International Journal of Multidisciplinary Allied Research Review and Practices
www.ijmarrp.com (Volume 1, Issue 1, August 2015)
IJMARRP

"An Approach for Mobile Phone SubscriberIdentity Modules: Mobile Forensic Tools"

Farman Ali
Research Scholar
Department of Computer Science
Shri JJT Univeristy, Jhunjhunu, Rajasthan

Abstract

The Mobile phones and various other handheld devices that incorporated Personal Digital Assistant are ubiquitous. These devices allow users to perform phonebook entry management and text messaging except placing calls. Forensic specialists are very important tools for speedy examination and retrieval of data that are present on the handheld devices if mobile phones and other handheld devices are involved in a crime or other incident. For devices fitting in with the Global System for Mobile Communications (GSM) principles, certain information, for example, dialed numbers, instant messages, and phonebook entries are kept up on a Subscriber Identity Module (SIM). This paper gives a preview of the best in class of forensic software tools for SIMs and a clarification of the sorts of advanced confirmation they can recoup.

Keywords: Mobile Phone, Forensic Tool, Subscriber Identity Module

1. Introduction

The Global System for Mobile Communications (GSM) benchmarks for cell systems, initially created by the European Conference of Postal and Telecommunications Administrations, were proceeded by the European Telecommunications Standards Institute and are presently kept up by the third Generation Partnership Project (3GPP).Commercial GSM administration was begun in mid-1991. By 1993, thirty-six GSM systems were working in twenty-two nations (Dechaux and Scheller 1993).Despite the fact that started in Europe, GSM is a universal standard with agreeable systems operational in more than 200 nations around the globe (GSM World 2006).

Subscriber Identity Modules (SIMs) are synonymous with cell telephones and devices that interoperate with GSM cell systems. Under the GSM system, a wireless is alluded to as a Mobile

Station and is parceled into two particular segments: the Subscriber Identity Module (SIM) and the Mobile Equipment (ME).As the name suggests, a SIM is a removable part that contains crucial data about the subscriber. The ME, the staying radio handset bit, can't work completely without one.The SIM's fundamental capacity involves verifying the client of the wireless to the system to obtain entrance to subscribed administrations. The SIM likewise gives a store to individual data, for example, telephone directory passages and instant messages, and in addition administration related data.

There are the numbers of ways; we can organize the GSM standards, i.e. phase of capabilities they support. There are three phase defined as phase 1, phase 2 and phase 2^+ and called as first, second and 2.5 generation networks. SIMs are regularly arranged by period of the determinations upheld, which is recorded in a component of its document framework (i.e., EFPhase). Another class of SIMs in ahead of schedule organization is UMTS SIMs (USIMS) utilized as a part of third era (3G) UMTS (Universal Mobile Telecommunications Service) systems. USIMs are upgraded adaptations of present-day SIMs, containing in reverse good data.

A percentage of the most punctual, broadly useful, forensic tools for cellular telephones focused on SIMs, not just as a result of detailed details accessible for them, additionally in view of the exceedingly important and helpful advanced confirmation that could be recouped. This paper gives an audit of present-day criminological instruments for SIMs and the sort of information they recuperate, in addition to an appraisal of their capacities and restrictions.

2. SIM CHARACTERISTICS

The SIM-ME parceling of a mobile phone stipulated in the GSM guidelines has realized a type of transportability. Moving a SIM between good PDAs consequently exchanges with it the supporter's personality and the related data and abilities.Interestingly, introduce day CDMA telephones don't utilize a SIM. Practically equivalent to SIM usefulness is rather straightforwardly fused inside of the gadget. While SIMs are most broadly utilized as a part of GSM frameworks, equivalent modules are additionally utilized as a part of iDEN (Integrated Digital Enhanced Network) telephones and UMTS client hardware (i.e., a USIM). Due to the adaptability a SIM offers GSM telephone clients to port their character, individual data, and administration between gadgets, in the long run every single mobile phone are relied upon to

incorporate (U)SIM-like capacity. For instance, prerequisites for a Removable User Identity Module (R-UIM), as an augmentation of SIM abilities, have been determined for cell situations fitting in with TIA/EIA/IS-95-An and - B determinations, which incorporate Wideband Spread Spectrum based CDMA (3GPP2 2001).

At its center, a SIM is an extraordinary kind of shrewd card that ordinarily contains a processor and between 16 to 128 KB of tireless electronically erasable, programmable read just memory (EEPROM). It likewise incorporates irregular access memory (RAM) for project execution, and read just memory (ROM) for the working framework, client validation and information encryption calculations, and different applications. The SIM's progressively sorted out document framework lives in constant memory and stores such things as names and telephone number passages, instant messages, and system administration settings. Contingent upon the telephone utilized, some data on the SIM may exist together in the memory of the telephone. Then again, data may dwell altogether in the memory of the telephone rather than accessible memory on the SIM. In spite of the fact that two sizes of SIMs have been institutionalized, just the littler size indicated in Figure 1 is comprehensively utilized as a part of GSM telephones today. The module has a width of 25 mm, a tallness of 15 mm, and a thickness of .76 mm, which is generally the foot shaped impression of a postage stamp. In spite of the fact that comparable in measurement to a MiniSD or aMMCmobile removable memory card upheld by some PDAs, SIMs take after an alternate arrangement of determinations with immensely distinctive attributes. For instance, their 8-pin connectors are not adjusted along a base edge as with removable media cards, however rather shape a roundabout contact cushion indispensable to the keen card chip, which is inserted in a plastic casing. Likewise, the opening for the SIM card is regularly not available from the outside of the telephone to encourage successive insertion and evacuation as with a memory card, and rather, normally found in the battery compartment under the battery.

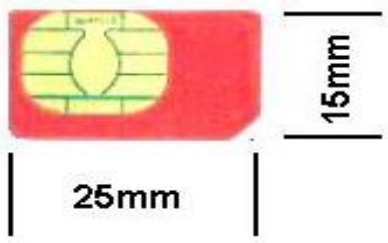

Figure 1: SIM Format

When a SIM is inserted into a phone handset and pin contact is made, a serialinterface is used for communicating between them. A SIM can be removedfrom a phone and read using a specialized SIM card reader and softwarethrough the same interface. Standard-size smart card adapters are alsoavailable for SIMs, which allows them to be inserted into and read with aconventional smart card reader.

3. DIGITAL EVIDENCE

Different sorts of computerized confirmation can be recouped from a SIM. Confirmation can be discovered scattered all through the record framework in different EFs situated under the MF, and also under the previously stated DFs. A few general classes of proof can be distinguished:

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

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

3.1 Service-related Information

The Integrated Circuit Card Identification (ICCID) is a remarkable numeric identifier for the SIM that can be up to 20 digits in length. It comprises of an industry identifier prefix (89 for information transfers), trailed by a nation code, a backer identifier number, and an individual record recognizable proof number (ITUT, 2006). Beside the prefix, the segments of an ICCID are variable, making them once in a while hard to translate. The ICCID can be perused from the SIM without giving a PIN and can never be redesigned. The nation code and backer identifier

can be utilized to focus the system administrator giving administration and get call information records for the subscriber.

The subscriber is assigned a 15-digit numeric identifier by the *International Mobile Subscriber Identity* (IMSI). It has a some degree comparable structure to the ICCID: a Mobile Country Code (MCC), a Mobile Network Code (MNC), and a Mobile Subscriber Identity Number (MSIN) assigned by the system administrator. The MCC is 3 digits, while the MNC may be either 2 or 3 digits, with the MSIN taking up the rest of. The forth byte of another EF, Administrative Data (AD), gives the length of the MNC (3GPP 2006). Systems use IMSIs to recognize which arrange a gadget proprietor subscribes and, if not their system, whether to permit those system endorsers of access service.

The ICCID and IMSI can be utilized dependably to recognize the subscriber and the system administrator giving service. Since these identifiers can be misjudged, in any case, other SIM information can help affirm a finding. The Mobile Station International Subscriber Directory Number (MSISDN) is proposed to pass on the phone number allocated to the supporter for getting calls on the telephone.Dissimilar to the ICCID and IMSI, the MSISDN is a discretionary EF. In the event that present, its worth can be overhauled by the endorser, making it a less solid information source, since it would then be conflicting with the genuine number appointed. The Service Provider Name (SPN) is a discretionary EF that contains the name of the service provider.On the off chance that present, it can be redesigned just by the chairman (i.e., Administrator access). Likewise, the Service Dialing Numbers (SDN) EF contains quantities of unique administrations, for example, client consideration and, if present, can help recognize to which arrange the SIM is enrolled.

3.2 Phonebook and Call Information

The subscriber's entered list of names and phone numbers is stored in the Abbreviated Dialling Numbers (AND) EF. The capacity permits generally dialed telephone numbers to be chosen by name and overhauled or called utilizing a menu or uncommon catches on the telephone, giving simple phonebook operation. Most SIMs give around 100 openings to ADN sections. The Last Numbers Dialed (LND) EF contains a rundown of the latest telephone numbers called by the gadget. A name might likewise be connected with a passage and put away with a number (e.g., a

called phonebook section). Despite the fact that a number shows up on the rundown, an association might not have been effective, just endeavored. Most SIMs gives just a predetermined number of openings (e.g., ten) for these passages. A few telephones don't store called numbers on the SIM and rather depend all alone memory for capacity.

3.3 Messaging Information

Text informing is a method for correspondence in which messages entered on one wireless are sent to another by means of the cellular telephone system. The Short Message Service (SMS) EF contains message and related parameters for messages got from or sent to the system, or are to be conveyed as a MS began message. SMS passages contain other data other than the text itself, for example, the time an approaching message was sent, as recorded by the cellular telephone arrange, the sender's telephone number, the SMS Center location, and the status of the section. The status of a message passage can be checked as free space or as involved by one of the accompanying: a got message to be perused, a got message that has been perused, an active message to be sent, or an active message that has been sent. Messages erased by means of the telephone interface are regularly basically stamped as free space and held on the SIM until they are overwritten. At the point when another message is composed to an accessible space, the unused bit is loaded with cushioning, overwriting any remainders of a past message that may arrive.

3.4 Location Information

A GSM system comprises of unmistakable radio cells used to build up interchanges with cellular telephones. Cells are gathered together into characterized ranges used to oversee correspondences. Telephones stay informed concerning the zone under which they succumb to both voice and information correspondences. The Location Information (LOCI) EF contains the Location Area Information (LAI) for voice correspondences. The LAI is made out of the MCC and MNC of the area region and the Location Area Code (LAC), an identifier for a gathering of cells. At the point when the telephone is killed, the LAI is held, making it conceivable to focus the general region where the telephone was last working. Since an area range can contain

hundreds or more cells, the region can be very expansive. Be that as it may, it can all things considered be helpful in narrowing down the area where the occasion happened.

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

4. FORENSICS TOOLS

The fundamental goal of a legal SIM instrument is to separate computerized proof present in the document framework. Other than securing, most legal SIM instruments bolster a scope of examination and reporting capacities. A few apparatuses bargain solely with SIMs, while others are a piece of a complete toolbox that likewise addresses handsets.

The most vital feature for a legal apparatus is its capacity to keep up the uprightness of the first information source being obtained furthermore that of the removed information. The previous is finished by blocking or generally wiping out compose solicitations to the gadget containing the information. The recent is finished by ascertaining a cryptographic hash of the substance of the confirmation records made and intermittently checking that this worth stays unaltered all through the lifetime of those documents. Protecting trustworthiness not just keeps up believability from a lawful point of view, it likewise permits any consequent examination utilize the same pattern for reproducing the analysis.

A number of products are available for managing user data on a SIM. Theyallow certain data to be read onto a personal computer, updated, and rewrittenback to the SIM. Tools such as these are questionable, since they are notdesigned specifically for forensic purposes. Given the number of forensic toolsavailable, SIM management tools should be avoided.

The SIM must be expelled from the telephone and embedded into a proper reader for securing. Dissimilar to scientific obtaining of a hard commute, catching an immediate picture of the information is not a sensible alternative as a result of the security systems incorporated with the SIM. Rather, order mandates called Application Protocol Data Units (APDUs) are sent to the

SIM to concentrate information, without alteration, from pertinent EFs in the record framework (Casadei 2005). The APDU convention is a basic command reaction exchange. Every component of the document framework characterized in the standard has a remarkable numeric identifier allocated, which can be utilized to reference the component and perform some operation, for example, perusing the substance on account of a procurement device (3GPP 2005a).

Forensic SIM tools require either a specialized reader that accepts a SIMdirectly or a general-purpose reader for a full-size smart card. For the latter, astandard-size smart card adapter is needed to house the SIM for use with thereader. Table 1 lists several SIM forensic tools and which of the primaryfunctions of acquisition, examination, and reporting are supported. The firstfour listed, Cell Seizure, GSM .XRY, Mobileditand TULP2G, also handlephone memory acquisition.

4.1 Evidence Recovery

While the greater part of the put away SIM information might possibly have evidentiary worth, a great arrangement of the information is system administration related and has minimal direct evidentiary quality. By and large, SIM measurable instruments don't recuperate each conceivable thing on a SIM. The broadness of scope additionally differs significantly among devices.

4.2 Decoding and Translation

Forensic tools can present obtained information to the client in a few routes, as delineated in Figure 3. Every stride, then again, can present blunders. The most fundamental structure is the crude encoded information got in light of an APDU ask. As specified prior, content encoded in the stuffed 7-bit GSM letters in order is difficult and time intensive to disentangle physically. Another less grave deciphering included paired coded decimal (BCD) numeric identifiers. Most, however not all, instruments translate crude information into a usable structure for understanding by the client, wherever conceivable.

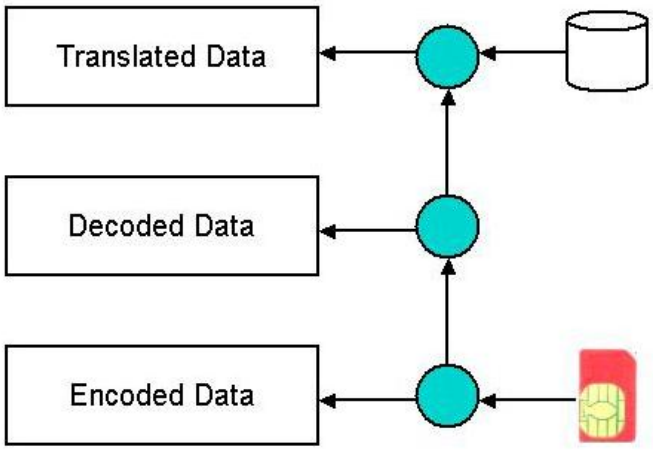

Figure 3: Data Decoding and Translation

Several tools go beyond decoding and attempt to translate the decoded datainto a form more meaningful to the user, using some database. Translation isparticularly the case with numeric data. For example, the BCD-encoded valueof 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 310is assigned to the United States, while the network code 410 is assigned toCingular.

5. CONCLUSIONS

Forensic examination of cell gadgets is a developing branch of knowledge in PC crime scene investigation. Forensic examination apparatuses make an interpretation of information to an organization and structure that is justifiable by the analyst and can be successfully used to distinguish and recoup proof. On the other hand, devices may contain some level of errors. For instance, the apparatus' usage may contain a programming slip; a determination utilized by the instrument to make an interpretation of encoded bits into information intelligible by the inspector may be mistaken or outdated; or the convention used to get the SIM may be off base, bringing on the device to work dishonourably in specific circumstances.

Over time, experience with a tool provides an understanding of its limitations,allowing an examiner to compensate where possible for any shortcomings or toturn to other means of recovery. Practice in mock examinations can help gainan in-depth understanding of a tool's

capabilities and limitations, which ofteninvolve subtle distinctions, and also provide the opportunity to customizefacilities of the tool for later use.

Forensic software tools for SIMs are in the mid-phases of development. While the instruments examined in this paper for the most part performed well and had sufficient usefulness, new forms are relied upon to enhance and better meet investigative necessities. Case in point, throughout setting up this paper, another variant for about each instrument was issued, which included usefulness improvements and sporadically a few insufficiencies. Since variability can happen between renditions of instruments, quality measures ought to be connected to guarantee that outcomes stay predictable and any varieties caught on.

REFERENCES

1. 3GPP (1999), Alphabets and Language-specific Information, 3rd Generation Partnership Project, TS 03.38, version 7.2.0 (Release 1998), Technical Specification (1999-07).
2. 3GPP (2005a), Specification of the Subscriber Identity Module – MobileEquipment (SIM - ME) interface, 3rd Generation Partnership Project,TS 11.11 V8.13.0 (Release 1999), Technical Specification, (2005-06).
3. 3GPP (2005b), Technical Realization of the Short Message Service (SMS), 3rdGeneration Partnership Project, TS 23.040 V6.6.0 (Release 6),Technical Specification (2005-12).
4. 3GPP (2006), Numbering, Addressing and Identification, 3rd GenerationPartnership Project, TS 23.003, V6.9.0 (Release 6), TechnicalSpecification (2006-03)
5. 3GPP2 (2001), Removable User Identity Module for Spread SpectrumSystems, 3rd Generation Partnership Program 2, 3GPP2 C.S0023-0,Version 4.0, June 15.
6. Ayers, R. et al. (2005), Cell Phone Forensic Tools: An Overview and Analysis, NIST Interagency Report - 7250,
7. 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.
8. Dearsley, T. (2005), Mobile Phone Forensics – Asking the Right Questions, New Law Journal, July 29, pp. 1164-1165.

9. Dechaux, C., Scheller, R. (1993), What are GSM and DECT?, Electrical Communication, 2nd Quarter, pp. 118-127.
10. 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.