Journal of Forensic Research: Open Access

Srivastava and Vatsal, J Forensic Res 2016, 7:2
http://dx.doi.org/10.4172/2157-7145.1000322

Research Article Open Access

Forensic Importance of SIM Cards as a Digital Evidence

Ankit Srivastava* and Pratik Vatsal

Institute of Forensic Science and Criminology, Bundelkhand University, Jhansi, UP, India

***Corresponding author:** Srivastava A, Institute of Forensic Science and Criminology, Bundelkhand University, Jhansi, UP-284128, India, Tel: 919415067667; E-mail: ankit_forensic81@rediffmail.com

Rec date: Dec 03, 2015; **Acc date:** Apr 29, 2016; **Pub date:** May 04, 2016

Abstract

Digital Forensics is a branch of Forensic Science pertaining to evidential articles of digital and electronic nature, of which mobile forensics is a major stream. A proliferation of handheld cellular devices and crimes involving mobile phones in the previous years has led to an enormous demand for specialists in the field of mobile forensics.

The interesting part is that any mobile phone is incomplete without a SIM card. Therefore, SIM cards are the most common type of forensic evidence to be found in cases where handheld devices are involved, a SIM card is imperative, no matter the phone belongs to the normal mobile phones category or the satellite phones that contain an iDEN (Integrated Digital Enhanced Network) SIM. These cards are all around us and are now being integrated in driving licenses, debit cards, credit cards, ATM cards, Identity cards, etc.

Digital Forensic Science is the skill of a forensic expert to apply the knowledge of computer sciences and the investigative measures for a legal cause requiring the analysis of digital evidences. It is the process of identifying, preserving, analyzing, and presenting digital evidence in a manner that is legally acceptable.

The motive of the process is to preserve any digital evidence in its most original form while performing a planned analysis by identifying, collecting and validating the digital information for the purpose of reconstructing past events.

Keywords: Digital forensic; Digital evidence; Mobile forensic; SIM cards; Digital evidence

Introduction

Digital evidence can be defined as "Information and data of value to an investigation that is stored, received or transmitted by an electronic device in binary form."

Digital Forensics comprises of several sub-divisions relating to the investigation of numerous types of media, devices or artifacts. A few of them are:

- Computer forensics
- Network forensics
- Forensic data analysis
- Database forensics
- Mobile device forensics

Computer forensics

It concerns with the present condition of a digital artifact; such as a computer system, storage medium, electronic document, etc. It is the art of obtaining, preserving and documenting evidences from electronic memory devices such as PCs, digital cameras, laptops, pen drives, CDs, DVDs and other digital storage devices [1]. It is used to investigate a wide variety of crimes, comprising of financial frauds, child pornography, espionage, cyber stalking, etc.

Network forensics

It deals with the analysis of computer network traffic, both local and WAN or internet, for evidence collection, information gathering or intrusion detection. Network Forensics is mainly concerned with the capture, recording, and analysis of network events in order to discover the source of security attacks.

Forensic data analysis

It examines structured data with the aim to discover and analyze patterns of fraudulent activities resulting from financial crime. Data forensics might focus on recovering information on the use of a mobile device, computer or other device. Data forensics investigators may also use various methodologies to pursue data forensics, such as decryption, advanced system searches, reverse engineering, or other high-level data analyses.

Database forensics

It is the forensic study of databases and their metadata. The investigations use database contents, log files and in-RAM data to build a timeline or recover relevant information. The discipline is similar to computer forensics, following normal forensic process and applying investigative techniques to database contents and metadata. Cached information may also exist in a server RAM requiring live analysis technique.

Mobile device forensics

It is a major sub-branch of digital forensics, relating to recovery of digital evidence or data from a mobile device. It differs from Computer forensics as a mobile device would have an inbuilt communication system (e.g. GSM) and, usually, proprietary storage mechanisms. Investigations usually focus on simple data such as call data and communications (SMS/E-mail) rather than in-depth recovery of deleted data. Mobile devices are also useful for providing location information; either from inbuilt GPS/location tracking or via cell site logs, which track the devices within their range.

SIM Cards

The chip that is generally referred to, as a SIM (Subscriber Identity Module) card is in fact, a UICC, i.e., Universal Integrated Circuit Card, which is a smart card that helps devices like, mobile phones, Set Top Boxes, etc., connect to its nearest cellular radio network tower for communication purposes. Instead of referring these smart cards as UICC, they are commonly referred to as SIM cards in day to day usage [2].

SIM Forensics

SIM card Forensics is an essential section of Mobile device forensics. The information that a SIM card can provide the forensic examiner can be crucial to an investigation. Obtaining a SIM card permits a plethora of information, which the suspect has dealt with over the phone to be investigated.

In general, some of this data can help an investigator determine:

- Phone numbers of calls made/received
- Contacts
- SMS details (time/date, recipient, etc.)
- SMS text (the message itself)

Service Provider Data

Some additional information the service providers might store:

- A customer database
- Call Detail Records (CDR)
- Home Location Register (HLR)

Location Area Identity

The networks for cell phone devices are distributed into Location Areas.

Each Location is identified by its unique identification number which is called Location Area Information or LAI. The LAI will be stored in the SIM card to receive service from the nearest cell phone tower. When the phone changes to a different Location Area, a new LAI in the list of the previous LAIs it has been to. In the condition when the phone powers down, after rebooting it can search the list of all the LAIs stored to find the LAIs stored to find the LAI it is in presently, to start the service again [3,4]. This saves time by avoiding searching the complete list of all the towers around.

This is a real plus point for forensic investigators because when a SIM card is reviewed, they can get a general idea of where the SIM card has been geographically. In turn this tells them where the phone has been and can then relate back to where the individual who owns the phone has been.

SIM Cards from a Technical Point of View

The card contains its own:

- Microprocessor (CPU)
- Program memory (ROM)
- Working memory (RAM)
- Data memory (EPROM or E2PROM)
- Serial communication module

Technically SIM (Subscriber Identity Module) is just one of several applications running on the smart card (the UICC). Theoretically, a single UICC can contain multiple SIMs, which allows managing multiple phone numbers or accounts to be accessed by a single UICC, but it is seldom seen in practice. Though nowadays "12 in 1" SIM card is being advertised, but is extremely rare or non-prevalent in India, at least.

The SIM card is actually a microcomputer that has its own microprocessor, input-output interface, volatile and non-volatile memory. These entire components meet together to mainly calculate the responses to the challenges presented. In the next figure we can see the functional and logical structure of a SIM card (Figure 1).

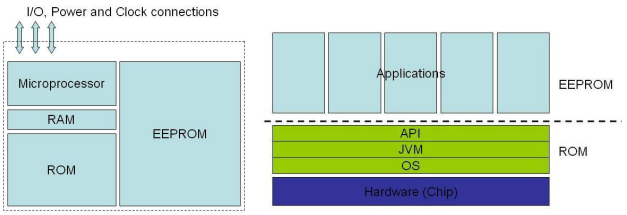

Figure 1: Functional and logical structure of a SIM card.

The way that the SIM Card interacts with the Mobile device is via a serial Input/output connection that serves as a link for the Mobile phone to handle commands to the SIM card and get a response. The most widely used protocol is T=0 that defines exactly the APDU (Application Protocol Data Unit) electrical coding for each command and the responses (Status Words) that the SIM card can return (Rankl and Effing, 2000). It must be said that at this level the SIM Card is a totally passive element, that is, it holds a slave position and cannot initiate the communication with the handset, just reply Status Words to questions (APDUs) from the handset [5].

A SIM Card has six pads that also correspond to the six SIM connector pins, but only five pins have connection on the entire layout (Figure 2).

- **SIM data** - This accesses the digital data being stored on a SIM memory.
- **SIM clock** - This is a clock frequency signal that synchronizes to the digital data to create data signal for transferring or sending and receiving data information.
- **SIM reset** - This is a frequency signal that is meant to trigger or reset all the synchronization processes.

- **VSIM B+ supply voltage** – It is a power supply voltage which is used to activate the circuit of a SIM card.
- **SIM ground** - A ground line voltage.
- The sixth one is not connected.

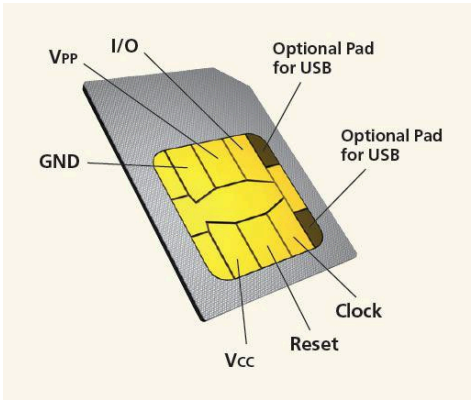

Figure 2: Layout of SIM connector pins.

The File System Organization of a SIM card

The file system of a SIM card is organized in a hierarchical tree structure, as given below:

Master File (MF) – Master file is the root of the file system organization. It contains all the dedicated and elementary files.

Dedicated File (DF) – Dedicated files are subordinate directories to the master file that contain dedicated and elementary files.

Elementary File (EF) – These are files that contain various types of formatted data structures, which can be a sequence of data bytes, a sequence of fixed size records, or a fixed set of fixed size records used cyclically (Figure 3).

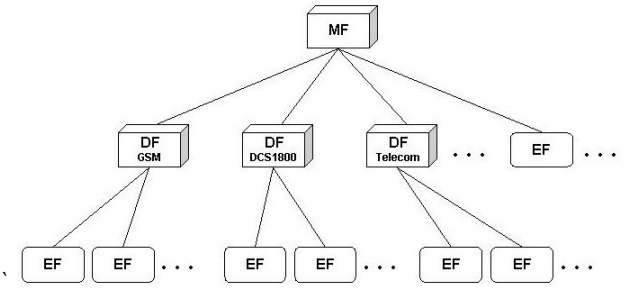

Figure 3: SIM file system.

Generally UICC cards hold only 16 to 64 KB of memory but, there has been a recent trend to produce SIM cards with much greater storage capacities, which could range from 512 MB to 1 GB memories SIM cards.

Iccid

Every SIM is identified internationally by its ICC-ID (Integrated Circuit Card ID). The ICC-IDs are stored in the SIM card and they may even be engraved or printed on the SIM card's body during a process which is called personalization. The number is generally up to 18 digits long with an addition of a single "check digit" that is used for error detection. This single digit allows us to detect mistyped digits, an input error of digits or a permutation of two successive digits. This digit is calculated with the use of the Luhn algorithm (Figure 4) [6].

Figure 4: SIM cards showing ICCID.

A typical SIM (19 digits) example 89 91 10 1200 00 320451 0, can provide us with several details in Table 1.

Digit Position	Example	Description of digit positions
First two digits	89	Major Industry Identifier
Next two digits	91	Country Code (91 is for India)
Next two digits	10	Issuer Identifier Number
Next four digits	1200	Month and Year of build
Next two digits	0	Switch Configuration Code
Next six digits	320451	SIM number
Last digit	0	Check Sum Digit

Table 1: Details of 19 digits in a typical SIM card.

These digits can be further grouped for additional information

- The Major Industry Identifier, Country Code, and Issuer Identifier Number make up the Issuer Identification Number (IIN) which is maximum upto 7 digits.
- The next several digits which may be of variable length represent the Individual Account Identification Number.
- The last digit is the checksum digit [7].

The Concept of Data Recovery from SIM Cards

SIM cards which are technically smart cards containing an embedded EEPROM memory chip. The EEPROM chip in the smart cards is the same flash memory devices that are the same flash memory devices that are present in pen drives, SSDs, etc. Hence, it is possible to recover data from other electronic memory chip devices.

But SIM cards in damaged conditions might become unrecognizable by the SIM extraction device being used. Therefore, the card should be properly cleaned before being subjected to the process of extraction. In the field of forensics, Digital Forensics laboratories may receive SIM cards in various unusual conditions, from soiled, dusty, to physically broken SIM cards. The connecting plates of the SIM cards might be rusted or soaked with blood.

Evidential Value of SIM cards

- SIM cards can contain crucial information, for example, messages having login IDs and passwords related to one's bank accounts and social networking sites.
- SIM cards may also contain personal and professional messages, important contact information, call logs, etc.
- Deleted messages can also be recovered from SIM cards.
- Data in SIM cards are not destroyed by heat, flame, dust, soil, moisture, stains or magnetic fields. Hence, environmental conditions have no effect on the data stored in SIM cards.
- Only after going through physical damage a SIM can be rendered unreadable, but scratches and striations do not make the SIM card unreadable.
- SIM cards inflicted by stone, hammer or bitten by teeth that create compression marks on the metallic circuit of the card become unreadable.
- Even SIM cards that have become unreadable can be read after replacing the EEPROM chip into a new SIM card or by connecting it to proper probes.
- People should be made aware that SIM cards should not be simply discarded without breaking it into two pieces to make it nearly impossible by a stranger or a criminal to steal private data easily, barely by using a SIM card reader.
- SIM cards are vital as forensic evidences as it contains location information and a list of all the network towers it has recently connected to. Call logs of a suspect or a criminal can be of immense value in the proceedings of an investigation.
- In cases of suicide, accidental drowning, road accidents, mass disasters where the mobile device of the unknown victim gets broken or gets switched off due to battery discharge, if the SIM card is taken out and read with a SIM card reader, we can get to know about the victim by extracting information from their SIM card.

References

1. Aritome S, Shirota R, Hemink G, Endoh T, Masuoka F (1993) "Reliability Issues of Flash Memory Cells" Institute of Electrical and Electronic Engineers 81: 4-7.
2. Gielen S, Poll E (2012) "SIM Toolkit in Practice" Norwegian University of science and technology p: 15-16.
3. Jones BJ, Kenyon AJ (2007) "Retention of data in heat-damaged SIM cards and potential recovery methods". National Institute of Standards and Technology p: 14.
4. Kamrul I (2012) "Effective use of smart cards - A case study of smart cards in Sweden" Department of informatics p: 12.
5. Thakur RS, Chourasia K, Singh B (2012) "Cellular Phone Forensics". International Journals of Scientific and Research Publications 2: 3.
6. Willassen SY (2003) "Forensics and the GSM mobile telephone system" International Journal of Digital Evidence 2: 21.
7. Jansen W and Ayers R (2007) "Forensic Software Tools for Cell Phone Subscriber Identity Modules" National Institute of Standards and Technology p: 44.