Use of Forensic Software Tools to Acquire Evidence from Mobile Devices

GRADUATE PROJECT

Submitted to the Faculty of
the Department of Computing Sciences
Texas A&M University – Corpus Christi
Corpus Christi, Texas

In Partial Fulfillment of the Requirements for the Degree of
Master of Science in Computer Science

by

Eduardo Arce
Fall 2008

Committee Members

Dr. Mario Garcia
Committee Chairperson

Dr. Dulal Kar
Committee Member

Dr. David Thomas
Committee Member
Use of Forensic Software Tools to Acquire Evidence from Mobile Devices

GRADUATE PROJECT

Submitted to the Faculty of
the Department of Computing Sciences
Texas A&M University – Corpus Christi
Corpus Christi, Texas

In Partial Fulfillment of the Requirements for the Degree of
Master of Science in Computer Science

by

Eduardo Arce
Fall 2008

Committee Members

Dr. Mario Garcia
Committee Chairperson

Dr. Dulal Kar
Committee Member

Dr. David Thomas
Committee Member
ABSTRACT

Mobile phone technology is evolving rapidly. Increasing connectivity, higher storage capacities, and more processing power are just some of the areas in which mobile phones have endured drastic improvements. The problem is that together with the growth of technology, new problems related to security appear. More mobile phones have become target of criminal attacks or become a tool used to perpetrate attacks. Another problem is that forensic techniques related to mobile phones are evolving slower than technology. This is in part because of the lack of methodologies and standards available for conducting a mobile phone forensic investigation.

The purpose of this graduate project is to perform an in-depth research of the software tools available in the market for conducting a mobile phone forensic investigation. After identifying the different options, a set of these tools were selected as the target tools of the project. These tools were thoroughly compared, examined and tested in order to identify the best options for specific situations. To accomplish this, a set of predefined scenarios was created and tested on several mobile phones using the different software tools previously selected. Finally, the results of the investigation were reported and explained in order to determine the capabilities and limitation of each forensic tool.
# TABLE OF CONTENTS

Abstract .............................................................................................................................. II

Table of Contents .............................................................................................................. III

List of Figures ................................................................................................................ VIII

List of Tables .................................................................................................................... X

1. Introduction and Background ................................................................................... 1
   1.1. Wireless Generations ........................................................................................... 2
       1.1.1. First Generation (1G) ............................................................................. 2
       1.1.2. Second Generation (2G) .......................................................................... 3
       1.1.3. Third Generation (3G) ............................................................................ 6
       1.1.4. Fourth Generation (4G) .......................................................................... 7
   1.2. Mobile Phone Characteristics ........................................................................... 8
   1.3. SIM Card Characteristics ................................................................................. 10
   1.4. Digital Forensics vs. Handheld Forensics ......................................................... 13
       1.4.1. File System ............................................................................................ 14
       1.4.2. Static/Active Device .............................................................................. 14
       1.4.3. Storage Capacity ................................................................................... 14
       1.4.4. Forensic Imaging ................................................................................... 15
   1.5. Legal Considerations ....................................................................................... 16
       1.5.1. Wiretap Act (Title I) ............................................................................. 16
       1.5.2. Stored Communication Act (Title II) ...................................................... 16
2. Use of Forensic Software Tools to Acquire Evidence from Mobile Devices

2.1. Evidence Sources

2.1.1. Data Stored in the Phone Memory

2.1.2. Data Stored in the SIM Card

2.1.3. Data Stored in the Phone’s Removable Card (Flash Memory)

2.1.4. Data Stored in the Service Provider

2.2. Procedural Models for Mobile Phone Forensics

2.3. Rules when Dealing with Handheld Devices

2.3.1. Rule 1: Stop Wireless Receiving

2.3.2. Rule 2: Charge Device

2.3.3. Rule 3: Cabling and Accessories

2.3.4. Rule 4: Acquire in Laboratory

2.4. Forensic Tools

2.4.1. SIM Tools

2.4.2. Handset Tools

2.4.3. Integrated Tools

2.5. Scenarios

2.5.1. Connectivity

2.5.2. Call Logs

2.5.3. SMS/MMS

2.5.4. Phonebook

2.5.5. Calendar

2.5.6. Graphics
2.5.7. Video ............................................................................................................. 40
2.5.8. Sounds ........................................................................................................... 41
2.5.9. Acquisition Consistency ................................................................................. 41
2.5.10. Internet Messaging (only available for some devices) .............................. 41
2.5.11. Text Files (only available for some devices) ............................................ 42
2.5.12. Web Content (only available for some devices) ....................................... 42
2.5.13. Memory Cards (only available for some devices) .................................... 42

3. Research .................................................................................................................... 43

3.1. Target Devices ................................................................................................... 43
3.2. Forensic Software .............................................................................................. 43
3.2.1. Paraben’s Device Seizure .............................................................................. 43
3.2.2. Mobiledit! ...................................................................................................... 44
3.2.3. BitPim ............................................................................................................ 45
3.3. Acquisition using Paraben’s Device Seizure .................................................... 46
3.3.1. Motorola V3m ............................................................................................... 46
3.3.2. Motorola L7c ................................................................................................. 50
3.3.3. Motorola Q .................................................................................................... 52
3.3.4. Blackberry 6510 ............................................................................................ 54
3.4. Acquisition using Mobiledit! ............................................................................ 56
3.4.1. Motorola V3m ............................................................................................... 56
3.4.2. Motorola L7c ................................................................................................. 60
3.5. Acquisition using BitPim .................................................................................. 61
3.5.1. Motorola V3m ............................................................................................... 61
3.6. Evidence on the SIM Card ................................................................. 67
  3.6.1. MF_EF_ELP ........................................................................... 70
  3.6.2. MF_EF_ICCID ................................................................. 70
  3.6.3. DF_GSM_EF_IMSI .......................................................... 70
  3.6.4. DF_GSM_EF_KC ............................................................. 71
  3.6.5. DF_GSM_EF_LOCI .......................................................... 72
  3.6.6. DF_TELECOM_EF_MSISDN ........................................... 72
  3.6.7. DF_TELECOM_EF_ADN ................................................. 73
  3.6.8. DF_TELECOM_EF_LND .................................................. 75
  3.6.9. DF_TELECOM_EF_SMS ................................................. 75

4. Evaluation and Results ..................................................................... 91
  4.1. Paraben’s Device Seizure ......................................................... 92
    4.1.1. Usability ........................................................................ 92
    4.1.2. Comprehensive ............................................................. 92
    4.1.3. Deterministic ................................................................. 93
    4.1.4. Verifiable ..................................................................... 93
    4.1.5. Quality ......................................................................... 93
    4.1.6. Capability .................................................................... 93
    4.1.7. Affordability ................................................................. 94
  4.2. BitPim .................................................................................... 94
    4.2.1. Usability ........................................................................ 94
    4.2.2. Comprehensive ............................................................. 95
    4.2.3. Deterministic ................................................................. 95
4.2.4. Verifiable
4.2.5. Quality
4.2.6. Capability
4.2.7. Affordability

4.3. Mobiledit!
4.3.1. Usability
4.3.2. Comprehensive
4.3.3. Deterministic
4.3.4. Verifiable
4.3.5. Quality
4.3.6. Capability
4.3.7. Affordability

5. Future Work

6. Conclusion

Bibliography and References

Appendix A – Acronyms

Appendix B – Device Seizure Screenshots

Appendix C – Mobiledit! Screenshots

Appendix D – BitPim Screenshots
LIST OF FIGURES

Figure 1.1. Organization of a GSM Network Supporting SMS .......................................... 5
Figure 1.2. SIM Card File System .................................................................................... 12
Figure 2.1. Generic Structure of a SIM Card ................................................................. 21
Figure 2.2. Configuration of a SMS Message................................................................. 23
Figure 3.1. Results of the Acquisition Using Paraben’s Device Seizure .......................... 47
Figure 3.2. Call Logs Folder Using Paraben’s Device Seizure ........................................ 48
Figure 3.3. SMS History folder Using Paraben’s Device Seizure .................................... 48
Figure 3.4. Pictures Folder Using Paraben’s Device Seizure .......................................... 49
Figure 3.5. Connectivity Options Using Mobiledit! ....................................................... 57
Figure 3.6. Folders Acquired Using Mobiledit! ............................................................. 57
Figure 3.7. Received SMS Folder Using Mobiledit! ...................................................... 58
Figure 3.8. Phonebook Folder Using Mobiledit! ........................................................... 58
Figure 3.9. Connectivity Options Using BitPim ........................................................... 62
Figure 3.10. Phone Info Dialog Using BitPim ............................................................... 62
Figure 3.11. Phonebook Folder Using BitPim .............................................................. 63
Figure 3.12. Picture Folder Using BitPim ..................................................................... 64
Figure 3.13. Device Type Selection Using Paraben’s Device Seizure ............................. 67
Figure 3.14. Connection Selection Using Paraben’s Device Seizure .............................. 68
Figure 3.15. Data Type Selection Using Paraben’s Device Seizure .............................. 68
Figure 3.16. Summary of Selections Using Paraben’s Device Seizure .......................... 69
Figure 3.17. SIM Card Folders Acquired Using Paraben’s Device Seizure ................. 69
Figure 3.18. Content of the IMSI Folder of the SIM Card in Hex ................................ 71
Figure 3.19. Content of the MSISDN Folder of the SIM Card in Hex ......................... 73
Figure 3.20. Content of the ADN Folder of the SIM Card in Hex ............................ 74
Figure 3.21. Content of the SMS Folder of the SIM Card in Hex ............................. 75
Figure 3.22. SMS Type of Address Layout ............................................................... 77
Figure 3.23. Values of the Type of Address ............................................................... 77
Figure 3.24. Values of the Numbering Plan Identification ......................................... 77
Figure 3.25. Layout of the SMS-deliver Message ....................................................... 78
Figure 3.26. Values of the Fields of the SMS-deliver Message ................................... 78
Figure 3.27. Values of Bit 5 of the Protocol ID .......................................................... 79
Figure 3.28. Values of the Encoding Scheme ............................................................ 80
Figure 3.29. Layout of the Time Stamp ................................................................. 80
Figure 3.30. Hex Value of the SMS “Soccer Tomorrow At Six.” ................................. 82
LIST OF TABLES

Table 1.1. Technologies on Each Generation ................................................................. 7
Table 1.2: Most Important Service Providers in the USA .............................................. 7
Table 1.3. Hardware Characterization........................................................................... 9
Table 1.4. Software Characterization.......................................................................... 10
Table 1.5. Differences Between Traditional and non-Traditional Forensics ............... 13
Table 2.1: Forensic Tools.............................................................................................. 33
Table 3.1. Forensic Tools vs Features.......................................................................... 66
Table 3.2. Hex and Binary Values of the SMS “Soccer Tomorrow At Six.” ............... 83
Table 3.3. Converting the 8-bit Message into a 7-bit Message..................................... 84
Table 3.4. Converting the Septets into Octets............................................................. 85
Table 3.5. Converting the Binary values into Hex....................................................... 86
Table 3.6. Hex and Binary Values of the SMS “Soccer Tomorrow At Six.” ............... 87
Table 3.7. Converting the Octets into Septets............................................................ 88
Table 3.8. Converting the Septets into Octets............................................................ 89
Table 3.9. Converting the Binary Values into their Hex and ASCII Equivalents......... 90
1. INTRODUCTION AND BACKGROUND

Nowadays mobile phones have become one of the most widely used forms of computer. In fact, recent studies have shown that the number of mobile phones in the world is three times the number of personal computers. Mobile phones are used for both personal and organizational purposes. Currently statistics show that the number of users with a mobile phone has greatly increased in the last 20 years. According to the International Association for the Wireless Communications Industry (CTIA), in 1987 there were approximately 883,778 subscribers. In 2007 there were about 243,428,202 users subscribed to a company in the United States. These numbers reflect that in 2007 there were about 275 times more users than in 1987. The increment in number of users has resulted in an increment in the amount of information generated by these devices. There is an extremely large volume of data produced by mobile phones, and, like in computers, this information needs to be analyzed using similar principles [CTIA 2007].

Mobile phones play an important role in people’s life. These devices are not only used to make calls but also as a personal organizer, a digital camera, or a music player. For these reasons, it is now common to find mobile phones at crime scenes. In most cases mobile phones contain valuable evidence that can help in solving the crime. For this reason it is necessary to have qualified people that can deal with this type of evidence. This is the main cause of the appearing of mobile phone forensics as a separate field. Mobile phone forensics is an emerging and new area within the computer forensics field. Unfortunately, the field of mobile phone forensics still lags behind computer forensics. The main reason of this lag is that there is a lack of standards for data acquisition when dealing with evidence in a mobile phone. This is due to the distinctive hardware and
software characteristics of these devices. Every phone has its own features and design, and therefore must be treated individually. This becomes a big challenge for forensic investigators since they must have an extensive knowledge of the different phones and be prepared for unusual scenarios.

Before start talking about computer and mobile phone forensics, it is important to understand the evolution of mobile technology and the development of the systems available for these technologies that are widely used at present time. The following sections of this chapter explain basic aspects of how mobile phones operate, what characteristics they have, and how different they are from computers. In the rest of this document, the terms “handhelds” and “cell phones” are indistinctively used to refer to mobile phones.

1.1. Wireless Generations

There have been three generations of mobile phones: analog (1G), digital (2G), and second generation digital (3G). There is a fourth generation in progress which is called the third generation digital (4G).

1.1.1. First Generation (1G)

The First Generation technology comprises the analog cell phone standards that were introduced in the 1980’s and used until they were replaced by 2G digital phones. 1G systems provided only basic voice service. They use frequency modulation (FM) for radio transmissions. 1G systems consist of Advanced Mobile Phone System (AMPS), Narrowband Advanced Mobile Phone Service (N-AMPS), Nordic Mobile Telephony (NMT), and Total Access Communications System (TACS) [Nichols 2002].
1.1.2. Second Generation (2G)

The Second Generation technology was introduced in the early 1990’s in an effort to solve the main problem with First Generation systems. 2G systems provide digital voice service and data services with improved quality. When calls are made, 1G systems acquire and use a selected frequency band which is released when the call is terminated, resulting in an overwhelmed analog infrastructure. Digital systems were designed to overcome this inefficiency. To accomplish this, voice is divided into fragments of frequency, time, and code for transmission in a more efficient way. Code Division Multiple Access (CDMA), Time Division Multiple Access (TDMA), and Global System for Mobile Communication (GSM) are the base standards for 2G technology [Nichols 2002].

*Time Division Multiple Access (TDMA)*

TDMA is a technology that divides each frequency channel into multiple time slots, each supporting an individual conversation. When a device uses TDMA to communicate, it is assigned a specific time position on the radio channel. TDMA increases its network capacity by allowing multiple users to use different time slots on the same channel. On TDMA, a single channel can serve several users.

The main problem with this technology is that it did not meet the 10-fold call-carrying desired capacity originally demanded by the industry. TDMA was able to multiplex up to three conversations over the same channel at the same time. The first technology that met this 10-fold standard was CDMA [Nichols 2002].
**Code Division Multiple Access (CDMA)**

CDMA is a technology developed by Qualcomm that employs spread spectrum communications and a special coding scheme for the radio link. CDMA spreads the digitalized data over the entire bandwidth available to allow multiple users to be multiplexed over the same physical channel. CDMA claims to have higher quality than GSM because it breaks down and spread data across the entire spectrum. CDMA also offers increased system capacity, fewer dropped calls, and IP data services [Wiki 2008a].

**Global System for Mobile Communication (GSM)**

GSM technology was designed in Europe mainly by Ericsson and Nokia. GSM was the first successful second-generation technology. The GSM cellular system uses a Time Division Multiple Access (TDMA) air interface that refers to a digital link technology whereby multiple phones share a single carrier, radio frequency channel by taking turns. A channel is used exclusively for a period of time and then it is released to let other phones use it [Ayers 2007a].

On GSM, voice channels can be full or half rate. Full rate systems assign only one time slot per frame to each user, each allowing eight users per channel at the same time. Half rate systems are not popular now, but they are expected to emerge in the next years. The idea of half rate GSM systems is to only assign one time slot to every other frame, allowing a maximum of 16 users per single channel at the same time [Nichols 2002].

GSM uses a Subscriber Identification Module (SIM) which is plugged into a card slot in the mobile device. The SIM card contains important information such as user-profile data, access privileges, and information about the cellular carrier. This SIM card can be used in any device that supports GSM technology.
One of the most important protocols available for the GSM standard is the Short Message Service (SMS). This protocol was initially developed as part of the GSM standard, but it is now widely used by the most important technologies. The use of SMSs has become so popular that it is nowadays the most used data application on the planet.

*Short Message Service (SMS)*

The SMS is a communication protocol that allows the interchange of short text messages between mobile phones over the mobile networks. The message is sent from a mobile phone to a central Short Message Center (SMC) which forwards it to the destination mobile phone. If the destination mobile phone is not available at that time, the SMS is stored in the SMC and sent later. A SMS can be no longer than 160 characters. These characters can be alphanumeric or binary non-text messages. Figure 1.1 shows the organization of a GSM network supporting SMS.

![Figure 1.1. Organization of a GSM Network Supporting SMS [Gupta 2008]](image)

**Figure 1.1. Organization of a GSM Network Supporting SMS [Gupta 2008]**

Short Message Service Center (SMSC): The SMSC stores and forwards the messages to and from the mobile stations. The Short Message Entity (SME) which is typically a
mobile phone located in the fixed network or a mobile station, receives and sends short messages.

SMS Getaway MSC (SMS GMSC): The SMS GMSC is the point of contact with other networks. When the GMSC receives a message from the SMC, it uses the SS7 network to find out from the Home Location Register (HLR) the current location of the mobile station.

Home Location Register (HLR): The HLR is a database that holds routing information for the subscriber as well as information of the subscription of the mobile. With this information, the GMSC is able to send the message to the corresponding MSC.

Mobile Switching Center (MSC): The MSC is in charge of switching connections between two mobile stations or between a mobile station and the fixed network.

Visitor Location Register (VLR): The VLR contains temporary information (mobile identification, cell) about the mobile station. The information provided by the VLR helps the MSC switch the message to the correct Base Station System (BSS), which then transfers the message to the destination mobile station.

1.1.3. Third Generation (3G)

The Third Generation technology was developed in response to the consumer’s demands. Cell phone users wanted to add more features to their phones, 3G technologies offer capabilities such as email, wireless Web, and paging services. The most popular 3G technology is Short Message Service (SMS). Other important 3G technologies are Enhanced Data GSM Environment (EDGE), Wideband Code Division Multiple Access (WCDMA), Unstructured Supplementary Service Data (USSD), and General Packet Radio Service (GPRS) [Nichols 2002].
1.1.4. Fourth Generation (4G)

The Fourth Generation has not been developed yet. The reach of this technology is still uncertain but what is known is that it will function on top of the current CDMA, GSM, TDMA, and others. Some of the characteristics of 4G are [Nichols 2002]:

- Entirely packet-switched networks
- On demand high quality audio and video
- Digital network elements
- Higher bandwidths to decrease costs (up to 100 Mbps while moving and 1Gbps while still)
- Tighter network security

To better understand the characteristics of each generation, table 1.1 shows the different architectures and technologies available on each generation.

<table>
<thead>
<tr>
<th>Generation</th>
<th>Architecture</th>
<th>Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st</td>
<td>Analog</td>
<td>AMPS, N-AMPS, NMT, TACS, FDMA</td>
</tr>
<tr>
<td>2nd</td>
<td>Digital</td>
<td>CDMA, TDMA, GSM</td>
</tr>
<tr>
<td>3rd</td>
<td>2nd Generation Digital</td>
<td>SMS, EDGE, GPRS, USSD, WCDMA, WATM</td>
</tr>
<tr>
<td>4th</td>
<td>3rd Generation Digital</td>
<td>Builds on CDMA, TDMA, GSM</td>
</tr>
</tbody>
</table>

Finally, table 1.2 shows the seven most important service providers in the USA and the number of subscribers on each technology.

<table>
<thead>
<tr>
<th>Voice Technology</th>
<th>Data Technology</th>
<th>Subscribers (in millions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT&amp;T</td>
<td>GSM, UMTS</td>
<td>GPRS, EDGE, UMTS, HSPA</td>
</tr>
<tr>
<td>Verizon Wireless</td>
<td>CDMA</td>
<td>CDMA2000, EV-DO</td>
</tr>
<tr>
<td>Sprint Nextel</td>
<td>CDMA, iDEN</td>
<td>CDMA2000, EV-DO</td>
</tr>
<tr>
<td>T-Mobile</td>
<td>GSM, UMTS, GAN</td>
<td>GPRS, EDGE, UMTS, HSPA</td>
</tr>
<tr>
<td>Alltel</td>
<td>CDMA</td>
<td>CDMA2000, EV-DO</td>
</tr>
<tr>
<td>TracFone Wireless</td>
<td>GSM, CDMA</td>
<td>GPRS, CDMA2000</td>
</tr>
<tr>
<td>U.S. Cellular</td>
<td>CDMA</td>
<td>CDMA2000, EV-DO</td>
</tr>
</tbody>
</table>
1.2. Mobile Phone Characteristics

Now that the different technologies in which mobile phones operate have been described, it is necessary to go over the characteristics of these devices to understand how they operate. Mobile phones perform different functions that can vary from a simple organizer to a personal computer. Every mobile phone has its own features; however, there are some basic characteristics about these devices that can be generally defined:

- Designed for mobility
- Compact size
- Battery powered
- Require specialized interface, media and hardware

[Ayers 2007a]

Furthermore, most mobile phones have this basic hardware:

- Microprocessor
- Read Only Memory (ROM)
- Random Access Memory (RAM)
- A Digital Signal Processor
- A Radio Module
- Microphone and Speaker
- A Liquid Crystal Display (LCD)
- Hardware keys

In order to better understand how these characteristics vary, mobile phones can be divided into three groups, basic, advanced and smart mobile phones. Hardware characteristics are different in each group. Table 1.3 shows how each characteristic varies on each group.
Table 1.3. Hardware Characterization [Ayers 2007a]

<table>
<thead>
<tr>
<th></th>
<th>Basic</th>
<th>Advanced</th>
<th>Smart</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Limited Speed</td>
<td>Improved Speed</td>
<td>Superior Speed</td>
</tr>
<tr>
<td>Memory</td>
<td>Limited Capacity</td>
<td>Improved Capacity</td>
<td>Superior Capacity, Built-in Hard Drive</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Possibility</td>
</tr>
<tr>
<td>Display</td>
<td>Grayscale</td>
<td>Color</td>
<td>Large size, 16-bit Color</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(65,536 colors) or Higher</td>
</tr>
<tr>
<td>Card Slots</td>
<td>None</td>
<td>MiniSD or MMCmobile</td>
<td>MiniSDIO or MMCmobile</td>
</tr>
<tr>
<td>Camera</td>
<td>None</td>
<td>Still</td>
<td>Still, Video</td>
</tr>
<tr>
<td>Text Input</td>
<td>Numeric Keypad</td>
<td>Numeric Keypad, Soft Keyboard</td>
<td>Touch Screen, Handwriting Recognition</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Built-in QWERTY-style Keyboard</td>
</tr>
<tr>
<td>Cell Interface</td>
<td>Voice and Limited Data</td>
<td>Voice and High Speed Data</td>
<td>Voice and Very High Speed Data</td>
</tr>
<tr>
<td>Wireless</td>
<td>IrDA</td>
<td>IrDA, Bluetooth</td>
<td>IrDA, Bluetooth, WiFi</td>
</tr>
<tr>
<td>Battery</td>
<td>Fixed, Rechargeable Lithium Ion Polymer</td>
<td>Removable, Rechargeable Lithium Ion Polymer</td>
<td>Removable, Rechargeable Lithium Ion</td>
</tr>
</tbody>
</table>

As it can be noted on this table, basic mobile phones support limited voice and data communication, and some basic Personal Information Management (PIM) applications, like the phonebook. More features are available on advanced mobile phones, like Internet, email services, instant messaging, and more advanced PIM applications such as a camera. Smart devices are capable of running general and special purpose applications. These devices are usually larger than regular phones, have a bigger display, and in some cases integrate a touch sensitive screen. Smart phones offer built-in wireless communications and synchronization protocols that can be used to exchange other types of data, such as audio, video, graphics. The following table shows the differences in software found on each group [Ayers 2007a].
Finally, it is important to indicate that these tables are only references and need to be flexible. This is mainly because over time advanced features appear on basic mobile phones and smart mobile phones tend to include new features like digital cameras, global positioning systems, and PDA’s [Ayers 2007a].

### 1.3. SIM Card Characteristics

The Subscriber Identity Module (SIM) is the removable component that is present in devices that operate with GSM cellular networks. The SIM contains essential information about the subscriber and the mobile phone cannot operate without the SIM. The main function of the SIM is to authenticate the user of the phone to the network in order to gain access to the services. It is also used to storage personal information, like text messages, phone book entries, and network configuration information [Ayers 2007a].

There are two sizes of SIMs available, but the most widely used is the smaller. The module has 25 mm of width, 15 mm of height, and a thickness of .76 mm. It has 8 pin connectors that form a circular contact pad. When the SIM is connected into a phone,
a serial interface is used to communicate with the computing platform using a half duplex protocol.

The SIM card is protected with a Personal Identification Number (PIN). Usually, there are two PINs, PIN1 and PIN2 that are used to restrict access. The SIM allows a preset number of attempts (usually 3) to enter the correct PIN before it blocks. The PIN Unblocking Key (PUK) is used to reset the PIN number and the attempt counter. It can be obtained from the service provider or the network operator. The preset number of attempts to enter the PUK is usually ten. If this number is exceeded the card is blocked permanently [Ayers 2007b].

The SIM card consists of the following modules: Central Processing Unit (CPU), Random Access Memory (RAM) to process commands, Electronically Erasable Programmable Read Only Memory (EEPROM) to store user files, and Read Only Memory (ROM) to store the card’s operating system. These five modules are integrated into an Integrated Circuit (IC).

When the SIM card is activated the CPU loads the operating system from ROM to the RAM of the SIM and starts processing the commands that the mobile equipment requests. The filesystem of SIM cards is stored in the internal EEPROM, and organized in a hierarchical tree structure (see Figure 1.2). The filesystem consists of the following elements [Nelson 2008]:

Master File (MF): this is the root of the file system which contains both directory and elementary files.

Directory or Dedicated Files (DF): these files are subordinated to the master files and can contain directory and elementary files.
Elementary Files (EF): these files contain the actual data (header and body).

There are several DF under the MF but three of special interest: DF$_{GSM}$, DF$_{DCS1800}$, and DF$_{TELECOM}$. The EFs under DF$_{GSM}$ and DF$_{DCS1800}$ contain network related data on different frequency bands. DF$_{GSM}$ contains EFs exclusively for GSM 900 MHz and DF$_{DCS1800}$ for DCS (Digital Cellular System) 1800 MHz band operation. The DF$_{TELECOM}$ contains EFs with more general service related data, such as the phonebook.

It is important to note that there is an EF linked directly to the MF. This EF is the Integrated Circuit Card Identity and is called EF$_{MF1}$. It contains the serial number of the SIM card which is unique. This is an electronic equivalent of the serial number located on the exterior of the SIM card. This information is important in a forensic point of view because it will help the examiner to determine the origin of the SIM card.
1.4. Digital Forensics vs. Handheld Forensics

Before going any deeper it is important to understand the definitions and relationship between digital and handheld forensics. The book “Alternate Data Storage Forensics”, gives a definition of Digital Forensics that is adequate for this purpose:

“Digital Forensics is the examination of hardware or software in the pursuit of evidence to disprove or prove an allegation.” [Cohen 2007]

Additionally, the authors provide a definition for Handheld Forensics:

“Handheld Forensics is the examination of hardware and software that are typically an integrated unit in the pursuit of evidence to disprove or prove an allegation.” [Cohen 2007]

By looking at these definitions, it is clear that digital forensics and handheld forensics have some likenesses but they also have many differences. This section details the main differences from a forensic point of view. The four main differences between the traditional computer forensics approach and the nontraditional handheld forensics approach are listed in table 1.5 and explained in detail in the following subsections:

Table 1.5. Differences between Traditional and non-Traditional Forensics

<table>
<thead>
<tr>
<th></th>
<th>Traditional Computer Forensics</th>
<th>Nontraditional Handheld Forensics</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Storage device requiring file system</td>
<td>Embedded system device</td>
</tr>
<tr>
<td>2.</td>
<td>Device is Static</td>
<td>Device is Active</td>
</tr>
<tr>
<td>3.</td>
<td>Larger storage capacity</td>
<td>Smaller on board storage capacity</td>
</tr>
<tr>
<td>4.</td>
<td>Forensic: Bit stream imaging</td>
<td>Forensic: active memory imaging</td>
</tr>
</tbody>
</table>
1.4.1. **File System**

Data on a hard drive is stored differently from data on a handheld. When a forensic investigator examines a hard drive or other type of media he/she knows it will contain data associated to a file system. Some common file systems are FAT, NTFS, EXT2, and some others.

Handhelds devices have a different design. They have an embedded system which is specifically designed for the device. Media cards or SIM cards associated to the device have file systems, but the data itself is bound to the actual device to gain its structure. This consideration has a dramatic impact in handheld forensics. It is extremely important for the examiner to fully understand both the operating system and the design of the device to reduce the chances of making mistakes [Cohen 2007].

1.4.2. **Static/Active Device**

Forensic in hard drives and media is said to be static because once the forensic procedures are performed, the device does not change its state while seized. A variety of write protection devices can be used to keep the hard drive or media in its original state. However, handhelds devices keep active even after the correct forensic procedures are applied. This is due to the way handhelds behave. Because of the limited storage capabilities, the handheld is continuously moving around data to form successive lines of storage to guarantee optimal use [Cohen 2007].

1.4.3. **Storage Capacity**

Traditionally, hard drives and media have had larger storage capacities than handheld devices. Former computers accommodated just 5 or 10 MB of hard drive. When
storage became cheaper, manufacturers started to raise the capacity of the hard drives. Just a few years ago, standard hard drives had a storage capacity of 8 GB. Nowadays, almost no computer comes with a hard drive smaller than 100 GB, and they can easily incorporate a hard drive of 200 or 300 GB [Cohen 2007].

Despite of not being as dramatic as in computers, handheld devices have also experienced a change in their storage capacity. In the past, handhelds had an on-board storage capacity of just 8 MB. At present time, storage capacity of modern handheld devices is 1 GB or more, depending on the storage structure of the device. Future trends indicate that as more functionality is added to the handheld device, higher storage capacity will be also necessary.

1.4.4. Forensic Imaging

In hard drives and media, a forensic acquisition is achieved by a bitstream image, which is a bit-by-bit copy of all allocated and unallocated data associated to the device. In handheld devices, an active memory image is performed to acquire data in a forensic manner. A bitstream image is similar to an active memory image since both copy all allocated and unallocated data. The difference is that there is some data on the handheld device which is either reserved by the manufacturer or encrypted and locked from access. This represents a big problem for the forensic investigator since there is some data on the device that is not accessible for examination.

Another main difference is that a bitstream image is verifiable and can be revised in the future for accuracy. On the other hand, since data on handheld devices is constantly moving and being reallocated, it is impossible to verify a hash value of an active memory
image. The forensic examiner can only verify an active image at one point and time [Cohen 2007].

1.5. Legal Considerations

Mobile devices are radios and therefore covered by the Electronic Communications Patriot Act (ECPA) and Title III. The Electronic Communications Privacy Act amended Title II of the Omnibus Crime Control and Safe Street Act of 1968. The ECPA included three titles and was passed by Congress in 1986. Title I (Wiretap Act) and Title II (Stored Communication Act) introduced two legal points that relate to mobile phone forensics.

1.5.1. Wiretap Act (Title I)

It protects wire, oral, and electronic communication while in transit. Title I makes it unlawful to listen to or observe the contents of a private communication without the permission of at least one party to the communication and regulates real-time electronic surveillance in federal criminal investigations. Because mobile devices are capable of receiving aural communication and because part of that communication travels along wires, they are included in the Wiretap Act [Wiki 2008c].

There is one exception to the Wiretapping Act that was designed for corporate environments. According to the act, there is no violation when one party has given specific authorization to have a communication intercepted.

1.5.2. Stored Communication Act (Title II)

It protects communication held in electronic storage. Title II prohibits the disclosure of user information to non-government entities. A warrant or court order must
be provided in order to obtain information about a user that is stored by a communication service provider. Since mobile devices can store SMS, MMS, pictures, e-mail, etc., they fall under the Stored Communication Act.

The USA Patriotic Act (USAPA) amended these provisions to permit disclosure of information to the government with the consent of one of the parties or when the service provider reasonably believes that there is an imminent danger of death or serious injury to any person [Wiki 2008c].
2. USE OF FORENSIC SOFTWARE TOOLS TO ACQUIRE EVIDENCE FROM MOBILE DEVICES

After reviewing all the characteristics of cell networks, mobile phones, and identity modules, it is clear that a forensic acquisition of this data is extremely important when dealing with mobile phones. There are many methods of acquiring data from mobile phones. The most effective is to use a software application (using a desktop) to communicate with the mobile phone and store the data retrieved from the phone in behalf of the computer.

2.1. Evidence Sources

There are four places where data can be found in mobile phones [McCarthy 2005]:

- The phone’s embedded memory
- The SIM card (if present)
- The phone’s removable card (if present)
- The service provider

The amount of data available from mobile phones and SIM cards depends in great manner on the storage capacity of the device and card. Greater storage capacity will result in more information to analyze. Also, it is important to mention that some devices have more or less information available depending on the manufacturer’s characteristics.
2.1.1. Data Stored in the Phone Memory

Memory is available to store additional data like phone numbers, call logs, settings, application executables, text messages, calendar events, location information, images from camera, and so on. While old phones had relatively small memory a few years ago, modern phones have a larger amount of memory. For this reason, the internal memory has become the most important source of evidence in mobile phones.

It is also important to point out that it is also possible to recover deleted items. The time that these items are stored in memory may vary according to the amount of memory available in the phone. This is why it is important for the investigator not to waste time and start as soon as possible [McCarthy 2005].

With that in mind, the following are some potential sources of evidence that must be inspected when conducting a mobile phone forensic investigation [Kipper 2007]:

- Calls: received calls, sent calls, missed calls, deleted calls.
- Graphics: downloaded images, pictures from camera.
- SMS: sent SMS, received SMS, unsent SMS, deleted SMS (SIM), and SMS templates.
- Sounds: downloaded sounds, ring tones, voice memos, music (MP3).
- Phonebook
  - Phone numbers: general, mobile, work, home, fax, and other.
  - Address Info: postal address, email, URL, street, city, state, zip, country.
  - Date: date, text date, and time zone (GMT offset).
  - Personal Info: name, last name, first name, company, job title, caller group.
  - Custom Fields: custom1, custom2, and so on.
Binary Data IDs: ring tone ID, picture ID.

- Calendar: reminder or date, call, meeting, birthday, anniversary, memo, travel, vacation, training reminder, alarm, alarm repeating each day, miscellaneous.
- Subscriber identifiers
- Equipment identifiers
- Service provider
- Other networks encountered

2.1.2. Data Stored in the SIM Card

The SIM card used in GSM phones enables the device to connect to GSM networks, and the user to be identified in the network. This card contains personal information like: The IMSI (International Mobile Subscriber Identity), which is the SIM’s identifier, language preferences, network information, location of the phone, phone book entries, sent and received SMS messages, dialed numbers. It is important to note that some of these features on a SIM card are optional, so they may or may not be available [Jansen 2006].

To access the SIM card in order to obtain evidence, the investigator needs to enter the PIN (Personal Identification Number) code or the PUK (Pin Unblock Key) code. In the case of the PIN, it can be obtained from the user; the PUK can be obtained either from the user or from the service provider [McCarth 2005].

Figure 2.1 shows the generic structure of a SIM card with the most important Directory and Elementary files. These files hold valuable evidence from a forensic point of view and therefore must be examined and analyzed when conducting a forensic investigation.
Extender Language Preferences (ELP)

This EF usually allocates 10 bytes to store an extended list of the preferred languages for the user interface. Each country code is made up of 2 alphanumeric characters according to ISO 639 using the 7-bit default GSM alphabet.

KC (Ciphering Key)

GSM authentication involves the SIM card in the mobile device and the Authentication Center (AC). The subscriber has one copy of a secret Ciphering Key (KC) stored in the SIM card and the other copy is stored in the AC. This EF holds the KC key
to encrypt data on the air interface. The size of this EF is usually 9 bytes and is coded according to the following scheme:

Bytes 1-8: used to hold the KC key.

Byte 9: used to identify the serial number of the key.

_Location Information (LOCI), Serial Number (ICCID), Subscriber ID (IMSI), and Phone Number (MSISDN)_

The bytes 5-9 of the LOCI file contain the network Location Area Identifier (LAI) where the mobile phone is currently located. This value is retained when the mobile phone is powered down. With this information the forensic investigator can determine the Location Area of the mobile phone when last used. The problem is that a Location Area can contain several cells, and this information is not stored in the SIM card [Willassen 2003].

The Integrated Circuit Card Identifier (ICCID), the International Mobile Subscriber Identity (IMSI) and the Mobile Station ISDN Number (MSISDN) provide unique identification of the customer. The serial number (ICCID) corresponds to the number printed on the surface of the SIM card. The Subscriber ID (IMSI) corresponds to a unique ID number for every subscription on the operator’s network. The MSISDN is the phone number to the mobile phone [Willassen 2003].

_Abbreviated Dialing Numbers (ADN)_

Most mobile phones have the ability to store commonly dialed phone numbers. SIM cards usually have more than 100 slots to store short dial numbers each with a variable size (usually 32 bytes). These records are stored in the Elementary File (EF) called Abbreviated Dialing Numbers (ADN). Each record holds the name and the
associated phone number. When a record is deleted, the slots are filled with FF hex value so deleted records cannot be recovered. However, since slots are allocated in sequence, empty slots between used slots indicate that one or more records have been removed from the file [Willassen 2003].

*Last Numbers Dialed (LND)*

SIM cards are also able to store information related to the last numbers dialed. Most cards have either 5 or 10 slots of variable size for this purpose. However, most phones use the phone’s memory for this feature and leave this file empty. In any case, it is important to investigate both places when looking for evidence. If used, it follows the same coding scheme as the ADN EF [Willassen 2003].

*Short Message Service (SMS)*

SMS messages are stored in the EF_SMS elementary file beneath the DF_TELECOM directory file. Each record stored in this elementary file has a fixed length. The length of SMS messages stored on the SIM card is 176 bytes. The configuration of a SMS message on the SIM card is shown in figure 2.2 [Willassen 2003]:

![Figure 2.2. Configuration of a SMS Message](image)

The First byte of the SMS is the Status byte. This byte can take any of the following values:

- 00000000 – Unused
- 00000001 – Mobile terminated message, read
00000011 – Mobile terminated message, unread

00000101 – Mobile originated message, sent

00000111 – Mobile originated message, not sent

When a SMS message is deleted the status byte is set to x/00 so that a new SMS message can be allocated into that space. The record retains the content of the message until a new messages arrives and overwrites the old message. It is also important to remark that when a previous message is overwritten by a new message that is smaller than the assigned space (176 bytes), the remaining space is overwritten with x/FF. For this reason it is extremely important to prevent that new messages destroy deleted messages by overwriting the same record.

The TPDU part of the SMS message also contains relevant information (175 bytes). However, there are some elements that are of special interest for the forensic investigator:

- The Integrated Services Digital Network (ISDN) number of the SMS service center
- The Integrated Services Digital Network (ISDN) number of the sender or receiver depending on the status of the message
- Date and time (in seconds) when the message was received by the SMS service center
- Phonebook number on the Mobile Station (i.e. inbox, sent, drafts)
- The message itself encoded according to the proper standard (the most common is 7-bit GSM encoding)
2.1.3. Data Stored in the Phone’s Removable Card (Flash Memory)

Some mobile phones include a flash memory to extend the storage capacity of the phone. These removable cards are usually used to store media files, like video, audio, pictures, MMS messages, and any other files that can be stored on the phone. These cards are not used to store phone related data. For example, some items that can not be stored in the removable card are phone numbers, dialing lists, text messages, and some others. These items are usually stored either in the SIM card or in the phone memory.

2.1.4. Data Stored in the Service Provider

The service provider holds important information about the subscriber, location, bills and call logs. Whenever a call is made or a message is sent, a data log is created and stored. This log contains the sender’s and receiver’s phone numbers, the location, and the length of the call [Mellars 2004]. Location information can be determined by looking at the cell site tower information that is stored in the service provider. Each cell can be associated to a geographical location to locate the area where the call was made. This information can help to establish if a person was in a specific place at a specific time. Also, it can help to determine the direction of travel or the behavioral pattern of the suspect. The problem is that some of these cell towers service phones at distances of up to 20 miles, so accuracy can be a problem in this case. Fortunately, densely populated areas have cell towers with limited coverage area where is much easier to determine the location of the device.

Depending on the service provider, other valuable information that can be obtained from the service provided is: subscriber’s name and address, billing name and address (if different), user name and address (if different), billing account details,
telephone number, IMSI, ICCID, PIN/PUK for the SIM, services available [Ayers 2007a].

2.2. Procedural Models for Mobile Phone Forensics

After reviewing the sources of evidence for mobile forensic it is important to introduce a standard procedure to deal with the evidence. There are several procedural models available when referring to digital evidence, most of them developed mainly for evidence in computer systems. Since handheld forensics is a relatively new field, there are limited procedures on how to deal with this type of evidence. However, procedures developed for digital forensics in general can be used as guidelines to develop a more specific methodology oriented towards mobile phones in particular. In the following section, some of the most well known procedural models for digital evidence are introduced and briefly explained.

According to the book “Alternate Data Storage Forensics”, four different phases of digital forensics are recognized and proposed [Cohen 2007]:

Collection: In this phase, a bitstream copy of the original media is created. This bitstream copy is then run through a hashing algorithm to make sure it is not altered. To accomplish this, the hard drive is removed from the device and connected to a write-blocking hardware to avoid contamination of the evidence. Finally, the duplicate is generated using some forensic software.

Examination: Here is where data is actually extracted to find the evidence. This usually includes the examination of document content, images, email, dates, metadata, and others.
Analysis: This is the process where the evidence previously recovered during examination is analyzed in an effort to solve the case. In this phase, all the pieces are put together in order to create a story of what happened.

Reporting: Is where all other phases are documented and explained. Usually, the report generated contains details of the hardware, software tools used, procedures and techniques followed, and documentation of the findings.

The document “Electronic Crime Scene Investigation – A Guide to First Responders”, developed by the U.S. Department of Justice, suggests the following methodology when dealing with digital evidence [ECSI 2001]:

Securing and Evaluating the Scene: The initial task of the first responder is to protect the integrity of the electronic evidence. After this, the first responder must identify potential evidence and determine if perishable evidence exists. Perishable evidence should be secured, documented and photographed. The first responder should evaluate the scene and devise a search plan.

Documenting the Scene: The purpose of this step is to create a perpetual historical record of the scene. There should be complete and detailed documentation of the scene. However, it is important to understand that documentation is an activity that must be present at every step of the investigation.

Evidence Collection: Digital evidence must be handled and collected carefully to conserve its evidentiary value. It is important to protect the evidence that can be altered by some factors such as static electricity, magnets, radio transmitters, and so on.

Packaging, Transportation, and Storage: The purpose of this step is to ensure that electronic evidence is properly packaged, transported, and stored to avoid alteration,
damage, or destruction of data. Forensic specialist must be aware that some evidence may be lost if exposed to extended storage.

There are also a few procedures specifically developed for evidence in mobile phones. One of the most popular procedural models is the one proposed in the “Guidelines on Cell Phone Forensics”. This model is made up of 4 different phases [Ayers 2007a]:

**Preservation**: This is the first phase of evidence recovery where the suspect’s property is seized without altering the content of data which reside on the devices and removable media. Preservation involves the search, recognition, documentation, and collection of electronic–based evidence.

**Acquisition**: This is the process of imaging the digital device and any removable media. Any information related to the device and its peripheral equipment is obtained in this phase. Usually, it is best to perform the acquisition at a forensics laboratory where all the technical equipment is available. However, there may some cases when it is necessary to perform acquisition at the scene to avoid loss of information due to power shortage, battery damage, and other problems that can occur during transportation and storage.

**Examination and Analysis**: The objective of the examination process is to uncover hidden or obscured digital evidence. It is important to separate relevant from irrelevant information to reduce the amount of data to be analyzed. The analysis process starts when examination ends. This process looks at the results from examination for its direct importance and value to the case. Examination needs to be performed by a technical forensic specialist but analysis can be done by someone other than a technical specialist, such as the investigator.
**Reporting:** This is the process of preparing a detailed synopsis and conclusions of all the previous phases followed and conducted. It is important to maintain a careful record of all actions, describe the results of tests and examinations, and explain the inferences obtained from the evidence. A competent report should rely on solid documentation, photographs, notes, and tool-generated content.

Finally, it is important to mention that due to the changing nature of handheld forensics, it may be necessary that the model selected be flexible in one or more stages to adjust to the needs of a particular case.

### 2.3. Rules when Dealing with Handheld Devices

Gregory Kipper in his book “Wireless Crime and Forensic Investigation” proposes the following set of forensic rules when dealing with cellular phones [Kipper 2007]:

#### 2.3.1. Rule 1: Stop Wireless Receiving

Before starting the investigation it is important to maintain the evidentiary integrity of the device. For this reason, some type Faraday equipment must be used. If the device is on, it is not recommended to turn it off because of the use of the Personal Identification Number (PIN). If the device is using a PIN and is turned off, the investigator will not be able to acquire the evidence.

#### 2.3.2. Rule 2: Charge Device

Since power cable and data transfer cable are plugged into the same area, it is recommended that the device at least have 50% charge before starting the acquisition so that the connection to the device via cable can be maintained during this process. A 50%
charge for the device is a good rule of thumb when performing data acquisition on the device.

2.3.3. **Rule 3: Cabling and Accessories**

Cables for cellular phones are usually designed specifically for a specific model. These cables are also used to connect the device to the computer and conduct the forensic acquisition. Manufacturers now offer a variety of cables for the different models. Additionally, some software vendors now provide cable kits for some of the most common phones available in the market.

On the other hand, it is also necessary to gather other potential accessories that are used to connect or communicate with the device. These accessories must be examined in the context of attachment to the phone.

2.3.4. **Rule 4: Acquire in Laboratory**

The best recommendation is to perform the acquisition in a laboratory where the investigator has all the technical equipment. A Faraday bag is generally used in a laboratory to ensure that the quality of the evidence is maintained. However, more advanced equipment such as a tent system or even a complete Faraday room is deployed in many laboratories.

2.4. **Forensic Tools**

Forensic software for mobile phones is different from the software used for computers. The previous chapter described how computers were different from mobile devices and the need of forensic software exclusive for mobile phones. These are some of the reasons that explain the large number of forensic tools available in the market.
exclusively for mobile phones. However, a problem is that most of these tools were
designed to operate on specific brands or models, operating systems, or hardware
architectures [Ayers 2007a].

Forensic tools acquire information from a device in two ways: Physical or Logical
acquisition. In a physical acquisition, a bit by bit copy of an entire physical store is made.
In a logical acquisition, a bit by bit copy of a logical object that resides on a logical store
is made. An example of a physical store is a memory chip, and a logical object can be a
directory.

A main difference between these two types is that physical acquisition allows
deleted data to be recovered. In a logical acquisition, deleted files would not be possible
to be recovered. On the other hand, in a logical acquisition a tool can easily extract and
provide a better organization of the system data structure that will be used during
examination. For these reasons, it is always better to perform both types of acquisition
when possible. Also, it is important to emphasize that the physical acquisition should be
done before the logical acquisition.

Most software tools are capable of performing all the functions: acquisition,
examination and reporting, and some tools concentrate just on a subset. This is the main
reason why the forensic investigator needs to be familiar with different and diverse
software tools and toolkits. For instance, Personal Information Management (PIM) data,
incoming/outcoming calls, text messages, email messages, content visited over the Web,
images, audio, video, are some examples of the information that a tool can acquire from a
mobile phone.
According to the *Cell Phone Forensic Tools: An Overview and Analysis* document [Ayers 2007b] there are several factors that influence the information present on a mobile phone. These factors include the following:

- The inherent characteristics implemented by the manufacturer
- The modifications made by the service provider or network operator
- The network services that the user is using
- The modifications made by the user

Table 2.1 shows some of the most important tools available for mobile phone investigations. In addition, the functions that each tool performs is provided to help the investigator compare between tools. Finally, it shows if the tools is intended to target SIM or USIM cards only, handset devices only or both.
Table 2.1: Forensic Tools [Ayers 2007a]

<table>
<thead>
<tr>
<th>Function</th>
<th>Target Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forensic Card Reader</td>
<td>Acquisition, Reporting</td>
</tr>
<tr>
<td>ForensicSIM</td>
<td>Acquisition, Examination, Reporting, SIM</td>
</tr>
<tr>
<td>SIMCon (now Paraben's SIM card Seizure)</td>
<td>Acquisition, Examination, Reporting, SIM and USIM</td>
</tr>
<tr>
<td>SIMIS</td>
<td>Acquisition, Examination, Reporting, SIM</td>
</tr>
<tr>
<td>USIMdetective</td>
<td>Acquisition, Examination, Reporting, SIM and USIM</td>
</tr>
<tr>
<td>BitPIM</td>
<td>Acquisition, Reporting</td>
</tr>
<tr>
<td>Oxygen PM (forensic version)</td>
<td>Acquisition, Examination, Reporting, Nokia Phones</td>
</tr>
<tr>
<td>Oxygen PM for Symbian (forensic version)</td>
<td>Acquisition, Examination, Reporting, Symbian Phones</td>
</tr>
<tr>
<td>PDA Seizure</td>
<td>Acquisition, Examination, Reporting, Palm OS, Windows Mobile/Pocket PC, and Blackberry devices</td>
</tr>
<tr>
<td>Pilot-Link</td>
<td>Acquisition</td>
</tr>
<tr>
<td>Device Seizure</td>
<td>Acquisition, Examination, Reporting, TDMA, CDMA and GSM phones. SIM and USIM</td>
</tr>
<tr>
<td>CellDEX</td>
<td>Acquisition, Examination, Reporting, GSM and CDMA phones. SIM and USIM</td>
</tr>
<tr>
<td>GSM .XRY</td>
<td>Acquisition, Examination, Reporting, GSM and CDMA phones. SIM and USIM</td>
</tr>
<tr>
<td>MobilEdit!</td>
<td>Acquisition, Examination, Reporting, GSM phones. SIM</td>
</tr>
<tr>
<td>PhoneBase</td>
<td>Acquisition, Examination, Reporting, GSM phones. SIM and USIM</td>
</tr>
<tr>
<td>Secure View</td>
<td>Acquisition, Examination, Reporting, TDMA, CDMA and GSM phones. SIM and USIM</td>
</tr>
<tr>
<td>TULP 2G</td>
<td>Acquisition, Reporting</td>
</tr>
</tbody>
</table>

As it can be seen on the table, three groups of tools can be distinguished: tools that target SIM cards, tools that target the handset, and integrated tools that perform both activities. The following sections will discuss the main characteristics and capabilities of each group of tools.
2.4.1. SIM Tools

Most of the tools that read the content of the (U) SIM module acquire some or all of the following data: International Mobile Subscriber Identity (IMSI), Integrated Circuit Card ID (ICCID), Abbreviated Dialing Number (ADN), Last Numbers Dialed (LND), SMS messages, and Location Information (LOCI).

More powerful tools are able to recover deleted SMS messages, rendered foreign language SMS messages, and EMS messages with simple graphics and sounds embedded. They also provide features like PIN administration [Ayers 2007a].

SIMCon (Now Paraben’s SIM Card Seizure)

Paraben has acquired SIMCon and has integrated it into SIM Card Seizure and Device Seizure. This tool is able to recover deleted SMS/text messages and perform comprehensive analysis of all directories and files present on the SIM card to acquire non-standardized directories and files. SIM Card Seizure works with any standard smart card reader compliant with the PC/SC standard. Examiners are able to create customized reports with relevant information [Paraben 2008].

SIMIS

This tool allows examiners to extract data from a SIM securely and protect the integrity with cryptographic hashes. SIMIS presents the recovered data in its original language, in an easily browsable format, complete with comprehensive print facilities and selectable scan depth. SIMIS recovers the following data: phonebook contacts and numbers, SMS text messages, deleted text messages, time and date information and more. This tool provides a detailed report in easily viewable HTML format [Simis 2008].
USIMdetective

USIMdetective allows the investigator to acquire, examine, and produce reports from any GSM SIM or USIM card using a PC/SC compatible reader. Some of the information that this tool retrieves is: phonebook contacts, phonebook numbers, SMS text messages, deleted text messages, call records, and more. Items acquired with this tool can be displayed in a textual or hexadecimal format [Usim 2008].

2.4.2. Handset Tools

There is a group of tools that deal exclusively with handsets. Some of these tools are targeted to PDA devices and are useful when dealing with smart phones that use operating systems such as Palm OD and Windows Mobile devices. In general, handset tools exclude the capability to acquire data from SIMs using a direct read [Ayers 2007a].

Oxygen Forensic Suite

Oxygen Forensic is a PC software designed to extract the maximum information from mobile phones and smartphones for investigation purposes. This tool allows examiners to acquire data from the devices and export the data into multiple supported formats. This tool can acquire the following data: contact list (phone numbers, photo, email, addresses, faxes, etc), caller groups, call history, SMS, MMS and email messages, calendar events, to-do elements, text notes, photos, video, sound, and more. Oxygen Forensics provides support for more than 300 mobile phones from Nokia, Vertu, Sony Ericsson, Samsung, Siemens, Motorola, Panasonic, and other [Oxygen 2008].
Pilot Link

This is an open source software tool that was built to transfer information between Palm OS devices and Linux hosts. Currently, it runs on Windows and Mac OS as well [Pilotlink 2008].

BitPIM

BitPIM is a phone management program that allows the examiner to view and manipulate data on many CDMA phones from LG, Samsung, Sanyo and others. To acquire data using this tool, examiners need the cable and driver required in order to establish the connection between the computer and cell phone. Data recovered with this tool includes: phonebook, calendar, wallpapers, ringtones, videos, memo, SMS, call history, and the filesystem for most Qualcomm CDMA chipset based phones. This tool is distributed as open source software and runs on Windows, Linux and Mac OS. SIMIS provides support for about 100 phone models [Bitpim 2008].

2.4.3. Integrated Tools

The last group includes all the toolkits that are able to perform the tasks of both (U) SIM and handset tools on under and integrated framework. Obviously, one advantage of these tools is that they can generate a single report with the results of both examinations. Integrated tools can be really helpful but in some cases it is also necessary to use (U) SIM or handset targeted tools [Ayers 2007a].

MOBILedit!

MOBILedit! Forensic is a commercial tool that can acquire data logically as well as search, examine, and report data from GSM, CDMA, and PCS cell phones. It analyzes the phone via Bluetooth, IrDA, or cable connection. Some of the data MOBILedit!
analyzes is: phonebook, last dialed numbers, missed calls, received calls, SMS messages, multimedia messages, photos, files, phone details, calendar, notes, and tasks. Data collected from the mobile phone can be printed or stored. Print reports are ready for use in court and can be generated in any language. Data is stored in the .med file format and can be exported into any supported format (Word, Excel, XML/XSL). The latest version of this tool supports 478 different mobile phones [Mobiledit 2008].

Device Seizure

This tool was recently launched by the Paraben’s group. It combines the functionality of Paraben’s PDA Seizure 1.0 and Paraben’s Cell Seizure. This tool allows examiners to acquire, search, examine, and report data associated with cell phones on CDMA, TDMA, and GSM networks. Device Seizure can perform a logical and a physical acquisition of the data. The amount and quality of data that can be acquired from a physical acquisition surpasses the information that can be acquired from a logical acquisition. Device Seizure can acquire the following data: SMS history, deleted SMS, phonebook, call history, datebook, scheduler, calendar, to-do list, filesystem (physical memory dumps) such as system files, multimedia files, Java files, deleted data, email, and more. This tool provides support for over 1900 handheld devices [Paraben 2008].

GSM.XRY

GSM.XRY is a forensic software toolkit for acquiring data from GSM, CDMA, 3G phones, and SIM/USIM cards. This tool permits the connection to cell phones via IR, Bluetooth, or a cable interface. Data acquired from cell phones are stored in the .XRY format and cannot be altered, but can be exported and into external formats and viewed with third-party applications. Some of the information that can be acquired with this tool
includes the following: summary screen, case data, general information, contacts, calls, calendar, SMS, pictures, audio, files, notes, tasks, MMS, network information, video, and more. This software tool is able to retrieve information from more than 500 mobile phone models [Gsm.xry 2008].

*TULP2G*

TULP2G is an open source .NET based forensic software framework for extracting and decoding data stored in electronic devices and SIM cards. This tool uses a cable, Bluetooth, or IrDA connection to acquire data from the mobile phone. To read data from the SIM card, it requires a PC/SC compatible smart card reader. TULP2G uses XML as the data storage format, and provides the ability to create a report on the entire or selected data and import archived case files [Tulp2g 2008].

### 2.5. Scenarios

Earlier in this chapter, distinctive evidence sources were identified as places that will be examined to gather information from mobile phones. In order to create standard test cases usable for a wide variety of models of phones, scenarios were created based on the different sources of evidence. Initially, twelve scenarios were created for testing and evaluating the tools.

#### 2.5.1. Connectivity

The purpose of this scenario was to verify if the software tool was able to connect to the device and recover information from it. User authentication mechanisms such as PIN and password were enabled on the device to check if the software tool was able to connect and retrieve information when user authentication is activated on the device.
Additionally, the three different ways in which the connection can be established were tested (cable, Bluetooth, and IrDA).

2.5.2. Call Logs

The objective of this scenario was to verify whether the software tool was capable of retrieving received, sent, missed, and deleted phone calls. To accomplish this, different call were made from and to the device from different phone numbers. Some of these calls were deleted to verify if the software tool was able to recover deleted information. Finally, the results generated by the software tool were compared with the original information stored on the device to check for accuracy.

2.5.3. SMS/MMS

This scenario was designed to verify whether the tool was able to recover sent, unsent, received, and deleted SMS/MMS messages. For this purpose, SMS/MMS messages were sent to and from the device, some messages were stored in the “Drafts” folder, and some messages were deleted to check whether the software tool was able to retrieve deleted information. Finally, the results generated by the software tool were compared with the original information stored on the device to check for accuracy.

2.5.4. Phonebook

This scenario was planned to verify if the software tool was able to retrieve information from the Phonebook. A variety of entries were created and stored on the phone, and some of these entries were deleted to check if the tool was capable of retrieving deleted items. Some of the items of interest are: phone numbers, names, address information, dates, and binary data (ringtones, pictures). Finally, the results
generated by the software tool were compared with the original information stored on the device to check for accuracy.

2.5.5. Calendar

The purpose of this scenario was to determine if the software tool could retrieve information from the calendar. Reminders, meetings, birthday and anniversary dates, memos, travel and vacation information, and alarms were some of the items of interest. Various items were placed on the device and some were deleted to test if the tool was able to retrieve deleted content. Finally, the results generated by the software tool were compared with the original information stored on the device to check for accuracy.

2.5.6. Graphics

This scenario was intended to verify if the tool can obtain graphics formatted files residing on the device, including deleted files. Downloaded graphics and digital camera pictures were some of the items that this scenario was looking for. Some of the extensions of these files are: .bmp, .jpg, .tif, .gif, .png. To accomplish this, the device was loaded with different types of graphic files, various pictures were taken, and some of these items were deleted to verify if the software tool was able to retrieve deleted information. Finally, the results generated by the software tool were compared with the original information stored on the device to check for accuracy.

2.5.7. Video

The purpose of this scenario was to determine whether the tool could obtain video content from the device, including deleted items. Downloaded videos and digital camera videos were of special interest on this scenario. A few videos were recorded by and
loaded into the device, and some were deleted to test if deleted content could be retrieved by the software tool. Finally, the results generated by the software tool were compared with the original information stored on the device to check for accuracy.

2.5.8. Sounds

This scenario was intended to verify if the tool was able to find and display sounds from the device, including deleted items. Some of these items were: downloaded sounds, ring tones, voice memos, and music (MP3). The device was loaded with several items and some of these items were deleted to check if the software tool can recover deleted information. Finally, the results generated by the software tool were compared with the original information stored on the device to check for accuracy.

2.5.9. Acquisition Consistency

The purpose of this case was to determine whether the software tool was able to generate consistent hash values of files on two back-to-back acquisitions. Hash values over files and hash values over the memory were created for logical and physical acquisitions respectively. File hashes should be consistent, but memory hashes are expected to be inconsistent.

2.5.10. Internet Messaging (only available for some devices)

The objective of this scenario was to determine if the software tool was able to find received and sent Instant Messages (IM) and emails. Both email and IM were sent from and to the device and some of these entries were deleted to check if the tool was able to retrieve deleted content. Finally, the results generated by the software tool were compared with the original information stored on the device to check for accuracy.
2.5.11. Text Files (only available for some devices)

This scenario was designed to determine if the software tool could find and display text files residing on the device. The device was first loaded with different types of files (.txt, .pdf, .doc.), and then some of these files were deleted to verify if the tool was able to recover deleted content. Finally, the results generated by the software tool were compared with the original information stored on the device to check for accuracy.

2.5.12. Web Content (only available for some devices)

The purpose of this scenario was to verify whether the software tool was able to find the websites visited on the device and the content exchanged over the internet. To accomplish this, specific websites were visited and navigated. Some of these data was deleted to check if the tool was able to retrieve deleted content. Finally, the results generated by the software tool were compared with the original information stored on the device to check for accuracy.

2.5.13. Memory Cards (only available for some devices)

The objective of this scenario was to verify if the software tool was able to find and acquire files stored on a peripheral memory card attached to the device. To attempt this, a memory card with a variety of files (text, graphic, archive) was inserted to the device and some of these items were deleted to verify if the tool was able to recover deleted information. Finally, the results generated by the software tool were compared with the original information stored on the device to check for accuracy.
3. RESEARCH

3.1. Target Devices

The first step on this project was to select the target mobile devices. The idea was to select a small but representative set of devices with differences in design, capabilities, operating system, network, and others. To accomplish this, the following set of mobile devices was selected: Motorola L7c, Motorola V3m, Motorola Q, and Blackberry 6510.

3.2. Forensic Software

Secondly, it was necessary to define the software tools that were going to be tested. It is important to remark that the selection of software tools was mainly affected by two factors: the price and the inherent capabilities of the tool. Most of the tools available in the market are commercial and the price ranges between $599 and $9490. The difference in price is mainly because more expensive tools support a greater number of phones and also offer more features to the investigator.

After a careful and dedicated research of all the software available, and considering the budget limitations of the project, the following tools were selected for this project: Paraben’s Device Seizure, Compelson Mobiledit!, and BitPim.

3.2.1. Paraben’s Device Seizure

Paraben Corporation is the leader in the handheld forensic software industry. The initial application available to the public in 2002 was PDA Seizure 1.0. Right after this, Paraben launched the first commercial application for cell phones Cell Seizure. A couple of years later, Paraben combined these two powerful tools and created Device Seizure
which was compatible with cell phones and PDAs. Additionally, Paraben acquired SIMCon and integrated it into Device Seizure so it could also acquire data from SIM cards.

Although Device Seizure is an expensive tool, it was important to have an integrated tool that covered both the device and the SIM card. Moreover, Device Seizure is one of the few tools that perform logical and physical acquisitions. The last version of Device Seizure can acquire and analyze data from over 1950 devices. It costs $1095 and is available to the public. The key features of this tool are:

- Comprehensive easy-to-use interface
- USB and serial support
- Recovers deleted data
- Verification of file integrity with use of MD5 and SHA1 hash values
- Acquires complete GSM SIM card information including deleted data
- Comprehensive HTML & Text reporting
- Encrypted image files to guarantee image integrity
- Text searching in the acquired data
- Export acquired data to PC

Device Seizure is compatible with the following cell phone manufactures: LG, Motorola, Nokia, Siemens, Samsung, Sony-Ericsson, iPhone. A complete list of supported models is available in their website.

3.2.2. Mobiledit!

This forensic tool gives the examiner the ability to perform a logical acquisition of data in a few steps when using the wizard. This tool provides support for 530 phones,
and this number is constantly growing. Some of the most important features of Mobiledit! are:

- Analyze phones via Bluetooth, IrDA, or cable connection
- Direct SIM analyzer through SIM readers.
- Reads deleted messages from the SIM card
- Prints reports ready for courtroom in any language
- Secure and tamper-proof using MD5 hash
- Export reports to Word, Excel, browser, XML
- Frequent updates and upgrades with new features and more phones

Mobiledit! is compatible with the following cell phone manufacturers: Alcatel, Apple, Ericsson, Kyocera, LG, Mivvy, Motorola, Nokia, Panasonic, Philips, Sagem, Samsung, Sharp, Siemens, Sony Ericsson, Ubiquam, ZTC. A complete list of supported models is available in their webpage.

3.2.3. BitPim

BitPim is an open source program that allows the investigator to view and manipulate data on many CDMA phones. Examiners must have the appropriate drivers and cables to establish the connection between BitPim and the device. The most significant features of BitPim are:

- Open source/ Free tool
- Acquires data via cable connection
- Ability to acquire the embedded filesystem
- Runs on Windows, Linux, and Mac
- Gives expert examiners the ability to edit the code to support new phones
BitPim is compatible with the following cell phone manufacturers: Audiovox, Kyocera, LG, Motorola, Nokia, Samsung, Sanyo, Toshiba, Palm. A complete list of supported phone models is available in their webpage.

After the target devices and software tools were selected, the next step was to load the information created in the scenarios described in chapter 2 to start the acquisition of data. When possible, each scenario was replicated on every target device so that useful information was available for the software tool.

Finally, each target device was connected to every software tool (when possible) to perform the data acquisition. The results of this activity are detailed in the following sections:

### 3.3. Acquisition using Paraben’s Device Seizure

Device Seizure version 2.1 was used to perform acquisition of the following cell phones: Motorola V3m, Motorola L7c, Motorola Q, and Blackberry 6510. Before starting the acquisitions, the *Device Seizure Drivers Pack* containing the drivers for the models supported was installed on the forensic station.

#### 3.3.1. Motorola V3m

According to the Supported Model Comparison Chart [Paraben 2008], Device Seizure is able to perform logical acquisition of this model. The following scenarios were conducted on a CDMA Motorola V3m device operated by Verizon Wireless:
Connectivity

The device was connected using a Motorola USB data cable. Device Seizure does not allow Bluetooth nor IrDA connection capabilities. Device Seizure recognized the device and retrieved basic subscriber and service provider information. Figure 3.1 shows the main screen with the acquisition’s results.

![Figure 3.1. Results of the acquisition using Paraben’s Device Seizure](image)

Call Logs

Dialed, received, and missed calls were found in the Call Logs folder. Deleted calls were not found. Figure 3.2 shows the results in the Call Logs folder.
Figure 3.2. Call Logs Folder using Paraben’s Device Seizure

**SMS/MMS**

Read, unread, sent, and unsent SMS messages were found in the SMS History Folder. Deleted messages were not found. The results of the SMS History folder are shown in Figure 3.3.

Figure 3.3. SMS History folder using Paraben’s Device Seizure
Phonebook

The complete address book was reported by the tool. Deleted entries were not recovered since this tool could only perform a logical acquisition.

Calendar

Information stored in the calendar was found in the Calendar folder. Deleted items were not recovered since this tool could only perform a logical acquisition.

Graphics

All graphic files (e.g., .bmp, .jpg, .gif) were found in the File System folder. Deleted entries were not recovered since this tool could only perform a logical acquisition. Figure 3.4 shows the folder structure in which the results are displayed in the left side and a picture within the Picture folder.

![Figure 3.4. Pictures folder using Paraben’s Device Seizure.](image)

Video

All video files were found in the File System folder. Deleted entries were not recovered since this tool could only perform a logical acquisition.
Sound

Ringtones were found and reported. Deleted items were not recovered.

Acquisition Consistency

Two acquisitions on the same phone with the same data produced the same results.

Internet Messaging

Not Available. Internet Messaging is not supported by this phone

Text Files

Not Available. Text files (e.g., .txt, .doc, .pdf) are not supported by this phone.

Web Content

Not Available. Internet connection is not available on this phone.

Memory Cards

This model was not tested using an external memory card.

3.3.2. Motorola L7c

According to their Supported Model Comparison Chart [Paraben 2008], Device Seizure is able to perform logical acquisition of this model. The following scenarios were conducted on a CDMA Motorola L7c device operated by Verizon Wireless:

Connectivity

The device was connected using a Motorola USB data cable. Device Seizure does not allow Bluetooth nor IrDA connection capabilities. Device Seizure recognized the device and retrieved basic subscriber and service provider information.
Call Logs

Dialed, received, and missed calls were found in the Call Logs folder. Deleted calls were not found.

SMS/MMS

Read, unread, sent, and unsent SMS messages were found in the SMS History Folder. Deleted messages were not found.

Phonebook

The complete address book was acquired by the tool. Deleted entries were not recovered since this tool could only perform a logical acquisition.

Calendar

Information stored in the calendar was found in the Calendar folder. Deleted items were not recovered since this tool could only perform a logical acquisition.

Graphics

All graphic files (e.g., .bmp, .jpg, .gif) were found in the File System folder. Deleted entries were not recovered since this tool could only perform a logical acquisition.

Video

All video files were found in the File System folder. Deleted entries were not recovered since this tool could only perform a logical acquisition.

Sound

Ringtones were found and reported. Deleted items were not recovered.
Acquisition Consistency

Two acquisitions on the same phone with the same data produced the same results.

Internet Messaging

Not Available. Internet Messaging is not supported by this phone

Text Files

Not Available. Text files (e.g., .txt, .doc, .pdf) are not supported by this phone.

Web Content

Not Available. Internet connection is not available on this phone.

Memory Cards

This model was not tested using an external memory card.

3.3.3. Motorola Q

According to the Supported Model Chart [Paraben 2008], Device Seizure is able to perform both logical and physical acquisition of this model. The following scenarios were conducted on a CDMA Motorola Q device operated by Verizon Wireless:

Connectivity

The device was connected using a Motorola USB data cable. Device Seizure does not allow Bluetooth nor IrDA connection capabilities. Device Seizure recognized the device and retrieved basic subscriber and service provider information.

Call Logs

Dialed, received, and missed calls were found in the Call Logs folder. Deleted calls were also recovered when performing a physical acquisition.
**SMS/MMS**

Read, unread, sent, and unsent SMS messages were found in the SMS History Folder. Deleted messages were also found when performing a physical acquisition.

**Phonebook**

The complete address book was acquired by the tool. Some deleted entries were also recovered.

**Calendar**

Information stored in the calendar was found in the Calendar folder. Deleted items were also recovered.

**Graphics**

All graphic files (e.g., .bmp, .jpg, .gif) were found in the File System folder. Deleted entries were also recovered when performing a physical acquisition.

**Video**

All video files (.mpg) were found and reported. Deleted items were also recovered by the tool.

**Sound**

All music files (.mp3, .wma) were recovered and reported by the tool. Some deleted items were also reported.

**Acquisition Consistency**

Two acquisitions on the same phone with the same data produced the same results.
Internet Messaging

All messages sent and received using the Internet Messaging option were recovered.

Text Files

All text files were recovered by the tool. Also, deleted items were possible to retrieve with a physical acquisition.

Web Content

Temporary Internet files were recovered. Also, a list of favorite URL was found in the Favorites folder. Folders with cookies and historic data were also found and reported.

Memory Cards

This model was not tested using an external memory card.

3.3.4. Blackberry 6510

According to the Supported Model Comparison Chart [Paraben 2008], Device Seizure is able to perform only a physical acquisition of this model. The following scenarios were conducted on a Blackberry 6510 device.

Connectivity

The device was connected using a Motorola USB data cable. Device Seizure does not allow Bluetooth nor IrDA connection capabilities. Device Seizure recognized the device and retrieved basic subscriber and service provider information.

Call Logs

Dialed, received, and missed calls were found in the Call Logs folder. Deleted calls were also recovered because a physical acquisition was performed.
**SMS/MMS**

Read, unread, sent, unsent and deleted SMS messages were found in the SMS History Folder.

**Phonebook**

The complete address book was acquired by the tool. Deleted entries were not recovered. Additionally, this model has a “Phone Hotlist” and “Quick Contacts” features which were also recovered by the tool.

**Calendar**

Information stored in the calendar was found in the Calendar folder. The information was available both in grid mode and binary mode.

**Graphics**

All graphic files (e.g., .bmp, .jpg, .gif) were found in the Picture subfolder under the Content Store folder.

**Video**

All video files (.mpg) were found and reported. Deleted items were also recovered by the tool.

**Sound**

All music files (.mp3, .wma) and ringtones were recovered and reported by the tool. Some deleted items were also reported.

**Acquisition Consistency**

Two acquisitions on the same phone with the same data produced the same results.
**Internet Messaging**

This feature was not tested on this particular model.

**Text Files**

All text files including deleted entries were recovered by the tool.

**Web Content**

This feature was not tested on this particular model.

**Memory Cards**

This model was not tested using an external memory card.

### 3.4. Acquisition using Mobiledit!

Mobiledit! version 2.99 (Demo) was used to perform the acquisition of the following cell phones: Motorola V3m and Motorola L7c.

#### 3.4.1. Motorola V3m

According to the list of supported models, Mobiledit! is able to perform a logical acquisition of this model. The following scenarios were conducted on a CDMA Motorola V3m device operated by Verizon Wireless:

**Connectivity**

The device was connected using a Motorola USB data cable. Mobiledit! also allows Bluetooth and IrDA connections. Both connections were successfully performed, but for security reasons the data was only acquired using a cable. Figure 3.5 shows the connectivity options with Mobiledit!.
General information about the mobile device and the folders containing the acquired data are displayed in figure 3.6:

**Call Logs**

Dialed, received, and missed calls were found in the Missed, Last Dialed, and Received calls folder. Deleted calls were not found.
**SMS/MMS**

Read, unread, sent, and unsent SMS messages were found in the SMS Folder. Deleted messages were not found. Figure 3.7 shows the Received SMS folder.

![Figure 3.7. Received SMS folder using Mobiledit!](image)

**Phonebook**

The complete address book was acquired by the tool. Deleted entries were not recovered. The results of the Phonebook are shown in figure 3.8:

![Figure 3.8. Phonebook folder using Mobiledit!](image)
Calendar

Information stored in the calendar was found in the Calendar folder. Deleted items were not recovered.

Graphics

All graphic files (e.g., .bmp, .jpg, .gif) were found in the File System folder. Deleted entries were not recovered.

Video

Video files were not found.

Sound

Ringtones nor music files were not found.

Acquisition Consistency

Two acquisitions on the same phone with the same data produced the same results.

Internet Messaging

Not Available. Internet Messaging is not supported by this phone

Text Files

Not Available. Text files (e.g., .txt, .doc, .pdf) are not supported by this phone.

Web Content

Not Available. Internet connection is not available on this phone.

Memory Cards

This model was not tested using an external memory card.
3.4.2. Motorola L7c

According to the list of supported models, Mobiledit! is able to perform a logical acquisition of this model. The following scenarios were conducted on a CDMA Motorola L7c device operated by Verizon Wireless:

Connectivity

The device was connected using a Motorola USB data cable. Mobiledit! also allows Bluetooth and IrDA connections. Both connections were successfully performed, but for security reasons the data was only acquired using a cable.

Call Logs

Dialed, received, and missed calls were found in the Missed, Last Dialed, and Received calls folder. Deleted calls were not found.

SMS/MMS

Read, unread, sent, and unsent SMS messages were found in the SMS Folder. Deleted messages were not found.

Phonebook

The complete address book was acquired by the tool. Deleted entries were not recovered.

Calendar

Information stored in the calendar was found in the Calendar folder. Deleted items were not recovered since this tool could only perform a logical acquisition.

Graphics

All graphic files (e.g., .bmp, .jpg, .gif) were found in the File System folder. Deleted entries were not recovered.
Video

Video files were not found.

Sound

Ringtunes and music files were not found.

Acquisition Consistency

Two acquisitions on the same phone with the same data produced the same results.

Internet Messaging

Not Available. Internet Messaging is not supported by this phone

Text Files

Not Available. Text files (e.g., .txt, .doc, .pdf) are not supported by this phone.

Web Content

Not Available. Internet connection is not available on this phone.

Memory Cards

This model was not tested using an external memory card.

3.5. Acquisition using BitPim

BitPim version 1.0.7 was used to perform acquisition of the following cell phones: Motorola V3m.

3.5.1. Motorola V3m

According to the list of supported models, BitPim is able to perform a logical acquisition of this model. The following scenarios were conducted on a CDMA Motorola V3m device operated by Verizon Wireless:
Connectivity

The device was connected using a Motorola USB data cable. BitPim does not allow Bluetooth nor IrDA connections. Connectivity options are displayed in figure 3.9.

Figure 3.9. Connectivity options using BitPim

BitPim shows general information in the Phone Info Dialog in figure 3.10:

Figure 3.10. Phone Info Dialog using BitPim
Call Logs

Dialed, received, and missed calls were found in the Call Logs folder. Deleted calls were not found.

SMS/MMS

Read, unread, sent, and unsent SMS messages were found in the SMS History Folder. Deleted messages were not found.

Phonebook

The complete address book was acquired by the tool. Deleted entries were not recovered. The results of acquiring the Phonebook are displayed in figure 3.11:

![Figure 3.11. Phonebook folder using BitPim](image)

Calendar

Information stored in the calendar was found in the Calendar folder. Deleted items were not recovered since this tool could only perform a logical acquisition.

Graphics

All graphic files (e.g., .bmp, .jpg, .gif) were found in the File System folder. Deleted entries were not recovered. The Picture folder is shown in figure 3.12:
Figure 3.12. Picture Folder using BitPim

Video

Videos were not found.

Sound

Ringtones and music files were not found.

Acquisition Consistency

Two acquisitions on the same phone with the same data produced the same results.

Internet Messaging

Not Available. Internet Messaging is not supported by this phone.

Text Files

Not Available. Text files (e.g., .txt, .doc, .pdf) are not supported by this phone.

Web Content

Not Available. Internet connection is not available on this phone.
Memory Cards

This model was not tested using an external memory card.

Table 3.1 shows a summary of the results obtained after acquiring data from the target devices using the three software tools previously selected:
<table>
<thead>
<tr>
<th>Device Identifiers</th>
<th>Paraben's Device Seizure</th>
<th>Mobiledit!</th>
<th>BitPim</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer &amp; Model</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Phone Number</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Serial Number</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Firmware</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Battery Level</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Signal Quality</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Connectivity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cable</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Bluetooth</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>IrDA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Call history</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Received calls</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Dialed calls</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Missed calls</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Call Dates &amp; Times</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Deleted calls</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Phonebook</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Actual entries</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Deleted entries</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>SMS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Read/Unred/Sent</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Deleted SMS</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Calendar</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reminders</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Memos</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Alarms</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Graphics</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Downloaded Images</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Pictures</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Video</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Deleted entries</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Sounds</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Downloaded Sounds</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Ring Tones</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Voice Memos</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Music</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Text Files</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internet Messaging</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Content</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIM support</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Reporting Capabilities</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
3.6. Evidence on the SIM Card

The following data was acquired from an AT&T SIM card using Paraben Device Seizure. The following steps were followed to get the data:

First, the type of acquisition was selected; in this case GSM SIM card Logical (Figure 3.13).

![Figure 3.13. Device Type Selection using Paraben’s Device Seizure](image)

Then, the connection type was chosen. A SIM card reader was used for this purpose, so the USB-to-Serial port was selected (see Figure 3.14).
The next step was to select the data to be acquired. All data was selected for this SIM card (see Figure 3.15).

The last step was to verify the selections before the acquisition started (see Figure 3.16).
The results of this acquisition were presented in 7 folders which are shown in figure 3.17:
3.6.1. MF_EF_ELP

In this case the value of ELP EF is 45 4e ff ff ff ff ff ff ff ff. This value indicates that there is only one preferred language because there are only 2 bytes used. The 7-bit default alphabet is used to convert the hex value to the corresponding character. The result of this conversion is [Dreamfabric 2008]:

Byte 1: 45 = E
Byte 2: 4e = N

Now, according to the ISO 639 specification, EN corresponds to English, so English is the preferred language in this phone [ISO639 2008].

3.6.2. MF_EF_ICCID

The Integrated Circuit Card Identifier corresponds to the number printed on the surface of the SIM card. In this case, the value of the EF ICCID is 98 10 14 30 12 51 35 31 35 60. The correct ICCID is obtained when the value of the EF ICCID is reversed: 89 01 41 03 21 15 53 13 53 06.

3.6.3. DF_GSM_EF_IMSI

The IMSI associated with a SIM card can be up to 15 digits long represented by 9 bytes. The IMSI coding is as follows:

Byte 1 of the IMSI represents its length in bytes.
Bits 1-3 of byte 2 are always fixed to 100.
Bit 4 of byte 2 is used for parity of the IMSI.
The first digit of the IMSI is in bits 5-8 of byte 2.
Bytes 3-9 contain digits 2-10 of the IMSI.
According to this, the actual value of the IMSI can be divided in 3 groups:

IMSI: MCC (3) || MNC (2-3) || MSIN (9-10)

The first 3 digits are the Mobile Country Code (MCC), and it is followed by the Mobile Network Code (MNC) which is either 2 or 3 digits. The fourth byte of the AD (Administrative) Elementary File gives the length of the MNC. The remaining digits are the Mobile Station Identification Number (MSIN) within the network’s customer base.

As shown in figure 3.18, the hex IMSI value on this EF is 08 39 01 14 10 55 13 53 03. The first byte 08 represents the length of the IMSI (8 bytes). After reversing bytes 2 to 10, bits 1 to 3 of byte 2 are equal to 100 (9 in decimal). Parity bit 4 of byte 2 is 1. The remainder value is the IMSI 3 10 41 01 55 31 35 30. Rearranging this number according to the specification we obtain:

\[ \text{MCC: 310 (USA)} \]
\[ \text{MNC: 410 (AT&T)} \]
\[ \text{MSIN: 155313530} \]

For a complete list of MCC and MNC see [Wiki 2008d] and [Wiki 2008e].

### 3.6.4. DF\textsubscript{GSM\_EF\_KC}

In this case, the KC EF has the value 76 25 50 9c 89 2b eb c0 04, where bytes 1-8 are the KC key 76 25 50 9c 89 2b eb c0, and 04 is the serial number of the key.
3.6.5. **DF\textsubscript{GSM\_EF\_LOCI}**

This file holds currently location information for the mobile device. The LOCI EF is 11 bytes long, and is coded according to the following specification:

Bytes 1-4: TMSI (Temporary Mobile Subscriber Identity)

Bytes 5-9: LAI (Location Area Information) which can be divided in 2 parts:

- LAI network code: 3 bytes (reverse nibbled)
- LAI area code: 2 bytes

Byte 10: TMSI TimeStamp (not used anymore)

Byte 11: Location update status, when bits 3-1 have the following values:

- 000: updated
- 001: not updated
- 010: forbidden PLMN
- 011: forbidden location area

In this case, the LOCI EF has the following value: 21 cd c5 c5 13 00 14 d6 0f ff 00. According to the previous specification it can be separated into the following:

- 21 cd c5 c5: TMSI
- 13 00 14: LAI network code => 31 00 41 (United States)
- d6 0f: LAI area code
- ff: TMSI timestamp => not used
- 00: Location update status => 000 (updated)

3.6.6. **DF\textsubscript{TELECOM\_EF\_MSISDN}**

The value of the MSISDN (Mobile Subscriber ISDN Number) is the phone number to the SIM card in a mobile device. In this case, the hex value of this Elementary
Folder is 07 81 31 16 78 06 46 F4 (see figure 3.19). The following value is obtained after reversing the original number: 70 18 13 61 87 60 64 4F. The actual mobile phone number is obtained after rearranging this last number: 1-361-876-0644. This number can be broken down in pieces to better understand each component:

**MSISDN: Country Code || Number Planning Area || Subscriber Number**

In this case, the MSISDN has the following values:

- **Country Code:** 1 = USA
- **Number Planning Area:** 361 = Corpus Christi, Texas
- **Subscriber Number:** 876 0644

![Hexadecimal representation of MSISDN](image)

**Figure 3.19. Content of the MSISDN folder of the SIM card in hex**

### 3.6.7. \textit{DF}_{TELECOM\_EF_{ADN}}

In this case, the file containing the Abbreviated Dialing Numbers is divided in 250 slots, and each slot has 32 bytes to store both the name and number. The name has \( n = 18 \) bytes available and the number has the remaining 32-\( n = 14 \) bytes. If the name is shorter than 18 bytes, the remaining bytes are overwritten with hex value FF. Figure 3.20 shows the layout of the ADN Elementary File.
Figure 3.20. Content of the ADN folder of the SIM card in hex

The third slot of this file has the hex value 44 69 61 6e 61 20 45 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff. Using the ASCII table to translate this value we get:

Byte 1 = 44: D

Byte 2 = 69: i

Byte 3 = 61: a

Byte 4 = 6e: n

Byte 5 = 61: a

Byte 6 = 20: space

Byte 7 = 45: E

This is the name of the contact: Diana E. Now there are 11 bytes left with a value of FF, this is because the name (7 bytes) is smaller than the size assigned (18 bytes). The number starts at byte 19 (n+1) and has a length of 14 bytes. In this case, the number has a hex value 06 81 63 81 61 22 89 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff. It is coded according to the following scheme:

Byte 19 = 06: length of the dialing number in bytes (in this case 6 bytes)

Byte 20 = 81: type of dialing number (in this case 81 is unknown type, ISDN dialing number scheme)
Bytes 21-30 = 63 81 61 22 89 ff ff ff ff: This is the actual number. Reversing this value we get: 36 18 16 22 98, which equals to 361-816-2298. The remaining 5 bytes of the slot are filled with hex value FF since they are not used.

Bytes 31-32: These 2 bytes are pointer to supplementary data for this entry in the EFs CCP and EXT1. In this and most cases both bytes have value FF because no pointers are used.

3.6.8. \textbf{DF\textsubscript{TELECOM}_EF\textsubscript{LND}}

Alike the ADN EF, the LND EF has 10 slots each with a size of 32 bytes. In this case this feature is not used because each record is filled with a hex value FF.

3.6.9. \textbf{DF\textsubscript{TELECOM}_EF\textsubscript{SMS}}

Figure 3.21 shows an actual SMS record extracted from an AT&T SIM card. This SMS is broken down in small pieces to better understand each component.

01: Message Status

07: Length of SMSC
91: Type of address

61 63 83 84 08 F6: SMSC number (reverse nibbled)

04: Start of the SMS-Deliver

0B: Length of sender address

81: Type of sender address

21 01 54 74 24 F8: Sender number reverse nibbled

00: Protocol ID

00: Encoding scheme

80 90 90 32 00 43 82: Time stamp (reverse nibbled)

35: SMS message length

ef 7c 19 d4 4e 83 da 61 b2 bc 0c 22 a7 d5 6f 50 bc 5e 06 d3 20 78 bd 4c 2e bb 5d 20
36 3b dc 0e b7 cb a0 71 3d ec 26 bf 41 f0 37 39 3c 07 ff ff ff ff ff ff ff ff ff ff ff
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
ff ff ff ff ff

The description of each byte of the SMS message folder is explained in detail in the following subsections.

Message Status

The value on the SMS is 01 which means that the message was terminated and read.

Length of SMSC

The value on the SMS is 07 which means the length of the SMSC is 7 bytes (including the identifier).
Type of Address

Figure 3.22 shows the layout of the type of address [Pettersson 2008]:

<table>
<thead>
<tr>
<th>Bit no</th>
<th>7</th>
<th>6</th>
<th>5</th>
<th>4</th>
<th>3</th>
<th>2</th>
<th>1</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Always set to 1</td>
<td>Type-of-number</td>
<td>Numbering Plan Identification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

![Figure 3.22. SMS Type of Address Layout](image)

The values of the Type of Number are displayed in Figure 3.23 [Pettersson 2008]:

<table>
<thead>
<tr>
<th>Bits 6 5 4</th>
<th>Meaning of the Type-of-number bits (6, 5 and 4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 0 0</td>
<td>Unknown. This is used when the user or network has no a priori information about the numbering plan. In this case, the Address-Value field is organized according to the network dialling plan, e.g. prefix or escape digits might be present.</td>
</tr>
<tr>
<td>0 0 1</td>
<td>International number.</td>
</tr>
<tr>
<td>0 1 0</td>
<td>National number. Prefix or escape digits shall not be included.</td>
</tr>
<tr>
<td>0 1 1</td>
<td>Network specific number. This is used to indicate administration/service number specific to the serving network, e.g. used to access an operator.</td>
</tr>
<tr>
<td>1 0 0</td>
<td>Subscriber number. This is used when a specific short number representation is stored in one or more SCs as part of a higher layer application. (Note that “Subscriber number” shall only be used in connection with the proper PID referring to this application).</td>
</tr>
<tr>
<td>1 0 1</td>
<td>Alphanumeric, (coded according to GSM TS 03 38 7-bit default alphabet)</td>
</tr>
<tr>
<td>1 1 0</td>
<td>Abbreviated number</td>
</tr>
<tr>
<td>1 1 1</td>
<td>Reserved for extension</td>
</tr>
</tbody>
</table>

![Figure 3.23. Values of the Type of Address](image)

Figure 3.24 shows the values of the Numbering Plan Identification [Pettersson 2008]:

<table>
<thead>
<tr>
<th>Bits 3 2 1 0</th>
<th>Meaning of the Numbering Plan Identification bits (3, 2, 1 and 0)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 0 0</td>
<td>Unknown.</td>
</tr>
<tr>
<td>0 0 1</td>
<td>ISDN/telephone numbering plan (E.164/E.163).</td>
</tr>
<tr>
<td>0 0 1</td>
<td>Data numbering plan (X.121).</td>
</tr>
<tr>
<td>0 1 0</td>
<td>Telex numbering plan</td>
</tr>
<tr>
<td>1 0 0</td>
<td>National numbering plan</td>
</tr>
<tr>
<td>1 0 0</td>
<td>Private numbering plan</td>
</tr>
<tr>
<td>1 0 1</td>
<td>ERMES numbering plan (ETSI DE/PS 3 01-3)</td>
</tr>
<tr>
<td>1 1 1</td>
<td>Reserved for extension</td>
</tr>
</tbody>
</table>

![Figure 3.24. Values of the Numbering Plan Identification](image)
In this case, the type of address has the value 91 = 1 001 0001

The values on the previous figures are used to obtain the following results:

Type of Number: 001 = International Number

Number Plain Identification: 0001 = ISDN/telephone numbering plan

**SMSC number (reverse nibbled)**

The value on the SMS is 61 63 83 84 08 F6. The number obtained after reversing the original value is: 16 36 38 48 80 6F. This number corresponds to 1-636-384-8806.

**Start of the SMS-Deliver**

The layout of the First octet of the SMS-Deliver message is presented in Figure 3.25 [Pettersson 2008]:

<table>
<thead>
<tr>
<th>Bit no</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>TP-RP</td>
</tr>
<tr>
<td>6</td>
<td>TP-UDHI</td>
</tr>
<tr>
<td>5</td>
<td>TP-SRI</td>
</tr>
<tr>
<td>4</td>
<td>(unused)</td>
</tr>
<tr>
<td>3</td>
<td>(unused)</td>
</tr>
<tr>
<td>2</td>
<td>TP-MMS</td>
</tr>
<tr>
<td>1</td>
<td>TP-MTI</td>
</tr>
<tr>
<td>0</td>
<td>TP-MTI</td>
</tr>
</tbody>
</table>

Figure 3.25. Layout of the SMS-deliver message

Where the values of the fields appear in Figure 3.26 [Pettersson 2008]:

<table>
<thead>
<tr>
<th>Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>TP-RP</td>
<td>Reply path. Parameter indicating that reply path exists.</td>
</tr>
<tr>
<td>TP-UDHI</td>
<td>User data header indicator. This bit is set to 1 if the User Data field starts with a header</td>
</tr>
<tr>
<td>TP-SRI</td>
<td>Status report indication. This bit is set to 1 if a status report is going to be returned to the SME</td>
</tr>
<tr>
<td>TP-MMS</td>
<td>More messages to send. This bit is set to 0 if there are more messages to send</td>
</tr>
<tr>
<td>TP-MTI</td>
<td>Message type indicator. Bits no 1 and 0 are both set to 0 to indicate that this PDU is an SMS-DELIVER</td>
</tr>
</tbody>
</table>

Figure 3.26. Values of the fields of the SMS-deliver message

So, in this case the first octet is 04 = 0000 0100. This means that:

TP-RP = 0: Reply path does not exist.

TP-UDHI = 0: User Data field does not start with a header.

TP-SRI = 0: The Status Report will not be returned to the SME.
Bits 4 and 3 are unused.

TP-MMS = 1: Indicates there are not more messages to send.

TP-MTI = 0: Indicates this PDU is an SMS-DELIVER.

TP-MTI = 0: Indicates this PDU is an SMS-DELIVER.

*Length of sender address*

The SMS has a value of 0B in this field, which equals to 11 (in decimal).

*Type of Sender Address*

In this case, the type of address has the value 81 = 1 000 0001

The values on the previous figures are used to obtain the following results:

- Type of Number: 000 = Unknown
- Number Plain Identification: 0001 = ISDN/telephone numbering plan

*Sender number (reverse nibbled)*

The value on the SMS is 21 01 54 74 24 F8. The phone number is obtained after reversing the original number:

12 10 45 47 42 8F, which equals to 1-210-454-7428.

*Protocol ID*

If bits 7 and 6 are 0, then Figure 3.27 shows the values used to define the Protocol ID [Pettersson 2008]:

<table>
<thead>
<tr>
<th>Bit 5</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>no interworking, but SME-to-SME protocol</td>
</tr>
<tr>
<td>1</td>
<td>telematic interworking</td>
</tr>
</tbody>
</table>

Figure 3.27. Values of Bit 5 of the Protocol ID

In this case, the SMS has a value of 00 = 0000 0000. Here the bit 5 = 0 so that means the message is using a SME-SME (Short Message Entity) protocol.
**Encoding scheme**

The following figure shows the values to identify the Encoding Scheme [Pettersson 2008]:

<table>
<thead>
<tr>
<th>Bit 3</th>
<th>Bit 2</th>
<th>Alphabet being used</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>Default alphabet</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>8 bit data</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>UCS2 (16bit)</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>Reserved</td>
</tr>
</tbody>
</table>

Figure 3.28. Values of the Encoding Scheme

In this case, the SMS has a value of 00 = 0000 0000. Looking at the table, it is clear that the bits 2 and 3 are 0, which means that the message is coded using the GSM 7-bit Default alphabet.

**Time stamp (reverse nibbled)**

The layout of the Time Stamp is displayed in Figure 3.29 [Pettersson 2008]:

<table>
<thead>
<tr>
<th>Field</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Year</td>
<td>1</td>
<td>These semi-octets are in &quot;Swapped Nibble&quot; mode</td>
</tr>
<tr>
<td>Month</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Day</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Hour</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Minute</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Second</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Timezone</td>
<td>1</td>
<td>Relation to GMT. One unit is 15min. If MSB=1, value is negative.</td>
</tr>
</tbody>
</table>

Figure 3.29. Layout of the Time Stamp

The Time Stamp value on this SMS is 80 90 90 32 00 43 82. The following number is obtained after reversing this value:

08 09 09 23 00 34 28 which is interpreted as:

08: year = 2008
09: month = September
09: day = 9
23: Hour = 23
00: Minute = 00
34: Second = 34
28: Timezone in quarters = 28/4 = +7 GMT

*SMS Message Length*

In this case, the value of the Message Length is 35. To find out the number of octets, the hex value 35h is converted to its decimal equivalent, which is 53. Then this number is divided by 8 (because there are 8 bits in one byte) and multiplied by 7 (because the GSM 7bit default alphabet was previously defined).

\[
53/8 = 6.625 \\
6.625 \times 7 = 46.375 \text{ or } 47
\]

This is the number of bytes containing the PDU-encoded message. In this case the result is not a multiple of seven, so this number must be rounded to the next multiple of seven to maintain the 7bit encoding scheme. The next multiple of seven is 49 so two extra bytes are added with an FF value (FF is the standard for 7bit encoding scheme). In this example, there are more bytes with FF (00) after the message because it is necessary to fill the rest of the record slot on the SIM, which has a size of 176 bytes.

*Message Data*

The rest of the record contains the actual message data.

```
ef 7c 19 d4 4e 83 da 61 b2 bc 0c 22 a7 d5 6f 50 bc 5e 06 cd d3 20 78 bd 4e 2e bb 5d 20
36 3b dc 0e b7 cb a0 71 3d ec 26 bf 41 f0 37 39 3c 07 ff ff ff ff ff ff ff ff ff ff ff ff ff
```
Encoding a Message Using the 7bit Default Alphabet

In order to show how a message is encoded and decoded, a shorter SMS message was selected as an example: “Soccer Tomorrow At Six.”. The hex value of this message is shown in figure 3.30:

The first grayed bit is the length of the message: 17h. To find out the number of octets, the hex value 17h is converted to its decimal equivalent, which is 23. Then this number is divided by 8 (because there are 8 bits in one byte) and multiplied by 7 (because the GSM 7bit default alphabet was previously defined).

\[
\frac{23}{8} = 2.875
\]

\[
2.875 \times 7 = 20.125
\]

This is the number of bytes containing the PDU-encoded message. In this case the result is not a multiple of seven, so this number must be rounded to the next multiple of seven to maintain the 7 bit encoding scheme. The next multiple of 7 is 21, so the length of the message is 21 octets.
The first thing that must be done is convert each character into its equivalent hex value to find out the binary equivalence. The hex and binary values are shown on table 3.2:

Table 3.2. Hex and Binary values of the SMS “Soccer Tomorrow At Six.”

<table>
<thead>
<tr>
<th>Character</th>
<th>Hex Value</th>
<th>Binary Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>S</td>
<td>53</td>
<td>01010011</td>
</tr>
<tr>
<td>o</td>
<td>6F</td>
<td>01101111</td>
</tr>
<tr>
<td>c</td>
<td>63</td>
<td>01100011</td>
</tr>
<tr>
<td>c</td>
<td>63</td>
<td>01100011</td>
</tr>
<tr>
<td>e</td>
<td>65</td>
<td>01100101</td>
</tr>
<tr>
<td>r</td>
<td>72</td>
<td>01110010</td>
</tr>
<tr>
<td>(space)</td>
<td>20</td>
<td>00100000</td>
</tr>
<tr>
<td>T</td>
<td>54</td>
<td>01010100</td>
</tr>
<tr>
<td>o</td>
<td>6F</td>
<td>01101111</td>
</tr>
<tr>
<td>m</td>
<td>6D</td>
<td>01101101</td>
</tr>
<tr>
<td>o</td>
<td>6F</td>
<td>01101111</td>
</tr>
<tr>
<td>r</td>
<td>72</td>
<td>01110010</td>
</tr>
<tr>
<td>r</td>
<td>72</td>
<td>01110010</td>
</tr>
<tr>
<td>o</td>
<td>6F</td>
<td>01101111</td>
</tr>
<tr>
<td>w</td>
<td>77</td>
<td>01110111</td>
</tr>
<tr>
<td>(space)</td>
<td>20</td>
<td>00100000</td>
</tr>
<tr>
<td>A</td>
<td>41</td>
<td>01000001</td>
</tr>
<tr>
<td>t</td>
<td>74</td>
<td>01110100</td>
</tr>
<tr>
<td>(space)</td>
<td>20</td>
<td>00100000</td>
</tr>
<tr>
<td>S</td>
<td>53</td>
<td>01010011</td>
</tr>
<tr>
<td>i</td>
<td>69</td>
<td>01101001</td>
</tr>
<tr>
<td>x</td>
<td>78</td>
<td>01111000</td>
</tr>
<tr>
<td>.</td>
<td>2E</td>
<td>00101110</td>
</tr>
<tr>
<td>null</td>
<td>00</td>
<td>00000000</td>
</tr>
</tbody>
</table>

The next step is to convert the 8-bit message into a 7-bit message (this is the encoding scheme used in this and most SMS messages). The first step of the conversion is to take the most significant bit of each octet and discard it. This operation is shown in table 3.3:
Table 3.3. Converting the 8-bit message into a 7-bit message

<table>
<thead>
<tr>
<th>Character</th>
<th>Binary Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>S</td>
<td>1010011</td>
</tr>
<tr>
<td>o</td>
<td>1101111</td>
</tr>
<tr>
<td>c</td>
<td>1100011</td>
</tr>
<tr>
<td>c</td>
<td>1100011</td>
</tr>
<tr>
<td>e</td>
<td>1100101</td>
</tr>
<tr>
<td>r</td>
<td>1110010</td>
</tr>
<tr>
<td>(space)</td>
<td>0100000</td>
</tr>
<tr>
<td>T</td>
<td>1010100</td>
</tr>
<tr>
<td>o</td>
<td>1101111</td>
</tr>
<tr>
<td>m</td>
<td>1101101</td>
</tr>
<tr>
<td>o</td>
<td>1101111</td>
</tr>
<tr>
<td>r</td>
<td>1110010</td>
</tr>
<tr>
<td>r</td>
<td>1110010</td>
</tr>
<tr>
<td>o</td>
<td>1101111</td>
</tr>
<tr>
<td>w</td>
<td>1110111</td>
</tr>
<tr>
<td>(space)</td>
<td>0100000</td>
</tr>
<tr>
<td>A</td>
<td>1000001</td>
</tr>
<tr>
<td>t</td>
<td>1110100</td>
</tr>
<tr>
<td>(space)</td>
<td>0100000</td>
</tr>
<tr>
<td>S</td>
<td>1010011</td>
</tr>
<tr>
<td>i</td>
<td>1101001</td>
</tr>
<tr>
<td>x</td>
<td>1111000</td>
</tr>
<tr>
<td>.</td>
<td>0101110</td>
</tr>
<tr>
<td>null</td>
<td>0000000</td>
</tr>
</tbody>
</table>

Now these septets need to be transformed into octets. To accomplish this, the rightmost bit of the second septet (1) is added at the beginning of the first septet so that it completes the 8 bits: 1+1010011 = 11010011. Now, the second septet needs 2 bits to make an 8 bit octet. These 2 bits are taken from the third octet: 11+110111 = 11110111. This process continues until no more septets are found and each septet is converted into an octet. Table 3.4 shows this process (bits bolded are moved to the most significant position of the previous octet):
Table 3.4. Converting the septets into octets

<table>
<thead>
<tr>
<th>Character</th>
<th>Septet</th>
<th>Octet</th>
</tr>
</thead>
<tbody>
<tr>
<td>S</td>
<td>1010011</td>
<td>1+1010011=11010011</td>
</tr>
<tr>
<td>o</td>
<td>1101111</td>
<td>11+110111=11110111</td>
</tr>
<tr>
<td>c</td>
<td>1100011</td>
<td>011+11000=01111000</td>
</tr>
<tr>
<td>e</td>
<td>1100011</td>
<td>0101+1100=01011100</td>
</tr>
<tr>
<td>r</td>
<td>1110010</td>
<td>100000+11=10000011</td>
</tr>
<tr>
<td>(space)</td>
<td>0100000</td>
<td>1010100+0=10101000</td>
</tr>
<tr>
<td>T</td>
<td>1010100</td>
<td>Removed</td>
</tr>
<tr>
<td>o</td>
<td>1101111</td>
<td>1+110111=1110111</td>
</tr>
<tr>
<td>m</td>
<td>1101101</td>
<td>11+110110=11110110</td>
</tr>
<tr>
<td>o</td>
<td>1101111</td>
<td>010+11011=0101101</td>
</tr>
<tr>
<td>r</td>
<td>1110010</td>
<td>0010+1100=00101110</td>
</tr>
<tr>
<td>r</td>
<td>1110010</td>
<td>01111+111=0111111</td>
</tr>
<tr>
<td>o</td>
<td>1101111</td>
<td>110111+11=1101111</td>
</tr>
<tr>
<td>w</td>
<td>1101011</td>
<td>0100000+1=01000001</td>
</tr>
<tr>
<td>(space)</td>
<td>0100000</td>
<td>Removed</td>
</tr>
<tr>
<td>A</td>
<td>1000001</td>
<td>0+1000001=0100001</td>
</tr>
<tr>
<td>t</td>
<td>1101000</td>
<td>00+11010=0011111</td>
</tr>
<tr>
<td>(space)</td>
<td>0100000</td>
<td>011+01000=0110100</td>
</tr>
<tr>
<td>S</td>
<td>1010011</td>
<td>1001+1010=10011010</td>
</tr>
<tr>
<td>i</td>
<td>1101001</td>
<td>11000+110=11000010</td>
</tr>
<tr>
<td>x</td>
<td>1111000</td>
<td>101110+11=10111011</td>
</tr>
<tr>
<td>.</td>
<td>0101110</td>
<td>0000000+0=0000000</td>
</tr>
<tr>
<td>null</td>
<td>0000000</td>
<td>Removed</td>
</tr>
</tbody>
</table>

Finally, the binary value of each octet is converted into its hex equivalent. This is shown on table 3.5:
Table 3.5. Converting the binary values into hex

<table>
<thead>
<tr>
<th>Character</th>
<th>Octet</th>
<th>Hex Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>S</td>
<td>1+1010011=11101011</td>
<td>D3</td>
</tr>
<tr>
<td>o</td>
<td>11+110111=11110111</td>
<td>F7</td>
</tr>
<tr>
<td>e</td>
<td>011+11000=01111000</td>
<td>78</td>
</tr>
<tr>
<td>c</td>
<td>0101+1100=01011100</td>
<td>5C</td>
</tr>
<tr>
<td>e</td>
<td>10010+110=10010110</td>
<td>96</td>
</tr>
<tr>
<td>r</td>
<td>100000+11=10000111</td>
<td>83</td>
</tr>
<tr>
<td>(space)</td>
<td>1010100+0=10101000</td>
<td>A8</td>
</tr>
<tr>
<td>T</td>
<td>Removed</td>
<td></td>
</tr>
<tr>
<td>o</td>
<td>1+1101111=11101111</td>
<td>EF</td>
</tr>
<tr>
<td>m</td>
<td>11+110110=11110110</td>
<td>F6</td>
</tr>
<tr>
<td>o</td>
<td>010+11011=01011101</td>
<td>5B</td>
</tr>
<tr>
<td>r</td>
<td>0010+1110=00110010</td>
<td>2E</td>
</tr>
<tr>
<td>r</td>
<td>01111+111=01111111</td>
<td>7F</td>
</tr>
<tr>
<td>o</td>
<td>110111+11=11011111</td>
<td>DF</td>
</tr>
<tr>
<td>w</td>
<td>0100000+1=0100001</td>
<td>41</td>
</tr>
<tr>
<td>(space)</td>
<td>Removed</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>0+1000001=0100001</td>
<td>41</td>
</tr>
<tr>
<td>t</td>
<td>00+111010=00110110</td>
<td>3A</td>
</tr>
<tr>
<td>(space)</td>
<td>011+01000=01101000</td>
<td>68</td>
</tr>
<tr>
<td>S</td>
<td>1001+1010=10011010</td>
<td>9A</td>
</tr>
<tr>
<td>i</td>
<td>11000+110=11000110</td>
<td>C6</td>
</tr>
<tr>
<td>x</td>
<td>101110+11=10111011</td>
<td>BB</td>
</tr>
<tr>
<td>.</td>
<td>0000000+0=00000000</td>
<td>00</td>
</tr>
<tr>
<td>null</td>
<td>Removed</td>
<td></td>
</tr>
</tbody>
</table>

Now these results can be compared to the original value on the SMS message to check that they match.

*Decoding a Message Using the 7bit Default Alphabet*

The first step to decode a message is to convert the hexadecimal values into their binary equivalents. Table 3.6 shows the hex and binary values:
Table 3.6. Hex and Binary values of the SMS “Soccer Tomorrow At Six.”

<table>
<thead>
<tr>
<th>Hex Value</th>
<th>Binary Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>null</td>
<td>00 0000000</td>
</tr>
<tr>
<td>BB</td>
<td>10111011</td>
</tr>
<tr>
<td>C6</td>
<td>11000110</td>
</tr>
<tr>
<td>9A</td>
<td>10011010</td>
</tr>
<tr>
<td>68</td>
<td>01101000</td>
</tr>
<tr>
<td>3A</td>
<td>00111010</td>
</tr>
<tr>
<td>41</td>
<td>01000001</td>
</tr>
<tr>
<td>null</td>
<td>01000001</td>
</tr>
<tr>
<td>DF</td>
<td>11011111</td>
</tr>
<tr>
<td>7F</td>
<td>01111111</td>
</tr>
<tr>
<td>2E</td>
<td>00101110</td>
</tr>
<tr>
<td>5B</td>
<td>01011011</td>
</tr>
<tr>
<td>F6</td>
<td>11101110</td>
</tr>
<tr>
<td>EF</td>
<td>11101111</td>
</tr>
<tr>
<td>null</td>
<td>11101111</td>
</tr>
<tr>
<td>A8</td>
<td>10101000</td>
</tr>
<tr>
<td>83</td>
<td>10000011</td>
</tr>
<tr>
<td>96</td>
<td>10010110</td>
</tr>
<tr>
<td>5C</td>
<td>01011100</td>
</tr>
<tr>
<td>78</td>
<td>01111000</td>
</tr>
<tr>
<td>F7</td>
<td>11101111</td>
</tr>
<tr>
<td>D3</td>
<td>11010011</td>
</tr>
</tbody>
</table>

Then, the reverse operation needs to be performed. It starts by converting these octets into septets. To do this, the seven most significant bits of the last octet (0000000) and place them into a new septet located after the last octet. Now, the next septet needs to be created. The six most significant bits of the next octet (101110) are taken and placed as the least significant bits of the next septet: 0+101110 = 0101110. This process continues until no new octets are found and every octet is converted into a septet. Table 3.7 shows the complete process. Note that the hex values are sorted in reverse order (bits bolded are moved to the least significant position of the previous septet):
Table 3.7. Converting the octets into septets

<table>
<thead>
<tr>
<th>Hex Value</th>
<th>Octet</th>
<th>Septet</th>
</tr>
</thead>
<tbody>
<tr>
<td>null</td>
<td>null</td>
<td>null+0000000=0000000</td>
</tr>
<tr>
<td>00</td>
<td>00000000</td>
<td>0+101110=0101110</td>
</tr>
<tr>
<td>BB</td>
<td>10111011</td>
<td>11+11000=1111000</td>
</tr>
<tr>
<td>C6</td>
<td>11000110</td>
<td>110+1001=1110101</td>
</tr>
<tr>
<td>9A</td>
<td>10011010</td>
<td>1010+011=1010011</td>
</tr>
<tr>
<td>68</td>
<td>01101000</td>
<td>010000+0=0100000</td>
</tr>
<tr>
<td>3A</td>
<td>00111010</td>
<td>111010+0=1110100</td>
</tr>
<tr>
<td>41</td>
<td>01000001</td>
<td>1000001+null=1000001</td>
</tr>
<tr>
<td>null</td>
<td>null</td>
<td>null+0100000=0100000</td>
</tr>
<tr>
<td>41</td>
<td>01000001</td>
<td>1+110111=1110111</td>
</tr>
<tr>
<td>DF</td>
<td>11011111</td>
<td>11+01111=1101111</td>
</tr>
<tr>
<td>7F</td>
<td>01111111</td>
<td>111+0010=1110010</td>
</tr>
<tr>
<td>2E</td>
<td>00101110</td>
<td>1110+010=1110010</td>
</tr>
<tr>
<td>5B</td>
<td>01011011</td>
<td>11011+11=1101111</td>
</tr>
<tr>
<td>F6</td>
<td>11110110</td>
<td>110110+1=1101101</td>
</tr>
<tr>
<td>EF</td>
<td>11101111</td>
<td>1101111+null=1101111</td>
</tr>
<tr>
<td>null</td>
<td>null</td>
<td>null+1010100=1010100</td>
</tr>
<tr>
<td>A8</td>
<td>10101000</td>
<td>0+100000=0100000</td>
</tr>
<tr>
<td>83</td>
<td>10000011</td>
<td>11+10010=1110010</td>
</tr>
<tr>
<td>96</td>
<td>10010110</td>
<td>110+011=1100101</td>
</tr>
<tr>
<td>5C</td>
<td>01011100</td>
<td>1100+011=1100011</td>
</tr>
<tr>
<td>78</td>
<td>01111000</td>
<td>11000+11=1100011</td>
</tr>
<tr>
<td>F7</td>
<td>11110111</td>
<td>110111+1=1101111</td>
</tr>
<tr>
<td>D3</td>
<td>11010011</td>
<td>1010011+null=1010011</td>
</tr>
</tbody>
</table>

The next step is to add the bit that was removed at the beginning of the encoding operation (which is 0) to convert the septets into octets and get the original message. This bit is placed at the beginning of each septet as is shown on table 3.8:
<table>
<thead>
<tr>
<th>Hex Value</th>
<th>Septet</th>
<th>Octet</th>
</tr>
</thead>
<tbody>
<tr>
<td>null</td>
<td>0000000</td>
<td>00000000</td>
</tr>
<tr>
<td>00</td>
<td>0101110</td>
<td>00101110</td>
</tr>
<tr>
<td>BB</td>
<td>1111000</td>
<td>01111000</td>
</tr>
<tr>
<td>C6</td>
<td>1101001</td>
<td>01101001</td>
</tr>
<tr>
<td>9A</td>
<td>1010011</td>
<td>01010011</td>
</tr>
<tr>
<td>68</td>
<td>0100000</td>
<td>00100000</td>
</tr>
<tr>
<td>3A</td>
<td>1110100</td>
<td>01110100</td>
</tr>
<tr>
<td>41</td>
<td>1000001</td>
<td>01000001</td>
</tr>
<tr>
<td>null</td>
<td>0100000</td>
<td>00100000</td>
</tr>
<tr>
<td>41</td>
<td>1110111</td>
<td>01110111</td>
</tr>
<tr>
<td>DF</td>
<td>1101111</td>
<td>01101111</td>
</tr>
<tr>
<td>7F</td>
<td>1110010</td>
<td>01110010</td>
</tr>
<tr>
<td>2E</td>
<td>1110001</td>
<td>01110010</td>
</tr>
<tr>
<td>5B</td>
<td>1101111</td>
<td>01101111</td>
</tr>
<tr>
<td>F6</td>
<td>1101101</td>
<td>01101101</td>
</tr>
<tr>
<td>EF</td>
<td>1101111</td>
<td>01101111</td>
</tr>
<tr>
<td>null</td>
<td>1010100</td>
<td>01010100</td>
</tr>
<tr>
<td>A8</td>
<td>0100000</td>
<td>00100000</td>
</tr>
<tr>
<td>83</td>
<td>1110010</td>
<td>01110010</td>
</tr>
<tr>
<td>96</td>
<td>1100101</td>
<td>01100101</td>
</tr>
<tr>
<td>5C</td>
<td>1100011</td>
<td>01100011</td>
</tr>
<tr>
<td>78</td>
<td>1100011</td>
<td>01100011</td>
</tr>
<tr>
<td>F7</td>
<td>1101111</td>
<td>01101111</td>
</tr>
<tr>
<td>D3</td>
<td>1010011</td>
<td>01010011</td>
</tr>
</tbody>
</table>

The last step is to convert these binary values into their hex equivalents and then get the ASCII values. After doing this, the original un-encoded message is recovered. Table 3.9 shows these conversions and the original message in reverse order:
Table 3.9. Converting the binary values into their hex and ASCII equivalents

<table>
<thead>
<tr>
<th>Hex Value</th>
<th>Octet</th>
<th>Hex Value</th>
<th>Character</th>
</tr>
</thead>
<tbody>
<tr>
<td>null</td>
<td>00000000</td>
<td>0</td>
<td>null</td>
</tr>
<tr>
<td>00</td>
<td>00101110</td>
<td>2E</td>
<td>.</td>
</tr>
<tr>
<td>BB</td>
<td>01111000</td>
<td>78</td>
<td>x</td>
</tr>
<tr>
<td>C6</td>
<td>01101001</td>
<td>69</td>
<td>i</td>
</tr>
<tr>
<td>9A</td>
<td>01010011</td>
<td>53</td>
<td>S</td>
</tr>
<tr>
<td>68</td>
<td>00100000</td>
<td>20</td>
<td>(space)</td>
</tr>
<tr>
<td>3A</td>
<td>01110100</td>
<td>74</td>
<td>t</td>
</tr>
<tr>
<td>41</td>
<td>01000001</td>
<td>41</td>
<td>A</td>
</tr>
<tr>
<td>null</td>
<td>00100000</td>
<td>20</td>
<td>(space)</td>
</tr>
<tr>
<td>41</td>
<td>01110111</td>
<td>77</td>
<td>w</td>
</tr>
<tr>
<td>DF</td>
<td>01101111</td>
<td>6F</td>
<td>o</td>
</tr>
<tr>
<td>7F</td>
<td>01110010</td>
<td>72</td>
<td>r</td>
</tr>
<tr>
<td>2E</td>
<td>01110010</td>
<td>72</td>
<td>r</td>
</tr>
<tr>
<td>5B</td>
<td>01101111</td>
<td>6F</td>
<td>o</td>
</tr>
<tr>
<td>F6</td>
<td>01101101</td>
<td>6D</td>
<td>m</td>
</tr>
<tr>
<td>EF</td>
<td>01101111</td>
<td>6F</td>
<td>o</td>
</tr>
<tr>
<td>null</td>
<td>01010100</td>
<td>54</td>
<td>T</td>
</tr>
<tr>
<td>A8</td>
<td>00100000</td>
<td>20</td>
<td>(space)</td>
</tr>
<tr>
<td>83</td>
<td>01110010</td>
<td>72</td>
<td>r</td>
</tr>
<tr>
<td>96</td>
<td>01100101</td>
<td>65</td>
<td>e</td>
</tr>
<tr>
<td>5C</td>
<td>01100011</td>
<td>63</td>
<td>c</td>
</tr>
<tr>
<td>78</td>
<td>01100011</td>
<td>63</td>
<td>c</td>
</tr>
<tr>
<td>F7</td>
<td>01101111</td>
<td>6F</td>
<td>o</td>
</tr>
<tr>
<td>D3</td>
<td>01010011</td>
<td>53</td>
<td>S</td>
</tr>
</tbody>
</table>
4. EVALUATION AND RESULTS

After acquiring, examining, and reporting information from mobile phones using the software tools, testing techniques need to be implemented to understand and measure the capabilities of each tool. There is a set of common requirements that should be satisfied by any software tool. The following general criteria have been proposed by Carrier in the publication “Digital Forensic Examination and Analysis Tools” as a basic set of requirements that should be considered when selecting a forensic tool [Carrier 2002]:

- **Usability**: the ability for the tool to present data in such a manner that is useful to the investigator.
- **Comprehensive**: the ability for the tool to present all data to the investigator so that inculpatory and exculpatory evidence can be identified.
- **Accuracy**: the ability for the tool to ensure that the output data is accurate and a margin of error is calculated so that the results can be interpreted appropriately.
- **Deterministic**: the ability for the tool to always produce the same output when given the same rule set and input.
- **Verifiable**: the ability for the tool to give the investigator access to the inputs and outputs so that the results can be verified.

In addition, the publication “Guidelines on Cell Phone Forensics” proposes other factors that should be taken into account when choosing among software tools [Ayers 2007a]:

- **Quality**: technical support, reliability, and upgrade version path of the tool.
- **Capability**: performance, supported feature set, and richness of features with regard to flexibility and customization.
• **Affordability**: relationship between cost and benefits.

These requirements were measured on each tool to decide whether the tool met the predefined expectations or not. Each scenario was intended to evaluate specific features and/or functionality of the device related to satisfy these requirements. The following subsections describe each requirement for every tool. A qualification was given based on how well the software tool met the requirement. The punctuation ranges from zero to five where zero means “deficient” and five means “outstanding”.

4.1. **Paraben’s Device Seizure**

After the acquisition on several mobile devices, the qualifications given to Paraben’s Device Seizure are explained in the following subsections.

4.1.1. **Usability**

This tool has a comprehensive easy-to-use user interface. The acquisition process is simple when using the wizard. Once the data has been acquired, results are shown in a format that is easy to understand. Additionally, the user has general information about the phone in the “Properties” window which is always available when clicking over the device.

4.1.2. **Comprehensive**

The amount of information presented by this tool really depends on the device being analyzed. In this project, several mobile phones were analyzed and the results were variable. In most cases, a physical and logical acquisition retrieved all the information available on the phone. However, the tool was not able to perform physical acquisitions of some devices and deleted items were not recovered in these cases. In both cases the
results were reported in such a manner that it was easy to identify and interpret the evidence.

4.1.3. Deterministic

One interesting and useful feature available in this tool is the “Validate Hash Codes” function. The integrity of a file can be validated at any time with this feature. To accomplish this, the tool uses two well known hash functions: MD5 and SHA1. The tool generates these two hash value for each case and each binary code. At any time, the investigator can compare two hash values to verify the data.

4.1.4. Verifiable

In most acquisitions, all data present on the mobile device was acquired and clearly displayed in the corresponding folders to make verification possible. However, there were a few cases where it was not possible to acquire data because that specific feature was not supported by the tool.

4.1.5. Quality

Paraben offers customer service and support for technical issues via web. The user can create a “ticket” and communicate with technical staff via web. On the other hand, upgrades are available for free for one year after the purchase of the software. The upgrades include support for new models when released by the company.

4.1.6. Capability

The tool was capable of acquiring the most relevant data in a forensic investigation. Call logs, SMS messages, address book, calendar, pictures, videos,
documents, are some of the most important items that the tool was able to acquire. The tool was also able to acquire the content of GSM SIM cards. Deleted data was also recovered by the tool for both the device and the SIM card when physical acquisition was available. Additionally, Device Seizure offers text searching options for the acquired data and the ability to compare two cases to find differences. Finally, all the information related to the case was documented using the “Generate Report” feature.

4.1.7. Affordability

The tool costs $1,095 and compared to most of the tools available, it has a good cost-benefit relationship. Moreover, Device Seizure is recognized by forensic specialists as the leader company in handheld digital forensics.

4.2. BitPim

After the acquisition on several mobile devices, the qualifications given to BitPim are explained in the following subsections.

4.2.1. Usability

BitPim has a comprehensive user interface that shows the acquired data in logical folders. One problem with BitPim is that the user needs to find and install the drivers for each device that is going to be analyzed. However, once the device is successfully connected and drivers are installed, the acquisition process is pretty straightforward. The program gives the option to select one or more items for the acquisition.
4.2.2. Comprehensive

Data is presented in folders and subfolders predefined by the tool. Alike other forensic software, the amount of data acquired depends on the device. BitPim is capable of performing a logical acquisition of the device to recover standard data (Phonebook, call logs, text messages, calendar, images, and so on) and it can also perform a logical dump of the filesystem to recover deleted items (phonebook entries, SMS, call logs, and so on).

4.2.3. Deterministic

BitPim has no built-in functionality that allows the investigator to validate the acquired data. The integrity of files cannot be verified with this tool.

4.2.4. Verifiable

Results are presented in folders where the investigator can compare the acquired data with the original data. In some cases the tool was not able to acquire part of the information available on the device and verification was not possible.

4.2.5. Quality

Since BitPim is a free tool, there is really no “customer service”. However, the program has a “Help” tab where instructions are given for the most important tasks. Additionally, the website periodically uploads new releases of the tool so that users can upgrade their version to get new features and support for new devices. The problem is that there is no “patch” available; the software needs to be re-installed every time the user wants to get the latest version.
4.2.6. Capability

The last version of BitPim can acquire information mainly from CDMA devices but the number of devices supported by this tool is shorter compared to commercial tools. In any case, BitPim was able to acquire basic data from most supported devices (phonebook, SMS, calendar, call history, images, sounds, to do list, and so on). In most cases, a logical dump of the filesystem recovered deleted data, but there were a few cases where the tool was not able to acquire the filesystem. BitPim has some disadvantages: it does not provide search functionality and it does not support reporting capabilities.

4.2.7. Affordability

Because BitPim is an open source software tool, it does not hurt to have it as part of the forensic toolkit. Anything obtained by the tool will be at no cost. Additionally, the investigator must consider that it is always better to perform the acquisition with as many tools as possible to compare the results and obtain the most information.

4.3. Mobiledit!

After the acquisition on several mobile devices, the qualifications given to Mobiledit! are explained in the following subsections.

4.3.1. Usability

This tool has an easy-to-use graphic interface that allows the user to acquire data on the mobile. The connection between the device and the software can be establish either manually or using the wizard. Three types of connections are available with this tool: IrDA, Bluetooth, and cable. Mobiledit! gives the user the option to select the items that will be acquired.
4.3.2. Comprehensive

Mobiledit! is only able to perform logical acquisitions on mobile devices. Alike with most tools, the information recovered by this tool depends on the device being analyzed. The resulting information was presented in a format were key evidence was easily identified and reported.

4.3.3. Deterministic

This tool has no feature that can be used to validate the acquired data.

4.3.4. Verifiable

In most cases, all the information acquired with this tool was immediately displayed. There were a few cases where the tool did not provide support for that specific model or that some specific feature was not supported for that particular model.

4.3.5. Quality

Mobiledit! does not provide direct support to the customer. However, they have a forum to post comments or questions and other users can provide feedback or instructions based on their previous experience.

4.3.6. Capability

Mobiledit! provides support mainly for CDMA and GSM devices. The tool was able to acquire the following information: call logs, SMS messages, phonebook, calendar, and the filesystem (pictures, video, and music). It was also capable of acquiring data directly from the SIM card using a SIM card reader. Deleted SMS messages where
recovered from the SIM card. Also, the tool was able to create different types of reports to show the information (word, excel, browser, XML/XSL).

4.3.7. Affordability

The price for the latest version of this tool is $599. The price includes a 12-month of free phone support updates. Mobiledit! is one of the cheapest commercial tools available and is widely used by investigators all over the world.
5. FUTURE WORK

Mobile phone forensics is an area that has gained a lot of attention in the last years. However, mobile phone forensics still lags behind computer forensics. In computer forensics there are standards clearly defined for conducting an investigation that have been used for many years. Additionally, software tools for computer forensics have been thoroughly tested and evaluated for several years so that a lot of information about them is available for investigators. This is not the case in mobile phone forensics. There are no standards procedures; there are just proposed guidelines that can be used for a mobile forensic investigation. Also, software tools for mobile phone forensics available in the market are relatively new and they have not been fully tested and evaluated. This situation hinders the work of the investigator because he/she needs to individually analyze and test each tool in order to decide which one is best for a specific situation.

Mobile devices will continue evolving in the following years. One of the areas in which GSM mobile phones will have a tremendous impact is the SIM card. Nowadays, about 70% of the world mobile subscribers use GMS technology in 168 countries, and this percentage will increase in the upcoming years. The main reason for this growth is that GSM systems will incorporate multimedia features to the SIM card. In the future, SIM cards will have multimedia phonebook, advanced SMS capabilities, pictures, movies, music, ring tones, and more. These new features will revolutionize the field of mobile forensics because new software tools will be needed to acquire this information from SIM cards. The filesystem of the SIM card will need to change to store the new information generated by the new features. These files will need to be thoroughly examined so that software tools can include them in their acquisition.
On the other hand, with the appearance of 4G systems, mobile devices have started to implement advanced features so that they can be used for banking transactions, online payments, video conference, and more upcoming features. Once these new features become available for common use, mobile devices will generate and store a lot more information and become a key component of forensic investigations. In addition, since mobile devices will manage such important information, they will quickly become an attractive target for criminals. These advanced features will need to be considered by mobile forensic software in the nearest years.
6. CONCLUSION

Cell phone forensics is a relatively new field within digital forensics. In the last decade, cell phone forensics has gained a lot of attention and it is now very common to find cell phones in a crime scene. For this reason, law enforcement personnel realized it was necessary to develop particular procedures when dealing with evidence in mobile devices. In addition, forensic software designed for computers was not able to acquire information from these devices so forensic software tools specifically designed for cell phones started to emerge in the last years to meet these requirements. Nowadays, information obtained from cell phones using the different software tools is widely used as evidence to incriminate or exculpate a suspect. However, as any emerging field, cell phone forensics has many challenges to face and shortcomings to solve.

When acquiring digital evidence from mobile phones, one of the most important decisions is the selection of the correct tool for the investigation. This emphasizes the importance of the study of forensic software tools in the field of mobile phones. There are many tools available, each with its own characteristics, strengths and limitations. However, since most of the tools are relatively new, a big problem is that they have been barely tested. In addition, there are only few publications that analyze some of the tools and test them with a limited number of mobile phones. During this project, some of the most respectable forensic tools were described and analyzed with different cell phones to determine their capabilities and impediments.

There are four places where evidence can be found when dealing with a cell phone forensic investigation: the phone’s embedded memory, the SIM card (if present), the phone’s removable memory (if present), and the service provider. The phone’s
embedded memory holds general information such as phonebook, call logs, SMS messages, calendar information, to do list, alarms, ringtones, and in some cases, pictures, graphics, videos, and music. The SIM card stores information related to the subscriber such as the phone number, IMSI, ICCID, MSISDN, and some general information such as basic phonebook, last dialed numbers, abbreviated numbers, location information, language preferences, SMS messages and others. The phone’s removable memory stores all media files such as pictures, graphics, videos, music, and other types of files like text documents and others. The service provider holds information about the subscriber like subscriber’s name and address, billing information, call logs, PIN/PUK codes (if phone uses the GSM system), services available on the phone, and more.

Along this project, these four main areas where discussed in detail and methods to obtain the information where explained. Forensic software tools were used to acquire information from the phone’s embedded memory, the SIM card, and the phone’s removable memory. Additionally, when acquiring data from the SIM card, the results obtained from the forensic software had to be analyzed and converted from hexadecimal to their decimal equivalents in order to get the results in an understandable format. Finally, the information held by the service provider needs to be obtained following all the legal steps which can involve a subpoena, a search warrant, and/or any other legal document required by the authorities.

Three different software tools were used in this project: the commercial version of Paraben’s Device Seizure, the demo version of Compelson Mobiledit!, and the open source tool BitPim. A representative set of mobile phones (basic, advanced, and smart devices) from diverse manufacturers and with varied characteristics was also selected as
the target devices for the project. Data from each target device was acquired using every software tool when possible.

In general, Device Seizure was able to acquire more data than Mobiledit! and BitPim. Device Seizure and Mobiledit! provided support for both CDMA and GSM devices. BitPim only supported a few CDMA devices. Device Seizure was the only tool capable of performing a physical acquisition in which deleted items were recovered. Mobiledit! and BitPim could only perform logical acquisitions. Device Seizure and BitPim could only establish a connection using a cable, and Mobiledit! additionally allowed Bluetooth and IrDA connections. However, these last two types of connection are not recommended for forensic use. Mobiledit! and Device Seizure provided reporting capabilities in which the results were exported to different types of files. BitPim did not have a reporting feature.

When dealing with evidence on devices operating under GSM networks, Device Seizure and Mobiledit! were the tools able to acquire data from the SIM card. BitPim did not provide support for SIM cards. The first two software tools were able to acquire relevant data stored in the file system such as the Master File, Data Files, and Elementary Files. SMS messages including deleted entries were also recovered by both tools. Finally, both Device Seizure and Mobiledit! provided reporting capabilities in different formats.

The results were compared to identify the strengths and limitation of each software tool and determine which tool works better in which situation. The results were individually grouped by tool and device based on the scenarios previously defined in the project. Finally, each tool was evaluated and a qualification was given for each of the basic requirements identified and explained in the “Evaluation and Results” section.


<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1G</td>
<td>First Generation Technology</td>
</tr>
<tr>
<td>2G</td>
<td>Second Generation Technology</td>
</tr>
<tr>
<td>3G</td>
<td>Third Generation Technology</td>
</tr>
<tr>
<td>4G</td>
<td>Fourth Generation Technology</td>
</tr>
<tr>
<td>AMPS</td>
<td>Advanced Mobile Phone System</td>
</tr>
<tr>
<td>AND</td>
<td>Abbreviated Dialing Number</td>
</tr>
<tr>
<td>ASCII</td>
<td>American Standard Code for Information Interchange</td>
</tr>
<tr>
<td>BMP</td>
<td>Bitmap</td>
</tr>
<tr>
<td>BSS</td>
<td>Base Station System</td>
</tr>
<tr>
<td>CDMA</td>
<td>Code Division Multiple Access</td>
</tr>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>CTIA</td>
<td>Cellular Telecommunications and Internet Association</td>
</tr>
<tr>
<td>DF</td>
<td>Data File</td>
</tr>
<tr>
<td>DOC</td>
<td>Document</td>
</tr>
<tr>
<td>ECPA</td>
<td>Electronic Communication Privacy Act</td>
</tr>
<tr>
<td>EDGE</td>
<td>Enhanced Data Rates for GSM Evolution</td>
</tr>
<tr>
<td></td>
<td>Electrically Erasable Programmable Read Only</td>
</tr>
<tr>
<td>EEPROM</td>
<td>Memory</td>
</tr>
<tr>
<td>EF</td>
<td>Elementary File</td>
</tr>
<tr>
<td>ELP</td>
<td>Extender Language Preferences</td>
</tr>
<tr>
<td>EMS</td>
<td>Enhanced Messaging Service</td>
</tr>
<tr>
<td>EV-DO</td>
<td>Evolution-Data Only</td>
</tr>
<tr>
<td>EXT2</td>
<td>Second Extended File System</td>
</tr>
<tr>
<td>FAT</td>
<td>File Allocation Table</td>
</tr>
<tr>
<td>FDMA</td>
<td>Frequency Division Multiple Access</td>
</tr>
<tr>
<td>FM</td>
<td>Frequency Modulation</td>
</tr>
<tr>
<td>GAN</td>
<td>Generic Access Network</td>
</tr>
<tr>
<td>GIF</td>
<td>Graphics Interchange Format</td>
</tr>
<tr>
<td>GMT</td>
<td>Greenwich Mean Time</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>GPRS</td>
<td>Generalized Packet Radio System</td>
</tr>
<tr>
<td>GSM</td>
<td>Global System for Mobile Telecommunications</td>
</tr>
<tr>
<td>HLR</td>
<td>Home Location Register</td>
</tr>
<tr>
<td>HSPA</td>
<td>High Speed Packet Access</td>
</tr>
<tr>
<td>HTML</td>
<td>Hyper Text Markup Language</td>
</tr>
<tr>
<td>IC</td>
<td>Integrated Circuit</td>
</tr>
<tr>
<td>ICCID</td>
<td>Integrated Circuit Card Identifier</td>
</tr>
<tr>
<td>iDEN</td>
<td>Integrated Digital Enhanced Network</td>
</tr>
<tr>
<td>IM</td>
<td>Instant Messaging</td>
</tr>
<tr>
<td>IMSI</td>
<td>International Mobile Subscriber Identity</td>
</tr>
<tr>
<td>IrDA</td>
<td>Infrared Data Association</td>
</tr>
<tr>
<td>ISDN</td>
<td>Integrated Services Digital Network</td>
</tr>
<tr>
<td>ISO</td>
<td>International Standards Organization</td>
</tr>
<tr>
<td>JPEG</td>
<td>Joint Photographic Experts Group</td>
</tr>
<tr>
<td>KC</td>
<td>Ciphering Key</td>
</tr>
<tr>
<td>LAI</td>
<td>Location Area Information</td>
</tr>
<tr>
<td>LCD</td>
<td>Liquid Crystal Display</td>
</tr>
<tr>
<td>LND</td>
<td>Last Dialed Numbers</td>
</tr>
<tr>
<td>LOCI</td>
<td>Location Information</td>
</tr>
<tr>
<td>MCC</td>
<td>Mobile Country Code</td>
</tr>
<tr>
<td>MD5</td>
<td>Message-Digest algorithm 5</td>
</tr>
<tr>
<td>MF</td>
<td>Master File</td>
</tr>
<tr>
<td>MMS</td>
<td>Multimedia Messaging Service</td>
</tr>
<tr>
<td>MNC</td>
<td>Mobile Network Code</td>
</tr>
<tr>
<td>MP3</td>
<td>Moving Picture Experts Group Layer-3 Audio</td>
</tr>
<tr>
<td>MSC</td>
<td>Mobile Switching Center</td>
</tr>
<tr>
<td>MSIN</td>
<td>Mobile Station Identification Number</td>
</tr>
<tr>
<td>MSISDN</td>
<td>Mobile Subscriber ISDN Number</td>
</tr>
<tr>
<td>N-AMPS</td>
<td>Narrowband AMPS</td>
</tr>
<tr>
<td>NMT</td>
<td>Nordic Mobile Telephony</td>
</tr>
<tr>
<td>NTFS</td>
<td>New Technology File System</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>PCS</td>
<td>Personal Communication Service</td>
</tr>
<tr>
<td>PDA</td>
<td>Personal Digital Assistant</td>
</tr>
<tr>
<td>PDF</td>
<td>Portable Document Format</td>
</tr>
<tr>
<td>PDU</td>
<td>Protocol Data Unit</td>
</tr>
<tr>
<td>PIM</td>
<td>Personal Information Management</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identifier Number</td>
</tr>
<tr>
<td>PLMN</td>
<td>Public Land Mobile Network</td>
</tr>
<tr>
<td>PNG</td>
<td>Portable Network Graphics</td>
</tr>
<tr>
<td>PUK</td>
<td>Personal Unblocking Key</td>
</tr>
<tr>
<td>RAM</td>
<td>Random Access Memory</td>
</tr>
<tr>
<td>ROM</td>
<td>Read Only Memory</td>
</tr>
<tr>
<td>SHA1</td>
<td>Secure Hash Algorithm</td>
</tr>
<tr>
<td>SIM</td>
<td>Subscriber Identity Module</td>
</tr>
<tr>
<td>SMC</td>
<td>Short Message Center</td>
</tr>
<tr>
<td>SME</td>
<td>Short Message Entity</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Message Service</td>
</tr>
<tr>
<td>SMS-GMSC</td>
<td>SMS Getaway MSC</td>
</tr>
<tr>
<td>SMSC</td>
<td>SMS Center</td>
</tr>
<tr>
<td>TACS</td>
<td>Total Access Communications System</td>
</tr>
<tr>
<td>TDMA</td>
<td>Time Division Multiple Access</td>
</tr>
<tr>
<td>TIFF</td>
<td>Tagged Image File Format</td>
</tr>
<tr>
<td>TMSI</td>
<td>Temporary Mobile Subscriber Identity</td>
</tr>
<tr>
<td>TPDU</td>
<td>Transport Protocol Data Unit</td>
</tr>
<tr>
<td>TXT</td>
<td>Text File</td>
</tr>
<tr>
<td>UMTS</td>
<td>Universal Mobile Telecommunications System</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
<tr>
<td>USAPA</td>
<td>United States of America Patriot Act</td>
</tr>
<tr>
<td>USB</td>
<td>Universal Serial Bus</td>
</tr>
<tr>
<td>USIM</td>
<td>Universal Subscriber Identity Module</td>
</tr>
<tr>
<td>USSD</td>
<td>Unstructured Supplementary Service Data</td>
</tr>
<tr>
<td>VLR</td>
<td>Visitor Location Register</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>WATM</td>
<td>Wireless Asynchronous Transfer Mode</td>
</tr>
<tr>
<td>WCDMA</td>
<td>Wideband Code Division Multiple Access</td>
</tr>
<tr>
<td>XML</td>
<td>Extensible Markup Language</td>
</tr>
<tr>
<td>XSL</td>
<td>Extensible Style sheet Language</td>
</tr>
</tbody>
</table>
### GSM SIM Card

<table>
<thead>
<tr>
<th>Properties</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program timestamp</td>
<td>10/19/2008 7:27:44 PM</td>
</tr>
<tr>
<td>Manufacturer</td>
<td>GSM</td>
</tr>
<tr>
<td>Model</td>
<td>GSM SIM card</td>
</tr>
<tr>
<td>Phone name</td>
<td></td>
</tr>
<tr>
<td>Phone number</td>
<td>17865213582</td>
</tr>
<tr>
<td>Service provider name</td>
<td>Not avail</td>
</tr>
</tbody>
</table>

### File System

#### MF

#### DF_GSM

### EF_IMSI (Parsed)

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>International Mobile Subscriber Identity (IMSI)</td>
<td>310410173531241 - United States</td>
</tr>
</tbody>
</table>

### EF_LOCI (Parsed)

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temporary Mobile Subscriber Identity (TMSI)</td>
<td>ff ff ff ff</td>
</tr>
<tr>
<td>Location Area Identity (LAI) network code</td>
<td>310041 - United States</td>
</tr>
<tr>
<td>Location Area Identity (LAI) area code</td>
<td>ff fe</td>
</tr>
<tr>
<td>TMSI timestamp</td>
<td>28</td>
</tr>
<tr>
<td>Location Update Status</td>
<td>not updated</td>
</tr>
</tbody>
</table>

### EF_ICCID (Parsed)

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card Identity</td>
<td>89014103211735312419</td>
</tr>
<tr>
<td>Record number</td>
<td>Name</td>
</tr>
<tr>
<td>---------------</td>
<td>------</td>
</tr>
</tbody>
</table>
| 12            | Read | +55555555555  | 1234567890123456    | 2006-08-22 12:15:00 UTC+1 | &gt; How's it going? I know you have &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;br&gt; &lt;br&gt;&lt;br&gt;&lt;b...
APPENDIX D – MOBILEDIT! SCREENSHOTS
APPENDIX D – BITPIM SCREENSHOTS