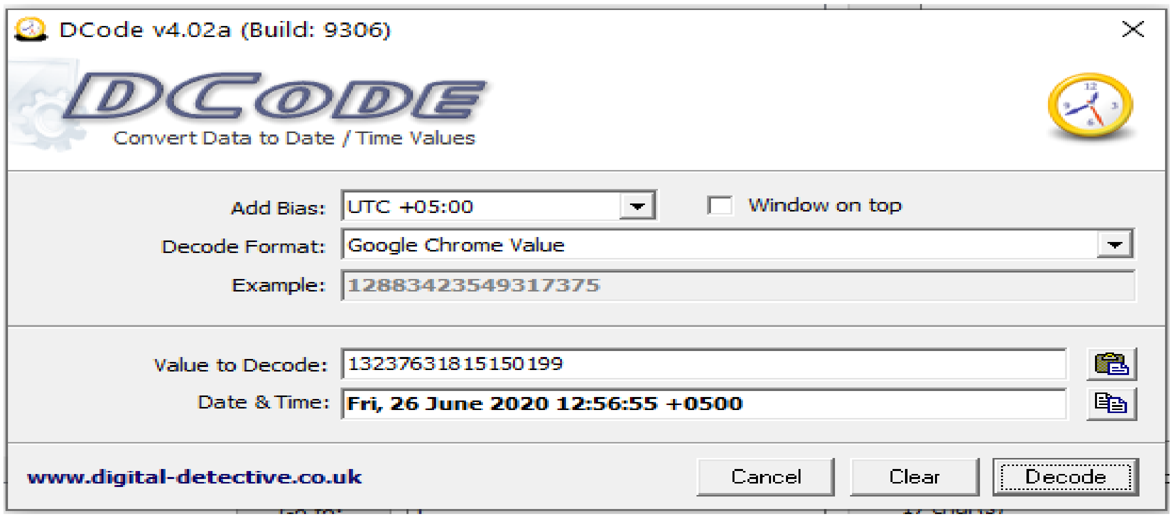
| Name | C | Modified Time | Size | Change Time | Access Time | Created Time | Flags(Dir |
|---|---|---|---|---|---|---|---|
| [current folder] | | 2020-06-26 12:56:57 PKT | 4096 | 2020-06-26 12:56:57 PKT | 2020-03-05 21:00:31 PKT | 2020-03-05 21:00:31 PKT | Allocated |
| [parent folder] | | 2020-03-05 21:00:31 PKT | 4096 | 2020-03-05 21:00:31 PKT | 2020-02-07 09:59:09 PKT | 2020-02-07 09:59:09 PKT | Allocated |
| blob_storage | | 2020-06-26 12:56:53 PKT | 4096 | 2020-06-26 12:56:53 PKT | 2020-03-05 21:00:31 PKT | 2020-03-05 21:00:31 PKT | Allocated |
| GPUCache | | 2020-03-05 21:00:32 PKT | 4096 | 2020-03-05 21:00:32 PKT | 2020-03-05 21:00:32 PKT | 2020-03-05 21:00:32 PKT | Allocated |
| Local Storage | | 2020-06-26 12:56:57 PKT | 4096 | 2020-06-26 12:56:57 PKT | 2020-06-26 12:56:57 PKT | 2020-06-26 12:56:57 PKT | Allocated |
| webrtc_event_logs | | 2020-03-05 21:00:31 PKT | 4096 | 2020-03-05 21:00:31 PKT | 2020-03-05 21:00:31 PKT | 2020-03-05 21:00:31 PKT | Allocated |
| Cookies | | 2020-06-26 12:57:25 PKT | 24576 | 2020-06-26 12:57:25 PKT | 2020-05-26 11:01:38 PKT | 2020-05-26 11:01:38 PKT | Allocated |
| Cookies-journal | | 2020-06-26 12:57:25 PKT | 0 | 2020-06-26 12:57:25 PKT | 2020-05-26 11:01:38 PKT | 2020-05-26 11:01:38 PKT | Allocated |

Table cookies    3 entries    Page 1 of 1

| creation_utc | host_key | name | value | path | expires_utc | is_secure | is_httponly | last_acc... |
|---|---|---|---|---|---|---|---|---|
| 132376318... | wallet.careem.com | JSESSIONID | D25A1886EDE8A67669CCEF6697009... | / | 0 | 1 | 1 | 13237631... |
| 132376318... | .careem.com | mp_d0bbc82285270808763c... | %7B%22distinct_id%22%3A%20%2... | / | 13269167... | 0 | 0 | 13237631... |
| 132376318... | wallet.careem.com | AWSALB | T7hF7e+keBHq5JN5d7mi9JQ8LubbPk... | / | 13238236... | 0 | 0 | 13237631... |

Figure 28 – Session information

It reveals critical information like last cookie name, cookies values, creation UTC, expiry and cookies last access time. Figure 29 shows the last access time of the cookies.


DCode v4.02a (Build: 9306)
DCODE
Convert Data to Date / Time Values

Add Bias: UTC +05:00

Decode Format: Google Chrome Value

Example: 12883423549317375

Value to Decode: 13237631815150199

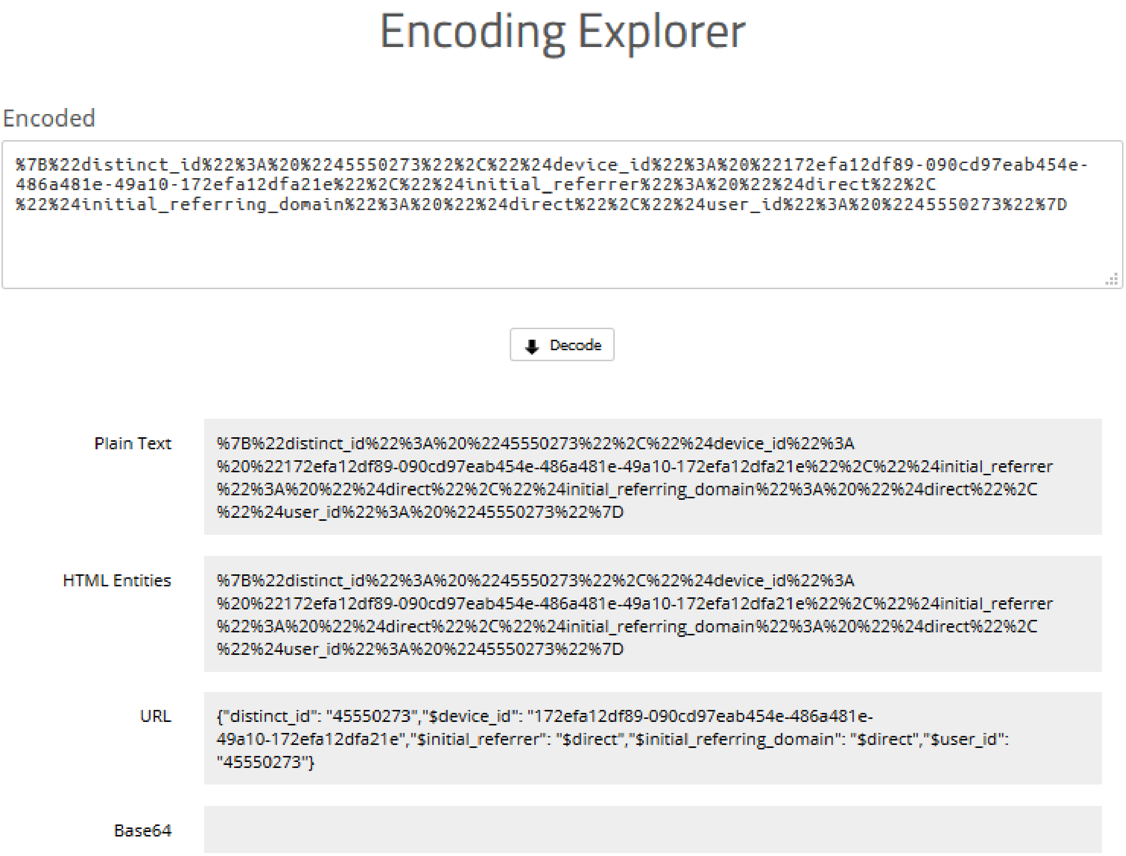
Date & Time: Fri, 26 June 2020 12:56:55 +0500

www.digital-detective.co.uk
Cancel
Clear
Decode

Figure 29 – Cookie last access time

When we have decode the session values of "mp_d0bbc82285270808763c59822c00f492_mixpanel" as shown in the figure 30, we got the following results:

{"distinct_id": "45550273","$device_id": "172efa12df89-090cd97eab454e-486a481e-49a10-172efa12dfa21e","$initial_referrer": "$direct","$initial_referring_domain": "$direct","$user_id": "45550273"}



Encoding Explorer

Encoded

```
%7B%22distinct_id%22%3A%20%2245550273%22%2C%22%24device_id%22%3A%20%22172efa12df89-090cd97eab454e-
486a481e-49a10-172efa12dfa21e%22%2C%22%24initial_referrer%22%3A%20%22%24direct%22%2C
%22%24initial_referring_domain%22%3A%20%22%24direct%22%2C%22%24user_id%22%3A%20%2245550273%22%7D
```

Plain Text

```
%7B%22distinct_id%22%3A%20%2245550273%22%2C%22%24device_id%22%3A
%20%22172efa12df89-090cd97eab454e-486a481e-49a10-172efa12dfa21e%22%2C%22%24initial_referrer
%22%3A%20%22%24direct%22%2C%22%24initial_referring_domain%22%3A%20%22%24direct%22%2C
%22%24user_id%22%3A%20%2245550273%22%7D
```

HTML Entities

```
%7B%22distinct_id%22%3A%20%2245550273%22%2C%22%24device_id%22%3A
%20%22172efa12df89-090cd97eab454e-486a481e-49a10-172efa12dfa21e%22%2C%22%24initial_referrer
%22%3A%20%22%24direct%22%2C%22%24initial_referring_domain%22%3A%20%22%24direct%22%2C
%22%24user_id%22%3A%20%2245550273%22%7D
```

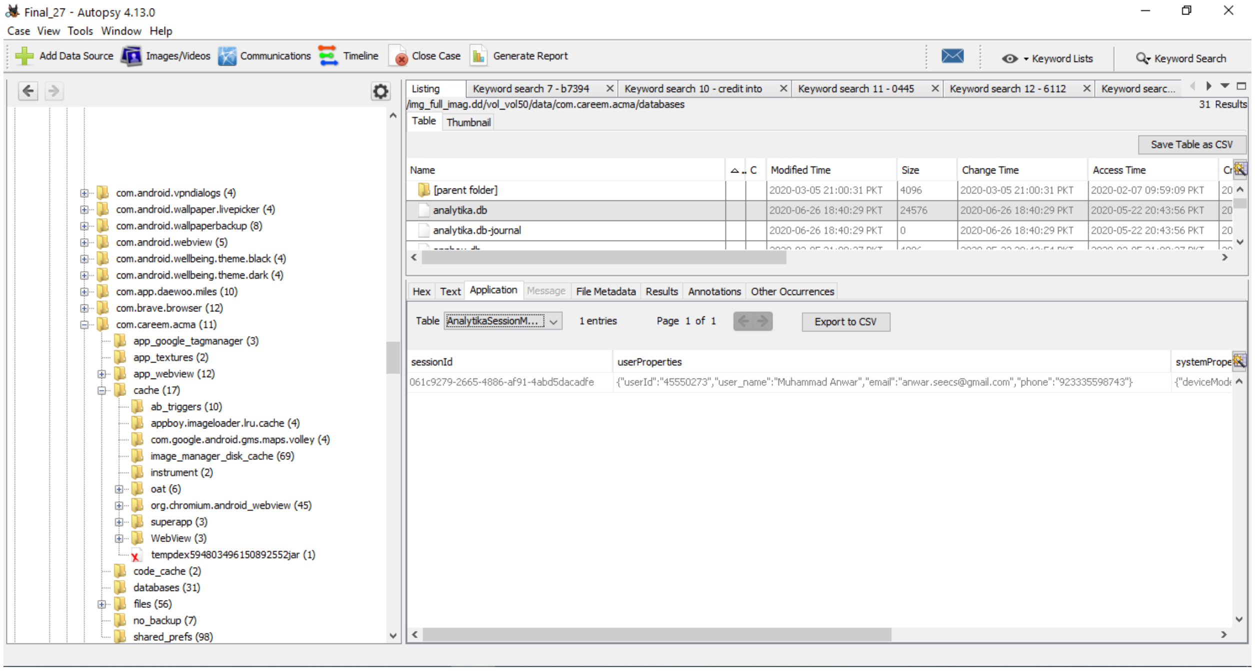
URL

```
{"distinct_id": "45550273","$device_id": "172efa12df89-090cd97eab454e-486a481e-
49a10-172efa12dfa21e","$initial_referrer": "$direct","$initial_referring_domain": "$direct","$user_id":
"45550273"}
```

Base64

Figure 30 – Session Cookie values

Path: /img_full_imag.dd/vol_vol50/data/com.careem.acma/databases/analytika.db



```
com.android.vpndialogs (4)
com.android.wallpaper.livepicker (4)
com.android.wallpaperbackup (8)
com.android.webview (5)
com.android.wellbeing.theme.black (4)
com.android.wellbeing.theme.dark (4)
com.app.daewoo.miles (10)
com.brave.browser (12)
com.careem.acma (11)
    app_google_tagmanager (3)
    app_textures (2)
    app_webview (12)
    cache (17)
        ab_triggers (10)
        appboy.imageloader.lru.cache (4)
        com.google.android.gms.maps.volley (4)
        image_manager_disk_cache (69)
        instrument (2)
        oat (6)
        org.chromium.android_webview (45)
        superapp (3)
        WebView (3)
        tempdex594803496150892552jar (1)
    code_cache (2)
    databases (31)
    files (56)
    no_backup (7)
    shared_prefs (98)
```

/img_full_imag.dd/vol_vol50/data/com.careem.acma/databases

31 Results

| Name | | C | Modified Time | Size | Change Time | Access Time | Cr |
|---|---|---|---|---|---|---|---|
| [parent folder] | | | 2020-03-05 21:00:31 PKT | 4096 | 2020-03-05 21:00:31 PKT | 2020-02-07 09:59:09 PKT | 20 |
| analytika.db | | | 2020-06-26 18:40:29 PKT | 24576 | 2020-06-26 18:40:29 PKT | 2020-05-22 20:43:56 PKT | 20 |
| analytika.db-journal | | | 2020-06-26 18:40:29 PKT | 0 | 2020-06-26 18:40:29 PKT | 2020-05-22 20:43:56 PKT | 20 |

Table AnalytikaSessionM... 1 entries Page 1 of 1

| sessionId | userProperties | systemPrope |
|---|---|---|
| 061c9279-2665-4886-af91-4abd5dacadfe | {"userId":"45550273","user_name":"Muhammad Anwar","email":"anwar.seecs@gmail.com","phone":"923335598743"} | {"deviceMode |

Figure 31 – Session information

Session id and user details with system specification were obtained as shown in the figure 31.

## 5.5 Remnants of C-BA

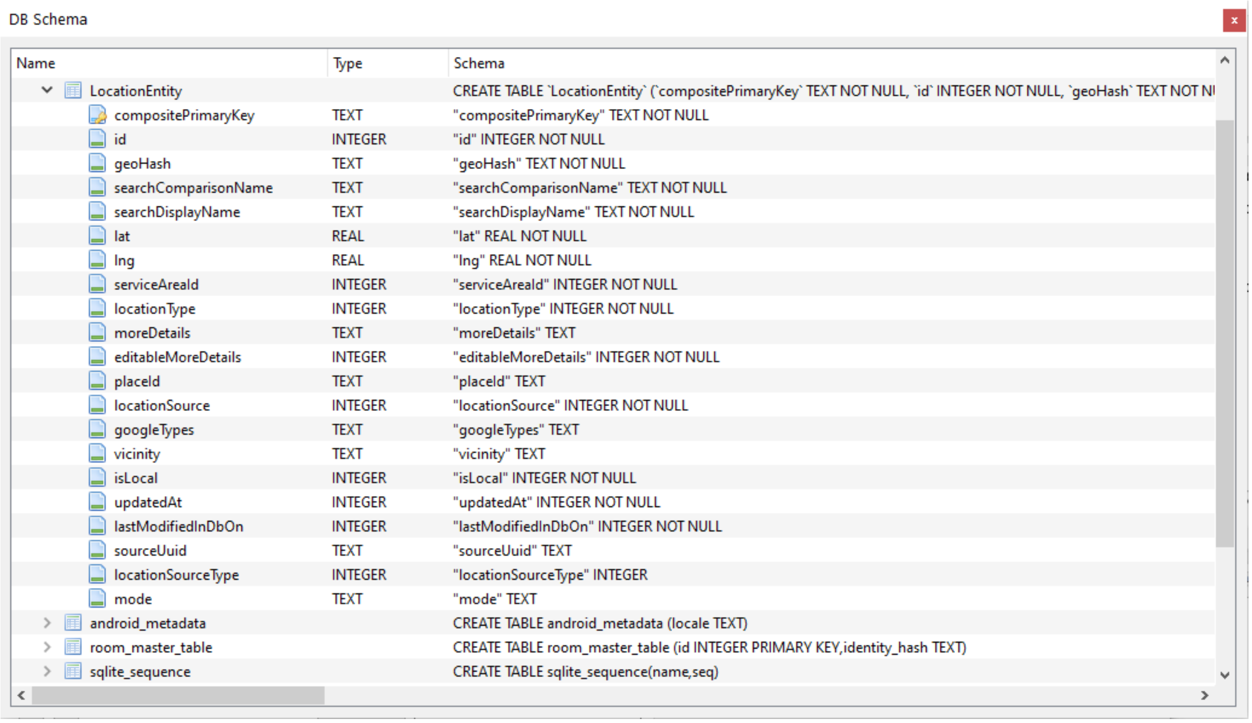
This section contains the remnants of booking activity which we have done experimentally on the application. All the artifacts are categorized by the type of activity done during the booking process. Application has multiple features to facilitate the booking process that includes chat option during the booking and location tracking option.

### 5.5.1 Search History

First step in the booking process is finding destination location on the map. Careem application maintains all the search results in the database in the following file location.

Path: *“/img_full_imag.dd/vol_vol50/data/com.careem.acma/databases/CareemDB”*

Database contains a table “locationEntity” which has following schema as shown in the figure 32.



| Name | Type | Schema |
|---|---|---|
| LocationEntity | | CREATE TABLE `LocationEntity` (`compositePrimaryKey` TEXT NOT NULL, `id` INTEGER NOT NULL, `geoHash` TEXT NOT N |
| compositePrimaryKey | TEXT | "compositePrimaryKey" TEXT NOT NULL |
| id | INTEGER | "id" INTEGER NOT NULL |
| geoHash | TEXT | "geoHash" TEXT NOT NULL |
| searchComparisonName | TEXT | "searchComparisonName" TEXT NOT NULL |
| searchDisplayName | TEXT | "searchDisplayName" TEXT NOT NULL |
| lat | REAL | "lat" REAL NOT NULL |
| lng | REAL | "lng" REAL NOT NULL |
| serviceAreaId | INTEGER | "serviceAreaId" INTEGER NOT NULL |
| locationType | INTEGER | "locationType" INTEGER NOT NULL |
| moreDetails | TEXT | "moreDetails" TEXT |
| editableMoreDetails | INTEGER | "editableMoreDetails" INTEGER NOT NULL |
| placeId | TEXT | "placeId" TEXT |
| locationSource | INTEGER | "locationSource" INTEGER NOT NULL |
| googleTypes | TEXT | "googleTypes" TEXT |
| vicinity | TEXT | "vicinity" TEXT |
| isLocal | INTEGER | "isLocal" INTEGER NOT NULL |
| updatedAt | INTEGER | "updatedAt" INTEGER NOT NULL |
| lastModifiedInDbOn | INTEGER | "lastModifiedInDbOn" INTEGER NOT NULL |
| sourceUuid | TEXT | "sourceUuid" TEXT |
| locationSourceType | INTEGER | "locationSourceType" INTEGER |
| mode | TEXT | "mode" TEXT |
| android_metadata | | CREATE TABLE android_metadata (locale TEXT) |
| room_master_table | | CREATE TABLE room_master_table (id INTEGER PRIMARY KEY,identity_hash TEXT) |
| sqlite_sequence | | CREATE TABLE sqlite_sequence(name,seq) |

Figure 32 – Location Search history table

“locationEntity” table contains information like geo hash, Search Comparison Name, Search Display name, Latitude, longitude, vicinity and other relevant information that can be seen in figure 33.

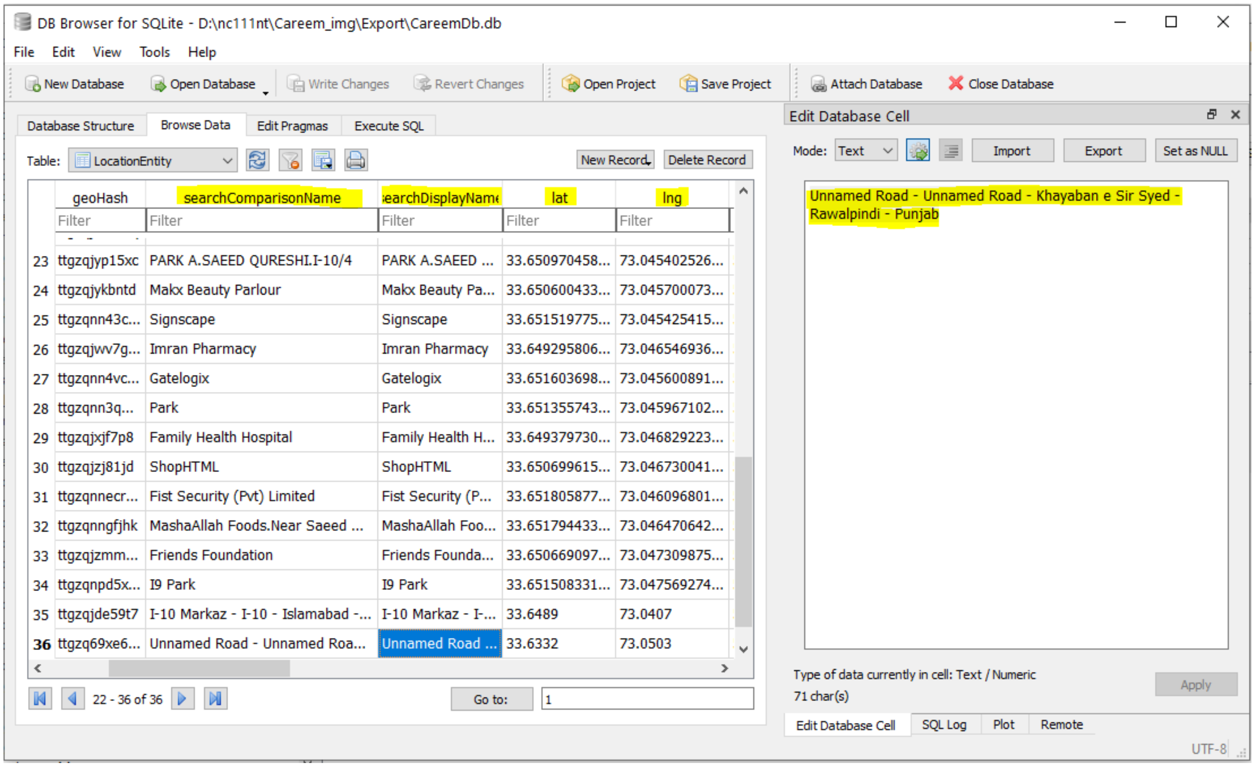


Table: LocationEntity

| | geoHash | searchComparisonName | searchDisplayName | lat | lng |
|---|---|---|---|---|---|
| 23 | ttgzqjyp15xc | PARK A.SAEED QURESHI.I-10/4 | PARK A.SAEED ... | 33.650970458... | 73.045402526... |
| 24 | ttgzqjykbntd | Makx Beauty Parlour | Makx Beauty Pa... | 33.650600433... | 73.045700073... |
| 25 | ttgzqnn43c... | Signscape | Signscape | 33.651519775... | 73.045425415... |
| 26 | ttgzqjwv7g... | Imran Pharmacy | Imran Pharmacy | 33.649295806... | 73.046546936... |
| 27 | ttgzqnn4vc... | Gatelogix | Gatelogix | 33.651603698... | 73.045600891... |
| 28 | ttgzqnn3q... | Park | Park | 33.651355743... | 73.045967102... |
| 29 | ttgzqjxjf7p8 | Family Health Hospital | Family Health H... | 33.649379730... | 73.046829223... |
| 30 | ttgzqjzj81jd | ShopHTML | ShopHTML | 33.650699615... | 73.046730041... |
| 31 | ttgzqnnecr... | Fist Security (Pvt) Limited | Fist Security (P... | 33.651805877... | 73.046096801... |
| 32 | ttgzqnngfjhk | MashaAllah Foods.Near Saeed ... | MashaAllah Foo... | 33.651794433... | 73.046470642... |
| 33 | ttgzqjzmm... | Friends Foundation | Friends Founda... | 33.650669097... | 73.047309875... |
| 34 | ttgzqnpd5x... | I9 Park | I9 Park | 33.651508331... | 73.047569274... |
| 35 | ttgzqjde59t7 | I-10 Markaz - I-10 - Islamabad -... | I-10 Markaz - I-... | 33.6489 | 73.0407 |
| 36 | ttgzq69xe6... | Unnamed Road - Unnamed Roa... | Unnamed Road ... | 33.6332 | 73.0503 |

22 - 36 of 36 Go to: 1

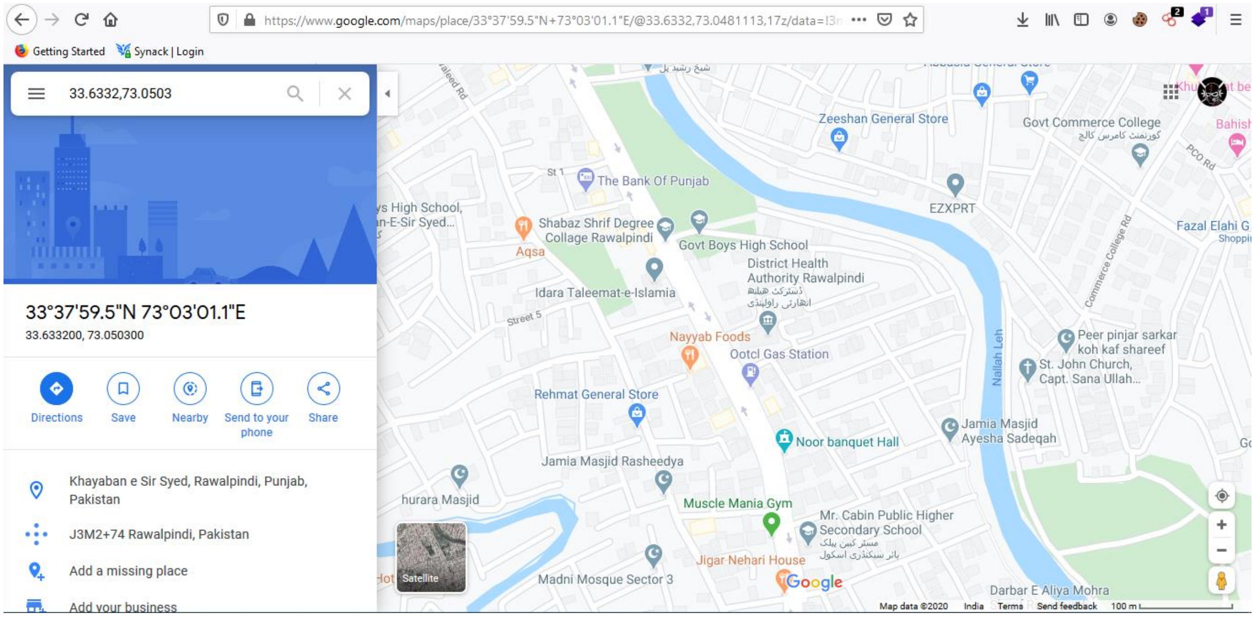
Mode: Text

Unnamed Road - Unnamed Road - Khayaban e Sir Syed - Rawalpindi - Punjab

Type of data currently in cell: Text / Numeric
71 char(s)

Figure 33A – CareemDB

This database contains the lat and lang of the location which helps us to reconstruct the location of the map which can be seen in figure 33B.



https://www.google.com/maps/place/33°37'59.5"N+73°03'01.1"E/@33.6332,73.0481113,17z/data=!3m

33.6332,73.0503

33°37'59.5"N 73°03'01.1"E
33.633200, 73.050300

Khayaban e Sir Syed, Rawalpindi, Punjab, Pakistan
J3M2+74 Rawalpindi, Pakistan
Add a missing place
Add your business

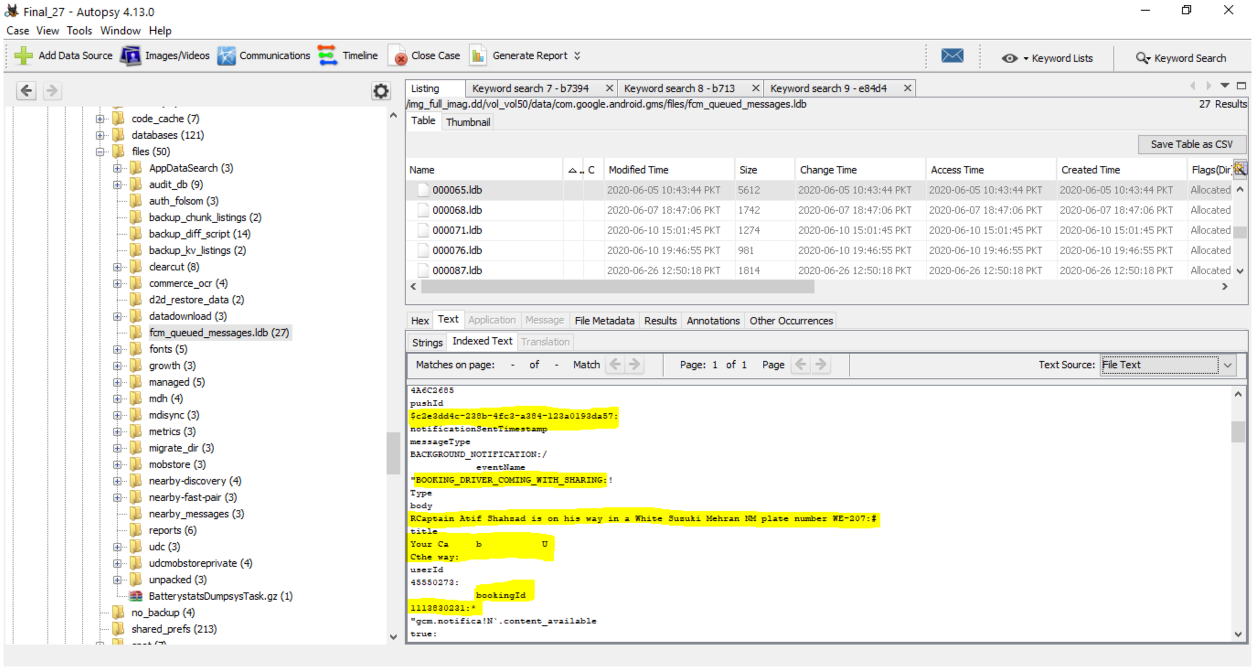
Figure 33B – Pickup Location Coordinates

### 5.5.2 Booking details

The next step in booking process is to confirm booking location and book a ride. Ride booking information can be obtained from following location.

Path:

*“/img_full_imag.dd/vol_vol50/data/com.google.android.gms/files/fcm_queued_messages.ldb/000065.ldb”*



/img_full_imag.dd/vol_vol50/data/com.google.android.gms/files/fcm_queued_messages.ldb — 27 Results

| Name | | C | Modified Time | Size | Change Time | Access Time | Created Time | Flags(Dir) |
|---|---|---|---|---|---|---|---|---|
| 000065.ldb | | | 2020-06-05 10:43:44 PKT | 5612 | 2020-06-05 10:43:44 PKT | 2020-06-05 10:43:44 PKT | 2020-06-05 10:43:44 PKT | Allocated |
| 000068.ldb | | | 2020-06-07 18:47:06 PKT | 1742 | 2020-06-07 18:47:06 PKT | 2020-06-07 18:47:06 PKT | 2020-06-07 18:47:06 PKT | Allocated |
| 000071.ldb | | | 2020-06-10 15:01:45 PKT | 1274 | 2020-06-10 15:01:45 PKT | 2020-06-10 15:01:45 PKT | 2020-06-10 15:01:45 PKT | Allocated |
| 000076.ldb | | | 2020-06-10 19:46:55 PKT | 981 | 2020-06-10 19:46:55 PKT | 2020-06-10 19:46:55 PKT | 2020-06-10 19:46:55 PKT | Allocated |
| 000087.ldb | | | 2020-06-26 12:50:18 PKT | 1814 | 2020-06-26 12:50:18 PKT | 2020-06-26 12:50:18 PKT | 2020-06-26 12:50:18 PKT | Allocated |

```
4A6C2685
pushId
$c2e3dd4c-238b-4fc3-a384-123a0193da57:
notificationSentTimestamp
messageType
BACKGROUND_NOTIFICATION:/
          eventName
"BOOKING_DRIVER_COMING_WITH_SHARING:!
Type
body
RCaptain Atif Shahzad is on his way in a White Suzuki Mehran NM plate number WE-207:#
title
Your Ca     b          U
Cthe way:
userId
45550273:
          bookingId
1113830231:*
"gcm.notifica!N`.content_available
true:
```

Figure 34 – Booking Process

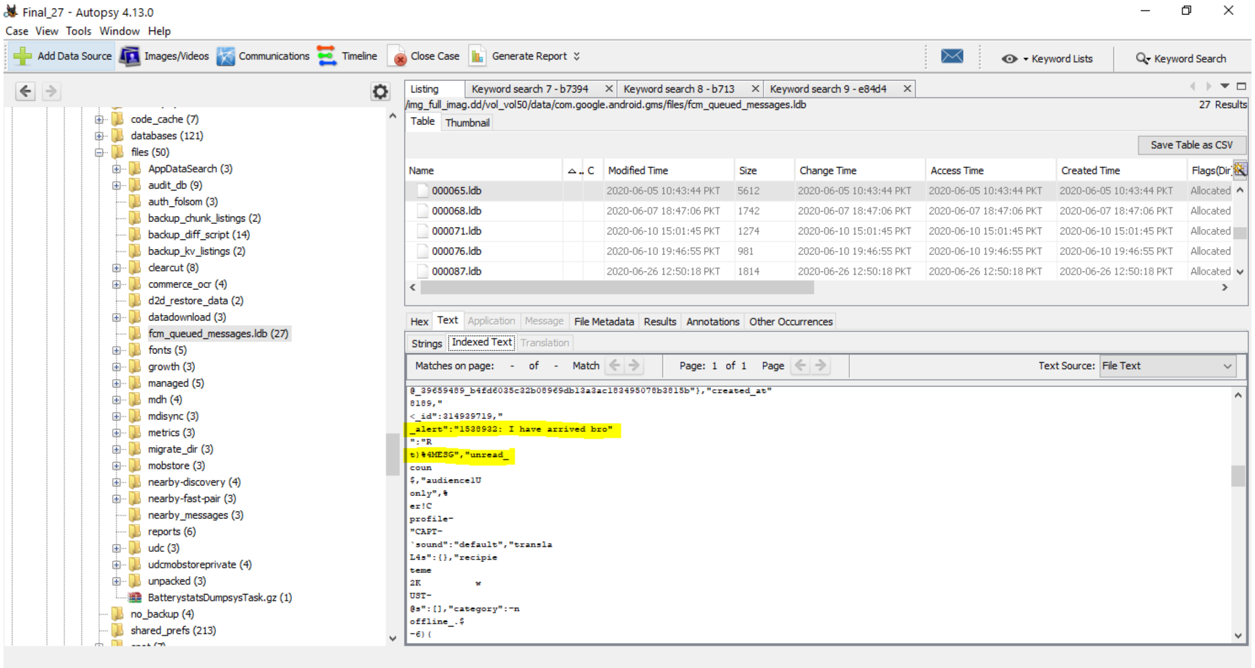
This file contains booking related artifacts like Captain name, Vehicle number, Vehicle type, Vehicle color and Booking ID as shown in the Figure 34.

### 5.5.3 Chat messages

Third step in booking involve Captain and App user conversation to help Captain to locate exact location of the app user from where he can pick app user for his ride. These chat message can be found on following location as shown in the Figure 35.

Path:

"/img_full_imag.dd/vol_vol50/data/com.google.android.gms/files/fcm_queued_messages.ldb/000065.ldb"



/img_full_imag.dd/vol_vol50/data/com.google.android.gms/files/fcm_queued_messages.ldb 27 Results

| Name | C | Modified Time | Size | Change Time | Access Time | Created Time | Flags(Dir) |
|---|---|---|---|---|---|---|---|
| 000065.ldb | | 2020-06-05 10:43:44 PKT | 5612 | 2020-06-05 10:43:44 PKT | 2020-06-05 10:43:44 PKT | 2020-06-05 10:43:44 PKT | Allocated |
| 000068.ldb | | 2020-06-07 18:47:06 PKT | 1742 | 2020-06-07 18:47:06 PKT | 2020-06-07 18:47:06 PKT | 2020-06-07 18:47:06 PKT | Allocated |
| 000071.ldb | | 2020-06-10 15:01:45 PKT | 1274 | 2020-06-10 15:01:45 PKT | 2020-06-10 15:01:45 PKT | 2020-06-10 15:01:45 PKT | Allocated |
| 000076.ldb | | 2020-06-10 19:46:55 PKT | 981 | 2020-06-10 19:46:55 PKT | 2020-06-10 19:46:55 PKT | 2020-06-10 19:46:55 PKT | Allocated |
| 000087.ldb | | 2020-06-26 12:50:18 PKT | 1814 | 2020-06-26 12:50:18 PKT | 2020-06-26 12:50:18 PKT | 2020-06-26 12:50:18 PKT | Allocated |

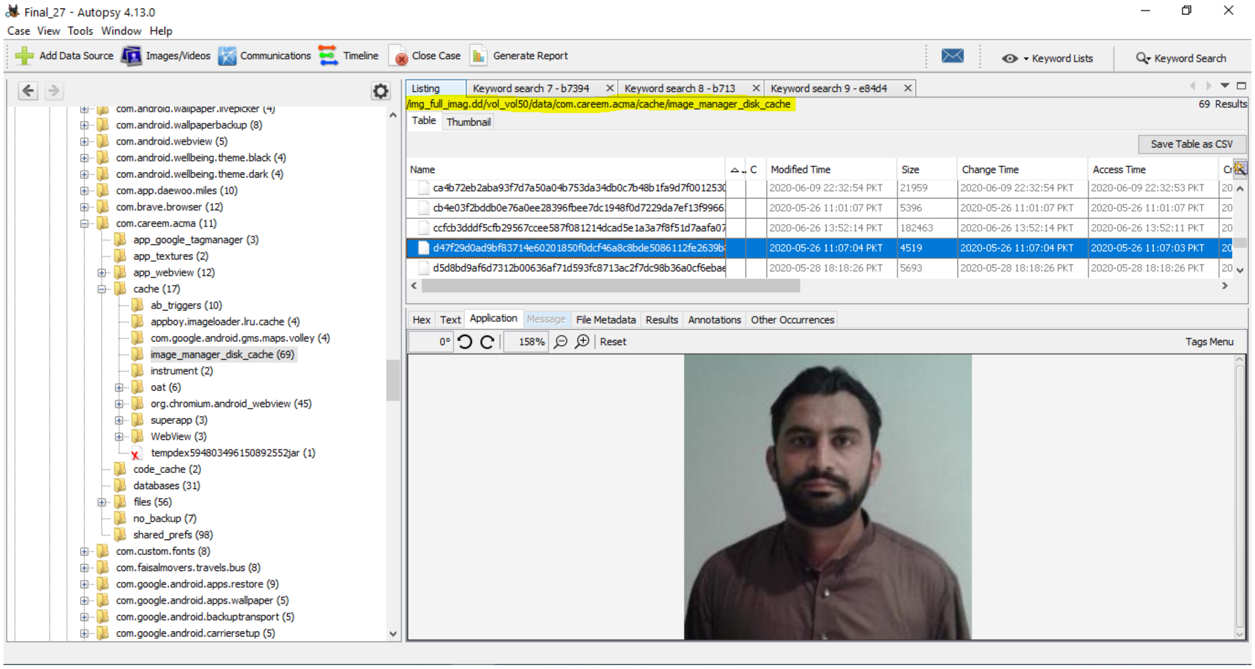
```
@_39659489_b4fd6035c32b08969db13a3ac183495078b3815b"},"created_at"
8189,"
<_id":314939719,"
_alert":"1538932: I have arrived bro"
":"R
t)%4MESG","unread_
coun
$,"audience1U
only",%
er!C
profile-
"CAPT-
`sound":"default","transla
L4s":{},"recipie
teme
2K         w
UST-
@s":[],"category":-n
offline_.$
-6)(
```

Figure 35 – Chat messages

### 5.5.4 Pictures

Once ride is booked for the application user, confirmation message is sent along with driver / Captain Information. That information contains the picture of the Captain and the vehicle information which include the vehicle number and vehicle color which we have already discussed. Captain picture can be found on the following location as shown in the Figure 36.

Path:
*"/img_full_imag.dd/vol_vol50/data/com.careem.acma/cache/image_manager_disk_cache/"*



```
com.android.wallpaper.livepicker (4)
com.android.wallpaperbackup (8)
com.android.webview (5)
com.android.wellbeing.theme.black (4)
com.android.wellbeing.theme.dark (4)
com.app.daewoo.miles (10)
com.brave.browser (12)
com.careem.acma (11)
    app_google_tagmanager (3)
    app_textures (2)
    app_webview (12)
    cache (17)
        ab_triggers (10)
        appboy.imageloader.lru.cache (4)
        com.google.android.gms.maps.volley (4)
        image_manager_disk_cache (69)
        instrument (2)
        oat (6)
        org.chromium.android_webview (45)
        superapp (3)
        WebView (3)
        tempdex594803496150892552jar (1)
    code_cache (2)
    databases (31)
    files (56)
    no_backup (7)
    shared_prefs (98)
com.custom.fonts (8)
com.faisalmovers.travels.bus (8)
com.google.android.apps.restore (9)
com.google.android.apps.wallpaper (5)
com.google.android.backuptransport (5)
com.google.android.carriersetup (5)
```

/img_full_imag.dd/vol_vol50/data/com.careem.acma/cache/image_manager_disk_cache

69 Results

| Name | ⏶ .. | C | Modified Time | Size | Change Time | Access Time | Cr |
|---|---|---|---|---|---|---|---|
| ca4b72eb2aba93f7d7a50a04b753da34db0c7b48b1fa9d7f0012530 | | | 2020-06-09 22:32:54 PKT | 21959 | 2020-06-09 22:32:54 PKT | 2020-06-09 22:32:53 PKT | 20 |
| cb4e03f2bddb0e76a0ee28396fbee7dc1948f0d7229da7ef13f9966 | | | 2020-05-26 11:01:07 PKT | 5396 | 2020-05-26 11:01:07 PKT | 2020-05-26 11:01:07 PKT | 20 |
| ccfcb3dddf5cfb29567ccee587f081214dcad5e1a3a7f8f51d7aafa07 | | | 2020-06-26 13:52:14 PKT | 182463 | 2020-06-26 13:52:14 PKT | 2020-06-26 13:52:11 PKT | 20 |
| d47f29d0ad9bf83714e60201850f0dcf46a8c8bde5086112fe2639b | | | 2020-05-26 11:07:04 PKT | 4519 | 2020-05-26 11:07:04 PKT | 2020-05-26 11:07:03 PKT | 20 |
| d5d8bd9af6d7312b00636af71d593fc8713ac2f7dc98b36a0cf6ebae | | | 2020-05-28 18:18:26 PKT | 5693 | 2020-05-28 18:18:26 PKT | 2020-05-28 18:18:26 PKT | 20 |

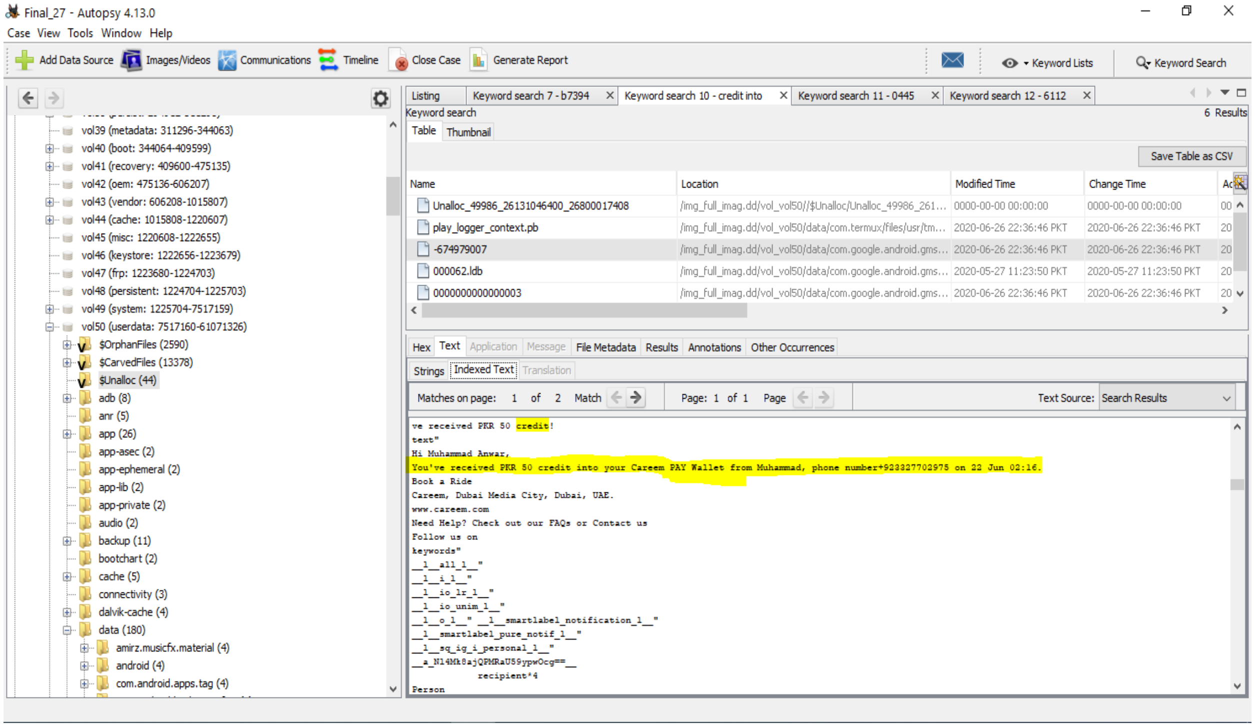
Figure 36 – Captain's picture

## 5.6 Remnants of C-TA

This section contains the remnants of Transactional activity which occurs just after the booking activity. Different types of transactional activities are performed during the experimentation. Application has multiple features to facilitate the application user to get different services through application. For example, application user can recharge mobile credit from the application. Application user can get delivery services from application. Application user can send credit to other application user.  Following are the location of the artifacts found which can be seen in figure 37.

Path:

*"/img_full_imag.dd/vol_vol50/data/com.google.android.gms/files/clearcut/0/MAGICTETHER_COUNTERS/-674979007"*



| Name | Location | Modified Time | Change Time | Ac |
|---|---|---|---|---|
| Unalloc_49986_26131046400_26800017408 | /img_full_imag.dd/vol_vol50//$Unalloc/Unalloc_49986_261... | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 00 |
| play_logger_context.pb | /img_full_imag.dd/vol_vol50/data/com.termux/files/usr/tm... | 2020-06-26 22:36:46 PKT | 2020-06-26 22:36:46 PKT | 20 |
| -674979007 | /img_full_imag.dd/vol_vol50/data/com.google.android.gms... | 2020-06-26 22:36:46 PKT | 2020-06-26 22:36:46 PKT | 20 |
| 000062.ldb | /img_full_imag.dd/vol_vol50/data/com.google.android.gms... | 2020-05-27 11:23:50 PKT | 2020-05-27 11:23:50 PKT | 20 |
| 0000000000000003 | /img_full_imag.dd/vol_vol50/data/com.google.android.gms... | 2020-06-26 22:36:46 PKT | 2020-06-26 22:36:46 PKT | 20 |

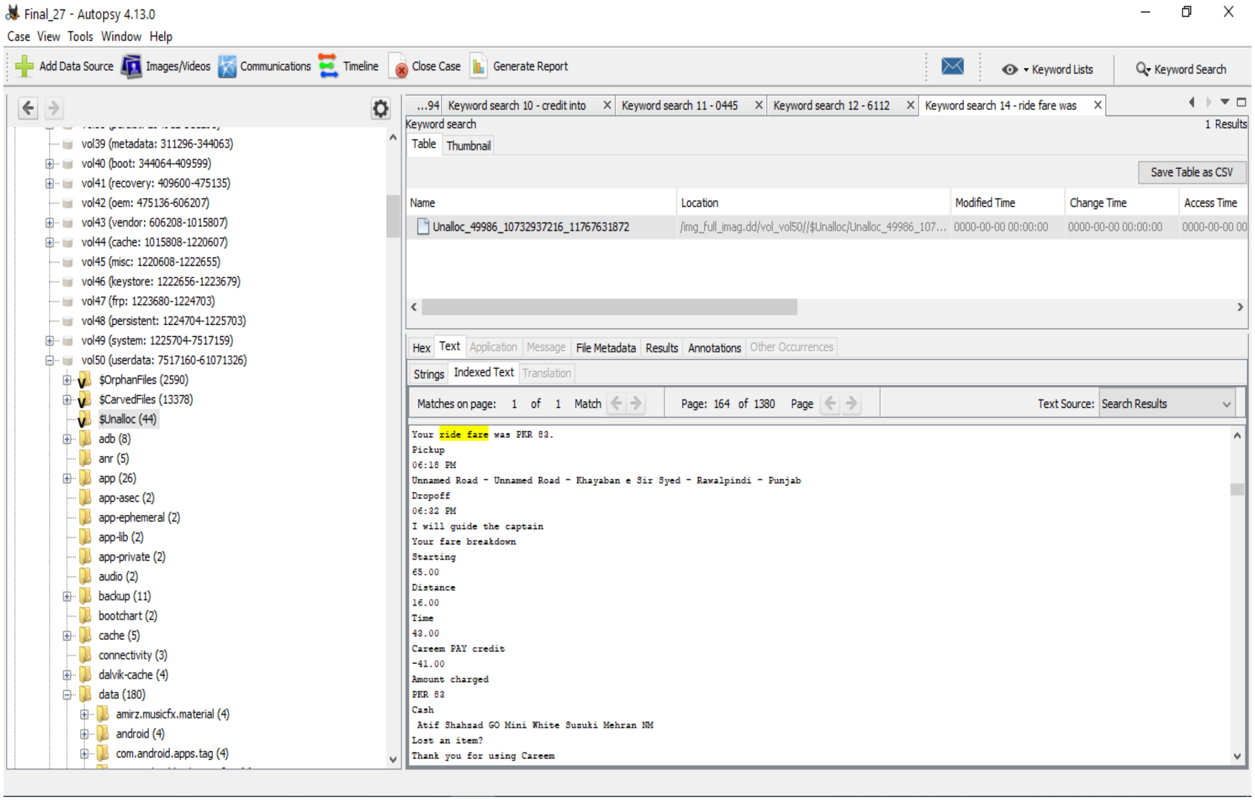
```
ve received PKR 50 credit!
text"
Hi Muhammad Anwar,
You've received PKR 50 credit into your Careem PAY Wallet from Muhammad, phone number+923327702975 on 22 Jun 02:16.
Book a Ride
Careem, Dubai Media City, Dubai, UAE.
www.careem.com
Need Help? Check out our FAQs or Contact us
Follow us on
keywords"
__1__all_1__"
__1__i_1__"
__1__io_lr_1__"
__1__io_unim_1__"
__1__o_1__" __1__smartlabel_notification_1__"
__1__smartlabel_pure_notif_1__"
__1__sq_ig_i_personal_1__"
__a_N14Mk8ajQPMRaU59ypwOcg==__
            recipient*4
Person
```

Figure 37 – Credit Received

In the figure 36 credit amount 50 PKR received from another user with phone number +923327702975 on 22 June 02:16.

Booking payment artifacts were found on following location as shown in the figure 38.

Path: *“/img_full_imag.dd/vol_vol50//$Unalloc/Unalloc_49986_10732937216_11767631872”*



```
Your ride fare was PKR 83.
Pickup
06:18 PM
Unnamed Road - Unnamed Road - Khayaban e Sir Syed - Rawalpindi - Punjab
Dropoff
06:32 PM
I will guide the captain
Your fare breakdown
Starting
65.00
Distance
16.00
Time
43.00
Careem PAY credit
-41.00
Amount charged
PKR 83
Cash
 Atif Shahzad GO Mini White Suzuki Mehran NM
Lost an item?
Thank you for using Careem
```

Figure 38 – Ride Fare

Following artifacts found on this location.

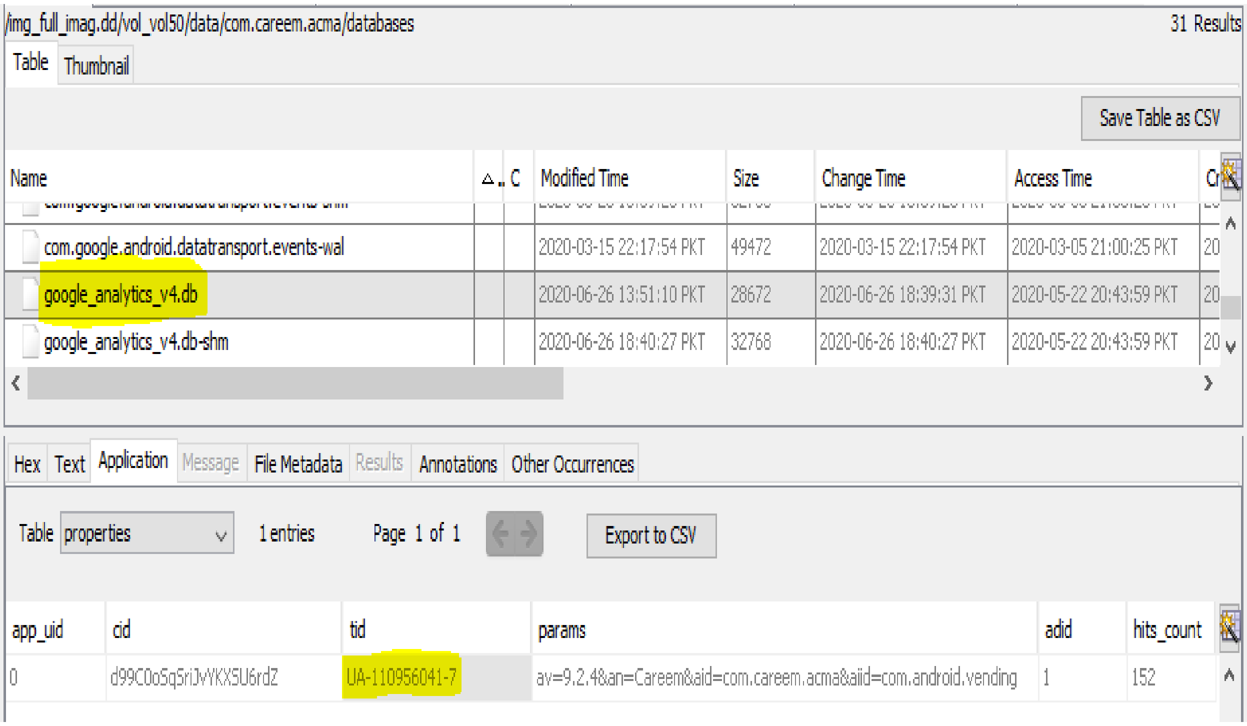
Table 7- Ride Fare Information

| **Ride Fare** | **Pickup Time** | **Pickup location** | **Dropoff time** | **Dropoff location** | **Fare breakdown** | | | **Careem PAY Credit** | **Amount Charged** | **Captain name** | **Vehicle info** |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Starting | Distance | Time | | | | |
| 83 | 06:18 PM | Unnamed Road - Unnamed Road - Khayaban e Sir Syed - Rawalpindi - Punjab | 06:32 PM | I will guide the captain | 65.00 | 16.00 | 43.00 | -41.00 | PKR 83 | Atif Shahzad | GO Mini White Suzuki Mehran NM |

## 5.7 Remnants of C-3PI

This section contains the remnants of 3rd party interaction with application. For example google map API are used for map tracking and application analytics. 3rd party artifacts were found on following location as shown in the figure 39.

Path: /img_full_imag.dd/vol_vol50/data/com.careem.acma/databases/google_analytics_v4.db



| Name | Modified Time | Size | Change Time | Access Time |
|---|---|---|---|---|
| com.google.android.datatransport.events-wal | 2020-03-15 22:17:54 PKT | 49472 | 2020-03-15 22:17:54 PKT | 2020-03-05 21:00:25 PKT |
| google_analytics_v4.db | 2020-06-26 13:51:10 PKT | 28672 | 2020-06-26 18:39:31 PKT | 2020-05-22 20:43:59 PKT |
| google_analytics_v4.db-shm | 2020-06-26 18:40:27 PKT | 32768 | 2020-06-26 18:40:27 PKT | 2020-05-22 20:43:59 PKT |

Table properties 1 entries Page 1 of 1

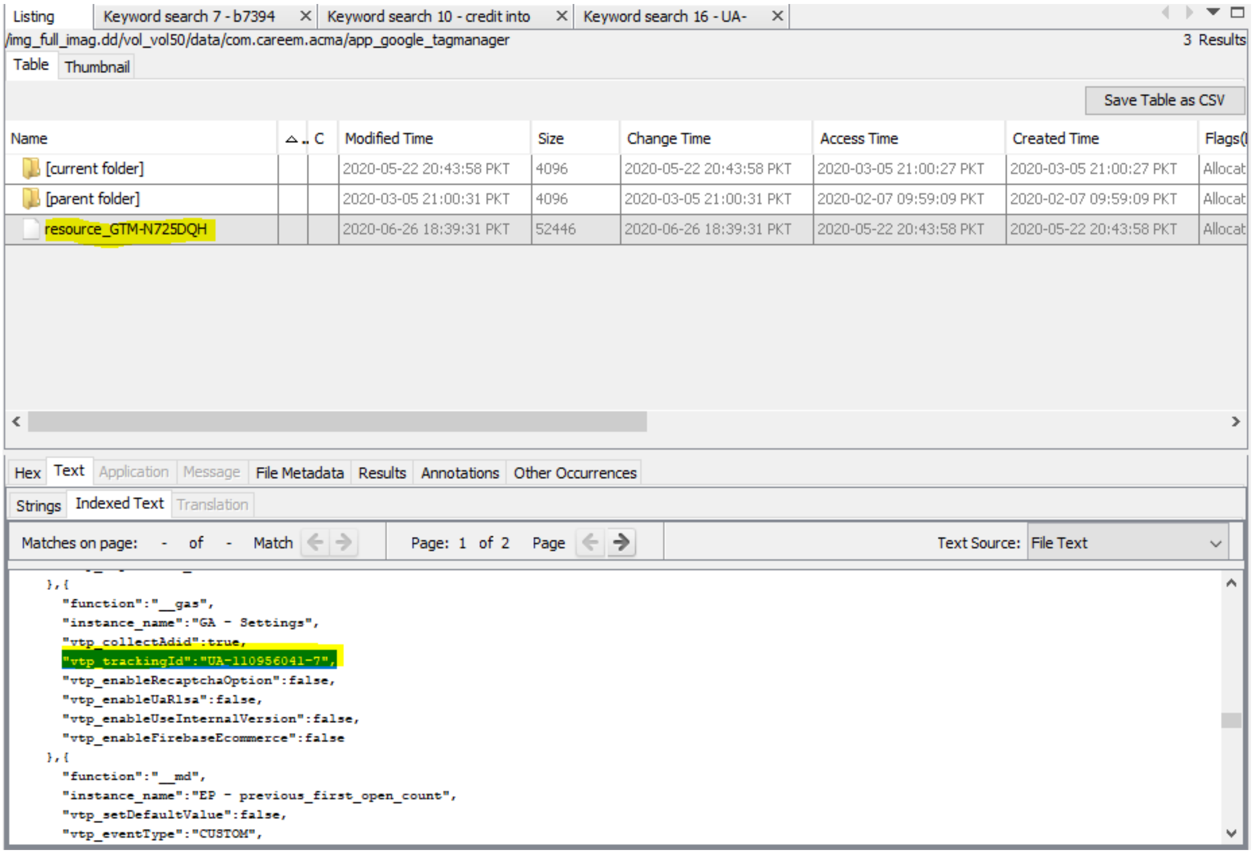
| app_uid | cid | tid | params | adid | hits_count |
|---|---|---|---|---|---|
| 0 | d99C0oSqSriJvYKXSU6rdZ | UA-110956041-7 | av=9.2.4&an=Careem&aid=com.careem.acma&aiid=com.android.vending | 1 | 152 |

Figure 39 – Google Analytics

Path:

*"/img_full_imag.dd/vol_vol50/data/com.careem.acma/app_google_tagmanager/resource_GTM-N725DQH"*

Google Tag Manager Tool allows you manage and deploy marketing tags on your application. Location is show in the figure 40.



/img_full_imag.dd/vol_vol50/data/com.careem.acma/app_google_tagmanager

| Name | C | Modified Time | Size | Change Time | Access Time | Created Time | Flags( |
|---|---|---|---|---|---|---|---|
| [current folder] | | 2020-05-22 20:43:58 PKT | 4096 | 2020-05-22 20:43:58 PKT | 2020-03-05 21:00:27 PKT | 2020-03-05 21:00:27 PKT | Allocat |
| [parent folder] | | 2020-03-05 21:00:31 PKT | 4096 | 2020-03-05 21:00:31 PKT | 2020-02-07 09:59:09 PKT | 2020-02-07 09:59:09 PKT | Allocat |
| resource_GTM-N725DQH | | 2020-06-26 18:39:31 PKT | 52446 | 2020-06-26 18:39:31 PKT | 2020-05-22 20:43:58 PKT | 2020-05-22 20:43:58 PKT | Allocat |

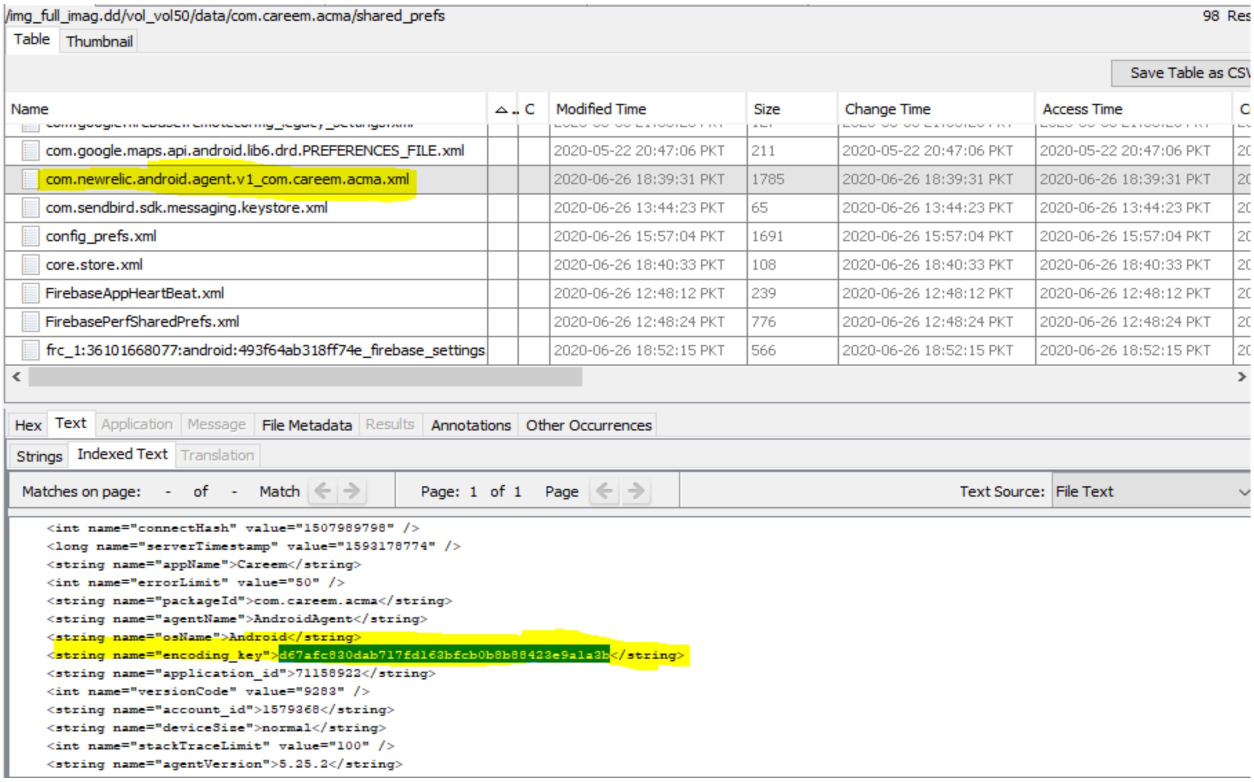
```
  },{
    "function":"__gas",
    "instance_name":"GA - Settings",
    "vtp_collectAdid":true,
    "vtp_trackingId":"UA-110956041-7",
    "vtp_enableRecaptchaOption":false,
    "vtp_enableUaRlsa":false,
    "vtp_enableUseInternalVersion":false,
    "vtp_enableFirebaseEcommerce":false
  },{
    "function":"__md",
    "instance_name":"EP - previous_first_open_count",
    "vtp_setDefaultValue":false,
    "vtp_eventType":"CUSTOM",
```

Figure 40 – Google Tracking ID

## 5.7 Misc. Remnants

This section contains artifacts related to encryption or encoding key.

Path:/img_full_imag.dd/vol_vol50/data/com.careem.acma/shared_prefs/com.newrelic.android.agent.v1_com.careem.acma.xml



/img_full_imag.dd/vol_vol50/data/com.careem.acma/shared_prefs
98 Res
Table
Thumbnail
Save Table as CSV

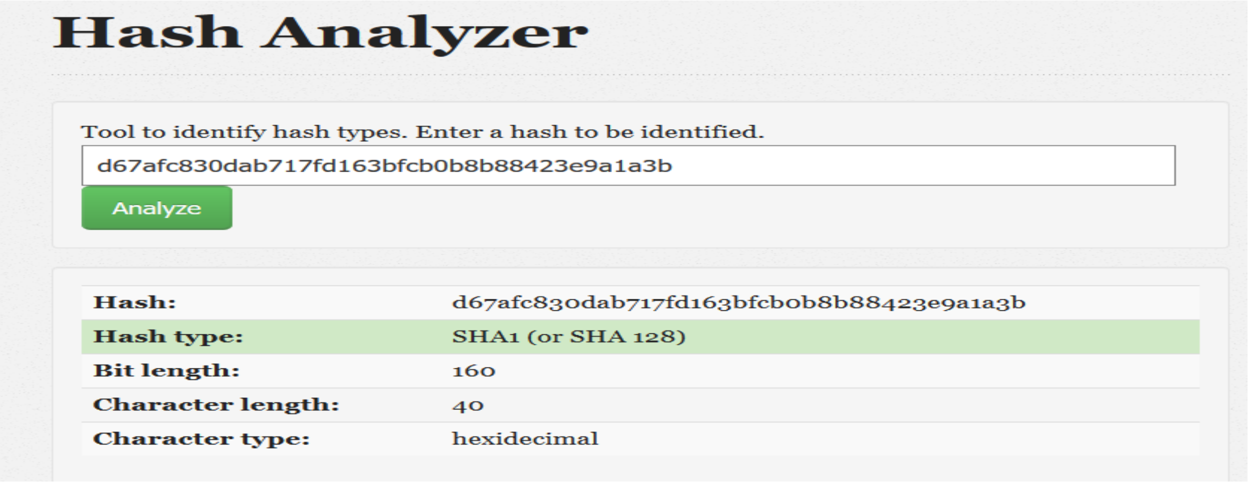
| Name | △.. | C | Modified Time | Size | Change Time | Access Time | C |
|---|---|---|---|---|---|---|---|
| com.google.maps.api.android.lib6.drd.PREFERENCES_FILE.xml | | | 2020-05-22 20:47:06 PKT | 211 | 2020-05-22 20:47:06 PKT | 2020-05-22 20:47:06 PKT | 20 |
| com.newrelic.android.agent.v1_com.careem.acma.xml | | | 2020-06-26 18:39:31 PKT | 1785 | 2020-06-26 18:39:31 PKT | 2020-06-26 18:39:31 PKT | 20 |
| com.sendbird.sdk.messaging.keystore.xml | | | 2020-06-26 13:44:23 PKT | 65 | 2020-06-26 13:44:23 PKT | 2020-06-26 13:44:23 PKT | 20 |
| config_prefs.xml | | | 2020-06-26 15:57:04 PKT | 1691 | 2020-06-26 15:57:04 PKT | 2020-06-26 15:57:04 PKT | 20 |
| core.store.xml | | | 2020-06-26 18:40:33 PKT | 108 | 2020-06-26 18:40:33 PKT | 2020-06-26 18:40:33 PKT | 20 |
| FirebaseAppHeartBeat.xml | | | 2020-06-26 12:48:12 PKT | 239 | 2020-06-26 12:48:12 PKT | 2020-06-26 12:48:12 PKT | 20 |
| FirebasePerfSharedPrefs.xml | | | 2020-06-26 12:48:24 PKT | 776 | 2020-06-26 12:48:24 PKT | 2020-06-26 12:48:24 PKT | 20 |
| frc_1:36101668077:android:493f64ab318ff74e_firebase_settings | | | 2020-06-26 18:52:15 PKT | 566 | 2020-06-26 18:52:15 PKT | 2020-06-26 18:52:15 PKT | 20 |

```
<int name="connectHash" value="1507989798" />
<long name="serverTimestamp" value="1593178774" />
<string name="appName">Careem</string>
<int name="errorLimit" value="50" />
<string name="packageId">com.careem.acma</string>
<string name="agentName">AndroidAgent</string>
<string name="osName">Android</string>
<string name="encoding_key">d67afc830dab717fd163bfcb0b8b88423e9a1a3b</string>
<string name="application_id">71158922</string>
<int name="versionCode" value="9283" />
<string name="account_id">1579368</string>
<string name="deviceSize">normal</string>
<int name="stackTraceLimit" value="100" />
<string name="agentVersion">5.25.2</string>
```

Figure 41 – Encoding Key

This location as shown in the Figure 41 keeps the encoding key which is in our case: d67afc830dab717fd163bfcb0b8b88423e9a1a3b

When this encoding key is analyzed by online software is appears to be SHA1 (or SHA 128) hash value which can be seen in Figure 42.

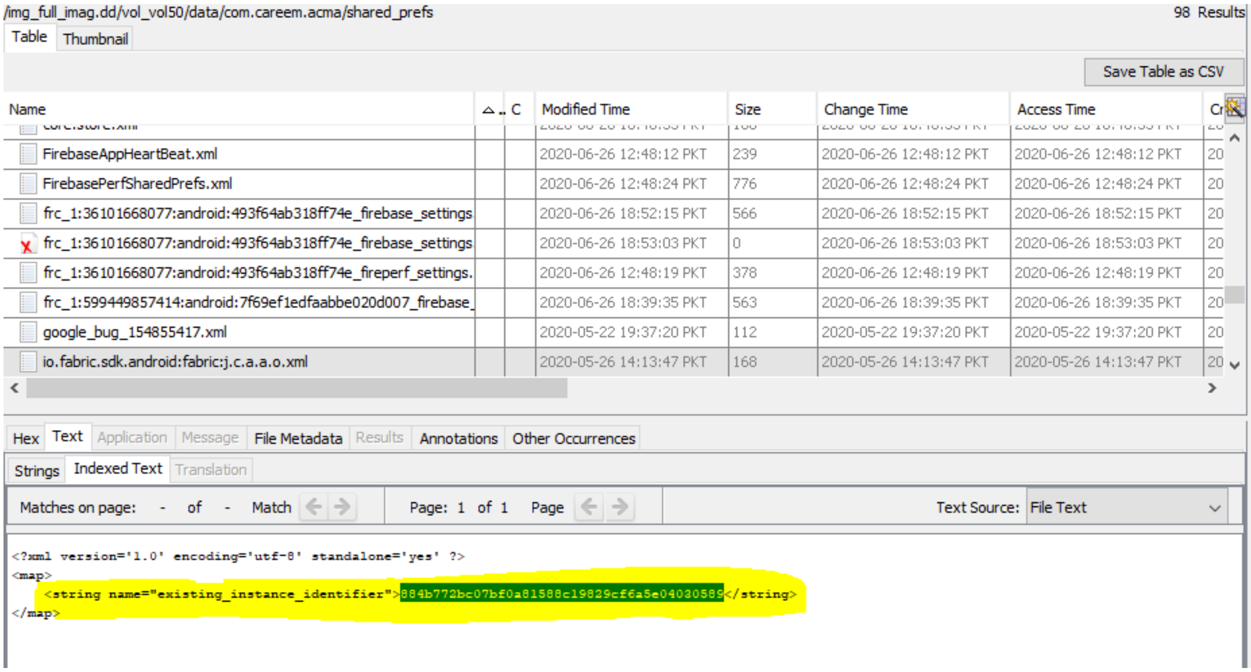


Hash Analyzer
Tool to identify hash types. Enter a hash to be identified.
d67afc830dab717fd163bfcb0b8b88423e9a1a3b
Analyze

| | |
|---|---|
| **Hash:** | d67afc830dab717fd163bfcb0b8b88423e9a1a3b |
| **Hash type:** | SHA1 (or SHA 128) |
| **Bit length:** | 160 |
| **Character length:** | 40 |
| **Character type:** | hexidecimal |

Figure 42 – Web based Hash Analyzer

Also existing instance identifier was SHA1 hash which can be seen in Figure 43.



/img_full_imag.dd/vol_vol50/data/com.careem.acma/shared_prefs    98 Results

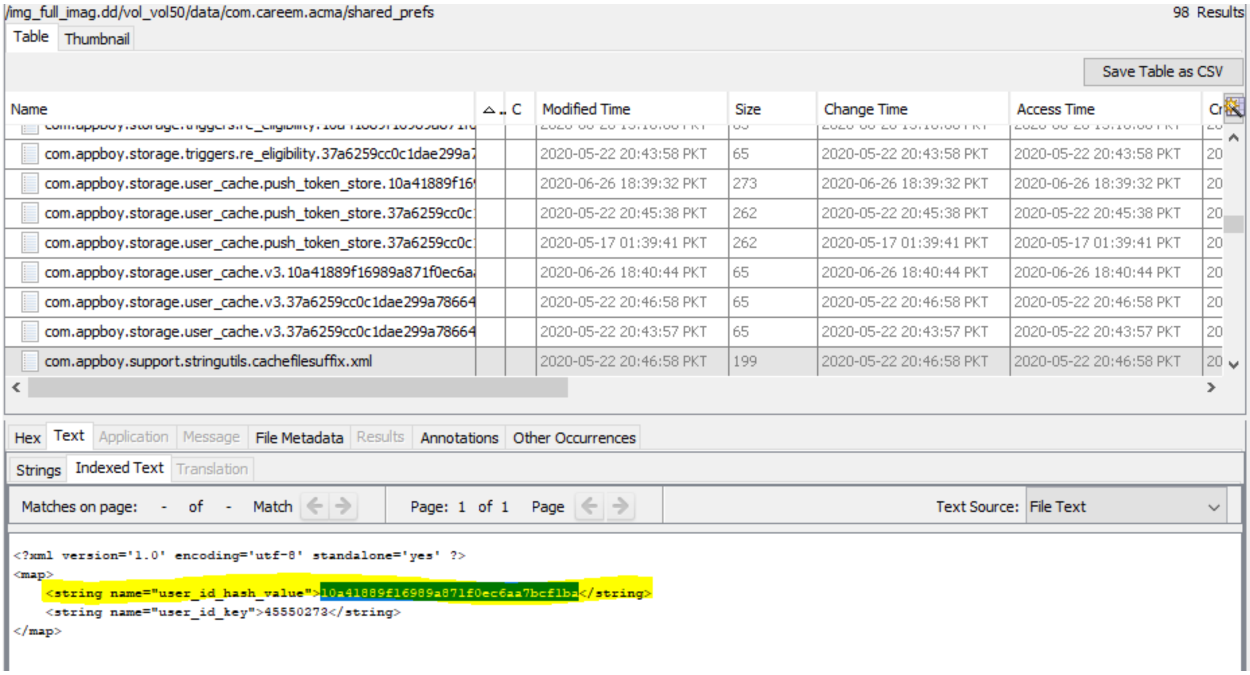
| Name | △ .. | C | Modified Time | Size | Change Time | Access Time | Cr |
|---|---|---|---|---|---|---|---|
| FirebaseAppHeartBeat.xml | | | 2020-06-26 12:48:12 PKT | 239 | 2020-06-26 12:48:12 PKT | 2020-06-26 12:48:12 PKT | 20 |
| FirebasePerfSharedPrefs.xml | | | 2020-06-26 12:48:24 PKT | 776 | 2020-06-26 12:48:24 PKT | 2020-06-26 12:48:24 PKT | 20 |
| frc_1:36101668077:android:493f64ab318ff74e_firebase_settings | | | 2020-06-26 18:52:15 PKT | 566 | 2020-06-26 18:52:15 PKT | 2020-06-26 18:52:15 PKT | 20 |
| frc_1:36101668077:android:493f64ab318ff74e_firebase_settings | | | 2020-06-26 18:53:03 PKT | 0 | 2020-06-26 18:53:03 PKT | 2020-06-26 18:53:03 PKT | 20 |
| frc_1:36101668077:android:493f64ab318ff74e_fireperf_settings. | | | 2020-06-26 12:48:19 PKT | 378 | 2020-06-26 12:48:19 PKT | 2020-06-26 12:48:19 PKT | 20 |
| frc_1:599449857414:android:7f69ef1edfaabbe020d007_firebase_ | | | 2020-06-26 18:39:35 PKT | 563 | 2020-06-26 18:39:35 PKT | 2020-06-26 18:39:35 PKT | 20 |
| google_bug_154855417.xml | | | 2020-05-22 19:37:20 PKT | 112 | 2020-05-22 19:37:20 PKT | 2020-05-22 19:37:20 PKT | 20 |
| io.fabric.sdk.android:fabric:j.c.a.a.o.xml | | | 2020-05-26 14:13:47 PKT | 168 | 2020-05-26 14:13:47 PKT | 2020-05-26 14:13:47 PKT | 20 |

Text Source: File Text

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="existing_instance_identifier">884b772bc07bf0a81588c19829cf6a5e04030589</string>
</map>
```

Figure 43 – Existing Instance ID

We found User id hash value which can be seen in Figure 44.



/img_full_imag.dd/vol_vol50/data/com.careem.acma/shared_prefs    98 Results

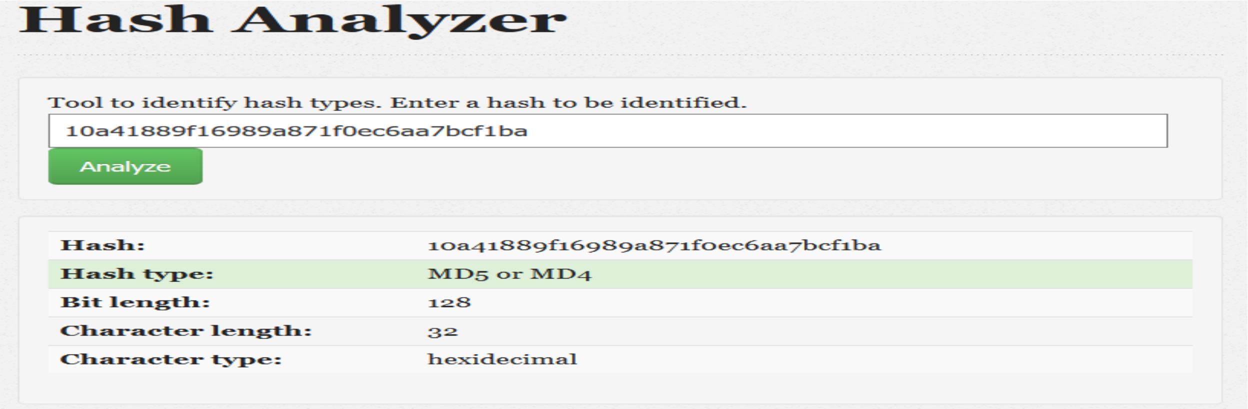
| Name | △ .. | C | Modified Time | Size | Change Time | Access Time | Cr |
|---|---|---|---|---|---|---|---|
| com.appboy.storage.triggers.re_eligibility.37a6259cc0c1dae299a7 | | | 2020-05-22 20:43:58 PKT | 65 | 2020-05-22 20:43:58 PKT | 2020-05-22 20:43:58 PKT | 20 |
| com.appboy.storage.user_cache.push_token_store.10a41889f16 | | | 2020-06-26 18:39:32 PKT | 273 | 2020-06-26 18:39:32 PKT | 2020-06-26 18:39:32 PKT | 20 |
| com.appboy.storage.user_cache.push_token_store.37a6259cc0c | | | 2020-05-22 20:45:38 PKT | 262 | 2020-05-22 20:45:38 PKT | 2020-05-22 20:45:38 PKT | 20 |
| com.appboy.storage.user_cache.push_token_store.37a6259cc0c | | | 2020-05-17 01:39:41 PKT | 262 | 2020-05-17 01:39:41 PKT | 2020-05-17 01:39:41 PKT | 20 |
| com.appboy.storage.user_cache.v3.10a41889f16989a871f0ec6a | | | 2020-06-26 18:40:44 PKT | 65 | 2020-06-26 18:40:44 PKT | 2020-06-26 18:40:44 PKT | 20 |
| com.appboy.storage.user_cache.v3.37a6259cc0c1dae299a78664 | | | 2020-05-22 20:46:58 PKT | 65 | 2020-05-22 20:46:58 PKT | 2020-05-22 20:46:58 PKT | 20 |
| com.appboy.storage.user_cache.v3.37a6259cc0c1dae299a78664 | | | 2020-05-22 20:43:57 PKT | 65 | 2020-05-22 20:43:57 PKT | 2020-05-22 20:43:57 PKT | 20 |
| com.appboy.support.stringutils.cachefilesuffix.xml | | | 2020-05-22 20:46:58 PKT | 199 | 2020-05-22 20:46:58 PKT | 2020-05-22 20:46:58 PKT | 20 |

Text Source: File Text

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="user_id_hash_value">10a41889f16989a871f0ec6aa7bcf1ba</string>
    <string name="user_id_key">45550273</string>
</map>
```

Figure 44 – User ID Hash

Hash analyzer reveals that it is MD5 hash value which can be seen in Figure 45.



Hash Analyzer

Tool to identify hash types. Enter a hash to be identified.

10a41889f16989a871f0ec6aa7bcf1ba

| | |
|---|---|
| Hash: | 10a41889f16989a871f0ec6aa7bcf1ba |
| Hash type: | MD5 or MD4 |
| Bit length: | 128 |
| Character length: | 32 |
| Character type: | hexidecimal |

Figure 45 – User ID MD5 Hash

## 5.8 Remnant’s Summary

Although it is very tough to conclude artifacts location due to fact that android application developers are constantly changing the internal structure of the application by empowering the application with new features. After analysis of the whole application, following visual representation of the artifacts in Figure 46 can be seen in term of the artifacts summary.

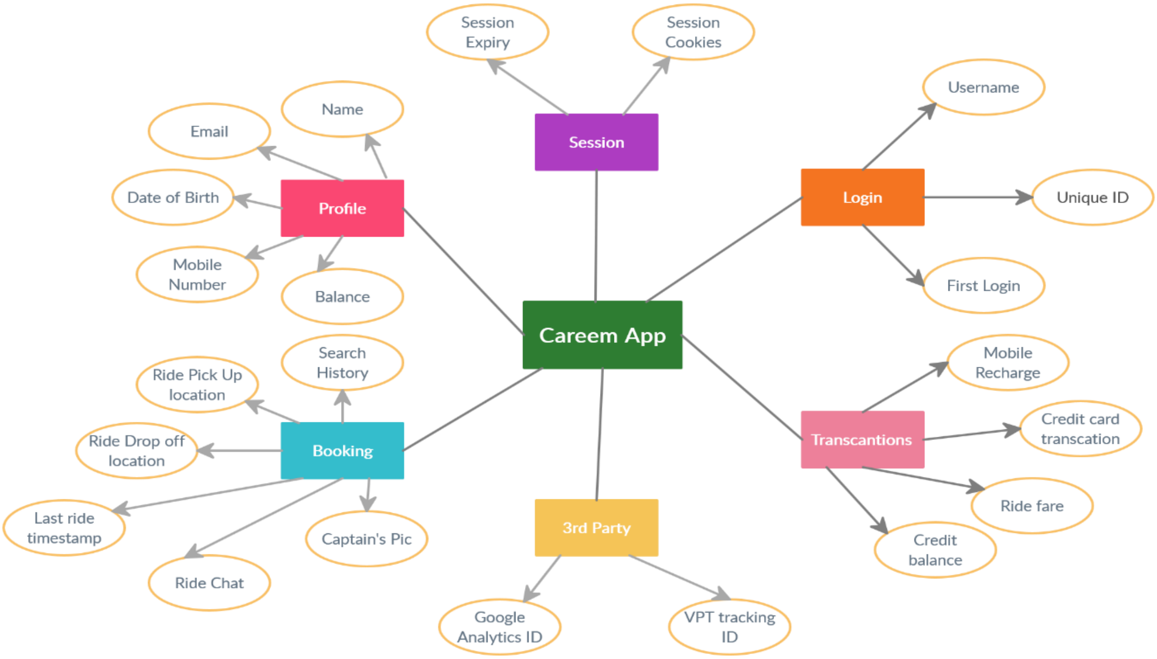


Figure 46 – Remnants summary

# Chapter 6

# 6. Results and conclusion:

## 6.1 Results & Conclusion

Generally, analyzing the mobile device for extracting the data from any application may require much effort and time. However, it is more important to study this area time to time to upgrade the investigation procedure. In this study, a Careem app for digital forensics have presented with all artifacts related to various activities done through this app. Proposed finding showed that user’s sensitive data that can be found on mobile device, which is not limited to location artifacts, user visited places, credit transfer, Credit card info, ride booking artifacts and in app chat artifacts can also be identified.

We have summarized all finding in a precise manner in a table format. This table gives a clear picture of the artifacts that can be found on mobile device after forensically analyzing the device.

Table 8 - Summary of all artifacts

| ID | Evidence Found | Visible to App User | Forensic Evidence | Path/location/Directory |
|---|---|---|---|---|
| 1 | Username | Yes | Yes | */img_img.dd/vol_vol50/data/com.careem.acma/shared_prefs/com.careem.acma.braze_user_attribute_store.xml* |
| 2 | User Email Address | Yes | Yes | */img_img.dd/vol_vol50/data/com.careem.acma/shared_prefs/com.careem.acma.braze_user_attribute_store.xml* |
| 3 | User Mobile Number | Yes | Yes | */img_img.dd/vol_vol50/data/com.careem.acma/shared_prefs/com.careem.acma.braze_user_attribute_store.xml* |
| 4 | User Date of Birth | Yes | Yes | */img_img.dd/vol_vol50/data/com.careem.acma/shared_prefs/com.careem.acma.braze_user_attribute_store.xml* |
| 5 | Credit Balance Information | Yes | Yes | */img_img.dd/vol_vol50/data/com.careem.acma/shared_prefs/com.careem.acma.braze_user_attribute_store.xml* |
| 6 | Credit Card Information | Partial | Yes | */img_img.dd/vol_vol50/data/com.careem.acma/shared_prefs/com.careem.acma.braze_user_attribute_store.xml*<br>*/img_img.dd/vol_vol50/data/com.careem.acma/shared_prefs/ACMASharedPreferenceKey.xml* |
| 7 | Active Time (App Activity) | No | Yes | */img_img.dd/vol_vol50/data/com.careem.acma/shared_prefs/com.google.android.gms.measurement.prefs.xml* |
| 8 | First Open Time | No | Yes | */img_img.dd/vol_vol50/data/com.careem.acma/shared_prefs/com.google.android.gms.measurement.prefs.xml* |
| 9 | app install Time | No | Yes | */img_img.dd/vol_vol50/data/com.careem.acma/shared_prefs/com.google.android.gms.measurement.prefs.xml* |
| 10 | Last Pause Time | No | Yes | */img_img.dd/vol_vol50/data/com.careem.acma/shared_prefs/com.google.android.gms.measurement.prefs.xml* |
| 11 | Device ID | No | Yes | */img_img.dd/vol_vol50/data/com.careem.acma/shared_prefs/com.newrelic.android.agent.v1_com.careem.acma.xml* |
| 12 | Encoding Key | No | Yes | */img_img.dd/vol_vol50/data/com.careem.acma/shared_prefs/com.newrelic.android.agent.v1_com.careem.acma.xml* |
| 13 | Ride Pickup Location | Partial | Yes | */img_img.dd/vol_vol50/data/com.careem.acma/databases/CareemDb* |
| 14 | Ride Dropoff Location | Partial | Yes | */img_img.dd/vol_vol50/data/com.careem.acma/databases/CareemDb* |
| 15 | Ride Pickup Time |  | Yes | */img_full_imag.dd/vol_vol50/data/com.google.android.gms/files/fcm_queued_messages.ldb/000092.ld* |
| 16 | Ride Dropoff Time |  | Yes | */img_full_imag.dd/vol_vol50/data/com.google.android.gms/files/fcm_queued_messages.ldb/000092.ld* |
| 17 | Google map Coordinates | No | Yes | */img_img.dd/vol_vol50/data/com.careem.acma/databases/CareemDb* |
| 18 | Search History | No | Yes | */img_img.dd/vol_vol50/data/com.careem.acma/databases/CareemDb* |

| ID | Evidance Found | Visible to App User | Forensic Evidance | Path/location/Directory |
|---|---|---|---|---|
| 19 | Credit Transaction Record | Partial | Yes | /img_img.dd/vol_vol50/data/com.google.android.gms/files/fcm_queued_messages.ldb/000062.ldb<br>/img_img.dd/vol_vol50/data/com.google.android.gm/databases/bigTopDataDB.3981793-wal |
| 20 | Cancelled Booking Information | No | Yes | /img_img.dd/vol_vol50/data/com.google.android.gms/files/fcm_queued_messages.ldb/000062.ldb |
| 21 | Credit Sender Information | Partial | Yes | /img_img.dd/vol_vol50/data/com.google.android.gms/files/fcm_queued_messages.ldb/000062.ldb<br>/img_img.dd/vol_vol50/data/com.google.android.gm/databases/bigTopDataDB.3981793-wal |
| 22 | app chat | No | Yes | /img_img.dd/vol_vol50/data/com.google.android.gms/files/fcm_queued_messages.ldb/000065.ldb |
| 23 | Booking Information | Partial | Yes | /img_img.dd/vol_vol50/data/com.google.android.gms/files/fcm_queued_messages.ldb/000065.ldb |
| 24 | Careem Captain Picture | No | Yes | /img_img.dd/vol_vol50/data/com.careem.acma/cache/image_manager_disk_cache |
| 25 | Google Tracking ID | No | Yes | /img_full_imag.dd/vol_vol50/data/com.careem.acma/databases/google_analytics_v4.db |
| 26 | Session Cookie | No | Yes | /img_img.dd/vol_vol50/data/com.careem.acma/app_webview/Cookies |
| 27 | 3rd Party Service Access Token | No | Yes | /img_img.dd/vol_vol50/data/com.careem.acma/shared_prefs/accessToken.xml |
| 28 | Last Storage Update | No | Yes | /img_img.dd/vol_vol50/data/com.careem.acma/shared_prefs/com.appboy.storage.content_cards_storage_provider.metadata.10a41889f16989a871f0ec6aa7bcf1ba.5d83dd70-af35-427d-84b8-cb0e55815612.xml |
| 29 | Vehical information | No | Yes | /img_img.dd/vol_vol50/data/com.google.android.gms/files/fcm_queued_messages.ldb/000065.ldb |
| 30 | Number of trips in a month | No | Yes | /img_img.dd/vol_vol50/data/com.careem.acma/shared_prefs/com.careem.acma.braze_user_attribute_store.xml |
| 31 | Last Location fetch CALL TIME | No | Yes | /img_img.dd/vol_vol50/data/com.careem.acma/shared_prefs/ACMASharedPreferenceKey.xml |
| 32 | captain Arived Time | No | Yes | /img_img.dd/vol_vol50/data/com.careem.acma/shared_prefs/ACMA_NOW_BOOKING_DATA.xml |

| ID | Evidance Found | Visible to App User | Forensic Evidance | Path/location/Directory |
|---|---|---|---|---|
| 33 | Registration Pin Code | Yes | Yes | */img_img.dd/vol_vol50/user_de/0/com.android.providers.telephony/databases/mmssms.db* |
| 34 | delivery ride information | Yes | Yes | */img_full_imag.dd/vol_vol50/data/com.google.android.gms/files/fcm_queued_messages.ldb/000092.ld* |

## 6.2 Future work

As in this study, Careem application was chosen for forensic analysis and we made our best attempt to collect all possible artifacts present on the application, However, all the application on the play store indeed are kept on updating, the application team is constantly adding new feature and changing the app structure which may require some additional forensics work by the passage of time. Also, there are several other applications in the market like Uber, Daewoo, Pakistan Railways official app which are also required forensics analysis. We have analyzed the Careem application and found many encoding keys and hashes that are used for either network communication or maintaining a session with Careem application servers. Analysis of these encoding keys are not included in the scope of this study but for forensics perspective, these encoding keys or hash values needs further analysis and it may help forensics investigator to get more useful insights of the Careem application

As discussed above there are several other application which needs forensics analysis, our idea is to collect all the artifacts of those travelling application and develop a framework to analyze the user travelling behavior based on those applications with some machine learning algorithms to predict the future travelling of the user.

# References

[1] En.wikipedia.org. 2020. *Forensic Science*. [online] Available at: https://en.wikipedia.org/wiki/Forensic_science

[2] National Institute of Justice. 2020. *Forensic Sciences*. [online] Available at: https://www.nij.gov/topics/forensics/Pages/welcome.aspx

[3] M Reith; C Carr; G Gunsch (2002). "An examination of digital forensic models". International Journal of Digital Evidence. CiteSeerX 10.1.1.13.9683

[4] En.wikipedia.org. 2020. *Digital Forensics*. [online] Available at: https://en.wikipedia.org/wiki/Digital_forensics#cite_note-ijde-2002-1

[5] Infosec Resources. 2020. The Mobile Forensics Process: Steps & Types. [online] Available at: https://resources.infosecinstitute.com/category/computerforensics/introduction/mobile-forensics/the-mobile-forensics-process-steps-types/#gref

[6] En.wikipedia.org. 2020. *Chain Of Custody*. [online] Available at: https://en.wikipedia.org/wiki/Chain_of_custody

[7] Statista. 2020. *Smartphone Users Worldwide 2020 | Statista*. [online] Available at: https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/.

[8] Creswell, John W. *Educational research: Planning, conducting, and evaluating quantitative*. Upper Saddle River, NJ: Prentice Hall, 2002.

[9] xda-developers. 2020. *What Is Magisk?* [online] Available at: https://www.xda-developers.com/what-is-magisk/

[10] En.wikipedia.org. 2020. Busybox. [online] Available at: https://en.wikipedia.org/wiki/BusyBox

[11] En.wikipedia.org. 2020. *Autopsy (Software)*. [online] Available at: https://en.wikipedia.org/wiki/Autopsy_(software)

[12] Lukito, Novelino Yona Pribadi, Fazmah Arif Yulianto, and Erwid Jadied. "Comparison of data acquisition technique using logical extraction method on Unrooted Android Device." In 2016 4th International Conference on Information and Communication Technology (ICoICT), pp. 1-6. IEEE, 2016

[13] Alghafli, Khawla Abdulla, Andrew Jones, and Thomas Anthony Martin. "Forensics data acquisition methods for mobile phones." In *2012 International Conference for Internet Technology and Secured Transactions*, pp. 265-269. IEEE, 2012.

[14] Sciencedirect.com. 2020. *Logical Acquisition - An Overview | Sciencedirect Topics*. [online] Available at: https://www.sciencedirect.com/topics/computer-science/logical-acquisition

[15] Kitsaki, Theodoula-Ioanna, Anna Angelogianni, Christoforos Ntantogian, and Christos Xenakis. "A forensic investigation of Android mobile applications." In *Proceedings of the 22nd Pan-Hellenic Conference on Informatics*, pp. 58-63. 2018.

[16] Zhang, Hao, Lei Chen, and Qingzhong Liu. "Digital forensic analysis of instant messaging applications on android smartphones." In *2018 International Conference on Computing, Networking and Communications (ICNC)*, pp. 647-651. IEEE, 2018.

[17] Osho, Oluwafemi, Uthman L. Mohammed, Nanfa N. Nimzing, Andrew A. Uduimoh, and Sanjay Misra. "Forensic Analysis of Mobile Banking Apps." In *International Conference on Computational Science and Its Applications*, pp. 613-626. Springer, Cham, 2019

[18] Srivastava, Himanshu, and Shashikala Tapaswi. "Logical acquisition and analysis of data from android mobile devices." *Information & Computer Security* (2015).

[19] Chanajitt, Rajchada, Wantanee Viriyasitavat, and Kim-Kwang Raymond Choo. "Forensic analysis and security assessment of Android m-banking apps." *Australian Journal of Forensic Sciences* 50, no. 1 (2018): 3-19.

[20] Kim, Dohyun, and Sangjin Lee. "Study of identifying and managing the potential evidence for effective Android forensics." *Forensic Science International: Digital Investigation* (2020): 200897.

[21] Counterpoint Research. 2020. *Average Storage Capacity In Smartphones To Cross 80GB By End-2019 - Counterpoint Research*. [online] Available at: https://www.counterpointresearch.com/average-storage-capacity-smartphones-cross-80gb-end-2019/

[22] Lwin, Htar Htar, Wai Phyo Aung, and Kyaw Kyaw Lin. "Comparative Analysis of Android Mobile Forensics Tools." In *2020 IEEE Conference on Computer Applications (ICCA)*, pp. 1-6. IEEE, 2020.

[23] Al-Sabaawi, Aiman, and Ernest Foo. "A Comparison Study of Android Mobile Forensics for Retrieving Files System." *International Journal of Computer Science and Security (IJCSS)* 13, no. 4 (2019): 148.

[24] Riadi, Imam, Anton Yudhana, and Muhamad Caesar Febriansyah Putra. "Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method." *Scientific Journal of Informatics* 5, no. 2 (2018): 235-247.

[25] Azfar, Abdullah, Kim-Kwang Raymond Choo, and Lin Liu. "Forensic taxonomy of android productivity apps." *Multimedia Tools and Applications* 76, no. 3 (2017): 3313-3341.

[26] La Polla, Mariantonietta, Fabio Martinelli, and Daniele Sgandurra. "A survey on security for mobile devices." *IEEE communications surveys & tutorials* 15, no. 1 (2012): 446-471.

[27] Careem.com. 2020. *The Careem Story – Learn More About Careem'S Mission*. [online] Available at: https://www.careem.com/en-ae/our-story/