DOI: http://dx.doi.org/10.26483/ijarcs.v9i1.5303

Volume 9, No. 1, January-February 2018

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

CASE STUDY

Available Online at www.ijarcs.info

COMPARATIVE STUDY OF VARIOUS DIGITAL FORENSICS LOGICAL ACQUISITION TOOLS FOR ANDROID SMARTPHONE'S INTERNAL MEMORY: A CASE STUDY OF SAMSUNG GALAXY S5 AND S6

Azimuddin Khan
Senior Manager Systems,
RSMM Limited
Udaipur, India

Zakir Hussain Mansuri
Research Scholar,
Department of Computer Science and IT
JRN Rajasthan Vidyapeeth University Udaipur, India.

Abstract: Due to the rich set of exciting features available in Android smartphones makes it possible to be used vastly by the user around the world and hence android occupies a large share from among other operating system based Smartphone. The popularity of Android smartphones is growing rapidly day by day and it plays a vital role in our daily lives. The feature-rich state of Android smartphones makes it possible to be used in criminal intended activities. The Android smartphones are merely used in criminal activities and hence it can be used as a solid source of digital evidence. A range of Smartphone's forensics tools are available in the market which can be used to recover digital evidence from the Android smartphones.

In this paper, authors have made efforts to highlights the range of Smartphone forensics tools which can be used to perform logical acquisition on the internal memory of android based smartphones and then provide the comparison between Smartphone forensics tools on the basis of their ability to acquire data from the internal memory of Android smartphones. It has been found that there no tool available which can extract the complete range of digital evidence from Android-based smartphones.

Keywords: Digital Forensic, Digital Evidences, Android Forensics, Smart Phones, Logical Acquisition.

1. INTRODUCTION

Android is a fast growing, feature rich and exciting mobile platform and operating system developed by Open Handset Alliance (OHA). The Android operating system was originally designed and created by the Android Inc. but was bought by Google in 2005. The Open Handset Alliance is a group of the carrier, component manufacturer and software vendors. The Open Handset Alliance was formed by Google and the OHA is responsible for continuous development of Android operating systems (1), (2).

Android is an open source Linux based operating system which can be able to download and install the application from android application market, able to store user data on the device, therefore, most of the Android smartphones come with On-Device Storage (using NAND Flash memory). It also includes an integrated browser, 2D, 3D graphics, multimedia, GSM and CDMA connectivity. The Android operating system also includes Bluetooth, WiFi, EDGE, SQLite, Camera, GPS, Compass, Accelerometer, 2G, 3G, and 4G. All these features are common in all android based smartphones (3), (4), (5).

A. Android Operating System Architecture and Components

Android software stack is composed of four-layer with five different components namely Application, Application Framework, Android Runtime, Libraries and Linux Kernel. The lowest layer of Android architecture is Linux 2.6 Kernel and the top layer is application layer. The above components of Android operating system architecture are briefly described in the following subsections (1), (2), (3), (6), (7).

a. Application

The application layer is the top layer and is the most important component of Android operating system architecture. The application layer directly interacts with the user and this layer contains a basic set of Android applications including web browsers, calendars, contacts, clock, Map etc. written in Java programming language. All the applications installed on Android smartphones deals with the application layer. Each and every application installed on an Android smartphone can be found in the application layer (1), (2), (3).

b. Application Framework

This is the second upper layer of Android operating system architecture and is just below to the application layer. The application framework is also a most important component of an Android operating system because it provides Application Programming Interfaces (APIs) used by different running Android applications means Application developer provides services through a set of Application Programming Interfaces (APIs), (1), (2).

The Application Framework component is consists of different subcomponents including Activity Manager, Window Manager, Content Providers, View System, Package Manager, Resource Manager, Location Manager, Notification Manager and Telephony Manager (3).

c. Android Runtime

The Android Runtime is the third important component of Android operating system architecture and is placed in the second bottom layer as well as the Android Runtime has key subcomponents namely Dalvik Virtual Machine and Core Libraries, (1), (2).

The Dalvik Virtual Machine (DVM) is like Java Virtual Machine (JVM) and is designed and optimized for the

Android operating system. The Core Libraries enables the developers to develop Android applications using standard Java language. Combination of both the Dalvik Virtual Machine and the Core Libraries makes an executing or runtime environment in which the android applications are executed (3)**.**

d. Libraries

This component is also placed in the second bottom layer of Android operating system architecture and it includes the key subcomponents namely Surface Manager, Media Framework, SQLite, Open GL/ES, FreeType, WebKit, SGL, SSL, Libc etc. In simple it includes a set of libraries written in C/C++ and these libraries are used by Android operating system components through the Application Framework (1)**,** (2)**,** (3)**.**

e. Linux Kernel

It is the bottom layer and a key component of an Android operating system architecture which contains a list of drivers used to run different android applications as well as associated hardware like Audios, Videos, Camera, WiFi, touch and display drivers. In simple, the Linux Kernel provides a level of abstraction between hardware and software and provides multitasking and low-level system services like power management, process management and memory management (1)**,** (2)**,** (3)**.**

B. Digital Forensic

Digital forensics is a branch of forensic science and is defined as "the use of scientifically derived and proven method towards the presentation, collection, validation, identification, analysis, interpretation, documentation and presentation of electronic evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be disruptive to planned operation" (6)**,** (8)**.**

The term electronic evidence is concerned with the set of information stored or transmitted over the network in digital form and is also known as "Digital Evidence". In simple the digital evidence is information stored or transmitted in digital form. Digital evidence is valid in court as documentary evidence according to the Indian Information Technology Act, 2000 [Indian IT Act, 2000**]** (3)**.**

Mobile device forensics is a branch of digital forensics and deal with the process of extraction of digital evidence from the mobile devices under the forensically sound conditions by using standard, verified and widely accepted mobile forensics tools and techniques. Similarly the android forensics is a sub-branch of mobile device forensics and deal with recovery of digital evidence contained in the Android smartphones under the forensically sound condition by using standard, verified and widely accepted android forensics tools and techniques (3)**,** (6)**,** (8)**,** (9)**,** (10)**,** (11)**.**

Android Smartphone forensics is the rapidly growing and evolving area of digital forensics discipline. A bunch of Android smartphone forensics tools and techniques are available in the market to perform the forensic investigation of Android-based smartphones. Due to the open source nature of Android platform, most of the manufacturer companies developing the feature-rich smartphones based on Android platform and making the smartphone feature rich. The rapid evolution and amendment of an advanced technological feature in Android smartphones possibly make the Android smartphone hard to be forensically investigated. The rich set of features available in the Android smartphone makes it possible to be used in criminal intended activities and this involvement makes the Android smartphone a powerful source of digital evidence and will further be investigated to retrieve digital evidence (12)**.**

According to the expert's perspective, the Android smartphones can contain a huge amount of data which can be counted as evidence at some places. To recover containing digital data, various Android smartphone forensic tools and techniques are available in the market. Some of the android forensics tools are commercial in nature and rests of them are open source. Similarly some of the Android smartphone forensic tools are individual stand-alone software solution whereas some are bundle of hardware and software solutions (toolkits) means these are comes in separate, preconfigured and preinstalled PC or tablet along with group of supporting small forensic software solution (like bypassing software tools, analyzing tools, reporting tools, viewers etc.) and hardware peripherals (like cable set, cloning card, flash drives, card readers, power supplies tool, chargers etc.).

In this paper, authors have highlighted a range of smartphone forensics tools and to perform comparison between them on the basis of the ability to acquire digital evidence resides in the internal memory of Android smartphones and measure performance of each and every smartphone forensics tools to be used for logical acquisition of internal memory of an Android smartphone. The measurement of comparison and performance will be based on a range of predefined and specified data elements resides in the internal memory of Android smartphones.

The mobile device forensics process is broken into four main categories namely "Seizure", "Acquisition", "Analysis/Examination" and "Reporting" (10)**.**

C. Acquisition Phase

The Acquisition is the process of creating or acquiring a duplicate copy of data resides in mobile devices. This process deals with the extraction of digital evidence or digital data from the mobile devices. The acquisition phase of mobile device forensics is broadly divided into the following sub-categories (9)**.**

Software-based acquisition
Physical Acquisition
Logical Acquisition
Hardware-Based Acquisition
JTAG (The Joint Test Action Group) Acquisition
Chip Off Acquisition
Other types of acquisition
Manual Acquisition
File System Acquisition
Bruit Force Acquisition

D. Logical Acquisition

Bit for bit copying of data from the logical storage of Android smartphones is known as the logical acquisition of Android smartphones. Logical storage (refers to the Directories and Files) is resides in the logical partition (refers to the File System Partition/Logical Drives) of the mobile devices. Deleted data can't be extracted using logical acquisition. The Logical acquisition is much easier for an investigator as well as for tool to extract data resides in the devices because the direct interaction is being done with the system data structure of the device during the logical acquisition (9)**.**

Almost all android smartphone forensic tools are able to perform logical acquisition as this is a fast, easy, reliable and secure process of extraction of data from the Android smartphones. The logical acquisition has enough strength to recover all potential data from the devices and acquisition is not possible if the device is broken beyond repair. Logical acquisition can be done by following four ways:

The first and the most way is partition imaging.

The second way is concerned with copying files and folders.

The third way is concerned with content providers

The fourth way is recovery mode.

E. Common Potential Data Available on Android Smartphones

The internal memory of android based smartphones contains common types of information which can be considered as digital evidence on android smartphone forensics perspective. Each and every Android smartphone forensics tools must acquire data contained in the internal memory of Android smartphones from among the common set of data or information partially or fully during the logical acquisition process. Here we have a range of a common set of data or information which can be contained in all kinds of Android-based smartphones with the variation in make, model, and manufacturer (9)**,** (10)**,** (11)**.**

Personal Information Management (PIM) – Contacts (with details like address, picture etc.) Calendar Entries, To-Do Tasks Entries, Notes, Memos etc.

Messages – SMS (Send, Received, Deleted), MMS (Send, Received, Deleted Image, Audios, and Videos), EMS (Send and Received), Voice Messages

Call Logs – Incoming, Outgoing, Missed calls

Emails – with attachments and Email contacts

Stand-Alone Files – Audio Files, Video Files, Images

Social Networking Application Data– Facebook, Twitter, Instagram, LinkedIn etc.

Instant Messaging Application Data– Whatsapp, Viber, Facebook Messenger etc.

Application Files– Word, Excel, PowerPoint, Text, PDF etc.

Browser Data– Bookmarks, Web Histories etc.

Location Data – Graphical Positioning System Co-ordinates (Longitude and Latitude) associated with different android applications which are live (3)**,** (13)**.**

2. REVIEW OF LITERATURE

Technological changes are made on daily basis in the development field smartphone especially in Android smartphones and that makes the smartphones more complex to be forensically investigated if they found in a criminal intended activities. Many Researchers, Forensic experts, and law enforcement personnel are working recently in the area of Android Smartphones Forensics investigation, mostly working on the tools and techniques of android smartphone forensic investigation.

V. Venkateswara, et al. (14) have explored the list of android forensic tools and techniques available in the market and can be used to performing logical and physical acquisition and analysis. The authors have briefly described the tools and perform a comparison of tools with respect to the key features. Some of the tools are commercial in nature and other some are open source.

The list explored by the author is divided into two categories namely logical acquisition tools and physical acquisition tools. The author has included the tools in the list of logical acquisition are SAFT, AFLogical, LiME Module, NandRoid Backups, OSAF-TK (Open Source Android Forensics ToolKit), Santoku Linux, Whatsapp Extract, and Andriller. The author has included the tools in the list of physical acquisition are JTAG (Joint Test Action Group), Chip-Off, Cellebrite UFED Physical Analyzer, Oxygen Forensics Suite, Paraben Device Seizure.

Alamin, et al. (7) have performed a survey on a range of tools and techniques used to perform a forensic investigation of Android smartphones and provide the recommendation for following best practice for forensic investigation of Android smartphones. The authors have performed the comparison between various Android forensic tools available in the market along with their role in the forensic process. The comparison was performed along with various types of data elements stored in the internal memory of Android smartphones. The comparison was also based on the ability of the Android smartphone forensic tool to extract data element from the supported Android smartphones.

Mallidi, et al. (13) have discussed two acquisition methods namely Logical Acquisition and Physical Acquisition and both of these were performed using well-known smartphone forensic acquisition tools available in the market. The comparison of both of the acquisition method was performed by using three smartphone forensic tools on three different Android-based smartphones and presented by the authors along with the direction of the comparative study.

The comparison was measured on the basis of a list of data elements extracted by using the three smartphone forensics tools from the internal memory of three different Android-based smartphones. The data elements measured in comparison are common entries for all three Android-based smartphones and are including contacts, call logs, SMS, MMS, Emails, Calendar entries, Bookmarks, web histories, audios, videos, images etc.

P.S. Aiswarya (15) has discussed the current trend and technologies used as well as work performed in the field of forensic examination and analysis of three most widely used and popular social media applications namely Facebook, WhatsApp, and Twitter. The author explored about three most used android forensics investigation tools along with their key features, limitations, and capabilities of extraction of data associated with these social media applications.

The main emphasis of this research is to provide information concerned to the latest trend and work performed currently in the area of android forensics as well as in the area of social media application forensics like WhatsApp, Facebook, and Twitter forensics. The aim of this research according to the author is to highlights key features of Android forensics tools currently available in the market and is supported for doing social media applications.

Kausar, et al. (2) have described that their research is a comprehensive perspective of various Android smartphone forensics tools which are able to perform physical forensic acquisition of Android smartphones. The emphasis of this research is to provide detailed description about the Android smartphone forensic tools which can perform physical forensic acquisition of android smartphone as well as to present a comparative analysis of these android smartphone

forensics tools. The comparison is based on the parameters like cost, integrity, data recovery, usability, and support. The comparison provides us a convenient way or enables us to select a suitable physical acquisition tool which can have enough capability to perform the desirable physical acquisition.

Mahajan, et al. (16) have emphasized on data analysis of two famous and widely used instant messaging application installed on Android-based smartphones namely Whatsapp and Viber. The test was conducted on five different Android smartphones based on three different versions of the Android operating system. The purpose of this test was to determine what data is extracted if the concentration is pointed on an instant messaging application because the data elements associated with the instant messaging application are also counted as a valid digital evidence in court. The data element associated with the instant messaging application can be either of these chat messaging logs, history, send and received media files (audio, video, and images), documents and locations etc. Cellebrite UFED Classic Version 1.8.0.0 was used for analyzing and finding artifacts presented on the internal memory of android based Smartphone.

Osho, et al. (17) have evaluated the ability of extraction of the Android forensic tool with respect to the deleted data and find a better android forensics tool or toolkit which is able to perform the desired extraction of deleted data from the internal memory of Android smartphone. The finding of this research shows that two out of four tools performed well during acquisition of deleted data. The four forensics tools are FTK Imager, Encase, MOBILedit and Oxygen Forensic Suite.

Junaid, et al. (18) have focused on comparison of smartphone forensics tools and pinpointed different problem associated with different smartphone forensic tools likewise requirement of different supporting tools, efforts the posses to process, expertness the tool needed to work over it, time taken by the tool to accomplish the process of extraction of artifacts etc. the author also proposed a generic methodology for smartphones forensic tools which help the investigator to overcome the above mentioned problems or limitations while doing forensic investigation of smartphone using smartphone forensic tools.

MRKAIC, (19) has performed a forensic investigation of android smartphone named Alcatel One Touch 6012X with android version 4.2.2 Jelly Bean using some open source Android forensic tools. The author used different tools at different step of forensic process namely King Root, ADB, SQLite Browser, Autopsy, AFLogical, MOBILedit, NowSecure Forensic Community Edition (ViaExtract) and acquired a range of data from the android device including Audios, Videos, Images, Deleted data, Viber (Call Logs, Participants and messages), web history, contacts, call logs, emails etc. The author also performed between ViaExtract and Bundle of the tool including DD, SQLite Browser, and Autopsy.

de L. Sumao, et al. (4) have proposed a method for acquisition of Android smartphones which has different workflow along with different scenarios and procedures. The author conducted an experiment followed by the proposed method in which six Android smartphones were examined. The smartphones were grouped into four scenarios, involving a different situation that an analyst can encounters.

Lessard, et al. (20) have conducted an experiment for android forensics using an experimental device based on Android platform named Sprint HTC Hero Android Version 1.5. After gaining root access using USB debugging enabled service they used dd command to make an image and FTK imager to get the image of SD card using export disc image option. The experiment was successful to acquire from the memory of an Android smartphone.

N. Umale, et al. (21) have revealed a list of challenges faces by mobile phone forensic investigator and list out some mobile device forensic tools categorized in the commercial and open source category.

Shadzik, et al. (22) have conducted an experiment on data extraction using three most widely used android forensic toolkits namely CAINF (Computer Aided Investigative Environment), Santoku Linux and Cellebrite UFED Forensic toolkit. Except for Cellebrite UFED both the other tools are open source. The author also performed a comparison between the open source tools and Cellebrite UFED forensic tool quantitatively and qualitatively.

The testing devices were Samsung Galaxy Core based on Android version 4.4.2, Samsung Galaxy S3 based on Android version 4.4.4, LG Optimus based on Android version 2.2.2. The data extraction methods used in the experiment was performed by Bulk Extractor, QphotoRec, Autopsy 4.0.0 Sluithkit, and Cellebrite Touch. The author found that the Bulk Extractor performed better quantitatively whether the Autopsy Sluithkit performed better qualitatively.

Alghafli, et al. (23) have described a list of recommended guidelines to be followed while doing forensic investigation of smartphones or during the forensic process of smartphones including seizure, acquisition and analysis/examination. As the digital forensic process is of four major step containing process including preservation, acquisition, examination/analysis, and presentation, the author presented a list of guidelines which should be followed at each step of the digital forensic process. The author also described the challenges encountered during the digital forensic process of smartphones.

Pinheiro dos Santos, et al. (24) have proposed a method or model named "One Way Form" to collect and analyze digital evidence contained in the Android smartphone by using android smartphone forensics tools and techniques in an easy, fast, forensically sound and clean way with full of data integrity.

The proposed model contained each and every necessary step to be followed for android forensics starting from seizing or preservation to the presentation. The proposed model contains steps including Seizure, First Analysis, Data Extraction, Documentation and Finalize the Analysis. Each step of this proposed model is simplified by sub-steps to be followed accordingly for android smartphone forensic process.

Faheem, et al. (25) have conducted an experiment to recover the data contained in an Android smartphone. The testing device used in the experiment was Samsung Galaxy S3 based on Android version 4.2.2 and the step involved in the experiment are: Gaining root access by enabling USB Debugging option and by installing and using srsroot tool on the machine, Creating DD Image of memory, and analyzing

DD Image using the one month trial version of Cellebrite UFED Physical Analyzer.

3. DIGITAL FORENSICS LOGICAL ACQUISITION TOOLS FOR ANDROID SMARTPHONES

A bunch of tools is available in the market to perform logical acquisition of Android smartphones in forensically sound manner. Some of the tools we briefly describe here are independent application soft integrated with a framework and some other are a combination of hardware and software solution assembled in a forensic toolkit with necessary peripherals and supporting forensic tools. The list of tools we used in our comparative study is the latest version. Here we have the following tools that are used to perform logical acquisition on Android smartphones.

A. EnCase Smartphone Examiner Version 7.10.00.103

A comprehensive smartphone forensic solution designed and developed by Guidance Software Inc. Guidance Software Inc. is a leading industry in digital forensics software product development. EnCase smartphone examiner is designed to acquire data from the internal memory (NAND Flash memory) of Android smartphones and to review and collect digital data from the Android smartphones (26).

EnCase Smartphone Examiner performs a forensically sound acquisition of Android smartphones and acquire data from the device like Audio, Video, Image, Contacts, Call Logs, Document, Web History, Instant messenger and Social Networking Application Data as well. EnCase Smartphone Examiner is basically designed for Logical and physical acquisition as well as for doing forensic data analysis and report generation from the variety of Android smartphones**.**

A new release EnCase Forensic 8.05 with inbuilt EnCase Mobile Investigator supports over 26,000 mobile devices of over 25 types as well as it provides forensically sound and flexible investigation to collect and analyze digital evidence from the mobile devices including SMS, Call Logs, Audios, Videos, Images and much more. EnCase Forensic 8.05 maintain the integrity of digital evidence and produce result report in an easily accessible file format as well as it includes bookmarking images. EnCase Forensic 8.05 allows the examiners to extract digital evidence from a wide range of mobile devices and enables the examiner to search and identifies digital evidence found in the mobile devices along with the priority basis. EnCase Forensic 8.05 is capable to decrypt encrypted data as well as EnCase Forensic 8.05 includes password recovery module (27)**.**

Encase Mobile Investigator is an acquisition tool which enables the examiner to extract and analyze digital evidence and generate desired forensic report. It is capable to extract and analyze digital evidence from a wide variety of mobile devices of different operating systems and installed application on the devices. It enables the examiner to view acquired digital evidence, analyze digital evidence and generate a report as well as it has bypassing feature which enables the investigator to investigate locked mobile device by bypassing the security lock of the device (28).

EnCase V4.20 is used to acquire data from two android mobile devices namely Samsung Galaxy GT-S5300 based on Android V-2.3.1 and HTC Desire 300 based on Android V-4.1.2. As a result, encase performed better in extracting deleted data during the acquisition of Samsung Galaxy GT-S5300 and performed better in extracting images, audios, and videos during acquisition of HTC Desire 300. Encase couldn't extract information concerned to the SIM and Equipment for both of the devices. The overall performance of EnCase is better among other used forensic tools (17).

PDA (Personal Digital Assistant) is a handheld device like mobile devices. A range of forensic tools is available for examination of PDA including Encase which cannot be used for all PDA due to the variation in the operating system but it supports the wide variety of PDA based on some operating systems. Encase cannot be used for forensic examination of Pocket PC but it supports Palm OS and creates a read-only physical image and further logical data acquired from it. Encase is feature rich, it includes bookmarking which enables the examiner to bookmark section of files, files and directories called folders for further utilization. Similarly encase also includes reporting feature which enables the examiner to search information of files and acquire report as case file which is created by EnCase (29).

B. Mobile Device Seizure Version 7.4

Mobile Device Seizure is also known as Paraben's Device Seizure and is an Android smartphone forensics tools designed and developed by Paraben Corporation established in 2001. Paraben's Device Seizure is a lightweight android forensics tool and it has minimum system requirements. Paraben's Device Seizure allows us or an investigator to extract or acquire digital data from the Android smartphones in a forensically sound condition. Paraben's Device Seizure allows us to acquire physical as well as the logical image of Android smartphones internal memory. Paraben's Device Seizure also analyzes data automatically (30).

Paraben’s Device Seizure supports over 24000+ mobile devices and it also has a key feature of auto detection facility during the process of acquisition of the Android smartphone. Paraben’s Device Seizure performs a forensically sound acquisition of Android smartphones and it acquires digital data from the Android smartphones like Contacts, Call logs, SMS, MMS, Audios, Videos, Images and many more. Paraben’s Device Seizure has an easy to use graphical user interface and it also has an ability to perform not only logical acquisition of an Android smartphone but also perform physical and file system acquisition. Paraben’s Device Seizure has an inbuilt bypassing tool which is used to bypass the security lock of the android device (31)**.**

New release of Paraben’s Device Seizure V7.6 also known as Mobile Device Seizure tool version 7.6 has a great range of key features along with the traditional features of smartphones forensics acquisitions. The Mobile Device Seizure version 7.6 key features include data acquisition, inbuilt password recovery software, SIM card information extractor, deleted data recovery tool as well as inbuilt Google Earth which makes it possible to view Geographical Positioning System Co-ordinates (Longitude and Latitude) of KML files contained in the Android smartphones (32).

The physical acquisition provides the examiner more digital evidence. The Paraben's Device Seizure is a forensic tool which can perform both the logical and the physical acquisition of internal memory of mobile devices but the focus of this tool is on the physical acquisition. It supports

and performs analysis of unsupported phones manufactured by the supported manufacturer. It can perform search operation over memory dumps acquired from the mobile devices to extract digital evidence. The Paraben's Device seizure needs minimum system requirements during installation on any computer (5).

Paraben's Device Seizure can perform not only logical acquisition but also perform physical acquisition, file system acquisition, in-depth analysis and generate a report of extracted data. Paraben's Device Seizure can also perform bypassing means it enables the examiner to extract password if the device has a security lock. Paraben's Device Seizure allows the examiner to recover most of the deleted data from the mobile devices mostly from the Android smartphones up to version 4.4.2 (2)**.**

A new release Paraben's Device Seizure version 7.6 can acquire data from Android smartphones as well as it supports over 26000+ mobile devices. Paraben's Device Seizure version 7.6 includes Samsung bootloader physical plug-in for physical acquisition of Samsung smartphones based on Android. Paraben's Device Seizure version 7.6 supports the logical acquisition of iOS 10 based smartphones as well as it allows the examiners to perform logical acquisition of Android smartphones based on Marshmallow android version. The newly released version of the LinkedIn application is also supported by Paraben's Device Seizure version 7.6. Data parsing of a range of Android application is also possible using Paraben's Device Seizure version 7.6 including a newly released version of applications like Whatsapp, Facebook, Twitter, LinkedIn, Skype, Snapchat, Facebook Messenger, EverNote, G-Mail, Google Chrome, BB Messenger and Google Map etc**.** Paraben's Device Seizure version 7.6 can export acquired data to PC and Import data from cloud services as well as it can generate a comprehensive report in HTML, text, XLSX and pdf formats. Paraben's Device Seizure version 7.6 can acquire SIM card information from CDMA and GSM SIM Cards whether deleted. Paraben's Device Seizure version 7.6 can acquire SMS, Contacts, Call Logs, and variety of passwords using an inbuilt function of password recovery (33).

C. Mobile Oxygen Forensics V8.3.1.105

Also known as Oxygen Forensics Kit or Oxygen Forensics Suite designed and developed by Oxygen Forensics Corporation founded in 2000. The products developed by Oxygen Forensics Corporation are used in over 100+ countries around the world and the product's customer includes various government agencies working on defense and security tasks of different countries. Oxygen Forensic kit is ready to use mobile forensics solution which does not need any additional installation and settings. Hence Oxygen Forensics kit is a customizable mobile forensic solution it includes Oxygen Forensics Extractor installed and configures, Windows installed and configured, Oxygen Forensics image pack installed and configured, Oxygen Forensics driver pack installed and configured, Microsoft Bluetooth driver pack installed and configured and at last it includes more than 200GB free space to install additional forensic software tool as well as to store data. Oxygen Forensics kit is designed for portability and it comes with full cable set. The key functionality of the Oxygen Forensics Kit includes: It contains 30+ data extraction methods from over 16000+ mobile devices as well as data extraction facility from over 35+ cloud storage services. The Oxygen Forensics kit supports over 380+ unique applications and over 3000+application versions. It allows us to import and analyze call data records and also allows us to extract and analyze geographical positioning data records.

Oxygen Forensics has three variants Oxygen Forensics@Extractor, Oxygen Forensics@Analyst and Oxygen Forensics@Detective.

Oxygen Forensics@Extractor:- it is just an extractor inbuilt with the Oxygen Forensics@Analyst and Oxygen Forensics Kit. It allows us to extract device information, contacts, call logs, organizers data, SMS, MMS, iMessage, Emails with attachments, Audios, Videos, Images, GPS data and stand-alone application data.

Oxygen Forensics@Analyst:- Oxygen Forensic Analyst is powerful forensics software used to extract data from the mobile device. It has an ability to acquire data from over 17520+ devices including Android smartphones as well as it has an ability to parse data over 410+ unique application and over 5850+ application versions. It also has an ability to recover deleted data. It enables us to search data by keyword and has an ability to generate extraction report in easily accessible file format like PDF, XLSX, and XML etc. The Oxygen Forensic Analyst key feature includes SQLite Viewer, Android Rooting and PList View where the SQLite viewer allows us to explore database file extracted from the Android device with the file extension .sqlite, .sqlite3, .sqlitedb, .db, .db3.

Oxygen Forensic V8.3.1.105 is a smartphone forensic tool which enables the examiners to acquire equipment information, contacts, call logs, organizers data (like Calendar data, to do list, tasks, schedules, events, and memos), SMS, MMS, Emails, Images, Audios, Videos, GPS Data and much more from an android devices as well. Oxygen Forensic has an inbuilt tool named Oxygen Forensic Analyst which further has an inbuilt small tool named SQLite Viewer which enables the examiner to explore database files**.**

Oxygen Forensic Analyst and Oxygen Forensic Detective both are the version of Oxygen Forensic Suite and has an ability to find and determine malicious and spyware applications installed on Android smartphones. Oxygen Forensic has an advanced feature for reporting artifacts found in the smartphones with variety graphs after acquisition and analysis of data from the smartphones. Oxygen Forensic Suite supports over 11000 mobile devices and over 300+ application as well as 1000+ application versions. Oxygen Forensic Suite enables the examiners to extract GPS data from the concerning sources resides in the smartphones or mobile devices (34).

Oxygen Forensic Suite can extract Skype and Whatsapp data (25).

According to an experiment of tool testing performed on two Android smartphones namely HTC Desire S and HTC Sensation XE using Oxygen Forensic Suite 2012 Standard. Oxygen Forensic Suite contains a range of USB drivers for all most all Android smartphones which need the USB debugging enabled during a forensic examination of Android smartphones. Oxygen Forensic Suite produces a report in pdf format. Oxygen Forensic Suite extracted data including equipment information, Contacts, Call Logs, Images, Audios, Videos, Calendar, and Standalone document files from HTC Desire S and Equipment

Information, Contact, Call Logs, Images, Audios, Videos and Stand Alone Files from HTC Sensation XE. SMS and MMS didn't extract by the Oxygen Forensic Suite from both of the devices (1).

Oxygen Forensic Suite Version 5.1.2.153 is a commercial forensic tool but the company offers the open source version for 6 months and it can extract Equipment Information, Contacts, Call Logs, SMS, MMS, Emails, Calendar Events, and files etc. limitation with this tool is that it can run only on windows. This tool is easy to use and it can perform acquisition and examination of Android smartphones as well. The inbuilt feature named Oxygen Forensic Extractor performs all the tasks if the device is properly connected to the workstation which has preconfigured and preinstalled Oxygen Forensic Suite. The open source version of Oxygen Forensic Suite has limited access but it can acquire enough data concerned with the devices (35).

D. MOBILedit Forensic V7.8.3.6085

A digital forensic product designed and developed by Compelson Labs. A list of products is developed by Compelson Labs and MOBILedit Forensic is a customizable mobile device forensic solution or all-in-one smartphone forensic tool consists of smartphone extractor, cloud extractor, data analyzer and report generator. MOBILedit Forensic tool is used for physical as well as the logical acquisition of Android smartphones and it has unique functionalities including application data analysis, deleted data recovery, report generation in an easily accessible file format. MOBILedit Forensic tool has a user-friendly graphical user interface and it also has password and PIN breaker tool as an inbuilt form.

MOBILedit Forensic tool allows us to extract data from the Android smartphone device fully on few click in forensically sound manner and the data it extracts includes deleted data, call logs, contacts, SMS, MMS, Audios, Videos, Images, Organizers Data, instant messaging app and social networking app data and much more easily and efficiently (36).

MOBILedit Forensic includes the following key features:

- Physical as well as logical data acquisition and analysis
- Advanced application data analysis
- Deleted data recovery
- Report generation in PDF, XLSX, and HTML formats
- Password Cracking with GPU Acceleration
- Easy to use GUI with concurrent data extraction of Android smartphone devices.
- Camera Ballistics- Scientific Image Analysis
- ICloud Analyzer, Photo Recognizer, report generation in any language, live updates.

The trial version of MOBILedit V-5.5.0.1148 is used to perform logical acquisition and analysis of android smartphone which has some limitations like the examiner cannot export files but is able to acquire equipment information and SIM card information as well as it can acquire contacts, Call logs, MMS and Calendar event information (19).

MOBILedit enables the examiner to perform acquisition, analysis, and reporting of data of an Android smartphone including deleted data. MOBILedit forensic tool supports a range of mobile devices including Android and iOS. MOBILedit is updated and upgraded by the COMPELSON Labs along the time with new and advanced features so that it can support newly released smartphones. MOBILedit Forensic tools can generate a report in any language and can be presented as it is produced (2).

MOBILedit Forensic tool enables the examiner to perform extraction, examination, and reporting of data from Android smartphones including contacts, call logs, SMS, MMS, Files, organizer data, equipment information, SIM card information, Location data and application data etc. MOBILedit Forensic tool can retrieve deleted data and can bypass security lock on an Android smartphone (34).

E. MPE+ Version 5.5.3.73

MPE+ is abbreviated as Mobile Phone Examiner plus Investigator and is designed and developed by AccessData Group. Mobile Phone Examiner Plus is a smartphone forensics software product which supports over 7000+ mobile devices with different platforms and different manufacturers including android based smartphones. Mobile Phone Examiner Plus as we know is a smartphone forensic software product but now it comes in Mobile Phone Examiner Plus tablets means Mobile Phone Examiner Plus tablet is also available for Smartphone forensic investigation. It is done because of to include portability feature in smartphone forensic investigation process for doing an investigation as fast as it can. The Mobile Phone Examiner Plus tablet is preconfigured with the Mobile Phone Examiner Plus as well as some more essential tools (Preinstalled and configured with the tablet pc) needed for smartphone phone forensic investigation. Mobile Phone Examiner Plus enables us to perform advanced smartphone forensics investigation without purchasing expensive smartphone forensics suites. Using Mobile Phone Examiner Plus we and the investigator can bypass locked devices, extract data safely and can create a forensic image to be used for further investigation. Mobile Phone Examiner Plus enables us to acquire a logical image of an Android smartphone and enables us to extract full data from the rooted Android smartphones.

Mobile Phone Examiner Plus is a standalone application provides the examiner different connectivity method including USM, Bluetooth, and Infrared. Mobile Phone Examiner Plus when integrated with AccessData's (FTK Forensic Toolkit), it becomes a more powerful forensic tool.

New release of Mobile Phone Examiner Plus supports over 10,000+ mobile devices including Chinese chipset mobile devices. Mobile Phone Examiner Plus can perform physical and logical acquisition of mobile devices (including Android smartphones) and has a security bypassing capability. Mobile Phone Examiner Plus is 30% faster than other forensic tools and has a SQL builder to perform parsing of application data consists of SQLite Database. Mobile Phone Examiner Plus has an inbuilt python script which allows the examiner to perform parsing everything from mobile devices with user-friendly interface and perform analysis with a graphical view as well as search, filter and collect data from mobile devices and produce a report of desired or all data in different formats.

Mobile Phone Examiner Plus is the only forensic tool which is able to identify and examine installed application on mobile devices and can extract and analyze potential data associated with these applications. By adding Mobile Phone

Examiner Plus add-on hardware named MPE+ VELOCITOR enables the examiner to extract data from over 95%+ Chinese mobiles similarly a combination of MPE+ and nField makes the Mobile Phone Examiner Plus powerful smartphone forensic extraction tool with user-friendly GUI.

F. Secure View Version 4.1.9

Secure View v4 is a mobile forensics investigation tool designed and developed by Susteen Inc. Industry. Secure View becomes the first mobile forensic software tool, the later version of secure view namely secure view v3 and secure view v4(current version) comes in a combination with both the hardware and software solutions. In simple, the Secure View v4 is an ultimate mobile phone forensic investigation toolkit with the combination of both hardware and software. It has an analyzing tool, bookmarking tool, reporting tool along with extraction. It can generate a complete report showing detailed information found on the smartphone including deleted data, document files, Audios, Videos, Images, SMS, MMS, Contacts, Call Logs and much more. Secure View v4 kit includes a software CD with complete data cable set, the kit contained in a solid state case and it also includes a quick instruction guide**.** It also enables the examiner to perform data extraction of social networking application data including Facebook, Twitter, and MySpace and can also extract equipment information (37).

Forensic tool Secure View has advance features including svSmart, svPin, svLoader and svReviewer. Each of these inbuilt features performs specific forensic tasks. The Secure View also performs extraction of SIM Card data by using SIM Card reader contained in Secure View forensic kit. Secure View has different connectivity methods including USB Cable, Bluetooth and IR (38).

G. Cellebrite UFED Touch v4.4.0.1

UFED Touch is smartphone forensic investigation software cum hardware toolkit designed and developed by Cellebrite Mobile Synchronization Inc. an Israel Company established in 1999. Cellebrite UFED is abbreviated as Cellebrite Universal Forensics Extraction Device. Cellebrite UFED offers a range of smartphone forensics investigation products for data acquisition and analysis of a range of mobile devices with different platforms and different manufacturers. Cellebrite UFED Touch logical is a commercial tool available for logical acquisition and analysis of data acquired from an Android device as well. Cellebrite UFED is the first and the most important tool for physical NAND flash memory acquisition or extraction. Cellebrite UFED touch enables us or the investigator to extract data from over more than 6800 mobile devices with different platforms and different manufacturers. Cellebrite has many variants like Cellebrite UFED Ultimate, Cellebrite UFED Touch Logical, Cellebrite UFED Touch Physical Analyzer and Cellebrite UFED Touch Logical Analyzer.

The Cellebrite UFED Touch Logical kit includes the following Software (Cellebrite UFED Logical Analyzer, Cellebrite UFED Phone detective and Cellebrite UFED Reader), Hardware (UFED Touch Device, UFED Solid Protector Case, Cable Sets, Cable organizers, Cloning Devices, Power Supplies , Card readers, Faraday Bag, External Hard Drives, Flash memory and many more).

Cellebrite UFED Touch allows full logical extraction of data from a range of smartphones, SIM Card Cloning, Bypass PIN, Locked SIM and Missing SIM Cards, Internal memory of an Android smartphones and can acquire data, passwords, instant messaging application data, SMS, MMS, E-Mails, Calendars, Audios, Videos, Images, Contacts, Call logs, phone Details and SIM Card Details. It enables the examiner to perform logical, physical and files system acquisition along with the password recovery.

H. ViaExtract Version 2.5

ViaExtract also called ViaExtract Community Edition (CE) Version 2.5 or NowSecure Forensic Community Edition is a smartphone forensics investigation software tool used for logical and physical extraction of data contained in the internal memory of android based smartphones. ViaExtract is designed and developed by NowSecure (Formerly known as ViaForensics) Corporation. Logical and physical acquisition can be performed by the commercial version of NowSecure forensic community edition. NowSecure Forensic Community Edition is now available free and it allows us or the investigator to perform logical acquisition with the File System Acquisition, backup, rooting facility and recovery of SMS, Contacts, Call Logs and much more easily and efficiently in a forensically sound manner. ViaExtract is available with the Santoku Linux but in a package. The Santoku Community Edition can be run in VirtualBox or VMWare and both of these are also open source. Due to the open-source availability of ViaExtract (NowSecure Forensic Community Edition), the forensic investigation of Android smartphone is now easier, faster and more powerful ever. The investigator can perform more powerful logical acquisition, analysis, and reporting of an Android smartphone.

The ViaExtract has the key features including easy to use Graphical User Interface for performing data acquisition on Android smartphones and allows the investigator to perform searching and sorting of desired data from over the acquired data of Android smartphone.

ViaExtract is a pre-configured Virtual machine which can run on Linux, Windows or MAC operating System means the ViaExtract requires a third party Virtual Environment to be used for forensic investigation. ViaExtract can find browser history but it does not support file curving (39).

I. XRY-XACT Version 6.10.1

A complete smartphone forensic investigation solution designed and developed by a Swedish company named Micro Systemation established in 1984. XRY-XACT completes Micro Systemation's range of forensics solution because the XRY-XACT enables the investigator to perform forensically sound extraction of data from a wide range of mobile devices based on a variety of different platforms and different make, model, and manufacturer. MSAB XRY-XACT is complete software cum hardware solution which allows the user or the investigator to perform physical acquisition to recover deleted data as well as allows the user or investigator to perform logical acquisition of data and generate a forensic report for a legal purpose. XRY-XACT generates a Hex Dump from the internal memory of mobile device during physical data acquisition and this Hex Dump allows the investigator to recover deleted data.

XRY-XACT allows the investigator to acquire data from a locked device and provides data protection guarantee. XRY-XACT allows the investigator to dump internal memory as well as memory card securely and automatically

decode the dump data into information. XRY-XACT as we know a complete mobile forensic solution, therefore, includes hardware, software, and cables set all at one place to access and recover data from mobile devices and memory cards. XRY-XACT also has an ability to extract protected data if exists in the mobile devices as well as it provides access to the raw files during logical acquisition (40)**.**

XRY version 5.5 enables the examiner to extract data about Viber including Chat and Call logs. It produces a report in pdf format and it preserves extracted data in X-Ways Evidence File Container (with .ctr format), the integrity of data is maintained using MD% hash values (25).

Newly released XRY version 7.0 is a powerful, lite and fast forensic tool which supports over 18625+ mobile device profiles and over 1117+ applications and their versions. XRY version 7.0 can extract data from a wide range of mobile devices as well as can extract data from cloud storage service application automatically or manually. A range of advanced feature added with XRY 7.0 as well as much more improvement has been done on XRY 7.0 including physical acquisition of Samsung Galaxy S5 and S6, easy rooting of Galaxy S5 and Note III for data dumping through bypassing, automatically dumping and decoding of extracted data, and support to LG devices (41).

4. COMPARISON OF ANDROID SPECIFIC MOBILE DEVICE FORENSIC TOOLS BASED ON LOGICAL ACQUISITION

This research is subjected to the comparative study of various digital forensics logical acquisition tools for Android smartphones. All the above tools are able to perform logical acquisition of Android smartphones and can acquire data available in an android device. There is no any generic tool currently available in the market which can perform full logical acquisition of all kind of Android smartphones made by all kind of manufacturing companies. Due to the variation in platform version, make, model and manufacturer as well as due to the fast technology evolution and association with the Android smartphones it is too much tedious and difficult to perform full logical acquisition using single generic logical acquisition tool.

The above-mentioned android forensic tools are able to perform logical acquisition of a limited range of Android-based smartphones not all and can acquire potential digital data from the Android smartphones partially or fully. The comparison between all the above mentioned logical acquisition tools will be based on the ability of the tools to acquire data from the internal memory (NAND Flash Memory) of the supported Android smartphone. The comparison between tools will be measured by analyzing data acquired from the internal memory of supported Android smartphone.

We have a list of data objects and which can be contained in the internal memory of supported Android smartphone. Supported Android devices are Samsung Galaxy S5 and S6. Both the Android smartphones are based on Android version 4.2.2 and version 5.1.1 respectively and both of these are CDMA handset. The tests were performed in NIST CFTT Lab. In this paper, researchers have used

Data objects and associated data elements to be considered during logical acquisition are:

various reports generated by NIST for various mobile devices. The researcher has focused on Samsung Galaxy S5 and S6 mobile and tried to compare extracted data objects by various tools.

Comparative measurement of tools has been done by using extracted data objects and associated data element stored in internal memory of Samsung Galaxy S5 and S6, we have a list of data objects and their associated data element. These data objects will be extracted and considered as a parameter of the comparative study of forensic tools.

S. NO.	DATA OBJECTS	DATA ELEMENTS
1	Equipment Data/ User Data	IMEI, MEID/ESN, MSISDN
2	PIM Data	Contacts, Calendar, To Do List, Tasks, Memos
3	Call Logs	Incoming, Outgoing, Missed and Deleted Calls
4	SMS	Incoming, Outgoing, and Deleted SMS
5	Multi-Media Messages	Incoming, Outgoing, and Deleted SMS
6	Stand-Alone Files	Audio Files, Video Files, and Images (Deleted also)
7	Application Data	Word Document, Excel Sheet, PowerPoint Slides, Text Documents and PDF files as well as other device-specific application data
8	Internet Data/ Browser	Bookmarks, Browser Histories, E-Mails with Attachments
9	Social Networking Application Data	Facebook, Twitter, LinkedIn and Instagram data
10	GPS Location Data	Coordinates

To understand the comparison table containing a comparison of logical acquisition tools we have following keywords.

As Expected (AE) – it indicates that the logical acquisition tool successfully acquired and reported corresponding data from the internal memory of supported Android smartphone.

Partial (P) – it indicates that the logical acquisition tool partially acquired and reported corresponding data from the internal memory of supported Android smartphone.

Not As Expected (NAE) – it indicates that the logical acquisition tool does not acquire and reported corresponding data from the internal memory of supported Android smartphone.

Not Applicable (NA) – it indicates that the logical acquisition tools do not support data element for acquisition.

Comparison of Android Forensics Logical Acquisition Tools										
Data Objects	Data Elements	EnCase Smartphone Examiner v7.10.00.103	Mobile Device Seizure v7.4	Mobile Oxygen Forensics v8.3.1.105	MOBILedit Forensic v7.8.3.6085	MPE+ v5.5.3.73	Secure View v4.1.9	UFED Touch v4.4.0.1	viaExtract v2.5	XRY-XACT v6.10.1
Connectivity	Non Disrupted	AE	…	…	AE	AE	…	AE	AE	AE
	Disrupted	AE	AE	AE	AE	AE	NAE	AE	AE	AE
Reporting	Preview Pane	AE	AE	AE	P	AE	AE	NA	AE	AE
	Generated Report	AE	AE	AE	P	AE	AE	P	AE	P
Equipment /User Data	IMEI	NA	AE	AE	NA	NA	AE	NA	NA	NA
	MEID/ESN	AE	NA	NA	AE	AE	NA	AE	AE	AE
	MSISDN	NAE	AE	NAE	NAE	NAE	AE	AE	NAE	NAE
PIM Data	Contacts	AE	AE	AE	AE	P	P	AE	P	P
	Calendar	AE	AE	AE	AE	NA	AE	AE	AE	AE
	To Do List /Tasks	NA	NAE	NAE	NA	NA	NAE	NA	NA	NA
	Memos	NAE	NAE	NAE	NAE	NA	NAE	NAE	NAE	NAE
Call Logs	Received	AE	AE	AE	AE	AE	AE	AE	NAE	AE
	Dialed	AE	AE	AE	AE	AE	AE	AE	NAE	AE
	Missed	AE	AE	AE	AE	AE	AE	AE	NAE	AE
SMS	Received	AE	AE	AE	AE	AE	AE	AE	AE	AE
	Send	AE	AE	P	AE	AE	P	AE	AE	AE
MMS	Image	AE	P	AE	P	AE	AE	AE	AE	AE
	Audio	AE	P	AE	P	AE	AE	AE	AE	AE
	Video	AE	P	AE	P	AE	AE	AE	AE	AE
Stand Alone Files	Image	AE	AE	AE	AE	AE	AE	AE	AE	AE
	Audio	AE	AE	AE	AE	AE	AE	AE	AE	AE
	Video	AE	AE	AE	AE	AE	AE	AE	AE	AE
Application Data	Document txt/pdf	AE	AE	AE	AE	NAE	AE	AE	NAE	NAE
	Excel Sheet	NA	…	…	NA	NA	…	NA	NA	NA
	Slides	NA	…	…	NA	NA	…	NA	NA	NA
Internet Data	Bookmarks	NAE	NAE	NAE	AE	AE	NAE	AE	AE	AE
	Web History	AE	NAE	NAE	AE	AE	NAE	AE	AE	AE
	E-Mail	…	NAE	NAE	…	…	NAE	…	…	…
Social Networking Application Data	Facebook	NAE	NAE	NAE	NAE	AE	NAE	AE	NAE	AE
	Twitter	NAE	NAE	NAE	AE	AE	NAE	AE	NAE	AE
	LinkedIn	NAE	NAE	NAE	AE	AE	NAE	AE	NAE	AE
	Instagram	…	NAE	P	…	…	NAE	…	…	…
Acquisition (Logical)	Acquired All	AE	AE	AE	NA	AE	AE	NA	AE	AE
	Selected All	AE	…	…	NA	AE	…	NA	NA	NA
	Selected Individual	AE	…	…	AE	AE	…	AE	NA	NA
Data Protection	Modified Case Data	AE	AE	AE	AE	AE	AE	AE	AE	AE
GPS Data	Coordinate Long./Lat.	AE	NAE	NAE	NAE	NA	NAE	AE	NA	AE

5. CONCLUSION

The purpose of this paper is to know and explore a variety of logical acquisition tools for Android-based smartphones as well as to know how what and how much data elements are can be acquired from the explored logical acquisition tools. The main emphasis of this research is to perform comparison between the explored logical acquisition tools along with its features embedded in the tools, strength of the tools, weaknesses of the tools, limitation of the tools, supporting tools to be used for complete logical acquisition, number of devices operating system, manufacturer supported by the tools and number of application and version supported by the tools as well as type of acquisition the tool can also perform.

By the comparison of tools, we conclude that some of the above-explored tools are surprisingly able to perform logical acquisition from a range of Android-based smartphone efficiently and effectively in forensically sound manner and produces the desired outcome.

All the above-explored tools were used to extract data logically from Samsung Galaxy S5 and S6. Researchers found that all the tools used during the study are able to extract data of data objects like contacts, calendar, SMS, MMS and standalone files. MPE+, Secure View, ViaExtract and XRY/XACT can partially extract contacts likewise Oxygen forensic and secure view both can partially extract send SMS data (Audios, Videos, and Images). Similarly Device Seizure and MOBILedit both forensic tools can partially extract MMS. MPE+ does not support calendar data to be extracted. All explored tool provides data protection against modification during acquisition and generates a forensic report. MOBILedit, Cellebrite UFED Touch, and XRY/XACT generate partial instead of full forensic report.

Call Logs (Incoming, Outgoing and Missed calls), all tools except ViaExtract are able to extract. Similarly, the text document and pdf files can be extracted by most of the tools except MPE+, ViaExtract, and XRY/XACT. Data elements namely Spreadsheet and Slides associated with application data objects do not support by most of the tools due to this fact they were not considered when the test was performed using Device Seizure, Oxygen Forensic, and Secure View.

Personal Information Management data namely To-Do List/ Task and Memos are the only data elements which couldn't be extracted by using the above forensic tools. Similarly, Memos data element is supported by all forensic tools except MPE+ but none of them could extract data about Memos data element

The mobile phone forensic tool development companies, law enforcement agencies, and Android-based smartphone manufacturer company need to be focused on this research and try to propose a generic solution.

We conclude that due to the unavailability of a unique generic logical acquisition tool for the android based smartphone this is impossible to perform full data acquisition using a single smartphone forensic logical acquisition tool. The emphasis of our research was to find logical acquisition tool from among the available mentioned tools which can acquire maximum data element from the internal memory of Samsung Galaxy S5 and S6. We also conclude that the variation in the version as well as in make, model, and manufacturer affects the ability or capability of tools to acquire data element from the Android smartphones.

REFERENCES

1. **Vijayan, Vijith.** Android Forensic Capabilities and Evaluation of Extraction Tools. Advanced Security & Digital Forensics, Edinburgh Napier University. Edinburgh, Scotland : Edinburgh Napier University, April, 2012. pp. 1-71, Thesis. Master of Science in Advanced Security & Digital Forensics.
2. Analysis of Physical Image Acquisition forensic tools for android smartphones. **Kausar, Firdous and Alyahya, Tadani Nasser.** 11, 11 01, 2016, International Journal of computer Science and Network Security , Vol. 16, pp. 38-45. ISSN: 1738-7906.
3. Digital evidence extraction and documentation from mobile devices. **V. Dharaskar, Dr. Rajiv, M. Thakare, Dr. Vilas and Rizwan, Ahmed.** 1, 01 01, 2013, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, pp. 1019-1024. ISSN (Print) : 2319-5940, ISSN (Online) : 2278-1021.
4. Acquisition of Digital Evidence in Android Smartphones. **de L. Sumao, Andre Morum, et al.** Brasil : 9th Australian Digital Forensic Conference, 12 05, 2011, Edith Cowan University Research Online, pp. 116-124. DOI:10.4225/75/57b2c3dc40cf3.
5. A Framework for Designing Benchmarks of Investigating Digital Forensics Tools for Mobile Devices. **Yates, Maynard and Chi, Hongmei.** Kennesaw, GA, USA : 49th ACM Southeast Conference, 03 24, 2011, pp. 179-184. ACM 978-1-4503-0686-7/11/03.
6. **PAUL, KARIUKI.** GENERIC PROCESS MODEL FOR ANDROID SMARTPHONES LIVE MEMORY FORENSICS. THE FACULTY OF COMPUTING AND INFORMATION MANAGEMENT, KCA UNIVERSITY. Nairobi, Kenya : THE FACULTY OF COMPUTING AND INFORMATION MANAGEMENT, 2014. pp. 1-87, PROJECT THESIS. 12/02782.
7. A Survey on Mobile Forensics For Android Smartphones. **Alamin, Abdalazim Abdallah Mohammad and A/Nabi Mustafa, Dr. Amin Babiker.** 17, 2015, International Organization of Scientific Research Journal Of Computer Engineering (IOSR-JCE), Vol. 2, pp. 15-19. ISSN (O): 2278-0661, ISSN (P): 2278-8727.
8. Forensic Presevation of Digital Evidence on Mobile Devices from the Perspective of Efficient Generalized Forensics Framework for Mobile Devices (EGFFMD). **Ahmed, Rizwan, Dharaskar, Rajiv V. and Thakare, Vilas M.** 4, s.l. : National Conference on Innovation and Advancement in Computing, Department of IT, GITAM UNIVERSITY Hyderabad (A.P.) India, 04 2014, International Journal of Advanced Research in Computer Science, Vol. 5, pp. 214-218. ISSN: 0976-5697.
9. **Ayers, Rick, Brothers, Sam Brothers and Jansen, Wayne.** Guidelines on Mobile Device Forensics. U.S. Department of Commerce, National Institute of Standards and Technology. USA : NIST Special Publication 800-101, Revision 1, May,2014. pp. 1-85,

Report of Guidelines on Mobile Device Forensics. http://dx.doi.org/10.6028/NIST.SP. 800-101r1.

10. Forensics Analysis On Smart Phones Using Mobile Forensics Tools. **Jones, G. Maria and Winster, S. Godfrey.** 08, s.l. : Research India Publications, 2017, International Journal of Computational Intelligence Research, Vol. 13, pp. 1859-1869. ISSN 0973-1873.
11. **Casey, Eoghan and Turnbull, Benjamin.** Digital Evidence on Mobile Devices, CHAPTER 20. [book auth.] Eoghan Casey. Digital Evidence and Computer Crime, Third Edition. 3. s.l. : Published by Elsevier Inc., 2011, Vol. 1, 20, pp. 1-44.
12. The State of the Art Forensic Techniques in Mobile Cloud Environment: A Survey, Challenges and Current Trends. **Faheem, Muhammad, Kechadi, Tahar and Le-Khac, Nhien An.** 2, 06 2015, International Journal of Digital Crime and Forensics, Vol. 7, pp. 1-19. http://dx.doi.org/10.4018/ijdcf.2015040101.
13. A Comprehensive Analysis of Smartphone Forensics and Data Acquisition. **Mallidi, S Kumar Reddy and Palli, Parimala.** 2, 02 01, 2016, International Journal Of Advance Research in Computer Science and Software Engineering, Vol. 6, pp. 270-276. ISSN: 2277-128X.
14. Survey on Android Forensics Tools and Methodologies. **V., Venkateswara Rao and Chakravarthy, A.S.N.** 8, 11 01, 2016, International Journal of Computer Applications, Vol. 154, pp. 17-21. ISSN- 0975-8887.
15. A Study on Existing Trend for Forensic Examination of Social Networking Application on Android Phones. **P.S, Aiswarya.** 5, 02 2016, International Journal of Advance Research trend in Engineering and Technology, Vol. 3, pp. 98-104. ISSN (O): 2394-3785, ISSN (P): 2394-3777.
16. Forensic Analysis of Instant Messenger Application on Android Device. **Mahajan, Aditya, Dahiya, M.S. and Singhvi, H.P.'.** 8, 04 15, 2013, International Journal Of Computer Application, Vol. 68, pp. 38-44. ISSN: 0975-8887.
17. Comparative Evolution of Mobile Forensics Tools. **Osho, Oluwafemi and Ohida, Sefiyat Oyiza.** 01 08, 2016, International Journal Of Information Technology and Computer Science, pp. 74-83. ISSN (O): 2074-9015, ISSN (P): 2074-9007.
18. Proposed Methodology For Smartphone Forensic Tools. **Junaid, Mohammad, et al.** 2, 2015, Asian Journal Of Computer Science and Technology, Vol. 4, pp. 1-5. ISSN: 2249-0701.
19. Android Forensics Using Some Open Source Tools. **MRKAIC, ISAK.** Belgrade, Serbia : BISEC-2016, 10 15, 2016, Business Information Security Conference, pp. 1-5.
20. Android Forensic: Simplifying Cell Phone Examination. **Lessard, Jeff and Kessler, Gary.** 1, s.l. : ECU Publication Pre 2011, 09 01, 2010, Digital Device Forensic Journal, Vol. 4, pp. 1-12. ISSN: 1941-6164.
21. Mobile Phone Forensics Challenges and Tools Classification: A Review. **N. Umale, Ms Mohini, Deshmukh, Prof A. B. and Tambhake, Prof. M.D.** 3, 03 15, 2014, International Journal on Recenmt and Innovation Trend in Computation and Communication, Vol. 2, pp. 622-626. ISSN: 2321-8169.
22. Comparison of Open Source Android Forensics and Mthodologies in Data Acquisition. **Shadzik, Ali, Jasra, Pradeep and Jasra, Shashi Kumar.** 2, s.l. : JEFSR, 2016, Journal of Emerging Forensic Sciences Research, Vol. 1, pp. 4-17.
23. Guidelines For The Digital Forensics Processing Of Smartphones. **Alghafli, Khawla Abdulla, Jones, Andrew and Martin, Thomas Anthony.** s.l. : Austalian Digital Forensic Conference, 12 15, 2011, Edith Cowan University Research Online, pp. 1-8. DOI:10.4225/75/57b2b82a40ce7.
24. Forensic Simplified Methodology for Android Data Extraction. **Pinheiro dos Santos, Matias Romario, Ferreira, Taisa Alves and da Cunha Neto, Raimundo Pereira.** 4, 04 10, 2016, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, pp. 1111-1117. ISSN(O): 2320-9801, ISSN(P): 2320-9798.
25. Smartphone Forensic Analysis: A Case Study for Obtaining Root Access of an Android Samsung Galaxy S3 Device and Analyze the Image without an Expensive Commercial Tool . **Faheem, Mohammad, Lekhac, N.A and Kechadi, Tahar.** 5, s.l. : Scientific Research Publication Inc., 07 01, 2014, Journal Of Information Security, Vol. 1, pp. 83-90. DOI:10.4236/JIS.2014.53009.
26. **NIST, Homeland Security Science and Technology.** Test Results for Mobile Device Acquisition Tool: EnCase Smartphone Examiner v7.10.00.103. Department of Homeland Security Science and Technology, National Institute of Standards and Technology. USA : Department of Homeland Security Science and Technology, 2015. pp. 1-14, Test Results for Mobile Device Acquisition Tool.
27. **Guidance_Software.** Guidance Software. [Online] Guidance Software. [Cited: 01 04, 2018.] https://www.guidancesoftware.com/.
28. **Encase_Mobile_Investigator.** EnCase Mobile Investigator. guidancesoftware.com. [Online] Guidence Software. [Cited: 01 05, 2018.] https://www.guidancesoftware.com/encase-mobile-investigator?cmpid=nav_r.
29. Efficient Forensic Tools For HandHeld Devices: A Comprehensive Perspective. **A.K.Kaladevi, Somasheker, Keesara, Himabindu and Luo, Xin.** pp. 349-359.
30. E3-DS Features. Paraben. [Online] Paraben Corporation. [Cited: 01 05, 2018.] https://www.paraben.com/downloads/features/E3%20DS%20Feature%20Chart.pdf.
31. **NIST.** Test Results for Mobile Device Acquisition Tool, Device Seizure v7.4 build 5921.15166. Department of Homeland Security Science and Technology, National Institute of Standards and Technology. USA : Homeland Security Science and Technology, 2016. pp. 1-18, Test Results for Mobile Device Acquisition Tool.
32. Paraben Device Seizure 7.6 release note. Paraben. [Online] Paraben Corporation. [Cited: 01 05, 2018.] https://www.paraben.com/downloads/release-notes/Paraben's%20DS%207.6%20Release%20Notes.pdf.
33. **Paraben_DS_V_7.6.** Paraben DS V-7.6 Release Note. Paraben.com. [Online] [Cited: 01 05, 2018.]

https://www.paraben.com/downloads/release-notes/Paraben's%20DS%207.6%20Release%20Notes.pdf.

34. Android Phone Forensic: Tools and Techniques. **Roy, Nihar Ranjan, Khanna, Anshul Kanchan and Aneja, Leesha.** s.l. : International Conference on Computing, Communication and Automation (ICCCA2016), 2016, International Conference on Computing, Communication and Automation, pp. 605-610. ISBN: 978-1-5090-1666-2/16.
35. **Landsborough, Jason.** EXAMINING ANDROID PRIVACY USING DIGITAL FORENSICS. Department of Computer Science, California State University, Sacramento. Sacramento, California : Department of Computer Science, 2013. pp. 1-78, A Project Report.
36. **NIST, MOBILedit.** MOBILedit Forensic v7.8.3.6085, Test Results for Mobile Device Acquisition Tool. Department of Homeland Security Science and Technology, National Institute of Standards and Technology. USA : Homeland Security Science and Technology, 2015. pp. 1-16, Test Results for Mobile Device Acquisition Tool, MOBILedit Forensic v7.8.3.6085.
37. Android Anti-Forensic: Modifying CyanogenMod. **Karlsson, Karl-Johan and Glisson, William Bradley.** s.l. : Hawaii International Conference of System Science, 2014, Hawaii International Conference of System Science, pp. 4828-4837. DOI:10.10.1109/HICSS.2014.593.
38. Novel Anti-forensics Approaches for Smart Phones. **Azadegan, S., et al.** s.l. : 45th Hawaii International Conference on System Sciences, 07 05, 2012, 45th Hawaii International Conference on System Sciences, pp. 5424-5431. DOI 10.1109/HICSS.2012.452.
39. **ViaExtract.** introducing-the-new-viaextract. nowsecure.com. [Online] NowSecure, Inc. [Cited: 01 05, 2018.] https://www.nowsecure.com/blog/2014/01/13/introducing-the-new-viaextract/.
40. **XRY.** XRY. msab.com. [Online] MSAB, Inc. [Cited: 01 05, 2018.] https://www.msab.com/products/xry/.
41. **XRY_7.0.** xry_7.0_release_notes. Cyber Forensic and Investigation. [Online] 04 25, 2016. [Cited: 01 05, 2018.] http://www.cfi.co.th/xry-forensic.html, http://www.cfi.co.th/uploads/1/0/6/0/10606523/xry_7.0_release_notes_en.pdf.