Department of Computer Science
Vanderbilt University
CS-8395-50
Digital Forensic

SIM Card Forensics

Rupak Mohanty

Contents

1 Introduction

With the rapid evolution of the smartphone industry, mobile device forensics has become essential in cybercrime investigation. Currently, evidence forensically-retrieved from a mobile device is in the form of call logs, contacts, and SMS. A mobile forensic investigator should also be aware of the vast amount of user data and network information that are stored in the mobile SIM card such as ICCID, IMSI, and ADN.

Regardless of its role in crime (direct or indirect), data within a mobile phone remains crucial. A wealth of information is stored on cell phones that includes, but is not limited to, call history, text messages, email messages, web pages, and photos. Mobile phone forensics, the most challenging digital forensics field, should be enriched with SIM card forensics.

Most of the existing research is focused on searching for the following key evidence in a mobile telephone

- ✓ Calls made, including numbers dialed,dates,and times.
- ✓ Calls received, including numbers received, dates, and times.
- ✓ Data stored within address book/phone book.
- ✓ SMS details.
- ✓ Pictures/video clips on the phone or memory card.

Mobile forensic investigators must be familiar with the different types of mobile phones and understand the intricacies of mobile phone forensics. In other words, acquiring and analyzing the data on the device, attached SIM cards, and inclusive memory cards. These procedures are well documented and should be adhered to in the forensics acquisition and analysis of mobile phone. However documented, it is well known that there is currently no one examination facilitation tool (hardware or software) that is universally used or recommended to remove the data from each and every mobile phone [1].

1.1 Objectives

A smartphone might be the key to an entire investigation, thus, an investigator's task in uncovering evidence will be much harder if it is not supported with the necessary knowledge. The motivation for this paper emerged from the fact that SIM card forensics is a new field with minor literature as far as we know. I intend the analysis of our results to contribute to the mobile forensic field with the essential knowledge needed to make informed decisions based on the tools' actual capabilities.

This study aims at performing a comparative analysis of mobile SIM forensic software tools. The Main objective of this research paper is to

- ✓ Exploring the amount of information extracted from SIM cards.
- ✓ Investigating whether the extractable SIM card evidence is tool dependent.
- ✓ Evaluating the various tools available in the market to conduct SIM card forensic and there limitations.

1.2 Assumption

This experiment has conducted on some 3G SIM cards connected to android phone with mostly open source softwares available for SIM card forensic analysis.

2 Background Informations

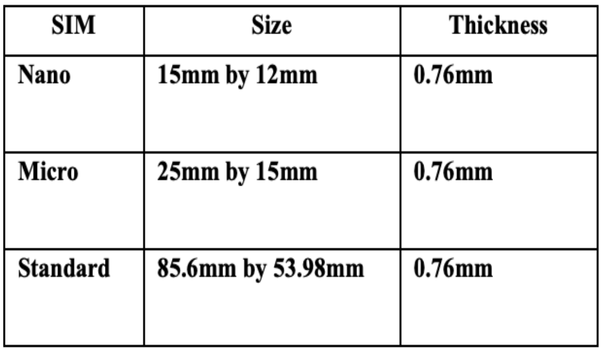
Most modern mobile cellular mobile phones carry a small removable smart card which is called a SIM card. The SIM (Subscriber Identity Module) is a fundamental component of mobile cellular phones that allows a phone user to connect to the GSM telecommunication network, own a cellular number and a subscriber account. It also has a little memory space that can store valuable user information..

2.1 Type and Size Of SIM

A SIM card has a tiny chip containing a file system, a processor and an operating system that runs on top of it to control all the actions and processes undertaking by the SIM card .Most SIM cards have a capacity range from 32 to 128 KB

GSM is abbreviation for Global System for Mobile Communication developed by the European Telecommunication Standards Institute (ETSI). It describes the protocols for 2G, 3G, and 4G digital cellular network for transmitting voice, text and data services. GSM operates in a number of different frequencies usually 900 MHz or 1.8 GHz and in Canada and United States it is 850 MHz or 1.9 GHZ.

CDMA is a short form for Code Division Multiple Access, a digital cellular technology where several transmitters can send information simultaneously over a single communication channel. Size SIM cards are manufactured into three sizes Nano, Micro, and Standard. All details related with SIM specification are given in table 1:



SIM	Size	Thickness
Nano	15mm by 12mm	0.76mm
Micro	25mm by 15mm	0.76mm
Standard	85.6mm by 53.98mm	0.76mm

Table 1: Size of SIM card

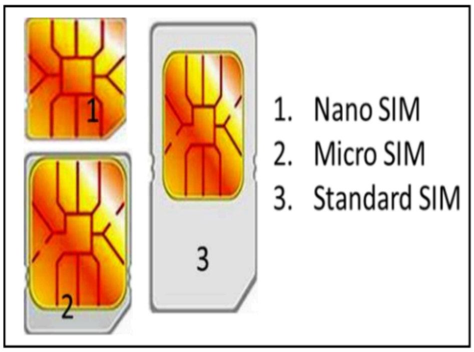
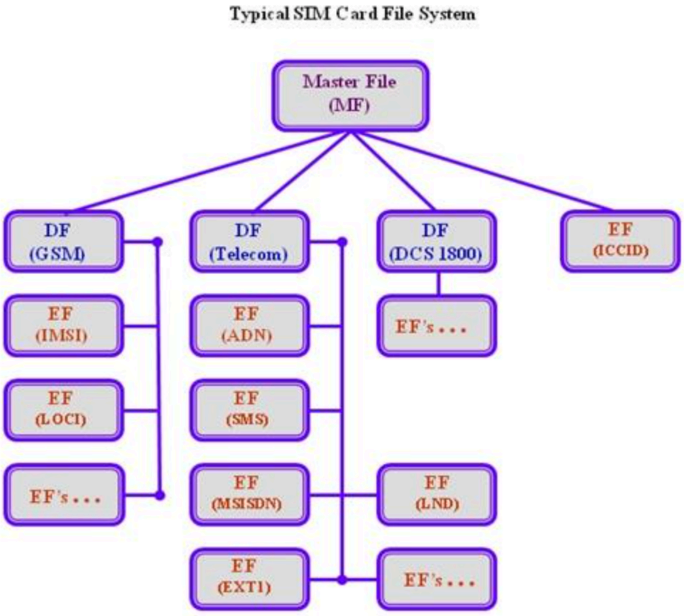


Fig 2: Size of SIM card

2.2 SIM Structure and file systems

A SIM card contains a processor and operating system with between 16 and 256 KB of persistent, electronically erasable, programmable read-only memory (EEPROM). It also contains RAM (random access memory) and ROM (read-only memory). RAM controls the program execution flow and the ROM controls the operating system work flow, user authentication, data encryption algorithm, and other applications. The hierarchically organized file system of a SIM resides in persistent memory and stores data as names and phone number entries, text messages, and network service settings.

The hierarchical file system resides in EEPROM. The file system consists of three types of files: master file(MF), dedicated files,(DF) and elementary files(EF). The master file is the root of the file system. Dedicated files are the subordinate directories of master files. Elementary files contain various types of data, structured as either a sequence of data bytes, a sequence of fixed-size records, or a fixed set of fixed-size records used cyclically.



As can be seen in the above figure, dedicated files are subordinate directories under the MF, their contents and functions being defined by the GSM11.11 standards. Three are usually present: DF (DCS1800), DF (GSM), and DF (Telecom). Also present under the MF are EFs (ICCID). Subordinate to each of the DFs are supporting EFs, which contain the actual data. The EFs under DF (DCS1800) and DF (GSM) contain network-related information and the EFs under DF (Telecom) contain the service-related information.

All the files have headers, but only EFs contain data. The first byte of every header identifies the file type and the header contains the information related to the structure of the files. The body of an EF contains information related to the application. Files can be either administrative- or application-specific and access to stored data is controlled by the operating system.

2.3 Security in SIM

SIM cards have built-in security features. The three file types, MF, DF, and EF, contain the security attributes. These security features filter every execution and allow only those with proper authorization to access the requested functionality. There are different level of access conditions in DF and EF files. They are

Always—This condition allows to access files without any restrictions.

Card holder verification 1 (CHV1)—This condition allows access to files after successful verification of the user's PIN or if PIN verification is disabled.

Card holder verification 2 (CHV2)—This condition allows access to files after successful verification of the user's PIN2 or if the PIN2 verification is disabled.

Administrative (ADM)—The card issuer who provides SIM to the subscriber can access only after prescribed requirements for administrative access are fulfilled.

Never (NEV)—Access of the file over the SIM/ME interface is forbidden.

2.4 Service Related Information's

ICCID: The integrated circuit card identification is a unique numeric identifier for the SIM that can be up to 20 digits long. It consists of an industry identifier prefix (89 for telecommunications), followed by a country code, an issuer identifier number, and an individual account identification number.

IMSI: The international mobile subscriber identity is a unique 15-digit number provided to the subscriber. It has a similar structure to ICCID and consists of the MCC, MNC, and MSIN. An example of interpreting a hypothetical 15-digit IMSI (302 720 123456789) is shown below:

> **MCC**—The first three digits identify the country. "302" refers to Canada.
>
> **MNC**—The next two (European Standard) or three digits (North American Standard) identify the operator. "720" refers to Rogers Communications.

MSISDN: The Mobile Station International Subscriber Directory Number is intended to convey the telephone number assigned to the subscriber for receiving calls on the phone. An example of the MSISDN format is shown below:

- CC can be up to 3 digits.
- NDC usually 2 or 3 digits.
- SN can be up to a maximum 10 digits.

2.5 Phonebook and call information

Abbreviated dialing numbers (ADN)—Any number and name dialed by the subscriber is saved by the ADN EF. The type of number and numbering plan identification is also maintained under this. This function works on the subscriber's commonly dialed numbers. The ADN cannot be changed by the service provider and they can be attributed to the user of the phone. Most SIMs provide 100 slots for ADN entries.

Fixed dialing numbers (FDN)—The FDN EF works similar to the ADN because it involves contact numbers and names. With this function, The user doesn't have to dial numbers; by pressing any number pad of the phone, he can access to the contact number.

Last number dialed (LND)—The LND EF contains the number most recently dialed by the subscriber . The number and name associated with that number is stored in this entry. Depending upon the phone, it is also conceivable that the information may be stored in the handset and not on the SIM. Any numbers that may be present can provide valuable information to an investigator.

2.6 Messaging Information's

Messaging is a communication medium by which text is entered on one cell phone and delivered via the mobile phone network. The short message service contains texts and associated parameters for the message. SMS entries contain other information besides the text itself, such as the time an incoming message was sent, as recorded by the mobile phone network, the sender's phone number, the SMS center address, and the status of the entry. An SMS is limited to either 160 characters (Latin alphabet) or 70 characters (for other alphabets). Longer messages are broken down by the sending phone and reassembled by the receiving phone.

3 Literature Review

The skills of a forensic investigator is useful for the detection and investigation of crime committed on mobile devices, computers and computer networks, the internet and other forms digital devices because such crimes have direct and indirect effects on businesses, government, individual's privacy and corporate organizations functions due to tremendous increased usage of internet and mobile services. Also criminals can take advantage of this large number of potential unsecured targets and ease of access to various offensive tools in order to gain unauthorized access to sensitive information. Therefore we have a need to investigate the ways and processes through which these crimes that are being committed [4]. Forensics based research works by various authors are reviewed for the purpose of this work.

3.1 SIM Data of forensic Interest

The SIM card contains sensitive data about service provider, subscriber. Some of which is listed in table no 2

1	Service Provider Name	2	IMSI (International Mobile Subscriber Identity)	3	ICCID (International Circuit Card Identifier)
4	Mobile Country Code (MCC)	5	Mobile Network Code (MNC)	6	Mobile Subscriber Identification Number (MSIN)
7	Mobile Station International Subscriber Directory Number (MSISDN)	8	Abbreviated Dialing Number (ADN)	9	Last Dialed Number (LDN)
10	Short Message Services (SMS)	11	Language Preference (LP)	12	Card Holder Verification (CHV1 & CHV2)
13	Fixed Dialed Number (FDN)	14	Local Area Identity (LAI)	15	Own Dialing Number
16	Temporary Mobile Subscriber Identity (TMSI)	17	Routing Area Identifier (RAI) Network Code		

Table 2: Data of Forensic Interest

3.2 Methodologies

This paper is aimed at carrying out comparative evaluation of a set of few existing software tools using two 4G enabled GSM mobile SIM cards as a case study. In this chapter all materials, methods, steps and processes undertaking to achieve the project's aim and objectives are listed and explained. Including all software tools used, how mobile evidence data was created, manipulated and sampling techniques used purpose of evaluation. The various tools used are listed with each capabilities as stated by their developers.

Considering the large number of already existing mobile forensic software tools for mobile forensics and the fact that software vendors generally do not follow a common methodology or established standard when developing these tools or their capabilities it was paramount to source tools from various different vendors. From an investigative perspective it is generally required that all evidence be acquired as quickly as possible and to examine the evidence proper so as to ensure that law enforcement professionals can defend their case in a court of law based on the strong probative evidence.

The simple fact is that forensic examiners looking to create the forensically sound image in a quick manner, as anything that forces them to delay the evidence will substantially reduce their chances of producing the evidence in the court of law. [21] Various mobile data and devices are used in order to successfully carry out comparative evaluation of the chosen forensic software set.

The research framework involved in this paper is briefly discussed by the Flow Chart below.

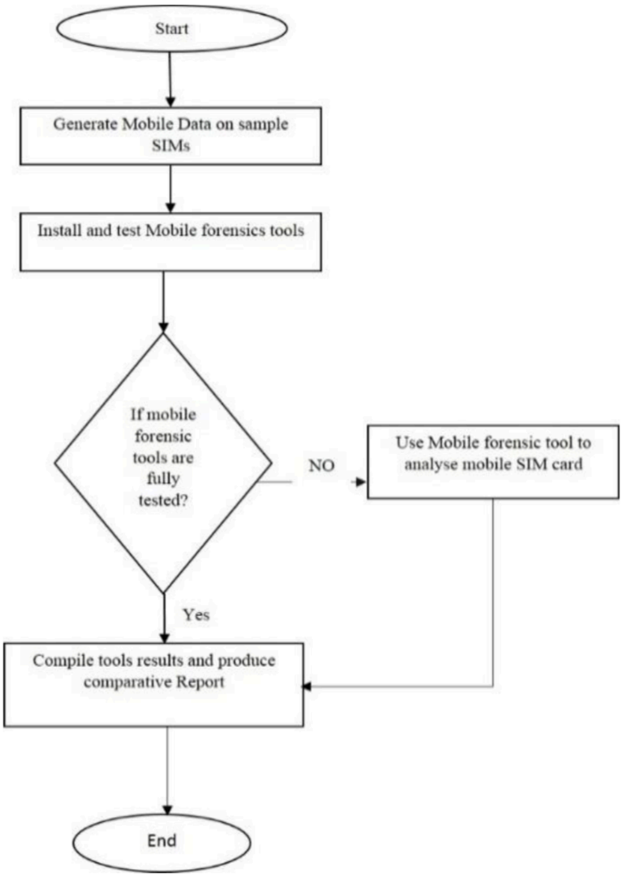

Start
Generate Mobile Data on sample SIMs
Install and test Mobile forensics tools
If mobile forensic tools are fully tested?
NO
Use Mobile forensic tool to analyse mobile SIM card
Yes
Compile tools results and produce comparative Report
End

Figure 1. Flow Chart of the framework

Tools assessment and testing criteria is based on whether these tools support

- ✓ Basic SIM Data recovery
- ✓ Location Information recovery
- ✓ Deleted data recovery
- ✓ Foreign language Data support
- ✓ Examine SIM and produce forensic standard results

4. Data Analysis Procedure

To perform forensic investigation on a SIM card ,it has to be removed from the cell phone and connect to a SIM card reader. The original data of SIM card is preserved by the elimination of write requests to the SIM during its analysis. Then we calculate the HASH value of the data; hashing is used for checking the integrity of the data, that is, whether it has changed or not. There are lots of forensic tools are available but all tools are not able to extract data from every type of cell phone and SIM card.

Data analysis is a process involving either qualitative or quantitative inspection, modelling or transformation of any data sample with an aim of discovering any useful information, suggesting conclusion and supporting good decision making.

Different number of SIM contacts and SMS in form of data evidence was created on both SIM cards with part of these data deleted to analyze the capabilities of each mobile forensic tools whether they could be used in retrieval of both stored and deleted SIM data. These various SIM forensic tools used in this project are listed below, their reviews and features as stated by manufacturers explained.

The below table displays List Of SIM Data generated for sampling

Mobile Evidence Data	Numbers Generated SIM-1	Numbers Generated SIM 2
Saved Contacts	78	67
Saved SMS	25	29
Deleted Contacts	12	15
Deleted SMS	45	32
Applications	22	17
Call Logs	64	75

4.1 Research Instrument

Mobile 4G enabled SIM cards: The two SIM cards have 3G capability and only varying in their individual memory capacity SIM 1 of Vodafone network has 64kb of memory while SIM 2 of the AIRTEL Network has 128kb of memory.

PC/SC Smart SIM card reader: A Dreamscreen USB SIM card reader is used to connect SIM cards directly to the computer system. It comes with a driver software disk which also holds a SIM data management software.

Motorola Android Mobile Phone: The RedMi 9A sport 4.2 Jelly Bean mobile phone was used to create new contacts, SMS messages and make calls with the two SIM cards. The Redmi has capacity for dual SIM support, with a 5.0 inch touch screen, 2.0 Ghz processor, 3G, Bluetooth 3.0 and Wi-Fi connectivity .

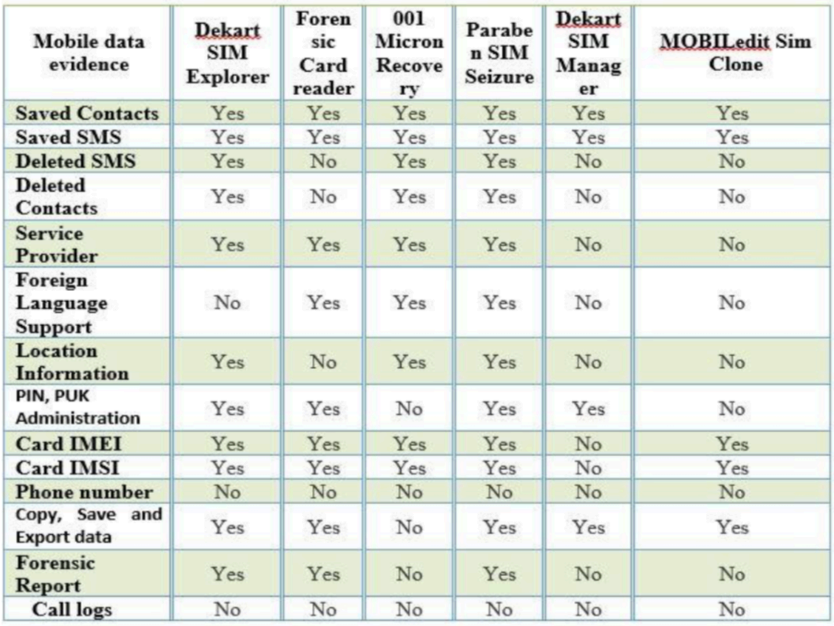
4.2 SIM Forensic Software Tools Used

A set of SIX different mobile forensic tools were used for this paper these include Dekart SIM Explorer version 2.5, Paraben SIM Seizure version 4.04954, MOBILedit SIM clone version 3.1, 001Micon Data recovery SIM Card version 5.4.1.2 and Forensic Card Reader version 2.2 are used in this research. The Paraben SIM seizure and Dekart SIM explorer were obtained by registering with the developers using a secure internet connection, demo version of the softwares were download from the links.

5. Analysis of Results

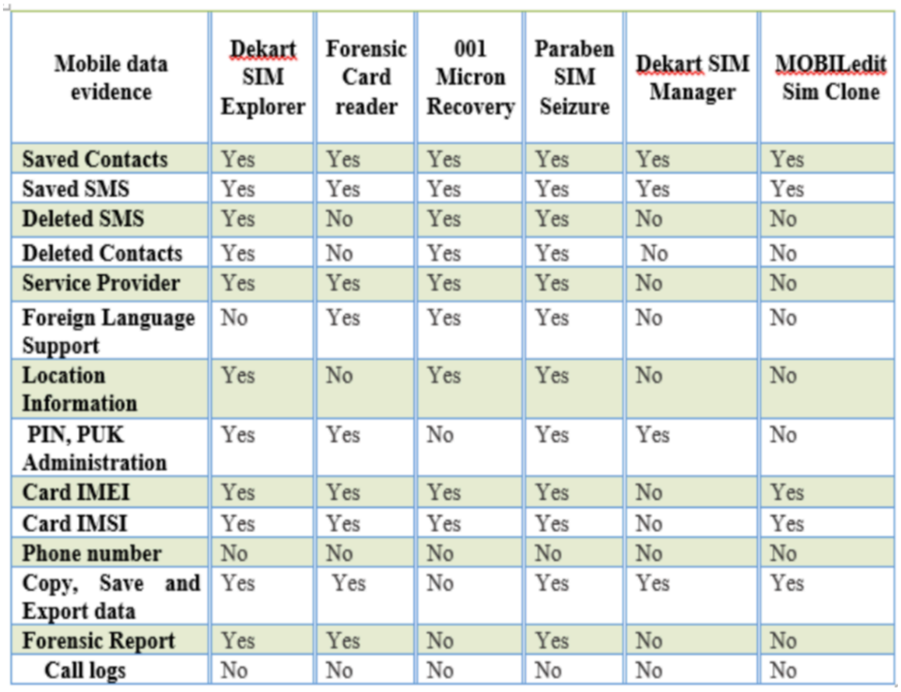
The evaluation of the results produced by all the chosen set of forensics tools when used for mobile evidence collection, against the mobile data evidence that was generated for the sole purpose of this project. For the results analysis two comparative table of results was created although all the tools produced the same results when the same tool is being used to analyze both SIM cards. The results produced by each forensic tool being tested for each specific criteria are analyzed below

Results for SIM-1



Mobile data evidence	Dekart SIM Explorer	Forensic Card reader	001 Micron Recovery	Paraben SIM Seizure	Dekart SIM Manager	MOBILedit Sim Clone
Saved Contacts	Yes	Yes	Yes	Yes	Yes	Yes
Saved SMS	Yes	Yes	Yes	Yes	Yes	Yes
Deleted SMS	Yes	No	Yes	Yes	No	No
Deleted Contacts	Yes	No	Yes	Yes	No	No
Service Provider	Yes	Yes	Yes	Yes	No	No
Foreign Language Support	No	Yes	Yes	Yes	No	No
Location Information	Yes	No	Yes	Yes	No	No
PIN, PUK Administration	Yes	Yes	No	Yes	Yes	No
Card IMEI	Yes	Yes	Yes	Yes	No	Yes
Card IMSI	Yes	Yes	Yes	Yes	No	Yes
Phone number	No	No	No	No	No	No
Copy, Save and Export data	Yes	Yes	No	Yes	Yes	Yes
Forensic Report	Yes	Yes	No	Yes	No	No
Call logs	No	No	No	No	No	No

Results for SIM-1



Mobile data evidence	Dekart SIM Explorer	Forensic Card reader	001 Micron Recovery	Paraben SIM Seizure	Dekart SIM Manager	MOBILedit Sim Clone
Saved Contacts	Yes	Yes	Yes	Yes	Yes	Yes
Saved SMS	Yes	Yes	Yes	Yes	Yes	Yes
Deleted SMS	Yes	No	Yes	Yes	No	No
Deleted Contacts	Yes	No	Yes	Yes	No	No
Service Provider	Yes	Yes	Yes	Yes	No	No
Foreign Language Support	No	Yes	Yes	Yes	No	No
Location Information	Yes	No	Yes	Yes	No	No
PIN, PUK Administration	Yes	Yes	No	Yes	Yes	No
Card IMEI	Yes	Yes	Yes	Yes	No	Yes
Card IMSI	Yes	Yes	Yes	Yes	No	Yes
Phone number	No	No	No	No	No	No
Copy, Save and Export data	Yes	Yes	No	Yes	Yes	Yes
Forensic Report	Yes	Yes	No	Yes	No	No
Call logs	No	No	No	No	No	No

From the analysis results forensic card reader could not recover deleted SMS and contact information but was able to recover basic SIM identification numbers and stored SMS and Contacts, it also has the capability to export such information to a Forensic report format.

While 001Micron Data Recovery was able to recover all basic SIM data including the deleted SMS and Contact details it did not allow the administration of PIN and PUK numbers, although the demo version was not able to save the recovered data evidence or export such as forensic report format.

On the other hand Paraben SIM seizure was able to recover all basic SIM identification data all stored and deleted SMS and Contacts and stored such with a hash value which could be exported in a forensic report format

From the analysis results we see that Dekart Sim Manager was only able to recover stored SMS and Contacts from both SIM cards with very little SIM identification information, although it allowed PIN administration. It was able to store such data in file but could not export such in a forensic report format.

All the tools were unable to recover any call records because they were stored on the mobile phone. From the performance results of these chosen set of forensic tools we see that to some extent Paraben SIM Seizure is one of the best mobile forensic tools to be considered when trying to investigate any case relating to mobile SIM cards with the capability to recover much information and produce a standard forensic report on such investigation. Also Dekart SIM Explorer is an extensively capable forensic tool for use in the forensic analysis of mobile SIM cards.

6. Conclusion

With the constant advancement of technology, the uses, and importance of mobile devices in our everyday way of life cannot be over emphasized. The process of properly and legally acquiring any form of mobile evidence data from any mobile devices or accessories must be carefully undertaken, in all stages of the forensic process. Proper care must be taken in selection of which set of tools to be used because some of these mobile forensic tools developed may not be compatible or well suitable to acquire evidence from a specific mobile phone and its SIM card. Great forensic importance is attached to a mobile SIM card considering it as the heart of a mobile phone and is very easily transferable cross devices. Therefore, the efficiency of any mobile forensic tool should be considered before for acquiring of evidence from any kind of mobile device and accessories.

Having used all the chosen mobile forensic tools and comparing each result with the manufacturer's advertised capabilities, it shows that some tools are limited and cannot be used singly to successfully acquire all the mobile data evidence needed for investigation. Therefore any individual or mobile forensic investigator working to legally acquire data from mobile SIM should read the software descriptions and capabilities by developer before proceeding purchase of that specific software tool for use in forensic acquisition. Considering the fact that some of the forensic tools used in this research were trial and demo versions some of their features could not be utilized, therefore a forensic investigator should ensure that they purchase full versions of these tools when there to be used recovering deleted mobile SIM card data evidence.

7. References

[1] Kyle D. Lute and Richard P. Mislan, "Challenges in Mobile Phone Forensics" International Institute of Informatics and Systemics, p.1, 2008fromwww.iiis.org/cds2008/cd2008sci/citsa2008/paperspdf/i649ok.pdf

[2] Infosec, "Computer Forensics Investigation case study" Retrieved July 20, 2015 from http://resources.infosecinstitute.com/computer- forensics-investigation-case-study/2014.

[3] Joel Lee, "Why do cellphones need a SIM Card". Retrieved Dec. 6, 2013 from http://www.makeuseof.com/tag/why-do-cellphones-need-a- sim-card

[4] D. R. Matthews, "E-Discovery versus Computer Forensics. Information Security Journal": A Global Perspective, vol 19 iss.3, pp. 118-123, 2010.