Integrity-Based Evaluation of Forensic Tools on Android Jelly Bean

OJENIYI, Joseph Adebayo
Department of Cyber Security Science,
Federal University of Technology
Minna, Nigeria
ojeniyija@futminna.edu.ng

ALHASSAN, John Kolo and OJERINDE, Oluwaseun Adeniyi
Department of Computer Science,
Federal University of Technology
Minna, Nigeria

AHMAD, Suleiman and OKEKE, Okechukwu Chukwuweike
Department of Cyber Security Science,
Federal University of Technology
Minna, Nigeria

OJENIYI, Alice Adekemi
Niger State Office,
National Examinations Council
Minna, Nigeria

ABSTRACT

In the earlier years, there has been an exponential growth in the figure of smartphone users. Smartphone protects and manages enormous amount of evidence pertaining to its owner. The tenacity of this work is to evaluate forensically TECNO S3 running the Jelly Bean Android operating system, using forensic tools, which is important for investigators as it offers greater safety relating to an individual's privacy rights. Furthermore, smart phones are moderately new form of digital devices that are intensifying speedily in the public. The smart phone is evaluated with following forensic tools: Paraben device seizure, Mobiledit, AFLogical - OSE. The work minimizes manual user interaction, delivers an outline of what can be acquired and the forensic integrity of such items upon recovery, and the reason for any changes to the device.

Keywords: Forensically sound, image, operating system, logical acquisition, physical acquisition and write blocker

1. INTRODUCTION

Smart phones are the latest fashion in mobile devices. They are influential pieces of technology wrapped into miniature packages, capable of tracking the communications, locations, and contacts of their users. Therefore, they have the impending to contain forensic information about someone usable in the courtrooms. According to (AdMob, 2010), "Users of the IOS and Android platforms regularly spend at least 79 minutes a day using apps." That means that the common user spends over an hour using their phone for somewhat other than calling or texting. The applications being used have the prospective to give the forensic analysts a deeper, more personal glance into the lives of the suspects in subject, away from what has been formerly obtainable to them when cell phones were merely a way to call your contacts on the go. With the recognition of the smart phones increasing, the significance of researching and perfecting methods of forensic analysis of smart phones is becoming more and more famous. As these devices become more accepted, criminals have more access and chance to use them for deceitful activities. Smart phones could be used for many criminal actions, such as committing email fraud, illegal substance related communications, harassment via texting, etc. Since smart phones are proficient of all this, the data stored on them could be a precious asset to a forensic analyst carrying out an investigation. Smart phones store a range of valuable data about a person just through fundamental information such as contacts, text messages, call logs, emails, saved account information, browser history and chat logs.

Although smart phones have a bunch of private data, it is hard to access because of the wide variety of software; there is a short of standardized methods to retrieve this data. Companies use enormously different media to store the data, diverse file system structures, and different operating systems. Even devices manufactured by the same manufacturer could have different USB connections as well as different size or type of data storage. With all the differences in phones, researchers are working hard to make smart phone forensics easier. As Android's popularity is increasing, people are getting more fascinated in it, allowing room to develop new ways to collect forensic data on the large number of phones out there now.

1.1 Introduction to the Android OS

The Android operating system was developed by the Open Handset Alliance (OHA). The OHA is a group of 84 technology and mobile companies with an ambition to accelerate innovation in mobile and offer consumers a richer, less expensive, and better mobile experience.

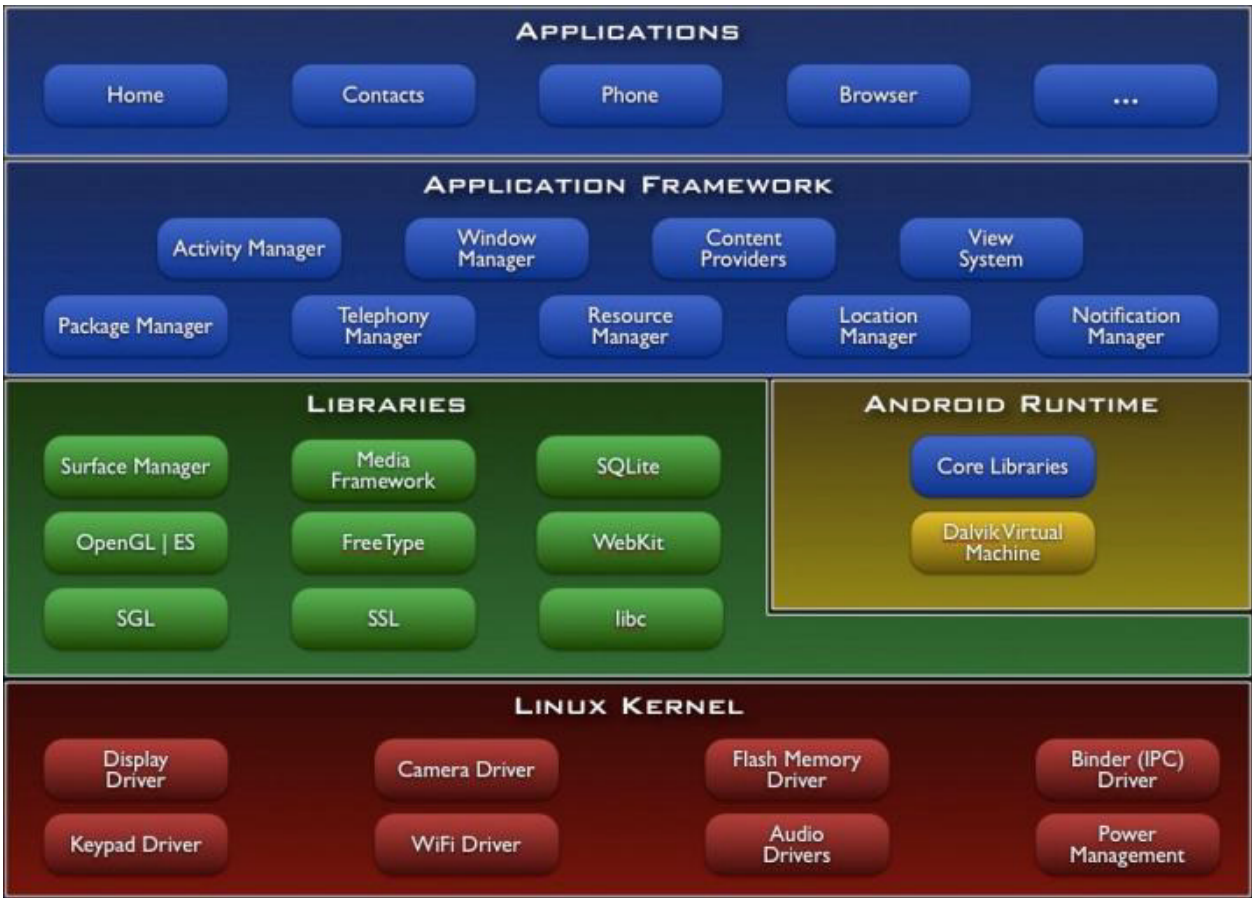

Fig. 1: Android architecture

As seen in figure 1. the applications level ships with a set of core applications, such as an email client, SMS program, calendar, maps, contacts, and a browser. All the applications are written in Java.

Underneath the applications level is the application framework. Android provides an open development platform. This provides developers with the control to build applications that take complete benefit of the devices' hardware, such as location information, background services, the ability to set alarms, adds notifications to the status bar, and many more features. Developers are given full right to use the framework API used by the core applications, which is designed to shorten the re-use of components. They services consist of views, which are used to develop the GUI of the application. Content providers used to allow applications to access data. Resource managers used to grant access to graphics and layouts. Notification managers are used to enable all applications to show alerts, and an activity manager which manages the lifecycle of an application.

Under the application framework is a group of libraries written in C/C++, which are used by numerous components of the Android system. The nucleus libraries include a System C Library for embedded Linux-based devices, Media Libraries for playback and footage of media, a surface manager which grants access to the 2D and 3D components, FreeType for bitmap and vector rendering, and SQLite for the database needs, a LibWebCore which is the recent browser engine for Android, SGL which is the 2D graphics engine, 3D libraries based on OpenGL for use of 3D accelerations and graphics. The Android runtime includes a group of core libraries that provides the functionality in the core libraries available to the Java programming language. As well the core libraries, every application that is run is executed using the Dalvik virtual machine (VM). The Dalvik VM runs applications in its own virtual machine. Android applications are compiled into .dex files, which are run by the Dalvik VM. The Dalvik VM depends on the Linux Kernel for its functionality and memory management. The Linux Kernel version 2.6 provides the core system services for Android, including memory management, process management, drivers, network stack, and most importantly, security.

All of these permit the Android phone to run, but as a forensic analyst the most important features of an Android are the SQLite databases, which lots of apps use to save their data on the device. Nearly all Android phones come with a removable microSD card, which is usually formatted in FAT32 and is easily extracted, imaged, and examined using traditional forensic tools. The Android file system is called Yet Another Flash File System 2 (YAFFS2) which was the foremost file system designed specifically for NAND flash memory. YAFFS2 allows for larger NAND flash devices.

1.2 Background

Smart phones create a new crisis for digital investigators as there are many diverse models and mobile devices update both software and hardware very speedily. Mobile devices are designed to be associated to a live network while on, this increases the threat of remote erasing of evidence as well as creating issues with evidence recovery.

One of the most frequent crimes investigated by digital investigators is viewing, distribution and production of child pornography (BJS, 2007). One general way for people to obtain child pornography is through the internet, and in particular with torrent programs. Torrent programs permit users to download files from other users across the internet peer to peer. With the boost in high speed data cellular networks these programs are current in mobile device market places. This allows users to download illicit material, such as child pornography, openly to a mobile device.

With the likelihood of mobile devices being the major device for obtaining and storing illicit content, investigators must take steps to scrutinize these devices in a forensically sound manner. Investigators may not be capable to rely on traditional computers for evidence. Unfortunately, the investigator may not have the necessary tools or the information necessary to recuperate evidence in a forensically sound technique from a mobile device. The legal and technical methods and procedures on traditional computer forensics have being altered a little in the last few years. The differences in techniques for creating physical images of evidence across different operating systems and manufacturers are minimal. In disparity, methods for getting evidence from mobile devices may differ extensively from device to device. The legal problems and technical issues that come with mobile devices are constantly changing and it can attest to difficult for investigators to uphold the suitable tools and training to keep tempo with the change.

1.3 Motivation

There are many varieties of smart phone operating systems available on the market, *i.e.* An IOS, Android and RIM. Google's Android operating system is one of the most admired OS for smart phones, television, gaming devices and notebooks. In 2013, android global market share is valued at over 78.4% as shown in Figure 2, the number of daily activation on android devices is 1.5 million, global shipment of android smart phones is 1.13 billion and distribution of android Jelly Bean is 25%.(statista.com) as shown in Figure 3.

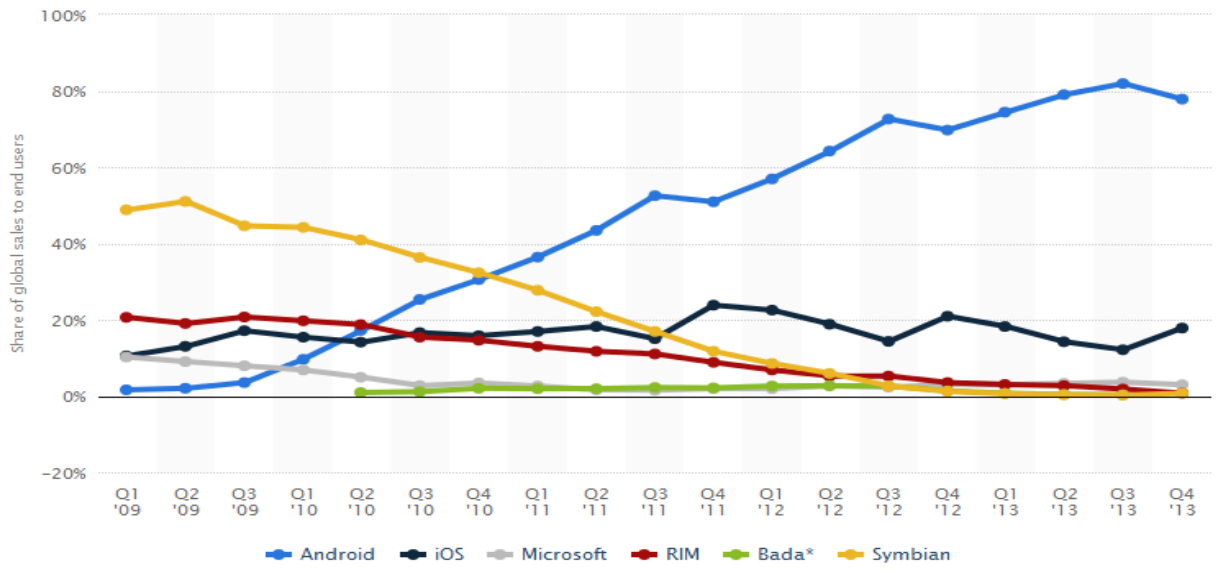

Fig. 2: Global market share held by the leading smartphone operating systems in sales to end users from 1st quarter 2009 to 4th quarter 2013

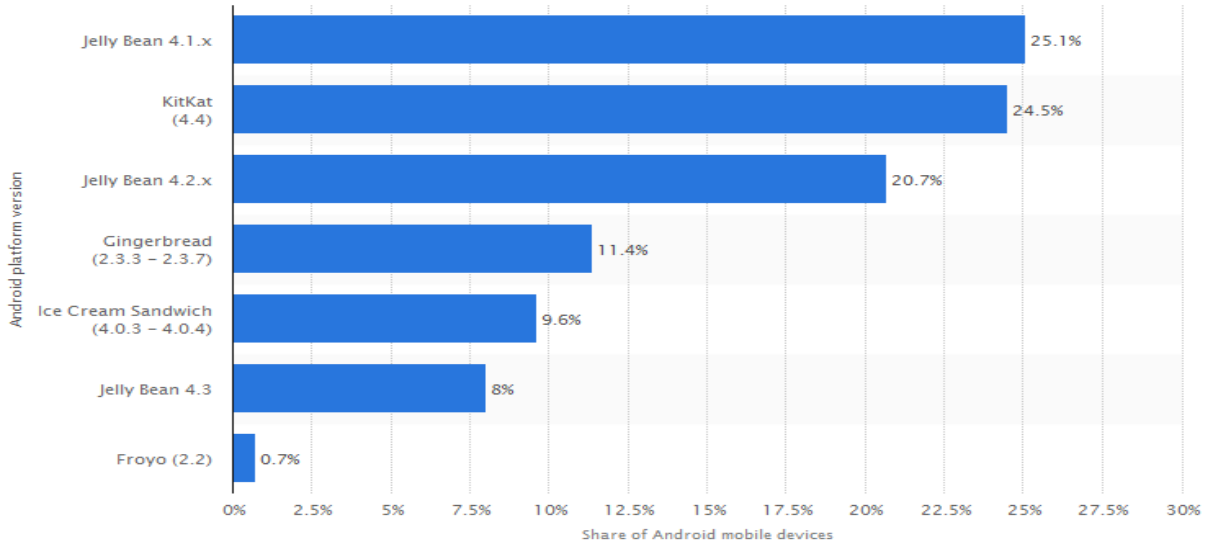

***Fig.* 3: Distribution of Android operating systems used by Android phone owners in October 2014, by platform version**

1.4 Objectives

i. To carry out evaluation of forensic tools on android jelly bean
ii. To compare the evidence from the different tools
iii. To recommend forensic tool to investigators based on identified strengths

2. RELATED WORKS

The most relevant research that was close to my case studies was done by following:

(SeyedHossein et al. 2011) In their project on 'Smartphone Forensics: A Case Study with Nokia E5-00 Mobile Phone' says that ubiquitous device is being regarded as a precious evidence item in forensic investigations. However owing to difference in smart phone models, retrieving complete data from all models using predefined instructions and tools is not constantly possible This paper studies demo or trial versions of four commonly used mobile forensics tools namely, Oxygen Forensic Suite, Paraben's Device Seizure, Mobile Internal Acquisition Tool, and MOBILedit! Forensic Lite, in extracting data from a Nokia E5-00 smart phone. The result of this paper presents that obtainable toolkits are deficient to assemble volatile data as well as deleted information. The results recommend that smart phones are able to store and deal with a massive quantity of information, but the types of gathered data by examined tools are not far superior to the types of data managed by ordinary mobile phones. The root of the problem is all experimental tools were unable to recover many deleted data. It has been also alleged that none of them can be employed in live investigation of Nokia E5-00. Another predicament could be the disability of the tools in bypassing security mechanisms like access codes applied to a Nokia E5-00.

(AlShidhani et al.2013) In their project on 'Smartphone Forensics Analysis: A Case Study' shows a contrast between the artifacts extracted from the smart phone using Oxygen and UFED tools. Although Oxygen has limited access to the device but it generally gives more information about WhatsApp application compared to UFED physical Analyzer. The comparison shows that each tool excels in extracting definite type of information valuable for forensic analysis. For example, information like images and contact numbers are better extracted by the UFED physical Analyzer compared to Oxygen. On the other hand, Oxygen outperforms UFED in extracting data from messaging services such as WhatsApp. Which found; The ISP established earlier that Ali did not send WhatsApp messages. On the other hand, Ali's contacts received WhatsApp messages from Ali's phone. To replicate the scenario, a similar device was tested using Oxygen Forensics and UFED physical analyzer and it was found that WhatsApp messages do not necessarily necessitate cellular communications to be delivered. WhatsApp messages can also be delivered over Wi-Fi network from the above mentioned facts we can derive two possible compromise scenarios. Scenario a, the Subscriber Identity Module (SIM) card was removed and the attacker used Wi-Fi network to deliver WhatsApp message. Scenario b, Ali sold his smart phone but didn't remove WhatsApp application and the new holder used a Wi-Fi network to deliver WhatsApp messages to Ali's contacts.

3. METHODOLOGY

The specifications of the materials used for the evaluation are:

i. A HP laptop was used to run evaluation the different forensic softwares installed in the laptop with specification of 6 GB RAM, 500 GB Hard disk space, Window 7 (Ultimate) OS.
ii. A TECNO S3 smart phone with the following specifications of 512MB RAM, 1GB ROM, android version 4.2.2 was used for evaluation
iii. A USB cord was used to connect smart phone to laptop

Three forensic tools being frequently used in mobile phone investigations are evaluated. They are:

i. Paraben's Device Seizure v6.6 (Demo)
ii. MOBILedit! Forensic Lite v7.5.6.4317
iii. AFLogical - OSE 1.5.2

3.1 Paraben Device seizure

Installation

Paraben DS version 6.6 was installed on the Windows forensic workstation. The setup process required the installation of many vital drivers that took an extensive amount of time. The software must be registered prior to use, which is achieved either using a hardware dongle or through a registration key file provided by Paraben. To install the registration key file, you simply copy the file into the DS install directory, which is likely C:\Program Files\Paraben Corporation\Device Seizure.

Acquisition

The acquisition begins on new Android device; you first open a new case and complete the necessary case information section. You then choose "Data Acquisition" and select 'Android logical'. According to these instructions, Android phones are supported. However, the acquisition of the TECNO S3 was successful. Follow the instructions and then click "Next" at which point DS attempts to identify the phone. Ensure the identified device information is accurate and click "Next".

`

The next screen provides a list of supported data types that DS can extract from the device. All were selected, which includes acquiring the part of the file system it can read and the SD card, so the acquisition process is slow.

3.2 MOBILedit! Forensic

Installation

The MOBILedit! Forensic application was downloaded from www.mobiledit.com and the install only took a few minutes. After the installation is completed and the application is run for the first time, you are presented with a prompt to check for updates. To activate the software, Compelson sends an e-mail with an "activation card" attachment. This PDF file includes installation instructions as well as an activation key that worked without any issues.

Acquisition

To begin the acquisition, the examiner must first connect the Android device to the forensic workstation using USB and ensure USB debugging is enabled. MOBILedit! attempts to detect the device. After clicking "Finish," there was a notification prompting the installation of the "Connector" app on the device. Following the quick installation, you create a name for the investigation and select the type of data you want to extract. The option to take a backup of the "Whole file system" was selected, which then executed without error and presented a success status, you can then decide if you want to add this to an already existing case or create a new one. Acquisition process, a new case was created and a data export format option of XLS was selected.

3.3 AFLogical - OSE

AFLogical is an Android forensics logical technique tool which is distributed free to law enforcement and government agencies. The app, developed by viaForensics, extracts data using Content Providers, which are a key feature of the Android platform. This is the same technique that commercial forensics tools use for logical forensics.

Recall that Android's security model is effective in limiting access to app data except in a few circumstances. Here is a quick recap of the key components of Android's security model:

i. Each application is assigned a unique Linux user and group id.
ii. Apps execute using their specific user ID in a dedicated process and Dalvik VM.
iii. Each app has dedicated storage, generally in "/data/data," that only the app can access.

However, the Android framework does provide a mechanism by which apps can share data. An app developer can include support for Content Providers within their application, which allows them to share data with other apps. The developer controls what data is exposed to other apps. During the install of an app, the user controls whether or not an app should gain access to the requested Content Providers. Some examples of Content Providers are:

1. SMS/MMS
2. Contacts
3. Calendar
4. Call logs

And there are many more.

The AFLogical app takes advantage of the Content Provider architecture to gain access to data stored on the device. Similar to commercial Android logical tools, USB debugging must be enabled on the device for AFLogical to extract the data. The current version, 1.5.2, extracts data from 41 Content Providers and provides the output information to the SD card in CSV format and as an info.xml file, which provides details about the device and installed apps. AFLogical supports devices running Android 1.5 and later, and has been specifically updated to support extraction of large data sets such as an SMS database with over 35,000 messages with data extraction completed message as shown

4. EXPERIMENT FRAMEWORK

4.1Difference between Logical and Physical Techniques

Forensics techniques on android are either logical or physical in nature. A logical technique extracts allocated data and is achieved by accessing the file system. The Allocated data basically means that the data are not deleted and are available on the file system. The recovery of the deleted data requires special tools and techniques; it is possible to recuperate deleted data from a logical acquisition. Physical techniques, on the other hand, aim the physical storage medium directly and do not depend on the file system itself to access the data. They advantages to this approach are; the most momentous is that physical techniques likely grant access to significant amounts of deleted data. File systems often only mark data as deleted or obsolete, and do not in reality erase the storage medium unless needed. As physical forensic techniques provide direct access to the storage medium, it is possible to recover both the allocated and the unallocated (deleted or obsolete) data. Physical acquisition is usually far more difficult and time consuming. Also, the physical techniques are more difficult to accomplish and missteps could leave the device inaccessible. In Android forensics, the most common logical technique does not provide direct access to the file system and operates at a more conceptual and less-effective level than the traditional logical techniques, which can obtain all non-deleted data directly from the file system (Hoog, 2011).

4.2 Principles of Computer-based Electronic Evidence

The guide, Good Practice Guide for Computer-Based Electronic Evidence (ACPO Good Practice Guide, n.d), establishes four principles of computer-based electronic evidence:

i. No action taken by law by investigator should alter data held on a computer or storage media, which may consequently be relied upon in court.
ii. In situation where a person finds it obligatory to access original data held on a computer or on storage media, that person must be experienced to do so and be able to give evidence explaining the significance and the implications of their actions.
iii. An inspection trail or other record of all processes applied to computer-based electronic evidence should be created and conserved. An independent third party should be able to examine those processes and achieve the same end result.
iv. The person in custody of the investigation (the case officer) has general responsibility for ensuring that the law and these principles are adhered to.

Three prerequisites for forensic tools as follows:

i. Changing data stored on the device as little as possible
ii. Extracting the maximum amount of data
iii. Minimizing investigator interaction with mobile phone.

5. RESULTS AND DISCUSSION

The designated tools mention in chapter three above have been examined after providing them with the TECNO S3 that some of its SMS messages, contact list entries, event logs, web histories, todo entries, user's files, and email messages were acquired.

5.1Paraben Device Seizure

At that point, the acquisition process was complete, shows the DS acquisition complete output.

Device Seizure displays the acquired data with the application in an easy to browse and navigate structure. Contacts provide not only the name, notes, phone numbers, and e-mail, but also helpful fields, such as number of times contacted, last time contacted, and a photo, if available.

The SMS reporting provides the expected fields, but deleted messages were not included. The report does not cross-reference the contact data with the phone number, so the examiner must either know the phone number or handle the crossreferencing themselves. However, the call logs do perform the cross-reference and display the date, message type, duration, number, number type, name, or whether the call was a new call (presumably the first time that number appeared in the call logs)

5.2 MOBILedit! Forensic

Immediately following the acquisition of the device, MOBILedit displays statistics on the devices that were acquired, as well as a view of the application data available for analysis and shows the main screen where the examiner can see specific device information including the IMEI number, serial number, and details on the amount of Phone memory, Battery signal, Network signal, and Memory card space available on the device. The next option in the Tree View is the Phonebook where the examiner can view all contacts stored within the Phonebook including e-mail address, phone numbers, nicknames, and any notes entered regarding the contact. Call logs are next and are separated into Missed calls, Last dialed numbers, and Received calls. SMS messages are similarly separated into categories including Inbox, Sent items, and Drafts. Each section contains the date and time the message was received (or sent), the message content, and who the message was from. Contact names are linked to the Phonebook, so both name and phone numbers are displayed. Any MMS messages are displayed within the "MMS Storage" folder.On the left-hand side, information about the message is displayed, including the subject, number it was sent from, number it was sent to, and date and time. On the right-hand side is a preview of the actual image.

Selecting the Calendar option will literally pull up a calendar within the reporting tool, additional data extracted from the device or SD card is shown within the "files" directory. This directory contains a listing of the file system on the device. While some of these folders are empty (such as cache, config, and data), there are also some folders which contain raw files acquired from the device. For example, within the SD.

5.3 AFLogical –OSE

And then complete the acquisition using the screen presented on the device .Otherwise, you can simply run the app directly from the All Apps screen on the device as shown in. First, access the Android app menu, look for a program called viaForensics and click on the icon to launch the app. You will then be presented with the AFLogical data extraction screen. You can select or deselect individual Content Providers or leave all of them selected. Next, you hit Capture which will start the data collection process. Once the data collection is complete, you will receive the corresponding message. The extracted data are saved to the SD card of the device in a directory called forensics and a subdirectory named after the date in YYYYMMDD.HHMM format. For this example, we moved the files from the SD card to an AFLogical directory on the local file system using adb pull. If you examine that folder, you see:

5.4 Comparison between the three forensic tools.

Table 1: Showing comparison of the three forensic tools

TECNO S3 (Information type)	Paraben Device Seizure	MOBILedit! Forensic	AFLogical- OSE
Phone book	Yes	Yes	Yes
SMS Messages	Yes	Yes	Yes
Event Log	No	Yes	No
Images	Yes	No	No
Music	No	Yes	No
Video	No	Yes	No
Database files	No	Yes	No
Application	No	Yes	No
WhatsApp Messenger	No	Yes	No
Bypassing locked smartphone	Yes	Yes	No
Call logs	Yes	Yes	Yes
Configured email	Yes	No	No
Contact information	Yes	Yes	Yes
Exporting features	Yes	Yes	Yes
Reporting features	No	Yes	No
MMS messages	Yes	No	Yes
User data files	No	Yes	No
Web browser cache	No	Yes	No
WLAN open sessions	No	No	No
Running processes	No	No	No
Organised events	Yes	No	No
Map History	No	No	No
Communities program logs	No	No	No

Mobiledit, Paraben and AFLogical, as forensic tools, could recover the significant amount of data stored on the flash memory of TECNO S3. However the foremost observed setback is none of them were able to retrieve all deleted information. Moreover, Mobiledit needed an agent to be installed on the mobile phone though Paraben does not run any application on the target smartphone, but it is stated that the tool changes some minor data as well. Paraben was able to discover picture of individual in the contact and its evaluation was much organised. Mobiledit is very good in reporting the evidence gathered. AFLogical is an excellent tool in gathering information on call logs, contacts and SMS messages. All these tools are, therefore, feeble in compliance with the first principle of the ACPO's requirements stated in chapter three despite that, none of the selected tools could collect any data from the RAM. Neither GPS nor communities applications logs were extracted by these tools. With the pervasive use of applications like Map and Facebook and the importance of retrieving history logs pertaining to these applications in forensic investigations it is another major drawback of the examined tools. Mobiledit and Paraben except AFLogical, required mobile phone to be connected to the forensic workstation as 'Android acquisition' and if 'Ask on connection'' is active - which in default is - investigator has to select 'Android'once the mobile phone gets connected to the workstation. That is to say if user enables the security code and investigator does not have access to that code, none of these tools can gather data. As shown in Figure 4 the priority of recommendation of the tools based on strength.

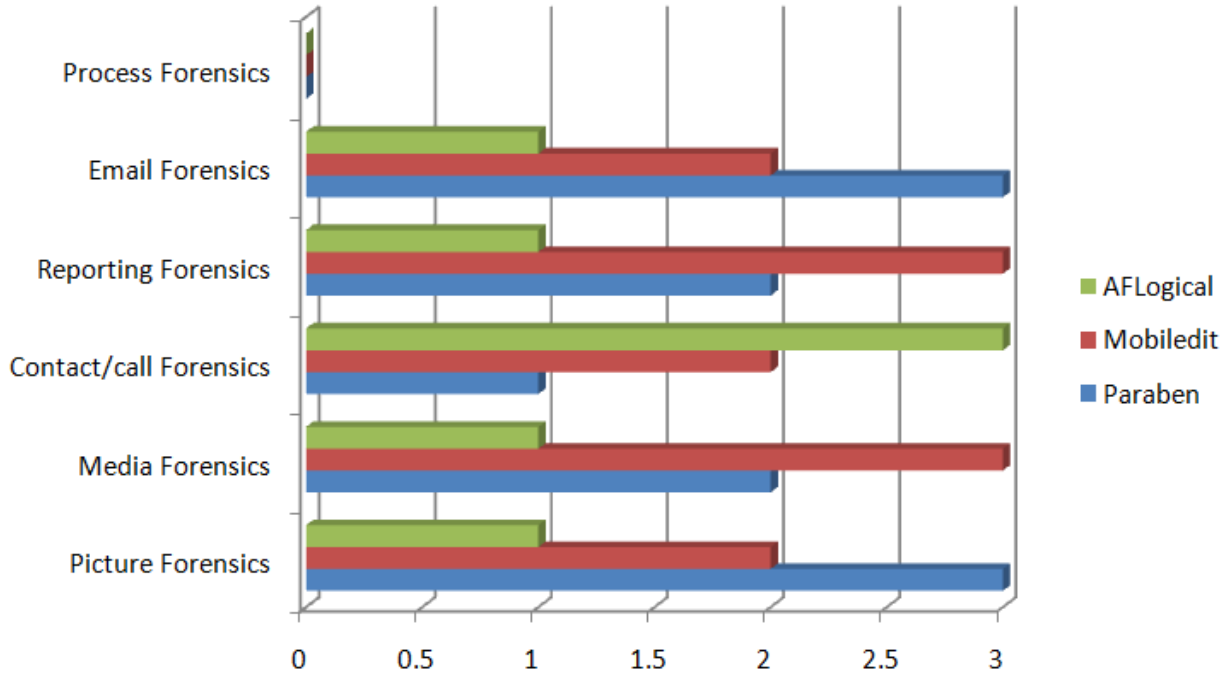

Fig. 4: Bar chart showing priority of recommended tools

6. CONCLUSION

Within this work, three mobile forensics tools in retrieving data from a TECNO S3 mobile phone were evaluated. The results suggest that while smart phones are able to store and manage a massive quantity of information, but the types of gathered data by examined tools are not far superior to the types of data managed by ordinary mobile phones. The crux of the problem is all observed tools were unable to recover many deleted data. It has been also perceived that these tools can be employed in live investigation of TECNO S3.

REFERENCES

1. AdMob. (2010, May). *Mobile Metrics*. Retrieved from http://www.metrics.admob.com/wp-content/uploads/2010/06/May-2010-AdMob-Mobile-Metrics-Highlights.pdf
2. C., R., & N., M. (2012). Android Forensics: A Case Study of the HTC Incredible Phone. *Proceedings of Student-Faculty Research Day, CSIS, Pace University* , 5-8.
3. Encryption, T. (2012). *TechTerms*. Retrieved July 7, 2012, from http://www.techterms.com/definition/encryption.
4. Hoog, A. (2011). *Android Forensics: Investigation, Analysis, and Mobile Security for Google Android.* Syngress Press.
5. Mubaraki, A.-H., & Ali, A. (2013). Smartphone Forensics Analysis: A Case Study. *Internatioinal Journal of Computer and Electrical engineering* , 6.
6. Muhammadi, F., N., L.-K., & Tahar, K. (2014). Smartphone Forensic Analysis: A Case Study for Obtaining Root Access of an Android Samsung S3 Device and Analyse the Image without an Expensive Commercial Tool. *Journal of Information Security* , 83-90.
7. Netmarketshare. (2012). *Mobile market share*. Retrieved July 7, 2012, from http://www.marketshare.hitslink.com/
8. Norton. (2011). *Symantec: Norton study calculates cost of global cybercrime: $114 billion annually*. Retrieved from http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02.
9. Security.(n.d)., A. G.-B. (n.d.). Retrieved February 19, 2011, from http://www.7safe.com/electronic_evidence/index.html#
10. SeyedHosseini, M., Ali, D., & Hoorang, G. B. (2011). Smartphone Forensics: A Case Study with Nokia E5-00 Mobile Phone . *International Journal of Digital Information and Wireless Communications* , 651-655.
11. Statisics, B. O. (2007). *Federal prosecution of child sex exploitation* . Retrieved from Bureau of justice stastistics bulletin: http://bjs.ojp.usdoj.gov/content/pub/pdf/fpcseo06.pdf
12. Statista. (2013). *Statistics of data*. Retrieved September 13, 2014, from http://statista.com/topics/876/android/
13. Statista. (2013). *Statistics of data*. Retrieved October 2, 2014, from http://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems/
14. System, T. O. (2012). Retrieved July 7, 2011, from TechTerm: