SIM Forensics: Extraction and Preparation of Digital Evidence using Sim Xtractor

C. Aanandha Subramanian, K. Suthendran, M. Satheesh Kumar

ABSTRACT-In each and every mobile phone the SIM card plays a major role in communicating the information. In a crime if a mobile phone is been taken as the evidence, the first and the foremost thing is to investigate the SIM card. Though the evolution of smart phone is very rapid without the SIM card the smart phone is uncertain in communication. The SIM card stores some valuable information like call logs, messages, contacts etc…. . For extracting those information we need a tool. In this experiment we are using a tool known as SIMXtractor from CDAC. It is not a open source tool. By using this tool we are able extract those information from the SIM card.

KEYWORDS - SIM card, SIMXtractor, SIM Analysis, Information in SIM.

I. INTRODUCTION

In the current days, smart phone are become essential part of life due to the rapid growth of technology. In recent years, smart phone has become emerging market compared to other technologies. Smart phones are uncertain in the communication without Subscriber Identity Module [SIM].The SIM card users are increased very rapidly in India.

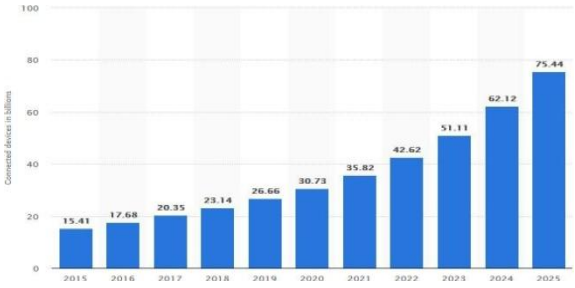

Fig1. SIM card users over years

In the recent years, smart phone are become emerging market compare to other technologies. Smart phones are uncertain the communication without Subscriber
Identity Module [SIM]. They are few possible ways that crime can emerge with smart phone along with SIM. This provides extensive information that hold for forensic analysis and investigation.

Revised Manuscript Received on December 16, 2019.

C. Aanandha Subramanian, Department Of Electronics, And Communication, National Engineering College, Kovilpatti.

Dr. K. Suthendran, Department Of Information Technology, Kalsalingam University, Srivilliputtur.

M. Satheesh Kumar, Department Of Electronics, And Communication, National Ngineering College, Kovilpatti.

- First, retrieve all information related about user. For instance, call logs, messages and other.
- Second, there are chances of evidence might be stored in device, before crime incident takes place.
- Third, any form of communication like call, message and other ways of communication. Will help to analyse the crime incident.

A SIM card, also known as a subscriber identity module, is a smart card that stores data for GSM cellular technology subscribers. Such data includes user identity, location and phone number, network authorization data, personal security keys, contact lists and stored text messages. After the invention of GSM 11.11, telecom industry has drastically developed in a period of time. It is initialized to divide the Mobile station into "Subscriber Module Identity [SIM] and Mobile equipment".[1]

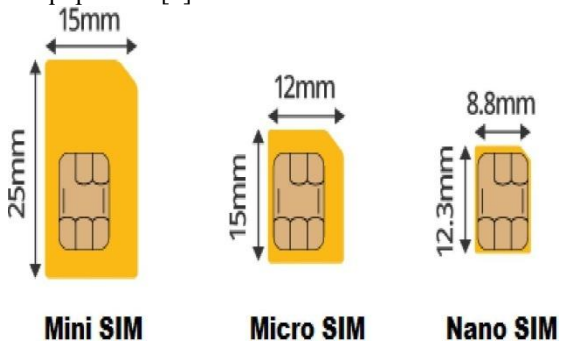

Fig2. Types of SIM cards

II. BACKGROUND INFORMATION

SIM card File system consists of three types of files namely
-Master File
-Elementary File
-Dedicated File

ICCID: ICCID is known as "*Integrated circuit card identifier"*, which contains the 20-digits unique identification number. They are categorized into two types respectively

- Account Identification Number [IIN]
- Issuer Identification Number [IIN]

The EF file containing the address of the ICCID is 0x2FE2. [2]

IMSI: It is known as "*International mobile subscriber identity"*, is a unique number associated with all Global System for Mobile Communications (GSM) and Universal Mobile Telecommunications System (UMTS) network mobile phone users used for identifying a GSM subscriber. IMSI size is 15 digits and the EF file containing the address of the IMSI number is 0x6F07.[3]

MSISDN: Mobile Switching Centre and central part of telecom system on network layer. The MSC Server is standards-based and communicates with other distributed elements using industry open standards such as media gateway control protocol. In mobile communications, switch is mechanism which established wireless communication channel, between two involved parties.[4]

SPN and SDN: SPN is referred as "Service Provider Name" and "Service Dailing Number", which is element file that elaborates GSM network service provider and special services provided by company.

TMSI: It abbreviates as "*Temporary Mobile Subscriber Identity",* as name it suggest is exchanged between the mobile phone and local network. For instance, if subscriber moves from one area to another area, it avoids the signal fading and also identifies the subscriber.[5]

ADN: It is abbreviated Dialing Number, in a simple word, the contacts number saved by subscriber.

LND: It is abbreviated as Last Number Dialed, Which records last phone number the user is been dialed.

SMS: It is "Short Message Service", which allows the subscriber to communicate them with a short message. That sent and received through the mobile network. SMS is actually considered of the valuable assets for forensic investigation purpose. Because sent, received and deleted messages are very crucial for digital forensic investigation.

PUBLIC LAND MOBILE NETWORK (PLMN): Any wireless communications system intended for use by terrestrial subscribers in vehicles or on foot [6]. Such a system can stand alone, but often it is interconnected with a fixed system such as the public switched telephone network (PSTN).It identified by Mobile Country Code (MCC) and Mobile Network Code (MNC).

III. METHODOLOGY

SIMXTRACTOR TOOL:

From Center for Development of Advanced Computing(CDAC) a tool called SIMXtractor was developed to extract the information from the SIM cards. It is not a open source tool[7] . This tool consists of three products

1) SIM card Reader
2) SIM Imager
3) SIM Analyser

SIM Card Reader:
It is a product that is used to connect the SIM card to the device that we are using for investigation purpose. It is a hardware based reader with a USB support.

SIM Imager:
It is a tool that is used to make an image of the SIM card for further investigation purposes. This tool supports MD5, SHA 1, SHA 2 hashing algorithms.

SIM Analyser:
This tool is used for analysing the image that is been imaged by the SIM imager .It analyze and says as the information of the SIM card like messages ,call logs contacts and network related information.

Experiments:

In this paper we experimented three kinds of SIM cards like

1) Normal SIM
2) Pin Protected SIM
3) Blocked SIM

We compared the information acquired by these types of SIM cards using SIM Xtractor and analyzed it.

Normal SIM:

In Normal SIM this tool extracted all the information from user like contacts, messages, information about the location ,IMSI,KC, SPN, ICCID are extracted.

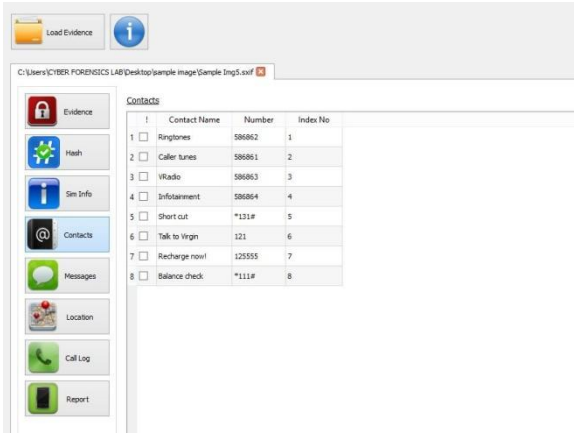

Fig 3. Contacts from a Normal SIM

Pin Protected SIM:
In this pin protected SIM we can extract the information only if we know the pin. We can also extract the information if we do not know the pin but some information might not be retrieved like the location, call logs, contacts, IMSI number, KC(ciphering key). Only the basic information like SPN,ICCID, service type only will be extracted.

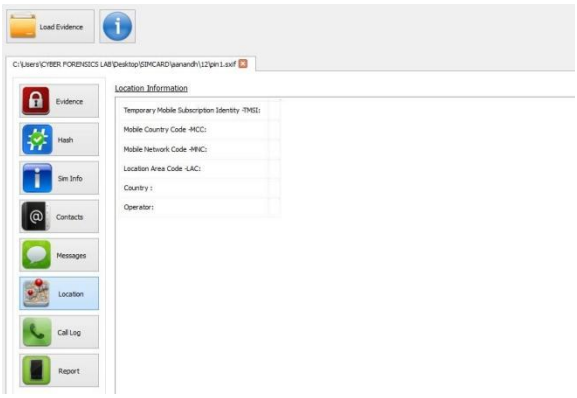

Fig 4. Information about the location of a pin protected SIM.

A Maximum of 10 number attempts can be made to identify the PIN. More than 10 attempts will lead to blockage of SIM.

3.3.3 Blocked SIM:

In this case we could not know the information about the location, call logs, messages. But the basic information like ICCID, IMSI, KC, SPN, Service type, Contacts will be extracted. But there is no use of those information extracted because the information that we extracted from the blocked cant be used for investigation purpose.

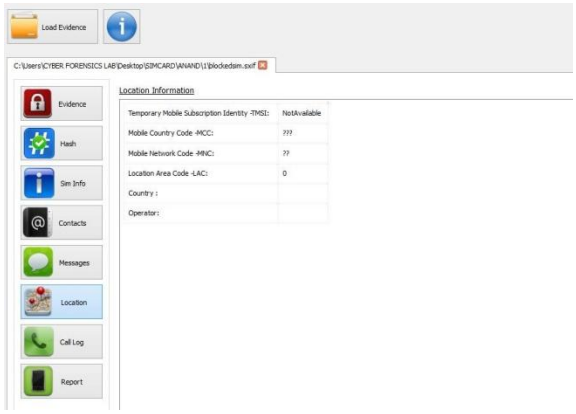

Fig 5. Information about the location of a blocked SIM.

In all the three cases SIM card we extracted different information from the SIM card we listed that in a table below.

[4] http://www.ing.unibs.it/~antonio.savoldi

[5] SIM and USIM Filesystem: a Forensics Perspective Antonio Savoldi and Paolo Gubia,University of Brescia .

S.No	SIM card information	NORMAL SIM	PROTECTED SIM	BLOCKED SIM
1	ICCID	F	F	F
2	SPN	F	F	F
3	MCC	F	N	N
4	MNC	F	N	N
5	MSISDN	F	N	N
6	IMSI	F	F	F
7	LDN	F	N	N
8	ADN	F	N	N
9	FDN	F	N	N
10	SMS	F	N	N
11	CALL LOGS	P	N	N
12	CONTACTS	F	N	F
13	MESSAGES (Deleted)	F	N	N

F-FULLY ACQUIRED
P-PARTIALLY ACQUIRED
N-NO INFORMATION ACQUIRED

IV. CONCLUSION

In this paper, SIM cards and the communication methods that would enable forensic data extraction from the SIM card were explained. The research demonstrated how a forensic analyst can extract vital forensic artifacts from a SIM card, such as: SMS, contacts, call logs, location information. The main contribution of the project is to test the capability of each SIMXtractor tool related to SIM card forensics, with different cases of SIM cards.

REFERENCES

1. Digital Forensic Analysis of SIM Cards Mohamed T. Abdelazim, Nashwa AbdelBaki, Ahmed F. Shosha Information Security Department, CIT School, Nile University, Cairo, Egypt
2. https://www.cdac.in/index.aspx?id=cs_cf_CSG_SI MCARD
3. http://commons.erau.edu/adfsl
4. Forensics and Sim cards: An overview Fabio Casadei ,Antonio Savoldi,Paolo Gubian,University of Brescia
5. Forensic Importance of SIM Cards as a Digital Evidence by Ankit Srivastava* and Pratik Vatsal Institute of Forensic Science and Criminology, Bundelkhand University, Jhansi, UP, India