Forensic Analysis of Cellular Phones

GRADUATE PROJECT REPORT

Submitted to the Faculty of
the Department of Computing Sciences
Texas A & M University- Corpus Christi
Corpus Christi, Texas

in Partial Fulfillment of the Requirements for the Degree of
Master of Science in Computer Science

by

Suman Paladugu

Fall 2008

Committee Members

Dr. Mario Garcia
Committee Chairperson

Dr. Long-zhuang Li
Committee Member

Dr. David Thomas
Committee Member
Forensic Analysis of Cellular Phones

GRADUATE PROJECT REPORT

Submitted to the Faculty of
the Department of Computing Sciences
Texas A & M University- Corpus Christi
Corpus Christi, Texas

in Partial Fulfillment of the Requirements for the Degree of
Master of Science in Computer Science

by

Suman Paladugu

Fall 2008

Committee Members

Dr. Mario Garcia
Committee Chairperson

Dr. Long-zhuang Li
Committee Member

Dr. David Thomas
Committee Member
ABSTRACT

The use of cell phone forensics has increased along with the rise in cell phone usage and technology. The ability to pinpoint recent locations, review call logs, examine existing and deleted text messages, pictures, videos and (in the case of wireless handheld devices) read email, has created a whole new source for evidence. Due to advanced improvements in cell phone technology, mobile phones can now be used in multiple ways. Not only is a cell phone used as a device with which to speak to others, but also as an editor and a portable data carrier. Securing a mobile phone for such data stored within it can be of utmost importance.

This paper examines the nature of some newer pieces of information which can become potential evidence on mobile phones. It also discusses some of the emerging technologies and their potential impact on mobile phone based evidence. Finally, this report shows the need for continuing in-depth examination of mobile phone evidence.
# TABLE OF CONTENTS

Abstract .............................................................................................................................................. ii  

Table of Contents ........................................................................................................................ iii  

List of Figures ................................................................................................................................... iv  

1. Background and Rationale ........................................................................................................... 1  
   1.1. Introduction ........................................................................................................................ 1  
   1.2. The Need of use of Mobile Forensics .............................................................................. 1  
      1.2.1 Law Enforcement, Cell Phones and Criminals .......................................................... 1  
      1.2.2 Mobile Phones in E-Commerce ................................................................................. 1  
   1.3. Mobile Forensics Background ......................................................................................... 2  
   1.4. Mobile Phone Data as Evidence .................................................................................... 4  
      1.4.1 Subscriber .................................................................................................................. 4  
      1.4.2 Mobile Station .......................................................................................................... 4  
      1.4.3 Mobile Network ....................................................................................................... 5  

2. Narrative ...................................................................................................................................... 7  
   2.1. Attacks and Crimes with Mobile Phones ..................................................................... 7  
   2.2. Mobile Phone Evidence ................................................................................................. 7  
      2.2.1 Locations of Memory in Mobile Phones ................................................................. 9  
   2.3. Techniques for Data Acquisition ................................................................................... 12  
   2.4. Evidence Collection ....................................................................................................... 14  
   2.5. Major Problems During Extraction of Data from Mobile Phones............................... 14  
   2.6. Scope of Present Research .......................................................................................... 11
2.7 Future Concerns in Mobile Forensics ..............................................................11
  2.7.1 Dealing with the Trust Issue .................................................................12
3. Proposed Research Work ..................................................................................19
  3.1 System Requirements ..................................................................................19
  3.2 Analysis and Comparison of Tools ..............................................................19
  3.3 Elucidation of Scenarios ..............................................................................20
  3.4 Procedure for Extracting Data from the Memory .......................................23
    3.4.1 Extracting the Data from Mobile Phones ..............................................23
    3.4.2 Extracting the Data from SIM Cards ....................................................24
    3.4.3 Extracting the Data from Phone Memory .............................................25
  3.5 Research on Freeware, Shareware and Commercial Tools .......................25
    3.5.1 Research on Mobile Phone Forensic Tools ..........................................25
    3.5.2 Research on Hashing Tools .................................................................33
    3.5.3 Research on Miscellaneous Tools .........................................................41
    3.5.4 Research on Steganography Tools .........................................................42
    3.5.5 Research on Recovery Tools .................................................................45
  3.6 Research on Commercial Tools – Encase ....................................................48
  3.7 Research on SIM Card tools ........................................................................51
    3.7.1 Dekart SIM Explorer ...........................................................................52
4. Testing and Evaluation ......................................................................................54
  4.1 Testing on Mobile Forensic Tools .................................................................54
    4.1.1 Mobiledit Forensic ...............................................................................54
    4.1.2 Mobile Phone Inspector .......................................................................58
4.2 Testing on Hashing Tools

4.2.1 Hashing Calculator

4.2.2 JSsummer

4.2.3 MD5 GUI

4.2.4 MUSASH

4.2.5 Fsum Frontend

4.3 Testing on Miscellaneous Tools:

4.3.1 Forensic IM Extractor

4.4 Testing on Steganography Tools

4.4.1 Duplicate File Finder

4.4.2 Dup Finder (DUFF)

4.5 Testing on Recovery Tools

4.5.1 Digital Picture Recovery Tool

4.5.2 F-Recovery for Memory Card

4.5.3 Undelete SD Card

4.6 Testing on SIM card Tools:

4.6.1 Dekart SIM Explorer

4.7 Testing on Commercial Tools-Encase

5. Future Concerns in Mobile Forensics

6. Conclusion

7. Bibliography
LIST OF FIGURES

Figure 1.1 Phase -1 of a SIM.................................................................  3
Figure 1.2 Phase -2 of a SIM.................................................................3
Figure 2.1 Showing the SIM card slot in the Phone .................................10
Figure 2.2 SIM Internal Architecture ..................................................11
Figure 2.3 External Memory Sticks for Mobile Phone............................12
Figure 3.1 Sony Ericsson w810i accessed via Mobiledit.........................28
Figure 3.2 SIM Phonebook..................................................................30
Figure 3.3 Exported address book from Mobiledit when accessed a SIM card from mobile phone.................................................................31
Figure 3.4 Mobile Inspector tool window .............................................32
Figure 3.5 Hash calculator..................................................................35
Figure 3.6 Hashing calculator options..................................................35
Figure 3.7 JSummer...........................................................................36
Figure 3.8 MD5 GUI window..............................................................37
Figure 3.9 MUSASH window..............................................................38
Figure 3.10 Fsum Frontend window....................................................39
Figure 3.11 Belkasoft window profiles .................................................41
Figure 3.12 Duplicate File Finder........................................................44
Figure 3.13 DUFF Window.................................................................45
Figure 3.14 Digital picture recovery tool.............................................46
Figure 3.15 Recovery tool window......................................................47
Figure 3.16 Undelete SD card tool window.........................................48
Figure 3.17 Encase tool....................................................................50
Figure 3.18 Dekart SIM card Explorer window………………………………………53
Figure 4.1 SIM card analysis using Mobiledit Forensic tool……………………55
Figure 4.2 Comparison of a ordinary file with a steganography file………………57
Figure 4.3 Mobiledit accessing phonebook from mobile phone…………………57
Figure 4.4 Extraction of data from Nokia 3220…………………………………….59
Figure 4.5 String input in the Hashing Calculator………………………………..61
Figure 4.6 Inserting a comma at the end of input string in Hashing Calculator…..62
Figure 4.7 Hashing Calculator with original string in the textbox………………..62
Figure 4.8 Comparison of hash values to calculate the checksum…………………..62
Figure 4.9 Checksum match………………………………………………………….62
Figure 4.10 JSummer supported algorithms ………………………………………..63
Figure 4.11 JSummer tool calculating md5 values of multiple files at the same
time……………………………………………………………………………………64
Figure 4.12 Status of checksum value of files………………………………………….66
Figure 4.1 MUSASH calculating the hash values and comparison of files…………68
Figure 4.14 Comparison of files using MUSASH………………………………….69
Figure 4.15 FSum Frontend tool ……………………………………………………..71
Figure 4.16 Selection of various messengers existed in the system…………………..73
Figure 4.17 Selecting one of the chat profiles from the list…………………………74
Figure 4.18 Selecting the contacts first to extract the history…………………………74
Figure 4.19 Summary of the extracted information from Forensic IM Extractor tool……75
Figure 4.20 Forensic IM extracted history opened in notepad………………………..76
Figure 4.21 Selecting the directory for finding duplicate files…………………………79
Figure 4.22 Duplicate files search
Figure 4.23 Tool displaying the duplicate files found in the given directory
Figure 4.24 DUFF window
Figure 4.25 DUFF scanning for duplicate files in selected directories
Figure 4.26 Duplicate files found in the selected directories
Figure 4.27 Recovered files from the memory card using Picture Recovery tool
Figure 4.28 Recovered pictures saved in the folder using Picture Recovery tool
Figure 4.29 Recovery process of images deleted in the memory stick using F-recovery tool
Figure 4.30 Deleted files recovered are saved in folder named “Deleted”
Figure 4.31 Recovered files saved in the folder named “Lost”
Figure 4.32 Results of Encase showing the image as Non standard image
Figure 4.33 Encase tracing the file as deleted
Figure 4.34 Encase tracing bad signature files
Figure 4.35 Encase tracing the deleted and overwritten file
## LIST OF TABLES

Table 3.1 Scenario Table ........................................................................................................20
Table 3.2 Encase Scenario Table .......................................................................................... 51
Table 4.1 Functionalities of Dekart Explorer .......................................................................96
Table 4.3 Encase process scenario table ............................................................................... 97
Table 4.4 Encase testing scenario table ............................................................................... 98
1. BACKGROUND AND RATIONALE

1.1 Introduction

The use of mobile technology has increased considerably in recent times. With advanced technology, the mobile phone is used in multiple ways, including camera, data storage device and as a tool for accessing the internet. Due to the personal nature of the mobile phone and its use, the capacity to store confidential information on the device itself is vital. This trend has increased the potential for stored information on mobile phone handsets to be used as evidence in civil or criminal cases.

1.2. The Need for use of Mobile Phone Forensics

The need for mobile phone forensics is discussed based on the following topics:

- Law enforcement, cell phones and criminals
- Mobile phones use in E-Commerce
- Use of mobile phones in storing and broadcasting messages

1.2.1 Law Enforcement, Cell Phones and Criminals

Since cellular phones are portable devices, they can be, and are, carried anywhere while roaming. Pagers were a popular device among criminal groups from their introduction until 1980. Criminals have since used mobile phones and pagers to accomplish illicit activities as well as to facilitate everyday operations.

1.2.2 Mobile Phones in E-Commerce

In the current trend, mobile phones have access to the internet and because of this, they are vulnerable to attacks. Mobile phones were actually used for e-commerce after
the innovation of WAP (Wireless Application Protocol). Later advancements in technology in the field of connectivity gave users access to the internet and had the ability to conduct business remotely by accessing websites related to stock trading, flight reservations, hotel room reservations, etc.

1.2.3 Use of Mobile Phones in Storing and Broadcasting Messages

Today’s mobile phones make use of word processors, editors and spreadsheets in order to edit, save and transmit files to another system or mobile device. In mobile forensics, the sources of evidence will consist of mainly,

- The subscriber
- The Mobile station
- The Network

It is believed that there are approximately one billion mobile subscribers worldwide. Of these, the greater number of subscribers is from developed countries like the United States, United Kingdom and Australia [Mobil-Wiki 2008]. It is estimated that each year, mobile phone fraud accounts for about 50 billion dollars. International smugglers have been accused of using mobile phones for illegal activities. A known drug dealer in Columbia, Pablo Escobar [Pablo 2008], has been tracked down using call logs and apprehended by police. The task of dealing with criminals has become easier via the use of mobile forensics used in tracking down their mobile activities.

1.3. Mobile Forensics Background

The most basic things to understand are:

- How is it possible to separate mobile identity from a subscriber?
- How and what types of evidence can be obtained from network units?
- The tools needed to extract evidence either from the network or the equipment without any injustice.

- How evidence is presented.

1.4. Mobile Phone Data as Evidence

According to the Scientific working Group on Digital Evidence (SWGDE), digital evidence is said to be “information of probative value that is stored or transmitted in binary form”. The main sources of evidence are the subscriber, the mobile station and the network [Carrie 2002].

1.4.1 Subscriber:

To identify a subscriber, telephone operators provide a unique SIM (Subscriber Identity Module) to the subscriber which has a unique code embedded in it. The code on a SIM contains the network provider’s name and unique identification number. The SIM card and the unique code can are shown in Figures 1.1 and 1.2.

Figure 1.1 Phase-1 of a SIM [TechSIM 2007]
In Figure 1.2 the SIM card belongs to Telenor Mobile. A SIM card is a removable smart card for mobile phones. They usually store a service-subscriber key (IMSI) which is helpful in finding the GSM (Global System for Mobile Communication) subscriber. The SIM card contains a small processor and volatile memory. The processor is used for securing data as well for granting access to that data. If it becomes necessary to collect data from a SIM card, a SIM card reader and software, like SIM-Manager Pro, SIM-scan, and ChipIt are used. Generally, the data image is taken and hash values are computed to validate the originality of the content [Noblett 1995].

A phone’s serial number, location information file, subscriber identifier, phone number and text message data (SMS) can be retrieved from a SIM card. The biggest threat to SIM card data is perhaps cloning of the SIM card. If a person’s unique SIM code is compromised, a criminal may use that code for performing illegal activities.

1.4.2 Mobile Station

One source of evidence is the mobile equipment itself. These days, due to advancements in technology, a mobile phone is used as a portable computer. It may have access to the internet, make online reservations and could, potentially, store a lot of confidential information. Each mobile system is given a unique identity called
International Mobile Equipment Identity (IMEI). Mobile phone data is stored in flash memories, which exists within the mobile phone. The forensic analyst can collect an image of all the contents when mobile phone data is required to be used as evidence. Much like SIM cloning, as discussed earlier, it is also possible to clone mobile phones. If the International Mobile Equipment Identity (IMEI) is compromised, the case could be much more difficult to solve if the phone has been cloned. Threats to data in the mobile phone can be i) removing the service provider lock (SP-Lock) which restrains a mobile to a single network ii) changing the IMEI on stolen phones which is otherwise called ‘mobile cloning’.

1.4.3 Mobile Network

Another source of evidence can be the service provider’s mobile network. Service providers can provide detailed call logs (message traffic, data transferred, and connection timing/location), which can be one of the most important sources of evidence for a forensic analyst. The network architecture can be seen in the Figure 2.2. The home location register on a network can provide customer name, address, billing account details, telephone number, IMEI, SIM serial number, etc.

Generally, police can determine where a culprit resides in a city with the help of mobile forensics. If any call, message, or data transfer is issued from a culprit to anyone else, Home Location Register (HLR) stores logs of this and could be information useful in locating the perpetrator. In technical terms, this use of data is called “Cell Site Analysis”. Cell Site Analysis can be defined as “the science of being able to pinpoint a specific position, or positions where a mobile phone was or is” [Site Analysis 2008].
The Base Transceiver Station (BTS) is used to transmit and receive data, which is then used to pinpoint the location of the mobile device. It is not possible to determine the exact location, but an approximate location can be revealed. The GSM networks which are 2G+ have an extra node which is helpful in finding a specific location. It uses base station triangulation, and the accuracy may be 0.2 to 10 kilometers. Equipment Identity Register (EIR) stores the identity of a given cell phone. An individual’s location data may be stored in HLR for a random amount of time after the handset is turned off [Site Analysis 2008].
2. NARRATIVE

2.1 Attacks and Crimes with Mobile Phones

According to a journal published by Etter on mobile phone forensics, every person who owns a laptop or a mobile phone or any other handheld device has the ability to commit a crime without any restrictions on mobility or time [Jansen 2004]. The mobile phone of today has become a mandatory or necessary device, largely because of its advanced features. Current mobile phones can be used as a camera, text editor, data storage device, as a music player and plays other roles, as well. Because of the mobile phone’s versatility, it can be used to attack or compete with another computer system.

The ability of mobile phones to run and install java applications is emerging. The java applications enable mobile phones to connect to the internet and give the user to access to websites. Applications running on a mobile phone will have vulnerability to attacks just as any other computer systems. The increase in the complexity of a mobile phone means that it is susceptible to attacks through various software and protocol vulnerabilities. A recent survey conducted by Symantec corporation reports that cases of mobile phones attacked by worms and viruses have increased. The report is mainly about worm SymbOS.CommWarrior.A, which targets mobiles working with a Symbian operating system duplicating itself using Bluetooth and Infrared [Paul 2005].

2.2 Mobile Phone Evidence

Mobile phones have become an important source of information for law enforcement, used to track illicit activities and providing evidence against suspects. The data found in mobile phones has great potential for use in a forensic investigation. The examples listed below show how mobile phones may be involved with a crime scene.
1. The increased appeal of mobile phone use is, in part, due to availability of mass storage within it. Storage capacity can be increased by embedding a memory stick into the mobile memory slots. Because of this feature, it is used as a handy tool for identity theft. For example, a bank employee has opportunity to steal valuable information from customers by uploading the necessary information into his phone.

2. According to a recent investigation by the Australian Institute of Criminology, the trading of heroin, cocaine and other drugs are facilitated largely by mobile phone usage.

3. In late 2004, the mobile subscriber information was stolen from a mobile carrier; a very serious issue. The thief used subscriber information for online shopping as he pleased. This made for a serious situation in South Korea and the mobile carrier was fined a huge sum, resulting in stricter laws. These laws were created in order to keep a subscriber’s information confidential [Paul 2005].

Mobile phones are also now used for online shopping, wherein there is a high potential for fraud. Mobile evidence is becoming more significant. These are the early days of mobile forensics, and possible misunderstanding of this new technology by the authorities, the attorneys and judges may lead to flawed decisions. Therefore, mobile evidence used in these types of cases must be carefully employed. Important characteristics which mobile phone evidence is used for include:

i. Reveal the date and time of a call from a given mobile phone

ii. Find contacts in the address book
iii. Determine phone numbers from which the calls have been received on the mobile phone
iv. Collect any data saved and deleted in the mobile phone memory
v. Find what ring tones are saved and games stored in the mobile device
vi. Know the details of SMS templates
vii. Capture the pictures and videos saved in either the SIM card or flash memory embedded in the phone
viii. Know the sender of the SMS message

2.2.1 Locations of Memory in Mobile Phones

Present research focuses mainly on the how the data is extracted from the mobile phone which it is stored in. Data stored on a mobile phone can be found in different locations within the unit. Locations where the data is stored in a mobile phone may be:

1. The SIM card (if present)
2. The phone device internal memory
3. The phone’s detachable memory (like memory card, SD Card etc. if present)

These locations can be seen in Figure 2.1. Information related to subscriber and calls made and received are also stored by the service provider [Willassen 2005].
Figure 2.1 Showing the SIM card slot in the phone [TechSIM 2007]

**Subscriber Identity Module**

Figure 2.2 shows the architectural diagram of a SIM card. The SIM card consists of a microprocessor which is used to store and recover data. Information concerning identification is stored in the card’s confined memory, which a user cannot access. For storing short messages on the card and to allow for extra features, additional memory is included [Lawrence Harte 2006].
**Figure 2.2 SIM internal architecture [e-Tutorial 2007]**

*Internal Phone Memory*

The internal memory in a phone device has the capability of storing contacts in the address book, calls made and received from another phone, short messages and phone
details. Most of the previous generation mobile phones had considerably less memory than today’s phones.

**Embedded Phone Memory**

Embedded phone memory is nothing more than memory which is connected externally to the device. The shape of a micro SD card is shown in Figure 2.3. The external memory devices vary according to the phone device. For example, Sony Ericsson mobile phones use the Memory Stick Pro Duo for their devices and Blackberry devices use the Memory Stick Micro M2. While they vary in architectural structure, apart from that architecture, these two memory sticks have similar features.

![Fig.2.3 External Memory Sticks for Mobile Phone [Micro 2007]](image)

**2.3 Techniques for Data Acquisition**

Since evidence is very important, forensic analysts should be certain that all information acquired is proper and accurate. To that purpose, imaging techniques are used. Until now, it has been commonly heard that bitstream image is a technique which is used for acquiring forensic data from hard drive and media forensics. Bitstream cannot
acquire forensic data from handheld devices like mobile phones and other PDAs. For this, another technique for forensic data acquisition called Active Memory Image (AMI) for extracting data in mobile phones is employed. AMI is similar to a bitstream image, as it is copying allocated and unallocated data. It is also dissimilar in the field, where there is more data available on a device either reserved by the manufacturer or encrypted/locked from access, making it inaccessible to the examiner. Active Memory Image is termed so because the data itself is steadily moving and being reallocated. This movement avoids the verification step of the hash value, assisting the same purpose.

2.4 Evidence Collection

After investigating memory locations in a mobile phone, it is equally important to gather the data carefully and accurately. Evidence collection is a very important step in a forensic investigation because if this is not handled properly, the rest of the forensic procedure is not going to be viable. Good quality tools and techniques are essential for obtaining good forensic evidence.

The fundamental rules for collecting information are relatively simple in terms of handhelds:

1. The forensic investigator should try to procure all necessary information available at the scene. There is a diverse range of devices which can simply blend into an atmosphere. These days, many devices look much like other items such as pens, cosmetic cases, watches, and so on.

2. It is advisable to remember that multiple points of evidence are possible. Mobile phones are often connected to a desktop or laptop for transferring data into them.
Because of this sharing of data, it is advisable to look into all accessories thoroughly.

3. It is important to know if there is a possibility that any biological evidence exists on or in digital evidence. Due to high volume usage of mobile phones, there may be fingerprints or other biological material present on it, which may be helpful as evidence [Jansen 2004].

Following the correct collection principles and applying them to everyone who becomes involved in the process can be very difficult. Most of the time, a digital clue is collected in the field by those who have come to be known as the first responders [Noblett 1995]. The analysis of how data is found and collected will be analyzed in a detailed manner in later sections.

2.5 Major Problems during Extraction of Data from Mobile Phones

The data found on a mobile phone has great potential for use as evidence. There is no tool that can acquire the data from all mobile phones, because of inaccessibility of mobile phones due to their various hardware and software designs. If a specific cable fits to a mobile phone to acquire data, there is no guarantee that the same cable fits any another mobile, because of differing hardware design. Forensic analysts are badly in need of a universal tool which can fit any mobile phone and be able to acquire data from it. An application can be added to an investigator’s toolbox only once it has been developed in such a way that it can acquire information in a forensic manner from any mobile phone [Jansen 2004].

Another problem is that the application forensic analysts need is difficult to develop. The reason behind this is the software used for mobile phones may alter a
mobile phone’s memory while extracting data from it. Altering of information cannot be allowed in a forensic investigation. There are also a few types of mobile software which will not alter memory; they take command from the phone or computer.

Today, different mobile carriers use different technologies, creating a big problem for application developers. The application developed for GSM phones may not work with Code Division Multiple Access (CDMA) phones. It has been stated that it is impossible to build an application which is feasible to extract information from any mobile because of different standards maintained by the manufacturers and the different technologies being used.

The commands of GSM phones, such as GSM AT, ensure that fundamental information can be accessed from any GSM phone. The advantage is that the code to run AT commands need be written only once and can be used for any GSM phone. Most mobile phones do not have all commands in common, but differ from one manufacturer to other. They would need an extended command set for extracting information from each specific model.

In reality, acquiring data from mobile phones is not a major problem. The phone interface used to obtain data from the phone is similar to an airplane’s “black box”. An input command is given and the response is received. If it cannot be determined how the phone interprets the input command then result is not known. The result is an application developed using these methods cannot claim to be able to obtain the data stored in a phone in forensically sound manner. Apart from this, law enforcement agencies require a case to be solved easily and quickly. A software application should be the answer to these issues [Paul 2005].
2.6 Scope of Present Research

The proposed research will concern the analysis and comparison of available freeware and commercial tools normally used by mobile forensic investigators. These tools are related to extraction of data in SIM card, memory stick and embedded phone memory. Tools like Mobile Investigator Tool and Mobiledit Forensic investigate whole mobile phone data information and save this data into a file. They can also investigate information sources which include phonebook, mobile IMEI number, SMS, battery status, model of the mobile, etc.

Summarizing this research, comparison and detailed analysis of each tool will be clearly elucidated. Comparison will be handled with respect to attributes including type of operating systems it is compatible with, features it can detect when scanning a mobile or a SIM, the capability of reading unreadable data present in the memory, etc. These tools are investigated in detail by testing various conditions, for various file formats and in different scenarios.

2.7 Future Concerns in Mobile Forensics

An important issue in computer forensics is to decide whether the mobile phone should be turned off or on while acquiring the data by imaging the disks, thereby accessing information at rest, or turning the machine on and also acquiring volatile information such as the contents of random access memory.

Currently, data from the random access memory is retrieved by using a combination of both hardware and software with much higher integrity, thanks to recent advancements in computer forensics. This helps forensic analysts to analyze whether the
system has been compromised or not. Malicious code is executed in the shell code of a
buffer instead of installing it on the hard disk. Despite all this, Rutkowska published a
journal based on the computer forensics, in which he stated that the acquisition of data
from the hardware may not always be considered reliable data [Rutkowska 2007].
Processors like AMD and a few models in Macintosh, there is a difference found in how
the CPU reads from the memory, unlike when any I/O devices are connected. Because of
this, different data may be presented by the system to the forensic evidence reader device.

The topics discussed above are highly applicable to mobile devices. Almost all
mobile phones have volatile memory space which will be very useful for forensic
evidence. This volatile memory will be lost if the mobile phone is switched off or the
battery is separated from the mobile. A sudden crash in the mobile phone may also result
in loss of volatile data. It is advisable to capture data from the phone when it is
operational or in working mode. Data recovery tools in general should examine existing
protocols developed by a phone’s designer to extract needed information.

2.7.1 Dealing with the Trust Issue

It is important for a forensic investigator to be aware that there can be many
issues which will affect the trustworthiness of evidence obtained. In developed countries
like the United States, there are no specific requirements posed on forensic analysts in
order for them to be allowed to provide proof in court of law. However, any submitted
evidence may certainly be disproved by superior evidence. The result of a forensic
investigation is liable to be contested by the party whose case is depreciated by its result.
Forensic investigators should therefore be careful and well prepared to respond to any
concerns issued, and provided with additional insurance wherever it is possible. Even
many technological issues are not determined; forensic investigators are advised to triangulate all information gathered from the scene. Triangulation here means that any statements based on the information gathered should be confirmed by rechecking and with ample proof. For example, if information is gathered showing SMS being sent from a given mobile at certain time, it should be confirmed by requesting the records from the service provider. The analyst, without this cross-reference, is at risk of losing the case by way of insufficient evidence. Honestly, in the real world, a forensic analyst has nothing to do with the details of a case, only the lead investigators will see whether there is enough proof to support given statements or not. In order to have a better understanding in the case, the forensic analysts should provide information in detail concerning potential issues in any forensic report destined for internal consumption.
3. RESEARCH

3.1 System Requirements

Forensic tools can be implemented in a system which can support UNIX or Microsoft Windows 98, ME, 2000 NT, XP, 2003 versions. System specifications are limited to a minimum of 32MB of RAM, 64MB disk space.

3.2 Analysis and Comparison of Tools

Present research is based on the analysis of mobile phones and all other forensic research is based on many other tools, which are available as free/shareware and commercially in today’s market. Although the processes performed by these tools are similar, results continue to vary when tested with different types of files. By conducting research and testing on these files, results are noted. The research done is based on scenarios explained in Table 3.1.

Table 3.1 Scenario Table

<table>
<thead>
<tr>
<th>Different Scenarios/Attributes for Mobile Phone Forensics</th>
<th>Detail Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Inspection</td>
<td>To determine whether the tool can inspect the entire device or not.</td>
</tr>
<tr>
<td>Data Acquisition</td>
<td>To determine if the tool used can find the data present in the device and is capable of acquiring that data.</td>
</tr>
<tr>
<td>Hashing</td>
<td>This attribute is for determining whether the tool has the option of detecting any</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Internet Applications</td>
<td>The tool should be able to detect whether the device supports any internet applications like e-mail, streaming, online banking, etc.</td>
</tr>
<tr>
<td>Software Detection</td>
<td>Used to tell whether the tool can able to detect any software present in the mobile device or PDA.</td>
</tr>
<tr>
<td>Imaging</td>
<td>To determine whether imaging is done using active imaging or bit by bit imaging</td>
</tr>
<tr>
<td>Deleted Files</td>
<td>To determine whether the tool can able to recognize deleted contact numbers, as well as any audio/video files etc. in the device</td>
</tr>
<tr>
<td>Misnamed Files</td>
<td>To determine if the tool can recognize misnamed files by measuring the header files.</td>
</tr>
<tr>
<td>Overwritten Files</td>
<td>This scenario is to determine whether the tool can recognize a file which has been overwritten by another file.</td>
</tr>
<tr>
<td>Detailed Summary Report</td>
<td>To determine whether the tool can give detailed output after it is run.</td>
</tr>
</tbody>
</table>
Detailed analysis of each tool is achieved with the help of certain conditions and scenarios/attributes which are quite useful in the process of forensic investigation. Different scenarios are discussed in order to reduce difficulty in evaluating the tools. Devices used for investigation are mobile phones and storage devices, such as memory sticks/ memory cards and SIM cards. SIM cards are investigated by inserting them into a SIM card adapter attached to the system as well as by examining the mobile phone.

### 3.3 Elucidation of Scenarios

Each scenario mentioned in Table 3.1 is described in a detailed manner in this section. In present research, comparison between the tools is performed based on these scenarios:

*Device Investigation*

For the device to be thoroughly investigated, the tool is installed on a system compatible to it and then run. It is recommended a technician confirm that the device is turned on before connecting to the system, and it should not be switched off while in the process of investigation. There are many freeware and commercial tools available in the market, including Mobile Inspector, Device Seizure, etc [Paul 2005].

*Data Acquisition*

The device stored is thoroughly investigated using the device investigation tools and data is acquired using data extraction tools. The obtained data may be documents containing text, audio, video, etc.

*Deleted Files*

There are several tools available in the market which can recover deleted files. Initially, recovery tools were only used for extracting files from a computer, but since mobile forensics emerged, recovery tools for mobile phones also appeared. The system
does not actually remove the file from the hard disk when a document is deleted; it just removes the file location from the File Allocation Table (FAT). Recovery tools find these deleted documents from the hard disk and allow access again.

*Hashing*

The hashing function is implemented using many algorithms like MD2, MD4, MD5, SHA, and PANAMA [Hash 2005].

*Internet Applications*

Mobile phones of the present generation have advanced feature; access to the web. Files and cookies may still be present in the temporary folder when some web applications are opened, and a few may be automatically deleted after closing the application. The capability of a tool can be assessed by detecting the deleted files and present files in the cache.

Forensic investigators initially focus on e-mail websites because these sites are an important source for information. The tool collects all the cached mails present in the temporary folder when it is run on a system.

*Imaging*

Usually, the process of imaging can be accomplished in one of two ways. The first involves bit-by-bit imaging (bitstream imaging) and the second concerns active imaging. If a forensic investigation is done on the hard disk, bit-by-bit imaging is generally utilized, and if the forensic investigation is performed on handheld devices, active imaging is used. Active memory image is similar to a bitstream image, as it is copying allocated and unallocated data.

*Misnamed Files*
Misnamed files are created by changing the extensions of another file. For example, if a text file with extension “.doc” is renamed to “.wma” and if media player is used to open the file, it would not open since it has a text header file and not video header file. These activities are generally used in order to prevent unauthorized people from opening the file.

*Detailed Summary Report*

It is advantageous if the tool has an option to summarize the report after completing the experiment. The detailed summary report should including such details as the date of the experiment, time, model number of device, memory present in the device, etc.

**3.4 Procedure for Extracting Data from the Memory**

It was discussed earlier that the data can be extracted from the different locations in the mobile phone. It is concluded that the data may be present in the internal memory of the phone, SIM card, and externally embedded memory stick.

**3.4.2 Extracting the Data from SIM Cards**

Extraction of data from a SIM card can be accomplished in two ways. A smart card reader is one way to obtain this data, another is to directly analyze the contents of the SIM card through other tools available on the market.

It is comparatively cheaper to extract data via a smart card reader and a card reader is easily obtainable. Generally, the SIM card is accessed by giving input commands using programs such as Microsoft Hyper Terminal. There are many free and commercial tools available for accessing information on a SIM card, like SIM Manager and SIMcon [Paul 2005].
Another way to access the SIM card is directly through the mobile phone. Mobile phones, like GSM, have to conform to a certain standard which specifies a command set. The set allows the command to be embedded in it and passes this to the SIM card in the mobile phone. The response is received in a similar fashion. This appears to be analogous to the direct analysis of a SIM card. This method has significance; if all mobile phones support this type of activity, the extraction of data through the SIM will easily minimize difficulties in using different types of tools.

3.5 Research on Freeware, Shareware and Commercial Tools

There are many tools which are available for use in forensic analysis. Choosing a single tool for the particular purpose of use in the field of mobile forensics is no easy task. Using present research each tool is briefly explained. Some of the available tools are tested using mobile phones, SIM cards, and memory sticks.

3.5.1 Research on Mobile Phone Forensic Tools

Mobile phones today have become adept at multi-tasking, just like personal computers. It is believed that there are many differences between mobile phones and personal computers. Basically, personal computers are designed as general purpose systems and cell phones are special purpose appliances which perform a set of predefined tasks [Ayers 2007].

Mobile phone manufacturers tend to rely on assorted proprietary operating systems, unlike personal computers, which employ a standardized approach. Due to the lack of standardization, mobile phone companies manufacture varied toolkits for their devices. The range of operating the devices are varied and narrowed to distinct platforms.
for a manufacture’s product line, type of hardware architecture, or an operating system family.

Forensic acquisition is basically handled in two ways, either by logical acquisition or by physical acquisition. Logical acquisition is managed through bit-by-bit copy of logical storage objects (directories, files, etc.). Physical acquisition is handled using bit-by-bit copy of the entire physical device. The difference between the physical and logical acquisition lies in the distinction between the memory as seen by the process through the operating system facilities, versus the memory as seen in the raw form by the processor and other related hardware components.

Extracting Data from Phone Memory

The data to be extracted can be found in the internal memory or the memory which is externally embedded in the memory slot. The data in the external memory stick can be analyzed and extracted using Encase [Willassen 2005]. Extracting data from the mobile phone memory is complicated. Willassen proposes two forensically sound methods to make it easier:

- Removal of the memory chip and accessing information directly.
- Tapping the motherboard of the mobile phone in order to access the memory chip directly.

An advantage of these methods is they detour the operating system and access the memory directly. Hence, exact memory image can be acquired. These tasks can be accomplished with the help of many available freeware and shareware tools like Mobile Inspector and Mobiledit. Another advantage of these tools is that they are compatible with almost all mobile phones [Mobil 2007].
Extracting Data from Mobile Phones

There is not a single standard maintained by mobile phone manufacturers for connecting the device to a computer. Each company has its own strategy for obtaining data. Few mobile phones use CDMA technology, which does not contain any SIM card in it, few companies use 3G techniques, and still fewer use WCDMA. In this fashion, the list goes on. Since data can be found on the SIM card and other memory locations, there are many techniques to extract data from them.

Willassen, a famous forensic researcher, proposed the following methodology for forensic analysis of the phone:

- The phone should be switched off as soon as possible after it is seized. This prevents further changes from being made in the cell phone because it is connected to the network.
- Find the access codes from the mobile phone service provider or from the user.
- After the mobile phone has been seized, the SIM card should be analyzed thoroughly.
- Analyze the external embedded memory thoroughly.
- Internal phone memory should be investigated [Willassen 2005].

Mobiledit Forensic

Mobiledit Forensic is a commercial tool which is helpful in acquiring information by scanning all memory contents in the mobile phone. Mobiledit Forensic tool is rapidly becoming a standard tool for mobile phone forensics all over the world. This tool is operated by connecting the mobile phone to a computer using a cable or by using
Bluetooth [Mobil 2007]. A sample screenshot for Mobiledit Forensic is as shown in Figure 3.1.

![Screenshot of Mobiledit Forensic](image)

**Figure 3.1** Screenshot taken when Sony Ericsson w810i is accessed via Mobiledit

Some of its features are listed below:

- Analyze phonebook, last dialed numbers, missed calls, received calls, SMS messages, multimedia messages, photos, files, phone details, calendar, notes, tasks etc.
- Supports almost all type of mobile phones.
- Can analyze a SIM card from the mobile phone and also through the SIM card reader.
- Extracts deleted messages from SIM card.
Backup can be explained and reports can be generated at later time. Many current tools do not have this option. In this way, Mobiledit is advantageous and convenient for forensic analysts.

- Forensic reports are automatically generated and can be exported.
- Hexadecimal code can also view through Hex-Dump viewer.
- Can analyze phones through Bluetooth, IrDA or via cable connection.

Present research is performed on the Sony Ericsson w810i, Nokia 1100, and Nokia 3250 mobile phones. Mobiledit software is so flexible that a forensic report can be generated in many languages around the world. The user also has an option to prepare templates accordingly. Templates can be prepared using a Microsoft Excel spreadsheet or Microsoft Word. A template should include all specifications required for analyzing the experiment. Mobiledit Forensic tool will read this template and insert into it all the data gathered from the device. There is no need to import or export stubs from either SIM card or mobile phone. In summary, Mobiledit Forensic allows the user to read data from a phone directly onto a PC. This data can be saved to a file or exported into any supported format.

Because no data can be altered, it is completely concrete and admissible in a court of law. Therefore, this tool is said to be a complete tool which can extract available data from all mobile components such as phone memory, SIM card and memory stick.

Another feature permits contacts in the address book to be exported in .med, .xml, .xls, .dia formats. The associated screenshot can be seen as in Figure 3.2. The address book has been exported in the form of an Excel spreadsheet is shown in Figure 3.3 [Mobil 2007].
Figure 3.2 Screenshot showing the SIM Phonebook
Figure 3.3 Exported address book from Mobiledit when accessing a SIM card from mobile phone

**Mobile Inspector Software**

Mobile Inspector software is another forensic tool which is used to extract data from a mobile phone. One appealing factor is that it can support almost all types of mobile phones in the current market. This software can extract International Mobile Equipment Identity (IMEI) number, SMS, signal quality, battery status, mobile model, etc. from any supported mobile phone. Figure 3.4 illustrates the implementation of Mobile Inspector software.
Figure 3.4 Screenshot displaying the Mobile Inspector tool window [Data 2007]

Some of its features are:

- Free utility tool which shows phone book entries (contact name/phone number) and phone book capacities for SIM card and mobile phone memory, both.
- Provides mobile phonebook numbers and SMS memory status for Symbian OS-based Nokia mobile phones.
- Facilitate the saving of all retrieved information in text format for future use.
- Due to GUI (Graphical User Interface), users with no computer background can also use this forensics utility easily and economically.

This tool is also compatible with all phone models manufactured by Sony Ericsson, Nokia, Motorola, Spice, Samsung, LG, as well as others. This software assures that all information extracted will be handled in a forensically safe manner. Mobile Inspector offers the option of displaying all information extracted and also has the option to produce a detailed forensic report. A forensic report typically consists of detailed cell phone configuration and SIM card information which helps forensic analysts to better understand a case [Data 2007].

### 3.5.2 Hashing Tools

Basically, hashing is converting a string of characters into usually a shorter fixed length value or key that characterizes the original string. This hash value is used as an index in huge databases to retrieve items very quickly. Hashing algorithm is usually termed a hashing function. Hashing algorithms are not only used for faster retrieval, but also used for encrypt and decrypt digital signatures [Hash 2005].

The hash function is used to index the original value or key and then also used to retrieve data at a later time. Therefore, it is said to be a one way operation. There is no need to “reverse engineer” the hash function by analysis the hashing values. Of course, the ideal hash function cannot be derived by analysis in this manner. A good hash function should not produce the same value for two different inputs. If it produces the same value, then it is considered a ‘collision’ [Hash 2005].
A hash function used for retrieval purposes and database storage may not work well for cryptographic or error checking. There are many other algorithms which will be used for cryptography. These other algorithms include MD2, MD4 and MD5 and SHA [Algorithms 2007].

**Hash Calculator**

Hash Calculator is a freeware forensic tool which is handy for forensic investigators in finding the hash value of any file. The Hash Calculator is a tool which can be useful in locating HMACs for files, hex strings, and the text. The major advantage of using this tool is it offers the option to calculate and support 12 different hash and checksum algorithms like MD2, MD4, MD5, SHA-1, SHA-2(256, 384, and 512), RIPEMD-160, PANAMA, TIGER, ADLER32, and CRC32. A user has the option to select different algorithms as shown in Figure 3.6.

![Figure 3.5 Screenshot for Hash calculator](image)

Other major features of Hash Calculator are listed as follows:

- Can support custom hash algorithm used in e-donkey and e-mule applications.
- Can support large files, up to 15 GB.
- Supports two modes of calculations Checksum/Hash and HMAC.
- Easy to configure and easy for investigators to handle.
- Supports three types of inputs: Hex string, text, and file.
- Calculates hash/checksum and HMAC for files of any type: music, audio, sound, video, image, icon, text, compression, etc., with the extensions: .mp3, .wav, .avi, .mpg, .midi, .mov, .dvd, .ram, .zip, .rar, .ico, .gif, .pif, .pic, .tif, .tiff, .txt, .doc, .pdf, .wps, .dat, .dll, .hex, .bin, .iso, .cpp, .dss, .par, .pps, .cue, .ram, .md5, .sfv, etc. [SlavaSoft 2007].

The testing part and other documentation relating to this tool are given in next chapter.

![Figure 3.6 Screenshot for Hashing Calculator to calculate hash for the options specified](image)

**JSummer**

JSummer is another forensic hash calculating tool. It helps compute and check the MD5, SHA-150, SHA-256 message digest. Since it is a java file, no installation of software is required in the system. If a user wants the tool to install in the windows, there is another option for installing it in the system. JSummer is illustrated as shown in Figure 3.7.
Figure 3.7 Screenshot for JSummer which calculates hash value using MD5, SHA-160, SHA-256

If installed on a system, JSummer should be opened from program files and then browsed to locate the appropriate folder. The shortcuts saved on the desktop may not always work for this tool. It is recommendable to open from program files present in the operating system installed hard drive. Although it is a useful tool, JSummer calculates an accurate hash value only for large files. Consideration of the file size before calculating the hash value is recommended.

**MD5 GUI**

MD5 GUI is a hashing tool which can evaluate MD5 for any file. Since the tool is developed in easy readable Graphical Interface, GUI (Graphical User Interface) is named after it. A basic screenshot is shown in the Figure 3.8. MD5 can be installed in a system
containing Windows NT/95/98, XP Home. This tool is also compatible with UNIX and its equivalent.

![MD5 GUI window](image)

**Figure 3.8** Screenshot displaying MD5 GUI window

This displays 32 hexadecimal digit MD5 hash checksum. Actually, it calculates 128 bit (16-byte) MD5 hashes, but for user convenience it is converted into hexadecimal digit and displayed in the window [Algorithms 2007].

**MUSASH**

MUSASH provides a utility to digest text, file, and a byte char. It is a freeware open tool. A big advantage of MUSASH is it has the option to compare two files and compare their checksum. The MUSASH tool is illustrated in Figure 3.9.

Some of its important features are listed below:

- Allows user to search for a string that evaluates the given hash value
- Allow a digest of not only text input but also file and a byte char
- Can compare two files; a file and text and char to a hash. [MUSASH 2007]

![Figure 3.9 Screenshot for MUSASH](image)

- Supports the MD5, SHA-1, SHA-2 family
- Written in c#, so if there is any error, it is easy to debug
- Compatible with almost all version of Windows (NT, 95, 98, XP) and Linux
- User friendly Graphical Interface
- Freeware open forensic tool

**Fsum Frontend**

Fsum Frontend is a freeware forensic tool for calculating hash values, generating, and verifying checksums. It is said to be excellent tool compared to all other tools explained earlier in the section. Some believe this to be the best because it has all the
features a hashing tool should contain. A significant feature of the tool is its ability to support 96 hash algorithms [FSum 2008]. Figure 3.10 illustrates the implementation of FSum Frontend tool.

![Screenshot for Fsum Frontend window](image)

**Figure 3.10 Screenshot for Fsum Frontend window**

**Features of Fsum Frontend:**

- Free, easy-to-use, and allows computing message digests checksums and HMACs for files and text strings
- Creates checksum of a file
- Supports drag and drop to facilitate easy handling of multiple files
- Used to check integrity of files using checksum generated
- Verify files using SFV/MD5/SHA1/SHA2 algorithms and notify the user if a file is corrupted or missing
- Supports 96 algorithms: lder8, adler16, adler32, ap hash, bdkr, cksum, cksum mpeg2, crc8, crc16, crc16 ccitt, crc16 ibm, crc16 x25, crc16 xmodem, crc16
zmodem, crc24, crc32, crc32 bzip2, crc32 jamcrc, crc32 mpeg2, crc64, crc64 ecma, djb hash, dha256, edonley/emule, elf32, fletcher8, fletcher16, fletcher32, fnv0-32, fnv0-64, fnv1-32, fnv1-64, fnv1a-32, fnv1a-64, fork256, ghash3, ghash5, gost, has160, haval (128, 160, 192, 224, 256 bits) (3, 4, 5 passes), jhash, js hash, md2, md4, md5, panama, pjw32, ripemd128, ripemd160, ripemd256, ripemd320, rs hash, sdbm, sha0, sha1, sha224, sha256, sha384, sha512, size64, snefru2 (128, 256 bits) (4, 8 passes), sum8, sum16, sum24, sum32, sum64, sumbsd, sumsyv, tiger128, tiger160, tiger192, tiger2, tiger tree, tiger tree 2, whirlpool0, whirlpool1, whirlpool2, xor8, and xum32

3.5.3 Research on Miscellaneous Tools

Forensic IM Extractor

Forensic IM extractor is a tool which is very useful for forensic analysts. This tool will extract any instant messages from a given user, both those being sent and received. This tool can extract messages from Yahoo Messenger, Mirabilis ICQ (99a-2003a), Mirabilis ICQ 2003b, Mirabilis ICQ 4/ICQ 5, Miranda IM, &RQ, and Microsoft Messenger (MSN).

This tool offers the option of extracting files using IDX (Internet Data Exchange) file, from which we can see the history of messages sent and received to a profile when logged into ICQ. Another good reason for using this tool for forensic purpose is it has an option to view deleted messages when extraction is done based on .DAT files. Belkasoft Forensic IM Extractor will allow extracting the IM history into readable formats such as plain text, XML, and HTML. It is possible to select the time period of interest and generate history for selected contacts.
Figure 3.11 Belkasoft window showing the profiles to select

It is also possible to extract the history in various sessions, i.e. history broken by contacts, and use command line for extraction. One must select the profile before extracting the history as shown in Figure 3.11. Belkasoft supports multi-byte codes like Chinese and other Asian languages. Chat histories can be split by conversation sessions using .xml file included in the package. Testing of this tool is more thoroughly explained in later sections [Belkasoft 2007].

3.5.4 Research on Steganography Tools

Steganography is the art and science of writing hidden messages in a file which no one realizes exist in the file except the sender and intended recipient. In the past few
years, police have found cases of hidden messages inside a picture or in any file and are saved in either mobile phone or SIM cards. Criminals do this because the risk of discovery in finding the files in the SIM cards is greatly reduced. This reduced risk is due to the lack of advanced tools which can detect these files in the SIM cards. Researchers have had a good topic on which to conduct research and found some important tools like SIM explorer, SIM scan, etc. Forensic analysts then improved their tools accordingly, but there are also other tools which can help them in determining whether the alleged person is involved in steganography or not [E-Forensics 2003].

**Duplicate Files Finder**

Duplicate Files Finder is a forensic tool which can find duplicate files in the system. This is used as a common sense approach for locating any clue in the system. Generally, when any image is about to be used for steganography purposes, a copy is created and the message is hidden in that image, then sent to the other person either using a mobile phone or a computer. After the task is complete, the user will try to delete the file from the hard drive.

Another reason of having the duplicate files in the system could be an error while performing the steganography task. For example, if there is an error while embedding the message into the image existed in the system, there is a chance of deleting that file, and again the culprit might try to insert the message into a copy of the original image. In that way, two copies are created in the system, one is deleted and another copy remains on the hard disk. So the task of a forensic investigator is to find these types of files and compare the sizes of both files. Thereby, steganography in forensics is revealed [Duplicate 2008]. The folder path must be set for scanning the files as depicted in Figure 3.12.
Figure 3.12 Screenshot for Duplicate File Finder

**DupFinder (DUFF)**

DUFF is an acronym for Duplicate File Finder. It is another forensic tool used for locating duplicate files. The DUFF window appears as shown in Figure 3.13. This tool makes use of the hashing function to determine if there are any duplicate values. Usually, duplicate files will have the same value. This tool is special in that it has the option to compare file types. It can compare file types of mp3, text data, binary name, and file name. The comparison can also be made with the sizes of the files. For example, if a file size is 1 MB and the user wants to search for a duplicate file, the user has the option of setting the file size difference between the two files.
Another feature is search filter, which helps the user to save time in searching files. Each and every task done is saved in the log report and will be generated each session [DUFF 2008].

Testing and other information is discussed later in the testing section.

3.5.5 Research on Recovery Tools

Recovery tools are very important for forensic analysts, namely because if any media device (hard drive, memory stick, floppy, CD/DVD, etc.) is seized from a scene, it usually undergoes process of testing. If a forensic analyst suspects that the required file is deleted from the hard disk, then it should be recovered to help solve the case. These types of tools are required for a forensic analyst and are very significant in the forensic toolkit.
Digital Picture Recovery

Digital picture recovery tool is used for recovering any deleted files either from the hard disk or from memory stick/SD card. This tool has excellent features in the recovering of picture files.

Figure 3.14 Screenshot for Digital Picture Recovery Tool

Usually this tool support the file formats listed below:

- GIF
- JPEG
- MP
- TIFF
- CRW
- WAV
- CR2
- MOD
- ORF

**F-Recovery for Memory Card**

This tool is used to recover files deleted from the memory card. An advantage of F-Recovery is that it can recover files easily, quickly and reliably in reconstructing lost data. This tool is being studied as a part of research, details and results of testing this tool are explained in next section. The screenshot for F-Recovery tool is as shown in Figure 3.15 [F-Recovery 2006].

![Figure 3.15 Screenshot displaying the recovery tool window](image-url)
Undelete SD Card

Undelete tool is used for recovering files from the hard disk as well as from memory cards like SD card, mini SD card, etc. The advantage of this tool is its ability to recover files even the disk has been formatted. The screenshot of the tool is as shown in Figure 3.16. The tool is being researched and tested, the results of testing scenarios are explained in the testing section.

![Undelete SD Card tool window](image)

Figure 3.16 Screenshot for Undelete SD Card tool window

3.6 Research on Commercial Tools – Encase

Encase is the industry standard in computer forensic investigation technology. Encase provides all the features expected by law enforcement official within a single tool and is capable of conducting large-scale and complex investigations from beginning to end with
an intuitive graphical user interface and powerful scripting engine. Law enforcement officials, government/corporate investigators and consultants around the world, benefit from the power of Encase in that it exceeds any other forensic solution. Encase can be investigated and analyzed in multiple platforms, such Windows, Linux, AIX, Solaris, etc. It also has the ability to support palm devices and can support its operating system. Encase contains a powerful search engine which utilizes various technologies like proximity search and internet/email search. This powerful search engine can locate information anywhere on physical or logical media. Some of its features are as follows:

- Supports multiple operating systems
- Powerful analytical functionality
- Can view deleted files and other unallocated data in context
- Analyzes and acquires mounted encrypted volumes and gives law enforcement officials full access to data on encrypted hard drives
- Due to the presence of active directory information extractor, it helps Encase to analyze forensically the active directory database (NTFS.dit) and extracts the username, home address directory, last login and last failed login
- Automatically rebuilds the structure of formatted NTFS and FAT volumes
- Encase can automatically create hash values for all the files used in a case [Encase 2006]

Encase is studied by using different type of memory cards, which include micro SD card, mini SD, etc. and results are explained in next section. The screenshot of encase window is shown in Figure 3.17.
Research is performed to study the Encase tool on various memory cards like Mini SD card, Micro SD card, etc. Various scenarios are listed in the table and given below:

**Table 3.2 Encase Scenario Table**

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Memory Card Acquisition</strong></td>
<td>To determine if the tool is able to acquire all data from the memory card</td>
</tr>
<tr>
<td><strong>Management of Personal Files</strong></td>
<td>To determine if the tool can extract all personal management files including calendar, email and phonebook</td>
</tr>
<tr>
<td><strong>Flash Video files</strong></td>
<td>To determine if the tool can detect and</td>
</tr>
<tr>
<td><strong>Different Types of Images</strong></td>
<td>Tool is tested to trace and extract different types of images like .png, .jpeg etc.</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Compressed Files</strong></td>
<td>To determine if the tool can extract compressed files like .tar, .zip</td>
</tr>
<tr>
<td><strong>Deleted Files</strong></td>
<td>To determine if the tool can trace and extract deleted files</td>
</tr>
<tr>
<td><strong>Misspelled Names</strong></td>
<td>To determine if the tool can find misspelled files</td>
</tr>
<tr>
<td><strong>Duplicate Files</strong></td>
<td>To determine if the tool can find any duplicate files existed in the memory card</td>
</tr>
<tr>
<td><strong>Hashing</strong></td>
<td>To determine if the tool is capable of calculating the hash values of existing files in the memory card</td>
</tr>
<tr>
<td><strong>Reporting</strong></td>
<td>To determine if the tool can provide a summary report at the end of investigation</td>
</tr>
<tr>
<td><strong>Internet Application files</strong></td>
<td>The tool is tested to see if it can trace logs and files which existed and were deleted in the history</td>
</tr>
</tbody>
</table>
3.7 Research on SIM Card tools

3.7.1 Dekart SIM Explorer

Dekart SIM Explorer is an efficient tool which is designed to view and edit the contents of a 3G USIM (Universal Subscriber Identity Module), CDMA SIM, and GSM SIM cards easily. This forensic tool mainly targets mobile operators, law enforcement officials, content provider, reverse engineers, developers and others who need flexible access to the structure of a SIM card.

Dekart operates in different scanning modes. They are as follows:

- Smart scan: This scan is very fast and can be able to find any standard GSM, USIM or CDMA R–UIM card (Re-Usable Identification Module).

- Full Scan: If this scan is performed, all files which existed in the directory are found, even if they are not defined to standards.

Figure 3.18 Screenshot displaying the SIM card Explorer window
- Manual Search: This is considered a flexible approach; the user can search with the file name or the file which has a specific property like size, record, count, etc.

Dekart SIM Explorer is compatible with all smart card readers, complying with PC/SC specification. The Dekart Explorer is tested as a part of the research and details are given in the next section. The screenshot for the Dekart Explorer window is shown in Figure 3.18 [Dekart 2007].
4. TESTING AND EVALUATION

Testing is a method of revealing error and inconsistency. Testing is the act of subjecting an item to experiment in order to determine how well something works [Princeton 2006]. Testing is done in several phases of the project. A set of testing schemes is used to determine whether the project is working as expected or not. These schemes are discussed later in this section.

4.1 Testing on Mobile Forensic Tools

4.1.1 Mobiledit Forensic

This tool is used to retrieve data from a mobile phone. The devices used in this project were a Sony Ericsson w810i and a Nokia phone. This tool was tested using different scenarios.

Recovery Test

The SMS (Short Message Service) messages were sent to both mobile phones at the same time. After some time a few of them were deleted from mobile phones. The test was performed to determine whether this tool can recover the files from both mobile phones or not.

Memory Stick Test

In the memory stick test, all contacts were loaded; a few media files like video clip, mp3 files, and image files of various formats were saved on the memory stick. The first step revealed whether the tool could detect them or not. A few files in various
Testing of Steganography Files

In this test, a message was encrypted and hidden in an image file. The test is to decide if the message can be located and retrieved from the file.

Results and Observations

- This tool helps a forensic analyst obtain IMEI, Network type, SIM card type, model and version of the mobile phone, etc.
- It also helps to derive call logs and the number of minutes the phone is used from the date of manufacture, battery status, ICCID, SIM card number, etc.

- SIM cards can be thoroughly analyzed by connecting the SIM cards either to a SIM card reader or by way of insertion into a mobile phone. Screenshot is shown in Figure 4.1.

- When tested with SMS recovery test, the tool positively supported for both mobiles used. (Sony Ericsson w810i and Nokia phone)

- The messages deleted were also viewed when the mobile phone was connected to this tool. The messages can even be exported into text file and xml file.

- If there is a memory stick available in the phone, this tool can automatically detect it and all the files stored on the stick can be accessed.

- The deleted files can also be exported to a specific folder.

- In the memory stick test, media files like mp3 and some video files are detected, but all the files cannot be opened with this tool.

- While undergoing the steganography test, two images with same name were saved on the memory stick. The secret message is embedded in one of the images. This image is then deleted. The memory stick is then tested with Mobiledit Forensic tool. The tool can detect the images, including the one which was deleted. Since there was a message embedded in one of the images, the tool displays a difference in file size. The screenshot shown in Figure 4.2 displays this difference. Mobiledit can tell forensic analyst that there may be steganography involved in an image, but it cannot extract the message from the image. For
extracting the data, the forensic analyst should make use of other special steganographic tools.

Figure 4.2 Screenshot showing same file, but with different file sizes
Figure 4.3 Screenshot for Mobiledit accessing phonebook from mobile

4.1.2 Mobile Phone Inspector

Mobile Phone Inspector is another forensic tool which can extract all data from a mobile phone. One advantage of this mobile phone inspection tool is that it can support almost any of today’s phones. A screenshot of the Mobile Phone Inspector is shown in Figure 4.4. The tool was tested using different scenarios given below:

Recovery Test

The SMS messages were sent to both mobile phones at the same time. After some time a few of them were deleted from mobile phones. The test was performed to determine whether this tool can recover the files from both mobile phones or not.
Memory Stick Test

In the memory stick test, all contacts were loaded; a few media files like video clip, mp3 files, and image files of various formats were saved on the memory stick. The first step revealed whether the tool could detect them or not. A few files in various formats were deleted from the memory stick, then examined with this tool to find out if the tool could locate and mention the deleted files in the forensic report.

Results and Observations

- This software presents full detailed information on all mobile phones based on the Symbian operating system.
- This software can support a few models by Nokia, Sony Ericsson, Motorola, Sagem, Spice, etc.
- It provides battery status, mobile manufacturer, mobile number, network type, signal quality, IMEI number and other general information of the selected mobile cell phones.
- In the recovery test, the SMS messages including the sent items, inbox and even deleted messages are also seen through this software. It was observed that not all mobile phones by Nokia or Ericsson are supported.
- The tool did not pass the memory stick test. This tool did not detect any memory stick but it detected the phone memory. The test was completed on the phone memory. After inserting some media files in the phone memory, a few images were deleted. This tool succeeded in detecting the deleted files.
4.2 Testing on Hashing Tools

4.2.1 Hashing Calculator

Hashing calculator is a tool used for finding the hash value of a file. The advantage of this tool is that it can be tested for both text input as well as file input.

Testing Scenario

- Test using the text mode: This test is used to find the accuracy of input text by making small corrections in the input text and applying it to the original text to see if their hash values are same. This test is also known as an accuracy test. Initially, an input string is entered and its hash value is calculated. Later, it is modified slightly by inserting a space or comma at the end of the string, and again
its hash value is noted. Again, the string is modified to the original string by deleting the space or comma inserted at the end of the string. This hash value is noted then and compared to the hash value noted for the original string.

- This tool is tested to determine the various types of hash values it can support.
- Test using the file mode: This test is helpful if there are any duplicate files present in the system. Initially, a file input is given and hash value is noted. The test is to observe whether it can find any other file with same hash value in the system. This test is also called a duplicate files test.

**Observations and Results**

- The advantage of this tool is that there is no need to install in the system. This software has executable jar file which is very easy to open and saves considerable time for law enforcement officials in its use.
- This tool can calculate MD2, MD5, SHA-1, SHA-256, SHA-396, and SHA-512 hash values of input text as selected from the combo box.
- It is observed that it can support larger files, up to 10 GB.
- In the accuracy test, it is observed that the hash value of the string, before modifying, is matched with the hash value of the re-modified string. The screenshots related to this test are shown from the Figures 4.5 to Figure 4.9.
- The duplicate file test is done with the help of checksum. It successfully located the duplicate files existing in the same directory.
- This duplicate file test is very useful for law enforcement officials to analyze if steganography is involved in the files.
- This tool also calculates the HMAC value using a cryptographic hash function in combination with a secret key.
- This tool has an option to print and save the summary of the files tested.

Figure 4.5 Screenshot taken when a string is entered in the text box

Figure 4.6 Screenshot taken after inserting a comma at the end of the input string

Figure 4.7 Screenshot taken after deleting comma at the end of the string
JSummer is forensic tool which helps law enforcement official to calculate the different types of hash values.

**Testing Scenario**

- This tool is tested to determine if it is proficient in checking the hash value of multiple files at the same time.
- This tool is tested to see if it can produce hash values for different file formats and larger files, too.
- This tool is examined to see if it can produce the SHA (Secure Hash Algorithm) value of different bit lengths.
- It is tested to find whether it can summarize the results and export into a spreadsheet.
Observations and Results

- There are many features in this tool. It has options to choose the calculation of hash values using different algorithms.

- In different bit lengths of secure hash algorithms, it supports only SHA-160 and SHA-250.

- It was observed that this tool cannot support files larger than 10GB. It took quite a bit of time to calculate hash value for 10GB file.
This tool successfully calculated the hash value for multiple files at the same time as shown in Figure 4.11.

It calculates the hash values of all files present in the same directory.

Since this tool is a GUI, it can summarize the hash value of the different files calculated and has the option to compare between the different algorithms. This tool can support file formats like .doc, .txt, .avi, etc.

4.2.3 MD5 GUI

MD5 is a hash tool which can calculate the MD5 hash value for any files.

Testing Scenario

This tool is tested to determine if it can calculate any type of hash value other than MD5.
- This tool is tested to see if it can produce the checksum value for the file
- This tool is examined to determine whether it can save the results and summarize, as it is important step for any law enforcement technician involved the investigation.

**Results and Observations**

- This tool has a user-friendly graphic interface so it is very simple to understand for first time users.
- It is not necessary to install the software in the system because the program is written in java code and executed with the help of a jar file.
- Accurate hash value of MD5 can be calculated for different file extensions
- A drawback of the tool is that checksum values are generated only in binary mode [Birtz 2006].
- It can support and calculate only MD5 hash value.
- When generating checksum files, all icons will be green as shown in Figure 4.12. Recursion is not yet supported.
- It has the option to save the summary report in many extensions, which makes it an even more versatile tool.
Figure 4.12 Screenshot displaying the status of checksum values of files

- In the above image, the little green circles indicate that a file checked out correctly.

  The little red flag means that a file did not match its checksum. A little "NOT" sign means that the file could not be opened.

**4.2.3 MUSASH**

MUSASH tool is studied as a part of research for hashing tools and testing is done with the help of the scenarios mentioned below:

**Testing Scenario**

- This tool is tested to reveal the various types of hash values it can support.

- This tool is tested to determine if it is proficient in checking the hash value of multiple files at one time.

- This tool is tested to see if it can produce hash values for different file formats and larger files, too.
- It is tested to observe whether it can summarize the results and export in a spreadsheet.

**Results and Observations**

- MUSASH is a software tool which can calculate the hash values using MD5, SHA-1, SHA-256, SHA-384, and SHA-512 algorithms.
- MUSASH is a utility to digest text, file, and a byte char.

![Figure 4.13 Screenshot for MUSASH calculating the hash values and comparison of files](image)

- The tool is capable to compare in two ways. i) string and a text file, ii) text file and a character.
- Calculation of checksum is also supported and compared to a hash value as shown in Figure 4.13.
- It allows a user to search for a string which evaluates a given hash value.
- One drawback of this tool is that it does not give an option to summarize the results and save to a file.
If two files are loaded as shown in the Figure 4.14, “match” is displayed in the third row when their checksum value is same. The phrase “does not match” is displayed if there is an error in a checksum value [MUSASH 2007].

**Figure 4.14 Screenshot for comparison of files using MUSASH**

### 4.2.4 Fsum Frontend

Fsum Frontend is a hashing tool which the forensic analysts are looking for. To date, it is said to be an aggressive tool for calculating hash values and checking the integrity of files. The screenshot is shown in Figure 4.15, and this tool is studied and tested with the aid of scenarios explained below:

**Testing Scenario:**
- This tool is tested to see if it can calculate the hash values of two or more files simultaneously.
- This tool is tested to determine if it can produce hash values for different file formats.
- This tool is examined to show whether it can save the results and summarize, as it is important step for any law enforcement technician in an investigation.
- It is tested to see if summarized results are exported in the form of a spreadsheet.

**Results and Observation:**

- The tool has the option to calculate hash values for multiple files simultaneously. In addition to calculating hash values for the files, it has the capability to generate hash value for the folder.
- This tool supports finding files related to cryptography. It can calculate HMAC (Hash Message Authentication Code) for files. It calculates the HMAC value using a specific algorithm involving a cryptographic hash function in combination with a secret key.
- The tool can easily support calculating hash value for large files.
- An important feature of this tool is that it can support 96 various algorithms and eases the task for law enforcement technicians when calculating checksum, hash values, etc. within a single tool.
- Checking the integrity of the tool is supported by using checksum values.
- The tool can summarize the results and can be exported in .html, .CSV, and .xls format [Fsum 2008].
4.3 Testing on Miscellaneous Tools:

4.3.1 Forensic IM Extractor

Belkasoft Forensic IM Extractor is a tool for e-crime/forensic professionals which can simplify analyzing instant messenger histories. This tool helps law enforcement technicians to investigate instant messages stored in the system. An advantage of this tool is that no login is required to extract messages. The messages are extracted using .DAT files saved in the installation folder of the messenger. Various testing scenarios are created in order to test the efficiency of the tool [Belkasoft 2007].
Testing Scenario

- The tool is tested to see if it can extract instant messages from various types of chat servers which use different file formats.
- It is evaluated to reveal whether it can extract deleted messages from the chat profile existing in the system.
- The tool is examined to determine if it can filter out messages with proper keywords.
- The tool is also tested to see if there is any exchange of files during conversation and if it can extract them.
- It is tested to determine whether it can extract messages in a remote system.
- The tool is also tested to see if it can generate report in the required readable file format.

Results and Observations

- One advantage of this tool is it requires no password to log in to the account to extract messages.
- Due to its compatibility with different file types, it can extract messages from ICQ, Yahoo Messenger, RQ and Miranda.
- The deep ICQ analysis using different methods (with and without usage of index file) will help the user to extract even deleted and overwritten messages.
- The tool has desirable features, including filtering, which makes the search easy for the user and brings up only the desired messages. Due to this feature, law enforcement technicians can save time by retrieving only required messages from hundreds of messages which may be present in the system.
Belkasoft forensic IM extractor can export messages in to readable format, such as .xml, .html, and plain text, as required by the user.

It is possible to extract the history when broken by contacts.

This tool cannot be operated remotely from another system, whether connected in the network or through internet. It does not have the source code implemented in java script, so it is not possible to operate this tool remotely [Fileforum 2006].

This tool can detect a file transfer during the conversation using log records, but it cannot be imported.

The process of message history extraction is shown in the form of screenshots, which are shown in Figures 4.16 to 4.20.

Figure 4.16 Selection of various messengers existing in the system
Figure 4.17 Selecting one of the profiles from the list

Figure 4.18 Selecting the contacts first to extract the history
Figure 4.19 Screenshot showing the summary of the extracted information
4.4 Testing on Steganography Tools

4.4.1 Duplicate File Finder

Duplicate File Finder is a tool which can find an image of the existing copy. This tool can be used as a steganography tool for the purpose of finding duplicate images. This tool is tested based on scenarios explained below:

Testing Scenario

- Rename Test: This tool is tested by creating a copy of the existing image in the hard drive and renaming it. In this test, the tool should be able to trace the copy of image even after it has been renamed.
Hidden file Test: The tool is tested to see if it can scan the system and trace the file if it is hidden.

Format Test: A copy of the image is renamed and the type of file is changed by changing the extension. The tool is tested to trace the file.

Steganography Test: The data is inserted into a copy of an already existing image through steganography methods. In this test, the tool should be able to trace the copy of image.

Data Extraction Test: The tool is tested to determine whether it can extract any confidential information stored in the images.

Performance Test: This tool is tested on various sizes of files and compared to DUFF tool.

Results and Observations:

The Duplicate File Finder is a very simple, but effective tool which can search duplicate files in one or more selected search paths [Snapfiles 2003].

The searching of files is performed on the basis of file name, size, type of file, etc. as shown in Figure 4.22.

The reason behind the speed of its scan is its multi-threading process.

The tool offers the option of searching files by masks and skips zero length files.

It has good user interface so that a new user can use the tool comfortably.

Rename Test: When performing the rename test, three different images are taken and copies of those are saved in the same hard disk of the system. Copies of images are renamed and the tool is run for the test. The tool successfully found all the three files saved in different locations on the disk.
- Hidden file Test: This test is done making a copy of the image hidden by checking the hidden option in the properties box. The original image is not hidden in the disk. The tool is unable to find the hidden file unless the option is checked to find the hidden values in the properties menu of the Duplicate File Finder toolbox.

- Format Test: The format test is done by changing the file extension of the copy of original file. The test is started, keeping the copy and original file in the same hard disk of the system. The tool could find only very a few files like .mp3 and text files.

- Steganography Test: This test is completed using files with different sizes. The data is entered into a copy of an image through steganography methods. Since the data is entered, the size of the file will be compared to the original. The tool failed to find the file when it was renamed and secret information stored in the file. This tool did find the file if name is same as the original file, even if the size of the file was different. The screenshot related to this test is given in Figure 4.23.

- Performance Test: The performance test is done based on how fast the tool could locate duplicate files when compared to DUFF. The Duplicate File Finder tool was very fast for a small number of duplicate files, whereas DUFF is very fast for finding a larger number of duplicate files. Considering overall performance, Duplicate File Finder tool was slower in searching the duplicates than DUFF.
Figure 4.21 selecting the directory for finding duplicate files
Figure 4.22 Tool searching for duplicate files

Figure 4.23 Tool displaying the duplicate files found in the given directory
4.4.2 Dup Finder (DUFF)

This tool has similar features to Duplicate File Finder tool. Both tools are compared in order to reveal the advantages and disadvantages of each. Both are tested with the same testing scenarios.

Testing Scenario

- Rename Test: This tool is tested by creating a copy of the existing image in the hard drive and renaming it. In this test, the tool should be able to trace the copy of image even after it has been renamed.
- Hidden file Test: The tool is tested to see if it can scan the system and trace the file if it is hidden.
- Format Test: A copy of the image is renamed and the type of file is changed by changing the extension. The tool is tested to trace the file.
- Steganography Test: The data is inserted in to a copy of an already existing image through steganography methods. In this test, the tool should be able to trace the copy of image.
- Data Extraction Test: The tool is tested to determine whether it can extract any confidential information stored in the images.
- Performance Test: This tool is tested on various sizes of files and compared to the Duplicate File Finder tool.

Results and Observations

- Rename test: In this test, a copy of the file was to be tested compared to the original file saved on the same disk. The files on a different disk may also be
compared, providing the different hard disks are included in the search. DUFF successfully located both files present in the disk, and files present in different disks.

- **Hidden file test:** The tool successfully found all hidden duplicate files existing in the system. DUFF not only found the hidden files, but could also find the archived, compressed, and encrypted system files in the system. The screenshot related to hidden file test is depicted in Figure 4.25.

- **File format test:** The tool discovered a file which was changed to a different format. The successful locating of the file was interesting; contrary to our discussion earlier, the search was done based on the name, size, and type of file. Another factor key for searching files is binary search. The tool successfully compares the files with byte-byte comparison of data and is effective in finding the header information of the file. If the header of the duplicate file matches the header of the original, then binary comparison is made; otherwise it is skipped. The screenshot for this test is shown in Figure 4.26.

- **Steganography test:** The tool succeeded in finding the file which had a secret message hidden in it. Success was due to the concept discussed above. Though the size of the file was varied, compared to the original file, the header remained the same. The tool used binary comparison for both header files and then traced the file.

- **Data extraction test:** The tool offers the option to extract the encrypted message from the file. This is limited to a few algorithms. If the encrypted message falls
under one of these few algorithms, the message is easily extracted, otherwise it throws an exception.

- Performance test: The performance test was done based on how fast the tool could locate duplicate files when compared to Duplicate File Finder. The Duplicate File Finder tool was very fast for a small number of duplicate files, and DUFF is very fast at finding a large number of duplicate files. Considering overall performance, DUFF was very quick to find the duplicates compared to Duplicate File Finder tool.

![Figure 4.24 Screenshot displaying DUFF window](image)

Figure 4.24 Screenshot displaying DUFF window
Figure 4.25 DUFF scanning for duplicate files in selected directories
4.5 Testing on Recovery Tools

Various types of recovery tools are analyzed and tested and compared in order to determine the best tool.

4.5.1 Digital Picture Recovery Tool

Testing Scenario

- The tool is implemented using different memory cards (Micro SD card, Mini SD card). Several type of files including images (.jpeg, .bmp, .gif), text (.doc, .txt, .rtf), zip, and .rar files were stored in the memory card using the forensic card writer, and a few of them were deleted in order to test the recovery feature of the tool. Few recovery tools do not support recovering zip, .rar and .tar files, so this tool was tested including those files in order to know its capability.
Results and Observations

- The tool successfully deployed all the content that is been deleted from SD card.
  
The screenshot shown as Figure 4.27 was taken during the experiment.

- The tool was able to recover all the deleted files in the system. The screenshot is shown as in figure 4.27.

- The tool was successful in saving all the recovered files onto another storage media.

- This tool even restored compressed files. Those files include zip, .rar, and .tar.
- The tool also produced a report about both recovered and pre-existing files in the storage device.

- The pictures are recovered and saved in a separate folder named “recovered” in the “my documents” folder as shown in the screenshot below (Figure 4.28).

![Recovered folder screenshot](image.png)

**Figure 4.28 Screenshot displaying the recovered pictures saved in the folder**

- The tool has the option to save the recovered files and the important feature is that the tool can also extract the video files including mpg, avi and wmv. The recovery folder is created in the system which is shown in Figure 4.28.
4.5.2 F-Recovery for Memory Card

Testing Scenario

- The tool is implemented using different memory cards (Micro SD card, Mini SD card). Several type of files including images (.jpeg, .bmp, .gif), text (.doc, .txt, .rtf), ZIP and .rar files were stored in the memory card using the forensic card writer, and a few were deleted in order to test the recovery feature of the tool. Some of the recovery tools do not support recovering zip, rar and tar files. So this tool is tested including those files in order to know its capability.

Results and Observations

- This tool can recover the data which was deleted from the hard disk.
- It can also recover data which was deleted from both the formatted disk and the corrupted disk.
- This tool supports all formats of pictures, videos and sound files.
- This tool when tested produced all type of files including zip, rar and tar files in the process of recovering deleted files.
- The disadvantage of the tool is that it does not provide previews of the recovered files before extracting and hence does not provide the option to choose which file to recover and which not to recover. The screenshot is attached in Figure 4.29.
- The tool did not provide the option to generate a report of all the files recovered.
Figure 4.29 Screenshot taken during the recovery process of images deleted in the memory stick using F-recovery tool

4.5.3 Undelete SD Card

Many times, memory cards will allow rewriting photo and video files and sometimes important files are deleted or lost by mistake. This tool will help to restore the deleted or corrupted image and video files at once.

Testing Scenario

- The tool is implemented using different memory cards (Micro SD card, Mini SD card). Several types of files, including images (.jpeg, .bmp, .gif), text (.doc, .txt, .rtf), zip, and .rar files were stored in the memory card using the forensic card writer, and a few of them were deleted in order to test the recovery feature of the tool. Some of the recovery tools do not support recovering zip, .rar and .tar files. So this tool is tested including those files in order to know its capability.
The tool is examined to see if it can recover the files from a partitioned disk.

The tool is also tested to determine whether or not it can recover the files from a formatted disk.

**Results and Observations**

- The tool was able to recover all formats of image files, including .png, .jpg, .bmp, .gif, etc., as well as video files like .avi, .wmv, .mpg, etc.

- An important feature of this tool is that it can recover the files from even a formatted and corrupted disk. This feature is advantageous for forensic officials since it can extract old data from the disk which may be useful for finding a clue.

- This tool successfully extracted all the zip, .rar and .tar files used to test the tool.

- It can recover photos and movie clips from the source memory card and saves them to the specified destination folder.

- The recovered files are saved in a separate folder named “Delete” for user convenience, as shown in Figure 4.30.
Figure 4.30 Screenshot showing the deleted files which are recovered and saved in the “Deleted” folder

- If the disk is formatted, then the tool can recover the files and save them in the folder “Lost” as shown in Figure 4.31.
Figure 4.31 Screenshot showing the files recovered from the formatted disk are stored in the folder “Lost”

4.6 Testing on SIM card Tools:

4.6.1 Dekart SIM Explorer

Dekart SIM Explorer is a very efficient tool which allows the user to extract and edit the contents very easily. The tool has a very good interface which allows the user to edit raw data and provides more convenient ways to display the information, interpret the file, and display the contents in human readable form.

Testing Scenario

- SIM card explorer was tested to see if it can show up and extract the deleted contacts from the phonebook.
- The tool was tested to see if it can find any steganography files present in the SIM card.
- The tool was tested to determine whether it can extract IMSI (International Mobile Subscriber Identity) and Ki.
- The tool was tested to reveal whether it can make a backup of SIM card.
- It was also tested if it can unblock the SIM card.

**Results and Observations**

- Dekart Explorer is a powerful tool which can more quickly extract the phone book details in human readable form. A large drawback is that it cannot extract deleted data from the SIM card.
- The tool can be used to view any type of file present in the USIM, GSM SIM cards.
- The tool fails to extract the secret data embedded in the files using steganographic methods, but the data can be seen in encrypted form. It is then easy for law enforcement official to trace these types of files and can save it to their hard disk for further analysis.
- IMSI and other information about SIM card can be easily extracted using this tool.
- SIM card access codes like status of PIN (Personal Identification Number) and PUK (Personal Unblocking Key) can be easily managed.
- If the SIM is locked by chance, it can easily be unlocked with this tool. The tool has the ability to unlock the SIM card using various algorithms.
- Backup for a single file as well as whole SIM card is supported.
• Besides viewing and editing, this application has the option to scan the SIM card, which reveals any hidden files and unknown files to the user.

• The user can conduct both live analysis (operate with the card directly) and offline analysis (saving the backup file to the hard disk and processing without using SIM card itself).

• Another excellent feature of this tool is that it can support many languages worldwide.

**Table 4.1 Functionalities of Dekart Explorer [Dekart 2007]**

<table>
<thead>
<tr>
<th>Activity</th>
<th>Operations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Files on the SIM Card</td>
<td>Open Template</td>
<td>Read the directory structure of a SIM card using a template file</td>
</tr>
<tr>
<td></td>
<td>Save Template</td>
<td>Save the directory structure of the SIM to a template file</td>
</tr>
<tr>
<td></td>
<td>Find File</td>
<td>Find File</td>
</tr>
<tr>
<td></td>
<td>View File Binary</td>
<td>View the file in a Hex-editor</td>
</tr>
<tr>
<td></td>
<td>Edit File Binary</td>
<td>Edit the file in a Hex-editor</td>
</tr>
<tr>
<td></td>
<td>Backup File</td>
<td>Backup file</td>
</tr>
<tr>
<td></td>
<td>Restore File</td>
<td>Restore file from a backup</td>
</tr>
<tr>
<td></td>
<td>Invalidate (Deactivate) File</td>
<td>Deactivate file</td>
</tr>
<tr>
<td></td>
<td>Rehabilitate (Activate) File</td>
<td>Activate file</td>
</tr>
<tr>
<td></td>
<td>Increase File (Cyclic)</td>
<td>Increase cyclic file</td>
</tr>
<tr>
<td><strong>Managing records</strong></td>
<td>View Record Binary</td>
<td>View the record in a Hex-editor</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td></td>
<td>Edit Record Binary</td>
<td>Edit the record in a Hex-editor</td>
</tr>
<tr>
<td><strong>Managing SIM card</strong></td>
<td>Security Access Codes</td>
<td>Manage access codes (enter PIN or PUK, enable or disable PIN protection, change PIN, unblock SIM)</td>
</tr>
<tr>
<td></td>
<td>Backup SIM</td>
<td>Backup the data of a SIM card</td>
</tr>
<tr>
<td><strong>Managing SIM Card</strong></td>
<td>Restore SIM</td>
<td>Restore SIM from a backup</td>
</tr>
<tr>
<td></td>
<td>ATR Details</td>
<td>Interprets the card's ATR</td>
</tr>
<tr>
<td></td>
<td>Scan</td>
<td>Scan SIM card</td>
</tr>
<tr>
<td><strong>Smart-card reader related Operations</strong></td>
<td>Refresh Readers List</td>
<td>Refresh the list of smart-card readers</td>
</tr>
<tr>
<td></td>
<td>Reader Attributes</td>
<td>View information about a smart-card reader and the SIM card plugged into it</td>
</tr>
<tr>
<td><strong>Code references</strong></td>
<td>PLMN Coding</td>
<td>Manage the PLMN codes list</td>
</tr>
<tr>
<td></td>
<td>Languages Coding</td>
<td>Manage the languages codes list</td>
</tr>
<tr>
<td></td>
<td>View (File Summary, File)</td>
<td>Enable or disable the display of SIM card's files</td>
</tr>
<tr>
<td>Application settings</td>
<td>Contents)</td>
<td>or their contents</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Customize</td>
<td>Customize SIM Explorer's appearance (interface language, and whether security codes masking is enabled or disabled)</td>
<td></td>
</tr>
<tr>
<td>Viewing information about the Program</td>
<td>About</td>
<td>View information about the program's version, as well as the registration information</td>
</tr>
<tr>
<td>Exit</td>
<td>Exit</td>
<td>Quit the application</td>
</tr>
</tbody>
</table>

4.7 Testing on Commercial Tools-Encase

Encase is a commercial forensic tool which helps investigate and analyze a forensic case from beginning to end. There are many features, including calculating hash values of files and extracting the deleted data from hard drives. Encase is widely used because of its support of multi-language independent operating systems [Encase 2006].

In the present project, the memory cards used for acquisition are MS PRO Duo card, Mini SD card and Micro SD card. Forensic read only and read write card readers are used.

Testing Scenario

Test Scenario 1:

The mobile phone is carefully switched off and the memory card is removed and plugged into the forensic card reader. Encase is used to take an image of the contents and then this image is observed to determine several things related to Encase tool. After the
imaging process is completed, several files, like mp3 and video files, are deleted, and again the memory card is inserted into a forensic read only card reader for imaging. The test is used to determine whether the tool can retrieve the deleted files from the memory card.

**Test Scenario 2:**

This test is focused mainly on detecting and extracting web applications and existing email files. They were loaded in the memory card and the image was taken to note which files existed on the memory card. A few of the files are deleted, then, again an image is taken. This is clearly visualized in the tables below.

**Table 4.3: Encase Testing Scenario Table-I**

<table>
<thead>
<tr>
<th>Process1</th>
<th>Process2</th>
<th>Process3</th>
<th>Loading Images</th>
<th>Loading Mp3s</th>
<th>Loading Videos</th>
<th>Imaging</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wiping</td>
<td>Imaging</td>
<td>Animation</td>
<td>AliciaKeys.mp3</td>
<td>Bartender.mp3</td>
<td>Cyclone.wav</td>
<td>Livin la.avi</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Aquarium</td>
<td></td>
<td></td>
<td>JOJO(flv)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Birds</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Don’t Break</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Harrah’s</td>
<td></td>
<td></td>
<td>ElectroPop</td>
<td>PrettyBoy(swf)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Jelly Fish</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Laptop</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Leica</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lexington Ship</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sunset</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 4.4: Encase Testing Scenario Table-II**

<table>
<thead>
<tr>
<th>Test1</th>
<th>Test 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read-only</td>
<td>R/W (Read-Write)</td>
</tr>
<tr>
<td>Animation</td>
<td>AliciaKeys.mp3</td>
</tr>
<tr>
<td>Aquarium</td>
<td>Bartender.mp3</td>
</tr>
</tbody>
</table>

95
Results and Observations:

The results are tabulated in the order of experiment done.

**Table 4.5: Encase Results Table**

<table>
<thead>
<tr>
<th>Question</th>
<th>Type of Memory Card</th>
<th>Result</th>
<th>Comments if any</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is Encase able to display all</td>
<td>MS Pro Duo</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>the image files that are not</td>
<td>Micro SD</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>been deleted?</td>
<td>Mini SD</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Is Encase able to display all</td>
<td>MS Pro Duo</td>
<td>Yes</td>
<td>Some of the video files cannot be played.</td>
</tr>
<tr>
<td>video files that are not been</td>
<td>Micro SD</td>
<td>No</td>
<td>Only flash video file was recovered exactly after it was deleted as shown in</td>
</tr>
<tr>
<td>deleted?</td>
<td></td>
<td></td>
<td>figure 4.33.</td>
</tr>
<tr>
<td></td>
<td>Mini SD</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Is Encase able to recover all</td>
<td>MS Pro Duo</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Micro SD</td>
<td>No</td>
<td>Few images were shown as corrupted as shown in figure 4.34</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------</td>
<td>--------------------------</td>
<td>-----------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Mini SD</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Is Encase able to recover all</td>
<td>MS Pro Duo</td>
<td>No</td>
<td>One file (flash format) is not recovered</td>
</tr>
<tr>
<td>the deleted videos (Mobile</td>
<td>Micro SD</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>delete option) from the</td>
<td>Mini SD</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>memory card?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is Encase able to recover all</td>
<td>MS Pro Duo</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>the deleted images (Externally</td>
<td>Micro SD</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>using Windows) from the</td>
<td>Mini SD</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>memory card?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is Encase able to recover all</td>
<td>MS Pro Duo</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>the deleted videos (Externally</td>
<td>Micro SD</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>using Windows) from the</td>
<td>Mini SD</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>memory card?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is Encase able to open all the</td>
<td>MS Pro Duo</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>images that have been</td>
<td>Micro SD</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>recovered?</td>
<td>Mini SD</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is Encase able to open all the</td>
<td>MS Pro Duo</td>
<td>No</td>
<td>One file cannot be played properly</td>
</tr>
<tr>
<td>videos that have been</td>
<td>Micro SD</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>recovered?</td>
<td>Mini SD</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Recovered?</td>
<td>Micro SD</td>
<td>Yes</td>
<td>Mini SD</td>
</tr>
<tr>
<td>-----------</td>
<td>----------</td>
<td>-----</td>
<td>---------</td>
</tr>
<tr>
<td>Is Encase able to recover mp3 files from the memory card?</td>
<td>MS Pro Duo</td>
<td>No</td>
<td>Some of the files were overwritten as shown in Figure 4.35</td>
</tr>
<tr>
<td></td>
<td>Micro SD</td>
<td>Yes</td>
<td>Mini SD</td>
</tr>
<tr>
<td>Does Encase show any special characteristics during the experiment?</td>
<td>MS Pro Duo</td>
<td>Yes</td>
<td>One of the JPG images is showed as a non-standard image as shown in Figure 4.32.</td>
</tr>
<tr>
<td></td>
<td>Micro SD</td>
<td>No</td>
<td>Mini SD</td>
</tr>
</tbody>
</table>
Figure 4.32 Screenshot displaying the non-standard image which was deleted
Figure 4.33 Screenshot displaying files which are deleted and ready to recover

Figure 4.34 Screenshot displaying bad signature files
Figure 4.35 Screenshot displaying that Encase tracing the deleted and overwritten file
5. FUTURE CONCERNS IN MOBILE FORENSICS

As a general method followed in a forensic investigation, investigators turn off the system or the computer in which they believe they have evidence, collect the hard disks, and retrieve the data with latest forensic tools. This data is volatile information and could be read only through the operating system and possibly modified by any illicit operators using toolkits and any other tools.

One notable item, there will be volatile information saved on many mobile systems. It must be saved in order to facilitate the investigation. If the mobile is switched off and the embedded memory and battery are removed, and later the battery is returned and power restored, the volatile memory is lost. This is not the case solely with the mobile phone itself, but with any electronic device which has embedded memory in it, as well. These items may be PDAs, GPS, vehicle navigation systems, among others. It is necessary to investigate a tool to resolve this type of issue. The tools should follow existing protocols developed by mobile architects to access information. Although there are many issues which have not yet been solved in the field of mobile forensics, scientists should attempt to triangulate all evidence collected. Triangulation is used to authenticate statements if there are any from the information assembled from the mobile provider. For example, if there is any SMS sent from a mobile, and if the analyst finds any message in the sent box folder, then that message needs to be authenticated by the service provider.

Another threat is mobile phone cloning. The mobile cloning process is accomplished by modifying the ESN (Electronic Serial Number) by placing the computer chip in the target mobile. ESN is normally transferred in the transmission signal along with Mobile Identification Number (MIN) or International Mobile Equipment Identity.
(IMEI) in order to show the cell phone provider that the call is made by the legitimate owner. Modifying MIN and ESN by placing the computer chip in the target phone allows the intruder to clone very easily. Specific modification should be performed on the mobile phones so that it will not accept the computer chip code, and thereby avoid mobile phone cloning.

Anti-cloning technology should be improved so that when a call is made from a mobile phone, a radio fingerprint which is unique to every mobile phone (so that cell phone providers know if there is a cloning attempt) is included, rather than sending both ESN and MIN in the mobile transmission signal [Phone Cloning 2007].
6. CONCLUSION

Present generation mobile phones are used for different purposes than those of earlier times. It can be used as browser, text editor, picture viewer, answer calls, and at the same time it can also be used as data storage device. Considering all the features most mobile phones now possess, there is the option of storing a lot of information within the mobile phone itself. This can be considered advantageous, but it is a two-sided coin; it can also be potentially dangerous. In calling these features a benefit, unwelcome intruders can attack very easily. They can use mobiles for taking pictures, sending confidential videos, and browsing the internet for various activities. For a perpetrator, the flip-side is that forensic officials can trace content using a variety of the tools mentioned in this project, once the mobile phone has been seized. Mobile phones, SIM cards and embedded memory cards are studied and results observed.

The use of mobile phones has steadily increased in recent times. With advanced technology, the mobile is used in multiple ways, including camera, data storage device and surfing the internet. The confidential nature of the information that can be stored on a mobile phone is vital to law enforcement technicians who would present the data as evidence in both civil and criminal cases.
BIBLIOGRAPHY AND REFERENCES


[Duplicate 2008] Information about Duplicate File Finder tool, Available from

Steganography system for secret information retrieval*, School of Information Systems, Curtin University of Technology, Perth, Western Australia March 2003.


(Accessed on Feb. 26, 2008)


(Accessed on May 27, 2008)


(Accessed on Feb. 24, 2008)


(Accessed on May 5, 2008)


[Mobil 2007] *Mobiledit forensic features*, Available from

[Mobil-Wiki 2008] *Information on number of mobile phone subscribers*, Available from


[MUSASH 2007] *Information related to MUSASH tool*, Available from


[Phone Cloning 2007] *Definition of Phone cloning*, Available from


[Rutkowska 2007] Mobile Forensics and Trust Factor, Available from


APPENDIX A: List of Files Used for Testing Encase and Other Tools

1. Text Files

   A. MS-Word Files:
      i) Hash_Files_Types
      ii) Encase_Research_Checklist
      iii) Hashing Calculator
      iv) ChipIt
      v) Forensic IM Extractor_Notes
      vi) MUSASH

   B. Text Files:
      i) List of Tools
      ii) mymobile_IMEI
      iii) Undelete SDcard
      iv) Junk_Text1
      v) Junk_Text11
      vi) Junk_Text2
      vii) Junk_Text21

2. Audio Files

   A. MP3 Files:
      i) AliciaKeys
      ii) Bartender
      iii) Cyclone1
      iv) I_am_Winner
v) Clock
vi) Fergie
vii) Electropop
viii) Florida

B. WAV Files:
i) Cyclone
ii) Jump_Skip
iii) Tajmahal
iv) Commentary

3. Video Files
A. Avi Files:
i) Blue Angels
ii) We_The_People

B. WMV Files:
i) Gud_Luck
ii) Forensics_1
iii) Cyclone

C. Flash Files(.FLV)
i) JOJO
ii) JOJO-1

D. Shock Wave Files(.SWF)
i) Pretty Boy
ii) Dance_High
4. Image Files

A. JPG Files
   i) Jellyfish
   ii) Laptop
   iii) Birds
   iv) Don’t Break
   v) Aquarium

B. BMP Files
   i) Animation
   ii) Toyota

C. GIF Images
   i) Laptop
   ii) World_Map
   iii) Mickey

5. ZIP Files
   i) Hyderabad
   ii) Forensic_Tools
   iii) MUSASH
   iv) SIMspyII
   v) Pduspy

6. RAR Files
   i) Vid_ZIP
   ii) Desk_Folder
7. TAR Files

   i) Fish_Dolphin
   
   ii) Fish_Star
   
   iii) OS_Doc_Folder
APPENDIX B: Abbreviations Used in the Document

2G: 2\textsuperscript{nd} Generation (wireless phone technology)

3G: 3\textsuperscript{rd} Generation (wireless phone technology)

AIX: Advanced Interactive eXecutive

AMI: Active Memory Image

BTS: Base Transceiver Station

CDMA: Code Division Multiple Access

CPU: Central Processing Unit

CRW: Canon Raw format

CSV: Comma-Separated Values

DUFF: Duplicate File Finder

EIR: Equipment Identity Register

FAT: File Allocation Table

GSM: Global System for Mobile communications

GSM AT: GSM Command

GUI: Graphical User Interface

HLR: Home Location Register

HMAC: Hash Message Authentication Code

ICCID: Integrated Circuit Card ID (20 digit serial number for SIM card)

IDX: Internet Data Exchange

IMEI: International Mobile Equipment Identity

IMSI: International Mobile Subscriber Identity

IT: Information Technology
IrDA: Infrared Data Adapter
MD 5: Message Digest Algorithm
MOD: Module format
MP: Media Player format
NTFS: New Technology File System
ORF: Olympus Raw Format
OS: Operating System
PC/SC: specification for Smart Card integration in computing environment
PDA: Personal Digital Assistant
SD: Secure Digital
SHA: Secure Hash Algorithm
SIM: Subscriber Identity Module
SMS: Short Message Service
TIFF: Tagged Image File Format
USIM: Universal Subscriber Identity Module
WCDMA: Wireless Code Division Multiple Access