Chapter 17

IMAGING AND ANALYSIS OF GSM SIM CARDS

Christopher Swenson, Gavin Manes and Sujeet Shenoi

Abstract Cellular phones are becoming ubiquitous. As of March 2005, there were more than 180 million cellular subscribers in the United States, over 60% of the population. Cellular devices invariably contain information that can aid criminal investigations. Nevertheless, extracting evidence from cellular phones is quite uncommon in the United States. The principal reasons are the lack of awareness and training on the part of law enforcement agents and the limited availability of inexpensive tools for extracting and analyzing evidence. This paper describes a toolkit for extracting and analyzing data from SIM cards, which are used for cryptographic authentication, key generation and data storage in GSM cellular phones.

Keywords: Digital forensics, cellular phones, GSM, SIM cards

1. Introduction

Tools for recovering evidence from computer hard drives and electronic devices are not new in the field of forensics [1, 7, 11]. Nevertheless, extracting evidence from cellular phones is quite uncommon in the United States. The principal reasons are the lack of awareness and training on the part of law enforcement agents and the limited availability of inexpensive tools for extracting and analyzing evidence.

This paper describes the design and implementation of a toolkit for extracting and analyzing data from SIM cards, which are used for cryptographic authentication, key generation and data storage in GSM cellular devices. The toolkit, which has been created specifically for law enforcement agents, will assist in bringing digital evidence from cellular devices to bear in criminal cases.

2. GSM Communications

The Global System for Mobile Communications (GSM) is a second-generation (2G) cellular phone protocol. GSM cellular phones have been selected as the focus of this research for two main reasons.

- GSM is completely standardized. GSM cellular devices are typically usable in any GSM-compliant country with few problems. Furthermore, GSM standards are available free-of-charge, which facilitates the development of forensic tools.
- Each GSM phone contains a smart card for cryptographic functions and data storage. Although GSM handsets differ considerably, the smart cards are standardized, allowing evidence to be extracted using common methods. Data stored on these smart cards can be vital to criminal investigations.

Until recently, GSM penetration in the United States was relatively limited. Most companies, e.g., Verizon, use different cellular networks, such as IS-136 [15] and cdma2000 [9]. However, Cingular and T-Mobile now provide mostly GSM service, and GSM is the fastest growing cellular network in the United States.

GSM cellular telephones incorporate a handset and a smart card. The handset, which is responsible for communicating with the Public Land Mobile Network (PLMN), stores user information and interfaces with the user. The smart card, called the Subscriber Identity Module (SIM), is housed inside the handset. The SIM stores user information and is also responsible for cryptographic authentication and key generation.

Although a considerable amount of information is stored on the handset, extracting it in a forensically sound manner is extremely difficult due to the variety of proprietary interfaces and the lack of documentation for each make and model. As such, the focus of this paper is on extracting and analyzing data from the SIM card rather than the handset.

3. Subscriber Identity Module (SIM) Cards

SIM cards are smart cards that support GSM communications. Smart cards were originally developed to address security issues with magnetic stripe cards that could be read and modified qute easily. The smart card solution incorporated a microprocessor to control access to the memory on the card, and to provide computational power for other operations, e.g., cryptography. The first smart cards deployed in the mid-1980s for use in telephone systems [14] met with immediate success. Smart card usage has increased as they have become more powerful and less expensive, which has enabled them to be used in modern cellular phones.

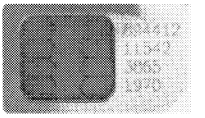

Figure 1. SIM Card (actual size: 25mm × 15mm).

Smart cards typically have two components: memory, which is usually in the form of an EEPROM chip, and a microprocessor, often used to access and protect the memory and to provide cryptographic functionality. These cards were originally made of plastic and were about the size of a credit card, but they have been getting smaller. Most smart cards communicate through a serial data channel using several contact pins. Recently, there has been a surge of contactless cards that communicate wirelessly with host devices.

SIMs are smart cards programmed to support specific GSM operations, notably cryptographic authentication and key generation. They also store some user information. Figure 1 shows a SIM card manufactured for Orange, a GSM provider in the United Kingdom.

4. SIM Card Forensics

During an investigation, it is necessary to ensure that all user information from a SIM card is retrieved. Also, non-user information, e.g., data related to the use of the SIM card as a cryptographic device, which may not be of much importance to the investigation must be retrieved (so long as it does not affect the integrity of the SIM card and user data). Finally, the integrity of the data must be maintained and should be verifiable. This is usually accomplished by computing and storing a series of hashes and checksums on the data.

4.1 SIM Card File Structure

SIM cards incorporate simple hierarchical file structures with certain classes of files used to organize and secure larger groups of files, providing directory-like functionality. Each file has a descriptor byte indicating the file's type, and a location byte that distinguishes individual files. Files can be elementary files, dedicated files or master files. Table 1 lists the different file types and the associated header numbers [6].

The Master File (MF) is a unique file present on all SIM cards. The MF acts as the root directory, and usually has a small number of elementary (data) files, with most files on the SIM card contained in directory-like objects called dedicated files (DFs). An Elementary File (EF) is a container for data, either in records or as a simple byte stream. Records

Table 1. SIM card file types.

Descriptor Byte (Hexadecimal)	File Type
3F	Master File (MF)
2F, 4F, 6F	Elementary File (EF)
5F, 7F	Dedicated File (DF)

can only be accessed in one of two modes for a given EF: "linear-fixed" mode, i.e., each record is accessed as a sequential list (appropriate for contact lists), and "circular" mode, i.e., access is based on recency using a queue (appropriate for call lists).

Table 2. Important SIM card files.

File Name/Location	Description
3F00 7F10 6F3A	Abbreviated Dialing Numbers
3F00 7F10 6F3C	Short Message Service storage
3F00 7F10 6F40	Mobile Subscriber ISDN
3F00 7F20 6F21	International Mobile Subscriber Identity

4.2 SIM Card Files

Table 2 lists the files found on a SIM card that may contain information valuable to investigations [6].

4.2.1 International Mobile Subscriber Identity. The International Mobile Subscriber Identity (IMSI) is a unique 15-digit decimal number, usually encoded as packed Binary Coded Decimal (BCD), that identifies each GSM network user. The IMSI is broken down into several digit groups. The first three digits correspond to the Mobile Country Code (MCC) [8], the next two or three digits constitute the Mobile Network Code (MNC), and the last nine or ten digits comprise the Mobile Subscriber Identification Number (MSIN). The MCC identifies the country where the IMSI is intended to be used, while the MNC identifies the service provider, e.g., T-Mobile, Cingular. Tables 3 and 4 list common MCCs and MNCs, respectively. The MSIN is used by the service provider to identify individual subscribers.

4.2.2 Mobile Subscriber ISDN. The Mobile Subscriber Integrated Services Digital Network (MSISDN) is the standard telephone

Table 3. Common mobile country codes.

Mobile Country Code	Country
208	France
234–235	United Kingdom
310–316	United States
330	Puerto Rico
332	Virgin Islands, U.S.
334	Mexico

Table 4. Common mobile network codes.

MCC	Mobile Network Code	Provider
310	090	Edge Wireless
310	15	BellSouth Mobility DCS
310	150	Cingular Wireless
310	20–27	T-Mobile
310	410	Cingular Wireless

number used to place or receive calls [4]. A SIM card can use several MSISDNs simultaneously – the elementary file has a linear-fixed structure, allowing a small number of MSISDNs to be allocated. However, in practice, it is common for a user to use one MSISDN at a given time.

4.2.3 Contact List. Contact list information is stored primarily in the Abbreviated Dialing Numbers (ADN) file. The ADN contains telephone numbers along with a small amount of text associated with each number, usually a name. Some cellular phones use special grouping information in the text area to assign different ring tones and to differentiate between home, mobile and work numbers.

4.2.4 Short Message Service. Short Message Service (SMS), a service offered by most wireless providers, allows subscribers to exchange short messages of a few hundred characters. This service is popularly called "text messaging." The message format, standardized in [2], contains a source messaging center (essentially a router), the source telephone number, and the message. The alphabet for encoding SMS messages typically has an uncompressed 7-bit format [3]. A message larger than the maximum number of characters is usually split into two or more messages. Normally, only incoming SMS messages are stored on SIM cards. Outgoing messages are stored only in the handset memory, if at all.

5. SIM Card Imaging

The standard forensics practice is to make an exact duplicate of the digital evidence and then perform the analysis on the copy. For SIM cards this is important, as SIM card storage is typically in the form of EEPROM, which has a limited number of read-write cycles. If an investigator were to perform all the analysis on the physical device, it is possible that the device could be permanently damaged. This would compromise the integrity of the evidence as well as undermine the ability to complete the investigation.

This section describes the design of an imaging tool for SIM cards. The tool uses standard smart card readers to obtain data from SIM cards according to the guidelines identified in the previous section.

Tools are available for acquiring data from SIM cards. However, they do not meet the stringent forensic requirements for data acquisition. For example, the `sim_scan` tool gathers most of the data from SIM cards. But it produces a simple text file rather than a secure image file. Also, the program has severe compatibility issues: it only works with certain smart card readers and is unstable with modern versions of Windows. The imaging tool described in this paper was designed from the ground up to satisfy five requirements.

- *Stability*: The imaging tool should work on modern operating systems without terminating unexpectedly.
- *Completeness*: The imaging tool should extract all the data from SIM cards without damaging them.
- *Preservation*: Evidence extraction techniques which are likely to damage the devices should be avoided. For example, no attempts should be made to read files that are marked as protected. These files are protected by numeric passwords. Attempting to guess a password too many times can render a SIM card unusable.
- *Compatiblity*: The tool should work with popular operating systems, smart cards and smart card readers.
- *Speed*: Although speed is not a primary concern, the image extraction process should be fast enough not to encumber investigations.

5.1 Communications

The SIM card imaging tool operates over USB ports, using the Personal Computer Smart Card (PC/SC) interface [13]. Although other

methods were employed in the development process, PC/SC ended up being the most stable.

Smart card readers used during development include the GemPC Twin and the GemPC Key, both distributed by GEMPLUS. The GemPC Twin was used for the initial serial development purposes, while the GemPC Key was used for PC/SC USB development.

Table 5. Image file format.

Size	Description
32 bits	Image Version (currently 0)
64 bits	Standard 64-bit Time-Stamp (milliseconds)
32 bits	Number of Files
0+ bits	Files
32 bits	XOR Checksum
128 bits	MD2 Signature
128 bits	MD5 Signature
160 bits	SHA1 Signature

5.2 SIM Card Image File

The SIM card image file is outlined in Table 5. It contains a version number, time-stamp, files, and the image file hashes and checksums. Each file is merely a small header, with entries for the file name, record size, etc., followed by the file contents.

The image file also contains multiple hashes and checksums of the entire image to ensure data integrity. The hashes are computed in a cascading manner, meaning that each hash depends on the previous hashes.

Multiple hashes help maintain the integrity of the data. Collision attacks are possible, if not practical, for many hashes and checksums [10, 16, 17]. However, even if almost every integrity check used in the file format is broken, it is unlikely that an attack can break all the checksums and hash functions at the same time. This fact ensures that the file format will remain intact for a reasonable period of time.

For example, to compromise the XOR checksum at the end of a chained hash, it is necessary to take the original XOR checksum, perform the XOR checksum on the changed file, and append the bit sequence that is the XOR of the two checksums to the end of the file. However, doing this would change every other hash in an unpredictable manner. Therefore, even if an attack were to compromise another hash function or checksum, it is unlikely that it would keep the XOR checksum intact.

5.3 Personal Computer Smart Card Interface

Initially, the imaging tool was developed solely for serial port communication protocols. However, serial port communication is slow, even for small data transfers. In addition, smart card readers operate poorly over serial ports with many stability problems. Furthermore, serial port communication protocols for GEMPLUS smart card readers change with each chipset revision.

To combat these problems, a more stable, generic smart card interface based on the Personal Computer Smart Card (PC/SC) interface was also implemented. PC/SC is an operating system and transmission medium independent interface, allowing programs to exchange Application Protocol Data Units (APDUs) with any smart card reader that has a valid PC/SC driver [13]. The drivers also allow the program to operate at speeds greater than standard serial port speeds by using a USB interface, which is present on practically every modern computer.

The PC/SC interface was integrated into Java code with the help of JPCSC [12], a set of wrapper classes built using the Java Native Interface (JNI). The JPCSC interface is now the standard used in the imaging program, as it enhances reliability, speed and compatibility.

Using the PC/SC interface, APDUs are sent to the smart card to read the contents [5, 6, 14], enumerate the SIM card files and extract the data from them. The extracted data are then stored in an image file.

6. SIM Card Analysis

This section describes the design and implementation of an image file analysis tool that complements the SIM card imaging tool presented in Section 5. The tool analyzes SIM card image files, but cannot work directly with SIM cards. Nevertheless, it is useful because investigators may not have access to a SIM card during an entire investigation. Moreover, repeated reading of a SIM card can stress and possibly damage its electronic components.

6.1 Interactive Graphical User Interface

The analysis tool incorporates an interactive graphical user interface (GUI) designed for investigators. The GUI integrates several plug-ins, which are responsible for displaying the contents of specific files. New files can be examined by the tool by incorporating additional plug-ins, without recompiling the entire GUI.

The GUI also enables investigators to print formatted reports of data found on SIM cards. These reports can be used for manual analysis as well as for courtroom presentations.

6.2 Recognized Files

Common types of files that are of interest to investigators are displayed in simple, descriptive formats. File locations are displayed in a list on the left-hand side of the GUI, while the contents of a particular file are displayed on the right-hand side.

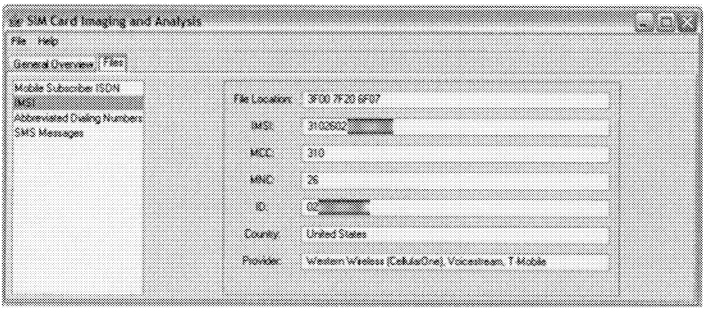

Figure 2. Image file analysis GUI (IMSI)

6.2.1 International Mobile Subscriber Identity. The contents of IMSI files on SIM cards are displayed and analyzed. See Section 4.2.1 for an outline of IMSI file contents. Figure 2 shows the GUI displaying an IMSI file. A portion of the IMSI has been censored so as not to reveal any sensitive information.

6.2.2 Mobile Subscriber ISDN. The MSISDN contains the phone number(s) associated with a SIM card. MSISDNs found on a SIM card are displayed in a standard format. For example, U.S. MSISDNs are presented in the form: `(xxx) yyy-zzzz`. Figure 3 shows the GUI displaying the MSISDN file.

6.2.3 Contact Lists. Contact lists are displayed as accurately as possible. The primary issue with contact lists is that manufacturers often append extra bits of information to the ends of names to provide grouping information, e.g., to assign a specific ring tone for a caller. However, the names and phone numbers should still be identifiable.

Contact lists are found in several SIM files. The most common is the Abbreviated Dialing Numbers (ADN) file, located at `3F00 7F10 3F3A`. Figure 4 shows a GUI display of contact information in an ADN file.

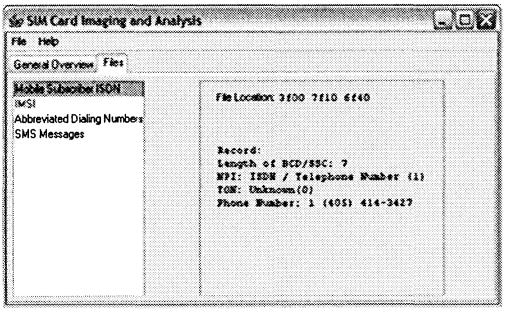

Figure 3. Image file analysis GUI (MSISDN).

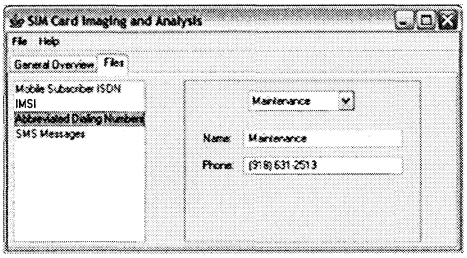

Figure 4. Image file analysis GUI (ADN).

6.2.4 Short Message Service. Short Message Service (SMS), or text messaging, is becoming very popular. The text messages often contain a wealth of information. However, an SMS file on a cellular phone will normally only store incoming messages. Outgoing messages are stored in the device memory, if at all. Figure 5 shows the GUI displaying an SMS file.

6.2.5 Unknown Files. SIM card files that do not have specific plug-ins for recognizing them are processed with a generic plug-in, which displays the data in hexadecimal. Bytes in the ASCII printable character range (numbers, letters, punctuation) are displayed as well.

7. Conclusions

The imaging and analysis tools described in this paper enable law enforcement agents to acquire and analyze information from SIM cards in GSM cellular phones. These tools do not allow investigators to acquire and examine the digital information stored in cellular phone handsets. Nevertheless, information stored in SIM cards is valuable and can be processed without compromising its integrity.

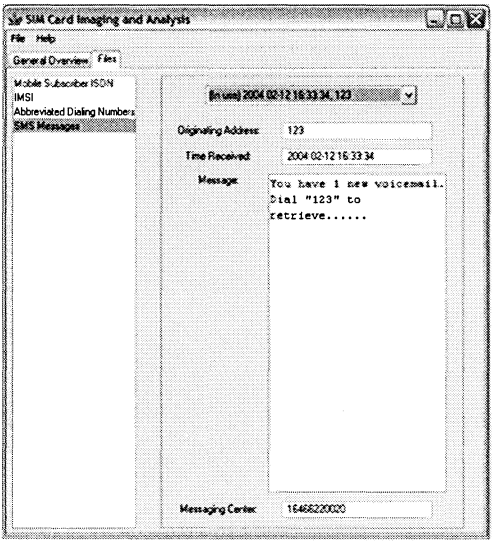

Figure 5. Image file analysis GUI (SMS).

The use of SIM cards as primary storage in cellular phones is waning as flash memory technology (e.g., Secure Digital and CompactFlash) becomes inexpensive. Nevertheless, SIM cards will not disappear anytime soon. The number of GSM subscribers continues to grow. Moreover, Universal SIM (USIM) cards are being deployed with the Universal Mobile Telecommunications System (UMTS), the third generation (3G) successor to GSM. USIM cards are similar to GSM SIM cards and share their physical and logical characteristics. This will permit the implemented tools to be easily extended to USIM card imaging and analysis.

References

[1] B. Carrier, Defining digital forensic examination and analysis tools, *International Journal of Digital Evidence*, vol. 1(4), 2003.

[2] European Telecommunications Standards Institute, 3GPP TS 24.011 v6.0.0 (2003-09), 3rd Generation Partnership Project, Technical Specification Group Core Network; Point-to-Point (PP) Short Message Service (SMS) Support on Mobile Radio Interface (Release 6), 2003.

[3] European Telecommunications Standards Institute, 3GPP TS 23.039 v6.1.0 (2004-09), 3rd Generation Partnership Project, Technical Specification Group Terminals, Alphabets and Language-Specific Information (Release 6), 2004.

[4] European Telecommunications Standards Institute, 3GPP TS 23.040 v5.5.0 (2004-09), 3rd Generation Partnership Project, Technical Specification Group Terminals, Technical Realization of Short Message Service (SMS), (Release 6), 2004.

[5] European Telecommunications Standards Institute, ETSI TS 102 221 v7.0.0 (2004-12), Smart Cards, UICC-Terminal Interface, Physical and Logical Characteristics (Release 7), 2004.

[6] European Telecommunications Standards Institute, ETSI TS 151 011 v4.11.0 (2004-03), Digital Cellular Telecommunications System (Phase 2+), Specification of the Subscriber Identity Module-Mobile Equipment (SIM-ME) Interface (3GPP TS 51.011 Version 4.11.0 Release 4), 2004.

[7] P. Hawkins, Macintosh forensics analysis using OS X (www.sans.org/rr/papers/34/269.pdf), 2002.

[8] International Telecommunications Union, List of E.212 mobile country codes (www.numberingplans.com).

[9] M. Karim and M. Sarraf, *W-CDMA and cdma2000 for 3G Mobile Networks*, McGraw-Hill Professional, Martinsburg, Virginia, 2002.

[10] V. Klíma, Finding MD5 collisions – A toy for a notebook (eprint.iacr.org/2005/075), 2005.

[11] K. Mandia and C. Prosise, *Incident Response: Investigating Computer Crime*, McGraw-Hill, Berkeley, California, 2001.

[12] M. Oestreicher, JPCSC: JNI-wrapper for PCSC (www.zurich.ibm.com/jcop/download/tools/data/jpcsc-0.7.txt).

[13] PC/SC Working Group, Interoperability specification for ICCs and personal computer systems (www.pcscworkgroup.com), 2004.

[14] W. Rankl and W. Effing, *Smart Card Handbook*, John Wiley, Chippenham Wiltshire, Great Britain, 2003.

[15] N. Sollenberger, N. Seshadri and R. Cox, The evolution of IS-136 TDMA for third-generation wireless services, *IEEE Personal Communications Magazine*, vol. 6(3), pp. 8-18, 1999.

[16] X. Wang, Y. Yin and H. Yu, Collision search attacks on SHA1 (theory.csail.mit.edu/~yiqun/shanote.pdf), 2005.

[17] X. Wang and H. Yu, How to break MD5 and other hash functions (www.infosec.sdu.edu.cn/paper/md5-attack.pdf), 2005.