IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-3, March 2019 E-ISSN: 2347-2693

A Decryption Process for Android Database Forensics

Nibedita Chakraborty[1*], Krishna Punwar[2]

[1,2]Dept. of Information Technology and Telecommunication, Raksha Shakti University, Ahmedabad, India

[*]*Corresponding Author: Nibeindia5.nibedita@gmail.com, Tel.: 7980118774*

DOI: https://doi.org/10.26438/ijcse/v7i3.2326 | Available online at: www.ijcseonline.org

Accepted: 18/Mar/2019, Published: 31/Mar/2019

Abstract— Nowadays, Databases are mostly usable in business applications and financial transactions in Banks. Most of the database servers stores confidential and sensitive information of a mobile device. Database forensics is the part of digital forensics especially for the investigation of different databases and the sensitive information stored on a database. Mobile databases are totally different from the major database and are very platform independent as well. Even if they are not attached to the central database, they can still linked with the major database to drag and change the information stored on this. . SQLite Database is mostly needed by Android application development. SQLite is a freely available database management system which is specially used to perform relational functional and it comes inbuilt with android to perform database functions on android appliance. This paper will show how a message can be decrypted by using block cipher modes and which mode is more secured and fast.

Keywords—Database Forensics,Mobile Device ,Android,SQLite, Modes, Tools

I. INTRODUCTION

Database is an assemble form of interrelated data which is used to fetch, enter and drop the data smoothly and firstly. It is also use to establish the data in the form of a table, schema, views, and reports, etc. However, databases are not only usable by the business applications but also it allows us to store data quickly, smoothly and in chronological manner and is used in multiple forms in our regular life. DBMS is a program which is mostly usable to maintain the database. For example SQL, MYSQL, Oracle, etc. are the most remarkable database available in the market which is applicable various applications. DBMS present a platform to achieve different operations like creating databases, storing data in the databases, altering the data, creating table in the database and many more. DBMS maintain the safety and preservation to the database. In the case of numerous users, it also manages data consistency.

Mobile phone device is not only use to communicate each other but also has various functionalities. Mobile phone data such as SMS, call log and MMS details are all stored in database. The mobile phone data is usually saved in SQLite. Mobile phone criminals can delete confidential information and data. Therefore, mobile phone forensics experts phases problems to decrypt the data stored in SQLite and to recovery actual plaintext message.

In android mobile phone device, SQLite is mainly based on ACID properties docile relational database management system. SQLite is the most famous database form available in various mobile phone devices and is used for frame data storage. SQLite is freeware, and distinct from many other databases, it is compact and offers lots of operation. Android guides SQLite over devoted application programming interface, and therefore programmer can take advantage of it. SQLite databases are the main medium of forensic evidence. The application which used SQLite are mainly reserved at/data/data/<applicationpackagename>/databases.

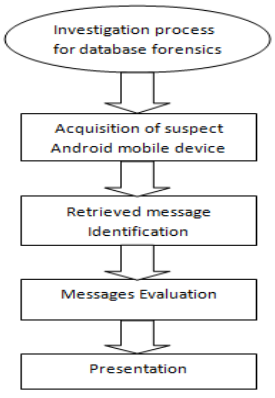

Fig 1: Process of Android database forensics

Database forensics is a discipline which is normally used database information and the data about data to extract criminal action on database structure in and IOT environment. Database forensics rebuilt database operations from log files, data files and folders, and backup storage to recover the database flexibility and found criminal actions. It offers various forensic approach to disclose, gather, preserve, evaluate, and reporting database act. Database forensics is used for investigates who is accessing the database and what behaviour of activity he/she are performed. The device which is applicable to access data using the mobile database can be mobile phone device, tablets, laptops etc.

II. RELATED WORK

In [1], the authors did a detailed study and mentioned one correlation of the execution hours for three types of algorithms based on the encryption and decryption keys. For this correlation, a Java application is develop and a testing a application to check the database is created. This testing application permits only that user, who has an assigned role to see the data from individual columns in a normal encoding format. The most influential part is the stage of the security of the comparison. Another great part is the key authority as decoding can be done only using a proper key during the encoding process.

In [2], the authors mentioned the basic database forensic investigation procedure, which is designed by analysing some appropriate digital investigation process models that have developed and analysed by studying which is based on basic investigation process. The output of this research indicates the certain procedure of the generally shared process; it will be understandable by the new users and also to deliver as primary elementary concept of advancement of the process. Therefore, they proposed this type of process model which will be helpful to solve the issue and complications related with the database forensics in normal. They mention that their future work will be on representing the details of all the procedures of the investigation phases of common process model.

In [3], author studies the approach of data gathering and evaluating the functionalities of the mobile device forensic system. During that time, in order to contract with the database outline, authors suggested one decoding process and the data extraction process which is based on SQLite database, which is the most influential part of this paper. This paper builds the whole framework of the mobile device forensic system, evaluates its working ethics, and recommends the forensic process of the framework. For SQLite database, the paper suggests one decryption method and a data recovery method which executes well in the investigation. Further, this study of Data Corporation and fragment restoration in the paper is problematic, which will be improved by author in the future.

In [4], the authors did a detailed study and provide a method to retrieve the blackout messages (SMS) by evaluating the SQLite file format and consign the way of data records. The output of this paper shows the process of data extraction which is capable for retrieving data mainly text messages for iPhone devices.

III. BACKGROUND

Android mobile devices have become the trendiest in modern era among the customers for their benefit and advanced functionalities. From the forensic prospect, that means an android mobile device could possibly contain a property of information related to an investigation, it includes SMS, MMS and call logs. The data recovery could be done in android mobile device by the two ways:

a) Using manual extraction tools(ADB)
b) Using commercial tools achievable in the market

Log cat is a command based tool which saved a snapshot of the log of a system messages, including error messages when the device throws an error and messages that we have written from the application with the log part. To access the database, the mobile device should be in rooted mode as the /data/ directory can only be read by the android system, and apps can also read their own /data/data/<package name> directory only. Just for simplifications, the SMS can be altered and reconstruct application which uses an application programming interface to get back the SMS messages via the messaging application, but for that the need is there should be the READ_SMS permissions.

There are a vast various tools present in the market to digital forensics investigators so that they can solve the specific cases and problems related to the database extractions. Of this tools, a class of them offers for reconstruction and withdrawal of information and data from the databases. When we did a study on market analysis, we have found that there is very less to none code related to the effective functionalities and utilities of such tools. Some tools are described below which are used to extract data in data forensic field.

Xplico: Xplico is a freeware, menu driven interface network forensic tool to analysis the network for Unix/Linux workstation. It supports protocols such as address resolution protocol, point to point protocol, VLAN trunking protocol, IPv4, IPV6. Transmission control protocol, domain name servers, Facebook chat, and internet relay chat. It is mainly applicable to retrieve the application data enclose from an internet traffic transit or packet seizer. Xplico is a packet capture decryption process that works in connection with a

packet seizer tool. After pcap files are seized, the decryption translates the pcap files and recovers network action such as email, VoIP and http. It is also used to find data details from data basis and files uses SQL and MYSQL files.

Kernel Data Recovery: it is an open source, menu driven interface based database forensic tool for windows workstation. It is mainly used to recover deleted data or depraved data from the databases such as MS SQL server, MS Access, database file and MYSQL etc. kernel data recovery mainly offers three types of data recreation options that are quick scan, extensive scan and file tracing. Quick scan is the most speedy recovery choice that only used to investigation a case for blackout data and damaged file. Extensive scan looks the whole drive for all blackout and present saved files on a drive. File trace performs a deep scan of the total drive to extract the bulk of recoverable data possible from the workstation. Normally kernel data recovery investigates as a extraction tool, even it can be usable as recovering loss table data, stored procedures and trigger, virtual table and primary keys. This tool allows the investigator to store the recovered databases as a new database or as an existing database.

SQL command: SQL command provides execution the queries, transact SQL sentences and SQL server scripts using the command line. SQL command is an impressive tool for investigation as well as process login. It can be used as ":out " and ":error" command. SQL command is a smooth, very powerful scripting status that helps with the automation of several task related to SQL server. SQL command is an advancement of the osql and isql command line utilities. The advantages of SQL command are (1) it's simple to mix the SQL in a .bat file. (2) It can run in any operating system platform so it is very platform independent. (3) Its very simple to pass command line arguments to SQL file using SQL command.

One big disadvantage is of SQL Command tool is its lacks to offer higher user friendly documentation via html or another format.

IV. PROBLEM STATEMENT

As we already mentioned in the related work, there are few research methodology already introduce previously for running out database forensic investigation on android mobile phone devices which is related to file system examination, investigation of diverse chat application, analysis of various messaging application. But, with the latest technology of android operating system introduce often and also with nonstop updates in the application, it is very crucial that regular research on the modification be tested. However, the forensic investigation of android database includes different forensic analysis method like manual extraction or logical extraction, the original text messages where not possible to be recovered due to the encrypted quality. In this paper we are going to introduce a database forensic methodology with different decryption modes to decrypt the messages and among those decryption modes which modes are more secure and fast will be introduced.

V. METHODOLOGY

The research is observed by using android mobile phone devices with variable android operating system on them. Research can be carrying on the both rooted and un-rooted mobile devices. This research not only elaborates the data storage on the file system but also gives the classification of the applications for which we can recover the data without having super user privileges (rooted device).
The following are the important specification in this paper:

Table 1: Hardware Specification

Android Mobile Device	Operating System Type	Types of Device
Redmi Y1	Android v7.1.2(Naught)	Un-rooted
Yu Yureka Plus	Android 5.1.1	Rooted
Sony Xperia M	Android 4.1	Un-rooted

A)While using ADB tool, attached the seized android mobile phone device to the forensic workstation by using USB cable and make sure whether the USB debugging on the android devices was enabled or not, so that the device can be identified by ADB tool and it allows accessing the android device.

B) Once the device is detected in the forensic workstation by ADB tool, check whether the seized mobile phone device is rooted or un-rooted. Un-rooted device can be temporary rooted and extract data from the database by using various forensic tools but this method can modify the data of the seized mobile phone device hence it is not recommended.

C) The backup command (adb backup –all –f <filestoragelocation>.ab) is used to extract the data from the un-rooted android device and pull command (adb pull /sdcard/forensics/-a) is used to extract the data from super privilege mobile phone device.

Decrypting Database:
The SQLite database of the messaging section of the seized android mobile phone device is saved in com.android.providers.telephony/smsmms.db and this database is encrypted by using the SQL cipher. To convert an encrypted database to unencrypted database, we have to open up the database first then apply the following commands:-

Table 2: commands used for decryption using SQL cipher

Purpose	Commands
To create a new database	ATTACH DATABASE 'forensicdatabase.db' AS encrypted 'secret';
Recreate schema in the new created database	CREATE TABLE forensicdatabase.t1(a:b);
Copy the data from the existing table to the new table in the encrypted database	INSERT INTO forensicdatabase.t1 SELECT * FROM t1;
	DETACH DATABASE forensicdatabase;

Block Cipher Modes:

ECB (electronic code book) mode:

It is the uncomplicated mode of encryption. Each plaintext block of the message is encrypted individually. Therefore, each cipher text of the message is decrypted separately. The disadvantage of encryption with ECB mode is encrypting a bitmap image (.bmp file). Even a strong encoding algorithm used with ECB mode cannot fully blur the plaintext. A message which is encoded with the ECB mode can be enlarged up to a size which is same to the integer multiple of the single length of the block. The ciphers used in the ECB mode are too much vulnerable to playback attacks.

CBC (cipher block chaining) mode:

This mode of operation includes adding XOR with each plaintext block of the message up to the cipher text block of the message which was formerly composed. This output is then encoded by using the cipher algorithm. Therefore, each cipher text block of the message builds upon the former one. The primary plaintext block of the message is combining with XOR to a random initialization vector. The vector is always the equal size as a plaintext block.

While doing decryption of a cipher text block of the message, we should combine XOR the result data which is received from the decrypting algorithm to the former cipher text block. The initialization vector is developed in constantly by the sender. While communication it will be integrated with cipher text block of the message, to pass the decryption of the message by the receiver.

Disadvantage of this mode is encryption done in CBC mode is only performed by using single thread.

The research work is executed on all the above mentioned android based mobile phone device separately and outputs are used for further research. This is the basic methodology used in this research paper, to extract the forensics artefacts of the message than decrypt it using different decryption modes available in the cryptography and assume the conclusion that which mode is more secured to decrypt the message.

VI. CONCLUSION AND DISCUSSION

In this paper we have to conclude that CBC mode is more secure than ECB because in CBC, we are using random initializing vector. And in the forensics investigation process, ECB mode can be easily decrypt the database and recovered it. When we are using CBC that time we have to face some decryption problem while trying to recover the database. So, If one bit of the plaintext message is impaired, then the cipher text block of the message will be also impaired and it is never been achievable to decode the cipher text message which was acquired from the plaintext msg. In case that the cipher text of the message bit is impaired, only two collected plain text block of the message will be impaired. And then it may be achievable to extract the data from the android mobile phone device.

REFERENCES

[1] Database encryption using asymmetric keys: a case study, AlexandruBoicea, Florin Radulescu, Ciprian-OctivianTruica, CritinaCostea, 2017 21st International Conference on Control System and computer science.

[2] Common Investigation Process Model for Database Forensic Investigation Discipline, Arafat Aldhaqm, ShukorAbdRazak, SitiHajar Othman, 1st ICRIL-International Conference on Innovation in Science and Technology (IICIST-2015).

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

[4] Research on the Data Recovery Method of Deleted SMS for iPhone, ZHANG Kai-xiang; ZHOU An-min, Modern Computer 2015.

[5] Cryptography and Network security, Tata McGraw-Hill education 2003, Atul Kahate.

