Towards a Unified Forensic Investigation Framework of Smartphones

S. H. Mohtasebi and A. Dehghantanha

***Abstract*—In recent years advanced capabilities of smartphones have enabled their users to store and manage copious information about their personal and professional life. Consequently, any seized smartphone might involve some useful evidence.**

However a wide variety of manufacturers, different operating systems, enormous hardware components and a huge number of programs that smartphones are using make it difficult to reach a unified forensic framework for all models.

This paper firstly reviews the previous works on remote and local data acquisition methods from smartphones. Afterwards, it reports difficulties in analyzing and examining retrieved data from smartphones. Additionally, it evaluates current forensic investigation process models in relation to smartphones in order to find a suitable model that can be applied to all smartphones forensic investigations.

This paper proposes solutions for addressing data acquisition, data examination, and investigation process model to ultimately come towards a unified framework for investigation of smartphones.

***Index Terms*—Mobile forensics, smartphone investigation, forensic framework.**

I. Introduction

Based on statistics published by Gartner [1] in the third quarter of 2010 smartphone sales have been raised to 96 percent from the third quarter of 2009. It is also expected that the number of smartphone users exceeds to the one billion by 2013 [2].

Smartphones with sophisticated capabilities and features facilitate storing different kinds of information of their owners and any piece of this information is potentially precious evidence.

In spite of many similarities between smartphones, the structure and configuration of each model is different from another one. There are a wide variety of operating systems, applications, and hardware components that are used in different models of smartphones. Additionally, a lot of worthy information stored on smartphones is volatile.

Notwithstanding existence of different software and hardware tools for data gathering from cell phones, none of them can recover all data without making alteration.

Moreover, almost every day new applications for smartphones are released. Even if the data is being successfully recovered, still there might be various barriers in examining some data like encrypted ones.

Another major issue in smartphone forensics is non-existence of any widely accepted standard investigation process model.

This paper reviews two common data acquisition methods to find a proper approach for gathering data from smartphones. Data examining and its obstacles to smartphone forensics are other issues that this paper encompasses. Furthermore, this paper evaluates two investigation process models that are introduced for investigation of Windows Mobile and Symbian operating systems to find an appropriate model which is capable of being employed in all smartphone forensic investigations.

Manuscript received October 1, 2012; revised November 12, 2012. This work was supported by Asia Pacific University College of Technology and Innovation.

The authors are with Asia Pacific University College of Technology and Innovation, Kuala Lumpur, Malaysia (e-mail: shomhtasebi@gmail.com, ali_dehqan@ucti.edu.my).

II. Literature Review

The crux of smartphone forensics is narrowing down the following issues:

Determining the most appropriate data acquisition method;

Examining collected data in an effective way;

Finding a reliable investigation process model.

The rest of this section encapsulates previous works have been done in these areas.

A. Data Acquisition Methods

There are two common methods in smartphone data acquisition as follows:

Remote data acquisition: In this method, the investigator collects data from the smartphone by either running a forensic software tool on a workstation or employing a forensic device [3]-[5]. In remote data acquisition, the smartphone needs to be connected to the workstation or the device through a cable or wireless protocols such as Bluetooth and infra-red. An example of the tools using this method is Paraben Device Seizure [6].

Local data acquisition: In this method, a forensic software tool is installed on the cell phone and it copies stored data to a removable memory. Mobile Internal Acquisition Tool (MIAT) [7] is an exemplar of this method which requires only a read-only permission to the internal memory file system by layering on the operating system APIs and obtains the smartphone data such as SMSs, contacts, etc.[7]. At the end of the execution, a logical image of the smartphone file system is saved on the selected removable storage volume [7].

Smartphones normally use three memory locations for storing the data [3]:

Subscriber Identity Module (SIM) card - It is the identification of the user in its provider network. SIM card is also capable to store small amounts of information such

as the phonebook entries and SMS messages [8].

- Memory card - It is employed as an extra memory for storing data.
- Internal memory - It comprises of the following three components [4]:
  1) ROM memory that keeps the operating system boot image;
  2) RAM memory which stores the running processes data. Data stored on RAM is highly volatile as it is unobtainable when the smartphone gets off;
  3) Flash memory that the user data are saved on that.

Forensic tools that are used for computing data acquisition can be also employed for gathering data from memory card. Additionally, there are a wide range of forensic tools that are appropriate for SIM card data acquisition [9]. Data stored on memory card or SIM card are classified under non-volatile data since the data can be retrieved even after turning off the smartphone.

The most profound problem in data acquisition relates to recovering data from the internal memory as it is organized as a unique block memory chip which is roughly impossible to isolate it for analyzing in a low level [3].

Distefano et al. [3] compared the MIAT acquisition performance with Paraben Device Seizure on Nokia N70 [10] and Nokia 6630 [10] which their result is presented in Table I.

TABLE I: THE OVERALL TIME OF GATHERING DATA BY MIAT AND PARABEN DEVICE SEIZURE

Exp. No.	Device	Tool	Time (min)
1	Nokia N70	MIAT	≈ 12
		Paraben	≈ 8
2	Nokia 6630	MIAT	≈ 50
		Paraben	≈ 15

The outcomes of this comparison demonstrate that the execution time in MIAT is highly dependent on the performance and capabilities of the cell phone itself [3].

Furthermore, MIAT corrupted a few number of operating system files, although they have an insignificant role in forensic analysis [3]. However Paraben had corrupted some files as well [3].

This comparison can be generalized to remote data acquisition method versus local data acquisition method as long as Paraben Device Seizure is considered as a remote method and MIAT is categorized as a local method.

To evaluate these two methods better, we have also referred to prerequisites of data acquisition methods mentioned by Mokhonoana et al. [5]. As they remarked any data acquisition method must fulfill the following requirements:

- It should minimize alteration to the device.
- It should recover data as far as possible.
- It should minimize investigator interaction with the smartphone.

With regard to the aforementioned comparison, local data acquisition method can be used simultaneously since it only needs a memory card [3]. Moreover, unlike remote data acquisition method which has a partial access to the system files as it relies on the communication protocol, local data acquisition manages data acquisition directly [3].

It is also obvious that local data acquisition method does not require many computing equipments [5], since the forensic investigator just connects a memory card and installs the tool on the target smartphone. But at the same time as it needs to be loaded on the target smartphone, it might modify data stored on the device [5]. Additionally, for each different series or model of smartphones, it must be recompiled [11].

As local data acquisition method can be quickly put on and it, thereby, reduces the possibility of occurring events such as appointment remainders and messages incoming before accomplishing the acquisition [3]. Nonetheless unlike remote method, the speed of the local method is extremely reliant on the cell phone performance [3].

Local data acquisition method needs to be supported by the target smartphone, while in remote method only communication protocols require to be compatible with the smartphone and since remote based forensic tools mostly employ common protocols this dependency is less obvious compared to local based tools [3], [4].

Broadly speaking, local data acquisition method is very helpful in situations where many smartphones need to be investigated expeditiously and there are not enough resources available. The major setback of the remote acquisition tools is they need to be supported on the target smartphones.

B. Data Examination

Examining the recovered data is another demanding issue in smartphone forensic investigations. There are a wide variety of smartphone manufacturers in the market each of which uses their own applications, hardware components, and operating systems. Smartphones operating systems are also different from the embedded operating systems that are run on normal cell phones as smartphones operating systems allow native third party applications to be run on their hardware [5]; which makes the situation more complex. Since many companies and individual developers sell and share their own applications, everybody can install any supported program on their smartphone.

The App Store [12], the BlackBerry App World [13], the OVI Store [14], the Palm App Catalog [15], and the Windows Marketplace for Mobile [16], each of which includes lots of programs developed by third parties for iPhone, BlackBerry, Nokia, Palm, and mobile phones that host Windows Mobile/Phone operating systems respectively.

Moreover, continual improvements in smartphones capabilities and memory capacities persuade users to run more applications that each of which might potentially involve precious information related to the investigation case. However the way an application stores its data on the smartphone is not only dependent on the operating system structure. For instance, the application may encrypt data before saving it. These kinds of circumstances might make it difficult for forensic investigator to examine the data from application without making any alteration.

Husain et al. [17] studied AOL Instant Messenger (AIM) [18], Yahoo! Messenger [19] and Google Talk [20], (in both client based and web based versions) on Apple iPhone. They were able to recover data from the iPhone through

Apple iTunes and discover some useful data contained usernames, passwords, and conversation logs associated with some of these instant messaging applications.

The diversity in structure of each operating system and smartphone makes programmers and companies develop different applications for each smartphone model or at least for each series of models. In [17] case, they tested Yahoo! version 1.1 while Yahoo! has not released any client based messenger for other smartphones models and available client based Yahoo Messengers that are run on other smartphones are developed by third parties developers and expectedly their structures are different. They [17] gathered the data through iTunes which clearly cannot be employed for any smartphone produced by manufacturers other than Apple. This example shows that regarding a wide variety of application released everyday and multiple versions of different operating systems making a comprehensive standard for examining all data is almost impossible.

C. Investigation Process Models

Association of Chief Police Officers (ACPO) [21] advices four principles regarding cell phone seizure and examination, briefly explained below:

Principle 1: Data that is held on the cell phone must not be altered and consequently it may be acceptable in the court.

Principle 2: In some situations investigator may find it necessary to access the original data stored on the cell phone. In these cases, investigator must be proficient enough to do so and be able to give evidence explaining the relevance and the implications of their actions.

Principle 3: The logs of actions of all processes applied to the cell phone should be taken and conserved. Same result must be achieved if an independent third party examines the evidence.

Principle 4: The person in charge of the investigation is responsible for making it certain that the law and the principles are stuck to.

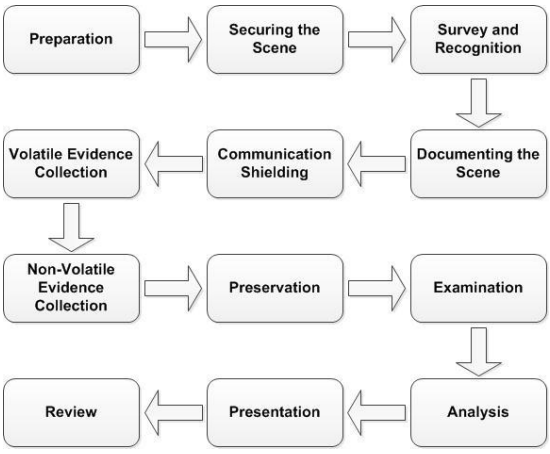

Fig. 1. Phases of Windows Mobile Device Forensic Model

Adhering to the mentioned principles assures that the integrity of the digital evidence in its entire life cycle is not compromised [9]. Thus forensic investigators need to follow a structural investigation model that relies on these principles as well as technical matters.

To the best of authors' knowledge, there is no widely accepted standard investigation process model in smartphone forensics. However there are some works have been done by other researchers which are very close to this area. Fig. 1 illustrates a twelve-stage model for Windows Mobile forensic [22].

There is also a process model for forensic analysis of Symbian smartphones [23] as shown in Fig. 2.

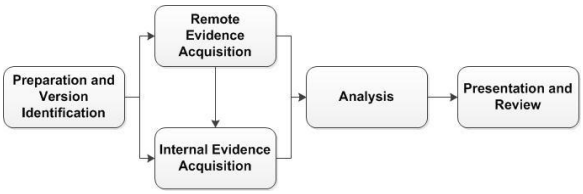

Fig. 2. Phases of Symbian Smart phones Forensic Process Model

Notwithstanding similarities between these two models, they differ in certain areas. Both of these models have preparation phase. However in Symbian model only technical issues related to Symbian operating system is considered, while Windows Mobile model involves more forensically sound matters such as organizing the necessary tools needed for investigations of mobile electronic device as well as obtaining search warrants [22].

Securing the scene, survey and recognition, documenting the scene, and communication shielding are four phases that are covered only in Windows Mobile model. As the name implies securing the scene is about protecting the crime scene and conserving the cell phone from being compromised. The next phase is about evaluating the scene in order to find any potential evidence source and also conducting preliminary interviews with people in the scene. Documenting properly, photographing, sketching, mapping the crime scene, and keeping a log of people on the scene are the main activities must be done in the fourth phase of Windows Mobile model. Communication shielding phase involves isolating the cell phone and disabling all its communication features [22].

Evidence acquisition phase is common between both Symbian and Windows Mobile models. In Windows Mobile model the author [22] recommends collecting data from volatile evidence (such as data stored on RAM). Evidence acquisition in Symbian model is divided into two remote and internal parts. Internal evidence acquisition is applicable when the investigation target is early Symbian smartphones without Trusted Computing Base (TCB) [23].

Preservation is another phase which is stated only in Windows Mobile model. It is about employing procedures that protect collected digital evidence from being altered. Labeling potential evidence sources, using suitable bags for packing, and using chain of custody are some examples of this phase activities [22].

The ninth and tenth phases of Windows Mobile model are examination and analysis respectively. In the examination phase of Windows Mobile the collected evidence by forensics investigator must be examined and all the data including deleted, hidden, etc. must be detected. Afterwards, in analysis phase the connection of the fragmented and hidden data should be discovered. These activities lead the investigation to reconstruct the events with regard to the retrieved data [22].

In Symbian model these two phases are combined into a single phase called analysis. Accordingly the data should be extracted from the memory of the smartphone and then it should be disassembled in order to cope with the code and password in consequence to crack mobile phone [23].

Both Windows Mobile and Symbian models cover Presentation and Review phases. Although in Symbian model these two stages appears as a single phase [22], [23].

Overall, Windows Mobile model involves more detailed phases and perfectly relies on ACPO principles.

III. Proposed Framework

In spite of many advantages of local data acquisition method, it cannot be employed in all smartphones as it needs to be supported by the target smartphone. Remote data acquisition method, on the other hand is supported by more smartphones. However it requires further resources compared to local method. Additionally, neither local nor remote methods can preserve 100 percent of the integrity of the data held on the internal memory of the smartphone. To narrow down these issues, applying both methods is advised. It enables forensic investigators to gather data as quickly as possible by using a local method tool in urgent cases that the smartphone is supported by the tool.

Moreover, computing forensic tools such as Forensic Toolkit [24] can be employed for gathering and examining the data stored on the smartphone permanent storage devices (e.g. memory card). Using SIM card forensic tools such as SIMCon [25] are also appropriate way for retrieving SIM card data.

To resolve matters stated in Data Examining subsection, it is recommended that a set of guidelines to be made for each model or at least a series of smartphones. Each set of guidelines should specify:

- Appropriate forensic tools for examining all data including default applications stored data;
- Authentication mechanisms and techniques for bypassing them.

It should guarantee that forensic investigators will be able to successfully examine and analyze at the very least data linked to the applications installed by default on the smartphone.

Since any digital evidence for being relied on in court needs to be recovered and examined within the law and forensic principles such as those stated in ACPO, Windows Mobile model appears a suitable investigation process model for investigation of smartphones.

By including tools used for investigating smartphones with operating systems other than Windows Mobile, preparation phase of Windows Mobile model can be generalized to all smartphones.

Securing the scene, survey and recognition, documenting the scene, and communication shielding phases of Windows Mobile model are applicable to investigation of all smartphones.

While methods stated in the Data Acquisition Methods subsection can be used in volatile evidence collection phase for gathering data from any model of smartphones, computing and SIM card forensic tools can be involved in non-volatile evidence collection phase.

Preservation phase is another Windows Mobile model phase that can be used for investigation of all smartphones.

Examining recovered data, on the other hand is greatly dependent upon the smartphone model, operating system, and installed applications. Therefore examination phase of each model should be based on a set of guidelines that meet the requirements stated earlier in this section.

Analysis, presentation, and review phases of Windows Mobile model are valid for investigation of all smartphones.

IV. Analysis of the Proposed Framework

Both local and remote data acquisition methods have difficulty in supporting some models of smartphones. Therefore, it is not possible only one method to be chosen for investigation of all models. Even though tools based on local method can speed up the investigation process especially when data gathering is done in a crime scene, but employing both methods for supported smartphones are recommended as it reinforces the validity of the recovered data.

Furthermore, forensic tools used for computing related investigations and SIM card forensic tools can forensically recover many data from permanent storage devices and SIM cards respectively.

About data examination, although preparing a set of guidelines for each smartphone model is a very time consuming task and even difficult in anomalous smartphones for example fake models, but on the other hand it saves a lot of time of investigators during the examination particularly in challenging situations such as when data is encrypted. Without using guidelines investigators have to either put much time and energy to find a solution for examining or ignore some data which each piece of that might potentially involve precious evidence. Specific set of guidelines for each model also helps forensic investigators to take advantage of resources and solutions provided by the guidelines in order to conquer problems associated with non-default programs.

Concerning investigation models, Windows Mobile investigation process model, by applying some changes can be used for investigating all smartphones. However technical issues of smartphones that are equipped with operating systems other than Windows Mobile should be considered in preparation, volatile evidence collection, and non-volatile evidence collection phases. Moreover, examination phase, unlike the other phases, cannot be generalized because of the reasons described above. Thus examination of each model of smartphones should be customized based on the prepared guidelines on that specific model.

V. Conclusion and Future Works

Among data acquisition methods we found remote method more practical as tools linked with this method are compatible with many smartphones compared to local data acquisition tools. However local data acquisition tools such

as MIAT need less resource and can be put on more rapidly. Employing both local and remote methods in supported smartphones strengthens the credibility of the gathered data.

In the next step, we will look into the smartphone forensic tools to identify the most suitable tools of each data acquisition method.

With regard to vast diversity in smartphones manufacturers, operating systems, and applications, making a set of guidelines for each smartphone model or at least for each series of models appears to be the only solution for effectively examining and analyzing the recovered data.

Further researches can be undertaken in order to discover common non-default programs run by users of each smartphone models. It will help forensic investigators to study how to deal with the data of those programs.

Comparing Windows Mobile investigation model with Symbian investigation model shows that the first model, by considering some changes, is an appropriate model for forensic investigation of smartphones. Its twelve phases, at least in theory, are adhered to legal issues as well as forensic principles such as APCO.

In view of the fact that this model has been made particularly for Windows Mobile operating systems, in the future, we will try to adopt its preparation, volatile evidence collection, and non-volatile evidence collection phases to other operating systems by studying their specifications and limitations.

REFERENCES

[1] Gartner. (2010, Nov. 10). Gartner Says Worldwide Mobile Phone Sales Grew 35 Percent in Third Quarter. 2010. [Online]. Available: http://www.gartner.com/it/page.jsp?id=1466313

[2] Informa. (2010, Sep. 20). One Billion Subscribers to Own Smart Phone Devices in 2013. [Online]. Available: http://www.informatm.com/itmgcontent/icoms/s/press-releases/20017810274.html

[3] A. Distefano and G. Me. (2008, August). An overall assessment of mobile internal acquisition tool. *DFRWS. Digital Forensic Research Workshop* Baltimore, *MD*. [Online]. Available: www.dfrws.org/2008/proceedings/p121-distefano.pdf

[4] G. Me and M. Rossi, "Internal forensic acquisition for mobile equipments," in *Proc. International Parallel and Distributed Processing Symposium*, 2008, pp.1-7.

[5] P. M. Mokhonoana and M. S. Olivier, "Acquisition of a symbian smart phone's content with an on-Phone forensic tool," in *Proc. Southern African Telecommunication Networks and Applications Conference*, Sugar Beach Resort, Mauritius, 2007.

[6] Paraben device seizure. [Online]. Available: http://www.paraben.com/device-seizure.html

[7] Mobile internal acquisition tool. [Online]. Available: http://www.miatforensics.org/index.php

[8] A. Martin. (2008). Mobile device forensics. *SANS*. [Online]. Available:http://www.sans.org/reading_room/whitepapers/forensics/mobile-device-forensics_32888

[9] W. Jansen and R. Ayers, "Guidelines on Cell Phone Forensics," *National Institute of Standards and Technology*, 2007.

[10] Nokia. [Online].Available: http://www.nokia.com

[11] MIAT Use Case Specification: Internal Memory Data Collection. (2009, June 27). *MIAT* [Online]. Available: http://www.miatforensics.org/contents/pdf/UCS_InternalMemoryDataCollection.pdf

[12] Apps for iPhone. [Online]Available: http://www.apple.com/iphone/apps-for-iphone

[13] Blackberry - app world. [Online]. Available: http://us.blackberry.com/apps-software/appworld

[14] Ovi by nokia. [Online]. Available: http://www.ovi.com

[15] HP Palm developer center. [Online]. Available: http://developer.palm.com

[16] Windows marketplace for mobile shop apps. [Online]. Available: http://marketplace.windowsphone.com/Default.aspx

[17] M. I. Husain and R. Sridhar, "iForensics: forensic analysis of instant messaging on smart phones," in *Proc. International Conference on Digital Forensics & Cyber Crime*, Albany, 2009.

[18] AOL Instant Messenger. [Online]. Available: http://www.aim.com

[19] Yahoo! Messenger. [Online]. Available: http://messenger.yahoo.com

[20] Google Chat. [Online]. Available: http://www.google.com/talk

[21] *Good Practice Guide for Computer-Based Electronic Evidence*, Association of Chief Police Officers, 2010.

[22] A. Ramabhadran. Forensic investigation process model for windows mobile devices. [Online]. Available: http://www.forensicfocus.com/downloads/windows-mobile-forensic-process-model.pdf

[23] X. Yu, L. Jiang, H. Shu, Q. Yin, and T. Liu, "A process model for forensic analysis of symbian smart phones," in *Proc. ASEA*, 2009, pp. 86-93.

[24] Forensic Toolkit (FTK). [Online]. Available: http://accessdata.com/products/forensic-investigation/ftk

[25] SIMconForensics. [Online]. Available: www.simcon.no

Seyed Hossein Mohtasebi holds a B.S. degree in Information Technology with specialism in Forensic Computing from Asia Pacific University College of Technology and Innovation and is MCSE and MCITP certified. He is currently working with Shabakeh Gostar Co. as a security engineer.

Ali Dehghantanha holds Ph.D degree in Computer Science with specialism in Security in Computing from University Putra Malaysia and currently is working in UPM as senior-lecturer.