2nd International Engineering Conference (IEC 2017)
Federal University of Technology, Minna, Nigeria

Comparative Analysis of the Accuracy of Forensic Results obtained from Window and Android Platforms

John K Alhassan, Hassan T Abdulazeez, Shafi'i Muhammad Abdulhamid, Suleiman Ahmad and Olawale S. Adebayo
Department of Cyber Security, Federal University of Technology, Minna, Nigeria.
jkalhassan@futminna.edu.ng, abdulazeezhassant@futminna.edu.ng, shafii.abdulhamid@futminna.edu.ng, ahmads@futminna.edu.ng, waleadebayo@futminna.edu.ng

ABSTRACT
The rapid rate of technology advancement cannot be left unnoticed especially when it comes to the ICT sector. Ironically, this has also brought about an increase in cybercrime worldwide, thus forensic agencies and analysts are constantly on the move to investigate and acquire evidences at various crime scenes. Amongst all digital devices relating to forensic analysis, mobile phones are one of the most troublesome. Acquiring, decoding and presenting information resident in mobile device is a complex and challenging process. Several tools and methods both commercial and open source have been and are being developed to ensure authenticity and integrity in mobile forensic investigation and evidence acquisition. However, the level of result accuracy of these tools based on the mobile platform must be understood before even employing them in an investigation process. This paper examines the Android and Windows phone platform comparing the accuracy level of information extracted.

Keywords*: Forensic Analysis, Mobile Phones, Andriod Platforms, Windows Platforms,*

1. INTRODUCTION

Mobile devices or hardware no longer known as just equipment for voice communication but a complex gadget still for communication but now with capabilities of a computers and even more. Gadgets with remote innovations having the ability of a PC and a telephone holding notoriety on the internet today is the thing that we know as Smart phones, mobile devices have caused a revolution in nowadays communication. Smart devices are very popular and vital apparatus in our day to day activities , and also ever increasing number of individuals makes utilization of these gadgets, it raises a security issue in this way, making smart phones an important item in digital evidence forensics or vital thing in computerized prove crime scene investigation

Smart phones and related devices are now a critical component of the global ICT sector. Smart phones can run several applications and have the capability of connecting to the World Wide Web, also to other Internet based services. As the smart phone have now brought the internet even closer to the ordinary man, it could also play an important role in cybercrime investigation. Evidence from mobile phones has played an increasing role in recent years, mobile phone evidence are used in courts and also used to locate and apprehend suspects tagged to crime (mobile phones and SIM cards examination).

New technologies and innovations have led new intelligent smart phones 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). 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).
Also, the Windows mobile is another of platform, introduced with the Pocket PC 2002 operating system for Pocket PCs. Although in the broad sense of the term "Smartphone", both Pocket PC phones and Microsoft branded Smart phones each fit into this category. Today however Windows Mobile is more in tune with the 'Live' suite Microsoft are pushing, which has a dazzling array of onscreen informatics e-mail messages, tasks, appointments and ownership details. As with Windows XP, the taskbar holds the current time, volume connectivity status, and resource processing.
The accuracy of information extracted from different smart phone platforms can be better understood by comparing the results obtained from a carefully prepared test device. A comparison demonstrates the limitations of different platforms; assists a forensic examiner in justifying why different data sets are recovered from different mobile operating systems; and helps to detect defects in the forensic software.

There are a few advanced forensic devices accessible with regards to PC forensic and different gadgets some of which move toward becoming industry standard (FTK and EnCase), these devices are sufficiently bad with regards to mobile phones as the do not have the capacity to viably extricate information in mobilel phones which are unstable, holding significant proof in examination procedures.
. The amount, type and accuracy of information that can be retrieved from mobile phones vary based on the variety of platforms that exist today. The extraction of data form smart/mobile phone up until now has no standard method and investigators encounter difficulties handling cases involving mobile devices based on its intrusive nature. The modification, deletion, destruction of data on mobile devices is relatively easy when it is in use by a savvy criminal or a person with some knowledge, this poses a problem for a forensic investigator as data in mobile phone can go a long way as to prove the origin of a criminal activity.

Digital forensic investigator and analysts have become increasingly concerned with the non-standardization of the architectural framework mobile device platforms as it relates to extraction of data. Also with the developers of forensic tools as they tend to design in order to fit a variety of mobile phone thus reducing the accuracy level of result from one mobile device to the other. The accuracy of mobile forensic case files is coming under increased examination as a greater emphasis is being put on the ability to maintain the integrity of acquired data. Despite the fact that all mobile platforms offer similar functionalities, they differ considerably in the ways data is stored and rights to access these data as well as security and other settings and characteristics.

2. REVIEW OF RELATED WORKS

This paper is mainly focused on the literature review to establish a basis for this paper as a whole. Literature review starts off with the Android platform detailing the architecture followed by the Windows phone platform architecture. It begins with a brief background o smart phones and the type of evidence that are resident in them. Next we go into details about the extraction tool used to forensically retrieve data from our test devices.
Smart 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. Smart 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.

2.1 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 organization reports number of desktop owners declined and people are depending more on mobile phones and tablets (Janna Anderson, 2010). Today's 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.
Android is an operating system (OS) developed by the Open Handset Alliance (OHA). The Alliance is a coalition of more than 50 mobile technology companies ranging from handset manufactures and service providers to semiconductor manufacturers and software developers, including Acer, ARM, Google, eBay, HTC, Intel, LG Electronics, Qualcomm, Sprint, and T-Mobile. The stated goal of the OHA is to "accelerate innovation in mobile and offer consumers a richer, less expensive, and better mobile experience" (OHA, 2009, n.p.).

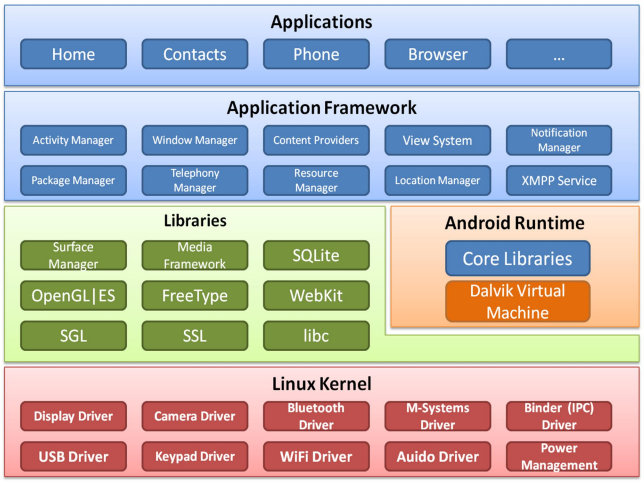

Figure 1: Android architecture

The basic architecture of Android is shown in the above figure. At its core, Android OS builds are based on the Linux 2.6 kernel. When running on a hard drive, the Linux system device defaults to the first physical hard drive, or /dev/hd0. In addition, Linux only understands character and block devices, such as keyboards and disk drives, respectively. With Linux on flash, however, a Flash Transition layer provides the system device functionality. A Memory Technology Device (MTD) is needed to provide an interface between the Linux OS and the physical flash device because flash memory devices are not seen as character or block devices (Dedekind, 2009).

The Android Runtime System utilizes the Dalvik virtual machine (VM), which allows multiple applications to be run concurrently as each application is its own separate VM. Android applications (the apps of today's common parlance) are compiled into Dalvik executable (.dex) files (DalvikVM.com, 2008). During a forensic examination one will be mainly concerned with the Libraries and, in particular, the SQLite databases. This is where one will find the majority of data that could be of interest in an investigation. Files can be stored on either the device's storage or on the removable secure digital (SD) memory card (Android.com, 2009b).

Unlike the typical desktop operating system, data or other files created by one Android app cannot automatically be viewed by other applications by default. The VM nature of Android allows each application to run its own process. Security is permissions-based and attached at the process level by assigning user and group identifiers to the applications. Application cannot interfere with each other without being given the explicit permissions to do so (Android.com, 2009a).

The security mechanisms of the Android OS could impede a forensic examination although some of the basic tools and techniques could allow investigators to recover data from the device. The first, most obvious step is to perform a traditional forensics analysis of the microSD card from the phone. This is the least effective method as it can only is access the data that apps directly store on the SD card. SD cards use the FAT32 file system and are easily imaged and examined using traditional forensics tools (including write-blocking hardware) (TalkForensics, 2009).

The Android file system is Yet Another Flash File System 2 (YAFFS2). YAFFS, developed in 2002, was the first file system designed for NAND (Not-AND) flash memory devices. YAFFS2 was designed in 2004 in response to the availability of larger sized NAND flash devices; older chips support a 512 byte page size whereas newer NAND memory has 2096 byte pages. YAFFS2 is backward compatible with YAFFS (Manning, 2002).

2.2 WINDOWS PHONE

Windows Phone (abbreviated as WP) is a smart phone operating system developed by Microsoft. It is the successor to Windows Mobile, although it is incompatible with the earlier platform. With Windows Phone, Microsoft created a new user interface, featuring a design language named "Modern" (which was formerly known as "Metro"). Unlike its predecessor, it is primarily aimed at the consumer market rather than the enterprise market. It was first launched in October 2010 with Windows Phone 7

WP utilizes a layered software and application architecture that is designed to run on multiple phones. To provide a consistent user experience and features that you can rely on, WP also defines a minimum set of hardware requirements that all WP phones must meet. Minimum hardware specifications include an ARM7 CPU, a DirectX capable GPU, a camera, and a multi-touch capacitive display. Standard sensors include: an A-GPS, an accelerometer, a compass, proximity and light sensors. There are three standard physical buttons on the phone – back, start and search. As we will see in a subsequent chapter, these buttons provide an easy and natural navigation model for the user.

WP Runtimes, i.e. Silverlight and the XNA Framework, along with Windows Phone -specific features, combine to provide a mature environment on which to build secure and graphically rich applications. WP Tools, namely Visual Studio and Expression Blend, create a complete developer experience for quickly creating, debugging, deploying and updating applications.

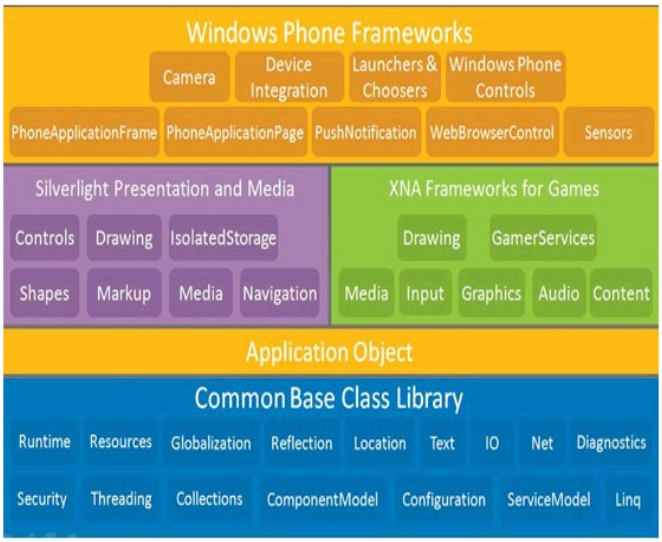

Figure 2: Windows phone framework

WP Cloud Services, i.e. Windows Azure, Xbox LIVE Services, Notifications services and Location services along

with a variety of other web services, allow developers to share data across the cloud and provides a seamless experience across devices. WP Portal Services and the Windows Phone Marketplace provide robust services allowing developers to register and certify and market their applications.

So far, there are only exploratory investigations of forensic approaches for WMSs. The Windows Mobile operating system has a number of similarities with the Windows desktop OS, including file system structure, directory layout and the common presence of many files and applications (Casey et al., 2010). WMSs use the Transaction Safe- FAT (TFAT) file system to manage persistent memory, which has a similar layout to the FAT file system on which it is based (Casey et al., 2010).

Whether it is a physical or a logical acquisition method used to examine a mobile phone, the problem identified from the literature is that different acquisition tools and methods recover different subsets of data from memory. This has left forensic investigators needing to use more than one tool to be confident that they are extracting all the evidence from the device they are examining. In addition, it is not clear that the superset of data recovered using all the different toolkits is consistent.

2.3 MOBILedit FORENSIC

MOBILedit Forensic is digital forensics product by Compelson Labs that searches, examines and report datas from GSM/CDMA/PCS cell phone devices. MOBILedit! connects to cell phone devices via an Infrared (IR) port, a Bluetooth link, Wi-Fi, or a cable interface. After connectivity has been established, the phone model is identified by its manufacturer, model number, and serial number (IMEI) and with a corresponding picture of the phone.

This forensic tool makes it possible to view, search or retrieve all data from a phone with only a few clicks. This data includes call history, phonebook, text messages, multimedia messages, files, calendars, notes, reminders and application data such as Skype, Dropbox, Evernote, etc. It will also retrieve all phone information such as IMEI, operating systems, firmware including SIM details (IMSI), ICCID and location area information. Where possible MOBILedit Forensic is also able to retrieve deleted data from phones and bypass the passcode, PIN and phone backup encryption.

Data acquired from cell phone devices are stored in the .med file format. After a successful logical acquisition, the following fields are populated with data: subscriber information, device specifics, Phonebook, SIM Phonebook, Missed Calls, Last Numbers Dialed, Received Calls, Inbox, Sent Items, Drafts, Files folder. Items present in the Files folder, ranging from Graphics files to Camera Photos and Tones, depend on the phone's capabilities. Additional features include the myPhoneSafe.com service, which provides access to the IMEI database to register and check for stolen phones

MOBILedit is a platform that works with a variety of phones and smart phones (a complete list of supported handsets is available on the manufacturer's website) and explores contents of the phone through a MS Outlook-like folder structure. This allows backup of the information stored on the phone, storing it on a PC or copy data to another phone via Phone Copier feature.

Figure 3: MOBILedit forensic version 7.5

3. RESEARCH METHODOLOGY

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 weight-age will be in question and eventually less chances that these can be proved in the court.

3.1 DATA COLLECTION

The collection of data is the basis on which this paper lies. Since it is a comparison of the accuracy level of data collected from two different smart pone platforms, as much data as possible is being extracted from both devices using the same extraction tool and then visually represented for 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 the smart phone 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.

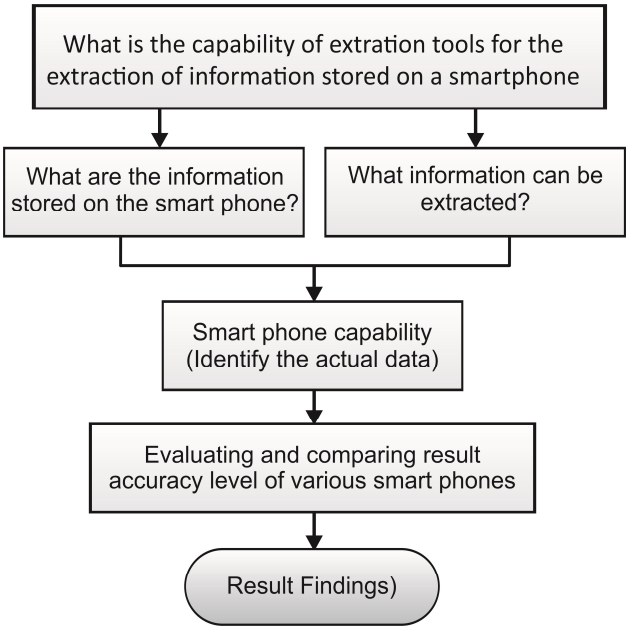

Figure 4: Data collection map-

In general, the same forensic principles that apply to any computing device also apply to mobile devices in order to enable others to authenticate acquired digital evidence. Recall that the purpose of a forensically sound process is to document that the evidence is what you claim and has not been altered or substituted since collection. At a minimum, all steps taken to extract data should be recorded to support transparency and repeatability, enabling others to assess and repeat your work. In addition, the MD5 hash of acquired data should be calculated and documented, allowing others to verify that nothing has been altered since the data were acquired. Any issues encountered during the acquisition process should also be noted, even when they are embarrassing or the cause is unknown. Documentation must also show continuous possession and control throughout its lifetime. Therefore, it is necessary not only to record details about the collection process, but also every time it is transported or transferred and who was responsible.

Keep in mind that some devices can receive data through wireless networks that might bring new evidence but might overwrite existing data. Therefore, an investigator must make a calculated decision to either prevent or allow the device to receive new data over wireless networks. Removing the battery from a mobile device will prevent it from communicating but may also activate security measures such as lock codes and encryption that could prevent further access to data on the device. In addition, when using acquisition methods that require the mobile device to be powered on, it is necessary to isolate the mobile device from networks.

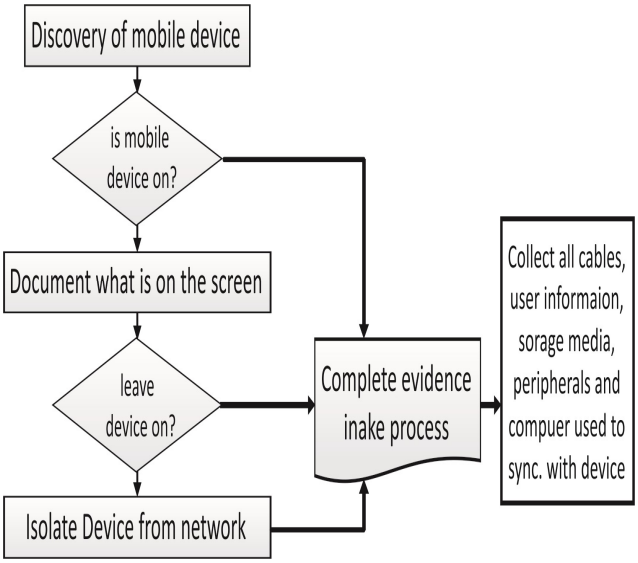

Figure 5: Flowchart for mobile device handling

Network separation or isloation guarantees that the contents of a phone mirror the time at which it was seized, refusing changes that may happen to it after it has been seized. Activities over the system that can change content include using phone to receive calls, messages,network activities, and the utilization of remote deletion systems; the last being an enterprise features include intended for corporate handset (smart phones). Such activities in the network can change the contents of smartphones, conceivably including new information or data, overwriting existing information or unallocated space, or deleting the phone content remotely.

4. RESULTS AND DISCUSSION

In undertaking the study, it is necessary to define the types of data that can be retrieved form a smart phone using a forensic tool. As we earlier said, smart phones vary in several ways based on the manufacturer specification, in

contrast they are certain common information that can be extracted and this is notable in all smart phones:

- Contact information
- Short Message service
- Multimedia message service
- Call logs
- Files
- User files
- Photos
- Videos
- Recording

However the security level of an advanced mobile phone can confine extraction of these normal data as found in this examination. Our scientific device utilized was not able concentrate data from the windows phone(Nokia lumia 620), because of the expanded security as it identifies with the collaboration with the measurable apparatus

.

4.1 ANDROID EXTARCTION

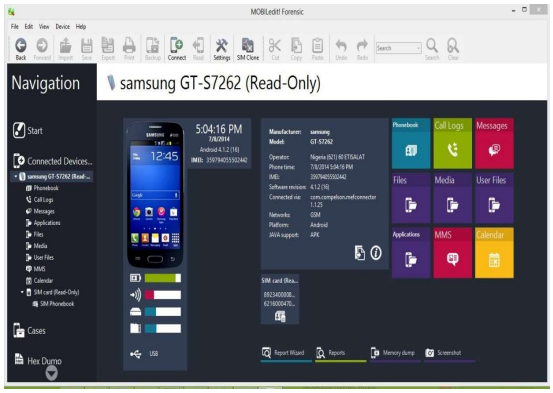

Figure 6: Android phone connection with the forensic tool (MOBILedit)

FIGURE 7: ANDROID PHONE DETAILS/INFORMATION EXTRACTED BY MOBILEDIT

4.2 WINDOWS PHONE EXTARCTION

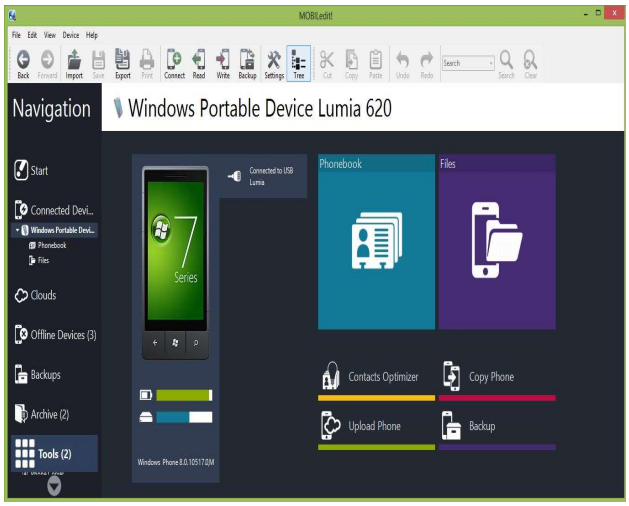

FIGURE 8: WINDOWS PHONE CONNECTION WITH THE FORENSIC TOOL (MOBILEDIT) AND PHONE DETAILS/INFORMATION

5. COMPARISON OF ACCURACY OF RESULT OF FORENSIC ON ANDROID AND WINDOWS PLATFORMS

Table 1: Comparison of accuracy result

INFORMATION	ANDRIOD	WINDOWS PHONE
PHONE INFORMATION	✓	✓
Manufacturer	✓	✓
Model	✓	✓
Operator	×	×
Phone time	×	×
IME	✓	✓
Software version	✓	×
Hardware version	×	✓
Networks	✓	✓
Platform	✓	✓
PHONEBOOK	✓	✓
CALL LOGS	✓	×
MESSAGES	✓	×
MMS	✓	×
FILES	✓	✓
USER FILES	✓	×
APPLICATION	✓	×
CALENDER	✓	×
MUSIC	✓	✓
VIDEOS	✓	✓
AUDIO(RECORDINGS)	✓	✓

Trying to get data for information that you can use to incriminate or exculpatory evidence requires patience because it can be time consuming or exculpatory confirmation takes persistence and can be tiring. A few tools have a basic serch engine that matches an information content or input text string precisely, permitting just for basic inquiries to be performed. Some tools incorporate more intelligent feature and rich search engines, making it easy for generalized regular expression patterns (grep), type searches, which include wildcard matches, filtering of files by extension, directory and batch scripts that search for specific types of content.

A new smart phone platform is always a challenge for forensic investigators and Windows Phone 7 is no exception. The main problem preventing investigators to access data on Windows Phone 7 devices is the limited access rights of normal user apps, in particular the isolated storage. However, this obstacle can be circumvented by methods already available in the internet community, e.g. through the use of native DLLs and simplified app installation methods. When these mechanisms are combined, a small set of tools can be installed on the device that allow for the acquisition of the file system and other system data. Once this data is available, it can be further analyzed. As a result, a large amount of interesting data can be obtained from a Windows Phone 7 phone, for instance emails of the user, SMSs, Facebook contacts or web pages visited with Internet Explorer.

6. FURTHER EXAMINATION AFTER DATA ACQUISITION

Once a duplicate of the acquisition results is accessible, the subsequent stages include looking or searching for data, distinguishing/identifying evidence or proof, making bookmarks, and developing the contents of your final report. At this stage, your knowledge and experience with the available tools used for examination are extremely very valuable, since your proficiency in using the available features and abilities of a forensic tool itself can extraordinarily speed the examination procedure.

Ownership and possession: Identify the people who made, changed, or acessed to a files, and the possession and ownership of questioned data or information by putting the subject with the gadget at a specific time and date, finding records of interest for non-default areas, retrieving passwords that demonstrate ownership or possession, and recognizing contents of documents or files that are particular to a user.

Application and file analysis – Identify information relevant to the investigation by examining file content, correlating files to installed applications, identifying relationships between files (e.g., e-mail files to e-mail attachments), determining the significance of unknown file types, examining system configuration settings, and examining file metadata (e.g., documents containing authorship identification).

Timeframe analysis – Determine when events occurred on the system to associate usage with an individual by reviewing any logs present and the date/time stamps in the file system, such as the last modified time. Besides call logs, the date/time and content of messages and e-mail can prove useful. Such data can also be corroborated with billing and subscriber records kept by the service provider.

Data hiding analysis – Detect and recover hidden data that may indicate knowledge, ownership, or intent by correlating file headers to file extensions to show intentional obfuscation; gaining access to password-protected, encrypted, and compressed files; gaining access to steganographic information detected in images; and gaining access to reserved areas of data storage outside the normal file system.

7. CONCLUSION

The main aim of this work was to acquire a better comprehension of the outcome of accuracy level of two well known mobile device using just one often use mobile forensic tool. These two mobile phones are using very popular operating systems (Android and Windows mobile phone) for smart phones around the world. Results or findings were mixed and it was deducted that the precision or acuuracy level of result extracted from the smart phones varies from these two different platforms. Additionally from the results, no single forensic tool can be exclusively depended upon to gather and present each thing of potential proof from a smart mobile gadget.

During this study, both innovative features and limitations were found. Some of the more innovative features the forensic tool presented included hex dump, file signature analysis on mobile devices to detect files with non-standard extensions, extraction of data (e.g. contacts, calendar) from multiple original sources and comprehensive collection of web records beyond the default browser. Limitations found included the requirement to ‘root’ a phone, which would result in the destruction of the data stored on the device, hard limits for the collection of text data from a mobile device and incoherent display of data making comparison of data such as contacts and messaging difficult, if not impossible. These limitations are not insurmountable as it is assumed that given time, many of them will be overcome as the mobile forensics tools are updated and upgraded. Due to

the sheer number of different handsets entering the world market, it is very unlikely that every tool will have the ability to support all phones as demonstrated in this study.

It should be noted that results may vary when analysing mobile devices that use operating systems designed for use by many different manufacturers (e.g. Android). Manufacturers will often customize their implementation of the operating system, which can result in data being stored in different locations to the standard operating system conventions (e.g. HTC Sense and Samsung TouchWiz).

To successfully collect the maximum amount of data from a mobile device, investigators and practitioners need to be aware of the key features and limitations of the tools they use and also the varying architecture employed by different manufacturers. This will allow them to make informed selections in an environment where timeliness is often critical and workloads are high. However, forensic tools are constantly updated to provide support for new devices and expand support for existing devices.

Finally, mobile forensic tools in the market today extract more vital and volatile information by interacting with the device which in itself can render the evidence inadmissible. Thus, these forensic tools should be subjected to basic admissibility guidelines, such as those introduced by Daubert, in determining the legal relevance of the tool and its results.

REFERENCES

[1]. Rehault, F. (2010). Windows mobile advanced forensics: An alternative to existing tools. Journal of Digital Investigation, 7(1–2).

[2]. Casey, E., Bann, M., & Doyle, J. (2009). Introduction to windows mobile forensics. Digital Investigation, 6(3–4).

[3]. McCarthy, P. (2005). "Forensic Analysis of Mobile Phones." Retrieved February 20, 2008, from http://esm.cis.unisa.edu.au/new_esml/resources/publications /forensic%20 analysis%20of%20mobile%20phones.pdf

[4]. Paraben Corporation. (2007b). "Frequently Asked Questions for Device Seizure." Retrieved February 29, 2008, from http://support.paraben.com/devicefaq.html

[5]. Ayers, R., Jansen, W., Moenner, L., Delaitre A.: Cell Phone Forensic Tools: An Overview and Analysis update, NISTIR 7387 (2007).

Lee S, Kim H, Lee S, Lim J. Digital evidence collection process in integrity and memory information gathering. Systematic Approaches to Digital Forensic Engineering 2005:236–47.

[6]. Chen S, Yang C. Design and implementation of live SD acquisition tool in Android smart phone. In: Fifth international conference on genetic and evolutionary computing 2011. p. 157–62.

[7]. Ayers, R, Jansen, W. (2005). An overview and Analysis of PDA Forensics Tool. The International Journal of Digital Evidence, 2005.

[8]. Canalys research release, "Google's Android becomes the world's leading smart phone platform", http://www.canalys.com/pr/2011/r2011013.html (2011, accessed on 28 February 2011)

[9]. "Wikipedia", [Online] Available: http://en.wikipedia.org