Android Forensic Capability and Evaluation of Extraction Tools

VIJITH VIJAYAN

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
Authorship Declaration

I, Vijith Vijayan, confirm that this dissertation and the work presented in it are my own achievement.

Where I have consulted the published work of others this is always clearly attributed;

Where I have quoted from the work of others the source is always given. With the exception of such quotations this dissertation is entirely my own work;

I have acknowledged all main sources of help;

If my research follows on from previous work or is part of a larger collaborative research project I have made clear exactly what was done by others and what I have contributed myself;

I have read and understand the penalties associated with Academic Misconduct.

I also confirm that I have obtained informed consent from all people I have involved in the work in this dissertation following the School's ethical guidelines

Signed:

Date:

Matriculation no:
Data Protection Declaration

Under the 1998 Data Protection Act, The University cannot disclose your grade to an unauthorised person. However, other students benefit from studying dissertations that have their grades attached.

Please sign your name below one of the options below to state your preference.

The University may make this dissertation, with indicative grade, available to others.

The University may make this dissertation available to others, but the grade may not be disclosed.
Abstract

Smart phones are one of the most troublesome technologies that exist today and steadily gaining popularity with better connectivity, functionality and productivity. The ever-increasing complexity of these smart phones gives a new level of threats. Android is one of the newer operating systems based on smart phones, is emerging as a significant force within the highly competitive smart phone market. Android phones stores an enormous amount of data that can be stored locally or remotely and allows forensic analysts to acquire these data and evidence, collecting this valuable information with regard to the investigation. There are number of forensic tools both open source and closed source are available in the market for the purpose of extracting data from the Android devices.

The key focus of this project is to evaluate the performances of extracting tools that support the Android phones. This research project reviews the literature in the field of digital forensic and methods of retrieving data and discusses the criteria and methodology to be achieved for a meaningful evaluation. Three different software tools are evaluated along with the manual method of extraction on two Android phones. The actual forensic data within the mobile devices were identified and counted. All the three software tools were tested on both phones, to find out how much data can be extracted and these results were compared and evaluated based on the actual data on the phones.

The conclusion made in this research emphasises the fact that the evaluation results were the ones expected, confirming that the methodology and criteria used to evaluate the tools are correct.
List of Tables

Table 4.1: Android Phones specification
Table 4.2: Actual data on both mobile phone
Table 5.1: Oxygen Forensic extracted data
Table 5.2: Extracted data with MOBILedt forensic
Table 5.3: Actual data vs. AFLogical
Table 5.4: Result from the manual searching for data

List of Figures

Figure 2.1: Android Architecture
Figure 2.2: Partition Information of an Android device
Figure 2.3: shared_pref folder under Application data
Figure 2.4: Forensic Tool Analysis Pyramid
Figure 2.5: Tool Assessment
Figure 3.1: Connecting Android with ‘adb’ and rooting into shell
Figure 3.2: Data map
Figure 4.1: HTC Desire S and HTC Sensation XE
Figure 4.2: Oxyagent extracting data from the mobile
Figure 4.3: Thumbnails extracted from Phone #2 shown in Oxygen forensic
Figure 4.4: Installing AFLogical through ADB
Figure 4.5: AFLogical OSE in the application list after adb push
Figure 4.6: FTK Imager is loaded with dd image of Android SD Card
Figure 5.1: Comparative graph on actual data vs. extracted data by Oxygen Forensic taken from Phone 2.
Figure 5.2: Oxygen forensic report showing ‘Section was not read’ under Messages
Figure 5.3: Actual data vs. MOBILedt data
Figure 5.4: Actual data vs. AFLogical
Figure 5.5: Actual data vs. Manual extraction
Figure 5.6: Percentage artifacts extracted by Oxygen Forensic
Figure 5.7: Percentage artifacts extracted by MOBILedt Forensic
Figure 5.8: Percentage artifacts extracted by AFLogical
Figure 5.9: Overall percentage of extraction by individual extraction tools with respect to Actual forensic artifacts
Figure 5.10: Percentage artifacts extracted by Manual method
This research has been conducted under the direction of:

Mr. Robert Ludwiniak, Lecturer

And

Mr. Greg McCara, Lecturer
Second Supervisor
Acknowledgements

I would like to show my gratitude to Mr. Robert Ludwiniak for acting as my supervisor for this work and all the help and guidance he provided.

I also thank Mr. Gregg McCara for acting as my internal supervisor for this thesis.

Finally, thanks go to my family who has been a constant support throughout this course of work.
## Contents

**Abstract** ......................................................................................................................... 4

**Acknowledgement** ............................................................................................................ 7

1 **Introduction**
   1.1 Context ....................................................................................................................... 10
   1.2 Aims and Objective ................................................................................................... 10
   1.3 Background ............................................................................................................... 11
   1.4 Thesis structure ......................................................................................................... 12

2 **Literature Review**
   2.1 Introduction ................................................................................................................. 14
   2.2 Mobile Devices ............................................................................................................ 14
      2.2.1 Types of Evidences .............................................................................................. 15
      2.2.2 Mobile Forensics ................................................................................................ 15
      2.2.3 Challenges .......................................................................................................... 16
      2.2.4 Forensic Best Practices ......................................................................................... 17
   2.3 Android ....................................................................................................................... 19
      2.3.1 Android Architecture ........................................................................................ 20
      2.3.2 Android File Systems ......................................................................................... 24
      2.3.3 Android Data Storage ........................................................................................ 25
   2.4 Extraction Tools ......................................................................................................... 26
      2.4.1 Method of Extraction ......................................................................................... 27
      2.4.2 Evaluation Criteria .............................................................................................. 28
      2.4.3 Testing and Validation ......................................................................................... 30
   2.5 Summary of Problem Area ......................................................................................... 30
   2.6 Conclusion .................................................................................................................. 31

3 **Methodology**
   3.1 Introduction ............................................................................................................... 32
   3.2 Methodology .............................................................................................................. 32
   3.3 Design ......................................................................................................................... 35
      3.3.1 Design Phases ..................................................................................................... 35
   3.4 Data Collection .......................................................................................................... 37
   3.5 Conclusion .................................................................................................................. 38

4 **Implementation**
   4.1 Introduction ............................................................................................................... 39
   4.2 Testing Implementation .............................................................................................. 39
      4.2.1 Testing Environment ............................................................................................ 41
   4.3 Tool Testing ............................................................................................................... 42
   4.4 Conclusion .................................................................................................................. 46
5 Evaluation
5.1 Introduction ................................................................. 48
5.2 Evaluation of Tools. .......................................................... 48
5.3 Comparison ................................................................. 53

6 Conclusion
6.1 Introduction ................................................................. 58
6.2 Meeting the Objectives. ..................................................... 58
6.3 Critical Analysis ............................................................. 60
6.4 Future Work ................................................................. 61

References ................................................................. 62
Acronyms ................................................................. 65
Appendix A ................................................................. 67
Appendix B ................................................................. 68
Appendix C ................................................................. 69
Appendix D ................................................................. 70
Project management .......................................................... 71
INTRODUCTION

1.1 CONTEXT

Today's Mobile devices have transformed from simple voice communication equipment to sophisticated communication devices with the capabilities of computer and far beyond. Smart phones are the devices with the capabilities of a phone and computer. Along with the latest advancements in wireless technologies and the popularity of Internet, mobile phones have revolutionised the modern communication in such a way that these devices replaced traditional wallets that people carry without fail. According to the telecommunication giant Ericsson global mobile penetration reached 85 per cent in 4th Quarter of the year 2011 and mobile subscriptions now total around 6 billion (Ericsson, 2012).

New technologies and innovations have led new intelligent smartphones with different operating systems capable of doing multiple complex tasks. One such mobile platform is Android Operating system. Android is an open source mobile device platform managed by Open Handset Alliance (OHA). OHA is a consortium led by Google and other industry leaders to develop open standards for mobile devices. Android-based smart phones became so popular among the mobile users in a short span of time and it already positioned as the largest market share in the mobile operating system market (Gartner, 2011).

Mobile phones become a very useful device in people pocket but at the same time it also became a tool for criminal activities. The newer features like location aware, GPS, Bluetooth hacking becomes easier way for criminals to reach out and launch sophisticated criminal activities. Criminals can remotely install the rootkit on mobile phone operating system and can access all the area of the phone including the touch screen and keypad. For example, organised criminal group can easily re-route a customer's phone call to his bank to crime gangs own spoofed call centre and can have access to the victims bank details and could use it to get away with the all money from the account. According to noted security expert Bruce Schneier warned in his blog that a mobile phone can be
turned into a microphone and transmitter for the purpose of listening to conversation of the phone (Schneier, 2006). This indicates that the criminals can remotely access the user's phone and they can operate and continue to maintain their criminal activities as long as they want.

Android forensic is part of digital forensic offers many opportunities and challenges. By looking at the volume of newer android devices and the misuse of these devices by criminals presented challenges how effectively extract and analyse the data for forensic purposes. A very detailed understanding of both the platform and forensic tools are required for acquisition and analysis of mobile data. There are numerous tools on making smart phone forensics easier. This research project evaluates the leading tools available in the market that support Android devices against its ability to extract and analyse the data on multiple parameters.

1.2 BACKGROUND

There are numerous tools available for the digital forensic that involves computers and other digital devices and become industry standard such as EnCase and FTK. But these tools lack the ability to extract the data from the mobile devices as mobile data is highly volatile and it is often easily altered. Data is information that has some value and these data holds lots of evidential value for a forensic investigator. Till now there is no standard method on how the data can be extracted from a mobile devices. Forensic investigators face enormous difficulties when dealing with mobile-based crimes because of its intrusive nature. Data in the mobile phone can be easily modified or even completely wiped out by people who have some knowledge. It is also challenging that these mobile phones stores more data that is well enough to prove the criminal activity originating from the mobile phones.

1.3 AIMS & OBJECTIVE

There are many tools both commercial and open source for the smart phone forensic evaluation, but there is no standard method for the analysis process. It is crucial for these softwares should posses a minimum level of effectiveness when dealing with a forensic analysis. By evaluating these tools it is possible to find the effectiveness of these tools with various parameters. The main aim of the project
is to evaluate the extraction tools that are advertised to support Android phones. The objectives to support the aim are

- To investigate and review the literature in the field of Mobile device forensic specific to Android forensic
- Identify and review the best practices currently in use for mobile forensics
- Determine the measurable criteria and desired outcomes required of Android Forensic tools
- Develop a methodology for evaluating the forensic tools for android devices
- Critically evaluate the tools based on the methodology against the actual forensic data identified from the Android phones.

1.4 THESIS STRUCTURE

Chapter two involves a review of literature in the area of Android forensic. Literature is reviewed in this chapter to form a background research for the whole project. The first area of the literature is reviewed on how Android platform transformed into powerful smart phones. A detailed research of the internals of Android platform is also carried out. This is extremely important when considering the Android forensic. The chapter discusses Android architecture, supported hardware and device types, boot process, various releases. The chapter also covers Android Software Development Kit (SDK), the Dalvik Virtual Machine (DVM). The chapter outlines the information related to how data is stored in the Android devices and file systems. This chapter also discusses in detail on various forensic techniques and challenges faced by the forensic examiners during a forensic investigation. Chapter two concludes with a summary of problems areas identified in the literature that are discussed earlier in the chapter.

In Chapter three discusses the methodologies that can be used in this project based on the various researches discussed in the Chapter two. Chapter three reviews three similar researches on forensic tool testing and the methodology adopted in their study. Based on the methodology and literature review four research phases are created. A detailed forensic process has implemented so that this could help to find how the data can be collected, analysed and processed for the implementation of the next phase of the project.
Chapter four outline the implementation of the forensic tool testing based on the forensic artifacts that can be extracted from the mobile device. Implementation of the testing environment for the tool testing is described in this Chapter. Four different tools were tested with the forensic artifacts extracted from the two mobile phones described in detail. The chapter also discusses the data collection and analysis for the evaluation of the tools.

The chapter five is Evaluation of the results that were taken from the implementation stage. The chapter discusses the graphical representation data collected from the implementation. The chapter concludes by recommending possible areas for future study.

The final and sixth chapter is Conclusion. This chapter discusses the resulted objectives from this research project describing each objective and how the objectives are achieved. A critical analysis of the whole project is done and outlined and possible future work that can be carried out by taking forward from this research.
LITERATURE REVIEW

2.1 INTRODUCTION

This Chapter is mainly focused on the literature review to establish a contextual basis for this thesis as a whole. Literature review starts off with the Android platform detailing the architecture. This chapter starts off with brief background on mobile devices, mobile forensic and types of evidence that can be collected from mobile phone. Section 2.3.2 also reviews literature on challenges while doing the investigation process especially acquiring data. The section 2.4 outlines various forensic techniques adopted by the investigators and number of studies conducted in this area. A detailed review of these studies has conducted and the best practices currently in use. The section 2.5 through 2.6 discuses the Android platform, android files system and various methods used to storing data with inputs from research studies. Section 2.7 is about the extraction tools that going to be evaluated in this project. Section 2.10 discuses the problems identified from various researches and to plan a basis for the design and Implementation.

2.2 MOBILE DEVICES

Mobile phones have become an integral part of peoples’ day-to-day life. Mobiles are used in all sorts of communications such as making calls, sending text messages, sending emails, connecting with friends and family through different social network or instant messaging applications. Mobile phone usage is not limited to basic communication but also heavily used in mobile banking, airline check-in, buy/sell products from various online auction sites, navigating the location, watching movies/videos real time and many other features. It was simply impossible to think the explosive growth of these intelligent devices few years back. There are different models of mobile devices and sub classifications like PDAs, handheld devices, eBook readers and smart phones etc.

Android-based smartphones are hybrid device capable of doing the job of a mobile phone and a computer but in a portable way. The explosive growth of
newer intelligent smart phones based on Android and IOS platforms are also initiated brand new methods of criminal activities. These devices carry large amount of data, which are, not limited to just call logs or text messages, but information regarding many other aspects of usage, behavior or other activities. The researches focused in the area of mobile device forensic increased momentum by seeing the value of data stored in these mobile phones.

2.2.1 Mobile Forensic

“Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods” (Wayne Jansen, Guidelines on Cell Phone Forensics, 2007)

There are a number of research have been conducted in the field of Mobile forensics and some are related to Mobile forensic in general and some are specific to Android and iPhone Forensics. Forensic can be done in many ways on GSM phones but this report mainly focused on the area of Android forensics. The growing number of feature rich phones makes it difficult to create a single forensic tool or standards specific to one platform. Digital evidence in Mobile device is easily susceptible as newer data can be easily overwritten or remote commands it receive from the wireless network. Mobile phones uses flash memory to store data. The advantage of flash memory is that it can sustain against impact, high temperature and pressure and making it more difficult to destroy. From a forensic perspective this is good as they can contain deleted information even after an individual attempted to destroy the evidence. The write life cycle of a flash memory is limited and data can be erased by block by block. Mobile devices erase data only when one block is full. Casey et al. describes why mobile devices are an excellent source of digital evidence and provide great insights that are not available on other devices. Additionally the personal nature of the device make it easy to establish the last mile evidence required to tie a device to an individual (Turnbull, 2011).

2.2.2 Types of Evidences

In Mobile device forensic the data extracted from the mobile phones are of probative in nature. These evidences are the corner stone when probing an investigation by the law enforcement agencies. There are number of evidences
that can be extracted from mobile phones. Punja & Mislan (2008) summarises types of evidences that can be extracted from mobile phone are contacts, call logs, test messages, audio files, email and internet history. These artifacts can be extracted in logical or physical methods. Logical is extracting data from the file system by directly interacting device with some special tools. The softwares or tools that extract these artifacts (or evidences) are limited. So forensic examiners find it difficult to execute this job in a timely fashion (Shafik G. Punja, 2008).

SIM (Subscriber Identity Module) is an essential part in the mobile phone. This small chip inserted into the mobile phone holds another place to acquire data. There are some special tools like SIMbrush is used for the purpose of extracting data from SIM. Casadei, et al., discuss how SIMbrush can be used to extract data from a SIM Card. The paper outline why the SIM card analysis is very critical piece of investigation as there is a univocal relationship between the user and his handset, and this is very interesting from an forensic analyst point of view (Fabio Casadei, 2005).

2.2.3 Challenges

Though the penetrations of mobile phones are increasing in large scale outnumbering the PC sales, the mobile forensic is still lags behind the digital forensics. The data acquired from mobile phones continues to be used as potential evidence in civil, criminal cases and even high profile cases (Aljazeera, 2005). However there is still a lot more to do in the field of mobile forensics as no common framework or a standard exist to acquire and analysis of mobile phone data. Forensic professionals often faced with challenges trying to extract evidence from a mobile device mainly due to the fact the small form factor that makes mobile devices so portable. Android mobile forensic tools and toolkits are still immature in dealing with the advances in mobile phone technology. The toolkits are not independently verified or tested for the precise forensic readiness. The developers of forensic tools are using different methods to gain access to memory on the mobile phones (McCarthy, 2005). Because of this most tools are limited to minimal number of handsets supported.

In forensic one of the area forensic professionals looks for evidence is the memory. If a user upgrades the new version there are chances that the memory will be overwritten losing potential evidence from the phone. The primary task of a forensic analyst is to create an exact copy of the device by using cryptographic hash function. But in the case of a mobile phone the hash values (MD5) tend to
change and the integrity of the copy will be in a question. The hash values will change each time when the mobile is switched on or off (Paul Owen P. T., 2010).

Mobile phones now days have better connectivity options that provides whole new world of communication possibilities. It also closely integrated into people lives in such a way that a person may virtually cut off from his peers or from the rest of the world if he missed this gadget. The traditional crimes are migrating to mobile phones and because of its sophisticated nature the criminals can easily modify or even simply wipe out every piece of information poses great challenges for forensic community.

2.2.4 Forensic Best Practices

Forensic analysts employ different techniques to extract the data out of the device like logical and physical techniques. There are a number of ways that will benefit from the results of an Android forensic investigation. But each may require different procedure and documentation. The first situation is that people think of in general investigations that are to be presented in civil court or criminal court of law. There are internal investigations in corporations that may end up litigated in courts and often used to determine the main cause of an issue. Countries now days face the hack attacks or other malicious hacktivism that threaten the very existence of their citizens well being. Forensic can play a critical role in thwarting attacks against a country by providing a valuable intelligence needed for their governments.

Mobile forensic also involves the same methods of the normal forensic investigation. There are some best practices that need to be followed. Though there are not much standardised format of investigation in mobile forensic the methods of investigation involved is more or less same as digital investigation. The phases of investigation processes that normally follow are (Wayne Jansen, Guidelines on Cell Phone Forensics, 2007)

- **Collection**: This is the first and foremost step involved in the investigation. The main purpose here is to collect the potential sources of evidences like mobile, SIM card and other accessories.
- **Identification**: This is focused on the recognition by labeling the potential sources of digital evidence.
- **Acquisition**: This is mainly involved in the extraction of data or potential evidence from different sources that have been captured.
• **Preservation:** One of the important steps involved in the investigation is preservation of evidence where adequate measures should be taken to secure the integrity of the evidence.

• **Examination and Analysis:** It involves searching, filtering, examining and evaluation of evidence.

• **Reporting:** As like any digital investigation reporting is the final part of documented proof of conclusive evidence.

Forensic investigation is a complex process where each and every step of the forensic analyst is very crucial for the preservation of evidence from the target device whether it is a computer or a mobile phone. But having its own removable storage on the computer it is fairly easy to dump or completely remove that specified hardware, but because of its small form factor and the complexity of keeping the hardware in a small area the forensic analyst faces more difficult task in order to acquire the image from the mobile phones. For example in order to acquire the forensic image of a desktop is fairly easy by removing the hardware, connect the physical write blocker and acquire bit-by-bit forensic image of the hard drive. The investigation can take place on the image and the original device would remain unchanged. But again the there are high chances of evidence loss while computer is in operation. Even a simple power on or power off will erase the contents of RAM. Mobile devices like Android devices are nearly impossible to forensically analyse without any changes to the device. Unlike desktop or notebook computers the storage part of the Android device cannot be easily removed and if the device is powered on or shutdown of the device again changes the device.

As different forensic examiners approach differently how the data must be acquired there are clearly some deep divide in the forensic community. The Association of Chief Police Officers (ACPO) in United Kingdom produces guidelines called as ‘Good Practice Guide for Computer Based Electronic Evidence establish four principles for mobile phone evidences (ACPO)

• “No action taken by law enforcement agencies or their agents should change data held on a computer or storage media, which may subsequently be relied upon in court.

• In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
• An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
• The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to" (ACPO).

These guidelines provides a clear advise on how to act when dealing with mobile phone investigation. As in the case of UK ACPO guidelines the United States also had issued their own guidelines for the Cell phone forensics. In the US, these are issued by NIST (National Institute of Standards and Technology). Special Publication 800-101, Guidelines on Cell Phone Forensics (Wayne Jansen, Guidelines on Cell Phone Forensics, 2007). The ACPO guidelines propose strict guidelines on procedures and practices. The NIST publication is however for to improve the field of mobile devices forensics and not a guide for how law enforcement should handle mobile devices during an investigation. But ACPO lacks the guidance in defining how law enforcement should handle mobile devices during investigations. Both these guidelines lack the primary concerns of mobile forensics as mobile devices are constantly evolving and their features becoming more ubiquitous (Paul Owen P. T., 2011).

2.3 ANDROID

“The term “Android” has its origin in the Greek word andr-, meaning “man or male” and the suffix -eides, used to mean “alike or of the species”. This together means as much as “being human” " (Speckmann, 2008).

According to Pew Research center, one of America’s think tank organisation reports number of desktop owners declined and people are depending more on mobile phones and tablets (Janna Anderson, 2010). Todays smart phones are evolved from the conventional wired telephone system. Apple’s first smart phone iPhone became one of the best ever designed smart phone with its ease of use, portability and great computing power that no other company couldn’t make it. Apple iPhone’s operating system IOS is proprietary and Apple has got great control on the devices whoever use it. To break this code Google acquired a small company called Android who is involved in the developing of mobile operating system. Google along with leading companies under the umbrella of
Open Handset Alliance (OHA) started to develop an open source Linux based operating system. Google launched the first mobile phone called G1 based on Android after an year. From there onwards Google released several new versions of Android with new features and improvements.

There are several version of Android in the market and the latest Android version is version 4.0 code named as Ice Cream Sandwich (ICS). Android already made its mark being the fastest growing mobile platform. Gartner reported the worldwide smart phone sale with Android topping the market with 50% market share way ahead of all the other mobile platform (Gartner, 2011). This is a clear indication of how Android based devices are capturing the markets of other mobile platforms.

2.3.1 Android Architecture

The beauty of Android design is its compatibility with wide range of hardwares. This is achieved mainly due to its Linux kernel which in fact famous for its compatibility to many different hardware platforms. This is the feature that allows the manufacturers freedom to design the devices according to their requirements. But the fact is that the flexibility of Android is big challenge for a forensic investigator. So the understanding of the Android internals and the architecture is at most important. Android platform is keep changing with the time. Though these changes effectively change the architecture also but there are core components that are static any time. The Android architecture (Figure 2.1) consists of a software stack, which combines an operating system, middleware and application framework. The software stack is divided in four different layers. The basic of Android architecture is Linux kernel.
**Linux Kernel**

Linux 2.6 kernel is the core of the Android platform. Linux kernel is the hardware abstraction layer that controls the hardware and its resources. The kernel also controls process management, memory management, network management and power management and proven to be very stable. Kernel maintains various drivers for almost all of the hardwares (Hoog, Android Forensics, 2011).

**Libraries**

The next layer in the Android Architecture is the Libraries. The libraries are written in C/C++. The core power of Android platform is utilised through the
libraries like surface manager for composing different drawing surfaces onto the
screen. The openGL/ES and SGL makes the core of the 3D and 2D graphics and
the media framework constitute various media packs like MPEG, AAC, mp3, mp4
etc., SQL lite for the data storage, WebKit for the open source browser engine
and freetype for the font engine (Sayed Hashimi, 2010).

**Android Runtime**

Android Runtime built mainly to support its embedded environment with limited
CPU, battery and small screen. Dalvik machines run dex files that are byte code
converted from jar files. Dalvik machines are customized version of Java suited
in the small platform environment. Dalvik uses highly optimized CPU, data
shared to other applications such a way that there might be multiple instances of
Dalvik virtual machines at a given time. The core libraries are the all the java
libraries for all the classes (Ehringer, 2010).

**Application Framework**

Application framework is written in Java. This is toolkit that all the applications
uses be the application written by Google or the application written by the
developers. All the applications use the same framework and same APIs making
it simple to write applications. By looking all the components, the activity
manager manages the application life cycle. The package manager keeps track
of all the application presently in the device and updates if any new application
been downloaded and installed. Window manager manages the windows UI.
Telephony manager uses APIs that used to build the telephone applications,
content provider is unique that share the data across all the applications like
contacts are shared to all the applications. Location manager and notification
manager allow developers to develop new, exciting and innovative pieces of
applications.

**Applications**

Android comes with set of basic application like Contacts, Calendar, maps, SMS
app, Email client and browser. All of these applications are written in Java
programming language. These applications are multi tasking. All applications run
its own processes. Android provides a feature rich APIs for building innovative
applications. APIs like Location manager and XMPP (Extensible Messaging and
Presence Protocol) services gives developers ability to build applications. Notification manager APIs to build the notification related applications.

**Android SDK & ADB**

One of the important features available in the Android Software Development kit (SDK) is the Android Debug Bridge (ADB). ADB provides a communication interface to an Android system using a computer. A computer is able to access a command shell, install or remove applications, transfer files when connected through ADB interface (Android, 2012).

Access to system partitions is restricted to the Android operating system. By default, users do not have permission to access system reserved areas. This is mainly to prevent malicious or poorly developed applications to affect Android OS stability and reliability. But as a forensic point of view this may be a bad ideas, but yes, it is possible to get super user or root access to the system. A forensic analyst always looking ways to get into the internals of the system so getting access to the root is very important. Forensic analyst can make a copy of all the system partitions as well as access files that are not accessible by normal access. But again this depends on the device manufacturer and model and also invasive in nature.

The Android SDK not only provides deep insight into the Android platform but also provides powerful tools to investigate the device, from both a forensic and security viewpoint. Once the SDK is installed on a forensic workstation, the forensic examiner has the ability to interact with an Android device connected via USB, provided the USB debugging feature is enabled. The Android SDK is an important tool used for forensic and security analysis.

For a comprehensive forensic analysis the forensic investigator required to know the boot process of Android device. So like any other device Android also has fairly standard boot process that allows the device to load the required firmware, OS and user data into memory to support full operation. Mattias Bjornheden of the Android Competence Center at Enea described in detail how and what are the methods of Android boot process in his blog post (Bjornheden, 2009). In his post he identifies seven steps to Android boot process and they are

- Power on and on-chip boot ROM code execution
- The boot loader
The device components vary from one manufacture to another but a basic understanding of these components and device type is helpful for the forensic analyst for a clear and concise investigation.

Android updates are not a centralized repository of updates where users run the updates from a central server. Instead the updates are the responsibilities of the carriers or the network service providers. Google take full responsibility of managing the Android OS as whole and not the updates. For a forensic analysts perspective this is a bit troublesome in many ways. Firstly a forensic investigator is never certain what version of Android a device is installed. There are a number of versions of Android in the market and they vary in their features and the way the data stored. It is a troublesome experiences for forensic analysts that both securing and acquiring images from an Android device which are of different versions. For example the techniques they employ to copy the images from a T-Mobile G1 running Android 1.5 is different from the same device running Android 1.6 or the different kernel. This is imaginable as with more number of manufacturers with over 400 Android devices, six major releases and hundreds of minor releases the forensic analysis may vary vastly. Each manufacturer may have their own specific set of drivers and softwares.

2.3.2 Android File Systems

A file system is way to organise the data in an efficient manner. There are different file system for computers and mobile phones. The efficiency of a file system is weighed on how fast the application can read, write and retrieve data. Android is based on Linux file system and many of them used to boot and run the device. Android uses EXT, FAT32 and YAFFS2 file systems for booting, data storage purposes. Extraction tools use many methods to pull the data out of these file systems. FAT and FAT32 are popular file system used by windows operating system. Android supports these files system mainly in the SD Cards. Although these files system lacks the security of the files this is used widely. YAFFS2 (Yet Another Flash File System 2) a file system designed for flash memory. The problem with YAFFS is that most forensic tools available are not
compatible with this file system. But researcher Andrew Hoog pointed out that some Android handsets were already using EXT4. This is due to the support for the dual core processor and multiprocessing and to use external memory cards (Hoog, Android Forensics, 2011).

Vidas, et al., (2011) describes different partitioning used in Android devices but exact partitioning depends upon handset manufacturer. The typical scheme found in the Android device is shown in the Figure 2.2. There are normally six partitions found on Android devices, user data, cache, boot, and recovery. The YAFFS2 file system was designed for flash memory. Vidas, et al., outlines methods of collection by using recovery partition. This piece of information is very critical while doing the forensic analysis of a mobile device.

<table>
<thead>
<tr>
<th>Path</th>
<th>Name</th>
<th>File System</th>
<th>Mount point</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/mtd/mtd0</td>
<td>pds</td>
<td>yaffs2</td>
<td>/config</td>
<td>Configuration data</td>
</tr>
<tr>
<td>/dev/mtd/mtd1</td>
<td>misc</td>
<td>–</td>
<td>N/A</td>
<td>Memory</td>
</tr>
<tr>
<td>/dev/mtd/mtd2</td>
<td>boot</td>
<td>bootimg</td>
<td>N/A</td>
<td>Partitioning data</td>
</tr>
<tr>
<td>/dev/mtd/mtd3</td>
<td>recovery</td>
<td>bootimg</td>
<td>N/A</td>
<td>Bootable (typical boot)</td>
</tr>
<tr>
<td>/dev/mtd/mtd4</td>
<td>system</td>
<td>yaffs2</td>
<td>/system</td>
<td>Bootable (recovery mode)</td>
</tr>
<tr>
<td>/dev/mtd/mtd5</td>
<td>cache</td>
<td>yaffs2</td>
<td>/cache</td>
<td>System files, Applications, Vendor additions, Read-Only, Cache Files, User data (Applications)</td>
</tr>
<tr>
<td>/dev/mtd/mtd6</td>
<td>user data</td>
<td>yaffs2</td>
<td>/data</td>
<td>Crash Log</td>
</tr>
<tr>
<td>/dev/mtd/mtd7</td>
<td>kpanic</td>
<td>–</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

Figure 2.2 Partition Information of an Android device (Timothy Vidas, 2011)

2.3.3 **Android Data storage**

Android phones store more data than any standard phone. Android stores data in five methods. Forensic examiners looks for the data in four of the five formats.
The five methods of storing data are shared preferences, internal storage, external storage, SQL lite and network (Hoog, Android Forensics, 2011). Shared preferences allow a developer to store key-value pairs of primitive data types in a lightweight XML format. Shared preferences files are stored in an application's data directory in the `shared_pref` folder.

Android phones store much of the data in internal memory such as NAND flash. The files are stored in the applications `/data/data` folder (Figure 2.3). This folder can only be visible if a root (administrator) access has gained.

```
ahoog@ubuntu:~/data/data/com.google.android.apps.maps$ ls -l
total 24
drwxr-x-x 5 ahoog ahoog 4096 2011-01-18 03:42 app_
drwxr-x-x 3 ahoog ahoog 4096 2010-09-15 10:59 cache
drwxr-x-x 2 ahoog ahoog 4096 2011-01-23 10:30 databases
drwxr-x-x 2 ahoog ahoog 4096 2011-01-23 20:55 files
drwxr-x-x 2 ahoog ahoog 4096 1980-01-06 09:41 lib
drwxr-x-x 2 ahoog ahoog 4096 2011-01-24 04:13 shared_prefs
```

Figure 2.3 s shared_pref folders under Application data

SD Cards are normally used as external storage and loaded with FAT32 file system. FAT32 is widely supported but lacks any security mechanism like in ext3, ext4, yaffs2 etc.

SQLite is a popular database format appearing in many mobile systems. SQLite is very lightweight and its entire code base is of high quality and open source. The SQLite files are generally stored on the internal storage under `/data/data/<packageName>/database`. Network can be used to store and retrieve data.

### 2.4 EXTRACTION TOOLS

Mobile forensics is relatively new area of digital forensics and the software and tools required to extract data from the mobile phones are still at the nascent stage. Extraction tools can be hardware or software based depending on how the data is extracted from mobile device. There are a number of extraction tools available in the market today and newer tools are emerging with some innovative ideas. It is found that almost all tools are commercial ones and few number of open source tools. However procuring these tools found to be very difficult given the privacy and security issues and the cost involved. As physical extraction was
not considered in this project so the leading tool like Cellebrite UFED and XRY are omitted. Other leading tools like AccessData Mobile phone Examiner Plus (MPE+) and viaForensics ViaExtract found to be difficult to procure. The extraction tools being tested in this project are

**AFlogical**

ViaForensic AFlogical OSE is an open source tool to extract the data. This is lightweight software purely used in the command line. This tool utilises the Android adb feature to communicate with a computer.

**Oxygen Forensic**

Oxygen Forensic is one of the leading tools in the mobile forensic field with a wide range of phone support. Oxygen extracts most of the information in an efficient way. This tool has a well-defined reporting system so that examiner can read and verify minute details of the evidence collected.

**MOBILedit Forensic**

MOBILedit! Forensic tool allows examiners to acquire logically, search and examine the mobile phone devices. This tool uses multiple connectivity mechanism than other similar tools especially the wireless connectivity. The software is well enough to acquire the phone system information and other contacts and messages lists.

### 2.4.1 Methods of Extractions

Mobile phones lack the traditional hard drives like in computers making it hard for the examiner to extract the data. In most cases it is up to the examiner's discretion whether to take a note of the modification happened. Any alteration of target device has to be reported and kept aside for future reference with a detailed explanation why and how the alteration has happened.

Brothers (2009) outlined five phases of extraction from the mobile devices (Figure 2.4). As shown in the figure the levels are divided two ways and are physical methods which are more forensically sound extraction methods but high level of technical competency required (Brothers, 2009). The bottom most layers are the manual methods which involves manually reviewing a mobile device by
simple straight through process. Manual method of extraction is very simple to perform and almost all devices can be analysed this method. The problem with method is there are chances that the examiner may miss out some critical area of evidence like deleted items. This could be serious implication while submitting the evidence to the court. This method is only suitable in situations where integrity of data is not that much important and a very limited time to produce the evidence.

The next extraction method is logical. This is mostly recommended method of data extraction. This technique involves copying a small Android Forensic application to the device then removing from the device. ViaExtract is one such application from the company called ViaForensics, it extract following information

- “Browser history
- Call Logs
- Contact Method
- External Image Media (meta data)
- External Image Thumbnail Media (meta data)
- External Media, Audio, and Misc. (meta data)
- External Videos (meta data)
- MMS
- Organizations
- People
Logical extraction is quick to perform and not require a high level of technical expertise. The method is repeatable however still can’t be considered forensically sound as changes may be made to the data on the device during the coping process (Westman, 2009).

The next three layers are physical extraction methods. Physical extractions are more into technical in nature but provides sound forensic results. The first physical layer is hex dump. Hex dumping involves uploading an altered boot loader to the device and boot from the newly loaded bootloader. This method can create a forensically sound image. Hex dumping of a mobile device is similar to booting a computer from a boot CD and acquiring image of the hard disk while computer running. Hex dumping requires a high level of technical expertise as this is mainly interacting with the code level access of the operating system (Brothers, 2009).

The next layer is ‘chip-off’ and this technique is to remove NAND flash chips physically and examined externally. This technique mainly used when the device is damaged and in some cases to override the passcode-protected devices. This process is quite a destructive process and attempted as a last resort when nothing is worked mainly due to damage of the NAND chip during this process (Hoog, Android forensic techniques, 2011).

The final extraction method is micro read that requires the most technical expertise to perform. The micro-read method uses an electron microscope to view the state of the memory on the device. But this method involves huge costs and not used a standard method. (Knight, 2010)

2.4.2 Evaluation Criteria

Forensic examiners use the term ‘Forensically Sound’ when referring the forensic investigation. The main purpose of keeping the forensic evidences as forensically
sound so that the data collected from the devices should not lose its evidential value when using in the court. One of the main requirements of a forensic tool is to produce the evidences that are forensically sound. There are several criteria for evaluating the forensic tools. However these criteria may change depends how an examiner conducts the testing. Reliability and Completeness is the two most important qualities that must be checked when evaluating the forensic tools. If both of these in question the evidential weightage will be in question and eventually less chances that these can be proved in the court.

2.4.3 Testing and Validation

Ayers, et al (2007, P.11-16) outlined simple methodology to perform the analysis of the mobile devices. The steps are illustrated in Figure 2.5

![Figure 2.5: Tool Assessment (Ayers, et al, 2007, p.16)](image)

Ayers, et al (2007) followed some simple methods by acquiring a set of target devices and then followed a set of prescribed activities like placing and receiving calls was performed on each phone. After that the contents of the phone and associated SIM were acquired using an available tool and examined to determine whether the evidence of the activity is recovered as expected. Finally a report has been taken (Rick Ayers, 2007).

2.5 SUMMARY OF PROBLEM AREA

Android is fairly a new platform but growing very fast because of its intuitive and open nature of the architecture. The handset manufacturers have got the freedom to modify and this made them follow a successful business model. Along with this there comes the serious issues related to the criminal activities originating from these devices. Android forensic is still in its early stages of development and studies shows the tools that claims to support the extraction of data from the Android devices are still limited in capability. Section 2.7.1
discusses the methods of extraction however the extraction is still can be possible at the logical level. As like any phones Android devices also faces the small form factor limitation when comes to the forensic analysis. Examiners faces huge task to extract the data without any alteration to the target device. Forensic professionals tend to spend more time to understand how the tools work on different models of Android devices. They also need to verify the test data to ensure the result is expected or erroneous. There are both commercial and open source forensic tools available in the market but both of these tools not provide the ‘forensically sound’ extracted data. Other methods of extraction should be tested and compared to pre-packaged software so the best option is selected.

2.6 CONCLUSION

The literature review has defined mobile devices and smart phones and how the Android phones are part of the smart phones category. Getting to know the internals of the Android architecture is important aspect of the Android forensics. Literature review outlined the various mobile forensic techniques can be adopted when extracting the data from Android mobile devices. Though there are no standardised methods for mobile forensic as of now, the guidelines from ACPO and NIST would give an outline how the basic guidelines are practiced in the forensic investigation community. Android phones are powerful devices and the understanding of what these devices can do and what can be expected from forensic perspective. Android versions are continuously updating and because of that the extraction tools needs to be up to date.

The researches around the Android forensics are reviewed through out this chapter. More number of researches is focused on mobile forensics as a whole and a less number of them are mainly trying to simplify the forensic of Android devices. Different forensic techniques are reviewed and not all the methods are feasible in case of Android. The logical techniques are more appropriate forensic technique that can be employed by the examiner.
METHODOLOGY

3.1 INTRODUCTION

Chapter two provides a literature review relevant to Android architecture, and its capability against the extraction tools. The literature outlined various researches on Android forensics and the extraction methods currently employed by the various forensic tools. The key focus of this chapter is to select the most suitable methodology and to ensure the research goals are met. In order to select the right methodology a good deal of data collection is required. The chapter also discusses the data requirements, method of data collection and data analysis. Section 3.2 discusses three study that have conducted in the similar area which are adopted a completely different methodology while examining the mobile phones. Section 3.3 focuses on the research design and describes how the research can be carried out in the different phases of the research. The data collection and analysis is carried out to meet the research goal. These details are described in the section 3.4

One of the key tasks of a forensic examiner is to quickly extract all available data from the Android phone with minimal effort. Most of the commercial tools available in the market are falling short of meeting the forensic investigators needs. At the same time there are some open source tools that meets their requirement without much hassle. Forensic investigators adopt different tools and methodology to find the evidence that is forensically sound or probative. Though not all investigations are intend to produce the evidence in the court of law but forensic analyst performs the analysis with the anticipation of producing the forensically sound image.

3.2 METHODOLOGY

The large number of forensic tools for Android and other smart phones constitute a validation problem for Forensic examiners. The software vendors do not follow a common methodology or certain standard when employing the forensic case
studies. For an investigative perspective it is required that the evidence to be acquired as quickly as possible and to examine the evidence so that the law enforcement professionals can be defended their case in the court 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. So those investigative teams always look for simple but efficient tools that wont make much overhead for their chances of collecting and producing the evidence.

It is very important that a number of data are required when analyzing and evaluating forensic tools. The collection of data is critical part of android forensics, as this will evaluate the measurable objective that have identified in the previous Chapter. The output data must be visualized in order to evaluate the performance of the tools. This is important, as some of data extracted from the Android devices are the raw data, which are of no value when the time is limited so that the investigator tends to procure the software, which give him an efficient reporting system too. The data from the Android mainly constitute information like call logs, text messages, GPS data, browser history etc., as outlined in section 2.7.1 of Chapter 2. For a forensic examiner he looks for the maximum available information from the device including the current memory dump or cached files, and deleted files or images etc. Given the wide range of Android phones the extraction tools behave on extracting these data differently.

There are number of researches have conducted in the field of mobile forensic and some of the researchers outlined methodology to adopt in the case of mobile forensic as a whole. But a standardized method specific to Android devices has yet to come into effect. It is worth to note few of the researches, which adopted different methodology while performing the Android forensic. Kessler and Lessard (2010) discuss the methods to simplify the Android forensics. The methods adopted here is first by acquiring the image from the external data card by using FTK Imager tool. All the hashes are verified and placed separately so that the integrity of the image is preserved. Kessler and Lessard (2010) explain for Android forensic the analysis of the device and the external card must be employed separately. Extraction of data or imaging of external memory can be done by any forensic imager like creating an image of computer hard disk. Kessler and Lessard (2010) also explain the importance of rooting the Android (or simply getting access to the root (/) directory) so that forensic examiner can
jump deep into the android architecture. A program called AsRoot2 can be used to root into the android device as shown the steps.

```
> adb push asroot2 /data/local/
> adb shell chmod 0755 /data/local/asroot2
> adb shell
$ /data/local/asroot2 /system/bin/sh
# mount -o remount,rw -t yaffs2 /dev/block/mtdblock3 /system
# cd /system/bin
# cat sh>su
# chmod 4755 su
```

![Figure 3.1: Connecting Android with 'adb' and rooting into the shell](image)

Once rooted into the device dd command can be used to create the image of the memory. Examination of the memory dump is done by the FTK (Jeff Lessard, 2010).

Kubi. et al., took a different methodology to evaluate the forensic tools. This paper outlines the data objects as the evidential information from the device and these information matrices are compared with the two different Android mobile phones by leading forensic tools. This method uses the NIST Cell Phone Tool
Specification with a number of baseline parameters. Two separate forensic objects are created - core and optional. To get the clear picture of the evaluation clear visualized results are produced (Appiah Kwame Kubi, 2011).

Punja & Mislan (2008) took a different approach on Mobile device analysis. The common mobile communication technologies are discussed in length and evaluated according to their characteristics. There is clearly a distinction between smartphones and baseline devices. Punja & Mislan (2008) outlined the types of evidences that can be analysed and that include call logs, contacts, email, pictures and SMS. The research also discusses on how the evidence should be collected like if the device has been brought in for analysis or it found on scene the state (on or off) should be noted. If the device is on its date and time should be documented and find out any inconsistencies by comparing the actual date and time. If the device is off this process can be completed once the device is turned on. The location information can be collected from service provider and to be verified with the information from the device (Shafik G. Punja, 2008). The research follows a methodology that splits into three phases – investigating what information can be extracted, where this evidence can be copied, and how the analysis can be done. Punja & Mislan (2008) recommend how commercial tool testing can do the investigation in systematic methods. The research states that there is no tool that supports all the mobile devices and the future tools must be intelligent enough to extract the physical data.

3.3 DESIGN

The research design will focus on the methods selected for this study. A detailed literature review has been conducted and documented the processes involved in the forensic analysis and different methodologies are reviewed and compared with other researches, which are closely related to Android forensics. The key focus here is to evaluate the tools against the forensic matrix (or artifacts). The forensic matrix consists of contacts, call logs, SMS, MMS.

3.3.1 Design phases

In order to analyse and evaluate the forensic tools a sufficient amount of data need to be collected. To make it in a structured way the research design has divided into four stages. The first stage is to test the capability of Android phone. Android phones maintain a high level of security both kernel level and application level. Though this is a bad news for a forensic examiner there are number ways
the data can be stored and extracted. Apart from secure nature Android phones also store enormous amount of information related to system information, user data, application data, audio, video files etc. Evaluating what information can be stored on the internal memory, external memory or in the lightweight databases like SQLite. As mentioned in Chapter 2 literature review Android phones are highly volatile when retrieving this information especially from the memory.

The second step of the research involves the extraction tools testing. The extraction tools selected for testing are the industry leading tools. While acquiring some of these tools involves huge cost the test has been done with the lite version or open source version of the same tools with some of the features are not available. A testing environment has been created with Android Software development kit. Two different models of phones from the same manufacturer have been selected for testing. This is to make sure all the forensic tools should supported by the extraction tools. Not all forensic tools support the entire majority of Android phones from many different hardware makers. The forensic artifacts are counted and benchmarked. Each forensic tool has tested against this benchmark data.

The next step consists mainly to compare the extraction tools tested on phase two. The comparison has based on the baseline artifacts that manually counted from the phones. The tools tested here are either open source or restricted download. The comparison is also done with the cost involved in procuring the software if a commercial based tool is used against the free open source. While most open source tools are require expert examiner to figure out what could be done in the tool configuration when initiating a forensic analysis. The ranking of tools are quiet hard as there is no such benchmark can enforce on the tools that employ different methodology to extract data. Some of the tools extract the data from the SD card or eMMC card while others don’t extract any of the data from the image. The forensic analysis of this external memory card doesn’t face much problem for a forensic investigator as these cards are partitioned with either with FAT or FAT32. The techniques employ to analyse the external memories are same as like in the computer hard disk. To ensure the accuracy of the tool testing a manual method of extraction of phone has been conducted in this phase.

Final step involves the graphical representation of the data carved out from the mobile phones by the forensic tools. Each tool uses different methodologies to get the extraction done. The graphical representation can be the best way to evaluate and compare these extraction tools as the data stored in the Android
phones are enormous and it require more time to analyse and evaluate if done with the other way.

3.4 DATA COLLECTION

Data collection is an important part of the research. The testing and evaluation of the tools produces enormous amount of data. These data is important to analyse the forensic evidences. There are three sources of data for this research. The first phase of the project returns data which is of probative value to investigators and that needs to be analysed. These data provide the baseline for testing each of the extraction tools. The actual forensic evidence will be collected from each of the phones so that this can be compared with the artifacts that have counted manually. The third and final sources of data are the evaluation outcomes with respect to the baseline data. These data are the actual data for the purpose of the visual representation of evaluation and comparison.

The data collection and analysis has been done with asking main question and sub question. The main question is what is the capability of Android devices for a device analysis. Based on the several questions a data map has been created. The data map clearly identifies how data can be identified, collected and processed.
The final stage of the data analysis is the data presentation. The results of the data during each stage of the tool testing will be presented with countless data. A clear visual representation of the result has been converted to get the comparative results. The results are graphed in each stage of the testing.

### 3.5 CONCLUSION

The Android forensic is a complex process. This project involves testing the extraction tools against the pre-set forensic artifacts. The literature review provided a detailed understanding of the Android’s capability of storing data. The similar studies shows different researchers adopt different methodologies. However there are no acceptable methods of extracting data from the Android devices barring some specification by some industry bodies but that too focused on the investigative aspects of forensic examination. The research design provides a platform for the actual implementation of the Tool testing and evaluation and this will be explained in the next chapter.
4 IMPLEMENTATION

4.1 INTRODUCTION

This chapter describes the implementation of how the evaluation has been conducted in a timely manner. Forensic tools are continues to grow in parallel with the proliferation of more Android devices. Forensic examiners are interested in tools that provide the most accurate results with minimal time. The Section 4.2 explains how the testing implementation can be done. This section will take the detailed step-by-step method to set up a Testing Platform. Next section discusses the Forensic tools testing and evaluation of these tools based on the actual data identified from the mobile devices.

4.2 TESTING IMPLEMENTATION

The implementation of testing has been conducted in this stage. Three different extraction tools are tested on two Android phones (Figure 4.1). The forensic evidences (or artifacts) within the phone were initially counted and each tool was compared based on what artifacts it could find. A manual forensic extraction also evaluated along with this tools. The Android phones used in this purpose are HTC Desire S and HTC Sensation XE. HTC is one the top handset manufacturer based on Android platform. The reason to select HTC mobile phone is because of its reputation of supporting many different Forensic extraction tools. HTC Sensation XE is a new model and this is selected purposefully to test the effectiveness of the extraction tools on newer models. Both phones communicate with computer using ADB (Android Device Bridge) to push and pull data from the phone.
The forensic extraction tools that are going to be tested in this project are
1. AFlogical
2. Oxygen Forensic suite 2012 standard
3. MOBILedit Forensic

Along with these tools a manual method of data extraction also tried with FTK imaging and winhex for analyzing the image extracted from the SD Card. The tools tested here are mostly open source or the tools have been procured from manufacturer after communicating purpose of this experiment. Some of the leading forensic tools are not publically available or procuring costs are high so that these tools cannot be tested. These can be considered as reference points while testing each tool. While there are more number of reference data can be identified not all the tools can produce the results. The less number of artifacts are using because these can be quantified and compared. The reference artifacts used in this project are

- System information
- Contacts (phone contacts)
- Call logs (incoming, outgoing and missed)
• SMS
• MMS
• Images
• Audio files (including ring tones)
• Videos
• Calendar items
• Files (PDFs, Word, Excel, and PowerPoint and no txt, system files)
• Applications
• Browser Bookmarks

4.2.1 Testing Environment

A testing lab has been set up to test the tools. Forensic tools use lots of resources of the computer while performing the extraction. Keeping this in mind a powerful computer has been used for the forensic workstation. The forensic workstation was running Intel i5 processor with Windows 7 Professional and had 4GB of RAM and 250GB of hard drive. Android SDK has been installed in the forensic workstation with the latest Java update. One of the tools extensively used to communicate with the Android phone is ADB and this tool is also installed as part of the Android SDK. ADB is a powerful tool to push, pull and can also used to get to the very root level of the phone. All the mobile forensic testing tools are installed in this workstation. While viaForensic AFlogical and MOBILedit are fairly a straightforward process to install it took more time to install Oxygen forensic.

Phone models used in this project is of different versions of Android operating system. The two phone specifications are listed in table 4.1.

<table>
<thead>
<tr>
<th></th>
<th>Phone #1</th>
<th>Phone #2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Handset</td>
<td>Desire S</td>
<td>Sensation XE</td>
</tr>
<tr>
<td>Manufacturer</td>
<td>HTC</td>
<td>HTC</td>
</tr>
<tr>
<td>Model No</td>
<td>S5510e</td>
<td>XE Beats Audio Z751e</td>
</tr>
<tr>
<td>Platform</td>
<td>Android</td>
<td>Android</td>
</tr>
<tr>
<td>OS Version</td>
<td>2.3.3</td>
<td>4.0.3</td>
</tr>
<tr>
<td>Processor</td>
<td>768MB, Qualcomm</td>
<td>1.5GHz, Qualcomm</td>
</tr>
</tbody>
</table>

Table 4.1: Android Phones specification
The phone 1 has less number of artifacts while Phone 2 has extensively used and stored more data including browser history, cache, emails etc. No change has been made in both the phones after initial acquisition. However few data are populated on both the phones. Five new contacts and five text messages are created on both phones and deleted after few hours. The phones are kept as a forensically acquired device so it is disconnected from the network in order to keep the data intact till the testing has been completed. The forensic artifacts are identified from both the phones are listed in the table 4.2 below.

<table>
<thead>
<tr>
<th>Phones</th>
<th>Sys Info</th>
<th>Contacts</th>
<th>Call Logs</th>
<th>SMS/MMS</th>
<th>Images</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desire S</td>
<td>YES</td>
<td>190</td>
<td>357</td>
<td>64</td>
<td>6</td>
</tr>
<tr>
<td>Sensation XE</td>
<td>YES</td>
<td>134</td>
<td>441</td>
<td>50</td>
<td>284</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phones</th>
<th>Audios</th>
<th>Videos</th>
<th>Calendar</th>
<th>Apps</th>
<th>Files</th>
<th>Bookmarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desire S</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>61</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Sensation XE</td>
<td>64</td>
<td>6</td>
<td>15</td>
<td>124</td>
<td>27</td>
<td>5</td>
</tr>
</tbody>
</table>

Table 4.2 Actual data on both mobile phone

The forensic extraction capabilities of the tools are compared against the actual artifacts that are manually identified and counted.

### 4.3 TOOL TESTING

The implementation of testing of tools has been done one by one. Each of these tools follows different techniques to extract data from both the mobile phones. Throughout this chapter the HTC Desire is called as Phone 1 and HTC Sensation XE as Phone 2.

**Oxygen Forensic**

Oxygen forensic is installed in the forensic workstation with a registration key provided by the company. The version installed in the forensic workstation is standard version with some limitation on viewing timeline, instant messengers and apps. Oxygen forensic maintains a large number of USB drivers for almost all android phones. This software requires the mobile device to be in USB debugging mode while connecting to the computer.
Oxygen software installed a client application called Oxygen Agent in the phone external memory and this agent pulls all the data and the output has been shown in the computer.

Figure 4.2 Oxyagent extracting data from the mobile

Figure 4.3 Thumbnails extracted from Phone #2 shown in Oxygen forensic
The results of the whole process were exported into a PDF file. Oxygen also creates a folder with images (including thumbnails) and partial copy of SD Card. The version of Oxygen tested in this project doesn’t have timeline enabled so not able to provide a timeline analysis.

**MOBILedit Forensic**

A lite version of MOBILedit is downloaded from the Internet. The installation is completed with minimal efforts. Like Oxygen, MOBILedit too have the USB debugging mode enabled in the mobile phones. Phones can be connected in either direct cable or through wireless connection. This is a big advantage that some phones not able detect this software and can utilize this wireless connection. MOBILedit installs a small application in the mobile phones to pull the data. The data extraction is limited to contacts, call lists, messages and files. The screen captures of the MOBILedit showed in the Appendix.

**AFLogical**

ViaForensic AFlogical OSE is the next tool implemented on the forensic workstation. This tool is an open source version of AFLogical. The full version is only available to law enforcement agencies so the open source version of this tool is used in this project. This tool is the lightweight software and no graphical front end unlike the tools tested before. The Android phones were connected to the forensic workstation with USB debugging mode enabled. It is required to remove the SD card as ViaForensic warning that the contents may delete. So an empty SD card with no data inserted into the phone. AFLogical need ADB to communicate with the Android devices. ADB can found under the Android Software Development (SDK) on the forensic workstation. This tool is part of the SDK kit. The next step is to push the AFLogical package file (.apk file). To push the file into the Android device following steps are executed on the forensic workstation:

```
adb devices
adb install AFLogical-forensic.apk
```
Figure 4.4 Installing AFLogical through ADB

This command installs the AFLogical into the phone. This is verified by checking the applications list in the Android phone.

On the Android device, click on the AFLogical and select all the parameters and select click capture button. AFLogical created a folder called ‘forensics’ in the external memory card. The extracted information is stored as Comma Separated Values (CSV) formats and a file called info.xml file with detailed phone system information. All the artifacts are stored as CSV format. The application can be uninstalled from the phones using these commands

```
adb uninstall com.viaforensics.android
```
The original SD card is replaced. The Alogical version used in this project is of open source and a number of artifacts cannot be checked with this method.

**Manual Extraction**

A manual extraction method utilised in the final step of this research. Physical image of the SD card was obtained from both the mobile phones. FTK imager is used for imaging the SD card. Bit-by-bit copies of images are stored in the forensic workstation hard disk as a DD file.

![FTK Imager is loaded with dd image of Android SD Card](image)

The idea here is to find the system information from the images. Winhex is used for searching through dd image. Keyword search is done to find the OEM manufacturer name. A search for the deleted files have resulted no matching. The search has conducted for to find out the images, files, audio and video etc.

**4.4 CONCLUSION**

This chapter has shown the successful implementation of Tool testing platform. A forensic testing environment has set up before testing the tools. A benchmark has identified by manually collecting the artifacts from the mobile phones. This benchmark is tested against the data extracted by the forensic tools from two
different phones running different Android operating system versions. Tools tested here are of using different methodology to extract the data. While MOBILedit not supported in extracting the data from the SD card all other tools have. All of these tools except the manual extraction are either using an agent application to pull the data from the Android phones. It is not known how this effect the files stored in the SD Card, as this is potential in the case of a real forensic. The results from the testing of each tool are collected and this is compared and evaluated in the next chapter.
5.1 INTRODUCTION

This chapter provides an analysis of the results obtained from the implementation stage. A review of the results obtained by individual extraction tools and the actual data are detailed in section 5.2. The detailed data collected from each stage is converted into a graph so that the results can be read visually. The section 5.3 discusses the individual data extraction capacity and finally finds the best method for the data extraction.

5.2 EVALUATION OF TOOLS

During the implementation of forensic tool testing each tool is tested against actual forensic data. The benchmark raw data is the reference point for all the output resulted after the testing of tools on both the mobile phones. Each stage of the testing the results are noted and tabled. The reference data is shown in the table 5.1

**Oxygen Forensic Evaluation**

The extracted data by Oxygen forensic tool is given below.

<table>
<thead>
<tr>
<th>Phones</th>
<th>Sys Info</th>
<th>Contacts</th>
<th>Call Logs</th>
<th>SMS/MMS</th>
<th>Images</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desire S</td>
<td>Yes</td>
<td>190</td>
<td>375</td>
<td>NA</td>
<td>6</td>
</tr>
<tr>
<td>Sensation XE</td>
<td>Yes</td>
<td>1328</td>
<td>500</td>
<td>NA</td>
<td>596</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phones</th>
<th>Audios</th>
<th>Videos</th>
<th>Calendar</th>
<th>Apps</th>
<th>Files</th>
<th>Bookmarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desire S</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>NA</td>
<td>6</td>
<td>NA</td>
</tr>
<tr>
<td>Sensation XE</td>
<td>39</td>
<td>16</td>
<td>NA</td>
<td>NA</td>
<td>215</td>
<td>NA</td>
</tr>
</tbody>
</table>

Table 5.1 Data extracted by Oxygen forensic
Out of all the tools tested Oxygen forensic has given a standardised and visible results. Though it looks ambiguous while checking the extracted data - contacts and call lists shows more data than actual. The result produced were not only the phone book contacts but also the contacts from all the social networking sites Facebook, LinkedIn, and twitter. This is due to the accounts configured in the Android and all the accounts are synced with the phone book. Though the contacts had given 1328 the actual phone book entries were 134 in Phone 2. Oxygen also produced a large number of images. This is quiet huge number while comparing with the actual data identified. It is evident not all the images (thumbnails) are not counted and this is a slight variation from analyzing the data as a whole.

This figure 5.1, Comparative graph shows the percentage of Oxygen forensic findings against the actual data. The graph is based on the data extracted from phone 2, as the findings on phone 1 is more or less equal. An interested fact in the result is that Oxygen did not produce the SMS/MMS list. In the report it is mentioned as ‘Section not found’ (Figure 5.2). Large number image files also produced and this is because the software has counted all the thumbnails as images.
Figure 5.2 Oxygen forensic report showing ‘Section was not read’ under Messages

**MOBILedit Forensic**

The results of this tool have limited features enabled so it only produced the contacts, call logs, messages and files. While message logs are accurately reported a large number of contacts and call logs are missing from the output.

<table>
<thead>
<tr>
<th>Phones</th>
<th>Sys Info</th>
<th>Contacts</th>
<th>Call Logs</th>
<th>SMS/MMS</th>
<th>Images</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desire S</td>
<td>Yes</td>
<td>168</td>
<td>168</td>
<td>64</td>
<td>NA</td>
</tr>
<tr>
<td>Sensation XE</td>
<td>Yes</td>
<td>112</td>
<td>227</td>
<td>50</td>
<td>NA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phones</th>
<th>Audios</th>
<th>Videos</th>
<th>Calendar</th>
<th>Apps</th>
<th>Files</th>
<th>Bookmarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desire S</td>
<td>NA</td>
<td>NA</td>
<td>0</td>
<td>NA</td>
<td>14</td>
<td>NA</td>
</tr>
<tr>
<td>Sensation XE</td>
<td>NA</td>
<td>NA</td>
<td>0</td>
<td>NA</td>
<td>11</td>
<td>NA</td>
</tr>
</tbody>
</table>

Table 5.2 Data extracted by MOBILedit tool

The MOBILedit is sometimes unreliable while doing the extraction, and there is no export option enabled of this particular version. The graph below shows the variation from the actual data produced by MOBILedit.
AFLogical

AFLogical is the simplest tool out of all. There is no GUI front end and can be installed and run from command mode. The open source version of the AFLogical has support only on extracting contacts, call logs, SMS and MMS. The exported data is stored as simple to use CSV format. It also produced xml file with detailed system information. One of the requirement of AFLogical is to remove the victim’s SD Card and this is the reason this tool is omitting wealth of other information that can be extracted. How ever given the open source version of the original AFLogical it is highly likely all these option and more could be in the professional software but more details about this software is unknown.

<table>
<thead>
<tr>
<th>Phones</th>
<th>Sys Info</th>
<th>Contacts</th>
<th>Call Logs</th>
<th>SMS/MMS</th>
<th>Images</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desire S</td>
<td>XML</td>
<td>190</td>
<td>375</td>
<td>64</td>
<td>NA</td>
</tr>
<tr>
<td>Sensation XE</td>
<td>XML</td>
<td>134</td>
<td>441</td>
<td>50</td>
<td>NA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phones</th>
<th>Audios</th>
<th>Videos</th>
<th>Calendar</th>
<th>Apps</th>
<th>Files</th>
<th>Bookmarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desire S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Not Available/Not Supported</td>
</tr>
<tr>
<td>Sensation XE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Not Available/ Not Supported</td>
</tr>
</tbody>
</table>

Table 5.3 Data extracted by AFLogical.
The graph shows the AFlogical produced the accurate output on three artefacts but some of the system information is missing.

### Manual Extraction

Manually extracting data is not the same as the way the software does. This is in fact to create image (DD) of the SD card and then opened with a hex editor and searched for various keywords. This is mainly to find out images and files. More number of images found when manually searched. The actual data is varied while manually searching for the images and files.

<table>
<thead>
<tr>
<th>Phones</th>
<th>Sys Info</th>
<th>Contacts</th>
<th>Call Logs</th>
<th>SMS</th>
<th>MMS</th>
<th>Images</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desire S</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>6</td>
</tr>
<tr>
<td>Sensation XE</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>556</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phones</th>
<th>Audios</th>
<th>Videos</th>
<th>Calendar</th>
<th>Apps</th>
<th>Files</th>
<th>Bookmarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desire S</td>
<td>1</td>
<td>0</td>
<td>NA</td>
<td>NA</td>
<td>0</td>
<td>NA</td>
</tr>
<tr>
<td>Sensation XE</td>
<td>64</td>
<td>6</td>
<td>NA</td>
<td>NA</td>
<td>3</td>
<td>NA</td>
</tr>
</tbody>
</table>

Table 5.4 Result from the manual searching for data.
5.3 COMPARISON

Forensic extraction tools produce large amount of data and comparing the results is a tedious process. Graphical representation of the results is used in this section in order to simplify and visually see without looking at the numbers. A percentage has taken by each artifact against the actual artifacts. The Figure 5.6 to Figure 5.10 shows the each of the forensic tools percentage and graphed. For example in the case of Oxygen forensic, the contacts, calls logs, Images, files and system information are all extracted above the actual artifacts identified making 100% data extracted on those particular artifacts. But Audio files extracted by Oxygen are 39 files against the actual audio data of 64. So Oxygen forensic tool has extracted 60% (39/64 X 100) of the total audio artifacts. Oxygen forensic has more percentage of data extraction capability than any other tools in this scenario.
MOBILedit has miserably failed to extract large number of artifacts like images, audio, video, calendar, apps, files and bookmarks. Though it can produce the contacts, call logs and messages, there are several contacts and call logs are missed making it the least performed extraction tool.
AFLogical is accurate in displaying the contacts, call lists, and messages in a nice readable csv format. However no further support for other data.

![Graph showing percentage artifacts extracted by AFLogical](image)

**Figure 5.8 Percentage artifacts extracted by AFLogical**

Manual extraction of data is not resulted the expected outcome. Searching of keywords is resulted no image files and documents. SD card mainly used to store Photos and audio files. So it is expected that finding too many of these forensic parameters is highly unlikely in the case of Manual extraction of SD Card. This method is most time consuming effort out of all mainly due to creating the images of both SD cards.
The final part of this evaluation is to find the most effective forensic tool in this context. The tools behave differently on different phones and may have different outcomes. From all of these artifacts the total percentage of data extraction has been calculated by adding all twelve individual artifacts and divided by the total number of artifacts. This has been graphed along with the actual data. The resulted graph is shown in Figure 5.10. So from the graphical representation Oxygen Forensic was extracted most data. Though Oxygen forensic is more effective it behaved slightly differently while extracting the SMS/MMS messages. It is unknown how this is omitted.
Fig 5.10: Overall percentage of extraction by individual extraction tools with respect to Actual forensic artifacts

Analysing the result above Oxygen forensic able to extract 45% of the actual data and AFLogical extracted around 25% while MOBILedit barely grabbed just above the 20% of the data. Oxygen forensic took more time to extract the data and AFLogical was quick to extract the data. However AFLogical is don’t extract all the artifacts. While looking at this scenario it is also noted that none of the tools are exceptionally performed to get the most data out of the two phones. While these all the tools tested in this project followed different methods to extract data there are also other factors like cost and time should decide the overall effectiveness of a forensic tool. Most forensic softwares cost more and the mobile forensic tools are no exception to this. The scenario may completely change if professional version of AFLogical has used so as MOBILedit pro version. So this method can be used as one of the method to evaluate the tools.
6 CONCLUSION

6.1 INTRODUCTION

This research project has focused on evaluating the efficiency of software tools that support the extraction of information stored on two Android Mobile phones. Three leading software tools were chosen for evaluation. The baseline data found on the mobile phones have identified and counted manually. All the tools were tested on both the mobile phones by extracting the data. The result taken from each one of these tests were matched against the baseline data and compared. The results of these evaluations were shown in the previous chapter.

This chapter outlines the resulted objectives of this project in section 6.2. The next sections 6.3 will discuss the reflection of the overall project. Final section 6.4 will recommend the future work that can be possible on this project.

6.2 MEETING THE OBJECTIVES

Five objectives were defined at the beginning of this project:

1. To investigate and review the literature in the field of Mobile device forensic and in specific to Android forensic
2. Identify and review the best practices currently in use for mobile forensics
3. Determine the measurable criteria and desired outcomes required of Android Forensic tools
4. Develop a methodology for evaluating the forensic tools for android devices
5. Critically evaluate the tools based on the methodology against the actual forensic data identified from the Android phones.

The discussion of each of the objective is described in each paragraph.
6.2.1 Objective 1 - To investigate and review the literature in the field of Mobile device forensic and in specific to Android forensic

A thorough literature search was conducted and reviewed in chapter two. The literature in the area of Mobile device analysis has conducted and reviewed. The first review has done on mobile device analysis mainly focused on the Android forensic. The different mobile forensic techniques and the challenges faced by the mobile forensic were presented. Forensic analysis mainly involved in analysing the files system. The review also discussed on the area of Android architecture, file system and data storage areas. Finally a review of the extraction tools that tested in this project and extraction methods used by previous researches. The objective is met by reviewing all the areas discussed.

6.2.2 Objective 2 - Identify and review the best practices currently in use for mobile forensics

The objective 2 was met in Chapter 2 by identifying and reviewing the literature and the methodologies suggested by some of the international agencies like NIST and ACPO. These best practices can be applied while investigating a forensic analysis. NIST’s ‘Guidelines on cell phone Forensics’ and ACPO’s Good practice guide for computer based electronic evidences identified and reviewed. There are few other methods, which are have not set rules or guidelines that follow certain good practices while doing the forensic analysis. These techniques are involved in the preservation, analysis and presentation of evidence as a whole. These facts are identified and reviewed in chapter 2 and chapter 3.

6.2.3 Objective 3 – Determine the measurable criteria and desired outcomes required of Android Forensic tools

Meeting this objective is difficult task of this project. Each forensic tool behave differently when the test done. A review of finding the criteria has conducted in chapter 2, literature review. The main measurable criteria that a forensic tool must follow are the reliability. Chapter 3 and 4 further discusses how these criteria can be met. The forensic tool is reliable only when it produces the same results repeatedly. However this is most challenging as different variable influences the reliability as per the testing environment. Chapter 4 outlines these counts in length. The desired outcome can also be guarantee as it also depends on the version of the tool is using and how the testing is conducted. The objective
is met by producing the result from the evaluation stage of this project with some variations from the desired results.

6.2.4 Objective 4 - Develop a methodology for evaluating the forensic tools for android devices

This objective is met in Chapter three, and four. It shows a successful design and implementation of testing of the tools. Various methodologies are identified and reviewed. A new methodology was proposed based on the various forensic evidences that can be extracted from the mobile phones. This is followed in each case and produces the results.

6.2.5 Objective 5 - Critically evaluate the tools based on the methodology

The final and critical part of this project is evaluation of tools. This objective is met by successfully evaluating the tools based on the methodology proposed. The data produced from the evaluation is huge and it is found to be difficult to table. So the method approached here is the graphical representation of data that can be easily readable and easy to be analysed.

Overall the results were expected with the desired outcome from the literature review and methodology. Although some of the results are not expected such as manual extraction however the evaluation produces moderate results and can be verified.

6.3 CRITICAL ANALYSIS

There are few difficulties encountered during this project. The first are is of finding the literatures specific to the device analysis. Although there are lots of information available in various sources but not are all to be the specific in nature. Most of the article researched is of not much of academic value. A great amount of time spends on finding the right papers. As this is a relatively new topic the literatures searches has conducted in the main topic of digital forensic.

Finding a meaningful evaluation framework is important in completing the project. This project also met with similar problem. During the initial stage of the project it was decided to do the evaluation of minimum five marketing leading tools. However most tools are not publically available and are close circled. Not all the software vendors are interested to publish their software and are mainly focused
for law enforcement agencies. The tools like AccessData MPE+, ViaExtract full version, Paraben device seizure are planned for this project but unfortunately not able to download or procure. Though unavailability of this software the current methods can be applied and can be easily evaluated.

6.4 FUTURE WORK

The area, which this project has done, has potential scope for further study. Mobile phones are evolving and mobile forensic is a challenge. Evaluations of forensic tools are complex unlike simply comparing software with pre-set parameters. The very nature of digital forensic process its self is a critical and time consuming, it is required a number of criteria to be set up before conducting a mobile forensic.

When the project was at the research proposal stage the idea was to develop a framework to easily evaluate the tools. But this found to be a lengthy process. Just designing and showing the results will not verify the effectiveness of a tool. It required a considerable amount of lab test. This is why more further study possible in this research. Handset manufacturers are adding new features every day and the way the data stored today in an Android phones can change in coming days. As the openness of Android and its huge developer and customer base is a challenge for an effective forensic analysis. More future research is possible in many ways analysing this research as a whole.
REFERENCES


<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACPO</td>
<td>Association of Chief Police Officers</td>
</tr>
<tr>
<td>ADB</td>
<td>Android Debug Bridge</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>CSV</td>
<td>Comma Separated Values</td>
</tr>
<tr>
<td>dd</td>
<td>Disk Dump</td>
</tr>
<tr>
<td>DVM</td>
<td>Dalvik Virtual Machine</td>
</tr>
<tr>
<td>FTK</td>
<td>Forensic Tool Kit</td>
</tr>
<tr>
<td>GB</td>
<td>Gigabyte</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>GSM</td>
<td>Global System for Mobile Communications</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>ICS</td>
<td>Ice Cream Sandwich</td>
</tr>
<tr>
<td>JDK</td>
<td>Java Development Kit</td>
</tr>
<tr>
<td>JTAG</td>
<td>Joint Test Action Group</td>
</tr>
<tr>
<td>MB</td>
<td>Megabyte</td>
</tr>
<tr>
<td>MD5</td>
<td>Message Digest</td>
</tr>
<tr>
<td>MMS</td>
<td>Multimedia Messaging Service</td>
</tr>
<tr>
<td>NAND</td>
<td>Not AND</td>
</tr>
<tr>
<td>OHA</td>
<td>Open Handset Alliance</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>RAM</td>
<td>Random Access Memory</td>
</tr>
<tr>
<td>SD</td>
<td>Secure Digital</td>
</tr>
<tr>
<td>SDK</td>
<td>Software Development Kit</td>
</tr>
<tr>
<td>SIM</td>
<td>Subscriber Identity Module</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Messaging Service</td>
</tr>
<tr>
<td>XMPP</td>
<td>Extensible Messaging and Presence Protocol</td>
</tr>
<tr>
<td>YAFFS</td>
<td>Yet Another Flash File System</td>
</tr>
</tbody>
</table>
Appendix A: Extraction Logs
(The full copy of all Appendices and other logs can be downloaded from: http://goo.gl/CPUqk )

AFLogical - System information extracted from Phone 2 – HTC Sensation XE
info.xml
<android-forensics>
<date-time>20120426.1506</date-time>
<IMSI>234308385235430</IMSI>
<IMEI-MEID>358313049279859</IMEI-MEID>
<phone-type>1</phone-type>
<MSISDN-MDN>+447534548613</MSISDN-MDN>
<ICCID>8944302001488426343</ICCID>
<build>
  <version.release>4.0.3</version.release>
  <version.sdk>15</version.sdk>
  <version.incremental>309896.105</version.incremental>
  <board>pyramid</board>
  <brand>htc_europe</brand>
  <device>pyramid</device>
  <display>IML74K</display>
  <fingerprint>htc_europe/htc_pyramid/pyramid:4.0.3/IML74K/30
9896.105:user/release-keys</fingerprint>
  <host>ABM014</host>
  <id>IML74K</id>
  <model>HTC Sensation XE with Beats Audio Z715e</model>
  <product>htc_pyramid</product>
  <tags>release-keys</tags>
  <time>1332343818000</time>
  <type>user</type>
  <user>unknown</user>
</build>
<applications>
  <app>
    <label>HinKhoj Dictionary</label>
    <className>null</className>
    <dataDir>/data/data/HinKhoj.Dictionary</dataDir>
    <descriptionRes>0</descriptionRes>
    <flags>48708</flags>
    <manageSpaceActivityName>null</manageSpaceActivityName>
    <name>null</name>
    <packageName>HinKhoj.Dictionary</packageName>
    <permission>null</permission>
    <processName>HinKhoj.Dictionary</processName>
    <publicSourceDir>/data/app/HinKhoj.Dictionary-2.apk</publicSourceDir>
    <sourceDir>/data/app/HinKhoj.Dictionary-2.apk</sourceDir>
Appendix B – AFLogical shell

Android shell from forensic workstation

Forensic folder created by AFlogical after extraction on SD Card
Appendix C - Extraction Log- Oxygen forensic
(The full electronic copy of Appendices can be downloaded from: [http://goo.gl/CPUqk](http://goo.gl/CPUqk))

### Device Data Report

<table>
<thead>
<tr>
<th>Device details</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Device alias</td>
<td>New device (Android Phone)</td>
</tr>
<tr>
<td>Retail name</td>
<td>Google Android Phone</td>
</tr>
<tr>
<td>Manufacturer</td>
<td>Google</td>
</tr>
<tr>
<td>Model</td>
<td>Android Phone</td>
</tr>
<tr>
<td>IMEI</td>
<td>350760441781061</td>
</tr>
<tr>
<td>SW revision</td>
<td>2.3.3</td>
</tr>
<tr>
<td>IMSI</td>
<td>234101033839587</td>
</tr>
<tr>
<td>SN</td>
<td>HT15XTJ03690</td>
</tr>
<tr>
<td>ICCID</td>
<td>8944110065195744005</td>
</tr>
<tr>
<td>Owner phone number</td>
<td>N/A</td>
</tr>
<tr>
<td>Voice mailer</td>
<td>901</td>
</tr>
<tr>
<td>Device owner numbers</td>
<td>O2 HTC, SAMIR: 07934855305</td>
</tr>
</tbody>
</table>

### Case details

- Extracted by version: 4.2.0.313
- Rooted: No
- Case assigned: 101

### Device notes
- Android Desire S forensic

### Extraction date
- 4/26/2012

### Extraction time
- 11:04:36 AM

### Device owner
- Samir

### Extraction made by
- Vijith

### Report details

- Generation date: 4/26/2012
- Generation time: 11:17:16 AM
- Extraction made by: Vijith

### Summary data

<table>
<thead>
<tr>
<th>Section</th>
<th>Phonebook</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statistic</td>
<td>190</td>
</tr>
<tr>
<td>Contacts</td>
<td>190</td>
</tr>
<tr>
<td>Caller groups</td>
<td>11</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statistic</td>
<td>64</td>
</tr>
<tr>
<td>Incoming</td>
<td>57</td>
</tr>
<tr>
<td>Sent</td>
<td>7</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Event Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statistic</td>
<td>375</td>
</tr>
<tr>
<td>Dialed calls</td>
<td>317</td>
</tr>
<tr>
<td>Answered calls</td>
<td>37</td>
</tr>
<tr>
<td>Missed calls</td>
<td>21</td>
</tr>
</tbody>
</table>

Logs from phone 1, Phone 2 logs can be downloaded from
Appendix D - Manual Method Extraction FTK/Winhex

Keyword searching through Phone image from winhex, FTK acquisition (below)
Android Data storage locations

*Typical Data storage location in an Android Device*

**Phone contacts, and call log:**
/data/data/com.android.providers.
\ contacts/databases/contacts2.db

**Calendar information:**
/data/data/com.android.providers.
\ calendar/databases/calendar.db

**SMS and MMS messages:**
/data/data/com.android.providers.
\ telephony/databases/mmssms.db

**Gmail and gtalk data:**
/data/data/com.google.android.providers.
\ gmail/databases/mailstore.napier.android.
\ <GMAILADDRESS>.db

Each of these databases are SQLite3 databases, the easiest way to ‘export’ data is via the sqlite3:
sqlite3/data/data/com.android.providers.
\ calendar/databases/calendar.db .dump \>calendar_raw.txt
Appendix E: Project Management
Gantt chart