IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Exploration of Android Data Recovery

Manuj Narayanaa Rajaram, Kadam Rutuja Subhash, Pandey Harshvardhan Mayashankar

Department of Information Technology, Pillai College of Engineering, Navi Mumbai,410209

Abstract— In this modern world, android devices and smartphones are used on a large scale. A lot of data is stored on our smartphones as a part of our daily lives. Many times, it may happen that we accidentally delete an important file or document,images. Usually we may have the feature of a recycle bin or backup storage in our android device, which may store recently deleted files, but it is not always the case. Also, data loss in Android devices can occur due to a multitude of reasons like malware, upgrades in OS, compromised devices, system reboots etc. In this paper we have discussed a proposed methodology for data recovery of deleted data from an Android by trying to gain temporary root access and recovering the data from internal storage.

Keywords— Android Data Recovery, Android Forensics, Digital Forensics, Mobile phones, Rooting

I. INTRODUCTION

With the widespread use of smartphones, Android devices have become an important data source in forensic investigation, and many tools which collect data from Android devices have also been introduced.
With the rapid development of Android, forensics and data recovery technology on it have become increasingly important. Especially for digital forensics and judicial investigation, the deleted information tends to have a higher evidentiary value. Research on Android database management strategy and recovery methods will be of great value and have very broad application prospects..
Forensic analysis makes users and app developers aware of what type of information should be stored in any particular device. This Information can be used by attackers in unauthorized ways.
Many criminals are aware of data recovery techniques and they always try to surpass them whereas the organizations always try to discover newer and more reliable recovery techniques to tackle this situation.
In this paper, we discuss, we also see different ways to recover data from android like physical or logical and propose a recovery method for safe and secure recovery of data.

Data recovery is the process of restoring data that has been lost, accidentally deleted, corrupted or made inaccessible.

Forensic data recovery is the extraction of data from damaged evidence sources in a forensically sound manner. This method of recovering data means that any evidence resulting from it can later be relied on in a court of law.

This method is used when the data is inaccessible by normal means i.e. either the data inside is corrupted or completely formatted, or when the storage device is damaged and the method is used on devices like SD Cards, Hard Disks (Internal and External), SSD Devices, CDs and DVDs, and any other storage device.

Today when there are more than 1 billion Android users all over the world, it shows that its popularity has no equal. These days mobile phones have become so intrusive in our daily lives that when they are needed they can give a huge amount of information to forensic examiners.

Recovering Deleted data from Android will be of great help to forensic experts to extract information from the mobile phones, android smartphone devices which have been used for criminal activity, and have been deleted to erase any evidence. But extracting data safely and immediately will help us uncover and help us to gain critical evidence while solving criminal cases.

While looking at personal level usage of data recovery, accidental loss of data because of accidents or unknown reasons or bugs can happen. Important images, videos and other form of data can be lost and this project might help us find a way to gain the lost data and keep personal memories intact.

On a commercial basis, this can be used as a method for data recovery for android devices and can be used as a reference for other forensic experts for future research and elaboration.

Data Storage in Android- The data in android devices is at the following places:

1.Internal Storage
2. External storage
3.Shared Preferences
4.Databases.

All app specific private files are stored in the Internal storage. External storage devices like sd cards, memory cards and pen drives are used to store multimedia data which is removable and is mounted on the device.

Rooting- Rooting is a process which allows users to gain privileged or root access to the Android device. It gives access to android devices which is similar to Super user or administrative access in Linux or Unix type operating systems. Goal of Rooting is to overcome the limitations put by hardware manufacturers on the android device. We can run specialized applications or do operations that are otherwise inaccessible to the normal user. In the process of data recovery following advantages of rooting can be beneficial:-

1. *Access to root files in internal storage:-* Gaining access to root files in Android will help us to gain access to Internal Storage of the device and help us to access the data that is otherwise inaccessible. Scan your phone's internal memory to search for those deleted and hidden file
2. *Installation of Data recovery software:-* Some softwares may require the root access to the Android device for doing specialized tasks.

There are risks associated with rooting which can be problematic for the data recovery process.

1. *Possible data loss-* Improper methods of rooting can cause data loss. Any misstep can cause data loss to occur and it becomes very difficult for the device to even properly function.
2. *Bricking the device-* Even the smallest of changes done to the files in the device after rooting may cause unforeseen changes in the functioning of the OS or any applications in the Android device. In a worst case scenario, it will render the device useless, thus preventing any chances of data recovery whatsoever.
3. *No guarantee of Complete data recovery as files may be overwritten-* Once the files are deleted, the location of the files in metadata is also erased. Once the Android device installs new applications or stores new data it can overwrite the previously deleted data from its memory to make space to store the new data. Because of this, complete data recovery becomes a challenge.

Types of Data in Android devices- When we speak of data in Data recovery in Android devices, we are talking about varied types of formats in which data is stored and presented in i.e. text files (.doc, .docx, .txt, .pdf, .odt), powerpoint presentations (.ppt , .pptx), images (.jpg , .jpeg , .png , .tiff, .bmp, .raw etc.), audio (.mp3, .wav, .aiff etc.) video (.mp4, .mov, .avi, .webm etc.) and many others. If we have to recover data which is from the popular formats like the ones mentioned above, there are higher chances of gaining resources that are targeted towards data recovery of those particular formats. Although if we are aiming for the data recovery of a very specific file format which may be obscure, custom or less in demand, it will be difficult to do so, as we may have a lack of resources or documentation for data recovery in that particular format or file type.

Android Systems- Android is an operating system developed for Mobile devices and smartphones. The latest version of Android released so far is Android 12. Android provides a lot of customization features

Kali Linux- Kali Linux is an open source Linux Operating system specifically designed for data forensics and is equipped with a lot of tools and resources for data recovery. It contains a lot of tools and techniques for Penetration testing, Forensic data analysis, Reverse Engineering and Security Auditing. This OS makes it easy to perform data extraction and analysis.

Autopsy- Autopsy is an end to end open source digital forensics platform. Many law enforcement, military, and corporate examiners use autopsy in their investigation process. It can also be used to recover photos from your camera's memory card.

Foremost- Foremost is a digital forensic software which can be used for data recovery. It can recover data from hard disk, memory drive, pen drive and also images of data created by other applications.

II. LITERATURE SURVEY

Following research papers were referenced for this project:

Digital forensics and analysis for Android devices

With the wide use of smartphones, Android devices have become an important data source in forensic investigation, and many tools which collect data from Android devices have also been introduced. However, most current studies consider only flashing the NAND card, nearly paying attention to eMMC cards. Therefore, based on Android Recovery Mode, this paper designed a general forensic tool giving consideration to both NAND and eMMC cards. And after exploring the possibility of data recovery when an application is uninstalled from an Android device which usually is formatted with extended file system version 4, a method for data recovery is put forward.

Android Phone Forensic: Tools and Techniques

These days mobile phones have become so intrusive in our daily lives that when they are needed they can give a huge amount of information to forensic examiners. With vast options of popular and less popular forensic tools and techniques available today, this paper aims to bring them together under a comparative study. During this survey they found scarcity for papers on tools for android forensic. This paper analyses different tools used in android forensics and it's techniques after which the results and findings are tabulated.

Data recovery in Forensics

Data recovery in cyber forensics and the procedures of cyber forensics are majorly discussed in this paper. Data recovery in harsh conditions like HDD that is burnt, the challenges experts face and those conditions where data recovery is not possible has also been described. It is discussed how cyber forensic comes into picture in crime scenes and for tracing evidences, different ways to recover data from all types of damages like physical or logical and discuss different recovery techniques is seen.

Database Management Strategy and Recovery Methods of Android

The two most important aspects of digital forensics are the recovery of deleted records and the database analysis. Based on the research results, a recovery method for database operating records from the WAL file is proposed. Sometimes the log file is emptied, there is a recovery method for the deleted log file for extended file system version 4, thus building a database operating record timeline. Images generated in different time and conditions are put forward for an experiment to validate the effectiveness and the limitations are discussed.

Key Technologies for Mobile Phone Forensics and Application

Mobile phones are an important source of evidence for judicial staff, but the research of mobile phone forensics systems is quite deficient compared with computer forensics. Toward this end, this paper proposed an integrated framework of the mobile phone forensics system, which is based on the characteristics and difficulties of mobile phone forensics. At the same time, in order to deal with the database scenario, it proposed a decryption method and a data-recovery method based on SQLite, which is the key part of this paper. Finally, the practicability of this system is shown by graphic demonstration.

III. Proposed Methodology For Data Recovery

There are two important requirements that should be met in order to make the Android phone recovery software work, allow the software to access your phone's storage and prevent the deleted data from being overwritten. if the deleted files have been overwritten, you can't get them back even after rooting the phone.

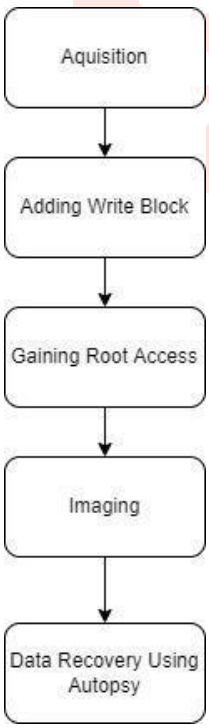

Fig.1 Block Diagram

Acquisition: The cybercrime crime scene includes the digital devices that hold digital evidence. The first responder's Job is to identify and preserve the crime scene from contamination.
There are certain steps that must be taken to preserve digital evidence on Android Device.

1. Check if the device is active or "ON"
2. If the device is "ON", check if you can access the system, disable Wi-Fi and Bluetooth. Turn On USB debugging and stay awake. Extend display screen timeout and lock time. If you cannot access the device, just collect device identifiers and preserve the device in a Faraday bag. A Faraday bag protects the device from outside signals to prevent data from being altered, deleted or added.
3. If the device is "OFF", don't try to turn it "ON". Check if the device is damaged, if yes remove battery (if possible) and collect device identifiers. If the device is found in a liquid, keep the device in until cleaned, collect device identifiers if possible, remove battery (if possible). If the device is not damaged, just remove its battery and collect the device identifiers.

Adding write block: We add write blocks to prevent data from being overwritten. Both software programs and hardware write blocks are available. The main difference is that software write blocks are installed on a forensic computer workstation, whereas hardware write blockers have write blocking software installed on a controller chip inside a portable physical device.

Gaining Root Access: Android OS uses the Linux kernel, hence gaining access to root gives similar administrative privileges as on Linux or any other UNIX-like operating system.

Imaging: Forensic experts connect the device to the toolkit using Android Debug Bridge (ADB). ADB allows the user to perform the actual function of creating the image. This process creates the complete image of internal memory.

Data Recovery using Autopsy: Data recovery is restoring data that had otherwise been lost by the owner of the device, or intentional removal of data after committing a cybercrime. Autopsy is a forensic tool, it only performs analysis and does not support/ allow the user to create an image of storage media.

Implementation of Proposed Method on a USB Drive:-
We have tested the proposed methodology on a USB Drive. Listed below are the USB Drive specifications, software tools and operating systems used while implementation of the process.

SD Card Specifications:-

Features	**Details**
Model	SanDisk Cruzer Blade SDCZ50-008G
Storage Space	8GB

OS and Software Tools:-

Software	**Details**
Virtual Machine	Oracle VirtualBox Version 6.2 /6.1
Host OS	Windows 10/ Windows 11
Guest OS	Kali Linux 2021
Tools	1. Foremost
	2. Autopsy

We have explored the following forensic tools :-

1. Foremost
2. Autopsy

The simplest way to use foremost is by providing a source to scan for deleted files.

Command:
sudo foremost -i /dev/sdb1

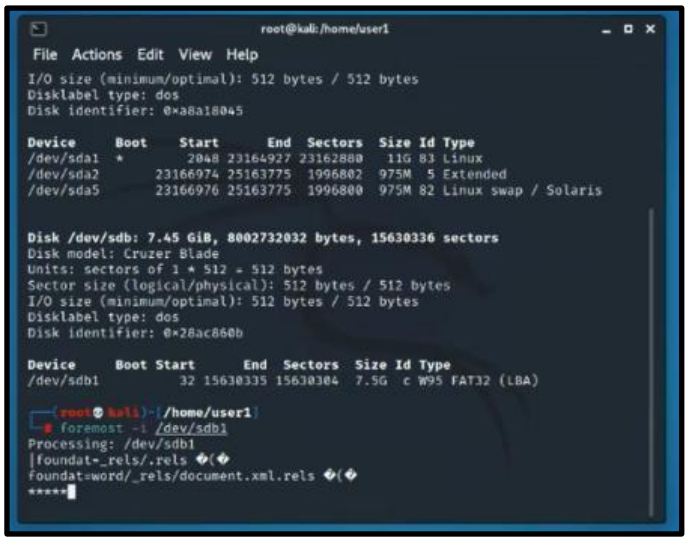

Fig.2 In the above figure using the foremost command we are reconstructing the data. This process may take a while depending on the size of the storage space of the device from which you are trying to extract.

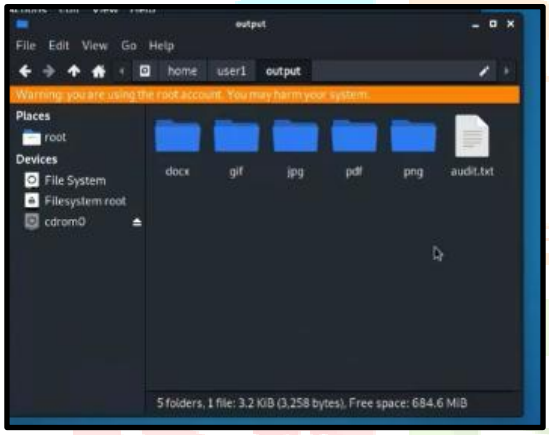

Fig.3 The files that were obtained after acquiring the image of the USB drive were of various types as shown in the figure above. We recovered (.docx, .gif, ,jpg, .pdf, .png, .txt) files from the image of the formatted USB drive.

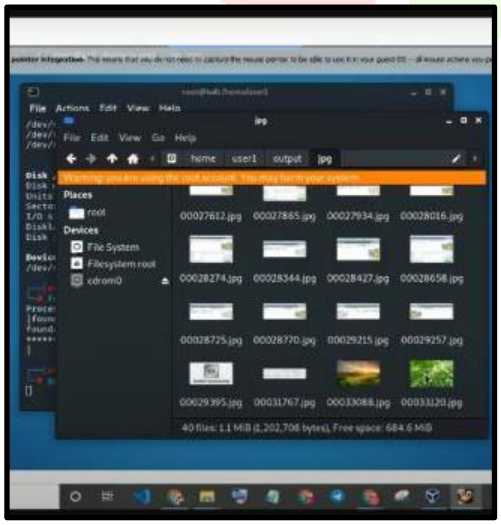

Fig.4 These are the recovered files in their respective formats in the output folder which was created by Foremost.

1. Autopsy:

Data Recovery using Autopsy **:**

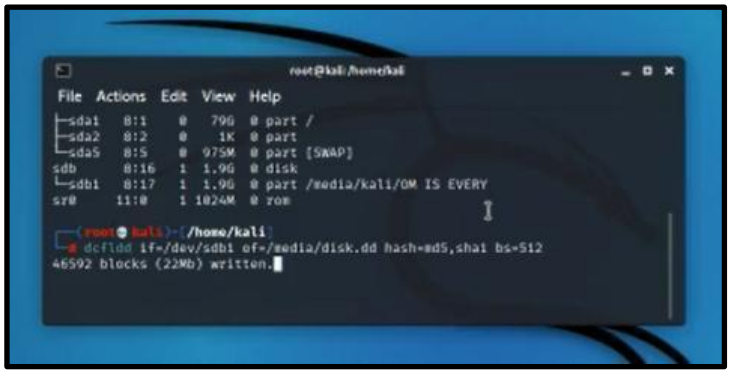

Fig.5 We created an image of the data using the above given command and created a .dd file for it.

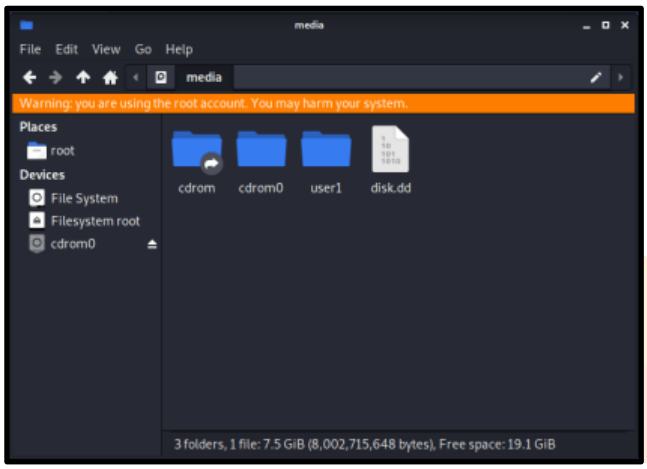

Fig.6 Image of .dd file

To open autopsy:

sudo autopsy

Steps:

1. Open a new case
2. Enter case name
3. Add Image from the location i.e /media/disk.dd
4. Click on analyze
5. Select File Analysis to view the recovered files

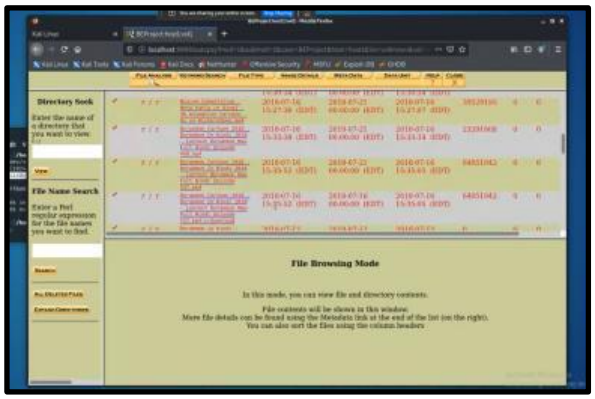

Fig.7 The files that are recovered are shown in red in Autopsy.

Future Scope-

This project can be further used for research in android data recovery development software and may serve as a guide to create new methods of exploration in data recovery mechanisms. This project will help the security organizations to see the loopholes in android applications and further strengthen the software development process. Commercial use of this application will help Android users to recover their lost data because of accidental deletion and make it easy for them to recover it. This field of research is still lacking behind and can be delved deeper so as to find new pathways for data recovery and forensic analysis.

Conclusion-In this, we have studied different ways to recover deleted data from a storage and implemented a combination of few techniques on a removable USB storage.

IV. ACKNOWLEDGEMENT

We would like to take this opportunity to express our gratitude to Dr. Prashant S Lokhande for his guidance and constant encouragement throughout the course of this project. We are immensely obliged for his cordial support, supervision and providing necessary information.

We remain immensely obliged to Dr. Prashant S Lokhande for introducing this topic, and for his invaluable support in garnering resources for us. We are thankful to our college, Pillai College of Engineering for providing us with a healthy environment and well equipped educational facilities that played an important role in keeping us highly motivated to achieve our goals.

V. REFERENCES

[1] Nihar Ranjan Roy, Anshul Kanchan Khanna and Leesha Aneja "Android Phone Forensic: Tools and Techniques" International Conference on Computing, Communication and Automation (ICCCA2016)

[2] Qian Li, Xueli Hu, Hao Wu "Database Management Strategy and Recovery Methods of Android",978-1-4799-3279-5 /14/$31.00 ©2014 IEEE

[3] Shashank Tomer, Aviral Apurva, Pranshu Ranakoti, Saurav Yadav, Nihar Ranjan Roy "Data recovery in Forensics" 978-1-5386-0627-8/17/$31.00 c 2017 IEEE

[4] Qingchao Su and Bin Xi "Key Technologies for Mobile Phone Forensics and Application"
2017 2nd International Conference on Multimedia and Image Processing

[5]Tiwari Mohini, Srivastava Ashish Kumar and Gupta Nitesh"Review on Android and Smartphone Security" Research Journal of Computer and Information Technology Sciences ISSN 2320 – 6527 Vol. 1(6), 12-19, November (2013)

[6] Android Documentation : https://developer.android.com/docs

[7] Android Forensics Blog : http://freeandroidforensics.blogspot.com/2014/08/live-imaging-android-device.html