An Overall Assessment Of Mobile Internal Acquisition Tool

By

Gianluigi Me, Alessandro Distefano

From the proceedings of

The Digital Forensic Research Conference

DFRWS 2008 USA

Baltimore, MD (Aug 11th - 13th)

available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/diin

Digital Investigation

An overall assessment of Mobile Internal Acquisition Tool

*Alessandro Distefano, Gianluigi Me**

Computer Science, Systems and Production Department, University of Rome Tor Vergata, Via del Politecnico 1, 00133 Rome, Italy

Keywords:
Symbian
Forensic acquisition
Memory card
TAC
API

ABSTRACT

The smartphone market provides a great variety of manufacturers and models causing a strong (and mandatory) heterogeneity of the hardware tools adopted to retrieve smartphone contents in a forensically sound way. Thus, in order to lighten the burden for already overtaxed police operators, with possible increase of forensics productivity, we already identified, in a previous work, a new Mobile Equipment (ME) acquisition paradigm. In fact, it's possible to avoid the practical problems related to the USB/mobile phone plug heterogeneity, currently used by the mobile forensics tools, through the use of the MMC/SD slot, part of the hardware equipment of the target ME. This solution overcomes the problems related to the acquisition through the cables, simply relying on a piece of software installed stored into the SD/MMC. The contribution of this paper enriches the methodology already presented by the authors and presents some fundamental properties of the Mobile Internal Acquisition Tool (MIAT) in order to assess the performance with respect to the state of the art of the mobile forensics tools. The results of the assessment encourage the adoption of this tool, since integrity, performances and operational methodology mostly overall benefit from this approach, while, in the worst case, remain at the same level of the state of the art COTS. Finally, this tool, intended to be released under an Open Source license, proposes the paradigm where the acquisition source code is in the public domain, while the analysis and presentation are left to self-made/proprietary tools.

1. Introduction

With about 2.6 billion subscribers around the world, mobile phones have out-diffused virtually every prior technology, whether TV sets, radios, wrist watches, wallets, wireline phones, or bicycles, and have done so in 25 years. The diffusion of mobile phones in the rural areas of the developing world appears to be the next frontier (Kalba, 2007): i.e., China Mobile declare that they have 317 million mobile customers in China today, adding 6 million new subscribers per month, and the total market is half a billion users. This states a projection of the very huge worldwide penetration of mobile phones worldwide, whose trend could be detected by Fig. 1.

Currently, the most part of purchased MEs has enhanced application capabilities and performances, regarding computational resources, connectivity and battery: these MEs are referred as smartphones, currently cell phones with PDA functionalities which can host custom applications.

Due to those enriched capabilities, the smartphones can collect lots of personal information, valuable source of analysis in a crime investigation.

In particular, during a forensic investigation, the data stored in a smartphone, phonebook, incoming/outgoing calls, calendar, docs and spreadsheets, e-mail, etc., can represent a very important source of information to silently witness private facts and crimes. In fact, many investigations have

* *Corresponding author*.
E-mail addresses: distale@gmail.com (A. Distefano), me@disp.uniroma2.it (G. Me).
1742-2876/$ – see front matter © 2008 Digital Forensic Research Workshop. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.diin.2008.05.010

	Mobile cellular subscribers					As % of total
	(000s)		CAGR (%)	per 100 inh	% Digital	phone Subscrib
	2001	2006	2001 - 06	2006	2006	2006
Africa	25'154.5	199'548.2	51.3	21.72	93.9	87.1
Americas	223'417.3	561'169.5	20.2	62.25	66.6	65.7
Asia	341'208.2	1'147'106.2	27.4	29.47	83.1	65.0
Europe	357'146.6	791'319.6	17.2	98.46	90.3	70.9
Oceania	13'701.2	24'315.5	12.2	73.21	98.9	66.7

Fig. 1 – ME penetration in the world (ITU).

seen mobile phone evidence used extensively (e.g. Williams) thus driving the crime analysis approach to an intensive use of data stored into the ME memory.

Moreover, at the time of writing, the Symbian devices represent an important part of the Smartphone market (Me and Rossi, 2008) and the most important manufacturers (Nokia, Siemens, Motorola, Ericsson, etc.) produce their devices running Symbian OS, which shipped on 77.3 million units in 2007, approximately a 50% growth over 2006 sales, with over 141 different phone models from eight licensees (http://www.engadget.com/2008/02/12/give-up-77-3m-symbian-phones-shipped-in-2007/).

The current smartphones usually have two or more of the following communication interfaces: GSM, GPRS, and UMTS for the long range, and IRDA, Bluetooth and WLAN for short range and a serial interface for wired communications. These devices can also support three memory locations to store the data to be acquired: the SIM (Subscriber Identity Module) card, the memory card (MMC, MultiMedia Card, or SD, Secure Digital) and the internal memory.

Unlike the general purpose devices as PCs, the smartphones have some peculiarities, which heavily influence the investigation process. In fact, the major problem related to these devices is represented by the internal memory acquisition, since it is organized as a unique block memory chip which makes impossible (unless to extract the chip and analyze it separately) to isolate it (e.g., an hard disk of a general purpose computer) for a low level analysis. Moreover, every manufacturer uses its own (proprietary) protocols to communicate with device, leading to a black box analysis by the operator.

For these reasons, currently, the smartphone live acquisition with external cables is widely accepted in the Courts, even if it presents some uncomfortable aspects.

2. State of the art

Many standards for the forensic investigation are currently available for the general purpose computers ACPO (http://www.acpo.police.uk/), IOCE (http://www.ioce.org/), and IACIS (http://www.cops.org/). Furthermore, recently the NIST released the guidelines on cell phone forensics (Jansen and Ayers, 2007).

The most crucial task in a forensic investigation is to acquire data from the devices: in the smartphone scenario, the content acquisition phase is represented by the acquisition of the data from the non-volatile storage locations. While data acquisition from SIM card and memory card represents a task close to the traditional forensic analysis due to the capability to isolate and analyze it separately, the acquisition of data from internal memory is very crucial. For this reason, this represents the target of our research tool MIAT. The internal memory of smartphones is composed of three types of volumes: ROM (read only) memory, storing the OS boot image, RAM (volatile) memory, storing the running processes data and the Flash memory (not volatile), storing the user multimedia files and documents, logs, videos and sounds.

The tools currently in use perform the acquisition of the internal memory in a remote way: a forensic tool is connected with the target device and, using the OS services, it extracts the data like SMS, MMS, TODO list, pictures, ring tones, etc. In order to achieve forensic seizure, closed and open source tools are available. The most important open source tool is TULP2G (TULP2G; van den Bos and van der Knijff, 2005), which implements standard modem protocols (e.g. Hayes commands) and OBEX protocol to communicate with the device. Unfortunately, if a smartphone model doesn't implement these standards, the tool is unusable for the investigation.

Among proprietary tools, the Paraben Device Seizure (Paraben Corporation, 2008) is one of the most important; it implements specific, proprietary protocols (like D-Bus for Nokia smartphone) but, as for the TULP2G tool, unknown protocols make the acquisition impossible. Recently Paraben Corporation released the "*CSI stick*" (Paraben Corporation; Dellutri and Ottaviani, 2008) a portable data gathering and forensic tool, which allows to acquire data without using the forensic workstation. This solution, however, still relies on proprietary plugs (currently, Motorola and Samsung).

The .XRY tool (MicroSystemation) adopts a quite similar approach to Paraben, with remote acquisition via hardware specific plugs. Finally, recently, Guidance Software added to Encase the mobile package, called Neutrino. For a more extensive review of tools available for Symbian, the reader could refer to Williamson et al. For the purpose of this paper we will compare Paraben Device Seizure features and performances with our forensic tool MIAT, as argued by the analysis described in Ayers and Jansen (2004).

3. Related works

In order to forensically acquire the smartphone memory content, all the tools adopt a remote-way procedure (connected-by-cable, or by-wireless), which represents a major operative drawback of this approach, due to the fact that acquisition phase could be inhibited when the appropriate jack is not available. This problem is strictly related to the development of a forensically sound way to address the problem of latency in coverage of new available phone models (and Symbian releases, with life cycle contained in one year) by forensic tools, presented in Jansen et al. (2008), where the authors present their solution, called "phone manager protocol filtering".

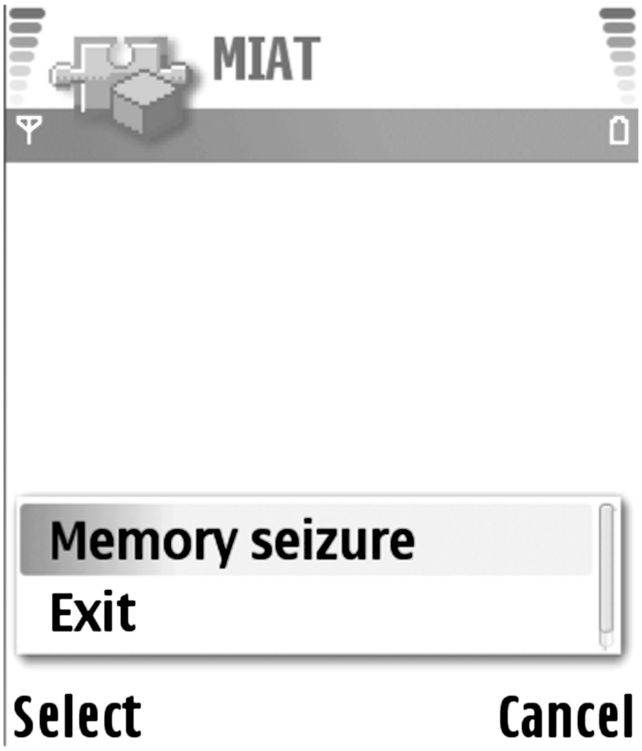

Fig. 2 – MIAT graphical user interface.

A further main disadvantage of the approach based on cables and proprietary tools is the partial access of the Symbian file system, which relies on the communication protocol. Since, to our best knowledge, it's not currently possible to perform a software bitstream copy of internal memory of the Symbian smartphones, we have proposed a solution (methodology and tool) for the major problem, cable-related, presented in Me and Rossi (2008) and Dellutri and Ottaviani (2008).

The approach described in Mokhonoana and Olivier (2007) is based on local acquisition and seems to be very similar to MIAT one. However, as a major appearing difference, the MIAT can retrieve the all Symbian file system, while the tool presented in Mokhonoana and Olivier (2007) cannot fetch several files.

The MIAT acquires data directly from the internal memory slot, spawning an acquisition application stored in the memory card (e.g. MMC) held by the forensic operator (Fig. 2). Even if the NIST guidelines say "*To acquire data from a phone, a connection must be established to the device from the forensic workstation…*" we believe that MIAT approach does not contrast those guidelines, but, extends the forensic workstation concept to the removable memory where the MIAT executable resides.

In this paper we focus on the overall performance of the MIAT (Memory Internal Acquisition Tool), presented in Me and Rossi (2008): the target is to present some of its performances benchmarked to a well-established tool as Paraben Device Seizure is.

4. The MIAT

As presented in Me and Rossi (2008) an alternative way to seize the internal memory data relies on local execution of an application which explores recursively the file system tree and copy each entry to a backup volume like an expansion memory card. During the acquisition process, files and directory are opened in read-only mode to preserve integrity: MIAT computes a digest in order to detect further corruptions. Firstly, to proceed with the acquisition, the device should be switched off. Then, if the SIM and/or the memory card are inserted in the smartphone, we must remove them to collect the stored data. We note that the SIM card is usually located under the battery, for this reason we must turn off the device. Once the SIM and the memory card have been acquired, we use the host memory card (different from the original memory card found in the device, part of the seizure) for the internal memory seizure: the acquisition application on the memory card is split into two files, the executable and the installation file for Symbian OS (.SIS file). The whole methodology and the arguments for the forensic soundness are in Me and Rossi (2008). Furthermore, we suppose that the memory space on the MMC hosting the forensic image is appropriately sanitized before the acquisition.

The adoption of this methodology forces saving hardware tools like USB cables specific for each device or additional equipment like notebook PC to perform the acquisition; the forensic workstation is now the seized ME equipped with a supplementary SD/MMC memory card with MIAT onboard.

A further benefit in using the MIAT is represented by the parallelism: in fact, MIAT can be used to seize *n* smartphones simultaneously, using *n* memory cards. In fact, since the forensic workstation can remotely acquire one device per time, MIAT can be mirrored into a number of memory cards in order to acquire several devices in parallel. This dramatically reduces the overall acquisition time when the number of device to be seized increases.

Furthermore, the MIAT acquisition tool, when definitively validated by the scientific community, will be released as an Open Source (Carrier, 2003), thus providing to the Court the Frye test passed. The tool realized as part of the methodology exposed in Me and Rossi (2008) needs two minor technical improvements. In fact:

1. At the time of writing is necessary to manually recompile the source code for every different device.
2. Notwithstanding the use of Backup Server, some files are still locked and so impossible to open and acquire.

Since almost every ME model needs its SDK (mainly due to graphic reasons), we believe it's uncomfortable to force the forensics operator to perform compilation in the crime scene. The capability of acquiring internal memory data of smartphones directly where they are discovered is good as stated in Jansen and Ayers (2007) because it increases the respect of integrity. Moreover, performing the acquisition as soon as possible reduces the probability of internal events (such alarms or appointment remainders) and external (such calls or messages incoming)[1] communications before the acquisition is made. We note that internal and external events are

[1] This could be avoided, always, using Faraday cages or removing the SIM card.

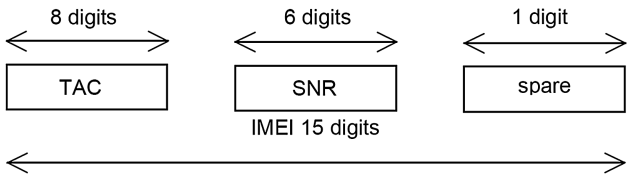

Fig. 3 – IMEI code structure.

represent threats to data integrity because they are not easily avoided nor predictable.

In order to automatically identify the manufacturer and the model of the ME, we use the IMEI number (unique and available in every smartphone). In fact, the IMEI can be discovered by inspection of physical location under the battery: the crime scene operator sends a request (e.g. via his ME) containing the IMEI of the seized ME to a listening server and waits. The server identifies the mobile phone model by checking the TAC number (which is part of IMEI number as specified in ETSI and 3GPP (2008)) as shown, e.g., in Fig. 6. Hence, the server sends the message back (e.g. via MMS), containing the ad-hoc compiled release of MIAT as attachment to the crime scene operator. The acquisition, now, can start. Fig. 5 summarizes the procedure, while Figs. 3 and 4 show the IMEI structures.

In order to improve the second technical item now we use a further alternative way to get access to such files we are unable to unlock. This way is accomplished by the Symbian `RFs` API method `ReadFileSection` Symbian Developer Library that allows to read from a file without open it. By this method it is possible to seize the entire file system tree including files which have a persistent lock on, furthermore this strategy preserves integrity because the access is established in read-only mode, guaranteed by the OS.

The identity between the MD5 hash code calculated on the seized filecopy (this file is already in the memory card) and the stored MD5 hash code of the same file that is in "checksum.xml" can be ensured using a straightforward PC checking. The acquisition time for a Nokia N70 internal memory is less than 15 min, see Section 6 for more details.

5. Property assessment by code reading

As stated in http://www.acpo.police.uk/, http://www.ioce.org/, http://www.cops.org/ and Jansen and Ayers (2007), forensic tools must have some fundamental properties, first of all integrity; in this section we explain how MIAT-S60 v1.0 (and v1.1 too) meets this property. The respect of integrity is ensured by using only *direct Symbian S60 File Server API methods in read-only mode.*

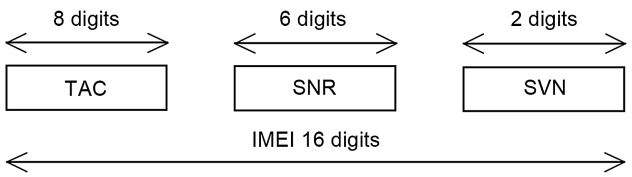

Fig. 4 – ImeiSV code structure.

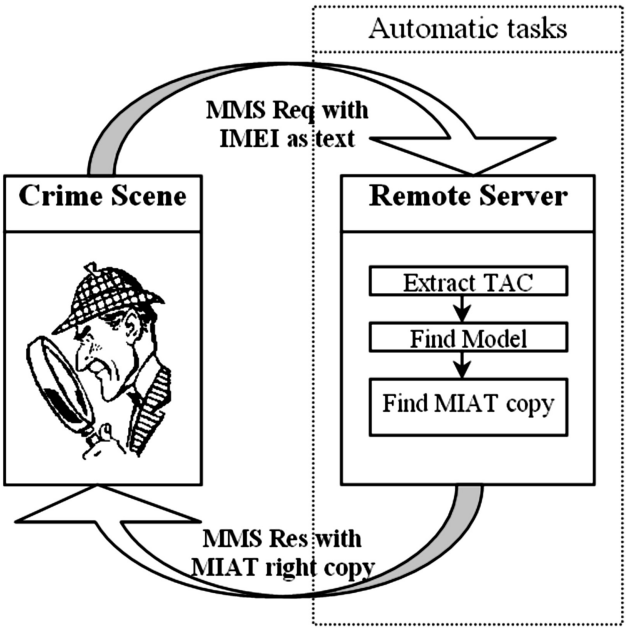

Fig. 5 – Automatic providing of MIAT right copy.

The difference between MIAT and some other forensic tools (e.g. TULP2G) is that the former dialogs directly with the Operating System while the latter require an intermediary (located in the mobile phone) in charge of managing the messages sent by remote forensic tool to the mobile phone. Since the intermediary code is quite always closed, the second case makes impossible to verify how intermediary code is written. *Whenever the source code is not available, obviously, it is impossible to state by code reading if the tool respects integrity and the other fundamental forensic properties required* (Carrier, 2003).

6. Property assessment by experimentation

In the previous section we show how the MIAT code is written to ensure integrity, however, this is just the first step in proving the correct functionalities of the tool; the second one is made by experimentation. With the following experiments we want to present the MIAT acquisition performance compared to the Paraben Device Seizure (Paraben Corporation, 2008).

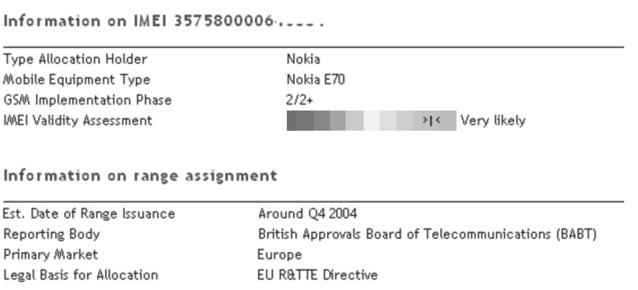

Fig. 6 – Query for a Nokia E70 to https://www.numberingplans.com/.

At the time of writing, MIAT has no Open Source forensic alternatives based on Symbian applications running on the mobile phone. For this reason we can consider in the experiments also an Open Source Client/Server application called P3nfs (Königh) that makes possible to mount Symbian file system into Linux file system. Since this application is not forensic our tests are made only to compare the MIAT technique efficiency of exploring the file system tree with the P3nfs one.

6.1. *Experiments*

The comparative experiments performed are the following:

1. MIAT-S60 v1.1 vs Paraben v1.3.2824.32812 on Nokia N70;
2. MIAT-S60 v1.1 vs P3nfs v5.19 on Nokia N70;
3. MIAT-S60 v1.1 vs Paraben v1.3.2824.32812 on Nokia 6630.

For each experiment the steps taken are the following:

- 1st acquisition by MIAT;
- 2nd acquisition by reference software (Paraben or P3nfs);
- 3rd acquisition by MIAT;
- 4th if the reference is Paraben, another acquisition by Paraben to ensure MIAT respect of memory integrity.

In the 4th point of the above list is anticipated our memory integrity verification schema: we use MIAT to verify the Paraben and P3nfs respect of memory integrity and Paraben to verify the MIAT one. Our checks are based on the last modification times produced by MIAT and Paraben executions (P3nfs does not produce this information so we can't use it for this purpose).

In order to state the coverage of the internal memory file system presented by the acquired data we use two approaches in each experiment: manual check of data seized between the two competitors and automatic check using the combination of ls and diff Linux commands. In all acquisitions the device is started in Offline (removing the SIM card) and Recovery Mode (holding the ''Edit'' key while the phone is bootstrapping), in this way we prevent, respectively, data corruption due to network events (call or message arrivals) and local execution interference due to other non-necessary programs running during the acquisition.

Table 1 briefly summarizes environment of the experiments.

Table 1 – Execution environment

Property	MIAT	Paraben	P3nfs
OS	Symbian-S60	WinXP-SP2	Ubuntu 7.04
Access to device	Local	Remote via USB-cable	Remote via Bluetooth

6.2. *Experimental results*

In this section we present and argue the results obtained by the experiments, focusing on the amount and typology of data acquired (and so on the coverage of the phone internal memory file system), the integrity of the internal memory and the execution time. Table 2 summarizes execution times and overall size of acquired data (including hashing, last modification time and all other information produced during the acquisition) across the experiments in function of tool used. In this table it is easy to note that MIAT execution time depends both on occupation of internal memory and capabilities of device seized. In fact, the last row presents execution times which are considerably higher than first row times. This is due to the different hardware capabilities: in Experiments 1 and 3 we used, respectively, the Nokia N70 and the Nokia 6630, while the overall size is quite similar, the execution time shown by both tools is rather different. We clarify the benefit of MIAT parallelism with a straightforward example. Suppose we need to perform the acquisition of 5 Nokia N70 internal memory, suppose each of them has a memory occupation quite similar to device used in our experiments. Using Paraben Device Seizure we need about $5 \times 8 = 40$ min while using MIAT we can parallelize the acquisitions and the overall time could be (including few minutes for MIAT mirroring) about 15 min! Parallelism drastically reduces the overall acquisition time needed.

Table 2 – Results of experiments

Exp	Tool	Time (min)	Size (MB)
1	MIAT	≈12	6.65
	Paraben	≈8	7.28
2	MIAT	≈12	6.65
	P3nfs	≈6	5.42
3	MIAT	≈50	5.73
	Paraben	≈15	8.86

Table 2 shows that Paraben acquisitions have a greater size than MIAT ones: this is only due to the additional information which are related to the Paraben acquired data management. In order to clarify the data shown, we focus that MIAT produces a single file for all seized entries named ''checksum.xml'' which contains the additional information like MD5 hashing codes and last modification times while Paraben produces multiple files (one file with ''property'' extension for each seized entry) each one containing additional informations about its entry as shown in Fig. 7.

In order to verify the respect of integrity we proceeded as explained in Section 6.1; *our overall checks stated that MIAT did not corrupt any file during the acquisition, but few local system files*. These files (strictly OS files with minor importance in forensic analysis) are shown in Table 3. However, our checks stated that Paraben corrupts some files too, as shown in Table 4. Tables 3 and 4 show how acquisitions are invasive in terms of last modification time changes; the first column contains the filename, the second contains **X** if, after a reboot, a change is discovered and the third contains **X** if, after an acquisition,

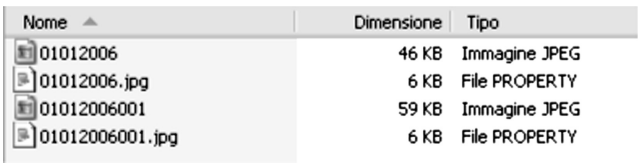

Fig. 7 – Paraben additional information.

Table 3 – MIAT last modification time changes

File	Reboot	Acquisition
smssmssegst.dat	X	
CommonData.D00	X	
LocaleData.D05	X	
Applications.dat	X	X
backupdb.dat	X	
btregistry.dat	X	
cbtopicsmsgs.dat	X	
CntModel.ini	X	
DRMHS.dat	X	
HAL.DAT	X	
ECom.lang	X	
ScShortcutEngine.ini	X	
nssvasdatabase.db	X	X
100056c6.ini	X	
101f6df0.ini	X	X
System.ini	X	

X means that a change happens.

a change is discovered. Data shown in Tables 3 and 4 are collected, both for MIAT and Paraben, as follows:

- In order to state the corruption due to the acquisition:
  1. boot the device in Recovery Mode;
  2. 1st acquisition with the forensic tool;
  3. 2nd acquisition with the same forensic tool;
  4. overall last modification time check;
- In order to state corruption due to acquisition combined with reboot:
  1. device boot in Recovery Mode;
  2. 1st acquisition with the forensic tool;
  3. device reboot in Recovery Mode;
  4. 2nd acquisition with the same forensic tool;
  5. overall last modification time check;

In order to verify the coverage of the several acquisitions we proceeded as explained in Section 6.1; our check stated that most of the files in the phone internal memory file system are seized by all the tools. However, Paraben missed the directory ''C:\Private'' in experiment 1 while MIAT and P3nfs did not. Another directory ignored by Paraben Device Seizure during the acquisition in all experiments (while the competitor did not) was ''_PAlbTN'', this folder normally contains thumbnails of Gallery elements but, as a file system directory, could also be used to store some other important information. Moreover, regarding these directories ignored by Paraben Device Seizure we don't have any information about and so we cannot state if the missing is due to underlying protocols used or Paraben acquisition strategy. Furthermore, regarding the experiment 2, *MIAT and P3nfs produced the same identical image of internal memory file system, both files and their properties always match*; the difference in size exposed in Table 2 is due to additional information such as hashing produced by MIAT. *This aspect states that MIAT is able to acquire the entire set of elements stored in the logical structure of file system, this set is composed by all elements reachable using the OS API. However, is still impossible to recover erased information using these three tools.*

Table 4 – Paraben last modification time changes

File	Reboot	Acquisition
CommonData.D00	X	X
LocaleData.D05	X	X
backupdb.dat	X	X
btregistry.dat	X	
cbtopicsmsgs.dat	X	
CntModel.ini	X	X
HAL.DAT	X	
ECom.lang	X	
ScShortcutEngine.ini	X	X
nssvasdatabase.db	X	X
100056c6.ini	X	
101f6df0.ini	X	X
System.ini	X	
AlarmServer.ini	X	X

X means that a change happens.

7. Current and future work

At the time of writing we are working in the following three directions: the first is a more extended experimentation, the second is to solve the first item listed in Section 4 and the third is to support Symbian v9 devices. As the experimental results came from very few replications in order to obtain more reliable data and so more general conclusions, we are trying to use MIAT in acquisition of internal memory data from smartphones discovered in real crime scenes. As the information stored in ME easily changes due to both environment and local events, in order to preserve its integrity is fundamental to acquire data as soon as possible (Jansen and Ayers, 2007). Since version 9 of Symbian embeds a mechanism of trusted computing managing the execution capabilities of running programs, the Backup server spawn can be inhibited. As we explained in Section 4 and is stated in Me and Rossi (2008) this service is used by MIAT to get access to some locked file; so in order to use this tool with Symbian v9 smartphones it has to be trusted by manufacturer.

8. Conclusions

Me and Rossi (2008) presented an alternative methodology to seize internal memory of smartphone, however, several further steps are necessary to reach its use in practical investigations. In this paper we presented the experimentation step made with Open Source paradigm in mind (Carrier, 2003). In this experimental phase we described two aspects: improvements and assessment of forensic properties. The process of experimentation needs massive replications to produce definitive data and so drawing more general conclusions, however, it seems that MIAT can reach the performance as well as Paraben Device Seizure. We presented also how to make easier the process of recompiling the tool for every smartphone in order to provide an actual and effective operational support to MIAT usage in real investigations. In this way, forensic operators could benefit in crime scene

acquisition of an Open Source and easy to use tool in order to perform a smartphone internal memory acquisition in a forensically sound way, without being overtaxed.

Acknowledgments

This work, partially funded by the Finanziaria Laziale di Sviluppo, Filas S.p.A., is the prosecution of the Maurizio Rossi's graduation thesis, defended in May 2007, whose results are published in Me and Rossi (2008). Further thanks to the Zetareticuli s.r.l. technical staff for the valuable discussions during the prototype engineering.

REFERENCES

Ayers R, Jansen W. PDA forensic tools: an overview and analysis. National Institute of Standards and Technology; 2004.

van den Bos J, van der Knijff R. TULP2G – an open source forensic software framework for acquiring and decoding data stored in electronic devices. International Journal of Digital Evidence 2005. Netherlands Forensic Institute.

Carrier B. Open source digital forensics tools – the legal argument; 2003.

Dellutri F, Ottaviani V, Me G. MIAT-WM5: forensic acquisition for Windows mobile PocketPC. In: Proceedings of the 2008 workshop on security and high performance computing systems, part of HPCS; 2008.

ETSI and 3GPP. ETSI TS 123 003 V7.6.0 technical specification; January 2008.

Jansen W, Ayers R. Guidelines on cell phone forensics – recommendations of the national institute of standards and technology. NIST; May 2007.

Jansen W, Delaitre A, Moenner L. Overcoming impediments to cell phone forensics, http://csrc.nist.gov/groups/SNS/mobile_security/documents/mobile_forensics/Impediments-formatted-final-post.pdf; 2008.

Kalba K. The adoption of mobile phones in emerging markets: global diffusion and the rural challenge. In: 6th annual global mobility roundtable 2007, Center for Telecom Management, Marshall School of Business, University of Southern California, Los Angeles, June 1–2; 2007.

Königh R. P3nfs client/server application. http://www.koeniglich.de/p3nfs.html.

Me G, Rossi M. Internal forensic acquisition for mobile equipments. In: 4th International workshop on security in systems and networks (SSN2008), proceedings of the international parallel and distributed processing symposium (IPDPS). IEEE Computer Society Press; 2008.

MicroSystemation. XRY project website, http://www.msab.com/en/.

Mokhonoana PM, Olivier MS. Acquisition of a Symbian smart phone's content with an on-phone forensic tool. Department of Computer Science – University of Pretoria; 2007.

Paraben Corporation. CSI stick, http://www.csistick.com/.

Paraben Corporation. Paraben device seizure. Paraben's Forensics Software, www.paraben.com; 2008.

Symbian Developer Library. Symbian file server API. http://www.symbian.com.

TULP2G project website. http://tulp2g.sourceforge.net/.

Williams C. Mobile forensics turns up heat on suspects. http://www.theregister.co.uk/2007/02/11/mobile_forensics_guidance/.

Williamson B, Apledoorn P, Cheam B, McDonald M. Forensic analysis of the contents of Nokia mobile phones. http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Williamson%20et%20al%20-%20Forensic%20Analysis%20of%20the%20Contents%20of%20Nokia%20 Mobile %20Phones.pdf.

Alessandro Distefano received the B.S. in Computer Science Engineering from the Università degli Studi di Roma ''Tor Vergata'', Italy. Currently is a candidate for M.S. in Computer Science Engineering. His thesis, covering Mobile Forensics acquisition and analysis, has provided a large contribution to this work.

Gianluigi Me, Ph.D., is an adjunct professor of Computer Systems Security in the Università degli Studi di Roma ''Tor Vergata'', Computer Science Engineering Department and in the Università degli Studi di Roma ''La Sapienza'', Criminology Department. He holds a wealth of experience in managing training for law enforcement high tech crime units. His research interests include mobile computing applications, digital forensics, electronic/mobile payments and game theory.