International Conference on Information and Communication Technology and Its Applications (ICTA 2016)
Federal University of Technology, Minna, Nigeria
November 28 – 30, 2016

SIM Cards Forensic Capability and Evaluation of Extraction Tools

Ismaila Idris[1], John K. Alhassan[2], Victor O. Waziri[3], and Muhammad Umar Majigi[4]
Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria
[1]ismi.idris@futminna.edu.ng, [2]jkalhassan@futminna.edu.ng, [3]victor.waziri@futminna.edu.ng, [4]majigiumar1@gmail.com

***Abstract*—Mobile phones have turned into a very essential tool for personal communication. Thus, it is of immense importance that forensic investigators have possibilities to extract proof items from mobile phones. The Modern mobile phones store facts items on inner memories as well as SIM cards. With the introduction of modern functionality, these accessories and their devices might be used as tools in a crime. Appropriate forensic examination of such memories, including recovery of deleted items has not been possible until now. This research paper presents two mobile SIM cards to assess a chosen set of six existing mobile forensic software tools that where developed mainly for mobile Subscriber Identification Module (SIM) forensics which is aimed to find out their capability and efficiency when compared with other software. This would help a forensic investigator decision making in choosing a tool unique for acquiring specific evidence from a SIM card, and hopefully bring about a save in time and resources.**

Keywords-forensic; mobile phone SIM card; Tecno android phone; software

I. INTRODUCTION

Communication technology is the major integral part of everyday human life. The invention of telecommunication technology, especially smart phones which are one of the most commonly used and dominant technology derived from the advent of Information and Communication Technology (ICT) over the past few decade, have brought about changes and re-defined the world's order and the way most things are done.

Mobile cellular phone usage is seen to have really increased tremendously over the past decade, with an estimated average global mobile subscription of 7.2 Billion in 1st Quarter of the year 2015 and 99 percent Global mobile penetration by 1st Quarter of 2015. Smartphones especially accounted for about 75 percent of all mobile phones that were sold in the 1st Quarter of 2015, compared to around 65 percent during 1st Quarter of 2014 [1]. While the estimated number of smartphones in particular is set to double by year 2020 [2]. Such portable communication devices which are now very advanced with great computing power have taken over the dominant role of personal computers. With a mobile phone, a person can make calls, send SMS messages and also browse the internet and store large amounts of digital data. Mobile phones are now much more popular than personal computers due to portability and can be used in most cases since it has the same content and has capability for the same computing tasks as that of personal computer [3].

In Nigeria for instance, mobile phone usage has continued to increase over the past few years from 0.02 to 67.68 per 100 inhabitants from year 2000 to 2012 [4].

Due to large and ubiquitous role played by mobile phones in our society, there is a great probability that such devices will tend to be part of many investigations as tools or accessories to a crime or other malicious incidents, forensic investigators require specialist tools that would enable the quick, proper retrieval and speedy analysis of any possible data which is present on the device. For devices conforming to the Global System for Mobile Communications (GSM) and related standards, certain data such as dialed numbers, SMS messages and phonebook contacts can also be stored on a Subscriber Identity Module (SIM) [5].

There are at least four major ways whereby a mobile phone or its accessory could be linked to crime:

- A mobile phone could be used as communication tool during the process of committing the crime.
- A mobile phone could contain stored data which is evidence to a crime
- A mobile could contain the victim's or target's information
- A mobile could be the actual means of committing the crime.

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 [6].

The demand for mobile forensics combined with the diversity of the mobile device market has led to a myriad of mobile forensics tools. In 2016, [7] compared existing tools according to their acquisition, examination and reporting functions concluding that typical mobile phone information such as the IMEI and SMS/MMS could be discovered by existing tools such as MOBILedit, SIM seizure, USIMDETECTIVE and Oxygen Phone Manager, etc.

Williamson et al. studied the performance of mobile forensic tools TULP 2G, Cell seizure and Oxygen Phone Manager etc peculiar to Nokia phones [8]. In 2007, Jansen and Ayers again compared existing tools on contemporary mobile phones and collected their work into a NIST report [9]. Later, [10] Yates notes the diversity of the mobile device market and the associated complexity presented to a practitioner attempting to select the appropriate digital forensics tool. Just the comparison papers mentioned here cover: Cell Seizure, GSM.XRY, MOBILedit! Forensic, TULP 2G, Forensic Card Reader, ForensicSIM, SIMCon, SIMIS and Oxygen Phone Manager.

A. The Subscriber Identification Module (SIM)

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. 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 [11]. Most SIM cards have a capacity range from 32 to 128 KB [12].

II. LITERATURE REVIEW

A. Introduction

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 [13]. Forensics based research works by various authors are reviewed for the purpose of this work.

B. SIM Data of Forensic Value

Depending on the type of mobile phone technology and access control scheme, various types of data such as contact list, SMS messages could be stored on the SIM, in the mobile phone, or even on the memory card [14]. A typical SIM card could contain a repository of data and information, some of which are listed below as given by [15]:

- SMS Messages
- Contact Numbers
- Deleted SMS and Contact
- International Mobile Subscriber Identity (IMSI)
- Integrated Circuit Card Identifier (ICCID)
- Abbreviated Dialing Numbers (ADN)
- Service Provider Name (SPN)
- Mobile Network Code (MNC)
- Mobile Subscriber Identification Number (MSIN)
- Abbreviated Dialing Numbers (ADN)
- Mobile Station International Subscriber Directory Number (MSISDN)
- Abbreviated Dialing Numbers (ADN)
- Mobile Country Code (MCC)
- Last Dialed Numbers (LDN)

C. Review of Related Works

This study aims at performing a comparative analysis of mobile SIM forensic software tools. This section reviews eight (8) literatures of related forensics based works. Below are Meta table reviews of literatures of related research background.

TABLE I. META-ANALYSIS TABLE

	ONE	**TWO**
Tittle of Article	Forensic Software Tools for Cell Phone Subscriber Identity Modules	Android Forensic Capability and Android Forensic Capability and
Authors (Date)	Wayne Jansen, Rick Ayers (2006)	VIJITH VIJAYAN (2002)
Focus	Analysis of existing forensic software tools existing for SIMs. To confirm capability to recover basic data, location information and EMS data	Comparative analysis of possible software tools for undertaking Andriod phone forensics
Methodology	GSM SIM, MobileEdit Forensics, Tulp 2G, Cell Seizure, GSM .XRY,SIMCon,SIMIS, Forensic Card Reader	AFLogical, Oxygen Forensic, MobileEdit Forensic, HTC Sensation XE, HTC Desire S
Result	Basic data recovered by most tools, also location information recovered by most tools with challeges of translation of LAI and RAI codes to network name	The test result showed data produced from the evaluation is huge and was quite difficult to table, graphical representation of data was used to ensure readability and easier analysis although of all the tools tested, Oxygen forensic gave a most visible and standardized results.
Limitation	They did not use the latest versions of software tools with enhanced functionalities for undertaking the analysis.	He used two android phones of the same manufacturer HTC.
	THREE	**FOUR**
Tittle of Article	Forensic Analysis of the content of Nokia mobile phones	Smartphone Forensics: A case study with Nokia E5-00 Mobile phone.
Authors (Date)	Williamson, B., Apeldoorn, P. Cheam, B., and McDonald, M. (2006)	Seyedhossein, M., Ali, D., & Hoorange, G. B. (2011) [16]

Focus	Performance evaluation of various mobile forensic software tools on Nokia mobile phone. Analysis of different contents of mobile devices	Comparing some of the mobile forensic tools. Studies demo and trial versions of some mobile forensic tools
Methodology	Cable, TULP2G, Paraben Cell seizure, oxygen forensic manager and, MOBILedit.	Bluetooth device, USB, memory card reader, oxygen forensic suite, paraben's device seizure, MIAT, MOBILedit, forensic lite
Result	No deleted data was recovered by either of the tools.	The toolkit cannot be use to acquire deleted data or information
Limitation	They stated that different handsets will be used in their analysis of which just two handsets were later used. TULP 2G was not used in the analysis after it has been stated in their methodology.	They make use of demo and trial version of software which cannot acquire deleted data. It uses only Nokia E5-00 series and it was not stated if other series where compatible with the toolkit or not
	FIVE	**SIX**
Tittle of article	Overview of potential analysis of an Android Smartphone	Smartphone analysis: A case study
Authors(date)	Stefan, S., Knut, K., & Reiner, C. (2012) [17]	Mubarak, A., & Ali, A. (2013). [18]
Focus	Forensic examination of HTC android smartphone and live analysis of Smartphones. Using android SDK to access internal memory	Investigate an Android phone with WhatsApp installed to check the activities carried out by the user. Compared the result of oxygen forensic tool and UFED physical analyzer
Methodology	USB, PC, Encase, oxygen forensic suite 2011, X-ways and MOBIL edit 5, Android SDK, SQLite data browser 2.0.	IPhone4 Oxygen forensic tool, UFED tool, PC, Wi-Fi connection. Micro SD cards
Result	The forensic tools cannot create a backup image of the internal memory of the Smartphone. Some tools cannot carry out live analysis of internal flash memory. Examination of all the data's was possible	They stated that similar android phone can actually install WhatsApp and user can carry out activities. Oxygen forensic tool is better in data accessing than UFED tool.
Limitation	They did not access external application installed on the phone using this toolkit	Oxygen forensic tool was not able to acquire password and username of the WhatsApp
	SEVEN	**EIGHT**
Tittle of Article	Forensic analysis of social networking application on Mobile devices	Forensic important of SIM Cards as a Digital Evidence
Authors(date)	Al Mutawa, N., Baggili, I., & Marrington, A. (2012). [19]	Ankit Srivastava & Pratik Vatsal (2016). [20]
Focus	Forensic analysis of FaceBook, Twitter and MySpace. Focused on whether the activities carried out on this social network are stored on mobile internal memory and can be retrieved.	Important of SIM Cards forensic as a digital evidence and SIM Cards from technical point of view
Methodology	Blackberry, iPhones and Android phones, Encase V6.5, USB data cable SQLite data browser v1.0.1	Deleted messages can also be recovered from SIM cards, SIM cards that have become unreadable can be read after replacing the EEPROM chip into a new SIM card or by connecting it to proper probes, People should be made aware that SIM cards should not be simply discarded without breaking it into two pieces to make it nearly impossible by a criminal to steal private data easily, scarcely by using a SIM card reader, SIM cards are vital as forensic evidences as it contains location information and a list of all the network towers it has recently connected to call logs of a suspect or a criminal can be of immense value in the proceedings of an investigation, SIM cards contain personal and professional messages such as call logs etc.
Result	In Blackberry no data was found in the internal memory hence nothing can be retrieved. IPhones and Android stores their activities in internal memory and can be retrieved.	Concept of data recovery from SIM Cards.
Limitation	They did not research on other social network application that can be on the stated mobile phones.	The concentrate only on forensic important of SIM Card as a digital evidence

III. METHODOLOGY

This paper is aimed at carrying out comparative evaluation of a set of six existing software tools using two 3G 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 for data recovery by various tools for the

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.

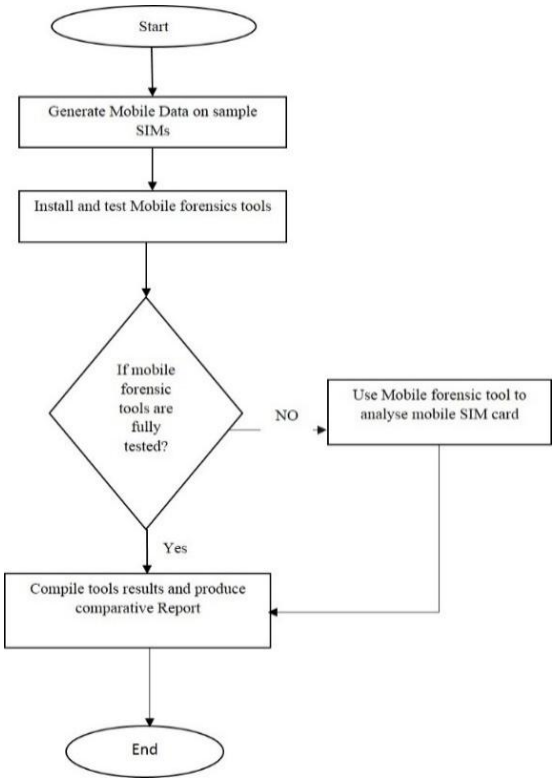

Figure 1. Flow Chart of the framework

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

Each mobile forensic tools method use against the mobile SIM data evidence are equally explained for the purpose of this research. Then the performance results of each mobile forensic analysis report generated by using each tools towards the acquisition of stored and deleted mobile SIM card data are explained. The general comparative performance and efficiency in retrieving such mobile SIM card data evidence is presented tabular against results produced by all the other tools.

A. Data Analysis Procedure

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 SIM data evidence used were created gradually over a period of 2 days. Half the contacts and SMS data were created on each day. While calls were made on the second day. Also half the SIM data evidence created including Contacts and SMS were then manually deleted from the SIM memory gradually one after the other on both SIM cards.

The mobile SIMs are then removed from the Phantom phone and then connected to the laptop via the SIM card reader. After which each software is used to try and recover various data on the both SIM cards.

TABLE II. LIST OF SIM DATA GENERATED FOR SAMPLING

Mobile evidence data	Number generated SIM 1 (64 Kb)	Number generated SIM 2(128 Kb)
Saved Contacts	40	60
Saved SMS	20	30
Deleted Contacts	20	30
Deleted SMS	10	15
Foreign Language SMS (French and Arabic)	4	4
Applications	--	--
Call logs (Dialled, received and missed calls)	20	40

Usually all the forensic tools will prompt you to connect the SIM card reader to the system and choose if to create a case file or directly carry out any data retrieval from a connected SIM card, which would allow for further analysis of the mobile forensic tools based on individual results being produced by each recovery tool.

To ensure that all tools do not change any data on the various SIM cards a write block is implemented for USB port by changing registry setting on the computer. Through /Run/HKEY_LOCAL_MACHINE\SYSTEM\CurrentContol Set\Control (right click and creating a new key

StorageDevicePolicies with a new Dword WriteProtect double click and value set to 1).

Each forensic software tool is used for data acquisition on the two different SIM cards generating twelve different forensic results which are presented in a tabular format showing each tool's capability compared to others.

B. *Research Instruments*

Several tools and software were used in this research work including various sampling mobile data in order to successfully carry out the comparative analysis all these are listed and explained below.

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

Figure 2. Picture of the two SIMs used for this research

*2) PC/SC Smart SIM card reader:*A SIYOTEAM SY-386 PC/SC mobile 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.

3) TECNO Android Mobile Phone: The TECNO Phantom A+ Andriod 4.2 Jelly Bean mobile phone was used to create new contacts, SMS messages and make calls with the two SIM cards. The phantom A+ has capacity for dual SIM support, with a 5.0 inch touch screen, 1.0 Ghz processor, 3G, Bluetooth 3.0 and Wi-Fi connectivity.

4) Forensic Software Tools: The choice of forensic software tools used in this work and all the components necessary to install them and carry out the digital forensic process are listed below:

- 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.
- The software were all installed on an Hp system running Microsoft windows 7 64 bit. Also .NET frameworks was installed to support operations of some of the tools.

Figure 3. SIYOTEAM PC/SC Smart SIM card reader and driver disk

Figure 4. TECNO Andriod phone (Phantom A+)

IV. RESULTS AND DISCUSSION

The results generated by use of each forensic tools are then comparatively evaluated based on the capabilities of each tool for collecting data evidence from the two sample SIM cards.

The SIM data being used for sampling was deliberately generated and partially deleted to test the retrieval capability of the chosen set of forensics tools. All the tools were able to connect to the SIM card reader and were able to access and retrieve at least some stored information from both SIM cards.

The forensic evidence data that these software tools were tested upon was contact phone numbers, SMS messages, and foreign language SMS messages and deleted SMS and Contacts.

A. *Evaluation 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:

TABLE III. RESULT EVALUATION FOR MTN SIM FORENSIC ANALYSIS (64KB)

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

TABLE IV. RESULT EVALUATION FOR ETISALAT SIM FORENSIC ANALYSIS (128KB)

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

The two tables above showed that using Dekart SIM Explorer we can recover basic evidence on both SIM cards and saved such data with a hash value for integrity before exporting in a forensic report format, with the only limitation of not supporting foreign languages such as Arabic SMS.

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.

V. SUMMARY

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. In order to carry out this forensic analysis mobile data evidence was gradually generated on two different memory capacity SIM card of 64kb and 128kb over a period of 2 days and then partially deleted using the same mobile phone. The chosen set of SIM forensic tools were installed on a HP laptop running window 7, 64 bit operating system. Then a Siyoteam PC/SC SIM card reader was used to connect the mobile SIM cards to the computer directly. The mobile SIM forensic tools used are Dekart SIM Explorer, Paraben SIM Seizure, Forensic Card reader V2, 001Micron Data Recovery Sim card, Dekart SIM Manager, MOBILedit SIM Clone. A Tecno Phanto A+ phone was used for data creation on the SIM cards. The result of this research shows Paraben SIM Seizure was able to recover most SIM identification information and stored data, and also produce a forensic standard report. Dekart SIM explorer was able to recover all stored and even deleted data it was also able to produce a forensic standard report. 001Micron was able to recover basic SIM identification but could not administer SIM pins and could not produce a forensic standard report. Forensic card Reader was able to recover basic SIM identification information and stored SMS and contacts but was unable to retrieve any deleted mobile data evidence, MOBILedit SIM clone was able to recover basic SIM identification Information and stored SMS and contacts and save such as a file but could not produce the results in a forensic standard report.

VI. CONCLUSION

All the chosen SIM forensic tools were tested on both SIM cards by extracting the data. The results of these

evaluations shows that it is not easy to retrieve all data especially deleted mobile data evidence from a SIM card by using only one type of mobile forensic tool because the capability of each tool may be developed just for use in acquiring some specific kind of mobile data evidence. Also the limitations of some of the tools in terms of foreign language support and generation of a forensic standard report was gotten The main contribution of this research is to test for the capability of each forensic tool as advertised and to check the compatibility of this specific tool for use in the forensic analysis of either a MTN 65kb Or Etisalat 128kb SIM for retrieval of any stored, deleted mobile data evidence in form of SIM identification and user generated data of SMS and contacts.

Modern mobile phones SIM are now ubiquitous in this world and have progress into full-fledge computing platforms. Thus, they are becoming more crucial as evidentiary devices in criminal and civil investigations. SIM Cards can yield an abundance of information such as saved contacts, call logs and text messages etc. Conversely, no single tool can be used by investigators to retrieve evidence from these devices that it can aid in investigations.

The possible deterrents to a vendor of forensic tools from creating single solution is: the number of hardware manufacturers and carriers the unique data formats used by vendors for storing relevant information and the security mechanisms put in place.

VII. RECOMMENDATION

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.

VIII. SUGGESTION FOR FURTHER WORK

With the wide spread use of social media and their applications on mobile phones, such applications are rich repository for potential forensics evidence data. The Compatibility of existing forensics tools for recovery of these data can be researched.

REFERENCES

[1] Ericsson, "*On the pulse of the networked society*" Ericsson News CenterRetrieved July20, 2015 from http://www.ericsson.com/res/docs/2015/tmd_report_feb_web.pdf. 2015.

[2] Ericsson, "Ericsson Mobility Report" Retieved June, 2015 from www.ericsson.com/res/docs/2015/ericsson-mobility-report-june-2015.pdf

[3] Dan Lohrmann, "Lohrmann on Cybersecurity & Infrastructure" Will a Smartphone Replace Your PC? April 24, 2016. Retrieved from http://www.govtech.com/blogs/lohrmann-on-cybersecurity/will-a-smartphone-replace-your-pc.

[4] O. Osho and S. O. Ohida, "Comparative Evaluation of Mobile Forensic Tools" I.J. Information Technology and Computer Science, 2016, 01, 74-83, doi: 10.5815/ijitcs.2016.01.09

[5] W. Jansen & R. Ayers, "Guidelines on cell phone forensics" *NIST Special Publication, 800,* 101. Retrieved June 30, 2015, from http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf 2007.

[6] Kyle D. Lute and Richard P. Mislan, "Challenges in Mobile Phone Forensics" International Institute of Informatics and Systemics, p.1, 2008from*www.iiis.org/cds2008/cd2008sci/citsa2008/pa**per**spdf/i649ok.pdf*

[7] Timothy V, Chengye Z and Nicolas C, "Towards a General Collection Methodology for Android Devices" pp.1-2 2016

[8] B. Williamson, P. Apeldoorn, B. Cheam, and M. McDonald, "Forensic analysis of the contents of nokia mobile phones" page 36, 2006.

[9] W. Jansen and R. Ayers, "Guidelines on cell phone forensics" NIST Special Publication, 800:101, 2007.

[10] I. Yates, "Practical investigations of digital forensics tools for mobile devices" pages 156–162. ACM, 2010.

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

[12] 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*

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

[14] LGC Forensics, "Mobile handset examination" Retrieved 2010 from http://www.ifblgc.de/sites/default/files/assets/Files/Mobile%20handset%20examination.pdf

[15] He, S., & Paar, I. C. "SIM card security". *Bochum: Ruhr-University*. 2007

[16] Seyedhossein, M., Ali, D., & Hoorange, G. B. "Smartphone Forensics: A Case Study with Nokia E5-00 Mobile Phone" International Journal of Digital Information and Wireless Communications (IJDIWC) 1(3): 651-655, 2011.

[17] Stefan, S., Knut, K., & Reiner, C. "Overview of potential forensic analysis of an Android smartphone" Conference Paper in Proceedings of SPIE - The International Society for Optical Engineering · Retrieved February, 2012 fromhttps://www.researchgate.net/publication/258332974_Overview_of_potential_forensic_analysis_of_an_Android_smartphone doi:10.1117/12.909657

[18] Mubarak A., & Ali A. "Smartphone Forensics Analysis: A Case Study" International Journal of Computer and Electrical Engineering, Vol. 5, No. 6, December 2013

[19] Al Mutawa, N., Baggili, I., & Marrington, A. "Forensic analysis of social networking applications on mobile devices," DigitalInvestigation, vol. 9, pp. S24-S33, 2012.

[20] Srivastava A & Vatsal P "Forensic Importance of SIM Cards as a Digital Evidence". J Forensic Res 7: 322. doi:10.4172/2157-7145.1000322, 2016

[21] Vijith Vijayan, "Android Forensic Capability and Evaluation of Extraction Tool" A thesis submitted in partial fulfillment of the requirement of Edinburgh Napier University for the Degree of Master of Science in Advanced Security & Digital Forensics. April, 2012.