Digital Forensics: Smart Aid for Digital Evidences

Mukul Kumar Srivastava
HMR Institute of Technology and Management, Hamidpur, Delhi India

Devansh Chopra
HMR Institute of Technology and Management, Hamidpur Delhi India

Vaishali
Dept. of Computer Science HMRITM, Delhi India

Abstract **--- In the digital era, most of the users have suffered from a loss of data, unauthorized modification of data which led to the origination of Digital Forensics. It is the application of science and technology used to find criminal and obey civil laws. It is mainly used for the investigation of the crime and is governed by certain legal standards of evidence and procedure of crime. This paper contains manually tested tools used for extraction of data from any storage device (it doesn't matter if a device is corrupted or blank), after data recovery, the recovery folder contains audit file from the help of this we have summarized the result of all types of data recovery and their metadata too. During the criminal investigation, the forensic scientists have to collect the Digital evidence, which might be, stored any digital device used by the suspect or victim that has been seized by investigators. The literature relevant to Forensic Science, as explored in this paper, focuses on the various categories of forensics, anti-forensics, architecture of various mobile operating systems like IOS and Android. It also throws light upon various categories of Digital Forensics and the digital investigation tools, which can be used to trace the criminal activities of a suspect involving the use of any digital device that is capable of storing data in it. It also contains the snapshots of the data recovery performed using the KALI LINUX (FORENSICS MODE).**

Keywords*—Digital forensics, Smartphone Forensics, Anti-forensic and Forensics Science.*

I. INTRODUCTION

In Digital period, it's very difficult to save our personal information to other and catch those who may miss use of technology for resolving this issue we use a term **Digital Forensics.**

Digital Forensics: It's makes involve through which we can able to consider any legal activity. Forensic is user to detect and prevent data communication from any kind of crime based on digital stored evidence. Mobile Forensics is directly related with Digital Forensics. We can do digital forensics through presence of network and mostly use Internet.

Internet: The Internet, allowing users to exchange information like Audio, Video and compressed format too. This type of communication where our information is shared broadly through Instant message (IM) just like SMS. Forensic identify specific objects from the trace evidence, which is left on the time of accident. In terms of forensic IM play important role that become heavy source of evidence because of analyzing data. Mobile forensics is a new type of digital evidence where the information can be easily stored and retrieved. **Cybercrime** is any illegal activity that is done through computer and any network connected device such as Smartphone it has the unusual way of working through which victim and the perpetrator may never come in touch directly they just make distance for doing his task. In present time where internet is the one of the common think which share data from hand to hand become faster and more stable in particular Connection in (2G), (3G), (4G) connection [1].

Last 7-8 years' online communication continuously increase his marketing. In today market, numbers of Android operating system exist Like Google's Android and Apple's iOS. These kinds of operating systems create major challenges for investigators for extraction data on it just because of complexity [2]. IOS contains four layers in which Layer one from which operating system provide direct access to main memory and kernel of the operating system. Layer second contains basic services written in C language. Layer three handles video, audio, image and graphics. Last layer provide interface between user and application [3]. Other hand android architecture [4] consists of five layers, applications layer this layer written in java, theses application are generally used by third party companies. Application programming interfaces available (APIs) that makes interface with the file system.

A. Smartphone Forensics

Smartphones become necessary part of our daily lives. From this we can do anything from smartphones like MS office, Document reader, Entertainment (both audio & video), Chatting with friends anywhere in earth and also find his/her current location using GPS. There is also storage Capacity in two parts internal (which is fixed in size) and external (adding external micro SD card and size can be varied) and there processing capabilities. The storage in Smartphones such as audio, video, images, documents, archives, emails, videos and sort messages (SMS) can be able to access remotely if and only if device is connected with internet this is the major challenge in forensics investigation. Whenever we dealing with smartphones, then there are three way of data storage first the SIM card, where all contact information and SMS. In the device memory, which stores overall user created data like images, video, massages, MMS and setting etc. We can store Applications such as Truecaller, Google Map, Twitter, WhatsApp and many more with their log details, which is also portable.

B. Smartphones Anti-Forensics Challenges

Anti-forensics, this technology is generally used to defeat forensic investigation. In past years, anti-forensics for mobiles makes more challenging. Attackers could hide digital evidence. Anti-forensics involve for taking personal and that sensitive information leaking them causes a high risk [5] [7].

Smartphone forensic investigators focus on operating system layers, the third-party developers can be able to access particular OS layers for application and that makes erase digital information. In market, few application present through slowdown logs and massages to hide digital signature from crime take place. This is the complexity of anti-forensics job of forensic analysis [4] [6].

II. FORENSIC SCIENCE

The ancient world lacked practices of standardized Forensic Science. It was in the early 16th century in Europe that forensic science was originated. It is the application of science and technology to criminal and civil laws. It is mainly used for the investigation of the crime and is governed by certain legal standards of evidence and procedure of crime.
During the criminal investigation, the forensic scientists have to collect the evidence. They preserve evidence and analyze it. Forensic scientists may have a laboratory to perform their tests on the collected evidence and they may work either for the defense or for the prosecution.
The reports of forensic scientists regarding the collected evidence play a major role in decision making as the collected evidence has been completely analyzed and the findings of analysis may aid to establish the guilt or innocence of the potential suspects which will help the judiciary to take a better decision by considering the evidence found at the crime scene and hence the criminal cannot escape from the punishment.
Hence, Forensic analysis of the evidence has become really important these days in the investigation of any criminal case.

A. Branches of Forensic Science

There are various branches of Forensic Science and a few are mentioned below:

1.) **Forensic Anthropology**: It is the study of social relationships and the human body.
2.) **Forensic Chemistry**: It is known as the study of the properties of matter, including its structure and interactions between them.
3.) **Forensic Entomology**: It is known as the study of bugs.
4.) **Forensic Mathematics**: It refers to finding patterns and relations in crime scenes and evidence.
5.) **Forensic Nursing**: It is the branch of forensic science that helps the victims of sexual assault.
6.) **Latent Print Identification**: It is the branch that deals with identification of latent prints (fingerprints, footprints, palm prints etc.).
7.) **Forensic Toxicology**: This branch deals with the studying of different poisons.
8.) **Digital Forensics**: This is the branch of forensic science that incorporates the recovery as well as the investigation of the data found in digital devices found at the crime scene.
9.) **Computer Forensics**: This is a sub branch of Digital Forensics and deals with the investigation of data stored in computers.

B. Digital Forensics and its branches

Digital Forensics is branch of the forensic science that is used to recover and investigate the data stored in various kinds of digital devices found at the crime scene. The period of growth of this branch was between 1980s to 1990s as the frequency of computer related crimes like unauthorized deletion and modification of the data of a computer system, cyber bullying, cyber stalking and child pornography etc. had increased a lot during this period.
The digital forensics of the evidence faced many problems in 1980s like the risk of modification of data during the investigation, which could lead to the claims of tampering of the evidence, due to the lack of proper forensic tools. Hence, in the early 1990s there were many forensic tools developed to counter this problem. Examples of forensic tools developed during the early 1990s are IMDUMP (by Michael White), SafeBack (developed by Sydex), DIBS etc.

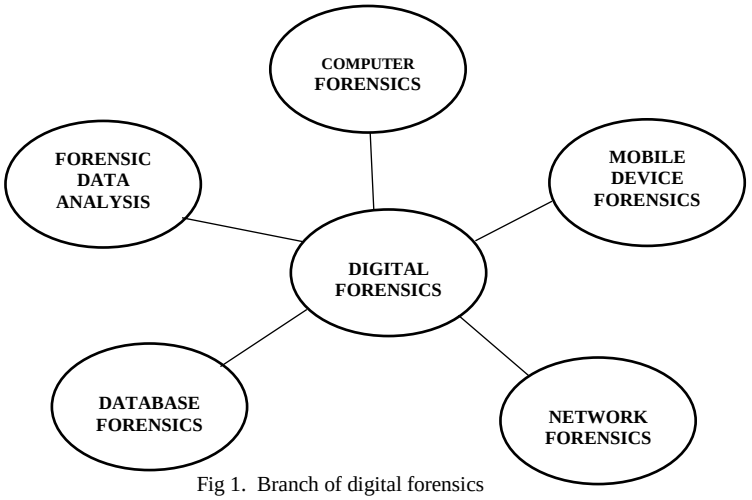

Fig 1. Branch of digital forensics

Various branches of Digital Forensics are described as follows:

1.) **Computer Forensics:** Its goal is to find and study the data retrieved from the digital devices that have computation power and onboard storage available with them like computer systems, embedded systems, static memory (USB pen drives).
2.) **Mobile Device Forensics:** It is a sub-branch of digital forensics, which has goal of recovering the digital evidence from mobile devices.
3.) **Network Forensics:** It is the sub-branch of digital forensics that is dedicated to monitor and analyze the traffic of a computer network to gather the evidence and is used for both LAN/WAN.
4.) **Forensic Data Analysis:** This sub-branch has a goal to examine the structured form of data to find and analyze the fraud activities, which may result in financial crimes.
5.) **Database Forensics:** The sub-branch has an aim of forensic study of the database and its metadata. In this branch log files are analyzed in order to find out the digital evidence.

C. Digital forensics process

Digital forensics process is a scientifically recognized forensic process used for digital investigations of criminal cases. This process is used for computer and mobile forensics. There have been multiple attempts to develop a process model for the digital forensics process but till now there is no generalized process that is accepted universally. A few of models are mentioned below:

1.) The Abstract Digital Forensic Model (Reith, et al., 2002)
2.) The Integrated Digital Investigative Process (Carrier & Spafford, 2003)
3.) An Extended Model of Cybercrime Investigations (Ciardhuain, 2004)
4.) The Enhanced Digital Investigation Process Model (Baryamureeba & Tushabe, 2004)
5.) The Digital Crime Scene Analysis Model (Rogers, 2004)

The digital forensics process can be divided into three steps:

1.) **Acquisition:** In this step, the forensic experts take the seized digital device and replicate the device's volatile memory (RAM) i.e. they try to create a sector-by-sector copy of the device's memory. This is done to ensure that during the investigation there is no modification caused to the original device that may lead to the tampering of the evidence.

2.) **Analysis:** It is a very important and crucial step of the whole process as it is the step that involves the extraction of all the important information, collection of the digital evidence from the captured image of the device. This step is also referred to as the in-depth search for the digital evidence and hence, plays an important role in the whole investigation process. In this step, the deleted files are also recovered to find important information.

3.) **Reporting:** After the investigation is complete and the recovered evidence has been analyzed completely to reach to certain conclusions then all the collected data and conclusions have to represent in a written report. Hence, in this step we convert all the collected data and conclusions into report.

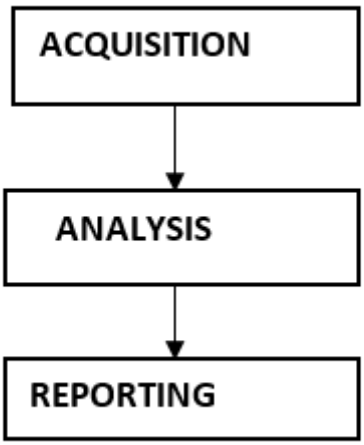

Figure 2: Digital Forensic Process

D. Limitations of digital forensics

The main limitation to a forensic analysis is that the device may contain the data in encrypted form. This means that the data could be in a encoded form that it could only be accessed by authorized party(person) with the help of a key. This encryption may disrupt the digital investigation process.

E. Digital forensics tools

Digital forensics is a very important branch of computer science in relation to internet and computer related crimes. The goal of Digital forensics is to perform criminal investigations by using the evidence that has been recovered from the seized device and to draw the conclusions on the basis of the analysis of the digital evidence.

For better investigation, developers have created many digital forensics tools. Police departments and investigation agencies based on different factors including budget and available experts in the team select these tools.

These computer forensics tools can be classified into various categories:

1. **File viewers**: These types of tools are used to view different files of various formats.
2. **Registry analysis tools**: These types of tools are used for clean unwanted or useless registry in device.
3. **Network forensics tools**: These types of tools are used for wireless network detector, sniffer system. Protocols supported: **SIP**, HTTP, **SMTP**, **TCP**, POP, **UDP**, IPv4, IPv6.
4. **Disk and data capture tools**: These types of tools are used for investigation on Digital data which is responsible for particular crime.

5. **File analysis tools:** These types of tools are used for check the file type in our database for trace system and library files.
6. **Email analysis tools**: These types of tools are used for check content present on email attachments like image, document file, archive etc.
7. **Mobile devices analysis tools**: These types of tools are used for analysis the data present in phone storage like images, massages, documents, MMS massage etc. This tool is a basis of Digital Forensics.
8. **Internet analysis tools**: These types of tools are used for analysis the content access through Internet. It's generally checks the data incoming to outgoing.
9. **Mac OS analysis tools**: These types of tools are used for the analysis of the digital devices that use Mac OS like MacBook air, iPhones etc.
10. **Database forensics tools**: These types of tools are used to analyze the contents of database and their metadata.

A few popular and important digital forensics tools are listed below:

1.) XRY

This forensics tool developed by Micro Systemation. XRY is used to analyze and recover crucial data from mobile devices. This tool contains hardware device & the software. That hardware is used connects mobile device to pc and the software programs is used to perform data analysis from the device & also used for extract data. In present time, this tool is mostly comparable with all Android device for data recovery including BlackBerry and iPhone. This tool is also use for gather all deleted information like massage, call record, text massage and images.

2.) Mobile Internal Acquisition Tool (MIAT)*:*

MIAT is a digital forensics tool that is used for mobile device analysis. This is the one of the great tools, which are used for the recovery of deleted SMS.

3.) ***via Forensics Forensics***

viaExtract, it makes a way where we can extract user data from mobile device, crack passphrases/PINS and also can able to examine images from storage both SD and EMMC. **viaForensics** compatible with all latest Android smart phone and mobile device too.

4.) BitPim*:*

In BitPim it allows user to view and data manipulation on CDMA phones.

5.) Cellebrite UFED

Cellebrite's UFED, this tool present a unified workflow that allow us investigation and examiners, it first responders for collect and then protect data, speed and accuracy is depends upon demands without any compromise from one too another. UFED Pro Series is developed on the basis of forensic investigation and examine who's mainly focus on up-to-date device data and their extraction and then also support decoding that handle the influx of new information sources. The UFED Field Series is designed for workflows between field and lab and also making it possible to view, access or share mobile data via in- laptop, car workstations, tablets or a self-service [8].

6.) iPhone-analyzer

The iPhone Analyzer, that's allows us to make forensically investigate and also used for recover data within an iOS. This tool is compatable to works with iTunes and all latest iOS. In iPhone Analyzer, this is a security tool, which is based on Java based, works on major OS. This tool is use full for recover "deleted" data and it also provides to browse the file structure and analyze jail broken over directly SSH.

7.) Katana Forensics' Lantern Lite Imager

This tool is best supported for IOS devices like iPod Touch, iPhone and iPads. This tool allows users to auditing, analyze and extraction of data from device.

8.) Oxygen Forensic Suite:

Oxygen Forensic Suite, that software is used to gather evidence from a mobile device that support for our case. This tool is used to gathering information (like manufacturer, IMEI number, OS and serial number), messages (emails, SMS, MMS), recover deleted messages, contacts, call logs. It also provides to access and then analyze device all data and their documents. At the end, it generates easy to understandable reports, which makes better understanding regarding mobile device.

9.) Digital Forensics Framework:

Digital Forensics Framework is a popular framework used for digital forensics. It is an open source. It can be used by the digital forensics experts for the digital investigation or it can also be used by a non-experienced person for their use. It can be used to access the remote or local devices, forensics of Windows or Linux OS, recovery hidden of deleted files, quick search for files' meta data, and various other things. It comes under GPL license.

10.) Open Computer Forensics Architecture

Open Computer Forensics Architecture (OCFA) is a distributed open-source computer forensics framework. It was built for Linux platform and it uses PostgreSQL database for storing various data related to the investigation. It was developed by the Dutch National Police Agency for digital forensics process. It comes under GPL license.

11.) CAINE

CAINE stands for Computer Aided Investigative Environment. It is an Italian GNU/Linux live distribution. It provides a complete forensic environment that is designed such that it can integrate existing tools and software modules. It offers a user-friendly GUI. The main design objectives of CAINE aim to guarantee is an interconnected environment that can support the digital investigation expert during different phases of the digital investigation.

12.) X-Ways Forensics

It is a popular and advance platform used for digital forensics examiners. It can run on every available version of Windows. It works very efficiently and requires very less resources. A few features of this tool are listed below:

- Cloning and imaging of Disk
- It has the ability of reading file system structures inside different image files.
- It supports most of the file systems including FAT12, FAT16, FAT32, NTFS, Ext2, Ext3, Ext4 etc.
- It can automatically detect deleted or lost hard disk partition.
- It consists of various techniques used for data recovery and powerful file carving.
- Memory and RAM analysis

13.) Computer Online Forensic Evidence Extractor (COFEE)

Computer Online Forensic Evidence Extractor or COFEE is a tool kit developed for digital forensics. This tool was developed by Microsoft to collect the digital evidence from Windows systems. It can be installed on an external hard disk or USB pen drive. To analyse a computer you just need to plug in the USB drive and it will start the live analysis of the computer system. It consists of GUI for using various tools and it consists of around 150 different tools. It is fast and can perform the whole analysis in as less as 20 minutes. It is a really efficient tool that can be used for digital forensics.

14.) EnCase

EnCase is another popular multi-purpose forensic platform with several tools for various areas of the digital forensics process. It is a fast tool that can rapidly collect important information and digital evidence from various devices. This tool does not come for free and has to be purchased. The license for using the tool can be purchased for $995 approx. It comes with an additional benefit which allows the tool to produce a report based on the evidence.

III. CHALLENGES FACED DURING FORENSIC

In any kind of forensic examination on Smartphone is based on method, which take most of part in Forensic. During analysis is based on environment, equipment and techniques to be used on the basis of cardinal rules of computer forensics. We have option to make analysis on virtual android device such as YouWave its virtualization platform [10]. It supports internal storage as VirtualBox storage file [12]. It supports Android v. 4.0.4. There will be not any kind of update happened in original data in both original and virtual device.

A. Android Challenges in Forensics

Whenever android version is get updated then API level also get update from this security also makes barriers to access data. We are mainly focus analyzing data from peer to peer massage transfer where first we have to locate and then extract data (file and folder) where the artifacts mixed with the application stored in internal storage of phone. But In forensic the present database is in Encrypted form so it's hard to extract data from that folder. Most of time users is connect to internet so they regularly update their programs that's makes hard to forensic analysis for understand new updates to ready to deal with this old method or tool only. Update creates more Challenges for Law of Enforcers and forensic investigation provided by the evidence in court of law [2006, Al-Zarouni, Marwan].

B. Basics Detail Of Android API level

First, we divide necessary Android smart phone detail into numbers of fields (including "Android Platform Version", "API level", "Cumulative Distribution"). On the basis of that, we have proper result of phone version related of Cumulative Distribution, after that we can analysis the market trend of using smartphone with respect to their version. Android phones have three different details shown below:

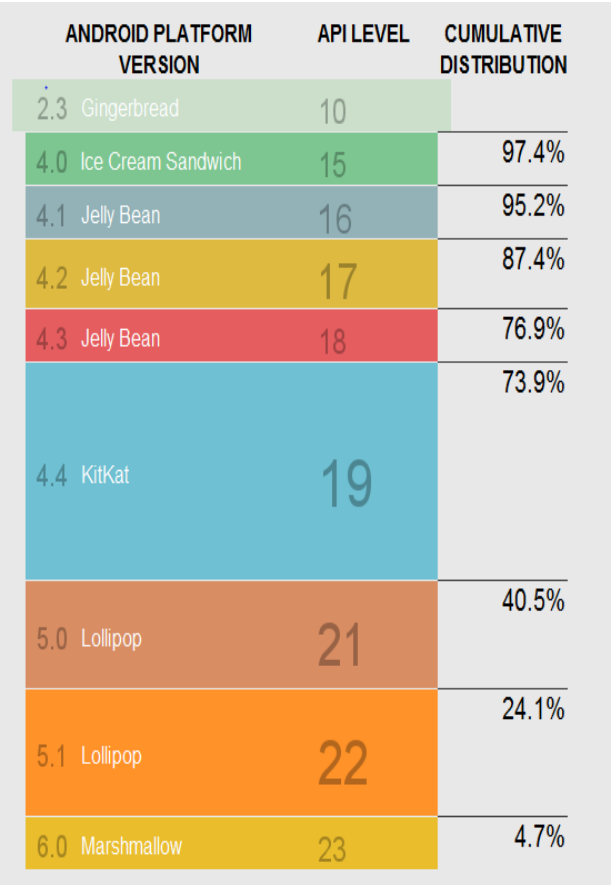

Figure 3: Android Platform with API Level

IV. FORENSIC ANALYSIS OF WHATSAPP MESSENGER

WhatsApp Messenger is a free, cross-platform instant messaging [9] application for smartphones. It was released in the year 2009, 8 years ago. It uses end-to-end encryption to provide more security to its users. It uses internet to send text messages, images, GIFs, voice notes, contact cards, documents, location, videos and to make voice and video calls. It is a popular instant messaging application [11] with more than 1 billion user base as of February, 2016.

Table-1 Features of WhatsApp

1. Send and receive text messages (Text Chat).
2. Send and receive images.
3. Send and receive video clips
4. Send and receive audio clips
5. Send and receive gifs
6. Voice calls
7. Video calls
8. Group chats
9. Sharing contact information
10. Sharing documents, PDFs etc.

These days each and every smartphone owner uses WhatsApp Messenger to share information, jokes, chat with friends and relatives. Many important data are shared through WhatsApp. WhatsApp is used by people of different age groups. Hence, the analysis of WhatsApp of a person can help in revealing many important information regarding him. It can help the digital investigators to collect the digital evidence from one's WhatsApp conversation.

WhatsApp artifacts can be very useful for the WhatsApp forensic analysis. WhatsApp contacts, attachments, messages can be very valuable to the forensic experts wanting to recover evidence for different types of investigations. Whether the forensic experts are analysing the mobile device of a victim or a suspect these artifacts can be very useful for them and can help them solve the case.
Like many other applications WhatsApp also uses SQLite database to store all its data. The location and structure of database differ from platform to platform.

Table-2 WhatsApp database structure for Android

File Name	Table Name
1.msgstore.db	(I) chat_list (II) messages (III) sqlite_sequence
2.wa.db	(I) android_metadata (II) sqlite_sequence (III) wa_contacts

In **Android**, the structure of database consists of two database files as shown in **Table-2**. These two databases comprise of various tables that contain different kinds of information. The description the two databases and its tables is given below:

1.) msgstore.db: This database file stores data related to chats, attachments, and the contact details of those person with whom the user has had a conversation but it does not contain details of all the WhatsApp contacts of the user for that we will have to refer to **wa.db**. This database contains two main tables namely:

(i) chat_list: This table is responsible to collect the contact information of all the persons that the user has had a conversation with. However, it does not store a complete list of the user's contacts.

(ii) messages: This table is responsible for storing all the data regarding the chat/conversation of the user. In this table, the fields for attachments will contain a null entry with a thumbnail and link to the photo/image being shared and the attachments are directly stored into the database file **msgstore.db**. Some more details that are stored in the table are:

1.) the contact's phone number,
2.) message contents,
3.) message status,
4.) timestamps, and
5.) Any details/message sent with the attachments.

2.) wa.db: The **wa.db** stores a complete list of a WhatsApp user's contacts including phone number, display name, timestamp, and any other information given upon registering with WhatsApp. This database contains a table **wa_contacts** which is used to store the user's contact details. The data in this table comes from two different locations i.e. WhatsApp System &Phonebook of the device

Data coming from WhatsApp System:
This data comprises of information like the user's unique sequence id, WhatsApp ID, photos, thumbnails, timestamps etc. This data is stored in the various fields of the **wa_contacts** table.

Data coming from the Phonebook of the device:
This data comprises of information that is stored in the phonebook of the user. It contains all the contact details of user's contacts like phone number, display name, raw contact id etc.

Table-3 Fields of wa_contacts table used for entering the data that comes from WhatsApp System

DATA COMING FROM WHATSAPP SYSTEM
FIELD NAME
Id
Jid
is_whatsapp_user
unseen_msgcount
photo_ts
thumb_ts
photo_id_timestamp
wa_name
status
sort_name

In **IOS**, the database structure of WhatsApp is a little complex than the database structure it has in android. It contains only one database file but it comprises of a total of **12 tables(**as shown in **Table-3)** which make it more complex. The name of the database is **ChatStorage.sqlite.** The location of the database is :

net.whatsapp.WhatsApp/Documents/ChatStorage.sqlite

In the ChatStorage.sqlite the data regarding contact details, messages , attachments are stored in different tables.

1.) ZWACHATSESSION and **ZWASTATUS** have the contacts.
2.) ZWAMESSAGE and **ZWAMEDIAITEM** collect the details on the messages, attachments, sender, recipient, timestamps, geolocation data, and the path/location of any media being shared between two contacts.

Table-4 WhatsApp database structure for IOS

File Name	Table Name
1.ChatStorage.sqlite	(I) ZWABLACKLISTITEM (II) ZWACHATPROPERTIES (III) ZWACHATSESSION (IV) ZWAFAVORITE (V) ZWAGROUPINFO (VI) ZWAGROUPMEMBER (VII) ZWAMEDIAITEM (VIII) ZWAMESSAGE (IX) ZWAMESSAGEWORD (X) ZWASTATUS (XI) Z_METADATA (XII) Z_PRIMARYKEY

NOTE: All the database files are in available onli in an encrypted format. WhatsApp uses end-to-end encryption technique to provide its users more security. WhatsApp uses different extensions to encrypt the database files like .crypt5, .crypt7, .crypt8 etc. as of now it has been using .crypt12.

To retreive all the details stored in the database in order to find out the digital evidence we need to decrypt the database files.

V. KALI FORENSICS MODE

Kali Linux contains several hundred of tools which are used for doing many security tasks such as Computer Forensics, Security Testing, Reverse Engineering and Penetration Testing. Kali help to examine data from any- where data can store like Hard Drive, USB Drive and Android device from this it plays important role in Digital Forensics. Here we use Kali Forensics mode for doing data extraction from formatted disk, corrupted disk and also make isolated disk. It is shown in fig.4 that Kali provides tools that help recover file from damage & rebuild data files and also makes perfect copy of storage.

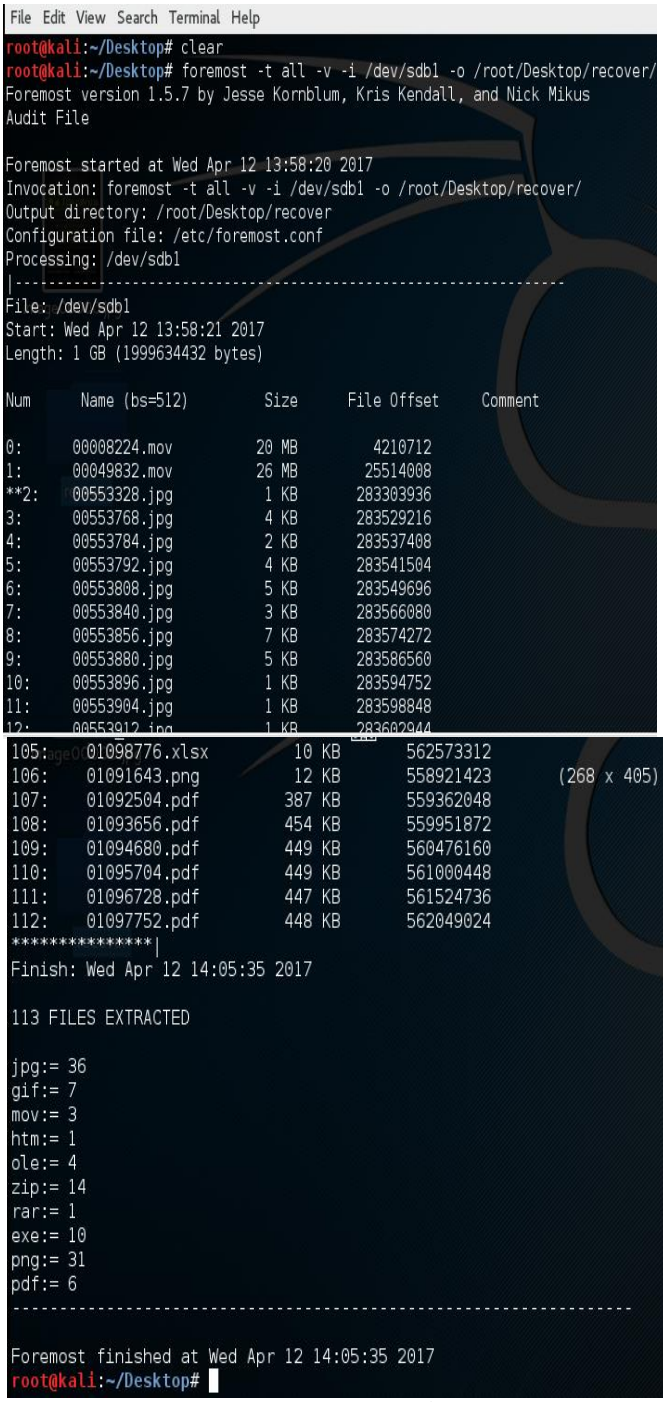

Figure 4: Recover all deleted data from storage.

REFERENCES

[1] E. Casey, *Digital Evidence and Computer Crime*, 2011.
[2] A. Hoog, *iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices*, Syngress Publishing, June 2011.
[3] A. Distefano, G. Me., and F. Pace, "Android anti-forensics through a local paradigm," *Digital Investigation*, vol. 7, pp. S83-S94, August 2010.
[4] M. A. Caloyannides, *Computer Forensics and Privacy*, ArtechHouse, 2011.
[5] A. Hoog. (November 2010). Independent research and reviews of iPhone forensic tools. via forensics. [Online]
[6] Rolfe Winkler. WhatsApp Hits 400 Million Users, Wants to Stay Independent. The Wall Street Journal - Digits, Oct. 2013.

[7] Vacca, John R. *Computer Forensics: Computer Crime Scene Investigation (Networking Series) (Networking Series)*. Charles River Media, Inc., 2005

[8] De Vel, Olivier, et al. "Mining e-mail content for author identification forensics." *ACM Sigmod Record* 30.4 (2001): 55-64.

[9] Garfinkel, Simson L. "Digital forensics research: The next 10 years." *digital investigation* 7 (2010): S64-S73.

[10] Popescu, Alin C., and Hany Farid. "Statistical tools for digital forensics." *International Workshop on Information Hiding*. Springer Berlin Heidelberg, 2004.

.