

# Cellular Phone Forensics

Roshan Singh Thakur<sup>1</sup>, Khyati Chourasia<sup>2</sup>, Bhupendra Singh<sup>3</sup>

<sup>1</sup>Student, Mtech (Computer Science & Engineering), CSE Department, Abha College of Engineering & Technology, Nagpur (M.S)

<sup>2</sup>Student, Mtech (Digital communication), Electronics & Comm.dept, Bansal Institute of Science and Technology Bhopal (M.P)

<sup>3</sup>Student, Mtech (Computer Science & Engineering), CSE Department, Shri Ram College of Engineering & Technology, Jabalpur (M.P)

**Abstract-** As mobile devices grow in popularity and ubiquity in everyday life, they are often involved in digital crimes and digital investigation as well. Cell phones, for instance, are becoming a media or tool in criminal cases and corporate investigation. Cellular phone forensics is therefore important for law enforcement and private investigators. Cell phone forensics aims at acquiring and analyzing data in the cellular phone, which is similar to computer forensics. However, the forensic tools for cell phones are quite different from those for personal computers. This paper briefly explains the basics of the GSM system. Evidence items that can be obtained from the Mobile Equipment, the SIM and the core network are explored. Tools to extract such evidence from the components of the system exist, but there is a need to develop more sound forensic procedures and tools for extracting such evidence.

**Index Terms-** cellular phone, GSM system, mobile equipment (ME), SIM card, digital forensic, UMTS.

## I. INTRODUCTION

As cell phone use becomes more widespread, cell phone forensics becomes more and more important as cell phones are often found in crime scenes. Forensics is used in all types of situations from internally in a corporate auditing case to a criminal investigation case commonly seen in the law enforcement world. Many crimes and other misconducts make forensics very important as a means of making the world a better place. Digital forensics is becoming important because our society is becoming more dependent of various computers and telecommunication tools and technologies. Cell phone forensics, being part of digital forensics, aims at the retrieval or gathering of data and evidence from mobile phones and similar devices used in daily life. Cell phone forensics allows investigators to answer questions of interest on a certain subject related to cell phone based communication. It is based on proven scientific methodology and norms to collect facts regarding an object, an event, or an artifact in certain time period to determine whether the object was in fact what it claims to be or is alleged as being. In these efforts of forensics, cell phone forensic specialists have encountered major challenges that hinder their work. As we know mobile devices are becoming the main mobile computing power with all its constant upgrades, changed, and new additions, this has caused the forensic specialists to undergo a lack in available

Forensic tools for retrieval that is compatible with today's uprising of newer model devices. The main difference between cell phone forensics and computer forensics is that in cell phone forensics, one has to deal with multiple different hardware and

software standards, which makes creating a universal standard tool near to impossible. Since the software is embedded and more special purpose than computers, solutions for obtaining data are non-standardized thus causing a need for vast solutions. With the advent of new phones coming into the market at an exponential rate, as well as new companies coming into the market using a whole different blend of proprietary software, the problem has been even more compounded as time progresses. The purpose of a cell phone forensic tool is to obtain data from a cell phone without modifying the data. The tool should provide critical updates in time to keep pace of the rapid changes of cell phone hardware and software. The tools can be either forensic or non-forensic, which each of them providing different challenges as well as allowing for different solutions. Forensic tools are tools that are designed primarily for uncovering data from cell phones, while non-forensic tools are not designed for uncovering data but can be manipulated for that purpose. Two different methodologies have been used to address this situation, either reduce the latency period between the introduction of the phone and the time the cell phone forensic software is available for that phone or create a baseline to determine the effectiveness of a tool on a certain device. The first method is to reduce the latency period between the time a cell phone gets on the market and the availability of the tools and this is primarily done by adding a new layer called a phone manager protocol filtering, which sits at a higher abstraction level between the programming interface and the library, thus in a way achieving a kind of program data independence. The value of this method is increased by the fact that most phone managers use the Windows operating system. The main approach for this method is to obtain a phone manager and modify it so dangerous "write" commands cannot be issued, i.e. forensic scientists will not accidentally write data onto a suspect phone and thus compromise or jeopardize a case. This modification to the phone manager is done by a program called a filter. This filter will not only block dangerous write commands, but also will intercept data from the target phone in binary form and then send it to the phone manager for further decoding.

The second method is to provide a baseline or test data to evaluate forensic tools. With this method, the user populates the phone with certain data and then attempts to retrieve it with a forensic tool. Thus the baseline is the original data that is populated on the telephone. The baseline is usually set up by Identity Module Programming (IMP). The data that is obtained by the forensic tool from the cell phone is tested against the baseline and therefore one can determine what the effectiveness of the cell phone forensic tool is. The major identity module that is used today is called the Subscriber Identity Module or SIM card which is used to separate the personal information from the actual mobile device as well as hold onto phone numbers, names

and network settings and allows for the portability between phones. The SIM card is broken up into a file system organization with root directory file subdivided into multiple directory files (DF) that contain the elementary files (EF) which holds the binary data. Thus creates another problem as the data that needs to be obtained could be contained anywhere in the elementary files. In order to insert the test data onto the SIM card an IMP (Identity Module Programmer) needs to be inserted and then it will be allowed to write test EF.

## II. OVERVIEW OF THE GSM SYSTEM

The GSM system is specified in 12 series of specifications. For phase 1, these specifications constitute over 4000 pages. In the following, a short overview of the system will be given

### Entities of the GSM system

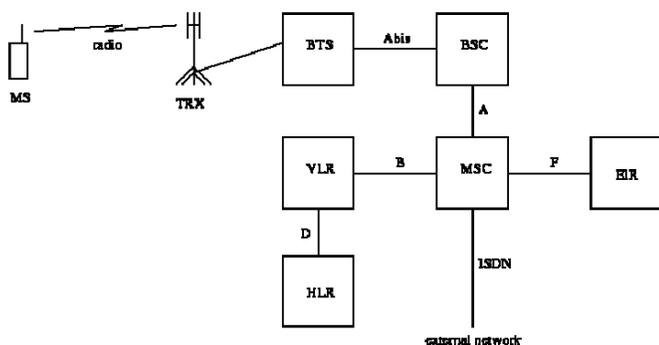


Fig 1 – Entities in the GSM system

The GSM system consists of a number of separate entities [GSM0302]. These are shown in figure 1. The entities are connected through interfaces with their own names according to the specifications; these names are shown on the figure.

### The Mobile Station:

The Mobile Station (MS) is the user equipment in GSM. The MS is what the user can see of the GSM system. The station consists of two entities, the Mobile Equipment (the phone itself), and the Subscriber Identity Module (SIM), in form of a smart card contained inside the phone.

### The Base Transceiver Station:

The Base Transceiver Station (BTS) is the entity corresponding to one site communicating with the Mobile Stations. Usually, the BTS will have an antenna with several TRXs (radio transceivers) that each communicate on one radio frequency. The link-level signaling on the radio-channels is interpreted in the BTS, whereas most of the higher-level signaling is forwarded to the BSC and MSC. Speech and data-transmissions from the MS is re-coded in the BTS from the special encoding used on the radio interface to the standard 64 Kbit/s encoding used in telecommunication networks. Like the radio-interface, the interface between the BTS and the BSC is highly standardized, allowing BTSs and BSCs from different manufacturers in one network.

### The Base Station Controller:

Each Base Station Controller (BSC) controls the magnitude of several hundred BTS's. The BSC takes care of a number of different procedures regarding call setup, location update and handover for each MS.

### The Mobile Switching Centre:

The Mobile Switching Centre is a normal ISDN-switch with extended functionality to handle mobile subscribers. The basic function of the MSC is to switch speech and data connections between BSCs, other MSCs, other GSM-networks and external non-mobile-networks. The MSC also handles a number of functions associated with mobile subscribers, among others registration, location updating and handover. There will normally exist only a few BSCs per MSC, due to the large number of BTSs connected to the BSC. The MSC and BSCs are connected via the highly standardized A-interface [GSM0808]. However, due to the lack of standardization on Operation and Management protocols, network providers usually choose BSCs, MSCs and Location Registers from one manufacturer.

### The Location Registers:

With each MSC, there is associated a Visitors Location Register (VLR). The VLR can be associated with one or several MSCs. The VLR stores data about all customers who are roaming within the location area of that MSC. This data is updated with the location update procedure initiated from the MS through the MSC, or directly from the subscriber Home Location Register (HLR). The HLR is the home register of the subscriber. Subscription information, allowed services, authentication information and localization of the subscriber are at all times stored in the HLR. This information may be obtained by the VLR/MSC when necessary. When the subscriber roams into the location area of another VLR/MSC, the HLR is updated. At mobile terminated calls, the HLR is interrogated to find which MSC the MS is registered with. Because the HLR is a centralized database that need to be accessed during every call setup and data transmission in the GSM network, this entity need to have a very large data transmission capacity.

### The Equipment Identity Register:

The Equipment Identity Register (EIR) is an optional register. Its purpose is to register IMEIs of mobile stations in use. By implementing the EIR the network provider can blacklist stolen or malfunctioning MS, so that their use is not allowed by the network.

## III. EVIDENCE IN THE SUBSCRIBER IDENTITY MODULE

The SIM contains information that can be of value as evidence. First, the SIM itself can have value as evidence. As shown on the picture, the name of the network-provider is usually printed on the SIM, along with a unique identification number that can be used to get information from the provider, such as the subscriber name and address and phone number associated with the SIM. Phone records can also be retrieved from this number as discussed below.

### Access to the SIM:

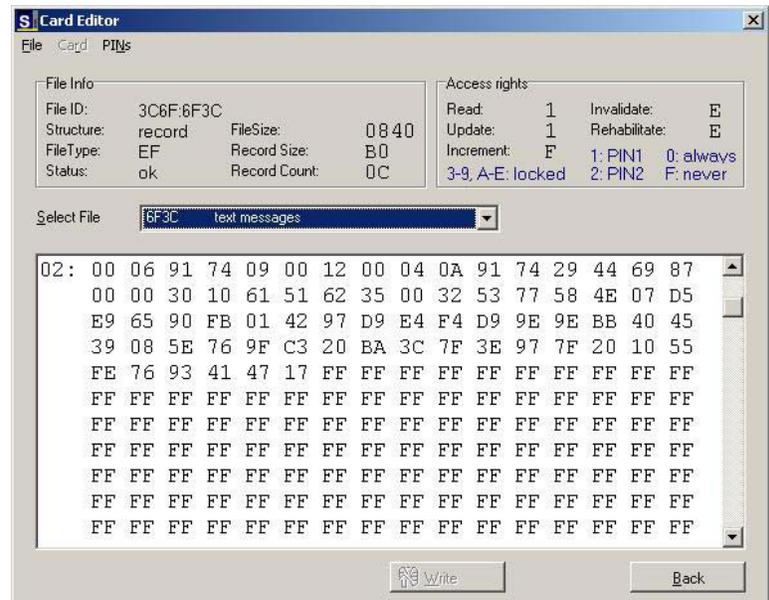
A PIN-code (Personal Identification Number) is usually required to access the SIM. This number is a four-digit code that must be entered to gain access. Since the phone cannot be used without access to the SIM, this number must be entered whenever the phone is turned on. If the user fails to enter a valid PIN through three attempts, the card becomes blocked, and the user must instead enter a 8-digit code called PUK to reopen it. If the user fails to enter the correct PUK during ten attempts, the card becomes permanently blocked and cannot be reopened. PIN-codes for a card can be changed and deactivated by the user. The PUK-codes are fixed and cannot be changed. Since the PUK-code is fixed, the network operator usually keeps track of the PUK-codes for all its users. Therefore, the investigator can almost always gain access to a SIM-card by asking the network operator for the PUK code. It might, however, be more efficient to ask the owner of the phone to provide correct PIN or PUK-codes. During searches, the PUK code might also be recovered, since phone owners usually keep the PUK code in writing in case they forget the PIN.

**Forensic analysis of SIM cards:**

The SIM card is a smart card, containing a processor and non-volatile memory. In GSM, the SIM card is used as a storage device for subscriber related data. The only purpose of the processor is to implement the access mechanism and security features. The physical and logical properties of the access mechanism are defined in GSM specifications. [GSM1111]

The SIM card can be accessed by mounting the card in a standard smart-card reader. To access the card logically software is needed that implement the GSM SIM access mechanism. The contents of the SIM card is organized as a series of files containing binary data that can be downloaded once the user has authenticated himself with a PIN or PUK code.

The best forensic procedure would be to image the entire contents by downloading the entire memory of the SIM and compute a hash value of this memory. There is currently no tool available to do this. There are however tools available to download binary contents of individual files and store them as individual files. Examples of such tools are Sim Manager Pro (previously Sim-Surf Profi) [SIMMAN], ChipIt [CHIPIT], PDU Spy [PDUSPY] and SIM-Scan [SIMSCAN]. There are also available administrative tools, which will synchronize data such as text messages between a SIM card and a computer. Such tools should be avoided in forensic analysis, since the contents of the card will be contaminated. The currently most popular tools in law enforcement communities is the tool Cards4Labs [C4L], developed by Netherlands Forensic Institute, available to law enforcement only. This tool does not store a digital copy of the SIM-files on the computer, but rather produces a text report on most of the content on the SIM card.



**Attacks on the SIM module:**

It is important for the investigator to understand that the Subscriber Identity Module can be attacked by crafty criminals. In a forensic context, the most obvious attack method is removal of evidence. Since the files on the GSM card can be accessed in raw, an attacker can remove evidence by overwriting storage space. For instance, a person knowing that deleted text messages are still accessible on the card, could use the card editor in Sim-Surf Profi to overwrite the messages with other information.

Of more interest to a criminal would be to attack the SIM to impersonate another subscriber. If this could be done, a criminal would be able to make calls on other subscriber's accounts, and impersonate other subscribers, as their caller identification would show up at the called party. In the GSM system, the subscriber identity is only stored on the SIM, so the protection against impersonation only rely on the SIM security features. The only information that identifies a user is the user IMSI and the secret encryption key Ki. Both are stored on the SIM and in the HLR in the network. As we have seen, the IMSI can be read directly from the SIM card if the user knows the PIN or PUK code. IMSI of other valid subscribers could also be obtained by listening to unencrypted network traffic on the air interface, since the IMSI will be transferred unencrypted across the air interface whenever a mobile registers with a new network. (This happens a lot at certain locations, such as international airports.)

But how can the criminal obtain the encryption key Ki? Since the Ki is stored only internally in the SIM card it is not accessible directly, but only through usage of the encryption algorithms stored on the card. However, since the user of a SIM card can feed the algorithm with known numbers, the Ki can be found if the algorithms contain weaknesses that allow such analysis. Such an attack is commonly known as a chosen-plaintext attack. The algorithms in GSM do indeed have such a weakness. A tool to extract Ki from a SIM has been implemented in the program Sim-Scan, available on the Internet [SIMSCAN]. Both IMSI and Ki can therefore be obtained by anyone with access to a SIM-card and knowledge of PIN or PUK.

The next step for the criminal is to produce a new SIM-card with the IMSI and Ki implemented. This cannot be done on SIM-cards in use, since IMSI is locked through the SIM access mechanism, and Ki is only internally stored. The attacker therefore needs to get hold of a fresh card without any subscriber information. These cards can be ordered from the same source where network providers get their cards. The card must then be programmed with a special tool for programming of fresh cards. Such a tool is distributed together with the Sim-Scan package. An attacker could also get hold of a generic smart card and smart card programmer, and then program the card to act as a SIM.

The conclusion is that impersonation of other GSM subscribers is indeed possible for anyone who can get hold of a subscriber card and corresponding PIN/PUK.

#### IV. EVIDENCE IN THE MOBILE EQUIPMENT

Specifications specify many functional requirements to the Mobile Equipment in the GSM system when it comes to the interface with the network and the SIM. As long as these requirements are met, it's up to the manufacturer to decide which other functions to implement on the ME, such as storage of different types of information. It therefore exist a long range of different phones on the market, each with it's own capabilities of information storage and each with its own potential as digital evidence. A study of all GSM mobile phones in a forensic context is therefore infeasible. This paper will focus on general principles and information that is commonly stored on different types of equipment.

##### ***Access to the phone:***

Since access to the SIM is needed to use the phone, all phones ask for the SIM PIN code when the phone is turned on, unless the PIN has been deactivated. Many phones also have the ability to ask for a separate access code for access to the phone memory. This feature is rarely used, since the user then will have to enter two access codes whenever the phone is turned on. In principle, the investigator will not have any means to get hold of the phone access code if it is activated. It is believed however, that most phones have an ability to circumvent the code by using special hardware/cables and software to access the contents of the phone.

##### ***Forensic analysis of GSM phones:***

Most, if not all, mobile phones implement information storage by means of one or several on-board flash memory chip(s). This memory contains all information stored on the phone as well as phone-internal software. The most forensically sound procedure for analysis of phones would therefore be to find a way to digitally image the contents of the phone memory chips, and analyze the contents off-line. Since most phones provides a way for the manufacturer to access the contents and upgrading the software, this procedure can actually be done for most phones. The procedure would however require knowledge of the programming interface of the phone, information that manufacturers usually keep for themselves. Tools for accessing the phone memory directly (called "flashers") are available on the Internet for many phones. (Phones from Nokia, Ericsson, Siemens and Motorola amongst others) These flashers seem to be

unauthorized by the phone manufacturers. Using such tools for forensic imaging would therefore in the author's opinion seem questionable, but might be the only way to retrieve information that could have relevance as evidence.

Most phones can be connected to a computer for data transfer. Connection can be done by means of a special cable from the manufacturer, or by using wireless interfaces such as IrDA or Bluetooth. The information on the phone can then be accessed by using special software from the manufacturer. Such software will commonly let the user download information contained within the phone, such as text messages, short numbers, dialed numbers, received calls, and configuration parameters. The contents of the memory will not be directly accessible using such tools.

A third method of forensic analysis of a mobile phone is simply to use the keypad of the phone to access the stored information, and photograph it as it comes on screen. Most information stored on the phones can be accessed using the phone menu system. The IMEI is on most phones available by typing \*#06#. As this method is cumbersome and the analyst risks to change the information on the phone, it should be avoided if possible.

The author has observed that some phones tie information stored on the phone to the subscriber identity on the SIM-card. This is probably meant as a security feature to prevent access to sensitive information by unauthorized users. As an example, Nokia phones store logs of outgoing and incoming calls in the phone. If a user removes the SIM card and insert another card, these logs will be cleared. Investigators should therefore be cautious with removing the card from the phone before relevant information has been secured.

##### ***Phone contents***

The following contents of modern mobile phones can have value as evidence:

- IMEI
- Short Dial Numbers
- Text Messages
- Settings (language, date/time, tone/volume etc)
- Stored Audio Recordings
- Stored Computer Files
- Logged incoming calls and dialed numbers
- Stored Executable Programs
- Stored Calendar Events
- GPRS, WAP and Internet settings

Most of this information is available through cable and manufacturer specific software. However, direct analysis of the memory could potentially reveal other hidden information, such as deleted text messages. Such analysis has to the authors knowledge not yet been performed.

##### ***Attacks on the phone:***

The before mentioned tools for direct access to the phone memory, so called flashers, also allow anyone to freely modify the contents of the phone, including phone software. Such modification is usually done to remove access constraints in the phone. The most common access constraint one would want to remove is a Service Provider lock (commonly called SP-lock). A SP-locked phone is locked to SIM cards from a certain service

provider. Such locked phones are often sold together with cheap subscriptions or prepaid subscriptions, to lock the customer to a certain service provider.

Another change one would want to do is to change the IMEI code of a phone. This is necessary to use stolen phones, since stolen phone IMEIs will be blacklisted in the EIR. The ability to change IMEI could also make it more difficult to trace the usage of specific phones. It is therefore desirable to find a way to detect that the IMEI of a phone has been changed. The obvious method to do this is to compare the internally stored IMEI with the IMEI printed on the phone (commonly located under the battery). To detect changes of IMEI and other changes to a mobile phone it could be useful to find a way to detect electronically if a phone has been "flashed". This could be an area of further research within mobile phone forensics.

## V. SUBSCRIBER DATABASE

The network provider maintains its own subscriber database. The database usually contains the following information about each customer:

- Customer name and address
- Billing name and address (if other than customer)
- User name and address (if other than customer)
- Billing account details
- Telephone Number (MSISDN)
- IMSI
- SIM serial number (as printed on the SIM-card)
- PIN/PUK for the SIM
- Services allowed

Some providers allow prepaid subscriptions, where the customers are not identified by name. Such subscriptions cannot be tied to a person unless a SIM card with the subscription was seized from a specific person. Given the SIM-card number, the network operator can always identify the associated IMSI and MSISDN, and then provide access codes and call details for that card.

### **Call Data Records:**

Call Data Records (CDRs) are produced every time a user makes a call or send a text message. The CDRs are produced in the switch (MSC) where the call or message originates. CDRs are then gathered in a centralized database and used for billing and other purposes.

Each CDR contains the following:

- Originating MSISDN (A-Number)
- Terminating MSISDN (B-Number)
- Originating and terminating IMEI
- Length
- Type of Service
- Initial serving Base Station (BTS) (not subsequent BTSs after handover)

CDRs can be filtered on any of the above parameters. This means that one can not only obtain a list of all calls made to/from a certain SIM, but also to/from a certain phone, regardless of which SIM was used. By looking at the serving BTS, the location of the subscriber can be pinpointed to the accuracy of a cell at

any time the subscribers sends or receives a call or a text message. Such information certainly has great evidentiary value.

## VI. CONCLUSION

Since GSM is the world's largest system for mobile communication today and also lay the foundation for the future UMTS, it is important to recognize the need to study the methods and tools for forensic analysis of the GSM system. Where current investigation is done with tools not specifically designed for forensics (except Cards4Labs), the future will hopefully see tools that let an investigator image and analyze contents of phones and SIM-cards in a forensically sound way. Further research is also needed into analysis of information stored on phones and SIM-cards.

It is clear that the GSM system contains large amounts of information valuable to the investigator. Most of the information is available today and can be retrieved and have a great potential to be used as evidence.

## REFERENCES

- [1] Jansen et. Al., Overcoming Impediments to Cell Phone Forensics.
- [2] Jansen W. and Delaitre A., Reference Material for Assessing Forensic SIM Tools.
- [3] Jansen W. and Ayers R., Guidelines on Cell Phone Forensics, NIST Special Publication 800-
- [4] 101, May 2007.
- [5] [MOULY92] Mouly, M. "The GSM System for Mobile Communications" Palasieu, France, 1992.
- [6] [GSM0302] Network Architecture, ETS 300 522 (GSM 03.02), ETSI recommendation, 1996
- [7] [GSM1110] Mobile Station (MS) conformance specification, ETS 300 607-1 (GSM 11.10), ETSI recommendation, 1997
- [8] [GSM0808] BSS-MSC layer 3 specification, ETS 300 590 (GSM 08.08), ETSI recommendation, 1996.
- [9] [GSM1111] Specification of the SIM – ME interface, ETS TS GSM 11.11, ETSI recommendation, 1996
- [10] [CHIPIT] Chip-It, Software package, Freeware [http://mobileoffice.co.za/download\\_chipit\\_sim\\_editor.htm](http://mobileoffice.co.za/download_chipit_sim_editor.htm)
- [11] [PDUSPY] PDU-Spy, Software package, Freeware <http://www.nobbi.com/download.htm>
- [12] [SIMSCAN] Sim-Scan, Software package, Freeware <http://users.net.yu/~dejan/>
- [13] [C4L] Cards4Labs, Software package, Law Enforcement only <http://www.forensischinstituut.nl/>
- [14] [WIL98] Willassen S., "Mobile Station Location in GSM", 1998. <http://www.willassen.no/msl/>
- [15] [KAR01] Kaaranen H. et al, "UMTS Networks" Helsinki, Finland, 2001.
- [16] [GSM0340] Technical realization of the Short Message Service (SMS), ETS TS GSM 03.40, ETSI recommendation, 1996
- [17] [SIMMAN] Sim-Manager Pro, Software package, Commercial <http://www.txsystems.com/>

## AUTHORS

**First Author** –Roshan Singh Thakur, Student, Mtech (Computer Science & Engineering), CSE Department Abha College of Engineering & Technology, Nagpur (M.S), Email: - roshanthakur11@gmail.com, Mob: +919552002195

**Second Author** – Khyati Chourasia , Student, Mtech (Digital communication), Electronics & Comm.dept, Bansal Institute of Science and Technology Bhopal (M.P), Email:- khyati.chourasia@gmail.com,Mob:09730960500

**Third Author** – Bhupendra Singh Thakur, Student, Mtech (Computer Science & Engineering), CSE Department, Shri Ram College of Engineering & Technology, Jabalpur (M.P), Email: - bhuppi87thakur87@gmail.com, Mob: 09630212133