THE JOURNAL OF
DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 1 | Number 2 Article 4

2006

Forensic Tools for Mobile Phone Subscriber Identity Modules

Wayne Jansen
National Institute of Standards and Technology

Rick Ayers
National Institute of Standards and Technology

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

Part of the Computer Engineering Commons, Computer Law Commons, Electrical and Computer Engineering Commons, Forensic Science and Technology Commons, and the Information Security Commons

Recommended Citation

Jansen, Wayne and Ayers, Rick (2006) "Forensic Tools for Mobile Phone Subscriber Identity Modules," *Journal of Digital Forensics, Security and Law*: Vol. 1 : No. 2 , Article 4.
DOI: https://doi.org/10.15394/jdfsl.2006.1006
Available at: https://commons.erau.edu/jdfsl/vol1/iss2/4

This Article is brought to you for free and open access by the Journals at Scholarly Commons. It has been accepted for inclusion in Journal of Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

(c)ADFSL

SAMSUNG 1042

Forensic Tools for Mobile Phone Subscriber Identity Modules

Wayne Jansen
National Institute of Standards and Technology
wjansen@NIST.gov

Rick Ayers
National Institute of Standards and Technology
rayers@NIST.gov

ABSTRACT

Mobile phones and other handheld devices incorporating cellular capabilities, such as Personal Digital Assistants, are ubiquitous. Besides placing calls, these devices allow users to perform other useful tasks, including text messaging and phonebook entry management. When cell phones and cellular devices are involved in a crime or other incident, forensic specialists require tools that allow the proper retrieval and speedy examination of data present on the device. For devices conforming to the Global System for Mobile Communications (GSM) standards, certain data such as dialed numbers, text messages, and phonebook entries are maintained on a Subscriber Identity Module (SIM). This paper gives a snapshot of the state of the art of forensic software tools for SIMs and an explanation of the types of digital evidence they can recover.[1]

Keywords: Mobile Phone, Forensic Tool, Subscriber Identity Module

1. INTRODUCTION

The Global System for Mobile Communications (GSM) standards for cellular networks, originally developed by the European Conference of Postal and Telecommunications Administrations, were continued by the European Telecommunications Standards Institute and are now maintained by the 3rd Generation Partnership Project (3GPP). Commercial GSM service was started in mid-1991. By 1993, thirty-six GSM networks were operating in twenty-two countries (Dechaux and Scheller 1993). Although begun in Europe, GSM is an international standard with compliant networks operational in more than 200 countries around the world (GSM World 2006).

Subscriber Identity Modules (SIMs) are synonymous with mobile phones and devices that interoperate with GSM cellular networks. Under the GSM framework, a cellular phone is referred to as a Mobile Station and is partitioned into two distinct components: the Subscriber Identity Module (SIM) and the Mobile Equipment (ME). As the name implies, a SIM is a removable

[1] Certain commercial products and trade names are identified in this paper to illustrate technical concepts. However, it does not imply a recommendation or an endorsement by NIST

component that contains essential information about the subscriber. The ME, the remaining radio handset portion, cannot function fully without one. The SIM's main function entails authenticating the user of the cell phone to the network to gain access to subscribed services. The SIM also provides a store for personal information, such as phone book entries and text messages, as well as service-related information.

GSM standards are organized in a number of ways, one of them being the phase of capabilities they support. The three phases defined are phase 1, phase 2, and phase 2+, which correspond roughly to first, second, and 2.5 generation network facilities. SIMs are often classified according to the phase of the specifications supported, which is recorded in an element of its file system (i.e., EF_{Phase}). Another class of SIMs in early deployment is UMTS SIMs (USIMS) used in third generation (3G) UMTS (Universal Mobile Telecommunications Service) networks. USIMs are enhanced versions of present-day SIMs, containing backward compatible information.

Some of the earliest, general purpose, forensic tools for mobile phones targeted SIMs, not only because of detailed specifications available for them, but also because of the highly relevant and useful digital evidence that could be recovered. This paper provides a review of present-day forensic tools for SIMs and the type of data they recover, plus an assessment of their capabilities and limitations.

2. SIM CHARACTERISTICS

The SIM-ME partitioning of a cell phone stipulated in the GSM standards has brought about a form of portability. Moving a SIM between compatible cell phones automatically transfers with it the subscriber's identity and the associated information and capabilities. In contrast, present-day CDMA phones do not employ a SIM. Analogous SIM functionality is instead directly incorporated within the device. While SIMs are most widely used in GSM systems, comparable modules are also used in iDEN (Integrated Digital Enhanced Network) phones and UMTS user equipment (i.e., a USIM). Because of the flexibility a SIM offers GSM phone users to port their identity, personal information, and service between devices, eventually all cellular phones are expected to include (U)SIM-like capability. For example, requirements for a Removable User Identity Module (R-UIM), as an extension of SIM capabilities, have been specified for cellular environments conforming to TIA/EIA/IS-95-A and -B specifications, which include Wideband Spread Spectrum based CDMA (3GPP2 2001).

At its core, a SIM is a special type of smart card that typically contains a processor and between 16 to 128 KB of persistent electronically erasable, programmable read only memory (EEPROM). It also includes random access memory (RAM) for program execution, and read only memory (ROM) for the operating system, user authentication and data encryption algorithms, and other

applications. The SIM's hierarchically organized file system resides in persistent memory and stores such things as names and phone number entries, text messages, and network service settings. Depending on the phone used, some information on the SIM may coexist in the memory of the phone. Alternatively, information may reside entirely in the memory of the phone instead of available memory on the SIM.

Though two sizes of SIMs have been standardized, only the smaller size shown in Figure 1 is broadly used in GSM phones today. The module has a width of 25 mm, a height of 15 mm, and a thickness of .76 mm, which is roughly the footprint of a postage stamp. Though similar in dimension to a MiniSD or an MMCmobile removable memory card supported by some cell phones, SIMs follow a different set of specifications with vastly different characteristics. For example, their 8-pin connectors are not aligned along a bottom edge as with removable media cards, but instead form a circular contact pad integral to the smart card chip, which is embedded in a plastic frame. Also, the slot for the SIM card is normally not accessible from the exterior of the phone to facilitate frequent insertion and removal as with a memory card, and instead, typically found in the battery compartment under the battery.

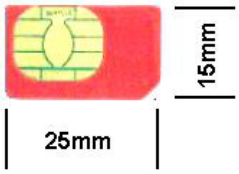

Figure 1: SIM Format

When a SIM is inserted into a phone handset and pin contact is made, a serial interface is used for communicating between them. A SIM can be removed from a phone and read using a specialized SIM card reader and software through the same interface. Standard-size smart card adapters are also available for SIMs, which allows them to be inserted into and read with a conventional smart card reader.

2.1 File System Organization

As shown in Figure 2, the file system of a SIM is organized in a hierarchical tree structure, composed of the following three types of elements (3GPP 2005a):

- **Master File (MF) -** the root of the file system that contains dedicated and elementary files.
- **Dedicated File (DF) -** a subordinate directory to the master file that contains dedicated and elementary files.

- **Elementary File (EF) -** a file that contains various types of formatted data, structures as either a sequence of data bytes, a sequence of fixed size records, or a fixed set of fixed size records used cyclically.

The GSM standards define several important dedicated files immediately under the MF: DF_{GSM}, $DF_{DCS1800}$, and $DF_{TELECOM}$. For the MF and these DFs, several EFs are defined, including many that are mandatory. The EFs under DF_{GSM} and $DF_{DCS1800}$ contain mainly network related information respectively for GSM 900 MHz and DCS (Digital Cellular System) 1800 MHz band operation. EFs for U.S. 850 MHz and 1900 MHz bands are found respectively under those DFs as well, and typically contain identical information. The EFs under $DF_{TELECOM}$ contain service related information. The contents of specific EFs are discussed later in the paper.

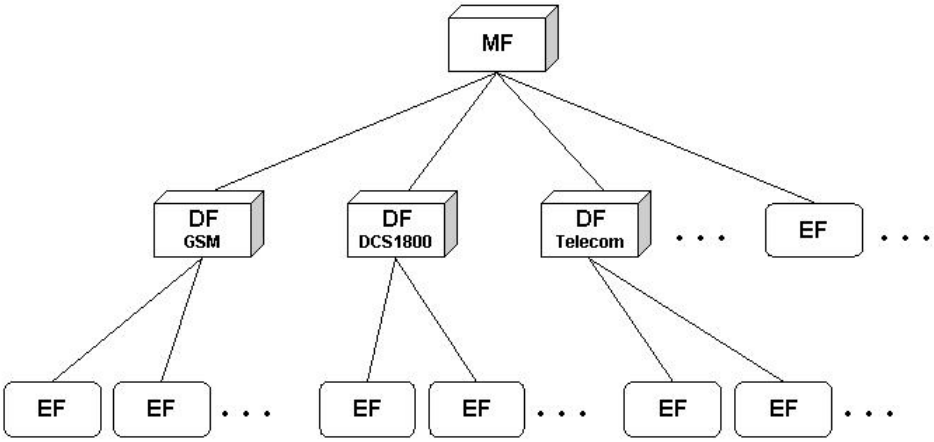

Figure 2: SIM File System

Though SIM file systems are highly standardized, the standards allow flexibility such that their content can vary among network operators and service providers. For example, a network operator might not use an optional file system element, might create an additional element on the SIM for use in its operations, or might install a built-in function to provide a specialized service.

2.2 Security

Smart cards, including SIMs, employ a range of tamper resistance techniques to protect the information they contain. In addition, various levels of rights exist that are assigned to a DF or EF, to control the conditions of access (3GPP 2005a):

- **Always -** Access can be performed without any restriction.

- **Card Holder Verification 1 (CHV1)** - Access can be performed only after a successful verification of the user's PIN, or if PIN verification is disabled.
- **Card Holder Verification 2 (CHV2)** - Access can be performed only after a successful verification of the user's PIN2, or if PIN2 verification is disabled.
- **Administrative** - Access can be performed only after prescribed requirements for administrative access are fulfilled.
- **Never** - Access of the file over the SIM/ME interface is forbidden.

The SIM operating system controls access to an element of the file system based on its access condition of and the type of action being attempted (3GPP 2005a). For example, actions on EFs include searching, reading, and updating the contents. While reading and searching the contents of a particular EF might be allowed without CHV1 verification (i.e., an Always access condition), updating might likely require CHV1 being correctly verified as a prerequisite (i.e., a CHV1 access condition). In general, CHV1 protects core SIM data selectively against unauthorized reading and updating, while CHV2 protects mainly optional data. Both CHVs contain 4-8 digits and can be modified or disabled by the user.

The SIM operating system allows only a preset number of attempts, usually a limit of three, to enter the correct CHV before further attempts are blocked. Submitting the correct Unblock CHV value, also known as a PUK (PIN Unblocking Key), resets the CHV and the attempt counter. If the identifier of the SIM (i.e., its Integrated Circuit Chip Identifier or ICCID) is known, the Unblock CHV for either CHV1 or CHV2 can be obtained from the service provider or the network operator. The ICCID is normally imprinted on the SIM along with the name of the network provider. If needed, the identifier can also be read with a SIM tool from an EF, EF_{ICCID}, since the Always access condition applies by definition. If the number of attempts to enter an Unblock CHV value correctly exceeds a set limit, normally ten attempts, the card becomes blocked permanently.

Authenticating a device to a network securely is a vital function performed via the SIM. Cryptographic key information and algorithms within the tamper resistant module provide the means for the device to participate in a challenge-response dialogue with the network and respond correctly, without exposing key material and other information that could be used to clone the SIM and gain access to a subscriber's services. Cryptographic key information in the SIM also supports stream cipher encryption to protect against eavesdropping on the air interface (Vedder 1993, Willassen 2003).

3. DIGITAL EVIDENCE

Various types of digital evidence can be recovered from a SIM. Evidence can be found scattered throughout the file system in various EFs located under the MF, as well as under the aforementioned DFs. Several general categories of evidence can be identified:

- Service-related Information
- Phonebook and Call Information
- Messaging Information
- Location Information.

The remainder of this section reviews EFs commonly used by forensic specialists, which fall under each category (Dearsley 2005, Willassen 2003). The standardized EF names and abbreviations found in the 3GPP TS 11.11 Technical Specification (3GPP, 2005a), though sometimes unusual, are used throughout this discussion for consistency.

3.1 Service-related Information

The *Integrated Circuit Card Identification* (ICCID) is a unique numeric identifier for the SIM that can be up to 20 digits long. It consists of an industry identifier prefix (89 for telecommunications), followed by a country code, an issuer identifier number, and an individual account identification number (ITU-T, 2006). Aside from the prefix, the components of an ICCID are variable, making them sometimes difficult to interpret. The ICCID can be read from the SIM without providing a PIN and can never be updated. The country code and issuer identifier can be used to determine the network operator providing service and obtain call data records for the subscriber.

The *International Mobile Subscriber Identity* (IMSI) is a unique 15-digit numeric identifier assigned to the subscriber. It has a somewhat similar structure to the ICCID: a Mobile Country Code (MCC), a Mobile Network Code (MNC), and a Mobile Subscriber Identity Number (MSIN) assigned by the network operator. The MCC is 3 digits, while the MNC may be either 2 or 3 digits, with the MSIN taking up the remainder. The forth byte of another EF, Administrative Data (AD), gives the length of the MNC (3GPP 2006). Networks use IMSIs to identify which network a device owner subscribes and, if not their network, whether to allow those network subscribers to access service.

The ICCID and IMSI can be used reliably to identify the subscriber and the network operator providing service. Since these identifiers can be misinterpreted, however, other SIM data can help confirm a finding.

The *Mobile Station International Subscriber Directory Number* (MSISDN) is intended to convey the telephone number assigned to the subscriber for

receiving calls on the phone. Unlike the ICCID and IMSI, however, the MSISDN is an optional EF. If present, its value can be updated by the subscriber, making it a less reliable data source, since it would then be inconsistent with the actual number assigned.

The *Service Provider Name* (SPN) is an optional EF that contains the name of the service provider. If present, it can be updated only by the administrator (i.e., Administrator access). Similarly, the *Service Dialling Numbers* (SDN) EF contains numbers of special services such as customer care and, if present, can help identify to which network the SIM is registered.

3.2 Phonebook and Call Information

The *Abbreviated Dialling Numbers* (ADN) EF retains a list of names and phone numbers entered by the subscriber. The storage allows commonly dialed phone numbers to be selected by name and updated or called using a menu or special buttons on the phone, providing rudimentary phonebook operation. Most SIMs provide around 100 slots for ADN entries.

The *Last Numbers Dialled* (LND) EF contains a list of the most recent phone numbers called by the device. A name may also be associated with an entry and stored with a number (e.g., a called phonebook entry). Though a number appears on the list, a connection may not have been successful, only attempted. Most SIMs provide only a limited number of slots (e.g., ten) for these entries. Some phones do not store called numbers on the SIM and instead rely on their own memory for storage.

3.3 Messaging Information

Text messaging is a means of communication in which messages entered on one cell phone are sent to another via the mobile phone network. The *Short Message Service* (SMS) EF contains text and associated parameters for messages received from or sent to the network, or are to be sent out as an MS-originated message. SMS entries contain other information besides the text itself, such as the time an incoming message was sent, as recorded by the mobile phone network, the sender's phone number, the SMS Center address, and the status of the entry. The status of a message entry can be marked as free space or as occupied by one of the following: a received message to be read, a received message that has been read, an outgoing message to be sent, or an outgoing message that has been sent. Messages deleted via the phone interface are often simply marked as free space and retained on the SIM until they are overwritten. When a new message is written to an available slot, the unused portion is filled with padding, overwriting any remnants of a previous message that might be there.

The capacity for stored messages varies among SIMs. Many cell phones also use their own internal memory for storing text messages. The choice of memory where messages are stored (i.e., SIM or phone) can vary depending on

the phone software and user settings (Willassen 2005). For example, a default arrangement might be for all incoming messages to be stored on the memory of the SIM before using internal phone memory, while outgoing messages are stored only if explicitly requested. Phone models of a particular generation and manufacturer often behave consistently in this respect (Willassen 2005).

The maximum length of a single SMS message entry is 160 characters of text. Messages exceeding that length must be broken down into smaller segments by the sending phone and reassembled by the receiving phone. This feature is especially useful for foreign languages character sets such as Chinese or Arabic whose encoding consumes more than twice the number of bits per character than with English. A reference number parameter identifies the entries whose segments require reassembly. Such messages are referred to as concatenated messages. SMS messages may originate through other means than a cell phone, such as from an Internet SMS server or through electronic mail.

An SMS message can be coded in different ways. The original and most common encoding scheme is a GSM-specific 7-bit character set packed into a bit stream (3GPP 1999). Such an encoding cannot be readily interpreted directly from the raw data using a hex editor, nor supports all languages. Support for other character sets, such as 16-bit Unicode, was added for languages whose alphabet cannot be represented using the original Western European character set (3GPP 2005b).

An *Enhanced Messaging Service* (EMS) was defined as a way to extend SMS message content to allow simple multimedia messages to be conveyed. EMS messages can contain not only formatted text with different font styles and fonts, but also black and white bitmap pictures and monophonic melodies (3GPP 2005b). EMS message content resides in the SMS EF along with SMS message content. EMS messaging is essentially an application-level content extension to SMS, which conforms to the general SMS message structure and support for concatenated messages. EMS-enabled devices are backward compatible by definition with SMS-enabled devices.

3.4 Location Information

A GSM network consists of distinct radio cells used to establish communications with mobile phones. Cells are grouped together into defined areas used to manage communications. Phones keep track of the area under which they fall for both voice and data communications. The *Location Information* (LOCI) EF contains the *Location Area Information* (LAI) for voice communications. The LAI is composed of the MCC and MNC of the location area and the *Location Area Code* (LAC), an identifier for a collection of cells. When the phone is turned off, the LAI is retained, making it possible to determine the general locale where the phone was last operating. Because a location area can contain hundreds or more cells, the locale can be quite broad.

However, it can nevertheless be useful in narrowing down the region where the event occurred.

Similarly, the *GPRS Location Information* (LOCIGPRS) EF contains the *Routing Area Information* (RAI) for data communications over the General Packet Radio Service (GPRS). The RAI is composed of the MCC and MNC of the routing area and the LAC, as well as a *Routing Area Code* (RAC), an identifier of the routing area within the LAC. Routing areas may be defined the same as location areas or they may involve fewer cells, providing greater resolution.

4. FORENSICS TOOLS

The main objective of a forensic SIM tool is to extract digital evidence present in the file system. Besides acquisition, most forensic SIM tools support a range of examination and reporting functions. Some tools deal exclusively with SIMs, while others are part of a complete toolkit that also addresses handsets.

The most important characteristic of a forensic tool is its ability to maintain the integrity of the original data source being acquired and also that of the extracted data. The former is done by blocking or otherwise eliminating write requests to the device containing the data. The latter is done by calculating a cryptographic hash of the contents of the evidence files created and recurrently verifying that this value remains unchanged throughout the lifetime of those files. Preserving integrity not only maintains credibility from a legal perspective, it also allows any subsequent investigation use the same baseline for replicating the analysis.

A number of products are available for managing user data on a SIM. They allow certain data to be read onto a personal computer, updated, and rewritten back to the SIM. Tools such as these are questionable, since they are not designed specifically for forensic purposes. Given the number of forensic tools available, SIM management tools should be avoided.

The SIM must be removed from the phone and inserted into an appropriate reader for acquisition. Unlike forensic acquisition of a hard drive, capturing a direct image of the data is not a sensible option because of the protection mechanisms built into the SIM. Instead, command directives called Application Protocol Data Units (APDUs) are sent to the SIM to extract data, without modification, from relevant EFs in the file system (Casadei 2005). The APDU protocol is a simple command-response exchange. Each element of the file system defined in the standard has a unique numeric identifier assigned, which can be used to reference the element and perform some operation, such as reading the contents in the case of an acquisition tool (3GPP 2005a).

Forensic SIM tools require either a specialized reader that accepts a SIM directly or a general-purpose reader for a full-size smart card. For the latter, a standard-size smart card adapter is needed to house the SIM for use with the reader. Table 1 lists several SIM forensic tools and which of the primary functions of acquisition, examination, and reporting are supported. The first four listed, Cell Seizure, GSM .XRY, Mobiledit!, and TULP2G, also handle phone memory acquisition. Note that some SIM data, but not all, can be recovered via the handset using such tools. However, some forensic issues may arise when acquiring SIM data via the phone. The most common one is that the status of an "unread" message can be changed to "read."

Table 1: SIM Tools

Tool	Function
Cell Seizure	Acquisition, Examination, Reporting[2]
GSM .XRY	Acquisition, Examination, Reporting[3]
Mobiledit! Forensic	Acquisition, Examination, Reporting[4]
TULP 2G	Acquisition, Reporting[5]
Forensic Card Reader	Acquisition, Reporting[6]
ForensicSIM	Acquisition, Examination, Reporting[7]
SIMCon	Acquisition, Examination, Reporting[8]
SIMIS	Acquisition, Examination, Reporting[9]

4.1 Evidence Recovery

While all of the stored SIM data may potentially have evidentiary value, a good deal of the data is network service related and has little direct evidentiary value. Generally, SIM forensic tools do not recover every possible item on a SIM. The breadth of coverage also varies considerably among tools. Table 2 entries give an overview of those items recovered, listed at the left, by the various SIM forensic tools, listed across the top.

[2] Version 2.0.0.33660, see www.paraben-forensics.com

[3] Version 2.5, see www.msab.com/en

[4] Version 1.95, see www.mobiledit.com

[5] Version 1.1.0.2, see tulp2g.sourceforge.net

[6] Version 1.0.1, see www.becker-partner.de/forensic/intro_e.htm

[7] Version 1.3.0.0, see www.radio-tactics.com/forensic_sim.htm

[8] Version 1.1, see www.simcon.no

[9] Version 2.0.13, see www.crownhillmobile.com

Table 2: Content Recovery Coverage

	Cell Seizure	GSM .XRY	Mobiledit!	TULP 2G	FCR	Forensic SIM	SIMCon	SIMIS
IMSI	X	X	X	X	X	X	X	X
ICCID	X	X	X	X	X	X	X	X
MSISDN	X	X		X	X	X	X	X
SDN	X			X		X	X	X
SPN	X			X		X	X	X
Phase	X	X	X			X	X	X
ADN	X	X	X	X	X	X	X	X
LND	X	X	X	X	X	X	X	X
SMS/EMS								
• ***Occupied***	X	X	X	X	X	X	X	X
• ***Deleted***	X	X		X		X	X	X
LOCI	X	X		X	X	X	X	X
GPRSLOCI	X					X	X	X

4.2 Decoding and Translation

Forensic tools can present acquired data to the user in several ways, as illustrated in Figure 3. Each step, however, can introduce errors. The most basic form is the raw encoded data received in response to an APDU request. As mentioned earlier, text encoded in the packed 7-bit GSM alphabet is onerous and time consuming to decode manually. Another less onerous decoding involved binary coded decimal (BCD) numeric identifiers. Most, but not all, tools decode raw data into a usable form for interpretation by the user, wherever possible.

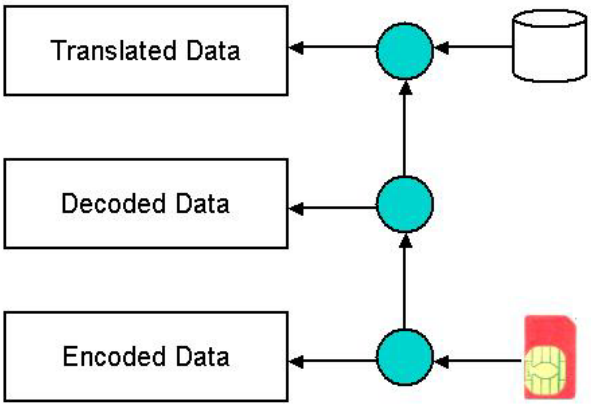

Figure 3: Data Decoding and Translation

Several tools go beyond decoding and attempt to translate the decoded data into a form more meaningful to the user, using some database. Translation is particularly the case with numeric data. For example, the BCD-encoded value of the MCC and MNC portion of the LAI, "130014," decodes to "310410," where 310 is the MCC value and 410 is the MNC value. The country code 310 is assigned to the United States, while the network code 410 is assigned to Cingular.

5. TOOL ASSESSMENT

SIMs are highly standardized devices whose interface, behavior, and content are relatively uniform. All of the SIM tools broadly support any SIM for acquisition via an external reader. Scenarios were used to populated SIM data to gauge the capabilities of the forensic tool to acquire information. The emphasis in the scenarios is on loading the SIM with specific kinds of information for recovery. Once a scenario is performed using a suitable GSM phone or SIM management program, the tool can logically acquire the SIM.

The scenarios are not intended to be exhaustive or to serve as a formal product evaluation. However, they attempt to cover a range of data commonly encountered when examining a SIM and are useful in determining the capabilities afforded an examiner. Table 3 gives an overview of the SIM scenarios. Note that none of the scenarios attempt to confirm whether the integrity of the data on a SIM is preserved when applying a tool – that topic was outside the scope of the effort.

Table 3: SIM Scenarios

Scenario	Description
Basic Data	Determine whether the tool can recover core subscriber (i.e., IMSI, ICCID, and SPN elementary files), phonebook (i.e., ADN elementary file), call (i.e., LND

Scenario	Description
	elementary file), and SMS message information on the SIM, including deleted SMS entries, and whether all of the data is properly decoded and displayed.
Location Data	Determine whether the tool can recover location-related information (i.e., LOCI and LOCIGPRS elementary files), on the SIM, and whether all of the data is properly decoded and displayed.
EMS Data	Determine whether the tool can recover EMS messages over 160 characters in length and containing non-textual content, and whether all of the data is properly decoded and displayed for both active and deleted messages.
Foreign Language Data	Determine whether the tool can recover SMS messages and phonebook data from the SIM that are in a foreign language, and whether all of the data is properly decoded and displayed.

The scenario results for each tool are weighed against the predefined expectations and assigned a ranking. The entry "Meet" indicates that the software met the expectations of the scenario for the device in question. Since the scenarios are acquisition oriented, this ranking generally means that all of the identified data was successfully recovered. Similarly, the entry "Below" indicates that the software fell short of fully meeting expectations.

A "Below" ranking is often a consequence of a tool performing a logical acquisition and being unable to recover deleted data, which is understandable. However, the ranking may also be due to active data on the device not being successfully recovered, which is more of a concern. A good example of this is SMS messages that have been deleted, but not overwritten by another message. The entry "Miss" indicates that the software unsuccessfully met any expectations, highlighting an area for improvement.

Table 4 gives a summary of the results for each tool used with several test SIMs: the 5343 from T-Mobile, the 8778 from Cingular, and the 1144 from AT&T. Note that very few misses were experienced. The main ones were due to difficulties that Cell Seizure and Forensic SIM had in successfully acquiring any data from the Cingular SIM. The remaining ones were due to the limited breadth of coverage Mobiledit! has for SIM data, as noted earlier in Table 2.

Table 4: Tool Result Summary

Tool	Scenario	SIM		
		5343	8778	1144
Cell Seizure	Basic Data	Meet	Miss	Meet
	Location Data	Meet	Miss	Meet
	EMS Data	Below	Miss	Below
	Foreign Language Data	Below	Miss	Below
GSM .XRY	Basic Data	Meet	Meet	Meet
	Location Data	Below	Below	Below
	EMS Data	Meet	Meet	Meet
	Foreign Language Data	Below	Below	Below
Mobiledit! Forensic	Basic Data	Below	Below	Below
	Location Data	Miss	Miss	Miss
	EMS Data	Below	Below	Below
	Foreign Language Data	Below	Below	Below
TULP 2G	Basic Data	Meet	Meet	Meet
	Location Data	Below	Below	Below
	EMS Data	Meet	Meet	Below
	Foreign Language Data	Meet	Meet	Meet
Forensic Card Reader	Basic Data	Below	Below	Below
	Location Data	Below	Below	Below
	EMS Data	Below	Below	Below
	Foreign Language Data	Below	Below	Below
ForensicSIM	Basic Data	Meet	Miss	Below
	Location Data	Meet	Miss	Below
	EMS Data	Below	Miss	Below
	Foreign Language Data	Below	Miss	Below
SIMCon	Basic Data	Meet	Below	Below
	Location Data	Meet	Meet	Meet
	EMS Data	Meet	Meet	Meet
	Foreign Language Data	Meet	Meet	Meet
SIMIS	Basic Data	Meet	Meet	Meet
	Location Data	Meet	Below	Below
	EMS Data	Below	Below	Below
	Foreign Language Data	Below	Below	Below

The remainder of this section discusses areas where the forensic tools fell below expectations and gives some specific examples. A more comprehensive discussion is available elsewhere (Ayers, R. et al. 2005).

5.1 Basic Data

Generally, recovering Basic Data posed little problems for most tools, with the exception of deleted SMS data. Certain tools did not recover some useful data, as noted in Table 2. A more serious concern was that a couple of the tools failed to acquire the SIM at all. One tool failed to display the full name of a maximum size phonebook entry and another truncated all names by one character. In both cases, other output provided by tools could be used to view the missing characters. One tool consistently prepended the IMSI with a parity quartet.

An interesting problem occurred in translating the IMSI values of the SIMs. Several European tools failed to translate the IMSI correctly, ignoring the AD value that contains the size of the MNC portion to use when decoding the value to a network name, and instead defaulting to 2-digits. Because North American MNCs are 3-digit in size, a translation error occurred. However, because the decoded data used for translation was also provided, one could manually perform a correct translation.

5.2 Location Data

As noted in Table 2, several tools recovered LOCI, but not LOCIGPRS data. One tool recovered neither. One of the tools that recovered data failed to report the MCC/MNC portions of the LAI, while another incorrectly presented a LOCI component value.

The MNC portion of the LAI, a three-digit value, was incorrectly decoded by one tool. A couple of the tools did not attempt to translate the LAI and RAI codes into a network name and avoided the problem. One of them did not even attempt to decode the raw data to simplify manual translation.

5.3 EMS Data

Recovery of EMS text messages greater that 160 characters posed little problems for most tools, except for two tools that had problems recovering deleted EMS messages, the same ones noted in Table 2 for deleted SMS messages. EMS messages bearing images were a different story. Two sizes of images were embedded with text: small 16x16 pixel and large 32x32 pixel images. The results are shown in Table 5.

Only two of the tools, GSM .XRY and SIMCon successfully acquired and displayed both size of embedded images. The only other tool to acquire an image successfully, TULP 2G, did so only for the small image. For the large image, it failed to report the presence of the message, missing it entirely. Two of the other tools successfully recovered the text, but misinterpreted the image

value, while another tool recovered the text and provided a notification that image data was present.

Table 5: Picture Messages with Text

	Text & Small Image	Text & Large Image
Cell Seizure	Unsuccessful Acquisition – Cingular SIM	lßìOß&/Ψà
GSM XRY	Picture msg	Emspictur
Mobiledit!	Picture msg	Emspictur
TULP 2G	Picture msg	Missed Entirely
SIMIS	@@@@@@@x?P¡K?□▯ ▯ ▯ 00@@@@@@@@**Picture msg**	?@@@□@@▯ 耀@??@@?@(@$@?@?@?□□?4p@@Dฆ?(Xq?x7□ @q,?@p巀@ba?@@D? @??P?@x였@?@p时@??@$?????8x셈@□□□S□▯ **mspictur**
Forensic SIM	Unsuccessful Acquisition – Cingular SIM	Header – Large Picture User Data – **Emspictur**
Forensic CR	#"èY@@@@@@@@@x£PòBaK?ààààlÆ??00@@@@@@@@**Picture msg**	¥!èL@@p£@@@ß@@@?è@@@££@@ò @@¡@ò@@è@$@¿@¿@üàà àààààààààà?4p@@DàøÆ¡(Xq¥x7? @q,¥@på7@@baù@¿Él@@D¥ @¡?P£@xì?@@à@¥@på0@@ü£ù@¿É¿@$ö¥ø¿¡?¡£8xìÆ @@àààààààààSàààà?**Emspictu**
SIMCon	Picture msg	Emspictur

5.4 Foreign Language Data

Foreign language data occurred in both the ADN phonebook and SMS message entries. Both French and Asian characters were used. Table 6 illustrates the

results for SMS messages. Only one tool failed to display French language messages correctly. However, using a dump feature, the correct data could be found. For Asian messages, only one tool, SIMCon, correctly displayed the message. Most of the others came close, but appended spurious characters. The remainder garbled the message contents, though the date/time stamp and other header information were presented correctly.

The results for French and Asian ADN entries generally followed those for SMS messages. However, one of the tools performed worse for French ADN entries than for SMS message entries, while another performed worse for Asian ADN entries than for SMS message entries.

Table 6: Foreign Language Messages

	French	**Asian**
Cell Seizure	Il est entété mais sincère	Headers OK, Message Garbled
GSM XRY	Il est entété mais sincère	阿婆家里面对于是否则的确实现在家里面对于—阿婆
Mobiledit!	Il est entété mais sincère	阿婆家里面对于是否则的确实现在家里面对于l啟签
TULP 2G	Il est entété mais sincère	阿婆家里面对于是否则的确实现在家里面对于—??
SIMIS	Il est ent鴩 mais sinc航	阿婆家里面对于是否则的确实现在家里面对于—
Forensic SIM	Il est entété mais sincère	Headers OK, Message Garbled
Forensic CR	Il est entété mais sincère	Headers OK, Message Garbled
SIMCon	Il est entété mais sincère	阿婆家里面对于是否则的确实现在家里面对于

6. CONCLUSIONS

Forensic examination of cellular devices is a growing subject area in computer forensics. Forensic examination tools translate data to a format and structure that is understandable by the examiner and can be effectively used to identify and recover evidence. However, tools may contain some degree of inaccuracies. For example, the tool's implementation may contain a programming error; a specification used by the tool to translate encoded bits into data comprehensible by the examiner may be inaccurate or out of date; or the protocol used to access the SIM may be incorrect, causing the tool to function improperly in certain situations.

Over time, experience with a tool provides an understanding of its limitations, allowing an examiner to compensate where possible for any shortcomings or to turn to other means of recovery. Practice in mock examinations can help gain an in-depth understanding of a tool's capabilities and limitations, which often involve subtle distinctions, and also provide the opportunity to customize facilities of the tool for later use.

Forensic software tools for SIMs are in the mid-stages of maturity. While the tools discussed in this paper generally performed well and had adequate functionality, new versions are expected to improve and better meet investigative requirements. For instance, during the course of preparing this paper, a new version for nearly every tool was issued, which included functionality enhancements and occasionally some deficiencies. Because variability can occur between versions of tools, quality measures should be applied to ensure that results remain consistent and any variations understood.

7. REFERENCES

3GPP (1999), Alphabets and Language-specific Information, 3rd Generation Partnership Project, TS 03.38, version 7.2.0 (Release 1998), Technical Specification (1999-07).

3GPP (2005a), Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface, 3rd Generation Partnership Project, TS 11.11 V8.13.0 (Release 1999), Technical Specification, (2005-06).

3GPP (2005b), Technical Realization of the Short Message Service (SMS), 3rd Generation Partnership Project, TS 23.040 V6.6.0 (Release 6), Technical Specification (2005-12).

3GPP (2006), Numbering, Addressing and Identification, 3rd Generation Partnership Project, TS 23.003, V6.9.0 (Release 6), Technical Specification (2006-03)

3GPP2 (2001), Removable User Identity Module for Spread Spectrum Systems, 3rd Generation Partnership Program 2, 3GPP2 C.S0023-0, Version 4.0, June 15.

Ayers, R. et al. (2005), Cell Phone Forensic Tools: An Overview and Analysis, NIST Interagency Report - 7250, <URL: http://csrc.nist.gov/publications/nistir/nistir-7250.pdf>

Casadei, F. et al. (2005), SIMbrush: an Open Source Tool for GSM and UMTS Forensics Analysis, First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05), November 7-9, pp. 105-119.

Dearsley, T. (2005), Mobile Phone Forensics – Asking the Right Questions, New Law Journal, July 29, pp. 1164-1165.

Dechaux, C., Scheller, R. (1993), What are GSM and DECT?, Electrical Communication, 2nd Quarter, pp. 118-127.

GSM World (2006), GSM Global Networks on Air, <URL: http://www.gsmworld.com/news/statistics/networks_complete.shtml>.

ITU-T (2006), Automatic International Telephone Credit Cards, International Telecommunications Union, Telecommunication Standardization Sector (ITU-T), Recommendation E.118, (02/01).

Vedder, K. (1993), Security Aspects of Mobile Communications, in Computer Security and Industrial Cryptography - State of the Art and Evolution, Lecture Notes in Computer Science, Vol. 741, pp. 193-210.

Willassen, S. (2003), Forensics and the GSM Mobile Telephone System, International Journal of Digital Evidence, Volume 2, Issue 1, <URL: http://www.utica.edu/academic/institutes/ecii/publications/articles/A0658858-BFF6-C537-7CF86A78D6DE746D.pdf>.

Willassen, S. (2005), Forensic Analysis of Mobile Phone Internal Memory, IFIP International Conference on Digital Forensics, National Center for Forensic Science, Orlando, Florida, February 13-16, in Advances in Digital Forensics, Vol. 194, Pollitt, M.; Shenoi, S. (Eds.), XVIII, 313 p., 2006.

AUTHOR BIOGRAPHIES

Wayne Jansen, BS and MS Computer Science, MS Engineering Management, is a Principal Computer Scientist at the National Institute of Standards and Technology, Computer Security Division, in Gaithersburg, Maryland. His research interests are in communications, distributed applications, and computer security. Currently, he leads the Mobile Security Project, focused on mobile software and handheld devices.

Rick Ayers is a Computer Scientist in the Information Technology Laboratory at the National Institute of Standards and Technology (NIST) in Gaithersburg, MD. Rick graduated from the University of Tulsa with a BS and MS in

Computer Science. His current research focus is on mobile device forensic tools and proper acquisition techniques.