Forensic Analysis of Credit Scoring Mobile Applications

Achini Dinusha Dissanayaka

This document is a dissertation towards
Master of Science

UNIVERSITY OF SALFORD

SCHOOL OF COMPUTING, SCIENCE AND ENGINEERING

SEPTEMBER 01, 2022

Table of Contents

List of Tables

List of Figures

List of Abbreviations

OS Operating System

NIST National Institute of Standards and Technology

VOIP Voice Over Internet Protocol

GPS Global Positioning System

PIN Personal Identification Number

UFED Universal Forensic Extraction Device

FRED Forensic Recovery of Evidence Device

TWRP Team Win Recovery Project

UUID Universally Unique Identifier

Acknowledgement

I would like to acknowledge all of the project supervisors for their comprehensive guidance and assistance in ensuring the completion of my dissertation successfully in such a timely manner. Finally, I would be glad to convey my sincere gratitude to all the academic lecturers; without their support, the required knowledge would not have been obtained to complete the project.

Abstract

Credit scoring applications are very popular in the United Kingdom as they provide instant access to information related to credit scores and credit reports. Users can use these applications to check their credit assessment, and entitlement for credit cards and loans, monitor the movement of their credit score, etc. Although credit scoring applications collect user-sensitive data, there is a lack of research to address credit scoring applications' privacy and security concerns on popular mobile platforms such as iOS and Android. Hence, the frequency of potential security and privacy breaches and their impacts are unknown. This study aims to identify the data remnants which are left by credit scoring applications as they can be a significant contributor to prospective security and privacy breaches. A comprehensive forensic analysis of three popular credit scoring applications: ClearScore, Credit Karma, and Experian was performed on both Android and iOS mobile platforms to identify the security and privacy concerns of the applications. Logical data images were acquired from the local storage, for two case scenarios: before and after uninstalling the applications. The user's personal information including name, address, phone number, email address, etc was recovered from the images. Thus, this study concludes that despite these applications incorporating various security features, it was possible to recover the user-sensitive data from the data remnants which were left behind. From the perspective of digital forensics, this study provides a rich source of forensic information related to credit scoring applications.

Keywords: mobile forensic analysis, credit scoring applications, Android, iOS

Chapter 1

Introduction

1.1 Introduction

Smartphones have become a very important part of modern society, from leisure activities such as photography, streaming, and gaming, to many complex tasks of navigating, banking, investing, etc. Worldwide smartphone users have increased at an accelerating rate from 49% in 2016 to a whopping 83% in 2022 Rolfe (2022). As a result of the covid 19 pandemic and social distancing, people rely even more on smartphones. (Meredith E. David, 2021).

With the rapidly growing usage of smartphones and their ability to handle complex tasks efficiently, more and more applications have been developed to manage our day-to-day tasks (Indeed, 2021). Many of these applications collect personal details such as phone numbers, postal codes, addresses, and birthdays. Most users do not know how their data are managed. Despite the various data protection law enforcement in the United Kingdom, bad actors can manipulate people into giving up their personal and sensitive information via bogus mobile applications (Fraudwatch, 2022). In 2021, cybercrimes have increased more dramatically by 600% than in previous years (Govindraj, 2022). Due to the covid pandemic, everyone holed up in their homes and almost all the people had to work remotely using information

technology. In this period mobile phone users increased exponentially as smartphones have become a companion for entertainment. Cybercriminals took this to their advantage and amplified their illicit activities. Cyber forensic practitioners suspect that more than 24 billion illegally acquired user login credentials are shared over dark websites (Muncaster, 2022).

The credit score is a numeric value that represents the creditworthiness of a person, which is used by financial institutions to make credit decisions such as credit cards, loans, buy now and pay later facilities, etc (Wu, 2021). Credit scoring mobile applications are very popular in the United Kingdom as they can provide instant access to information related to credit scores and credit reports (Wollit, 2021). Using these apps, users can check their credit assessment, and entitlement for credit cards and loans, and monitor the movement of their credit score (Bahrynovska, 2022). Users are able to keep up a good credit score by maintaining an up-to-date credit profile and these applications will often provide tips and tricks to improve the credit score, as an added advantage, credit scoring applications employ a mechanism called soft search, which allows users to check their eligibility for financial services without having an impact on the credit score (Wollit, 2021). Even though the users are generally cautious when using mobile applications that utilize user personal information (University, 2015) such as banking, and finance apps, credit scoring applications are commonly overlooked.

1.2 Motivation of Study

At the initial stage of this case study, it was discovered that there are no previous research materials related to the forensic investigations of credit scoring applications, even though these applications are widely used. The potential for breach of personal data is significant, although credit scoring applications do not collect users' financial data, they do allow users to link their bank accounts. On the other hand, these applications do collect personal data such as email addresses, contact numbers, and postal codes. If user accounts were to be compromised, users could be targeted with marketing materials or advertisements that could be bogus or

legitimate. Either way, it would be a violation of privacy as users did not consent. There is a huge potential for enhanced social engineering if the credit score value was compromised. Especially when there are no previous studies and the frequency of such occurrences or the impact is unknown, it could be difficult to minimize the impact of such an incident until it is too late. Hence, it is necessary and motivating to understand how credit scoring applications operate and identify the data evidence that is left behind, which would lead to prospective privacy concerns.

1.3 Problem statement

Implementing an application that is free from any security flaw is near impossible, even though these flaws can aid forensics investigators to combat cyber threats. They are the root of the problem as these flaws made it possible to carry out cyber-crimes in the first place, not to mention the aspects of social engineering. Digital forensic analysts and researchers must stay up to date with mobile application forensics, as newer versions of existing operating systems are released frequently by the manufacturers, and they may introduce new vulnerabilities as well. This leads to a lack of comprehensive forensic analysis research for most of the popular mobile applications. Furthermore, cyber crimes are increasing rapidly, and it seems to be that there are no research papers on mobile forensics related to credit scoring applications. Hence it is not only a crucial requirement but also there is a sense of urgency to carry out forensic investigations on this topic.

1.4 Aim and Objectives

The main purpose of this study is to examine data remnants and to recover user sensitive data that is left behind by credit scoring applications. The study uses a case study of three credit scoring applications named ClearScore, Credit Karma and Experian on both Android and iOS operating systems in two case scenarios: before

and after uninstalling the applications, to identify the security and privacy concerns of all the applications from the perspective of the end users. The objectives of the proposed work are as below.

- To identify the research gap in forensic analysis of credit scoring mobile applications with the aid of previous research papers.
- To choose a set of credit scoring mobile applications and identify the security features provided by each application on both android and iOS platforms.
- To create user accounts in the selected set of applications with frictional data to evaluate the security of the selected set of applications at two stages: before and after uninstalling the applications.
- To examine the recoverable personal data of these applications at each stage to identify the security concerns of each application.
- To carry out a comparative analysis between the three applications and the two platforms based on the recovered personal data.

1.5 Approach to Project

In this dissertation, the quantitative approach was used to accomplish the objectives of the project. Mobile devices with the newest versions of operating systems were used to carry out forensic analysis to widen the mobile forensics field while addressing a missed spot. Multiple approaches and tools were adopted to focus on the new technologies. As the initial step of the project, the following steps needed to be fulfilled.

- Selecting applications using the quantitative approach
- Identify the tools required for the experimental setup.

- Install the applications and tools accordingly on the two mobile devices and the laptop that is used to collect the data remnants.
- Create frictional user accounts in ClearScore, Credit Karma, and Experian applications.
- Root and jailbreak the mobile devices to achieve privileged access to the internal storage of the mobile phones.

Once the above steps were accomplished, the mobile forensic investigation and analysis process was initiated.

1.6 Project Plan

In this study, a comprehensive forensic analysis of credit scoring mobile applications is conducted to address the aforementioned problems (figure 1.1). The research outline of this project is as follows:

- Literature review.
- Forensic investigation of the applications.
- Analysis of findings.
- Comparison of the three applications and the two platforms.
- Report writing.

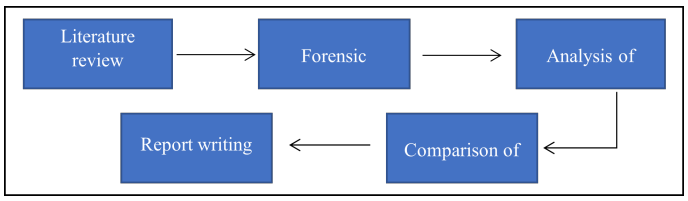

Figure 1.1: Research methodology outilne

1.7 Dissertation Structure

The remainder of this dissertation is structured as follows. Section 2 provides background information about credit scoring applications, cyber crimes related to financial mobile applications and previous research work related to mobile forensic investigations. In section 3, the outlines of the research methodology and experimental setup for acquiring data remnants from both Android and iOS platforms before and after uninstalling the applications are presented. Section 4 elaborates on the research findings and section 5 presents a discussion on the findings of the research and carries out a comparison between the data remnants recovered from each application and Operating System (OS). In section 6, a critical evaluation of the project is carried out. Finally, section 7 concludes the paper and suggests future research concepts.

Chapter 2

Literature review

Credit scoring applications are quite popular and widely used among people as they provide instant access to information related to credit scores and credit reports Wollit (2021) including the ability to check their credit assessment, entitlement for credit cards and loans, monitor the movement of their credit score Bahrynovska (2022), maintain a good credit score by staying up-to-date, improve the credit score by utilizing the tips and tricks provided by these applications, check their eligibility for financial services without having an impact on the credit score etc Wollit (2021). Even though the credit scoring applications collect user personal details including user's name, address, phone number, email address, date of birth, credit score, etc, there is a lack of research to address the security and privacy concerns of these applications. According to Carnegie Endowment for International Peace organisation, there are about 200 reported cyber incidents related to financial institutions since. In December 2020, a massive bank theft was identified by a group of cyber forensics. According to their estimations, the hackers spoofed around 16,000 mobile phones of the customers of European and American banks to steal money from their mobile bank accounts. A mobile malware that targeted to steal personal data from over 2,000 mobile banking users in Brazil was discovered in 2018. This malware entered the users' mobile devices as a trojan of Google play store applications in 2007 (Carnegie Endowment, 2022). Thus, there is an unknown

frequency of security and privacy breaches for mobile applications related to the financial field.

Previous studies have forensically analysed a wide range of iOS and Android mobile applications such as banking, messaging, financial, navigation, cloud storage, and social networking applications (ALThebaity, 2020), (Menahil et al., 2021), (Salamh et al., 2021), (Kim et al., 2022), (Dargahi et al., 2017), (Yuliani & Riadi, 2019), (Shin et al., 2022), (Kang et al., 2020), (Kitsaki et al., 2018), (Zhang et al., 2017), (Duncan & Karabiyik, 2018), (Gilbert & Seigfried-Spellar, 2022), (Uduimoh et al., 2019). Even though credit scoring mobile applications have a very high risk of potential security and privacy breaches, there were no research papers as they seem to be commonly overlooked. From the perspective of digital forensic analysis, there is a vital requirement to examine the applications that collect user-sensitive data, so the investigators can efficiently accumulate forensic evidence required for cyber-crimes-related court cases.

2.1 Mobile forensic analysis

Due to the rapid growth of mobile fraud and cybercrimes, the need for smartphone forensics has risen. Thus, the researchers of previous studies coined several efficient models for forensic analysis of mobile devices. Amine Chelihi et al. (2017), forensically analysed android mobile cloud-based storage applications using XRY forensic tool and suggested a comprehensive forensics taxonomy that reveals recoverable data remnants of mobile cloud applications which aid to correlate with the evidence of user activities for investigation purposes. Out of the 31 cloud applications they examined, some applications revealed no data artefacts on XRY, some of the apps stored database files in the local storage but not the dataset files while some apps led to the recovery of the files of the dataset. The taxonomy was devised according to the above categories.

As there are limitations of manual reverse engineering and dynamic analysis to locate critical data, Lin et al. (2018) proposed an efficient, static forensic tool named Fordroid for android mobile applications to automatically locate all the information

related to sensitive data stored in the local storage. Due to the complexity of generating the program path to the critical code, they were unable to locate the files using dynamic analysis. With the aid of their proposed tool, they evaluated 100 random android applications that were classified under four categories: communication, news and information, entertainment and games, and tools. The authors observed that 56% of applications disclose crucial data whilst 36% store crucial data in the local storage. According to their observations, Fordroid takes an average of 38 minutes to analyse one application and it was 98% successful in discovering the storage location of critical information. They recommend this proposed work for analysing normal applications, whilst using it for analysing Android malware by combining it with other techniques such as binary analysis, dynamic analysis, unpacking, and deobfuscation to enhance the accuracy of revealing the sensitive information paths as malware usually tends to adopt native code, obfuscation and packing to protect itself.

2.2 Data remnants acquisition

With the exponential growth of smartphone users, third-party mobile application usage has increased rapidly. Due to this excessive usage of mobile applications, cybercriminals are actively targeting low-secured mobile applications which leads the user's sensitive information or data artefacts available in the local storage of the device to be exposed to cybercrimes, and digital exploitations (SSL2Buy, 2022). In this regard, ALThebaity (2020) discovered the location and types of recoverable data artefacts left by the Facebook mobile application on an android smartphone upon the deletion of the app. The researchers utilized two android mobile devices to explore the data remnants of the Facebook application before and after uninstalling the app. Their observations revealed that there were three critical database files that consist of Facebook user activities: analytics, friends, and messages SQLite database file. By correlating all these files, they were able to retrieve a substantial amount of evidence relating to the cybercrimes that arose on the Facebook application.

The authors in (Menahil et al., 2021) focused on analysing five social networking apps: Instagram, LINE, whisper, WeChat, and Wickr on android smartphones with the aid of four tools named Magnet AXIOM, Autopsy, and XRY to determine whether there are data artifacts inside the local storage of the device. They comparatively analysed the capability and performance of these forensic tools with regard to the National Institute of Standards and Technology (NIST) standards whilst discovering that a significant amount of crucial data remains in the internal storage of smartphones after using them. The number of artifacts retrieved by each tool was used to calculate the index number which emphasizes the percentage of useful extractions recovered by the tool. According to their calculations, the index of Magnet AXIOM, Autopsy, and XRY was 76%, 71.5%, and 65.5% respectively. Based on these results they ranked Magnet AXIOM as number 1, Autopsy as number 2, and XRY as number 3.

Likewise, Salamh et al. (2021) carried out a forensic examination on both iOS and Android operating systems to discover forensic artefacts and determine security and privacy concerns in popular mobile applications that are classified under the categories: Instant messaging, social networks, Voice Over Internet Protocol (VOIP), and vault apps while validating the investigation on selected forensic software for verification and reproducibility. The authors of this research successfully analysed 27 Android applications and 33 iOS applications using Autopsy and Magnet AXIOM tools and discovered vital evidence for a forensic practitioner. The retrieved data of each app was compared with the data artefacts of older app versions obtained from previous studies.

In a similar line of study, a forensic analysis of two system default applications: Gallery, Messages and two user-installed applications: KakaoTalk and Facebook Messenger applications have been carried out to discover the deleted data remaining on android mobile devices and expose the possibility of deleted data recovery which is vital in enhancing user data privacy (Kim et al., 2022). The deleted data analysis was carried out using three different scenarios: Data deletion using the app's own delete function, deletion using the cache deletion function, and uninstalling installed apps. The authors were able to observe that the data recovery was feasible for all the applications in scenario 1. In the second scenario, data retrieving was probable only for the Message and gallery app based on the journal area or

backed-up inode but not possible for the Facebook messenger and KakaoTalk apps. As the third scenario requires uninstalling the apps for data deletion, the data recovery of Message and Gallery apps cannot be performed. The data recovery was achievable in the KakaoTalk app through the journal area, but not conceivable in the Facebook messenger app.

Moreover, Dargahi et al. (2017) explored forensic remnants of three popular instant messaging mobile applications: Viber, Skype, and WhatsApp on Android mobile devices. This research was performed under three phases: The setup phase, the logical acquisition phase, and the Identification and analysis phase. In the first phase, the source of evidence was discovered. Logical image acquisition of the Android device was the second phase in which rooting of the android smartphone was performed using the Odin3 tool. The last phase was the identification of evidence files and their locations on the logical image with the aid of AccessData FTK Imager. The researchers discovered possible data remnants of these applications which provide a rich source of artifacts that could head off a lawsuit if any cybercrime related to mobile applications takes place. The final outcomes of this study are a comparative analysis of different VOIP apps and a guideline for forensic analysts for their future investigations.

A similar effort has also been carried out to forensically analyse WhatsApp on Android smartphones by Yuliani & Riadi (2019). In this study, they utilized two android mobile applications, one as the offender's mobile device and the other as the victim's mobile device. The approach used by the authors of this research was guided by the mobile forensic method of NIST. With the aid of Oxygen forensic software and Andriller utility, they managed successfully to obtain artifact evidence in the form of conversational messages by exploring the WhatsApp database file which is stored in the local storage.

Shin et al. (2022) forensically analysed note and journal mobile applications that consist of security features within the app. In this study, they analysed 56 applications to identify the vulnerabilities of the applications by determining the processes of storing user-created content, and secret values utilized for locking purposes. In this piece of work, they examined and categorized the default security features provided by the applications into three groups such as no applied security to user content and secret value, security applied to secret value or user content,

and security applied to both user content and secret value. The data acquisition was performed in android smartphones by rooting the devices whilst acquiring the data in iOS devices using the backups provided by the manufacturer. The observations emphasize that 95% of the applications that provide security features within the app do not provide enough protection to store user data securely. Finally, the authors proposed several methods to acquire the password using the secret value obtained from the artefacts of each application.

Moreover, Kang et al. (2020) compared the functionality of two fitness tracking devices named Fitbit Alta HR and Xiaomi Mi Band 2 that is connected to android mobile applications and provided general aspects of fitness tracker analysis to make aware a forensic practitioner. In this study, they highlighted the core features of the devices, the approach for obtaining data from android devices, and ways to analyse user activities (the heart rate, sleep cycle, distance or altitude walked, the number of steps, Global Positioning System (GPS) data, speed of walking etc.) from the recovered data, and an effective approach for recovering deleted data from android fitness tracking mobile applications.

Kitsaki et al. (2018) performed a forensic investigation on a set of android mobile applications that related to banking, mobile network carrier, and public transport categories. The researchers utilized two techniques: cod and disk analysis for the analysis process of applications. In the analysis phase of the study, they revealed that the e-banking application stores the user's Personal Identification Number (PIN) in plain text or using a static key. Mobile network carriers and public transport applications store user-sensitive information such as username, password, credit cardholder's name, credit card number, etc. in unencrypted format. Thus, this research revealed that the set of applications is unable to provide the required security to ensure the protection of user-sensitive data which leads to a violation of user privacy.

2.3 Financial Applications

Unlike the other mobile applications, most finance applications provide adequate security for user-sensitive information. Zhang et al. (2017) presented a forensic analysis of 18 android vault applications by exploring data remnants and performing reverse engineering. Out of the 18 applications, 12 apps obfuscated their code while 5 apps employed local libraries to impend reverse engineering. Although, the authors managed to retrieve data from 10 applications without root access to the smartphone. According to the data recovered, 6 vault applications stored photos without encryption, 8 apps stored videos without encryption and 7 apps stored passwords in cleartext. Even though the developers code their applications to protect from reverse engineering techniques, the researchers were able to recover hidden evidence that aid in the restoration of media files that are related to a court case.

A similar effort has been made by Duncan & Karabiyik (2018), to identify the installed vault applications on an android device and recover the hidden files of android vault applications. To accomplish this goal, they proposed an efficient vault application detection system for android devices and tested it on six different android versions running on six unique devices. The research was performed under five phases: scenario creation, list creation, device analysis, program creation, and program testing. The observations of this research revealed a comprehensive list of installed vault applications in android smartphones and unencrypted images, and hidden files uploaded to the applications by users.

Likewise, Gilbert & Seigfried-Spellar (2022) analysed five iOS photo vault applications: KeepSafe, Calculator +, Photo Vault, Secret Safe, and Purple Photo Vault to evaluate the artefacts that can be retrieved forensically and innovate new techniques to recover data remnants. Using three forensic tools: Magnet Axiom, Universal Forensic Extraction Device (UFED) Cellebrite, and Black bag Mobilyze they analysed the vault applications and examined similar results from the three tools. The project results demonstrated that each app left evidence and photos behind as these vaults are not providing asserted security for user-sensitive data. Other than this evidence, the Cellebrite tool was able to discover the PIN number

of the Photo vault, which was verified as the PIN to unlock the phone.
Furthermore, a forensic analysis of mobile banking applications in Nigeria was carried out by Uduimoh et al. (2019) to identify the amount of user data created and maintained by the applications upon registration and utilization. In this research, they used UFED Touch and Forensic Recovery of Evidence Device (FRED) tools to recover the data artefacts of the applications. Analysis results of the project revealed that user-sensitive data such as account number, account balance, cash transfer details, login credentials, and transaction details were found in the unencrypted form inside the local memory of the mobile applications which helps to identify the transactions and other user activities performed by the user.

The previous work carried out by digital forensic practitioners and academic researchers empowered the identification of a research gap that this study pursues to fill. In this study, the recovery of data remnants of three popular credit scoring mobile applications, namely Clear Score, Experian, and Credit Karma on Android and iOS platforms will be forensically analysed to fill a critical, existing research gap in mobile forensics. The information gathered from previous studies greatly contributed to creating the methodology outline and identifying the tools required to achieve the objectives and final goal of the project. Thus, the experimental implementation, data acquisition, and data analysis approach will abide by the related studies. Unlike the previous research areas, this study is exploring forensically meticulous evidence in both android and iOS platforms and offers a comprehensive comparison of remnants among different credit scoring applications and platforms while evolving forensics attention to credit scoring mobile applications as there are no research papers on this topic.

Chapter 3

Experimental Methodology

This research adopts the quantitative research approach to accomplish the objectives of the study. The data collecting and analysis process of this study was carried out using categorical and numerical variables for the identification of correlations. The experimental methodology outline was as follows:

- Perform a factory reset and wiped all data on mobile devices.
- Install the three selected credit scoring applications on both devices.
- Create frictional user accounts in each application.
- The population of data in each user account.
- Root and jailbreak the Android and iOS mobile devices respectively.
- Perform a full data acquisition on both devices individually.
- Uninstall the applications from both devices.
- Perform the second data acquisition process on both devices individually.
- Identify the data remnant folders and their paths.

- Analyse and compare the results between the applications and platforms.

This experimental setup was carried out under five phases: selection of applications, setting devices and applications, identifying and classifying default security features of applications, data acquisition, and analysis of data remnants. The five phases are discussed further in the next section.

3.1 Selection of applications

With the aid of the quantitative approach, a set of credit scoring mobile applications was selected (figure 3.1 and figure 3.2) based on the following facts:

1. Apps with the highest number of downloads / top ranking applications
2. Have very good ratings/ number of reviews
3. Free to download and install from Google Play Store and Apple Store.

The set of selected credit scoring applications are:

1. Clear Score,
2. Experian,
3. Credit Karma

The selected applications have more than 19,000 reviews and 1 million plus downloads in Google Play Store (Table 3.1). Unlike the Play store, the Apple App store does not provide the number of downloads of these applications, so the selected applications were compared with the rankings of the Similarweb website that listed the top-ranking financial applications of the App store (Similarweb, 2022).

	Google Play Store			Apple App Store		
Application Name	Number of down-loads	Number of reviews	Ratings	Ranking on App Store (among finance apps)	Number of reviews	Ratings
Clear Score	1M +	59,409	4.5	18	63,795	4.8
Experian	1M +	19,529	4.6	20	162,331	4.9
Credit Karma	1M +	40,216	4.6	27	19,195	4.8
Money su-permarket	500K+	11,310	4.7	91	25,915	4.8
Totally money	100K+	2,681	4.6	61	4,019	4.7
Pave - build credit	100K+	1,565	4.1	184	3343	4.7

Table 3.1: Facts considered for the selection of credit scoring applications

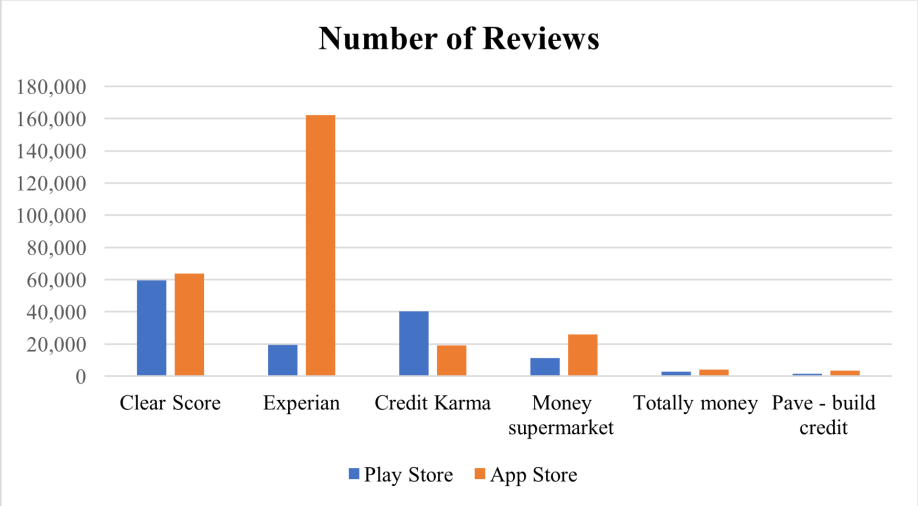

Figure 3.1: Number of reviews of popular credit scoring applications on android and iOS

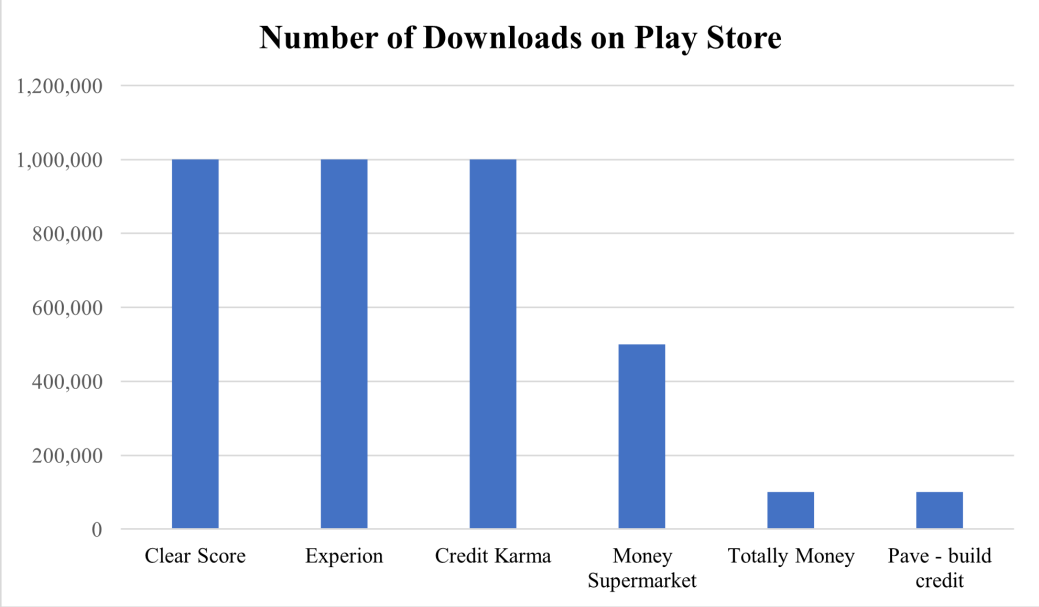

Figure 3.2: Number of downloads of popular credit scoring applications on the Play Store

3.2 Setting devices and applications

In this study, we use the OnePlus 6 android smartphone with Android version 11.0 and iPhone 13 Pro Max with iOS version 15.6.1. First, a factory reset was performed on both devices to switch on the factory settings. After, the devices were wiped to remove the unnecessary data available in the devices. The ClearScore, Experian, and Credit Karma credit scoring applications were then downloaded from the Google Play store and Apple App store in August 2022 and installed on both smartphones (figures 3.3, 3.4, and 3.5). New frictional user accounts were created in the set of applications on both devices using frictional data. All the tools necessary for the methodology were identified as shown in table 3.2 and then downloaded and installed accordingly.

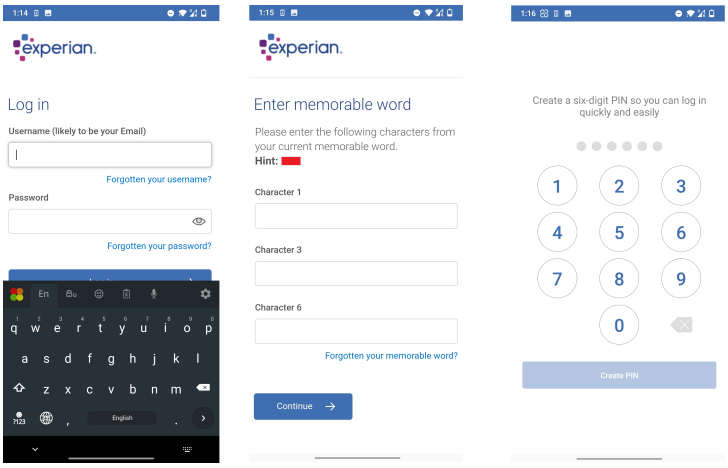

Figure 3.3: Login page, memorable word creation page, and PIN creation page of the Experian app

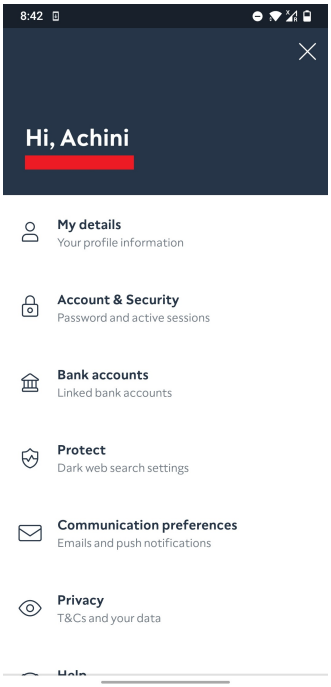

Figure 3.4: Account created in ClearScore application

As most of the data files are inaccessible by default, it is required to have root access on android mobile devices to acquire the data evidence expected for the analysis process. The newer versions of the Android operating system are unable to root with most of the rooting software and the older versions (lower versions than

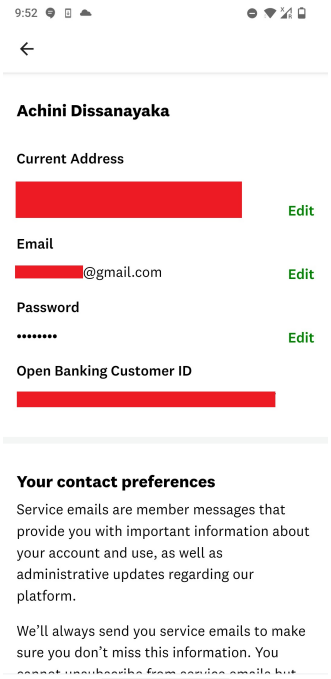

Figure 3.5: Account created in Credit Karma application.

v 22.0) of the Magisk rooting software. Thus, the android mobile phone used in this experimental setup (OnePlus 6 with firmware 11.0) was rooted using Magisk version 25.2 and Team Win Recovery Project (TWRP) v 3.6.2 (enchilada) software in order to acquire privileged access over the operating system by evading the restrictions employed by the phone manufacturer. The process utilised for rooting the android device was adopted from the "GIZMOCHINA" blog by the author Simranpal Singh (Singh, 2019).

In this study, the iOS mobile device was jailbroken using uncover++ software and gained root access to privileged files and folders of the iPhone 13 Pro Max (Lee, 2022).

Tool	Version	Details
Android smartphone	OnePlus 6 Firmware version 11.0	Android mobile device used to install the credit scoring applications
Apple smartphone	iPhone 13 Pro Max Firmware version 15.6.1	iOS mobile device used to install the credit scoring applications
DB Browser for SQLite	V 3.12.2	For viewing the SQLite database files
Magisk	V 25.0	For rooting the android device
TWRP	V 3.6.2 (enchilada)	For the Recovery purposes
AccessData FTK Imager	V 4.5.0.3	For the analysis of evidence
Magnet Axiom Process	V 4.10.0.23663	For data acquisition
Magnet Axiom Examine	V 4.10.0.23663	For the analysis of evidence
HxD	V 2.5.0.0	For the analysis of evidence
Uncover++	-	For jailbreaking the iPhone.
Credit Karma	V 22.27 (android) / V 22.35 (iOS)	Credit scoring app 2
Experian	V 5.41.0	Credit scoring app 3

Table 3.2: Tools used to carry out the methodology

Security Feature	ClearScore	Experian	Credit Karma
Verify email address	✔	✔	✔
Biometrics login (Fingerprint ID)	✔	✔	✔
Auto logout option	✔(Can select time)	✔	✔
Screenshots disabled	Can enable or disable using the feature 'Hide ClearScore'	✔	X
Two-factor authentication	✔	X	X
Log out other devices	✔	X	X
Change app login pin or password	✔	✔	✔
Hide content after minimising the app	Only if the 'Hide ClearScore' function is enabled.	✔	X
Link bank accounts	✔(Via the app)	X	✔(Via the browser)
Phone number validation	X	X	✔

Table 3.3: Classified default security features of the selected credit scoring applications on the Android platform

3.3 Identifying and classifying default security features of applications

In this phase, default security features of the credit scoring applications on both operating systems were checked and classified as shown in tables 3.3 and 3.4 . The purpose of this phase is to identify whether the default security provided by each application is providing adequate and fundamental protection for the data privacy of the end users of each application (see figures 3.6, 3.7, 3.8, 3.9, 3.11 and 3.10).

Security Feature	ClearScore	Experian	Credit Karma
Verify email address	✔	✔	✔
FaceID login	✔	✔	✔
Auto logout option	✔	✔	✔
Screenshots disabled	X	X	X
Two-factor authentication	✔	X	X
Log out other devices	✔	X	X
Change app login pin or password	✔	✔	✔
Hide content after minimising the app	✔	✔	✔
Link bank accounts	✔(Via the app)	X	✔(Via the browser)
Phone number validation	X	X	✔

Table 3.4: Classified default security features of the selected credit scoring applications on the iOS platform

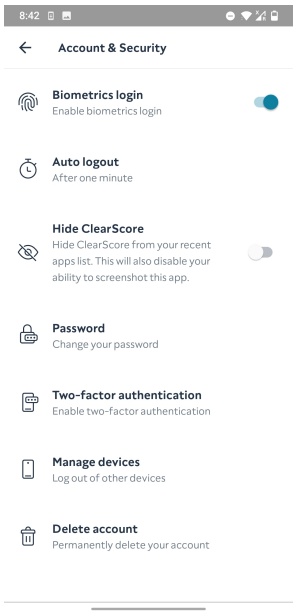

Figure 3.6: ClearScore android app security settings

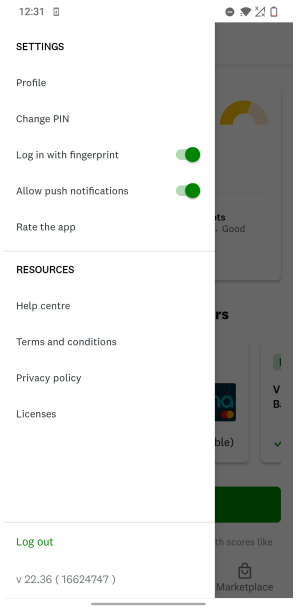

Figure 3.7: Credit Karma android app security settings

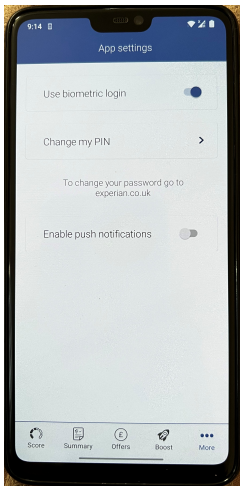

Figure 3.8: Experian android app security settings

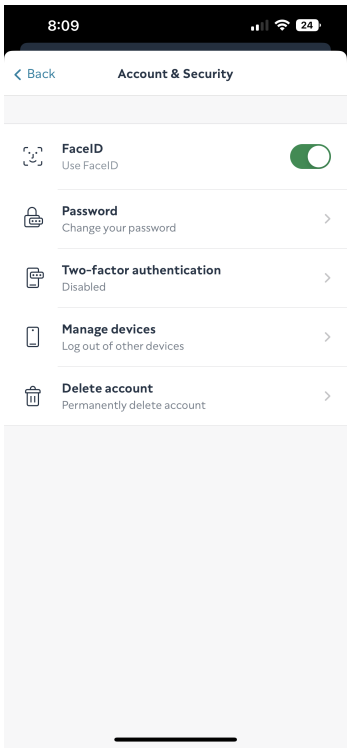

Figure 3.9: ClearScore iOS app security settings

3.4 Data acquisition

The fourth phase of the methodology includes full data acquisition (logical acquisition) from both smartphones. In mobile forensic investigations, this is the

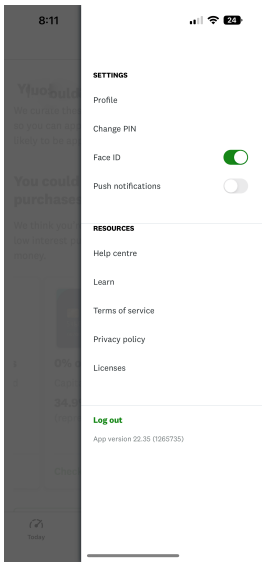

Figure 3.10: Credit Karma iOS app security settings

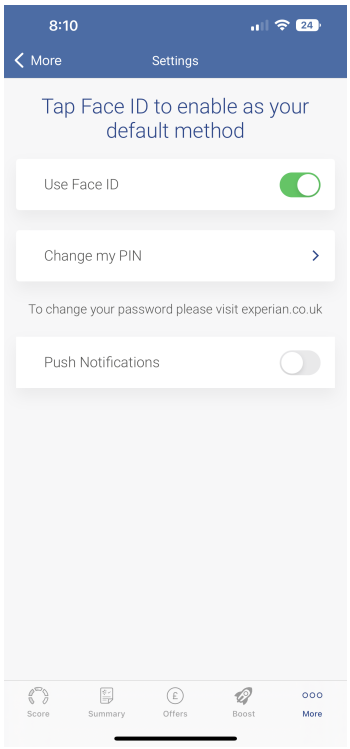

Figure 3.11: Experian iOS app security settings

most significant phase as the hash values generated in this process are very crucial for court cases. Once the frictional accounts are created, the required directories *(\data\data\...* and *\private\var\...)* for the data analysis process were backed up using Magnet AXIOM Process software. To obtain the data evidence upon the uninstallation of applications, a second backup was taken after the uninstallation of the three applications by adopting the same approach on both smartphone devices. The four logical acquisition images (before Android, after Android, before iOS, after iOS) were obtained in .zip format. In the next phase of the methodology, the in-depth analysis of these logical images is discussed.

3.5 Analysis of data remnants

In this phase, the data captured from the credit scoring applications at two stages; after creating frictional user accounts in credit scoring applications and after uninstalling credit scoring apps were examined and analysed to determine the paths of files in which the data remnants available on both devices.
The analysis process on both operating systems was the same and it consists of three stages as mentioned below:

1. Data evidence of the three credit scoring applications including the user ID, login credentials, user activities, address, phone number, email address, and other information necessary for this project were gathered with the aid of three forensic tools: Magnet Axiom Examine, AccessData FTKImager, and HxD to explore the full data images acquired in the previous phase.
2. Identifying the security and privacy concerns of all the applications from the perspective of the end-user.
3. Recovering the most significant data evidence for digital forensic purposes.

For the minimalism of the analysis process both manual and automated techniques of the Magnet Axiom Examine software were utilised. As some of the data were

not fully recoverable using one tool, AccessData FTKImager and HxD tools were also used for the examination of data remnants of all the applications one by one separately.

Figures 3.12 and 3.13 show the folders of the three credit scoring applications that require privilege (root) permission to access. The package names and package paths of the three applications on both platforms were identified as illustrated in tables 3.5, 3.6, and 3.7.

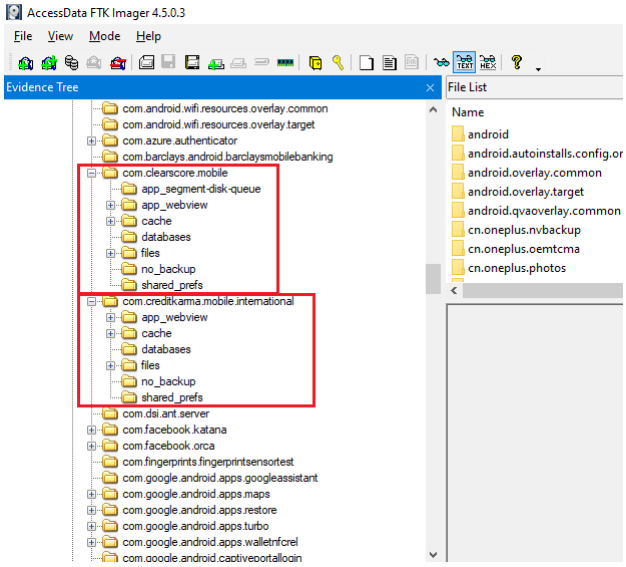

Figure 3.12: Acquired directories of ClearScore and Credit Karma applications

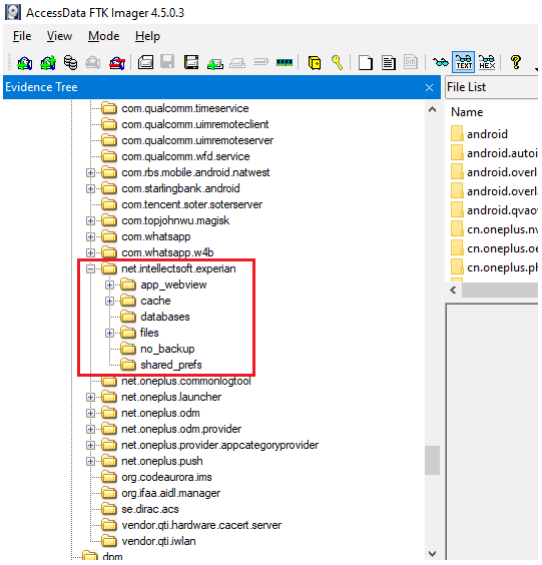

Figure 3.13: Acquired directories of Experian before uninstalling the application

Application	Package name in Android	Package name in iOS
ClearScore	com.clearscore.mobile	com.clearscore.wrapper
Experian	net.intellectsoft.experian	uk.co.creditexpert.companion
Credit Karma	com.creditkarma.mobile.international	com.creditkarma.canada

Table 3.5: Package names of the three applications on iOS and Android platforms

Application	Location of application package
ClearScore	\data\data\com.clearscore.mobile
Experian	\data\data\net.intellectsoft.experian
Credit Karma	\data\data\com.creditkarma.mobile.international

Table 3.6: Package path of Android mobile device

Application	Locations of application package
ClearScore	\private\var\mobile\Containers\Data\Application\C349C761-1CB3-49C4-8C38-C52410ED3E9E\ \private\var\mobile\Containers\Shared\AppGroup\DDA5A35D-95C3-457F-A46F-A3844A55A320\
Experian	\private\var\mobile\Containers\Data\Application\73CC5371-147C-4508-B499-BF1C0AA9A87C\ \private\var\mobile\Containers\Shared\AppGroup\C84C3967-00D6-40B8-9E94-F2847D3AE6FA\textbackslash
Credit Karma	\private\var\mobile\Containers\Data\Application\AA8049B8-39BE-11ED-BEF8-FBD6B86E8750\ \private\var\mobile\Containers\Shared\AppGroup\C036639C-39BD-11ED-981B-F7CA77472ACE\

Table 3.7: Package paths of iOS mobile device

Chapter 4

Experimental Results

Upon the completion of digital forensic analysis of credit scoring mobile applications on both Android and iOS operating systems, a significant amount of data remnants that would lead to a security breach were discovered. In this chapter, the findings of all the applications are presented separately.

4.1 ClearScore in Android

Data remnants of the Clearscore android application such as the user's activity timestamps, the package name of the app, the user's email address, user ID, and the first time the application was opened were gathered from several locations of the internal storage. Most of the evidence related to the Clearscore was found in the path *\data\data\com.clearscore.mobile\shared_prefs*. As shown in figure 4.1, the file *com.clearscore.mobile.ClearScorePreferences.xml* holds default security features provided by the application. Figure 4.2 shows the package name of the Clearscore app.
The user's activity timestamps were able to discover from the file *info.xml*, while the user's email address and user ID were recovered from the

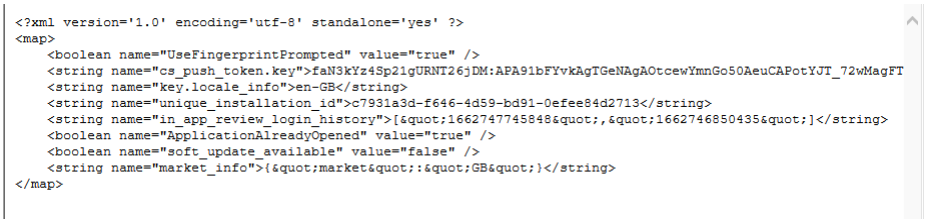

Figure 4.1: Default security features of ClearScore android app

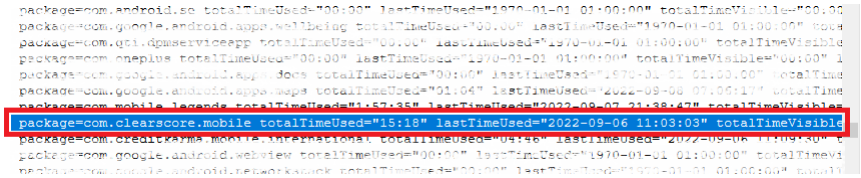

Figure 4.2: Package name last used date and time of the application

com.clearscore.mobile.user_info_file.xml file in the same location as above (see figures 4.3 and 4.4 respectively). Application details such as the first time the application was opened, and the last pause time were discovered in Unix Epoch format 1662738311822 from the file *com.google.android.gms.measurement.prefs.xml* (figure 4.5). The timestamps were then decoded into an understandable format using the DCode software that we mentioned in the table1. Thus, these times were converted into a human-understandable format as in figure 4.6.

The first time the application opened (1662738311822)
Friday, 09 September 2022 15:45:11 (UTC+00:00)

The last pause time of the app (1662749661957)
Friday, 09 September 2022 18:54:21 (UTC+00:00).

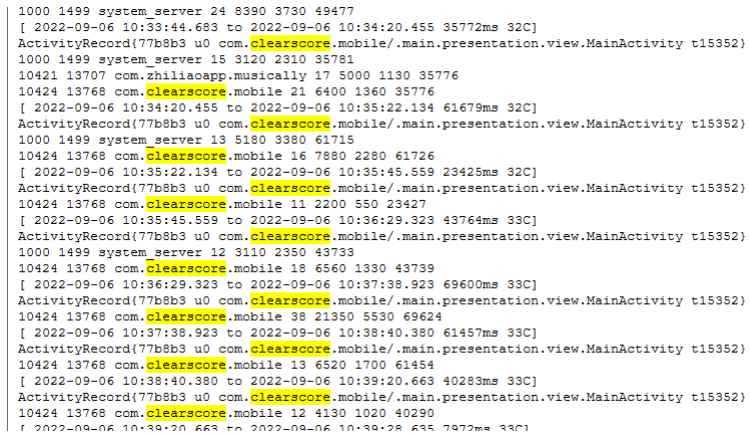

Figure 4.3: User's activity timestamp

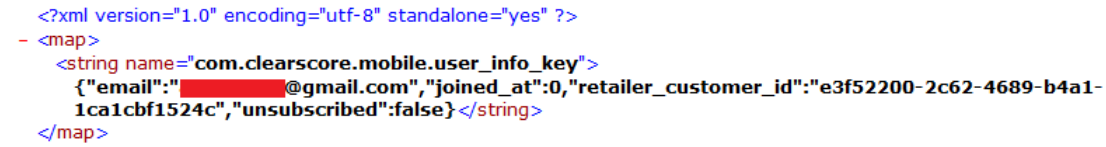

Figure 4.4: The email address customer-id

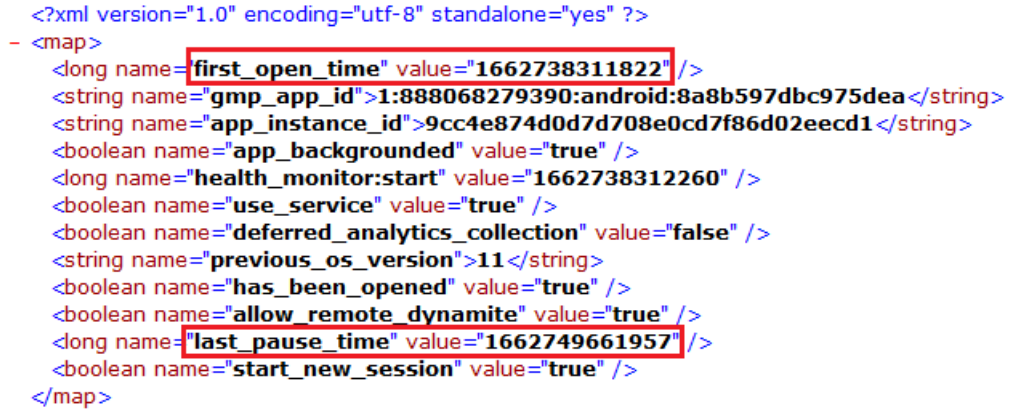

Figure 4.5: Application details (First open date of the app, etc)

In the file named *app_installed.xml*, the application's installed version was mentioned as shown in figure 4.7. The fingerprint id of the end user, installation date of the application, and numerous information related to the application were revealed from the file *branch_referral_shared_pref.xml* (figure 4.8).

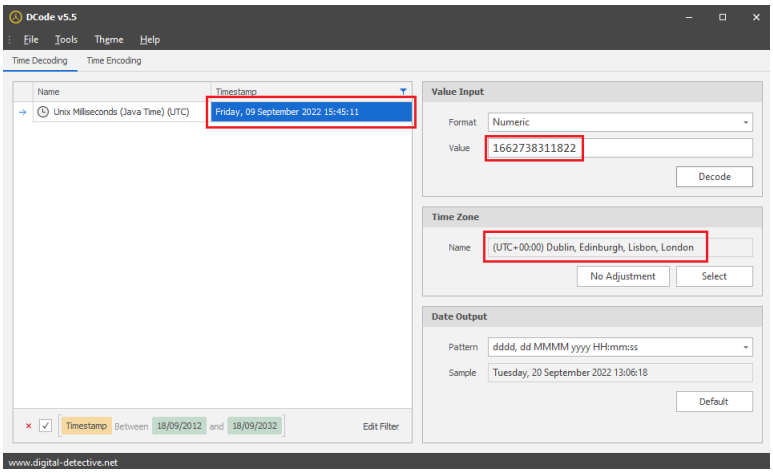

Figure 4.6: Conversion of first open date of the clearscore application in Unix Epoch format to a readable format

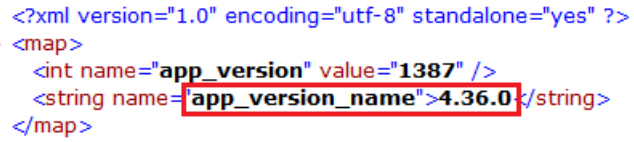

Figure 4.7: Version of the application

The full address of the end-user was also discovered from the file *\data\data\com.clearscore.mobile\app_webview\Default\Session Storage\000016.ldb*. This address consists of the following information (see figure 4.9).

- Flat / House number
- Road Name
- City
- County
- Postal Code

In this study, a bank account was connected with the ClearScore application to identify if any data remnants are there inside the internal storage as it has a high risk of

Figure 4.8: Install date, fingerprint ID and other info

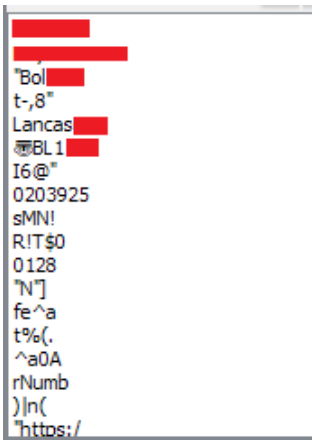

Figure 4.9: Address of the user

a security breach. The bank account connected to the user account was partially exposed from the file *\data\data\net.oneplus.launcher\databases\hidden_apps.db*, however the critical information related to the bank account was not recoverable (figure 4.10).

Figure 4.10: Banks connected with the credit scoring app

Furthermore, the email notifications of the ClearScore application were retrieved

from the file *\data\data\com.google.android.gm\databases\bigTopDataDB.-45848498-wal* using the Magnet Axiom software as shown in figure 4.11.

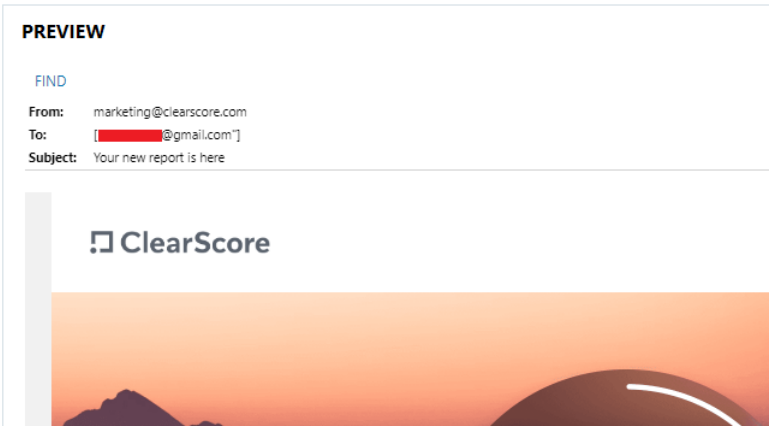

Figure 4.11: ClearScore emails recovered from the bigTopDataDB.-45848498-wal file

After uninstalling the Clearscore android application, the email address of the user was able to be discovered from the database file *\data\data\com.android.vending\databases\localappstate.db* as in figure 4.12. The email address of the user was also recovered from the *\data\data\com.android.vending\cache\streamdatastore\streamdatastore.db* database file.

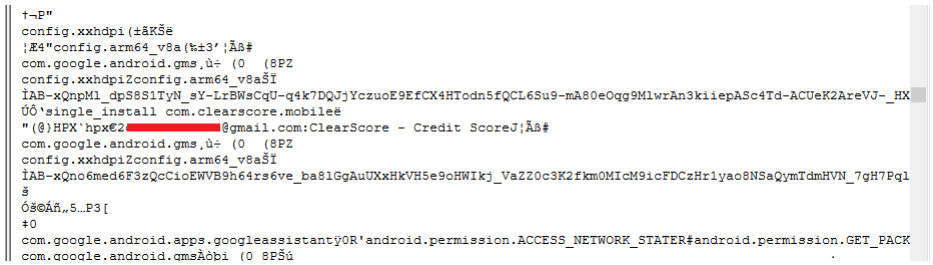

Figure 4.12: Email address recovered after uninstalling the Clear Score android application

4.2 ClearScore in iOS

A limited number of data remnants were discovered from the iOS application of ClearScore credit scoring app. The application's package name was able to recover from a plist file which is located in *private**var**mobile**Containers**Data*\\ *Application**C349C761-1CB3-49C4-8C38-C52410ED3E9E*\\ as shown in figure 4.13. Most of the information of this application was discovered from the location *private**var**mobile**Containers**Shared**AppGroup**DDA5A35D-95C3-457F-A46F-A3844A55A320*\\. The user's name, ID, email address, installed date and the last accessed date of the application were recovered from the database file *ClearScoreDb.* (figure 4.14). As the last accessed timestamp and the app's installed timestamps were in Unix Epoch format, the DCode software was utilised to convert them into a readable format. Therefore, the app's installed date and last access date are Friday, 09 September 2022 15:43:24 (UTC+00:00), and Tuesday, 13 September 2022 13:52:33 (UTC+00:00) respectively. Moreover, the table in the *Cache.db* database file at the location *Library**Caches**com.clearscore.wrapper*\\ consists of similar data as the *ClearScoreDb.sqlite* database. The email notifications received from the Clearscore application were retrieved from a plist file at \\Documents\\Emails using the Magnet Axiom tool (see figure 4.15).

Figure 4.13: Package name of ClearScore iOS application

ZINSTALLEDTIMESTAMP	ZNAME	ZUSERID	ZEMAIL	ZLASTUSEDDATE
Filter	Filter	Filter	Filter	Filter
1662738204211	Achini	20368941728...	[redacted]@gmail.com	1663077153000

Figure 4.14: User's name, email address, user ID, last accessed time to the application, and the application's installed time

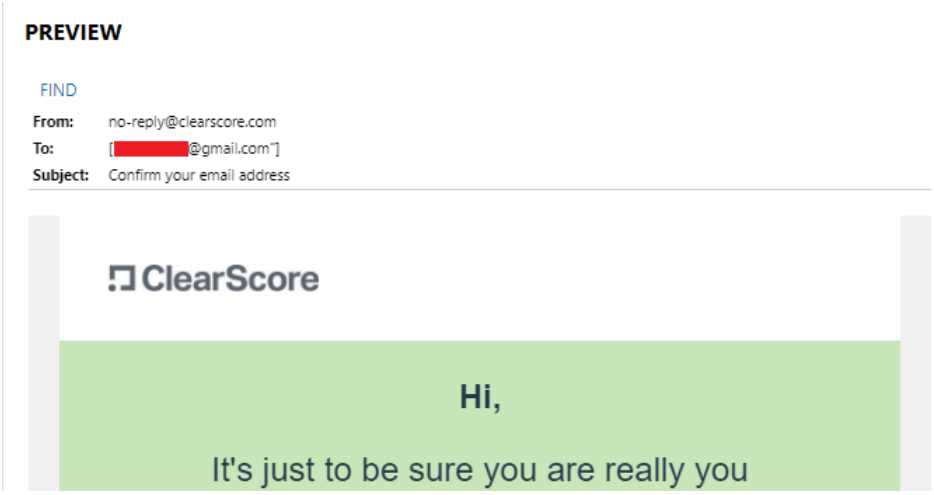

Figure 4.15: Recovered notifications received from the ClearScore

After uninstalling the Clearscore iOS application, a database file was detected with the email address of the user in the \Library\Preferences\directory as shown in figure 4.16.

id	account_name	data
clearscore	Filter	Filter
com.clearscore.wrapper	[redacted]@gmail.com	BLOB

Figure 4.16: Email address found after uninstalling the application

4.3 Credit Karma in Android

After analysing the Credit Karma Android application, a number of crucial data remnants including the package name of the application, user's activity timestamp, country code, Universally Unique Identifier (UUID) key of the app, first open date

of the app, last accessed date of the app, user ID, and the device fingerprint ID were recovered from the files in the location *\data\data\com.creditkarma.mobile.international\shared_prefs*. The end user's activity timestamp was discovered from the info.xml file (see figure 4.17). Figure 4.18 illustrates the package name and the last accessed time of the application. Moreover, the default security features of the application such as bio code, etc were found inside the *CREDITKARMA_USER_DATA.xml* file as illustrated in figure 4.19. Furthermore, the UUID key of the app and the country code of the user were discovered in the *CREDITKARMA_APP_DATA.xml* file (figure 4.20).
Additionally, the application's first open date, last accessed date, last pause time, user ID, and device fingerprint ID were also recovered from the file *com.google.android.gms.measurement.prefs.xml* at the same location as above (see figures 4.21, 4.22, 4.23, and 4.24). As the first open time of the application is in Unix Epoch format, it was converted into an understandable format: Friday, 09 September 2022 15:47:41 (UTC+00:00).

```
.000 1499 system_server 18 7990 4610 68472
: 2022-09-06 11:04:47.135 to 2022-09-06 11:05:47.154 60019ms 35C]
ctivityRecord{efa7e80 u0 com.creditkarma.mobile.international/.webview.ui.WebViewActivity t15358}
.000 1150 surfaceflinger 12 4500 3070 59971
.0438 1327 com.creditkarma.mobile.international 35 16470 4960 59968
.000 1499 system_server 16 6960 3020 59965
: 2022-09-06 11:05:47.154 to 2022-09-06 11:06:19.847 32693ms 35C]
ctivityRecord{efa7e80 u0 com.creditkarma.mobile.international/.webview.ui.WebViewActivity t15358}
.0438 1327 com.creditkarma.mobile.international 30 7680 2370 32731
.000 1499 system_server 13 2470 1790 32734
9670 28224 com.google.android.webview:sandboxed_process0:org.chromium.content.app.SandboxedProcessService0:0 5
: 2022-09-06 11:06:19.847 to 2022-09-06 11:08:02.932 103085ms 34C]
ctivityRecord{78e72f8 u0 com.creditkarma.mobile.international/.webview.ui.WebViewActivity t15358}
.000 1150 surfaceflinger 13 8450 5770 103091
.0438 1327 com.creditkarma.mobile.international 35 28130 8620 103092
9670 28224 com.google.android.webview:sandboxed_process0:org.chromium.content.app.SandboxedProcessService0:0 3
: 2022-09-06 11:08:02.932 to 2022-09-06 11:09:22.124 79192ms 34C]
ctivityRecord{c1596ff u0 com.creditkarma.mobile.international/.webview.ui.WebViewActivity t15358}
.0438 1327 com.creditkarma.mobile.international 24 15210 4390 79177
9670 28224 com.google.android.webview:sandboxed_process0:org.chromium.content.app.SandboxedProcessService0:0 1
: 2022-09-06 11:09:22.124 to 2022-09-06 11:09:32.693 10569ms 34C]
```

Figure 4.17: User's activity timestamp

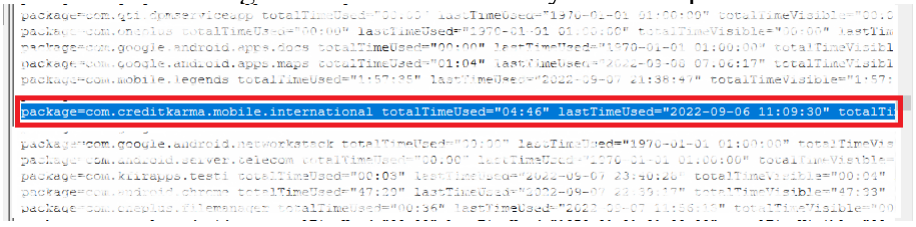

Figure 4.18: Package name

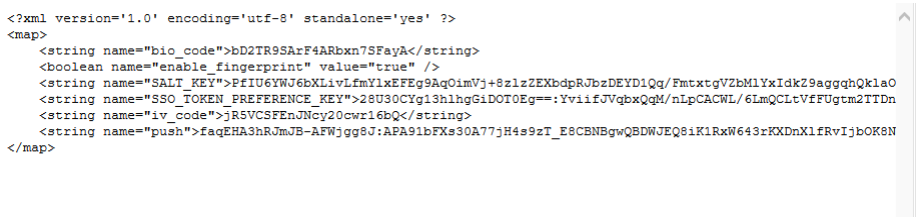

Figure 4.19: Default security features of the application

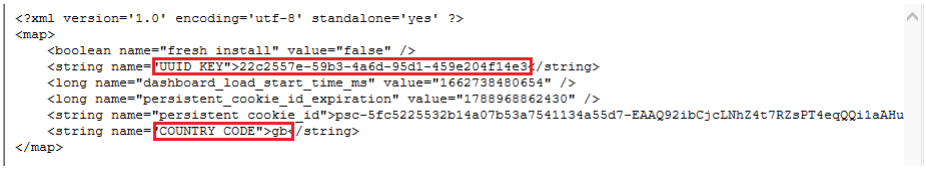

Figure 4.20: The UUID key and the country code of the end user

Figure 4.21: The fingerprint ID of the device

The email address of the user was discovered from a previous login session stored in the *\data\data\com.android.chrome\app_chrome\Default\Login Data* file as shown in figure 4.25. Figure 4.26 reveals the credit information of a transaction which performed before installing the application, and it was retrieved from the file *\data\data\com.android.chrome\app_chrome\Default\History*.

Upon the uninstallation of the Credit Karma Android application, all except the email address were unable to recover from the files left over inside the internal storage of the smartphone device (see figure 4.27). The email address was found inside

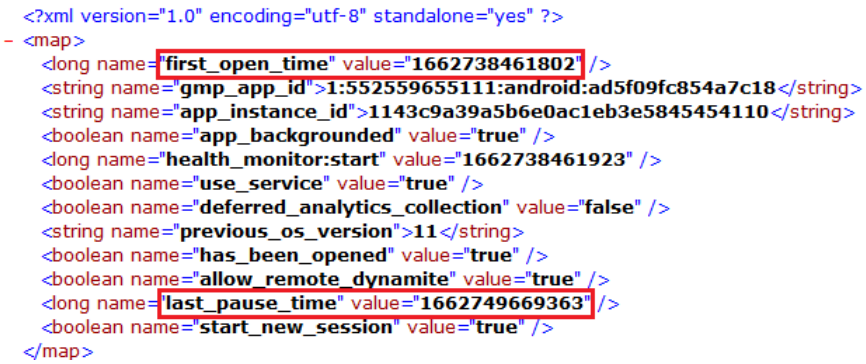

Figure 4.22: The first open date of the application in Unix Epoch format

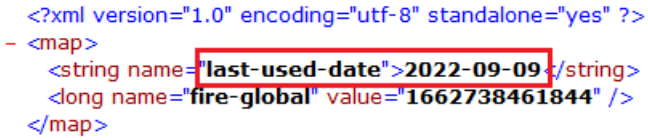

Figure 4.23: Last access date of the application in a readable format

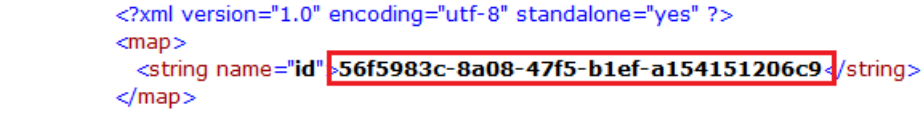

Figure 4.24: The user ID recovered

Figure 4.25: The email address identified from a previous login session

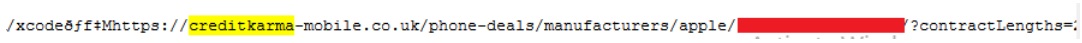

Figure 4.26: User's credit details related to a contract

the *localappstate.db* database file at *data**data**com.android.vending**databases*\ folder. Moreover, the table in the *streamdatastore.db* database file at the location *data**data**com.android.vending**cache**streamdatastore*\ also consists of the user email address.

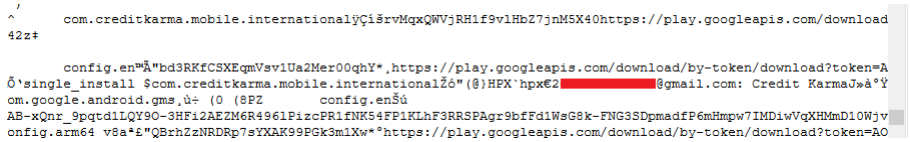

Figure 4.27: The email address recovered after uninstalling the Credit Karma Android application

4.4 Credit Karma in iOS

The package name of the Credit Karma iOS application was discovered from a plist file at *\private\var\mobile\Containers\Data\Application\AA8049B8-39BE-11ED-BEF8-FBD6B86E8750* as shown in figure 4.28. For this application, most of the data remnants were examined from the database file *\private\var\mobile\Containers\Shared\AppGroup\C036639C-39BD-11ED-981B-F7CA77472ACE\creditkarma.sqlite*. Using the aforementioned database file, several pieces of data evidence were recovered including the user's first name, user ID, email address, phone number, installed date of the application, and last accessed date of the app (see figure 4.29). The table in the Cache.db database file at the location *\Library\Caches\com.creditkarma.canada* consists of similar data as the *creditkarma.sqlite database*. Furthermore, the end user's phone number was also recovered from the *com.creditkarma.canada.plist* file at *\Library\Preferences*.

After uninstalling the iOS Credit Karma application from the mobile device, a database file was recovered from the directory *\Library\Preferences* which contains the email address of the Credit Karma user's account as in figure 4.30.

4.5 Experian in Android

The data remnants retrieved from the Experian Android application include the package name (figure 4.31), user's name (figure 4.35), user ID, email address, installed date of the app, user's activity timestamps (figure 4.33), first and last ac-

```
</dict>
<key>com.creditkarma.canada</key>
- <dict>
    <key>ApplicationSINF</key>
    <data>AAAEIHNpbmYAAAAMZnJtYWdhbWUAAAAUc2NobQAAAABpdHVuAAAA
      AAAAA3BzY2hpAAAADHVzZXIg8CXAAAAADGNyZHTfP0/5AAAADGFz
      ZHQAAAAAAAAADGtleSAAAAACAAAAGGl2aXbnRFCGi+DqKPitkLop
      gDDEAAAAWHJpZ2h2ZUlEABD/MHBsYXQAAAACYXZlcgEBAQB0cmFu
      3z9P+XNpbmcAAAAAc29uZ1NcTcd0b29sUDYwNW1lZGkAAACAbW9k
      ZQAAIABoaTMyAAAABAAAAQhuYW1lU2hhbGl0aGEgRGVoaWdhc3Bp
      dGl5YWdlAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAcBwcml2HfA5YCYqOF4iQCO2nm9Mvu3IPwDRLIzVBDP4
      29haB09wkdOjvMF239uDUQQB2sDk5kesoCeXiKnOdhwwDS2GmPdg
      sxgluJEkHWWmxVCupOjpLzU/Mbg5zvA0jlFyBO415VUgjGNNt8BU
      oslrJF3yx7L8brb6Ef5RPh4IjHG3fyJGTMM4BETaASFv3tuG+4GU
      olPzZ8dtxVWBLS/EzdkzZ55hTfyeiNnzPMP3uqMyDZFXjgE2n8ya
      R6tw9+yVNKdGibYkY0cwS0Ygco/Rh4i24/55trqivcNv3RfUY1j3
      SEAI93P/5rB5Iji/+o7tbkmvfsjRUiHiByvZxqbms7NroA3Ibdc0
      g3MjM/lHKZUxH3nQ1la73H6138OmoPiOsmlpa/OAtsPSMwru9/5b
      zpCaAXFjxrGbkPC2f0pkkZyN/GXQDc9r/u+eRXhfJGB0hQzhEbwq
      2ZRR2H3IBFdFnrfDf1Gkb8q7oIQqNQ8v2smI9cpxroMvqtHaDHK0
      4GVtsPmaZxqAb/4J/4/LETSj8/Rx39ApvuAvOUE/SlO+Ip/62bU5
```


Figure 4.28: Package name of the iOS Credit Karma application

ZFIRSTNAME	ZCKUSERID	ZINSTALLEDDATE	ZEMAIL	ZPHONENUMBER	ZLASTACCESSEDDATE
Filter	Filter	Filter	Filter	Filter	Filter
Achini	54137345442...	1662738305168	[redacted]@gmail.com	+44756138[redacted]	1662880935000

Figure 4.29: User's first name, user ID, email address, phone number, installed date of the application and the last accessed date of the app

cessed time of the app, email notifications of the application, encrypted installation date of the application (figure 4.34), user's credit score, etc. The majority of these data were discovered from the path *data**data**net.intellectsoft.experian*\ *shared_prefs*\.

The email notifications (see figures 4.35, and 4.36) of the application were found in the file *data**data**com.google.android.gm**databases**bigTopDataDB.-45848498-wal*. The user's name was examined from these email notifications.

The first open date and last pause time of the app was also found from the file *com.google.android.gms.measurement.prefs.xml* as shown in figure 4.37. As the first open date and last pause time of the application were in Unix Epoch format, it

id ▲1	account_name	data
creditkarma	Filter	Filter
com.creditkarma.canada	[redacted]@gmail.com	BLOB

Figure 4.30: Email address recovered after uninstallation of the Credit Karma iOS application

was converted into an understandable format.

The first open date of the application – 1662738376835

Friday, 09 September 2022 15:46:16 (UTC+00:00)

The last pause time – 1662749655805

Friday, 09 September 2022 18:54:15 (UTC+00:00)

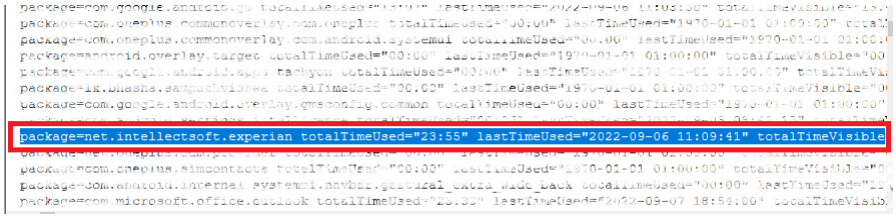

Figure 4.31: Package name and the last accessed time of the application

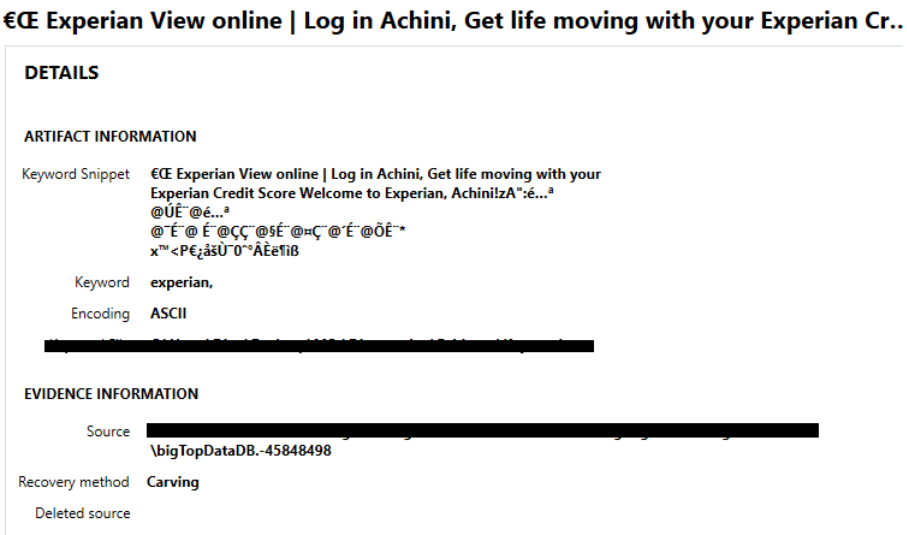

Figure 4.32: Email notifications recovered from bigTopDataDB.-45848498-wal file

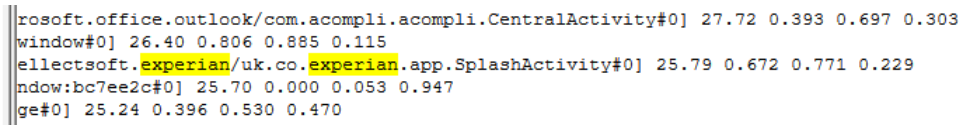

Figure 4.33: Recovered user ID, credit score, etc

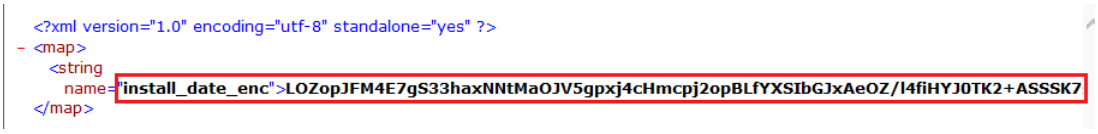

Figure 4.34: Encrypted installed date of the app

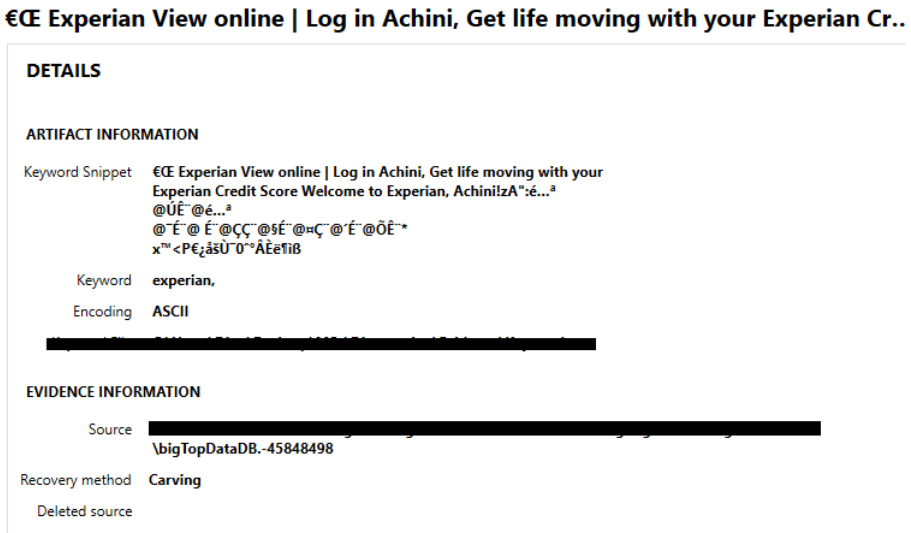

Figure 4.35: Email notifications recovered from bigTopDataDB.-45848498-wal file

Unlike the other applications investigated in this study, the credit score and the score band of the user were discovered from the Experian Android application (see figure 4.38). Figure 4.39 shows the credit score, and score band displayed in the Android Experian application. Besides the credit score related information, basic information related to the user account such as account type, user ID, etc were also recovered from the *\data\data\net.intellectsoft.experian\shared_prefs\com.mixpanel.android.mpmetrics.MixpanelAPI_42dd5abbff6e197dd27b1291a27476ed* file.
Once the Experian app was uninstalled from the android device, only the email

Figure 4.36: An email notification of the Experian application

```
<?xml version="1.0" encoding="utf-8" standalone="yes" ?>
- <map>
    <boolean name="measurement_enabled_from_api" value="true" />
    <long name="first_open_time" value="1662738376835" />
    <string name="gmp_app_id">1:796790439969:android:e2e9e9e07af44162</string>
    <string name="app_instance_id">86900f213ec3a42c8874e846b7db07cc</string>
    <boolean name="app_backgrounded" value="true" />
    <long name="health_monitor:start" value="1662746373268" />
    <boolean name="use_service" value="true" />
    <boolean name="deferred_analytics_collection" value="true" />
    <boolean name="measurement_enabled" value="true" />
    <string name="previous_os_version">11</string>
    <boolean name="has_been_opened" value="true" />
    <boolean name="allow_remote_dynamite" value="true" />
    <long name="last_pause_time" value="1662749655805" />
    <boolean name="start_new_session" value="true" />
</map>
```

Figure 4.37: The first open date of the app

address of the user was examined in both of the database files *streamdatastore.db* and *localappstate.db* (in figure 4.40) at *data**data**com.android.vending**cache*\ *streamdatastore*\ and *data**data**com.android.vending**databases*\ locations respectively.

```
<?xml version="1.0" encoding="utf-8" standalone="yes" ?>
- <map>
    <boolean name="events_user_id_present" value="true" />
    <string name="people_distinct_id">7a280822-e31f-4e12-8b6e-d0057ddc8ed1</string>
    <string name="events_distinct_id">7a280822-e31f-4e12-8b6e-d0057ddc8ed1</string>
    <string
      name="push_id">f0tlw6ZUSIWXFmvV70yjq6:APA91bF35xcBybVQO8XyEjss1BO6DMUSyogbusTOmLYdRBzuFDn7hAjeW
      -fFYt1ZZHYxpUbddu-Y1YvL6lcmbPjYjHNIjZ3cYmrlojaG-s9fPTSgeXcEBAKfpVS4tVNmzqPc</string>
    <string name="anonymous_id">ca9e7720-4766-487f-b844-2aa9025c2932</string>
    <boolean name="had_persisted_distinct_id" value="false" />
    <string name="super_properties">{"mobile-app-incentive-test":"not-
      shown","account_type":"free","customer_number":"125671456646","marketplace-vertical-mortgages-
      android":"shown","boost_status":"signup","salesforce_migrated":"yes","offer":"offer022","mobile-app-
      applepay":"shown","score":829,"mobile-app-score-android":"shown","mobile-app-boost-
      android":"shown","mobile-upsell-free-trial-banner":"shown","mobile-upsell-payment":"native","mobile-app-
      new-contact-form-
      android":"shown","eligible_for_free_trial":"yes","boost_user":"false","score_band":"Fair","tenure":"1-
      7","boost_nearly_expired":false,"marketing_permission":"on","mobile-app-send-to-boost-page":"not-
      shown","mobile-app-googlepay":"not-shown","cl-access-mobile":"not-shown","marketplace-vertical-car-
      insurance-android":"shown","mobile-app-optimisation-tests":"shown","mobile-app-boost-expiry-
      banner":"not-shown","mobile-app-boost-display":"variant-tab","mobile-app-offers-vertical-car-
      finance":"not-shown","customer_id":"7a280822-e31f-4e12-8b6e-d0057ddc8ed1"}</string>
  </map>
```


Figure 4.38: Recovered user ID, credit score, etc

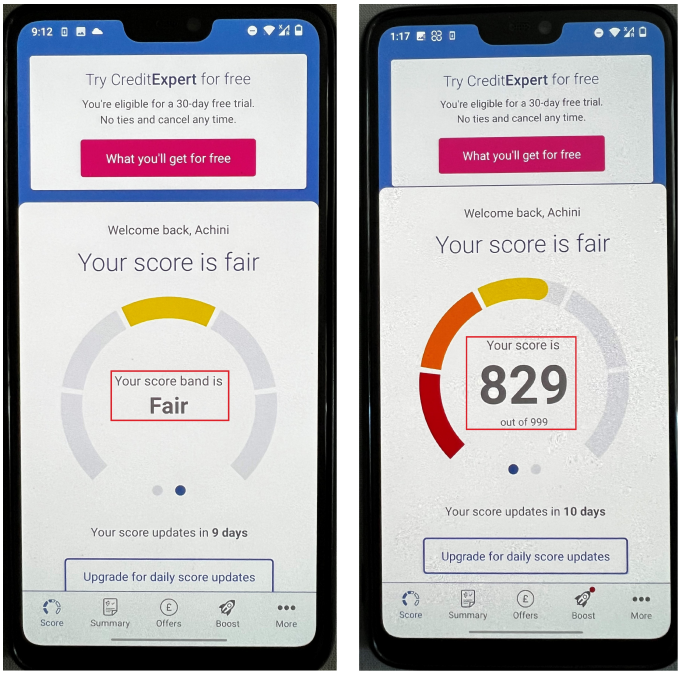

Figure 4.39: Generated credit score and score band of the user in the Android Experian app

4.6 Experian in iOS

In the iOS Experian application, most of the data evidence was stored in the *\private\var\mobile\Containers\Shared\AppGroup\C84C3967-00D6-40B8-9E94-F2847D3AE6FA*. The Experian app's package name was found in a plist file at the

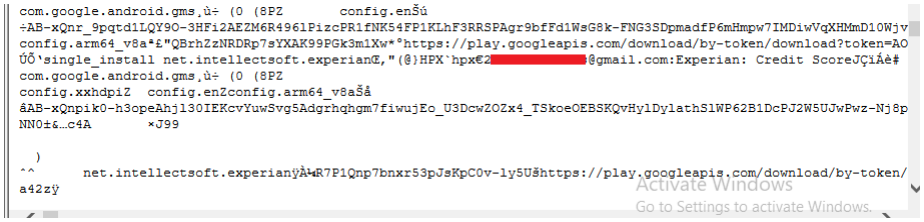

Figure 4.40: Email address found after uninstalling the app

location *private**var**mobile**Containers**Data**Application**73CC5371-147C-4508-B499-BF1C0AA9A87C*\ (see figure 4.41). The email and notification messages of the Experian app were examined from a plist file at *Documents**Emails* using the AccessData FTKImager and the Magnet Axiom tools as demonstrated in figures 4.42, 4.43, and 4.44. With the aid of these notification messages, the user's activities were able to be determined. Furthermore, the database file *creditexpert.sqlite* provided more information about the user ID, user's full name, email address, application installed timestamp, and last access timestamp (figure 4.45). Both these timestamps were in Unix Epoch format and were converted into the readable format using the DCode tool as follows.

App Installed Timestamp
1662802989000 → *Saturday, 10 September 2022 09:43:09 (UTC+00:00)*

Last Accessed Timestamp
1663085216000 → *Tuesday, 13 September 2022 16:06:56 (UTC+00:00)*

Moreover, the *Cache.db* database file at the location *Library**Caches*\ *uk.co.creditexpert.companion*\consists of similar data as the *creditexpert.sqlite* database.

Figure 4.41: The package name of the application

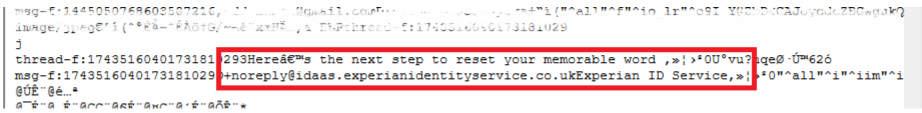

Figure 4.42: Memorable word resetting session

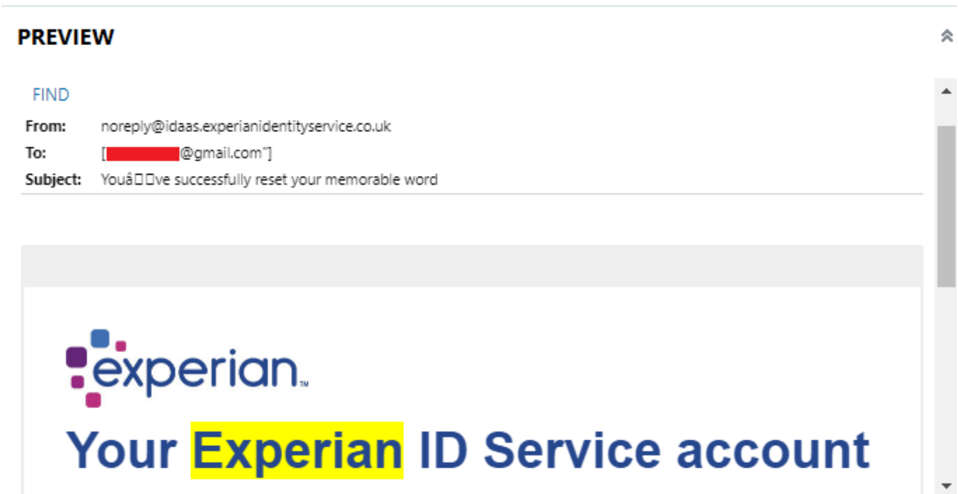

Figure 4.43: Email notification received after resetting the memorable word successfully

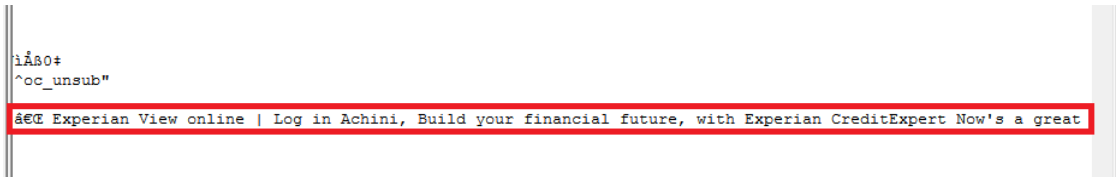

Figure 4.44: Notification messages received from Experian

ZID	ZNAME	ZEMAIL	ZINSTALLEDTIMESTAMP	ZLASTACCESSTIMESTAMP
Filter	Filter	Filter	Filter	Filter
11568470361...	Achini Dissanayaka	[redacted]@gmail.com	1662802989000	1663085216000

Figure 4.45: User ID, user's name, email address, application installed timestamp, and last access time

In the analysis process after uninstalling the Experian iOS application, the email address and the app installed date were able to be discovered from the *analytics.sqlite* database file in *\Library\Preferences* as shown in figure 4.46.

id	account_name	data
experian	Filter	Filter
uk.co.creditexpert.companion	[redacted]@gmail.com	BLOB

Figure 4.46: The mail address and application installed date recovered after uninstalling the app

The results gathered in this chapter will be analysed, compared and discussed further in the next chapter.

Chapter 5

Discussion

In this chapter, the findings of the research will be discussed in detail. A comparison was carried out against the findings of this research and the previous research findings, which are related to Android and iOS smartphones.
The main purpose of this research was to recover user-sensitive data from the three credit scoring applications named ClearScore, Credit Karma and Experian on both Android and iOS operating systems and to identify the most secured credit scoring mobile applications from the perspective of the end user. This aim was accomplished by achieving the objectives of the project as discussed in the next sections of the document.

5.1 Identification of research gap

The identification of the research gap was performed by following the previous research papers, articles related to modern cyber crimes, and reports related to forensic investigations. Based on all the gathered information, a lack of research to address the privacy and security concerns of credit scoring applications on popular mobile operating systems such as iOS and Android was identified.

5.2 Selection of credit scoring applications

A set of credit scoring mobile applications were selected using a quantitative approach. For this process, the facts such as the number of downloads, reviews, and ratings of each application on the Google Play Store and Apple App Store were considered. After having a wide comparison among the most popular credit scoring applications, the three most popular applications (ClearScore, Credit Karma, and Experian) were selected for this project. The selected applications were then installed on two smartphones running Android and iOS operating systems.

5.3 Creation of frictional user accounts

Frictional user accounts were created in each application on both operating systems using frictional data to evaluate the security of the selected set of applications before and after uninstalling the applications. The default security features of all the applications were explored and summarised as shown in tables 1 and 1 to identify the protection provided to user personal data.

5.4 Identification of recoverable user data

To examine the recoverable personal data of these applications, logical images of both Android and iOS mobile devices were necessary to be acquired, before and after uninstalling the applications. In order to acquire logical images, it is necessary to have root access on both mobile devices for accessing the privileged files. Thus, the newer versions of Magisk and Uncover++ software were used to root and jailbreak the Android and iOS mobile phones to obtain privileged access. The logical images were then acquired using the forensic software Magnet Axiom Process. The acquired images were then analysed separately for each application using three forensic analysis tools: Magnet Axiom Examine, AccessData FTKIm-

ager and HxD as some of the data were not fully recoverable using one tool. The user sensitive data such as name, email address, phone number, address, credit score, credit bands, installed date of the application, first and last access date of applications, etc were discovered from the internal storage of the devices. Based on the findings of this project, the security and privacy concerns of each application were identified from the perspective of the end user. It seems that even though the credit scoring applications provide various security features, it was possible to recover user sensitive data from the data remnants left behind by the applications.

5.5 Comparative analysis of recoverable data

A summarised comparison of data evidence recovered from the Android and iOS operating systems was illustrated in Table 1. Although there were no plain text passwords discovered, a significant amount of personal information was recovered from all the Android and iOS applications. The information presented in this study contributes a rich source of evidence related to the credit scoring applications and newer versions of mobile operating systems to aid forensic investigations whilst encouraging the software developers to enhance the security and privacy concerns of mobile applications.

The evidence gathered in this project appears different for each mobile application, which may be a result of different file systems in the two operating systems and different software designs with different security features.
All the software and hardware tools required for this study were selected after considering the factors such as the most popular credit scoring mobile applications, the most widely used forensic tools, the most popular mobile platforms, etc. The three forensic analysis tools utilised in this study delivered different results in some instances.
From the findings of this study, it seems to be that all the credit scoring mobile applications on both platforms store information not only inside the application package but also in the database and system files located outside (e.g. Cache

	Android Operating System						**iOS Operating System**					
Data Remnants	ClearScore		Credit Karma		Experian		ClearScore		Credit Karma		Experian	
	Before	After	Before	After	Before	After	Before	After	Before	After	Before	After
Plain text passwords	x	x	x	x	x	x	x	x	x	x	x	x
User's name	✔	✔	X	X	✔	✔	✔	X	✔	X	✔	X
Email address (username)	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Phone number	x	x	x	x	x	x	x	x	✔	x	x	x
User activities	✔	✔	✔	X	✔	✔	✔	X	✔	X	✔	X
User's address	✔	x	✔(only country name)	x	x	x	x	x	X	x	x	x
Fingerprint / Face ID	✔	x	x	x	✔	x	x	x	x	x	x	x
Last access date	✔	✔	✔	✔	✔	✔	✔	X	✔	X	✔	X
User ID	✔	✔	✔	✔	✔	✔	✔	X	✔	X	✔	X
Install date	✔	✔	✔	✔	✔	✔	✔	X	✔	X	✔	X
Bank accounts connected	✔(the names of banks)	✔(the names of banks)	x	x	x	x	x	x	x	x	x	x
Email Messages	✔	✔	X	X	✔	✔	✔	✔	✔	✔	✔	✔

Table 5.1: Comparison of the three applications based on the data remnants recovered on the Android and iOS platforms (data remnants recovered before and after uninstalling all the applications are tabulated separately as shown in columns 'Before' and 'After')

Data Remnants	Location / File name
User Data	/data/ data/$\langle Packagename \rangle / shared\_prefs/...$
User's activity timestamp	/data/data/ $\langle PackageName \rangle / shared\_prefs/$ $com.google.android.gms.measurement.prefs.xml$
Uninstalled application details	/data/data/com.android.vending/databases/localappstate.db , /data/data/com.android.vending/cache/streamdatastore/streamdatastore.db
Email notifications	/data/data/com.google.android.gm/databases/bigTopDataDB.-...-wal

Table 5.2: Paths / File names of general data evidence for Android 11.0 Applications

images). Also, it came to the attention that the files such as the *WAL* files, and *com.google.android.gms.measurement.prefs.xml* file on the Android platform play a crucial role in mobile forensic investigations as a rich source of user data. The locations and file names of general data evidence of Android 11.0 mobile applications were summarised in Table 5.2. In the analysis process of Clearscore and Experian applications, *\data\data\com.google.android.gm\databases\bigTopDataDB.-45848498-wal* file was used to retrieve the email notifications sent to the user from these applications which led to identifying some of the user's activities, user details, etc. All three android credit scoring applications stored information about the application in their own *com.google.android.gms.measurement.prefs.xml* file. With the aid of this file, it was able to discover the application installed time, first open time of the application, and last pause time of the app which are quite important if the user data is not retrievable. Same as on android, there were common data retrievable locations in the iOS platform as shown in Table 5.3. The package paths of all the credit scoring iOS mobile applications were located under *\private\var\mobile\Containers*.

In this study, the data recovered from Android and iOS operating systems were compared with previous research work to identify if there are any differences in

Data Remnants	**Path**
User Data	\private\var\mobile\Containers\Shared\AppGroup\⟨*AppPackage*⟩, \Library\Caches\⟨*AppPackage*⟩
User's activity timestamp	\private\var\mobile\Containers\Data\Application\⟨*AppPackage*⟩
Uninstalled application details	\Library\Preferences\
Email notifications	\Documents\Emails\

Table 5.3: Path of general data remnants for iOS 15.6.1 Applications

data remnants that can be retrievable from the newer versions of operating systems. Some of the files and file locations from which the data was recovered in this study were the same as the locations discovered in previous research studies (Salamh et al., 2021). Thus, Android version 10.0 and Android version 11.0 both have similar data recoverable files and folders as demonstrated in table 5.4. Same as on the Android platform, there were similar file locations in iOS 13.3.1 and 15.6.1 as shown in table 5.5.

Similar data recoverable files / file locations	Description
/data/data/$\langle Packagename \rangle$/	Application Package path
/data/data/$\langle Packagename \rangle / shared_prefs/...$	User data
com.google.android.gms.measurement.prefs.xml	Application usage information
bigTopDataDB.-...-wal	Contents of emails

Table 5.4: Similar data recoverable files and file locations of Android 10.0 and 11.0

Similar data recoverable files / file locations	Description
/private/var/mobile/Containers/Data/Application/$\langle AppPackage \rangle$	Application Package path
/private/var/mobile/Containers/Shared/AppGroup/$\langle AppPackage \rangle$ /Library/Caches/ $\langle AppPackage \rangle$	User data
/Library/Preferences/ $\langle AppPackage \rangle .plist$	Application usage information

Table 5.5: Similar data recoverable file locations of iOS 13.3.1 and 15.6.1

Chapter 6

Critical Evaluation

This research study was a great learning experience of using the knowledge which I acquired through the lectures, practical sessions, and self-studies, to solve problems individually and meet deadlines in an effective and successful way. It was an opportunity to learn how to use forensics tools to retrieve information from different mobile operating systems, analyse them to gather relevant evidence, and draw conclusions based on them. As I did use a number of forensic-related software for this study, it enhanced my exposure to the forensic tools which are used in the industry and was able to obtain hands-on experience. Furthermore, enhancement of report writing skills with the aid of gathered evidence, the use of quantitative approaches to achieve the objectives of the project and identifying previous research approaches and their findings were some of the added advantages of this dissertation. All these aspects usually do not come from theoretical lessons, but by completing this assignment I have gained a firm grip on how to succeed in individual projects.

In this study, there were some limitations as the operating systems used for the experiment were new and the number of methods and guides to root and jailbreak the smartphones was limited. At the beginning of the experimental procedure, it required rooting the android smartphone to gain privileged access to the device. To achieve this, TWRP, a software which is used for recovery purposes of the device

was employed, but the version of the TWRP was incompatible with the android version of the device. As a result of this, when accessing the recovery mode of the device, it automatically entered the Qualcomm crash dump mode. The device was not able to boot the operating system, after several attempts I managed to boot into Fastboot mode. Then I had to do a completely new installation of the operating system of the device which allowed me to boot to a newer version of the TWRP application via the laptop to access the recovery mode of the mobile device. Finally, I was able to access the recovery mode to uninstall the TWRP application from the device. Once the device was restarted it was able to boot the operating system successfully. Afterwards, a newer version of the TWRP application was installed and successfully rooted the android device with the Magisk application. As I had to do a new installation of the operating system, all the data on the device was lost in the process and had to start everything from the beginning (installing applications, creating frictional users in all applications, etc). Another limitation of this project was some of the data were unable to recover fully using the analytical tools employed in this project. So, I had to find alternative forensic tools, which turned out to be beneficial for me as I was exposed to quite a number of forensic analysis tools.

To conclude things, I would like to mention that this was a great opportunity for me, not just to use my knowledge and skills to achieve the aims and objectives of a practical scenario, but also to work as a responsible individual in problem solving to meet a deadline in an effective and successful way.

Chapter 7

Conclusion

Credit scoring mobile applications are very popular in the United Kingdom since they provide tips and tricks to improve the credit score, allow users to check their own credit assessment, monitor the movement of credit score, etc. Although credit scoring applications do not collect users' financial data, they do allow users to link their bank accounts hence the potential risk of security and privacy breaches is quite high. Furthermore, with the frequent release of newer versions of the mobile operating system, digital forensic investigators must stay up to date as there might be differences compared to previous versions. All these facts make it a crucial requirement to carry out forensic investigations on this topic.

In this study, an in-depth mobile forensic investigation of the three most popular credit scoring applications in the United Kingdom: ClearScore, Credit Karma, and Experian was performed on both android 11.0 and iOS 15.6.1 operating systems. The logical images of both smartphones were acquired after creating frictional user accounts and after uninstalling the application. Using three popular forensic software, the acquired data was analysed and gathered several personal information related to the user such as the user's email address, phone number, name, etc. The recovered data remnants of Android and iOS mobile devices were compared with the previous versions of operating systems which were collected from older research findings.

From the perspective of the mobile application user, the data remnants that are left inside the local storage of mobile devices reveal various personal information of the end user which could lead to a violation of privacy and security, in the forms of social engineering, phishing, targeted marketing etc. Thus, it can be concluded that despite the various security features, credit scoring applications do leave behind data remnants in the local storage of mobile devices, of which user-sensitive data can be recovered and potentially exploited. Additionally, this study provides a rich source of personal information of the end users that can be used in forensic investigations whilst encouraging software developers to enhance the security and privacy concerns of mobile application users.

From the perspective of the mobile application user, the data remnants that are left inside the local storage of mobile devices reveal various personal information of the end user which could lead to a violation of privacy and security, in the forms of social engineering, phishing, targeted marketing etc. Thus, it can be concluded that despite the various security features, credit scoring applications do leave behind data remnants in the local storage of mobile devices, of which user-sensitive data can be recovered and potentially exploited. Additionally, this study provides a rich source of personal information of the end users that can be used in forensic investigations whilst encouraging software developers to enhance the security and privacy concerns of mobile application users.

Future research should investigate the newer versions of the operating systems and credit scoring applications by applying additional case scenarios such as by engaging malware to the test devices to observe the behaviours, network traffic, penetration testing etc. The other mobile operating systems should also be considered and compared with Android and iOS platforms for a better understanding of security and privacy concerns among the platforms. Ultimately, the continued investigation in this field will address the security and privacy concerns of credit scoring applications.

References

ALThebaity, S., Mishra. (2020, 08). Forensic analysis of third-party mobile application. , *10*, 32-38.

Amine Chelihi, M., Elutilo, A., Ahmed, I., Papadopoulos, C., & Dehghantanha, A. (2017). Chapter 15 - an android cloud storage apps forensic taxonomy. In K.-K. R. Choo & A. Dehghantanha (Eds.), *Contemporary digital forensic investigations of cloud and mobile applications* (p. 285-305). Syngress. Retrieved from https://www.sciencedirect.com/science/article/pii/B9780128053034000150 doi: https://doi.org/10.1016/B978-0-12-805303-4.00015-0

Bahrynovska, T. (2022). *How credit scoring software solutions help assess creditworthiness.* Retrieved from https://forbytes.com/blog/credit-scoring-software/

Carnegie Endowment, f. I. P. (2022). *Timeline of cyber incidents involving financial institutions.* Retrieved from https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline

Dargahi, T., Dehghantanha, A., & Conti, M. (2017). Chapter 2 - forensics analysis of android mobile voip apps. In K.-K. R. Choo & A. Dehghantanha (Eds.), *Contemporary digital forensic investigations of cloud and mobile applications* (p. 7-20). Syngress. Retrieved from https://www.sciencedirect.com/science/article/pii/B9780128053034000022 doi: https://doi.org/10.1016/B978-0-12-805303-4.00002-2

Duncan, M., & Karabiyik, U. (2018). Detection and recovery of anti-forensic (vault) applications on android devices.

Fraudwatch. (2022). *The rise of the fraudulent mobile app.* Retrieved from https://fraudwatch.com/the-rise-of-the-fraudulent-fake-mobile-app-how-to-protect-your-brand-and-business/

Gilbert, A., & Seigfried-Spellar, K. C. (2022). Forensic discoverability of ios vault applications.

Govindraj, B. (2022). *Mobile application security trends to watch out for in 2022.* Retrieved from https://www.appsealing.com/app-security-trends-2022/

Indeed, E. T. (2021). *What is a mobile app? (with definition, types and examples).* Retrieved from https://uk.indeed.com/career-advice/career-development/what-is-mobile-app

Kang, S., Kim, S., & Kim, J. (2020). Forensic analysis for iot fitness trackers and its application. *Peer-to-Peer Networking and Applications*, *13*(2), 564–573.

Kim, H., Shin, Y., Kim, S., Jo, W., Kim, M., & Shon, T. (2022, 05). Digital forensic analysis to improve user privacy on android. *Sensors*, *22*, 3971. doi: 10.3390/s22113971

Kitsaki, T.-I., Angelogianni, A., Ntantogian, C., & Xenakis, C. (2018). A forensic investigation of android mobile applications. In *Proceedings of the 22nd pan-hellenic conference on informatics* (p. 58–63). New York, NY, USA: Association for Computing Machinery. Retrieved from https://doi.org/10.1145/3291533.3291573 doi: 10.1145/3291533.3291573

Lee, M. (2022). *Jailbreak ios 15.6 - how to jailbreak ios 15.6 / 15.6.1 with unc0ver (no computer).* Retrieved from https://www.youtube.com/watch?v=geJzAa7gD1I

Lin, X., Chen, T., Zhu, T., Yang, K., & Wei, F. (2018). Automated forensic analysis of mobile applications on android devices. *Digital Investigation*, *26*, S59-S66. Retrieved from https://www.sciencedirect.com/science/article/pii/S1742287618301889 doi: https://doi.org/10.1016/j.diin.2018.04.012

Menahil, A., Iqbal, W., Iftikhar, M., Shahid, W., ul Hassan, K., & Rubab, S. (2021, 07). Forensic analysis of social networking applications on an android smartphone. *Wireless Communications and Mobile Computing*, *2021*, 1-36. doi: 10.1155/2021/5567592

Meredith E. David, J. A. R. (2021). Smartphone use during the covid-19 pandemic: Social versus physical distancing. *International Journal of Environmental Research and Public Health*. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7908126/ doi: 10.3390/ijerph18031034

Muncaster, P. (2022). *5 ways cybercriminals steal credit card details.* Retrieved from https://www.welivesecurity.com/2022/06/27/5-ways-cybercriminals-steal-credit-card-details/

Rolfe, A. (2022). The rising issue surrounding mobile app fraud. Retrieved from https://www.paymentscardsandmobile.com/the-rising-issue-surrounding-mobile-app-fraud/

Salamh, F. E., Mirza, M. M., Hutchinson, S., Yoon, Y. H., & Karabiyik, U. (2021). What's on the horizon? an in-depth forensic analysis of android and ios applications. *IEEE Access*, *9*, 99421-99454. doi: 10.1109/ACCESS.2021.3095562

Shin, S., Kim, G., Kim, S., & Kim, J. (2022). Forensic analysis of note and journal applications. *Forensic Science International: Digital Investigation*, *40*, 301355. Retrieved from https://www.sciencedirect.com/science/article/pii/S2666281722000245 doi: https://doi.org/10.1016/j.fsidi.2022.301355

Similarweb. (2022). *Top free finance iphone apps in app store in united kingdom.* Retrieved from https://www.similarweb.com/apps/top/apple/store-rank/gb/finance/top-free/iphone/

Singh, S. (2019). *How to install twrp on oneplus 6 and root with magisk.* Retrieved from https://www.gizmochina.com/2019/06/10/install-twrp-oneplus-6-root-magisk/

SSL2Buy, g. S. P. (2022). *Mobile application security and privacy: An inevitable aspect in mobile app development.* Retrieved from https://www.ssl2buy.com/cybersecurity/mobile-application-security-privacy

Uduimoh, A. A., Osho, O., Ismaila, I., & Shafi'i, M. A. (2019). Forensic analysis of mobile banking applications in nigeria. *i-manager's Journal on Mobile Applications and Technologies*, *6*(1), 9.

University, C. M. (2015). *Knowledge of location sharing by apps prompts privacy action.* Retrieved from https://www.sciencedaily.com/releases/2015/03/150323132846.htm

Wollit. (2021). Best credit score apps in the uk. Retrieved from https://www.wollit.com/money-hub-resource/best-credit-score-apps-in-the-uk

Wu, Y. P., Yi;. (2021). Application analysis of credit scoring of financial institutions. *Complexity*, *2021*, 12. Retrieved from https://www.hindawi.com/journals/complexity/2021/9222617/

Yuliani, V., & Riadi, I. (2019, 09). Forensic analysis whatsapp mobile application on android-based smartphones using national institute of standard and technology (nist) framework. *International Journal of Cyber-Security and Digital Forensics*, *8*, 223-231. doi: 10.17781/P002615

Zhang, X., Baggili, I., & Breitinger, F. (2017). Breaking into the vault: Privacy, security and forensic analysis of android vault applications. *Computers Security*, *70*, 516-531. Retrieved from https://www.sciencedirect.com/

science/article/pii/S0167404817301529 doi: https://doi.org/10.1016/j.cose.2017.07.011

Appendix A

Approved Ethical Application and Documents

A.1 Ethical Approval Form