International Journal of Digital Information and Wireless Communications (IJDIWC) 1(3): 688-692
The Society of Digital Information and Wireless Communications, 2012(ISSN 2225-658X)

Smartphone Forensics: A Case Study with Nokia E5-00 Mobile Phone

SeyedHossein Mohtasebi
Asia Pacific University College of Technology and Innovation
Kuala Lumpur, Malaysia
shmohtasebi@gmail.com

Ali Dehghantanha
Asia Pacific University College of Technology and Innovation
Kuala Lumpur, Malaysia
ali_dehqan@ucti.edu.my

Hoorang Ghasem Broujerdi
Asia Pacific University College of Technology and Innovation
Kuala Lumpur, Malaysia
hoorang@ucti.edu.my

Abstract— **In the past few years, there has been an exponential increase in the number of smartphone users. By its very nature, smartphone saves and manages vast amount of information pertaining to its owner. As a result, this ubiquitous device is being regarded as a valuable evidence item in forensic investigations. Nevertheless owing to disparity in smartphone models, retrieving whole data from all models using predefined instructions and tools is not always possible. This paper studies demo or trial versions of four widely 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 smartphone. The result of this paper presents that existing toolkits are deficient to gather volatile data as well as deleted information.**

Keywords-component; Mobile forensics; smartphone; data acquisition

I. INTRODUCTION

According to Berg Insight [1], smartphone users grew by 38 percent in 2010, reaching an estimated 470 million active users and it is predicted this number will increase to 2.8 billion by 2015. In addition to common capabilities that all mobile phones have, a smartphone enables its user to store and organize a tremendous range of personal and business data and above all keeps them frequently connected to the Internet. Consequently, many communications and activities that user is engaging on are being, somehow, witnessed by this device. Therefore, a profile of user and last deeds done by them would be revealed by a proper forensic investigation.

However, different companies manufacture smartphones and over and above existence of several operating systems (OS), copious range of components and applications are installed on each model. Forensic examiner, thereby, has to attempt various tools in order to gather the maximum amount of data from each model.

The main contributions of this paper are to experiment and compare prominent trial and free mobile forensics tools in investigation of a Nokia E5-00 smartphone and propose a framework of effective examination of this model model. The remainder of this paper is organized as follows: Section II reviews Nokia E5-00 specifications, Symbian OS, and digital forensics principles. It also outlines forensic tools employed in this research. Section III presents the experimental results of the studied tools and the outcomes are analyzed in Section IV. In section V a framework of forensic investigation of Nokia E5-00 smartphone is proposed. Finally, Section VI concludes the work and describes possible future work.

II. II. LITERATURE REVIEW

This section briefly reviews the structure and specifications of Nokia E5-00 and Symbian OS focusing on elements that affect investigation process. It also delves into principles and concerns associated with mobile forensics. The section eventually explores prominent free and trial forensic tools that are applicable to investigating smartphones.

A. *Nokia E5-00 Specifications*

The internal flash memory of Nokia E5-00 stores up to 250 MB data [2]. This smartphone is also equipped with NAND and SDRAM memories with, respectively, 512 MB and 256 MB capacity [2]. Micro Secure Digital (SD) memories with up to 32 GB capacity are compatible with Nokia E5-00 and by default a 2 GB microSD card is included in each package [2]. Its 5 megapixel camera is able to take photos in 2592*1944 pixel and record videos in 640*480 pixel resolution [2].

Nokia E5-00 is capable of connecting simultaneously to up to ten email servers that use either the Internet Mail Access Protocol v4 (IMAP4) or the Post Office Protocol v3 (POP3) [2]. Text, Excel, PDF, PowerPoint, and Word files can be read by the device without needing to install any additional applications [2].

Nokia E5-00 also supports General Packet Radio Service (GPRS), Enhanced GPRS (EGPRS), High-Speed Downlink Packet Access (HSDPA), High-Speed Uplink Packet Access (HSUPA), WLAN IEEE 802.11 b/g protocols, and Wideband Code Division Multiple Access (WCDMA) [2]. It also features Global Positioning System (GPS) and Ovi Maps. Furthermore, Universal Plug and Play (UPnP), Bluetooth 2.0 + Enhanced Data Rate (EDR), and Universal Serial Bus 2.0 (USB) are used by this smartphone for establishing connection with other devices [2].

Nokia E5-00 can be charged through a 2.0 mm charger connector or USB [2]. Under optimal network conditions, its BL-4D battery allows up to 13.16 hours of talk time in Global System for Mobile Communications (GSM) networks while in Wideband Code Division Multiple Access (WCDMA) networks this value is up to 5.25 hours [2]. It may also be kept on standby for 26 and 28 days in GSM and WCDMA networks respectively [2].

User may configure a security code (aka lock code) on Nokia E5-00 to prevent unauthorized access to the device [3]. The default security code is 12345 which is not activated by default [3]. Nokia E5-00 will encrypt data stored on its flash memory and attached memory card if user enables encryption option [3].

B. Symbian OS

Symbian is one of the widely used OSs in smartphone industry [4]. Nokia E5-00 is equipped with version 9.3 of this OS and relies on S60 3rd Edition with Feature Pack 2 [2]. Mobile phones hosted by S60 enable their users to install and run their own applications at any time [5]. Applications developed in Java Micro Edition (ME), Symbian C++, Python and Adobe Flash Lite are supported by S60 [5].

From S60 3rd Edition onwards, Symbian has adopted a new security approach known as Symbian Platform Security Model which involves the following modules [6]:

1) Trusted Computing Base: It is a set of software that manages data caging and capabilities modules. Trusted Computing Base (TCB) includes kernel, file system, and software installer.

2) Data caging: It aims to restrict application to getting access just to areas of file system that are allocated for that specific application. These areas are classified as follows [6]*:*

a) Resource: Includes application's resources such as icons and bitmaps that are copied during the installation of application. The contents of this folder can be read by everyone.

b) Sys: It is the location of binaries like application installation registry and root certificates. Writing is allowed only during installation and only backup application might be permitted to read.

c) Private: Each application has its own private folder and only that specific application has read and write access to that folder. Backup programs may, however, have read and write permissions to this directory as well.

d) All the rest: Any other folders and their contents like user's documents are available to everyone.

3) Capabilities: They provide access to collections of application programming interfaces (API) and are divided into four levels as below:

a) Open to all: APIs are categorized in this group can be employed by any applications. Approximately, 60% of APIs are available to all applications.

b) Granted by user during installation phase: There are some capabilities such as ReadUserData that user can concede to application at installation phase.

c) Granted through Symbian Signed: Assigning capabilities like ReadDeviceData requires application passes the Symbian Signed tests.

d) Granted by the manufacturer: Privileges like the TCB and the Digital Rights Management (DRM) need to be granted by device's manufacturer.

Memory Management Unit (MMU) controls and protects all access to memory as well as memory mapped hardware [7]. MMU insures that the OS presents a so-called virtual memory machine model to running applications in order they to be appeared at the same virtual address during execution and be prevented from directly accessing each other's memory [7].

In Symbian OS any process that is not executed from the read only memory (ROM) requires to be placed in the random access memory (RAM) to be invoked [7].

There are also three types of identifiers (ID) used in Symbian OS as follows: (1) Unique Identifier (UID) assigned to each application and can be requested from www.symbiansigned.com, (2) Product ID that demonstrates product that application aims to be run on, and (3) Manufacturer ID which as its name implies is used for specifying manufacturer [6].

C. Forensic Principles and Concerns

In digital forensics, the investigation process must comply with legal regulations and certain procedures. [8-10] explain in detail stages needed to be taken in digital forensic investigations. The Association of Chief Police Officers (ACPO) [11] also prescribes four principles of computer-based electronic evidence including mobile phones as follows:

1) Principle 1: The data stored on mobile phone or its storage devices should not be changed by law enforcement agencies or their agents.

2) Principle 2: In case investigator realizes direct access to stored data is essential, they must make sure that are proficient enough to do so and able to provide evidence of implications of their actions.

3) Principle 3: All processes need to be documented and all evidence should be preserved. The same result should be produced if an independent third party examines those processes.

4) Principle 4: Case officer is responsible for making certain that the investigation process adheres to law and these principles.

The main objective of the aforesaid principles is to insure the integrity of original data saved on smartphone does not alter during investigation [8].

Overall, data can be saved on SIM card, memory card, and internal memory of smartphone [12]. Forensic data acquisition from SIM card and memory card is not as challenging as internal memory since with the help of SIM card readers and computer forensic tools stored data can be duplicated and extracted without being compromised. Internal memory is, nonetheless, divided into three components as follows: (1) the ROM that hosts OS and boot image, (2) the RAM which saves data pertaining to running processes, and (3) flash memory that stores user's data like images files [12,13]. Among them data copied to RAM are the most volatile items in smartphone forensics [12,13].

There are two methods for gathering data from smartphone, namely, physical and logical [8]. In physical data acquisition a bit-by-bit image of an entire physical store is made, while in logical data acquisition only logical objects such as directories and files are copied. Thus in the latter, unlike the former, deleted data cannot be extracted [8].

D. *Mobile Forensics Tools*

Mokhonoana et al. [14] specify three prerequisites for forensic tools as follows: (1) changing data stored on the device as little as possible, (2) extracting the maximum amount of data, and (3) minimizing investigator interaction with mobile phone.

This research analyzes four forensic tools being commonly used in mobile phone investigations namely, (1) Oxygen Forensic Suite v3.3.0.270 (Trial) [15], (2) Paraben's Device Seizure v4.3 (Demo) [16], (3) Mobile Internal Acquisition Tool (MIAT) [17], and (4) MOBILedit! Forensic Lite v5.5.0.1140 [18]. Additionally, a non-forensic utility called Nokia Ovi Suite 3.0.0.290 [19] developed for synchronizing and making backup of Nokia mobile phones from PC is included as well.

Table I presents the supported connection types of the delegated tools that are compatible with Nokia E5-00.

TABLE I. SUPPORTED CONNECTION TYPES OF FORENSIC TOOLS

Tool Name	Supported and Compatible Connection Types
Oxygen Forensic Suite Trial	USB and Bluetooth
Paraben's Device Seizure Demo	USB
MIAT	Memory card
MOBILedit! Forensic Lite	USB and Bluetooth
Nokia Ovi Suite	USB and Bluetooth

III. EXPERIMENTAL RESULTS

The designated tools have been examined after providing them with a Nokia E5-00 that some of its SMS messages, contact list entries, event logs, web histories, to-do entries, user's files, and email messages were deleted. The Nokia E5-00 has been also configured to be connected to Gmail and Facebook through a Wi-Fi connection using, respectively, Nokia Email and Facebook applications. A webpage was also loaded and at the same time a chat conversation was going on in Yahoo! Messenger (YM) via Nokia Chat application.

The test has been repeated after wiping the memory of the mobile phone using *#7370# command. The outcomes of each tool are explained in the rest of this section.

A. *Oxygen Forensic Suite*

Oxygen Forensic Suite (OFS) requires a file named OxyAgent_S60V3.sis to be installed and invoked on target mobile phone and investigator has to follow the setup instruction in order to execute the agent. The tool offers several hash algorithms and one of which can be selected in each investigation case.

OFS provided general information about the smartphone and the network that the device was connected to. The tool recovered all contacts, SMS and MMS messages, and user's files. Likewise, all non-removed memos, anniversaries, and meetings defined in the calendar and also to-do entries were extracted. It acquired all email messages that were stored on the mobile phone. Additionally, OFS gathered event logs up to 30 days. Based on the event logs and their corresponding date and time, Timeline feature organizes and sorts all SMS and MMS messages, emails and Internet connections.

The tool enables investigator to search for any texts or contacts. Investigator may employ File Browser of OFS to browser all recovered files. The flash memory, the RAM, and the ROM of the internal memory were respectively shown as 'C:', 'D:', and 'Z:'. We could collect browser history files and some information related to applications such as Activenotes and diverse other data like an email address provided for registering Quick Office from 'C:'. However many folders like 'Private' and 'Sys' were found empty. The only file we were able to recover from drive 'D:' was miplog.txt that saves the latest assigned IP address and the name of the access point that device is connected to. Moreover, no data from drive 'Z:' were gathered.

Aside from some binary files pertaining to Facebook application located in 'C:\Resource\ App', we were not able to recover any data or log linked to YM conversations and Facebook visited profiles. The tool did not also acquire any bookmarks and GPS logs. OFS could not extract any wiped data as well.

OFS restored SMS messages and event logs that had been removed for maximum 30 days, although deleted information concerning the rest of the data were not retrieved. An interesting point to note regarding the mentioned period is Nokia E5-00 by default keeps logs for 30 days. The duration may be changed by user to either 10 days, 1 day, or no log. As expected setting the smartphone not to keep any log resulted in none of the deleted events was extracted by OFS.

B. *Paraben's Device Seizure*

Nokia Symbian 9.x plug-in of Paraben's Device Seizure (PDS), logically, acquired files stored in the memory through the OBEX (Object Exchange) protocol. The gathered data were organized in six categories as follows:

1) *Backup Data:* Saved data on the flash memory of the device (C:) which belonged to different applications were presented in this group.

2) *Splited Backup:* The data of the previous group were split, decrypted, and demonstrated in more decipherable manner in this part. Resources like pictures associated to various applications were found under Splited Backup. Moreover, the configuration of several applications and even information like username and password linked to logged in user in Nokia Ovi were discovered in this group. We also observed a history of chat conversations of YM among the existing files in this part. However all presented date in Splited Backup were in binary format, unorganized,

and vague which may make the examining process cumbersome.

3) Parsed Backup: It structures collected database files in the form of table and field. Some formless data like bookmarks shown in the previous group were imparted more intelligibility in this part. A folder named 'contacts.cdb' contained the contacts information.

4) Logs: This group included the event logs of the device. This part also showed that the maximum number of events kept on Nokia E5-00 is 1000 and any event that passes 30 days is deleted which is analogous with the acquired event logs via OFS.

5) ToDo List: The only data we found in this group was a binary file which contained all memos, anniversaries, and meetings, and to-do entries.

6) Calendar: The same file found in the ToDo List group was listed in this part as well.

7) MailBox: SMS and MMS messages and configured emails and corresponding messages were shown under this group.

PDS employs both MD5 and SHA1 hashing algorithms and involves them in its reports. It also provides investigator with a search feature that facilitates finding data. PDS were capable of restoring the logs that had been deleted for not more than the assigned period for keeping event logs on the mobile phone. PDS could not also extract wiped data.

C. MIAT

MIAT needs to be installed on the target mobile phone to take image from its internal memory. However we were not able to execute it on Nokia E5-00 as MIAT is only compatible with mobile phones hosted by Symbian - S60 2nd Edition.

D. MOBILedit! Forensic

At the time of testing, MOBILedit! Forensic v5.5.0.1140 (MEF) was the first and the only version of this tool that supports Nokia E5-00. The tool could extract all contact information and the majority of non-deleted SMS and MMS messages. MEF also retrieved data stored on 'C:\Data' and all other data saved on 'E:' but yet again it was not able to acquire any deleted file. The Hex Dump tool included in MEF enables investigator to examine the files gathered from the mentioned paths. The tool can also be employed for making backup from the extracted data.

Although its user-friendly interface has options for calendar, notes, and tasks, but none of these data types has been recovered from the tested Nokia E5-00 mobile phone.

The Lite version of MEF does not provide reporting and exporting feature.

E. Nokia Ovi Suite

Nokia Ovi Suite (NOS) installed an agent named SeConUpdater on the target smartphone. It was capable of extracting contacts, photos, SMS and MMS messages, calendar's entries, bookmarks and notes although the deleted data could not be recovered by NOS.

Using the same machine employing for synchronization allows investigator to identify which information like messages have been removed since last synchronization.

During the backup NOS closed all applications running on the mobile phone. Another major disadvantage of this utility, in view of digital forensics, is it does not provide any hashing system for checking the integrity of data. NOS did not retrieve any wiped data.

Table II summarizes the outcomes of this section.

TABLE II. OVERVIEW OF THE TEST RESULTS

Information Type	**Oxygen Forensic Suite Trial**	**Paraben's Device Seizure Demo**	**MIAT**	**MOBIL edit! Forensic Lite**	**Nokia Ovi Suite**
Bypassing locked smartphone	No	No	-	No	No
Call logs	Yes	Yes	-	No	No
Communities programs logs	No	No	-	No	No
Configured emails	Yes	Yes	-	No	Yes
Configured messengers	No	Yes	-	No	No
Contact information	Yes	Yes	-	Yes	Yes
Exporting and reporting features	Yes	Yes	-	No	No
Map history	No	No	-	No	No
Organized events	Yes	Yes	-	No	Yes
Running processes	No	No	-	No	No
SMS and MMS messages	Yes	Yes	-	Yes	Yes
User data files	Yes	No	-	Yes	No
Web browser cache history	Yes	No	-	No	No
WLAN open sessions	No	No	-	No	No

IV. ANALYSIS

Both OFS and PDS, as forensic tools, could recover the significant amount of data stored on the flash memory of Nokia E5-00. However the foremost observed setback is none of them were able to retrieve all deleted information.

Moreover, both OFS and NOS need an agent to be installed on the mobile phone. Even though PDS does not run any application on the target smartphone, but it is stated that the tool changes some minor data as well [20]. All these tools are, therefore, feeble in compliance with the first principle of the ACPO's requirements stated in Section 2. 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.

OFS, PDS, MEF, and NOS, all, require mobile phone to be connected to the forensic workstation as 'PC Suite' and if 'Ask on connection' is active - which in default is - investigator has to select 'PC Suite' 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. With regard to achieved results, it is obvious that NOS and MEF have no advantage over OFS and PDS.

V. Proposed Framework

OFS and PDS are competent to extract call logs, contact information, organized events, and SMS and MMS messages. However some data like user's files and web browser cache history can be recovered by only one of the aforementioned tools and thereby investigator has to employ both of which for data acquisition purposes.

Inability of the tools to recover RAM's data makes manual examination indispensable. Investigator may keep mobile phone charged to avoid erasure of volatile data before accomplishing the examination. Switching a Nokia E5-00 mobile phone to offline mode disconnects and isolates the device from all networks and possible corresponding interruptions. Investigator may diligently examine default applications like Facebook in which if the user enabled saving username and password, valuable information would be revealed. In these cases the device should, nevertheless, be connected to the Internet and that might make alteration in the state of the original evidence.

Given that the structure of smartphones is very similar to PCs, similar approaches and methods used for live investigation of computers should be taken into consideration for smartphone forensics. In particular, as mentioned above, some of the mobile forensics tools need an agent to be installed on the target smartphone. The agent can, thereby, have the functionality of gathering the following data and exporting them to a file:

- Running applications
- Running servers
- Clipboard data
- Configured communities programs and their stored logs
- Configured messengers and their saved logs
- Configured emails and their stored logs
- WLAN open sessions
- IP address and subnet mask

Symbian's security platform may, however, restrict the agent from getting access to the majority of these data unless appropriate privileges are granted.

VI. Conclusion and Future Work

Within this paper we studied four mobile forensics tools in retrieving data from a Nokia E5-00 mobile phone. The results suggest that while smartphones 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 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.

Our future work will focus on development an on-phone toolkit capable of gathering volatile data from mobile phones hosted by Symbian S60 3rd Edition, Feature Pack 2. Furthermore, employing techniques for forensically getting access to a mobile phone protected by access code remain to be studied in future.

We hope this work will eventually lead to a compendious framework of investigation of smartphones.

References

[1] "News Archive: Shipments of smartphones grew 74 percent in 2010," *www.berginsight.com/News.aspx?m_m=6*, 2011.

[2] Nokia E5–00 Device Details, *www.forum.nokia.com/Devices/Device_specifications/E5-00*, 2010.

[3] "Nokia E5–00 User Guide," *http://nds1.nokia.com/files/support/apac/phones/guides/Nokia_E5-00_UG_en.pdf*, 2010.

[4] T. Jowitt, "Gartner Says Symbian Still Leads Smartphone Race," *www.eweekeurope.co.uk/news/gartner-says-symbian-still-leads-smartphone-race-20622*, 2011.

[5] P. Coulton, R. Edwards, and H. Clemson, *S60 Programming: A Tutorial Guide*. Wiley, 2007.

[6] "Testing and Signing with Symbian Platform Security," *www.forum.nokia.com/info/sw.nokia.com/id/ecf0292f-e59b-4f6e-b7d1-6008679dba1e/Testing_and_Signing_with_Symbian_Platform_Security_v1_4_en.pdf.html*, 2006.

[7] R. Harrison and M. Shackman, *Symbian OS C++ for Mobile Phones*. Wiley, 2007.

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

[9] "Digital Evidence: Standards and Principles, Scientific Working Group on Digital Evidence (SWGDE)," *International Organization on Digital Evidence (IOCE), Forensic Science Communications*, Vol. 2, No. 2, www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm, 2000.

[10] M. Reith, C. Carr, and G. Gunsch, "An Examination of Digital Forensic Models," *International Journal of Digital Evidence*, Vol. 1, Issue 3, 2002.

[11] "Good Practice Guide for Computer-Based Electronic Evidence," www.7safe.com/electronic_evidence, 2010.

[12] G. Me and M. Rossi, "Internal forensic acquisition for mobile equipments," *IPDPS. Proceedings of the International Parallel and Distributed Processing Symposium*, 2008.

[13] "Types of Memory in Symbian OS," *http://wiki.forum.nokia.com/index.php/Types_of_Memory_in_Symbian_OS*, 2011.

[14] P. M. Mokhonoana and M. S. Olivier, "Acquisition of a Symbian Smart Phone's Content with an On-Phone Forensic Tool," *SATNAC. Proceedings of the Southern African Telecommunication Networks and Applications Conference*, Sugar Beach Resort, Mauritius, 2007.

[15] "Oxygen Forensic Suite 2011," *www.oxygen-forensic.com/en/download*, 2011.

[16] "Paraben Forensic Software - Device Seizure," *www.paraben.com/device-seizure.html*, 2011.

[17] "MIAT Forensics," *http://miatforensics.org/index.php*.

[18] "MOBILedit! Forensic," *www.mobiledit.com/downloads.htm?show=8*.

[19] "Nokia Ovi Suite," *www.ovi.com/suite*.

[20] "Paraben's Customer Support," *http://support.paraben.com/devicefaq.html*.