A **MAJOR REPORT ON**

A MOBILE RECOVERY TOOL USING LIVE ACQUISITION APPROACH

Submitted in partial fulfillment of the Requirement
for the award of the degree of

MASTER OF TECHNOLOGY
(INFORMATION SYSTEMS)

Submitted by
RAJENDRA KUMAR
(09/IS/2K10)

Under the Guidance of
RITU AGARWAL
(Asst. Professor)
Dept. of Information Technology

DEPARTMENT OF INFORMATION TECHNOLOGY
DELHI TECHNOLOGICAL UNIVERSITY
BAWANA ROAD, DELHI-110042

2010-12

CERTIFICATE

This is to certify that **Mr. Rajendra Kumar** (09/IS/2k10) has carried out the major project titled "A Mobile Recovery Tool Using Live Acquisition Approach" as a partial requirement for the award of Master of Technology degree in Information Systems by Delhi Technological University.

The major project is a bonafide piece of work carried out and completed under my supervision and guidance during the academic session 2010-2012.The matter contained in this report has not been submitted elsewhere for the award of any other degree.

(Project Guide)
Ms. RITU AGARWAL
(Asst. Professor)
Department of Information Technology
Delhi Technological University
Bawana Road, Delhi-110042

ACKNOWLEDGEMENT

I express my gratitude to my major project guide **Ms. Ritu Agarwal**, Asst. Professor, IT Dept., Delhi Technological University, for the valuable support and guidance he provided in making this major project. It is my pleasure to record my sincere thanks to my respected guide for her constructive criticism and insight without which the project would not have shaped as it has.

I would like to thank **Prof. O.P. Verma**, HOD, IT Dept., Delhi Technological University, for his useful insights and guidance towards the project. His suggestion and advice proved very valuable throughout. I am thankful to my parents, all teaching or non-teaching staff at D.T.U., and my fellows, who have helped in completion of this thesis report.

RAJENDRA KUMAR

M.TECH (INFORMATION SYSTEM)

ROLL NO. 09/IS/2K10

Abstract

This thesis focuses on file carving which is a forensic technique to retrieve the data without using any file system or metadata. Especially focus is on recovering the mobile data from smart phones. In today's scenario Google's Android operating system is most popular operating system for smart phones; So many big companies are using android in mobile phones example: Samsung, Sony Ericsson, LG etc. In all mobile phones, data acquisition is an important part in forensics. As the mobile forensic software becomes more strong and popular, most of them are now facing the problem where to internal collecting tools must be installed in the mobile phones first so that the data collecting could be started in order vice. Proper forensic examination of such memories, including recovery of deleted items, has not been possible until now. So our process is usable after the OS is corrupt or not booting and we want to recover a data through this new concept called Live acquisition approach. We are trying to boot the phone from SD card with some recovery software's and all tools work at boot time. It utilizes the concept of data recovery to perform physical data acquisition in Android smart phones. This data-acquisition methodology differs from the current ones in most mobile forensics software and can effectively perform the recovery of the deleted data.

TABLE OF CONTENTS

List of Figures

Chapter 1 : INTRODUCTION OF FILE CARVING

The news sites are regularly reporting about the fact that confidential or secret information was compromised. The loss of an USB-stick or device from any type of financial institute or government agency is happening quite frequently. Most of the time, the information was present on the device, but what if the information was deleted or even better, the device was formatted? After deletion, formatting and/or repartitioning we can use a technique called “Carving”. File Carving or simply carving, is the process of extracting a collection of data from a huge data set. Data carving techniques are mostly occurring during a digital investigation when the unallocated file system space is analyzed to extract files. The files are "carved" from the disk using file type-specific header and footer values.

1.1 FILE CARVING

The news sites are regularly reporting about the fact that confidential or secret information was or carving, is the practice of searching an input for files or other kinds of objects based on contents, rather than on metadata. File carving is a most powerful tool for retrieving files and fragments of files when directory entries are corrupt or missing, as may be the case with old files that have been deleted or when performing an analysis on damaged media. Carving of a memory is a useful tool for analyzing virtual and physical memory dumps when the memory structures are unknown or have been overwritten. File carvers operate by looking for file headers and footers, and then "carving out" the blocks between these two boundaries [1].

Semantic Carving performs carving only bases of the contents of the proposed files. So many carving tools have an option to only look at or near sector boundaries where headers are found. However, searching the entire files can find that have been embedded into other files, such as JPEGs being embedded into Microsoft Word documents [1] [2]. This may be considered as an advantage or a disadvantage, depending on the circumstances.

In this process file system structures are not used. File carving is a powerful tool for retrieving files and fragments of files when directory entries are corrupt or missing. Carving is also useful in criminal cases, where the use of carving techniques can recover evidence. In some cases related to child pornography, Law Enforcement agents were able to recover more images from the suspect’s hard-disks by using carving techniques. Memory carving is a useful technique for analyzing physical and virtual memory dumps when the memory structures are unknown or have been overwritten. An example of memory carving is the recovery of files from a mobile phone. In this chapter some basics and tooling of carving files will be explained.

With this huge increase in digital data storage, the need to recover data due to human error, device malfunction, or deliberate sabotage has also increased. Once the data has been extracted, software recovery techniques are often required to order and make sense of the data. In this article, we will be solely discussing software techniques for recovery of data with a focus on digital forensics. We will begin by providing a quick overview of traditional data recovery techniques and then describe the problems involved with such techniques. We then introduce the techniques involved in file carving.

1.2 FORENSIC SCIENCE

Forensic science (often shortened to forensics) is the application of a broad spectrum of sciences to answer questions of interest to a legal system. This may be in relation to a crime or a civil action. The word forensic comes from the Latin adjective forensic, meaning "of or before the forum." In Roman times, a criminal charge meant presenting the case before a group of public individuals in the forum. Both the person accused of the crime and the accuser would give speeches based on their sides of the story [4]. The individual with the best argument and delivery would determine the outcome of the case. This origin is the source of the two modern usages of the word forensic – as a form of legal evidence and as a category of public presentation. In modern use, the term "forensics" in the place of "forensic science" can be considered correct as the term "forensic" is effectively a synonym for "legal" or "related to courts". However the term is now so closely associated with the scientific field that many dictionaries include the meaning that equates the word "forensics" with "forensic science".

The ancient world lacked standardized forensic practices, which aided criminals in escaping punishment. Criminal investigations and trials relied on forced confessions and witness testimony. However ancient sources contain several accounts of techniques that foreshadow the concepts of forensic science that is developed centuries later, such as the "Eureka" legend told of Archimedes (287–212 BC). The first written account of using medicine and entomology to solve (separate) criminal cases is attributed to the book of Xi Yuan Lu (translated as "Washing Away of Wrongs"), written in Song Dynasty China by Song Ci (, 1186–1249) in 1248. In one of the accounts, the case of a person murdered with a sickle was solved by a death investigator who instructed everyone to bring his sickle to one location. (He realized it was a sickle by testing various blades on an animal carcass and comparing the wound.) Flies, attracted by the smell of blood, eventually gathered on a single sickle. In light of this, the murderer confessed. The book also offered advice on how to distinguish between a drowning (water in the lungs) and strangulation (broken neck cartilage), along with other evidence from examining corpses on determining if a death was caused by murder, suicide or an accident.

1.3 FILE RECOVERY VS. CARVING

When data is lost on a medium, people want to recover it. There is a big difference between file recovery techniques and carving. File recovery techniques make use of the file system information that remains after deletion of a file. By using this information, many files can be recovered [38] [39]. A disadvantage is that the file system information needs to be correct. If not, the files can’t be recovered. If a system is formatted, the file recovery techniques will not work either.

Carving works with the raw data and doesn’t use the file system structure during its process. A File system is a structure for storing and organizing computer files and the data they contain. Examples of often used file systems are: FAT16, FAT32, NTFS and EXT etc [1]. Although carving doesn’t care about which file system is used to store the files, it could be very helpful to understand how the specific file system works.

But how does carving work?

Carving makes use of the internal structure of a file. A file is a block of stored information like an image in a jpeg file. A computer is using extensions in file names to identify what these files contain. Let’s have a look of the internal structure of a “jpeg” file.

In a jpeg file there are certain structures which could help the carving software to distinguish this type of file from the rest of the raw data. First of all, there is the header. The header is an identification string which is unique for every file type. This could be very useful to identify the beginning of file types. In our example of the JPEG file structure, the Start of Image (Size of a jpeg file starts with the byte values „ 0xFF D8‟ (header). Following the SOI are a series of “Marker” blocks of data used for file information. Each of these “Markers” begin with a signature “FF XX”, where “XX” identifies the type of marker. The 2 bytes following each marker header is the size of the marker data. The marker data immediately follows the size and then the next marker header “FF XX” immediately follows the previous marker data [1]. There is no standard as to how many markers will exist, but following the markers, the signature “FF DA” indicates the “Start of Stream” marker.

Short Name	**Bytes**	**Payload**	**Name**
SOI	0x FF D8	None	Start Of Image
SOF0	0x FF C0	Variable size	Start Of Frame (Baseline DCT)
SOF2	0x FF C2	Variable size	Start Of Frame (Progressive DCT)
DHT	0x FF C4	Variable size	Define Huffman Table(s)
DQT	0x FF DB	Variable size	Define Quantization Table(s)
DRI	0x FF DD	2 bytes	Define Restart Interval
SOS	0x FF DA	Variable size	Start Of Stream
RSTn	0x FF D0 … 0XFFD7	None	Restart
APPn	0x FF En	Variable size	Application-specific
COM	0x FF FE	Variable size	Comment(text)
EOI	0x FF D9	None	End Of Image

Figure 1.1: Jpeg File Structure

The SOS marker is followed by 2-byte value of the size of the SOS data and is immediately followed by the Image stream that makes up the graphic. A jpeg file ends with the bytes “0xFF D9” (footer). The constant values “0xFF D8” and “0x FF D9” are also called the “magic numbers”. The 2 bytes following each marker header is the size of the marker data. The marker data immediately follows the size and then the next marker header “FF XX” immediately follows the previous marker data. There is no standard as to how many markers will exist, but following the markers, the signature “FF DA” indicates the “Start of Stream” marker.

The SOS marker is followed by a 2-byte value of the size of the SOS data and is immediately followed by the Image stream that makes up the graphic. A jpeg file ends with the bytes “0xFF D9‟(footer). The constant values “0xFF D8” and “0x FF D9” are also called the “magic numbers‟ As an example, a jpeg image was viewed into Pspad Hex. In the following Figures the header of the jpeg file will be shown:

```
00000 FFD8 FFE0 0010  4A46 4946 0001 0201 0048  yeya.. JFEF…….H
00010 0048  0000  FFE1 3846  4578 6966 0000 4D4D .H..ya8FExif…MM
```

Figure 1.2: Header of the Jpeg File

1.4 FILE CARVING TOOLS

There are different carving tools available, most of them are open-source and others are commercial solutions offered by companies. Due to the fact that carving is a developing technique, more and more tools are becoming available [3] [5]. Some of the most common used carving tools are:

1.4.1 Foremost

Originally designed by the U.S. Air force, is a carver designed for recovering files based on their headers, footers, and internal data structures [6].

1.4.2 Scalpel

Scalpel is a rewrite of Foremost focused on performance and a decrease of memory usage. It uses a database of header and footer definitions and extracts matching files from a set of image files or raw device files. Scalpel is file system-independent and will carve files from FATx, NTFS, ext2/3, or raw partitions. Scalpel will not allow you to output to the same directory you're carving from [7] [30][53].

1.4.3 Photorec

Photorec is a data recovery software tool designed to recover lost files from digital camera memory (Compact Flash, Memory Stick, Secure Digital, Smart Media, Micro drive, MMC, USB flash drives etc.), hard disks and CD-ROMs. It recovers most common photo formats, including JPEG, audio files including MP3, document formats such as Microsoft Office, PDF and HTML, and archive formats including ZIP [8].

PhotoRec does not attempt to write to the damaged media you are about to recover from. Recovered files are instead written to the directory from where you are running PhotoRec or any other directory you choose.

1.4.4 Encase

EnCase is a family of all-in-one computer forensics suites sold by **Guidance Software**. These products include EnCase Enterprise, EnCase Forensic Edition, EnCase eDiscovery, and EnCase Lab Edition [9]. These programs use a proprietary image file format that has been reverse engineered. Users can create scripts, called **EnScripts**, to automate tasks.

1.5 FILE CARVING IN MOBILE PHONES

In the previous parts we discussed carving files out of raw data and file systems. For people working in forensics, or interested in forensics, mobile phones are also very interesting sources of data. As with file systems, when you delete a file it's only deleted when it's overwritten by other data. In FAT when a file is deleted, the file's directory entry is changed to show that the file is no longer needed. The 1st character of the filename is replaced with a "marker", but the file data itself is left unchanged. Until it's overwritten, the data is still present. For mobile phones it's the same [10]. If you delete an SMS -message, it will still be in the memory of the phone until that memory space is overwritten.

Recovering data from a mobile phone is different. All phone models have an Operating system: Windows CE, Symbian, Android, and MacOSX. These operating systems also store their files in the memory of the phone. Samsung makes use of the FAT file system. Every mobile-phone vendor has its own way for storing data into the phone memory. Some vendors store the IMSI code (subscriber identification) in a certain field in the right order, but other vendors use „reverse nibbling" to store this code in the phone memory.

But how is it possible to recover data from a mobile phone? You need to understand the principles how the data is being stored on the mobile phone. For example the content of an SMS message is compressed by the PDU format from 8 ASCII characters into 7 bytes. There are two ways of sending and receiving SMS messages: by text mode and by PDU (protocol description unit) mode. The text mode (unavailable on some phones) is just an encoding of the bit stream represented by the PDU mode. Alphabets may differ and there are several encoding alternatives when displaying an SMS message.

Photos and music are usually stored on the onboard memory card. There is no standard solution for recovering data from mobile phones. For computers, though, images of the disk and memory can be made by using the tool “dd” For mobile phones you need a “flasher” to dump the physical file system of a mobile unit. From a practitioner’s point of view a “Hex Dump” is a snapshot of the entire contents of the handsets memory [10]. Forensic examiners are striving to grab this data, preserve it and analyze it in the hope of finding information normally hidden from view and/or deleted data. Most of the Mobile Phone forensic examination applications are a progression of “backup software” that concentrates on the user’s data.

Chapter 2 : MOBILE PHONE AND DIGITAL FORENSIC

In the information age, every byte of data matters. Cell phones are capable of storing a wealth of personal information, often intentionally, and sometimes unintentionally. This holds true for almost all mobile devices, such as PDAs and Smart phones as well. Cell phone forensic experts specialize in the forensic retrieval of data from cell phones and other mobile devices in a manner that preserves the evidence under forensically acceptable conditions, ensuring that it is court-admissible.

A cell phone forensic investigation includes possible full data retrieval dependent upon the cell phone or PDA model. The cell phone and PDA forensic engineers at Kessler International will conduct a thorough examination of the data found on the cell phone's SIM/USIM, the cell phone body itself, and any optional memory cards [12].

Some of the kinds of data that may be retrieved and examined during a cell phone forensic investigation, even after being deleted, include:

- Call times; dialed and received calls, and call durations
- Text messages or SMS messages
- Contact names & phone numbers
- Address book entries; residential addresses and email addresses
- Photos & graphics
- Videos

Law enforcement officials and legal firms realize the importance of evidence contained on cell phones and other mobile devices, and how it can greatly affect the outcome of a trial. Whether working to document evidence of "white collar crime" or tasked by law enforcement to extract data for a criminal trial, the integrity of the firm selected for a cell phone forensic audit is as important as the integrity of the data recovered. More and more court cases are being won with the proper submittal of electronic evidence, so it's imperative that the cell phone forensics investigator understands the legal issues and imperatives surrounding electronic evidence gathering.

2.1 MOBILE EVIDENCES

Mobile phones are digital media. In principle, this means that mobile phones have the same evidentiary possibilities as other digital media, such as hard drives. For example it is, as will be explored in this paper, possible to extract deleted information from a mobile phone, in the same way it is possible on a hard drive. However, mobile phones also suffer from the same evidentiary problems as other digital media. As with a computer, the content of a mobile phone is fragile and can easily be deleted and overwritten [11] [13]. Mobile phones should therefore be handled with great care and insight, just as any other digital media.

Many issues pose a threat to the validity of mobile phone forensics. There are difficulties in acquiring certain types of data that stem from the proprietary nature of mobile phones. In addition, features such as Bluetooth and the ability to run third-party applications can create additional problems. As a result, mobile forensic tools are struggling to reliably acquire data from a wide range of mobile phones. As the amount of evidence and different types of mobile phones 6 increases, the tools must also advance in functionality to accommodate these changes without sacrifice.

Up until recently, the majority of mobile forensic tools did not implement any form of integrity protection. Forensic examiners were relied upon to ensure evidence was not tampered with or corrupted [23]. For example, Oxygen's Mobile Phone Manager is a phone-syncing tool that was used for at least two years by law enforcement to gather evidence from mobile phones before being updated. An updated tamper-resistant "forensic" version was released in April 2007 that uses hash values to help maintain the integrity of acquired data. Before this version was available, it was unclear how integrity management was addressed.

2.2 FORENSIC TOOL FOR MOBILES

Mobile forensic tools typically use AT commands, FBUS, OBEX or other similar communication protocols to acquire data [14] [18]. The method depends on the phone. All of these methods rely on proprietary phone software, and carry with them the following issues:

- Data can be indirectly altered when using AT commands or Nokia FBUS.

- Important data may be omitted from the phone's response to a command.

- Some data will never be accessible over software interface.

- Data that is accessible on one phone may not be accessible on other, similar phones, using the same commands.

This creates a problematic situation with mobile forensic tools because the methods relied on to investigate phones may be inherently unreliable. At the same time, forensic investigations cannot wait for an unlikely standardized mobile phone protocol. Therefore, it is critical to make sure that obtainable data remains forensically sound.

When involved in crimes or other incidents, proper tools and techniques are needed to recover evidence from such devices and their associated media:

2.2.1 OXYGEN FORENSIC SUITE

Oxygen Forensic Suite 2012 is mobile forensic software that goes beyond standard logical analysis of cell phones, Smartphone's and PDA. Using advanced proprietary protocols permits Oxygen Forensic Suite 2012 to extract much more data than usually extracted by logical forensic tools,especially for smartphones [14] [26].

Strong support for Symbian OS, Apple iPhone, Android, Windows Mobile and RIM BlackBerry devices. The popularity of smartphones is constantly growing. These devices store tons of vital forensic data that cannot be extracted by standard PC-to-mobile protocols. In 2002 Oxygen Software invented the advanced Agent application approach that allows Oxygen Forensic Suite to extract much more information from Smartphone than other logical tools.

Messages stored in custom folders and subfolders**.** Besides standard SMS, MMS and E-mail folders, Smartphone permit to create the custom ones and organize multi-level folders tree. SMS messages deleted from phone memory**.** Even if a message was deleted from phone memory, each Symbian OS device stores information about it as a part of extended event log. Do not confuse this feature with extracting deleted messages from SIM card offered by many other tools. Extended phonebook information**.** These data include: contact photos, caller groups, speed dials, custom field labels, and more than 5 numbers of the same type, last contact modification date and time.

- Deleted contacts and calls history in Windows Mobile devices. Oxygen Forensic Suite can access PIM.VOL file that stores removed contacts, deleted call records and lots of other important data.
- MMS and E-mail attachments**.** Oxygen Forensic Suite can get access to MMS and E-mail messages with their attachments for the devices supporting these features.
- Web Browsers Analyzer add-on allows extracting and examining cache files of mobile web browsers - preinstalled as well as 3rd party ones.
- Individual approach to each phone model. Besides the advanced Agent application usage, Oxygen Forensic Suite operates with almost all logical protocols allowing safe data extraction from the each specific device - cell phone, smart phone or tablet.
- No special hardware needed. Oxygen Forensic Suite connects to mobile devices via standard cables and adapters, including 3rd-party ones.
- User-friendly interface for data analysis. The data is grouped according to its classes. A convenient search, sorting, grouping and content filtering engine allows you to quickly find the needed information.

2.2.2 MOBILedit!

MOBILedit users enjoy a long list of features which you can find here. From its extensive Phonebook utilities to its SMS handling, MOBILedit! not only supports more makes and models than any other, but the list of features grows equally as fast [14]. Our team is working at full throttle to bring you more and more features that allow you to maximally utilize your mobile phone to your advantage.

Main Features

- The only universal PC Studio with thousands of phones supported
- Manage, improve and print a phonebook from the comfort of a computer
- Copy phonebook from any phone to a new phone regardless of manufacturer or system
- Backup all phone content to a PC or Internet cloud storage
- Complete ringtone editor
- Built-in video editor
- Live view of phone and card memory, battery, signal, IMEI and more

- Contact optimization and internationalization
- Copy pictures and videos between phone and PC
- Download, read, store and print text messages
- Send text messages using PC keyboard
- Install applications to the phone from a PC

2.3 SMART PHONES VS NORMAL PHONES

Today, smart phones have more things in common to computers rather than cell phones. A compact or full keyboard often comes as standard in smart phones as it is necessary for quickly typing messages and emails. The middleware structure of smart phone shown below in figure 2.1 Smart phones utilize an operating system that is identifiable and is often used on other phones. It provides a stable platform where users can install third party applications.

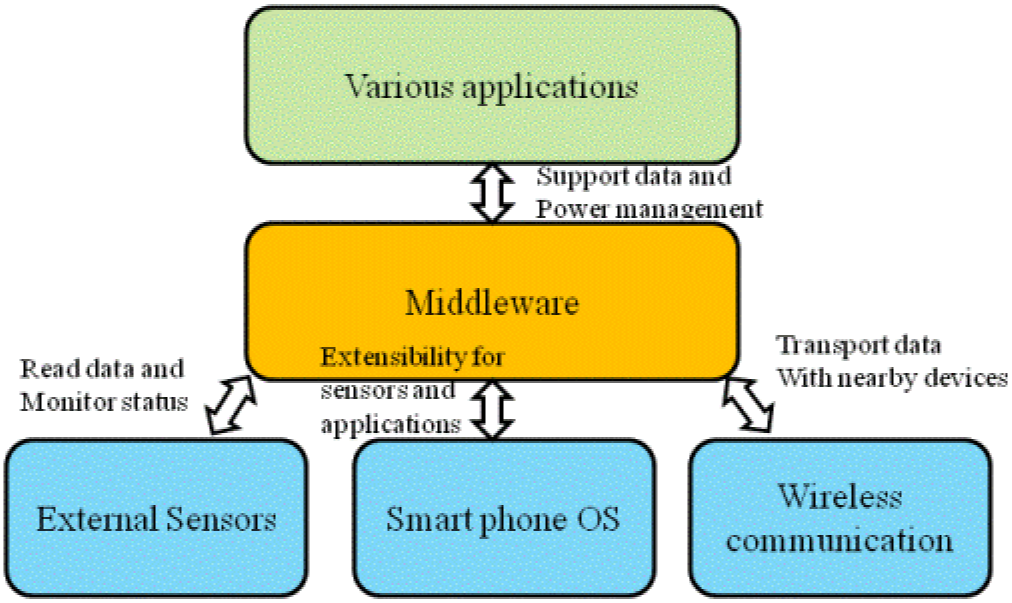


Figure 2.1: Middleware structure of Smartphone

Cell phones can typically send and receive text, picture and video messaging. Many cell phones can email, too. While many cell phones now have full QWERTY keyboards, this is a basic requirement for smart phones. The keyboard is much like your computer's keyboard. Smart phones, though, typically go a step further by syncing with the email server of your personal or corporate provider. Cell phones have been around for some time. At first, its only function was to provide people with a means to call and be called anytime without being connected to any line. It eventually evolved and added more features like text messaging.

Smart phones have more advanced capabilities compared to cell phones. A smart phone is both a PDA and a cell phone. Today’s smart phone has more in common with computers than cell phones. Smartphone usually have a touch screen and a full QWERTY keyboard while cell phones come with a regular small screen and a number pad. A Smartphone uses an operating system that allows third party applications to run on it.

2.4 USES OF MOBILE PHONES

In today’s scenario mobile devices are most frequently used by each and every people, this is a basic need of each person. Criminals are also used mobile phones for crime, so mobile devices are most commonly used by normal person and criminals. Mobile devices are an evolving form of computing, used widely for personal and organizational purposes. These compact devices are useful in managing information, such as contact details and appointments, and corresponding electronically. Over time, they accumulate a sizeable amount of information about the owner.

The use of a mobile phone is not limited to speaking alone it is being used in making video, recording information and transmitting it to a phone or a computer as was being done by a computer. Mobile phone can be connected to a computer to download information from it or vice versa. Other facilities like on line chatting, conferencing, sending text, transferring MMS information by a mobile phone are compatible with a computer.

Mobile phone is not only used for the welfare of humankind but also its misuse has serious effects on our society worldwide. Time and again, there are the reports that mobile phones are being misused by antisocial and miscreant elements to carry out their inhumane activities. Good or bad are the two sides of a coin, but it is up to the users, to make a best use of mobile phone. Mobile phone technology has opened up a world of opportunity for people everywhere. Unfortunately, that includes criminals. Mobile phones have been used in some pretty hilarious crimes.

2.5 ROLE OF MOBILE IN CRIME

There will come a time when we will have to educate ourselves with the technology. Mobile phones can be used for good. They can also be used for bad. In crime mobile devices are most commonly used. It is used in terrorist attack, stealing, MMS, and many more crimes. Criminals are used smart phones and mobile phones to communicate each other, the role of mobile phone in crime is a huge hand because in most of the cases criminals do all the work through mobile phones like they give instruction to our team member and follow [22]. In now days criminals are also aware about the new technologies of mobile phone like they have a knowledge about the smart phones and the features of smart phones. Mobile phone is one of the way of crime for criminals.

There are multiple reports on the web about the smart phones apps being fraught with privacy or security risks. Experts also believe smart phone users now need to be more watchful. According to them, cyber criminals are now setting their sights on smart phone users, especially those using the Android operating system.

The most obvious criminal implication of mobile phones is that an awful lot of them get stolen. Figures released last week by the Metropolitan Police revealed that there was a 31.4% increase in street robberies and snatch thefts in the first six months of this year (see chart). Half of all those offences involved a mobile phone, and in two-thirds of those, the phone was the only thing stolen. Such phone robberies in London have quadrupled in two years. The national picture is similar: overall crime is falling, but robbery and theft from the person are rocketing, driven in part by the fad for pinching phones.

On the other hand, phone data can be used to establish the whereabouts of suspects. At the moment the results are only approximate, but they will be much less so when third generation mobile phones arrive. Libertarians worry that this technology, and newly acquired government surveillance powers, could compromise civil liberties. You might as well be carrying a tracking device, says Caspar Bowden, of the Foundation for Information Policy Research. But whilst gathering such data might be intrusive, it is unlikely to be of much use in court. The men suspected of the bombing rebuffed mobile phone evidence, claiming that their phones had been lost or borrowed.

Chapter 3 : LITERATURE REVIEW

Computers in the 1940s were the size of a large room and consumed as much power as several hundred modern personal computers (Penn Computing, 2010). A mobile device can perform many of the same tasks as a personal computer with a greater mobile form factor. An emerging subcategory of mobile devices is smart phones. Smart phones are hybrid device between a cellular phone and PDA (Portable Digital Assistant). Smart phones can be used to perform a wide range of business tasks and have capabilities approaching a desktop PC [12]. Tasks a mobile device can do include those typical of a cellular phone, such as: calling and SMS (Short Message Service) messaging as well as personal computer tasks, such as: email, web browsing and listening to music.

Literature will be reviewed contextual basis for the research as a whole. Literature on several topics that relate to the mobile forensics will be reviewed. The first area literature has been selected from is within the topic of Smart phones [48]. Literature on Smart phones helps identify what data can be extracted from a mobile and the tested methodologies for extraction of data. SIM (Subscriber Identity Module) cards are another area a forensic professional can find digital evidence. There are challenges involved with performing a robust forensic examination on a mobile device []. Limitations with extraction tools make it difficult for an examiner to create a forensic copy of a mobile device while maintaining data integrity. The Smart phone exists in multiple environments: the physical environment, information systems environment and end user environment.

As a result of the communication between the smart phones and cellular provider the cellular provider may store relevant digital evidence. As part of the imaging procedure of a mobile device, wireless communication should be blocked so changes can't be made to the data stored on the device. The Smart phone supports a feature that device calls "remote wipe". Remote wipe allows a remote user to send a command to the Phone instructing it to erase all data stored on the device using the Mobile.

The lower-level methods are less complex for a forensic examiner to perform but are less forensically robust as data integrity can't be maintained. The advantages and limitations of each method of extraction are discussed.

3.1 SMART PHONES

A smart phone is a mobile device built on a mobile computing platform, with more advanced computing capability and connectivity than a feature phone. The first smart phones mainly mixed the functions of a personal digital assistant (PDA) and a mobile phone or camera phone.

In today's models also used combine the functions of portable media players, low-end compact digital cameras, pocket video cameras, and GPS navigation units. Smart phones typically also combine high-resolution touch screens, web browsers that can access and properly display standard web pages rather than just mobile-optimized sites, and high-speed data access via Wi-Fi and mobile broadband [18] [25].

The common mobile operating systems (OS) used by modern smart phones include Google's Android, RIM OS BlackBerry , Samsung's Bada, Microsoft's Windows Phone, HP's web OS, Apple's iOS, Nokia's Symbian and embedded Linux distributions such as Maemo and MeeGo. Some operating systems can be installed on many different phone models, and typically each device can receive multiple OS software updates over its lifetime.

The distinction between smart phones and feature phones there is no official definition for what constitutes the difference between them. One of the most significant differences is that the advanced APIs (application programming interfaces) on smart phones for running third-party applications can allow those applications to have better integration with the phone's OS and hardware than is typical with feature phones. In comparison, feature phones commonly run on proprietary firmware, with third-party software support through platforms such as Java. An additional complication in distinguishing between smart phones and feature mobile phones is that over time the capabilities of new models of feature phones can increase to exceed those of phones that had been promoted as smart phones in the past.

The Android phone is a smart phone. A smart phone is a hybrid of a cell phone and PDA. Essentially, a mobile device can do much of what a computer or laptop can do, just on a smaller scale. Research into mobile device forensics has grown over recent years as researchers see the value in data stored on a mobile device.

3.2 EVIDENCE ON SMART PHONES

The types of evidence that can be extracted from a mobile device [18]. The types of evidence outlined in the thesis include data found on a cell phone, including: contacts, call history and SMS (Short Message Service) messages as well as data found on a PDA, including: audio files, email and Internet history. The Smartphone stores data that could be used as digital evidence. The difficult part of getting a forensic copy of the evidence stored on the Smartphone for analysis is in the extraction as tools are currently limited to extracting a logical copy of the data.

A fundamental component for cellular communication of a smart phone is the SIM card. Forensic examination of SIM cards is not new as SIM cards have been used in cell phones for a long time but it’s still relevant for the Smartphone as information can be stored on the SIM card. Forensic department discuss a forensic tool for examining SIM cards called SIM brush. Forensic department outline the evidence that can be extracted from a SIM card as well as the limitations of SIM card forensics.

3.3 CHALLENGES

Forensic professionals attempting to extract evidence from a mobile device are often faced with challenges [35]. Challenges arise because of the small form factor that makes mobile devices so portable. “The cumulative experience of building several prototypes leads us to believe that mobile devices in the future will continue to integrate more function and cost less”. Unlike forensic examinations of a desktop or laptop personal computer where the hard disk is easily removable the storage components used in a mobile device are more difficult to remove as they’re soldered onto the logic board. Maintaining data integrity of a forensic copy is difficult when the storage components can’t be physically removed. If the storage components can’t be removed for a forensic copy to be obtained another method of extraction needs to be used. A forensic copy of the internal flash memory could be made to removable storage if the mobile device supports removable media.

3.3.1 Storage

Manufacturers design mobile devices to fit hardware components in a small space. Fitting the hardware components in tightly means it’s more difficult to remove hardware components [45].

A difference between a personal computer and a mobile device is the type of disk used for storage. In a personal computer, magnetic hard disks are used because they're cost effective, provide a good level of performance and can store a lot of data. Modern mobile devices don't use magnetic hard disks because they contain moving parts that can cause damage if dropped. Flash memory stores data by storing an electrical charge in a floating gate of a transistor. Solid-state storage doesn't involve moving parts and is more suitable for mobile devices.

3.4 VOLATILITY OF CELLULAR PROVIDER EVIDENCE

Not only can valuable evidence be stored on the Smartphone itself but due to the connectivity mechanisms discussed about later in thesis there can also be evidence stored by the cellular provider. Any situations where the Smartphone has had to communicate with the cellular provider could be an instance where evidence could be held at the cellular provider. Such communication could include: MMS, call history and Internet usage. Evidence may have been erased off the Smartphone or the examiner may be using an extraction method that could miss some evidence. The cellular provider could be a source of evidence in addition to evidence obtained from the Smartphone. Obtaining evidence from a cellular provider may be outside any existing legal allowances, such as a warrant and may require an additional warrant be served. Another limitation of digital evidence stored by the cellular provider is that it may not be complete or accurate. Information stored by the cellular provider is managed by the cellular provider who has no commitment to ensuring their data is unchanged. Time is a constraint when working with digital evidence, especially evidence stored by the cellular provider.

Due to the high penetration rate of mobile phones, they will inevitably be connected to and increasing number of criminal activities. Since they may contain information comparable to that of a desktop computer, they are a prime source of evidence. The following list of potential evidence can be found in a mobile phone:

- Subscriber and equipment identifiers
- Date/time, language, and other settings
- Phonebook information
- Appointment calendar information

- Text messages
- Dialed, incoming, and missed call logs
- Electronic mail
- Photos
- Audio and video recordings
- Multi-media messages
- Instant messaging and Web browsing activities
- Electronic documents

3.5 RELATED WORK

This related work only the bases of the concept to perform digital forensics applying Live acquisition method on Google Android, so the related terms and references are firstly studied.

Smart phone is the converged Mobile device and PDA. They will be working on different platforms Android is one of them. Though the smart phones we will not access only has basic function of voice communication but also access wireless internet, email and PIM (Personal Information Management), and expand the function with the application software of games.

Now, Android is most developing and popular operating system for smart phones. It is capable of software applications and contains personal information where makes people rely on these devices. In last year's, information criminal cases are expanding rapidly than ever, personal information leakage. As a result, besides user's daily prevention, how forensic examiners can help acquire information from victims' phones after harm happens becomes the most important issue now.

The present business-edition digital forensic software is not affordable for the public, and most of them adopt internal logical acquisition. This methodology is questionable because it cannot be confirmed if the scenes have been modified, which is forbidden in forensics, after the software is installed to the mobile phone. Moreover, another potential issue is the damaged data may not be recovered because logical acquisition utilizes API to access the data.

3.6 USAGE OF EXTERNAL MEMORY, INTERNAL MEMORY AND SIM

In order to understand the value of analyzing mobile phone internal memory, one must understand where the different information items in mobile phones are stored. In order to understand this properly, a range of mobile phones with SIM, intern al storage, and to a certain extent external flash storage was analyzed to determine what information items are stored on the different media types [40]. The phones were examined by sending and receiving text messages, taking pictures, store contacts and calendar events, exchanging SIM cards and external Memory cards, and observe the behavior. The results indicate that each manufacturer is consistent in the way data is handled, but the variation between manufacturers is significant.

The results are summarized in the following, grouped on each manufacturer [13].

3.6.1 Nokia

The models 3200, 3410, 3510i, 5110, 6110, 6150, 6210, 6230, 6310i and 6610 were analyzed.

The following behavior was observed on the analyzed Nokia phones: Text messages are stored on the SIM. When the SIM is full (max 20-30 messages), the phone uses internal memory (up to 150 messages common on most models). Older models store only incoming messages, but newer models store both outgoing and incoming, but only incoming is stored on SIM. With Nokia phones, deleted messages on SIM can be recovered. Contacts can be stored on SIM or internal memory, and the user can select which memory to use. Older Nokia phones cannot store contacts in internal memory. Of the analyzed phones, this was the case only with the 5110.

The analyzed Nokia phones use internal memory for all other data such as calendar events, caller logs, pictures etc. The call log file on the SIM is not used by Nokia. If the SIM is changed, the phone will delete the caller logs, but all other data will remain.

3.6.2 Sony Ericsson

The models A2618s, GH688, R380s, S868, T68, T68i, T610 and T630 were analyzed.

For the analyzed Sony Ericsson phones, it was ob served that text messages are stored on internal memory until it is full and only then will the phone start to use the SIM. As a consequence, SIM cards\ will in most cases contain nothing when they have been used in Sony Ericsson phones. It was also discovered that the phone deletes all messages in internal memory if the user switches the SIM card. Other items, such as pictures and calendar events are all stored in internal memory. For phones with external memory cards, it is similar to Nokia only possible to copy pictures and sounds to these, and only at the user's explicit request.

3.6.3 Siemens

The models A60, C25, C60, C62, M55 and M65 were analyzed.

The analyzed Siemens phones use SIM as primary storage for text messages and log of outgoing calls. When the SIM memory is full, internal memory is used. For contacts, the user can choose whether to use internal or SIM memory, but internal memory is the default. None of the Siemens phones deleted items when switching the SIM card. No Siemens phone with external memory was analyzed.

From the above it should be very clear that many, in fact most, information items on modern mobile phones are stored in internal flash memory as opposed to the SIM or external flash memory. It is therefore of outmost importance to find methods to perform sound forensic analysis of mobile phone internal memory.

Chapter 4 : PROPOSED SYSTEM

Mobile phones are most commonly used device by criminals they communicate each other through mobile phone after the crime they will destroy the device. Mobile phones are used in most of the crimes, most of the criminals are using mobile phones to communicate each other and after that they will be destroy all the information. This information is very useful for forensic department if they will be finding this phone.

Our work makes use of the characteristic where Android allows users to update software packages legally to design and implement the Live SD physical acquisition forensic tool referring to Live USB/CD/DVD forensics in computers. This methodology utilizes the Recovery mode in Android platform to perform data acquisition and copy the data from the database, which means the forensic software does not need to be installed to prevent potential issue of modifying the crime scene. In the future, we will pay more focus on the damaged data recovery and instant data acquisition based on this work.

4.1 INTRODUCTION

Android is a Linux-kernelled open source mobile phone operating system. In 2005, Google merged the mobile phone OS developer Android, and Google continued to develop it after the mergence. Until November 5th 2007, Open Handset Alliance which is composed of Google and other 33 mobile device manufacturers announces this operating system [15] [19]. The latest version of Android is 4.0, and according to statistics up to March 15th 2012 from Android Market, the market share of different versions is 3% for Version 1.5, 4.8% for Version 1.6, 29% for Version 2.1, 61.3% for Version 2.2, 0.7% for Version 2.3, 1% for Version 2.3.3, 0.2% for Version 3.0. , and 28% for version 4.0.

In all mobile phones, data acquisition is an important part in forensics. As the mobile forensic software becomes more strong and popular, most of them are now facing the problem where to internal collecting tools must be installed in the mobile phones first so that the data collecting could be started in order vice [28]. Proper forensic examination of such memories, including recovery of deleted items, has not been possible until now. So our process is usable after the OS is corrupt or not booting and we want to recover a data through this new concept called Live acquisition approach. We are trying to boot the phone from SD card with some recovery software's and all tools work at boot time. It utilizes the concept of data recovery to perform physical data acquisition in Android smart phones. This data-acquisition methodology differs from the current ones in most mobile forensics software and can effectively perform the recovery of the deleted data. There are three important things in smart phones are CPU, RAM and Flash memory the basic structures are shown in below in figure 4.1.

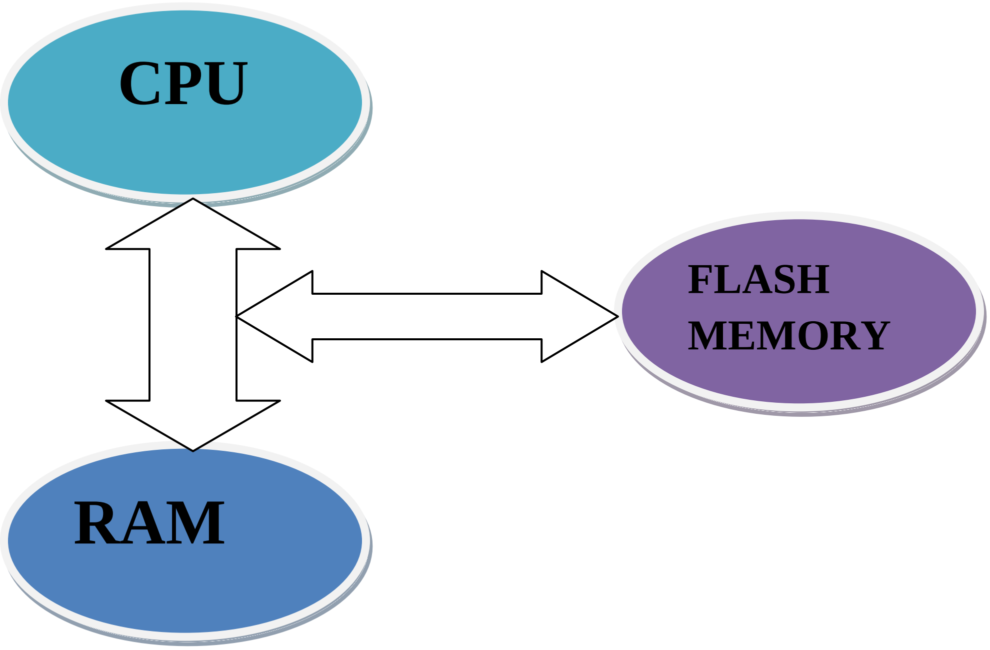


Figure 4.1: Basic structure of mobile phones

4.2 OUR APPROACH

If the mobile OS (Android) is crashed or if it is not properly working, in this case we want to recover the data. Our approach is working it in run time or boot time that is called live acquisition approach. There are 4 applications visible on the command prompt these are used for different purposes if we want to recover a SMS then we use a SMS recovery, or recover a data from memory card use memory card recovery, recover a data from FAT file system using FAT recovery and one more additional software is NTFS file system recovery for windows OS in mobiles.

4.3 THE SYSTEM ARCHITECTURE OF ANDROID OS

The system architecture is totally composed of four layers, as shown in Figure 4.1. The bottom layer is the Linux kernel and hardware driver, and the second layer is C\C++ libraries which offer the software function for the bottom layer [16] [17]. Besides, kernel libraries and Dalvik virtual machine, which are aimed to provide a runtime environment to Android applications, are at the same layer as well. The third layer is the frame of the applications offering Application programming interface (API) for Android applications. The top layer is the interface of Android applications.

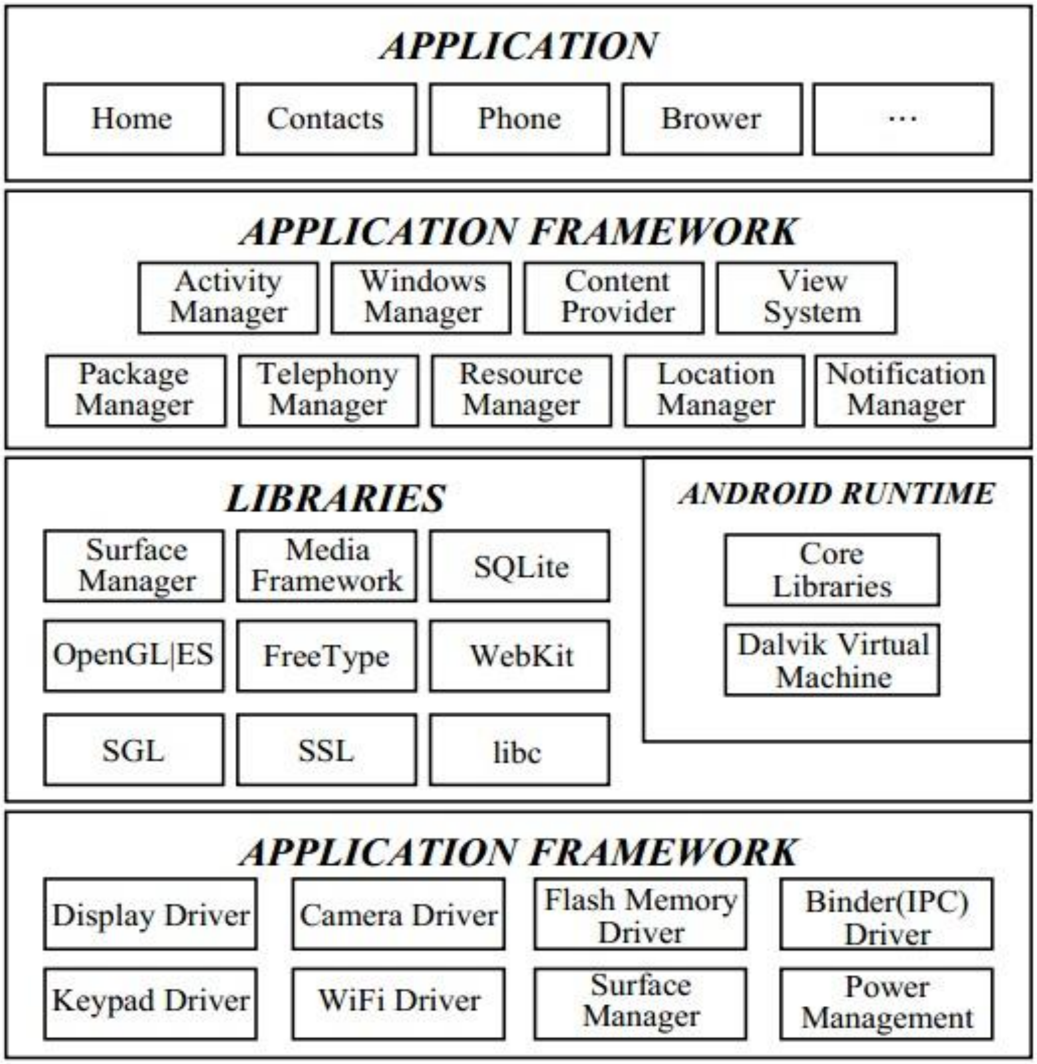


Figure 4.2 System architecture of Android OS

4.4 BOOT PROCESS OF ANDROID PHONES

Since mobile platforms and embedded systems has some differences compared to Desktop systems in how they initially start up and boot this post will discuss the initial boot stages of an Android phone shown in Figure 4.3.

- Power on and boot ROM code execution: At power on the CPU will be in a state where no initializations have been done. Internal clocks are not set up and the only memory available is the internal RAM. When power supplies are stable the execution will start with the Boot ROM code. This is a small piece of code that is hardwired in the CPU ASIC.

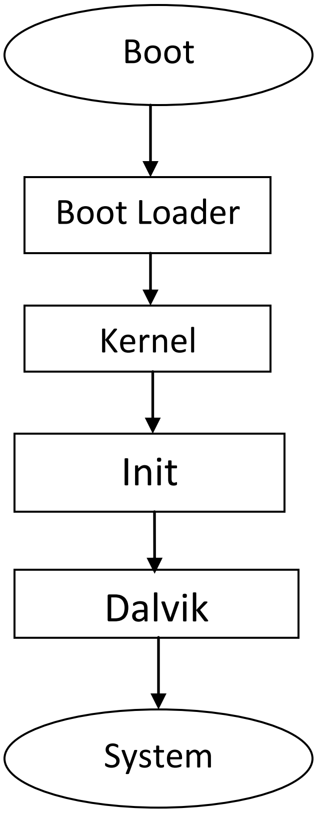


Figure 4.3 Boot process in Android

- Power on and boot ROM code execution: At power on the CPU will be in a state where no initializations have been done. Internal clocks are not set up and the only memory available is the internal RAM. When power supplies are stable the execution will start with the Boot ROM code. This is a small piece of code that is hardwired in the CPU ASIC.

- The boot loader: The boot loader is a special program separate from the Linux kernel that is used to set up initial memories and load the kernel to RAM. On desktop systems the boot loaders are programs like GRUB and in embedded Linux uBoot is often the boot loader of choice. Device manufacturers often use their own proprietary boot loaders. The requirements on a boot loader for Linux running on an ARM system can be found in the Booting document under /Documentation/arm in the kernel source tree.
- The Linux kernel: The Linux kernel starts up in a similar way on Android as on other systems. It will set up everything that is needed for the system to run. Initialize interrupt controllers, set up memory protections, caches and scheduling.
- The init process: The init process is the “grandmother” of all system processes. Every other process in the system will be launched from this process or one of its descendants.
- Dalvik: The Dalvik is launched by the init process and will basically just start executing and initialize the Dalvik VM. The system server: The system server is the first java component to run in the system. It will start all the Android services such as telephony manager and Bluetooth. Start up of each service is currently written directly into the run method of the system server.
- Boot completed: Once the System Server is up and running and the system boot has completed there is a standard broadcast action called ACTION_BOOT_COMPLETED. To start your own service, register an alarm or otherwise make your application perform some action after boot you should register to receive this broadcast intent.

4.5 FLOW CHART OF BOOTING PROCESS OF ANDROID

In this flow diagram shows (figure 4.4) how android work with bootable device (SD card). Our approach is working also though this process. This bootable process is also helpful for update the OS in Smart phone. They will be start with boot and the boot loader ask about the device is run with SD card or flash memory (Linux kernel).

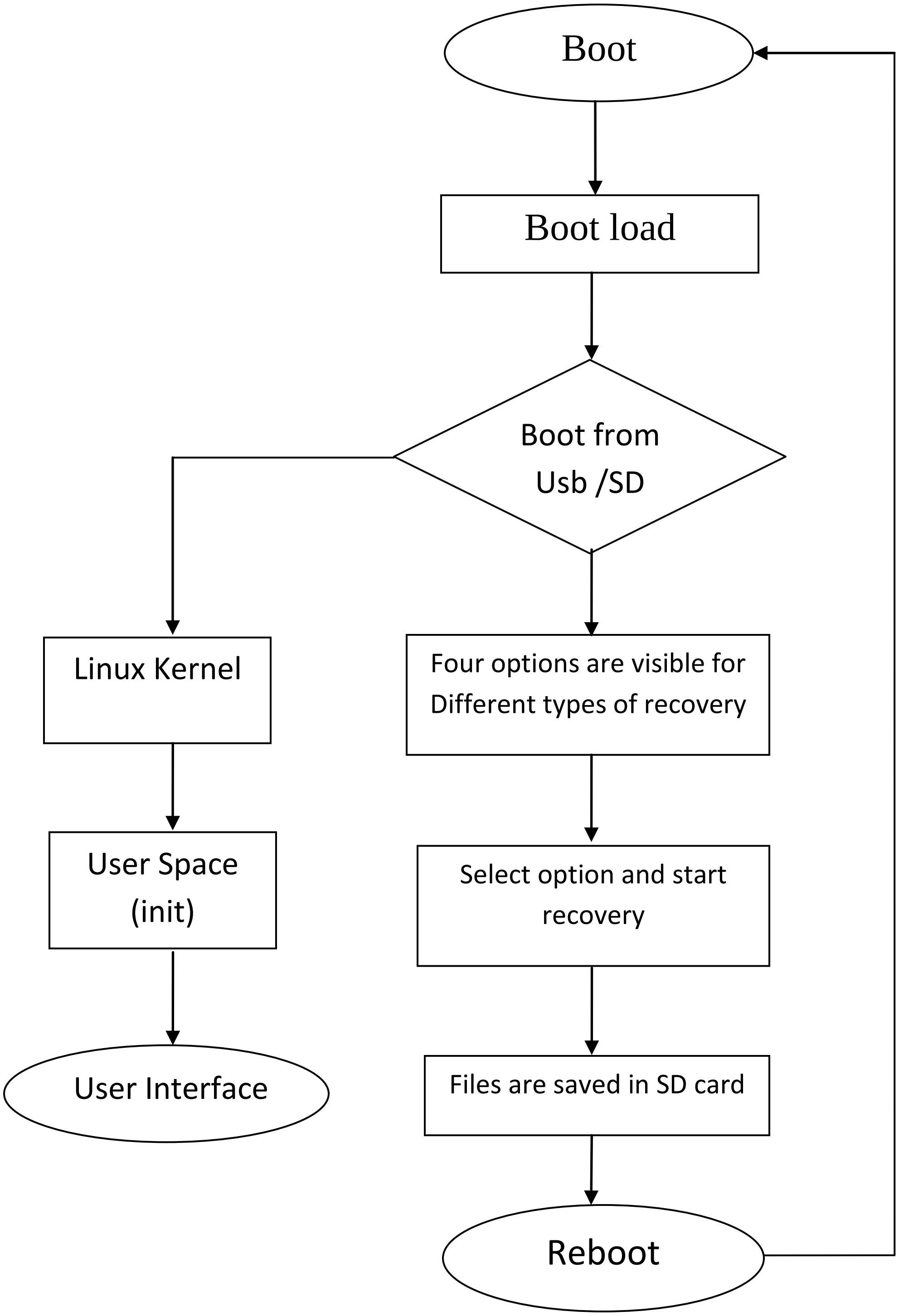

Boot
Boot load
Boot from Usb /SD
Linux Kernel
User Space (init)
User Interface
Four options are visible for Different types of recovery
Select option and start recovery
Files are saved in SD card
Reboot

Figure 4.4 Flow chart of Recovery Tool

4.6 SYSTEM ARCHITECTURE

In this research, physical acquisition is performed with Live SD on Android-platform smart phone. As soon as Live SD is started by Recovery tool, the internal data in the mobile phone can be acquired physically. In this work, the user-controlled all recovery software which is allowed in Android is implemented to legally interrupt booting procedure. The recovery tool interface is designed and implemented as well to complete internal data acquisition by user’s instructions. A complete Live SD forensic program is composed of Preprocedure and Forensic Task.

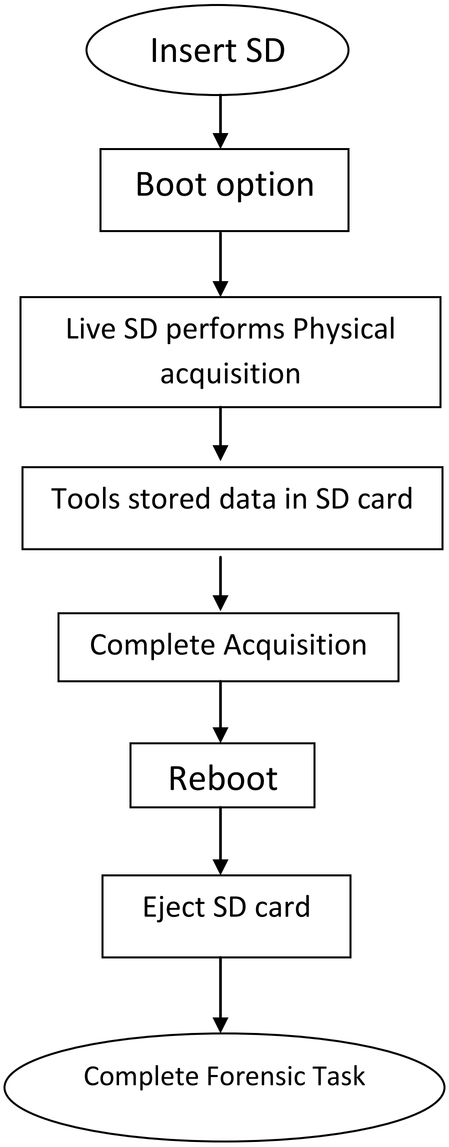


Figure 4.5 Flow chart of forensic task

Mobile phones have become a very important tool for personal communication. It is therefore of great importance that forensic investigators have possibilities to extract evidence items from mobile phones. Modern mobile phones store evidence items on SIM-cards as well as internal memories. With the advent of modern functionality, such as camera and multimedia messaging, more and more of these items are stored in internal memory. Proper forensic examination of such memories, including recovery of deleted items, has not been possible until now.

4.6.1 Preprocedure

The goal of preprocedure is preparing the required software and hardware for forensic tasks. The SD card which is to store the recovery tools and acquired data needs to be FAT32 formatted in order to correctly perform mount, read, or write operation. After format operation completes, the self-developed recovery tool can be copied and SD will be make bootable.

4.6.2 Forensic Task

As shown in Figure 4.5, forensic task is the procedure to perform forensics on the Android smart phone. The SD card should be inserted first, in turn Live acquisition mode should be entered during booting, and finally Live SD will perform physical acquisition through the users instruction in the targeted phone. The acquisition tool will run at boot time and recover and copy all the data in the SD card, and then the operating system should be rebooted to eject the SD card to continue the following data analysis.

Chapter 5 : EXPERIMENTATION RESULTS

We create an interface as a tool in this thesis we use four different applications for mobile data recovery. Here this tool is working only on Android platform. The application is work at boot time of the android OS. We already discuss how to boot android by SD card in previous chapter. These different applications are work for recover different type of data. All application is run by the user's instruction and after recover a data are saved in SD card. The description of the tools and result will be shown below with snapshots.

The Snapshots of the recovery tool is:

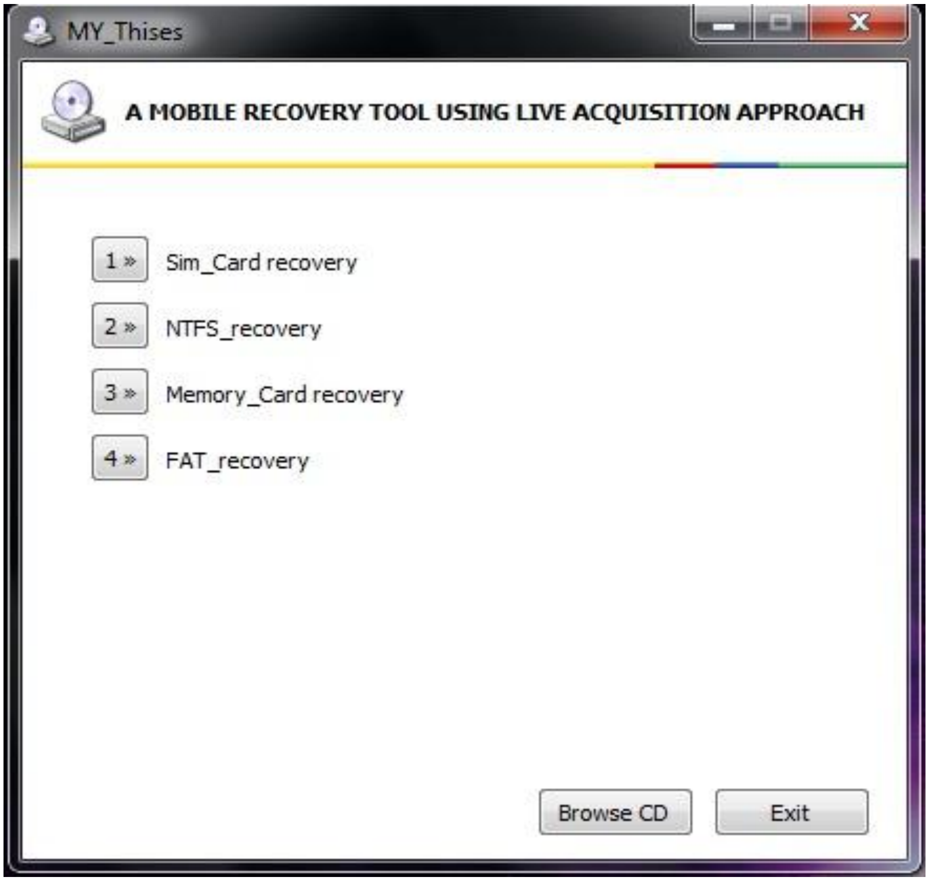


Figure 5.1 Recovery tool Interface Snapshot

Working:

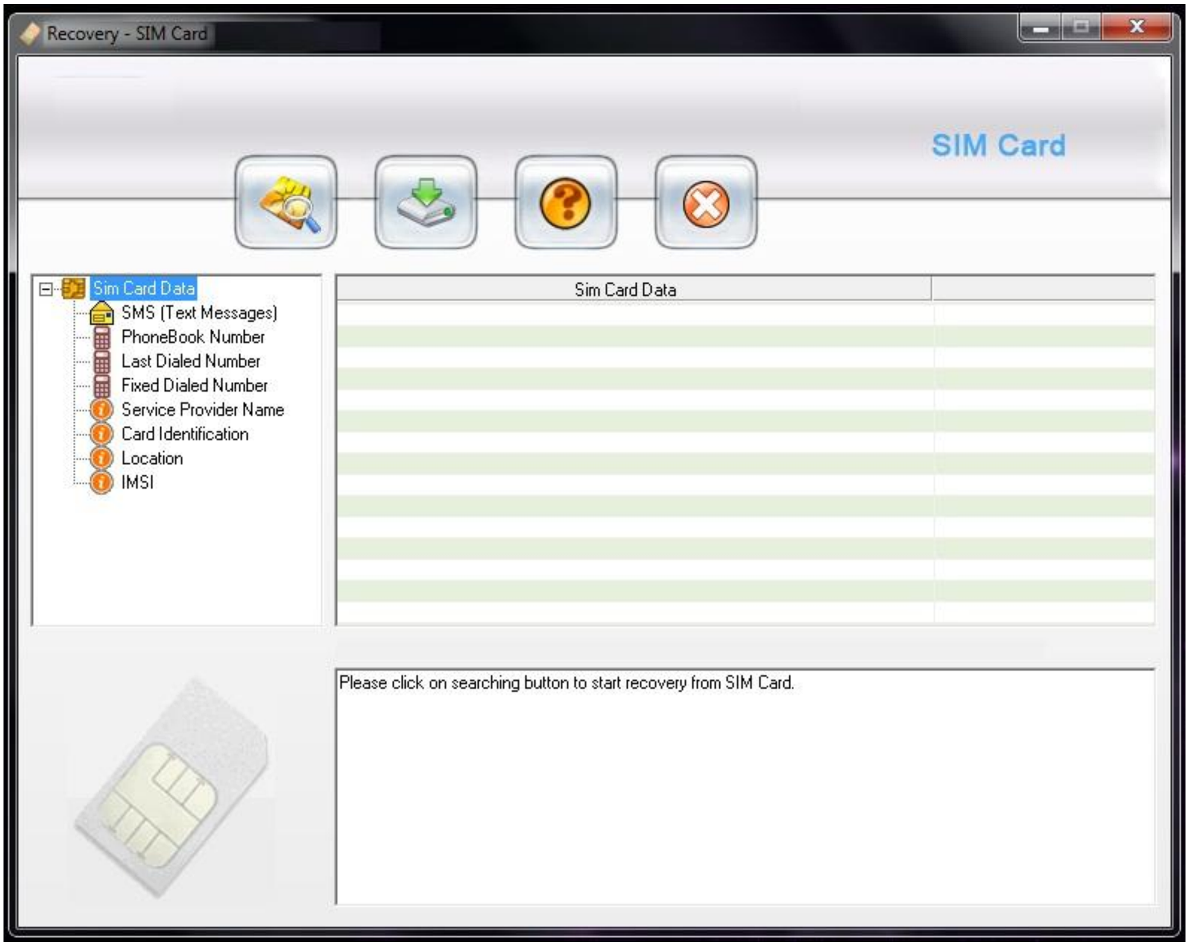
First insert the SD card into the mobile then enable the Fastboot mode in Android mobile to boot the phone through SD card. After that application is run and shows the options then user is deicide which one they will use. There are four different types of recovery tools. After recovery the data will be save in SD card.

The advantage of this tool is its working at the time of OS is crashed or corrupted. Forensic use is if they found the criminals mobile phone then they will easily recover all the data from the mobile but it must condition the mobile is in working condition.

5.1 RESULT AND DISCUSSION

In this interface we use following four tools are :

5.1.1 SIM Card Recovery



Please click on searching button to start recovery from SIM Card.

Figure 5.2 SIM Card recovery

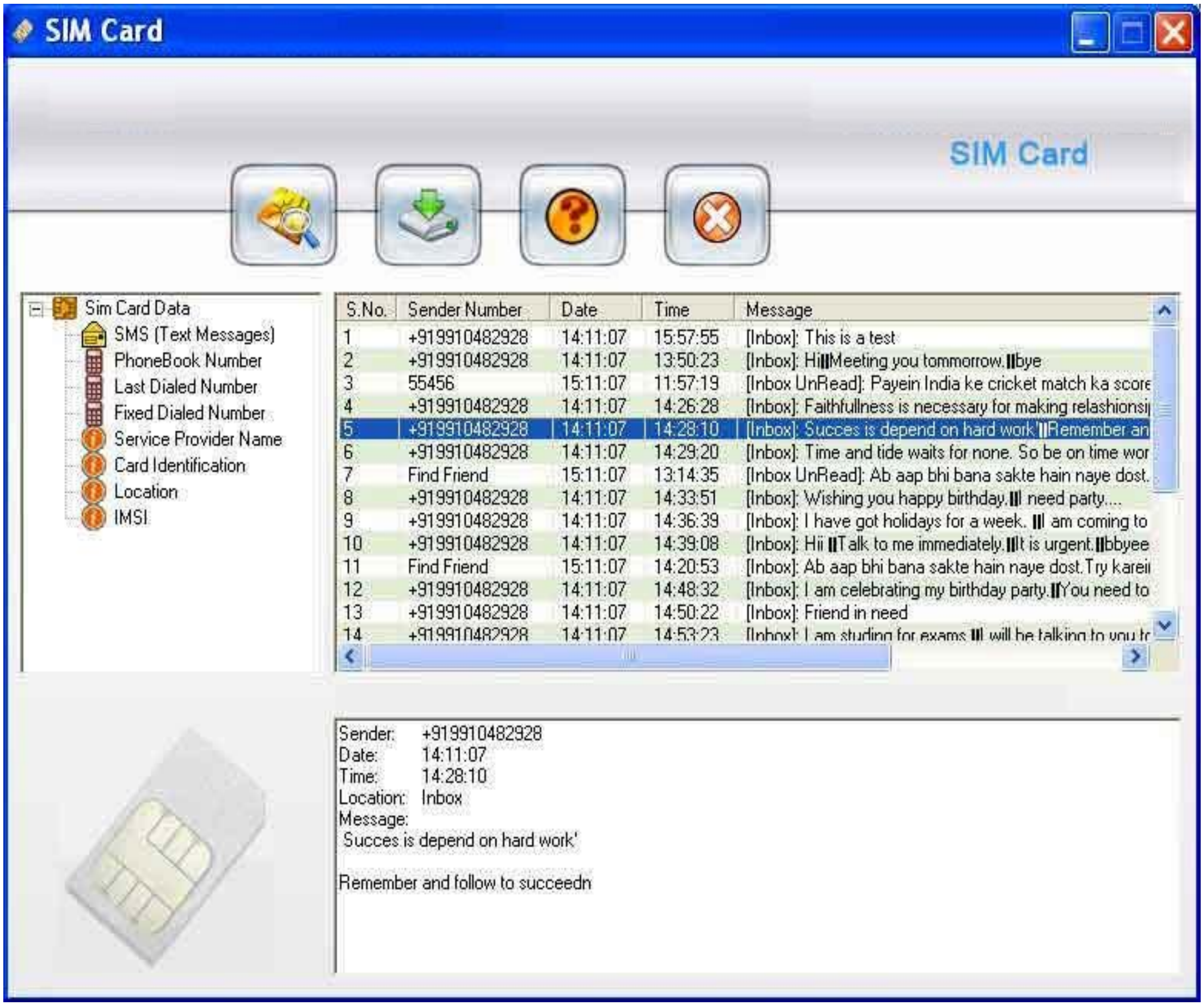
Mobile phone sim card message recovery tool supports retrieval of read and unread short messages SMS, contact name and number, phonebook directory from simcard. Software provides restoration of visible and invisible inbox, outbox, sent items messages. Utility provides rescue of encrypted text files that is corrupted due to computer viruses. Mobile data recovery software recovers sim card ICC-ID (identification number) and service provider name.

Software Features:

- Robust, flexible and economical application used to undelete all lost sim card details.
- Easily works with all GSM sim card readers of any service provider network (national and international).
- Safely revives text messages stored in Inbox/Outbox folders, Drafts messages, Send items, Phonebook numbers, Contact names, Sender Number with Date, Time and Location etc of mobile phone sim cards.
- Recovers entire sim card details missing due to accidental data deletion, Human fault, Software or Hardware malfunction and many more.
- Displays sim card IMSI number, ICC Mobile Identification number, Service provider name and many other sim cards details.
- Supports all PC/SC standards or Phoenix standard sim card reader used to connect the sim card with your computer.
- Offers user-friendly graphical interface that makes sim data recovery process simpler and easier for you.
- No technical skills or learning required while working with the sim card data recovery software.
- Simple, professional and profitable tool for mobile users, investigation agencies and forensic research.

Results:

SIM card message recovery solution is non-destructive and read only tool that recovers all corrupted data from your mobile phone SIM card. Cell phone SIM card data files recovery services retrieve read and unread inbox messages, outbox messages, sent items SMS (short message services) messages. Mobile SIM card data restoration tool restores accidentally deleted visible and invisible text messages, recovers contact name and number, phonebook directory from SIM card.



S.No.	Sender Number	Date	Time	Message
1	+919910482928	14:11:07	15:57:55	[Inbox]: This is a test
2	+919910482928	14:11:07	13:50:23	[Inbox]: Hi▮Meeting you tommorrow.▮bye
3	55456	15:11:07	11:57:19	[Inbox UnRead]: Payein India ke cricket match ka score
4	+919910482928	14:11:07	14:26:28	[Inbox]: Faithfullness is necessary for making relashionsi
5	+919910482928	14:11:07	14:28:10	[Inbox]: Succes is depend on hard work'▮Remember an
6	+919910482928	14:11:07	14:29:20	[Inbox]: Time and tide waits for none. So be on time wor
7	Find Friend	15:11:07	13:14:35	[Inbox UnRead]: Ab aap bhi bana sakte hain naye dost.
8	+919910482928	14:11:07	14:33:51	[Inbox]: Wishing you happy birthday.▮I need party....
9	+919910482928	14:11:07	14:36:39	[Inbox]: I have got holidays for a week. ▮I am coming to
10	+919910482928	14:11:07	14:39:08	[Inbox]: Hii ▮Talk to me immediately.▮It is urgent.▮bbyee
11	Find Friend	15:11:07	14:20:53	[Inbox]: Ab aap bhi bana sakte hain naye dost.Try karei
12	+919910482928	14:11:07	14:48:32	[Inbox]: I am celebrating my birthday party.▮You need to
13	+919910482928	14:11:07	14:50:22	[Inbox]: Friend in need
14	+919910482928	14:11:07	14:53:23	[Inbox]: I am studing for exams.▮I will be talking to you to

```
Sender:    +919910482928
Date:      14:11:07
Time:      14:28:10
Location:  Inbox
Message:
 Succes is depend on hard work'

Remember and follow to succeedn
```

Figure 5.3 Output of SIM Card recovery

5.1.2 NTFS Recovery

Deleted NTFS partition crashed hard disk drive data recovery repair corrupted files. Restore lost, damaged, Windows XP 2000 2003 file system volume recover MBR master boot record MFT master file table, root directory. undelete, unformat, formatted missing word excel documents pictures, photo from desktop laptop not detected ide ata sata scsi drive, virus attack power failure boot up problem permanent deletion or executing fdisk command.

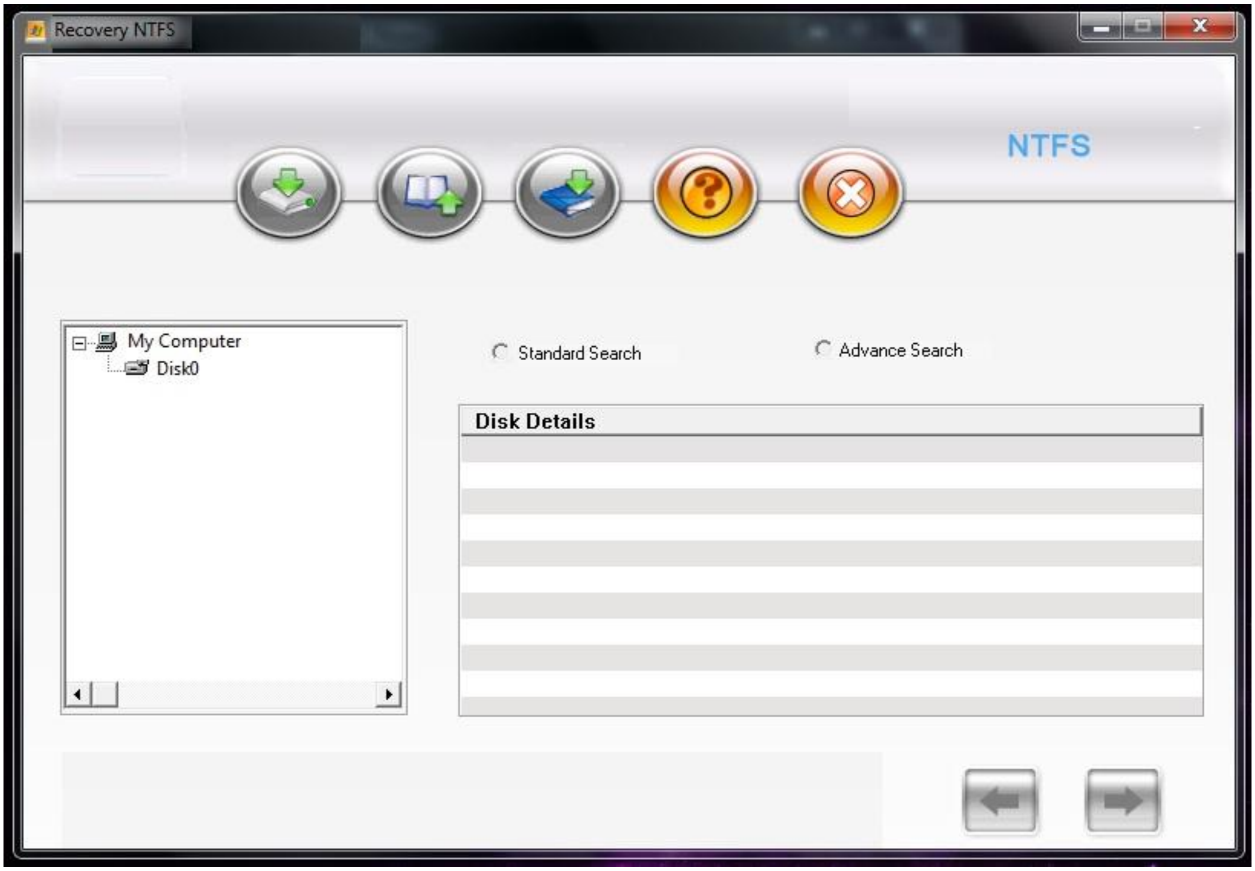
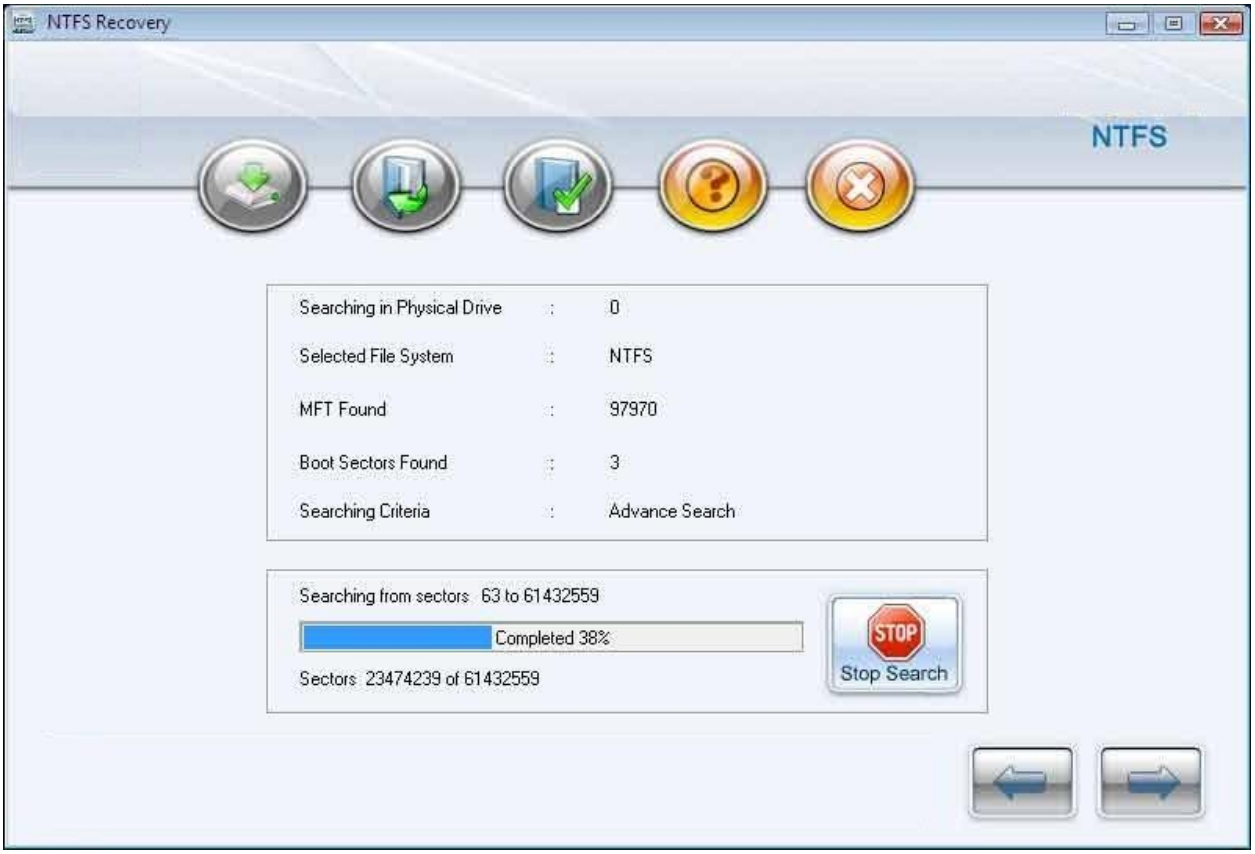


Figure 5.4 NTFS Recovery

Software Features:

- Read only, non-destructive, professional and easy to use NTFS data salvage utility.
- Recover deleted data from NTFS and NTFS5 file systems supported mass storage devices.
- Provides powerful disk scanning technique that helps in easy recovery of missing digital pictures, photos, snaps, images, songs folder (audio, video), documents and other confidential files.
- Easy recovery of deleted files due to Human mistake, System failure, Corrupted MFT and MBR files, Software/Hardware faults, Power failure etc.
- NTFS data recovery software for Windows is an effective tool to restore data deleted from Recycle Bin, OS failure, Boot sector failure, power fault and other similar reasons.
- Support all hard disks mass storage standards including SATA, ATA, IDE, EIDE and SCSI disk devices.

- Easy recovery of files from all major hard disk brands like Hitachi, Seagate, Samsung, Sony, Maxtor, HP, Toshiba, IBM, Fujitsu and many more.
- Software has new streamlined user interface with enhanced graphics that helps in easy to work even for non-technical users.



```
Searching in Physical Drive   :   0
Selected File System          :   NTFS
MFT Found                     :   97970
Boot Sectors Found            :   3
Searching Criteria            :   Advance Search

Searching from sectors  63 to 61432559
Completed 38%
Sectors  23474239 of 61432559
```

Figure 5.5 Output of NTFS Recovery

5.1.3 Memory Card Recovery

Memory card files retrieval SD compact flash multimedia mmc data recovery software utility retrieve rescue repair restore recover undelete unerase unformat lost erased accidentally deleted formatted corrupted pictures images photos audio video files folders usb Smart Media digital camera storage JPG JPEG TIF GIF RiFF TIFF AVI PNG BMP 3gp MPEG MOV WAV MIDI restoration mobile phone 3gp mms mobile communicator chip nokia sony Samsung

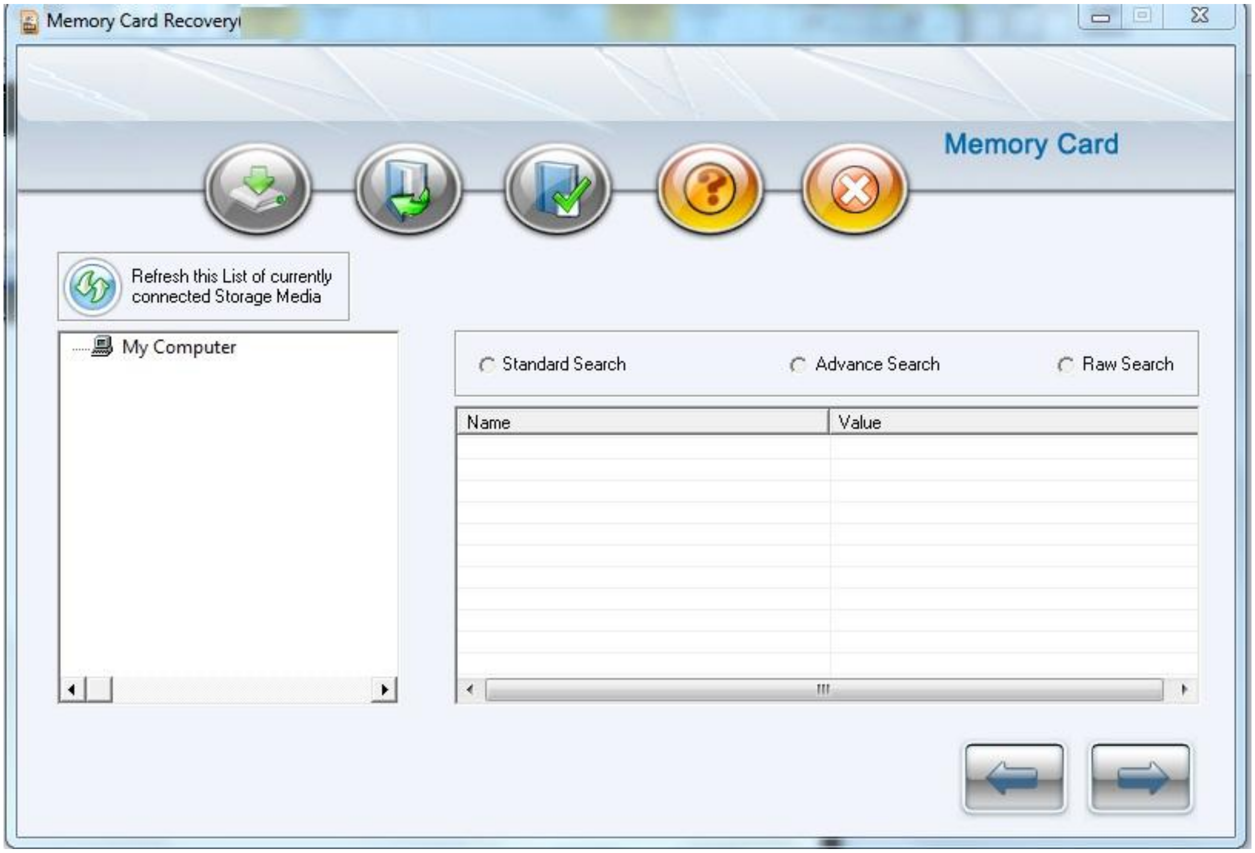


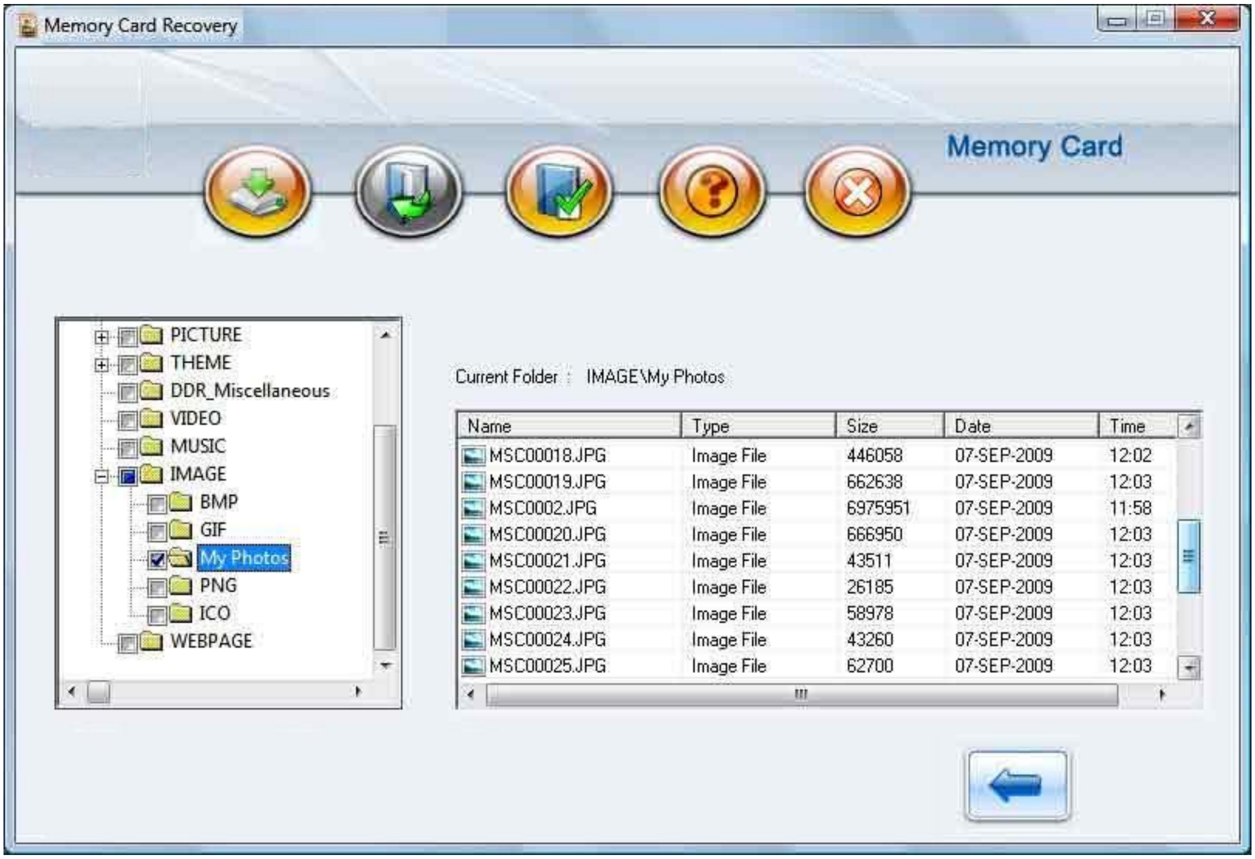
Figure 5.6 Memory Card

Software Features:

- Safe and secure retrieval of deleted, erased or missing files and information from corrupted or damaged memory cards.
- Supports easy recovery of all media files including image files (tiff, png, bmp, gif, jpg), video files (asf, 3gp, avi, mpeg, mov), audio files (midi, mp3, aac, mpa, ram), text file (txt, doc, dbt) and many more file formats from undetectable memory cards.
- Support all USB memory card storage media devices including Compact Flash Memory card, Secure Digital SD (micro SD, SDHC, mini SD, SDHC Plus), Multimedia Card, xD Picture card, Memory Stick (MS Pro, Micro M2, MS Pro DUO, MS) and other commonly used memory card storage media.
- Support all branded memory cards like Sanyo, Kodak, Olympus, Sony, Umax, Aiptek, BenQ, Casio, Lumicron, Konica, Canon, Nikon, Acer, Philips, Yakumo, Digital Dream and many more.

- Provide user-friendly graphical interface and no special technical training needed to work with software.

Results:



Current Folder : IMAGE\My Photos

Name	Type	Size	Date	Time
MSC00018.JPG	Image File	446058	07-SEP-2009	12:02
MSC00019.JPG	Image File	662638	07-SEP-2009	12:03
MSC0002.JPG	Image File	6975951	07-SEP-2009	11:58
MSC00020.JPG	Image File	666950	07-SEP-2009	12:03
MSC00021.JPG	Image File	43511	07-SEP-2009	12:03
MSC00022.JPG	Image File	26185	07-SEP-2009	12:03
MSC00023.JPG	Image File	58978	07-SEP-2009	12:03
MSC00024.JPG	Image File	43260	07-SEP-2009	12:03
MSC00025.JPG	Image File	62700	07-SEP-2009	12:03

Figure 5.7 Output of Memory Card Recovery

Memory Card Files retrieval data recovery software is easy and Non-Destructive Data restoration software utility and reliable solution to recover retrieve rescue repair restore undelete unerase or unformat your lost erased formatted deleted pictures images photos audio video files and folders from mmc multimedia memory card and flash memory of your Digital camera mobile phone pocket pc mp3 player mobile communicator pda handheld computer and other memory card chip storage media.

5.1.4 FAT Recovery

Recovery software restores missing FAT12 FAT16 FAT32 VFAT format partition file systems. FAT partition recovery software recover hard disk drive data files folders like outlook express

MBX DBX files acrobat PDF Microsoft Office Word *.doc, Access *.MDB, PowerPoint *.PPT files and mp3, mp4, DAT, MPEG, MPG, MOV, MIDI audio video movies and corrupted pictures like Jpg GIF, PNG, RIFF and PSD compressed and encrypted data support all most all formats. Software provides recovery from previously existing partition. Full support for long files names, encrypted and compressed files. Logically damaged or corrupted partition can be recovered by the software. Software is read only and non destructive support windows operating systems.

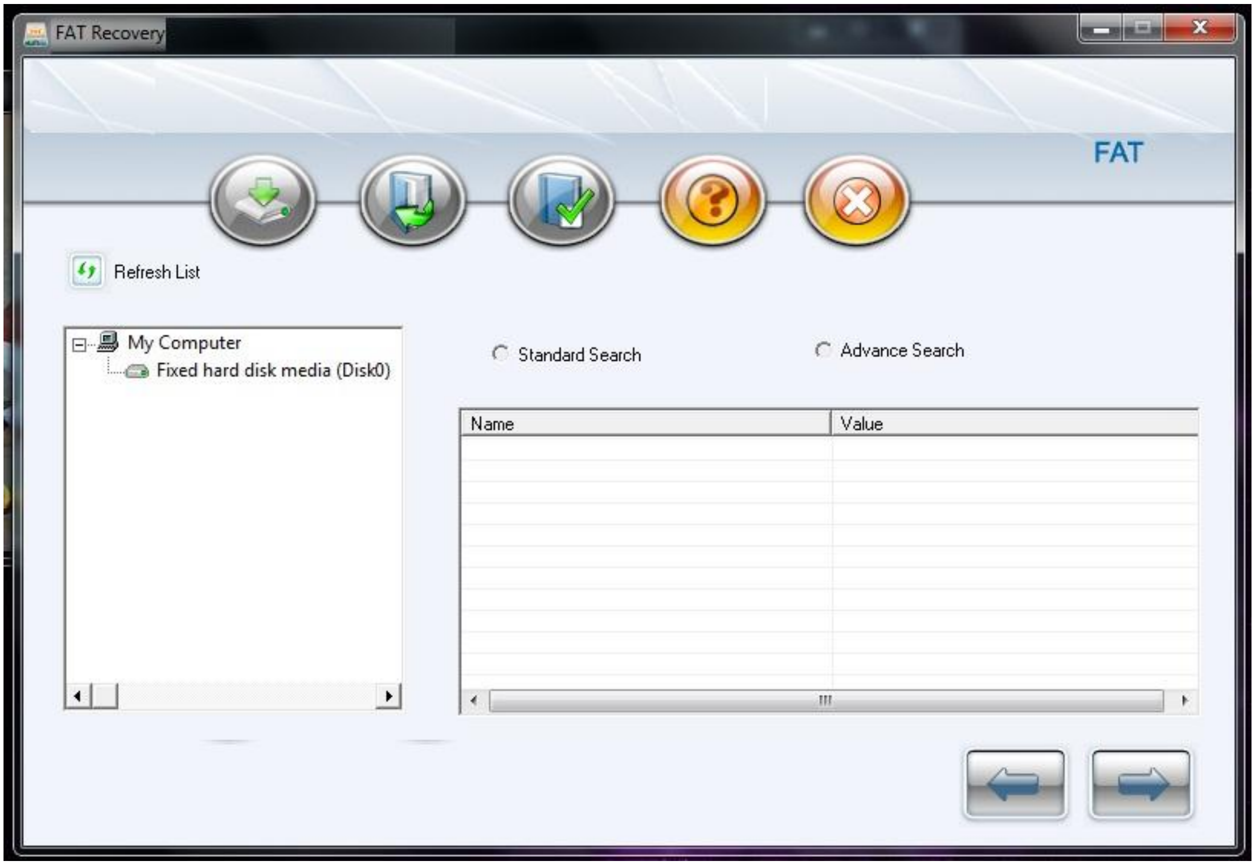


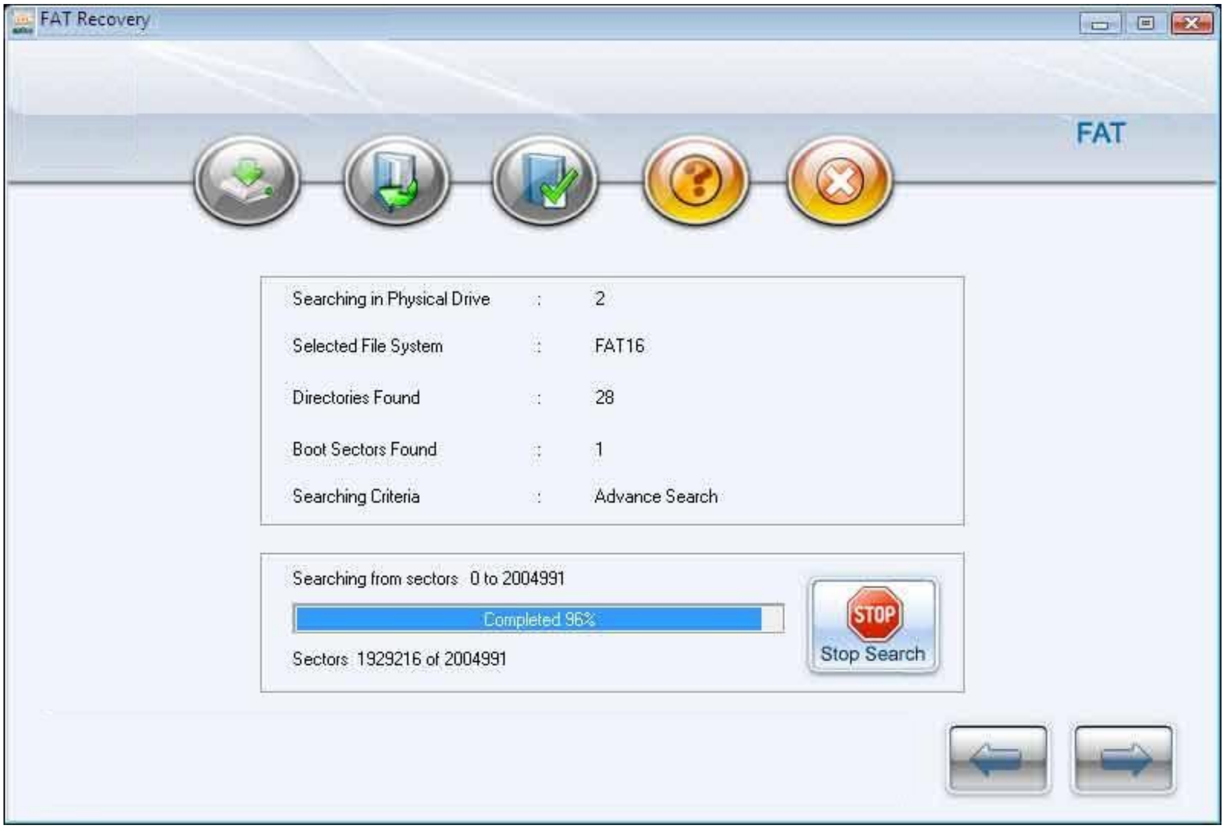
Figure 5.8 FAT Recovery

Software Features:

- Efficient, effective with simple functionality and a cost-effective easily affordable program for your lost data recovery.
- Recovers lost deleted, or corrupted audio-video files, digital images, photos, pictures, snaps, important documents from logically corrupted disk drives.

- Recover data even from Re-formatted hard disk, MFT or MBR failure, BIOS error, Operating System failure and many more.
- Support all hard disks types including IDE, SATA, ATA, EIDE and SCSI disk devices.
- Efficiently works with all major hard disk brands like Samsung, Hitachi, Seagate, Sony, Toshiba, Maxtor, HP, IBM, Quantum and many more.
- Friendly graphical interface, thus user can directly interact with the software without requiring any expert knowledge.

Results:



Searching in Physical Drive : 2
Selected File System : FAT16
Directories Found : 28
Boot Sectors Found : 1
Searching Criteria : Advance Search

Searching from sectors 0 to 2004991
Completed 96%
Sectors 1929216 of 2004991

Figure 5.9 Output FAT Recovery

Tool recovers Compressed and encrypted data lost by power surges inaccessible disk. Data recovery software for all windows FAT file systems partition hard disk drive files folders provides rescue from data loss due to unexpected shutdown of system, accidentally deleted crashed disk data. Recovery software scans inaccessible hard disk, retrieve data and restore at safe location on your storage media.

Chapter 6 : CONCLUSION AND FUTURE WORK

6.1 CONCLUSION

Android is a fast-developing and popular smart phone operating system. It is capable of software augmentation and contains rich personal information where makes people rely on these devices. In recent years, information criminal cases are mushrooming than ever, personal information leakage and Bot Network are no news anymore.

As a result, besides users' daily prevention, how forensic examiners can help acquire information from victims' phones after harm happens becomes the most important issue now. The present business-edition digital forensic software is not affordable for the public, and most of them adopt internal logical acquisition.

This methodology is questionable because it cannot be confirmed if the scenes have been modified, which is forbidden in forensics, after the software is installed to the mobile phone. Moreover, another potential issue is the damaged data may not be recovered because logical acquisition utilizes API to access the data. Our work makes use of the characteristic where Android allows users to update software packages legally to design and implement the Live SD physical acquisition forensic tool referring to Live CD/DVD/USB forensics in computers. This methodology utilizes the Booting mode in Android platform to perform data acquisition and copy the data from the database in SD card, which means the forensic software does not need to be installed to prevent potential issue of modifying the crime scene.

6.2 FUTURE WORK

In the future, we will pay more focus on the damaged data recovery and instant data acquisition based on this work. The number of unique mobile phones is extensive. Phonescoop.com is a comprehensive database of 992 mobile phones, and covers information for thirty seven phone manufacturers and fifteen carriers. Standards are not only different across manufacturers and carriers but they differ from phone to phone as well. This makes acquiring data very difficult since each phone must be individually addressed.

As a result, forensic tool manufacturers maintain lists of compatible phones and supported features for their software. Although mobile forensic tools provide solutions for multiple types of phones, familiarity with multiple toolkits is necessary for thorough coverage. As the evidentiary value of data contained in mobile phones becomes more apparent, tools must become increasingly reliable and continuously improved to ensure data integrity.

Particularly, forensic tools must increase the granularity on how hashes are calculated for distinct data objects such as address books, text messages, call logs, etc. Each data type provides a unique fingerprint that is believed to remain consistent across multiple acquisitions. Data types that are independent from the phone software such as standard image and sound formats should remain consistent across various phones as well. Although phones will still require proprietary methods to acquire data, a more standardized way of organizing and maintaining acquired data is possible.

References

[1] Anandabrata Pal and Nasir Memon "The Evolution of File Carving", IEEE Signal Processing Magazine, 1053-5888/09©2009IEEE.

[2] Mo Chen, Ning Zheng, Ming Xu, Yongjian Lou, Xia Wang , College of Computer, Hangzhou Dianzi University Hangzhou, 310018, China, "Validation Algorithms Based on Content Characters and Internal Structure: The PDF File Carving Method", 2008 IEEE ,DOI 10.1109/ISISE.2008.209.

[3] http://www.forensicswiki.org/wiki/Tools:Data_Recovery

[4] http://en.wikipedia.org/wiki/Forensic_analyst

[5] Lei Pan Lynn, M. Batten [ln, lmbatteng]@deakin.edu.au, School of Engineering and Information Technology, Deakin University, 221 Burwood Highway, Burwood, Melbourne, Victoria 3125, Australia "An Effective and Efficient Testing Methodology fo Correctness Testing for File Recovery Tools" 2005.

[6] http://foremost.sourceforge.net/

[7] http://www.digitalforensicssolutions.com/Scalpel/

[8] http://www.cgsecurity.org/wiki/PhotoRec

[9] http://www.forensicswiki.org/wiki/EnCase

[10] Christiaan Beek, Principal Security Consultant McAfee® Foundstone® Professional Services , "Introduction to File Carving", Copyright © 2011 McAfee, Inc.39301wp_file-carving_1111_fnl_ETMG

[11] Carlos Gutierrez, Secretary, U.S. Department of Commerce, Technology Administration Robert C. Cresanti, Under Secretary for Technology William Jeffrey, Director , National Institute of Standards and Technology ,"Guidelines on Cell Phone Forensics" MD 20899-8930 May 2007.

[12] www.investigation.com/cell_phone_forensics.htm

[13] Svein Y. Willassen, Norwegian University of Science and Technology, "Forensic analysis of mobile phone internal memory", year may 2004.

[14] R. Ayers, W. Jansen, L. Moenner, and A. Delaitre, "Cell Phone Forensic Tools: An Overview and Analysis Update," National Institute of Standards and Technology, 2007.

[15] Android.com, Android Timeline, http://www.android.com/about/timeline.html, Retrieved March, 2011.

[16] Gartner, Worldwide Smartphone Sales to End Users by Operating System in 2009, http://www.gartner.com/it/page.jsp?id=1306513, Retrieved February, 2011.

[17] Gartner, Worldwide Smartphone Sales to End Users by Operating System in 2Q10, http://www.gartner.com/it/page.jsp?id=1421013, Retrieved February, 2011

[18] W. N. Wu, Y. L. Lin and C. P. Chang, Explore the Smart phone digital forensic study of operating procedures and tools, 2009.

[19] Androids Dream, Lookout, http://blog.mylookout.com/2011/03/do-androids-dream, Retrieved March, 2011.

[20] Y. J. Chen, A Study of Influential Factors on Smartphone Third Party Application Developers' Decisions of Preferential Linkage, 2007.

[21] S. Raghav and A. K. Saxena, Mobile Forensics: Guidelines and Challenges in Data Preservation and Acquisition, 2009.

[22] R. Ahmed and R. V. Dharaskar, "Mobile Forensics: an Overview, Tools, Future trends and Challenges from Law Enforcement perspective, " 2008.

[23] S. J. Wang, Y. H. Ke and ICCL- Information Cryptology & Construction Lab, Computer forensics and digital evidence: Information security technology, technology crime prevention, identification and scene reconstruction, DrMaster Press Co., Ltd., 2007.

[24] S. J. Wang and C. H. Lin and ICCL Information Cryptology & Construction Lab, "Security and forensics of digital technology: high-tech crime prevention and digital evidence gathering", DrMaster Press Co., Ltd., 2009.

[25] W. Jansen, and R. Ayers, "An overview and analysis of PDA forensic tools," Digital Investigation", Volume 2, Issue 2, pp. 120-132, June 2005.

[26] Oxygen Phone Manager , Software Package, Commercial. Available: http://www.oxygensoftware.com/

[27] R. Ayers, W. Jansen, L. Moenner, and A. Delaitre, "Cell Phone Forensic Tools: An Overview and Analysis Update," National Institute of Standards and Technology, 2007.

[28] Android.com, Platform Version, http://developer.android.com/intl/zh-TW/resources/dashboard/platform-versions.html, Retrieved March, 2011.

[29] B. Carrier. “ Defining Digital Forensics Examination and Analysis Tools ” . In Digital Research Workshop , 2002.

[30] Richard, Golden, Roussev, V., "Scalpel: a frugal, high performance file carver”, in Proceedings of the 2005 digital forensics research workshop, DFRWS, August 2005.

[31] S.Garfinkel , “ Carving contiguous and fragmented files with fast object validation ,” in Proc. 2007 Digital Forensics Research Workshop (DFRWS) ,Pitts-burgh , PA , Aug. 2007.

[32] http://www.cnwrecovery.com/html/data_carving.html

[33] Carving contiguous and fragmented files with fast object validation Simson L. Garfinkela,b aNaval Postgraduate School, Monterey, CA,USA bCenter for research on Computation and Society, School of Engineering and Applied Sciences, Harvard University, Cambridge, MA, USA.

[34] DFRWS 2006 Forensics Challenge File Image Details. Retrieved Jan. 09, 2011 from Digital Forensics Research Conference (DFRWS):

http://www.dfrws.org/2006/challenge/submission.shtml

[35] Bora Park, Antonio Savoldi, Paolo Gubiar, Jungheum Park, Seokhee Lee and Sangjin Lee, “Recovery of Damaged Compressed Files for Digital Forensic Purposes”, MUE 2008 Vol.2 No.1, SERSC, Korea, 24 April 2008, pp. 365-372.

[36] Brian Carrier, File System Forensic Analysis, Addison-Wesley Professional, 22 March 2009.

[37] S. L. Garfinkel, P. Farrell, V. Roussev, and G. Dinolt, “Bringing sci-ence to digital forensics with standardized forensic corpora,” in Proc. 9th Annual Digital Forensic Research Workshop (DFRWS), Quebec,Canada, Aug. 2009.

[38] S. Axelsson, “Using normalized compression distance for classifying file fragments,” in IEEE International Conference on Availability, Reliability and Security, 2010, pp. 641–646.

[39] Luigi Sportiello, Stefano Zanero,Dipartimento di Elettronica e Informazione,Politecnico di Milano,Milan, Italy{sportiello, zanero}@elet.polimi.” File Block Classification by Support Vector Machines ” 2011 Sixth International Conference on Availability, Reliability and Security.

[40] Svein Y. Willassen, Norwegian University of Science and Technology, "Forensic analysis of mobile phone internal memory"

[41] K. Kalajdzic and A. Patel. A fast practical method for recovery of lost files in digital forensics, Journal of Internet Technology, 10(5), pp. 539-546, October 2009.

[42] Yingjie Wei, Computer and Software Institute, Hangzhou Dianzi University, Hangzhou Zhejiang, China weiyjhz@live.cn, Ning Zheng, Ming Xu Computer and software Institute

[43] Hangzhou Dianzi University Hangzhou Zhejiang, China nzheng@hdu.edu.cn, mxu@hdu.edu.cn, 2010 Second International Conference on Information Technology and Computer Science.

[44] John Haggerty, Member, IEEE, Qi Shi, Member, IEEE, and Madjid Merabti, Member, IEEE, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 23, NO. 10, OCTOBER 09.

[45] STORAGE search.com. Data Recovery from Flash SSDs?[Online] Available: http://www.storagesearch.com/recovery.html

[46] Amiya Kumar Maji, Kangli Hao, Salmin Sultana, and Saurabh Bagchi , School of Electrical and Computer Engineering, Purdue University, West Lafayette, Indiana, USA, famaji, khao, ssultana, sbagchig@purdue.edu "Characterizing Failures in Mobile OSes: A Case Study with Android and Symbian" .

[47] EnCase, Software Package, Commercial. Available: http://www.encase.com/

[48] S. Willassen, Forensics and the GSM mobile telephone system, International Journal on Digital Evidence 2003:2:1.

[49] R.F. Erbacher and J. Mulholland. Identification and localization of data types within large-scale file sys-tems. In Second International Workshop on Sys-tematic Approaches to Digital Forensic Engineering, (SADFE'07), pages 55–70. IEEE Computer Society, 2007.

[50] W. C. Calhoun and D. Coles, "Predicting the types of file fragments,"in Proceedings of the 2008 DFRWS Conference, 2008, pp. S14–S20.

[51] S. Axelsson, "The normalised compression distance as a file fragment classifier," in Proceedings of the 2010 DFRWS Conference , 2010, pp. S24–S31

[52] G. G. Richard, III and V. Roussev, “Scalpel: A Frugal, High Performance File Carver,” inRefereed Proceedings of the 5th Annual Digital Forensic Research Workshop (DFRWS’05),2005.

[53] S. L. Garfinkel, “Carving Contiguous and Fragmented Files with Fast Object Validation,”Digital Investigation, vol. 4, no. S1, pp. 2–12, 2007, Proceedings of the Seventh Annual DFRWS Conference.

[54] S. Axelsson, “The Normalised Compression Distance as a file fragment classifier,”Digital Investigation, vol. 7, no. S1,pp. 24–31, 2010, Proceedings of the Tenth Annual DFRWS Conference.

[55] HCG Leitao, J Stolfi. A Multiscale Method for the Reassembly of Two-dimensional Fragmented Objects. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2002, 24(9): 1239-1251.

[56] Ryan M. Harris, “Using Artificial Neural Networks for Forensic File Type Identification”. CERIAS Tech Report 2007-19, Purdue University, 2007.

[57] NIST. Deleted file recovery tool specification. Technical report, NIST, 2005.

[58] L. Pan and L. M. Batten. Reproducibility of Digital Ev-idence in Forensic Investigations. In 5th Digital Forensic Research Workshop (DFRWS 2005), 2005.

[59] W. Adrion, M. Branstad, and J. Cherniavsky. Validation, verification, and testing of computer software. ACM Com puter Survey, 14(2):159–192, 1982.

[60] L. Pan and L. M. Batten. A Lower Bound on Effective Per-formance Testing for Digital Forensic Tools. In IEEE the 2nd International Workshop on Systematic Approaches to Digital Forensic Engineering, (SADFE 2007), pages 117–130, 2007.

[61] M. McDaniel and M. Hossain Heydari. Content based file type detection algorithms. In Proceedings of the 36th Hawaii I nternational Conference on Systems Sci-ences (HICCS’03), volume 09, page 332a. IEEE Com-puter Society, 2003.

[62] A.Chou, J.Yang, B.Chelf, S.Hallem, and D.Engler. “An Empirical Study of Operating Systems Errors,” In Proc. of 18th ACM Symposium on Operating Systems Principles (SOSP), P. 73–88, 2001.