How to Cite:
Jeyaseeli, J. A. M., & Shanthi, C. (2022). A smart techniques to extract the deleted data form the android application. *International Journal of Health Sciences*, *6*(S1), 2864–2871.
https://doi.org/10.53730/ijhs.v6nS1.5284

A Smart Techniques to Extract the Deleted Data Form the Android Application

J. Annies Mary Jeyaseeli
Research Scholar, Department of Computer Science, VISTAS, Chennai, Tamil Nadu, India
Email: annies.phd@velsuniv.ac.in

C. Shanthi
Assistant Professor, Department of Computer Science, VISTAS, Chennai, Tamil Nadu, India.
Email: shanthi.scs@velsuniv.ac.in

***Abstract*---**Today we are living in the mobile world, a man without a mobile were considered to be an exception in the recent machine world. A mobile without internet connection were not considered to be significant role in the real time environment. A valuable data of the android mobile phone may be deleted accidently or incidentally. These deleted data must be extracted becomes a complex task. This complex task can be accomplished with various methodologies and techniques. This paper consists of three phases such as first phases describes about the types of files can be retrieved or extracted after deletion. Second phases consist of three different types of recovery techniques used to extracted the deleted data. Third phase about the experimental result to determine the accuracy. This paper provides the different smart techniques to extract to deleted data from the android applications.

***Keywords*---**Extracted data, android application, shared preferences, rooting, without rooting.

Introduction

Today we are living in the mobile world, a mobile without person it finds it very difficult in the real-world scenario. The Mobile with internet connection plays a vital role in day today life. A Mobile phone had many functionalities which provide the necessary data in the machine world. The Data such as contacts, username, password, images with remarkable events, PIN Number and other personal details which are considered to be the valuable data. These Valuable data may be accidently or incidentally deleted to the various reason. Since these data must be

extracted even the person deleted in the mobile, which act as one of the tedious processes. This Process of extracting a data may be called as restoration process.

As a survey of Computer Security Institute Reported in the year of 2007 (Rayarikar, 2012), approximately 71% of companies used an encryption technique in order to protect the valuable data. These valuable data must be retrieved or extracted even when the person deleted the data accidently or incidentally. Two Technical terms such as “Loading and Saving” plays a significant role in the field of extracting data. The data which transmit from permanent memory to main memory termed as loading, these loading depends upon memory size, operating system, processor with mega byte transfer rate. The data which transmit from main memory to permanent memory termed as Saving. These Saving depends upon the memory size.

According to the survey of CTIA, United States, more than 6.5 million text messages and more than 330 million multimedia messages had been transmitted per day (December 2013). Therefore, Apple corporation in the year of 2016 (Salamh, 2019)announced that the user must send an average of 200000 messages per seconds. As increase of Message data extraction provide a complex issued in the data recovery world.

This paper mainly focused with types of extracted deleted data done by the user in their mobile devices. Extraction of deleted (Jones, 2017) data from mobile devices can be supported with several forensic tools. Forensic Tools were mainly used to retrieve mobile data and generate the appropriate reported data. Mobile Devices consist of various information in the form of multimedia such as audio, video, text, animation and graphics format. It’s also included location about the particular devices, subscriber details and identifier with data/time, call logs.

Literature Review

Wang et.al (2019) explained about country migration is taking great interest (Wang, 2019)in each geographical and social sciences. Compared to the central study, we change to explain the templates of the migrants with the appropriate and small space permissions of the knowledge collected at the overall location of the US overall US device. Mobile positioning holder, this paper set data set, initial analysis of the space model aims to disclose social and economic factors related to the MAEP of MAEP (MAEP) and immigrants' modifications that migrate.

Cozzolino et.al (2018) proposed an article provides a new data model of a multimedia social network (Cozzolino, 2018), that is, a specific social networking network that combines with content that is generated and used in a related environment in a related environment. The focus of the work shows the data of a mobile device that enriches a series of series of series of information related to the media associated with the media separated by the community. The proposed model depends on the data structure of Hypergraph for capture, especially in a simple way of all types of relationships in social networking networks, as well as user and multimedia contents. To activate a variety of search applications, some customized and multimedia rating features are also entered. Finally, some

experiments related to the effectiveness of the approach to support the relevant activities of information are reported and discussed.

Aljahdali et. Al (2021) formulates the culmination of the global spread of smartphones is the expansion of the collection and exchanging vast amounts of data that can be used as digital evidence in forensics. Like this, the mobile industry continues to grow and becomes more likely to be used for criminal activities. Smartphones are often loaded with various applications, new technologies and operating systems. system. Therefore, it is difficult for investigators to extract evidence (ALJAHDALI, 2021)from smartphones. collection Related evidence, forensic analysis and forensic tools for smartphones and their function is required. This study investigates the investigation process for mobile forensics. Paper presents the limitations of the use of tools and forensic techniques used in smartphone device research. The purpose of this article is to allow researchers to examine all Researchers.

Kim et.al (2022) provides details about mobile devices play an important role in digital forensics, and their artifacts are often used as valuable evidence in court. People use various applications (applications) on mobile devices, and application data is managed and stored in the form of a database. Users can arbitrarily delete data from the database. This possibility works in an anti-criminal way. Restoring deleted data (Kim, 2022) is important to getting more data and can help you overcome these limitations. In this work, we focused on the Realm database, which is optimized for mobile devices. We analysed the structure of the Realm database and the various delete functions. We have developed a method to recover deleted Realm database data based on data structure and unallocated area. The proposed method was tested using proof-of-concept code and average recovery rates were determined for MiniTalk and Xabber applications.

Android data recovery techniques

The Moments accidentally or incidentally deleted data which were more significant data on the mobile phone. These deleted data which may be a valuable data must be retrieved from the android operating system. Others may intentionally or unknowingly do this to your phone data. It happened to all of us at some point. However, there are many software on the market today that can help you recover deleted files. This type of software belongs to the category of data recovery software. There are many programs on the market that can recover deleted files. This blog describes the Android data recovery process for internal memory and external memory card. This blog specifically discusses Android data recovery software.

Types of files to be recovered

Android Recovery Software to extracted the deleted data can be recovered with the following types of files as shown in Figure.1. It extracted data can be segregated based on their directory type such as

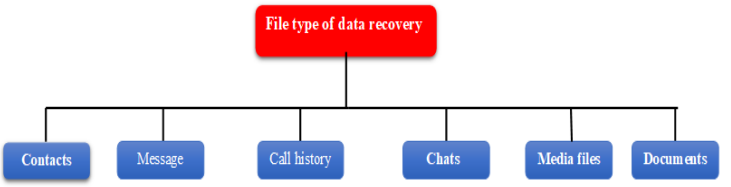

Figure 1: File Types of Data Recovery

a) Contacts: Contact which stored in both internal and external storage
b) Messages: Messages sent and received from all message android applications
c) Call History: Call received, dialled Call and missed Call were three types of History
d) Chats: The Person who chats with android applications
e) Media Files: Files include image, video and audio
f) Documents.: Files which consist of document file such as word, excel, pdf etc.,

Proposed work

This Paper Consist of three phases of extracted deleted data such as Opensource Recovery, Smart Recovery and User Defined Recovery as shown in Figure 2 below.

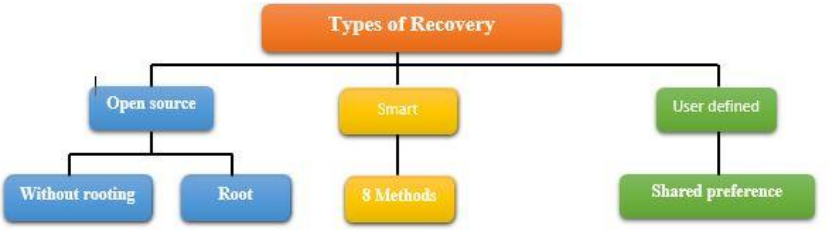

Figure 2. Types of Extracted Data Recovery

Opensource recovery

Its is common and quite nature to delete the old files by the people who uses android phone to free up space but sometimes important files may be deleted accidently. This section consists of the steps involved to retrieve data recovery from the android phone. The Process of Opensource recovery consist of two steps such as with rooting and without rooting as shown in Figure 3.

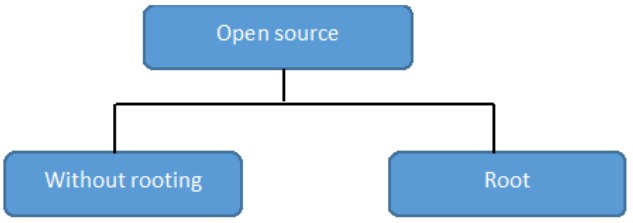

Figure 3. Open-Source Recovery

a) Without Rooting

This process without rooting recovers the deleted data from the mobile phone. The File which had been deleted were not deleted permanently, rather it had been moved to a hidden folder or may be replaced with another file. Its tedious task to find out the missing file and there may be chance of file which had been overwritten. The following steps involved to retrieve the data file without rooting.

// **Steps for extracted the deleted data without rooting**

Step 1. Install the appropriate tool for Data Recovery in normal computer or laptop
Step 2. In main menu select android data recovery
Step 3. Now connect mobile with computer or laptop using USB Cable
Step 4. Give Permission for USB Debugging of Android
Step 5. USB act as an intermediate which doesn't lose any data during connection.
Step 6. Select the types of files wants to recover, select next to continues
Step 7. Select the Quick Fast Scanning process
Step 8. View the recovered file and stored in the destination path.

The algorithm used to extract the data without rooting process.

b) With Rooting

Rooting process used to find the physical location of the deleted data. The Data can be deleted in both internal storage and external storage. The Extracted deleted were more comfortable in the external storages rather than internal storages. The Data in the internal memory were copied in terms of RAW file which would be converted in the Virtual hard disk format. The following steps described about the extracted data with rooting.

Step 1. Download FTP Server and make a copy of phone memory
Step 2. Move to the General Setting, Launch File Zila and set port to 40 for connection
Step 3. Set User Password and save to the root c:\cygwin64\
Step 4. Download and install android copy all .exe and .dll to the root folder
Step 5. Enable USB and Execute the command in cmd prompt
Step 6. Convert the given RAW file into VHD format.
Step 7. Open the file in the appropriate root folder which consist of the recovered file.

These steps involved in extracted the deleted data with rooting under open source recovery.

Smart Recovery

Smart Recovery techniques used to extract the deleted data with existing smart recovery tools with eights steps. Various tools had been launched to extracted the deleted data used in the android mobile phone. The 8 Steps to followed to extracted the deleted data using existing smart recovery tools as follows.
// 8 methods to be followed
Step 1. Tools, to be download and install in your PC or Laptop
Step 2. Mobile should be connected with PC or Laptop using USB
Step 3. Execute Tools
Step 4. Select the option of which type of file should be recover
Step 5. Choose the appropriate location to scanned
Step 6. Select the start options
Step 7. Select the file wants to recover
Step 8. Stop the process.
There are various tools based on smart recovery such as DiskDigger Photo, Wondershare Dr.Fone, Recuva and Fone Paw etc.,

User Defined Recovery

This phase mainly used by the programmer who can create their own android code to extracted the deleted data from the internal and external memory. The following figure represent the persisting of data in User Defined Recovery with shared preferences.

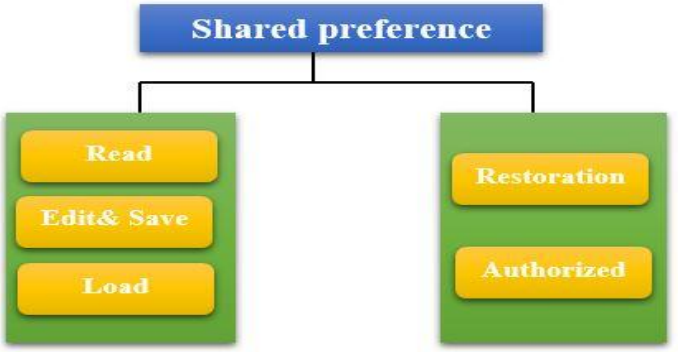

Figure 4. Shared Preferences -User Defined Recovery

Persisting of Object which consist of storage and retrieval of deleted data in the mobile devices. These persisting functionalities provide by the default interface of shared preferences. This Shared Preference which consists of four processes of recovery of data such as authorization, backup, restoration and compression techniques. Authorization used to verify the data belongs to the concern person or authorized person. Backup process used to retain the valuable data in the particular location with appropriate root folder. Restoration which consists of loading and saving the valuable data, which were retrieved after deletion. Compression techniques which used to compression the extracted data in the particular locations.

```
//Steps of Shared Preferences
SharedPreferences sf1 = this.getSharedPreferences("sample.app”, Context.MODE_PRIVATE);
```

Sf1 refer as object of SharedPreferences with mode as private in terms of authentications.

Using Shared Preference, the deleted data can be retrieved with the help of persisting object.

Experimental Result

Three set of Data Extraction techniques used for the experimental result such as open source with rooting and without rooting, smart and user defined techniques in terms of category A, Category B and Category C respectively. Sample size of same file were deleted and *extracted the data with three different techniques as shown in table given below.*

Data Recovery	Accuracy
Category A	87.5
Category B	85.6
Category C	86.3

Table 1. Experimental Result

From the above the table the following graph were generated based on the experimental result in the following Figure.5.

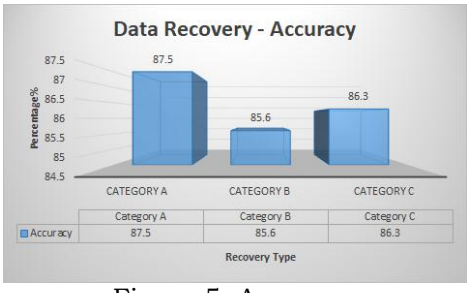

Figure 5. Accuracy

From the above graph, it conclude that all the three types of category leads to the accuracy of 85 to 87% of extracting the deleted data in the android mobile applications.

Conclusion

This paper conclude that various approach or techniques used to extract the deleted data in the android application. There were three types of techniques discussed in this paper. Opensource techniques with rooting and without rooting concept in order to extract the deleted data in the android mobile phone which proved with accuracy of 87.5%. Smart Techniques with existing tool which act as free ware and open source where the normal user can retrieve the extracted data

in the android application with 85.6% accuracy. Finally, where the professional android programmer can implement their own code to extracted the deleted data from the internal and external storage with capacity of 86.3% accuracy. This paper concludes with various methodology to extracted the deleted data in the android phone which act effectively and efficiently.

Reference

1. ALJAHDALI, A. N. (2021). Mobile device forensics. *Romanian Journal of Information Technology and Automatic Control*.
2. Baresi, L. a. (2021). IDEA: Runtime Collection of Android Data. *In 2021 IEEE International Symposium on Software Reliability Engineering Workshops*.
3. Chow, X. Q. (2021). A Mobile Forensic Visualization Tool For Android Data Partition. *Applied Information Technology And Computer Science*.
4. Cozzolino, G. (2018). Using semantic tools to represent data extracted from mobile devices. *In 2018 IEEE International Conference on Information Reuse and Integration* .
5. Eriş, F. G. (2021). Forensic Analysis of Popular Social Media Applications on Android Smartphones. *Balkan Journal of Electrical and Computer Engineering*.
6. Ichsan, A. N. (2021). Mobile Forensic on Android-based IMO Messenger Services using Digital Forensic Research Workshop (DFRWS) Method. *International Journal of Computer Applications* .
7. Jeyaseeli, J. A. (2021). Physical Data Extraction from Android mobile using Apeaksoft Android toolkit and Android Debug Bridge. *NVEO-NATURAL VOLATILES & ESSENTIAL*.
8. Jones, G. M. (2017). Forensics analysis on smart phones using mobile forensics tools. *International Journal of Computational Intelligence Research* .
9. Kim, S. G. (2022). Methods for recovering deleted data from the Realm database: Case study on Minitalk and Xabber. *Forensic Science International: Digital Investigation*.
10. Miao, Z. Y. (2021). Research and Practice on Data Acquisition of Android-based Application. *In 2021 2nd International Symposium on Computer Engineering and Intelligent Communications* .
11. Rayarikar, R. S. (2012). SMS encryption using AES algorithm on android. *International Journal of Computer Applications*.
12. Reilly, J. S. (2013). Mobile phones as seismologic sensors: Automating data extraction for the iShake system. *IEEE Transactions on Automation Science and Engineering 10,*.
13. Salamh, F. E. (2019). An In-Depth Forensic Analysis of Android and iOS Applications. *IEEE Access 9* .
14. Sharma, T. a. (2021). Malicious application detection in android—a systematic literature review. *Computer Science Review* .
15. Wang, Y. L. (2019). Migration patterns in China extracted from mobile positioning data. *Habitat International*.
16. Xiao, J. (2022). Online Interactive Data Extraction and Intelligent Analysis of College Vocal Music Courses Oriented to Mobile Android Platform. *In 2022 4th International Conference on Smart Systems and Inventive Technology*.