Annual ADFSL Conference on Digital Forensics, Security and Law

2016 Proceedings

May 26th, 9:00 AM

SIM Card Forensics: Digital Evidence

Nada Ibrahim
Zayed University, College of Technological Innovation

Nuha Al Naqbi
Zayed University, College of Technological Innovation

Farkhund Iqbal
Zayed University, College of Technological Innovation, farkhund.uqbal@zu.ac.ae

Omar AlFandi
Zayed University, College of Technological Innovation, omar.alfandi@zu.ac.ae

Follow this and additional works at: https://commons.erau.edu/adfsl

 Part of the Aviation Safety and Security Commons, Computer Law Commons, Defense and Security Studies Commons, Forensic Science and Technology Commons, Information Security Commons, National Security Law Commons, OS and Networks Commons, Other Computer Sciences Commons, and the Social Control, Law, Crime, and Deviance Commons

Scholarly Commons Citation

Ibrahim, Nada; Al Naqbi, Nuha; Iqbal, Farkhund; and AlFandi, Omar, "SIM Card Forensics: Digital Evidence" (2016). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 3.
https://commons.erau.edu/adfsl/2016/thursday/3

This Peer Reviewed Paper is brought to you for free and open access by the Conferences at Scholarly Commons. It has been accepted for inclusion in Annual ADFSL Conference on Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

EMBRY-RIDDLE Aeronautical University SCHOLARLY COMMONS

(c)ADFSL

FORENSIC INVESTIGATION OF SIM CARD

Nada Ibrahim, Nuha Al Naqbi, Farkhund Iqbal and Omar AlFandi
Zayed University
College of Technological Innovation
Abu Dhabi, P.O. Box 144534
{M80006330, M80004910, Farkhund.Iqbal, Omar.AlFandi}@zu.ac.ae

ABSTRACT

With the rapid evolution of the smartphone industry, mobile device forensics has become essential in cybercrime investigation. Currently, evidence forensically-retrieved from a mobile device is in the form of call logs, contacts, and SMSs; a mobile forensic investigator should also be aware of the vast amount of user data and network information that are stored in the mobile SIM card such as ICCID, IMSI, and ADN. The aim of this study is to test various forensic tools to effectively gather critical evidence stored on the SIM card. In the first set of experiments, we compare the selected forensic tools in terms of retrieving specific data; in the second set, genuine user data from eight different SIM cards is extracted and analyzed. The experimental results on a real-life dataset support the effectiveness of the SIM card forensics approach presented in this paper.

Keywords: SIM card, Digital Forensics, Forensic tools, ICCID, IMSI

1. INTRODUCTION

Regardless of its role in crime (direct or indirect), data within a mobile phone remains crucial. A wealth of information is stored on cell phones that includes, but is not limited to, call history, text messages, email messages, web pages, and photos. Mobile phone forensics, the most challenging digital forensics field, should be enriched with SIM card forensics.

Most of the existing research is focused on searching for the following key evidence in a mobile telephone:

- Calls made, including numbers dialed, dates, and times.
- Calls received, including numbers received, dates, and times.
- Data stored within address book/phone book.
- SMS details.
- Pictures/video clips on the phone or memory card.

The SIM (Subscriber Identity Module) is a smart card that is used in mobile phones to store user data and network information that is required to activate the handset for use. SIM card demand has been growing worldwide on a yearly basis (ABIResearch, 2015) and is expected to break the record of 5.4 billion shipments for the year 2015 alone. Given this widespread usage, a massive amount of information is available for forensic investigators.

Since the introduction of UMTS, better known as 3G technologies, USIM cards are favored. While SIM cards provide network access, the tiny computer within a USIM enables it to handle several mini-applications and video calls if it is supported by the network and the handset. Integrated algorithm users are protected from unauthorized access

© 2016 ADFSL

to their phone lines. Furthermore, data exchanges are encrypted with stronger keys than those provided by SIMs. Additionally, a USIM's phonebook is much bigger, with the ability to store thousands of richer contacts that might contain email addresses, photos, and several additional phone numbers.

SIM card forensics provide valuable information about contacts, SMSs, call logs, and much more. There are commercial and open-source tools that can assist an investigator in extracting relevant evidence from SIM cards.

The CDR, or 'call detailed records' in a SIM card, led to the arrest of the suspect Sameer Vishnu Gaikwak in the murder of Govind Pansare in Kolhapur earlier this year. The records proved that the phone was active at the time of the murder and led the police to discover another 23 mobile phones used by the suspect due to his frequent SIM card change. (Indian Express September 2015).[1]

In another case, the fraudsters used cell phone information to illegally transfer bank funds. The scammer managed to transfer funds from an online bank account of the original post-paid subscriber through a "SIM-swap" promotion where an existing SIM card was replaced with a new one. This replacement allowed the fraudster to take over the victim's mobile number and use it for fraudulent activities (Manila Times, July 2015)[2]

In our research we aim to contribute to the field of SIM card forensics through:

- Exploring the amount of information extracted from SIM cards;
- Investigating whether the extractable SIM card evidence is tool dependent;
- Evaluating the contribution of obtained evidence to SIM card forensics;
- Investigating whether SIM cards from different GSM Service Providers offer different evidentiary data;

A smartphone might be the key to an entire investigation; thus, an investigator's task in uncovering evidence will be much harder if it is not supported with the necessary knowledge. Our motivation emerged from the fact that SIM card forensics is a new field with minor literature as far as we know. We intend the analysis of our results to contribute to the mobile forensic field with the essential knowledge needed to make informed decisions based on the tools' actual capabilities. We also believe that the analysis of the retrieved data will play a crucial role in proving suspects guilty or not.

The remainder of the paper is organized as follows: Background information and fundamental concepts needed to understand SIM forensics are discussed in Section 2; literature review is presented in Section 3. Experimental tools and setup are explained in Section 4; experimental results are discussed in Section 5, followed by the conclusion and future work in Section 6.

2. BACKGROUND INFORMATION

The introduction of the Global System for Mobile Communications (GSM) standard for transmitting text, voice, and data services

[1] http://indianexpress.com/article/india/india-others/suspects-sim-card-was-active-at-spot-of-pansare-murder-police/

[2] http://www.manilatimes.net/nbi-probes-sim-card-swap-scam/199564/

 © 2016 ADFSL

through cellular networks marked a telecommunication revolution that affected all aspects of our lives. Ever since the European Telecommunications Standards Institute (ETSI) released their GSM 11.11 Specifications of the SIM-ME interface in the 1990s, the industry has experienced a radical growth. It was initiated by the recommendation to split the Mobile Station (i.e., Cellular Phone) into two components: a removable Subscriber Identity Module (SIM), which contains all network related subscriber information, and a Mobile Equipment (ME) that is the remaining part of the Mobile Station, i.e., the mobile handset (ETSI, 1994).

As the name implies, a SIM card holds the identity of the subscriber, which enables users to be registered in the telecommunication network. In addition to identification and authentication, the SIM card can also store the subscriber's contacts, messages, calls, location information, and other subscriber-specific data. The components of a SIM card, as explored thoroughly by Savoldi and Gubian (2007), include a central processor unit (CPU) and an operating system (OS) with electronically erasable programmable read-only memory (EEPROM). It also contains a Random Access Memory (RAM) that controls the program execution flow. Moreover, it includes a Read-Only Memory (ROM) which controls the operating system workflow, user authentication, data encryption algorithm, and other applications. The SIM card file system is organized in a hierarchal tree structure and resides in the EEPROM for storing data such as names and phone number entries, text messages, and network service settings.

The anatomy of the file system—as demonstrated in Figure 1—includes three types of files: Master File (MF), Dedicated Files (DF), and Elementary Files (EF). The Master File is the root of the file system. Dedicated files are the child directories of the master files such as the DF (DCS1800) and DF (GSM), which contain network-related information, and DF (Telecom), which holds service/carrier-related information. Furthermore, elementary files contain the actual data in various types, structured as either a sequence of data bytes, a sequence of fixed-size records, or a fixed set of fixed-size records used cyclically. It is important to note that all the files have headers, but only EFs contain data (Savoldi and Gubian, 2007).

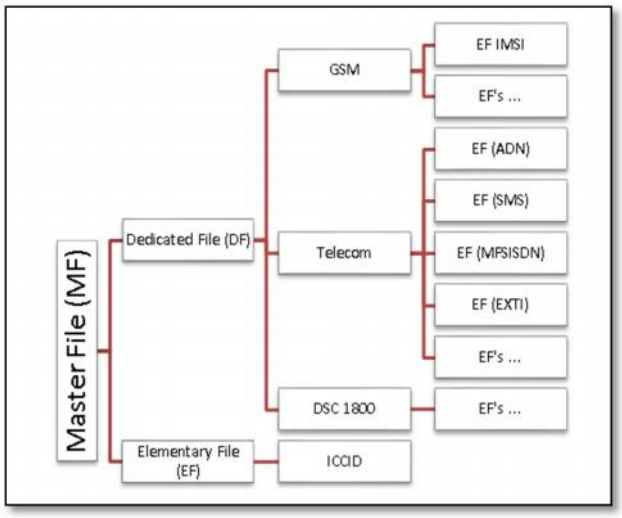

Figure 1. SIM Card File System Hierarchy

SIM cards have certain physical dimensions that follow the ISO/IEC 7816 standard, managed jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). This standard is structured in 15 parts, in which parts 1 and 2 specify in detail the physical characteristics of the identification Integrated Circuit Cards (ICC, SIM Cards is a particular type of ICC) along with contacts, location, and dimensions. Manufacturers adopted the ISO/IEC 7816 standard and created SIM cards in the following sizes (Singh, 2015): Full Size, Mini, Micro, and Nano SIMs. Full-size SIM cards were the first cards produced and are the size of a credit card. Shrinking in size over the years, the Mini SIM

© 2016 ADFSL

was introduced and was about 1/3 the size of the previous Full-size SIM card. Smaller versions exist now, and they are the Micro-SIM and Nano-SIMs.

SIM cards can also be embedded into devices (i.e., Embedded Universal Integrated Circuit Card [eUICC]), which can be fused directly onto a circuit board for machine-to-machine (M2M) applications. Irrespective of size, SIM cards possess the same internal components and file system hierarchy described earlier (Singh, 2015).

To help readers understand terminologies of the data found, we list below some definitions that were extracted and rephrased from the Third Generation Partnership Project (3GPP) Technical Specifications. 3GPP (GSM) TS 11.11.

ICCID: up to twenty digits long, this *Integrated Circuit Card Identifier* uniquely identifies a SIM card and is mainly divided into two parts: the *Issuer Identification Number* (IIN) and the *Account Identification Number* (AIN). The Issuer identification is interpreted as follows: The first two digits are reserved for the *Major Industry Identifier* (MII) (i.e., 89 for the SIM telecommunications industry), followed by a two-digit Country Code, in addition to a three-digit Issuer Identifier Number. The Account Identification Number includes four digits for the manufacturing month/year, two digits for the Configuration Code, six-digits for the Individual SIM Number, and finally a checksum digit for error-detection.

IMSI: A fifteen-digit long number, the *International Mobile Subscriber Identifier* is primarily used for signaling and messaging over a GSM network. Similar to the ICCID, the IMSI is structured as follows: three-digits for the *Mobile County Code* (MCC), plus two to three digits for the *Mobile Network Code* (MNC), and the rest is an allocated sequential serial number that pinpoints the *Mobile Subscriber Identity Number* (MSIN).

MSISDN: with a maximum of fifteen digits, the *Mobile Station International Subscriber Directory Number* is assigned for a subscriber to receive calls but is not signaled to or from a device. A subscriber can have multiple MSISDNs, and each one refers to the full subscriber phone number, including the country code. In general, MSISDN consists of a Country Code (CC – up to three-digits), the National Destination Code (NDC – up to 3 digits), and the Subscriber Number (SN – up to 10 digits), with a maximum of 15-digits total. MSIDSN is an optional elementary file (i.e., Optional EF does not need to be stored on the SIM card itself), which differentiates it from both ICCID and IMSI (which are mandatory fields). Own Dialing Number is a similar service that allows mobile users to inquire about their telephone numbers by dialing a specific numeric code.

SPN and **SDN** (*Service Provider Name* and *Service Dialing Numbers,* respectively) are also optional elementary files that convey the name of the GSM Network Service Provider and the unique services it provides (i.e., customer care number). As per the standard, if a network provider chooses a field to be of variable length, then remaining digits should be set to hexadecimal digit "F."

TMSI: Temporary Mobile Subscriber Identity. As the name implies, this is a temporary identifier that is exchanged between the mobile phone and the local network nearby. The TMSI is automatically updated when the subscriber moves between geographical locations to avoid signal fade, thus providing the mobility freedom supported by GSM cellular networks.

ADN: *Abbreviated Dialing Numbers* refers to the contacts list saved by the subscriber on the SIM card. LND (*Last Numbers Dialed)*, on

 © 2016 ADFSL

the other hand, is associated with the most recent number the subscriber called. Limited by the number of contacts it can contain due to its small capacity, a SIM can store additional digits from ADN and LND into the *dialing extensions* EXT1 and EXT2 elementary fields. FDN, *Fixed Dialing Numbers,* is similarly related to those fields in the same way because it contains a phonebook that can only be accessed once a specific mode is activated. A possible scenario in which this might be applicable is in the case of a company SIM card that restricts outgoing calls to only those numbers previously configured in order to refrain staff from using the company's assets for personal calls. The parameters above are also combined in a *Capability Configuration Parameters* (CCP) along with the associated mobile equipment and subscriber configuration (Markantonakis, 2007).

SMS: *Short Message Service* allows subscribers to communicate via messages that are sent and received through the cellular network. SMS data is considered forensically valuable information as it contains not only the message text exchanged but also the time, date, sender's phone number, and the message status (i.e., read, unread, sent, etc.). Deleted messages are even more valuable as it might indicate a suspicious content worth examining. When a message is deleted, the data it contains is not automatically erased; yet, its reference is marked as free space until new data can overwrite it. SMSs can be stored on the SIM card itself or on the Mobile Equipment (ME). Due to the SIM's limited storage size, many manufacturers design their mobile phone handsets to automatically use their own internal storage memory instead of SIM cards (i.e., iPhone). Others' models differ, and it depends on the phone software and user settings to explicitly indicate which storage to use. SMS, SMSP, and SMSS (*Short Messages Service*, *Short Message Service Parameters*, *and Short Message Service Status,* respectively) are elementary files that contain Short Message Service information such as the address of the operator's short message switching center, lifetime/timeout of messages, and coding format (Willassen, 2005).

Location information can be found by thoroughly examining the LOCI, LAI, LAC, RAC, and RAI voice and data communication fields. *Location Information* (LOCI) includes the *Location Area Identifier* (LAI), which is comprised of the *Mobile Country Code* (MCC), *Mobile Network Code* (MNC), and the *Location Area Code* (LAC) along with the *Routing Area Code* (RAC) and the *Routing Area Information* (RAI).

Built-in security features can be found in SIM cards, and these fields are established by the use of *Card Holder Verification* (CHV1) and (CHV2). These two fields restrict file access to those users with valid verification PIN codes (*Personal Identification Numbers*). Other features control various mobile users' access to the GSM Network, and this is achieved by assigning a specific ACC (*Access Control Class*) to each group. Encryption is also utilized to avoid tampering and ensure data security by the use of a *Ciphering Key* (Kc) to authenticate the SIM on the mobile network and a *Ciphering Key Sequence Number* (Boudriga, 2009).

Other information related to the GSM cellular network configuration residing in the SIM card includes, for instance, *Phase Identifier*. GSM Services were delivered in phases where Phase 1 introduced SIM cards, ciphering, voice telephony, international roaming, call forwarding, and SMS services. Further features were added at later stages (i.e., call waiting) based on services that were offered by the previous stage. Using the *SIM Service Table* (SST) elementary file, one can identify which services are allocated and activated in the SIM and which are not (i.e.,

© 2016 ADFSL

SMS, FDN, and, and so on). Other settings such as language preferences for menu interaction are set using the *Preferred Languages* Variable (PL). The SIM card can also contain two Group Identifiers (GID1) and (GID2). The GSM Service Provider is the only entity to modify these two fields in order to identify a group of SIM cards for particular applications and associations. *Emergency Call Code* is another service-provider specific and can be defined to set up an emergency call, for instance, to 999 in the event of threats. *Higher Priority PLMN Search Period* (HPLMN) is also configured by the Service Provider and states how often the mobile equipollent should search for the home network (range is between 6 minutes to 8 hours). Set by the service provider, *Preferred Network List* (PLMN) allows subscribers to select a network from a pre-configured list to connect to while roaming abroad. *Forbidden Networks* (FPLMN), on the contrary, are those networks to which a phone is not permitted to connect. A broadcast control channel (BCCH) is a pattern that contains system information messages of the identity and configuration of the base transceiver station in the GSM cellular standard. *Cell Broadcast Message Identifier* (CBMI) specifies the content of the cell broadcast messages a subscriber would receive by the Service Provider partners (preferred networks). In addition to the previous parameters, Service Providers also set the Accumulated Call Meter (ACM) to manage subscriber cell phone expenses before reaching a certain maximum (ACMmax). Using a *Price per Unit and Currency Table* (PUCT), the costs can be calculated in a currency chosen by the subscriber (Bidgoli, 2010).

3. LITERATURE REVIEW

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.

 © 2016 ADFSL

4. TOOLS AND EXPERIMENTAL SETUP

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:_From TULP2G, pySIM is an open forensic software framework for extraction and decoding of data stored within electronic devices.

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

SIMScan:_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.

UFED Cellebrite: UFED provides access to mobile data and exposes every segment of a device's memory using advanced logical, file system, and physical extractions. It also provides in-depth decoding, analysis, and reporting features.

USIMdetective: From Quantaq Solutions, USIMDetective is a forensic tool that has been specifically designed to manage the complex data storage mechanisms found in smart cards.

XRY: Is a comprehensive digital forensics examination tool used for mobile devices. With

© 2016 ADFSL

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 above-mentioned 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 1
Forensic Tools

Tool	Version
Encase Forensics	7.09.03.40
UFED Cellebrite	4.1.2.49
Oxygen Forensic	7.4.0.121
Paraben (SIM Card Seizure)	4.0
Dekart (SIM Manager)	3.3
Quanta (USIMdetective)	V3.0.4

The following table summarizes the main specifications of the mobile phones used:

Table 2
Smartphones Used

	iOS	**Android**
Device	iPhone 4s	Galaxy SIII
Version	8.4.1	4.3
Model	MD 258AE/A	GT-I9300

5. EXPERIMENT RESULTS AND DISCUSSION

Open source software were not available for testing either due to discontinuation of the software itself (i.e., SIMBrush) or unobtainable download links that led to invalid owner websites (i.e., SIMScan). The authors were able to download pySIM, but faced an error, as it only provided a connection through serial socket communication, which is no longer valid in new mobile devices.

UFED logical analyzer provided an unexpected error when the authors tried to test it with the iPhone 4s. Alternatively, UFED did not support logical acquisition to Android devices, which limited the ability to perform an acquisition to the Samsung Galaxy SIII mobile phone.

The results provided by EnCase with regards to Apple iPhone 4s were available through iTunes backup analysis only. This option was not available for the Android device, as EnCase was unable to read the Samsung Android backup.

Although MOBILedit was able to connect and read both phones, no data was retrieved from either mobile device; however, and this might be because it was a trial version.

Both MPE & nFIELD trial versions were downloaded; nevertheless the authors experienced difficulty in running these programs due to licensing errors that prevented the downloaded trial versions from running.

While any recovered information that was stored and retrieved from a SIM card is of evidentiary value, not all tools have the ability to retrieve or extract all of the required information. The results of the first part of this experiment display a comparison of the useable tools and their ability to extract pre-defined criteria set by the authors; we focused on 40 items of various possible extractable SIM card information based on the Third Generation Partnership Project (3GPP) Technical Specifications (GSM) TS 11.11.

The best tools that were able to extract the highest number of items included Paraben SIM Card Seizure, Quantaq USIMDetective, and XRY, respectively. Both SIM Card Seizure and USIMDetective were able to list all the items

 © 2016 ADFSL

in its report despite the fact that some of these items did not contain any data value. As for XRY, only fields with data were displayed, which drives us to inquire whether it is a tool/version limitation. Only fields that contained data were reported in XRY, while in SIM Card Seizure, all the fields in the comparison criteria were displayed along with additional extra fields. It was also clearly reported that there was no data to be displayed in that criteria. This could be due to service provider SIM card configuration, which led us to another area of research, and that is to investigate more SIM cards from different providers for comparison.

Furthermore, Paraban and USIMDetective displayed the SIM card file system hierarchy in a clear, simple view that made it easier to locate and further examine each master file and its sub-items. The latter provided an additional HEX format view for the extracted data that could provide a further examination and verification means. XRY, on the other hand, provided two tabs with information about the logical acquisition of SIM and USIM (other tools presented the extracted data in one view). The obtained content for both SIM and USIM were identical except for an added evidence about the Cyphering key.

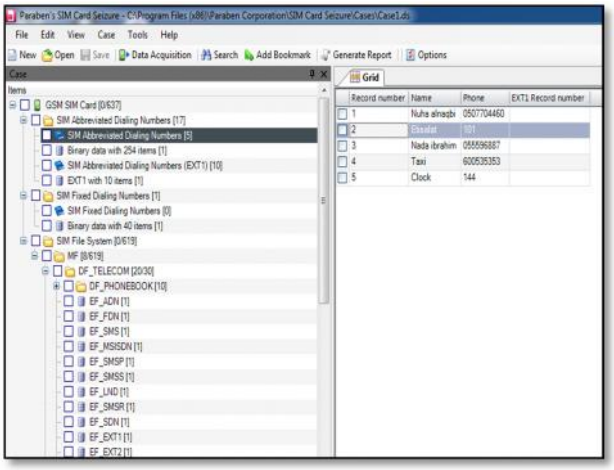

Figure 2. Paraban SIM Card Seizure

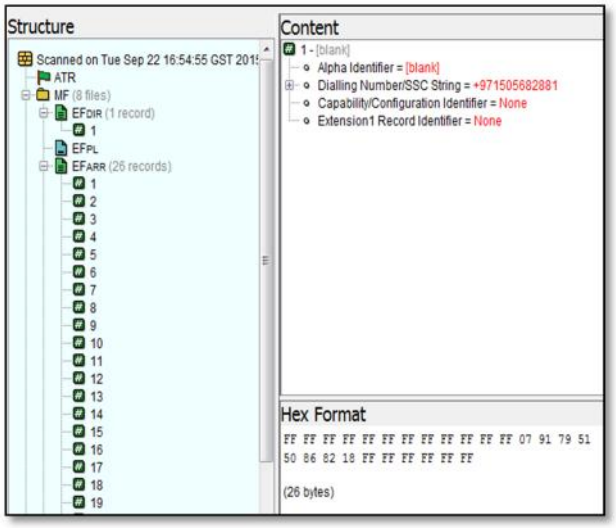

Figure 3. USIMDetective

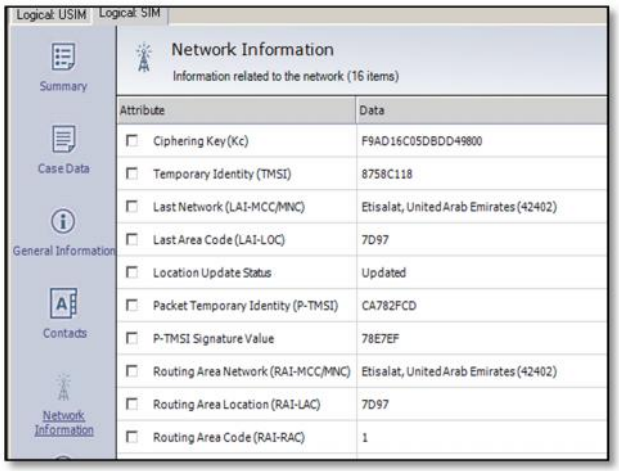

Figure 4. XRY

With the least amount of information retrieved, EnCase, Oxygen, and Dekart SIM Manger come at the end of the comparison. EnCase was only able to read the iTunes backup, and this was not a valid option for the Android backup. EnCase comes with an extra module for mobile phones acquisition that was not available to the authors at the time of conducting this experiment for the phone/SIM card acquisition.

Oxygen was able to get basic information about the SIM card. It differed though between both phones as it was able to display its own dialing number in iPhone 4s and not in Samsung SIII. While Oxygen was able to

© 2016 ADFSL

display SIM contacts on both phones, there was no visual indication that those contacts were saved on the SIM cards. The authors reached this conclusion as they saved those contacts in both SIMs intentionally for testing and experiment purposes.

With the ability to write to the SIM and the possibility of changing the PIN code, data extracted from Dekart SIM Manager would not be forensically sound. Reset of the PIN code is a debatable question as it might be required in case of accessing a locked SIM. Although the authors did not manipulate any evidence data, writing to the SIM will lead to contamination resulting in inadmissible evidence. This feature can also be misused by suspects to forge the data.

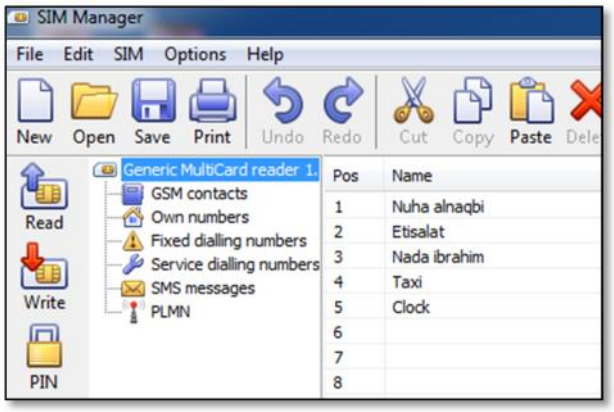

Figure 5. Dekart SIM Manager

Table 3 Overview of the assessment between the tools through the various acquisitions that were conducted either to the mobile devices or to the SIM cards.

 © 2016 ADFSL

Table 3
40 Evidentiary information and tools capability to extract them.

SN	SIM Card Information	Tool											
		XRY		Paraben		Oxygen		Dekart		USIM Det.		EnCase	
		Etisalat	DU	Etisalat	DU	4S	SIII	Etisalat	DU	4S	SIII	4S	SIII
1	ICCID	✓	✓	✓	✓	✓	-	-	-	✓	x	-	xx
2	SPN	✓	✓	✓	✓	-	-	-	-	✓	x	-	xx
3	MCC	✓	✓	✓	✓	-	✓	-	-	✓	x	-	xx
4	MNC	✓	✓	✓	✓	-	✓	-	-	✓	x	-	xx
5	MSIN	✓	✓	✓	✓	-	-	-	-	✓	x	-	xx
6	MSISDN	✓	*	✓	✓	✓	-	✓	✓	✓	x	✓	xx
7	IMSI	✓	✓	✓	✓	-	-	-	-	✓	x	-	xx
8	LDN	*	*	✓	✓	-	-	-	-	✓	x	-	xx
9	LOCI	✓	✓	✓	✓	-	-	-	-	✓	x	-	xx
10	LAI	✓	✓	✓	✓	-	-	-	-	✓	x	-	xx
11	ADN	✓	✓	✓	✓	✓	✓	✓	✓	✓	x	✓	xx
12	FDN	*	*	✓	✓	-	-	✓	✓	✓	x	-	xx
13	SMS	*	*	✓	✓	-	-	✓	✓	✓	x	-	xx
14	SMSP	✓	✓	✓	✓	-	-	-	-	✓	x	-	xx
15	SMSS	*	*	✓	✓	-	-	-	-	✓	x	-	xx
16	Phase	✓	✓	✓	✓	-	-	-	-	✓	x	-	xx
17	SST	*	*	✓	✓	-	-	-	-	✓	x	-	xx
18	LP	*	✓	✓	✓	-	-	-	-	✓	x	-	xx
19	CHV 1 & 2	*	*	✓	✓	-	-	-	-	-	x	-	xx
20	EXT1	*	*	✓	✓	-	-	-	-	✓	x	-	xx
21	EXT2	*	*	✓	✓	-	-	-	-	✓	x	-	xx
22	GID1	✓	✓	✓	✓	-	-	-	-	✓	x	-	xx
23	GID2	✓	✓	✓	✓	-	-	-	-	✓	x	-	xx
24	CBMI	*	*	✓	✓	-	-	-	-	✓	x	-	xx
25	PUCT	*	*	✓	✓	-	-	-	-	✓	x	-	xx
26	ACM	*	*	✓	✓	-	-	-	-	✓	x	-	xx
27	ACMmax	*	*	✓	✓	-	-	-	-	✓	x	-	xx
28	HPLMNSP	*	*	✓	✓	-	-	-	-	✓	x	-	xx
29	PLMNsel	✓	✓	✓	✓	-	-	✓	✓	✓	x	-	xx
30	FPLMN	*	*	✓	✓	-	-	✓	✓	✓	x	-	xx
31	CCP	*	*	✓	✓	-	-	-	-	✓	x	-	xx
32	ACC	*	*	✓	✓	-	-	-	-	✓	x	-	xx
33	BCCH	*	*	✓	✓	-	-	-	-	-	x	-	xx
34	Kc	✓	✓	✓	✓	-	-	-	-	✓	x	-	xx
35	Kc Seq. #	*	*	✓	✓	-	-	-	-	✓	x	-	xx
36	Emergency Call Code	*	*	✓	✓	-	-	-	-	-	x	-	xx
37	Own Dialing Number	✓	-	✓	✓	✓	-	✓	✓	-	x	✓	xx
38	TMSI	✓	✓	✓	✓	-	-	-	-	✓	x	-	xx
39	RIA	✓	✓	✓	✓	-	-	-	-	-	x	-	xx
40	SDN	*	*	✓	✓	-	-	-	-	✓	x	-	xx

***** → Please refer to the discussion section.

x → USIMDetective was unable to read DU SIM card information, displaying an error that this card does not seem to support 2G or 3G mode communication.

xx → EnCase was unable to read Android backup

In the second part of this experiment, the authors were eager to pursue actual data that SIM cards might contain (again with reference to the 40 criteria items previously chosen). For this purpose, the authors used the XRY tool to extract actual data from 8 different SIM cards.

The cards were accessed logically using the tool and its reader and the following segments were extracted:

ICCID: 89971122126964102877																		
8	9	9	7	1	1	2	2	1	2	6	9	6	4	1	0	2	8	7	7

- 89 is interpreted as the Major Industry Identifier (Telecommunications administrations and private operating agencies)
- 971 as the Country Code (i.e., United Arab Emirates)
- 12 is the Issuer Identifier and that is Etisalat.
- 212696410287 is the Individual Account Identification number including the month/year of manufacturing, Configuration code, and SIM number.
- 7 is the Checksum calculated from the other 19 digits.

The ICCID is engraved on the SIM itself to uniquely identify the chip internationally and cannot be changed or updated later, which makes it a reliable data source from a forensic point of view. Also, using the Issuer Identifier, investigators could contact the service provider identified by the ICCID to get the logs of a certain suspect/victim after getting a search warrant for further analysis.

For the International Mobile Subscriber Identifier (IMSI), it is interpreted as follows:

IMSI: 424021445434857														
4	2	4	0	2	1	4	4	5	4	3	4	8	5	7

- 424 reflects the Mobile Country Code, in this case, the United Arab Emirates.
- 02 refers to the Mobile Network Code, which is the Emirates Telecommunications Corporation (Etisalat).
- The remainder of the digits signify the Mobile Subscriber Identification Number (1445434857).

Both the ICCID and IMSI can be used to identify a specific subscriber and are of great forensic value since examiners can approach mobile network providers and obtain all data records of a potential suspect/victim (i.e., subscriber).

The Mobile Station International Subscriber Directory Number (MSISDN) was extracted as well, and it contains the following info:

MSISDN: +971505682881											
9	7	1	5	0	5	6	8	2	8	8	1

- 971 represents the Country Code (United Arab Emirates)
- 50 identifies the National Destination Code (Mobile Phone by Etisalat)
- 5682881 refers to the Subscriber Number

It is noteworthy to know that other than the ICCID, the information contained within the SIM can be modified later (i.e., MSISDN) and hence, the reliability of such evidence is sometimes questioned in a court of law.

Abbreviated Dialing Numbers (ADN) are of significant importance since they may link

 © 2016 ADFSL

an unidentified phone to a suspect/victim or pinpoint possible connections and relations of the mobile owner. Some modern mobile phones, however (specifically the iPhone 4S tested in this experiment) rely on the Mobile Equipment (ME) storage to save these numbers instead of the SIM Card itself.

Similarly, SMS data is crucial in forensic investigations but, unfortunately, none of the SIM cards tested in this experiment revealed any SMSs stored on the SIM card itself. The authors speculate that this is due to the mobile phone manufacturers' default settings that prevent saving SMS data into the SIM cards and utilize the phone internal memory instead.

On the other hand, location information (i.e., Local Area Code: 7D97) can be used by forensic examiners to locate where the phone was last operating and geographically indicate where a suspect has been or where an event occurred.

Forensic examiners should not neglect the possibility of combining the above information extracted from SIM cards with other evidence collected from the mobile phone and the crime scene itself and construct the case accordingly.

We were able to extract the below information from all SIM cards. The wealth of information varied between various network providers, which proves that the amount of SIM card information can also be reliant on the service provider.

- Integrated Circuit Card Identifier (ICCID)
- International Mobile Subscriber Identifier (IMSI)
- Mobile Station International Subscriber Directory Number (MSISDN) "Own Dialing Num"
- Temporary Mobile Subscriber Identity (TMSI)
- Short Message Service Parameters (SMSP)
- Last Network (LAI-MCC/MNC) & Routing Area Network (RAI-MCC/MNC)
- Last Area Code (LAI-LOC) & Routing Area Location (RAI-LAC)
- Ciphering Key (Kc)
- Abbreviated Dialing Numbers (AND)
- Service Provider Specific Fields

6. CONCLUSION AND FUTURE WORK

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 provides a vast area of possible future work to be conducted, for example, either verification of the extracted data against the real data from the various network providers, a deep extensive search within the SIM card file system, or inspection

© 2016 ADFSL

of extracted data against retrieved user data from various applications and exploring if any of these applications embed any of the SIM data.

 © 2016 ADFSL

REFERENCES

ABI Research: SIM Card Shipments to Reach a Record 5.4 Billion in 2015, but Declining ASPs Force a Shift in Vendor Strategy (2015). Retrieved September 9th, 2015 from: https://www.abiresearch.om/press/sim-card-shipments-to-reach-a-record-54-billion-in/,

Bidgoli, H. (2010). The Handbook of Technology Management, Supply Chain Management, Marketing and Advertising, and Global Management (Vol. 2). John Wiley & Sons.

Boudriga, N. (2009). Security of mobile communications..

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

Cilardo, A.; Mazzocca, N.; Coppolino, L., "TrustedSIM: Towards Unified Mobile Security," in Ubiquitous Intelligence and Computing, 2013 IEEE 10th International Conference on and 10th International Conference on Autonomic and Trusted Computing (UIC/ATC), pp.563-568, 18-21 Dec. 2013
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6726260&isnumber=6726171

European Telecommunications Standards Institute (1994): Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface TS 11.11. Retrieved September 23rd, 2015 from http://www.3gpp.org/specifications.

ISO/IEC 7816: Identification cards -Integrated circuit cards-Part 1: Cards with contacts — Physical characteristics. Retrieved September 10th, 2015 from: https://www.iso.org/obp/ui/#iso:std:iso-iec:7816:-1:ed-2:v1:en

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).

Markantonakis, K. (Ed.). (2007). Smart cards, tokens, security and applications. Springer Science & Business Media.

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.

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.

Singh V., Chauhan S. and Khan G. (2015). Forensic Analysis of SIM Cards for Data Acquisition. AJMS, 3(1), 24-28

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

Willassen, S. (2005). Forensic analysis of mobile phone internal memory. In Advances in Digital Forensics (pp. 191-204). Springer US.

© 2016 ADFSL

 © 2016 ADFSL