A Review of Mobile and SIM Forensics Tools

Mohammed Abdul Rahman AlShehri

CCIS, Majmaah University Al Majmaah, Kingdom of Saudi Arabia.

Summary
The technological advancements in Smartphones and in secure elements makes their use of value for the criminal community as a secure and tamper resistant data terminal in conducting organized crime. When smartphones and secure elements are used in crimes by criminals, so forensic examiners need tools which allow secure retrieval and prompt examination of data present on mobile devices and secure elements. Substantial amount of information is stored on mobile device's internal memory and external memory modules and SIM cards which play vital role as evidence. This paper focusses on the currently available mobile and SIM forensic tools that help in carrying forensic investigation. Security features of SIMs hamper in many ways the possibility to dump a bit for bit internal memory image. SIM card forensics is a promising area that can provide investigators with a plethora of evidentiary data, given that they have the right knowledge and tools to extract it in a forensically-sound manner.

Key words:
Secure elements, SIM Forensics, Smartphones, SIM and SIMbrush

1. Introduction

In April 2004, the number of GSM registered users exceeded the amount of a billion [4], or a sixth of the world population. Considering several hundred million users of non-GSM mobile telephony systems, it is the probably is the one that most penetrated technology in our lives: people bring with themselves mobile phones for the majority uses such as to communicate with others. These bring it with them even when they are acting illegally. From a Forensic Sciences point of view, there is nothing better, to confirm evidences, clear, impartial, non-contradictory and true witness. These are exactly the characteristics of digital evidence extracted from a SIM card by means of a forensically sound process. Despite huge advantages investigations could gain from such digital evidence, a very small number of tools exists that can help investigators in their job. SIMbrush is a new forensic imaging tool for SIM/USIM cards. It is an open source tool which caters the need of SIM forensics. Following are the advantages of this tool:

a) This tool interfaces with SIM/USIM card in a standard way without discriminating based on the manufacturer, the issuer or the provider of the card

b) It will retrieve hidden information from non-standard files

c) Many instances can be executed in parallel with in the same system without overloading the system.

d) The output generated using this tool is in textual XML format helping for the purpose of archiving and for Web integration.

Following are the limitations of this tool

a) The consumption of time for brushing a SIM/USIM is more.

b) It cannot extract the body of those files with ADM or NEV access conditions.

2. SIM Features

Smart cards are standardized by ISO according to ISO SIMs are contact (as opposed to contactless) smart cards specified in [10]. It is impossible to get the bit for bit image of a SIM card if digital integrity is a constraint, SIMbrush tool does not guarantee to extract all the data from the SIM card but can be very useful in real investigative processes. All the existing SIMs are a subset of existing smart cards. The main concern of smart cart design is the security of the data stored in the SIM. The term "security" can be further specified into four basic properties of security are confidentiality, authentication, non-repudiation and integrity. Being the SIM a smart card, the aforementioned requisites are used to accomplish the subsequent tasks:

Confidentiality: Client's confidentiality must be ensured by encrypting voice and data that transit Over The Air (OTA). Cryptographic keys are implemented in the SIM.

Authentication: no unauthorized client can access the system. Authentication keys reside in the SIM.

Non repudiation: no one should be able to access the signing keys without proper authentication i.e. compromising the private key.

Integrity: no one should be able to tamper or modify data that is protected. A lot of protections aimed at this target are implemented in smart cards and SIM cards.

A smart card is considered as tamper resistant so it is not easy to access data from the smartcard without proper authentication. From a forensics perspective we can

Manuscript received March 5, 2018
Manuscript revised March 20, 2018

conclude that we cannot use tools that require a physical manipulation so SIMbrush tool does not make use of any "black hat" methods; it interfaces, instead, itself with the SIM in the standard way. This tool only tries to extract data from the filesystem. A smart card's filesystem is stored in an internal EEPROM, with a hierarchical tree structure, containing root as Master File (MF). There are two classes of files: directories, called Dedicated Files (DF) and files, called Elementary Files (EF). These can be called as the nodes and leaves of a tree, respectively. The MF is a DF. The main difference between a DF and an EF is that a DF contains only a header, whereas an EF contains a header and a body. The header contains all the control data or meta data that quantitatively relates the file with the structure of the filesystem (available space under a DF, number of direct children, length of a record, etc.) and security information, whereas the body contains information related to the application for which the smart card has been issued. The body structure has four types of EF which are listed below:

Transparent EF: the organization of files is in the form of a sequence of bytes. The content can be read by specifying a numeric interval.

Linear-fixed EF: A record is a group of bytes that have a known coding: every record of the same file represent the same kind of information. Record is a unit in files instead of the byte. All the records have the same length in a linear-fixed EF.

Linear-variable EF: This is similar to linear-fixed EF with one exception i.e. record's length may vary from one record to the other.

Cyclic EF: Cyclic EF files implement a circular buffer where the atomic unit is a record. Therefore, the concepts of first and last are substituted by those of previous and next. SIM cards only implement transparent, linear-fixed and cyclic EFs. Every file is uniquely identified with its ID that is the name of the file. No two files will have the same ID. The operations allowed on the filesystem are coded into a set of commands that the interface device (IFD), which is the device capable of interfacing with a smartcard and setting up a session of communication, issues to the smart-card, then waiting for responses.

3. Literature Survey

SIM Forensics is still in its infancy due to the extensive in-depth knowledge and expertise required; hence, previous research efforts are limited to the best of the authors' knowledge. There have been, some pioneering attempts that have paved the way for SIM Forensics which are summarized below. Using the GSM 11.11 Technical Specification, Willassen (2003) focused on the subscriber's sensitive information that can be extracted from a SIM card. He identified 21 extractable items and demonstrated how the GSM mobile telephone system can play a significant role in forensics examination. Highlighting the challenges in the field of digital forensics, Savoldi and Gubian (2007) provided a proof-of-concept with regards to the possibility of data hiding in a SIM/USIM card through various techniques that are widespread due to the absence of a nonstandard part in the SIM/USIM image memory. Cilardo, Mazzocca, and Coppolino proposed a unified architecture, "TrustedSIM," inherently relying on a subscriber's identification module (SIM) as its core component. This, according to them, was due to the tamper-resistant domain and flexible multiplication environment that could manage users' security profiles. Given the above potential data that could be transformed into forensically-sound evidence, general forensic examination tools were used to extract and recover these data. Jansen and Ayers (2006) demonstrated that some of these tools, however, may yield inaccurate results because they were not specifically designed for SIM Card Forensics. This inefficiency may also be referred to a programming error, utilization of an incorrect protocol, or an out of date specification that might lead to improper functionality. Casadei et al (2006), on the other hand, tried to experiment with an open-source SIM-specific forensic tool instead of commercial and proprietary restricted software. The researchers presented their SIMbrush tool analysis through conducting an experiment to extract all observable memory and non-standard files of the SIM Card.

4. Forensics Tools

The number of forensic tools for smart phones are very few compared with personal computers due to different operating systems, or a type of hardware architecture and manufacturer's product line (e.g. palm OS, Windows CE and others). Some of the forensic tools provides all the functionalities comprising acquisition, examination, and reporting functions, (Paraben, 2006) but other tools focuses on a one function such as SIM forensic, external memory modules (CP, SO, MMC & other) and phone itself, (Ayers, 2004, 2006). Forensic tools can use many interfaces (e.g., Bluetooth, IrOA, serial cable and USB) to acquire device contents. Information retrieved from the tools depends on the tools specification and vendors hardware and software compatibility. Most common data available is PIM data, logs of calls, messages, email, URLs (Uniform Resource Locator), video, audio, image, and SIM data. So in order to retrieve all the data from mobile phones we can sub-categorize as follows:

a) Handset based Tools
b) Operating System Based Tools

c) SIM based Tools

The setup for the experiment required the arrangement of a mobile device and a SIM card reader. We prepared two mobile devices, an Apple iPhone 4s and a Samsung Galaxy SIII that included an Etisalat and DU SIM cards, respectively, in addition to an external SIM card reader. The selection of two different service providers was made to investigate the difference—if any—between the various service providers. To complete the setup for the experiment, data creation was required on both mobiles, such as saving user data (i.e., contacts) to the SIM card. For the iPhone, this was not directly possible because by default, iPhone does not support saving to the SIM card. The authors have to manually move the SIM card to another mobile device that supports this feature (a Nokia device). The authors additionally set up various social media accounts, i.e., Facebook, Instagram, Dropbox, etc., and created dummy user data on them. For our experiments, we planned to explore both commercial and open source tools. The following tools were chosen for comparison due to their support of SIM card forensic investigations:

EnCase Forensics: From Guidance software, EnCase is a tool widely used in the digital forensics field. EnCase's Smartphone Examiner module collects information from different smart devices, SIM card readers, or through device backups.

MOBILedit: a mobile forensic tool that not only provides viewing, searching, or retrieval from a phone; but also retrieves information such as IMEI, OS, and firmware, SIM card details such as IMSI, ICCID, and location area information.

Mobile Phone Examiner: MPE from AccessData includes an enhanced smart device acquisition and analysis capabilities. With the integration of nFIELD, it provides forensic mobile device data collections that support both USIM and SIM acquisition with reporting abilities.

Oxygen Forensic Suite: Oxygen is developed by Oxygen Software Company and performs digital forensic analysis of smartphones through the use of proprietary protocols.

Paraben SIM Card Seizure: SIM Card Seizure is a tool from Paraben Cooperation that performs a forensic SIM card acquisition and analysis with the ability to recover deleted text messages from SIM cards.

pySIM: This open forensic tool is from TULP2G used for extracting and decoding of data stored within the electronic devices.

SIMBrush: Is an open-source tool which can be used to extract all observable memory from SIM/USIM cards.

SIMScan: This forensic tool is an open-source toolkit used to recover SIM card information by downloading the binary contents of individual files and storing them as individual files.

Table 1: Handset Based Tools Comparisons, (Ayers, 2004, 2006)

Name	Function	Features
Pilotlink	Acquisition	a) Targets Palm OS phones b) Open source non-forensic software c) No support for recovering SIM information d) Supports only cable interface
Device Seizure	Acquisition, Examination and Reporting	a) Targets certain models of GSM, TDMA, CDMA ' with Palm OS, Pocket PC, and RIM OS advance Device Examination, handheld devices support b) Supports data recovery of internal and external memory c) Supports cable, Bluetooth, and IR interfaces
GSMXRY	Acquisition, Examination and Reporting	a) Targets certain models of GSM phones b) Supports recovery of internal and external SIM c) Supports cable, Bluetooth, and IR interfaces
OXYGENPM	Acquisition, Examination and Reporting	a) Targets certain models of GSM phones (forensic) b) Supports only internal SIM acquisition
MOBILedit! Forensic	Acquisition, Examination and Reporting	a) Targets certain models of GSM phones b) Internal and external SIM support c) Supports cable and IR interfaces
BitPIM	Acquisition and Examination	a) Targets certain models of COMA phones b) Open source software with write-blocking BitPIM capabilities c) No support for recovering SIM information
TULP2G	Acquisition and Reporting	a) Targets GSM and COMA phones that use supported protocol s to establish connectivity b) Internal and external SIM support c) Requires PC/SC-compatible smart card reader for external SIM cards d) Cable, Bluetooth , and IR interfaces supported

UFED Cellebrite: This forensic tool access mobile data and exposes every segment of a device's memory using advanced logical file system, and physical extractions. Additional features of this tool includes in-depth decoding, analysis, and reporting.

USIMdetective: This forensic tool is from Quantaq Solutions designed especially for the management of

complex data storage mechanisms which is found in smart cards.

XRY: Is a comprehensive digital forensics examination tool used for mobile devices. With its ability to grab mobile information, XRY also retrieves specific SIM card information. XRY Viewer is an easy-to-use tool for viewing and accessing retrieved data. Different tools provide different acquisition techniques, and with respect to the abovementioned tools, some of them acquire SIM card information through phone acquisitions like EnCase, MOBILedit, Oxygen, and UFED, while others provide the acquisition of SIM cards through a SIM card reader like Encase, SIM card seizure, SIM Manager, USIMDetective, and XRY.

Table 2: OS Based Tools Comparisons, (Ayers, 2004, 2006)

	Palm OS	***Pocket PC***	***Linux***
Device Seizure	Acquisition, Examination and Reporting	Acquisition, Examination and Reporting	_____
Pilot Link	Acquisition		
Encase	Acquisition, Examination and Reporting	_____	Examination and Reporting

Table 3: SIM based Tools Comparisons. (Ayers. 2004. 2006)

Name	***Function***	***Features***
Device Seizure	Acquisition, Examination and Reporting	External/ Internal SIM cards (direct I indirect)
USIM Detective	Acquisition, Examination and Reporting	External SIM cards only (direct)
TULP2G	Acquisition and Reporting	Recover information from SIM card. When inserted in handset (No direct SIM support) .
GSM XRY	Acquisition, Examination and Reporting	Recover information from SIM card, when Reporting inserted in handset (No direct SIM support).
MOBI Ledit! Forensic	Acquisition, Examination and Reporting	Recover information from SIM card. When Forensic Reporting inserted in handset (No direct SIM support).
SIMIS	Acquisition, Examination and Reporting	External SIM cards only (direct)
ForensicSIM	Acquisition, Examination and Reporting	External SIM cards only (direct) Produces physical Reporting facsimiles of SIM for prosecutor and defense, and as a storage record.
Forensic Card Reader	Acquisition and Reporting	External SIM cards only (direct)
SIMCon	Acquisition, Examination and Reporting	External SIM cards only (direct)

5. Conclusion

This paper focusses on the currently available mobile and SIM forensic tools that help in carrying forensic investigation. Security features of SIMs hamper in many ways the possibility to dump a bit for bit internal memory image. SIM card forensics is a promising area that can provide investigators with a plethora of evidentiary data, given that they have the right knowledge and tools to extract it in a forensically-sound manner. Currently, over-the counter tools are generally built to aid examiners in analyzing the mobile phone as a whole unit, neglecting the fact that some vital information is often left out in smaller modules (i.e., the Subscriber Identity Module). Some of the tools used in this paper's experiment did yield vital information regarding the subscriber, but further development is needed to ensure the reliability of the information gathered. Having knowledge of the tools' strengths and limitations helps investigators develop an in-depth expertise on the right tool to use in different situations. Forensic examiners are advised not to rely solely on one tool and to opt instead to cross-validate findings. SIM card forensics research is a promising realm for future research, which includes a SIM card file system, data acquired in raw format (binary data) and represents digital evidence.

References

[1] Ayers, R. & Jansen, W. (2006). 'Forensic Software Tools for Cell Phone Subscriber Identity Modules'. National Institute of Standards and Technology

[2] Ayers, R. & Jansen, W. (2004). 'Guidelines on PDA Forensics'. National Institute of Standards and Technology (NIST Special Publication 800-72)

[3] Ayers, R. & Jansen, W. (2004). 'PDA Forensic Tools: An Overview and Analysis'. National Institute of Standards and Technology (NISTIR 7100)

[4] GSM Association: "Membership & Market Statistics as at the End of March 2004", GSM Association, 2004. Downloadable at http://gsmworld.com/news/statistics/pdf/mar04.pdf.

[5] Casadei, F., Savoldi, A., & Gubian, P. (2006). Forensics and SIM cards: An Overview. International Journal of Digital Evidence, 5(1), 1-21.

[6] Jansen, W., & Ayers, R. (2006). Forensic software tools for cell phone subscriber identity modules. In Proceedings of the Conference on Digital Forensics, Security and Law (pp. 93-106).

[7] Savoldi, A., & Gubian, P. (2007). Sim and usim filesystem: A forensics perspective. In Proceedings of the 2007 ACM symposium on Applied computing (pp. 181-187). ACM.

[8] Savoldi, A.; Gubian, P., "Data Hiding in SIM/USIM Cards: A Stenographic Approach," in Systematic Approaches to Digital Forensic Engineering, 2007. SADFE 2007. Second International Workshop pp.86-100, 10-12 April 2007.

[9] Willassen, S. (2003). Forensics and the GSM mobile telephone system. International Journal of Digital Evidence, 2(1), 1-17.

Mohammed Abdul Rahman AlShehri is working as a Vice Dean for Academic Affairs in CCIS, Majmaah University Al Majmaah, Kingdom of Saudi Arabia. His research interests include Computer Networks and applications, E-services, E-learning, IS, Mobile Applications. He can be reached at ma.alshehri@mu.edu.sa